

# Contrast ドキュメント

---

May 17, 2023 EOP 3.10.3

本ドキュメントには、Contrast Security の製品の基本の使用方法、サポートされる使用方法、および推奨の使用方法を記載しています。



# 目次

はじめに .....	11
カスタマイズ .....	11
次の手順 .....	13
Contrast の仕組み .....	13
Contrast は開発サイクル全体で使用可能 .....	14
解析手法とデータソース .....	14
Contrast エージェント .....	14
エージェントの設定 .....	14
静的スキャン .....	15
クラウドネイティブアプリケーションの保護 .....	15
インテグレーション .....	15
Contrast を体験する .....	15
Contrast の環境をカスタマイズ .....	16
手順 1：セキュリティテストのためのアプリケーション設定 .....	18
手順 2：攻撃の防御のためのアプリケーション設定 .....	20
手順 3：コードの修正とアプリケーションの再テスト .....	22
Contrast Assess .....	22
機能 .....	23
カスタマイズ .....	23
Contrast SCA .....	23
機能 .....	23
Contrast データ .....	24
Contrast Protect .....	24
Contrast Protect の仕組み .....	25
カスタマイズ .....	25
Contrast Scan .....	25
機能 .....	26
関連項目 .....	26
Contrast Serverless .....	26
機能 .....	27
利点 .....	27
仕組み .....	27
セキュリティとプライバシー .....	27
関連項目 .....	28
パフォーマンス .....	28
Community Edition (CE) .....	29
Community Edition の機能 .....	29
Community Edition ポータルサイト .....	29
次の手順 .....	30
エージェント .....	31
エージェントのインストールを始める .....	32
Java .....	33
.NET Framework .....	33
.NET Core .....	33
Node .....	34
PHP .....	34
Python .....	34
Ruby .....	34
Go .....	35
エージェントのインストールと設定 .....	35
インストール .....	35
設定 .....	35
優先順位 .....	36

エージェントキーの検索 .....	37
YAML 設定 .....	38
エージェント設定エディタ .....	39
エージェントオペレータ(Kubernetes オペレータ) .....	41
環境変数 .....	56
Java (Kotlin、Scala) .....	57
サポート対象テクノロジー .....	57
インストール .....	59
設定 .....	78
旧 Java エージェント .....	136
Java エージェントのテレメトリ .....	136
.NET Framework .....	137
サポート対象テクノロジー .....	137
システム要件 .....	138
インストール .....	139
設定 .....	152
IIS Express で使用 .....	185
Azure で使用 .....	185
Azure Service Fabric .....	186
プロファイラチェーン .....	187
.NET エージェントエクスプローラ .....	189
.NET Framework Contrast トレイ .....	191
アプリケーションプール .....	193
テレメトリ .....	194
.NET Core .....	195
サポート対象テクノロジー .....	196
システム要件 .....	197
インストール .....	198
設定 .....	213
.NET エージェントエクスプローラ .....	243
プロファイラチェーン .....	245
テレメトリ .....	246
Azure Functions .....	248
Node.js .....	250
Contrast サービス .....	250
サポート対象テクノロジー .....	251
システム要件 .....	252
インストール .....	253
設定 .....	262
コンテナ起動時間の短縮 .....	294
ESM で Node.js エージェントを使用する .....	295
トランスパイラ、コンパイラ、ソースマップ .....	296
テレメトリ .....	297
PHP .....	297
サポート対象テクノロジー .....	298
システム要件 .....	298
インストール .....	298
設定 .....	301
Python .....	316
システム要件 .....	316
サポート対象テクノロジー .....	317
インストール .....	317
設定 .....	319
テレメトリ .....	392
Ruby .....	392

システム要件	393
サポート対象テクノロジー	393
インストール	395
設定	397
テレメトリ	450
Go	450
サポート対象テクノロジー	451
システム要件	451
インストール	451
設定	456
Contrast サービス	472
インストール	472
設定	473
インストール	474
設定	474
ユーザガイド	476
ユーザの設定	477
ログイン	477
パスワードの変更	477
2段階認証	478
プロファイルの管理	478
API キーの確認	478
通知の管理	479
権限の表示	480
アプリケーション	480
表示	480
アプリケーションの設定の編集	484
タグ	484
マージ	485
アーカイブ	486
リセット	487
削除	488
セッションメタデータ	489
ルートカバレッジ	492
フローマップ	497
スキャン	499
Contrast Scan リリース情報	499
スキャンのプロセス	500
Contrast Scan のサポート対象テクノロジー	502
スキャンパッケージの準備	502
スキャンプロジェクトの作成	503
スキャンプロジェクトの削除	504
スキャンの開始	505
スキャンのキャンセル	506
スキャンの確認	506
Contrast Scan ローカルエンジン	507
結果の分析	513
スキャンポリシーの表示	524
スキャン設定の変更	524
スキャンプロジェクトのアーカイブ	524
スキャンプロジェクトのアーカイブ解除	525
ビルドパイプラインでのインテグレーション	525
サーバ	528
サーバの設定	528
設定ファイルの定義	529

エージェントの設定手順 .....	529
オプションの設定 .....	529
設定 .....	530
Syslog への出力 .....	531
ライブラリ .....	534
関連項目 .....	535
ライブラリの表示 .....	535
検出と削除 .....	537
タグ .....	538
送信 .....	539
ランタイムライブラリの使用状況 .....	540
エクスポート .....	541
オープンソースライセンス .....	543
依存関係ツリーの表示 .....	543
ライブラリのスコアガイド .....	544
CVE 検索 .....	545
サーバレス .....	545
関連項目 .....	546
インベントリ .....	546
Contrast Serverless のサポート対象の言語 .....	546
Contrast Serverless のサポート対象のプラットフォーム .....	546
スキャンの種類と監視について .....	546
AWS で使い始める .....	547
Azure で使い始める .....	554
オンデマンドで関数をスキャン .....	555
結果の表示 .....	556
インベントリ基準の変更 .....	561
サーバレスのスキャン設定の変更 .....	562
関数とサービスの関係の表示 .....	562
コンテキストのリスクスコア .....	565
Contrast Serverless のアップグレード .....	567
アカウントのブロック .....	571
オフボード .....	571
アンインストール .....	572
Contrast CLI .....	572
開始する前に .....	572
Contrast CLI について .....	572
Contrast CLI のサポート対象言語とパッケージマネージャ .....	573
Contrast CLI のインストール .....	573
Contrast CLI の実行 .....	574
Contrast CLI コマンド .....	575
旧 Contrast CLI .....	579
脆弱性 .....	587
組織の表示 .....	587
アプリケーションの脆弱性の表示 .....	588
脆弱性の発生率の表示 .....	590
脆弱性の削除 .....	591
シンクで脆弱性をグループ化 .....	592
脆弱性のマージ .....	592
タグ .....	592
追跡 .....	594
イベント .....	595
修正 .....	596
エクスポート .....	596
ステータス .....	598

深刻度の変更 .....	602
プロジェクト .....	602
関連項目 .....	603
攻撃 .....	603
イベントデータの保持 .....	603
操作 .....	604
攻撃の表示 .....	604
攻撃の監視 .....	606
攻撃の管理 .....	607
攻撃にタグを付ける .....	609
攻撃スクリプトの実行 .....	610
レポート .....	611
コンプライアンス対応レポート .....	611
セキュリティ基準レポート .....	613
DISA STIG Viewer チェックリスト .....	613
SBOM(ソフトウェア部品表) .....	614
脆弱性の傾向レポート .....	615
組織の統計値 .....	617
インテグレーション .....	618
クラウドでの連携 .....	618
チャットツール .....	619
コードリポジトリとの連携 .....	620
継続的インテグレーション(CI)とビルドツール .....	621
エンタープライズおよび拡張 .....	622
IDE プラグイン .....	624
インシデント管理システム .....	625
SIEM ツール .....	626
作業管理プラットフォーム .....	627
Azure Boards .....	628
関連項目 .....	629
接続 .....	629
チケットの自動作成 .....	629
双方向インテグレーション .....	630
個人用アクセストークン .....	631
Agile Central .....	631
認証情報の管理 .....	632
Azure Pipelines .....	633
インストールと設定 .....	633
タスクの設定 .....	633
リリースゲートの追加 .....	634
Azure Service Fabric .....	635
Bamboo .....	636
インストール .....	636
しきい値の設定 .....	637
Bugzilla .....	637
Eclipse .....	638
Generic Webhook .....	639
Generic Webhook .....	639
変数 .....	641
イベントと変数 .....	643
GitHub .....	644
Gradle .....	645
サンプルアプリケーション .....	645
プラグインの使用 .....	646
IntelliJ プラグイン .....	646

IntelliJ プラグインをインストールして設定し、使用するには :	647
IntelliJ で Java エージェントを設定	647
Jenkins	647
Jenkins プラグインのインストールと使用	648
関連項目	648
接続の定義	648
システムレベルのセキュリティ制御	649
ジョブレベルのセキュリティ制御	650
パイプラインのセキュリティ制御	650
Jenkins でのセキュリティ制御	652
ジョブ結果ポリシーの定義	652
ビルドの実行	656
Jira	656
関連項目	656
Jira に接続する	656
Assess と Jira の設定	657
サーバレスと Jira の設定	658
認証情報の管理	660
Maven	661
関連項目	661
Microsoft Teams	661
PagerDuty	662
Solutions Business Manager	663
Slack	663
VictorOps	664
Visual Studio	664
Visual Studio Code	665
Visual Studio for Mac	666
管理ガイド	668
ルールとポリシー	668
Assess ルール	670
セキュリティ制御	671
脆弱性ポリシー	674
Protect ルール	680
CVE シールド	684
仮想パッチ	689
ログエンハンサー	690
アプリケーションの例外	692
コンプライアンスポリシー	695
IP の管理	696
ライブラリポリシー	698
機密データのマスクング	699
通知	701
組織	701
Assess を有効にする	701
Protect を有効にする	702
設定	704
通知	716
レポート	719
スコア	719
Scan のアクセス制御	719
脆弱性の承認	735
監査ログの表示	736
なりすまし	739
システム管理(EOP)	741



はじめに .....	741
Contrast のインストール .....	742
次の手順 .....	742
Contrast のシステム要件 .....	742
サイジングの推奨 .....	743
curl で Contrast をダウンロード .....	744
Contrast インストーラのダウンロード .....	745
インストール .....	746
WAR ファイルを使用して Contrast をデプロイ .....	749
分散型 MySQL .....	750
分散環境の構成 .....	753
Contrast の実行 .....	756
認証情報の管理 .....	756
Contrast の再起動 .....	757
アンインストール .....	757
インストール後の作業 .....	758
インストール後の作業 .....	758
Tomcat .....	758
JRE .....	759
HTTPS の設定 .....	759
MySQL のカスタマイズ .....	762
プロキシ構成の設定 .....	762
レポート用ストレージの設定 .....	764
Contrast のログ .....	765
Redis を共有キャッシュに使う(オンプレミス版) .....	766
システムの更新とアップグレード .....	767
更新およびアップグレード .....	768
Contrast のアップグレード .....	768
エージェントのアップグレード(オンプレミス版) .....	769
IP アドレスの更新 .....	769
SCA ライブラリデータを手動で更新 .....	770
SCA ライブラリデータを自動で更新 .....	771
Contrast ライセンスの更新 .....	771
運用管理 .....	772
複数の組織の管理 .....	773
組織の追加/編集 .....	774
ユーザと権限 .....	775
ユーザの追加 .....	776
複数ユーザの追加 .....	777
SuperAdmin の指定 .....	778
アクセスグループの追加 .....	779
Protect 権限の付与(オンプレミス版) .....	780
ユーザの自動追加 .....	781
認証情報の管理 .....	783
ユーザのなりすまし .....	784
認証 .....	785
2 段階認証 .....	786
Active Directory .....	786
LDAP .....	790
SSO .....	795
HTTPS プロキシ .....	798
パスワード .....	798
キー .....	800
システムの設定 .....	800
手順 .....	801

その他のシステム設定 .....	801
全般的な設定 .....	802
診断サービス .....	802
ライセンス .....	803
スコア .....	806
ライブラリコンプライアンスポリシー .....	806
メール .....	807
メンテナンス .....	807
暗号化プロパティエディタ .....	807
MySQL のバックアップ .....	809
SSL の管理 .....	811
リファレンス .....	813
用語集 .....	813
ルールと権限 .....	817
アプリケーションルール .....	817
組織ルール .....	819
システムルール .....	821
アプリケーションのスコアガイド .....	822
ライブラリのスコアガイド .....	823
ログレベル .....	824
イベントと変数 .....	824
変数 .....	825
正規表現 .....	827
対応ブラウザ .....	827
ベータ版利用規約 .....	828
プライバシーとデータの収集 .....	828

# はじめに

Contrast へようこそ！

Contrast は、ソフトウェア開発ライフサイクル(SDLC)の全てのフェーズで、リアルタイムのアプリケーションセキュリティを提供します。

Contrast の使用例として、[Contrast を体験する \(15ページ\)](#)を参照ください。

ご要望は...	Contrast が提供するのは...
<p>SDLC の開発フェーズ・テスト(QA)フェーズでアプリケーションの脆弱性を分析したい：</p> <ul style="list-style-type: none"> <li>開発フェーズで：アプリケーションや使用するライブラリの脆弱性に関する高精度なフィードバックを即座に得たい アプリケーションを実行することで、アプリケーション内の疎通ルートをシミュレートし、Contrast からの情報を使用して安全なコードをチェックイン</li> <li>テストフェーズで：手動・自動化されたテストケースを適用する時や、CI/CD パイプラインにおいて、アプリケーションの脆弱性は検証済みであることを保証したい</li> <li>本番環境で：SDLC の運用フェーズで、攻撃を完全に把握し、悪意のある不正利用からアプリケーションを防御したい</li> </ul>	<ul style="list-style-type: none"> <li><a href="#">エージェント (31ページ)</a>：アプリケーションにセンサーを搭載し、解析します。さまざまなプログラミング言語、フレームワーク、コンテナテクノロジーをサポートします。</li> <li><a href="#">Contrast Assess (22ページ)</a>：調整可能な検出ルールを使用して、脆弱性を高精度に検出します。問題が検出された経緯、再現方法、修正方法についての情報を提供します。</li> <li><a href="#">Contrast Scan (25ページ)</a>：高速で効率的な静的スキャンの実行により、アップロードされたバイナリパッケージの脆弱性を特定します。</li> <li><a href="#">Contrast Protect (24ページ)</a>：攻撃を自動的に特定し、本番環境での攻撃を監視したり悪用されるのを防ぎます。Protect は実行中のアプリケーション内から攻撃を検知してブロックしますが、WAF(Web アプリケーションファイアウォール)と統合することもできます。</li> </ul>
<p>アプリケーションが使用するライブラリを解析したい</p>	<p><a href="#">Contrast SCA : (23ページ)</a> アプリケーションの実行時に使用されるオープンソースライブラリがもたらすセキュリティリスクや法的な問題を可視化します。Contrast SCA は、オープンソースライブラリの脆弱性を検出します。また、使用中のライブラリが古く、更新する必要があるかどうかも明らかにします。</p>
<p>SDLC の早い段階でコードの脆弱性を見つけ、その修正方法について分かりやすい説明が知りたい</p>	<p>Contrast Assess、Scan、SCA で検出された脆弱性 (<a href="#">587ページ</a>)の情報は、<a href="#">修正方法 (596ページ)</a>が記載されます。</p>
<p>組織内や組織外でデータやリソースが共有されている箇所をインタラクティブに表示するアーキテクチャを図で見たい</p>	<p><a href="#">フローマップ (497ページ)</a>により、アプリケーション、アプリケーション内のテクノロジー層、アプリケーションが接続しているバックエンドシステムなどを表す詳細な構成図を参照できます。</p>
<p>CI/CD パイプラインに Contrast を組み込みたい</p>	<p>多種多様な <a href="#">インテグレーション (618ページ)</a>機能により、Contrast の処理やデータを、開発者用の IDE やビルドシステム、コミュニケーションツールなどと連携することができます。</p>

## カスタマイズ

Contrast にはさまざまなオプションがあり、Contrast に登録したアプリケーションのデータアクセスやデータ表示、データ収集などをカスタマイズできます。カスタマイズすることにより、Contrast で提供されるデータをより分かりやすく効果的に参照できるようになります。

オプション	説明
ロールベースのアクセス制御	<p> <a href="#">アクセスグループ (708ページ)</a>を使用すると、特定のユーザに権限と機能を割り当てることができます。グループに関連付けたアプリケーションごとに、役割(ロール)に応じた異なる種類のアクセス権を割り当てることができます。                 </p> <p>                     Contrast にアプリケーションを登録する前に、グループ構成を検討しておくとう便利です。                 </p> <p>                     最初にアプリケーションを Contrast に登録する際に、Contrast 設定ファイルにグループを指定しない場合は、Contrast Web インターフェイスからのみグループに追加できます。Contrast 設定ファイルを使用してアプリケーションを登録したい場合は、アクセスグループに関連付けるために、アプリケーションを一度削除してから再度登録する必要があります。                 </p> <p>                     まず、Contrast Web インターフェイスで、既存のグループにユーザやアプリケーション(またはその両方)を作成または追加します。                 </p> <p>                     次に、各アプリケーションの Contrast 設定ファイルを使用して、アプリケーションをアクセスグループに関連付けて Contrast に登録することができます。                 </p> <pre data-bbox="520 633 1385 757">                     # application:                      # Add the name of the application group with which this                     # application should be associated in the Contrast UI.                     # group: NEEDS_TO_BE_SET                 </pre>
カスタムフィルタ	<p>                     Contrast では、カスタマイズしたフィルタを作成できるタグオプションがいくつかあります。カスタムフィルタを作成する利点は、デフォルトのフィルタを使用するだけでなく、特定のニーズに合わせてデータを表示できることです。                 </p> <p> <a href="#">アプリケーションのメタデータ (715ページ)</a>を使用して、カスタムフィルタを作成できます。                 </p> <p>                     また、特定の<a href="#">アプリケーション (484ページ)</a>データや<a href="#">脆弱性 (592ページ)</a>情報にタグを適用することもできます。アプリケーションや脆弱性にタグを付けた後は、アプリケーションのページや脆弱性のページでフィルタとしてそれらのタグを使用できます。                 </p> <p> <b>例：アプリケーションメタデータ</b> </p> <p>                     アプリケーションのメタデータを収集するために、Contrast Web インターフェイスでカスタムフィールドを作成できます。以下は、フリーフォーマットのカスタムフィールドの例です。                 </p> <ul data-bbox="520 1122 863 1283" style="list-style-type: none"> <li>• <b>カスタムフィールド</b> : managersInfo 値 : "John Doe"</li> <li>• <b>カスタムフィールド</b> : businessUnit 値 : "NodeGoat Group"</li> <li>• <b>カスタムフィールド</b> : officeLocation 値 : "New York City"</li> </ul> <p> <b>例：アプリケーションのタグ</b> </p> <ul data-bbox="520 1361 1262 1469" style="list-style-type: none"> <li>• <b>Appname</b> : 特定のアプリケーション名</li> <li>• <b>Groupname</b> : アクセスグループの名前</li> <li>• <b>Environment</b> : アプリケーションをテストする環境(開発、QA、または本番環境)</li> <li>• <b>Server Name</b> : アプリケーションをホストするサーバの名前</li> </ul> <p> <b>例：脆弱性のタグ</b> </p> <ul data-bbox="520 1547 863 1601" style="list-style-type: none"> <li>• <b>Build</b> : 特定のビルド番号</li> <li>• <b>Version</b> : 特定のリリースバージョン</li> </ul>

オプション	説明
アプリケーションのカスタムデータ	<p><a href="#">セッションメタデータ (489ページ)</a>により、アプリケーションの脆弱性のソースを特定できます。</p> <p>セッションメタデータに必要なプロパティをエージェントの設定ファイルに追加すると、標準の脆弱性データと一緒に、セッションメタデータがエージェントにより報告されるようになります。そして、そのセッションメタデータを Contrast Web インターフェイスでフィルタとして使用することができます。</p> <p>Contrast エージェントの設定ファイル内でセッションメタデータの値を変更すると、異なる値で脆弱性データをフィルタ処理できます。例えば、ブランチ名やバージョンの値を変更すると、異なるブランチやバージョンでデータをフィルタできます。</p> <p><b>例：</b></p> <p>以下の Java アプリケーションの例では、javaagent フラグを追加する行にエントリを追加しています。この例では、<code>contrast.application.session_metadata</code> プロパティにブランチ名 (<code>branchName</code>)、コミットしたユーザ (<code>committer</code>)、リポジトリ (<code>repository</code>) のメタデータプロパティに対して、キーと値をペアにして指定しています。</p> <pre>-Dcontrast.application.session_metadata="branchName=build22,committer=Jane,repository=Contrast-Java"</pre>
名前のカスタマイズ	<p><a href="#">アプリケーション (484ページ)</a> や <a href="#">アプリケーションをホストするサーバ (530ページ)</a> の名前を変更することができます。</p> <p>デフォルトでは、Contrast エージェントがコード内で検出したデータに基づいて名前が付けられます。</p> <p>カスタム名を指定するには、<a href="#">アプリケーションを追加 (35ページ)</a> する際にエージェント設定ファイルで指定するか、アプリケーションを追加した後に Contrast Web インターフェイスで名前を変更します。</p>

## 次の手順

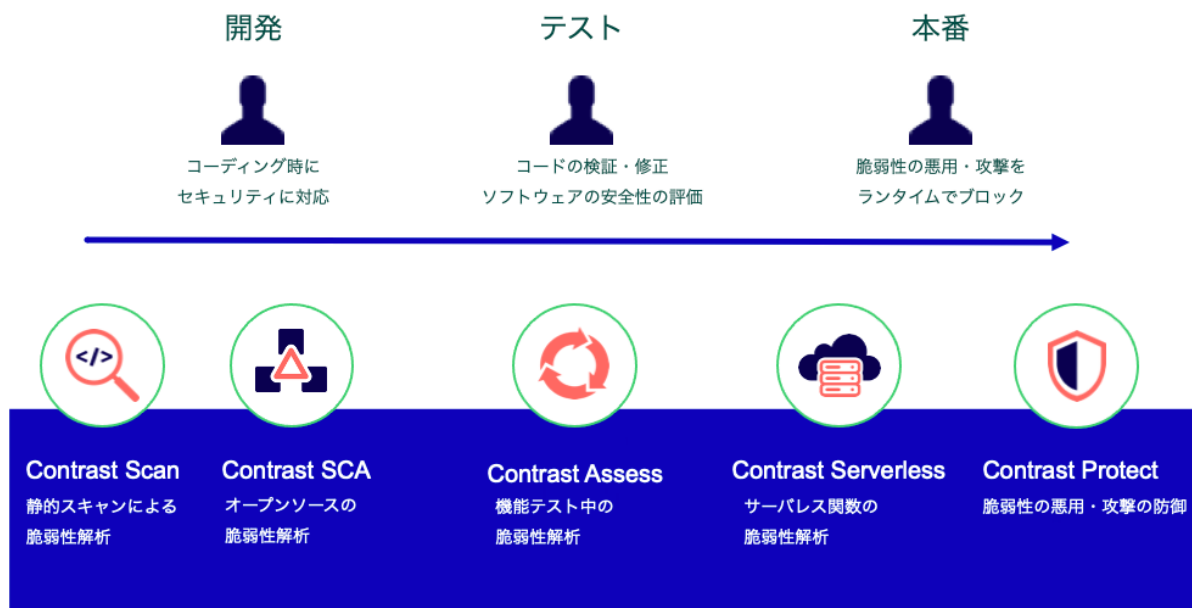
- [Contrast の仕組み \(13ページ\)](#) について概要を把握する
- [Contrast を無料で試す - Community Edition \(CE\) \(29ページ\)](#)
- [Contrast エージェントをインストール・設定する \(35ページ\)](#)
- [Contrast をインストールする\(オンプレミス版\) \(741ページ\)](#)
- [特定のツールやテクノロジーとインテグレーション \(618ページ\)](#) する

## Contrast の仕組み

Contrast Security は、アプリケーションポートフォリオにおいて、高精度で継続的なリアルタイムのアプリケーションセキュリティテストと攻撃のブロックを実現可能にします。Contrast が各アプリケーション内で動作し、ソフトウェア開発ライフサイクル(SDLC)全体を通して、アプリケーションを安全なものにします。

Contrast を使用して実施する機能テストがセキュリティテストになります。そのため、品質管理の作業としてアプリケーションを疎通するたびに、セキュリティフィードバックを得ることができます。Contrast の結果は継続的かつリアルタイムに得られるため、ソースコードから実行中のアプリケーションまで、開発パイプライン全体にセキュリティを統合することができます。

## Contrast は開発サイクル全体で使用可能



### 解析手法とデータソース

Contrast では、以下のように様々なデータソースと解析手法が統合されています。

- ランタイムの制御フローやデータフロー(IAST)
- アプリケーションのコードや API(SAST)
- HTTP リクエストとレスポンス
- アプリケーション内の全てのライブラリおよびフレームワークとその使用状況(SCA)
- 設定情報
- バックエンドの接続状況
- ローカルファイルの静的スキャン(SAST)

### Contrast エージェント

Contrast Assess と Contrast Protect は、[エージェント \(31ページ\)](#)を使用してデータフローを解析し、実行中のアプリケーションから脆弱性を検出します。Contrast Assess と Contrast Protect は、同じエージェントを使用して、データフローの解析や脆弱性の検出を行います。Assess 用のエージェントと Protect 用のエージェントの両方が必要になるわけではありません。

[エージェントを追加・設定する \(35ページ\)](#)と、カスタムコードやライブラリ全体にわたって、アプリケーションの既存のメソッドに Contrast のセンサーが組み込まれることになります。エージェントのセンサーは、データがアプリケーションに入って出る場所(ルート)を観測します。この動作により、アプリケーションのデータの流れがリアルタイムに可視化され、そのコードパスにあるセキュリティ上の欠陥や脆弱性が検出されて、Contrast に報告されます。また、エージェントによって Contrast は攻撃を検知して、攻撃のブロックが可能になります。

### エージェントの設定

エージェントの設定は、YAML 設定ファイルの編集、コマンドラインでの環境変数の使用、または使用している言語やツールに固有のその他の方法で行います。

アプリケーションにエージェントを設定する際に、以下の情報を指定します。

- エージェントが Contrast と通信するための情報
- エージェント固有の設定

- Assess および Protect ルールの設定
- アプリケーション固有の設定
  - ここでの設定には、セッションメタデータやカスタムメタデータも含まれます。メタデータは、報告された各脆弱性の追加情報として、またはフィルタとして利用できます。
- アプリケーションとエージェントをホストするサーバ：
  - 統合開発環境(IDE)で実行している開発者のローカルアプリケーションサーバ
  - 自動テストプロセスで使用している CI(継続的インテグレーション)アプリケーションサーバ
  - アプリケーションのテストサーバ
  - アプリケーションのステージングサーバ
  - アプライアンスに組み込まれているサーバ
  - 仮想マシンで実行中のアプリケーションサーバ
  - クラウドで実行中のリモートアプリケーションサーバ
  - 本番環境用のアプリケーションサーバ

## 静的スキャン

[Contrast Scan \(499ページ\)](#)は、ソフトウェア開発ライフサイクル(SDLC)の開発フェーズにおいて、脆弱性の検出と修正を容易にする静的アプリケーションセキュリティテスト(SAST)ツールです。

アプリケーションをスキャンするには、[ソースコードがバイトコードファイルをアップロード \(503ページ\)](#)します。Contrast のテクノロジーにより、Contrast が定義済した一連のルールに基づいて脆弱性が特定されます。

## クラウドネイティブアプリケーションの保護

[Contrast Serverless \(26ページ\)](#)は、サーバレススペースのアプリケーションを対象とした、次世代のアプリケーションセキュリティテストツールです。

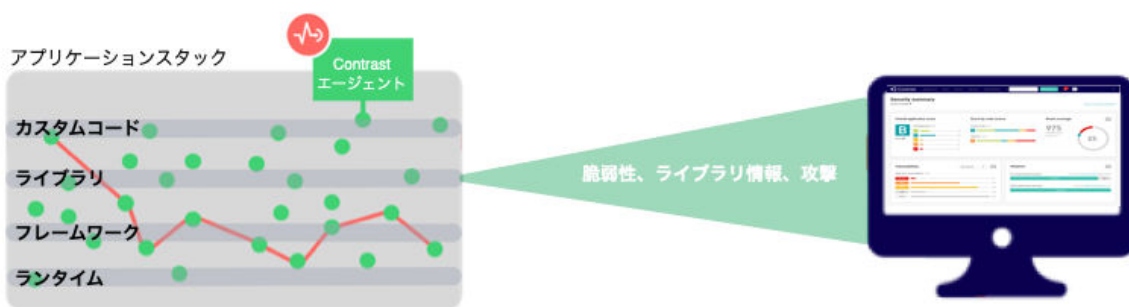
Contrast Serverless は、クラウドネイティブアーキテクチャを使用して環境内の全てのリソースをマッピングし、自動的にその結果を検証して優先順位付けを行い、誤検知や不用なアラートを解消します。AWS アカウントに読み取りモードで接続し、継続的に環境を監視し、関連情報を収集します。

## インテグレーション

Contrast は、さまざまなツールやテクノロジーと[インテグレーション \(618ページ\)](#)できるため、現在ご利用中のツールから脆弱性に関する高精度なフィードバックを得ることができます。このアプローチにより、セキュリティチームと開発チーム間の連携が効果的に促進され、ソフトウェアの開発プロセスが加速します。

## Contrast を体験する

Contrast を使用して、重大な脆弱性がコードに導入されるのを防ぎ、アプリケーションを攻撃から守る方法について詳しく見ていきましょう。



本項では、Contrast Java エージェントを使用して、アプリケーションを疎通しながらセキュリティテストと攻撃の防御を行うために、アプリケーションを設定する例をご紹介します。

## Contrast の環境をカスタマイズ

Contrast Web インターフェイスにアクセスできるようになったら、Contrast データへのアクセス制御や重大な検査結果の検索が簡単にできるように、環境をカスタマイズすることを検討しましょう。

### アクセスグループ

例えば、お使いの財務アプリケーションに 3 つの担当が関与しているとします。その場合、これら 3 つの担当用のアクセスグループを作成し、Contrast の設定ファイルに指定します。

- **Team1-Dev** は開発者向けで、次のような設定をします。

### 👤 グループを追加

グループ名

アプリケーションアクセス

[+ アクセスを追加](#)

開発者には、検出結果の修正、タグの追加、脆弱性の管理、属性の編集、アプリケーションのマージ、アプリケーションの追加・削除、サーバの作成などを可能にします。



- **Team2-Test** はテスト担当用で、次のような設定をします。

### グループを追加

---

グループ名

アプリケーションアクセス

 View ▼

[+ アクセスを追加](#)

テスト担当者は、スコア、ライブラリ、脆弱性、コメントの参照が可能で、アプリケーションのトレースの編集はできません。

- **Team3-AppSec** はアプリケーションセキュリティ担当用で、次のような設定をします。

### グループを追加

---

グループ名

アプリケーションアクセス

 Rules Admin ▼

[+ アクセスを追加](#)

アプリケーションセキュリティ担当には、アプリケーションのルールやポリシーの編集、Protect の有効化、組織の通知やスコア付けの管理ができるようにします。

## アプリケーション名とサーバ名

すべての担当が同じアプリケーションで作業しているため、Contrast の各設定ファイルには同じアプリケーション名を使用することになります。開発環境用に 1 つの設定ファイル、テスト環境用に 1 つの設定ファイルを使用する予定です。

2 つの設定ファイルを使用することになりますが、両方の設定ファイルでアプリケーションに同じ名前を指定するため、Contrast ではアプリケーションのインスタンスが 1 つしかないかのようにデータが表示されることになります。

サーバ名は指定せずに、Contrast で検出される名前をそのまま使用することになります。

## セッションメタデータ

アプリケーションに関して、特定のブランチ、コミットしたユーザ、リポジトリなどに対する脆弱性やルート情報を表示することができます。このような情報を収集するには、Contrast の設定ファイルでセッションメタデータの値を定義します。

```
-Dcontrast.application.session_metadata="branchName=release24,committer=Jane,repository=finapp-Java"
```

## 手順 1: セキュリティテストのためのアプリケーション設定

開発時には、開発者が安全なコードをチェックインしていることを確実にしたいと考えます。また、テスト中には、本番環境での攻撃を可能にする脆弱性がアプリケーションにないことを検証したいと考えます。

Contrast をアプリケーションに追加して、製品を一般公開する前に必要なセキュリティテストを行うことにしました。アプリケーションは Java を使用しているため、Contrast の Java エージェントを使用することになります。

1. ビルドプロセスに Maven を使用しているため、Maven Central リポジトリから [Contrast エージェントをダウンロード \(60ページ\)](#) します。また、Contrast の Web インターフェイスから [YAML 設定ファイル \(38ページ\)](#) をダウンロードします。
2. 開発環境では YAML 設定ファイルを編集して、次のような設定をします。

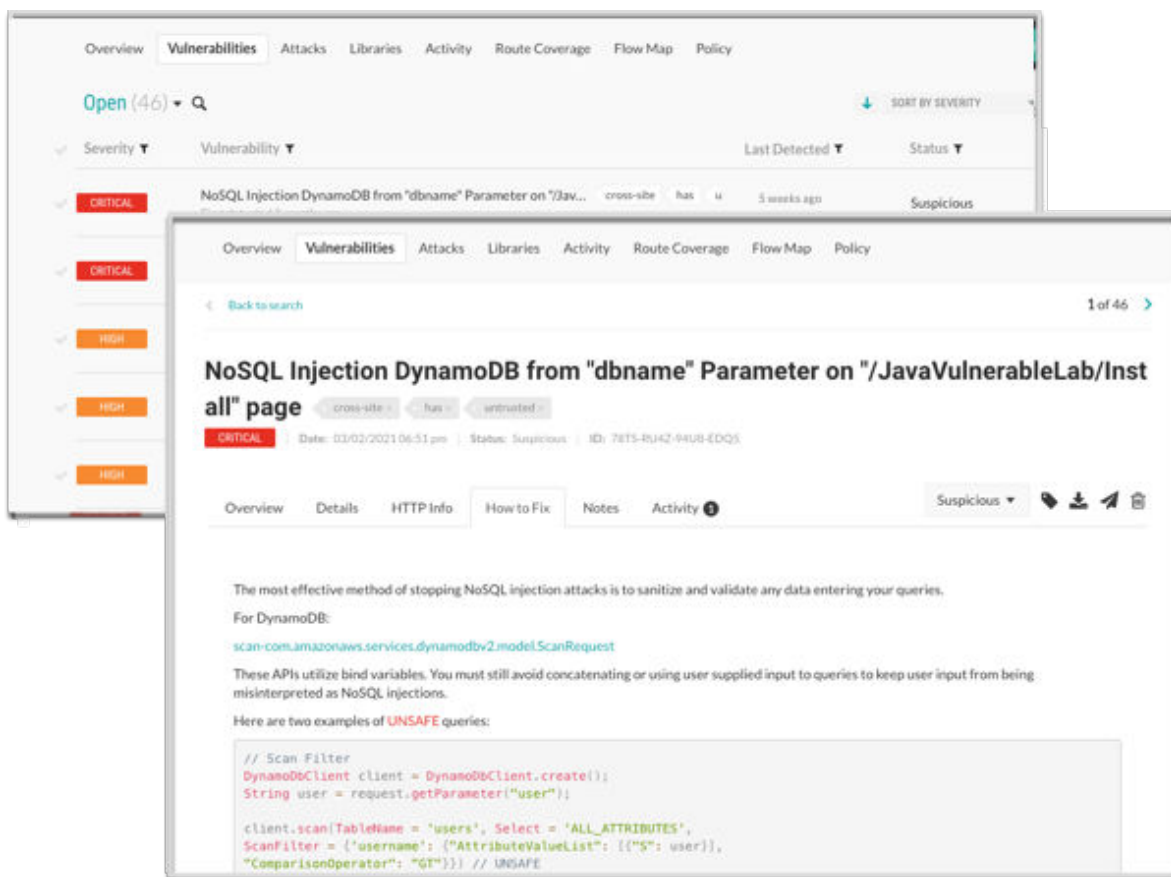
```
api:
  # ***** REQUIRED *****
  # Set the URL for the Contrast UI.
  url:https://mycontrast.mycompany.com:8080/Contrast/
  # ***** REQUIRED *****
  # Set the API key needed to communicate with the Contrast UI.
  api_key:A2xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxG9N
  # ***** REQUIRED *****
  # Set the service key needed to communicate with the Contrast
  # UI. It is used to calculate the Authorization header.
  service_key:service_key:88xxxxxxxxxxxxx5Z
  # ***** REQUIRED *****
  # Set the user name used to communicate with the Contrast
  # UI. It is used to calculate the Authorization header.
  user_name:agent_xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx@mydevorg
.
.
.
# \
=====
====
# server
# Use the properties in this section to set
# metadata for the server hosting this agent.
# \
=====
====
# server:
  # Override the reported server environment.
  environment: development
.
.
.
```

3. テスト環境では YAML 設定ファイルを編集して、次のような設定をします。

```
api:
  # ***** REQUIRED *****
  # Set the URL for the Contrast UI.
  url:https://mycontrast.mycompany.com:8080/Contrast/
  # ***** REQUIRED *****
  # Set the API key needed to communicate with the Contrast UI.
  api_key:A2xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxG9N
  # ***** REQUIRED *****
  # Set the service key needed to communicate with the Contrast
  # UI. It is used to calculate the Authorization header.
  service_key:service_key:88xxxxxxxxxxxx5Z
  # ***** REQUIRED *****
  # Set the user name used to communicate with the Contrast
  # UI. It is used to calculate the Authorization header.
  user_name:agent_xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx@mydevorg
.
.
.

# \
=====
=====
# server
# Use the properties in this section to set
# metadata for the server hosting this agent.
# \
=====
=====
# server:
# Override the reported server environment.
environment: QA
.
.
.
```

4. 次に、アプリケーションを起動して機能テストを実行し、アプリケーションやビジネスロジックで公開されるの全ルートとデータエンドポイントを疎通します。
5. まず、Contrast Web インターフェイスの「アプリケーション」のページにアクセスして、Contrast でアプリケーションが認識されていることを確認します。次に、脆弱性の有無を確認し、脆弱性に対しては修正方法を参照してコードを安全にするための修正や対策を決めます。



- 最初のテストの後に、CI/CD プロセスで Contrast と連携するために [Maven プラグイン \(661ページ\)](#) を使用することになりました。この連携では、深深度がまたはの脆弱性を Contrast が検出した場合にビルドが失敗するように設定します。

## 手順 2：攻撃の防御のためのアプリケーション設定

開発とテストの段階で Contrast を使用してきましたが、ユーザが製品を使用する際に悪意のある行為を受けないようにしたいと思います。アプリケーション、ユーザ、およびデータを保護するために、本番環境にあるアプリケーションに Contrast を追加することになりました。

まず Protect ライセンスがあり、組織で Protect が有効になっていることを確認します。

開発時とテスト時にアプリケーションにエージェントをインストールして設定した方法と同様に、本番環境でも Contrast の Protect を有効にするための新しい設定ファイルが必要になります。新しい設定ファイルを作成した後にアプリケーションを実行し、Contrast Web インターフェイスに本番環境のアプリケーションが表示されることを確認します。

```
api:
# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url:https://mycontrast.mycompany.com:8080/Contrast/
# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key:A2xxxxxxxxxxxxxxxxxxxxxxxxG9N
# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key:service_key:88xxxxxxxxxxxxx5Z
# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
```

```
user_name:agent_XXXXXXXX-XXXX-XXXX-XXXX-XXXXXXXXXXXX@myprodorg
.
.
.
# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:
# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: true
.
.
.
# \
=====
==
# server
# Use the properties in this section to set
# metadata for the server hosting this agent.
# \
=====
==
# server:
# Override the reported server environment.
environment: production
.
.
.
```

アプリケーションが本番運用になったら、Contrast Web インターフェイスの「攻撃」ページを参照して、攻撃が発生していないか監視します。

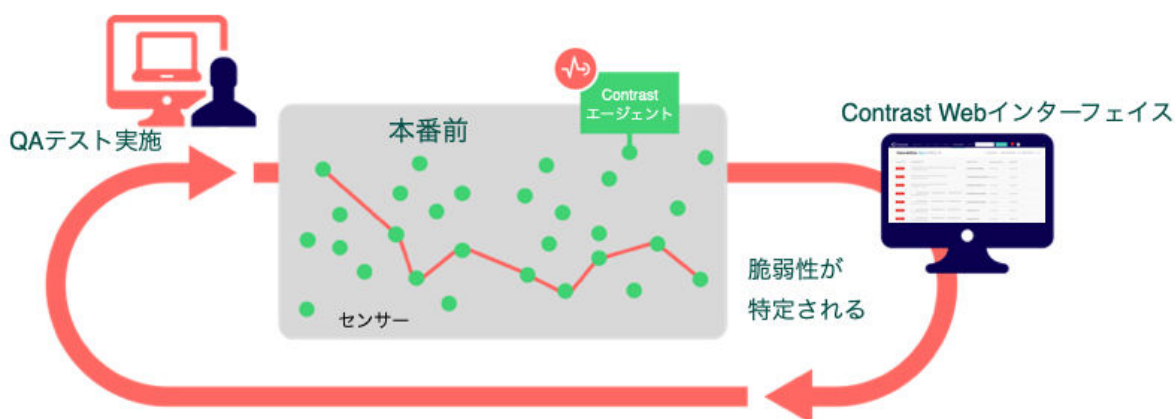
Source IP	Status	Application	Server	Rule	Start	End	Events
01	EXPLOITED	Cat-Engine-2	Cat-Server	Command Injection Cross-Site Scripting Path Traversal	5 hours ago	5 hours ago	55
01	EXPLOITED	Cat-Engine-2	Cat-Server	Command Injection Cross-Site Scripting Path Traversal	8 hours ago	8 hours ago	22
01	EXPLOITED	Cat-Engine-2	Cat-Server	Command Injection Cross-Site Scripting Path Traversal	a day ago	a day ago	11
01	EXPLOITED	Cat-Engine-1 Cat-Engine-2	Cat-Server	Command Injection Cross-Site Scripting Path Traversal	5 days ago	5 days ago	66
01	BLOCKED IP!	Grape-on-rack	Grape-Server	Cross-Site Scripting	7 days ago	7 days ago	8

### 手順 3 : コードの修正とアプリケーションの再テスト

Contrast を使用したテストの結果や検知された攻撃を調査したら、アプリケーションのコードを修正します。アプリケーションの最新バージョンが Contrast に表示されていることを確認します。アプリケーションの最新バージョンに、本番環境でブロックした脆弱性が含まれていないことを確認したら、アプリケーションを再デプロイします。

## Contrast Assess

Contrast Assess は、静的アプリケーションセキュリティテスト(SAST)、動的アプリケーションセキュリティテスト(DAST)、インタラクティブアプリケーションセキュリティテスト(IAST)のアプローチを組み合わせた、アプリケーションセキュリティのテストツールです。アプリケーションの脆弱性に関して、極めて正確な情報を継続的に得ることができます。



Contrast Assess はエージェントを使用して、アプリケーションにセンサーを配置します。このセンサーがデータフローをリアルタイムで監視し、アプリケーションを内部から解析し、以下のような様々なデータソースから脆弱性を特定するために機能します。

- ライブラリ、フレームワーク、カスタムコード
- 設定情報
- ランタイムの制御フローやデータフロー
- HTTP リクエストとレスポンス

## バックエンドの接続状況

Contrast Assess は、テストサーバ、QA サーバ、ステージングサーバなど、開発環境や試験環境に適しています。また、開発者のワークステーションにも適用できます。Visual Studio などで Contrast とのインテグレーションを利用することで、開発者は利用中の統合開発環境(IDE)から脆弱性を検出し、修正に対応できます。

## 機能

エージェントをインストールして設定 (35ページ)し、Contrast Assess を有効 (701ページ)にしたら、次の機能を利用できるようになります。

- アプリケーションの脆弱性 (587ページ)の一覧と脆弱性を修復するためのガイダンス
- アプリケーションのセキュリティを一目で判定できるアプリケーションのスコア (822ページ)
- 脆弱性と元の Web リクエストを関連付けることで、可能な限りのルートを検出するルートカバレッジ (492ページ)
- 実行中のアプリケーションのアーキテクチャを把握できるフロアマップ (497ページ)
- コンプライアンス対応などのレポート (611ページ)の作成

## カスタマイズ

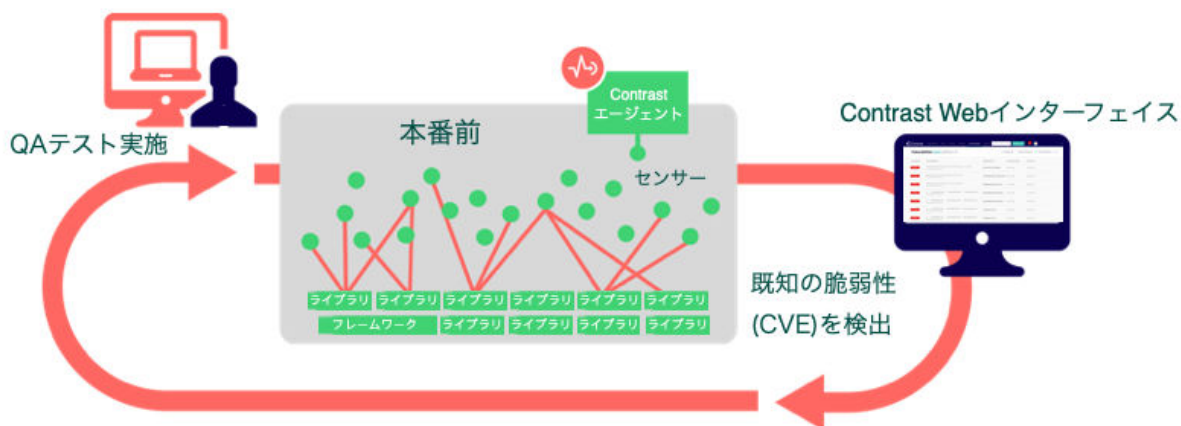
以下のポリシーの設定を変更する事で、特定の要件に合わせて Assess をカスタマイズできます。

- Assess ルール (670ページ): 特定の種類の脆弱性を検出するルールを有効または無効にでき、Contrast Assess の検出機能を調整できます。
- セキュリティ制御 (671ページ): コード内でデータを安全に使用するためのメソッドを設定します。

## Contrast SCA

Contrast SCA は、ランタイム分析、ファイルシステムのスキャン、依存関係の解析によって、オープンソースコンポーネントを特定します。Contrast SCA ではこれらの手法を活用し、正確なインベントリを報告します。

デフォルトで、Contrast Assess には優れた SCA 機能が備わっています。SCA ライセンスを取得すると、さらに高度な SCA 機能を利用できます。



## 機能

SCA 機能は、Contrast プラットフォームの一部として組み込まれています。プロセスを簡素化し、オープンソースの解析とカスタムコードの解析を統合するためです。Contrast SCA で実行できることは、以下のとおりです(一部の機能は無料ですが、その他には SCA ライセンスが必要です)。

- オープンソースライセンスの管理: Contrast SCA によって、オープンソースコンポーネントに関連付けられたライセンス情報 (543ページ)が表示されます。この情報により、知的財産のコンプライアンスを理解し、運用リスクを軽減できます。

この機能には、SCA ライセンスが必要です。

- **オープンソースポリシーの設定**：ポリシーを設定して、オープンソースライセンスの使用を制限することができます。使用を制限したライセンスがアプリケーションでデプロイされた場合、警告を発生します。ライブラリの使用を安全に保つには、組織の [コンプライアンスポリシーを設定 \(695ページ\)](#) します。特定のオープンソースライブラリやライセンスの使用を制限したり、バージョン要件を指定するには、[ライブラリポリシーを設定 \(698ページ\)](#) します。

この機能には、SCA ライセンスが必要です。

- **脆弱性(CVE)の特定**：Contrast SCA は、アプリケーションが使用している各ライブラリの脆弱性(CVE)の情報を提供します。この情報には、ライブラリの各 CVE の説明と、そのライブラリを使用しているアプリケーションの数などが含まれます。

この機能は、SCA ライセンスがなくても利用できます。

- **CLI および依存関係ツリー**：Contrast CLI は、アプリケーションに対して SCA(ソフトウェアコンポジション解析)を実行し、オープンソースライブラリ間の依存関係を、脆弱性が導入された場所を含めて表示します。

[Contrast CLI \(579ページ\)](#)で収集されるデータは [依存関係ツリー \(543ページ\)](#)を表示するために使用され、ライブラリの依存関係を認識することができます。

この機能は、SCA ライセンスがなくても利用できます。

- **GitHub Action**：このインテグレーション機能を使用すると、プロジェクトの依存関係の脆弱性を解析できます。Contrast SCA Action を実行することによって、脆弱なライブラリが検出されます。詳細は、[Contrast SCA Action](#) を参照してください。

## Contrast データ

Contrast にライブラリの情報が報告されると、以下を利用できるようになります。

- 脆弱なコンポーネントが実際にアプリケーションで使用されているかを確認するためのライブラリの使用状況分析
- 使用されているライブラリのバージョンと最新バージョンの情報
- ライブラリで検出されている脆弱性の情報
- ポートフォリオ全体で、オープンソースコンポーネントをリアルタイムに報告

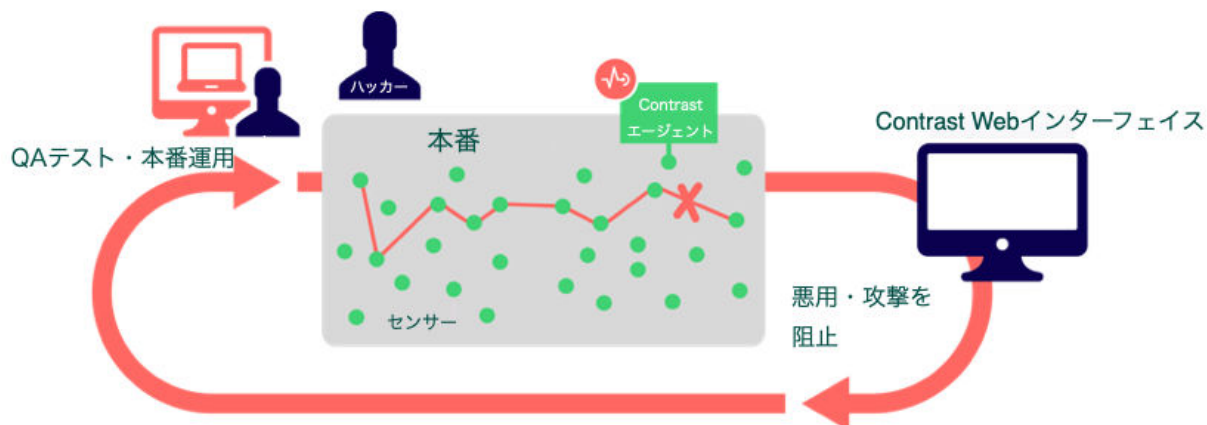
## Contrast Protect

Contrast Protect は本番環境向けの防御制御で、特定の脆弱性(例えばコマンドインジェクションなど)に応じて、アプリケーションを積極的に防御します。

NIST 800-53、PCI-DSS、PCI-SSS、およびその他の業界標準に準拠する「ランタイムアプリケーション自己保護(RASP)」を提供します。Contrast Protect は、[Java \(57ページ\)](#)、[.NET \(137ページ\)](#)、[.NET Core \(195ページ\)](#)、[Node.js \(250ページ\)](#)、[Ruby \(392ページ\)](#)、[Python \(316ページ\)](#)のランタイム内部で直接動作し、手動で調整をすることなくアプリケーション内のインテリジェンスを活用します。

Contrast Protect は、Web アプリケーションや API を攻撃する自動化された脅威と高度な脅威の両方をブロックし、アプリケーションポートフォリオ全体に渡って、的確で価値ある脅威情報をタイムリーに提供します。





## Contrast Protect の仕組み

Contrast Protect は、ネットワークトラフィックではなく、完全なデータフローを把握するために、アプリケーションソフトウェア内で動作します。受信データを解析するだけでなく、そのデータを見て、完全な SQL クエリやコマンド回数など、基になるアクションへの影響を観察します。

この解析は、検知精度を向上させ、誤検知の可能性のある多くの攻撃のノイズを分離し、意図したターゲットに合致する攻撃に焦点を当てることができます。この情報を SIEM などの外部システムと共有して、主要な攻撃イベントに焦点を絞ることができます。

Contrast Protect は、アプリケーションと同じ共有メモリで運用することでアプリケーションのパフォーマンスへの影響を抑え、オーバーヘッドの増加を防ぎます。コンテキストに関する防御に不要なアクションを回避することで、パフォーマンスは向上します。例えば、NoSQL アプリケーションでは、SQL API が呼び出される事がなければ、SQL インジェクションに対するチェックは必要ありません。

## カスタマイズ

Contrast Protect が有効な場合、以下のポリシーやルールをカスタマイズできます。

- **Protect ルール (680ページ)** : 攻撃を監視するアプリケーションを設定します。
- **CVE シールド (684ページ)** : 脆弱性をブロックするために CVE シールドを指定します。
- **仮想パッチ (689ページ)** : 特定の脆弱性に対するカスタム防御を定義します。
- **ログエンハンサー (690ページ)** : Contrast エージェントによりアプリケーションのパラメータやデータを追加でログに記録できるよう指定します。
- **IP 管理 (697ページ)** : 拒否リストと許可リスト(信頼できるホスト)を管理します。

## Contrast Scan

**Contrast Scan (499ページ)** は、脆弱性の検出と修復を容易にする静的アプリケーションセキュリティテスト(SAST)ツールです。これは、アプリケーションの開発フェーズで使用できる便利なツールです。ライセンスをお持ちで SaaS 版をご利用のお客様は、この機能をご利用いただけます。

アプリケーションをスキャンするには、アプリケーションのバイナリパッケージを Contrast の環境にアップロードします。アプリケーションコードをアップロードしたら、スキャンが開始します。スキャンは、ソースコード内のデータフローを確認し、悪意のある攻撃を可能にする脆弱性を特定します。悪意のある攻撃の例としては、SQL インジェクション、コマンドインジェクション、サーバサイドインジェクションなどがあります。

スキャンの結果、カスタムコード内の脆弱性が特定されます。これらの問題を修正して、スキャンを再度実行すると、コードの変更によって脆弱性が無くなったことを確認できます。

オープンソースのコードとライブラリはスキャンの対象に含まれません。



## 機能

- 複数のスキャン結果を追跡できるスキャングループの作成
- スキャンの設定(スキャン名の変更)
- スキャンの開始と停止
- 検出された脆弱性の情報の表示
- スキャンの進行状況と履歴の照会
- 脆弱性情報へのステータスの設定
- CI/CD パイプラインへのスキャンの組み込み
- 各脆弱性のリスクと修正方法に関する説明

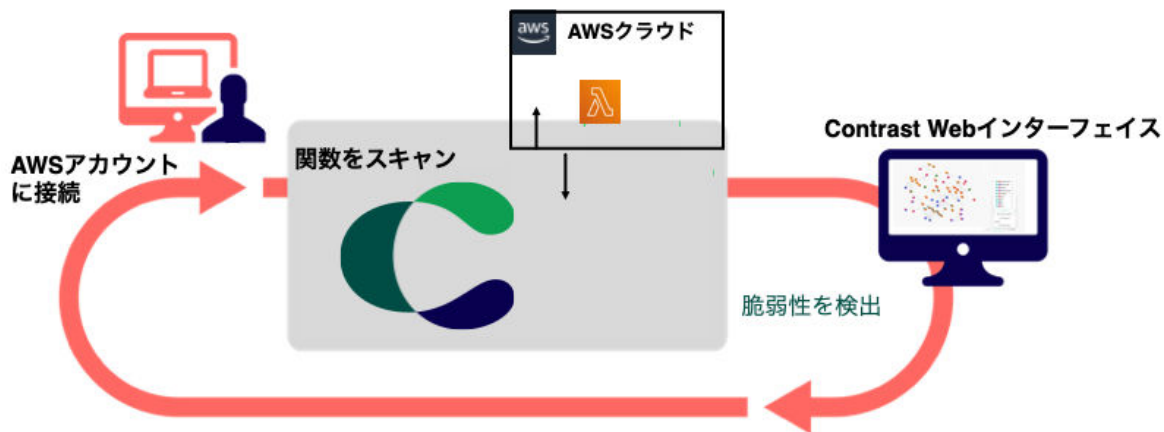
## 関連項目

[Contrast Scan のサポート対象テクノロジー \(502ページ\)](#)

## Contrast Serverless

Contrast Serverless は、サーバレススペースのアプリケーションを対象とした、次世代のアプリケーションセキュリティテストツールです。

Contrast Serverless は、クラウドネイティブアーキテクチャを使用して環境内の全てのリソースをマッピングし、自動的にその結果を検証して優先順位付けを行い、誤検知や不用なアラートを解消します。カスタムコードの脆弱性(インジェクション攻撃など)、依存関係(ライブラリの CVE など)、および設定のリスク(過剰に権限が設定された関数ポリシー)をスキャンします。



## 機能

- **AWS への容易な接続**  
2 回のクリックと数分で、Contrast の Web インタフェースから AWS アカウントに接続できます。
- **インベントリの検出**  
AWS アカウントに接続すると、AWS 環境にある関数、リソース、ポリシー、サービスのインベントリが作成されます。
- **脆弱性の解析**  
動的スキャンと静的スキャンによってコードが解析され、アプリケーションの弱点やデータフロー、攻撃対象、および脆弱性にさらされている箇所が検出されます。
- **継続的な監視**  
Contrast は常に Lambda 関数を監視し、コードが変更されると、注意が必要な脆弱性を特定します。
- **攻撃のシミュレーション**  
動的スキャンは、コードに変更を加えることなく、リソースとデータフローに対して情報収集のための攻撃を生成して実行します。
- **関数とサービスの関連性を可視化**  
アカウント内の関数とサービスの関連性を表示するだけでなく、各要素に含まれるリスクの詳細を表示できます。
- **レポート作成**  
スキャン結果には、コードにある CVE、権限違反、脆弱性、およびその他のリスクが一覧表示されます。

## 利点

- **導入がスピーディで簡単**  
Contrast と連携するために、多数の専門家やコンサルタント、また多くの時間は必要ありません。
- **連携に煩わされることがない**  
開発プロセスに大幅な変更を加えることなく、サーバレスセキュリティを強化できます。開発フェーズの早い段階で悪用可能な脆弱性を簡単に見つけて修正できるため、アプリケーションを本番環境にデプロイする際に、アプリケーションをより安全な状態にすることができます。

## 仕組み

Contrast は、AWS アカウントに読み取りモードで接続します。この接続を使用して継続的に環境を監視し、関連情報を収集します。

そして、監視対象の環境内に 1 つの Lambda 関数(Cloud Agent)を配置して、コード解析やスキャンしたリソースに関するメタデータを Contrast へ送信するなどの処理を実行します。

これらの情報は全て、Contrast のコンテキストエンジンによって使用され、この環境の全てのリソースと変更に合わせて攻撃プロファイルを生成します。攻撃のシミュレーションは、お客様のアカウント内でクラウドエージェント(Cloud Agent)によって実行されます。

全ての検出結果は、内部検証メカニズムによって検証することにより、誤検知をなくし、現実的な優先順位を付けた結果として提供されます。

## セキュリティとプライバシー

- Contrast は、監視対象のアカウントからコードやコードスニペットを収集することはありません。Contrast は、次のようなメタデータ情報のみを利用します。
  - 確認された脆弱性
  - 関数名とメタデータ(ポリシーハンドラなど)
  - 使用しているライブラリ
  - 使用している AWS の API(例 : Boto3、asw-sdk)
  - サービスの構成(バケット通知、API Gateway のパスやメソッドなど)

- Contrast は、お客様のコードに変更を加えることはありません。ただし、スキャン中に(例えば、関数のデプロイ時や変更時)、スキャンされた関数にレイヤーを一時的に組み込んだり、いくつかの設定変更(例えば、タイムアウトやハンドラ)を行うことがあります。  
スキャンが完了すると、レイヤーや設定は元の状態に戻されます。この処理は完全に透過的で影響を与えず、自動的に実行されます。  
スキャン中でも、引き続き独自のテスト(関数呼び出し)を実行できます。
- 動的スキャンでは、Contrast は悪意のあるデータを使用してスキャンする関数を実行します。この処理は、コードには影響を与えません。ただし、関数が行うアクションはトリガーされる可能性があります。  
この機能はデフォルトで無効になっています。これは、設定タブを使用して、いつでも有効にできます。
- 監視対象の AWS アカウントから Contrast が受信する全てのデータは、転送中および保存時に暗号化されます。  
Contrast は、共有シークレットを用いた Amazon EventBridge を使用して、全てのデータを送受信します。Contrast が AWS アカウントとの通信に使用する Web API や REST API はありません。

## 必要となる権限

Contrast を使用して AWS アカウントに接続する場合、次のアクセス許可に同意するものとします。

- Contrast の AWS アカウントから監視対象の AWS アカウントへの読み取り専用アクセス権。  
このポリシーは、ベータ版の処理を行う際だけ使用されます。
- Contrast の AWS アカウントから監視対象の AWS アカウントにデプロイされた Lambda 関数への Lambda 読み取り/書き込みアクセス。
- Contrast が監視対象の AWS アカウントにインストールする Lambda 関数には、次のアクセスポリシーが必要です。
  - CloudWatch ログの読み取り
  - Lambda Layer バージョンの読み取り
  - 関数の呼び出し
  - 関数設定の変更
  - イベントバスへのメッセージの書き込み
  - KMS キーの読み取り
  - 特定の S3 バケットへのオブジェクトの読み取り / 書き込み(Contrast はこれらのバケットを作成します)

## 関連項目

- [はじめに\(Contrast Serverless\) \(547ページ\)](#)

## Contrast のパフォーマンスとリソース消費について

適切な設定を使用することで、本番サーバで Contrast の影響を最小限に抑えることができます。

- **開発環境** : Contrast Assess はオンにして、Contrast Protect はオフにします。この設定により、開発時にアプリケーションのセキュリティの状況を的確に把握することができます。パフォーマンスよりも、開発者がセキュリティ上の欠陥を特定することに焦点を当てて、詳細な状況を把握する必要があります。
- **テスト環境** : プロジェクトの必要性に応じて、Contrast Assess または Contrast Protect を有効にします。プロジェクト全体の目標に合わせて、バランスを取ります。
  - 開発時にテストがほとんど実施されていない場合、Contrast Assess を活用して、アプリケーションを使用しながら脆弱性を見つける必要があります。
  - パフォーマンスを評価する場合は、Contrast Assess をオフにして、Protect のみを有効にしてください。パフォーマンスを優先しながらも、修正処置が必要な場合にはコードレベルの情報を取得するという修正対応が可能になります。
- **本番環境** : Contrast Protect のみをオンにします。この設定により、パフォーマンスを優先しながらコンテキストに応じた防御が可能になります。

## Community Edition (CE)

Community Edition では、Contrast の製品 (Assess、SCA、Protect) をほぼ完全に利用することができます。インタラクティブアプリケーションセキュリティテスト (IAST)、ソフトウェアコンポジション解析 (SCA)、ランタイムアプリケーション自己保護 (RASP) を無料でお試しください。

利用を開始するには、[Community Edition のアカウントに登録](#)して、Contrast エージェントをインストールします。詳細については、[Community Edition に関するブログ](#)を参照ください。



### 注記

Community Edition で利用できるアプリケーションは 1 つで、Java、.NET Core、Node.js アプリケーションのいずれかになります。

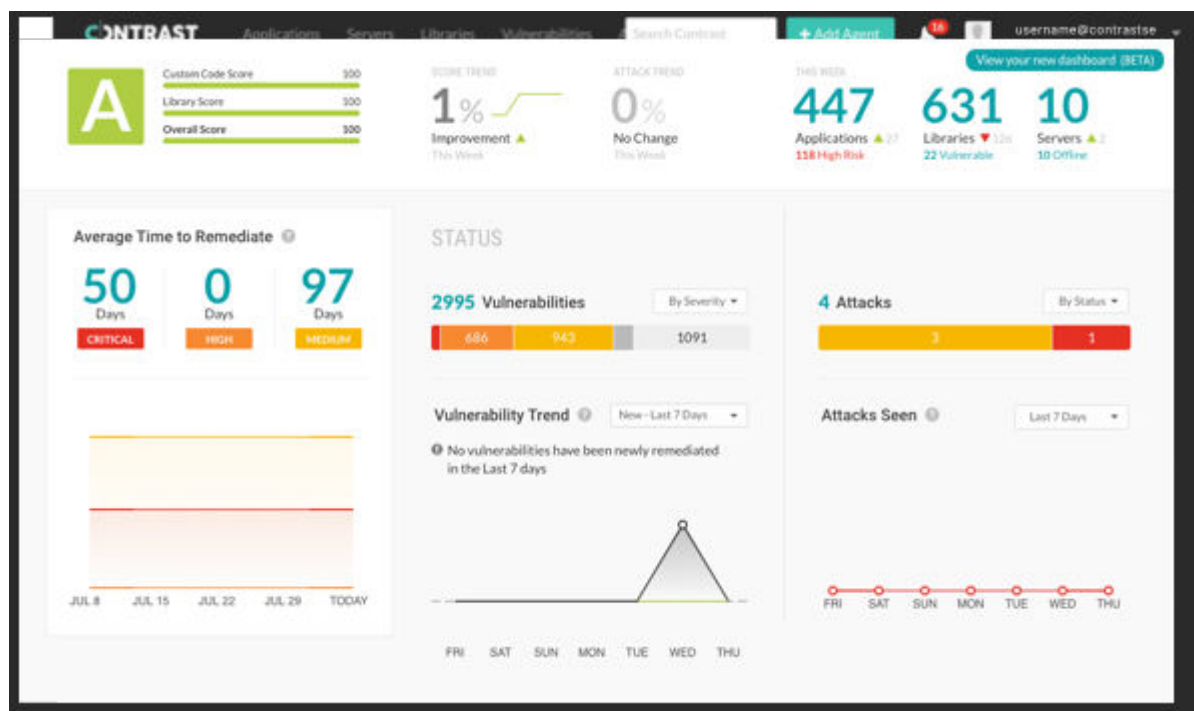
## Community Edition の機能

Community Edition で提供する機能：

- Contrast Assess：実際に問題となるカスタムコードに起因する脆弱性を検出し、開発者は脆弱性の修正に焦点を当てることができます。
- Contrast SCA：オープンソースおよびサードパーティのライブラリがもたらす脆弱性を高度に可視化し、セキュリティリスクの管理が可能になります。  
Contrast SCA は、オープンソースセキュリティまたはソフトウェアコンポジション解析 (SCA) のソリューションです。
- Contrast Protect：自作のコードやオープンソースのライブラリに脆弱性が残っている場合でも、アプリケーション内に組み込んだエージェントのセンサーが、アプリケーションへの攻撃を監視し、自動的にブロックします。

## Community Edition ポータルサイト

Contrast を使用する際の Community Edition ポータルサイトは、以下のような画面になります。



## 次の手順

- [.NET Core エージェントのインストール \(198ページ\)](#)
- [Java エージェントのインストール \(59ページ\)](#)
- [Node.js エージェントのインストール \(253ページ\)](#)

# エージェント

Contrast エージェントは、アプリケーションからセキュリティに関連するデータを収集し、そのデータを解析して、必要に応じて検出結果を Contrast に報告します。特定の条件で、Contrast エージェントは悪用を防止したり、セキュリティ防御を有効にしたりするために、アプリケーション内で処理を実行することもあります。

Contrast エージェントは、コードスキャン、ライブラリスキャン、[アプリケーションの解析 \(35ページ\)](#)、設定ファイルのスキャン、その他の手法など、さまざまなセキュリティ計測技術を使用してセキュリティに関連する情報を収集します。このさまざまなセキュリティ計測技術となって情報を収集するのが、センサーです。

センサーによって、アプリケーション内からスナップショットで直接情報が取得されイベントが生成されます。例えば、センサーは、受信した HTTP パラメータやデータベースに対して実行される SQL クエリの詳細を取得します。センサーによっては、必要に応じて、防御機能を強化したり悪意のある攻撃をブロックしたりするために、脆弱性を迂回させるセキュリティ例外をスローする処理などを行う場合もあります。

センサーによって生成されたイベントは全て、エージェントによる追跡と解析対象として Contrast サーバに報告されます。解析エンジンはアプリケーションのあらゆるコードから [イベントを受け取り \(595ページ\)](#)、それらのイベントによって次第にトレースが構築されていきます。解析エンジンは、これらのトレースを監視して、Contrast ルールに違反する動作パターンを探します。

例えば、解析エンジンは以下のようなデータフローを確認します。

- 受信した HTTP リクエストのパラメータに関するイベント
- 次に、そのパラメータが SQL クエリに追加されていることを示す別のイベント
- 最後に、そのクエリがデータベースに送信されていることを示す別のイベント

適切な防御策(エスケープ処理やパラメータ化)がないデータフローを解析エンジンが検出した場合は、そのトレースが SQL インジェクションの Contrast ルールに一致すると認識され、Contrast サーバに報告されます。解析の大部分はエージェント内でローカルに行われるため、Contrast の拡張性とパフォーマンスが向上します。

検査対象のアプリケーションの言語と一致するエージェントを使用してください。

- [Go \(450ページ\)](#) エージェントは、ライブラリのサポートと脆弱性報告のために、Go の Web アプリケーションを計測します。
- [Java \(57ページ\)](#) エージェントは、コンテナで実行される Java の Web アプリケーションおよび Web API を計測します。
- [.NET Framework \(137ページ\)](#) エージェントは、IIS で実行される .NET Framework の Web アプリケーションおよび API を計測します。
- [.NET Core \(195ページ\)](#) エージェントは、.NET Core ランタイムで実行されるアプリケーションおよび API を計測します。
- [Node.js \(250ページ\)](#) エージェントは、Node.js の Web アプリケーションおよび API を計測します。
- [Ruby \(392ページ\)](#) エージェントは、Ruby on Rails の Web アプリケーションを計測します。
- [PHP \(297ページ\)](#) エージェントは、PHP の Web アプリケーションを実行時に解析し、ライブラリの使用状況や脆弱性の検出を行います。
- [Python \(316ページ\)](#) エージェントは、Django、Flask および Pyramid の Web アプリケーションを計測します。



## 注記

Contrast エージェントは、リリース後 1 年間サポートされます。古いエージェントは、引き続き機能し互換性を維持できる可能性もありますが、完全にサポート対象外になります。

Contrast では、バグの修正の適用や新機能の開発は、エージェントの最新バージョンが対象となります。コードの修正は、古いバージョンにはバックポートされません。バグに対して回避策が提供されている場合でも、問題を解決するには、その問題が修正されたリリースに更新してください。

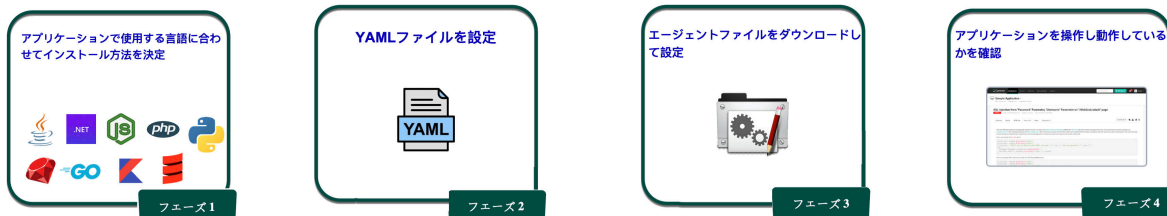
## Contrast でエージェントをインストールしてみる

Contrast では、コードの脆弱性をモニターするセンサーを配置するために、エージェントを使用します。エージェントは、開発環境で脆弱性を解析し、実行時の本番環境で攻撃を検知します。

アプリケーションを実行すると、エージェントは情報(HTTP リクエスト、データフロー、バックエンド接続、ライブラリの依存関係など)を解析し、脆弱性や攻撃を Contrast サーバに送信します。これらの情報は Contrast Web インターフェイスで確認することができ、優先順位付けを行い、すぐに対策を取ることができます。

本項は、アプリケーションで Contrast をすぐに使用できるようになり、Contrast がどのように機能するかを確認するための参考にしてください。

Contrast エージェントをアプリケーションに組み込んで検査を行うには、いくつかのフェーズがありますが、本項はそれらの過程をサポートするものです。



一度、仕組みを理解したら、後は自分のニーズに合わせて調整することができます。そのための方法がたくさんあります。Contrast ドキュメント を参照して、利用する状況に合わせて Contrast を調整してください。



## ヒント

今後の導入にあたっては、利用するビルドツールやデプロイパイプライン、セキュリティ目標、Contrast を使用する環境などの検討が必要な場合があります。ご利用状況に合わせて、[インテグレーションによって Contrast をインストールする方法 \(618ページ\)](#) も参照ください。



## Java

実行可能な JAR のインストール	アプリサーバインストール	ビルド自動化ツールと連携してインストール	コンテナにインストール	クラウドオーケストレーションサービスでインストール
<p>JAR ファイルを使って1つのアプリケーションにエージェントをインストールします。</p> <p><a href="#">Maven Central (60ページ)</a>、<a href="#">Debian (61ページ)</a>、<a href="#">RPM (62ページ)</a>を参照し、各リポジトリを使用してインストールします。</p>	<p>アプリケーションサーバにエージェントをインストールし、テスト/QA 環境や本番環境で動作するアプリケーションのセキュリティ検査を行います。</p> <p><a href="#">JBoss/Wildfly の場合はこちらを参照。(71ページ)</a></p> <p><a href="#">Jetty の場合はこちらを参照。(72ページ)</a></p> <p><a href="#">Tomcat の場合はこちらを参照。(73ページ)</a></p> <p><a href="#">Weblogic の場合はこちらを参照。(74ページ)</a></p> <p><a href="#">Websphere の場合はこちらを参照。(75ページ)</a></p> <p><a href="#">Axis2 の場合はこちらを参照。</a></p> <p><a href="#">Glassfish の場合はこちらを参照。</a></p>	<p>Contrast プラグインを使用したエージェントのインストールを自動化します。</p> <p><a href="#">Maven の場合はこちらを参照。(661ページ)</a></p> <p><a href="#">Gradle の場合はこちらを参照。(645ページ)</a></p> <p><a href="#">Bamboo の場合はこちらを参照。(636ページ)</a></p> <p><a href="#">Azure Pipelines の場合はこちらを参照。(633ページ)</a></p> <p><a href="#">VMWare Tanzu の場合はこちらを参照。</a></p>	<p>コンテナにエージェントをインストール、または Kubernetes オペレータでエージェントをインストールします。</p> <p><a href="#">Docker ベースイメージまたはアプリケーションイメージにエージェントを追加する場合はこちらを参照。(64ページ)</a></p> <p><a href="#">OpenShift の場合はこちらを参照。</a></p> <p><a href="#">Contrast K8s オペレータで Kubernetes Pod にエージェントを追加する場合はこちらを参照。(41ページ)</a></p>	<p>Google App Engine でエージェントをインストールします。</p> <p><a href="#">こちらを参照。</a></p> <p>AWS Elastic Beanstalk でエージェントをインストールします。</p> <p><a href="#">こちらを参照。</a></p>

また、Contrast Java エージェントを使用して、Contrast Assess や Contrast SCA で、[Scala ベース \(70ページ\)](#)のアプリケーションや [Kotlin ベース \(70ページ\)](#)のアプリケーションを解析することができます。

## .NET Framework

インストーラによるインストール	Azure でインストール	コンテナにインストール
<p>セルフホストのアプリケーションや IIS 上のアプリケーションに、エージェントをインストールします。</p> <p><a href="#">こちらを参照ください。(140ページ)</a></p>	<p>Azure App Service でエージェントをインストールします。</p> <p><a href="#">こちらを参照ください。(143ページ)</a></p>	<p>コンテナイメージにエージェントをインストールします。</p> <p><a href="#">こちらを参照ください。(145ページ)</a></p>

## .NET Core

### Windows

基本のインストール	インストーラによるインストール	Azure でインストール	コンテナにインストール
<p>基本のインストールで、.NET Core エージェントをインストールします。</p> <p>こちらを参照ください。(198ページ)</p>	<p>セルフホストのアプリケーションや IIS 上のアプリケーションに、エージェントをインストールします。</p> <p>こちらを参照ください。(204ページ)</p>	<p>Azure App Service でエージェントをインストールします。</p> <p>こちらを参照ください。(203ページ)</p>	<p>コンテナにエージェントをインストール、または Kubernetes オペレータでエージェントをインストールします。</p> <p>Docker ベースイメージまたはアプリケーションイメージにエージェントを追加する場合はこちらを参照。(207ページ)</p> <p>Contrast K8s オペレータで Kubernetes Pod にエージェントを追加する場合はこちらを参照。(41ページ)</p>

## Linux

基本のインストール	コンテナにインストール
<p>基本のインストールで、.NET Core エージェントをインストールします。</p> <p>こちらを参照ください。(198ページ)</p>	<p>コンテナイメージにエージェントをインストールします。</p> <p>Docker ベースイメージまたはアプリケーションイメージにエージェントを追加する場合はこちらを参照。(207ページ)</p>

## Node

基本のインストール	コンテナにインストール	クラウド環境のデプロイにインテグレーションしてインストール
<p>基本のインストールで、Node エージェントをインストールします。</p> <p>こちらを参照ください。(253ページ)</p>	<p>コンテナイメージにエージェントをインストールします。</p> <p>Docker ベースイメージまたはアプリケーションイメージにエージェントを追加する場合はこちらを参照。(254ページ)</p>	<p>IBM Cloud でインストールします。</p> <p>こちらを参照ください。(259ページ)</p> <p>VMWare Tanzu でインストールします。</p> <p>こちらを参照ください。</p>

## PHP

リポジトリによるインストール
<p>Debian または RPM リポジトリを使用して、PHP エージェントをインストールします。</p> <p>Debian の場合はこちらを参照。(298ページ)</p> <p>RPM の場合はこちらを参照。(300ページ)</p>

## Python

ミドルウェアによるインストール
<p>ミドルウェア(AIOHTTP、Bottle、Django、Falco、Fast API、Flask、Pyramid、Quart、WSGI)によって、Python エージェントをインストールします。</p> <p>こちらを参照ください。(318ページ)</p>

## Ruby

ミドルウェアによるインストール
<p>ミドルウェア(Rails、Sinatra、または Grape)によって、Ruby エージェントをインストールします。</p> <p>こちらを参照ください。(395ページ)</p>

## Go

### インストーラによるインストール

Contrast インストーラで、Go エージェントをインストールします。

[こちらを参照ください。\(452ページ\)](#)

## エージェントのインストールと設定

Contrast でアプリケーションを検査するには、アプリケーションで使用している言語に応じて Contrast エージェントをインストールして設定する必要があります。ほとんどの Contrast エージェントが、パッケージマネージャやリポジトリからダウンロードできます。

インストール方法は、インストールする Contrast エージェントや使用する Contrast 製品、Contrast をインストールする場所によって異なります。例えば、以下のようなことが考えられます。

- アプリケーションサーバや Web サーバ上
- ビルドパイプラインやコンテナ内
- 開発、テスト(QA)、本番などの環境

## インストール

ご利用の環境に応じて、Contrast エージェントを直接インストールするか、Contrast と連携する [インテグレーション \(618ページ\)](#) を使ってインストールしてください。

Contrast を利用する目的を考え、使用する Contrast エージェントのインストール手順を確認してください。

- [Go \(453ページ\)](#)
- [Java \(59ページ\)](#)
- [.NET Framework \(139ページ\)](#)
- [.NET Core \(198ページ\)](#)
- [Node.js \(253ページ\)](#)
- [PHP \(298ページ\)](#)
- [Python \(317ページ\)](#)
- [Ruby \(395ページ\)](#)

## 設定

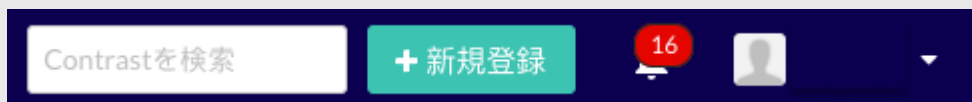
Contrast エージェントをインストールしたら、エージェントがアプリケーションを認識して、Contrast サーバに情報を通信できるように設定しなければなりません。最低限、4 つの基本のエージェントキー ([検索方法はこちらを参照 \(37ページ\)](#)) を指定する必要があります。

- **api.api\_key** : 所属する組織の API キー
- **api.user\_name** : Contrast のユーザアカウント名(通常、自分のログイン ID)
- **api.service\_key** : Contrast のユーザアカウントのサービスキー
- **api.url** : Contrast エージェントが報告する Contrast サーバのアドレス。デフォルトは、<https://app.contrastsecurity.com> です。



## ヒント

組織のキーがあらかじめ入力されている YAML 設定ファイルをダウンロードすることができます。Contrast Web インターフェイスで[新規登録](#)を選択し、アプリケーションの言語を選択すると、YAML 設定ファイルをダウンロードするリンクが表示されます。また、[YAML 設定エディタを開く](#)のリンクから [Contrast エージェント設定エディタ \(39ページ\)](#)を開いて、ファイルを編集することもできます。



Contrast エージェントの設定は、[環境変数 \(56ページ\)](#)、[YAML 設定ファイル \(38ページ\)](#)、コマンドラインを使用したり、ご利用の言語やツール固有の方法などによって、さらに指定できます。設定した値が有効になる[優先順位 \(36ページ\)](#)があります。

Contrast を利用する状況に合わせて、使用する Contrast エージェントを設定する方法を確認してください。

- [Go \(456ページ\)](#)
- [Java \(78ページ\)](#)
- [.NET Framework \(152ページ\)](#)
- [.NET Core \(213ページ\)](#)
- [Node.js \(152ページ\)](#)
- [PHP \(301ページ\)](#)
- [Python \(319ページ\)](#)
- [Ruby \(397ページ\)](#)

## 優先順位

設定値が有効になる順序は、以下の優先順位を使用します(1 が最も高い)。

1. ライセンスの有効期限が切れていたり、ライセンス数を超過していたりすると、設定に関係なく全てのエージェントの動作が無効になります。
2. コマンドラインまたはシステムのプロパティ値(使用している言語に合わせて適切なプロパティが指定されている場合)  
例: `-Dcontrast.enable`
3. 環境変数  
例: `CONTRAST__ENABLE`
4. アプリケーション固有の設定ファイル(.NET Framework のみ)  
例: [web.config \(153ページ\)](#)
5. YAML ファイルの設定値。設定値は以下の順で最初に見つかったファイルから取得されます。
  - a. ユーザが指定した YAML ファイル  
例:
    - Java: `contrast.config.path` [システムプロパティ \(79ページ\)](#)
    - Node.js: `--configFile` [コマンドラインフラグ](#)  
Node.js: `--configFile` [コマンドラインフラグ](#)
    - すべてのエージェント: `CONTRAST_CONFIG_PATH` [環境変数 \(56ページ\)](#)
  - b. 現在の作業ディレクトリにある `contrast_security.yaml` ファイル(Java を除く全てのエージェント)  
例: `./contrast_security.yaml`
  - c. アプリケーションの構成ディレクトリにある `contrast_security.yaml` ファイル(Ruby および Python のみ)

例 :

- Ruby on Rails : `./config/contrast_security.yaml`
  - Django : `./settings/contrast_security.yaml`
- d. エージェント固有の設定ディレクトリにある `contrast_security.yaml` ファイル。エージェントがサービスを使用しており、エージェントとサービスに個別の YAML ファイルを使用する必要がある場合に、このディレクトリを使用します。

例 :

- `/etc/contrast/agentname/contrast_security.yaml` (agentname は次のいずれか : `dotnet`、`go`、`java`、`node`、`python`、`ruby`、`webserver`)
  - `%ProgramData%\Contrast\agentname\contrast_security.yaml`(agentname は次のいずれか : `dotnet`、`dotnet-core`、`java`、`node`、`python`、`ruby`、`webserver`)
- e. サーバの `/etc/contrast` ディレクトリ内にある `contrast_security.yaml` ファイル(.NET Framework と .NET Core 以外の全てのエージェント)。エージェントがサービスを使用しており、エージェントとサービス間で共有する YAML ファイルを使用する必要がある場合に、このディレクトリを使用します。

例 :

- `/etc/contrast/contrast_security.yaml`
  - `%ProgramData%\Contrast\contrast_security.yaml`
6. Contrast Web インターフェイスで設定されている値  
例 : Contrast Web インターフェイスでの Assess や Protect モードのトグルボタンでの切り替えは、`assess.enable` や `protect.enable` に対応付けられます。
7. Contrast Security が設定したデフォルト値

## エージェントキーの検索



### 重要

Contrast Web インターフェイスの**新規登録**を選択して、YAML 設定ファイルをダウンロードすると、YAML 設定ファイルにはあらかじめエージェントキーが入力されます。

独自に YAML ファイルを作成する場合は、自分でエージェントキーを追加する必要があります。

エージェントキーは、組織内の全てのエージェントに共通です。エージェントキーの情報は、アクセスする組織とエージェントを表し、識別するための値です。

エージェントをインストールする場合には、次の全てのキーが必要です。

- エージェントユーザ名
- エージェントサービスキー
- API キー  
こちらの API キーは、全てのエージェント用の API キーとなります。カスタムスクリプトで使用する API キーは、「ユーザの設定」にある API キーを使用してください。
- Contrast URL

## 手順

1. 右上隅にある**ユーザ名 > 組織の設定**を選択します。
2. **エージェント**を選択すると、**エージェントキー**の値が表示されます。

### 組織の設定

組織

- グループ
- ユーザ
- セキュリティ
- エージェント
- インテグレーション
- サーバ
- アプリケーション
- 通知
- スコアの設定

#### エージェントキー

Contrast APIにより、脆弱性情報の取得、エージェントのダウンロード、インテグレーションの設定などを行います。詳細はAPIドキュメントをご確認ください。エージェントキーは、エージェントがContrastと通信するために設定する場合に使用します。

**エージェントキー**

エージェントユーザ名  
agent\_1[redacted]ity

エージェントサービスキー  
PK [redacted] G **ローテーション**

APIキー  
demo **ローテーション**  
これは、あなたのAPIキーではありません。あなたのAPIキーは、ユーザの設定をご覧ください。

Contrast URL  
http://localhost:30080/Contrast

あなたのAPIキーをお探しますか? [ユーザの設定](#)をご覧ください。

[サンプルAPIリクエストを生成](#)

Contrast URL は、<https://app.contrastsecurity.com/Contrast>、もしくはオンプレミス版かプライベートクラウドのインスタンスの URL になります。



### 注記

このページにエージェントユーザ名やエージェントサービスキーが表示されない場合は、所属する組織にライセンスが適用されていない可能性があります。その場合は[サポート](#)にお問い合わせください。

3. 認証情報が侵害された場合は、エージェントキーをローテーションして新しいキーを生成できません。



### 重要

エージェントサービスキーをローテーションすると、全てのエージェントがオフラインになります。アプリケーションは引き続き機能しますが、データは Contrast に送信されなくなります。新しい認証情報の使用を開始するには、エージェントを再設定し、アプリケーションを再起動します。認証情報管理システムなどを使用して、システム間でこの変更を調整してください。

## YAML 設定

YAML 設定ファイルを使用して、Contrast エージェントの設定プロパティを指定できます。YAML 設定ファイルの値は、環境変数またはコマンドラインの引数で上書きできます。

すべての Contrast エージェントで、YAML 設定ファイルのプロパティは同じフォーマットを使用できますが、各エージェントに適用される固有のプロパティがあるため、各エージェントで固有の指定ファイルを使用する必要があります。

設定ファイルは `contrast_security.yaml` という名前で、[ロードパス \(36ページ\)](#) に正しく置かれている必要があります。

Contrast Web インターフェイスからエージェントの設定ファイルをダウンロードすると、設定ファイルには Contrast サーバと通信するために最低限必要な基本のプロパティが入ります。独自の設定ファイルを作成する場合は、[基本のキー \(37ページ\)](#) を自分で追加してください。

全てのエージェントで最低限必要な `contrast_security.yaml` の内容は、以下のようになります。

```
api:  
  url: https://app.contrastsecurity.com
```

```
user_name: contrast_user
api_key: demo
service_key: demo
```



## ヒント

- [Contrast エージェント設定エディタ \(39ページ\)](#)を使用すると、YAML 設定ファイルの作成やアップロード、YAML の検証、推奨される設定値の表示などができます。
- YAML は JSON のスーパーセットとなっているため、YAML ファイルで JSON を使用して Contrast エージェントを設定することもできます。

以下より参照できる YAML テンプレートを使用して、各エージェントの `contrast_security.yaml` を作成できます。

- [Go \(457ページ\)](#)
- [Java \(79ページ\)](#)
- [.NET Framework \(154ページ\)](#)
- [.NET Core \(214ページ\)](#)
- [Node.js \(264ページ\)](#)
- [PHP \(301ページ\)](#)
- [Python \(320ページ\)](#)
- [Ruby \(397ページ\)](#)



## 注意

YAML テンプレートでは空白が認識されます。スペースは使用できますがタブは使用できないため、編集時には注意が必要です。各プロパティの説明は、テンプレート内のコメントとして記載されています(スペースの後にシャープ記号「#」で続く行がコメントになります)。

## Contrast エージェント設定エディタを使う

[Contrast エージェント設定エディタ](#)は、Contrast エージェントの設定を検証および生成するための Web アプリケーションです。

### 開始する前に

- このエディタは、Contrast エージェントの設定を編集、検証、生成するために使用してください。
- 既に YAML 設定ファイルがある場合は、**Import** を選択するとエディタにファイルを取り込むことができます。
- エディタは完全にブラウザ内だけで実行され、API キーなどの機密情報がローカルマシンから出ることはありません。

### 手順

1. ブラウザで [Contrast エージェント設定エディタ](#)を開きます。

Validate using the .NET Core Agent Reset Import Export Share

```

1 api:
2   url: https://app.contrastsecurity.com/Contrast/
3   api_key: TODO
4   service_key: TODO
5   user_name: TODO
6

```

Type	Message	Line number
TODO	Placeholder value 'TODO' should be replaced for setting: api.api_key	3
TODO	Placeholder value 'TODO' should be replaced for setting: api.service_key	4
TODO	Placeholder value 'TODO' should be replaced for setting: api.user_name	5

Contrast Agent Configuration Editor 2.0.0 - Copyright © 2023 Contrast Security, Inc.

Filter Options

Show advanced settings

- api.url**  
Set the URL for the Contrast UI.
- api.api\_key**  
Set the API key needed to communicate with the Contrast UI.
- api.service\_key**  
Set the service key needed to communicate with the Contrast UI. It is used to calculate the Authorization header.
- api.user\_name**  
Set the user name used to communicate with the Contrast UI. It is used to calculate the Authorization header.
- inventory.tags**  
Apply a list of labels to libraries. Labels must be formatted as a comma-delimited list. Example - label1, label2, label3
- assess.tags**  
Apply a list of labels to vulnerabilities and preflight messages. Labels must be formatted as a comma-delimited list. Example - label1, label2, label3
- application.name**  
Override the reported application name. Note - On Java systems where multiple, distinct applications may be served by a single process, this configuration causes the agent to report all discovered applications as one application with the given name.
- application.group**  
Add the name of the application group with which this application should be associated in the Contrast UI.
- application.code**  
Add the application code this application should use in the Contrast UI.
- application.version**

2. **Import** を選択して既存の YAML ファイルをインポートするか、YAML ファイルの内容を貼り付けます。
3. テキストを編集する際に、無効な YAML を入力すると、エラー警告が表示されます。エージェント固有の YAML 検証をするために、**Validate using the** の一覧からエージェントのプログラム言語を選択します。  
ここでは次のような検証が行われます。
  - **YAML 構文解析** により、テキストが YAML であることを確認します。YAML が無効な場合、**Error** が表示され、それ以降の検証は行われません。
  - **設定キーの検証** により、YAML ノードが選択したエージェントでサポートされているキーであることを確認します。認識できないキーには **Warning** が表示されます。
  - **設定値の検証** により、YAML 値がブール値、数値、列挙型(例：ログレベル)などの型の期待値と一致するかどうかを確認します。値が無効な場合、**Warning** が表示されます。
  - **設定の整合性の検証** により、相容れない設定が同時に存在していないことを確認します。この検証は現在のところ、`application.session_id` と `application.session_metadata` の設定のみに限定されています。整合性のない設定には、**Warning** が表示されます。
  - **未定値の検証** により、設定に未定値の `TODO` がある場合に通知されます。未定値には、**TODO** が注として表示されます。**Error**、**Warning** や **TODO** が表示されている行をクリックすると、その設定行の先頭にカーソルが置かれます。
4. 右側のパネルを使用して、利用可能な設定(説明あり)を検索できます。プラスアイコン(+)をクリックすると、その設定がエディタ画面の YAML に追加されます。  
この機能を使用して新しい設定を追加すると、YAML がフォーマットされ、ノードが並べ替えられ、YAML 内の余分な空白が削除されます。  
**Reset** をクリックすると、元のファイル設定に戻ります。



### 注記

テキストエディタの YAML に構文エラーがあるか、有効な YAML でない場合、生成した YAML は無効となります。

5. 編集が終了したら、エージェント設定ファイルを YAML または環境変数としてエクスポートします。他の共同作業者とファイルを共有することもできます。





### 注記

この時点で、Contrast エージェント設定エディタは完全にオフラインで実行されます(つまり、最初のアクセス後、インターネット接続がなくてもページを操作できます)。エディタに更新がある場合は、自動的にバックグラウンドでダウンロードされます。新しいバージョンへ更新するには、エージェント設定エディタの全てのブラウザのタブを閉じる必要があります。ページのリフレッシュだけでは、新しいバージョンには更新されません。

## Contrast エージェントオペレータ(Kubernetes オペレータ)

Contrast エージェントオペレータは、Kubernetes クラスタおよび OpenShift クラスタ内で実行される標準の **Kubernetes オペレータ** で、既存のワークロードへの Contrast エージェントの組み込み、組み込まれたエージェントの設定、およびエージェントのアップグレードを自動化します。

まずは、[エージェントオペレータをインストール \(42ページ\)](#)するか、導入例として[エージェントオペレータのチュートリアル \(43ページ\)](#)をご覧ください。

オペレータは、宣言的な Kubernetes ネイティブのリソースタイプを使用して設定します。リソースタイプについては、[エージェントオペレータの設定 \(51ページ\)](#)に記載しています。



### 注記

Contrast エージェントオペレータは、オープンソースプロジェクトです。コードは[こちら](#)で確認でき、開発に貢献することができます。

## 関連項目

- [エージェントオペレータのサポート対象テクノロジー \(41ページ\)](#)
- [エージェントオペレータのテレメトリ \(56ページ\)](#)
- [エージェントオペレータの最小設定 \(47ページ\)](#)

## エージェントオペレータのサポート対象テクノロジー

### Kubernetes/OpenShift のサポート

Kubernetes のバージョン	OpenShift のバージョン	サポート対象	サポート終了
v1.23	v4.10	○	2023-02-28
v1.22	v4.9	○	2022-10-28
v1.21	v4.8	○	2022-06-28

- Contrast エージェントオペレータは、アップストリームである **Kubernetes コミュニティのサポートポリシー** に従います。サポート終了日については、**Kubernetes のリリースページ**に記載されています。
- OpenShift のサポートは、含まれる Kubernetes のバージョンに依存します。例えば、OpenShift v4.10 は Kubernetes v1.23 を使用しており、Contrast では 2023 年 2 月 28 日までサポートします。OpenShift に含まれる Kubernetes バージョンについては、Red Hat の[サポート記事](#)を参照してください。
- Contrast エージェントオペレータは、Linux の amd64 ホスト上での実行のみをサポートし、互換性のないノードでのスケジューリングは拒否されます。また、Contrast エージェントが他のプラットフォーム

ームをサポートしている場合でも、エージェントオペレータは Linux の amd64 ホスト上で実行されているワークロードの組込のみをサポートします。Windows や arm64 での Kubernetes のサポートを希望される場合は、[Contrast サポート](#)にお問い合わせください。

## エージェントタイプ

エージェント	エージェントタイプ	サポート状況	互換性情報
.NET Core	dotnet-core	サポート対象	<a href="#">サポート対象の .NET Core テクノロジ (196ページ)</a>
Java	java	サポート対象	<a href="#">サポート対象の Java テクノロジ (57ページ)</a>
Node.js	nodejs または nodejs-protect	サポート対象	<a href="#">サポート対象の Node.js テクノロジ (251ページ)</a>
PHP	php	ベータ版	<a href="#">サポート対象の PHP テクノロジ (298ページ)</a>



### 注記

- PHP アプリケーションでのエージェントの組み込みはベータ版です。ベータ版は機能が変更されたり、予期しない動作をしたりする可能性があります。この機能を利用することで、お客様は [Contrast ベータ版利用規約 \(828ページ\)](#) に同意することになります。
- Node.js エージェントを組み込むと、エージェントを組み込まれたアプリケーションの起動時間が大幅に増加する場合があります。起動時間が許容できない場合は、コンパイル時にエージェントを組み込むことをお勧めします。コンパイル時に Node.js エージェントを組み込む場合は、オペレータによるランタイム時の組み込みは無効化して下さい。詳しくは、[リライター CLI \(294ページ\)](#) を参照してください。

## エージェントオペレータのインストール

Contrast は、クラスタに直接適用できる単一のインストール用 YAML ファイルを提供し、適切なデフォルト値を提供します。お客様の環境に応じて追加で修正することも可能です。

### カスタムレジストリ

エアギャップ環境でエージェントオペレータを使用する場合(もしくは、Docker Hub を使用できない場合は)、[☑ Contrast カスタムレジストリのサンプル](#)を参考にしてください。

### 手順

1. クラスタ管理者として kubectl(Kubernetes)または oc(OpenShift)を使用して以下を実行し、オペレータマニフェストを適用します。

```
kubectl apply -f https://github.com/Contrast-Security-OSS/agent-operator/releases/latest/download/install-prod.yaml
```

```
oc apply -f https://github.com/Contrast-Security-OSS/agent-operator/releases/latest/download/install-prod.yaml
```

このマニフェストによって以下が行われます。

- contrast-agent-operator ネームスペースを作成
- オペレータのデプロイメントワークロードをインストール
- 必要なカスタムリソース定義(CRD)をインストール
- 最低限必要な権限でロールベースのアクセス制御(RBAC)を設定

- オペレータを Admission Webhook へ登録



### 注記

デフォルトの `contrast-agent-operator` 以外のネームスペースにインストールすることも可能ですが、その場合はデプロイメントマニフェストの修正が必要になります。

2. オペレータマニフェストを適用した後、クラスタが集約されるのを待ちます。

```
kubectl -n contrast-agent-operator wait pod --for=condition=ready --selector=app.kubernetes.io/name=operator,app.kubernetes.io/part-of=contrast-agent-operator --timeout=30s
```

```
oc -n contrast-agent-operator wait pod --for=condition=ready --selector=app.kubernetes.io/name=operator,app.kubernetes.io/part-of=contrast-agent-operator --timeout=30s
```

3. Wait コマンドが成功すると、オペレータは [設定可能 \(47ページ\)](#) な状態になります。

### 関連項目

- [エージェントオペレータのチュートリアル \(43ページ\)](#)
- [エージェントオペレータの最小設定 \(47ページ\)](#)
- [エージェントオペレータのテレメトリ \(56ページ\)](#)

## エージェントオペレータのチュートリアル

### 開始する前に

ここでは、Vanilla Kubernetes を使用して、Contrast エージェントオペレータのインストールと、クラスタ管理者としてサンプルワークロードを組み込む方法について説明します。

OpenShift を使用してこの例を実行するには、Kubernetes のコマンドを同等の OpenShift コマンドに置き換えてください。すべてのコマンドは、Bash などのターミナル内で実行します。

Kubernetes および関連するソフトウェアの仕組みについて、基本的な理解があることを前提としています。必要に応じて、お客様の環境に合わせて手順を調整してください。

### 手順 1: オペレータのインストール

オペレータをインストールするには、オペレータのマニフェストをクラスタに適用する必要があります。Contrast は、クラスタに直接適用できる単一のインストール用 YAML ファイルを提供し、適切なデフォルト値を提供します。お客様の環境に応じて追加で修正することも可能ですが、その場合は [Kustomize](#) などの設定管理ツールを使用することをお勧めします。



### 注記

このインストール用 YAML ファイルによって、`contrast-agent-operator` ネームスペースが作成されてインストールが行われます。このネームスペースを後で使用します。

クラスタが集約されるのをしばらく待つと、オペレータのステータスが `Running` になります。

```
% kubectl -n contrast-agent-operator get pods
```

NAME	READY	STATUS	RESTARTS	AGE
contrast-agent-operator-57f5cfbf7-9svtt	1/1	Running	0	27s
contrast-agent-operator-57f5cfbf7-fp4vp	1/1	Running	0	39s

オペレータを設定する準備ができました。

## 手順 2：オペレータの設定

クラスタのワークロードを組み込む前に、まずオペレータを設定する必要があります。

Kubernetes のシークレットを使用して、接続の認証キーを保存します。以下を実行すると、default-agent-connection-secret という名前で Secret が作成され、contrast-agent-operator ネームスペースに作成されます。

```
% kubectl -n contrast-agent-operator \  
  create secret generic default-agent-connection-secret \  
  --from-literal=apiKey=TODO \  
  --from-literal=serviceKey=TODO \  
  --from-literal=username=TODO  
  
secret/default-agent-connection-secret created
```



### 注記

TODO を、ご利用の Contrast サーバで該当する値に置き換えてください。[エージェントキーの検索 \(37ページ\)](#)で、Contrast Web インタフェースからエージェントキーを取得する方法について説明しています。

接続の設定を完了するには、ClusterAgentConnection が必要です。以下を実行すると、contrast-agent-operator ネームスペースで ClusterAgentConnection が作成され、前述の手順で作成した Secret のキー値を参照します。

```
% kubectl apply -f - <<EOF  
apiVersion: agents.contrastsecurity.com/v1beta1  
kind: ClusterAgentConnection  
metadata:  
  name: default-agent-connection  
  namespace: contrast-agent-operator  
spec:  
  template:  
    spec:  
      url: https://app.contrastsecurity.com/Contrast  
      apiKey:  
        secretName: default-agent-connection-secret  
        secretKey: apiKey  
      serviceKey:  
        secretName: default-agent-connection-secret  
        secretKey: serviceKey  
      userName:  
        secretName: default-agent-connection-secret  
        secretKey: userName  
EOF
```

```
clusteragentconnection.agents.contrastsecurity.com/default-agent-connection created
```



### 注記

ClusterAgentConnection の名前は重要ではなく、任意の名前を付けることができます。

これでオペレータが設定され、既存のワークロードにエージェントを組み込めるようになりました。

### 手順 3 : ワークロードへの組み込み

この例では、Deployment ワークロードを使用する [ASP.NET Core のサンプルアプリケーション](#) に Contrast .NET Core エージェントを組み込む方法について説明します。

まず、ASP.NET Core のサンプルアプリケーションをクラスタにデプロイします。以下を実行すると、default のネームスペースに Deployment が作成されます。

```
% kubectl apply -f - <<EOF
apiVersion: apps/v1
kind: Deployment
metadata:
  name: hello-world-app
  namespace: default
  labels:
    arbitrary-label: arbitrary-value
spec:
  selector:
    matchLabels:
      app: hello-world-app
  template:
    metadata:
      labels:
        app: hello-world-app
    spec:
      containers:
        - image: contrast/sample-app-aspnetcore:latest
          name: hello-world-app
EOF

deployment.apps/hello-world-app created
```

クラスタが集約されるのをしばらく待つと、デプロイされたワークロードのステータスが Running になります。

```
$% kubectl -n default get pods

NAME                                READY   STATUS    RESTARTS   AGE
hello-world-app-7479d5ff96-p28zx    1/1     Running   0           19s
```

次に、AgentInjector 設定エンティティを使用して、.NET Core エージェントを組み込むようにオペレータを設定します。この場合、AgentInjector は、前述の Deployment がデプロイされたのと同じネームスペース(この場合は default)に作成する必要があります。

```
% kubectl apply -f - <<EOF
apiVersion: agents.contrastsecurity.com/v1beta1
```

```
kind: AgentInjector
metadata:
  name: injector-for-hello-world
  namespace: default
spec:
  type: dotnet-core
  selector:
    labels:
      - name: arbitrary-label
        value: arbitrary-value
EOF

agentinjector.agents.contrastsecurity.com/injector-for-hello-world created
```

hello-world-app の Pod のログを見ると、Contrast の .NET Core エージェントがアプリケーションに組み込まれていることを確認できます。

```
% kubectl -n default logs Deployment/hello-world-app

Defaulted container "hello-world-app" out of: hello-world-app, contrast-init (init)
warn: \
Microsoft.AspNetCore.DataProtection.Repositories.FileSystemXmlRepository[60]
  Storing keys in a directory '/root/.aspnet/DataProtection-Keys' that \
may not be persisted outside of the container. Protected data will be \
unavailable when container is destroyed.
warn: Microsoft.AspNetCore.DataProtection.KeyManagement.XmlKeyManager[35]
  No XML encryptor configured. Key \
{0ad20893-267f-4635-99b0-1ee74bccbc8b} may be persisted to storage in \
unencrypted form.

  _.-|_____|                | \_ / , |   ( ` \
  [  |_____|                | o o |__ _ )
  `-.|_____|                _.( T   ) ` /
app.contrastsecurity.com
  .--'-`-.      _(( _ `^--' /_< \
  .+|_____|__.-||__>`-'(((/  (((/
Contrast .NET Core Agent 2.1.13.0
Contrast UI: https://
Mode:          Assess & Protect

info: Microsoft.Hosting.Lifetime[14]
  Now listening on: http://[::]:80
info: Microsoft.Hosting.Lifetime[0]
  Application started. Press Ctrl+C to shut down.
info: Microsoft.Hosting.Lifetime[0]
  Hosting environment: Production
info: Microsoft.Hosting.Lifetime[0]
  Content root path: /app/
```

#### 手順 4 : オペレータのアンインストール(任意)

クラスタを元の状態に復元するには、まず既存の AgentInjector を削除します。

```
% kubectl -n default delete agentinjector injector-for-hello-world

agentinjector.agents.contrastsecurity.com "injector-for-hello-world" deleted
```

その後、オペレータは、組み込まれた全てのワークロードを組み込み前の状態に復元します。クラスタが集約されたら、オペレータを安全に削除できます。

```
% kubectl delete -f https://github.com/Contrast-Security-OSS/agent-operator/
releases/latest/download/install-prod.yaml

namespace "contrast-agent-operator" deleted
customresourcedefinition.apiextensions.k8s.io "agentconfigurations.agents.co
ntrastsecurity.com" deleted
customresourcedefinition.apiextensions.k8s.io "agentconnections.agents.contr
astsecurity.com" deleted
customresourcedefinition.apiextensions.k8s.io "agentinjectors.agents.contras
tsecurity.com" deleted
customresourcedefinition.apiextensions.k8s.io "clusteragentconfigurations.ag
ents.contrastsecurity.com" deleted
customresourcedefinition.apiextensions.k8s.io "clusteragentconnections.agent
s.contrastsecurity.com" deleted
serviceaccount "contrast-agent-operator-service-account" deleted
clusterrole.rbac.authorization.k8s.io "contrast-agent-operator-service-
role" deleted
clusterrolebinding.rbac.authorization.k8s.io "contrast-agent-operator-
service-role-binding" deleted
service "contrast-agent-operator" deleted
deployment.apps "contrast-agent-operator" deleted
poddisruptionbudget.policy "contrast-agent-operator" deleted
mutatingwebhookconfiguration.admissionregistration.k8s.io "contrast-web-
hook-configuration" deleted
```

## 関連項目

- [エージェントオペレータのインストール \(42ページ\)](#)
- [エージェントオペレータの最小設定 \(47ページ\)](#)
- [エージェントオペレータの設定 \(51ページ\)](#)

## エージェントオペレータの最小設定

オペレータのすべての設定は、[カスタムリソース定義\(CRD\)](#)によって定義された Kubernetes ネイティブの設定エンティティを使用することで処理されます。CRD はオペレータと共にデプロイされ、オペレータの設定エンティティの処理方法が定義されます。

Visual Studio Code の Kubernetes [拡張機能](#)などのツールは、クラスタ内でエンティティを正しい構文で作成するのに役立ちます。

完全なスキーマは、[エージェントオペレータの設定 \(51ページ\)](#)に記載しています。本項では、必要な最小限の設定についてのみ説明し、すべての設定は記載していません。

## 最小限の設定

最小限の設定では、3つのマニフェストが必要です。

1. 1つ目は、標準の Kubernetes の Secret に Contrast サーバインスタンスへの認証に必要な接続キーを含めます。この Secret は、ClusterAgentConnection エンティティと同じネームスペースにデプロイする必要があります。指定するエージェントキーは、[エージェントキーの検索 \(37ページ\)](#)で確認できます。

```
apiVersion: v1
kind: Secret
metadata:
  name: default-agent-connection-secret
  namespace: contrast-agent-operator
type: Opaque
stringData:
```

```
apiKey: TODO
serviceKey: TODO
userName: TODO
```

2. 2つ目は、ClusterAgentConnection の設定エンティティです。ClusterAgentConnection には、クラスタ内のエージェントのデフォルトの接続設定を指定し、接続の認証キーが含まれる前述の Secret をマップします。セキュリティ上、ClusterAgentConnection エンティティは、オペレータを使用するのと同じ名前スペースに配置する必要があります。この例では、デフォルトの名前スペース contrast-agent-operator がカスタマイズされていないことを前提にしています。

```
apiVersion: agents.contrastsecurity.com/v1beta1
kind: ClusterAgentConnection
metadata:
  name: default-agent-connection
  namespace: contrast-agent-operator
spec:
  template:
    spec:
      url: https://app.contrastsecurity.com/Contrast
      apiKey:
        secretName: default-agent-connection-secret
        secretKey: apiKey
      serviceKey:
        secretName: default-agent-connection-secret
        secretKey: serviceKey
      userName:
        secretName: default-agent-connection-secret
        secretKey: userName
```

3. 3つ目に必要なのは、AgentInjector の設定エンティティです。AgentInjector は、AgentInjector がデプロイされる名前スペース内で metadata.labels などのワークロードのラベルを使用して、自動でエージェントを組み込む対象となるワークロードを選択します。

```
apiVersion: agents.contrastsecurity.com/v1beta1
kind: AgentInjector
metadata:
  name: dotnet-hello-world
  namespace: default
spec:
  type: dotnet-core
  selector:
    labels:
      - name: app
        value: dotnet-hello-world
```

このマニフェストの例では、Contrast エージェントオペレータは、デフォルトの名前スペースで app = dotnet-hello-world というラベルが付いているワークロード(Deployment、DeploymentConfig など)に Contrast の .NET エージェントを自動的に組み込みます。

## 関連項目

- [エージェントオペレータの設定 \(51ページ\)](#)
- [エージェントオペレータのサポート対象テクノロジー \(41ページ\)](#)

## オペレータのアップグレード

Contrast エージェントオペレータは、[セマンティックバージョンング](#)に従います。



- バージョンには、オペレーター API への重大な変更が含まれる場合があります。メジャーバージョンのアップグレードでは、マニフェストが変更されていたり、既存の CRD の更新が必要な場合があるため注意が必要です。
- バージョンには新機能が含まれていますが、完全な後方互換性があり既存のクラスタに適用しても安全です。新しい機能を使用するために、オプションのマニフェストの変更が必要な場合があります。
- にはセキュリティおよびバグフィックスが含まれており、完全な後方互換性があるため既存のクラスタに安全に適用することができます。マニフェストの変更は必要ありません。

Contrast では、以下の形式でイメージタグを公開しています。

```
:2
:2.1
:2.1.10
:latest
```

ここで、:2 は 2.X.X セマンティックバージョンブランチの最新リリースを表します。アップグレードを簡素化するために、リスク許容度に基づいて接頭辞のバージョンを使用することもできます (imagePullPolicy が Always に設定されていることを確認してください)。



### 注記

Contrast エージェントオペレータは、複数のレプリカとリーダーリースを使用する可用性の高い構成をサポートしていますが、すべてのオペレーターインスタンスが同じバージョンを長期間実行しているデプロイメントのみをサポートします。

imagePullPolicy オプションを使用して、複数のインスタンスを同じバージョンに維持しないでください。自動アップグレードが必要な場合は、Keel などのオペレータを使用して安全にアップグレードすることをお勧めします。

## マイナーおよびパッチアップグレード

新しいバージョンへのアップグレードは、新しいクラスタにインストールするのと同じ手順で行います。クラスタ管理者として kubectl(Kubernetes)または oc(OpenShift)を使用して以下を実行し、オペレータマニフェストを適用します。

```
kubectl apply -f https://github.com/Contrast-Security-OSS/agent-operator/releases/latest/download/install-prod.yaml
```

```
oc apply -f https://github.com/Contrast-Security-OSS/agent-operator/releases/latest/download/install-prod.yaml
```

## メジャーアップグレード

メジャーアップグレードには、マニフェストの追加変更が含まれる場合があります。contrast-agent-operator ネームスペースのみを削除すれば、インストールされた CRD(さらにクラスタ構成も)は維持されます。

```
kubectl delete namespace contrast-agent-operator
kubectl apply -f https://github.com/Contrast-Security-OSS/agent-operator/releases/latest/download/install-prod.yaml
```

```
oc delete project contrast-agent-operator
oc apply -f https://github.com/Contrast-Security-OSS/agent-operator/releases/latest/download/install-prod.yaml
```

ここでの一般的な手順はほとんどのメジャーアップグレードで有効ですが、メジャーアップグレードを確実にを行うためにはリリースノートに記載される移行手順がある場合には、その手順に従ってください。

## 関連項目

- [エージェントオペレータの設定 \(51ページ\)](#)
- [オペレータのサポート対象テクノロジー \(41ページ\)](#)

## エージェントオペレータのアンインストール

Contrast エージェントオペレータは、すべてのデータを Kubernetes のバックプレーンに保存し、クラスタから削除するとすべての変更が完全に削除されるように設計されています。すべてを正しくクリアするために、以下のステップを順番に実行することをお勧めします。

```
kubectl delete crd agentconfigurations.agents.contrastsecurity.com
kubectl delete crd agentconnections.agents.contrastsecurity.com
kubectl delete crd agentinjectors.agents.contrastsecurity.com
kubectl delete crd clusteragentconfigurations.agents.contrastsecurity.com
kubectl delete crd clusteragentconnections.agents.contrastsecurity.com
```

```
oc delete crd agentconfigurations.agents.contrastsecurity.com
oc delete crd agentconnections.agents.contrastsecurity.com
oc delete crd agentinjectors.agents.contrastsecurity.com
oc delete crd clusteragentconfigurations.agents.contrastsecurity.com
oc delete crd clusteragentconnections.agents.contrastsecurity.com
```

CRD を削除すると、オペレータの設定エンティティが自動的に削除されます。設定エンティティが削除された後、Contrast エージェントオペレータがクラスタワークロードに加えた変更が元に戻ります。



### 注記

これにより、オペレータが組み込んだワークロードの数によっては、Kubernetes が影響を受けたワークロードを再度デプロイするため、デプロイされたポッドが大幅に入れ替わる可能性があります。大規模なクラスタでは注意が必要です。

クラスタが静止した後、オペレータは安全に削除できます。

```
kubectl delete -f https://github.com/Contrast-Security-OSS/agent-operator/releases/latest/download/install-prod.yaml
```

```
oc delete -f https://github.com/Contrast-Security-OSS/agent-operator/releases/latest/download/install-prod.yaml
```



### 注記

推奨通りに最初の手順で CRD を削除した場合は、CRD の欠落に関するエラーは正常です。

## エージェントオペレータの設定

ここでは、Contrast エージェントオペレータがアクセスする全ての設定エンティティのスキーマについて説明します。一部のエンティティは、オプション(任意)となります。

### AgentConfiguration

```
apiVersion: agents.contrastsecurity.com/v1beta1
kind: AgentConfiguration
metadata:
  name: example-agent-configuration
  namespace: default
spec:
  yaml: |
    server:
      environment: QA
  suppressDefaultServerName: false
  suppressDefaultApplicationName: false
```

プロパティ	型	必須	デフォルト値	説明
spec.yaml	string	任意		ドキュメントの「YAML 設定」で説明している YAML 設定ファイル
spec.suppressDefaultServerName	boolean	任意	False	False の場合、デフォルト(通常は Pod 名)を使用せずに、挿入されるワークロード('kubernetes-{namespace}')に Contrast サーバ名が自動的に設定されます。
spec.suppressDefaultApplicationName	boolean	任意	False	False の場合、デフォルト(エージェントが生成)を使用せずに、挿入されるワークロード(ワークロード名)に Contrast アプリケーション名が自動的に設定されます。



#### 注記

接続キーは、YAML ファイルで指定しても無視されるので、YAML ファイルで指定しないでください。

### AgentConnection

```
apiVersion: agents.contrastsecurity.com/v1beta1
kind: AgentConnection
metadata:
  name: example-agent-connection
  namespace: default
spec:
  url: https://app.contrastsecurity.com/Contrast
  apiKey:
    secretName: example-agent-connection-secret
    secretKey: apiKey
  serviceKey:
    secretName: example-agent-connection-secret
    secretKey: serviceKey
  userName:
    secretName: example-agent-connection-secret
    secretKey: userName
```

プロパティ	型	必須	デフォルト値	説明
spec.url	string	○		Contrast サーバの URL
spec.apiKey.secretName	string	○		apiKey(API キー)を指定している Secret の名前
spec.apiKey.secretKey	string	○		apiKey(API キー)を指定している Secret での値に対するキー
spec.serviceKey.secretName	string	○		serviceKey(エージェントサービスキー)を指定している Secret の名前
spec.serviceKey.secretKey	string	○		serviceKey(エージェントサービスキー)を指定している Secret での値に対するキー
spec.userName.secretName	string	○		userName(エージェントユーザ名)を指定している Secret の名前
spec.userName.secretKey	string	○		userName(エージェントユーザ名)を指定している Secret での値に対するキー



**重要**

セキュリティ上、これらの Secret は AgentConnection と同じネームスペースに含まれる必要があります。

## AgentInjector

```
apiVersion: agents.contrastsecurity.com/v1beta1
kind: AgentInjector
metadata:
  name: example-injector-dotnet-core
  namespace: default
spec:
  enabled: true
  version: latest
  type: dotnet-core
  image:
    registry: docker.io/contrast
    name: agent-dotnet-core
    pullSecretName: contrastdotnet-pull-secret
    pullPolicy: Always
  selector:
    images:
      - "*"
    labels:
      - name: app
        value: example-*
  connection:
    name: example-agent-connection
  configuration:
    name: example-agent-configuration
```

プロパティ	型	必須	デフォルト値	説明
spec.enabled	boolean	任意	TRUE	このエージェントの組み込みを有効または無効にします。

プロパティ	型	必須	デフォルト値	説明
spec.version	string	任意	latest	組み込む Contrast エージェントのバージョン。リテラルの 'latest' は、最新バージョンを組み込みます。バージョンの部分一致に対応しています。例えば、'2' を指定すると、バージョン '2.1.0' が選択されます。
spec.type	agentType	○		組み込むエージェントのタイプ。'dotnet-core'、'java'、'nodejs' が 'nodejs-protect'、'php' のいずれかを指定できます。
spec.image.registry	string	任意	docker.io/contrast	エージェントイメージをダウンロードするために使用するイメージレジストリ。このレジストリには、組み込まれる Pod とオペレータがアクセスできる必要があります。
spec.image.name	string	任意	{タイプによる}	組み込むイメージに使用する名前
spec.image.pullSecretName	string	任意		Pod の imagePullSecrets リストに追加するプルシークレットの名前
spec.image.pullPolicy	string	任意	Always	Contrast のイメージを取得する際に使用するプルポリシー。詳細は、Kubernetes の imagePullPolicy を参照してください。
spec.selector.images	string[]	任意	Pod にあるすべてのコンテナを選択	エージェントを組み込むコンテナイメージ。Glob パターン(ワイルドカード)に対応しています。
spec.selector.labels	labelSelector[]	任意	ネームスペースにあるすべてのワークロードを選択	Deployment/StatefulSet/DaemonSet/DeploymentConfig のラベルで、その Pod がエージェントを組み込みむ対象となります。
spec.connection.name	string	任意	ClusterAgentConnection で指定された AgentConnection がデフォルト	AgentConnection のリソース名。同じネームスペース内に存在する必要があります。
spec.configuration.name	string	任意	ClusterAgentConfiguration で指定された AgentConfiguration がデフォルト	AgentConfiguration のリソース名。同じネームスペース内に存在する必要があります。

- 既存の AgentInjector を無効にすると、選択したワークロードから全てのエージェントの組み込みが削除されます。
- 参照する AgentConnection と AgentConfiguration は、AgentInjector と同じネームスペースに存在する必要があります。
- カスタムレジストリを使用する場合、挿入される Pod とオペレータの両方が、デフォルトのプルシークレットまたはカスタムのプルシークレットを通じて、アクセスできる必要があります。
- 本番前の環境でエージェントを使用する場合は、エージェントバージョンの latest を推奨します。
- AgentInjector は、Deployment、StatefulSet、DaemonSet、および DeploymentConfig(OpenShift 上) ワークロードを選択することをサポートします。Pod を直接挿入することはサポートされていません。
- 選択したワークロードが 1 つの Pod で多くのコンテナを作成する場合、spec.selector.images を使用して、組み込まれるコンテナをフィルタリングすることができます。

## labelSelector

プロパティ	型	必須	デフォルト値	説明
name	string	<input type="radio"/>		一致させるラベルの名前
value	string	<input type="radio"/>		一致させるラベルの値。Glob パターン(ワイルドカード)に対応していません。



### 注記

ラベルの選択(複数)は、論理 AND 演算を使用して累積します。

## agentType

エージェント	エージェントタイプ
.NET Core	dotnet-core
Java	java
Node.js	node.js
	または nodejs-protect
PHP	php

タイプの情報については、[オペレータのサポート対象テクノロジー \(41ページ\)](#)も参照してください。

## ClusterAgentConfiguration

```

apiVersion: agents.contrastsecurity.com/v1beta1
kind: ClusterAgentConfiguration
metadata:
  name: default-agent-configuration
  namespace: contrast-agent-operator
spec:
  namespaces:
    - default
  template:
    spec:
      yaml: |
        server:
          environment: QA
    
```

プロパティ	型	必須	デフォルト値	説明
spec.namespaces	string[]	任意	全てのネームスペース	この AgentConfiguration テンプレートを適用するネームスペース。Glob パターン(ワイルドカード)に対応しています。
spec.template	AgentConfiguration	<input type="radio"/>		'spec.namespaces'で選択したネームスペースに適用するデフォルトの AgentConfiguration



### 注記

セキュリティ上、ClusterAgentConfiguration マニフェストは、オペレータと同じネームスペースにデプロイする必要があります。

## ClusterAgentConnection

```

apiVersion: agents.contrastsecurity.com/v1beta1
kind: ClusterAgentConnection
metadata:
  name: default-agent-connection
  namespace: contrast-agent-operator
spec:
  namespaces:
    - default
  template:
    spec:
      url: http://app.contrastsecurity.com/Contrast
      apiKey:
        secretName: default-agent-connection-secret
        secretKey: apiKey
      serviceKey:
        secretName: default-agent-connection-secret
        secretKey: serviceKey
      userName:
        secretName: default-agent-connection-secret
        secretKey: userName
  
```

プロパティ	型	必須	デフォルト値	説明
spec.namespaces	string[]	任意	全てのネームスペース	この AgentConfiguration テンプレートを適用するネームスペース。Glob パターン(ワイルドカード)に対応しています。
spec.template	AgentConnection	○		'spec.namespaces'で選択したネームスペースに適用するデフォルトの AgentConnection



### 注記

- セキュリティ上、ClusterAgentConnection マニフェストは、オペレータと同じネームスペースにデプロイする必要があります。
- ClusterAgentConnection で参照する Secret は、ClusterAgentConnection エンティティをデプロイするのと同じネームスペースに存在する必要があります。

### 関連項目

- [エージェントオペレータのインストール \(42ページ\)](#)
- [エージェントオペレータのサポート対象テクノロジー \(41ページ\)](#)
- [エージェントオペレータのテレメトリ \(56ページ\)](#)

### .NET Core エージェントによるプロファイラチェーンのサポート

.NET Core エージェントは、[Contrast エージェントオペレータ \(41ページ\)](#)と組み合わせて、[Dynatrace オペレータ](#)を使用する Dynatrace でのプロファイラチェーンをサポートします。Dynatrace オペレータを使用して Dynatrace エージェントをワークロードに組み込むと、自動的にサポートが有効になります。

Dynatrace オペレータを classicFullStack モードで使用する場合は、Contrast エージェントオペレータの環境変数の `CONTRAST_ENABLE_EARLY_CHAINING=true` を設定し、対象のポッドを再起動します。こちらの [マニフェストのサンプル](#)も参考にしてください。

ベンダー	バージョン	サポート対象の検証日
Dynatrace	Operator バージョン 0.6.0	2022/06/09

今後の Dynatrace のバージョンによっては、チェーンが壊れる可能性があります。チェーンによって非互換性が生じる可能性があり、`agent.dotnet.enable_chaining: false` オプションを使用して無効にすることができます。

## エージェントオペレータのテレメトリ

Contrast エージェントオペレータは、テレメトリを使用して、使用状況に関するデータを収集します。テレメトリは、オペレータが最初にクラスタにインストールされた時に収集され、その後も定期的に(数時間ごと)に収集されます。

弊社では、お客様のプライバシーは非常に大切であると考えています。このテレメトリ機能は、アプリケーションのデータを収集するものではありません。データは匿名化されてから、Contrast に安全に送信されます。そして、集約されたデータは暗号化されて保存され、アクセスが制限されます。収集されたデータは、全て 1 年後に削除されます。

テレメトリ機能を停止するには、`CONTRAST_AGENT_TELEMETRY_OPTOUT` という環境変数に 1 または `true` を設定してください。

テレメトリのデータは、`telemetry.dotnet.contrastsecurity.com` に安全に送信されます。ネットワークレベルで通信をブロックすることで、テレメトリ機能を停止することもできます。

テレメトリ機能で収集されるのは、以下のデータです。

### オペレータ バージョン 0.3.0

- オペレータのバージョン
- オペレータの稼働時間
- Kubernetes API によって公開されたクラスタのバージョン情報とプラットフォーム
- クラスタ ID の暗号化(SHA256)匿名ハッシュで、オペレータが最初に起動した時にランダムに生成されてオペレータのネームスペースに Secret として格納される GUID
- クラスタ内の監視対象リソースの数(全てのオペレータエンティティ、DaemonSets、DeploymentConfigs、Deployments、Namespaces、Pods、Secrets、StatefulSets など)
- オペレータが内部でスローした例外(ログメッセージ、例外タイプ、例外メッセージ、スタックトレースフレームなど)

## 環境変数

環境変数を使用して、サポート対象のプロパティをエージェントに設定することができます。

環境変数は、エージェントの起動前に指定し、エージェントがアクセスできる場所に設定する必要があります。環境変数は、同じプロセス内でもシステム全体でも設定できます。



### 重要

システム全体の環境変数を設定する場合、同じサーバで実行中の他の Contrast エージェントに影響を与える可能性があります。

Contrast のプロパティは、コマンドライン、YAML 設定、環境変数に変換できます。

コマンドライン形式の変数を環境変数に変換するには、パスセグメントの区切り記号(.)をアンダースコア 2 つ(\_)に置き換えます。



YAML 形式の変数を環境変数に変換するには、最上位のプロパティから始めて、ネストされたすべてのプロパティをアンダースコア 2 つ( )で区切ります。

そして、「contrast」というネームスペース( contrast.か CONTRAST\_)を先頭に付けます。

環境変数はすべて大文字で、スペースを入れないでください。

例 :

コマンドライン	YAML プロパティ	環境変数
contrast.server.name	server: name:	CONTRAST_SERVER_NAME
contrast.api.api_key	api: api_key:	CONTRAST_API_API_KEY

各エージェントでサポートされているすべてのプロパティの一覧は、それぞれの YAML テンプレートで確認できます。

- [Go \(456ページ\)](#)
- [Java \(79ページ\)](#)
- [.NET Framework \(154ページ\)](#)
- [.NET Core \(214ページ\)](#)
- [Node.js \(264ページ\)](#)
- [PHP \(301ページ\)](#)
- [Python \(320ページ\)](#)
- [Ruby \(397ページ\)](#)

## Java エージェント

Contrast の Java エージェントによって、Java ベースのアプリケーションで、Contrast Assess や Contrast Protect による解析が可能になります。エージェントは、従来のアプリケーションサーバで構築される Java の Web アプリケーションや、Netty、Play、Spring Boot などで構築される新しい Java の Web アプリケーションを解析します。JVM があれば、Java エージェントは詳細なセキュリティ情報を提供できます。

アプリケーションが実行されると、Java エージェントのセンサーがアプリケーションのセキュリティ、アーキテクチャ、ライブラリに関する情報を収集します。エージェントによる解析の結果は、Contrast Web インターフェイスで確認できます。

アプリケーションの解析を開始するには、[Java エージェントをインストール \(59ページ\)](#)します。

## Java(Kotlin、Scala)エージェントのサポート対象テクノロジー

### Java エージェント

テクノロジー	サポート対象バージョン	備考
Java ランタイム	<ul style="list-style-type: none"> <li>• IBM 8</li> <li>• Oracle 8 *バージョン 11 以降は OpenJDK のサポートに従う</li> <li>• OpenJDK 8、11、12、13、14、15、16、17、18、19</li> </ul>	<p>OpenJDK のサポートは、ここに示す現在のサポート対象バージョンの範囲内で、全ての公開中のビルドで動作するように設計されています。一般的によく利用される Azul や Amazon Corretto などもサポート対象の JDK のカテゴリに入ります。</p> <p><b>サポート対象外 :</b></p> <p>JDK プレビュー機能</p>

テクノロジー	サポート対象バージョン	備考
旧 Java エージェント (136ページ)の Java ランタイム  Java エージェント 3.x のみ での使用	<ul style="list-style-type: none"> <li>• IBM 6、7</li> <li>• Oracle 6、7</li> <li>• OpenJDK 6、7</li> </ul>	<b>参考</b> <ul style="list-style-type: none"> <li>• <a href="#">☑サポート速報 : Java6 および Java7 のサポート終了について</a></li> <li>• <a href="#">☑FAQ : Java6 および Java7 のサポート終了について</a></li> </ul>
アプリケーションサーバ	<ul style="list-style-type: none"> <li>• GlassFish 4</li> <li>• Grizzly 2.3.20 以降</li> <li>• JBoss EAP 6.x および 7.x</li> <li>• Jetty 7、8、9、10、11</li> <li>• Karaf 3.0.x</li> <li>• Netty 4.x</li> <li>• Play 2.4</li> <li>• Resin 4</li> <li>• Tomcat 5、6、7、8、9、10</li> <li>• Vert.x 3.1.0、4.x</li> <li>• WebLogic 10、11g、12c</li> <li>• WebSphere* 8.5、9.0</li> <li>• WebSphere Liberty 22</li> <li>• WildFly 10、11、14、18</li> </ul>	* zSeries および AIX の環境ではサポートが限定されません。SPARC Solaris で WebSphere を使用する場合、バージョン 8.5.5.11 が必須となります。  <b>ルートカバレッジのサポート :</b> <ul style="list-style-type: none"> <li>• GlassFish 4</li> <li>• Jetty 11.0、10.0、9.4、8.1、7.6</li> <li>• Resin 4.0</li> <li>• Tomcat 5、6、7、8、9</li> <li>• WebLogic 12</li> <li>• WebSphere 8.5、9.0</li> <li>• Wildfly 10、11、14、18</li> </ul>
オプティマイザ	Proguard	Proguard にある Java バイトコードの最適化機能は、Contrast のようなランタイムエージェントが基本前提とする動きに反します。Proguard ユーザが、Contrast を利用してアプリケーションを保護する場合は、Proguard の <code>-dontoptimize</code> 設定オプションを使用して最適化を行わないようにする必要があります。
データベース	<ul style="list-style-type: none"> <li>• DB2</li> <li>• DynamoDB</li> <li>• MySQL</li> <li>• Oracle</li> <li>• PostgreSQL</li> <li>• SQL Server</li> <li>• SQLite JDBC ドライバ</li> </ul>	
メッセージングサービス	<ul style="list-style-type: none"> <li>• JMS 2.0</li> <li>• IBM MQ 9.x</li> <li>• Spring JMS 2.x</li> </ul>	<ul style="list-style-type: none"> <li>• エージェントのバージョン : Java 4.7.0 以降</li> <li>• Contrast のバージョン : 3.9.9 以降</li> </ul>
	<ul style="list-style-type: none"> <li>• Kafka メッセージキュー・ストリーミング</li> </ul>	<ul style="list-style-type: none"> <li>• エージェントのバージョン : Java 5.0.0 以降</li> </ul>

テクノロジー	サポート対象バージョン	備考
その他の Java テクノロジー	<ul style="list-style-type: none"> <li>• ADF JSF</li> <li>• Apache POI、Fileupload、HttpComponents</li> <li>• Axis (RPC)、XMLRPC、RMI、Apache CXF、JMS (javax.jms)</li> <li>• Direct Web Remoting (DWR)</li> <li>• DropWizard</li> <li>• Freemarker</li> <li>• Glowroot*</li> <li>• GSON、Kryo、minidev、org.json</li> <li>• Google Web Toolkit (GWT)</li> <li>• Hibernate</li> <li>• http4k(4.6.0.0 と 4.17、Contrast Assess 対象)</li> <li>• J2SE</li> <li>• JDBC、JDBI、MongoDB</li> <li>• JSF (MyFaces、RichFaces、Sun)</li> <li>• java.nio、java.beans</li> <li>• Java EE/J2EE、Servlet/JSP</li> <li>• Jersey</li> <li>• MyBatis</li> <li>• OWASP ESAPI、AntiSamy、Coverity</li> <li>• Quarkus RESTEasy</li> <li>• Seam</li> <li>• Spring、Spring Boot、Spring AOP</li> <li>• Struts、Struts 2</li> <li>• Wicket</li> <li>• XStream、Jackson (JSON/XML)</li> <li>• Xerces、JAXB、nu.xom</li> </ul>	<p>* Glowroot を使用する場合、glowroot.jar よりも前に、Contrast エージェントの jar を指定して、ロードする必要があります。</p> <p><b>ルートカバレッジのサポート：</b></p> <ul style="list-style-type: none"> <li>• http4k-core 4.17</li> <li>• http4k-core 4.6</li> <li>• Jersey 2.25、2.28、2.36、2.6</li> <li>• Quarkus RESTEasy 2.15</li> <li>• Spring Web VMC 4.2、5.3、6.0</li> <li>• Struts 2</li> </ul>

## Kotlin

テクノロジー	サポート対象バージョン
Contrast エージェント	3.9.1.25108 以降
Java ランタイム	JDK 8 以上
Kotlin のバージョン	1.5.x

## Scala

テクノロジー	サポート対象バージョン
Contrast エージェント	3.8.11.23624 以降
Java ランタイム	JDK 8 以上
Scala のバージョン	2.12、2.13
	ルートカバレッジのサポート対象
Play のバージョン	2.6、2.7、2.8
Akka HTTP	10.2.4

## WebSphere の設定

WebSphere をアプリケーションサーバとして使用している場合は、エージェントをデプロイする前に、[WebSphere で Java エージェントを設定する \(75ページ\)](#)に記載されている情報もご確認ください。

## Java エージェントのインストール

Java エージェントのインストール方法はいくつかありますので、ご利用の環境に合わせて選択してください。Contrast を使用する場所(例えば、開発環境で Assess、本番環境では Protect など)、既存のビルドツール、アプリケーションのデプロイ方法などを考慮する必要があります。



## ヒント

エージェントベースのテクノロジーを複数使用していて、Contrast Java エージェントを並行して使用する場合は、起動時にロードされる最初のエージェントとして、Contrast Java エージェントを必ず指定してください。例：

```
java -javaagent:contrast.jar -javaagent:newrelic.jar
```

Contrast Java エージェントを最初にロードすることで、パフォーマンスへの影響を抑えることができます。

## クイックスタート

Java エージェントがどのように動作するか試してみたい場合は、こちらの [Java クイックスタートガイド \(77ページ\)](#) をご覧ください。

## 基本のインストール

Java エージェントのインストールは、ほとんどの場合(Tomcat のなどのアプリケーションサーバ、Docker などのコンテナを使用する場合)、Java エージェントを取得するリポジトリを選択し、各リポジトリの手順に従ってエージェントをダウンロードしてインストールしてください。

- [Maven Central \(60ページ\)](#)
- [Debian \(61ページ\)](#)
- [RPM \(62ページ\)](#)

## ビルドに組み込むインストール

開発環境で Assess を使用しており、脆弱性検出時に既存のソフトウェアプロジェクトでビルド結果を設定したい場合は、以下を参照してエージェントをインストールしてください。

- [Maven プラグイン \(661ページ\)](#)
- [Gradle プラグイン \(645ページ\)](#)
- [Jenkins プラグイン \(647ページ\)](#)

## Maven Central を使用して Java エージェントをインストール

Contrast Java エージェントは、グループ IDcom.contrastsecurity とアーティファクト IDcontrast-agent を使用して、[Maven Central](#) から入手できます。Java エージェントをインストールするには：

1. Maven Central から *contrast-agent.jar* を入手します(Maven リポジトリからダウンロードする方法は [例を参照](#))。
2. [Java エージェントを設定 \(78ページ\)](#) します。 [YAML 設定ファイル \(38ページ\)](#) を作成またはダウンロードします。設定ファイルには、[エージェントキー \(37ページ\)](#) を使用して、Contrast の接続パラメータを指定する必要があります。
3. エージェントがファイルを認識できるように YAML 設定ファイル(contrast.yaml)の場所を指定します。以下の例では、<YourContrastJarPath>を Contrast JAR ファイルのパス(これは内部のファイル構造やダウンロードした方法によって異なります)に、<ApplicationJar>をアプリケーションの JAR ファイル名に置き換えます。

```
java -javaagent:<YourContrastJarPath> -  
Dcontrast.config.path=contrast.yaml -jar <ApplicationJar>.jar
```



### 注記

YAML の代わりにシステムプロパティや環境変数を使って設定する、またはエージェントが自動的に検索できる [標準の場所 \(36ページ\)](#) に YAML 設定ファイルを置いている場合は、Java エージェントを含めるよう JVM パラメータを設定してください。

```
java -javaagent:<YourContrastJarPath> -jar <AppName>.jar
```

4. 通常通りにアプリケーションを使用します(例えば、アプリケーションの Web インターフェイスをクリックして、API コマンドを送信するなど)。Contrast でアプリケーションが認識されていることを確認します(例えば、Contrast の Web インターフェイスでアプリケーションを参照したり、ログを表示するなど)。

Maven Central にデプロイされている Contrast アーティファクトは、<https://keyserver.ubuntu.com> がホストする GPG キーで署名されています。Contrast の公開署名キーの ID は 1AAD9AFB3FC5CCA6940D021534D84B137E8F1053 で、次のコマンドでローカル鍵にインストールできます。

```
gpg --keyserver keyserver.ubuntu.com --recv-keys \  
1AAD9AFB3FC5CCA6940D021534D84B137E8F1053
```

また、以下のようなアプリケーションサーバと一緒に Contrast エージェントをインストールすることで、テスト環境や本番環境で動作するアプリケーションのセキュリティ分析を行うことができます。

- [Jetty \(72ページ\)](#)
- [JBoss/Wildfly \(71ページ\)](#)
- [Tomcat \(73ページ\)](#)
- [WebLogic \(74ページ\)](#)
- [WebSphere \(75ページ\)](#)

Docker などのコンテナを使用してインストール ([64ページ](#))することもできます。



### ヒント

[Pivotal Cloud Foundry\(現 VMware Tanzu\)](#)のようなツールを使用する場合など、エージェントのインストールで互換性があるその他の方法については、[Contrast サポートポータル](#)を参照してください。

## Debian リポジトリを使用して Java エージェントをインストール

Contrast Debian リポジトリから Java エージェントを取得してインストールするようシステムを設定できます。これを行うには、以下の手順を実行します。

1. 以下のコマンドを使用して、リポジトリからパッケージを受け取るようシステムを設定します。

```
curl https://pkg.contrastsecurity.com/api/gpg/key/public | sudo apt-key \  
add -  
echo "deb https://pkg.contrastsecurity.com/debian-public/ all contrast" |  
sudo tee /etc/apt/sources.list.d/contrast-all.list
```

2. Contrast Java エージェントをインストールします。

```
sudo apt-get update && sudo apt-get install contrast-java-agent
```

3. `/opt/contrast/contrast-agent.jar`として、Java 用の Contrast エージェントの JAR ファイルがインストールされます。
4. [Java エージェントを設定 \(78ページ\)](#)します。[YAML 設定ファイル \(38ページ\)](#)を作成またはダウンロードします。[エージェントキー \(37ページ\)](#)を使用して、Contrast の接続パラメータを指定する必要があります。
5. エージェントがファイルを認識できるように YAML 設定ファイル(`contrast.yaml`)の場所を指定します。以下の例では、`<YourContrastJarPath>`を Contrast JAR ファイルのパス(これは内部のファイル構造やダウンロードした方法によって異なります)に、`<ApplicationJar>`をアプリケーションの JAR ファイル名に置き換えます。

```
java -javaagent:<YourContrastJarPath> -  
Dcontrast.config.path=contrast.yaml -jar <ApplicationJar>.jar
```



### 注記

YAML の代わりにシステムプロパティや環境変数を使って設定する、またはエージェントが自動的に検索できる[標準の場所 \(36ページ\)](#)に YAML 設定ファイルを置いている場合は、Java エージェントを含めるよう JVM パラメータを設定してください。

```
java -javaagent:<YourContrastJarPath> -jar <AppName>.jar
```

6. 通常通りにアプリケーションを使用します(例えば、アプリケーションの Web インターフェイスをクリックして、API コマンドを送信するなど)。Contrast でアプリケーションが認識されていることを確認します(例えば、Contrast の Web インターフェイスでアプリケーションを参照したり、ログを表示するなど)。

また、以下のようなアプリケーションサーバと一緒に Contrast エージェントをインストールすることで、テスト環境や本番環境で動作するアプリケーションのセキュリティ分析を行うことができます。

- [Glassfish](#)
- [Jetty \(72ページ\)](#)
- [JBoss/Wildfly \(71ページ\)](#)
- [Tomcat \(73ページ\)](#)
- [WebLogic \(74ページ\)](#)
- [WebSphere \(75ページ\)](#)

[Docker などのコンテナを使用してインストール \(64ページ\)](#)することもできます。



### ヒント

[Pivotal Cloud Foundry\(現 VMware Tanzu\)](#)のようなツールを使用する場合など、エージェントのインストールで互換性があるその他の方法については、[Contrast サポートポータル](#)を参照してください。

## RPM リポジトリを使用して Java エージェントをインストール

RPM リポジトリを使用して Java エージェントをインストールするには：

1. 以下のコマンドを使用して、Contrast RPM リポジトリからパッケージを取得するようシステムを設定します。

```
OSREL=$(rpm -E "%{rhel}")  
sudo -E tee /etc/yum.repos.d/contrast.repo << EOF
```

```
[contrast]
name=contrast repo
baseurl=https://pkg.contrastsecurity.com/rpm-public/centos- $\$$ OSREL/
gpgcheck=0
enabled=1
EOF
```

2. 設定をしたら、Contrast Java エージェントをインストールします。

```
sudo yum install contrast-java-agent
```

3. Contrast Java エージェントの JAR ファイルが、`/opt/contrast/contrast-agent.jar` として、インストールされます。
4. [Java エージェントを設定 \(78ページ\)](#) します。[YAML 設定ファイル \(38ページ\)](#) を作成またはダウンロードします。設定ファイルには、[エージェントキー \(37ページ\)](#) を使用して、Contrast の接続パラメータを指定する必要があります。
5. エージェントがファイルを認識できるように YAML 設定ファイル(`contrast.yaml`)の場所を指定します。以下の例では、`<YourContrastJarPath>` を Contrast JAR ファイルのパス(これは組織内のファイル構造やダウンロードした方法によって異なります)に、`<ApplicationJar>` をアプリケーションの JAR ファイル名に置き換えます。

```
java -javaagent:<YourContrastJarPath> -
Dcontrast.config.path=contrast.yaml -jar <ApplicationJar>.jar
```



### 注記

YAML の代わりにシステムプロパティや環境変数を使って設定する、またはエージェントが自動的に検索できる [標準の場所 \(36ページ\)](#) に YAML 設定ファイルを置いている場合は、Java エージェントを含めるよう JVM パラメータを設定してください。

```
java -javaagent:<YourContrastJarPath> -jar <AppName>.jar
```

6. 通常通りにアプリケーションを使用します(例えば、アプリケーションの Web インターフェイスをクリックして、API コマンドを送信するなど)。Contrast でアプリケーションが認識されていることを確認します(例えば、Contrast の Web インターフェイスでアプリケーションを参照したり、ログを表示するなど)。

また、以下のようなアプリケーションサーバと一緒に Contrast エージェントをインストールすることで、テスト環境や本番環境で動作するアプリケーションのセキュリティ分析を行うことができます。

- [Glassfish](#)
- [Jetty \(72ページ\)](#)
- [JBoss/Wildfly \(71ページ\)](#)
- [Tomcat \(73ページ\)](#)
- [WebLogic \(74ページ\)](#)
- [WebSphere \(75ページ\)](#)

[Docker などのコンテナを使用してインストール \(64ページ\)](#) することもできます。



### ヒント

[Pivotal Cloud Foundry\(現 VMware Tanzu\)](#) のようなツールを使用する場合など、エージェントのインストールで互換性があるその他の方法については、[Contrast サポートポータル](#) を参照してください。

## コンテナを使用して Java エージェントをインストール

### インストールを行う前に

本項では、Docker を例として、コンテナ化されたアプリケーションに Contrast Java エージェントをインストールするための一般的な手順について説明します。

コンテナや関連ソフトウェアの仕組みを基本的に理解している必要があります。実際の手順は、ご利用の環境に合わせて調整してください。

### ECS のサポート

Amazon ECS(Amazon Elastic Container Service)環境で Docker コンテナを使用する場合、この手順を使用して Contrast Java エージェントをインストールすることができます。

### 手順 1 : エージェントをインストール

Contrast エージェントは、アプリケーションをコンテナイメージに追加する前または後のどちらでも追加できます。推奨される方法は、名前を付けた **マルチステージビルド** を使用することです。例 :

```
FROM eclipse-temurin:17

# Hidden for brevity...

# Copy the required agent files from the official Contrast agent image.
COPY --from=contrast/agent-java:latest /contrast/contrast-agent.jar /opt/contrast/contrast.jar
```

この例では、最新の Java エージェントが使用されます。 **使用可能なタグ** は、DockerHub を確認して下さい。

### 手順 2 : エージェントを設定

Java エージェントの設定は、有効になる優先順位があります。コンテナにインストールする場合 :

- 共通の設定には **YAML 設定ファイル** を使用して、ベースイメージで指定できるようにします。例えば、共通の設定には、ログをコンソール出力にリダイレクトすることや、プロキシの設定、パフォーマンスのチューニングなどがあります。以下は、YAML 設定ファイルのサンプルです。

```
agent:
  java:
    scan_all_classes: false
    scan_all_code_sources: false
  logger:
    stdout: true
```

YAML 設定ファイルを作成し、ベースイメージにコピーします。次の行を追加して、この YAML 設定ファイルをベースイメージの Dockerfile にコピーします。

```
COPY WORKSPACE/contrast_security.yaml /opt/contrast/contrast_security.yaml
```

- アプリケーション固有の設定値には、**Java のシステムプロパティ** や **環境変数** を使用して、各アプリケーションのオプションをそれぞれ指定します。

Contrast の設定	機能	Java システムプロパティ	
アプリケーションのメタデータ	アプリケーションに関連付けるメタデータを指定	-Dcontrast.application.metadata	CONTRAST_AF



Contrast の設定	機能	Java システムプロパティ	
アプリケーションのセッションメタデータ	ビルド番号、バージョン、ハッシュなどの情報でセッションの新規作成時に使用されるセッションメタデータ (489ページ)を指定	-Dcontrast.application.session_metadata	CONTRAST__AP
アプリケーショングループ	このアプリケーションを関連付けるアクセスグループをオンボード時に指定(アプリケーションのアクセスグループ (708ページ)は先に Contrast で作成しておく必要あり)	-Dcontrast.application.group	CONTRAST__AP
サーバの環境	アプリケーションを実行する環境を指定、このオプションで有効な値 : Development、QA、Production	-Dcontrast.server.environment	CONTRAST__SE

### 手順 3 : JVM パラメータを更新

Java アプリケーションにプロファイラをアタッチするために、`JAVA_TOOL_OPTIONS` 環境変数を設定して、アプリケーションに `-javaagent` オプションを指定する必要があります。

Contrast 共通の JVM パラメータをベースイメージ内の別の環境変数にあらかじめ設定しておき、アプリケーションチームがそれを `JAVA_TOOL_OPTIONS` で利用できるようにします。例 :

- ベースイメージの Dockerfile :

```
ENV CONTRAST_OPTS "-javaagent:/opt/contrast/contrast.jar \
-Dcontrast.config.path=/opt/contrast/contrast_security.yaml"
```

- アプリケーションイメージの Dockerfile :

```
ENV JAVA_TOOL_OPTIONS $CONTRAST_OPTS \
-Dcontrast.application.metadata=bU=<value>,contactEmail=<value>,contactName=<value> \
-Dcontrast.application.group=APP_GROUP
```

### 手順 4 : アプリケーションイメージを実行

Docker イメージにエージェントを追加 (64ページ)して設定 (64ページ)したら、イメージを実行します。

エージェントが Contrast サーバにデータを送信するには、[エージェントの認証情報 \(37ページ\)](#)が必要です。エージェントの認証情報を保護するために、Docker secret を利用して、デプロイ時に環境変数として渡すことができます。以下は、Docker run コマンドの例です。

```
docker run -e CONTRAST__API__URL=https://app.contrastsecurity.com -e \
CONTRAST__API__API_KEY=<value> -e CONTRAST__API__SERVICE_KEY=<value> -e \
CONTRAST__API__USER_NAME=<value> -e CONTRAST__SERVER__NAME=<value> -e \
CONTRAST__SERVER__ENVIRONMENT=<value> image_with_contrast
```

Contrast が実行されているかを確認するには、コンテナのログをチェックしてください。次のようなメッセージが表示されているはずで

```
2020-05-28 22:36:29,910 [main STDOUT] INFO - Copyright: 2019 Contrast \
Security, Inc
2020-05-28 22:36:29,910 [main STDOUT] INFO - Contact: \
support@contrastsecurity.com
2020-05-28 22:36:29,910 [main STDOUT] INFO - License: Commercial
```

```
2020-05-28 22:36:29,910 [main STDOUT] INFO - NOTICE: This Software and the \
patented inventions embodied within may only be used as part of
2020-05-28 22:36:29,910 [main STDOUT] INFO - Contrast Security's \
commercial offerings. Even though it is made available through public
2020-05-28 22:36:29,910 [main STDOUT] INFO - repositories, use of this \
Software is subject to the applicable End User Licensing Agreement
2020-05-28 22:36:29,910 [main STDOUT] INFO - found at https://
www.contrastsecurity.com/enduser-terms-0317a or as otherwise agreed between
2020-05-28 22:36:29,910 [main STDOUT] INFO - Contrast Security and the End \
User. The Software may not be reverse engineered, modified,
2020-05-28 22:36:29,910 [main STDOUT] INFO - repackaged, sold, \
redistributed or otherwise used in a way not consistent with the End User
2020-05-28 22:36:29,910 [main STDOUT] INFO - License Agreement.
[Contrast] Thu May 28 22:36:30 EDT 2020 Effective instructions: \
Assess=false, Protect=true
[Contrast] Thu May 28 22:36:30 EDT 2020 String Supporter has been disabled
[Contrast] Thu May 28 22:36:30 EDT 2020 Logging security messages to /Users/
usernamehere/.contrast/security.log
[Contrast] Thu May 28 22:36:31 EDT 2020 Starting JVM [1862ms]
```

## 関連項目

[Contrast エージェントオペレータ\(Kubernetes オペレータ\) \(41ページ\)](#)

Contrast サポートポータル : [AWS Fargate と Contrast エージェント](#)、[Docker 環境での Java エージェント](#)

## Docker 利用の Gradle プロジェクトに Java エージェントをインストール

ここでは、[アプリケーションプラグイン](#)と [Docker プラグイン](#)を含む Gradle プロジェクトをサンプルとして使用し、Java の Web アプリケーションを構築します。また、Web アプリケーションの動作を検証する JUnit5 の統合テストも実行します。プロセスの一環として、統合テスト時に Contrast Assess でコードが解析されるよう、テストに使用する Docker イメージに Contrast を組み込む手順を解説します。サンプルについては、GitHub リポジトリの [Gradle プロジェクトの例](#)を参照してください。



### 注記

以下の手順において、パッケージングや配布に関して言及している部分はいかなる形式でも、全て組織内での使用を目的としています。Contrast をアプリケーションや Docker コンテナと一緒に組織外に配布しないでください。詳細については、[Contrast のサービス利用規約](#)を参照してください。

Docker を使用する既存の Gradle プロジェクトに Contrast Java エージェントを追加する手順 :

1. コマンドプロンプトを開き、以下のコマンドを実行して **contrast-java-examples** リポジトリをクローンします。

```
$ git clone https://github.com/Contrast-Security-OSS/contrast-java-examples.git
```

2. gradle-docker ディレクトリに移動します。

```
$ cd contrast-java-examples/gradle-docker
```

3. テストビルドを実行し、正常に機能することを確認します。

```
$ ./gradlew build
```

```
BUILD SUCCESSFUL in 3s
4 actionable tasks: 3 executed, 1 up-to-date
```



### 注記

Windows では、代わりに `gradlew.bat build` を実行してください。

4. テストビルドがうまくいかない場合は、Java 11 が正しくインストールされていることを確認して下さい(サンプルアプリケーションをビルドするには、Java 11 以降が必要です。 [Java エージェントのサポート対象 \(57ページ\)](#) ページで、Contrast の Java エージェントでサポートされる Java のバージョンを参照できます。)

```
$ java -version
openjdk version "11.0.18" 2023-01-17
OpenJDK Runtime Environment Temurin-11.0.18+10 (build 11.0.18+10)
OpenJDK 64-Bit Server VM Temurin-11.0.18+10 (build 11.0.18+10, mixed \
mode)
```

5. 変更を加えたら、再度ビルドを実行します。それでも機能しない場合は、この問題の詳細を記載して問題を報告してください。
6. [エージェントキー \(37ページ\)](#) を使用して、Contrast エージェントが Contrast サーバと通信するための設定をします。以下のキーが必要です。
  - Contrast URL : `https://app.contrastsecurity.com/Contrast` か、オンプレミス版がプライベートクラウドの URL になります。
  - 組織用 API キー
  - エージェントユーザ名
  - エージェントサービスキー
7. [Gradle のユーザホームディレクトリ](#) にある `gradle.properties` ファイルに、Gradle のプロパティとしてキーを追加します。このファイルが存在しない場合は、作成して下さい。

<contrast\_url>、<your\_api\_key>、<agent\_user\_name>、および  
<agent\_user\_service\_key>を Contrast URL、API キー、ユーザ名、およびサービスキーの値に置き換えます。

```
contrastUrl=<contrast_url>
contrastAgentUserName=<agent_user_name>
contrastAgentServiceKey=<agent_user_service_key>
contrastApiKey=<your_api_key>
```

8. `build.gradle` の `createDockerfile` タスクを修正して、Contrast エージェントを追加し、それを使用するようにアプリケーションを設定します。

```
task createDockerfile(type: Dockerfile) {
    // ... rest of block omitted

    copyFile(new Dockerfile.CopyFile("/contrast/contrast-agent.jar", "/contrast.jar").withStage("contrast/agent-java:latest"))
    environmentVariable("JAVA_TOOL_OPTIONS", "-javaagent:/contrast.jar")
}
```

9. `build.gradle` の `createContainer` タスクに以下のコマンドを追加し、Contrast の設定変数をコンテナに渡します。

```
task createContainer(type: DockerCreateContainer) {
    // ... rest of the config omitted

    envVars = [
        CONTRAST__API__URL: project.property("contrastUrl"),
        CONTRAST__API__USER_NAME: \
```

```
project.property("contrastAgentUserName"),
    CONTRAST__API__SERVICE_KEY: \
project.property("contrastAgentServiceKey"),
    CONTRAST__API__API_KEY: project.property("contrastApiKey"),
    CONTRAST__APPLICATION__NAME: "${project.name}-how-to"
    ]
}
```

10. ビルドを再度実行します。

```
./gradlew clean build
```



### 注記

Windows では、代わりに `gradlew.bat clean build` を実行します。

これで、Docker コンテナで Contrast を有効にしてアプリケーションを実行できるようになりました。総合テストを実行すると、脆弱なエンドポイントが検出され、Contrast に報告されます。報告された脆弱性を参照するには、Contrast Web インターフェイスで [脆弱性ページ \(587ページ\)](#) にアクセスし、アプリケーション名の `gradle-application-how-to` でフィルターをかけます。

## Linux で自動更新を使用して Java エージェントをインストール

ユーザによっては、Contrast の Java エージェントを自動的に最新バージョンに更新したい場合があります。Linux ユーザの場合、一般的な Linux ツールである `cron` や `curl` を使用して、Maven Central から Java エージェントの更新をスケジュールできます。

ここでは、Ubuntu 18.04 Linux ホストで Java エージェントの更新ジョブをスケジュールするよう設定する方法について説明します。



### 注記

本項で説明する内容のファイルの作成には、お好きなエディタを使用してください。以下の例では、`tee` コマンドを使用してファイルを作成します。

1. ここでの手順に沿って各ステップを実行したい場合は、[Vagrant](#) や [VirtualBox](#) を使用して、Ubuntu 18.04 の仮想マシンを新規に作成することもできます。

```
vagrant init ubuntu/bionic64
```

```
vagrant up
```

```
vagrant ssh
```

2. Contrast ソフトウェア用の共有ディレクトリを作成します。

```
sudo mkdir -p /opt/contrast
```

3. 最新の Java エージェントをインストールするためのスクリプトを `/etc/cron.daily` ディレクトリに作成します。このディレクトリ内のスクリプトは毎日 1 回実行され、その結果、ホストで毎日 Java エージェントが最新に更新されます。

4. `tee` を使用してこのスクリプトを作成します。全ての行を入力し終わったら、`CTRL+D` を押します。

```
$ sudo tee -a /etc/cron.daily/install-latest-contrast-agent > /dev/null
#!/bin/bash -u
```

```

CONTRAST_DIRECTORY=/opt/contrast
CONTRAST_FILE_NAME=contrast-agent.jar

curl --fail --silent --location "https://repository.sonatype.org/service/
local/artifact/maven/redirect?r=central-
proxy&g=com.contrastsecurity&a=contrast-agent&v=LATEST" -o /tmp/
$CONTRAST_FILE_NAME
if [ $? -ne 0 ]; then
    echo "Failed to download Contrast Java agent" >&2
    exit 1
fi
mv /tmp/$CONTRAST_FILE_NAME $CONTRAST_DIRECTORY/$CONTRAST_FILE_NAME

```

- 新しいスクリプトファイルに実行権限を設定します。

```
sudo chmod +x /etc/cron.daily/install-latest-contrast-agent
```

- スクリプトをテストするために、スクリプトを実行します。stat を使用してファイルが存在することを確認します。

```

$ sudo /etc/cron.daily/install-latest-contrast-agent
$ stat /opt/contrast/contrast-agent.jar
stat /opt/contrast/contrast-agent.jar
  File: /opt/contrast/contrast-agent.jar
  Size: 10568283          Blocks: 20648          IO Block: 4096   regular file
Device: 801h/2049d      Inode: 256034          Links: 1
Access: (0644/-rw-r--r--)  Uid: (   0/   root)   Gid: (   0/   root)
Access: 2019-04-11 02:02:01.265775928 +0000
Modify: 2019-04-11 02:24:47.849796936 +0000
Change: 2019-04-11 02:24:47.849796936 +0000
 Birth: -

```

- Contrast エージェントには、Contrast サーバと通信するための設定が必要です。[エージェントのキー情報はこちら \(37ページ\)](#)を参照してください。
- Contrast エージェントを Linux ホストにインストールしたら、通常は、ホスト上で Contrast が有効な各 Web アプリケーションが、Contrast サーバへの接続に必要なパラメータなどの基本的な設定値を共有できるように構成します。通常、Contrast は Linux ホスト上のパス `/etc/contrast/java/contrast_security.yaml` にある YAML ファイルの設定を探します。
- `/etc/contrast/java` ディレクトリを作成してください。

```
sudo mkdir -p /etc/contrast/java
```

- tee コマンドを使用して、設定ファイルを作成します。<contrast\_url>、<your\_api\_key>、<agent\_user\_name>、<agent\_user\_service\_key>を、前述のステップで Contrast から取得した値に置き換えます。

```

$ sudo tee -a /etc/contrast/java/contrast_security.yaml > /dev/null
api:
  url: <contrast_url>
  api_key: <your_api_key>
  user_name: <agent_user_name>
  service_key: <agent_user_service_key>

```

- 全ての行を入力し終わったら、CTRL+D を押してください。
- Contrast がインストールされ、正しく設定されていることを確認するために、診断テストを実行します。診断テストを実行するには、ホストに Java がインストールされている必要があります。

```
sudo apt install --yes openjdk-11-jre-headless
```

- 最後に、Java エージェントの診断テストを実行します。エージェントが正しくインストールされ、`/etc/contrast/java/contrast_security.yaml` の設定パラメータを使用して、Contrast サーバと通信できることを確認します。

```
$ java -jar /opt/contrast/contrast-agent.jar diagnostic
*** Contrast Agent (version 3.6.3-SNAPSHOT)
[!] Attempting to connect to the Contrast TeamServer at https://
apptwo.contrastsecurity.com/Contrast (No proxy).
[!] Attempting to resolve domain: apptwo.contrastsecurity.com
    Resolved domain apptwo.contrastsecurity.com to IP Address \
52.200.215.12
[+] Client successfully resolved the DNS of the Contrast TeamServer. No \
proxy needed.
[!] Issuing HTTP request to Contrast...
    Executing request...
    Reading response [200]
    Response size = 4209
    Snippet: <!doctype html> <!--[if gt IE 8]><!--> <html class="no-
js" i
[+] Client can connect directly to the Contrast TeamServer. No proxy \
needed.
```

## Scala

Contrast Java エージェントを使用して、Contrast Assess や Contrast SCA で、Scala ベースのアプリケーションを解析することができます。

Java エージェントは、従来のアプリケーションサーバで構築される Scala Web アプリケーションや、Play フレームワークなどで構築されるような新しい Scala Web アプリケーションを解析できます。JVM があれば、Scala に組み込んだ Java エージェントがセキュリティ情報を提供します。

アプリケーションが実行されると、Java エージェントのセンサーがアプリケーションのセキュリティ、アーキテクチャ、ライブラリに関する情報を収集します。エージェントによる解析の結果は、Contrast Web インタフェースで確認できます。

Scala のエージェントは次の機能を提供します。

- ルートカバレッジ
- フローマップ
- SCA ライブラリの検出

## Kotlin

Contrast Java エージェントを使用して、Contrast Assess や Contrast SCA で、Kotlin のアプリケーションを解析することができます。

Java エージェントは、従来のアプリケーションサーバで構築された Kotlin の Web アプリケーションや、SpringBoot などの新しい Kotlin のサーバサイドアプリケーションを解析できます。

JVM があれば、Kotlin に組み込む Java エージェントがセキュリティ情報を提供します。アプリケーションが実行されると、Java エージェントのセンサーがアプリケーションのセキュリティ、アーキテクチャ、ライブラリに関する情報を収集します。エージェントによる解析の結果は、Contrast Web インタフェースで確認できます。

Contrast Java エージェントを使用する場合と同様に、アプリケーションを実行します。自動的に Kotlin がサポートされます。

## Java アプリケーションサーバ



### 注記

本ドキュメントでは、サポート対象の内容について説明します。🔗アイコンが付いたリンクは、参考として、他のドキュメントを参照するリンクとなっています。

次のアプリケーションサーバを使用できます。

- 🔗 [Axis2](#)
- 🔗 [Glassfish](#)
- [JBoss / Wildfly \(71ページ\)](#)
- [Jetty \(72ページ\)](#)
- [Tomcat \(73ページ\)](#)
- [Weblogic \(74ページ\)](#)
- [WebSphere \(75ページ\)](#)

### 関連項目

- [Java エージェントのインストール \(59ページ\)](#)
- [Java エージェントのサポート対象テクノロジー \(57ページ\)](#)
- [Java エージェントの設定 \(78ページ\)](#)

### JBoss EAP、JBoss AS、WildFly で Java エージェントを設定する



### 注意

バージョン番号を混同しないように注意してください。バージョン 7 より前の JBoss EAP は、JBoss AS をベースにしています。JBoss EAP 7.x は、WildFly をベースにしています。

### Java エージェントを使用して JBoss を実行

1. 次のいずれかのリポジトリから、Contrast Java エージェント(JAR ファイル)をダウンロードします。
  - [Maven Central \(60ページ\)](#)
  - [Debian \(61ページ\)](#)
  - [RPM \(62ページ\)](#)
2. JBoss は、BAT ファイルから実行するか、ドメインモードで実行できます。
  - **BAT ファイル** : `.conf` ファイルを使用して `bat` ファイル(`domain.bat`、`standalone.bat`、または `run.bat`)から JBoss を実行する場合は、設定ファイル(`.conf` ファイル)を変更します。Contrast JVM パラメータを有効にして、起動スクリプトに返す必要があります。  
この変更を行うには、`<YourContrastJarPath>`を [Contrast JAR \(57ページ\)](#)ファイルへのパスに置き換え、ご利用の環境の JBoss サーバディレクトリを指定します。そして、`.conf` ファイルの最後の行にその行を追加します。
  - **Windows** :

```
set JAVA_OPTS=-javaagent:<YourContrastJarPath> %JAVA_OPTS%
```

- **UNIX :**

```
JAVA_OPTS=-javaagent:<YourContrastJarPath> $JAVA_OPTS
```

- **ドメインモード :** *domain.bat* または *domain.sh* を使用して、JBoss 6 EAP または JBoss AS 7.x をドメインモードで実行する場合は、*\$JBASS\_HOME/domain/configuration/domain.xml* の JVM オプションに `-javaagent` スイッチを追加する必要があります。

この例では、*<YourContrastJarPath>* を [Contrast JAR \(57ページ\)](#) ファイルへのパスに置き換えてください。

```
<server-group ...>
  <jvm name="default">
    <jvm-options>
      <option value="-javaagent:<YourContrastJarPath>" />
    </jvm-options>
  </jvm>
  ...
</server-group>
```

## Java 2 セキュリティマネージャでの WildFly の使用

[Java 2 セキュリティ \(135ページ\)](#) で WildFly を使用する場合、Java エージェントを設定できます。WildFly のバージョン 9 から 20 まで対応しています。WildFly 8 はサポートされていません。

Wildfly で Java 2 セキュリティマネージャを有効にするには :

1. コマンドライン引数 `-secmgr` を渡すか、環境変数 `SECMGR` を `true` に設定します。

```
SECMGR="true"
```

2. Java エージェントの権限を有効にするには、以下の Contrast ポリシーを *\$JAVA\_HOME/jre/lib/security/java.policy* (JDK 6-8 の場合)、または *\$JAVA\_HOME/lib/security/default.policy* (JDK 9 以降の場合) に追加します。*<YourContrastJarPath>* は [Contrast JAR \(57ページ\)](#) ファイルへのパスに置き換えて、以下のコマンドを使用します。

```
grant codeBase "file:<YourContrastJarPath>" {
  permission java.security.AllPermission;
};
```

3. エージェントが Wildfly のクラスローダーシステムで機能するようにするには、環境変数 `JBASS_MODULES_SYSTEM_PKGS` (本来は `org.jboss.byteman`) の値を変更して、Java エージェントのベースパッケージ `com.contrastsecurity.agent,org.jboss.byteman` も含めるようにします。



### ヒント

詳細については、[Java EE 7 セキュリティマネージャを WildFly で使用する方法](#)についてや、[デフォルトのポリシー実装やポリシーファイルの構文](#)を参照して下さい。

## Jetty で Java エージェントを設定する

Jetty で Java エージェントを設定するには :

1. 次のいずれかのリポジトリから、Contrast Java エージェント (JAR ファイル) をダウンロードします。
  - [Maven Central \(60ページ\)](#)
  - [Debian \(61ページ\)](#)



- [RPM \(62ページ\)](#)

2. お使いの Jetty の環境に合わせて、<YourContrastJarPath>を [Contrast JAR \(57ページ\)](#)ファイルのパスに置き換えます。次に、以下の行を<JettyDirectory>/start.ini ファイルに追加します。

```
-javaagent:<YourContrastJarPath>
```

3. Java 2 セキュリティマネージャを使用する場合は、以下のコードを含む `contrast.policy` ファイルを作成します(<YourContrastJarPath>は [Contrast JAR \(57ページ\)](#)ファイルへのパスに置き換えます)。

```
grant codeBase "file:<YourContrastJarPath>" {  
    permission java.security.AllPermission;  
};
```

次に、以下を設定します。

- **Jetty 7-8** : そのファイルを `JETTY_HOME/lib/policy` フォルダにコピーします。環境変数 `JETTY_ARGS --secure` を追加します。
- **Jetty 9** : 作成したポリシーを、自分で設定したポリシーに追加します。<YourPolicy>の箇所を自分のポリシー名に置き換えると、一般的な環境変数の設定でセキュリティマネージャが有効になります。

```
-Djava.security.manager -Djava.security.policy=<YourPolicy>
```



### 重要

Jetty 9 以降では、セキュリティ管理ポリシーは正式にサポートされていません。



### ヒント

Java2 セキュリティマネージャで Jetty を使用方法についての詳細は、[Jetty Policy](#)(Jetty ポリシー)を参照してください。

## Tomcat で Java エージェントを設定する

最初に、次のいずれかのリポジトリから、Contrast Java エージェント(JAR ファイル)をダウンロードします。

- [Maven Central \(60ページ\)](#)
- [Debian \(61ページ\)](#)
- [RPM \(62ページ\)](#)

Tomcat で Contrast を実行する方法に応じて、以下を参考にして Java エージェントを設定してください。

## Windows または Unix で実行

`CATALINA_OPTS` 環境変数を使用して、Tomcat サーバを実行する JVM に設定フラグやシステムプロパティを渡します。

Tomcat では、`setenv` スクリプトを使用して環境変数を指定することを推奨しています。スクリプトの作成や検索など `setenv` スクリプトの詳細については、Tomcat のディストリビューションに同梱されている `RUNNING.txt` を参照してください。

Contrast を有効にするには、Unix 系 OS であれば `setenv.sh` に、Windows であれば `setenv.bat` のいずれかで、`-javaagent` フラグを `CATALINA_OPTS` に追加します。例えば、以下のようになります。

- **Windows :**

```
set "CATALINA_OPTS=%CATALINA_OPTS% -javaagent:<YourContrastJarPath>"
```

- **Unix :**

```
export CATALINA_OPTS="$CATALINA_OPTS -javaagent:<YourContrastJarPath>"
```

## Windows の Tomcat サービスで実行

1. Tomcat をサービスとして実行する場合は、Tomcat サービスマネージャを開き、JVM オプションを変更してエージェントを追加します。
2. システムトレイの Tomcat アイコンをダブルクリックします(または、右クリックして **Configure** を選択します)。(アイコンがない場合は、Tomcat の bin ディレクトリにある *tomcat9w.exe* を実行して手動で起動する必要があります。)
3. **Java** タブに切り替えて、`-javaagent` フラグを追加する箇所を確認します。

## Java2 セキュリティを使用して Tomcat を実行

1. 以下のコードを含む *contrast.policy* ファイルを作成します(もしくは、*catalina.policy* ファイルにコードを追加します)。`<YourContrastJarPath>`は、[Contrast JAR \(57ページ\)](#)ファイルのパスに置き換えてください。例：

```
grant codeBase "file:<YourContrastJarPath>" {  
    permission java.security.AllPermission;  
};
```

2. *contrast.policy* ファイルを `$CATALINA_HOME/conf/catalina.policy` ファイルに追加(append)します。追加の設定は必要ありません。コマンドラインで、`-security` オプションを付けて Tomcat を起動します。

## WebLogic で Java エージェントを設定する

最初に、次のいずれかのリポジトリから、Contrast Java エージェント(JAR ファイル)をダウンロードします。

- [Maven Central \(60ページ\)](#)
- [Debian \(61ページ\)](#)
- [RPM \(62ページ\)](#)

WebLogic で Contrast を実行する方法に応じて、以下を参考にして Java エージェントを設定してください。

### Unix

1. WebLogic を自分で起動する場合は、インストール先の *bin* ディレクトリにある *startWebLogic* ファイルに Contrast の JVM パラメータを追加してください。UNIX ベースのオペレーティングシステムの場合、このファイルのパスは以下のようになります。

```
/path/to/appserver/userprojects/domains/base_domain/bin/startWebLogic.sh
```

2. このファイルで、Java 実行ステップの前に、Contrast エンジン `-javaagent` として `JAVA_OPTIONS` 環境変数に追加します。`<YourContrastJarPath>`は [Contrast JAR \(57ページ\)](#) ファイルへのパスに置き換えてください。例：

```
export JAVA_OPTIONS="$JAVA_OPTIONS -javaagent:<YourContrastJarPath>"
```

### Windows

1. Windows システムの場合、パスは以下のようになります。

```
C:\Oracle\Middleware\userprojects\domains\base_domain\bin\startWebLogic.bat
```

- このファイルの先頭で、Contrast エンジンを `-javaagent` として `JAVA_OPTIONS` 環境変数に追加します。<YourContrastJarPath>は [Contrast JAR \(57ページ\)](#) ファイルへのパスに置き換えます。お使いの環境に合わせた WebLogic サーバの情報に置き換えてください。例：

```
set "JAVA_OPTIONS=%JAVA_OPTIONS% -javaagent:<YourContrastJarPath>"
```

## WebLogic で Java2 を使用する

- 以下のコードを含む `contrast.policy` ファイルを作成します(もしくは、`catalina.policy` ファイルにコードを追加します)。<YourContrastJarPath>は [Contrast JAR \(57ページ\)](#) ファイルのパスに置き換えてください。例：

```
grant codeBase "file:<YourContrastJarPath>" {  
    permission java.security.AllPermission;  
};
```

- WebLogic には、`@WL_HOME/server/lib/weblogic.policy` というテンプレートファイルがあります。このファイルには、Java セキュリティマネージャを有効にして WebLogic サーバを起動するためのサンプル定義があります。旧バージョン(10 以前)の WebLogic の場合は、テンプレートファイルの `@WL_HOME` を WebLogic をインストールしたルートディレクトリへの実際のパスに置き換える必要があります。
- セキュリティマネージャを有効にすると、ポリシーファイルである `@WL_HOME/server/lib/weblogic.policy` がデフォルトとして機能します。もしくは、`-Djava.security.policy==<YourPath>` でカスタムのポリシーファイルを指定することもできます。その場合、<YourPath>はカスタムファイルへのパスになります。==は、WebLogic が起動する際のデフォルトのパス設定を上書きするため、重要です。



### ヒント

詳細は、[Java セキュリティを使用して WebLogic のリソースを保護する](#) を参照してください。

## WebSphere で Java エージェントを設定する

最初に、次のいずれかのリポジトリから、Contrast Java エージェント(JAR ファイル)をダウンロードします。

- [Maven Central \(60ページ\)](#)
- [Debian \(61ページ\)](#)
- [RPM \(62ページ\)](#)

WebSphere で Contrast を実行する方法に応じて、以下を参考にして Java エージェントを設定してください。



### 注記

IBM J9 では、[共有クラス\(Shared Classes\)](#)機能を使用する場合、Java の計測 API(Instrumentation API)でコアの Java クラスを変更することができません。JVM パラメータに `-Xshareclasses:none` を指定して、この機能を無効にする必要があります。

同様に、`-Dcom.ibm.oti.shared.enabled=true` が設定されている場合、旧 J9 の JRE でも問題が発生する可能性があります。

## WebSphere のトラストストアとキーストア

WebSphere は、Java JRE の一部として組み込まれるトラストストアとは別に、独自のトラストストアとキーストアを保持します。エージェントは、WebSphere が初期化される前に起動するため、WebSphere 独自のトラストストアは設定されません。そのため、エージェントは、JVM に特別な設定がされていない限り、Java の JRE/lib/security/cacerts ファイルにあるデフォルトのトラストストアを使用します。

ただし、内部専用や自己署名証明書を使用するプロキシサーバが必要な場合などには、特定の追加手順が必要になります。選択できる方法は、次のとおりです。

1. JRE cacerts のトラストストアと WebSphere のトラストストアの両方に必要な証明書をインストールします。これにより、証明書チェーンがエージェントと Web アプリケーションの両方で検証されます。
2. 標準のトラストストアのシステムプロパティを Java に指定し、トラストストアを WebSphere のトラストストアと同じものに変更します。その例を以下に記載します。この方法では、証明書を 1 つの場所(WebSphere のトラストストア)にインストールするだけでよいという利点があります。  
例：

```
-Djavax.net.ssl.trustStore=opt/IBM/WebSphere/AppServer/profiles/AppSrv01/  
config/cells/DefaultCell01/nodes/DefaultNode01/trust.p12  
-Djavax.net.ssl.trustStoreType=PKCS12  
-Djavax.net.ssl.trustStorePassword=secret
```

WebSphere 自体は、パスワードをエンコードする方法をサポートしていますが、WebSphere が起動する前に実行されるため、エージェントのトラストストアのパスワードを設定するときには使用できません。

## WebSphere で Contrast を追加する

WebSphere を自分で起動する場合は、セルのディレクトリにある `server.xml` ファイルに Contrast の JVM パラメータを追加します。<CellName>と<NodeName>の箇所を、セルとノードの名前に置き換えます。<YourContrastJarPath>は [Contrast JAR \(57ページ\)](#) ファイルへのパスに置き換えてください。例：

```
<WebsphereDirectory>\AppServer\profiles\AppSrv01\config\cells\<CellName>\nodes\<NodeName>\servers\server1\server.xml  
  
<jvmEntries genericJvmArguments="-javaagent:<YourContrastJarPath> -  
Xshareclasses:none">  
  ...  
</jvmEntries>
```

## WebSphere 管理コンソールで Contrast を追加する

[WebSphere サポートサイト](#)の手順に従って、WebSphere の管理コンソールから Contrast を追加することもできます。

## WebSphere で Java2 を使用する

1. 以下のコードを含む `contrast.policy` ファイルを作成します(もしくは、`server.policy` ファイルにコードを追加します)。<YourContrastJarPath>は [Contrast JAR \(57ページ\)](#) ファイルへのパスに置き換えてください。例：

```
grant codeBase "file:<YourContrastJarPath>" {  
  permission java.security.AllPermission;  
};
```

2. `$WEBSHERE_HOME/AppServer/profiles/AppSrv01/properties/server.policy` に `contrast.policy` ファイルを追加(append)します。

- wsadmin ツールでセキュリティマネージャを有効にします。
  - Jacl** : `$AdminTask setAdminActiveSecuritySettings {-enforceJava2Security true}`
  - Jython** : `AdminTask.setAdminActiveSecuritySettings('-enforceJava2Security true')`



### ヒント

詳細については、[Java セキュリティマネージャやスクリプトを使用した Java 2 セキュリティマネージャの有効/無効化についてのドキュメント](#)を参照してください。

## Java クイックスタートガイド

Contrast では、コードの脆弱性を監視するためのセンサーを配置するために、エージェントをインストールする必要があります。エージェントは、開発環境では脆弱性を解析し、実行時の本番環境では攻撃を検知します。

アプリケーションが実行されると、エージェントは情報(HTTP リクエスト、データフロー、バックエンド接続、ライブラリの依存関係など)を解析し、脆弱性や攻撃を Contrast サーバに送信します。Contrast でそれらの情報を参照でき、優先順位を付け、直ちに対策を講じることができます。

このガイドで、Contrast がわずか数分でアプリケーションで動作するようになり、Contrast の機能を確認することができます。



### ヒント

将来的なインストールに関しては、必要に応じて、組織のビルドツールやデプロイメントパイプライン、セキュリティ目標、Contrast を使用する環境なども考慮してください。ご利用状況に合わせて、[Contrast をインストールする他の方法 \(618ページ\)](#)を参照ください。

## 前提条件

このガイドで使用する Web アプリケーションは、以下の前提条件を満たすものをお選びください。

- Web アプリケーションがプロキシを経由せずにインターネットにアクセスできること。
- Web アプリケーションが JAR ファイルとしてパッケージ化されていること。
- Contrast でサポートされている[バージョン、フレームワーク、ツール \(57ページ\)](#)を使用していること。

また、コマンドラインインターフェース(エージェントをダウンロードするためのディレクトリを選択するため)と、ご利用になる組織の Contrast サーバのアクセスも必要です。まだ Contrast をお持ちでない方は、[Community Edition \(29ページ\)](#)を無料にご利用いただけます。

## インストール

- 次のコマンドを使用して、Maven Central からエージェントの JAR ファイルをダウンロードします。コマンドラインインターフェースから、以下の curl リクエストを入力して、最新バージョンのエージェントを現在のディレクトリに配置します。

**Linux :**

```
curl -L 'https://repository.sonatype.org/service/local/artifact/maven/redirect?r=central-proxy&g=com.contrastsecurity&a=contrast-agent&v=LATEST' -o contrast.jar
```

#### Windows :

```
curl -L "https://repository.sonatype.org/service/local/artifact/maven/redirect?r=central-proxy&g=com.contrastsecurity&a=contrast-agent&v=LATEST" -o contrast.jar
```

完了したら、現在のディレクトリに `contrast.jar` というファイルがあることを確認します (例: `./contrast.jar`)。

2. エージェントを追加するための画面から YAML 設定ファイルをダウンロードします(まだダウンロードしていない場合)。これを行うには、Contrast Web インターフェイスで、**新規登録**を選択します。



言語に **Java** を選択したら、**Java エージェントの YAML 設定ファイルをダウンロード**を選択します。ファイルはローカルにダウンロードされ、アプリケーションを Contrast に接続するための組織固有のエージェントキーが含まれます。

3. YAML 設定ファイルをエディタで開き、エージェントの設定を指定します。

```
api:
  url: https://xxx.contrastsecurity.com/Contrast
  api_key: A2xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxG9N
  service_key: 88xxxxxxxxxxxxxxxx5Z
  user_name: agent_xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxxxxx@OrgName
```

4. コマンドラインインターフェイスで以下のコマンドを入力して、YAML 設定ファイルがどこにあるかをエージェントに伝えます。

```
java -javaagent:./contrast.jar -
Dcontrast.config.path=contrast_security.yaml -jar <ApplicationJarPath>
```

<ApplicationJarPath>は必ずお使いのアプリケーションへのパスに置き換えてください。

例: `./MyApplication.jar`

5. Contrast が機能しているかを確認するために、通常通りにアプリケーションを使用します。例えば、アプリケーションの Web インターフェイスをクリックしたり、API コマンドを送信してみてください。

そして、Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択します。アプリケーションの名前が表示されているはずですが、

また、Contrast Web インターフェイスのナビゲーションバーで**サーバ**を選択すると、一覧にサーバ(ローカル)のホスト名が表示されているはずですが、

## Java エージェントの設定

すべての Contrast エージェントには**基本の設定 (35ページ)**があり、設定値には**優先順位 (36ページ)**があります。

Java エージェントは、以下を使用して設定できます。

- Java システムプロパティ
- [環境変数 \(56ページ\)](#)
- Java YAML テンプレート



## ヒント

[Contrast エージェント設定エディタ \(39ページ\)](#)を使用すると、YAML 設定ファイルの作成やアップロード、YAML の検証、推奨される設定値の表示などができます。

システムで以下のような構成を使用している場合は、Contrast エージェントと効率的に連携させるために、アプリケーションの Java 環境に設定が必要な場合もあります。

- **マルチテナントアプリケーション構成** : デプロイ中に JVM アプリケーションサーバが複数のアプリケーションをホストしている場合は、アプリケーションをそれぞれ区別して、個々の設定オプションを適用することができます。  
**マルチテナントアプリケーション構成** : デプロイ中に JVM アプリケーションサーバが複数のアプリケーションをホストしている場合は、アプリケーションをそれぞれ区別して、個々の設定オプションを適用することができます。
- [TLS 証明書 \(134ページ\)](#)
- [Java 9 モジュール \(135ページ\)](#)
- [Java 2 セキュリティ \(135ページ\)](#)
- [インテグレーション \(618ページ\)](#) : Contrast Java エージェントは、プラグインやサードパーティ製ツールを使用したり、外部のシステムと連携することができます。他の製品の動作については、その製品のマニュアルを参照してください。

## Java システムプロパティ

<YourContrastJarPath>を [Contrast JAR ファイル \(57ページ\)](#)へのパスに置き換えて以下のコマンドを実行すると、システムプロパティの詳細情報を確認できます。

- 以下のコマンドにより、Contrast エージェントの JAR ファイルを使用して、一般的なプロパティの一覧を表示することができます。

```
java -jar <YourContrastJarPath> properties
```

- コマンドを検索するには、ツール名を指定してコマンドラインを使用します。例えば、以下のコマンドでプロキシ関連のプロパティの一覧が表示されます。

**filter オプションを使用する場合 :**

```
java -jar <YourContrastJarPath> properties --filter=proxy
```

## Java の YAML 設定ファイルのテンプレート

YAML 設定ファイルを使用して Java エージェントを設定する場合には、以下のテンプレートをご利用ください(YAML 設定については、[こちらの説明 \(38ページ\)](#)を参照してください)。

YAML 設定ファイルは、デフォルトの場所に配置します。

- **Unix** : /etc/contrast/java/contrast\_security.yaml
- **Windows** : C:/ProgramData/contrast/java/contrast\_security.yaml

```
# \  
=====  
==  
# Use the properties in this YAML file to configure a Contrast agent.  
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html  
# to determine the order of precedence for configuration values.  
# \  
=====  
==
```

```

# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# Set the timeout for communicating with TeamServer. This property will be
# respected over the deprecated legacy configuration *contrast.timeout*.
# timeout_ms: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid **contrast.proxy.host**
# and **contrast.proxy.port** will enable the proxy.
# enable: NEEDS_TO_BE_SET

# Set the proxy host. It must be set with port and scheme.

```



```
# host: localhost

# Set the proxy port. It must be set with host and scheme.
# port: 1234

# Set the proxy scheme (e.g., `http` or
# `https`). It must be set with host and port.
# scheme: http

# Set this property as an alternate for `scheme://host:port`. It takes
# precedence over the other settings, if specified; however, an error
# will be thrown if both the URL and individual properties are set.
# url: NEEDS_TO_BE_SET

# Set the proxy user.
# user: NEEDS_TO_BE_SET

# Set the proxy password.
# pass: NEEDS_TO_BE_SET

# Set the proxy authentication type. Value
# options are `NTLM`, `Digest`, and `Basic`.
# auth_type: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.reporting
# Use the following settings to configure reporting to the Contrast UI.
# \
=====
# reporting:

# Set the grace period (in milliseconds) after
# agent shutdown to allow draining pending reports.
# shutdown_grace_period_ms: 120000

# \
=====
# agent.effective_config
# None
# \
=====
# effective_config:
```

```
# \  
=====
```

```
# agent.effective_config.reporting  
# None  
# \  
=====
```

```
# reporting:  
  
# Defaults to `true`. Controls whether configuration  
# setting reports are sent to the Contrast web interface.  
# enable: true  
  
# \  
=====
```

```
# agent.logger  
# Define the following properties to set logging values.  
# If the following properties are not defined, the  
# agent uses the logging values from the Contrast UI.  
# \  
=====
```

```
# logger:  
  
# Enable diagnostic logging by setting a path to a log file.  
# While diagnostic logging hurts performance, it generates  
# useful information for debugging Contrast. The value set here  
# is the location to which the agent saves log output. If no  
# log file exists at this location, the agent creates a file.  
#  
# Example - `/opt/Contrast/contrast.log` creates a log in the  
# `/opt/Contrast` directory, and rotates it automatically as needed.  
#  
# path: ./contrast_agent.log  
  
# Set the the log output level. Valid options are  
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.  
# level: INFO  
  
# Set to `true` to redirect all logs to  
# `stdout` instead of the file system.  
# stdout: false  
  
# Set to `true` to redirect all logs to `stderr` instead of  
# the file system. May be combined with the corresponding  
# `stdout` configuration to write to both streams.  
# stderr: false  
  
# Change the Contrast logger from a file-sized based rolling scheme  
# to a date-based rolling scheme. At midnight server time, the  
# previous day log is renamed to *file_name.yyyy-MM-dd*. Note -  
# this scheme does not have a size limit; manual log pruning is  
# required. You must set this flag to use the backups and size flags.  
# roll_daily: false  
  
# Set the roll size for log files in megabytes. The agent will  
# attempt to prevent the log file from being larger than this size.
```

```

# roll_size: 100

# Set the number of backup files to keep. Set to `0` to disable.
# backups: 10

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# Change the Contrast security logger from a file-sized based rolling
# scheme to a date-based rolling scheme. At midnight server time,
# the log from the previous day is renamed to *file_name.yyyy-MM-dd*.
# Note - this scheme does not have a size limit; manual log
# pruning will be required. This flag must be set to use the
# backups and size flags. Value options are `true` or `false`.
# roll_daily: NEEDS_TO_BE_SET

# Specify the file size cap (in MB) of each log file.
# roll_size: NEEDS_TO_BE_SET

# Specify the number of backup logs that the agent will create before
# Contrast cleans up the oldest file. A value of `0` means that no \
backups
# are created, and the log is truncated when it reaches its size cap.
#
# Note - this property must be used with
# `agent.security_logger.roll_daily=false`; otherwise,
# Contrast continues to log daily and disregard this limit.
#
# backups: NEEDS_TO_BE_SET

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

```

```

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.security_logger.syslog.heartbeat
# Define the following properties to
# set the Syslog heartbeat properties.
# \
=====
# heartbeat:

# Set to `true` to enable the Syslog heartbeat.
# The heartbeat will issue a Syslog message at
# the INFO level after every interval passes.
# enable: false

# Set the interval at which to send heartbeat
# messages to the Syslog server (in milliseconds).
# interval_ms: 60000

# \
=====

```

```
# agent.java
# The following properties apply to any Java agent-wide configurations.
# \
=====
# java:

# Configure the Java agent to skip its application discovery
# algorithm, and instead associate all libraries, vulnerabilities,
# and web traffic to a single application with the name specified
# by this property. This configuration is preferred when deploying
# Java SE applications with embedded web servers (e.g., applications
# built with Spring Boot, Dropwizard, and embedded Jetty). When used
# with an application server, this configuration associates all
# web traffic with the single, standalone application, including
# web traffic handled by application server-hosted endpoints that
# would not be associated with a discovered application otherwise.
#
# Note - This settings takes preferences
# over the `application.name` setting.
#
# standalone_app_name: NEEDS_TO_BE_SET

# By default, the Java agent visits all classes at startup to look
# for vulnerabilities, which the agent may detect by scanning a
# class (e.g., hardcoded passwords). Set this property to `false`
# to disable the default behavior. If disabled, the agent will
# only visit classes which are likely to require sensors; this
# can improve application startup time, but may produce fewer
# findings (most likely findings that require static analysis).
#
# scan_all_classes: true

# By default, the Java agent deeply inspects all JAR and WAR files \
loaded
# by the JVM to build a comprehensive understanding of the type \
hierarchy.
# This understanding allows Contrast to instrument sensors into types
# that it might have overlooked. In most cases, this produces a slight
# increase in accuracy at the cost of increased application startup
# time. Set this property to `false` to disable this level of \
inspection.
#
# scan_all_code_sources: true

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
```

```
# enable: true

# Define a list of directories where libraries are stored.
# Directories must be formatted as a semicolon-delimited list.
# Example - `path1;path2;path3`
#
# library_dirs: NEEDS_TO_BE_SET

# Set the maximum archive unpacking depth when analyzing libraries.
# library_depth: 10

# Set the boolean to more aggressively limit the
# manifest information reported for libraries. If true,
# the limit is 1,000 characters, otherwise it's 3,000.
# prune_package_details: true

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
```

```
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# profile
# Set configuration values under a profile name to enable
# multi-tenant application configuration on web servers. See
# https://support.contrastsecurity.com/hc/en-us/articles/360052187171-Multi-Application-configuration-with-Contrast-Profiles
# for more details.
# \
=====
==
# profile: {}

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false
```

```
# \  
=====\  
# protect.rules  
# Use the following properties to set simple rule configurations.  
# \  
=====\  
# rules:  
  
# Define a list of Protect rules to disable in the agent.  
# The rules must be formatted as a comma-delimited list.  
# disabled_rules: NEEDS_TO_BE_SET  
  
# \  
=====\  
# protect.rules.bot-blocker  
# Use the following selection to configure if the  
# agent blocks bots. Set to `true` to enable blocking.  
# \  
=====\  
# bot-blocker:  
  
# Set to `true` for the agent to block known bots.  
# enable: false  
  
# \  
=====\  
# protect.rules.sql-injection  
# Use the following settings to configure the sql-injection rule.  
# \  
=====\  
# sql-injection:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or off.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# Tell the agent to detect when semantic analysis of the query  
# reveals tautologies used in exfiltration attacks (e.g., "or  
# 1=1" or "or 2<>3"). The agent blocks if blocking is enabled.  
# detect_tautologies: true  
  
# Tell the agent to detect when semantic analysis of the query  
# reveals the invocation of dangerous functions typically used in  
# weaponized exploits. The agent blocks if blocking is enabled.  
# detect_dangerous_functions: true  
  
# Tell the agent to detect when semantic analysis of the query  
# reveals chained queries, which is uncommon in normal usage but  
# common in exploit. The agent blocks if blocking is enabled.  
# detect_chained_queries: true
```



```

# Tell the agent to detect when semantic analysis of the query
# reveals database queries are being made for system tables and
# sensitive information. The agent blocks if blocking is enabled.
# detect_suspicious_unions: true

# Tell the agent to be more aggressive in detecting user
# inputs as SQL comments. This enables the agent to better
# detect SQL Injection input vectors that use comments to
# terminate queries. The agent blocks if blocking is enabled.
# aggressive_comment: false

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Detect when the agent sees user parameters being executed as
# system commands. The agent blocks if blocking is enabled.
# detect_parameter_command_backdoors: true

# Detect when a system command is issued which contains
# chained commands. The agent blocks if blocking is enabled.
# detect_chained_commands: true

# Detect when a system command is issued with an argument matching a
# known dangerous file path. The agent blocks if blocking is enabled.
# detect_dangerous_path_args: true

# Tell the agent to detect when commands come directly
# from input. The agent blocks if blocking is enabled.
# detect_phased_commands: true

# \
=====
# protect.rules.cmd-injection-process-hardening
# Use the following settings to configure whether
# the agent blocks all attempts to start an external
# process. To enable blocking, set to 'true'.
# \
=====
# cmd-injection-process-hardening:

# Set to `true` to enable the agent to block

```

```

# all attempts to start external processes.
# enable: false

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Detect when custom code attempts to access sensitive
# system files. The agent blocks if blocking is enabled.
# detect_custom_code_accessing_system_files: true

# Detect when users attempt to bypass filters by
# using ":::$DATA" channels or null bytes in file
# names. The agent blocks if blocking is enabled.
# detect_common_file_exploits: true

# \
=====
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

```

```

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.padding-oracle
# Use the following properties to configure
# how the padding-oracle rule works.
# \
=====
# padding-oracle: {}

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.

