Unix 認証

認証スキャンに関心をお寄せいただきありがとうございます。認証を設定して使用すると、ホストをさらに詳しく評価し、最も正確な結果を取得し、誤検出を減らすことができます。本書では、Qualys クラウドスイート 8.10 以降を使用して Unix 認証を設定する際のヒントとベストプラクティスについて説明します。

Qualys は、Unix、Cisco、Checkpoint Firewall を実行しているシステムの認証をサポートしています。

考慮すべきこと

認証を使用する理由

認証を使用すると、提供された資格情報で対象の各システムにリモートからログインすることができます。ログインすることで、テスト中にさらに多くのことが行えるようになります。そのため、各システムのセキュリティ状態について、より適切に可視化することができます。認証は、コンプライアンススキャンでは必須であり、脆弱性スキャンでも推奨されています。

資格情報の安全性について

資格情報は、読み取り（READ）専用としてシステムへのアクセスに使用されます。デバイス上で資格情報を修正したり、何かを書き込んだりするということは、決してありません。資格情報は安全性を確保した状態で扱われ、スキャンの実行中にのみ使用されます。

操作手順

まず、対象のホスト上で認証済みのスキャン用のユーザアカウントを設定します。次に、Qualys を使用して次の手順を実行します。1）認証レコードを追加して、資格情報とホスト（IP）を関連付けます。レコードは、Unix 用、Cisco 用、Checkpoint Firewall 用にそれぞれ追加します。2）オプションプロファイルを使用してスキャンを開始します。VM スキャンの場合は、オプションプロファイルで認証が有効になっていることを確認してください。3）認証レポートを実行して、スキャン対象の各ホストで認証が成功または失敗したかを確認します。

複数のレコードの作成

Qualys では、レコードの作成は、異なる IP アドレスを使用すれば可能です。各 IP アドレスは、Unix タイプのレコード（Unix レコード、Cisco レコード、または CheckPoint Firewall レコード）の 1 つに含めることができます。

無断複写・転載を禁じます。2009-2020 年 クォリスジャパン株式会社

ログイン資格情報

資格情報は、認証レコードで指定します。さまざまなサードパーティの Vault をサポートしています。詳細は、オンラインヘルプの「Vault のサポートマトリックス」を参照してください。

脆弱性スキャンに必要な特権

提供するアカウントには、特定のコマンドを実行できる権限が必要です。例えば 1)“ uname ”を実行してパッケージのプラットフォームを検出する、2)/etc/redhat-release を読み取り、“ rpm ”を実行する(対象ホストで Red Hat が実行されている場合)、3)/etc/debian_version を読み取り、“ dpkg ”を実行する(対象ホストで Debian が実行されている)などがあります。この他にも実行する必要のあるコマンドは数多くあります。

コマンドのリストがある場所: 記事「*NIX Authenticated Scan Process and Commands(*NIX 認証済みのスキャンの処理とコマンド)」(英語)には、実行するコマンドの種類に関して説明しています。また、実行したコマンドの影響と範囲に関する考え方についても説明しています。この記事にあるリストのコマンドは、Qualys のサービスアカウントのスキャン中に実行される可能性があります。毎回、すべてのコマンドが実行されるわけではありません。*nix ディストリビューションによって異なります。このリストは、実行するコマンドを網羅したものではありません。また、更新も頻繁に行われません。

コンプライアンススキャンに必要な特権

すべてのコンプライアンスチェックを評価するには、スーパーユーザ(ルート)権限を持ったアカウントを指定する必要があります。コンプライアンススキャンでは、最初の SSH アクセスがルート権限を持たないユーザに付与されている場合でも、UID=0 のフルアクセスが付与されていることを確認します。UID=0 のフルアクセスがない場合、スキャンは続行されません。アカウントは、“ sh ”シェルまたは“ bash ”シェルでも設定されている必要があります。

スキャン対象のシステムでリモートのルートログインが無効になっている場合、システムで Sudo または PowerBroker ルート権限の委譲を使用することができます。ただし、sudoers ファイル(またはこれと同等の方法)で指定されたアカウントに特定のルートレベルのコマンドを委譲することによって、制限付き Unix/Linux アカウントを使用することはできません。ルート以外のアカウントを使用して最初の SSH 接続を確立することはできますが、そのアカウントで“ sudo su - ”コマンド(またはこれと同等のコマンド)を実行できる権限が必要になります。権限を高めることで、アカウントがコンプライアンススキャンの続行に必要なルートレベル(UID=0)のアクセスを取得することができます。

