IBM Security QRadar Incident Forensics
Version 7.3.0

Installationshandbuch

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 33 gelesen werden.

Produktinformation

Dieses Dokument bezieht sich auf IBM QRadar Security Intelligence Platform V7.3.0 und alle nachfolgenden Releases, bis es durch eine aktualisierte Version dieses Dokuments ersetzt wird.

Inhaltsverzeichnis

Einführung in die Installation von IBM Security QRadar Incident Forensics

Dieser Abschnitt enthält Informationen zur Installation von IBM® Security QRadar Incident Forensics und zur Integration des Produkts mit IBM Security QRadar. QRadar Incident Forensics-Appliances enthalten vorinstallierte Software und das Betriebssystem Red Hat Enterprise Linux. Sie können QRadar Incident Forensics-Software auch auf Ihrer eigenen Hardware installieren.

Zielgruppe

Netzadministratoren, die für die Installation und Konfiguration von QRadar Incident Forensics-Systemen verantwortlich sind.

Administratoren müssen über praktische Erfahrungen mit dem Netzbetrieb und Linux-Betriebssystemen verfügen.

Technische Dokumentation

Die Produktdokumentation zu IBM Security QRadar im Web, einschließlich aller Übersetzungen, finden Sie 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 im Dokument Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Kontaktierung der Kundenunterstützung

Informationen zur Kontaktierung der Kundenunterstützung finden Sie im Dokument Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

Erklärung zu geeigneten Sicherheitsvorkehrungen

Zur Sicherheit von IT-Systemen gehört der Schutz von Systemen und Informationen in Form von Vorbeugung, Erkennung und Reaktion auf unbefugten Zugriff innerhalb des Unternehmens und von außen. Unbefugter 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 unbefugte Verwendung oder einen unbefugten Zugriff mit vollständiger Wirksamkeit verhindern. IBM Systeme, Produkte und Services werden als Teil eines umfassenden gesetzlichen 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 vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter geschützt sind oder dass Systeme, Produkte oder Services Ihr Unternehmen vollkommen vor böswilligem oder rechtswidrigem Verhalten Dritter schützen.

Bitte beachten:

Bei der Nutzung dieses Programms muss ggf. eine Reihe von Gesetzen und Bestimmungen beachtet werden, einschließlich solcher, die sich auf den Datenschutz, die Datensicherheit, arbeitsrechtliche Angelegenheiten sowie die elektronische Kommunikation und die Speicherung beziehen. IBM Security QRadar darf nur für gesetzlich zulässige Zwecke und in rechtmäßiger Weise verwendet werden. Der Kunde verpflichtet sich, dieses Programm gemäß geltendem Recht, geltenden Regelungen und Richtlinien zu verwenden und übernimmt die gesamte Verantwortung für die Einhaltung dieser Bestimmungen. Der Lizenznehmer versichert, dass er alle Zustimmungen, Genehmigungen oder Lizenzen einholen wird oder eingeholt hat, die für eine rechtmäßige Nutzung von IBM Security QRadar erforderlich sind.

Hinweis

IBM Security QRadar Incident Forensics soll Unternehmen dabei helfen, ihre Sicherheitsumgebung und -daten zu verbessern. Genauer gesagt, soll IBM Security QRadar Incident Forensics Unternehmen helfen, zu untersuchen und besser zu verstehen, was bei Netzsicherheitsvorfällen passiert. Mit dem Tool können Unternehmen erfasste Netzpaketdaten (PCAPs) indexieren und durchsuchen. Außerdem enthält es eine Funktion, mit der solche Daten in ihrem ursprünglichen Format wiederhergestellt werden können. Mithilfe dieser Wiederherstellungsfunktion lassen sich Daten und Dateien, einschließlich E-Mail-Nachrichten, Datei- und Bildanhänge, VoIP-Anrufe und Websites, wiederherstellen. Weitere Informationen zu den Produktmerkmalen und Funktionen des Programms sowie zu deren Konfiguration finden Sie in den Handbüchern und sonstigen Dokumentationen, die dem Programm beigefügt sind. Die Verwendung dieses Programms kann verschiedene Gesetze oder Regelungen einschließen. Diese können sich auf die Geheimhaltung, den Datenschutz, die Benutzung und elektronische Kommunikation sowie auf die Speicherung beziehen. IBM Security QRadar Incident Forensics darf nur für gesetzlich zulässige Zwecke und in rechtmäßiger Weise verwendet werden. Der Kunde erklärt, dass er dieses Programm gemäß geltenden Rechten, Verordnungen und Richtlinien verwenden wird und die volle Verantwortung für deren Einhaltung übernimmt. Der Lizenznehmer versichert, dass er alle Zustimmungen, Genehmigungen oder Lizenzen einholen wird oder eingeholt hat, die für eine rechtmäßige Nutzung von IBM Security QRadar Incident Forensics erforderlich sind.

Kapitel 1. Upgrade von QRadar Incident Forensics durchführen

Sie müssen alle IBM Security QRadar-Produkte Ihrer Implementierung auf die gleiche Version aktualisieren. Zum Upgrade von IBM Security QRadar Incident Forensics V7.2.8 auf V7.3.0 verwenden Sie das Installationsprogramm für das entsprechende Upgrade.

Sollen ein Upgrade von QRadar Incident Forensics V7.2.4 oder früheren Versionen vorgenommen werden und die Daten dabei erhalten bleiben, wenden Sie sich an den zuständigen IBM Vertriebsbeauftragten. Wenn Sie andernfalls jedoch ein Upgrade von QRadar Incident Forensics V7.2.4 oder früheren Versionen durchführen möchten, ohne dass Ihre Daten erhalten bleiben sollen, dann führen Sie ein Upgrade direkt auf V7.3.0 durch, indem Sie eine Neuinstallation vornehmen.

Einschränkung: Eine Änderung der Größe logischer Datenträger mithilfe eines Logical Volume Manager (LVM) wird nicht unterstützt.

Vorgehensweise

1. Laden Sie die Datei *<QRadar_patchupdate>.sfs* von IBM Fix Central (www.ibm.com/support/fixcentral) herunter.
2. Melden Sie sich über SSH als Rootbenutzer bei Ihrem System an.
3. Kopieren Sie die Patchdatei in das Verzeichnis `/tmp` oder an eine andere Position mit ausreichendem Plattenspeicherplatz.
4. Geben Sie folgenden Befehl ein, um das Verzeichnis `/media/updates` zu erstellen:

   ```
   mkdir -p /media/updates
   ```
5. Wechseln Sie in das Verzeichnis, in das Sie die Patchdatei kopiert haben.
6. Geben Sie folgenden Befehl ein, um die Patchdatei an das Verzeichnis `/media/updates` anzuhängen:

   ```
   mount -o loop -t squashfs <QRadar_patchupdate>.sfs /media/updates/
   ```
7. Geben Sie zur Ausführung des Installationsprogramms für das Upgrade folgenden Befehl ein:

   ```
   /media/updates/installer
   ```

   Wenn Sie das Installationsscript für den Patch zum ersten Mal ausführen, kann es eine Weile dauern, bis das erste Menü des Installationsprogramms angezeigt wird.
8. Geben Sie die Antworten auf die Vorinstallationsfragen entsprechend Ihrer Implementierung ein.
9. Verwenden Sie das Installationsprogramm für das Upgrade zum Aktualisieren aller Hosts Ihrer Implementierung.

   Wenn Sie nicht die Option **Patch auf alle Systeme anwenden** auswählen, müssen Sie Ihre Systeme in folgender Reihenfolge aktualisieren:

   - QRadar-Konsole
   - QRadar Incident Forensics

Sollte Ihre SSH-Sitzung während des Upgrades getrennt werden, so wird das Upgrade, sobald Sie die Sitzung wiederherstellen und das Installationsprogramm neu starten, genau an der Stelle fortgesetzt, an der es zuvor abgebrochen wurde.

10. Nach Beendigung des Upgrades hängen Sie das Software-Upgrade mit folgendem Befehl ab: **umount /media/updates**

Nächste Schritte

Aktualisieren Sie Ihre Paketaufzeichnungseinheiten. Weitere Informationen finden Sie im Handbuch *IBM Security QRadar Packet Capture-Kurzübersicht*.

Kapitel 2. QRadar Incident Forensics-Installationskomponenten

QRadar Incident Forensics ist in die skalierbare Architektur von IBM QRadar Security Intelligence Platform integriert. Je nach Ihren Anforderungen können Sie IBM Security QRadar Incident Forensics-Komponenten auf nur einer Appliance (*All-in-one*) oder auf mehreren Appliances installieren.

Installationsoptionen

Je nach den Komponenten, die Sie installieren, sind möglicherweise nicht alle Sicherheitsfunktionen verfügbar. Wenn Sie beispielsweise QRadar Incident Forensics auf einer einzigen Appliance installieren, ist nur die Netzforensik verfügbar. Wenn Sie dagegen einen verwalteten QRadar Incident Forensics-Host installieren, stehen noch weitere Sicherheitsfunktionen zur Verfügung. Bei den meisten Installationen werden die QRadar-Konsole, mindestens ein QRadar Incident Forensics Processor sowie eine oder mehrere QRadar Packet Capture-Appliances installiert.

