IBM Security QRadar

アダプター構成ガイド

2016 年 9 月

注記

本書および本書で紹介する製品をご使用になる前に、 61 ページの『特記事項』に記載されている情報をお読みください。

お客様の環境によっては、資料中の円記号がバックスラッシュと表示されたり、バックスラッシュが円記号と表示されたりする場合があります。

原典： IBM Security QRadar
Adapter Configuration Guide
September 2016

発行： 日本アイ・ビー・エム株式会社

担当： トランスレーション・サービス・センター

目次

QRadar Risk Manager のアダプター構成の概要

IBM® Security QRadar® Risk Manager は、デバイス構成のモニター、ネットワーク環境に対する変更のシミュレーション、リスクおよび脆弱性の優先順位付けを行うために使用するアプライアンスです。QRadar Risk Manager はアダプターを使用して、ネットワーク上のデバイスと統合します。

対象読者

アダプターのインストールと構成を担当するネットワーク管理者は、ネットワーク・セキュリティーの概念とデバイスの構成を十分に理解している必要があります。

テクニカル・ドキュメント

Web 上で IBM Security QRadar の製品資料 (翻訳されたすべての資料を含む) を検索するには、 IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome) にアクセスしてください。

QRadar 製品ライブラリー内のより技術的な資料にアクセスする方法については、Accessing IBM Security QRadar Documentation (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644) を参照してください。

お客様サポートへの連絡

お客様サポートへのお問い合わせについては、Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144) を参照してください。

適切なセキュリティーの実践に関する注意事項

IT システムのセキュリティーでは、企業内および企業外からの不適切なアクセスの防止、検出、およびそれらのアクセスへの対応により、システムおよび情報を保護する必要があります。不適切なアクセスにより、情報が改ざん、破壊、盗用、または悪用されたり、あるいはご使用のシステムの損傷または他のシステムへの攻撃のための利用を含む悪用につながる可能性があります。 完全に安全と見なすことができる IT システムまたは IT 製品は存在せず、また単一の製品、サービス、またはセキュリティー対策が、不適切な使用またはアクセスを防止する上で、完全に有効となることもありません。IBM のシステム、製品およびサービスは、合法かつ包括的なセキュリティーの取り組みの一部となるように設計されており、これらには必ず追加の運用手順が伴います。また、最高の効果を得るために、他のシステム、製品、またはサービスを必要とする場合があります。IBM は、何者かの悪意のある行為または違法行為によって、システム、製品、またはサービスのいずれも影響を受けないこと、またはお客様の企業がそれらの行為によって影響を受けないことを保証するものではありません。

注意**:**

本プログラムの利用は、様々な法律または規制に関わる場合があります。これには、プライバシー、データ保護、雇用、電子通信、および電子保管に関連するものが含まれます。IBM Security QRadar は、合法的な目的のために合法的な手段を用いてのみ使用することができます。お客様は、適用される法律、規制、およびポリシーに従って本プログラムを使用することに同意し、かかる法律、規制、およびポリシーを遵守する全責任を負うものとします。ライセンシーは、IBM Security QRadar の合法的な使用に必要なすべての同意、許可、または使用権を取得するか、取得済みであることを表明するものとします。

第 1 章 アダプターの概要

アダプターは、IBM Security QRadar Risk Manager をネットワーク・デバイスと統合するために使用します。アダプターを構成することで、 QRadar Risk Manager はネットワーク・デバイス (ファイアウォール、ルーター、スイッチなど) の構成パラメーターの問い合わせを行い、それらをインポートできます。

ネットワーク・トポロジーおよびネットワーク構成

QRadar Risk Manager はアダプターを使用して、ネットワーク構成を収集します。アダプターは、その構成情報を、サポートされているデバイス・モデル、製造元、およびタイプについて統一された形式に変換します。QRadar Risk Manager はこのデータを使用して、ネットワーク・デバイスの構成とネットワーク・トポロジーを認識します。

ネットワークの外部デバイスを接続するには、QRadar Risk Manager はそのデバイスにアクセスできる必要があります。 QRadar Risk Manager はデバイスにアクセスして構成をダウンロードするために、QRadar で構成されているユーザー資格情報を使用します。

ネットワーク・デバイスの統合プロセス

ネットワーク・デバイスを QRadar Risk Manager と統合するには、以下の手順に従います。

1. QRadar Risk Manager と通信できるようにネットワーク・デバイスを構成します。
2. QRadar Risk Manager アプライアンスに、ネットワーク・デバイスに対応した適切なアダプターをインストールします。
3. 構成ソース管理を使用して、ネットワーク・デバイスを QRadar Risk Manager に追加します。
4. ネットワーク・デバイスとの通信に必要なネットワーク・プロトコルを定義します。

   詳しくは、「*IBM Security QRadar Risk Manager* ユーザー・ガイド」を参照してください。

アダプターのタイプ

IBM Security QRadar Risk Manager は、いくつかのアダプター・タイプをサポートします。

以下のアダプターがサポートされています。

- F5 BIG-IP
- Check Point SecurePlatform アプライアンス
- Check Point Security Management Server

- Cisco Catalyst (CatOS)
- Cisco インターネット・オペレーティング・システム (IOS)
- Cisco Nexus
- Cisco セキュリティー・アプライアンス
- Fortinet FortiOS
- HP Networking ProVision
- Juniper Networks ScreenOS
- Juniper Networks JUNOS
- Juniper Networks NSM
- Palo Alto
- Sourcefire 3D Sensor
- 汎用 SNMP
- TippingPoint IPS
- McAfee Sidewinder

第 2 章 アダプターのインストール

アダプター・ファイルを IBM Security QRadar SIEM Console にダウンロードし、それを IBM Security QRadar Risk Manager にコピーする必要があります。

始める前に

初期接続が確立されたら、QRadar SIEM Console は QRadar Risk Manager と直接通信できる唯一のデバイスになります。

手順

1. SSH を使用して、root ユーザーとして QRadar SIEM Consoleにログインします。
2. QRadar Risk Manager アダプターの圧縮ファイルを Fix Central (www.ibm.com/support/fixcentral/) から QRadar SIEM Console にダウンロードします。
3. 圧縮ファイルを QRadar SIEM Console から QRadar Risk Manager にコピーするには、以下のコマンドを入力します。

   ```
   scp adapters.zip root@IP_address:
   ```

   IP_address オプションは、QRadar Risk Manager の IP アドレスまたはホスト名です。

   例えば、以下のようにします。

   ```
   scp adapters.bundle-2014-10-972165.zip root@100.100.100.100:
   ```
4. QRadar Risk Manager アプライアンスで、root ユーザーのパスワードを入力します。
5. QRadar SIEM Console から SSH を使用して、root ユーザーとして QRadar Risk Manager アプライアンスにログインします。
6. アダプターを解凍してインストールするため、圧縮ファイルが含まれているルート・ディレクトリーから以下のコマンドを入力します。

   ```
   unzip adapters.zip

   yum install -y adapters*.rpm
   ```

   例えば、以下のようにします。

   ```
   unzip adapters.bundle-2014-10-972165.zip

   yum install -y adapters*.rpm
   ```

   注:

   V.7.2.8 より前のバージョンの QRadar Risk Manager の場合は、**rpm** コマンドを使用してください。

例えば、以下のようにします。

```
rpm -Uvh adapters*.rpm
```

7. ziptie サーバーのサービスを再始動してインストールを完了するため、以下のコマンドを入力します。

```
service ziptie-server restart
```

重要: ziptie サーバーのサービスを再始動すると、構成ソース管理で進行中のデバイス・バックアップがすべて中断されます。

アダプターのアンインストール

IBM Security QRadar Risk Manager からアダプターを削除するには、**yum** コマンドを使用します。

手順

1. SSH を使用して、root ユーザーとして IBM Security QRadar SIEM Console にログインします。
2. アダプターをアンインストールするには、以下のコマンドを使用します。

```
yum remove -y アダプター・パッケージ
```

例: `yum remove -y adapters.cisco.ios-2011_05-205181.noarch`

注:

V.7.2.8 より前のバージョンの QRadar Risk Manager の場合は、**rpm** コマンドを使用してください。

例えば、以下のようにします。

```
rpm -e adapter file
```

```
rpm -e adapters.cisco.ios-2011_05-205181.noarch.rpm
```

第 3 章 ネットワーク・デバイスの追加方法

ネットワーク・デバイスを IBM Security QRadar Risk Manager に追加するには、構成ソース管理を使用します。

以下の表で、ネットワーク・デバイスを追加する方法を説明します。

表 *1. QRadar Risk Manager* にネットワーク・デバイスを追加する方法

方法	説明
デバイスの追加	1 つのデバイスを追加します。
デバイスのディスカバー	複数のデバイスを追加します。
NSM からのディスカバー	Juniper Networks NSM コンソールで管理されているデバイスを追加します。
Check Point SMS のディスカバー	Check Point Security Manager Server (CPSMS) で管理されているデバイスを追加します。
SiteProtector™ からのディスカバー	SiteProtector からデバイスを追加します。
Defense Center からのディスカバー	Sourcefire Defense Center からデバイスを追加します。

ネットワーク・デバイスの追加

ネットワーク・デバイスを IBM Security QRadar Risk Manager に追加するには、構成ソース管理を使用します。

始める前に

ご使用のネットワーク・デバイスでサポートされているソフトウェア・バージョン、資格情報、および必要なコマンドを確認してください。詳しくは、 19 ページの『第 5 章 サポートされるアダプター』を参照してください。

手順

1. 「管理」タブをクリックします。
2. 「管理」ナビゲーション・メニューで、「プラグイン」をクリックします。
3. 「Risk Manager」 ペインで、「構成ソース管理」をクリックします。
4. ナビゲーション・メニューで「資格情報 **(Credentials)**」をクリックします。
5. 「ネットワーク・グループ (Network Groups)」ペインで、「新規ネットネットワーク・グループの追加 **(Add a new network group)**」をクリックします。
   a. ネットワーク・グループの名前を入力し、「**OK**」をクリックします。
   b. ご使用のデバイスの IP アドレスを入力して、「追加」をクリックします。

1 つの IP アドレス、IP アドレス範囲、CIDR サブネット、またはワイルドカードを入力できます。

例えば、ワイルドカードの形式として `10.1.*.*` を使用します。

例えば、CIDR の形式として `10.2.1.0/24` を使用します。

制約事項: 構成ソース管理で、他のネットワーク・グループに含まれているデバイス・アドレスを複製しないでください。

c. 追加するアドレスが「アドレスの追加 **(Add address)**」ボックスの横の「ネットワーク・アドレス **(Network address)**」ボックスに表示されることを確認します。

d. 追加する IP アドレスごとに、上記の 2 つのステップを繰り返します。

6. 「資格情報 (Credentials)」ペインで、「新規資格情報セットの追加 **(Add a new credential set)**」をクリックします。

a. 資格情報セットの名前を入力し、「**OK**」をクリックします。

b. 作成した資格情報セットの名前を選択し、パラメーターの値を入力します。

以下の表は、パラメーターについて説明しています。

表 2. 資格情報のパラメーター・オプション

パラメーター	説明

ユーザー名	アダプターにログインするための有効なユーザー名。
	
	アダプターの場合、指定するユーザー名とパスワードには、以下のようなさまざまなファイルへのアクセス権限が必要です。
	
	`rule.C`
	
	`objects.C`
	
	`implied_rules.C`
	
	`Standard.PF`

パスワード	デバイスのパスワード。
パスワードを有効にする **(Enable Password)**	第 2 レベル認証のパスワード。 これは、資格情報のプロンプトでエキスパート・モードのアクセス・レベルに必要なユーザー資格情報が求められる場合に必要なパスワードです。
SNMP Get コミュニティー **(SNMP Get Community)**	オプション
SNMPv3 認証ユーザー名 **(SNMPv3 Authentication Username)**	オプション
SNMPv3 認証パスワード **(SNMPv3 Authentication Password)**	オプション

