IBM Security QRadar Risk Manager
Version 7.2.2

Installationshandbuch

GC12-5039-00

IBM Security QRadar Risk Manager
Version 7.2.2

Installationshandbuch

GC12-5039-00

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 23 gelesen werden.

Diese Veröffentlichung ist eine Übersetzung des Handbuchs
IBM Security QRadar Risk Manager, Version 7.2.2, Installation Guide,
IBM Form GC27-6239-00,
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 Installation von IBM Security QRadar Risk Manager

Diese Informationen gelten für IBM® Security QRadar Risk Manager. QRadar Risk Manager ist eine Appliance, mit der Einheitenkonfigurationen (Gerätekonfigurationen) überwacht, Änderungen an Ihrer Netzumgebung simuliert sowie Risiken und Schwachstellen in Ihrem Netz priorisiert werden können.

Dieses Handbuch enthält Anweisungen für die Installation von QRadar Risk Manager und das Hinzufügen von QRadar Risk Manager als verwalteten Host auf einer IBM Security QRadar SIEM-Konsole.

Auf den QRadar Risk Manager-Appliances ist bereits Software und das Betriebssystem Red Hat Enterprise Linux installiert. Sie können die QRadar Risk Manager-Software auch auf Ihrer eigenen Hardware installieren.

Zielgruppe

Dieses Handbuch richtet sich an Netzadministratoren, die für die Installation und Konfiguration der QRadar Risk Manager-Systeme in Ihrem Netz verantwortlich sind.

Administratoren benötigen praktische Erfahrung mit dem Netzbetrieb und Linux-Systemen.

Technische Dokumentation

Informationen zum Zugriff auf weitere technische Dokumentation, technische Hinweise und Releaseinformationen finden Sie im Dokument Accessing IBM Security Documentation Technical Note (Technische Hinweise zum Zugriff auf die IBM Security-Dokumentation) (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Kundenunterstützung kontaktieren

Informationen zur Kontaktierung der Kundenunterstützung finden Sie im Dokument Support and Download Technical Note (Technische Hinweise zum Support und Download) (http://www.ibm.com/support/docview.wss?rs=0&uid=swg21612861).

Hinweis zu sinnvollen Sicherheitsverfahren

Die IT-Systemsicherheit beinhaltet den Schutz von Systemen und Informationen mittels Vorbeugung und Erkennung von falschem Zugriff sowie Intervention bei falschem Zugriff durch Personen innerhalb oder außerhalb Ihres Unternehmens. Durch falschen Zugriff können Informationen geändert, zerstört und falsch oder unsachgemäß verwendet werden. Auch können Ihre Systeme dadurch beschädigt oder missbraucht werden, um z. B. andere zu attackieren. Kein IT-System oder Produkt sollte als vollkommen sicher betrachtet werden. Kein einzelnes Produkt, kein einzelner Service und keine einzelne Sicherheitsmaßnahme können eine falsche Verwendung oder einen unbefugten Zugriff hundertprozentig verhindern.

IBM Systeme, Produkte und Services stellen einen Teil eines umfassenden Sicherheitsansatzes dar, der notwendigerweise mit weiteren betrieblichen Verfahren einhergeht und für den möglicherweise andere Systeme, Produkte oder Services erforderlich sind, um eine größtmögliche Effizienz zu gewährleisten. 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. Installation von IBM Security QRadar Risk Manager vorbereiten

Sie können eine IBM Security QRadar Risk Manager-Appliance als verwalteten Host auf Ihrer IBM Security QRadar SIEM-Konsole installieren. Auf einer QRadar SIEM-Konsole kann immer nur jeweils ein QRadar Risk Manager vorhanden sein.

Ab Version 7.1 von QRadar Risk Manager verwenden QRadar SIEM und QRadar Risk Manager denselben Installationsprozess und dieselbe ISO-Version für die Installation. Daher können Sie QRadar Risk Manager mit dem Implementierungseditor in QRadar SIEM zu Ihrer Implementierung hinzufügen. Die Installation einer QRadar Risk Manager-Appliance umfasst die QRadar Risk Manager-Software und ein Red Hat Enterprise Linux-Betriebssystem.

