Red Hat Subscription Management 2022

検出のインストールおよび設定

検出のインストール

Last Updated: 2022-10-16

Red Hat Subscription Management 2022 検出のインストールおよび設定

検出のインストール

Enter your first name here. Enter your surname here.
Enter your organisation's name here. Enter your organisational division here.
Enter your email address here.

法律上の通知

概要

目次

パート I. 検出について 3

第1章 検出とは 4

第2章 検出対象となる製品 5

第3章 検出が適切かどうか 6

パート II. 検出の前提条件のインストール 7

第4章 ハードウェアの前提条件 8

第5章 ソフトウェアの要件 9

第6章 その他の環境の前提条件 10

パート III. オンラインインストールプロセスによる検出のインストール 11

第7章 ANSIBLE および DISCOVERY-TOOLS の有効化およびインストール 12

第8章 オンラインインストールプロセスを使用したインストール 13
8.1. サーバーのインストール 13
8.2. コマンドラインインターフェイスのインストール 14

第9章 DISCOVERY-TOOLS INSTALL コマンドのオプション 15
9.1. サーバーのインストールオプション 15
9.2. コマンドラインインターフェイスのインストールオプション 16

パート IV. 検出の設定と維持 17

第10章 検出接続の設定 18

第11章 ネットワークスキャン用の検出サーバーに SSH キーを追加 19

パート V. 検出ユーザーインターフェイスへのアクセス 20

第12章 検出ユーザーインターフェイスへのログイン 21

第13章 検出ユーザーインターフェイスからログアウト 22

第14章 検出コマンドラインインターフェイスへのログイン 23

第15章 検出コマンドラインインターフェイスからのログアウト 24

パート I. 検出について

製品検出ツールは、特定の Red Hat ソフトウェアの使用に関するデータをユーザーが収集できるように設計されています。検出を使用すると、Red Hat 製品の使用状況を計算して報告するのに必要な時間と作業量を減らすことができます。

詳細情報

検出の目的、利点、および特長の詳細は、以下の情報を参照してください。

- 検出とは

検出が可能な製品および製品バージョンの詳細は、以下の情報を参照してください。

- 検出対象となる製品

検出が正しいソリューションであるかどうかを評価するには、以下の情報を参照してください。

- 検出が適切かどうか

第1章 検出とは

検出とも呼ばれる製品検出ツールは、検査およびレポートツールです。これは、ネットワーク上の物理システムと仮想システムの数、そのシステムのオペレーティングシステム、その他の設定データなどの環境データまたは事実を検出、識別、および報告するように設計されています。さらに、ネットワーク内の IT リソースの主要な Red Hat パッケージおよび製品の一部のバージョンについて、より詳細な事実を見つけ、特定し、報告するように設計されています。

ネットワーク上で実行中のソフトウェアおよびシステムを検査する機能は、エンタイトルメントの使用状況を把握して報告する機能を強化します。最終的に、この検査およびレポートプロセスは、インベントリーを管理する大規模なシステム管理タスクの一部となります。

プロダクト検出ツールでは、IT リソースにアクセスし、検査プロセスを実行するために、2 つの基本的な構造を設定する必要があります。**認証情報** は、特定のソースまたはそのソースの一部のアセットで検査プロセスを実行するための十分な権限を持つユーザーのユーザー名とパスワードまたは SSH キーなどのユーザーアクセスデータが含まれています。**ソース** には、検証される単一のアセットまたは複数のアセットに関するデータが含まれます。これらのアセットは、ホスト名、IP アドレス、IP 範囲、またはサブネットとして識別される物理マシン、仮想マシン、またはコンテナーです。これらのアセットは、vCenter Server や Red Hat Satellite Server などのシステム管理ソリューションです。

複数の認証情報およびソースを保存し、検査プロセスまたは **スキャン** の実行時にさまざまな組み合わせで検出と使用することができます。スキャンが完了したら、フォーマットされたデータ、または **report** のコレクションとして出力にあるこれらのファクトにアクセスし、結果を確認することができます。