表 2. 資格情報のパラメーター・オプション (続き)

パラメーター	説明
SNMPv3 プライバシー・パスワード **(SNMPv3 Privacy Password)**	オプション SNMPv3 トラップの復号に使用するプロトコル。

制約事項**:** ネットワーク・デバイスが以下のいずれかの条件に該当する場合は、構成ソース管理でプロトコルを構成する必要があります。

- デバイスが通信プロトコル用に非標準ポートを使用している。
- IBM Security QRadar Risk Manager が特定の IP アドレスとの通信に使用するプロトコルを構成する。

ソースの構成について詳しくは、「*IBM Security QRadar Risk Manager* ユーザー・ガイド」を参照してください。

7. ナビゲーション・メニューで 1 つまたは複数のデバイスを追加します。
   - 1 つのネットワーク・デバイスを追加するには、「デバイスの追加 **(Add Device)**」をクリックします。
   - ネットワーク・デバイスの複数の IP アドレスを追加するには、「デバイスのディスカバー **(Discover Devices)**」をクリックします。
8. デバイスの IP アドレスを入力し、アダプター・タイプを選択し、「追加」をクリックします。

   デバイスをバックアップしていない場合、アダプターの横に青色の疑問符が表示されます。
9. デバイス・リストに追加するデバイスをバックアップするには、デバイスを選択し、「バックアップ」をクリックします。
10. デバイス・リストに追加するネットワーク・デバイスごとに、これらのステップを繰り返します。

次のタスク

必要なデバイスをすべて追加したら、プロトコルを構成できます。詳しくは、「*IBM Security QRadar Risk Manager* ユーザー・ガイド」を参照してください。

NSM コンソールで管理されているデバイスの追加

Juniper Networks NSM (Network and Security Manager) コンソールからすべてのデバイスを IBM Security QRadar Risk Manager に追加するには、構成ソース管理を使用します。

始める前に

ご使用のネットワーク・デバイスでサポートされているソフトウェア・バージョン、資格情報、および必要なコマンドを確認してください。詳しくは、 19 ページの『第 5 章 サポートされるアダプター』を参照してください。

手順

1. IBM Security QRadar SIEM で「管理」タブをクリックします。
2. 「管理」ナビゲーション・メニューで、「プラグイン」をクリックします。
3. 「Risk Manager」 ペインで、「構成ソース管理」をクリックします。
4. ナビゲーション・メニューで「資格情報 **(Credentials)**」をクリックします。
5. 「ネットワーク・グループ (Network Groups)」ペインで、「新規ネットネットワーク・グループの追加 **(Add a new network group)**」をクリックします。
   a. ネットワーク・グループの名前を入力し、「**OK**」をクリックします。
   b. ご使用のデバイスの IP アドレスを入力して、「追加」をクリックします。

      1 つの IP アドレス、IP アドレス範囲、CIDR サブネット、またはワイルドカードを入力できます。

      制約事項**:** 構成ソース管理で、他のネットワーク・グループに含まれているデバイス・アドレスを複製しないでください。
   c. 追加するアドレスが「アドレスの追加 **(Add address)**」ボックスの横の「ネットワーク・アドレス **(Network address)**」ボックスに表示されることを確認します。
   d. 追加する IP アドレスごとに、上記の 2 つのステップを繰り返します。
6. 「資格情報 (Credentials)」ペインで、「新規資格情報セットの追加 **(Add a new credential set)**」をクリックします。
   a. 資格情報セットの名前を入力し、「**OK**」をクリックします。
   b. 作成した資格情報セットの名前を選択し、パラメーターの値を入力します。

      以下の表は、パラメーターについて説明しています。

表 *3. Juniper NSM Web* サービス資格情報のパラメーター・オプション

パラメーター	説明
ユーザー名	Juniper NSM (Network and Security Manager) Web サービスにログインするための有効なユーザー名。 Juniper NSM Web サービスの場合、このユーザーは Juniper NSM サーバーにアクセスできる必要があります。
パスワード	デバイスのパスワード。
パスワードを有効にする **(Enable Password)**	不要です。

      制約事項**:** Juniper Networks NSM (Network and Security Manager) は SNMP をサポートしていません。
7. ナビゲーション・メニューで「**NSM** からのディスカバー **(Discover from NSM)**」をクリックします。
8. IP アドレスおよびユーザー資格情報の値を入力し、「**OK**」をクリックし、「実行」をクリックします。
9. デバイス・リストに追加したデバイスを選択し、「バックアップ」をクリックし、「はい」をクリックします。

次のタスク

必要なデバイスをすべて追加したら、プロトコルを構成できます。詳しくは、「*IBM Security QRadar Risk Manager* ユーザー・ガイド」を参照してください。

CPSMS コンソールによって管理される QRadar Risk Manager へのデバイスの追加

Check Point Security Manager Server (CPSMS) から IBM Security QRadar Risk Manager にデバイスを追加するには、構成ソース管理を使用します。

デバイスを QRadar Risk Manager に追加するには、ご使用の Check Point Security Manager Server のバージョンに応じて、以下のいずれかのディスカバリー方式を選択する必要があります。

OPSEC を使用した、CPSMS により管理されるデバイスの追加

OPSEC を使用してデバイスのディスカバーおよび追加を行うことにより、バージョン NGX R60 から R77 までの Check Point Security Manager Server により管理されるデバイスを IBM Security QRadar Risk Manager に追加します。

始める前に

ご使用のネットワーク・デバイスでサポートされているソフトウェア・バージョン、資格情報、および必要なコマンドを確認してください。詳しくは、 19 ページの『第 5 章 サポートされるアダプター』を参照してください。

この手順を開始する前に、OPSEC エンティティー SIC 名、OPSEC アプリケーション・オブジェクト SIC 名、および *pull certificate* パスワードのワンタイム・パスワードを確認しておく必要があります。詳しくは、CPSMS の資料を参照してください。

注**:** デバイス・インポート機能は CPSMS アダプターと互換性がありません。

このタスクについて

接続し、管理対象ファイアウォールのディスカバリーを開始する CPSMS ごとに以下の手順を繰り返します。

手順

1. 「管理」タブをクリックします。
2. 「管理」ナビゲーション・メニューで、「プラグイン」をクリックします。
3. 「Risk Manager」 ペインで、「構成ソース管理」をクリックします。
4. ナビゲーション・メニューで「資格情報 **(Credentials)**」をクリックします。
5. 「ネットワーク・グループ (Network Groups)」ペインで、「新規ネットネットワーク・グループの追加 **(Add a new network group)**」をクリックします。
   a. ネットワーク・グループの名前を入力し、「**OK**」をクリックします。
   b. CPSMS デバイスの IP アドレスを入力して、「追加」をクリックします。

制約事項: 構成ソース管理で、他のネットワーク・グループに含まれているデバイス・アドレスを複製しないでください。

c. 追加するアドレスが「アドレスの追加 **(Add address)**」ボックスの横の「ネットワーク・アドレス **(Network address)**」ボックスに表示されることを確認します。

6. 「資格情報 (Credentials)」ペインで、「新規資格情報セットの追加 **(Add a new credential set)**」をクリックします。
   a. 資格情報セットの名前を入力し、「**OK**」をクリックします。
   b. 作成した資格情報セットの名前を選択し、デバイスの有効なユーザー名とパスワードを入力します。
7. ディスカバー対象ファイアウォール・デバイスを管理する CPSMS の OPSEC エンティティー SIC 名を入力します。ディスカバリーの発生元のデバイスのタイプによってフォーマットが異なるため、この値は正確な値でなければなりません。OPSEC エンティティー SIC 名のフォーマットを参照する際には以下の表を使用してください。

Type	名前
管理サーバー	`CN=cp_mgmt,O=<take O value from DN field>`
管理サーバーへのゲートウェイ	`CN=cp_mgmt_<gateway hostname>,O=<take O value from DN field>`

例えば、管理サーバーからディスカバリーを実行する場合は次のようになります。

- OPSEC アプリケーション DN: `CN=cpsms226,O=vm226-CPSMS..bs7ocx`
- OPSEC アプリケーション・ホスト: `vm226-CPSMS`

エンティティー SIC 名は `CN=cp_mgmt,O=vm226-CPSMS..bs7ocx` となります。

例えば、管理サーバーへのゲートウェイからのディスカバリーを実行する場合は次のようになります。

- OPSEC アプリケーション DN: `CN=cpsms230,O=vm226-CPSMS..bs7ocx`
- OPSEC アプリケーション・ホスト: `vm230-CPSMS2-GW3`

エンティティー SIC 名は `CN=cp_mgmt_vm230-CPSMS2-GW3,O=vm226-CPSMS..bs7ocx` となります。

8. Check Point SmartDashboard アプリケーションを使用して、CPSMS で作成された OPSEC アプリケーション・オブジェクト SIC 名を入力します。

   例: `CN=cpsms230,O=vm226-CPSMS..bs7ocx`
9. 次のようにして、OPSEC SSL 証明書を入手します。
   a. 「証明書の取得 **(Get Certificate)**」をクリックします。
   b. 「認証局の **IP**」フィールドに IP アドレスを入力します。
   c. 「証明書パスワードのプル **(Pull Certificate Password)**」フィールドに、OPSEC アプリケーションのワンタイム・パスワードを入力します。
   d. 「**OK**」をクリックします。

10. 「**OK**」をクリックします。
11. 「プロトコル」をクリックし、「**CPSMS**」プロトコルが選択されていることを確認します。

    CPSMS プロトコルのデフォルトのポートは 18190 です。
12. 「**Check Point OPSEC** からディスカバー **(Discover From Check Point OPSEC)**」をクリックし、CPSMS IP アドレスを入力します。
13. 「**OK**」をクリックします。
14. 追加する CPSMS デバイスごとに、これらのステップを繰り返します。

次のタスク

必要なデバイスをすべて追加したら、デバイスをバックアップし、トポロジーで確認します。

HTTPS を使用した、CPSMS により管理されるデバイスの追加

HTTPS プロトコルを使用してデバイスのディスカバーおよび追加を行うことにより、バージョン R80 の Check Point Security Manager Server により管理されるデバイスを IBM Security QRadar Risk Manager に追加します。