```

```
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
```

```
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET
```

```
# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==

# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
```

```

service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# Set the timeout for communicating with TeamServer. This property will be
# respected over the deprecated legacy configuration *contrast.timeout*.
# timeout_ms: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid **contrast.proxy.host**
# and **contrast.proxy.port** will enable the proxy.
# enable: NEEDS_TO_BE_SET

# Set the proxy host. It must be set with port and scheme.
# host: localhost

# Set the proxy port. It must be set with host and scheme.
# port: 1234

# Set the proxy scheme (e.g., `http` or
# `https`). It must be set with host and port.
# scheme: http

# Set this property as an alternate for `scheme://host:port`. It takes
# precedence over the other settings, if specified; however, an error
# will be thrown if both the URL and individual properties are set.
# url: NEEDS_TO_BE_SET

# Set the proxy user.
# user: NEEDS_TO_BE_SET

# Set the proxy password.
# pass: NEEDS_TO_BE_SET

# Set the proxy authentication type. Value
# options are `NTLM`, `Digest`, and `Basic`.
# auth_type: NEEDS_TO_BE_SET

# \
=====
==

```

```
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.reporting
# Use the following settings to configure reporting to the Contrast UI.
# \
=====
# reporting:

# Set the grace period (in milliseconds) after
# agent shutdown to allow draining pending reports.
# shutdown_grace_period_ms: 120000

# \
=====
# agent.effective_config
# None
# \
=====
# effective_config:

# \
=====
# agent.effective_config.reporting
# None
# \
=====
# reporting:

# Defaults to `true`. Controls whether configuration
# setting reports are sent to the Contrast web interface.
# enable: true

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
```

```

#
# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
#
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Set to `true` to redirect all logs to
# `stdout` instead of the file system.
# stdout: false

# Set to `true` to redirect all logs to `stderr` instead of
# the file system. May be combined with the corresponding
# `stdout` configuration to write to both streams.
# stderr: false

# Change the Contrast logger from a file-sized based rolling scheme
# to a date-based rolling scheme. At midnight server time, the
# previous day log is renamed to *file_name.yyyy-MM-dd*. Note -
# this scheme does not have a size limit; manual log pruning is
# required. You must set this flag to use the backups and size flags.
# roll_daily: false

# Set the roll size for log files in megabytes. The agent will
# attempt to prevent the log file from being larger than this size.
# roll_size: 100

# Set the number of backup files to keep. Set to `0` to disable.
# backups: 10

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: ./contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# Change the Contrast security logger from a file-sized based rolling
# scheme to a date-based rolling scheme. At midnight server time,
# the log from the previous day is renamed to *file_name.yyyy-MM-dd*.
# Note - this scheme does not have a size limit; manual log
# pruning will be required. This flag must be set to use the
    
```



```
# backups and size flags. Value options are `true` or `false`.
# roll_daily: NEEDS_TO_BE_SET

# Specify the file size cap (in MB) of each log file.
# roll_size: NEEDS_TO_BE_SET

# Specify the number of backup logs that the agent will create before
# Contrast cleans up the oldest file. A value of `0` means that no \
backups
# are created, and the log is truncated when it reaches its size cap.
#
# Note - this property must be used with
# `agent.security_logger.roll_daily=false`; otherwise,
# Contrast continues to log daily and disregard this limit.
#
# backups: NEEDS_TO_BE_SET

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE
```

```
# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.security_logger.syslog.heartbeat
# Define the following properties to
# set the Syslog heartbeat properties.
# \
=====
# heartbeat:

# Set to `true` to enable the Syslog heartbeat.
# The heartbeat will issue a Syslog message at
# the INFO level after every interval passes.
# enable: false

# Set the interval at which to send heartbeat
# messages to the Syslog server (in milliseconds).
# interval_ms: 60000

# \
=====
# agent.java
# The following properties apply to any Java agent-wide configurations.
# \
=====
# java:

# Configure the Java agent to skip its application discovery
# algorithm, and instead associate all libraries, vulnerabilities,
# and web traffic to a single application with the name specified
# by this property. This configuration is preferred when deploying
# Java SE applications with embedded web servers (e.g., applications
# built with Spring Boot, Dropwizard, and embedded Jetty). When used
# with an application server, this configuration associates all
# web traffic with the single, standalone application, including
# web traffic handled by application server-hosted endpoints that
# would not be associated with a discovered application otherwise.
#
# Note - This settings takes preferences
# over the `application.name` setting.
#
# standalone_app_name: NEEDS_TO_BE_SET

# By default, the Java agent visits all classes at startup to look
# for vulnerabilities, which the agent may detect by scanning a
# class (e.g., hardcoded passwords). Set this property to `false`
# to disable the default behavior. If disabled, the agent will
# only visit classes which are likely to require sensors; this
```

```
# can improve application startup time, but may produce fewer
# findings (most likely findings that require static analysis).
#
# scan_all_classes: true

# By default, the Java agent deeply inspects all JAR and WAR files \
loaded
# by the JVM to build a comprehensive understanding of the type \
hierarchy.
# This understanding allows Contrast to instrument sensors into types
# that it might have overlooked. In most cases, this produces a slight
# increase in accuracy at the cost of increased application startup
# time. Set this property to `false` to disable this level of \
inspection.
#
# scan_all_code_sources: true

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Define a list of directories where libraries are stored.
# Directories must be formatted as a semicolon-delimited list.
# Example - `path1;path2;path3`
#
# library_dirs: NEEDS_TO_BE_SET

# Set the maximum archive unpacking depth when analyzing libraries.
# library_depth: 10

# Set the boolean to more aggressively limit the
# manifest information reported for libraries. If true,
# the limit is 1,000 characters, otherwise it's 3,000.
# prune_package_details: true

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
```

```
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
```

```
=====  
==  
# profile  
# Set configuration values under a profile name to enable  
# multi-tenant application configuration on web servers. See  
# https://support.contrastsecurity.com/hc/en-us/articles/360052187171-Multi-Application-configuration-with-Contrast-Profiles  
# for more details.  
# \  
=====  
==  
# profile: {}  
  
# \  
=====  
==  
# protect  
# Use the properties in this section to override Protect features.  
# \  
=====  
==  
# protect:  
  
# Use the properties in this section to determine if the  
# Protect feature should be enabled. If this property is not  
# present, the decision is delegated to the Contrast UI.  
# enable: false  
  
# \  
=====  
# protect.rules  
# Use the following properties to set simple rule configurations.  
# \  
=====  
# rules:  
  
# Define a list of Protect rules to disable in the agent.  
# The rules must be formatted as a comma-delimited list.  
# disabled_rules: NEEDS_TO_BE_SET  
  
# \  
=====  
# protect.rules.bot-blocker  
# Use the following selection to configure if the  
# agent blocks bots. Set to `true` to enable blocking.  
# \  
=====  
# bot-blocker:  
  
# Set to `true` for the agent to block known bots.  
# enable: false  
  
# \  
=====  
# protect.rules.sql-injection
```

```
# Use the following settings to configure the sql-injection rule.
# \
=====
# sql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Tell the agent to detect when semantic analysis of the query
# reveals tautologies used in exfiltration attacks (e.g., "or
# 1=1" or "or 2<>3"). The agent blocks if blocking is enabled.
# detect_tautologies: true

# Tell the agent to detect when semantic analysis of the query
# reveals the invocation of dangerous functions typically used in
# weaponized exploits. The agent blocks if blocking is enabled.
# detect_dangerous_functions: true

# Tell the agent to detect when semantic analysis of the query
# reveals chained queries, which is uncommon in normal usage but
# common in exploit. The agent blocks if blocking is enabled.
# detect_chained_queries: true

# Tell the agent to detect when semantic analysis of the query
# reveals database queries are being made for system tables and
# sensitive information. The agent blocks if blocking is enabled.
# detect_suspicious_unions: true

# Tell the agent to be more aggressive in detecting user
# inputs as SQL comments. This enables the agent to better
# detect SQL Injection input vectors that use comments to
# terminate queries. The agent blocks if blocking is enabled.
# aggressive_comment: false

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# Detect when the agent sees user parameters being executed as
# system commands. The agent blocks if blocking is enabled.
# detect_parameter_command_backdoors: true

# Detect when a system command is issued which contains
# chained commands. The agent blocks if blocking is enabled.
# detect_chained_commands: true

# Detect when a system command is issued with an argument matching a
# known dangerous file path. The agent blocks if blocking is enabled.
# detect_dangerous_path_args: true

# Tell the agent to detect when commands come directly
# from input. The agent blocks if blocking is enabled.
# detect_phased_commands: true

# \
=====
# protect.rules.cmd-injection-process-hardening
# Use the following settings to configure whether
# the agent blocks all attempts to start an external
# process. To enable blocking, set to 'true'.
# \
=====
# cmd-injection-process-hardening:

# Set to `true` to enable the agent to block
# all attempts to start external processes.
# enable: false

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Detect when custom code attempts to access sensitive
# system files. The agent blocks if blocking is enabled.
# detect_custom_code_accessing_system_files: true

# Detect when users attempt to bypass filters by
# using ":::$DATA" channels or null bytes in file
# names. The agent blocks if blocking is enabled.
```

```

# detect_common_file_exploits: true

# \
=====
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====

```



```
# protect.rules.padding-oracle
# Use the following properties to configure
# how the padding-oracle rule works.
# \
=====
# padding-oracle: {}
# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
```

```
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET
```

## Java システムプロパティ

<YourContrastJarPath>を [Contrast JAR ファイル \(57ページ\)](#)へのパスに置き換えて以下のコマンドを実行すると、システムプロパティの詳細情報を確認できます。

- 以下のコマンドにより、Contrast エージェントの JAR ファイルを使用して、一般的なプロパティの一覧を表示することができます。

```
java -jar <YourContrastJarPath> properties
```

- コマンドを検索するには、ツール名を指定してコマンドラインを使用します。例えば、以下のコマンドでプロキシ関連のプロパティの一覧が表示されます。

**filter オプションを使用する場合：**

```
java -jar <YourContrastJarPath> properties --filter=proxy
```

## Java の YAML 設定ファイルのテンプレート

YAML 設定ファイルを使用して Java エージェントを設定する場合には、以下のテンプレートをご利用ください(YAML 設定については、[こちらの説明 \(38ページ\)](#)を参照してください)。

YAML 設定ファイルは、デフォルトの場所に配置します。

- **Unix** : /etc/contrast/java/contrast\_security.yaml
- **Windows** : C:/ProgramData/contrast/java/contrast\_security.yaml

```
# \  
=====\  
==  
# Use the properties in this YAML file to configure a Contrast agent.  
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html  
# to determine the order of precedence for configuration values.  
# \  
=====\  
==  
  
# Use this setting if you want to temporarily disable a Contrast agent.  
# Set to `true` to enable the agent; set to `false` to disable the agent.  
# enable: true  
  
# \  
=====\  
==  
# api  
# Use the properties in this section to connect the agent to the Contrast \  
UI.  
# \  
=====\  
==  
api:  
  
# ***** REQUIRED *****  
# Set the URL for the Contrast UI.  
url: https://app.contrastsecurity.com/Contrast  
  
# ***** REQUIRED *****  
# Set the API key needed to communicate with the Contrast UI.  
api_key: NEEDS_TO_BE_SET  
  
# ***** REQUIRED *****  
# Set the service key needed to communicate with the Contrast  
# UI. It is used to calculate the Authorization header.  
service_key: NEEDS_TO_BE_SET  
  
# ***** REQUIRED *****  
# Set the user name used to communicate with the Contrast
```

```
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# Set the timeout for communicating with TeamServer. This property will be
# respected over the deprecated legacy configuration *contrast.timeout*.
# timeout_ms: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid **contrast.proxy.host**
# and **contrast.proxy.port** will enable the proxy.
# enable: NEEDS_TO_BE_SET

# Set the proxy host. It must be set with port and scheme.
# host: localhost

# Set the proxy port. It must be set with host and scheme.
# port: 1234

# Set the proxy scheme (e.g., `http` or
# `https`). It must be set with host and port.
# scheme: http

# Set this property as an alternate for `scheme://host:port`. It takes
# precedence over the other settings, if specified; however, an error
# will be thrown if both the URL and individual properties are set.
# url: NEEDS_TO_BE_SET

# Set the proxy user.
# user: NEEDS_TO_BE_SET

# Set the proxy password.
# pass: NEEDS_TO_BE_SET

# Set the proxy authentication type. Value
# options are `NTLM`, `Digest`, and `Basic`.
# auth_type: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
```

```

=====
==
# agent:

# \
=====
# agent.reporting
# Use the following settings to configure reporting to the Contrast UI.
# \
=====
# reporting:

# Set the grace period (in milliseconds) after
# agent shutdown to allow draining pending reports.
# shutdown_grace_period_ms: 120000

# \
=====
# agent.effective_config
# None
# \
=====
# effective_config:

# \
=====
# agent.effective_config.reporting
# None
# \
=====
# reporting:

# Defaults to `true`. Controls whether configuration
# setting reports are sent to the Contrast web interface.
# enable: true

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
#
# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
#

```

```
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Set to `true` to redirect all logs to
# `stdout` instead of the file system.
# stdout: false

# Set to `true` to redirect all logs to `stderr` instead of
# the file system. May be combined with the corresponding
# `stdout` configuration to write to both streams.
# stderr: false

# Change the Contrast logger from a file-sized based rolling scheme
# to a date-based rolling scheme. At midnight server time, the
# previous day log is renamed to *file_name.yyyy-MM-dd*. Note -
# this scheme does not have a size limit; manual log pruning is
# required. You must set this flag to use the backups and size flags.
# roll_daily: false

# Set the roll size for log files in megabytes. The agent will
# attempt to prevent the log file from being larger than this size.
# roll_size: 100

# Set the number of backup files to keep. Set to `0` to disable.
# backups: 10

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: ./contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# Change the Contrast security logger from a file-sized based rolling
# scheme to a date-based rolling scheme. At midnight server time,
# the log from the previous day is renamed to *file_name.yyyy-MM-dd*.
# Note - this scheme does not have a size limit; manual log
# pruning will be required. This flag must be set to use the
# backups and size flags. Value options are `true` or `false`.
# roll_daily: NEEDS_TO_BE_SET

# Specify the file size cap (in MB) of each log file.
```

```

# roll_size: NEEDS_TO_BE_SET

# Specify the number of backup logs that the agent will create before
# Contrast cleans up the oldest file. A value of `0` means that no \
backups
# are created, and the log is truncated when it reaches its size cap.
#
# Note - this property must be used with
# `agent.security_logger.roll_daily=false`; otherwise,
# Contrast continues to log daily and disregard this limit.
#
# backups: NEEDS_TO_BE_SET

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

```

```
# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.security_logger.syslog.heartbeat
# Define the following properties to
# set the Syslog heartbeat properties.
# \
=====
# heartbeat:

# Set to `true` to enable the Syslog heartbeat.
# The heartbeat will issue a Syslog message at
# the INFO level after every interval passes.
# enable: false

# Set the interval at which to send heartbeat
# messages to the Syslog server (in milliseconds).
# interval_ms: 60000

# \
=====
# agent.java
# The following properties apply to any Java agent-wide configurations.
# \
=====
# java:

# Configure the Java agent to skip its application discovery
# algorithm, and instead associate all libraries, vulnerabilities,
# and web traffic to a single application with the name specified
# by this property. This configuration is preferred when deploying
# Java SE applications with embedded web servers (e.g., applications
# built with Spring Boot, Dropwizard, and embedded Jetty). When used
# with an application server, this configuration associates all
# web traffic with the single, standalone application, including
# web traffic handled by application server-hosted endpoints that
# would not be associated with a discovered application otherwise.
#
# Note - This settings takes preferences
# over the `application.name` setting.
#
# standalone_app_name: NEEDS_TO_BE_SET

# By default, the Java agent visits all classes at startup to look
# for vulnerabilities, which the agent may detect by scanning a
# class (e.g., hardcoded passwords). Set this property to `false`
# to disable the default behavior. If disabled, the agent will
# only visit classes which are likely to require sensors; this
# can improve application startup time, but may produce fewer
# findings (most likely findings that require static analysis).
#
# scan_all_classes: true
```



```
# By default, the Java agent deeply inspects all JAR and WAR files \
loaded
# by the JVM to build a comprehensive understanding of the type \
hierarchy.
# This understanding allows Contrast to instrument sensors into types
# that it might have overlooked. In most cases, this produces a slight
# increase in accuracy at the cost of increased application startup
# time. Set this property to `false` to disable this level of \
inspection.
#
# scan_all_code_sources: true

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Define a list of directories where libraries are stored.
# Directories must be formatted as a semicolon-delimited list.
# Example - `path1;path2;path3`
#
# library_dirs: NEEDS_TO_BE_SET

# Set the maximum archive unpacking depth when analyzing libraries.
# library_depth: 10

# Set the boolean to more aggressively limit the
# manifest information reported for libraries. If true,
# the limit is 1,000 characters, otherwise it's 3,000.
# prune_package_details: true

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:
```

```

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# profile
# Set configuration values under a profile name to enable

```

```

# multi-tenant application configuration on web servers. See
# https://support.contrastsecurity.com/hc/en-us/articles/360052187171-Multi-
Application-configuration-with-Contrast-Profiles
# for more details.
# \
=====
==
# profile: {}

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
# protect.rules
# Use the following properties to set simple rule configurations.
# \
=====
# rules:

# Define a list of Protect rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
# protect.rules.bot-blocker
# Use the following selection to configure if the
# agent blocks bots. Set to `true` to enable blocking.
# \
=====
# bot-blocker:

# Set to `true` for the agent to block known bots.
# enable: false

# \
=====
# protect.rules.sql-injection
# Use the following settings to configure the sql-injection rule.
# \
=====
# sql-injection:

```

```
# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Tell the agent to detect when semantic analysis of the query
# reveals tautologies used in exfiltration attacks (e.g., "or
# 1=1" or "or 2<>3"). The agent blocks if blocking is enabled.
# detect_tautologies: true

# Tell the agent to detect when semantic analysis of the query
# reveals the invocation of dangerous functions typically used in
# weaponized exploits. The agent blocks if blocking is enabled.
# detect_dangerous_functions: true

# Tell the agent to detect when semantic analysis of the query
# reveals chained queries, which is uncommon in normal usage but
# common in exploit. The agent blocks if blocking is enabled.
# detect_chained_queries: true

# Tell the agent to detect when semantic analysis of the query
# reveals database queries are being made for system tables and
# sensitive information. The agent blocks if blocking is enabled.
# detect_suspicious_unions: true

# Tell the agent to be more aggressive in detecting user
# inputs as SQL comments. This enables the agent to better
# detect SQL Injection input vectors that use comments to
# terminate queries. The agent blocks if blocking is enabled.
# aggressive_comment: false

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Detect when the agent sees user parameters being executed as
# system commands. The agent blocks if blocking is enabled.
# detect_parameter_command_backdoors: true
```

```
# Detect when a system command is issued which contains
# chained commands. The agent blocks if blocking is enabled.
# detect_chained_commands: true

# Detect when a system command is issued with an argument matching a
# known dangerous file path. The agent blocks if blocking is enabled.
# detect_dangerous_path_args: true

# Tell the agent to detect when commands come directly
# from input. The agent blocks if blocking is enabled.
# detect_phased_commands: true

# \
=====
# protect.rules.cmd-injection-process-hardening
# Use the following settings to configure whether
# the agent blocks all attempts to start an external
# process. To enable blocking, set to 'true'.
# \
=====
# cmd-injection-process-hardening:

# Set to `true` to enable the agent to block
# all attempts to start external processes.
# enable: false

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Detect when custom code attempts to access sensitive
# system files. The agent blocks if blocking is enabled.
# detect_custom_code_accessing_system_files: true

# Detect when users attempt to bypass filters by
# using "::$DATA" channels or null bytes in file
# names. The agent blocks if blocking is enabled.
# detect_common_file_exploits: true

# \
=====
```

```
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.padding-oracle
# Use the following properties to configure
# how the padding-oracle rule works.
# \
```

```
=====
# padding-oracle: {}
# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET
```

```

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==
# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.

```



```

# enable: true

# \
=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# Set the timeout for communicating with TeamServer. This property will be
# respected over the deprecated legacy configuration *contrast.timeout*.
# timeout_ms: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid **contrast.proxy.host**
# and **contrast.proxy.port** will enable the proxy.
# enable: NEEDS_TO_BE_SET

# Set the proxy host. It must be set with port and scheme.
# host: localhost

# Set the proxy port. It must be set with host and scheme.
    
```

```
# port: 1234

# Set the proxy scheme (e.g., `http` or
# `https`). It must be set with host and port.
# scheme: http

# Set this property as an alternate for `scheme://host:port`. It takes
# precedence over the other settings, if specified; however, an error
# will be thrown if both the URL and individual properties are set.
# url: NEEDS_TO_BE_SET

# Set the proxy user.
# user: NEEDS_TO_BE_SET

# Set the proxy password.
# pass: NEEDS_TO_BE_SET

# Set the proxy authentication type. Value
# options are `NTLM`, `Digest`, and `Basic`.
# auth_type: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.reporting
# Use the following settings to configure reporting to the Contrast UI.
# \
=====
# reporting:

# Set the grace period (in milliseconds) after
# agent shutdown to allow draining pending reports.
# shutdown_grace_period_ms: 120000

# \
=====
# agent.effective_config
# None
# \
=====
# effective_config:

# \
=====
# agent.effective_config.reporting
```

```
# None
# \
=====
# reporting:

# Defaults to `true`. Controls whether configuration
# setting reports are sent to the Contrast web interface.
# enable: true

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
#
# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
#
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Set to `true` to redirect all logs to
# `stdout` instead of the file system.
# stdout: false

# Set to `true` to redirect all logs to `stderr` instead of
# the file system. May be combined with the corresponding
# `stdout` configuration to write to both streams.
# stderr: false

# Change the Contrast logger from a file-sized based rolling scheme
# to a date-based rolling scheme. At midnight server time, the
# previous day log is renamed to *file_name.yyyy-MM-dd*. Note -
# this scheme does not have a size limit; manual log pruning is
# required. You must set this flag to use the backups and size flags.
# roll_daily: false

# Set the roll size for log files in megabytes. The agent will
# attempt to prevent the log file from being larger than this size.
# roll_size: 100

# Set the number of backup files to keep. Set to `0` to disable.
```

```

# backups: 10

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# Change the Contrast security logger from a file-sized based rolling
# scheme to a date-based rolling scheme. At midnight server time,
# the log from the previous day is renamed to *file_name.yyyy-MM-dd*.
# Note - this scheme does not have a size limit; manual log
# pruning will be required. This flag must be set to use the
# backups and size flags. Value options are `true` or `false`.
# roll_daily: NEEDS_TO_BE_SET

# Specify the file size cap (in MB) of each log file.
# roll_size: NEEDS_TO_BE_SET

# Specify the number of backup logs that the agent will create before
# Contrast cleans up the oldest file. A value of `0` means that no \
backups
# are created, and the log is truncated when it reaches its size cap.
#
# Note - this property must be used with
# `agent.security_logger.roll_daily=false`; otherwise,
# Contrast continues to log daily and disregard this limit.
#
# backups: NEEDS_TO_BE_SET

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

```

```
# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.security_logger.syslog.heartbeat
# Define the following properties to
# set the Syslog heartbeat properties.
# \
=====
# heartbeat:

# Set to `true` to enable the Syslog heartbeat.
# The heartbeat will issue a Syslog message at
# the INFO level after every interval passes.
# enable: false

# Set the interval at which to send heartbeat
# messages to the Syslog server (in milliseconds).
# interval_ms: 60000

# \
=====
# agent.java
# The following properties apply to any Java agent-wide configurations.
# \
```

```
=====
# java:

# Configure the Java agent to skip its application discovery
# algorithm, and instead associate all libraries, vulnerabilities,
# and web traffic to a single application with the name specified
# by this property. This configuration is preferred when deploying
# Java SE applications with embedded web servers (e.g., applications
# built with Spring Boot, Dropwizard, and embedded Jetty). When used
# with an application server, this configuration associates all
# web traffic with the single, standalone application, including
# web traffic handled by application server-hosted endpoints that
# would not be associated with a discovered application otherwise.
#
# Note - This settings takes preferences
# over the `application.name` setting.
#
# standalone_app_name: NEEDS_TO_BE_SET

# By default, the Java agent visits all classes at startup to look
# for vulnerabilities, which the agent may detect by scanning a
# class (e.g., hardcoded passwords). Set this property to `false`
# to disable the default behavior. If disabled, the agent will
# only visit classes which are likely to require sensors; this
# can improve application startup time, but may produce fewer
# findings (most likely findings that require static analysis).
#
# scan_all_classes: true

# By default, the Java agent deeply inspects all JAR and WAR files \
loaded
# by the JVM to build a comprehensive understanding of the type \
hierarchy.
# This understanding allows Contrast to instrument sensors into types
# that it might have overlooked. In most cases, this produces a slight
# increase in accuracy at the cost of increased application startup
# time. Set this property to `false` to disable this level of \
inspection.
#
# scan_all_code_sources: true

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Define a list of directories where libraries are stored.
```

```
# Directories must be formatted as a semicolon-delimited list.
# Example - `path1;path2;path3`
#
# library_dirs: NEEDS_TO_BE_SET

# Set the maximum archive unpacking depth when analyzing libraries.
# library_depth: 10

# Set the boolean to more aggressively limit the
# manifest information reported for libraries. If true,
# the limit is 1,000 characters, otherwise it's 3,000.
# prune_package_details: true

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5
```

```

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# profile
# Set configuration values under a profile name to enable
# multi-tenant application configuration on web servers. See
# https://support.contrastsecurity.com/hc/en-us/articles/360052187171-Multi-Application-configuration-with-Contrast-Profiles
# for more details.
# \
=====
==
# profile: {}

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
# protect.rules

```



```
# Use the following properties to set simple rule configurations.
# \
=====
# rules:

# Define a list of Protect rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
# protect.rules.bot-blocker
# Use the following selection to configure if the
# agent blocks bots. Set to `true` to enable blocking.
# \
=====
# bot-blocker:

# Set to `true` for the agent to block known bots.
# enable: false

# \
=====
# protect.rules.sql-injection
# Use the following settings to configure the sql-injection rule.
# \
=====
# sql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Tell the agent to detect when semantic analysis of the query
# reveals tautologies used in exfiltration attacks (e.g., "or
# 1=1" or "or 2<>3"). The agent blocks if blocking is enabled.
# detect_tautologies: true

# Tell the agent to detect when semantic analysis of the query
# reveals the invocation of dangerous functions typically used in
# weaponized exploits. The agent blocks if blocking is enabled.
# detect_dangerous_functions: true

# Tell the agent to detect when semantic analysis of the query
# reveals chained queries, which is uncommon in normal usage but
# common in exploit. The agent blocks if blocking is enabled.
# detect_chained_queries: true

# Tell the agent to detect when semantic analysis of the query
# reveals database queries are being made for system tables and
# sensitive information. The agent blocks if blocking is enabled.
```

```

# detect_suspicious_unions: true

# Tell the agent to be more aggressive in detecting user
# inputs as SQL comments. This enables the agent to better
# detect SQL Injection input vectors that use comments to
# terminate queries. The agent blocks if blocking is enabled.
# aggressive_comment: false

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Detect when the agent sees user parameters being executed as
# system commands. The agent blocks if blocking is enabled.
# detect_parameter_command_backdoors: true

# Detect when a system command is issued which contains
# chained commands. The agent blocks if blocking is enabled.
# detect_chained_commands: true

# Detect when a system command is issued with an argument matching a
# known dangerous file path. The agent blocks if blocking is enabled.
# detect_dangerous_path_args: true

# Tell the agent to detect when commands come directly
# from input. The agent blocks if blocking is enabled.
# detect_phased_commands: true

# \
=====
# protect.rules.cmd-injection-process-hardening
# Use the following settings to configure whether
# the agent blocks all attempts to start an external
# process. To enable blocking, set to 'true'.
# \
=====
# cmd-injection-process-hardening:

# Set to `true` to enable the agent to block
# all attempts to start external processes.
# enable: false

```

```
# \  
=====\  
# protect.rules.path-traversal  
# Use the following properties to configure  
# how the path traversal rule works.  
# \  
=====\  
# path-traversal:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# Detect when custom code attempts to access sensitive  
# system files. The agent blocks if blocking is enabled.  
# detect_custom_code_accessing_system_files: true  
  
# Detect when users attempt to bypass filters by  
# using "::$DATA" channels or null bytes in file  
# names. The agent blocks if blocking is enabled.  
# detect_common_file_exploits: true  
  
# \  
=====\  
# protect.rules.method-tampering  
# Use the following properties to configure  
# how the method tampering rule works.  
# \  
=====\  
# method-tampering:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====\  
# protect.rules.reflected-xss  
# Use the following properties to configure how  
# the reflected cross-site scripting rule works.  
# \  
=====\  
# reflected-xss:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#
```

```
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.padding-oracle
# Use the following properties to configure
# how the padding-oracle rule works.
# \
=====
# padding-oracle: {}

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
```

```
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
```

```
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET
```

## スタンドアロンアプリケーションの Java エージェントを設定



### 注記

Java エージェント 4.x では、スタンドアロンアプリケーションの設定は必要ありません。

バージョン 3.x を使用している場合は、[旧 Java エージェント \(136ページ\)](#)のドキュメントを確認してください。

## TLS(Transport Layer Security)

Contrast Java エージェントは、Contrast サーバと通信するために安全な TLS 接続を使用しています。

Contrast の SaaS 版では、よりセキュリティが強化された TLS 1.2 の接続と業界標準の認証局(CA)によって署名された証明書を使用しております。また、オンプレミス版をご利用のお客様は、エンタープライズ CA を使用するために Java エージェントを設定し、Java エージェントが TLS ハンドシェイクでクライアント証明書を送信するよう設定する必要があります。

Contrast Java エージェントは、TLS を構成するために標準の [Java 暗号化アーキテクチャ\(JCA\)](#)を使用します。具体的に、Java エージェントは、システムの「TLS」の [javax.net.ssl.SSLContext](#) を使用します。そのため、ほとんどのユーザは、標準の [javax.net.ssl.trustStore](#) システムプロパティを使用して、エージェントが信頼できる証明書を指定できます。また、標準の [javax.net.ssl.keyStore](#) システムプロパティを使用して、TLS サーバがクライアント証明書を要求する際にエージェントから送信される証明書を指定することもできます。

以下は、カスタムキーストアとトラストストアを使用して、Java エージェントを設定している例です。

```
java \  
-javaagent:contrast.jar \  
-Djavax.net.ssl.trustStore=/etc/pki/tls/my-enterprise-truststore.p12 \  
-Djavax.net.ssl.trustStorePassword=changeit \  
-Djavax.net.ssl.trustStoreType=PKCS12 \  
-Djavax.net.ssl.keyStore=/etc/pki/tls/server-client-certificate.p12 \  
-Djavax.net.ssl.keyStorePassword=password \  
-Djavax.net.ssl.keyStoreType=PKCS12 \  
-jar my-server.jar
```

## JPMS(Java Platform Module System)で Java エージェントを使用

JPMS は Java 9 で導入されており、コードをカプセル化する機能を提供します。Contrast は、JPMS で書かれたモジュールの検査とアプリケーションの起動をサポートします。

Java エージェントを使用するには、アプリケーションの `module-info.java` ファイルに `java.sql` パッケージの利用を宣言する必要があります。

```
module mymodule {
    requires java.sql;
}
```

または、ランタイムに `--add-modules` というコマンドラインの引数で指定します。

```
java -javaagent:/opt/contrast/contrast-agent.jar --add-modules java.sql --
module-path libs --module mymodule/mycompany.App
```

## Java 2 セキュリティ

Java 2 セキュリティマネージャを使用すると、システム管理者は、JVM 内の Java コードに対して使用可能な権限を規定するポリシーを適用できます。

Java エージェントで Java 2 セキュリティマネージャを使用する場合は、Java セキュリティポリシーファイルを設定して、Java コードのプリンシパルに権限を適用する必要があります。

Java コードのプリンシパルは、通常 `CodeSource` (JAR など)によって識別され、まれに署名付き JAR のエンティティによる場合もあります。

例えば、Tomcat のデフォルトの `catalina.policy` ファイルで、このポリシーは JDBC ドライバの JAR に権限を付与しています。

```
// The permission granted to your JDBC driver
grant codeBase "jar:file:${catalina.base}/webapps/examples/WEB-INF/lib/
driver.jar!/-" {
    permission \
java.net.SocketPermission "dbhost.mycompany.com:5432", "connect";
};
```

Java 2 セキュリティマネージャは、ユーザがデプロイするコードをシステム管理者が完全に信頼できない場合には便利です。例えば、マルチテナントの Tomcat インスタンスでユーザのアプリケーションをホストする場合、Java 2 セキュリティマネージャを使用して、ユーザのアプリケーションによってサービス全体が停止されないように制御できます(例、`System.exit()`の呼出しを許可しないなど)。

Contrast の Java エージェントで Java 2 セキュリティマネージャを使用する場合は、セキュリティポリシーファイルで、Java エージェントに全権限を付与する必要があります(`java.security.AllPermission`)。これを行うには、`<YourContrastJarPath>`を [Contrast JAR \(57ページ\)](#)ファイルへのパスに置き換えて、以下を使用してください。

```
grant codeBase "file:<YourContrastJarPath>" {
    permission java.security.AllPermission;
};
```

Java 2 セキュリティマネージャと、以下のいずれかの環境を使用する場合は、さらに設定が必要になる場合があります。

- [Glassfish](#)
- [Jetty \(72ページ\)](#)
- [Tomcat \(73ページ\)](#)
- [WebLogic \(74ページ\)](#)

- [WebSphere \(75ページ\)](#)
- [WildFly \(71ページ\)](#)

## 旧 Java エージェント

Java エージェントのバージョン 4.x および EOP のバージョン 3.9.5 のリリースに伴い、次のようなシグナテクノロジーで動作する Java 6・Java 7 の Web アプリケーションを検査するには、Contrast の旧 Java エージェント(3.x 以前)を使用してください。

- Jboss 4.2、6.1、7.1
- Weblogic 9、10、11

旧エージェントには、CVE-45046 に対する保護を提供する JNDI ルールが Contrast Protect に含まれています。

## 手順

エージェントのバージョンが 3.15 以前の場合、ルートカバレッジなどの特定の機能を利用するには、追加のプロパティの設定が必要です。

1. YAML 設定ファイルをエディタで開きます。
2. あらかじめ入力されている認証キーに加えて、`agent.java.standalone_app_name` プロパティを追加します。  
このプロパティには、Contrast で表示させたいアプリケーションの名前を割り当てます。この例では、`<MyAppName>`を使用したい名前に置き換えてください。

```
api:
  url: https://xxx.contrastsecurity.com/Contrast
  api_key: A2xxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxxG9N
  service_key: 88xxxxxxxxxxxxx5Z
  user_name: agent_xxxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxxx@OrgName
agent:
  java:
    standalone_app_name: <MyAppName>
```

旧 Java エージェントは、[Maven Central Repository Search](#) よりダウンロードしてください。

## Java エージェントのテレメトリ

Contrast の Java エージェントは、テレメトリを使用して、使用状況に関するデータを収集します。テレメトリは、エージェントを組み込んだアプリケーションでエージェントのセンサーが最初にロードされた時に収集され、その後も定期的に(数時間ごと)に収集されます。

弊社では、[お客様のプライバシーは非常に大切である \(828ページ\)](#)と考えています。このテレメトリ機能は、アプリケーションのデータを収集するものではありません。データは匿名化されてから、Contrast に安全に送信されます。そして、集約されたデータは暗号化されて保存され、アクセスが制限されます。収集されたデータは、全て 1 年後に削除されます。

テレメトリ機能はオプションです。テレメトリ機能で収集されるのは、以下のデータです。

エージェントのバージョン	収集されるデータ
Java 3.16.x	<ul style="list-style-type: none"> <li>• オペレーティングシステムとバージョン</li> <li>• エージェントがコンテナ内で実行されているかどうか</li> <li>• JVM に設定されているメモリ制限</li> <li>• Java のバージョンとベンダ情報</li> <li>• 利用可能な物理メモリ</li> <li>• CPU 数</li> </ul>





### 注記

テレメトリ機能を停止するには、`CONTRAST_AGENT_TELEMETRY_OPTOUT` という環境変数に `true` または `1` を設定してください。テレメトリのデータは、`telemetry.java.contrastsecurity.com` に安全に送信されます。ネットワークレベルで通信をブロックすることで、テレメトリ機能を停止することもできます。

## .NET Framework エージェント

Contrast .NET Framework エージェントは、ユーザが .NET Web アプリケーションを操作する際のアプリケーションの動きを解析します。

.NET Framework エージェントをインストールすると、IIS にデプロイされた ASP.NET アプリケーションにエージェントが自動的に組み込まれます。エージェントによる解析は、ユーザによって(または自動化されたスクリプトやテストによって)アプリケーションが操作される時に実行されます。

エージェントの解析結果は、Contrast Web インターフェイスで確認できます。Contrast .NET Framework エージェントは、以下のように複数のコンポーネントで構成されています。

- **バックグラウンドの Windows サービス** : (*DotnetAgentService.exe*)このサービスは、エージェントを組み込むための環境を準備し、エージェントコンポーネント間の通信を管理します。主要となるサービスで、エージェントの動作を制御します。このバックグラウンドの Windows サービスを停止することで、Contrast エージェントの組み込みと解析を無効にできます。
- **.NET プロファイラ** : エージェントセンサーへのメソッドの呼び出しに組み込まれて、アプリケーションを計測します。
- **センサー** : 複数のセンサーが、セキュリティ、アーキテクチャ、ライブラリに関する情報を収集します。
- **.NET Framework Contrast トレイ (191ページ)** : Windows システムトレイアプリケーションで、エージェントの状態に関する情報を概要レベルで表示します。

次のステップ :

- [.NET Framework エージェントをインストールする \(139ページ\)](#)
- [サポート対象テクノロジーを確認する \(137ページ\)](#)
- [システム要件を確認する \(138ページ\)](#)
- [IIS Express で .NET Framework エージェントを使用する \(185ページ\)](#)
- [IIS でアプリケーションプールを使用する \(193ページ\)](#)

### .NET Framework エージェントのサポート対象テクノロジー

Contrast .NET エージェントは、以下のテクノロジーで構築される Web アプリケーションの解析をサポートします。

テクノロジー	サポート対象のバージョン	注記
Windows 版 .NET Framework		

テクノロジー	サポート対象のバージョン	注記
アプリケーションのランタイムバージョン	4.5 以降	古いバージョンの .NET 4 をアプリケーションがターゲットにしている場合でも、.NET Framework アプリケーションの互換性により、ほとんどのアプリケーションで最新の .NET Framework エージェントを使用できます。  <b>サポート対象外：</b>  <ul style="list-style-type: none"> <li>Classic ASP Classic ASP のアプリケーションは .NET ランタイムで動作しません。</li> <li>Mono ランタイム Contrast エージェントは、CLR のプロファイル API を使用してアプリケーションを計測します。CLR プロファイル API は、CLR によって公開される COM(Component Object Model)ベースのインターフェイスです。Linux では COM をサポートしません。したがって、Mono は CLR プロファイル API をサポートしないため、Contrast は Mono をサポートできません。</li> </ul>
サーバのランタイムバージョン	4.7.1, 4.7.2, 4.8	
CLR	CLR4	
Web サーバ	<ul style="list-style-type: none"> <li>IIS</li> <li>IIS Express</li> </ul>	
アプリケーションフレームワーク	<ul style="list-style-type: none"> <li>ASP.NET MVC 3-5</li> <li>ASP.NET Web Forms</li> <li>ASP.NET Web Pages</li> <li>IIS-ホストの ASMX ベース Web サービス</li> <li>IIS ホストの Web API</li> <li>IIS ホストの WCF サービス</li> <li>OWIN ホストの Web API(Windows サービスまたはコマンドラインアプリケーション経由)</li> </ul>	これらのフレームワークは、テスト済みのものを明示的に記載していますが、フレームワークが単に典型的な ASP.NET クラス(例えば、System.Web.HttpRequest など)をラップしている場合は、他のアプリケーションを解析できる場合があります。  <b>サポート対象外：</b>  <ul style="list-style-type: none"> <li>.NET Framework の ASP.NET Core アプリケーションの解析(.NET Core アプリケーションを解析するには、<a href="#">.NET Core エージェント (195ページ)</a> を使用)。</li> <li>部分的な信頼(trust)レベルで実行されているアプリケーション。</li> </ul>



### 注記

- Azure App Service の場合、.NET Framework アプリケーションは .NET Framework の **拡張機能** または **NuGet パッケージ** を使用する必要があります。
- .NET Core アプリケーションは、.NET Core の **拡張機能** または **NuGet パッケージ** を使用する必要があります。

## .NET Framework エージェントのシステム要件

.NET Framework エージェントをインストールする前に、以下のシステム要件を満たす必要があります。

- Web サーバへの管理者権限があり、そのサーバは Contrast のサポート対象であること。
- 検査対象のアプリケーションがデプロイされており、その Web アプリケーションのテクノロジーは Contrast のサポート対象であること。
- IIS を再起動できること。
- Web サーバが Contrast とネットワークで接続されていること。
- サーバが最低限の要件を満たしていること。

要件	推奨	備考
サーバのランタイムバージョン	4.7.1 以降	.NET Framework エージェントのインストールには、.NET 4.7.1 以降を必要としますが、.NET Framework アプリケーション自体の互換性により、.NET 4.5 以降をターゲットとするアプリケーションを解析できます。
オペレーティング システム	<ul style="list-style-type: none"> <li>Windows 10</li> <li>Windows Server 2012、2012 R2、2016、2019</li> <li>Azure Virtual Machines、Cloud Services、Mobile Services</li> <li>Azure App Service</li> </ul>	
プロセッサのアーキテクチャ	<ul style="list-style-type: none"> <li>32 ビット</li> <li>64 ビット</li> </ul>	64 ビットシステムでは、エージェントを使用して 32 ビットと 64 ビットの両方の Web アプリケーションを解析できます。
CPU	4 個以上	最低：2
メモリ	8 GB 以上	最低：4 GB
	.NET エージェントを使用する場合、検査対象のアプリケーションのメモリ要件がおよそ 2 倍になります。.NET エージェントがインストールされていない場合に、アプリケーションが使用するメモリは全メモリ容量の半分以下である必要があります。	
サーバ	<ul style="list-style-type: none"> <li>.NET Framework 4.7.1</li> <li>CLR 4 (.NET 4.0 以降)</li> </ul>	これより古いバージョンを使用するサーバでは、 <a href="#">旧 .NET Framework エージェント</a> を使用してください。



## 注記

- .NET Framework エージェントでは CLR プロファイル API を使用して、データとコードフローの解析(SQL インジェクション、XSS、脆弱な暗号化の検出など)や、検査対象のアプリケーションが使用するライブラリやテクノロジーを検出します。
- Contrast エージェントは、`agent.dotnet.enable_chaining` の設定を有効にすることで、パフォーマンスツールや APM ツールなどの他の .NET プロファイルエージェントと共存 (187ページ) できます。
- 古いバージョンを使用するサーバでは、[旧 .NET Framework エージェント](#)を使用してください。

## .NET Framework エージェントのインストール

.NET Framework エージェントのインストールは、通常、ほとんどの環境でインストーラが拡張機能を使用して自動的に行うことができます。.NET Framework エージェントの基本的なインストールは、次のようになります。

- インストーラをダウンロードし、サーバに置きます。
- インストーラを実行します。
- 通常通りにアプリケーションを疎通し、Contrast でアプリケーションが認識されていることを確認します。



### 注記

Windows 2008 を使用していて、.NET Framework のバージョンが 4.7.1 よりも前である、または、アプリケーションが CLR2 を対象としている場合は、[旧 .NET Framework エージェントのインストーラ](#)を使用してください。

具体的に、.NET Framework エージェントをどのようにインストールするかによって、インストール方法は異なります。

- [.NET Framework エージェントの Windows インストーラ \(140ページ\)](#)
- [Azure App Service \(143ページ\)](#)
- [Docker などのコンテナ内 \(145ページ\)](#)
- [Web API-OWIN \(147ページ\)](#)

エージェントを自動アップグレードするには、[エージェントアップグレードサービス \(150ページ\)](#)のオプションを有効にします。

## .NET Framework エージェントの Windows インストーラ

Contrast .NET Framework エージェントのインストーラは、標準の MSI を利用して作られた Windows アプリケーションの一般的なインストーラです。インストーラは、対象となるサーバが要件(サーバのオペレーティングシステムがサポート対象であることなど)を満たしているかを検証します。サーバが全ての要件を満たしていれば、インストーラによって以下が行われます。

- .NET Framework エージェントを Windows の標準プログラムとして登録します。
- 指定されたインストール場所(例、`C:\Program Files\Contrast\dotnet`)にエージェントのファイルを配置します。これには、いくつかのダイナミックリンクライブラリ(DLL)や、エージェントをバックグラウンドで動作させる Windows サービスなどの実行ファイルが含まれます。
- エージェントのログファイルや設定を主に保存するためのデータディレクトリ(例、`C:\ProgramData\Contrast\dotnet`)を作成します。
- エージェントをバックグラウンドで実行させる Windows サービスをオペレーティングシステムに登録します。
- エージェントのネイティブモジュールを IIS に追加します。ネイティブモジュールは、環境変数によってエージェントのプロファイラコンポーネントを IIS に登録します。これにより、CLR はエージェントのプロファイラをロードし、解析対象のアプリケーションにエージェントが組み込まれます。
- エージェントの Windows サービスと [Contrast トレイ \(191ページ\)](#)アプリケーションを起動します。このサービスは次の処理を行います。
  - ローカルの名前付きパイプによって、プロファイラとセンサコンポーネントとを通信します。



### 注記

- [OWIN を使用したセルフホスト Web API \(147ページ\)](#)(IIS 以外)でエージェントを使用する場合は、さらに設定が必要です。
- Windows 2008 を使用していて、.NET Framework のバージョンが 4.7.1 よりも前である、または、アプリケーションが CLR2 を対象としている場合は、[旧 .NET Framework エージェントのインストーラ](#)を使用してください。

Contrast Web インターフェイスから .NET Framework エージェントをインストール :

## Contrast Web インターフェイスから .NET Framework エージェントをインストール

1. Contrast Web インターフェイスで、右上の **新規登録** を選択します。
2. アプリケーション言語のドロップダウンメニューで **.NET Framework** を選択し、**IIS でホスト** を選択したら、**エージェントと YAML 設定ファイルをダウンロード** へのリンクを選択します。
3. ダウンロードした ZIP アーカイブを Web サーバに展開し、*ContrastSetup.exe* を実行します。これで、.NET Framework エージェントがインストールされます。  
 インストーラによって、*contrast\_security.yaml* ファイルがエージェントのデータディレクトリにコピーされます。デフォルトは、*C:\ProgramData\Contrast\dotnet\contrast\_security.yaml* になります。コピー先に既に YAML ファイルが存在する場合は、インストーラは YAML ファイルをコピーしません。
  - **コマンドラインを使用 (152ページ)** すると、.NET Framework エージェントの Windows インストーラでサポートされるその他のオプションを利用できます。
  - この環境で別のプロファイラ (New Relic や AppDynamics などの APM など) を使用している場合は、**Contrast プロファイラチェーン (187ページ)** を有効にする必要があります。
4. **NET Framework エージェントの YAML テンプレート (154ページ)** を使用して、.NET Framework エージェントの設定をより詳細に指定できます。
5. 通常通りにアプリケーションを疎通し、Contrast でアプリケーションが認識されていることを確認します。  
 解析する必要のないアプリケーションがある場合や、パフォーマンスの有効活用を考える場合には、**アプリケーションプール (193ページ)** を利用して検査対象のアプリケーションの数を制限することを検討してください。

## コマンドラインから .NET Framework エージェントをインストール

コマンドラインを使用してインストールすると、.NET Framework エージェントの Windows インストーラでサポートされるその他のオプションを利用できます。

.NET エージェントは、Windows のインターフェイスを使用してインストールし、Windows の標準機能 (コントロールパネルのプログラムと機能や Powershell など) を使用してアンインストールや修復を行うことができます。ただし、自動化されたスクリプトなどの特定のシナリオでは、.NET Framework エージェントの Windows インストーラを使用して、以下の操作が必要な場合があります。

有人モードには、以下のコマンドを使用します。

- **インストール** : `ContrastSetup.exe`
- **アンインストール** : `ContrastSetup.exe -uninstall`
- **修復** : `ContrastSetup.exe -repair`

無人モードまたはサイレントモードには、以下のコマンドを使用します。

- **インストール** : `ContrastSetup.exe -s -norestart`
- **アンインストール** : `ContrastSetup.exe -uninstall -s -norestart`
- **修復** : `ContrastSetup.exe -repair -s -norestart`

コマンドラインを使用してのインストールでは、.NET Framework エージェントの Windows インストーラで利用できるその他のオプションを指定できます。

オプション	説明	例
INSTALLFOLDER	インストール先ディレクトリを指定します。このディレクトリに、プログラムファイルが書き込まれます。デフォルトは OS の変数によって異なります。	<code>INSTALLFOLDER="D:\Programs\Contrast"</code>
AGENT_EXPLORER_INSTALLFOLDER	Agent Explorer のファイルのディレクトリを指定します。	<code>AGENT_EXPLORER_INSTALLFOLDER="C:\Program Files\Contrast\agent-explorer"</code>

オプション	説明	例
DATAFOLDER	データディレクトリを指定します。このディレクトリに、ログや contrast_security.yaml ファイルが書き込まれます。デフォルトは OS の変数によって異なります。	DATAFOLDER = "D:\Data\Contrast"
PathToYaml	カスタムの YAML 設定ファイルを指定します。デフォルトの値は、インストーラの場所を基準にして置かれている contrast_security.yaml ファイルです。	PathToYaml=c:\contrast_security.yaml
SERVICE_STARTUP_TYPE_MANUAL	このオプションは、エージェントのインストール、更新、修復を行う場合に必要です。このオプションの値を 1 に設定すると、Contrast サービスのスタートアップの種類が設定されます。デフォルトの値は 0 で、「自動(遅延開始)」です。	SERVICE_STARTUP_TYPE_MANUAL=1
SUPPRESS_SERVICE_START	このオプションは、エージェントのインストール、更新、修復を行う場合に必要です。このオプションの値を 1 に設定すると、サービスが自動で起動されなくなります。デフォルトの値は、0 です。	SUPPRESS_SERVICE_START=1
SUPPRESS_RESTARTING_IIS	このオプションの値を 1 に設定すると、インストーラは IIS を再起動しません。  デフォルトの値は、0 です。	SUPPRESS_RESTARTING_IIS=0
<div style="display: flex; align-items: center; justify-content: center;">  <div> <p><b>注記</b></p> <p>IIS が再起動されるまで、アプリケーションにエージェントは組み込まれません。</p> </div> </div>		
USE_VIRTUAL_SERVICE_ACCOUNT	制限された仮想サービスアカウントで、エージェントサービスを実行します。SYSTEM の代わりに、仮想アカウント NT Service\DotnetAgentSvc としてサービスを実行するように構成します。	USE_VIRTUAL_SERVICE_ACCOUNT=0
INSECURE_YAML_FILE	昇格していないユーザの contrast_security.yaml ファイルへの編集を制限します。	INSECURE_YAML_FILE=0
INSTALL_AGENT_EXPLORER	Agent Explorer をインストールしない場合は、このオプションの値を 0 に設定して下さい。  デフォルトの値は 1 で、Agent Explorer はインストールされます。	INSTALL_AGENT_EXPLORER=1
INSTALL_UPGRADE_SERVICE	エージェントアップグレードサービスをインストールしない場合は、このオプションの値を 0 に設定して下さい。デフォルトの値は 1 で、エージェントアップグレードサービスはインストールされます。	INSTALL_UPGRADE_SERVICE=1
UPGRADE_SERVICE_INSTALLFOLDER	アップグレードサービスのファイルのディレクトリを指定します。	UPGRADE_SERVICE_INSTALLFOLDER="C:\Program Files(x86)\Contrast\upgrade-service"



### ヒント

例えば、スクリプトを使用して .NET エージェントをインストールするには、以下のコマンドを使用します。

```
ContrastSetup.exe -s PathToYaml=C:\Temp\custom.yaml
```

このコマンドでは、.NET エージェントのインストールを無人/サイレントモードで行い、YAML 設定ファイルのカスタムパスを使用します。



### 重要

エージェントをインストールすると、Contrast は自動的に IIS を再起動します。

## Azure App Service で .NET Framework エージェントをインストール



### 注記

拡張機能を利用できない場合は、[NuGet を使用して .NET Framework エージェントを手動でインストール \(147ページ\)](#) できます。

### 手順

Azure Portal の拡張機能を使用して .NET Framework エージェントをインストールするには：

1. Azure App Service でホストするアプリケーションを作成します。  
これを行うには、[Azure アカウント](#)を持っており、[ASP.NET Framework の Web アプリケーション](#)を作成する必要があります。アプリケーションを Azure に公開し、Contrast エージェントなしで想定通りに機能することを確認します。
2. アプリケーションのメニューより **構成** を選択し、**アプリケーション設定** の画面で以下の値を追加し、エージェントが Contrast サーバに接続するための設定をします。

キー	値
CONTRAST_API_USER_NAME	自分の <a href="#">エージェントユーザ名 (37ページ)</a> を指定します。
CONTRAST_API_SERVICE_KEY	自分の <a href="#">エージェントサービスキー (37ページ)</a> を指定します。
CONTRAST_API_API_KEY	自分の <a href="#">API キー (37ページ)</a> を指定します。
CONTRAST_API_URL	デフォルトは、 <a href="https://app.contrastsecurity.com">https://app.contrastsecurity.com</a> です。別の場所でホストされている Contrast サーバを使用する場合は、その URL を指定します。

3. App Service にデプロイ中のアプリケーションを選択します。
4. メニュー画面より、**拡張機能** を選択します。
5. **+追加** を選択します。
6. 拡張機能の選択をクリックし、一覧より **Contrast .NET Site Extension** を選択します。これが、.NET Framework アプリケーション用の拡張機能になります。
7. 法律条項に同意して、**OK** ボタンをクリックします。
8. 拡張機能のインストールが完了するまでしばらく待ったら、正しくインストールされていることを確認します。
9. アプリケーションの概要に戻り、アプリケーションを **再起動** します。

10. アプリケーションを疎通し、検査結果が Contrast に報告されることを確認します。



### ヒント

アプリケーションの SCM サイト(Kudu)の「Site Extensions」メニューからも Contrast エージェントをインストールできます。



### 重要

Contrast エージェントの新しいバージョンが利用可能な場合、Azure Portal または Kudu のダッシュボードに通知されます。エージェントの更新を行う前にサイトを停止してください。停止しない場合、更新が失敗する可能性があります。



### 注記

サイトの拡張機能により、以下のような環境変数がいくつか設定されます。

```
COR_ENABLE_PROFILING=1
COR_PROFILER={EFEB8EE0-6D39-4347-A5FE-4D0C88BC5BC1}
COR_PROFILER_PATH_32=D:\home\siteextensions\Contrast.Net.Azure.SiteExtension\ContrastAppService\runtimes\win-x86\native\ContrastProfiler.dll
COR_PROFILER_PATH_64=D:\home\siteextensions\Contrast.Net.Azure.SiteExtension\ContrastAppService\runtimes\win-x64\native\ContrastProfiler.dll
CONTRAST_INSTALL_DIRECTORY=D:\home\siteextensions\Contrast.Net.Azure.SiteExtension\ContrastAppService\
MicrosoftInstrumentationEngine_ConfigPath32_ContrastX86Config=D:\home\siteextensions\Contrast.Net.Azure.SiteExtension\runtimes\win-x86\ContrastCieProfiler.config
MicrosoftInstrumentationEngine_ConfigPath64_ContrastX64Config=D:\home\siteextensions\Contrast.Net.Azure.SiteExtension\runtimes\win-x64\ContrastCieProfiler.config
```

CLR Instrumentation Engine(CIE)がアプリケーションに設定されている場合(例えば、Application Insights が有効になっているために)、Azure は自動的に `COR_PROFILER*` 変数を上書きし、CIE のプロファイラを指すようにします。

そして、CIE では、`MicrosoftInstrumentationEngine_*`変数を使用して Contrast エージェントをロードするようになります。

CIE がアプリケーションに設定されていない場合は、Contrast エージェントのロードに標準の `COR_PROFILER*`変数が使用されます。



## コンテナを使用して .NET Framework エージェントをインストール

### インストールを行う前に

本項では、Docker を例として、コンテナ化されたアプリケーションに Contrast .NET Framework エージェントをインストールするための一般的な手順について説明します。

コンテナや関連ソフトウェアの仕組みを基本的に理解している必要があります。必要に応じて、お客様の環境に合わせて手順を調整してください。

### 手順 1：エージェントをインストール

コンテナイメージにアプリケーションを追加する前でも後でもインストールすることができます。推奨される方法は、名前を付けた **マルチステージビルド** を使用することです。例：

```
FROM mcr.microsoft.com/dotnet/framework/sdk:4.8

# Hidden for brevity...

# Copy the required agent files from the official Contrast agent image.
COPY --from=contrast/agent-dotnet-framework:latest C:\Contrast C:\Contrast
```

この例では、最新の .NET Framework エージェントをコピーしています。利用可能なタグは DockerHub で確認してください。

### 手順 2：エージェントを設定

Contrast エージェントは、複数のソースからの設定を受け入れますが、設定の **優先順位 (36ページ)** は優先順位セクションに記載されています。

設定方法を組み合わせて利用することをお勧めします。

- YAML ファイルを使用して、複数のアプリケーションで共有する共通の設定を指定します。
- アプリケーション固有の設定値や、YAML ファイルで指定した値を上書きする場合や、実行時に組み込む機密情報などには、環境変数を使用します。

#### YAML ファイルの設定：

**YAML ファイル (38ページ)** を使用してエージェントを設定する場合に、環境変数の `CONTRAST_CONFIG_PATH` を使用して、YAML ファイルがコンテナ内のどこにあるかを指定することもできます。

例えば、`contrast_security.yaml` という名前の YAML 設定ファイルが Docker のビルドコンテキストに存在するとします。

```
agent:
  logger:
    path: /var/tmp
    level: WARN
```

環境変数 `CONTRAST_CONFIG_PATH` を使用して、以下のようにコンテナイメージにエージェント YAML ファイルを追加することができます。

```
FROM mcr.microsoft.com/dotnet/framework/sdk:4.8

# Hidden for brevity...

# Add the Contrast agent to the image.
COPY --from=contrast/agent-dotnet-framework:latest C:\Contrast C:\Contrast

# Copy the contrast_security.yaml file from Docker build context.
```

```
COPY ./contrast_security.yaml /contrast_security.yaml

# Finally configure the agent to use the YAML file previously \
copied.
ENV CONTRAST_CONFIG_PATH=/contrast_security.yaml
```

**環境変数の設定 :**

アプリケーション固有の設定を指定するために、[環境変数 \(56ページ\)](#)を使用します。以下は、一般的によく使用される設定オプションです。

項目	用途	環境変数
アプリケーション名	Contrast サーバに報告されるアプリケーション名を指定します。	CONTRAST__APPLICATION__NAME
アプリケーショングループ	オンボード時にこのアプリケーションと関連付けるアクセスグループを指定します。	CONTRAST__APPLICATION__GROUP
 <p><b>注記</b> この変数を使用する前に、Contrast でアプリケーションアクセスグループを作成してください。</p>		
アプリケーションのタグ	アプリケーションにタグを追加します。	CONTRAST__APPLICATION__TAGS
サーバ名	Contrast に報告されるサーバ名を指定します。	CONTRAST__SERVER__NAME
サーバの環境	アプリケーションを実行する環境を指定します。このオプションで有効な値 : Development、QA、Production	CONTRAST__SERVER__ENVIRONMENT
サーバのタグ	サーバにタグを追加します。	CONTRAST__SERVER__TAG

**手順 3 : プロファイル変数と認証情報を追加**

アプリケーションに .NET エージェントを組み込んで検査を行うには、[さらに環境変数 \(56ページ\)](#)が必要です。COR\_CLR 変数はエージェントをロードし、CONTRAST\_ 変数は Contrast サーバに対するエージェントの認証用です。

前述の Dockerfile の例を使用すると、以下のようになります。

```
FROM mcr.microsoft.com/dotnet/framework/sdk:4.8

COPY --from=contrast/agent-dotnet-framework:latest C:\Contrast C:\Contrast

ENV COR_ENABLE_PROFILING=1 \
    COR_PROFILER={EFEB8EE0-6D39-4347-A5FE-4D0C88BC5BC1} \
    COR_PROFILER_PATH_32=C:\Contrast\runtimes\win-x86\native\ContrastProfiler.dll \
    COR_PROFILER_PATH_64=C:\Contrast\runtimes\win-x64\native\ContrastProfiler.dll
```

さらに、サーバに対するエージェント認証のために、[以下の環境変数 \(37ページ\)](#)が必要です。

```
CONTRAST__API__URL=https://app.contrastsecurity.com/Contrast
CONTRAST__API__API_KEY={API }
CONTRAST__API__SERVICE_KEY={ }
```

API の値([エージェントキー \(37ページ\)](#))は Contrast Web インターフェイスで確認するか、.NET Framework エージェント用の [YAML ファイルをダウンロード \(154ページ\)](#) することで取得できます。

## 例

こちらの [GitHub リポジトリ](#) で、設定が完了したコードの例を参照できます。特に、以下の ASP.NET アプリケーションのサンプルなどを参考にしてください。

- デフォルトのアプリケーションプールを使用：
  - [Dockerfile](#)
  - [エントリポイントスクリプト](#)
- カスタムのアプリケーションプールを使用：
  - [Dockerfile](#)
  - [エントリポイントスクリプト](#)

## 関連項目

Contrast サポートポータル：[Kubernetes での Contrast エージェント](#)

Contrast サポートポータル：[AWS Fargate と Contrast エージェント](#)

## NuGet で .NET Framework エージェントを手動インストール

.NET Framework エージェントは、NuGet を使用して手動でインストールすることもできます。このインストール方法は、[Azure App Service の拡張機能 \(143ページ\)](#) を利用できない場合や、.NET Framework エージェントを依存関係に含めたい場合などに便利です。

1. アプリケーションに Contrast の NuGet パッケージをインストールします。  
Visual Studio で、ソリューションエクスプローラーのアプリケーションのプロジェクトで [参照](#) を右クリックし、[NuGet パッケージの管理](#) を選択します。  
**Contrast.Net.Azure.AppService** パッケージを検索して選択し、プロジェクトに追加します。  
アプリケーションをビルドします。Contrast アセンブリ(例えば、`ContrastProfiler.dll`) が、アプリケーションのルートディレクトリに新規に作成された `contrastsecurity` フォルダにあることを確認します。
2. Contrast サーバに対するアプリケーションの認証情報を追加します。  
認証情報の設定は、Visual Studio の「Azure App Service に公開する」の App Service 設定画面から追加するか、Azure App Service ポータルから直接追加できます。  
エージェントが Contrast に接続するために必要な Contrast 認証キーを設定し、**保存** を選択します。  
プロファイル画面で [キーを見つける \(37ページ\)](#) ことができます。
3. dotnet ソースコードリポジトリ のビルドプロセスに従います。
4. Azure Portal でお使いのアプリケーションの **アプリケーション設定** セクションにアクセスします。  
エージェントが Contrast に接続するために必要な Contrast 認証キーを設定し、**保存** を選択します。
5. Visual Studio を使用して、Azure にアプリケーションを公開します。  
アプリケーションがロードされたら、アプリケーションを疎通してから、Contrast を開き、サーバとアプリケーションがアクティブになっていること、および何か脆弱性が表示されていることを確認します。

## Web API および Owin で .NET Framework エージェントをインストール

.NET Framework エージェントは、Open Web Interface for .NET (OWIN) でセルフホストされる Web API アプリケーションの解析をサポートします。Web API は、コマンドラインアプリケーションや Windows サービスとしてデプロイできます。



### 注記

SystemWeb の HttpModule を使用して IIS 統合パイプラインにホストされている Web API アプリケーションや、OWIN ホストでデプロイされている Web API アプリケーションは **サポート対象外** です。

1. [.NET Framework エージェントの Windows インストーラ \(140ページ\)](#)を使用して、.NET Framework エージェントをインストールします。
2. OWIN ホストの Web API をどのようにデプロイするかによって、環境変数を設定します。
  - **コマンドラインアプリケーションとしてデプロイ**：OWIN をセルフホストにするために使用されるコマンドラインアプリケーションを実行する前に、以下の環境変数を設定します。

環境変数	値
COR_ENABLE_PROFILING	1
COR_PROFILER	{EFEB8EE0-6D39-4347-A5FE-4D0C88BC5BC1}
COR_PROFILER_PATH_32	C:\Program Files\Contrast\dotnet\runtimes\win-x86\native\ContrastProfiler.dll
COR_PROFILER_PATH_64	C:\Program Files\Contrast\dotnet\runtimes\win-x64\native\ContrastProfiler.dll



### 注記

COR\_PROFILER\_PATH\_32 / COR\_PROFILER\_PATH\_64 は、.NET Framework エージェントのインストールで選択したインストールディレクトリと一致する必要があります。

- **Windows サービスとしてデプロイ**：

Web API アプリケーションを含むサービスをインストールします。サービスの名前を確認します。

サービスのレジストリキーの下に、Environment という名前の REG\_MULTI\_SZ 値を作成します。既に Environment 値がある場合は、既存の値の下に新しい値を追加します。

必要な環境変数を設定します。各環境変数はキーと値をペアにして、それぞれ改行してください。各サービスに固有の環境変数は、そのサービスのレジストリキーの下に設定できます。サービスのレジストリキーは次の場所にあります：

HKLM\SYSTEM\CurrentControlSet\Services\YourServiceName

環境変数	値
COR_ENABLE_PROFILING	1
COR_PROFILER	{EFEB8EE0-6D39-4347-A5FE-4D0C88BC5BC1}
COR_PROFILER_PATH_32	C:\Program Files\Contrast\dotnet\runtimes\win-x86\native\ContrastProfiler.dll
COR_PROFILER_PATH_64	C:\Program Files\Contrast\dotnet\runtimes\win-x64\native\ContrastProfiler.dll
CONTRAST_CONFIG_PATH	C:\ProgramData\contrast\dotnet\contrast_security.yaml



### 注記

COR\_PROFILER\_PATH\_32 / COR\_PROFILER\_PATH\_64 は、.NET Framework エージェントのインストールで選択したインストールディレクトリと一致する必要があります。

3. サービスを再起動して、新しい値をロードします。必要な環境変数を設定するために、以下の PowerShell スクリプトを使用できます。

```
param (
    # Name of the service that it was given at installation.
    [Parameter(Mandatory=$true)]
    [string]
    $ServiceName,
```

```
# Path to the 64-bit Contrast profiler DLL.
# Defaults to: "C:\Program Files\Contrast\dotnet\runtimes\win-
x64\native\ContrastProfiler.dll"
[string]
$ProfilerPath64 = "C:\Program Files\Contrast\dotnet\runtimes\win-
x64\native\ContrastProfiler.dll",

# Path to the 32-bit Contrast profiler DLL.
# Defaults to: "C:\Program Files\Contrast\dotnet\runtimes\win-
x86\native\ContrastProfiler.dll"
[string]
$ProfilerPath32 = "C:\Program Files\Contrast\dotnet\runtimes\win-
x86\native\ContrastProfiler.dll",

# Path to the Contrast agent configuration YAML file.
# Defaults \
to: "C:\ProgramData\contrast\dotnet\contrast_security.yaml"
[string]
$ConfigYamlPath \
= "C:\ProgramData\contrast\dotnet\contrast_security.yaml"
)

if (-Not (Test-Path -Path $ProfilerPath64 -PathType Leaf)) {
    Write-Host "Cannot find 64-bit profiler DLL at path \
`"$ProfilerPath64`"."
    exit 1
}

if (-Not (Test-Path -Path $ConfigYamlPath -PathType Leaf)) {
    Write-Host "Cannot find configuration YAML file at path \
`"$ConfigYamlPath`"."
    exit 1
}

if (-Not (Test-Path -Path $ProfilerPath32 -PathType Leaf)) {
    Write-Host "Cannot find 32-bit profiler DLL at path \
`"$ProfilerPath32`"."
    exit 1
}

# Check if there is a service with the specified name installed.
$service = Get-Service -Name $ServiceName -ErrorAction Ignore

if ($null -Eq $service) {
    Write-Host "The service `"$ServiceName`" was not found."
    exit 2
}

# Create value for multiline registry string.
$values = @(
    "COR_ENABLE_PROFILING=1",
    "COR_PROFILER={EFEB8EE0-6D39-4347-A5FE-4D0C88BC5BC1}",
    "COR_PROFILER_PATH_64=$ProfilerPath64",
    "COR_PROFILER_PATH_32=$ProfilerPath32",
    "CONTRAST_CONFIG_PATH=$ConfigYamlPath"
)
```

```
)

$registryKey = "HKLM:\SYSTEM\CurrentControlSet\Services\$ServiceName"

# Check if the Environment value already exists.
$environmentValue = Get-ItemProperty -Path $registryKey -
Name "Environment" -ErrorAction Ignore

if ($null -Ne $environmentValue) {
    # Add the Contrast environment variables to the existing variables.
    $existingValues = \
[System.Collections.ArrayList]@($environmentValue.Environment)
    foreach ($item in $values) {
        $idx = $existingValues.Add($item)
    }
    $values = $existingValues
}

# Set the environment variables for the service.
Set-ItemProperty -Path $registryKey -Type MultiString -
Name "Environment" -Value $values

# Restart the service so it picks up the new environment variables.
Restart-Service -Name $ServiceName
```

## エージェントアップグレードサービス

エージェントアップグレードサービスは、Windows のバックグラウンドサービスで、Windows 上の .NET Framework エージェントおよび IIS 用 .NET Core エージェントを最新のバージョンに自動的に更新することができます。エージェントアップグレードサービスは、.NET Framework エージェントのインストーラと IIS 用 .NET Core エージェントのインストーラに含まれており、エージェントインストーラは以下の 2 つの製品をインストールします。

- 該当のエージェント
- エージェントアップグレードサービス

デフォルトでは、エージェントアップグレードサービスは、サービスの初回起動時 (Windows Server の再起動時) に、NuGet にリリースされている新しいエージェントをチェックします。新しいエージェントのバージョンが見つかった場合、アップグレードサービスは、新しいバージョンをダウンロードし、インストーラの署名を検証してから、最後にインストーラを実行します。

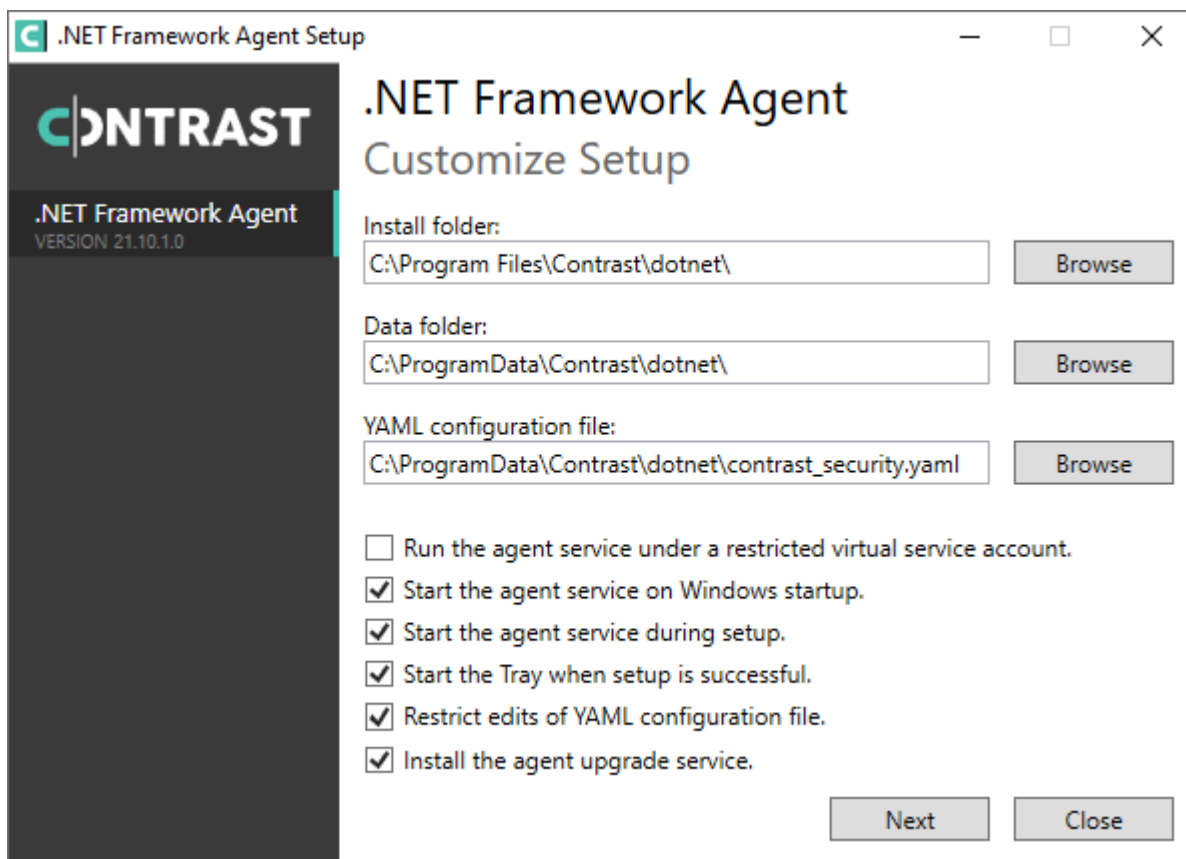


### 注記

新しいバージョンのエージェントがインストールされると、IIS は再起動されます。

エージェントアップグレードサービスはオプションコンポーネントであり、エージェントの Assess および Protect 機能には必須ではありません。

- エージェントアップグレードサービスを使用しない場合は、**Install the agent upgrade service** (エージェントアップグレードサービスをインストールする) のチェックボックスをオフにしてください。
- コマンドラインでエージェントをインストールする場合は、`INSTALL_UPGRADE_SERVICE=0` の引数を追加すれば、エージェントアップグレードサービスはインストールされません。



エージェントアップグレードサービスの動作は、Contrast のデータディレクトリにあるエージェント用の設定ファイルで変更できます。デフォルトの場所は、C:\ProgramData\Contrast\upgrade-service です。

.NET Core エージェントをアップグレードする際の設定は、.NET Core エージェントの YAML ファイル内にあります。

```
enable: true # Set to `true` for the agent to automatically upgrade to \
newer versions.
checks: Startup # Set the frequency with which the agent checks for \
updates. Valid values are `daily` for every 24 hours and on startup, or \
`startup` for *only* when service starts up.
timeout_ms: 60000 # Set the time allocated to execute the downloaded agent \
installer before cancelling.
nuget_repository_url: https://api.nuget.org/v3/index.json # Set the URL of \
the Nuget repository to be used for the .NET Core Agent for IIS Installer
nuget_package_name: Contrast.CoreIIS.Installer # Set the name of the .NET \
Core Agent for IIS Nuget package.
installer_upgrade_code: 82468c04-dfc0-4a4c-9eb9-c4b314c67fdc # Used \
internally to retrieve the current installed agent version from Windows.
```



### 注記

エージェントアップグレードサービスは、エージェントインストーラにのみ含まれます。手動で取得する.NET Core エージェント、エージェントの NuGet パッケージ、Azure App Service のサイト拡張機能には含まれません。

## .NET Framework エージェントのアップデート

.NET Framework エージェントには、新旧 2 つのバージョンがあります。エージェントを最新に保つ方法は、新旧どちらのエージェントを使用しているかによって異なります。

.NET Framework をアップデートするには、3 つの方法があります。

- 自動的にエージェントを更新
- JFrog リポジトリからエージェントをダウンロード(旧エージェントのみ)
- Contrast API を使用してコマンドでダウンロードとインストール

### 開始する前に

- .NET Framework アプリケーションが、Contrast の .NET Framework エージェントなしで正常に動作することを確認してください。
- Contrast の .NET Framework エージェントを正常にインストールしたことがあること。
- 変更管理ポリシーと使用する環境に基づいて、エージェントをアップデートする方法とタイミングを決めておくこと。
- PowerShell を含む Windows スクリプトにある程度の知識があること。

### エージェントを自動更新(新エージェント)

最新のエージェントは、[エージェントアップグレードサービス \(150ページ\)](#)によって自動的に更新されます。対象のエージェントは、バージョン 20.5.1 以降です。ただし、[サポートされていない環境 \(137ページ\)](#)の場合、自動更新はされません。

### JFrog リポジトリからエージェントをダウンロード(旧エージェント)

旧エージェントを使用し続ける必要がある場合は、JFrog Artifactory からエージェントをダウンロードします。旧エージェントは自動的に更新されないため、手動で更新する必要があります。

1. 新しいバージョンを[ダウンロード](#)します。
2. コマンドラインからサイレントインストールを使用して更新します。

```
ContrastSetup.exe -s -norestart
```

### Contrast API によるエージェントのダウンロード(新エージェント)

1. Contrast API から直接 Contrast エージェントをダウンロードします。これは、Contrast の SaaS 版とオンプレミス版の両方で有効な方法です。  
Contrast API にアクセスする(サービスまたはユーザ)ためのアカウントが必要です。
2. エージェントのダウンロード後、コマンドラインからサイレントインストールを行います。  
アカウントの資格情報は、[組織のキーと個人のキーの確認 \(478ページ\)](#)で参照できます。

### 関連項目

- [エージェントアップグレードサービス \(150ページ\)](#)

### .NET Framework エージェントを設定する

エージェントには[基本の設定 \(35ページ\)](#)があり、設定値には[優先順位 \(36ページ\)](#)があります。

.NET Framework エージェントを設定します：

- [Azure App Service で設定する場合 \(153ページ\)](#)
- [web.config ファイルで設定する場合 \(153ページ\)](#)
- [YAML テンプレートを使用する場合 \(154ページ\)](#)





## ヒント

エージェント設定エディタ (39ページ)を使用すると、YAML 設定ファイルの作成やアップロード、YAML の検証、推奨される設定値の表示などができます。

## Azure App Service での .NET Framework エージェントの設定

Azure Portal で Azure App Service の .NET Framework エージェントを設定するには、3 つの方法があります。

- Contrast エージェントの環境変数の表記規則を使用します。Azure Portal の構成画面よりアプリケーション設定セクションに、エージェントの環境変数の構文 (56ページ)を使用して全ての設定を追加します。
- アプリケーションの web.config ファイルに、application という設定オプションを指定します。web.config に指定したアプリケーションの設定を Contrast エージェントに認識させるためには、これらの設定をアプリケーションの web.config ファイルのルートの appSettings セクション内に記述する必要があります。詳細は、web.config ファイルで設定 (153ページ)を参照してください。
- Azure Portal で個々のオプションを設定する代わりに、Contrast の設定を含む YAML 設定ファイルを使用することもできます。まず、ファイルをアプリケーションのデプロイメントに含めるか、Kudu コンソールを使用して、Azure Web アプリケーションにこのファイルをアップロードします。次に、このファイルの場所を指す設定である CONTRAST\_CONFIG\_PATH を追加します。  
例えば、アプリケーションのルートにある contrast\_security.yaml ファイルを使用する場合は、CONTRAST\_CONFIG\_PATH というキーに D:\Home\site\wwwroot\contrast\_security.yaml という値で、アプリケーションの設定を追加します。Azure App Service のアプリケーションファイルは、D:\home\site\wwwroot にデプロイされます。

## .NET Framework エージェントを web.config ファイルで設定

エージェントの設定オプションは、アプリケーションの web.config ファイルまたは YAML 設定ファイルを使用して指定できます。web.config に指定したアプリケーションの設定を Contrast エージェントに認識させるためには、これらの設定をアプリケーション web.config ファイルのルート<configuration>の appSettings セクション内に記述する必要があります。

例えば、同じアプリケーションプールにホストされている 2 つのアプリケーションは、各アプリケーションの web.config ファイルで appSettings に contrast.server.name プロパティを設定すると異なるサーバとして報告されます。また、web.config を使用して次のように contrast.application.name を指定することもできます。

```
<configuration>
  <appSettings>
    <add key="contrast.application.name" value="MyWebAppName" />
    <add key="contrast.application.version" value="1.2.3" />
  </appSettings>
  <system.web>
    ...
```

その他の利用可能なプロパティの説明は、.NET Framework エージェントの YAML テンプレート (154ページ)を参照してください。

エージェントのバージョンが 21.1.4 より前の場合、web.config で設定できるのは、以下のように一部のプロパティのみとなります。

プロパティ	導入された .NET Framework エージェントのバージョン
contrast.application.code	19.6.3
contrast.application.group	19.1.3

プロパティ	導入された.NET Framework エージェントのバージョン
contrast.application.metadata	19.1.3
contrast.application.name	19.1.3
contrast.application.session_id	20.6.6
contrast.application.session_metadata	20.6.6
contrast.application.tags	19.1.3
contrast.application.version	19.1.3
contrast.assess.tags	19.1.3
contrast.inventory.tags	19.1.3



## 注記

`contrast.application.name` が指定されていない場合、.NET Framework エージェントは、アプリケーションの仮想パスをアプリケーション名として使用します。アプリケーションがサイトのルートでホストされている場合(つまり、仮想パスが/の場合)、.NET Framework エージェントはこのサイトの名前をアプリケーション名として使用します。



## 重要

エージェントのバージョン 21.1.4 以降、ほとんどのエージェントの設定が、アプリケーションの `web.config` ファイル、またはアプリケーションと同じディレクトリにある `contrast_security.yaml` で指定できるようになりました。例えば、同じアプリケーションプールにホストされている 2 つのアプリケーションは、各アプリケーションの `web.config` ファイルの `appSettings` に `contrast.server.name` を設定すると異なるサーバとして報告されます。

以下の設定オプションは、*process* レベルで適用され、アプリケーションごとに個別に指定できません。これらのプロパティは、*web.config* を使用して設定できません。別の方法(YAML など)で設定する必要があります。

- `agent.dotnet.app_pool_denylist`
- `agent.dotnet.app_pool_allowlist`
- `agent.dotnet.enable_instrumentation_optimizations`
- `agent.dotnet.enable_jit_inlining`
- `agent.dotnet.enable_transparency_checks`
- `agent.dotnet.enable_struct_dataflow`
- `assess.enable_control_detection`

また、以下のキーについては、エージェントのプロファイラコンポーネントはプロセスレベルの設定を使用し、エージェントのセンサーコンポーネントはアプリケーション個別の設定(指定されている場合)を使用します。

- `agent.logger.level`
- `agent.logger.stdout`

## .NET Framework エージェントの YAML テンプレート

[YAML 設定 \(38ページ\)](#) ファイルを使用して、.NET Framework エージェントを設定します。

`contrast_security.yaml` ファイルは、インストーラによってエージェントのデータディレクトリにコピーされます(デフォルトでは、`C:\ProgramData\Contrast\dotnet\contrast_security.yaml`)。コピー先に既に YAML ファイルが存在する場合は、インストーラは YAML ファイルをコピーしません。

以下のテンプレートには、このエージェントで有効な YAML オプションがすべてあります。例えば、このファイルを使用して .NET Framework エージェントによって報告されるサーバ名を設定することができます。その場合、`contrast_security.yaml` ファイルに新しい行として以下のコードを追加してファイルを更新してから、通常通りにインストールを続けます。

```
server:
  name: MyServerName

# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==

# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET
```

```
# Set the version of the TLS protocol the agent uses to communicate with \
the
# Contrast UI. The .NET agent default behavior is \
(SecurityProtocolType.Tls
# | SecurityProtocolType.Tls11 | SecurityProtocolType.Tls12).
# tls_versions: tls|tls11|tls12

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Determine the location from which the agent loads a client
# certificate. Value options include `File` or `Store`.
# certificate_location: NEEDS_TO_BE_SET

# Set the absolute path to the client certificate's
# .CER file for communication with Contrast UI. The
# `certificate_location` property must be set to `File`.
# cer_file: NEEDS_TO_BE_SET

# Specify the name of certificate store to open. The
# `certificate_location` property must be set to `Store`.
# Value options include `AuthRoot`, `CertificateAuthority`,
# `My`, `Root`, `TrustedPeople`, or `TrustedPublisher`.
# store_name: NEEDS_TO_BE_SET

# Specify the location of the certificate store. The
# `certificate_location` property must be set to `Store`.
# Value options include `CurrentUser` or `LocalMachine`.
# store_location: NEEDS_TO_BE_SET

# Specify the type of value the agent uses to find the certificate
# in the collection of certificates from the certificate store.
# The `certificate_location` property must be set to `Store`.
# Value options include `FindByIssuerDistinguishedName`,
# `FindByIssuerName`, `FindBySerialNumber`,
# `FindBySubjectDistinguishedName`, `FindBySubjectKeyIdentifier`,
# `FindBySubjectName`, or `FindByThumbprint`.
# find_type: NEEDS_TO_BE_SET

# Specify the value the agent uses in combination with
# `find_type` to find a certification in the certificate store.
#
# Note - The agent will use the first certificate from
# the certificate store that matches this search criteria.
#
```

```

# find_value: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate
# with the Contrast web interface over a proxy. Set
# value to `false` if you don't want to use the proxy.
# enable: NEEDS_TO_BE_SET

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# Set the proxy user.
# user: NEEDS_TO_BE_SET

# Set the proxy password.
# pass: NEEDS_TO_BE_SET

# Set the proxy authentication type. Value
# options are `NTLM`, `Digest`, and `Basic`.
# auth_type: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

```

```
# Set to `true` to redirect all logs to
# `stdout` instead of the file system.
# stdout: false

# Set the roll size for log files in megabytes. The agent will
# attempt to prevent the log file from being larger than this size.
# roll_size: 100

# Set the number of backup files to keep. Set to `0` to disable.
# backups: 10

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
```

```
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# Set the connection type used for Syslog messages.
# Value options are `UNENCRYPTED` and `ENCRYPTED`.
# connection_type: UNENCRYPTED

# \
=====
# agent.dotnet
# The following properties apply to any .NET agent-wide configurations.
# \
=====
# dotnet:

# Set a list of application pool names that the agent does not
# instrument or analyze. Names must be formatted as a comma-separated
# list. New after .NET Framework 19.1.3 and .NET Core 4.0.2.
# app_pool_denylist: NEEDS_TO_BE_SET

# Set a list of application pool names that the agent instruments or
# analyzes. If set, other application pools are ignored. Allowlist takes
# precedence over denylist. Names must be formatted as a comma-separated
# list. New after .NET Framework 19.1.3 and .NET Core 4.0.2.
# app_pool_allowlist: NEEDS_TO_BE_SET

# Set a list of application names that the agent does not
# analyze. (The applications are still instrumented).
# Names must be formatted as a comma-separated list.
# New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# application_denylist: NEEDS_TO_BE_SET

# Set a list of application names that the agent analyzes.
# If set, other applications are not analyzed, but are
# still instrumented. Allowlist takes precedence over
# denylist. Names must be formatted as a comma-separated
# list. New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# application_allowlist: NEEDS_TO_BE_SET

# Enable a profiler chaining feature to allow Contrast to
# work alongside other tools that use the CLR Profiling
# API. Defaults to `true`. New after .NET Framework 19.1.3
```

```
# (Installed Only) and .NET Core 1.9.3 (Installed Only).
# enable_chaining: true

# Indicate that the agent should produce a report that
# summarizes application hosting on the server (e.g.,
# CLR versions, bitness or pipeline modes). Defaults to
# `true`. New after .NET Framework 19.1.3 (Installed Only).
# enable_dvnr: true

# Indicate that the agent should allow CLR optimizations
# of JIT-compiled methods. Defaults to `true`. New
# after .NET Framework 19.1.3 and .NET Core 1.0.0.
# enable_instrumentation_optimizations: true

# Indicate that the agent should allow the CLR to inline
# methods that are not instrumented by Contrast. Defaults to
# `true`. New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# enable_jit_inlining: true

# Indicate that the agent should allow the CLR to perform
# transparency checks under full trust. Defaults to `false`.
# New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# enable_transparency_checks: false

# Responses for request paths (e.g., HttpRequest.Path)
# that match this regex are not analyzed. Defaults to
# `WebResource.axd`. New after .NET Framework 19.1.3.
# web_module_allowlist: WebResource.axd

# Set to display ASCII art to std::out on agent startup. Defaults
# to `true`. New after .NET Framework 20.6.3 and .NET Core 1.0.0.
# enable_cat: true

# Sets the maximum amount of time a Protect regular expression
# is allowed to run before being cancelled. Set to -1 to never
# cancel regular expression execution. Defaults to `20_000`.
# New after .NET Framework 20.4.3 and .NET Core 1.5.0.
# protect_searchers_single_pattern_deadline_ms: 20_000

# Sets the maximum amount of time a 'Probe Analysis' Protect
# regular expression is allowed to run before being cancelled. Set
# to -1 to never cancel regular expression execution. Defaults to
# `5_000`. New after .NET Framework 20.7.3 and .NET Core 1.5.11.
# protect_searchers_probe_analysis_single_pattern_deadline_ms: 5_000

# Sets the maximum amount of time a Protect rule is
# allowed to run before being cancelled. Set to -1 to never
# cancel Protect rule execution. Defaults to `60_000`.
# New after .NET Framework 20.4.3 and .NET Core 1.5.0.
# protect_searchers_total_rule_deadline_ms: 60_000

# Sets the maximum amount of time a 'Probe Analysis' Protect
# rule is allowed to run before being cancelled. Set to -1 to
# never cancel Protect rule execution. Defaults to `10_000`.
# New after .NET Framework 20.7.3 and .NET Core 1.5.11.
```



```

# protect_searchers_probe_analysis_total_rule_deadline_ms: 10_000

# Sets the maximum duration of time agent log files should be kept
# since last write before being deleted by the agent. Defaults to
# `604_800_000`. New after .NET Framework 20.6.1 and .NET Core 1.5.5.
# log_cleanup_maximum_age_ms: 604_800_000

# Suppresses gathering process-level metrics (process level metrics are
# gathered by default), used to identify performance problems. Metric
# counters may further decrease the stability of already unstable
# systems and can be disabled (set to true) if issues occur. Defaults
# to `false`. New after .NET Framework 20.6.6 and .NET Core 1.5.10.
# suppress_metric_counters: false

# Enable file based application watching. Set to false if
# file watching is causing locking issues. Defaults to `true`.
# New after .NET Framework 20.7.3 and .NET Core 1.5.11.
# enable_file_based_app_watching: true

# Enables HttpClient isolation using AppDomain remoting. This can be \
used
# to workaround .NET TLS version limitations at the cost of performance
# and stability. Enabled by default on applications targeting .NET
# Framework < 4.7.0, else disabled. New after .NET Framework 21.5.1.
# enable_http_client_app_domain_isolation: false

# Enables LINQ optimizations to improve performance
# at the cost of possible false negatives. Defaults
# to `true`. New after .NET Framework 50.0.1.
# enable_linq_optimizations: true

# \
=====
# agent.dotnet.file_analysis_time_ms
# Controls the interval in milliseconds to perform file
# analysis for supported rules. Setting a value > 0 will
# result in the job running at that interval and not just when
# the application loads. If set to `-1`, the job just runs
# once. Defaults to `-1`. New after .NET Framework 50.0.15.
# \
=====
# file_analysis_time_ms: {}

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

```

```
# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Control the values captured by Assess vulnerability events. `Full`
# captures most values by calling ToString on objects, which can
# provide more info but causes increased memory usage. `Minimal`
# has better performance as it only captures String type objects
# as strings and uses type name for other object type values.
# event_detail: minimal

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Value options are `ALL`, `SOME`, or `NONE`.
# stacktraces: ALL

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
```

```

# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
# protect.rules
# Use the following properties to set simple rule configurations.
# \
=====
# rules:

# Define a list of Protect rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
# protect.rules.bot-blocker
# Use the following selection to configure if the
# agent blocks bots. Set to `true` to enable blocking.
# \
=====

```

```

# bot-blocker:

# Set to `true` for the agent to block known bots.
# enable: false

# \
=====
# protect.rules.sql-injection
# Use the following settings to configure the sql-injection rule.
# \
=====
# sql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.sql-injection-semantic-chaining
# Use the following properties to configure how the
# sql injection semantic analysis chaining rule works.
# \
=====
# sql-injection-semantic-chaining:

# Set the mode of the rule. Value options
# are `monitor`, `block` or `off`.
# mode: off

# \
=====
# protect.rules.sql-injection-semantic-dangerous-functions
# Use the following properties to configure how the sql
# injection semantic analysis dangerous functions rule works.
# \
=====
# sql-injection-semantic-dangerous-functions:

# Set the mode of the rule. Value options
# are `monitor`, `block` or `off`.
# mode: off

# \
=====
# protect.rules.sql-injection-semantic-suspicious-unions
# Use the following properties to configure how the sql
# injection semantic analysis suspicious unions rule works.
# \
=====
# sql-injection-semantic-suspicious-unions:

```

```

# Set the mode of the rule. Value options
# are `monitor`, `block` or `off`.
# mode: off

# \
=====
# protect.rules.sql-injection-semantic-tautologies
# Use the following properties to configure how the sql
# injection semantic analysis tautologies rule works.
# \
=====
# sql-injection-semantic-tautologies:

# Set the mode of the rule. Value options
# are `monitor`, `block` or `off`.
# mode: off

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Tell the agent to detect when commands come directly
# from input. The agent blocks if blocking is enabled.
# detect_phased_commands: true

# \
=====
# protect.rules.cmd-injection-semantic-chained-commands
# Use the following properties to configure how the
# 'command injection - chained commands' rule works
# \
=====
# cmd-injection-semantic-chained-commands:

# Set the mode of the rule. Value options
# are `monitor`, `block`, or `off`.
# mode: off

# \
=====
# protect.rules.cmd-injection-semantic-dangerous-paths

```

```

# Use the following properties to configure how the
# 'command injection - dangerous paths' rule works
# \
=====
# cmd-injection-semantic-dangerous-paths:

# Set the mode of the rule. Value options
# are `monitor`, `block`, or `off`.
# mode: off

# \
=====
# protect.rules.cmd-injection-command-backdoors
# Use the following properties to configure how the
# 'command injection - command backdoors' rule works
# \
=====
# cmd-injection-command-backdoors:

# Set the mode of the rule. Value options
# are `monitor`, `block`, or `off`.
# mode: off

# \
=====
# protect.rules.path-traversal-semantic-file-security-bypass
# Use the following properties to configure how the
# 'path traversal - file security bypass' rule works
# \
=====
# path-traversal-semantic-file-security-bypass:

# Set the mode of the rule. Value options
# are `monitor`, `block`, or `off`.
# mode: off

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====

```

```
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.unsafe-file-upload
# Use the following properties to configure
# how the unsafe file upload rule works.
# \
=====
# unsafe-file-upload:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
```

```

=====
# xxe:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====

# protect.rules.untrusted-deserialization
# Use the following properties to configure
# how the untrusted deserialization rule works.
# \
=====

# untrusted-deserialization:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

```



```
# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
```

```

#
# tags: NEEDS_TO_BE_SET

# Override the reported server path. New after
# .NET Framework v21.3.1 and .NET Core v1.8.0.
# path: NEEDS_TO_BE_SET

# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==

# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# Set the version of the TLS protocol the agent uses to communicate with \
the
# Contrast UI. The .NET agent default behavior is \
(SecurityProtocolType.Tls

```

```
# | SecurityProtocolType.Tls11 | SecurityProtocolType.Tls12).
# tls_versions: tls|tls11|tls12

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Determine the location from which the agent loads a client
# certificate. Value options include `File` or `Store`.
# certificate_location: NEEDS_TO_BE_SET

# Set the absolute path to the client certificate's
# .CER file for communication with Contrast UI. The
# `certificate_location` property must be set to `File`.
# cer_file: NEEDS_TO_BE_SET

# Specify the name of certificate store to open. The
# `certificate_location` property must be set to `Store`.
# Value options include `AuthRoot`, `CertificateAuthority`,
# `My`, `Root`, `TrustedPeople`, or `TrustedPublisher`.
# store_name: NEEDS_TO_BE_SET

# Specify the location of the certificate store. The
# `certificate_location` property must be set to `Store`.
# Value options include `CurrentUser` or `LocalMachine`.
# store_location: NEEDS_TO_BE_SET

# Specify the type of value the agent uses to find the certificate
# in the collection of certificates from the certificate store.
# The `certificate_location` property must be set to `Store`.
# Value options include `FindByIssuerDistinguishedName`,
# `FindByIssuerName`, `FindBySerialNumber`,
# `FindBySubjectDistinguishedName`, `FindBySubjectKeyIdentifier`,
# `FindBySubjectName`, or `FindByThumbprint`.
# find_type: NEEDS_TO_BE_SET

# Specify the value the agent uses in combination with
# `find_type` to find a certification in the certificate store.
#
# Note - The agent will use the first certificate from
# the certificate store that matches this search criteria.
#
# find_value: NEEDS_TO_BE_SET

# \
=====
```

```
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate
# with the Contrast web interface over a proxy. Set
# value to `false` if you don't want to use the proxy.
# enable: NEEDS_TO_BE_SET

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# Set the proxy user.
# user: NEEDS_TO_BE_SET

# Set the proxy password.
# pass: NEEDS_TO_BE_SET

# Set the proxy authentication type. Value
# options are `NTLM`, `Digest`, and `Basic`.
# auth_type: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Set to `true` to redirect all logs to
# `stdout` instead of the file system.
# stdout: false
```

```
# Set the roll size for log files in megabytes. The agent will
# attempt to prevent the log file from being larger than this size.
# roll_size: 100

# Set the number of backup files to keep. Set to `0` to disable.
# backups: 10

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
```

```
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# Set the connection type used for Syslog messages.
# Value options are `UNENCRYPTED` and `ENCRYPTED`.
# connection_type: UNENCRYPTED

# \
=====
# agent.dotnet
# The following properties apply to any .NET agent-wide configurations.
# \
=====
# dotnet:

# Set a list of application pool names that the agent does not
# instrument or analyze. Names must be formatted as a comma-separated
# list. New after .NET Framework 19.1.3 and .NET Core 4.0.2.
# app_pool_denylist: NEEDS_TO_BE_SET

# Set a list of application pool names that the agent instruments or
# analyzes. If set, other application pools are ignored. Allowlist takes
# precedence over denylist. Names must be formatted as a comma-separated
# list. New after .NET Framework 19.1.3 and .NET Core 4.0.2.
# app_pool_allowlist: NEEDS_TO_BE_SET

# Set a list of application names that the agent does not
# analyze. (The applications are still instrumented).
# Names must be formatted as a comma-separated list.
# New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# application_denylist: NEEDS_TO_BE_SET

# Set a list of application names that the agent analyzes.
# If set, other applications are not analyzed, but are
# still instrumented. Allowlist takes precedence over
# denylist. Names must be formatted as a comma-separated
# list. New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# application_allowlist: NEEDS_TO_BE_SET

# Enable a profiler chaining feature to allow Contrast to
# work alongside other tools that use the CLR Profiling
# API. Defaults to `true`. New after .NET Framework 19.1.3
# (Installed Only) and .NET Core 1.9.3 (Installed Only).
# enable_chaining: true

# Indicate that the agent should produce a report that
```

```
# summarizes application hosting on the server (e.g.,
# CLR versions, bitness or pipeline modes). Defaults to
# `true`. New after .NET Framework 19.1.3 (Installed Only).
# enable_dvnr: true

# Indicate that the agent should allow CLR optimizations
# of JIT-compiled methods. Defaults to `true`. New
# after .NET Framework 19.1.3 and .NET Core 1.0.0.
# enable_instrumentation_optimizations: true

# Indicate that the agent should allow the CLR to inline
# methods that are not instrumented by Contrast. Defaults to
# `true`. New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# enable_jit_inlining: true

# Indicate that the agent should allow the CLR to perform
# transparency checks under full trust. Defaults to `false`.
# New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# enable_transparency_checks: false

# Responses for request paths (e.g., HttpRequest.Path)
# that match this regex are not analyzed. Defaults to
# `WebResource.axd`. New after .NET Framework 19.1.3.
# web_module_allowlist: WebResource.axd

# Set to display ASCII art to std::out on agent startup. Defaults
# to `true`. New after .NET Framework 20.6.3 and .NET Core 1.0.0.
# enable_cat: true

# Sets the maximum amount of time a Protect regular expression
# is allowed to run before being cancelled. Set to -1 to never
# cancel regular expression execution. Defaults to `20_000`.
# New after .NET Framework 20.4.3 and .NET Core 1.5.0.
# protect_searchers_single_pattern_deadline_ms: 20_000

# Sets the maximum amount of time a 'Probe Analysis' Protect
# regular expression is allowed to run before being cancelled. Set
# to -1 to never cancel regular expression execution. Defaults to
# `5_000`. New after .NET Framework 20.7.3 and .NET Core 1.5.11.
# protect_searchers_probe_analysis_single_pattern_deadline_ms: 5_000

# Sets the maximum amount of time a Protect rule is
# allowed to run before being cancelled. Set to -1 to never
# cancel Protect rule execution. Defaults to `60_000`.
# New after .NET Framework 20.4.3 and .NET Core 1.5.0.
# protect_searchers_total_rule_deadline_ms: 60_000

# Sets the maximum amount of time a 'Probe Analysis' Protect
# rule is allowed to run before being cancelled. Set to -1 to
# never cancel Protect rule execution. Defaults to `10_000`.
# New after .NET Framework 20.7.3 and .NET Core 1.5.11.
# protect_searchers_probe_analysis_total_rule_deadline_ms: 10_000

# Sets the maximum duration of time agent log files should be kept
# since last write before being deleted by the agent. Defaults to
```

```
# `604_800_000`. New after .NET Framework 20.6.1 and .NET Core 1.5.5.
# log_cleanup_maximum_age_ms: 604_800_000

# Suppresses gathering process-level metrics (process level metrics are
# gathered by default), used to identify performance problems. Metric
# counters may further decrease the stability of already unstable
# systems and can be disabled (set to true) if issues occur. Defaults
# to `false`. New after .NET Framework 20.6.6 and .NET Core 1.5.10.
# suppress_metric_counters: false

# Enable file based application watching. Set to false if
# file watching is causing locking issues. Defaults to `true`.
# New after .NET Framework 20.7.3 and .NET Core 1.5.11.
# enable_file_based_app_watching: true

# Enables HttpClient isolation using AppDomain remoting. This can be \
used
# to workaround .NET TLS version limitations at the cost of performance
# and stability. Enabled by default on applications targeting .NET
# Framework < 4.7.0, else disabled. New after .NET Framework 21.5.1.
# enable_http_client_app_domain_isolation: false

# Enables LINQ optimizations to improve performance
# at the cost of possible false negatives. Defaults
# to `true`. New after .NET Framework 50.0.1.
# enable_linq_optimizations: true

# \
=====
# agent.dotnet.file_analysis_time_ms
# Controls the interval in milliseconds to perform file
# analysis for supported rules. Setting a value > 0 will
# result in the job running at that interval and not just when
# the application loads. If set to `-1`, the job just runs
# once. Defaults to `-1`. New after .NET Framework 50.0.15.
# \
=====
# file_analysis_time_ms: {}

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
```



```
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Control the values captured by Assess vulnerability events. `Full`
# captures most values by calling ToString on objects, which can
# provide more info but causes increased memory usage. `Minimal`
# has better performance as it only captures String type objects
# as strings and uses type name for other object type values.
# event_detail: minimal

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Value options are `ALL`, `SOME`, or `NONE`.
# stacktraces: ALL

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000
```

```
# \  
=====
```

```
# assess.rules  
# Use the following properties to control simple rule configurations.  
# \  
=====
```

```
# rules:  
  
# Define a list of Assess rules to disable in the agent.  
# The rules must be formatted as a comma-delimited list.  
#  
# Example - Set `reflected-xss,sql-injection` to disable  
# the reflected-xss rule and the sql-injection rule.  
#  
# disabled_rules: NEEDS_TO_BE_SET
```

```
# \  
=====
```

```
==  
# protect  
# Use the properties in this section to override Protect features.  
# \  
=====
```

```
==  
# protect:  
  
# Use the properties in this section to determine if the  
# Protect feature should be enabled. If this property is not  
# present, the decision is delegated to the Contrast UI.  
# enable: false
```

```
# \  
=====
```

```
# protect.rules  
# Use the following properties to set simple rule configurations.  
# \  
=====
```

```
# rules:  
  
# Define a list of Protect rules to disable in the agent.  
# The rules must be formatted as a comma-delimited list.  
# disabled_rules: NEEDS_TO_BE_SET
```

```
# \  
=====
```

```
# protect.rules.bot-blocker  
# Use the following selection to configure if the  
# agent blocks bots. Set to `true` to enable blocking.  
# \  
=====
```

```
# bot-blocker:  
  
# Set to `true` for the agent to block known bots.  
# enable: false
```

```
# \  
=====
```

```
# protect.rules.sql-injection  
# Use the following settings to configure the sql-injection rule.  
# \  
=====
```

```
# sql-injection:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or off.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====
```

```
# protect.rules.sql-injection-semantic-chaining  
# Use the following properties to configure how the  
# sql injection semantic analysis chaining rule works.  
# \  
=====
```

```
# sql-injection-semantic-chaining:  
  
# Set the mode of the rule. Value options  
# are `monitor`, `block` or `off`.  
# mode: off  
  
# \  
=====
```

```
# protect.rules.sql-injection-semantic-dangerous-functions  
# Use the following properties to configure how the sql  
# injection semantic analysis dangerous functions rule works.  
# \  
=====
```

```
# sql-injection-semantic-dangerous-functions:  
  
# Set the mode of the rule. Value options  
# are `monitor`, `block` or `off`.  
# mode: off  
  
# \  
=====
```

```
# protect.rules.sql-injection-semantic-suspicious-unions  
# Use the following properties to configure how the sql  
# injection semantic analysis suspicious unions rule works.  
# \  
=====
```

```
# sql-injection-semantic-suspicious-unions:  
  
# Set the mode of the rule. Value options  
# are `monitor`, `block` or `off`.  
# mode: off
```

```
# \  
=====\  
# protect.rules.sql-injection-semantic-tautologies  
# Use the following properties to configure how the sql  
# injection semantic analysis tautologies rule works.  
# \  
=====\  
# sql-injection-semantic-tautologies:  
  
# Set the mode of the rule. Value options  
# are `monitor`, `block` or `off`.  
# mode: off  
  
# \  
=====\  
# protect.rules.cmd-injection  
# Use the following properties to configure  
# how the command injection rule works.  
# \  
=====\  
# cmd-injection:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# Tell the agent to detect when commands come directly  
# from input. The agent blocks if blocking is enabled.  
# detect_phased_commands: true  
  
# \  
=====\  
# protect.rules.cmd-injection-semantic-chained-commands  
# Use the following properties to configure how the  
# 'command injection - chained commands' rule works  
# \  
=====\  
# cmd-injection-semantic-chained-commands:  
  
# Set the mode of the rule. Value options  
# are `monitor`, `block`, or `off`.  
# mode: off  
  
# \  
=====\  
# protect.rules.cmd-injection-semantic-dangerous-paths  
# Use the following properties to configure how the  
# 'command injection - dangerous paths' rule works  
# \  
=====
```

```

# cmd-injection-semantic-dangerous-paths:

# Set the mode of the rule. Value options
# are `monitor`, `block`, or `off`.
# mode: off

# \
=====
# protect.rules.cmd-injection-command-backdoors
# Use the following properties to configure how the
# 'command injection - command backdoors' rule works
# \
=====
# cmd-injection-command-backdoors:

# Set the mode of the rule. Value options
# are `monitor`, `block`, or `off`.
# mode: off

# \
=====
# protect.rules.path-traversal-semantic-file-security-bypass
# Use the following properties to configure how the
# 'path traversal - file security bypass' rule works
# \
=====
# path-traversal-semantic-file-security-bypass:

# Set the mode of the rule. Value options
# are `monitor`, `block`, or `off`.
# mode: off

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \

```

```

=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.unsafe-file-upload
# Use the following properties to configure
# how the unsafe file upload rule works.
# \
=====
# unsafe-file-upload:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are

```

```

# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.untrusted-deserialization
# Use the following properties to configure
# how the untrusted deserialization rule works.
# \
=====
# untrusted-deserialization:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must

```

```

# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Override the reported server path. New after

```



```
# .NET Framework v21.3.1 and .NET Core v1.8.0.  
# path: NEEDS_TO_BE_SET
```

## 証明書の例外について

証明書の例外が発生していて、無視しても問題ないと思われる場合は、YAML 設定ファイルに次の設定を追加します。

```
api:  
  certificate:  
    ignore_cert_errors: true
```

[サポートポータルの記事](#)にて、証明書の問題に対処するための詳細を参照できます。

## IIS Express で .NET Framework エージェントを使用 する

.NET エージェントは、IIS Express でホストされる ASP.NET アプリケーションを解析できますが、IIS Express でエージェントの組み込みを有効にするには、作業が少々必要です。IIS Express がサーバにインストールされている場合は、Contrast トレイに IIS Express のタブが表示されます。

[Contrast トレイ \(191ページ\)](#)には、IIS Express ホストのアプリケーションでエージェントの組み込みを有効にするための **Set Environment Variables**(環境変数を設定)ボタンが最初に表示されます。このボタンを選択すると、現在のユーザの環境変数が設定され、新しい IIS Express プロセスによって .NET エージェントのプロファイラがロードされ、エージェントの組み込みと解析が行われるようになります。

環境変数を設定すると、トレイに **Remove Environment Variables**(環境変数を削除)ボタンが表示されます。このボタンを使用すると IIS Express ホストのアプリケーションで Contrast の解析を無効にできます。

IIS Express で実行中のアプリケーションでエージェントが組み込まれたものがあれば、観測された URL(querystring なし)の件数とともに IIS Express タブに表示されます。



### 注記

IIS Express のプロセスインスタンスは、通常、Visual Studio やコマンド画面などの他のプログラムから起動されます。上記のユーザ環境変数を設定した後は、これらのプログラムを再起動してください。ユーザ環境変数を設定する前に実行されていたプログラム(Visual Studio など)は、環境変数なしで IIS Express を起動していることとなりますので、その IIS Express でホストされるアプリケーションにはエージェントが組み込まれず解析されません。

また、ユーザ環境変数を設定すると、そのユーザが起動する全ての .NET アプリケーションで Contrast プロファイラがロードされることになります。Contrast プロファイラは、IIS 以外および IIS Express 以外のプロセスから安全にデタッチされます。Windows では、プロファイラ DLL のデタッチが Windows イベントログでエラーメッセージとして処理されますが、このエラーは無視して構いません。

## Azure のアプリケーションで .NET Framework エージェントを使用 する

Contrast .NET Framework エージェントを使用して、Azure Virtual Machines (VM)、Azure Cloud Services、Azure Mobile Services、Azure App Service (旧 Azure Web Sites)で実行される ASP.NET アプリケーションを解析できます。

Azure Virtual Machines で .NET Framework エージェントをインストールするには :

1. 通常どおり Azure VM または Azure Cloud Services をセットアップし、検査対象の ASP.NET アプリケーションをデプロイします。
2. Contrast Web インターフェイスにログインして、.NET Framework エージェントの ZIP ファイルをダウンロードします。
3. [Azure VM](#) または [Azure Cloud Services](#) インスタンスにリモートデスクトップ接続します。
4. .NET Framework エージェントの ZIP ファイルを、Azure VM または Azure Cloud Services インスタンスにコピーし、アーカイブを解凍します。
5. .NET Framework エージェントのインストーラ(*ContrastSetup.exe*)を実行します。
6. アプリケーションを疎通すると、Contrast で解析が行われます。



### ヒント

Azure App Service(旧 Azure Web Apps)でインストールを行う場合は、[NuGet \(147ページ\)](#)か [Azure Portal の拡張機能 \(143ページ\)](#)を使用します。

## Azure Service Fabric で.NET Framework または.NET Core エージェントを使用する

コンテナイメージを使用する場合は、[コンテナにインストール \(145ページ\)](#)する手順に従ってください。そうでない場合は、Azure Service Fabric サービスに Contrast .NET Framework または.NET Core エージェントを追加します。



### ヒント

スタンドアロンの実行サービスの場合、*ServiceManifest.xml* ファイルは最上位の Azure Service Fabric プロジェクト(例、*sfproj* ファイル)にあります。

1. 適切な NuGet パッケージをサービスのメインプロジェクトにインストールします。
  - **.NET Framework の場合**： *Contrast.NET.Azure.AppService* をインストールします。*contrastsecurity* フォルダにあるすべてのファイルは、プロパティがに設定されている必要があります。
  - **.NET Core の場合**： *Contrast.SensorsNetCore* をインストールします。*contrast* フォルダにあるすべてのファイルは、プロパティがに設定されている必要があります。
2. *ServiceManifest.xml* の *ServiceManifest/CodePackage/EntryPoint/ExeHost/WorkingDirectory* を *CodePackage* に設定します。

```
<CodePackage Name="Code" Version="1.0.0">
  <EntryPoint>
    <ExeHost>
      <Program>DemoNetFxStatelessService.exe</Program>
      <WorkingFolder>CodePackage</WorkingFolder>
    </ExeHost>
  </EntryPoint>
</CodePackage>
```

3. *ServiceManifest.xml* で環境変数を定義して、プロファイラを指定します。

- **.NET Framework の場合**：

```
<CodePackage>
  <EnvironmentVariables>
    <EnvironmentVariable Name="COR_ENABLE_PROFILING" \
Value="1"/>
  </EnvironmentVariables>
</CodePackage>
```

```

        <EnvironmentVariable Name="COR_PROFILER" \
Value="{EFEB8EE0-6D39-4347-A5FE-4D0C88BC5BC1}"/>
        <EnvironmentVariable Name="COR_PROFILER_PATH_32" \
Value=". \contrastsecurity\runtimes\win-
x86\native\ContrastProfiler.dll" />
        <EnvironmentVariable Name="COR_PROFILER_PATH_64" \
Value=". \contrastsecurity\runtimes\win-
x64\native\ContrastProfiler.dll" />
        <EnvironmentVariable Name="CONTRAST_CONFIG_PATH" \
Value="contrast_security.yaml"/>
    
```

• **.NET Core の場合 :**

```

<CodePackage>
  <EnvironmentVariables>
    <EnvironmentVariable Name="CORECLR_ENABLE_PROFILING" \
Value="1"/>
    <EnvironmentVariable Name="CORECLR_PROFILER" \
Value="{8B2CE134-0948-48CA-A4B2-80DDAD9F5791}"/>
    <EnvironmentVariable Name="CORECLR_PROFILER_PATH_32" \
Value="contrast\runtimes\win-x86\native\ContrastProfiler.dll"/>
    <EnvironmentVariable Name="CORECLR_PROFILER_PATH_64" \
Value="contrast\runtimes\win-x64\native\ContrastProfiler.dll"/>
    <EnvironmentVariable Name="CONTRAST_CONFIG_PATH" \
Value="contrast_security.yaml"/>
  
```

4. 次のいずれかで、エージェントを設定します。

- **YAML 設定ファイル :** このファイルをサービスのメインプロジェクトに追加します。ファイルのプロパティが、に設定されていることを確認してください。以下のように、ファイルの場所を指定する環境変数を ServiceManifest.xml に追加します。

```

<CodePackage>
  <EnvironmentVariables>
    <EnvironmentVariable Name="CONTRAST_CONFIG_PATH" \
Value="contrast_security.yaml"/>
  
```

- **環境変数 :** 以下のように、環境変数を ServiceManifest.xml に追加します。

```

<CodePackage>
  <EnvironmentVariables>
    <EnvironmentVariable Name="CONTRAST__API__URL" \
Value="https://teamserver-staging.contsec.com"/>
    <EnvironmentVariable Name="CONTRAST__API__API_KEY" \
Value="aBcD0123"/>
    <EnvironmentVariable Name="CONTRAST__API__SERVICE_KEY" \
Value="ABCD0123"/>
    <EnvironmentVariable Name="CONTRAST__API__USER_NAME" \
Value="agent_123@Team"/>
  
```

5. 通常どおり、Azure Service Fabric アプリケーションをデプロイします。

## .NET Framework エージェントのプロファイラチェーン

プロファイラチェーンを使用すると、パフォーマンスツールや APM ツールなどの、.NET プロファイラエージェントと併せて .NET Framework エージェントを実行することができます。

Contrast .NET Framework エージェントは、以下のプロファイリングツールとの互換性をテストおよび実証済みです。

プロファイリングツール	検証済バージョン
AppDynamics	4.5.18.1

プロファイリングツール	検証済バージョン
Dynatrace OneAgent	1.253.245
New Relic	8.23.107
リバーヘッド SteelCentral Aternity APM	12.9.0



### 注記

その他のプロファイリングツールでも、CLR のプロファイル API の規則に準拠しており、プロファイリング環境に関する前提条件がない場合は、エージェントはそのツールと互換性がある可能性があります。

プロファイラチェーンは、デフォルトでは有効になっています。プロファイラチェーンを無効にするには、`agent.dotnet.enable_chaining` オプションを `false` にするよう、[.NET Framework エージェントを設定 \(152ページ\)](#) します。例えば、次のように YAML 設定を使用して指定できます。

```
agent:  
  dotnet:  
    enable_chaining: false
```

設定が完了したら、エージェントを再起動する必要があります。再起動すると、Contrast .NET Framework エージェントは、IIS に登録されている他のプロファイリングツールの存在を自動的に検出し、Contrast .NET Framework エージェントとサードパーティの両方のプロファイラをロードするよう環境を構成します。

**重要**

プロファイラチェーンの使用方法に応じて、以下の各手順に従ってください。

- **IIS :**

サードパーティのエージェントをインストールしてから、Contrast .NET Framework エージェントをインストールしてください。

(サードパーティのエージェントの前に Contrast .NET Framework エージェントをインストールした場合は、**Windows サービス**で Contrast.NET Main Service を再起動する必要があります。)

- **IIS 以外 :**

以下のようなアプリケーションでプロファイラチェーンを使用している場合、`agent.dotnet.enable_chaining` オプションは機能しません。

- IIS 以外でホストされているアプリケーション
- (インストールされたエージェントではなく)サードパーティエージェントの Nuget パッケージを使用するアプリケーション

上記に該当する場合は、プロファイリングツールの CLR 環境変数を `CONTRAST_CCC_COR` バージョンに置き換えてください。以下の環境変数名はいずれも置き換える必要があります。

変更すべき変数名	変更後
<code>COR_PROFILER</code>	<code>CONTRAST_CCC_COR_PROFILER</code>
<code>COR_PROFILER_PATH</code>	<code>CONTRAST_CCC_COR_PROFILER_PATH</code>
<code>COR_PROFILER_PATH_32</code>	<code>CONTRAST_CCC_COR_PROFILER_PATH_32</code>
<code>COR_PROFILER_PATH_64</code>	<code>CONTRAST_CCC_COR_PROFILER_PATH_64</code>

次に、ご利用の環境とアプリケーションに合わせて、通常のセットアップ手順を行ってください。

- **Azure App Service の Application Insights :**

バージョン 20.9.3 より、Contrast .NET Framework Site Extension は、Application Insights との互換性をサポートするようになりました(CLR Instrumentation Engine (CIE)を使用)。

Contrast.NET Framework Site Extension で、Application Insights を使用するために追加の操作は必要ありません。.NET Framework エージェントのプロファイラは、(Application Insights が有効になっているなどの理由で)Azure AppService インスタンスでプロファイリングツールとして登録されている場合、CIE によってロードされます。

## .NET エージェントエクスプローラ

**重要**

.NET Core エージェント 4.0.0 および .NET Framework エージェント 51.0.0 より、Contrast トレイアプリケーションを .NET エージェントエクスプローラに置き換えました。

.NET エージェントエクスプローラは、.NET Core エージェントおよび .NET Framework エージェントの稼働状況に関する概要情報を表示するアプリケーションです。このアプリケーションを使用すると、工

エージェントが想定通りに動作しているかを確認できます。特にエージェントを最初にインストールした後にご利用ください。

エージェントをインストールすると、このアプリケーションもインストールされます。両方の種類のエージェントをインストールした場合は、エージェントエクスプローラのインスタンスは1つだけインストールされます。

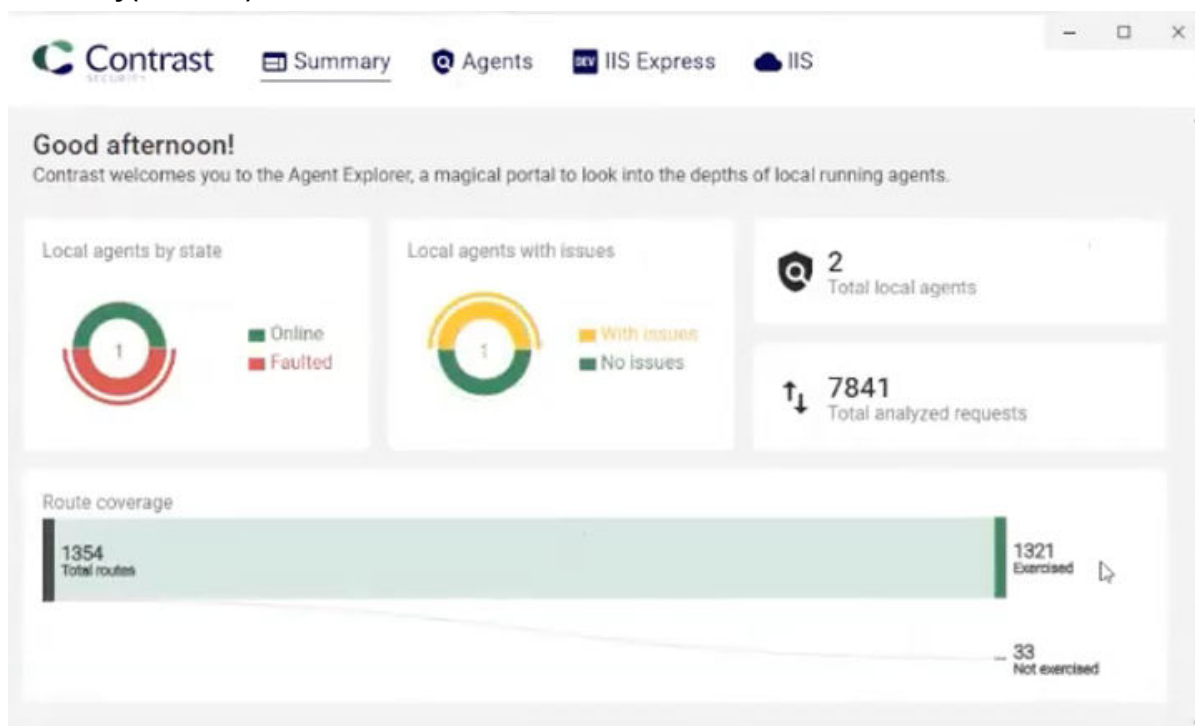
## エージェントエクスプローラへのアクセス

.NET Core エージェントが .NET Framework エージェントをインストールした後、エージェントエクスプローラのアイコン(🔍)がトレイに表示されます。アイコンを右クリックすると、アプリケーションが開きます。

## エージェントエクスプローラでの情報

エージェントエクスプローラには、以下の情報が表示されます。

- **Summary(サマリー)**



このダッシュボードには、エージェントのステージ、問題のあるエージェントの有無、ルートカバレッジなど、エージェントに関する概要レベルの情報が表示されます。

- **Agents(エージェント)**

The screenshot shows the Contrast Security web interface. At the top, there are navigation tabs: Summary, Agents, IIS Express, and IIS. Below the navigation, there are breadcrumb links: < Return, Overview, Configuration, Advanced information, Agent specific metadata. The main content area is titled ".NET" and displays the following information:

Application name	Agent language	Runtime version	Total requests	Running since
DotnetCore5	.NET Core	.NET 5.0.17	5152	19 minutes ago
Application PID	Agent version	Runtime bitness	Exercised routes	Agent modes
532188	19.9.0.0	x64	1321/1354	<input type="button" value="assess"/> <input type="button" value="protect"/> <input type="button" value="inventory"/>

YAML file path  
 [D:\Development\dotnet\dotnet-agent\tests\integration-tests\DotnetCore5\localAgent.yaml](#)

Logs directory  
 [C:\ProgramData\contrast\dotnet-core\logs](#)

**Configuration**

Name	Value	
enable	true	<input type="button" value="yml-config"/>
api.url	https://teamserver-...com	<input type="button" value="yml-config"/>

このタブには、.NET Core エージェントおよび .NET Framework エージェントの稼働状況に関する情報が表示されます。Configuration(設定)セクションには、特定の問題が発生していることをエージェントエクスペローラが検知した場合に、メッセージが表示されます。

Overview(概要)セクションにあるリンクから、エージェントの設定ファイル(YAML ファイル)に直接アクセスすることができます。下にスクロールすると、エージェントの設定内容、詳細情報、セッションメタデータの情報が表示されます。

- **IIS Express**

このタブには、IIS Express で実行されている Web アプリケーションの情報が表示されます。

- **IIS**

このタブには、IIS サーバで実行されている Web アプリケーションの情報が表示されます。

## .NET Framework Contrast トレイ

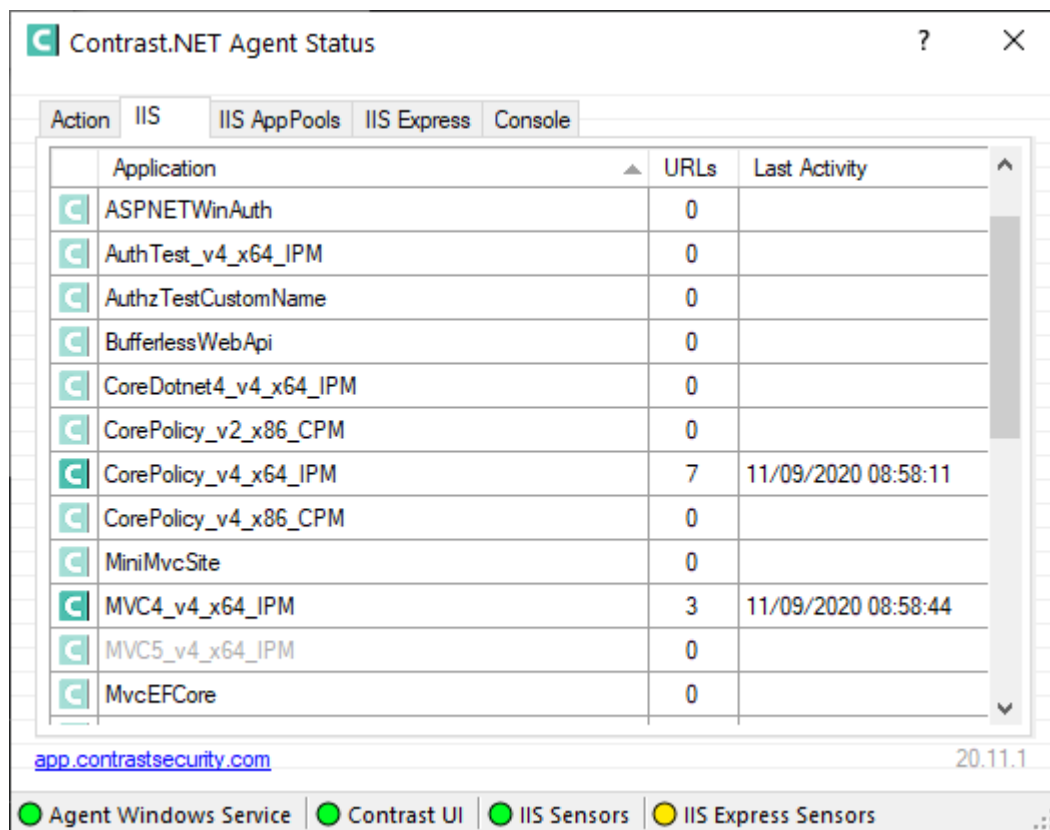
Contrast トレイをサポートするエージェントの最後のバージョンは、50.0.0 です。それより後のエージェントのバージョンでは、[Contrast エージェントエクスペローラ \(189ページ\)](#)を使用します。

.NET Framework Contrast トレイは、Windows システムトレイアプリケーション(*ContrastTray.exe*)で、エージェントの状態に関する情報を概要レベルで表示します。



### 注記

Contrast を使用してアプリケーションを解析するために、.NET Framework Contrast トレイを実行する必要はありません。Contrast トレイは、エージェントのステータス情報を提供するためだけのものです。特に最初にエージェントをインストールした時などに、エージェントが正しく動作しているかを確認できます。



Contrast トレイには以下のステータスインジケータがあります。

- **Agent Windows Service**(エージェントの Windows サービス) : Contrast Service が正しくインストールされて実行されていると、緑色に点灯します。
- **Contrast UI** : エージェントの Windows サービスが Contrast サーバと通信できると、緑色に点灯します。通信に失敗する最も一般的なエラーは、プロキシの設定の誤りです。
- **IIS Sensors**(IIS センサー) : IIS でホストされているアプリケーションにエージェントが正しく組み込まれると、緑色に点灯します。黄色に点灯する場合は、アプリケーションにエージェントは組み込まれていますが、IIS でまだそのアプリケーションがロードされていないことを示します。
- **IIS Express Sensors**(IIS Express センサー) : IIS Express でホストされているアプリケーションがロードされ、Contrast エージェントが正しくインストールされて実行されると、緑色に点灯します。黄色に点灯する場合は、アプリケーションに Contrast エージェントは正しくインストールされていますが、IIS Express でまだそのアプリケーションがロードされていないことを示します。赤色の点灯は、IIS Express で環境変数が設定されていないことを示します。

Contrast トレイの各タブを選択すると、詳細情報が表示されます。

- **Action**(アクション) : .NET Framework エージェントを使用するためのユーザへの指示が概要レベルで表示されます。ここで表示される指示は、エージェントの状態により変わります。例えば、エージェントが Contrast サーバに接続できない場合、Action タブにはエラーの詳細情報と問題を解決する方法が提示されます。
- **IIS** : IIS サーバで実行されている全ての Web アプリケーションが一覧で表示されます。表示されるアプリケーション名は、[カスタムのアプリケーション名を指定 \(152ページ\)](#)しない限り、IIS がアプリケーションを識別するために使用するエイリアスと同じものになります。URL 列には、エージェントがアプリケーションで観測したユニークな URL (クエリストリングを含まない)の件数が表示されます。Last Activity(最後のアクティビティ)列には、そのアプリケーションに対してエージェントが最後に解析したリクエストの時間が表示されます。
- **IIS AppPools**(IIS アプリケーションプール) : IIS サーバ上の全てのアプリケーションプールが一覧で表示されます。各アプリケーションプールの構成の詳細(アーキテクチャ、パイプラインモード、CLR バージョン、ID)を確認できます。また、このアプリケーションプールのアプリケーションが Contrast



で解析されるかどうかを確認できます。IIS で、.NET Framework エージェントの [アプリケーションプールのフィルターを設定 \(193ページ\)](#) できます。

- **IIS Express** : IIS Express で実行されている全ての Web アプリケーションが一覧で表示されます。
- **Console(コンソール)** : Contrast .NET エージェントの問題のトラブルシュー트에役立つ、ステータスやエラーメッセージが表示されます。

## IIS でアプリケーションプールを使用する

.NET エージェントは、IIS にデプロイされている全ての ASP.NET アプリケーションに自動的に組み込まれます。.NET エージェントがインストールされ、エージェントのバックグラウンドの Windows サービスが実行されていることが確認されると、IIS でホストされる全てのアプリケーションに対してエージェントが組み込まれます。

以下のような理由などにより、一部のアプリケーションでエージェントの組み込みを対象外にすることもできます。

- いくつかのアプリケーションは、セキュリティやライブラリ情報を収集する必要がない
- アプリケーションがあるサーバにリソースの制約があるか、あるいは Contrast エージェントを組み込むために追加のパフォーマンス要件は避けたい

IIS でホストされる Web アプリケーションは、アプリケーションプールで実行されます。アプリケーションの .NET エージェントを無効にする必要がある場合、そのアプリケーションが実行される [アプリケーションプールを拒否 \(193ページ\)](#) します。

特定のアプリケーションが実行されるアプリケーションプールを検索する方法は 3 つあります。

- **インターネット インフォメーション サービス (IIS) マネージャー**  
%windir%\system32\inetsrv\InetMgr.exe コマンドを使用して、IIS マネージャーを起動します。対象の Web アプリケーションを選択し、**基本設定**を選択します。アプリケーションプール名を表すフィールドが表示されます。
- **AppCmd.exe**  
管理者権限がある場合は、cmd.exe を実行します。C:\Windows\System32\inetsrv に移動します。appcmd list apps と入力すると、アプリケーションの一覧とそれぞれのアプリケーションプールが表示されます。
- **Contrast .NET ログ**  
Contrast .NET エージェントを起動します。アプリケーションを操作します。そしてログディレクトリに移動します。Windows の場合、C:\ProgramData\Contrast\dotnet\LOGS に移動します。最新のプロファイルログ(XXXXX\_Profiler\_[AppDomain]XXXXX[XX].log)を開きます。アプリケーションプール名は、**ApplicationPool Name** で始まる行にあります。

## アプリケーションプールの拒否と許可リスト

拒否リストと許可リストは、アプリケーションプール名に基づいて設定されます。アプリケーションプールの拒否リストと許可リストには、\*もワイルドカード文字として使用できます(AppPool\*は、AppPool1 や AppPool\_arb などと一致します)。

許可リストは、拒否リストよりも優先されます。両方のリストを満たすアプリケーションプールは、解析されません。

特定のアプリケーションのエージェントを無効にするには、C:\ProgramData\Contrast\dotnet\contrast\_security.yaml で、agent.dotnet.app\_pool\_denylist オプションに該当のアプリケーションプールを指定します。

```
# Comma-separated list of application pools ignored by Contrast
agent:
  dotnet:
    app_pool_denylist: ExampleAppPoolName
```

IIS でホストされるアプリケーションで特定のアプリケーションにのみエージェントを有効にするには、特定のアプリケーションプールのみを解析するよう agent.dotnet.app\_pool\_allowlist を設

定めます。アプリケーションプールが許可リストに指定されている場合、エージェントは一致するプールを解析します。他のアプリケーションへの影響はありません。

特定のアプリケーションプールにのみエージェントを有効にするには、`C:\ProgramData\Contrast\dotnet\contrast_security.yaml` で、`agent.dotnet.app_pool_allowlist` オプションに該当のアプリケーションプールを指定します。

```
# Comma-separated list of application pools exclusively profiled by Contrast
agent:
  dotnet:
    app_pool_allowlist: ExampleAppPoolName
```



### ヒント

詳細については、[YAML 設定 \(38ページ\)](#)を参照してください。

## .NET Framework および .NET Core のテレメトリ

.NET Framework エージェントおよび .NET Core エージェントは、テレメトリを使用して、使用状況に関するデータを収集します。テレメトリは、エージェントを組み込んだアプリケーションでエージェントのセンサーが最初にロードされた時に収集され、その後も定期的(数時間ごと)に収集されます。

弊社では、[お客様のプライバシーは非常に大切 \(828ページ\)](#)であると考えています。このテレメトリ機能は、アプリケーションのデータを収集するものではありません。データは匿名化されてから、安全に Contrast に送信されます。そして、集約されたデータは暗号化されて保存され、アクセスが制限されます。収集されたデータは、全て 1 年後に削除されます。

テレメトリ機能で収集されるのは、以下のデータです。

エージェントのバージョン	データ	
.NET Framework 2020.8.3 以降	エージェントのバージョン	
.NET Core 1.5.15 以降	オペレーティングシステムとバージョン	
	エージェントがコンテナ内で実行されているかどうか	
	エージェントが Azure App Services で実行されているかどうか	
	ハッシュ化されたメディアアクセス制御(MAC)アドレス：暗号化(SHA256)された、匿名の一意なマシン ID	
	カーネルのバージョン	
	プロセスの実行時間	
	Assess が有効であるかどうか	
	Protect が有効であるかどうか	
	.NET Framework 2020.8.3 以降	.NET Framework ランタイムのバージョン
	.NET Core 1.5.15 以降	.NET Core ランタイムのバージョン
.NET Framework 20.9.1 以降	Contrast インスタンスが SaaS 版がオンプレミス版であるか	
.NET Core 1.5.17 以降		
.NET Framework 20.9.3 以降	CLR Instrumentation Engine (CIE)の使用状況	
.NET Core 1.5.19 以降	アプリケーションのフレームワーク	

エージェントのバージョン	データ
	連携しているプロファイリングツール
.NET Framework 20.10.1 以降	プロセスのホスティングモード
.NET Core 1.5.20 以降	CIE ネイティブプロファイラフックの使用状況
.NET Framework 20.10.2 以降	デフォルト以外の値が指定されている設定名
.NET Core 1.5.21 以降	無効にされている Assess ルール名
.NET Framework 20.12.2 以降	エージェントのプロファイラコンポーネントが初期化されるまでに経過した時間
.NET Core 1.7.2 以降	エージェントから Contrast Web インターフェイスへの最初のリクエストまでに経過した時間
	エージェントのプロファイラコンポーネントが初期化されるまでに経過した時間
	エージェントの初期化から最初のリクエストが終了するまでに経過した時間
.NET Framework 21.1.1 以降	IIS でホストされているアプリケーションに関する測定値 : <ul style="list-style-type: none"> <li>合計アプリケーション数</li> <li>解析対象となるアプリケーション数(アプリケーションの許可/拒否リストで設定)</li> <li>CLR4 のアプリケーションプールでホストされているアプリケーション数</li> <li>CLR2 のアプリケーションプールでホストされているアプリケーション数</li> </ul> IIS のアプリケーションプールに関する測定値 : <ul style="list-style-type: none"> <li>合計数</li> <li>エージェントが接続されている数</li> <li>CLR4 の数</li> <li>CLR2 の数</li> </ul> 単独のアプリケーションプールでのアプリケーションの最小数 単独のアプリケーションプールでのアプリケーションの最大数 全てのアプリケーションプールにあるアプリケーション数の中央値
.NET Framework 21.1.2 以降	Protect の各ルールのモード(例、監視やブロック)
.NET Core 1.7.5 以降	
.NET Framework 21.4.2 以降	エージェントのセンサーコード内でスローされキャッチされた例外。ログメッセージ、例外タイプ、例外のメッセージ、System メソッドおよび Contrast メソッドのスタックトレースフレームなど。
.NET Core 1.8.4 以降	
.NET Framework 21.7.1 以降	<ul style="list-style-type: none"> <li>プロセスアーキテクチャ(x86/x64)</li> </ul>
.NET Core 1.9.7 以降	OS アーキテクチャ(x86/x64) Azure App Service における以下の環境変数の値 : <ul style="list-style-type: none"> <li>WEBSITE_PHYSICAL_MEMORY_MB</li> <li>WEBSITE_PLATFORM_VERSION</li> <li>WEBSITE_SKU</li> </ul>
.NET Framework 21.9.2 以降	YAML 設定ファイルを読み込んだ場所(環境変数で指定したパス、デフォルトの場所、アプリケーションディレクトリなど)に関する説明
.NET Core 2.0.1 以降	

テレメトリ機能を停止するには、`CONTRAST_AGENT_TELEMETRY_OPTOUT` という環境変数に 1 または `true` を設定してください。

テレメトリのデータは、[telemetry.dotnet.contrastsecurity.com](https://telemetry.dotnet.contrastsecurity.com) に安全に送信されます。ネットワークレベルで通信をブロックすることで、テレメトリ機能を停止することもできます。

## .NET Core エージェント

Contrast .NET エージェントは、ユーザが .NET Core の Web アプリケーションを操作する際のアプリケーションの動きを解析します。

ホストプロセスにプロファイリング用の環境変数やアプリケーション起動プロファイルが設定されると、エージェントは自動的に ASP.NET Core アプリケーションに組み込まれます。

Contrast .NET Core エージェントは 2 つのコンポーネントで構成され、どちらもアプリケーションと同じプロセス内で動作します。

- **.NET プロファイラ**は、アプリケーションによって使用されるセキュリティ関連の API とその依存関係に Contrast センサーコードへの呼び出しを追加することで、アプリケーションに組み込まれます (IL Weaving と呼ばれます)。
- **センサー**は、セキュリティ情報、アーキテクチャ情報、ライブラリ情報を収集します。

[.NET Core エージェントをインストール \(198ページ\)](#)したら、ユーザがアプリケーションを実行する際に、エージェントのセンサーがアプリケーションのセキュリティ、アーキテクチャ、ライブラリに関する情報を収集します。エージェントによる解析結果は、Contrast Web インターフェイスで確認できます。エージェントには、こちらの[サポート対象テクノロジー \(196ページ\)](#)と[システム要件 \(197ページ\)](#)で動作します。

## .NET Core のサポート対象テクノロジー

このエージェントでは、以下のテクノロジーをサポートします。

テクノロジー	サポート対象バージョン	備考
アプリケーションフレームワーク	<ul style="list-style-type: none"> <li>• ASP.NET Core(3.1.x、5.0.x、6.0.x、7.0.x)</li> <li>• Model-View-Controller (MVC)</li> <li>• Razor Pages</li> </ul>	<p><b>限定サポート：</b></p> <p>ASP .NET Core 3.1.x、5.0.x</p> <p><b>サポート対象外：</b></p> <ul style="list-style-type: none"> <li>• .NET Core または ASP.NET Core バージョン 2.1 以前</li> <li>• .NET Framework (Windows)または Mono (Linux/Windows)上で動作する ASP.NET Core アプリケーション</li> </ul>
ランタイム	<ul style="list-style-type: none"> <li>• .NET Core ランタイム：3.1.x、5.0.x、6.0.x、7.0.x</li> <li>• .NET Core ターゲットフレームワーク： <ul style="list-style-type: none"> <li>• netcoreapp3.1</li> <li>• net5.0</li> <li>• net6.0</li> <li>• net7.0</li> </ul> </li> </ul>	<p><b>限定サポート：</b></p> <p>.NET Core ランタイム 3.1.x、5.0.x</p> <p><b>サポート対象外：</b></p> <ul style="list-style-type: none"> <li>• ランタイムよりも上位バージョンの ASP.NET Core アプリケーションでの実行(例、ASP.NET Core 5.0 を参照する .NET Core 3.1 ランタイムのアプリケーションなど)</li> <li>• 参照する ASP.NET Core のバージョンとコンパイル時に選択したターゲットのランタイムが一致しない .NET Core アプリケーションでの実行</li> </ul>
<b>.NET Core for Windows</b>		
Windows オペレーティングシステム	<ul style="list-style-type: none"> <li>• Windows Server (LTSC) (x86, x64)：2012 R2、2016、2019、2022</li> <li>• Windows Server (SAC) (x64)：1809、1903</li> <li>• Windows ワークステーション (x86、x64)：7、8/8.1、10</li> </ul>	<p>64 ビットシステムでは、エージェントを使用して 32 ビットと 64 ビットの両方の Web アプリケーションを解析できます。</p> <p><b>サポート対象外：</b></p> <ul style="list-style-type: none"> <li>• ARM 版 Windows</li> </ul>
サーバコンテナ	Kestrel、IISHttpServer	<p><b>サポート対象外：</b></p> <p>Http.sys (旧 WebListener)</p>
ホスティングコンテナ	セルフホスト、IIS、IIS Express	
<b>.NET Core for Linux</b>		
Linux オペレーティングシステム	<ul style="list-style-type: none"> <li>• Ubuntu：16.04 以降</li> <li>• Debian：9 以降</li> <li>• openSUSE：15 以降</li> <li>• Alpine：3.12 以降</li> <li>• CentOS：7 以降</li> <li>• Red Hat Enterprise Linux：7、8</li> </ul>	<p>すべてのシステムで x64 アーキテクチャが必須です。</p> <p><b>サポート対象外：</b> Red Hat Enterprise Linux 6</p>
サーバコンテナ	Kestrel	

テクノロジー	サポート対象バージョン	備考
ホスティング コンテナ	セルフホスト	



### 重要

- .NET Core 2.2 は、.NET Core エージェントのバージョン 1.5.20 以降ではサポートされません。 .NET Core 2.2 を使用している場合、アプリケーションの .NET Core ランタイムをアップグレードするまでは、.NET Core エージェントのバージョン 1.5.20 以前のものを使用してください。
- .NET Core エージェントのバージョン 1.9.9 をもって、.NET Core 2.1 のサポートを終了しました。 .NET Core 2.1 を使用している場合、アプリケーションの .NET Core ランタイムをアップグレードするまでは、.NET Core エージェントのバージョン 1.9.9 以前のものを使用してください。
- Microsoft は、2022 年 5 月 10 日をもって .NET 5.0 のサポートを終了し、2022 年 12 月 13 日をもって .NET Core 3.1 のサポートを終了しました。 .NET 5.0 および .NET Core 3.1 に関する Contrast のサポートは、.NET Core エージェントのバージョン 3.0.0 による限定的なサポートとなります。 Contrast の限定サポートでは、サポート対象の言語バージョンで再現可能な問題のみを解決します。 お使いのアプリケーションを .NET のサポート対象バージョンにアップグレードすることを強く推奨します。



### 注記

.NET Core エージェントは、System.Runtime および ASPNET Core を参照していないアプリケーションをサポートしません。 また、エージェントが依存しているアセンブリをコンパイラがトリムする可能性があるため、エージェントは **トリミングされた自己完結型のデプロイと実行可能ファイル** もサポートしません。

## .NET Core のシステム要件

.NET Core エージェントをインストールする前に、以下の要件を満たしていることを確認してください。

- サーバへの管理者権限があり、そのサーバは [Contrast のサポート対象 \(196ページ\)](#) であること。
- 検査対象のアプリケーションがデプロイされており、その [Web アプリケーションのテクノロジーは Contrast のサポート対象 \(196ページ\)](#) であること。
- Web サーバが Contrast とネットワークで接続されていること。
- サーバが最低限の要件(以下に記載)を満たしていること。

要件	推奨	最小	備考
.NET Core のバージョン	3.1.x, 5.0.x, 6.0.x	2.1, 3.0, 3.1	
CPU	4 個以上	2	
メモリ	8 GB 以上	4 GB	Assess でエージェントを実行するには、検査対象のアプリケーションのメモリ要件がおよそ 2 倍になります。 エージェントがインストールされていない場合に、アプリケーションが使用するメモリは全メモリ容量の半分以下である必要があります。

要件	推奨	最小	備考
プロセッサのアーキテクチャ	<ul style="list-style-type: none"> <li>32ビットプロセッサ</li> <li>64ビットプロセッサ</li> </ul>		.NET Core エージェントは、ARM ベースのプロセッサ(例えば、Apple M1 プロセッサ)を搭載したシステムを <b>サポートしていません</b> 。この制限には、これらのシステム上のコンテナ内でのエージェントの使用も含まれます。

## .NET Core エージェントのインストール

.NET Core エージェントをインストールするには：

1. エージェントのコンポーネントをサーバのファイルシステムに置きます。
2. .NET ランタイムがエージェントのプロファイルコンポーネントをロードするように環境変数を設定します。
3. 通常通りにアプリケーションを疎通し、Contrast でアプリケーションが認識されていることを確認します。

利用する環境に合わせて、以下のいずれかのインストール方法を使用してください。

- [手動インストール \(198ページ\)](#) (Windows、Linux または Docker で実行するセルフホスト Web アプリケーションを使用する場合)
- [IIS 用 .NET Core エージェントのインストーラ \(204ページ\)](#) (IIS を使用している場合)
- [Azure App Service \(203ページ\)](#)
- [NuGet \(201ページ\)](#)

エージェントを自動アップグレードするには、[エージェントアップグレードサービス \(150ページ\)](#)のオプションを有効にします。

## .NET Core エージェントを手動でインストール

IIS でホストされている Web アプリケーションを使用している、もしくは、Windows、Linux、Docker 上でセルフホストの Web アプリケーションを実行している場合は、この方法で .NET Core エージェントをインストールします。

インストールを開始する前に、[システム要件 \(197ページ\)](#)と[サポート対象テクノロジー \(196ページ\)](#)を確認し、インストールが可能で最適なパフォーマンスを得られる環境であるかを確認してください。



### 注記

コンテナへのインストールは複雑になる可能性があり、本項での手順がお客様の利用状況に合わない可能性もあります。Docker でのインストールについては、[こちらの記事](#)を参照してください。

1. Contrast Web インターフェイスの右上で**新規登録**を選択します。**.NET Core**を選択し、.NET Core エージェントをダウンロードするボタンを選択します。
2. Web サーバ上のディレクトリで、ダウンロードした ZIP アーカイブ(例、*Contrast.NET.Core\_1.0.1.zip*)を解凍します。ディレクトリには、アプリケーションがアクセスするのに十分な権限を付与してください。
3. アプリケーションのプロセスに次の環境変数を設定します。ご利用のオペレーティングシステムに適した CORECLR\_PROFILER\_PATH の設定を指定します。<UnzippedDirectoryRoot>をアーカイブディレクトリに置き換えます。
  - **Windows**

環境変数	値
CORECLR_PROFILER_PATH_64	<UnzippedDirectoryRoot>\runtimes\win-x64\native\ContrastProfiler.dll
CORECLR_PROFILER_PATH_32	<UnzippedDirectoryRoot>\runtimes\win-x86\native\ContrastProfiler.dll
CORECLR_PROFILER	{8B2CE134-0948-48CA-A4B2-80DDAD9F5791}
CORECLR_ENABLE_PROFILING	1
CONTRAST_CONFIG_PATH	<path_to_contrast_security.yaml>



### 重要

同じサーバで、.NET Core エージェントと .NET Framework エージェントを実行している場合、CONTRAST\_CONFIG\_PATH オプションが両方のエージェントのロードパス (36ページ) 適用されます。各エージェントに対して個別のパスを適用するには、次のオプションを使用してデータディレクトリを指定します。

- CONTRAST\_CORECLR\_DATA\_DIRECTORY
- CONTRAST\_DATA\_DIRECTORY

#### Linux

環境変数	値
CORECLR_PROFILER_PATH_64	<UnzippedDirectoryRoot>/runtimes/linux-x64/native/ContrastProfiler.so
CORECLR_PROFILER	{8B2CE134-0948-48CA-A4B2-80DDAD9F5791}
CORECLR_ENABLE_PROFILING	1
CONTRAST_CONFIG_PATH	<path_to_contrast_security.yaml>

4. アプリケーションのランタイムユーザが以下のパスにアクセスできることを確認してください。

パス	用途	カスタマイズ可能	権限
.NET Core エージェントの YAML (214ページ) へのパス	エージェントを設定	可、環境変数 CONTRAST_CONFIG_PATH を設定	読取り
<UnzippedDirectoryRoot>	「インストール」のルートディレクトリ、エージェントバイナリを格納	不可	読取り
<ul style="list-style-type: none"> <li>• Windows: %ProgramData%\Contrast\dotnet-core\logs</li> <li>• Linux: /var/tmp/contrast/dotnet-core/logs</li> </ul>	Contrast エージェントログのディレクトリ、ない場合は生成される	可、環境変数 CONTRAST_CORECLR_LOGS_DIRECTORY を設定	読取り/書き込み (または親ディレクトリから継承)



### 注記

IIS で実行する場合、アプリケーションプールがこれらのパスにアクセスできることを確認してください。

例えば、デフォルトの ID である ApplicationPoolIdentity を使用する Default Web Site という名前のアプリケーションプールがある場合、ユーザの IIS AppPool\Default Web Site に、解凍されたディレクトリのルートへの有効な読取り権限があることを確認します。

5. Contrast サーバに接続するための認証情報やプロキシ情報を [エージェントに設定 \(213ページ\)](#) します。
6. アプリケーションがロードされたら、アプリケーションを疎通して、Contrast でサーバとアプリケーションがアクティブになり、脆弱性が報告されることを確認します。



## ヒント

[エージェントを更新 \(211ページ\)](#)するには、エージェントディレクトリ内のエージェントファイルを置き換え、アプリケーションを再起動します。エージェントはアプリケーションと一緒に実行されているため、エージェント自体を更新することはできません。

環境が適切に設定されていれば、エージェントはアプリケーションと一緒に自動的に起動します。

エージェントを停止するには、アプリケーションを停止し、環境からエージェントを削除します。または、`CORECLR_ENABLE_PROFILING` の設定を `0` に変更することもできます。

環境変数の設定は、以下の例を参考にしてください。

- [IIS \(200ページ\)](#)
- [Bash \(Linux\) \(201ページ\)](#)
- [Powershell または Powershell Core\(Windows\) \(201ページ\)](#)
- [起動プロファイル\(dotnet.exe\) \(201ページ\)](#)

## IIS および IIS Express

以下のいずれかの方法によって、環境変数を設定します：

- [アプリケーションの `web.config` の `environmentVariables` セクション](#)

```
<?xml version="1.0" encoding="utf-8"?>
<configuration>
  <system.webServer>
    <!-- ... -->
    <aspNetCore processPath="dotnet" \
arguments=".\ExampleNetCoreApp.dll" stdoutLogEnabled="false" \
stdoutLogFile=".\logs\stdout">
      <environmentVariables>
        <environmentVariable name="CORECLR_PROFILER_PATH_64" \
value="C:\contrast\dotnetcore\runtimes\win-
x64\native\ContrastProfiler.dll" />
        <environmentVariable name="CORECLR_PROFILER_PATH_32" \
value="C:\contrast\dotnetcore\runtimes\win-
x86\native\ContrastProfiler.dll" />
        <environmentVariable name="CORECLR_ENABLE_PROFILING" \
value="1" />
        <environmentVariable name="CORECLR_PROFILER" \
value="{8B2CE134-0948-48CA-A4B2-80DDAD9F5791}" />
        <environmentVariable name="CONTRAST_CONFIG_PATH" \
value="C:\contrast\dotnet-core\contrast_security.yaml" />
      </environmentVariables>
    </aspNetCore>
  </system.webServer>
</configuration>
```



```
</system.webServer>
</configuration>
```

- サーバの[アプリケーションプール設定](#)

## Bash (Linux)

```
export CORECLR_PROFILER_PATH_64=/usr/local/contrast/runtimes/linux-x64/
native/ContrastProfiler.so
export CORECLR_ENABLE_PROFILING=1
export CORECLR_PROFILER={8B2CE134-0948-48CA-A4B2-80DDAD9F5791}
export CONTRAST_CONFIG_PATH=/etc/contrast/contrast_security.yaml
```

次に、アプリケーションを実行します。

```
dotnet ./MyAppWithContrastAgent.dll
```

## Powershell または Powershell Core (Windows)

```
$env:CORECLR_PROFILER_PATH_64 = 'C:\contrast\dotnetcore\runtimes\win-
x64\native\ContrastProfiler.dll'
$env:CORECLR_PROFILER_PATH_32 = 'C:\contrast\dotnetcore\runtimes\win-
x86\native\ContrastProfiler.dll'
$env:CORECLR_ENABLE_PROFILING = '1'
$env:CORECLR_PROFILER = '{8B2CE134-0948-48CA-A4B2-80DDAD9F5791}'
$env:CONTRAST_CONFIG_PATH = 'C:\contrast\dotnet-
core\contrast_security.yaml'
```

次に、アプリケーションを実行します。

```
dotnet .\MyAppWithContrastAgent.dll
```

## 起動プロファイル(dotnet.exe)

```
{
  "MyAppWithContrastAgent": {
    "environmentVariables": {
      "CORECLR_PROFILER_PATH_64": "C:\\contrast\\dotnetcore\\runtimes\\
win-x64\\native\\ContrastProfiler.dll",
      "CORECLR_PROFILER_PATH_32": "C:\\contrast\\dotnetcore\\runtimes\\
win-x86\\native\\ContrastProfiler.dll",
      "CORECLR_ENABLE_PROFILING": "1",
      "CORECLR_PROFILER": "{8B2CE134-0948-48CA-A4B2-80DDAD9F5791}",
      "CONTRAST_CONFIG_PATH": "c:\\contrast\\config\\MyApp\\
contrast_security.yaml"
    }
  }
}
```

次に、アプリケーションを実行します。

```
dotnet run --launch-profile MyAppWithContrastAgent
```

## NuGet で .NET Core エージェントを手動でインストール

.NET Core エージェントは、NuGet を使用して手動でインストールすることができます。このインストール方法は、[Azure App Service の拡張機能 \(203ページ\)](#)が利用できない場合や、.NET Core エージェントを依存関係に含めたい場合などに便利です。

NuGet を使用して .NET Core エージェントを手動でインストールするには、以下の手順を実行します。

1. アプリケーションに Contrast の NuGet パッケージをインストールします。  
dotnet コマンドラインを使用する場合：

```
dotnet add package Contrast.SensorsNetCore
```

Visual Studio を使用する場合：

- ソリューションエクスプローラーで、アプリケーションのプロジェクトまたは参照のどちらかを右クリックし、**NuGet パッケージの管理**を選択します。
  - **Contrast.SensorsNetCore** パッケージを検索して選択し、プロジェクトに追加します。
  - アプリケーションをビルドします。プロジェクトに *contrast* フォルダが表示されることを確認してください。アプリケーションが公開されると、このフォルダはビルドの出力ディレクトリにも表示されます。
2. .NET ランタイムでエージェントのプロファイラコンポーネントがロードされるよう環境変数を設定します。

**Windows :**

```
CORECLR_ENABLE_PROFILING: 1
CORECLR_PROFILER: {8B2CE134-0948-48CA-A4B2-80DDAD9F5791}
CORECLR_PROFILER_PATH_32: <application directory>\contrast\runtimes\win-x86\native\ContrastProfiler.dll
CORECLR_PROFILER_PATH_64: <application directory>\contrast\runtimes\win-x64\native\ContrastProfiler.dll
```

**Linux :**

```
CORECLR_ENABLE_PROFILING: 1
CORECLR_PROFILER: {8B2CE134-0948-48CA-A4B2-80DDAD9F5791}
CORECLR_PROFILER_PATH: <application directory>/contrast/runtimes/linux-x64/native/ContrastProfiler.so
```

3. [YAML 設定ファイル \(214ページ\)](#)または[環境変数 \(213ページ\)](#)を使用して、基本のオプションを設定します。例：

```
CONTRAST_CONFIG_PATH: [Path to yaml config file]
```

最低限、以下の環境変数が必要です。

```
CONTRAST__API__URL: [IF USING ANOTHER SERVER THAN THE DEFAULT: https://app.contrastsecurity.com]
CONTRAST__API__USER_NAME: [REPLACE WITH YOUR AGENT USERNAME]
CONTRAST__API__SERVICE_KEY: [REPLACE WITH YOUR AGENT SERVICE KEY]
CONTRAST__API__API_KEY: [REPLACE WITH YOUR AGENT API KEY]
```

4. 前の手順で指定した設定を使用して、アプリケーションをデプロイします。
5. アプリケーションがロードされたら、アプリケーションを疎通して、Contrast でサーバとアプリケーションがアクティブになり、脆弱性が報告されることを確認します。



### 重要

Contrast エージェントを実行中の Web アプリケーションを再デプロイする際に、*ContrastProfiler.dll* でファイルが使用中というエラーが発生することがあります。これは、エージェントの DLL ファイルが .NET によってロックされており、アプリケーションの実行中には上書きできないために発生します。

## Azure App Service で .NET Core エージェントをインストール

インストールを開始する前に、[システム要件 \(197ページ\)](#)と[サポート対象テクノロジー \(196ページ\)](#)を確認し、インストールが可能で最適なパフォーマンスを得られる環境であることを確認してください。

Azure Portal の拡張機能を使用して、.NET Core エージェントを簡単にインストールするには、以下の手順を行います。

1. [Azure アカウント](#)がない場合は、アカウントを作成してください。
2. [.NET Core Web アプリケーション](#)を作成し、Azure App Service にデプロイします。
3. アプリケーションを Azure に公開し、Contrast エージェントなしで想定どおりに機能することを確認します。
4. アプリケーションが Windows プランを使用してデプロイされていることを確認します(Linux プランの場合は、拡張機能を利用できません)。



### 注記

拡張機能を利用できない場合は、[NuGet を使用して .NET Core エージェントを手動でインストール \(201ページ\)](#)できます。

5. App Service でデプロイ中のアプリケーションを選択します。
6. **設定より構成**を選択し、エージェントが Contrast サーバに接続するための設定をします。
7. **新しいアプリケーションの設定**を選択し、以下の値を指定します。

キー	値
CONTRAST__API__USER_NAME	自分の <a href="#">エージェントユーザ名 (37ページ)</a> を指定します。
CONTRAST__API__SERVICE_KEY	自分の <a href="#">エージェントサービスキー (37ページ)</a> を指定します。
CONTRAST__API__API_KEY	自分の <a href="#">API キー (37ページ)</a> を指定します。
CONTRAST__API__URL	デフォルトは、 <a href="https://app.contrastsecurity.com">https://app.contrastsecurity.com</a> です。別の場所でホストされている Contrast サーバを使用する場合は、その URL を指定します。

8. **メニュー画面より拡張機能**を選択します。

9. **+ 追加**を選択します。
10. 拡張機能の選択をクリックし、一覧より **Contrast .NET Core Site Extension for Azure App Service** を選択します。これが、.NET Core アプリケーション用の拡張機能になります。
11. 法律条項に同意して、**OK** ボタンをクリックします。
12. 拡張機能のインストールが完了するまでしばらく待ったら、正しくインストールされていることを確認します。
13. アプリケーションの概要に戻り、アプリケーションを**再起動**します。
14. アプリケーションを疎通し、**検査結果**が Contrast に報告されることを確認します。



### ヒント

アプリケーションの SCM サイト(Kudu)の「Site Extensions」メニューからも Contrast エージェントをインストールできます。



### 重要

.NET Core エージェントの新しいバージョンが利用可能な場合は、Azure Portal または Kudu のダッシュボードに通知されます。エージェントの更新を行う前にサイトを停止してください。停止しない場合、更新が失敗する可能性があります。



### 注記

サイトの拡張機能により、以下のような環境変数がいくつか設定されます。

```
CORECLR_ENABLE_PROFILING=1
CORECLR_PROFILER={8B2CE134-0948-48CA-A4B2-80DDAD9F5791}
CORECLR_PROFILER_PATH_32=D:\Home\siteextensions\Contrast.NetCore
.Azure.SiteExtension\ContrastNetCoreAppService\runtimes\win-
x86\native\ContrastProfiler.dll
CORECLR_PROFILER_PATH_64=D:\Home\siteextensions\Contrast.NetCore
.Azure.SiteExtension\ContrastNetCoreAppService\runtimes\win-
x64\native\ContrastProfiler.dll
CONTRAST_INSTALL_DIRECTORY=D:\Home\siteextensions\Contrast.NetCore
.Azure.SiteExtension\ContrastNetCoreAppService\
MicrosoftInstrumentationEngine_ConfigPath32_ContrastCoreX86Confi
g=D:\Home\siteextensions\Contrast.NetCore.Azure.SiteExtension\Co
ntrastCieCoreClrProfiler-32.config
MicrosoftInstrumentationEngine_ConfigPath64_ContrastCoreX64Confi
g=D:\Home\siteextensions\Contrast.NetCore.Azure.SiteExtension\Co
ntrastCieCoreClrProfiler-64.config
```

CLR Instrumentation Engine (CIE)がアプリケーションに設定されている場合(例えば、Application Insights が有効になっているために)、Azure は自動的に `CORECLR_PROFILER*`変数を上書きし、CIE のプロファイラが指すようにします。

そして、CIE は `MicrosoftInstrumentationEngine_*`変数を使用して Contrast エージェントをロードするようになります。

アプリケーションに対して CIE が設定されていない場合は、Contrast エージェントのロードに標準の `CORECLR_PROFILER*`変数が使用されます。

## IIS 用 .NET Core エージェントのインストーラで .NET Core エージェントをインストール


IIS 用 .NET Core エージェントのインストーラは、標準の MSI を利用して作られた Windows アプリケーションの一般的なインストーラです。インストーラは、対象となるサーバが要件(サーバのオペレーティングシステムがサポート対象であることなど)を満たしているかを検証します。サーバが全ての要件を満たしていれば、インストーラによって以下が行われます。

- IIS 用 .NET Core エージェントを Windows の標準プログラムとして登録します。
- 指定された場所(例、C:\Program Files\Contrast\dotnet-core)にエージェントのファイルを配置します。これには、いくつかのダイナミックリンクライブラリ(DLL)などが含まれます。
- エージェントのログファイルや設定を主に保存するためのデータディレクトリ(例、C:\ProgramData\Contrast\dotnet-core)を作成します。
- IIS に .NET Core エージェントのネイティブモジュールを追加します。

### インストールを行う前に

インストールを開始する前に、[システム要件 \(197ページ\)](#)と[サポート対象テクノロジー \(196ページ\)](#)を確認し、インストールを行うことができ、最適なパフォーマンスを得られることを確認してください。

### Contrast を使用してエージェントをインストール

1. Contrast Web インターフェイスで、**新規登録**を選択します。
2. **エージェントを選択**のドロップダウンメニューから .NET Core を選択します。
3. **IIS でのインストール**の下で、**IIS 用 .NET Core エージェントインストーラ**のリンク  を選択します。ZIP アーカイブがダウンロードされます。
4. ダウンロードした ZIP アーカイブを Web サーバ上で解凍したら、contrast-dotnet-core-agent-for-iis-installer.exe を実行します。これで、IIS 用の .NET Core エージェントがインストールされます。



#### ヒント

コマンドラインを使用してインストールすると、IIS 用 .NET Core エージェントインストーラでサポートされるその他のオプションを利用できます。

5. [YAML 設定ファイルを使用して .NET Core エージェントを設定 \(214ページ\)](#)し、[認証キー \(37ページ\)](#)およびアプリケーション固有の設定を指定します。
6. YAML ファイルを C:\ProgramData\Contrast\dotnet-core にコピーします(まだコピーしていない場合)。
7. IIS を再起動して変更を反映します。
8. 通常通りにアプリケーションを疎通し、Contrast でアプリケーションが認識されていることを確認します。

### コマンドラインを使用してエージェントをインストール

コマンドラインを使用すると、IIS 用 .NET Core エージェントインストーラでサポートされるその他のオプションを利用できます。

IIS 用 .NET Core エージェントは、Windows のインターフェイスを使用してインストールでき、Windows の標準機能(コントロールパネルのプログラムと機能や Powershell など)を使用して、アンインストールや修復を行うことができます。ただし、自動化されたスクリプトなどの特定のシナリオでは、IIS 用 .NET Core エージェントのインストーラを使用して、以下の操作を実行する場合があります。

有人モードには、以下のコマンドを使用します。

- **インストール** : `contrast-dotnet-core-agent-for-iis-installer.exe`
- **アンインストール** : `contrast-dotnet-core-agent-for-iis-installer.exe -uninstall`
- **修復** : `contrast-dotnet-core-agent-for-iis-installer.exe -repair`

無人モードまたはサイレントモードには、以下のコマンドを使用します。

- **インストール** : `contrast-dotnet-core-agent-for-iis-installer.exe -s SUPPRESS_RESTARTING_IIS=1`
- **アンインストール** : `contrast-dotnet-core-agent-for-iis-installer.exe -uninstall -s SUPPRESS_RESTARTING_IIS=1`

- **修復**: `contrast-dotnet-core-agent-for-iis-installer.exe -repair -s SUPPRESS_RESTARTING_IIS=1`

コマンドラインを使用してインストールすると、IIS 用.NET Core エージェントインストーラで利用できるその他のオプションがあります。

オプション	説明	例
INSTALLFOLDER	エージェントファイルのインストールディレクトリを指定します。	INSTALLFOLDER=C:\Program Files\Contrast\dotnet-core
AGENT_EXPLORER_INSTALLFOLDER	Agent Explorer のファイルのディレクトリを指定します。	AGENT_EXPLORER_INSTALLFOLDER="C:\Program Files\Contrast\agent-explorer"
INSTALL_AGENT_EXPLORER	Agent Explorer をインストールしない場合は、このオプションの値を 0 に設定して下さい。  デフォルトの値は 1 で、Agent Explorer はインストールされます。	INSTALL_AGENT_EXPLORER=1
DATAFOLDER	エージェントのログファイルと設定ファイルのデフォルトの場所を指定します。	DATAFOLDER=C:\ProgramData\Contrast\dotnet-core
SUPPRESS_RESTARTING_IIS	このオプションの値を 1 に設定すると、インストーラは IIS を再起動しません。  デフォルトの値は、0 です。	SUPPRESS_RESTARTING_IIS=0
<div style="display: flex; align-items: center; justify-content: center;">  <div> <p><b>注記</b></p> <p>IIS が再起動されるまで、アプリケーションにエージェントは組み込まれません。</p> </div> </div>		
INSTALL_UPGRADE_SERVICE	エージェントアップグレードサービスをインストールしない場合は、このオプションの値を 0 に設定して下さい。  デフォルトの値は 1 で、エージェントアップグレードサービスはインストールされます。	INSTALL_UPGRADE_SERVICE=1
UPGRADE_SERVICE_INSTALLFOLDER	アップグレードサービスのファイルのディレクトリを指定します。	UPGRADE_SERVICE_INSTALLFOLDER="C:\Program Files (x86)\Contrast\upgrade-service"



**重要**

IIS 用.NET Core エージェントインストーラは、エージェントを初めてインストールする際に IIS を自動的に再起動します。必要があれば、IIS の再起動時に警告を発するよう Web サーバ監視ツールの設定を変更してください。

.NET プロファイル API では、プロファイルするプロセスをプロファイラで起動する必要があります。そのため、.NET Core エージェントは Contrast プロファイラをロードするために IIS(および IIS のワーカースレッド)を再起動する必要があります。この処理は、他のプロファイル製品(例、メモリやパフォーマンスプロファイラなど)の動作と同様です。

## コンテナを使用して .NET Core エージェントをインストール

### インストールを行う前に

本項では、Docker を例として、コンテナ化されたアプリケーションに Contrast .NET Core エージェントをインストールするための一般的な手順について説明します。

コンテナや関連ソフトウェアの仕組みを基本的に理解している必要があります。必要に応じて、お客様の環境に合わせて手順を調整してください。

### 手順 1：エージェントをインストール

Contrast エージェントは、アプリケーションをコンテナイメージに追加する前または後のどちらでも追加できます。推奨される方法は、名前を付けた [マルチステージビルド](#) を使用することです。例：

```
FROM mcr.microsoft.com/dotnet/aspnet:6.0

# Hidden for brevity...

# Copy the required agent files from the official Contrast agent image.
COPY --from=contrast/agent-dotnet-core:latest /contrast /contrast
```

この例では、最新の .NET Core エージェントを使用します(利用可能なタグは DockerHub で確認してください)。

### 手順 2：エージェントを設定

Contrast エージェントは、複数のソースからの設定を受け入れますが、設定の優先順位は [優先順位 \(36ページ\)](#) セクションに記載されています。

設定方法を組み合わせて利用することをお勧めします。

- YAML ファイルを使用して、複数のアプリケーションで共有する共通の設定を指定します。
- アプリケーション固有の設定値や、YAML ファイルで指定した値を上書きする場合や、実行時に組み込む機密情報などには、環境変数を使用します。

#### YAML ファイルの設定：

[YAML ファイル \(38ページ\)](#) を使用してエージェントを設定する場合に、環境変数の `CONTRAST_CONFIG_PATH` を使用して、YAML ファイルがコンテナ内のどこにあるかを指定することもできます。

例えば、`contrast_security.yaml` という名前の YAML 設定ファイルが Docker のビルドコンテキストに存在するとします。

環境変数 `CONTRAST_CONFIG_PATH` を使用して、YAML ファイルの場所を指定することもできます。

```
agent:
  logger:
    path: /var/tmp
    level: WARN
```

YAML ファイルは、以下のようにコンテナイメージに追加することができます。

```
FROM mcr.microsoft.com/dotnet/aspnet:6.0

# Hidden for brevity...


# Add the Contrast agent to the image.
COPY --from=contrast/agent-dotnet-core:latest /contrast /contrast
```

```
# Copy the contrast_security.yaml file from Docker build context.
COPY ./contrast_security.yaml /contrast_security.yaml

# Finally configure the agent to use the YAML file previously \
copied.
ENV CONTRAST_CONFIG_PATH=/contrast_security.yaml
```

**環境変数の設定 :**

アプリケーション固有の設定を指定するには、[環境変数 \(56ページ\)](#)を使用します。以下は、一般的によく使用される設定オプションです。

項目	用途	環境変数
アプリケーション名	Contrast サーバに報告されるアプリケーション名を指定します。	CONTRAST__APPLICATION__NAME
アプリケーショングループ	オンボード時にこのアプリケーションと関連付けるアクセスグループを指定します。	CONTRAST__APPLICATION__GROUP
 <b>注記</b> アプリケーションのアクセスグループは、先に Contrast で作成しておく必要があります。		
アプリケーションのタグ	アプリケーションにタグを追加します。	CONTRAST__APPLICATION__TAGS
サーバ名	Contrast に報告されるサーバ名を指定します。	CONTRAST__SERVER__NAME
サーバの環境	アプリケーションを実行する環境を指定します。このオプションで有効な値 : Development、QA、Production	CONTRAST__SERVER__ENVIRONMENT
サーバのタグ	サーバにタグを追加します。	CONTRAST__SERVER__TAG

**手順 3 : プロファイル変数と認証情報を追加**

アプリケーションに .NET エージェントを組み込んで検査を行うには、[さらに環境変数 \(198ページ\)](#)が必要です。CORECLR\_ 変数はエージェントをロードし、CONTRAST\_ 変数は Contrast サーバに対するエージェントの認証用です。

前述の Dockerfile の例を使用すると、以下のようになります。

```
FROM mcr.microsoft.com/dotnet/aspnet:6.0

# Hidden for brevity...

COPY --from=contrast/agent-dotnet-core:latest /contrast /contrast

# Required variables to load the agent.
ENV CORECLR_PROFILER_PATH_64=/contrast/runtimes/linux-x64/native/ContrastProfiler.so \
    CORECLR_ENABLE_PROFILING=1 \
    CORECLR_PROFILER={8B2CE134-0948-48CA-A4B2-80DDAD9F5791}
```

サーバへのエージェントの認証には、以下の環境変数に [API の値 \(37ページ\)](#)を設定する必要があります。

```
CONTRAST__API__URL=https://app.contrastsecurity.com/Contrast
CONTRAST__API__API_KEY={Your API KEY here}
CONTRAST__API__SERVICE_KEY={Your Service key here}
CONTRAST__API__USER_NAME={Your agent username here}
```



API の値([エージェントキー \(37ページ\)](#))は Contrast Web インターフェイスで確認するか、.NET Core エージェント用の YAML ファイルをダウンロードすることで取得できます。



### 重要

API\_KEYSERVICE\_KEY、USER\_NAME の各キーは、機密データとなりますので、取り扱いにはご注意ください。Contrast では、これらのデータは、シークレットストア(例: Kubernetes Secret など)から実行時に取り込むことをお勧めします。

## 手順 4 : アプリケーションを検査

これで、Contrast を有効にしてアプリケーションイメージを実行できます。アプリケーションの起動時に Contrast エージェントが組み込まれて解析が始まり、Contrast サーバに脆弱性が報告されます。Contrast が実行されているかを確認するには、コンテナをチェックしてください。

## エージェントアップグレードサービス

エージェントアップグレードサービスは、Windows のバックグラウンドサービスで、Windows 上の .NET Framework エージェントおよび IIS 用 .NET Core エージェントを最新のバージョンに自動的に更新することができます。エージェントアップグレードサービスは、.NET Framework エージェントのインストーラと IIS 用 .NET Core エージェントのインストーラに含まれており、エージェントインストーラは以下の 2 つの製品をインストールします。

- 該当のエージェント
- エージェントアップグレードサービス

デフォルトでは、エージェントアップグレードサービスは、サービスの初回起動時(Windows Server の再起動時)に、NuGet にリリースされている新しいエージェントをチェックします。新しいエージェントのバージョンが見つかった場合、アップグレードサービスは、新しいバージョンをダウンロードし、インストーラの署名を検証してから、最後にインストーラを実行します。

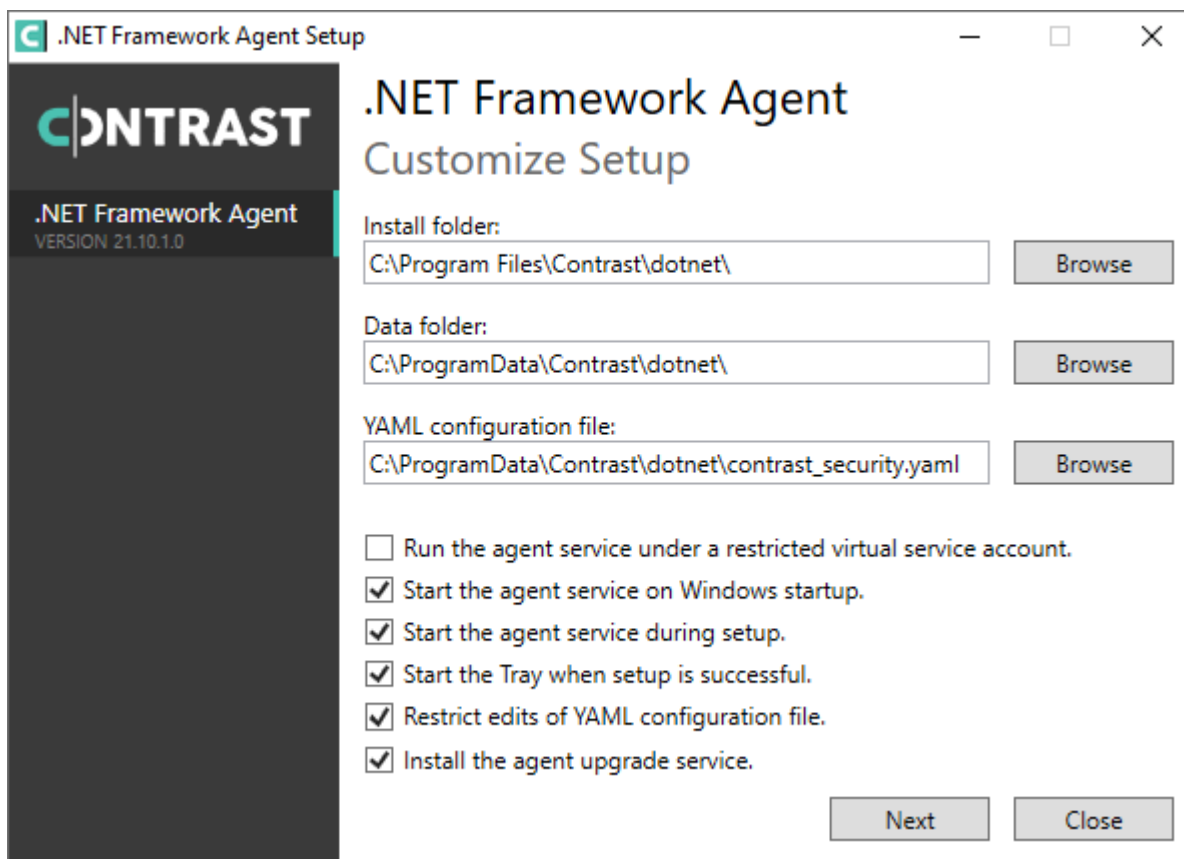


### 注記

新しいバージョンのエージェントがインストールされると、IIS は再起動されます。

エージェントアップグレードサービスはオプションコンポーネントであり、エージェントの Assess および Protect 機能には必須ではありません。

- エージェントアップグレードサービスを使用しない場合は、**Install the agent upgrade service**(エージェントアップグレードサービスをインストールする)のチェックボックスをオフにしてください。
- コマンドラインでエージェントをインストールする場合は、INSTALL\_UPGRADE\_SERVICE=0 の引数を追加すれば、エージェントアップグレードサービスはインストールされません。



エージェントアップグレードサービスの動作は、Contrast のデータディレクトリにあるエージェント用の設定ファイルで変更できます。デフォルトの場所は、C:\ProgramData\Contrast\upgrade-service です。

.NET Core エージェントをアップグレードする際の設定は、.NET Core エージェントの YAML ファイル内にあります。

```
enable: true # Set to `true` for the agent to automatically upgrade to \
newer versions.
checks: Startup # Set the frequency with which the agent checks for \
updates. Valid values are `daily` for every 24 hours and on startup, or \
`startup` for *only* when service starts up.
timeout_ms: 60000 # Set the time allocated to execute the downloaded agent \
installer before cancelling.
nuget_repository_url: https://api.nuget.org/v3/index.json # Set the URL of \
the Nuget repository to be used for the .NET Core Agent for IIS Installer
nuget_package_name: Contrast.CoreIIS.Installer # Set the name of the .NET \
Core Agent for IIS Nuget package.
installer_upgrade_code: 82468c04-dfc0-4a4c-9eb9-c4b314c67fdc # Used \
internally to retrieve the current installed agent version from Windows.
```



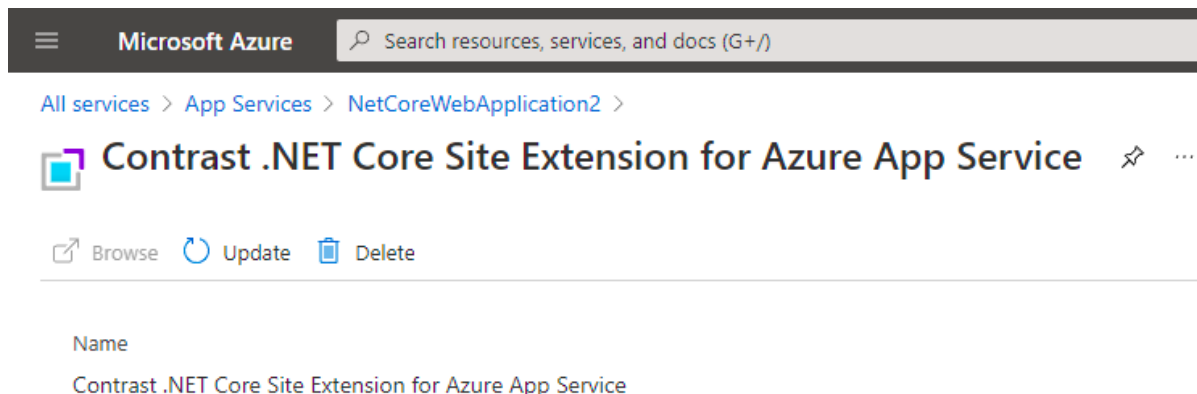
### 注記

エージェントアップグレードサービスは、エージェントインストーラにのみ含まれます。手動で取得する .NET Core エージェント、エージェントの NuGet パッケージ、Azure App Service のサイト拡張機能には含まれません。

## .NET Core エージェントのアップデート

Contrast エージェントは新しいバージョンが頻繁にリリースされますが、ここでは、NuGet パッケージや手動で .NET Core エージェントを簡単にアップデートし最新にする方法について説明します。インストールの種別により、以下の方法でアップデートします。

- **IIS 用 .NET Core エージェントのインストーラ** : [エージェントアップグレードサービス \(150ページ\)](#) を使用します。
- **Azure App Service** : Azure Portal を使用します。



- **手動インストール** : 以下の手順に従い、独自に自動化を設定します。

### 開始する前に

- Contrast .NET Core エージェントを使用しない状態で .NET Core アプリケーションが正常に実行されることを確認します。
- 事前に Contrast .NET Core エージェントをインストールしておきます。
- 変更管理ポリシーと使用する環境に基づいて、エージェントをアップデートする方法とタイミングを決めます。
- アプリケーションの依存関係とアップデートを管理するワークフローを決めます。

### 手順

1. Contrast .NET Core エージェントを同じインストール場所にダウンロードしますが、Contrast リポジトリを使用します。
  - SaaS 版の Contrast をご利用の場合 : .NET Core エージェントは公開 NuGet リポジトリの最新リリースと同期されています。
  - オンプレミス版の Contrast をご利用の場合 : お使いの Contrast インスタンスより新しいバージョンの Contrast エージェントを使用することは推奨されません。Contrast Web インターフェイスからダウンロードできるものと同じバージョンの .NET Core エージェントのバージョンを使用してください。
2. 次の API 情報を準備します。

```
CONTRAST_URL=<TeamServer URL e.g. https://app.contrastsecurity.com >  
ORG_ID=<YOUR TEAMSERVER ORGANIZATION ID>  
AUTH_TOKEN=<YOUR TEAMSERVER AUTHENTICATION TOKEN>  
API_KEY=<YOUR TEAMSERVER API KEY>
```

3. 次のいずれかのスクリプトを使用して、Contrast .NET Core エージェントをダウンロードします。アプリケーションの起動スクリプトや自動化されたデプロイメントパイプライン、cron ジョブなどにこのスクリプトを追加すると、エージェントを自動的にアップデートできます。
  - Bash スクリプト

```
CONTRAST_URL=https://app.contrastsecurity.com  
ORG_ID=xxxx
```

```
AUTH_TOKEN=xxxx
API_KEY=xxxx
curl -X GET $CONTRAST_URL/Contrast/api/ng/$ORG_ID/agents/default/
DOTNET_CORE /-o ./Contrast.NET.Core.zip -H 'Authorization: \
$AUTH_TOKEN' -H 'API-Key: $API_KEY' /-H 'Accept: application/json' -OJ
```

- Powershell

```
$ContrastUrl = "https://app.contrastsecurity.com/Contrast"
$UserId = ""
$ServiceKey = ""
$ApiKey = ""
$OrganizationId = ""
$InstallPath = ".\dotnet-core"

# Needed if the OS defaults to Tls1.1.
[Net.ServicePointManager]::SecurityProtocol = \
[Net.SecurityProtocolType]::Tls12

New-Item -ItemType Directory $InstallPath

Invoke-WebRequest `
  -Uri "$ContrastUrl/api/ng/$OrganizationId/agents/default/
DOTNET_CORE" `
  -Headers @{
    "API-Key" = $ApiKey
    "Authorization" = \
[Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes("$
{UserId}:${ServiceKey}"))
  } `
  -OutFile "$InstallPath\Contrast.zip"

Invoke-WebRequest -Uri `
  "$ContrastUrl/api/ng/$OrganizationId/agents/external/default/
DOTNET_CORE" `
  -Headers @{
    "Accept" = "text/yaml"
    "API-Key" = $ApiKey
    "Authorization" = \
[Convert]::ToBase64String([System.Text.Encoding]::UTF8.GetBytes("$
{UserId}:${ServiceKey}"))
  } `
  -OutFile "$InstallPath\contrast_security.yaml"

Expand-Archive "$InstallPath\Contrast.zip" -DestinationPath \
$InstallPath
Remove-Item "$InstallPath\Contrast.zip"
```

4. ダウンロードしたファイルを解凍して、現在の Contrast エージェントの配置場所に保存します。配置する場所がわからない場合は、お使いのシステムの以下のコマンドで環境変数を調べてください。

- Windows(64 ビット)

```
echo %CORECLR_PROFILER_PATH_64%CORECLR_PROFILER_PATH_64
```

- Windows(32 ビット)

```
CORECLR_PROFILER_PATH_32
```

- Linux(64 ビット)

```
CORECLR_PROFILER_PATH_64
```

- Powershell

```
printenv CORECLR_PROFILER_PATH_64
```

## .NET Core エージェントの設定

全てのエージェントには[基本の設定 \(35ページ\)](#)があり、設定値には[優先順位 \(36ページ\)](#)があります。

ご利用の環境に合わせて、.NET Core エージェントを設定してください。

- [Azure App Service \(213ページ\)](#)
- [環境変数 \(213ページ\)](#)
- [YAML 設定ファイル \(214ページ\)](#)
- [インテグレーション \(618ページ\)](#)



### ヒント

[Contrast エージェント設定エディタ \(39ページ\)](#)を使用すると、YAML 設定ファイルの作成やアップロード、YAML の検証、推奨される設定値の表示などができます。

## Azure App Service の.NET Core エージェントを設定

Azure App Service を使用している場合、次の方法で.NET Core エージェントを設定できます。

- **Azure Portal** : [環境変数 \(213ページ\)](#)を使用して.NET Core エージェントを設定します。  
環境変数の構文を使用して、**構成メニューのアプリケーション設定**の画面で全ての設定を追加します。
- **Web.config ファイルの環境変数** : `<aspNetCore>` 要素の`<environmentVariables>`セクションに、環境変数の構文を使用してオーバーライドを指定します。
- **YAML 設定ファイル** : アプリケーションのデプロイメントに含めるか、Kudu コンソールを使用して、このファイルを Azure Web アプリケーションにアップロードします。  
**構成アプリケーション設定**画面で、`CONTRAST_CONFIG_PATH` という新しいアプリケーション設定を追加して、このファイルを指す値を指定します。  
例えば、アプリケーションルートの `contrast_security.yaml` ファイルを使用するには、**構成アプリケーション設定**画面にアクセスし、`CONTRAST_CONFIG_PATH` というキーに `D:\Home\site\wwwroot\contrast_security.yaml` という値で、新しいアプリケーション設定を追加します。Azure App Service のアプリケーションファイルが、`D:\home\site\wwwroot` にデプロイされます。

### 関連項目

- [Azure App Service で.NET Core エージェントをインストール \(203ページ\)](#)

## 環境変数を使用して.NET Core エージェントを設定する

環境変数は、いくつかの方法で設定できます。

- IIS では、[web.config ファイルを使用してアプリケーションの環境変数を設定できます](#)。
- Azure App Service では、Web サイトの環境変数を設定するための UI が Azure プラットフォームに用意されています。
- 開発時には、`launchSettings.json` ファイルを使用して、起動されるアプリケーションの環境変数を設定できます。



### ヒント

.NET Core エージェントの [YAML テンプレート \(214ページ\)](#)にあるプロパティは、いずれも環境変数に変換できます。

- エージェントのログレベル(`agent.logger.level`)を"TRACE"に変更するには、`CONTRAST__AGENT__LOGGER__LEVEL` というキーに"TRACE"という値を指定します。
- エージェントのサーバ名(`server.name`)を"MyServer"に変更するには、`CONTRAST__SERVER__NAME` というキーに"MyServer"という値を指定します。

最も一般的な設定のいくつかは次のとおりです。

環境変数	目的
<code>CONTRAST__APPLICATION__NAME</code>	Contrast サーバに報告されるアプリケーション名を指定
<code>CONTRAST__APPLICATION__GROUP</code>	このアプリケーションを関連付けるアクセスグループを指定( <a href="#">アクセスグループ (708ページ)</a> は作成済みであること)。
<code>CONTRAST__APPLICATION__SESSION__METADATA</code>	Contrast でセッションの新規作成時に使用されるメタデータを指定。エージェントによって検出された脆弱性は、この新しいセッションメタデータに関連付けられます。
<code>CONTRAST__SERVER__NAME</code>	Contrast に報告されるサーバ名を指定
<code>CONTRAST__SERVER__ENVIRONMENT</code>	アプリケーションを実行する環境を指定(Development、QA、Production)

その他の利用可能なプロパティの説明は、[.NET Core エージェントの YAML テンプレート \(214ページ\)](#)を参照してください。

### .NET Core の YAML 設定ファイルのテンプレート

YAML 設定ファイルを使用して.NET Core エージェントを設定する場合には、以下のテンプレートをご利用ください(YAML 設定については、[YAML 設定の説明 \(38ページ\)](#)を参照してください)。

YAML 設定ファイルは、デフォルトの場所に配置します。

- **Windows** : `C:/ProgramData/contrast/dotnet-core/contrast_security.yaml`
- **Unix** : `/etc/contrast/dotnet-core/contrast_security.yaml`

```
# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==

# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
```

```
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# Set the version of the TLS protocol the agent uses to communicate with \
the
# Contrast UI. The .NET agent default behavior is \
(SecurityProtocolType.Tls
# | SecurityProtocolType.Tls11 | SecurityProtocolType.Tls12).
# tls_versions: tls|tls11|tls12

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Determine the location from which the agent loads a client
# certificate. Value options include `File` or `Store`.
# certificate_location: NEEDS_TO_BE_SET

# Set the absolute path to the client certificate's
# .CER file for communication with Contrast UI. The
# `certificate_location` property must be set to `File`.
# cer_file: NEEDS_TO_BE_SET
```

```
# Specify the name of certificate store to open. The
# `certificate_location` property must be set to `Store`.
# Value options include `AuthRoot`, `CertificateAuthority`,
# `My`, `Root`, `TrustedPeople`, or `TrustedPublisher`.
# store_name: NEEDS_TO_BE_SET

# Specify the location of the certificate store. The
# `certificate_location` property must be set to `Store`.
# Value options include `CurrentUser` or `LocalMachine`.
# store_location: NEEDS_TO_BE_SET

# Specify the type of value the agent uses to find the certificate
# in the collection of certificates from the certificate store.
# The `certificate_location` property must be set to `Store`.
# Value options include `FindByIssuerDistinguishedName`,
# `FindByIssuerName`, `FindBySerialNumber`,
# `FindBySubjectDistinguishedName`, `FindBySubjectKeyIdentifier`,
# `FindBySubjectName`, or `FindByThumbprint`.
# find_type: NEEDS_TO_BE_SET

# Specify the value the agent uses in combination with
# `find_type` to find a certification in the certificate store.
#
# Note - The agent will use the first certificate from
# the certificate store that matches this search criteria.
#
# find_value: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate
# with the Contrast web interface over a proxy. Set
# value to `false` if you don't want to use the proxy.
# enable: NEEDS_TO_BE_SET

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# Set the proxy user.
# user: NEEDS_TO_BE_SET

# Set the proxy password.
# pass: NEEDS_TO_BE_SET

# Set the proxy authentication type. Value
# options are `NTLM`, `Digest`, and `Basic`.
# auth_type: NEEDS_TO_BE_SET
```



```
# \  
=====  
==  
# agent  
# Use the properties in this section to control the way and frequency  
# with which the agent communicates to logs and the Contrast UI.  
# \  
=====  
==  
# agent:  
  
# \  
=====  
# agent.logger  
# Define the following properties to set logging values.  
# If the following properties are not defined, the  
# agent uses the logging values from the Contrast UI.  
# \  
=====  
# logger:  
  
# Set the the log output level. Valid options are  
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.  
# level: INFO  
  
# Set to `true` to redirect all logs to  
# `stdout` instead of the file system.  
# stdout: false  
  
# Set the roll size for log files in megabytes. The agent will  
# attempt to prevent the log file from being larger than this size.  
# roll_size: 100  
  
# Set the number of backup files to keep. Set to `0` to disable.  
# backups: 10  
  
# \  
=====  
# agent.security_logger  
# Define the following properties to set security  
# logging values. If not defined, the agent uses the  
# security logging (CEF) values from the Contrast UI.  
# \  
=====  
# security_logger:  
  
# Set the log level for security logging. Valid options  
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.  
# level: ERROR  
  
# \  
=====  
# agent.security_logger.syslog  
# Define the following properties to set Syslog values. If the \  

```

```
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# Set the connection type used for Syslog messages.
# Value options are `UNENCRYPTED` and `ENCRYPTED`.
# connection_type: UNENCRYPTED

# \
=====
# agent.dotnet
# The following properties apply to any .NET agent-wide configurations.
# \
=====
# dotnet:

# Set a list of application pool names that the agent does not
```

```
# instrument or analyze. Names must be formatted as a comma-separated
# list. New after .NET Framework 19.1.3 and .NET Core 4.0.2.
# app_pool_denylist: NEEDS_TO_BE_SET

# Set a list of application pool names that the agent instruments or
# analyzes. If set, other application pools are ignored. Allowlist takes
# precedence over denylist. Names must be formatted as a comma-separated
# list. New after .NET Framework 19.1.3 and .NET Core 4.0.2.
# app_pool_allowlist: NEEDS_TO_BE_SET

# Set a list of application names that the agent does not
# analyze. (The applications are still instrumented).
# Names must be formatted as a comma-separated list.
# New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# application_denylist: NEEDS_TO_BE_SET

# Set a list of application names that the agent analyzes.
# If set, other applications are not analyzed, but are
# still instrumented. Allowlist takes precedence over
# denylist. Names must be formatted as a comma-separated
# list. New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# application_allowlist: NEEDS_TO_BE_SET

# Enable a profiler chaining feature to allow Contrast to
# work alongside other tools that use the CLR Profiling
# API. Defaults to `true`. New after .NET Framework 19.1.3
# (Installed Only) and .NET Core 1.9.3 (Installed Only).
# enable_chaining: true

# Indicate that the agent should allow CLR optimizations
# of JIT-compiled methods. Defaults to `true`. New
# after .NET Framework 19.1.3 and .NET Core 1.0.0.
# enable_instrumentation_optimizations: true

# Indicate that the agent should allow the CLR to inline
# methods that are not instrumented by Contrast. Defaults to
# `true`. New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# enable_jit_inlining: true

# Indicate that the agent should allow the CLR to perform
# transparency checks under full trust. Defaults to `false`.
# New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# enable_transparency_checks: false

# Set to display ASCII art to std::out on agent startup. Defaults
# to `true`. New after .NET Framework 20.6.3 and .NET Core 1.0.0.
# enable_cat: true

# Sets the maximum amount of time a Protect regular expression
# is allowed to run before being cancelled. Set to -1 to never
# cancel regular expression execution. Defaults to `20_000`.
# New after .NET Framework 20.4.3 and .NET Core 1.5.0.
# protect_searchers_single_pattern_deadline_ms: 20_000

# Sets the maximum amount of time a 'Probe Analysis' Protect
```

```
# regular expression is allowed to run before being cancelled. Set
# to -1 to never cancel regular expression execution. Defaults to
# `5_000`. New after .NET Framework 20.7.3 and .NET Core 1.5.11.
# protect_searchers_probe_analysis_single_pattern_deadline_ms: 5_000

# Sets the maximum amount of time a Protect rule is
# allowed to run before being cancelled. Set to -1 to never
# cancel Protect rule execution. Defaults to `60_000`.
# New after .NET Framework 20.4.3 and .NET Core 1.5.0.
# protect_searchers_total_rule_deadline_ms: 60_000

# Sets the maximum amount of time a 'Probe Analysis' Protect
# rule is allowed to run before being cancelled. Set to -1 to
# never cancel Protect rule execution. Defaults to `10_000`.
# New after .NET Framework 20.7.3 and .NET Core 1.5.11.
# protect_searchers_probe_analysis_total_rule_deadline_ms: 10_000

# Sets the maximum duration of time agent log files should be kept
# since last write before being deleted by the agent. Defaults to
# `604_800_000`. New after .NET Framework 20.6.1 and .NET Core 1.5.5.
# log_cleanup_maximum_age_ms: 604_800_000

# Suppresses gathering process-level metrics (process level metrics are
# gathered by default), used to identify performance problems. Metric
# counters may further decrease the stability of already unstable
# systems and can be disabled (set to true) if issues occur. Defaults
# to `false`. New after .NET Framework 20.6.6 and .NET Core 1.5.10.
# suppress_metric_counters: false

# Enable file based application watching. Set to false if
# file watching is causing locking issues. Defaults to `true`.
# New after .NET Framework 20.7.3 and .NET Core 1.5.11.
# enable_file_based_app_watching: true

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
```

```
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Control the values captured by Assess vulnerability events. `Full`
# captures most values by calling ToString on objects, which can
# provide more info but causes increased memory usage. `Minimal`
# has better performance as it only captures String type objects
# as strings and uses type name for other object type values.
# event_detail: minimal

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Value options are `ALL`, `SOME`, or `NONE`.
# stacktraces: ALL

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
```

```

# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
# protect.rules
# Use the following properties to set simple rule configurations.
# \
=====
# rules:

# Define a list of Protect rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
# protect.rules.bot-blocker
# Use the following selection to configure if the
# agent blocks bots. Set to `true` to enable blocking.
# \
=====
# bot-blocker:

# Set to `true` for the agent to block known bots.
# enable: false

# \
=====
# protect.rules.sql-injection
# Use the following settings to configure the sql-injection rule.