デフォルトでは、検出の使用中に作成された認証情報およびソースはデータベースで暗号化されます。値は AES-256 暗号化で暗号化されます。検出サーバーは、Vault パスワードを使用してスキャンを実行してデータベースに保存されている暗号化された値にアクセスする際に復号化されます。

製品検出ツールはエージェントレス検査ツールであるため、検査されるすべてのソースにツールをインストールする必要はありません。ただし、検出がインストールされているシステムは、検出および検証されるシステムにアクセスできる必要があります。

第2章 検出対象となる製品

製品検出ツールは、以下の Red Hat 製品を見つけます。各バージョンまたはリリースについて、最も古いバージョンが一覧表示され、後続のリリースは該当と示されています。

製品の名前が最近変更されており、その製品の現在の名前をよく理解している場合は、その名前が追加情報として提供されます。また、製品の特定のバージョンも記載されない限り、新しいバージョンの製品名が含まれることはありません。

Red Hat Enterprise Linux

- Red Hat Enterprise Linux バージョン 5 以降
- Red Hat Enterprise Linux バージョン 6 以降
- Red Hat Enterprise Linux バージョン 7 以降
- Red Hat Enterprise Linux バージョン 8 以降

Red Hat ミドルウェア製品

- Red Hat JBoss BRMS バージョン 5.0.1 以降、バージョン 6.0.0 以降 (現在の製品名は Red Hat Decision Manager)
- JBoss Enterprise Web Server バージョン 1 以降、バージョン 2.0 以降、バージョン 2.1.0 以降、Red Hat JBoss Web Server 3.0.1 以降、バージョン 3.1 以降、バージョン 5.0.0
- Red Hat JBoss Enterprise Application Platform バージョン 4.2 以降、バージョン 4.3 以降、バージョン 5 以降、バージョン 6 以降、バージョン 7
- Red Hat Fuse バージョン 6.0 以降、バージョン 6.1 以降、バージョン 6.2 以降、バージョン 6.3.0

第3章 検出が適切かどうか

製品検出ツールは、複雑なネットワーク全体での未知の製品の使用状況など、Red Hat 製品のインベントリーを見つけて理解できるように支援することを目的としています。検出によって生成されたレポートは、Red Hat Solution Architect (SA) または Technical Account Manager (TAM) とのパートナーシップ、または Subscription and Awareness Program (SEAP) が提供する分析およびサポートを解することで、理解を深めることができます。現在進行中のパイロットプログラムには、ソフトウェアインベントリーを他の新しく確立された Red Hat 管理製品と統合するのに役立つ 1 つのツールとしての検出が含まれています。

個別に検出をインストールして使用し、レポートデータを生成して表示できますが、検出ドキュメントではレポート結果の解釈に役立つ情報は提供していません。さらに、Red Hat サポートは製品検出ツールのインストールおよび使用方法に関する基本的なサポートを提供しますが、サポートチームはお客様がレポートを理解できるようにサポートするわけではありません。段階的パイロットプログラムは、Red Hat 製品のプロファイルおよびその他の要因に基づいて認証を得る Red Hat のお客様のサブセットを対象に設計されています。このようなパイロットプログラムは、レポート情報の取り込み、レンダリング、分析、および使用状況を管理ソリューションの一部として改良し、オンプレミス、クラウド、またはコンテナーのいずれかの環境全体で製品インベントリーを理解するのに役立ちます。

パート II. 検出の前提条件のインストール

インストールプロセスを開始する前に、検出の前提条件に関する情報を確認してください。次に、前提条件のインストールタスクまたは設定タスクを実行します。

手順

検出をインストールして使用するハードウェア、ソフトウェア、および環境には、以下の要件をインストールします。

第4章 ハードウェアの前提条件

検出をインストールするシステムが、以下のハードウェア要件を満たしているか、それを超える必要があります。

- **CPU:** 2 コア以上、4 コア推奨
- **ディスクストレージ :** 30 GB
- **RAM:** 1 GB 以上、2 GB 推奨

第5章 ソフトウェアの要件

検出をインストールするシステムには、以下のソフトウェア要件がインストールされている必要があります。

- **オペレーティングシステム**: 以下のオペレーティングシステムバージョンの最新リリース
  - Red Hat Enterprise Linux 8

これらのソフトウェア要件に加えて、検出には他のソフトウェアへの依存関係があります。ただし、インストール中にこれらの依存関係がインストールされている場合や、インストールの手順は検出インストールプロセスの一部として統合されている場合があります。依存関係をインストールするプロセスは、オペレーティングシステムや、オフラインインストールまたはオンラインインストールを行うかどうかなど、さまざまな要素によって異なる場合があります。したがって、検出インストール手順の指示どおりに依存関係をインストールします。