手順

1. 「管理」タブをクリックします。
2. 「管理」ナビゲーション・メニューで、「プラグイン」をクリックします。
3. 「Risk Manager」 ペインで、「構成ソース管理」をクリックします。
4. ナビゲーション・メニューで「資格情報 **(Credentials)**」をクリックします。
5. 「ネットワーク・グループ (Network Groups)」ペインで、「新規ネットネットワーク・グループの追加 **(Add a new network group)**」をクリックします。
   a. ネットワーク・グループの名前を入力し、「**OK**」をクリックします。
   b. Check Point デバイスの IP アドレスを入力して、「追加」をクリックします。
   c. そのアドレスが「ネットワーク・アドレス **(Network address)**」ボックスに表示されることを確認します。
6. 「資格情報 (Credentials)」ペインで、「新規資格情報セットの追加 **(Add a new credential set)**」をクリックします。
   a. 資格情報セットの名前を入力し、「**OK**」をクリックします。
   b. 作成した資格情報セットの名前を選択し、デバイスの有効なユーザー名とパスワードを入力します。
7. 「**OK**」をクリックします。
8. 「プロトコル」をクリックし、「**HTTPS**」プロトコルが選択されていることを確認します。
9. 「**Check Point HTTPS** からディスカバー **(Discover From Check Point HTTPS)**」をクリックし、Check Point の IP アドレスを入力します。
10. 「**OK**」をクリックします。

次のタスク

必要なデバイスをすべて追加したら、デバイスをバックアップし、トポロジーで確認します。

SiteProtector で管理されるデバイスの追加

SiteProtector から IBM Security QRadar Risk Manager にデバイスを追加するには、構成ソース管理を使用します。

始める前に

デバイスを追加するには、事前に IBM Internet Security Systems GX アダプターと IBM Security SiteProtector System アダプターをインストールしておく必要があります。

Microsoft SQL Server ポート 1433 を使用するには、Microsoft SQL プロトコルを有効にしておく必要があります。

手順

1. 「管理」タブをクリックします。
2. 「管理」ナビゲーション・メニューで、「プラグイン」をクリックします。
3. 「Risk Manager」 ペインで、「構成ソース管理」をクリックします。
4. ナビゲーション・メニューで「資格情報 **(Credentials)**」をクリックします。
5. 「ネットワーク・グループ (Network Groups)」ペインで、「新規ネットネットワーク・グループの追加 **(Add a new network group)**」をクリックします。
   a. ネットワーク・グループの名前を入力し、「**OK**」をクリックします。
   b. SiteProtector デバイスの IP アドレスを入力して、「追加」をクリックします。
   c. 追加するアドレスが「アドレスの追加 **(Add address)**」ボックスの横の「ネットワーク・アドレス **(Network address)**」ボックスに表示されることを確認します。
6. 「資格情報 (Credentials)」ペインで、「新規資格情報セットの追加 **(Add a new credential set)**」をクリックします。
   a. 資格情報セットの名前を入力し、「**OK**」をクリックします。
   b. 作成した資格情報セットの名前を選択し、デバイスの有効なユーザー名とパスワードを入力します。

      制約事項**:** ユーザー名とパスワードは、 SiteProtector Microsoft SQL Server データベースへのアクセスに使用される資格情報と同一です。
7. 「**OK**」をクリックします。
8. 「**SiteProtector** からディスカバー **(Discover From SiteProtector)**」をクリックし、 SiteProtector の IP アドレスを入力します。
9. 「**OK**」をクリックします。

次のタスク

必要なデバイスをすべて追加したら、デバイスをバックアップし、トポロジーで確認します。

第 4 章 デバイスのディスカバリーおよびバックアップのトラブルシューティング

デバイスのディスカバリーおよびバックアップの問題を修正します。ログやエラー・メッセージおよび警告メッセージで詳細を確認して、トラブルシューティングに役立てることができます。

デバイスのバックアップ障害

デバイスのログイン資格情報を確認します。

1. 「管理」タブで、「構成ソース管理」をクリックします。
2. ターゲット・デバイスにアクセスするための資格情報が正しいことを確認します。
3. ターゲット・デバイスで資格情報をテストします。

デバイス・バックアップ・エラーの表示

バックアップ・エラーを表示するには、以下の手順を実行します。

1. 「管理」タブで、「構成ソース管理」をクリックします。
2. デバイスをクリックしてから「エラーの表示 **(View error)**」をクリックします。

以下の表に、エラー・メッセージの ID、メッセージの説明、およびトラブルシューティングの推奨アクションをリストします。

表 4. デバイス・バックアップ・エラー

バックアップ・エラー	エラーの説明	推奨トラブルシューティング手順
UNEXPECTED_RESPONSE	接続試行がタイムアウトになった	正しいアダプターを使用していることを確認します。
INVALID_CREDENTIALS	資格情報が正しくない	「構成ソース管理」で資格情報を確認します。
SSH_ERROR	接続エラー	デバイスが機能していて、ネットワークに接続されていることを確認します。その他のネットワーク接続プロトコルおよびトラブルシューティング・ツールを使用して、デバイスにアクセス可能であることを確認します。SSH 接続プロトコルが許可されていて、正しく構成されていることを確認します。

表 4. デバイス・バックアップ・エラー (続き)

バックアップ・エラー	エラーの説明	推奨トラブルシューティング手順
TELNET_ERROR	接続エラー	デバイスが機能していて、ネットワークに接続されていることを確認します。その他のネットワーク接続プロトコルおよびトラブルシューティング・ツールを使用して、デバイスにアクセス可能であることを確認します。Telnet 接続プロトコルが許可されていて、正しく構成されていることを確認します。
SNMP_ERROR	接続エラー	デバイスが機能していて、ネットワークに接続されていることを確認します。その他のネットワーク接続プロトコルおよびトラブルシューティング・ツールを使用して、デバイスにアクセス可能であることを確認します。SNMP が許可されていて、正しく構成されていることを確認します。
TOO_MANY_USERS	このデバイスの構成済みアクセス・ユーザー数を超えた。	デバイスへのアクセスが許可されるユーザーの最大数を確認します。それには、デバイスにログオンし、そのデバイスに同時にアクセスできる最大ユーザー数の構成を確認します。
DEVICE_MEMORY_ERROR	デバイス構成エラー	デバイスが正常に機能していることを確認します。デバイスにアクセスし、構成を検証して、ログにエラーがないかを確認します。デバイスの資料を参照して、エラーのトラブルシューティングに役立ててください。
NVRAM_CORRUPTION_ERROR	デバイスのアクセス権限の問題	「構成ソース管理」で、デバイスにアクセスするために構成されているユーザー名のアクセス・レベルを確認します。
INSUFFICIENT_PRIVILEGE	デバイスにアクセスするように構成されたユーザーの特権が不十分	「構成ソース管理」で、デバイスにアクセスするために構成されているユーザー名のアクセス・レベルを確認します。
DEVICE_ISSUE	デバイスでのエラー	「構成ソース管理」でデバイスを選択し、「エラーの表示 **(View error)**」をクリックして詳細を表示します。

バックアップ終了時に構文解析に関する警告が出る

警告の詳細を表示するには、以下の手順を実行します。

1. 「リスク」タブをクリックします。
2. ナビゲーション・メニューで、「構成モニター **(Configuration Monitor)**」をクリックします。
3. 「デバイス・リスト **(Device List)**」の表で、選択したデバイスの「ログの表示 **(See Log)**」をクリックします。

アダプターのバージョンは最新になっていますか**?**

アダプターのバージョンを確認するには、QRadar Risk Manager アプライアンスに root としてログインし、以下のコマンドを入力します。

```
yum list adapter¥*
```

アダプター名の日付情報を確認することでリリース日を判定できます。

最新のアダプター・バンドルをダウンロードするには、以下の手順を実行します。

1. IBM Fix Central (https://www.ibm.com/support/fixcentral/) にアクセスします。
2. 「製品セレクター」フィールドに `Risk Manager` と入力して、選択をフィルターに掛けます。
3. IBM Security QRadar Risk Manager をクリックします。
4. 「インストール済みのバージョン」リストで、システムにインストールされているバージョンを選択します。
5. 「プラットフォーム」リストから、ご使用のシステムにインストールされているオペレーティング・システムを選択し、「続行」をクリックします。
6. 「フィックスの参照」を選択し、「続行」をクリックします。
7. 最新のアダプター・バンドルをダウンロードするために、「アダプター」リストの最上部にあるアダプター・バンドル・リンクをクリックします。

デバイスのバックアップは最新か**?**

バックアップが最新かを確認するには、以下の手順を実行します。

1. 「リスク」タブをクリックします。
2. ナビゲーション・メニューで、「構成モニター **(Configuration Monitor)**」をクリックします。
3. 「デバイス・リスト **(Device List)**」の表で、デバイスをダブルクリックします。
4. ツールバーから「履歴」をクリックします。インポートされている最新の構成が表示されます。

構成が最新のものではないと思われる場合は、バックアップを再実行して確認してください。

デバイスからの構成のインポート時のエラー

CSV ファイルの形式が誤っていると、デバイスのバックアップが失敗する原因になります。以下の手順を実行して、CSV ファイルを確認します。

1. CSV ファイルを確認して、エラーを修正します。
2. 更新した CSV ファイルを使用して、デバイスの構成を再インポートします。

Check Point SMS (OPSEC) からのデバイスのディスカバー失敗

「*IBM Security QRadar Risk Manager* アダプター構成ガイド」の『CPSMS コンソールで管理されているデバイスの追加』セクションのすべての手順に従います。特に、手順 7 および 8 で OPSEC フィールドを正確に指定してください。

関連タスク:

9 ページの『OPSEC を使用した、CPSMS により管理されるデバイスの追加』
OPSEC を使用してデバイスのディスカバーおよび追加を行うことにより、バージョン NGX R60 から R77 までの Check Point Security Manager Server により管理されるデバイスを IBM Security QRadar Risk Manager に追加します。

第 5 章 サポートされるアダプター

IBM Security QRadar Risk Manager は、セキュリティー製品のさまざまな製造元およびベンダーと統合します。

サポートされるアダプターごとに、次の情報が記載されています。

サポート対象のバージョン

サポートされている製品の名前とバージョンを示します。

近隣データのサポート

近隣データがこのアダプターでサポートされているかどうかを示します。デバイスで近隣データがサポートされている場合、Simple Network Management Protocol (SNMP) およびコマンド・ライン・インターフェース (CLI) を使用してデバイスから近隣データを取得します。

SNMP ディスカバリー

SNMP を使用したディスカバリーがデバイスで許可されているかどうかを示します。

SNMP ディスカバリーを実行するには、デバイスで標準 MIB-2 がサポートされている必要があります。また、デバイスの SNMP 構成がサポートされており、正しく構成されている必要があります。

必須資格情報パラメーター

QRadar Risk Manager とデバイスが接続するために必要なアクセス要件を示します。

QRadar Risk Manager とデバイスで構成されているデバイス資格情報が同一であることを確認してください。

パラメーターが不要な場合は、そのフィールドをブランクのままにしておくことができます。

QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。

接続プロトコル

ネットワーク・デバイスのサポートされているプロトコルを示します。

QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。

必要なコマンド

ログインしてデータを収集するためにアダプターが必要とするコマンドのリストを示します。

リストされているコマンドをアダプターに対して実行するには、 QRadar Risk Manager に指定されている資格情報に適切な特権が含まれている必要があります。