```

```
# \  
=====
```

```
# sql-injection:
```

```
  # Set the mode of the rule. Value options are  
  # `monitor`, `block`, `block_at_perimeter`, or off.  
  #  
  # Note - If a setting says, "if blocking is enabled",  
  # the setting can be `block` or `block_at_perimeter`.  
  #  
  # mode: off
```

```
# \  
=====
```

```
# protect.rules.sql-injection-semantic-chaining  
# Use the following properties to configure how the  
# sql injection semantic analysis chaining rule works.  
# \  
=====
```

```
# sql-injection-semantic-chaining:
```

```
  # Set the mode of the rule. Value options  
  # are `monitor`, `block` or `off`.  
  # mode: off
```

```
# \  
=====
```

```
# protect.rules.sql-injection-semantic-dangerous-functions  
# Use the following properties to configure how the sql  
# injection semantic analysis dangerous functions rule works.  
# \  
=====
```

```
# sql-injection-semantic-dangerous-functions:
```

```
  # Set the mode of the rule. Value options  
  # are `monitor`, `block` or `off`.  
  # mode: off
```

```
# \  
=====
```

```
# protect.rules.sql-injection-semantic-suspicious-unions  
# Use the following properties to configure how the sql  
# injection semantic analysis suspicious unions rule works.  
# \  
=====
```

```
# sql-injection-semantic-suspicious-unions:
```

```
  # Set the mode of the rule. Value options  
  # are `monitor`, `block` or `off`.  
  # mode: off
```

```
# \  
=====
```

```
# protect.rules.sql-injection-semantic-tautologies  
# Use the following properties to configure how the sql
```

```
# injection semantic analysis tautologies rule works.
# \
=====
# sql-injection-semantic-tautologies:

# Set the mode of the rule. Value options
# are `monitor`, `block` or `off`.
# mode: off

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Tell the agent to detect when commands come directly
# from input. The agent blocks if blocking is enabled.
# detect_phased_commands: true

# \
=====
# protect.rules.cmd-injection-semantic-chained-commands
# Use the following properties to configure how the
# 'command injection - chained commands' rule works
# \
=====
# cmd-injection-semantic-chained-commands:

# Set the mode of the rule. Value options
# are `monitor`, `block`, or `off`.
# mode: off

# \
=====
# protect.rules.cmd-injection-semantic-dangerous-paths
# Use the following properties to configure how the
# 'command injection - dangerous paths' rule works
# \
=====
# cmd-injection-semantic-dangerous-paths:

# Set the mode of the rule. Value options
# are `monitor`, `block`, or `off`.
# mode: off
```



```
# \  
=====
```

```
# protect.rules.cmd-injection-command-backdoors  
# Use the following properties to configure how the  
# 'command injection - command backdoors' rule works  
# \  
=====
```

```
# cmd-injection-command-backdoors:  
  
# Set the mode of the rule. Value options  
# are `monitor`, `block`, or `off`.  
# mode: off  
  
# \  
=====
```

```
# protect.rules.path-traversal-semantic-file-security-bypass  
# Use the following properties to configure how the  
# 'path traversal - file security bypass' rule works  
# \  
=====
```

```
# path-traversal-semantic-file-security-bypass:  
  
# Set the mode of the rule. Value options  
# are `monitor`, `block`, or `off`.  
# mode: off  
  
# \  
=====
```

```
# protect.rules.path-traversal  
# Use the following properties to configure  
# how the path traversal rule works.  
# \  
=====
```

```
# path-traversal:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====
```

```
# protect.rules.method-tampering  
# Use the following properties to configure  
# how the method tampering rule works.  
# \  
=====
```

```
# method-tampering:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.
```

```
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.unsafe-file-upload
# Use the following properties to configure
# how the unsafe file upload rule works.
# \
=====
# unsafe-file-upload:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
```

```
# mode: off

# \
=====
# protect.rules.untrusted-deserialization
# Use the following properties to configure
# how the untrusted deserialization rule works.
# \
=====
# untrusted-deserialization:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET
```

```
# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Override the reported server path. New after
# .NET Framework v21.3.1 and .NET Core v1.8.0.
# path: NEEDS_TO_BE_SET

# \
=====
```

```

==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==

# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# Set the version of the TLS protocol the agent uses to communicate with \
the
# Contrast UI. The .NET agent default behavior is \
(SecurityProtocolType.Tls
# | SecurityProtocolType.Tls11 | SecurityProtocolType.Tls12).
# tls_versions: tls|tls11|tls12

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \

```

```
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Determine the location from which the agent loads a client
# certificate. Value options include `File` or `Store`.
# certificate_location: NEEDS_TO_BE_SET

# Set the absolute path to the client certificate's
# .CER file for communication with Contrast UI. The
# `certificate_location` property must be set to `File`.
# cer_file: NEEDS_TO_BE_SET

# Specify the name of certificate store to open. The
# `certificate_location` property must be set to `Store`.
# Value options include `AuthRoot`, `CertificateAuthority`,
# `My`, `Root`, `TrustedPeople`, or `TrustedPublisher`.
# store_name: NEEDS_TO_BE_SET

# Specify the location of the certificate store. The
# `certificate_location` property must be set to `Store`.
# Value options include `CurrentUser` or `LocalMachine`.
# store_location: NEEDS_TO_BE_SET

# Specify the type of value the agent uses to find the certificate
# in the collection of certificates from the certificate store.
# The `certificate_location` property must be set to `Store`.
# Value options include `FindByIssuerDistinguishedName`,
# `FindByIssuerName`, `FindBySerialNumber`,
# `FindBySubjectDistinguishedName`, `FindBySubjectKeyIdentifier`,
# `FindBySubjectName`, or `FindByThumbprint`.
# find_type: NEEDS_TO_BE_SET

# Specify the value the agent uses in combination with
# `find_type` to find a certification in the certificate store.
#
# Note - The agent will use the first certificate from
# the certificate store that matches this search criteria.
#
# find_value: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate
# with the Contrast web interface over a proxy. Set
```

```

# value to `false` if you don't want to use the proxy.
# enable: NEEDS_TO_BE_SET

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# Set the proxy user.
# user: NEEDS_TO_BE_SET

# Set the proxy password.
# pass: NEEDS_TO_BE_SET

# Set the proxy authentication type. Value
# options are `NTLM`, `Digest`, and `Basic`.
# auth_type: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Set to `true` to redirect all logs to
# `stdout` instead of the file system.
# stdout: false

# Set the roll size for log files in megabytes. The agent will
# attempt to prevent the log file from being larger than this size.
# roll_size: 100

# Set the number of backup files to keep. Set to `0` to disable.
# backups: 10

# \
=====

```

```
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
```



```

# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# Set the connection type used for Syslog messages.
# Value options are `UNENCRYPTED` and `ENCRYPTED`.
# connection_type: UNENCRYPTED

# \
=====
# agent.dotnet
# The following properties apply to any .NET agent-wide configurations.
# \
=====
# dotnet:

# Set a list of application pool names that the agent does not
# instrument or analyze. Names must be formatted as a comma-separated
# list. New after .NET Framework 19.1.3 and .NET Core 4.0.2.
# app_pool_denylist: NEEDS_TO_BE_SET

# Set a list of application pool names that the agent instruments or
# analyzes. If set, other application pools are ignored. Allowlist takes
# precedence over denylist. Names must be formatted as a comma-separated
# list. New after .NET Framework 19.1.3 and .NET Core 4.0.2.
# app_pool_allowlist: NEEDS_TO_BE_SET

# Set a list of application names that the agent does not
# analyze. (The applications are still instrumented).
# Names must be formatted as a comma-separated list.
# New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# application_denylist: NEEDS_TO_BE_SET

# Set a list of application names that the agent analyzes.
# If set, other applications are not analyzed, but are
# still instrumented. Allowlist takes precedence over
# denylist. Names must be formatted as a comma-separated
# list. New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# application_allowlist: NEEDS_TO_BE_SET

# Enable a profiler chaining feature to allow Contrast to
# work alongside other tools that use the CLR Profiling
# API. Defaults to `true`. New after .NET Framework 19.1.3
# (Installed Only) and .NET Core 1.9.3 (Installed Only).
# enable_chaining: true

# Indicate that the agent should allow CLR optimizations
# of JIT-compiled methods. Defaults to `true`. New
# after .NET Framework 19.1.3 and .NET Core 1.0.0.
# enable_instrumentation_optimizations: true

# Indicate that the agent should allow the CLR to inline
# methods that are not instrumented by Contrast. Defaults to
# `true`. New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# enable_jit_inlining: true
    
```

```
# Indicate that the agent should allow the CLR to perform
# transparency checks under full trust. Defaults to `false`.
# New after .NET Framework 19.1.3 and .NET Core 1.0.0.
# enable_transparency_checks: false

# Set to display ASCII art to std::out on agent startup. Defaults
# to `true`. New after .NET Framework 20.6.3 and .NET Core 1.0.0.
# enable_cat: true

# Sets the maximum amount of time a Protect regular expression
# is allowed to run before being cancelled. Set to -1 to never
# cancel regular expression execution. Defaults to `20_000`.
# New after .NET Framework 20.4.3 and .NET Core 1.5.0.
# protect_searchers_single_pattern_deadline_ms: 20_000

# Sets the maximum amount of time a 'Probe Analysis' Protect
# regular expression is allowed to run before being cancelled. Set
# to -1 to never cancel regular expression execution. Defaults to
# `5_000`. New after .NET Framework 20.7.3 and .NET Core 1.5.11.
# protect_searchers_probe_analysis_single_pattern_deadline_ms: 5_000

# Sets the maximum amount of time a Protect rule is
# allowed to run before being cancelled. Set to -1 to never
# cancel Protect rule execution. Defaults to `60_000`.
# New after .NET Framework 20.4.3 and .NET Core 1.5.0.
# protect_searchers_total_rule_deadline_ms: 60_000

# Sets the maximum amount of time a 'Probe Analysis' Protect
# rule is allowed to run before being cancelled. Set to -1 to
# never cancel Protect rule execution. Defaults to `10_000`.
# New after .NET Framework 20.7.3 and .NET Core 1.5.11.
# protect_searchers_probe_analysis_total_rule_deadline_ms: 10_000

# Sets the maximum duration of time agent log files should be kept
# since last write before being deleted by the agent. Defaults to
# `604_800_000`. New after .NET Framework 20.6.1 and .NET Core 1.5.5.
# log_cleanup_maximum_age_ms: 604_800_000

# Suppresses gathering process-level metrics (process level metrics are
# gathered by default), used to identify performance problems. Metric
# counters may further decrease the stability of already unstable
# systems and can be disabled (set to true) if issues occur. Defaults
# to `false`. New after .NET Framework 20.6.6 and .NET Core 1.5.10.
# suppress_metric_counters: false

# Enable file based application watching. Set to false if
# file watching is causing locking issues. Defaults to `true`.
# New after .NET Framework 20.7.3 and .NET Core 1.5.11.
# enable_file_based_app_watching: true

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
```

```
# \  
=====\  
==  
# inventory:  
  
# Set to `false` to disable inventory features in the agent.  
# enable: true  
  
# Apply a list of labels to libraries. Labels  
# must be formatted as a comma-delimited list.  
# Example - `label1, label2, label3`  
#  
# tags: NEEDS_TO_BE_SET  
  
# \  
=====\  
==  
# assess  
# Use the properties in this section to control Assess.  
# \  
=====\  
==  
# assess:  
  
# Include this property to determine if the Assess  
# feature should be enabled. If this property is not  
# present, the decision is delegated to the Contrast UI.  
# enable: false  
  
# Control the values captured by Assess vulnerability events. `Full`  
# captures most values by calling ToString on objects, which can  
# provide more info but causes increased memory usage. `Minimal`  
# has better performance as it only captures String type objects  
# as strings and uses type name for other object type values.  
# event_detail: minimal  
  
# Apply a list of labels to vulnerabilities and preflight  
# messages. Labels must be formatted as a comma-delimited list.  
# Example - `label1, label2, label3`  
#  
# tags: NEEDS_TO_BE_SET  
  
# Value options are `ALL`, `SOME`, or `NONE`.  
# stacktraces: ALL  
  
# \  
=====\  
# assess.sampling  
# Use the following properties to control sampling in the agent.  
# \  
=====\  
# sampling:  
  
# Set to `true` to enable sampling.  
# enable: false
```

```

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
# protect.rules
# Use the following properties to set simple rule configurations.
# \
=====
# rules:

# Define a list of Protect rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
# disabled_rules: NEEDS_TO_BE_SET

```

```
# \  
=====\  
# protect.rules.bot-blocker  
# Use the following selection to configure if the  
# agent blocks bots. Set to `true` to enable blocking.  
# \  
=====\  
# bot-blocker:  
  
# Set to `true` for the agent to block known bots.  
# enable: false  
  
# \  
=====\  
# protect.rules.sql-injection  
# Use the following settings to configure the sql-injection rule.  
# \  
=====\  
# sql-injection:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or off.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====\  
# protect.rules.sql-injection-semantic-chaining  
# Use the following properties to configure how the  
# sql injection semantic analysis chaining rule works.  
# \  
=====\  
# sql-injection-semantic-chaining:  
  
# Set the mode of the rule. Value options  
# are `monitor`, `block` or `off`.  
# mode: off  
  
# \  
=====\  
# protect.rules.sql-injection-semantic-dangerous-functions  
# Use the following properties to configure how the sql  
# injection semantic analysis dangerous functions rule works.  
# \  
=====\  
# sql-injection-semantic-dangerous-functions:  
  
# Set the mode of the rule. Value options  
# are `monitor`, `block` or `off`.  
# mode: off  
  
# \  
=====
```

```
=====
# protect.rules.sql-injection-semantic-suspicious-unions
# Use the following properties to configure how the sql
# injection semantic analysis suspicious unions rule works.
# \
=====
```

```
# sql-injection-semantic-suspicious-unions:
```

```
# Set the mode of the rule. Value options
# are `monitor`, `block` or `off`.
# mode: off
```

```
# \
=====
```

```
# protect.rules.sql-injection-semantic-tautologies
# Use the following properties to configure how the sql
# injection semantic analysis tautologies rule works.
# \
=====
```

```
# sql-injection-semantic-tautologies:
```

```
# Set the mode of the rule. Value options
# are `monitor`, `block` or `off`.
# mode: off
```

```
# \
=====
```

```
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
```

```
# cmd-injection:
```

```
# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# Tell the agent to detect when commands come directly
# from input. The agent blocks if blocking is enabled.
# detect_phased_commands: true
```

```
# \
=====
```

```
# protect.rules.cmd-injection-semantic-chained-commands
# Use the following properties to configure how the
# 'command injection - chained commands' rule works
# \
=====
```

```
# cmd-injection-semantic-chained-commands:
```

```
# Set the mode of the rule. Value options
# are `monitor`, `block`, or `off`.
# mode: off

# \
=====
# protect.rules.cmd-injection-semantic-dangerous-paths
# Use the following properties to configure how the
# 'command injection - dangerous paths' rule works
# \
=====
# cmd-injection-semantic-dangerous-paths:

# Set the mode of the rule. Value options
# are `monitor`, `block`, or `off`.
# mode: off

# \
=====
# protect.rules.cmd-injection-command-backdoors
# Use the following properties to configure how the
# 'command injection - command backdoors' rule works
# \
=====
# cmd-injection-command-backdoors:

# Set the mode of the rule. Value options
# are `monitor`, `block`, or `off`.
# mode: off

# \
=====
# protect.rules.path-traversal-semantic-file-security-bypass
# Use the following properties to configure how the
# 'path traversal - file security bypass' rule works
# \
=====
# path-traversal-semantic-file-security-bypass:

# Set the mode of the rule. Value options
# are `monitor`, `block`, or `off`.
# mode: off

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
```

```
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.unsafe-file-upload
# Use the following properties to configure
# how the unsafe file upload rule works.
# \
=====
# unsafe-file-upload:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```



```

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.untrusted-deserialization
# Use the following properties to configure
# how the untrusted deserialization rule works.
# \
=====
# untrusted-deserialization:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

```

```
# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost
```

```
# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Override the reported server path. New after
# .NET Framework v21.3.1 and .NET Core v1.8.0.
# path: NEEDS_TO_BE_SET
```

## .NET エージェントエクスペローラ



### 重要

.NET Core エージェント 4.0.0 および .NET Framework エージェント 51.0.0 より、Contrast トレイアプリケーションを .NET エージェントエクスペローラに置き換えました。

.NET エージェントエクスペローラは、.NET Core エージェントおよび .NET Framework エージェントの稼働状況に関する概要情報を表示するアプリケーションです。このアプリケーションを使用すると、エージェントが想定通りに動作しているかを確認できます。特にエージェントを最初にインストールした後にご利用ください。

エージェントをインストールすると、このアプリケーションもインストールされます。両方の種類のエージェントをインストールした場合は、エージェントエクスペローラのインスタンスは 1 つだけインストールされます。

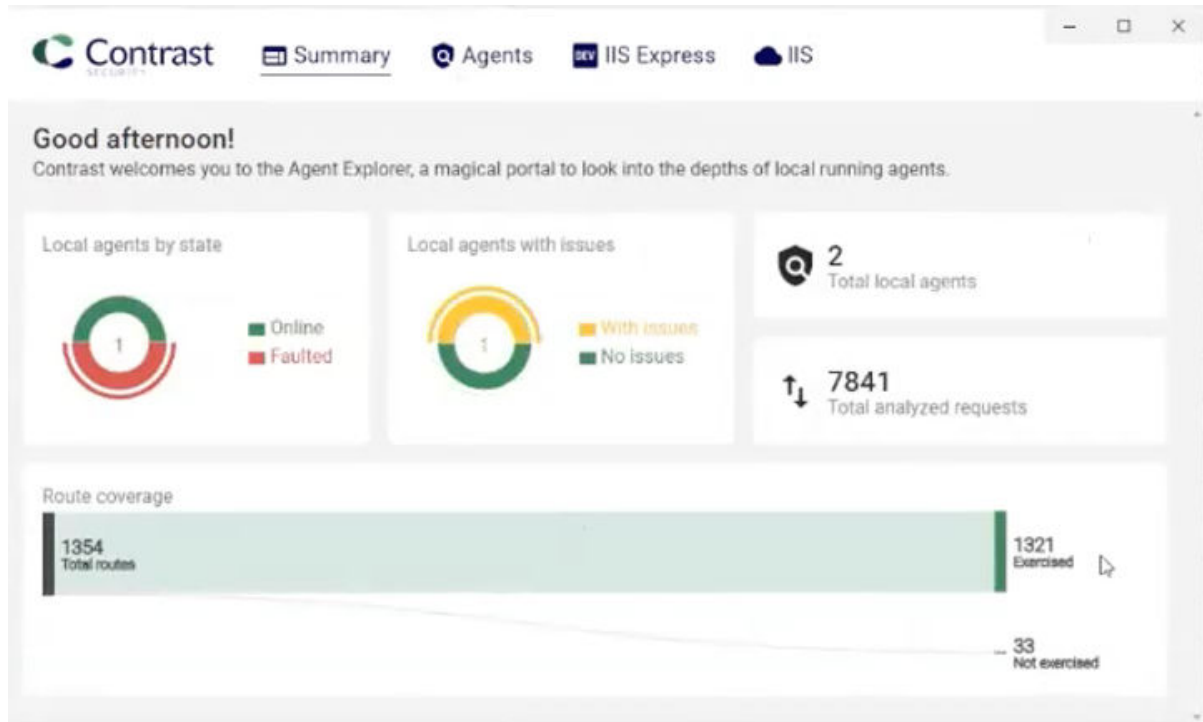
### エージェントエクスペローラへのアクセス

.NET Core エージェントが .NET Framework エージェントをインストールした後、エージェントエクスペローラのアイコン (🔍) がトレイに表示されます。アイコンを右クリックすると、アプリケーションが開きます。

### エージェントエクスペローラでの情報

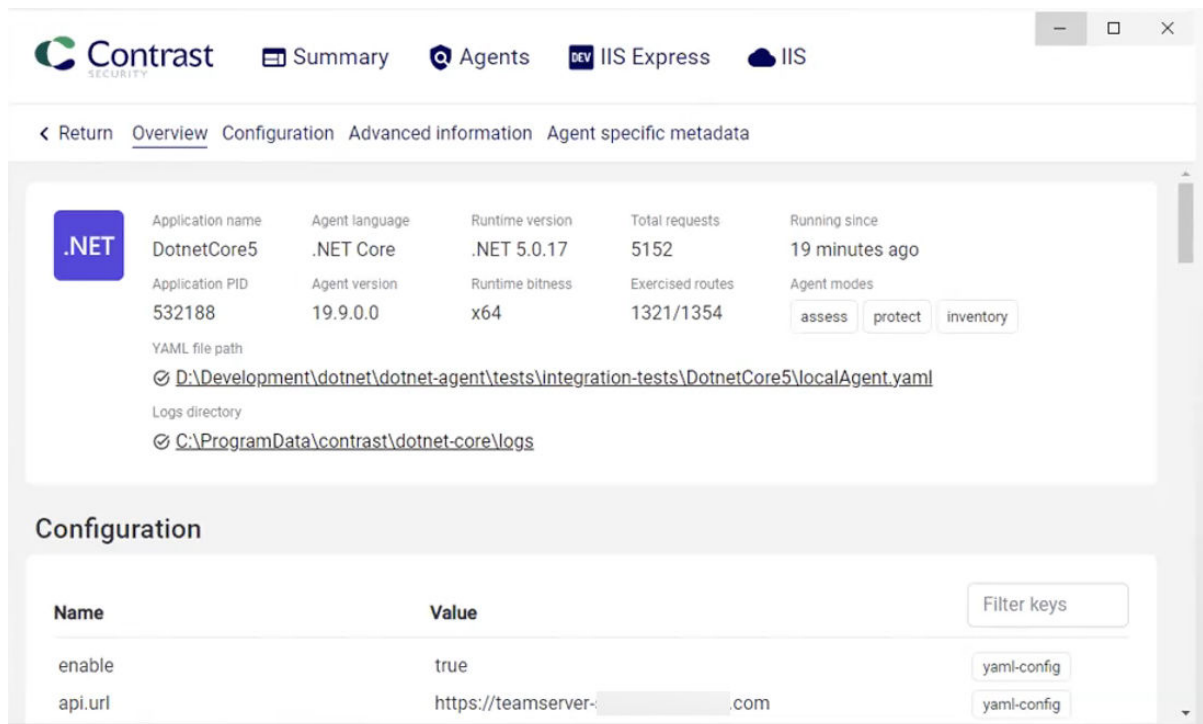
エージェントエクスペローラには、以下の情報が表示されます。

- Summary(サマリー)



このダッシュボードには、エージェントのステータス、問題のあるエージェントの有無、ルートカバレッジなど、エージェントに関する概要レベルの情報が表示されます。

• **Agents(エージェント)**



このタブには、.NET Core エージェントおよび.NET Framework エージェントの稼働状況に関する情報が表示されます。Configuration(設定)セクションには、特定の問題が発生していることをエージェントエクスプローラが検知した場合に、メッセージが表示されます。

Overview(概要)セクションにあるリンクから、エージェントの設定ファイル(YAML ファイル)に直接アクセスすることができます。下にスクロールすると、エージェントの設定内容、詳細情報、セッションメタデータの情報が表示されます。

• **IIS Express**

このタブには、IIS Express で実行されている Web アプリケーションの情報が表示されます。

## • IIS

このタブには、IIS サーバで実行されている Web アプリケーションの情報が表示されます。

## .NET Core エージェントのプロファイラチェーン

プロファイラチェーンを使用して、.NET Core APM プロファイラと併せて .NET Core エージェントを実行できます。

Contrast .NET Core エージェントは、ランタイム、デプロイタイプ、OS の特定の組み合わせを前提として、以下のプロファイリングツールとの互換性をテストおよび検証済みです。

プロファイリングツール	検証済バージョン	.NET Core ランタイム	サードパーティプロファイラのデプロイタイプ	OS
AppDynamics	21.8.1	6.0	NuGet パッケージ	Windows
AppDynamics	21.8.1	6.0	インストーラ使用	Windows
AppDynamics	21.8.1	6.0	NuGet パッケージ	Windows
Dynatrace OneAgent	1.253.245	6.0	インストーラ使用	Windows、Ubuntu
New Relic	8.23.107	6.0	NuGet パッケージ	Windows
New Relic	8.23.1076	6.0	NuGet パッケージ	Ubuntu
リバーベッド SteelCentral Aternity	12.9.0	6.0	インストーラ使用	Windows



### 注記

その他のプロファイリングツールでも、CoreCLR プロファイリング API の規則に準拠しており、プロファイリング環境に関する前提条件がない場合は、エージェントはそのプロファイリングツールと互換性がある可能性があります。

チェーンはデフォルトで有効になっており、`agent.dotnet.enable_chaining` を `false` に設定することで無効にできます。

```
agent:
  dotnet:
    enable_chaining: false
```

## 自動(Windows、IIS)

IIS 用 .NET Core エージェントのインストーラを使用する場合、ホストされている全ての .NET Core アプリケーションに対して、インストーラが自動でチェーンを構成します。

1. サードパーティのエージェントを最初にインストールし(推奨)、それから Contrast .NET Core エージェントをインストールしてください。
2. IIS ワークを再起動します(デフォルトでは、これはエージェントのインストーラによって自動的に行われます)。再起動すると、Contrast .NET Core エージェントは、IIS に登録されている他のプロファイリングツールの存在を自動的に検出し、Contrast .NET Core エージェントとサードパーティの両方のプロファイラを読み込むよう環境を構成します。

## 自動(Linux)

Linux では、`LD_PRELOAD` 環境変数を設定することで自動チェーンを設定することができます。

```
LD_PRELOAD=<path to the extracted Contrast files>/runtimes/linux-x64/native/ContrastChainLoader.so
```

例えば、Contrast エージェントを /contrast に解凍した場合、以下のようにするとチェーンが自動的に設定されます。

```
LD_PRELOAD=/contrast/runtimes/linux-x64/native/ContrastChainLoader.so \  
dotnet ./HelloWorld
```

APM プロファイラによっては、既に LD\_PRELOAD が設定されているものもあります(例、Dynatrace)。この場合、Contrast のモジュールが最初にロードされ、他の LD\_PRELOAD はコロン:で区切られていることを確認してください。例：

```
LD_PRELOAD=/contrast/runtimes/linux-x64/native/ContrastChainLoader.so:\  
<path to Dynatrace>/liboneagentproc.so dotnet ./HelloWorld
```



### 注記

Kubernetes の環境で実行する場合、[Contrast エージェントオペレータ \(55ページ\)](#)は、自動的にチェーンを設定するため、既存の Kubernetes ワークロードに対してエージェントを追加するのに推奨する方法です。

## 手動

以下のような環境では、チェーンを手動で設定する必要があります。

- IIS 以外でホストされている
- (インストールされたエージェントではなく)サードパーティエージェントの Nuget パッケージを使用する環境



### 注記

Dynatrace エージェントとのチェーンは、上記の自動オプションを使用した場合にのみサポートされます。

1. プロファイリングツールの CLR 環境変数を CONTRAST\_CCC\_CORECLR バージョンに置き換えてください。以下の環境変数名はいずれも置き換える必要があります。

変更すべき変数名	変更後
CORECLR_PROFILER	CONTRAST_CCC_CORECLR_PROFILER
CORECLR_PROFILER_PATH	CONTRAST_CCC_CORECLR_PROFILER_PATH
CORECLR_PROFILER_PATH_32	CONTRAST_CCC_CORECLR_PROFILER_PATH_32
CORECLR_PROFILER_PATH_64	CONTRAST_CCC_CORECLR_PROFILER_PATH_64

2. そして、エージェントを [手動 \(198ページ\)](#) で追加します。

## .NET Framework および .NET Core のテレメトリ

.NET Framework エージェントおよび .NET Core エージェントは、テレメトリを使用して、使用状況に関するデータを収集します。テレメトリは、エージェントを組み込んだアプリケーションでエージェントのセンサーが最初にロードされた時に収集され、その後も定期的(数時間ごと)に収集されます。

弊社では、[お客様のプライバシーは非常に大切 \(828ページ\)](#) であると考えています。このテレメトリ機能は、アプリケーションのデータを収集するものではありません。データは匿名化されてから、安全に

Contrast に送信されます。そして、集約されたデータは暗号化されて保存され、アクセスが制限されま  
す。収集されたデータは、全て 1 年後に削除されます。

テレメトリ機能で収集されるのは、以下のデータです。

エージェントのバージョン	データ	
.NET Framework 2020.8.3 以降	エージェントのバージョン	
.NET Core 1.5.15 以降	オペレーティングシステムとバージョン	
	エージェントがコンテナ内で実行されているかどうか	
	エージェントが Azure App Services で実行されているかどうか	
	ハッシュ化されたメディアアクセス制御(MAC)アドレス：暗号化(SHA256) された、匿名の一意なマシン ID	
	カーネルのバージョン	
	プロセスの実行時間	
	Assess が有効であるかどうか	
	Protect が有効であるかどうか	
	.NET Framework 2020.8.3 以降	.NET Framework ランタイム のバージョ ン
	.NET Core 1.5.15 以降	.NET Core ランタイム のバージョ ン
.NET Framework 20.9.1 以降	Contrast インスタンスが SaaS 版かオンプレミス版であるか	
.NET Core 1.5.17 以降		
.NET Framework 20.9.3 以降	CLR Instrumentation Engine (CIE)の使用状況	
.NET Core 1.5.19 以降	アプリケーションのフレームワーク	
	連携しているプロファイリングツール	
.NET Framework 20.10.1 以降	プロセスのホスティングモード	
.NET Core 1.5.20 以降	CIE ネイティブプロファイラフックの使用状況	
.NET Framework 20.10.2 以降	デフォルト以外の値が指定されている設定名	
.NET Core 1.5.21 以降	無効にされている Assess ルール名	
.NET Framework 20.12.2 以降	エージェントのプロファイラコンポーネントが初期化されるまでに経過し た時間	
.NET Core 1.7.2 以降	エージェントから Contrast Web インターフェイスへの最初のリクエストま でに経過した時間	
	エージェントのプロファイラコンポーネントが初期化されるまでに経過し た時間	
	エージェントの初期化から最初のリクエストが終了するまでに経過した時 間	
.NET Framework 21.1.1 以降	IIS でホストされているアプリケーションに関する測定値：	
	<ul style="list-style-type: none"> <li>合計アプリケーション数</li> <li>解析対象となるアプリケーション数(アプリケーションの許可/拒否リスト で設定)</li> <li>CLR4 のアプリケーションプールでホストされているアプリケーション 数</li> <li>CLR2 のアプリケーションプールでホストされているアプリケーション 数</li> </ul>	
	IIS のアプリケーションプールに関する測定値：	
	<ul style="list-style-type: none"> <li>合計数</li> <li>エージェントが接続されている数</li> <li>CLR4 の数</li> <li>CLR2 の数</li> </ul>	
	単独のアプリケーションプールでのアプリケーションの最小数	
	単独のアプリケーションプールでのアプリケーションの最大数	

エージェントのバージョン	データ
	全てのアプリケーションプールにあるアプリケーション数の中央値
.NET Framework 21.1.2 以降	Protect の各ルールのモード(例、監視やブロック)
.NET Core 1.7.5 以降	
.NET Framework 21.4.2 以降	エージェントのセンサーコード内でスローされキャッチされた例外。ログメッセージ、例外タイプ、例外のメッセージ、System メソッドおよび Contrast メソッドのスタックトレースフレームなど。
.NET Core 1.8.4 以降	
.NET Framework 21.7.1 以降	<ul style="list-style-type: none"> <li>プロセスアーキテクチャ(x86/x64)</li> </ul>
.NET Core 1.9.7 以降	OS アーキテクチャ(x86/x64) Azure App Service における以下の環境変数の値 : <ul style="list-style-type: none"> <li>WEBSITE_PHYSICAL_MEMORY_MB</li> <li>WEBSITE_PLATFORM_VERSION</li> <li>WEBSITE_SKU</li> </ul>
.NET Framework 21.9.2 以降	YAML 設定ファイルを読み込んだ場所(環境変数で指定したパス、デフォルトの場所、アプリケーションディレクトリなど)に関する説明
.NET Core 2.0.1 以降	

テレメトリ機能を停止するには、`CONTRAST_AGENT_TELEMETRY_OPTOUT` という環境変数に 1 または `true` を設定してください。

テレメトリのデータは、`telemetry.dotnet.contrastsecurity.com` に安全に送信されます。ネットワークレベルで通信をブロックすることで、テレメトリ機能を停止することもできます。

## Azure Functions のサポートバージョン

ランタイムバージョン	言語のバージョン	サポート対象	サポート対象外
1.x	.NET Framework 4.8	<ul style="list-style-type: none"> <li>Windows アプリケーション : Azure の .NET Framework 拡張機能でサポート</li> </ul>	<ul style="list-style-type: none"> <li>Docker Linux イメージ</li> <li>Linux アプリケーション</li> </ul>
3.x	.NET 5	<ul style="list-style-type: none"> <li>Windows アプリケーション : ローカル、および .NET Core 拡張機能によって Azure でサポート</li> <li>Docker Linux イメージ : ローカルおよび Azure でサポート</li> </ul>	<ul style="list-style-type: none"> <li>Linux アプリケーション</li> </ul>
4.x	.NET 6	<ul style="list-style-type: none"> <li>Windows アプリケーション : ローカル、および .NET Core 拡張機能によって Azure でサポート</li> <li>Docker Linux イメージ : ローカルおよび Azure でサポート</li> </ul>	<ul style="list-style-type: none"> <li>Linux アプリケーション</li> </ul>



### 注記

すべてのバージョンで、Azure Functions アプリケーションを分離プロセスで実行している場合は、.NET エージェントのサポート対象外です。

### サポート対象のトリガー

- HTTP
- Service Bus

### 設定

Azure Functions では、3 つのデプロイシナリオがサポートされています。Windows アプリケーション、Linux アプリケーション、Docker Linux イメージの 3 つです。この 3 つのうち、.NET エージェントが対



応しているのは、Windows アプリケーションと Docker Linux イメージのみです。Linux アプリケーションのデプロイは、.NET エージェントではサポートされません。

## Windows アプリケーション

Windows アプリケーションのデプロイは、Azure Functions のバージョン 1、3、4 に対して完全にサポートされます。ローカルでは、アプリケーションは Contrast .NET Core エージェントの NuGet パッケージを参照します。Azure 上には、Contrast .NET Core の拡張機能をインストールする必要があります。ツール(Visual Studio や Core Tools など)や、CI/CD パイプライン、または Azure Functions のポータルベースのエディタを使用して、Azure Functions のアプリケーションをデプロイすると、サイト拡張機能は必要なアプリケーション設定を自動的に設定しません。アプリケーション設定を手動で指定する必要があります。

そのためには、以下のアプリケーション設定(設定 > 構成 > アプリケーション設定)を行ってください。

```
CORECLR_ENABLE_PROFILING=1
CORECLR_PROFILER={8B2CE134-0948-48CA-A4B2-80DDAD9F5791}
CORECLR_PROFILER_PATH_32=C:\home\SiteExtensions\Contrast.NetCore.Azure.SiteExtension\ContrastNetCoreAppService-<version>\runtimes\win-x86\native\ContrastProfiler.dll
CORECLR_PROFILER_PATH_64=C:\home\SiteExtensions\Contrast.NetCore.Azure.SiteExtension\ContrastNetCoreAppService-<version>\runtimes\win-x64\native\ContrastProfiler.dll
```

上記の<version>の箇所には、「0.0.0.0」という形式でエージェントのバージョンを指定します。例えば、エージェントのバージョンが「2.1.8」であれば、パスは次のようになります。

す：C:\home\SiteExtensions\Contrast.NetCore.Azure.SiteExtension\ContrastNetCoreAppService-2.1.8.0\runtimes\win-x64\native\ContrastProfiler.dll

Contrast サーバへの接続情報は、アプリケーション設定を使用するか、アプリケーション設定から参照される設定ファイルで指定します。

アプリケーション設定：

```
CONTRAST_API_USER_NAME=my_username
CONTRAST_API_SERVICE_KEY=my_service_key
CONTRAST_API_API_KEY=my_api_key
CONTRAST_API_URL=my_api_url
```

設定ファイルで Contrast サーバの接続情報を指定する場合は、次のアプリケーション設定を指定する必要があります：CONTRAST\_CONFIG\_PATH=C:\home\site\wwwroot\contrast\_security.yaml

## Docker Linux イメージ

カスタム Linux イメージのデプロイは、Azure Functions のバージョン 3 および 4 でサポートされます。カスタム Linux イメージが必要で、イメージにはアプリケーションと Contrast .NET Core エージェントの NuGet パッケージが含まれている必要があります。Linux アプリケーションは、カスタム Linux イメージから実行されない場合、.NET エージェントではサポート対象外であることに注意してください。

エージェントを組み込むために、以下のアプリケーション設定を行う必要があります。これらの設定は、イメージ自体(環境変数として)に含めるか、またはアプリケーション設定(設定 > 構成 > アプリケーション設定)として設定します。

```
CORECLR_ENABLE_PROFILING=1
CORECLR_PROFILER={8B2CE134-0948-48CA-A4B2-80DDAD9F5791}
CORECLR_PROFILER_PATH=/home/site/wwwroot/contrast/runtimes/linux-x64/native/ContrastProfiler.so
CORECLR_PROFILER_PATH_64=/home/site/wwwroot/contrast/runtimes/linux-x64/
```

```
native/ContrastProfiler.so
CONTRAST_CORECLR_INSTALL_DIRECTORY=/home/site/wwwroot/bin/contrast/
```

Contrast サーバへの接続情報は、アプリケーション設定/環境変数を使用するか、アプリケーション設定/環境変数から参照される設定ファイルで指定します。

アプリケーション設定/環境変数：

```
CONTRAST__API__USER_NAME=my_username
CONTRAST__API__SERVICE_KEY=my_service_key
CONTRAST__API__API_KEY=my_api_key
CONTRAST__API__URL=my_api_url
```

設定ファイルで Contrast サーバの接続情報を指定する場合は、次のアプリケーション設定/環境変数を指定する必要があります： `CONTRAST_CONFIG_PATH=/home/site/wwwroot/contrast_security.yaml`

## Node.js エージェント

Contrast Node.js エージェントは、トランスコンパイルなどの確立された技術を駆使して、Node.js の Web アプリケーションの動作を解析し、実行前にアプリケーションに Contrast のセンサーを追加します。

Contrast Node.js エージェントは、セマンティックバージョンing(major.minor.patch)に従います。エージェントは、こちらの[サポート対象テクノロジー \(251ページ\)](#)と[システム要件 \(252ページ\)](#)で最適に動作します。

Node.js エージェントは、Babel コンパイラを使用してアプリケーションの起動前にアプリケーションコードを変換します。起動後、エージェントは[サポート対象のフレームワークやモジュール \(251ページ\)](#)に必要な関数をパッチします。

[Node.js エージェントをインストール \(253ページ\)](#)すると、アプリケーションの動作を監視するために、2つの主要なソースコード変換が行われます。

- **AST 変換**は、エージェントによって作成されたコード本体の抽象的な構文ツリーを操作し、この構文ツリーに基づいて新しいソースコードを作成するプロセスです。エージェントはこのプロセスによって、関数フックが機能しない状況进行处理します。例えば、変換によって Contrast は JavaScript に演算子のオーバーロードを追加できるため、信頼されないデータの流れを適切に追跡できるようになります。
- **関数フック**は、`child_process.exec` など特定の関数の実行を引き継ぎ、その引数や戻り値に関するデータを収集し、エージェントの解析部分にこのデータを送信します。その結果、エージェントは特定の関数について報告できるようになります。

## Contrast サービス

[Contrast サービス \(472ページ\)](#)は、Node.js エージェント内にパッケージ化された実行可能ファイルで、別のプロセスで実行されます。エージェントのバージョン 4.x.x では、Contrast サービスはエージェントと一緒に自動的に起動します。

このサービスによって、Node.js エージェントと Contrast サーバ間の通信が可能になります。エージェントと同様に、[環境変数 \(56ページ\)](#)や [YAML 設定ファイル \(38ページ\)](#)で[設定 \(473ページ\)](#)できます。Contrast サービスは、エージェントと Contrast 間の HTTP 通信に、デフォルトで 30555 番ポートを使用します。

エージェントと Contrast 間のポートおよび通信プロトコルは設定できます。利用可能なプロトコルは、HTTP、Linux ソケット(ファイル記述子)、gRPC です。サービスは、エージェントと 1 対 1 でデプロイすることも、複数のコンテナをホストする単一のサーバ上のエージェントを 1 つのグループとして共有することもできます。

## Node.js のサポート対象テクノロジー

このページは、注記で特に記載されていない限り、[npmjs.com](https://npmjs.com)(npm 公式 Web サイト)で入手可能な最新バージョンのサポート対象テクノロジーや機能を反映しています。



### 注記

Contrast Node.js エージェントは、[npmjs.com](https://npmjs.com) で非推奨(deprecated)とタグ付けされたモジュールでは機能しない場合があります。非推奨のモジュールは、セキュリティ上のリスクが高く、エージェントの機能に悪影響を及ぼす可能性があります。

また、webpack、parcel、esbuild などのバンドラーを使用してサーバサイドの JavaScript コードをパッケージ化したり圧縮したりするアプリケーションもサポートしません。

#### 言語のバージョン

- JavaScript ECMAScript 5
- JavaScript ECMAScript 6
- ECMAScript モジュール(ESM)
- TypeScript

#### 注記

Contrast は、「アクティブ LTS」または「メンテナンス LTS」ステータスの Node.js の偶数番号バージョンをサポートします。

Node.js LTS バージョンは、[JavaScript ECMAScript5 と 6](#) の機能をサポートします。

Contrast Node.js エージェントは、ESM を使用するアプリケーションで限定的なサポートを提供します。

TypeScript がサポートされるのは、エージェントがアプリケーションのコンパイル済みエントリポイントを指すように設定されている場合のみです。

#### Node.js LTS(長期サポート)版

現在、アクティブおよびメンテナンス LTS ステータスの全てのバージョン：

- 12\*、14\*
- 16 (エージェントバージョン 4.5.0 以降のみ)
- 18 (エージェントバージョン 4.25.0 以降)

#### 注記

常にアクティブまたはメンテナンスステータスの Node.js の LTS バージョンを使用してください。

\*12 LTS および 14 LTS を実行している場合、Contrast エージェントは機能するはずですが、それぞれ 2022 年 4 月末、2023 年 4 月末に EOL(サポート期間終了)になっています。これらの EOL バージョンは、パッチが適用されなくなったため、深刻なセキュリティリスクがあります。また、エージェントのバージョン 5.x.x には、Node.js のバージョン 14.15.0 以上が必要であることにご注意ください。

Node.js エージェントは、実験的(Stability: 1)な実装に分類される Node.js の機能のサポートを保証しません。また、ネイティブな net モジュールにエージェントは組み込まれません。この表にあるサポート対象のアプリケーションフレームワークを使用して構築された HTTP(S) アプリケーションサーバにのみ機能します。

HTTP/2 は、Node.js core の HTTP/2 または spdy ライブラリが使用されている場合に、Node.js エージェントのサポート対象となります。

Contrast Node.js エージェントで HTTP/2 を使用するアプリケーションでは、`assess.enable_lazy_tracking: false` を使用するようにエージェントを設定する必要があります。

Node.js のバージョンステータスは、[Node.js の LTS リリーススケジュール](#)に記載されています。

#### パッケージ管理システム(npm)

npm バージョン：

- 6.13.7 以降
- 7.11.0 以降
- 8.5.5 以降

Node.js エージェントが、Contrast Web インターフェイスに正確にライブラリを報告するためには、これらの npm バージョンのいずれかにアクセスする必要があります。バージョン 7 よりも、バージョン 6 または 8 を推奨します。

#### アプリケーションフレームワーク

<ul style="list-style-type: none"> <li>Express 4</li> <li>hapi 16*, 17*, 18*, 19*, 20</li> <li>Fastify 3</li> <li>Koa 2.3 以降</li> <li>Kraken 2.2.0、2.3.0</li> <li>LoopBack 3*, 4</li> <li>Restify 8</li> <li>Sails 1.2.3 以降</li> </ul>	<p><b>注記</b></p> <p>*これらのライブラリは保守管理者によって非推奨(deprecated)とされており、セキュリティ上のリスクの可能性がります。</p>
<p><b>データベースドライバとオブジェクト関係マッピング(ORM)</b></p>	
<ul style="list-style-type: none"> <li>DynamoDB(Assess のみ) AWS SDK for JavaScript : 2.x、3.x</li> <li>MongoDB 2.2.36*, 3.3.0 以降、4.x(データベースバージョン 3.6、4.x、5.x に対応)</li> <li>MySQL2 2.0.0 以降(MySQL データベースバージョン 5.6.51、5.7.x、8.0.x に対応)</li> <li>Mongoose 5.x、6.x</li> <li>MSSQL 6.4.0 以降</li> <li>Postgres driver 7.5.0 以降、8.x</li> <li>RethinkDB ドライバ バージョン 2.4.0 以降</li> <li>Sequelize 5.x、6.x</li> <li>SQLite3 driver 4.x(データベースバージョン 3.26.0 以降に対応)</li> </ul>	<p><b>注記</b></p> <p>*このバージョンではエージェントはまだ機能しますが、保守管理者によって非推奨(deprecated)とされており、セキュリティ上のリスクの可能性がります。</p>
<p><b>検証モジュール</b></p>	
<ul style="list-style-type: none"> <li>Joi 17 以降</li> <li>Validator 13 以降</li> <li>Class-validator 0.13.0 以降</li> </ul>	
<p><b>テンプレートエンジン</b></p>	
<ul style="list-style-type: none"> <li>Handlebars 4</li> <li>Pug 3</li> <li>EJS 2.6.2、3.0.1</li> <li>Mustache 4.x 以降</li> </ul>	
<p><b>その他のテクノロジー</b></p>	
<ul style="list-style-type: none"> <li>Express-session 1.15.6、1.16.0 以降</li> </ul>	
<p><b>テストスイート</b></p>	
<ul style="list-style-type: none"> <li>Node Test Benches(Node テストベンチ)</li> </ul>	<p>Node.js エージェントに変更が加えられると、Contrast は一連の自動化テストを実行し、サポート対象のすべての Node バージョン内でサポート対象テクノロジーでの検出結果を確認します。Node Test Benches には、Contrast のサポート対象のフレームワークでエージェントを実行するテストが含まれています。エージェントにサードパーティのライブラリサポートが追加されると、モノレポ(Monorepo)内の各フレームワークが更新されます。</p>

## Node.js エージェントのシステム要件



### 重要

Node.js エージェントは、M1/M2 チップを搭載した Mac での実行を制限付きでサポートするようになりました。制限としては、Apple M1/M2(ARM64)で Alpine ベースの Docker コンテナの実行は、まだ Node.js エージェントのサポート対象ではありません。Slim ベースの Docker イメージの実行はサポート対象です。

このページは、注記で特に記載されていない限り、[npmjs.com](https://npmjs.com)(npm 公式 Web サイト)で入手可能な最新バージョンのシステム要件や機能を反映しています。

Node.js エージェントをインストールする前に、以下の要件を満たしていることを確認してください。

- 検査対象となるデプロイ済みアプリケーションには `package.json` ファイルがあり、その Web アプリケーションのテクノロジーは Contrast のサポート対象であること。
- エージェントが Contrast サーバとネットワークで接続されていること。

Node.js エージェントを使用すると、受信情報の処理や解析が増加するため、アプリケーションで使用可能な CPU とメモリを増やす必要があります。Node.js エージェントを使用すると、アプリケーション単体で使用するよりも多くのリソースが必要となります。CPU の負荷も増加しますが、これはアプリケーションのアーキテクチャや既存の CPU 使用状況に大きく影響されます。

Assess を使用する場合、Contrast Node.js エージェントを使用しない場合と比較して、各コンテナで使用可能なメモリを 2 倍にする必要があります。

<p><b>オペレーティングシステム</b></p> <ul style="list-style-type: none"> <li>• CentOS/RHEL 7.9、8 以降</li> <li>• Ubuntu 14.04 LTS、16.04 LTS、18.04 LTS、20.04 LTS、22.04 LTS</li> <li>• Debian 9、10、11</li> <li>• Windows</li> <li>• macOS</li> </ul>
<p><b>プロセスマネージャ</b></p> <ul style="list-style-type: none"> <li>• PM2 : 4.5.0 以降、5.1.0 以降</li> <li>• Contrast Node.js エージェントは、フォーク(fork)モードおよびクラスター(cluster)モードの両方の実行をサポートしています。</li> <li>• Contrast Node.js エージェントを実行する際に使用する起動コマンドに、インストール済の <code>@contrast/agent</code> モジュールへの完全なパスを指定する必要があります。例：</li> </ul> <pre>node -r /Users/michael/Dev/my-app/node_modules/@contrast/agent app.js</pre>
<p><b>コンテナ</b></p> <ul style="list-style-type: none"> <li>• Distroless コンテナ</li> <li>• Contrast Node.js エージェントが正しく機能するためには、<code>npm</code> と <code>/bin/sh</code> へアクセスする必要があります。これらのプログラム/パッケージを含まない Distroless コンテナイメージで実行するアプリケーションにインストールすると、エージェントの機能が低下し、検出結果やライブラリが報告されない場合があります。</li> </ul>
<p><b>CPU</b></p> <ul style="list-style-type: none"> <li>• AMD 64、x86_64、およびその互換</li> <li>• Apple M1/M2 ARM64 (限定サポート)</li> </ul>

## Node.js エージェントのインストール

エージェントのインストール方法はいくつかあり、ご利用の環境によって異なりますが、一般的には次のような流れになります。

1. Node.js エージェントを `npm` から取得します。
2. [エージェントの認証キー \(37ページ\)](#) を設定します。
3. エージェントを有効にしてアプリケーションを実行するために、`package.json` ファイルにコマンドを追加します。
4. エージェントを有効にしてアプリケーションを実行します。
5. 通常通りにアプリケーションを疎通し、Contrast でアプリケーションが認識されていることを確認します。

具体的な手順については、アプリケーションのデプロイ方法に応じて、以下の各手順に従ってください。

- [手動でのインストール \(253ページ\)](#)
- [コンテナでのインストール \(254ページ\)](#)
- [IBM Cloud でのインストール \(259ページ\)](#)

## Node.js エージェントを手動でインストール

エージェントを手動でインストールまたは更新するには：

1. アプリケーションのルートディレクトリで以下のコマンドを実行して、`npm` からエージェントの最新バージョンをインストールします。

```
npm install @contrast/agent
```

または、yarn を使用する場合、次のコマンドを実行してエージェントをインストールします。

```
yarn add @contrast/agent
```



### 注記

Node.js エージェントに含まれるオプションの依存関係をインストールしたくない場合は、インストールコマンドに CLI フラグの `--no-optional` を追加するか、NPMRC ファイルに `optional=false` を追加してください。

2. [環境変数 \(56ページ\)](#) を使用して、エージェントの [認証キー \(37ページ\)](#) を指定します。Node.js アプリケーションが実行時に環境変数にアクセスできるようにしてください。  
または、こちらの [テンプレート \(264ページ\)](#) を使用して [YAML 設定 \(38ページ\)](#) ファイル (`contrast_security.yaml`) を作成し、認証キーを指定することもできます。  
`contrast_security.yaml` は、アプリケーションのルートディレクトリに作成してください。
3. アプリケーションの `package.json` ファイルの "scripts" セクションに次のコマンドを追加します。

```
"scripts": {  
  "contrast": "node -r @contrast/agent <app-main>.js",  
  "start": ...,  
  "test": ...  
}
```

4. エージェントを有効にしてアプリケーションを実行します。

```
npm run contrast
```



### ヒント

上記の npm スクリプトを変更して、別の設定ファイルの場所など [実行時の他の設定 \(262ページ\)](#) を指定することもできます。

5. 手動または自動テストを行ってアプリケーションを操作し、エージェントがインストールされた状態でアプリケーションが正しく機能することを確認してください。
6. アプリケーションサーバが Contrast に認識され、アプリケーションが Contrast に報告されていることを確認します。

## コンテナを使用して Node.js エージェントをインストール

### インストールを行う前に

本項では、Docker を例として、コンテナ化されたアプリケーションに Contrast Node.js エージェントをインストールするための一般的な手順について説明します。

コンテナや関連ソフトウェアの仕組みを基本的に理解している必要があります。実際の手順は、ご利用の環境に合わせて調整してください。

### エージェントをインストール

以下のいずれかの方法で、Node.js エージェントをインストールします。

- **アプリケーションの開発時にエージェントを追加 (推奨)**

この方法の場合、アプリケーションの `package.json` でエージェントを取り込みます。  
次のコマンドを使用して、パイプラインやコンテナイメージにエージェントを追加します。

```
npm install @contrast/agent --no-optional
```

## • Dockerfile にエージェントを追加

アプリケーションのイメージを別々に管理したい場合(Contrast エージェントを使用する場合と使用しない場合)は、コンテナのビルド時にエージェントを追加します。

次のコマンドを使用して、既存の Dockerfile、またはアプリケーションのイメージをベースイメージとして使用する新規の Dockerfile にエージェントを追加します。

```
npm install @contrast/agent --no-optional
```

## エージェントを設定

Node.js エージェントを Docker などのコンテナにデプロイしたアプリケーションで設定する場合は、以下の手順に従ってください(そうでない場合は、通常の [Node.js エージェントの設定 \(262ページ\)](#) を参照してください)。Node.js エージェントの設定には、設定した値が有効になる [優先順位 \(36ページ\)](#) があります。

### 1. YAML 設定ファイルを作成します。

作成した YAML 設定ファイル(`contrast_security.yaml`)は、コンテナのファイルシステムにコピーされるように、アプリケーションのディレクトリに置いてください。

YAML 設定ファイルでは：

- `<YourURL>`、`<YourUserName>`、`<YourAPIKey>`、`<YourServiceKey>`の箇所をご利用の認証情報に置き換えます。認証情報の検索については、[こちらの説明 \(37ページ\)](#) を参照。

コンテナにインストールする場合の一般的な YAML 設定ファイルは、以下のようになります。

```
api:
  url: <URLtoContrast>
  user_name: <YourUserName>
  api_key: <YourAPIKey>
  service_key: <YourServiceKey>
agent:
  service:
    grpc: true
assess:
  enable_lazy_tracking: false
```

### 2. 以下のコマンドを使用して、ベースイメージに YAML ファイルをコピーします(この例では、`/app/contrast_security.yaml` はイメージ内のアプリケーションのベースディレクトリにあります)。

```
COPY WORKSPACE/contrast_security.yaml /app/contrast_security.yaml
```

### 3. 環境変数を使用して、アプリケーション固有の設定値を指定します。これらは、Dockerfile 内で ENV 命令を定義するか、Docker run コマンドの実行時に `-e` オプションで指定することができます。アプリケーション固有の値を設定するためによく使用される [環境変数の一覧 \(263ページ\)](#) をご覧ください。

## 実行して確認

### 1. Node.js エージェントのリライタ CLII(バージョン 4.x 以降より利用可)を使用する場合は、RUN 命令を追加して、`contrast-transpile` 実行ファイルを呼び出すコマンドを指定します。そして、アプリケーションのエントリーポイントを指定します。

```
RUN npx -p @contrast/agent --no contrast-transpile index.js
```

`npx` コマンドが Contrast Security からのものであり、サプライチェーン攻撃を試みる悪意のある人物からではないことを確認するために、`-p @contrast/agent --no` オプションを使用することが重要です。

`-p` は、`--package` の省略形で、`@contrast/agent` パッケージにのみコマンドを使用するように `npx` に指定します。

`--no` は、非推奨となった `--no-install` オプションの新しいオプション名で、コマンドのバイナリが見つからない場合に `npm` からインストールを行わないよう `npx` に指定します。

`npm` コマンドを実行する前に、Contrast エージェントと `npm` バイナリが正常にインストールされていることを想定しています。

- アプリケーションを起動する際に、Contrast エージェントを先にロードしておく必要があります。通常は、これは Dockerfile の CMD 文で行いますが、`package.json` に定義した `npm` スクリプトも使用できます。

例えば、通常アプリケーションを次のように起動する場合：

```
CMD ["node", "app"]
```

次のコマンドを使用すると、Contrast を有効にしてアプリケーションを実行できます。

```
CMD ["node", "-r", "@contrast/agent", "app"]
```

- エージェントが起動すると、YAML 設定ファイルに記述されたエージェントの [認証キー \(37ページ\)](#) を使用して Contrast サーバに接続します。



### ヒント

エージェントの認証情報を保護するために、Docker secret を利用して、デプロイ時に環境変数として渡すこともできます。例：

```
docker run -e CONTRAST_API -e \
CONTRAST_API_API_KEY=<value> -e \
CONTRAST_API_SERVICE_KEY=<value> -e \
CONTRAST_API_USER_NAME=<value> -e \
CONTRAST_SERVER_ENVIRONMENT=<value> image_with_contrast
```

- コンテナのログのアクティビティをチェックして、Contrast が実行されていることを確認します。例えば、ログアクティビティは以下のようになります。

```
@contrast/agent 2.16.8-----
2020-07-20T19:05:14.407Z INFO contrast-service: BUILD \
{"programe": "Contrast Service", "version": "2.8.1", "buildTime": ""}
2020-07-20T19:05:14.407Z INFO Building timer for orphan request cleanup \
{"programe": "Contrast Service", "cleanupMs": 5000}
2020-07-20T19:05:14.408Z INFO Building timer for orphan app cleanup \
{"programe": "Contrast Service", "time": 5000}
2020-07-20T19:05:14.450Z INFO Creating New Application Server \
{"programe": "Contrast Service", "uuid": "96299b72-f867-4354-
b9c9-1eb23511cb8a", "serverName": "bc1bd6e5cd3a", "clientId": "1", "pid":
1}
2020-07-20T19:05:14.450Z WARN Failed to initialize secure client, \
falling back to insecure client {"programe": "Contrast Service"}
2020-07-20T19:05:15.473Z INFO setting new server features for \
context{"programe": "Contrast Service", "uuid": "96299b72-f867-4354-
b9c9-1eb23511cb8a", "serverName": "bc1bd6e5cd3a"}
2020-07-20T19:05:15.474Z ERROR Error setting up CEF syslog \
{"programe": "Contrast Service", "err": "open /juice-shop/security.log: \
permission denied"}
2020-07-20T19:05:15.475Z INFO starting event scanner \
{"programe": "Contrast Service", "report": {}}
2020-07-20T19:05:15.486Z INFO Creating new application \
{"programe": "Contrast Service", "uuid": "96299b72-f867-4354-
b9c9-1eb23511cb8a", "serverName": "bc1bd6e5cd3a", "appName": "juiceshop-
guide", "language": "Node", "clientId": "1", "pid": 1}
2020-07-20T19:05:15.486Z INFO AppCreate: creating and initializing new \
application {"programe": "Contrast Service", "uuid": "96299b72-f867-4354-
```



```
b9c9-1eb23511cb8a", "server_name": "bc1bd6e5cd3a", "app_name": "juiceshop-
-guide", "app_lang": "Node", "client_id": "1", "pid": 1}
2020-07-20T19:05:15.921Z INFO setting new application settings \
{"progname": "Contrast Service", "uuid": "96299b72-f867-4354-
b9c9-1eb23511cb8a", "serverName": "bc1bd6e5cd3a", "appName": "juiceshop-
guide", "language": "Node"}
2020-07-20T19:05:15.922Z INFO Setting session id on app context: \
{"progname": "Contrast Service", "uuid": "96299b72-f867-4354-
b9c9-1eb23511cb8a", "clientId": "1", "appName": "juiceshop-
guide", "applang": "Node", "apppath": "/juice-shop/
package.json", "sessionId": "cd0b271e66974162bf5fcca8b32e37b1"}
Entering main at /juice-shop/appinfo: All dependencies in ./
package.json are satisfied (OK)...
```



### 注記

また、[Docker イメージの作成時にエージェントをインストール \(257ページ\)](#)したり、[distroless の Node.js コンテナ \(258ページ\)](#)を使用してコンテナにインストールすることも可能です。

### 関連項目

Contrast サポートポータル : [Kubernetes での Node.js エージェント](#)

Contrast サポートポータル : [AWS Fargate と Contrast エージェント](#)

### Docker イメージの作成時にエージェントをインストール

Node.js アプリケーションに Contrast エージェントをインストールする別の方法として、ソースコードリポジトリの `package.json` ファイルを変更する代わりに、`npm install` コマンドを Docker イメージ作成の一部として実行できます。

Docker ファイルのみを修正して、Contrast エージェントを使用してセキュリティ検査を実行できるようにしたい場合に適しています。

例 :

```
FROM node:18 as installer
COPY . /juice-shop
WORKDIR /juice-shop
RUN npm i -g typescript ts-node
RUN npm install --omit=dev --unsafe-perm
RUN npm install @contrast/agent@4.x
RUN npm dedupe

# Need to explicitly set Assess mode
ENV CONTRAST__APPLICATION__NAME=juice-assess-docker-slim
ENV CONTRAST__ASSESS__ENABLE=true
ENV CONTRAST__AGENT__LOGGER__STDOUT=true
ENV CONTRAST__AGENT__LOGGER__PATH=/dev/null
ENV DEBUG="contrast:*"

ENV CONTRAST__AGENT__NODE__REWRITE_CACHE__PATH="/juice-shop/rewrite_cache"
RUN npx contrast-transpile build/app.js
```

```
RUN rm -rf frontend/node_modules
RUN rm -rf frontend/.angular
RUN rm -rf frontend/src/assets
RUN mkdir logs
RUN chgrp -R 0 ftp/ frontend/dist/ logs/ data/ i18n/
RUN chmod -R g=u ftp/ frontend/dist/ logs/ data/ i18n/
#RUN rm data/chatbot/botDefaultTrainingData.json || true
#RUN rm ftp/legal.md || true
#RUN rm i18n/*.json || true

FROM node:18-slim
ARG BUILD_DATE
ARG VCS_REF

WORKDIR /juice-shop
COPY --from=installer /juice-shop .

EXPOSE 3000
# The following environment variables were added
ENV CONTRAST__APPLICATION__NAME=juice-assess-docker-slim
ENV CONTRAST__AGENT__SERVICE__GRPC=true
ENV CONTRAST__AGENT__LOGGER__STDOUT=true
ENV CONTRAST__AGENT__LOGGER__PATH=/dev/null
ENV DEBUG="contrast:*"

ENV CONTRAST__AGENT__NODE__REWRITE_CACHE__PATH="/juice-shop/rewrite_cache"

# This explicitly turns on Assess mode
ENV CONTRAST__ASSESS__ENABLE=true
ENV CONTRAST__ASSESS__ENABLE_LAZY_TRACKING=false
ENV CONTRAST__AGENT__NODE__APP_ROOT=/juice-shop

CMD ["node", "-r", "@contrast/agent", "build/app.js"]
```

## Distroless コンテナ

*distroless* の Node.js コンテナを使用している場合、コンテナイメージに **npm** や **shell** はインストールされていません。必須モジュールとしてエージェントを実行するために、`NODE_OPTIONS` 環境変数を指定する必要があります。

ただし、`NODE_OPTIONS` を使用すると、すべての **node** または **npm** コマンドでエージェントが実行され、意図しない実行によって起動時間が長くなる可能性があるため、注意が必要です。

例：

```
FROM node:18 as installer
COPY . /juice-shop
WORKDIR /juice-shop
RUN npm i -g typescript ts-node
RUN npm install --omit=dev --unsafe-perm
RUN npm install @contrast/agent@4.x

RUN npm dedupe

RUN rm -rf frontend/node_modules
RUN rm -rf frontend/.angular
```

```
RUN rm -rf frontend/src/assets
RUN mkdir logs
RUN chown -R 65532 logs
RUN chgrp -R 0 ftp/ frontend/dist/ logs/ data/ i18n/
RUN chmod -R g=u ftp/ frontend/dist/ logs/ data/ i18n/
RUN rm data/chatbot/botDefaultTrainingData.json || true
RUN rm ftp/legal.md || true
RUN rm i18n/*.json || true

FROM gcr.io/distroless/nodejs:18
ARG BUILD_DATE
ARG VCS_REF
LABEL maintainer="Bjoern Kimminich <bjoern.kimminich@owasp.org>" \
  org.opencontainers.image.title="OWASP Juice Shop" \
  org.opencontainers.image.description="Probably the most modern and \
sophisticated insecure web application" \
  org.opencontainers.image.authors="Bjoern Kimminich \
<bjoern.kimminich@owasp.org>" \
  org.opencontainers.image.vendor="Open Web Application Security \
Project" \
  org.opencontainers.image.documentation="https://help.owasp-juice.shop" \
  org.opencontainers.image.licenses="MIT" \
  org.opencontainers.image.version="14.5.1" \
  org.opencontainers.image.url="https://owasp-juice.shop" \
  org.opencontainers.image.source="https://github.com/juice-shop/juice-
shop" \
  org.opencontainers.image.revision=$VCS_REF \
  org.opencontainers.image.created=$BUILD_DATE
WORKDIR /juice-shop
COPY --from=installer --chown=65532:0 /juice-shop .
USER 65532
EXPOSE 3000

ENV NODE_OPTIONS "-r @contrast/agent"
CMD ["/juice-shop/build/app.js"]
```

## Node.js エージェントを IBM Cloud でインストール

1. [Node.js LTS\(長期サポート\)の最新版をインストール](#)します。
2. エージェントを `npm` からインストールする場合は、アプリケーションのルートディレクトリで次のコマンドを実行します。

```
npm install @contrast/agent
```

または、`yarn` を使用する場合、次のコマンドを実行してエージェントをインストールします。

```
yarn add @contrast/agent
```

3. YAML 設定ファイルを使用して [Node.js エージェントを設定 \(262ページ\)](#)し、エージェントの [認証キー \(37ページ\)](#) およびアプリケーション固有の設定を指定します。

以下は、YAML 設定ファイル(`contrast_security.yaml`)のサンプルです。<URL>、<UserName>、<APIKey>、<ServiceKey>の箇所をご利用の認証情報に置き換え、<ServerName>にはアプリケーションがレポートする IBM Cloud のサーバ名を指定できます(このようにサーバ名を指定すると、Contrast Web インターフェイスで表示した際にサーバを特定できます)。

```
contrast:
  url: <URL>
  user_name: <UserName>
```

```
api_key: <APIKey>
service_key: <ServiceKey>
server:
  name: <ServerName>
```

4. アプリケーションのルートディレクトリに `contrast` という名前のフォルダを作成し、`node-contrast.tgz` ファイルと `contrast_security.yaml` ファイルを `contrast` フォルダに移動します。
5. アプリケーションの `package.json` ファイルの "scripts": セクションに次のコマンドを追加します。

```
"ibmcloud-with-contrast": "npm install @contrast/agent && node -r \
@contrast/agent index.js -c /home/vcap/app/contrast/
contrast_security.yaml",
```

6. IBM Cloud ではデフォルトで起動スクリプトが実行されるため、前述の手順で指定した `ibmcloud-with-contrast` の行で開始するよう起動コマンドを変更する必要があります。次のコマンドを使用して、エージェントを実行します。

```
"start": "npm run bluemix-with-contrast"
```

そして、`package.json` の "scripts" セクションは以下になるはずですが、

```
"scripts": {
  "bluemix-with-contrast": "npm install @contrast/agent && node -r \
@contrast/agent index.js -c /home/vcap/app/contrast/
contrast_security.yaml",
  "start": "npm run bluemix-with-contrast"
},
```

7. 次のコマンドを使用して、アプリケーションを IBM Cloud にプッシュします。

```
cf push <application-name> -t 180
```

8. 次のコマンドを使用して、エージェントを実行します。

```
npm start contrast
```

9. 手動または自動テストを行なってアプリケーションを操作し、エージェントがインストールされた状態でアプリケーションが正しく機能することを確認してください。
10. アプリケーションサーバが Contrast に認識され、アプリケーションが Contrast に報告されていることを確認します。

## Node.js エージェントのアップデート

Contrast の Node.js エージェントを自動的に更新するのに最も信頼性が高く効果的な方法は、Node.js の npm パッケージマネージャを使用し、利用可能な最新バージョンをダウンロードしてインストールすることです。

npm は通常、Node.js アプリケーションのすべての依存関係を管理するため、すでにビルド環境の一部として利用可能になっているはずですが、Node.js エージェントを更新する頻度と更新の取得先は、組織の設定と Contrast の実装(SaaS 版またはオンプレミス版)によって異なります。

エージェントのアップデートは、手動または自動のどちらでも行うことができます。

### 開始する前に

設定を開始する前に、以下が必要です。

- DevOps の実践と Node の npm パッケージマネージャにある程度の知識があること。
- Contrast エージェントの npm リポジトリへアクセスできること。
- Node.js アプリケーションが Contrast エージェントなしで想定どおりに機能すること。
- 事前に Contrast の Node.js エージェントが正常にインストールされていること。
- 変更管理ポリシーと使用する環境に基づいて、エージェントをアップデートする方法とタイミングを決めていること。



## 重要

Contrast サポートからのアドバイスがない限り、Contrast インスタンスで利用できるバージョンよりも先行したバージョンの Node.js エージェントを使用しないでください。

## 手順

1. Node.js エージェントを npm のパブリック(またはプライベート)リポジトリからインストールします。Contrast の利用状況に応じて、いずれかまたは両方のソースを使用して最新の Node.js エージェントを取得します。
  - **SaaS 版**: npm からエージェントの最新バージョンを入手します。エージェントを使用する前に検証を必要とする場合、承認されたバージョンのみがあるプライベートの npm リポジトリを使用することもできます。
  - **オンプレミス(EOP)版**: M オンプレミス版を利用しているお客様の多くが、Contrast で新しいソフトウェアがリリースされても、コアソフトウェアやエージェントをすぐには更新しません。通常、パブリックリポジトリ(npm など)は、新しいバージョンのエージェントを提供しますが、新しいバージョンのエージェントは、古いバージョンの Contrast で動作するように設計やテストされていません。オンプレミス版をご利用の場合は、インストールしたオンプレミス版の Contrast と一致するエージェントのバージョンのみを保存するプライベート npm リポジトリから、エージェントの更新を取得してください。
2. エージェントをインストールし、スクリプトにより最適な方法で自動アップデートを行います。
  - **package.json を使う**: このファイルには、npm(パブリックまたはプライベート)からのアーティファクトを使用して、Node.js アプリケーションをビルドするたびに自動的に解決する依存関係を指定します。ここに Contrast の Node.js エージェントを含めることで、アプリケーションの新しいビルドを常に最新バージョンのエージェントに合わせることが簡単にできます。例:

```
{
  "name": "sample_application",
  "version": "1.0.0",
  "description": "",
  "main": "index.js",
  "scripts": {
    "start": "nodemon",
    "contrast": "node -r @contrast/agent index.js"
  },
  "keywords": [],
  "author": "",
  "license": "ISC",
  "dependencies": {
    "express": "^4.17.1",
    "@contrast/agent": "latest",
  },
  "devDependencies": {
    "nodemon": "^1.19.2"
  }
}
```

そして、アプリケーションをビルドする際には常に `$ npm update` コマンドを使用します。これにより、Node.js エージェントが npm から Node.js アプリケーションに自動的にダウンロードされ、追加または更新されます。

- **コマンドラインによる手動インストールおよび更新**: 組織によっては、`package.json` ファイルが環境間で一貫している必要がある場合や、すべての環境に Contrast の Node.js エージェント

をインストールする予定がない場合があります。このような場合、手動でエージェントをインストールします。Node.js のビルドプロセスの一部として手動でエージェントを更新できます。次のコマンドを使用して、Contrast の Node.js エージェントを手動で取得し、npm(パブリックまたはプライベート)から Node.js アプリケーションに追加または更新します。

```
$ npm install @contrast/agent --no-optional
```

3. いずれの方法でインストールしても、インストール後に以下のような出力が表示されます。

```
$ npm install @contrast/agent

> grpc@1.24.4 install /Users/<aUserName>/Documents/test-apps/juice-shop/node_modules/grpc> node-pre-gyp install --fallback-to-build --library=static_library

node-pre-gyp WARN Using request for node-pre-gyp https download[grpc] \
Success: "/Users/<aUserName>/Documents/test-apps/juice-shop/node_modules/grpc/src/node/extension_binary/node-v72-darwin-x64-unknown/grpc_node.node" is installed via remotenpm WARN jest-config@26.6.1 \
requires a peer of ts-node@>=9.0.0 but none is installed. You must \
install peer dependencies yourself.npm WARN jsdom@16.4.0 requires a \
peer of canvas@^2.5.0 but none is installed. You must install peer \
dependencies yourself.npm WARN ws@7.3.1 requires a peer of \
bufferutil@^4.0.1 but none is installed. You must install peer \
dependencies yourself.npm WARN ws@7.3.1 requires a peer of utf-8-validate@^5.0.2 but none is installed. You must install peer \
dependencies yourself.

+ @contrast/agent@3.4.0added 19 packages from 43 contributors, updated \
5 packages and audited 1995 packages in 14.904sfound 19 vulnerabilities \
(5 low, 7 moderate, 4 high, 3 critical)
  run `npm audit fix` to fix them, or `npm audit` for details
```

4. インストール/アップデートが成功したかどうかを確認するには、次のコマンドを実行して、出力結果を確認してください。

```
$ npm list | grep contrast
@contrast/agent@3.4.0
@contrast/distinguish-prebuilt@2.0.0
@contrast/escodegen@1.16.0
@contrast/esprima@4.1.1
@contrast/estraverse@5.1.0
@contrast/flat@4.2.0
@contrast/fn-inspect@2.3.0
@contrast/heapdump@1.0.0
@contrast/protobuf-api@2.2.3
@contrast/require-hook@1.1.2
@contrast/synchronous-source-maps@1.1.0
```

## 関連項目

- [Node.js のサポート対象テクノロジー \(251ページ\)](#)
- [Node.js エージェントのインストール \(253ページ\)](#)

## Node.js エージェントの設定

全てのエージェントには[基本の設定 \(35ページ\)](#)があり、設定値には[優先順位 \(36ページ\)](#)があります。

Node.js エージェントを設定する方法はいくつかありますが、一般的には以下のようになります。

- 組織やコンテナ内の全てのアプリケーションに共通する設定値(例えば、ログのリダイレクトやプロキシの設定など)を指定するには、YAML 設定ファイルを使用します。こちらの[テンプレート \(264ページ\)](#)には、Node.js エージェントで有効な設定オプションが全てあります。YAML 設定については、[こちらの説明 \(38ページ\)](#)を参照してください。
- エージェントの認証キーやアプリケーション固有の設定値を指定するには、[環境変数 \(263ページ\)](#)を使用します。環境変数については、[こちらの説明 \(56ページ\)](#)を参照してください。



### ヒント

[Contrast エージェント設定エディタ \(39ページ\)](#)を使用すると、YAML 設定ファイルの作成やアップロード、YAML の検証、推奨される設定値の表示などができます。エディタでは、必要に応じて適切な環境変数も表示されます。

## 環境変数

アプリケーション固有の設定値(サーバの環境、アプリケーション名、エージェントログの設定など)には、環境変数を使用します。また、Node.js エージェントで有効なその他のプロパティの設定にも環境変数を使用できます。

有効なプロパティの全リストは [Node.js エージェントの YAML テンプレート \(264ページ\)](#) にありますが、ここではよく使用される環境変数をいくつか紹介します。

環境変数	説明
CONTRAST__API__SERVICE_KEY	Contrast との通信に必要なサービスキーを設定します。
CONTRAST__API__API_KEY	Contrast との通信に必要な API キーを設定します。
CONTRAST__API__USER_NAME	Contrast との通信に必要なユーザ名を設定します。
CONTRAST__API__URL	Contrast Web インターフェイスの URL を設定します。
CONTRAST__APPLICATION__NAME	Contrast に報告されるアプリケーション名を設定します。
CONTRAST__CONFIG__PATH	設定すると、YAML 設定ファイルのデフォルトの場所を上書きします。(他の環境変数とは異なり、この環境変数は YAML プロパティとして設定することはできず、アンダースコアは 1 つだけです。)
CONTRAST__SERVER__PATH	Contrast に報告されるサーバのパスを上書きします。
CONTRAST__SERVER__NAME	コンテナ化されたアプリケーションで多数のサーバレコードが生成される場合に、一貫したサーバ名を指定します。マイクロサービス名やアプリ名になることが考えられます。
CONTRAST__AGENT__DIAGNOSTICS__ENABLE	診断やトラブルシューティングの情報を追跡するために、起動時に設定ファイルとシステムファイルを作成します。デフォルトは、true です。
CONTRAST__AGENT__LOGGER__APPEND	false に設定すると、毎日ログファイルを追加してローテーションする代わりに、起動時に新しいログファイルを作成します。デフォルトは、true です。
CONTRAST__AGENT__LOGGER__LEVEL	ログのレベル: FATALERRORWARNINFODEBUGTRACE のいずれかを設定します。デフォルトは、ERROR です。
CONTRAST__AGENT__LOGGER__PATH	Contrast のデバッグログを保存するパスを指定します。デフォルトは、 <i>node-contrast.log</i> です。
CONTRAST__AGENT__LOGGER__STDOUT	false に設定すると、(stdout)へ出力されなくなります。デフォルトは、true です。



## 注記

Node.js エージェントでは、環境変数 DEBUG に手動の設定が必要です。環境変数 DEBUG に Contrast の名前空間を含むように設定(DEBUG=contrast:\*)しない限り、INFO レベルのメッセージはコンソールには記録されません。名前空間を操作して、特定のパスの表示/非表示を切り替えることもできます。これは、ファイルシステムにアクセスできない環境(Docker や ECS など)で有用です。

Node.js のログをリダイレクトしたい場合は、[npm のサイト](#)の他の例を参考にするか、[サポートまでお問い合わせ](#)ください。

## Node.js エージェントの YAML テンプレート

YAML 設定ファイルを使用して Node.js エージェントを設定する場合には、以下のテンプレートをご利用ください(YAML 設定については、[こちらの説明 \(38ページ\)](#)を参照してください)。

YAML 設定ファイルは、デフォルトの場所に配置します : /etc/contrast/  
contrast\_security.yaml

```
# \  
=====\  
==\  
# Use the properties in this YAML file to configure a Contrast agent.  
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html  
# to determine the order of precedence for configuration values.  
# \  
=====\  
==\  
  
# Use this setting if you want to temporarily disable a Contrast agent.  
# Set to `true` to enable the agent; set to `false` to disable the agent.  
# enable: true  
  
# \  
=====\  
==\  
# api  
# Use the properties in this section to connect the agent to the Contrast \  
UI.  
# \  
=====\  
==\  
api:  
  
# ***** REQUIRED *****  
# Set the URL for the Contrast UI.  
url: https://app.contrastsecurity.com/Contrast  
  
# ***** REQUIRED *****  
# Set the API key needed to communicate with the Contrast UI.  
api_key: NEEDS_TO_BE_SET  
  
# ***** REQUIRED *****
```



```
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# Set the default request timeout.
# timeout_ms: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Certificate
# PEM file for communication with the Contrast UI.
# cert_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Key PEM
# file for communication with the Contrast UI.
# key_file: NEEDS_TO_BE_SET

# If the Key file requires a password, it can be set here or in
# the matching ENV value (`CONTRAST__CERTIFICATE__KEY_PASSWORD`).
# key_password: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid **contrast.proxy.host**
# and **contrast.proxy.port** will enable the proxy.
```

```

# enable: NEEDS_TO_BE_SET

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# Set to limit the length of Error stack traces to a specified number.
# stack_trace_limit: 10

# \
=====
# agent.diagnostics
# Use the properties in this section to specify
# whether diagnostic files should be created or not
#
# \
=====
# diagnostics:

# Creates config and system info files
# at startup if true. True by default.
#
# The same thing can be achieved by setting the
# CONTRAST_AGENT_DIAGNOSTICS_ENABLE=[true/false] env variable.
#
# enable: true

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
#
# Example - `/opt/Contrast/contrast.log` creates a log in the

```

```

# `/opt/Contrast` directory, and rotates it automatically as needed.
#
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Set to `false` for the agent to always create a
# new log file instead of appending and rolling.
# append: true

# Set to `true` to redirect all logs to
# `stdout` instead of the file system.
# stdout: false

# Set the roll size for log files in megabytes. The agent will
# attempt to prevent the log file from being larger than this size.
# This feature is only available in agent version >=4.0.0
# roll_size: 100M

# Set the number of backup files to keep. Set to `0` to disable.
# This feature is only available in agent version >=4.0.0
# backups: 10

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

```

```
# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.service
# The following properties are used by the Contrast Service.
# \
=====
# service:

# Set to `false` to disallow the service to be started, and
# effectively disable the agent, if read by the service. If the
# agent reads this property, it disallows service auto-start.
# enable: true

# Set to `true` to enable listening for gRPC connections.
# The `socket`, `host` and `port` fields will be used for
# configuring the gRPC server in place of the legacy RPC server.
# grpc: false

# If this property is defined, the service is
# listening on a Unix socket at the defined path.
# socket: /tmp/service.sock
```

```

# ***** REQUIRED *****
# Set the the hostname or IP address of the Contrast
# service to which the Contrast agent should report.
host: localhost

# ***** REQUIRED *****
# Set the the port of the Contrast service
# to which the Contrast agent should report.
port: 30555

# \
=====
# agent.service.teamserver_retry
# The following properties are used by the Teamserver HTTP client
# to configure failed request retrying in the Contrast service.
# \
=====
# teamserver_retry:

# Enable retrying HTTP requests to the Teamserver endpoint.
# enable: true

# How long to wait between retries in milliseconds.
# interval_ms: 5000

# How many times to retry HTTP requests to Teamserver before giving \
up.
# max_attempts: 3

# \
=====
# agent.service.logger
# The following properties are used by the logger in the
# Contrast service. If the properties are not defined, the
# service uses the logging values from the Contrast UI.
# \
=====
# logger:

# Set the the log output level. Options are `OFF`, `FATAL`,
# `ERROR`, `WARN`, `INFO`, `DEBUG`, `TRACE`, and `ALL`.
# level: ERROR

# Override the name of the process used in logs.
# progname: Contrast Service

# Set to `true` to send log output to `stdout`.
# stdout: false

# \
=====
# agent.heap_dump
# The following properties are used to trigger heap dumps from within
# the agent to snapshot the behavior of instrumented applications.
# \

```

```

=====
# heap_dump:

# Set to `true` for the agent to automatically
# take heap dumps of the instrumented application.
# enable: false

# Set the location to which to save the heap dump files. If relative,
# the path is determined based on the process' working directory.
# path: contrast_heap_dumps

# Set the amount of time to wait, in milliseconds,
# after agent startup to begin taking heap dumps.
# delay_ms: 10_000

# Set the amount of time to wait, in milliseconds, between each heap \
dump.
# window_ms: 10_000

# Set the number of heap dumps to take before disabling this feature.
# count: 5

# \
=====
# agent.node
# The following properties apply to any Node configurations.
# \
=====
# node:

# Set the location of the application's `package.json` file.
# app_root: NEEDS_TO_BE_SET

# \
=====
# agent.node.rewrite_cache
# Use the following properties to set up rewrite caching in the agent.
# \
=====
# rewrite_cache:

# Set to `true` to enable rewrite caching.
# enable: false

# Set the location of the rewrite cache source.
# path: NEEDS_TO_BE_SET

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==

```

```
# inventory:

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Set to `true` to trust incoming strings when they pass
# custom validators (Mongoose, Joi, validator, fastify-static)
# This feature is only available in agent version 4.10.0 and later
# trust_custom_validators: false

# When set to `true`, string tracking will occur lazily as user-controlled
# values are accessed by application code. When `false`, tracking will
# occur at the time of input parsing and will be limited to 250 values.
# This feature is only available in agent version 4.18.0 and later
# enable_lazy_tracking: true

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5
```

```
# \  
=====\  
==  
# protect  
# Use the properties in this section to override Protect features.  
# \  
=====\  
==  
# protect:  
  
# Use the properties in this section to determine if the  
# Protect feature should be enabled. If this property is not  
# present, the decision is delegated to the Contrast UI.  
# enable: false  
  
# \  
=====\  
# protect.probe_analysis  
# Use the settings in this section to  
# control the behavior of probe analysis.  
# Support for this option is limited to Node agent versions >= 5  
# \  
=====\  
# probe_analysis:  
  
# Set to `false` to disable probe analysis.  
# enable: true  
  
# \  
=====\  
# protect.rules  
# Use the following properties to set simple  
# rule configurations for the Node protect agent.  
# \  
=====\  
# rules:  
  
# Define a list of Protect rules to disable in the agent.  
# The rules must be formatted as a comma-delimited list.  
# disabled_rules: NEEDS_TO_BE_SET  
  
# \  
=====\  
# protect.rules.bot-blocker  
# Use the following selection to configure if the  
# agent blocks bots. Set to `true` to enable blocking.  
# \  
=====\  
# bot-blocker:  
  
# Set to `true` for the agent to block known bots.  
# enable: false  
  
# \  
=====
```



```
# protect.rules.sql-injection
# Use the following settings to configure the sql-injection rule.
# \
=====
# sql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.cmd-injection-semantic-chained-commands
# Use the following properties to configure how the
# 'command injection - chained commands' rule works
# \
=====
# cmd-injection-semantic-chained-commands:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.cmd-injection-semantic-dangerous-paths
# Use the following properties to configure how the
# 'command injection - dangerous paths' rule works
# \
=====
```

```
# cmd-injection-semantic-dangerous-paths:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# \
```

```
=====
# protect.rules.cmd-injection-command-backdoors
# Use the following properties to configure how the
# 'command injection - command backdoors' rule works
# \
```

```
=====
# cmd-injection-command-backdoors:
```

```
# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# \
```

```
=====
# protect.rules.path-traversal-semantic-file-security-bypass
# Use the following properties to configure how the
# 'path traversal - file security bypass' rule works
# \
```

```
=====
# path-traversal-semantic-file-security-bypass:
```

```
# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# \
```

```
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
```

```
=====
# path-traversal:
```

```
# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
```

```
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.unsafe-file-upload
# Use the following properties to configure
# how the unsafe file upload rule works.
# \
=====
# unsafe-file-upload:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
```

```

# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.untrusted-deserialization
# Use the following properties to configure
# how the untrusted deserialization rule works.
# \
=====
# untrusted-deserialization:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.ssjs-injection
# Use the following properties to configure
# how the SSJS Injection rule works.
# \
=====
# ssjs-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====

```

```
# protect.rules.nosql-injection
# Use the following properties to configure
# how the NOSQL Injection rule works.
# \
=====
# nosql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.nosql-injection-mongo
# Use the following properties to configure
# how the NOSQL Injection rule works.
# \
=====
# nosql-injection-mongo:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET
```

```

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Pass arguments to the underlying application.
# args: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

```

```
# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET
```

```
# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==

# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
```

```

# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# Set the default request timeout.
# timeout_ms: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Certificate
# PEM file for communication with the Contrast UI.
# cert_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Key PEM
# file for communication with the Contrast UI.
# key_file: NEEDS_TO_BE_SET

# If the Key file requires a password, it can be set here or in
# the matching ENV value (`CONTRAST__CERTIFICATE__KEY_PASSWORD`).
# key_password: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid contrast.proxy.host
# and contrast.proxy.port will enable the proxy.
# enable: NEEDS_TO_BE_SET
    
```



```
# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# Set to limit the length of Error stack traces to a specified number.
# stack_trace_limit: 10

# \
=====
# agent.diagnostics
# Use the properties in this section to specify
# whether diagnostic files should be created or not
#
# \
=====
# diagnostics:

# Creates config and system info files
# at startup if true. True by default.
#
# The same thing can be achieved by setting the
# CONTRAST_AGENT_DIAGNOSTICS_ENABLE=[true/false] env variable.
#
# enable: true

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
#
# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
```

```

#
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Set to `false` for the agent to always create a
# new log file instead of appending and rolling.
# append: true

# Set to `true` to redirect all logs to
# `stdout` instead of the file system.
# stdout: false

# Set the roll size for log files in megabytes. The agent will
# attempt to prevent the log file from being larger than this size.
# This feature is only available in agent version >=4.0.0
# roll_size: 100M

# Set the number of backup files to keep. Set to `0` to disable.
# This feature is only available in agent version >=4.0.0
# backups: 10

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

```

```

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.service
# The following properties are used by the Contrast Service.
# \
=====
# service:

# Set to `false` to disallow the service to be started, and
# effectively disable the agent, if read by the service. If the
# agent reads this property, it disallows service auto-start.
# enable: true

# Set to `true` to enable listening for gRPC connections.
# The `socket`, `host` and `port` fields will be used for
# configuring the gRPC server in place of the legacy RPC server.
# grpc: false

# If this property is defined, the service is
# listening on a Unix socket at the defined path.
# socket: /tmp/service.sock

# ***** REQUIRED *****

```

```
# Set the the hostname or IP address of the Contrast
# service to which the Contrast agent should report.
host: localhost

# ***** REQUIRED *****
# Set the the port of the Contrast service
# to which the Contrast agent should report.
port: 30555

# \
=====
# agent.service.teamserver_retry
# The following properties are used by the Teamserver HTTP client
# to configure failed request retrying in the Contrast service.
# \
=====
# teamserver_retry:

# Enable retrying HTTP requests to the Teamserver endpoint.
# enable: true

# How long to wait between retries in milliseconds.
# interval_ms: 5000

# How many times to retry HTTP requests to Teamserver before giving \
up.
# max_attempts: 3

# \
=====
# agent.service.logger
# The following properties are used by the logger in the
# Contrast service. If the properties are not defined, the
# service uses the logging values from the Contrast UI.
# \
=====
# logger:

# Set the the log output level. Options are `OFF`, `FATAL`,
# `ERROR`, `WARN`, `INFO`, `DEBUG`, `TRACE`, and `ALL`.
# level: ERROR

# Override the name of the process used in logs.
# progname: Contrast Service

# Set to `true` to send log output to `stdout`.
# stdout: false

# \
=====
# agent.heap_dump
# The following properties are used to trigger heap dumps from within
# the agent to snapshot the behavior of instrumented applications.
# \
=====
```

```
# heap_dump:

# Set to `true` for the agent to automatically
# take heap dumps of the instrumented application.
# enable: false

# Set the location to which to save the heap dump files. If relative,
# the path is determined based on the process' working directory.
# path: contrast_heap_dumps

# Set the amount of time to wait, in milliseconds,
# after agent startup to begin taking heap dumps.
# delay_ms: 10_000

# Set the amount of time to wait, in milliseconds, between each heap \
dump.
# window_ms: 10_000

# Set the number of heap dumps to take before disabling this feature.
# count: 5

# \
=====
# agent.node
# The following properties apply to any Node configurations.
# \
=====
# node:

# Set the location of the application's `package.json` file.
# app_root: NEEDS_TO_BE_SET

# \
=====
# agent.node.rewrite_cache
# Use the following properties to set up rewrite caching in the agent.
# \
=====
# rewrite_cache:

# Set to `true` to enable rewrite caching.
# enable: false

# Set the location of the rewrite cache source.
# path: NEEDS_TO_BE_SET

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:
```

```
# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Set to `true` to trust incoming strings when they pass
# custom validators (Mongoose, Joi, validator, fastify-static)
# This feature is only available in agent version 4.10.0 and later
# trust_custom_validators: false

# When set to `true`, string tracking will occur lazily as user-controlled
# values are accessed by application code. When `false`, tracking will
# occur at the time of input parsing and will be limited to 250 values.
# This feature is only available in agent version 4.18.0 and later
# enable_lazy_tracking: true

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# \
```

```
=====  
==  
# protect  
# Use the properties in this section to override Protect features.  
# \  
=====  
==  
# protect:  
  
# Use the properties in this section to determine if the  
# Protect feature should be enabled. If this property is not  
# present, the decision is delegated to the Contrast UI.  
# enable: false  
  
# \  
=====  
# protect.probe_analysis  
# Use the settings in this section to  
# control the behavior of probe analysis.  
# Support for this option is limited to Node agent versions >= 5  
# \  
=====  
# probe_analysis:  
  
# Set to `false` to disable probe analysis.  
# enable: true  
  
# \  
=====  
# protect.rules  
# Use the following properties to set simple  
# rule configurations for the Node protect agent.  
# \  
=====  
# rules:  
  
# Define a list of Protect rules to disable in the agent.  
# The rules must be formatted as a comma-delimited list.  
# disabled_rules: NEEDS_TO_BE_SET  
  
# \  
=====  
# protect.rules.bot-blocker  
# Use the following selection to configure if the  
# agent blocks bots. Set to `true` to enable blocking.  
# \  
=====  
# bot-blocker:  
  
# Set to `true` for the agent to block known bots.  
# enable: false  
  
# \  
=====  
# protect.rules.sql-injection
```

```
# Use the following settings to configure the sql-injection rule.
# \
```

```
=====
# sql-injection:
```

```
# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# \
```

```
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
```

```
=====
# cmd-injection:
```

```
# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# \
```

```
=====
# protect.rules.cmd-injection-semantic-chained-commands
# Use the following properties to configure how the
# 'command injection - chained commands' rule works
# \
```

```
=====
# cmd-injection-semantic-chained-commands:
```

```
# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# \
```

```
=====
# protect.rules.cmd-injection-semantic-dangerous-paths
# Use the following properties to configure how the
# 'command injection - dangerous paths' rule works
# \
```

```
=====
# cmd-injection-semantic-dangerous-paths:
```



```
# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# \
```

```
=====
# protect.rules.cmd-injection-command-backdoors
# Use the following properties to configure how the
# 'command injection - command backdoors' rule works
# \
```

```
=====
# cmd-injection-command-backdoors:
```

```
# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# \
```

```
=====
# protect.rules.path-traversal-semantic-file-security-bypass
# Use the following properties to configure how the
# 'path traversal - file security bypass' rule works
# \
```

```
=====
# path-traversal-semantic-file-security-bypass:
```

```
# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# \
```

```
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
```

```
=====
# path-traversal:
```

```
# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
```

```
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.unsafe-file-upload
# Use the following properties to configure
# how the unsafe file upload rule works.
# \
=====
# unsafe-file-upload:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# \  
=====
```

```
# protect.rules.xxe  
# Use the following properties to configure  
# how the XML external entity works.  
# \  
=====
```

```
# xxe:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====
```

```
# protect.rules.untrusted-deserialization  
# Use the following properties to configure  
# how the untrusted deserialization rule works.  
# \  
=====
```

```
# untrusted-deserialization:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====
```

```
# protect.rules.ssjs-injection  
# Use the following properties to configure  
# how the SSJS Injection rule works.  
# \  
=====
```

```
# ssjs-injection:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====
```

```
# protect.rules.nosql-injection
```

```
# Use the following properties to configure
# how the NOSQL Injection rule works.
# \
=====
# nosql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.nosql-injection-mongo
# Use the following properties to configure
# how the NOSQL Injection rule works.
# \
=====
# nosql-injection-mongo:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
```

```
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Pass arguments to the underlying application.
# args: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
```

```
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET
```

## コンテナの起動時間を短縮する

Contrast エージェントをインストールしたアプリケーションを起動すると、アプリケーションおよびアプリケーションがロードする依存関係のあるコードの両方にコード変換が適用されます。このコード変換が行われるため、Contrast エージェントを使用したアプリケーションの起動時間が長くなります。

Node.js エージェントのバージョン 4.x 以降、アプリケーションを起動する前にプリコンパイルできるコマンドラインユーティリティを提供するようになりました。Contrast エージェントを有効にしてプリコンパイルされたアプリケーションを起動すると、変換済みファイルがディスクからロードされて起動時間が大幅に改善されます。

## リライタ CLI を使用する

1. Node.js エージェントの設定ファイル(`contrast_security.yaml`)で以下を行います。
  - リライタのキャッシュを有効にし、キャッシュのパスを指定します。
  - ログレベルを指定します。



### 注記

CLI 変数または環境変数 (263ページ)を指定してリライタを起動して、YAML 設定をオーバーライドすることができます。例えば、標準出力(stdout)やディスクへのログ出力を防ぐ場合に、次の様にオーバーライドします。

```
npx -p @contrast/agent --no contrast-transpile index.js --
agent.logger.stdout false --agent.logger.path /dev/null;
```

`npx` コマンドが Contrast Security からのものであり、サプライチェーン攻撃を試みる悪意のある人物からではないことを確認するために、`-p @contrast/agent --no` オプションを使用することが重要です。

- `-p` は、`--package` の省略形で、`@contrast/agent` パッケージにのみコマンドを使用するよう `npx` に指定します。
- `--no` は、非推奨となった `--no-install` オプションの新しいオプション名で、コマンドのバイナリが見つからない場合に `npm` からインストールを行わないよう `npx` に指定します。

`npx` コマンドを実行する前に、Contrast エージェントと `npx` バイナリが正常にインストールされていることを想定しています。

- また、Protect か Assess を明示的に有効にする必要があります。

例：

```
agent:
  logger:
    level: info
    path: ./node-contrast
  node:
    rewrite_cache:
      enable: true
      path: ./rewrite_cache
assess:
  enable: true
protect:
  enable: false
```

2. アプリケーションのエントリーポイント(例えば、index.js)を指定して、実行ファイルを起動します。例：

```
npx -p @contrast/agent --no contrast-transpile index.js --
agent.logger.level trace;
...
trace: 2021-07-12T18:31:15.128Z 2934603 contrast:rewrite - successfully \
rewrote code for /path/to/app/index.js
trace: 2021-07-12T18:31:15.186Z 2934603 contrast:rewrite - successfully \
rewrote code for /path/to/app/node_modules/koa/lib/application.js
trace: 2021-07-12T18:31:15.251Z 2934603 contrast:rewrite - successfully \
rewrote code for /path/to/app/node_modules/koa-router/lib/router.js
trace: 2021-07-12T18:31:15.314Z 2934603 contrast:rewrite - successfully \
rewrote code for /path/to/app/node_modules/@koa/router/lib/router.js
...
info: 2021-07-12T18:31:41.608Z 2946030 contrast:cli-rewriter - \
rewriting complete [26.625s]
```



### 注記

現在、Node.js エージェントのリライタ CLI は、Assess を有効にして実行するアプリケーションのプリコンパイルのみをサポートしています。Protect と Assess のどちらが有効であるかによって、エージェントがソースコードを変換する方法は異なります。Protect では、Assess よりも必要なソース変換が少なく、同じ起動遅延が発生することはありません。

3. リライタ処理が完了したら、通常と同じように Contrast を有効にしてアプリケーションを起動します。(例、`node -r @contrast/agent index.js`)

## ESM で Node.js エージェントを使用する

Contrast Node.js エージェントは、Node.js のサーバサイドアプリケーションで ECMAScript モジュール(ESM)を使用する場合に限定的なサポートを提供します。ESM は JavaScript クライアントサイドのコードをパッケージ化するための標準仕様で、現在 Node.js は ESM をサポートしています。

ESM のサーバサイドアプリケーションを使用する場合、Contrast Node.js エージェントを実行する方法は 2 つあります。

- 実行中のコードが ESM であり、ESM として実行される必要があることを明示的にするために、MJS ファイル拡張子を使用します。ファイル拡張子によるモジュールシステムの決定についての詳細は、Node.js のドキュメントを参照してください。

MJS 拡張子を使用すると、Node.js は ESM が記述されていることを認識し、JavaScript は ESM として解析されます。CJS についても同様で、Node.js は CJS ファイル拡張子を CommonJS として実行する必要があることを認識し、JavaScript は CommonJS として解析されます。

- もしくは、次のように package.json に "type": "module" を指定することで、CommonJS ではなく ESM として Node.js アプリケーションを実行できます。

```
"main": "index.js",  
"type": "module",
```

これにより、Node.js は package.json 下の JS ファイルを ESM として解析するようになります。それ以外の場合、デフォルトでは(または、"type": "commonjs" 指定している場合)、Node.js は JS ファイルを CommonJS として解析します。



### 注記

Contrast Node.js エージェントは、ESM の条件付きエクスポート(Conditional Exports)をサポートしていません。

ECMAScript でのエージェントによる検査は試験的であり、Contrast でサポートするには少なくとも Node.js のバージョン 14.15.0 が必要です。

ESM(または ESM と CJS の組み合わせ)を使用するアプリケーションに Contrast エージェントを組み込む場合は、次のようにアプリケーションを起動します。

```
Usage: node --experimental-loader @contrast/agent/esm.mjs  
app-main.mjs [agent arguments] -- [app arguments]
```

## トランスパイラ、コンパイラ、ソースマップおよび Node.js エージェント

Node.js エージェントは、TypeScript など JavaScript にコンパイルされる言語で書かれたアプリケーションをサポートします。Node.js エージェントは、JavaScript のみに組み込まれますが、アプリケーションを JavaScript にコンパイルするようトランスパイラを設定した場合、TypeScript も使用できます。



### 注記

結果として生成される JavaScript とソースが一致しない場合があります。そのため、報告されるメタデータ(やなど)は、元のソースではなくコンパイルした結果を参照します。

TypeScript など一部の言語では、ランタイム前にコードのプリコンパイルが必要なものがあります。このような場合、Node.js エージェントは、アプリケーションのコンパイル済エントリポイントを指す必要があります。

これを行うには、-r オプションを使用して Node.js エージェントを設定します。

```
scripts: {  
  "test": "...",  
  "start": "...",  
  "contrast": "node -r @contrast/agent /path/to/transpiled/entrypoint.js"  
}
```



## ソースマップ

ソースマップを使用すると、TypeScript のソースとトランスパイルされた JavaScript 間で対応する行番号を確認できます。

ソースマップを使用するには、YAML 設定で Babel 変換(enable\_babel)と変換キャッシュ(rewrite\_cache)を有効にする必要があります。

```
agent:
  node:
    rewrite_cache:
      enable: true
      path: ./cache
    enable_babel: true
```

有効にすると、エージェントはロードされているソースと同じディレクトリにあるソースマップ(map ファイル)を検索します(例: /home/app/index.js ファイルがロードされると、/home/app/index.js.map が検索されます)。

ソースマップがまだない場合は、ソースマップを生成するために必要なフラグを使用して再コンパイルする必要があります。これはトランスパイラによって異なりますので、お使いのトランスパイラのオプションを確認してください。例えば、TypeScript の場合は、--source-map フラグを TypeScript コンパイラ(tsc)に追加するか、tsconfig.json の"compilerOptions"セクションに"sourceMap": true エントリを追加します。

## Node.js のテレメトリ

Node.js エージェントは、テレメトリを使用して、使用状況に関するデータを収集します。テレメトリは、エージェントを組み込んだアプリケーションでエージェントのセンサーが最初にロードされた時に収集されます。現在は、起動時のみデータが送信されます。将来的には、エージェントを組み込んだアプリケーションが実行され、疎通されているときに、エージェントからエラーや測定値が送信される予定です。

弊社では、お客様のプライバシーは非常に大切である(828ページ)と考えています。このテレメトリ機能は、アプリケーションのデータを収集するものではありません。データは匿名化されてから、Contrast に安全に送信されます。そして、集約されたデータは暗号化されて保存され、アクセスが制限されます。収集されたデータは、全て 1 年後に削除されます。

テレメトリ機能で収集されるのは、以下のデータです。

エージェントのバージョン	データ
@contrast/agent 4.12.0 以降	エージェントのバージョン
	オペレーティングシステムとバージョン
	Node.js のバージョン
	アプリケーションがコンテナで実行されているか(Y/N)

テレメトリ機能を停止するには、CONTRAST\_AGENT\_TELEMETRY\_OPTOUT という環境変数に 1 または true を設定してください。

テレメトリのデータは、<http://telemetry.nodejs.contrastsecurity.com> に安全に送信されます。ネットワークレベルで通信をブロックすることで、テレメトリ機能を停止することもできます。

## PHP エージェント

Contrast PHP エージェントは、PHP の Web アプリケーションを実行時に解析し、ライブラリの使用状況や脆弱性を検出します。PHP エージェントは、PHP の拡張モジュールとして実装されます。

**注記**

PHP エージェントは、現在、Assess と SCA のみに対応しています。

次のステップ：

- [PHP エージェントをインストール \(298ページ\)](#)
- [PHP エージェントのシステム要件を確認 \(298ページ\)](#)
- [PHP エージェントのサポート対象テクノロジーを確認 \(298ページ\)](#)

**PHP エージェントのサポート対象テクノロジー**

このエージェントでは、以下のテクノロジーをサポートしています。

テクノロジー	サポート対象バージョン	備考
言語のバージョン	• 7.4、8.0、8.1 (NTS)	エージェントは、mbstring および curl 拡張モジュールに依存します。
オペレーティングシステム	• Debian • RHEL/CentOS	
アプリケーションフレームワーク	• Laravel • Symfony • Drupal 8、9	
プロセッサのアーキテクチャ	• AMD64	
サーバ	• Apache	その他、mod_php や php-fpm を使用しているサーバでも動作する可能性がありますが、現在はサポートされていません。
パッケージ管理	• Composer	SCA でサポートされています。

**PHP エージェントのシステム要件**

PHP エージェントをインストールする前に、以下のシステム要件を満たす必要があります。

要件	バージョン	備考
ランタイムシステム	• 64 ビット Linux	

**PHP エージェントのインストール**

PHP エージェントの基本的なインストールは、次のようになります。

1. エージェントパッケージをインストールします。
2. `contrast_security.yaml` をダウンロードし、適切なパスに置きます。
3. Contrast エージェント拡張機能を有効にするよう PHP インタプリタを設定します。
4. アプリケーションの疎通やテストを行います。
5. Contrast でアプリケーションが認識されていることを確認します。

具体的なインストール手順については、ご利用の環境に合わせて以下より選択してください。

- [Debian で PHP エージェントをインストール \(298ページ\)](#)
- [RPM で PHP エージェントをインストール \(300ページ\)](#)

**Debian で PHP エージェントをインストール****手順**

PHP エージェントをインストールするには：

1. <https://pkg.contrastsecurity.com> からエージェントパッケージを取得します。以下のコマンドで、Contrast のパッケージリポジトリをシステムに登録します。

```
curl \
  https://pkg.contrastsecurity.com/api/gpg/key/public | sudo apt-key \
add -

echo "deb https://pkg.contrastsecurity.com/debian-public/ $(sed -rne 's/
^VERSION_CODENAME=(.*)$/\1/p' /etc/*ease) contrast" \
  | sudo tee /etc/apt/sources.list.d/contrast.list

echo "deb https://pkg.contrastsecurity.com/debian-public/ all contrast" \
  | sudo tee -a /etc/apt/sources.list.d/contrast.list
```

- 完了したら、以下のコマンドでエージェントをインストールします。

```
sudo apt-get update && sudo apt-get install contrast-php-agent
```



### 注記

PHP がこの拡張モジュールを使用するように設定されると、インタプリタが実行されるたびにこの拡張モジュールが使用されるようになります。このステップは、アプリケーション自体を実行する直前まで遅らせる必要があります。これにより、artisan や他の PHP コマンドの実行時に予期せぬ動作が発生するのを防ぐことができます。

- PHP の設定ファイルである `php.ini` を探します。ほとんどの場合、`/usr/local/etc/php/`内にあります。

`php-config` コマンドを使用できる場合は、`php-config --ini-path` を使用して設定ファイルのパスを検索できます。このパスに設定ファイルがまだ存在しない場合は、作成する必要があります。

- PHP 設定ファイルを編集します。

```
echo "extension=/usr/local/lib/contrast/php/contrast.so" >> `php-
config --ini-path`/php.ini
```

- PHP エージェントの [YAML テンプレート \(301ページ\)](#) が環境変数を使用して、[PHP エージェントを設定 \(301ページ\)](#) します。
- 通常の方法でアプリケーションを開始します。
- アプリケーションの疎通やテストを行います。
- PHP エージェントが実行されているかを確認するには、Contrast Web インターフェイスを確認するか、(設定によっては)PHP エージェントのログ出力を確認するなどしてください。

### 注記

- コマンドラインにフラグを追加することで、PHP CLI を使ってエージェントを使用することが可能です。

```
php -d extension=/usr/local/lib/contrast/php/contrast.so
```

- 現在、ライブラリ解析とルート検出は、アプリケーションへの最初のリクエストで実行されます。そのため、最初のリクエストは、それ以降のリクエストに比べてかなり遅くなることが予想されます。
- このエージェントは、サードパーティの PHP 拡張モジュールとはテストされていません。他のサードパーティの拡張モジュール(xdebug、APM などを含む)が使用された場合のエージェントの動作は不確定です。
- プリロードを有効にすると、エージェントが正しく動作しない場合があります。このエージェントを使用する場合は、プリロードを無効にすることをお勧めします。
- デフォルトでは、エージェントは PHP アプリケーションを実行する際のサーバの作業ディレクトリが、アプリケーションのソースツリーのトップレベルのディレクトリと同じであると想定しています。エージェントは、このパスを使用して、ライブラリ解析とルート検出を行います。パスが異なる場合は、`application.path` の設定を使用して、アプリケーションのトップレベルのディレクトリを指定する必要があります。

## RPM(Red Hat Package Manager)で PHP エージェントをインストール

### 手順

PHP エージェントをインストールするには：

1. <https://pkg.contrastsecurity.com> からエージェントパッケージを取得します。以下のスクリプトをシェルで実行し、お使いの RPM ベースのシステムに Contrast のパッケージリポジトリを設定します。sudo の権限が必要になる場合があります。

```
tee /etc/yum.repos.d/contrast.repo <<-"EOF"  
[contrast]  
name=Contrast centos-$releasever repo  
baseurl=https://pkg.contrastsecurity.com/rpm-public/centos-$releasever/  
gpgcheck=0  
enabled=1  
EOF
```

2. 完了したら、以下のコマンドでエージェントをインストールします。

```
sudo yum install contrast-php-agent
```



#### 注記

PHP がこの拡張モジュールを使用するように設定されると、インタプリタが実行されるたびにこの拡張モジュールが使用されるようになります。このステップは、アプリケーション自体を実行する直前まで遅らせる必要があります。これにより、artisan や他の PHP コマンドの実行時に予期せぬ動作が発生するのを防ぐことができます。

3. PHP の設定ファイルである php.ini を探します。ほとんどの場合、/usr/local/etc/php/内にあります。

php-config コマンドを使用できる場合は `php-config --ini-path` を使用して設定ファイルのパスを検索できます。このパスに設定ファイルがまだ存在しない場合は、作成する必要があります。

4. PHP 設定ファイルを編集します。

```
echo "extension=/usr/local/lib/contrast/php/contrast.so" >> `php-config --ini-path`/php.ini
```

5. [PHP エージェントの YAML テンプレート \(301ページ\)](#) が環境変数を使用して、[PHP エージェントを設定 \(301ページ\)](#) します。
6. 通常の方法でアプリケーションを開始します。
7. アプリケーションの疎通やテストを行います。
8. PHP エージェントが実行されているかを確認するには、Contrast Web インターフェイスを確認するか、(設定によっては)PHP エージェントのログ出力を確認するなどしてください。

### 注記

- コマンドラインにフラグを追加することで、PHP CLI を使ってエージェントを使用することが可能です。

```
php -d extension=/usr/local/lib/contrast/php/contrast.so
```

- 現在、ライブラリ解析とルート検出は、アプリケーションへの最初のリクエストで実行されます。そのため、最初のリクエストは、それ以降のリクエストに比べてかなり遅くなることが予想されます。
- このエージェントは、サードパーティの PHP 拡張モジュールとはテストされていません。他のサードパーティの拡張モジュール(xdebug、APM などを含む)が使用された場合のエージェントの動作は不確定です。



```

=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate
# with the Contrast web interface over a proxy. Set
# value to `false` if you don't want to use the proxy.
# enable: NEEDS_TO_BE_SET

# Set the proxy host. It must be set with port and scheme.
# host: localhost

```

```

# Set the proxy port. It must be set with host and scheme.
# port: 1234

# Set the proxy scheme (e.g., `http` or
# `https`). It must be set with host and port.
# scheme: http

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# Set the proxy user.
# user: NEEDS_TO_BE_SET

# Set the proxy password.
# pass: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
#
# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
#
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Set to `true` to redirect all logs to

```

```

# `stdout` instead of the file system.
# stdout: false

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# \
=====
# agent.service
# The following properties are used by the Contrast Service.
# \
=====
# service:

# Set to `false` to disallow the service to be started, and
# effectively disable the agent, if read by the service. If the
# agent reads this property, it disallows service auto-start.
# enable: true

# Set to `true` to enable listening for gRPC connections.
# The `socket`, `host` and `port` fields will be used for
# configuring the gRPC server in place of the legacy RPC server.
# grpc: false

# If this property is defined, the service is
# listening on a Unix socket at the defined path.
# socket: /tmp/service.sock

# ***** REQUIRED *****
# Set the the hostname or IP address of the Contrast
# service to which the Contrast agent should report.
host: localhost

# ***** REQUIRED *****
# Set the the port of the Contrast service
# to which the Contrast agent should report.
port: 30555

# ***** REQUIRED *****
# Timeout (in milliseconds) that the agent-init
# should wait for the contrast-service

```



```

timeout_ms: 30000

# Set to `true` to enable direct communication with Teamserver.
# bypass: false

# \
=====
# agent.service.logger
# The following properties are used by the logger in the
# Contrast service. If the properties are not defined, the
# service uses the logging values from the Contrast UI.
# \
=====
# logger:

# Set the location to which the Contrast service saves log output.
# If no log file exists at this location, the service creates one.
#
# Example - `/opt/Contrast/contrast_service.log` will
# create a log in the `/opt/Contrast` directory.
#
# path: ./contrast_service.log

# Set the the log output level. Options are `OFF`, `FATAL`,
# `ERROR`, `WARN`, `INFO`, `DEBUG`, `TRACE`, and `ALL`.
# level: ERROR

# Override the name of the process used in logs.
# progname: Contrast Service

# Set to `true` to send log output to `stdout`.
# stdout: false

# \
=====
# agent.go
# The following properties apply to any Go agent-wide configurations.
# \
=====
# go:

# Enable opt-in Go agent features.
# preview: NEEDS_TO_BE_SET

# Enable Go agent self-profiling features.
# profile: NEEDS_TO_BE_SET

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==

```

```
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Set to `false` to disable library analysis.
# analyze_libraries: true

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:
```

```
# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
```

```
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET
```

```
# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==
```

```

# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.

```

```
# \  
=====  
# proxy:  
  
# Set value to `true` for the agent to communicate  
# with the Contrast web interface over a proxy. Set  
# value to `false` if you don't want to use the proxy.  
# enable: NEEDS_TO_BE_SET  
  
# Set the proxy host. It must be set with port and scheme.  
# host: localhost  
  
# Set the proxy port. It must be set with host and scheme.  
# port: 1234  
  
# Set the proxy scheme (e.g., `http` or  
# `https`). It must be set with host and port.  
# scheme: http  
  
# Set the URL for your Proxy Server. The URL form is `scheme://  
host:port`.  
# url: NEEDS_TO_BE_SET  
  
# Set the proxy user.  
# user: NEEDS_TO_BE_SET  
  
# Set the proxy password.  
# pass: NEEDS_TO_BE_SET  
  
# \  
=====  
==  
# agent  
# Use the properties in this section to control the way and frequency  
# with which the agent communicates to logs and the Contrast UI.  
# \  
=====  
==  
# agent:  
  
# \  
=====  
# agent.logger  
# Define the following properties to set logging values.  
# If the following properties are not defined, the  
# agent uses the logging values from the Contrast UI.  
# \  
=====  
# logger:  
  
# Enable diagnostic logging by setting a path to a log file.  
# While diagnostic logging hurts performance, it generates  
# useful information for debugging Contrast. The value set here  
# is the location to which the agent saves log output. If no  
# log file exists at this location, the agent creates a file.
```

```
#
# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
#
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Set to `true` to redirect all logs to
# `stdout` instead of the file system.
# stdout: false

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# \
=====
# agent.service
# The following properties are used by the Contrast Service.
# \
=====
# service:

# Set to `false` to disallow the service to be started, and
# effectively disable the agent, if read by the service. If the
# agent reads this property, it disallows service auto-start.
# enable: true

# Set to `true` to enable listening for gRPC connections.
# The `socket`, `host` and `port` fields will be used for
# configuring the gRPC server in place of the legacy RPC server.
# grpc: false

# If this property is defined, the service is
# listening on a Unix socket at the defined path.
# socket: /tmp/service.sock

# ***** REQUIRED *****
# Set the the hostname or IP address of the Contrast
```

```

# service to which the Contrast agent should report.
host: localhost

# ***** REQUIRED *****
# Set the the port of the Contrast service
# to which the Contrast agent should report.
port: 30555

# ***** REQUIRED *****
# Timeout (in milliseconds) that the agent-init
# should wait for the contrast-service
timeout_ms: 30000

# Set to `true` to enable direct communication with Teamsserver.
# bypass: false

# \
=====
# agent.service.logger
# The following properties are used by the logger in the
# Contrast service. If the properties are not defined, the
# service uses the logging values from the Contrast UI.
# \
=====
# logger:

# Set the location to which the Contrast service saves log output.
# If no log file exists at this location, the service creates one.
#
# Example - `/opt/Contrast/contrast_service.log` will
# create a log in the `/opt/Contrast` directory.
#
# path: ./contrast_service.log

# Set the the log output level. Options are `OFF`, `FATAL`,
# `ERROR`, `WARN`, `INFO`, `DEBUG`, `TRACE`, and `ALL`.
# level: ERROR

# Override the name of the process used in logs.
# progname: Contrast Service

# Set to `true` to send log output to `stdout`.
# stdout: false

# \
=====
# agent.go
# The following properties apply to any Go agent-wide configurations.
# \
=====
# go:

# Enable opt-in Go agent features.
# preview: NEEDS_TO_BE_SET
    
```



```
# Enable Go agent self-profiling features.
# profile: NEEDS_TO_BE_SET

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Set to `false` to disable library analysis.
# analyze_libraries: true

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET
```

```
# \  
=====\  
==  
# protect  
# Use the properties in this section to override Protect features.  
# \  
=====\  
==  
# protect:  
  
# Use the properties in this section to determine if the  
# Protect feature should be enabled. If this property is not  
# present, the decision is delegated to the Contrast UI.  
# enable: false  
  
# \  
=====\  
==  
# application  
# Use the properties in this section for  
# the application(s) hosting this agent.  
# \  
=====\  
==  
# application:  
  
# Override the reported application name.  
#  
# Note - On Java systems where multiple, distinct applications may be  
# served by a single process, this configuration causes the agent to \  
report  
# all discovered applications as one application with the given name.  
#  
# name: NEEDS_TO_BE_SET  
  
# Override the reported application path.  
# path: NEEDS_TO_BE_SET  
  
# Add the name of the application group with which this  
# application should be associated in the Contrast UI.  
# group: NEEDS_TO_BE_SET  
  
# Add the application code this application should use in the Contrast UI.  
# code: NEEDS_TO_BE_SET  
  
# Override the reported application version.  
# version: NEEDS_TO_BE_SET  
  
# Apply labels to an application. Labels must  
# be formatted as a comma-delimited list.  
# Example - `label1,label2,label3`  
#  
# tags: NEEDS_TO_BE_SET
```

```
# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET
```

## Python エージェント

Python エージェントは、最も一般的な Web アプリケーションフレームワークと互換性がある、WSGI およびフレームワーク固有のミドルウェアです。このエージェントは、他の Web フレームワークと完全な WSGI 互換を実現し、WSGI やそれらのフレームワークで構築されたアプリケーションに、IAST(Interactive Application Security Testing)および RASP(Runtime Application Self-Protection)機能を提供します。

Assess では、アプリケーションを通常どおり実行している間にエージェントが脆弱なデータフローパスやその他の問題を特定します。エージェントはこれらの検出結果を Contrast 内の組織に報告します。そのため、アプリケーションを実際の環境にデプロイする前に脆弱性に対処することができます。

Protect では、Python エージェントは HTTP リクエストを検査して、問題を引き起こす可能性のある入力ベクトルを特定します。リクエスト中に、エージェントはデータベースクエリやファイル書き込みのほか、リクエストに起因するその他の有害なアクションを検査します。リクエストの最後に、エージェントはレンダリングされた出力を検査して、攻撃が成功したかどうかを確認し、成功した攻撃がユーザに転送されないようにブロックすることができます。そのうえ、パフォーマンス向上など多くの利点が得られるよう、エージェントは全ての解析を内部でネイティブに処理します。



### 注記

Python エージェントは、Contrast Assess、Contrast Protect、Contrast SCA に対応しています。

次のステップ：

- [Python エージェントをインストール \(317ページ\)](#)する
- [Python エージェントのサポート対象テクノロジーを確認 \(317ページ\)](#)する

## Python エージェントのシステム要件



### 警告

現在、Python エージェントは、M1 チップを搭載した Mac での実行をサポートしていません。

Python エージェントをインストールする前に、以下のシステム要件を満たす必要があります。

- 検査対象のアプリケーションがデプロイされており、その Web アプリケーションのテクノロジーは Contrast のサポート対象であること。
- アプリケーションは再起動可能であること。
- Web サーバが Contrast とネットワークで接続されていること。
- Web サーバが PyPI とネットワークで接続されているか、エージェントが手動でインストールされていること。
- サーバが以下の表に示す最小要件を満たしていること。

要件	バージョン	備考
オペレーティングシステム	<ul style="list-style-type: none"> <li>64 ビット OS X</li> <li>64 ビット Linux</li> </ul>	<p>エージェントのバージョン 2.3.0 以降で、パッケージのインストール時に C 拡張のコンパイルが必要になります。この処理は自動的に行われますが、ターゲット環境に特定のソフトウェアがインストールされている必要があります。</p> <ul style="list-style-type: none"> <li>必須: gcc、make、automake、autoconf。パッケージ名はプラットフォームによって異なる場合があります。お使いのプラットフォームのバージョンの build-essential のインストールやシステムヘッダのインストールが必要な場合があります。Alpine でエージェントを実行する場合は、libtool が必要です。</li> </ul>
Python パッケージ	<ul style="list-style-type: none"> <li>protobuf: 3.12 以降</li> <li>psutil: 5.7 以降</li> <li>pip: 6 以降</li> </ul>	

## Python エージェントのサポート対象テクノロジー

このエージェントでは、以下のテクノロジーをサポートしています。

テクノロジー	サポート対象バージョン	備考
言語のバージョン	<ul style="list-style-type: none"> <li>3.11.x: 最初にサポート対象となったエージェントは 5.19.0</li> <li>3.10.x: 最初にサポート対象となったエージェントは 5.2.0</li> <li>3.9.x: 最初にサポート対象となったエージェントは 4.2.0</li> <li>3.8.x: 最初にサポート対象となったエージェントは 2.8.0</li> <li>3.7.x: 最初にサポート対象となったエージェントは 1.5.0</li> </ul>	<p>Contrast は、<b>バグフィックス</b>および <b>セキュリティステータス</b>の Python LTS(長期サポート)バージョンをサポートします。Python バージョンのサポートは、ワーキンググループが <b>LTS 期間</b>をシフトするのに合わせて行われます。</p> <p><b>サポート対象外:</b></p> <ul style="list-style-type: none"> <li>3.6.x、3.5x、2.7.x: 最後のサポート対象となったエージェントは 4.14.3</li> </ul>
アプリケーションフレームワーク	<ul style="list-style-type: none"> <li>Aiohttp: 3.7 以降</li> <li>Bottle: 0.11、0.12</li> <li>Django: 1.11、2.x、3.x、4.x</li> <li>Django Rest Framework: 3.12 以降</li> <li>Falcon (ASGI): 3.0、3.1</li> <li>Falcon (WSGI): 2.x、3.x</li> <li>FastAPI: 0.68* - 0.95*</li> <li>Flask: 1.x、2.x</li> <li>Pyramid: 1.10、2.x</li> <li>Quart: 0.15 以降</li> </ul>	<p>Python エージェントは WSGI 互換です。ガイドラインに従う限り、この他の WSGI アプリケーションと互換性がある場合があります。</p> <p>また、Python エージェントは FastAPI フレームワークのみ ASGI と互換性があります。</p> <p>* FastAPI および Starlette(FastAPI が依存している)は比較的新しいライブラリで、継続的な開発変更が行われているため、Contrast が対応できなくなる可能性があります。FastAPI は、<b>開発スピードが速い</b>とされています。Contrast は記載のバージョンまでサポートを続け、新しいサポート対象がリリースされたときはドキュメントを更新します。</p>
プロセッサのアーキテクチャ	エージェントのテストは x86_64 で実施	他のアーキテクチャで機能する可能性もありますが、正式にはサポートされていません。
Web サーバ	<ul style="list-style-type: none"> <li>Gunicorn 0.16.1 - 20.1.x</li> <li>uWSGI 2.0.14 - 2.0.x</li> <li>Uvicorn 0.14* - 0.17*</li> </ul>	
データベース	<ul style="list-style-type: none"> <li>Mongo (pymongo)</li> <li>MySQL (PyMySQL、mysql-connector)</li> <li>PostgreSQL (psycopg2)</li> <li>SQLite3 (sqlite3、pysqlite2)</li> </ul>	
オブジェクト関係マッピングデータベース (ORM)	<ul style="list-style-type: none"> <li>Flask-SQLAlchemy</li> <li>SQLAlchemy</li> </ul>	

## Python エージェントのインストール

Python エージェントは、Python の標準パッケージとしてインストールされます。

旧バージョン(バージョン 5.19.0 より前)の Python エージェントでは、検出結果を報告するために Contrast サービスを使用します。デフォルトでは、アプリケーションの起動時にサービスが自動的に開始します。エージェントは、個別に実行するスタンドアローンの **Contrast サービス (472ページ)**と通信するように設定することもできます。

バージョン 5.19.0 以降の Python エージェントでは、Contrast サービスを使用しません。

Python エージェントは、[PyPI を使用してインストール \(318ページ\)](#)するか、[Python エージェントのアップデート \(318ページ\)](#)を使用します。



### 警告

現在、Python エージェントは、M1 チップを搭載した Mac での実行をサポートしていません。

## PyPI を使用した Python エージェントのインストール

PyPI を使用して Python エージェントをインストールするには：

1. pip を使用してエージェントをインストールします。

```
pip install contrast-agent
```



### ヒント

requirements.txt ファイルがある場合は、このファイルに contrast-agent を追加し、`pip install -r requirements.txt` でインストールできます。

2. [ミドルウェアを設定します。 \(363ページ\)](#)
3. [エージェントを設定します。 \(319ページ\)](#)
4. エージェントを実行するシステムに autoconf がインストールされていることを確認します。
5. 通常どおりアプリケーションを起動して疎通します。
6. アプリケーションサーバが Contrast に認識され、アプリケーションの検査結果が Contrast に報告されていることを確認します。

## Python エージェントのアップデート

Contrast の Python エージェントを自動的に更新するのに信頼性が高く確実な方法は、Python の pip を使用して、利用可能な最新バージョンをダウンロードしてインストールすることです。pip は Python アプリケーションのすべての依存関係を管理するため、すでに利用可能でビルド環境の一部になっているはずで、Python エージェントを更新する頻度と更新の取得先は、組織の設定と Contrast の実装 (SaaS 版またはオンプレミス版)によって異なります。

主な手順：

1. Contrast の Python エージェントの入手元を決めます。
2. エージェントをインストールします。
3. スクリプトを使って自動アップデートを行います。

### 開始する前に

- Contrast エージェントの PyPI リポジトリへアクセスできること。
- Python アプリケーションが Contrast エージェントなしで想定どおりに機能すること。
- 事前に Contrast の Python エージェントが正常にインストールされていること。
- 変更管理ポリシーと使用する環境に基づいて、エージェントをアップデートする方法とタイミングを決めていること。

### 自動アップデートのスクリプトを使用

1. Contrast の Python エージェントの入手元を決めます。

- PyPI のパブリック(またはプライベート)リポジトリ
2. Contrast の Python エージェントを `requirements.txt` に依存関係として指定します。  
`requirements.txt` は、Python アプリケーションが PyPI(パブリックまたはプライベート)リポジトリからのアーティファクトでビルドされるたびに自動的に解決する依存関係を指定するファイルです。このファイルに Contrast の Python エージェントを指定することで、アプリケーションの新しいビルドを常に最新バージョンのエージェントに合わせることが簡単になります。Contrast エージェント(`contrast-agent`)のバージョンは指定しないで下さい。そうすれば最新のバージョンが取得されます。
  3. `requirements.txt` を更新した後、アプリケーションをビルドする際に次のコマンドを使用します。これにより、Contrast の Python エージェントが PyPI から自動的にダウンロードされ、Python アプリケーションに追加または更新されます。

```
$ pip install -U -r requirements.txt
```

## 手動でアップデート

組織によっては、`requirements.txt` ファイルを環境間で一貫させる必要がある場合や、すべての環境に Contrast の Python エージェントをインストールする予定がない場合があります。このような場合、手動でエージェントをインストールします。Python のビルドプロセスの一環として手動でエージェントを更新できます。

1. Contrast の Python エージェントの入手元を決めます。
  - PyPI のパブリック(またはプライベート)リポジトリ
2. 次のコマンドを使用して、Contrast の Python エージェントを手動で取得し、PyPI(パブリックまたはプライベート)から Python アプリケーションに追加または更新します。

```
$ pip install -U contrast-agent
```

## 関連項目

- [Python エージェントのサポート対象テクノロジー \(317ページ\)](#)
- [Python エージェントのインストール \(317ページ\)](#)

## Python エージェントの設定

全てのエージェントには[基本の設定 \(35ページ\)](#)があり、設定値には[優先順位 \(36ページ\)](#)があります。

また、[ミドルウェアを設定 \(363ページ\)](#)して、YAML 設定ファイルで Python エージェントを設定する必要があります。

## Contrast サービスの設定(5.19.0 より前のバージョンのみ)

旧バージョン(バージョン 5.19.0 より前)の場合、Python エージェントは起動時に実行ファイルを起動し、この実行ファイルにも設定ファイルへのアクセスが必要です。サービスは通常、Python エージェントのプロセスによって起動されるため、サービスはエージェントと同じ設定ファイルにアクセスすることができます。ただし、サービスが単独で起動された場合には、設定ファイルの[優先順位 \(36ページ\)](#)が同じになるよう試みます。

つまり、(通常の場合のように)サービスの作業ディレクトリがアプリケーションのベースディレクトリでもある場合、サービスはアプリケーションの設定ファイルを共有できるということです。エージェントとサービスの両方で、`/etc/contrast/contrast_security.yaml` パスを使用するということです。



### ヒント

[Contrast エージェント設定エディタ \(39ページ\)](#)を使用すると、YAML 設定ファイルの作成やアップロード、YAML の検証、推奨される設定値の表示などができます。

## Python エージェントの YAML テンプレート

YAML 設定ファイルを使用して Python エージェントを設定する場合には、以下のテンプレートをご利用ください(YAML 設定については、[こちらの説明 \(38ページ\)](#)を参照してください)。

YAML 設定ファイルは、デフォルトの場所に配置します : /etc/contrast/  
contrast\_security.yaml



### 注記

YAML 設定ファイルの agent.service セクションは、旧バージョンの Python エージェント(バージョン 5.19.0 より前)のみに適用されます。

```
# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==

# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
```



```

# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Certificate
# PEM file for communication with the Contrast UI.
# cert_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Key PEM
# file for communication with the Contrast UI.
# key_file: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid contrast.proxy.host
# and contrast.proxy.port will enable the proxy.
# enable: NEEDS_TO_BE_SET

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.

```

```
# \  
=====
```

```
==  
# agent:  
  
# \  
=====
```

```
# agent.logger  
# Define the following properties to set logging values.  
# If the following properties are not defined, the  
# agent uses the logging values from the Contrast UI.  
# \  
=====
```

```
# logger:  
  
# Enable diagnostic logging by setting a path to a log file.  
# While diagnostic logging hurts performance, it generates  
# useful information for debugging Contrast. The value set here  
# is the location to which the agent saves log output. If no  
# log file exists at this location, the agent creates a file.  
#  
# Example - `/opt/Contrast/contrast.log` creates a log in the  
# `/opt/Contrast` directory, and rotates it automatically as needed.  
#  
# path: ./contrast_agent.log  
  
# Set the the log output level. Valid options are  
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.  
# level: INFO  
  
# Override the name of the process the agents uses in logs.  
# progname: Contrast Agent  
  
# \  
=====
```

```
# agent.security_logger  
# Define the following properties to set security  
# logging values. If not defined, the agent uses the  
# security logging (CEF) values from the Contrast UI.  
# \  
=====
```

```
# security_logger:  
  
# Set the file to which the agent logs security events.  
# path: /.contrast/security.log  
  
# Set the log level for security logging. Valid options  
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.  
# level: ERROR  
  
# Change the Contrast security logger from a file-sized based rolling  
# scheme to a date-based rolling scheme. At midnight server time,  
# the log from the previous day is renamed to *file_name.yyyy-MM-dd*.  
# Note - this scheme does not have a size limit; manual log  
# pruning will be required. This flag must be set to use the
```

```
# backups and size flags. Value options are `true` or `false`.
# roll_daily: NEEDS_TO_BE_SET

# Specify the file size cap (in MB) of each log file.
# roll_size: NEEDS_TO_BE_SET

# Specify the number of backup logs that the agent will create before
# Contrast cleans up the oldest file. A value of `0` means that no \
backups
# are created, and the log is truncated when it reaches its size cap.
#
# Note - this property must be used with
# `agent.security_logger.roll_daily=false`; otherwise,
# Contrast continues to log daily and disregard this limit.
#
# backups: NEEDS_TO_BE_SET

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE
```

```
# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.python
# The following properties apply to any Python agent-wide configurations.
# \
=====
# python:

# Allow the agent to dump `cProfile` data to file for each request.
# enable_profiler: false

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Set to `false` to disable library analysis.
# analyze_libraries: true

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false
```

```

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Value options are `ALL`, `SOME`, or `NONE`.
# stacktraces: ALL

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====

```

```

==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
# protect.rules
# Use the following properties to set simple rule configurations.
# \
=====
# rules:

# Define a list of Protect rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
# protect.rules.bot-blocker
# Use the following selection to configure if the
# agent blocks bots. Set to `true` to enable blocking.
# \
=====
# bot-blocker:

# Set to `true` for the agent to block known bots.
# enable: false

# \
=====
# protect.rules.sql-injection
# Use the following settings to configure the sql-injection rule.
# \
=====
# sql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Tell the agent to detect when semantic analysis of the query
# reveals tautologies used in exfiltration attacks (e.g., "or
# 1=1" or "or 2<>3"). The agent blocks if blocking is enabled.
# detect_tautologies: true

# Tell the agent to detect when semantic analysis of the query
# reveals the invocation of dangerous functions typically used in

```

```
# weaponized exploits. The agent blocks if blocking is enabled.
# detect_dangerous_functions: true

# Tell the agent to detect when semantic analysis of the query
# reveals chained queries, which is uncommon in normal usage but
# common in exploit. The agent blocks if blocking is enabled.
# detect_chained_queries: true

# Tell the agent to detect when semantic analysis of the query
# reveals database queries are being made for system tables and
# sensitive information. The agent blocks if blocking is enabled.
# detect_suspicious_unions: true

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Detect when custom code attempts to access sensitive
# system files. The agent blocks if blocking is enabled.
# detect_custom_code_accessing_system_files: true

# Detect when users attempt to bypass filters by
# using ":::DATA" channels or null bytes in file
# names. The agent blocks if blocking is enabled.
# detect_common_file_exploits: true
```

```
# \  
=====  
# protect.rules.method-tampering  
# Use the following properties to configure  
# how the method tampering rule works.  
# \  
=====  
# method-tampering:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====  
# protect.rules.reflected-xss  
# Use the following properties to configure how  
# the reflected cross-site scripting rule works.  
# \  
=====  
# reflected-xss:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====  
# protect.rules.xxe  
# Use the following properties to configure  
# how the XML external entity works.  
# \  
=====  
# xxe:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====  
==
```



```
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
```

```

# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==
# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
# api

```

```
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Certificate
# PEM file for communication with the Contrast UI.
# cert_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Key PEM
# file for communication with the Contrast UI.
# key_file: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
```

```

# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid contrast.proxy.host
# and contrast.proxy.port will enable the proxy.
# enable: NEEDS_TO_BE_SET

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
#
# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
#
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Override the name of the process the agents uses in logs.
# progname: Contrast Agent

# \

```

```
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# Change the Contrast security logger from a file-sized based rolling
# scheme to a date-based rolling scheme. At midnight server time,
# the log from the previous day is renamed to *file_name.yyyy-MM-dd*.
# Note - this scheme does not have a size limit; manual log
# pruning will be required. This flag must be set to use the
# backups and size flags. Value options are `true` or `false`.
# roll_daily: NEEDS_TO_BE_SET

# Specify the file size cap (in MB) of each log file.
# roll_size: NEEDS_TO_BE_SET

# Specify the number of backup logs that the agent will create before
# Contrast cleans up the oldest file. A value of `0` means that no \
backups
# are created, and the log is truncated when it reaches its size cap.
#
# Note - this property must be used with
# `agent.security_logger.roll_daily=false`; otherwise,
# Contrast continues to log daily and disregard this limit.
#
# backups: NEEDS_TO_BE_SET

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET
```

```
# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.python
# The following properties apply to any Python agent-wide configurations.
# \
=====
# python:

# Allow the agent to dump `cProfile` data to file for each request.
# enable_profiler: false

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Set to `false` to disable library analysis.
# analyze_libraries: true
```

```
# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Value options are `ALL`, `SOME`, or `NONE`.
# stacktraces: ALL

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
```

```

# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
# protect.rules
# Use the following properties to set simple rule configurations.
# \
=====
# rules:

# Define a list of Protect rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
# protect.rules.bot-blocker
# Use the following selection to configure if the
# agent blocks bots. Set to `true` to enable blocking.
# \
=====
# bot-blocker:

# Set to `true` for the agent to block known bots.
# enable: false

# \
=====

```



```
# protect.rules.sql-injection
# Use the following settings to configure the sql-injection rule.
# \
=====
# sql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Tell the agent to detect when semantic analysis of the query
# reveals tautologies used in exfiltration attacks (e.g., "or
# 1=1" or "or 2<>3"). The agent blocks if blocking is enabled.
# detect_tautologies: true

# Tell the agent to detect when semantic analysis of the query
# reveals the invocation of dangerous functions typically used in
# weaponized exploits. The agent blocks if blocking is enabled.
# detect_dangerous_functions: true

# Tell the agent to detect when semantic analysis of the query
# reveals chained queries, which is uncommon in normal usage but
# common in exploit. The agent blocks if blocking is enabled.
# detect_chained_queries: true

# Tell the agent to detect when semantic analysis of the query
# reveals database queries are being made for system tables and
# sensitive information. The agent blocks if blocking is enabled.
# detect_suspicious_unions: true

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
```

```
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Detect when custom code attempts to access sensitive
# system files. The agent blocks if blocking is enabled.
# detect_custom_code_accessing_system_files: true

# Detect when users attempt to bypass filters by
# using "::$DATA" channels or null bytes in file
# names. The agent blocks if blocking is enabled.
# detect_common_file_exploits: true

# \
=====
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# \  
=====  
# protect.rules.xxe  
# Use the following properties to configure  
# how the XML external entity works.  
# \  
=====  
# xxe:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====  
==  
# application  
# Use the properties in this section for  
# the application(s) hosting this agent.  
# \  
=====  
==  
# application:  
  
# Override the reported application name.  
#  
# Note - On Java systems where multiple, distinct applications may be  
# served by a single process, this configuration causes the agent to \  
report  
# all discovered applications as one application with the given name.  
#  
# name: NEEDS_TO_BE_SET  
  
# Override the reported application path.  
# path: NEEDS_TO_BE_SET  
  
# Add the name of the application group with which this  
# application should be associated in the Contrast UI.  
# group: NEEDS_TO_BE_SET  
  
# Add the application code this application should use in the Contrast UI.  
# code: NEEDS_TO_BE_SET  
  
# Override the reported application version.  
# version: NEEDS_TO_BE_SET  
  
# Apply labels to an application. Labels must  
# be formatted as a comma-delimited list.  
# Example - `label1,label2,label3`  
#
```

```
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
```

```
# tags: NEEDS_TO_BE_SET
```

## Python エージェントの YAML テンプレート

YAML 設定ファイルを使用して Python エージェントを設定する場合には、以下のテンプレートをご利用ください(YAML 設定については、[こちらの説明 \(38ページ\)](#)を参照してください)。

YAML 設定ファイルは、デフォルトの場所に配置します : /etc/contrast/  
contrast\_security.yaml



### 注記

YAML 設定ファイルの `agent.service` セクションは、旧バージョンの Python エージェント(バージョン 5.19.0 より前)のみに適用されます。

```
# \  
=====\  
==\  
# Use the properties in this YAML file to configure a Contrast agent.  
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html  
# to determine the order of precedence for configuration values.  
# \  
=====\  
==\  
  
# Use this setting if you want to temporarily disable a Contrast agent.  
# Set to `true` to enable the agent; set to `false` to disable the agent.  
# enable: true  
  
# \  
=====\  
==\  
# api  
# Use the properties in this section to connect the agent to the Contrast \  
# UI.  
# \  
=====\  
==\  
api:  
  
# ***** REQUIRED *****  
# Set the URL for the Contrast UI.  
url: https://app.contrastsecurity.com/Contrast  
  
# ***** REQUIRED *****  
# Set the API key needed to communicate with the Contrast UI.  
api_key: NEEDS_TO_BE_SET  
  
# ***** REQUIRED *****  
# Set the service key needed to communicate with the Contrast  
# UI. It is used to calculate the Authorization header.
```

```

service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Certificate
# PEM file for communication with the Contrast UI.
# cert_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Key PEM
# file for communication with the Contrast UI.
# key_file: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid contrast.proxy.host
# and contrast.proxy.port will enable the proxy.
# enable: NEEDS_TO_BE_SET

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# \
=====
==

```

```
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
#
# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
#
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Override the name of the process the agents uses in logs.
# progname: Contrast Agent

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# Change the Contrast security logger from a file-sized based rolling
# scheme to a date-based rolling scheme. At midnight server time,
```

```
# the log from the previous day is renamed to *file_name.yyyy-MM-dd*.
# Note - this scheme does not have a size limit; manual log
# pruning will be required. This flag must be set to use the
# backups and size flags. Value options are `true` or `false`.
# roll_daily: NEEDS_TO_BE_SET

# Specify the file size cap (in MB) of each log file.
# roll_size: NEEDS_TO_BE_SET

# Specify the number of backup logs that the agent will create before
# Contrast cleans up the oldest file. A value of `0` means that no \
backups
# are created, and the log is truncated when it reaches its size cap.
#
# Note - this property must be used with
# `agent.security_logger.roll_daily=false`; otherwise,
# Contrast continues to log daily and disregard this limit.
#
# backups: NEEDS_TO_BE_SET

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
```



```
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.python
# The following properties apply to any Python agent-wide configurations.
# \
=====
# python:

# Allow the agent to dump `cProfile` data to file for each request.
# enable_profiler: false

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Set to `false` to disable library analysis.
# analyze_libraries: true

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
```

```
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Value options are `ALL`, `SOME`, or `NONE`.
# stacktraces: ALL

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# protect
```

```
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
# protect.rules
# Use the following properties to set simple rule configurations.
# \
=====
# rules:

# Define a list of Protect rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
# protect.rules.bot-blocker
# Use the following selection to configure if the
# agent blocks bots. Set to `true` to enable blocking.
# \
=====
# bot-blocker:

# Set to `true` for the agent to block known bots.
# enable: false

# \
=====
# protect.rules.sql-injection
# Use the following settings to configure the sql-injection rule.
# \
=====
# sql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Tell the agent to detect when semantic analysis of the query
# reveals tautologies used in exfiltration attacks (e.g., "or
# 1=1" or "or 2<>3"). The agent blocks if blocking is enabled.
# detect_tautologies: true
```

```
# Tell the agent to detect when semantic analysis of the query
# reveals the invocation of dangerous functions typically used in
# weaponized exploits. The agent blocks if blocking is enabled.
# detect_dangerous_functions: true

# Tell the agent to detect when semantic analysis of the query
# reveals chained queries, which is uncommon in normal usage but
# common in exploit. The agent blocks if blocking is enabled.
# detect_chained_queries: true

# Tell the agent to detect when semantic analysis of the query
# reveals database queries are being made for system tables and
# sensitive information. The agent blocks if blocking is enabled.
# detect_suspicious_unions: true

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Detect when custom code attempts to access sensitive
# system files. The agent blocks if blocking is enabled.
# detect_custom_code_accessing_system_files: true

# Detect when users attempt to bypass filters by
```

```
# using ":::$DATA" channels or null bytes in file
# names. The agent blocks if blocking is enabled.
# detect_common_file_exploits: true

# \
=====
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# \  
=====\  
==  
# application  
# Use the properties in this section for  
# the application(s) hosting this agent.  
# \  
=====\  
==  
# application:  
  
# Override the reported application name.  
#  
# Note - On Java systems where multiple, distinct applications may be  
# served by a single process, this configuration causes the agent to \  
report  
# all discovered applications as one application with the given name.  
#  
# name: NEEDS_TO_BE_SET  
  
# Override the reported application path.  
# path: NEEDS_TO_BE_SET  
  
# Add the name of the application group with which this  
# application should be associated in the Contrast UI.  
# group: NEEDS_TO_BE_SET  
  
# Add the application code this application should use in the Contrast UI.  
# code: NEEDS_TO_BE_SET  
  
# Override the reported application version.  
# version: NEEDS_TO_BE_SET  
  
# Apply labels to an application. Labels must  
# be formatted as a comma-delimited list.  
# Example - `label1,label2,label3`  
#  
# tags: NEEDS_TO_BE_SET  
  
# Define a set of `key=value` pairs (which conforms to RFC 2253) for  
# specifying user-defined metadata associated with the application. The  
# set must be formatted as a comma-delimited list of `key=value` pairs.  
# Example - `business-unit=accounting, office=Baltimore`  
#  
# metadata: NEEDS_TO_BE_SET  
  
# Provide the ID of a session which already exists in the Contrast  
# UI. Vulnerabilities discovered by the agent are associated with  
# this session. If an invalid ID is supplied, the agent will be  
# disabled. This option and `application.session_metadata` are  
# mutually exclusive; if both are set, the agent will be disabled.  
# session_id: NEEDS_TO_BE_SET  
  
# Provide metadata which is used to create a new session ID in the  
# Contrast UI. Vulnerabilities discovered by the agent are associated with
```

```
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==
# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
```

```

=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Certificate
# PEM file for communication with the Contrast UI.
# cert_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Key PEM
# file for communication with the Contrast UI.
# key_file: NEEDS_TO_BE_SET

# \
=====

```



```
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid **contrast.proxy.host**
# and **contrast.proxy.port** will enable the proxy.
# enable: NEEDS_TO_BE_SET

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
#
# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
#
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Override the name of the process the agents uses in logs.
```

```

# progname: Contrast Agent

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# Change the Contrast security logger from a file-sized based rolling
# scheme to a date-based rolling scheme. At midnight server time,
# the log from the previous day is renamed to *file_name.yyyy-MM-dd*.
# Note - this scheme does not have a size limit; manual log
# pruning will be required. This flag must be set to use the
# backups and size flags. Value options are `true` or `false`.
# roll_daily: NEEDS_TO_BE_SET

# Specify the file size cap (in MB) of each log file.
# roll_size: NEEDS_TO_BE_SET

# Specify the number of backup logs that the agent will create before
# Contrast cleans up the oldest file. A value of `0` means that no \
backups
# are created, and the log is truncated when it reaches its size cap.
#
# Note - this property must be used with
# `agent.security_logger.roll_daily=false`; otherwise,
# Contrast continues to log daily and disregard this limit.
#
# backups: NEEDS_TO_BE_SET

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

```

```

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.python
# The following properties apply to any Python agent-wide configurations.
# \
=====
# python:

# Allow the agent to dump `cProfile` data to file for each request.
# enable_profiler: false

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

```

```
# Set to `false` to disable library analysis.
# analyze_libraries: true

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Value options are `ALL`, `SOME`, or `NONE`.
# stacktraces: ALL

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000
```

```
# \  
=====\  
# assess.rules  
# Use the following properties to control simple rule configurations.  
# \  
=====\  
# rules:  
  
# Define a list of Assess rules to disable in the agent.  
# The rules must be formatted as a comma-delimited list.  
#  
# Example - Set `reflected-xss,sql-injection` to disable  
# the reflected-xss rule and the sql-injection rule.  
#  
# disabled_rules: NEEDS_TO_BE_SET  
  
# \  
=====\  
==  
# protect  
# Use the properties in this section to override Protect features.  
# \  
=====\  
==  
# protect:  
  
# Use the properties in this section to determine if the  
# Protect feature should be enabled. If this property is not  
# present, the decision is delegated to the Contrast UI.  
# enable: false  
  
# \  
=====\  
# protect.rules  
# Use the following properties to set simple rule configurations.  
# \  
=====\  
# rules:  
  
# Define a list of Protect rules to disable in the agent.  
# The rules must be formatted as a comma-delimited list.  
# disabled_rules: NEEDS_TO_BE_SET  
  
# \  
=====\  
# protect.rules.bot-blocker  
# Use the following selection to configure if the  
# agent blocks bots. Set to `true` to enable blocking.  
# \  
=====\  
# bot-blocker:  
  
# Set to `true` for the agent to block known bots.  
# enable: false
```

```
# \  
=====\  
# protect.rules.sql-injection  
# Use the following settings to configure the sql-injection rule.  
# \  
=====\  
# sql-injection:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or off.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# Tell the agent to detect when semantic analysis of the query  
# reveals tautologies used in exfiltration attacks (e.g., "or  
# 1=1" or "or 2<>3"). The agent blocks if blocking is enabled.  
# detect_tautologies: true  
  
# Tell the agent to detect when semantic analysis of the query  
# reveals the invocation of dangerous functions typically used in  
# weaponized exploits. The agent blocks if blocking is enabled.  
# detect_dangerous_functions: true  
  
# Tell the agent to detect when semantic analysis of the query  
# reveals chained queries, which is uncommon in normal usage but  
# common in exploit. The agent blocks if blocking is enabled.  
# detect_chained_queries: true  
  
# Tell the agent to detect when semantic analysis of the query  
# reveals database queries are being made for system tables and  
# sensitive information. The agent blocks if blocking is enabled.  
# detect_suspicious_unions: true  
  
# \  
=====\  
# protect.rules.cmd-injection  
# Use the following properties to configure  
# how the command injection rule works.  
# \  
=====\  
# cmd-injection:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====
```

```
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Detect when custom code attempts to access sensitive
# system files. The agent blocks if blocking is enabled.
# detect_custom_code_accessing_system_files: true

# Detect when users attempt to bypass filters by
# using "::$DATA" channels or null bytes in file
# names. The agent blocks if blocking is enabled.
# detect_common_file_exploits: true

# \
=====
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
```

```
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
```



```

# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels

```

```
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET
```

## Python エージェントの設定の検証

Python エージェントには、エージェントの設定を検証し、テストするためのスクリプトが含まれていません。

### スクリプトを実行する手順

1. `pip` を使用して、`contrast-agent` のバージョン 5.1.0 以降をインストールします。
2. [YAML ファイル \(320ページ\)](#)や[環境変数 \(56ページ\)](#)、またはその両方を使用して、Contrast エージェントの設定を準備します。
3. `contrast-validate-config` というコマンドを実行します。このスクリプトは、現在の設定を検証し、Contrast と通信できるかをテストします。



### 注記

**Response: 400 Bad Request** のメッセージが表示されても、Contrast への接続は成功しています。

以下の例の場合、Contrast Web インターフェイスにまだアプリケーションのサーバが作成されていないことを示しています。

```
[contrast-validate-config] Sending test request to Contrast UI
[contrast-validate-config] Response: 400 Bad Request
[contrast-validate-config] {
  "success" : false,
  "messages" : [ "Invalid agent request" ]
}
[contrast-validate-config] 400 status code indicates success \
for this endpoint
[contrast-validate-config] Connection to the Contrast UI \
successful
```

そして、以下の例では、既に Contrast Web インターフェイスにはサーバが作成されていることを示しています。

```
[contrast-validate-config] Sending test request to Contrast UI
[contrast-validate-config] Response: 304 Not Modified
[contrast-validate-config] 304 status code indicates success \
for this endpoint
[contrast-validate-config] Connection to the Contrast UI \
successful
```

### 関連項目

- [Python エージェントの設定 \(319ページ\)](#)

## ミドルウェアの設定

ミドルウェアは、Web アプリケーションの一部を構成するソフトウェアコンポーネントであり、リクエストを受け取って必要な処理を行いレスポンスを返すことができます。

Python エージェントは、Contrast がサポートする全てのフレームワークのミドルウェアとして実装されます。Python エージェントを使用するには、アプリケーションで使用しているフレームワークのミドルウェアを設定する必要があります。

### AIOHTTP

AIOHTTP ミドルウェア は、aiohttp の `web.Application` コンストラクタに引数として渡されるクラススペースのミドルウェア です。次の例は、Contrast ミドルウェアクラスを使用する AIOHTTP アプリケーションの例です。

```
from aiohttp import web
from contrast.aiohttp import ContrastMiddleware

routes = web.RouteTableDef()

@routes.get("/")
def index(request):
    raise web.HTTPFound("/hello")

middlewares = [ContrastMiddleware(app_name="app name")]
app = web.Application(middlewares=middlewares)
app.add_routes(routes)

web.run_app(app)
```

### Bottle

Contrast の Bottle ミドルウェアは、Bottle アプリケーションのインスタンスをラッピングすることによって動作する WSGI ミドルウェアです。

Bottle で Python エージェントを設定するには：

1. アプリケーションのコードベースで、Bottle アプリケーションのオブジェクトを検索します。これは、`bottle.Bottle` のインスタンスになります。以下はサンプルの Bottle アプリケーションで、`app` はお使いの Bottle アプリケーションのオブジェクトになります。

```
from bottle import Bottle, run

app = Bottle(__name__)

@app.route("/")
def index():
    return "hello world"

<InstallContrastHere>

run(app)
```

2. Bottle アプリケーションのオブジェクトを Contrast のミドルウェアでラップします。上記の例では、`<InstallContrastHere>` を次のように置き換えます。

```
from contrast.bottle import ContrastMiddleware
app = ContrastMiddleware(app)
```



### 重要

まれに、WSGI アプリケーションオブジェクトに加えて、元の `bottle.Bottle` アプリケーションインスタンスを `ContrastMiddleware` に直接渡すことが必要になる場合があります。アプリケーションが起動しない場合は、元の `Bottle` アプリケーションを検索し、Contrast のミドルウェアに渡します。例えば、以下のようになります。

```
app = ContrastMiddleware(  
    app,  
    original_bottle_app, # instance of bottle.Bottle  
)
```

## Django

**新設定手順：Contrast Python エージェントのバージョン 4.6.0 以降はこの手順を利用します**

Contrast の Django ミドルウェアは WSGI ミドルウェアであり、Django スタイルのミドルウェアではありません。

1. WSGI アプリケーションのオブジェクトを検索します。WSGI\_APPLICATION という Django の設定オプションでプロジェクトの WSGI アプリを指定しますが、通常これは `wsgi.py` にあります。WSGI\_APPLICATION をまだ設定していない場合は、設定する必要があります。以下はサンプルの `wsgi.py` で、`application` はお使いの WSGI アプリケーションのオブジェクトになります。

```
from django.core.wsgi import get_wsgi_application  
application = get_wsgi_application()
```

<InstallContrastHere>

2. WSGI アプリケーションのオブジェクトを Contrast のミドルウェアでラップします。上記の例では、<InstallContrastHere>を次のように置き換えます。

```
from contrast.django import ContrastMiddleware  
application = ContrastMiddleware(application)
```

**旧設定手順：Contrast Python エージェントのバージョン 5.0.0 以降でこの手順は利用できません**

Django ミドルウェアの設定は、`settings.py` ファイルで行います。

1. `settings.py` ファイルを検索してください。このファイルは、すべてのアプリケーションで同じ場所にあるわけではありませんが、通常はアプリケーションソースツリーの最上部などにあります。一般的な場所は次のとおりです。
  - `/settings.py`
  - `config/settings.py`
  - `app/settings.py`



### 注記

ソースツリーで `settings.py` を検索する場合は、Python の仮想環境に該当するディレクトリは必ず除外してください。

アプリケーションによって、複数の `settings.py` ファイルが存在し、さまざまなアプリケーション構成(例えば、本番環境やテスト環境など)に対応している場合があります。そのような場合には、Contrast エージェントのミドルウェアを使用する全ての設定に追加してください。

## 2. Contrast エージェントモジュールをリストに追加してください。

Contrast ミドルウェアを可能な限りリストの最初の方に追加してください。ただし、状況によって、アプリケーションを動作させるために順序の変更が必要になる場合があります。

- **Django 1.10 以降** : 配列になっている `MIDDLEWARE` という設定変数を検索します。リストに Contrast エージェントモジュールを追加します。

```
MIDDLEWARE = [  
    'contrast.agent.middlewares.django_middleware.DjangoMiddleware',  
    # OTHER MIDDLEWARE,  
]
```

- **Django 1.6 から 1.9** : `settings.py` で `MIDDLEWARE_CLASSES` という設定変数を検索し、リストに Contrast エージェントモジュールを追加します。

```
MIDDLEWARE_CLASSES = [  
    \  
    'contrast.agent.middlewares.legacy_django_middleware.DjangoMiddleware'  
    ,  
    # OTHER MIDDLEWARE  
]
```

ミドルウェアの組み込みの詳細については、[Django のドキュメント](#)を参照してください。

## Falcon(ASGI)

Falcon(ASGI)ミドルウェアは、Falcon(ASGI)アプリケーションのインスタンスをラッピングすることによって動作する ASGI ミドルウェアです。

以下の例は、Falcon(ASGI)アプリケーションを Contrast ミドルウェアのクラスでラップするサンプルです。



### 注記

Falcon(ASGI)アプリケーションで Contrast 以外のミドルウェアを使用している場合、特定の機能を動作させるために、Contrast を最初の中ドキュメントとして初期化する必要があります。

```
import falcon.asgi  
from contrast.falcon_asgi import ContrastMiddleware  
  
class Home(object):  
    async def on_get(self, req, resp):  
        resp.status = falcon.HTTP_200  
        resp.body = "Hello World"  
  
def create():  
    # This is where the example app is declared. Look for something \  
similar in your  
    # application since this instance needs to be wrapped by Contrast \  
middleware  
    _app = falcon.asgi.App()  
  
    # Add routes to your app  
    home = Home()
```

```
_app.add_route("/home", home)

# This line wraps the application instance with the Contrast middleware
# NOTE: Contrast should be the first middleware if others are used
_app = ContrastMiddleware(_app)
return _app
```

```
app = create()
```

## Falcon(WSGI)

Contrast の Falcon ミドルウェアは WSGI ミドルウェアであり、Falcon スタイルのミドルウェアではありません。

1. Falcon アプリケーションのオブジェクトを検索します。これは、Falcon のバージョンによって、`falcon.API` または `falcon.App` のインスタンスとなります。  
以下はサンプルの Falcon アプリケーションで、`app` はお使いの Falcon アプリケーションのオブジェクトになります。

```
import falcon
from views import Home

app = falcon.API()

home = Home()
app.add_route('/home', home)
```

<InstallContrastHere>

2. Falcon アプリケーションのオブジェクトを Contrast のミドルウェアでラップします。上記の例では、<InstallContrastHere>を次のように置き換えます。

```
from contrast.falcon import ContrastMiddleware
app = ContrastMiddleware(app)
```



### 重要

まれに、WSGI アプリケーションオブジェクトに加えて、元の `falcon.App` や `falcon.API` アプリケーションインスタンスを `ContrastMiddleware` に直接渡すことが必要になる場合があります。アプリケーションが起動しない場合は、元の Falcon アプリケーションを検索し、Contrast のミドルウェアに渡します。例えば、以下のようになります。

```
app = ContrastMiddleware(
    app,
    original_falcon_app, # instance of falcon.App or \
    falcon.API
)
```



### 重要

ルート登録が完了後、Falcon インスタンスをラップする必要があります。

## FastAPI

FastAPI ミドルウェアは、`starlette.middleware.BaseHTTPMiddleware` に依存する、クラスベースの ASGI ミドルウェアです。Contrast がサポートする FastAPI のバージョンについては、[Python 工](#)

エージェントのサポート対象テクノロジー (317ページ)を確認してください。次の例は、Contrast ミドルウェアクラスを使用した FastAPI アプリケーションのサンプルです。

```
from fastapi import FastAPI
from contrast.fastapi import ContrastMiddleware

app = FastAPI()
app.add_middleware(ContrastMiddleware, original_app=app)

@app.get("/")
def read_root():
    return RedirectResponse("/home")
```

FastAPI アプリケーションで Contrast 以外のミドルウェアを使用している場合、特定の機能を動作させるために、Contrast を最初のミドルウェアとして初期化する必要があります。

```
from fastapi import FastAPI
from fastapi.middleware.httpsredirect import HTTPSRedirectMiddleware
from contrast.fastapi import ContrastMiddleware

app = FastAPI()

# ContrastMiddleware must be the first middleware
app.add_middleware(ContrastMiddleware, original_app=app)
app.add_middleware(HTTPSRedirectMiddleware)
```

一部の機能で、FastAPI の `app` を `original_app` キーワードの引数として渡す必要があるため、現時点では `add_middleware` メソッドでミドルウェアを追加する方法のみがサポートされます。ミドルウェアを直接 FastAPI クラスの初期化に渡すことでミドルウェアを初期化する方法は、Contrast では現在サポートされていません。

```
# Not currently supported.
app = FastAPI(middleware=[...])
```



### 警告

`add_middleware` を複数回呼ぶと、前のミドルウェアが全て再初期化されます。

## Flask

Contrast の Flask は、Flask アプリケーションのインスタンスをラッピングすることによって動作する WSGI ミドルウェアです。

1. Flask アプリケーションのオブジェクトを検索します。これは、`flask.Flask` のインスタンスになります。  
以下はサンプルの Flask アプリケーションで、`app` はお使いの Flask アプリケーションのオブジェクトになります。

```
import Flask

app = Flask(__name__)

<InstallContrastHere>
```

```
@app.route('/')
def index():
    return render_template('index.html')

app.run(...)
```

2. Flask アプリケーションのオブジェクトを Contrast のミドルウェアでラップします。上記の例では、<InstallContrastHere>を次のように置き換えます。

```
from contrast.flask import ContrastMiddleware
app.wsgi_app = ContrastMiddleware(app)
```



### 注記

Contrast の Flask ミドルウェアは `flask.Flask.wsgi_app` ではなく、`flask.Flask` のインスタンスを引数として必要とします。

## Pyramid

**旧設定手順：Contrast Python エージェントのバージョン 5.0.0 以降でこの手順は利用できません**

Pyramid では、ミドルウェアは「tween」と呼ばれています。

1. アプリケーションのコードベースで、Configurator オブジェクトを検索します。例えば、次のようなものです。

```
from pyramid.config import Configurator
config = Configurator()
```

<InstallContrastHere>

2. Contrast のミドルウェアを設定に追加します。上記の例では、<InstallContrastHere>を次のように置き換えます。

```
config.add_tween('contrast.agent.middlewares.pyramid_middleware.PyramidMiddleware')
```

tween の設定に関する詳細については、[Pyramid のドキュメント](#)を参照してください。

**新設定手順：Contrast Python エージェントのバージョン 4.6.0 以降ではこの手順を利用します**

Contrast の Pyramid ミドルウェアは WSGI ミドルウェアであり、Pyramid スタイルの「tween」ではありません。

1. WSGI アプリケーションのオブジェクトを検索します。これは、多くの場合 `Configurator.make_wsgi_app()` への呼び出しによって作成されます。例えば、以下のようになります。

```
from pyramid.config import Configurator

config = Configurator()
app = config.make_wsgi_app()
```

<InstallContrastHere>

2. WSGI アプリケーションのオブジェクトを Contrast のミドルウェアでラップします。上記の例では、<InstallContrastHere>を次のように置き換えます。

```
from contrast.pyramid import ContrastMiddleware
app = ContrastMiddleware(app)
```





### 重要

まれに、アプリケーションのレジストリ(Registry)オブジェクトもミドルウェアに渡す必要がある場合があります。レジストリは通常、Configurator インスタンスと Pyramid アプリケーションオブジェクトの両方の属性として利用できます。

アプリケーションが起動しない場合は、アプリケーションのレジストリを検索し、Contrast のミドルウェアに渡します。以下は、その例です。

```
app = ContrastMiddleware(app, config.registry)
```

## Quart

Quart ミドルウェアは、Quart アプリケーションオブジェクトをラップして `asgi_app` 属性に割り当てる必要があります。以下の例は、Contrast ミドルウェアクラスを使用する Quart アプリケーションのサンプルです。

```
from quart import Quart, redirect
from contrast.quart import ContrastMiddleware

app = Quart(__name__)
app.asgi_app = ContrastMiddleware(app)

@app.route("/")
async def index():
    return redirect("/home")
```

## WSGI

Contrast は、エージェントのコア機能を全て含む汎用の WSGI ミドルウェアを提供しています。ルート探索などのフレームワーク固有の機能は、汎用の WSGI ミドルウェアには実装されていません。

Contrast を使用して WSGI 準拠のアプリケーションを検査するには：

1. アプリケーションのコードベースで、WSGI アプリケーションのオブジェクトを検索します。例えば、次のように作成された WSGI アプリケーションがあるとします。

```
from example.module import make_app
wsgi_app = make_app()

<InstallContrastHere>
```

2. WSGI アプリケーションのオブジェクトを Contrast のミドルウェアでラップします。上記の例では、`<InstallContrastHere>` を次のように置き換えます。

```
from contrast.wsgi import ContrastMiddleware
wsgi_app = ContrastMiddleware(wsgi_app)
```

WSGI ミドルウェアの詳細については、[WSGI の仕様](#)を参照してください。

## Python Web サーバ

Python エージェントは、いくつかの一般的な Web サーバで検証済みです。一部のサーバでは、Contrast を適切に動作させるために特定の設定オプションが必要です。

### Gunicorn

Gunicorn は、Django、Pyramid、Tornado などの一般的なフレームワークと一緒に組み合わせて使うことができます。

Gunicorn を起動するには次のコマンドを使用します：`gunicorn app.wsgi_app:application`  
(`app` はアプリケーションフォルダ名)

Gunicorn サーバで次のような設定ができます。

- **バインド：**

```
-b ADDRESS1
gunicorn -b 127.0.0.1:8000
```

- **タイムアウト：**

```
-t INT --timeout INT
```

この秒数以上反応がないワーカーは、強制終了されて、再起動されます。

値は、正の数か 0 になります。0 を設定すると、全てのワーカーのタイムアウトが完全に無効になり、タイムアウトは無限になります。

デフォルトは 30 秒です。同期処理のワーカー(Sync ワーカー)への影響が確実な場合にのみ、この値を大きくします。非同期処理のワーカーの場合には、ワーカープロセスは通信中となるため、1 つのリクエストを処理するために必要な時間の長さが影響することはありません。

## Uvicorn

Uvicorn は非同期の Web サーバで、`pip install uvicorn[standard]` でインストールすることができます。

以下は、推奨される設定です。

- `--loop=uvloop`
- `--http=httptools`  
`uvloop` と `httptools` はどちらも Cython で書かれており、パフォーマンスが向上しますが、Windows や PyPy との互換性がありません。
- `--interface`  
いくつかの ASGI プロトコルに対してこのオプションを設定できます。WSGI を使用していて、`--ws=websockets` を使用している場合、`websockets` は使用されず、デフォルトの `auto` になります。
- `--ws`  
`--ws-max-size`、`--ws-ping-interval`、`--ws-ping-timeout` を設定しており、`--ws` が `websockets` で設定されていない場合、全て無視されます。
- Uvicorn のマネージャとして `gunicorn` を使用する場合は、以下を実行します。

```
gunicorn -k uvicorn.workers.UvicornWorker
```
- **UvicornWorker のデプロイ** では、`uvloop` と `httptools` を使用します。PyPy で実行する場合には、代わりに `pure-Python` の実装を使用する必要があります。これを行うには、

```
UvicornH11Worker class.gunicorn -k uvicorn.workers.UvicornH11Worker
```

 を使用します。

## uWSGI の設定

uWSGI で Contrast を実行する場合は、次の設定オプションが必要です。コマンドラインまたは uWSGI 設定(.ini)ファイルで指定します。

- `--enable-threads`：スレッドの使用を有効にします。エージェントがバックグラウンドスレッドを開始できるように、このオプションを有効にする必要があります。
- `--single-interpreter`：初期化された Python プロセスで、Python エージェントが有効になるようにします。このオプションを指定すると、アプリケーションのリクエストを処理するプロセスと同じプロセスで Contrast が初期化されます。
- `--master` を指定する場合は、`--lazy-apps` も指定します。マスターモードで実行すると、uWSGI はマスタープロセスでアプリケーションを初期化しますが、リクエストを処理するワーカーにこのプロセスがフォークされます。正しく動作させるためには、各ワーカープロセスで個々に Contrast を初期化する必要がありますが、`--lazy-apps` で実現できます。

## Python エージェントの YAML テンプレート

YAML 設定ファイルを使用して Python エージェントを設定する場合には、以下のテンプレートをご利用ください(YAML 設定については、[こちらの説明 \(38ページ\)](#)を参照してください)。

YAML 設定ファイルは、デフォルトの場所に配置します : /etc/contrast/  
contrast\_security.yaml



### 注記

YAML 設定ファイルの agent.service セクションは、旧バージョンの Python エージェント(バージョン 5.19.0 より前)のみに適用されます。

```
# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==

# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
```

```

# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Certificate
# PEM file for communication with the Contrast UI.
# cert_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Key PEM
# file for communication with the Contrast UI.
# key_file: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid contrast.proxy.host
# and contrast.proxy.port will enable the proxy.
# enable: NEEDS_TO_BE_SET

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.

```

```
# \  
=====\  
==  
# agent:  
  
# \  
=====\  
# agent.logger  
# Define the following properties to set logging values.  
# If the following properties are not defined, the  
# agent uses the logging values from the Contrast UI.  
# \  
=====\  
# logger:  
  
# Enable diagnostic logging by setting a path to a log file.  
# While diagnostic logging hurts performance, it generates  
# useful information for debugging Contrast. The value set here  
# is the location to which the agent saves log output. If no  
# log file exists at this location, the agent creates a file.  
#  
# Example - `/opt/Contrast/contrast.log` creates a log in the  
# `/opt/Contrast` directory, and rotates it automatically as needed.  
#  
# path: ./contrast_agent.log  
  
# Set the the log output level. Valid options are  
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.  
# level: INFO  
  
# Override the name of the process the agents uses in logs.  
# progname: Contrast Agent  
  
# \  
=====\  
# agent.security_logger  
# Define the following properties to set security  
# logging values. If not defined, the agent uses the  
# security logging (CEF) values from the Contrast UI.  
# \  
=====\  
# security_logger:  
  
# Set the file to which the agent logs security events.  
# path: /.contrast/security.log  
  
# Set the log level for security logging. Valid options  
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.  
# level: ERROR  
  
# Change the Contrast security logger from a file-sized based rolling  
# scheme to a date-based rolling scheme. At midnight server time,  
# the log from the previous day is renamed to *file_name.yyyy-MM-dd*.  
# Note - this scheme does not have a size limit; manual log  
# pruning will be required. This flag must be set to use the
```

```
# backups and size flags. Value options are `true` or `false`.
# roll_daily: NEEDS_TO_BE_SET

# Specify the file size cap (in MB) of each log file.
# roll_size: NEEDS_TO_BE_SET

# Specify the number of backup logs that the agent will create before
# Contrast cleans up the oldest file. A value of `0` means that no \
backups
# are created, and the log is truncated when it reaches its size cap.
#
# Note - this property must be used with
# `agent.security_logger.roll_daily=false`; otherwise,
# Contrast continues to log daily and disregard this limit.
#
# backups: NEEDS_TO_BE_SET

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE
```

```
# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.python
# The following properties apply to any Python agent-wide configurations.
# \
=====
# python:

# Allow the agent to dump `cProfile` data to file for each request.
# enable_profiler: false

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Set to `false` to disable library analysis.
# analyze_libraries: true

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false
```

```
# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Value options are `ALL`, `SOME`, or `NONE`.
# stacktraces: ALL

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
```



```

==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
# protect.rules
# Use the following properties to set simple rule configurations.
# \
=====
# rules:

# Define a list of Protect rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
# protect.rules.bot-blocker
# Use the following selection to configure if the
# agent blocks bots. Set to `true` to enable blocking.
# \
=====
# bot-blocker:

# Set to `true` for the agent to block known bots.
# enable: false

# \
=====
# protect.rules.sql-injection
# Use the following settings to configure the sql-injection rule.
# \
=====
# sql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Tell the agent to detect when semantic analysis of the query
# reveals tautologies used in exfiltration attacks (e.g., "or
# 1=1" or "or 2<>3"). The agent blocks if blocking is enabled.
# detect_tautologies: true

# Tell the agent to detect when semantic analysis of the query
# reveals the invocation of dangerous functions typically used in

```

```
# weaponized exploits. The agent blocks if blocking is enabled.
# detect_dangerous_functions: true

# Tell the agent to detect when semantic analysis of the query
# reveals chained queries, which is uncommon in normal usage but
# common in exploit. The agent blocks if blocking is enabled.
# detect_chained_queries: true

# Tell the agent to detect when semantic analysis of the query
# reveals database queries are being made for system tables and
# sensitive information. The agent blocks if blocking is enabled.
# detect_suspicious_unions: true

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Detect when custom code attempts to access sensitive
# system files. The agent blocks if blocking is enabled.
# detect_custom_code_accessing_system_files: true

# Detect when users attempt to bypass filters by
# using ":::DATA" channels or null bytes in file
# names. The agent blocks if blocking is enabled.
# detect_common_file_exploits: true
```

```
# \  
=====  
# protect.rules.method-tampering  
# Use the following properties to configure  
# how the method tampering rule works.  
# \  
=====  
# method-tampering:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====  
# protect.rules.reflected-xss  
# Use the following properties to configure how  
# the reflected cross-site scripting rule works.  
# \  
=====  
# reflected-xss:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====  
# protect.rules.xxe  
# Use the following properties to configure  
# how the XML external entity works.  
# \  
=====  
# xxe:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====  
==
```

```
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
```

```
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==
# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
# api
```

```
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Certificate
# PEM file for communication with the Contrast UI.
# cert_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Key PEM
# file for communication with the Contrast UI.
# key_file: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
```

```
# \  
=====\  
# proxy:  
  
# Set value to `true` for the agent to communicate with  
# the Contrast web interface over a proxy. Set value to  
# `false` if you don't want to use the proxy. If no value is  
# indicated, the presence of a valid **contrast.proxy.host**  
# and **contrast.proxy.port** will enable the proxy.  
# enable: NEEDS_TO_BE_SET  
  
# Set the URL for your Proxy Server. The URL form is `scheme://  
host:port`.  
# url: NEEDS_TO_BE_SET  
  
# \  
=====\  
==  
# agent  
# Use the properties in this section to control the way and frequency  
# with which the agent communicates to logs and the Contrast UI.  
# \  
=====\  
==  
# agent:  
  
# \  
=====\  
# agent.logger  
# Define the following properties to set logging values.  
# If the following properties are not defined, the  
# agent uses the logging values from the Contrast UI.  
# \  
=====\  
# logger:  
  
# Enable diagnostic logging by setting a path to a log file.  
# While diagnostic logging hurts performance, it generates  
# useful information for debugging Contrast. The value set here  
# is the location to which the agent saves log output. If no  
# log file exists at this location, the agent creates a file.  
#  
# Example - `/opt/Contrast/contrast.log` creates a log in the  
# `/opt/Contrast` directory, and rotates it automatically as needed.  
#  
# path: ./contrast_agent.log  
  
# Set the the log output level. Valid options are  
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.  
# level: INFO  
  
# Override the name of the process the agents uses in logs.  
# progname: Contrast Agent  
  
# \  
=====
```

```
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# Change the Contrast security logger from a file-sized based rolling
# scheme to a date-based rolling scheme. At midnight server time,
# the log from the previous day is renamed to *file_name.yyyy-MM-dd*.
# Note - this scheme does not have a size limit; manual log
# pruning will be required. This flag must be set to use the
# backups and size flags. Value options are `true` or `false`.
# roll_daily: NEEDS_TO_BE_SET

# Specify the file size cap (in MB) of each log file.
# roll_size: NEEDS_TO_BE_SET

# Specify the number of backup logs that the agent will create before
# Contrast cleans up the oldest file. A value of `0` means that no \
backups
# are created, and the log is truncated when it reaches its size cap.
#
# Note - this property must be used with
# `agent.security_logger.roll_daily=false`; otherwise,
# Contrast continues to log daily and disregard this limit.
#
# backups: NEEDS_TO_BE_SET

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET
```



```
# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.python
# The following properties apply to any Python agent-wide configurations.
# \
=====
# python:

# Allow the agent to dump `cProfile` data to file for each request.
# enable_profiler: false

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Set to `false` to disable library analysis.
# analyze_libraries: true
```

```

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Value options are `ALL`, `SOME`, or `NONE`.
# stacktraces: ALL

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====

```

```
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
# protect.rules
# Use the following properties to set simple rule configurations.
# \
=====
# rules:

# Define a list of Protect rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
# protect.rules.bot-blocker
# Use the following selection to configure if the
# agent blocks bots. Set to `true` to enable blocking.
# \
=====
# bot-blocker:

# Set to `true` for the agent to block known bots.
# enable: false

# \
=====
```

```
# protect.rules.sql-injection
# Use the following settings to configure the sql-injection rule.
# \
=====
# sql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Tell the agent to detect when semantic analysis of the query
# reveals tautologies used in exfiltration attacks (e.g., "or
# 1=1" or "or 2<>3"). The agent blocks if blocking is enabled.
# detect_tautologies: true

# Tell the agent to detect when semantic analysis of the query
# reveals the invocation of dangerous functions typically used in
# weaponized exploits. The agent blocks if blocking is enabled.
# detect_dangerous_functions: true

# Tell the agent to detect when semantic analysis of the query
# reveals chained queries, which is uncommon in normal usage but
# common in exploit. The agent blocks if blocking is enabled.
# detect_chained_queries: true

# Tell the agent to detect when semantic analysis of the query
# reveals database queries are being made for system tables and
# sensitive information. The agent blocks if blocking is enabled.
# detect_suspicious_unions: true

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
```

```
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# Detect when custom code attempts to access sensitive
# system files. The agent blocks if blocking is enabled.
# detect_custom_code_accessing_system_files: true

# Detect when users attempt to bypass filters by
# using "::$DATA" channels or null bytes in file
# names. The agent blocks if blocking is enabled.
# detect_common_file_exploits: true

# \
=====
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off
```

```
# \  
=====\  
# protect.rules.xxe  
# Use the following properties to configure  
# how the XML external entity works.  
# \  
=====\  
# xxe:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====\  
==  
# application  
# Use the properties in this section for  
# the application(s) hosting this agent.  
# \  
=====\  
==  
# application:  
  
# Override the reported application name.  
#  
# Note - On Java systems where multiple, distinct applications may be  
# served by a single process, this configuration causes the agent to \  
report  
# all discovered applications as one application with the given name.  
#  
# name: NEEDS_TO_BE_SET  
  
# Override the reported application path.  
# path: NEEDS_TO_BE_SET  
  
# Add the name of the application group with which this  
# application should be associated in the Contrast UI.  
# group: NEEDS_TO_BE_SET  
  
# Add the application code this application should use in the Contrast UI.  
# code: NEEDS_TO_BE_SET  
  
# Override the reported application version.  
# version: NEEDS_TO_BE_SET  
  
# Apply labels to an application. Labels must  
# be formatted as a comma-delimited list.  
# Example - `label1,label2,label3`  
#
```