Installationsvorbereitung

Vor der Installation von IBM Security QRadar Risk Manager müssen Sie den Installationsprozess für eine IBM Security QRadar SIEM-Konsole vollständig ausgeführt haben. Ein bewährtes Verfahren ist die Installation von QRadar SIEM und QRadar Risk Manager auf demselben Netzswitch.

Sie finden Informationen zur Installation von QRadar SIEM im *IBM Security QRadar SIEM Installationshandbuch*. Dort werden auch die Hardware- und Softwarevoraussetzungen aufgelistet.

Da es sich bei IBM Security QRadar Risk Manager um eine 64-Bit-Appliance handelt, müssen Sie darauf achten, dass Sie die richtige Installationssoftware für Ihr Betriebssystem herunterladen.

Netzeinstellungen ermitteln

Vor Beginn des Installationsprozesses müssen Sie Informationen zu Ihren Netzeinstellungen zusammenstellen.

Stellen Sie die folgenden Informationen zu Ihren Netzeinstellungen zusammen:

- Hostname
- IP-Adresse
- Netzmaskenadresse
- Teilnetzmaske
- Adresse des Standardgateways
- Serveradresse des primären Domänennamenssystems (DNS)
- Adresse des sekundären DNS-Servers (optional)
- Öffentliche IP-Adresse für Netze, die für den Namen des E-Mail-Servers eine Netzadressumsetzung (Network Address Translation, NAT) verwenden
- Name des E-Mail-Servers
- Name des NTP-Servers (NTP = Network Time Protocol) (nur bei der Konsole) oder Zeitservers

Portzugriff in Firewalls konfigurieren

Die Firewalls zwischen der IBM Security QRadar SIEM-Konsole und IBM Security QRadar Risk Manager müssen den Datenverkehr an bestimmten Ports ermöglichen.

Stellen Sie sicher, dass alle Firewalls, die sich zwischen der QRadar SIEM-Konsole und QRadar Risk Manager befinden, den Datenverkehr an folgenden Ports ermöglichen:
- Port 443 (HTTPS)
- Port 22 (SSH)
- Port 37 UDP (Zeit)

Nicht unterstützte Funktionen in QRadar Risk Manager

Es ist wichtig, dass Sie die Funktionen kennen, die nicht von IBM Security QRadar Risk Manager unterstützt werden.

Die folgenden Funktionen werden in QRadar Risk Manager nicht unterstützt:
- Hochverfügbarkeit (High Availability, HA)
- Dynamisches Routing für Border Gateway Protocol (BGP), Open Shortest Path First (OSPF) oder Routing Information Protocol (RIP)
- IPv6
- Nicht zusammenhängende Netzmasken
- Weiterleitungen zum Lastausgleich
- Referenzzuordnungen
- Store-and-forward-Verfahren

Zusätzliche Hardwarevoraussetzungen

Damit Sie IBM Security QRadar Risk Manager installieren können, ist zusätzliche Hardware erforderlich.

Vor der Installation von IBM QRadar Risk Manager-Systemen müssen Sie sicherstellen, dass Ihnen die folgenden Hardwarekomponenten zur Verfügung stehen:
- Bildschirm und Tastatur oder eine serielle Konsole
- Unterbrechungsfreie Stromversorgung (USV)

QRadar Risk Manager-Appliances oder -Systeme, auf denen QRadar Risk Manager-Software zur Speicherung von Daten ausgeführt wird, müssen mit einer unterbrechungsfreien Stromversorgung (USV) ausgestattet sein. Die Verwendung einer unterbrechungsfreien Stromversorgung stellt sicher, dass Ihre QRadar Risk Manager-Daten (zum Beispiel Konsolen, Ereignisprozessoren und QFlow-Kollektoren) bei einem Stromausfall nicht verloren gehen.

Zusätzliche Softwarevoraussetzungen

Damit Sie IBM Security QRadar Risk Manager installieren können, ist zusätzliche Software erforderlich.

