IBM Security QRadar Risk Manager
Version 7.2.2

Adapter-Konfigurationshandbuch

SC12-5040-00

IBM Security QRadar Risk Manager
Version 7.2.2

Adapter-Konfigurationshandbuch

SC12-5040-00

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 39 gelesen werden.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Security QRadar Risk Manager, Version 7.2.2., Adapter Configurations Guide,
IBM Form SC27-6248-00,
herausgegeben von International Business Machines Corporation, USA

Informationen, die nur für bestimmte Länder Gültigkeit haben und für Deutschland, Österreich und die Schweiz nicht zutreffen, wurden in dieser Veröffentlichung im Originaltext übernommen.

Möglicherweise sind nicht alle in dieser Übersetzung aufgeführten Produkte in Deutschland angekündigt und verfügbar; vor Entscheidungen empfiehlt sich der Kontakt mit der zuständigen IBM Geschäftsstelle.

Änderung des Textes bleibt vorbehalten.

Herausgegeben von:
TSC Germany
Kst. 2877
März 2014

Inhaltsverzeichnis

Einführung in die Konfiguration von Adaptern für QRadar Risk Manager v

Kapitel 1. Übersicht über Adapter 1
Adaptertypen 1

Kapitel 2. Adapter installieren 3
Adapter deinstallieren 4

Kapitel 3. Methoden zum Hinzufügen von Netzeinheiten 5
Netzeinheit hinzufügen 5
Von einer Juniper Networks NSM-Konsole verwaltete Einheiten hinzufügen 7
Von einer CPSMS-Konsole verwaltete Einheiten hinzufügen 8
Von SiteProtector verwaltete Einheiten hinzufügen 10

Kapitel 4. Unterstützte Adapter 13
BIG-IP 14
Check Point SecurePlatform Appliances 18
Check Point Security Management Server-Adapter 19
Cisco CatOS 20
Cisco IOS 22
Cisco Nexus 24
Methoden zum Hinzufügen von VDCs für Cisco Nexus-Einheiten 27
VDCs als untergeordnete Einheiten einer Cisco Nexus-Einheit hinzufügen 27
VDCs als separate Einheiten hinzufügen. 28
Cisco Security Appliances 29
HP Networking ProVision 31
Juniper Networks JUNOS 33
Juniper Networks NSM 35
Juniper Networks ScreenOS 35
Palo Alto 37

Bemerkungen 39
Marken 41
Hinweise zur Datenschutzrichtlinie 41

Index 43

Einführung in die Konfiguration von Adaptern für QRadar Risk Manager

IBM® Security QRadar Risk Manager ist eine Appliance für die Überwachung der Einheitenkonfiguration, die Simulation von Änderungen an Netzumgebungen und die Priorisierung von Risiken und Schwachstellen.

Zielgruppe

Netzadministratoren, die für die Installation und Konfiguration von Adaptern zuständig sind, müssen mit den Konzepten der Netzsicherheit und der Einheitenkonfiguration vertraut sein.

Technische Dokumentation

Die IBM Security QRadar-Produktdokumentation finden Sie einschließlich der übersetzten Dokumentation im IBM Knowledge Center(http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

Informationen zum Zugriff auf weitere technische Dokumentationen in der QRadar-Produktbibliothek finden Sie in den technischen Hinweisen der Accessing IBM Security Documentation (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Kontaktaufnahme mit der Kundenunterstützung

Informationen zur Kontaktaufnahme mit der Kundenunterstützung finden Sie in den technischen Hinweisen von Support and Download (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Erklärung zu geeigneten Sicherheitsvorkehrungen

Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Vorbeugung, Erkennung und Reaktion auf unzulässigen Zugriff innerhalb des Unternehmens und von außen. Unzulässiger Zugriff kann dazu führen, dass Informationen geändert, gelöscht, veruntreut oder missbräuchlich verwendet werden. Ebenso können Ihre Systeme beschädigt oder missbräuchlich verwendet werden, einschließlich zum Zweck von Attacken. Kein IT-System oder Produkt kann umfassend als sicher betrachtet werden. Kein einzelnes Produkt, kein einzelner Service und keine einzelne Sicherheitsmaßnahme können eine unzulässige Verwendung oder einen unzulässigen Zugriff mit vollständiger Wirksamkeit verhindern. IBM Systeme, Produkte und Services werden als Teil eines umfassenden Sicherheitskonzepts entwickelt, sodass die Einbeziehung zusätzlicher Betriebsprozesse erforderlich ist. Ferner wird vorausgesetzt, dass andere Systeme, Produkte oder Services so effektiv wie möglich sind. IBM übernimmt keine Gewähr dafür, dass Systeme, Produkte oder Services vor zerstörerischen oder unzulässigen Handlungen Dritter geschützt sind oder dass Systeme, Produkte oder Services Ihr Unternehmen vor zerstörerischen oder unzulässigen Handlungen Dritter schützen.

Kapitel 1. Übersicht über Adapter

Über Adapter wird IBM Security QRadar Risk Manager mit Ihren Netzeinheiten integriert. Über die passenden Adapter kann QRadar Risk Manager die Konfigurationsparameter von Netzeinheiten (z. B. Firewalls, Router und Switches) abfragen und importieren.

Netztopologie und Konfiguration

QRadar Risk Manager verwendet zur Erfassung von Netzkonfigurationen Adapter. Diese Adapter konvertieren die Konfigurationsdaten in ein für alle unterstützten Einheitenmodelle, Hersteller und Typen einheitliches Format. Die Daten benötigt QRadar Risk Manager zum Verständnis Ihrer Netztopologie und der Konfiguration Ihrer Netzeinheiten.

Zum Verbinden externer Einheiten mit dem Netz muss QRadar Risk Manager auf die Einheiten zugreifen können. Zum Zugriff auf diese Einheiten und zum Herunterladen der Konfigurationen verwendet QRadar Risk Manager konfigurierte Benutzerberechtigungsnachweise.

Integration von Netzeinheiten

Führen Sie zur Integration von Netzeinheiten mit QRadar Risk Manager die folgenden Schritte aus:

1. Konfigurieren Sie Ihre Netzeinheit mit dem erforderlichen Zugriff auf QRadar Risk Manager.
2. Installieren Sie den Adapter für Ihre Netzeinheit auf Ihrer QRadar Risk Manager-Appliance.
3. Fügen Sie Ihre Netzeinheiten in Configuration Source Management zu QRadar Risk Manager hinzu.
4. Definieren Sie das Kommunikationsverfahren (Protokoll) für die Kommunikation mit Ihren Netzeinheiten.

   Weitere Informationen finden Sie im *IBM Security QRadar Risk Manager User Guide*.

Falls sich zwischen QRadar Risk Manager und Ihren Netzeinheiten keine Kommunikation herstellen lässt, lesen Sie den Abschnitt zum Konfigurationstoolkit für getrennte Verbindungen im *IBM Security QRadar Risk Manager User Guide*.

Adaptertypen

IBM Security QRadar Risk Manager unterstützt verschiedene Adaptertypen.

Die folgenden Adapter werden unterstützt:

- BIG-IP
- Check Point SecurePlatform Appliances
- Cisco Internet Operating System (IOS)
- Cisco Catalyst (CatOS)
- Check Point Security Management Server
- Cisco Security Appliances

- HP Networking ProVision
- Juniper Networks ScreenOS
- Juniper Networks JUNOS
- Juniper Networks NSM
- Palo Alto

Kapitel 2. Adapter installieren

Zur Installation eines Adapters müssen Sie den Adapter auf Ihre IBM Security QRadar SIEM-Konsole herunterladen und die Adapterdateien dann in IBM Security QRadar Risk Manager kopieren.

Vorbereitende Schritte

Adapter stehen auf Fix Central (www.ibm.com/support/fixcentral/) zum Download bereit. Die RPM-Dateien sind im Download enthalten.

Nach der Einrichtung einer erstmaligen Verbindung ist QRadar SIEM-Konsole die einzige Einheit, die direkt mit QRadar Risk Manager kommunizieren kann.

Vorgehensweise

1. Melden Sie sich über SSH als Rootbenutzer auf Ihrer QRadar SIEM-Konsole an.
2. Laden Sie die Adapterdatei von der IBM Support-Website (www.ibm.com/support) auf Ihre QRadar SIEM-Konsole herunter.
3. Geben Sie zum Kopieren der Adapterdatei von Ihrer QRadar SIEM-Konsole in QRadar Risk Manager folgenden Befehl ein:

   `scp` *`Adapter`*`.rpm root@`*`IP-Adresse`*

   IP-Adresse ist die IP-Adresse oder der Hostname von QRadar Risk Manager.