```
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
```

```
# tags: NEEDS_TO_BE_SET
```

## Python のテレメトリ

Python エージェントは、テレメトリを使用して、使用状況に関するデータを収集します。テレメトリは、エージェントを組み込んだアプリケーションでエージェントのセンサーが最初にロードされた時に収集され、その後も定期的に(数時間ごと)に収集されます。

弊社では、**お客様のプライバシーは非常に大切 (828ページ)** であると考えています。このテレメトリ機能は、アプリケーションのデータを収集するものではありません。データは匿名化されてから、Contrast に安全に送信されます。そして、集約されたデータは暗号化されて保存され、アクセスが制限されます。収集されたデータは、全て 1 年後に削除されます。

テレメトリ機能で収集されるのは、以下のデータです。

エージェントのバージョン	データ
Python 4.14.0	エージェントのバージョン
	オペレーティングシステムとバージョン
	Python のバージョン
	アプリケーションのフレームワークとバージョン
	Web サーバとバージョン
	Contrast インスタンスが SaaS 版かオンプレミス版であるか

テレメトリ機能を停止するには、`CONTRAST_AGENT_TELEMETRY_OPTOUT` という環境変数に 1 または true を設定してください。

テレメトリのデータは、`telemetry.python.contrastsecurity.com` に安全に送信されます。ネットワークレベルで通信をブロックすることで、テレメトリ機能を停止することもできます。

## Ruby エージェント

Ruby エージェントは、最も一般的な Web アプリケーションフレームワークとの互換性がある Rack ミドルウェアです。Ruby エージェントは、Rack との高度な互換性を実現し、Rack を基盤とするアプリケーションに IAST(Interactive Application Security Testing)および RASP(Runtime Application Self-Protection)機能を提供します。

Assess では、アプリケーションを通常どおり実行している間にエージェントが脆弱なデータフローパスやその他の問題を特定します。エージェントはこれらの検出結果を Contrast 内の組織に報告します。そのため、アプリケーションを実際の環境にデプロイする前に脆弱性に対処することができます。

Protect では、Ruby エージェントが HTTP リクエストを検査して、問題を引き起こす可能性のある入力ベクトルを特定します。リクエスト中に、データベースクエリとファイル書込みのほか、リクエストの結果が原因で損害を及ぼす可能性のあるその他のアクションをエージェントが検査します。リクエストの最後に、エージェントはレンダリングされた出力を検査し、攻撃が成功したかどうかを確認し、成功した攻撃がユーザに転送されないようにブロックすることができます。そして、攻撃の詳細が Contrast サーバに送信され、その後アラートが送信されると攻撃の詳細がインターフェイスに表示されます。



### 注記

Ruby エージェントは、Contrast Assess、Contrast Protect、Contrast SCA に対応しています。

次のステップ：



- [Ruby エージェントをインストール \(395ページ\)](#)する
- [Ruby エージェントのサポート対象テクノロジーを確認 \(393ページ\)](#)する

## Ruby エージェントのシステム要件

Ruby エージェントをインストールする前に、以下のシステム要件を満たす必要があります。

- 検査対象のアプリケーションがデプロイされており、その Web アプリケーションのテクノロジーは Contrast のサポート対象であること。
- アプリケーションは再起動可能であること。
- Web サーバが Contrast とネットワークで接続されていること。
- Web サーバが RubyGems とネットワークで接続されているか、エージェントが手動でインストールされていること。
- サーバが以下の表に示す最小要件を満たしていること。

要件	バージョン	備考
オペレーティングシステム	<ul style="list-style-type: none"> <li>• 64 ビット Linux (推奨)</li> <li>• 64 ビット OS X</li> <li>• 64 ビット Alpine</li> </ul>	<p>エージェントのバージョン 3.0.0 以降で、gem インストール時に C 拡張のコンパイルが必要になります。この処理は自動的に行われますが、ターゲット環境で以下のインストールが必要な場合があります。</p> <ul style="list-style-type: none"> <li>• gcc、make、automake、autoconf (パッケージ名は異なる場合があります。また、お使いのプラットフォームのバージョンの build-essential のインストールが必要な場合があります。)</li> <li>• システムヘッダ</li> </ul> <p>エージェントは、Ruby のアプリケーション層で実行する際に C との依存関係がいくつかあるため、<i>glibc</i> または <i>musl libc</i> ベースのシステムでのコンパイルを許可するために <code>--platform ruby</code> フラグを付けてインストールしなければならない場合があります。</p>
Ruby gems	<ul style="list-style-type: none"> <li>• ougai : ~&gt;1.8 (1.8 以降、2 より前)</li> <li>• parser : ~&gt;2.6 (2.6 以降、3 より前)</li> <li>• protobuf : ~&gt;3.10 (3.10 以降、4 より前)</li> <li>• rack : ~&gt;2.0 (2.0 以降、3 より前)</li> </ul>	

## Ruby エージェントのサポート対象テクノロジー

このエージェントでは、以下のテクノロジーをサポートしています。

テクノロジー	サポート対象バージョン	備考
言語のバージョン	<ul style="list-style-type: none"> <li>3.2.x: 最初のサポート対象エージェントは 6.13.0</li> <li>3.1.x: 最初のサポート対象エージェントは 6.0.0</li> <li>3.0.x: 最初のサポート対象エージェントは 4.6.0</li> </ul>	<p>Contrast は、通常のメンテナンスおよびセキュリティメンテナンスステータスの Ruby LTS(長期サポート)バージョンをサポートします。Ruby バージョンのサポートは、ワーキンググループが LTS 期間をシフトするのに合わせて変更されます。</p>
	<p>具体的なリリース日については、<a href="#">Ruby メンテナンスブランチのスケジュール</a>を参照してください。</p>	<p><b>サポート対象外:</b></p>
		<ul style="list-style-type: none"> <li>2.5.x: 最後のサポート対象エージェントは 4.14.1</li> <li>2.4.x: 最後のサポート対象エージェントは 3.9.1</li> <li>2.6.x: 最後のサポート対象エージェントは 5.3.0</li> <li>2.7.x: 最後のサポート対象エージェントは 6.15.3</li> </ul>
アプリケーションフレームワーク	<ul style="list-style-type: none"> <li>Rails 6.x - 7.x</li> <li>Grape 1.5.x</li> <li>Sinatra 3.x</li> </ul>	<p>正式にサポートされていない <a href="#">Rack ベースの Web フレームワーク</a>でもエージェントは動作しますが、サポート対象のフレームワークの場合と比べて具体性の低い検出結果となる可能性があります。アプリケーションコード内で発生した脆弱性が報告されるのではなく、Rack メソッドと直接のインターフェイスとなるフレームワークコード内の脆弱性が報告される可能性があります。</p>
		<p><b>サポート対象外:</b></p>
		<ul style="list-style-type: none"> <li>Rails 3.x: 最後のサポート対象エージェントは 3.11.0</li> <li>Rails 4.x: 最後のサポート対象エージェントは 3.11.0</li> <li>Rails 5.x: 最後のサポート対象エージェントは 6.15.3</li> </ul>
データベース	<ul style="list-style-type: none"> <li>MongoDB</li> <li>Mysql2</li> <li>PG</li> <li>SQLite3</li> </ul>	<p>Contrast は、古いバージョンや非推奨バージョンのサードパーティモジュールをサポートしません。</p>

テクノロジー	サポート対象バージョン	備考
テスト環境	サポート対象のオペレーティングシステム、アプリケーションフレームワーク、Web サーバの組み合わせでテストを実施し、Ruby Mspec Suite も実行します。	エージェントに変更が加えられると、Contrast は一連の自動化テストを実行し、サポート対象のすべての Ruby バージョンについてサポート対象テクノロジーでの検出結果を確認します。Contrast 独自のテストに加えて、エージェントを有効にした環境で Ruby Spec Suite を実行します。
Web サーバ	<ul style="list-style-type: none"><li>• <a href="#">Passenger</a> 5.37、6.x</li><li>• <a href="#">Puma</a> 3.7 - 5.x</li><li>• <a href="#">Thin</a> 1.7.2 - 1.8.x</li><li>• <a href="#">Unicorn</a> 5.0.x - 6.x</li></ul>	

## Ruby エージェントのインストール

`contrast-agent.gem` は、アプリケーションの Gemfile に追加する標準の Ruby ライブラリです。

Ruby エージェントを [RubyGems](#) を使用して `gem source` として ([395ページ](#))インストールする、もしくは [Ruby エージェントをアップデート](#) ([396ページ](#))してください。

## RubyGems から gem source として Ruby エージェントをインストール

RubyGems から Ruby エージェントをダウンロードするには：

1. 以下をアプリケーションの gemfile に追加します。

```
gem 'contrast-agent'
```

2. インストールを実行します。

```
bundle install
```

または更新を実行します。

```
bundle update contrast-agent
```

3. [ミドルウェアを設定します](#) ([397ページ](#))(Rails、Sinatra または Grape)。
4. [エージェントを設定します](#)。 ([397ページ](#))
5. エージェントを実行するシステムに `autoconf` がインストールされていることを確認します。
6. Contrast にアプリケーションが表示されることを確認します。



### 注記

Alpine にインストールする場合は、インストール前に `bundle config force_ruby_platform true` コマンドを実行する必要があります。



### 注記

特定の環境でのみ Contrast で実行したい場合は、[Bundler のグループ機能](#)を使用して実行できます。

## Ruby エージェントのアップデート

Contrast の Ruby エージェントを自動的に更新するのに最も信頼性が高く効率的な方法は、Ruby Bundler を使用し、利用可能な最新バージョンをダウンロードしてインストールすることです。Ruby の Bundler は通常、Ruby アプリケーションのすべての依存関係を管理するため、すでにビルド環境の一部として利用可能になっているはずですが、Ruby エージェントを更新する頻度と更新の取得先は、組織の設定と Contrast の実装(SaaS 版またはオンプレミス版)によって異なります。

主な手順：

1. Contrast Ruby エージェントの入手元を決めます。
2. エージェントをインストールします。
3. スクリプトを使って自動アップデートを行います。

### 開始する前に

- Ruby の Bundler パッケージマネージャにある程度の知識があること。
- Contrast エージェントの RubyGems リポジトリへアクセスできること。
- Ruby アプリケーションが Contrast エージェントなしで想定どおりに機能すること。
- 事前に Contrast の Ruby エージェントが正常にインストールされていること。
- 変更管理ポリシーと使用する環境に基づいて、エージェントをアップデートする方法とタイミングを決めていること。

### エージェントのインストールとスクリプトによる自動アップデート

1. Contrast の Ruby エージェントの入手元を決めます。
  - RubyGems のパブリック(またはプライベート)リポジトリ
2. Gemfile に Contrast の Ruby エージェントを含めると、アプリケーションの新しいビルドで常に最新バージョンのエージェントを使用できるよう合わせることができます。Contrast エージェント (contrast-agent) のバージョンは指定しないで下さい。そうすれば最新のバージョンが取得されます。

Gemfile は、Ruby アプリケーションが RubyGems(パブリックまたはプライベート)リポジトリからのアーティファクトでビルドされるたびに自動的に解決する依存関係を指定するファイルです。
3. Gemfile を更新した後、アプリケーションをビルドするときに次のコマンドを使用します。これにより、Contrast の Ruby エージェントが RubyGems から自動的にダウンロードされ、Ruby アプリケーションに追加または更新されます。

```
$ bundle install
```

4. Gemfile に contrast-agent を追加した後は、次のように Bundler を使用してエージェントを更新できます。

```
bundle update contrast-agent
```

### Gem を手動でインストールする

Ruby のビルドプロセスの一部として手動でエージェントを更新することができます。この場合、2つの方法があります。お客様の組織とワークフローに最適な方法を選択してください。

- **RubyGems** : 次のコマンドを使用して、RubyGems(パブリックまたはプライベート)から Contrast の Ruby エージェントを取得してアプリケーションにインストールします。

```
$ gem install contrast-agent
```

上記のコマンドはエージェントをローカルにインストールするのみのため、Bundler で更新を管理するには、Gemfile に次の行を追加します。

```
gem "contrast-agent"
```

次に、Bundler を使用してエージェントをインストールまたは更新するには、次のコマンドを実行します。

```
$ bundle install
```

- 上記のコマンドはエージェントをローカルにインストールするのみのため、Bundler で更新を管理するには、Gemfile に次の行を追加します。

```
gem "contrast-agent"
```

## 関連項目

- [Ruby エージェントのサポート対象テクノロジー \(393ページ\)](#)
- [Ruby エージェントのインストール \(395ページ\)](#)

## Ruby エージェントの設定

全てのエージェントには基本の[設定 \(35ページ\)](#)があり、設定値には[優先順位 \(36ページ\)](#)があります。YAML 設定ファイルを使用して、エージェントを設定します。



### ヒント

[Contrast エージェント設定エディタ \(39ページ\)](#)を使用すると、YAML 設定ファイルの作成やアップロード、YAML の検証、推奨される設定値の表示などができます。

ご利用の環境に合わせて、次の各ガイドラインに従ってください。

- [フレームワーク \(418ページ\)](#)
  - [Grape \(418ページ\)](#)
  - [Rails \(418ページ\)](#)
  - [Sinatra \(419ページ\)](#)
- [Web サーバ \(419ページ\)](#)
  - [Passenger \(419ページ\)](#)
  - [Puma \(422ページ\)](#)
  - [Thin \(425ページ\)](#)
  - [Unicorn \(426ページ\)](#)

## 関連項目

- [Ruby エージェントのサポート対象テクノロジー \(393ページ\)](#)

## Ruby エージェントの YAML テンプレート

YAML 設定ファイルを使用して Ruby エージェントを設定する場合には、以下のテンプレートをご利用ください(YAML 設定については、[YAML 設定の説明 \(38ページ\)](#)を参照してください)。

YAML 設定ファイルは、デフォルトの場所に配置します : /etc/contrast/  
contrast\_security.yaml

```
# \  
=====  
==  
# Use the properties in this YAML file to configure a Contrast agent.  
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html  
# to determine the order of precedence for configuration values.
```

```
# \  
=====  
==  
  
# Use this setting if you want to temporarily disable a Contrast agent.  
# Set to `true` to enable the agent; set to `false` to disable the agent.  
# enable: true  
  
# \  
=====  
==  
# api  
# Use the properties in this section to connect the agent to the Contrast \  
UI.  
# \  
=====  
==  
api:  
  
# ***** REQUIRED *****  
# Set the URL for the Contrast UI.  
url: https://app.contrastsecurity.com/Contrast  
  
# ***** REQUIRED *****  
# Set the API key needed to communicate with the Contrast UI.  
api_key: NEEDS_TO_BE_SET  
  
# ***** REQUIRED *****  
# Set the service key needed to communicate with the Contrast  
# UI. It is used to calculate the Authorization header.  
service_key: NEEDS_TO_BE_SET  
  
# ***** REQUIRED *****  
# Set the user name used to communicate with the Contrast  
# UI. It is used to calculate the Authorization header.  
user_name: NEEDS_TO_BE_SET  
  
# \  
=====  
# api.certificate  
# Use the following properties for communication  
# with the Contrast UI using certificates.  
# \  
=====  
# certificate:  
  
# If set to `false`, the agent will ignore the  
# certificate configuration in this section.  
# enable: true  
  
# Set the absolute or relative path to a CA for communication  
# with the Contrast UI using a self-signed certificate.  
# ca_file: NEEDS_TO_BE_SET
```

```
# Set the absolute or relative path to the Certificate
# PEM file for communication with the Contrast UI.
# cert_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Key PEM
# file for communication with the Contrast UI.
# key_file: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid **contrast.proxy.host**
# and **contrast.proxy.port** will enable the proxy.
# enable: NEEDS_TO_BE_SET

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
#
```

```

# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
#
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Override the name of the process the agents uses in logs.
# progame: Contrast Agent

# Set to `true` for the agent to tag
# logs with `!AM!` for the metrics tool.
# metrics: true

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

```



```
# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.heap_dump
# The following properties are used to trigger heap dumps from within
# the agent to snapshot the behavior of instrumented applications.
# \
=====
# heap_dump:

# Set to `true` for the agent to automatically
# take heap dumps of the instrumented application.
# enable: false

# Set the location to which to save the heap dump files. If relative,
# the path is determined based on the process' working directory.
# path: contrast_heap_dumps

# Set the amount of time to wait, in milliseconds,
# after agent startup to begin taking heap dumps.
# delay_ms: 10_000

# Set the amount of time to wait, in milliseconds, between each heap \
dump.
# window_ms: 10_000

# Set the number of heap dumps to take before disabling this feature.
# count: 5

# Set to `true` for the agent to trigger garbage collection before
# taking a heap dump to remove temporary objects from the dump.
# clean: false
```

```
# \  
=====
```

```
# agent.ruby  
# The following properties apply to any Ruby agent-wide configurations.  
# \  
=====
```

```
# ruby:
```

```
  # Allow the agent to track frozen Objects returned by  
  # source methods. This configuration is on by default.  
  # track_frozen_sources: NEEDS_TO_BE_SET
```

```
  # Allow the agent to track propagation through interpolated  
  # Strings. This configuration is on by default.  
  # interpolate: NEEDS_TO_BE_SET
```

```
  # Set a comma-separated string of rake tasks  
  # in which to disable agent operation.  
  # disabled_agent_rake_tasks: \  
about,assets:clean,assets:clobber,assets:environment,assets:precompile,asset  
s:precompile:all,db:create,db:drop,db:migrate:status,db:rollback,db:schema:c  
ache:clear,db:schema:cache:dump,db:schema:dump,db:schema:load,db:seed,db:set  
up,db:structure:dump,db:version,doc:app,log:clear,middleware,notes,notes:cus  
tom,rails:template,rails:update,routes,secret,spec,spec:features,spec:reques  
ts,spec:controllers,spec:helpers,spec:models,spec:views,spec:routing,spec:rc  
ov,stats,test,test:all,test:all:db,test:recent,test:single,test:uncommitted,  
time:zones:all,tmp:clear,tmp:create,webpacker:compile
```

```
# \  
=====
```

```
==  
# inventory  
# Use the properties in this section to override the inventory features.  
# \  
=====
```

```
==  
# inventory:
```

```
  # Set to `false` to disable inventory features in the agent.  
  # enable: true
```

```
  # Apply a list of labels to libraries. Labels  
  # must be formatted as a comma-delimited list.  
  # Example - `label1, label2, label3`  
  #  
  # tags: NEEDS_TO_BE_SET
```

```
# \  
=====
```

```
==  
# assess  
# Use the properties in this section to control Assess.  
# \  
=====
```

```
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Value options are `ALL`, `SOME`, or `NONE`.
# stacktraces: ALL

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET
```

```
# \  
=====  
==  
# protect  
# Use the properties in this section to override Protect features.  
# \  
=====  
==  
# protect:  
  
# Use the properties in this section to determine if the  
# Protect feature should be enabled. If this property is not  
# present, the decision is delegated to the Contrast UI.  
# enable: false  
  
# \  
=====  
# protect.rules  
# Use the following properties to set simple rule configurations.  
# \  
=====  
# rules:  
  
# Define a list of Protect rules to disable in the agent.  
# The rules must be formatted as a comma-delimited list.  
# disabled_rules: NEEDS_TO_BE_SET  
  
# \  
=====  
# protect.rules.bot-blocker  
# Use the following selection to configure if the  
# agent blocks bots. Set to `true` to enable blocking.  
# \  
=====  
# bot-blocker:  
  
# Set to `true` for the agent to block known bots.  
# enable: false  
  
# \  
=====  
# protect.rules.sql-injection  
# Use the following settings to configure the sql-injection rule.  
# \  
=====  
# sql-injection:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or off.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off
```

```
# \  
=====
```

```
# protect.rules.cmd-injection  
# Use the following properties to configure  
# how the command injection rule works.  
# \  
=====
```

```
# cmd-injection:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====
```

```
# protect.rules.path-traversal  
# Use the following properties to configure  
# how the path traversal rule works.  
# \  
=====
```

```
# path-traversal:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====
```

```
# protect.rules.method-tampering  
# Use the following properties to configure  
# how the method tampering rule works.  
# \  
=====
```

```
# method-tampering:  
  
# Set the mode of the rule. Value options are  
# `monitor`, `block`, `block_at_perimeter`, or `off`.  
#  
# Note - If a setting says, "if blocking is enabled",  
# the setting can be `block` or `block_at_perimeter`.  
#  
# mode: off  
  
# \  
=====
```

```
# protect.rules.reflected-xss  
# Use the following properties to configure how
```

```

# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.

```

```
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET
```

```
# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET
```

```
# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==

# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
```



```

# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Certificate
# PEM file for communication with the Contrast UI.
# cert_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Key PEM
# file for communication with the Contrast UI.
# key_file: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid contrast.proxy.host
# and contrast.proxy.port will enable the proxy.
# enable: NEEDS_TO_BE_SET

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \

```

```
=====  
==  
# agent:  
  
# \  
=====  
# agent.logger  
# Define the following properties to set logging values.  
# If the following properties are not defined, the  
# agent uses the logging values from the Contrast UI.  
# \  
=====  
# logger:  
  
# Enable diagnostic logging by setting a path to a log file.  
# While diagnostic logging hurts performance, it generates  
# useful information for debugging Contrast. The value set here  
# is the location to which the agent saves log output. If no  
# log file exists at this location, the agent creates a file.  
#  
# Example - `/opt/Contrast/contrast.log` creates a log in the  
# `/opt/Contrast` directory, and rotates it automatically as needed.  
#  
# path: ./contrast_agent.log  
  
# Set the the log output level. Valid options are  
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.  
# level: INFO  
  
# Override the name of the process the agents uses in logs.  
# progname: Contrast Agent  
  
# Set to `true` for the agent to tag  
# logs with `!AM!` for the metrics tool.  
# metrics: true  
  
# \  
=====  
# agent.security_logger  
# Define the following properties to set security  
# logging values. If not defined, the agent uses the  
# security logging (CEF) values from the Contrast UI.  
# \  
=====  
# security_logger:  
  
# Set the file to which the agent logs security events.  
# path: ./contrast/security.log  
  
# Set the log level for security logging. Valid options  
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.  
# level: ERROR  
  
# \  
=====
```

```
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.heap_dump
# The following properties are used to trigger heap dumps from within
# the agent to snapshot the behavior of instrumented applications.
# \
=====
# heap_dump:

# Set to `true` for the agent to automatically
# take heap dumps of the instrumented application.
```

```

# enable: false

# Set the location to which to save the heap dump files. If relative,
# the path is determined based on the process' working directory.
# path: contrast_heap_dumps

# Set the amount of time to wait, in milliseconds,
# after agent startup to begin taking heap dumps.
# delay_ms: 10_000

# Set the amount of time to wait, in milliseconds, between each heap \
dump.
# window_ms: 10_000

# Set the number of heap dumps to take before disabling this feature.
# count: 5

# Set to `true` for the agent to trigger garbage collection before
# taking a heap dump to remove temporary objects from the dump.
# clean: false

# \
=====
# agent.ruby
# The following properties apply to any Ruby agent-wide configurations.
# \
=====
# ruby:

# Allow the agent to track frozen Objects returned by
# source methods. This configuration is on by default.
# track_frozen_sources: NEEDS_TO_BE_SET

# Allow the agent to track propagation through interpolated
# Strings. This configuration is on by default.
# interpolate: NEEDS_TO_BE_SET

# Set a comma-separated string of rake tasks
# in which to disable agent operation.
# disabled_agent_rake_tasks: \
about,assets:clean,assets:clobber,assets:environment,assets:precompile,asset
s:precompile:all,db:create,db:drop,db:migrate:status,db:rollback,db:schema:c
ache:clear,db:schema:cache:dump,db:schema:dump,db:schema:load,db:seed,db:set
up,db:structure:dump,db:version,doc:app,log:clear,middleware,notes,notes:cus
tom,rails:template,rails:update,routes,secret,spec,spec:features,spec:reques
ts,spec:controllers,spec:helpers,spec:models,spec:views,spec:routing,spec:rc
ov,stats,test,test:all,test:all:db,test:recent,test:single,test:uncommitted,
time:zones:all,tmp:clear,tmp:create,webpacker:compile

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \

```

```
=====  
==  
# inventory:  
  
# Set to `false` to disable inventory features in the agent.  
# enable: true  
  
# Apply a list of labels to libraries. Labels  
# must be formatted as a comma-delimited list.  
# Example - `label1, label2, label3`  
#  
# tags: NEEDS_TO_BE_SET  
  
# \  
=====  
==  
# assess  
# Use the properties in this section to control Assess.  
# \  
=====  
==  
# assess:  
  
# Include this property to determine if the Assess  
# feature should be enabled. If this property is not  
# present, the decision is delegated to the Contrast UI.  
# enable: false  
  
# Apply a list of labels to vulnerabilities and preflight  
# messages. Labels must be formatted as a comma-delimited list.  
# Example - `label1, label2, label3`  
#  
# tags: NEEDS_TO_BE_SET  
  
# Value options are `ALL`, `SOME`, or `NONE`.  
# stacktraces: ALL  
  
# \  
=====  
# assess.sampling  
# Use the following properties to control sampling in the agent.  
# \  
=====  
# sampling:  
  
# Set to `true` to enable sampling.  
# enable: false  
  
# This property indicates the number of requests  
# to analyze in each window before sampling begins.  
# baseline: 5  
  
# This property indicates that every *nth*  
# request after the baseline is analyzed.  
# request_frequency: 10
```

```
# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
# protect.rules
# Use the following properties to set simple rule configurations.
# \
=====
# rules:

# Define a list of Protect rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
# protect.rules.bot-blocker
# Use the following selection to configure if the
# agent blocks bots. Set to `true` to enable blocking.
# \
=====
# bot-blocker:
```

```
# Set to `true` for the agent to block known bots.
# enable: false

# \
=====
# protect.rules.sql-injection
# Use the following settings to configure the sql-injection rule.
# \
=====
# sql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
```

```
=====
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
==
# application
# Use the properties in this section for
```



```
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
```

```
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET
```

## Ruby フレームワーク

アプリケーションフレームワークとはソフトウェアのライブラリで、アプリケーション開発を支援するための基礎的な構造を提供します。

お使いのフレームワークに合わせて、以下の各ガイドラインに従ってください。

### Grape での設定

Grape フレームワークを使用している場合、Ruby エージェントを使用するためにアプリケーションを設定する必要があります。Ruby エージェントを使用するように設定した簡単なアプリケーションは、以下の例のようになります。

```
require 'grape'
require 'contrast-agent'

class App < Grape::API
  use Contrast::Agent::Middleware, true
end
```

### Rails での設定

Rails を使用している場合、Ruby エージェントは [Railtie](#) として機能するため追加の設定は必要ありません。

## Sinatra での設定

Sinatra フレームワークを使用している場合、Ruby エージェントを使用するためにアプリケーションを設定する必要があります。Ruby エージェントを使用するように設定した簡単なアプリケーションは、以下の例のようになります。

```
require 'sinatra'
require 'contrast-agent'

class App < Sinatra::Base
  use Contrast::Agent::Middleware, true
end
```

### 関連項目

- [Ruby エージェントの設定 \(397ページ\)](#)
- [Ruby エージェントのサポート対象テクノロジー \(393ページ\)](#)

## Ruby Web サーバ

Web サーバは、Web アプリケーションフレームワークをデプロイするための技術です。これらのサーバは、アプリケーションプロセスを管理し、HTTP リクエストを受信して、Web アプリケーションフレームワークに転送します。

お使いの Web サーバのガイドラインに従ってください。

- [Passenger \(419ページ\)](#)
- [Puma \(422ページ\)](#)
- [Thin \(425ページ\)](#)
- [Unicorn \(426ページ\)](#)

### 関連項目

- [Ruby エージェントの設定 \(397ページ\)](#)
- [Ruby エージェントのサポート対象テクノロジー \(393ページ\)](#)

## Passenger での設定

Ruby エージェントがアプリケーションをタイムアウトさせてしまい、サーバが起動できなくなることがあります。これはサーバの設定によって防ぐことができます。

Passenger の設定は、スタンドアロンモードでも、HTTP サーバ(*Passenger + NGINX* や *Passenger + Apache*)の組合せでも指定できます。

スタンドアロンモードでの標準的な設定方法は、次の 3 つから選択できます。

1. コマンドライン引数 :

```
$ passenger start --start-timeout 100
```

2. 環境変数 :

```
$ env PASSENGER_START_TIMEOUT=100 passenger start
```

3. Passengerfile.json(アプリケーションディレクトリに配置) :

```
{
  "start_timeout": "100"
}
```

設定の順序(優先順位の高い順) :

- コマンドライン引数
- 環境変数
- Passengerfile.json ファイル



### 注記

大規模なデプロイメントの場合は例外で、コマンドライン引数と環境変数の両方の設定は、アプリケーションで事前に設定された値で上書きされます。

Passenger を NGINX や Apache と組み合わせる場合は、NGINX や Apache の設定ファイルを使用します。この場合、Passengerfile.json は使用しません。

```
# example of an Nginx configuration file which also configures Passenger:
```

```
server {
    server_name yourserver.com;
    root /var/www/myapp/code/public;
    passenger_enabled on;
    passenger_ruby /usr/bin/ruby2.0;
    passenger_sticky_sessions on;
}
```

```
# example of an Apache configuration file which also configures Passenger:
```

```
<VirtualHost *:80>
    ServerName yourserver.com
    DocumentRoot /var/www/myapp/code/public
    PassengerStickySessions on

    <Directory /var/www/myapp/code/public>
        Allow from all
        Options -MultiViews
        Require all granted
    </Directory>
</VirtualHost>
```

## タイムアウトの設定

- **最大リクエスト時間** - アプリケーションプロセスがリクエストを処理するのにかかる最大時間を秒単位で指定します。リクエストの処理にかかる時間がこの時間を超えた場合、アプリケーションプロセスは強制的にシャットダウンされ、次のリクエスト時に再起動されます。値が 0 の場合は、時間制限が無いことを意味します。これは Passenger エンタプライズ版のみ有効な設定です。

- デフォルト値: 0
- コマンドライン:

```
$ passenger start --max-request-time SECONDS
```

- 環境変数:

- Passengerfile.json ファイル:

```
{
    "max_request_time": integer
}
```

- **最大リクエストキュー時間** - 同時に処理されるリクエストが最大数に達すると、Passenger は全ての受信リクエストをキューに入れます。このオプションでは、リクエストがキューに保持される最大時間を指定します。キュー内のリクエストが指定された上限に達した場合、そのリクエストに対して「504 Gateway Timeout」エラーが返されます。値が 0 の場合は、キューの時間に制限が無いことを意味します。これは Passenger エンタープライズ版のみ有効な設定です。

- デフォルト値 : 0
- コマンドライン :

```
$ passenger start --max-request-queue-time NUMBER
```

- 環境変数 :

```
PASSENGER_MAX_REQUEST_QUEUE_TIME=integer
```

- Passengerfile.json ファイル :

```
{  
  "max_request_queue_time": integer  
}
```

- **プールのアイドル時間** - アプリケーションプロセスの最大アイドル時間です。指定された秒数を超えてもアプリケーションプロセスが何のトラフィックも受信しない場合、メモリを節約するためにアプリケーションプロセスをシャットダウンします。この値を 0 に設定すると、手動で停止するかクラッシュが発生しない限り、アプリケーションプロセスはシャットダウンされません。この値を小さくすると、アプリケーションプロセスの起動がより頻繁に必要になります。

- デフォルト値 : 300(5 分)
- コマンドライン :

```
$ passenger start --pool-idle-time SECONDS
```

- 環境変数 :

```
PASSENGER_POOL_IDLE_TIME=integer
```

- Passengerfile.json ファイル :

```
{  
  "pool_idle_time": integer  
}
```

- **最大プリロードアイドル時間** - 一定時間プリロードプロセスが何も処理をしていない場合に、自動的にシャットダウンするためのタイムアウトの時間です。このオプションは秒数で設定します。値が 0 の場合は、アイドル状態のタイムアウトが発生しないことを意味します。値を大きくすると、プリロードプロセスが長く存在することになり、メモリ使用量が若干増加する可能性があります。但し、プリロードサーバが実行されている限り、Ruby アプリケーションプロセスの起動に要する時間は、通常起動に必要とされる時間の約 10% で済みます。

- デフォルト値 : 300(5 分)
- コマンドライン :

```
$ passenger start --max-preloader-idle-time SECONDS
```

- 環境変数 :

```
PASSENGER_MAX_PRELOADER_IDLE_TIME=integer
```

- Passengerfile.json ファイル :

```
{  
  "max_preloader_idle_time": integer  
}
```

- **起動タイムアウト** - アプリケーションの起動のタイムアウトです。アプリケーションプロセスがこのタイムアウト時間内に起動できなかった場合、シグナル(SIGKILL)で強制終了され、エラーがログに記録されます。

- デフォルト値 : 90

- コマンドライン :

```
$ passenger start --start-timeout SECONDS;
```

- 環境変数 :

```
PASSENGER_START_TIMEOUT=integer
```

- Passengerfile.json ファイル :

```
{  
  "start_timeout": integer  
}
```

## フォーク

Passenger はプロセスマネージャのようなもので、自分のプロセス領域でアプリケーションを実行するのではなく、外部プロセスとして起動して、その管理を行います。これには、使用されていないプロセスのシャットダウンやクラッシュしたプロセスの再起動などが含まれます。アプリケーションのインスタンスは、プロセスと呼ばれます。Passenger はアプリケーションの起動や停止を行います。

Passenger がアプリケーションのインスタンスを起動すると、プロセスの生成が行われます。Passenger でアプリケーションのプロセスを生成するには、次の 2 つの方法があります。

- **direct** : アプリケーションコードと Web フレームワークの完全なコピーをメモリ上に持つ新しい Ruby プロセスを生成します。この方法は、より多くのメモリを使用し、起動に時間がかかります。
- **smart** : Ruby アプリケーションの場合、この方法がデフォルトです。最初にプリロード(preloader)処理が実行されます。この処理は、config.ru ファイルを読み込むことで、Web フレームワークと一緒にアプリケーション全体をロードします。プリロード処理は、リクエスト処理には関与しません。新しいアプリケーションプロセスが必要になるたびに、子プロセスを生成します(fork システムコールを使用)。

新しいフォークを作成するためのコマンドは以下のようになります。

```
$ bundle exec passenger start --min-instances 2
```

これにより、Passenger はアプリケーションのインスタンスを 2 つ保持することになります。

- デフォルト値 : 1
- インスタンスの最大プール数のデフォルト : 6
- Passengerfile.json ファイル :

```
{  
  "max_pool_size": 6  
}
```

Passenger は、リクエストを受け付けると、リクエスト数が最も少ないプロセスにそのリクエストを渡します。プロセスが強制終了すると、Passenger が自動的にプロセスを再起動します。また、プロセスはトラフィックに応じて動的に拡張され、最大プール数までフォークにより新しいプロセスを生成します。

## 関連項目

- [Ruby エージェントの設定 \(397ページ\)](#)
- [Ruby エージェントのサポート対象テクノロジー \(393ページ\)](#)

## Puma での設定

Ruby エージェントがアプリケーションをタイムアウトさせてしまい、サーバが起動できなくなることがあります。これは、サーバの設定によって防ぐことができます。

Puma の設定は、CLI を使用して config/puma.rb または config.ru ファイルで直接指定できます。

## タイムアウトの設定

Contrast エージェントは、デフォルトの設定またはカスタム設定で動作するはずですが、最初のリクエスト処理でオーバーヘッドがかかります。そのため、タイムアウトの設定時間を増やす必要がある場合があります。



### 重要

一部のオプションは、クラスタモードでのみ利用できます。タイムアウトに利用できる全てのオプションは、[puma/dsl.rb](#) に記載されています。

- **persistent\_timeout(seconds)** - Puma が持続的接続を閉じるまでのアイドル時間を定義します。seconds(秒数)には、整数を指定します。
- **first\_data\_timeout(seconds)** - データが受信されなかった場合に、TCP ソケットを開けている時間を定義します。seconds(秒数)には、整数を指定します。
- **\*force\_shutdown\_after(val=:forever)\*** - スレッドをシャットダウンする際に、スレッドが停止するまで待機する時間を定義します。秒数も指定することができますが、`:forever` もしくは `:immediately` を指定できます。
  - `:forever` - 値は -1 に設定されます。
  - `:immediately` - 値は 0 に設定されます。
  - `seconds` - タイムアウト値として、秒数を直接設定します。



### 注記

Puma は即時モードであっても、シャットダウンの前に常に数秒間は待機します。

以下のオプションは、クラスタモードでのみ利用できます。

- **worker\_timeout(seconds)** - 指定したタイムアウト(秒数)内に、全てのワーカがマスタープロセスにチェックインしたかどうかを検証します。これはリクエストのタイムアウトではなく、プロセスの停止やハングアップを防ぐためのものです。この値を設定しても、時間の掛かるリクエストを防げるわけではありません。最小値は 6 秒、デフォルト値は 60 秒です。
- **worker\_boot\_timeout(seconds)** - ワーカが起動する際のデフォルトのタイムアウトを変更します。指定されていない場合は、デフォルトは `worker_timeout` の値になります。
- **worker\_shutdown\_timeout(seconds)** - ワーカがシャットダウンする際のタイムアウトを設定します。
- **wait\_for\_less\_busy\_worker(val=0.005)** - ソケットのリッスンを遅らせることにより、ビジーでないワーカにトラフィックをルーティングし、リクエストを最初に取得してもらうための待ち時間です。



### 注記

この設定は MRI でのみ機能します。他のインタプリタでは、この設定は無効です。

Puma では、最初に 2 つのデフォルトのタイムアウト値が設定されます。

- `DefaultWorkerTimeout = 60`
- `DefaultWorkerShutdownTimeout = 30`

全てのタイムアウトの設定を適用するには、Puma をクラスタモードに設定してください。

## フォーク

クラスタモードが Puma 5 から導入され、Puma はマスタプロセスから直接ではなく、ワーカ 0 からワーカをフォークできるようになりました。

`preload_app` オプションと同様に、`fork_worker` オプションを使用すると、アプリケーションは一度だけ初期化され、コピーオンライト(COW)メモリを削減できます。

このモードにはいくつかの利点があり、まず第一に、段階的な再起動(phased restart)と互換性があります。マスタプロセス自体は最初にアプリケーションをプリロードしませんので、このモードによって段階的な再起動が有効になります。段階的な再起動の一環としてワーカ 0 がリロードされると、最初にアプリケーションの新しいコピーが初期化されます。次に、他のワーカが、この新しいプリロード済みのアプリケーションが既にある新しいワーカから、フォークされてリロードされます。



### ヒント

段階的な再起動は、Puma クラスタ内の実行中のすべてのワーカを再起動します。これは、最初に古いワーカを終了させて、新しいワーカを起動し、新しいワーカが正常に起動するまで待ってから次のワーカに進みます。これを全てのワーカをに対して行います。マスタプロセスは再起動されません。

この段階的な再起動は、ホットリスタートのように短時間で完了しつつ、クラスタのワーカを順に再起動することによりダウンタイムを最小限に抑えることができます。

もう一つの利点は、新しく追加された `refork` コマンドによるコピーオンライト(COW)の改善です。ワーカ 0 からリフォーク(`refork`)することで、ワーカ 0 以外の全てのワーカをリロードします。

このコマンドは、起動時に完全に初期化できないような大規模や複雑なアプリケーションでのメモリ使用率を改善できる可能性があります。これは、リフォークされたワーカが、すでにリクエストを処理している実行中のワーカとコピーオンライト(COW)メモリを共有できるためです。

また、リフォークは、一定の数のリクエスト(デフォルトは 1000)がワーカ 0 によって処理された場合にも、自動的に 1 度トリガーされます。自動リフォークされるまでのリクエスト数を設定するには、`fork_worker` に正の整数値(例えば、`fork_worker 1000`)を指定するか、もしくは 0 を指定して無効にします。

### 制限事項 :

- クラスタモードは `preload_app` と互換性がありません。
- 新しいワーカを正常にフォークするために、ワーカ 0 はサーバをシャットダウンし、リクエストの処理を停止します。これにより、プロセス間で共有されてオープン中のファイル記述子やその他のグローバルな共有状態がなくなり、新しくフォークされたワーカ間でコピーオンライト(COW)の効率が最大化されます。このため、段階的な再起動/リフォーク中にクラスタの総処理能力が一時的に減少する場合があります。

`fork_worker` および `refork` コマンドについて説明しましたが、ほかにも以下のようなクラスタコマンド(`fork` ワーカ)があります。

- \*workers(count)\*** - 実行するワーカプロセスの数。通常、使用可能な CPU コア数を設定します。環境変数 `WEB_CONCURRENCY` に値が設定されている場合は、それがデフォルトです。それ以外の場合は 0 です。
- before\_fork(&block)** - マスタプロセスがワーカをフォークする前に実行(起動時に 1 回)するコード。プロセスが終了する前に、Puma が関与しないバックグラウンド操作が終了するのを待機する必要がある場合に指定します。



- **on\_worker\_boot(&block)** - アプリを起動する前にプロセスをセットアップするために、ワーカの起動時に実行するコード。
- **on\_worker\_shutdown(&block)** - ワーカがシャットダウンする直前(HTTP リクエストの処理が完了した後)に実行するコード。
- **on\_worker\_fork(&block)** - ワーカが起動する直前にマスタプロセスで実行するコード。ワーカのインデックスが引数として渡されます。
- **after\_worker\_fork(&block)** - ワーカが起動された後にマスタプロセスで実行するコード。ワーカのインデックスが引数として渡されます。
- **on\_refork(&block)** - サーバがリクエストの受け付けを一時的に停止した後、ワーカ 0 が他の全てのワーカをこのプロセスからリフォークする前に実行するコード(リフォークごとに 1 回呼び出されます)。コピーオンライト(COW)の効率を最大化するために追加のガベージコレクションのトリガとして使用できます。また、リモートサーバ(データベース、Redis など)との接続を閉じるためにも使用できます。
- **out\_of\_band(&block)** - ワーカがアイドル状態の時に不定期に実行されるコード。リクエスト処理が終わりワーカにビジー状態のスレッドが存在しなくなった直後に実行されます。このコードが終了するまで、ワーカは新しいリクエストを受け付けません。これは、不定期のガベージコレクションを実行したり、レスポンスの後に実行する非同期タスクをスケジュールする場合に便利です。
- **fork\_worker(after\_request=1000)** - この設定を有効にすると、ワーカはマスタプロセスからではなくワーカ 0 からフォークされます。このオプションは、アプリケーションがフォークする前にプリロードされるため"preload\_app"に似ていますが、段階的な再起動と互換性があります。このオプションで `refork` コマンドも有効になります。
- **nakayoshi\_fork(enabled=true)** - これは少し異なるオプションですが、ワーカをフォークする前に Puma が 4 回 GC(ガベージコレクション)を実行します。起動とフォークの所要時間が長くなります。起動処理にかかる時間の詳細については、ログを参照してください。ほとんどのアプリケーションでは 1 秒以下になると考えられます。このフォーク方法は、笹田耕一氏と Aaron Patterson 氏の研究に基づいており、このオプションはプリロードを有効にしたクラスタモードの Puma のメモリ使用量を削減できる可能性があります。



### 注記

利用可能(Ruby 2.7 以降)な場合、GC.compact も実行されます。

MRI 以外の Ruby では推奨されません。

## 関連項目

- [Ruby エージェントの設定 \(397ページ\)](#)
- [Ruby エージェントのサポート対象テクノロジー \(393ページ\)](#)

## Thin での設定

Ruby エージェントがアプリケーションをタイムアウトさせてしまい、サーバが起動できなくなることがあります。これはサーバの設定によって防ぐことができます。

Thin は軽量の Web サーバで、クラスタをサポートし、タイムアウトと待機時間を設定するオプションを提供しています。Thin では、すべてのオプションを CLI コマンドの引数、または `config.yml` ファイルで設定できます。

## タイムアウトの設定

`wait` オプションは、クラスタ内でサーバを再起動する際の最大待機時間です。

このタイムアウトオプションは、通信が切断されるまでデータ受信を待機する最大秒数です。

## フォーク

Thin はクラスタをサポートしており、異なるポートで複数のサーバインスタンスを実行できます。

利用可能なオプションは次のとおりです。

```
cluster options:
-s, --servers NUM           Number of servers to start
-o, --only NUM              Send command to only one server of the \
cluster
-C, --config FILE          Load options from config file
-O, --onebyone              Restart the cluster one by one (only \
works with restart command)
-w, --wait NUM             Maximum wait time for server to be \
started in seconds (use with -O)
```

クラスタと一緒に実行できる実験的なチューニングオプションもあります。

```
--threaded                  Call the Rack application in threads \
[experimental]
```

## 関連項目

- [Ruby エージェントの設定 \(397ページ\)](#)
- [Ruby エージェントのサポート対象テクノロジー \(393ページ\)](#)

## Unicorn での設定

Unicorn はシングルスレッドで、マルチプロセスで動作します。Unicorn には、トラフィックに基づいて自動的にプロセス数を調整する機能がありません。これは、`unicorrf.conf.rb` か `unicorn.conf.minimal.rb` ファイル、またはスクリプトを使用して設定する必要があります。

- `unicorn.conf.rb` の例：

```
# Define your root directory.
root = "/home/deployer/apps/gifroll/current"

# Define worker directory for Unicorn.
working_directory "/path/to/app/current"

# Define number of worker processes.
# Each forked OS process consumes additional memory.
worker_processes 4

# Define timeout for hanging workers before they are restarted.
timeout 30

# Location of PID file.
pid "/path/to/app/shared/pids/unicorn.pid"

# Define log paths:

# Allow redirecting $stderr to a given path. Unlike doing this from the \
shell,
# this allows the Unicorn process to know the path being written to and \
rotates
# the file if it is used for logging.
stderr_path "#{root}/log/unicorn.log"

# Same as stderr_path, except for $stdout. Not many Rack applications \
write
# to $stdout, but any that do will have their output written here.
stdout_path "#{root}/log/unicorn.log"
```

```
# Loads Rails before forking workers for better worker spawn time.
# Preloading your application reduces the startup time of individual
# Unicorn worker_processes and allows you to manage the external \
connections
# of each individual worker using the before_fork and after_fork calls.
#
# Please check if other external connections work properly with
# Unicorn forking. Many popular gems (dalli memcache client, Redis) will \
have
# compatibility confirmation with Unicorn and the process model.
# Check the gem documentation for more information.
preload_app true

# When enabled, Unicorn will check the client connection by writing the
# beginning of the HTTP headers before calling the application. This will
# prevent calling the application for clients who have disconnected while
# their connection was queued.
check_client_connection false

# Enable a local variable to guard against running a hook (before_fork, \
after_fork)
# multiple times
run_once = true

# For example, use of before_fork and after_fork:
#
# POSIX Signals are a form of interprocess communication, and signal
# events or state changes.
# QUIT: Signals a process to exit, but creates a core dump.
# TERM: Tells a process to terminate, but allows the process
# to clean up after itself.
#
# Unicorn uses the QUIT signal to indicate a graceful shutdown.
# The master process receives it and sends it to all workers, telling \
them to
# shutdown after any in-flight request.
before_fork do |server, worker|
  Signal.trap 'TERM' do
    puts 'Unicorn master intercepting TERM and sending myself QUIT \
instead'
    Process.kill 'QUIT', Process.pid
  end
end

# You may want to execute code in the master process, before the forking
# begins, to deal with operations that causes changes in state.
# You need them to run once:
if run_once
  # do_something_once_here ...
  run_once = false # prevent from firing again
end
end

after_fork do |server, worker|
  Signal.trap 'TERM' do
    puts 'Unicorn worker intercepting TERM and doing nothing. Wait for \
```

```

master to send QUIT'
  end
  # ...
end

# For more information, check the Unicorn Configurator: https://misp-greg.github.io/unicorn/Unicorn/Configurator.html

```

- unicorn.conf.minimal.rb の例 :

```

listen 2007 # by default Unicorn listens on port 8080
worker_processes 2 # this should be >= nr_cpus
pid "/path/to/app/shared/pids/unicorn.pid"
stderr_path "/path/to/app/shared/log/unicorn.log"
stdout_path "/path/to/app/shared/log/unicorn.log"

```

## フォークの設定

Unicorn には、利用可能な CPU コアをより有効に活用するためのマルチプロセスアーキテクチャがあります。起動時に、Unicorn マスタプロセスはアプリケーションコードをロードし、マスタプロセスからアプリケーションコードを継承するワーカを生成します。リクエストはワーカによってのみ処理され、マスタプロセスでは処理されません。オペレーティングシステムのネットワークスタックは、受信したリクエストをキューに入れ、ワーカに配布されます。

Unicorn はユーザのリクエストを切らずに、クラッシュしたワーカを再起動するように設計されています。ワーカがリクエストタイムアウトに達すると、マスタプロセスはワーカを `kill -9` で終了させ、新しいプロセスに置き換えます。ワーカプロセスの数やリクエストのタイムアウトは、設定できます。

設定	説明
<code>worker_processes (nr)</code>	<code>worker_processes</code> (ワーカプロセス)の数を <code>nr</code> に指定します。各ワーカプロセスは、一度に 1 つのクライアントだけを処理します。 <code>SIGTTIN</code> または <code>SIGTTOU</code> のシグナルをマスタプロセスに送信することで、設定ファイルをリロードすることなく、実行時にこの値を増減できます。  シグナルについての詳細は、 <a href="#">☑ Unicorn のサイト</a> を参照ください。
<code>Unicorn::Configurator#after_fork</code>	<code>after_fork</code> (フォーク後)に特定のブロックに対してフックを指定します。
<code>Unicorn::Configurator#before_fork</code>	<code>before_fork</code> (フォーク前)に特定のブロックに対してフックを指定します。
<code>Unicorn::Configurator#preload_app(bool)</code> <code>ObjectEnabling</code>	この設定は、ワーカプロセスをフォークする前にアプリケーションをプリロードします。これは、コピーオンライトに適した GC を使用する際にメモリを節約できますが、ソケットのようなりソースがマスタプロセスによってロード時に開かれて複数の子プロセスで共有される場合、問題が生じる可能性があります。

## タイムアウトの設定

変数	説明	デフォルトの値
<code>timeout 30</code>	ワーカプロセスのタイムアウトを 30 秒に設定します。デフォルトは、60 秒です。タイムアウトの設定により、この制限を超えたワーカを終了させることができます。このタイムアウトは、マスタプロセスによって強制実行され、ワーカプロセスによるスケジューリングの制限の影響を受けません。	60 秒
<code>delay integer</code>	ソケットのバインドの試行を待機する時間を秒単位で指定します。	0.5 秒



## ヒント

Unicorn は、[NGINX と連携する場合に多くの設定があります。](#)

## APM ツールの設定

次の APM ツールは Unicorn をサポートしています。

- [Scout](#) には、Unicorn とインテグレーションするためのクラスがあります。
- [New Relic](#)
- [AppDynamics](#)

## 関連項目

- [Ruby エージェントの設定 \(397ページ\)](#)
- [Ruby エージェントのサポート対象テクノロジー \(393ページ\)](#)

## Ruby エージェントの YAML テンプレート

YAML 設定ファイルを使用して Ruby エージェントを設定する場合には、以下のテンプレートをご利用ください(YAML 設定については、[YAML 設定の説明 \(38ページ\)](#)を参照してください)。

YAML 設定ファイルは、デフォルトの場所に配置します : /etc/contrast/  
contrast\_security.yaml

```
# \  
=====\  
==  
# Use the properties in this YAML file to configure a Contrast agent.  
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html  
# to determine the order of precedence for configuration values.  
# \  
=====\  
==  
  
# Use this setting if you want to temporarily disable a Contrast agent.  
# Set to `true` to enable the agent; set to `false` to disable the agent.  
# enable: true  
  
# \  
=====\  
==  
# api  
# Use the properties in this section to connect the agent to the Contrast \  
UI.  
# \  
=====\  
==  
api:  
  
# ***** REQUIRED *****  
# Set the URL for the Contrast UI.  
url: https://app.contrastsecurity.com/Contrast
```

```

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Certificate
# PEM file for communication with the Contrast UI.
# cert_file: NEEDS_TO_BE_SET

# Set the absolute or relative path to the Key PEM
# file for communication with the Contrast UI.
# key_file: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid contrast.proxy.host
# and contrast.proxy.port will enable the proxy.
# enable: NEEDS_TO_BE_SET

```

```
# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
#
# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
#
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Override the name of the process the agents uses in logs.
# progname: Contrast Agent

# Set to `true` for the agent to tag
# logs with `!AM!` for the metrics tool.
# metrics: true

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
```

```
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19

# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING
```



```
# \  
=====
```

```
# agent.heap_dump  
# The following properties are used to trigger heap dumps from within  
# the agent to snapshot the behavior of instrumented applications.  
# \  
=====
```

```
# heap_dump:  
  
# Set to `true` for the agent to automatically  
# take heap dumps of the instrumented application.  
# enable: false  
  
# Set the location to which to save the heap dump files. If relative,  
# the path is determined based on the process' working directory.  
# path: contrast_heap_dumps  
  
# Set the amount of time to wait, in milliseconds,  
# after agent startup to begin taking heap dumps.  
# delay_ms: 10_000  
  
# Set the amount of time to wait, in milliseconds, between each heap \  
dump.  
# window_ms: 10_000  
  
# Set the number of heap dumps to take before disabling this feature.  
# count: 5  
  
# Set to `true` for the agent to trigger garbage collection before  
# taking a heap dump to remove temporary objects from the dump.  
# clean: false  
  
# \  
=====
```

```
# agent.ruby  
# The following properties apply to any Ruby agent-wide configurations.  
# \  
=====
```

```
# ruby:  
  
# Allow the agent to track frozen Objects returned by  
# source methods. This configuration is on by default.  
# track_frozen_sources: NEEDS_TO_BE_SET  
  
# Allow the agent to track propagation through interpolated  
# Strings. This configuration is on by default.  
# interpolate: NEEDS_TO_BE_SET  
  
# Set a comma-separated string of rake tasks  
# in which to disable agent operation.  
# disabled_agent_rake_tasks: \  
about,assets:clean,assets:clobber,assets:environment,assets:precompile,asset  
s:precompile:all,db:create,db:drop,db:migrate:status,db:rollback,db:schema:c  
ache:clear,db:schema:cache:dump,db:schema:dump,db:schema:load,db:seed,db:set
```

```

up,db:structure:dump,db:version,doc:app,log:clear,middleware,notes,notes:custom,rails:template,rails:update,routes,secret,spec,spec:features,spec:requests,spec:controllers,spec:helpers,spec:models,spec:views,spec:routing,spec:rcov,stats,test,test:all,test:all:db,test:recent,test:single,test:uncommitted,time:zones:all,tmp:clear,tmp:create,webpacker:compile

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Value options are `ALL`, `SOME`, or `NONE`.
# stacktraces: ALL

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====

```

```
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
# protect.rules
# Use the following properties to set simple rule configurations.
# \
=====
# rules:
```

```
# Define a list of Protect rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
# protect.rules.bot-blocker
# Use the following selection to configure if the
# agent blocks bots. Set to `true` to enable blocking.
# \
=====
# bot-blocker:

# Set to `true` for the agent to block known bots.
# enable: false

# \
=====
# protect.rules.sql-injection
# Use the following settings to configure the sql-injection rule.
# \
=====
# sql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.cmd-injection
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
```

```

=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are

```

```
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
```

```

# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==

```

```
# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true
```

```
# \
```

```
=====
==
```

```
# api
```

```
# Use the properties in this section to connect the agent to the Contrast \
UI.
```

```
# \
```

```
=====
==
```

```
api:
```

```
# ***** REQUIRED *****
```

```
# Set the URL for the Contrast UI.
```

```
url: https://app.contrastsecurity.com/Contrast
```

```
# ***** REQUIRED *****
```

```
# Set the API key needed to communicate with the Contrast UI.
```

```
api_key: NEEDS_TO_BE_SET
```

```
# ***** REQUIRED *****
```

```
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
```

```
service_key: NEEDS_TO_BE_SET
```

```
# ***** REQUIRED *****
```

```
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
```

```
user_name: NEEDS_TO_BE_SET
```

```
# \
```

```
=====
```

```
# api.certificate
```

```
# Use the following properties for communication
# with the Contrast UI using certificates.
```

```
# \
```

```
=====
```

```
# certificate:
```

```
# If set to `false`, the agent will ignore the
# certificate configuration in this section.
```

```
# enable: true
```

```
# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
```

```
# ca_file: NEEDS_TO_BE_SET
```

```
# Set the absolute or relative path to the Certificate
# PEM file for communication with the Contrast UI.
```

```
# cert_file: NEEDS_TO_BE_SET
```



```

# Set the absolute or relative path to the Key PEM
# file for communication with the Contrast UI.
# key_file: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate with
# the Contrast web interface over a proxy. Set value to
# `false` if you don't want to use the proxy. If no value is
# indicated, the presence of a valid contrast.proxy.host
# and contrast.proxy.port will enable the proxy.
# enable: NEEDS_TO_BE_SET

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
#
# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
#

```

```
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Override the name of the process the agents uses in logs.
# progname: Contrast Agent

# Set to `true` for the agent to tag
# logs with `!AM!` for the metrics tool.
# metrics: true

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# \
=====
# agent.security_logger.syslog
# Define the following properties to set Syslog values. If the \
properties
# are not defined, the agent uses the Syslog values from the Contrast \
UI.
# \
=====
# syslog:

# Set to `true` to enable Syslog logging.
# enable: NEEDS_TO_BE_SET

# Set the IP address of the Syslog server
# to which the agent should send messages.
# ip: NEEDS_TO_BE_SET

# Set the port of the Syslog server to
# which the agent should send messages.
# port: NEEDS_TO_BE_SET

# Set the facility code of the messages the agent sends to Syslog.
# facility: 19
```

```
# Set the log level of Exploited attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_exploited: ALERT

# Set the log level of Blocked attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked: NOTICE

# Set the log level of Blocked At Perimeter
# attacks. Value options are `ALERT`, `CRITICAL`,
# `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_blocked_perimeter: NOTICE

# Set the log level of Probed attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_probed: WARNING

# Set the log level of Suspicious attacks. Value options are `ALERT`,
# `CRITICAL`, `ERROR`, `WARNING`, `NOTICE`, `INFO`, and `DEBUG`.
# severity_suspicious: WARNING

# \
=====
# agent.heap_dump
# The following properties are used to trigger heap dumps from within
# the agent to snapshot the behavior of instrumented applications.
# \
=====
# heap_dump:

# Set to `true` for the agent to automatically
# take heap dumps of the instrumented application.
# enable: false

# Set the location to which to save the heap dump files. If relative,
# the path is determined based on the process' working directory.
# path: contrast_heap_dumps

# Set the amount of time to wait, in milliseconds,
# after agent startup to begin taking heap dumps.
# delay_ms: 10_000

# Set the amount of time to wait, in milliseconds, between each heap \
dump.
# window_ms: 10_000

# Set the number of heap dumps to take before disabling this feature.
# count: 5

# Set to `true` for the agent to trigger garbage collection before
# taking a heap dump to remove temporary objects from the dump.
# clean: false

# \
=====
```

```
# agent.ruby
# The following properties apply to any Ruby agent-wide configurations.
# \
=====
# ruby:

# Allow the agent to track frozen Objects returned by
# source methods. This configuration is on by default.
# track_frozen_sources: NEEDS_TO_BE_SET

# Allow the agent to track propagation through interpolated
# Strings. This configuration is on by default.
# interpolate: NEEDS_TO_BE_SET

# Set a comma-separated string of rake tasks
# in which to disable agent operation.
# disabled_agent_rake_tasks: \
about,assets:clean,assets:clobber,assets:environment,assets:precompile,asset
s:precompile:all,db:create,db:drop,db:migrate:status,db:rollback,db:schema:c
ache:clear,db:schema:cache:dump,db:schema:dump,db:schema:load,db:seed,db:set
up,db:structure:dump,db:version,doc:app,log:clear,middleware,notes,notes:cus
tom,rails:template,rails:update,routes,secret,spec,spec:features,spec:reques
ts,spec:controllers,spec:helpers,spec:models,spec:views,spec:routing,spec:rc
ov,stats,test,test:all,test:all:db,test:recent,test:single,test:uncommitted,
time:zones:all,tmp:clear,tmp:create,webpacker:compile

# \
=====
==
# inventory
# Use the properties in this section to override the inventory features.
# \
=====
==
# inventory:

# Set to `false` to disable inventory features in the agent.
# enable: true

# Apply a list of labels to libraries. Labels
# must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:
```

```
# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# Value options are `ALL`, `SOME`, or `NONE`.
# stacktraces: ALL

# \
=====
# assess.sampling
# Use the following properties to control sampling in the agent.
# \
=====
# sampling:

# Set to `true` to enable sampling.
# enable: false

# This property indicates the number of requests
# to analyze in each window before sampling begins.
# baseline: 5

# This property indicates that every *nth*
# request after the baseline is analyzed.
# request_frequency: 10

# This property indicates the duration for which a sample set is valid.
# window_ms: 180_000

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
```

```
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====

# protect.rules
# Use the following properties to set simple rule configurations.
# \
=====

# rules:

# Define a list of Protect rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
# disabled_rules: NEEDS_TO_BE_SET

# \
=====

# protect.rules.bot-blocker
# Use the following selection to configure if the
# agent blocks bots. Set to `true` to enable blocking.
# \
=====

# bot-blocker:

# Set to `true` for the agent to block known bots.
# enable: false

# \
=====

# protect.rules.sql-injection
# Use the following settings to configure the sql-injection rule.
# \
=====

# sql-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or off.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====

# protect.rules.cmd-injection
```

```
# Use the following properties to configure
# how the command injection rule works.
# \
=====
# cmd-injection:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.path-traversal
# Use the following properties to configure
# how the path traversal rule works.
# \
=====
# path-traversal:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.method-tampering
# Use the following properties to configure
# how the method tampering rule works.
# \
=====
# method-tampering:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.reflected-xss
# Use the following properties to configure how
# the reflected cross-site scripting rule works.
# \
=====
```

```
# reflected-xss:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
# protect.rules.xxe
# Use the following properties to configure
# how the XML external entity works.
# \
=====
# xxe:

# Set the mode of the rule. Value options are
# `monitor`, `block`, `block_at_perimeter`, or `off`.
#
# Note - If a setting says, "if blocking is enabled",
# the setting can be `block` or `block_at_perimeter`.
#
# mode: off

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
```



```
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET
```

```
# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET
```

## Ruby のテレメトリ

Ruby エージェントは、テレメトリを使用して、使用状況に関するデータを収集します。テレメトリは、エージェントを組み込んだアプリケーションでエージェントのセンサーが最初にロードされた時に収集され、その後も定期的に(数時間ごと)に収集されます。

弊社では、お客様のプライバシーは非常に大切 (828ページ) であると考えています。このテレメトリ機能は、アプリケーションのデータを収集するものではありません。データは匿名化されてから、Contrast に安全に送信されます。そして、集約されたデータは暗号化されて保存され、アクセスが制限されます。収集されたデータは、全て 1 年後に削除されます。

テレメトリ機能で収集されるのは、以下のデータです。

エージェントのバージョン	データ
Ruby 4.13	エージェントのバージョン
	オペレーティングシステムとバージョン
	Ruby のバージョン
	アプリケーションのフレームワークとバージョン
	Web サーバとバージョン
	Contrast インスタンスが SaaS 版かオンプレミス版であるか

テレメトリ機能を停止するには、`CONTRAST_AGENT_TELEMETRY_OPTOUT` という環境変数に 1 または true を設定してください。

テレメトリのデータは、`telemetry.ruby.contrastsecurity.com` に安全に送信されます。ネットワークレベルで通信をブロックすることで、テレメトリ機能を停止することもできます。

## Go エージェント

Go エージェントは、ライブラリや脆弱性のレポートのために Go アプリケーションに組み込まれるソースコードリライタ(rewriter)です。これにより、アプリケーションを構成するソースコードとライブラリを実行時に把握することができます。



### 注記

ソースコードリライタとして、アプリケーションに Go エージェントをインストールするには、アプリケーションのビルド環境へのアクセスが必要になります。

Go エージェントは現在、Contrast Assess と Contrast SCA のみに対応しています。

次のステップ：

- [Go エージェントをインストールする \(451ページ\)](#)
- [Go エージェントのシステム要件を確認する \(451ページ\)](#)
- [Go エージェントのサポート対象テクノロジーを確認する \(451ページ\)](#)

## Go エージェントのサポート対象テクノロジー

Go エージェントでは、以下のテクノロジーをサポートしています。

テクノロジー	サポート対象バージョン	備考
言語のバージョン	<ul style="list-style-type: none"> <li>• 1.19.x</li> <li>• 1.20.x</li> </ul>	<p>Contrast は、<a href="#">Go リリースのサポートポリシー</a>に従います。このポリシーは、直近にリリースされた 2 つのメジャーバージョンをサポートします。Go 言語のサポート対象バージョンは、新しいメジャーバージョンがリリースされると変わります。アプリケーションの依存関係は、go.mod ファイルで指定する必要があります。</p> <p><b>サポート対象外：</b></p> <ul style="list-style-type: none"> <li>• 1.18.x：最後にサポート対象となったエージェントは 4.2.0</li> <li>• 1.17.x：最後にサポート対象となったエージェントは 3.6.0</li> <li>• 1.16.x：最後にサポート対象となったエージェントは 3.6.0</li> <li>• 1.15.x：最後にサポート対象となったエージェントは 1.12.0</li> </ul>
オペレーティングシステム	<ul style="list-style-type: none"> <li>• Linux</li> <li>• Darwin</li> </ul>	
アプリケーションフレームワーク	<ul style="list-style-type: none"> <li>• Go 標準ライブラリ</li> <li>• Gin 1.x</li> <li>• Chi 5.x</li> </ul>	他のフレームワークでは、ランタイムで特定の機能が制限される可能性があります。
プロセッサのアーキテクチャ	<ul style="list-style-type: none"> <li>• AMD64</li> <li>• ARM64</li> </ul>	Go エージェントのリライタと生成されたランタイムは、他のアーキテクチャでも動作する可能性はありますが、正式にはサポートされていません。
データベースのサポート	Go 標準ライブラリ	一部のサードパーティのデータベースライブラリは互換性があるかもしれませんが、サポート対象ではありません。
依存関係の管理方法	Go mod	エージェントは依存関係システムとしてモジュールのみをサポートします。詳細は、 <a href="#">Using Go modules</a> (Go モジュールの使用)を参照。アプリケーションは、go mod init を実行することで、モジュールを使用して初期化できます。
HTTP ルーター	julienschmidt/ httprouter	
HTTP 以外のソース	gRPC 1.3.0 以降	<a href="https://google.golang.org/grpc">google.golang.org/grpc</a>
その他のパッケージ	go-swagger 2.0	<a href="https://github.com/go-swagger/go-swagger">https://github.com/go-swagger/go-swagger</a> 詳細は、 <a href="#">Swagger 2.0 のウェブサイト</a> をご覧ください。

## Go エージェントのシステム要件

Go エージェントをインストールする前に、以下のシステム要件を満たす必要があります。

要件	バージョン	備考
ビルドシステム	<ul style="list-style-type: none"> <li>• 64 ビット OS X</li> <li>• 64 ビット Linux</li> </ul>	<p><b>必須：</b> Go のビルドツールバージョン 1.16 以降。</p> <p>これらのオペレーティングシステムの AMD64 および ARM64 アーキテクチャがサポートされます。</p>
ランタイムシステム	<ul style="list-style-type: none"> <li>• 64 ビット OS X</li> <li>• 64 ビット Linux</li> </ul>	これらのオペレーティングシステムの AMD64 および ARM64 アーキテクチャがサポートされます。

## Go エージェントのインストール

アプリケーションにエージェントを組み込むために、contrast-go を使用して実行ファイルをビルドする必要があります。Go エージェントの基本的なインストールは、主に実行可能ファイルを作成することと起動することの 2 つに分かれます。インストールの概要は、次のようになります。

1. 以下をダウンロードして、適切なパスに配置します。

- Go エージェント
  - `contrast_security.yaml`
- 2. 適切な権限を設定します。
- 3. Go アプリケーションをビルドします。go コマンドを `contrast-go` に置き換えて、Go エージェントを含めた最終的なアプリケーション成果物を生成します。
- 4. アプリケーションを起動します。
- 5. アプリケーションの疎通やテストを行います。
- 6. Contrast でアプリケーションが認識されていることを確認します。



### ヒント

`contrast-go` のコマンドライン引数で利用可能なフラグの一覧を表示するには、`contrast-go -h` を入力します。

具体的なインストール手順については、ご利用の環境に合わせて以下より選択してください。

- [contrast-go-installer でインストール \(452ページ\)](#)
- [RPM\(.rpm\)から Go エージェントをインストール \(455ページ\)](#)
- [Debian\(.deb\)から Go エージェントをインストール \(455ページ\)](#)
- [直接ダウンロードしてインストール \(456ページ\)](#)



### 注記

3.0.0 より前のバージョンでは、Go エージェントには Contrast サービスが必要でした。[Go エージェントのインストール\(旧手順\) \(453ページ\)](#)を参照してください。

## contrast-go-installer で Go エージェントをインストール

`contrast-go-installer` は、Go エージェントのインストールを簡素化します。



### 注記

`contrast-go-installer` は、オープンソースプロジェクトです。コードは[こちら](#)で確認でき、開発に貢献することができます。

## 手順

1. 次のコマンドで、`contrast-go-installer` を実行します。

```
go run github.com/contrast-security-oss/contrast-go-installer@latest \
latest
```

2. 次のコマンドで、アプリケーションをビルドします。

```
contrast-go build -o output-name-of-application
```

- Go エージェントの [YAML テンプレート \(457ページ\)](#) や環境変数を使用して、Go エージェントを設定 ([456ページ](#)) します。
- 手順 2 で生成された実行可能ファイルを使用して、アプリケーションを実行します。
- アプリケーションの疎通やテストを行います。
- Contrast Web インターフェイスで、アプリケーション一覧にアプリケーションがあることを確認してください。

## Go エージェントのインストール(旧手順)



### 重要

[Contrast サービスを使用しない Go エージェントをインストール \(451ページ\)](#) することで、エージェントが Contrast に直接報告するように設定できます。

Go エージェントを使用する場合、2 つのアーティファクトが必要になります。アプリケーションにエージェントを組み込むために、`contrast-go` を使用して実行ファイルをビルドする必要があります。そして、実行時に Contrast サーバと通信するためにアプリケーションには `contrast-service` が必要です。Go エージェントの基本的なインストールは、主に実行可能ファイルを作成することと起動することの 2 つに分かれます。インストールの概要は、次のようになります。

- 以下をダウンロードして、適切なパスに配置します。
  - Go エージェント
  - [Contrast サービス \(472ページ\)](#)
  - `contrast_security.yaml`  
yaml ファイルに `bypass:false` が設定されていることを確認します。

```
agent:
  service:
    bypass: false
```

- 適切な権限を設定します。
- Go アプリケーションをビルドします。`go` コマンドを `contrast-go` に置き換えて、Go エージェントを含めた最終的なアプリケーション成果物を生成します。
- アプリケーションを起動します。
- アプリケーションの疎通やテストを行います。
- Contrast でアプリケーションが認識されていることを確認します。



### ヒント

`contrast-go` の [コマンドライン引数](#) で利用可能なフラグの一覧を表示するには、`contrast-go -h` を入力します。

具体的なインストール手順については、ご利用の環境に合わせて以下より選択してください。

- [RPM\(.rpm\)から Go エージェントをインストール \(455ページ\)](#)
- [Debian\(.deb\)から Go エージェントをインストール \(455ページ\)](#)
- [直接ダウンロードしてインストール \(456ページ\)](#)

## コンテナを使用して Go エージェントをインストール

Go エージェントには、2つの主要なコンポーネントがあります。contrast-go(ビルドツール)とエージェント本体(contrast-go によってビルド時にアプリケーションに組み込まれるパッケージ)です。

contrast-go は、curl コマンドを使用するか、リポジトリまたはパッケージマネージャからダウンロードします。また、エージェントが Contrast と接続するように設定する必要があります。YAML 設定ファイルまたは環境変数を使用して設定します。YAML 設定ファイルは Contrast Web インターフェイスからダウンロードすることもできますし、テンプレートから自分で作成することもできます。

Contrast の Go エージェントをコンテナにインストールする場合は、コンテナイメージファイルで次の手順を実行するだけです。



### ヒント

Go エージェントを使用するアプリケーションを別のコンテナでサンプルとして試してみたい場合は、[Go Test Bench オープンソースプロジェクト](#)をご利用ください。

### 開始する前に

本項では、Docker を例として、コンテナ化されたアプリケーションに Contrast Go エージェントをインストールするための一般的な手順について説明します。

コンテナや関連ソフトウェアの仕組みを基本的に理解している必要があります。実際の手順は、ご利用の環境に合わせて調整してください。

### contrast-go でアプリケーションをビルド

手順に従って Go エージェントをインストールします。

1. Go エージェントをダウンロードします。以下の curl コマンドを使用するか、[Debian \(455ページ\)](#)でインストールしてください。

```
RUN curl -L https://pkg.contrastsecurity.com/go-agent-release/latest/linux-amd64/contrast-go > contrast-go
```

2. 適切な権限を設定してください。

```
RUN chmod u+x contrast-go
```

3. 通常の go build コマンドを contrast-go build に置き換えます。これにより、Contrast が組み込まれた実行ファイルが得られます。

```
RUN ./contrast-go build -o instrumented-app
```



### 注記

-o instrumented-app には、以降の手順で使用する instrumented-app(検査対象のアプリケーション名)を指定します。名前を変更するか、もしくは、-o オプションを完全に省略するとパッケージに基づいてデフォルト名が生成されます。

### エージェントを組み込んだアプリケーションを実行

- アプリケーションを実行します。

```
CMD ./instrumented-app
```

## 関連項目

- [Kubernetes と Contrast エージェント](#)
- [AWS Fargate と Contrast エージェント](#)

## Debian で Go エージェントをインストール

Go エージェントをインストールするには :

1. <https://pkg.contrastsecurity.com> からエージェントのファイルをダウンロードします。以下のコマンドで、Contrast のパッケージリポジトリをシステムに登録します。

```
curl \
  https://pkg.contrastsecurity.com/api/gpg/key/public | sudo apt-key \
  add -

echo "deb https://pkg.contrastsecurity.com/debian-public/ $(sed -rne 's/^VERSION_CODENAME=(.*)$/\1/p' /etc/*ease) contrast" \
  | sudo tee /etc/apt/sources.list.d/contrast.list

echo "deb https://pkg.contrastsecurity.com/debian-public/ all contrast" \
  | sudo tee -a /etc/apt/sources.list.d/contrast.list
```

2. 設定をしたら、以下のコマンドを実行してエージェントをインストールします。

```
sudo apt-get update && sudo apt-get install contrast-go
```

3. 依存関係を表すために必要な go.mod ファイルがアプリケーションにあることを確認してください。アプリケーションのソースディレクトリで、以下のコマンドを実行します。

```
go mod init
```

4. アプリケーションをビルドします。

```
contrast-go build -o output-name-of-application
```

5. [Go エージェントの YAML テンプレート \(457ページ\)](#)や環境変数を使用して、[Go エージェントを設定 \(456ページ\)](#)します。
6. 前述の手順でビルドした実行可能ファイルを使用して、アプリケーションを起動します。
7. アプリケーションの疎通やテストを行います。
8. Contrast でアプリケーションが認識されていることを確認します。

## RPM(Red Hat Package Manager)で Go エージェントをインストール

Go エージェントをインストールするには :

1. <https://pkg.contrastsecurity.com> からエージェントのファイルをダウンロードします。以下のスクリプトをシェルで実行し、お使いの RPM ベースのシステムに Contrast のパッケージリポジトリを設定します。sudo の権限が必要になる場合があります。

```
tee /etc/yum.repos.d/contrast.repo <<- "EOF"
[contrast]
name=Contrast centos-$releasever repo
baseurl=https://pkg.contrastsecurity.com/rpm-public/centos-$releasever/
gpgcheck=0
enabled=1
EOF
```

2. 設定をしたら、以下のコマンドを実行してエージェントをインストールします。

```
sudo yum install contrast-go
```

3. 依存関係を表すために必要な go.mod ファイルがアプリケーションにあることを確認してください。アプリケーションのソースディレクトリで、以下のコマンドを実行します。

```
go mod init
```

4. アプリケーションをビルドします。

```
contrast-go build -o output-name-of-application
```

5. [Go エージェントの YAML テンプレート \(457ページ\)](#)や環境変数を使用して、[Go エージェントを設定 \(456ページ\)](#)します。
6. 前述の手順でビルドした実行可能ファイルを使用して、アプリケーションを起動します。
7. アプリケーションの疎通やテストを行います。
8. Contrast でアプリケーションが認識されていることを確認します。

## Go エージェントを直接ダウンロードしてインストール

Go エージェントをインストールするには：

1. <https://pkg.contrastsecurity.com> からエージェントをダウンロードします。  
contrast-go 実行可能ファイルは、Mac および Linux オペレーティングシステム用に直接ダウンロードできます。利用可能なバージョンは、[go-agent-release](#) のサイトで確認できます。  
<version>の箇所を利用するバージョン番号に置き換えます。または、最新バージョンを利用する場合は latest に置き換えます。

### • Mac の場合：

```
wget https://pkg.contrastsecurity.com/go-agent-release/<version>/darwin-amd64/contrast-go
```

または

```
curl -L https://pkg.contrastsecurity.com/go-agent-release/<version>/darwin-amd64/contrast-go > contrast-go
```

### • Linux の場合：

```
wget https://pkg.contrastsecurity.com/go-agent-release/<version>/linux-amd64/contrast-go
```

または

```
curl -L https://pkg.contrastsecurity.com/go-agent-release/<version>/linux-amd64/contrast-go > contrast-go
```

2. ダウンロードしたら、エージェントが実行可能であることを確認します。例：

```
chmod u+x contrast-go
```

3. 依存関係を表すために必要な go.mod ファイルがアプリケーションにあることを確認してください。アプリケーションのソースディレクトリで、以下のコマンドを実行します。

```
go mod init
```

4. アプリケーションをビルドします。

```
./contrast-go build -o output-name-of-application
```

5. [Go エージェントの YAML テンプレート \(457ページ\)](#)や環境変数を使用して、[Go エージェントを設定 \(456ページ\)](#)します。
6. 前述の手順でビルドした実行可能ファイルを使用して、アプリケーションを起動します。
7. アプリケーションの疎通やテストを行います。
8. Contrast でアプリケーションが認識されていることを確認します。

## Go エージェントの設定

全てのエージェントには[基本の設定 \(35ページ\)](#)があります。設定値には[優先順位 \(36ページ\)](#)があり、ここでは他に有効な設定ファイルの場所など、エージェントを設定する他の方法についても説明しております。



Go エージェントを設定する方法は、いくつかあります。

- [YAML 設定ファイル\(詳細はこちら\) \(38ページ\)](#) : アプリケーションを実行するには YAML 設定ファイルが必要です。Go エージェントの実行には必要ありません。独自に YAML 設定ファイルを作成するか、Go エージェント用に有効な全てのプロパティがある[テンプレート \(457ページ\)](#)を利用することもできます。

アプリケーションを実行するディレクトリ(" . ")に設定ファイルを置きます。[エージェントキーを確認 \(37ページ\)](#)して、設定ファイルにエージェントキーの値を指定します。

```
api:
  url:
  api_key:
  service_key:
  user_name:
```

- [環境変数 \(56ページ\)](#) : ビルドを設定するために使用できます。
- コマンドラインの引数を使用して、エージェントのプロパティを指定することもできます。



### ヒント

[Contrast エージェント設定エディタ \(39ページ\)](#)を使用すると、YAML 設定ファイルの作成やアップロード、YAML の検証、推奨される設定値の表示などができます。

## Go エージェントの YAML テンプレート

YAML 設定ファイルを使用して Go エージェントを設定する場合には、以下のテンプレートをご利用ください(YAML 設定については、[こちらの説明 \(38ページ\)](#)を参照してください)。

```
# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==

# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

# \
=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:
```

```
# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

# Set value to `true` for the agent to communicate
# with the Contrast web interface over a proxy. Set
# value to `false` if you don't want to use the proxy.
# enable: NEEDS_TO_BE_SET

# Set the proxy host. It must be set with port and scheme.
# host: localhost

# Set the proxy port. It must be set with host and scheme.
# port: 1234
```

```
# Set the proxy scheme (e.g., `http` or
# `https`). It must be set with host and port.
# scheme: http

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# Set the proxy user.
# user: NEEDS_TO_BE_SET

# Set the proxy password.
# pass: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
#
# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
#
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Set to `true` to redirect all logs to
# `stdout` instead of the file system.
# stdout: false

# \
```

```

=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# \
=====
# agent.service
# The following properties are used by the Contrast Service.
# \
=====
# service:

# Set to `false` to disallow the service to be started, and
# effectively disable the agent, if read by the service. If the
# agent reads this property, it disallows service auto-start.
# enable: true

# Set to `true` to enable listening for gRPC connections.
# The `socket`, `host` and `port` fields will be used for
# configuring the gRPC server in place of the legacy RPC server.
# grpc: false

# If this property is defined, the service is
# listening on a Unix socket at the defined path.
# socket: /tmp/service.sock

# ***** REQUIRED *****
# Set the the hostname or IP address of the Contrast
# service to which the Contrast agent should report.
host: localhost

# ***** REQUIRED *****
# Set the the port of the Contrast service
# to which the Contrast agent should report.
port: 30555

# ***** REQUIRED *****
# Timeout (in milliseconds) that the agent-init
# should wait for the contrast-service
timeout_ms: 30000

# Set to `true` to enable direct communication with Teamserver.
# bypass: false

```

```
# \  
=====
```

```
# agent.service.logger  
# The following properties are used by the logger in the  
# Contrast service. If the properties are not defined, the  
# service uses the logging values from the Contrast UI.  
# \  
=====
```

```
# logger:  
  
# Set the location to which the Contrast service saves log output.  
# If no log file exists at this location, the service creates one.  
#  
# Example - `/opt/Contrast/contrast_service.log` will  
# create a log in the `/opt/Contrast` directory.  
#  
# path: ./contrast_service.log  
  
# Set the the log output level. Options are `OFF`, `FATAL`,  
# `ERROR`, `WARN`, `INFO`, `DEBUG`, `TRACE`, and `ALL`.  
# level: ERROR  
  
# Override the name of the process used in logs.  
# progame: Contrast Service  
  
# Set to `true` to send log output to `stdout`.  
# stdout: false  
  
# \  
=====
```

```
# agent.go  
# The following properties apply to any Go agent-wide configurations.  
# \  
=====
```

```
# go:  
  
# Enable opt-in Go agent features.  
# preview: NEEDS_TO_BE_SET  
  
# Enable Go agent self-profiling features.  
# profile: NEEDS_TO_BE_SET  
  
# \  
=====
```

```
# inventory  
# Use the properties in this section to override the inventory features.  
# \  
=====
```

```
# inventory:  
  
# Set to `false` to disable inventory features in the agent.  
# enable: true
```

```

# Set to `false` to disable library analysis.
# analyze_libraries: true

# \
=====
==
# assess
# Use the properties in this section to control Assess.
# \
=====
==
# assess:

# Include this property to determine if the Assess
# feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# Apply a list of labels to vulnerabilities and preflight
# messages. Labels must be formatted as a comma-delimited list.
# Example - `label1, label2, label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
# assess.rules
# Use the following properties to control simple rule configurations.
# \
=====
# rules:

# Define a list of Assess rules to disable in the agent.
# The rules must be formatted as a comma-delimited list.
#
# Example - Set `reflected-xss,sql-injection` to disable
# the reflected-xss rule and the sql-injection rule.
#
# disabled_rules: NEEDS_TO_BE_SET

# \
=====
==
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

```

```
# \  
=====\  
==  
# application  
# Use the properties in this section for  
# the application(s) hosting this agent.  
# \  
=====\  
==  
# application:  
  
# Override the reported application name.  
#  
# Note - On Java systems where multiple, distinct applications may be  
# served by a single process, this configuration causes the agent to \  
report  
# all discovered applications as one application with the given name.  
#  
# name: NEEDS_TO_BE_SET  
  
# Override the reported application path.  
# path: NEEDS_TO_BE_SET  
  
# Add the name of the application group with which this  
# application should be associated in the Contrast UI.  
# group: NEEDS_TO_BE_SET  
  
# Add the application code this application should use in the Contrast UI.  
# code: NEEDS_TO_BE_SET  
  
# Override the reported application version.  
# version: NEEDS_TO_BE_SET  
  
# Apply labels to an application. Labels must  
# be formatted as a comma-delimited list.  
# Example - `label1,label2,label3`  
#  
# tags: NEEDS_TO_BE_SET  
  
# Define a set of `key=value` pairs (which conforms to RFC 2253) for  
# specifying user-defined metadata associated with the application. The  
# set must be formatted as a comma-delimited list of `key=value` pairs.  
# Example - `business-unit=accounting, office=Baltimore`  
#  
# metadata: NEEDS_TO_BE_SET  
  
# Provide the ID of a session which already exists in the Contrast  
# UI. Vulnerabilities discovered by the agent are associated with  
# this session. If an invalid ID is supplied, the agent will be  
# disabled. This option and `application.session_metadata` are  
# mutually exclusive; if both are set, the agent will be disabled.  
# session_id: NEEDS_TO_BE_SET  
  
# Provide metadata which is used to create a new session ID in the
```

```

# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# \
=====
==
# Use the properties in this YAML file to configure a Contrast agent.
# Go to https://docs.contrastsecurity.com/en/order-of-precedence.html
# to determine the order of precedence for configuration values.
# \
=====
==

# Use this setting if you want to temporarily disable a Contrast agent.
# Set to `true` to enable the agent; set to `false` to disable the agent.
# enable: true

```



```

# \
=====
==
# api
# Use the properties in this section to connect the agent to the Contrast \
UI.
# \
=====
==
api:

# ***** REQUIRED *****
# Set the URL for the Contrast UI.
url: https://app.contrastsecurity.com/Contrast

# ***** REQUIRED *****
# Set the API key needed to communicate with the Contrast UI.
api_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the service key needed to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
service_key: NEEDS_TO_BE_SET

# ***** REQUIRED *****
# Set the user name used to communicate with the Contrast
# UI. It is used to calculate the Authorization header.
user_name: NEEDS_TO_BE_SET

# \
=====
# api.certificate
# Use the following properties for communication
# with the Contrast UI using certificates.
# \
=====
# certificate:

# If set to `false`, the agent will ignore the
# certificate configuration in this section.
# enable: true

# Set the absolute or relative path to a CA for communication
# with the Contrast UI using a self-signed certificate.
# ca_file: NEEDS_TO_BE_SET

# \
=====
# api.proxy
# Use the following properties for communication
# with the Contrast UI over a proxy.
# \
=====
# proxy:

```

```

# Set value to `true` for the agent to communicate
# with the Contrast web interface over a proxy. Set
# value to `false` if you don't want to use the proxy.
# enable: NEEDS_TO_BE_SET

# Set the proxy host. It must be set with port and scheme.
# host: localhost

# Set the proxy port. It must be set with host and scheme.
# port: 1234

# Set the proxy scheme (e.g., `http` or
# `https`). It must be set with host and port.
# scheme: http

# Set the URL for your Proxy Server. The URL form is `scheme://
host:port`.
# url: NEEDS_TO_BE_SET

# Set the proxy user.
# user: NEEDS_TO_BE_SET

# Set the proxy password.
# pass: NEEDS_TO_BE_SET

# \
=====
==
# agent
# Use the properties in this section to control the way and frequency
# with which the agent communicates to logs and the Contrast UI.
# \
=====
==
# agent:

# \
=====
# agent.logger
# Define the following properties to set logging values.
# If the following properties are not defined, the
# agent uses the logging values from the Contrast UI.
# \
=====
# logger:

# Enable diagnostic logging by setting a path to a log file.
# While diagnostic logging hurts performance, it generates
# useful information for debugging Contrast. The value set here
# is the location to which the agent saves log output. If no
# log file exists at this location, the agent creates a file.
#
# Example - `/opt/Contrast/contrast.log` creates a log in the
# `/opt/Contrast` directory, and rotates it automatically as needed.
#

```

```
# path: ./contrast_agent.log

# Set the the log output level. Valid options are
# `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: INFO

# Set to `true` to redirect all logs to
# `stdout` instead of the file system.
# stdout: false

# \
=====
# agent.security_logger
# Define the following properties to set security
# logging values. If not defined, the agent uses the
# security logging (CEF) values from the Contrast UI.
# \
=====
# security_logger:

# Set the file to which the agent logs security events.
# path: /.contrast/security.log

# Set the log level for security logging. Valid options
# are `ERROR`, `WARN`, `INFO`, `DEBUG`, and `TRACE`.
# level: ERROR

# \
=====
# agent.service
# The following properties are used by the Contrast Service.
# \
=====
# service:

# Set to `false` to disallow the service to be started, and
# effectively disable the agent, if read by the service. If the
# agent reads this property, it disallows service auto-start.
# enable: true

# Set to `true` to enable listening for gRPC connections.
# The `socket`, `host` and `port` fields will be used for
# configuring the gRPC server in place of the legacy RPC server.
# grpc: false

# If this property is defined, the service is
# listening on a Unix socket at the defined path.
# socket: /tmp/service.sock

# ***** REQUIRED *****
# Set the the hostname or IP address of the Contrast
# service to which the Contrast agent should report.
host: localhost

# ***** REQUIRED *****
```

```
# Set the the port of the Contrast service
# to which the Contrast agent should report.
port: 30555

# ***** REQUIRED *****
# Timeout (in milliseconds) that the agent-init
# should wait for the contrast-service
timeout_ms: 30000

# Set to `true` to enable direct communication with Teamsserver.
# bypass: false

# \
=====
# agent.service.logger
# The following properties are used by the logger in the
# Contrast service. If the properties are not defined, the
# service uses the logging values from the Contrast UI.
# \
=====
# logger:

# Set the location to which the Contrast service saves log output.
# If no log file exists at this location, the service creates one.
#
# Example - `/opt/Contrast/contrast_service.log` will
# create a log in the `/opt/Contrast` directory.
#
# path: ./contrast_service.log

# Set the the log output level. Options are `OFF`, `FATAL`,
# `ERROR`, `WARN`, `INFO`, `DEBUG`, `TRACE`, and `ALL`.
# level: ERROR

# Override the name of the process used in logs.
# progame: Contrast Service

# Set to `true` to send log output to `stdout`.
# stdout: false

# \
=====
# agent.go
# The following properties apply to any Go agent-wide configurations.
# \
=====
# go:

# Enable opt-in Go agent features.
# preview: NEEDS_TO_BE_SET

# Enable Go agent self-profiling features.
# profile: NEEDS_TO_BE_SET

# \
```

```
=====  
==  
# inventory  
# Use the properties in this section to override the inventory features.  
# \  
=====  
==  
# inventory:  
  
# Set to `false` to disable inventory features in the agent.  
# enable: true  
  
# Set to `false` to disable library analysis.  
# analyze_libraries: true  
  
# \  
=====  
==  
# assess  
# Use the properties in this section to control Assess.  
# \  
=====  
==  
# assess:  
  
# Include this property to determine if the Assess  
# feature should be enabled. If this property is not  
# present, the decision is delegated to the Contrast UI.  
# enable: false  
  
# Apply a list of labels to vulnerabilities and preflight  
# messages. Labels must be formatted as a comma-delimited list.  
# Example - `label1, label2, label3`  
#  
# tags: NEEDS_TO_BE_SET  
  
# \  
=====  
# assess.rules  
# Use the following properties to control simple rule configurations.  
# \  
=====  
# rules:  
  
# Define a list of Assess rules to disable in the agent.  
# The rules must be formatted as a comma-delimited list.  
#  
# Example - Set `reflected-xss,sql-injection` to disable  
# the reflected-xss rule and the sql-injection rule.  
#  
# disabled_rules: NEEDS_TO_BE_SET  
  
# \  
=====  
==
```

```
# protect
# Use the properties in this section to override Protect features.
# \
=====
==
# protect:

# Use the properties in this section to determine if the
# Protect feature should be enabled. If this property is not
# present, the decision is delegated to the Contrast UI.
# enable: false

# \
=====
==
# application
# Use the properties in this section for
# the application(s) hosting this agent.
# \
=====
==
# application:

# Override the reported application name.
#
# Note - On Java systems where multiple, distinct applications may be
# served by a single process, this configuration causes the agent to \
report
# all discovered applications as one application with the given name.
#
# name: NEEDS_TO_BE_SET

# Override the reported application path.
# path: NEEDS_TO_BE_SET

# Add the name of the application group with which this
# application should be associated in the Contrast UI.
# group: NEEDS_TO_BE_SET

# Add the application code this application should use in the Contrast UI.
# code: NEEDS_TO_BE_SET

# Override the reported application version.
# version: NEEDS_TO_BE_SET

# Apply labels to an application. Labels must
# be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET

# Define a set of `key=value` pairs (which conforms to RFC 2253) for
# specifying user-defined metadata associated with the application. The
# set must be formatted as a comma-delimited list of `key=value` pairs.
# Example - `business-unit=accounting, office=Baltimore`
```

```
#
# metadata: NEEDS_TO_BE_SET

# Provide the ID of a session which already exists in the Contrast
# UI. Vulnerabilities discovered by the agent are associated with
# this session. If an invalid ID is supplied, the agent will be
# disabled. This option and `application.session_metadata` are
# mutually exclusive; if both are set, the agent will be disabled.
# session_id: NEEDS_TO_BE_SET

# Provide metadata which is used to create a new session ID in the
# Contrast UI. Vulnerabilities discovered by the agent are associated with
# this new session. This value should be formatted as `key=value` pairs
# (conforming to RFC 2253). Available key names for this configuration
# are branchName, buildNumber, commitHash, committer, gitTag, repository,
# testRun, and version. This option and `application.session_id` are
# mutually exclusive; if both are set the agent will be disabled.
# session_metadata: NEEDS_TO_BE_SET

# \
=====
==
# server
# Use the settings in this section to set metadata for the server
# hosting this agent. Contrast recognizes common, supported server
# names, paths, types and environments. Doing this may require a new
# server or license, and it may affect functionality of some features.
# \
=====
==
# server:

# Override the reported server name.
# name: localhost

# Override the reported server path.
# path: NEEDS_TO_BE_SET

# Override the reported server type.
# type: NEEDS_TO_BE_SET

# Override the reported server environment. Valid
# values include `QA`, `PRODUCTION` and `DEVELOPMENT`.
# environment: development

# Apply a list of labels to the server. Labels
# must be formatted as a comma-delimited list.
# Example - `label1,label2,label3`
#
# tags: NEEDS_TO_BE_SET
```

## Contrast サービス



### 重要

Contrast サービスは、旧バージョンの Node エージェントと Python エージェント (Python バージョン 5.19.0 より前) で動作します。新しいバージョンのエージェントでは、Contrast サービスを必要としない、より高性能でネイティブな解析を使用します。この変更が発生するバージョンを確認するには、各エージェントのドキュメントを参照してください。

Contrast サービスはスタンドアロンの実行可能ファイルで、マルチプロセスの動的言語エージェント (Node.js エージェント、Python エージェント) と Contrast サーバ間の通信を可能にします。Contrast サービスは、Contrast 側の設定オプションをエージェントに渡したり、エージェントからの情報を集約して Contrast へ送り返します。

Contrast サービスは、サポート対象のアーキテクチャ用にコンパイルされています。

- Linux 64 ビット
- Macintosh 64 ビット
- Windows 64 ビット

Node.js エージェントと Python エージェントには、サービスと一緒にパッケージ化されており、エージェントを有効にしたアプリケーションが起動すると自動的に開始します。Go エージェントには、サービスはパッケージ化されておらず、自動的に開始しません。Go エージェントでサービスを機能させるには、サービスをインストールして設定し、起動する必要があります。Node.js や Python エージェントで実行する場合でも、同様の設定を行い、より管理しやすくすることもできます。

### Contrast サービスのインストール

インストール方法は、お使いのシステムによって異なります。

- **Linux** : システムのパッケージマネージャで Contrast サービスをインストールします。
- **Debian** : コマンドを使用して、適切な Debian リポジトリからインストールします。

1. 使用している Ubuntu の CODENAME(コードネーム)を調べます。

```
grep VERSION_CODENAME /etc/os-release
```

2. その CODENAME で以下のコマンドを更新し、コマンドを実行します。

```
curl https://pkg.contrastsecurity.com/api/gpg/key/public | sudo apt-key add -  
echo "deb https://pkg.contrastsecurity.com/debian-public/ CODENAME \\  
contrast" | sudo tee /etc/apt/sources.list.d/contrastc.list
```

3. Contrast サービスをインストールします。

```
sudo apt-get update && sudo apt-get install contrast-service
```

4. [Contrast サービスを設定 \(473ページ\)](#) します。

- **RPM(Red Hat Package Manager)** : 以下のコマンドを使用して、Contrast の yum リポジトリからインストールします。

1. リポジトリを使用するよう、システムを設定します。

```
OSREL=$(rpmquery -E "%{rhel}")  
sudo -E tee /etc/yum.repos.d/contrast.repo << EOF
```



```
[contrast]
name=contrast repo
baseurl=https://pkg.contrastsecurity.com/rpm-public/centos- $\$$ OSREL/
gpgcheck=0
enabled=1
EOF
```

2. Contrast サービスをインストールします。

```
yum install contrast-service
```

3. [Contrast サービスを設定 \(473ページ\)](#)します。



### ヒント

`contrast-service` package を削除するには、`apt-get remove contrast-service` または `yum remove contrast-service` を実行してください。

## Contrast サービスの設定

Contrast サービスには接続パラメータが事前に設定されていません。YAML 設定ファイルを使用してサービスを設定する必要があります。

Contrast サービスをシステムサービスとしてインストールした場合、Contrast サービスは `/etc` ディレクトリにある YAML 設定ファイルによって制御されます。サービスが、同じサーバ上の他のアプリケーションと同じ YAML 設定ファイル(`contrast_security.yaml`)を共有することがよくありますので、全ての接続値(ソケット名やポート番号など)が一致していることを確認してください。

アプリケーション用の設定ファイルがアプリケーションの作業ディレクトリにまだインストールされていない場合、YAML 設定ファイルの場所によって、同じサーバ上のエージェントと YAML ファイルを共有するかが決まります。

- **共有しない**場合は、YAML 設定ファイル `/etc/contrast/webserver/contrast_security.yaml` に置きます。
- **共有する**場合は、YAML 設定ファイルを `/etc/contrast/contrast_security.yaml` に置きます。

デフォルトの YAML 設定ファイルが、Contrast サービスの Linux パッケージと一緒に `/etc/contrast/webserver/contrast_security.yaml` にインストールされます。このテンプレートファイルには、エージェントの設定に最低限必要な項目のプレースホルダがありますが、以下の項目は更新してください。

- **api** : API のプロパティを設定します。この設定によって、Contrast サービスがどのように Contrast サーバに接続するかが決まります。
- **agent** : エージェントに関連する設定を構成するセクションの最上位レベルです。
  - **service** : このセクションのオプションは、エージェントと Contrast サービス間の通信に影響します。接続の設定は、Contrast サービスと、そのサービスと通信するエージェント間で同一である必要があります。
    - **socket** : ローカルの Unix ソケットへのパス(例、`/tmp/contrast.sock`)です。
    - **host および port** : オプションとして、ソケット(socket)の代わりに、ホストとポートで接続するよう Contrast サービスを設定できます。
    - **grpc** : (Go と Node.js エージェントにのみ適用)エージェントからサービスへの通信に gRPC を使用するには、"true"を設定します。この設定は任意ですが、エージェントのパフォーマンスを若干向上させることができます。

設定に問題があったり、正しい値が指定されていない場合、または Contrast サービスが Contrast に接続できない場合などは、`/var/log/contrast/service.log` で接続の失敗をトラブルシューティングできます。

## Contrast サービスのインストール

インストール方法は、お使いのシステムによって異なります。

- **Linux** : システムのパッケージマネージャで Contrast サービスをインストールします。
- **Debian** : コマンドを使用して、適切な Debian リポジトリからインストールします。

1. 使用している Ubuntu の CODENAME(コードネーム)を調べます。

```
grep VERSION_CODENAME /etc/os-release
```

2. その CODENAME で以下のコマンドを更新し、コマンドを実行します。

```
curl https://pkg.contrastsecurity.com/api/gpg/key/public | sudo apt-key add -  
echo "deb https://pkg.contrastsecurity.com/debian-public/ CODENAME \\  
contrast" | sudo tee /etc/apt/sources.list.d/contrastc.list
```

3. Contrast サービスをインストールします。

```
sudo apt-get update && sudo apt-get install contrast-service
```

4. [Contrast サービスを設定 \(473ページ\)](#)します。

- **RPM(Red Hat Package Manager)** : 以下のコマンドを使用して、Contrast の yum リポジトリからインストールします。

1. リポジトリを使用するよう、システムを設定します。

```
OSREL=$(rpmquery -E "%{rhel}")  
sudo -E tee /etc/yum.repos.d/contrast.repo << EOF  
[contrast]  
name=contrast repo  
baseurl=https://pkg.contrastsecurity.com/rpm-public/centos-$OSREL/  
gpgcheck=0  
enabled=1  
EOF
```

2. Contrast サービスをインストールします。

```
yum install contrast-service
```

3. [Contrast サービスを設定 \(473ページ\)](#)します。



### ヒント

`contrast-service` package を削除するには、`apt-get remove contrast-service` または `yum remove contrast-service` を実行してください。

## Contrast サービスの設定

Contrast サービスには接続パラメータが事前に設定されていません。YAML 設定ファイルを使用してサービスを設定する必要があります。

Contrast サービスをシステムサービスとしてインストールした場合、Contrast サービスは `/etc` ディレクトリにある YAML 設定ファイルによって制御されます。サービスが、同じサーバ上の他のアプリケ

ーションと同じ YAML 設定ファイル(`contrast_security.yaml`)を共有することがよくありますので、全ての接続値(ソケット名やポート番号など)が一致していることを確認してください。

アプリケーション用の設定ファイルがアプリケーションの作業ディレクトリにまだインストールされていない場合、YAML 設定ファイルの場所によって、同じサーバ上のエージェントと YAML ファイルを共有するかが決まります。

- **共有しない場合は**、YAML 設定ファイル `/etc/contrast/webserver/contrast_security.yaml` に置きます。
- **共有する場合は**、YAML 設定ファイルを `/etc/contrast/contrast_security.yaml` に置きます。

デフォルトの YAML 設定ファイルが、Contrast サービスの Linux パッケージと一緒に `/etc/contrast/webserver/contrast_security.yaml` にインストールされます。このテンプレートファイルには、エージェントの設定に最低限必要な項目のプレースホルダがありますが、以下の項目は更新してください。

- **api** : API のプロパティを設定します。この設定によって、Contrast サービスがどのように Contrast サーバに接続するかが決まります。
- **agent** : エージェントに関連する設定を構成するセクションの最上位レベルです。
  - **service** : このセクションのオプションは、エージェントと Contrast サービス間の通信に影響します。接続の設定は、Contrast サービスと、そのサービスと通信するエージェント間で同一である必要があります。
    - **socket** : ローカルの Unix ソケットへのパス(例、`/tmp/contrast.sock`)です。
    - **host および port** : オプションとして、ソケット(socket)の代わりに、ホストとポートで接続するよう Contrast サービスを設定できます。
    - **grpc** : (Go と Node.js エージェントにのみ適用)エージェントからサービスへの通信に gRPC を使用するには、"true"を設定します。この設定は任意ですが、エージェントのパフォーマンスを若干向上させることができます。

設定に問題があったり、正しい値が指定されていない場合、または Contrast サービスが Contrast に接続できない場合などは、`/var/log/contrast/service.log` で接続の失敗をトラブルシューティングできます。

# ユーザガイド

[en]

Contrast を操作する方法は、お使いの環境や特定の要件によって異なります。使用するツールやインテグレーション、ユーザに割り当てられたロールや権限、また Contrast へのアクセス方法(Web インターフェイス、コマンドラインツール、または REST API 経由)などによって異なります。



## 注記

本ドキュメントで使用する全てのコマンドは、Contrast がインストールされたディレクトリから管理者権限でコマンドシェルにて実行してください。

[en]

Contrast ユーザのほとんどが、Edit ロールが権限として割り当てられたアカウントになります(自分のアカウントに割り当てられている権限レベル (480ページ)はユーザの設定 (477ページ)から確認できます)。

Edit 権限では、[アプリケーションを検査 \(35ページ\)](#)して、Contrast で検出結果を確認できます。また、Contrast Web インターフェイスで、以下の基本機能を実行できます。これらは、全て Contrast Web インターフェイスのナビゲーションバーからアクセスできます。

- [アプリケーション \(480ページ\)](#)  
組織のアプリケーションの一覧(検索可能)を表示します。アプリケーションのライセンス付与、マーキング、タグ付け、アーカイブ、復元などを行うことができます。
- [サーバ \(528ページ\)](#)  
組織のサーバの一覧(検索可能)を表示します。サーバ環境の指定、Assess および Protect の有効化、設定、タグ付け、削除などを行うことができます。
- [ライブラリ \(534ページ\)](#)  
組織内の全てのアプリケーションで使用されているライブラリの一覧(検索可能)を表示します。ライブラリにタグを付けたり、ライブラリに存在する既知の脆弱性やリスクの高いライブラリに関する統計情報も表示することができます。
- [脆弱性 \(587ページ\)](#)  
検出された脆弱性の一覧(検索可能)を表示します。この脆弱性の一覧は、組織内の各アプリケーションごとに表示することができます。脆弱性のステータス変更、マーキング、共有、タグ付け、エクスポートなどを行うことができます。脆弱性の詳細までドリルダウンすると、その脆弱性を修正するための詳細情報や対策方法を参照できます。
- [攻撃 \(603ページ\)](#)  
組織内の全てのアプリケーションで発生している攻撃や発生した攻撃の一覧(検索可能)を表示します。攻撃を最上位レベルで表示したり、ドリルダウンして個別の攻撃イベントの詳細情報を参照することができます。

また、Contrast には他にも便利な機能やツールがあります。

- [レポート \(611ページ\)](#)  
データを収集し、CSV または PDF としてエクスポートして Contrast の外部で共有できます。
- [インテグレーション \(618ページ\)](#)  
バグ追跡システム、ビルドツール、アプリケーションサーバ、SIEM(Security Incident Event Management)、通知、チャットなどの外部のツールと Contrast を連携して使用できます

- [Contrast CLI \(579ページ\)](#)  
アプリケーションでソフトウェアコンポジション解析(SCA)を実行し、オープンソースライブラリとの依存関係を表示します。

これらの機能の設定に関しては、ほとんどの場合[システム管理者 \(741ページ\)](#)が[組織の管理者 \(701ページ\)](#)であるか、または [RulesAdmin \(668ページ\)](#)ルールが権限が必要になりますが、Edit 権限では以下のことを行えます。

- [エージェントのインストールと設定 \(35ページ\)](#)
- 通知の送信
- [スコア設定のカスタマイズ \(719ページ\)](#)

## ユーザの設定の管理

Contrast でユーザの設定を管理するには、[ユーザメニュー](#) (Contrast Web インターフェイスの右上にある自分の名前)を開いて、[ユーザの設定](#)を選択します。ここでは、自分のアカウントに関して以下を管理できます。

- [パスワードの変更 \(477ページ\)](#)
- [2段階認証の設定 \(478ページ\)](#)
- [プロフィールの編集 \(478ページ\)](#)
- [API キーの確認 \(478ページ\)](#)
- [通知の管理 \(479ページ\)](#)
- [権限の表示 \(480ページ\)](#)

## Contrast へのログイン

初めて Contrast にログインする場合は、管理者が作成した招待メールを承認する必要があります。Eメールに記載されているリンクを選択して、Contrast にログインします。

組織で[シングルサインオン\(SSO\) \(713ページ\)](#)を使用している場合は、ログインページのチェックボックスを選択して、パスワード入力フィールドを無効にします。Eメールアドレスの入力のみが必要になります。Eメールが認証されたら、SSO の認証情報を使用してログインできます。

[2段階認証 \(478ページ\)](#)を使用している場合は、SSO 認証が成功した後にログインプロセスが行われます。

## パスワードの変更

アカウントのパスワードを変更するには、以下の手順を実行します。

1. Contrast Web インターフェイスにログインします。
2. ユーザメニューで、[ユーザの設定](#) > [パスワードの変更](#)を選択します。
3. 画面の各フィールドで、現在のパスワードと新しいパスワードを入力します。最後のフィールドには、確認のために新しいパスワードを再度入力します。



### 注記

新しいパスワードは[管理者が設定した \(712ページ\)](#)パスワードポリシーに従う必要があります。パスワードの入力を開始すると、パスワード要件が表示されて判定されます。

4. チェックボックスをオンにして[利用規約](#)に同意します。
5. 変更を[保存](#)します。



### 注記

シングルサインオン(SSO)を使用してログイン (477ページ)する場合は、パスワードを変更するオプションはありません。

## 2段階認証の設定

組織 (712ページ)またはシステム (786ページ)レベルで管理者が2段階認証を有効にしている場合、ユーザ名とパスワード以外に安全にログインする仕組みを指定できます。2段階認証を設定するには：

1. ユーザメニューで、**ユーザの設定 > 2段階認証**を選択します。
2. トグルを使用して、2段階認証を有効にします。
3. ラジオボタンを使用して、認証コードを受け取る方法を選択します。
  - **Eメール**：Contrastと関連付けているメールアドレスで、認証用のコードを受け取ることができます。この設定を選択すると、認証コードが記載されたEメールが送信されますので、設定画面で認証コードを入力します。
  - **Google Authenticator**：モバイルデバイスにアプリのダウンロードが必要な場合がありますが、モバイルデバイスのアプリで、認証コードを受け取ることができます。この設定を選択するとQRコードが表示されますので、QRコードを読み取り、手順に従ってデバイスを検証します。
4. 2段階認証の設定を完了する前に、.txtファイル形式でバックアップコードをダウンロードしておくことができます。このコードにより、ログインエラーが発生した場合や、アカウントがロックアウトされた場合でもログインが許可されます。バックアップコードをダウンロードしたら、安全な場所に保存してください。
5. 認証コードの受け取り方法を変更する場合は、2段階認証タブの通知設定で再度設定できます。通知設定の選択を変更すると、新しいバックアップコードが自動的に発行されます。通知設定の変更は、保存する必要はありません。



### ヒント

いずれの方法でも問題が発生した場合は、提供されたバックアップコードを使用することができます。**サインインできませんか**を選択するか、**Google Authenticatorのデバイスをリセット**のリンクを使用してください。

## プロフィールの管理

プロフィールの画面では、名前の編集、時刻・日付形式、言語の設定などを更新して、Contrastの使用環境をカスタマイズできます。

1. ユーザメニューで、**ユーザの設定 > プロファイル**を選択します。
2. **一般情報**で、名前やタイムゾーンなどのアカウントの基本情報を設定します。
3. 新しいプロフィール画像をアップロードするには、サムネイルをクリックします。
4. **あなたのキー**のセクションには、**組織のキーと個人のキーが表示 (478ページ)**されます。
5. 変更を**保存**します。

## API キーの確認

エージェントまたはカスタムスクリプトでContrastとの通信を確立するためには、APIキーを使用します。以下の目的により、エージェントおよびContrast APIでキーが必要になります。

- アクセスする組織を識別するため
- 有効なユーザとして識別するため

## 手順

1. ユーザメニュー > ユーザの設定 > プロファイルに移動します。  
あなたのキーのセクションで、API キーと次のキーを含む **API キー情報**を確認できます。
  - **組織 ID**：アクセスする組織を識別するものです。
  - **サービスキー**：認証情報を使用して Contrast サービスに接続するためのものです。
  - **認証ヘッダー**：有効なユーザとして識別するためのものです。

あなたのキー

あなたのAPIキーは、Contrastと対話するスクリプトを書く場合に使用します。Contrast REST APIの使用方法については、こちらの[APIドキュメント](#)を参照してください。

**あなたのAPIキー情報**

組織ID  
12[REDACTED]6d5

あなたのAPIキー  
demo  
これは、エージェントのAPIキーではありません。エージェントのAPIキーは、[組織の設定](#)をご覧ください。

サービスキー  
demo **ローテーション**  
認証情報を使ってサービスに接続します。

認証ヘッダー  
**コピー**

エージェントキーをお探しですか? [組織の設定](#)をご覧ください。

サンプルAPIリクエストを生成

2. 認証ヘッダーをコピーするには、**コピー**を選択します。
3. サービスキーをローテーションするには、**ローテーション**をクリックします。  
サービスキーをローテーションすると、このキーを使用しているインテグレーションに影響します。再接続するために、このキーを使用しているインテグレーションで認証情報を更新してください。
4. **サンプル API リクエストを生成**をクリックすると、サンプル API リクエストが生成されてクリップボードにコピーされます。

## アカウントの通知の管理

通知の設定を変更するには：

1. ユーザメニューで、**ユーザの設定 > 通知**を選択します。
2. **通知の登録**のフィールドをクリックして、通知を受け取りたいアプリケーションを選択します(複数選択可)。デフォルトでは「全てのアプリケーション」が選択されます。
3. **Contrast 内と E メール**の列にあるトグルボタンを使用して、以下のイベントに対する通知を有効または無効にします。
  - **積極的な攻撃**：Protect が有効なアプリケーションへの積極的な攻撃が発生。
  - **新しい脆弱性**：Contrast で新たに脆弱性を検出。特定の深刻度やライブラリの通知を受け取るよう指定するには、フィールドをクリックします。デフォルトでは「全て」が選択されます。
  - **脆弱なライブラリ**：新たに脆弱性のあるライブラリが検出されたか、ライブラリに新たな CVE が検出された場合に通知を受け取ることができます。
  - **サーバのメッセージ**：サーバの信頼性に関するメッセージを取得。
  - **サーバのオフライン**：サーバへのアクセス不可。
  - **新しいコメント**：チームメンバーが検出結果に関してコメントを投稿。
  - **新しいアセット**：[アクセス権 \(480ページ\)](#)のある新しいアセット(アプリケーションやサーバ)が追加。フィールドをクリックすると、「アプリケーション」か「サーバ」のいずれかにこの通知を設定できます。デフォルトでは「全て」が選択されます。
  - **ライセンス切れ間近**：アプリケーションのライセンスの有効期限が間近。
  - **ポリシー違反**：コンプライアンスポリシー、ライブラリポリシー、修復ポリシーでの違反。チェックボックスをオンにすると、ポリシー違反の E メールをまとめてダイジェストとして通知できます。

- **Eメールダイジェスト**： Contrast での 1 日のアクティビティを要約して毎日配信。

## 権限の表示

権限のページでは、組織およびアクセス可能なアプリケーションの両方について、割り当てられている権限の詳細が表示されます。権限を表示するには：

1. **ユーザメニュー > ユーザの設定 > 権限**にアクセスします。
2. ページの上部には、自分の組織が自分の組織ロールと一緒に表示されます。**アプリケーションの権限**の表には、組織内の各アプリケーションに対して割り当てられているロールが表示されます。
3. 各ロールの横にあるヘルプアイコンをクリックして、「詳細を表示」を選択すると、各レベルで使用可能なデータアクセスと操作について参照できます。

## 関連項目

- [アプリケーションロール \(817ページ\)](#)
- [組織ロール \(819ページ\)](#)

## アプリケーション

[アプリケーションにエージェントを組み込んだら \(35ページ\)](#)、Contrast Web インターフェイスで**アプリケーションを確認 (480ページ)**します。アプリケーションに関して、以下のような機能があります。

- [ルートカバレッジ \(492ページ\)](#)
- [セッションメタデータ \(489ページ\)](#)
- [フローマップ \(497ページ\)](#)
- [アプリケーションのスコア \(822ページ\)](#)



### 注記

これらの機能を使用するには、組織の管理者がアプリケーションの管理者(Admin ロールのあるアカウント)が、[アプリケーションにライセンスを付与 \(706ページ\)](#)する必要があります。

## アプリケーションの表示

Contrast Web インターフェイスでアプリケーションの情報を表示するには、いくつかの方法があります。

### 手順

1. ナビゲーションバーで**アプリケーション**を選択すると、組織内で検出された全てのアプリケーションが一覧表示されます。
2. アプリケーションの一覧からアプリケーション名をクリックすると、そのアプリケーションの**概要**タブにアクセスできます。
3. アプリケーションのステータスに基づいて一覧にフィルタをかけるには、アプリケーションの一覧の最上部にある小さい三角形を選択します  
または、特定のアプリケーションを名前前で検索するには、**虫眼鏡アイコン**(🔍)を選択します。



# アプリケーション 全て (447)

全て (447)

オンライン (0)

オフライン (447)

マージ済 (4)

ライセンスあり (71)

ライセンスなし (376)

高リスク (117)

アーカイブ済 (46)

フィルタには次のものがあります。

- **全て**： Contrast に追加したアプリケーション(アーカイブされたアプリケーションを除く)。
  - **オンライン**： エージェントが過去 5 分以内に Contrast に接続したアプリケーションのみ。アーカイブされたアプリケーションを除く。
  - **オフライン**： エージェントが 5 分以上 Contrast に接続していないアプリケーションのみ。アーカイブされたアプリケーションを除く。
  - **マージ済**： マージされたアプリケーションの一部であるアプリケーションのみ(メインアプリケーションとそのコンポーネント)。アーカイブされたアプリケーションを除く。
  - **ライセンスあり**： Contrast のライセンスが適用されているアプリケーションのみ。アーカイブされたアプリケーションを除く。
  - **ライセンスなし**： Contrast のライセンスが適用されていないアプリケーションのみ。アーカイブされたアプリケーションを除く。
  - **高リスク**： 深刻度が重大か高の脆弱性があり、ステータスが、のアプリケーションのみ。アーカイブされたアプリケーションを除く。
  - **ポリシー違反**： このフィルタは、組織がコンプライアンスポリシーを有効にしている場合に利用できます。コンプライアンスポリシーに違反しているアプリケーションのみ。アーカイブされたアプリケーションを除く。
  - **アーカイブ済**： 履歴として参照するために表示されるアプリケーションのみ。アーカイブされたアプリケーションのエージェントは、Contrast に脆弱性を報告しなくなります。
4. アプリケーションのスコアで表示を絞り込むには、「スコア」列のヘッダの横にあるフィルターアイコン(▼)を選択し、1つまたは複数のスコアを選択します。  
フィルターを解除するには、列のヘッダの横にあるクリアを選択します。

## アプリケーション 全て



- アプリケーションの一覧で表示を絞り込むには、「アプリケーション」列のヘッダの横にあるフィルターアイコン(▼)を選択します。フィルタには次のものがあります。
  - **アプリケーションのメタデータ(設定した場合)**：アプリケーションに関連付けたカスタムメタデータ。
  - **アプリケーションのタグ(作成した場合)**：アプリケーションに割り当てたタグ。
  - **言語**：アプリケーションで使用されている言語。
  - **サーバ**：アプリケーションが実行されているサーバ。
  - **オープン中の脆弱性の深刻度**：オープン中の脆弱性の深刻度。
  - **テクノロジー**：アプリケーションで使用されているテクノロジー。例えば、JSON や jQuery など。フィルターを解除するには、列のヘッダの横にある**クリア**を選択します。
  - **環境**：アプリケーションに関連付けられている環境(開発、QA、本番)。
  - **アプリケーションの重要度**：アプリケーションの設定で指定したアプリケーションの重要性。


# アプリケーション 全て (5301)

スコア ▼ アプリケーション ▼

A	<input type="checkbox"/> フィルターを検索...
A	<input type="checkbox"/> BUSINESSUNIT <input type="checkbox"/> Death Star Security (1)
A	<input type="checkbox"/> TESTNUMERICFIELD <input type="checkbox"/> 421 (1)
A	<input type="checkbox"/> TESTPOINTOFCONTACTFIELD <input type="checkbox"/> TK-421 (1)
A	<input type="checkbox"/> アプリケーションのタグ
A	<input type="checkbox"/> (3)
A	<input type="checkbox"/> 28052021 (2)
A	<input type="checkbox"/> abc (4)
A	<input type="checkbox"/> abc123 (5)
A	<input type="checkbox"/> app-other-tag (6) 5/1208 <a href="#">もっと見る</a>
A	<input type="checkbox"/> 言語
A	<input type="checkbox"/> Java (4809)
A	<input type="checkbox"/> .NET Framework (206)
A	<input type="checkbox"/> .NET Core (22)
A	<input type="checkbox"/> Node (115)
A	<input type="checkbox"/> Ruby (39) 5/9 <a href="#">もっと見る</a>
A	<input type="checkbox"/> サーバ
A	<input type="checkbox"/> 0035f200-f1b6-11ec-8a53... (9)
A	<input type="checkbox"/> 01c8dd20-f1ad-11ec-b32a... (9)
A	<input type="checkbox"/> 023b1f90-f1b0-11ec-b415... (10)
A	<input type="checkbox"/> 023b1f90-f1b0-11ec-b415... (10)
A	<input type="checkbox"/> 028da1d0-f1af-11ec-afa4-... (10) 5/1171 <a href="#">もっと見る</a>
A	<input type="checkbox"/> オープン中の脆弱性の深刻度

## アプリケーションの設定の編集

アプリケーションに関して、以下のような特定の情報を参照したり、編集することができます。

- **アプリケーション名**：組織内の各アプリケーションには、一意の名前が必要です。アプリケーションの名前を変更するには、アプリケーションの一覧からアプリケーション名をクリックして、アプリケーションの**概要**ページに移動します。ページ上部の名前をクリックしてテキストを更新します。または、概要ページの右上にある**設定**アイコンを選択し、**アプリケーションの設定**画面で、アプリケーション名を更新します。  
システム管理者(SuperAdmin ロールのあるユーザ)の場合、ユーザメニューで **SuperAdmin** を選択して**アプリケーション**ページにアクセスし、一覧上で名前をクリックしてアプリケーション名を編集することもできます。
  - **アプリケーション ID**：アプリケーション ID は、ブラウザの URL にある最後の URI セグメントです。アプリケーション ID を調べるには、アプリケーションの一覧からアプリケーションを選択します。URL の `applications/` の後のセグメントがアプリケーション ID です。
  - **アプリケーションの重要性**：この値は、アプリケーションのメタデータとして表示され、組織のインテグレーションの設定にも使用できます。アプリケーションの重要度を設定するには、アプリケーション名を選択して、**概要**ページを表示し、**設定**アイコンを選択します。**アプリケーションの設定**画面で、**重要性**フィールドを使用してドロップダウンからレベルを選択します。
1. **アプリケーション**タブで、アプリケーションを選択します。選択したアプリケーションの概要が表示されます。
  2. アプリケーションの概要で**設定**  アイコンを選択します。**アプリケーションの設定**画面が表示されます。
  3. 必要に応じてフィールドを編集してください。
  4. 更新したアプリケーションの設定を保存するには、**保存**をクリックします。

## フィールドの説明



- **アプリケーション名**：組織内の各アプリケーションには、一意の名前が必要です。アプリケーションの名前を変更するには、アプリケーションの一覧からアプリケーション名をクリックして、アプリケーションの**概要**ページに移動します。ページ上部の名前をクリックしてテキストを更新します。または、概要ページの右上にある**設定**アイコンを選択し、**アプリケーションの設定**画面で、アプリケーション名を更新します。  
システム管理者(SuperAdmin ロールのあるユーザ)の場合、ユーザメニューで **SuperAdmin** を選択して**アプリケーション**ページにアクセスし、一覧上で名前をクリックしてアプリケーション名を編集することもできます。
- **アプリケーションコード**：組織内部で識別するコードや番号で、アプリケーションやマイクロサービスに対して一意のものです。これらのアプリケーションの一意の識別子を連携して Contrast で利用する場合は、このフィールドを使用します。このコードは、アプリケーション起動時に設定でき、エージェントの設定のアプリケーションプロパティのセクションで指定できます。
- **優先する URL**：脆弱性を再現するために使用される URL です。  
**[en]**
- **重要性**：この値は、アプリケーションのメタデータとして表示され、組織のインテグレーションの設定にも使用できます。アプリケーションの重要度を設定するには、アプリケーション名を選択して、**概要**ページを表示し、**設定**アイコンを選択します。**アプリケーションの設定**画面で、**重要性**フィールドを使用して、ドロップダウンメニューからレベルを選択します。

## アプリケーションにタグを付ける

アプリケーションにタグを付けることで、アプリケーションが整理され、効率的な検索が可能になります。

### 手順


1. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択します。

2. タグを付けるには：
  - a. 1つのアプリケーションにタグを付けるには、アプリケーションの行の最後にカーソルを合わせて、**タグアイコン**()を選択します。  
もしくは、アプリケーションの「概要」ページに移動し、一覧の上部にある**タグアイコン**()を選択します。
  - b. 複数のアプリケーションにタグを付けるには、各アプリケーションの横にあるチェックマークをオンにし、一覧の下部にあるアクションメニューから**タグアイコン**を選択します。



3. 「アプリケーションにタグを付ける」画面で、文字を入力すると、既存のタグの一覧が表示されます。使用するタグを選択するか、新しいタグを入力します。  
タグを追加すると、そのアプリケーションの「概要」タブでアプリケーション名の横にタグが表示されるようになります。  
タグを外すには、タグ名の **x** をクリックします。



4. タグを使用してフィルターをかけるには、アプリケーションの列の横にあるフィルターアイコン()を選択し、「アプリケーションのタグ」から選択します。

## アプリケーション **全て** (12)





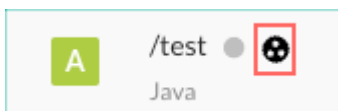
### アプリケーションのマージとマージ解除

複数のアプリケーションをマージすることで、メインアプリケーションとなる1つのアプリケーションにまとめることができます。これは、組織の管理者がアプリケーションを管理する上で一般的な操作です。

マージを行う主な目的は、スコア付け、脆弱性の検出や修復などを単一のアプリケーションとして参照するためです。複数のモジュールから構成されているアプリケーションは、アプリケーションの一覧で個別に表示される場合があります。マージすることで、アプリケーションの全てのモジュールを論理的に Contrast で1つの実体としてまとめることができます。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択し、チェックマークを使用して**マージするアプリケーション**を選択します。
2. ページ下部に表示されるメニューで**マージアイコン**()を選択します。
3. 「アプリケーションをマージ」画面で、ドロップダウンにあるマージ対象のアプリケーションから、メインアプリケーションとなるアプリケーションを1つ選択します。
4. アプリケーションがマージされると、メインアプリケーションの名前の横にメインアプリケーションのアイコン()が表示されます。




5. マージされたアプリケーションにあるアプリケーションモジュールと、疎通されたルート情報を確認するには、アプリケーションの行でメインアプリケーションのアイコンを選択します。

アプリケーションモジュール (2) ×

/testはライセンスのあるアプリケーションで、2つのモジュールがまとめられています。

<input type="checkbox"/>	スコア	アプリケーション	疎通済ルート
<input type="checkbox"/>		/test  ● Java	7 / 7
<input type="checkbox"/>		app-01a057e4-5f7a-478c-af13-3b1763fe2ce7 ● Java	4 / 4

キャンセル 選択項目のマージを解除

6. メインアプリケーションから全てのアプリケーションモジュール、または特定のアプリケーションモジュールのマージを解除するには、アプリケーションの行または概要ページでメインアプリケーションアイコン()を選択します。「アプリケーションモジュール」画面で、任意の数のモジュールを選択したら、**選択項目のマージを解除**を選択します。

## アプリケーションのアーカイブとアーカイブ解除

アプリケーションで脆弱性の収集の必要がなくなっても履歴のために組織に残したい場合は、そのアプリケーションをアーカイブするのが最適な方法です。

アプリケーションをアーカイブすると、脆弱性やライブラリなど、過去のアプリケーションデータの整合性は維持されますが、エージェントは Contrast に脆弱性を報告しなくなります。



アーカイブされたアプリケーションは総合スコアに含まれないため、ポートフォリオ全体のスコアも改善します。

管理者は、アーカイブされたアプリケーションを復元できます。アプリケーションのアーカイブを解除すると、そのアプリケーションはデフォルト表示のアプリケーション一覧で表示されます。全ての脆弱性や問題は、すぐにスコアに反映されます。


## 開始する前に

- アプリケーションをアーカイブしても、Contrast のライセンスは解放されません。ライセンスを利用可能なライセンスプールに戻すには、アプリケーションをアーカイブして、完全に削除 (488ページ) する必要があります。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択します。
2. アーカイブするアプリケーションを検索します。
3. アプリケーションをアーカイブするには：
  - a. 1つのアプリケーションをアーカイブするには、アプリケーションの行の最後にカーソルを合わせて**アーカイブアイコン**()を選択します。
  - b. 複数のアプリケーションをアーカイブするには、各アプリケーションの横にあるチェックマークをオンにし、一覧の下部にあるアクションメニューから**アーカイブアイコン**()を選択します。



- c. 表示された画面で、**アーカイブ**を選択し処理を確定します。
4. アプリケーションのアーカイブを解除するには：
    - a. アプリケーション一覧の上部で、アプリケーションの見出しの横にある小さい三角形(▼)を選択します。
    - b. **アーカイブ済**を選択します。
    - c. 1つのアプリケーションのアーカイブを解除するには、アプリケーションの行の最後にカーソルを合わせて**アーカイブを解除のアイコン**()を選択します。
    - d. 複数のアプリケーションのアーカイブを解除するには、各アプリケーションの横にあるチェックマークをオンにし、一覧の下部にあるアクションメニューから**アーカイブを解除のアイコン**を選択します。



- e. 表示された画面で、**アーカイブを解除**を選択して処理を確定します。

## アプリケーションのリセット

アプリケーションをリセットすると、そのアプリケーションに関連付けられているデータが全て消去されますが、アプリケーションは削除されません。アプリケーションのリセットは、特定のアプリケーションに関する全ての履歴や検出結果を消去したい場合に便利です。

アプリケーションを削除する前にリセットを行い、関連する全ての脆弱性、URL、コンポーネントなどを適切に消去するのが一般的です。

## リセットによる処理

- **基本的な処理：**  
アプリケーションをリセットすると、過去の脆弱性データ、ライブラリデータ、およびルートカバレッジのデータが失われます。ライセンスの関連付けとエントリは Contrast で保持され、サーバとの関連付けも保持されます。
- **アプリケーションまたはサーバがオンラインの場合：**

オンラインのアプリケーション、またはサーバがオンラインのアプリケーションをリセットすると、脆弱性、ライブラリ、およびルートの数は0になります。アプリケーションのエンドポイントをいくつか閲覧すると、脆弱性、ライブラリおよびルートのデータが再度作成されます。ただし、ルート検索はアプリケーションの起動時に行われるため、検出されたルートは無いままとなります。

• **アプリケーションまたはサーバがオフラインの場合：**

アプリケーションまたはサーバがオフラインの時にアプリケーションをリセットした場合、再起動後、全てのデータが想定通りに読み込まれます。

## 開始する前に



1度にリセットできるのは、1つのアプリケーションのみです。



### 注意

アプリケーションをリセットした場合、消去されたデータを回復する方法はありません。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択します。
2. 行の右端にカーソルを合わせ、**リセットアイコン**()を選択します。  
あるいは、アプリケーションの「概要」タブで**設定アイコン**()を選択し、**アプリケーションをリセット**を選択します。
3. 「アプリケーションをリセット」の画面で、**リセット**を選択します。

## アプリケーションの削除



アプリケーションを削除すると、関連する検出結果(脆弱性やライブラリなど)が全て完全に削除されます。

アプリケーションに適用されたライセンスは、最大許容アプリケーション数に対して永続的にカウントされます。ライセンスが適用されたアプリケーションを削除しても、アプリケーションに許容されるライセンス数には影響はありません。

## 開始する前に

- 組織管理者のロール(Admin)が必要です。
- **任意**：アプリケーションをアーカイブして削除する前に**アプリケーションをリセット (487ページ)**します。  
アプリケーションをリセットすると、そのアプリケーションに関連付けられているデータが全て消去されますが、アプリケーションは削除されません。アプリケーションをリセットして、特定のアプリケーションに関連する全ての履歴や結果を消去するのは、よくあるユーザ操作です。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択します。
2. 削除するアプリケーションを検索します。
3. アプリケーションをアーカイブするには：
  - a. 1つのアプリケーションをアーカイブするには、アプリケーションの行の最後にカーソルを合わせて**アーカイブアイコン**()を選択します。
  - b. 複数のアプリケーションをアーカイブするには、各アプリケーションの横にあるチェックマークをオンにし、一覧の下部にあるアクションメニューから**アーカイブアイコン**()を選択します。



- c. 表示された画面で、**アーカイブ**を選択します。
4. ページ上部のアプリケーションの見出しの横にある**ドロップダウンアイコン(▼)**を選択し、**アーカイブ済**を選択します。
5. アプリケーションを削除するには：
  - a. 1つのアプリケーションを削除するには、削除したいアプリケーションの行の最後にカーソルを合わせて**削除(🗑️)**アイコンを選択します。
  - b. 複数のアプリケーションを削除するには、各アプリケーションの横にあるチェックマークをオンにし、一覧の下部にあるアクションメニューから**削除アイコン(🗑️)**を選択します。



- c. 表示された画面で、**削除**を選択します。

## セッションメタデータフィルタの使用

セッションメタデータを使用すると、特定のブランチ、ビルド、コミットしたユーザ、リポジトリなどによって、脆弱性やルート情報をフィルタリングできます。エージェントの設定ファイルにセッションメタデータとして**必要な設定情報を追加 (491ページ)**すると、標準の脆弱性データとともに追加の情報がエージェントによって Contrast に報告されます。



### 注記

この機能は、現在、オンプレミス版のお客様はご利用できません。

セッションには、エージェントの設定ファイルで設定したメタデータ値を組み合わせることができません。定義した値に応じて、各エージェントの実行を単独のセッションの一部にすることもできますし、全てのエージェントの実行に独自のセッション情報を持たせることもできます。Contrast を CI/CD パイプラインに組み込んでいる場合は、アプリケーションの新しいバージョンをデプロイするたびに、一意のセッションメタデータ値を少なくとも1つ送信するようにします。例えば、コミットハッシュ (commitHash) やビルド番号 (buildNumber) などの値は、アプリケーションのデプロイごとに変わる可能性が高いため、これらのメタデータがエージェントから送信されるように設定します。

特定のセッションメタデータフィルタを選択しない場合、脆弱性一覧の「セッション」列には、エージェントの設定ファイルで指定された値のうち最大10個までが表示されます。この制限は、Contrast Web インターフェイスで脆弱性とシンクグループのデータを正しく表示するためのものです。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択します。
2. 一覧からアプリケーション名をクリックします。
3. **脆弱性**タブまたは**ルートカバレッジ**タブのいずれかを選択します。
4. 画面の右上にあるセッションメタデータのアイコン(🗑️)を選択します。  
セッションメタデータフィルタを適用すると、「脆弱性」および「ルートカバレッジ」の一覧に影響します。
5. **最新のセッション**を選択し、**フィルタを適用**を選択すると、直近のセッションのデータが表示されます。  
脆弱性一覧では、「セッション」列と「〜で表示」(〜はプロパティ名)フィルタが非表示になり、直近のセッションの情報が、セッションメタデータのアイコンの上に表示されます。



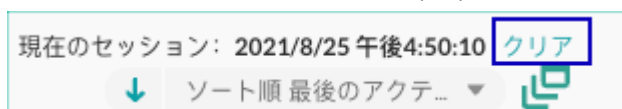
6. 特定のセッションの情報を表示するには、**カスタムのセッション**を選択し**フィルタを適用**を選択します。
  - a. **システムプロパティ**で、表示されているプロパティを1つ選択します。
  - b. **値**で入力し始めると、選択したプロパティに対する値を検索できます。



7. セッションメタデータフィルタをクリアするには、以下のいずれかの方法を使用します。
  - セッションメタデータのアイコン(🗑️)を選択し、**フィルタをクリア**を選択します。



- セッションメタデータのアイコン(🗑️)の上に表示されている**クリア**を選択します。



脆弱性一覧では、セッションメタデータフィルタをクリアすると、「セッション」列が表示されません。

## セッションメタデータの設定

アプリケーションのセッションメタデータを Contrast に送信するには、エージェントの設定ファイルにプロパティを追加で指定する必要があります。

エージェントが、メタデータとして Contrast サーバに報告できるのは、以下のビルドプロパティです。以下のプロパティの全てまたは一部を指定することができます。プロパティを設定ファイルに指定すると、メタデータが利用できるようになり、メタデータを各脆弱性の追加情報として参照したり、フィルターに使用することができます。

この設定は、システムプロパティ、環境設定、または YAML 設定ファイルのプロパティとして指定できます。

名前	値
コミットハッシュ	commitHash
コミットしたユーザ	committer
ブランチ名	branchName
Git タグ	gitTag
リポジトリ	repository
テストラン	testRun
バージョン	version
ビルド番号	buildNumber

以下の例で、セッションメタデータを設定する方法をいくつか紹介します。

- **Java のシステムプロパティを使用する場合**：javaagent フラグを指定している行に、追加のプロパティを含めます。この場合、contrast.application.session\_metadata プロパティを設定し、実行したテストを識別するためのキーと値をペアにして指定(RFC 2253 に準拠)します。

```
-Dcontrast.application.session_metadata="branchName=feature/some-new-thing,committer=Jane,repository=Contrast-Java"
```

- **.NET Framework で app.config または web.config を使用する場合**：設定ファイルに項目を追加して、メタデータのプロパティを指定します。

```
<?xml version="1.0"?>
<configuration>
  <connectionStrings />
  <appSettings>
    <add key="contrast.application.session_metadata" \
value="branchName=feature/some-new-thing,committer=Jane,repository=Contrast-DotNet" />
  </appSettings>
</configuration>
```

- **YAML 設定ファイルの場合**：contrast\_security.yaml ファイルに項目を追加して、メタデータのプロパティを指定します。

```
application:
  session_metadata: branchName=feature/some-new-thing,committer=Jane,repository=Contrast-Ruby
```

- **CI(継続的インテグレーション)のビルドスクリプトの場合**：環境変数を使用して値を指定できます。

```
-Dcontrast.application.session_metadata="branchName=feature/some-new-thing,committer=Jane,repository=Contrast-Java,buildNumber=$BUILD_NUMBER"
```

```
-Dcontrast.application.session_metadata="branchName=$GIT_BRANCH,committer=$GIT_COMMITTER_NAME,commitHash=$GIT_COMMIT_HASH,repository=$GIT_URL,buildNumber=$BUILD_NUMBER"
```

## ルートカバレッジ

ルートカバレッジにより、Assess ユーザは脆弱性と元の Web リクエストを関連付けることができます。

ルートカバレッジによって、どのルートが疎通されていて、どのルートが疎通されていないかなど、アプリケーションのコンポーネントに関する詳細な情報を確認できます。これは、どこにテストや修復を重点的に行うかを判断するのに役立ちます。

## Web リクエストの例

Web リクエストは、Web アプリケーションの最も基本となるインターフェイスです。リクエストを処理する関数は、他のサービスやデータベース、ファイルなどと連携を行う後続の関数を呼び出す場合があります。

リクエストを処理するプロセスで、Contrast はアプリケーション全体のデータフローを監視し、脆弱性を特定します。1 つの Web リクエストが、複数の種類の攻撃に対して脆弱な場合があります。Contrast では、これらの脆弱性を元のリクエストに関連付けます。

以下は、Web リクエストの例です。

```
GET /users?active=true
Host: YourDomain.com
Accept: application/json
```

以下は、上記の Web リクエストがどのように関数で処理されるかの例です。

```
@Controller
public class UserController {
    @GetMapping("/users")
    public String users(@RequestParam(name="active", required=false, \
defaultValue=true) Bool active) {
        ...
    }
}
```

## ルートカバレッジの仕組み

アプリケーションのルートは、次の 3 つの要素の組み合わせです。

- HTTP 動詞(上記の例では、GET)
- リソースのパス(上記の例では、/users)
- コントローラのメソッドシグネチャ(上記の例では、UserController.users(Bool active))

Contrast エージェントを起動すると、アプリケーション内の関数にエージェントが組み込まれ、アプリケーションを実行中に Web リクエストの脆弱性が評価されます。関数に Web リクエストを処理するためのフレームワークが実装されていれば、リクエストが処理される前に Contrast でルートが識別されます。そのようなルートは、Contrast では**検出済**というステータスになります。

アプリケーションがリクエストを処理すると、そのアクティビティは Contrast によって観察されて、**疎通済**ルートとなります。

## フレームワーク

Contrast では、以下のフレームワークのルート検出をサポートします。

- **Java** : 現在 [サポート対象のテクノロジー \(57ページ\)](#)
- **Scala** : 現在 [サポート対象のテクノロジー \(59ページ\)](#)
- **.NET Framework** : 現在 [サポートされている全てのフレームワーク \(137ページ\)](#)
- **.NET Core** : 現在 [サポートされている全てのフレームワーク \(196ページ\)](#)

- **Node.js** : 現在サポートされている全てのフレームワーク (251ページ)
- **Python** : 現在サポートされている全てのフレームワーク (317ページ)
- **Ruby** : 現在サポートされている全てのフレームワーク (395ページ)
- **Go** : 現在サポートされている全てのフレームワーク (451ページ)

お使いのフレームワークがサポートされていない場合は、**サポートまでお問い合わせ**してください。サポート対象外のフレームワークの場合、Contrast では観測されたリクエストに基づいてルートを推測しようとはしますが、ルートは検出されず Contrast には表示されません。

## 対象外(内蔵されたルートやアプリケーション)

Contrast のルートカバレッジには、一部の Web フレームワークやアプリケーションに内蔵されたルートは含まれません。例えば、以下のような場合です。

- Java アプリケーションの Jersey フレームワークには、WADL ファイルを提供するため機能があり、そのルートが内蔵されています。このルートは、Contrast のルートカバレッジには含まれません。他の Web フレームワークにも同様に、フレームワークに内蔵されているルートがあります。
- Contrast Java エージェントは、Tomcat の管理マネージャ (Tomcat Manager Application) などの備え付けのアプリケーションからのルートを報告しません。

## ルート情報の表示

**ルートカバレッジ (492ページ)**は、脆弱性がアプリケーションの攻撃対象領域に対して、どのように関連付けられるかを理解するのに役立ちます。

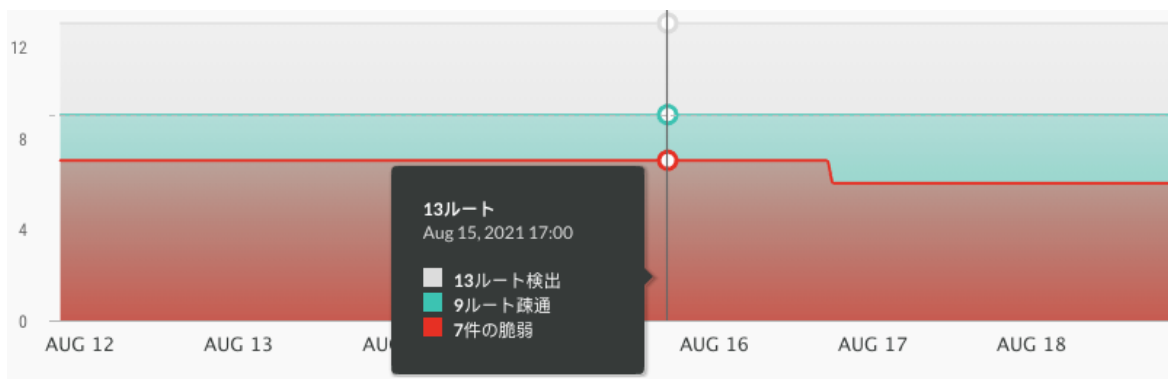
ルートカバレッジの一覧からルートを削除しても(手順 7 および 8)、サーバの再起動時やアプリケーションの疎通時にルートがまだ存在する場合に、そのルートは再度カバレッジの対象に含まれることになります。ルートを完全にカバレッジの対象外にする場合は、そのルートの行の右端にある**除外アイコン** (🚫)を選択してください。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択します。
2. アプリケーションの名前を選択します。  
アプリケーションの概要タブには、アプリケーションの合計ルート数に対する疎通済みのルート数が表示されます。
3. 概要タブで、疎通済みのルート数を選択するか、**ルートカバレッジ**タブを選択します。



4. ルートカバレッジタブでは、グラフの上にカーソルを置くと、特定期間のルートが表示されます。



グラフには、ルートのステータスに基づいてルートの詳細が表示されます。

- Contrast で検出されたルート
  - Contrast エージェントを使用して疎通されたルート
  - 疎通されて脆弱性があると判明したルート
5. 各ルートの詳細が一覧で表示されます。
- **ルート**：Contrast で特定されたルート、または追跡中のルート。
  - **環境**：アプリケーションをホストしているサーバの環境(開発、QA、本番環境のいずれか)。
  - **サーバ**：アプリケーションが稼働しているサーバ。

デフォルトでは、サーバ列に表示されるのは3サーバまでです。3サーバを超える場合に、サーバの全リストを表示するには、**全て(xサーバ)を表示**を選択します(xはサーバの合計数)。

ルート	環境	サーバ	脆弱性	アプリケーション	最後のアクティビティ	ステータス
hello.ContactController.contactForm(org.springframework.ui.Model)	開発環境	CONTRAST-SVR1 CONTRAST-SVR2 CONTRAST-SVR3	0	8885-test-app	5分前	疎通済

全て(xサーバ)を表示



### 注記

サーバを削除すると、サーバはグレー表示されるのではなく一覧から削除されます。

- **脆弱性**：そのルートに関連付けられた脆弱性の数。
- **アプリケーション**：そのルートに関連付けられたアプリケーション。
- **最後のアクティビティ**：そのルートのアクティビティ期間。
- **ステータス**：そのルートのステータス。

6. 一覧より各項目を選択すると、アプリケーションで特定された各ルートの詳細情報が表示されます。

- ルートの URL を表示するには、ルート名を選択します。
- 特定のルートの脆弱性の詳細を表示するには、脆弱性列の番号を選択します。  
赤色の警告マークは、重大な脆弱性を表します。

### 脆弱性

3 1

- 特定のステータスのルートのみを表示するには、ページ上部の三角形(▼)を選択し、フィルタを選択します。
  - **全て**：除外されていない全てのルートを表示します。
  - **疎通済**：疎通されたルートのみを表示します。
  - **未疎通**：検出されたルートで、まだ疎通されていないルートを表示します。

- **脆弱なもの**：脆弱性が関連付けられているルートのみを表示します。
  - **対象外**：アプリケーションのスコア付けの計算から除外されるルートのみを表示します。
- d. 特定の環境のルートを表示するには、「環境」列の横にあるフィルタアイコン(▼)を選択します。
  - e. マージされたアプリケーションの特定のモジュールのルートを表示するには、「アプリケーション」列の横にあるフィルタアイコン(▼)を選択します。
  - f. アクティビティ期間に基づいてルートを表示するには、「最後のアクティビティ」列の横にあるフィルタアイコン(▼)を選択します。  
期間を変更すると、ルートカバレッジのグラフの期間も変更されます。  
フィルタの選択を解除するには、列の見出しの横にあるクリアを選択します。
7. 一覧から1つのルートを削除するには：
    - a. 行の右端にカーソルを合わせ、**削除アイコン**(🗑️)をクリックします。
    - b. ルートの削除の確認画面で、**削除**をクリックします。
  8. 一覧から複数のルートを削除するには：
    - a. 1つまたは複数のルートの行でチェックマークを選択します。また、全てのルートを選択する場合は、ルートの横にあるチェックマークを選択します。
    - b. ページの下部に表示される一括アクションメニューで、**削除アイコン**(🗑️)を選択します。
    - c. ルートの削除の確認画面で、**削除**をクリックします。
  9. ルートの情報を Contrast の外部で参照・共有するには：
    - a. 1つまたは複数のルートの行でチェックマークを選択します。また、全てのルートを選択する場合は、ルートの横にあるチェックマークを選択します。
    - b. ページの下部に表示される一括アクションメニューで、**エクスポートアイコン**(📄)を選択します。  
この操作によって、ルート情報が CSV ファイルにエクスポートされます。ファイルは、デフォルトのダウンロード先にダウンロードされます。  
CSV ファイルには次のものが含まれます：
      - アプリケーションのルートの一覧
      - ルートが検出されたサーバの情報
      - ルートが最後に疎通された日付
      - 脆弱性の一覧、各脆弱性の深刻度およびステータス

## 関連項目

- [ルートを除外する \(496ページ\)](#)
- [ルートを含める \(496ページ\)](#)

## 除外ルートと含めるルート

セキュリティ上の理由から特定の割合のルートカバレッジが必要な場合、ルートカバレッジの計算から無関係なルートやアクセスできないルートを含めないよう除外するオプションが Contrast にはありません。

既に除外したルートは、再度対象に含めることもできます。

ルートを除外したり含めるには、Admin(管理者)ロールが必要です。

## ルートを対象に含めない場合の影響

- Contrast では、除外されたルートの脆弱性データは収集されますが、このデータはアプリケーションのスコア付けの計算に含まれなくなります。
- ルートを除外すると、Contrast がそのルートを検出した全ての環境から除外されます。
- セッションメタデータを定義してアプリケーションで疎通やルート検出した場合、ルートを除外すると、このデータも除外されます。
- 監査ログには、除外された各ルートのエントリは含まれます。

## ルートを対象に含める場合の影響

- 除外されていないルートのデータは、アプリケーションのスコア付けの計算に含まれます。
- ルートを対象に含めると、Contrast がそのルートを検出した全ての環境にそのルートが含まれるようになります。
- 監査ログには、対象に含めた各ルートのエントリが含まれます。

## ルートを除外する


無関係なルートやアクセスできないルートを除外する (495ページ) ことで、アプリケーションのルートカバレッジの計算が正確になります。

ルートを確実に除外したままにするには、ルートを除外した後に、そのルートを削除しないことです。ルートを除外してから削除すると、アプリケーションサーバの起動時やアプリケーションの疎通後にそのルートが検出された場合に、ルートは再度カバレッジに含まれる対象となります。

## 開始する前に

- Admin ロールが必要です。
- カバレッジから除外するルートを決めます。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーでアプリケーションを選択します。
2. アプリケーション名を選択します。
3. ルートカバレッジタブを選択します。
4. 1つまたは複数のルートを除外します：
  - a. 除外したいルートが1つの場合は、行の最後にカーソルを合わせ除外アイコン()を選択します。
  - b. 複数ルートを除外したい場合は、左側の列のチェックマークを使用して、ルートを選択します。次に、ページ下部にある一括アクションメニューから除外アイコンを選択します。



- c. 表示される画面でルートの除外を確定します。  
選択したルートのステータスが、対象外に変わります。

## ルートを含める

除外されたルートは、再度カバレッジにルートを含める (495ページ) ことができます。除外されたルートは、ルートカバレッジのページで対象外のステータスになります。

## 開始する前に


- Admin ロールが必要です。
- カバレッジに含めるルートを決めます。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーでアプリケーションを選択します。
2. アプリケーション名を選択します。
3. ルートカバレッジタブを選択します。
4. 一覧の上部にある三角形(▼)を選択して対象外を選択すると、カバレッジから除外されているルートが表示されます。





5. 1つまたは複数のルートをかバレッジに含めます：
  - a. 除外されている1つのルートをかバレッジに含めるには、行の最後にカーソルを合わせ**再度含めるアイコン**()を選択します。
  - b. 除外されている複数のルートを選択するには、左の列のチェックマークを使用してルートを選択します。次に、ページ下部にある一括アクションメニューから**再度含めるアイコン**を選択します。



- c. 表示される画面で、ルートをかバレッジに含めることを確定します。ステータスは、ルートを除外する前のステータスに戻ります。

## フローマップ

アプリケーションのフローマップによって、組織内および組織外のデータとリソースの共有状況がインタラクティブに表示されます。

アプリケーションを実行するたびに、Contrast エージェントから報告されるデータを使用して、アプリケーション、アプリケーション内のテクノロジ層、およびアプリケーションが接続しているバックエンドシステムなどの構成を表すダイアグラムが Contrast で作成されます。組織内でより多くのアプリケーションが実行され、エージェントによってアプリケーションのバックエンドシステムが認識されると、現在参照中のアプリケーションに対して、共有バックエンドシステムで接続しているアプリケーションも認識されます。

[フローマップを表示 \(498ページ\)](#)すると、アプリケーションに関連付けられているシステムとリソースの全体像を確認できます。個々のシステムとアプリケーション間の接続に注目することで、組織内のユーザーや接続されたアプリケーションが、現在のアプリケーションとアプリケーションに関連する可能性のある機密情報に対して、適切なアクセスがあるかを判断することもできます。詳細については、[フローマップの理解 \(498ページ\)](#)を参照してください。

エージェントは、文字列認証によりアプリケーションの照合を行います。計測された他のアプリケーションで、共通の文字列認証情報(例えば、REST エンドポイント、データベース接続、その他の一意のホストとポートの組み合わせなど)を共有しているものが、接続中のアプリケーションとして表示されません。



### 注記

接続中のアプリケーションの情報を表示する**権限のない (708ページ)**ユーザーには、フローマップにそのアプリケーションは表示されません。

## フローマップの表示

アプリケーションのフローマップによって、組織内および組織外のデータとリソースの共有状況がインタラクティブに表示されます。

アプリケーションのフローマップを表示するには：

1. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択して、アプリケーションの一覧よりアプリケーション名をクリックします。
2. **フローマップ**タブをクリックします。
3. フローマップタブには、3つの関連するセクションがあります：**アプリケーションアーキテクチャ**、**バックエンドシステム**、**アプリケーション**です。詳細については、[フローマップデータの理解 \(498ページ\)](#)を参照してください。

## フローマップの理解

アプリケーションのフローマップによって、組織内および組織外のデータとリソースの共有状況がインタラクティブに表示されます。

アプリケーションの**フローマップ (498ページ)**は、3つの関連セクションで情報が編成されます。

- **アプリケーションアーキテクチャ**：このセクションでは、アプリケーションのフロントエンドをビュー、プレゼンテーション、サービスの階層に分類します。また、アプリケーションがデプロイされている環境、レターグレード、脆弱性ステータスおよび攻撃ステータスなどアプリケーションに関する基本的な情報も確認できます。このセクションの3つの層は、以下の通りです。
  - **ビュー**：ブラウザでの表示および処理を決定するテクノロジー層を表します。
  - **プレゼンテーション**：アプリケーションのビューを生成するライブラリ層を表します。
  - **サービス**：アプリケーションロジックを実行しているデータベース、LDAP ドライバ、バックエンドコードなどで構成される層を表します。リスト内の項目にカーソルを合わせると、アプリケーションで使用されている各タイプのライブラリのインスタンス数が表示されます。また、ライブラリをクリックするとライブラリのページに移動します。エージェントから脆弱性が報告されると、検出されたライブラリの横に警告アイコンが表示されます。アイコンにカーソルを合わせると脆弱性の**概要**ページへのリンクが表示されます。
- **バックエンドシステム**：アプリケーションが接続されている各システムを表示します。データベースのシリンダアイコン、URL のグローブアイコン、または LDAP データベースのプラグアイコンにカーソルを合わせると、各システムの詳細を参照できます。アイコンをクリックすると、ほかのアプリケーションへの接続が強調表示されます。鍵付きの実線は、接続が暗号化されていることを表します。破線は、接続が暗号化されていないか、暗号化の状態が不明であることを表します。
- **接続中のアプリケーション**：バックエンドシステムによってプライマリアプリケーションに接続されている各アプリケーションの一覧を表します。特定の条件を満たす接続中のアプリケーションを表示するには、ファネルアイコンをクリックし、ドロップダウンから、環境、アプリケーション言語、カスタムタグなどのフィルターを選択します。このメニューには、参照可能な場合、プライマリアプリケーション(接続されているアプリケーションではありません)のセッションメタデータフィールドも表示されます。**フローマップを表示**のリンクをクリックすると、そのアプリケーションの**フローマップ**タブに移動します。



### 注記

現在のアプリケーションに対してエージェントから報告されているデータがない場合は、**バックエンドシステム**と**接続中のアプリケーション**のセクションは空欄のままです。



## ヒント

フローマップを表示しているときに別のユーザがアプリケーションにアクセスしている場合は、**ブラウザタブ**が表示され、アクセスしているブラウザの一覧が表示されます。アイコンにカーソルを合わせると、ブラウザの種類やバージョンなどの詳細を参照できます。

## スキャン

Contrast Scan では、次のことができます。

- [スキャンプロジェクトの作成 \(503ページ\)](#)
- [スキャンの確認 \(506ページ\)](#)
- [スキャン結果の分析 \(513ページ\)](#)
- [新規スキャンの開始 \(505ページ\)](#)
- [スキャンのキャンセル \(506ページ\)](#)
- [スキャン設定の変更 \(524ページ\)](#)

## Contrast Scan リリース情報

### スキャンエンジン・ローカルスキャンエンジン

#### Contrast Scan 0.0.60

リリース日：2023年5月22日

##### 新機能と改善点：

- プロジェクトを始めてスキャンする時に、ローカルスキャンエンジンのパラメータとして、リソースグループを指定できる機能が追加されました。  
この機能を利用するには、組織でロールベースのアクセス制御が有効になっており、新しいプロジェクトを作成するための十分な権限(Manage Project ロール以上)が必要です。  
リソースグループ名は、`-r` パラメータで指定します。

#### Contrast Scan 0.0.56

リリース日：2023年4月6日

##### 新機能と改善点：

- 複数 JAR のスキャンに対応  
このリリースでは、複数の JAR ファイルを1つのアーティファクトとしてスキャンできる機能が追加されました。複数の JAR ファイルを ZIP ファイルに追加し、1つのアーティファクトとしてスキャンすることができます。  
複数 JAR の ZIP ファイルをスキャンするには、最上位レベルで JAR ファイルを ZIP ファイルにパッケージし、通常通り Contrast Scan ローカルエンジンを使用してスキャンします。例：

```
multiple-jar-artifact.zip
-> artifact1.jar
-> artifact2.jar
-> artifact3.jar
```

スキャンが完了すると、Contrast Web インターフェイスでは、「スキャン」タブの下に1つのプロジェクトとして表示されます。

## スキャン Web インターフェイス

### 5 月リリース : スキャン Web インターフェイス

リリース日 : 2023 年 5 月

#### 新機能と改善点 :

- Java バイナリスキャナが複数 JAR のスキャンに対応するようになりました。  
SaaS 版の Java バイナリスキャナを使用する場合(Contrast CLI または Contrast Web インターフェイスを使用)、1 つの ZIP ファイルに複数の JAR ファイルを含めることができるようになりました。  
アップロードできる ZIP ファイルのサイズの上限は、1GB です。

### 4 月リリース : スキャン Web インターフェイス

リリース日 : 2023 年 4 月

#### 新機能と改善点 :

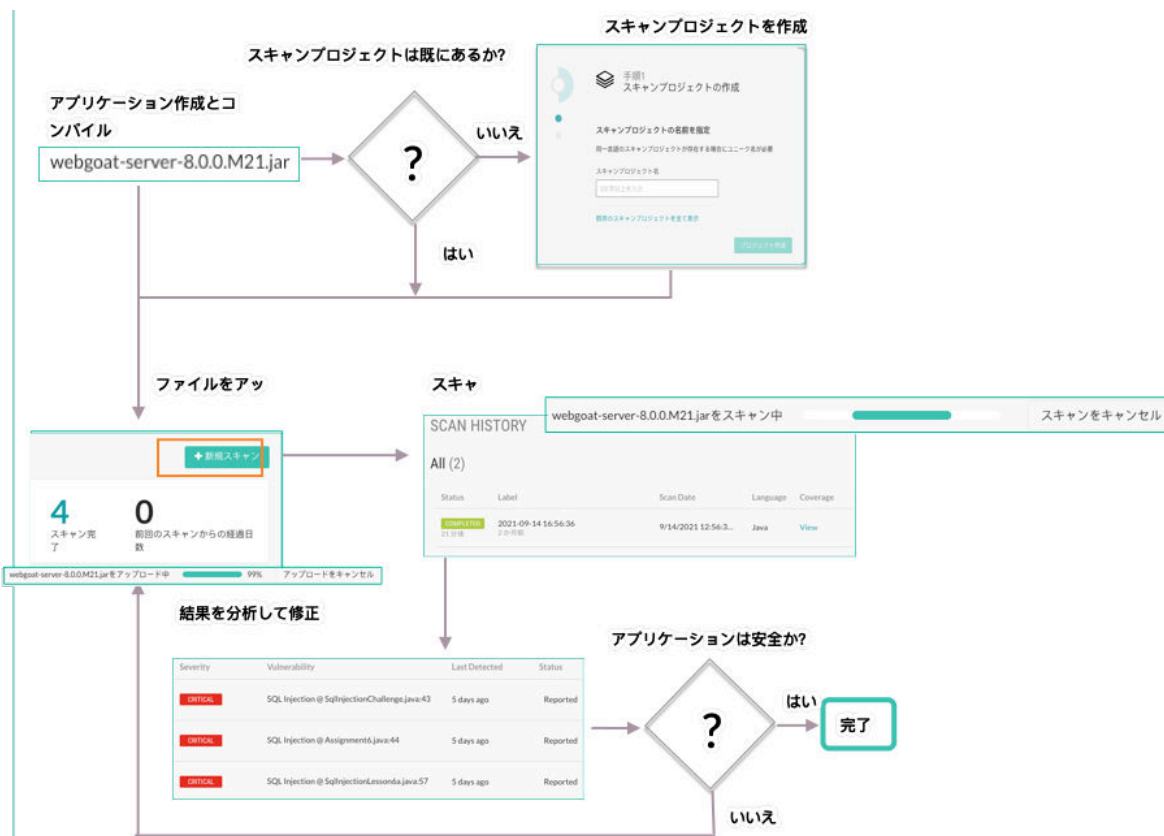
- プロジェクト内の脆弱性に対して行われたステータスの変更に関する情報を表示する、脆弱性のアクティビティタブを追加しました。  
このタブを表示するには、選択したスキャンプロジェクトの「脆弱性」タブを選択し、特定の脆弱性を選択します。
- プロジェクト内の脆弱性のステータスを変更する際に、コメントを追加できるようになりました。
- 全てのプロジェクトを管理できるロールのあるユーザに対して、Contrast Web インターフェイスでプロジェクトと関連する全てのデータを削除できる機能を追加しました。

## スキャンのプロセス

本項では、Contrast Scan を使用する際のワークフローと、Contrast Scan がコードの解析に使用するプロセスについて説明します。

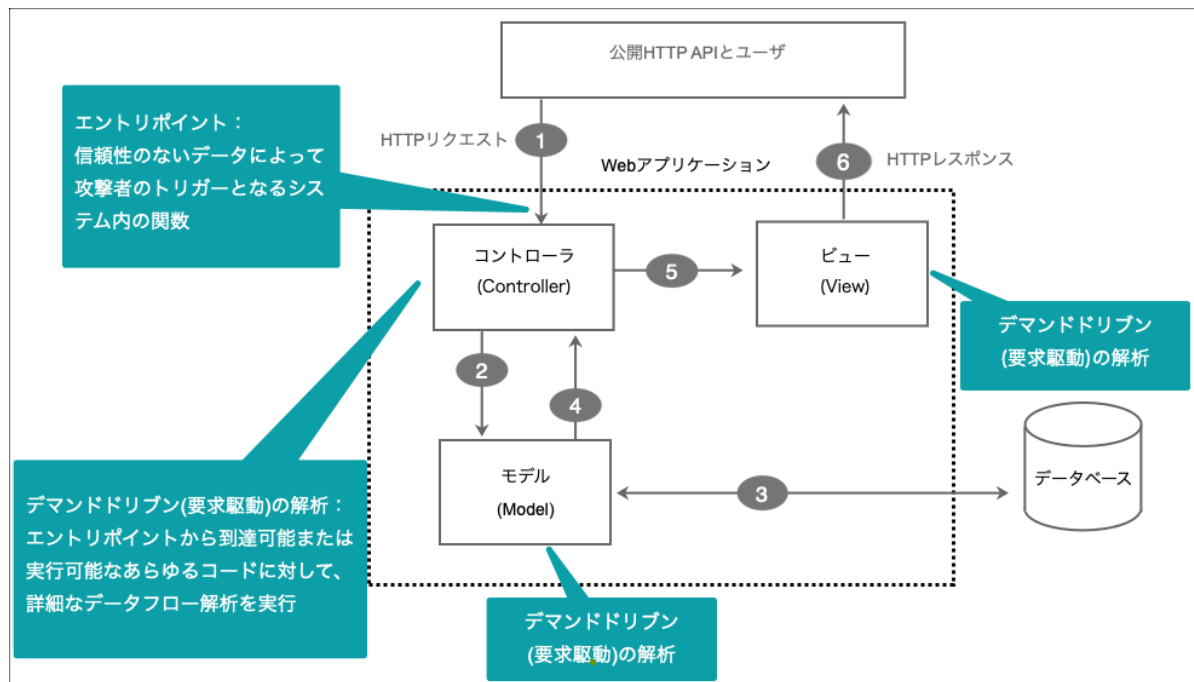
## スキャンのワークフロー

次の図は、Contrast Scan を使用する場合のワークフローを示しています。

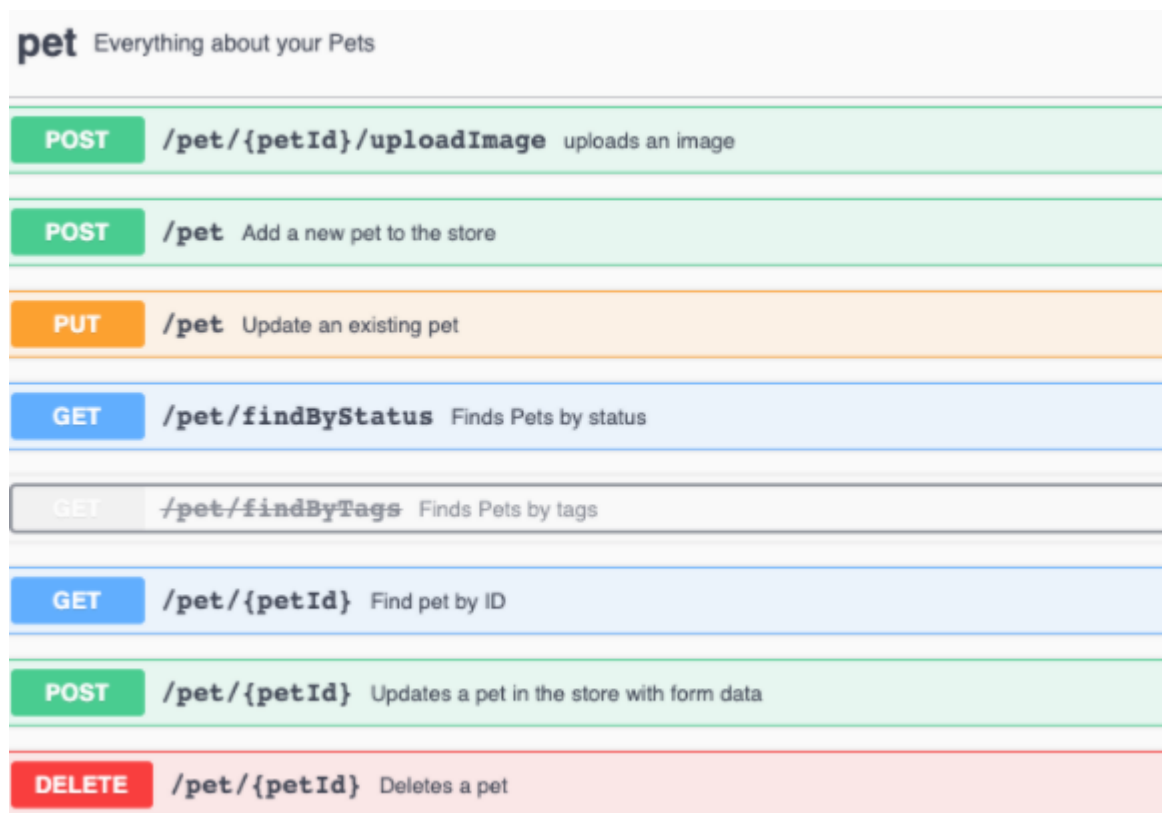


## アプリケーションの参照

次の図は、データフローの解析を目的として、Contrast Scan が一般的な Web アプリケーションをどのように参照するかを示しています。



Contrast Scan は、データのエントリーポイントを調べて、スキャン対象のコードを検索します。Contrast Scan によって調査される代表的なデータエントリーポイントの例は、以下のようになります。



## Contrast Scan のサポート対象テクノロジー

Contrast Scan は、以下の言語をサポートします。

言語	ファイル形式
Java(例 : J2EE、JSP、Spring MVC など)	JAR ファイル、WAR ファイル
JavaScript	JS ファイル、ZIP ファイル
<ul style="list-style-type: none"><li>• Angular バージョン 8 以降</li><li>• JQuery(全てのバージョン)</li><li>• React バージョン 16 以降</li><li>• Vue.js 2 以降</li><li>• TypeScript 4.2 以降</li></ul>	

### スキャンパッケージの準備

スキャンで最良の結果を得るには、スキャンするパッケージをアップロードする前に、以下のベストプラクティスを参考に準備してください。

### アーティファクトの種類

- Java の場合、WAR または JAR パッケージのいずれかをアップロードしてください。
- JavaScript の場合、JS または ZIP パッケージをアップロードしてください。

### クラスファイルと依存関係へのアクセス

パッケージ化されたファイルが、ここで説明しているものと異なる場合には、Contrast Scan はコードについて仮定を立てます。そのため、得られる結果が正確では無くなる可能性があります。検知漏れや誤検知になる可能性があります。

Contrast Scan がすべての必要なクラスファイルと依存関係にアクセスできれば、結果に擬似クラスは含まれることはありません。擬似クラスとは参照されるクラスですが、スキャンでそのバイトコードを検出できないか、もしくはスキャンで中間表現(IR)に逆コンパイルできないものを指します。

- Contrast Scan は、以下のファイルへのアクセスが必要です。
  - アプリケーションのクラスファイル
  - アプリケーションの依存関係にある JAR ファイルやクラスファイル
- Oracle Java™ の仕様に従って、アプリケーションおよび依存関係を WAR ファイルで構成してください。
- Spring Boot の JAR ファイルと同様に、アプリケーションおよび依存関係を JAR ファイルで構成してください。  
Spring Boot JAR ファイルは、アプリケーションと依存関係を既知の場所に配置します。
- 標準の JDK ファイルや一般的なサーブレットコンテナが提供する依存関係は含める必要はありません。Contrast Scan 側で、これらの依存関係を提供します。

### フレームワーク

正確な結果を得るために、Web アプリケーションで使用されているフレームワークが Contrast Scan のサポート対象である必要があります。

Contrast Scan は、次のフレームワークに対応しています。

- Angular 8 以降
- J2EE
- Jakarta EE 2.0-3.0
- jQuery
- React 16 以降
- SpringBoot

- Spring MVC
- Vue.JS 2 以降

## シン JAR ファイルの使用回避

シン JAR(thin JAR)ファイルは、アプリケーションのバイトコードのみを含むファイルです。これらのファイルには、依存関係に動的にアクセスするための特別な実行ローダーが必要です。シン JAR ファイルをアップロードした場合、アプリケーションコードのスキャンは実行されません。正確なスキャンのためのアプリケーションの依存関係へのアクセスができません。

## スキャンプロジェクトの作成

スキャンプロジェクトは、スキャンしたいアーティファクトのためのコンテナです。

スキャンプロジェクトを作成すると、アップロードするファイルの最初のスキャンを開始できます。

## 開始する前に

- スキャン用にアップロードするアーティファクトを準備します。  
スキャンでは、プログラミング言語ごとに異なるファイル形式をサポートしています。例えば、Java の場合は、JAR ファイルまたは WAR ファイルをアップロードして下さい。

## 手順

1. Contrast Web インターフェイスで、右上の **新規登録** を選択します。



このオプションは、Contrast Scan が有効な場合に利用できます。このオプションが利用できない場合は、[サポートにお問い合わせ](#)ください。

2. ローカルファイルのスキャンプロジェクトを追加を選択します。そして、次へを選択します。



3. プロジェクトの名前を入力します。  
スキャンプロジェクトの名前は一意である必要があります。また、Contrast 内でスキャンプロジェクトを簡単に識別できるような名前を指定してください。  
アーティファクトの名前と一致するようなプロジェクト名を付けることをお勧めします。例えば、アーティファクトが `webgoat.jar` であれば、プロジェクトの名前を `webgoat` や `webgoat.jar` などとします。
4. プロジェクトに含まれるファイルの言語を選択します。

## Contrastを使い始める

Contrastで、アプリケーション、コード、オープンソースライブラリを解析すると、潜在的な脆弱性やセキュリティリスクが表示されます。

手順1  
スキャンプロジェクトの作成

スキャンプロジェクトの名前を指定

同一言語のスキャンプロジェクトが存在する場合にユニーク名が必要

スキャンプロジェクト名

3文字以上を入力

スキャンプロジェクトの言語

Java(.war、.jar)

JavaScript(.js、.zip)

.NET(.exe、.zip)

既存のスキャンプロジェクトを全て表示

プロジェクト作成

5. プロジェクト作成を選択します。

## スキャンプロジェクトの削除

スキャンプロジェクトを完全に削除したい場合、以下の手順で削除することができます。プロジェクトに関連付けられた全てのデータが完全に削除されます。

この操作は元に戻すことができません。

### 手順

[en]

1. Contrast Web インターフェイスのナビゲーションバーで**スキャン**を選択します。
2. スキャンプロジェクトを選択します。
3. 設定アイコン(⚙️)を選択します。
4. 「スキャンプロジェクトの設定」の画面で、**削除**を選択します。





5. 「プロジェクトを削除」の画面で削除を選択して、プロジェクトを削除することを確定します。



## スキャンの開始

次の様な作業を実行したい場合に、スキャンを開始します。

- 新しいアプリケーションの解析
- 以前にスキャンし、アプリケーションの脆弱性を修正したコードのテスト

## 開始する前に

- 再度スキャンするファイルを含むスキャンプロジェクトを選択するか、新たにプロジェクトを作成する

## 手順

1. Contrast Web インターフェイスのナビゲーションバーでスキャンを選択します。
2. スキャンプロジェクトを選択します。
3. 新規スキャンを選択します。

+ 新規スキャン

4. 表示された画面から、アップロードするファイルを選択し、開くまたはアップロードを選択します。

スキャンプロジェクトに以前のスキャンがある場合は、以前にスキャンしたファイルの新しいバージョンを選択します。

ファイルのアップロードが完了すると、自動的にスキャンが開始されます。

5. [スキャンの確認 \(506ページ\)](#)でスキャンの進行状況を確認します。

## スキャンのキャンセル

進行中のスキャンをキャンセルできます。

スキャンをキャンセルすると、スキャン履歴でのステータスが「キャンセル」に変わります。

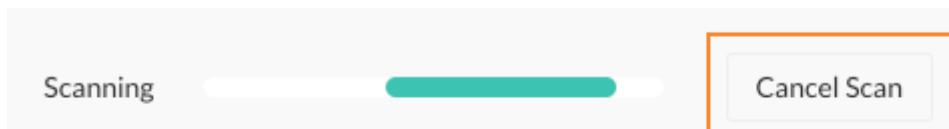
### 開始する前に

進行中のスキャンプロジェクトを検索します。

### 手順

スキャンをキャンセルするには：

1. Contrast Web インターフェイスのナビゲーションバーでスキャンを選択します。
2. 進行中のスキャンプロジェクトを選択します。
3. アクティビティバーのスキャンをキャンセルを選択します。



スキャンはすぐに停止します。

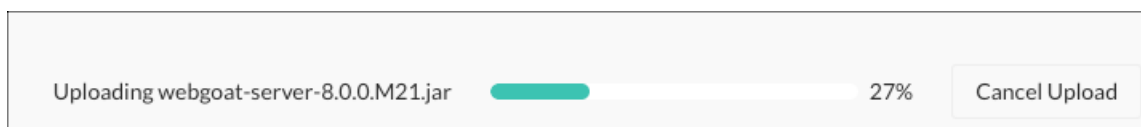
## スキャンの確認

スキャンを開始した後、スキャンのどのタブでもファイルのアップロードとスキャンの進行状況を確認することができます。

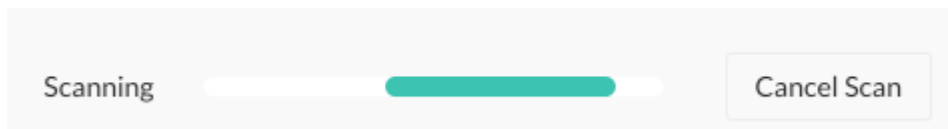
選択したプロジェクトのスキャン履歴は、概要タブに表示されます。

### 手順

1. Contrast Web インターフェイスのナビゲーションバーでスキャンを選択します。  
スキャンのページでは、スキャンに関する以下の情報が表示されます。
  - 各スキャンプロジェクトのスコア
  - スキャンプロジェクトの名前
  - オープン中の脆弱性の数とステータス
  - 最後のスキャンが完了した時間
2. スキャンプロジェクトを選択します。
3. [スキャンの開始 \(505ページ\)](#)
4. ファイルのアップロード中やスキャンの実行中は、スキャンページの上で進行状況を確認することができます。
  - ファイルのアップロード中は、以下のようなプログレスバーが表示されます：



- ファイルスキャン中は、以下のようなアクティビティバーが表示されます：



5. 選択したプロジェクトのスキヤンの履歴を確認するには、スキヤン画面で**概要タブ**を選択してスキヤン履歴を表示します。

Vulnerabilities	Label	Scan Date	Language	Coverage
37 <span style="color: red;">7</span>	2022-04-28 13:34:28	1 分前	Java	<a href="#">View</a>
37 <span style="color: red;">7</span>	2022-04-28 13:29:43	6 分前	Java	<a href="#">View</a>
3	2022-04-05 14:37:15	3 週間前	Java	<a href="#">View</a>

Results per page: 10

6. スキヤンの詳細を表示するには、スキヤンのラベル列の日時を選択するか、カバレッジ列の表示を選択します。

## Contrast Scan ローカルエンジン

Contrast Scan ローカルエンジンを使用すると、Contrast CLI または Contrast Web インターフェイスの代わりに、Docker CLI コマンドまたは Java JAR ファイルを使用してアプリケーションをスキヤンできます。スキヤンが正常に完了すると、Contrast Scan ローカルエンジンによって結果が Contrast プラットフォームにアップロードされ、そこで結果を確認することができます。アップロードされるのは以下のファイルです。

- 静的分析結果形式(SARIF)で記述されたスキヤン結果の JSON ファイル
- スキヤンの出力情報の LOG ファイル

この方法は、スキヤンするファイルを Contrast プラットフォームにアップロードせずに、ローカルでスキヤンしたい場合に便利です。

## サポート対象プラットフォーム

Contrast Scan ローカルエンジンは、Linux システムと Docker コンテナでサポートされています。

## ローカルスキヤンでのプロキシサーバの設定

セキュリティ上の理由から、ローカルスキヤンエンジンと Contrast プラットフォーム間の通信にプロキシサーバを使用している場合があります。[ローカルスキヤンを実行 \(510ページ\)](#)する際にプロキシサーバを有効にするには、以下の環境変数を使用してください。

変数	説明
CONTRAST_API_PROXY_ENABLE	プロキシの設定を有効にします。
CONTRAST_API_PROXY_URL	<b>必須</b> プロキシサーバの URL(例、http://host:port)
CONTRAST_API_PROXY_TYPE	<b>必須</b> プロキシサーバの方式(例、BASIC)
CONTRAST_API_PROXY_USERNAME	<b>任意</b> プロキシサーバのユーザ名
CONTRAST_API_PROXY_PASSWORD	<b>任意</b> プロキシサーバのパスワード

## スキヤンの手順

Contrast Scan ローカルエンジンを使用するには：

- ローカスキャンの実行方法を選択します。
  - Contrast Security から、ローカスキャナアプリケーションが含まれる [Docker コンテナをダウンロード \(508ページ\)](#)
  - [Contrast Scan ローカルエンジンの JAR ファイルをダウンロード \(508ページ\)](#)
- 検査結果のアップロードにプロキシサーバを使用するかどうかを判断します。
- [ローカルシステムでスキャンを実行 \(510ページ\)](#)します。
- Contrast Web インタフェースで[結果を確認 \(513ページ\)](#)します。

## Docker コンテナのダウンロード

Contrast ローカスキャナを使用するには、Contrast の GitHub リポジトリから Docker コンテナをダウンロードします。

Docker コンテナの代わりに Java JAR ファイルを使用する場合は、[JAR ファイル \(508ページ\)](#)をダウンロードしてください。

### 開始する前に

- [Docker CLI をインストール](#)します。
- Docker に 12GB のメモリを割り当てるよう設定します。
- 個人用アクセストークン(PAT)を [Contrast サポート](#)から入手します。

### 手順

- ローカルシステムで次の変数を設定します。

```
export CONTRAST_PAT=<ContrastProvidedPAT>
```

<ContrastProvidedPAT>は、Contrast サポートから入手した PAT に置き換えて下さい。

- 次のコマンドを使用して、リポジトリにログインして Docker コンテナをダウンロードします。

```
docker login ghcr.io/contrast-security-inc -u local-scanner -p \  
$CONTRAST_PAT  
docker pull ghcr.io/contrast-security-inc/contrast-sast-scanner-  
java:latest
```

## Java JAR ファイルのダウンロード

Contrast ローカスキャンエンジンの Java JAR ファイルをダウンロードするには、以下のいずれかを使用します。

- Maven からダウンロードする
- curl コマンドでダウンロードする

### 開始する前に

- 個人用アクセストークン(PAT)を [Contrast サポート](#)から入手します。

### Maven からダウンロード

- 以下の情報を含む POM(Project Object Model)ファイルを作成します。

```
<server>  
  <username>local-scanner</username>  
  <password>ContrastProvidedPAT</password>  
  <id>github</id>  
</server>
```

```
<repository>
  <id>github</id>
  <name>github</name>
  <url>https://maven.pkg.github.com/Contrast-Security-Inc/sast-local-
scan-runner</url>
</repository>

<dependency>
  <groupId>com.contrastsecurity</groupId>
  <artifactId>sast-local-scan-runner</artifactId>
  <version>latest</version>
</dependency>
```

ContrastProvidedPAT は、Contrast サポートから入手した PAT に置き換えて下さい。

2. POM ファイルを右クリックして**実行(Run As) > Maven Install** を選択するか、`mvn install` コマンドを使用します。

### curl コマンドでダウンロード

- Java JAR ファイルをダウンロードするには、次の curl コマンドを使用します。

```
curl -L -H 'Accept: application/vnd.github.v3.raw' -s https://
<ContrastProvidedPAT>@maven.pkg.github.com/Contrast-Security-Inc/sast-
local-scan-runner/com.contrastsecurity.sast-local-scan-runner/
<VersionNumber>/sast-local-scan-runner-<version number>.jar -o \
scanner.jar
```

- <ContrastProvidedPAT>は、Contrast サポートから入手した PAT に置き換えて下さい。
- <VersionNumber>を特定のバージョン番号に置き換えるか、latest を指定して最新バージョンをダウンロードして下さい。利用可能なバージョンについて、確認が必要であれば、Contrast の担当者までお問い合わせください。

### ローカルスキャンエンジン環境変数

Contrast Scan ローカルエンジンで、以下の環境変数を使用できます。

変数	必須/任意	説明
CONTRAST_API_URL	必須	スキャン結果を報告する Contrast プラットフォームのアドレスを指定します。URL の後ろに /api/sast を追加してください。
CONTRAST_API_USER_NAME	必須	Contrast のユーザアカウントのユーザ名(通常、自分のログイン ID)
CONTRAST_API_API_KEY	必須	Contrast API キー
CONTRAST_API_SERVICE_KEY	必須	Contrast サービスキー
CONTRAST_API_ORGANIZATION	必須	Contrast の組織 ID
CONTRAST_API_PROXY_ENABLE	任意	プロキシの設定を有効にします。
CONTRAST_API_PROXY_URL	プロキシ設定が有効な場合は必須	プロキシサーバの URL(例、http://host:port)
CONTRAST_API_PROXY_TYPE	プロキシ設定が有効な場合は必須	プロキシサーバの方式(例、BASIC)
CONTRAST_API_PROXY_USERNAME	任意	プロキシサーバのユーザ名
CONTRAST_API_PROXY_PASSWORD	任意	プロキシサーバのパスワード
UMBRELLA_LAUNCHER_JAVA_PATH	任意	Umbrella Java のスキャナ jar ファイルのパス(例、/app/contrast-scan-java-cli.jar)

## ローカルスキャンの実行

Contrast Scan ローカルエンジンは、Docker コンテナまたは Java JAR ファイルとして提供されます。スキャンを実行するために、ビルドした成果物が必要です。

### 開始する前に

- スキャンしたいビルド済み成果物の場所を確認します。
- スキャン結果をローカルシステム上のどこに保存するかを決めます。  
出力結果のパスを指定しない場合、ローカル エンジンは結果を `results.sarif` という名前のファイルで現在の作業ディレクトリに書き込みます。
- Contrast Scan ローカルエンジンの JAR 版を使用する場合、以下のソフトウェアがシステムにインストールされていることを確認します。
  - Java 11
  - JavaScript のプロジェクトファイルをスキャンする場合、Semgrep App バージョン 0.114.0
- ローカルスキャナがスキャン結果とスキャナ出力を Contrast にアップロードできるように、インターネットに接続してください。
- 1CPU(Contrast Scan ローカルエンジンはシングルスレッド)、12GB の RAM があることを確認します。

### 手順

1. Contrast Web インタフェースにログインします。
2. ユーザメニューより、**ユーザの設定**を選択します。
3. プロファイルにある、「あなたのキー」のセクションの以下の情報を取得します：
  - 組織 ID
  - あなたの API キー
  - サービスキー
  - Contrast URL

#### 4. ローカルスキャナが Contrast と通信するための環境変数を設定します。



#### 注記

ローカルスキャンエンジンと Contrast プラットフォーム間の通信にプロキシサーバを使用する場合は、[プロキシサーバの環境変数 \(507ページ\)](#)も指定します。

```
export CONTRAST__API__URL=<URL>
export CONTRAST__API__USER_NAME=<Username>
export CONTRAST__API__API_KEY=<APIKey>
export CONTRAST__API__SERVICE_KEY=<ServiceKey>
export CONTRAST__API__ORGANIZATION=<OrgId>
export LOCAL_ARTIFACT_LOCATION=<LocalArtifactLocation>
export LOCAL_OUTPUT_LOCATION=<LocalOutputLocation>
```

- <URL>は、スキャン結果を報告する Contrast の URL アドレスに置き換えます。URL の後ろに /api/sast を追加してください。
- <Username> は、自分の Contrast アカウント(通常はログイン ID)に置き換えます。
- <APIKey>は、Contrast の API キーに置き換えます。

- <ServiceKey>は、Contrast のサービスキーに置き換えます。
- <OrgID>は、Contrast の組織 ID に置き換えます。
- <LocalArtifactLocation>は、スキャンしたいファイルがあるフォルダのパスに置き換えます。

**オプション**：変数を使用する代わりに、コマンドでパスを指定することもできます。

- <LocalOutputLocation>は、スキャン結果のファイルを保存するローカルシステムのパスに置き換えます。

**オプション**：変数を使用する代わりに、コマンドでパスを指定することもできます。

#### 5. スキャンを開始します。

- **Docker 版**のローカルエンジンを使用する場合、次のコマンドでスキャンを開始します。

```
docker run -v $LOCAL_ARTIFACT_LOCATION:/app/artifacts \
-v $LOCAL_OUTPUT_LOCATION:/app/results \
-e CONTRAST__API__URL=${CONTRAST__API__URL} \
-e CONTRAST__API__USER_NAME=${CONTRAST__API__USER_NAME} \
-e CONTRAST__API__API_KEY=${CONTRAST__API__API_KEY} \
-e CONTRAST__API__SERVICE_KEY=${CONTRAST__API__SERVICE_KEY} \
-e CONTRAST__API__ORGANIZATION=${CONTRAST__API__ORGANIZATION} \
ghcr.io/contrast-security-inc/contrast-sast-scanner-java:latest \
--project-name "<ProjectName>-${CONTRAST__API__ORGANIZATION}" \
--label "<LabelName>" \
/app/artifacts/<FileName> \
-o $LOCAL_TARGET_OUTPUT_LOCATION/results.sarif
```

- <ProjectName>は、スキャンプロジェクトの名前に置き換えます。
- <LabelName>は、スキャンのラベルに置き換えます。例えば、ビルド番号を"build:1.0.1"のように指定できます。
- <FileName>は、スキャンしたいファイルの名前に置き換えます。このファイルは、\$LOCAL\_ARTIFACT\_LOCATION で指定したディレクトリに存在する必要があります。
- **Java JAR 版**のローカルエンジンを使用する場合、次のコマンドでスキャンを開始します。