ルート権限委譲ツールの使用

(Unix 認証の Unix レコード設定で使用可能)。これらのルート権限委譲ツールが使用できる Unix 認証は、Sudo、Pismu、PowerBroker です。ルート権限委譲を有効にすると、比較的権限の低いユーザアカウントをレコードで指定した場合でも、スーパーユーザ(root)に昇格した権限でスキャンテストを実行できます。

ヒント: 複数のツールがある場合は、レコード内で特定の順番に並べ替えることができます。この設定した順番で、それぞれのルート権限委譲の方法が次々に試行されます。

パスワードの Vault にあるパスワードにアクセスする方法

サービスでは、CyberArk PIM Suite、CyberArk AIM、Thycotic Secret Server、Quest Vault、Lieberman ERPM など、複数のサードパーティのパスワード Vault との統合がサポートされています。「Scans」→「Authentication」→「New」→「Authentication Vaults」に移動して、使用している Vault システムを設定します。次に認証レコードで「Authentication Vault」を選択し、Vault 名を選択します。スキャン時には、レコード内のアカウント名と Vault で見つかったパスワードを使用してホストへの認証が行われます。

秘密鍵の使用

Unix 認証では、ssh2 でのみ鍵認証がサポートされています。秘密鍵は、Unix 認証レコード内で定義することができます。

「Clear Text Password」オプション

提供される資格情報を使用して、ssh、telnet、rlogin など、さまざまなコマンドラインサービスへのリモートアクセスを行います。レコードで「Clear Text Password」設定を選択すると、強力なパスワード暗号化をサポートしていないサービスへの接続時に、資格情報を平文でパスワードを送信するように指定することができます。

「Clear Text Password」が選択されていない場合（デフォルト）

パスワードは平文で送信されません。スキャンエンジンは、リモートログインに強力なパスワード暗号化のみを使用します。この設定にすると、強力なパスワード暗号化をサポートしていないホストでは、スキャンエンジンが一部の脆弱性を検出できないことがあります。

「Clear Text Password」が選択されている場合

パスワードは平文で送信されます。スキャンエンジンは、リモートログイン時には可能な限り、強力に暗号化したパスワードを使用します。、強力に暗号化されたパスワードを使用します。強力なパスワード暗号化をサポートしていないサービスには、弱い暗号化または平文に強度を下げて資格情報を送信します。注意すべき点として、これらの資格情報が悪意ある人物に傍受されると、ホストが非常に危険な状態になって攻撃を受け、情報が盗まれる恐れがあります。telnet や rlogin などの安全でないサービスを安全な ssh に変えることをお勧めします。安全でないコマンドラインサービスを利用する必要がある場合、SSL/TLS や VPN のように安全なトンネル内で利用することをお勧めします。

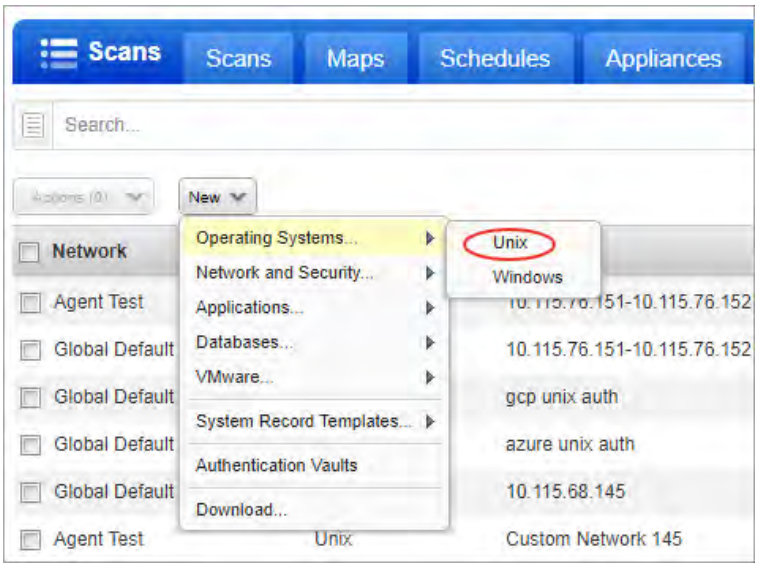
対象の種類

Unix（SSH2）認証レコードの作成時または更新時に対象の種類を指定できます。
このフィールドでは、シェルベース以外の対象の種類を SSH2 認証
レコードで定義することができます。標準の Unix シェルの対象は引き続き自動検出されます。このような
レコードに対して、対象の種類が「Auto (default)」に設定されます。現時点では、Qualys で提供されるオプションは「Auto (default)」だけです。今後のリリースで、更に多くの対象の種類が利用可能になります。