   Beispiel: `scp adapters.cisco.ios-2011_05-205181.noarch.rpm root@100.100.100.100:`
4. Geben Sie auf Ihrer QRadar Risk Manager-Appliance das Kennwort für den Rootbenutzer ein.
5. Melden Sie sich von Ihrer QRadar SIEM-Konsole über SSH als Rootbenutzer auf Ihrer QRadar Risk Manager-Appliance an.
6. Führen Sie im Stammverzeichnis mit der Adapterdatei den folgenden Befehl aus, um den Adapter zu installieren:

   `rpm -Uvh` *`RPM-Dateiname`*

   Beispiel: `rpm -Uvh adapters.cisco.ios-2011_05-205181.noarch.rpm`
7. Geben Sie für den Neustart der Services für den ziptie-Server und zum Abschluss der Installation folgenden Befehl ein:

   `service ziptie-server restart`

   Wichtig: Durch den Neustart der Services für den ziptie-Server werden zur Zeit aktive Einheitenbackups in Configuration Source Management unterbrochen.

Adapter deinstallieren

Zum Entfernen eines Adapters aus IBM Security QRadar Risk Manager verwenden Sie den Befehl **rpm**.

Vorgehensweise

1. Melden Sie sich über SSH als Rootbenutzer auf der IBM Security QRadar SIEM-Konsole an.
2. Geben Sie zum Deinstallieren eines Adapters folgenden Befehl ein:

   `rpm -e Adapterdatei`

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

Kapitel 3. Methoden zum Hinzufügen von Netzeinheiten

Zum Hinzufügen von Netzeinheiten zu IBM Security QRadar Risk Manager verwenden Sie Configuration Source Management.

In der folgenden Tabelle werden die Methoden zum Hinzufügen von Netzeinheiten beschrieben.

Tabelle 1. Methoden zum Hinzufügen von Netzeinheiten zu QRadar Risk Manager

Methode	Beschreibung
Add Device (Einheit hinzufügen)	Fügt eine Einheit hinzu.
Discover Devices (Einheiten erkennen)	Fügt mehrere Einheiten hinzu.
Discover NSM (NSM erkennen)	Fügt von der Juniper Networks NSM-Konsole verwaltete Einheiten hinzu.
Discover CPSMS From SiteProtector (CPSMS von SiteProtector erkennen)	Fügt von einem Check Point Security Manager Server (CPSMS) verwaltete Einheiten hinzu.
Discover (Erkennen)	Fügt Einheiten von SiteProtector hinzu.

Netzeinheit hinzufügen

Zum Hinzufügen einer Netzeinheit zu IBM Security QRadar Risk Manager verwenden Sie Configuration Source Management.

Vorbereitende Schritte

Lesen Sie zunächst, welche Softwareversionen unterstützt, welche Berechtigungsnachweise benötigt und welche Befehle für Ihre Netzeinheiten verwendet werden. Weitere Informationen finden Sie im Abschnitt Kapitel 4, „Unterstützte Adapter", auf Seite 13.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung (Admin)**.
2. Klicken Sie im Navigationsmenü **Verwaltung** auf **Plug-ins**.
3. Klicken Sie im Bereich **Risk Manager** auf **Configuration Source Management**.
4. Klicken Sie im Navigationsmenü auf **Berechtigungsnachweise**.
5. Klicken Sie im Bereich **Network Groups** (Netzgruppen) auf **Add a new network group** (Neue Netzgruppe hinzufügen).
   a. Geben Sie einen Namen für die Netzgruppe ein und klicken Sie auf **OK**.
   b. Geben Sie die IP-Adresse Ihrer Einheit ein und klicken Sie auf **Hinzufügen**.

      Sie können eine IP-Adresse, einen IP-Adressbereich, ein CIDR-Teilnetz oder einen Platzhalter eingeben. Für einen Platzhalter geben Sie zum Beispiel `10.1.*.*` ein, für ein CIDR-Teilnetz `10.2.1.0/24`.

      Einschränkung: Geben Sie Einheitenadressen, die bereits in anderen Netzgruppen vorkommen, nicht ein zweites Mal in Configuration Source Management ein.

c. Vergewissern Sie sich, dass die Adressen, die Sie hinzufügen, neben dem Feld **Add address** (Adresse hinzufügen) im Feld **Network address** (Netzadresse) angezeigt werden.

d. Wiederholen Sie die vorangegangenen zwei Schritte für jede IP-Adresse, die Sie hinzufügen möchten.

6. Klicken Sie im Bereich **Credentials** (Berechtigungsnachweise) auf **Add a new credential set** (Neue Berechtigungsnachweisgruppe hinzufügen).

   a. Geben Sie einen Namen für die Berechtigungsnachweisgruppe ein und klicken Sie auf **OK**.

   b. Wählen Sie den Namen der von Ihnen erstellten Berechtigungsnachweisgruppe aus und geben Sie die angefragten Parameterwerte ein.

      In der folgenden Tabelle werden die Parameter beschrieben.

Tabelle 2. Parameter für die Berechtigungsnachweise

Parameter	Beschreibung
Benutzername	Ein gültiger Benutzername für die Anmeldung beim Adapter. Für Adapter ist für den Benutzernamen und das Kennwort Zugriff auf verschiedene Dateien, wie die folgenden, erforderlich: • `rule.C` • `objects.C` • `implied_rules.C` • `Standard.PF`
Kennwort	Das Kennwort für die Einheit.
Kennwort aktivieren	Das Kennwort für die Authentifizierung auf zweiter Ebene. Dieses Kennwort ist nur erforderlich, wenn bei der Authentifizierung nach den Benutzerberechtigungsnachweisen im Expertenmodus gefragt wird.
SNMP Get Community	Optional
SNMPv3 Authentication Username (Benutzername für die SNMPv3-Authentifizierung)	Optional
SNMPv3 Authentication Password (Kennwort für die SNMPv3-Authentifizierung)	Optional
SNMPv3 Privacy Password (Datenschutzkennwort für SNMPv3)	Optional Das Protokoll für die Entschlüsselung von SNMPv3-Alarmnachrichten.

Einschränkung: Wenn Ihre Netzeinheit eine der folgenden Voraussetzungen erfüllt, müssen Sie in Configuration Source Management Protokolle konfigurieren:

- Ihre Einheit verwendet für das Kommunikationsprotokoll keinen Standardport.
- Sie möchten, dass das von IBM Security QRadar Risk Manager verwendete Protokoll mit bestimmten IP-Adressen kommuniziert.

Weitere Informationen zum Konfigurieren von Quellen finden Sie im *IBM Security QRadar Risk Manager User Guide*.

7. Fügen Sie über das Navigationsmenü eine Einheit hinzu.
   - Klicken Sie zum Hinzufügen einer Einheit auf **Add Device** (Einheit hinzufügen).
   - Klicken Sie zum Hinzufügen mehrerer IP-Adressen für Netzeinheiten auf **Discover Devices** (Einheiten erkennen).
8. Geben Sie die IP-Adresse der Einheit ein, wählen Sie den Adaptertyp aus und klicken Sie auf **Hinzufügen**.

   Noch nicht gesicherte Einheiten sind in der Einheitenliste durch ein blaues Fragezeichen gekennzeichnet.
9. Wählen Sie die Einheit aus, die Sie der Einheitenliste hinzugefügt haben, und klicken Sie dann auf **Backup** (Sichern).
10. Wiederholen Sie diese Schritte für jeden Netzeinheitentyp, den Sie hinzufügen möchten.

Nächste Schritte

Nachdem Sie die erforderlichen Einheiten hinzugefügt haben, können Sie die Protokolle konfigurieren. Weitere Informationen finden Sie im *IBM Security QRadar Risk Manager User Guide*.

Von einer Juniper Networks NSM-Konsole verwaltete Einheiten hinzufügen

Zum Hinzufügen aller Einheiten von einer Juniper Networks NSM-Konsole zu IBM Security QRadar Risk Manager verwenden Sie Configuration Source Management.

Vorbereitende Schritte

Lesen Sie zunächst, welche Softwareversionen unterstützt, welche Berechtigungsnachweise benötigt und welche Befehle für Ihre Netzeinheiten verwendet werden. Weitere Informationen hierzu finden Sie im Abschnitt Kapitel 4, „Unterstützte Adapter", auf Seite 13.