Das folgende Diagramm stellt eine Übersicht über die verschiedenen Sicherheitsfunktionen und das Architekturframework von IBM QRadar Security Intelligence Platform dar.

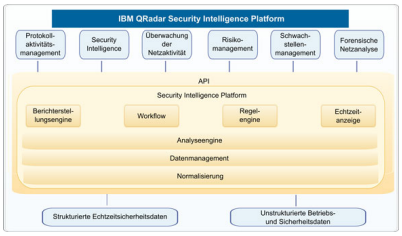


Abbildung 1. Übersicht über die QRadar Security Intelligence-Architektur

All-in-one-Implementierungen

Bei eigenständigen Implementierungen (All-in-one-Implementierungen) wird die IBM Security QRadar Incident Forensics Standalone-Software installiert. Diese Implementierungen auf einer einzigen Appliance entsprechen in etwa der Installation der QRadar-Konsole und des verwalteten QRadar Incident Forensics-Hosts auf einer einzigen Appliance, jedoch ohne Protokollmanagement, Überwachung der

Netzaktivität oder andere Security Intelligence-Funktionen. Für eine eigenständige Netzforensiklösung wird QRadar Incident Forensics Standalone in kleinen bis mittleren Implementierungen installiert.

QRadar Packet Capture-Appliances können wie im folgenden Diagramm veranschaulicht mit IBM Security QRadar Incident Forensics Standalone verbunden werden.

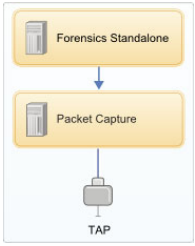


Abbildung 2. Beispiel für eine IBM Security QRadar Incident Forensics Standalone-Implementierung

Einschränkung: QRadar Incident Forensics Standalone können keine verwalteten Hosts hinzugefügt werden; es ist auch nicht möglich, QRadar Incident Forensics Standalone mit der QRadar-Konsole zu verbinden.

Verteilte Implementierungen

Bei Implementierungen, für die die forensische Netzanalyse und weitere Security Intelligence-Funktionen benötigt werden, werden die QRadar-Konsole sowie mindestens ein verwalteter QRadar Incident Forensics-Host installiert. Die QRadar-Konsole stellt SIEM (Security Information and Event Management), das Protokollmanagement, die Anomalieerkennung, das Risikomanagement und das Schwachstellenmanagement bereit.

In einer verteilten Implementierung sind drei Appliances vorhanden:

- QRadar-Konsole
- Ein verwalteter QRadar Incident Forensics-Host (QRadar Incident Forensics Processor)
- QRadar Packet Capture (optional)

Alle IBM Security QRadar-Appliances in einer Implementierung müssen Software derselben Version und mit demselben Fix-Level haben. Implementierungen, in denen unterschiedliche Softwareversionen verwendet werden, werden nicht unterstützt.

Das folgende Diagramm veranschaulicht die Verbindung mehrerer verwalteter QRadar Incident Forensics-Hosts mit der QRadar-Konsole. Sie können QRadar Packet Capture-Einheiten mit den verwalteten QRadar Incident Forensics-Hosts verbinden (QRadar Incident Forensics Processor).

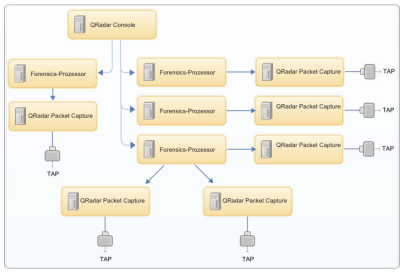


Abbildung 3. Beispiel für eine verteilte Implementierung

QRadar Incident Forensics-Komponenten

QRadar-Implementierungen können sich aus den folgenden Komponenten zusammensetzen:

QRadar-Konsole
Stellt die Benutzerschnittstelle des QRadar-Produkts bereit. Über die Schnittstelle werden Echtzeitanzeigen von Ereignissen und Datenflüssen, Berichte, Angriffe, Informationen zu Assets sowie Verwaltungsfunktionen bereitgestellt.

In verteilten Implementierungen werden mehrere QRadar Incident Forensics Processor-Hosts über die QRadar-Konsole verwaltet.

QRadar Incident Forensics Processor

Stellt die QRadar Incident Forensics-Produktschnittstelle bereit. Die Schnittstelle stellt Tools zur Verfügung, mit denen die einzelnen Schritte von Cyberverbrechern zurückverfolgt, Netzrohdaten in Zusammenhang mit Sicherheitszwischenfällen wiederhergestellt, Suchläufe in allen verfügbaren unstrukturierten Daten durchgeführt und Sitzungen und Ereignisse visuell wiederhergestellt werden können.

Sie müssen QRadar Incident Forensics Processor als verwalteten Host hinzufügen, damit Sie die Security Intelligence-Forensikfunktionen nutzen können.

QRadar Incident Forensics Standalone
Stellt die Benutzerschnittstelle des QRadar Incident Forensics-Produkts bereit. Mit der Installation von QRadar Incident Forensics Standalone werden

die Tools zur Verfügung gestellt, die für forensische Untersuchungen erforderlich sind. Es stehen nur Funktionen für die forensische Untersuchung sowie die zugehörigen Verwaltungsfunktionen zur Verfügung.

QRadar Packet Capture

Sie haben die Möglichkeit, eine optionale QRadar Packet Capture-Appliance zu installieren. Ist keine andere Einheit zur Aufzeichnung von Netzpaketdaten (PCAP) vorhanden, können Sie mit dieser Appliance die von QRadar Incident Forensics verwendeten Daten speichern. Sie können beliebig viele dieser Appliances als Netz-TAP oder Teilnetz zur Erfassung unstrukturierter Paketdaten installieren.

Ist keine Paketaufzeichnungseinheit verbunden, können Sie die Paketaufzeichnungsdateien entweder manuell oder über FTP in die Benutzerschnittstelle hochladen.

Kapitel 3. Installation von QRadar Incident Forensics - Übersicht

Sie können die QRadar Incident Forensics-Software auf Ihrer eigenen Appliance oder auf einer virtuellen Appliance installieren. Auf QRadar Incident Forensics-Appliances ist die QRadar Incident Forensics-Software installiert.

QRadar Incident Forensics muss unter dem Betriebssystem Red Hat Enterprise Linux installiert werden.

Auswahl der Appliance-ID

Meistens werden für QRadar Incident Forensics mindestens zwei ISO-Images installiert:

- QRadar-Konsole

  QRadar-Produkte verwenden dasselbe Installationssoftwareimage. Über den *Aktivierungsschlüssel* werden der Appliancetyp und die Komponenten angegeben, die installiert werden sollen. Bei Eingabe des Aktivierungsschlüssels werden Sie zur Angabe des Appliancetyps aufgefordert. Die QRadar-Konsole muss installiert werden.
- 6000 QRadar Incident Forensics Processor (verwalteter Host)

  Aufgrund von Exportbestimmungen werden QRadar Incident Forensics-Komponenten über ein anderes ISO-Image installiert. Sie müssen den verwalteten QRadar Incident Forensics-Host installieren und ihn so konfigurieren, dass er mit der QRadar-Konsole verbunden ist.

Bei All-in-one-Installationen wird nur das ISO-Image für 6100 QRadar Incident Forensics installiert und die Komponente QRadar Incident Forensics Standalone ausgewählt.

Bei der Installation von QRadar Incident Forensics erhalten Sie über einen Standardlizenzschlüssel fünf Wochen lang Zugriff auf das Produkt. Vor Ablauf dieser Standardlizenz müssen Sie dem System einen Lizenzschlüssel zuordnen.

Installationsschritte

Führen Sie bei verteilten Installationen die folgenden Installationsschritte aus:

1. Überprüfen Sie die Hardware- und Softwarevoraussetzungen.
2. Installieren Sie die Software der QRadar-Konsole.
3. Installieren Sie den verwalteten QRadar Incident Forensics-Host.
4. Implementieren Sie den verwalteten QRadar Incident Forensics-Host.
5. Fügen Sie Paketaufzeichnungseinheiten hinzu.

Aktivierungsschlüssel und Lizenzschlüssel

Bei der Installation von IBM Security QRadar-Appliances müssen Sie einen Aktivierungsschlüssel eingeben. Nach der Installation müssen Sie Ihre Lizenzschlüssel anwenden. Um zu verhindern, dass im Installationsprozess der falsche Schlüssel eingegeben wird, ist es wichtig, den Unterschied zwischen den Schlüsseln zu kennen.

Aktivierungsschlüssel

Der Aktivierungsschlüssel ist eine aus 24 Zeichen und vier Teilen bestehende alphanumerische Zeichenfolge, die Sie von IBM erhalten. Alle Installationen von QRadar-Produkten verwenden dieselbe Software. Der Aktivierungsschlüssel gibt jedoch an, welche Softwaremodule für die einzelnen Appliance-Typen anzuwenden sind. Verwenden Sie beispielsweise den IBM Security QRadar QFlow Collector-Aktivierungsschlüssel, um nur die QRadar QFlow Collector-Module zu installieren.