検出の依存関係には、以下のソフトウェアが含まれます。

- Ansible 2.4 以降 (オペレーティングシステムの要件によって異なります)。
- Podman コンテナーソフトウェア。
- PostgreSQL データベース。
- オペレーティングシステムの要件に応じて、Python 3.4 または 3.6。

第6章 その他の環境の前提条件

検出を使用する環境は、以下の要件を満たす必要があります。これらの要件の一部は、検出を実行するシステムに影響します。その他は、検出でスキャンする IT インフラストラクチャーのシステムに影響します。

検出がインストールされているマシンで以下を行います。

- 検出サーバーおよび CLI パッケージを異なるマシンにインストールする場合は、各インストールを実行するために両方のマシンに discovery-tools をインストールする必要があります。
- 検出サーバーおよび CLI パッケージを別のマシンにインストールする場合、CLI マシンはサーバーマシンに接続できるようにする必要があります。
- 検出サーバーは、スキャンされる IT インフラストラクチャーアセットにアクセスできる必要があります。

検出がスキャンされるシステムで、以下を行います。

- スキャンをターゲットとするネットワークソースは、Secure Shell (SSH) プロトコルを実行している必要があります。
- スキャンの認証情報として使用されるユーザーアカウントには、**bash** シェルが必要です。シェルは、**/sbin/nologin** シェルまたは **/bin/false** シェルは使用できません。
- ネットワークスキャンの認証情報として使用されるユーザーアカウントには、これらのシステムでコマンドを実行し、特定のファイルを読み取りするための適切な権限が必要です。たとえば、スキャン中に実行するコマンドによっては、スキャンのファクトをすべて収集するために特権の昇格が必要になります。**製品検出の使用**ガイドには、ネットワークスキャン用の認証情報の作成に関する追加情報と、ネットワークアセットのより完全なスキャンを可能にするためにこれらの認証情報に関連する権限が記載されています。
- SSH キーで認証を行うネットワークスキャンの認証情報として使用されるユーザーアカウントには、検出サーバーの秘密鍵のコピーが必要です。秘密鍵は、サーバーのインストール時にこのディレクトリーのデフォルトの場所である **~/discovery/server/volumes/sshkeys** ディレクトリーに保存する必要があります。

パート III. オンラインインストールプロセスによる検出のインストール

オンラインインストールプロセスでは、Ansible を使用してコマンドラインインターフェイスツール、サーバーイメージ、およびデータベースイメージをインストールするインストーラーを実行します。

オンラインインストールプロセスを実行すると、サーバーパッケージおよび CLI パッケージがデフォルトのオプションとともにインストールされます。ただし、インストールプロセスで使用されるデフォルトの一部を変更するには、discovery-tools install コマンドの Options で定義したオプションを設定します。

前提条件

- すべての前提条件がインストールされ、設定されていることを確認してください。
- オンラインインストールプロセスを使用するには、インストーラーをダウンロードし、検出をインストールするマシンがインターネットに接続されている必要があります。

手順

オンラインインストールプロセスで検出をインストールするには、以下の作業を行います。

1. Ansible リポジトリーおよび discovery-tools リポジトリーを有効にし、discovery-tools をインストールします。詳細は Ansible および discovery-tools の有効化およびインストール を参照してください。
2. discovery-tools で検出インストールを実行します。詳細は、オンラインインストールプロセスを使用したインストール を参照してください。