Vorgehensweise

1. Klicken Sie in IBM Security QRadar SIEM auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü **Verwaltung** auf **Plug-ins**.
3. Klicken Sie im Bereich **Risk Manager** auf **Configuration Source Management**.
4. Klicken Sie im Navigationsmenü auf **Berechtigungsnachweise**.
5. Klicken Sie im Bereich **Network Groups** (Netzgruppen) auf **Add a new network group** (Neue Netzgruppe hinzufügen).
   a. Geben Sie einen Namen für die Netzgruppe ein und klicken Sie auf **OK**.
   b. Geben Sie die IP-Adresse Ihrer Einheit ein und klicken Sie auf **Hinzufügen**.

      Sie können eine IP-Adresse, einen IP-Adressbereich, ein CIDR-Teilnetz oder einen Platzhalter eingeben. Für einen Platzhalter geben Sie zum Beispiel `10.1.*.*` ein, für ein CIDR-Teilnetz `10.2.1.0/24`.

      Einschränkung: Geben Sie Einheitenadressen, die bereits in anderen Netzgruppen vorkommen, nicht ein zweites Mal in Configuration Source Management ein.

c. Vergewissern Sie sich, dass die Adressen, die Sie hinzufügen, neben dem Feld **Add address** (Adresse hinzufügen) im Feld **Network address** (Netzadresse) angezeigt werden.

d. Wiederholen Sie die vorangegangenen zwei Schritte für jede IP-Adresse, die Sie hinzufügen möchten.

6. Klicken Sie im Bereich **Credentials** (Berechtigungsnachweise) auf **Add a new credential set** (Neue Berechtigungsnachweisgruppe hinzufügen).

   a. Geben Sie einen Namen für die Berechtigungsnachweisgruppe ein und klicken Sie auf **OK**.

   b. Wählen Sie den Namen der von Ihnen erstellten Berechtigungsnachweisgruppe aus und geben Sie die angefragten Parameterwerte ein.

      In der folgenden Tabelle werden die Parameter beschrieben.

Tabelle 3. Parameter für die Berechtigungsnachweise der Juniper NSM-Web-Services

Parameter	Beschreibung
Benutzername	Ein gültiger Benutzername für die Anmeldung bei Juniper NSM-Web-Services. Der Benutzer muss auf den Juniper NSM-Server zugreifen können.
Kennwort	Das Kennwort für die Einheit.
Kennwort aktivieren	Nicht erforderlich.

Einschränkung: Juniper Networks NSM unterstützt kein SNMP.

7. Klicken Sie im Navigationsmenü auf **Discover from NSM** (Von NSM erkennen).
8. Geben Sie die Werte für die IP-Adresse und die Benutzerberechtigungsnachweise ein und klicken Sie dann auf **OK** und auf **GO** (Los).
9. Wählen Sie die Einheit aus, die Sie der Einheitenliste hinzugefügt haben, und klicken Sie dann auf **Backup** (Sichern) und auf **Yes** (Ja).

Nächste Schritte

Nachdem Sie die erforderlichen Einheiten hinzugefügt haben, können Sie die Protokolle konfigurieren. Weitere Informationen hierzu finden Sie im *IBM Security QRadar Risk Manager User Guide*.

Von einer CPSMS-Konsole verwaltete Einheiten hinzufügen

Zum Hinzufügen aller Einheiten eines Check Point Security Manager Server (CPSMS) zu IBM Security QRadar Risk Manager verwenden Sie Configuration Source Management.

Vorbereitende Schritte

Lesen Sie zunächst, welche Softwareversionen unterstützt, welche Berechtigungsnachweise benötigt und welche Befehle für Ihre Netzeinheiten verwendet werden. Weitere Informationen hierzu finden Sie im Abschnitt Kapitel 4, „Unterstützte Adapter", auf Seite 13.

Für dieses Verfahren benötigen Sie den PSEC Entity SIC-Namen, den OPSEC Application Object SIC-Namen und das einmalig verwendbare Pull Certificate-Kennwort. Weitere Informationen hierzu finden Sie in Ihrer CPSMS-Dokumentation.

Anmerkung: Die Funktion "Device Import" (Geräteimport) ist mit CPSMS-Adaptern nicht kompatibel.

Informationen zu diesem Vorgang

Dieses Verfahren muss für jeden CPSMS wiederholt werden, für den Sie die Erkennung der von ihm verwalteten Firewalls aktivieren möchten.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung**.
2. Klicken Sie im Navigationsmenü **Verwaltung** auf **Plug-ins**.
3. Klicken Sie im Bereich **Risk Manager** auf **Configuration Source Management**.
4. Klicken Sie im Navigationsmenü auf **Berechtigungsnachweise**.
5. Klicken Sie im Bereich **Network Groups** (Netzgruppen) auf **Add a new network group** (Neue Netzgruppe hinzufügen).
   a. Geben Sie einen Namen für die Netzgruppe ein und klicken Sie auf **OK**.
   b. Geben Sie die IP-Adresse Ihrer CPSMS-Einheit ein und klicken Sie auf **Hinzufügen**.

      Einschränkung: Geben Sie Einheitenadressen, die bereits in anderen Netzgruppen vorkommen, nicht ein zweites Mal in Configuration Source Management ein.
   c. Vergewissern Sie sich, dass die Adressen, die Sie hinzufügen, neben dem Feld **Add address** (Adresse hinzufügen) im Feld **Network address** (Netzadresse) angezeigt werden.
6. Klicken Sie im Bereich **Credentials** (Berechtigungsnachweise) auf **Add a new credential set** (Neue Berechtigungsnachweisgruppe hinzufügen).
   a. Geben Sie einen Namen für die Berechtigungsnachweisgruppe ein und klicken Sie auf **OK**.
   b. Wählen Sie den Namen der von Ihnen erstellten Berechtigungsnachweisgruppe aus und geben Sie einen gültigen Benutzernamen und ein gültiges Kennwort für die Einheit ein.
7. Geben Sie den OPSEC Entity SIC-Namen des CPSMS ein, der die zu erkennenden Firewalleinheiten verwaltet. Beispiel: `CN=cp_mgmt_vm230-cpsms2-gw3,O=vm226-CPSMS..bs7ocx`
8. Geben Sie den OPSEC Application Object SIC-Namen ein, der mit der Anwendung Check Point SmartDashboard auf dem CPSM erstellt wurde. Beispiel: `CN=cpsms230,O=vm226-CPSMS..bs7ocx`
9. Rufen Sie ein OPSEC-SSL-Zertifikat ab:
   a. Klicken Sie auf **Get Certificate** (Zertifikat abrufen).
   b. Geben Sie im Feld **Certificate Authority IP** (IP der Zertifizierungsstelle) die IP-Adresse der Zertifizierungsstelle ein.
   c. Geben Sie im Feld **Pull Certificate Password** (Pull Certificate-Kennwort) das einmalig verwendbare Kennwort für die OPSEC-Anwendung ein.
   d. Klicken Sie auf **OK**.
10. Klicken Sie auf **OK**.
11. Klicken Sie auf **Discover From Check Point SMS** (Von Check Point SMS erkennen) und geben Sie dann die IP-Adresse des CPSMS ein.
12. Klicken Sie auf **OK**.

13. Wiederholen Sie diese Schritte für jede CPSMS-Einheit, die Sie hinzufügen möchten.

Nächste Schritte

Wenn Sie alle erforderlichen Einheiten hinzugefügt haben, können Sie diese sichern und dann in der Topologie anzeigen.

Von SiteProtector verwaltete Einheiten hinzufügen

Fügen Sie in Configuration Source Management Einheiten aus SiteProtector zu IBM Security QRadar Risk Manager hinzu.

Vorbereitende Schritte

Zum Hinzufügen dieser Einheiten müssen die Adapter für IBM Internet Security Systems GX und IBM Security SiteProtector System installiert sein.