Sie finden den Aktivierungsschlüssel an folgenden Orten:

- Wenn Sie eine Appliance erworben haben, die mit QRadar-Software vorinstalliert wird, ist der Aktivierungsschlüssel in einem Dokument auf der beigefügten CD enthalten.
- Wenn Sie QRadar-Software oder eine virtuelle Appliance heruntergeladen haben, enthält das Dokument *Erste Schritte* eine Liste mit Aktivierungsschlüsseln. Das Dokument *Erste Schritte* ist an die Bestätigungs-E-Mail angehängt.

Lizenzschlüssel

Ihr System schließt einen temporären Lizenzschlüssel ein, mit dem Sie fünf Wochen lang Zugriff auf QRadar-Software haben. Nach der Installation der Software und vor Ablauf des Standardlizenzschlüssels müssen Sie Ihre erworbenen Lizenzen hinzufügen.

Wenn Sie ein QRadar-Produkt kaufen, sendet Ihnen IBM eine E-Mail mit dem permanenten Lizenzschlüssel. Diese Lizenzschlüssel erweitern die Funktionalität Ihres Appliance-Typs und definieren die Betriebsparameter Ihres Systems. Sie müssen Ihre Lizenzschlüssel anwenden, bevor die Standardlizenz abläuft.

Hardwarezubehör- und Desktop-Software-Voraussetzungen für QRadar-Installationen

Stellen Sie vor der Installation von IBM Security QRadar-Produkten sicher, dass Sie Zugriff auf das erforderliche Hardwarezubehör und die erforderliche Desktop-Software haben.

Hardwarezubehör

Stellen Sie sicher, dass Sie auf folgende Hardwarekomponenten zugreifen können:

- Monitor und Tastatur
- Unterbrechungsfreie Stromversorgung für alle Systeme, auf denen Daten gespeichert werden (beispielsweise QRadar-Konsole, Ereignisprozessor-Komponenten oder QRadar QFlow Collector-Komponenten)

Wichtig: QRadar-Produkte unterstützen hardwarebasierte RAID-Implementierungen (Redundant Array of Independent Disks), aber keine softwarebasierten RAID-Installationen.

Desktop-Software-Voraussetzungen

Stellen Sie sicher, dass folgende Anwendungen auf allen Desktopsystemen installiert sind, die Sie für den Zugriff auf die Benutzerschnittstelle des QRadar-Produkts verwenden:

- Java™ Runtime Environment (JRE) Version 1.7 oder IBM 64-Bit Runtime Environment for Java V7.0

- Adobe Flash Version 10.x

Unterstützte Web-Browser

In der folgenden Tabelle sind die unterstützten Web-Browser aufgeführt:

Tabelle 1. Unterstützte Web-Browser für QRadar-Produkte

Web-Browser	**Unterstützte Versionen**
Mozilla Firefox	45.2 Extended Support Release
64-Bit-Version Microsoft Internet Explorer mit aktiviertem Microsoft Edge-Modus.	11.0
Google Chrome	Neueste Version

Bei Verwendung von Microsoft Internet Explorer müssen Sie den Dokumentmodus und den Browsermodus aktivieren:

1. Drücken Sie im Web-Browser Internet Explorer auf die Taste F12, um das Fenster **Entwicklertools** zu öffnen.
2. Klicken Sie auf **Browsermodus** und wählen Sie die Version Ihres Web-Browsers aus.
3. Klicken Sie auf **Dokumentmodus**.
   - Wählen Sie bei Verwendung von Explorer V9.0 den Eintrag **Internet Explorer 9-Standards** aus.
   - Wählen Sie bei Verwendung von Internet Explorer V10.0 den Eintrag **Internet Explorer 10-Standards** aus.

Ports, die für die Kommunikation zwischen QRadar Incident Forensics-Hosts geöffnet sein müssen

In der folgenden Tabelle sind die Ports aufgelistet, die zwischen den QRadar Incident Forensics-Hosts geöffnet sein müssen:

Tabelle 2. Offene Ports zwischen Hosts

Port	**Beschreibung**
443	Muss für die Analyse der Artefakte geöffnet sein.
28080	Muss für die verteilte Suche geöffnet sein.

Kapitel 4. QRadar Incident Forensics-Softwareinstallationen auf Ihrer eigenen Appliance

Damit IBM Security QRadar Incident Forensics erfolgreich auf Ihrer eigenen Appliance installiert werden kann, müssen Sie das RHEL-Betriebssystem (Red Hat Enterprise Linux), die QRadar-Konsole und den verwalteten QRadar Incident Forensics-Host installieren.

Bei neuen Softwareinstallationen, bei denen QRadar Incident Forensics mit IBM Security QRadar kombiniert ist, werden zwei ISO-Dateien installiert:

- QRadar

  Mit einer einzigen ISO-Datei kann (mit Ausnahme von QRadar Incident Forensics) jedes QRadar-Produkt installiert werden. Welcher QRadar-Appliancetyp installiert wird, hängt von dem Aktivierungsschlüssel ab, den Sie eingeben.
- QRadar Incident Forensics

  Dieses ISO-Image enthält den QRadar Incident Forensics Processor und QRadar Incident Forensics Standalone. Der QRadar Incident Forensics Processor muss installiert werden.

Voraussetzungen für die Installation von QRadar Incident Forensics auf einer eigenen Appliance

Bevor Sie das Betriebssystem Red Hat Enterprise Linux (RHEL) auf einer eigenen Appliance installieren, müssen Sie sicherstellen, dass Ihr System die Systemvoraussetzungen erfüllt.

In der folgenden Tabelle werden die Systemvoraussetzungen beschrieben:

Tabelle 3. Systemvoraussetzungen für RHEL-Installationen auf einer eigenen Appliance

Voraussetzung	**Details**
Unterstützte Softwareversion	Version 6.7
Bitversion	64 Bit
Kickstart-Platten	Nicht unterstützt
Arbeitsspeicher (RAM) für Forensics-Prozessor	Mindestens 128 GB **Wichtig:** Sie müssen den Systemspeicher vor der Installation von QRadar aufrüsten.
Freier Plattenspeicherplatz für Forensics-Prozessor	Mindestens 5 % des Gesamtplattenspeicherplatzes **Wichtig:** Für eine optimale Leistung ist sicherzustellen, dass zusätzlich das Zwei- bis Dreifache des minimalen Plattenspeicherplatzes verfügbar ist.

Tabelle 3. Systemvoraussetzungen für RHEL-Installationen auf einer eigenen Appliance (Forts.)

Voraussetzung	Details
Firewallkonfiguration	WWW (http, https) aktiviert SSH aktiviert **Wichtig:** Inaktivieren Sie die Option SELinux, bevor Sie die Firewall konfigurieren. Die QRadar-Installation schließt eine Standardfirewallvorlage ein, die Sie im Fenster **Systeminstallation** aktualisieren können.

Einschränkung: Eine Änderung der Größe logischer Datenträger mithilfe eines Logical Volume Manager (LVM) wird nicht unterstützt.

Partitionseigenschaften des Betriebssystems Linux für QRadar-Installationen auf Ihrer eigenen Appliance

Bei Verwendung einer eigenen Appliance können Sie Partitionen im Betriebssystem Red Hat Enterprise Linux löschen und neu erstellen, statt die Standardpartitionen zu ändern.

Orientieren Sie sich an den Werten in der folgenden Tabelle, wenn Sie die Partitionierung im Betriebssystem Red Hat Enterprise Linux neu erstellen.

Das Dateisystem für jede Partition ist XFS.

Tabelle 4. Partitionsleitfaden für RHEL

Mountpfad	LVM-unterstützt?	In Softwareinstallation vorhanden?	Größe
`/boot`	Nein	Ja	1 GB
`/boot/efi`	Nein	Ja	200 MB
`/recovery`	Nein	Nein	8 GB
`/var`	Ja	Ja	5 GB
`/var/log`	Ja	Ja	15 GB
`/var/log/audit`	Ja	Ja	3 GB
`/opt`	Ja	Ja	10 GB
`/home`	Ja	Ja	1 GB
`/storetmp`	Ja	Ja	15 GB
`/tmp`	Ja	Ja	3 GB
`swap`	nicht zutreffend	Ja	Auslagerungsformel: Konfigurieren Sie für die Auslagerungspartition eine Größe von 75 % des Arbeitsspeichers (mit einem Mindestwert von 12 GiB und einem Maximalwert von 24 GiB).

Tabelle 4. Partitionsleitfaden für RHEL (Forts.)

Mountpfad	LVM-unterstützt?	In Softwareinstallation vorhanden?	Größe
/	Ja	Ja	Bis zu 15 GB
/store	Ja	Ja	80 % des restlichen Speicherplatzes
/transient	Ja	Ja	20 % des restlichen Speicherplatzes

RHEL auf eigener Appliance installieren

Sie können das Betriebssystem Red Hat Enterprise Linux für die gemeinsame Nutzung mit QRadar Incident Forensics auf einer eigenen Appliance installieren.