Die folgende Software muss auf dem Desktopsystem installiert sein, das Sie für den Zugriff auf die Benutzerschnittstelle von QRadar Risk Manager verwenden:
- Java™ Runtime Environment
- Adobe Flash, Version 10 oder höher

Unterstützte Web-Browser

Damit die Funktionen in IBM Security QRadar-Produkten ordnungsgemäß ausgeführt werden können, müssen Sie einen unterstützen Web-Browser verwenden.

Wenn Sie auf das QRadar-System zugreifen, werden Sie aufgefordert, einen Benutzernamen und ein Kennwort einzugeben. Der Benutzername und das Kennwort müssen vorab vom Administrator konfiguriert werden.

In der folgenden Tabelle werden die unterstützten Web-Browser-Versionen aufgelistet.

Tabelle 1. Unterstützte Web-Browser für QRadar-Produkte

Web-Browser	Unterstützte Version
Mozilla Firefox	17.0 Extended Support Release 24.0 Extended Support Release
32-Bit-Version von Microsoft Internet Explorer mit aktiviertem Dokument- und Browsermodus	9.0
Google Chrome	Die am Freigabedatum der Produkte aus IBM Security QRadar V7.2.2 aktuelle Version

Dokument- und Browsermodus in Internet Explorer aktivieren

Wenn Sie Microsoft Internet Explorer für den Zugriff auf die IBM Security QRadar-Produkte verwenden, müssen Sie den Browsermodus und den Dokumentmodus aktivieren.

Vorgehensweise

1. Drücken Sie in Ihrem Internet Explorer-Web-Browser 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 für Internet Explorer V9.0 den Eintrag **Internet Explorer 9** aus.
   - Wählen Sie für Internet Explorer V8.0 den Eintrag **Internet Explorer 7.0-Standards** aus.

Kapitel 2. IBM Security QRadar Risk Manager-Appliances installieren

Eine IBM Security QRadar Risk Manager-Implementierung beinhaltet eine IBM Security QRadar SIEM-Konsole und eine QRadar Risk Manager-Appliance, die als verwalteter Host genutzt wird.

Die Installation von QRadar Risk Manager umfasst die folgenden Schritte:

1. Ihre Appliance vorbereiten
2. QRadar Risk Manager installieren
3. QRadar Risk Manager zu QRadar SIEM hinzufügen

Ihre Appliance vorbereiten

Sie müssen Ihre Appliance entsprechend vorbereiten, bevor Sie eine IBM Security QRadar Risk Manager-Appliance installieren.

Vorbereitende Schritte

Sie müssen die gesamte erforderliche Hardware installieren. Außerdem benötigen Sie einen Aktivierungsschlüssel. Der Aktivierungsschlüssel ist eine alphanumerische Zeichenfolge mit 24 Stellen und vier Teilen, die Sie von IBM erhalten. Sie finden den Aktivierungsschlüssel an folgenden Stellen:

- Als Ausdruck auf einem Aufkleber, der an Ihrer Appliance angebracht ist.
- Auf dem Packzettel; alle Appliances werden gemeinsam mit ihren zugehörigen Schlüsseln aufgelistet.

Zur Vermeidung von Eingabefehlern werden der Buchstabe I und die Zahl 1 (Eins) sowie der Buchstabe O und die Zahl 0 (Null) gleichwertig behandelt.

Wenn Sie keinen Aktivierungsschlüssel für Ihre QRadar Risk Manager-Appliance erhalten haben, wenden Sie sich an die Kundenunterstützung (http://www.ibm.com/support).

Sie finden Informationen zu Ihrer Appliance im Handbuch *IBM Security QRadar Hardware Installation Guide*.

Vorgehensweise

1. Wählen Sie eine der folgenden Optionen aus:
   - Schließen Sie ein Notebook an den seriellen Anschluss auf der Rückseite der Appliance an.