Das Microsoft SQL-Protokoll muss für Microsoft SQL Server-Port 1433 konfiguriert sein.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung (Admin)**.
2. Klicken Sie im Navigationsmenü **Verwaltung** auf **Plug-ins**.
3. Klicken Sie im Bereich **Risk Manager** auf **Configuration Source Management**.
4. Klicken Sie im Navigationsmenü auf **Berechtigungsnachweise**.
5. Klicken Sie im Bereich **Network Groups** (Netzgruppen) auf **Add a new network group** (Neue Netzgruppe hinzufügen).
   a. Geben Sie einen Namen für die Netzgruppe ein und klicken Sie auf **OK**.
   b. Geben Sie die IP-Adresse Ihrer SiteProtector-Einheit ein und klicken Sie auf **Hinzufügen**.
   c. Vergewissern Sie sich, dass die Adressen, die Sie hinzufügen, neben dem Feld **Add address** (Adresse hinzufügen) im Feld **Network address** (Netzadresse) angezeigt werden.
6. Klicken Sie im Bereich **Credentials** (Berechtigungsnachweise) auf **Add a new credential set** (Neue Berechtigungsnachweisgruppe hinzufügen).
   a. Geben Sie einen Namen für die Berechtigungsnachweisgruppe ein und klicken Sie auf **OK**.
   b. Wählen Sie den Namen der von Ihnen erstellten Berechtigungsnachweisgruppe aus und geben Sie einen gültigen Benutzernamen und ein gültiges Kennwort für die Einheit ein.

      Einschränkung: Als Benutzername und Kennwort werden die gleichen Berechtigungsnachweise verwendet, wie für die von SiteProtector verwendete Microsoft SQL Server-Datenbank.
7. Klicken Sie auf **OK**.
8. Klicken Sie auf **Discover From SiteProtector** (Aus SiteProtector erkennen) und geben Sie die IP-Adresse von SiteProtector ein.
9. Klicken Sie auf **OK**.

Nächste Schritte

Wenn Sie alle erforderlichen Einheiten hinzugefügt haben, können Sie diese sichern und dann in der Topologie anzeigen.

Kapitel 4. Unterstützte Adapter

IBM Security QRadar Risk Manager lässt sich mit Sicherheitsprodukten der verschiedensten Hersteller und Anbieter integrieren.

Die Liste der unterstützten Adapter und die zugehörige Dokumentation wächst beständig. Falls Sie für Ihre Netzeinheit keinen Adapter finden, wenden Sie sich an Ihren IBM Vertriebsbeauftragten.

Für jeden unterstützten Adapter werden folgende Informationen bereitgestellt:

Unterstützte Versionen

Hier werden der Produktname und die unterstützten Versionen angegeben.

Neighbor-Datenunterstützung

Hier wird angegeben, ob für diesen Adapter Neighbor-Daten unterstützt werden. Wenn Ihre Einheit Neighbor-Daten unterstützt, erhalten Sie diese über das Simple Network Management Protocol (SNMP) und eine Befehlszeilenschnittstelle (CLI) von der Einheit.

SNMP-Erkennung

Hier wird angegeben, ob die Einheit die Erkennung mittels SNMP zulässt.

Generische SNMP-Einheiten verfügen über keine Routen und übertragen daher keinen Datenverkehr.

Erforderliche Parameter für Berechtigungsnachweise

Hier werden die Zugriffsanforderungen für die Verbindung zwischen QRadar Risk Manager und der Einheit angegeben.

Die Berechtigungsnachweise für eine Einheit können in Configuration Source Management festgelegt werden. Die in QRadar Risk Manager konfigurierten Berechtigungsnachweise und die Berechtigungsnachweise auf der Einheit müssen identisch sein.

Die Positionen nicht erforderlicher Parameter lassen Sie einfach leer.

Verbindungsprotokolle

Hier werden die für die Netzeinheit unterstützten Protokolle angegeben.

Erforderliche Befehle

Hier werden die Befehle aufgelistet, die der Adapter zur Anmeldung und Erfassung der Daten benötigt.

Zur Ausführung dieser Befehle auf dem Adapter müssen die in QRadar Risk Manager bereitgestellten Berechtigungsnachweise über die entsprechenden Berechtigungen verfügen.

Erfasste Dateien

Hier werden die Dateien aufgelistet, auf die der Adapter Zugriff benötigt. Der Adapter muss über die entsprechenden Berechtigungsnachweise für den Zugriff auf diese Dateien verfügen.

BIG-IP

IBM Security QRadar Risk Manager unterstützt den BIG-IP-Adapter.

In der folgenden Tabelle werden die Integrationsanforderungen für den BIG-IP-Adapter beschrieben.

Tabelle 4. Integrationsanforderungen für den BIG-IP-Adapter

Integrationsanforderungen	**Beschreibung**
Versionen	BIG-IP-Version 10 und höher
Neighbor-Datenunterstützung	Unterstützt
SNMP-Erkennung	Gleicht in der SNMP sysDescr BIG-IP ab
Erforderliche Parameter für Berechtigungsnachweise	`Benutzername` `Kennwort`
Verbindungsprotokolle	Telnet SSH

Tabelle 4. Integrationsanforderungen für den BIG-IP-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`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`
	`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`
	`b db snat.anyipprotocol`

Tabelle 4. Integrationsanforderungen für den BIG-IP-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Fortsetzung	`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 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`
	
	`tmsh -q list net tunnels`

Tabelle 4. Integrationsanforderungen für den BIG-IP-Adapter (Forts.)

Integrationsanforderungen	**Beschreibung**

Erfasste Dateien	`/config/bigip.license`
	
	`/config/snmp/snmpd.conf`
	
	`/etc/passwd`

Check Point SecurePlatform Appliances

IBM Security QRadar Risk Manager unterstützt den Check Point SecurePlatform Appliances-Adapter.

In der folgenden Tabelle werden die Integrationsanforderungen für den Check Point SecurePlatform Appliances-Adapter beschrieben.

Tabelle 5. Integrationsanforderungen für den Check Point SecurePlatform Appliances-Adapter

Integrationsanforderungen	Beschreibung
Versionen	Version R65 und höher **Einschränkung:** Nokia IPSO-Appliances werden für Backups nicht unterstützt.
Neighbor-Datenunterstützung	Nicht unterstützt
SNMP-Erkennung	Gleicht in der SNMP sysDescr NGX ab

Erforderliche Parameter für Berechtigungsnachweise	`Benutzername`
	
	`Kennwort`
	
	`Kennwort aktivieren` (Expertenmodus)

Verbindungsprotokolle	Telnet SSH

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`hostname`
	
	`dmidecode`
	
	`ver`
	
	`uptime`
	
	`dmesg`
	
	`route -n`
	
	`show users`
	
	`ifconfig -a`
	
	`echo $FWDIR`

Erfasste Dateien	`rules.C`
	
	`objects.C`
	
	`implied_rules.C`
	
	`Standard.pf`
	
	`snmpd.com`

Check Point Security Management Server-Adapter

Mit dem Check Point Security Management Server (CPSMS)-Adapter erkennen und sichern Sie die von CPSMS verwalteten Endknoten. Auf diesen Endknoten werden CheckPoint FireWall-1 und die Produktfamilie VPN-1 ausgeführt.

Der CPSMS-Adapter basiert auf der CPMI OPSEC-SDK-API-Bibliothek.

Aufwärtskompatibilität für CPMI-Verbindungen

CPMI-Verbindungen sind mit höheren Versionen kompatibel. Eine CPMI-Anwendung mit NG FP3 OPSEC-SDK kann zum Beispiel mit VPN-1 NGX R60 kommunizieren.

Abwärtskompatibilität für CPMI-Verbindungen

Mit früheren Versionen sind CPMI-Verbindungen nicht kompatibel. Eine CPMI-Anwendung mit OPSEC SDK 6.0 kann zum Beispiel nicht mit VPN-1-Versionen vor NGX R60 kommunizieren.

Konfigurationsanforderungen für CPSMS

Für CPSMS gelten zwei Konfigurationsanforderungen. Diese Anforderungen werden bei der Installation von CPSMS standardmäßig installiert. Sie müssen jedoch sicherstellen, dass sie auch erhalten bleiben.

Die CPSMS-Clientanwendung cpsms_client ist im CPSMS-Adapter integriert. cpsms_client richtet für CPSMS über einen Secure Internal Communication (SIC)-Kanal eine asymmetrische Authentifizierungsmethode ein. Diese asymmetrische Methode wird auch als OPSEC_SSLCA-Methode bezeichnet.

Die asymmetrische Authentifizierungsmethode wird in Konfigurationsanforderungen umgesetzt. Damit cpsms_client mit CPSMS kommunizieren kann, müssen Sie Secure Internal Communication (SIC) auf dem Firewall-Verwaltungsserver konfigurieren und aktivieren.