Vorgehensweise

1. Kopieren Sie die ISO-DVD mit dem Betriebssystem Red Hat Enterprise Linux auf eines der folgenden tragbaren Speichermedien:
   - DVD (Digital Versatile Disk)
   - Bootfähiges USB-Flashlaufwerk

     Informationen zum Erstellen eines bootfähigen USB-Flashlaufwerks finden Sie im *IBM Security QRadar-Installationshandbuch*.
2. Legen Sie das tragbare Speichermedium in Ihre Appliance ein und führen Sie einen Neustart der Appliance durch.
3. Wählen Sie im Eingangsmenü eine der folgenden Optionen aus.
   - Wählen Sie das USB- oder DVD-Laufwerk als Bootoption aus.
   - Für die Installation auf einem System, das Extensible Firmware Interface (EFI) unterstützt, müssen Sie das System im Modus legacy (traditionell) starten.
4. Melden Sie sich bei einer entsprechenden Aufforderung als Rootbenutzer bei Ihrem System an.
5. Sie können ein Problem mit der Ethernet-Schnittstellenadressenbenennung verhindern, indem Sie auf der Seite **Willkommen** die Tabulatortaste drücken und am Ende der Zeile Vmlinuz initrd=initrd.image den Eintrag biosdevname=0 hinzufügen.
6. Folgen Sie den Anweisungen im Installationsassistenten, um die Installation durchzuführen:
   a. Wählen Sie die Option **Basisspeichermedien** aus.
   b. Bei der Konfiguration des Hostnamens kann der Wert für die Eigenschaft **Hostname** Buchstaben, Zahlen und Bindestriche einschließen.
   c. Wählen Sie bei der Konfiguration des Netzes im Fenster **Netzverbindungen** den Eintrag **System eth0** aus. Klicken Sie dann auf **Bearbeiten** und wählen Sie **Automatisch verbinden** aus.
   d. Wählen Sie auf der Registerkarte **IPv4-Einstellungen** in der Liste **Methode** den Eintrag **Manuell** aus.
   e. Geben Sie im Feld **DNS-Server** eine durch Kommas getrennte Liste ein.
   f. Wählen Sie die Option **Angepasstes Layout erstellen** aus.
   g. Konfigurieren Sie EXT4 als Dateisystemtyp für die Partition /boot.
   h. Führen Sie eine Neuformatierung der Auslagerungspartition mit dem Dateisystemtyp 'swap' durch.

i. Wählen Sie **Basisserver** aus.

7. Klicken Sie nach Abschluss der Installation auf **Neu starten**.
8. Stellen Sie sicher, dass die Onboard-Netzschnittstellen die Namen `eth0`, `eth1`, `eth2` und `eth3` haben.

Nächste Schritte

Kapitel 7, „QRadar-Konsole installieren", auf Seite 21

Kapitel 5. QRadar Incident Forensics-Softwareinstallation auf einer QRadar Incident Forensics-Appliance

IBM Security QRadar Incident Forensics-Appliances werden mit einem vorinstallierten RHEL-Betriebssystem (Red Hat Enterprise Linux) und vorinstallierter QRadar-Software geliefert.

Bei neuen Softwareinstallationen, bei denen QRadar Incident Forensics mit IBM Security QRadar kombiniert ist, werden die beiden vorinstallierten ISO-Dateien konfiguriert:

- QRadar

  Mit einer einzigen ISO-Datei kann (mit Ausnahme von QRadar Incident Forensics) jedes QRadar-Produkt installiert werden. Welcher QRadar-Appliancetyp installiert wird, hängt von dem Aktivierungsschlüssel ab, den Sie eingeben.
- QRadar Incident Forensics

  Dieses ISO-Image enthält den QRadar Incident Forensics Processor und QRadar Incident Forensics Standalone. Der QRadar Incident Forensics Processor muss installiert werden.

Bei neuen Softwareinstallationen, für die nur die Forensikfunktionen erforderlich sind, wird QRadar Incident Forensics Standalone über das ISO-Image für QRadar Incident Forensics installiert.

Kapitel 6. Installation von QRadar Incident Forensics auf virtuellen Appliances

Sie haben die Möglichkeit, IBM Security QRadar Incident Forensics auf einer virtuellen Appliance zu installieren. Dabei müssen Sie sicherstellen, dass eine unterstützte virtuelle Appliance verwendet wird, die die Systemmindestvoraussetzungen erfüllt.

Bei einer virtuellen Appliance handelt es sich um ein QRadar Incident Forensics-System, bei dem die QRadar Incident Forensics-Software auf einer virtuellen VMWare ESX -Maschine installiert wird.

Eine virtuelle Appliance bietet in Ihrer virtuellen Netzinfrastruktur dieselbe Sichtbarkeit und dieselben Funktionen wie QRadar-Appliances in Ihrer physischen Umgebung.

Installationsprozess

So installieren Sie eine virtuelle Appliance:

__ • Erstellen Sie eine virtuelle Maschine.

__ • Installieren Sie die IBM Security QRadar Incident Forensics-Software auf dieser virtuellen Maschine.

__ • Wenn Sie QRadar Incident Forensics Processor installiert haben, fügen Sie Ihre virtuelle Appliance der Implementierung hinzu.

Systemvoraussetzungen für virtuelle Appliances

Stellen Sie vor der Installation der virtuellen Appliance sicher, dass sie die folgenden Mindestvoraussetzungen erfüllt:

Tabelle 5. Voraussetzungen für virtuelle Appliances.

Voraussetzung	**Beschreibung**
VMware-Client	VMware ESXi Version 5.0 VMware ESXi Version 5.1 VMware ESXi Version 5.5 Weitere Informationen zu VMWare-Clients finden Sie auf der VMware-Website (www.vmware.com).
Größe der virtuellen Platte	Minimum: 256 GB **Wichtig:** Um eine optimale Leistung zu erhalten, sollten Sie sicherstellen, dass darüber hinaus die zwei- bis dreifache Menge des mindestens erforderlichen Plattenspeichers zur Verfügung steht.

Virtuelle Maschine erstellen

Damit eine virtuelle Appliance installiert werden kann, müssen Sie zunächst mithilfe von VMWare ESX eine virtuelle Maschine erstellen.

Vorgehensweise

1. Klicken Sie im VMware vSphere Client auf **Datei** > **Neu** > **Virtuelle Maschine**.
2. Fügen Sie Name und Position hinzu und wählen Sie den Datenspeicher für die neue virtuelle Maschine aus.
3. Gehen Sie wie folgt vor:
   a. Wählen Sie im Teilfenster **Konfiguration** des Fensters **Neue virtuelle Maschine erstellen** die Option **Angepasst** aus.
   b. Wählen Sie im Teilfenster **Version der virtuellen Maschine** die Option **Version der virtuellen Maschine: 7** aus.
   c. Wählen Sie **Linux** und anschließend **Red Hat Enterprise Linux 6 (64 Bit)** als **Betriebssystem** aus.
   d. Konfigurieren Sie auf der Seite **CPUs** die Anzahl der virtuellen Prozessoren für die virtuelle Maschine. Wählen Sie 40 oder höher aus.
   e. Geben Sie im Feld **Speicherkapazität** den erforderlichen RAM-Wert für Ihre Implementierung ein bzw. wählen Sie den Wert aus. Wählen Sie 128 GB oder höher aus.
   f. Konfigurieren Sie die Netzverbindungen entsprechend den Angaben in der folgenden Tabelle.

Tabelle 6. Beschreibung der Netzkonfigurationsparameter

Parameter	Beschreibung
Wie viele NICs sollen angeschlossen werden	Sie müssen mindestens einen Netzschnittstellencontroller (NIC) hinzufügen.
Adapter	`VMXNET3`

   g. Wählen Sie im Teilfenster **SCSI-Controller** die Option **VMware Paravirtual** aus.
   h. Wählen Sie im Teilfenster **Platte** die Option **Neue virtuelle Platte erstellen** aus und konfigurieren Sie die Parameter der virtuellen Platte entsprechend den Angaben in der folgenden Tabelle.

Tabelle 7. Einstellungen für die Größe der virtuellen Platte und Parameter für die Einrichtungsrichtlinie

Eigenschaft	Option
Kapazität	2 oder höher (TB)
Platteneinrichtung	Thin Provisioning
Erweiterte Optionen	Nicht konfigurieren

4. Überprüfen Sie auf der Seite **Bereit für die Fertigstellung** die von Ihnen vorgenommenen Einstellungen und klicken Sie auf **Fertigstellen**.

Nächste Schritte

Installieren Sie die QRadar-Software auf Ihrer virtuellen Maschine.

QRadar Incident Forensics-Software auf einer virtuellen Maschine installieren

Nach der Erstellung der virtuellen Maschine müssen Sie die IBM Security QRadar-Software auf dieser virtuellen Maschine installieren.