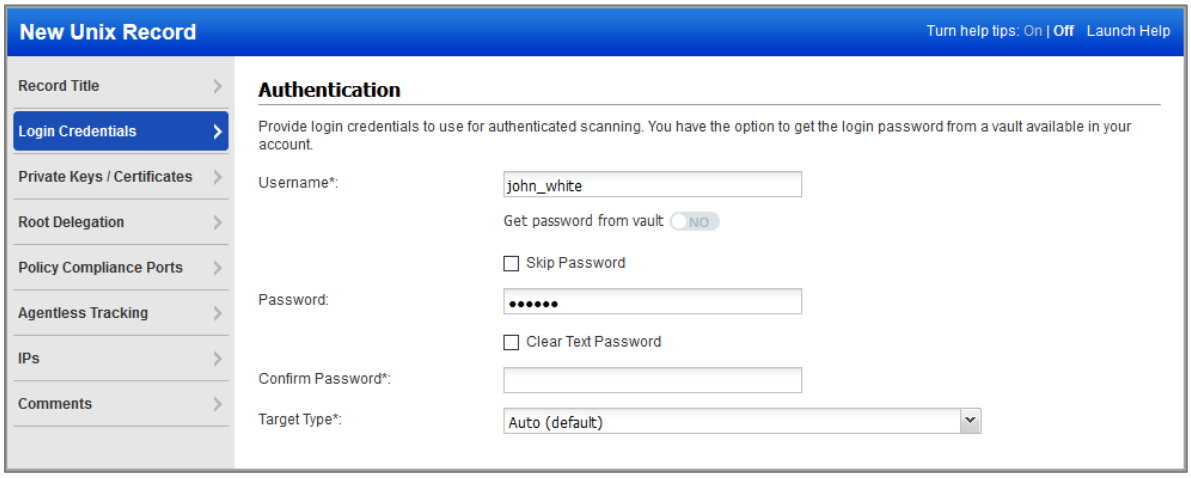
Unix 認証レコード

Unix レコードを追加する方法

「Scans」→「Authentication」に移動します。その後、「New」→「Operating Systems」→「Unix」を選択します。Unix のサブタイプが必要になる場合があります。サブタイプは、Cisco 認証や Checkpoint Firewall 認証のレコードに表示されます。



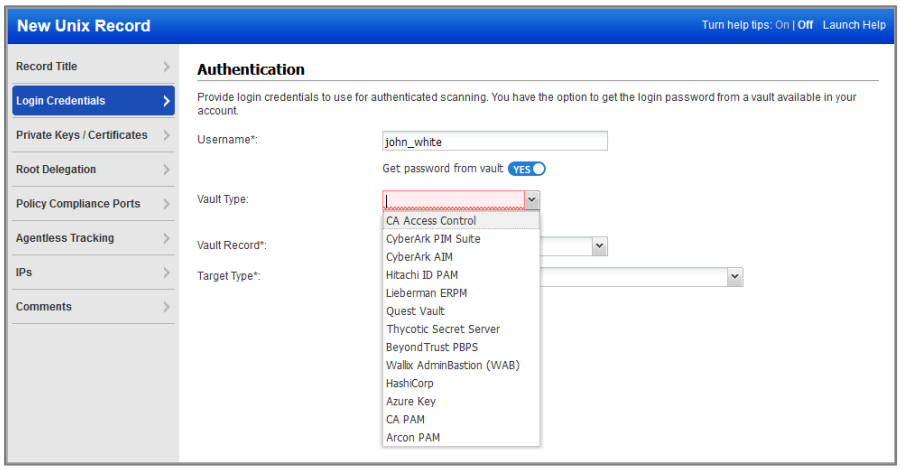
スキャン時にサービスが Unix ホストへログインする際に使用する Unix ログイン資格情報（ユーザ名とパスワード）を入力します。ウィザードに従い、秘密鍵、ルート権限委譲、ポリシーコンプライアンス、対象の IP に関するそれぞれのオプションをニーズに合わせて選択します。サポートが必要な場合は、いつでもオンラインヘルプが利用できます。