注記

このインストールプロセスでは、すべてのオプションのデフォルト設定で検出がインストールされます。ただし、その他の設定を使用してインストールをカスタマイズできます。これらの設定の詳細は、discovery-tools install コマンドのオプション を参照してください。

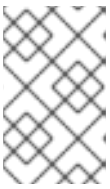
第7章 ANSIBLE および DISCOVERY-TOOLS の有効化およびインストール

discovery-tools パッケージには、検出のインストールおよび維持に使用するツールが含まれます。

discovery-tools インストールプロセスは、Ansible Playbook と統合してインストールを完了します。したがって、Ansible バージョン 2.4 以降 (オペレーティングシステムの要件によります) は discovery-tools の依存関係です。インストールプロセスの一環として、discovery-tools は Ansible をインストールしますが、Ansible に必要なリポジトリーを手動で有効にする必要があります。

手順

1. RHEL Ansible Engine リポジトリーを有効にします。この手順の詳細は、Red Hat Ansible Engine のダウンロードおよびインストール方法の Ansible の限定サポートバージョンのリポジトリーを有効にする手順を参照してください。カスタマーポータルの記事 (https://access.redhat.com/articles/3174981)。Ansible の詳細情報は、https://docs.ansible.com/#coreversionselect を参照してください。

   注記

   このリンクの手順には、Ansible をインストールするステップが含まれます。discovery-tools は Ansible をインストールするため、Ansible をインストールするコマンドを実行する必要はありません。

2. システムを Red Hat Subscription Manager に登録します。

   ```
   # subscription-manager register
   ```

3. 以下のコマンドを使用して、検出サブスクリプションを見つけ、サブスクリプションのプール ID を書き留めます。

   ```
   # subscription-manager list --available
   ```

4. サブスクリプションを割り当てます。**pool_ID** は検出サブスクリプションのプール ID です。

   ```
   # subscription-manager attach --pool=pool_ID
   ```

5. 検出リポジトリーを有効にします。

   ```
   # subscription-manager repos --enable discovery-0-for-rhel-8-x86_64-rpms
   ```

6. discovery-tools をインストールします。

   ```
   # yum install discovery-tools
   ```

第8章 オンラインインストールプロセスを使用したインストール

検出インストールプロセス時に、コマンドを入力してサーバーとコマンドラインインターフェイス (CLI) をインストールします。検出をインストールする最も簡単な方法は、すべてのデフォルトオプションを指定してオンラインインストールを実行することです。この方法では、インストールプロセスにより、以下のアクションの実行が求められます。

- Red Hat Container Catalog のユーザー名およびパスワードを入力します。
- 検出サーバー管理者のパスワードを設定します。
- データベースユーザーのパスワードを設定します。

以下の情報には、デフォルトのインストールプロセスのコマンドが含まれます。ただし、インストールプロセスで使用されるデフォルトの一部を変更するには、discovery-tools install コマンドの Options で定義したオプションを設定します。

手順

検出サーバーおよび CLI パッケージをインストールするには、以下の手順に従います。

8.1. サーバーのインストール

サーバーをインストールします。デフォルトのサーバーインストールプロセスでは、Red Hat Container Catalog (registry.redhat.io Web サイト) のユーザー名とパスワードを入力するように求められます。また、検出サーバー管理者のパスワードと、PostgreSQL データベースユーザーのパスワードを入力するように求められます。

重要

ベストプラクティスとして、組織が使用するパスワード管理システム内の検出サーバー管理者と PostgreSQL データベースユーザーパスワードに注意してください。製品検出ツールは、これらのパスワードを復元する方法を提供しません。

さらに、後で discovery-tools を使用して検出をアップグレードする場合は、アップグレード中に同じデータベースのユーザー名とパスワードを使用する必要があります。同じデータベース認証情報を使用しないと、データが失われる可能性があります。

1. 以下のコマンドを入力してサーバーをインストールします。

```
# dsc-tools server install
```

2. プロンプトで、registry.redhat.io イメージレジストリーの Web サイトとして知られる Red Hat Container Catalog のユーザー名を入力します。
3. プロンプトで、Red Hat Container Catalog のパスワードを入力します。
4. プロンプトで、検出サーバー管理者のパスワードを設定します。
5. プロンプトで、PostgreSQL データベースユーザーのパスワードを設定します。