Folgende Ports müssen auf CPSMS offen sein:

- Port 18190 für den Check Point Management Interface-Service (CPMI)
- Port 18210 für den Check Point Internal CA Pull Certificate-Service (FW1_ica_pull)

Falls Sie Port 18190 nicht als Empfangsport für die CPMI verwenden können, muss die Portnummer des CPSMS-Adapters dem zugehörigen Wert in der Datei `$FWDIR/conf/fwopsec.conf` für die CPMI auf dem CPSMS entsprechen. Beispiel: cpmi_server auth_port 18190.

Damit cpsms_client mit Check Point Management Server kommunizieren kann, muss die Datei `$CPDIR/conf/sic_policy.conf` auf dem CPSMS mindestens die folgende Zeile enthalten:

```
# OPSEC applications default
ANY ; SAM_clients ; ANY ; sam ; sslca, local, sslca_comp
# sam proxy
ANY ; Modules, DN_Mgmt ; ANY; sam ; sslca
ANY ; ELA_clients ; ANY ; ela ; sslca, local, sslca_comp
ANY ; LEA_clients ; ANY ; lea ; sslca, local, sslca_comp
ANY ; CPMI_clients; ANY ; cpmi ; sslca, local, sslca_comp
```

Cisco CatOS

IBM Security QRadar Risk Manager unterstützt den Cisco Catalyst (CatOS)-Adapter.

Der Cisco CatOS-Adapter erfasst Einheitenkonfigurationen, indem er die in QRadar Risk Manager anzeigbaren CatOS-Netzeinheiten sichert.

In der folgenden Tabelle werden die Integrationsanforderungen für den Cisco CatOS-Adapter beschrieben.

Tabelle 6. Integrationsanforderungen für den Cisco CatOS-Adapter

Integrationsanforderungen	Beschreibung
Versionen	Catalyst 6500 Series-Chassiseinheiten. **Einschränkung:** Der CatOS-Adapter sichert nur den essentiellen Teil der Switch-Port-Struktur. CatOS-Adapter für Multilayer Switch Feature Card (MSFC) werden durch Cisco IOS-Adapter gesichert. CatOS-Adapter für das Firewall Services Module (FWSM) werden durch Cisco ASA-Adapter gesichert.
Neighbor-Datenunterstützung	Unterstützt
SNMP-Erkennung	Gleicht in der SNMP sysDescr CATOS oder Catalyst Operating System ab

Erforderliche Parameter für Berechtigungsnachweise	`Benutzername`
	
	`Kennwort`
	
	`Kennwort aktivieren`

Verbindungsprotokolle	Telnet SSH

Tabelle 6. Integrationsanforderungen für den Cisco CatOS-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`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 unterstützt den Cisco Internet Operating System (IOS)-Adapter.

Der Cisco IOS-Adapter erfasst Einheitenkonfigurationen, indem er IOS-basierte Netzswitches und -router sichert.

In der folgenden Tabelle werden die Integrationsanforderungen für Cisco IOS beschrieben.

Tabelle 7. Integrationsanforderungen für Cisco IOS

Integrationsanforderungen	Beschreibung
Versionen	10.1 und höher für Router und Switches Cisco Catalyst 6500-Switches mit MSFC. Verwenden Sie den Cisco IOS-Adapter zum Sichern der Konfiguration und des Status von MSFC Card Services. Wenn ein Cisco IOS 7600 Series-Router einen FWSM hat, verwenden Sie zu dessen Sicherung den Cisco ASA-Adapter.
Neighbor-Datenunterstützung	Unterstützt
SNMP-Erkennung	Gleicht in der SNMP sysDescr ISO oder Cisco Internet Operation System ab

Erforderliche Parameter für Berechtigungsnachweise	`Benutzername`
	
	`Kennwort`
	
	`Kennwort aktivieren`

Verbindungsprotokolle	Telnet SSH und SCP TFTP

Tabelle 7. Integrationsanforderungen für Cisco IOS (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`show access lists`
	`show cdp neighbors detail`
	`show eigrp neighbors`
	`show diagbus`
	`show diag`
	`show install running`
	`show interfaces`
	`show inventory`
	`show file systems`
	`show mac-address-table dynamic`
	`show module`
	`show mod version`
	`show power`
	`show startup-config`
	`show object-group`
	`show running-config`
	`show snmp`
	`show glbp`
	`show spanning-tree`
	`show standby`
	`set terminal length`
	`show vlan`
	`show vtp status`
	`show version`
	`show vrrp`

Tabelle 7. Integrationsanforderungen für Cisco IOS (Forts.)

Integrationsanforderungen	Beschreibung

`show ip` Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`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 neighbor`
	`show ip protocols`
	`show ipv6 neighbors`
	`show ip ospf interface`
	`show ip route eigrp`

Cisco Nexus

Für die Integration von IBM Security QRadar Risk Manager mit Ihren Netzeinheiten müssen folgende Voraussetzungen für den Cisco Nexus-Adapter erfüllt sein.

In der folgenden Tabelle werden die Integrationsanforderungen für den Cisco Nexus-Adapter beschrieben.

Tabelle 8. Integrationsanforderungen für den Cisco Nexus-Adapter

Integrationsanforderungen	Beschreibung
Versionen	Keine Versionseinschränkungen
Neighbor-Datenunterstützung	Unterstützt
SNMP-Erkennung	Gleicht in der SNMP sysDescr *Cisco NX-OS* und eine optionale Qualifizierungszeichenfolge ab, die auf *Software* endet. **Beispiel:** *(Cisco NX\-OS.* Software)*

Erforderliche Parameter für Berechtigungsnachweise	`Benutzername`
	`Kennwort`
	`Kennwort aktivieren`
	Wenn Sie virtuelle Gerätekontexte (VDCs = Virtual Device Contexts) als separate Einheiten hinzufügen, müssen Sie sicherstellen, dass mit den erforderlichen Berechtigungsnachweisen folgende Aktionen ausgeführt werden können:
	• Zugriff auf das für die VDCs aktivierte Konto
	• Verwendung der erforderlichen Befehle im virtuellen Kontext

Tabelle 8. Integrationsanforderungen für den Cisco Nexus-Adapter (Forts.)

Integrationsanforderungen	**Beschreibung**
Verbindungsprotokolle	Telnet SSH

Erforderliche Dateien von Drittanbietern	`adapters-common-2013.03_05-515182.noarch.rpm`
	
	`perl-Net-CIDR-Set-0.11-1.noarch.rpm`
	
	`perl-XML-Twig-3.42-1.noarch.rpm`

Tabelle 8. Integrationsanforderungen für den Cisco Nexus-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`terminal length 0`
	
	`show version`
	
	`show hostname`
	
	`show vdc`
	
	`snow snmp`
	
	`show module`
	
	`dir` *fs* (*fs* ist das Dateisystem auf der Einheit)
	
	`show interface brief`
	
	`show interface snmp-ifindex`
	
	`show interface` *if* (*if* sind alle Schnittstellen aus `show interface brief` mit Konfigurationsabschnitten)
	
	`show running-config`
	
	`show startup-config`
	
	`show static-route`
	
	`show ip access-lists`
	
	`show object-group`
	
	`show vlan`
	
	`show vtp status`
	
	`show hsrp`
	
	`show vrrp`
	
	`show vtp`
	
	`show glbp`
	
	`show ip arp`
	
	`show mac address-table`
	
	`show ip route`
	
	`show ipv6 route`
	
	`show ipv6 ndp`
	
	`show cdp entry all`
	
	`switchto` *vdc* (für alle unterstützten virtuellen Gerätekontexte)

Methoden zum Hinzufügen von VDCs für Cisco Nexus-Einheiten

Zum Hinzufügen von Nexus-Netzeinheiten und virtuellen Gerätekontexten (VDCs = Virtual Device Contexts) zu IBM Security QRadar SIEM verwenden Sie Configuration Source Management. Es gibt zwei Methoden zum Hinzufügen mehrerer VDCs zu IBM Security QRadar Risk Manager.

VDCs können Nexus-Einheiten als untergeordnete oder als separate Einheiten hinzugefügt werden.

Virtuelle Gerätekontexte anzeigen

Als separate Einheiten hinzugefügte VDCs werden in der Topologie als eigene Einheiten angezeigt.

Als untergeordnete Einheiten hinzugefügte VDCs werden in der Topologie nicht angezeigt. Diese VDCs können Sie nur im Configuration Monitor anzeigen.