     Wenn Sie für die Herstellung einer Verbindung zum System ein Notebook nutzen, müssen Sie ein Terminalprogramm (zum Beispiel HyperTerminal) für die Verbindung mit dem System verwenden. Achten Sie darauf, dass Sie unter **Connect Using** (Verbindung mit) den richtigen COM-Anschluss des seriellen Anschlusses festlegen. Außerdem müssen Sie den Wert von **Bits per second** (Bits pro Sekunde) auf 9600 setzen. Darüber hinaus müssen Sie Werte für **Stop Bits** (Stoppbits), **Data bits** (Datenbits) und **Parity** (Parität) festlegen, und zwar jeweils 1 für Stoppbits, 8 für Datenbits und 'None' (Keine) für die Parität.

- Schließen Sie eine Tastatur und einen Bildschirm an die entsprechenden Anschlüsse an.

2. Schalten Sie das System ein und melden Sie sich an. Der Benutzername, bei dem die Groß-/Kleinschreibung beachtet werden muss, lautet 'root'.
3. Drücken Sie die Eingabetaste.
4. Lesen Sie die Informationen in dem Fenster. Mit der Leertaste können Sie jeweils um ein Fenster vorspringen, bis Sie zum Ende des Dokuments gelangen.
5. Geben Sie yes (Ja) ein, um die Vereinbarung zu akzeptieren, und drücken Sie dann die Eingabetaste.
6. Geben Sie Ihren Aktivierungsschlüssel ein und drücken Sie die Eingabetaste.

Auf die Benutzerschnittstelle von IBM Security QRadar Risk Manager zugreifen

IBM Security QRadar Risk Manager verwendet für die URL, den Benutzernamen und das Kennwort Standardanmeldeinformationen.

Sie greifen über die QRadar SIEM-Konsole auf IBM Security QRadar Risk Manager zu. Verwenden Sie die Informationen in der folgenden Tabelle, wenn Sie sich bei Ihrer IBM Security QRadar SIEM-Konsole anmelden.

Tabelle 2. Standardanmeldeinformationen für QRadar Risk Manager

Anmelde-informationen	**Standardwert**
URL	https://<IP-Adresse>. Dabei steht <IP-Adresse> für die IP-Adresse der QRadar SIEM-Konsole.
Benutzername	admin
Kennwort	Das Kennwort, das für QRadar Risk Manager während des Installationsprozesses zugewiesen wurde.
Lizenzschlüssel	Ein Standardlizenzschlüssel ermöglicht für fünf Wochen den Zugriff auf das System.

Informationen zu den Netzparametern für Internet Protocol Version 4 (IPv4)

Bei der Installation von IBM Security QRadar Risk Manager oder der Änderung Ihrer Netzeinstellungen werden Netzinformationen für die Netzeinstellungen von Internet Protocol Version 4 (IPv4) benötigt.

Netzinformationen sind erforderlich, wenn Sie IBM Security QRadar Risk Manager installieren oder erneut installieren. Sie werden außerdem auch benötigt, wenn Sie Netzeinstellungen ändern müssen.

Die Einstellung für das öffentliche IP-Netz ist optional. Mit dieser sekundären IP-Adresse wird auf den Server zugegriffen. Der Zugriff erfolgt in der Regel von einem anderen Netz oder dem Internet aus und wird von Ihrem Netzadministrator gesteuert. Die öffentliche IP-Adresse wird häufig unter Verwendung der NAT-Services (NAT = Network Address Translation, Netzadressumsetzung) in Ihrem Netz oder über die Firewalleinstellungen in Ihrem Netz konfiguriert. Die Netzadressumsetzung setzt eine IP-Adresse in einem Netz in eine andere IP-Adresse in einem anderen Netz um.

IBM Security QRadar Risk Manager installieren

Nachdem Sie Ihre Appliance entsprechend vorbereitet haben, können Sie IBM Security QRadar Risk Manager installieren.

Vorbereitende Schritte

Sie müssen die Vorbereitungsschritte vollständig ausgeführt haben, bevor Sie QRadar Risk Manager installieren.