検証手順

1. server パッケージのインストールに成功すると、以下のような出力が表示されます。

```
Installation of the server was successful.
```

8.2. コマンドラインインターフェイスのインストール

コマンドラインインターフェイスをインストールします。

検出サーバーのポートおよび IP アドレスを設定するオプションを追加することが推奨されます。検出コマンドラインインターフェイスがサーバーと通信できるように、このオプションを設定する必要があります。

1. 以下のコマンドを入力してコマンドラインインターフェイスをインストールします。**server_port** は検出サーバーが通信に使用するポートで、**server_host** はサーバーの IP アドレスに置き換えます。

```
# dsc-tools cli install --server-port=server_port --server-host=server_host
```

検証手順

1. インストールコマンドラインインターフェイスパッケージが成功すると、出力は以下の例のようになります。

```
Installation of the CLI was successful.
```

第9章 DISCOVERY-TOOLS INSTALL コマンドのオプション

本ガイドのインストール手順では、すべてのデフォルトオプションで検出サーバーおよび CLI パッケージをインストールします。ただし、検出サーバーとコマンドラインインターフェイスパッケージをインストールする **install** サブコマンドには、インストールプロセスをカスタマイズするオプションが含まれます。

以下の情報には、**install** サブコマンドオプションと、サーバーパッケージおよび CLI パッケージの該当する使用情報およびデフォルト値が記載されています。

9.1. サーバーのインストールオプション

--version=version.patch.release

特定の検出サーバーバージョンのインストールを有効にします。インストールする検出サーバーのセマンティクスバージョン管理形式 (version.release.patch (0.9.0 など)) が含まれます。このオプションには、最新バージョンのデフォルトがあります。

--home-dir=server_home_dir

検出サーバーのインストールディレクトリーへの完全修飾パスを設定します。デフォルトは ~/**discovery**/ です。

--port=server_port

検出サーバーのポート番号を設定します。デフォルトは **9443** です。

--open-port=true|false

インストール時にファイアウォールのポートを開くかどうかを決定します。このオプションを使用すると、検出サーバーと、**port** オプションで定義されたポートを介したリモートクライアント間の通信が可能になります。true または false の値が含まれます。デフォルトは true です。ファイアウォールでサーバーポートを開かずにインストールする場合は **false** を指定します。インストールスクリプトは、サーバーポートを開く権限を昇格して実行する必要があります。

--registry-user=registry_website_username

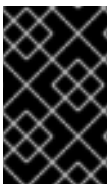
registry.redhat.io イメージレジストリーの Web サイトとして知られる Red Hat Container Catalog のユーザー名を指定します。サーバーのインストール時にこの値を入力するように求められます。

--registry-password=registry_website_password

registry.redhat.io イメージレジストリーの Web サイトとして知られる Red Hat Container Catalog のパスワードを指定します。サーバーのインストール時にこの値を入力するように求められます。

--db-user=database_username

PostgreSQL のデータベースユーザー名を設定します。デフォルトは **postgres** です。



重要

後で discovery-tools を使用して検出をアップグレードする場合は、アップグレード中に同じデータベースのユーザー名とパスワードを使用する必要があります。同じデータベース認証情報を使用しないと、データが失われる可能性があります。

--db-password=database_password

PostgreSQL のデータベースユーザーパスワードを設定します。このオプションにはデフォルト値がありません。省略すると、discovery-tools はパスワードを要求します。

重要

後で discovery-tools を使用して検出をアップグレードする場合は、アップグレード中に同じデータベースのユーザー名とパスワードを使用する必要があります。同じデータベース認証情報を使用しないと、データが失われる可能性があります。

--username=server_username

検出サーバーの管理者ユーザー名を設定します。デフォルトは **admin** です。

--password=server_password

検出サーバーの管理者パスワードを設定します。このオプションにはデフォルト値がありません。省略すると、discovery-tools はパスワードを要求します。

9.2. コマンドラインインターフェイスのインストールオプション

--version=version.patch.release

特定の検出 CLI バージョンのインストールを有効にします。インストールする検出 CLI のセマンティクスバージョン管理形式 (version.release.patch (0.9.0 など)) が含まれます。このオプションには、最新バージョンのデフォルトがあります。