```
java -jar sast-local-scan-runner.jar <ScanArtifact> --project- \
name <ProjectName> --label <LabelName>
```

- <ScanArtifact>は、スキャンする JAR、WAR、または ZIP ファイルのパスに置き換えます。また、フォルダを指定することもできます。
- <ProjectName>は、スキャンプロジェクトの名前に置き換えます。例："my project name"
- <LabelName>は、スキャンのラベルに置き換えます。例えば、ビルド番号を"build:1.0.1"のように指定できます。

#### 6. スキャン完了後、数分待つと、Contrast Web インタフェースに結果が表示されます。アップロードと処理時間の関係で、結果はすぐに表示されません。

### コマンドのオプション

Docker コンテナまたは Java JAR ファイルで、次のコマンドオプションが使用できます。

オプション	説明
-o, --output-results	出力結果の保存場所を指定します。 指定しない場合、ローカルスキャナは現在の作業ディレクトリに結果を書き込みます。
-v, --version	バージョン情報を表示します。



オプション	説明
<code>--project-name</code> <code>&lt;ProjectName&gt;</code>	<p>スキャンプロジェクトの名前を指定します。</p> <p>既に存在するプロジェクト名を指定した場合、ローカルエンジンはそのプロジェクトにスキャンを追加します。存在しない場合は、指定された名前の新しいプロジェクトを作成します。</p> <p>プロジェクト名にスペースが含まれる場合は、二重引用符(")で囲んでください。例: "My Scan Project"</p> <p>プロジェクト ID を使用しない場合、このオプションは必須です。</p>
<code>--project-ID</code>	<p>既存のプロジェクトの ID を指定します。</p> <p>プロジェクト名を使用しない場合、このオプションは必須です。</p>
<code>--label &lt;label&gt;</code>	このスキャンのラベルを指定します。

## 終了コード

ローカルエンジンは、スキャンが完了すると以下の終了コードを返します。

終了コード	説明
0	スキャンは正常に終了し、結果を Contrast にアップロードしました。
1	入力値の検証エラーです。
2	Contrast API サーバへの接続エラーです。
3	Contrast API サーバからエラーが返されました。
4	ローカルエンジンがエラーを返しました、詳細はログファイルにあります。
5	予期せぬエラーが発生しました、詳細はログファイルにあります。

## ローカルスキャン結果の確認

Contrast Web インターフェイスでローカルスキャンの詳細と結果が確認できます。

出力結果の場所を指定した場合、スキャンによってローカルシステムに作成された SARIF ファイルも見ることができます。

## 手順

1. Contrast Web インタフェースにログインします。
2. スキャンタブを選択します。
3. リストからローカルスキャンのスキャンプロジェクトを選択します。
4. ローカルスキャンの結果を表示するには、概要、脆弱性、ポリシーのタブを選択してください。Contrast ドキュメントには、[スキャン結果の分析](#)に関する詳細情報があります。

## スキャン結果の分析

スキャンは、アプリケーション内のデータフローを観察し、検出した脆弱性を報告します。

結果を調査した後、アプリケーションのコードを修正して再度スキャンを実行し、脆弱性が修正されているか確認します。

## 手順

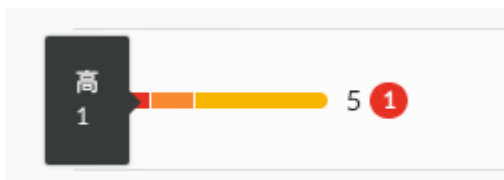
スキャン完了後の脆弱性の情報を確認するには：

1. Contrast Web インターフェイスのナビゲーションバーでスキャンを選択します。スキャンのページでは、スキャンプロジェクトの一覧が表示されます。
2. 検出された脆弱性の一覧とその深刻度を表示するには：
  - a. スキャンプロジェクトを選択します。
  - b. 概要タブで脆弱性の数をクリックするか、脆弱性タブを選択します。

The screenshot shows the Contrast Security dashboard with the following elements:

- Navigation tabs: 概要 (Overview), 脆弱性 (Vulnerabilities), ポリシー (Policy). The 脆弱性 tab is active.
- Summary cards: A red card with 'F' and '55/100'; a blue-bordered card with '5' labeled '脆弱性'; another blue-bordered card with '5' labeled '新たな脆弱性'; a green card with '0' labeled '修復済'; a blue card with '1' labeled 'スキャン完了'; and a blue card with '17' labeled '前回のスキャンからの経過日数'.
- Buttons: '+ 新規スキャン' (New Scan).
- Section: 'スキャン履歴' (Scan History) with '全て (1)' (All (1)).
- Table: A table with columns for '脆弱性' (Vulnerability), 'ラベル' (Label), 'スキャン日付' (Scan Date), '言語' (Language), and 'カバレッジ' (Coverage). The first row shows a vulnerability with a score of 5 and 1, scanned on 2023-04-17 19:17:20, in Java, with a '先月' (Last Month) label and a '表示' (Show) button.

また、特定のステータスの脆弱性を表示するには、ステータスにある脆弱性の棒グラフで該当部分をクリックします。



- 脆弱性タブで、脆弱性をステータスや深刻度でソートするには、ステータスまたは深刻度の列の横にあるフィルタアイコン( )を選択し、1つまたは複数の項目を選択します。  
深刻度のフィルタ :



ステータスのフィルタ :



フィルタをクリアするには、深刻度またはステータス列の横にある**クリア**を選択します。

4. 特定の脆弱性に関する詳細情報を表示するには、脆弱性タブで該当の脆弱性を選択します。
  - 選択した脆弱性の概要タブには、アプリケーションコードで発生した内容や脆弱性に関するリスクなど、脆弱性の説明が表示されます。
5. 脆弱性の詳細やアプリケーションコード内での脆弱性の場所を参照するには、**詳細**タブを選択すると次の情報が表示されます。
  - 脆弱性が存在するメソッド
  - スキャンによって脆弱性が検出されたファイル
  - スキャンによって脆弱性が検出されたアプリケーションコードの最初の行
6. コードの修正方法を参照するには、**修正方法**タブを選択します。
7. 脆弱性に関するその他の詳細情報は、**備考**タブを選択すると、次のような情報が表示されます。
  - 脆弱性の検出時間
  - 脆弱性が検出されたコードモジュール
  - 脆弱性の種類(インジェクションなど)
  - 深刻度
  - リスクの信頼性
  - 脆弱性に適用されるセキュリティ基準
8. 脆弱性に関するアクティビティを参照したい場合、**アクティビティ**タブを選択すると、次のような情報が表示されます。
  - 変更を行ったユーザ
  - 脆弱性のステータスの変更
  - コメント

## スキャン情報の表示

スキャン情報には、以下が含まれます。

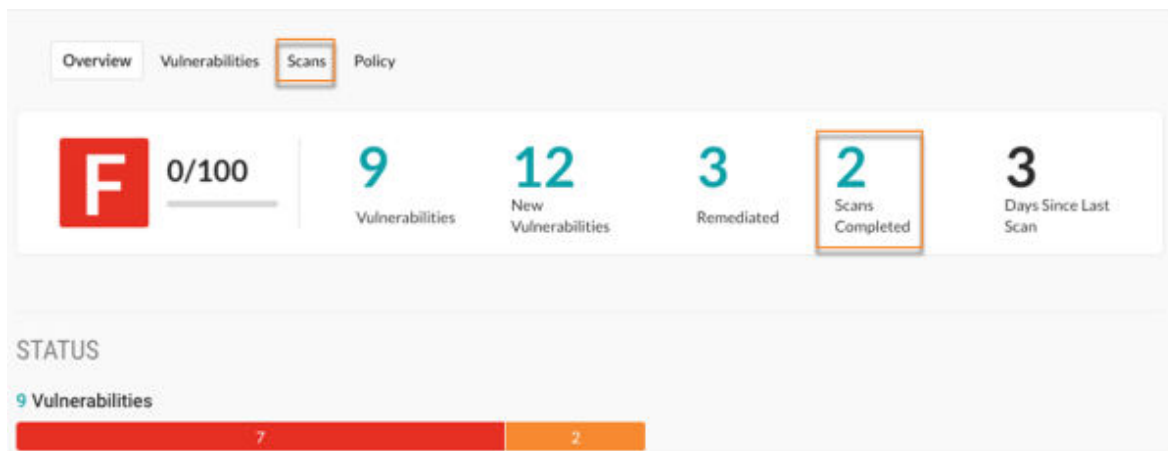
- スキャン結果の概要
- スキャンのカバレッジ詳細

## 開始する前に

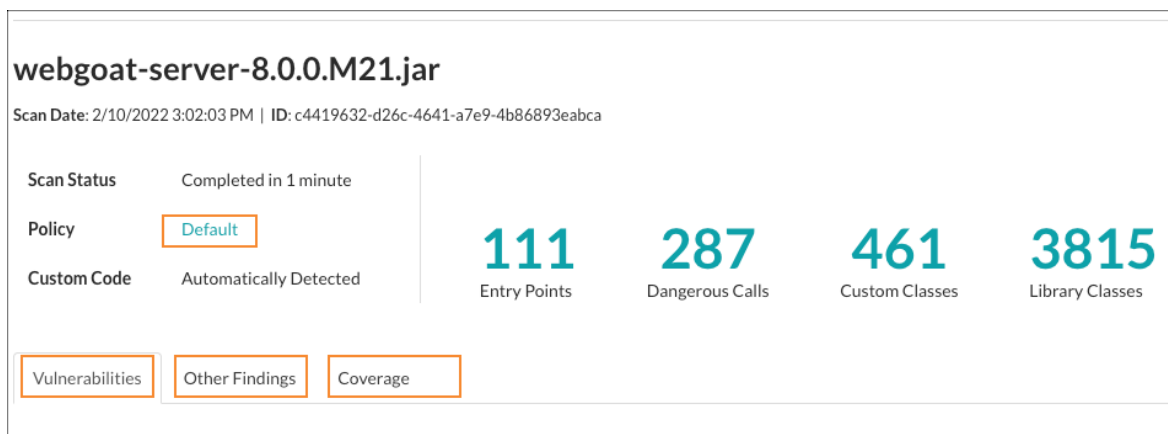
- 情報を表示したいスキャン(スキャンプロジェクト)を決めます。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーでスキャンを選択します。
2. スキャンプロジェクトを選択します。
3. スキャン完了の数字を選択するか、スキャンタブを選択します。



4. 「スキャン履歴」でスキャンを選択するか、カバレッジ列で表示を選択します。
5. スキャンの詳細が表示されます。



- 一覧の上部に、スキャンの詳細の概要が表示されます。スキャンで使用されたルールを表示するには、ポリシーの横のデフォルトを選択します。
- 「脆弱性」タブに、スキャンで検出された脆弱性が表示されます。この一覧にある脆弱性は、対策が必要であると確信されるものです。
- 「その他の検出結果」タブに、スキャンで検出されたその他の脆弱性が表示されます。これらの脆弱性の報告時にスキャンで行われた仮定により、この一覧にある脆弱性への対策の必要性はより低くなります。
- 「カバレッジ」タブに、スキャンに含まれたクラスとスキャンの対象外となったクラスが表示されます。

## スキャン結果のダウンロード

スキャンが完了したら、結果を SARIF(Static Analysis Results Interchange Format)ファイルでダウンロードできます。これは静的解析データを出力するための標準的な JSON 形式のファイルです。

ストレージの使用量を最適化するため、ダウンロードが可能なのは、スキャン完了後 5 日間です。それより古いスキャンはダウンロードできません。

## 開始する前に

- 結果をダウンロードするスキャンを決めます

## 手順

1. Contrast Web インターフェイスのナビゲーションバーでスキャンを選択します。
2. スキャンプロジェクトを選択します。
3. スキャン履歴からスキャン結果をダウンロードするには、該当スキャンの行の最後にカーソルを合わせ、ダウンロードアイコン(📄)を選択します。
4. スキャンの詳細ページからスキャン結果をダウンロードするには：
  - a. スキャン履歴でスキャンを選択するか、カバレッジ列の表示を選択します。
  - b. 概要タブまたは脆弱性タブで、ダウンロードアイコン(📄)を選択します。

## SARIF ファイルのデータ

スキャンの結果は、SARIF ファイルでダウンロードできます。

SARIF は、静的解析結果を記述する標準的なデータモデルでシリアル化された出力形式です。SARIF ファイルのデータを理解することで、スキャンの結果をより深く考察できます。

SARIF ファイルには、次のような情報が含まれます。

- Contrast が使用するスキャナに関する情報
- スキャン対象とスキャン構成に関するデータ
- 脆弱性の検出結果に関するデータ
- スキャン中に適切に処理されたエラーや通知内容
- スキャンのカバレッジ情報

## スキャナの情報

Contrast で使用したスキャナに関する情報は、以下の例のようになります。

```
5   "tool" : {
6     "driver" : {
7       "name" : "Contrast Scan",
8       "organization" : "Contrast Security, Inc.",
9       "version" : "pkg: 2.0.0-SNAPSHOT, engine: 2.0.0-SNAPSHOT, policy: 2.0.0-SNAPSHOT",
10      "informationUri" : "https://www.contrastsecurity.com"
11    }

```

## 脆弱性の情報

ここでは、1つの脆弱性のデータを例として使用します。スキャンによる脆弱性の検出結果は、results セクションにあります。

### • オブジェクト

以下は、SQL インジェクションの脆弱性についてのスキャン結果の例です。threadFlows セクションにあるオブジェクトは、ソースからシンクまでのスキャン情報を示します。

```

13  "artifacts" : [ ],
14  "results" : [ {
15    "ruleId" : "sql-injection",
16    "level" : "error",
17    "message" : {
18      "text" : "sql-injection in User.fetch() reachable from LoginController.login()"
19    },
20    "locations" : [ {
21      "physicalLocation" : {
22        "artifactLocation" : {
23          "uri" : "file:///github/workspace/src/main/java/com/scalesec/vulnado/User.java"
24        },
25        "region" : {
26          "startLine" : 49,
27          "startColumn" : 1,
28          "snippet" : {
29            "text" : "public static User fetch(String un) {\n  ...\n  rs = stmt.executeQuery(query);    // Java line
30              49\n  ...}\n"
31          }
32        },
33        "contextRegion" : {
34          "snippet" : { }
35        }
36      } ],
37      "partialFingerprints" : {
38        "GITHUB_SOURCECODE_LSH/v1" :
39          "e86a7a0c38715f4a:1-158823731d54d12e:1-6b692237789f9a2a:1-64ed8e6526b79cf4:1-13db8c734146ff90:1"
40      },
41      "codeFlows" : [ {
42        "message" : {
43          "text" : "Untrusted data flow from LoginController.java:19 to User.java:49 via variable `query`"
44        },
45        "threadFlows" : [ {
46          "locations" : [ {
47            "location" : {
48              "physicalLocation" : {
49                "artifactLocation" : {
50                  "uri" : "com/scalesec/vulnado/LoginController.java"
51                },
52                "region" : {
53                  "startLine" : 19,
54                  "snippet" : {
55                    "rendered" : {
56                      "text" : "@CrossOrigin(origins={\"*\"})\n@RequestMapping(value=\"/login\"), method={\"POST\"},
57                        produces={\"application/json\"}, consumes={\"application/json\"})\nLoginResponse login(**@RequestBody
58                          LoginRequest input**) {\n  ...\n}"
59                    }
60                  }
61                },
62                "properties" : {
63                  "ir" : [ "@CrossOrigin(origins={\"*\"})\n@RequestMapping(value=\"/login\"), method={\"POST\"},
64                    produces={\"application/json\"}, consumes={\"application/json\"})\nLoginResponse login(**@RequestBody
65                      LoginRequest input**) {", " ...", "}" ]
66                }
67              }
68            }
69          ]
70        }
71      } ]
72    }
73  ]
74 }

```

## • シンクの場合

脆弱性の問題がある場所やシンクの例です。

```

"locations" : [ {
  "physicalLocation" : {
    "artifactLocation" : {
      "uri" : "file:///github/workspace/src/main/java/com/scalesec/vulnado/User.java"
    },
    "region" : {
      "startLine" : 49,
      "startColumn" : 1,
      "snippet" : {
        "text" : "public static User fetch(String un) {\n  ...\n  rs = stmt.executeQuery(query);    // Java line
          49\n  ...}\n"
      }
    },
    "contextRegion" : {
      "snippet" : { }
    }
  }
}

```

## • スレッドフローのステップ

データフローの実行ステップの例です。

```

44     "threadFlows" : [ {
45         "locations" : [ {
46             "location" : {
47                 "physicalLocation" : {
48                     "artifactLocation" : {
49                         "uri" : "com/scalesec/vulnado/LoginController.java"
50                     },
51                     "region" : {
52                         "startLine" : 19,
53                         "snippet" : {
54                             "rendered" : {
55                                 "text" : "@CrossOrigin(origins={\"*\"})\n@RequestMapping(value={\"/login\"}, method={\"POST\"},
56                                     produces={\"application/json\"}, consumes={\"application/json\"})\nLoginResponse login(**@RequestBody
57                                     LoginRequest input**) {\n  ...\n}"
58                             }
59                         },
60                     "properties" : {
61                         "ir" : [ "@CrossOrigin(origins={\"*\"})\n@RequestMapping(value={\"/login\"}, method={\"POST\"},
62                             produces={\"application/json\"}, consumes={\"application/json\"})\nLoginResponse login(**@RequestBody
63                             LoginRequest input**) {\", \" ...\", \"} ]
64                     }
65                 },
66             "logicalLocations" : [ {
67                 "name" : "LoginController.login()",
68                 "fullyQualifiedName" : "com.scalesec.vulnado.LoginController.login(com.scalesec.vulnado.LoginRequest)"
69             } ]
70         } ],
71     }, {
72         "location" : {
73             "physicalLocation" : {
74                 "artifactLocation" : {
75                     "uri" : "com/scalesec/vulnado/LoginController.java"
76                 },
77                 "region" : {
78                     "startLine" : 20,
79                     "snippet" : {
80                         "rendered" : {
81                             "text" : "@CrossOrigin(origins={\"*\"})\n@RequestMapping(value={\"/login\"}, method={\"POST\"},
82                                     produces={\"application/json\"}, consumes={\"application/json\"})\nLoginResponse login(@RequestBody
83                                     LoginRequest input) {\n  ...\n  $stack0 = input.username; // Java line 20\n  user = User.fetch
84                                     ($stack0); // Java line 20\n  ...\n}"
85                         }
86                     },
87                     "properties" : {
88                         "ir" : [ "$stack0 = input.<com.scalesec.vulnado.LoginRequest:java.lang.String username>; // Java
89                             line 20\", \"user = staticinvoke <com.scalesec.vulnado.User: com.scalesec.vulnado.User fetch(java.lang.
90                             String)>($stack0); // Java line 20\" ]
91                     }
92                 }
93             },
94             "logicalLocations" : [ {
95                 "name" : "LoginController.login()",
96                 "fullyQualifiedName" : "com.scalesec.vulnado.LoginController.login(com.scalesec.vulnado.LoginRequest)"
97             } ],
98             "message" : {
99                 "text" : "un"
100             }
101         } ],
102     }, {
103         "state" : {
104             "un" : {
105                 "text" : "tainted",
106                 "properties" : {
107                     "taintTags" : [ "untrusted", "cross-site" ]
108                 }
109             }
110         }
111     } ]

```

#### • 脆弱性の物理的および論理的な場所

ここでの例は、脆弱性がある物理的および論理的な場所を示しています。

このセクションには、中間表現(IR)データのコードスニペットやレンダリングデータを含めた実行ステップの情報があります(通常はユーザコードは表示されません)。Contrastはこのデータを使用して、スキャンで確認する内容を解析します。

1. 中間表現(IR)の実行ステートメントの例です。
2. アプリケーションで実行ステップが発生する場所を示す例です。

```
44     "threadFlows" : [ {
45       "locations" : [ {
46         "location" : {
47           "physicalLocation" : {
48             "artifactLocation" : {
49               "uri" : "com/scalesec/vulnado/LoginController.java"
50             },
51             "region" : {
52               "startLine" : 19,
53               "snippet" : {
54                 "rendered" : {
55                   "text" : "@CrossOrigin(origins={\"*\"})\n@RequestMapping(value={\"/login\"},
56                     method={\"POST\"}, produces={\"application/json\"}, consumes={\"application/
57                     json\"})\nLoginResponse login(**@RequestBody LoginRequest input**) {\n ...}\n"
58                 }
59               }
60             }
61           }
62         },
63         "logicalLocations" : [ {
64           "name" : "LoginController.login()",
65           "fullyQualifiedName" : "com.scalesec.vulnado.LoginController.login(com.scalesec.
66             vulnado.LoginRequest)"
67         } ]
68       } ]
69     } ]
```

- **信頼できないデータの所在**

ここでの例は、スキャンで検出された信頼できないデータを示しています。

スキャンは、コードソースからデータシンクまでの実行ステップを調べます。スキャン結果には、信頼できないデータに触れる全ての実行ステップが含まれます。

importance(重要性)の結果が essential(必要)な場合は、このコードの部分に脆弱性がないかを確認する必要があります。

1. スキャンが追跡する汚染データの場所を示す例です。
2. 追跡対象のデータが実行ステップで扱われる場所を示す例です。スキャン結果は、importance(重要性)が essential(必要)であることが分かります。このコードでは脆弱性を確認する必要があります。



```

"location" : {
  "physicalLocation" : {
    "artifactLocation" : {
      "uri" : "com/scalesec/vulnado/User.java"
    },
    "region" : {
      "startLine" : 47,
      "snippet" : {
        "rendered" : {
          "text" : "public static User fetch(String un) {\n  ..\n  $stack0 = new\n  StringBuilder(); // Java line 47\n  $stack1 = \"select * from users where\n  username = \""; // Java line 47\n  $stack0 = $stack0.append($stack1); //\n  Java line 47\n  $stack0 = $stack0.append(un); // Java line 47\n  $stack1 =\n  \"' limit 1\"; // Java line 47\n  $stack0 = $stack0.append($stack1); //\n  Java line 47\n  query = $stack0.toString(); // Java line 47\n  ..\n}"
        }
      }
    },
    "message" : {
      "text" : "Propagation event of untrusted data occurred at 'User.java:47' in the\n  method 'User.fetch()' to variable 'query'"
    },
    "properties" : {
      "ir" : [ "$stack0 = new java.lang.StringBuilder; // Java line 47", "$stack1 =\n  \"select * from users where username = \"; // Java line 47", "$stack0 =\n  virtualinvoke $stack0.<java.lang.StringBuilder: java.lang.StringBuilder append\n  (java.lang.String)>($stack1); // Java line 47", "$stack0 = virtualinvoke\n  $stack0.<java.lang.StringBuilder: java.lang.StringBuilder append(java.lang.String)>\n  (un); // Java line 47", "$stack1 = \"' limit 1\"; // Java line 47", "$stack0\n  = virtualinvoke $stack0.<java.lang.StringBuilder: java.lang.StringBuilder append\n  (java.lang.String)>($stack1); // Java line 47", "query = virtualinvoke $stack0.\n  <java.lang.StringBuilder: java.lang.String toString>(); // Java line 47" ]
    }
  }
},
"logicalLocations" : [ {
  "name" : "User.fetch()",
  "fullyQualifiedName" : "com.scalesec.vulnado.User.fetch(java.lang.String)"
} ],
"message" : {
  "text" : "query"
}
},
"state" : {
  "query" : {
    "text" : "tainted",
    "properties" : {
      "taintTags" : [ "untrusted", "cross-site" ]
    }
  }
}
},
"importance" : "essential"

```

## スキャン結果の分析

ここでは、SARIF ファイルの内容でスキャン結果の分析に役立つ情報について、いくつか例を用いて説明します。

### データの追跡に使用されたクラス

これらのクラスは、スキャンの実行時間に影響します。

```
2344 "scannedData" : {
2345   "scannedBodyClasses" : [ "com.scalesec.vulnado.ServerError",
2346     "com.scalesec.vulnado.LoginResponse",
2347     "org.springframework.lang.UsesSunMisc",
2348     "com.scalesec.vulnado.Postgres",
2349     "com.scalesec.vulnado.LinksController",
2350     "com.scalesec.vulnado.BadRequest",
2351     "com.scalesec.vulnado.Unauthorized",
2352     "com.scalesec.vulnado.Comment",
2353     "org.springframework.lang.NonNullFields",
2354     "org.springframework.lang.NonNull",
2355     "org.springframework.lang.UsesJava7",
2356     "org.springframework.lang.UsesJava8",
2357     "com.scalesec.vulnado.CowController",
2358     "com.scalesec.vulnado.LoginController",
2359     "org.springframework.lang.NonNullApi",
2360     "org.springframework.lang.Nullable",
2361     "org.springframework.lang.UsesSunHttpServer",
2362     "com.scalesec.vulnado.CommentsController",
2363     "com.scalesec.vulnado.Cowsay",
2364     "com.scalesec.vulnado.VulnadoApplication",
2365     "com.scalesec.vulnado.LoginRequest",
2366     "com.scalesec.vulnado.LinkLister",
2367     "com.scalesec.vulnado.User",
2368     "java.util.Optional",
2369     "com.scalesec.vulnado.CommentRequest" ],
```

- **型階層の解決に使用したクラス**

ここに表示されるクラスは、スキャンで型の階層を解決するためだけに使用されています。ライブラリのクラスは、セキュリティの問題に関連していないか、または関連する API に対する特定のポリシーが Contrast にあります。このセクションに表示されるクラスがカスタムコードに関連している場合、スキャン結果に検知漏れや誤検知の可能性がります。

```

2134 "nonScannedBodyClasses" : [
2135   "java.nio.file.WatchEvent$Modifier",
2136   "java.awt.Color", "java.awt.peer.WindowPeer",
2137   "java.util.function.IntUnaryOperator",
2138   "sun.awt.datatransfer.DataTransferer",
2139   "java.awt.JobAttributes$MultipleDocumentHandlingType",
2140   "java.lang.Integer",
2141   "java.awt.image.SampleModel",
2142   "javax.swing.border.Border",
2143   "java.awt.peer.ScrollbarPeer",
2144   "java.util.Vector",
2145   "java.sql.DriverAction",
2146   "java.sql.SQLType",
2147   "org.springframework.core.ParameterizedTypeReference$1",
2148   "java.nio.file.Path",
2149   "java.nio.channels.Channel",
2150   "org.springframework.core.io.Resource",
2151   "java.awt.peer.ContainerPeer",
2152   "javax.swing.KeyStroke",
2153   "java.lang.CharSequence",
2154   "java.awt.dnd.DropTargetDragEvent",
2155   "java.time.temporal.TemporalField",
2156   "org.springframework.beans.factory.InjectionPoint",
2157   "java.util.logging.ErrorManager",
2158   "java.awt.Scrollbar",
2159   "java.io.Serializable",
2160   "java.util.concurrent.CompletionStage",
2161   "java.lang.LayerInstantiationException",
2162   "org.jsoup.parser.Token$EndTag",
2163   "java.lang.invoke.BoundMethodHandle$Specializer$Factory",
2164   "java.lang.invoke.MemberName",
2165   "java.util.function.ToDoubleFunction",
2166   "java.io.ObjectInputStream$GetField",

```

#### • 擬似クラス

擬似(phantom)クラスとは、参照されるクラスですが、スキャンでそのバイトコードを検出できないか、もしくはスキャンでコードを中間表現(IR)に逆コンパイルできないものを指します。

スキャン結果に擬似クラスが含まれないことが理想的です。スキャン結果に擬似クラスが含まれる場合、より正確な結果を提供するための情報をスキャンで検出できなかったことを意味します。このセクションにアプリケーションコードまたはライブラリが表示されている場合は、コードを調べて問題が存在するかどうかを確認してください。

```

2400 "phantomClasses" : [ "BOOT-INF.classes.com.scalesec.vulnado.LoginController",
2401   "javax.annotation.Nonnull",
2402   "groovy.lang.Closure",
2403   "javax.annotation.meta.TypeQualifierDefault",

```

#### • 信頼できないデータのルート検出

ここでの例は、信頼できないデータがアプリケーションに入るルートが検出されたことを示しています。

スキャンは、このセクションに表示されている関数からのデータフローの動きのみを調べます。脆弱な暗号化など、データフローに関連する他の機能については解析されません。

```
2769     "routesDiscovered" : [ {
2770         "routeSignature" : "com.scalesec.vulnado.LoginController.login(com.scalesec.vulnado.
LoginRequest)"
2771     }, {
2772         "routeSignature" : "com.scalesec.vulnado.CowController.cowsay(java.lang.String)"
2773     }, {
2774         "routeSignature" : "com.scalesec.vulnado.CowController.cowsay2(java.lang.String)"
2775     }, {
2776         "routeSignature" : "com.scalesec.vulnado.LinksController.links(java.lang.String)"
2777     }, {
2778         "routeSignature" : "com.scalesec.vulnado.LinksController.linksV2(java.lang.String)"
2779     }, {
2780         "routeSignature" : "com.scalesec.vulnado.CommentsController.comments(java.lang.String)"
2781     }, {
2782         "routeSignature" : "com.scalesec.vulnado.CommentsController.createComment(java.lang.String,com.
scalesec.vulnado.CommentRequest)"
2783     }, {
2784         "routeSignature" : "com.scalesec.vulnado.CommentsController.deleteComment(java.lang.String,
java.lang.String)"
2785     } ]
2786 },
2787 "invocations" : [ {
2788     "commandLine" : "java -XX:MaxRAMPercentage=80 -jar /app/contrast-scan-java-cli.jar
--prescan-metadata /tmp/
cb9757b4-4fdf-4de9-bdf1-7769058307eb_e1a6403d-be7c-46ee-82aa-6b7e47ce97d2_metadata.json -o /tmp/
results.sarif.json /tmp/
cb9757b4-4fdf-4de9-bdf1-7769058307eb_e1a6403d-be7c-46ee-82aa-6b7e47ce97d2_vulnado-0.0.1-SNAPSHOT.
jar",
2789     "toolExecutionNotifications" : [ ],
2790     "executionSuccessful" : true

```

## スキャンポリシーの表示

Contrast がアプリケーションコード内でどのような脆弱性を検索するかを確認するには、ポリシーを表示します。

現時点では、ポリシーの編集や追加はサポートされていません。

1. Contrast Web インターフェイスのナビゲーションバーで**スキャン**を選択します。
2. スキャンプロジェクトを選択します。
3. **ポリシー**を選択します。  
スキャンに使用されるポリシーが一覧で表示されます。
4. ポリシータブでは、検索ボックスに 1 文字以上の文字を入力して特定のポリシーを検索できます。


## スキャン設定の変更

スキャン設定では、スキャンプロジェクトの名前を変更することができます。

### 開始する前に

- 管理者権限(Admin ロール)が必要です。

### 手順

1. Contrast Web インターフェイスのナビゲーションバーで**スキャン**を選択します。
2. スキャンプロジェクトを選択します。
3. 画面の右上にある**設定アイコン**()を選択します。
4. プロジェクトの新しい名前を入力します。
5. **保存**を選択します。

## スキャンプロジェクトのアーカイブ

特定のスキャンプロジェクトをスキャンプロジェクトの一覧から外したい場合(例えば、そのプロジェクトを使用しなくなった場合など)、スキャンプロジェクトをアーカイブすることができます。

アーカイブされたプロジェクトに関連するデータは、Contrast で保持されます。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーで**スキャン**を選択します。
2. スキャンプロジェクトを選択します。
3. 設定アイコン(⚙️)を選択します。
4. 「スキャンプロジェクトの設定」の画面で、**アーカイブ**を選択します。

5. 「プロジェクトをアーカイブ」の画面で、**アーカイブ**を選択します。  
フィルタで「アーカイブ済」を選択しない限り、アーカイブされたプロジェクトは一覧に表示されなくなります。

## スキャンプロジェクトのアーカイブ解除

アーカイブされたスキャンプロジェクトの情報を表示・使用するには、アーカイブを解除します。

### 開始する前に

- 組織の Admin ロールが必要です。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーで**スキャン**を選択します。
2. スキャンの一覧の上部にある小さい三角形(▼)を選択し、**アーカイブ済**を選択して、アーカイブされたプロジェクトを表示します。
3. プロジェクトの行の最後にカーソルを合わせ、**アーカイブを解除**のアイコン(🗑️)を選択します。
4. 「プロジェクトのアーカイブを解除」の画面で、**アーカイブを解除**を選択します。

## ビルドパイプラインでのインテグレーション

[Contrast CLI \(575ページ\)](#)には、Contrast Web インターフェイスを使用せずにスキャンを実行できるコマンドがあります。

本項では、Contrast CLI を使用してビルドパイプラインにスキャンを組み込む手順について説明します。

[Contrast Maven プラグイン \(661ページ\)](#)を使用して、プロジェクトの Maven ビルドに Contrast Scan を組み込むこともできます。

### 開始する前に

- Contrast Web インターフェイスのユーザメニューより**ユーザの設定 > プロファイル**を選択し、以下の情報を取得してください。
  - API キー

- 組織 ID
  - Contrast URL
  - 認証ヘッダー
- WAR ファイルまたは JAR ファイルがアクセス可能な場所にあることを確認してください。

## 手順

1. お使いのビルドパイプラインのワークフローに、最新バージョンの Contrast CLI をダウンロードするコマンドを追加します。

```
npm install --location=global @contrast/contrast@2.0.0
```

2. API キー、組織 ID、Contrast URL、認証ヘッダーの環境変数を設定します。  
以下は、GitHub のシークレットを使用して環境変数を設定する例です。ご利用の環境に適した方法をご使用ください。

```
CT_API_KEY: ${ secrets.CONTRAST__API__API_KEY }
CT_AUTH_TOKEN: ${ secrets.CONTRAST__API__AUTH_TOKEN }
ORG_ID: ${ secrets.CONTRAST__API__ORGANIZATION_ID }
URL: ${ secrets.CONTRAST__API__URL }
```

3. スキャンを開始するために、以下のようなコマンドを追加します。

```
contrast-cli --scan ../scan-cli-testing/java/apps/param.war \
--api_key $CT_API_KEY \
--authorization $CT_AUTH_TOKEN \
--organization_id $ORG_ID \
--host $URL \
--project_name MY-Project \
--language JAVA --wait_for_scan
```

このコマンドを初めて実行すると、`--project_name` オプションで指定した名前でプロジェクトが作成されます。

コマンドの出力は、次のサンプルのようになります。

```
project created ID is 788f9734-b933-4f05-b391-c130931baf88
Uploaded file successfully.
Response: {
  id: '5091d134-93ea-4873-8110-8cf99d14606e',
  organizationId: '74f4cd04-6ca9-4eb7-a7a7-78909c2101cc',
  projectId: '788f9734-b933-4f05-b391-c130931baf88',
  filename: 'param.war',
  createTime: '2022-04-04T10:06:16.952+00:00'
}
Timeout set to 5 minutes
Waiting for results...
New Results: 5
Fixed Results: 0
Total Results: 5
```

次回、同じプロジェクトに対してこのコマンドを実行すると、アップロードするファイルがそのプロジェクトに追加されます。コマンドの出力は、次のサンプルのようになります。

```
project already exists with this name. Getting ID...
project ID is 788f9734-b933-4f05-b391-c130931baf88
Uploaded file successfully.
Response: {
  id: '94b4e065-0e0f-46bb-b1d8-9f85bd03c602',
  organizationId: '74f4cd04-6ca9-4eb7-a7a7-78909c2101cc',
```

```

projectId: '788f9734-b933-4f05-b391-c130931baf88',
filename: 'param.war',
createdTime: '2022-04-04T10:07:01.230+00:00'
}

```

Timeout set to 5 minutes

Waiting for results...

New Results: 5

Fixed Results: 0

Total Results: 5

4. スキャン完了後、Contrast Web インターフェイスにスキャンプロジェクトの詳細と結果が表示され  
ます。

The screenshot shows the Contrast Web interface for a project named 'MY-Project'. The top navigation bar includes 'Contrast', 'アプリケーション', 'スキャン' (highlighted with a red box), 'サーバ', 'ライブラリ', '脆弱性', '攻撃', and 'サーバレス'. Below the navigation bar, the project name 'MY-Project' is displayed with '言語: Java' and '前回のスキャン: 30秒前'. The main content area shows a summary of scan results:

- Overall score: **F** 0/100
- 脆弱性 (Vulnerabilities): **37**
- 新たな脆弱性 (New vulnerabilities): **0**
- 修復済 (Fixed): **0**
- スキャン完了 (Scans completed): **2**
- 前回のスキャンからの経過日数 (Days since last scan): **0**

Below the summary, there is a section for 'スキャン履歴' (Scan History) showing a list of scans. The table has columns for '脆弱性' (Vulnerabilities), 'ラベル' (Label), 'スキャン日付' (Scan Date), '言語' (Language), and 'カバレッジ' (Coverage).

脆弱性	ラベル	スキャン日付	言語	カバレッジ
37		2022-04-29 19:28:44	Java	表示
37		2022-04-29 19:20:51	Java	表示

At the bottom right, there is a pagination control showing '1ページごとの表示件数 10'.

## インテグレーションの例

- [GitHub にスキャンを組み込む \(527ページ\)](#)
- [Jenkins にスキャンを組み込む \(528ページ\)](#)

### 例 : GitHub にスキャンを組み込む

GitHub に Contrast Scan を組み込む前にスキャンのインテグレーション手順 (525ページ) について確認してください。

以下は、GitHub のワークフローに Contrast Scan を設定する例です。

```

- name: Set up contrast-cli
2 run: |
3 npm install --location=global @contrast/contrast@2.0.0
4- name: Scan file
5 env:
6 CT_API_KEY: ${{ secrets.CONTRAST__API__API_KEY }}
7 CT_AUTH_TOKEN: ${{ secrets.CONTRAST__API__AUTH_TOKEN }}
8 ORG_ID: ${{ secrets.CONTRAST__API__ORGANIZATION_ID }}
9 URL: ${{ secrets.CONTRAST__API__URL }}

```

```
10 run: |
11 contrast-cli --scan ./target/${{ inputs.SERVICE_NAME }}-${{ steps.build-
12 --api_key $CT_API_KEY \
13 --authorization $CT_AUTH_TOKEN \
14 --organization_id $ORG_ID \
15 --host $URL \
16 --project_name MY-Project \
17 --language JAVA --wait_for_scan
```

## 例：Jenkins にスキャンを組み込む

Jenkins に Contrast Scan を組み込む前に [スキャンのインテグレーション手順 \(525ページ\)](#) について確認してください。

Contrast Security は、Jenkins パイプラインに Contrast Scan を組み込むためのスクリプトを提供しています(これらのスクリプトにアクセスするには、[サポートにお問い合わせください](#))。

- **Jenkins パイプラインスクリプト**： Jenkins\_Script\_SCAN スクリプトでは、Contrast Scan ローカルエンジンの JAR ファイルを使用します。プロジェクトの JAR ファイルが、GitHub リポジトリにあることを前提としています。
- **Docker コンテナで使用する Jenkins パイプラインスクリプト**： Jenkins\_Script\_SCAN\_GH\_Container\_Image スクリプトでは、パイプラインスクリプトで [Docker コンテナ \(508ページ\)](#) を使用します。

## インテグレーション手順

この例では、Contrast Scan を Jenkins に組み込むための設定方法について説明します。

1. ご利用のローカル環境に Jenkins インスタンスをセットアップします([Jenkins のドキュメント](#)を参照ください)。 Jenkins のインスタンスが既にある場合は、この手順をスキップしてください。
2. 以下のソフトウェアをインストールします(まだインストールしていない場合)：
  - Java 11
  - 使用している環境用のプラグイン(例えば、Docker プラグイン)
3. 新しいパイプラインを作成し、Contrast のスクリプトをコピーします。
4. Contrast の認証情報をグローバル変数または環境変数に設定します。  
例：URL、USER\_NAME、API\_KEY、SERVER\_KEY、ORGANIZATION、CONTRAST\_PAT
  - CONTRAST\_PAT には、Contrast サポートからお客様に提供される個人用アクセストークン(PAT)を指定します。PAT のアクセス権により、GitHub にログインし、Contrast Scan ローカルエンジンのファイルをダウンロードできます。
  - Jenkins に認証情報を追加するには、**Jenkins の管理 > Manage Credentials > 認証情報の追加 (Secret Text として)**を選択します。
5. お使いのパイプラインスクリプトで、全ての認証情報と変数を参照してください。

## サーバ

Contrast Web インターフェイスのサーバページで、サーバに関する情報を表示して、各環境(開発、テストおよび本番)ごとにサーバを設定することができます。そして、各環境でコードを実行して環境間の違いを比較できます。Contrast では、サーバを指定するためのシエルが用意されます。シエルが設定されると、Contrast で脆弱性の検知が始まります。

## サーバの設定

Contrast での各サーバエントリは、アプリケーションに組み込んだ Contrast エージェントに設定した値によって表されます。各エージェントで以下を設定すると、新規に一意的なサーバエントリが作成されます。



サーバのカスタム設定を定義するには、エージェントの設定ファイルで以下のオプションを使用します。

- **サーバ名(server name)** : デフォルト値は、ホスト名です。
- **サーバパス(server path)** : エージェントのプロセスが実行されているパス。
- **サーバタイプ(server type)** : アプリケーションをホストしているサーバの種類。

これらの設定にデフォルトの値ではなくカスタム値を使用することで、サーバエントリの重複を避けることができます。

以下の設定でサーバの環境を指定します。

- **サーバの環境(server environment)** : このサーバを使用する環境。  
有効な値は、DEVELOPMENT、QA、PRODUCTION です。これらの値では、大文字と小文字を区別しません。デフォルト値は、DEVELOPMENT です。

Contrast エージェントは、サポート対象となる全てのサーバタイプを自動的に認識します。サーバタイプが自動的に認識されない場合は、サポート対象外のテクノロジーでエージェントが実行されている可能性があります。各[エージェント \(31ページ\)](#)のサポート対象テクノロジーのセクションをご確認ください。サポート対象外の環境での実行は、ルートカバレッジなどの一部の機能に影響が出る可能性があります。

## 設定ファイルの定義

以下は、サーバに関するプロパティで、設定ファイルでカスタムの値を指定できます。

```
# server
# Use the settings in this section to set
# metadata for the server hosting this agent.

server:

  # Override the reported server name.
  name: localhost

  # Override the reported server path.
  path: NEEDS_TO_BE_SET

  # Override the reported server type.
  type: NEEDS_TO_BE_SET

  # Override the reported server environment.
  # environment: DEVELOPMENT
```

## エージェントの設定手順

サーバのカスタム設定を定義する際は、使用しているエージェントの各設定手順を参照してください。

- [.NET Core エージェントの設定 \(213ページ\)](#)
- [.NET Framework エージェントの設定 \(152ページ\)](#)
- [Go エージェントの設定 \(456ページ\)](#)
- [Java エージェントの設定 \(78ページ\)](#)
- [Node.js エージェントの設定 \(262ページ\)](#)
- [Python エージェントの設定 \(319ページ\)](#)
- [Ruby エージェントの設定 \(397ページ\)](#)

## オプションの設定

Contrast Web インターフェイスには、サーバを設定するためのその他のオプションがあります。

- [サーバの設定 \(530ページ\)](#)
- [Syslog への出力 \(531ページ\)](#)

## サーバの設定

サーバの設定画面より、各環境(開発、テスト、本番)でサーバがどのように機能するかを設定できます。

### 手順

1. Contrast Web インターフェイスのナビゲーションバーで、**サーバ**を選択します。
2. 以下のいずれかの方法で、設定を変更するサーバを検索します。
  - サーバ列の上部にあるフィルターアイコン(▼)を選択
  - 虫眼鏡のアイコン(🔍)を使用して検索
3. 以下のいずれかの方法で、「サーバの設定」にアクセスします。
  - サーバの行の最後にカーソルを合わせ、**設定アイコン(⚙)**を選択
  - サーバの名前を選択してドリルダウンして、画面右上の**設定アイコン(⚙)**を選択
4. 必要に応じて、設定を変更します。
  - サーバ名を変更する。
  - サーバが稼働する環境(Development、QA、Production)を指定する。
  - 「サーバログファイル」のフィールドに、優先するパスを入力して、既存のサーバログファイルのパスを上書きする。



#### 注記

サーバのログファイルは、ファイル形式が.LOG または.TXT のみに制限されます。

- サーバの[ログレベル \(824ページ\)](#)を設定する。
- ポットのブロックを設定する。  
ポットをブロックすることで、スクレーパー、攻撃ツール、その他の自動化からの不要なトラフィックをブロックできます。  
ブロックされたポットのアクティビティを表示するには、**攻撃 > 攻撃イベント**で、フィルターに**自動化**を選択します。  
**サポート対象の言語**：Java、.NET Framework、.NET Core、Ruby、Python



#### 注記

ポットのブロックは、各言語(Java、.NET Framework、.NET Core、Ruby、Python)のエージェントの[YAML 設定ファイル \(38ページ\)](#)で指定できます。

- **パフォーマンス向上のためサンプリングを有効にする**を選択する。  
この設定は、Assess が有効な時に利用できます。  
サンプリングによって、リクエストが選別され、Contrast で繰り返しの解析を避けることができます。
  1. Contrast で同じ URL が複数回呼び出されているのが確認されると、「基準」の設定に指定した回数に基づいて URL が解析されます。
  2. その後、Contrast で同じ URL が引き続き確認された場合、「頻度」の設定に基づいてのみチェックが行われます。
  3. サンプルは、「サンプル保持」の設定で指定した秒数だけ保持されます。「サンプル保持」の設定で指定した時間が経過すると、「基準」の設定に従って再度 URL が解析されます。  
サンプリングには、以下を設定します。
    - **基準**：サンプリングが完了するまでに、Contrast で URL を解析する回数。デフォルトの設定は、**5**です。

- **頻度**：基準のサンプル回数を取得後、毎回 N 番目のリクエストのみを解析します。頻度には、N の値を指定します。デフォルトの設定は、**10** です。
- **サンプル保持画面**：基準に戻る前に、Contrast でサンプルを保持する秒数。指定した秒数が経過すると、サンプリングはリセットされ基準サンプルが再度行われます。デフォルトの設定は、**180** です。

例：

```
contrast.assess.sampling.request_frequency    25
contrast.assess.sampling.window_ms          360_000
contrast.assess.sampling.baseline            1
```

- [Syslog へ Protect イベントの出力を有効にする \(531ページ\)](#) を選択する。

この設定は、Protect が有効な時に利用できます。

サーバが syslog に出力する syslog メッセージの重要度レベルを選択します。Contrast で提供される syslog メッセージの重要度は、[syslog RFC 3164](#) の仕様に従って分類されます。

## Syslog への出力

Contrast では、Contrast Security のログだけでなく、リモートの syslog サーバにセキュリティログを送信できます。Syslog データは、共通イベント形式(CEF)で、ほとんどの SIEM(Security Incident Event Management)ソフトウェアで解析できます。



### 重要

Syslog 出力を有効にするサーバには、Protect ライセンスを適用する必要があります。

Syslog が外部メッセージを受信できるように、リモートログを有効にしなければならない場合があります。

サーバの Syslog メッセージは、エージェントによって送信されます。

Syslog 出力は TCP ではサポートされません。

1. 組織レベルで [サーバのデフォルト設定 \(713ページ\)](#) を指定する場合、**Syslog へ Protect イベントの出力を有効にする** のチェックボックスをオンにします。追加のフィールドが表示されるので、必要な設定を入力します。
2. Contrast Web インターフェイスのナビゲーションバーで **サーバ** を選択すると、サーバの一覧が表示されます。Syslog 出力の設定は、個々のサーバまたは同時に複数のサーバに有効にすることができます。Syslog のデフォルト値がすでに [組織レベルで設定 \(713ページ\)](#) されている場合は、サーバレベルでの設定時に値が事前に入力されます。
  - **個々のサーバ**：個々のサーバで syslog を有効にするには、該当サーバの行にカーソルを合わせ、**サーバの設定** アイコンを選択します。
  - **複数のサーバ**：チェックマークを使用して複数のサーバを選択し、ページの下部に表示される一括アクションメニューで **サーバの設定** アイコンを選択します。



### 注記

選択した 1 つ以上のサーバで syslog を有効にできない場合は、対象となるサーバでのみ syslog が有効になります。

3. **サーバの設定** 画面で、**Syslog へ Protect イベントの出力を有効にする** のチェックボックスをオンにします(複数サーバの場合、最初にチェックボックス横の **編集** をクリックする必要があります)。

**注記**

選択した対象のサーバが異なる環境にある場合は、該当するサーバのデフォルトの設定を使用するか、全てのサーバの設定を手動で構成するかを選択できます。

## サーバの一括設定



これを実行すると選択中の全てのサーバの設定が上書きされます。

環境

ログレベル

スタックトレース

ボットのブロック

 Edit パフォーマンス向上のためサンプリングを有効にする ? 編集 SyslogへProtectイベントの出力を有効にする 編集済

Syslogサーバホスト

ポート

機能

攻撃イベントの結果

攻撃検出済

疑わしい

ブロック済

ブロック済  
(P)

探査検出

Syslogメッセージの重要度

Undo edits

キャンセル

保存

4. **Syslog サーバホスト**を入力します。ここでは、完全修飾ドメイン名(ホスト名だけでなく)または IP アドレスを指定します。例：*email.mydomainname.com* や 38.124.154.50
5. **ポート**を入力します。

6. 機能を入力します。
7. **Syslog メッセージの重要度**を選択します。
8. 設定を保存すると、サーバで syslog が有効になります。
9. Syslog が有効になると、サーバの一覧でサーバ名の横に灰色の矢印アイコンが表示されます。アイコンにカーソルを合わせると、Protect イベントの出力場所を参照できます。  
サーバの設定を編集するには、上記のステップを繰り返して画面の必要な値を更新し、変更を保存してください。

## ライブラリ

アプリケーションで使用されるライブラリのセキュリティは、アプリケーション全体のセキュリティに影響を及ぼします。

ライブラリには、公開または内製のものがあります。公開ライブラリは、Maven (Java)、NuGet (.NET)、npm (Node.js)、RubyGems (Ruby)、PyPI (Python)、pkg.go (Go)、Composer (PHP)から提供されるオープンソースのライブラリで、Contrast では A から F の **スコア (544ページ)**が付けられます。内製のライブラリは、サードパーティ製の商用ライブラリや独自に作成されたカスタムライブラリです。内製のライブラリは、Contrast でスコア付けされません。

Contrast エージェントは、アプリケーションに含まれるオープンソースライブラリを自動的に識別します。ライブラリで検出された脆弱性を特定し、ライブラリがランタイムで使用されているのかも確認します。

そのため、Contrast でライブラリファイルのハッシュ値が作成されます。このハッシュ値を使用して、ファイルの内容が既知のライブラリファイルのデータベースと比較されます。データベースにハッシュがある場合は、ライブラリに **スコア (544ページ)**が割り当てられ、ライブラリのバージョン情報やライブラリで検出された全ての脆弱性情報(CVE)が Contrast サーバに報告されます。



### 注記

ライブラリがカスタムファイルの場合、ハッシュがデータベースに無いため、このライブラリは Contrast エージェントによって「不明(Unknown)」として報告されます。これは、最新のライブラリがリリースされたタイミングや、Contrast EOP(オンプレミス版)をエアギャップ環境で利用中で **ライブラリデータの更新 (770ページ)**をしていない場合にも発生することがあります。

Java クライアントの場合、WebSphere では実行時にライブラリが再パッケージ化されるため、SHA-1 ハッシュが Contrast で認識されるものとは異なります。デプロイ時に SHA-1 を保持するには、JVM システムプロパティ

```
org.eclipse.jst.j2ee.commonarchivecore.ignore.web.fragment  
を"true"に設定します。
```

また、全ての wsadmin の呼出しに同じパラメータが必要になります。

```
wsadmin -javaoption "-  
Dorg.eclipse.jst.j2ee.commonarchivecore.ignore.web.fragment=true  
"
```

Contrast Web インターフェイスのナビゲーションバーで **ライブラリ**を選択すると、ポートフォリオ内の全てのライブラリの概要を参照でき、ライブラリを一括管理できます。

- [ライブラリの表示 \(535ページ\)](#)
- [オープンソースライセンスの参照 \(543ページ\)](#)

- ライブラリのスコアについて (544ページ)

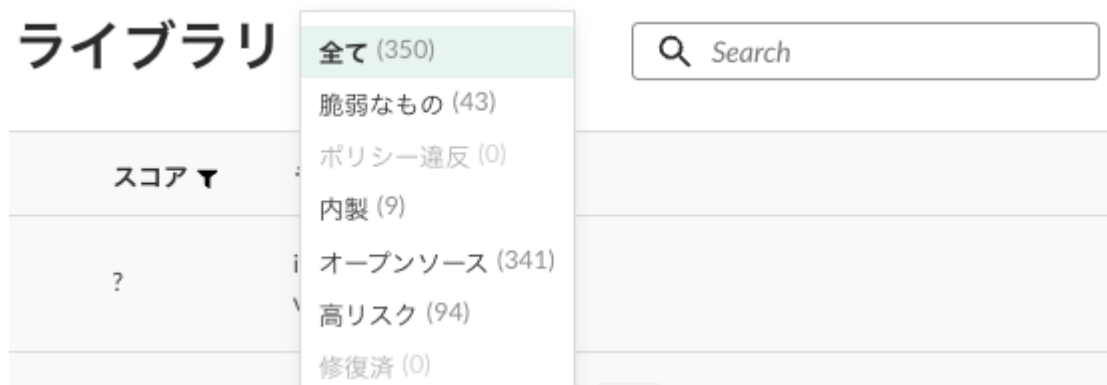
## 関連項目

[CVE 検索 \(545ページ\)](#)

## ライブラリの表示

ライブラリの情報を表示する方法はいくつかあります。

- Contrast Web インターフェイスのナビゲーションバーで**ライブラリ**を選択すると、組織で使用されている全てのライブラリが一覧で表示されます。より詳細な情報は、一覧でライブラリ名をクリックします。
- 個々のアプリケーションやサーバの詳細ページからも、ライブラリの情報を確認できます。
  - Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択し、アプリケーション名をクリックするとアプリケーションの詳細ページが表示されます。**ライブラリタブ**を選択します。
  - Contrast Web インターフェイスのナビゲーションバーで**サーバ**を選択し、サーバ名をクリックするとサーバの詳細ページが表示されます。**ライブラリタブ**を選択します。
- ライブラリ一覧の上部にある小さい三角形を選択すると、ライブラリの絞り込みができます。また、虫眼鏡のアイコンをクリックして、特定のライブラリを検索することもできます。



フィルタには次のものがあります。

- 全て**：全てのライブラリを表示します。
- 脆弱なもの**：CVE があると識別されたライブラリのみを表示します。
- ポリシー違反**：ライブラリポリシーに違反しているライブラリのみを表示します。
- 内製**：コード内で検出された商用のサードパーティ製ライブラリまたはカスタムビルドライブラリのみを表示します。
- オープンソース**：コード内で検出されたオープンソースのライブラリのみを表示します。
- 高リスク**：[スコア \(544ページ\)](#)が C 以下のライブラリのみを表示します。
- 修復済**：修復済のステータスのライブラリが表示されます。
- ライブラリページの上部にある**ライブラリ統計を表示**を選択すると、組織のライブラリデータの分析を参照できます。各図には、高リスクとなる年数やライブラリのスコアなど、各カテゴリの統計的な平均値と内訳が表示されます。  
ライブラリは、[スコア \(544ページ\)](#)の評価が C 以下の場合、リスクが高いとみなされます。

## 静的タブとランタイムタブ

Contrast でのライブラリ情報は、2つのタブに分かれます。

- 静的**：[Contrast CLI \(575ページ\)](#)で解析された **マニフェスト**(`package.json` や `pom.xml` など)からの検出結果が表示されます。
- ランタイム**：実行時に解析されたアプリケーションの検出結果が表示されます。

🔍 ライブラリ統計を表示

ライブラリ All (5001)  Static Runtime ↑ ソート順 スコア

スコア	ライブラリ	最新バージョン	脆弱性	アプリケーション	使用状況	処理
?	idna tagtest1 v2.8	?		django.nV	使用されていません 0/8	(1) 🗑️ 🔄 📄
F	snakeyaml-1.28.jar tagtest1 v1.28 (2021年2月22日)	2023年2月26日 v2.0	(7)	agent-metrics-3 protect-perf-baseline-#2	使用されていません 0/224	(1) 🗑️ 🔄 📄
F	jaakson-databind-2.12.5.jar tagtest1 v2.12.5 (2021年8月26日)	2023年1月28日 v2.14.2	(3)	agent-metrics-3 protect-perf-baseline-#2	352/701	(1) 🗑️ 🔄 📄
F	commons-fileupload-1.3.1.jar asdf tagtest1 v1.3.1 (2014年2月6日)	2018年12月24日 v1.4	(3)	WebGoat	3/49	(2) 🗑️ 🔄 📄
F	checker-qual-3.5.0.jar tagtest1 v3.5.0 (2020年7月1日)	2022年12月1日 v3.28.0		PF:1678677931 PF:1678683946 ImperialGoat	使用されていません 0/321	(1) 🗑️ 🔄 📄
F	snakeyaml-1.29.jar tagtest1 v1.29 (2023年6月9日)	2023年2月26日 v2.0	(7)	PF:1678677931 pocnonhttpweb PF:1678683946 ImperialGoat	使用されていません 0/226	(1) 🗑️ 🔄 📄
F	commons-text-1.9.jar tagtest1 v1.9 (2020年7月21日)	2023年9月24日 v1.10.0	(1)	WebGoat WebGoat-Metadata	14/135	(1) 🗑️ 🔄 📄
F	rack tagtest1 v2.2.3 (2020年6月15日)	2023年3月13日 v3.0.6.1	(5)	PF-RUBY:1678795327 PF-RUBY:1678795398 PF-RUBY:1678795335	40/65	(1) 🗑️ 🔄 📄
F	sqlite3 tagtest1 v1.4.2 (2019年12月18日)	2023年2月22日 v1.6.1		RailsEngine	11/23	(1) 🗑️ 🔄 📄
F	slf4j-log4j12-1.7.12.jar tagtest1 v1.7.12 (2015年3月26日)	2022年12月12日 v2.0.6		WebGoat	3/6	🗑️ 🔄 📄

Page 1 of 501 Results per page 10 25 50

一覧でフィルター付きの列ヘッダーを使用して、スコア、ライブラリ、深刻度、プロジェクト別にライブラリを絞り込むこともできます。ライブラリ一覧には、以下の項目が表示されます。

- **スコア**：ランタイムタブでのみ表示されます。スコアガイド (544ページ)に基づいて評価されたライブラリのスコアがレターグレードで表示されます。
- **深刻度**：静的タブでのみ表示されます。ここには、ライブラリに存在するすべての脆弱性(CVE)で最も重大な深刻度が表示されます。フィルタを使用して、深刻度に基づいてライブラリを検索できます。なお、フィルタの **Other** オプションは、最も重大な深刻度が無し(CVSS スコアが 0)で、CVE が無く、かつ内製か未知のライブラリであるものが検索されます。
- **ライブラリ**：一覧でライブラリ名をクリックすると、そのライブラリの詳細ページに移動します。詳細ページには、ライブラリが存在するアプリケーションとサーバのリスト、およびライブラリ内で Contrast が検出した既知の脆弱性(CVE)が表示されます。フィルタを使用して、結果を絞り込むことができます。
  - **言語**：特定の言語で脆弱なライブラリを検索
  - **ライセンス**：ライセンス毎にライブラリを表示
  - **環境**：環境ごとにライブラリを表示、本番環境の脆弱なライブラリを見つけるのに役立つ
  - **サーバ**：サーバタイプで脆弱なライブラリを検索
- **最新バージョン**：ライブラリの最新バージョン。



### 注記

.NET のライブラリに関して：最新バージョンの値は、パッケージのアップグレードが可能な推奨バージョンに関連しています。ライブラリのバージョンとハッシュは、Contrast エージェントが検出したファイルによって決定されます。ハッシュはライブラリファイルのバージョンを表し、最新バージョンに表示されるアップグレードバージョンは、パッケージのバージョンを表します。

- **脆弱性**：ライブラリで検出された CVE の情報。修復時の優先順位付けの目安となります。脆弱性の棒グラフにカーソルを合わせると、深刻度別の CVE 数が表示されます。棒グラフをクリックすると、詳細パネルが開きます。





脆弱性が存在する場合、一覧で表示され、深刻度別に色分けされます。深刻度が重大な脆弱性は、一覧の一番上に赤色で表示されます。

- **アプリケーション**：ランタイムタブでのみ表示されます。ライブラリを使用しているアプリケーションの一覧。
- **使用状況**：ランタイムタブでのみ表示されます。ライブラリ内のクラスの総数のうち、ランタイムで使用されているクラスの総数が表示されます。ランタイムで使用されていないクラスがない場合は、この列には「使用されていません」と表示されます。アプリケーションでクラスがロードされる時に、Contrast エージェントが使用状況を判断します。今まで使用されていなかったクラスの場合は、使用数は減少します。数字をクリックすると、[ライブラリの使用状況を分析 \(540ページ\)](#)できます。ここでは、ロードされたクラスの情報だけでなく、ライブラリに関連するリスクやポリシー違反の情報も確認することができます。
- **処理**：ランタイムタブでのみ表示されます。ここで、ライブラリに[タグ \(538ページ\)](#)を付けたり、送信や[削除 \(537ページ\)](#)を行うことができます。
- **ステータス**：ランタイムタブでのみ表示されます。ステータスを変更するには組織の [Edit \(819ページ\)](#) ロールが最低限必要です(ステータス列が表示されていない場合は、弊社サポートに連絡して、この列を有効にするよう依頼してください)。アプリケーション > アプリケーション名 > ライブラリタブにアクセスすると参照できます。表示/適用できるステータスには、3種類あります。
  - **問題無し**：このライブラリにある脆弱性は認識済みでリスクは許容できる、またはこのライブラリは使用されていない状況。
  - **修復済**：脆弱なライブラリに対応・対策済である状況。
  - **報告済**：Contrast で脆弱性のあるライブラリが検出された状況。
- **プロジェクト**：静的タブでのみ表示されます。ライブラリを使用しているプロジェクトが一覧表示されます。

## ライブラリの検出と削除



### 注記

ランタイムタブでのみ表示されます。静的に解析されたライブラリでは使用できません。

ライブラリは、ライブラリを使用するアプリケーションと、これらのアプリケーションがデプロイされているサーバに関連付けられています。

エージェントから送信されるライブラリ情報に、これまでに報告されたライブラリが含まれなくなると、そのライブラリにはそのサーバと関連付けがなくなります。

ライブラリを報告している全てのサーバからそのライブラリの情報が送信されなくなるか、そのライブラリを報告しているサーバが削除されると、アプリケーションからライブラリは削除されます。(サーバの削除は、サーバの [設定 \(713ページ\)](#)に従います)。

ライブラリは、アプリケーションから手動で削除することもできます。

ライブラリを削除するには：

1. Contrast Web インターフェイスのナビゲーションバーで、**ライブラリ**を選択し、ライブラリ一覧から削除するライブラリの行を探します。

2. **処理列**にある**削除アイコン**をクリックします。このアイコンは、ライブラリの詳細ページの右上にもあります。  
複数のライブラリを一括で削除するには、左側の列でチェックマークを使用し、削除するライブラリを選択してから、ページの下部に表示される一括アクションバーから**削除アイコン**を選択します。



3. 表示される画面で、**削除**を選択して処理を確定します。処理を確定すると、ライブラリが削除されて一覧に表示されなくなります。エージェントが、以前に削除されたライブラリを報告した場合、そのライブラリはアプリケーションに含まれるため、ライブラリの一覧に再度追加されます。

## ライブラリへのタグの追加



### 注記

ランタイムタブでのみ表示されます。静的に解析されたライブラリでは使用できません。

ライブラリにタグを追加するには：

1. Contrast Web インターフェイスのナビゲーションバーで**ライブラリ**を選択して、タグを付けるライブラリの行を探します。
2. **処理列**にある**タグアイコン**を選択します。このオプションは、ライブラリの詳細ページの右上からもアクセスできます。



3. 表示される画面で入力を始めると、既に作成済みのタグの一覧が表示されます。既存のタグを使用する場合は、ドロップダウンから1つ以上のタグを選択します。もしくは、新規にタグを作成する場合は、フィールドに新しいタグを入力します。タグを外すには、タグ名の横にある**X**をクリックします。変更を保存するには、**保存**を選択します。
4. 複数のライブラリにタグを付けるには、ライブラリー覧の左側の列にあるチェックマークを使用してライブラリを選択します。ページの下部に表示される一括アクションメニューで、**タグアイコン**を選択します。
5. タグごとに絞り込むには、ライブラリー覧で**ライブラリ**列の横にあるフィルターを選択して、絞り込むタグを選択します。

# ライブラリ 全て (350) ▾



6. タグは、ライブラリの詳細ページでもライブラリ名の横に表示されます。タグの横にある X を選択すると、タグを外すことができます。

## ライブラリ情報の送信



### 注記

ランタイムタブでのみ表示されます。静的に解析されたライブラリでは使用できません。

脆弱なライブラリを追跡するために、電子メールアドレスや連携しているバグ管理システム(開発担当者のためにチケットを作成)に、ライブラリ情報を送信できます。

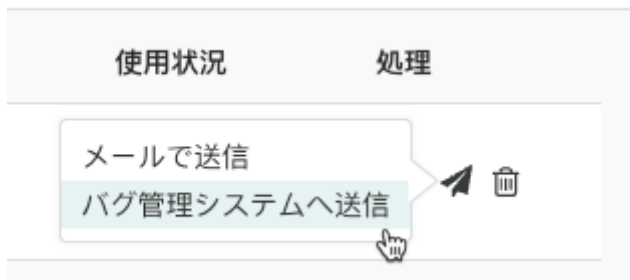
選択した各ライブラリに対して次のデータを、メールアドレスやバグ管理システムに Contrast から送信できます。

- ライブラリ名
- 使用中のバージョン
- 脆弱性(CVE)の情報
- 影響のあるアプリケーションとサーバ
- バージョンの遅れ(現在のバージョンと最新バージョンとの比較)
- 使用状況(現在、Java および .NET でのみサポート)
- [スコア \(544ページ\)](#)

ライブラリの情報を送信するには :

1. Contrast Web インターフェイスのナビゲーションバーで**ライブラリ**を選択し、追跡したいライブラリの行を探します。

2. 処理列にある送信アイコンをクリックしたら、メールで送信またはバグ管理システムへ送信を選択します。  
このオプションは、ライブラリの詳細ページの右上からもアクセスできます。



3. 表示する画面で、使用するバグ管理システム (618ページ)を選択します。オプションを選択し、送信を選択するとチケットが作成されます。メールで送信する場合は、Eメールアドレスを入力し、送信をクリックします。
4. 複数のライブラリの情報を送信する場合は、ライブラリ一覧の左側の列にあるチェックマークを使用して、ライブラリを選択します。ページの下部に表示される一括アクションメニューで、送信アイコンを選択します。選択した全てのライブラリには、共通のアプリケーションが少なくとも1つ必要です。

## ランタイムライブラリの使用状況の分析

ランタイムライブラリの使用状況を確認することで、ライブラリのどの部分がアプリケーションで実際に使用されているかを知ることができます。そして、ライブラリがアプリケーションに与える影響を把握できるため、脆弱性(CVE)に関する調査時間を短縮できます。また、セキュリティ担当者は、アプリケーションがランタイムで脆弱なライブラリを使用していることを開発担当者と一緒に確認できるので、作業の効率も向上します。



### 注記

Contrast SCA ライセンス (23ページ)のある組織のみで、使用状況の完全な情報を参照できます。詳細については、弊社営業担当の [JPNsales@contrastsecurity.com](mailto:JPNsales@contrastsecurity.com) にお問い合わせください。

Contrast Web インターフェイスのナビゲーションバーでライブラリを選択します。ランタイムをクリックして使用状況列を参照すると、実行時にライブラリが使用されているかどうか、およびどのくらい使用されているかを確認することができます。使用数は、そのライブラリで使用可能であることが判明している項目の合計数のうち、エージェントを組み込んだアプリケーションで使用されている項目の数を表します。

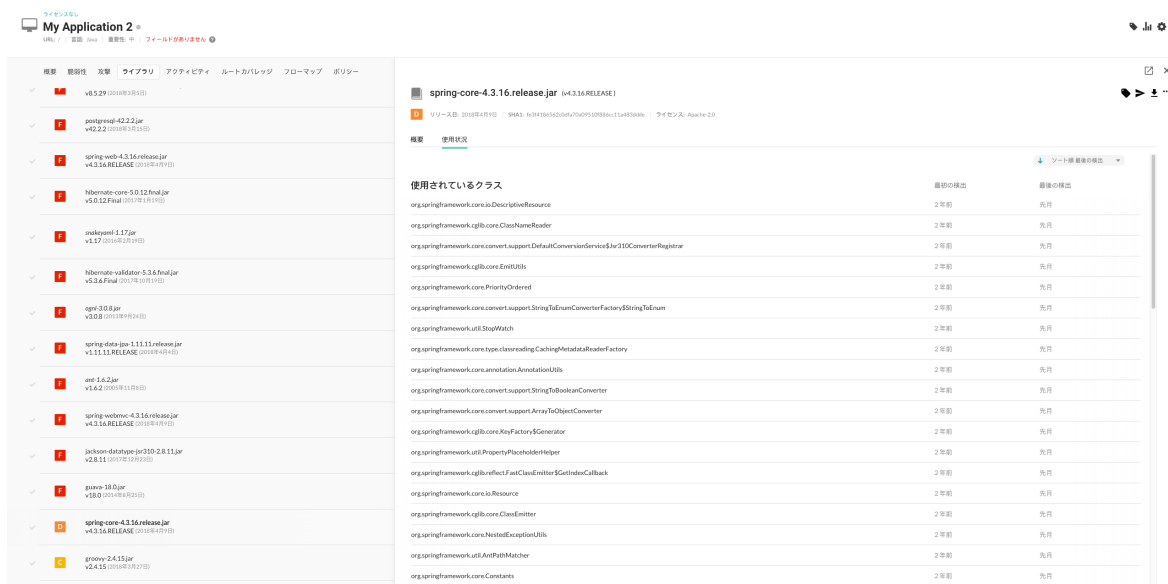
スコア	ライブラリ	最新バージョン	脆弱性	アプリケーション	使用状況	処理
?	idna tagtest1 v2.8	?		django.nv	使用されていません 0/0	(1) [icon] [icon]
F	snakeyaml-1.28.jar tagtest1 v1.28 (2021年2月22日)	2023年2月26日 v2.0	1 1 5	agent-metrics-3 protect-perf-baseline-#2	使用されていません 0/224	(1) [icon] [icon]
F	jackson-databind-2.12.5.jar tagtest1 v2.12.5 (2021年8月26日)	2023年1月28日 v2.14.2	3	このライブラリのすべてのアプリケーションでの使用状況 最大使用数 / 最大検知数	352/701	(1) [icon] [icon]
F	commons-fileupload-1.3.1.jar asdf tagtest1 v1.3.1 (2014年2月4日)	2018年12月24日 v1.4	1 2	WebGoat	3/49	(2) [icon] [icon]

ここでの項目は、このライブラリを使用するアプリケーションの言語に応じて異なり、クラス、ファイル、または関数となります。メインアプリケーションに同じライブラリを使用する複数のアプリケーションがマージされている場合、使用中の項目はマージアプリケーションを表すものになります。


アプリケーションがライブラリを使用している場合、Contrast エージェントはライブラリ内で使用された項目を報告します。アプリケーションがライブラリ内のより多くの項目を使用すると、使用数も増加します。

適切なライセンスをお持ちの場合、以下の手順を行うことで、特定のアプリケーションにおけるライブラリの使用状況の詳細も確認できます。

1. アプリケーションのページで、詳細を確認するアプリケーションを選択します。
2. アプリケーションのライブラリタブを選択します。
3. 確認したいライブラリの使用数をクリックすると、概要と使用状況のパネルが表示されます。



4. 使用状況タブをクリックすると、使用されている各クラス、ファイル、関数を確認できます。特定のクラスを検索するには、検索アイコン🔍をクリックします。また、Contrast でその使用が観測された最初と最後の時刻を確認することもできます。[ライブラリのエクスポート \(541ページ\)](#)にも、使用状況の全データを含めることができます。[概要タブ](#)をクリックすると、*何が起こったか?*(問題の説明)と*どんなリスクであるか?*(深刻度、CVSS のスコア、CVE のタイトル、ポリシー違反)が表示されます。

 **注記**

マージされたアプリケーションの場合、**最後の検出**と**最初の検出**の列に対する情報がある全てのアプリケーションについて、いつクラスが最初と最後に検出されたかが表示されます。

5. ライブラリに[タグ \(538ページ\)](#)を付けたり、ライブラリに関する情報を[送信 \(539ページ\)](#)することもできます。
6. パネル右上にある[さらに \(...\)](#)をクリックすると、パッケージ詳細やリポジトリ情報の参照、ライブラリの[削除 \(537ページ\)](#)、使用状況を CSV 形式でエクスポートすることができます。
7. 詳細パネルを閉じるには、**X** を選択します。

## ライブラリ情報のエクスポート

エクスポートされたファイルには、各ライブラリの以下のデータフィールドが含まれます。

ライブラリ情報をエクスポートするには：

1. Contrast Web インターフェイスのナビゲーションバーで**ライブラリ**を選択し、ライブラリー一覧の左側の列にあるチェックマークを使用してエクスポートに使用するライブラリを選択します。
2. ページの下部に表示される一括アクションメニューで、**エクスポート**アイコンを選択して、エクスポートする形式(CSV または XML)を選択します。



3. エクスポートファイルは、デスクトップにダウンロードされます。エクスポートされたファイルには、ライブラリごとに以下のデータフィールドが含まれます。
  - Library Name (ライブラリ名)
  - Language (言語)
  - Version (バージョン)
  - Release Date (リリース日)
  - Latest Version (最新バージョン)
  - Score (スコア)
  - SHA1
  - CVE Count (CVE 数)
  - Application Count (アプリケーション数)
  - Server Count (サーバ数)
  - Number of Classes (クラス数)
  - Number of Used Classes (使用中のクラス数)
  - Open source License (オープンソースライセンス)
  - Policy Violation(ポリシー違反)



## ヒント

アプリケーションに関して、より詳細なカスタムのソフトウェアコンポジション解析 (SCA) レポートを作成する場合、**ライブラリ API** を使用して Contrast のライブラリデータにアクセスできます。また、手動でライブラリの詳細情報を調べることもできます。

例えば、以下の curl リクエストは、ライブラリの一覧を取得します。各ライブラリには、このライブラリの一覧にあるライブラリを使用しているアプリケーション一覧が含まれます。カスタムレポートで使用するために、jq ツールでデータを CSV 形式にしています。

```
$ curl -H "Authorization: $(echo -n $username:$servicekey  
base64)" -H "API-Key: $apikey" https://app.contrastsecurity.com/  
Contrast/api/ng/$org_id/libraries/filter?expand=apps  
jq -r '.libraries[]  
{name: .file_name, app_name: .apps[].name}  
[.name, .app_name]  
@csv'
```

## オープンソースライセンスの参照



### 重要

Contrast SCA をご利用のお客様のみ、オープンソースライセンスを表示できます。Contrast SCA を有効にするには、組織の管理者にご連絡ください。

オープンソースライブラリのライセンス情報(SPDX 形式)を表示するには、Contrast Web インターフェイスのナビゲーションバーで**ライブラリ**を選択し、ライブラリ一覧を表示します。ライセンス情報を表示するには、次のような方法があります。


- 個々のライブラリのライセンスを表示するには、ライブラリ一覧でライブラリ名にカーソルを合わせます。
- 特定のライセンスのライブラリを検索するには、**ライブラリ**列の見出しの横にある**フィルター**アイコンを選択して、絞り込むライセンスを選択します。
- ライブラリ名を選択して、そのライブラリの詳細ページを表示すると、ページの上部にもライセンス情報があります。
- **パッケージ**詳細を選択すると、そのパッケージのタイトル、バージョン、作成者などを参照できます (**パッケージ**詳細は、ライブラリ一覧でライブラリ名にカーソルを合わせて表示されるヒントから、またはライブラリの詳細ページの右上の情報アイコンを選択すると表示されます)。
- 各ライブラリのライセンス情報は、**Contrast でエクスポート (541ページ)**できる CSV または XML ファイルにも含まれます。

### 依存関係ツリーの表示


アプリケーションにオープンソースライブラリを追加すると、そのライブラリの依存関係もすべて継承されます。このような推移的依存関係の中には、アプリケーションに脆弱なコードをもたらす可能性のあるものがあります。**Contrast CLI (579ページ)**を使用すると、すべてのライブラリの依存関係が識別され、そのデータが Contrast に送信されます。そのデータによって、Contrast でこれらのライブラリを階層的な依存関係ツリーとして可視化することができます。

アプリケーションのライブラリを階層で表示するには、Contrast がコンパイル前のアプリケーションコードにアクセスする必要があります。これは、ソフトウェア開発ライフサイクル(SDLC)の中で、Contrast エージェントがデータを収集するステージとは異なります。コンパイル前のデータ収集を行うために、アプリケーションに **Contrast CLI (579ページ)**をインストールして実行しておく必要があります。

アプリケーションのライブラリの依存関係ツリーを表示するには：

1. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択します。
2. アプリケーションを選択します。
3. アプリケーションの**概要**ページが表示されたら、**ライブラリ**タブを選択します。
4. 右上の**依存関係ツリー**アイコンを選択すると、アプリケーションのライブラリの依存関係が階層で表示されます。

このビューに表示されるライブラリの依存関係ツリーは、**Contrast CLI (579ページ)**によって収集されたデータに基づいています。

- クイックビューメニューを使用すると、脆弱性のあるライブラリのみを表示できます。デフォルトでは、全てのライブラリが表示されます。右矢印を使用して個々のセクションを展開して詳細を表示したり、「全て開く」オプションを選択して全ての情報を一度に表示することができます。
- また、既知の脆弱性があるライブラリには、ライブラリ名の横に警告アイコンが表示されます。警告アイコンをクリックすると脆弱性の情報が表示されます。

- 特定のライブラリを検索するには、検索アイコン🔍をクリックします。
- カスタム日付を選択して、依存関係ツリーの履歴を表示することもできます。
- フィルターアイコン▼をクリックすると、試験・開発環境で利用するライブラリや本番環境で利用するライブラリを選択でき、その依存関係を表示できます。デフォルトでは、本番用ライブラリを表示するオプションが選択されています。
- **マージされた (485ページ)**アプリケーションには**アプリケーション**のドロップダウンが表示されるので、マージされたアプリケーションで、脆弱なライブラリがどのように使用されているかを確認することができます。依存関係ツリーは、親アプリケーションや子アプリケーションごとに表示できます。

## ライブラリのスコアガイド

Contrast では、アプリケーションのライブラリの安全性を文字で表したグレードで提供し、分析時の目安として使用することができます。以下のとおり、スコアをグレード(A から F の文字)に置き換えます。

- A : 90 - 100
- B : 80 - 89
- C : 70 - 79
- D : 60 - 69
- F : 35 - 59

スコアは、次の 3 つのペナルティ要素に基づきます。

- **時間**：ライブラリの古さです。アプリケーションで使用されているバージョンのリリース日から最新バージョンのリリース日までの年数に、2.5 を掛けた数が減算されます。
- **ステータス**：ステータスは、ライブラリの日付以降のバージョン数です。アプリケーションの現在のライブラリ以降にリリースされたバージョンの数に、10 を掛けた数が減算されます。
- **セキュリティ**：ライブラリに影響を与える CVE 数です。ライブラリの CVE ペナルティは、このライブラリの全ての既知の CVE の中で最も高い深刻度に、10 を掛けた数が減算されます。



### 注記

組織の管理者は、セキュリティ要素のみを対象とするよう**スコアの設定方法を調整 (719ページ)**できます。





## ヒント

例：

2010年1月にリリースされたライブラリを使用していて、最新版が2013年9月にリリースされた場合は、経過した年数は2となります。そのため、時間のペナルティは次のようになります。

$$2 \times 2.5 = 5$$

バージョン 1.1.1 を使用しているが、バージョン 1.1.2 と 1.1.3 がリリースされている場合は、ペナルティは次のようになります。

$$2 \times 10 = 20$$

セキュリティのスコアに 2.4 と 2.2 があるライブラリがある場合、ペナルティは次のようになります。

$$2.4 \times 10 = 24$$

ライブラリの最終的なスコアは、3つのペナルティそれぞれの値を100から引くことによって計算されます。

$$100 - 5 - 20 - 24 = 51$$

51のスコアには、「F」という文字が評価として割り当てられます。

## CVE 検索

[ライブラリ \(534ページ\)](#)内の特定の CVE を探すには、検索バーを使用します。

- 検索バーで CVE 番号を入力すると、CVE が検出されているライブラリが検索結果に自動表示されます。

(26) ▼ 🔍 名前またはCVEでライブラリを検索

- 該当するライブラリを選択すると、ライブラリの詳細が表示されます。
- [組織 \(698ページ\)](#)、[アプリケーション \(480ページ\)](#)、[サーバ \(528ページ\)](#)のライブラリが検索可能です。

## Contrast Serverless

Contrast Serverless は、サーバレスアプリケーション向けのセキュリティツールで、動的・静的スキャン、グラフによる可視化、リソースの可観測性などを提供し、お使いの環境の状況を把握するのに役立ちます。

Contrast Serverless では、以下が可能です。

- [必要に応じた関数のスキャン \(555ページ\)](#)
- [検出結果の表示 \(556ページ\)](#)
- [インベントリ基準の変更 \(561ページ\)](#)
- [サーバレスのスキャン設定の変更 \(524ページ\)](#)
- [関数とサービスの関係の表示 \(562ページ\)](#)

## 関連項目

- [Contrast Serverless と JIRA のインテグレーション \(658ページ\)](#)

## インベントリ

Contrast から AWS アカウントに接続すると、対象の環境内のすべての Lambda 関数と、さまざまなリソース(S3、API Gateway、DynamoDB など)との関係が自動的に検出されます。

[特定の基準を指定 \(561ページ\)](#)しない限り、デフォルトではインベントリのすべての関数がスキャンされます。

## インベントリの基準

Contrast ではスキャンの対象とする関数を決定するのに、次のような基準を指定できます。

- **Tag** : このオプションを使用すると、指定したタグ、およびタグの値に関連付けられた関数を含めたり除外したりできます。
- **Name** : このオプションを使用すると、関数の名前の一致(または前方一致や後方一致)で対象に含めたり除外したりできます。

## Contrast Serverless のサポート対象の言語

Contrast Serverless では、以下のプログラミング言語をサポートしています。

言語	ランタイムバージョン
Java	8.x、11.x
.NET	.NET 5.x、6.x .NET Core 3.1
Node.js	12.x、14.x、16.x、18.x
Python	3.6、3.7、3.8、3.9

## Contrast Serverless のサポート対象のプラットフォーム

Contrast Serverless では、以下のプラットフォームをサポートしています。

- AWS Lambda
- Microsoft Azure

## スキャンの種類と監視について

Contrast Serverless では、次の種類のスキャンをサポートします。

### 静的スキャン

このスキャンでは、関連する静的コードや設定評価をほぼリアルタイムで自動的にスキャンし、以下のカテゴリにおいて新たな脆弱性を検出します。

- **最小権限** : デプロイ前のサーバレスワークロード内の IAM の脆弱性(過剰に権限が設定されている関数)を検出し、推奨するアクセス許可を修正案として表示します。
- **Contrast SCA** : Contrast SCA エンジンを使用して、オープンソースライブラリの SCA を行います。

このスキャンによる、コードへの永久的な影響はありません。

## 動的スキャン

このスキャンでは、検査対象の環境で発生する特定の更新に基づいて動的な検査を行います。

これは、検査対象の環境で生じた特定の更新に合わせて、ほぼリアルタイムで自動的に実行され、動的な検査が行われます。動的スキャンは、OWASP Top 10 の判定を基準としています。例：

- SQL インジェクション
- コードインジェクション
- ローカルファイルインクルード(LFI)

動的スキャンでは、Contrast は悪意のあるデータを送信して関数の実行を試行し、脆弱性を検出します。この動作はコードに影響を与えませんが、スキャン対象の関数は呼び出されます。

## IAST 解析



### 注記

IAST 解析を実行する場合は、[テストカバレッジ](#)を使用する必要があります。

スキャンの設定を指定する際に、このオプションを選択することを推奨します。

IAST 解析により、AWS アカウントで悪用可能な全ての AWS Lambda 関数が明らかになります。最新の AWS Lambda サービスに対するサポートにより、AWS Step Functions(複数の Lambda 関数を柔軟なワークフローに調整するサービス)のセキュリティの問題を明らかにすることができます。

以下のような OWASP トップ 10 の脆弱性を検出できます。

- コンテンツインジェクション、OS コマンドインジェクション、SQL インジェクション(限定的)、コードインジェクション
- クロスサイトスクリプティング(XSS)
- ローカルファイルインクルード(LFI)

さらに、[未使用の関数](#)(シャドウ関数)を含め、サーバレスアカウントの全ての資産が明らかになります。これにより、AWS アカウントの観測性が向上し、セキュリティカバレッジが広がります。未使用の関数は、通常のメンテナンスがされておらず、脆弱性につながる古い依存関係が含まれている可能性があります。

## 継続的な監視

Contrast からアカウントに接続すると、Contrast Serverless がこのアカウントを監視します。関数のコードや設定が変更されると、Contrast は自動的に新しいスキャンを開始します。

## AWS で Contrast Serverless を使い始める

Contrast Serverless の使用を開始するには、Contrast Web インタフェースを開き、AWS アカウントに接続して、新しいスタックを作成します。

## 開始する前に

- AWS アカウントの情報を準備します。
- Contrast Serverless のスタックをデプロイ/更新/削除するために最小限の権限 ([549ページ](#))が必要です。

## 手順

1. Contrast Web インタフェースのページ上部の**新規登録**を選択します。



2. **アカウントに接続**を選択し、**次へ**をクリックします。



3. **クラウドプロバイダ**のセクションで **AWS** を選択します。
4. 必要に応じて、スキャンの設定をします。
  - **インベントリ**：インベントリにはスキャンの対象とする関数を指定します。デフォルトでは、AWS アカウントのすべての関数が対象になります。
  - **初回スキャン**：この設定には、関数をスキャンするアクションを指定します。

静的解析	動的解析
対象： <ul style="list-style-type: none"> <li>• <b>最小権限</b>：使用されていない権限を検出します。Java、.NET Core 6、.NET Core 7、Node.js、Python が対象です。</li> <li>• <b>CVE</b>：脆弱な OSS ライブラリを検出します。Java、.NET Core 6、.NET Core 7、Node.js、Python が対象です。</li> <li>• <b>SAST</b>：カスタムコードの脆弱性を検出します。Java が対象です。</li> <li>• <b>マルウェア</b>：悪意のあるファイルを検出します。Python が対象です。</li> </ul>	対象： <ul style="list-style-type: none"> <li>• アプリケーションのストレステストを行い、潜在的な脆弱性を検出します。</li> <li>• <b>IAST 解析</b>オプションを使用すると、アカウント環境全体および全てのサービスにおいて、関数の脆弱性を見つけることができます。詳細は、<a href="#">スキャンの種類と監視について (546ページ)</a>を参照してください。この解析機能をアカウントに完全に設定するには、<a href="#">IAST 解析の手順</a>セクションにある手順に従ってください。Node.js と Python が対象です。</li> </ul>

- **Deployment**：AWS で新しいスタックにデプロイするか、パイプラインで使用する CFT をダウンロードします。

上記の設定は、「設定」タブでいつでも[設定の変更 \(562ページ\)](#)ができます。

5. **Create new stack** を選択します。

- 表示される AWS の画面で、アカウント情報を入力し**スタックの作成**を選択します。または、AWS CloudFormation のテンプレートをダウンロードして、開発パイプラインで使用することもできます。  
この操作により、アカウントの AWS CloudFormation スタックコンソールに接続し、最初のスキャンが開始します。
- AWS のコンソールでスタックのデプロイを承認します。  
スタックのデプロイには、完了するまでに約 2 分かかります。
- Contrast Web インタフェースに戻り、アカウント接続とスキャン開始のメッセージが表示されることを確認します。
- 関数の詳細やスキャンの結果を見るには、「アカウントに接続」のメッセージ内にある**関数**を選択して表示するか、ナビゲーションバーから**サーバレスタブ**を選択します。

## 次の手順

- [オンデマンドで関数をスキャン \(555ページ\)](#)
- [結果の表示 \(556ページ\)](#)
- [インベントリ基準の変更 \(561ページ\)](#)
- [スキャン設定の変更 \(562ページ\)](#)

## Contrast Serverless を実行するための AWS ポリシーと権限

ここでは、Contrast Serverless を実行するための AWS アカウントのポリシーと権限のサンプルを紹介します。

### アクセス管理の例

以下は、アカウントの権限とポリシーのサンプルです。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CustomResources",
      "Effect": "Allow",
      "Action": [
        "sns:Publish"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SNS2",
      "Effect": "Allow",
      "Action": [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns>DeleteTopic"
      ],
      "Resource": "*"
    }
  ],
  {
    "Sid": "IAM",
    "Effect": "Allow",
    "Action": [
      "iam:AttachRolePolicy",
      "iam:CreatePolicy",
      "iam:CreateRole",
      "iam:CreateServiceLinkedRole",
```

```

        "iam:DeletePolicy",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DetachRolePolicy",
        "iam:GetPolicy",
        "iam:GetRole",
        "iam:GetRolePolicy",
        "iam:ListPolicyVersions",
        "iam:ListRoleTags",
        "iam:PassRole",
        "iam:PutRolePolicy",
        "iam:TagRole",
        "iam:UntagRole"
    ],
    "Resource": "*"
},
{
    "Sid": "S3",
    "Effect": "Allow",
    "Action": [
        "s3:CreateBucket",
        "s3:DeleteBucket",
        "s3:DeleteBucketPolicy",
        "s3:GetBucketPolicy",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutEncryptionConfiguration",
        "s3:PutLifecycleConfiguration"
    ],
    "Resource": "*"
},
{
    "Sid": "Lambda",
    "Effect": "Allow",
    "Action": [
        "lambda:GetFunction",
        "lambda:CreateFunction",
        "lambda:DeleteFunctionEventInvokeConfig",
        "lambda:DeleteFunction",
        "lambda:TagResource",
        "lambda:PutFunctionEventInvokeConfig"
    ],
    "Resource": "*"
},
{
    "Sid": "S3LambdaCode",
    "Effect": "Allow",
    "Action": [
        "s3:GetObject"
    ],
    "Resource": "*"
},
{
    "Sid": "EventsRule",

```

```
    "Effect": "Allow",
    "Action": [
      "events:DeleteRule",
      "events:DescribeRule",
      "events:PutRule",
      "events:PutTargets",
      "events:RemoveTargets"
    ],
    "Resource": "*"
  },
  {
    "Sid": "CloudTrail",
    "Effect": "Allow",
    "Action": [
      "cloudtrail:AddTags",
      "cloudtrail:CreateTrail",
      "cloudtrail>DeleteTrail",
      "cloudtrail:StartLogging",
      "cloudtrail:PutEventSelectors"
    ],
    "Resource": "*"
  }
]
}
```

AWS の iam create-policy を実行 :

```
aws iam create-policy --policy-name Contrast-create-stack --policy-
document '{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "CustomResources",
      "Effect": "Allow",
      "Action": ["sns:Publish"],
      "Resource": "*"
    },
    {
      "Sid": "SNS2",
      "Effect": "Allow",
      "Action": [
        "sns:CreateTopic",
        "sns:GetTopicAttributes",
        "sns>DeleteTopic"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAM",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:CreatePolicy",
        "iam:CreateRole",
        "iam:CreateServiceLinkedRole",
        "iam>DeletePolicy",
```

```
    "iam:DeleteRole",
    "iam:DeleteRolePolicy",
    "iam:DetachRolePolicy",
    "iam:GetPolicy",
    "iam:GetRole",
    "iam:GetRolePolicy",
    "iam:ListPolicyVersions",
    "iam:ListRoleTags",
    "iam:PassRole",
    "iam:PutRolePolicy",
    "iam:TagRole",
    "iam:UntagRole"
  ],
  "Resource": "*"
},
{
  "Sid": "S3",
  "Effect": "Allow",
  "Action": [
    "s3:CreateBucket",
    "s3:DeleteBucket",
    "s3:DeleteBucketPolicy",
    "s3:GetBucketPolicy",
    "s3:PutBucketPolicy",
    "s3:PutBucketPublicAccessBlock",
    "s3:PutBucketTagging",
    "s3:PutEncryptionConfiguration",
    "s3:PutLifecycleConfiguration"
  ],
  "Resource": "*"
},
{
  "Sid": "Lambda",
  "Effect": "Allow",
  "Action": [
    "lambda:GetFunction",
    "lambda:CreateFunction",
    "lambda:DeleteFunctionEventInvokeConfig",
    "lambda:DeleteFunction",
    "lambda:TagResource",
    "lambda:PutFunctionEventInvokeConfig"
  ],
  "Resource": "*"
},
{
  "Sid": "S3LambdaCode",
  "Effect": "Allow",
  "Action": ["s3:GetObject"],
  "Resource": "*"
},
{
  "Sid": "EventsRule",
  "Effect": "Allow",
  "Action": [
    "events:DeleteRule",
```



```

    "events:DescribeRule",
    "events:PutRule",
    "events:PutTargets",
    "events:RemoveTargets"
  ],
  "Resource": "*"
},
{
  "Sid": "CloudTrail",
  "Effect": "Allow",
  "Action": [
    "cloudtrail:AddTags",
    "cloudtrail:CreateTrail",
    "cloudtrail>DeleteTrail",
    "cloudtrail:StartLogging",
    "cloudtrail:PutEventSelectors"
  ],
  "Resource": "*"
}
]
}

```

レスポンスを取得：

```

{
  "Policy": {
    "PolicyName": "Contrast-serverless-create-stack",
    "PolicyId": "ANPAV3I66HSEE4ILG6XJ3",
    "Arn": "arn:aws:iam::402181209224:policy/Contrast-serverless-create-stack",
    "Path": "/",
    "DefaultVersionId": "v1",
    "AttachmentCount": 0,
    "PermissionsBoundaryUsageCount": 0,
    "IsAttachable": true,
    "CreateDate": "2023-01-24T16:36:49+00:00",
    "UpdateDate": "2023-01-24T16:36:49+00:00"
  }
}

```

ユーザポリシーをアタッチ：

```

aws iam attach-user-policy --policy-arn
arn:aws:iam::402181209224:policy/Contrast-serverless-create-stack --user-
name
<USER-NAME></USER-NAME>

```

レスポンスを取得：

```

4ppsec@TMEELAMED-C02DX3Q2ML85:~/cn-mono (*)
> aws iam list-attached-user-policies --user-name xrays --profile xrays
{
  "AttachedPolicies": [
    {
      "PolicyName": "Contrast-serverless-create-stack",
      "PolicyArn": "arn:aws:iam::402181209224:policy/Contrast-serverless-create-stack"
    }
  ]
}

```

これで、デプロイメントを実行できるようになりました。

## Azure で Contrast Serverless を使い始める

Azure で Contrast Serverless の使用を開始するには、Contrast Web インタフェースを開き、Azure アカウントに接続して、新しいスタックを作成します。

### 開始する前に

- 有効なサブスクリプションを持つ Azure アカウントがあること。
- Active Directory テナントにアプリ登録を作成できる権限があること。
- アカウントに所有者ロールがあること。これによりアプリ登録にロールを割り当てることができます。

### 手順

1. Contrast Web インタフェースのページ上部の**新規登録**を選択します。



2. **アカウントに接続**を選択し、次へをクリックします。



3. クラウドプロバイダのセクションで **Azure** を選択します。
4. 必要に応じて、スキャンの設定をします。
  - **インベントリ**： Azure では利用できません。
  - **初回スキャン**： この設定には、関数をスキャンするアクションを指定します。

静的解析	動的解析
<p>内容：</p> <ul style="list-style-type: none"> <li>• <b>最小権限</b>- 使用されていない権限を検出します。Java、.NET Core 6、.NET Core 7、Node.js、Python が対象です。</li> <li>• <b>CVE</b> - 脆弱な OSS ライブラリを検出します。Java、.NET Core 6、.NET Core 7、Node.js、Python が対象です。</li> <li>• <b>SAST</b> - カスタムコードの脆弱性を検出します。Java が対象です。</li> <li>• <b>マルウェア</b> - 悪意のあるファイルを検出します。Python が対象です。</li> </ul>	<p>Azure では利用できません。</p>

上記の設定は、「設定」タブでいつでも[設定の変更 \(562ページ\)](#)ができます。

5. **Deployment** セクションの手順を続けます。
6. Contrast Web インタフェースに戻り、アカウント接続とスキャン開始のメッセージが表示されることを確認します。

## 次の手順

- [オンデマンドで関数をスキャン \(555ページ\)](#)
- [結果の表示 \(556ページ\)](#)

## オンデマンドで関数をスキャン

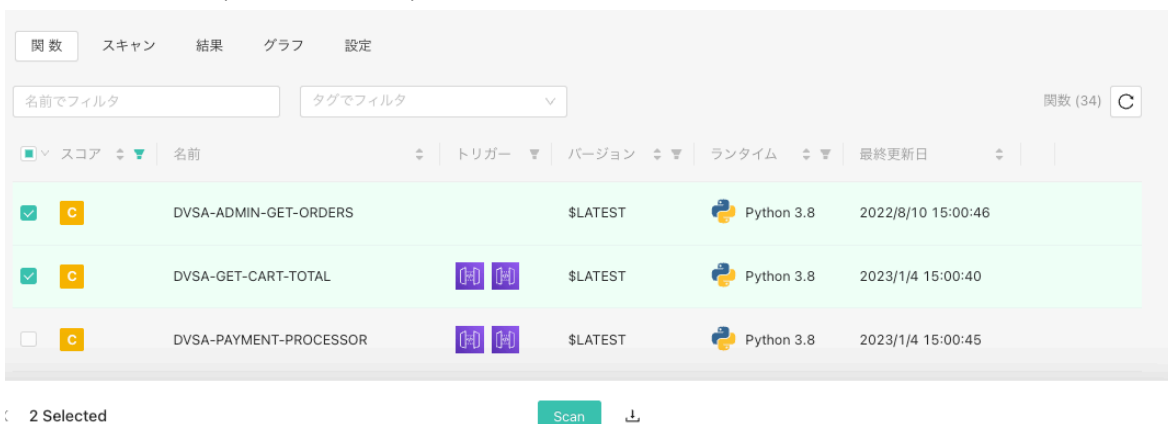
アカウントの全ての関数のスキャンは自動的に行われますが、必要に応じて特定の関数をスキャンすることもできます。

### 開始する前に

- スキャンする関数を決めます。

### 手順

1. Contrast Web インタフェースのナビゲーションバーで**サーバレス**を選択します。
2. 一覧からアカウントを選択します。
3. スキャンする関数(1つまたは複数)の横にあるチェックボックスを選択します。



4. **Scan** を選択します。
5. 「スキャンを確認」の画面で、選択した関数のスキャンタイプを確認または変更し、**OK** を選択します。  
「スキャン開始」のメッセージが表示されます。



6. スキャンの結果を確認するにはスキャン開始のメッセージにある**スキャンを表示**を選択します。または、**スキャンタブ**を選択し **Ad Hoc Scan** を選択します。スキャンした関数で同じ脆弱性が複数検出された場合、新たな脆弱性として報告されるのではなく、報告済みの既存の脆弱性が新しいデータ(タイムスタンプなど)で更新されます。




## 結果の表示

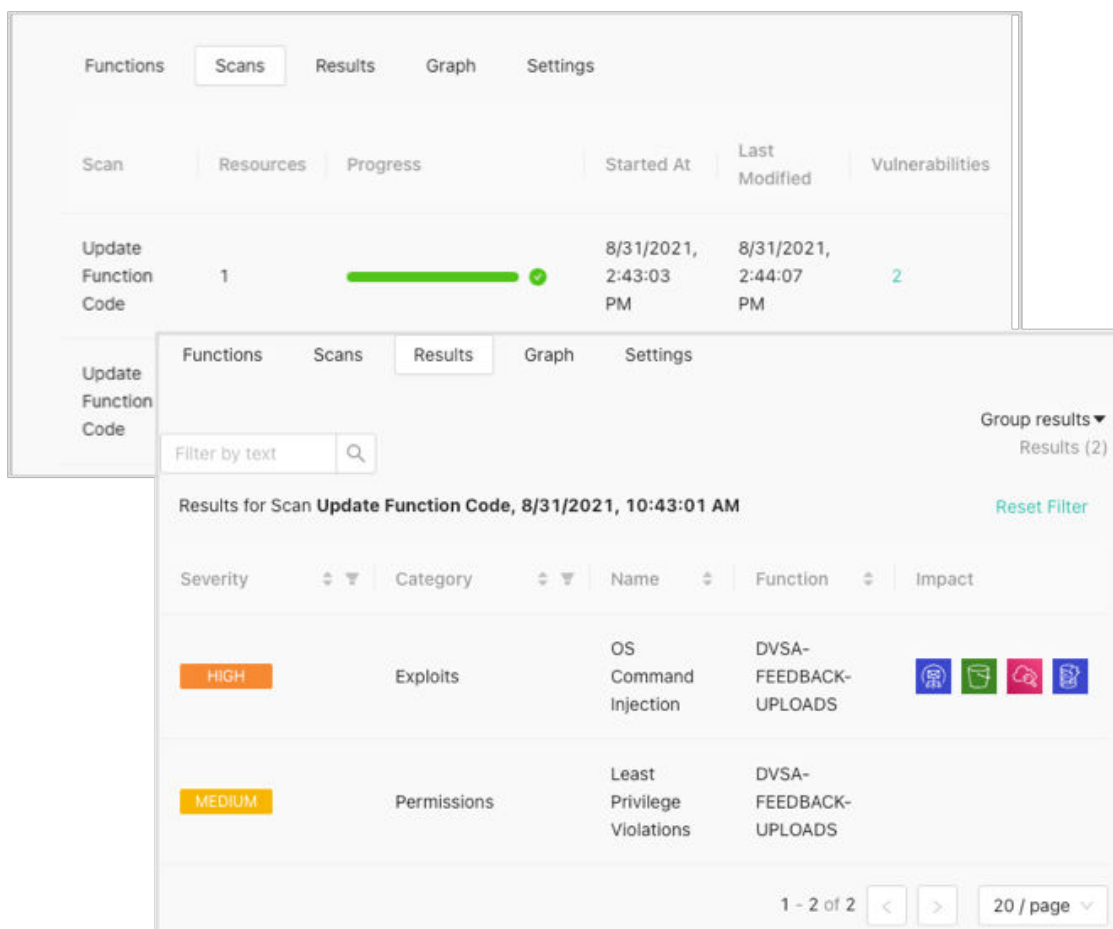
結果を表示して、権限、依存関係、攻撃、CVE などの脆弱性に関する情報を確認することができます。

## 開始する前に

- 少なくとも 1 つのスキャンが完了していること。

## 手順

1. Contrast Web インタフェースのナビゲーションバーで**サーバレス**を選択します。
2. すべてのスキャンの結果を表示するには、**Results** タブを選択します。
3. 「Results」タブでフィルタをかけるには、列のヘッダの横にある**フィルタアイコン**()を選択します。
  - a. **Severity** は、アプリケーションの脆弱性に基づいています。レベルについては、[アプリケーションのスコアガイド \(822ページ\)](#)を参照してください。
  - b. **Category** は。関数の種類に応じた脆弱性で分類しています。
  - c. 画面右側の **Group results** でオプションを選択すると、結果を **Category** や **Function** でグループ化することもできます。フィルタを解除するには列のヘッダの横にある緑色の**フィルタアイコン**()を選択し、**Reset** を選択します。
4. 「Results」タブで関数を検索するには、**虫眼鏡アイコン**()を選択します。
5. 1 つのスキャンの結果を表示するには、「Scans」タブでスキャンの行を選択します。この操作により、スキャンの詳細ページが表示されます。
6. 関数の検出結果の詳細を表示するには：
  - a. 「Results」タブからは、一覧で該当の行を選択します。
  - b. スキャンの詳細ページからは、関数の「Vulnerabilities」列にある数字をクリックします。



結果の詳細ページは、以下の例のようになります。

## Least Privilege Violations ✕

MEDIUM

Category: Function: [arn:aws:lambda:us-east-1:733980656228:function:DVSA-ADMIN-GET-ORDERS](#)

Permissions

---

### Description

The Attached Role [arn:aws:iam::733980656228:role/DVSA-AdminRole-dev](#) has an over permissive policy that may violate the principle of least privilege. For more information on aws least privilege [docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege](https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#grant-least-privilege).

### What happened

- DVSA-AdminRolePolicy-dev: Permissions for service s3 should be removed
- DVSA-AdminRolePolicy-dev: Use of wildcard in service dynamodb is inadvisable

### Violating policies

**DVSA-AdminRolePolicy-dev**

> View violating policy

### Remediation

Replace the existing policy with one of the following:

JSON
YAML
TERRAFORM

```

{
  "PolicyName": "DVSA-AdminRolePolicy-dev",
  "PolicyDocument": {
    "Version": "2012-10-17",
    "Statement": [
      {
        "Sid": "1",
        "Effect": "Allow",
        "Action": [
          "logs:CreateLogGroup",
          "logs:CreateLogStream",
          "logs:PutLogEvents"
        ],
        "Resource": [
          "arn:aws:logs:us-east-1:7XXXXXXXXXX:log-group:/aws/lambda/*:*:*"
        ]
      }
    ]
  }
},

```

## 結果の詳細

表示される結果の詳細は、脆弱性の種類によって異なります。

全ての脆弱性に、以下の情報が表示されます。

- Description** : 脆弱性についての概要。

- **What happened** : スキャンで脆弱性検出時に発生していたイベント。
- **Remediation** : 脆弱性を修正するための手順。

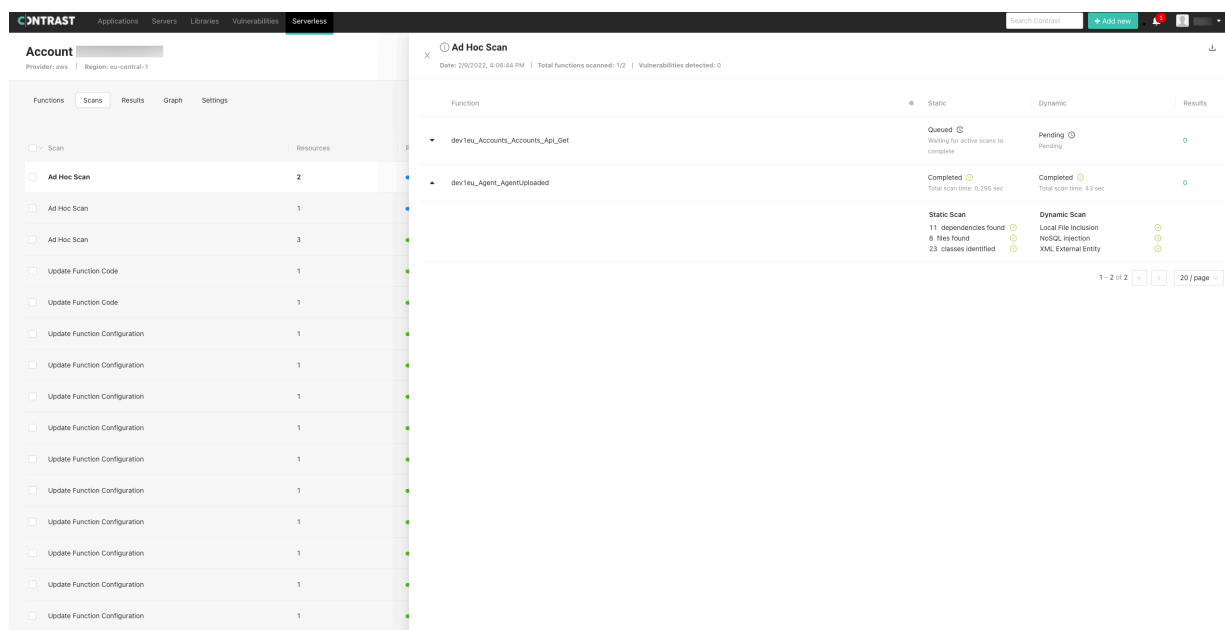
以下の情報も表示される場合があります。

- **Violated policies** : 脆弱性が違反しているポリシー。
- **Impact** : 脆弱性の影響を受ける領域。例、SES、S3、Logs、DynamoDB など。
- **Severity and Metrics** : 脆弱性に対して算出された深刻度のスコア、および脆弱性が影響を与える特性を評価するための基準。

## スキャンのステータス情報

サーバレスの Scans タブでは、システムがスキャンしている内容と、関数が検査されたスキャンのタイプについて確認できます。

Scans ページで、スキャン名をクリックすると、スキャンのステータスの詳細タブが開きます。



以下は、静的スキャンと動的スキャンのステータスに関する情報です。

ステータス	説明
Scanning.....	スキャン中
Pending	静的スキャンの結果を保留中
Queued	X 個のアクティブなスキャンを完了待ち X は、アクティブなスキャンの数になります。スキャンはキューに入っており、まもなく開始されます。
Completed	スキャン完了
Unsupported	サポート対象外の Lambda ランタイム 関数のランタイム言語がサポート対象外です。 サポート対象外の Lambda トリガー 関数にサポート対象外のトリガー設定があるか、識別できないトリガー設定がある。
Excluded	設定 (562ページ) でスキャンが無効になっている
Canceled	スキャンするには、インベントリの設定を変更するか、関数でアドホックスキャン(Ad Hoc Scan)を実行します。 より新しいスキャンが開始 この関数の新しいバージョンが既にキューに入っています。 Lambda のステータスが非アクティブ

ステータス	説明
	Lambda が 5 レイヤーの制限に達した Contrast では、上限値である 5 つのレイヤーがある関数はスキャンできません。
	Lambda のスキャンが既に進行中 Lambda の最終ステータスの更新に失敗
Failed	エージェントを確認できない 環境変数を復号化/暗号化できない エージェントのエラー Contrast の Cloud Agent 関数が起動できないが、静的解析中にスキャンが失敗しています。
	エージェントが変更された Lambda ハンドラーの設定ミス 解析エラー

- 矢印アイコンをクリックして詳細を展開すると、スキャンで検出された依存関係、ファイル、クラスの情報が表示されます。
- 「Results」列の下の数字をクリックすると、[Results \(556ページ\)](#)タブが開きます。

## サーバレスのスキャン結果のダウンロード

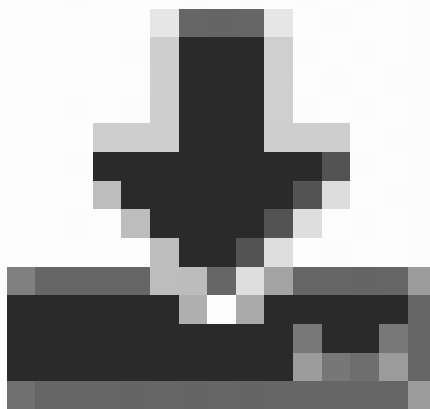
スキャンが完了したら、結果を CSV ファイルでダウンロードできます。

### 開始する前に

- 結果をダウンロードするスキャンを決めます。

### 手順

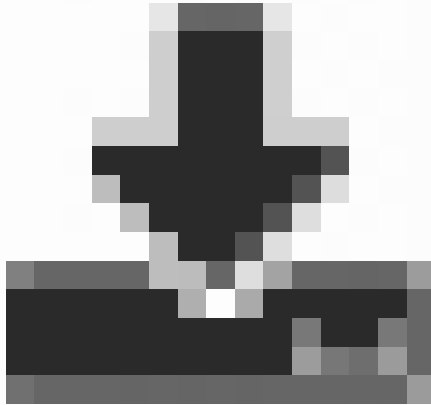
1. Contrast Web インターフェイスのナビゲーションバーで**サーバレス**を選択します。
2. **Scans** タブまたは **Results** タブを選択します。
3. **Scans** タブからダウンロードするには、スキャンの行の最後に表示されるダウンロードアイコンを選択します。
4. **Results** タブからダウンロードするには:
  - a. スキャンの行の最後に表示されるダウンロードアイコン



(  ) を選択します。



- または
- b. スキャンの行をクリックし、詳細ページの右上にあるダウンロードアイコン



( )を選択します。

結果が CSV ファイルでダウンロードされます。

## インベントリ基準の変更

インベントリ基準を登録することにより、Contrast Serverless でスキャンされる関数を指定できます。デフォルトでは、AWS アカウント内で検知されたすべての関数がスキャンされます。

関数を除外するように指定すると、その関数はインベントリやスキャンの対象から外されます。

## 開始する前に

- スキャンの対象とする関数、または対象外とする関数を決めます。
- インベントリ基準の変更には管理者権限(Admin ロール)が必要です。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーで**サーバレス**を選択します。
2. **Settings** タブを選択します。
3. 「Inventory」でインベントリ基準を指定します。
  - 関数に関連付けられたタグ名を登録することによって、関数をスキャン対象に含むか対象外とするかを指定します。必要に応じて、タグの値も指定します。
  - 関数の名前によって、スキャン対象に含むか、対象外とするかを指定します。関数名を指定するためのオプションは、**Name is**(名前一致)、**Name starts with**(前方一致)、**Name ends with**(後方一致)より選択します。

Functions Scans Results Graph Settings

### Inventory

Contrast will discover all functions in your AWS account.

To edit tags, names or environment variables that limit the scan inventory, edit the inventory criteria:

Include	Tag	Build123	Tag value - leave empty for any
Exclude	Name	starts with	cron

[+ Add criteria](#)

Any functions or results that no longer apply will be marked as inactive.

4. **Save and Rescan** を選択します。  
新しいインベントリ基準で自動的に再スキャンが行われます。

## サーバレスのスキャン設定の変更

このスキャン設定は、Contrast Serverless ですべての関数に対して実行されるスキャンの種類に影響します。

選択した関数を手動でスキャンするために、[これらの設定を変更 \(555ページ\)](#)できます。

### 開始する前に

- 静的スキャン、動的スキャンもしくは両方を使うか決めておくこと。
- 管理者権限(Admin ロール)が必要です。

### 手順

1. Contrast Web インターフェイスのナビゲーションバーで**サーバレス**を選択します。
2. **設定**タブを選択します。
3. **スキャン**のセクションで、使用するスキャンの種類を選択します。
  - **静的解析**：このスキャンでは、該当する静的コードと設定評価を調べて、脆弱性を検出します。静的スキャン中に、Contrast によって Lambda 関数がアカウントに追加されます。スキャンが完了すると、この関数は終了します。
  - **動的解析**：AWS アカウントのみが対象です。このスキャンでは、検査対象の環境で発生する特定の更新に基づく動的な検査を行います。動的スキャンでは、Contrast は悪意のあるデータを送信して関数の実行を試行し、脆弱性を検出します。  
IAST 解析に関する詳細は、[スキャンの種類と監視について \(546ページ\)](#)を参照してください。



#### 重要

Contrast Serverless のスキャンによって、関数のコードが変更されることはありません。

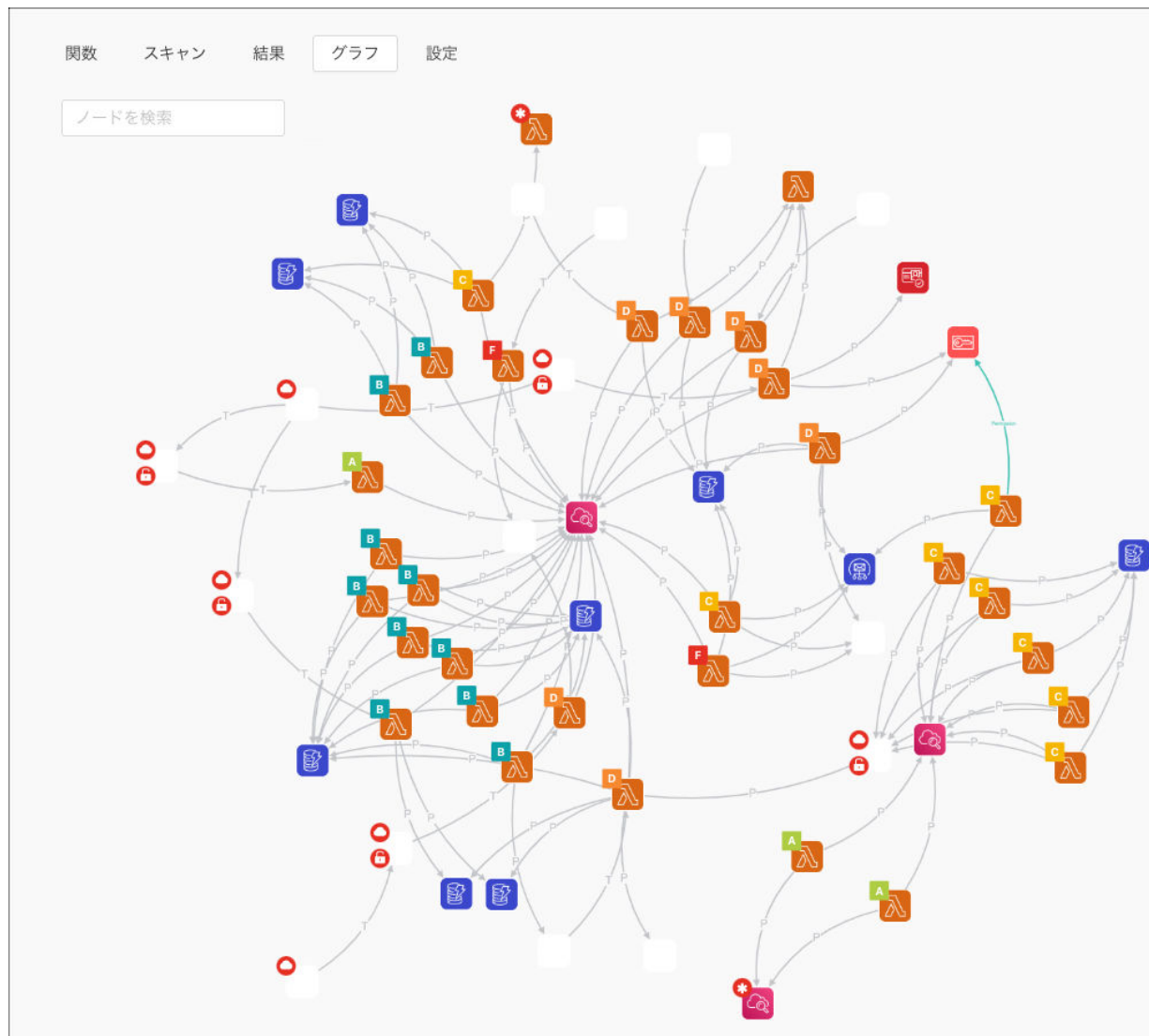
4. **保存**を選択します。

## 関数とサービスの関係の表示

「グラフ」タブでは、関数とサービスの関係を表す図が表示されます。図の各要素について、以下のような情報も参照できます。

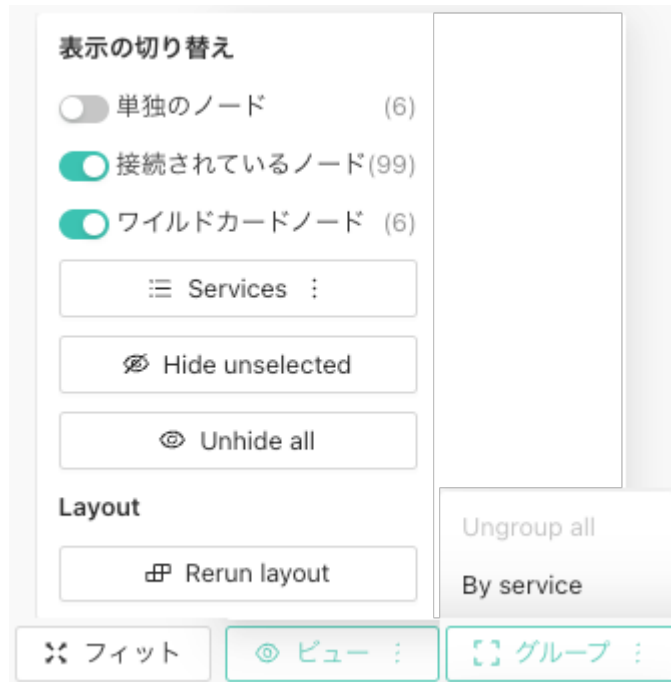
- タグ
- 脆弱性の検出結果

- 権限
- セキュリティ状況を表すスコア：セキュリティ状況のスコアは、関数のトリガー設定に基づいています。インターネットからアクセス可能なトリガーや、公開されたバケットや認証されていない API などの設定ミスは、低いスコアになります。
- IAST 解析による未使用の関数(シャドウ関数)



## 手順

1. Contrast Web インタフェースのナビゲーションバーでサーバレスを選択します。
2. グラフタブを選択します。
3. 表示を調整するには、下部にあるオプションを使用します。



- **フィット**：画面に合わせてグラフのサイズを変更できます。
  - **ビュー**：ノードやサービスで表示にフィルタをかけることができます。ノードを表示・非表示に切り替えることもできます。
  - **グループ**：サービスをグループにまとめることができます。
4. 要素をクリックすると、各要素の詳細情報を参照できます。  
 選択した要素の詳細ウィンドウが表示されます。タグを選択すると、グラフの表示がフィルタされます。

**DVSA-INIT**

× ランタイム: python3.8 | バージョン: SLATEST | 最終更新日: 2022/8/10 15:00:44 | アカウント: | リージョン: us-east-1 | AWSコンソールで表示 | ID: arn:aws:lam...

**Aws Tags**

キー	値
aws:cloudformation:logical-id	InitFunctionLambda
aws:cloudformation:stack-id	arn:aws:cloudformation:us-east-1:733980656228:stack/serverlessrepo-DVSA/f546cbd0-76c3-11eb-a1ca-12dc156c2e93
aws:cloudformation:stack-name	serverlessrepo-DVSA
lambda:createdBy	SAM
serverlessrepo:applicationid	arn:aws:serverlessrepo:us-east-1:1.88948553959:applications/DVSA
serverlessrepo:semanticVersion	1.2.4
STAGE	dev

**D**

- 影響度 (アクセスレベル) 5
- 可能性 (到達可能性) 100
- 脆弱性 80
- 総合スコア 65

1件の結果

重大 Least Privilege Violations

## コンテキストのリスクスコア

Contrast ではコンテキストに基づいてリスクをスコアで表しますが、これは、ユーザが実際のリスクポイントがどこにあり、何を優先すべきかを理解できるようにすることを目的としています。関数のコンテキストスコアは、各関数の全体的な評価を把握するのに役立ちます。

<input type="checkbox"/>	スコア	名前
<input type="checkbox"/>	C	contrast-221wr-dev1_Agent_1-0-0
<input type="checkbox"/>	C	contrast-221wr-dev1_Inspector_0-45-0
<input type="checkbox"/>	C	contrast-221wr-dev1_JavaAgent_0-45-0
<input type="checkbox"/>	A	serverless-cn-slack-bot-dev-scheduler
<input type="checkbox"/>	B	serverless-cn-slack-bot-dev-webhooks

関数には、関数の総合評価を表す A から F までのレターグレードと、35 から 100 までの数値スコアがあります。

- A : 90 - 100
- B : 80 - 89
- C : 70 - 79
- D : 60 - 69
- F : 35 - 59

総合のコンテキストのリスクスコアの計算 :  $\text{平均} = (\text{脆弱性スコア} + \text{影響度スコア} + \text{可能性スコア}) / 3$

### 脆弱性スコア

関数のスキャン(静的および動的)中に特定された脆弱性。

- 脆弱性の種類 :
  - カスタムコードの脆弱性(静的および動的)
  - 依存関係(CVE)
  - 最小権限違反
- カスタムコードの脆弱性スコアの算出は 100 点から始まり、関数で検出された脆弱性の数に、深刻度に応じたペナルティの重み付けを掛けたペナルティ点数が差し引かれます。
  - 重大 : 脆弱性の数  $\times$  20
  - 高 : 脆弱性の数  $\times$  10
  - 中 : 脆弱性の数  $\times$  5
  - 低 : 脆弱性の数  $\times$  1
  - 例えば、関数の脆弱性が、「重大」0 件、「高」1 件、「中」0 件、「低」2 件だった場合、スコアは次のようになります :  $100 - (20 \times 0) - (10 \times 1) - (5 \times 0) - (1 \times 2) = 88$

## 影響度(アクセスレベル)スコア

関数に与えられた権限(IAM ロール)。関数の権限が多いほど、リスクは高くなります。

影響度スコアを計算するために、各サービスに対して5つのアクセスレベル分類(List、Read、Write、Tagging、Permissions Management)を検査してスコアを付けます。そして、100点から開始して、各サービスのアクセスレベルに応じてペナルティ点数を減算していきます。

例えば、以下のような IAM ポリシーがあるとします。

```
{
  "Effect": "Allow" ,
  "Action": [
    "s3:GetObject",
    "sqs:*"
  ],
  "Resource": "*"
}
```

各サービスのアクセスレベルのスコアが、以下のように算出されたとします。

```
{
  "s3": {
    "Read": 6,
    "Write": 3,
    "List": 3,
    "Tagging": 1,
    "Permissions management": 12
  },
  "sqs": {
    "Read": 3,
    "Write": 3,
    "List": 1,
    "Tagging": 1,
    "Permissions management": 6
  }
}
```

総合スコアは、次のように算出されることになります。

- s3: [6], sqs: [3,3,1,1,6] -->  $100 - (6+3+3+1+1+6) = 80$

## 可能性(到達可能性)スコア

攻撃者が関数に到達する可能性は、関数のトリガーの設定に基づきます。

各サービスには、攻撃者がその関数にアクセスできるかどうかだけでなく、トリガーの設定(例えば、認証あり/認証なし)に基づいた、異なるスコアがあります。

例：

例えば、関数に EventBus がトリガーとして設定されている場合、潜在的な攻撃者がこの Lambda 関数にアクセスできる可能性は、API Gateway がトリガーとして設定されている Lambda にアクセスするよりも低くなります。さらに、API Gateway が認証なし(つまり Open)で設定されている場合には、その関数には誰でもどこからでもアクセスできることになります。

そのため、関数の可能性スコアは以下のようになります。

- EventBus をトリガーとして設定している場合：90

- API Gateway(認証あり)をトリガーとして設定している場合：75
- API Gateway(認証なし)をトリガーとして設定している場合：5 (最低スコア)
- トリガーがない場合：100 (最高スコア)

## Contrast Serverless のアップグレード

Contrast Serverless は、ほとんどの場合、自動更新に設定されています。手動でアップグレードする必要がある場合は、このページに記載されている手順に従って下さい。

### 開始する前に

- 必要最低限のポリシーを持つロール/ユーザを作成すること。設定方法は、[こちらの例 \(549ページ\)](#)を参照して下さい。

### 手順

1. 前回のデプロイメントまでに Contrast Serverless のスタックに手動で変更を加えていない場合は、現在の Contrast Serverless スタックを[アンインストール \(572ページ\)](#)するだけでよいです。  
以前の Contrast Serverless スタックに手動で変更を加えた場合は、[スタックの変更セットを作成 \(569ページ\)](#)してから、次の手順に進むことをお勧めします。
2. ツールバーで[新規登録](#)をクリックします。
3. **Download CFT** を選択して、Contrast から新しいテンプレートをダウンロードします。

## 始めましょう

以下のデフォルト設定でスタックを新規に作成するか、関数の条件を指定してデプロイして下さい。

### クラウドプロバイダ

アカウントを保有するクラウドプロバイダを選択

**AWS** Azure

### インベントリ

Contrastは、AWSアカウント内のすべての関数を検索します。

スキャンのインベントリを制限するタグ、名前、環境変数を指定するには、条件を追加します。

[+ 条件を追加](#)

### 初回スキャン

アカウント内の全ての関数をスキャンし、すべての変更を継続的にスキャンして、以下を特定します。

インベントリの条件に合致する関数

#### 静的解析

最小権限 - 使用されていない権限を検出

CVE - 脆弱な依存関係を検出

SAST - カスタムコードの脆弱性を検出

マルウェア - 悪意のあるファイルを検出

動的解析 - カスタムコードの脆弱性をファジング(関数を呼び出す)

### Deployment

AWSで新しいスタックにデプロイするか、パイプラインで使用するCFTをダウンロードします。

**Create new stack**  [Download CFT](#)

4. JSON または YAML のいずれかを選択します。
5. スタックを更新します。



st-z3nl9 > スタックの更新

## スタックの更新

**前提条件 - テンプレートの準備**

テンプレートの準備  
各スタックはテンプレートに基づきます。テンプレートとは、スタックに含む AWS リソースに関する設定情報を含む JSON または YAML ファイルです。

現在のテンプレートの使用  既存テンプレートを置き換える  デザイナーでテンプレートを編集する

**テンプレートの指定**

テンプレートは、スタックのリソースおよびプロパティを表す JSON または YAML ファイルです。

テンプレートソース  
テンプレートを選択すると、保存先となる Amazon S3 URL が生成されます。

Amazon S3 URL  テンプレートファイルのアップロード

テンプレートファイルのアップロード

ファイルが選択されていません  
JSON または YAML 形式のファイル

S3 URL: テンプレートファイルをアップロードすると生成されます。

### 6. 表示された画面で、送信をクリックします。

機能

 The following resource(s) require capabilities: [AWS::IAM::ManagedPolicy]  
このテンプレートには、ご利用の AWS アカウントに変更を加えるエンティティにアクセスを与える可能性を持つ Identity and Access Management (IAM) リソースが含まれています。これらのリソースを個別に作成し、それぞれに最小限必要な権限を与えるかどうか確認してください。 [詳細はこちら](#)

AWS CloudFormation によって IAM リソースが作成される場合があることを承認します。

## スタックの変更セット

スタックの変更セットを作成するには、次の手順を実行して下さい。

### 開始する前に

- AWS CloudFormation コンソールで、Contrast Serverless のスタックを確認して下さい。

### 手順

1. Contrast Web インターフェイスにログインし、**Download CFT** を選択して、Contrast から新しいテンプレートをダウンロードします。

## 始めましょう

以下のデフォルト設定でスタックを新規に作成するか、関数の条件を指定してデプロイして下さい。

### クラウドプロバイダ

アカウントを保有するクラウドプロバイダを選択

AWS Azure

### インベントリ

Contrastは、AWSアカウント内のすべての関数を検索します。

スキャンのインベントリを制限するタグ、名前、環境変数を指定するには、条件を追加します。

+ 条件を追加

### 初回スキャン

アカウント内の全ての関数をスキャンし、すべての変更を継続的にスキャンして、以下を特定します。

インベントリの条件に合致する関数

#### 静的解析

最小権限 - 使用されていない権限を検出

CVE - 脆弱な依存関係を検出

SAST - カスタムコードの脆弱性を検出

マルウェア - 悪意のあるファイルを検出

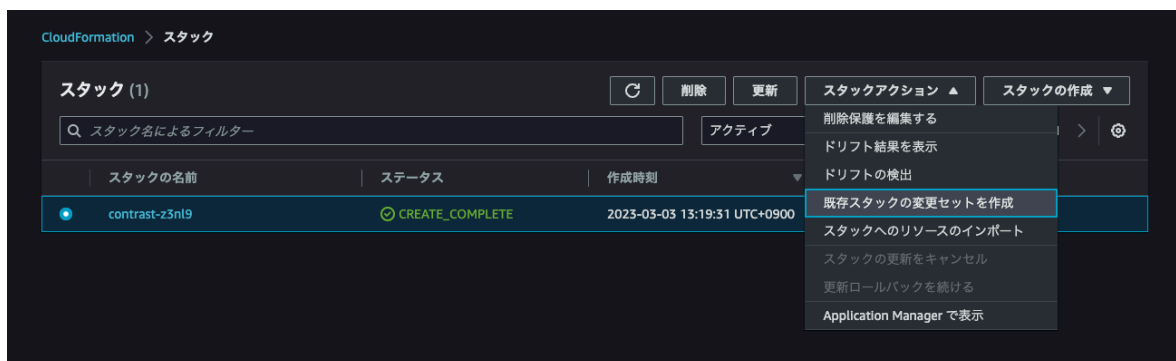
動的解析 - カスタムコードの脆弱性をファジング(関数を呼び出す)

### Deployment

AWSで新しいスタックにデプロイするか、パイプラインで使用するCFTをダウンロードします。

Create new stack Download CFT

- JSON または YAML のいずれかを選択します。
- AWS アカウントにログインするか、AWS CLI/API を使用します。
- Contrast Serverless のスタック**を選択します。
- スタックアクション > 既存スタックの変更セットを作成**を選択します。



- 既存テンプレートを置き換える > テンプレートファイルのアップロード**を選択して、手順 1 でダウンロードしたテンプレートファイルをアップロードします。



## アカウントのブロック

アカウントのすべての Contrast Serverless アクティビティをブロックできます。

1. Contrast Web インターフェイスのナビゲーションバーで**サーバレス**を選択します。
2. **Settings** タブを選択します。
3. ページの下部にスクロールし **Block Account** をクリックします。

これにより、自動的なスキャンやユーザが要求したスキャン、機能の更新など、すべてのアクティビティがブロックされます。



### 注記

アカウントのブロックを解除するには、[Contrast サポート](#)に連絡してください。

## Contrast Serverless のオフボード

Azure から Contrast Serverless のアカウントをオフボーディングするには、スクリプトを使用してデプロイを削除する必要があります。

### 開始する前に

- 削除する対象を特定します

### 手順

1. Contrast Web インターフェイスのナビゲーションバーで**サーバレス**を選択します。
2. オフボードさせるアカウントを選択します。
3. **設定**タブを選択します。
4. **アカウントのオフボードセクション**までスクロールして、スクリプトをコピーします。
5. 認証済みの `az` コマンドを使用して、シェルで実行します。例えば、`Bash Azure CloudShell` などです。

## Contrast Serverless のアンインストール

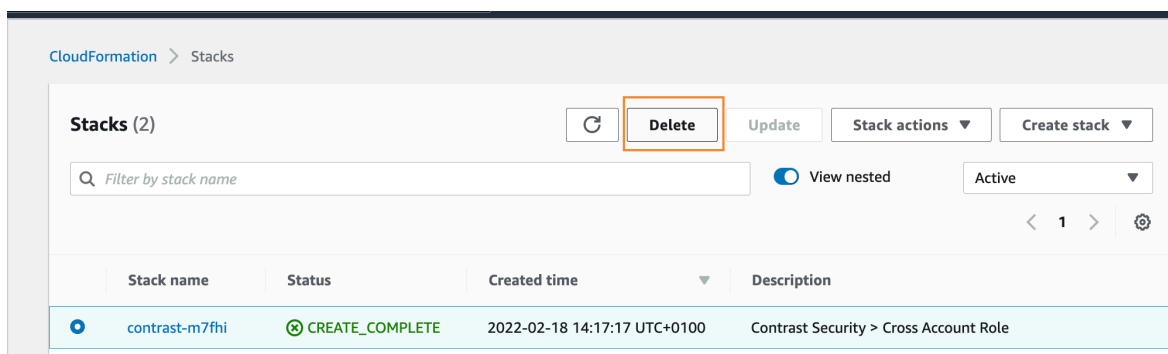
Contrast Serverless をアンインストールするには、AWS コンソールでスタックを削除する必要があります。

### 開始する前に

- 削除する対象を特定します

### 手順

- AWS アカウントにログインするか、AWS CLI/API を使用します。
- スタックを削除するための手順を続行します。☞ [AWS でのスタックの削除](#)を参照してください。



## Contrast CLI

Contrast CLI は、SCA、SAST、サーバレスの機能をコマンドラインで実現します。Contrast CLI はローカルで使用するか、CI/CD パイプラインの自動化で使用できます。

### 開始する前に

次の点に注意して下さい。

- CodeSec 利用者は、[こちら](#)から開始します。
- Contrast の企業ユースの場合は、Contrast CLI を [インストール \(573ページ\)](#)して使用を開始します。
- 従来の Contrast CLI は、2022 年 10 月をもって非推奨となります。

### Contrast CLI について

Contrast Security の Contrast CLI により、開発者の端末で直接セキュリティテストを行うことが可能になります。迅速なスキャン時間、業界トップの検出精度、すぐに対策可能な検出結果、シームレスなインテグレーションなどにより、ソースコードやサーバレスのセキュリティがシンプルかつ効率的になります。

Contrast CLI は、以下を提供します。

- 最速で高精度の SAST スキャナ
- ソースコードやサーバレス環境のスキャン結果 - すぐに対策できる検出結果
- SCA 機能 - 脆弱性が導入された箇所も含めてオープンソースライブラリ間の依存関係を表示

簡単な手順で [スキャンを開始](#) できます。Contrast アカウントが既にある場合は、[こちらのコマンド \(574ページ\)](#)を使用して、スキャンを開始できます。

### 関連項目

- [Contrast CLI のインストール \(573ページ\)](#)
- [Contrast CLI の実行 \(574ページ\)](#)

## Contrast CLI のサポート対象言語とパッケージマネージャ

Contrast CLI では、audit コマンドを使用する場合に次の言語をサポートします。

パッケージマネージャ	言語	必要なファイル	備考
RubyGems	Ruby	gemfile と gemfile.lock	
Composer	PHP	composer.json と composer.lock	
PyPI	Python	pipfile と pipfile.lock	
NuGet	.NET Core .NET Framework	MSBuild 15.0 以上と packages.lock.json	packages.lock.json ファイルがない場合、各*.csproj ファイル内で RestorePackagesWithLockFile を「true」に設定して dotnet build を実行することで生成できます。  .NET では、--legacy オプションの使用のみがサポートされます。
Maven Central	Java	pom.xml  build.gradle	Maven ビルドプラットフォーム(依存関係プラグインを含む)が必要  ./gradlew dependencies (または、Windows の場合 gradlew dependencies) が必要
npm	JavaScript	JavaScript	ロックファイルは、バージョン 2 とバージョン 3 の両方がサポートされています。
Gopm	Go	go.mod	

## Contrast CLI のインストール

スキャンを実行する前に Contrast CLI をインストールしてください。



### 注記

Contrast CLI V2.0 は、npm でインストールする場合のみ利用できます。

## Homebrew を使用する場合

以下のコマンドを実行し、Homebrew 経由で Contrast の tap からインストールします。

```
brew tap contrastsecurity/tap
brew install contrast
```

## NPM/YARN を使用する場合



### 注記

現在は、Node.js 16 以降のみがサポートされます。

npm または yarn @contrast/contrast を使用してインストールします。

CLI V2.0 には、以下のコマンドを使用します。

```
npm install --location=global @contrast/contrast@2.0.0
```

CLI V1.0 には、以下のコマンドを使用します。

```
npm install --location=global @contrast/contrast@1
```

## バイナリを使用する場合

- [アーティファクト](#)にアクセスします。
- 最新のパッケージをダウンロードします。
- OS によっては、ファイルに実行権限を設定する必要があります。

インストールが完了したら、[Contrast CLI の実行 \(574ページ\)](#)に進みます。

## Contrast CLI の実行

Contrast を企業ユースでご利用の場合、Contrast CLI を使用してスキャンを実行したり、脆弱なライブラリを見つけて Contrast で結果を参照することができます。CodeSec をご利用の場合は、[こちら](#)をご覧ください。

## 開始する前に

- 現在、Contrast のユーザであることが必要です。
- Contrast CLI が [インストール \(573ページ\)](#)されている必要があります。
- [Contrast CLI コマンド \(575ページ\)](#)について理解しておいてください。
- Contrast Web インターフェイスで、[ユーザメニュー](#) > [ユーザの設定](#) > [プロフィール](#)にアクセスし、以下の情報を取得してください。
  - API キー
  - 組織 ID
  - 認証ヘッダー
- Contrast のホストドメインの URL を取得してください。例、<https://app.contrastsecurity.com> (末尾のスラッシュは無し)

## 手順

### 1. 認証

脆弱性をスキャンする前に認証を行い、認証情報を保存します。以下の auth コマンドを実行して、認証情報をローカルに保存します。

```
contrast auth
--api-key <your API key>
--authorization <your authorization header>
--host <your host domain>
--organization-id <your organization ID>
```

### 2. 解析

#### • SAST スキャンの実行：

1. ターミナルで、次のコマンドを入力します：`contrast scan -f <file name>`
2. 検出結果で、リンクをクリックして[スキャン結果 \(513ページ\)](#)を確認します。

#### • 脆弱なライブラリの検査：

1. ターミナルで、次のコマンドを入力します：`contrast audit`
2. 'audit'コマンドで--track フラグを使用した場合、検出結果でリンクをクリックして[ライブ ラリを表示 \(535ページ\)](#)します。

- **AWS Lambda 関数の脆弱性の検査 :**

1. ターミナルで、次のコマンドを入力します : `contrast lambda--function-name []`
2. 検出結果で、推奨事項を確認し、提供された情報を基にポリシーを更新します。

## Contrast CLI コマンド

以下は、CodeSec 利用者およびエンタープライズユーザ(企業ユース)が利用できる Contrast CLI コマンドの一覧です。

**使用法 :** `contrast [] []`

### 認証/接続

#### auth

CodeSec 利用者の場合、GitHub または Google アカウントを使用して認証します。ログイン用の新しいブラウザ画面が開きます。

- **使用法 :** `contrast auth`

Contrast のアカウントを既にお持ちの場合は、以下の `auth` コマンドを実行すると、認証情報がローカルに保存されます。

- **使用法 :**

```
contrast auth
--api-key <your API key>
--authorization <your authorization header>
--host <your host domain>
--organization-id <your organization ID>
```

そして、コマンドを使用してスキャンを開始 (574ページ)します。

#### config

保存されている認証情報を表示します。

- **使用法 :** `contrast config`
- **オプション :**
  - `-c`、`--clear`  
保存されている認証情報を削除します。

#### version

Contrast CLI のバージョンを表示します。

- **使用法 :** `contrast version`

## メイン機能

#### audit

作業ディレクトリ内にある依存関係の設定ファイルを検索して依存関係のセキュリティ検査を実行し、結果を返します。

- **使用法 :** `contrast audit []`
- **オプション :**
  - `--fail`  
検出された CVE の深刻度に基づいて、ビルドを失敗させます。`--severity` オプションと一緒に使用します。例えば、`contrast audit --fail --severity high` です。深刻度を指定しない場合、すべての深刻度で失敗が返ります。失敗が検出された場合、CLI コマンドはコード 2 で終了します。

- `--file`  
依存関係が宣言されているディレクトリまたはファイルを指定します(デフォルトでは、Contrast CLI によって現在のディレクトリ内でプロジェクトファイルが検索されます)。ディレクトリ内で複数のプロジェクトファイルが見つかった場合、監査するファイルを確認するプロンプトが表示されます。  
**エイリアス:** `-f`
- `--ignore-dev`  
検査結果から開発・試験用ライブラリの依存関係を除外します。デフォルトでは、全ての依存関係が結果に含まれます。  
**エイリアス:** `-i`
- `--legacy`  
Contrast Web インターフェイスにアプリケーションを作成します(旧 CLI のワークフロー)。コードの[依存関係ツリー \(543ページ\)](#)を表示し、メタデータを利用します。これは、Contrast CLI V2.0 でのみ利用可能であることにご注意ください。
- `--name`  
カスタムのプロジェクト名を設定します。名前が既に使用されている場合は、そのプロジェクトの検出結果を置き換えます。特殊文字は使用しないで下さい。
- `--save`  
SBOM(ソフトウェア部品表)を SPDX や CycloneDX 形式で生成して保存します。有効なオプション: `--save cyclonedx`、`--save spdx` (CycloneDX 形式がデフォルト)  
**エイリアス:** `-s`
- `--severity`  
ビルドを失敗させる CVE の最低レベルの深刻度を指定します。`--fail` オプションと一緒に使用します。例えば、`contrast audit --fail --severity high` です。深刻度は、*critical*、*high*、*medium*、*low*、または *note* です。
- `--track`  
デフォルトでは、結果は保持・保存されないため、コンソールでローカルチェックを行うことになります。`--track` フラグを追加すると、Contrast Web インターフェイスの[ライブラリ \(535ページ\)](#)ページにある静的タブに、プロジェクトの SCA 結果を表示できます。これは、Contrast CLI V2.0 でのみ利用可能使用であることにご注意ください。
- **詳細オプション:**
  - `--api-key`  
エンタープライズユーザには必須です。Contrast で提供されるエージェントの API キーを指定します。キーの検索方法については、[エージェントキー \(37ページ\)](#)を参照してください。
  - `--application-id`  
Contrast に登録されているアプリケーションの ID を指定します。
  - `--application-name`  
Contrast に登録されているアプリケーションの名前です。
  - `--app-groups`  
アプリケーションのオンボーディング時に、1 つ以上の既存のグループにアプリケーションを割り当てます。グループリストは、カンマで区切る必要があります。
  - `--authorization`  
エンタープライズユーザには必須です。Contrast で提供される認証ヘッダーです。
  - `--code`  
Contrast でアプリケーションに使用するアプリケーションコードです。
  - `--host`  
エンタープライズユーザには必須です。ホスト名を指定します。(例) `https://app.contrastsecurity.com/`
  - `--maven-settings-path`  
maven の `settings.xml` ファイルのパスを表示します。
  - `--metadata`



アプリケーションに関連付けるユーザ定義のメタデータを指定するための、キーと値のペアのセット(RFC 2253 に準拠)を定義します。

- `--organization-id`  
エンタープライズユーザには必須です。Contrast での組織 ID を指定します。ID の検索方法については、[エージェントキー \(37ページ\)](#)を参照してください。
- `--tags`  
アプリケーションにタグを適用します。タグは、カンマ区切りのリストとして書式設定する必要があります。(例) `label1,label2,label3`
- **プロキシの設定 :**
  - `--cacert`  
CaCert(認証局(CA)による証明書)ファイルのパスを表示します。
  - `--cert`  
Cert(証明書)ファイルのパスを表示します。
  - `--cert-self-signed`  
ローカルインストールした Contrast オンプレミス(EOP)をご利用のお客様の場合、SSL 証明書をバイパスして自己署名証明書を認識します。
  - `--key`  
証明書の鍵のパスを表示します。
  - `--proxy`  
プロキシサーバ経由の接続を許可します。認証が必要な場合は、ユーザ名とパスワード、プロトコル、ホスト、ポートを例のように指定します。(例) `"http://username:password@<host>:<port>"`

## scan

SAST スキャンを実行します。

- **使用法 :** `contrast scan []`
- **オプション :**
  - `--fail`  
検出された脆弱性の深刻度に基づいて、ビルドを失敗させます。`--severity` オプションと一緒に使用します。例えば、`contrast scan --fail --severity high` です。深刻度を指定しない場合、すべての深刻度で失敗が返ります。失敗が検出された場合、CLI コマンドはコード 2 で終了します。
  - `--file`  
スキャンするファイルのパスを指定します。ファイルが指定されていない場合は、Contrast はサポート対象ファイル(.jar、.war、.js、.zip ファイル)を作業ディレクトリ内で検索します。  
エイリアス : `-f`
  - `--host`  
エンタープライズユーザには必須です。ホスト名を指定します。(例) `https://app.contrastsecurity.com/`
  - `--language`  
有効な値 : JAVA、JAVASCRIPT、DOTNET  
エイリアス : `-l`
  - `--name`  
Contrast のプロジェクト名を指定します。指定されていない場合、Contrast は `contrast.settings` を使用してプロジェクトを識別するか、プロジェクトを作成します。  
エイリアス : `-n`
  - `--save`  
検出結果を SARIF(Static Analysis Results Interchange Format)ファイルでダウンロードします。ファイルは、デフォルトの名前の `results.sarif` で現在の作業ディレクトリにダウンロードされます。このファイルは、任意のテキストエディタで表示できます。  
エイリアス : `-s`
  - `--severity`

ビルドを失敗させる脆弱性の最低レベルの深刻度を指定します。--fail オプションと一緒に使用します。例えば、**contrast scan --fail --severity high** です。深刻度は、*critical*、*high*、*medium*、*low*、または *note* です。

- --timeout  
スキャンが完了するまでの待機時間(wait)を秒数で指定します。デフォルトの値は、300 秒です。  
エイリアス: -t
- **詳細オプション:**
  - --api-key  
エンタープライズユーザには必須です。Contrast で提供されるエージェントの API キーを指定します。キーの検索方法については、[エージェントキー \(37ページ\)](#)を参照してください。
  - --authorization  
エンタープライズユーザには必須です。Contrast で提供される認証ヘッダーです。
  - -ff  
ファイア・アンド・フォーゲット(Fire-&forget)。実行させておくだけで、結果を監視・待つ必要がありません。
  - --host  
エンタープライズユーザには必須です。ホスト名を指定します。(例) `https://app.contrastsecurity.com/`
  - --label  
スキャンにラベルを付けます。デフォルトは、*CLI ツールで開始した日付[現在の日付]*です。
  - --organization-id  
エンタープライズユーザには必須です。Contrast での組織 ID を指定します。ID の検索方法については、[エージェントキー \(37ページ\)](#)を参照してください。
  - --project-id  
スキャンプロジェクトに関連付けられた ID です。ID は、Contrast Web インターフェイスでスキャンプロジェクトを選択した際の URL にある最後の文字列です。
- **プロキシの設定:**
  - --cacert  
CaCert(認証局(CA)による証明書)ファイルのパスを表示します。
  - --cert  
Cert(証明書)ファイルのパスを表示します。
  - --cert-self-signed  
ローカルインストールした Contrast オンプレミス(EOP)をご利用のお客様の場合、SSL 証明書をバイパスして自己署名証明書を認識します。
  - --key  
証明書の鍵のパスを表示します。
  - --proxy  
プロキシサーバ経由の接続を許可します。認証が必要な場合は、ユーザ名とパスワード、プロトコル、ホスト、ポートを例のように指定します。(例) `"http://username:password@<host>:<port>"`

## lambda

AWS Lambda 関数をスキャンします。スキャンする AWS Lambda の関数名を指定してください。

- **使用法:** `contrast lambda --function-name <> []`
- **エイリアス:** -f
- **オプション:**
  - --endpoint-url  
AWS エンドポイントを上書きします。AWS CLI と同様です。  
エイリアス: -e
  - --region  
AWS リージョンを上書きします。デフォルトは、`AWS_DEFAULT_REGION` です。AWS CLI と同様です。  
エイリアス: -r

- `--profile`  
AWS の設定プロファイルを上書きします。AWS CLI と同様です。  
エイリアス: `-p`
- `--json`  
人が判読できるデフォルトのフォーマットではなく、レスポンスを JSON 形式で返します。  
エイリアス: `-j`
- `--verbose`  
ターミナルに詳細情報を返します。  
エイリアス: `-v`
- `--list-functions`  
スキャン可能な Lambda 関数を一覧表示します。
- `--help`  
使用方法を表示します。  
エイリアス: `-h`
- **プロキシの設定:**
  - `--cacert`  
CaCert(認証局(CA)による証明書)ファイルのパスを表示します。
  - `--cert`  
Cert(証明書)ファイルのパスを表示します。
  - `--cert-self-signed`  
ローカルインストールした Contrast オンプレミス(EOP)をご利用のお客様の場合、SSL 証明書をバイパスして自己署名証明書を認識します。
  - `--key`  
証明書の鍵のパスを表示します。
  - `--proxy`  
プロキシサーバ経由の接続を許可します。認証が必要な場合は、ユーザ名とパスワード、プロトコル、ホスト、ポートを例のように指定します。(例) "`http://username:password@<host>:<port>`"

## ヘルプと学習コンテンツ

### help

使用方法を表示します。CLI コマンドの詳細なヘルプを一覧表示するには、`-h` か `--help` フラグをコマンドに追加します。

- **使用法:** `contrast scan --help`
- **エイリアス:** `-h`

### learn

[Contrast の Secure Code ラーニングハブ](#)を表示します。

- **使用法:** `contrast learn`

## 旧 Contrast CLI



### 重要

従来の Contrast CLI は、2022 年 10 月をもって非推奨となります。新しい [Contrast CLI \(572ページ\)](#) をご利用頂きますようお願いします。

Contrast コマンドラインインターフェイス(Contrast CLI)を使用すれば、ソフトウェア開発ライフサイクル(SDLC)の初期段階でライブラリを解析できます。

Contrast CLI は Node.js で実行しますが、あらゆるアプリケーションで使用でき、コマンドラインでコンポジション解析機能が提供されます。サポート対象のプラットフォームや言語については、[Contrast CLI のサポート対象言語 \(580ページ\)](#)のページを参照してください。

このコンポジション解析によって、以下が可能です。

- 脆弱なライブラリを特定する
- CVE の深刻度に基づいてビルドを失敗させる
- [依存関係ツリー \(543ページ\)](#)を表示し、ライブラリ間の依存関係や脆弱性がある箇所を把握する
- 依存関係かく乱の危険性がある Node.js ライブラリを特定する
- SBOM を作成する

Contrast CLI は、Contrast エージェントによる既存のランタイムの解析を補完し、コンパイル前の解析(通常、ランタイムには不可)を実現するものです。

[Contrast CLI をインストール \(580ページ\)](#)して、[アプリケーションを登録 \(581ページ\)](#)すれば、開発フェーズで[コマンドラインオプション \(583ページ\)](#)を使用してライブラリの解析を開始できます。

## 旧 Contrast CLI のサポート対象言語

Contrast CLI でサポートされる言語と要件は以下の通りです。

言語	要件	備考
Java	Maven	Maven プロジェクトは、pom.xml ファイルで定義され、 <a href="#">Apache Maven Dependency プラグイン</a> が必要です。CLI がプロジェクトで動作するかをテストするには、 <code>mvn dependency:tree</code> を実行して依存関係ツリーを表示します。
	Gradle (バージョン 4.8 以上)	<code>build.gradle</code> ファイルが必須となり、 <code>gradle dependencies</code> または <code>.gradlew dependencies</code> にも対応している必要があります。
.NET Framework、.NET Core	MSBuild 15.0 以上と <code>packages.lock.json</code> ファイル	<code>packages.lock.json</code> ファイルがない場合、各 <code>csproj</code> 内で <code>RestorePackagesWithLockFile</code> を <code>true</code> に設定して、.NET build を実行することで生成できます。
Node.js	<code>package-lock.json</code> または <code>yarn.lock</code> ファイルのいずれかが必要です。	脆弱性の報告は、React や Angular などのフロントエンドテクノロジーに対してサポートされます。
PHP	<code>compose.lock</code> ファイルと <code>composer.json</code> ファイルが存在している必要があります。	
Python	<code>pipfile</code> および <code>pipfile.lock</code> ファイルが必要です。	
Ruby	<code>gemfile</code> および <code>gemfile.lock</code> ファイルが必要です。	
Go	<code>go.mod</code> ファイルが必要です。	



### 注記

現時点では、単一言語のアプリケーションのみがサポートされます。

## 旧 Contrast CLI のインストール

[Contrast CLI \(579ページ\)](#)をインストールするには：

1. [Node.js をインストール](#)します。Contrast CLI は Node.js パッケージとして実行されるため、これは必須です。現在、バージョン 10、12、14 に対応しています。

2. 検査対象のアプリケーションに Contrast エージェントを組み込んで起動します。これによって、Contrast CLI で参照するためのアプリケーション ID を取得できます。



### 注記

まだエージェントが組み込まれていないアプリケーションも、[Contrast CLI で登録 \(581ページ\)](#)することができます。ただし、アプリケーションの[ライブラリスコア \(544ページ\)](#)を評価して、ライブラリー一覧を作成するには、エージェントを組み込んでアプリケーションを起動する必要があります。

3. プロキシ経由で Contrast と通信を行うには、エージェントの設定で `cli_proxy` プロパティを使用してください。  
認証が必要な場合は、ユーザ名とパスワード、プロトコル、ホスト、ポートを以下の例のように指定します。例：

```
http://username:password@<host>:<port>
```

4. Contrast CLI で解析を行うには、対象のアプリケーションのソースコードが、ローカルで利用できる必要があります。アプリケーションの[言語 \(580ページ\)](#)の要件に従ってください。
5. 以下のコマンドを実行して、Contrast CLI をインストールします。

```
npm install -g @contrast/contrast-cli
```

または、以下のコマンドで yarn を使用して Contrast CLI をインストールすることもできます。

```
yarn global add @contrast/contrast-cli
```



### 注記

Contrast CLI のインストールは、グローバルインストールで行う必要があります。

6. Contrast CLI のインストールが完了したら、[アプリケーションを登録 \(581ページ\)](#)して、コードの解析を始めることができます。

## 旧 Contrast CLI でアプリケーションを登録

[Contrast CLI をインストール \(580ページ\)](#)したら、結果を Contrast Web インターフェイスで確認するために、アプリケーションを最初に登録する必要があります。



### ヒント

Contrast CLI を CI パイプラインの一部として呼び出し、ビルドプロセスの一部として自動化することもできます。

1. アプリケーション ID を確認します。アプリケーション ID は、ブラウザの Contrast URL の最後の URI セグメントです。



2. 認証に関する[キー \(478ページ\)](#)を確認します。以下が必要です。
  - API キー
  - 組織 ID

- 認証ヘッダー
- Contrast URL のサーバホスト名



### 注記

入力する必要があるのは、サーバホスト名だけです。例えば、Contrast URL が `https://app.contrastsecurity.com/file/path/` の場合は、以下のように入力します。

```
--host app.contrastsecurity.com
```

3. 以下のオプションのいずれかを使用して CLI を実行し、解析を開始します。
  - <APIKey>、<AuthorizationKey>、<OrganizationID>、<Host>および<ApplicationID>を、自分の API キー、認証ヘッダ、組織 ID、ホスト名およびアプリケーション ID に置き換えて、以下のコマンドを実行します。

```
contrast-cli \  
--api_key <APIKey> \  
--authorization <AuthorizationKey> \  
--organization_id <OrganizationId> \  
--host <Host> \  
--application_id <ApplicationId>
```

- 上記と同様に<>の箇所を置き換えて、認証情報を YAML ファイル内に指定します。

```
cli:  
  api_key: <APIKey>  
  authorization: <AuthorizationKey>  
  organization_id: <OrganizationId>  
  host: <Host>  
  application_id: <ApplicationId>
```

<path/to/yaml>を自分の YAML パスに置き換えて、以下のコマンドを実行して開始します。

```
contrast-cli --yaml_path <path/to/yaml>
```



### 注記

TLS(Transport Layer Security)などの通信プロトコルを経由する必要がある場合は、YAML ファイルに以下のパラメータを追加します。

```
key: pathToKey  
cert: pathToCert  
cacert: pathToCaCert
```

4. 「SUCCESS」のメッセージが表示されたら、[依存関係ツリーを表示 \(543ページ\)](#)できます。



## ヒント

まだ Contrast で検査を行っていないアプリケーションでも、`--catalogue_application` と `--application_name` オプションを使用して、新規にアプリケーションを Contrast に登録することができます。ただし、Contrast Web インターフェイスでライブラリのスコア (544ページ) とライブラリ一覧が表示されるようにアプリケーションにエージェントを組み込んで (35ページ) 起動することをお勧めします。

例：

```
contrast-cli \  
--catalogue_application \  
--api_key <YourApiKey> \  
--authorization <YourAuthorizationKey> \  
--organization_id <YourOrganizationID> \  
--host <YourHost> \  
--application_name <YourApplicationName> \  
--language <YourApplicationLanguage>
```

<ApiKey>、<AuthorizationKey>、<OrganizationID>、<Host>、<ApplicationName>を、自分の API キー、認証ヘッダ、組織 ID、ホスト名、およびアプリケーション名に置き換えます。また<ApplicationLanguage>は、解析するアプリケーションの言語に置き換えます。指定できる言語の値は、JAVA、DOTNET、NODE、PHP、PYTHON、RUBY、GO です。

この登録(catalogue)操作が成功すると、コンソールにアプリケーション ID が出力されます。



## 注記

CLI コマンドの一連のオプション (583ページ) を指定することで、アプリケーションの登録と SBOM レポートの作成を同時に行うこともできます。

## 旧 Contrast CLI のコマンド

CLI で `-h` または `--help` オプションを指定すると、コマンドラインのヘルプを参照できます。ヘルプガイドには、Contrast の設定、アプリケーション、脆弱性などに関する情報を理解するために使用できる以下のコマンドオプションがあります。

下記の例では、<string>や<level>をご利用の環境に合わせた値に置き換えてください。

### 一般的なコマンド

接続や設定に関するコマンドオプションです。

オプション	説明
<code>--api_key &lt;string&gt;</code>	Contrast で提供されるエージェントの API キー (37ページ)(必須)
<code>--application_id &lt;string&gt;</code>	Contrast に登録されているアプリケーションの ID(必須)
<code>--application_name &lt;string&gt;</code>	Contrast に登録されているアプリケーションの名前(任意)

オプション	説明
<code>--authorization &lt;string&gt;</code>	Contrast で提供されるユーザの認証ヘッダ(必須)
<code>-h, --help</code>	ヘルプを表示します。
<code>--host &lt;string&gt;</code>	ホスト名。オプションでポートを<host>:<port>と指定することもできます。URL のプロトコル要素 ( <code>https://</code> )は含めません。デフォルトは、 <code>app.contrastsecurity.com</code> です。(任意)
<code>--language &lt;string&gt;</code>	アプリケーションの言語。有効な値は、JAVA、DOTNET、NODE、PHP、PYTHON、RUBY、GO。 <code>project_path</code> に複数のプロジェクトの設定ファイルがある場合、言語の指定が必須。(catalogue 操作には必須)
<code>--organization_id &lt;string&gt;</code>	Contrast での組織 ID (37ページ)(必須)
<code>--project_path &lt;string&gt;</code>	検査したいプロジェクトやアプリケーションのディレクトリのルート。デフォルトは現在のディレクトリです。(任意、但し Windows で実行する場合は必須)
<code>--proxy &lt;string&gt;</code>	Proxy サーバ経由の接続を許可します。認証が必要な場合は、ユーザ名とパスワード、プロトコル、ホスト、ポートを例のように指定します(任意)。例、 <code>http://username:password@&lt;host&gt;:&lt;port&gt;</code>
<code>--silent</code>	JSON 出力をサイレントにします。(任意)
<code>--sub_project &lt;string&gt;</code>	Gradle アプリケーション内のサブプロジェクトを指定します。(任意)
<code>-v, --version</code>	現在使用している CLI のバージョンを表示します。
<code>--yaml_path &lt;string&gt;</code>	YAML ファイルからパラメータを読み込む場合に指定する YAML ファイルへのパス(任意)  <code>yaml_path</code> を使用すると、ターミナルからの以下の接続パラメータは無視されます。  <ul style="list-style-type: none"> <li>• <code>yamlOnly:</code></li> <li>• <code>key:pathToKey</code></li> <li>• <code>cert:pathToCert</code></li> <li>• <code>cacert:pathToCaCert</code></li> </ul>



### 注記

特殊文字の問題を回避するために、これらのコマンドのパラメータを引用符で囲む必要がある場合があります。例：

```
--application_name = "My_app_name_${+}(</\>"
```

## SCA

Contrast SCA の検査に関するコマンドオプションです。

オプション	説明
<b>アプリケーションのカタログ作成</b>	
<code>--app_groups &lt;string&gt;</code>	<code>catalogue</code> コマンドを使用時に、アプリケーションを1つ以上の既存のグループに割り当てます。グループリストは、カンマで区切る必要があります。(任意)
<code>--catalogue_application</code>	アプリケーションを登録( <code>catalogue</code> )します(必須)。アプリケーション名が存在しない場合は、アプリケーションを作成して依存関係ツリーが送信され、存在する場合は既存のアプリケーションに依存関係ツリーが追加されます。
<code>--code &lt;string&gt;</code>	Contrast でこのアプリケーションに使用するアプリケーションコード(任意)



オプション	説明
<code>--metadata &lt;string&gt;</code>	アプリケーションに関連付けるユーザ定義のメタデータを指定するための、キーと値のペアのセット(RFC 2253 に準拠)を定義します。(任意)
<code>--tags &lt;string&gt;</code>	アプリケーションにタグを適用します。タグは、カンマ区切りのリストとして書式設定する必要があります(任意)。例 : label1,label2,label3
<b>スナップショット - Java のみ</b>	
<code>--maven_settings_path &lt;PathToFile&gt;</code>	Maven の settings.xml ファイルの別の場所を指定できます。<PathToFile>の箇所をファイルのフルパスに置き換えます。 <a href="#">Contrast CLI でアプリケーションを登録 (581ページ)</a> するとき、一連のキーにこのパスを追加してください。(任意)
<b>アプリケーションの登録</b>	
<code>--cli_api_key &lt;string&gt;</code>	アプリケーションの登録と SBOM レポートの取得を同時に行うには、この一連のコマンドオプション(値は前述と後述の表に記載)を使用します。
<code>--cli_authorization &lt;string&gt;</code>	
<code>--cli_organization_id &lt;string&gt;</code>	注 : パラメータの"cli_"という接頭辞は、将来のリリースで廃止される予定です。
<code>--cli_host &lt;string&gt;</code>	
<code>--language &lt;string&gt;</code>	
<code>--application_name &lt;string&gt;</code>	
<code>--sbom</code>	
<b>レポート</b>	
<code>--cve_severity &lt;level&gt;</code>	<code>--report</code> と組み合わせると、選択した <a href="#">深刻度 (602ページ)</a> 以上の脆弱性があるライブラリが報告されます。例えば、 <code>cve_severity medium</code> を指定すると、 <b>中(Medium)</b> と中より高い深刻度の脆弱性のみが報告されます。
<code>--cve_threshold &lt;number&gt;</code>	ビルドが失敗するまでに許容する CVE の数をしきい値として設定します。しきい値を超える CVE があると、ビルドは失敗になります。
<code>--fail</code>	脆弱性が検出された場合、ビルドを失敗にします。 <code>cve_severity</code> と組み合わせると、定義した深刻度の脆弱性検出時にビルドを失敗にすることができます。
<code>--report</code>	コンパイル時のアプリケーションの脆弱性情報を表示します。
<code>--ignore_dev</code>	<code>--report</code> コマンドと組み合わせると、開発: 試験用ライブラリの依存関係を脆弱性レポートから除外します。デフォルトでは、全ての依存関係がレポートに含まれます。
<b>SBOM</b>	
<code>--sbom</code>	<a href="#">SBOM(ソフトウェア部品表) (614ページ)</a> を CycloneDX JSON フォーマットで生成してダウンロードします。



## ヒント

`--report` コマンドを使用すると、全ての脆弱なライブラリの情報がターミナルに返されます。検出された全ての CVE は、以下のように出力されます。

```
org.webjars/jquery-ui/1.11.4 is vulnerable

CVE-2016-7103 MEDIUM Cross-site scripting (XSS) vulnerability \
in jQuery UI before 1.12.0 might allow remote attackers to \
inject arbitrary web script or HTML via the closeText \
parameter of the dialog function.
```

`--cve_severity` パラメータを使用して、レポートする CVE の最小しきい値を設定することで、出力される脆弱性情報を制限できます。

`--fail` パラメータを、自動化された CI/CD パイプラインの一部に使用することで、深刻度のしきい値を超えたライブラリでアプリケーションがデプロイされないようにできます。例えば、次のように YAML ファイルを使用して CLI を実行できます。

```
contrast-cli --yaml_path path/to/yaml --report --cve_severity \
high --fail
```

## スキャン

Contrast Scan に関連するコマンドオプションです。[ビルドとスキャンのインテグレーション \(525ページ\)](#) もご覧ください。

Contrast Scan は、.NET プロジェクトの EXE および ZIP ファイルをサポートします。アプリケーションの言語は DOTNET に設定し、ZIP は DLL を含む .bin フォルダの ZIP である必要があります。

オプション	説明
<code>--project_id &lt;ProjectID&gt;</code>	<p>スキャンプロジェクトに関連付けられた ID。&lt;ProjectID&gt; をスキャンプロジェクトの ID に置き換えます。ID は、Contrast Web インターフェイスでスキャンプロジェクトを選択した際の URL にある最後の文字列です。</p> <p><b>推奨:</b> 最初のスキャンでは、このオプションの代わりに <code>--project_name</code> オプションを使用してください。スキャンによってプロジェクトが作成されます。</p>
<code>--project_name</code>	<p>スキャンプロジェクトの名前を指定します。プロジェクト名にスペースが含まれる場合は、二重引用符(")で囲みます。</p> <p>新しい名前を指定すると、プロジェクトが作成されます。既存の名前を指定すると、アップロードされたファイルはそのプロジェクトに追加されます。</p>
<code>--save_scan_results</code>	<p>このオプションが指定された場合は、SARIF ファイルが <code>results.json</code> として現在のディレクトリに保存されます。(任意)</p>
<code>--scan&lt;FileToBeScanned&gt;</code>	<p>指定された WAR または JAR ファイルの静的スキャンを開始します。&lt;FileToBeScanned&gt; を、スキャン用にアップロードする WAR または JAR ファイルのパスに置き換えます。</p>
<code>--scan_results_file_name</code>	<p>JSON ファイル形式である必要があります。このオプションが指定された場合は、SARIF ファイルを保存するためのデフォルトファイル名が上書きされます。(任意)</p>
<code>--scan_timeout</code>	<p>スキャンがタイムアウトするまでの時間(秒単位で)を指定します。scan_timeout が設定されていない場合、デフォルトのタイムアウトは 20 秒です。</p>

オプション	説明
--wait_for_scan	スキャンの結果を待機(wait)します。

## 脆弱性

アプリケーションにエージェントを組み込む (35ページ)と、アプリケーションで検出された全ての脆弱性が Contrast に表示され、最も一般的で重大なリスクやその他の多くの脆弱性に対処することができます。

Contrast エージェントにより、アプリケーションにあるコードの欠陥が検出されて報告されます。これらの脆弱性は深刻度を付けて表示・分類されるので、必要に応じて、対処する脆弱性の優先順位を決め、脆弱性のステータスを更新することができます。

- [脆弱性の表示 \(587ページ\)](#)
- [アプリケーションの脆弱性を表示 \(588ページ\)](#)
- [脆弱性の解析 \(595ページ\)](#)
- [脆弱性の追跡 \(594ページ\)](#)
- [脆弱性の修正 \(596ページ\)](#)

## 組織レベルで脆弱性を表示

### 開始する前に

- Contrast で脆弱な箇所を検出して結果を表示できるよう、アプリケーションを疎通(閲覧や操作)します。
- より詳細な脆弱性情報を参照したい場合は、[セッションメタデータ \(489ページ\)](#)を報告するよう Contrast エージェントを設定します。

### 手順

1. Contrast Web インターフェイスのナビゲーションバーで**脆弱性**を選択します。
2. 脆弱性一覧の一番上で、**ライセンスありのみを表示**を選択すると、ライセンスのあるアプリケーションのみが表示されます。
3. 列でフィルタをかけるには、列のヘッダの横にある**フィルタアイコン(▼)**を選択します。フィルタには以下のオプションがありますが、選択したアプリケーションに適用可能な場合に利用できます。
  - **深刻度**：利用可能なフィルタは、重大、高、中、低、注意です。
  - **脆弱性**：利用可能なフィルタは次の通りです。
    - **脆弱性のタグ**：作成したカスタムタグに関連付けられた脆弱性。
    - **種類**：脆弱性の種類。
    - **サーバ**：選択したサーバに関連するアプリケーションの脆弱性。
    - **環境**：選択した環境(開発、QA、本番)にあるアプリケーションの脆弱性。
    - **シンク**：共通のシンクに起因する脆弱性。  
シンクは、複数のデータフローの脆弱性間で共有されているカスタムコードです。  
シンクでフィルタをかけることで、複数の脆弱性の原因となっているコード行を特定することができます。
    - **URL**：特定の URL に関連する脆弱性。
    - **コンプライアンスポリシー**：コンプライアンスポリシーに関連する脆弱性。
  - **アプリケーション**：利用可能なフィルタは次の通りです。
    - **アプリケーション名**：アプリケーションに関連付けられた名前。
    - **カスタムタグ**：アプリケーションに割り当てたタグ。
    - **言語**：アプリケーションで使用されている言語。
    - **テクノロジー**：アプリケーションで使用されているテクノロジー。例えば、JSON や jQuery など。
    - **アプリケーションの重要度**：アプリケーションの設定で指定したアプリケーションの重要性。

- **アプリケーションのメタデータ**：アプリケーションに関連付けたカスタムメタデータ。
- **最後の検出**：利用可能なフィルタは、最初の検出、最後の検出、時間範囲です。特定の日付と時刻を指定する場合は、**カスタム**を選択します。
- **ステータス**：利用可能なフィルタは、ステータスおよび脆弱性を追跡中かどうかです。フィルタを解除するには、列のヘッダの横にある**クリア**を選択します。

脆弱性 ▼ **クリア**

4. 脆弱性の詳細を表示するには、脆弱性の名前を選択します。以下のカテゴリの情報が表示されます。
  - HTTP 情報
  - 脆弱性を修正する方法
  - ビルド番号、脆弱性を報告しているサーバ、脆弱性のカテゴリ、セキュリティ基準など、脆弱性の識別やタイミング、場所に関する詳細な情報。

## 関連項目

[アプリケーションの脆弱性を表示 \(588ページ\)](#)

## アプリケーションの脆弱性の表示

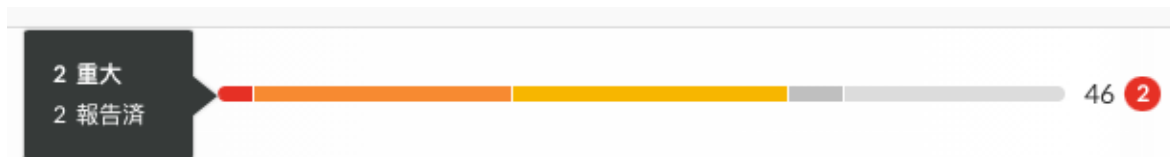
アプリケーションページのアプリケーション一覧から、特定のアプリケーションの脆弱性を表示できます。

### 開始する前に

- Contrast で脆弱な箇所を検出して結果を表示できるよう、アプリケーションを疎通(閲覧や操作)します。
- より詳細な脆弱性情報を参照したい場合は、[セッションメタデータ \(489ページ\)](#)を報告するように Contrast エージェントを設定します。

### 手順

1. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択します。アプリケーションの一覧には、各アプリケーションでオープン中の脆弱性の数が表示されます。特定の種類(重大、高など)の脆弱性に関する情報を表示するには、「オープン中の脆弱性」の列にある棒グラフで該当する箇所を選択します。





- オープン中の脆弱性とは、ステータスが報告済、疑わしい、確認済のものです。
2. あるいは、アプリケーションの一覧でアプリケーション名を選択して、**脆弱性タブ**を選択します。選択したアプリケーションの脆弱性の一覧が表示されます。
  3. 脆弱性タブで脆弱性にフィルタをかけるには、一覧の最上部にある小さい三角形を選択します。

オープン中 (1877) ▼ 🔍

利用できるフィルタ：

- オープン中
  - 信頼性の高い問題
  - ポリシー違反
  - レビュー待ち
4. 特定の脆弱性を検索するには、虫眼鏡アイコン(🔍)を選択します。

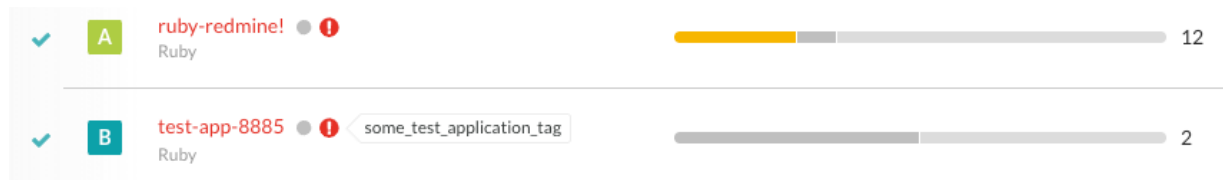
5. 一覧の上部にある**傾向線**のマーク(  )を選択すると、脆弱性のタイムラインが表示されます。グラフの上のボタンを使用すると、**深刻度**(Severity)または**検出**(Discovery)別にデータの表示が切り替わります。グラフの傾向線にカーソルを合わせると、その時点でのデータの内訳(脆弱性の数、タイムスタンプまたはステータス)が表示されます。脆弱性一覧のフィルタを適用すると、グラフのデータも更新されます。**最後の検出**の列のフィルタを使用すると、タイムラインに表示される期間が更新されます。
6. 列でフィルタをかけるには、列のヘッダの横にあるフィルタアイコン  を選択します。フィルタには以下がありますが、選択したアプリケーションに適用可能な場合に利用できます。
  - **深刻度**：利用可能なフィルタは、重大、高、中、低、注意です。
  - **脆弱性**：選択したアプリケーションで適用可能な場合、利用可能なフィルタは以下の通りです。
    - **脆弱性のタグ**：脆弱性に割り当てたカスタムタグ。
    - **バグ管理システム**：バグ管理システムとの連携を利用して、脆弱性を追跡しているかどうか。
    - **種類**：脆弱性の種類。
    - **モジュール**：脆弱性に関連するアプリケーションモジュール(マージされたアプリケーションのモジュールも含む)。
    - **サーバ**：アプリケーションをホストしているサーバ。
    - **環境**：開発環境、QA 環境、本番環境。
    - **シンク**：共通のシンクに起因する脆弱性。  
シンクは、複数のデータフローの脆弱性間で共有されているカスタムコードです。  
シンクでフィルタをかけることで、複数の脆弱性の原因となっているコード行を特定することができます。
    - **URL**：特定の URL に関連する脆弱性。
    - **コンプライアンスポリシー**：選択したコンプライアンスポリシーに関連する脆弱性。
    - **ルート**：選択したルートに関連する脆弱性。
  - **アプリケーション**：アプリケーションに含まれるモジュール。  
マージされていないアプリケーションを参照している場合は、選択したアプリケーションの脆弱性がこのフィルタによって表示されます。  
マージされたアプリケーションの脆弱性を参照している場合は、マージされたアプリケーションのモジュールの脆弱性がこのフィルタによって表示されます。
  - **最後の検出**：利用可能なフィルタは、最初の検出、最後の検出、時間範囲です。特定の日付と時刻を指定する場合は、**カスタム**を選択します。
  - **ステータス**：利用可能なフィルタは、ステータスおよび脆弱性を追跡中であるかどうかです。
  - **セッション**：この列は、エージェントの設定ファイルにセッションメタデータが設定されているが、セッションメタデータフィルタを選択していない場合に表示されます。「セッション」列フィルタを使用して、結果を絞り込むことができます。  
一覧の上にある**〜で表示**(〜はプロパティ名)メニューを使用して、エージェントの設定ファイルで指定したセッションメタデータ値で、データを絞り込みます。このフィルタは、「セッション」列に表示される値を更新します。  
「〜で表示」メニューは、エージェントの設定ファイルにセッションメタデータが設定されているが、セッションメタデータフィルタを選択していない場合に表示されます。

## マージしたアプリケーションでオープン中の脆弱性

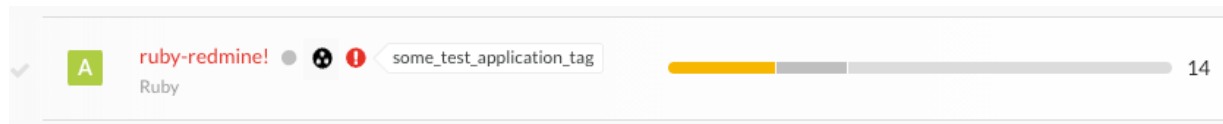
マージしたアプリケーションの場合、アプリケーション一覧の「オープン中の脆弱性」列には、メインアプリケーションにある全てのアプリケーションモジュールの脆弱性の数が表示されます。アプリケーション一覧には、メインアプリケーションは表示されますが、メインアプリケーションに含まれるモジュールは表示されません。

例：

アプリケーションをマージする前の「オープン中の脆弱性」列が、以下のものであるとします。



アプリケーションをマージしたら、「オープン中の脆弱性」列にある棒グラフには、メインアプリケーションとマージされた全てのモジュールの脆弱性が表示されます。



マージされたアプリケーションの「脆弱性」タブを表示して、「アプリケーション」列のフィルタを使用すると、Contrastで脆弱性が検出されたモジュール名が表示されます。



## 関連項目

[組織レベルで脆弱性を表示 \(587ページ\)](#)

## 脆弱性の発生率の表示

オープン中およびクローズされた脆弱性の比率を表すグラフは、組織内のすべてのアプリケーションの脆弱性の傾向を示します。

## 手順

1. **新しいダッシュボードを表示**を選択して、新しいダッシュボードを表示します。

**新しいダッシュボードを表示 (ベータ)**

2. 新しいダッシュボードにある、**オープン中とクローズ済みの脆弱性の比率**のグラフを使用します。
3. グラフの期間を選択：
  - **過去 7 日間**：現在の日付から 7 日前までの脆弱性の発生率が表示されます。グラフには、各日のデータポイントが表示されます。
  - **過去 30 日間**：現在の日付から 30 日前までの脆弱性の発生率が表示されます。グラフには、各日のデータポイントが表示されます。
  - **過去 12 か月間**：現在の日付から 12 か月前までの脆弱性の発生率が表示されます。グラフには、各月のデータポイントが表示されます。
  - **カスタマイズ**：選択した期間の脆弱性の発生率が表示されます。グラフには、選択した期間に応じて、各日、各週、または各月のデータポイントが表示されます。

選択した期間の一部でデータが存在しない場合、グラフにはその期間のデータは表示されません。例えば、過去 12 か月の期間を選択しても、Contrast の使用開始が 9 か月前の場合、グラフにはその期間の最初の 3 か月のデータは表示されません。

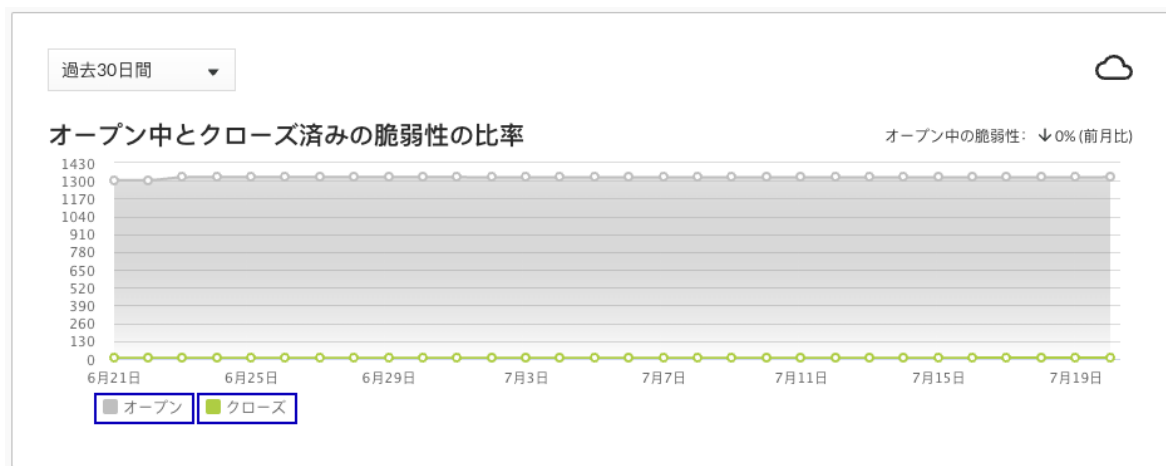
4. 選択した期間内での変化率を参照するには、グラフの上部にある値を確認してください。



5. オープン中の脆弱性のみ、またはクローズされた脆弱性のみを表示するようグラフにフィルタをかけるには、グラフの下部にあるキーを選択します。

キーを再度選択すると、選択は解除されます。

- オープン中の脆弱性のみを表示するには、**クローズキー**を選択します。
- クローズされた脆弱性のみを表示するには、**オープンキー**を選択します。



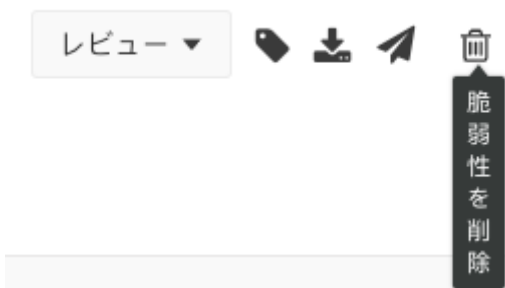
## 脆弱性の削除

アプリケーションにエージェントを組み込むと、脆弱性が自動的に検出され、脆弱性を **Contrast で確認 (587ページ)** できるようになります。これらの脆弱性は、セキュリティの問題に関する具体的な対応方針や問題の切り分け方に応じて、リスクを評価して、誤検知を排除し、修正対象の優先順位を付けることができます。

参照する必要がなくなった脆弱性は、削除することができます。

脆弱性を削除するには：

1. Contrast Web インターフェイスのナビゲーションバーで**脆弱性**を選択します。
2. 削除する脆弱性の行にカーソルを合わせて、行の右端にある**削除アイコン**を選択します。このアイコンは、脆弱性の詳細ページの右上にもあります。  
複数の脆弱性を一括で削除するには、左側の列にあるチェックマークを使用し、削除する脆弱性を選択してから、ページの下部に表示される一括アクションバーから**削除アイコン**を選択します。



3. 表示される画面で、**削除**を選択して処理を確定します。確定すると、脆弱性は削除され、Contrast で再検出されない限り一覧に表示されなくなります。

## シンクで脆弱性をグループ化

脆弱性をグループ化する場合に、同じシンクを共有する脆弱性をまとめることができます。グループ内にある脆弱性は複数のアプリケーションに影響を与えます。

脆弱性をグループ化することにより、脆弱性一覧に表示される件数が少なくなります。グループ内の個々の脆弱性のデータは、引き続き参照できます。

### 開始する前に

シンクごとのグループ化は、Contrast Assess ライセンスがあるアプリケーションの脆弱性のみ適用できます。「シンクごとにグループ化」を選択すると、**ライセンスありのみを表示**が自動的に選択されます。

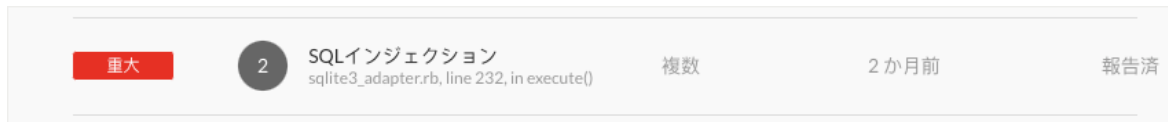
### 手順

1. Contrast Web インタフェースのナビゲーションバーで**脆弱性**を選択します。
2. 一覧の上のシンクごとに**グループ化**を選択します。

シンクごとにグループ化  ライセンスありのみを表示

一覧に使用するフィルタによっては、グループを見つけるために下にスクロールする必要がある場合があります。

グループは、次の例のような表示になります：



数字は、グループ内の脆弱性の数を示します。

グループ内の脆弱性の深刻度が異なる、対象のアプリケーションが複数ある、またはステータスが異なるものがある場合は、「深刻度」、「アプリケーション」、「ステータス」列の値が**複数**に変わります。

3. 一覧をさらに絞り込むには、**脆弱性フィルタ**を1つ以上選択します。
4. グループ内の個々の脆弱性を参照するには、そのグループをクリックします。そのグループの脆弱性のみのが一覧に表示されます。
5. グループ化を解除するには、**シンクごとにグループ化**のチェックを外します。

### 脆弱性のマージ

同じアプリケーションから同じ種類の脆弱性が検出された場合に、これらをマージして検出結果をまとめることができます。これを行うには：

1. Contrast Web インターフェイスのナビゲーションバーで**脆弱性**を選択します。
2. 左側の列にあるチェックマークを使用して、マージする2つ以上の脆弱性を選択します。
3. ページの下部に表示される一括アクションバーで、**マージアイコン**を選択します。

マージするには、脆弱性は同じ種類で、ライセンスがある同じアプリケーションのものである必要があります。

問題無し

4. 表示される画面で、このマージのまとめ先となる脆弱性を選択します。

### 脆弱性へのタグの追加

脆弱性にタグを付けることで、脆弱性を整理することができ、検索機能が向上します。タグを付けるには、以下の手順を実行します。



1. Contrast Web インターフェイスのナビゲーションバーで**脆弱性**を選択して脆弱性を一覧表示し、タグを付ける脆弱性の行にカーソルを合わせます。
2. 行の右端にある**タグアイコン**を選択します。このアイコンは、脆弱性の詳細ページの右上からもアクセスできます。



複数の脆弱性にタグを付けるには、脆弱性一覧の左側の列にあるチェックマークを使用して、タグを付ける脆弱性を選択します。ページの下部に表示される一括アクションメニューで、**タグアイコン**を選択します。

3. 表示される画面で入力を始めると、既に作成済みのタグの一覧が表示されます。既存のタグを使用する場合は、ドロップダウンから1つ以上のタグを選択します。もしくは、新規にタグを作成する場合は、フィールドに新しいタグを入力します。タグを外すには、タグの横にあるXをクリックします。変更を保存するには、**保存**を選択します。
4. タグで脆弱性を絞り込むするには、一覧の**脆弱性**列の横にあるフィルターを選択して、絞り込むタグのチェックボックスを選択します。



## 脆弱性 レビュー待ち (2) ▾ 🔍



5. タグは、脆弱性の詳細ページでも脆弱性名の横に表示されます。タグの横にある X を選択すると、タグが外れます。

## 脆弱性の追跡

バグ管理システムを Contrast とインテグレーションしている場合、複数の方法で脆弱性を追跡することができます。

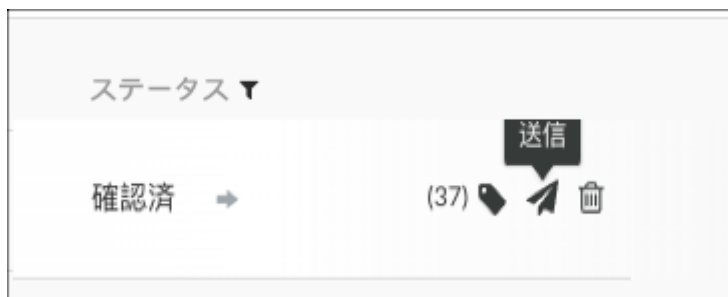
- 脆弱性の情報を組織の他のメンバーに送信する。
- 攻撃を防ぐためにタイムリーなパッチ適用を計画し、管理する。
- 脆弱性の情報をバグ管理システムに直接送信することで、ワークフローを効率化する。
- 深刻度が高または重大の脆弱性が新たにアプリケーションで検出された場合に、通知を受信する。

## 開始する前に

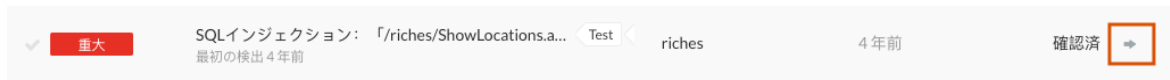
少なくとも 1 つの [バグ管理システム \(618ページ\)](#) と Contrast を連携してください。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーで **脆弱性** を選択します。
2. 1 つの脆弱性を追跡するには、追跡したい脆弱性の行の最後にカーソルを合わせます。
3. 行の右端にある **送信** アイコンを選択します  
この送信アイコンは、脆弱性の詳細ページの右上からもアクセスできます。



4. 複数の脆弱性を追跡する場合：
  - a. 追跡したい各脆弱性の横にあるチェックマークを選択します。
  - b. ページの下部に表示される一括アクションメニューで、 **送信** アイコン(📧)を選択します。
  - c. **バグ管理システムへ送信** を選択します。  
脆弱性の追跡情報をメールで送信するよう選択することもできます。
5. 「脆弱性を送信」の画面で、ドロップダウンから使用するバグ管理システムを選択し(複数のシステムと連携している場合)、関連する情報を追加して、 **送信** を選択します。  
脆弱性のステータスが自動的に **報告済** に更新され、脆弱性の行のステータスの横に矢印アイコンが表示されます。矢印アイコンの上にカーソルを合わせると、バグ管理システム名や対応するチケット番号などの詳細情報が表示されます。



6. バグ管理システムで追跡中の脆弱性を確認するには、 **脆弱性列** のフィルタを使用して、 **追跡中** のチェックボックスを選択します。



### ヒント

カスタムレポートなどのカスタマイズ処理用に、脆弱性データを CSV や XML ファイルに [エクスポート \(596ページ\)](#) できます。また、API を使用して Contrast Web インターフェイスの外部でデータを収集することもできます。

## 脆弱性イベントの解析

Contrast では、脆弱性イベントというものを使用して、アプリケーションの操作中に観察された内容を情報として提供します。これらのイベントには、脆弱性がコード内のどこで検出されたかや、コードがどのように使用されたかの情報があります。脆弱性イベントには、いくつかの種類があります。

- **ソースイベント**：ソースイベントは、脆弱性の開始点で発生します。ソースイベントのファイルと行番号を使用して、呼出しが行われた箇所を確認できます。そして、ソースのスタックトレースを使用して、注目すべきメソッドがプログラムでどのように呼び出されているかを理解できます。また、以下のようなメソッドに関する全てのデータも参照できます。
  - **オブジェクト**：このコールを呼び出しているオブジェクトのインスタンス(静的な呼出しでない場合)。
  - **リターン**：このコールから返される値(void の場合は null)。
  - **パラメータ**：このコールに渡されている値。
- **伝播イベント**：各脆弱性には、1つまたは複数の伝播イベントが含まれる場合があります。伝播イベントには、ソースイベントと同じ情報が含まれていますが、データが伝播された方法を示すタイプも含まれます。例えば、P2R の伝播イベントでは、1つ以上のパラメータからデータを受け取り ("P2R" の "P")、そのデータをメソッドの戻り値に送ります ("P2R" の "R")。
- **タグイベント**：**validated** や **html-encoded** などのタグを脆弱性に追加するイベントです。これらのタグは、誤検知を排除し、安全で信頼できる結果を得るのに役立ちます。また、他の種類のイベント

と同じコンテキスト情報もあります。タグイベントは脆弱性内で発生する場合がありますが、検出された脆弱性とは無関係です。

- **トリガーイベント**：トリガーは、脆弱性の最後のイベントです。トリガーとなった呼び出しによって、Contrast の JVM プラグインのルールエンジンの解析が実行されて脆弱性が認識され、トレースが生成されます。



### 重要

Contrast では、アプリケーションの実際の動作のみを検出します。脆弱性の問題が正当ではないと思われる場合、管理者は[適切なポリシーを設定 \(671ページ\)](#)して、この問題が再び発生しないようにする必要があります。最もよく報告される誤検知は、アプリケーションに Contrast で認識されていないカスタム制御がある場合です。

オンプレミス版(EOP)をご利用のお客様は、Contrast のポリシーで、適切なタグリストにカスタムメソッドの呼出しを登録できます。例えば、HTML エンコードを行うカスタムメソッドで、文字列を受け取り HTML エンコードされた文字列を返す場合、データに **html-encoded** のタグを追加します。

誤検知に対処するために、[セキュリティ制御 \(671ページ\)](#)や[アプリケーションの例外 \(692ページ\)](#)を使用することができます。

## 脆弱性の修正

脆弱性が検出されたら、自社のセキュリティ要件に応じてリスクを評価する必要があります。検出された脆弱性のリスクを評価して、その脆弱性を修正すると判断した場合は：

1. 脆弱性の名前を選択して詳細ページを開き、脆弱性の詳細情報を確認します。**修正方法**タブを選択して、この問題を解決するための推奨策を確認します。
2. 適切と思われる方法で、脆弱性を修正します。
3. 修正した脆弱性を確認します。確認する方法は、3つあります。
  - **リクエストを再生**：問題を修正して適切なステータスに変更したら、HTTP リクエストを再生します。**HTTP 情報**タブから HTTP リクエストを再生して、問題が修正されているか確認します。修正されていない場合、その問題は報告済みのステータスで再度表示されます。
  - **ビルド番号を確認**：アプリケーションごとに、ビルドのバージョン番号を割り当てることができます。[セッションメタデータ \(489ページ\)](#)を使用して、脆弱性のビルド番号を識別できます。  
-javaagent コマンドに以下のプロパティを追加します：

```
-Dcontrast.override.appversion
```

アプリケーションの起動時にビルド番号を指定すれば、ビルド番号をフィルターとして使用できます。備考タブを参照するか、ドロップダウンメニューでビルド番号を選択することで、そのビルドバージョンにまだ問題があるかを確認できます。