Einschränkung: Eine Änderung der Größe logischer Datenträger mithilfe eines Logical Volume Manager (LVM) wird nicht unterstützt.

Vorgehensweise

1. Wählen Sie im Navigationsbereich links im VMware vSphere Client Ihre virtuelle Maschine aus.
2. Klicken Sie im rechten Teilfenster auf die Registerkarte **Zusammenfassung**.
3. Klicken Sie im Teilfenster **Befehle** auf **Einstellungen bearbeiten**.
4. Klicken Sie im linken Teilfenster des Fensters **Virtuelle Maschine - Eigenschaften** auf **CD-/DVD-Laufwerk 1**.
5. Aktivieren Sie im Teilfenster **Einheitenstatus** das Kontrollkästchen **Beim Einschalten verbinden**.
6. Wählen Sie im Teilfenster **Einheitentyp** die Option **ISO-Datenspeichertyp** aus und klicken Sie auf **Durchsuchen**.
7. Suchen Sie im Fenster **Datenspeicher durchsuchen** auf die ISO-Datei des Produkts; wählen Sie die Datei aus und klicken Sie auf **Öffnen** und anschließend auf **OK**.
8. Klicken Sie nach der Installation des ISO-Produktimages mit der rechten Maustaste auf die virtuelle Maschine und klicken Sie auf **Stromversorgung** > **Einschalten**.
9. Melden Sie sich bei der virtuellen Maschine an, indem Sie `root` als Benutzername eingeben.

   Bei der Eingabe des Benutzernamens muss die Groß-/Kleinschreibung beachtet werden.
10. Stellen Sie sicher, dass die **Endbenutzerlizenzvereinbarung** angezeigt wird.

    Tipp: Die Navigation durch das Dokument erfolgt durch Drücken der Leertaste.
11. Wählen Sie auf der Seite **Appliance-ID auswählen** die QRadar Incident Forensics-Komponente aus, die installiert werden soll:
    - Bei einer verteilten Installation: **6000 QRadar Incident Forensics Processor**.
    - Bei eigenständigen Implementierungen: **6100 QRadar Incident Forensics Standalone**.
12. Wählen Sie **normal** als Installationsoption aus.
13. Folgen Sie den Anweisungen im Installationsassistenten, um die Installation durchzuführen.

    Die folgende Tabelle enthält Beschreibungen und Hinweise, die Ihnen bei der Konfiguration der Installation helfen.

Tabelle 8. Beschreibung von Netzeinstellungen

Netzeinstellung	Beschreibung
Hostname	Vollständig qualifizierter Domänenname
Sekundäre DNS-Serveradresse	Optional

Tabelle 8. Beschreibung von Netzeinstellungen (Forts.)

Netzeinstellung	Beschreibung
Öffentliche IP-Adresse für Netze, die die Netzadressumsetzung verwenden	Nicht unterstützt
E-Mail-Servername	Wenn kein E-Mail-Server vorhanden ist, verwenden Sie `localhost`.
Rootkennwort	Das Kennwort muss folgende Bedingungen erfüllen: • Mindestens 5 Zeichen • Keine Leerzeichen • Zulässige Sonderzeichen: @, #, ^ und *

Nachdem Sie die Installationsparameter konfiguriert haben, wird eine Folge von Nachrichten angezeigt. Der Installationsprozess kann mehrere Minuten dauern.

Nächste Schritte

Wenn Sie keine IBM Security QRadar Incident Forensics Standalone-Instanz installieren, fahren Sie mit Kapitel 9, „Verwalteten QRadar Incident Forensics-Host zu QRadar-Konsole hinzufügen", auf Seite 25 fort.

Kapitel 7. QRadar-Konsole installieren

Bei verteilten Installationen werden die QRadar-Konsole und der verwaltete IBM Security QRadar Incident Forensics-Host jeweils auf einer eigenen Appliance installiert.

Einschränkung: Alle Appliances in einer Implementierung müssen Software derselben Version und mit demselben Fix-Level haben. Implementierungen, in denen unterschiedliche Softwareversionen verwendet werden, werden nicht unterstützt.

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

- Die erforderliche Hardware ist installiert.
- Sie besitzen den erforderlichen Lizenzschlüssel für Ihre Appliance.
- Eine Tastatur und ein Monitor sind über den VGA-Anschluss verbunden.
- Informationen zur Konfiguration verbundener Netzschnittstellen finden Sie unter www.ibm.com/developerworks (http://www.ibm.com/developerworks/library/se-nic4qradar/).
- Es gibt weder auf der Konsole noch auf den verwalteten Hosts abgelaufene Lizenzen.

Wichtig: Wenn Sie vor dem Start des Installationsassistenten zur Eingabe eines Benutzernamens und Kennworts aufgefordert werden, geben Sie `root` als Benutzername und `password` als Kennwort ein.

Vorgehensweise

1. Bei Installationen auf Ihrer eigenen Hardware oder auf virtuellen Maschinen wird das ISO-Image der QRadar-Konsole dem Stammverzeichnis hinzugefügt.
   a. Geben Sie folgenden Befehl ein, um das Verzeichnis `/media/dvd` zu erstellen:
      `mkdir /media/dvd`
   b. Geben Sie folgenden Befehl ein, um das ISO-Image der QRadar-Konsole anzuhängen:
      `mount -o loop <QRadar_ISO> /media/dvd`
2. Starten Sie die Installation mit dem Setup-Script.
   a. Wechseln Sie mit folgendem Befehl das Arbeitsverzeichnis: `cd /media/dvd`
   b. Starten Sie das Setup-Script durch Eingabe des folgenden Befehls: `setup.sh`
3. Gehen Sie entsprechend den Anweisungen im Installationsassistenten vor.
   - Wenn Sie zur Eingabe des Aktivierungsschlüssels aufgefordert werden, geben Sie in dem entsprechenden Feld die alphanumerische 24-stellige Zeichenfolge (in vier Blöcken angeordnet) ein, die Sie von IBM erhalten haben.

     Der Buchstabe I und die Zahl 1 (eins) werden gleich behandelt. Auch der Buchstabe O und die Zahl 0 (null) werden gleich behandelt.
   - Wenn Sie über keinen E-Mail-Server verfügen, geben Sie auf der Seite **Netzinformationen eingeben, die verwendet werden sollen** im Feld **Name des E-Mail-Servers** `localhost` ein.
   - Erstellen Sie im Feld **Rootkennwort** ein Kennwort, das folgende Bedingungen erfüllt:

- Es enthält mindestens fünf Zeichen
- Es enthält keine Leerzeichen
- Es kann die folgenden Sonderzeichen enthalten: @, #, ^ und *

Der Installationsprozess kann mehrere Minuten dauern.

4. Wenden Sie Ihren Lizenzschlüssel an.
   a. Melden Sie sich bei QRadar an:

      `https://`*`IP-Adresse_QRadar`*

      Der Standardbenutzername ist `admin`. Das Kennwort entspricht dem Kennwort des Rootbenutzerkontos.
   b. Klicken Sie auf **Bei QRadar anmelden**.
   c. Klicken Sie auf die Registerkarte **Verwaltung**.
   d. Klicken Sie in der Navigationsleiste auf **Systemkonfiguration**.
   e. Klicken Sie auf das Symbol **System- und Lizenzverwaltung**.
   f. Wählen Sie im Listenfeld **Anzeige** die Option **Lizenzen** aus und laden Sie Ihren Lizenzschlüssel hoch.
   g. Wählen Sie die nicht zugeordnete Lizenz aus und klicken Sie auf **System einer Lizenz zuordnen**.
   h. Wählen Sie in der Liste der Systeme ein System aus und klicken Sie auf **System einer Lizenz zuordnen**.

Nächste Schritte

Sie können jetzt QRadar Incident Forensics installieren.

Kapitel 8. QRadar Incident Forensics installieren

Bei verteilten Installationen werden die QRadar-Konsole und der verwaltete IBM Security QRadar Incident Forensics-Host (QRadar Incident Forensics Processor) jeweils auf einer eigenen Appliance installiert. Bei einer eigenständigen Implementierung wird nur die QRadar Incident Forensics Standalone-Komponente installiert.

Einschränkung: Alle Appliances in einer Implementierung müssen Software derselben Version und mit demselben Fix-Level haben. Implementierungen, in denen unterschiedliche Softwareversionen verwendet werden, werden nicht unterstützt.

Vorbereitende Schritte

Stellen Sie sicher, dass die folgenden Voraussetzungen erfüllt sind:

__ • Die erforderliche Hardware ist installiert.

__ • Eine Tastatur und ein Monitor sind über den VGA-Anschluss verbunden.

__ • Der Aktivierungsschlüssel ist verfügbar.

Einschränkung: Eine Änderung der Größe logischer Datenträger mithilfe eines Logical Volume Manager (LVM) wird nicht unterstützt.