VDCs als untergeordnete Einheiten einer Cisco Nexus-Einheit hinzufügen

Zum Hinzufügen von VDCs als untergeordnete Einheiten einer Cisco Nexus-Einheit verwenden Sie Configuration Source Manager.

Vorgehensweise

1. Fügen Sie die IP-Verwaltungsadresse jedes VDCs in Configuration Source Manager hinzu.

   Weitere Informationen finden Sie im Abschnitt „Netzeinheit hinzufügen" auf Seite 5.
2. Rufen Sie die Konfigurationsdaten der Nexus-Einheit über Configuration Source Manager ab.

   Weitere Informationen zum Abrufen von Einheitenkonfigurationen finden Sie im *IBM Security QRadar Risk Manager User Guide*.
3. Aktivieren Sie für den in den Berechtigungsnachweisen angegebenen Benutzer die folgenden Befehle:
   - `show vdc` (im Verwaltungskontext)
   - `switchto vdc` *x*; dabei sind *x* die unterstützten VDCs.

   In Configuration Monitor können Sie die Nexus-Einheit sowie die untergeordneten VDC-Einheiten anzeigen. Die übergeordnete Einheit wird in der Topologie angezeigt. Weitere Informationen zum Anzeigen von Einheiten finden Sie im *IBM Security QRadar Risk Manager User Guide*.

VDCs als separate Einheiten hinzufügen

Zum Hinzufügen eines VDCs als separate Einheit verwenden Sie Configuration Source Manager. Wenn Sie diese Methode verwenden, werden die Nexus-Einheit sowie die VDCs in der Topologie angezeigt.

In der Topologie wird das Chassis getrennt von der Cisco Nexus-Einheit und den VDCs dargestellt.

Vorgehensweise

1. Fügen Sie die IP-Verwaltungsadresse jedes VDC in Configuration Source Manager hinzu.

   Weitere Informationen finden Sie im Abschnitt „Netzeinheit hinzufügen" auf Seite 5.
2. Rufen Sie die Konfigurationsdaten Ihrer VDCs über Configuration Source Manager ab.
3. Inaktivieren Sie auf der Cisco Nexus-Einheit in der Cisco Nexus-CLI den Befehl **switchto vdc** für den Benutzernamen, der dem Adapter zugeordnet ist.

   Beispiel: Der Benutzername für eine Cisco Nexus-Einheit sei *qrmuser*. In diesem Fall geben Sie folgenden Befehl ein:

   ```
   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 2 permit command terminal
   NexusDevice(config-role)# rule 2 permit command dir
   ```

Cisco Security Appliances

Für die Integration von IBM Security QRadar Risk Manager mit Ihren Netzeinheiten müssen folgende Voraussetzungen für den Cisco Security Appliances-Adapter erfüllt sein.

Der Cisco Security Appliances-Adapter erfasst Einheitenkonfigurationen, indem er Einheiten der Cisco-Produktfamilie sichert. Nachfolgend einige Beispiele für Cisco-Firewalls, die der Adapter für Cisco Security Appliances unterstützt:

- Stand-alone Adaptive Security Appliance
- Firewall Service Module (FWSM)
- Ein Modul in einem Catalyst-Chassis
- Established Private Internet Exchange-Einheiten (PIX)

In der folgenden Tabelle werden die Integrationsanforderungen für den Cisco Security Appliances-Adapter beschrieben.

Tabelle 9. Integrationsanforderungen für den Cisco Security Appliances-Adapter

Integrationsanforderungen	**Beschreibung**
Versionen	Adaptive Security Appliances (ASA) mit einem Private Internet Exchange-Betriebssystem (PIX-OS) ASA-Router oder Switches mit FWSM Cisco IOS 7600 Series-Router mit FWSM Verwenden Sie den ASA-Adapter zum Sichern der Konfiguration und des Status von FWSM Card Services.
Neighbor-Datenunterstützung	Unterstützt
SNMP-Erkennung	Gleicht in der SNMP sysDescr PIX oder Adaptive Security Appliance oder Firewall Service Module ab.

Erforderliche Parameter für Berechtigungsnachweise	`Benutzername`
	
	`Kennwort`
	
	`Kennwort aktivieren`

Verbindungsprotokolle	Telnet SSH und SCP

Tabelle 9. Integrationsanforderungen für den Cisco Security Appliances-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`change context`
	
	`change context` *`Admin-Kontext`*
	
	`change context` *`Kontext`*
	
	`change system`
	
	`get startup-config`
	
	`show arp`
	
	`show context`
	
	`show interface`
	
	`show interface detail`
	
	`show ipv6 interface`
	
	`show ipv6 neighbor`
	
	`show mac-address-table`
	
	`show names`
	
	`show ospf neighbor`
	
	`show pager`
	
	`show route`
	
	`show running-config`
	
	`show shun`
	
	`show version`
	
	`terminal pager 0`
	
	`terminal pager 24`
	Dabei gilt::
	
	Der Befehl `show pager` muss zum Zugriff auf Konten aktiviert sein, die QRadar Risk Manager verwenden.
	
	Der Befehl `context` *`Kontext`* wird für jeden Kontext auf der ASA-Einheit verwendet.
	
	Der Befehl `change system` ermittelt, ob das System Konfigurationen mit mehreren Kontexten aufweist. Außerdem ermittelt er den Administratorkontext.
	Der Befehl `change context` wird benötigt, wenn der Befehl `change system` zu einer Konfiguration mit mehreren Kontexten oder zu einem Administratorkontext wechselt.
	Die `terminal pager`-Befehle werden zum Festlegen und Zurücksetzen des Auslagerungsverhaltens verwendet.

HP Networking ProVision

IBM Security QRadar Risk Manager unterstützt den HP Networking ProVision-Adapter.

In der folgenden Tabelle werden die Integrationsanforderungen für den HP Networking ProVision-Adapter beschrieben.

Tabelle 10. Integrationsanforderungen für den HP Networking ProVision-Adapter

Integrationsanforderungen	**Beschreibung**
Versionen	HP Networking ProVision Switches K/KA.11.XX und höher. **Einschränkung:** HP-Switches auf einem Comware-Betriebssystem werden nicht unterstützt.
Neighbor-Datenunterstützung	Unterstützt
SNMP-Erkennung	Gleicht in der sysDescr Versionsnummern mit dem Format `HP(.*)Switch(.*)(revision [A-Z]{1,2}\.(\d+)\.(\d+))` ab.

Erforderliche Parameter für Berechtigungsnachweise	`Benutzername`
	
	`Kennwort`
	
	`Kennwort aktivieren`

Verbindungsprotokolle	SSH

Tabelle 10. Integrationsanforderungen für den HP Networking ProVision-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Vom Adapter an die Einheit ausgegebene Backup-Befehle	`dmesgshow system power-supply`
	`getmib`
	`show access-list vlan <VLAN-ID>`
	`show access-list`
	`show access-list <Name oder Zahl>`
	`show access-list ports <Portnummer>`
	`show config`
	`show filter`
	`show filter <ID>`
	`show running-config`
	`show interfaces brief`
	`show interfaces <Schnittstellen-ID>` - für jede Schnittstelle
	`show jumbos`
	`show trunks`
	`show lacp`
	`show module`
	`show snpm-server`
	`show spanning-tree`
	`show spanning-tree config`
	`show spanning-tree instance <ID oder Liste>` - für jeden auf der Einheit konfigurierten Spanning Tree
	`show spanning-tree mst-config`
	`show system information`
	`show version`
	`show vlans`
	`show vlans <ID>` - für jedes VLAN
	`show vrrp`
	`walkmib`

Tabelle 10. Integrationsanforderungen für den HP Networking ProVision-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

`show ip` Vom Adapter an die Einheit ausgegebene Backup-Befehle	`show ip`
	`show ip route`
	`show ip odpf`
	`show ip odpf redistribute`
	`show ip rip`
	`show ip rip redistribute`

Telemetry- und Neighbor-Datenbefehle	`getmib`
	`show arp`
	`show cdp neighbors`
	`show cdp neighbors detail <Portnummer>`
	`show interfaces brief`
	`show interface`
	`show ip route`
	`show lldp info remote-device`
	`show lldp info remote-device <Portnummer>`
	`show mac-address or show mac address`
	`show system information`
	`show vlans`
	`show vlans custom id state ipaddr ipmask`
	`walkmib`

Juniper Networks JUNOS

Für die Integration von IBM Security QRadar Risk Manager mit Ihren Netzeinheiten müssen folgende Voraussetzungen für den Juniper Networks JUNOS-Adapter erfüllt sein.