--home-dir=cli_home_dir

検出 CLI のインストールディレクトリーへの完全修飾パスを設定します。デフォルトは ~/**discovery**/ です。

--server-host=server_IP_address

検出サーバーへの接続に使用する IP アドレスを設定します。このオプションにはデフォルト値がありません。CLI パッケージのインストール時に値を設定するか、コマンドラインインターフェイスのサーバー接続を設定して値を設定する必要があります。

--server-port=server_port

検出サーバーへの接続に使用するポート番号を設定します。このオプションにはデフォルト値がありません。CLI パッケージのインストール時に値を設定するか、コマンドラインインターフェイスのサーバー接続を設定して値を設定する必要があります。

パート IV. 検出の設定と維持

インストールが完了したら、検出を設定または維持するためにその他の手順を行う必要がある場合があります。インストール時に選択したオプションと、検出を使用する方法により、実行する必要のある設定タスクおよびメンテナーンスタスクの種類が決まります。

詳細情報

インストール時に検出サーバーとコマンドラインインターフェイスとの間の接続を設定する値を指定しなかった場合は、検出の使用を開始する前に、これらの値を設定する必要があります。詳細は、以下の情報を参照してください。

- 検出接続の設定

SSH キーを認証方法として含む認証情報を使用してネットワークスキャンを実行する場合は、検出サーバーがキーファイル情報にアクセスできる必要があります。検出サーバーに SSH キーを追加する方法は、次の情報を参照してください。

- ネットワークスキャン用の検出サーバーに SSH キーを追加

第10章 検出接続の設定

検出コマンドラインインターフェイスは、特定のポートおよび IP アドレスを使用して検出サーバーと通信する必要があります。

CLI パッケージのインストール時に、**--server-port** オプションおよび **--server-host** オプションの値を設定して、この情報を提供している可能性があります。CLI パッケージのインストール時にこれらの値を指定しなかった場合は、これらの値を設定する必要があります。以下の手順を使用して、必要に応じてこれらの値を編集することもできます。

手順

サーバーと通信するようにコマンドラインインターフェイスを設定するには、以下のコマンドを実行します。サーバーおよび CLI パッケージが異なるマシンにインストールされている場合は、CLI パッケージがインストールされているマシンから以下のコマンドを実行します。

1. 以下のコマンドを入力します。**server_port** は、検出サーバーが HTTPS 通信にに使用するポートで、**server_host** は、サーバーの IP アドレスに置き換えます。

```
# dsc server config --port=server_port --host=server_host
```

第11章 ネットワークスキャン用の検出サーバーに SSH キーを追加

ネットワークスキャンのソースおよび認証情報を設定する場合は、スキャンされるネットワークアセットに対して認証するために使用する認証情報のタイプを選択します。認証情報に使用できるオプションの 1 つは、ユーザー名と SSH キーファイルで認証することです。このオプションを選択する場合は、検出がこれらのアセットに対して認証を行い、スキャン中に発生するプロセスを完了できるように、サーバー上の特定のディレクトリーに秘密鍵のコピーを追加する必要があります。

ネットワークスキャンに必要な認証情報を作成して改良するため、これらのステップを継続してメンテナーンスタスクとして実行しなければならない場合があります。

手順

SSH キーファイルを検出サーバーに追加するには、次を行います。

1. 選択したコピー方法を使用して、キーファイルから秘密鍵をコピーします。
2. サーバーのインストール時に、このディレクトリーのデフォルトの場所である検出サーバーの **~/discovery/server/volumes/sshkeys** ディレクトリーに秘密鍵を追加します。
3. 必要に応じて、SSH キーファイルを使用するすべての認証情報に対して、認証方法として手順を繰り返します。

パート V. 検出ユーザーインターフェイスへのアクセス

ブラウザー接続を使用して、検出グラフィカルユーザーインターフェイスにアクセスできます。コマンドラインインターフェイスにアクセスするには、コマンドを実行してサーバーに接続します。