Vorgehensweise

1. Wählen Sie den Standardtyp für die Installation aus. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
2. Wählen Sie den Kontinent oder das Land Ihrer Zeitzone aus. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
3. Wählen Sie die Region Ihrer Zeitzone aus. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
4. Wählen Sie eine Internet Protocol-Version aus. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
5. Wählen Sie die Schnittstelle aus, die Sie als Verwaltungsschnittstelle angeben möchten. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
6. Geben Sie Ihren Hostnamen, Ihre IP-Adresse, Ihre Netzmaske, Ihr Gateway, Ihr primäres und sekundäres Domänennamenssystem (Domain Name System, DNS) sowie Ihr öffentliches IP und Ihren E-Mail-Server ein. Sie finden Informationen zu den Netzparametern im Abschnitt „Informationen zu den Netzparametern für Internet Protocol Version 4 (IPv4)" auf Seite 6.
7. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
8. Geben Sie ein Kennwort ein, um das Rootkennwort für QRadar Risk Manager zu konfigurieren.
9. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
10. Geben Sie Ihr neues Kennwort zur Bestätigung erneut ein. Wählen Sie **Beenden** aus und drücken Sie die Eingabetaste. Dieser Prozess dauert in der Regel einige Minuten.

Nächste Schritte

Verwenden Sie den Implementierungseditor zum Hinzufügen von QRadar Risk Manager als verwalteten Host zu Ihrer QRadar SIEM-Konsole.

QRadar Risk Manager zu QRadar SIEM hinzufügen

Sie müssen IBM Security QRadar Risk Manager als verwalteten Host zu IBM Security QRadar SIEM hinzufügen.

Vorbereitende Schritte

Wenn Sie die Komprimierung aktivieren möchten, muss für jeden verwalteten Host mindestens die Version QRadar SIEM 7.1 oder QRadar Risk Manager 7.1 verwendet werden.

Wenn Sie Ihrer Implementierung einen verwalteten Host hinzufügen möchten, auf dem die Netzadressumsetzung nicht aktiviert ist, und die Netzadressumsetzung aber auf der Konsole aktiviert ist, müssen Sie die QRadar SIEM-Konsole in einen

Host mit aktivierter Netzadressumsetzung ändern. Sie müssen die Konsole ändern, bevor Sie Ihrer Implementierung den verwalteten Host hinzufügen. Sie finden weitere Informationen hierzu im *IBM QRadar SIEM - Administrationshandbuch*.

Vorgehensweise

1. Öffnen Sie Ihren Web-Browser.
2. Geben Sie die URL `https://<IP-Adresse>` ein. Dabei steht <IP-Adresse> für die IP-Adresse der QRadar SIEM-Konsole.
3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.
4. Klicken Sie auf der Registerkarte **Verwaltung (Admin)** auf **Implementierungseditor**.
5. Wählen Sie im Menü zunächst **Aktionen** und anschließend **Add a Managed Host** (Verwalteten Host hinzufügen) aus.
6. Klicken Sie auf **Weiter**.
7. Geben Sie Werte für die folgenden Parameter ein:

Option	Bezeichnung
Enter the IP of the server or appliance to add (IP des Servers oder der Appliance eingeben, der bzw. die hinzugefügt werden soll)	Die IP-Adresse von QRadar Risk Manager.
Enter the root password of the host (Rootkennwort des Hosts eingeben)	Das Rootkennwort für den Host.
Confirm the root password of the host (Rootkennwort des Hosts bestätigen)	Bestätigung Ihres Kennworts.
Host is NATed (Netzadressumsetzung auf Host aktiviert)	Wenn Sie die Netzadressumsetzung (Network Address Translation, NAT) für einen verwalteten Host aktivieren möchten, muss das Netz mit aktivierter Netzadressumsetzung die statische Netzadressumsetzung verwenden. Sie finden weitere Informationen hierzu im *IBM QRadar SIEM - Administrationshandbuch*.
Enable Encryption (Verschlüsselung aktivieren)	Erstellt einen SSH-Verschlüsselungstunnel für den Host. Damit die Verschlüsselung zwischen zwei verwalteten Hosts aktiviert werden kann, muss auf jedem verwalteten Host QRadar SIEM 7.1 oder QRadar Risk Manager 7.1 ausgeführt werden.
Enable Compression (Komprimierung aktivieren)	Aktiviert die Datenkomprimierung zwischen zwei verwalteten Hosts.