- **単体テストの時間で確認**：単体テストを実行した時間でフィルターをかけることもできます。脆弱性の一覧で日付範囲を指定して表示を絞りこみます。

## 脆弱性の検出結果のエクスポート

脆弱性の情報をエクスポートするには：

1. Contrast Web インターフェイスのナビゲーションバーで**脆弱性**を選択し、脆弱性の一覧の左側の列にあるチェックマークを使用して、エクスポートしたい脆弱性を選択します(複数選択可)。
2. ページの下部に表示される一括アクションメニューで**エクスポート**アイコンを選択して、エクスポートする形式(CSV または XML)を選択します。



3. エクスポートファイルは、デスクトップにダウンロードされます。脆弱性ごとに、以下のデータフィールドがエクスポートされます。
- Vulnerability Name (脆弱性名)
  - Vulnerability ID (脆弱性 ID)
  - Category (カテゴリー)
  - Rule Name (ルール名)
  - Severity (深刻度)
  - Status (ステータス)
  - Number of Events (イベント数)
  - First Seen (最初の検出)
  - Last Seen (最後の検出)
  - Application Name (アプリケーション名)
  - Application ID (アプリケーション ID)
  - Application Code (アプリケーションコード)
  - CWE ID (CWE 識別子)
  - Request Method (リクエストメソッド)
  - Request Port (リクエストポート)
  - Request Protocol (リクエストプロトコル)
  - Request Version (リクエストバージョン)
  - Request URI (リクエスト URI)
  - Request Qs (リクエストクエリ)
  - Request Body (リクエストボディ)
  - Instance ID(インスタンス ID)



## ヒント

アプリケーションに関して、より詳細なカスタムのソフトウェアコンポジション解析 (SCA) レポートを作成する場合、[アプリケーション API](#) を使用して Contrast の脆弱性データにアクセスできます。

また、手動で脆弱性の詳細情報を調べることもできます。

例えば、次の cURL リクエストは、脆弱性の一覧を取得し、各脆弱性が検出されたアプリケーションの一覧も表示します。カスタムレポートで使用するために、jq ツールでデータを CSV 形式にしています。

```
curl \
  -H "Authorization: $(echo -n $username:$servicekey | \
base64)" \
  -H "API-Key: $apikey" \
  https://app.contrastsecurity.com/Contrast/api/ng/$orgid/
orgtraces/filter?expand=request | \
  jq -r '.traces[] | {uuid: .uuid, \
protocol: .request.protocol} | [ .uuid, .protocol ] | @csv'
```

## 脆弱性のステータス

脆弱性のステータスは脆弱性一覧に表示され、以下の表に示すいずれかのステータスになります。脆弱性のステータスは、更新できます。

ステータス	このステータスをいつ設定するか
報告済	Contrast で脆弱性が検出された時のデフォルトのステータスです。アプリケーションでこの脆弱性が悪用される可能性があります。
確認済	ソースコードをレビューする、脆弱性を悪用してみることなどで、この脆弱性が真の判定であると確認した場合のステータスです。
疑わしい	脆弱性は、Contrast から提供された情報に基づくと真の判定のように見えますが、その有効性を判断するにはさらに調査が必要な場合のステータスです。
問題無し	脆弱性は、ソースコードを変更することなく対処した場合のステータスです。このステータスを設定するには、以下のいずれの理由を選択する必要があります。このステータスを設定した脆弱性は、再検出されても <b>報告済</b> のステータスに戻ることはありません。 <ul style="list-style-type: none"> <li>外部制御により防御された攻撃：WAF などの別のコンポーネントが環境にあり、この脆弱性の悪用は防御されません。</li> <li>誤検知：この脆弱性は誤って報告されたものです。Contrast でこれが脆弱性として判定された理由を確認するには、<a href="#">サポートにお問い合わせ</a>ください。</li> <li>内部のセキュリティ制御を通過：アプリケーション内にカスタムの修正コードがあり、この脆弱性の悪用は防御されます。</li> <li>信頼できるパワーユーザのみがアクセスできる URL：この脆弱性は、テストなどの特定の環境にのみ存在し、本番環境には存在しない可能性があります。</li> <li>上記以外：この脆弱性の対応に関してソースコードの変更が必要ではない理由が他にある場合、このオプションを選択します。上記以外というラベルを<a href="#">カスタム定義に置き換え (600ページ)</a>で、脆弱性が<b>問題無し</b>である理由として指定できます。</li> </ul>
修復済	脆弱性は、アプリケーション内のソースコードや設定ファイルなどを変更することで修正された場合のステータスです。
修正完了	この脆弱性は、ソースコードの変更もしくは <b>問題無し</b> のステータスで指定された理由によって、修正された場合のステータスです。このステータスを設定した脆弱性は、再検出されても <b>報告済</b> のステータスに戻ることはありません(このオプションは、管理者のみ使用可能です)。
修復済 - 自動検証	このステータスは、自動でのみ設定されます(ユーザが手動で設定することはできません)。脆弱性のポリシー ( <a href="#">674ページ</a> )で設定した期間内に脆弱性が報告されなければ、自動的に <b>修復済 - 自動検証</b> のステータスに変わります。

報告済、確認済、疑わしいのステータスが設定されている脆弱性は、オープン中の脆弱性となります。問題無し、修復済、修正完了、または修復済 - 自動検証のステータスの脆弱性は、クローズされたものとなります。脆弱性の一覧で**オープン中**のフィルターを選択すれば、オープン中のステータスの脆弱性のみが表示されます。全てを選択すると、オープン中とクローズされた両方のステータスの脆弱性が表示されます。



エージェントから報告された脆弱性が、それまでに Contrast で検出されたことがない場合、その脆弱性のエントリが Contrast で新規に作成されます。この脆弱性が既に存在する場合、Contrast は、既存の工

ントリ、問題数、および最後に検出されてからの日数を更新します。再検出時に全ての脆弱性は、**修復済**または**修復済 - 自動検証**に設定されていたものを除いて、以前と同じステータスで再オープンされます。修復済と修復済 - 自動検証の場合は、**報告済**として再オープンされます。

## 脆弱性のステータスの変更

1つまたは複数の脆弱性のステータスを変更するには：

1. Contrast Web インターフェイスのナビゲーションバーで**脆弱性**を選択します。
2. 1つの脆弱性ステータスを変更するには、ステータスを変更する脆弱性の行で**ステータス列**をクリックし、ステータスを選択します。脆弱性の概要ページの右上にあるステータスからも変更できます。

最後の検出 ▼	ステータス ▼
4 か月前	報告済 疑わしい
4 か月前	確認済 問題無し 修復済
4 か月前	修正完了

複数の脆弱性のステータスを一括で更新するには、左側の列にあるチェックマークを使用して、更新する脆弱性を選択します。ページの下部に表示される一括アクションメニューに、現在のステータスが表示されます。クリックすると、ステータスの一覧が表示されます。

の"	Java	報告済
ner	Java	オープン 疑わしい 確認済
wel	Net	クローズ 問題無し 修復済 修正完了

報告済 ▲ 🏷️ 📧 📄 📌 🗑️

3. 新しいステータスを選択します。ステータスの定義については、[ステータスの一覧 \(598ページ\)](#)を参照ください。



## 注記

脆弱性には、クローズする前に組織の管理者の承認を必要 (735ページ) とするよう設定することもできます。

管理者の承認が必要な脆弱性をクローズする場合は、ステータス変更の理由を入力する必要があり、組織の管理者が RulesAdmin 権限のあるユーザにレビューされるまで保留中のステータスになります。ステータス列の保留中にカーソルを合わせると、保留とされた日付を確認できます。

深堀度	脆弱性	アプリケーション	最後の検出	ステータス
重大	SQLインジェクション: 「/WebGoat/SqlInjection/atta...」 最初の検出 3 年前	Syd's webgoat-server	昨年	問題無し 保留中
重大	SQLインジェクション: 「/umbraco/backoffice/UmbracoApi...」 最初の検出 2 年前	UmbracoNewRelic	2 年前	問題無し 保留中

保留中の脆弱性のステータスは変更できる場合があります。新しいステータスへの変更に承認の必要がない場合は、脆弱性のステータスには保留中が表示されなくなります。

管理者がステータスの変更を承認または拒否すると、通知が送信されます。拒否の場合、脆弱性のステータスは以前の状態に戻りますが、管理者はその判定の理由を入力する必要があります。入力された理由は、脆弱性のアクティビティタブに表示されます。

4. (問題無しの場合)表示される画面で、ステータスを変更する理由を選択し、説明を入力します。問題無しの理由には、カスタムラベルを定義 (600ページ) することができます。

## 問題無しの脆弱性の理由をカスタム定義

セキュリティ担当が、特定の脆弱性についてコードの変更による修正は不要と判断し、脆弱性のステータスを問題無しに更新する場合があります。これにより、チームは脆弱性の修正に集中ことができ、Contrast でこれらの脆弱性が再検出されるのを防ぎます。

脆弱性のステータスに問題無しを指定する場合、理由を選択する必要があります。Contrast では、標準の理由 (598ページ) に加えて上記以外(標準の理由以外)というオプションがあります。

上記以外というラベルを組織にとってわかりやすい独自の値に変更できます。変更をするには、以下の手順を実行します。

1. 組織のポリシーの管理の画面を開きます。
2. 脆弱性の管理を選択します。
3. 上記以外の理由のカスタムラベルを設定を選択します。
4. 独自に設定したい理由を入力します。25 文字以内で入力してください。
5. 保存を選択します。



## ポリシーの管理

### ASSESS

Assessルール

セキュリティ制御

脆弱性の管理

### PROTECT

Protectルール

CVEシールド

仮想パッチ

ログエンハンサー

IP管理

### 概要

アプリケーションの例外

### 脆弱性の動作

#### 承認ワークフロー

脆弱性のクローズ時に管理者の承認が必要

全てのステータス

全ての深刻度

#### 問題無しステータスのオプション

これにより、脆弱性が「問題無し」の場合の「上記以外」の理由が置き換わります。ユーザーに表示・使用させたいラベルを設定してください。

上記以外の理由のカスタムラベルを設定

保存

これにより、脆弱性のステータスを問題無しにすると、理由の一覧には上記以外ではなくカスタム定義の理由が表示されるようになります。



### 注記

上記以外をカスタムラベルに変更する、またはカスタムラベルを上記以外に戻すと、そのラベルが付いている全ての脆弱性に更新が適用されます。

## 保留中の脆弱性ステータス変更のレビュー

組織の管理者が、特定の脆弱性について承認を必要とする (735ページ) ように設定している場合、そのステータス (598ページ) は承認されるまで変更されません。これは、手動による脆弱性ステータスの変更、双方向のバグ管理システムとの連携、および自動修復ポリシーに適用されます。

脆弱性のクローズを承認または拒否するには、組織ルールに RulesAdmin 権限があり、対象アプリケーションに対して RulesAdmin がある必要があります。

これを行うには：

1. Contrast Web インターフェイスの通知内のリンクを選択するか、ナビゲーションバーの脆弱性を選択してから、一覧の上部にあるフィルターを選択して全ての保留中のレビューを表示します。



2. 左側の列のチェックマークを使用して、1つ以上の脆弱性を選択します。ページの下部に表示される一括アクションメニューで、**レビュー**を選択します。次に**承認**または**拒否**を選択します。脆弱性の概要ページの右上にある**レビュー**を選択することもできます。
3. ステータスの変更を拒否する場合は、理由を入力する必要があります。拒否された脆弱性は、以前のステータスに戻ります。承認された脆弱性は新しいステータスに変わり、**保留中**の表示がなくなります。どちらの場合も、レビューの結果は脆弱性の**アクティビティ**タブに表示されます。

### 脆弱性の深刻度の変更

Contrast では、アプリケーションの脆弱性は 5 つの深刻度レベルに分類されます。この分類は、アプリケーションの脆弱性の可能性と影響度を基準にしており、最も深刻度の高いものから低いものまでがあります。

- 重大
- 高
- 中
- 低
- 注意

脆弱性の深刻度は、以下の手順で変更できます。

1. Contrast Web インターフェイスのナビゲーションバーで**脆弱性**を選択し、脆弱性の一覧を表示します。
2. **深刻度**の列で色付きのバッジをクリックし、リストから新たに設定する深刻度を選択します(複数の脆弱性の深刻度を一括で変更することはできません)。

## プロジェクト













### 注記

プロジェクトページに結果を表示するには、Contrast CLI 2.0 を **npm** でインストール ([573ページ](#))する必要があります。

**マニフェスト**に対して CLI を実行した後、Contrast Web インターフェイスに関連するプロジェクトが表示されて検査結果を確認できます。これにより、エージェント組み込みが不可能であったり、ソフトウェア開発ライフサイクル(SDLC)の中で対応するのでは遅すぎたりするオープンソフトウェアの脆弱性を、より早く広範囲を可視化することができます。

プロジェクト 全て (24)

ソート順  
名前

名前	前回処理日	脆弱なライブラリ
another faisa react project JavaScript	03/13/2023 04:56 午後	 (4)
dougi-0313-crazy-testing-sesh Java	03/13/2023 02:23 午後	 (1)
dougi-0313-crazy-testing-sesh-2 Java	03/13/2023 02:26 午後	 (4)
dougi-0313-crazy-testing-sesh-3 Java	03/13/2023 02:29 午後	 (2)
dougi-0313-crazy-testing-sesh-express-app1 JavaScript	03/13/2023 02:35 午後	 (3)
dougi-0313-crazy-testing-sesh-micronaut Java	03/13/2023 02:42 午後	 (1)
dougi-0313-crazy-testing-sesh-some-random-js-app JavaScript	03/13/2023 02:56 午後	 (4)
dougi-0313-crazy-testing-sesh-webgoater Java	03/13/2023 03:00 午後	 (13)
dougi-0313-spring-boot-saml Java	03/13/2023 03:10 午後	 (11)
dougi-0313-webgoat-again Java	03/13/2023 03:02 午後	 (13)

&lt; Page 1 of 3 &gt;

Results per page 10 25 50

このページには以下が表示されます。

- **名前** : CLI 用にローカルに保存されたマニフェストが含まれるプロジェクトの名前、または GitHub アカウントとリポジトリ名。
- **前回処理日** : 直近の処理日。
- **脆弱なライブラリ** : プロジェクト内のライブラリで脆弱性(CVE)が確認されたもの。脆弱なライブラリをクリックすると、ライブラリのページが表示され、詳細を確認できます。

## 関連項目

Contrast CLI のサポート対象の [言語とパッケージマネージャ \(573ページ\)](#)

## 攻撃

攻撃とは、アプリケーションやサーバを標的とした攻撃イベントのグループです。Contrast で攻撃として含める攻撃イベントには次のように複数ありますが、これらに限定されるものではありません。

- SQL インジェクション
- 信頼できないデータのデシリアライゼーション
- コマンドインジェクション
- その他、多数の一般的に広く知られている脆弱性

同一の IP アドレスから 30 分以内に複数の攻撃イベントを検出した場合、Contrast ではこれらのイベントを攻撃としてグループ化します。コードを修正した後に、同じ IP アドレスから新たなイベントが検出されると、新たな攻撃として表示されます。

ダッシュボードに表示される攻撃の日付は、ローカルのタイムゾーンではなく、Contrast タスクが実行された Contrast サーバ上の時間に基づきます。

## イベントデータの保持

Contrast では、攻撃イベントのデータは 30 日間保持されてから、削除されます。攻撃データをより長期間保持するには、以下を行います。

- [Syslog に出力 \(531ページ\)](#)
- [Generic Webhook \(639ページ\)](#)を設定  
Webhook は、指定されたイベントが発生した場合にのみ、POST リクエストでデータを受信します。Webhook はイベントを確認すると、データを収集して指定された URL に送信します。
- 攻撃の行の最後にある矢印を選択し、ドロップダウンメニューから**攻撃をエクスポート(CSV か XML 形式)**を選択します。

ソースIP	ステータス	アプリケーション	サーバ	ルール	開始	終了	イベント
<input type="checkbox"/> 127.0.0.1	ブロック済			Command Injection	4日前	4日前	1
<input type="checkbox"/> 1.2.3.5	ブロック済			Command Injection - Command Backdoors	8日前	8日	

IPを拒否リストに登録  
 攻撃を消去  
**攻撃をエクスポート (CSV)**  
**攻撃をエクスポート (XML)**

## 操作

Contrast では、次のような操作ができます。

- [攻撃情報の表示 \(604ページ\)](#) : 攻撃されたアプリケーションやサーバ、攻撃が発生したコード箇所など、攻撃の情報を確認します。
- [攻撃の管理 \(607ページ\)](#) : 攻撃や攻撃イベントに対してアクションを実行します。例えば、特定の攻撃イベントに対して Protect ルールを設定することができます。
- [攻撃の監視 \(606ページ\)](#) : 現在および過去の攻撃について概要画面でモニターします。

## 攻撃の表示

攻撃の一覧には、組織内で発生した全ての攻撃が表示されます。

ソースIP	ステータス	アプリケーション	サーバ	ルール	開始	終了	イベント
<input type="checkbox"/> 127.0.0.1	攻撃検出済	myapplication/new	myserver-local-mycompany	Command Injection Command Injection - Chained Commands Command Injection - Command Backdoors	7時間前	7時間前	3
<input type="checkbox"/> 127.0.0.1	ブロック済	myapplication/new	myserver-local-mycompany	Path Traversal Server-Side JavaScript Injection	1日前	1日前	9
<input type="checkbox"/> 127.0.0.1	ブロック済	myapplication/new	myserver-local-mycompany	Path Traversal	1日前	1日前	9
<input type="checkbox"/> 127.0.0.1	ブロック済	myapplication/new	myserver-local-mycompany	Path Traversal	1日前	1日前	12

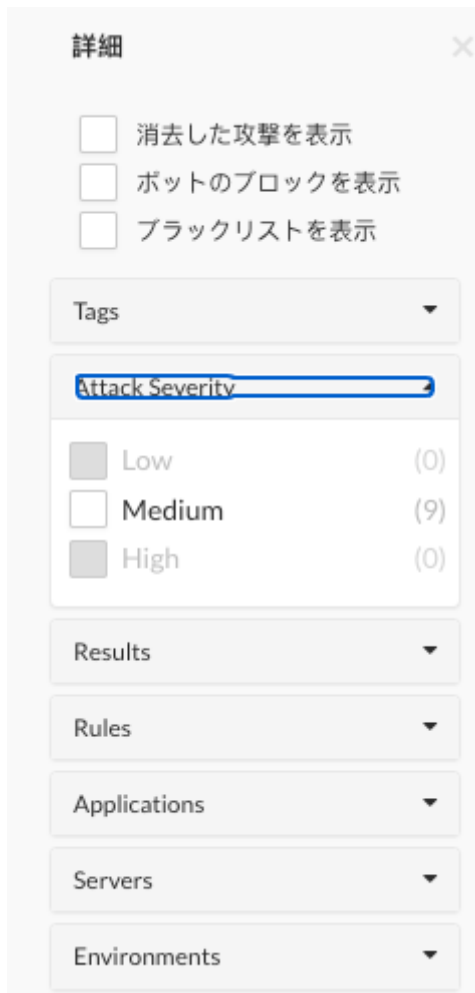
## 手順

1. Contrast Web インターフェイスのナビゲーションバーで**攻撃**を選択します。
2. 組織内で発生した全ての攻撃を表示するには、**攻撃**タブを選択します。
3. 表示を絞り込むには、次のいずれかのフィルタを選択します。
  - **全て** : 全ての攻撃を表示
  - **効果的** : ステータスが**ブロック済**、**疑わしい**、**攻撃検出済**の攻撃を表示
  - **本番** : 本番サーバで発生した攻撃を表示
  - **積極的な攻撃** : 現在進行中の攻撃を表示
  - **マニュアル** : 1秒あたりのリクエストが 20 未満の攻撃を表示。人間のマニュアル操作によって攻撃が発生している可能性あり。

- **自動化**：1秒あたりのリクエストが20を超える攻撃を表示。悪質なボットによって攻撃が発生している可能性あり。



4. 攻撃の詳細を表示するには、ソース IP 列でソース名か **IP アドレス** を選択します。
5. 攻撃内の攻撃イベントを確認するには、**概要** タブを選択します。
6. さらに表示を絞り込むには、日付範囲の横にある **詳細** をクリックするとフィルタを選択できます。



7. 攻撃イベントの詳細を表示するには、**ソース IP** を選択します。
8. 各イベントの時刻を表示するには、**攻撃期間** の下にある **タイムライン** を表示を選択します。



- 備考タブを選択すると、イベントの発生率、深刻度、攻撃者などの情報が表示されます。
- 履歴タブを選択すると、チーム内でコメントを共有したり参照できます。  
既存のコメントを参照したり、コメントを追加をクリックして新規のコメントを入力できます。

## 攻撃の詳細

Contrast で参照できる攻撃データには、以下の項目があります。

- ソース IP：攻撃が発生している IP アドレス。
- ステータス：攻撃の現在のステータス。  
攻撃のステータスは、攻撃内の攻撃イベントで最も深刻度が高いものによって決定されます。攻撃内に攻撃検出済のステータスのイベントがある場合、その攻撃のステータスは攻撃検出済になります。「攻撃検出済」のイベントがない場合、ステータスは次に高い深刻度のイベントのステータスになります。深刻度の順序は、最も高い順に次のようになります。
  - 攻撃検出済：Contrast が明らかな攻撃を検知して確定したとしても、該当するルールモードが監視に設定されている場合、そのリクエストはブロックされません。  
このステータスは、Contrast が攻撃が発生したと確定したルール(入力トレース)にのみ適用されます。Contrast で攻撃の発生が確定されるのは、ペリメータで高い信頼性のしきい値に達した攻撃、またはシンクで監視・確認された攻撃です。
  - 疑わしい：Contrast が攻撃を検知して、該当するルールによって攻撃が疑わしいと報告されたとしても、そのルールモードが監視に設定されている場合、そのリクエストはブロックされません。このステータスは、Contrast が攻撃が発生したことを確認できないルール(非入力トレース)に適用されます。
  - ブロック済：Contrast が攻撃を検知し、該当するルールモードがブロックに設定されている場合、リクエストがブロックされます。
  - ブロック済(P)：このステータスは、「ペリメータでブロック」と「ブロック」の両方のモードをサポートするルールに適用されます。  
アプリケーションでリクエストが処理される前に Contrast が攻撃を検知し、該当するルールがペリメータでブロックに設定されている場合、リクエストがブロックされます。  
ルールモードがペリメータでブロックに設定されていたとしても、ペリメータではない攻撃を Contrast が検知した場合には、リクエストはブロックされ、ステータスはブロック済になります。
  - 探査検出：Contrast が攻撃を検知しても確定せず、該当するルールモードが監視に設定されている場合、攻撃はブロックされません。確定されない攻撃とは、ペリメータで高い信頼度のしきい値まで達しなかった攻撃であり、シンクで監視はされても検知されなかった攻撃です。
- アプリケーション：攻撃が行われている間に、その IP アドレスからの攻撃イベントが確認された全てのアプリケーション。
- サーバ：攻撃が行われている間に、その IP アドレスからの攻撃イベントが確認された全てのサーバ。
- ルール：攻撃が行われている間に、その IP アドレスから発生した全ての攻撃の種類。
- 開始：攻撃の時間範囲内で、その IP アドレスから検知された最初の攻撃イベントのタイムスタンプ。
- 終了：攻撃の時間範囲内で、その IP アドレスから検知された最後の攻撃イベントのタイムスタンプ。
- イベント：攻撃を構成する攻撃イベントの数。

## 攻撃の監視

Contrast Web インターフェイスで、現在および過去の攻撃の概要、攻撃者の IP アドレス、攻撃の種類、攻撃が検出されたアプリケーションなどを確認できます。

- Contrast Web インターフェイスのナビゲーションバーで攻撃を選択します。
- 攻撃者にソース名 (698ページ)がある場合は、その上にカーソルを合わせると、関連する IP アドレスのリストが表示されます。  
攻撃者にソース名がない場合、攻撃者のアバターにクエスチョンマークが表示されます。攻撃者がアプリケーションの不正利用に成功した場合、アバターが赤色になります。



### 注記

攻撃イベントについて報告されたデータが複数のソース名と一致する場合、最後に更新された名前が適用されます。

攻撃者の情報を参照するには、IP アドレスまたはソース名をクリックします。

3. 攻撃の表示は、以下の方法でフィルターをかけることができます。
  - 日付範囲と環境をフィルターで指定する
  - 攻撃者の IP やソース名で攻撃一覧を検索する
  - 影響を受けたアプリケーション、Assess や Protect のルールで検索する
  - 探査検出も表示のチェックボックスをオンにして、「探査検出」された攻撃イベントの情報も表示する
4. 攻撃イベントタブには、検知された攻撃の種類の一覧と、種類ごとの攻撃イベントの合計数が表示されます。
5. 対象アプリケーションでは、攻撃の対象となった各アプリケーションを確認できます。

## 攻撃の管理

### 開始する前に



アプリケーションをホストしているサーバで Protect が有効になっていることを確認します。Protect が有効な場合、Contrast Web インターフェイスのナビゲーションバーに「攻撃」タブが表示されます。

### 手順

以下の手順に従って、攻撃および攻撃イベントに対して各操作を実行します。

1. 攻撃・攻撃イベントを表示する
  - a. Contrast Web インターフェイスのナビゲーションバーで**攻撃**を選択します。



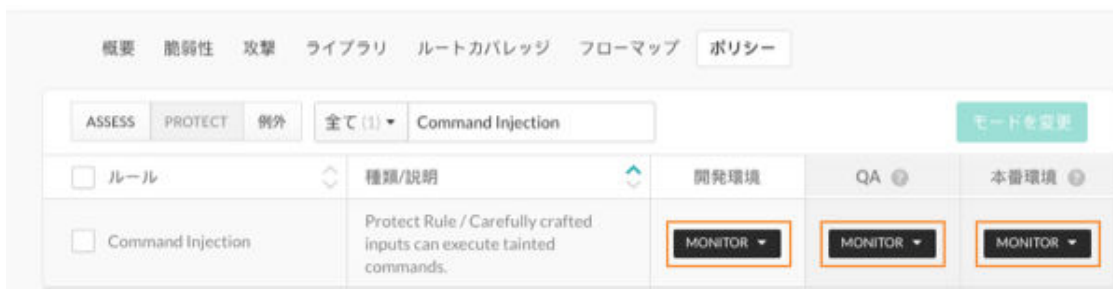
- b. **攻撃タブ**または**攻撃イベント**タブを選択します。
2. (オプション)攻撃・攻撃イベントにタグを付ける  
攻撃や攻撃イベントにタグを付けると、整理ができ検索しやすくなります。
    - a. 1つ以上の攻撃または攻撃イベントを選択します。
    - b. 一覧の上にあるタグアイコン(  )を選択します。
    - c. 表示される画面で、1つ以上のタグ名を入力します。
  3. 攻撃・攻撃イベントを消去する  
攻撃の消去を選択すると、攻撃および関連するイベントがビューから削除されます。攻撃または攻撃イベントを消去するには、以下の手順を行います。
    - a. 攻撃や攻撃イベントの一覧より、1つまたは複数の行のチェックボックスをオンにし、**攻撃を消去**または**イベントを消去**アイコン(  )をクリックします。  
または、行の最後にある矢印をクリックして、ドロップダウンメニューを表示し、**攻撃を消去**または**イベントを消去**を選択します。
    - b. **消去**をクリックします。
  4. IP アドレスをブロックする  
このオプションは、指定した IP アドレスからのアクセスをブロックするためのものです。IP アドレスをブロックすると、以後はその IP アドレスからの不要なアクセスを防ぐことができます。  
特定の攻撃や攻撃イベントの IP アドレスをブロックするための [Protect ルールを作成 \(681ページ\)](#)するには、以下の手順を行います。
    - a. 攻撃または攻撃イベントの行の右端にある矢印をクリックします。

- b. メニューから **IP を拒否リストに登録**を選択します。
  - c. 名前のフィールドに、指定した IP アドレスをブロックするためのポリシー名を入力します。
  - d. ブロックの有効期限を選択します。
  - e. **保存**をクリックします。
5. 例外を追加する(攻撃イベント)
- [アプリケーションに例外を追加 \(692ページ\)](#)することにより、特定のアプリケーションまたはその一部をセキュリティ検査の対象から外すことができます。
- これは、Java、.NET Framework、または.NET Core エージェントを使用している場合に利用できます。
- a. 攻撃イベントの一覧で、攻撃イベントの行の右端にある矢印をクリックします。
  - b. **例外を追加**を選択します。
  - c. 例外の名前を入力します。
  - d. 例外の種類を選択し、その種類に関する詳細情報を入力します。
  - e. 例外を適用するルールを選択します。
- 対象ルール**のフィールドをクリックすると、ルールが一覧表示されます。



- f. (オプション)例外と一致する全てのイベントを消去するには、チェックボックスをオンにします。
  - g. **追加**をクリックします。
6. 仮想パッチを作成する(攻撃イベント)
- [仮想パッチ \(689ページ\)](#)とは短期的なカスタムの防御ルールで、コード内で新たに検出された特定の脆弱性に対して防御するためのものです。
- a. 攻撃イベントの一覧で、攻撃イベントの行の右端にある矢印をクリックします。
  - b. **仮想パッチを作成**を選択します。
  - c. [仮想パッチを追加 \(689ページ\)](#)するための画面で、仮想パッチの詳細を入力します。
  - d. **保存**をクリックします。
7. Protect ルールを設定する(攻撃イベント)
- [Protect ルール \(680ページ\)](#)により、アプリケーション環境における特定の種類のサイバー攻撃を監視またはブロックすることができます。
- a. 攻撃イベントの一覧で、攻撃イベントの行の右端にある矢印をクリックします。
  - b. ルールを選択します。
  - c. 必要に応じて、**モードを変更**や**現在のモード**、または特定の環境を選択して、モードを変更します。



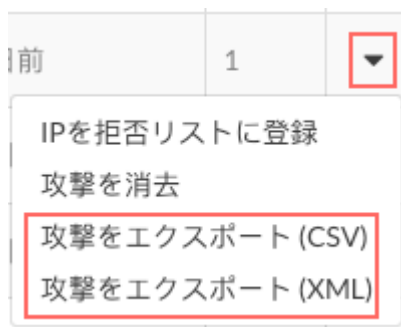


d. それぞれの環境で必要なモードを選択してください。

8. 攻撃データを保存する

Contrast では、攻撃イベントのデータは 30 日間保持されてから、削除されます。データの保存には、いくつかの方法があります。

- [Syslog \(531ページ\)](#)にデータを出力する。
- [Generic Webhook \(639ページ\)](#)を設定する。  
Generic Webhook は、POST メッセージを受信するあらゆる URL に通知できます。
- データを CSV や XML ファイルにエクスポートする。  
攻撃の一覧で、攻撃の行の右端にある矢印をクリックし**攻撃をエクスポート(CSV)**または **攻撃をエクスポート(XML)**を選択します。



## 攻撃にタグを付ける

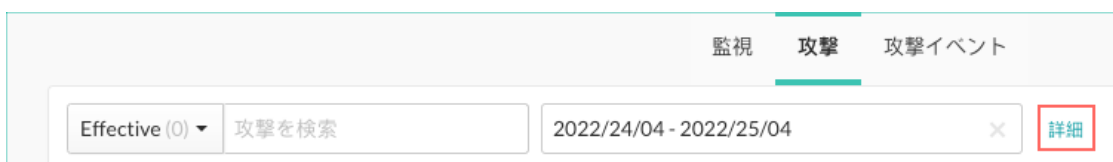
タグを使用すると、特定の攻撃や攻撃イベントを見つけやすくなります。

### 開始する前に

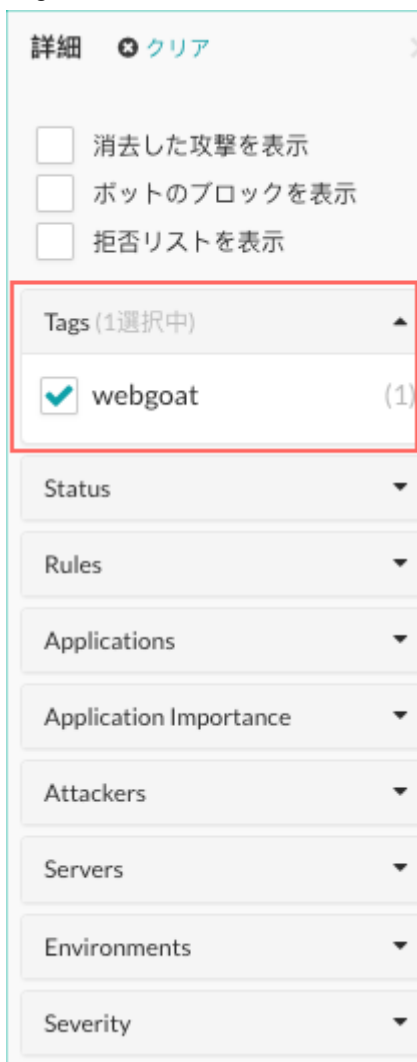
- 組織の Edit ロールまたは Admin ロールが必要です。


### 手順

1. 攻撃または攻撃イベントにタグを付けます。
  - a. Contrast Web インターフェイスのナビゲーションバーで**攻撃**を選択します。
  - b. **攻撃**または**攻撃イベント**を選択します。
  - c. 1 つ以上の攻撃または攻撃イベントの横にあるチェックボックスを選択し、タグのアイコン (📌)を選択します。
  - d. 「攻撃にタグ付け」または「攻撃イベントにタグ付け」の画面で、既存のタグを選択するか新規に作成します。
  - e. **保存**を選択します。
2. タグを使用して攻撃や攻撃イベントを検索します。
  - a. 攻撃ページまたは攻撃イベントページで、検索ボックスの横にある**詳細**を選択します。



- b. Tags セクションをクリックして展開します。



詳細  クリア

消去した攻撃を表示

ボットのブロックを表示

拒否リストを表示

Tags (1選択中) ▲

webgoat (1)

Status ▼

Rules ▼

Applications ▼

Application Importance ▼

Attackers ▼

Servers ▼

Environments ▼

Severity ▼

- c. 1つまたは複数のタグの横にあるチェックボックスを選択します。  
表示が変わり、選択したタグのある攻撃または攻撃イベントが表示されます。

## 攻撃スクリプトの実行

Contrast で攻撃データがどのようにキャプチャされるかを確認したい場合は、オープンソースの Web 脆弱性スキャナである [Nikto](#) を使って、攻撃スクリプトを実行してみましょう。



### 注記

攻撃スクリプトを実行するには、[Contrast エージェントがインストール済 \(35ページ\)](#) で、[Contrast Protect が有効な \(702ページ\)](#) アプリケーションが必要です。

攻撃スクリプトを実行するには：

1. ターミナルで `./nikto.pl` を実行し、Nikto が正しく設定されていることを確認します。正しく設定されていれば、デフォルトのヘルプメッセージが返されます。
2. Contrast で、Nikto を実行するマシンの IP アドレスがブロックリストに登録されていないことを確認します。

3. ターミナルで、`program` ディレクトリに移動します。
4. 以下を実行してスキャンを開始します。

```
./nikto.pl -useragent "MyAgent (Demo/1.0)" -h http://www.your-site.com
```



### 注記

Web アプリケーションのファイルが特定のディレクトリにある場合は、`-r` オプションを使用してディレクトリを追加します。

5. スクリプトの実行が完了すると、Contrast Web インターフェイス内や E メールで新しい攻撃に関する警告が通知されます。
6. 警告を選択するか、**攻撃** ページにアクセスし、攻撃の概要を確認します。個々の攻撃の詳細は、ソース IP を選択します。

## レポート

Contrast の全てのレポートは、ソフトウェア部品表(SBOM)以外はタイムスタンプ付きの PDF としてローカルにダウンロードできます。

以下のレポートを作成できます。

- [コンプライアンス対応レポート \(611ページ\)](#)
- [セキュリティ基準レポート \(613ページ\)](#)
- [DISA STIG Viewer チェックリスト \(613ページ\)](#)
- [ソフトウェア部品表\(SBOM\) \(614ページ\)](#)
- [脆弱性の傾向レポート \(615ページ\)](#)
- [組織の統計値 \(617ページ\)](#)

### コンプライアンス対応レポート

コンプライアンス対応レポートは、脆弱性に対応したことを証明するもので、アプリケーションの最新の情報に基づいて PDF 形式で作成されます。この PDF レポートによって、コンプライアンスや監査要件に対応できます。



### 注記

このレポートは作成してから 7 日後に期限切れになります。この期限が切れるとレポートは Contrast サーバから削除されます。

コンプライアンス対応レポートには、以下の情報が含まれます。

- レポート作成時に使用したフィルタの設定項目の一覧
- アプリケーションのセキュリティ対応状況の概要
- カスタムコードおよびオープンソースライブラリに対する脆弱性の評価。既存の組織で CVSS 3.1 が有効になっていない場合、オープンソースの脆弱性に重大(critical)の深刻度は表示されないことに注意してください。これを有効にするには、[サポートにお問い合わせ](#)ください。
- セキュリティ評価の指標としてのルートカバレッジ
- セキュリティ基準の評価(オプション)、アプリケーションでオープン中の脆弱性の詳細情報(オプション)
- 評価方法や用語を説明する付録

## 開始する前に

コンプライアンス対応レポートには、最大 1,250 件までの脆弱性、またはルートと脆弱性を合わせて最大 16,000 件まで含めることができます。

これらの制限を超えると、エラーメッセージが表示され、レポートは生成されません。このような場合は、レポートの選択項目を変更して、レポートの情報量を減らしてください。

## コンプライアンス対応レポートの作成手順

1. Contrast Web インターフェイスのナビゲーションバーでアプリケーションを選択します。
2. アプリケーションの一覧からアプリケーション名をクリックします。
3. アプリケーションページの右上にあるレポートアイコン(📄)をクリックします。
4. ドロップダウンで、コンプライアンス対応レポートを生成を選択します。
5. 「コンプライアンス対応レポート」の画面で、レポートに含める脆弱性、環境およびオプションでセキュリティ基準を選択します。

コンプライアンス対応レポート
×

コンプライアンス対応レポートは、脆弱性に対応したことを証明するもので、アプリケーションの最新の情報に基づいてPDF形式で作成されます。このPDFレポートによって、コンプライアンスや監査要件に対応できます。

**脆弱性**

全てのルール (83)

脆弱性の詳細を含める  
 ルートの観測情報を含める

**環境**

全ての環境 (3)

**セキュリティ基準**

基準を選択..

注記: セキュリティ基準を適用すると、生成されるレポートにセキュリティ基準のセクションが追加されます。

🔔 ルート合計数および脆弱性合計数: 0ルート、1の脆弱性

キャンセル
作成

デフォルトで、全ての脆弱性と全ての環境が選択されていますが、フィールドをクリックして選択項目を絞り込むことができます。生成されるレポートにセキュリティ基準のセクションを含める場合は、**セキュリティ基準**から追加したい基準を選択します。

オプションで、オープン中の脆弱性の情報と観測されたルートの情報を含めるかを選択できます。次の表は、コンプライアンスレポートの作成時に指定できるカテゴリの概要です。

カテゴリ	デフォルト	フィルターオプション
脆弱性	全て	<ul style="list-style-type: none"> <li>ステータス(報告済、疑わしい、確認済、問題無し、修復済、修正完了、修復済 - 自動検証)</li> <li>深刻度(注意、低、中、高、重大)</li> <li>Assess ルール</li> </ul>
脆弱性の詳細	含めない	脆弱性の詳細を含めるにはチェックボックスを選択
ルートの観測情報	含めない	ルートの観測情報を含めるにはチェックボックスを選択
環境	全て	<ul style="list-style-type: none"> <li>開発環境</li> <li>QA</li> <li>本番環境</li> </ul>

カテゴリ	デフォルト	フィルターオプション
セキュリティ基準	指定なし	<ul style="list-style-type: none"> <li>• DISA ASD STIG</li> <li>• IPA - 7.0</li> <li>• OWASP 2013 Top 10</li> <li>• OWASP 2017 Top 10</li> <li>• OWASP 2021 Top 10</li> <li>• OWASP Top10 API 脆弱性 2019</li> <li>• PCI DSS - 2.0</li> <li>• PCI DSS - 3.0</li> <li>• PCI DSS - 3.2.1</li> <li>• PCI DSS - 4.0</li> </ul>

6. **作成**を選択します。

Contrast でレポートが生成されると、**通知**パネルにダウンロードリンクが表示されます。リンクを選択すると、レポートをダウンロードできます。

### セキュリティ基準レポート

Contrast でアプリケーションの監視中に確認されたセキュリティの問題に関して、タイムスタンプ付きの PDF レポートを作成できます。作成できるレポートの種類は、次のとおりです。


- **DISA ASD STIG** : DISA のアプリケーションセキュリティと開発 STIG レポートは、セキュリティプログラムのポリシー要件や情報保証(IA)が可能なアプリケーションのベストプラクティスに関連したセキュリティ状況を報告します。
- **OWASP 2013 Top 10, OWASP 2017 Top 10, OWASP 2021 Top 10** : OWASP(Open Web Application Security Project)レポートは、「修正すべき」問題やトップ 10 の脆弱性を報告します。
- **OWASP トップ 10 API 脆弱性 2019** : OWASP(Open Web Application Security Project)レポートは、「修正すべき」問題やトップ 10 の脆弱性を報告します。
- **PCI DSS - 2.0, 3.0, 3.2.1** : PCI DSS (Payment Card Industry Data Security Standard)は、データ漏洩などにおけるクレジットカード会員情報の保護を目的として策定された基準です。コンプライアンスを達成するには、組織は重大な脆弱性を全て特定し修復する必要があります。

各レポートには、アプリケーションのセキュリティ状況の概要、および各脆弱性と修復ガイドの詳細が含まれます。

レポートには、アプリケーションで検出された各脆弱性に以下の情報が含まれます。

- 技術的な情報
- 問題のリスク
- 修復する方法・対応策
- 外部の参照情報
- アプリケーションにある既知の脆弱なライブラリ
- セキュリティスコアカード

セキュリティ基準レポートを作成するには :

1. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択して、レポートを作成するアプリケーションを選択します。
2. アプリケーションの一覧からアプリケーション名をクリックします。
3. アプリケーションのページの右上にある**レポートアイコン**  をクリックします。
4. ドロップダウンで、**コンプライアンス対応レポートを生成**を選択します。
5. 表示される画面で、レポートに含める**レポートの種類、脆弱性のステータス/深刻度、および脆弱性のタグ**を選択します。
6. **作成**をクリックします。  
レポートが作成されると、自動的にダウンロードされます。

### DISA STIG Viewer チェックリスト

アメリカ国防情報システム局(DISA)のセキュリティ技術導入ガイド (STIG) は、全ての政府機関のアプリケーションセキュリティの評価基準となっています。STIG は、アプリケーションのセキュリティを

保証するために、アプリケーションのライフサイクルを通じて使用されることが推奨されています。Contrast のレポート機能で、アプリケーションで検出された脆弱性に関して、STIG の要件に反する脆弱性一覧を作成することができます。



### 重要

DISA STIG レポートを生成するには、アプリケーションに Assess ライセンスが必要で

す。

DISA STIG のレポート作成を実行する前に、システム管理者(SuperAdmin 権限のあるユーザ)がオプションを有効にする必要があります。ユーザメニューで **SuperAdmin** を選択して、ナビゲーションバーで**組織**を選択します。DISA STIG のオプションを有効にする組織の名前をクリックすると、組織の編集画面が表示されます。表示される画面で、**DISA STIG チェックリストのレポート作成を有効にする**のボックスをオンにして、**保存**を選択します。

STIG Viewer で、セキュリティ基準レポート用に複数の STIG を指定してカスタムチェックリストを作成します。Contrast でアプリケーションの脆弱性に関する DISA STIG レポートを作成するには、アプリケーションのチェックリストをインポートする必要があります。

STIG Viewer チェックリストを作成するには：

1. **アプリケーション**ページにアクセスして、アプリケーション名をクリックします。
2. アプリケーションの**概要**ページで、レポートアイコンをクリックして、**STIG Viewer チェックリストを作成**を選択します。
3. 表示される画面で、STIG Viewer チェックリスト(.ckl)ファイルをインポートします。このファイルは、STIG Viewer アプリケーションからエクスポートされたチェックリストである必要があります。
4. **作成**をクリックし、更新された STIG Viewer チェックリスト(.ckl)ファイルをダウンロードします。

## SBOM(ソフトウェア部品表)

ソフトウェア部品表(SBOM)は、政府のセキュリティ規制に準拠するために必要となる場合があります。

SBOM は、Contrast Web インターフェイスで生成したり、簡単な API や Contrast コマンドラインインターフェイス(CLI)を使用して生成できます。

Contrast の SBOM は、OWASP の CycloneDX SBOM 規格および国際標準の SPDX 形式に準拠しています。Contrast の SBOM には、アプリケーションが使用するソフトウェアに関する次のような情報が含まれます。

- ライブラリ - コード本体に存在するオープンソースおよびサードパーティコンポーネント
- ソフトウェアコンポーネントに適用されているライセンス
- コード本体で使用されているソフトウェアコンポーネントのバージョン



### 注記

現在、CycloneDX v1.4 と SPDX 2.2 をサポートしています。

また、Contrast の SBOM は、米国商務省電気通信情報局(NTIA)の要件も満たしています。データ作成者、サプライヤー名、コンポーネント名、コンポーネントのバージョン、依存関係、タイムスタンプ、その他のユニーク ID(PURL やパッケージの SPDX 識別子など)が含まれます。


## 開始する前に

- Contrast Web インターフェイスからエクスポートする場合には Contrast Assess ライセンスが必要
- サポートされている言語 : Java、.NET Framework、.NET Core、Node.js、Python、Ruby、Go、PHP

## 手順

SBOM レポートを生成するには、3 つの方法があります。

### 1. Contrast インターフェイスから生成 :

- a. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択します。
- b. アプリケーションのページの右上にある**レポートアイコン**() をクリックします。
- c. ドロップダウンで、**SBOM(ソフトウェア部品表)を生成**を選択すると、レポートが作成され自動的にダウンロードされます。CycloneDX と SPDX 形式に対応しています。

### 2. API を使用してレポートを生成 :

- a. CycloneDX の場合 : **GET**<HOST>/Contrast/api/ng/<ORG\_ID>/applications/<APP\_ID>/libraries/sbom/cyclonedx リクエストをします。
- b. SPDX の場合 : **GET**<HOST>/Contrast/api/ng/<ORG\_ID>/applications/<APP\_ID>/libraries/sbom/spdx リクエストをします。

API の使用についての詳細は、[REST API](#) を参照してください。

### 3. CLI でレポートを生成 :

- `--save` オプションを使用します。`--save cyclonedx` または `--save spdx` で形式を選択できます。詳細は、[CLI コマンド \(575ページ\)](#) を参照してください。



### 注記

- 現在、CLI での .NET のサポートには制限があります。
- [静的 SCA \(535ページ\)](#) の検出結果で SBOM を作成するには、CLI を使用します。
- CLI を使用して作成された SBOM には、CLI で登録されたライブラリデータのあるアプリケーションのクラス利用状況の情報が提供されます。

## 脆弱性の傾向レポート

脆弱性の傾向レポートを使用して、アプリケーションで直面している脆弱性とそれらがどのように管理されているかを認識できます。

脆弱性の傾向レポートを表示するには :

1. ユーザメニューで、**レポート**を選択します。**表示**を選択すると、詳細がグラフで表示されます。
2. **新規**を選択すると、新規に検出された脆弱性のグラフが表示されます。**合計**を選択すると、報告されているすべての脆弱性と修復されたすべての脆弱性を比較したグラフが表示されます。  
黒色の各データポイントは、その日付で発生した脆弱性の総数を表しますが、ステータスが**疑わしい**、**確認済**、**報告済**の脆弱性の総数になります。緑色の各データポイントは、ステータスが**問題無し**、**修復済**または**修正完了**の脆弱性の総数を表します。各データポイントにカーソルを合わせるとステータスの内訳が表示されます。
3. レポートのデフォルトは、全てのアプリケーション、全てのサーバ、および全てのルールです。グラフの上の各フィールドをクリックすれば、表示する脆弱性にフィルターを適用できます。次の表は、カスタムレポート作成時に指定できるカテゴリの概要です。

フィールド	デフォルト	フィルターオプション
日付	過去 7 日間	過去 30 日間 過去 12 週間 過去 12 か月間
アプリケーション	全て	重要度(重大、高、中、低、重要でない) アプリケーションのタグ ライセンスあり(全アプリケーションの一覧)
サーバ	全て	環境(開発、QA、本番) サーバのタグ サーバ(全サーバの一覧)
ルール	全て	深刻度(重大、高、中、低、注意) 脆弱性のタグ 脆弱性ルール(全ルールの一覧)

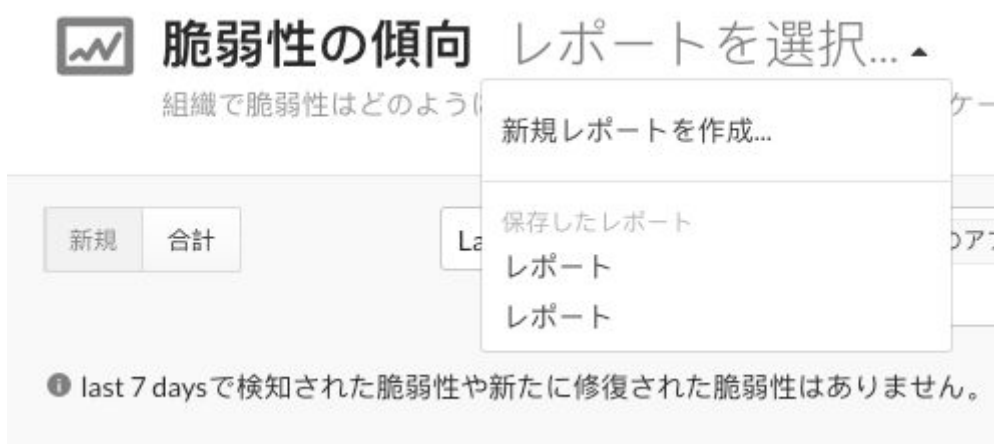
4. **表示**を選択し、右上にある**レポートを保存**アイコンを選択すると、このレポートのフィルター条件が保存されます。表示される画面でレポート名を入力したら、**保存**を選択します。レポートはユーザ別に保存されるため、各ユーザが脆弱性の傾向レポートを独自に定義して保存できます。これらのレポートはいつでも編集や削除ができます。

保存したレポートを表示中にフィルターオプションを変更すると、星印のアイコンが未保存の状態に変わり、レポート名の横に**編集済**と表示されます。同じアイコンを使用して、**既存レポートを保存**または**新規レポートとして保存**することができます。**既存レポートを保存**を選択すると、保存したレポートが現在のフィルターで更新され、**編集済**のステータスが消えます。**新規レポートとして保存**を選択すると、現在のフィルターで表示中のレポートが別の名前で新しいレポートとして保存されます。

**削除**をクリックすると現在参照中のレポートは完全に削除されます。

既存のレポートで保存していない編集内容を消去してレポートのデフォルト設定からやり直す場合は、ドロップダウンで**新規レポートを作成**を選択します。

保存したレポートが5つを超えると、**保存したレポート**のドロップダウンに**管理**のリンクが表示されます。「管理」を選択してこの画面を開きます。ここではレポート名の変更(名前をクリックして編集)やレポートの検索が行えるほか、各レポートの横にあるチェックボックスを使用(または**全て選択**のチェックボックスを使用)して削除するレポートを選択できます。



5. また、脆弱性の傾向をタイムスタンプ付きの PDF レポートとして作成し、脆弱性管理のスナップショットを取ることができます。ページの右上にある**エクスポート**アイコンを選択します。デスクトップにレポートがダウンロードされます。この PDF レポートには、カスタマイズしたビューに含まれる値の概要、傾向グラフ、各データポイントの指標と内訳の表が含まれます。



## 組織の統計値

ユーザメニューからレポートを選択すると、[脆弱性の傾向 \(615ページ\)](#)や組織レベルで次の情報を確認できます。

- **ライセンス**：ライセンスのグラフには、組織内の Access と Protect の合計ライセンス数、およびライセンスのないアプリケーション数とサーバ数が表示されます。
- **アプリケーション**：アプリケーションのグラフでは、内側の円は言語別の内訳を表します。外側の円は、ドロップダウンからテクノロジーまたはスコアを選択して、比較したい分類を選択します。
- **サーバ**：ドロップダウンからコンテナまたは環境を選択し、値の表示方法を選択します。

ドロップダウンのフィルターを使用して、比較するためのデータを簡単に選択できます。

各グラフで表示を選択すると、以下のような詳細情報が表示されます。

- **ライセンス：アクティビティ**には、過去 1 年間のライセンス消費に関するアクティビティの傾向グラフが表示されます。  
Assess または Protect の傾向グラフ線のデータポイントにカーソルを合わせると、各月で使用されたライセンス数を確認できます。点線は購入されたライセンス数を示します。  
グラフの縦線をクリックすると、各日の Protect ライセンスの使用時間が表示されます。最大使用時間は、縦線の一番上に明るい緑色が掛かって表示されます。ライセンスアクティビティデータの表示に戻るには、**ライセンスのアクティビティに戻る**を選択します。  
アクティビティグラフの下にある **Protect の使用状況を表示**すれば、Protect に関する当月のデータと使用状況の統計が表示されます。別の月のデータを表示するには、ドロップダウンを使用します。  
**使用量**には、Assess と Protect のライセンスに関する棒グラフとタイムラインがあります。棒グラフには、購入したライセンスの合計数と比較して、使用中のライセンス数が表示されます。タイムラインには、特定の日付で期限が切れるライセンスの数が表示されます。  
右側の円グラフで、Assess と Protect の割合と使用率の内訳を参照できます。組織に Protect または Assess ライセンスが無い場合は、ライセンスの無いアセットの数がグラフに表示されます。
- **アプリケーション：ステータス**には、ライセンスあり、ライセンスなし、アーカイブ済のアプリケーションごとの合計数、および組織で利用可能なライセンス数があります。  
言語別内訳の円グラフは、内側の円は言語別のアプリケーション数を表し、外側の円ではテクノロジーまたはスコア別にアプリケーション数が表示されます。詳細を参照するには、カーソルを合わせます。  
**高リスク**にはオープン中の重大な脆弱性があるアプリケーション数、**有効期限**にはライセンスの期限切れが近いアプリケーション数が表示されます。  
**防御範囲**には、本番サーバで防御範囲が不完全なアプリケーションの数が表示されます。詳細を参照するには、**内訳を表示**を選択します。  
最近(1 週間以内に)追加されたアプリケーション、オフラインのサーバにあるアプリケーションが、サイドバーにそれぞれ表示されます
- **サーバ：環境**で、デプロイ中の全てのサーバを環境ごとに確認できます。  
**コンテナ別内訳**には、指定した環境にデプロイされている各言語のサーバ数が表示されます。別の環境のデータを表示するには、ドロップダウンを使用します。  
**スナップショット**には、指定した環境のサーバ総数と比較して、Assess が有効なサーバ数、Protect が有効なサーバ数、およびオンラインのサーバ数が表示されます。  
右のサイドバーには、新規にオンボードされたサーバ、オフラインのサーバ、削除されたサーバ、およびライセンス切れが近いサーバの一覧が表示されます。

# インテグレーション

ここでは、サポート対象のインテグレーションに関して、Contrast を使用する推奨方法を記載したドキュメントを提供します。サポート対象外のその他のツールやシナリオでも、Contrast と互換性がある場合があります。サードパーティのツールやテクノロジーの具体的な情報については、その製品のドキュメントを参照してください。また、[☑ Contrast サポートポータル](#)に特定の使用例や問題に対する回避策などの記事もありますので、そちらもご覧ください。





## 注記




サポート対象のインテグレーションについては、左側のナビゲーションメニューから詳細の説明を参照できます。完全にはサポート対象ではありませんが、互換性の可能性があるインテグレーションは、外部のドキュメントにリンクされています。Contrast サポートポータルやサードパーティサイトのドキュメントへのリンクは、[☑アイコン](#)が付いています。

組織で利用可能なインテグレーションを表示するには、Contrast の組織管理者のロールが必要です。

## クラウドでの連携



お使いの PaaS でアプリケーションをデプロイしたまま、Contrast を有効にしてアプリケーションを実行できます。

	<b>AWS Elastic Beanstalk</b>	<a href="#">☑AWS Elastic Beanstalk での Java エージェント</a>
	<b>Google App Engine</b>	<a href="#">☑Google App Engine で Java エージェントを設定 Google App Engine で Java エージェントを設定</a>

	<p><b>Microsoft Azure</b></p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> .NET エージェントと Azure App Service</li> <li><input checked="" type="checkbox"/> .NET エージェントと Azure ARM</li> <li><input checked="" type="checkbox"/> .NET エージェントと Terraform</li> </ul>
	<p><b>Red Hat OpenShift</b></p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Contrast Security コンテナ</li> </ul>
	<p><b>VMware Tanzu</b> (旧 Pivotal Cloud Foundry)</p>	<ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> VMware Tanzu で Java エージェントを設定</li> <li><input checked="" type="checkbox"/> VMware Tanzu で Node.js エージェントを設定</li> </ul>









## チャットツール




アプリケーションで新たな脆弱性が発生したり、アプリケーションに対して攻撃が行われている場合に、Contrast はリアルタイムでこれらのセキュリティの問題を検知して、いち早くお知らせします。

	<p><b>Microsoft Teams</b></p>	<p><a href="#">Teams とのインテグレーション (661ページ)</a></p>
	<p><b>Slack</b></p>	<p><a href="#">Slack とのインテグレーション (663ページ)</a></p>

## コードリポジトリとの連携

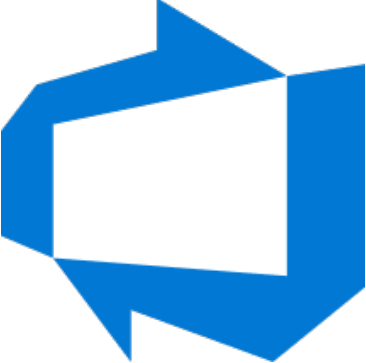




リポジトリに GitHub Actions を追加します。

	<p>Amazon Elastic Kubernetes Service のビルド・デプロイ</p>	<p> <a href="#">Contrast Amazon EKS Build Deploy</a></p>
	<p>Azure Kubernetes Service のビルド・ デプロイ</p>	<p> <a href="#">Contrast AKS Build Deploy</a></p>
	<p>Azure Spring Cloud のデプロイ</p>	<p> <a href="#">Azure Spring Cloud Deploy</a></p>
	<p>Contrast SCA による解析</p>	<p> <a href="#">Contrast SCA Action</a></p>

	<p>Contrast Scan による解析</p>	<p> Contrast Scan Analyze</p>
	<p>アプリケーションの検証</p>	<p><input checked="" type="checkbox"/> Contrast Verify</p>

## 継続的インテグレーション(CI)とビルドツール

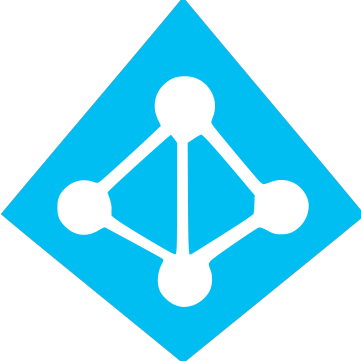



自動化されたパイプラインにアプリケーションのセキュリティゲートを追加することで、脆弱性が本番環境にデプロイされるのを防ぎます。




	<p>Azure DevOps</p>	<p>Azure Pipelines の拡張機能 (633ページ)</p> <p><input checked="" type="checkbox"/> Azure Marketplace</p>
	<p>Bamboo</p>	<p>Bamboo プラグイン (636ページ)</p> <p><input checked="" type="checkbox"/> Atlassian Marketplace</p> <p> Contrast Bamboo プラグインのソースコード</p>
	<p>CircleCI</p>	<p><input checked="" type="checkbox"/> Orb レジストリ</p> <p> Contrast Security Orb ソースコード</p>

	<p><b>GitLab</b></p>	<p><a href="#">☑GitLab パイプラインに Contrast を組み込む方法</a></p>
	<p><b>Gradle</b></p>	<p><a href="#">Gradle プラグイン (645ページ)</a></p> <p><a href="#">☑Gradle.org</a></p> <p><a href="#">🔗Contrast Gradle プラグインのソースコード</a></p> <p><a href="#">🔗サンプルプロジェクト</a></p>
	<p><b>Jenkins</b></p>	<p><a href="#">Jenkins プラグイン (647ページ)</a></p> <p><a href="#">☑Contrast Continuous Application Security</a></p> <p><a href="#">🔗Jenkins プラグインのソースコード</a></p>
	<p><b>Maven</b></p>	<p><a href="#">Maven プラグイン (60ページ)</a></p> <p><a href="#">☑Maven Central リポジトリ</a></p> <p><a href="#">🔗Maven プラグインのソースコード</a></p> <p><a href="#">🔗サンプルプロジェクト</a></p>

## エンタープライズおよび拡張


Contrast の SDK や Webhook を使用してカスタムサービスを作成したり、Webhook を使って新たな脆弱性や攻撃の検出時に通知を送信します。

	<b>Azure Active Directory</b>	<a href="#">☑ Azure Active Directory シングルサインオン(SSO)との統合</a>
	<b>Contrast CLI</b>	<a href="#">Contrast CLI (579ページ)</a> <a href="#">☑ NPM</a>
	<b>Java SDK</b>	<a href="#">☑ Contrast TeamServer Java SDK</a>
	<b>JavaScript SDK</b>	<a href="#">☑ Contrast SDK Javascript</a> <a href="#">☑ NPM</a>


	<p><b>.NET SDK</b></p>	<p><a href="#">Contrast SDK .NET</a>  <a href="#">NuGet</a></p>
	<p><b>Python SDK</b></p>	<p><a href="#">Contrast SDK Python</a></p>
	<p><b>Webhook</b></p>	<p><a href="#">Generic Webhook (639ページ)</a></p>

## IDE プラグイン

ご利用中の開発環境で、アプリケーションの脆弱性の詳細情報を表示し、修正方法や対応について知ることができます。



	<p><b>Eclipse</b></p>	<p><a href="#">Eclipse Marketplace</a></p>
---	-----------------------	--



	<p><b>IntelliJ</b></p>	<p><a href="#">Contrast IntelliJ プラグイン (646ページ)</a></p> <p><a href="#">☑IntelliJ Marketplace</a></p>
	<p><b>Visual Studio</b></p>	<p><a href="#">Visual Studio プラグイン (664ページ)</a></p> <p><a href="#">☑Visual Studio Marketplace</a></p>
	<p><b>Visual Studio Code</b></p>	<p><a href="#">Visual Studio Code プラグイン (665ページ)</a></p> <p><a href="#">☑Visual Studio Code Marketplace</a></p>
	<p><b>Visual Studio for Mac</b></p>	<p><a href="#">Visual Studio for Mac プラグイン (666ページ)</a></p> <p><a href="#">📁拡張ファイル</a></p>



## インシデント管理システム

アプリケーションへの攻撃に対して、オンコール担当者が必要な対応を取ることができるようになります。

	<p><b>PagerDuty</b></p>	<p>PagerDuty とのインテグレーション (662ページ)</p>
	<p><b>Splunk On-Call</b> (旧 VictorOps)</p>	<p>VictorOps とのインテグレーション (664ページ)</p>



## SIEM ツール

Contrast エージェントによるアクティビティから、アプリケーションセキュリティの脅威に関して運用面での新たな情報を SIEM で直接得ることができます。

	<p><b>Azure Sentinel</b></p>	<p><input checked="" type="checkbox"/> Contrast Protect Azure Sentinel Solution</p> <p><input checked="" type="checkbox"/> Azure Sentinel</p>
	<p><b>Datadog</b></p>	<p><input checked="" type="checkbox"/> ソースコード</p>

	<p><b>Splunk</b></p>	<p><a href="#">☑ Splunk と Contrast を連携する方法</a></p>
	<p><b>Sumo Logic</b></p>	<p><a href="#">☑ ソースコード</a></p>

## 作業管理プラットフォーム

	<p><b>Azure Boards</b></p>	<p><a href="#">Azure Boards とのインテグレーション (628ページ)</a></p>
	<p><b>Bugzilla</b></p>	<p><a href="#">Bugzilla とのインテグレーション (637ページ)</a></p>

	<p><b>GitHub</b></p>	<p><a href="#">GitHub とのインテグレーション (644ページ)</a></p>
	<p><b>Jira</b></p>	<p><a href="#">Jira とのインテグレーション (656ページ)</a></p>
	<p><b>Kenna Security</b></p>	<ul style="list-style-type: none"> <li><a href="#">Kenna ツールキット</a></li> <li><a href="#">Contrast タスクの実行方法</a></li> </ul>
	<p><b>Rally</b> (旧 CA Agile Central)</p>	<p><a href="#">Agile Central とのインテグレーション (631ページ)</a></p>
	<p><b>Solutions Business Manager</b> (旧 Serena)</p>	<p><a href="#">Serena Business Manager とのインテグレーション (663ページ)</a></p>
	<p><b>ThreadFix</b></p>	<ul style="list-style-type: none"> <li><a href="#">Contrast Remote Provider (ThreadFix)</a></li> <li><a href="#">Contrast Remote Provider</a></li> </ul>

## Azure Boards とのインテグレーション

Contrast と Azure Boards を連携し、バグ管理のためのチケットの自動作成、コメントの同期、アプリケーションのプッシュ通知などを可能にします。

インテグレーションには、以下が必要になります。

- Azure Boards または TFS のアカウント認証情報：ユーザ名と個人用アクセストークン(PAT)
- PAT のスコープにワークアイテム(Work Items)の読み取りと書き込み(Read & write)を含める
- Azure Boards または TFS インスタンスがあり、HTTP で Contrast にアクセスできる
- Contrast エージェントが組み込まれたアプリケーションがあり、Azure Boards プロジェクトに関連付けられている
- 詳細については、Microsoft の [Azure Boards ドキュメント](#) を参照

## 関連項目

- [Azure Boards への接続 \(629ページ\)](#)
- [チケットの自動作成 \(629ページ\)](#)
- [双方向インテグレーション \(630ページ\)](#)
- [個人用アクセストークンの設定 \(631ページ\)](#)

## Azure Boards への接続

### 手順

1. Contrast Web インターフェイスで、**組織の設定 > インテグレーション**を選択します。
2. Azure Boards の行で、**接続**を選択します。
3. 以下の値を入力します。
  - **名前**：Contrast の検出結果を Azure Boards のバグ管理システムに送信するときに表示されるラベル。
  - **URL**：Azure Boards または TFS の URL。Contrast からこの URL にアクセスできる必要があります。
  - **バージョン**：Contrast は API v2 を使用し、Azure DevOps Services、TFS 2015 および TFS 2017 をサポートします。
  - **パーソナルアクセストークン(PAT)**：パスワードの代わりにホストを認証するために使用します。
4. **URL をテストする**を選択します。Azure Boards または TFS プロジェクトの数によっては、数分かかる場合があります。接続テストは、入力した Azure Boards または TFS インスタンスに Contrast が接続できるか、またユーザの PAT でログインが許可されるかを確認します。
5. Azure Boards と接続したら、表示される設定画面で、バグ管理システムとの連携を有効にする **アプリケーション**を選択します。
6. **プロジェクト**と、デフォルトの**担当先**およびデフォルトの**ワークアイテム**を選択します。
7. **チーム**を選択し、そのチームにある**エリア**を選択します。これにより、特定のバックログにチケットが送信されます。
8. 脆弱性の深刻度に対する**デフォルト Priority**を設定します。この設定により、選択されたアプリケーションの脆弱性を修正するためのチケットに、深刻度に基づいて優先順位が付けられます。ここで、Contrast は API を呼び出し、Azure Boards または TFS のチケットのステータスの一覧が返ります。
9. Contrast で脆弱性のステータスを自動的に更新するための**双方向のインテグレーション (630ページ)**や Azure Boards で**チケットを自動作成 (629ページ)**するように設定することもできます。

## 関連項目

- [チケットの自動作成 \(629ページ\)](#)
- [双方向インテグレーション \(630ページ\)](#)
- [個人用アクセストークンの設定 \(631ページ\)](#)

## チケットの自動作成

Contrast で脆弱性が新たに検出されるたびに、**チケットを自動的に作成**できます。手順は、以下のとおりです。

## 手順

1. [Azure Boards の接続の設定画面 \(628ページ\)](#)で、**新たに検知された脆弱性に対してチケットを自動的に作成する**のチェックボックスをオンにします。ルールと深刻度の複数選択フィールドが表示されます。
2. Azure Boards または TFS で新しいチケット作成のトリガーとなるルールや深刻度を選択します。デフォルトでは、**重大と高**が選択されます。



### 注記

この設定は、この選択を行った後に新規に検出された脆弱性にのみ有効です。

## 関連項目

- [Azure Boards への接続 \(629ページ\)](#)
- [双方向インテグレーション \(630ページ\)](#)
- [個人用アクセストークンの設定 \(631ページ\)](#)

## 双方向インテグレーション

Azure Boards と双方向のインテグレーションが可能です。双方向のインテグレーションにより、Azure Boards や TFS で脆弱性に関連する課題をクローズや再オープンした際に、Contrast の脆弱性のステータスが自動的に更新されます。

## 手順

1. [Azure Boards の接続の設定画面 \(628ページ\)](#)で、**双方向のインテグレーションを有効にする**を選択します。脆弱性ステータスのフィールドが表示されます。
2. ドロップダウンメニューを選択して、Azure Boards または TFS チケットの各ステータスに対応する Contrast の脆弱性ステータスを設定します。
3. **保存**を選択します。Azure Boards/TFS チケットの脆弱性ステータスが Contrast によって更新されるようになります。
4. Azure Boards や TFS でチケットのステータスが更新されると、Contrast ではその脆弱性の**アクティビティ**タブにコメントが自動的に作成されます。各コメントには、バグ管理システム名とチケットへのリンクが含まれます。



### 注記

Azure Boards または TFS のチケットのステータスとして、**問題無し**の脆弱性ステータスを選択する場合、Contrast で**理由**も選択する必要があります。デフォルトの値は、**上記以外**です。



### 注意

複数の脆弱性を 1 つの問題として、Azure Boards または TFS に送信した場合、チケットのステータスは、そのチケットに関連付けられている全ての脆弱性に適用されます。逆に、複数のチケットを 1 つの脆弱性にリンクした場合は、脆弱性を更新する前に、関連付けられているチケットを全て更新してください。例えば、チケットのステータスを **New** から **Active** に変更した場合、その脆弱性に関連付けられた全てのチケットのステータスが **Active** である場合にのみ、Contrast で脆弱性のステータスが更新されます。

## 関連項目

- [個人用アクセストークンの設定 \(631ページ\)](#)
- [Azure Boards への接続 \(629ページ\)](#)
- [チケットの自動作成 \(629ページ\)](#)

## Azure Boards の個人用アクセストークンの設定

個人用アクセストークン(PAT)は、Contrast が Azure Boards にアクセスするために使用します。PAT には、フルアクセスまたはカスタムアクセスを設定できます。

### 手順

1. Azure で **User Settings** にアクセスし、「Profile」を選択します。
2. 「Security」で、**Personal access tokens** を選択します。既存の個人用アクセストークンがある場合は、表示されます。
3. **New Token** をクリックします。 **Create a new personal access token** の画面が表示されます。
4. **Create a new personal access token** の画面で、新しい PAT の必須フィールドを入力して、Scopes(アクセス範囲)を選択します。



### 注記

Contrast で使用するには、**Work Items** の **Read, write, & manage** を必ず選択してください。

**Work Items**  
Work items, queries, backlogs, plans, and metadata

Read     Read & write     Read, write, & manage

5. **Create** をクリックして完了すると、新しい個人用アクセストークンが保存されます。

## 関連項目

- [Azure Boards への接続 \(629ページ\)](#)
- [チケットの自動作成 \(629ページ\)](#)
- [双方向インテグレーション \(630ページ\)](#)

## Agile Central とのインテグレーション

Contrast と Agile Central を連携することで、アプリケーションの脆弱性を自動的に追跡できます。

設定を開始する前に、以下が必要です。

- Agile Central アカウントの URL
- 対象プロジェクトで課題を作成するための権限
- HTTP 経由で Contrast にアクセス可能な Agile Central の実行インスタンス
- Contrast に登録されたアプリケーションと関連付けるプロジェクト

Agile Central と接続するには :

1. ユーザメニューで、**組織の設定 > インテグレーション**にアクセスします。
2. Agile Central の行で、**接続**を選択します。
3. **Agile Central** への接続の設定画面で、バグ管理システムのエントリ名、**URL** および **API キー**を各フィールドに入力します。Agile Central の URL には、設定する Contrast インスタンスからアクセスできる必要があります。



#### 注記

Agile Central の API キーを取得するには、Agile Central Application Manager にログインして、**API Keys** を選択します。Contrast では、設定したユーザ名、パスワード、Agile Central の URL は認証情報セットとして保存されます。

4. フィールドに入力したら、**接続をテスト**を選択します。接続テストでは、Contrast が Agile Central のインスタンスに到達でき、指定したユーザがログインできることを確認します。
5. 接続したら、このインテグレーションを有効にする**アプリケーション**を選択します。
6. ドロップダウンから、**プロジェクト名とオーナー**を選択します。
7. **デフォルトの優先順位**のセクションでは、ドロップダウンを使用して、各脆弱性の深刻度に対する優先度レベルを選択します。
8. チケットを作成する**環境**を選択します。
9. **デフォルトの状態**を選択します。
10. チケット送信者の名前を以下により**サブミット**で指定します。



#### 注記

これらの設定フィールドはいずれも必須ではありませんが、空白のままにしたフィールドについては、Agile Central で独自のデフォルト値を使用してチケットが生成される場合があります。

11. Contrast で接続を設定した後に別のインテグレーションを追加するには、Agile Central の行で**設定を追加**を選択します。
12. 新たに検出される脆弱性のチケットを自動的に作成するには、設定画面で自動作成のオプションをチェックします。表示される複数選択フィールドで、チケットを生成する脆弱性の**ルール**および**深刻度**を選択します。



#### 注記

このオプションの選択は、過去にさかのぼってチケットを生成するものではありません。

## Agile Central の認証情報の管理

Contrast には、Agile Central の設定で入力された最新の認証情報が保存されているので、次の新しい接続を簡単に設定できます。最初の設定で入力した API キーと URL の値が、それ以降のインテグレーション設定でデフォルトの認証情報となります。

以降の設定で、このデフォルトの認証情報がフィールドにあらかじめ入力されますが、必要に応じて値を変更できます。保存されている認証情報を管理して、影響を受ける全ての設定を同時に更新することもできます。



デフォルトの認証情報とは異なる認証情報で、設定を作成または編集するには：

1. **認証情報を管理**のリンクを選択します。
2. **URL** フィールドでドロップダウンを使用して保存済みの認証情報セットを選択する、または **URL**、**ユーザ名**、**パスワード**フィールドの値を手動で更新します。
3. フィールドを更新したら、**接続をテスト**を選択します。
4. **保存**を選択します。新しい認証情報を使用する場合、指定した名前で既存の認証情報セットを上書きするか、別の名前で新しい値を新しい認証情報セットとして保存するかを選択する必要があります。
5. 保存済みの既存の認証情報セットを修正する場合は、必要に応じて**名前を変更**を選択します。**接続をテスト**を選択して、**保存**します。



#### 注記

認証情報セットを更新すると、そのセットを使用している全ての設定に影響します。

## Azure Pipelines の拡張機能

Azure Pipelines の拡張機能を使用して、アプリケーションのデプロイのワークフローに Contrast を連携します。本項では、Contrast と連携するための拡張機能を設定する方法と手順を説明します。

拡張機能を設定する前に、Microsoft の拡張機能をインストールする権限があることを確認してください。アクセス権限をお持ちでない場合は、プロジェクトの**拡張機能を要求**できます。

### Azure Pipelines の拡張機能のインストールと設定

Azure Pipelines の拡張機能をインストールして設定するには：

1. **Microsoft の手順**に従って、**Contrast Integration** という拡張機能を検索して、インストールします。  
**Microsoft の手順**に従って、**Contrast Integration** という拡張機能を検索して、インストールします。
2. サイドバーの下にある **Project Settings**(プロジェクトの設定)を選択します。この設定を変更するには、プロジェクト管理グループに属しているか、設定を変更するのに十分な権限を持っている必要があります。
3. プロジェクトの設定ページの **Pipelines**(パイプライン)セクションで、**Service connections**(サービス接続)を選択します。
4. **New Service connection**(新しいサービス接続)を選択し、**Contrast Server Connection** を選択します。
5. 全てのフィールドに、**個人のキー (478ページ)**から必要なデータを入力します。



#### 注記

Contrast URL には、末尾に **/Contrast** を含めず、ホストのみを指定してください。

### Azure Pipelines の拡張機能でタスクを設定

Azure Pipelines の拡張機能で、リリースパイプラインまたはビルドパイプラインにタスクを設定するには：

1. タスクを追加するパイプラインを選択して、**Edit**(編集)を選択します。

2. リリースパイプラインの場合は、タスクを追加するステージを選択します。
3. タスクを追加するために、省略符号(...)メニューをクリックして、**Add an agentless job**(エージェントレスジョブの追加)を選択します。
4. エージェントレスジョブの横にある[+]ボタンをクリックして、**Contrast Assess - Application Vulnerability Detection** タスクを追加します。
5. 接続先とアプリケーションを選択するために、**Contrast Service Connection** メニューで、接続したいサービス接続を選択します。**Manage**(管理)を選択して、**Project Settings**(プロジェクトの設定)ページの **Service connections**(サービス接続)の設定画面にアクセスすることもできます。
6. **Application** メニューで、アプリケーションを1つ選択します。
7. タスクの設定として、**Allowed Status**(許可するステータス)フィールドと **Build Number**(ビルド番号)フィールドを使用して、Contrast からの結果にフィルターをかけます。結果にフィルターをかけたくない場合は、空欄のままにします。これらのフィールドで設定した値が、以降のフィールドで設定する条件に対して検証されます。
8. 深刻度の設定に進み、深刻度ごとに許容する脆弱性の上限数を設定する必要があります。選択したアプリケーションに、その深刻度で許容する数を超える脆弱性がある場合、タスクは失敗になります。

ビルドパイプラインの場合のみ：タスクが失敗した場合にジョブが実行されないようにするには、Contrast のタスクを含むエージェントレスジョブへの依存をジョブに設定する必要があります。

1. タスク失敗時に実行したくないジョブを選択します。
2. **Dependencies**(依存関係)セクションで、**Agentless job**(エージェントレスジョブ)を追加します。



#### 注記

このタスクは、エージェントレスジョブにのみ使用できます。

## Azure Pipelines のパイプラインにリリースゲートを追加

リリースゲートは、特定のアプリケーションの脆弱性が一定のしきい値を超えた場合に、デプロイを止める保護機能です。Azure Pipelines の拡張機能を使用して、リリースゲートを追加するには：

1. ゲートを追加するリリースパイプラインを検索して、**Edit**(編集)を選択します。
2. ゲートを設定するステージとデプロイの条件を選択します。ゲートは、デプロイ前条件またはデプロイ後条件のいずれかになります。同じ条件に複数のゲートを追加することができます。
3. ステージのデプロイ条件アイコンを選択し、トグルボタンを選択して **Gates**(ゲート)を有効にします。
4. **Add**(追加)をクリックし、**Contrast Assess - Application Vulnerability Detection** を選択します。
5. Contrast Service Connection で、サービス接続を選択します。サービス接続を新規に作成するには、サービス接続のドロップダウンメニューの横にある **New**(新規)を選択して、全てのフィールドに入力し、**OK** を選択します。  
**Refresh list**(リストをリフレッシュ)を選択して、新規に作成した接続を選択します。
6. Application フィールドをクリックするか、**Refresh Application**(アプリケーションをリフレッシュ)を選択すると、アプリケーションの一覧が表示されます。リリースパイプラインで検証するアプリケーションを選択します。
7. 必要に応じて、ゲートでの検証データを取得する際に、フィルターをかける脆弱性のステータスやビルド番号を選択できます。
8. 深刻度ごとに許容される脆弱性の上限数を設定します。パイプラインがこのゲート達して検証が失敗した場合、パイプラインが有効になるか、検証がタイムアウトするまでサンプリングが要求され続けます。  
ステージのゲートの定義方法やゲートの設定方法については、Microsoft ドキュメントに詳しい説明があります。

ステージのゲートの定義方法やゲートの設定方法については、Microsoft ドキュメントに詳しい説明があります。



### ヒント

**Evaluation**(検証)オプションをカスタマイズして、ゲートの再検証までの時間を設定できます。例えば、この値を 24 時間に設定することで、ゲートが毎日検証されるようになります。これにより、パイプラインの実行を最初からやり直すことなく(または、手動での承認を構成している場合は承認が要求されずに)、脆弱性を修正して、必要なゲート条件を通過できます。

## Azure Service Fabric で .NET Framework または .NET Core エージェントを使用する

コンテナイメージを使用する場合は、[コンテナにインストール \(145ページ\)](#)する手順に従ってください。そうでない場合は、Azure Service Fabric サービスに Contrast .NET Framework または .NET Core エージェントを追加します。



### ヒント

スタンドアロンの実行サービスの場合、ServiceManifest.xml ファイルは最上位の Azure Service Fabric プロジェクト(例、sfproj ファイル)にあります。

- 適切な NuGet パッケージをサービスのメインプロジェクトにインストールします。
  - .NET Framework の場合**： Contrast.NET.Azure.AppService をインストールします。contrastsecurity フォルダにあるすべてのファイルは、プロパティがに設定されている必要があります。
  - .NET Core の場合**： Contrast.SensorsNetCore をインストールします。contrast フォルダにあるすべてのファイルは、プロパティがに設定されている必要があります。
- ServiceManifest.xml の ServiceManifest/CodePackage/EntryPoint/ExeHost/WorkingDirectory を CodePackage に設定します。

```
<CodePackage Name="Code" Version="1.0.0">
  <EntryPoint>
    <ExeHost>
      <Program>DemoNetFxStatelessService.exe</Program>
      <WorkingFolder>CodePackage</WorkingFolder>
    </ExeHost>
  </EntryPoint>
</CodePackage>
```

- ServiceManifest.xml で環境変数を定義して、プロファイラを指定します。
  - .NET Framework の場合**：

```
<CodePackage>
  <EnvironmentVariables>
    <EnvironmentVariable Name="COR_ENABLE_PROFILING" \
Value="1" />
    <EnvironmentVariable Name="COR_PROFILER" \
Value="{EFEB8EE0-6D39-4347-A5FE-4D0C88BC5BC1}" />
    <EnvironmentVariable Name="COR_PROFILER_PATH_32" \
Value=".\\contrastsecurity\\runtimes\\win-
```

```
x86\native\ContrastProfiler.dll" />
    <EnvironmentVariable Name="COR_PROFILER_PATH_64" \
Value=". \contrastsecurity\runtimes\win-
x64\native\ContrastProfiler.dll" />
    <EnvironmentVariable Name="CONTRAST_CONFIG_PATH" \
Value="contrast_security.yaml" />
```

- **.NET Core の場合 :**

```
<CodePackage>
  <EnvironmentVariables>
    <EnvironmentVariable Name="CORECLR_ENABLE_PROFILING" \
Value="1" />
    <EnvironmentVariable Name="CORECLR_PROFILER" \
Value="{8B2CE134-0948-48CA-A4B2-80DDAD9F5791}" />
    <EnvironmentVariable Name="CORECLR_PROFILER_PATH_32" \
Value="contrast\runtimes\win-x86\native\ContrastProfiler.dll" />
    <EnvironmentVariable Name="CORECLR_PROFILER_PATH_64" \
Value="contrast\runtimes\win-x64\native\ContrastProfiler.dll" />
    <EnvironmentVariable Name="CONTRAST_CONFIG_PATH" \
Value="contrast_security.yaml" />
```

4. 次のいずれかで、エージェントを設定します。

- **YAML 設定ファイル :** このファイルをサービスのメインプロジェクトに追加します。ファイルのプロパティが、に設定されていることを確認してください。以下のように、ファイルの場所を指定する環境変数を ServiceManifest.xml に追加します。

```
<CodePackage>
  <EnvironmentVariables>
    <EnvironmentVariable Name="CONTRAST_CONFIG_PATH" \
Value="contrast_security.yaml" />
```

- **環境変数 :** 以下のように、環境変数を ServiceManifest.xml に追加します。

```
<CodePackage>
  <EnvironmentVariables>
    <EnvironmentVariable Name="CONTRAST__API__URL" \
Value="https://teamserver-staging.contsec.com" />
    <EnvironmentVariable Name="CONTRAST__API__API_KEY" \
Value="aBcD0123" />
    <EnvironmentVariable Name="CONTRAST__API__SERVICE_KEY" \
Value="ABCD0123" />
    <EnvironmentVariable Name="CONTRAST__API__USER_NAME" \
Value="agent_123@Team" />
```

5. 通常どおり、Azure Service Fabric アプリケーションをデプロイします。

## Contrast Bamboo プラグイン

このプラグインは、Bamboo に機能を追加して、Contrast に接続するためのプロファイルを設定し、脆弱性のしきい値に対してビルドを検証できるようにします。

### インストールと設定

Bamboo プラグインをインストールして設定するには :

1. Contrast Bamboo プラグイン( *contrast-bamboo-plugin-#.##.jar*)を [Bamboo Marketplace](#)(マーケットプレイス)からダウンロードします。
2. Bamboo インスタンスにログインし、左上の設定メニューから、**Add-Ons** を選択します。
3. **Upload add-on** を選択します。
4. ファイルのアップロードを促すメッセージが表示されたら、*contrast-bamboo-plugin-#.##.SNAPSHOT.jar* を選択します。

5. **User-installed add-ons** にプラグインが表示されていることを確認します。
6. プラグインがインストールされたら、Contrast のプロファイルを設定します。サイドナビゲーションバーにある **Add-Ons** で、**Contrast Profiles** を選択します。
7. **Profile Configuration** ページで **New Profile** を選択して、フォームに入力します。



### 注記

SaaS 版をご利用のお客様の場合は、Contrast URL を入力する必要はありません。

8. **Test Connection** を選択して、設定が正しいことを確認します。接続できると、成功(Success!)のメッセージが表示されます。

## 脆弱性のしきい値の設定

Bamboo プラグインは、ビルドジョブに対して、設定した脆弱性の条件をチェックするためのタスクとして追加できます。これにより、アプリケーションに存在する脆弱性の数や種類を Contrast で確認できます。

ビルドジョブにタスクを追加するには：

1. **Create a New Build Plan** を選択します(既存のプランを使用することもできます)。
2. プロジェクト(Project)、プラン名(Plan name)、リポジトリホスト(Repository host)を入力または選択します。プロジェクトキーとプランキーは自動生成されます。
3. プランを作成したら、ビルドプロセスにタスクを追加するために **Add Task**(タスクの追加)を選択します。
4. 表示される画面で、**Contrast CI for Assess** というタスクを検索して選択します。  
**Contrast CI for Assess configuration** 画面では、Contrast Profile(プロファイル)だけでなく、Server Name(サーバ名)、Application Name(アプリケーション名)、**Passive**(パッシブ)パラメータを指定します。サーバ名は必須ではありませんが、指定する場合は Contrast 内のサーバと一致している必要があります。アプリケーション名は指定されたサーバ上にある必要があります。  
**Passive** パラメータを選択した場合、プラグインは(ビルド固有の脆弱性だけでなく)アプリケーションに対して全ての脆弱性のクエリを実行します。これを行うと、Bamboo ビルドでビルド後の Contrast の処理を行う前に、アプリケーションの統合テストを実行する必要がなくなります。
5. 次に、ビルドを失敗させるための条件を定義します。
  - **Threshold Count**(しきい値の数)：ビルドを失敗させるのに必要な検出数の最小値。
  - **Threshold Severity**(しきい値の深刻度)：検出結果をしきい値の数として数えるための最小レベルの深刻度。
  - **Threshold Vulnerability Type**(しきい値の脆弱性の種類)：検出結果をしきい値の数として数える対象とする脆弱性の種類。



### 注記

**Any** オプションを使用すると、全ての深刻度や全ての脆弱性の種類がしきい値の数にカウントされます。

6. タスクごとに複数の条件を設定するには、**Add New Threshold Condition**(新しいしきい値条件の追加)を選択します。
7. **Save**(保存)を選択します。
8. 左下のチェックボックスを選択して、ビルドプランを有効にします。

## Bugzilla とのインテグレーション

Bugzilla とインテグレーションするには：

1. ユーザメニューで、**組織の設定 > インテグレーション**にアクセスします。
2. Bugzilla の行で、**接続**を選択します。

- 表示される画面で、Bugzilla のプロパティフィールドに入力します。

フィールド	説明
名前	バグ管理システムのエントリ名、Contrast の検出結果を送信するときに表示されるラベル
ユーザ名	Bugzilla に接続するアカウントのユーザ名
パスワード	指定したユーザ名のパスワード
ホスト	Bugzilla インスタンスの URL
アプリケーション	Bugzilla のプロダクト(product)/コンポーネント(component)にマップするアプリケーション
プロダクト	アプリケーションにマップする Bugzilla プロダクト(product)
コンポーネント	アプリケーションにマップする Bugzilla コンポーネント(component)
バージョン	アプリケーションにマップする Bugzilla バージョン番号(version)
優先度	Bugzilla に検出結果をエクスポートする際に使用する優先度

- 接続をテスト**を選択して、接続を確認します。接続テストによって、Contrast が Bugzilla インスタンスとの通信と認証を行い、指定した**プロダクト**(product)、**コンポーネント**(component)、**バージョン**(version)の存在を確認します。

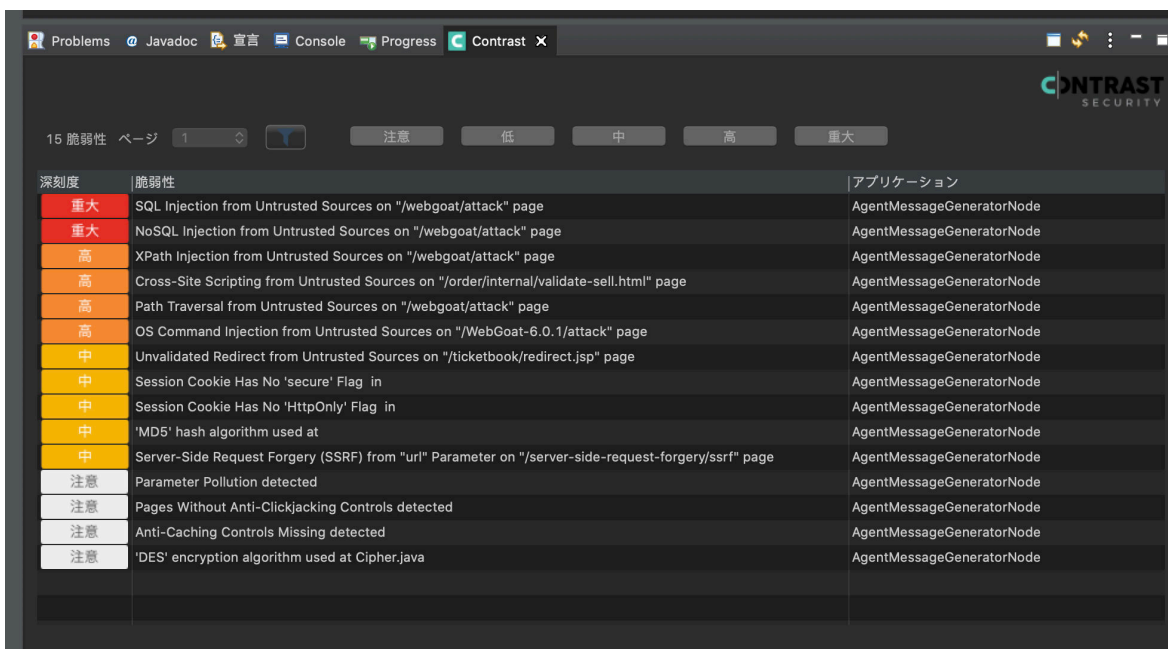
## Eclipse

Contrast エージェントが組み込まれているアプリケーションでは、Contrast からの脆弱性情報を開発中の Eclipse IDE で直接表示することができ、迅速な修正が可能になります。影響を受けるコード行を確認し、脆弱性について Contrast Web インターフェイスでさらに詳細を参照できます。

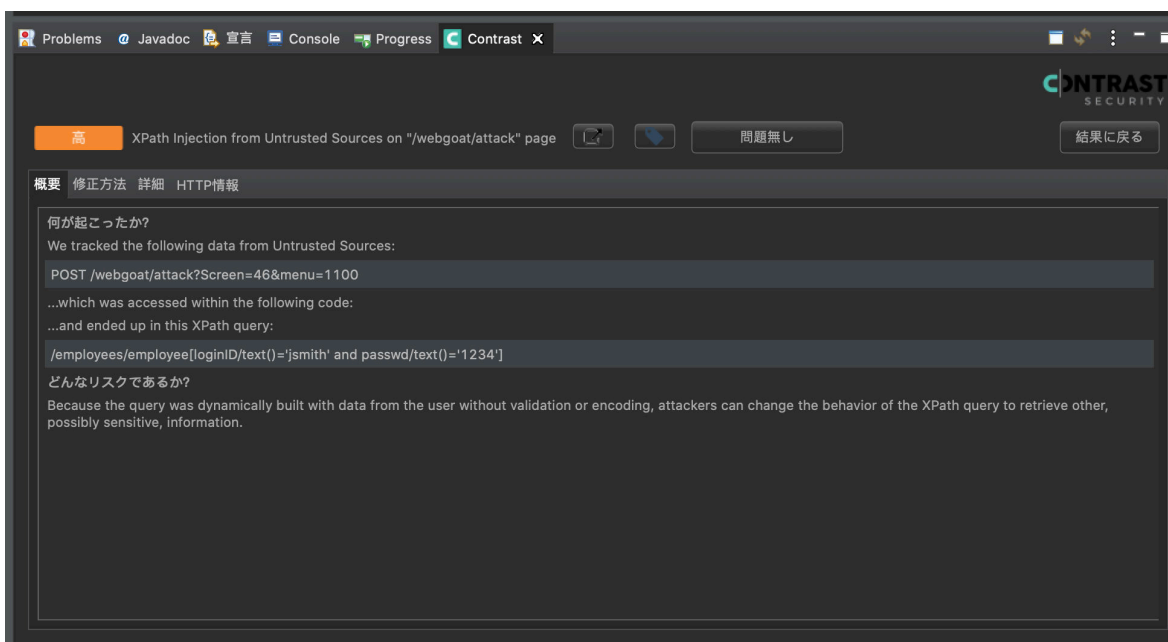
このプラグインは Mac/OS、Linux および Windows で利用でき、最新バージョンの Eclipse をサポートします。

Eclipse プラグインをインストールするには、[Eclipse マーケットプレイス](#)にアクセスするか、以下の操作を行います。

- Eclipse で、**ヘルプ > Eclipse マーケットプレイス**を選択します。
- 「Contrast Security」を検索します。
- インストール**を選択します。
- ウィンドウ > ビューの表示 > その他**を選択し、プラグインを設定します。
- 「Contrast」を検索し、検索で表示されたビューを追加します。
- 設定ページで、**ユーザ名**、**API キー**、**組織 ID**、および**サービスキー**を入力します。[これらのキー \(478ページ\)](#)は Contrast Web インターフェイスのユーザの設定画面で確認できます。
- 追加**を選択します。
- 脆弱性ビュー**に、Contrast からの全ての脆弱性の一覧が表示されます。これらの脆弱性はソートしたり、フィルターで絞り込んだりできます。



9. 特定の脆弱性に関する情報を参照するには、その脆弱性のタイトルを選択します。そこから、修正方法のタブを選択すると、その脆弱性の対処方法が表示されます。詳細を選択し、Java スタックトレースをダブルクリックすると、特定のソースコード行にフォーカスできます。ここでは、脆弱性のステータスを変更することもできます。



10. ページに移動アイコンを選択すると、Contrast Web インターフェイスが開き、より詳細な脆弱性の情報を確認できます。

## Generic Webhook

Contrast では汎用の Webhook によるインテグレーションをサポートしており、POST メッセージを受信するあらゆる URL で通知を受信することができます。Contrast のイベント (643ページ)でトリガーされる、\$ApplicationName や\$ServerId などのカスタム変数をペイロードに追加 (641ページ)できます。

### 接続

Generic Webhook に接続するために、以下を行います。

1. Contrast からの通知を受信する URL を取得します。
2. ユーザメニューで**組織の設定 > インテグレーション**を選択します。
3. **Generic Webhook** の行で、**接続**を選択します。
4. Webhook に名前を付け、URL を指定のフィールドに貼り付けます。
5. インテグレーションするアプリケーションを選択します(複数選択可)。
6. **ペイロード**フィールドに **変数** を入力します。例：

```
{  
  "title": "$Title",  
  "message": "$Message"  
}
```

7. **追加**を選択します。





## 注記

この Webhook は、5 回試行しても応答しない場合、切断されます。設定を復元するには、接続を再テストし、再保存する必要があります。

Contrast で Generic Webhook が切断された時に、すべての管理者に Contrast 内と E メールで通知するよう、インテグレーションを設定できます。

この設定を行うには、**組織の設定 > インテグレーション > Generic Webhook > 設定を表示**にアクセスします。設定を行う接続名を選択します。そして、**接続失敗時に通知**のチェックボックスを選択し、**保存**をクリックします。

## Generic Webhook の変数

NEW\_VULNERABILITY や SERVER\_OFFLINE などの Contrast イベントからのデータを使用して、[Generic Webhook \(639ページ\)](#)のレスポンスをカスタマイズできます。各イベントには、ペイロードのリクエストで呼び出すことができる変数があります。変数には、一般的な共通情報として利用するもの、もしくは、アプリケーション用、サーバ用、脆弱性用があります。

変数	説明
共通変数	

変数	説明
\$EventType	Webhook のトリガーとなるイベントタイプ 例：SERVER_OFFLINE
\$Message	Webhook のトリガーとなったイベントの概要を表すメッセージ
\$OrganizationId	Contrast で組織の作成時に、組織に割り当てられた一意の ID
\$OrganizationName	組織の名前
\$Title	常に“Contrast Security”を返す
<b>アプリケーション変数</b>	
\$ApplicationChild	アプリケーションが子アプリケーションの場合は真(true)を返し、そうでない場合は偽(false)を返す
\$ApplicationCode	アプリケーションのタイトルに表示されるアプリケーション名の省略形、デフォルトでは空白 例：TEST
\$ApplicationContextPath	アプリケーションのコンテキストパス 例：/example/somethingelse
\$ApplicationFirstSeen	アプリケーションが最初に検知された日時(Unix 時間) 例：1572033840000
\$ApplicationHasParentApp	アプリケーションに親がある場合は真(true)を返し、そうでない場合は偽(false)を返す
\$ApplicationImportance	アプリケーションの重要度の列挙値(enum 値) 例：MEDIUM
\$ApplicationId	Contrast でアプリケーションの登録時に、アプリケーションに割り当てられた一意の ID 例：49fe2978-1833-4441-83db-2b70486d9413
\$ApplicationImportanceDescription	アプリケーションに割り当てられた重要度、例：Medium
\$ApplicationLanguage	アプリケーションのプログラミング言語
\$ApplicationLastSeen	アプリケーションが最後に検知された日時(Unix 時間)、例：1572033840000
\$ApplicationLicenseLevel	アプリケーションに Assess ライセンスがあるかどうか、値：Licensed、Unlicensed
\$ApplicationMaster	アプリケーションがマスターアプリケーションである場合は真(true)を返し、そうでない場合は偽(false)を返す
\$ApplicationName	アプリケーションの名前
\$ApplicationParentAppId	Contrast でアプリケーション(この場合は親アプリケーション)の登録時に、アプリケーションに割り当てられた一意の ID(存在する場合) 例：49fe2978-1833-4441-83db-2b70486d9413
\$ApplicationTags	アプリケーションのタグのカンマ区切りリスト
\$ApplicationTotalModules	アプリケーションにあるモジュールの数
<b>サーバ変数</b>	
\$Environment	サーバの環境、値：DEVELOPMENT、QA、PRODUCTION
\$ServerId	イベントに関与しているサーバの ID 複数サーバが関与している場合、カンマ区切りのサーバ ID リスト
\$ServerName	イベントに関与しているサーバの名前 複数サーバが関与している場合、カンマ区切りのサーバ名リスト
<b>脆弱性変数</b>	
\$Severity	イベントのトリガーが脆弱性の場合、脆弱性の深刻度を返す
\$Status	イベントのトリガーが脆弱性の場合、脆弱性のステータスを返す
\$TraceId	イベントのトリガーが脆弱性の場合、脆弱性 ID を返す
\$VulnerabilityAgentLanguage	脆弱性が検知されたアプリケーションの言語またはフレームワーク名 (例：.Java、.NET、Ruby など)

変数	説明
\$VulnerabilityAppVersionTags	脆弱性が検出されたアプリケーションのバージョン 例：v1.2.3
\$VulnerabilityAutoRemediatedExpirationPeriod	脆弱性が自動修復される有効期間(Unix 時間) 例：1572033840000
\$VulnerabilityBugTrackerTickets	脆弱性情報がバグ管理システムに送信されて、作成されたチケットのリスト(カンマ区切り) 例：ticket1, ticket2, ticket3
\$VulnerabilityCategory	検出された脆弱性のカテゴリ、例：Injection
\$VulnerabilityClosedTime	脆弱性がクローズされた日時(Unix 時間) 例：1572033840000
\$VulnerabilityConfidence	脆弱性の信頼度
\$VulnerabilityDefaultSeverity	脆弱性のデフォルトの深刻度
\$VulnerabilityDiscovered	脆弱性が最初に検出された日時(Unix 時間) 例：1572033840000
\$VulnerabilityEvidence	脆弱性のエビデンス
\$VulnerabilityInstanceUuid	Contrast で脆弱性インスタンスの作成時に、脆弱性インスタンスに割り当てられた一意の ID 例：R33T-N00B-TGIF-RM6P
\$VulnerabilityFirstTimeSeen	脆弱性が最初に検出された日時(Unix 時間)、例：1572033840000
\$VulnerabilityImpact	脆弱性の影響度レベル、値：Low、Medium、High
\$VulnerabilityLastTimeSeen	脆弱性が最後に確認された日時(Unix 時間)、例：1572033840000
\$VulnerabilityInstanceLastTimeSeen	脆弱性が最後に確認された日時(Unix 時間)、例：1572033840000
\$VulnerabilityLicenseLevel	脆弱性のライセンスレベル
\$VulnerabilityLikelihood	脆弱性の可能性レベル 値：Low、Medium、High
\$VulnerabilityReportedToBugTracker	脆弱性がバグ管理システムに送信された日時(Unix 時間) 例：1572033840000
\$VulnerabilityReportedToBugTrackerTime	脆弱性がバグ管理システムに送信された場合、真(true)を返す
\$VulnerabilityRule	脆弱性に関連付けられたルール
\$VulnerabilityRuleName	脆弱性に関連付けられたルールの名前
\$VulnerabilityRuleTitle	脆弱性に関連付けられたルールのタイトル
\$VulnerabilitySubStatus	脆弱性のサブステータス
\$VulnerabilityTags	脆弱性に関連付けられたカスタムタグ 例：my-custom-tag
\$VulnerabilityTitle	脆弱性のタイトル
\$VulnerabilitySubStatusKeyCode	脆弱性サブステータスのキーコード
\$VulnerabilityTotalTracesReceived	脆弱性が受信された合計回数
\$VulnerabilityUuid	脆弱性を検索するために使用される一意の ID
\$VulnerabilityVisible	脆弱性にライセンスがあり参照可能である場合は真(true)を返し、そうでない場合は偽(false)を返す
\$VulnerabilityRule	イベントのトリガーが脆弱性の場合、脆弱性が違反したルールを返す
\$VulnerabilityTags	イベントのトリガーが脆弱性の場合、脆弱性に関連付けられたタグのリスト(カンマ区切り)を返す

## イベントと Generic Webhook 変数

NEW\_VULNERABILITY や SERVER\_OFFLINE などの Contrast のイベントからのデータを使って、[Generic Webhook \(639ページ\)](#)のレスポンスをカスタマイズできます。各イベントには、[共通 \(641ページ\)](#)変数、[アプリケーション \(642ページ\)](#)変数、[サーバ \(642ページ\)](#)変数、または[脆弱性 \(642ページ\)](#)変数があり、ペイロードのリクエストで呼び出すことができます。

イベント	変数
ATTACK_END	共通 (641ページ)、アプリケーション (641ページ)、サーバ (642ページ)
ATTACK_EVENT_COMMENT	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)
ATTACK_UPDATE	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)
EXPIRING_LICENSE	共通 (641ページ)、アプリケーション (642ページ)
NEW_ASSET (新規アプリケーションの場合)	共通 (641ページ)、アプリケーション (642ページ)およびサーバ (642ページ)(新規アプリケーションの場合)
NEW_ATTACK_APPLICATION	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)
NEW_ATTACK_UPDATE	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)
NEW_ATTACK	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)
NEW_VULNERABILITY_COMMENT	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)、脆弱性 (642ページ)
NEW_VULNERABILITY	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)、脆弱性 (642ページ)
NEW_VULNERABLE_LIBRARY	共通 (641ページ)、アプリケーション (642ページ)
SERVER_OFFLINE	共通 (641ページ)、サーバ (642ページ)
VULNERABILITY_CHANGESTATUS_CLOSED	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)、脆弱性 (642ページ)
VULNERABILITY_CHANGESTATUS_OPEN	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)、脆弱性 (642ページ)
VULNERABILITY_DUPLICATE	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)、脆弱性 (642ページ)

## GitHub とのインテグレーション

インテグレーションを設定して、Contrast でアプリケーションの脆弱性が検出された際に、自動で GitHub に問題が送信されるようにします。

設定を開始する前に、以下を準備してください。

- GitHub アカウントの認証情報(ユーザ名と個人用アクセストークン)。個人用アクセストークンを作成する際に、必ず **repo** の権限を有効にしてください。
- アプリケーションに対する GitHub 組織とリポジトリへのアクセス
- リポジトリへの書き込み権限(**push アクセス**)。設定フォームで、ラベル、マイルストーン、担当者を設定するために必要です。
- HTTP 経由で Contrast にアクセス可能な GitHub の実行インスタンス

GitHub に接続するために、以下を行います。

1. ユーザメニューで、**組織の設定 > インテグレーション**にアクセスします。
2. GitHub の行にある**接続**をクリックします。
3. **GitHub** への接続の設定画面で、インテグレーション名、GitHub に接続するアカウントのユーザ名、個人用アクセストークンを各フィールドに入力します。GitHub の URL は、設定する Contrast インスタンスからアクセスできる必要があります。
4. 設定画面の下部にあるチェックボックスをオンにすると、新たに検出された脆弱性に対して GitHub でチケットが自動的に作成されます。表示される複数選択フィールドで、チケットを作成する脆弱性のルールと深刻度を選択します。デフォルトでは、**重大**と**高**が選択されます。
5. フィールドに入力したら、**接続をテスト**を選択します。この処理は、GitHub の組織とリポジトリの数によっては、数分かかる場合があります。接続テストでは、Contrast から GitHub インスタンスにアクセスでき、指定したユーザがログインできることを確認します。
6. 接続できたら、このバグ管理システムとの連携を有効にする**アプリケーション**を選択します。
7. ドロップダウンで **GitHub の組織**と**リポジトリ**フィールドの値を選択します。



### 注記

GitHub の組織またはリポジトリの値を変更した場合は、オプションフィールドの値を再入力する必要があります。

- 必要に応じて、GitHub の課題のラベル(Labels)、担当者(Assignees)、マイルストーン(Milestone)を各フィールドを使用して指定できます。



### 注記

複数の脆弱性を 1 つの課題として GitHub に一括送信した場合、GitHub でのチケットのステータスは、そのチケットに関連付けられている全ての脆弱性に反映されます。複数の課題が 1 つの脆弱性に関連付けられている場合は、全てのチケットをクローズするまでその脆弱性をクローズできません。

## Gradle プラグイン

Contrast Gradle プラグインは、*Contrast.jar* とビルドを統合するのに使用されます。Contrast で認証を行い、最新の Java エージェントをダウンロードしてビルドを検証することができます。



### 注記

Gradle は、*build.gradle* ファイルを活用してアプリケーションを設定するビルドツールです。さまざまな種類のアプリケーションをビルド、パッケージ化、テストするのに使用されます。

## サンプル Web アプリケーションの複製

プロジェクトを設定する最も簡単な方法は、Gradle ベースの Web アプリケーションのサンプルを複製することです。このアプリケーションは Maven から Gradle へと移行され、MongoDB に依存します。

- インストールしてデータベースパスを設定します。

```
git clone https://github.com/Contrast-Security-OSS/Contrast-Sample-Gradle-Application
brew install mongodb
sudo mkdir -p /data/db
brew services start mongodb
```

- アプリケーションの実行準備が整います。*Contrast-Sample-Gradle-Application/build.gradle* ファイルを開きます。スクロールして *contrastConfiguration* 拡張機能を見つけます。 *appName* と *serverName* 以外の値は、全て [個人のキー \(478ページ\)](#) にあります。

```
contrastConfiguration {
    username = "username"
    apiKey = "apiKey"
    serviceKey = "serviceKey"
    apiUrl = "apiUrl"
    orgUuid = "orgUuid"
    appName = "editLATER"
```

```
serverName = "editLATER"
}
```

- contrastInstall タスクを呼び出して、Contrast JAR ファイルをインストールします。これにより、プロジェクトのビルドディレクトリに Contrast JAR がインストールされます。

```
cd path/to/Contrast-Sample-Gradle-Application
gradle build -x test contrastInstall
```

- Java エージェントでアプリケーションを実行します。サーバが起動します。

```
cd path/to/Contrast-Sample-Gradle-Application/build
java -Dcontrast.agent.java.standalone_app_name=mytestapp -
Dcontrast.server=mytestserver -jar libs/Contrast-Sample-Gradle-
Application-0.0.1-SNAPSHOT.jar
```

- localhost:8080 でアプリケーションが実行されていることと、Contrast にアプリケーションが表示されることを確認します。
- Contrast 内で、前述のコマンドで指定された appName のアプリケーションが表示されていることを検証します。
- Contrast-Sample-Gradle-Application プロジェクトの build.gradle で contrastConfiguration を編集して、前のステップで Java エージェントのオプションとして指定した appName と serverName を指定します。

```
contrastConfiguration {
    username = "alreadySetup"
    apiKey = "alreadySetup"
    serviceKey = "alreadySetup"
    apiUrl = "alreadySetup"
    orgUuid = "alreadySetup"
    appName = "mytestapp"
    serverName = "mytestserver"
}
```

- いつでも検証タスクを実行して脆弱性を確認できます。

```
gradle build contrastVerify -x test
```

## プラグインの使用

プラグインのコードは [GitHub リポジトリ](#) で参照できます。プラグインによって追加される 2 つのタスク (contrastInstall および contrastVerify) とその仕組みを確認できます。

プラグインの最新バージョンは、[Gradle プラグインの Web ページ](#) にあります。

タスク	説明
contrastInstall	<p>ローカルプロジェクトに Contrast Java エージェントをインストールします。Contrast エージェントで JVM が起動するよう、プラグインによって <code>gradle.properties</code> ファイルの <code>org.gradle.jvmargs</code> プロパティが編集されます。contrastVerify タスクで脆弱性を絞り込むためのアプリケーションバージョンは、このタスク中に生成されます。プラグインでは、以下の順番でアプリケーションバージョンが生成されます。</p> <ul style="list-style-type: none"> <li>TravisCI でビルドが実行されている場合、Contrast は <code>appName-\$TRAVIS_BUILD_NUMBER</code> を使用します。</li> <li>CircleCI でビルドが実行されている場合、Contrast は <code>appName-\$CIRCLE_BUILD_NUM</code> を使用します。</li> <li>TravisCI と CircleCI 以外でビルドが実行されている場合、Contrast は <code>appName-yyyyMMddHHmm</code> 形式でアプリケーションバージョンを生成します (yyyyMMddHHmm は、ビルドの生成時刻です)。</li> </ul>
contrastVerify	Web アプリケーションで新規の脆弱性をチェックします。

## Contrast IntelliJ プラグイン

IntelliJ プラグインを使用すると、Contrast エージェントが組み込まれたアプリケーションの脆弱性情報を IntelliJ IDE から確認できます。

このプラグインによって、脆弱性の影響を受けるコード行が IntelliJ 内で表示され、詳細を Contrast Web インターフェイスで確認することができます。このようにして、開発者は開発中にアプリケーションセキュリティに関するフィードバックを得ることができ、脆弱性に迅速に対応することができます。

このプラグインは、IntelliJ バージョン 2017.1.5 以降をサポートします。

## IntelliJ プラグインをインストールして設定し、使用するには：

1. Windows の場合は、**File > Settings > Plugins > Browse Repositories** にアクセスします。OSX の場合は、**Preferences > Plugins > Search in Repositories** にアクセスします。
2. **Contrast Security** を検索します。
3. **Install** を選択します。
4. Windows の場合は、**File > Settings > Contrast** にアクセスします。OSX の場合は、**Preferences > Other settings > Contrast** にアクセスします。
5. **Contrast URL**、**Username**(ユーザ名)、**Service Key**(サービスキー)、**API Key**(API キー)、および **Organization ID**(組織 ID)を入力します。これらの情報は[プロファイル \(478ページ\)](#)で確認できます。
6. **Add** を選択して、新しい組織を追加します。
7. Contrast の画面で **Refresh**(リフレッシュ)を選択すると、脆弱性の一覧が更新されます。IntelliJ の **脆弱性ビュー**に、Contrast からの全ての脆弱性が一覧で表示されます。脆弱性をソートするには、列のヘッダを選択します。フィルターを使用するには、ファネルアイコンを選択します。詳細を表示するには、脆弱性の名前を選択します。

## IntelliJ で Java エージェントを設定

IntelliJ IDE のサポート対象のアプリケーションサーバを使用するアプリケーションに Contrast エージェントを追加するには：

1. アプリケーションツールバーで **Run** をクリックして、ドロップダウンメニューから **Edit Configuration...** をクリックします。
2. IntelliJ サーバの設定インスタンスを選択します。
3. **サーバの設定タブ**を選択して、**VM Options** に Contrast ランチャー文字列となる - `javaagent:<YourContrastJarPath>`を入力します。<YourContrastJarPath>をお使いの [Contrast JAR \(57ページ\)](#)ファイルへのパスに置き換えます。
4. **Apply** をクリックして、**OK** をクリックします。
5. **サーバ**を起動します。  
サーバのコンソールに、Contrast の起動メッセージが表示されます(サーバの起動には、1〜2 分ほど時間がかかります)。
6. アプリケーションにアクセスし、起動するまでにさらに 1 分ほどお待ちください。

## Jenkins とのインテグレーション

**Jenkins** は、アプリケーションのビルド、テスト、デプロイ、実行のプロセスを自動化する継続的インテグレーション(CI)ツールです。

Contrast の Jenkins プラグインを使用すると、このパイプラインにアプリケーションセキュリティゲートを追加できます。セキュリティゲートとして、脆弱なアプリケーションの Jenkins ジョブを「FAILURE(失敗)」や「UNSTABLE(不安定)」などのビルド結果で失敗させる基準を指定できます。



### ヒント

このプラグインのソースコードは、[Jenkins プラグインの Github リポジトリ](#)で参照できます。

互換性を保つために、次のバージョンを使用してください。

Jenkins	Contrast-Jenkins プラグイン	Contrast
2.60.3	3.4	3.7.6
2.60.3	3.7	3.7.10
2.60.3	3.8	3.8.0

## Jenkins プラグインのインストールと使用

1. Contrast と Jenkins 間の [接続を定義 \(648ページ\)](#) します。
2. お使いの環境に合わせて、Jenkins をどのように利用するかを決めます。
  - フリースタイルのジョブを使用している場合、[システムレベル \(649ページ\)](#)がビルド後の処理 ([650ページ](#))として、脆弱性に対するセキュリティ制御を定義できます。
  - [パイプラインのステップ \(650ページ\)](#)に脆弱性のセキュリティ制御を定義します。
  - Contrast の組織管理者が[ジョブ結果ポリシー \(652ページ\)](#)を定義することもできます。
3. [ビルドを実行 \(656ページ\)](#) します。

## 関連項目

- [Jenkins から Contrast へ接続 \(648ページ\)](#)
- [Jenkins でセキュリティ制御を定義 \(652ページ\)](#)
- [Contrast でジョブ結果ポリシーを定義 \(652ページ\)](#)
- [Jenkins でのビルドの実行 \(656ページ\)](#)

## 接続

### 開始する前に

- Contrast Security の全てのインテグレーションで、接続を設定するために[組織管理者のロール \(819ページ\)](#)が必要です。
- [Jenkins](#) をインストールしてください。
- [Jenkins](#) [パイプライン](#)が既にセットアップ済みであること。

### 接続を定義

Jenkins で Contrast への接続を定義するには：

1. Jenkins のダッシュボードで、左のサイドバーの **Jenkins の管理** を選択します。
2. **System Configuration** で **プラグインの管理** を選択します。
3. **インストール済み** タブで、**Contrast Continuous Application Security** プラグインを有効にするためにチェックします。
4. 再度、**Jenkins の管理** を選択します。
5. **システムの設定** を選択し、**Contrast Connections** のセクションを探してください。
6. **Contrast Username** の項目に、Contrast のユーザ名を入力します。このユーザ名は、Contrast のアカウントに使用する E メールアドレスです。
7. 以下を入力します。
  - **Contrast API Key**(Contrast API キー)
  - **Contrast Service Key**(Contrast サービスキー)
  - **Contrast URL**
  - **Organization ID**(組織 ID)これらの情報は [プロファイル \(478ページ\)](#) にあり、[ユーザの設定 > プロファイル > あなたのキー](#) でアクセスできます。
8. **Result of a vulnerable build** を選択して、アプリケーションが脆弱である場合に Contrast から Jenkins ジョブの結果をどのように返すかを選択します。指定できるオプションは以下の通りです。



- **FAILURE**(失敗)
  - **UNSTABLE**(不安定)
  - **SUCCESS**(成功)
  - **NOT\_BUILT**(ビルドしない)
  - **ABORTED**(停止)
9. Jenkins インスタンスがアプリケーションを見つけられないときに Jenkins ジョブを自動的に失敗させたい場合は、**Apply this vulnerable build result to the job when Jenkins encounters an error with Contrast** のボックスにチェックをします。
  10. アプリケーションが Jenkins のシステムレベルで脆弱であるかを判断するために、Contrast プラグインで使用する基準を定義できます。ジョブレベルの制御をシステムレベルの制御より優先したい場合は、**Allow job level application vulnerability security controls to override those controls set here at the system level** の横にあるボックスにチェックをします。インスタンス内のすべての Jenkins ジョブで基準の一貫性を持たせたい場合は、このボックスをオフのままにします。



### 注記

[ジョブ結果ポリシー \(652ページ\)](#) を使用してセキュリティ制御を設定している場合、それらのポリシーはジョブレベルまたはシステムレベルで設定されたポリシーよりも優先されます。

11. プラグインが Contrast に認証され、アプリケーションの脆弱性に関する情報を取得できることを確認するために、**Test Contrast connection** をクリックします。
  - プラグインが認証されると成功のメッセージが表示されます。
  - 認証に失敗した場合は、Contrast の認証情報(URL など)を確認してください。

## 関連項目

- [Jenkins でセキュリティ制御を定義 \(652ページ\)](#)
- [Contrast でジョブ結果ポリシーを定義 \(652ページ\)](#)
- [Jenkins でのビルドの実行 \(656ページ\)](#)

## システムレベルのセキュリティ制御を定義

Jenkins で [接続を定義 \(648ページ\)](#) した後、フリースタイルのジョブを使用している場合は、システムレベルで Contrast の脆弱性によるセキュリティ制御を設定することができます。または、[ジョブレベルでセキュリティ制御を設定 \(650ページ\)](#) することもできますし、[ジョブ結果ポリシー \(652ページ\)](#) を使用して、それらのセキュリティ制御より優先させることもできます。

1. **Contrast Connections > Contrast Vulnerability Security Controls** で、ドロップダウンから以前作成した **Connection** を選択します。
2. **Number of Allowed Vulnerabilities** を設定します。この数字は除かれるので、「5」に設定すると、6 件以上の脆弱性がある場合に Jenkins が失敗します。このフィールドは必須です。
3. ドロップダウンのオプションから **Vulnerability Severity** を選択します(これらは、Contrast の [脆弱性の深刻度オプション \(602ページ\)](#) と同じです)。プラグインにより、このフィールドに指定された深刻度以上の全ての脆弱性について API コールにフィルターが設定されます。このフィールドは必須ではありませんが、選択すると結果を絞り込むことができます。従って、この数値を「5」に設定し、深刻度に **High**(高)を選択した場合、深刻度の高い脆弱性が 6 件以上あると Jenkins は失敗します。
4. ドロップダウンから **Vulnerability Type**(ルール名)を選択します。プラグインは、選択したルール名で脆弱性の数をチェックし、そのルールで許容される脆弱性の数と比較します。このフィールドは必須ではありませんが、選択すると結果を絞り込むことができます。セキュリティ制御ごとに 1 つの深刻度と 1 つのルール名を選択できます。
5. **Vulnerability Statuses** を選択します。これらの脆弱性のステータスは必須ではありませんが、便利な場合があります。例えば、**Confirmed** と **Suspicious** を選択すると、ステータスがオープン中

の脆弱性のみが返されます。ステータスで脆弱性をフィルタリングしない場合は、選択しないままにします。

脆弱性のセキュリティ制御は複数登録することができますが、プラグインは最初に合致した悪条件でジョブを失敗させます。最初に違反した脆弱性のセキュリティ制御でビルド結果が返されます。

## ビルド後の処理としてセキュリティ制御を定義

Jenkins の [システムレベル \(649ページ\)](#) でセキュリティ制御を設定した後に、Jenkins のパイプラインに含まれないフリースタイルのジョブに対して、ジョブレベルでセキュリティ制御を追加することもできます。これを行うには：

- Jenkins でジョブを定義する際に、**ビルド後の処理**セクションを探します。
- ドロップダウンから、以前作成した**接続**を選択します。
- アプリケーションを選択します。このフィールドは必須です。
  - アプリケーションで既に Contrast エージェントを使用している場合は、**Choose your application** ドロップダウンからアプリケーションを選択します。
  - アプリケーションでまだ Contrast エージェントを使用していない場合は、**Application Name** と **Application Language** フィールドを使用して、アプリケーションを指定します。Contrast で検査するアプリケーションと同じアプリケーション名を Jenkins に指定してください。アプリケーションで Contrast エージェントが有効になったら、Contrast によるビルド後の処理時に、そのアプリケーションと同じ名前と同じ言語が使用されます。
- [システムレベルの脆弱性セキュリティ制御を上書きできる \(649ページ\)](#) ように接続が設定されている場合は、**Override Vulnerability Security Controls at the Jenkins system level** の横にあるチェックボックスをオンにすることで、その設定を上書きできます。  
この場合、このジョブの **Number of Allowed Vulnerabilities**、**Vulnerability Severity**、**Vulnerability Type**、**Vulnerability Statuses** も指定する必要があります。
- Query vulnerabilities by** でオプションを選択して、脆弱性のクエリ方法を選択します。そうすると、そのジョブで検出される脆弱性のみが対象となります。デフォルトでは、最初のオプションである、`appVersionTag`、`format: applicationId-buildNumber` がプラグインで使用されます。

## Jenkins のパイプラインで脆弱性のセキュリティ制御を定義

`contrastAgent` というパイプラインステップを使用すると、Contrast エージェントをダウンロードして、アプリケーションにエージェントを組み込み、実行することができます。

`contrastVerification` というパイプラインステップを使用すると、アプリケーションを検証し、セキュリティ制御のパラメータを設定できます。

## contrastAgent でダウンロード

`contrastAgent` という名前のパイプラインステップは、最新の Contrast エージェントをダウンロードします。

パラメータ	必須項目	説明	例
<code>profile</code>	必須	Contrast との通信に使用する Contrast 接続プロファイル	<code>MyConnection</code>
<code>outputDirectory</code>	必須	ダウンロードしたエージェントを配置する場所を定義	<code>env.WORKSPACE</code>
<code>agentType</code>	<code>applicationId</code> が定義されていない場合は必須	アプリケーションに組み込んだエージェントのタイプ(大文字と小文字の区別なし) オプション: : <code>Java</code> 、 <code>.NET</code> 、 <code>.NET_Core</code> 、 <code>Node</code> 、 <code>Ruby</code> 、 <code>Python</code>	<code>Java</code>

`contrastAgent` という名前のパイプラインステップを追加する例を次に示します。

- ```
node{
  stage('Download Latest Contrast Agent'){
    contrastAgent profile:'MyConnection', outputDirectory: \
env.WORKSPACE, agentType: 'Java'
```

```
}
}
```

## contrastVerification でアプリケーションを検証

contrastVerification という名前のパイプラインステップを使用して、アプリケーションが脆弱かどうか検証できます。

| パラメータ           | 必須項目                                       | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 | 例                                    |
|-----------------|--------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| profile         | 必須                                         | profile を使用して、Contrast との通信に使用する接続を指定します。                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Contrast Connection                  |
| queryBy         | 必須                                         | queryBy を使用して、ビルドに関連する脆弱性にフィルタをかけます。オプション 1、2、4 の場合、この値は、アプリケーションの実行中に Contrast エージェントに渡された contrast.override.appversion パラメータと一致する必要があります。<br><br>脆弱性をクエリする方法をオプション番号で指定します(デフォルトの値は 1)：<br><br>1. appVersionTag,<br>format: applicationId-\${BUILD_NUMBER}<br>2. appVersionTag,<br>format: applicationId-\${JOB_NAME}-\${BUILD_NUMBER}<br>3. startDate (これはビルドのタイムスタンプです。ビルド開始後に検出された脆弱性のみを調べます。)<br>4. APPVERSIONTAG (これは、ジョブパラメータが環境変数です。独自のテキストを指定する場合は、このオプションを選択し、Jenkins ジョブ内の環境変数として APPVERSIONTAG をエクスポートしてください。JOB_NAME と BUILD_NUMBER の両方は、既に Jenkins の環境変数として利用可能です。) | 1                                    |
| applicationId   | applicationName と agentType が定義されていない場合は必須 | 検証しようとしているアプリケーションまたはアプリケーションモジュールの ID                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | cb3ea678-38c8-4487-ba94-692a117e7966 |
| applicationName | applicationId が定義されていない場合は必須               | 検証しようとしているアプリケーションの名前(大文字と小文字の区別なし)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | MyApp                                |
| count           | オプション                                      | 許容する脆弱性の総数、デフォルトは 0                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                | 10                                   |
| rule            | オプション                                      | デフォルトは All                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | xss                                  |
| severity        | オプション                                      | デフォルトは All。その他のオプション：<br><b>Critical、High、Medium、Low</b>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           | <b>High</b>                          |
| appVersionTag   | オプション                                      | Contrast エージェントの contrast.override.appversion パラメータに渡された値                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | v1.2.3                               |

contrastVerification という名前でパイプラインステップを追加する方法の例をいくつか示します。

- queryBy startDate を使用：

```
contrastVerification applicationId: '1e6ad9c6-89d4-4f06-bdf6-92c569ec89de', count: 1, profile: 'new-profile', queryBy: 3, \
rule: 'cache-controls-missing', severity: 'High'
```

- queryBy のカスタム appVersionTag パラメータを使用：

```
contrastVerification applicationId: '1e6ad9c6-89d4-4f06-bdf6-92c569ec89de', count: 1, profile: 'new-profile', queryBy: 4, \
appVersionTag: 'v1.2.3' rule: 'cache-controls-missing', severity: 'High'
```

- `applicationName` と `AgentType` を使用してアプリケーションを定義 :

```
contrastVerification applicationName: 'MyApp', agentType: 'Java', count: \
1, profile: 'new-profile', queryBy: 3, rule: 'cache-controls-missing', \
severity: 'High'
```

- 事前設定またはオーバーライドされている脆弱性のセキュリティ制御でアプリケーションを検証します。

[Contrast \(652ページ\)](#)で脆弱性のセキュリティ制御が事前に設定されていることがわかっている場合は、プロファイルおよび、`applicationId` が(`applicationName` と `agentType`)のいずれかを定義するだけで良いです。

```
contrastVerification applicationId: '35ae7b89-1c76-414b-b317-
c444ce27608b', profile: 'ContrastConnection'
```

## Jenkins でのセキュリティ制御

Jenkins で、以下のセキュリティ制御を定義できます。

- システムレベルでの制御 ([649ページ](#))
- ビルド後の処理としての制御 ([650ページ](#))
- パイプラインでの制御 ([650ページ](#))

## ジョブ結果ポリシーの定義

ジョブ結果ポリシー(Contrast Jenkins プラグインのバージョン 3.3 以降でサポート)は、Contrast プラグインを使用する Jenkins ジョブにビルド結果を割り当てます。ジョブ結果ポリシーにより、設定した基準に基づいて、ジョブのビルド結果に **FAILURE**(失敗)、**UNSTABLE**(不安定)、**SUCCESS**(成功)などのステータスが付けられます。

## 開始する前に

Contrast でジョブ結果ポリシーを定義するには、組織の管理者である必要があります。

## ポリシーを定義

ジョブ結果ポリシーを定義するには :

1. Contrast Web インターフェイスで[組織の設定 \(704ページ\)](#)を選択し、左のナビゲーションで**インテグレーション**を選択します。
2. **Jenkins** の行で、**ジョブ結果ポリシーを追加**を選択します。

 Jenkins ジョブ結果ポリシーを定義

ジョブ結果ポリシーは、アプリケーションおよび脆弱性に関して定義されているプロパティに基づいて、Jenkins ジョブにビルド結果を割り当てます。詳細はこちらです。

名前\*

このジョブ結果ポリシーの名前を入力

アプリケーション

アプリケーション名 ▼ 全てのアプリケーション (152) ✕

脆弱性プロパティ

環境

全ての環境 (3) ✕

脆弱性ルールと深刻度 ⓘ 許容される脆弱性数 ⓘ

全てのルール ▼ - 件の脆弱性

+ 別のルールを追加

脆弱性ステータス

報告済 ✕ | 確認済 ✕ | 疑わしい ✕

最初に検知された脆弱性

開始 アプリケーションのオンボード時 ▼ 終了 JenkinsでContrastステップ実行 ▼

脆弱性にフィルターをかける時にプラグインのQuery vulnerabilities byで選択したオプションを適用します。

ポリシー結果

ポリシー違反の場合は、ジョブ結果を割り当て:

失敗

不安定

成功

ⓘ ジョブ結果ポリシーが競合するアプリケーションには、結果が最も深刻なポリシーが適用されます。

このジョブ結果ポリシーを有効化

- ジョブ結果ポリシーの名前を定義します(必須)。
- アプリケーションで、ポリシーを適用するアプリケーションを指定します。アプリケーションは、名前や重要度、またはタグで指定できます。アプリケーション名で選択する場合、個々のアプリケーションやマージされたアプリケーション (485ページ) を選択できます。
- 脆弱性プロパティでは、ポリシーの対象とする脆弱性の制限や環境などを定義します。環境、脆弱性ステータス、最初に検知された脆弱性を使用して、ポリシーの対象とする脆弱性を絞り込みます。脆弱性ルールと深刻度を使用して、ジョブ結果のステータス変更のトリガーとなるルール(特定の深刻度)とその数をしきい値として指定します。
  - 環境：ポリシーを適用する環境を選択します(複数選択可)。例えば、テスト(QA)環境にある脆弱性が本番環境で発生してしまうのを防ぐには、QA を選択します。(ただし、この場合、開発環境の脆弱性は考慮されません。それらの脆弱性を対象とするには、開発環境も選択します。または、すべての環境の脆弱性を対象とする場合は、全ての環境を選択します。)
  - 脆弱性ステータス：どのステータスを対象とするかを選択します(複数選択可)。脆弱性のステータス (598ページ) は、Contrast で決定されます。



### ヒント

ほとんどの場合、報告済、確認済、疑わしいなどのオープン中のステータスのみを選択します(問題無し、修復済や修正完了などのクローズのステータスではなく)。そうすれば、既に開発者が対応した脆弱性によって、Jenkins のジョブが失敗したり不安定になることはありません。

- 最初に検知された脆弱性：脆弱性が最初に検知された時間に基づいて、ポリシーの対象とする脆弱性の時間範囲を設定します。

開始と終了フィールドを使用して、時間範囲の開始と終了を設定します。時間範囲の開始に、ジョブ開始時か、Contrast ステップを実行する前の所定の日数、またはアプリケーションをオンボードした日を選択します。時間範囲の終了に、Contrast ステップを実行する前の所定の日数か、Jenkins で Contrast ステップを実行するまで、または特定の期間のオプションを選択します。カスタマイズを選択して、いずれかのフィールドに特定の日付を選択することもできます。脆弱性がこの時間範囲外で最初に検出された場合、その脆弱性はポリシーの対象にはなりません。



### ヒント

開発者に一定期間(例えば、1週間)内に脆弱性を修正させるためには、7日以上前に検出された脆弱性のみをポリシー違反とさせるよう、ポリシーを定義します。これを行うには、開始にアプリケーションのオンボード時を、終了に過去7日間を設定します。

- **脆弱性ルールと深刻度**：このセクションを使用して、ポリシーで許可する脆弱性の件数、種類および深刻度によるしきい値を設定します。ルールごとに、深刻度が **Assess** ルールを選択したら、**許容する脆弱性数**を選択します。別のルールを追加をクリックすれば、複数のルールを登録できます。**許容される脆弱性数**は、この深刻度の脆弱性を、このビルドに影響を与えずに許容する脆弱性の数を決定します。「0」に設定すると、1つの脆弱性でビルド結果のステータスが変更されます。「10」に設定した場合は、指定した種類の脆弱性が 11 件検出されるまで、ビルド結果のステータスは変わりません。特定のルールや深刻度に対して、**許容される脆弱性数**を空欄のままにすると、そのルールや深刻度の全ての脆弱性が許容されます。例えば、全てのルールと 1 件の脆弱性を設定した場合、1つの脆弱性がポリシーのトリガーとなります。また、別のルールを追加して、このポリシーを 5つの重大な脆弱性のルールと 2つのクロスサイトスクリプティングの脆弱性に制限することもできます。
  - **脆弱性にフィルターをかける時にプラグインの"Query vulnerabilities by"で選択したオプションを適用します**の横のチェックボックスにチェックをします。Contrast Assess の**ビルド後の処理 (650ページ)**または**パイプラインステップ (651ページ)**を使用して、Jenkins ジョブの脆弱性をクエリするよう定義できます。例えば、AppVersionTag や、脆弱性が最後に検出された日などを使用できます。このチェックボックスを選択すると、ジョブ結果ポリシーの評価時にこのクエリが含まれるようになります。
- 以下は、ジョブ結果ポリシーの可能なルールと設定で、これらの条件が満たされた場合に Jenkins での結果ステータスを変更する例です。

## 脆弱性プロパティ

## 環境

全ての環境 (3)

## 脆弱性ルール ?

All rules

Critical

SQLインジェクション

## 許容される脆弱性数 ?

3

脆弱性

0

脆弱性

-

脆弱性

+ 別のルールを追加

## 脆弱性ステータス

Reported ×

Confirmed ×

Suspicious ×

## 最初に検知された脆弱性

## 開始

Application onboarding

## 終了

The Contrast step runs i...

この例では、次のような脆弱性がポリシー違反の対象となります。

- QA 環境として指定されたサーバで検出された全ての脆弱性
- ステータスが報告済、確認済、疑わしい全ての脆弱性
- アプリケーションのオンボード時から Jenkins で Contrast ステップが実行されるまでの間に初めて検出された全ての脆弱性

次のいずれかのうち少なくとも 1 つが発生すると、ポリシー違反となり、結果ステータスが変更されます。

- 重大な脆弱性が 1 つ以上ある
- SQL インジェクションを除く全てのルールで、高、中、低または注意の深刻度の脆弱性が合計で 4 つ以上ある



## 注記

脆弱性は 1 回だけカウントされ、最も具体性が高い設定(例、特定の脆弱性ルール)が、最も具体性が低い設定(全てのルール)より優先されます。ルールの種類と深刻度の両方で脆弱性の制限が設定されている場合、その脆弱性はルールの種類の数としてカウントされますが、深刻度の脆弱性としてカウントされません。従って、この例では、重大な脆弱性は深刻度の脆弱性数としてカウントされますが、高、中、低および注意の深刻度は全てのルールとしてまとめられます。

6. **ポリシー結果**で、ポリシーの結果を選択します。選択した基準に一致するジョブを Contrast で失敗 (FAILURE)、不安定 (UNSTABLE) または成功 (SUCCESS) のステータスにします。複数のジョブ結果ポリシーが指定されているアプリケーションには、違反しているすべてのポリシーで最も重大な結果が適用されます。
7. このジョブ結果ポリシーを有効化の横にあるチェックボックスをオフにすると、個々のポリシーを削除しなくても、Jenkins ジョブに Contrast のポリシーが適用されるのを一時停止できます。

## Jenkins でのビルドの実行

初めてビルドを実行するには：

1. Jenkins で、実行するジョブまたはプロジェクトを選択します。
2. 左側のメニューで、**Build Now** を選択します。
3. 詳細を見るには、ログ出力を表示します。
4. フリースタイルのジョブを使用している場合は、タスクからのデータを表示できます。実行を選択して、左側のメニューで **Vulnerability Report** を選択します。



### 重要

ジョブまたはプロジェクトの概要でグラフを見ることもできます。ただし、Contrast パイプラインステップを使用した場合、または 1 つ以上の選択されたアプリケーションがジョブ結果ポリシーで上書きされている場合は、グラフが表示されません。

## Jira とのインテグレーション

Contrast と Jira を連携し、チケットの自動生成、コメントの同期、アプリケーションのプッシュ通知などを可能にします。

設定を開始する前に、以下が必要です。

- Jira アカウントの認証情報。Jira Cloud の場合は、これはユーザ名と API キーになります。オンプレミスの Jira をインストールしている場合は、ユーザ名とパスワードです。
- 対象プロジェクトで課題を作成するための権限。
- HTTP 経由で Contrast にアクセス可能な Jira の実行インスタンス。
- Contrast に登録済みのアプリケーションと関連付けるプロジェクト

### 関連項目

- [Jira に接続する \(656ページ\)](#)
- [Assess と Jira の設定 \(657ページ\)](#)
- [サーバーレスと Jira の設定 \(658ページ\)](#)
- [Jira 認証情報の管理 \(660ページ\)](#)

### Jira に接続する

Jira とインテグレーションするには：

### Contrast で Jira を設定

1. Contrast Web インターフェイスで、**ユーザメニュー > 組織の設定 > インテグレーション**を選択します。
2. Jira の行にある **接続**を選択します。
3. **Jira への接続の設定画面**で、Jira インテグレーションの名前、ユーザ名および API キー(もしくは、オンプレミスの場合は Jira のパスワード)を入力します。Jira インスタンスの URL も入力したら、Contrast が URL にアクセスできるかを確認します。
  - Jira インテグレーションの名前を **接続名**に入力します。
  - Jira インスタンスの **URL** を入力します。
  - **Assess** が **Serverless** を選択します。



### 注記

Contrast では、ユーザ名、API キー(またはパスワード)および URL が認証情報セットとして、このインテグレーション用に保存されます。



4. **接続をテスト**を選択します。Jira プロジェクトが多数ある場合は、接続テストに数分かかることがあります。接続テストでは、Contrast が指定の Jira インスタンスにアクセスでき、ユーザがログインできることを確認します。
5. 接続をテストしたら、**Assess と Jira の設定 (657ページ)**または**サーバレスと Jira の設定 (658ページ)**を行います。

## 関連項目

- [Assess と Jira の設定 \(657ページ\)](#)
- [サーバレスと Jira の設定 \(658ページ\)](#)
- [認証情報の管理 \(660ページ\)](#)

## Assess と Jira の設定

Jira との接続をテストしたら、指定したトリガーに基づいて Jira チケットを作成するように設定できます。

## 開始する前に

- [Jira と接続 \(656ページ\)](#)ができることを確認してください。

## 手順

1. Contrast から Jira に接続できたら、**アプリケーション**フィールドをクリックして、セキュリティの問題に対して Jira チケットのトリガーとなるアプリケーションを指定します。また、Contrast で特定の重要度が設定されているアプリケーションに対してのみ、Jira チケットをトリガーすることもできます。その場合は、**アプリケーションの重要度**フィールドを選択して、Jira チケット作成のフィルターとして使用する重要度を指定します。

2. **プロジェクト名**、**デフォルトのエピック**、**デフォルトの割当先**、**デフォルトの課題タイプ**フィールドを使用して、Contrast 側で作成する Jira チケットの値を選択します。Contrast での脆弱性の深刻度レベルと Jira の優先度をマップすることもでき、担当者間でセキュリティチケットが管理しやすくなります。その他の Jira フィールドに事前入力したい場合は、**JIRA フィールドを追加**を選択します。ドロップダウンから、追加するフィールドとフィールドのデフォルト値を選択します。



### 注記

プロジェクト名やデフォルトの課題タイプを変更すると、関連する Jira のフィールドや選択できる値も変わります。Contrast Web インターフェイスでは選択済みの値が保持され、新たに選択したプロジェクトや課題タイプに対しても適用されません。

3. Jira 側で課題がクローズや再オープンされるたびに Contrast の脆弱性ステータスも更新したい場合は、**双方向のインテグレーションを有効にする**のオプションを選択してください。このオプション

ンを選択すると、チェックボックスの下に URL が生成されます。Jira 管理者は、この URL を使用して [Jira に Webhook を登録](#) してください。

脆弱性ステータスのドロップダウンを使用して、Jira チケットのステータス更新によって Contrast の脆弱性ステータスをどのように更新するかを設定します。



#### 注記

問題無しのステータスを選択する場合、ドロップダウンで理由を選択する必要があります。デフォルトでは、ドロップダウンの上記以外が選択されます。

双方向のインテグレーションを保存すると、関連する Jira チケットのステータス変更が Contrast で自動的に追跡されます。追跡情報は、脆弱性の **アクティビティ** タブにコメントとして表示されます。各コメントには、Jira インテグレーション名とチケットへのリンクが含まれます。



#### 注記

Atlassian は、https 以外の URL で Webhook を登録する機能を廃止しました。そのため、Contrast のオンプレミス版をご利用のお客様は、Jira の双方向インテグレーションを有効にする前に [HTTPS を設定 \(759ページ\)](#) する必要があります。

4. Contrast で脆弱性の検出時に Jira チケットを新規に作成したい場合は、**新たに検知された脆弱性に対してチケットを自動的に作成する**のオプションを選択してください。そして、どの深刻度やルールを Jira チケットのトリガーとするかを選択します。

複数の脆弱性を Jira の 1 つのチケットとして作成した場合、チケットのステータスは、そのチケットに関連付けられている全ての脆弱性に適用されます。1 つの脆弱性に対して複数のチケットを作成した場合は、Contrast で脆弱性をクローズする前に、全ての Jira チケットをクローズする必要があります。



#### 注記

自動作成のオプションは遡及しないため、過去の脆弱性に対する Jira チケットは生成されません。

5. **保存**を選択して、Jira インテグレーションの使用を開始します。インテグレーションを削除するには、**設定を削除**を選択します。

## サーバレスと Jira の設定

Jira の接続をテストした後に、インテグレーションによって Jira チケットを自動作成するために、脆弱性の深刻度と種類のサブセットを設定することができます。

### 開始する前に

- [Jira に接続 \(656ページ\)](#) できることと、Contrast に AWS アカウントがあることを確認してください。

### 手順

1. Jira との接続を確認したら、**設定を追加**をクリックして、検査結果から Jira チケットを作成する AWS アカウントを設定していきます。

2. 以下の情報を入力します。
  - **接続名**：作成する Jira インテグレーション名を入力します。
  - **認証情報名**：認証に使用するログイン情報を指定します。
3. 認証情報を編集または新規に作成するには、**認証情報名**フィールドの上にある**認証情報を管理**をクリックします。
4. 以下の情報を入力します。
  - **認証情報名**：前の手順で入力した名前
  - **URL**：Jira インスタンスの URL
  - **ユーザ名**
5. **API キー**を入力します。Contrast からのコールを認証するために、Jira の API キーを指定する必要があります。
  - API キーフィールド名の横にある情報アイコンをクリックして、**開始する**のリンクをクリックします。
  - 「API トークンを作成する」を選択します。
  - ラベルを入力します。
  - 作成をクリックします。
  - 「コピー」をクリックして、API トークンをクリップボードにコピーします。
  - Contrast Web インターフェイスに戻り、その API トークンを API キーフィールドに貼り付けます。
6. **接続をテスト**をクリックして、接続を確認します。
7. **保存**または**完了**をクリックします。
8. 特定のアプリケーションやアカウントに関連する脆弱性の Jira チケットを作成するために、**Serverless** オプションを選択します。
9. Jira チケットを作成したい**アカウント**を選択します。
10. チケットを作成する Jira の**プロジェクト名**を選択します。
11. **デフォルトのエピック**を設定します。新しいチケットを作成した場合のエピックを指定します(該当する場合)。
12. **デフォルトの割当先**を設定します。チケットを割り当てる担当者を指定します。
13. **デフォルトの課題タイプ**を設定します。作成するチケットのデフォルトの課題タイプ(タスク、ストーリー、バグなど)を選択します。



### 注記

プロジェクト名またはデフォルトの課題タイプを変更すると、関連する Jira のフィールドや選択できる値も変わります。Contrast Web インターフェイスでは選択済みの値が保持され、新たに選択したプロジェクトや課題タイプに対しても適用されます。

14. チケットを作成する結果の種類を選択します。
  - Permissions(権限)
  - Exploits(脆弱性)
  - Dependencies(CVE)
  - 深刻度(注意、低、中、高、重大)
15. チケットを作成する結果の種類を選択します。
  - **Jira フィールドを追加**を選択します。
  - 報告者フィールドやワークタイプフィールドなどを追加します。
16. 必要に応じて、Contrast での脆弱性の深刻度レベルを、該当する Jira の優先度レベル(Critical、Major、Standard など)にマッピングします。
17. **保存**を選択して、Jira インテグレーションの使用を開始します。インテグレーションを削除するには、**設定を削除**を選択します。

以下のビデオで、インテグレーション手順のデモをご覧ください。

<https://player.vimeo.com/video/827314961?h=f049a72b04>

新規に脆弱性を検出した場合に関しては、以下のビデオを参照してください。

<https://player.vimeo.com/video/827318792?h=78a2e50f7f>

## Jira 認証情報の管理

Contrast には、Jira インテグレーションの設定で入力された最新の認証情報が保存されているので、次の新しい接続を簡単に設定できます。最初の設定で入力したユーザ名、API キー(またはパスワード)と Jira の URL が、それ以降の Jira インテグレーション設定でデフォルトの認証情報となります。以降の Jira 設定では、このデフォルトの認証情報がフィールドにあらかじめ入力されますが、必要に応じて値を変更できます。保存されている認証情報を管理して、影響を受ける全ての設定を同時に更新することもできます。

デフォルト設定とは異なる認証情報にするために、1つの設定を作成・編集するには：

1. **ユーザメニュー > 組織の設定 > インテグレーション**にアクセスします。
2. **設定を表示**を選択し、既存の Jira インテグレーションの一覧を表示します。更新するインテグレーション名を選択します。
3. **認証情報を管理**を選択して、Jira 接続の設定情報を表示します。
4. **URL** フィールドでドロップダウンメニューを使用して保存されている認証情報セットを選択するか、**URL**、**ユーザ名**、**API キー(またはパスワード)**を手動で更新します。
5. フィールドを更新したら、**接続をテスト**を選択し、変更した情報で問題なく接続できることを確認します。
6. **保存**を選択します。



### 注記

新しい認証情報を使用する場合、指定した名前でも既存の認証情報セットを上書きするか、別の名前でも新しい認証情報セットとして保存するかを選択する必要があります。

複数の Jira 設定を同時に編集するには：

1. Contrast Web インターフェイスで、**ユーザメニュー > 組織の設定 > インテグレーション**を選択します。
2. Jira インテグレーションの**認証情報を管理**を選択します。
3. **管理 Jira 認証情報**の画面で、ドロップダウンを使用して保存されている認証情報セットを選択します。

4. ユーザ名、API キー(またはパスワード)、Jira の URL を編集します。
5. 編集した認証情報に別の名前を使用する場合は、**名前を変更**を選択します。



#### 注記

認証情報セットを更新すると、そのセットを使用している全ての設定に影響します。

6. **接続をテスト**を選択して、インテグレーションが機能することを確認します。
7. **保存**を選択します。



#### 注記

認証情報セットを更新すると、このセットを使用する全ての設定が更新されます。

### 関連項目

- [Jira とのインテグレーション \(656ページ\)](#)
- [Jira に接続する \(656ページ\)](#)
- [Assess と Jira の設定 \(657ページ\)](#)
- [サーバレスと Jira の設定 \(657ページ\)](#)

## Contrast Maven プラグイン

**Maven** は、Java アプリケーションのビルド、パッケージ化、およびテストを行うビルドツールです。

Contrast Maven プラグインにより、Contrast Assess や Contrast Scan をプロジェクトの Maven ビルドに連携できます。

以下の詳細については、[Contrast Maven Plugin Reference Documentation](#) を参照してください。

- [ゴール](#)
- [使用方法](#)

### ゴール

- **スキャン(scan)** : scan ゴールは、Contrast Scan を使用して Maven プロジェクトのアーティファクトを解析し、静的分析により脆弱性を検出します。
- **インストール(install)** : install ゴールは、統合テストに Contrast Java エージェントを組み込み、Contrast Assess によるランタイムのセキュリティ分析を行います。
- **検証(verify)** : verify ゴールは、統合テスト中に Contrast Assess で検出される脆弱性により、プロジェクトのセキュリティポリシーに違反していないことを検証します(違反が検知された場合はビルドは失敗します)。

### 関連項目

- [Contrast Scan \(499ページ\)](#)
- [Java エージェントのインストール \(59ページ\)](#)

## Microsoft Teams とのインテグレーション

インテグレーションを設定して、Microsoft Teams のインスタンスで Contrast からの通知を受け取るようになります。

Microsoft Teams に接続するために、以下を行います。

1. Microsoft Teams アカウントで自分のチームにアクセスし、通知を受信するチャンネルを選択します。
2. **その他のオプションアイコン**を選択します。
3. メニューから**コネクタ**を選択します。
4. **Incoming Webhook** の**構成**を選択します。
5. 着信 Web フック(Incoming Webhook)の名前を入力して、**作成**をクリックします。
6. Webhook の URL をクリップボードにコピーします。この URL を使用して、Contrast のインテグレーションを設定します。
7. **完了**を選択します。
8. Contrast Web インターフェイスにログインし、**ユーザメニュー**から**組織の設定 > インテグレーション**を選択します。
9. Microsoft Teams の行で、**接続**を選択します。
10. インテグレーション名を入力します。
11. URL のフィールドに、Microsoft Teams からコピーした Webhook の URL をペーストします。
12. 通知を有効にするアプリケーションを選択します。
13. **保存**を選択します。



### 重要

このインテグレーションによる接続は、Contrast で 5 回試行しても応答しない場合、切断されます。

## PagerDuty とのインテグレーション

インテグレーションを設定して、PagerDuty のインシデント管理で Contrast から攻撃の通知を受け取るようにします。

PagerDuty に接続するために、以下を行います。

1. Contrast Web インターフェイスにログインし、**ユーザメニュー**から**組織の設定 > インテグレーション**を選択します。
2. PagerDuty の行で、**接続**を選択します。
3. 設定画面で、インテグレーションの**名前**を入力します。この名前が、Contrast からの通知に表示されます。
4. **メッセージの重大度**のドロップダウンで、警告の深刻度レベルを選択します。デフォルトでは、「Critical」が選択されます。インシデントの深刻度レベルの詳細については、[PagerDuty のドキュメント](#)を参照してください。
5. **インテグレーションキー**を入力します。このフィールドに入力するインテグレーションキーを取得するには、[PagerDuty のドキュメント](#)の手順に従ってください。
6. Contrast から PagerDuty でインシデントを自動生成するアプリケーションを**アプリケーション**で選択します。デフォルトでは、「全てのアプリケーション」が選択されます。
7. 全てのフィールドに入力したら、**接続をテスト**を選択します。この処理は、PagerDuty プロジェクトの数によっては、数分かかる場合があります。接続テストでは、Contrast が PagerDuty のインスタンスに到達できて、メッセージが送信できるかを確認します。

[組織の通知 \(716ページ\)](#)で、PagerDuty と連携させる通知を管理してください。



### 重要

このインテグレーションによる接続は、Contrast で 5 回試行しても応答しない場合、切断されます。

## Solutions Business Manager とのインテグレーション

インテグレーションを設定して、Contrast からの通知を Solutions Business Manager で受け取るようにします。

設定を開始する前に、以下が必要です。

- Solutions Business Manager アカウントの認証情報(ユーザ名とパスワード)
- HTTP 経由で Contrast にアクセス可能な Solutions Business Manager の実行インスタンス
- Contrast に登録されたアプリケーションと関連付けるプロジェクト

Solutions Business Manager に接続するために、以下を行います。

1. ユーザーメニューで、**組織の設定 > インテグレーション**にアクセスします。
2. Solutions Business Manager の行で、**接続**をクリックします。
3. **Serena** への接続ページで、インテグレーションの名前を入力します。この名前は、バグ管理システムに検出結果を送信する際に表示されます。
4. Solutions Business Manager インスタンスに接続するアカウントのユーザ名を入力します。
5. 指定したユーザ名のパスワードを入力します。
6. **ホストフィールド**に、Solutions Business Manager インスタンスへの URL を入力します。
7. Solutions Business Manager インスタンスにマップするアプリケーションを選択します。
8. そのアプリケーションと関連付ける **Solutions Business Manager のプロジェクト ID** を入力します。
9. **接続をテスト**を選択して、通信を確認します。接続テストは、指定したプロジェクトの存在を確認するだけでなく、Contrast がインスタンスと通信し認証されるかを確認します。

## Slack とのインテグレーション

Slack とのインテグレーションにより、Slack 側で Contrast からの通知をアプリ内通知と同様の形式で受け取ることができます。

Slack に接続するために、以下を行います。

1. Slack で、チームの**アプリの管理**画面にアクセスします。
2. **Incoming Webhook** を検索し、Slack に追加します。
3. Contrast からの通知を受信するチャンネルを選択して追加します。
4. **Webhook URL** をコピーします。
5. Contrast Web インターフェイスにログインし、**ユーザーメニュー**から**組織の設定 > インテグレーション**にアクセスします。
6. Slack の行で、**接続**を選択します。
7. インテグレーションの名前を入力して、URL を貼り付けます。
8. 通知を有効にするアプリケーションを選択します。
9. **保存**を選択します。

次の手順でインテグレーションを確認します。

1. **組織の設定 > 通知**を選択します。
2. **インテグレーション**のドロップダウンで、Slack のインテグレーション名を選択します。
3. 通知を受けたい**イベントタイプ**(通知の登録)ごとに、**インテグレーション列**のトグルボタンをクリックします。
4. イベントを発生させて、指定した Slack チャンネルで通知を受信していることを確認してください。



### 重要

このインテグレーションによる接続は、Contrast で 5 回試行しても応答しない場合、切断されます。

## Splunk On-Call(旧 VictorOps)とのインテグレーション

インテグレーションを設定して、VictorOps のインシデント管理で Contrast から攻撃の通知を受け取るようにします。

VictorOps に接続するために、以下を行います。

1. Contrast Web インターフェイスにログインし、**ユーザメニュー**から**組織の設定 > インテグレーション**を選択します。
2. VictorOps の行で、**接続**を選択します。
3. インテグレーションの**名前**を入力します。この名前が、Contrast からの通知に表示されます。
4. ドロップダウンを使用して、警告の**メッセージタイプ**を選択します。デフォルトでは、「Critical」が選択されます。メッセージタイプの詳細については、VictorOps のドキュメントの [Incident Fields](#) を参照してください。
5. 接続の **URL** を入力します。VictorOps の URL は、REST API エンドポイントを使用して生成できます。URL の取得やその他の情報については、VictorOps のドキュメントの [REST endpoint](#) を参照してください。
6. **URL をテストする**を選択します。この処理は、VictorOps プロジェクトの数によっては、数分かかる場合があります。接続テストでは、Contrast が VictorOps のインスタンスに到達でき、指定したユーザがログインできるかを確認します。
7. 接続が確立したら、複数選択フィールドをクリックして、通知を送信する**アプリケーション**を選択します。デフォルトでは、「全てのアプリケーション」が選択されます。



### 重要

このインテグレーションによる接続は、Contrast で 5 回試行しても応答しない場合、切断されます。

## Contrast Visual Studio プラグイン

Visual Studio プラグインを使用すると、Contrast エージェントが組み込まれたアプリケーションの脆弱性情報を Visual Studio IDE から確認できます。

このプラグインによって、脆弱性の影響を受けるコード行が Visual Studio 内で表示され、関連する情報を Contrast Web インターフェイスで確認することができます。この方法により、開発者は開発時にアプリケーションのセキュリティに関するフィードバックを得ることができ、迅速な修正が可能になります。

このプラグインは、Visual Studio のバージョン 2017 (15.0 以降)、2019、2022 をサポートしています。

Visual Studio プラグインをインストールして設定し、使用するには：

1. Visual Studio で、**拡張機能**を選択します。
2. 拡張機能の管理画面で、左ナビゲーションパネルから**オンライン**を選択します。
3. 「Contrast」を検索して、**ダウンロード**を選択します。
4. ダウンロードが完了したら、IDE を再起動します。
5. Visual Studio で、**ツール > オプション**の順に移動します。
6. 検索フィールドに「Contrast Security」と入力して、**Contrast Security - Connection**を選択します。
7. **Contrast Connection** 画面で、適切なフィールドに **Contrast URL**、**ユーザ名**、**サービスキー**、**API キー**および**組織 ID**を入力します。これらの情報は[プロファイル \(478ページ\)](#)で確認できます。





### 注記

API キーは、アクセスしようとする組織に属している必要があります。そうでない場合は、認証エラーが発生します。試行に何度も失敗すると、アカウントがロックされます。

8. **追加**を選択します。Visual Studio が自動的に接続をテストして、Contrast からの組織の取得を試みます。
9. **Organizations** フィールドで組織を選択して、**OK** を選択します。
10. Visual Studio で、**表示 > その他のウィンドウ > Contrast Security Integration** にアクセスします。「Contrast Security Integration」を検索することもできます。このビューには、Contrast からの全ての脆弱性の一覧が表示されます。
11. 一覧を絞り込むには、ページの右上にある**フィルター**アイコンをクリックします。
12. 表示される画面で、サーバ、アプリケーション、深刻度レベル、状態、最後の検出日などの複数のフィルターから選択します。
13. 脆弱性の一覧が表示されない場合は、**Refresh** を選択します。選択済フィルターを全てクリアするには、クリアアイコンをクリックします。これは、サーバおよびアプリケーションの一覧にも適用されます。



### 注記

一覧を更新しても脆弱性が表示されない場合は、脆弱性を絞り込む必要があります。フィルターおよび脆弱性が適切に更新されるよう、**Connection** 設定で異なる組織を選択して、このプロセスを繰り返す必要があります。

14. **Actions** 列で、虫眼鏡アイコンをクリックすると、脆弱性の詳細情報を確認できます。このアイコンを使用すると、Contrast 内の**脆弱性**ページに移動します。

## Contrast Visual Studio Code プラグイン

Visual Studio Code プラグインを使用すると、機能テスト中に Contrast でセキュリティの問題が検出されたときに、検査対象のアプリケーションの脆弱性情報を Visual Studio Code 環境から確認できます。

このプラグインによって、アプリケーションで検出された全ての脆弱性の概要に加え、脆弱性にさらされている HTTP リクエストなど、各脆弱性の詳細情報が表示されます。

このプラグインは Visual Studio Code のバージョン 1.42.1 以降をサポートしています。

Visual Studio Code プラグインをインストールして設定し、使用するには：

1. Visual Studio Code で、**拡張機能**の画面にアクセスし、「Contrast Security」を検索します。
2. **インストール**を選択します。インストールが完了したら、Visual Studio Code を再起動します。
3. **Contrast Security** のビューから**設定**アイコンを選択して、Contrast アカウントを認証します。
4. **ワークスペース**を選択し、**API キー**、**組織 ID**、**Contrast URL**、**認証ヘッダ**を各フィールドに入力します。これらの情報は**プロファイル (478ページ)**で確認できます。
5. **Test Contrast connection** アイコンを選択して、認証情報を確認します。接続に成功したか、または無効な認証情報についてのメッセージが表示されます。
6. **リフレッシュ**アイコンを選択すると、脆弱性情報が更新されます。**CONTRAST SECURITY** 下に、**深刻度**別にグループ化された脆弱性が**ステータス**順に表示されます。脆弱性を選択すると、**概要**、**詳細**、**HTTP 情報**、**修正方法**などの詳細が表示されます。また、最後に脆弱性が検出された日時や現在のステータスも表示されます。脆弱性の詳細は、出力のコードエディターに表示されます。



## ヒント

プラグインを使用すると、以下の項目で脆弱性を絞り込みます。

- 脆弱性メタデータ：
  - アプリケーション名
  - ステータス(報告済、問題無し、修復済など)
  - 環境(開発、テスト、本番)
  - タグ(脆弱性に適用されたカスタムラベル)
  - 検出日(特に、最初と最後の検出日)
- セッションメタデータ：
  - コミット
  - コミットハッシュ
  - ブランチ名
  - Git タグ
  - リポジトリ
  - テスト実行
  - バージョン
  - ビルド番号

例えば、ユーザは特定の機能ブランチ(ブランチ名)で検出され、自分(コミット)が直接コミットした脆弱性のみを表示するよう選択して、別の機能ブランチで別の開発者によってもたらされた脆弱性を除外することができます。

他のユーザは、脆弱性を絞り込んで、自分のセキュリティチームによってブロックされた、特定のビルド(ビルド番号)からの結果のみを表示することができます。マージされた機能ブランチをデプロイする前に解決する必要がある脆弱性のサブセットを直ちに特定できます。

## Contrast Visual Studio for Mac プラグイン

Visual Studio for Mac プラグインを使用すると、Contrast エージェントが組み込まれたアプリケーションの脆弱性情報を Visual Studio for Mac IDE から確認できます。

このプラグインにより、コード行が表示され、ユーザは Contrast Security 用のウィンドウで詳細を確認できます。この方法により、開発者はアプリケーションのセキュリティに関するフィードバックを開発時に取得でき、迅速な修復につながります。

このプラグインは Visual Studio for Mac のバージョン 8.3.0 以降をサポートしています。

Visual Studio for Mac プラグインをインストールして設定し、使用するには：

- Contrast の配布リポジトリのリリースから、Visual Studio for Mac プラグインのファイル(.mpack)をダウンロードします。
- Visual Studio for Mac で、**Visual Studio > 拡張機能**にアクセスします。
- ファイルからインストール...**をクリックして、ダウンロードした.mpack ファイルを選択します。プラグインのインストールを行い、Visual Studio for Mac を再起動します。
- 表示 > その他のウィンドウ > Contrast** を選択します。**設定アイコン**を選択して、**Contrast URL**、**ユーザ名**、**サービスキー**、**API キー**および**組織 ID**を各フィールドに入力します。これらの情報は**プロファイル (478ページ)**で確認できます。
- Test connection** を選択して、Contrast への接続を確認します。接続できたら、**Save** を選択します。
- プラグインをインストールしたら、**表示 > その他のウィンドウ > Contrast**に戻り、虫眼鏡アイコンを選択して、脆弱性を参照したいアプリケーションを選択します。これにより、選択したアプリ

ケーションに対して Contrast で検出された脆弱性が読み込まれます。脆弱性の一覧が表示されない場合は、リフレッシュアイコンを選択します。脆弱性が深刻度順、ステータスなどの情報と一緒に表示されます。

脆弱性を選択すると、その概要や詳細情報を確認できます。**General Information** のセクションには、深刻度、アプリケーション、ステータス、履歴などがあります。**Details** セクションには、その脆弱性の詳細や備考、アクティビティなど、Contrast から取得された情報があります。

選択済フィルターを全てクリアするには、ほうきのアイコンを選択します。この方法でサーバおよびアプリケーションの一覧も表示できます。

## 管理ガイド

ユーザにはそれぞれ異なる [ロールや権限 \(817ページ\)](#) があり、Contrast でのアクセスレベルが異なります。この異なるアクセスレベルにより、企業内の様々なユーザやチームが、それぞれの職務に応じて Contrast を最適に利用することができます。

- [ルールとポリシーの管理 : \(668ページ\)](#) RulesAdmin ロール(組織のルール管理者)により、ポリシーの作成と編集ができます。Edit ロール(組織の編集者)では、アプリケーションを追加したり、スコアや通知などのコンテンツ情報を管理できます。
- [組織の管理 : \(701ページ\)](#) Admin ロール(組織管理者)は、特定の組織の設定を構成できます。
- [システム管理 : \(741ページ\)](#) オンプレミス版のお客様の場合、SuperAdmin ロール(スーパー管理者)が、Contrast のインストール、設定、管理をシステムレベルで行います。また、ServerAdmin ロール(サーバ管理者)や SystemAdmin ロール(システム管理者)もシステム管理業務をサポートします。

### ルールとポリシーの管理

Contrast でアプリケーションをメンテナンスするには、実行する操作に応じて異なるロールや権限が必要です。

RulesAdmin 権限のあるユーザで、[ユーザメニューのポリシーの管理](#)を選択します。

| ルール                                                                       | 深刻度 | 説明                                                                        | 開発環境 | QA  | 本番環境 |
|---------------------------------------------------------------------------|-----|---------------------------------------------------------------------------|------|-----|------|
| ASPXのトレース機能の有効化<br>.NET Framework                                         | 注意  | 単一のASPXページに設定しているASP.NETのトレース機能によって、技術情報をアプリケーションで誤って公開していないことを確認します。     | 77   | 77  | 77   |
| Cache-Controlヘッダの無効化<br>.NET Framework                                    | 中   | ブラウザのキャッシュを経由して機密情報が漏洩するのを防ぐCache-Controlヘッダが、アプリケーションで無効にされていないことを確認します。 | 77   | 77  | 77   |
| Cookieのsecure属性が無効なアプリケーション<br>Java                                       | 中   | Cookieに「secure」属性が付与されていることを確認します。                                        | 75   | 75  | 75   |
| DynamoDBのNoSQLインジェクション<br>Java, Node                                      | 重大  | 動的データベースクエリで、信頼できないデータが使用されていないことを確認します。                                  | 86   | 86  | 86   |
| ELインジェクション<br>Java                                                        | 高   | JSPの式言語(EL)の評価で、信頼できないデータが使用されていないことを確認します。                               | 75   | 75  | 75   |
| HQLインジェクション<br>Java                                                       | 重大  | 動的に構築されるHibernateクエリに信頼できないデータが追加されていないことを確認します。                          | 75   | 75  | 75   |
| HttpOnly属性がないセッションCookie<br>.NET Framework, .NET Core, Java, Node, Python | 中   | セッションCookieにHttpOnly属性が付与されていることを確認します。                                   | 178  | 178 | 178  |
| HttpOnly属性が無効なCookie<br>.NET Framework                                    | 注意  | アプリケーションで発行されるCookieのHttpOnly属性が無効にされていないことを確認します。                        | 77   | 77  | 77   |
| LDAPインジェクション<br>.NET Framework, .NET Core, Java                           | 高   | 動的LDAPクエリで、信頼できないデータが使用されていないことを確認します。                                    | 153  | 153 | 153  |
| NoSQLインジェクション<br>.NET Framework, .NET Core, Java, Node, Python, Ruby      | 重大  | 動的データベースクエリで、信頼できないデータが使用されていないことを確認します。                                  | 181  | 181 | 181  |
| OSコマンドインジェクション<br>全てのアプリケーション言語                                           | 高   | オペレーティングシステムに送信されるコマンドで、信頼できないデータが使用されていないことを確認します。                       | 184  | 184 | 184  |

管理できる項目は、以下の通りです。

- [Assess ルール \(670ページ\)](#)
- [セキュリティ制御 \(671ページ\)](#)
- [脆弱性ポリシー \(674ページ\)](#)
- [Protect ルールの設定 \(681ページ\)](#)
- [CVE シールド \(684ページ\)](#)
- [仮想パッチ \(689ページ\)](#)
- [ログエンハンサー \(690ページ\)](#)
- [IP アドレスのブロック/許可 \(697ページ\)](#)
- [ソース名の編集 \(698ページ\)](#)
- [アプリケーションの例外 \(692ページ\)](#)
- [コンプライアンスポリシー \(695ページ\)](#)
- [ライブラリポリシー \(698ページ\)](#)
- [機密データ \(700ページ\)](#)

RulesAdmin 権限があるユーザは、次の操作も実行できます。

- [エージェントのインストールと設定 \(35ページ\)](#)

- [Protect の有効化 \(702ページ\)](#)
- [保留中の脆弱性ステータスの変更の承認/拒否 \(601ページ\)](#)
- [通知の有効化 \(701ページ\)](#)
- [デフォルトの評価方法の設定 \(719ページ\)](#)

## Assess ルールの設定

適用されている全てのルールの一覧を表示するには、**アプリケーション > アプリケーション名 > ポリシー > ASSESS** を選択するか、ユーザメニューで **ポリシーの管理 > Assess ルール** を選択します。各ルールには、深刻度と説明があり、そのルールがどの環境に適用されているかも表示されます。

また、[組織のデフォルトの Assess ルール \(670ページ\)](#) も設定できます。

### 設定を行う前に

- 組織管理者(Admin ロール)またはルール管理者(Rules Admin ロール)であることを確認してください。
- ログインして、該当する組織を選択します。

### 手順

Assess ルールの適用と更新：

1. アプリケーションの特定の環境に Assess ルールを適用するには：
  - a. **アプリケーション** ページでルールの一覧を表示している場合は、トグルボタンを使用して各環境の各ルールをオンまたはオフにします。また、複数のルールに変更を適用するには、左側の列のチェックボックスを使用して複数のルールを選択し、**モードを変更** を選択します。表示される画面で、各環境のルールのオンとオフを切り替え、**保存** を選択します。
  - b. または、**ポリシーの管理 > Assess ルール** の場合は、ルールを選択すると、そのルールに関連付けられているアプリケーションの一覧が表示されます。トグルボタンを使用して、アプリケーションごとにルールをオンまたはオフにします。
2. 個々の Assess ルールの設定を更新するには：
  - a. **ポリシー管理** にて、ルール名を選択すると、そのルールに関連付けられているアプリケーションの一覧が表示されます。
  - b. 1 つまたは複数のアプリケーションを選択するには、各アプリケーションの横にあるチェックボックスをオンにします。  
全てのアプリケーションを選択する場合は、**アプリケーション** のチェックボックスを選択します。
  - c. 右上にある **設定アイコン** ( \* ) を選択します。
  - d. 表示される画面で、このルールの対象となる脆弱性の **可能性**、**影響度**、**信頼度** を選択します。
  - e. 必要に応じて **上書き** チェックボックスをオンにして、設定を保存後にこれらのフィールドを更新するオプションを有効にします。
  - f. **リスクの説明** フィールドには、この脆弱性がどんなリスクであるかの追加情報を入力します。また、修正方法として **推奨** する情報を入力することもできます。
  - g. **参照** フィールドには、ルールに関する詳細な情報として、特定の脆弱性に関する外部参照へのリンクを入力します。
  - h. **保存** を選択します。

## 組織の Assess ルールの設定

アプリケーションにエージェントを追加・設定したり、新しい組織を作成すると、デフォルトの Assess ルールセットが適用されます。

組織レベルで Assess ルールのデフォルト設定を変更するには、以下の手順を実行してください。ここでの設定は、Contrast の組織に新規に追加される全てのアプリケーションに適用され、組織内の既存のアプリケーションには影響しません。

## 設定を行う前に

- 組織管理者(Admin ロール)またはルール管理者(Rules Admin ロール)であることを確認してください。
- ログインして、該当する組織を選択します。

## 手順

- ユーザメニューから、**ポリシーの管理**を選択します。
- デフォルトポリシーを設定**を選択します。



- フィルターで**全て**を選択します。



- 各 Assess ルールで、トグルボタンを使用して環境ごとに各ルールをオンまたはオフにします。

| ルール                     | 深刻度 | 説明                                                                   | 開発環境                                | QA                                  | 本番環境                                |
|-------------------------|-----|----------------------------------------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| ASPXのトレース機能の有効化<br>.NET | 注意  | 単一のASPXページに設定しているASPNETのトレース機能によって、技術情報をアプリケーションで誤って公開していないことを確認します。 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

## セキュリティ制御

セキュリティ制御とは、コード内でデータを安全に使用するためのメソッドです。Contrast で認識される組み込みのセキュリティ制御を通過した情報は信頼できる情報とされます。Contrast は、サードパーティライブラリの多くのメソッドを監視して、データフローが安全かどうかを判断します。

組織によっては、Contrast で認識されない独自のセキュリティ制御の構築が必要な場合があります。その場合は、カスタムメソッドを Contrast に認識させるためにセキュリティ制御を作成します。カスタムのセキュリティ制御を追加すると、Contrast はより正確な結果を報告します。

## セキュリティ制御の種類

- 入力バリデーション**：バリデーションは、アプリケーションの他の部分にデータが渡される前に、適切に形成され、フォーマットされたデータのみが入力として受け入れられることを確認するためのメソッドです。入力フィールドで特定の文字を受け入れたり拒否したりできるように定義されます。入力バリデータは、SQLi、XSS、およびその他の入力検証に関連する攻撃を防ぐための主要な方法です。

- **無害化**：入力を検証する代わりに、データベースなどのアプリケーションの他の部分に渡される前に、入力を安全にレンダリングします。例えば、潜在的なインジェクション攻撃で使用される可能性のある一重引用符を取り、それを二重引用符に変更します。

## セキュリティ制御を行うタイミング

アプリケーションで使用しているメソッド、クラス、ライブラリを Contrast が正確に把握できない場合にセキュリティ制御を作成し、アプリケーションを入力検証の問題(無害化や入力バリデーション)から守ります。

アプリケーションで使用するバリデーションや無害化が分かっている場合は、それらを手動で追加したり、Contrast が自動的に検出した推奨のセキュリティ制御をアプリケーションに適用するセキュリティ制御として追加することができます。

セキュリティ制御を追加して有効にすると、Contrast Assess で、そのセキュリティ制御で緩和するように定義した入力に関する脆弱性が表示されなくなります。セキュリティ制御を適切な脆弱性ルールに適用することが非常に重要です。

## セキュリティ制御の影響

セキュリティ制御は、指定されたルールの脆弱性と検出に影響を与えます。入力バリデーションと無害化は、通常、特定の種類のデータ、特定のフィールドやページ、または特定のアプリケーションのために定義・適用されます。すべてのルールに対してセキュリティ制御を有効にすると、検知漏れとなる可能性があります。

セキュリティ制御の使用は、慎重に行ってください。セキュリティ制御の適用は、特定のルールにのみに必要な場合があります。例えば、バリデーションや無害化によって XSS からアプリケーションを保護できても、SQL インジェクションに対しては効果的ではない可能性があります。すべてのルールにセキュリティ制御を適用すると、SQLi の脆弱性が非表示になり、結果として検知漏れとなる可能性があります。

セキュリティ制御は、さまざまな攻撃からアプリケーションを保護することを保証するためのものであるべきです。

## セキュリティ制御の管理ロール

RulesAdmin 以上の組織ロールが割り当てられたユーザーのみが、セキュリティ制御を表示または変更できます。

## サポートされる言語

セキュリティ制御が適用される言語は、Java、.NET Framework、.NET Core のみです。

## セキュリティ制御の例

安全でない暗号化アルゴリズムの使用について報告されている `com.Acme.OldSecurity` というクラス内に `DoLegacySecurity()` というメソッドがあると仮定します。セキュリティ制御を作成し、次のメソッドシグネチャを指定します。

```
com.Acme.OldSecurity.DoLegacySecurity(java.lang.String*)
```



### ポリシーの管理

ASSESS

- Assessルール
- セキュリティ制御
- 脆弱性の管理

PROTECT

- Protectルール
- CVEシールド
- 仮想パッチ
- ログエンハンサー
- IP管理

概要

- アプリケーションの例外
- コンプライアンスポリシー
- ライブラリポリシー
- 機密データ

#### Add Security Control

名前  
このセキュリティ制御名を入力

言語  
Java

種類  
Input Validator

API  
com.Acme.OldSecurity.DoLegacySecurity(java.lang.String\*)

対象ルール  
未検証のリダイレクト

キャンセル Add

この例では、`Java.lang.String*`がマークされたパラメータで検査対象となります。

セキュリティ制御の作成時には、末尾のパラメータ定義や余分な文字が含まれないように注意します。

Contrast では、検出された脆弱性のスタックトレースとこのメソッドシグネチャが照合され、マッチする脆弱性が非表示になります。

## セキュリティ制御の追加、編集、削除

セキュリティ制御が適用される言語は、Java、.NET Framework、.NET Core のみです。

### 手順

1. ユーザーメニュー > ポリシーの管理を選択し、**セキュリティ制御**を選択します。  
既にセキュリティ制御がある場合は、セキュリティ制御の一覧に表示されます。
2. 編集する場合は既存のセキュリティ制御の名前を選択します。新規に作成する場合は、**セキュリティ制御を追加**を選択します。
3. 表示される画面で、以下の項目を入力します。
  - **名前**
  - **言語** : Java、.NET Framework、.NET Core から選択します。
  - **種類** : 以下のいずれかのメソッドを選択します。
    - **入力バリデーション**(Input Validator)は、ユーザ入力を受け付けて、安全でないデータを受信した場合に修正処理を行います。
    - **無害化**(Sanitizer)は、渡されたデータをクリーンにして、どのインタプリタでも安全に使用できるようにします。無害化によって、ある種類の攻撃を防ぐことができても、他の種類の攻撃が防げるわけではありません。
  - **API** : API を指定する際は、以下の規約を考慮してください。
    - Java の場合には、メソッド名とパラメータを含める必要があります。完全修飾型を使用し、`java.lang.String` パラメータ(boolean、int、long、short double、float などでない)のみを対象とします。
    - **.NET Framework および .NET Core** の場合 :
      - 戻り値の型(または void)、メソッド名、パラメータを含めます。完全修飾型を使用し、`System.String` パラメータのみを対象とします。
      - パラメータ間にスペースが無いことを確認してください。
      - バリデーションまたは無害化されるパラメータにアスタリスク(\*)を付けます。
    - **対象ルール** : 全ての脆弱性ルールを選択することも、個別の脆弱性ルールを 1 つ以上選択することもできます。

4. **保存**を選択して新しいセキュリティ制御を作成します。既存のセキュリティ制御を編集する場合は、このパネルから**削除**アイコンを使用してセキュリティ制御を削除することもできます。
5. 表の下部に、Contrast が検出した潜在的なセキュリティ制御の候補が**推奨**として、クラスとメソッドとともに表示されます(このセクションは、ヘッダ行のキャレットをクリックして非表示にできません)。

セキュリティ制御が初めて自動的に検出された場合は、該当するアプリケーションの View 権限以上を持つ全てのユーザに通知されます。

API にカーソルを合わせて、この推奨が検出された場所を確認します。また、必要に応じてアプリケーション名を選択し、そのアプリケーションのコンテキストで脆弱性を確認します。

推奨されるセキュリティ制御の行の端にある**プラス記号**のアイコン(+)を使用して、推奨を新しいセキュリティ制御として追加し、上の表に含めます。追加する前に、名前、API、種類フィールドを直接編集できます。セキュリティ制御の追加後、名前を選択し、セキュリティ制御が正しいアプリケーションルールに適用されることを確認します。

推奨を削除するには、**ゴミ箱**アイコン(🗑️)を使用します。Contrast からの推奨は繰り返されないもので、一度削除するとその API が再度推奨されることはありません。過去の推奨を表示したり、戻す方法はありません。



### 注記

サーバの再起動が必要な場合があります。選択した内容によって、影響を受けるサーバの一覧が表示されます。

## 特定の脆弱性に対応したセキュリティ制御の作成

タグイベントを使用して、特定の脆弱性のコンテキストでセキュリティ制御を作成することもできます。

Contrast によって脆弱性のランタイムのデータフローがキャプチャされた場合、**脆弱性 > 脆弱性の名前 > 詳細**を選択して、その脆弱性の詳細情報を確認できます。検出された潜在的なセキュリティ制御によってタグイベントがトリガーされ、それが深刻度の低い(緑色の)イベントとして表示されます。イベントを展開すると、**セキュリティ制御の追加**を選択できます。

また、「内部のセキュリティ制御を通過」という理由で脆弱性を**問題無し**とマークした場合は、そのセキュリティ制御をその時点で定義できます。

## 脆弱性の管理ポリシー

脆弱性ポリシーを使用して、組織の RulesAdmin または Admin ロールのある管理者が、ポリシーのトリガー時に脆弱性のステータスを変更したり、確認のためにフラグを立てる基準を定義することができます。ポリシーを定義する基準には、脆弱性のルール、深刻度、アプリケーション、ルートなどを指定できます。

脆弱性ポリシーによって、どの脆弱性に注意が必要であるか、またどの脆弱性が修復済みでクローズしたと見なされているかをより正確に把握できます。自動検証ポリシーと違反ポリシーを設定できます。

脆弱性がこれらのポリシーに違反する場合、**アプリケーション内で通知 (717ページ)**するように設定できます。管理者には、Contrast アプリケーション内と E メール の両方で違反が通知されます。

## 自動検証ポリシーのタイプ

**自動検証 (676ページ)**ポリシーは、特定の条件を満たす脆弱性のステータスを自動的に**修復済 - 自動検証**に変更します。脆弱性の修正・検証後のステータス変更を手動で行うことに依存するのではなく、注意が必要な脆弱性のステータスをより正確に認識したい場合、自動検証ポリシーは便利です。

自動検証ポリシーのタイプには、セッションベース、ルートベース、または時間ベースがあります。

- **セッションベースの自動検証(推奨)**：エージェントの設定ファイルに指定したメタデータ値の組み合わせによって、セッションを定義します。テストランの最後に Contrast API を呼び出すことで、セッション終了のタイミングを制御します。  
このタイプの自動検証には、自動化されたテストスイートが必要です。
- **ルートベースの自動検証**：エージェントの設定ファイルに指定したメタデータ値の組み合わせによって、セッションを定義します。セッションベースの自動検証を使用できない場合は、この自動検証タイプを使用して下さい。  
このタイプの自動検証には、自動化されたテストスイートが必要です。
- **時間ベースの自動検証**：指定された期間内でアプリケーションの全てのルートを疎通できることが確実な場合は、この自動検証タイプを使用して下さい。  
このタイプの自動検証では、自動テストまたは手動テストを利用できます。

## 自動検証の動き方

- Contrast で、ある脆弱性が 2 つの異なるセッションに渡って同じルートで検出されない場合、この脆弱性は**修復済 - 自動検証**というステータスになります。2 つのセッションで全く同じセッションメタデータ値が報告された場合、2 つのセッションは 1 つの単独セッションとして見なされます。  
定義した値に応じて、各エージェントの実行を単独のセッションの 1 部にすることもできますし、各エージェントの実行に独自のセッション情報を持たせることもできます。Contrast を CI/CD パイプラインに組み込んでいる場合は、アプリケーションの新しいバージョンをデプロイするたびに、一意であるセッションメタデータのキーと値のペアを少なくとも 1 つ送信して下さい。例えば、コミットハッシュ(commitHash)やビルド番号(buildNumber)、バージョン(version)などのメタデータは、アプリケーションのデプロイごとに更新される場合が多いため、これらの値がエージェントから送信されるように設定すると良いです。
- Contrast で以前に**修復済 - 自動検証**のステータスにされた脆弱性が、同じルートを実行した際に再度検出された場合は、その脆弱性のステータスは**報告済**に変わります。その場合、脆弱性の詳細ページにある「アクティビティ」タブに情報が更新されます。
- 自動検証ポリシーを無効または削除した後に、Contrast で以前に**修復済 - 自動検証**のステータスにされた脆弱性が、同じルートを疎通した際に再度検出された場合は、その脆弱性のステータスは**報告済**に変わります。その場合、脆弱性の詳細ページにある「アクティビティ」タブに情報が更新されます。

## セッションベースおよびルートベースの自動検証のためのセッションメタデータ

セッションベースまたはルートベースの脆弱性ポリシーには、エージェントの設定ファイルに**セッションメタデータを追加 (491ページ)**して下さい。

- 一意のセッションメタデータを指定することによって、検出結果のベースラインができ、ルート比較に基づいて脆弱性が修復されたかどうかを検証できるようになります。
- テストラン(testRun)のセッションメタデータフィールドを使用すると、テスト実行中にエージェントやアプリケーションを何度も再起動しても、1 つのテスト実行内でのルートと脆弱性を確実に追跡できます。  
Contrast では、一意のメタデータのキーと値のペアごとに、一意のセッション ID が作成されます。この方法でセッションメタデータを使用すれば、複数のテスト実行が 1 つのテストセッションとして統合されます。この操作は、同じルートで異なるコードパスをテストする際に便利です。
- コミットハッシュ(commitHash)やビルド番号(buildNumber)、バージョン(version)などのメタデータは、アプリケーションのデプロイごとに値が更新される場合が多いため、利用すると便利です。

## 違反ポリシー

**違反ポリシー (679ページ)**は、脆弱性が特定の基準に一致した場合に、違反の通知をトリガーします。トリガーされると、脆弱性一覧で脆弱性が赤字で表示されます。脆弱性のフィルタを使用すると、ポリシー違反の脆弱性のみを表示できます。



## ポリシーのトリガー

以下のトリガータイプが、脆弱性ポリシーに有効です。

- セッションベース(推奨)**：セッション中の特定のルートで、脆弱性が検出された場合、または検出されなかった場合に、自動検証ポリシーをトリガーします。このトリガーを使用する場合は、Contrast API を使用してセッションを終了させます。この機能では、テストランの結果をすぐに取得できるよう、セッションの終了タイミングを定義できます。
- セッションベース(推奨)**：セッション中の特定のルートで、脆弱性が検出された場合、または検出されなかった場合に、自動検証ポリシーをトリガーします。このトリガーを使用する場合は、Contrast API を使用してセッションを終了させます。この機能では、テストランの結果をすぐに取得できるよう、セッションの終了タイミングを定義できます。
- 時間**：指定した日数が経過すると、違反ポリシーまたは自動検証ポリシーがトリガーされます。

## 環境

最適な結果を得るためには、テストの自動化を行っている環境に脆弱性ポリシーを適用するよう設定します。複数のサーバで同じアプリケーションを実行している場合は、各サーバが開発、QA または本番環境用に設定されていることを確認してください。

## 複数ポリシーの処理

複数のポリシーが同じ脆弱性に影響を与える場合、以下のルールによって Contrast の処理が決定されます。

- 自動検証ポリシーは、違反ポリシーよりも優先されます。例えば、最初に自動検証の期限が適用された場合、脆弱性はクローズされフラグは立てられません。
- 2つの時間ベースのトリガーが影響する場合は、期限が最も近い処理が先に適用されます。例えば、最初に違反期限が適用された場合、脆弱性にフラグが立てられ、後の期限が適用された時に脆弱性が自動検証されます。

## 脆弱性の自動検証ポリシーの設定

[脆弱性の自動検証ポリシー \(674ページ\)](#)の条件を満たす脆弱性のステータスを自動的に修復済 - 自動検証に変更します。自動検証ポリシーには、セッションベース、ルートベース、または時間ベースを設定できます。

ポリシーを追加すると、デフォルトでポリシーが有効になります。ポリシーの有効/無効は、自動検証タブの「有効」の列で切り替えることができます。

| 自動検証                |        | 違反       |       |           |                                     |    |  |
|---------------------|--------|----------|-------|-----------|-------------------------------------|----|--|
| ポリシーを検索             |        |          |       | + ポリシーを追加 |                                     |    |  |
| ポリシー                | 脆弱性ルール | アプリケーション | 説明    | 環境        | 有効                                  |    |  |
| test                | 注意     | 全て       |       | 全て        | <input checked="" type="checkbox"/> | 🗑️ |  |
| Simon Test<br>時間ベース | 全て     | WebGoat7 | 7日の期間 | 全て        | <input type="checkbox"/>            | 🗑️ |  |

## 開始する前に

- 組織の RulesAdmin または Admin ロールが必要です。
- Contrast のバージョン 3.7.2 以降を使用してください。
- Contrast エージェントでサポート対象となる最小バージョン以降を使用していることを確認してください。
  - .NET Framework 20.4.1
  - .NET Core 1.0
  - Java 3.7.3.14895
  - Node.js 2.11.0
  - Python 3.4.0
- [サポート対象のフレームワーク \(679ページ\)](#)を使用していることを確認してください。
- セッションベースまたはルートベースの自動検証を使用する場合は、エージェントの設定ファイルに一意の[セッションメタデータを設定 \(491ページ\)](#)して下さい(例、コミットハッシュ、ビルド番号、バージョンなど)。

## 自動検証ポリシーの設定

1. ユーザメニューから、**ポリシーの管理**を選択します。
2. **脆弱性の管理**を選択します。
3. 脆弱性ポリシーにある**自動検証**タブを選択します。
4. **ポリシーを追加**を選択します。
5. **名前**に、ポリシーの名前を入力します。
6. **脆弱性ルール**に、ポリシーに関連付ける 1 つ以上の深刻度や Assess ルールを選択します。
7. **アプリケーション**に、ポリシーに関連付ける 1 つ以上の重要性やアプリケーションを選択します。具体的な重要性やアプリケーションを検索する場合、「アプリケーション」欄に値を入力してみてください。
8. **環境**には、ポリシーを適用する 1 つ以上のサーバ環境を選択します(全ての環境、開発環境、QA、本番環境)。
9. **トリガー**では、ポリシーに使用するトリガーの種類を選択します(トリガーのタイプを 1 つまたは両方選択)。
  - 時間ベースのトリガーを設定するには、**指定日数以降に全ての脆弱性を自動検証によって修復済のステータスにする**を選択し、脆弱性ポリシーが自動検証されたステータスになるまでの日数を選択します。  
このトリガーは、選択した期間内に脆弱性を修正し、全てのルートを疎通できることが確実な場合に便利です。Contrast で再びその脆弱性が確認された場合、その脆弱性は再オープンされます。



### ヒント

時間ベースの自動検証を、セッションベースまたはルートベースの自動検証と併用することで、ビルドごとにルートが大きく変化する状況を検知できます。例：

- 新しいルートを追加して、古いルートを削除するなど、コードの大幅なリファクタリングを行った場合。
- ルートが有効ではなくなり、疎通されなくなった場合。

- セッションベースまたはルートベースの自動検証を設定するには：
  - a. **ルートまたはセッションに基づく自動検証**を選択します。  
セッションまたはルートベースの自動検証は、時間ベースのトリガーよりも優先されます。
  - b. 以下のオプションのいずれかひとつを選択します(両方のオプションを同時に使用することはできません)。
    - **セッションベースの自動検証(推奨)**：このタイプの自動検証ポリシーでは、セッションの終了タイミングを定義でき、ビルドの可否も判断できるなど、テストランの結果をすぐに取得できます。自動検証として推奨されるのは、セッションベースの自動検証です。この

オプションを選択する場合、テストランの最後に Contrast API を呼び出すことで、セッションを終了します。

- **ルートベースの自動検証**：セッションベースの自動検証を使用できない場合に、ルートベースの自動検証の使用を検討します。この場合、エージェントに設定したセッションメタデータによって、セッションが定義されます。  
ルートベースのトリガーは、ルートが識別できる特定のテクノロジーに対してのみ機能しません。

10. **保存**を選択します。

### セッションベースの自動検証のためのテストランの設定

セッションベースの自動検証は、自動検証の方法として推奨されますが、テストランの最後に Contrast SBAVRouteSession API を呼び出す必要があります。以下に、セッションをクローズする例をいくつか示します。