検出ユーザーインターフェイスを使用するには、ユーザーインターフェイスを実行するシステムが、検出サーバーがインストールされているシステムと通信できる必要があります。

詳細情報

検出グラフィカルユーザーインターフェイスへのログインおよびログアウトを行う要件および手順の詳細は、以下の情報を参照してください。

- 検出ユーザーインターフェイスへのログイン
- 検出ユーザーインターフェイスからログアウト

検出コマンドラインインターフェイスへのログインおよびログアウトを行う要件および手順の詳細は、以下の情報を参照してください。

- 検出コマンドラインインターフェイスへのログイン
- 検出コマンドラインインターフェイスからのログアウト

第12章 検出ユーザーインターフェイスへのログイン

前提条件

検出ユーザーインターフェイスにログインするには、検出サーバーがインストールされているシステムの IP アドレス、サーバーのインストール時にデフォルトのポートが変更された場合は接続のポート番号、ログイン時に使用するユーザー名およびパスワードが必要です。この情報がない場合は、検出サーバーをインストールした管理者にお問い合わせください。

手順

1. ブラウザーで、検出サーバーの URL を **https://IPaddress:port** の形式で入力します。**IPaddress** は検出サーバーの IP アドレスで、 **ポート** は公開されたサーバーポートです。以下の例は、ログインしているシステムとデフォルトのポートを使用するかどうかに基づいて、URL を入力する 2 つの方法を示しています。

   - サーバーがインストールされ、デフォルトのポートが使用されるシステムからログインする場合はは、以下の例のようにループバックアドレス (localhost とも呼ばれる) を IP アドレスとして使用できます。

     ```
     https://127.0.0.1:9443
     ```

   - サーバーからリモートのシステムからログインすると、サーバーは IP アドレス **192.0.2.0** で実行され、インストール中にデフォルトのポートが **8443** に変更すると、以下の例のようにログインします。

     ```
     https://192.0.2.0:8443
     ```

   サーバーの URL を入力すると、検出ログインページが表示されます。

2. ログインページでユーザー名とパスワードを入力し、**Log in** をクリックしてサーバーにログインします。

検証手順

検出に初めてログインすると、Welcome ページが表示されます。まず、スキャンで使用できるソースおよび認証情報を追加します。検出に以前にログインしている場合は、Welcome ページはスキップされ、以前に作成したソース、認証情報、およびスキャンと対話できます。

第13章 検出ユーザーインターフェイスからログアウト

手順

1. アプリケーションツールバーで、人のアイコンまたはユーザー名をクリックします。
2. **Logout** をクリックします。

第14章 検出コマンドラインインターフェイスへのログイン

前提条件

検出コマンドラインインターフェイスにログインするには、検出サーバーがインストールされているシステムの IP アドレスと、接続用のポート番号が必要です。これらの値は、CLI パッケージのインストール時に、または設定手順としてインストールした後に、コマンドラインインターフェイスに対して設定されます。ログイン時に使用するユーザー名とパスワードも必要です。この情報がない場合は、検出サーバーをインストールした管理者にお問い合わせください。

login コマンドは、後続のコマンドラインインターフェイスコマンドによる認証に使用されるトークンを取得します。そのトークンは、サーバーからログアウトすると削除され、毎日有効期限が切れます。

手順

1. コマンドラインインターフェイスにログインするには、以下のコマンドを入力します。ここで、**server_port** は検出サーバーが HTTPS 通信に使用するポートで、 **server_host** はサーバーの IP アドレスになります。

```
# dsc server login --port=server_port --host=server_host
```

2. プロンプトで、検出用にユーザー名とパスワードを入力します。

第15章 検出コマンドラインインターフェイスからのログアウト

サーバーからログアウトするコマンドにより、サーバーへのログイン時に作成されたトークンが削除されます。このトークンも毎日有効期限が切れます。

手順

1. コマンドラインインターフェイスからログアウトするには、以下のコマンドを入力します。

```
# dsc server logout
```