収集されるファイル

アダプターがアクセスできる必要があるファイルのリストを示します。これらのファイルにアクセスするには、アダプターに対して適切な資格情報が構成されている必要があります。

Check Point SecurePlatform アプライアンス

IBM Security QRadar Risk Manager は Check Point SecurePlatform アプライアンス アダプターをサポートします。

Check Point SecurePlatform アプライアンス アダプターとともに以下のフィーチャーを使用できます。

- 動的 NAT
- 静的 NAT
- SNMP ディスカバリー
- 静的ルーティング
- Telnet 接続プロトコルおよび SSH 接続プロトコル

以下の表で、Check Point SecurePlatform アプライアンス アダプターの統合要件を説明します。

表 *5. Check Point SecurePlatform* アプライアンス アダプターの統合要件

統合要件	説明
バージョン	R65 から R77.30 まで **制約事項:** Nokia IPSO アプライアンスは、バックアップに対してはサポートされていません。
SNMP ディスカバリー	SNMP sysDescr 内の NGX を突き合わせます。
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	ユーザー名 パスワード パスワードを有効にする **(Enable Password)** (エキスパート・モード)
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	以下のいずれかのサポート対象接続プロトコルを使用します。 **Telnet** **SSH**

表 5. *Check Point SecurePlatform* アプライアンス アダプターの統合要件 (続き)

統合要件	説明
ログインしてデータを収集するためにアダプターが必要とするコマンド	hostname dmidecode ver uptime dmesg route -n show users ifconfig -a echo $FWDIR
収集されるファイル	rules.C objects.C implied_rules.C Standard.pf snmpd.com

Check Point Security Management Server アダプター

Check Point アダプターを使用して、Security Management Server (CPSMS) により管理されるエンド・ノードをディスカバーおよびバックアップします。

CPSMS により管理されるエンド・ノードをディスカバーおよびバックアップするには、以下のいずれかのアダプターを選択してください。

Check Point Security Management Server OPSEC アダプター

Check Point Security Management Server OPSEC アダプターを使用して、バージョン NGX R60 から R77 までの CPSMS により管理されるエンド・ノードをディスカバーおよびバックアップします。

Check Point Security Management Server OPSEC アダプターとともに以下のフィーチャーを使用できます。

- OPSEC プロトコル
- 動的 NAT
- 静的 NAT
- 静的ルーティング

CPSMS アダプターは OPSEC SDK 6.0 に基づいて構築されており、SHA-1 を使用して署名された証明書のみを使用するように構成された Check Point 製品をサポートします。

以下の表で、CPSMS アダプターの統合要件を説明します。

表 6. *CPSMS* アダプターの統合要件

統合要件	説明
バージョン	NGX R60 から R77 まで
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	『CPSMS コンソールで管理されているデバイスの追加』で設定した資格情報を使用します。
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	**CPSMS**
構成の要件	cpsms_client と Check Point Management Server の間の通信を許可するには、CPSMS の $CPDIR/conf/sic_policy.conf に以下の行が含まれている必要があります。 # OPSEC applications defaultANY ; SAM_clients ; ANY ; sam ; sslca, local, sslca_comp# sam proxyANY ; Modules, DN_Mgmt ; ANY; sam ; sslcaANY ; ELA_clients ; ANY ; ela ; sslca, local, sslca_compANY ; LEA_clients ; ANY ; lea ; sslca, local, sslca_compANY ; CPMI_clients; ANY ; cpmi ; sslca, local, sslca_comp
必要なポート	以下のポートは QRadar Risk Manager によって使用され、CPSMS で開いている必要があります。 ポート 18190: Check Point Management Interface サービス（CPMI）用ポート ポート 18210: Check Point Internal CA Pull Certificate Service (FW1_ica_pull) 用ポート 18190 を CPMI の listen ポートとして使用できない場合は、CPSMS アダプター・ポート番号が、CPSMS の CPMI 用 $FWDIR/conf/fwopsec.conf ファイルにリストされている値と類似している必要があります。例: cpmi_server auth_port 18190。

Check Point Security Management Server HTTPS アダプター

Check Point Security Management Server HTTPS アダプターを使用して、バージョン R80 の Security Management Server により管理されるファイアウォール・ブレードに接続されたエンド・ノードをディスカバーおよびバックアップします。

Check Point Security Management Server HTTPS アダプターとともに以下のフィーチャーを使用できます。

- 静的 NAT
- 静的ルーティング
- HTTPS 接続プロトコル

以下のフィーチャーは、Check Point Security Management Server アダプターではサポートされていません。

- 動的オブジェクト (ネットワーク・オブジェクト)
- セキュリティー・ゾーン (ネットワーク・オブジェクト)
- RPC オブジェクト (サービス)
- DCE-RPC オブジェクト (サービス)
- ICMP サービス (サービス)
- GTP オブジェクト (サービス)
- 複合 TCP オブジェクト (サービス)
- Citrix TCP オブジェクト (サービス)
- その他のサービス (サービス)
- ユーザー・オブジェクト
- 時間オブジェクト
- アクセス制御ポリシー基準否定

注:

以前のバージョンの Check Point SMS から Check Point Security Management Server R80 にアップグレードする場合は、デバイスが「構成ソース管理」で記録されている場合でも、「**Check Point HTTPS** からディスカバー **(Discover From Check Point HTTPS)**」ディスカバリー方式を使用してそのデバイスを再ディスカバーする必要があります。

以下の表で、Check Point Security Management Server アダプターの統合要件を説明します。

表 7. Check Point Security Management Server アダプターの統合要件

統合要件	説明
バージョン	R80
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。 **注:** デバイスのディスカバリーを構成する前に、Check Point Security Management Server の資格情報を追加する必要があります。	ユーザー名 パスワード

表 7. *Check Point Security Management Server* アダプターの統合要件 (続き)

統合要件	説明
デバイスのディスカバリーの構成 QRadar でデバイスのディスカバリーを構成するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。 ディスカバリー方式を構成するには、「**Check Point HTTPS** からディスカバー **(Discover From Check Point HTTPS)**」をクリックし、Check Point Security Management Server の IP アドレスを入力してから「**OK**」をクリックします。	Check Point HTTPS からディスカバー
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	HTTPS
ユーザー・アクセス・レベルの要件	すべてに対する読み取り/書き込みアクセス権限
要求される API エンドポイント	以下の形式を使用して、リストされているコマンドをデバイスに発行します。 https://*<managemenet server>*:*<port>*/web_api/*<command>* show-simple-gateways show-hosts show-networks show-address-ranges show-groups show-groups-with-exclusion show-services-tcp show-services-udp show-service-groups show-packages show-access-rulebase show-nat-rulebase run-script show-task

Cisco CatOS

IBM Security QRadar Risk Manager は Cisco Catalyst (CatOS) アダプターをサポートします。

Cisco CatOS アダプターは、QRadar Risk Manager がアクセスできる CatOS ネットワーク・デバイスをバックアップすることで、デバイス構成を収集します。

Cisco CatOS アダプターとともに以下のフィーチャーを使用できます。

- 隣接データのサポート
- SNMP ディスカバリー
- 静的ルーティング
- Telnet 接続プロトコルおよび SSH 接続プロトコル

以下の表で、Cisco CatOS アダプターの統合要件を説明します。

表 8. Cisco CatOS アダプターの統合要件

統合要件	説明
バージョン	Catalyst 6500 シリーズ・シャーシのデバイス。 4.2 6.4 **制約事項:** CatOS 用アダプターは、重要なスイッチング・ポート構造だけをバックアップします。 Multilayer Switch Feature Card (MSFC) CatOS アダプターは Cisco IOS アダプターによりバックアップされます。 Firewall Services Module (FWSM) CatOS アダプターは Cisco ASA アダプターによりバックアップされます。
SNMP ディスカバリー	SNMP sysDescr 内の CATOS または Catalyst Operating System を突き合わせます。
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	ユーザー名 パスワード パスワードを有効にする **(Enable Password)**
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	以下のいずれかのサポート対象接続プロトコルを使用します。 **Telnet** **SSH**

表 8. Cisco CatOS アダプターの統合要件 (続き)

統合要件	説明
ログインしてデータを収集するためにアダプターが必要とするコマンド	show version whichboot show module show mod ver show system show flash devices show flash ... show snmp ifalias show port ifindex show interface show port show spantree show ip route show vlan show vtp domain show arp show cdp show cam dynamic show port status show counters

Cisco IOS

IBM Security QRadar Risk Manager は Cisco インターネット・オペレーティング・システム (IOS) アダプターをサポートします。

Cisco IOS アダプターは、IOS ベースのネットワーク・スイッチとルーターをバックアップすることで、デバイス構成を収集します。

Cisco IOS アダプターとともに以下のフィーチャーを使用できます。

- 隣接データのサポート
- 動的 NAT
- 静的 NAT
- SNMP ディスカバリー

- 静的ルーティング
- EIGRP 動的ルーティングおよび OSPF 動的ルーティング
- P2P トンネリング/VPN
- Telnet 接続プロトコルおよび SSH 接続プロトコル

以下の表で、Cisco IOS の統合要件を説明します。

表 *9. Cisco IOS* の統合要件

統合要件	説明
バージョン	IOS 12.0 から 15.1 (ルーターおよびスイッチ) Cisco Catalyst 6500 スイッチ (MSFC あり)。 MSFC カード・サービスの構成と状態をバックアップするには、Cisco IOS アダプターを使用します。 Cisco IOS 7600 シリーズ・ルーターに FWSM がある場合、FWSM のバックアップには Cisco ASA アダプターを使用します。
ユーザー・アクセス・レベル	ログインしてデータを収集するためにアダプターが必要とする各コマンドに対するコマンド実行特権レベルを持つユーザー。例えば、ローカル・データベース認証を使用するカスタム特権レベル 10 ユーザーを構成できます。 以下の例は、すべての `show ip` コマンドを特権レベル 10 に設定します。 `privilege exec level 10 show ip`
SNMP ディスカバリー	SNMP sysDescr 内の ISO または Cisco Internet Operation System を突き合わせます。
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	ユーザー名 パスワード ユーザー名を有効にする **(Enable Username)** (オプション) デバイスへのログイン時に特定の特権レベルを入力する必要がある場合、このフィールドを使用します。形式は `level-<n>` を使用します。 *n* は特権レベル [0-15] です。例えば、特権レベル 10 を入力するには、以下のコマンドを入力します。 `level-10` これにより、**`enable 10`** コマンドが Cisco デバイスに送信されます。 パスワードを有効にする **(Enable Password)** (オプション)

表 9. *Cisco IOS* の統合要件 (続き)

統合要件	説明
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	以下のいずれかのサポート対象接続プロトコルを使用します。 **Telnet** **SSH**