認証ヘッダーと API キーを検索するには、Contrast Web インターフェイスにログインし、ユーザーメニューより**ユーザの設定**を選択します。

- セッション ID とアプリケーション ID でセッションを終了する場合。以下の例のようなコマンドを使用して下さい。

```
curl --location --request POST 'https://<HOST>/Contrast/api/ng/organizations/<ORG-UUID>/agent-sessions/sbav' \
--header 'Authorization: <Your-Auth-Header-Value>' \
--header 'API-Key: <API-KEY>' \
--header 'Content-Type: application/json' \
--data-raw '{
  "sessionId": "0",
  "appId": "5b4960b3-a111-4f2a-bf24-7367be7c8302"
}'
```

- セッション ID、アプリケーション名、アプリケーション言語でセッションを終了する場合。以下の例のようなコマンドを使用して下さい。

```
curl --location --request POST 'https://<HOST>/Contrast/api/ng/organizations/<ORG-UUID>/agent-sessions/sbav' \
--header 'Authorization: <Your-Auth-Header-Value>' \
--header 'API-Key: <API-KEY>' \
--header 'Content-Type: application/json' \
--data-raw '{
  "sessionId": "0",
  "appName": "FakeRubyApp",
  "appLanguage": "JAVA"
}'
```

- アプリケーションに設定されているメタデータのキーと値のペア、およびアプリケーション ID でセッションを終了する場合。以下の例のようなコマンドを使用して下さい。

```
curl --location --request POST 'https://<HOST>/Contrast/api/ng/organizations/<ORG-UUID>/agent-sessions/sbav' \
--header 'Authorization: <Your-Auth-Header-Value>' \
--header 'API-Key: <API-KEY>' \
--header 'Content-Type: application/json' \
--data-raw '{
  "appId": "abc",
  "metadata": [
    { "label": "developer", "value": "carlos" },
    { "label": "repo", "value": "ts" }
  ]
}'
```

- アプリケーションに設定されているメタデータのキーと値のペア、およびアプリケーション名とアプリケーション言語でセッションを終了する場合。以下の例のようなコマンドを使用して下さい。

```
curl --location --request POST 'https://<HOST>/Contrast/api/ng/organizations/<ORG-UUID>/agent-sessions/sbav' \  
--header 'Authorization: <Your-Auth-Header-Value>' \  
--header 'API-Key: <API-KEY>' \  
--header 'Content-Type: application/json' \  
--data-raw '{  
  "appName": "FakeJavaApp",  
  "appLanguage": "JAVA",  
  "metadata": [  
    {"label": "developer", "value": "carlos"},  
    {"label": "repo", "value": "ts"}  
  ]  
'
```

## 脆弱性ポリシーの更新

1. ユーザメニューから、**ポリシーの管理**を選択します。
2. **脆弱性の管理**を選択します。
3. 脆弱性ポリシーにある**自動検証**タブを選択します。
4. 自動検証タブで、ポリシーを選択します。
5. 必要に応じて、値を更新します。
6. **更新**を選択します。

## 自動検証のサポート対象フレームワーク

次のフレームワークが、自動検証ポリシーに対応しています。

- **Java** : Jersey 2、Spring MVC 4、Struts 1、Struts 2、Servlet(ベータ)
- **.NET Framework** : ASP.NET MVC(バージョン 4 と 5)、WebForms、WebAPI、WCF
- **.NET Core** : ASP.NET Core MVC(バージョン 2.1、2.2、3.0、3.1)、ASP.NET Core Razor Pages(バージョン 2.1、2.2、3.0、3.1)
- **Node.js** : Express、Hapi 17 以降、Koa、Kraken
- **Ruby** : Rails、Sinatra
- **Python**: Django、Pyramid、Flask

## 脆弱性の違反ポリシーの設定

違反ポリシーは、脆弱性がポリシーに違反していることをマークするものです。このポリシーが適用されると、脆弱性の一覧で違反が赤字で表示されます。

ポリシーを追加すると、デフォルトでポリシーが有効になります。ポリシーの有効/無効は、違反タブの「有効」の列で切り替えることができます。

| 自動検証                                         |         | 違反       |        |                                          |                                     |                                  |  |
|----------------------------------------------|---------|----------|--------|------------------------------------------|-------------------------------------|----------------------------------|--|
| <input type="text" value="ポリシーを検索"/>         |         |          |        | <input type="button" value="+ ポリシーを追加"/> |                                     |                                  |  |
| ポリシー                                         | 脆弱性ルール  | アプリケーション | 説明     | 環境                                       | 有効                                  |                                  |  |
| All must be remediated in 28 days<br>時間ベース   | 全て      | 全て       | 28日の期間 | 全て                                       | <input checked="" type="checkbox"/> | <input type="button" value="🗑"/> |  |
| All High must be remediated in o...<br>時間ベース | 重大<br>高 | 全て       | 7日の期間  | 全て                                       | <input type="checkbox"/>            | <input type="button" value="🗑"/> |  |

## 開始する前に

- 組織の Rules Admin ロールか組織の Admin ロールが必要です。

## 手順

- ユーザメニューから、**ポリシーの管理**を選択します。
- 脆弱性の管理**を選択します。
- 違反**タブを選択します。
- ポリシーを追加するには：
  - ポリシーを追加**を選択します。
  - 名前にポリシーの名前を入力します。
  - 脆弱性のルールで、ポリシーに関連付ける深刻度や Assess ルールを選択します。
  - アプリケーションで、ポリシーに関連付ける重要性やアプリケーションを選択します。
  - 環境で、ポリシーを適用するアプリケーションがホストされているサーバ環境を選択します。
  - トリガーでは、**指定日数以降に既存の脆弱性にフラグを立てる**を選択し、日数を選択します。
  - 保存**を選択します。
- ポリシーを更新するには：
  - 違反タブで、ポリシーを選択します。
  - 必要に応じて、値を更新します。
  - 更新**を選択します。

## Protect ルール

Protect ルールを適用することで、アプリケーション環境における特定の種類のサイバー攻撃を監視またはブロックします。各ルールは、SQL インジェクションやクロスサイトスクリプティングなど、カスタムコードやオープンソースライブラリの脆弱性を悪用する攻撃の種類を表しています。

Contrast には多数の Protect ルールがあり、以下のような攻撃を監視したりブロックするために使用できます。

- コマンドインジェクション**：巧妙に作成された入力により、オペレーティングシステムレベルで不正なコマンドを実行されてしまう脆弱性。
- クロスサイトスクリプティング**：ユーザが他のユーザのブラウザで任意の JavaScript を実行できてしまう Web アプリケーションの脆弱性。
- EL インジェクション**：多くのフレームワーク やカスタムコードに存在する脆弱性で、アプリケーションがユーザ入力を OGNL、SpEL、JSP EL などの式言語(EL)として誤って評価した時に発生。
- メソッドの改ざん**：セキュリティ設定で、暗黙的に「全てを許可する」ような設定がある認証・承認システムに対する攻撃のこと。
- パストラバーサル/ローカルファイルインクルード**：アプリケーションで開いて読み込むファイルをユーザが制御できてしまう脆弱性。



- **SQL インジェクション・NoSQL インジェクション**：巧妙に作成された入力により、アプリケーションで使用される SQL クエリや NoSQL クエリが変更され、データが盗まれたりコードが実行されてしまう脆弱性。
- **安全でないファイルのアップロード**：悪意のあるファイルがアップロードの保護をバイパスして、悪意のある処理を実行できてしまう、アップロード処理の脆弱性。このルールは、一般的に使用される次のような拡張子を持つファイルに適用されます(ただし、これらに限定されるものではありません)：SVG、ASP、ASPX、\*SH、JAR、JAVA など。このルールによって、監視モードの場合には、安全でない可能性のあるファイルのアップロードが報告されます。ブロックモードの場合は、これらのファイルはブロックされます。
- **信頼できないデータのデシリアライゼーション**：ユーザが任意のオブジェクトをデシリアライズ処理に渡し、リモートからのコード実行が可能になる、Web アプリケーションの脆弱性。
- **XML 外部実体参照処理(XXE)**：ユーザがファイルに対してファイルを読み書きしたり、リモートコードを実行できる可能性がある、XML 処理の脆弱性。

## Protect ルールの設定

アプリケーション環境で攻撃を監視・ブロックする [Protect ルール \(680ページ\)](#)を設定することができます。

新しいアプリケーションを追加すると、Contrast はデフォルトの Protect ルールを適用します。組織の [デフォルトの Protect ルール \(683ページ\)](#)のモードは変更できます。

## 設定を行う前に

- アプリケーションに対して Protect ルールを設定するには、アプリケーションロールとしてルール管理者(Rules Admin)ロールが必要です。
- 組織に対して Protect ルールを設定するには、組織ロールとしてルール管理者(Rules Admin)または組織管理者(Admin)ロールが必要です。
- Contrast Security(SaaS 版のお客様の場合)、もしくは SuperAdmin(オンプレミス版のお客様の場合)によって、組織に [Protect 権限が付与 \(780ページ\)](#)されていることを確認してください。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択します。
2. アプリケーション名を選択し、**ポリシー**タブを選択します。
3. **Protect**を選択します。

| ルール                                                     | 種類/説明                                                                                                                                                                                                                       | 開発環境    | QA      | 本番環境    |
|---------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|---------|---------|
| <input type="checkbox"/> Padding Oracle                 | Protect Rule / A padding oracle attack can be used to decrypt cipher text. Monitor mode only.                                                                                                                               | MONITOR | MONITOR | MONITOR |
| <input type="checkbox"/> Unsafe File Upload             | Protect Rule / A vulnerability in the upload process that allows malicious files to bypass upload protections and perform malicious actions. Consequences can range from complete system takeover to web server defacement. | OFF     | OFF     | OFF     |
| <input type="checkbox"/> XML External Entity Processing | Protect Rule / A vulnerability in XML processing that can lead to file read/writes and remote code execution.                                                                                                               | MONITOR | MONITOR | MONITOR |

4. 特定のルールを検索するには、検索ボックスにルール名を入力します。
5. ルールごとに、各環境のモードを設定します。
  - a. 各環境のドロップダウンを選択します。
  - b. 次のいずれかのモードを選択します。
    - **オフ**：ルールは完全に無効になります。
    - **監視**：エージェントは攻撃を特定し、報告します。
    - **ブロック**：エージェントは攻撃を特定して報告し、ブロックします。



### 重要

攻撃がルールと一致し、そのルールがブロックモードに設定されている場合、エージェント(Java、.NET Framework、.NET Core)は `AttackBlockedException` をスローします。

アプリケーションがクラッシュしないように、`AttackBlockedException` を処理するようにアプリケーションを設定してください。

- **ペリメータでブロック**：エージェントは、アプリケーションが攻撃を処理する前に、攻撃の可能性をブロックします。このオプションは全てのルールで利用できるわけではありません。
  - **ペリメータで監視**：エージェントは、アプリケーションが攻撃を処理する前に、攻撃の可能性の特定と報告を試みます。このオプションは全てのルールで利用できるわけではありません。
- ペリメータでブロックまたは監視をする場合、エージェントは **シンク** で攻撃を検証しません。この処理は、誤検知の結果となる可能性があります。



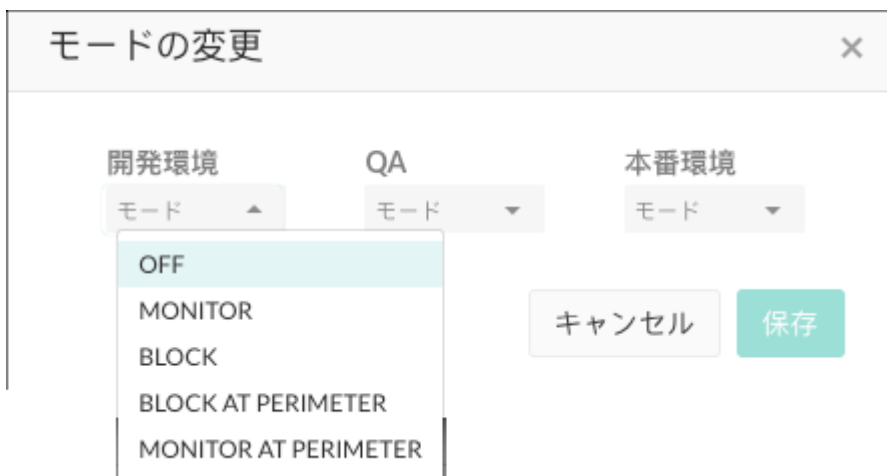
### ヒント

環境ごとに Protect ルールを異なるモードに設定することで、ポリシーをテストできます。これにより、本番前にさまざまなオプションがどのように機能するかを確認でき、本番環境での防御を妨げることはありません。

6. 複数のルールに設定を適用するには、次のいずれかの方法を使用します。
  - a. 変更したい各ルールの横にあるチェックボックスを選択し、**モードを変更**を選択します。
  - b. 全てのルールを設定を変更するには、**ルール**の横にあるチェックボックスを選択し、**モードを変更**を選択します。



- c. 「モードの変更」画面で、各環境のモードを選択し、**保存**を選択します。



7. 特定のルールを使用する組織内の全てのアプリケーションに Protect ルールを設定するには：この手順には、組織ロールとしてルール管理者(Rules Admin)ロールが必要です。
  - a. **ユーザメニュー > ポリシーの管理 > Protect ルール**を選択します。
  - b. ルールの一覧にフィルタを適用するには、ドロップダウンを使用して言語でフィルタをかけるか、検索フィールドを使用して名前でもルールを検索します。

- c. ルール名を選択すると、現在そのルールを使用している全てのアプリケーションの設定を管理できます。

**ポリシーの管理**

ASSESS

- Assessルール
- セキュリティ制御
- 脆弱性の管理

PROTECT

- Protectルール
- CVEシールド
- 仮想パッチ
- ログエンハンサー
- IP管理

概要

- アプリケーションの例外
- コンプライアンスポリシー
- ライブラリポリシー
- 機密データ

PROTECTルール

■ オフ ■ 監視/ペリメータで監視 ■ ブロック ■ ペリメータでブロック

All (45) | ルールを検索 | 組織の新しいアプリケーションにデフォルトポリシーを設定します。

| ルール                                                                             | 説明                                                                                                                                                        | 開発環境 | QA | 本番環境 |
|---------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------|------|----|------|
| <b>Command Injection</b><br>.NET Framework, .NET Core, Java, Node, Python, Ruby | Carefully crafted inputs can execute tainted commands.                                                                                                    | 4 9  | 1  |      |
| Chained Commands - Command Injection<br>.NET Framework, .NET Core, Node         | Detects chained commands as potential attacks since command chaining is often used by attackers to invoke sensitive system commands.                      | 3 1  |    |      |
| Command Backdoors - Command Injection<br>.NET Framework, .NET Core, Node        | Detects when user input is executed as a system command or is passed as a command parameter to common shell programs (e.g. /bin/sh -c "some user input"). | 4    |    |      |
| Dangerous Paths - Command Injection<br>.NET Framework, .NET Core, Node          | Detects dangerous paths as part of system commands as attackers often try to get access to sensitive paths or files.                                      | 4    |    |      |

- d. ドロップダウンを使用して、各環境の Protect モードを設定します。

**ポリシーの管理**

ASSESS

- Assessルール
- セキュリティ制御
- 脆弱性の管理

PROTECT

- Protectルール
- CVEシールド
- 仮想パッチ
- ログエンハンサー
- IP管理

**Command Injection**  
Carefully crafted inputs can execute tainted commands.

All (14) | アプリケーションを検索 | モードを変更

| アプリケーション                                                                | 重要性    | 開発環境    | QA      | 本番環境    |
|-------------------------------------------------------------------------|--------|---------|---------|---------|
| <input type="checkbox"/> bugfindy                                       | Medium | BLOCK   | BLOCK   | BLOCK   |
| <input type="checkbox"/> DonetCoreApp1                                  | Medium | OFF     | BLOCK   | BLOCK   |
| <input type="checkbox"/> DonetCoreApp2                                  | Medium | BLOCK   | BLOCK   | BLOCK   |
| <input type="checkbox"/> github.com/Contrast-Security-OSS/go-test-bench | Medium | MONITOR | MONITOR | MONITOR |

## 組織の Protect ルールの設定

アプリケーションにエージェントを追加・設定したり、新しい組織を作成すると、デフォルトの Protect ルールセットが適用されます。



### 注記

2021年8月から、新しい組織には最適化された Protect ルールセットが含まれます。この構成は、パフォーマンスの向上など、Contrast をご利用の皆様には最高の価値を提供するためのものです。

組織レベルで Protect ルールのデフォルト設定を変更するには、以下の手順を実行してください。ここでの設定の変更は、Contrast の組織に追加する新しいアプリケーションに適用されます。組織内の既存のアプリケーションには影響しません。

## 設定を行う前に

- 組織管理者(Admin ロール)またはルール管理者(Rules Admin ロール)であることを確認してください。
- ログインして、該当する組織を選択します。

## 手順

1. ユーザーメニューから、**ポリシーの管理**を選択します。
2. **Protect ルール**を選択します。
3. **デフォルトポリシーを設定**を選択します。



4. Protect ルールごとに、アプリケーションがホストされている環境(開発環境、QA、本番環境)のドロップダウンを選択します。
5. 次のいずれかのモードを選択します。
  - **オフ**：ルールは完全に無効になります。
  - **監視**：エージェントは攻撃を特定し、報告します。
  - **ブロック**：エージェントは攻撃を特定して報告し、ブロックします。
  - **ペリメータでブロック**：エージェントは、アプリケーションが攻撃を処理する前に、攻撃の可能性をブロックします。このオプションは全てのルールで利用できるわけではありません。
  - **ペリメータで監視**：エージェントは、アプリケーションが攻撃を処理する前に、攻撃の可能性の特定と報告を試みます。このオプションは全てのルールで利用できるわけではありません。

## CVE シールド

共通脆弱性識別子(CVE)は、特定の脆弱性やリスクを標準化した識別子を表します。CVE は、ツールのカバレッジを評価するためのベースラインにもなります。

Contrast では、CVE があるアプリケーションを保護するために役立つ CVE シールドをいくつか提供しています。CVE シールドは、アップデートするのが難しい脆弱なライブラリを使用しているレガシーアプリケーションに有効です。

CVE シールドが必要となるのは、脆弱性が SQL インジェクションや信頼されていないデシリアライゼーションのような一般的な攻撃でない場合のみです。攻撃の発生を防ぐ既存の Protect ルールがある場合でも、特定の脅威に特化したより多くのデータを得るために Contrast で CVE シールドを作成することもあります。これにより、攻撃の状況をより詳しく把握しやすくなり、進行中の攻撃をセキュリティエコシステム全体の傾向にマッピングするのにも役立ちます。

[CVE シールドを表示する \(684ページ\)](#)

[CVE シールドのモードを設定する \(686ページ\)](#)

## CVE シールドを表示

CVE シールドの一覧には、次の情報が表示されます。

### ポリシーの管理

ASSESS

Assessルール

セキュリティ制御

脆弱性の管理

---

PROTECT

Protectルール

**CVEシールド**

仮想パッチ

ログエンハンサー

IP管理

---

概要

アプリケーションの例外

CVEシールド ■ オフ ■ 監視/ペリメータで監視 ■ ブロック

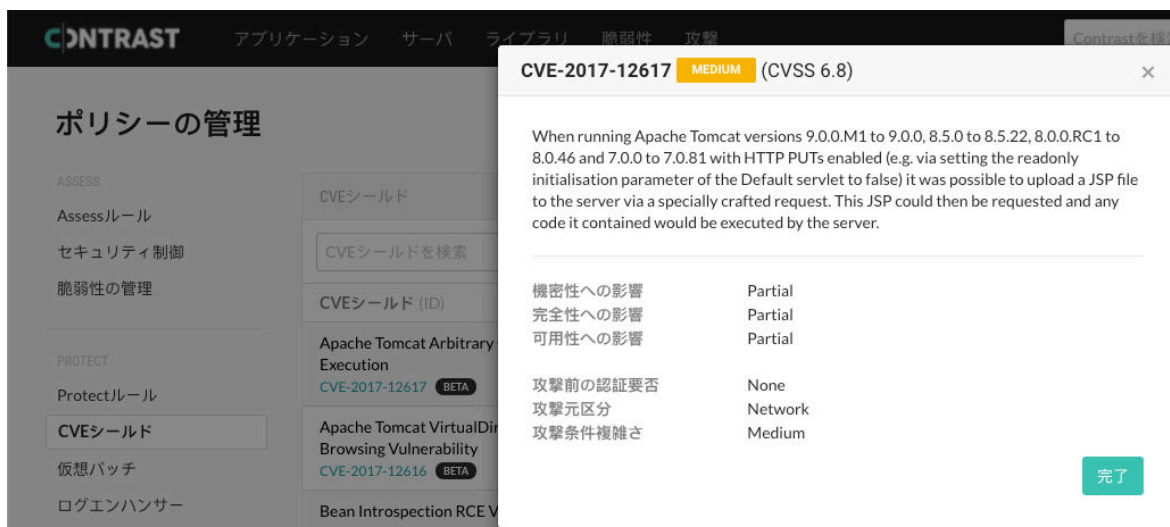
| CVEシールド (ID)                                                                                                                                                          | 説明                                                                                                                                               | 開発環境 | QA | 本番環境 |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------|------|----|------|
| Apache Tomcat Arbitrary Code Execution<br>CVE-2017-12617 <span style="background-color: #ccc; border: 1px solid #ccc; padding: 2px;">BETA</span>                      | A remote code execution vulnerability in Tomcat 7.0.0 through 7.0.81, 8.0.0.RC1 through 8.0.46, 8.5.0 through 8.5.22, and 9.0.0.M1 through 9.0.0 | 1    |    |      |
| Apache Tomcat VirtualDirContext File Browsing Vulnerability<br>CVE-2017-12616 <span style="background-color: #ccc; border: 1px solid #ccc; padding: 2px;">BETA</span> | A flaw in VirtualDirContext in Tomcat 7.0.0 through 7.0.80, allows an attacker to view sourcecode and other files on the system.                 | 1    |    |      |

- Contrast が特定の CVE に対して提供する CVE シールド
- CVE の説明
- アプリケーションをホストするサーバが稼働している環境
- CVE シールドに設定されているモード：
  - **オフ**：このモードでは、CVE シールドが完全に無効になります。
  - **監視**：このモードでは、CVE シールドが攻撃を特定し報告します。
  - **ペリメータで監視**：このモードでは、アプリケーションが攻撃を処理する前に、CVE シールドが攻撃の可能性の特定と報告を試みます。このオプションは、全ての CVE シールドで利用できるわけではありません。
  - **ブロック**：このモードでは、CVE シールドが攻撃を特定して報告し、ブロックします。
- 特定の CVE を含むアプリケーション(存在する場合)  
 CVE シールドはこの脆弱性を攻撃から守ります。

## 手順

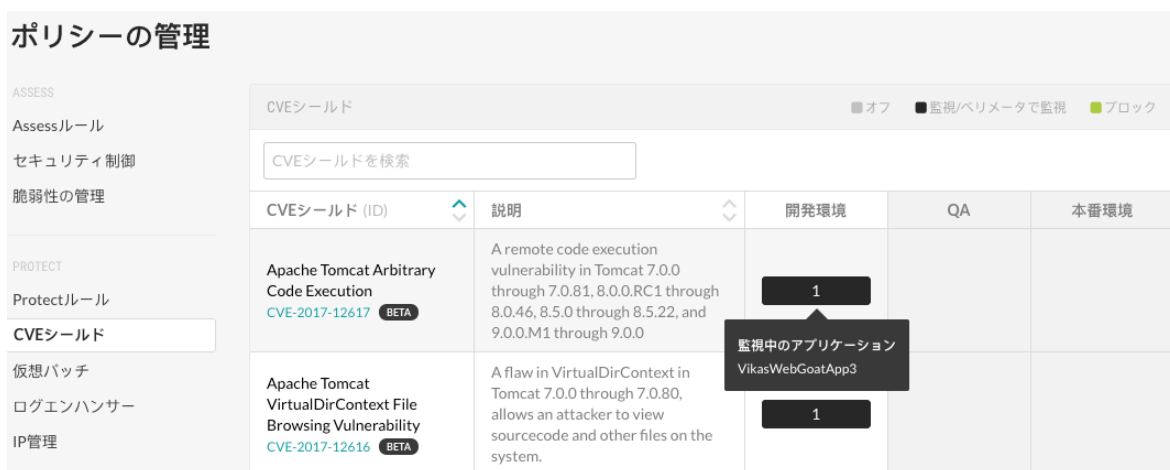
CVE シールドを表示するには：

1. ユーザメニューから、**ポリシーの管理**を選択します。
2. 左ペインの Protect より、**CVE シールド**を選択します。
3. 特定の CVE を検索するには、検索ボックスに CVE シールド名の全部または一部分を入力します。
4. 特定の CVE の詳細を参照するには、CVE 名の下にあるリンクをクリックします。



5. CVE があるアプリケーションを確認するには、サーバ環境の列の 1 つで、数字の上にカーソルを合わせます。ツールチップには、CVE シールドが防御しているアプリケーションの一覧が表示されます。

数字は、その CVE を含むアプリケーションの数を示します。モードは、CVE シールドがどのモードで設定されているかを示します。



## CVE シールドのモードを設定

CVE シールドは、攻撃のカテゴリを検知するのではなく、アプリケーションに含まれる特定の CVE を攻撃から守るものです。

開発環境、QA 環境または本番環境で実行中のサーバでホストされているアプリケーションに対して、以下のいずれかのモードを設定します。

- **オフ**：このモードでは、CVE シールドが完全に無効になります。
- **監視**：このモードでは、CVE シールドが攻撃を特定し報告します。
- **ペリメータで監視**：このモードでは、アプリケーションが攻撃を処理する前に、CVE シールドが攻撃の可能性の特定と報告を試みます。このオプションは、全ての CVE シールドで利用できるわけではありません。
- **ブロック**：このモードでは、CVE シールドが攻撃を特定して報告し、ブロックします。

## 設定を行う前に

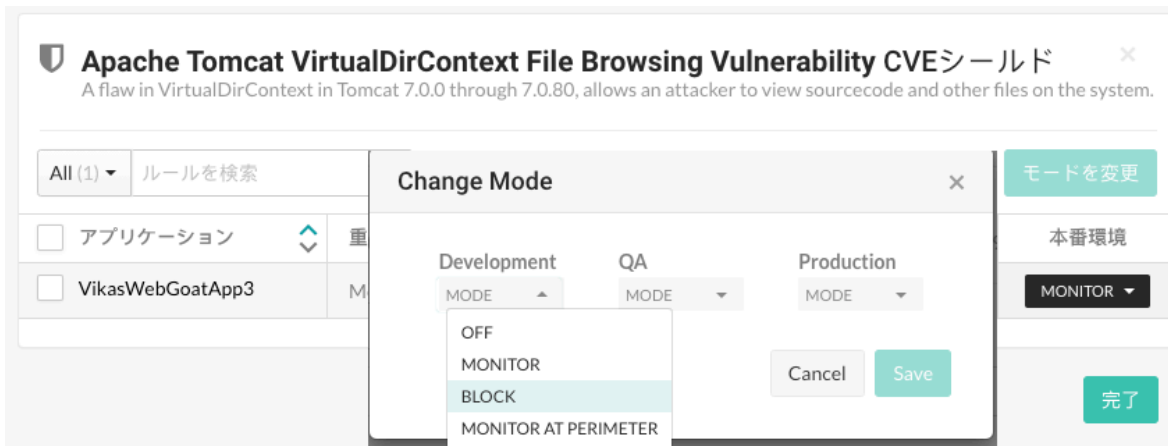
- **必須**：組織またはルールの管理者権限(Admin もしくは Rules Admin ロール)があることを確認してください。

- **サーバの設定 (530ページ)**を確認し、アプリケーションをホストするサーバの環境が正しく設定されていることを確認してください。

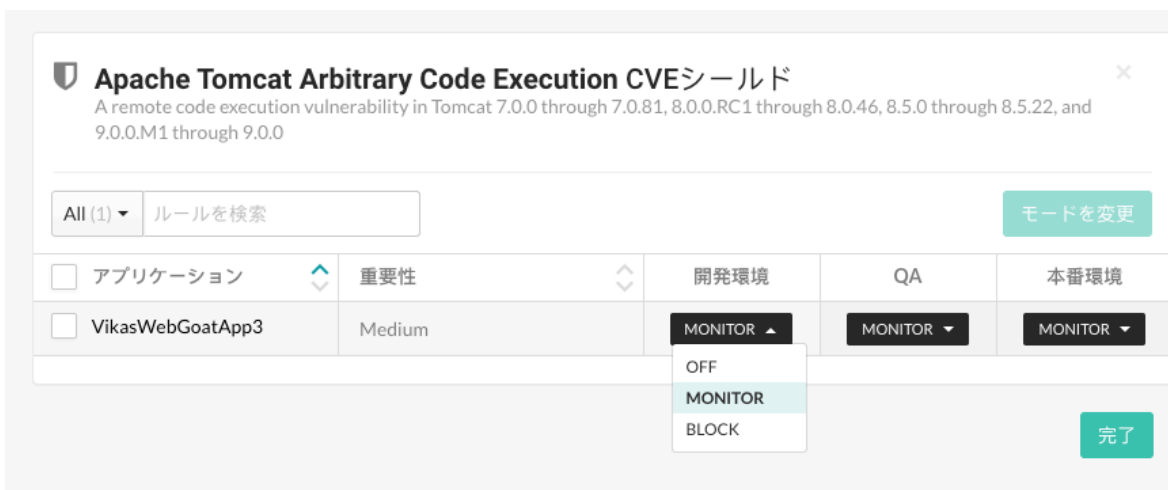
## 手順

CVE シールドのモードを設定するには：

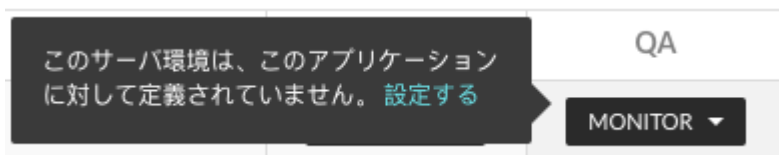
1. ユーザメニューから、**ポリシーの管理**を選択します。
2. **CVE シールド**を選択したら、CVE シールド名をクリックします。  
特定の CVE を検索するには、検索ボックスに CVE シールド名の全文または一部分を入力します。
3. 全てまたは複数のアプリケーションのモードを設定するには：



- a. 全てのアプリケーションを選択する場合は、**アプリケーション**のチェックボックスを選択します。複数のアプリケーションを選択する場合は、各アプリケーションのチェックボックスを選択します。
  - b. **モードを変更**をクリックします。
  - c. 「モードの変更」画面で、選択したアプリケーションの CVE シールドのモードを 1 つまたは複数の環境で選択したら、保存します。
  - d. **完了**をクリックします。
4. 1 つのアプリケーションのモードを設定するには：



- a. アプリケーションの行の最後にある、環境の列でメニューを選択します。  
アプリケーションをホストするサーバに環境が定義されていない場合、その環境にカーソルを合わせると、ツールチップが表示されます。その環境にサーバを設定するには、**設定する**をクリックして、サーバの行の最後にある設定アイコン(⚙️)を選択します。



- b. 選択した環境で、アプリケーションの CVE シールドのモードを選択します。
- c. 完了をクリックします。

## 組織の CVE シールドのモードを設定

Contrast の組織内のアプリケーションにエージェントを追加して設定すると、デフォルトの CVE シールドセットが適用されます。



### 注記

2021 年 8 月から、新しい組織には最適化された CVE シールドセットが含まれます。この構成は、パフォーマンスの向上など、Contrast をご利用の皆様には最高の価値を提供するためのものです。

組織レベルで CVE シールドのデフォルト設定を変更するには、以下の手順を実行してください。ここでの設定は、Contrast の組織に新規に追加される全てのアプリケーションに適用され、組織内の既存のアプリケーションには影響しません。

## 設定を行う前に

- 組織管理者(Admin ロール)またはルール管理者(Rules Admin ロール)であることを確認してください。
- 正しい組織にログインするか、選択してください。

## 手順

CVE シールドのモードを変更するには :

1. ユーザメニューから、**ポリシーの管理**を選択します。
2. **CVE シールド**を選択します。
3. **デフォルトポリシーを設定**を選択します。



4. CVE シールドごとに、アプリケーションがホストされている環境(開発環境、QA、本番環境)のド롭ダウンを選択します。
5. 次のいずれかのモードを選択します。
  - **オフ** : このモードでは、CVE シールドが完全に無効になります。
  - **監視** : このモードでは、CVE シールドが攻撃を特定し報告します。
  - **ペリメータで監視** : このモードでは、アプリケーションが攻撃を処理する前に、CVE シールドが攻撃の可能性の特定と報告を試みます。このオプションは、全ての CVE シールドで利用できるわけではありません。



- **ブロック** : このモードでは、CVE シールドが攻撃を特定して報告し、ブロックします。

## 仮想パッチの管理

仮想パッチとは、暫定的なカスタムルールで、特定の条件(URL、パラメータのキーや値など)を満たす HTTP リクエストをアプリケーションが処理する前にブロックできます。

組織の管理者(Admin)とルール管理者(RulesAdmin)は、仮想パッチの表示と管理ができます。

仮想パッチを追加するには :

1. **ユーザメニューで、ポリシーの管理より仮想パッチを選択します。**
2. **言語フィルターや一覧表の上にある検索フィールドを使用して、仮想パッチを検索します。**

**ポリシーの管理**

ASSESS

- Assessルール
- セキュリティ制御
- 脆弱性の管理

PROTECT

- Protectルール
- CVEシールド
- 仮想パッチ**
- ログエンハンサー
- IP管理

概要

- アプリケーションの例外
- コンプライアンスポリシー
- ライブラリポリシー
- 機密データ

| 名前                         | 説明                                                   | 開発環境                                | QA                                  | 本番環境                                |  |
|----------------------------|------------------------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--|
| Anertix on                 | Autogenerated patch for Anertix on ErikTomcatEclipse | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |  |
| spring cmd injection       | spring cmd injection                                 | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |  |
| struts-content-type-header | Struts2 S2-045 Remote Command Execution Patch        | <input type="checkbox"/>            | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |  |
| Test                       | Test                                                 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |  |

3. **ルールの設定を編集するには、仮想パッチ名をクリックします。または、新規に作成するには、仮想パッチを追加を選択します。**  
**削除アイコン**を選択してルールを削除したり、一覧表にあるトグルボタンを使用して各環境を有効/無効にすることもできます。
4. **表示される画面で、名前と説明を入力します。**

**ポリシーの管理**

ASSESS

- Assessルール
- セキュリティ制御
- 脆弱性の管理

PROTECT

- Protectルール
- CVEシールド
- 仮想パッチ**
- ログエンハンサー
- IP管理

概要

- アプリケーションの例外
- コンプライアンスポリシー
- ライブラリポリシー
- 機密データ

**+ 仮想パッチを追加**

名前  
この仮想パッチ名を入力

説明  
この仮想パッチの説明を入力

適用対象 <sup>?</sup>

アプリケーション

アプリ言語

アプリケーションテクノロジー

条件 <sup>?</sup>

ユーザージェエ... が次と一致する 値

+ 条件を追加

キャンセル 追加

5. **適用対象**の欄では、ラジオボタンを使用して、特定の**アプリケーション**、**アプリケーション言語**、または**アプリケーションテクノロジー**のいずれにルールを適用するか選択します。該当のボタンをクリックしたら、複数選択が可能なフィールドが表示されるので、選択をさらに絞り込むことができます。
6. **条件**では、ドロップダウンメニューを使用して、パッチがアプリケーションに適用される条件を選択します。必要であれば、別の行に**条件を追加**します。  
仮想パッチの値の適用方法を指定する場合は、次のいずれかを選択します。
  - 「が次と等しい」
  - 「に次が含まれる」
  - 「が次と一致する」 (Perl 互換正規表現 - PCRE を使用)
  - 「が次と等しくない」
  - 「に次が含まれない」
  - 「が次と一致しない」 (Perl 互換正規表現 - PCRE を使用)「**が次と一致する**」オプションと「**が次と一致しない**」オプションはどちらも Perl 互換正規表現 (PCRE) の使用をサポートしています。「**が次と一致する**」オプションか「**が次と一致しない**」オプションを選択した場合、HTTP リクエストの選択したフィールドの値に対して一致する正規表現を定義できます。  
式が一致する場合、または定義通りに一致しない場合、仮想パッチが適用されて緩和策が実行されます。



### 注記

正規表現はとても効果的ですが、複雑で正しく定義するのが難しい場合もあります。PCRE 形式がよくわからない場合は、セキュリティ専門家または [Contrast Security](#) にサポートを依頼して、仮想パッチが正しく効果的に設定されるように確認して下さい。

手始めに、[正規表現リファレンス \(694ページ\)](#)を参照することもできます。このリファレンスには、PCRE 形式で可能な表現の例がいくつかあります。

7. **追加**を選択して、設定を保存します。

## ログエンハンサーの追加や編集

ログエンハンサーとは、ソースコードの変更を必要とせずに、Contrast エージェントがアプリケーションのパラメータやデータを追加でログに記録するためのエージェント型手法の指示となるものです。

この高度なエージェント型手法を使用することで、ユーザはログに記録する API やパラメータを指定でき、Contrast エージェントは RASP ログの一部として *security.log* ファイルにこの情報を追加します。



### 注記

2021年8月から、新しい組織には最適化されたログエンハンサーセットが含まれます。この構成は、パフォーマンスの向上など、Contrast をご利用の皆様には最高の価値を提供するためのものです。

ログエンハンサーを追加、編集、削除するには：

1. [ポリシーの管理 \(668ページ\)](#)で、**ログエンハンサー**を選択します。
2. 言語でフィルタをかけるか検索を使用して、編集する既存のログエンハンサーを検索して名前を選択します。もしくは、**ログエンハンサーの追加**を選択します。各環境でルールを有効または無効にするには、一覧表の行にあるトグルを使用します。

| ログエンハンサー                                     |                                                                                 |                                     |                          |                                     |  |
|----------------------------------------------|---------------------------------------------------------------------------------|-------------------------------------|--------------------------|-------------------------------------|--|
| All (18) ▾ ログエンハンサーを検索                       |                                                                                 | + ログエンハンサーを追加                       |                          |                                     |  |
| ログエンハンサー                                     | 説明                                                                              | 開発環境                                | QA                       | 本番環境                                |  |
| Apache SSL HostName Verifier Changed<br>Java | The SSL hostname verifier changed after the SSLSocketFactory object was created | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |  |
| ESAPI Default Login<br>Java                  | ESAPI login using current request                                               | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |  |
| ESAPI Exception<br>Java                      | ESAPI threw a runtime security exception                                        | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |  |
| ESAPI Exception with cause<br>Java           | ESAPI threw a runtime security exception                                        | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> |  |

3. 表示される画面で、名前と説明を入力します。

**ログエンハンサーを追加** ×

---

名前

説明

ログレベル:       ログタイプ:

ログを記録するAPI  
 言語:       API:       フォーマット:

4. **ログレベル (824ページ)**と**ログタイプ**を入力します。

5. **ログを記録する API** では、以下を入力します。

- **言語**
- **API** : <class\_name>.<method\_name>(<argument\_types>) の構文を使用します。例 :

```
public boolean com.acme.Authenticator.authenticate(String user, \
String password)
```

- **フォーマット** : 関数呼び出しからの関連データを含めて、ログの説明を入力します。次のプレースホルダーをメッセージに含めることができます。
  - **{{O}}** : この呼び出しが行われたオブジェクトの文字列表記を出力します。メソッドが static の場合、これは NULL か空となる場合があります。
  - **{{Pn}}** : インデックス n で指定されたパラメータを出力します。n は、1 から始まることに注意してください。
  - **{{P1}}** : 最初のパラメータをメッセージに出力します。
  - **{{R}}** : 関数の戻り値を出力します。

6. **追加**を選択して、ログエンハンサーを保存します。

## アプリケーションの例外

何らかの理由により報告が不要なイベントを制御するために、例外を使用できます。Contrast エージェントの検査範囲外で外部のセキュリティ制御を使用している場合は、イベントの制御が必要になる場合があります。例：

- 管理者としては、クロスサイトスクリプティング(XSS)の脆弱性に該当するとしても、Web ページに表示される HTML の変更が必要な場合があります。この場合、例外を作成して、このような変更が報告されないようにすることができます。
- エッジデバイスを使用して、アウトバウンド HTTP のレスポンスに正しいヘッダを含めることで、クリックジャッキング攻撃を防いでいるとします。ただし、アプリケーションには必要な防御がされていないために、この問題が適切に報告される可能性があります。
- ベータ版のルールをテストする際などに、例外を使用することで誤検知を抑えることができます。

Java、Node.js、.NET、Python、Ruby エージェントを使用している場合は、ポリシーの管理から、または攻撃イベントの一覧から [アプリケーションの例外を追加 \(692ページ\)](#) できます。

定義済みの例外の一覧を表示するには、[アプリケーション > アプリケーション名 > ポリシー > 例外](#)、または [ユーザメニュー > ポリシーの管理 > アプリケーションの例外](#) を選択します。

## アプリケーションの例外の追加

Java、.NET Framework、.NET Core、Node.js、Python、Ruby エージェントを使用している場合、[アプリケーションの例外 \(692ページ\)](#) を使用して、特定のアプリケーションやアプリケーションの一部をセキュリティ検査の対象から外すことができます。

現在、Go エージェントと PHP エージェントは、アプリケーションの例外をサポートしていません。



### 注記

メッセージキューの例外は、Java エージェントでのみ利用できます。この機能は、まだ正式にリリースしておりません。メッセージキューの例外を利用するには、[Contrast サポート](#)までご連絡ください。

## 開始する前に

- 管理者(Admin)ロール、またはルール管理者(Rules Admin)ロールが必要です。
- Node.js、Python、Ruby エージェントは、コードの例外をサポートしていません。
- Java エージェントのみ、メッセージキューの例外をサポートしています。

## 手順

1. Contrast Web インターフェイスのナビゲーションバーで [アプリケーション](#) を選択して、アプリケーションの一覧よりアプリケーション名をクリックします。  
例外を適用できるのは、その例外を作成したアプリケーションだけです。
2. [ポリシー](#) タブを選択したら、[例外](#) を選択します。
3. [例外を追加](#) を選択します。



## ヒント

既存の攻撃イベントから例外を作成することもできます。攻撃イベントの一覧を表示する場合は、**攻撃 > 攻撃イベント**を選択します。一番右の列にある三角形を選択して、**例外を追加**を選択します。このボタンを選択すると、そのイベントの情報に基づいて例外の各フィールドにデータが事前に入力されます。

作成後、この例外は例外の一覧に表示されます。

4. 「例外を追加」の画面で、この例外の**名前**を入力します(覚えやすい名前にします)。
5. **例外の種類**を選択します。  
入力、URL、キュー/トピックベースによる例外定義には、以下の値を含む Perl 互換正規表現(PCRE)のサブセットを使用できます。

```
. * for 0 or more of any character
. + for 1 or more of any character
. ? for 0 or 1 of any character
. for 1 of any character
\. for an escaped literal of . for usage Example: somefile\.jsp
```

詳細は、[こちらの正規表現の例 \(694ページ\)](#)を参考にしてください。

以下のいずれかの種類を選択してください。

- **コード**：例外にするメソッドシグネチャを指定します。例えば、com.Acme.OldSecurity というクラス内に doLegacySecurity() と呼ばれるメソッドがあり、安全でない暗号化アルゴリズムの使用が報告されている場合、以下の行を入力することで、無視させることができます。

```
Com.Acme.OldSecurity.DoLegacySecurity
```

完全なメソッドシグネチャを指定し、末尾のパラメータ定義が欠如したり他の余分な文字を含めないようにしてください。このメソッドシグネチャが、検出された脆弱性のスタックトレースに対して照合されます。一致するものが含まれるメソッドシグネチャは全て検査の対象外になります。

- **入力**：入力タイプを選択し、入力名を入力します。この入力を使用される検出結果は、全て表示されなくなります。
  - **Parameter**、**Header**、**Cookie** の場合：検出結果を非表示にする特定の入力名を指定してください。ワイルドカード\*を使用すると、選択した入力タイプの全ての検出結果が非表示となります。
  - **QueryString** および **Body** の場合：それぞれ QueryString と Body 全体の検出結果が表示されなくなります。QueryString と Body は、以下で定義されている URL の例外パターンとの組合せでのみ例外として有効になります。

例外の種類が入力の場合、「適用する URL」の項目で、URL の適用範囲を選択します。

- **全ての URL**：指定された入力タイプと入力名が使用されている検出結果は、どこから発生したかに関係なく表示されなくなります。
- **以下の URL**：例外を適用するパスを指定します。[正規表現 \(694ページ\)](#)と[ワイルドカード表記 \(695ページ\)](#)を使用できます。



## 重要

プロトコルスキーム(http://または https://)やホスト名は含めず、/で始まるパス名のみを使用してください。

スラッシュの後にワイルドカード(/.\*)を指定すると、全ての URL を記述する代わりに使用できます。

特定のルールで無視する必要がある URL を指定します。

- **URL** : 特定のルールで無視する必要がある URL を指定します。例外にする URL のパスを 1 行ずつ記述します。正規表現 (694ページ)とワイルドカード表記 (695ページ)を使用できます。
  - **キュー/トピック** : 特定のルールで無視されるべきメッセージキューやトピックを指定します。メッセージキューには 1 つのコンシューマがあり、トピックには複数のコンシューマがあります。  
現在、このオプションは Java エージェントのみでサポートされています。  
キュー/トピックの例外タイプの場合、「適用するキュー」で、キューまたはトピック名の適用方法を選択します。
    - **全てのキュー/トピック** : 全てのキュー/トピックからの結果が表示されなくなります。
    - **以下のキュー** : 例外とするキュー名またはトピック名のリストを指定します。キュー名を指定するか、正規表現 (694ページ)とワイルドカード表記 (695ページ)を使用できます。
6. **対象ルール**には、例外の影響を受けるルールの範囲を指定します。デフォルトでは全てのルールが対象になります。チェックボックス内をクリックして複数のオプションを選択できます。
- **全てのルール**を選択すると、Assess と Protect の両方で検出される全ての脆弱性に対して例外が適用されます。
  - 「ASSESS」下にある**全ての Assess ルール**を選択すると、Assess が有効になっている場合、検出された全ての脆弱性に適用されます。
  - 「PROTECT」下にある**全ての Protect ルール**を選択すると、Protect が有効になっている場合、全ての攻撃イベントに適用されます。
  - 「ASSESS」セクションおよび「PROTECT」セクション下で、個々のルールを選択することで、適用対象をさらに絞り込むことができます。例外は、選択したルールで検出された脆弱性のみ適用されます。  
例外の種類として入力を選択した場合は、ユーザ入力によってトリガーされないルールのみを選択します。
  - 「ASSESS」および「PROTECT」下では、Assess と Protect で検出される個々のルールを複数選択できます。
7. 既に報告されているイベントを非表示にする場合は、この例外と一致する全てのイベントを消去の横のチェックボックスをオンにします。
8. **追加**を選択します。  
例外が、例外の一覧に追加されます。定義した条件に一致する入力は、適用したルールによって処理が行われなくなります。  
例外の一覧は、アプリケーション > アプリケーション名 > ポリシー > 例外または、ユーザメニュー > ポリシーの管理 > アプリケーションの例外で確認できます。一覧にあるトグルボタンを使用して、Assess または Protect の例外を有効/無効にできます。

## 正規表現リファレンス

アプリケーションの例外を追加 (692ページ)する際には、以下の表と例を参考にしてください。

| 適用                      | パターン     | パターン例     | 一致例                    |
|-------------------------|----------|-----------|------------------------|
| 文字列の先頭                  | ^        | ^w+       | Start of a string      |
| 文字列の末尾                  | \$       | w+\$      | End of a string        |
| 後に続く文字列の大文字と小文字を区別しない一致 | (?i)     | (?i)%0a   | %0a or %0A             |
| a、b、または c の内の 1 文字      | [abc]    | [abc]+    | a bb ccc               |
| a、b、c 以外の文字             | [^abc]   | [^abc]+   | Anythingbutabc.        |
| a-z までの範囲内の 1 文字        | [a-z]    | [a-z]+    | Only a-z               |
| a-z までの範囲内でない 1 文字      | [^a-z]   | [^a-z]+   | Anythingbuta-z.        |
| a-z または A-Z の範囲内の 1 文字  | [a-zA-Z] | [a-zA-Z]+ | abc123DEF              |
| 任意の 1 文字                | .        | .+        | abc                    |
| 空白文字                    | \s       | \s        | anywhitespacecharacter |
| 空白以外の文字                 | \S       | \S+       | any non-whitespace     |
| 10 進数字                  | \d       | \d        | not 1 not 2            |
| 10 進数字以外                | \D       | \D+       | not 1 not 2            |
| 0 個または 1 個の a           | a?       | ba?       | ba b a                 |

| 適用               | パターン   | パターン例  | 一致例                       |
|------------------|--------|--------|---------------------------|
| 0 個以上の a         | a*     | ba*    | a ba baa aaa ba b         |
| 1 個以上の a         | a+     | a+     | a aa aaa aaaa bab baab    |
| ちょうど 3 個の a      | a{3}   | a{3}   | a aa aaa aaaa             |
| 3 個以上の a         | a{3,}  | a{3,}  | a aa aaa aaaa aaaaaa      |
| 3 個以上 6 個以下の a   | a{3,6} | a{3,6} | a aa aaa aaaa aaaaaa aaaa |
| ピリオド(ドット)はリテラル文字 | .      | a.b    | string .string            |

## ワイルドカード表記

アプリケーションで、入力、URL、キュー/トピックの例外を指定する場合に、以下を使用してワイルドカード式を作成できます。

- .\*は、任意の文字が 0 個以上あることを意味します。
- .+は、任意の文字が 1 個以上あることを意味します。
- .?は、任意の文字が 0 個か 1 個あることを意味します。
- .は、任意の 1 文字を意味します。
- \.は、.というリテラルをエスケープするために使用します。

例：somefile\.jsp

## ワイルドカード表記の例

| 期待される結果                                       | 正規表現                | 例                                             |
|-----------------------------------------------|---------------------|-----------------------------------------------|
| 全てのサブパスを例外にする                                 | /myapp/.+           | /myapp/で始まる URL があるパスを全て例外にする                 |
| サブパスの 1 文字を外したものを例外とする                        | /.yapp              | yapp で終わる 5 文字のサブパス (myapp など) を全て例外にする       |
| 1 つのサブパスを明示的に例外とする                            | /myapp/<br>thispath | /myapp/thispath のみを例外とする                      |
| パスの末尾によって例外とする                                | /. *ignore          | ignore で終わるパスを全て例外とする                         |
| 指定値を含むパスを例外とする                                | /. *value.*         | value を含むパスを全て例外とする                           |
| 指定値を含むパスを例外とする                                | /. ?value.*         | value で始まるパス、または value の前に 1 文字あるパスを全て例外とする   |
| ピリオド(ドット)がワイルドカードではなくリテラル文字として使用されているパスを例外とする | /myapp\.js          | myapp.js のみを例外とする<br><br>この表記は 3 インスタンスまで使用可能 |

## コンプライアンスポリシーの設定

組織内のアプリケーションのコンプライアンスに対するポリシーを定義できます。指定されたアプリケーションのいずれかがこのポリシーに違反している場合は、Contrast によってマークが付けられるので、すぐに確認して修正することができます(管理者にも E メールで違反が通知されます)。

コンプライアンスポリシーを設定するには：

1. [ポリシーの管理 \(668ページ\)](#)でコンプライアンスポリシーを選択します。
2. 既存のコンプライアンスポリシーがある場合は、そのリストが表示されます。トグルボタンを使用してポリシーを有効/無効にできます。また、[ゴミ箱アイコン](#)を使用してポリシーを削除できます。
3. 編集するポリシーの名前を選択するか、グリッドの上部にある[ポリシーを追加](#)を選択して新しいコンプライアンスポリシーを作成します。
4. 表示されるパネルに以下の項目を入力します。
  - **名前**：ポリシーの名前を選択します。
  - **ポリシー基準**：デフォルトは**全てのルール**ですが、脆弱性名を入力して、深刻度レベル、セキュリティ基準または Assess ルールごとに脆弱性を選択できます。
  - **アプリケーション**：デフォルトは**全てのアプリケーション**ですが、アプリケーション名を入力して、重要度レベルや個々の名前ごとにアプリケーションを選択できます。

## 5. 追加または保存を選択します。



### 注記

デフォルトポリシーでは、名前とポリシー基準のフィールドがロックされていて削除できません。ただし、デフォルトポリシーのアプリケーションの選択は変更できます。



### ヒント

有効化されたポリシーを使用して、コンプライアンスポリシーごとにアプリケーションを絞り込むことができます。これを行うにはアプリケーションを選択します。アプリケーションページで詳細リンクをクリックして、コンプライアンスポリシーごとにアプリケーションを絞り込みます。



### 注記

Contrast では、対象の脆弱性が修復されていない場合や対象のセキュリティ標準や Assess ルールの違反がある場合に、アプリケーションページで該当するアプリケーションにフラグが立てられます。アプリケーショングリッドの警告アイコンにカーソルを合わせるか、アプリケーションの詳細ページに移動すると、違反しているポリシーへのリンクが表示されます。

## IP の管理

拒否リスト、許可リスト(信頼できるホスト)、ソース名に関して、組織の IP ポリシーを管理できます。



### 注記

拒否リストおよび許可リストに対して、Contrast は `X-Forwarded-For` リクエストヘッダをチェックして、IP アドレスがリストにあるエントリと一致するかどうかを確認します。

- **IP 拒否リスト** : Contrast Protect でリスト内の全ての IP アドレスをブロックするようにルールを設定します。  
拒否リストの使用は、より永続的な Protect ポリシーを導入できるまでの間か、調査を実施できるようになるまでの間の、即時的なトリアージに適しています。
- **IP 許可リスト** : 脆弱性スキャンを実行する信頼できるホストを登録して、安全な IP アドレスとして設定します。このリストに登録された IP アドレスからのデータは Contrast では表示されなくなります。  
IP 許可リストのエントリ(登録された IP アドレス)は、IP 拒否リストのエントリを上書きしません。Contrast Assess 機能には影響せず、通常通り機能します。  
Contrast Protect は、このリストにあるエントリと一致する全ての IP アドレス(または IP 範囲)を無視します。リストに指定されている IP アドレスからの攻撃を監視したり、ブロックをしません。



- **ソース名**：1つ以上の IP アドレスまたはサブネットマスクで、既知のソース(ペネトレーションテスト担当者など)から発生する攻撃イベントにラベルを付けることができます。  
**攻撃 > 監視および攻撃の詳細**ページで攻撃を表示すると、攻撃者の IP 情報の代わりにソース名が表示されます。この値を表示することによって、想定しているイベントと注意が必要な攻撃イベントをすばやく特定して区別することができます。

## 関連項目

- [IP の拒否/許可 \(697ページ\)](#)
- [ソース名の管理 \(698ページ\)](#)

## IP アドレスの拒否と許可

IP 拒否リストと IP 許可リストを使用して、組織内の [IP アドレスを管理 \(696ページ\)](#) します。

### 開始する前に

- 組織のロールとして、管理者(Admin)またはルール管理者(Rules Admin)が必要です。
- CIDR(Classless Inter Domain Routing)表記を使用して、サブネットマスクを指定します。

### 手順

1. ユーザメニューから、**ポリシーの管理 > IP 管理**を選択します。
2. 拒否リストの管理：
  - a. **IP 拒否リスト**タブを選択します。
  - b. 既存の拒否リストを編集する場合は、拒否リスト名を選択して情報を変更したら、**保存**を選択します。
  - c. 拒否リストに IP アドレスを新規に登録する場合は、**拒否リストに IP を登録**を選択して情報を入力したら、**追加**を選択します。

The screenshot shows a dialog box titled "拒否リストにIPを登録" (Add IP to Deny List). It contains the following fields and controls:

- 名前** (Name): A text input field containing "test".
- IPアドレス/サブネットマスク** (IP Address/Subnet Mask): A text input field containing "1.1.1.1". Below it, a note reads "1.1.1.1 - 1.1.1.1で一致します" (Matches 1.1.1.1 - 1.1.1.1).
- 有効期限** (Validity Period): A dropdown menu set to "1 week".
- Buttons: "キャンセル" (Cancel) and "追加" (Add).

3. 許可リストの管理：
  - a. **IP 許可リスト**タブを選択します。
  - b. 既存の許可リストを編集する場合は、許可リスト名を選択して情報を変更したら、**保存**を選択します。
  - c. 許可リストに信頼できるホストを新規に登録する場合は、**信頼できるホスト**を登録を選択して情報を入力したら、**追加**を選択します。

信頼できるホストとしてIPを登録

名前  
test-now

IPアドレス/サブネットマスク ②  
2.2.2.2  
2.2.2.2 - 2.2.2.2で一致します

有効期限  
1 week

キャンセル 追加

## ソース名の管理

ソース名を使用すると、組織内の攻撃イベントを監視しながら、脅威ではない内部トラフィックやテストをすばやく特定できます。

1つまたは複数の IP アドレスやサブネットマスクに、任意のソース名を付けることができます。ソース名を保存すると、**攻撃 > 監視**を選択する、または**攻撃の詳細**ページを表示すると、(ユーザの IP 情報ではなく)ソース名を確認できます。これにより、攻撃イベントを評価する際に、ソース名の付いた攻撃者を既知の攻撃元として、すばやく特定できます。

ソース名を作成するには：

1. **ユーザメニュー > ポリシーの管理 > IP 管理 > ソース名**にアクセスします。
2. **ソース名を登録**を選択します。
3. 1つまたは複数の IP アドレスを識別するために使用する**名前**を入力します。
4. このソース名で識別する **IP アドレス/サブネットマスク**を追加します。必要に応じて、**IP アドレス/サブネットマスクを追加**のリンクをクリックして、IP アドレスまたはサブネットマスクをさらに追加します。
5. ドロップダウンメニューを使用して、ソース名を使用する**開始日時**と**終了日時**を選択します。過去の日付を開始日時とするカスタム期間を作成することもできます。この場合、ソース名は過去の攻撃イベントに遡って適用されます。
6. 入力が完了したら、**追加**をクリックしてソース名を保存します。  
組織にソース名が追加されると、**監視**ページや**攻撃**の詳細ページで、条件が一致する攻撃に対してソース名が表示されます。これは、**攻撃を監視 (606ページ)**するのに役立ちます。  
攻撃イベントについて報告されたデータが複数のソース名と一致する場合、Contrast では最後に更新された名前が適用されます。
7. ソース名を編集するには、ソース名を選択します。ソース名を**編集**画面が表示されますので、変更をし、**保存**を選択します。
8. ソースを削除するには、**ソース名一覧**で**削除**アイコンを選択するか、**ソース名を編集**の画面の下にある**削除**アイコンを選択します。名前を削除すると、その名前への全ての参照は、IP 情報に置き換わります。

## ライブラリポリシーの設定



### 重要

ライセンスポリシーは、Contrast SCA をご利用のお客様のみが利用できます。Contrast SCA を有効にするには、組織の管理者にご連絡ください。

Contrast では、組織の基準を満たさないライブラリにフラグが立てられるため、アプリケーションが安全であるかを確認できます。

ライブラリが制限されている、もしくは、特定のバージョンより古いものがアプリケーションで使用されている場合、Contrast ではポリシー違反としてマークされます。また、Contrast のインターフェイスで"F"という文字を付けてポリシー違反のライブラリを自動的に評価付けすることもできます(管理者には、Contrast 内と Eメールの両方で違反が通知されます)。



### 注記

ライブラリのバージョンには、メジャーバージョン、マイナーバージョン、パッチバージョンが含まれます。

ライブラリポリシーを設定するには：

1. ユーザメニューで**ポリシーの管理** > **ライブラリポリシー**を選択します。
2. **ライブラリを制限**するチェックボックスをオンにして、ポートフォリオから除外するライブラリを選択します。ライブラリは複数選択できます。
3. **バージョン要件を有効化**するチェックボックスをオンにして、指定したバージョン数の範囲内とする 1 つ以上のライブラリを選択します。
4. **他の要件を追加**のリンクをクリックすると、追加のライブラリのバージョン要件を作成できます。
5. **ライセンスを制限**のチェックボックスをオンにして、制限するオープンソースライセンスにポリシーを設定します。オープンソースライセンスが制限されている場合、その制限されたライセンスを使用するライブラリはポリシー違反としてマークされます。  
ライセンスポリシーでは、オープンソースライブラリが SPDX 形式で、識別子にフルネームが続く形式でリストされます。制限するライセンスの種類を選択する必要があります。ポートフォリオ内で認識される「以降」のライセンスも含まれます。例えば、GPL-3.0-only でライセンスを制限する場合、GPL-3.0 以降のライセンスは全てその制限に含まれます。
6. **ポリシー違反のライブラリ**のチェックボックスをオンにすると、設定されたポリシーに違反するライブラリに対して、低いスコアが自動的に割り当てられます。  
設定されたポリシーに準拠していないライブラリは、**ライブラリページ**で、名前と警告アイコンおよびライブラリスコアが赤色で強調表示されます。違反の詳細については、アイコンの上にカーソルを合わせるか、ライブラリの**概要ページ**にアクセスしてください。  
ライブラリを自動的に低いスコアにするように選択した場合、**スコア設定を調整 (719ページ)**すると、組織管理者に通知されます。

## 機密データのマスクング

機密データのマスクング機能は、組織のリスクを低減し、コンプライアンスの要件を満たすのに役立ちます。

データマスクングは、Contrast Web インターフェイス、Syslog またはセキュリティログに送信される脆弱性や攻撃レポートの情報にマスクをかけることで、アプリケーション内の機密データを保護します。

Contrast では、機密データやデータタイプをいくつかのカテゴリに分類しています。これらは特定のキーワードで構成され、エージェントが自動的に識別しレポート内でマスクされます。RulesAdmin 以上の権限を持つユーザは、**機密データを管理 (700ページ)**できます。

Contrast エージェントにより、クエリパラメータ、リクエストヘッダ、Cookie およびボディの機密データがマスクされます。エージェントによって、入力名に使用されている特定のキーワードが検索されて機密データが認識されます。一致するものが見つかった場合、その入力値にはマスクがかけられ、contrast-redacted-`{datatype}`という形式のプレースホルダに置き換えられます。datatype の部分は、キーワードが含まれる機密データの分類になります。

Contrast エージェントは、application/x-www-form-urlencoded 以外のコンテンツタイプがあるリクエストボディの個々のフィールドはマスクしません。ただし、リクエストボディ全体をマスクするようにエージェントを設定することができます。また、Assess を使用している場合の脆弱性レポートのデータフローに表示されるデータや、Protect を使用している場合の攻撃イベントのベクトルで表示されるデータもマスクされません。



## 注記

Contrast ログに記録されるステートメントには、Contrast エージェントによって「可能な限り」機密データが出力されないようにしていますが、ログレベルが DEBUG 以下に設定されていると、Contrast ログに機密データが記録される可能性があります。できる限り、本番環境のシステムでは、DEBUG 以下でログを記録するよう設定しないでください。機密データを扱うシステムが、DEBUG 以下でログを記録するように設定されている場合は、機密データの漏洩を防ぐために、これらのログが外部システムに送信されていないことを確認する手順を実行する必要があります。

例えば、以下は脆弱性レポートの一部としてエージェントによって送信された HTTP リクエストで、エージェントによって機密データと判断された 2 つの入力があります。これらは、Contrast Web インターフェイス、syslog サーバやセキュリティログに送信される前に入力値をマスクするために使用されたブレースホルダを示しています。

```
PUT /employee/5 HTTP/1.1
Host: yourdomain.com
Content-Type: application/x-www-form-urlencoded
Content-Length: 30
apikey: contrast-redacted-authentication-info

ssn=contrast-redacted-government-id&department=sales
```

この場合、ヘッダの値の「apikey」が「Authentication Info」データタイプにあるキーワードと一致しているためマスクされます。また、Contrast の組織にある「Government ID」データタイプのキーワードと「ssn」が一致しているため、フォームパラメータもマスクされます(キーワードの一致では、大文字と小文字は区別されません)。

## 機密データタイプの管理

[機密データのマスキング \(699ページ\)](#)は、組織のリスクを低減し、コンプライアンス要件を満たすのに役立ちます。

1. ポリシーの管理で**機密データ**を選択します。
2. ここでは機密データタイプのリストがアルファベット順に表示されます。検索フィールドを使用して、名前またはキーワードで特定のタイプを検索できます。
3. **本文全体をマスクする**の横にあるチェックボックスをオンにして、HTTP リクエストボディ全体のリダクションを有効にします。これは、組織内の全てのアプリケーションに適用されます。
4. Contrast で重大と判断されているデータタイプとキーワードは、デフォルトで組織内の全てのアプリケーションに適用され、編集したり無効にしたりすることはできません。Contrast で重大と判断されていないデータタイプに関しては、グリッドのトグルボタンを使用して、組織で有効/無効にできます。
5. グリッドでデータタイプの名前をクリックして、カスタムキーワードを追加します。**機密データタイプを編集画面で、カスタムキーワードを追加**を選択するとキーワードを追加でき、これらが適用されるアプリケーションを指定できます。**デフォルトキーワード**は編集できず、全てのアプリケーションに適用されます。
6. **保存**を選択します。

## ルール管理者として通知を追加/編集

通知のデフォルト設定は組織管理者(Admin)によって行われますが、ルール管理者(Rules Admin)も既存の通知を有効/無効にしたり、新しい通知を作成することができます。

1. [組織の設定 \(704ページ\)](#)で、**通知**を選択します。
2. トグルボタンを使用して、既存の通知を有効または無効にします。
3. 新しい通知を作成するには、**通知を作成**を選択します。
4. 表示される画面で、以下の項目を入力します。
  - 名前
  - 頻度
  - 説明
  - アプリケーション
  - アプリケーションのタグ
  - ユーザ
5. **保存**を選択します。

## 組織

組織の管理者権限(Admin)がある場合は、[ルール管理\(Rules Admin\) \(668ページ\)](#)や[編集\(Edit\) \(476ページ\)](#)権限で実行できる全ての操作に加えて、組織レベルで次の操作を実行できます。

- [組織の設定を行う \(704ページ\)](#)
- [Assess を有効にする \(701ページ\)](#)
- [Protect を有効にする \(702ページ\)](#)



### 注記

組織管理者(Admin)は、組織レベルで最も高い権限を持ちます。その他の[組織ロール \(819ページ\)](#)にも、組織全体におよぶ機能があります。

[システムレベルで設定 \(779ページ\)](#)すると、ユーザは複数の組織にわたって組織管理(Admin)ロールを持つことになります。

## Assess を有効にする

Assess を有効にするには :

1. 組織管理者(組織の Admin ロール)またはアプリケーション管理者(アプリケーションの Admin ロール)として、Contrast Web インターフェイスにログインします。
2. ナビゲーションバーで、**サーバ**を選択します。
3. サーバの一覧をスクロールするか、ページ上部の検索アイコンを選択して使用して、解析を行うサーバを検索します。

Assess のトグルボタンをオン(緑色)にします。これは以下の3つの方法で行えます。

  - サーバの一覧にある Assess 列のトグルボタンを選択する。
  - サーバ名をドリルダウンして詳細情報を表示し、サーバの概要画面でトグルを選択します。
  - 組織の設定で**サーバ**を選択して、Assess のトグルをオンにします。
4. Assess を有効にするには、Assess(アプリケーション)ライセンスが必要です。アプリケーションにライセンスを適用するには、ナビゲーションバーで**アプリケーション**を選択します。アプリケーション名の横にある**ライセンスなし**を選択すると、ライセンスの適用を促すメッセージが表示されず。



### 注記

[組織の設定 \(704ページ\)](#)で、組織管理者は左側のナビゲーションパネルで組織を選択し、[新しいアプリケーションにライセンスを自動で適用](#)の横にあるボックスをオンにできます。そうすることで、全てのアプリケーションで同じ操作を手動で行う必要がなくなります。

5. アプリケーションサーバを再起動して、Contrast エージェントが Assess 機能によってアプリケーションに組み込まれるようにします。再起動が完了すると、Contrast で脆弱性の解析情報の受信が始まります。アプリケーションの横に[ライセンスなし](#)が表示されなくなります。これは、Assess ライセンスが割り当てられていることを意味します。



### 注記

Assess ライセンスなしでも Contrast で検出された脆弱性の種類が表示されますが、詳細情報はライセンスなしでは取得できません。

## Protect を有効にする

ユーザに対して Protect を有効にすると、そのユーザが Protect データにアクセスして表示できるようになります。サーバに対して Protect を有効にすると、アプリケーションが Protect を使用して攻撃の監視やブロックができるようになります。



### 注記


既存のアプリケーションがあるサーバで Protect を有効にした場合は、Protect を有効にするためにアプリケーションを再起動する必要があります。

## 開始する前に

- [組織の設定](#) > [ユーザ](#)に移動し、Protect データと Protect の設定にアクセスする権限があることを確認します。
  - SaaS 版をご利用のお客様の場合、Contrast Security が組織全体および組織内のユーザロールに Protect 権限を付与します。
  - オンプレミス版をご利用のお客様の場合、[組織に Protect 権限を付与する \(780ページ\)](#)には、SuperAdmin か ServerAdmin、または SystemAdmin ロールが必要です。これらのロールは、どのユーザロールが Protect データにアクセスできるかを設定することもできます。
- サーバに適用できる[ライセンス \(706ページ\)](#)があることを確認してください。
- ユーザに対して Protect を有効にするには、組織管理者(Admin)ロールが必要です。

## 手順


1. Contrast Web インターフェイスで Protect の設定を行うために、Contrast Web インターフェイスにログインします。
2. ユーザが Protect データを表示・使用できるようにするには：
  - a. ユーザメニューで、[組織の設定](#)を選択します。

- b. ユーザを選択します。
  - c. Protect データへのアクセスを必要とするユーザごとに、Protect のトグルボタン(  )をオンにします。
  - d. 新しい設定を有効にするために、ユーザは Contrast Web インターフェイスからログアウトし、再度ログインするよう指示してください。
3. サーバで Protect を有効にするには :



### 注記

自動的にライセンスを適用 (706ページ)するには、組織管理者(Admin)またはルール管理者(Rules Admin)ロールが必要です。このオプションは、サーバの Protect を 1 台ずつ手動で有効にしたい場合に便利です。

- a. Contrast Web インターフェイスのナビゲーションバーで、サーバを選択します。
- b. サーバを選択します。
- c. Contrast Web インターフェイスで Protect を有効にするには、Protect のトグルボタン(  )をオンにします。以下のいずれかの方法で行います。
  - サーバの一覧にある **Protect** 列でトグルボタンをオンにします。
  - サーバ名を選択し、概要タブで Protect のトグルボタンをオンにします。
  - 組織の設定で**サーバ (713ページ)**を選択し、環境を選択して、Protect のトグルボタンをオンにします。




### 重要

エージェントの設定ファイルでの Protect の設定は、Contrast Web インターフェイスでの設定よりも優先されます。

4. 特定のサーバで Protect がオンになっていることを確認するには、「サーバ」タブでそのサーバを選択し、**概要**を選択します。  
サーバがホストしている 1 つ以上のアプリケーションで Protect を使用するよう設定されていない場合は、Protect のトグルの横に警告アイコンが表示されます。



5. 特定のアプリケーションに関して、アプリケーションをホストしている各サーバで Protect が有効であるかを確認するには、「アプリケーション」ページにアクセスします。
- a. Contrast Web インターフェイスのナビゲーションバーで**アプリケーション**を選択します。
  - b. アプリケーションの一覧で、アプリケーション名をクリックします。
  - c. 概要タブの各環境で、Protect のステータスが**オン**になっていることを確認します。  
アプリケーションをホストしているサーバのうち、Protect がオンになっている数が、Protect のステータスの横に **y サーバ中の x サーバ**という形式で表示されます(例、**17 サーバ中の 11 サーバ**)
  - d. アプリケーションをホストしている各サーバで、そのアプリケーションが Protect を使用するよう設定されているかを確認するには、**Protect** のステータス(  )を選択します。  
アプリケーションが特定のサーバで Protect を使用するよう設定されていない場合は、サーバ名の横に警告アイコンが表示されます。



6. (任意)Protect を使用するようにアプリケーションを設定：
  - a. エージェントの設定ファイル (35ページ)で Protect の設定を true にします。
  - b. Protect を有効にするために、アプリケーションを再起動します。  
アプリケーションを再起動すると、Contrast は攻撃の監視、攻撃のブロック、および攻撃データの Contrast Web インターフェイスへの表示を開始します。



### 重要

エージェントの設定ファイルでの Protect の設定は、Contrast Web インターフェイスでの設定よりも優先されます。

## ライセンス適用の動き

次の条件の場合、サーバに自動的に Protect ライセンスが適用されます。

- 組織で Protect が有効である。
- 組織で Protect ライセンスの自動適用が有効である。
- サーバは、ライセンスの自動適用が有効になっている 1 つ以上の環境に存在する。

また、エージェントの設定ファイルで Protect の設定を使用する場合、ライセンス適用の動きは次のようになります。

- **エージェントの設定ファイルで Protect が有効**
  - アプリケーションの起動時に Protect ライセンスが利用可能な場合は、非常に短時間でサーバにライセンスが適用されます。エージェントがアプリケーションを登録すると同時に、自動的にライセンスが消費されます。
  - アプリケーションの起動時に利用可能な Protect ライセンスが無い場合は、エージェントが Contrast と通信するたびに、Contrast はサーバへのライセンスの適用を試みます。
- **エージェントの設定ファイルで Protect が無効**
  - アプリケーションの起動時に Protect ライセンスが利用可能な場合、サーバにライセンスが適用されます。アプリケーションが Contrast に登録されると、サーバに適用されたライセンスが消費されます。
  - アプリケーションの起動時に利用可能な Protect ライセンスが無い場合、サーバにライセンスは適用されません。

## 組織の設定を行う

組織管理者の権限(組織の Admin ロール)があるユーザは、組織の設定を行うことができます。



**組織の設定**

組織

グループ  
ユーザ  
セキュリティ  
エージェント  
シングルサインオン  
インテグレーション  
サーバ  
アプリケーション  
...

組織

グループ  
ユーザ  
セキュリティ  
エージェント  
シングルサインオン  
インテグレーション  
サーバ  
アプリケーション  
通知  
レポートの設定  
スコアの設定  
Access Control

一般情報 UUID: 119844AF-42FF-4293-B04B-81D426E9A4A9

組織名  
Test Org Testing RBAC 2018/07/09に作成

タイムゾーン  
(GMT-05:00) Eastern Time (US & Canada) 言語 English

日付形式  
MM/dd/yyyy 時刻形式  
hh:mm a

管理者

もっと見る

編集

**ライセンス**

Assess  
91ライセンス購入済 5,199アプリケーションがライセンスなし

72/91

新しいアプリケーションにライセンスを自動で適用

Protect  
2,120ライセンス購入済 1,759サーバがライセンスなし

487/2120

新しいサーバにライセンスを自動で適用

ライセンスを自動的に適用する環境を選択(複数可):

開発環境  QA  本番環境

一般設定

製品の使用状況分析  全てのサーバ環境に適用されます。  
パフォーマンスを向上させ製品の改善を優先付けるためにContrastのアクティビティデータを送信します。詳細

1. 組織管理者として Contrast Web インターフェイスにログインします。
2. 複数の組織がある場合は、**ユーザメニュー**より設定する組織の名前を選択します。
3. **ユーザメニュー**で、**組織の設定**を選択します。以下を設定できます。
  - 組織(一般情報 (706ページ)、ライセンス管理 (706ページ)、使用状況分析 (711ページ))
  - ユーザ、グループ、権限 (708ページ)
  - セキュリティ(パスワード (712ページ)、2段階認証 (712ページ)、IP 範囲 (712ページ)、Eメールドメインの制限 (712ページ))
  - API(組織キーとエージェントキーの表示)
  - シングルサインオン(SSO) (713ページ)
  - インテグレーション (618ページ)
  - サーバ (713ページ)
  - アプリケーション (715ページ)
  - 通知 (716ページ)

- [レポートの設定 \(719ページ\)](#)
- [スコアの設定 \(719ページ\)](#)

## 組織の一般情報の設定

1. [組織の設定 \(704ページ\)](#)より、左側のナビゲーションメニューから**組織**を選択します。
2. 右上にこの組織の UUID が表示されます(これは、[ユーザの一括登録 \(777ページ\)](#)の際に便利です)。
3. このパネルには、以下のように組織の一般的な情報も表示されます。
  - 組織の名前
  - 組織のデフォルトの日付形式と時刻形式
  - 組織のデフォルトの言語設定：日本語(スーパー管理者によって有効にされている場合)、英語、またはスペイン語



### 注記

個々のユーザ設定は、言語設定を除き、組織のほとんどの一般情報(時間や日付のフォーマットなど)よりも優先されます。ユーザの言語設定は、ユーザへの通知や電子メールなど、ユーザ固有の項目については、組織の言語設定よりも優先されます。ただし、組織レベルの通知など、組織に固有のものについては、ユーザの言語設定は組織の言語設定を上書きしません。

4. このパネルにある情報を変更するには、**編集**を選択します。
5. 変更を加えたら、**保存**を選択します。

## 組織、アプリケーション、サーバへのライセンス割当て

### 開始する前に

- 組織管理者のロール(Admin)が必要です。
- 割り当てられた Assess ライセンスが全て組織で使用された場合、SaaS 版をご利用のお客様は[弊社サポート](#)にお問い合わせください。
- オンプレミス版のお客様は、スーパー管理者(SuperAdmin ロールのユーザ)が[システムレベルで利用可能なライセンスを増やす \(803ページ\)](#)ことができます。

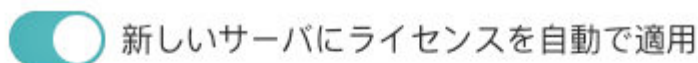
### 手順

1. 組織でのライセンス使用状況の概要を確認します。
  - a. ユーザメニューから、**組織の設定**を選択します。
  - b. **組織**を選択します。
  - c. **ライセンス管理**の下で、Assess ライセンスと Protect ライセンスについての情報を確認できます。
    - 使用可能および使用中の Assess(アプリケーション)ライセンス数、ライセンスなしのアプリケーションの数。
    - 使用可能および使用中の Protect(サーバ)ライセンス数、ライセンスなしのサーバの数。購入したライセンスより多くのライセンスを利用している場合は、ライセンスバーの使用可能なライセンス欄が、追加で使用中のライセンス数の表示に置き換わります。
2. (任意)**ライセンス管理**で、新しいアプリケーションやサーバにライセンスを自動的に適用するよう設定できます。
  - a. Assess ライセンスの場合、**新しいアプリケーションにライセンスを自動で適用**をオンにします。



新しいアプリケーションにライセンスを自動で適用

- b. Protect ライセンスの場合、新しいサーバにライセンスを自動で適用をオンにします。サーバの環境を選択します。



ライセンスを自動的に適用する環境を選択(複数可):

- 開発環境  QA  本番環境

エージェントの設定ファイルにある Protect の設定は、そのアプリケーションをホストするサーバのこの設定より優先されます。

例えば、この設定をオンにして、エージェント設定ファイルの Protect の設定を false にすると、そのアプリケーションをホストしているサーバの Protect は無効になります。Protect ライセンスは、そのサーバに適用されません。

3. 必要に応じて、個々のアプリケーションに対して Assess ライセンスを適用できます。
  - a. Contrast Web インターフェイスのナビゲーションバーでアプリケーションを選択します。アプリケーションの一覧で、ライセンスが付与されていないアプリケーションは、アプリケーション名の横にライセンスなしと表示されます。アプリケーションにライセンスが付与されていない場合、アプリケーションの脆弱性情報は表示されません。
  - b. ライセンスが付与されていないアプリケーションにライセンスを適用するには、ライセンスなしを選択します。
  - c. 「ライセンスを適用」画面で、ライセンスを適用を選択します。
4. 必要に応じて、アプリケーションを削除する (488ページ) ことによって、アプリケーションから Assess ライセンスを削除できます。アプリケーションに適用されたライセンスは、最大許容アプリケーション数に対して永続的にカウントされます。ライセンスが適用されたアプリケーションを削除しても、アプリケーションに許容されるライセンス数には影響はありません。
5. 必要に応じて、個々のサーバから Protect ライセンスを追加または削除できます。
  - a. Contrast Web インターフェイスのナビゲーションバーで、サーバを選択します。
  - b. サーバの Protect 設定をオンまたはオフにします。



- c. そのサーバがホストしているアプリケーションを再起動します。



#### 重要

エージェントの設定ファイルにある Protect の設定は、この設定より優先されます。

### Protect ライセンス適用の動き

以下の条件が揃う場合、サーバに自動的に Protect ライセンスが適用されます。

- 組織で Protect が有効である。

- 組織で Protect ライセンスの自動適用が有効である。
- サーバは、ライセンスの自動適用が有効になっている 1 つ以上の環境に存在する。

また、エージェントの設定ファイルで Protect の設定を使用する場合、ライセンス適用の動きは次のようになります。

- **エージェントの設定ファイルで Protect が有効**
  - アプリケーションの起動時に利用可能な Protect ライセンスが無い場合は、エージェントが Contrast と通信するたびに、Contrast はサーバへのライセンスの適用を試みます。
- **エージェントの設定ファイルで Protect が無効**
  - 組織の設定によりサーバの Protect がオフになっている場合、またはサーバを Contrast に登録後 Protect をオフにした場合は、ライセンスは適用されません。
  - 組織の設定によりサーバの Protect がオンになっている場合、またはサーバを Contrast に登録後 Protect をオンにした場合は、ライセンスは適用されますが、エージェントでは Protect はオフになります。

## 組織レベルでのユーザ、グループ、権限の管理

システムレベルで許可 (776ページ)されている場合、組織管理者(Admin ロールのあるユーザ)は以下の方法で組織のユーザ権限を管理できます。

- [ユーザを追加またはユーザ設定を編集する \(708ページ\)](#)
- [アクセスグループ \(708ページ\)](#)で組織の権限を管理する

## 組織レベルでのユーザの追加/編集

組織内でユーザを追加すると、その組織内のアプリケーションのアクセスグループにユーザを割り当てることができます。ほとんどの Contrast インストールでは、[デフォルト \(776ページ\)](#)ではロールと権限を組織レベルで設定しますが、複数の組織にアクセスする必要のあるユーザがいる場合は、[システムレベルにそれらのユーザを追加 \(775ページ\)](#)します。

ユーザを追加するには：

1. 組織の管理者権限(Admin ロール)のあるユーザとして、Contrast にログインします。
2. **ユーザメニュー**で、**組織の設定**を選択します。
3. 左側のナビゲーションで**ユーザ**を選択します。
4. 一覧からユーザ名を選択してエントリを編集するか、**ユーザを追加**を選択して新規ユーザを追加します。
5. ユーザについて、以下の項目を入力します。
  - **組織ロール**：この組織内の全てのアプリケーションに適用されるデフォルトの**組織ロール (819ページ)**の 1 つを選択するか、**カスタムアクセスグループを作成 (708ページ)**します。
  - **アプリケーションアクセスグループ**：この組織の全てのアプリケーションに適用されるデフォルトの**アプリケーションロール (817ページ)**の 1 つを選択するか、カスタムアクセスグループを作成して特定のアプリケーションへの特定の権限を付与します。
  - **アクセス権限**：ユーザに、API、Contrast の Web インターフェイス、Protect データへのアクセス権を付与できます(Protect 権限は、[システムレベルで付与 \(780ページ\)](#)することもできます)。



### ヒント

ユーザに管理者ロールを割り当てる場合は、API と Contrast の Web インターフェイスの両方についてアクセス権を付与するようにしてください。

6. **追加または保存**を選択します。

## 組織のアクセスグループの追加/編集/削除

組織のアクセスグループを使用して、[ロール \(817ページ\)](#)ごとにユーザに権限や機能を割り当てることができます。

Contrast ではデフォルトのアクセスグループを提供しており、自分で作成する代わりに使用することができます。

- **View** : このグループのメンバーは、Contrast インターフェイスに読み取り専用でアクセスし、スコア、ライブラリ、脆弱性、コメントなどを参照できます。
- **Edit** : このグループのメンバーは、検出結果の修復、タグの追加、脆弱性の管理、属性の編集、アプリケーションのマージ、アプリケーションの追加・削除、サーバの作成などが可能です。
- **Rules Admin** : このグループのメンバーは、アプリケーションのルールとポリシーの編集、Protect の有効化、通知とスコアの管理を行うことができます。
- **Admin** : このグループのメンバーは、組織の設定を構成し、管理することができます。

## 開始する前に

組織管理者のロール(Admin)が必要です。

## 手順

1. [組織の設定 \(704ページ\)](#)より、グループを選択します。
2. 既存のグループを選択して編集するか、**グループを追加**を選択して新しいグループを作成します。



### ヒント

グループを検索するには、クイックフィルターのドロップダウンまたは左上の検索フィールドを使用します。または、各列の上部にある上下方向の矢印を使用して並び替えを行います。

Contrast が提供するデフォルトグループはロックアイコン付きで表示されますが、アプリケーションとロールは固定されており、削除はできません。これらのデフォルトグループには、ユーザの追加か削除のみが可能です。

3. 画面で以下の項目に入力します。
  - **グループ名** : このグループに割り当てる権限、機能、目的を反映したものを選んでください。
  - **アプリケーションアクセス** : ここでアプリケーション名を選択すると、このグループとアプリケーションが関連付けられます。新しいアプリケーションを設定する際に、グループ名を指定することもできます。
  - **ロール** : このグループのメンバに対してアプリケーション内で持たせるアプリケーションロールを選択します。
  - さらにアプリケーションとロールを追加するには、**アクセスを追加**を選択します。
4. **メンバー**では、フィールドに文字を打鍵するとユーザが表示されるので、グループに割り当てる 1 人以上のユーザを選択します。
5. 入力が完了して**追加**を選択すると、新しいグループが作成されます。



### 注記

ユーザが、全てのアプリケーションや組織のロールに対して競合する 2 つのグループに割り当てられた場合は、アクセスの制限が最も厳しいロールが適用されます。

6. グループを削除するには、**ユーザメニュー > 組織の設定 > グループ**を選択します。削除するグループを探し、その行の削除アイコンを選択します。  
この操作を確定すると、グループが削除され、そのグループによって提供されたアクセス権が、そのグループに割り当てられた全てのユーザから取り消されます。



## ヒント

組織内の全てのアプリケーションに対するロールをユーザに割り当てるには、デフォルトロールグループの組織ロールとアプリケーションロールの両方を割り当てます(例、組織とアプリケーションの両方のロールに管理者権限である「Admin」を設定すると、組織内の全てのアプリケーションの管理者権限を持つことになります)。

特定のアプリケーションへのアクセス権をユーザに付与するには、そのアプリケーションのアクセスグループを作成し、そのグループにユーザを追加する必要があります。どのアプリケーションアクセスグループにも割り当てられていないユーザは、アクセスがありません。ユーザは、1つの組織内の各アプリケーションで様々なロールを持つことができます。

Contrast のほとんどのお客様は、単一の組織で展開しています。組織レベルで作成されたグループは、その組織全体のロールと権限に影響を与えます。組織のアクセスグループをシステムレベル (779ページ) で作成し、ユーザを複数の組織にアクセスさせることも可能です。

## API のみのユーザの作成

全てのプラグインやインテグレーションで使用できる、API のみのユーザを作成します。

**参考:** ベストプラクティスとして、プラグインやインテグレーションを使用するためだけのユーザアカウントを登録することを推奨します。この専用ユーザにより、あるユーザが会社や組織を離れた際に、使用しているプラグインやインテグレーションが機能するよう継続できます。そのユーザアカウントが削除されて問題が発生するような状況を避けることができます。

API のみのアカウントは、通知設定が有効になっている場合でも、電子メールの通知を受信しません。

## インストールを行う前に

- 組織の Admin ロールが必要です。
- API のみのユーザは、Contrast の REST API にアクセスできますが、Contrast Web インターフェイスにはログインできません。

## 手順

API のみのユーザを作成するには :

1. ユーザメニューから、**組織の設定**を選択します。
2. **ユーザ**を選択します。
3. **ユーザを追加**を選択します。

**+ ユーザを追加**

4. ユーザの名前と名字、メールアドレスを入力し、タイムゾーンを選択します。
5. **組織ロール**を選択します。  
**参考:** ベストプラクティスとして、組織ロールには **Edit (819ページ)** を選択して、最小の許容ロールを付与します。  
API のみのユーザに Admin 権限を付与することは推奨されません。
6. **アプリケーションアクセスグループ**を選択します。  
**参考:** ベストプラクティスとして、アプリケーションアクセスグループには **View (817ページ)** または **Edit (817ページ)** を選択します。呼び出したい API エンドポイントや、GET(読み取り)や POST(書き込み)を実行する場合には、API のみのユーザには View ではなく、より高い Edit 権限が必要になることがあります。

## 7. API のみのチェックボックスを選択します。



## 注記

API のみのチェックボックスをオンにすると、アクセスのオプションがオンになっている場合は無効になります。API のみのユーザは、Contrast Web インターフェイスにアクセスできません。

## 8. 組織の設定 &gt; ユーザで、新規に作成したユーザ名の横に API のみのラベルがあることを確認します。

| 名前 (ユーザ名)                      | ステータス | 組織ロール | 前回のログイン | UI利用                                | サーバーレス                   | Protect                  |
|--------------------------------|-------|-------|---------|-------------------------------------|--------------------------|--------------------------|
| Smith Jane<br>ApiUser@acme.com | APIのみ | Edit  |         | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

9. 特定のアプリケーションに対してアクセスを制限するためにアクセスグループを使用している場合は、API ユーザにアクセスさせたいアプリケーションのグループ (708ページ) に、API のみのユーザを追加します。ユーザの設定の権限でアクセスを確認してください。
10. API のみのユーザを使用するには、接続文字列を取得します。
  - a. ユーザメニューから、組織の設定を選択します。
  - b. ユーザを選択します。
  - c. ユーザ名の横にある API のみのラベルにカーソルを合わせ、表示されたサービスキーをコピーします。
  - d. 以下の例のように、コマンドを使用して認証ヘッダを作成します。

```
echo -n `[email address of the API only account:Service Key]' | \
base64
```

## 使用状況分析の管理

Contrast では、より良い製品を開発するために使用状況のデータを収集しています。お客様のデータは追跡されず、全てのユーザデータは匿名化されて、集約された情報に対して分析が行われます。

組織管理者は、組織の使用状況データの収集を有効/無効にできます。

1. 組織の設定 (704ページ) で、組織を選択します。
2. 一般設定で、トグルボタンを使用して製品の使用状況分析を有効/無効にします。デフォルトでは有効になっています。

診断サービスもシステムレベルで管理 (802ページ) できます。

## 組織レベルでのパスワードポリシーの設定

システムレベルで許可 (798ページ) されている場合は、組織管理者はパスワードポリシーを作成し、組織内のパスワードを規制することができます。

1. **組織の設定 (704ページ)** で、**セキュリティ** を選択します。
2. ポリシーについて、以下の設定を入力します。
  - パスワード強度：弱、中、強、複雑またはカスタムを選択できます。  
カスタムを選択した場合は、**最小限必要な大文字、小文字、数字、記号の文字数**を入力します。
  - 必要な文字数を**最小桁数**フィールドに入力します。
  - ドロップダウンを使用して、**パスワード期限**が切れるまでの時間を選択します。
  - **ログインのロックアウト**までのログイン試行回数を入力します。
  - **非アクティブアカウントの有効期限**が切れるまでの時間を選択します。
  - **パスワードの再利用を制限**のチェックボックスをオンにし、ドロップダウンを使用して、各パスワードを再利用できる回数を選択します。
  - **パスワードのリセットを制限**のチェックボックスをオンにし、ドロップダウンを使用して、リセットのリクエストの送信後にユーザがパスワードをリセットできる日数を選択します。
  - ドロップダウンを使用して、**アイドルタイムアウト**および**セッションタイムアウト**までの経過時間を選択します。
3. **保存**を選択します。

## E メールドメインの制限

Contrast の情報を受信できる E メールアドレスのドメインを制限します。

1. 組織の設定で、**セキュリティ** を選択します。
2. **E メールドメイン**に、Contrast からの情報の受信を許可する E メールドメイン名をカンマ区切りで入力します。例えば、yourbusiness.com のように入力します。
3. **保存**を選択します。

## IP 範囲の設定

Contrast アカウントにアクセスできる IP アドレスを制限します。これは、ブラウザと API の両方のアクセスに影響します。

1. **組織の設定 (704ページ)** で、**セキュリティ** を選択します。
2. アクセスを許可する IP アドレスを入力します。追加アドレスを入力するには、**IP アドレスを登録**を選択します。CIDR 表記(10.0.0.0/24)を使用して、IP アドレスの範囲を指定することもできます。
3. **保存**を選択します。

## 組織レベルでの 2 段階認証の有効化

2 段階認証を有効/無効にするには：

1. **組織の設定 (704ページ)** で、左側のナビゲーションにある**セキュリティ**を選択します。
2. トグルボタンをオン(緑色)にして 2 段階認証を有効にします。
3. 2 段階認証が有効になり、ユーザは **2 段階認証の通知を受け取る方法を選択 (478ページ)** できます。



### 注記

オンプレミス版のお客様の場合、これは**システムレベルで許可 (786ページ)**されている必要があります。

ユーザが複数の組織に属している場合は、デフォルトの組織によって 2 段階認証の設定が決まります。



## 組織レベルでのシングルサインオン(SSO)の設定

オンプレミス版のお客様の場合は、シングルサインオンをシステムレベルで設定 (795ページ) できます。SaaS 版のお客様の場合は、Contrast Security が認証を設定しますが、組織管理者に組織の SSO を設定する権限が付与される場合があります。



### 注記

ユーザがメールアドレスではなくユーザ ID で識別されている場合、それらのアカウントは自動的に SSO 設定に移行されず、再作成する必要があります。

1. 組織の設定でシングルサインオンを選択して、**開始する**のリンクをクリックします。
2. 認証方法の変更による影響に関して、警告メッセージが表示される場合があります。警告をよく読んでから作業を進めてください。
3. 提供された情報を使用して、Contrast と IdP との設定を行います。
4. IdP の名前と、Contrast と接続するための関連メタデータを入力します。
5. Contrast にログインするための SAML リクエストがあった時に、新しいユーザアカウントを自動的に作成する場合は、**ユーザプロビジョニングを有効にする**のボックスにチェックします。
  - ドロップダウンを使用して、新規ユーザのデフォルトの**組織ロール**と**デフォルトのアプリケーションアクセスグループ**を選択します。
  - ユーザプロビジョニングをトリガーするのに必要な**承認されているドメイン**を追加します(例: contrastsecurity.com)。
6. **接続をテスト**ボタンをクリックして、設定をテストします。エラーが発生した場合は、トラブルシューティングのためのデバッグログが提供されます(このテストでは、メタデータの検証と、Contrast が IdP と接続できるかのみを検証します)。
7. テストが成功したら、**保存**を選択します。
8. **新しいブラウザ画面**、**プライベートブラウザのセッション**または**シークレットウィンドウ**を開いて、自分のアカウントで SSO ログインを試してください。ログインに失敗した場合は、ログイン状態のブラウザに戻り、組織の SSO を無効にしてから、Contrast 管理認証に戻すを選択します。

### 関連項目

[Okta を使用してユーザとグループのプロビジョニングを設定する](#)

[グループにユーザを自動的に追加するように ADFS を構成する](#)

## 組織レベルでのサーバのデフォルト設定

サーバの設定では、Contrast に追加する新しいサーバ(およびそのエージェント)に対するデフォルトの設定を定義します。これらの設定をカスタマイズして、各環境ごとに特定のデフォルトを設定することができます。

### 開始する前に

- 組織管理者のロール(Admin)が必要です。

### 手順

1. **組織の設定 (704ページ)**で、**サーバ**を選択します。
2. ドロップダウンを使用して、デフォルトにする**環境**(開発、QA、本番環境のいずれか)を選択します。サーバのデフォルトの環境に指定する場合、**デフォルト環境**として**設定する**の横にあるチェックボックスをオンにします。
3. ドロップダウンを使用して、**ログレベル**を選択します。デフォルトの**ログレベル (765ページ)**は、**ERROR** が選択されます。

4. **サーバクリーンアップを自動化オプション**では、サーバがオフラインになってから自動的にクリーンアップされるまでの時間を指定します。デフォルトの値は、30 日です。  
バックグラウンドタスクが 5 分ごとに実行され、自動サーバクリーンアップが有効になっている組織があるかどうかチェックが行われます。  
設定された時間内にアクティビティが受信されなかったサーバが 1 つ以上ある場合、サーバは自動的に無効になります。無効になったサーバは、Contrast Web インターフェイスのサーバ画面に表示されなくなります。  
サーバが無効化された後も、そのサーバに関連する脆弱性や攻撃の情報は Contrast に保持されま  
す。無効化されたサーバの Protect ライセンスは、ライセンスプールに戻されます。
5. **Assess** セクションでは、以下を設定します。
  - a. キャプチャするスタックトレースを選択します。ALL(全て)、SOME(一部)、NONE(なし)から選択します。
  - b. **パフォーマンス向上のためサンプリングを有効にする**を選択すると、解析のパフォーマンスが最適化されます。
    - Contrast で同じ URL が複数回呼び出されているのが確認された場合、「基準」に指定された回数に基づいて URL が解析されます。
    - その後、Contrast で同じ URL が引き続き確認された場合、「頻度」の設定に基づいてのみチェックが行われます。
    - サンプルは、「サンプル保持」の設定で指定した秒数だけ保持されます。「サンプル保持」の設定で指定した時間が経過すると、「基準」の設定に従って再度 URL が解析されます。以下を設定します。
    - **基準**：サンプリングが完了するまでに、Contrast で URL を解析する回数。デフォルトの設定は、5 です。
    - **頻度**：基準のサンプル回数を取得後、毎回 N 番目のリクエストのみを解析します。頻度には、N の値を指定します。デフォルトの設定は、10 です。
    - **サンプル保持画面**：基準に戻る前に、Contrast でサンプルを保持する秒数。指定した秒数が経過すると、サンプリングはリセットされ基準サンプルが再度行われます。デフォルトの設定は、180 です。
6. **Protect** セクションでは、以下を設定します。
  - a. Protect を有効にするには、Protect トグルをオンにします。



### 重要

Protect を有効にすると、新しいサーバに Protect ライセンスを自動的に適用する設定が選択されます。

管理者は、サーバにライセンスが適用されるたびに E メールを受け取ります。サーバが頻繁にアップ/ダウンしたりする場合に、不要なトラフィックに対してメールのフィルタを設定するとよいです。

- このセクションのライセンスバーには、購入済みの Protect ライセンスで使用中のライセンス数が表示されます。購入したライセンス数よりも多くのライセンスを使用している場合は、ライセンスバーには追加で使用中のライセンス数も表示されます。
- b. **ポットのブロックを有効にする**を選択すると、ポットのブロックがオンになります。  
ポットをブロックすることで、スクレーパー、攻撃ツール、その他の自動化からの不要なトラフィックをブロックできます。  
ブロックされたポットのアクティビティを表示するには、**攻撃 > 攻撃イベント**で、**自動化フィルター**を使用します。



### 注記

ポットのブロックは、各言語(Java、.NET Framework、.NET Core、Ruby、Python)のエージェントの [YAML 設定ファイル \(38ページ\)](#) で指定できます。

- c. **Syslog へ Protect イベントの出力を有効にする**を選択すると、Protect イベントが syslog に送信されます。  
以下を設定します。
  - 所定のフィールドに **IP アドレス**と **ポート**を入力します。ドロップダウンを使用して**機能**を選択します。
  - 攻撃イベントの深刻度バッジをクリックして、ドロップダウンを使用し、Syslog の各メッセージの**重要度**を選択します。デフォルトは次の通りです。
    - 「攻撃検出済」は、**1 - Alert** になります。
    - 「ブロック済」は、**4 - Warning** になります。
    - 「探査検出」は、**5 - Notice** になります。
7. **ライブラリデータを保持**のトグルをオンにすると、ライブラリのデータを保持する機能が有効になります。この機能を有効にすると、サーバのクリーンアップ時に、Contrast から最後に削除されたサーバのライブラリデータが保持されます。
8. **エージェント診断**のトグルをオンにすると、エージェントのデータが Contrast に送信されます。Contrast では、このデータをルールやパフォーマンスの改善、製品改良の優先順位付けのために使用します。

## 組織レベルでのアプリケーションのデフォルト設定

組織レベルでアプリケーションのデフォルト設定を選択するには、以下の手順を使用します。

### 開始する前に

- 組織の Admin ロールが必要です。

### 手順

1. **組織の設定 (704ページ)**で、**アプリケーション**を選択します。
2. ドロップダウンを使用して、アプリケーションの**重要性**レベルを選択します。**重大**、**高**、**中**、**低**、**重要でない**から選択できます。デフォルトでは、「中」が選択されます。
3. **ポリシー**のドロップダウンでは、自動的にアプリケーションに適用する修復ポリシーや**コンプライアンスポリシー (695ページ)**を選択します。  
デフォルトの設定に含まれないアプリケーションは、後からポリシーに追加することもできます。
4. 「セッションメタデータ」では、デフォルトの**セッションメタデータのフィルタリング (489ページ)**を最新のセッションに設定する場合、**最新のセッションでアプリケーションの詳細をフィルタリング**を選択します。  
この設定は、アプリケーションの「脆弱性」タブと「ルートカバレッジ」タブに影響があります。
5. ライセンスを自動で適用する場合、「動作」の欄で**新しいアプリケーションにライセンスを自動で適用**を選択します。  
ステータスバーには、使用可能なライセンス数のうち、使用されているライセンス数が表示されます。ライセンスのリンクを選択すると、組織のライセンスの内訳を参照することができます。
6. **カスタムフィールド**セクションを使用して、組織の各アプリケーションで利用するのに必要な**カスタムメタデータを設定 (715ページ)**します。
7. **保存**を選択します。

### アプリケーションメタデータを要求するカスタムフィールドの作成

Contrast に新しいアプリケーションを追加するたびにカスタムメタデータが収集されるように設定できます。

**エージェントをインストールして設定する (35ページ)**際に、作成したカスタムフィールドのメタデータを入力して、エージェントの設定ファイルに情報を追加するよう要求できます。メタデータは、**アプリケーション**ページの一覧に表示され、メタデータを使用してアプリケーションをフィルタリングすることができます。また、Contrast Web インターフェイスのアプリケーションの**詳細**ページにもメタデータは表示されます。



### 注記

カスタムメタデータフィールドは、以下のエージェントバージョンでサポートされません。

- Java 3.5.6.591 以降
- .NET 18.10.35 以降
- Node 1.35.0
- Python 1.2.0
- Ruby 2.0.8



### 重要

カスタムフィールドに提供するデータは、エージェントの設定および YAML ファイルのダウンロードに必要です。このデータが指定されないと、ダウンロードは有効になりません。

## 開始する前に

- 組織管理者のロール(Admin)が必要です。

## 手順

1. 組織の設定で、**アプリケーション**を選択します。
2. カスタムフィールドで、各フィールドに以下の項目を入力します。
  - **フィールドタイプ**：フリーフォーマット、数値、連絡先のいずれかを選択します。フィールドタイプにより、適切な検証が決定されます。
  - **名前**：カスタムフィールドの名前を入力します。  
Contrast API と互換性を保つために、先頭を小文字にしたキャメルケース(camel-case)の表記を使用します。例えば、BusinessID や Business ID ではなく、businessID を使用します。
  - **値の条件**：チェックボックスを使用して、提供されるメタデータの値を**必須がユニークにするか**を指定します。
3. **フィールドを追加**を選択して、必要な行を追加します。
4. 各フィールドに情報を入力すると、フォーマットされたプロパティが表示されるので、エージェントの設定ファイルにコピー&ペーストします。エージェントの設定ファイルには、key=value(キー=値)の形式でメタデータ情報を追加します。
5. 必須フィールドが含まれていないアプリケーションのデータを報告しないようにする場合は、**必須フィールドが足りないアプリケーションを制限する**のチェックボックスを選択します。これは、組織の新規のアプリケーション、もしくは新規と既存のアプリケーションに適用できます。  
このオプションを選択すると、アプリケーションで必須フィールドが指定されていない場合、Contrast Web インターフェイスで警告メッセージが表示されます。Contrast Web インターフェイスにはアプリケーションは表示されますが、エージェントからは、疎通済ルートや脆弱性などのデータは報告されません。  
アプリケーションを制限しない場合は、必須フィールドが指定されていないアプリケーションでも正常に登録され、エージェントからデータが報告されます。Contrast Web インターフェイスには、1つ以上のフィールドが足りないという警告メッセージが表示されます。

## 組織レベルでの通知の管理

通知により、ユーザは脆弱性の検出やアプリケーションへの攻撃など、特定の状況に関するアラートを受信することができます。組織管理者は、組織内の全てのユーザに対して Contrast の通知の**デフォルト**

を設定 (717ページ)できます。個々のユーザは、各種の通知を受け取る方法を選択 (479ページ)できます。

通知には主要なチャネルが 2 つあります。

- **Contrast 内**：直接 Contrast Web インターフェイス内に通知されます。通知を確認するには、トップメニューにある通知アイコンを選択します。
- **E メール**：適切な SMTP システムと通信して通知を E メールで受信するよう、システム管理者が Contrast を設定 (807ページ)します。



### 注記

Contrast では、ユーザ通知が必要な一部の機能について Contrast 管理者がその機能を有効にすると、影響を受けるユーザに自動的に通知が送信されます(この通知は通知ページでは制御できません)。Contrast では、脆弱性ステータスの承認 (735ページ)やその他のポリシーの管理の設定などの機能について、ユーザと管理者に通知する必要があります。

## 管理者用通知の設定

管理者は、Contrast アプリケーション内と E メールで、組織全体のイベントに関する以下の通知を自動的に受信します。

- **アプリケーションライセンスの付与**：Contrast で新しいアプリケーションにライセンスが付与 (706ページ)された。
- **アプリケーションライセンス期限切れ間近**：有効なアプリケーションのライセンスの期限が切れる (ライセンス有効期限の 2 か月前、1 か月前、1 週間前にこの通知が送信)。
- **ライセンス期限切れ間近**：関連付けられたアプリケーションの無い既存のライセンスの期限が切れる (ライセンス有効期限の 2 か月前、1 か月前、1 週間前にこの通知が送信)。
- **修復ポリシーの違反**：脆弱性が既存の修復ポリシー (674ページ)に違反している。
- **ライブラリポリシーの違反**：ライブラリが既存のライブラリポリシー (698ページ)に違反している。
- **コンプライアンスポリシーの通知**：アプリケーションが既存のコンプライアンスポリシー (695ページ)に違反している。

アプリケーションおよび組織レベルの Admin および RulesAdmin ユーザは、ポリシー違反の通知を受信する必要があります。通知を管理 (479ページ)することで、通知件数を最小限にしたり、1 つのメールに通知をまとめたりすることができます。

また、ユーザが特定の脆弱性をクローズしようクエストした時に、承認を得るための通知を受信することができます。これは、組織管理者が設定 (735ページ)する必要があります。

## ユーザのデフォルトの通知設定

組織管理者は、組織内の全てのユーザを対象に、インテグレーションおよび Contrast 内/E メールでの通知に関するデフォルトの通知設定を定義できます。個々のユーザは、各種の通知を受け取る方法を選択 (479ページ)できます。

組織でのデフォルトの通知設定を定義するには：

1. **組織の設定 (704ページ)**で、通知を選択します。
2. トグルボタンを使用して、左側に表示されている通知登録を有効/無効にします。
  - **積極的な攻撃**：Protect が有効なアプリケーションで積極的な攻撃が発生。
  - **新しい脆弱性**：Contrast で新たに脆弱性を検出。フィールドをクリックして、特定の深刻度レベルや「ライブラリ(Library)」を指定します。デフォルトでは、「全て」が選択されます。

- **サーバのオフライン**：サーバへのアクセス不可。
- **新しいコメント**：チームメンバーが検出結果についてコメントを投稿。
- **新しいアセット**：アクセス権限のある新しいアセットが追加。フィールドをクリックすると、「アプリケーション」が「サーバ」のいずれかに通知を設定できます。デフォルトでは「全て」が選択されます。
- **Eメールダイジェスト**：Contrastの毎日のアクティビティをまとめたものです(Eメールのみ)。



### 注記

特定のインテグレーションの通知登録を有効にするには、**インテグレーションを追加**を選択してインテグレーションを追加します。または、インテグレーション列の上部にあるドロップダウンから既存のインテグレーションを選択します。

## カスタム通知の作成

組織の管理者は、通知のデフォルト設定を指定したり、カスタム通知を作成したりすることができます。

カスタム通知を作成するには：

**組織の設定 > 通知 > カスタム通知**にアクセスし、**通知を作成**を選択します。表示される画面で、次のフィールドに入力します。

1. ラジオボタンを使用して、**脆弱性が攻撃**を選択します。
2. 通知の**名前**を入力します。
3. ドロップダウンを使用して、通知の**頻度**を、またはに設定します。
4. 通知の目的などを**説明**に入力します。
5. フィールドをクリックして(複数選択可)、この通知が適用される**アプリケーション**を選択します。
6. この通知に適用する**アプリケーションのタグ**を選択します。
7. 通知を受信する組織の**ユーザ**を選択します。
8. ドロップダウンを使用して、**条件**を選択します。

条件を追加するには、**条件を追加**をクリックします。

Contrastのカスタム通知には、以下の条件を指定できます。

| 通知タイプ            | 条件               | 説明                                                                                             |
|------------------|------------------|------------------------------------------------------------------------------------------------|
| カテゴリ (Category)  | 等しい(=)、等しくない(≠)  | カテゴリとは、認証やインジェクション、暗号化などのルールタイプに関する上位レベルのグループです。Contrastのルールタイプには、11のカテゴリがあります。                |
| 影響度(Impact)      | 等しい(=)、より低い、より高い | 影響度とは、ルールタイプが特定の組織にどのように影響するかに基づいて、高、中、低の評価で測定されます。全てのルールタイプには、デフォルトの影響度が設定されていますが、カスタマイズできます。 |
| 可能性 (Likelihood) | 等しい(=)、より低い、より高い | 可能性とは、ルールタイプが発生する頻度に基づいて、高、中、低の評価で測定されます。すべてのルールタイプには、デフォルトの可能性が設定されていますが、カスタマイズできます。          |
| URL              | 等しい(=)、含む、一で始まる  | アプリケーションの特定のURLです。                                                                             |
| クラス (Class)      | 等しい(=)、含む、一で始まる  | Javaまたは.NETの特定のクラスです。                                                                          |
| メソッド (Method)    | 等しい(=)、含む、一で始まる  | Javaまたは.NETの特定のメソッドです。                                                                         |



### 重要

複数の条件を選択した場合、ContrastはANDロジックで通知を行います。選択した条件が全て該当した場合に通知が生成されます。

## レポートのデフォルト設定

レポートの設定では、組織管理者が[セキュリティ基準レポート \(613ページ\)](#)のテンプレートを定義する単独のインターフェイスを提供します。

1. [組織の設定 \(704ページ\)](#)で、[レポートの設定](#)を選択します。
2. 組織内で作成されるレポートのデフォルト値を定義します。
  - [レポートの種類](#)：レポートの種類を選択します。
  - [脆弱性のステータス](#)：確認済、問題無し、修復済、報告済、修正完了から選択します。
  - [脆弱性のタグ](#)：指定のタグが付いている全ての脆弱性に適用されます。
  - [含む内容](#)：脆弱性ステータスや脆弱性に関する備考をレポートに含む場合はチェックボックスをオンにします。
  - [カスタムフッタ](#)：レポートに表示するカスタムフッタを追加します。
3. レポートを生成して結果を確認できます。レポート生成画面ではデフォルト値が事前に入力されて表示されますが、ユーザは必要に応じて変更できます。

## 組織レベルでのスコア設定のカスタマイズ

Contrast では[アプリケーションのスコア \(822ページ\)](#)が算出されますが、必要に応じて[ライブラリのスコア \(544ページ\)](#)に依存させることができます。組織レベルでスコア設定をカスタマイズするには：

1. [組織の設定 \(704ページ\)](#)で、[スコアの設定](#)を選択します。
2. [総合スコア](#)では、この組織内のアプリケーションをどのようにスコア付けするかを選択します。
  - [デフォルトの評価方法](#)は、アプリケーションのライブラリスコアとカスタムコードのスコアの平均です。
  - [カスタムコードのみを評価対象とする](#)場合は、アプリケーション全体のスコア計算にライブラリのスコアが含まれなくなります。このオプションを選択した場合、特定の言語を選択するか、全ての言語に適用するかを、クリックして選択します。
3. [ライブラリのスコア](#)で、アプリケーション内のライブラリをどのようにスコア付けするかを選択します。
  - [デフォルトの評価方法](#)では、ライブラリの脆弱性だけでなく、ライブラリの古さやバージョン管理を含むアルゴリズムが使用されます。
  - [脆弱性のみを評価対象とする](#)方法では、ライブラリに存在する脆弱性のみに基づいてスコア付けされます。
4. [保存](#)を選択します。



### ヒント

ルール管理者(Rules Admin)は、[ポリシーの管理](#)でポリシーの設定を行い、ポリシーに違反するライブラリを自動的に低いスコア(F)にすることができます。この設定が選択されると、スコアの設定に警告メッセージが表示されます。警告にあるポリシーのリンクをクリックすると、ライブラリポリシーページに移動します。ここで、管理者はそれらの設定を確認して更新ができます。

## Contrast Scan のロールベースのアクセス制御

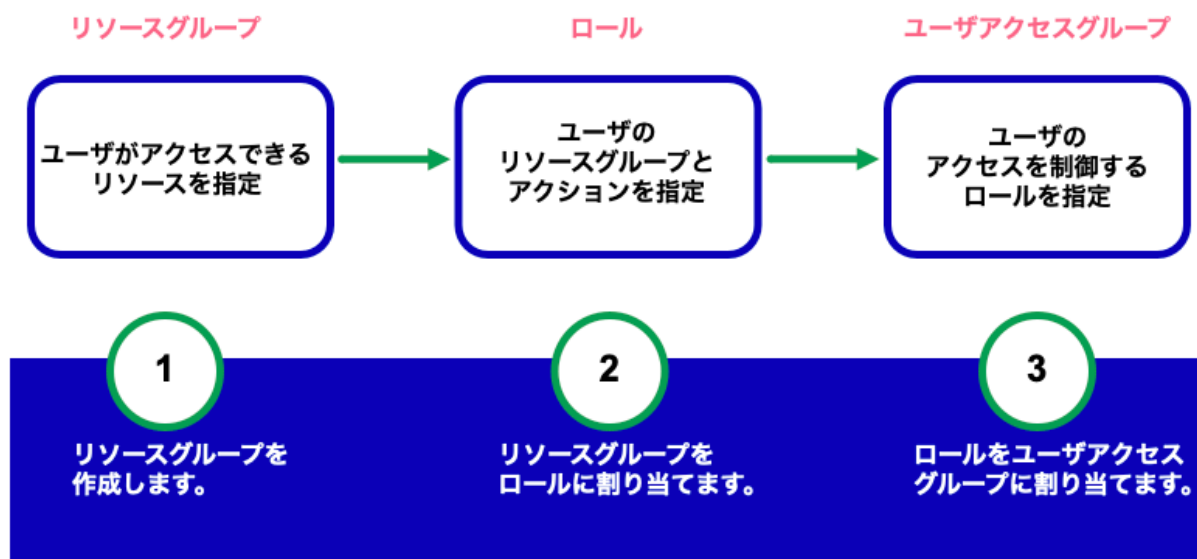
ユーザに Contrast Scan へのアクセス権を与えるには、リソースグループ、ロール、およびユーザアクセスグループを設定します。



### 注記

Contrast Web インターフェイスで、組織の設定にこのアクセス制御(Access Control)の設定が表示されていない場合は、[Contrast サポート](#)までご連絡ください。

Contrast のその他の機能のアクセス管理は、[組織レベルでユーザとアクセスグループ \(708ページ\)](#)を設定します。



## アクセス制御の設定

Scan のアクセス制御には、以下の設定が必要です。

- **リソースグループ : (721ページ)** リソースグループとは、割り当てるロールに従って、どのスキャンプロジェクトにアクセスできるかを決定するものです。  
標準のリソースグループを使用することも、カスタムグループを作成することもできます。
- **ロール : (725ページ)** ロールとは、ユーザが実行権限を持つスキャン操作を定義するものです。  
標準のロールを使用することも、カスタムロールを作成することもできます。  
標準の「RBAC Admin」ロールは、組織の Admin ロールがある全てのユーザに自動的に含まれます。  
この標準ロールは、Contrast Scan の全てのユーザアクセスグループ、ロール、およびリソースグループを管理することができます。
- **ユーザアクセスグループ : (730ページ)** ユーザアクセスグループとは、ユーザにロールを割り当てるものです。  
標準のユーザアクセスグループを使用することも、カスタムのユーザアクセスグループを作成することもできます。

## アクセス制御の管理方法

アクセス制御を管理するには、以下のいずれかの方法を使用します。

- **Contrast Web インターフェイス**  
Contrast Web インターフェイスを使用すると、アクセス制御の設定と管理を視覚的に行えます。この方法には、組織の Admin ロールが必要です。
- **アクセス制御の API**  
アクセス制御の管理を自動化したい場合や、既存のシステムに統合したい場合に、アクセス制御 API を使用すると便利です。この方法には、PLATFORM\_ORG\_MANAGE 権限が必要です。



詳しくは、[アクセス制御の API](#) をご覧ください。

## 命名規則と要件

リソースグループ、ロール、およびユーザアクセスグループの名称は、各組織で一意にする必要があります。例えば、**MyAdmins** という名前のロールを 2 つ作成することはできません。

カスタムのロールやグループを作成する前に、すべてのカスタム要素の命名規則の定義を検討することをお勧めします。命名規則を定義しておくことで、多数のカスタム要素の管理が容易になります。1 つの方法として、リソースグループの名前を、そのグループに関連付けるロールとマップさせる方法があります。例えば、**Ecommerce** というリソースグループを作成する場合、**Ecommerce Developer** というロール名などは適切でしょう。この場合、このロールのあるユーザは、e コマースのアプリケーションに携わる開発者と定義することができます。

すべてのカスタム要素の要件は、以下の通りです。

- 名前には、最大 50 文字まで使用できます。
- 説明文には、最大 1024 文字まで使用できます。
- 名前と説明文には、特殊文字やスペースを使用できます。

## Contrast Scan のリソースグループ

リソースグループは、ユーザがアクセスできる Contrast Scan の機能を、割り当てたロールに基づいて指定することができます。



### 注記

現在、リソースグループでサポートされているのは、スキャンプロジェクトのみです。

## リソースグループ(Resource groups)タブ

「Resource groups」タブには、既存のグループの一覧が表示されます。このタブから、次のことを行えます。

- リソースグループの一覧を表示  
検索を使用して、特定のグループを見つけることができます。
- リソースグループの管理
  - [Contrast Scan のリソースグループを追加 \(722ページ\)](#)
  - [Contrast Scan のリソースグループを編集 \(723ページ\)](#)
  - [Contrast Scan のリソースグループを削除 \(724ページ\)](#)

The screenshot shows the Contrast Security web interface. The top navigation bar includes 'Contrast', 'Applications', 'Scans', 'Servers', 'Libraries', 'Vulnerabilities', 'Attacks', and 'Serverless'. A search bar and a '+ Add new' button are on the right. The main content area is titled 'Organization Settings' and has tabs for 'Resource Groups', 'Roles', and 'User Access Groups'. The 'Resource Groups' tab is selected. On the left is a sidebar menu with items like 'Organization', 'Groups', 'Users', 'Security', 'Agent', 'Single Sign-On', 'Integrations', 'Servers', 'Applications', 'Notifications', 'Report Settings', 'Score Settings', and 'Access Control'. The main area has a search bar with the text 'Search' and a '+ Add Group' button. Below is a table with two columns: 'RESOURCE GROUP' and 'DESCRIPTION'. The table contains two rows: 'All Projects' with description 'All Projects' and 'Ecommerce projects' with description 'Ecommerce applications'. Each row has edit and delete icons. At the bottom, it shows 'Page 1 of 4' and 'Results per page 10 25 50'.

## Contrast Scan の標準リソースグループ

次の標準リソースグループを、Contrast Scan のロールに選択することができます。

- **All projects** : 組織内の全てのスキャンプロジェクトを含める



### 注記

標準リソースグループの設定を変更することはできません。

## Contrast Scan のリソースグループの追加

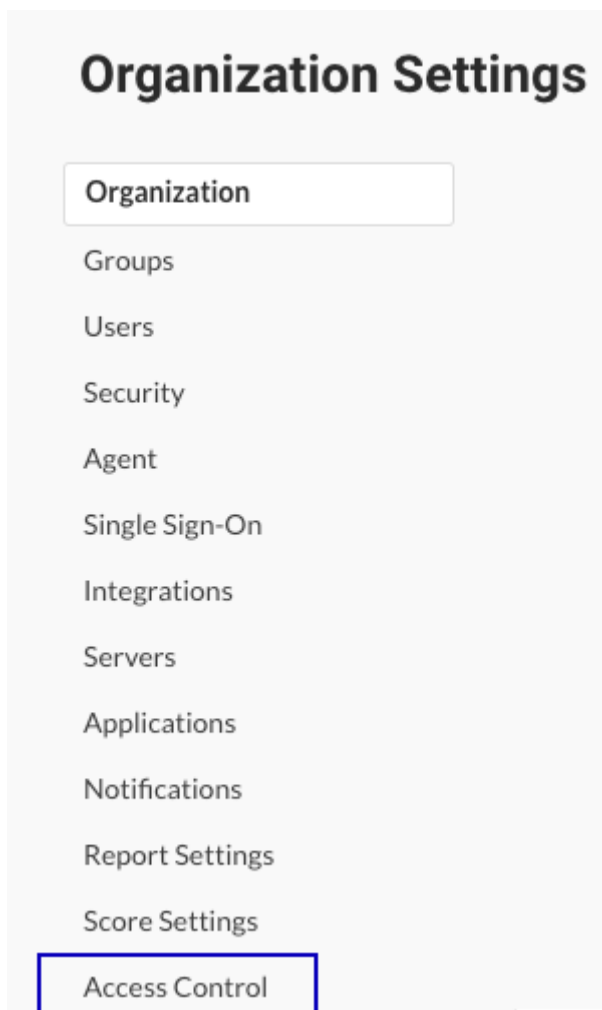
リソースグループを使用して、ユーザがアクセスできる Scan コンポーネントを指定します。現在、サポート対象となっているリソースは、スキャンプロジェクトのみです。

### 開始する前に

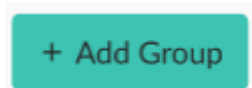
- 組織の Admin ロールが必要です。

### 手順

1. ユーザーメニューから、**組織の設定**を選択します。
2. **Access control** を選択します。



3. **Resource groups** タブを選択します。
4. **Add Group** を選択します。



5. 「Add resource group」の画面で、以下の設定を行います。

?

- **Resource group name** : リソースグループの名前を入力します。  
名前は、組織内で一意である必要があります。スペースや特殊文字を含め、最大 50 文字まで使用できます。
  - **Resource group description** : リソースグループの説明を入力します。  
このリソースグループの目的が分かるような説明を入力してください。スペースや特殊文字を含め、最大 1024 文字まで使用できます。
  - **Resource groups** : このグループに含めるリソースグループを選択します。  
リソースグループを選択した場合、個々のプロジェクトの選択は任意です。
  - **Projects** : このグループに含めるスキャンプロジェクトを個々に選択します。  
プロジェクトを選択した場合、リソースグループの選択は任意です。
6. **Add** を選択します。  
これで、このリソースグループをロールに割り当てることができます。

### Contrast Scan のリソースグループの編集

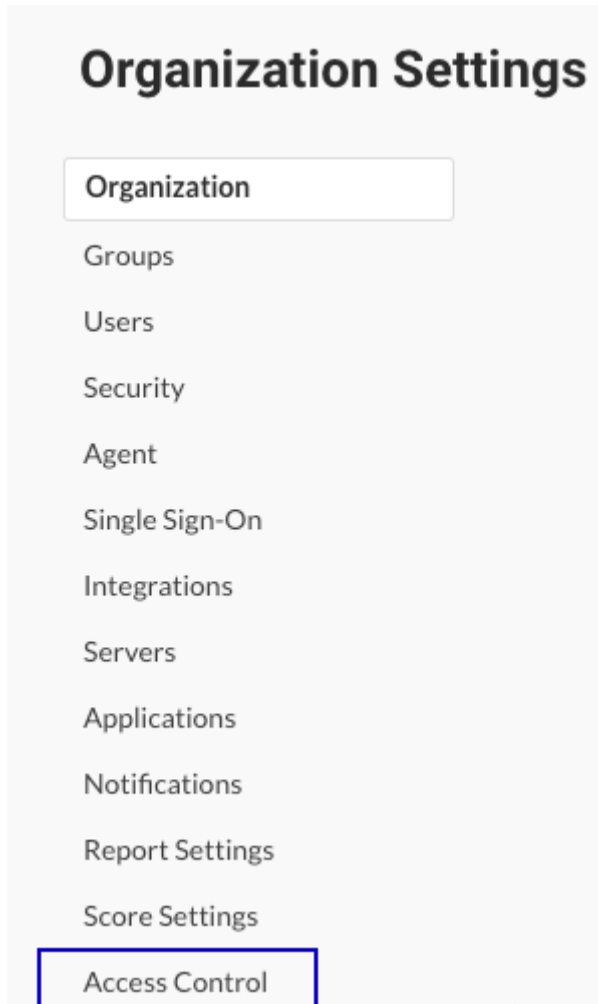
リソースグループの設定を変更する場合は、以下の手順を使用します。設定の一部または全てを変更できます。

## 開始する前に

- 組織の Admin ロールが必要です。

## 手順

1. ユーザーメニューから**組織の設定**を選択します。
2. **Access control** を選択します。



3. **Resource groups** タブを選択します。
4. 変更したいリソースグループの行の末尾にある **Edit** アイコン(✎)を選択します。
5. リソースグループの設定を変更したら、**Save** を選択します。

## Contrast Scan のリソースグループの削除

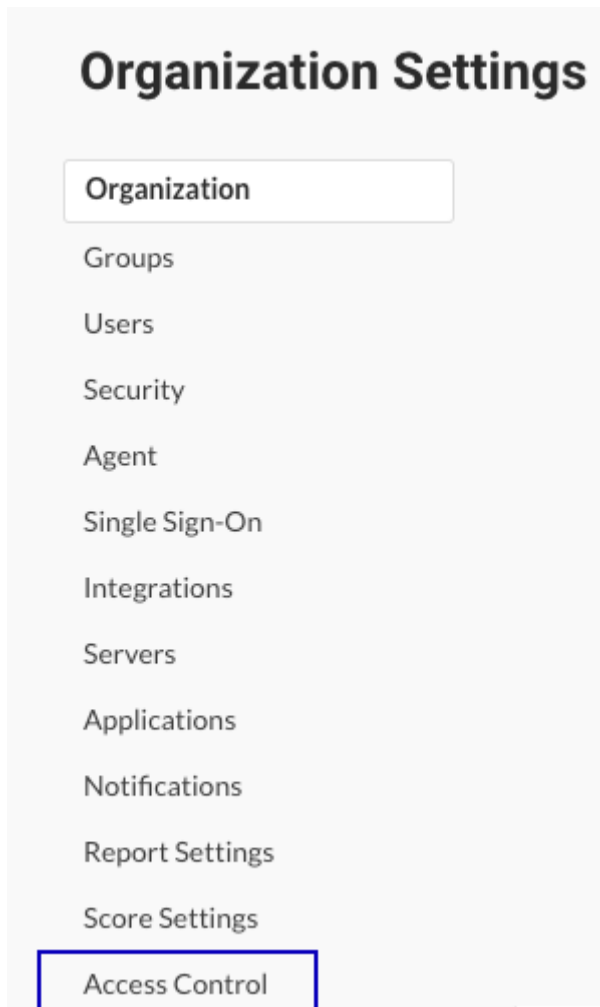
リソースグループを削除するには、以下の手順を使用します。

## 開始する前に

- 組織の Admin ロールが必要です。

## 手順

1. ユーザーメニューから**組織の設定**を選択します。
2. **Access control** を選択します。



3. **Resource groups** タブを選択します。
4. 削除したいリソースグループの行の末尾にある **Delete** アイコン(■)を選択します。
5. 「Delete resource groups」画面で、**Delete** を選択します。

## Contrast Scan のロール

ロールを使用して、特定のユーザがアクセスできる Contrast Scan の機能を定義します。

### ロール(Roles)タブ

「Roles」タブには、既存のロールの一覧が表示されます。このタブから、次のことを行えます。

- ロールの一覧を表示  
検索を使用して、特定のロールを見つけることができます。
- [Contrast Scan のカスタムロールを追加 \(726ページ\)](#)
- [Contrast Scan のカスタムロールを編集・コピー \(728ページ\)](#)
- [Contrast Scan のカスタムロールを削除 \(729ページ\)](#)

Organization Settings

Resource Groups Roles User Access Groups

Roles

Search

+ Add Role

| ROLE                     | DESCRIPTION                                      |  |
|--------------------------|--------------------------------------------------|--|
| MANAGE_ALL_PROJECTS_ROLE | System Role to Manage All Projects               |  |
| UPLOAD_ARTIFACTS         | System Role to Upload Artifacts for All Projects |  |
| MANAGE_ORGANIZATION      | System Role to Manage Organization               |  |
| View Projects            | View all Projects                                |  |
| VIEW_ALL_PROJECTS        | System Role to View All Projects                 |  |

Page 1 of 1

Results per page 10 25 50

## Contrast Scan の標準ロール

ユーザアクセスグループで、次の標準ロールを選択することができます。



### 注記

標準ロールの設定を変更することはできません。

- **RBAC Admin** : 組織の全てのスキャン操作が含まれます。Contrast で組織の Admin ロールがあるユーザには、このロールが自動で割り当てられます。
- **View All Projects** : 次の操作が含まれます。
  - スキャンとスキャンプロジェクトの全ての情報を表示
  - スキャン結果を SARIF か CSV ファイルでダウンロード
- **Upload Artifacts** : 次の操作が含まれます。
  - スキャンするファイルをアップロード
  - スキャンを開始
- **Manage All Projects**: 次の操作が含まれます。
  - スキャンとスキャンプロジェクトの全ての情報を表示
  - スキャン結果を SARIF か CSV ファイルでダウンロード
  - スキャンプロジェクトを作成
  - スキャンプロジェクトの詳細を更新

## Contrast Scan のロールの追加

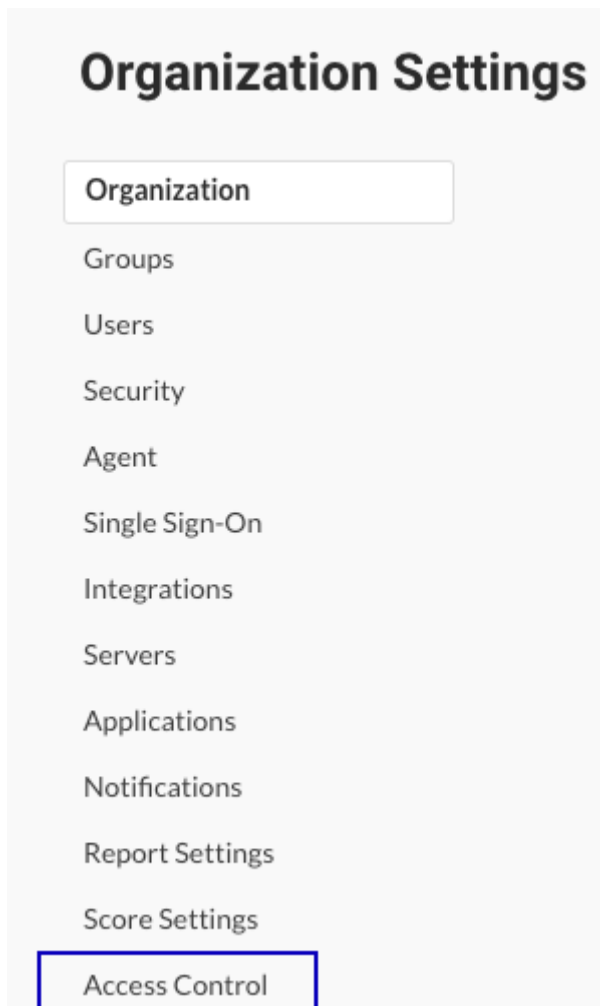
ロールを作成して、ユーザがアクセスできるスキャンリソースや操作をカスタマイズして指定します。

## 開始する前に

- 組織の Admin ロールが必要です。
- ロールに [カスタムのリソースグループを追加 \(722ページ\)](#) する必要があるかどうかを決めます。

## 手順

1. ユーザーメニューから、**組織の設定**を選択します。
2. **Access control** を選択します。



3. **Roles** タブを選択します。
  4. **Add Role** を選択します。
- 
5. ロールの設定を指定します。

## Organization Settings

Organization Settings

Resource Groups Roles User Access Groups

Organization  
Groups  
Users  
Security  
Agent  
Single Sign-On  
Integrations  
Servers  
Applications  
Notifications  
Report Settings  
Score Settings  
Access Control

### Add role

Roles define the actions and projects that users can access

Role name \*  
Ecommerce developer

Role description \*  
Developers on the Ecommerce team

Actions determine which features a user with this role can access. Resource groups define which projects and applications a user can access. Selecting both actions and resource groups is optional.

Resource groups \*  
Ecommerce developers x

Actions \*  
EDIT x VIEW x

Your role summary ⓘ

Resource Group Name  
Ecommerce developer

Resource Group Description  
Developers on the Ecommerce team

Resource Groups  
Ecommerce developers

Actions  
EDIT  
VIEW

Cancel Add

- a. **Role name** : ロールの名前を入力します。  
名前は、組織内で一意である必要があります。スペースや特殊文字を含め、最大 50 文字まで使用できます。
  - b. **Role description** : ロールの説明を入力します。  
このロールの目的が分かるような説明を入力してください。スペースや特殊文字を含め、最大 1024 文字まで使用できます。
  - c. **Resource groups** : リソースグループを 1 つ以上選択します。  
[標準のリソースグループ \(721ページ\)](#)や[カスタムグループ \(722ページ\)](#)を選択できます。
  - d. **Actions** : グループのスキャン操作を選択します。
    - **PLATFORM\_ORG\_MANAGE** : 組織のユーザアクセスグループ、ロール、リソースグループなど、全てのアクセス制御要素を管理します。
    - **SAST\_PROJECT\_MANAGE** : スキャン情報の表示、アーティファクトのアップロード、スキャンプロジェクトの作成、およびスキャンプロジェクトの詳細の更新を行います。
    - **SAST\_PROJECT\_VIEW** : 脆弱性、その他の検出結果、ポリシーなど、スキャンプロジェクトの詳細およびスキャン情報を表示します。
    - **SAST\_SCAN\_UPLOAD** : スキャンするファイルをアップロードし、スキャンを開始します。
6. **Add** を選択します。  
これで、このロールをユーザアクセスグループに割り当てることができます。

## Contrast Scan のロールの編集

既存のカスタムロールを編集またはコピーするには、以下の手順を使用します。

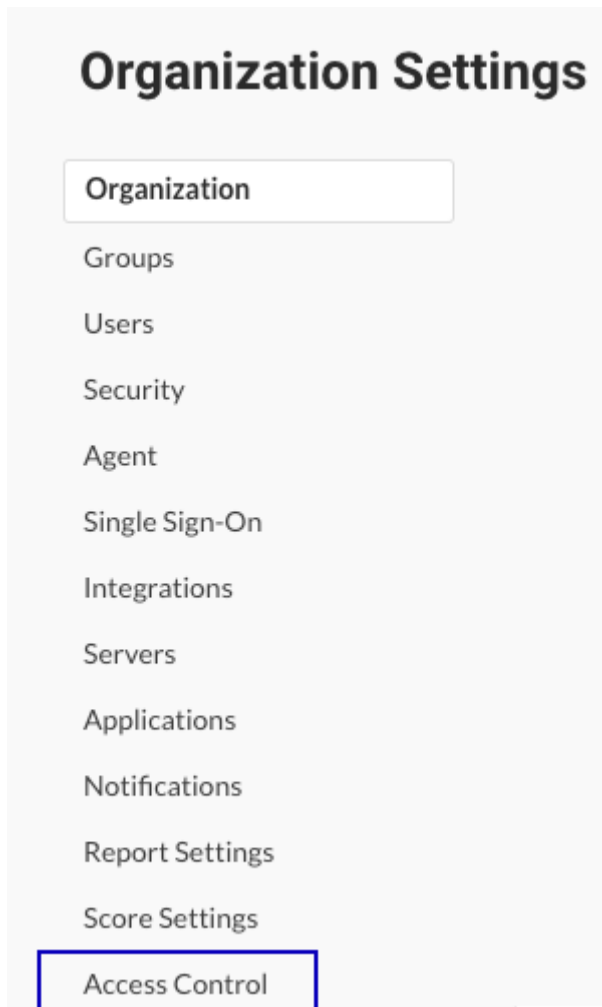
## 開始する前に

- 組織の Admin ロールが必要です。
- 既存のロールをコピーして編集し、新しいロールを作成することができます。

## 手順

1. ユーザメニューから**組織の設定**を選択します。
2. **Access control** を選択します。





3. **Roles** タブを選択します。
4. 既存のロールを編集するには、変更したいロールの行の末尾にある **Edit** アイコン(✎)を選択します。
5. 必要に応じて設定を変更したら、**Save** を選択します。

### Contrast Scan のロールの削除

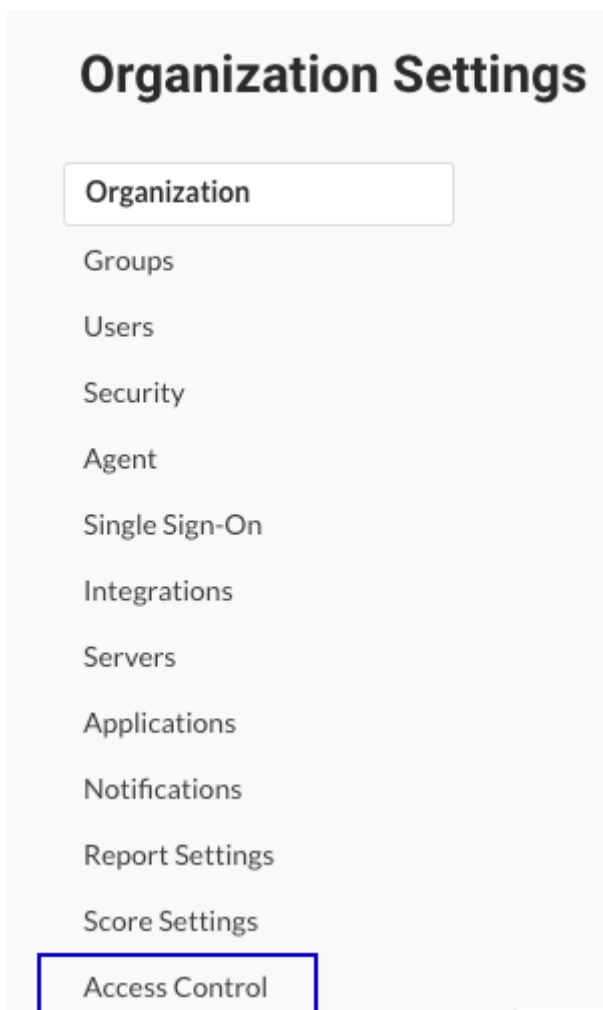
カスタムロールを削除するには、以下の手順を使用します。

#### 開始する前に

- 組織の Admin ロールが必要です。
- 削除できるのはカスタムロールのみで、標準のロールは削除できません。

#### 手順

1. ユーザメニューから**組織の設定**を選択します。
2. **Access control** を選択します。



3. **Roles** タブを選択します。
4. 削除したいロールの行の末尾にある **Delete** アイコン(🗑️)を選択します。
5. 「Delete role」画面で、**Delete** を選択します。

### Contrast Scan のユーザアクセスグループ

ユーザアクセスグループを使用して、1人以上のユーザに対して、特定のロールとリソースグループを指定します。

標準のユーザアクセスグループにユーザを追加することも、[カスタムグループ \(731ページ\)](#)を作成することもできます。

### ユーザアクセスグループ(User access groups)タブ

「User access groups」タブには、既存のグループの一覧が表示されます。このタブから、次のことを行えます。

- ユーザアクセスグループの一覧を表示  
検索を使用して、特定のグループを見つけることができます。
- [Contrast Scan のユーザアクセスグループを追加 \(731ページ\)](#)
- [Contrast Scan のユーザアクセスグループを編集 \(733ページ\)](#)
- [Contrast Scan のユーザアクセスグループを削除 \(734ページ\)](#)

| GROUP                     | DESCRIPTION                                                 | MEMBERS |
|---------------------------|-------------------------------------------------------------|---------|
| SCAN Developer User Group | System User Group to View All Projects and Upload Artifacts | 3       |
| SCAN Admin User Group     | System User Group to Manage RBAC And All Projects           | 27      |
| SCAN Manager User Group   | System User Group to View All Projects                      | 2       |
| Ecommerce                 | Ecommerce team                                              | 2       |

## Contrast Scan の標準ユーザアクセスグループ

Contrast Scan 用にあらかじめ定義された標準のユーザアクセスグループがあります。以下の標準ユーザアクセスグループに、ユーザを追加することができます。

- **Scan Admin Group** : 次のロールが含まれます。
  - RBAC Admin (組織の全スキャン操作・管理)
  - 全組織の Manage All Projects(全プロジェクトの管理)
- **Scan Manager Group** : 次のロールが含まれます。
  - View All Projects(全プロジェクトの表示)
- **Scan Developer Group** : 次のロールが含まれます。
  - View All Projects(全プロジェクトの表示)
  - Upload Artifacts(アーティファクトのアップロード)



### 注記

ユーザを追加する以外は、標準のユーザアクセスグループの設定を変更することはできません。

## Contrast Scan のユーザアクセスグループの追加

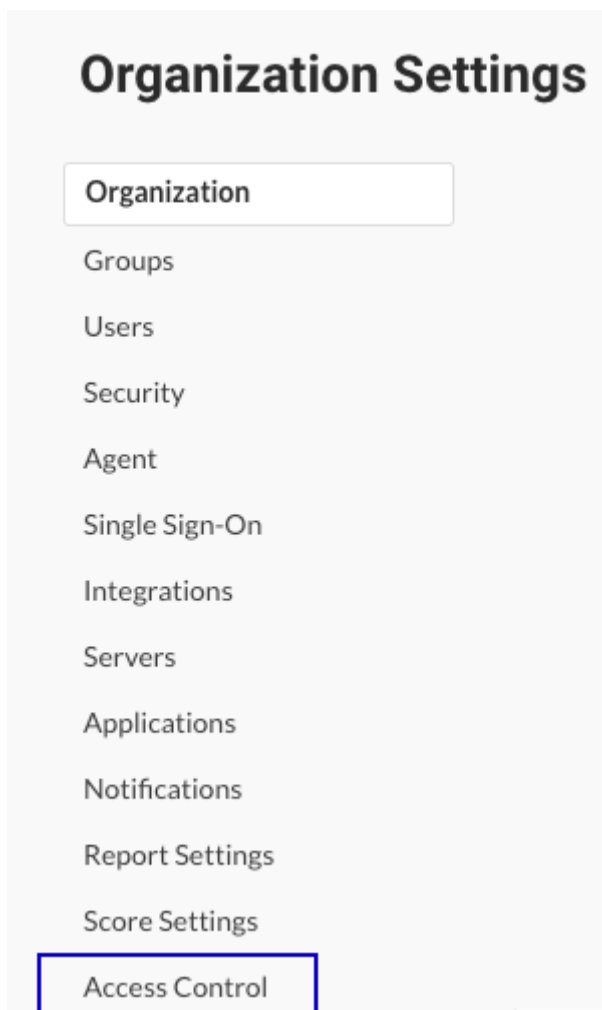
ユーザアクセスグループを作成して、複数のユーザをまとめて Contrast Scan にアクセスできるようします。グループ内のユーザに割り当てるロールによって、ユーザがアクセスできるスキャン機能が決まります。

### 開始する前に

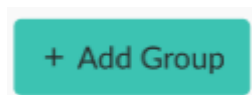
- 組織の Admin ロールが必要です。
- 必要に応じて、[組織にユーザを追加 \(708ページ\)](#)します。
- [カスタムロールを追加 \(726ページ\)](#)したり、[カスタムのリソースグループ \(722ページ\)](#)が必要であるかどうか判断してください。

## 手順

1. ユーザメニューから、**組織の設定**を選択します。
2. **Access control** を選択します。



3. 「User access groups」タブで、**Add Group** を選択します。



4. 「Add user access group for Scan」の画面で、以下の設定を行います。

Organization Settings

Resource Groups Roles **User Access Groups**

Organization  
Groups  
Users  
Security  
Agent  
Single Sign-On  
Integrations  
Servers  
Applications  
Notifications  
Report Settings  
Score Settings  
Access Control

### Add user access group

For easier management of user access groups, use descriptive names and easy-to-identify descriptions.

User access group name

User access group description

Users

Roles

Your user access group summary ⓘ

User access group name  
Ecommerce

User access group description  
Ecommerce team

Users  
user1@mycompany.com  
user2@mycompany.com

Roles  
UPLOAD\_ARTIFACTS\_FOR\_ALL\_PROJECTS\_ROLE

Cancel Add

- **User access group name** : ユーザグループの名前を入力します。  
名前は、組織内で一意である必要があります。スペースや特殊文字を含め、最大 50 文字まで使用できます。
- **User access group description** : グループの説明を入力します。  
このグループの目的が明確に分かるような説明を入力してください。スペースや特殊文字を含め、最大 1024 文字まで使用できます。
- **Users** : グループに所属するユーザを指定します。  
ユーザの一覧を表示するには、ボックスの端にある三角形▼を選択するか、名前を入力してみてください。  
特定のユーザが表示されない場合は、**ユーザメニュー > 組織の設定よりユーザ**にアクセスして、そのユーザが Contrast の組織のユーザであることを確認してください。
- **Roles** : ドロップダウンから、グループ内の全てのユーザに適用されるロールを 1 つ以上選択します。  
[標準のロール \(725ページ\)](#)や[カスタムロール \(726ページ\)](#)を選択できます。

5. **Add** を選択します。

## Contrast Scan のユーザアクセスグループの編集

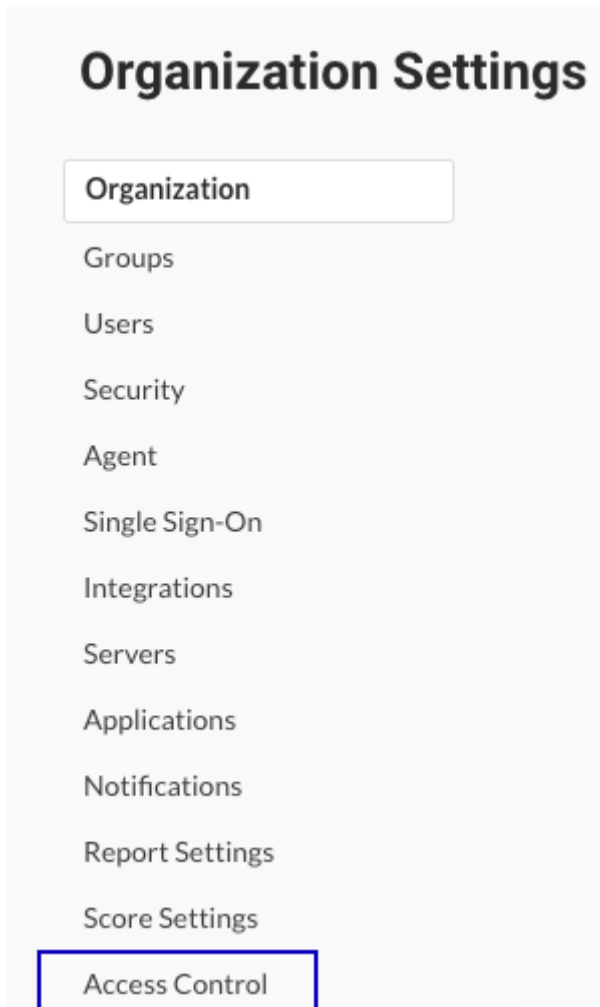
既存のユーザアクセスグループを編集するには、以下の手順を使用します。設定の一部または全てを変更できます。

### 開始する前に

- 組織の Admin ロールが必要です。

### 手順

1. ユーザメニューから**組織の設定**を選択します。
2. **Access control** を選択します。



3. **User access groups** タブを選択します。
4. 変更したいグループの行の末尾にある **Edit** アイコン(✎)を選択します。
5. 必要に応じて設定を変更したら、**Save** を選択します。

### Contrast Scan のユーザアクセスグループの削除

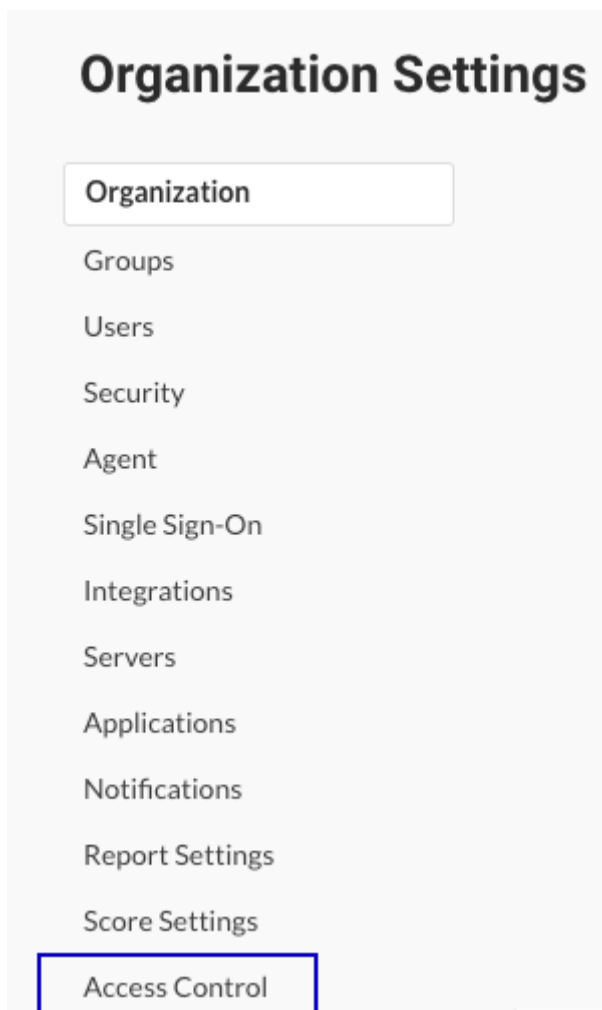
既存のユーザアクセスグループを削除するには、以下の手順を使用します。

#### 開始する前に

- 組織の Admin ロールが必要です。

#### 手順

1. ユーザーメニューから**組織の設定**を選択します。
2. **Access control** を選択します。



3. **User access groups** タブを選択します。
4. 削除したいグループの行の末尾にある **Delete** アイコン(■)を選択します。
5. 「Delete user access group」画面で、**Delete** を選択します。

## 脆弱性クローズの承認

組織の管理者は、組織内の脆弱性のクローズ時に管理者の承認を必要 (674ページ) とすることができません。脆弱性のクローズを承認または却下 (601ページ) するには、組織ロールに Rules Admin があり、対象アプリケーションに対しても Rules Admin ロールが必要です。

この要件を設定するには：

1. ユーザメニューで、ポリシーの管理 > 脆弱性の管理 > 脆弱性の動作を選択します。
2. 脆弱性のクローズ時に管理者の承認が必要な横にあるチェックボックスをオンにします。
3. ユーザが脆弱性をクローズするときに自動的に保留中になる脆弱性のステータスと深刻度を選択します。
4. 対象となる脆弱性のクローズがユーザから要求されると、全ての組織の管理者にレビューが必要であることが Contrast 内で通知されます。  
各脆弱性のステータスは、組織の管理者がクローズのレビューを送信するまで保留中のままになります。管理者の承認を得るには、ステータスと深刻度の両方を選択する必要があります。  
レビュー担当者が脆弱性のクローズを却下する場合は、却下する理由を提供する必要があります。  
レビューが完了すると、レビュー担当者からのフィードバックが脆弱性のアクティビティタブに表示されます。  
この機能を無効にすると、保留中のクローズ処理は自動的に承認されます。



### 注記


保留中の状態でも、それまでの脆弱性のステータスが、組織のレポートや統計情報に反映されます。

## 監査ログの表示

Contrast では、設定やライセンスの変更、脆弱性に対するアクションなど、全てのユーザセッションに関するアクティビティがキャプチャされます。

1. ユーザメニューで**組織の設定** > **セキュリティ**を選択します。
2. 画面右上の**監査ログを表示**をクリックします。

Contrastは全てのユーザセッションに関するアクティビティをキャプチャします。 [監査ログを表示](#)



監査ログのページが表示されます。



組織の設定

- 組織
- グループ
- ユーザ
- セキュリティ
- API
- シングルサインオン
- インテグレーション
- サーバ
- アプリケーション
- 通知
- レポートの設定
- スコアの設定

監査ログ

Contrastは、設定やライセンスの変更、脆弱性に関する処理等、全てのユーザセッションに関するアクティビティをキャプチャします。

監査ログを検索    57594件中80件イベント

| 作成日時             | メッセージ                                                                                                                                               |
|------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|
| 01/20/2022 14:46 | - User @contrastsecurity.com successfully logged in from [99.239.113.31].                                                                           |
| 01/20/2022 14:06 | - @contrastsecurity.com at [99.239.113.31] was logged out due to inactivity.                                                                        |
| 01/20/2022 13:35 | User @contrastsecurity.com updated their account: [language=en] differs from [language=ja]                                                          |
| 01/20/2022 13:29 | - User @contrastsecurity.com successfully logged in from [75.164.138.150].                                                                          |
| 01/20/2022 12:38 | - @contrastsecurity.com at [75.108.58.4] was logged out due to inactivity.                                                                          |
| 01/20/2022 12:37 | @contrastsecurity.com impersonating @contrastsecurity.com @contrastsecurity.com @contrastsecurity.com successfully logged in from [109.149.234.37]. |
| 01/20/2022 12:37 | - User @contrastsecurity.com successfully logged in from [73.87.185.16].                                                                            |
| 01/20/2022 12:08 | - User @contrastsecurity.com successfully logged in from [75.108.58.4].                                                                             |
| 01/20/2022 11:43 | - User @contrastsecurity.com successfully logged in from [73.87.185.16].                                                                            |
| 01/20/2022 10:47 | Remediation Policy 'test' disabled by @contrastsecurity.com                                                                                         |
| 01/20/2022 10:47 | Remediation Policy 'test' enabled by @contrastsecurity.com                                                                                          |
| 01/20/2022 10:36 | @contrastsecurity.com @contrastsecurity.com - User @contrastsecurity.com successfully logged in from [109.149.234.37].                              |
| 01/20/2022 10:26 | - @contrastsecurity.com at [73.87.185.16] was logged out due to inactivity.                                                                         |
| 01/20/2022 10:13 | - User @contrastsecurity.com successfully logged in from [75.108.58.4].                                                                             |
| 01/20/2022 10:12 | - User @contrastsecurity.com successfully logged in from [75.108.58.4].                                                                             |
| 01/20/2022 09:52 | @contrastsecurity.com impersonating @contrastsecurity.com User @contrastsecurity.com is now impersonating user @contrastsecurity.com                |
| 01/20/2022 09:51 | @contrastsecurity.com impersonating @contrastsecurity.com User @contrastsecurity.com is now impersonating user @contrastsecurity.com                |
| 01/20/2022 09:48 | @contrastsecurity.com @contrastsecurity.com - User @contrastsecurity.com successfully logged in from [109.149.234.37].                              |
| 01/20/2022 09:47 | @contrastsecurity.com @contrastsecurity.com - User @contrastsecurity.com successfully logged in from [109.149.234.37].                              |
| 01/20/2022 08:45 | - User @contrastsecurity.com successfully logged in from [31.154.49.58].                                                                            |
| 01/20/2022 08:36 | @contrastsecurity.com impersonating @contrastsecurity.com User @contrastsecurity.com is now impersonating user @contrastsecurity.com                |
| 01/20/2022 07:45 | Server 'PLogan-1' is offline                                                                                                                        |
| 01/20/2022 07:40 | - User @contrastsecurity.com successfully logged in from [31.154.49.58].                                                                            |

以下の様な情報が表示されます。

|          |                                                                                          |
|----------|------------------------------------------------------------------------------------------|
| エージェント   | エージェントのダウンロード/起動/Contrast サービス                                                           |
| 警告       | 生成<br>削除<br>更新                                                                           |
| アプリケーション | ライセンスの適用<br>アーカイブ<br>Assess ルールの設定変更<br>組織の設定変更<br>ルールの有効/無効化<br>マージ/マージ解除<br>復元<br>リセット |

|                     |                                                                                                                                                                             |
|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 攻撃                  | イベントに備考を入力<br>備考の作成/編集/削除<br>消去                                                                                                                                             |
| バグ管理システム            | 生成<br>更新                                                                                                                                                                    |
| Eメール                | ドメインの追加<br>ライブラリの共有                                                                                                                                                         |
| グループ                | 組織のグループへのメンバの作成/更新/修正                                                                                                                                                       |
| IPアドレスの範囲           | 追加<br>削除                                                                                                                                                                    |
| キー                  | APIおよびエージェントのサービスキーのローテーション                                                                                                                                                 |
| 通知の設定               | 組織やユーザの設定の更新                                                                                                                                                                |
| バッチ                 | 仮想バッチの生成/更新/オンやオフ/削除                                                                                                                                                        |
| ポリシー                | クリーンアップの設定の変更<br>ライブラリの制限の変更<br>パスワードの変更<br>スコア付けの変更<br>タイムアウトの変更<br>コンプライアンスポリシーの作成/削除/無効化/有効化/更新<br>組織の修復ポリシーの作成/削除/更新/有効化<br>セキュリティ制御の作成/削除/更新/有効化<br>例外ルールの作成/削除/更新/有効化 |
| レポート                | レポートの作成<br>脆弱性の傾向レポート                                                                                                                                                       |
| サーバ                 | デフォルト値の変更<br>通知の作成<br>ライセンスの削除/無効化/更新/削除<br>Protectの有効/無効化                                                                                                                  |
| システム管理者(SuperAdmin) | 作成<br>ユーザのなりすまし<br>更新                                                                                                                                                       |
| トレース                | 備考の追加/編集/削除<br>自動修復<br>トレースの共有/削除/マージ/ステータス変更<br>深刻度の更新                                                                                                                     |
| ユーザ                 | 追加<br>アクティベーション<br>アクセスの変更<br>プロビジョニング/バルクによる作成/作成<br>削除<br>Protectの付与/取消<br>組織へのインポート<br>非特権ユーザによる試行<br>更新                                                                 |

Webhook

作成



## ヒント

検索フィールドを使用して、日付や名前で特定のログを検索できます。

## なりすまし

なりすまし機能により、[システムロール \(821ページ\)](#)のある他のユーザが既存のユーザとして組織にアクセスし、問題のトラブルシューティングを行うことが可能になります。

組織のなりすましは、24 時間後に自動的に無効になります。

SaaS 版をご利用のお客様で、組織になりすましの設定が表示されていない場合は、[Contrast サポート](#)にご連絡ください。オンプレミス版のお客様は、必要に応じてなりすましを管理・使用できます。

## なりすましアクセス

デフォルトでは、全ての組織でなりすましの設定が有効です。組織内で別のユーザになりすますかどうかは、組織管理者が管理します。

なりすましを行うためのアクセスを変更するには：

- SuperAdmin ユーザは[組織を編集 \(774ページ\)](#)して、特定の組織のなりすましを有効にできるオプションをオンまたはオフに設定します。  
この設定は、組織管理者が組織のなりすまし設定を表示できるかどうかに影響します。
- 組織管理者は、[組織のセキュリティの設定を編集 \(739ページ\)](#)して、なりすましの使用を管理します。

なりすましをオンにすると：

- SuperAdmin ロールがある場合は、組織のページより該当の組織の行でなりすまを選択すれば、[なりすまし \(784ページ\)](#)を使用できます。  
その組織内の最初の組織管理者に対して、なりすますることができます。
- SuperAdmin ロールがある場合は、ユーザのページより、なりすまユーザを選択することができます。
- ServerAdmin または SystemAdmin ロールがあるユーザの場合は、組織のページより該当の組織の行でなりすまを選択することで、[なりすまし \(784ページ\)](#)を使用できます。  
その組織内の最初の組織管理者に対して、なりすますることができます。組織へのアクセス権が必要です。

## 監査ログ

Contrast の監査ログには、以下のような、なりすましのアクティビティが記録されます。

- なりすましの有効化/無効化
- なりすましが発生した組織
- なりすましのステータス変更に関連付けられたサーバキー
- なりすまし試行の拒否

## なりすましを有効にする

組織でなりすまし ([739ページ](#))を有効にするには、次の手順を実行します。

## 開始する前に

- 組織の Admin ロールが必要です。
- 組織の設定 > セキュリティにアクセスし、なりすましを有効にするための設定が表示されていることを確認してください。  
設定が表示されていない場合：
  - SaaS 版のお客様： [Contrast サポート](#)にご連絡ください。
  - オンプレミス版のお客様： SuperAdmin ユーザに [組織を編集 \(774ページ\)](#)して、なりすましを有効にできるの設定をオンにするよう依頼してください。

## 手順

1. ユーザーメニューから、**組織の設定**を選択します。
2. **セキュリティ**を選択します。
3. なりすましのセクションで、有効にする設定を選択し、**保存**を選択します。

### なりすまし

なりすましを有効にすると、システム管理者(SuperAdmin)は組織内のユーザに成り代わり、サポートやトラブルシューティングを行うことができます。このアクセス権の有効期限は、24時間です。

有効      保存をクリックすると、この組織のなりすましが有効になります。

[保存](#)

## システム管理(EOP)

オンプレミス版のお客様のみ、システム管理が必要です。SaaS 版のお客様のシステム管理は、Contrast Security が行います。

[オンプレミス版の利用を開始する \(741ページ\)](#)方法を参照したり、[システム運用の管理方法 \(772ページ\)](#)方法などを検討してください。

### オンプレミス版をはじめめる

オンプレミス版のお客様は、インターネットに接続せずに独自の Contrast インスタンスを管理でき、セキュリティポリシー、データベース、認証などを設定できます。この設定は、1 組織につき 1 回だけ必要です。



#### 重要

Contrast を SaaS 版として使用できる場合は、オンプレミス版 Contrast の追加のインストールやメンテナンスを行う必要はありません。

SaaS 版 Contrast は SOC-2 Type II に準拠しており、継続的に機能の更新が行われます。SaaS 版 Contrast に接続するには、管理者から提供された認証情報を使用してログインします。そして、続けて[エージェントをインストール \(35ページ\)](#)してください。

オンプレミス版のお客様は、Assess や Protect、もしくは両方を使用するために、少なくとも以下の 2 つのインストールを完了する必要があります。

- [Contrast のインストール \(746ページ\)](#)
- [各アプリケーションサーバのエージェントのインストール \(35ページ\)](#)

Contrast のインストールには、Tomcat サーブレットコンテナ、MySQL データベースインスタンス、AdoptOpenJDK Hotspot Java 仮想マシンなど、システムを構成する全ての組込みコンポーネントが含まれています。これらのコンポーネントは全て、インストールバイナリ内に組み込まれており、Contrast アーキテクチャの一部として単一サーバにデプロイされます。

Contrast をインストールする前に、ご使用の環境が以下の要件を満たしていることを確認してください。

- [システム要件 \(742ページ\)](#)
- [サイジングの推奨 \(743ページ\)](#)

以下の項目は、インストール後さらに設定できます。

- [Tomcat \(758ページ\)](#)
- [JRE \(759ページ\)](#)
- [HTTPS \(759ページ\)](#)
- [Contrast の設定 \(800ページ\)](#)

長期的には、以下についての計画が必要となります。

- [システム管理 \(772ページ\)](#)
- [設定の構成 \(800ページ\)](#)
- [Contrast システムの保守 \(807ページ\)](#)

## Contrast のインストール

オンプレミス環境で Contrast をインストールし、デプロイするためのオプションには、次のものがあります。

- [Contrast インストーラでインストールする \(746ページ\)](#)
- [分散 MySQL データベース \(750ページ\)](#)を使用する
- [WAR ファイルを使用してデプロイする \(749ページ\)](#)
- [分散環境 \(753ページ\)](#)で導入する

### 次の手順

- [Contrast のシステム要件 \(742ページ\)](#)を確認する
- [Contrast のサイジング推奨事項 \(743ページ\)](#)を確認する
- [Contrast Hub または curl コマンド \(744ページ\)](#)で Contrast インストーラをダウンロードする

### Contrast のシステム要件

次の表に、Contrast アプリケーションをインストールするためのシステム要件を示します。

Contrast をインストールする前に :

- [Contrast Hub または curl コマンド \(744ページ\)](#)を使用して、[Contrast インストーラをダウンロード \(745ページ\)](#)してください。
- [サイジングの推奨 \(743ページ\)](#)を確認してください。

| 要件           | 推奨                                                                                                                                                                                                                                                                                                                                              | 最小                                                                                                                                    | 備考                                                   |
|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------|
| OS アーキテクチャ   | 64 ビット                                                                                                                                                                                                                                                                                                                                          | 64 ビット                                                                                                                                | メモリの要件のため、Contrast アプリケーションは 64 ビットアーキテクチャでのみ実行できます。 |
| オペレーティングシステム | <ul style="list-style-type: none"> <li>• RHEL 8</li> <li>• RHEL/CentOS 7</li> <li>• Microsoft Windows 2019</li> <li>• Ubuntu 18.04 LTS 以降 (20.04 LTS まで)</li> </ul>                                                                                                                                                                             | <ul style="list-style-type: none"> <li>• RHEL/CentOS 7</li> <li>• Microsoft Windows 2012 R2 以降</li> <li>• Ubuntu 16.04 LTS</li> </ul> | CentOS 6 のサポートは、2020 年 12 月 1 日に終了しました。              |
| Java         | Java はインストーラにバンドルされています。                                                                                                                                                                                                                                                                                                                        |                                                                                                                                       |                                                      |
| MySQL        | <ul style="list-style-type: none"> <li>• Contrast のバージョン 3.8.11 以前のオンプレミス版には、MySQL 5.7.23 がインストーラにバンドルされています。</li> <li>• Contrast 3.9.0 以降のオンプレミス版では、MySQL 8 が Linux インストーラにバンドルされています。</li> <li>• Contrast 3.9.3 以降のオンプレミス版では、MySQL 8 が Linux インストーラと Windows インストーラにバンドルされています。</li> </ul> <p>何か問題がありましたら、<a href="#">弊社サポート</a>にご連絡ください。</p> |                                                                                                                                       |                                                      |



### 重要

- MySQL 8(デフォルトでバイナリログが有効)を使用しているオンプレミス版のお客様は、Contrast でストアプロシージャが作成できるように、システム変数 `log_bin_trust_function_creators` を **ON** に設定する必要があります。詳細については、[MySQL のドキュメント](#)を参照してください。
- MySQL 8 を使用しているオンプレミス版のお客様は、Contrast で CSV ファイルを受け取り SCA データのインポートができるように、システム変数 `local_infile` を **ON** に設定する必要があります。詳細については、[LOAD DATA LOCAL のセキュリティ上の考慮事項](#)を参照してください。

## 分散インストールの場合の MySQL と Java の要件

Contrast を分散アプリケーションとしてデプロイする場合、または独自の MySQL データベースを使用する場合は、以下の要件を使用してください。それ以外の全てのオンプレミスインストールでは、Contrast インストーラに含まれる MySQL および Java ソフトウェアを使用してください。

何か問題がありましたら、[弊社サポート](#)にご連絡ください。

| 要件    | 推奨                                                                                                             | 最小                                                                                                             |
|-------|----------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------|
| Java  | 11                                                                                                             | 11                                                                                                             |
| MySQL | <ul style="list-style-type: none"> <li>8.0.30(Contrast 3.9.1 以降)</li> <li>5.7.23(Contrast 3.9.0 以前)</li> </ul> | <ul style="list-style-type: none"> <li>8.0.27(Contrast 3.9.1 以降)</li> <li>5.7.23(Contrast 3.9.0 以前)</li> </ul> |

## SuperAdmin アカウント

インテグレーションでの接続が正しく動作するように、Contrast Security で作成したデフォルトのアカウントとは異なる SuperAdmin アカウントを作成してください。デフォルトの SuperAdmin アカウントを使用し続けると、接続エラーが発生する可能性があります。

## エージェントが多数の場合の分散構成

接続されているエージェントの数が 100 を超えて利用する予定がある場合は、[分散環境の構成 \(753ページ\)](#)を検討してください。このような場合に分散構成を使用しないと、パフォーマンスの問題が発生する可能性があります。

## Contrast アプリケーションのサイジング推奨事項

Contrast のための CPU とメモリのリソースは、接続するエージェントの数と Contrast アプリケーションに通信を返すアプリケーションのトラフィックによって異なります。このページの推奨事項は、アプリケーションのサービスに適用されます。

パフォーマンスに影響を与えるその他の要因には、以下があります。

- Contrast に報告されるデータの利用者による Web トラフィック**  
 Contrast は、高度なトランザクションシステムで、リアルタイムでデータセットを計算しデータの利用者に返します。より多くのユーザがシステムを利用するほど、より多くのコンピューティングリソースとメモリリソースが必要になります。
- 長期間にわたりアプリケーションに保持される大量のデータ**  
 時間の経過に合わせてデータを積極的に削除することも、データを保持することもできます。どのトランザクションシステムでも、クエリの対象となるデータセットが大きくなるほど、コンピューティング要件も大きくなります
- 100 を超えるエージェントの接続**  
 接続されているエージェントの数が 100 を超えて利用する予定がある場合は、[分散環境の構成 \(753ページ\)](#)を検討してください。このような場合に分散構成を使用しないと、パフォーマンスの問題が発生する可能性があります。

次のガイドラインを参考にして、ワークロードに合わせて要件を拡張するために、適切なリソースの組み合わせを選択してください。

- 小規模構成** : Contrast と通信するエージェント数のが 3~30 程度、エンドユーザが 5~25 人規模の Web トラフィックを処理する場合に推奨される構成です。エンドユーザは、1 日に複数回システムにアクセスし、アラートやレポート、インテグレーションなどを積極的に使用します。  
 接続するエージェントの数が多いほど、Contrast が実行中のトレース処理をするためのメモリ要件が大きくなります。ストレージは、トレースデータの寿命とシステム管理者によるログファイルの保存状況によって異なります。

| vCPU 数 | クロック速度          | RAM         | ストレージ         |
|--------|-----------------|-------------|---------------|
| 4~8 個  | 2.5 GHz~3.3 GHz | 16 GB~24 GB | 100 GB~200 GB |

- 大規模構成** : Contrast と通信するエージェントが 30~100 程度のより大きな作業負荷や、エンタープライズ規模で展開される 25 ユーザ以上の大規模な Web トラフィックを想定しています。エンドユ

ーザは 1 日に複数回システムにアクセスし、アラートやレポート、インテグレーションなどの Contrast の機能を積極的に使用します。

接続しているエージェントの数やエンドユーザーが多いほど、Contrast が実行中のトレース処理をするためのメモリ要件が大きくなります。ストレージは、トレースデータの寿命とシステム管理者によるログファイルの保存状況によって異なります。

| vCPU 数   | クロック速度            | RAM           | ストレージ           |
|----------|-------------------|---------------|-----------------|
| 8 ~ 16 個 | 2.5 GHz ~ 3.3 GHz | 24 GB ~ 48 GB | 200 GB ~ 500 GB |



### 重要

作業負荷や構成規模に関係なく、最低 16GB の RAM を Contrast アプリケーションに割り当ててください。



### ヒント

Contrast REST API アーキテクチャを自動化またはデータ抽出の目的で使用している場合、および大規模な自動リグレーションスイートでエージェントの継続的インテグレーション(CI)を目的として使用している場合は、大規模構成のガイドラインに従ってください。

## curl コマンドによる Contrast ソフトウェアのダウンロード

ライセンスが提供されたら、curl コマンドを使用して Contrast のインストーラとライセンスをダウンロードすることができます。会社のアクセス権を誰が持っているか不明な場合は、[サポートにお問い合わせください](#)。

Contrast のその他のソフトウェアのファイルも、curl コマンドを使用して、ダウンロードできます。

また、インストーラやライセンスファイルは [Contrast Hub](#) からダウンロードすることもできます。



### 注記

Contrast 3.9.10 より、インストーラにライブラリ・CVE データが含まれなくなりました。エアギャップでのインストールの場合は、このデータを手動でダウンロードする必要があります。インターネットに接続できる場合は、[このデータを自動で更新 \(771ページ\)](#)するようにシステムを設定できます。

## インストーラファイルのダウンロード手順

1. Contrast の最新の Linux 用インストーラをダウンロードするには、以下のコマンドを使用します。

```
curl -L https://hub.contrastsecurity.com/h/api/artifacts/installer/sh/nocache -u <ContrastHubUsername> -o "contrast-latest-nocache.sh"
```

<ContrastHubUsername>は、お客様の Contrast Hub アカウントに置き換えてください。コマンドを実行すると、パスワードの入力を求められます。

2. Contrast の最新の Windows 用インストーラをダウンロードするには、以下のコマンドを使用します。



```
curl -L https://hub.contrastsecurity.com/h/api/artifacts/installer/exe/nocache -u <ContrastHubUsername> -o "contrast-latest-nocache.exe"
```

<ContrastHubUsername>は、お客様の Contrast Hub アカウントに置き換えてください。コマンドを実行すると、パスワードの入力を求められます。

3. **エアギャップでのインストールの場合**：以下のコマンドを使用して、ライブラリ・CVE データをダウンロードします。

```
curl -JLO https://hub.contrastsecurity.com/h/api/artifacts/ardy_export -u <ContrastHubUsername>
```

<ContrastHubUsername>は、お客様の Contrast Hub アカウントに置き換えてください。コマンドを実行すると、パスワードの入力を求められます。

4. **最新の Contrast WAR ファイルは**、以下のコマンドでダウンロードします。

```
curl -JLO https://hub.contrastsecurity.com/h/api/artifacts/war -u \<ContrastHubUsername>
```

<ContrastHubUsername>は、お客様の Contrast Hub アカウントに置き換えてください。この WAR ファイルは、既存の Tomcat サーバがあり、そのサーバに Contrast をインストールする場合に便利です。

5. 以下のコマンドを使用して、ライセンスファイルをダウンロードします。

```
curl --request GET --url https://hub.contrastsecurity.com/h/rest/customer/license/text -u <ContrastHubUsername> > license.lic
```

<ContrastHubUsername>は、お客様の Contrast Hub アカウントに置き換えてください。コマンドを実行すると、パスワードの入力を求められます。

6. ファイルをダウンロードしたら、[Contrast をインストール \(746ページ\)](#)します。

## その他のソフトウェアダウンロード

次の curl コマンドで、Contrast のその他のソフトウェアをダウンロードすることができます。

```
curl -JLO https://hub.contrastsecurity.com/h/api/artifacts/<OtherSoftware> -u <ContrastHubUsername>
```

<Other Software>を次のいずれかに置き換えてください。

- .NET Framework エージェントの場合は、dotnet
- .NET Core エージェントの場合は、dotnet\_core
- IIS 用の .NET Core インストーラの場合は、dotnetcore\_installer\_for\_iis

## Contrast インストーラのダウンロード

ライセンスが提供されると、[Contrast Hub](#) アカウントにアクセスできるようになり、そのアカウントでインストーラとライセンスをダウンロードできます。会社のアクセス権を誰が持っているか不明な場合は、[サポートにお問い合わせください](#)。

または、Contrast Hub の代わりに [curl コマンド \(744ページ\)](#)を使用してインストーラやライセンスをダウンロードすることもできます。



### 注記

Contrast 3.9.10 より、インストーラにライブラリ・CVE データが含まれなくなりました。エアギャップでのインストールの場合は、このデータを手動でダウンロードする必要があります。インターネットに接続できる場合は、[このデータを自動で更新 \(771ページ\)](#)するようにシステムを設定できます。

## 手順

1. 提供された認証情報を使用して Contrast Hub にログインします。
2. お使いのオペレーティングシステムの Contrast インストーラをダウンロードします。
  - a. ナビゲーションバーで、**Downloads**(ダウンロード)を選択します。
  - b. **Installers** (インストーラ)を選択します。
  - c. ダウンロードするファイルを選択します。



### TeamServer

| Version           | OS      | Release Date | File Name                                   | File Size |                                                  |
|-------------------|---------|--------------|---------------------------------------------|-----------|--------------------------------------------------|
| 3.8.11.1683721903 | linux   | 01/11/2022   | Contrast-3.8.11.1683721903-NO-CACHE.sh      | 869.91 MB | <a href="#">Download</a> <a href="#">MD5 Sum</a> |
| 3.8.11.1683721903 | windows | 01/11/2022   | Contrast-3.8.11.1683721903-NO-CACHE-x64.exe | 874.14 MB | <a href="#">Download</a> <a href="#">MD5 Sum</a> |

- **Linux インストーラ** : Contrast<version>-NO-CACHE.sh
  - **Windows インストーラ** : Contrast<version>-NO-CACHE-x64.exe
3. エアギャップでのインストールの場合：[ライブラリ・CVE データをダウンロード \(770ページ\)](#)します。

インターネットに接続できる場合は、データをダウンロードする必要はありません。インストール後に、[ライブラリ・CVE データを自動で更新 \(771ページ\)](#)するようにシステムを設定します。
  4. Contrast のライセンスファイルをダウンロードします。

ライセンスファイルには、[SuperAdmin \(821ページ\)](#)アカウントと通常のユーザアカウントが設定されています。Contrast アプリケーションのインストールを完了するには、ライセンスが必要です。

    - a. ナビゲーションバーで、**Home**(ホーム)を選択します。
    - b. **Licenses**(ライセンス)を選択します。
    - c. ダウンロードするライセンスファイルを選択します。
  5. ファイルをダウンロードしたら、[Contrast をインストール \(746ページ\)](#)します。

## オンプレミス版 Contrast のインストール



### 重要

このインストール手順は、オンプレミス版専用です。

SaaS 版の Contrast をお使いのお客様は、本インストールを行わずに[アプリケーションを検査 \(35ページ\)](#)できます。[エージェントをインストール \(35ページ\)](#)すれば、検査を開始できます。

Contrast は、約 24 時間ごとにライブラリデータを更新します。インターネットアクセスがあれば、お使いのオンプレミス版 Contrast は、クラウドにホストされている Contrast データベースからデータを取得します。インターネットに接続できない環境(エアギャップでのインストール)の場合は、手動でデータをダウンロードしてください。

## 開始する前に

- [Contrast Hub](#) または [curl コマンド \(744ページ\)](#) を使用して、[Contrast インストーラをダウンロード \(745ページ\)](#) してください。
- インターネットに接続できない環境(エアギャップでのインストール)の場合は、[手動でライブラリデータをダウンロード \(770ページ\)](#) してください。
- [システム要件 \(742ページ\)](#) と [サイジングの推奨事項 \(743ページ\)](#) を確認してください。

## 手順

1. お使いのオペレーティングシステムで MySQL を実行するための共有ライブラリを事前に設定します。また、Linux の場合にはフォントをインストールするためにシステムパッケージの `fontconfig` も必要です。お使いのオペレーティングシステムのコマンドを実行してください。

- **RHEL 8.6** の場合：

```
[contrast@myserver ~]# dnf install -y ncurses-compat-libs libaiol \
fontconfig
```

- **CentOS** または **RHEL 7** の場合：

```
[contrast@myserver ~]# yum install -y libaiol fontconfig
```

- **Ubuntu** または **Debian** の場合：

```
[contrast@myserver ~]# apt-get install -y libaiol libaiol-dev fontconfig
```


- **Windows** の場合：MySQL を実行するために [Microsoft Visual C++ 2015-2022 再頒布可能パッケージ](#) が必要です。

2. 特権ユーザとしてインストーラを実行します。

- Windows の場合、インストーラを右クリックして**管理者として実行**を選択します。
- Linux の場合、`sudo` コマンドを使用してインストーラを起動します。

3. ご利用の環境に合わせて、インストーラの問いに回答します(例えば、[MySQL バックアップの作成 \(809ページ\)](#)や [JRE の設定 \(759ページ\)](#)など)。

Contrast の起動後でも設定はできます。インストールスクリプトの実行時に、以下のコマンドライン引数を使用して、インストーラの動作をカスタマイズできます。

| コマンドライン引数                      | 説明                                                                                                                                                     |
|--------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>-h -help</code>          | 一般的なコマンドライン引数のヘルプを表示します。                                                                                                                               |
| <code>-c</code>                | インストールをコンソールモードで実行します。                                                                                                                                 |
| <code>-q</code>                | インストーラを無人モードで実行します。                                                                                                                                    |
| <code>-g</code>                | インストールを GUI モードで実行します(Windows のみ)。                                                                                                                     |
| <code>-console</code>          | インストーラを無人モードで実行し、Windows で <code>-console</code> 引数を指定すると、2 つ目のコンソールにインストーラの出力が表示されます。                                                                 |
| <code>-overwrite</code>        | インストーラに指定した上書きポリシーに関係なく、無人モードでインストーラが全てのファイルを強制的に上書きします。                                                                                               |
|                                |  <b>注意</b><br>これにより、設定が上書きされてデフォルト値に戻る場合があります。                      |
| <code>-dir</code>              | 無人モードでのみ有効で、Contrast をインストールするディレクトリを指定します。                                                                                                            |
| <code>-dinstall4j.debug</code> | デフォルトでは、インストーラは全ての例外を取得してクラッシュログを作成し、そのログファイルの場所をユーザに通知します。これはインストーラのデバッグ時に不便な場合があります。そのため、このシステムプロパティがデフォルトの仕組みをオフにして、例外を <code>stderr</code> に出力します。 |

| コマンドライン引数                                                         | 説明                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|-------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| -Dinstall4j.keepLog=true<br>-Dinstall4j.alternativeLogfile=[path] | <p>インストーラによって、全てのインストールとアンインストールで i4j_log という接頭辞が付いたログファイルが temp ディレクトリに作成されます。このログファイルは、デバッグに役立ちます。インストーラに <b>Install files</b> アクションがあり、正常に終了した場合は、ログファイルが [installation dir]/install4j/installation.log にコピーされます。そうでない場合は、デフォルトでは、インストールやアンインストール終了後にファイルは削除されます。</p> <p>-Dinstall4j.keepLog=true option を使用すると、ログファイルは削除されません。-</p> <p>Dinstall4j.alternativeLogfile=[path] オプションを使用すると、ログファイルは [path] で指定されたファイルにコピーされます。ここには絶対パス名を指定してください。ログファイルが既にインストールディレクトリにコピーされている場合は、どちらのオプションも無効です。</p> |
| -varfile (filename)                                               | <p>使用する変数ファイルを指定します。無人モードでインストールする場合に、インストーラで設定するデフォルト値をカスタマイズできます。</p>                                                                                                                                                                                                                                                                                                                                                                                                                                |
| --skip-preflight                                                  | <p>事前チェック(現在のユーザが root であるか、依存関係があるか)をスキップします。このパラメータを使用する場合は、コマンドラインで渡す最初のパラメータでなければなりません。</p>                                                                                                                                                                                                                                                                                                                                                                                                        |



### 注記

Contrast を分散環境で使用する場合は、セットアップ時に分散型の MySQL インスタンスを使用する必要があります。



### 重要

クライアントであるエージェントは、Contrast URL を使用して Contrast サーバと通信します。Contrast では、ホスト名を決定してこの値を事前に指定できますが、指定したホスト名がネットワーク上のクライアントで解決できない場合、サーバと通信できなくなります。

この値には、エージェントホストから到達可能な Contrast ホストかロードバランサを設定してください。

4. インストールが完了し、Contrast アプリケーションで初期設定が行われます。完了したことを確認するには、上記で指定した URL にアクセスします。



### 注記

Contrast のバージョンをアップグレード (768ページ) している場合は、ここで必要な更新タスクが行われます。

5. インストール後、初めて Contrast アプリケーションを起動した時に、ユーザインターフェイスに **ログインできるのは 2 ユーザだけです (756ページ)**。デフォルトのスーパー管理者(SuperAdmin)とデフォルトの組織管理者(Admin)です。http://<ContrastServer>:8080/Contrast (<ContrastServer> はインストール時に指定した IP アドレスかホスト名)にアクセスして、両方のユーザとしてログインして、それぞれのパスワードを変更してください。



### 重要

アプリケーションを安全に保つために、これらのデフォルトのログインを無効にして新しいユーザを作成するか、少なくともデフォルトのパスワードを変更してください。

- Contrast のインストールが完了したら、次は[システムの設定 \(800ページ\)](#)(ライセンスの割当て、認証の設定、ユーザへの通知、レポートの実行など)を行ってください。  
ライブラリデータを最新に保つために、[ライブラリデータを自動で更新 \(771ページ\)](#)するようにシステムを設定してください。インターネットに接続できない環境(エアギャップでのインストール)の場合は、[ライブラリデータを手動で更新 \(770ページ\)](#)してください。

## その他のオプション

Contrast のインストール後に、インストールを拡張することができます。

- [分散 MySQL データベース \(750ページ\)](#)を使用する
- [WAR ファイル \(749ページ\)](#)を使用してデプロイする
- [分散環境 \(753ページ\)](#)で導入する

## WAR ファイルを使用して Contrast をデプロイ

この手順を使用すると、Contrast インストールのさまざまなコンポーネントを個別に管理できます。この方法を使用して Contrast をデプロイした後、既存の WAR ファイルを新しいファイルに置き換えることで、設定をアップグレードできます。

## 開始する前に

- [Contrast をインストール \(746ページ\)](#)します。

## 手順

- Contrast をインストールしたディレクトリ(例、`/usr/local/contrast`)から、以下のファイルを含む圧縮ファイルを作成します。

- `data/agents/`
- `data/conf/`
- `data/esapi/`
- `data/.contrast`
- `data/.initialized`
- `data/cache/`
- `data/contrast.lic`
- `webapp/Contrast.war`

例：以下の例は、Contrast ファイルを含む TAR ファイルを作成する方法を示します。

```
$ cd /usr/local/contrast
$ tar -czvf ~/ctdc.tar.gz data/agents data/conf data/contrast.lic data/
esapi/ data/cache/ data/.initialized data/.contrast webapp/Contrast.war
```

- Tomcat と Java をインストールします。

- Tomcat は、Contrast インストーラに含まれるものと同じバージョンを使用してください。
- [サポート対象の Java バージョン \(742ページ\)](#)

- `contrast-data` ディレクトリをセットアップします。

このディレクトリを作成するボリュームは、ログファイル、キャッシュ、ActiveMQ の永続性(パーシステンス)に対して十分な大きさである必要があります。最適なパフォーマンスを確保するには、システム全体に影響を与えずに、拡張を処理する別のボリュームを使用します。

- 以下のようなコマンドを使用して、`contrast-data` ディレクトリを作成します。

```
$ mkdir /opt/contrast-data
```

この例では、`/opt` ディレクトリにディレクトリが作成されますが、任意の場所に作成できます。

- 手順 1 で作成した圧縮ファイルを `contrast-data` ディレクトリに解凍します。
- 以下のコマンドなどを使用して、ディレクトリの内容を確認します。

```
ls /opt/contrast-data/conf
```

general.properties や database.properties という名前のファイルなどがあることを確認できるはずですが。

- d. アクセスの問題が無いようにするために、以下のようなコマンドで contrast-data ディレクトリの所有者とグループを変更します。

```
$ chown -R tomcat7:tomcat7 /opt/contrast-data
```

4. 設定を完了するには、JAVA\_OPTS 環境変数で contrast.home と contrast.data.dir の場所を、圧縮ファイルを解凍した場所に設定します。

以下は、JAVA\_OPTS 変数を設定する 1 つの例です。お使いの環境のドキュメントを参照して、この変数を設定する最適な方法を決定してください。

```
-XX:+UseTLAB
-XX:+UseCompressedOops
-XX:+UseConcMarkSweepGC
-XX:+UseParNewGC
-XX:CMSFullGCsBeforeCompaction=1
-XX:+CMSParallelRemarkEnabled
-XX:+PrintVMOptions
-XX:+PrintCommandLineFlags
-Xmx4g
-Xms4g
-server
-XX:MaxPermSize=768m
-Dcontrast.data.dir=/opt/contrast-data
-Dcontrast.home=/opt/contrast-data
-XX:+HeapDumpOnOutOfMemoryError
-Xloggc:/opt/contrast-data/gc.out
```

5. Contrast.war ファイルを Tomcat の webapps ディレクトリに配置します。シンボリックリンクを作成するか、圧縮したファイルを解凍した場所から Contrast.war ファイルを Tomcat の webapps ディレクトリにコピーまたは移動します。
  - 以下は、Ubuntu 環境でファイルへのシンボリックリンクを作成する方法の例です。

```
$ sudo ln -s /opt/contrast-data/webapp/Contrast.war /var/lib/tomcat7/webapps/Contrast.war
```

- 以下は、Ubuntu 環境でファイルをコピーする方法の例です。

```
$ cp /opt/contrast-data/webapp/Contrast.war /var/lib/tomcat7/webapps/Contrast.war
```

## 分散型 MySQL 環境の作成

オンプレミス版の既存のインストールで、外部の MySQL データベース(Windows と Linux の両方で動作するオープンソースデータベース)を使用することができます。例えば、これは [Contrast の分散環境 \(753ページ\)](#) を使用する場合などに必要となります。



## ヒント

運用担当者やデータベース担当者と協力して、安全で耐久性のあるインストールを行ってください。

**Ansible のスニペット**を使用して、Ubuntu 14.04 に MySQL をインストールすることもできます。

また、**GPG キーファイル**は MySQL からダウンロードすることもできます。Contrast では、バインドアドレス(bind\_address)を「\*」に変更していますが、ご利用の MySQL サーバとアプリケーションサーバの IP にバインドすることをお勧めします。ユーザを作成して、Contrast スキーマのみへアクセス、ホストの IP アドレスとサブネットに制限する権限を与えてください。

## 手順

以下の手順で、<jdbc.host><jdbc.port><jdbc.user>、<jdbc.pass>、<jdbc.schema>をご利用のホスト、ポート、ユーザ、パスワード、スキーマに置き換えてください。

1. データベースサーバのホストに**サポート対象バージョン (742ページ)**の MySQL をインストールして構成します。
2. Contrast のダウンタイムのためのメンテナンス時間を設けます。
3. **組み込みの MySQL データベースをバックアップ (809ページ)**します。
4. MySQL に接続します。

- **Windows :**

```
mysql -h <jdbc.host> -P <jdbc.port> -u <jdbc.user> -p <jdbc.schema>
```

- **Linux :**

```
./mysql -h <jdbc.host> -P <jdbc.port> -u <jdbc.user> -p <jdbc.schema>
```

5. 次のコマンドで Contrast のデータベースを作成します。

```
create database <jdbc.schema>;
```

6. 次のコマンドで MySQL ユーザを作成します。

```
CREATE USER '<jdbc.user>'@'%' IDENTIFIED BY '<jdbc.pass>';
```

7. 次のコマンドで Contrast ユーザに権限を付与します。

```
GRANT ALL PRIVILEGES ON *.* to '<jdbc.user>'@'%;
```

8. MySQL を終了(exit)します。
9. MySQL のバックアップを復元します。<backup\_location>をバックアップファイルの場所に、<backup\_filename>をバックアップファイル名に置き換えてください。

- **Windows :**

```
mysql -h <jdbc.host> -P <jdbc.port> -u <jdbc.user> -p <jdbc.schema> < \<br><backup_location>/<backup_filename>
```