オプションの選択

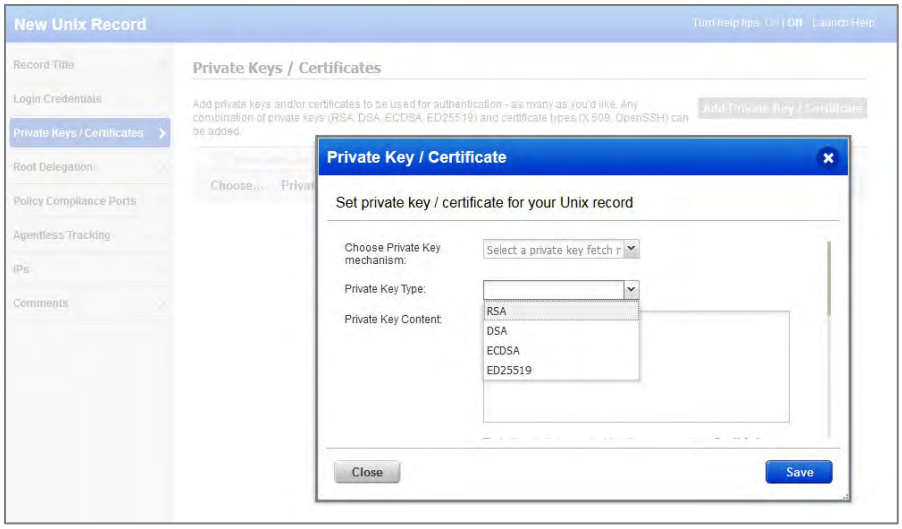
複数の資格情報がある場合、認証は以下の順で試行されます。
1）RSA 鍵、2）DSA 鍵、3）パスワード