ログインしてデータを収集するためにアダプターが必要とするコマンド	`show access-lists`
	
	`show cdp neighbors detail`
	
	`show diag`
	
	`show diagbus`
	
	`show file systems`
	
	`show glbp`
	
	`show install running`
	
	`show interfaces`
	
	`show inventory`
	
	`show ip route ospf`
	
	`show mac address-table dynamic`
	
	`show module`
	
	`show mod version`
	
	`show object-group`
	
	`show power`
	
	`show snmp`
	
	`show spanning-tree`
	
	`show standby`
	
	`show startup-config`
	
	`show version`
	
	`show vlan`
	
	`show vrrp`
	
	`show vtp status`

表 9. *Cisco IOS* の統合要件 (続き)

統合要件	説明
ログインしてデータを収集するためにアダプターが必要とする show ip コマンド	show ip arp show ip bgp neighbors show ip eigrp interface show ip eigrp neighbors show ip eigrp topology show ip ospf show ip ospf interface show ip ospf neighbor show ip protocols show ip route eigrp terminal length 0

Cisco Nexus

IBM Security QRadar Risk Manager をネットワーク・デバイスと統合するには、必ず Cisco Nexus アダプターの要件を確認してください。

Cisco Nexus アダプターとともに以下のフィーチャーを使用できます。

- 隣接データのサポート
- SNMP ディスカバリー
- EIGRP 動的ルーティングおよび OSPF 動的ルーティング
- 静的ルーティング
- Telnet 接続プロトコルおよび SSH 接続プロトコル

以下の表で、Cisco Nexus アダプターの統合要件を説明します。

表 10. *Cisco Nexus* アダプターの統合要件

統合要件	説明
バージョンおよびサポートされる OS レベル	Nexus 5548: OS レベル 6.0 Nexus 7000 シリーズ: OS レベル 6.2 Nexus 9000 シリーズ: OS レベル 6.1
SNMP ディスカバリー	SNMP sysDescr 内の *Cisco NX-OS* と *Software* で終わるオプションの修飾ストリングを突き合わせます。 例: *(Cisco NXY-OS.* Software)*

表 *10. Cisco Nexus* アダプターの統合要件 *(*続き*)*

統合要件	説明
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	ユーザー名 パスワード パスワードを有効にする **(Enable Password)** 仮想デバイス・コンテキスト **(VDC)** を個別のデバイスとして追加する場合は、必要な資格情報によって以下の操作が可能になることを確認します。 VDC に対して有効なアカウントへのアクセス。 その仮想コンテキストでの必須コマンドの使用。
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	以下のいずれかのサポート対象接続プロトコルを使用します。 **Telnet** **SSH**

表 10. *Cisco Nexus* アダプターの統合要件 (続き)

統合要件	説明
ログインしてデータを収集するためにアダプターが必要とするコマンド	show hostname show version show vdc show vdc current-vdc switchto vdc <*vdc*>。ここで、*vdc* は、コマンド show vdc の入力時にリストされるアクティブな vdc です。 show snmp dir <*filesystem*> 。ここで、*filesystem* は、bootflash、slot0、volatile、log、logflash、または system です。 show running-config show startup-config show module show interface brief show interface snmp-ifindex show ip access-lists show vlan show vtp status show spanning-tree summary show object-group show interface <*interface*>。ここで、*interface* は、コマンド show running-config の入力時にリストされるいずれかのインターフェースです。 show hsrp show vrrp show vtp show glbp ｙshow ip eigrp show ip route eigrp show ip ospf show ip route ospf show ip rip show ip route rip

表 10. *Cisco Nexus* アダプターの統合要件 (続き)

統合要件	説明

テレメトリー・コマンド	`terminal length 0`
	
	`show hostname`
	
	`show vdc`
	
	`switchto vdc <vdc>`。ここで、*vdc* は、コマンド `show vdc` の入力時にリストされるアクティブな `vdc` です。
	
	`show cdp entry all`
	
	`show interface brief`
	
	`show ip arp`
	
	`show mac address-table`
	
	`show ip route`

Cisco Nexus デバイスの VDC の追加方法

Nexus ネットワーク・デバイスと仮想デバイス・コンテキスト (VDC) を IBM Security QRadar SIEM に追加するには、構成ソース管理を使用します。複数の VDC を IBM Security QRadar Risk Manager に追加するには 2 とおりの方法があります。

VDC を Nexus デバイスのサブデバイスまたは個別のデバイスとして追加できます。

仮想デバイス・コンテキストの表示

VDC を個別のデバイスとして追加すると、各 VDC はトポロジーでデバイスとして表示されます。

VDC をサブデバイスとして追加すると、VDC はトポロジーで表示されません。VDC は「構成モニター」ウィンドウで確認できます。

Cisco Nexus デバイスのサブデバイスとしての VDC の追加

Cisco Nexus デバイスのサブデバイスとして VDC を追加するには、構成ソース管理を使用します。

手順

1. 資格情報に指定されているユーザーに対し以下のコマンドを有効にします。
   - `show vdc` (admin context)
   - `switchto vdc x` (ここで *x* は、サポートされている VDC です。)

   「構成モニター (Configuration Monitor)」で、トポロジーの Nexus デバイスと VDCサブデバイスを確認できます。デバイスの表示について詳しくは、「*IBM Security QRadar Risk Manager* ユーザー・ガイド」を参照してください。
2. 構成ソース管理を使用して、Nexus デバイスの *admin context* IP アドレスを追加します。

詳しくは、 5 ページの『ネットワーク・デバイスの追加』を参照してください。

個別デバイスとしての VDC の追加

各 VDC (仮想デバイス・コンテキスト) を個別のデバイスとして追加するには、構成ソース管理を使用します。この方法を使用する場合、Nexus デバイスと VDC はトポロジーで表示されます。

トポロジーで Cisco Nexus デバイスと VDC を確認すると、シャーシ包含が個別に表示されています。

手順

1. 構成ソース管理を使用して、各 VDC の管理 IP アドレスを追加します。

   詳しくは、 5 ページの『ネットワーク・デバイスの追加』を参照してください。
2. 構成ソース管理を使用して、VDC の構成情報を取得します。
3. Cisco Nexus デバイスで Cisco Nexus CLI を使用して、アダプターに関連付けられているユーザー名に対して **switchto vdc** コマンドを無効にします。

   例: Cisco Nexus デバイスのユーザー名が *qrmuser* の場合は、以下のコマンドを入力します。

```
NexusDevice(config)# role name qrmuser
NexusDevice(config-role)# rule 1 deny command switchto vdc
NexusDevice(config-role)# rule 2 permit command show *
NexusDevice(config-role)# rule 3 permit command terminal
NexusDevice(config-role)# rule 4 permit command dir
```

Cisco セキュリティー・アプライアンス

IBM Security QRadar Risk Manager をネットワーク・デバイスと統合するには、必ず Cisco セキュリティー・アプライアンス アダプターの要件を確認してください。

Cisco Security Appliances アダプターとともに以下のフィーチャーを使用できます。

- 隣接データのサポート
- 静的 NAT
- SNMP ディスカバリー
- EIGRP 動的ルーティングおよび OSPF 動的ルーティング
- 静的ルーティング
- IPSEC トンネリング
- Telnet 接続プロトコルおよび SSH 接続プロトコル

Cisco セキュリティー・アプライアンス アダプターは、Cisco ファミリー・デバイスをバックアップすることでデバイス構成を収集します。Cisco セキュリティー・アプライアンス・アダプターは、以下のファイアウォールをサポートします。

- Cisco Adaptive Security Appliances (ASA) 5500 シリーズ

- Firewall Service Module (FWSM)
- Catalyst シャーシ内のモジュール
- 設定された Private Internet Exchange (PIX) デバイス。

注**:** Cisco ASA 透過コンテキストは QRadar Risk Manager トポロジー内に配置できないため、そのような透過コンテキストに対してパス検索を実行することはできません。

以下の表で、Cisco セキュリティー・アプライアンス アダプターの統合要件を説明します。

表 *11. Cisco* セキュリティー・アプライアンス アダプターの統合要件

統合要件	説明
バージョン	ASA: 8.2、8.4 から 9.1.7 PIX: 6.1, 6.3 FWSM: 3.1, 3.2

表 *11. Cisco* セキュリティー・アプライアンス アダプターの統合要件 (続き)

統合要件	説明

最小ユーザー・アクセス・レベル	特権レベル 5
	
	特権レベル 5 のアクセス・レベルでデバイスをバックアップできます。例えば、ローカル・データベース認証を使用するレベル 5 ユーザーを構成するには、次のコマンドを実行します。
	
	`aaa authorization command LOCAL`
	
	`aaa authentication enable console LOCAL`
	
	`privilege cmd level 5 mode exec command terminal`
	
	`privilege cmd level 5 mode exec command changeto` (*multi-context* のみ)
	
	`privilege show level 5 mode exec command running-config`
	
	`privilege show level 5 mode exec command startup-config`
	
	`privilege show level 5 mode exec command version`
	
	`privilege show level 5 mode exec command shun`
	
	`privilege show level 5 mode exec command names`
	
	`privilege show level 5 mode exec command interface`
	
	`privilege show level 5 mode exec command pager`
	
	`privilege show level 5 mode exec command arp`
	
	`privilege show level 5 mode exec command route`
	
	`privilege show level 5 mode exec command context`
	
	`privilege show level 5 mode exec command mac-address-table`

SNMP ディスカバリー	SNMP sysDescr 内の PIX、Adaptive Security Appliance、または Firewall Service Module を突き合わせます。
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	ユーザー名 パスワード パスワードを有効にする **(Enable Password)**

表 *11. Cisco* セキュリティー・アプライアンス アダプターの統合要件 (続き)

統合要件	説明
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	以下のいずれかのサポート対象接続プロトコルを使用します。 **Telnet** **SSH** **SCP**

表 *11. Cisco* セキュリティー・アプライアンス アダプターの統合要件 (続き)

統合要件	説明
アダプターがログインしてデータを収集するために必要なコマンド	changeto context <context> changeto system show running-config show startup-config show arp show context show interface show mac-address-table show names show ospf neighbor show route show shun show version terminal pager 0 show interface detail show crypto ipsec sa show eigrp topology show eigrp neighbors show firewall changeto context <context> コマンドは、ASA デバイスの各コンテキストに対して使用されます。 changeto system コマンドは、システムに *multi-context* 構成があるかどうかを検出し、*admin-context* を判別します。 changeto context コマンドは、changeto system コマンドに *multi-context* 構成または *admin-configuration* コンテキストが指定されている場合に必要です。 terminal pager コマンドは、ページング動作をオフにするために使用します。

F5 BIG-IP

IBM Security QRadar Risk Manager は F5 BIG-IP アダプターをサポートします。

F5 BIG-IP アダプターとともに以下のフィーチャーを使用できます。

- 隣接データのサポート
- 動的 NAT
- 静的 NAT
- SNMP ディスカバリー
- 静的ルーティング
- Telnet 接続プロトコルおよび SSH 接続プロトコル

Local Traffic Manager (LTM) を実行する F5 BIG-IP ロード・バランサー・アプライアンスがサポートされています。

F5 BIG-IP デバイスで、QRadar Risk Manager がバックアップの際に使用するユーザー名の「管理」役割、および端末アクセス用の拡張シェルを構成する必要があります。