8. Wählen Sie eine der folgenden Optionen aus:
   - Wenn Sie das Kontrollkästchen **Host is NATed** (Netzadressumsetzung auf Host aktiviert) ausgewählt haben, müssen Sie Werte für die Parameter der Netzadressumsetzung eingeben.

Option	Bezeichnung
Enter public IP of the server or appliance to add (Öffentliches IP des Servers oder Geräts eingeben, das hinzugefügt werden soll)	Die öffentliche IP-Adresse des verwalteten Hosts. Der verwaltete Host verwendet diese IP-Adresse für die Kommunikation mit anderen verwalteten Hosts in anderen Netzen, die die Netzadressumsetzung verwenden.

Option	Bezeichnung
Select NATed network (Netz mit aktivierter Netzadressumsetzung auswählen)	Das Netz, das von diesem verwalteten Host verwendet werden soll. Wenn sich der verwaltete Host in demselben Teilnetz befindet wie die QRadar SIEM-Konsole, wählen Sie die Konsole des Netzes mit aktivierter Netzadressumsetzung aus. Wenn sich der verwaltete Host nicht in demselben Teilnetz befindet wie die QRadar SIEM-Konsole, wählen Sie den verwalteten Host des Netzes mit aktivierter Netzadressumsetzung aus.

- Wenn Sie das Kontrollkästchen **Host is NATed** (Netzadressumsetzung auf Host aktiviert) nicht ausgewählt haben, klicken Sie auf **Weiter**.

9. Klicken Sie auf **Beenden**. Die Ausführung dieses Prozesses kann einige Minuten dauern. Falls Ihre Implementierung Änderungen enthält, müssen Sie alle Änderungen implementieren.
10. Klicken Sie auf **Implementieren**.

Nächste Schritte

Löschen Sie den Inhalt Ihres Web-Browser-Cache und melden Sie sich anschließend bei QRadar SIEM an. Die Registerkarte **Risks** (Risiken) ist jetzt verfügbar.

Inhalt des Web-Browser-Cache löschen

Sie müssen den Inhalt des Web-Browser-Cache löschen, damit Sie auf die Registerkarte **Risks** (Risiken) in QRadar SIEM zugreifen können.

Vorbereitende Schritte

Stellen Sie sicher, dass nur ein Web-Browser geöffnet ist. Falls mehrere Browser geöffnet sind, kann der Inhalt des Cache möglicherweise nicht ordnungsgemäß gelöscht werden.

Wenn Sie den Web-Browser Mozilla Firefox verwenden, müssen Sie den Cache auch in Ihrem Web-Browser Microsoft Internet Explorer löschen.

Vorgehensweise

1. Öffnen Sie Ihren Web-Browser.
2. Löschen Sie den Inhalt Ihres Web-Browser-Cache. In der Dokumentation Ihres Web-Browsers finden Sie entsprechende Anweisungen.

Risk Manager-Benutzerrolle

Sie müssen Benutzern, die Zugriff auf die Registerkarte **Risks** (Risiken) benötigen, die Risk Manager-Benutzerrolle zuweisen.

Ein Benutzerkonto definiert das Standardkennwort und die E-Mail-Adresse für einen Benutzer. Sie müssen jedem neuen Benutzerkonto eine Benutzerrolle und ein Sicherheitsprofil zuweisen.

Bevor Sie anderen Benutzern in Ihrem Unternehmen den Zugriff auf die Funktionen von IBM Security QRadar Risk Manager ermöglichen können, müssen Sie die entsprechenden Benutzerrollenberechtigungen zuweisen. QRadar SIEM stellt standardmäßig eine Standardbenutzerrolle für Verwaltungsaufgaben zur Verfügung, die den Zugriff auf alle Bereiche von QRadar Risk Manager ermöglicht.

Sie finden Informationen zur Erstellung und Verwaltung von Benutzerrollen im *IBM Security QRadar SIEM - Administrationshandbuch*.