Vorgehensweise

1. Bei Installationen auf Ihrer eigenen Hardware oder auf virtuellen Maschinen wird das ISO-Image von QRadar Incident Forensics dem Stammverzeichnis hinzugefügt.
   a. Geben Sie folgenden Befehl ein, um das Verzeichnis `/media/dvd` zu erstellen:
      ```
      mkdir /media/dvd
      ```
   b. Geben Sie folgenden Befehl ein, um das ISO-Image der QRadar-Konsole anzuhängen:
      ```
      mount -o loop <QRadar_Incident_Forensics_ISO>/media/dvd
      ```
2. Starten Sie die Installation mit dem Setup-Script.
   a. Wechseln Sie mit folgendem Befehl das Arbeitsverzeichnis: `cd /media/dvd`
   b. Starten Sie das Setup-Script durch Eingabe des folgenden Befehls: `setup.sh`
3. Gehen Sie entsprechend den Anweisungen im Installationsassistenten vor.

   Wählen Sie auf der Seite **Appliance-ID auswählen** die QRadar Incident Forensics-Komponente aus, die installiert werden soll:
   - Bei einer verteilten Installation: **6000 QRadar Incident Forensics Processor**
   - Bei eigenständigen Implementierungen: **6100 QRadar Incident Forensics Standalone**

   Einschränkung: Die folgenden Konfigurationsoptionen werden für QRadar Incident Forensics nicht unterstützt:
   - Die Option **Konfiguration für HA-Wiederherstellung** auf der Seite **Konfigurationstyp auswählen**
   - Die Option **Verbundenen Schnittstellenkonfigurationsmodus verwenden** auf der Seite **Verbundenen Schnittstellenkonfigurationsmodus auswählen**

   Die Installation der QRadar Incident Forensics Processor-Instanz kann mehrere Minuten dauern.

4. Wenden Sie Ihren Lizenzschlüssel an.
   a. Melden Sie sich bei QRadar an:

      `https://`*`IP-Adresse_QRadar`*

      Der Standardbenutzername ist `admin`. Das Kennwort entspricht dem Kennwort des Rootbenutzerkontos.
   b. Klicken Sie auf die Anmeldeoption.
   c. Klicken Sie auf die Registerkarte **Verwaltung**.
   d. Klicken Sie in der Navigationsleiste auf **Systemkonfiguration**.
   e. Klicken Sie auf das Symbol **System- und Lizenzverwaltung**.
   f. Wählen Sie im Listenfeld **Anzeige** die Option **Lizenzen** aus und laden Sie Ihren Lizenzschlüssel hoch.
   g. Wählen Sie die nicht zugeordnete Lizenz aus und klicken Sie auf **System einer Lizenz zuordnen**.
   h. Wählen Sie in der Lizenzliste eine Lizenz aus und klicken Sie auf **Lizenz dem System zuordnen**.

   Anmerkung: Bei der Installation einer eigenständigen Implementierung (6100) müssen Sie der IBM Security QRadar Incident Forensics Standalone-Appliance zwei Lizenzschlüssel zuordnen. Eine Lizenz ist für QRadar Incident Forensics Standalone, die andere für den Zugriff auf die Registerkarte **Forensik**.

   Möglicherweise benötigen Sie für jede verteilte Installation (6000) in einer bestehenden IBM Security QRadar SIEM-Umgebung eine Lizenz für jeden verwalteten Forensics-Host (6000) und außerdem eine Einfachlizenz zur Aktivierung der Registerkarte **Forensics** auf der Konsole. Wenn der vorhandene Lizenzschlüssel der QRadar-Konsole auch den Zugriff auf die Registerkarte **Forensics** ermöglicht, benötigen Sie nur den Installationslizenzschlüssel. Wenn der vorhandene Lizenzschlüssel der QRadar-Konsole keinen Zugriff auf die Registerkarte **Forensics** ermöglicht, benötigen Sie neben dem Installationslizenzschlüssel auch einen aktualisierten Forensics-Aktivierungsschlüssel.

Nächste Schritte

Implementieren Sie den verwalteten QRadar Incident Forensics Processor-Host. Weitere Informationen finden Sie in Kapitel 9, „Verwalteten QRadar Incident Forensics-Host zu QRadar-Konsole hinzufügen”, auf Seite 25.

Kapitel 9. Verwalteten QRadar Incident Forensics-Host zu QRadar-Konsole hinzufügen

Bei verteilten Installationen müssen Sie IBM Security QRadar Incident Forensics Processor als verwalteten Host zur QRadar-Konsole hinzufügen.

Jede QRadar-Appliance in der Implementierung, bei der es sich nicht um eine Konsolen-Appliance handelt, ist ein *verwalteter Host*. Um eine verteilte Verarbeitung zu ermöglichen, können Sie mehr als einen QRadar Incident Forensics Processor als verwalteten Host hinzufügen.

Einschränkung: Es ist nicht möglich, verwaltete QRadar Incident Forensics-Hosts über den Implementierungseditor hinzuzufügen bzw. zu entfernen. Dies ist nur über das Tool 'System- und Lizenzverwaltung' möglich.

Vorbereitende Schritte

Die Software der QRadar-Konsole muss zuerst installiert werden. Weitere Informationen finden Sie in Kapitel 7, „QRadar-Konsole installieren", auf Seite 21.

Vorgehensweise

1. Melden Sie sich als Administrator bei der QRadar-Konsole an:

   `https://IP-Adresse_QRadar`

   Der Standardbenutzername ist `admin`. Bei dem Kennwort handelt es sich um das Kennwort des Rootbenutzerkontos, das bei der Installation eingegeben wurde.
2. Klicken Sie auf die Registerkarte **Verwaltung**.
3. Klicken Sie im Teilfenster **Systemkonfiguration** auf **System- und Lizenzverwaltung**.
4. Klicken Sie in der Hosttabelle auf den Host der QRadar-Konsole und anschließend auf > **Implementierungsaktionen** > **Host hinzufügen**.
5. Geben Sie die Informationen zur QRadar Incident Forensics Processor-Appliance ein und klicken Sie auf **Hinzufügen**.

   Einschränkung: Die Eigenschaften **Host verschlüsseln** und **Netzadressumsetzung (NAT)** werden nicht unterstützt.
6. Klicken Sie in der Menüleiste der Registerkarte **Verwaltung** auf **Änderungen implementieren**.
7. Aktualisieren Sie den Web-Browser.

   Die Registerkarte **Forensik** wird jetzt angezeigt.

Nächste Schritte

Sie können die IBM Security QRadar Packet Capture-Einheit zum QRadar Incident Forensics Processor hinzufügen. Weitere Informationen finden Sie im Abschnitt „Paketaufzeichnungseinheiten zu QRadar Incident Forensics-Hosts hinzufügen" auf Seite 31.

Verwalteten QRadar Incident Forensics-Host entfernen

Wenn Netzkonfigurationseinstellungen geändert werden sollen oder Probleme bei der Anzeige der Registerkarte **Forensics** auftreten, können Sie den verwalteten QRadar Incident Forensics-Host (IBM Security QRadar Incident Forensics Processor) aus der QRadar-Implementierung entfernen. Wenn der verwaltete QRadar Incident Forensics-Host für Forensics-Wiederherstellungen zuständig war, gehen die Daten beim erneuten Hinzufügen der QRadar Incident Forensics Processor-Instanz verloren.

Wenn Sie den verwalteten QRadar Incident Forensics-Host nicht entfernen, dieser jedoch aufgrund eines Stromausfalls oder aufgrund anderer Probleme vorübergehend nicht erreichbar ist, sind die für den verwalteten Host geplanten Jobs weiterhin vorhanden; sie werden verarbeitet, sobald der verwaltete Host wieder online ist.

Einschränkung: Es ist nicht möglich, verwaltete QRadar Incident Forensics-Hosts über den Implementierungseditor hinzuzufügen bzw. zu entfernen. Dies ist nur über das Tool 'System- und Lizenzverwaltung' möglich.

Vorgehensweise

1. Melden Sie sich als Administrator bei der QRadar-Konsole an:

   `https://`*`IP-Adresse_QRadar`*

   Der Standardbenutzername ist `admin`. Bei dem Kennwort handelt es sich um das Kennwort des Rootbenutzerkontos, das bei der Installation eingegeben wurde.
2. Klicken Sie auf die Registerkarte **Verwaltung**.
3. Klicken Sie im Teilfenster **Systemkonfiguration** auf **System- und Lizenzverwaltung**.
4. Klicken Sie in der Hosttabelle auf den QRadar Incident Forensics Processor-Host, der entfernt werden soll, und klicken Sie auf > **Implementierungsaktionen** > **Host entfernen**.
5. Klicken Sie in der Menüleiste der Registerkarte **Verwaltung** auf **Änderungen implementieren**.
6. Aktualisieren Sie den Web-Browser.

Kapitel 10. Verbindungen zwischen Paketaufzeichnungseinheiten und QRadar Incident Forensics

Damit Paketaufzeichnungsdaten abgerufen werden können, müssen Sie mindestens eine Paketaufzeichnungseinheit mit einem verwalteten IBM Security QRadar Incident Forensics-Host oder einer QRadar Incident Forensics Standalone-Komponente verbinden. Ist keine Paketaufzeichnungseinheit verbunden, können Sie die Paketaufzeichnungsdateien entweder manuell oder über FTP in die Benutzerschnittstelle hochladen.