以下の表で、F5 BIG-IP アダプターの統合要件を説明します。

表 *12. F5 BIG-IP* アダプターの統合要件

統合要件	説明
バージョン	10.1.1 11.4.1
SNMP ディスカバリー	SNMP sysDescr 内の F5 BIG-IP を突き合わせます。
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	ユーザー名 パスワード
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	**SSH**

表 *12. F5 BIG-IP* アダプターの統合要件 *(*続き*)*

統合要件	説明
ログインしてデータを収集するためにアダプターが必要とするコマンド	cat filename dmesg uptime route -n ip addr list snmpwalk -c public localhost 1.3.6.1.4.1.3375.2.1.2.4.3.2.1.1 snmpwalk -c public localhost 1.3.6.1.4.1.3375.2.1.2.4.3.2.1.2

表 12. F5 BIG-IP アダプターの統合要件 (続き)

統合要件	説明
ログインして bigpipe データを収集するためにアダプターが必要とするコマンド	bigpipe global bigpipe system hostname bigpipe platform bigpipe version show bigpipe db packetfilter bigpipe db packetfilter.defaultaction bigpipe packet filter list bigpipe nat list all bigpipe vlan show all bigpipe vlangroup list all bigpipe vlangroup bigpipe interface show all bigpipe interface all media speed bigpipe trunk all interfaces bigpipe stp show all bigpipe route all list all bigpipe mgmt show all bigpipe mgmt route show all bigpipe pool bigpipe self bigpipe virtual list all bigpipe snat list all bigpipe snatpool list all
ログインしてデータを収集するためにアダプターが必要とするコマンド	b db snat.anyipprotocol

表 12. F5 BIG-IP アダプターの統合要件 (続き)

統合要件	説明
ログインして tmsh データを収集するためにアダプターが必要とするコマンド	tmsh -q list sys global-settings hostname tmsh -q show sys version tmsh -q show sys hardware tmsh -q list sys snmp sys-contact tmsh -q show sys memory tmsh -q list /net interface all-properties tmsh -q list net trunk tmsh -q list /sys db packetfilter tmsh -q list /sys db packetfilter.defaultaction tmsh -q list /net packet-filter tmsh -q list /net vlan all-properties tmsh -q show /net vlan tmsh -q list /net vlan-group all all-properties tmsh -q list net tunnels
ログインして tmsh データを収集するためにアダプターが必要とするコマンド (続き)	tmsh -q show /net vlan-group tmsh -q list ltm virtual tmsh -q list ltm nat tmsh -q list ltm snatpool tmsh -q list ltm snat tmsh -q list sys db snat.anyipprotocol tmsh -q list net stp-globals all-properties tmsh -q list net stp priority tmsh -q list net stp all-properties tmsh -q list net route tmsh -q list sys management-ip tmsh -q list sys management-route tmsh -q list ltm pool tmsh -q list net self tmsh -q list net ipsec

表 12. F5 BIG-IP アダプターの統合要件 (続き)

統合要件	説明
収集されるファイル	/config/bigip.license /config/snmp/snmpd.conf /etc/passwd

Fortinet FortiOS

Fortinet FortiOS 用 IBM Security QRadar Risk Manager アダプターは、Fortinet オペレーティング・システム (FortiOS) を実行する Fortinet FortiGate アプライアンスをサポートします。

Fortinet FortiOS アダプターとともに以下のフィーチャーを使用できます。

- 静的 NAT
- 静的ルーティング
- Telnet 接続プロトコルおよび SSH 接続プロトコル

Fortinet FortiOS アダプターは Telnet または SSH 経由で FortiOS と対話します。以下のリストで、QRadar Risk Manager と Fortinet FortiOS アダプターのいくつかの制限を説明します。

- 地域ベースのアドレスと参照ポリシーは、QRadar Risk Manager ではサポートされていません。
- ID ベース、VPN、およびインターネット・プロトコル・セキュリティーのポリシーは、QRadar Risk Manager ではサポートされていません。
- Unified Threat Management (UTM) プロファイルを使用するポリシーは、Fortinet FortiOS アダプターではサポートされていません。レイヤー 3 ファイアウォール・ポリシーのみがサポートされています。
- ポリシー・ルートはサポートされていません。
- IP アドレスの一部が指定された仮想リンクまたは IP アドレスが指定されていない仮想リンクを持つ仮想ドメインはサポートされていません。

以下の表で、Fortinet FortiOS アダプターの統合要件を説明します。

表 13. Fortinet FortiOS アダプターの統合要件

統合要件	説明
バージョン	4.0 MR3 から 5.2.4
SNMP ディスカバリー	いいえ
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	ユーザー名 パスワード

表 13. *Fortinet FortiOS* アダプターの統合要件 (続き)

統合要件	説明
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	以下のいずれかのサポート対象接続プロトコルを使用します。 **Telnet** **SSH**
ユーザー・アクセス・レベルの要件	VDOM が有効化された Fortinet ファイアウォールに対する読み取り/書き込みアクセス権限 VDOM が有効化されていない Fortinet ファイアウォールに対する読み取り専用アクセス権限

ログインしてデータを収集するためにアダプターが必要とするコマンド	`config system console`
	
	`set output standard`
	注: `config system console` コマンドと `set output standard` コマンドでは、システム構成に対する読み取り/書き込み権限を持つユーザーが必要です。ページ編集が有効な読み取り専用ユーザーを使用している場合、Fortigate デバイスのバックアップ時に、パフォーマンスが大幅に低下します。
	
	`show system interface`
	
	`get hardware nic <variable>`
	
	`get system status`
	
	`get system performance status`
	
	`get router info routing-table static`
	
	`get test dnsproxy 6`
	
	`show firewall addrgrp`
	
	`show firewall address`
	
	`show full-configuration`
	
	`get firewall service predefined <variable>`
	
	`show firewall service custom`
	
	`show firewall service group`
	
	`show firewall policy`
	
	`show system zone`
	
	`show firewall vip`
	
	`show firewall vipgrp`
	
	`show firewall ippool`

表 13. *Fortinet FortiOS* アダプターの統合要件 (続き)

統合要件	説明
VDOM で使用するコマンド	`config global` により、グローバル構成モードに入ります `config vdom; edit <vdom-name>` により、VDOM 間を切り替えます

汎用 SNMP アダプター

IBM Security QRadar Risk Manager は、汎用 SNMP アダプターを使用して SNMP エージェントを実行するアプライアンスをサポートしています。

このアダプターは、SNMP 照会を使用して SNMP エージェントと対話します。

オブジェクト ID (OID) は SNMP MIB-2 に含まれており、すべての SNMP エージェントがこれらの OID を公開すると想定できます。

アダプターには以下の制限があります。

- 基本インターフェース情報と基本システム情報のみを収集します。ルールとルーティング情報は収集されません。
- 「構成ソース管理」UI に表示された場合でも、 アダプターは SNMPv3 を使用した AES 暗号化をサポートしていません。
- 「構成ソース管理」ウィンドウで、SNMPv3 を使用した AES 暗号化がサポートされるように見える場合でも、アダプターはこの暗号化をサポートしません。

以下の表で、汎用 SNMP アダプターの統合要件を説明します。

統合要件	説明
バージョン	SNMPv1, SNMPv2c, SNMPv3
隣接データのサポート	いいえ
SNMP ディスカバリー	いいえ
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	SNMPv1 および SNMPv2c で必要: **SNMP Get** コミュニティー **(SNMP Get Community)** SNMPv3 で必要: **SNMPv3** 認証ユーザー名 **(SNMPv3 Authentication Username)** SNMPv3 には、以下の資格情報のいずれか 1 つを使用できます。 **SNMPv3** 認証パスワード **(SNMPv3 Authentication Password)** **SNMPv3** プライバシー・パスワード **(SNMPv3 Privacy Password)**

統合要件	説明
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	以下のいずれかのサポート対象接続プロトコルを使用します。 **SNMPv1** **SNMPv2c** **MD5** を使用した **SNMPv3** **SHA** および **DES**
ログインしてデータを収集するためにアダプターが必要とするコマンド	SNMP Get コマンド .1.3.6.1.2.1.1.1.0 .1.3.6.1.2.1.1.2.0 .1.3.6.1.2.1.1.3.0 .1.3.6.1.2.1.1.4.0 .1.3.6.1.2.1.1.5.0 .1.3.6.1.2.1.1.6.0 SNMP Walk コマンド .1.3.6.1.2.1.2.2.1.2 .1.3.6.1.2.1.2.2.1.3 .1.3.6.1.2.1.2.2.1.4 .1.3.6.1.2.1.2.2.1.5 .1.3.6.1.2.1.2.2.1.6 .1.3.6.1.2.1.2.2.1.7 .1.3.6.1.2.1.4.20

HP Networking ProVision

IBM Security QRadar Risk Manager は HP Networking ProVision アダプターをサポートします。

HP Networking ProVision アダプターとともに以下のフィーチャーを使用できます。

- 隣接データのサポート
- SNMP ディスカバリー
- RIP 動的ルーティング
- Telnet 接続プロトコルおよび SSH 接続プロトコル

以下の表で、HP Networking ProVision アダプターの統合要件を説明します。

表 *14. HP Networking ProVision* アダプターの統合要件

統合要件	説明
バージョン	HP Networking ProVision Switches K/KA.15.X **制約事項:** Comware オペレーティング・システムを実行する HP スイッチは、このアダプターではサポートされていません。
SNMP ディスカバリー	sysDescr 内のバージョン番号 (形式: `HP(.*)Switch(.*)(revision [A-Z]{1,2}¥.(¥d+)¥.(¥d+))` を突き合わせます。
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	ユーザー名 パスワード パスワードを有効にする **(Enable Password)**
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	**SSH**

表 14. HP Networking ProVision アダプターの統合要件 (続き)

統合要件	説明
アダプターからデバイスに対して発行されるバックアップ操作コマンド	dmesgshow system power-supply getmib show access-list vlan <*vlan id*> show access-list show access-list <*name or number*> show access-list ports <*port number*> show config show filter show filter <*id*> show running-config show interfaces brief show interfaces <*interface id*> (各インターフェース用)。 show jumbos show trunks show lacp show module show snmp-server show spanning-tree show spanning-tree config show spanning-tree instance <*id or list*> (デバイスで構成されている各 spanning-tree 用) show spanning-tree mst-config show system information show version show vlans show vlans <*id*> (各 VLAN 用) show vrrp walkmib

表 14. *HP Networking ProVision* アダプターの統合要件 (続き)

統合要件	説明
アダプターからデバイスに対して発行される show ip バックアップ操作コマンド	show ip show ip route show ip odpf show ip odpf redistribute show ip rip show ip rip redistribute
テレメトリー・データおよび隣接データ・コマンド	getmib show arp show cdp neighbors show cdp neighbors detail *<port number>* show interfaces brief show interface show ip route show lldp info remote-device show lldp info remote-device *<port number>* show mac-address or show mac address show system information show vlans show vlans custom id state ipaddr ipmask walkmib