Risk Manager-Benutzerrolle zuweisen

Sie können Benutzern, die Zugriff auf die Registerkarte **Risk** (Risiken) benötigen, die Risk Manager-Benutzerrolle zuweisen.

Vorgehensweise

1. Klicken Sie auf die Registerkarte **Verwaltung (Admin)**.
2. Klicken Sie im Navigationsmenü auf **Systemkonfiguration**.
3. Klicken Sie im Teilfenster **Benutzerverwaltung** auf das Symbol **Benutzerrollen**.
4. Klicken Sie neben der Benutzerrolle, die Sie bearbeiten möchten, auf das Symbol **Bearbeiten**.
5. Wählen Sie das Kontrollkästchen **Risk Manager** aus.
6. Klicken Sie auf **Weiter**. Wenn Sie Risk Manager einer Benutzerrolle hinzufügen, die über die Berechtigung 'Protokollaktivität' verfügt, müssen Sie die Protokollquellen definieren, auf die die Benutzerrolle zugreifen kann. Sie können eine gesamte Protokollquellengruppe hinzufügen, indem Sie im Teilfenster **Protokollquellengruppe** auf **Hinzufügen** klicken. Sie können mehrere Protokollquellen auswählen, indem Sie beim Auswählen der einzelnen Protokollquellen, die Sie hinzufügen möchten, die Steuertaste gedrückt halten.
7. Klicken Sie auf **Zurück**.
8. Klicken Sie im Menü **Verwaltung** auf **Änderungen implementieren**.

Fehler bei der Registerkarte 'Risks' (Risiken) beheben

Sie können eine Fehlerbehebung durchführen, wenn die Registerkarte **Risks** (Risiken) nicht ordnungsgemäß angezeigt wird oder nicht zugänglich ist.

Wenn die Registerkarte 'Risks' (Risiken) nicht ordnungsgemäß angezeigt wird oder nicht zugänglich ist, müssen Sie IBM Security QRadar Risk Manager entfernen und als verwalteten Host erneut hinzufügen.

Verwalteten Host entfernen

Sie können Ihren verwalteten IBM Security QRadar Risk Manager-Host zur Änderung von Netzeinstellungen oder bei einem Problem mit der Registerkarte **Risks** (Risiken) aus IBM Security QRadar SIEM entfernen.

Vorgehensweise

1. Öffnen Sie Ihren Web-Browser.
2. Geben Sie die URL `https://<IP-Adresse>` ein. Dabei steht <IP-Adresse> für die IP-Adresse der QRadar SIEM-Konsole.
3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.

   Sie finden die Standardanmeldeinformationen im Abschnitt Tabelle 2 auf Seite 6.

4. Klicken Sie auf der Registerkarte **Verwaltung (Admin)** auf **Implementierungseditor**.
5. Klicken Sie auf die Registerkarte **Systemansicht**.
6. Klicken Sie mit der rechten Maustaste auf den verwalteten Host, den Sie löschen möchten, und wählen Sie **Löschen** aus. Wiederholen Sie diesen Vorgang für jeden verwalteten Host ohne Konsole, bis alle Hosts gelöscht sind.
7. Klicken Sie auf **Speichern**.
8. Schließen Sie den Implementierungseditor.
9. Klicken Sie auf der Registerkarte **Verwaltung (Admin)** auf **Änderungen implementieren**.

QRadar Risk Manager erneut als verwalteten Host hinzufügen

Sie können QRadar Risk Manager erneut als verwalteten Host hinzufügen, wenn er zuvor entfernt wurde.

Vorgehensweise

1. Öffnen Sie Ihren Web-Browser.
2. Geben Sie die URL `https://<IP-Adresse>` ein. Dabei steht <IP-Adresse> für die IP-Adresse der QRadar SIEM-Konsole.
3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.