- **Linux :**

```
./mysql -h <jdbc.host> -P <jdbc.port> -u <jdbc.user> -p <jdbc.schema> \<br>< <backup_location>/<backup_filename>
```

10. **暗号化プロパティエディタ (807ページ)**で設定を更新します。暗号化ファイルの \$CONTRAST\_HOME/data/conf/database.properties を編集します。database.type を検索してください。存在しない場合は、プロパティを新規に作成してください。このプロパティの値に distributed を指定し、使用する分散データベースを指すようデータベースの接続に関する値も更新します。

```

user@ubuntu:/opt/contrast/bin$ ./edit-properties -e ../data/esapi/ -
f ../data/conf/database.properties
jdbc.type : MYSQL
database.prod.dir : /opt/contrast/data/db
jdbc.debug : false
jdbc.pass : pass
jdbc.schema : contrast
jdbc.host : ubuntu
database.bk.time : 6:39:14
jdbc.port : 3306
database.bk.enabled : false
database.enabled : true
jdbc.url : jdbc:mysql://
ubuntu:3306/contrast
jdbc.user : contrast
database.bk.dir : /opt/contrast/data/
backups/db
jdbc.dialect : \
com.aspectsecurity.contrast.teamserver.persistence.CustomMySQL5Dialect
jdbc.driver : com.mysql.jdbc.Driver

Enter the name of the property to edit [q to Quit]: database.type
Create new Property [database.type](y/N): y
Enter a value for the property: distributed

jdbc.type : MYSQL
database.prod.dir : /opt/contrast/data/db
jdbc.debug : false
jdbc.pass : pass
jdbc.schema : contrast
jdbc.host : ubuntu
database.bk.time : 6:39:14
jdbc.port : 3306
database.bk.enabled : false
database.enabled : true
database.type : distributed
jdbc.url : jdbc:mysql://
ubuntu:3306/contrast
jdbc.user : contrast
database.bk.dir : /opt/contrast/data/
backups/db
jdbc.dialect : \
com.aspectsecurity.contrast.teamserver.persistence.CustomMySQL5Dialect
jdbc.driver : com.mysql.jdbc.Driver

Enter the name of the property to edit [q to Quit]:

```



### 注記

デフォルトの組み込みデータベースから分散環境に切り替える場合は、`database.bk.enabled` を `false` に設定することも必要です。分散データベース構成で Contrast を実行する場合、バックアップの設定は各自の責任で行ってください。



11. オンプレミス版を Windows システムにインストールしている場合は、MySQL に対する `contrast-server` サービスの依存関係を削除します。  
Contrast を再起動する前に、以下のコマンドを使用して、MySQL サービスに対する `contrast-server` サービスの依存関係を削除してください。

```
sc config contrast-server depend= ""
```

12. Contrast を再起動 (757ページ)します。

## 分散環境における Contrast の構成

Contrast を分散環境で構成するには、データベースとアプリケーションサーバを別々のサーバに配置します。分散構成は、次のような場合に使用します。

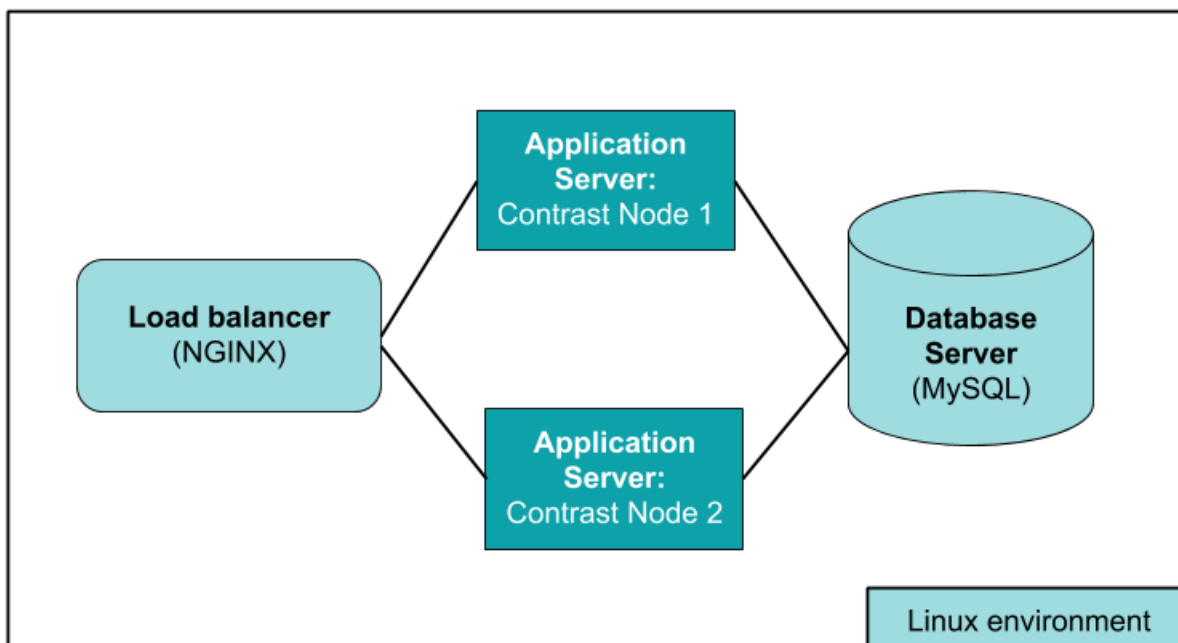
- 接続するエージェント数が 100 以上になる予定がある  
このような場合に分散構成を使用しないと、パフォーマンスの問題が発生する可能性があります。
- パフォーマンスとスケーラビリティの向上のためロードバランシングを利用したい
- 追加の管理や運用が必要

## 分散構成の例

ここでは、Linux 環境で Contrast を `/usr/local/contrast` にインストールする場合の設定を例として使用します。ご利用の組織で異なる環境を使用する場合や、サードパーティ製ソフトウェアのインストール先に関するガイドラインが異なる場合があります。

本項では、以下のように各サーバを使用する構成を例とします。

- 1 台のロードバランサー
- 1 台のデータベースサーバ
- Contrast アプリケーションを実行する 2 台のアプリケーションサーバ  
必要に応じて、さらにサーバを増やすことができます。



## 開始する前に

- Contrast を分散環境で構成するには、ご利用の環境およびその環境で問題なく処理できる負荷等について理解している必要があります。  
分散環境の導入が適しているか、もしくはお客様専用の Contrast の SaaS インスタンスを使用するのが最適かを判断するために、まずは弊社サポートまでお問い合わせください。

- 既に **Contrast** を使用している場合は、既存のインスタンスを **アプリケーションサーバ 1**(Contrast Node 1)に使用し、分散データベース構成を使用していることを確認してください。続行する前に、次の操作を行う必要があります。
  - MySQL の分散環境をまだ構築していない場合は、[分散型 MySQL を作成 \(750ページ\)](#)します。
  - VERSION ファイル(/usr/local/contrast/VERSION)を参照して、Contrast アプリケーションのバージョン番号を取得します。次のコマンドで、Contrast のデータベースバージョンを取得します。

```
select `version` from schema_version ORDER BY `installed_on` DESC LIMIT \1;
```

上記のバージョン番号は、タスクの順序を決めるために必要です。

例えば、アプリケーションのバージョンが 3.3.2 で、データベースのバージョンが 3.3.2.012 の場合、データベースのバージョン番号から .012 を除いても問題ないため、バージョンは同じと言えます。そのため、既存のアプリケーションサーバ A は、バージョン 3.3.2 の別のデータベース B で実行できます。新しいアプリケーションサーバ C にアプリケーションバージョン 3.4.2 をインストールして、データベース B に接続したい場合は、サーバ C にバージョン 3.4.2 をインストールする前に、サーバ A を停止するか更新する必要があります。

- **Contrast** を新規にインストールする場合は、次の操作が必要です。
- [Contrast のシステム要件 \(742ページ\)](#)に従い、データベースサーバに MySQL をインストールして構成します。リモート接続の権限を持つ MySQL ユーザを作成します。Contrast への接続には、この認証情報を使用します。
- **アプリケーションサーバ 1**(Contrast Node 1)に、分散データベース構成で [Contrast をインストール \(746ページ\)](#)します。
- 分散 MySQL インスタンス(Distributed [2])のオプションを選択します。データベースの作成をデータベースサーバに指定します。以下は、その例です。

```
Choose a MySQL database configuration.
Default [1, Enter], Distributed [2]2
Host
[localhost]
<enter hostname of Mysql server>

Port
[13306]
3306

Credentials
Username
contrast

Password
<enter mysql password for contrast account>
```

## 各分散サーバの設定

1. アプリケーションサーバ 1(Contrast Node 1)以下の設定ファイルをアーカイブして、TAR ファイルを作成します。
  - data/conf/
  - data/esapi/
  - data/contrast
  - data/initialized
  - data/contrast/lic
  - webapp/Contrast.war
  - VERSION

以下の例のようなコマンドを使用します。

```
$ cd /usr/local/contrast
$ tar -czvf ~/ctdc.tar.gz data/agents data/conf data/contrast.lic data/
esapi/ data/.initialized data/.contrast webapp/Contrast.war/.contrast \
VERSION
```

2. **アプリケーションサーバ 2(Contrast Node 2)**に **Contrast をインストール (746ページ)**します。インストールの処理は、特権ユーザとして実行してください。
  - Windows の場合、インストーラを右クリックして、**管理者として実行**を選択します。
  - Linux の場合、`sudo` コマンドを使用してインストーラを起動します。



### 重要

```
Full or Application Only Install
Choose the desired installation type:
Full install [1, Enter], Application Server Only [2]
2
```

**Application Server Only** を選択し、前の手順で作成した TAR ファイルを使用します。分散構成に追加する他のアプリケーションサーバについても同じ手順を実行します。

3. Contrast で作成された **デフォルトユーザ (756ページ)**でテストして、Contrast の両方の **アプリケーションサーバ (Node 1 および Node 2)**が機能することを確認してください。
4. 4 台目のサーバにロードバランサ(NGINX など)を設定します。NGINX を選択した場合は、**基本的なインストール手順**を使用してください。



### 注記

Contrast では、パフォーマンスを向上させるためにパーシステンスまたはステイキセッションが必要です。例えば、NGINX ロードバランサでは、IP ハッシュ方式を使用して、同じアドレスからのリクエストが使用可能な場合に、同じサーバに届くことを保証します。

5. サーバをセットアップしたら、ロードバランサを指定するように Contrast を設定する必要があります。この設定を行うには、各ノードの `/data/conf/general.properties` ファイルを編集します。YAML 設定ファイルの `teamserver.url` の値をロードバランサの値に変更し、Contrast アプリケーションサーバを再起動します。

ロードバランサのヘルスチェックを行う場合は、以下の URL を使用します。

```
<CONTRAST_SERVER>/Contrast/api/public/ng/information
```

ここで、`<CONTRAST_SERVER>`は Contrast アプリケーションのサーバのホスト名になります。



### 重要

エージェントは、Contrast URL を使用してアプリケーションと通信します。Contrast はホスト名を判断することで、この値をあらかじめ設定します。ネットワーク上のクライアントが指定されたホスト名を解決できない場合、クライアントはサーバと通信できなくなります。この値には、エージェントが到達可能な Contrast のホストかロードバランサを設定してください。

インストールが完了すると、Contrast の初期設定が始まります。完全に起動するまでに 2〜3 分かかることがあります。

6. 設定の進行状況を確認するには、`server.log` と `contrast.log` をチェックしてください。サーバが正常に起動すると、`server.log` に次のようなメッセージが表示されます。

```
260916 20.18.25,837 {} {} {} INFO (Server.java:303) Contrast \
TeamServer Ready -
```

## Contrast の実行

Contrast を実行するには :

- **Windows** : Windows では、Contrast はシステムサービスとしてインストールされます。サービスは Windows Service Manager アプリケーションを通じて開始および停止できます。
- **Linux** : Contrast デーモンは `init.d` として登録されます。サービスを開始および停止するには以下のコマンドを使用します。

```
/etc/init.d/contrast-server <start|stop|restart|status>
```

または

```
service contrast-server <start|stop|restart|status>
```

親シェルとは別に Contrast サーバを起動するには、以下のコマンドを実行します。

```
nohup /path/to/installation/contrast/bin/contrast-server start >/dev/
null 2>1
```

この時点で、サーバログに対して `tail` を実行すると便利です。

```
$ tail -f $CONTRAST_HOME/logs/server.log
```

次に、アプリケーションログに対して実行します。

```
$ tail -f $CONTRAST_HOME/logs/contrast.log
```

Contrast が正常に起動すると、`server.log` に以下のメッセージが表示されます。

```
190116 21.22.15,703 {} {} {} INFO (ConnectionTester.java:50) Received \
code 200 from TeamServer
190116 21.22.15,707 {} {} {} INFO (ConnectionTester.java:60) Server start \
has been verified
190116 21.22.15,709 {} {} {} INFO (Server.java:319) Contrast TeamServer \
Ready - Took 208323ms
```

## デフォルト認証情報と SuperAdmin 認証情報の管理

Contrast をインストールするシステム管理者には、管理すべき認証情報が 3 セットあります。

- **Contrast Hub の認証情報** : 新規のお客様は、ユーザ名とパスワードを設定するためのリンクが記載された電子メールが届きます。 [インストーラのダウンロード \(746ページ\)](#) と [Contrast Hub](#) へのログインには、この認証情報が必要です。
  - **ユーザ名** : Contrast から、`example@domain.com` の形式でユーザ名が提供されます。これは、デフォルトの組織管理者(Admin)と同じユーザ名です。
  - **パスワード** : アクティベーションメールのリンクを選択した際に、このパスワードを作成します。
- **デフォルトのスーパー管理者(SuperAdmin)の認証情報** : SuperAdmin の認証情報は、ライセンスに含まれています。 [SuperAdmin ロール \(821ページ\)](#) で Contrast アプリケーションを管理するために使用します。
  - **ユーザ名** : Contrast から、`contrast_superadmin@domain.com` の形式でユーザ名が提供されます。`domain` の部分は、お客様の会社のメールアドレスになります。
  - **パスワード** : デフォルトのパスワードは `default1!` です。
- **デフォルトの組織管理者(Admin)の認証情報** : 組織管理者は、この認証情報を使って、 [インストール \(746ページ\)](#) 後に Contrast にログインして、組織の設定や管理を行います。
  - **ユーザ名** : Contrast から、`example@domain.com` の形式でユーザ名が提供されます。これが、デフォルトの組織管理者のユーザ名です。

- **パスワード** : デフォルトのパスワードは、default1!です。



### 重要

ログインに成功したら、提供されたデフォルトのパスワードをすぐに変更してください。SuperAdmin のパスワードをリセットするには、[Contrast UI を使用 \(477ページ\)](#)するか、[Windows \(800ページ\)](#)または [Linux \(799ページ\)](#)のコマンドラインを使用してください。

## Contrast の再起動

Contrast を再起動するには :

1. 再起動するには、以下のコマンドを使用します。

- **Windows** :

```
net stop "Contrast Server"
```

サービスが完全にシャットダウンしたら、以下のコマンドを使用します。

```
net start "Contrast Server"
```

- **Linux** :

```
sudo service contrast-server restart
```

2. この時点で、サーバログに対して tail を実行すると便利です。

```
$ tail -f $CONTRAST_HOME/logs/server.log
```

3. 次に、アプリケーションログに対して実行します。

```
$ tail -f $CONTRAST_HOME/data/logs/contrast.log
```

4. Contrast が正常に起動すると、server.log に以下のメッセージが表示されます。

```
190116 21.22.15,703 {} {} {} INFO (ConnectionTester.java:50) Received \
code 200 from TeamServer
190116 21.22.15,707 {} {} {} INFO (ConnectionTester.java:60) Server \
start has been verified
190116 21.22.15,709 {} {} {} INFO (Server.java:319) Contrast \
TeamServer Ready - Took 208323ms
```

## Contrast のアンインストール

インストールには、Contrast と、Java、Tomcat、MySQL などのすべての組み込みコンポーネントを安全にアンインストールするためのスクリプトが含まれます。このスクリプトは、Contrast インストールの root ディレクトリ内にパッケージ化されています。Unix では、このファイルは *uninstall* とラベル付けされた実行可能なスクリプトです。Windows では、コマンドファイルが *uninstall.cmd* というインストールディレクトリ内にパッケージ化されています。

アンインストールする前に以下を実行します。

- Contrast で提供されるデータベースのバックアップツールを使用して [MySQL のバックアップを作成 \(809ページ\)](#)します。
- Windows または Unix のサービススクリプトを使用して Contrast をシャットダウンします。

**Windows** を使用して Contrast をサーバから削除するには :

1. Windows エクスプローラーを開きます。
2. Contrast のインストールディレクトリに移動します。
3. `uninstall.exe` のファイルをクリックして実行します。インストールを実行したときと同じ(管理者としての)権限でアンインストールを実行します。
4. プロンプトに従ってアンインストールを実行します。

Unix を使用して Contrast をサーバから削除するには :

1. Linux コンソールを開きます。
2. ディレクトリ(`cd`)を Contrast のインストールディレクトリに変更します。
3. コマンド `uninstall` を実行します。
4. プロンプトに従ってアンインストールを実行します。



### 注記

アンインストールを実行すると、ファイルの大半は削除されます。ただし、管理者は以下のようないくつかの残りのファイルを手動で削除しなければならない場合があります。

- *Contrast HOME* ディレクトリ
- *Contrast DATA* ディレクトリ
- *Contrast LOGS* ディレクトリ
- *Contrast MYSQL* ディレクトリ

## インストール後の作業

Contrast をインストールした後に、Contrast の環境を改善したい場合に設定できるオプションがいくつかあります。

### インストール後の作業

インストール後の作業には、以下のようなオプションがあります。

- [Tomcat の設定 \(758ページ\)](#)
- [Java ランタイム環境\(JRE\)の設定 \(759ページ\)](#)
- [HTTPS の設定 \(759ページ\)](#)
- [MySQL のカスタマイズ \(762ページ\)](#)
- [レポート用ストレージの設定 \(764ページ\)](#)
- [ログの設定 \(766ページ\)](#)
- [Redis を共有キャッシュに使う \(766ページ\)](#)

### Tomcat の設定

[インストール \(746ページ\)](#)中、Contrast が実行されている組込みの Tomcat サーバが使用するメモリについて、いくつか値を設定します。

アプリケーションを追加したり、検出する脆弱性を増やしたりすると、パフォーマンスが低下する場合があります。その場合は、このサーバで許可されている最大メモリに達したことを示している可能性があります。

メモリ設定を増やすには :

1. `contrast-server stop` コマンドを実行して、Contrast サーバを停止します。
2. サーバが停止し、`Contrast/logs/contrast-stdout.log` の末尾に `[MysqldResource] shutdown complete` が記録されていれば、メモリ設定を安全に変更できます。

- Contrast bin ディレクトリ `c:/Program Files/Contrast/bin` またはデフォルトの `/opt/Contrast/bin` にある `contrast-server.vmoptions` という名前のファイルを開きます。このファイルには以下のような内容が記述されています。

```
-XX:+UseG1GC
-XX:+UseStringDeduplication
-XX:+PrintVMOptions
-XX:+PrintCommandLineFlags
-XX:+UseContainerSupport
-XX:InitialRAMPercentage=50.0
-XX:MaxRAMPercentage=50.0
-XX:MinRAMPercentage=50.0
-Dcontrast.data.dir=/opt/contrast-data
-Dcontrast.home=/opt/contrast-data
-XX:+HeapDumpOnOutOfMemoryError
-Xloggc:/opt/contrast-data/gc.out
-server
```

- 以下の値を更新できます。
  - `Xms` : 起動時にサーバに割り当てられたメモリの量
  - `Xmx` : サーバが使用できる最大メモリ
  - `MaxPermSize`これらの値は、Contrast をホストするマシンで使用可能なメモリに応じて変わる可能性があります。
- ファイルを保存し、`contrast-server start` コマンドを使用して Contrast を再度起動します。



### ヒント

チューニングのヘルプについては、[JVM のドキュメント](#)を参照してください。

## Java ランタイム環境(JRE)の設定

[インストール \(746ページ\)](#)中には、組み込みの JRE または事前インストールされた JRE のいずれかを使用できます。

JRE を設定するには :

- テキストエディタを使用して `$CONTRAST_HOME/install4j/pref_jre.cfg` を開きます。
- 使用する Java バージョンへの完全なパスを追加します。例 :

```
C:\Program Files\Java\jre11
```

## HTTPS の設定

デフォルトでは、Contrast とエージェント間の接続に HTTP が使用されます。必要に応じて、Contrast とエージェントの両方の通信で HTTP を HTTPS に追加または置き換えます。これは Tomcat のコネクタ機能で実現できます。これを行う方法は 2 つあります。

- Contrast HTTPS コネクタ** : 証明書を Java キーストアに追加して、指定したポートで HTTPS 接続するように Contrast を設定します。
- リバースプロキシ方式** : Apache や NGINX などの標準 Web サーバを Contrast サーバの前面に構築し、Contrast の AJP コネクタを使用してリバースプロキシとなるように設定します。

[オンプレミス版の Contrast サーバで TLS バージョンや暗号スイートを変更する方法](#)で説明しているように、設定をさらにカスタマイズすることもできます。

## Contrast HTTPS コネクタの使用法

以下の手順で、オンプレミス版の Contrast アプリケーションサーバが使用する署名付き証明書を含む Java キーストア(JKS)を作成します。

1. Java の `keytool` コマンドを使用して、`contrast-server` というエイリアス名で証明書の秘密鍵と公開鍵を含む Java キーストア(JKS)ファイル(例、`contrast.jks`)を作成します。

```
keytool -genkeypair -alias contrast-server -keyalg RSA -keystore \
contrast.jks
```



### 重要

Java キーストア(JKS)と秘密鍵を作成する際に、両方のパスワードが同じであることが重要です。パスワードが異なる場合、HTTPS コネクタは動作しません。

2. 証明書署名要求(CSR)ファイル(`contrast.csr`)を生成します。必要に応じて、DNS 名や IP アドレスのフィールドを追加して、証明書に Subject Alternative Names(サブジェクトの別名)を含めることができます。

```
keytool -certreq -alias contrast-server -file contrast.csr -keystore \
contrast.jks -ext san=dns:your_hostname.your_company.com,ip:10.0.0.1
```

3. 生成した証明書署名要求(CSR)ファイルを CA(認証局)に送信します。CA(認証局)から、PEM 形式の複数ファイルか、PKCS#7 形式の 1 ファイルのいずれかが提供されます。
4. CA から提供されたファイルを Java キーストア(JKS)にインポートします。以下の手順を、提供されたファイルの形式に合わせて使用してください。



### 注記

Contrast で SSL 証明書を使用するためには、証明書をパスワードで保護することはできません。

- **複数の PEM 形式ファイル** : これらのファイルの拡張子は、.CRT または .PEM です(PEM ファイルは読み取り可能なテキストとして開けます)。そのうち 1 つにはサーバ証明書が含まれ、その他のファイルはルート証明書と中間証明書が含まれることになります。これらの証明書は、上位(ルート証明書)から順にキーストアにインポートし最後にサーバ証明書をインポートする必要があります。サーバ証明書には、キーストアの作成時に使用したのと同じエイリアス名が必要です。例えば、`root.cer`、`inter.cer`、`server.cer` が提供された場合は次のようにインポートします。

```
keytool -import -trustcacerts -alias root -file root.cer -keystore \
contrast.jks
keytool -import -trustcacerts -alias intermediate -file inter.cer -
keystore contrast.jks
keytool -import -trustcacerts -alias contrast-server -file server.cer -
keystore contrast.jks
```

- **PKCS#7 形式のファイル** : このファイルの拡張子は、.P7B か .CER で、場合によっては .CRT となります。このファイルには、必要な全てのルート証明書と中間証明書およびサーバ証明書が含まれています。サーバ証明書には、キーストアの作成時に使用したのと同じエイリアス名が必要です。例えば、`.p7b` のファイル証明書は次の様にインポートします。

```
keytool -import -trustcacerts -alias contrast-server -file \
certificate.p7b -keystore contrast.jks
```





### 注記

その他の形式で証明書が提供された場合は、異なる方法でキーストアを作成する必要があります。例えば、次のような場合です。

- server.crt、priv.key、inter.crt ファイルがある場合：以下のコマンドを使用して、ファイルを PKCS#12 形式に変換して、キーストアを作成します。

```
openssl pkcs12 -export -out cert.pfx -inkey priv.key -in \
server.crt -certfile inter.crt -name "contrast-server"
keytool -importkeystore -srckeystore cert.pfx -
srcstoretype pkcs12 -destkeystore contrast.jks -
deststoretype jks
```

- PKCS#12 形式のファイルの場合：以下のコマンドでキーストアを作成します。

```
keytool -importkeystore -srckeystore cert.pfx -
srcstoretype pkcs12 -destkeystore contrast.jks -
deststoretype jks
```

5. キーストアの設定が完了したら、テキストエディタで<YourPath>/data/conf/server.properties ファイルを開きます。<YourPath>は Contrast をインストールしたパスです。

<port>、<file>、<password>、<hostname> をそれぞれ、keytool コマンドで指定したポート、JKS ファイルのパス、パスワード、ホスト名のエイリアスに置き換えてください。

```
https.enabled=true
https.port=<port>
https.keystore.file=<file>
https.keystore.pass=<password>
https.keystore.alias=<hostname>
```



### 重要

Windows を使用している場合は、JKS ファイルへのフルパスをエスケープする必要があります。例えば、以下のようになります。

```
https.keystore.file=C:\\Program\\ Files\\Contrast\\data\\
\\conf\\ssl\\contrast-server.jks
```

http.enabled および ajp.enabled オプションを false に設定し、HTTPS 経由で行われた接続のみを Contrast サーバで許可するようにすると便利です。

6. <YourPath>/data/conf/general.properties ファイルをテキストエディタで開き、teamserv.url プロパティの値を編集して変更を反映します。この変更を行った後、一度エージェントを手動で更新する必要があります。それ以降のエージェントに対する更新は、自動的に行われます。
7. **任意**： TLS バージョンや暗号スイートを変更します。
8. Contrast server サービスを再起動し、設定した HTTPS ポートになっていることを確認してください。



### 注記

自己署名証明書で HTTPS コネクタを使用することもできます。

## リバースプロキシ方式の使用方法

リバースプロキシ方式で AJP(Apache JServ Protocol)を使用するには：

1. Contrast サーバが AJP プロトコルを使用して接続できるように設定します。テキストエディタで `CONTRAST_HOME/data/conf/server.properties` ファイルを開き、以下のオプションを設定します。

```
ajp.enabled=true
ajp.port=8009
ajp.secretRequired=true|false
ajp.secret=somesecret
```

`ajp.port` には、サーバが着信接続を待ち受けるポート番号を設定します。サーバへのアクセスを AJP コネクタによる接続のみにする場合は、`http.enabled` と `https.enabled` オプションを無効にします。

`secretRequired` を `true` にした場合は、`ajp.secret` に秘密キーワードを指定する必要があります。リクエストワークには、秘密キーワードが必要になり、そうでない場合はリクエストが拒否されます。ワーク間で一致する秘密キーワードを設定してください。一致しない場合、`secretRequired` の設定に関わらずリクエストは拒否されます。

2. `server.properties` ファイルを更新したら、Contrast server サービスを再起動して変更を有効にします。
3. フロントエンドサーバの構成については、お使いのサーバのドキュメントを参照して、AJP の設定方法を確認してください([Apache](#) や [NGINX](#) の AJP に関するドキュメントなど)。

## MySQL のカスタマイズ



### 注記

ここでの手順は、分散環境用の設定ではなく、組み込みの MySQL データベースに適用されるものです。

ご利用中の環境に合わせて、Contrast が MySQL データベースに指定したデフォルト設定の変更が必要になる場合があります。例えば、アップグレード後に、`innodb_buffer_pool_size` の設定の値の調整が必要になる場合などがあります。

デフォルトの MySQL の設定を変更するには、`my_extra.cnf` オプションファイルを使用します。このファイルは、オンプレミス版インストールの一部として Contrast インストーラに組み込まれています。

Contrast は、最初にデフォルトのオプションファイルをロードしてから、その後 `my_extra.cnf` ファイルに指定されたカスタム設定を適用します。

## 手順

1. `CONTRAST_HOME/data/conf/my_extra.cnf` ファイルを検索してください。
2. 必要に応じて、[MySQL の設定](#)を追加または変更します。
3. [Contrast を再起動 \(756ページ\)](#)します。または、Microsoft Windows を使用している場合は、MySQL サービスを再起動します。

## プロキシ構成の設定

オンプレミス版の Contrast でプロキシ構成を設定することによって、Contrast と同じネットワーク内に存在する(プロキシを必要としない)ツールと、ネットワーク外にある(Web プロキシアクセスを必要とする)ツールとを連携することができます。

## 設定方法

プロキシの設定を行うには、以下のいずれかを使用します。

- `contrast-server.vmoptions` ファイルにある JVM 引数
- Contrast Web インターフェイスでのプロキシ設定  
オプションファイルの JVM 引数は、Contrast Web インターフェイスの設定を上書きします。

## 手順

### • JVM 引数を使用する(推奨される方法) :

1. Contrast の bin ディレクトリ(`c:/Program Files/Contrast/bin` またはデフォルトディレクトリの `/opt/Contrast/bin`)で、`contrast-server.vmoptions` を開きます。
2. このファイルに、以下の JVM 引数を追加します(セキュリティ上、`https` 引数を使用するのが望ましいです)。
  - `https.proxyHost` または `http.proxyHost`  
プロキシサーバのホスト名です。この引数を使用して、外部にホストされているソフトウェアと通信します。
  - `https.proxyPort` または `http.proxyPort`  
プロキシサーバが、トラフィックをリッスンするポート番号です。
  - `http.nonProxyHosts`  
プロキシサーバを通過しないで直接接続するホストのリストを、縦線(|)で区切って指定します。この引数は、`https` および `http` の両方の設定で機能します。この引数を使用すると、Contrast のインストール先と同じネットワークにデプロイされているオンプレミスのホストを除外することができます。例えば、オンプレミス版の Jira をインストールしており、クラウド上の MS Teams とインテグレーションしている場合、以下の例のように `http.nonProxyHosts` 引数を使用すれば、Jira との連携にはプロキシサーバを経由しないよう除外することができます。

```
-Dhttps.proxyHost=89.148.22.17  
-Dhttps.proxyPort=3128  
-Dhttp.nonProxyHosts=jira.mycompany.com|*.internal.mycompany.com
```

この例では、プロキシホストは `89.148.22.17` で、トラフィックをリッスンするポート番号は `3128` です。この設定では、`jira.mycompany.com` のホストおよび `*.internal.mycompany.com` に一致するホストと通信する場合にプロキシサーバを経由しなくなります。

### • Contrast Web インターフェイスを使用する :

1. ユーザメニューで、**SuperAdmin** を選択します。
2. **システムの設定**を選択します。
3. 「インターネットの設定」で、**プロキシ**を選択します。



4. プロキシサーバのホスト名、ポート番号、ユーザ名、パスワードを指定します。

5. 保存を選択します。

## システムのレポート用ストレージを設定する

レポート用ストレージのオプションを設定するには、SuperAdminとして、`contrast/data/conf/general.properties` ファイルに以下のプロパティを追加します。

- `reporting.storage.mode` : ストレージモードのオプション値は、DB か `FILE_SYS` です。
- `reporting.storage.path` : 上記のストレージモードを `FILE_SYS` に設定した場合に必要です。

`reporting.storage.mode` の推奨設定は、`FILE_SYS` です。DB を設定する場合、ファイルはデータベースに格納され、不必要な競合がデータベースに追加されることとなります。

`FILE_SYS` オプションを使用する場合には、全ての Contrast ノードがファイルバスにアクセスできるファイル共有サービスを設定する必要があります。そのパスを `reporting.storage.path` の値として指定してください。



### 注記

パスは、`/Users/user1/reporting` のように絶対パスを指定します。

Windows の場合は、コロンをエスケープしないと、パスが機能しません。例えば、次のようなパスは機能しません。

```
reporting.storage.path=C:\Contrast\data\reports
```

パスを機能させるには、以下のようにコロンの前後にスラッシュまたは 2 つのバックスラッシュを使用する必要があります。

```
reporting.storage.path=C:\\Contrast\\datareports
```

デフォルトの設定では、コンプライアンス対応レポートから 1,250 件の脆弱性をエクスポートできます。1,250 件以上の脆弱性を含む大きなレポートを実行したい場合があるかもしれませんが、インスタンスのサイズによっては、Contrast のヒープ領域の問題が発生する可能性があります。

制限を増減するには、`general.properties` ファイルの `reporting.generation.limit` プロパティを設定して、Contrast を再起動してください。

## Contrast のログ

Contrast アプリケーションでは、**カスタムレベルに対応する Log4j** がログフレームワークとして使用されます。

ユーザは**ログのしきい値を設定 (766ページ)**し、ログファイルの宛先を管理し、Contrast 内で利用可能な各ログの概要を表示できます。

以下のログは、`$CONTRAST_HOME/logs` ディレクトリにあります。

- `server.log`
- `catalina.out`

以下のようなその他のログは、`$CONTRAST_HOME/data/logs` にあります。

- `contrast.log`
- `ldap_ad.log`
- `migration.log`
- `audit.log`
- `mysql_error.log`

以下の表に、Contrast 内の全てのプライマリログファイルを示します。

| ログファイル                           | 説明                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <code>audit.log</code>           | <p>以下のような監査イベントを記録します。</p> <ul style="list-style-type: none"> <li>• アプリケーションへのログインとログアウト</li> <li>• ほかのユーザへのなりすまし</li> <li>• 組織の切替え</li> <li>• 管理者ポータルへのアクセス</li> <li>• SuperAdmin アカウントによる Contrast の設定変更</li> <li>• ユーザアカウントサービスの問題(アカウントのロック、パスワードの変更、ほか)</li> <li>• トレースの削除</li> <li>• ライセンスの変更または期限切れライセンスの通知</li> <li>• API キーの変更</li> </ul> |
| <code>console.log</code>         | デフォルトのアプリケーションイベントログ                                                                                                                                                                                                                                                                                                                               |
| <code>contrast-error.log</code>  | <code>stderr</code> に出力されるログメッセージ                                                                                                                                                                                                                                                                                                                  |
| <code>contrast-stdout.log</code> | <code>stdout</code> に出力されるログメッセージ                                                                                                                                                                                                                                                                                                                  |
| <code>contrast.log</code>        | <p>Tomcat の <code>stdout</code> または <code>console</code> ログ同様、<code>contrast.log</code> ファイルは Contrast 内で発生する最も重要なイベントを表示して通知またはデバッグをサポートします。これには以下の情報が含まれます。</p> <ul style="list-style-type: none"> <li>• アプリケーション</li> <li>• サーバ</li> <li>• ライブラリ</li> <li>• トレース</li> <li>• ユーザ</li> <li>• サーバの例外発生時のデバッグ目的の Java スタックトレース</li> </ul>           |
| <code>security-events.log</code> | このログファイル(旧称 <code>esapi.log</code> )は、特定のプロパティファイルの読み込みなど、Contrast での重要なイベントを取得するために使用されます。                                                                                                                                                                                                                                                        |
| <code>migration.log</code>       | Contrast アプリケーションに対して更新までの間に発生する全てのデータベース移行の概要が含まれます。Contrast バージョン、実行された移行スクリプト、スクリプトのステータスを参照します。                                                                                                                                                                                                                                                |

## システムレベルでのログの設定

Contrast では、[イベントやメッセージを記録する複数のログファイル \(765ページ\)](#)が収集されます。

ユーザは、Contrast アプリケーションにパッケージ化された Log4j 設定をホストするために使用される `log4j2.xml` ファイルを設定でき(任意で [Log4j カスタムレベル](#)を適用でき)ます。



### 注意

フォーマットが構文的に正しいことを確認するため、このファイルに変更を加える前に、[変更が正しく入力されている場合はサーバを再起動する必要はありません。](#)

1. `$(CONTRAST_HOME)/data/conf` でファイルを検索します。
2. 以下に示すファイルの最初のパラメータは、定義された変数に基づいて設定を更新する監視インターバルです。デフォルトでは、Contrast は 60 秒ごとにログ設定をチェックして更新を行います。

```
<Configuration monitorInterval="60">
```

3. 必要に応じてファイルを編集します。



### ヒント

Appender およびログイベントの配信の詳細については [Log4j のドキュメント](#)を参照してください。Contrast では主に [Rolling File Appender](#) を使用します。これは `OutputStreamAppender` であり、`fileName` パラメータで指定されたファイルに書き込み、`TriggeringPolicy` および `RolloverPolicy` に応じてファイルをロールオーバーします。

`contrast.log` のアペンダのサンプルファイルを以下に示します。これは最大 1GB のファイルサイズポリシーとロールオーバーするファイル数が 15 以内に指定されたデイリーアペンダです。また、このアペンダでは毎日ファイルが圧縮され名前が変更されます。

```
<RollingFile name="DAILY" fileName="${contrast.logs.dir}/
logs/contrast.log"
    filePattern="${contrast.logs.dir}/logs/
contrast.%d.%i.log.gz" immediateFlush="true">
  <PatternLayout>
    <Pattern>%d{ddMMyy HH:mm:ss,SSS} {%X{session.id}} \
{%X{user.name}} {%X{remote.addr}} %-5p (%F:%L) %m%n
    </Pattern>
  </PatternLayout>
  <Policies>
    <TimeBasedTriggeringPolicy/>
    <SizeBasedTriggeringPolicy size="1 GB"/>
  </Policies>
  <DefaultRolloverStrategy max="15"/>
</RollingFile>
```

ファイルの `logger` セクションには、どの Java パッケージが特定のログレベルで特定のアペンダにログするかが定義されています。

## Redis を共有キャッシュに使う(オンプレミス版)

Redis サーバで共有キャッシュを使用するように Contrast を構成できます。

本項では、Redis サーバの設定についての詳細は説明しません。

## Redis の Contrast プロパティ

以下のプロパティを使用します。

プロパティ名	説明
cache.userredis	Contrast がキャッシュに Redis を使用するかどうかを示す Boolean 値を指定します。
contrast.cache.redis.db.index	Contrast がキャッシュ情報を保存するデータベース・インデックスを整数値で指定します。
contrast.cache.redis.proto	Contrast が Redis サーバに接続する際に使用するプロトコルを指定します。
contrast.cache.redis.host	Redis サーバのホスト名または IP アドレスを指定します。
contrast.cache.redis.port	Redis サーバが新しいクライアントの接続を待ち受けるために使用する TCP/IP ポートの番号を指定します。
contrast.cache.redis.password	クライアントから Redis サーバへのアクセスを許可するために使用されるパスワードを指定します。
contrast.cache.redis.client.name	クライアントを識別するための文字列を指定します。

## 開始する前に

- 以下の情報を準備してください。
  - Redis サーバのホスト名または IP アドレス
  - 接続を待ち受けるために使用する TCP/IP ポートの番号
  - Redis サーバのユーザアカウントのパスワード
  - キャッシュの対象となるデータベースのインデックス
- Redis サーバが TLS(REDIS)を使用するように設定されていることを確認してください。

## 手順

- /data/conf/フォルダ contrast.properties ファイルを作成します。  
このファイルに、contrast\_server ユーザがアクセスできる権限があることを確認してください。
- プロパティファイルに、Redis の Contrast プロパティを追加します。  
少なくとも、Redis サーバのホスト名、接続ポート番号、パスワードを設定してください。  
プロパティファイルの例：

```
cache.userredis=true
contrast.cache.redis.db.index=0
contrast.cache.redis.proto=rediss
contrast.cache.redis.host=contrast-redis-server.company.com
contrast.cache.redis.port=6379
contrast.cache.redis.password=changeme
contrast.cache.redis.client.name=contrast
```

- Contrast を再起動 (757ページ)します。
- 設定を確認するには /data/logs/contrast.log ファイルを確認します。  
このファイルには、現在の設定と Redis との操作に関する全ての情報が含まれます。確認すべきキーワードは以下の通りです。
  - RedissonCache
  - Redisson
  - CacheConfiguration

## システムの更新およびアップグレード

Contrast Security では、定期的にオンプレミス版 Contrast のソフトウェアの更新やアップグレードを行います。

## 更新およびアップグレード

以下の各手順を参照してください。

- [Contrast のアップグレード \(768ページ\)](#)
- [エージェントのアップグレード \(769ページ\)](#)
- [IP アドレスの更新 \(769ページ\)](#)
- [ライブラリデータの更新 \(770ページ\)](#)
- [ライブラリデータの自動更新 \(771ページ\)](#)
- [ライセンスの更新 \(771ページ\)](#)

## Contrast のアップグレード

Contrast のパッチやアップグレードは、オンプレミス版のインストーラファイルの一部として組み込まれてリリースされ、Contrast Hub(ハブ)からダウンロードできます。

インストーラは、指定されたシステムに Contrast の以前のバージョンがあるかを判断します。アップデートプログラムの処理を実行するか、別の場所でのインストールを実行するかを選択できます。前のバージョンのインストールが存在する場合は、並行してインストールを行い、別のポートで実行するように構成する必要があります。

## 開始する前に

`$CONTRAST_INSTALLATION/jre/lib/security` ディレクトリにある `cacerts` ファイルをバックアップしてください。

アップグレードの処理によってこのファイルが上書きされて、ログインの問題が発生する可能性があります。これらの証明書は [LDAP を統合 \(795ページ\)](#) する際に使用されます。

## 手順

1. [MySQL バックアップを作成 \(809ページ\)](#)し、バックアップファイルを別のファイルシステムまたはドライブに保存して、リストア時の問題を回避します。インストーラはアップグレード処理の一環としてデータベースのバックアップを作成しようとしていますが、安全のために手動で行ってください。また、`$CONTRAST_HOME/data/conf` にある全ての設定ファイルをバックアップしてください。
2. インストールプロセスを開始するときに、Contrast アプリケーションが実行されていることを確認します。この間、エージェントは脆弱性やライブラリのメッセージを送信し続けます。アプリケーションが自動的にシャットダウンを開始すると、エージェントはアプリケーションに到達できるまでメッセージの送信を延期します。
3. アップグレードプロセスは、最初に [Contrast アプリケーションをインストール \(746ページ\)](#)したプロセスとほぼ同じです。ただし、既存のインストールを更新するか、新規インストールを実行するかを選択するよう求められます。既存のインストールの更新を選択する必要があります。
4. アップグレードでは、最初にデータベースのバックアップが実行されます。データベースのサイズによって、この処理には数秒から数分までかかる場合があります。この処理の間、エージェントとエンドユーザは、アプリケーションにアクセスできているはずですが。
5. 次に、アップデートにより、インストールディレクトリ配下に新しいファイルシステムがデプロイされます。これは主に、`$CONTRAST_HOME/webapps` ディレクトリに `Contrast.war` ファイルをデプロイすることで行われます。ファイルシステムの更新中は、アプリケーションにアクセスできません。
6. ファイルシステムの更新が正常に完了すると、アプリケーションが起動します。アプリケーションの起動中に、ログファイル(具体的には `migration.log` や `contrast.log` など)の内容を確認できます。ファイルシステムおよびデータベースの両方の更新に関するログエントリが順次書き込まれます。



### 注記

設定ファイルやデータベースコンポーネントは、最初の起動ステップまで更新されません。



- 更新成功の最初の目安となるのは、Contrast の Web インターフェイスにログインするか API リクエストを使用して、Contrast アプリケーションにアクセスできるようになることです。



### ヒント

ユーザメニューに、使用中のバージョンのリリース情報へのリンクが表示されません。

- アップグレードの直後に *migration.log* の内容を確認してください。このログには、更新プロセスの一部で発生した問題が記録されます。



### 注記

アップグレードの数分後に、デプロイ済のエージェントが最新のエージェントバージョンへの更新を試みる場合があります。これらのエージェントでは、それぞれが再起動されて Contrast アプリケーションとの接続が確立されるまで、エージェント自体の更新は反映されません。

## エージェントのアップグレード (オンプレミス版)

ほとんどのエージェントは、パブリックリポジトリからダウンロードすることができます。.NET エージェントと .NET Core エージェントのダウンロードは、Contrast Hub にアクセスします。

ダウンロードしたエージェントを、Contrast サーバの `$CONTRAST_HOME/data/agents` ディレクトリ下にある各エージェント言語のサブディレクトリにコピーします。Contrast のオンプレミス版では、このディレクトリをサポートするよう自動的に構成されています。

### 手順

- 適切なリポジトリから最新版のエージェントをダウンロードします。
  - .NET : [Contrast Hub](#) からダウンロード
  - .NET Core: [Contrast Hub](#) から、.NET Core エージェントまたは IIS 用 .NET Core エージェントのインストーラをダウンロード
  - Java : [Maven](#) からダウンロード
  - Node.js : [NPM](#) からダウンロード
  - Python : [PyPI](#) からダウンロード
  - Ruby : [RubyGems](#) からダウンロード
  - Go : [Debian \(455ページ\)](#) または [RPM \(455ページ\)](#) からダウンロード
- ダウンロードした各エージェントを、`$CONTRAST_HOME/data/agents` ディレクトリ内にある各エージェント言語に対応するサブディレクトリにコピーします。  
例えば、Java エージェントをダウンロードした場合、Java エージェントを `$CONTRAST_HOME/data/agents/java` ディレクトリにコピーします。  
Contrast を再起動する必要はありません。エージェントは動的にリロードされ、ダウンロードできるようになります。

## IP アドレスの更新

Contrast アプリケーションのインストールを移動した場合やホスト名または IP アドレスを変更しなければならなかった場合は、以下のステップを実行する必要があります。

- SuperAdmin として Contrast にログインします。
- 右上で、**SuperAdmin > システムの設定 > 一般設定** を選択します。

3. 概要パネルで、TeamServer の URL を `IP:port/Contrast` に変更します。
4. 保存を選択します。
5. Contrast を再起動 (757ページ)して、変更を適用します。

## SCA ライブラリデータを手動で更新

Contrast バージョン 3.7.4 以降、SCA ライブラリデータを Contrast Hub から手動でダウンロードできるようになりました。これは、インターネットにアクセスできない場合(エアギャップでのインストール)に便利です。

### 開始する前に

- Contrast Hub のアカウントが必要です。
- 最適なパフォーマンスを得るために、ライブラリデータは毎月ダウンロードするよう計画してください。
- 複数のサーバを使用して分散環境でデプロイ (753ページ)している場合は、本項での手順を 1 つのインスタンスに対して使用してください。ダウンロードした同じライブラリデータファイルを複数のインストール先に使用できます。



#### 重要

MySQL 8 を使用しているオンプレミス版のお客様は、Contrast で CSV ファイルを受け取ることができるように、システム変数 `local_infile` を **ON** に設定する必要があります。詳細については、[LOAD DATA LOCAL のセキュリティ上の考慮事項](#)を参照してください。

### 手順

1. Contrast Hub にログインします。
2. Downloads(ダウンロード)を選択します。
3. Library Data Exports(ライブラリデータのエクスポート)から、必要なアーカイブバージョンをダウンロードしてください。



#### TeamServer

[Installers](#)

[Wars](#)

#### Library Data Exports

Release Date	File Name	File Size			
09/14/2021	Contrast-Data-Export-202109141732.zip	2.96 GB	<a href="#">Archive</a>	<a href="#">Download</a>	<a href="#">MD5 Sum</a>
09/13/2021	Contrast-Data-Export-202109131732.zip	2.95 GB	<a href="#">Archive</a>	<a href="#">Download</a>	<a href="#">MD5 Sum</a>
09/12/2021	Contrast-Data-Export-202109121732.zip	2.94 GB	<a href="#">Archive</a>	<a href="#">Download</a>	<a href="#">MD5 Sum</a>

- ダウンロードした ZIP ファイルを解凍して、CSV ファイルを `data/libraries` ディレクトリに配置します。  
ファイル名によっては非表示になっている可能性があるため、解凍した全てのファイルをこのディレクトリに移動したことを確認してください。
- Contrast を再起動します。(757ページ)**  
Contrast が再起動すると、バックグラウンドでデータがインポートされます。CSV ファイルは、インポートされる度にフォルダから削除されます。
- 各スクリプトの完了時に、`data/logs/contrast.log` ファイルに成功のメッセージが表示されます。例えば、次のようなメッセージです。

```
Beginning CSV import from 'C:\Program \
Files\Contrast\data\libraries\java.csv' into 'artifacts_java' Import \
temporary table 'artifacts_java' completed, time: 36.6886968s
```

## SCA ライブラリデータを自動で更新

Contrast バージョン 3.6.4 以降、Contrast の SCA ライブラリデータを自動で更新するよう設定できるようになりました。

Contrast は、約 24 時間ごとにライブラリデータを更新します。新しく追加された CVE は 30 分ごとに更新され、その後 24 時間のスケジュールに含まれます。お使いのオンプレミス版 Contrast で、クラウドにホストされている Contrast データベースからデータが取得されます。

## 開始する前に

- 以下の URL へのアクセスを許可するようにファイアウォールを設定してください。  
`https://ardy.contrastsecurity.com/production`
- SuperAdmin ロールが必要です。

## 手順

- Contrast Web インターフェイスに SuperAdmin ユーザとしてログインします。
- ユーザメニューから、**システムの設定**を選択します。
- 全般的な設定**を選択します。
- 「インターネットの設定」の下にある、**Contrast HUB** をオンにします。



## オンプレミス版の Contrast ライセンスの更新

Contrast のオンプレミス版をご利用のお客様は、ライセンス更新時に新しいライセンスファイルが必要になります。ライセンスファイルを更新する方法は、2 つあります。

- スーパー管理者(SuperAdmin)として Contrast アプリケーションにログインして、Contrast Web インターフェイスでライセンスを更新
- ローカルファイルシステムで、ライセンスファイルを置き換え(ライセンスの期限が切れている場合は、この方法で行う必要があります)

Contrast の Web インターフェイスでライセンスを置き換えるには：

1. SuperAdmin としてログインします。
2. 左側のナビゲーションでライセンス管理を選択します。
3. パネルの下部にある、このライセンスを更新をクリックします。
4. デフォルトの認証情報 (756ページ) を入力して、Contrast Hub(ハブ)から最新のライセンスをダウンロードして適用します。
5. にアクセスできない場合は、ライセンスをアップロードをクリックして、表示されたフィールドにライセンスをペーストします。
6. 更新を選択します。
7. Contrast を再起動 (757ページ) して、新しいライセンスの変更を適用します。

Contrast のファイルシステムでライセンスを置き換えるには：

1. 新しいライセンスを、Contrast Hub(ハブ)が御社のアカウント管理者、またはテクニカルサポート担当者から取得します。
2. 新しいライセンスファイルの名前を *contrast.new.lic* に変更します。
3. Contrast アプリケーションのサービスを停止します。
  - **Windows**：サービスコントロールパネルを使用します。
  - **Linux**：`sudo service contrast-server stop` を実行するか、ディストリビューションの設定に合わせて適切なコマンドを実行します。`ps aux | grep contrast` を実行し、Contrast アプリケーションの全てのプロセスが停止しており、実行中のプロセスがないことを確認します。`mysqld` がまだ実行中の場合、サービスの停止後にプロセス自体が終了するまでに数分かかることがあります。終了しない場合は、サポートにお問い合わせください。プロセスを強制終了しないでください。



### 重要

現在の *contrast.lic* ファイルは移動しないでください。Contrast では、ライセンスを更新するために、古いライセンスファイルと新しいライセンスファイルの両方が必要です。

4. 新しいライセンスファイルを `<contrast_home>/data` ディレクトリに配置します。  
Linux の場合は、新しいライセンスファイルの所有者、グループ、権限がそのディレクトリにあるほかのファイルと同一であることを確認します(`ls -l` を実行すると、ディレクトリの内容が権限と所有者の情報とともに表示されます)。起動時に新しいライセンスファイルが使用されると、*contrast.lic.bak* という名前で、現在のライセンスのバックアップが同じディレクトリ内に作成されます。  
ライセンスファイルの所有者とグループを変更するには、`sudo chown contrast_service:contrast_service contrast.new.lic` を実行します。  
権限を変更するには、`sudo chmod 644 contrast.new.lic` を実行します。
5. 通常どおりに Contrast アプリケーションを起動します。
  - **Windows**：サービスコントロールパネルを使用します。
  - **Linux**：`sudo service contrast-server start` を実行するか、ディストリビューションの設定に合わせて適切なコマンドを実行します。
6. 新しいライセンスが有効になります。

Contrast アプリケーションの全てのインスタンスを更新するには、実行中のアプリケーションインスタンスごとに、前述のファイルシステムを使用する方法に従ってください。

## システム運用の管理

組織の規模や Contrast をどのように管理するかによって、システムを運用する上で最適な [ロール \(821ページ\)](#) を設定できます。

小規模な組織では、1人のスーパー管理者(SuperAdmin ロール)が全てのシステム管理業務を行うことができます。業務を共有して行いたい場合は、追加のスーパー管理者(SuperAdmin)やサーバ管理者(ServerAdmin)を指定 (778ページ)することができます。

- **SuperAdmin** : スーパー管理者。Contrast のシステム管理を担当します。このロールは、1人または複数の個人に割り当てることができます。ユーザメニューの **SuperAdmin** オプションを利用し、組織、アプリケーション、サーバ、脆弱性、ユーザおよびグループを設定できます。
- **ServerAdmin** : サーバ管理者。ユーザやグループにアクセスできない以外は、SuperAdmin と同じです。ユーザメニューの ServerAdmin オプションを利用し、組織、アプリケーション、サーバおよび脆弱性を設定できます。

エンドユーザやエージェントのライセンスを管理する個人やグループが別にある場合は、システムのアクセスグループを追加 (779ページ)して、ユーザに **SystemAdmin** ロールや **Observer** を指定できます。

- **SystemAdmin** : システム管理者。組織やグループの管理を担当します。ユーザメニューの SuperAdmin オプションを利用し、組織、アプリケーション、サーバ、脆弱性、ユーザおよびグループを設定できます。また、組織レベルで管理者になりますことができます。
- **Observer** : システムのオブザーバ。組織、ユーザ、アプリケーション、グループおよびトレースの読取り専用権限があります。ユーザメニューの **Observer** オプションで読取り専用アクセスを利用し、組織、アプリケーション、サーバ、脆弱性およびユーザを参照できます。



#### 注記

**No Access** を指定されたユーザは、指定された組織へのシステムレベルのアクセスがブロックされます。

## 複数の組織の管理

マルチテナント環境でデプロイするオンプレミス版のユーザは、同じシステム内で複数の組織をサポートするように Contrast を設定できます。インストールプロセス中に、デフォルトの組織が作成されます。その後、SuperAdmin 権限を持つユーザが追加の組織を作成できます。これを行うには :

1. SuperAdmin として Contrast にログインします。
2. ユーザメニューで **SuperAdmin** を選択して、システム管理の選択肢を表示します。
3. ヘッダで**組織**を選択します。
4. **組織を追加**を選択します。
5. 新しい組織の有効な情報を入力し、組織の管理(Admin)ロールを担うユーザの認証情報を入力して、組織管理者を指定します。
6. ユーザが(上記のステップを通じて、または**組織アクセスグループ (708ページ)**のメンバーになることで)新しい組織へのアクセス権を付与されると、**ユーザメニュー**で組織名を選択することで組織間を移動できるようになります。



#### 重要

組織管理者(Admin)が特定の組織の設定を変更するには、**組織の設定**を選択する前に、まず**ユーザメニュー**でその組織に切り替える必要があります。アクティブな組織は、**ユーザメニュー**の組織名の横に緑色のチェックマークが表示されます。

## 組織の追加/編集

Contrast において、組織とは、ユーザとアプリケーションをビジネス上の共通の目的で関連付けた 1 つのグループです。Contrast はマルチテナントアーキテクチャを採用しており、Contrast のそれぞれのお客様はテナントであり、組織として表現されます。

## 開始する前に

- 組織を作成するためには、[システム管理者 \(821ページ\)](#)のロールが必要です。
- 全ての組織にはユニーク名が必要であり、また組織を管理する[組織管理者 \(819ページ\)](#)が必要です。

## 手順

- 組織を追加するには：
  1. ユーザメニューで **SuperAdmin** を選択します。
  2. ナビゲーションバーで**組織**を選択し、次に**組織を追加**を選択します。
  3. 「組織を追加」の画面で、組織の情報を指定します。

### 組織を追加

組織名

AdminのEメール

Adminの名前

Adminの名字

Adminパスワード

Adminパスワードを確認

メールでの承認が必要

Protect  SCAを有効にする

ライセンス使用状況

割り当てられたライセンスをユーザが手動で適用する必要あり

割り当てられたライセンスを自動で適用

Assess (アプリケーションのライセンス)

Protect (サーバライセンス)

言語

日付形式  時刻形式

タイムゾーン

追加オプション

重複する脆弱性の通知を有効にする

ルートベースの自動検証を有効にする

セキュリティ基準レポートを有効にする

DISA STIGチェックリストのレポート作成を有効にする

ベータ言語のテストを許可する

Harmonyを有効にする

SASTを有効にする

CloudNativeを有効にする

エージェント診断

アプリケーションのライブラリーステータス

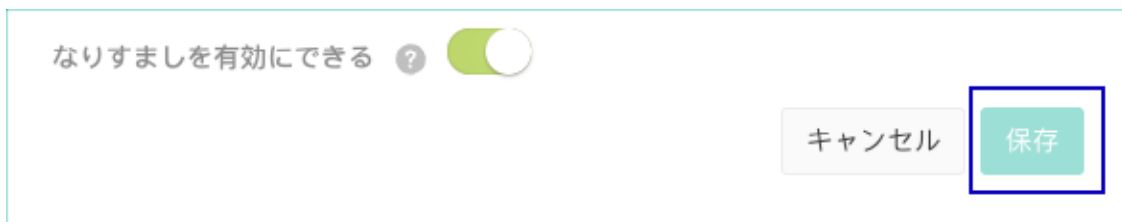
キャンセル

- 新規に作成する**組織名**を入力します。
- 必要に応じて、トグルを使用して **Protect** を有効にします。
- 必要に応じて、**SCA を有効にする**トグルを使用して SCA ライセンスを有効にします。
- **ライセンス使用状況**の下でラジオボタンを使用して、割り当てられたライセンスの適用を手動と自動のどちらで行うかを指定します。
- 組織のデフォルトの**言語**を選択します。

- ドロップダウンを使用して、**日付形式**と**時刻形式**、**タイムゾーン**を選択します。
  - 重複する脆弱性の通知、**ルートベースの自動検証 (674ページ)**、**DISA STIG チェックリストのレポート作成 (613ページ)**、**診断 (802ページ)**など、その他の機能に関する追加オプションを選択します。
  - Eメール、名前、パスワードなど、組織の管理者に関するプロフィール情報を入力します。
  - Contrast アプリケーションにメールサーバを設定している場合のみ、**メールでの承認が必要な**のチェックボックスをオンにします。
4. **追加**を選択すると、組織が作成されます。続けて、マルチテナントのサポートに必要な分だけ組織を作成してください。
- **組織を編集するには**：
    1. **ユーザメニュー**で、**SuperAdmin** を選択します。
    2. 編集する組織の名前を選択します。
    3. 必要に応じて情報を更新し、**保存**をクリックして変更内容を保存します。組織の編集画面でのその他の設定項目には、次のものがあります。
      - **CVSS 3.1** : Contrast は、CVSS 3.1 に対応しています。オンプレミス版(EOP)をご利用の場合は、SuperAdmin ユーザが **CVSS 3.1 を有効にする**をオンにすることで、CVSS 3.1 によるスコア評価を有効にできます。SaaS 版をご利用の場合、この設定を有効にするには **Contrast サポート**までご連絡ください。



- **なりすまし** : SuperAdmin ユーザが、**なりすましを有効にできる**の設定を変更することで、全ての組織に対して**なりすまし (739ページ)**を無効または有効にできます。デフォルトでは、この設定は有効になっています。  
この設定を無効にすると、組織管理者は自分の組織のなりすま시를管理できなくなります。SaaS 版をご利用の場合、この設定を変更するには **Contrast サポート**までご連絡ください。



## システムレベルでのユーザと権限の管理

Contrast を設定してユーザを追加する前に、以下の項目について理解しておいてください。

- **ユーザ** : ユーザは、**1人ずつ (776ページ)**登録することも、**複数ユーザを一括で登録 (777ページ)**することもできます。**ユーザメニュー**の **SuperAdmin** を選択して、ナビゲーションバーで**ユーザ**を選択すると、全てのユーザと各ユーザのステータス(アクティベーション待ち、有効/無効、セキュリティポリシーによりロックアウトなど)が表示されます。
- **認証** : 独自の内部ディレクトリを使用するか、**LDAP や Active Directory などの外部ディレクトリ (785ページ)**を使用するように Contrast を設定できます。
- **グループと権限** : アクセスと権限は、**ロール (817ページ)**によって決まります。ほとんどのロールは、**アクセスグループ (779ページ)**で割り当てます。SuperAdmin ロールと ServerAdmin ロールの**指定方法 (778ページ)**は異なります。**Protect 権限の付与 (780ページ)**はシステムレベルで行えるだけでなく、**新規ユーザ登録 (776ページ)**時や**ユーザの一括登録 (777ページ)**時にも行うことができます。

スーパー管理者(SuperAdmin ロール)およびシステム管理者(SystemAdmin ロール)は、システムレベルまたは組織レベルでユーザを追加できます。

システムグループにユーザを追加すると、システム管理用のインターフェイスにアクセスできるようになり、横断的な組織グループ内の全ての組織で操作ができるようになります。

1つの組織にユーザを追加して、その組織にユーザのアプリケーションへのアクセスと権限を決定するルールを定義することもできます。

## システムレベルでのユーザの追加/編集

システムおよび組織の管理者は、個別にユーザを作成したり、グループ、または [Microsoft Active Directory \(AD\) \(786ページ\)](#) や [LDAP \(790ページ\)](#) などと連携してユーザを作成することができます。

### 開始する前に

- システム管理者(SystemAdmin)または組織管理者(Admin)ルールが必要です。
- 全てのユーザには、デフォルトの組織とその組織内でのデフォルトルールが必要です。  
[SuperAdmin と ServerAdmin ルール \(778ページ\)](#)の指定は異なります。
- 個々のユーザを追加する場合、または複数のユーザを一括で追加する場合、ユーザに Protect 権限を付与することもできます。

### 手順

- スーパー管理者(SuperAdmin)またはシステム管理者(SystemAdmin)としてログインします。
- ユーザメニューで **SuperAdmin** を選択します。
- ナビゲーションバーで、**ユーザ**を選択します。
- ユーザ名**を選択して既存ユーザを編集するか、**ユーザを追加**を選択して新規ユーザを追加します。
- 表示されるフィールドに、ユーザの**名前**、**名字**、**Eメールアドレス**を入力します。
- パスワードを要求する代わりに、メールによるアクティベーションを使用する場合は、**メールでの承認が必要**を選択します。
- ユーザに適用する[システムルール \(821ページ\)](#)を選択します。  
デフォルトのルールは、**None(なし)**です。
- ユーザが所属する**組織**を選択します。
- デフォルトの**組織ルール**を選択します。
- カスタム、またはデフォルトの**アプリケーションアクセスグループ**を選択します。  
Contrast には、以下のデフォルトグループがあります。
  - View** : このグループのメンバーは、Contrast インターフェイスに読み取り専用でアクセスし、スコア、ライブラリ、脆弱性、コメントなどを参照できます。
  - Edit** : このグループのメンバーは、検出結果の修復、タグの追加、脆弱性の管理、属性の編集、アプリケーションのマージ、アプリケーションの追加・削除、サーバの作成などが可能です。
  - Rules Admin** : このグループのメンバーは、アプリケーションのルールとポリシーの編集、Protect の有効化、通知とスコアの管理を行うことができます。
  - Admin** : このグループのメンバーは、組織の設定を構成し、管理することができます。
- 日付形式、時刻形式、タイムゾーンを選択します。
- 組織管理者が組織レベルでユーザ設定を変更できるようにするには、**組織の設定を使用**を選択します。  
このチェックボックスはデフォルトで選択されています。  
システムレベルでユーザ設定を作成するには、このチェックボックスをオフにします。
  - 組織の設定を使用**をオフにします。
  - ユーザを Contrast Web インターフェイスではなく、API のみの利用に制限するには、**API のみのユーザ**を選択します。
  - ユーザに Assess データの参照と使用を許可するには、**アクセス**をオンにします。
  - ユーザに Protect データの参照と使用を許可するには、**Protect** をオンにします。



#### ヒント

組織レベルで [Protect 権限を付与 \(780ページ\)](#)することもできます。



13. 追加または保存を選択します。

## 組織への複数ユーザの追加

CSV ファイルを使用して、複数のユーザを組織に追加することができます。

### 開始する前に

- オンプレミス版をご利用の場合は、SuperAdmin ロールが必要です。
- SaaS 版をご利用の場合は、組織の Admin ロールが必要です。

### 手順

1. ユーザページにアクセスします。
  - a. SaaS 版をご利用の場合、メニューで**組織の設定**を選択したら、**ユーザ**を選択します。
  - b. オンプレミス版をご利用の場合、SuperAdmin メニューより、ナビゲーションバーで**ユーザ**を選択します。
2. 推奨情報を入力したスプレッドシートを作成して、CSV ファイルとして保存します。
  - 各ユーザには必須フィールドを含めます。
  - 全フィールドの見出しと値は、以下の表に示す通りのフォーマットにします。
  - 任意のフィールドについては、新しい列を追加してください。

### ヒント

アップロードアイコンにカーソルを合わせ、ツールチップのリンクを選択すると、CSV テンプレートをダウンロードできます。

The screenshot shows a user management interface with a tooltip. The tooltip text reads: 'CSVでユーザをインポート 以下の情報が必要です: 名前, 名字, Eメール, 組織ロール, 組織ID. 簡単な方法として、こちらのCSVテンプレートをご利用ください。独自のCSVを作成したり追加フィールドを入れる場合は、こちらのドキュメントをご覧ください。' The background shows a '+ユーザを追加' button and a table with columns for 'アクセス' and '09 AM'.

### CSV のフィールド :

フィールド名	必須	値
First Name	必須	ユーザの名前
Last Name	必須	ユーザの名字
Email または Username	必須	Contrast 内部ディレクトリ(デフォルト)を使用している場合は、ユーザの E メールを入力します。 外部ディレクトリ使用している場合は、CSV で Email を Username に変更して、外部ディレクトリと完全に一致するユーザ名を入力します。
Organization UUID	オンプレミス版をご利用の場合は必須	この値は、組織の設定の <b>一般情報 (706ページ)</b> から取得します。
Organization Role	必須	値は、View、Edit、Rules_admin または Admin になります。

フィールド名	必須	値
Date Format	任意	デフォルトの値は、組織の設定の日付形式で、MM/dd/YYYY になります。
Time Format	任意	デフォルトの値は、組織の設定の時刻形式で、hh:mm a になります。
Timezone	任意	デフォルトの値は、組織のタイムゾーンです。
Protect	任意	デフォルトの値は、Off(無効)です。
Groups	任意	値は、View、Edit、Rules Admin、Admin またはカスタムグループ名です。複数のグループ名は、GroupA&&GroupB&&GroupC の形式にします。
Language	任意	デフォルトは、組織で設定 (706ページ) した値です。
System Administration	任意	デフォルトの値は、Off(無効)です。
Email Activation	任意	値が None(なし)の場合、デフォルトは Required Password(パスワードが必要)になります。
Password	任意	Email Activation フィールドに false を指定した場合、このフィールドは必須です。
Api Only	任意	デフォルトの値は、Off(無効)です。
Access	任意	デフォルトの値は、On(有効)です。

3. ユーザを追加の横にある黒いアップロードアイコンを選択し、作成した CSV を選択します。スプレッドシートのアップロード処理が開始したら、そのページを離れて Contrast の他の処理を続けることができます。アップロードが成功すると、アップロードされたユーザ数を含む確認メッセージが表示されます。アップロードが失敗すると、スプレッドシートのエラーの原因を示すエラーメッセージが表示されます。

## SuperAdmin または ServerAdmin の指定

SuperAdmin には、最高レベルのシステム管理権限があります。

ServerAdmin には、ユーザとグループにアクセスできないことを除いて、SuperAdmin と同じ権限と機能があります。

少なくとも 1 人のユーザを SuperAdmin として指定する必要があります。複数のユーザを SuperAdmin に指定する場合は、ログインを共有しないでください。代わりに以下を実行してください。

1. SuperAdmin としてログインします。
2. ユーザメニュー > SuperAdmin > ユーザを選択します。
3. SuperAdmin に指定するユーザを検索します(名前、Eメール、組織で検索するか、一覧で名前を探してください)。
4. ユーザ名を選択すると、ユーザを編集の画面が開きます。
5. システム管理フィールドで、SuperAdmin または ServerAdmin を選択します。
6. 保存を選択します。



### ヒント

SuperAdmin または ServerAdmin に指定された全てのユーザは、右上にあるユーザメニューで SuperAdmin を利用できます。また、SuperAdmin > ユーザの一覧で、ユーザ名の横に小さい鍵のアイコンが表示されます。鍵にカーソルを合わせると、割り当てられているロールを確認できます。

## システムアクセスグループの追加/編集/削除



### 注記

システムアクセスグループは、オンプレミス版のお客様のみが利用できます。システムアクセスグループを追加するには、SuperAdmin である必要があります。

システムアクセスグループを追加するには：

1. ユーザメニュー > **SuperAdmin** > **グループ** を選択します。
2. 既存のグループを選択して編集するか、**グループを追加** を選択して新しいグループを作成します。



### ヒント

グループを検索するには、クイックフィルターのドロップダウンまたは左上の検索フィールドを使用します。または、各列の上部にある上下方向の矢印を使用して並び替えを行います。

3. 画面で以下の項目に入力します。
  - **グループ名**：このグループに割り当てる権限、機能、目的を反映したものを選んでください。
  - **種類**： **System**(システム)を選択します。



### ヒント

**組織レベルでアクセスグループを追加する (708ページ)** こともできます。ただし、システムレベルでアクセスグループを追加すると、組織間を横断できるグループを作成することができます。

横断的な組織グループは、それぞれが独自の組織を持つ複数の事業部門をサポートするセキュリティチームなどには便利です。

横断的な組織グループのメンバーは、ユーザメニューで名前を選択することで組織を切り替えることができます。

- **システムアクセス**：このグループでアクセスできる組織を選択します。
  - **ロール**：このグループのメンバーが該当の組織内で持つべき **システムロール (821ページ)** を選択します。
  - さらに組織とロールを追加するには、**システムアクセスを追加** を選択します。
4. **メンバー** では、フィールドに文字を打鍵するとユーザが表示されるので、グループに割り当てる 1 人以上のユーザを選択します。メンバーを削除するには、**X** を選択します。



### 注記

ユーザは、複数のグループに所属することができます。特定の組織にアクセスするために、その組織内で作成される必要はありません。

5. 完了したら、**追加** を選択して新しいグループを作成するか、既存のグループを編集している場合は **保存** を選択します。このグループに追加したメンバーに、それぞれのロールに対応する権限が付与されます。



### 重要

ユーザが、全てのアプリケーションや組織のロールに対して競合する 2 つのグループに割り当てられた場合は、アクセスの制限が最も厳しいロールが適用されます。

[ユーザに表示される \(480ページ\)](#) のは、組織レベルとアプリケーションレベルのグループのみであることに注意してください。アクセスレベルが不明な場合は、システムレベルでより厳しい権限が適用されている可能性があります。

ただし、特定のアプリケーションに割り当てられたロールに関しては、全てのアプリケーションに割り当てられたロールより制限が緩くても、特定のアプリケーションに割り当てられたロールが、全てのアプリケーションに割り当てられたロールよりも優先されます。

ユーザが 2 つのカスタムグループに割り当てられ、同じアプリケーションに対してロールが割り当てられている場合は、権限が最も少ないロールが適用されます。

[システム \(821ページ\)](#)、[組織 \(819ページ\)](#)、[アプリケーション \(817ページ\)](#) の各ロールは、制限の緩いものから厳しいものの順に表示されます。

以下はロールの権限が競合する例ですが、グループ 2 の権限が優先されます。

グループ 1	グループ 2(優先されます)
全てのアプリケーションに対して <b>アプリケーションの Edit</b> ロール	全てのアプリケーションに対して <b>アプリケーションの View</b> ロール
全てのアプリケーションに対して <b>組織の View</b> ロール	Red アプリケーションに対して <b>アプリケーションの Admin</b> ロール
Red アプリケーションに対して <b>Rules Admin</b> ロール	Red アプリケーションに対して <b>No Access</b>



### ヒント

グループを削除するには、**ユーザメニュー > SuperAdmin > グループ** を選択します。削除したいグループを探し、その行の削除アイコンを選択します。

この操作を確定すると、グループが削除され、そのグループによって提供されたアクセス権が、そのグループに割り当てられた全てのユーザから取り消されます。

## Protect 権限の付与(オンプレミス版)

オンプレミス版をご利用のお客様は、1 つまたは複数の組織で、全てのユーザロールや一部のユーザロールに Protect データへのアクセス権限を与えることができます。

### 開始する前に

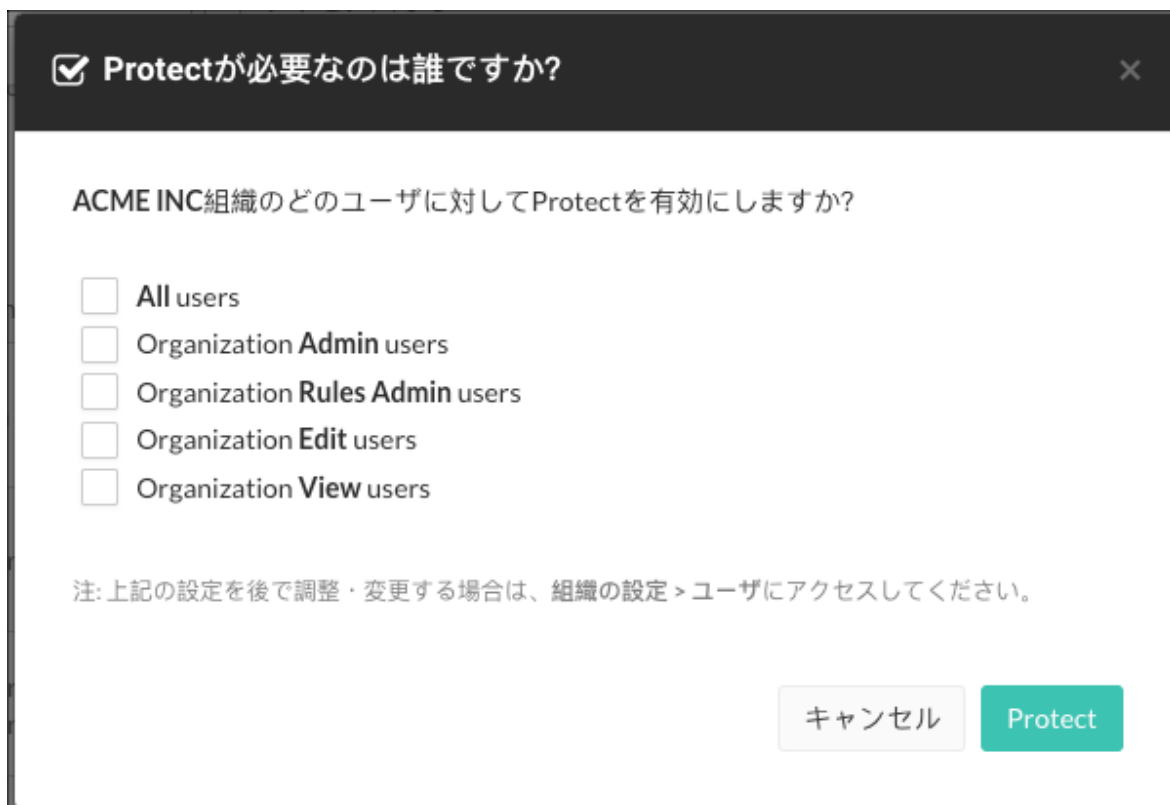
- SuperAdmin ロールが必要です。
- Protect データへのアクセスが必要となるユーザが所属するのは、どの組織であるかを確認してください。
- 組織内で Protect データへのアクセスが必要なのは、どのユーザロールであるか確認してください。

## 手順

1. SuperAdmin としてログインします。
2. ユーザメニューで **SuperAdmin** を選択します。
3. Contrast Web インターフェイスのナビゲーションバーで**組織**を選択します。
4. Protect を有効にする組織を検索します。該当する組織の行の右端にある Protect 列で、トグルボタンをオン(緑)にします。



5. 「Protect が必要なのは誰ですか？」の画面で、Protect データの参照とアクセス権限が必要なロールを選択します。



**All users**(全てのユーザ)または特定のユーザロールを選択します。

[個々のユーザ \(776ページ\)](#)に対して Protect のアクセスを有効または無効にすることもできます。

6. **Protect** を選択します。  
この変更を行うと、選択したロールのあるユーザが Protect データにアクセスできるようになります。

## SSO を使用してユーザをグループに自動追加

シングルサインオン(SSO)を使用してユーザをグループに自動的に追加できます。

1. IDP の SAML 設定を以下のように更新します。

```
<saml2:AttributeStatement \
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
```

```
<saml2:Attribute Name="contrast_groups" \
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
  <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
xsi:type="xs:string"
>GROUP1</saml2:AttributeValue>
  <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
xsi:type="xs:string"
>GROUP2</saml2:AttributeValue>
  ...
</saml2:Attribute>
</saml2:AttributeStatement>
```



### 重要

contrast\_groups に列挙する属性値は、既存のグループ名と完全に一致する必要があります。Contrast では、この属性に列挙された値に基づいて新しいグループは作成されません。

- 次に Contrast Web インターフェイスの [組織の設定 \(704ページ\)](#) で、**シングルサインオン** を選択し、画面の下部にあるチェックボックスを使用して、以下のいずれかまたは両方を有効にします。
  - **SSO ログイン時にユーザを Contrast グループに追加** : ログイン時に、Contrast は SAML アサーションの contrast\_groups 属性に列挙されているグループにユーザを追加します。
  - **SSO ログイン時にユーザを Contrast グループから削除** : ログイン時に、Contrast は SAML アサーションの contrast\_groups 属性に列挙されていないグループからユーザを削除します。

### 参考

- NameID としてのユーザの E メール

```
<md:NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</
md:NameIDFormat>
```

- 名前と名字

```
<saml2:Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/
claims/givenname"
\
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
>
  <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/
XMLSchema"
xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
xsi:type="xs:string"
>Dan</saml2:AttributeValue>
</saml2:Attribute>

<saml2:Attribute Name=" http://schemas.xmlsoap.org/ws/2005/05/identity/
claims/surname"
\
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
>
```

```
<saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/
XMLSchema"
xmlns:xsi="http://www.w3.org/2001/
XMLSchema-instance"
xsi:type="xs:string"
>Dan</saml2:AttributeValue>
</saml2:Attribute>
```

• ユーザグループ管理

```
<saml2:AttributeStatement \
xmlns:saml2="urn:oasis:names:tc:SAML:2.0:assertion">
<saml2:Attribute Name="contrast_groups" \
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
<saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/
XMLSchema"xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xsi:type="xs:string">GROUP1</saml2:AttributeValue>
<saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/
XMLSchema"xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"xsi:type="xs:string">GROUP2</saml2:AttributeValue>
...
</saml2:Attribute></saml2:AttributeStatement>
```

関連項目

[Okta](#) を使用してユーザとグループのプロビジョニングを設定する

[グループにユーザを自動的に追加するように ADFS を構成する](#)

デフォルト認証情報と SuperAdmin 認証情報の管理

Contrast をインストールするシステム管理者には、管理すべき認証情報が 3 セットあります。

- **Contrast Hub の認証情報**：新規のお客様は、ユーザ名とパスワードを設定するためのリンクが記載された電子メールが届きます。 [インストーラのダウンロード \(746ページ\)](#)と [Contrast Hub](#) へのログインには、この認証情報が必要です。
  - **ユーザ名**：Contrast から、*example@domain.com* の形式でユーザ名が提供されます。これは、デフォルトの組織管理者(Admin)と同じユーザ名です。
  - **パスワード**：アクティベーションメールのリンクを選択した際に、このパスワードを作成します。
- **デフォルトのスーパー管理者(SuperAdmin)の認証情報**：SuperAdmin の認証情報は、ライセンスに含まれています。 [SuperAdmin ロール \(821ページ\)](#)で Contrast アプリケーションを管理するために使用します。
  - **ユーザ名**：Contrast から、*contrast\_superadmin@domain.com* の形式でユーザ名が提供されます。*domain* の部分は、お客様の会社のメールアドレスのドメイン名になります。
  - **パスワード**：デフォルトのパスワードは default1! です。
- **デフォルトの組織管理者(Admin)の認証情報**：組織管理者は、この認証情報を使って、 [インストール \(746ページ\)](#)後に Contrast にログインして、組織の設定や管理を行います。
  - **ユーザ名**：Contrast から、*example@domain.com* の形式でユーザ名が提供されます。これが、デフォルトの組織管理者のユーザ名です。
  - **パスワード**：デフォルトのパスワードは、default1! です。



### 重要

ログインに成功したら、提供されたデフォルトのパスワードをすぐに変更してください。SuperAdmin のパスワードをリセットするには、[Contrast UI を使用 \(477ページ\)](#)するか、[Windows \(800ページ\)](#)または [Linux \(799ページ\)](#)のコマンドラインを使用してください。

## ユーザのなりすまし

ユーザになりすます機能を利用すると、なりすましたユーザと同じロールと権限を持っているかのように、組織にアクセスできます。なりすましは、問題のトラブルシューティングを行う場合に便利です。

SuperAdmin ロールがある場合、組織のページより該当の組織の行で**なりすます**を選択すると、その組織の最初の組織管理者に対してなりすますことができます。また、ユーザのページにて**なりすます**を選択して、任意のユーザになりすますことができます。

ServerAdmin または SystemAdmin ロールがある場合、組織のページより該当の組織の行で**なりすます**を選択すると、その組織の最初の組織管理者に対してなりすますことができます。なりすましを利用するには、対象の組織へのアクセス権が必要です。

Contrast では、24 時間後に自動的になりすましが無効になります。

## 開始する前に

- なりすます対象のユーザに**組織のロール (819ページ)**が必要です。
- なりすましのオプションが組織に表示されていない場合は、SuperAdmin ユーザがその組織の**なりすましを有効にできる (774ページ)**の設定をオンにする必要があります。
- 組織管理者は、アクセスしたい組織の**なりすましを有効にする (739ページ)**必要があります。

## 手順

- ユーザレベルでなりすましを開始するには：
  1. Contrast Web インターフェイスに SuperAdmin としてログインします。
  2. **ユーザ**を選択します。
  3. なりすましをしたいユーザの行の最後にある三角形(▼)を選択し、**なりすます**を選択します。
  4. 「ご確認ください」の画面で、**なりすます**をクリックして、選択したユーザへのなりすましを確定します。



本当にこのユーザとしてログインしても良いですか?



なりすましたユーザとして、Contrast のセッションが開始します。

- 組織レベルでなりすましを開始するには：
  1. SuperAdmin、ServerAdmin、または SystemAdmin として Contrast Web インターフェイスにログインします。



2. **組織**を選択します(まだ選択していない場合)。
3. アクセスしたい組織の行の最後にある三角形(▼)をクリックして、**なりすます**を選択します。
4. 「ご確認ください」の画面で、**はい**を選択して、表示されたユーザになりすますことを確定するか、アクセスしたい組織の管理者である別のユーザを選択します。



## 認証の設定



### 注記

SaaS 版をご利用の場合は、Contrast Security が認証を設定します。ただし、SSO の設定を含め、この設定を上書きする権限を組織管理者に付与できる場合があります。

この変更を希望する場合は、[Contrast サポート](#)にご連絡ください。

デフォルトでは、ユーザのログイン名、認証情報、およびアプリケーションの認証に関するその他の詳細情報を含むユーザ情報がユーザディレクトリに格納されます。ユーザ名とパスワードは Contrast データベースの内部ディレクトリに(一方向ハッシュを使用して)格納されます。Contrast ユーザに[パスワードポリシー \(798ページ\)](#)および[2 段階認証 \(786ページ\)](#)を設定できます。

また、認証に外部ディレクトリを使用することもできます。この場合、ユーザ名のみが Contrast のデータベースに格納されます。Contrast では、以下をサポートします。

- [LDAP \(790ページ\)](#)
- [Active Directory \(786ページ\)](#)
- [シングルサインオン \(795ページ\)](#)
- [信頼される HTTPS プロキシ \(798ページ\)](#)

認証の設定を変更した場合は、[Contrast を再起動 \(757ページ\)](#)する必要があります。認証の設定を変更するには、[システムの設定 \(800ページ\)](#)で**認証**を選択します。



### 重要

認証モードを切り替える時は、以下の点に注意してください。

- 変更前の認証モードで作成されたユーザは、ユーザの E メールアドレスが新旧の認証プロバイダ間で同じでない限り、機能しなくなります。
- 新しい認証モードを設定してサーバを再起動すると、ユーザは自分のアカウントが新しい組織または既存の組織に追加されるまで、Contrast にログインできなくなります。オンプレミス版をご利用の場合は、スーパー管理者(SuperAdmin)が組織管理者(Admin)のアカウントを管理し、その後各組織管理者がその組織内のユーザを管理します。



### 注記

外部の認証プロバイダ(LDAP または AD)を使用するモードの場合、ユーザを追加する際にユーザ名フィールドはライブ検索として機能し、適切なグループ内のユーザが表示されます。



### ヒント

ロールと権限はユーザディレクトリではなくアクセスグループによって管理されるため、認証を設定する前にアクセスグループを作成することをお勧めします。管理者用とユーザ用に、少なくとも 2 つの一意のアクセスグループが必要になります。

## システムレベルでの 2 段階認証の有効化

2 段階認証を有効/無効にするには：

1. [システムの設定 \(800ページ\)](#)の左ナビゲーションで**セキュリティ**を選択します。
2. トグルボタンをオン(緑色)にして 2 段階認証を有効にします。
3. [組織の上書きを許可](#)の横にあるチェックボックスをオンにして、組織管理者が**ユーザにとってこの機能を必須にするかどうかを選択 (712ページ)**できるようにします。



### 注記

ユーザが複数の組織に属している場合は、デフォルトの組織によって 2 段階認証の設定が決まります。

また、ユーザは [2 段階認証の通知を受け取る方法を選択 \(478ページ\)](#) することができます。

## Microsoft Active Directory の設定

[システムの管理者 \(821ページ\)](#)は、Microsoft Active Directory(AD)に接続するように Contrast を設定できます。このインテグレーションを設定するには、AD Connector を使用します。AD はディレクトリの構造が明確に定義されているため、設定する選択肢も少なくなり、より直接的な設定ができます。



## 注記

ローカルデータベースなど、別の認証方法から AD に切り替えると、ユーザ ID 属性に一貫性がない場合は問題が発生する可能性があります。

## AD がオフラインの場合のアクセス

AD サービスで接続や設定の問題が発生した場合、デフォルトの SuperAdmin アカウントを使用して Contrast にログインしてください。これにより、AD がオフラインの場合でも、引き続き Contrast アカウントに直接アクセスできます。

## 手順

1. はじめに、Active Directory サーバに読み取り専用ユーザを作成します。ユーザには、検索ベース (Search Base) のみの権限を持つユーザを含め、ディレクトリに対する読み取り権限を持つ必要があります。このユーザは、[AD のユーザを設定 \(789ページ\)](#) する際やユーザにバインドする際に、検索ベースを設定するために必要となります。
2. 外部の AD サーバで、ユーザグループを作成します。このグループは、後で Contrast の [SuperAdmin 権限を割り当てる \(788ページ\)](#) ために使用します。
3. [システムの設定 \(800ページ\)](#) で **認証** を選択します。
4. **認証方法を変更** を選択したら手順に従って、サーバ、グループ、詳細を設定します。
5. **Active Directory** を選択します。
6. 以下の値を入力します。LDAPS(LDAP over SSL)では、一部の設定が異なる場合があります。

The screenshot shows the 'システムの設定' (System Settings) page in the Contrast web interface. The '認証' (Authentication) section is selected in the left sidebar. A modal window titled '認証の設定' (Authentication Settings) is open, showing the 'ステップ2サーバを設定' (Step 2: Configure Server) configuration. The '接続先サーバ' (Target Server) section includes fields for 'プロトコル' (Protocol) set to 'LDAP - 安全でない経路 (最も一般的)' (LDAP - Insecure path (most common)), 'ホスト名' (Host name) set to 'ad.contecsec.com', 'ポート' (Port) set to '389', and '検索ベース' (Search base) set to 'dc=contrastsecurity,dc=com'. The 'サーバにバインド' (Bind to server) section includes fields for 'ユーザ名' (Username) set to 'cn=Directory Manager' and 'パスワード' (Password) masked with dots. Navigation buttons '前へ' (Previous), '接続を試す' (Test connection), and '次へ' (Next) are at the bottom right.

接続先サーバで、以下の項目に入力します。

- **プロトコル** : LDAP サーバとの通信に使用するプロトコルです。ドロップダウンから、**LDAP** か **LDAPS** を選択します。デフォルトは、**LDAP** です。[AD で自己署名証明書またはプライベート証明書を使用 \(790ページ\)](#) している場合は、**LDAPS** オプションで追加の設定が必要になる場合があります。
- **ホスト名** : LDAP サーバと通信する際に接続するホスト名です。AD サーバの DNS ホスト名または IP アドレスを入力します。マルチテナントフォレストでは、これはグローバルカタログサーバになります。デフォルトは、**localhost** です。
- **ポート** : LDAP サーバと通信する際に接続するポートです。標準(シングルテナント、シングルドメイン)ディレクトリの場合、**389 (LDAP)**番か **636 (LDAPS)**番のポートを指定してください。マルチテナントまたはマルチドメインフォレストでは、**3268 (LDAP)**番か **3269 (LDAPS)**番を指定してください。

- **検索ベース**：LDAP サーバとの通信に使用するベース DN(AD 環境でグローバルベースレベルのコンテナを表す識別名)です。通常、これはドメイン名またはサブドメイン名です。デフォルトは、`dc=contrastsecurity,dc=com` です。ログインドメインが `yourdomain.com` であれば、ベース DN は `dc=yourdomain,dc=com` となります。
- サーバにバインドで、以下の項目に入力します。
- **ユーザ名**：検索機能を実行するために、ディレクトリにバインドするユーザの完全な DN 名を入力します。デフォルトは、`cn=Directory Manager` です。
  - **パスワード**：アプリケーションが LDAP サーバに接続する際に使用するユーザアカウントのパスワードです。
7. **接続をテスト**を選択して、サーバへの接続を確認します。接続を確認したら、**次へ**を選択します。
  8. **グループを設定**します。(788ページ)
  9. **詳細設定を指定**します。(789ページ)
  10. 全ての設定オプションを指定したら、**ログインをテスト**ボタンを使用して、スーパー管理者(SuperAdmin)と組織管理者(Admin)の両方でログインできることを確認します。



### 注記

テストに時間がかかり過ぎると思われる場合は、**詳細設定 (789ページ)の Referral(照会)機能をフォローオプションの設定が間違っている可能性**があります。設定を切り替えると、ログイン機能の検証が早くなるはずですが。

11. **完了**を選択して、設定を完了します。

## Active Directory のグループの設定

**Active Directory の設定 (786ページ)**一環として、グループを設定する必要があります。

Contrast では、連携している AD サーバを使用してのデータアクセス制御は行われません。つまり、ロールやアプリケーション内のデータへのアクセスはアプリケーションによって行われ、組織管理者(Admin)がユーザロールを設定します。ただし、ログイン時や新規ユーザ作成時に、指定されたユーザが Active Directory(AD)内の正しいグループに属しているかどうか、アクセス制御のチェックが行われません。

### 手順

ステップ 3 グループを設定 ?

#### Contrast ユーザグループ

`cn=ContrastUsers,cn=Users,dc=contrastsecurity,dc=co`

グループのクエリ

#### Contrast SuperAdminグループ

`cn=ContrastAdmins,cn=Users,dc=contrastsecurity,dc=`

1. 外部 AD サーバで作成したグループを使用して、ユーザを以下のいずれかの Contrast グループに割り当てます。
  - **SuperAdmin グループ**：このグループを使用すると、ユーザはスーパー管理者用のインターフェイスにログインできます。このグループのユーザは、Contrast に初めてログインした時に認証され、権限が付与されます。
  - **ユーザグループ**：このグループを使用すると、ユーザは組織に追加され、Contrast Web インターフェイスにログインできます。このグループは、他の全てのユーザに適しています。

ユーザがログインできるようにするために、Contrast Web インターフェイスで組織に手動でユーザを追加 (708ページ) してください。



### 注記

AD インスタンスで両方のグループにユーザを追加した場合、そのユーザは Contrast で設定時に自動的に SuperAdmin グループに追加されます。

2. グループのクエリを選択すると、入力フィールドに入力する際に既存のグループをライブ検索できません。



### 注記

アクセス制御のチェックを通さずに Contrast で AD 認証を持つユーザを作成するには、データベースで以下のクエリを実行します。

```
UPDATE teamserver_preferences SET property_value='true' \
WHERE \
property_name='directory.skip.user_existence.validation'
```

## Active Directory の設定

Active Directory の設定 (786ページ) では、詳細設定で以下の項目を入力してください：

- **ユーザ・ベース DN**：デフォルトは `cn=Users` で、AD のデフォルトコンテナです。ただし、AD が異なる方法で設定されている場合は、これはユーザがディレクトリに格納されている最上位のコンテナへのパスになります。  
例えば、ユーザが DN `CN=Engineering,CN=GlobalUsers,DC=intranet,dc=example,dc=com` に格納されており、ベース DN が `DC=intranet,DC=example,DC=com` である場合、ユーザ DN のサフィックスの値は、`CN=Engineering,DC=GlobalUsers` になります。
- **ユーザ ID の属性**：ユーザが Contrast アプリケーションにログインする際に、ユーザ名として入力する属性を入力します。ユーザが最も使い慣れた属性を指定します。デフォルトは、**Eメールアドレス** です。
- **ログイン ID**：AD の `sAMAccountName` 属性です。これは通常、Windows にログインする際に使用するユーザ名です。

- **E メールアドレス** : AD の mail 属性で、ユーザの E メールアドレスが含まれます。
- **ユーザプリンシパル** : AD の userPrincipal 属性、完全なユーザ名が含まれます。
- **ネストしたグループ内を検索** : ネストしたグループ内の検索を有効または無効にします。このトグルはデフォルトで無効になっています。
- **Referral(照会)機能をフォロー** : マルチテナントまたはマルチドメインのエンタープライズフォレストでは、より詳細な情報を得るために LDAP クエリをほかのサーバに照会する場合があります。このトグルはデフォルトで無効になっています。
- **Referral(照会)の範囲** : AD が Referral() の応答を返したときにフォローする Referral(照会)の回数を制限します。デフォルトは「5回」です。

## Active Directory での自己署名/プライベート証明書の使用

SSL を使用してサーバに接続するよう [AD インテグレーションを設定 \(786ページ\)](#) している場合は、サーバの証明書を Contrast JRE が使用する新しい信頼ストアにインポートしなければならない場合があります。

1. 管理者から、サーバの証明書を PKCS#12 フォーマットで取得します。自己署名証明書を使用している場合、これは実際の AD サーバの証明書になります。プライベート認証局がある場合は、そのサーバの CA 証明書が必要になります。
2. このサーバの証明書を入手したら、この証明書を含む信頼ストアを作成します。Contrast がインストールされているディレクトリのコマンドシェルから、管理者として以下のコマンドを実行します。

```
$ mkdir data/conf/ssl
$ jre/bin/keytool -import -file <path to certificate> -alias <hostname> \
-keystore data/conf/ssl/truststore.jks
```

3. サーバまたは CA の証明書を含む信頼ストアを作成したら、`bin/contrast-server.vmoptions` ファイルに以下のコマンド行を追加します。

```
-Djavax.net.ssl.trustStore=<full path to truststore>
-Djavax.net.ssl.trustStorePassword=<password you set for the \
trustStore, if any>
```

4. Contrast Server サービスを再起動して、AD に対するクエリで SSL が使用されていることを確認します。

## LDAP の設定

Contrast は、さまざまな種類の LDAP (Lightweight Directory Access Protocol)サーバと連携します。LDAP は、Web アプリケーションが LDAP ディレクトリサーバに登録されているユーザーやグループを検索するために使用できるインターネットプロトコルです。

Contrast は、以下の種類の LDAP サーバをサポートしています。

- OpenLDAP
- OpenDS
- ApacheDS
- Fedora Directory Server
- Microsoft Active Directory
- 汎用 LDAP サーバ

社内ディレクトリでユーザやグループを管理していて、アプリケーションのユーザアクセスの管理を社内ディレクトリ管理者に委任する場合、LDAP ディレクトリサーバに接続すると便利です。



### 注記

ローカルデータベースなど、別の認証方法から LDAP に切り替えると、ユーザ ID 属性に一貫性がない場合は問題が発生する可能性があります。

システム管理者は、以下の手順で LDAP サーバを設定できます。



**重要**

SSL を使用してサーバに接続するように LDAP 連携を設定する場合は、**自己署名証明書またはプライベート証明書 (795ページ)**の追加手順が必要になることがあります。

## LDAP がオフラインの場合のアクセス

LDAP サービスで接続や設定の問題が発生した場合、デフォルトの SuperAdmin アカウントを使用して Contrast にログインしてください。これにより、LDAP がオフラインの場合でも、引き続き Contrast アカウントに直接アクセスできます。

### 手順

1. はじめに、LDAP サーバに専用のユーザを作成します。Contrast が LDAP ディレクトリと連携する設定方法によりますが、読み取り専用ユーザまたは読み書き可能なユーザを作成してください。ユーザは、検索ベース(Search Base)のみの権限を持つユーザを含め、ディレクトリに対する読み取り権限を持つ必要があります。このユーザは、**LDAP にユーザを設定する (794ページ)**際やユーザにバインドする際に、検索ベースを設定するために必要になります。
2. 外部の LDAP サーバで、ユーザグループを作成します。これらのグループは、後で Contrast の **SuperAdmin 権限を割り当てる (792ページ)**ために使用します。
3. **システムの設定 (800ページ)**で、**認証**を選択します。
4. **認証方法を変更**を選択します。
5. **LDAP** を選択します。
6. **接続先サーバとサーバにバインドに必要な情報**を入力します。

オプション	説明	デフォルト
接続先サーバ		

オプション	説明	デフォルト
プロトコル	LDAP サーバとの通信に使用するプロトコルです。LDAP または LDAPS(LDAP with SSL)を選択します。	LDAP
ホスト名	LDAP サーバと通信する際に使用するホスト名です。	localhost
ポート	LDAP サーバと通信する際に使用するポートです。	389 (LDAP)、636 (LDAPS)
検索ベース	LDAP サーバと通信する際に使用するベース識別名(DN)です。ログインドメインが、 <i>yourdomain.com</i> であれば、ベース DN は <code>dc=yourdomain,dc=com</code> となります。	<code>dc=contrastsecurity,dc=com</code>
<b>サーバにバインド</b>		
方式	LDAP サーバと通信する際に使用する方法を選択します。オプションについては、次の表に示します。	Simple(シンプル)
ユーザ名	クエリの実行や認証確認のためにディレクトリにバインドするユーザの完全な DN です。	N/A
パスワード	ユーザ名フィールドで指定したバインドユーザのパスワードです。	N/A

Contrast で使用できるバインドメカニズムは 4 つあります。それぞれ必須項目が異なります。

方式	説明	必須項目	オプション項目
匿名(Anonymous)	管理者は、ディレクトリへの匿名の読み取り専用アクセスを提供します。	なし	N/A
シンプル (Simple)	ユーザ名とパスワードによる標準的な認証です。ユーザ名とパスワードは、LDAP サーバから提供される情報で認証されます。	ユーザ名、パスワード	N/A
DIGEST-MD5	認証されるサーバに送信する前に、MD5 を使用してユーザ名とパスワードが提供・ハッシュされます。	ユーザ名、パスワード	SASL レルム
CRAM-MD5	LDAP サーバが事前認証チャレンジを発行し、認証されるべきユーザ名とパスワードを MD5 でハッシュ化して送信します。	ユーザ名、パスワード	SASL レルム

- LDAP サーバへの接続を設定したら、**接続をテスト**を選択します。接続テストでは、アプリケーションが LDAP サーバに接続してクエリを実行できるかどうかを確認します。
- [LDAP のグループを設定します \(792ページ\)](#)。
- [LDAP のユーザを設定します。\(794ページ\)](#)
- グループとユーザのマッピングが適切に設定されていることを確認するには、**ログインをテスト**を選択します。
- スーパー管理者(SuperAdmin)と組織管理者(Admin)の両方が正常にログインできることを確認したら、**完了**を選択して設定を完了します。

## LDAP のグループの設定

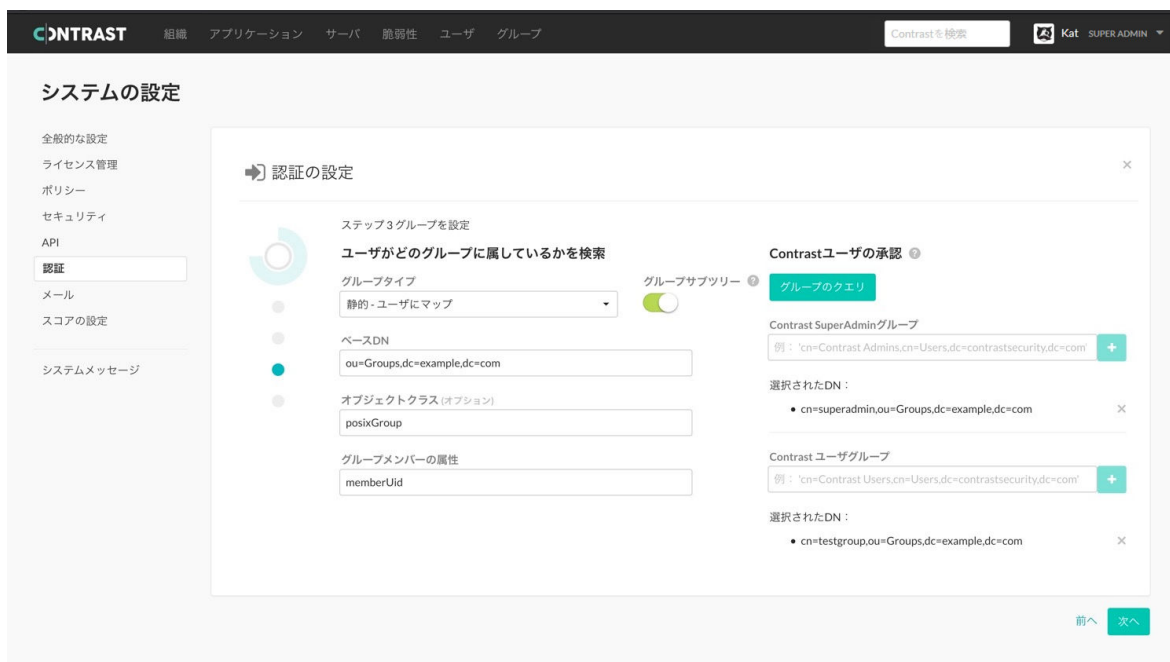
[LDAP の設定 \(790ページ\)](#)の一環として、グループを設定する必要があります。

組織管理者がユーザの[ロールと権限 \(817ページ\)](#)を設定したら、それぞれのアプリケーションがデータに対するロールとアクセスをそのアプリケーション内で処理します。ユーザを設定するときは、[ログイン時にユーザをアクセスグループに追加 \(794ページ\)](#)するよう選択することができます。ただし、この機能が有効になっていない場合でも、Contrast は LDAP ディレクトリを使用して、そのユーザが適切なグループに割り当てられるようにします。

グループを設定するには：

- 以下の値を入力します。





オプション	説明	デフォルト
グループタイプ	グループタイプは、サーバの機能と設定によって異なります。グループは以下のいずれかになります。 <ul style="list-style-type: none"> <li>静的: uniqueMember などのオブジェクトの属性を通じて、グループがメンバーを追跡します。この表の残り 4 つのオプションは、静的グループにのみ適用されます。</li> <li>動的: ユーザオブジェクトが自身のメンバーシップを追跡します。ユーザがグループのメンバーになると、ユーザオブジェクトに対してグループが動的に追加されます。</li> </ul>	静的
グループサブツリー	ディレクトリ内でグループを検索するときに、ベース DN のサブツリーを含めるかどうかを設定します。	有効
ベース DN	これは、(ユーザベース DN と同様に)アプリケーションが LDAP サーバ内のグループを見つけるための識別名(DN)です。	ou=Groups
オブジェクトクラス	空欄のままにすると、アプリケーションでは「group」、「groupOfUsers」、「groupOfUniqueUsers」のデフォルト値が使用されます。これは LDAP 環境において標準的であるため、必須のフィールドではありません。	N/A
グループメンバーの属性	ディレクトリのグループオブジェクト内の属性であり、そのグループのメンバーを含めます。これは LDAP 環境によって異なる場合があるため、LDAP 管理者に確認して適切な属性を使用していることを確認してください。  グループの各メンバーは、相対識別名(RDN)ではなく、完全識別名(DN)として、列挙する必要があります(例: "cn=smith,ou=Users,cn=support,dc=test,dc=org")。  RDN を使用すると、Contrast では LDAP グループでそのユーザが認識されません。	uniqueMember

- 外部 LDAP サーバで事前に作成したグループを使用して、ユーザを以下のいずれかのグループに割り当てます。
  - SuperAdmin グループ**: このグループでは、ユーザは SuperAdmin 権限でログインできます。
  - ユーザグループ**: このグループを使用すると、ユーザは組織に追加され、標準インターフェイスにログインできます。このグループは、他の全てのユーザに適しています。

**重要**

ユーザが両方のグループに属していて、プロビジョニングが無効な場合、このユーザは SuperAdmin として作成されます。プロビジョニングが有効な場合は、ユーザは SuperAdmin 権限なしで作成されます。

- グループのクエリを選択すると、入力フィールドに入力する際に既存のグループをライブ検索できます。

## LDAP のユーザの設定

LDAP の設定 (790ページ)の一環として、ユーザを設定する必要があります。

LDAP ディレクトリと完全に統合するため、Contrast では LDAP サーバへの接続方法、およびディレクトリ内のユーザとグループの検索方法に関する情報が必要になります。

1. Contrast でディレクトリ内のユーザを検索する方法について、以下の情報を入力します。ほとんどの LDAP 環境ではデフォルト設定が適切です。

オプション	説明	デフォルト
ベース DN	Contrast がユーザの検索を開始する、(グローバルベース DN の下にある)コンテナを示します。多くの組織では、これは単一のコンテナ(例: <code>ou=Users</code> )ですが、適切なコンテナを検索していることを LDAP 管理者が確認する必要があります。	<code>ou=users</code>
オブジェクトクラス	ディレクトリ内のユーザオブジェクトの LDAP オブジェクトクラスを示します。	<code>inetOrgPerson</code>
名前の属性	ユーザの名前を含む LDAP フィールドを示します。	<code>givenName</code>
名字の属性	ユーザの名字を含む LDAP フィールドを示します。	<code>sn</code>
E メール属性	ユーザの E メールアドレスを含む LDAP フィールドを示します。	<code>mail</code>
ユーザサブツリー	有効にすると、ユーザを検索するときにベース DN のサブツリーが含まれます。	<b>有効</b>
ユーザ ID の属性	ユーザ ID として識別される LDAP フィールドを示します。これは、Contrast にログインするときに入力するユーザ名です。	<code>uid</code>
認証ストラテジー	ユーザが認証情報を提供したときの、Contrast によるユーザの認証方法を選択します。 <b>バインド</b> とは、認証のために、ユーザの認証情報がアプリケーションからサーバに送信されることを意味します。 <b>比較</b> とは、サーバによりユーザの認証情報がハッシュ化され、パスワード属性の値と比較されることを意味します。	<b>バインド</b>
パスワード属性	ユーザのパスワードを含む LDAP フィールドです。 認証ストラテジーで <b>比較</b> を選択した場合、この属性にはユーザのハッシュ化されたパスワードが含まれます。	<code>userPassword</code>

- 誰かがログインするために LDAP リクエストを行った場合に自動的に新規ユーザアカウントを作成するには、**ユーザプロビジョニングを有効にする**の横にあるチェックボックスをオンにします。ドロップダウンメニューを使用して、新規ユーザのデフォルトの**組織**、**デフォルトの組織ロール**、**デフォルトのアプリケーションアクセスグループ**を選択します。
- Contrast では、ログイン時にユーザの LDAP グループに応じてユーザを自動的にプロビジョニングしたり、プロビジョニングを解除したりできます。この機能が LDAP ベースの認証について有効になっている場合、ユーザは対応する LDAP グループにマッピングされた Contrast アクセスグループに追加され、禁止された Contrast グループから削除されます。ユーザは複数のグループに追加でき、また複数の組織へのアクセス権が付与されるグループにも追加できます。



### 重要

これを機能させるには、Contrast グループが既に存在している必要があり、(プロビジョニング目的の)LDAP のグループの名前が Contrast グループの名前と一致する必要があります。

- Contrast にログインするときにユーザをグループに追加するには、**ログイン時にユーザを Contrast グループに追加**の横にあるチェックボックスをオンにします。Contrast にログインするときにユーザをグループから削除するには、**ログイン時にユーザを Contrast グループから削除**の横にあるチェックボックスをオンにします。

## LDAP での自己署名/プライベート証明書の使用

SSL を使用してサーバに接続するよう [LDAP インテグレーションを設定 \(790ページ\)](#)している場合は、サーバの証明書を Contrast JRE が使用する新しい信頼ストアにインポートしなければならない場合があります。

- はじめに、管理者から、サーバの証明書を PKCS#12 フォーマットで取得します。自己署名証明書を使用している場合、これは実際の LDAP サーバの証明書になります。プライベート証明書(CA)がある場合は、そのサーバの CA 証明書が必要になります。
- サーバの証明書を入手したら、これを Contrast を実行する JRE が使用する信頼ストアにインポートします。Contrast がインストールされているディレクトリのコマンドシェルから、管理者として以下のコマンドを実行します。

```
$ jre/bin/keytool -import -file <path to certificate> -alias <hostname> \
  \-keystore <ts install>/jre/lib/security/cacerts
```

- Contrast Server サービスを再起動して、LDAP に対するクエリで SSL が使用されるようになったことを確認します。

## システムレベルでのシングルサインオン(SSO)の設定

シングルサインオン(SSO)は、ひとつの資格情報を使用して複数のアプリケーションにアクセスできる認証サービスです。システム管理者は、このサービスを SAML 2.0 でサポートされるプロバイダで使用するよう Contrast を設定できます。



### 注記

詳細については、[SAML 2.0 仕様](#)を参照してください。

認証は、ID プロバイダ(IDP)を介して行われます。独自の汎用 IDP を使用することもできますし、[Okta](#)、[OneLogin](#)、[Ping Identity](#)、[ADFS](#) などの一般的なサードパーティのプロバイダを使用することもできます。

IDP のメタデータ情報を準備したら、XML ファイルまたはメタデータの URL で Contrast に接続するためのメタデータを指定します。

オンプレミス版のお客様の場合、スーパー管理者(SuperAdmin)がシステムレベルで SSO を設定します。SaaS 版をご利用のお客様は、組織レベルで SSO を設定できます。マルチテナントホストのインスタンスでは、1 つの Contrast インスタンスに複数の IDP を設定できます。



### 注記

ユーザがメールアドレスではなくユーザ ID で識別されている場合、それらのアカウントは自動的に SSO 設定に移行されず、再作成する必要があります。

## 開始する前に

SSO を使用する場合は、ユーザの電子メールを渡すよう NameID を設定する必要があります。

オプションとして、ユーザの名前と名字を設定する場合には、次のように SAML アサーションを使用して追加の属性を渡すように IdP を設定する必要があります。

- **名前** : `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname`
- **名字** : `http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname`

これらのフィールドが存在しないか空白の場合、デフォルトでは NameID フィールドが使用されます。また、ユーザプロビジョニングが有効になっている場合は、ユーザの名字と名前が自動的に入力されます。

```
1<saml2:Attribute Name="http://schemas.xmlsoap.org/ws/2005/05/identity/
2      \
3      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified"
4      >
5      <saml2:AttributeValue xmlns:xs="http://www.w3.org/2001/
6      XMLSchema"
7      xmlns:xsi="http://www.w3.org/2001/
8      XMLSchema-instance"
9      xsi:type="xs:string"
10     >Dan</saml2:AttributeValue>
11</saml2:Attribute>
```

## 手順

1. Contrast では、SAML 認証用のキーは提供されません。秘密キーを指定せずに SSO を有効にした場合、IDP によるログインのみを実行できます。Java キーツールを使用して、独自の自己署名キーを生成する必要があります。

```
keytool -genkeypair -alias some-alias -keypass changeit -keyalg RSA -
keystore samlKeystore.jks
```

2. [暗号化プロパティエディタ \(807ページ\)](#)を使用して `saml.properties` を変更し、前の手順で作成したキーストアに対する値を更新します。

```
authenticator.saml.keystore.path           : /path/to/
samlKeystore.jks
authenticator.saml.keystore.default.key    : some-alias
authenticator.saml.keystore.passwordMap   : some-alias=changeit
authenticator.saml.keystore.password      : changeit
```

3. 変更を行ったら、Contrast を再起動して、新しいキーストアを認識させます。
4. Contrast の [システムの設定 \(785ページ\)](#) で、**認証** を選択し、次に **認証方法を変更** を選択します。
5. **シングルサインオン** を選択します。
6. 指定した情報を使用して、お使いの IDP と Contrast を設定します (IDP の設定では、**エンティティ ID とメタデータ URL** の入力も必要です)。

➔ 認証の設定
✕

ステップ 2 ID プロバイダの設定  
SAML 認証を使用してユーザーを認証するために ID プロバイダ (IdP) と Contrast を連携します。

**Contrast サービスプロバイダ情報** [メタデータ URL をコピー](#)

エンティティ ID *	メタデータ URL	属性
http://ec2-52-68-234-25.ap-northeast-1.compute.amazonaws.com/Contrast/saml/metadata	http://ec2-52-68-234-25.ap-northeast-1.compute.amazonaws.com/Contrast/saml/metadata	None required
バージョン	バイディング方式	Assertion Consumer URL
2.0	HTTP-POST	http://ec2-52-68-234-25.ap-northeast-1.compute.amazonaws.com/Contrast/saml/metadata

必要な設定 :

ID プロバイダ \*

メタデータ URL へアクセス可

IdP メタデータ \*

```
<EntityDescriptor xmlns="urn:oasis:names:tc:SAML:2.0:metadata" entityID="http://ec2-52-68-234-25.ap-northeast-1.compute.amazonaws.com/Contrast/saml/metadata">
  <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="false"
    protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol
urn:oasis:names:tc:SAML:1.1:protocol http://schemas.xmlsoap.org/ws/2003/07/secext">
    <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="http://ec2-52-68-234-25.ap-northeast-1.compute.amazonaws.com/Contrast/saml/metadata" />
  </SPSSODescriptor>
</EntityDescriptor>
```

承認されているドメイン (新ユーザ) \*

+ ドメインの追加

デフォルトの組織       デフォルトの組織ロール (新ユーザ)       デフォルトのアプリケーションアクセスグループ

ユーザプロビジョニングを有効にする

SSO ログイン時にユーザを Contrast グループに追加

SSO ログイン時にユーザを Contrast グループから削除

7. **ID プロバイダ** の名前を入力します。
8. IDP メタデータを入力します。メタデータ URL にアクセスできる場合、チェックボックスをオンにし、URL を入力します。
9. Contrast にログインするための SAML リクエストがあった時に、新しいユーザアカウントを自動的に作成する場合は、**ユーザプロビジョニングを有効にする** のチェックボックスをオンにします。
  - ドロップダウンを使用して、新規ユーザのデフォルトの組織ロールとデフォルトのアプリケーションアクセスグループを選択します。
  - ユーザプロビジョニングのトリガーに使用する必要のある承認されているドメインを追加します (例 : yourdomain.com)。

**注記**

[ユーザをグループに自動追加 \(781ページ\)](#) することもできます。

10. **保存** を選択します。エラーが発生した場合は、[デバッグログを確認 \(765ページ\)](#) してトラブルシューティングを行ってください。
11. **Contrast を再起動 (757ページ)** して、変更を適用します。

接続が完了したら、**SSO** タブに戻って設定を確認・編集します(変更を適用するには、再テストして **Contrast を再起動 (757ページ)**してください)。組織の設定をデフォルトに戻すには、**Contrast 管理認証に戻す**を選択して、変更を確定します。

インストール時に SuperAdmin を無効にした場合は、パブリックノード用とシークレットノード用の2つのメタデータが提供されます。両方の設定を Contrast インターフェイスで行う必要があります。

## 関連項目

- [☑ SAML インテグレーションのトラブル解決方法](#)
- [☑ Okta を使用してユーザとグループのプロビジョニングを設定する](#)
- [☑ グループにユーザを自動的に追加するように ADFS を構成する](#)

## HTTPS プロキシ認証の有効化

認証に、信頼できるプロキシを使用することができます。このプロキシを使用して、ユーザを認証し、ユーザ名を HTTP ヘッダで Contrast に送信できます(このタイプの認証は、特に x 509 クライアントで便利です)。

認証の設定を開始する前に、ユーザを Contrast で設定しておく必要があります。また、認証後に Contrast にアクセスできるよう、両方の設定で同じメールアドレスをユーザ名として使用する必要があります。

信頼できる HTTPS プロキシ認証を有効にするには：

1. `~/path_to_contrast_installation/data/conf/auth.properties` で認証モードを `http_header` に変更し、`auth.properties` プロパティファイルを更新します。
2. デフォルトの HTTP ヘッダ名は、`Contrast-Authentication` です。これは、`auth.properties` ファイルで `auth.http.header.field.name` の値を更新することによっても設定できます。
3. Contrast を再起動した後は、それぞれのリクエストに HTTP ヘッダの `Contrast-Authentication: username` を含めてログインする必要があります。



### 注記

信頼できる HTTPS プロキシ認証を使用できるのは、全ての Contrast ノードが信頼できるプロキシを通じてのみアクセスできる場合に限られます。ノードには直接アクセスできないようにしてください。さもなければ攻撃者が任意の認証されたユーザになります。恐れがあります。

## システムレベルでのパスワードの設定

パスワードポリシーを作成して、システムレベルでパスワードを規制します。

1. [システムの設定 \(800ページ\)](#)で**セキュリティ**を選択します。
2. デフォルトパスワードポリシーで、**組織の上書きを許可**する場合は、このチェックボックスをオンにします。これにより、組織管理者は**組織のパスワードポリシーを設定 (712ページ)**できるようになります。
3. ポリシーについて、以下の設定を入力します。
  - パスワード強度を設定します。弱、中、強、複雑またはカスタムを選択できます。カスタムを選択した場合は、**最小限必要な大文字、小文字、数字、記号の文字数**を入力します。
  - 必要な文字数を**最小桁数**フィールドに入力します。
  - ドロップダウンメニューを使用して、**パスワード期限**が切れるまでの時間を選択します。

- ログインのロックアウトまでのログイン試行回数を入力します。
- 非アクティブアカウントの有効期限が切れるまでの時間を入力します。
- パスワードの再利用を制限のチェックボックスをオンにし、ドロップダウンメニューを使用して、各パスワードを再利用できる回数を選択します。
- パスワードのリセットを制限のチェックボックスをオンにし、ドロップダウンメニューを使用して、リセットのリクエストの送信後にユーザがパスワードをリセットできる日数を選択します。
- ドロップダウンメニューを使用して、アイドルタイムアウトおよびセッションタイムアウトまでの経過時間を選択します。

#### 4. 保存を選択します。

## Linux で SuperAdmin パスワードをリセット

SuperAdmin のパスワードを変更するには、`contrast-server.vmoptions` ファイルを編集するか、環境変数を使用します。

ほとんどの場合、`contrast-server.vmoptions` ファイルを編集するのが最も簡単な方法です。Contrast アプリケーションをコンテナで使用している場合は、パスワードのリセットには環境変数を使用してください。

### 手順

1. コマンドプロンプトを開き、インストール時に作成した Contrast サービスのアカウントでログインします。例：

```
sudo -su contrast_service
```

2. 次のコマンドを実行して、Contrast サーバをシャットダウンします。

```
$CONTRAST_INSTALLATION/bin/contrast-server stop
```

3. パスワードをリセットするために `contrast-server.vmoptions` ファイルを使用しますか？
  - 使用する場合は、**手順 4** に進みます。
  - 使用しない場合は、**手順 5** に進みます。
4. `contrast-server.vmoptions` ファイルを使用してパスワードをリセットするには、以下の手順を実行します。
  - a. `$CONTRAST_INSTALLATION/bin` ディレクトリに移動します。ほとんどのシステムで、このディレクトリは `/opt/Contrast/bin` です。
  - b. テキストエディタで、`contrast-server.vmoptions` ファイルを開きます。
  - c. ファイルに以下のオプションを追加します(`youremaildomain.com` を自分の E メールドメインに置き換えてください)。

```
-Dreset.superadmin=true  
-Dsuperadmin.username=contrast_superadmin@<your.email.domain.com>  
-Dsuperadmin.password=<password>
```

5. `vmoptions` ファイルの代わりに環境変数を使用してパスワードをリセットするには、以下の手順を実行します。
  - a. `$CONTRAST_INSTALLATION` ディレクトリに移動します。ほとんどのシステムで、このディレクトリは `/opt/Contrast` です。
  - b. 次のコマンドを入力します。

```
export INSTALL4J_ADD_VM_PARAMS="$INSTALL4J_ADD_VM_PARAMS -  
Dreset.superadmin=true -  
Dsuperadmin.username=contrast_superadmin@<your.email.domain.com> -  
Dsuperadmin.password=<new password>"
```

6. 次のコマンドを実行して、Contrast サーバを起動します。

```
$CONTRAST_INSTALLATION/bin/contrast-server start
```

サーバが起動したら、**手順 4** または **手順 5** で指定したパスワードを使用します。

7. 次のコマンドを実行して、Contrast サーバをシャットダウンします。

```
$CONTRAST_INSTALLATION/bin/contrast-server stop
```

8. `contrast-sersver.vmoptions` ファイルを使用した場合、手順 4 で追加したオプションを削除します。
9. 通常通りに Contrast サーバを起動してから、シェルを終了します。  
環境変数を使用してパスワードをリセットした場合、この手順により `INSTALL4J_ADD_VM_PARAMS` 環境変数からパスワードがクリアされます。

## Windows で SuperAdmin パスワードをリセット

Contrast アプリケーションで SuperAdmin のパスワードをリセットするには：

1. Contrast Server サービスを停止します。
2. `cmd.exe` を右クリックして**管理者として実行**を選択し、管理者としてコマンドプロンプト (`cmd.exe`)を起動します。
3. `Contrast\bin` ディレクトリに移動します(ほとんどの場合、これは `C:\Program Files\Contrast\bin` です)。
4. 以下のコマンドを使用して、JVM オプションを編集します。

```
notepad contrast-server.vmoptions
```

5. ファイルに以下のオプションを追加します(`youremaildomain.com` を自分の E メールドメインに置き換えてください)。

```
-Dreset.superadmin=true  
-Dsuperadmin.username=contrast_superadmin@<your.email.domain.com>  
-Dsuperadmin.password=<password>
```

6. ファイルを保存し、メモ帳を終了します。
7. 次のコマンドを使用して、Contrast サービスを起動します。

```
net start "Contrast Server"
```

8. 新しいパスワードでログインできることを確認します。
9. 次のコマンドを入力して Contrast サービスを停止します。

```
net stop "Contrast Server"
```

10. 次のコマンドを入力して、JVM オプションを編集します。

```
notepad contrast-server.vmoptions
```

11. ステップ 5 で追加したオプションを削除します。
12. ファイルを保存し、メモ帳を終了します。
13. コマンドプロンプトを終了します。
14. Contrast Server サービスを通常どおりに(サービスコントロールパネルから)起動します。

## キーの管理

システム管理者は、全ての組織でキーにポリシーを設定して、常にセキュリティ基準を満たすようにすることができます。

1. [システムの設定 \(800ページ\)](#)の左ナビゲーションで**セキュリティ**を選択します。
2. **API キー**のセクションで、キーに必要な文字数、数字、大文字および小文字の最小数を選択します。これらの規則は、[API キーのローテーション \(37ページ\)](#)時に適用されます。
3. **ログオン時に無効な IP をマスクする**場合は、画面上部のチェックボックスをオンにします。
4. **保存**を選択します。

## システムの設定

システムの設定のページでは、システムレベルの標準の設定を指定できます。

Contrast を[分散環境で構成する \(753ページ\)](#)場合には、異なる設定が必要になります。



## 手順

1. スーパー管理者(SuperAdmin)、サーバ管理者(ServerAdmin)またはシステム管理者(SystemAdmin)としてログインします。
2. ユーザメニューで **SuperAdmin** を選択します。
3. ユーザメニューで**システムの設定**を選択します。  
以下を利用できます。
  - [全般的な設定 \(802ページ\)](#)
  - [ライセンス管理 \(803ページ\)](#)
  - [ポリシー \(806ページ\)](#) (ライブラリコンプライアンスの設定)
  - [セキュリティ\(パスワード \(798ページ\)、2段階認証 \(478ページ\)、キーの管理 \(800ページ\)\)](#)
  - [エージェントキー\(組織の設定にあるものと同じエージェントキー \(37ページ\)\)](#)です)
  - [認証 \(785ページ\)](#)
  - [メール \(807ページ\)](#)
  - [スコアの設定 \(719ページ\)](#)

## その他のシステム設定

システムの設定は、上記に加えて以下が可能です。

- [Tomcat の設定 \(758ページ\)](#)
- [Java ランタイム環境\(JRE\)の設定 \(759ページ\)](#)
- [HTTPS の設定 \(759ページ\)](#)
- [組織の追加 \(774ページ\)](#)
- [ログレベルの設定 \(766ページ\)](#)
- [レポート用ストレージの設定 \(764ページ\)](#)

## システムの全般的な設定

全般的な設定は、[システムの設定 \(800ページ\)](#)の一部です。ここでは、以下の設定を構成できます。

- **デフォルトの言語**：ユーザインターフェイスの言語を選択します。
- **X-Forwarded-For ヘッダを使用**：このヘッダを監査に使用する場合は、チェックボックスをオンにします。
- **プロキシ**：インターネットトラフィックの宛先に接続します。
- **Contrast HUB**：Contrast Hub (ハブ)と連携して、ライブラリと CVE を更新します。
- **診断**：スムーズなサポートと迅速な問題解決のために Contrast の稼働状態の統計を送信します。
- **エージェント診断**：ルールやパフォーマンスを改善し、製品の改善に優先順位を付けるために Contrast エージェントのデータを送信します。
- **Heroku の設定**：Heroku 連携のパスワードと SSO ソルトを入力します。

## システムレベルでの診断サービスの管理

Contrast 診断サービスでは、お客様による製品の利用状況が測定され、より迅速で積極的なサポートや新機能を提供できるようになります。

Contrast では、Contrast の SaaS 版プラットフォームの診断サービスに対して、関連するデータ要素とデータ集約のスナップショットが定期的に送信されます。顧客や組織を特定するために使用される可能性のあるデータには一方向ハッシュが使用され、転送中と保存中の両方で暗号化されます。プライバシーの問題により、データにはアプリケーション名、個人識別情報、コード、脆弱性 ID、顧客ネットワーク識別子は含まれません。

このデータは Contrast のデータベースに保存され、承認されたサポートおよび開発チームが分析やレポートに使用できます。データベース内でデータはお客様に帰属しており、Contrast のお客様により良いサポートを提供するのに役立てられます。

診断サービスは、以下の 3 つの方法でカスタマーサポートを向上します。

- カスタマーサポートは、診断データを分析することで、お客様に積極的に連絡して問題を防ぐことができます。
- 収集されたデータを使用して既存の問題を迅速に診断し、サポートケースを解決するためのサイクル時間を短縮できます。
- Contrast の製品開発チームは、デプロイや使用状況に関する知見を得ることで、お客様のニーズをより的確に満たすよう調整して新機能を提供できます。

SuperAdmin、ServerAdmin または SystemAdmin として、オンプレミスシステム全体の診断サービスを有効/無効にすることができます。

1. システム設定の左側のナビゲーションで、**一般設定**を選択します。
2. **インターネットの設定**で、トグルボタンを使用して無効/有効を切り替えます。診断サービスはデフォルトで有効になっています。
3. プロキシ設定は、と診断の設定に適用されます。



## ヒント

REST API を使用して、これらの診断サービスで Contrast に送信されるデータをプレビューすることもできます。

## システムレベルでのライセンスの割当て

Contrast のライセンスには、次のような種類があります。

- オンプレミス版のお客様は、Contrast サーバを [インストール \(746ページ\)](#) および [アップグレード \(768ページ\)](#) するためのライセンスが必要です。
- SaaS 版およびオンプレミス版のお客様は、Assess(アプリケーションライセンス)、Protect(サーバライセンス)、SCA(ライブラリライセンス)の各製品のライセンスが必要です。

以下の手順に従って、Assess ライセンスや Protect ライセンスを組織に割り当てます。

## 開始する前に

- オンプレミス版のお客様の場合、Assess および Protect ライセンスを特定の組織に割り当てるには、SuperAdmin ロールか ServerAdmin ロールが必要です。  
SaaS 版をご利用の場合は、Contrast Security がこのライセンス処理を行います。
- アプリケーションに適用されたライセンスは、最大許容アプリケーション数に対して永続的にカウントされます。ライセンスが適用されたアプリケーションを削除しても、アプリケーションに適用可能な最大ライセンス数に影響はありません。

## ライセンスを割り当てる手順

1. ユーザメニューで **SuperAdmin** または **ServerAdmin** を選択します。  
組織の一覧が表示されます。ライセンス列には、各組織で使用可能な Assess ライセンスと Protect ライセンスの総数が表示され、続けて未使用のライセンス数が括弧書きで表示されます。
2. 以下のいずれかの方法で「ライセンス概要」を開きます。
  - 組織ページの「ライセンス」列で **Assess** または **Protect** を選択。



- 組織の行の右端にある三角形(▼)を選択して**ライセンス概要**を選択。



3. 利用可能な Assess ライセンスを組織に追加するには：

- a. Assess のライセンスバーの上にある、**ライセンスを追加**を選択します。
- b. **Assess** ライセンスに、この組織で利用できるようにするライセンスの数を入力します。
- c. **有効期限**には、追加するライセンスの有効期限を入力します。
- d. **割り当て**を選択します。

### ライセンス概要

AZTestOrg組織のライセンス概要です。

#### 10 Assessライセンス

0/10

ライセンスを追加

🚫 使用されていないライセンスを取消

#### ライセンスの割り当て ×

< 戻る

AZTestOrg組織にライセンスを割り当てます。

Assessライセンス	有効期限
5	02/01/2023 <span style="float: right;">×</span>

9999999999ライセンスのうち9999969602ライセンス使用可能

キャンセル
割り当て

4. 使用されていない Assess ライセンスを組織から削除する場合は、Assess ライセンスバーの下にある**使用されていないライセンスを取消**を選択します。
5. 組織に割り当てられている、購入済み Protect ライセンスの数を変更するには：
  - a. Protect ライセンスバーの上にある**ライセンスの割り当てを変更**を選択します。
  - b. **ライセンスの割り当て**に、組織で使用させたいライセンス数を入力します。  
デフォルト値は、購入したライセンス数です。組織のライセンスを取り消すには、購入したライセンス数より少ない値を入力してください。購入したライセンス数以上のライセンスを取り消すことはできません。
  - c. **変更を保存**を選択します。

ライセンス概要

AZTestOrg組織のライセンス概要です。

5 Assessライセンス ライセンスを追加

0/5

使用されていないライセンスを取消 ×

未使用を取消

5 5/5

10 Protectライセンス ライセンスの割り当てを変更

0/10

ライセンス概要

[< 戻る](#)

Protectライセンスの割り当て

AZTestOrg組織のライセンスの割り当てを変更します。

20 Protectライセンス

0/20

ライセンスの割り当て

20

Cancel 変更を保存

## ライセンス情報と設定に関する手順

- 各組織で利用可能なライセンス数を表示するには、ナビゲーションバーの**組織**を選択します。  
ライセンス列には、各組織で使用可能な Assess ライセンスと Protect ライセンスの総数が表示され、その後に括弧で未使用のライセンス数が表示されます。  
Assess ライセンスの有効期限が近い場合は、赤い警告アイコンが表示されます。アイコンにカーソルを合わせると、失効するライセンス数が表示されます。
- 利用可能なライセンス数や、ライセンスがないアプリケーション数・サーバ数を参照するには、ユーザメニューから**システムの設定 > ライセンス管理**を選択します。
- 新しいアプリケーションまたはサーバに自動でライセンスを適用するには、「ライセンス管理」で「Assess ライセンス」または「Protect ライセンス」のトグルを選択します。次に、この設定をすべてのアプリケーションまたはサーバに適用するか、新しいものだけに適用するかを選択します。  
SuperAdmin、ServerAdmin、SystemAdmin は、[組織作成 \(774ページ\)](#)時にライセンスを自動適用するよう指定することもできます。

4. 「ライセンス管理」の右上で**組織の上書きを許可**するボックスを選択すると、組織管理者はこれらの設定を上書きすることが許可されます(これはデフォルトで有効になっています)。

## システムレベルでのスコア設定のカスタマイズ

Contrast では **アプリケーションのスコア (822ページ)** が算出されますが、必要に応じて **ライブラリのスコア (544ページ)** に依存させることができます。システムレベルでスコア設定をカスタマイズするには：

1. **システムの設定 (800ページ)** で **スコアの設定** を選択します。
2. **総合スコア** でオプションを選択して、Contrast でアプリケーションをどのようにスコア付けするかを決定します。
  - **デフォルトの評価方法** は、アプリケーションの **ライブラリのスコア (544ページ)** とカスタムコードのスコアの平均値です。
  - **カスタムコードのみを評価対象とする** 場合は、アプリケーション全体のスコア計算にライブラリのスコアが含まれなくなります。このオプションを選択した場合、特定の言語を選択するか、全ての言語に適用するかを、クリックして選択します。
3. **ライブラリのスコア** でオプションを選択して、Contrast でライブラリをどのようにスコア付けするかを決定します。
  - **デフォルトの評価方法** では、ライブラリの脆弱性だけでなく、ライブラリの古さやバージョン管理を含むアルゴリズムが使用されます。
  - **脆弱性のみを評価対象とする** 方法では、ライブラリに存在する脆弱性のみに基づいてスコアが計算されます。
4. **組織の上書きを許可** の横にあるチェックボックスを選択すると、組織管理者が **組織レベルでスコアの設定を決定 (719ページ)** できるようになります。
5. **保存** を選択します。



### 注記

ルール管理者(Rules Admin)は、**ポリシーの管理**でポリシーの設定を行い、ポリシーに違反するライブラリを自動的に低いスコア(F)にすることができます。この設定が選択されると、スコアの設定に警告メッセージが表示されます。警告にあるポリシーのリンクをクリックすると、ライブラリポリシーページに移動します。ここで、管理者はそれらの設定を確認して更新ができます。

## ライブラリコンプライアンスポリシーの管理

ライブラリコンプライアンスポリシーは、システムレベルで管理できます。ライブラリコンプライアンスポリシーでは、アプリケーションが安全に使用できるライブラリを制限でき、特定のライブラリにバージョン要件を設定できます。Contrast では、制限されたライブラリを使用するアプリケーションや、コンプライアンスポリシーに違反するライブラリにフラグを立てたり、スコアを低くさせることができます。

ライブラリコンプライアンスポリシーを管理するには：

1. **ユーザメニュー**(Contrast の右上にある自分の名前)を開き、**システムの設定 (800ページ)** を選択します。
2. **ポリシー** を選択します。
3. ポリシーのコンプライアンス要件(使用が制限されたライブラリ、ライブラリバージョンの要件、Contrast でポリシー違反のライブラリを不合格にするか)を設定します。
4. 組織の管理者(Admin)またはルール管理者(Rules Admin)が組織レベルで **コンプライアンスポリシーを設定 (695ページ)** する場合は、**組織の上書きを許可** を選択します。

## システムレベルでの E メール通知の管理

システム管理者は、Contrast が適切な SMTP システムと通信してこれらの通知を受信できるように設定し、有効/無効を切り替えることができます。

通知により、Contrast ユーザはアプリケーションの脆弱性の検出や攻撃、またはパスワードがリセットされた場合など、特定の状況に関するアラートを受信することができます。

組織の管理者は、組織レベルで Contrast の通知のデフォルトを設定 (716ページ) できます。個々のユーザは各自の設定を調整 (479ページ) できます。

システムレベルで通知を設定するには：

1. [システムの設定 \(800ページ\)](#) の左側のナビゲーションで **メール** を選択します。
2. 以下の設定を行います。
  - **メールの有効化**：トグルボタンを使用して、この機能を有効/無効にします。
  - **メールプロトコル**：値は「SMTP」または「SMTPs」になります。
  - **メールホスト**：SMTP サーバの完全修飾アドレスです。
  - **メールポート**：可能性のある値は「25」です。
  - **SMTP 認証を使用**：この設定を有効にするには、チェックボックスをオンにします。
  - **メールユーザ**：SMTP システムでの認証目的のユーザアカウントです。
  - **メールパスワード**：SMTP システムに関連付けられたメールユーザのパスワードです。
  - **差出人**：システム通知の送信元の電子メールアドレスを入力します。
  - **STARTTLS を有効にする**：この設定を有効にするには、チェックボックスをオンにします。
3. **保存** を選択します。

## オンプレミス版 Contrast のメンテナンス

システム管理者には、システムの保守に必要な継続的な作業があります。以下の作業が必要になる場合があります。

- [MySQL データベースのバックアップ \(809ページ\)](#)
- [パフォーマンスの改善 \(28ページ\)](#)
- [Contrast のアップグレード \(768ページ\)](#)
- [エージェントのアップグレード \(769ページ\)](#)
- [ライブラリデータの更新 \(770ページ\)](#)
- [Contrast ライセンスの更新 \(771ページ\)](#)
- [IP アドレスの更新 \(769ページ\)](#)
- [SSL の管理 \(811ページ\)](#)
- [暗号化プロパティエディタの使用 \(807ページ\)](#)

### 暗号化プロパティエディタの使用

Contrast では、`$CONTRAST_HOME/data/conf` ディレクトリにいくつかの設定ファイルが含まれています。デフォルトでは、Contrast はセキュリティのために設定ファイルを暗号化しますが、Contrast のワークフローを介してこれらのファイルの一部を変更できます。

例えば、以下はオンプレミス版インストール用の暗号化されたプロパティファイルの一部です。

名前	内容
<code>ad.properties</code>	Active Directory グループの認証用に Contrast を接続および構成するための設定。
<code>ldap.properties</code>	LDAP グループの認証用に Contrast を接続および構成するための設定。
<code>database.properties</code>	Contrast と MySQL の間で通信するためのホストと接続の設定。
<code>saml.properties</code>	SAML キーストアのセキュリティ設定

Contrast には、これらのファイルを復号化し設定を支援する編集ツールも含まれています。このツールは、[Contrast の実行 \(756ページ\)](#) 中に、アプリケーションの外部の暗号化されたプロパティファイルが

ら値を取得したり、自動パスワードローテーションなど、ファイル内のプロパティを自動的に更新したりする必要がある場合に役立ちます。

暗号化されたプロパティファイルを編集するには：

1. `$CONTRAST_HOME/bin` ディレクトリで以下の復号化ツールを見つけます。
  - **Linux** : `edit-properties` という名前のシェルスクリプト
  - **Windows** : `edit-properties.cmd` という名前の Windows コマンドファイル
2. コマンドプロンプトからツールを実行します。これにより、暗号化されたプロパティの値を更新できるアプリケーションが開きます。

```
$CONTRAST_HOME/bin/edit-properties -e $CONTRAST_HOME/data/esapi -f \
$CONTRAST_HOME/data/conf/ad.properties
```

3. 暗号化されたプロパティファイルを表示または編集するには、入力の詳細を指定する必要があります。入力が必要な基本項目は以下のとおりです。

- *ESAPI.properties* へのパス。
- 編集するターゲットプロパティファイル。

暗号化プロパティエディタ用にこの情報を見つけるには、引数を指定せずに `edit-properties` を実行します。

```
contrast@EOP-TeamServer:~/contrast/bin$ ./edit-properties

usage: property-editor
  -c,--comment <text>          The comment for the top of the file
  -e,--esapi <path>           The path to the ESAPI.properties file
  -f,--targetFile <file>      The properties file to edit
  -o,--print-value             Print out the value of the property and exit
  -p,--property <name>       The name of the property to set
  -v,--value <val>           The value of the property
```

4. この例は、暗号化ファイルの編集方法を示しています。*ESAPI.properties* へのパスと編集するターゲットプロパティファイルを指定します。ファイル内で暗号化されている編集可能な既存の値が表示されます。上記の usage オプションでは、単一のプロパティを表示または編集できます。

```
contrast@TeamServer:~/contrast/bin$ ./edit-properties -e ../data/esapi/ -f ../data/conf/ad.properties

ad.userDn : cn=Directory Manager
ad.identity.attribute.name : mail
ad.password : NotARealPassword
ad.nested.groups.enabled : false
ad.group.users : \
cn=ContrastUsers,cn=Users,dc=contrastsecurity,dc=com
ad.group.admin : \
cn=ContrastAdmins,cn=Users,dc=contrastsecurity,dc=com
ad.url : ldap://localhost:389
ad.base : \
dc=contrastsecurity,dc=com
```

5. プロパティの暗号化されていない値を取得または更新することもできます。値を取得するには、プロパティエディタに別のパラメータを渡します。この例では、データベースプロパティに関する詳細を調べています。

```
$CONTRAST_HOME/bin/edit-properties \
  -e $CONTRAST_HOME/data/esapi \
  -f $CONTRAST_HOME/data/conf/database.properties \
  -p jdbc.username \
  -o
```



暗号化されていない値を更新するには、プロパティエディタに別の引数セットを渡します。

```
$CONTRAST_HOME/bin/edit-properties \  
-e $CONTRAST_HOME/data/esapi \  
-f $CONTRAST_HOME/data/conf/database.properties \  
-p jdbc.username \  
-v joe.user \  
-c "Updating JDBC Password"
```



### 注記

暗号化されているプロパティファイルを編集した場合は、編集内容を示すコメントを追加しておきます。これは、設定の変更を追跡する必要がある監査担当者などのために役立ちます。

## MySQL のバックアップ

次の手順を使用して、Contrast インストーラで作成された MySQL のデータベースを管理します。

これらの手順は、お客様が分散環境用に作成した MySQL データベースには適用できません。

- [MySQL の自動バックアップを作成する \(809ページ\)](#)
- [MySQL を手動でバックアップする \(809ページ\)](#)
- [データベースのバックアップを復元する \(810ページ\)](#)
- [自動バックアップを無効にする \(810ページ\)](#)

## MySQL を手動でバックアップする

Contrast に含まれる backup-db スクリプトを使用しても、バックアップが可能です。

### 開始する前に

- backup-db スクリプトを実行するための権限があることを確認してください。通常、これを行うには、Contrast のインストール所有者、root、Windows の管理者アカウントである必要があります。
- Contrast が実行中であり、MySQL が利用可能であることを確認してください。

### 手順

1. まだ行っていない場合は、データベースバックアップの場所を設定します。[暗号化工具エディタ \(807ページ\)](#)を使用して `$CONTRAST_HOME/data/conf/database.properties` ファイルを編集することで、`database.bk.dir` の場所を設定します。
2. 環境に応じたバックアップコマンドを実行します。
  - **Windows:** `$CONTRAST_HOME\bin\backup-db.cmd`
  - **Linux:** `$CONTRAST_HOME/bin/backup-db.sh`

## MySQL の自動バックアップを作成する

Contrast の MySQL データベースのバックアップを定期的にスケジュールして作成することができます。このオプションは [インストール \(746ページ\)](#) 時に選択して、データベースのバックアップの保存先と時刻を指定することができます。

インストール時にこの手順を省略しても、後で Contrast を設定してデータベースのバックアップをスケジュールできます。

## 手順

1. `$CONTRAST_HOME/data/conf/database.properties` で、Contrast のデータベースの設定を探してください。
2. [暗号化プロパティエディタを使用 \(807ページ\)](#)して、データベースの設定を判別します。以下の例は、Contrast データベースのバックアップが有効で、スケジュールされており、特定の場所にあることを示しています。オプションを変更する必要がある場合は、これらの設定を編集することができます。

```
contrast@TeamServer:~/contrast/bin$ ./edit-properties -e ../data/esapi/ -f ../data/conf/database.properties
```

```
database.bk.time           : 4:0:0
database.bk.enabled       : true
database.bk.dir           : /mnt/backups/mysql/
contrast
```

3. Contrast をアップグレードする場合は、最後にスケジュールしたバックアップ以降に作成・更新されたデータを取り込む必要があります。

## 自動バックアップを無効にする

Contrast の MySQL データベースの自動バックアップは停止することができます。スケジュールされたバックアップは、Windows では `schtasks`、Linux では `crontab` を使用して実行されます。

自動バックアップを無効にするには：

**Windows** の場合、タスクスケジューラを使用して `ContrastBackup` を無効にするか、削除します。

**Linux** の場合：

1. Contrast をインストールしたユーザに切り替えて `crontab -l` を実行します。
2. これにより、スケジュールされたジョブの一覧が表示されます。以下のように表示されます。

```
0 2 * * * /usr/local/contrast/bin/backup-db.sh
```

3. バックアップを 1 つ削除する場合には、`crontab -e` を実行します。全てのバックアップを削除するには、`crontab -r` を実行します。



### 注意

`-e` オプションでは、Vim で編集して選択したバックアップを削除できます。`-r` オプションを使用すると全てが削除されます。使用の際は注意が必要です。

## データベースのバックアップを復元する

次の手順は、Contrast インストーラで作成された MySQL データベース用の復元手順です。

この手順は、お客様が分散環境用に作成した MySQL データベースには適用できません。

### 開始する前に

データベースの復元は、MySQL データベース管理者が実行する必要があります。

## 手順

1. [暗号化プロパティエディタ \(807ページ\)](#)を使用して、MySQL データベースの設定を確認します。

2. Contrast をシャットダウンします。
3. Contrast にパッケージ化された MySQL サービスを使用して、MySQL を個別に起動します。  
<YourPath>は、Contrast ホームディレクトリへのパスに置き換えてください。

- **Windows :**

```
"<YourPath>\mysql\bin\mysqld.exe" --defaults-  
file="<YourPath>\data\conf\my.cnf"
```

- **Linux :**

```
sudo -u contrast_service <YourPath>/mysql/bin/mysqld --defaults-  
file=<YourPath>/data/conf/my.cnf --basedir=<YourPath>/mysql --  
datadir=<YourPath>/data/db --plugin-dir=<YourPath>/mysql/lib/plugin --  
lc-messages-dir=<YourPath>/mysql/share --tmpdir=/tmp --lc-  
messages=en_US --log-error=<YourPath>/logs/mysql_error.log --pid-  
file=<YourPath>/data/proc/MysqldResource.pid --port=13306
```

4. MySQL に接続します。<jdbc.host>、<jdbc.port>、<jdbc.user>、<jdbc.schema>を、ご利用のホスト、ポート、ユーザ、スキーマに置き換えてください。

- **Windows :**

```
mysql -h <jdbc.host> -P <jdbc.port> -u <jdbc.user> -p <jdbc.schema>
```

- **Linux :**

```
./mysql -h <jdbc.host> -P <jdbc.port> -u <jdbc.user> -p <jdbc.schema>
```

5. drop database <jdbc.schema>;で、Contrast データベースをドロップします。
6. create database <jdbc.schema>;で、Contrast データベースを作成します。
7. GRANT ALL PRIVILEGES ON \*.\* to 'contrast'@'%';で、Contrast ユーザに権限を付与します。
8. MySQL を終了(exit)します。
9. MySQL のバックアップを復元します。<backup\_location>をバックアップファイルの場所に、<backup\_filename>はバックアップファイル名に置き換えてください。

- **Windows :**

```
mysql -h <jdbc.host> -P <jdbc.port> -u <jdbc.user> -p <jdbc.schema> < \  
<backup_location>/<backup_filename>
```

- **Linux :**

```
./mysql -h <jdbc.host> -P <jdbc.port> -u <jdbc.user> -p <jdbc.schema> \  
< <backup_location>/<backup_filename>
```

10. MySQL をシャットダウンします。

- **Windows :**

Windows のサービスマネージャーを使用して、MySQL サービスをシャットダウンします。

- **Linux :**

```
$(CONTRAST_HOME)/mysql/bin/mysqladmin.exe shutdown -h localhost -P \  
13306 -u contrast -p
```

暗号化プロパティエディタで設定されたパスワードの入力が必要になります。

11. 完全に復元された Contrast と MySQL を一緒に再起動します。

## SSL の管理

オンプレミス版のお客様は、以下の状況で Secure Sockets Layer (SSL)を使用する必要がある場合があります。

- [HTTPS プロキシ認証 \(798ページ\)](#)を設定する場合
- [LDAP \(790ページ\)](#)または [Active Directory \(786ページ\)](#)と連携する場合

- エージェントと Contrast アプリケーション間の通信を保護する場合

# リファレンス

Contrast の使用方法に関する参考資料として、以下をご利用ください。

- [用語集 \(813ページ\)](#)
- [ルールと権限 \(817ページ\)](#)
- [エージェントのサポート対象テクノロジー \(Java \(57ページ\)、.NET Framework \(137ページ\)、\(旧\).NET Framework、.NET Core \(196ページ\)、Node.js \(251ページ\)、Python \(317ページ\)、Ruby \(393ページ\)、Go \(451ページ\)\)](#)
- [アプリケーションのスコアガイド \(822ページ\)](#)
- [ライブラリのスコアガイド \(544ページ\)](#)
- [ログレベル \(824ページ\)](#)
- [対応ブラウザ \(827ページ\)](#)
- [アプリケーションの例外の正規表現 \(694ページ\)](#)

## 用語集

ここでは、Contrast のユーザ向けに各用語の定義を掲載します。他のトピック内でこれらの用語にカーソルを合わせると、文中に定義が表示されます。

Contrast Hub	<a href="#">Contrast Hub</a> は、オンプレミス版をご利用のお客様が Contrast のインストーラとライセンスファイルをダウンロードしたり、エージェントの更新を確認できる場所です。
Contrast コマンドラインインターフェイス (Contrast CLI)	Contrast CLI は、テキストベースのユーザインターフェイスです。開発環境で実行することで、ビルドやデプロイを行う前に早い段階で、オープンソースライブラリのソフトウェアコンポジション解析(SCA)を可視化できます。CLI による結果は、テキストベースのレスポンスで確認することができ、Contrast Web インターフェイスでは <a href="#">依存関係ツリー (543ページ)</a> としても表示されます。
Contrast サービス	Contrast サービスは Go で書かれたプログラムで、Contrast Web インターフェイスと Node.js、Ruby、Python エージェントを接続します。
distroless イメージ	Distroless イメージとは、アプリケーションおよびアプリケーション実行時の依存関係のみが含まれるイメージです。パッケージマネージャやシェルなど、標準的な Linux ディストリビューションに含まれるその他のプログラムは含まれていません。
IP 拒否リスト	IP 拒否リストとは、そのリストにある IP アドレスからの HTTP リクエストをブロックするルールです。
IP 許可リスト	IP 許可リストとは、そのリストにある IP アドレスからの HTTP リクエストを許可するルールです。
LDAP (Lightweight Directory Access Protocol)	LDAP は、ディレクトリサービスに接続・管理するためのクライアントサーバプロトコルの一つです。Contrast のオンプレミス版では、 <a href="#">LDAP を使用 (790ページ)</a> してユーザやログインを管理できます。
OWASP (Open Web Application Security Project)	<a href="#">Open Web Application Security Project®</a> は、セキュリティプロジェクトの共有や会員の教育をサポートするオープンプラットフォームによって、ソフトウェアのセキュリティを向上するための非営利団体です。 <a href="#">OWASP Top 10</a> には、Web アプリケーションにおける最も重大なセキュリティ上の欠陥がリストアップされています。

SAML (Security Assertion Markup Language)	SAML は、シングルサインオン認証など、オンラインパートナー間で認証情報を作成・交換するために使用される XML ベースの標準規格です。
SIEM (Security Incident Event Management)	SIEM システムは、他のシステムからセキュリティイベントや関連データを収集して分析し、脅威の検知やコンプライアンス、セキュリティインシデントの管理をサポートします。Contrast は、いくつかの代表的な SIEM システムと連携できます。
SQL インジェクション (SQLi)	SQL インジェクションは、クライアントからのユーザ入力データ内に SQL クエリを挿入(「インジェクション」)して、アプリケーションに取り込ませる攻撃です。この攻撃の目的は、データベースのデータの読み取りや変更、データベースへのコマンドの送信です(例)。
WAF (Web Application Firewall)	WAF は、Web トラフィックを検査・フィルタリングし、一般的な攻撃からアプリケーションを防御するためのものです。
Webhook	指定したイベントが発生するたびに、あるアプリケーションから別のアプリケーションに対して HTTP 経由でリアルタイムに情報を送信するための仕組みのこと。
アカウント乗っ取り (ATO)	アカウント乗っ取りは、ログイン認証情報を盗んだり、Web アプリケーションの認証に侵入したりする攻撃の結果です。
アプリケーション	アプリケーションは、Contrast エージェントによって検査されるカスタムコードの論理的なグループです。
アメリカ国立標準技術研究所 (NIST)	NIST は、サイバーセキュリティを含む複数の分野で、計測学、標準規格、産業技術を進歩させることにより、米国の技術革新と産業競争力を促進するための政府機関です。
インストゥルメント (instrument)	ランタイムにデータを観測・報告するソフトウェアエージェントがアプリケーションをモニタリングすることです。Contrast では、アプリケーションに Contrast エージェントを組み込むことを意味します。Contrast エージェントは、疎通されたルートに基づいてアプリケーションの脆弱性データを送信します。
インタラクティブアプリケーションセキュリティテスト (IAST)	実行中のアプリケーション内のデータフローを分析し、セキュリティ上の脆弱性の可能性を検出・報告するセキュリティ技術。
エージェント	エージェントとは、Web アプリケーションにインストールされる言語固有のコードで、セキュリティデータを収集・解析し、必要に応じて検出結果を Contrast に報告します。
クレデンシャルスタッフィング	クレデンシャルスタッフィングはブルートフォース攻撃の一種で、漏洩したユーザ名とパスワードの組み合わせを自動的に実行してユーザアカウントにアクセスします。
クロスサイトスクリプティング (XSS)	クロスサイトスクリプティングとは、ユーザ入力によって悪意のあるスクリプトが Web アプリケーションに注入されて、検証やエンコードを行わずにその出力が生成された場合に発生する攻撃です。
コマンドインジェクション	コマンドインジェクション攻撃は、脆弱なアプリケーションを介してホストのオペレーティングシステムを標的とするものです。この攻撃は、ユーザがフォーム、Cookie、HTTP ヘッダ、またはアプリケーションのその他の部分から安全でないデータをシステムシェルに渡すことで発生します。

コンテナイメージ	コンテナイメージは、コンピュータシステム上にコンテナを作成できる実行可能コードが含まれた静的ファイルです。
シンク	シンクとは、 <a href="#">データフローの解析 (595ページ)</a> でデータが終着する場所です。シンクは、データが書き込まれる外部フォーマットや出力先のことです。
シングルサインオン (SSO)	シングルサインオンは、ユーザが 1 セットの資格情報だけで複数のシステムにアクセスできるユーザ識別・認証サービスです。
スコア	Contrast では、アプリケーションやライブラリの現在のセキュリティの状況を反映した <a href="#">ライブラリ (544ページ)</a> のスコアと <a href="#">アプリケーション (822ページ)</a> のスコアが提供されます。
スタックトレース	スタックトレースは、問題の発生となった一連のイベントを一覧表示するものです。Contrast では、スタックトレースにはセキュリティの脆弱性に至るまでのイベントが表示されます。
ソース	ソースとは、 <a href="#">データフローの解析 (595ページ)</a> でデータが発生する場所です。ソースは、システムに入力されるあらゆる入力データやリクエストのことです。
ソフトウェアコンポジション解析 (SCA)	脆弱なライブラリを特定し、CVE の深刻度に基づいてビルドを失敗させ、依存関係ツリーを表示して、ライブラリの依存関係や脆弱性が存在する箇所を把握することができます。
ソフトウェア開発ライフサイクル (SDLC)	企画がソフトウェアの生産に至るまでの一連の工程のこと。
テストカバレッジ	実行されたテストの数を把握するテスト手法です。
パストラバーサル	パストラバーサルは、Web のルートフォルダ外に保存されている重要なシステムファイルやディレクトリにアクセスしようとする攻撃です。この攻撃では、絶対ファイルパスや「ドット-ドット-スラッシュ」(..)の並びでファイルを参照する変数が使用されます。
フールスポジティブ(false positive)	誤って脆弱性として報告してしまうこと。誤検知のこと。
フローマップ	フローマップは、Contrast エージェントが組み込まれているアプリケーションを可視化したもので、そのアプリケーションが使用しているすべてのバックエンドシステムと、接続されているその他のアプリケーションを表します。これにより、脆弱なアプリケーションに影響を与えるその他の要素を分析し、リスクを評価できます。
ブルートフォース攻撃	ブルートフォース攻撃は、最終的に正しく推測することを目的として、多くのパスワードやパスフレーズを体系的に送信することです。
プロファイラチェーン	プロファイラチェーンは、パフォーマンスツールや APM ツールなどの他の.NET プロファイラエージェントと一緒に.NET Framework エージェントまたは.NET Core エージェントを実行する方法です。
ポリシー	ポリシーとは、特定のアプリケーションやライブラリについて、指定の条件が満たされたときにセキュリティ違反やステータス変更、通知をトリガーする一連のルールのことです。ポリシーにより、アプリケーションやチーム全体でより一貫したセキュリティ基準が保証されます。
マニフェスト	プロジェクトに必要な依存関係を宣言するためにプロジェクトに保存されるファイル。

ライブラリ	ライブラリとは、アプリケーションに含まれるパッケージ化されたコードのことです。 <a href="#">ライブラリ (534ページ)</a> には、公開と内製のものがあります。
ランタイムアプリケーションセルフプロテクション (RASP)	Contrast は、RASP の手法を用いて攻撃を監視し、本番環境のアプリケーションを積極的に防御します。
ルール	ルールとは、脆弱性イベントや攻撃イベントを特定するために使用されるセキュリティ制御です。ルールが一致すると、影響を受けるアプリケーションの脆弱性イベントや攻撃イベントをエージェントが Contrast サーバに送信します。
依存関係かく乱	依存関係かく乱は、「置換攻撃(substitution attack)」とも呼ばれ、攻撃者が組織の内部リポジトリに脆弱なコードや悪意のあるコードを入れ込むために、組織の内部ライブラリと同じ名前を公開パッケージのインデックスに登録することで発生します。
環境	Contrast では、アプリケーションの環境として「開発」、「テスト(QA)」、「本番」の 3 つの環境のいずれかを設定できます。
環境変数	環境変数は、実行時にソフトウェアに渡すことができる値で、通常はキーと値のペアであり、アプリケーションの外部で定義します。Contrast では、環境変数はアプリケーションを検査する <a href="#">エージェントを設定する (35ページ)</a> ために使用します。これらの変数によって、利用したいフレームワーク内でアプリケーションが予想どおりに動作し、Contrast で表示したいメタデータが報告されるようになります。
機密データのマスキング	この機能は、Contrast ログや Contrast エージェントから送信されるその他のデータに含まれる機密データを、アプリケーションでのデータ処理に影響を与えることなくデータにマスクをかけます。
共通言語ランタイム (CLR)	共通言語ランタイム(CLR)は、.NET Framework のプログラムを実行するための動作環境です。
共通脆弱性識別子 (CVE)	<a href="#">共通脆弱性識別子(CVE)</a> は一般的に公開されている情報セキュリティの脆弱性のリストで、脆弱性の種類を特定し追跡するために国際的に使用されています。
継続的インテグレーション/ 継続的デリバリ (CI/CD)	ビルド、テスト、デプロイにおいて継続的な繰返しと自動化を促進するアジャイルの実践を指します。
攻撃	<a href="#">攻撃 (603ページ)</a> は、一定の時間内に発生する 1 つまたは複数の攻撃イベントで構成されます。
攻撃イベント	攻撃イベントとは、Contrast エージェントが組み込まれたアプリケーションにおいて、Protect ルールへの違反やその他の疑わしいアプリケーションアクティビティのことです。イベントは、HTTP リクエストや SQL クエリなどの単一の攻撃ベクトルに該当します。複数の攻撃イベントが 1 つの攻撃を構成しますが、通常は同じコード領域と同じ時間枠内で発生します。
最高情報セキュリティ責任者 (CISO)	最高情報セキュリティ責任者(CISO、Chief Information Security Officer)は、組織の情報セキュリティ対策を指揮し、機密資産が十分に保護されていること、スタッフが脆弱性を管理・防止できることを保証し、実証します。
修復済	<a href="#">ライブラリ</a> のステータスとして、脆弱なライブラリに対応・対策済であることを表します。



静的アプリケーションセキュリティテスト (SAST)	アプリケーションをインストールや実行せずに、アプリケーションに潜在する脆弱性を検出する手法。
報告済	ライブラリのステータスとして、脆弱性のあるライブラリが Contrast で検出された場合のデフォルトステータスです。
未使用の関数	シャドウ関数とも呼ばれます。90 日以上呼び出されていないクラウド環境上の関数です。
問題無し	ライブラリのステータスとして、このライブラリにある脆弱性は認識済みであり、そのリスクは許容できるものを表します。

## ロールと権限

ユーザには、割り当てられたロールに応じて権限と機能が付与されます。ロールは、[アプリケーション \(817ページ\)](#)レベルと[組織 \(819ページ\)](#)レベルで、そして(オンプレミス版のお客様の場合は)[システム \(821ページ\)](#)レベルで設定されます。これらのロールの多くは、ユーザが[アクセスグループ \(708ページ\)](#)に割り当てられたときに定義されます。

また、以下が可能です。

- [自分の権限の確認 \(480ページ\)](#)
- [組織の権限の管理 \(708ページ\)](#)
- [システム権限の管理 \(772ページ\)](#)
- [Protect 権限の付与 \(780ページ\)](#)



### 注記

API のみのユーザは、Contrast の REST API にはアクセスできますが、ユーザインターフェイスにはログインできません。Contrast では、API の管理者アカウントの作成を推奨していません。

## アプリケーションロール

アプリケーションロールは、特定のアプリケーション内で権限や機能をユーザに与えるものです。組織ロールに加えて、アプリケーションロールを定義して、アプリケーションに対するユーザ権限をより細かく制御します。アプリケーションロールは、[アクセスグループ \(708ページ\)](#)に割り当てます。

以下のアプリケーションロールを使用して、アプリケーション内の権限と機能を付与します。

**View**

アプリケーションの View ロール(アプリケーションの閲覧者)は、Contrast インターフェイスに読み取り専用でアクセスできます。アプリケーション情報の編集はできず、スコア、ライブラリ、脆弱性およびコメントなどを参照するのみに制限されます。

**Viewの権限詳細 (アプリケーション)**

アプリケーション

- Archive
- Delete
- Edit
- License
- Merge
- Reset
- Restore
- Tag
- View

脆弱性

- Delete
- Discussion
- Edit
- Export
- HTTP Replay
- Merge
- Send to Bugtracker
- Tag
- View

ライブラリ

- Manifest
- Tag
- View

ポリシー

- Edit
- View

例外

- Create
- View

レポート

- Generate

アーキテクチャ

- View

完了

**Edit**

アプリケーションの Edit ロール(アプリケーションの編集者)は、検出結果の対策、タグの追加、脆弱性の管理、属性の編集、アプリケーションのマージ、アプリケーションの追加・削除、サーバの登録などが可能です。Contrast 利用者の大半に割り当てるのが、このロールです。

**Editの権限詳細 (アプリケーション)**

アプリケーション

- Archive
- Delete
- Edit
- License
- Merge
- Reset
- Restore
- Tag
- View

脆弱性

- Delete
- Discussion
- Edit
- Export
- HTTP Replay
- Merge
- Send to Bugtracker
- Tag
- View

ライブラリ

- Manifest
- Tag
- View

ポリシー

- Edit
- View

例外

- Create
- View

レポート

- Generate

アーキテクチャ

- View

完了

**Rules Admin**

アプリケーションの Rules Admin ロール(アプリケーションのルール管理者)は、Edit ロールの機能に加えて、ルールの編集ができます。アプリケーションのルールやポリシーの編集、Protectの有効化、アプリケーションに関する通知やスコア付けの管理などができます。

**Rules Adminの権限詳細 (アプリケーション)** ×

アプリケーション	脆弱性	ライブラリ	ポリシー
<input checked="" type="checkbox"/> Archive	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Manifest	<input checked="" type="checkbox"/> Edit
<input type="checkbox"/> Delete	<input checked="" type="checkbox"/> Discussion	<input checked="" type="checkbox"/> Tag	<input checked="" type="checkbox"/> View
<input type="checkbox"/> Edit	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> View	
<input type="checkbox"/> License	<input checked="" type="checkbox"/> Export		<b>例外</b>
<input checked="" type="checkbox"/> Merge	<input checked="" type="checkbox"/> HTTP Replay	<b>レポート</b>	<input checked="" type="checkbox"/> Create
<input type="checkbox"/> Reset	<input checked="" type="checkbox"/> Merge	<input checked="" type="checkbox"/> Generate	<input checked="" type="checkbox"/> View
<input checked="" type="checkbox"/> Restore	<input checked="" type="checkbox"/> Send to Bugtracker		
<input checked="" type="checkbox"/> Tag	<input checked="" type="checkbox"/> Tag	<b>アーキテクチャ</b>	
<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> View	

完了

---

**Admin**

アプリケーションの Admin ロール(アプリケーション管理者)には制限がなく、他のユーザのアプリケーションへのアクセスを管理できます。

**Adminの権限詳細 (アプリケーション)** ×

アプリケーション	脆弱性	ライブラリ	ポリシー
<input checked="" type="checkbox"/> Archive	<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Manifest	<input checked="" type="checkbox"/> Edit
<input checked="" type="checkbox"/> Delete	<input checked="" type="checkbox"/> Discussion	<input checked="" type="checkbox"/> Tag	<input checked="" type="checkbox"/> View
<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> Edit	<input checked="" type="checkbox"/> View	
<input checked="" type="checkbox"/> License	<input checked="" type="checkbox"/> Export		<b>例外</b>
<input checked="" type="checkbox"/> Merge	<input checked="" type="checkbox"/> HTTP Replay	<b>レポート</b>	<input checked="" type="checkbox"/> Create
<input checked="" type="checkbox"/> Reset	<input checked="" type="checkbox"/> Merge	<input checked="" type="checkbox"/> Generate	<input checked="" type="checkbox"/> View
<input checked="" type="checkbox"/> Restore	<input checked="" type="checkbox"/> Send to Bugtracker		
<input checked="" type="checkbox"/> Tag	<input checked="" type="checkbox"/> Tag	<b>アーキテクチャ</b>	
<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> View	<input checked="" type="checkbox"/> View	

完了

**No Access** ロールは、アプリケーションへのユーザアクセスをブロックします。

アプリケーションロールの追加は、[組織のアクセスグループの作成または編集 \(708ページ\)](#)で行います。

## 関連項目

[権限の表示 \(480ページ\)](#)

## 組織ロール

組織ロールは、ユーザが所属する組織内のアクセスを制御するものです。ユーザには、組織によって異なるロールを割り当てることができます。

全てのユーザに、デフォルトの組織のデフォルトロールを指定します。

組織ロールは以下のとおりです。

リファレンス

819

**View**

組織の View ロール(組織の閲覧者)は、Contrast インターフェイスに読み取り専用でアクセスできます。アプリケーション情報の編集はできず、スコア、ライブラリ、脆弱性およびコメントなどを参照するのみに制限されます。

**Viewの権限詳細 (組織)** ✕

**概要**

- Org Info
- Report Settings
- Score Settings

**サーバ**

- Delete
- Edit
- License
- Tag
- View

**セキュリティ**

- Audit
- Get API Keys
- IP Range
- Rotate API Keys
- Password Policy
- Session Timeouts

**インテグレーション**

- Edit
- View

**ライブラリ**

- Manifest
- Tag
- View

**ポリシー**

- App Exclusions
- Assess Rules
- Library Policy
- Protection Policy
- Remediation Policy

完了

**Edit**

組織の Edit ロール(組織の編集者)は、検出結果の対策、タグの追加、脆弱性の管理、属性の編集、アプリケーションのマージ、アプリケーションの追加・削除、サーバの登録などが可能です。Contrast 利用者の大半に割り当てるのが、このロールです。

**Editの権限詳細 (組織)** ✕

**概要**

- Org Info
- Report Settings
- Score Settings

**サーバ**

- Delete
- Edit
- License
- Tag
- View

**セキュリティ**

- Audit
- Get API Keys
- IP Range
- Rotate API Keys
- Password Policy
- Session Timeouts

**インテグレーション**

- Edit
- View

**ライブラリ**

- Manifest
- Tag
- View

**ポリシー**

- App Exclusions
- Assess Rules
- Library Policy
- Protection Policy
- Remediation Policy

完了

**Rules Admin**

組織の Rules Admin ロール(組織のルール管理者)は、組織レベルでルールやポリシーを管理できます。また、Protectの有効化、アプリケーションに関する通知やスコア付けの管理ができます。

**Rules Adminの権限詳細 (組織)** ×

<p><b>概要</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Org Info</li> <li><input type="checkbox"/> Report Settings</li> <li><input checked="" type="checkbox"/> Score Settings</li> </ul> <hr/> <p><b>サーバ</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Delete</li> <li><input type="checkbox"/> Edit</li> <li><input type="checkbox"/> License</li> <li><input checked="" type="checkbox"/> Tag</li> <li><input checked="" type="checkbox"/> View</li> </ul>	<p><b>セキュリティ</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Audit</li> <li><input checked="" type="checkbox"/> Get API Keys</li> <li><input type="checkbox"/> IP Range</li> <li><input type="checkbox"/> Rotate API Keys</li> <li><input type="checkbox"/> Password Policy</li> <li><input type="checkbox"/> Session Timeouts</li> </ul> <hr/> <p><b>インテグレーション</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Edit</li> <li><input type="checkbox"/> View</li> </ul>	<p><b>ライブラリ</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Manifest</li> <li><input checked="" type="checkbox"/> Tag</li> <li><input checked="" type="checkbox"/> View</li> </ul> <hr/> <p><b>ポリシー</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> App Exclusions</li> <li><input checked="" type="checkbox"/> Assess Rules</li> <li><input checked="" type="checkbox"/> Library Policy</li> <li><input checked="" type="checkbox"/> Protection Policy</li> <li><input checked="" type="checkbox"/> Remediation Policy</li> </ul>
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

完了

**Admin**

組織の Admin ロール(組織管理者)は、組織の設定と管理を行います。

**Adminの権限詳細 (組織)** ×

<p><b>概要</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Org Info</li> <li><input checked="" type="checkbox"/> Report Settings</li> <li><input checked="" type="checkbox"/> Score Settings</li> </ul> <hr/> <p><b>サーバ</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Delete</li> <li><input checked="" type="checkbox"/> Edit</li> <li><input checked="" type="checkbox"/> License</li> <li><input checked="" type="checkbox"/> Tag</li> <li><input checked="" type="checkbox"/> View</li> </ul>	<p><b>セキュリティ</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Audit</li> <li><input checked="" type="checkbox"/> Get API Keys</li> <li><input checked="" type="checkbox"/> IP Range</li> <li><input checked="" type="checkbox"/> Rotate API Keys</li> <li><input checked="" type="checkbox"/> Password Policy</li> <li><input checked="" type="checkbox"/> Session Timeouts</li> </ul> <hr/> <p><b>インテグレーション</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Edit</li> <li><input checked="" type="checkbox"/> View</li> </ul>	<p><b>ライブラリ</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> Manifest</li> <li><input checked="" type="checkbox"/> Tag</li> <li><input checked="" type="checkbox"/> View</li> </ul> <hr/> <p><b>ポリシー</b></p> <ul style="list-style-type: none"> <li><input checked="" type="checkbox"/> App Exclusions</li> <li><input checked="" type="checkbox"/> Assess Rules</li> <li><input checked="" type="checkbox"/> Library Policy</li> <li><input checked="" type="checkbox"/> Protection Policy</li> <li><input checked="" type="checkbox"/> Remediation Policy</li> </ul>
-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

完了

組織ロールは、[組織のアクセスグループにユーザを追加 \(708ページ\)](#)することで割り当てられます。

## 関連項目

[権限の表示 \(480ページ\)](#)

## システムロール



### 注記

システムロールは、オンプレミス版のお客様のみが利用できます。

どのようにシステム管理を行う ([772ページ](#))かを決める際に、システムロールを使用して権限や機能を割り当てることができます。

- **SuperAdmin** : スーパー管理者。オンプレミス版インスタンスのインストールと設定を担当します。このロールは、Contrast のシステム管理も担当するものにもなりますが、1人以上の管理者に割り当てることができます。**SuperAdmin** は、組織、アプリケーション、サーバ、脆弱性、ユーザ、グループを設定できます。
- **ServerAdmin** : サーバ管理者。ユーザやグループにアクセスできない以外は、SuperAdmin と同じです。ユーザメニューの **ServerAdmin** オプションを利用し、組織、アプリケーション、サーバおよび脆弱性を設定できます。
- **SystemAdmin** : システム管理者。組織やグループの管理を担当します。ユーザメニューの **SuperAdmin** オプションを利用し、組織、アプリケーション、サーバ、脆弱性、ユーザおよびグループを設定できます。
- **Observer** : システムのオブザーバ。組織、ユーザ、アプリケーション、グループ、およびトレースの読み取り専用権限があります。ユーザメニューの **Observer** オプションで読み取り専用アクセスを利用し、組織、アプリケーション、サーバ、脆弱性、ユーザを参照できます。
- **No Access** : アクセス権なし。このロールは、指定の組織へのユーザのアクセスをブロックします。

## アプリケーションのスコアガイド

Contrast では、アプリケーションは文字で表したグレードでスコア付けされ、アプリケーションの全体的な評価を把握するのに役立ちます。

アプリケーションのスコアは、アプリケーションがどれだけ疎通されているかによりますが、アプリケーションで検出された脆弱性の数と深刻度に基づき算出されます。

算出されたスコアはグレード(A から F の文字)に置き換えられて、Contrast で表示されます。

- **A** : 90-100
- **B** : 80-89
- **C** : 70-79
- **D** : 60-69
- **F** : 35-59

アプリケーションのスコアの算出には、アプリケーションの [ライブラリのスコア \(544ページ\)](#) とカスタムコードのスコアの平均を求めます。

カスタムコードのスコアの算出は 100 点から始まり、アプリケーションで検出された脆弱性の数に、以下に示す深刻度に応じたペナルティの重み付けを掛けたペナルティ点数が差し引かれます。

- **重大** : 脆弱性の数×20
- **高** : 脆弱性の数×10
- **中** : 脆弱性の数×5
- **低** : 脆弱性の数×1

脆弱性の重み付けは、悪用される可能性やその影響の深刻さにより異なります。

例えば、SQL インジェクションは、専門知識が無くても悪用できる自動化ツールなどが存在するため、深刻度を **重大** としています。アプリケーションやスキーマについて何も知らない攻撃者が、データベースの全ての内容を盗み出せる可能性があります。

一方、SHA-1 などのハッシュアルゴリズムの使用は、深刻な弱点があることで知られているため、**低リスク** と見なされます。また、実際に悪用するには、組織や国家レベルでの大規模な支援のもと、非常に熟練した攻撃者のリソースが必要です。



## ヒント

アプリケーションのスコアの算出例：

まず、カスタムコードのスコアを決定します。アプリケーションの脆弱性が、**重大**が 0、**高**が 1、**中**が 2、**低**が 1 だった場合、カスタムコードのスコアは以下のようになります。

$$100 - (20 \times 0) - (10 \times 1) - (5 \times 2) - (1 \times 1) = 79$$

ライブラリのスコアが 85、カスタムコードのスコアが 79 のアプリケーションの場合、アプリケーションのスコアは 82 となり、B という評価になります。

$$85 + 79 = 164$$

$$164 / 2 = 82$$

スコアを改善するには：

- CVE シールドや **Protect ルールを有効 (680ページ)** にして、防御した脆弱性をスコアの計算から除きます。
- カスタムコードに存在する **重大・高** リスクの脆弱性を修正します。
- 脆弱なライブラリに対処します。
- **高** リスクのライブラリを更新します。

## ライブラリのスコアガイド

Contrast では、アプリケーションのライブラリの安全性を文字で表したグレードで提供し、分析時の目安として使用することができます。以下のとおり、スコアをグレード(A から F の文字)に置き換えます。

- A : 90 - 100
- B : 80 - 89
- C : 70 - 79
- D : 60 - 69
- F : 35 - 59

スコアは、次の 3 つのペナルティ要素に基づきます。

- **時間**：ライブラリの古さです。アプリケーションで使用されているバージョンのリリース日から最新バージョンのリリース日までの年数に、2.5 を掛けた数が減算されます。
- **ステータス**：ステータスは、ライブラリの日付以降のバージョン数です。アプリケーションの現在のライブラリ以降にリリースされたバージョンの数に、10 を掛けた数が減算されます。
- **セキュリティ**：ライブラリに影響を与える CVE 数です。ライブラリの CVE ペナルティは、このライブラリの全ての既知の CVE の中で最も高い深刻度に、10 を掛けた数が減算されます。



## 注記

組織の管理者は、セキュリティ要素のみを対象とするよう **スコアの設定方法を調整 (719ページ)** できます。



## ヒント

例：

2010年1月にリリースされたライブラリを使用していて、最新版が2013年9月にリリースされた場合は、経過した年数は2となります。そのため、時間のペナルティは次のようになります。

$$2 \times 2.5 = 5$$

バージョン1.1.1を使用しているが、バージョン1.1.2と1.1.3がリリースされている場合は、ペナルティは次のようになります。

$$2 \times 10 = 20$$

セキュリティのスコアに2.4と2.2があるライブラリがある場合、ペナルティは次のようになります。

$$2.4 \times 10 = 24$$

ライブラリの最終的なスコアは、3つのペナルティそれぞれの値を100から引くことによって計算されます。

$$100 - 5 - 20 - 24 = 51$$

51のスコアには、「F」という文字が評価として割り当てられます。

## ログレベル

ログレベルの設定により、サーバのログ出力で処理されるイベントを制御でき、イベントをより効果的に取得できます。ログレベルは[システムレベルで設定 \(766ページ\)](#)できるほか、Edit権限を持つユーザーが[特定のサーバ \(530ページ\)](#)に対して設定できます。

ログレベルは、Log4jに準拠し、可能な限りLog4jのレベル指定に沿っています。

デフォルト値はINFOです。問題が発生してより詳細なデータ収集が必要にならない限り、ほとんどの場合はERRORレベルで十分です。

ログレベル	説明
ERROR	対処する必要がある、不安定な状態を招く恐れのある深刻なエラーに関する情報を提供します。
WARN	予期しないイベントについて、ユーザーに警告します。このレベルで発生するメッセージでは、システムの進行が停止しない場合があります。
INFO	進捗と設定された状態についての情報を提供します。このレベルはエンドユーザーにとって便利です。
DEBUG	開発者がアプリケーションをデバッグするのに役立ちます。記録されるメッセージのレベルは、アプリケーション開発者にサポートを提供することに重点が置かれています。
TRACE	DEBUGレベルよりも詳細な情報を提供します。

## イベントと Generic Webhook 変数

NEW\_VULNERABILITY や SERVER\_OFFLINE などの Contrast のイベントからのデータを使って、[Generic Webhook \(639ページ\)](#)のレスポンスをカスタマイズできます。各イベントには、[共通 \(641ページ\)](#)変数、[アプリケーション \(642ページ\)](#)変数、[サーバ \(642ページ\)](#)変数、または[脆弱性 \(642ページ\)](#)変数があり、ペイロードのリクエストで呼び出すことができます。

イベント	変数
ATTACK_END	<a href="#">共通 (641ページ)</a> 、 <a href="#">アプリケーション (641ページ)</a> 、 <a href="#">サーバ (642ページ)</a>



イベント	変数
ATTACK_EVENT_COMMENT	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)
ATTACK_UPDATE	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)
EXPIRING_LICENSE	共通 (641ページ)、アプリケーション (642ページ)
NEW_ASSET (新規アプリケーションの場合)	共通 (641ページ)、アプリケーション (642ページ)およびサーバ (642ページ)(新規アプリケーションの場合)
NEW_ATTACK_APPLICATION	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)
NEW_ATTACK_UPDATE	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)
NEW_ATTACK	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)
NEW_VULNERABILITY_COMMENT	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)、脆弱性 (642ページ)
NEW_VULNERABILITY	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)、脆弱性 (642ページ)
NEW_VULNERABLE_LIBRARY	共通 (641ページ)、アプリケーション (642ページ)
SERVER_OFFLINE	共通 (641ページ)、サーバ (642ページ)
VULNERABILITY_CHANGESTATUS_CLOSED	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)、脆弱性 (642ページ)
VULNERABILITY_CHANGESTATUS_OPEN	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)、脆弱性 (642ページ)
VULNERABILITY_DUPLICATE	共通 (641ページ)、アプリケーション (642ページ)、サーバ (642ページ)、脆弱性 (642ページ)

## Generic Webhook の変数

NEW\_VULNERABILITY や SERVER\_OFFLINE などの Contrast イベントからのデータを使用して、[Generic Webhook \(639ページ\)](#)のレスポンスをカスタマイズできます。各イベントには、ペイロードのリクエストで呼び出すことができる変数があります。変数には、一般的な共通情報として利用するもの、もしくは、アプリケーション用、サーバ用、脆弱性用があります。

変数	説明
<b>共通変数</b>	
\$EventType	Webhook のトリガーとなるイベントタイプ 例：SERVER_OFFLINE
\$Message	Webhook のトリガーとなったイベントの概要を表すメッセージ
\$OrganizationId	Contrast で組織の作成時に、組織に割り当てられた一意の ID
\$OrganizationName	組織の名前
\$Title	常に“Contrast Security”を返す
<b>アプリケーション変数</b>	
\$ApplicationChild	アプリケーションが子アプリケーションの場合は真(true)を返し、そうでない場合は偽(false)を返す
\$ApplicationCode	アプリケーションのタイトルに表示されるアプリケーション名の省略形、デフォルトでは空白 例：TEST
\$ApplicationContextPath	アプリケーションのコンテキストパス 例：/example/somethingelse
\$ApplicationFirstSeen	アプリケーションが最初に検知された日時(Unix 時間) 例：1572033840000
\$ApplicationHasParentApp	アプリケーションに親がある場合は真(true)を返し、そうでない場合は偽(false)を返す
\$ApplicationImportance	アプリケーションの重要度の列挙値(enum 値) 例：MEDIUM
\$ApplicationId	Contrast でアプリケーションの登録時に、アプリケーションに割り当てられた一意の ID 例：49fe2978-1833-4441-83db-2b70486d9413

変数	説明
\$ApplicationImportanceDescription	アプリケーションに割り当てられた重要度、例：Medium
\$ApplicationLanguage	アプリケーションのプログラミング言語
\$ApplicationLastSeen	アプリケーションが最後に検知された日時(Unix 時間)、例： 1572033840000
\$ApplicationLicenseLevel	アプリケーションに Assess ライセンスがあるかどうか、値： Licensed、Unlicensed
\$ApplicationMaster	アプリケーションがマスターアプリケーションである場合は真 (true)を返し、そうでない場合は偽(false)を返す
\$ApplicationName	アプリケーションの名前
\$ApplicationParentAppId	Contrast でアプリケーション(この場合は親アプリケーション)の 登録時に、アプリケーションに割り当てられた一意の ID(存在する 場合)  例：49fe2978-1833-4441-83db-2b70486d9413
\$ApplicationTags	アプリケーションのタグのカンマ区切りリスト
\$ApplicationTotalModules	アプリケーションにあるモジュールの数
<b>サーバ変数</b>	
\$Environment	サーバの環境、値：DEVELOPMENT、QA、PRODUCTION
\$ServerId	イベントに関与しているサーバの ID  複数サーバが関与している場合、カンマ区切りのサーバ ID リスト
\$ServerName	イベントに関与しているサーバの名前  複数サーバが関与している場合、カンマ区切りのサーバ名リスト
<b>脆弱性変数</b>	
\$Severity	イベントのトリガーが脆弱性の場合、脆弱性の深刻度を返す
\$Status	イベントのトリガーが脆弱性の場合、脆弱性のステータスを返す
\$TraceId	イベントのトリガーが脆弱性の場合、脆弱性 ID を返す
\$VulnerabilityAgentLanguage	脆弱性が検知されたアプリケーションの言語またはフレームワー ク名(例：.Java、.NET、Ruby など)
\$VulnerabilityAppVersionTags	脆弱性が検出されたアプリケーションのバージョン  例：v1.2.3
\$VulnerabilityAutoRemediatedExpirationPeriod	脆弱性が自動修復される有効期間(Unix 時間)  例：1572033840000
\$VulnerabilityBugTrackerTickets	脆弱性情報がバグ管理システムに送信されて、作成されたチケッ トのリスト(カンマ区切り)  例：ticket1、ticket2、ticket3
\$VulnerabilityCategory	検出された脆弱性のカテゴリー、例：Injection
\$VulnerabilityClosedTime	脆弱性がクローズされた日時(Unix 時間)  例：1572033840000
\$VulnerabilityConfidence	脆弱性の信頼度
\$VulnerabilityDefaultSeverity	脆弱性のデフォルトの深刻度
\$VulnerabilityDiscovered	脆弱性が最初に検出された日時(Unix 時間)  例：1572033840000
\$VulnerabilityEvidence	脆弱性のエビデンス
\$VulnerabilityInstanceUuid	Contrast で脆弱性インスタンスの作成時に、脆弱性インスタ ンスに割り当てられた一意の ID  例：R33T-N00B-TGIF-RM6P
\$VulnerabilityFirstTimeSeen	脆弱性が最初に検出された日時(Unix 時間)、例：1572033840000
\$VulnerabilityImpact	脆弱性の影響度レベル、値：Low、Medium、High
\$VulnerabilityLastTimeSeen	脆弱性が最後に確認された日時(Unix 時間)、例：1572033840000
\$VulnerabilityInstanceLastTimeSeen	脆弱性が最後に確認された日時(Unix 時間)、例：1572033840000
\$VulnerabilityLicenseLevel	脆弱性のライセンスレベル

変数	説明
\$VulnerabilityLikelihood	脆弱性の可能性レベル 値：Low、Medium、High
\$VulnerabilityReportedToBugTracker	脆弱性がバグ管理システムに送信された日時(Unix 時間) 例：1572033840000
\$VulnerabilityReportedToBugTrackerTime	脆弱性がバグ管理システムに送信された場合、真(true)を返す
\$VulnerabilityRule	脆弱性に関連付けられたルール
\$VulnerabilityRuleName	脆弱性に関連付けられたルールの名前
\$VulnerabilityRuleTitle	脆弱性に関連付けられたルールのタイトル
\$VulnerabilitySubStatus	脆弱性のサブステータス
\$VulnerabilityTags	脆弱性に関連付けられたカスタムタグ 例：my-custom-tag
\$VulnerabilityTitle	脆弱性のタイトル
\$VulnerabilitySubStatusKeyCode	脆弱性サブステータスのキーコード
\$VulnerabilityTotalTracesReceived	脆弱性が受信された合計回数
\$VulnerabilityUuid	脆弱性を検索するために使用される一意の ID
\$VulnerabilityVisible	脆弱性にライセンスがあり参照可能である場合は真(true)を返し、そうでない場合は偽(false)を返す
\$VulnerabilityRule	イベントのトリガーが脆弱性の場合、脆弱性が違反したルールを返す
\$VulnerabilityTags	イベントのトリガーが脆弱性の場合、脆弱性に関連付けられたタグのリスト(カンマ区切り)を返す

## 正規表現リファレンス

アプリケーションの例外を追加 (692ページ) するには、以下の表と例を参考にしてください。

適用	パターン	パターン例	一致例
文字列の先頭	^	^w+	Start of a string
文字列の末尾	\$	w+\$	End of a string
後に続く文字列の大文字と小文字を区別しない一致	(?i)	(?i)%0a	%0a or %0A
a、b、または c の内の 1 文字	[abc]	[abc]+	a bb ccc
a、b、c 以外の文字	[^abc]	[^abc]+	Anythingbutabc.
a-z までの範囲内の 1 文字	[a-z]	[a-z]+	Only a-z
a-z までの範囲内でない 1 文字	[^a-z]	[^a-z]+	Anythingbuta-z.
a-z または A-Z の範囲内の 1 文字	[a-zA-Z]	[a-zA-Z]+	abc123DEF
任意の 1 文字	.	.+	abc
空白文字	\s	\s	anywhitespacecharacter
空白以外の文字	\S	\S+	any non-whitespace
10 進数字	\d	\d	not 1 not 2
10 進数字以外	\D	\D+	not 1 not 2
0 個または 1 個の a	a?	ba?	ba b a
0 個以上の a	a*	ba*	a ba baa aaa ba b
1 個以上の a	a+	a+	a aa aaa aaaa bab baab
ちょうど 3 個の a	a{3}	a{3}	a aa aaa aaaa
3 個以上の a	a{3,}	a{3,}	a aa aaa aaaa aaaaaa
3 個以上 6 個以下の a	a{3,6}	a{3,6}	a aa aaa aaaa aaaaaa aaaa
ピリオド(ドット)はリテラル文字	.	a.b	string.string

## 対応ブラウザ

Contrast は、HTML5 の Web ベースアプリケーションです。インターフェイスは React と AngularJS をベースにしています。最新のブラウザであれば、問題なく動作します。Contrast は、以下のブラウザの最新のメジャーバージョンでテストを行なっています。

- Chrome
- Edge
- Firefox
- Safari

Opera ブラウザまたは古いバージョンの Internet Explorer、Firefox、Safari ブラウザでも引き続き機能する場合がありますが、一部の機能は意図したとおりに表示されない可能性があります。

## Contrast ベータ版利用規約

Contrast のベータ版製品および機能について、次の利用条件を定めます。

- 本製品は現在開発中であり、継続的な改善を行っています。
- 弊社のベータ版製品は現状のまま提供され、いかなる保証もありません。
- ベータ版製品は開発中であるため、問題が発生する可能性があります。本番環境では、ベータ版を使用しないでください。
- 利用者は、ベータ版製品を使用するために、その他の規約への同意が必要になる場合があります。
- ベータプログラムは、新機能や拡張機能への早期アクセスを希望し、フィードバックの提供に同意頂けるお客様を対象としております。ベータ版製品に関するご意見、ご質問、不具合の報告は、[support@contrastsecurity.com](mailto:support@contrastsecurity.com) までご連絡ください。

## プライバシーとデータの収集

Contrast Security は、お客様がどのように弊社の製品を使用しているかを理解し、改善していくことが重要と考えております。この情報は、弊社が問題を解決し、不具合を修正するために役立っています。

情報は次の方法で収集されます。

- [システム診断 \(802ページ\)](#)
- [.NET Framework および .NET Core エージェントのテレメトリ \(194ページ\)](#)
- [Ruby エージェントのテレメトリ \(450ページ\)](#)
- [Python エージェントのテレメトリ \(392ページ\)](#)

収集されるデータは匿名で、アプリケーションのデータは含まれません。この情報は Contrast Security によって収集され、共有されることはありません。[Contrast Security のプライバシーポリシー](#)が適用されます。

お客様のプライバシーの保護は、弊社にとって重要です。弊社が機密データを収集していると思われる場合や、データの取り扱いが安全で無いか不適切であると思われる場合は、調査致しますので、[security@contrastsecurity.com](mailto:security@contrastsecurity.com) までメールにてご連絡ください。