Juniper Networks JUNOS

IBM Security QRadar Risk Manager をネットワーク・デバイスと統合するには、必ず Juniper Networks JUNOS アダプターの要件を確認してください。

Juniper Networks JUNOS アダプターとともに以下のフィーチャーを使用できます。

- 隣接データのサポート
- SNMP ディスカバリー
- OSPF 動的ルーティング
- 静的ルーティング
- Telnet 接続プロトコルおよび SSH 接続プロトコル

以下の表で、Juniper Networks JUNOS アダプターの統合要件を説明します。

表 *15. Juniper Networks JUNOS* アダプターの統合要件

統合要件	説明
バージョン	10.4 11.2 から 12.3 13.2
SNMP ディスカバリー	SNMP sysOID: 1.3.6.1.4.1.2636 を突き合わせます。
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	ユーザー名 パスワード
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	以下のいずれかのサポート対象接続プロトコルを使用します。 **Telnet** **SSH** **SCP**

表 15. *Juniper Networks JUNOS* アダプターの統合要件 (続き)

統合要件	説明
ログインしてデータを収集するためにアダプターが必要とするコマンド	show version show system uptime show chassis hardware show chassis firmware show chassis mac-address show chassis routing-engine show configuration snmp show snmp mib walk system configure show configuration firewall show configuration firewall family inet6 show configuration security show configuration security zones show interfaces show interfaces filters show ospf interface detail show bgp neighbor show configuration routing-option show arp no-resolve show ospf neighbor show rip neighbor

Juniper Networks NSM

IBM Security QRadar Risk Manager アダプターは Juniper Networks NSM (Network and Security Manager) をサポートしています。

1 つの Juniper Networks デバイスをバックアップする場合や、Juniper Networks NSM コンソールからデバイス情報を入手する場合に、QRadar Risk Manager を使用できます。

Juniper Networks NSM (Network and Security Manager) コンソールには、Juniper Networks NSM コンソールにより管理される Juniper Networks ルーターおよびスイッチの構成情報とデバイス情報が含まれています。

Juniper Networks NSM では、HTTPS 接続プロトコルと SOAP 接続プロトコルを使用できます。

以下の表で、Juniper Networks NSM でサポートされる環境について説明します。

表 16. *QRadar Risk Manager* アダプターによりサポートされる *Juniper Networks NSM* の環境

サポートされる環境	説明
バージョン	NSM (Network and Security Manager) により管理される IDP アプライアンス
SNMP ディスカバリー	サポートされていません
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	ユーザー名 パスワード
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	以下のいずれかのサポート対象接続プロトコルを使用します。 **SOAP** **HTTP**

Juniper Networks ScreenOS

IBM Security QRadar Risk Manager をネットワーク・デバイスと統合するには、必ず Juniper Networks ScreenOS アダプターの要件を確認してください。

Juniper Networks ScreenOS アダプターとともに以下のフィーチャーを使用できます。

- 隣接データのサポート
- 動的 NAT
- 静的 NAT
- SNMP ディスカバリー
- 静的ルーティング
- Telnet 接続プロトコルおよび SSH 接続プロトコル

以下の表で、Juniper Networks ScreenOS アダプターの統合要件を説明します。

表 17. *Juniper Networks ScreenOS* アダプターの統合要件

統合要件	説明
バージョン	5.4 6.2
SNMP ディスカバリー	SNMP sysDescr 内の netscreen または SSG を突き合わせます。

表 17. *Juniper Networks ScreenOS* アダプターの統合要件 (続き)

統合要件	説明
必須資格情報パラメーター	ユーザー名 パスワード
サポート対象接続プロトコル	以下のいずれかのサポート対象接続プロトコルを使用します。 **Telnet** **SSH**

ログインしてデータを収集するためにアダプターが必要とするコマンド	`set console page 0`
	
	`get system`
	
	`get config`
	
	`get snmp`
	
	`get memory`
	
	`get file info`
	
	`get file`
	
	`get service`
	
	`get group address` *`zone group`*
	
	`get address`

表 17. *Juniper Networks ScreenOS* アダプターの統合要件 (続き)

統合要件	説明

ログインしてデータを収集するためにアダプターが必要とするコマンド (続き)	`get service group`
	
	`get service group` *`variable`*
	
	`get interface`
	
	`get interface` *`variable`*
	
	`get policy all`
	
	`get policy id` *`variable`*
	
	`get admin user`
	
	`get route`
	
	`get arp`
	
	`get mac-learn`
	
	`get counter statistics interface` *`variable`*
	
	ここで *zone* は、`get config` コマンドから返されるゾーン・データです。
	
	group は、`get config` コマンドから返されるグループ・データです。
	
	variable は、`get service group`、`get interface`、または `get policy id` コマンドから返されるデータのリストです。

Palo Alto

IBM Security QRadar Risk Manager は Palo Alto アダプターをサポートします。Palo Alto アダプターは、PAN-OS XML ベースの Rest API を使用して Palo Alto ファイアウォール・デバイスと通信します。

Palo Alto アダプターとともに以下のフィーチャーを使用できます。

- 隣接データのサポート
- 動的 NAT
- 静的 NAT
- SNMP ディスカバリー
- IPSEC トンネリング/VPN
- アプリケーション
- ユーザー/グループ
- HTTPS 接続プロトコル

注:

Palo Alto アダプターは、Palo Alto Panorama ネットワーク・セキュリティー管理システムによりデバイスにプッシュされる共有ポリシーをサポートしません。

以下の表で、Palo Alto アダプターの統合要件を説明します。

表 *18. Palo Alto* アダプターの統合要件

統合要件	説明
バージョン	PAN-OS バージョン 5.0 から 7.0
最小ユーザー・アクセス・レベル	ダイナミック・ブロック・リストが設定されている PA デバイスがシステムレベルのコマンドを実行するには、スーパーユーザー (全アクセス権限) が必要です。 その他のすべての PA デバイスにはスーパーユーザー (読み取り専用) が必要です。
SNMP ディスカバリー	SysDescr が「Palo Alto Networks(.*)series firewall」と一致するか、または sysOid が「panPA」と一致します。
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	ユーザー名 パスワード
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	**HTTPS**

バックアップ操作に使用する必須コマンド。	`/api/?type=op&cmd=<show><system><info></info></system>/show>`
	
	`/api/?type=op&cmd=<show><config><running></running></config></show>`
	
	`/api/?type=op&cmd=<show><interface>all</interface></show>`

バックアップ操作に使用するオプションのコマンド。	`/api/?type=op&cmd=<show><system><resources></resources></system></show>`
	
	`/api/?type=op&cmd=/config/predefined/service`
	
	`/api/?type=op&cmd=<request><system><external-list><show><name>$listName</name>< /show></external-list></system></request>` *`$listName`* はこのコマンド内の変数です。このコマンドは複数回実行されます。
	
	`/api/?type=op&cmd=<show><object><dynamic-address-group><all></all></dynamic-address-group></object></show>`
	
	`/api/?type=config&action=get&xpath=/config/predefined/application`

表 18. Palo Alto アダプターの統合要件 (続き)

統合要件	説明
テレメトリー・データおよび近隣データに使用する必須コマンド。	/api/?type=op&cmd=<show><system><info></info></system></show> /api/?type=op&cmd=<show><interface>all</interface></show> /api/?type=op&cmd=<show><routing><interface></interface></routing></show>
テレメトリー・データおよび近隣データに使用するオプションのコマンド。	/api/?type=op&cmd=<show><counter><interface>all</interface></counter></show> /api/?type=op&cmd=<show><arp>all</arp></show> <show><mac>all</mac></show> /api/?type=op&cmd=<show><arp>all</arp></show> /api/?type=op&cmd=<show><routing><route></route></routing></show>
GetApplication に使用する必須コマンド。	/api/?type=config&action=get&xpath=/config/predefined/application

Sidewinder

IBM Security QRadar Risk Manager は、SecureOS を実行する McAfee Enterprise Firewall (Sidewinder) アプライアンスをサポートしています。

Sidewinder アダプターとともに以下のフィーチャーを使用できます。

- 静的 NAT
- 静的ルーティング
- Telnet 接続プロトコルおよび SSH 接続プロトコル

Sidewinder アダプターは、Telnet または SSH 経由で CLI ベースの McAfee オペレーティング・システム (SecureOS) と対話します。

Sidewinder アダプターには以下の制限があります。

- レイヤー 3 ファイアウォール・ポリシーだけがサポートされています。これは、Sidewinder アプリケーション防御機能を使用するレイヤー 7 ポリシーがサポートされていないためです。
- ID ベース、地域ベース、および IPv6 のポリシーは QRadar Risk Manager でサポートされていないため、削除されます。

以下の表で、Sidewinder アダプターの統合要件を説明します。

表 19. Sidewinder アダプター

統合要件	説明
サポート対象のバージョン	8.3.2

表 19. *Sidewinder* アダプター (続き)

統合要件	説明
最小ユーザー・アクセス・レベル	admin **cf appdb list verbose=on** コマンドを使用してデータベースから事前定義サービス情報を取得するには、admin ユーザー・アクセス・レベルが必要です。
SNMP ディスカバリー	いいえ
必須資格情報パラメーター	ユーザー名 パスワード
サポート対象接続プロトコル	以下のいずれかのサポート対象接続プロトコルを使用します。 **SSH** **Telnet**

ログインしてデータを収集するためにアダプターが必要とするコマンド	`hostname`
	
	`uname -r`
	
	`uptime`
	
	`cf license q`
	
	`cf route status`
	
	`cf ipaddr q`
	
	`cf iprange q`
	
	`cf subnet q`
	
	`cf domain q`
	
	`cf domain q` からの各ドメイン出力に対して `"dig $address +noall +answer"` を使用します。
	
	`cf host q`
	
	`cf netmap q`
	
	`cf netgroup q`
	
	`cf appdb list verbose=on`
	
	`cf application q`
	
	`cf appgroup q`
	
	`cf policy q`
	
	`cf interface q`
	
	`cf zone q`

Sourcefire 3D Sensor

IBM Security QRadar Risk Manager をネットワーク・デバイスと統合するには、必ず Sourcefire 3D Sensor アダプターの要件を確認してください。

Sourcefire 3D Sensor アダプターとともに以下のフィーチャーを使用できます。

- IPS
- SSH 接続プロトコル

制限:

- 個別のアクセス制御ルールに付加されている侵入ポリシーは QRadar Risk Manager では使用されません。デフォルトの侵入ポリシーだけがサポートされています。
- NAT と VPN はサポートされていません。

以下の表で、Sourcefire 3D Sensor アダプターの統合要件を説明します。

表 *20. Sourcefire 3D Sensor* アダプターの統合要件

統合要件	説明
バージョン	5.2
サポートされている 3D センサー (シリーズ 2 デバイス)	3D500 3D1000 3D2000 3D2100 3D2500 3D3500 3D4500 3D6500 3D9900
SNMP ディスカバリー	いいえ
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	ユーザー名 パスワード
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	**SSH**

表 20. *Sourcefire 3D Sensor* アダプターの統合要件 (続き)