ログイン資格情報のパスワードを Vault から取得するためのオプションです。アカウント内で使用可能な Vault から選択します。

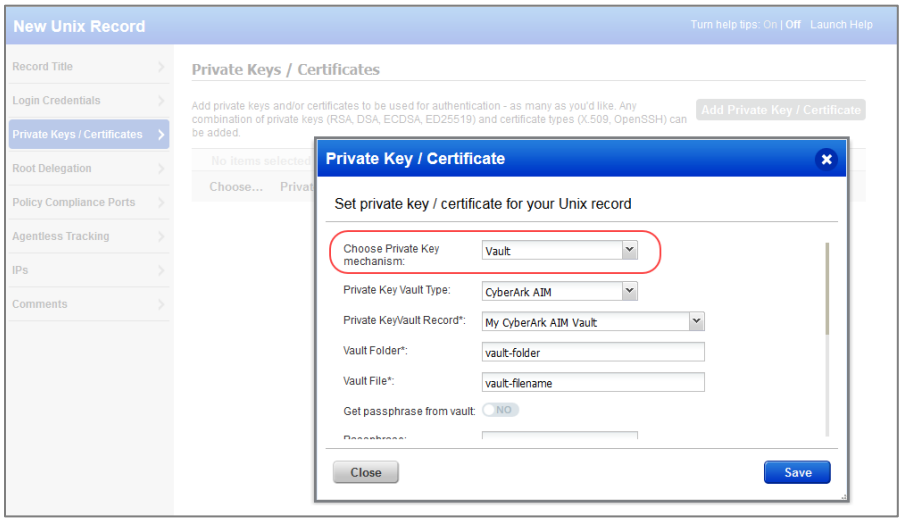


認証には、秘密鍵（RSA、DSA、ECDSA、ED25519）と証明書（OpenSSH、X.509）を任意に組み合わせて使用します。

鍵認証は、ssh2 でのみサポートされています。

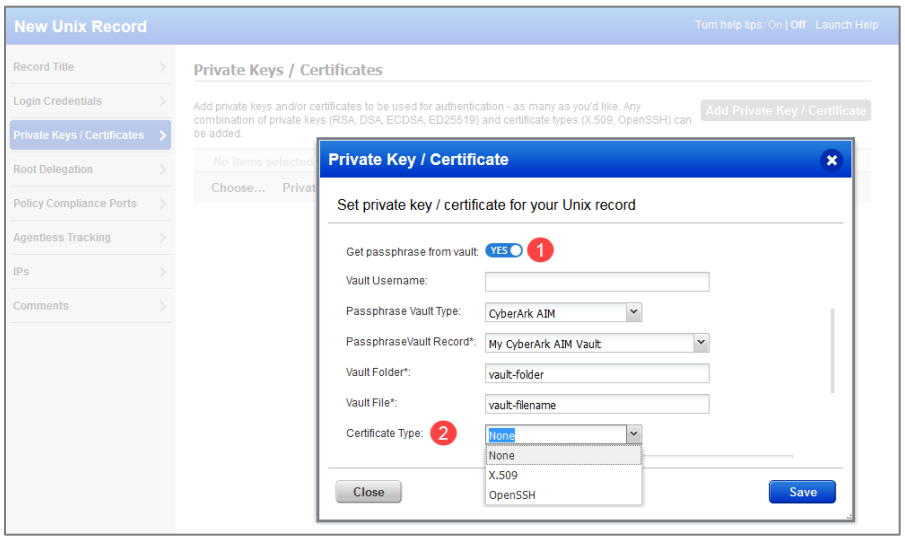


秘密鍵を Vault から取得するオプションです。アカウント内で使用可能な Vault から選択します。



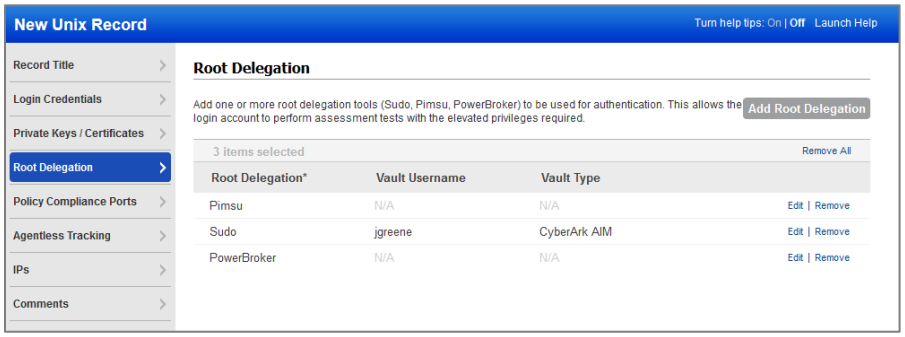
(1) 秘密鍵のパスフレーズを Vault から取得するオプションです。アカウント内で使用可能な Vault から選択します。