In der folgenden Tabelle werden die Integrationsanforderungen für den Juniper Networks JUNOS-Adapter beschrieben.

Tabelle 11. Integrationsanforderungen für den Juniper Networks JUNOS-Adapter

Integrationsanforderungen	Beschreibung
Versionen	Version 9 und höher
Neighbor-Datenunterstützung	Unterstützt
SNMP-Erkennung	Gleicht SNMP sysOID 1.3.6.1.4.1.2636 ab
Erforderliche Parameter für Berechtigungsnachweise	`Benutzername` `Kennwort`

Tabelle 11. Integrationsanforderungen für den Juniper Networks JUNOS-Adapter (Forts.)

Integrationsanforderungen	**Beschreibung**
Verbindungsprotokolle	Telnet SSH und SCP

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`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`
	`show bgp neighbor`
	`show ipv6 neighbors`

Juniper Networks NSM

IBM Security QRadar Risk Manager-Adapter unterstützt Juniper Networks NSM.

Mit QRadar Risk Manager können Sie eine einzelne Juniper Networks-Einheit sichern oder Einheitendaten von einer Juniper Networks NSM-Konsole abrufen.

Die Juniper Networks NSM-Konsole enthält die Konfigurations- und Einheitendaten der von der Konsole verwalteten Juniper Networks-Router und -Switches.

In der folgenden Tabelle werden die für Juniper Networks NSM unterstützten Umgebungen beschrieben.

Tabelle 12. Von QRadar Risk Manager-Adapter unterstützte Umgebungen für Juniper Networks NSM

Unterstützte Umgebung	Beschreibung
Versionen	Von NSM verwaltete IDP-Appliances
Neighbor-Datenunterstützung	Nicht unterstützt
SNMP-Erkennung	Nicht unterstützt
Erforderliche Parameter für Berechtigungsnachweise	• `Benutzername` • `Kennwort`
Verbindungsprotokolle	• SOAP • HTTP

Juniper Networks ScreenOS

Für die Integration von IBM Security QRadar Risk Manager mit Ihren Netzeinheiten müssen folgende Voraussetzungen für den Juniper Networks ScreenOS-Adapter erfüllt sein.

In der folgenden Tabelle werden die Integrationsanforderungen für den Juniper Networks ScreenOS-Adapter beschrieben.

Tabelle 13. Integrationsanforderungen für den Juniper Networks ScreenOS-Adapter

Integrationsanforderungen	Beschreibung
Versionen	Firewalls, die ein ScreenOS-Betriebssystem nutzen
Neighbor-Datenunterstützung	Unterstützt
SNMP-Erkennung	Gleicht in der SNMP sysDescr netscreen oder SSG ab

Erforderliche Parameter für Berechtigungsnachweise	`Benutzername`
	
	`Kennwort`

Verbindungsprotokolle	Telnet SSH

Tabelle 13. Integrationsanforderungen für den Juniper Networks ScreenOS-Adapter (Forts.)

Integrationsanforderungen	Beschreibung

Befehle, die der Adapter zur Anmeldung und zum Abrufen der Daten benötigt	`set console page 0`
	
	`get system`
	
	`get config`
	
	`get snmp`
	
	`get memory`
	
	`get file info`
	
	`get file`
	
	`get service`
	
	`get group address`*`ZoneGruppe`*
	
	`get address`
	
	`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`*
	Dabei gilt::
	
	Zone sind die vom Befehl `get config` zurückgegebenen Zonendaten.
	
	Gruppe sind die vom Befehl `get config` zurückgegebenen Gruppendaten.
	
	D*Variable* ist eine Liste der vom Befehl `get service group`, `get interface` oder `get policy id` zurückgegebenen Daten.

Palo Alto

IBM Security QRadar Risk Manager unterstützt den Palo Alto-Adapter. Der Palo Alto-Adapter verwendet zur Kommunikation mit Einheiten die XML-basierte REST-Anwendungsprogrammierschnittstelle (API) des PAN-OS.

Zum Senden eines Befehls an eine Einheit verwenden Sie eine HTTPS-Anforderung an eine URL. Das Befehlsformat dieser Anforderung ist `https://EinheitenIPAdresse/api/?type=op&cmd=<Befehl>`

Dabei ist *Befehl* ein XML-Tag-Satz oder ein XPath.

Beispiel für einen XML-Tag-Satz:

```
<show><system><info></info></system></show>
```

Beispiel für einen XPath:

```
/config/predefined/service
```

In der folgenden Tabelle werden die Integrationsanforderungen für den Palo Alto-Adapter beschrieben.

Tabelle 14. Integrationsanforderungen für den Palo Alto-Adapter

Integrationsanforderungen	**Beschreibung**
Versionen	PAN-OS-Version 4.1.0 und höher
Neighbor-Datenunterstützung	Unterstützt
SNMP-Erkennung	Gleicht in der SysDescr 'Palo Alto Networks(.*)series firewall' ab und in der sysOid 'panPA'.

Erforderliche Parameter für Berechtigungsnachweise	`Benutzername`
	
	`Kennwort`
	
	Für Berechtigungsnachweise wird SuperReader-Zugriff benötigt.

Verbindungsprotokolle	HTTPS

Tabelle 14. Integrationsanforderungen für den Palo Alto-Adapter (Forts.)

Integrationsanforderungen	Beschreibung
Backup-Befehle	<show><system><info></info></system></show> <show><config><running></running></config></show> <show><routing><route></route></routing></show> <show><virtual-wire>all</virtual-wire></show> <show><vlan>all</vlan></show> <show><interface>all</interface></show> <show><system><disk-space></disk-space></system></show> <show><system><resources></resources></system></show> /config/predefined/service
Befehle für Telemetry- und Neighbor-Daten	<show><system><info></info></system></show> <show><interface>all</interface></show> <show><routing><interface></interface></routing></show> <show><counter><interface>all</interface></counter></show> <show><arp>all</arp></show> <show><mac>all</mac></show> <show><routing><route></route></routing></show>
Befehle für GetApplication	<show><config><running></running></config></show> /config/predefined/application

Bemerkungen

Die vorliegenden Informationen wurden für Produkte und Services entwickelt, die auf dem deutschen Markt angeboten werden.

Möglicherweise bietet IBM die in dieser Dokumentation beschriebenen Produkte, Services oder Funktionen in anderen Ländern nicht an. Informationen über die gegenwärtig im jeweiligen Land verfügbaren Produkte und Services sind beim zuständigen IBM Ansprechpartner erhältlich. Hinweise auf IBM Lizenzprogramme oder andere IBM Produkte bedeuten nicht, dass nur Programme, Produkte oder Services von IBM verwendet werden können. Anstelle der IBM Produkte, Programme oder Services können auch andere, ihnen äquivalente Produkte, Programme oder Services verwendet werden, solange diese keine gewerblichen oder anderen Schutzrechte von IBM verletzen. Die Verantwortung für den Betrieb von Produkten, Programmen und Services anderer Anbieter liegt beim Kunden.

Für in diesem Handbuch beschriebene Erzeugnisse und Verfahren kann es IBM Patente oder Patentanmeldungen geben. Mit der Auslieferung dieses Handbuchs ist keine Lizenzierung dieser Patente verbunden. Lizenzanforderungen sind schriftlich an folgende Adresse zu richten (Anfragen an diese Adresse müssen auf Englisch formuliert werden):

IBM Director of Licensing
IBM Europe, Middle East & Africa
Tour Descartes
2, avenue Gambetta
92066 Paris
France

Trotz sorgfältiger Bearbeitung können technische Ungenauigkeiten oder Druckfehler in dieser Veröffentlichung nicht ausgeschlossen werden. Die hier enthaltenen Informationen werden in regelmäßigen Zeitabständen aktualisiert und als Neuausgabe veröffentlicht. IBM kann ohne weitere Mitteilung jederzeit Verbesserungen und/oder Änderungen an den in dieser Veröffentlichung beschriebenen Produkten und/oder Programmen vornehmen.

Verweise in diesen Informationen auf Websites anderer Anbieter werden lediglich als Service für den Kunden bereitgestellt und stellen keinerlei Billigung des Inhalts dieser Websites dar. Das über diese Websites verfügbare Material ist nicht Bestandteil des Materials für dieses IBM Produkt. Die Verwendung dieser Websites geschieht auf eigene Verantwortung.