統合要件	説明

ログインしてデータを収集するためにアダプターが必要とするコマンド	`show version`
	`show memory`
	`show network`
	`show interfaces`
	`expert`
	`sudo`
	`su`
	`df`
	`hostname`
	`ip addr`
	`route`
	`cat`
	`find`
	`head`
	`mysql`

TippingPoint IPS アダプター

IBM Security QRadar Risk Manager は、TOS が稼働し、SMS により制御される TippingPoint IPS (侵入防止システム) アプライアンスをサポートしています。

TippingPoint IPS アダプターとともに以下のフィーチャーを使用できます。

- IPS
- Telnet 接続プロトコルおよび SSH+HTTPS 接続プロトコル

このアダプターは、以下のデバイスと対話する必要があります。

- Telnet または SSH 経由で TippingPoint オペレーティング・システム (TOS) を使用し、IPS と直接対話する。
- HTTPS を介した Web サービス API で TippingPoint Secure Management Server (SMS) と対話する。

TippingPoint SMS への接続は、SMS により管理される最新の Digital Vaccineシグネチャーを取得するには必須です。

このアダプターは、SMS の制御下にある IPS デバイスのみと連携します。バックアップを正常に行うには、SMS Web サービスが有効になっている必要があります。

以下のリストは、TippingPoint アダプターの制限です。

- QRadar Risk Manager は、IPS ルールおよびフィルターの送信元 IP アドレスおよび宛先 IP アドレスを処理しません。以下の TippingPoint の機能はサポートされていません。
  - トラフィック管理フィルター
  - プロファイルまたはフィルターの例外および制限
  - ユーザー定義フィルター
- 関連付けられている CVE がない IPS フィルターはモデリングされません。これは、IPS をどの QRadar 脆弱性にもマップできないためです。

以下の表で、TippingPoint アダプターの統合要件を説明します。

表 21. TippingPoint IPS アダプター

統合要件	説明
サポート対象のバージョン	TOS 3.6 および SMS 4.2
最小ユーザー・アクセス・レベル	IPS: Operator SMS: Operator (カスタム) *custom operator* ロールが設定されており、「SMS Web サービスへのアクセス (Access SMS Web Services)」オプションが有効なグループに属するユーザー。.
SNMP ディスカバリー	いいえ
必須資格情報パラメーター QRadar で資格情報を追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	以下の資格情報を入力します。 ユーザー名: *<IPS CLI username>* パスワード: *<IPS CLI password>* ユーザー名を有効にする **(Enable Username)**: *<SMS username>* パスワードを有効にする **(Enable Password)**: *<SMS password>*
サポート対象接続プロトコル QRadar でプロトコルを追加するには、管理者としてログインし、「管理」タブの「構成ソース管理」を使用します。	以下のいずれかのサポート対象接続プロトコルを使用します。 **Telnet** (IPS CLI の場合) **SSH** (IPS CLI の場合) **HTTPS** (SMS の場合)

表 21. *TippingPoint IPS* アダプター (続き)

統合要件	説明

ログインしてデータを収集するためにアダプターが必要とするコマンド	`show config`
	
	`show version`
	
	`show interface`
	
	`show host`
	
	`show sms`
	
	`show filter $filterNumber` (Digital Vaccine で検出される各シグネチャー用)

最新のシグネチャーを取得するために SMS に送信される API コマンド	`https://<sms_server>/dbAccess/tptDBServlet?method=DataDictionary&table=SIGNATURE&format=xml`

特記事項

本書は米国 IBM が提供する製品およびサービスについて作成したものです。

本書に記載の製品、サービス、または機能が日本においては提供されていない場合があります。日本で利用可能な製品、サービス、および機能については、日本 IBM の営業担当員にお尋ねください。本書で IBM 製品、プログラム、またはサービスに言及していても、その IBM 製品、プログラム、またはサービスのみが使用可能であることを意味するものではありません。これらに代えて、IBM の知的所有権を侵害することのない、機能的に同等の製品、プログラム、またはサービスを使用することができます。ただし、IBM 以外の製品とプログラムの操作またはサービスの評価および検証は、お客様の責任で行っていただきます。

IBM は、本書に記載されている内容に関して特許権 (特許出願中のものを含む) を保有している場合があります。本書の提供は、お客様にこれらの特許権について実施権を許諾することを意味するものではありません。実施権についてのお問い合わせは、書面にて下記宛先にお送りください。

〒103-8510
東京都中央区日本橋箱崎町19番21号
日本アイ・ビー・エム株式会社
法務・知的財産
知的財産権ライセンス渉外

IBM およびその直接または間接の子会社は、本書を特定物として現存するままの状態で提供し、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任を負わないものとします。国または地域によっては、法律の強行規定により、保証責任の制限が禁じられる場合、強行規定の制限を受けるものとします。

この情報には、技術的に不適切な記述や誤植を含む場合があります。本書は定期的に見直され、必要な変更は本書の次版に組み込まれます。IBM は予告なしに、随時、この文書に記載されている製品またはプログラムに対して、改良または変更を行うことがあります。

本書において IBM 以外の Web サイトに言及している場合がありますが、便宜のため記載しただけであり、決してそれらの Web サイトを推奨するものではありません。それらの Web サイトにある資料は、この IBM 製品の資料の一部ではありません。それらの Web サイトは、お客様の責任でご使用ください。

IBM は、お客様が提供するいかなる情報も、お客様に対してなんら義務も負うことのない、自ら適切と信ずる方法で、使用もしくは配布することができるものとします。

本プログラムのライセンス保持者で、(i) 独自に作成したプログラムとその他のプログラム (本プログラムを含む) との間での情報交換、および (ii) 交換された情報の相互利用を可能にすることを目的として、本プログラムに関する情報を必要とする方は、下記に連絡してください。

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

本プログラムに関する上記の情報は、適切な使用条件の下で使用することができますが、有償の場合もあります。

本書で説明されているライセンス・プログラムまたはその他のライセンス資料は、IBM 所定のプログラム契約の契約条項、IBM プログラムのご使用条件、またはそれと同等の条項に基づいて、IBM より提供されます。

記載されている性能データとお客様事例は、例として示す目的でのみ提供されています。実際の結果は特定の構成や稼働条件によって異なります。

IBM 以外の製品に関する情報は、その製品の供給者、出版物、もしくはその他の公に利用可能なソースから入手したものです。IBM は、それらの製品のテストは行っておりません。したがって、他社製品に関する実行性、互換性、またはその他の要求については確証できません。IBM 以外の製品の性能に関する質問は、それらの製品の供給者にお願いします。

IBM の将来の方向または意向に関する記述については、予告なしに変更または撤回される場合があり、単に目標を示しているものです。

表示されている IBM の価格は IBM が小売り価格として提示しているもので、現行価格であり、通知なしに変更されるものです。卸価格は、異なる場合があります。

本書には、日常の業務処理で用いられるデータや報告書の例が含まれています。より具体性を与えるために、それらの例には、個人、企業、ブランド、あるいは製品などの名前が含まれている場合があります。これらの名称はすべて架空のものであり、名称や住所が類似する企業が実在しているとしても、それは偶然にすぎません。

商標

IBM、IBM ロゴおよび ibm.com® は、世界の多くの国で登録された International Business Machines Corporation の商標です。他の製品名およびサービス名等は、それぞれ IBM または各社の商標である場合があります。現時点での IBM の商標リストについては、http://www.ibm.com/legal/copytrade.shtml をご覧ください。

Microsoft、Windows、Windows NT および Windows ロゴは、Microsoft Corporation の米国およびその他の国における商標です。

製品資料に関するご使用条件

これらの資料は、以下のご使用条件に同意していただける場合に限りご使用いただけます。

適用度

IBM Web サイトの「ご利用条件」に加えて、以下のご使用条件が適用されます。

個人使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、非商業的な個人による使用目的に限り複製することができます。ただし、IBM の明示的な承諾をえずに、これらの資料またはその一部について、二次的著作物を作成したり、配布 (頒布、送信を含む) または表示 (上映を含む) することはできません。

商業的使用

これらの資料は、すべての著作権表示その他の所有権表示をしていただくことを条件に、お客様の企業内に限り、複製、配布、および表示することができます。ただし、IBM の明示的な承諾をえずにこれらの資料の二次的著作物を作成したり、お客様の企業外で資料またはその一部を複製、配布、または表示することはできません。

権限

ここで明示的に許可されているもの以外に、資料や資料内に含まれる情報、データ、ソフトウェア、またはその他の知的所有権に対するいかなる許可、ライセンス、または権利を明示的にも黙示的にも付与するものではありません。

資料の使用が IBM の利益を損なうと判断された場合や、上記の条件が適切に守られていないと判断された場合、IBM はいつでも自らの判断により、ここで与えた許可を撤回できるものとさせていただきます。

お客様がこの情報をダウンロード、輸出、または再輸出する際には、米国のすべての輸出入 関連法規を含む、すべての関連法規を遵守するものとします。

IBM は、これらの資料の内容についていかなる保証もしません。これらの資料は、特定物として現存するままの状態で提供され、商品性の保証、特定目的適合性の保証および法律上の瑕疵担保責任を含むすべての明示もしくは黙示の保証責任なしで提供されます。

IBM オンラインでのプライバシー・ステートメント

サービス・ソリューションとしてのソフトウェアも含めた IBM ソフトウェア製品 (「ソフトウェア・オファリング」) では、製品の使用に関する情報の収集、エンド・ユーザーの使用感の向上、エンド・ユーザーとの対話またはその他の目的のために、Cookie はじめさまざまなテクノロジーを使用することがあります。多くの場合、ソフトウェア・オファリングにより個人情報が収集されることはありません。IBM の「ソフトウェア・オファリング」の一部には、個人情報を収集できる機能を

持つものがあります。ご使用の「ソフトウェア・オファリング」が、これらの Cookie およびそれに類するテクノロジーを通じてお客様による個人情報の収集を可能にする場合、以下の具体的事項を確認ください。

このソフトウェア・オファリングは、展開される構成に応じて、セッション管理および認証の目的のために、それぞれのお客様のセッション ID を、セッションごとの Cookie を使用して収集する場合があります。これらの Cookie は無効にできますが、その場合、これらを有効にした場合の機能を活用することはできません。

この「ソフトウェア・オファリング」が Cookie およびさまざまなテクノロジーを使用してエンド・ユーザーから個人を特定できる情報を収集する機能を提供する場合、 お客様は、このような情報を収集するにあたって適用される法律、ガイドライン等を遵守する必要があります。これには、エンドユーザーへの通知や同意の要求も含まれますがそれらには限られません。

このような目的での Cookie を含む様々なテクノロジーの使用の詳細については、IBM の『IBM オンラインでのプライバシー・ステートメント』(http://www.ibm.com/privacy/details/jp/ja/) の『クッキー、ウェブ・ビーコン、その他のテクノロジー』および『IBM Software Products and Software-as-a-Service Privacy Statement』(http://www.ibm.com/software/info/product-privacy) を参照してください。

Printed in Japan

日本アイ・ビー・エム株式会社
〒103-8510 東京都中央区日本橋箱崎町19-21