(2) 証明書タイプ(OpenSSH または X.509)を選択します。

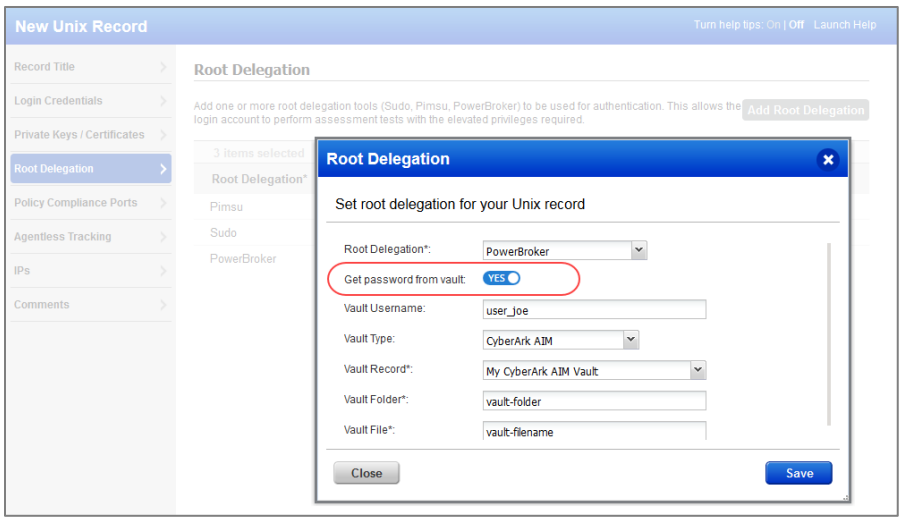


複数のルート権限委譲ツール(Sudo、Pimsu、PowerBroker)が使用できます。

この設定した順番で、それぞれのルート権限委譲の方法が次々に試行されます。



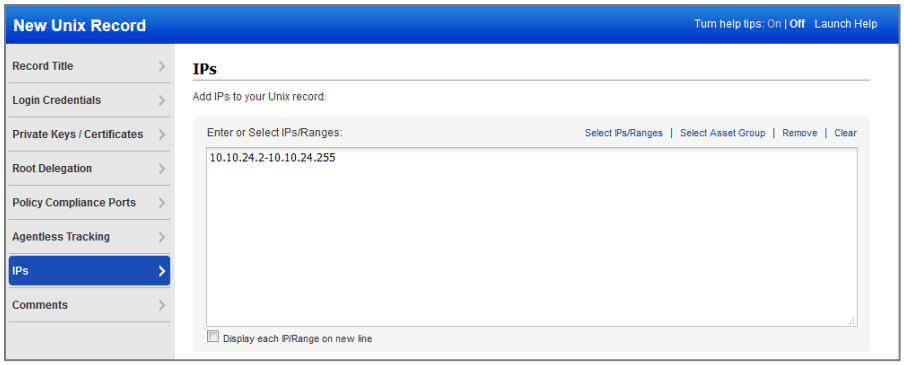
ルート権限委譲のパスワードを Vault から取得するオプションです。アカウント内で使用可能な Vault から選択します。



IP の追加

「IPs」タブでスキャン対象とする IP を追加します。

各 IP は、Unix タイプのレコード（Unix、Cisco、または CheckPoint Firewall）の 1 つに含めることができます。



コンプライアンススキャンのポート

「Policy Compliance Ports」タブでは、サービス（ssh、telnet、rlogin）がスキャン対象ホストの well-known ポートで実行されていない場合に、カスタムポートリストを定義することができます。デフォルトでは、スキャン対象になる well-known ポートとして、22（ssh）、23（telnet）、513（rlogin）が含まれます。これらのサービスはいずれも認証に使用できます。役立つヒント - 実際にスキャンされるポートは、スキャン時に使用されるコンプライアンスオプションプロファイルの「Ports」の設定によっても異なる点に注意してください。

秘密鍵/証明書の使用

認証を成功させるには、すべての対象ホストにユーザアカウントを追加し、ユーザのホームディレクトリにある“ ssh/authorized_keys2 ”ファイルに対応する公開鍵を付加する必要があります。サービスを利用するには、スキャン中、対象ホストへのフルアクセス権が必要です。“ ssh/authorized_keys2 ”ファイルに手動で追加されたオプション（no-pty など）によってサービスがロックアウトされる可能性があり、その場合、セキュリティテストを実行することはできません。サポートされている ssh 鍵と証明書は以下の通りです。すべての秘密鍵は、パスフレーズを使用して暗号化または暗号化の解除を行うことができます。

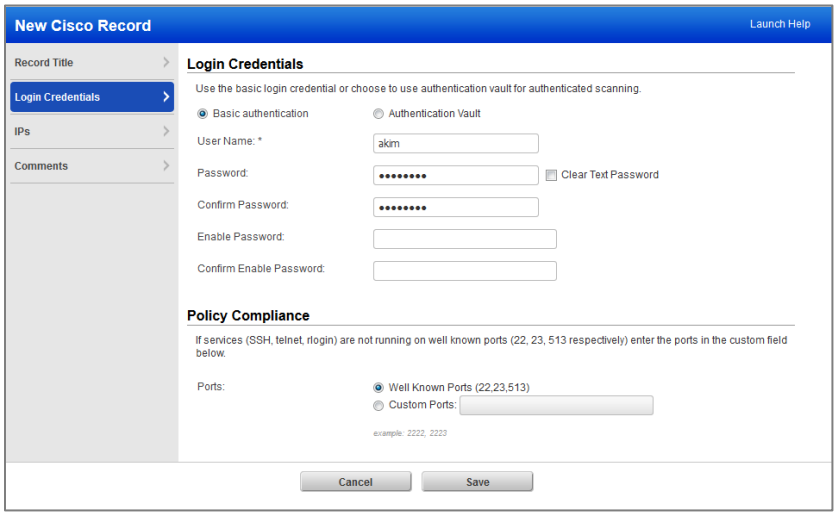
ssh 秘密鍵

PEM でエンコードされた RSA 秘密鍵
PEM でエンコードされた DSA 秘密鍵
PEM でエンコードされた ECDSA 秘密鍵
OpenSSH でエンコードされた RSA 秘密鍵
OpenSSH でエンコードされた DSA 秘密鍵
OpenSSH でエンコードされた ECDSA 秘密鍵
OpenSSH でエンコードされた EDDSA（現在は ED25519 のみ）秘密鍵