Werden an IBM Informationen eingesandt, können diese beliebig verwendet werden, ohne dass eine Verpflichtung gegenüber dem Einsender entsteht.

Lizenznehmer des Programms, die Informationen zu diesem Produkt wünschen mit der Zielsetzung: (i) den Austausch von Informationen zwischen unabhängig voneinander erstellten Programmen und anderen Programmen (einschließlich des vorliegenden Programms) sowie (ii) die gemeinsame Nutzung der ausgetauschten Informationen zu ermöglichen, wenden sich an folgende Adresse:

IBM Corporation
170 Tracer Lane,
Waltham MA 02451, USA

Die Bereitstellung dieser Informationen kann unter Umständen von bestimmten Bedingungen - in einigen Fällen auch von der Zahlung einer Gebühr - abhängig sein.

Die Lieferung des in diesem Dokument beschriebenen Lizenzprogramms sowie des zugehörigen Lizenzmaterials erfolgt auf der Basis der IBM Rahmenvereinbarung bzw. der Allgemeinen Geschäftsbedingungen von IBM, der IBM Internationalen Nutzungsbedingungen für Programmpakete oder einer äquivalenten Vereinbarung.

Alle in diesem Dokument enthaltenen Leistungsdaten stammen aus einer kontrollierten Umgebung. Die Ergebnisse, die in anderen Betriebsumgebungen erzielt werden, können daher erheblich von den hier erzielten Ergebnissen abweichen. Einige Daten stammen möglicherweise von Systemen, deren Entwicklung noch nicht abgeschlossen ist. Eine Gewährleistung, dass diese Daten auch in allgemein verfügbaren Systemen erzielt werden, kann nicht gegeben werden. Darüber hinaus wurden einige Daten unter Umständen durch Extrapolation berechnet. Die tatsächlichen Ergebnisse können davon abweichen. Benutzer dieses Dokuments sollten die entsprechenden Daten in ihrer spezifischen Umgebung prüfen.

Alle Informationen zu Produkten anderer Anbieter stammen von den Anbietern der aufgeführten Produkte, deren veröffentlichten Ankündigungen oder anderen allgemein verfügbaren Quellen. IBM hat diese Produkte nicht getestet und kann daher keine Aussagen zu Leistung, Kompatibilität oder anderen Merkmalen machen. Fragen zu den Leistungsmerkmalen von Produkten anderer Anbieter sind an den jeweiligen Anbieter zu richten.

Aussagen über Pläne und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

Alle von IBM angegebenen Preise sind empfohlene Richtpreise und können jederzeit ohne weitere Mitteilung geändert werden. Händlerpreise können u. U. von den hier genannten Preisen abweichen.

Diese Veröffentlichung enthält Beispiele für Daten und Berichte des alltäglichen Geschäftsablaufs. Sie sollen nur die Funktionen des Lizenzprogramms illustrieren und können Namen von Personen, Firmen, Marken oder Produkten enthalten. Alle diese Namen sind frei erfunden; Ähnlichkeiten mit tatsächlichen Namen und Adressen sind rein zufällig.

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der IBM Corporation in den USA und/oder anderen Ländern. Sind diese und weitere Markennamen von IBM bei ihrem ersten Vorkommen in diesen Informationen mit einem Markensymbol (® oder ™) gekennzeichnet, bedeutet dies, dass IBM zum Zeitpunkt der Veröffentlichung dieser Informationen Inhaber der eingetragenen Marken oder der Common-Law-Marken (common law trademarks) in den USA war. Diese Marken können auch eingetragene Marken oder Common-Law-Marken in anderen Ländern sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite Copyright and trademark information (www.ibm.com/legal/copytrade.shtml).

Die folgenden Namen sind Marken oder eingetragene Marken anderer Unternehmen:

Microsoft, Windows, Windows NT und das Windows-Logo sind Marken der Microsoft Corporation in den USA und/oder anderen Ländern.

Weitere Unternehmens-, Produkt- oder Servicenamen können Marken anderer Hersteller sein.

Hinweise zur Datenschutzrichtlinie

IBM Software-Produkte, einschließlich "Software as a Service"-Lösungen (Softwareangebote) verwenden möglicherweise Cookies oder andere Technologien, um Nutzungsinformationen zum Produkt zu erfassen, die Erfahrung der Endbenutzer zu verbessern, Interaktionen mit dem Endbenutzer zu optimieren usw. In vielen Fällen werden von den Softwareangeboten keine personenbezogenen Daten erfasst. Einige der IBM Softwareangebote können Sie jedoch bei der Erfassung personenbezogener Daten unterstützen. Wenn dieses Softwareangebot Cookies zur Erfassung personenbezogener Daten verwendet, sind nachfolgend nähere Informationen über die Verwendung von Cookies durch dieses Angebot zu finden.

Je nachdem, welche Konfigurationen bereitgestellt sind, kann dieses Softwareangebot Sitzungscookies verwenden, die für das Sitzungsmanagement und die Authentifizierung die Sitzungs-ID jedes Benutzers erfassen. Diese Cookies können inaktiviert werden, dadurch geht aber auch die von diesen bereitgestellte Funktionalität verloren.

Wenn die für dieses Softwareangebot genutzten Konfigurationen Sie als Kunde in die Lage versetzen, personenbezogene Daten von Endbenutzern über Cookies und andere Technologien zu erfassen, müssen Sie sich zu allen gesetzlichen Bestimmungen in Bezug auf eine solche Datenerfassung, einschließlich aller Mitteilungspflichten und Zustimmungsanforderungen, rechtlich beraten lassen.

Weitere Informationen zur Nutzung verschiedener Technologien, einschließlich Cookies, für diese Zwecke finden Sie in der IBM Datenschutzrichtlinie unter http://www.ibm.com/privacy, in der IBM Online-Datenschutzrichtlinie unter http://www.ibm.com/privacy/details im Abschnitt "Cookies, Web-Beacons und sonstige Technologien" und im "IBM Software Products and Software-as-a-Service Privacy Statement" unter http://www.ibm.com/software/info/product-privacy.

Index

A

Adapter 13
  Konfigurationsübersicht 1
  Typen 1
Adapterinstallieren auf QRadar Risk Manager 3

B

BIG-IP 14

C

Check Point SecurePlatform 1
Check Point SecurePlatform Appliances
  Integrationsanforderungen 18
Check Point Security Management Server 19
Cisco Catalyst 1
Cisco CatOS
  unterstützte Umgebungen 20
Cisco Internet Operating System 1
Cisco IOS
  Integrationsanforderungen 22
Cisco Nexus
  Integrationsanforderungen 24
  VDCs hinzufügen 27
Cisco Security Appliance 1
Cisco Security Appliances
  Integrationsanforderungen 29
Configuration Source Management
  Netzeinheiten hinzufügen 5
  von Juniper Networks verwaltete Netzeinheiten hinzufügen 7
CPSMS 19

D

Deinstallieren
  Adapter 4
Dokumentation v

E

Erfasste Dateien
  Adapterunterstützung 13
Erforderliche Befehle
  Adapterunterstützung 13
Erforderliche Berechtigungsnachweise
  Adapter 13

H

HP Networking ProVision 31

I

Installieren
  Adapter 3

J

Juniper Networks JunOS 1
Juniper Networks JUNOS
  Integrationsanforderungen 33
Juniper Networks NSM 1
  unterstützte Umgebungen 35
Juniper Networks ScreenOS 1
  Integrationsanforderungen 35

K

Kundenunterstützung
  Kontaktinformationen v

N

Neighbor-Daten
  Definition 13
Netzadministrator
  Beschreibung v
Netzeinheiten
  hinzufügen und konfigurieren 5
  von Juniper Networks verwaltete Einheiten zu Risk Manager hinzufügen 7
  zu Risk Manager hinzufügen 5
Nexus-Einheit
  VDCs als untergeordnete Einheiten hinzufügen 27
Nexus-Einheiten
  VDCs als separate Einheiten hinzufügen 28

P

Palo Alto 37

S

SiteProtector-Erkennung 10
SNMP-Erkennung
  Adapter 13

T

Technische Bibliothek v

U

Unterstützte Adapter
  Übersicht 13

V

VDC
  Methoden zum Hinzufügen zu Cisco Nexus-Einheiten 27
Verbindungsprotokolle
  Adapterunterstützung 13
Virtuelle Gerätekontexte
  siehe VDC

SC12-5040-00