Mastersystem für die Paketaufzeichnung

Abhängig von Ihren Netz- und Paketaufzeichnungsanforderungen können Sie bis zu fünf Paketaufzeichnungseinheiten mit einer QRadar Incident Forensics-Appliance verbinden. Bei der Übergabe einer Wiederherstellung wird für jede Paketaufzeichnungseinheit an jeder QRadar Incident Forensics-Appliance jeweils ein eigener Job übergeben. Wenn Sie beispielsweise zwei verwaltete QRadar Incident Forensics-Hosts haben, die mit je zwei Paketaufzeichnungseinheiten verbunden sind, werden vier Jobs übergeben.

Das folgende Diagramm veranschaulicht die Verbindung mehrerer Paketaufzeichnungseinheiten mit einem verwalteten QRadar Incident Forensics-Host (QRadar Incident Forensics Processor) oder mit QRadar Incident Forensics Standalone-Appliances.

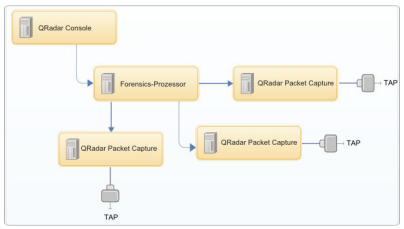


Abbildung 4. Beispiel mit mehreren Paketaufzeichnungseinheiten, die mit einem verwalteten QRadar Incident Forensics-Host verbunden sind

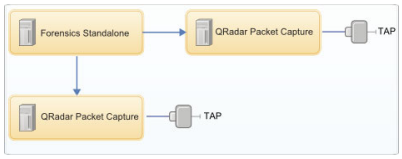
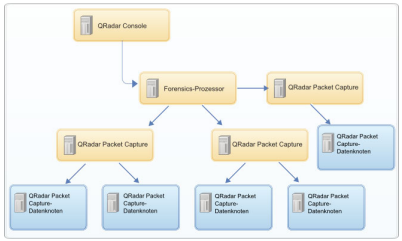


Abbildung 5. Beispiel mit mehreren Paketaufzeichnungseinheiten, die mit einem QRadar Incident Forensics Standalone-Host verbunden sind

QRadar Packet Capture-Datenknotenappliances

Um zusätzliche Speicherkapazität zu erhalten, können Sie jedes QRadar Packet Capture-Mastersystem mit bis zu zwei QRadar Packet Capture-Datenknotenappliances verbinden. Jede PCAP-Datenknotenappliance stellt 37 TB zusätzlichen Speicher bereit.



Nachdem Sie die QRadar Packet Capture-Datenknotenappliances mit dem Mastersystem verbunden haben, können Sie in der QRadar Packet Capture-Benutzerschnittstelle den Cluster konfigurieren.

Informationen zu den physischen Verbindungen zwischen dem Mastergerät und der QRadar Packet Capture-Datenknotenappliance finden Sie in der *QRadar Packet Capture-Kurzübersicht*, weitere Informationen zur Konfiguration des Paketaufzeichnungsclusters im *QRadar Packet Capture-Benutzerhandbuch*.

QRadar Packet Capture-Software auf der eigenen Appliance installieren

Um eine erfolgreiche Installation von IBM Security QRadar Packet Capture auf Ihrer eigenen Appliance sicherzustellen, müssen Sie das Betriebssystem Red Hat Enterprise Linux und die QRadar Packet Capture-Software installieren. Darüber hinaus muss Ihre Appliance die Systemvoraussetzungen erfüllen.

Wichtig: Das System, auf dem die QRadar Packet Capture-Software installiert wird, muss für QRadar Packet Capture vorgesehen sein. Es dürfen keine RPM-Pakete installiert werden, die von IBM nicht genehmigt wurden. Die Installation nicht genehmigter RPM-Pakete kann bei einem Upgrade zu Abhängigkeitsfehlern führen und Leistungsprobleme in Ihrer Implementierung verursachen. Das Betriebssystem darf nicht mithilfe von YUM aktualisiert werden; ebenso darf keine nicht genehmigte Software auf QRadar Packet Capture-Systemen installiert werden.

Einschränkung: Softwareinstallationen auf einer virtuellen Maschine werden nicht unterstützt.

Vorbereitende Schritte

Stellen Sie sicher, dass die Appliance die folgenden Systemvoraussetzungen erfüllt:

Tabelle 9. Systemvoraussetzungen für eine QRadar Packet Capture-Softwareinstallation

Spezifikation	Beschreibung
Prozessoren	Prozessoren der Intel E5-Serie V2 oder V3. Für V4-Versionen sind mindestens 6 Kerne erforderlich.
Prozessor-BIOS-Einstellungen	Muss die Intel-AES- und AVX-Standards unterstützen, die Intel 2011 eingeführt hat. Stellen Sie über die BIOS-Systemeinstellungen sicher, dass Hyper-Threading aktiviert ist.
Speicher	24 GB
Hardware-RAID-Controller und Speicher zum Aufzeichnen und Extrahieren	RAID-Konfiguration (bei einer Kombination von RAID 0, 1 oder 5) über mindestens vier Festplattenlaufwerke; jedes Festplattenlaufwerk mit einer Leistung von mindestens 7200 RPM und mindestens 1 TB pro Laufwerk
Betriebssystemlaufwerk	SATA- oder SAS-Festplattenlaufwerk der Unternehmensklasse mit mindestens 500 GB und 7200 RPM
Betriebssystem	Red Hat Enterprise Linux V6.7 **Anmerkung:** Das 1G-SFS-Installationsprogramm muss auf dem System installiert werden, auf dem 1G PCAP als dedizierte PCAP-Appliance installiert ist. Es darf für keine anderen Zwecke als die Paketaufzeichnung verwendet werden.
Mindestens erforderlicher Gesamtplattenspeicherplatz	4 TB

Tabelle 9. Systemvoraussetzungen für eine QRadar Packet Capture-Softwareinstallation (Forts.)

Spezifikation	Beschreibung
Erfassung NIC (Einzelerfassung 1G- oder 10G-Schnittstelle mit Unterstützung von 1Gbps+)	Von Intel hergestellte PCI Express-Netzkarten: • Intel E1G44ET2BLK Ethernet PCI Express Adapter http://ark.intel.com/products/49187/Intel-Gigabit-ET2-Quad-Port-Server-Adapter • Intel X520-SR2 Dual Ports 10 Gigabit Ethernet Converged Network Adapter, PCI Express 2.0 x8, Low Profile http://ark.intel.com/products/39774/Intel-Ethernet-Converged-Network-Adapter-X520-SR2 ODER Intel Ethernet-Controller (jede Steuerplatine bzw. jeder Netzadapter mit diesem Controller sollte funktionieren): • Intel 82576 Gigabit Ethernet-Controller http://ark.intel.com/products/series/32261/Intel-82576-Gigabit-Ethernet-Controller ODER Dell-basierte Computernetzkarten: • Intel X520 DP 10Gb DA/SFP+ Server Adapter (DELL SKU#540-BBCT) http://accessories.ap.dell.com/sna/productdetail.aspx?c=sg&l=en&s=dhs&cs=sgdhs1&sku=540-11353 • Intel Ethernet i350 QP 1Gb Network Daughter Card (DELL SKU#540-BBCB) http://accessories.dell.com/sna/productdetail.aspx?c=us&l=en&s=gen&sku=430-4437 • Intel Ethernet i350 QP 1Gb Network PCI express Card (DELL SKU#540-11357) http://accessories.ap.dell.com/sna/productdetail.aspx?c=au&l=en&s=bsd&cs=aubsd1&sku=540-11357
PCAP-UI-Netzschnittstelle	Jede 1G- oder (optional) 10G-Netzschnittstelle, z. B. eth0

Bevor Sie QRadar Packet Capture-Software auf Ihrer Appliance installieren, sollten Sie drei separate virtuelle Laufwerke einrichten und konfigurieren. Diese virtuellen Laufwerke sind für das Betriebssystem, für die Extraktion und für die Speicherung vorgesehen. Das Speicherlaufwerk sollte das größte der drei sein und muss mindestens 4000 GB groß sein.

Siehe folgendes Beispiel:

Tabelle 10. Beispiel einer RAID-Konfiguration für eine QRadar Packet Capture-Softwareinstallation

Virtuelles Laufwerk	RAID-Stufe	Größe
0	RAID 1	128 GB

Tabelle 10. Beispiel einer RAID-Konfiguration für eine QRadar Packet Capture-Softwareinstallation (Forts.)