サポートされる証明書

PEM でエンコードされた X.509 証明書（RSA を使用）
PEM でエンコードされた X.509 証明書（DSA を使用）
PEM でエンコードされた X.509 証明書（ECDSA を使用）
OpenSSH 証明書（RSA を使用）
OpenSSH 証明書（DSA を使用）
OpenSSH 証明書（ECDSA を使用）
OpenSSH 証明書（EDDSA（現在は ED25519 のみ）を使用）

Cisco 認証レコード



サポートされるテクノロジ

Cisco IOS、Cisco ASA、Cisco IOS XE、Cisco NX-OS、Cisco ACS（バージョン 5.8 はサポート対象外）

サポートされる Vault

CyberArk AIM、CyberArk PIM Suite

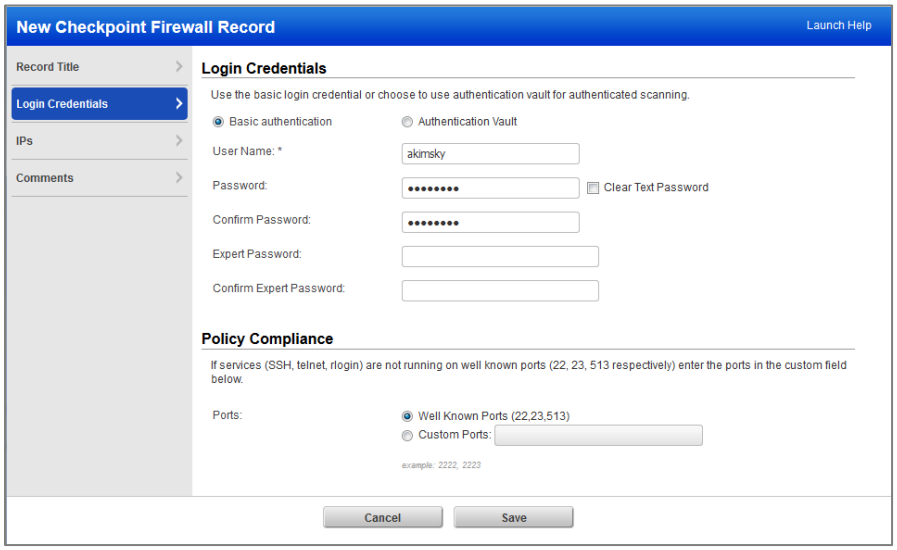
Cisco 認証で必要なログイン資格情報

1）認証で使用するユーザアカウントには、すべてのチェックを実行するために、Cisco 製デバイスに対してレベル 15 の特権（root ユーザレベルの特権と同等）が必要です。アカウントで実行できる必要があるコマンドのリスト、オンラインヘルプで確認できます。

2）ポート 22（ssh 認証用）またはポート 23（telnet 認証用）が必要です。対象のオプションが telnet だけの場合、telnet はセキュリティで保護されていないプロトコルである（すべての情報は平文で送信される）ため、「Clear Text Password」オプションを選択する必要があります。リモートログインには、できるだけ強力に暗号化したパスワードを使用し、「Clear Text Password」オプションが選択されている場合にのみ、平文で資格情報を送信する設定に戻すようにしてください。

3）使用するパスワードに空白を含めることはできません。

Checkpoint Firewall 認証レコード



サポートされるテクノロジ

CheckPoint GAiA および SecurePlatform PRO オペレーティングシステム
- CheckPoint GAiA R75-R77
- CheckPoint SecurePlatform PRO R75-77

サポートされる Vault

CyberArk AIM、CyberArk PIM Suite

Checkpoint Firewall 認証で必要なログイン資格情報

1）認証で使用するユーザアカウントには、すべてのチェックを実行し、また、以下のコマンドを実行するために、Checkpoint 製デバイスに対する管理者レベルの特権が必要です。

```
ver
expert (to switch to expert mode)
cpstat os
```

2）ssh 認証では、スキャン対象の TCP ポート 22 を開放する必要があります。

3）使用するパスワードに空白を含めることはできません。

「Expert Password」オプションについて

対象のホストでの“ expert ”コマンドの実行にパスワードが必要な場合は、レコードでの expert パスワードの入力も必要です（注記: “ expert ”コマンドの実行にパスワードが必要で、そのパスワードが指定されている場合、プールされた資格情報を使用する機能はサポートされません）。

最終更新日: 2020 年 7 月 28 日