1	RAID 1	3587 GB
2	RAID 5	33527 GB

Vorgehensweise

1. Legen Sie den Datenträger mit dem Betriebssystem Red Hat Enterprise Linux in Ihre Appliance ein und starten Sie die Appliance neu.
2. Folgen Sie den Anweisungen im Installationsassistenten, um die Installation durchzuführen:
   a. Wählen Sie die Option **Basisspeichermedien** aus.
   b. Bei der Konfiguration des Hostnamens kann der Wert für die Eigenschaft **Hostname** Buchstaben, Zahlen und Bindestriche einschließen.
   c. Wählen Sie auf der Registerkarte **IPv4-Einstellungen** in der Liste **Methode** den Eintrag **Manuell** aus.
   d. Wählen Sie auf der Seite **Installationstyp auswählen** die Option **Gesamten Bereich verwenden** und anschließend die kleinste Partition (Bootpartition) aus, auf der das Betriebssystem dann installiert werden soll.
   e. Wählen Sie für die Installation nur die Option **Basissystem** aus.
3. Klicken Sie nach Abschluss der Installation auf **Neu starten**.
4. Kopieren Sie die SFS-Datei für QRadar Packet Capture auf Ihre Appliance.
5. Hängen Sie die SFS-Datei für QRadar Packet Capture an:
   a. Erstellen Sie das Verzeichnis `/tmp/qpc_install`, indem Sie den folgenden Befehl eingeben:
      ```
      mkdir -p /tmp/qpc_install
      ```
   b. Hängen Sie die SFS-Datei für QRadar Packet Capture an:
      ```
      mount -o loop -t squashfs <QRadar_Packet_Capture-Datei.sfs>
      /tmp/qpc_install
      ```
   c. Wechseln Sie in das Verzeichnis `/tmp/qpc_install`.
      ```
      cd /tmp/qpc_install
      ```
6. Führen Sie das Installationsscript aus, indem Sie den folgenden Befehl eingeben:
   ```
   sh installer.sh
   ```

Paketaufzeichnungseinheiten zu QRadar Incident Forensics-Hosts hinzufügen

Damit Prüfer Zugriff auf Paketaufzeichnungsdaten haben, können Sie bis zu fünf Paketaufzeichnungseinheiten mit einem verwalteten IBM Security QRadar Incident Forensics-Host oder einem IBM Security QRadar Incident Forensics Standalone-Host verbinden. Die verbundenen Paketaufzeichnungseinheiten verarbeiten die Aufzeichnungsdateien für Forensics-Wiederherstellungen.

Ist keine Paketaufzeichnungseinheit verbunden, können Sie die Paketaufzeichnungsdateien entweder manuell oder über FTP in die Benutzerschnittstelle hochladen.

Einschränkung: Es ist nicht möglich, Paketaufzeichnungseinheiten über den Implementierungseditor hinzuzufügen. Dies ist nur über das Tool 'System- und Lizenzverwaltung' möglich.

Vorbereitende Schritte

Sie müssen einen verwalteten QRadar Incident Forensics-Host installieren und implementieren oder einen QRadar Incident Forensics Standalone-Host installieren. Weitere Informationen finden Sie in Kapitel 8, „QRadar Incident Forensics installieren", auf Seite 23 und Kapitel 9, „Verwalteten QRadar Incident Forensics-Host zu QRadar-Konsole hinzufügen", auf Seite 25.

Das folgende interaktive Diagramm zeigt die wichtigsten Installationsschritte bei verteilten Installationen. Für eigenständige Implementierungen gilt derselbe Installationsprozess, allerdings wird kein verwalteter Host implementiert.

Die Zeitzone für QRadar Packet Capture wird standardmäßig auf UTC (Coordinated Universal Time; koordinierte Weltzeit) gesetzt.

Vorgehensweise

1. Melden Sie sich als Administrator bei der QRadar-Konsole an:

   `https://`*`IP-Adresse_QRadar`*

   Der Standardbenutzername ist `admin`. Bei dem Kennwort handelt es sich um das Kennwort des Rootbenutzerkontos, das bei der Installation eingegeben wurde.
2. Klicken Sie auf die Registerkarte **Verwaltung**.
3. Klicken Sie im Teilfenster **Systemkonfiguration** auf **System- und Lizenzverwaltung**.
4. Wählen Sie in der Hosttabelle den QRadar Incident Forensics Processor (**Gerätetyp** 6000) oder den QRadar Incident Forensics Standalone-Host (**Gerätetyp** 6100) aus und klicken Sie auf **Implementierungsaktionen** > **Host bearbeiten**.
5. Klicken Sie auf **Komponentenmanagement**.
6. Um Paketaufzeichnungseinheiten hinzuzufügen, klicken Sie auf das Symbol zum Hinzufügen (+) und geben Sie die Informationen zu der betreffenden Einheit ein.

   Tipp: Der Standardbenutzername für die QRadar Packet Capture-Einheit ist `continuum`.
7. Klicken Sie auf **Speichern**.

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 La Défense
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 Director of Licensing
IBM Corporation

North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

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.

Die hierin genannten Beispiele zu Leistungsdaten und Kunden dienen nur zur Veranschaulichung. Tatsächliche Leistungsergebnisse können abhängig von bestimmten Konfigurationen und Betriebsbedingungen davon abweichen.

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 unter Umständen 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 Personen oder Unternehmen 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. Weitere Produkt- oder Servicenamen können Marken von IBM oder anderen Unternehmen sein. Eine aktuelle Liste der IBM Marken finden Sie auf der Webseite "Copyright and trademark information" unter www.ibm.com/legal/copytrade.shtml.

Adobe, das Adobe-Logo, PostScript und das PostScript-Logo sind entweder eingetragene Marken oder Marken von Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Linux ist eine eingetragene Marke von Linus Torvalds in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken von Oracle und/oder dessen verbundenen Unternehmen.

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

Bedingungen für die Produktdokumentation

Die Berechtigungen zur Nutzung dieser Veröffentlichungen werden Ihnen auf der Basis der folgenden Bedingungen gewährt.

Anwendbarkeit

Diese Bedingungen sind eine Ergänzung der Nutzungsbedingungen auf der IBM Website.

Persönliche Nutzung

Sie dürfen diese Veröffentlichungen für Ihre persönliche, nicht kommerzielle Nutzung unter der Voraussetzung vervielfältigen, dass alle Eigentumsvermerke erhalten bleiben. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM nicht weitergeben, anzeigen oder abgeleitete Werke davon erstellen.

Kommerzielle Nutzung

Sie dürfen diese Veröffentlichungen nur innerhalb Ihres Unternehmens und unter der Voraussetzung, dass alle Eigentumsvermerke erhalten bleiben, vervielfältigen, weitergeben und anzeigen. Sie dürfen diese Veröffentlichungen oder Teile der Veröffentlichungen ohne ausdrückliche Genehmigung von IBM außerhalb Ihres Unternehmens nicht vervielfältigen, weitergeben, anzeigen oder abgeleitete Werke davon erstellen.

Rechte

Abgesehen von den hier gewährten Berechtigungen erhalten Sie keine weiteren Berechtigungen, Lizenzen oder Rechte (veröffentlicht oder stillschweigend) in Bezug auf die Veröffentlichungen oder darin enthaltene Informationen, Daten, Software oder geistiges Eigentum.

IBM behält sich das Recht vor, die in diesem Dokument gewährten Berechtigungen nach eigenem Ermessen zurückzuziehen, wenn sich die Nutzung der Veröffentlichungen für IBM als nachteilig erweist oder wenn die obigen Nutzungsbestimmungen nicht genau befolgt werden.

Sie dürfen diese Informationen nur in Übereinstimmung mit allen anwendbaren Gesetzen und Vorschriften, einschließlich aller US-amerikanischen Exportgesetze und Verordnungen, herunterladen und exportieren.

IBM übernimmt keine Gewährleistung für den Inhalt dieser Veröffentlichungen. Diese Veröffentlichungen werden auf der Grundlage des gegenwärtigen Zustands (auf "as-is"-Basis) und ohne eine ausdrückliche oder stillschweigende Gewährleistung für die Handelsüblichkeit, die Verwendungsfähigkeit für einen bestimmten Zweck oder die Freiheit von Rechten Dritter zur Verfügung gestellt.

IBM Online-Datenschutzerklärung

IBM Softwareprodukte, einschließlich Software as a Service-Lösungen ("Softwareangebote"), können Cookies oder andere Technologien verwenden, um Informationen zur Produktnutzung zu erfassen, die Endbenutzererfahrung zu verbessern und Interaktionen mit dem Endbenutzer anzupassen oder zu anderen Zwecken. 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, damit wird aber zugleich die dadurch ermöglichte Funktionalität inaktiviert.

Wenn es die für dieses Softwareangebot bereitgestellten Konfigurationen Ihnen als Kunde ermöglichen, 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 den Schwerpunkten der IBM Datenschutzerklärung unter http://www.ibm.com/privacy, in der IBM Online-Datenschutzerklärung unter http://www.ibm.com/privacy/details im Abschnitt "Cookies, Web-Beacons und sonstige Technologien" und unter "IBM Software Products and Software-as-a-Service Privacy Statement" (http://www.ibm.com/software/info/product-privacy).

Gedruckt in Deutschland