   Sie finden die Standardanmeldeinformationen im Abschnitt Tabelle 2 auf Seite 6.
4. Klicken Sie auf der Registerkarte **Verwaltung (Admin)** auf **Implementierungseditor**.
5. Klicken Sie auf die Registerkarte **Systemansicht**.
6. Wählen Sie im Menü nacheinander **Aktionen** > **Add a managed host** (Verwalteten Host hinzufügen) aus.
7. Klicken Sie auf **Weiter**.
8. Geben Sie im Fenster **Add new managed host** (Neuen verwalteten Host hinzufügen) die entsprechenden Werte ein.
9. Klicken Sie auf **Weiter**.
10. Klicken Sie auf **Beenden**. Es kann einige Minuten dauern, bis der QRadar Risk Manager hinzugefügt wurde.
11. Schließen Sie den Implementierungseditor.
12. Klicken Sie auf der Registerkarte **Verwaltung** auf **Änderungen implementieren**.

Kapitel 3. IBM Security QRadar Risk Manager mithilfe der Wiederherstellungspartition erneut installieren

Wenn Sie IBM Security QRadar Risk Manager auf Basis der IBM Security QRadar SIEM-ISO in der Wiederherstellungspartition erneut installieren, wird Ihr System auf die werkseitig voreingestellte Konfiguration zurückgesetzt. Dies bedeutet, dass Ihre aktuellen Konfigurations- und Datendateien überschrieben werden.

Diese Informationen beziehen sich auf neue Installationen von QRadar Risk Manager oder auf Upgrades von neuen QRadar Risk Manager-Installationen auf QRadar Risk Manager-Appliances. Wenn Sie QRadar Risk Manager installieren, wird das Installationsprogramm (QRadar SIEM-ISO) in die Wiederherstellungspartition kopiert. Auf der Grundlage dieser Partition können Sie QRadar Risk Manager erneut installieren. Dabei wird QRadar Risk Manager auf die werkseitigen Voreinstellungen zurückgesetzt.

Anmerkung: Wenn Sie Ihre Software nach der Installation von QRadar Risk Manager aufrüsten, wird die ISO-Datei durch die neuere Version ersetzt.

Wenn Sie Ihre QRadar Risk Manager-Appliance neu starten, wird eine Option für die Neuinstallation der Software angezeigt. Da QRadar SIEM und QRadar Risk Manager dieselbe ISO-Installationsdatei verwenden, wird der QRadar SIEM-ISO-Name angezeigt.

Wenn Sie nicht innerhalb von fünf Sekunden auf die Systemanfrage reagieren, wird das System wie üblich neu gestartet. In diesem Fall bleiben Ihre Konfigurations- und Datendateien erhalten. Wenn Sie sich für eine Neuinstallation der QRadar SIEM-ISO-Version entscheiden, wird eine Warnung angezeigt und Sie müssen bestätigen, dass Sie die Software tatsächlich erneut installieren möchten. Nach der Bestätigung wird das Installationsprogramm ausgeführt und Sie können den Installationsprozess mithilfe der Bedienerführung durchlaufen.

Nach einem Festplattenfehler ist keine Neuinstallation auf Basis der Wiederherstellungspartition möglich, da diese nicht mehr verfügbar ist. Wenden Sie sich bei einem Festplattenfehler an die Kundenunterstützung, die Ihnen behilflich sein wird.

QRadar Risk Manager mithilfe der Factory-Neuinstallation erneut installieren

Sie können Ihre QRadar Risk Manager-Appliance neu starten und mit der Factory-Neuinstallationsoption erneut installieren.

Vorbereitende Schritte

Stellen Sie sicher, dass Sie über Ihren Aktivierungsschlüssel verfügen. Dieser ist eine alphanumerische Zeichenfolge mit 24 Stellen und vier Teilen, die Sie von IBM erhalten. Sie finden den Schlüssel an folgenden Stellen:

- Als Ausdruck auf einem Aufkleber, der an Ihrer Appliance angebracht ist.
- Auf dem Packzettel; die Appliances werden gemeinsam mit ihren zugehörigen Schlüsseln aufgelistet.

Zur Vermeidung von Eingabefehlern werden der Buchstabe I und die Zahl 1 (Eins) sowie der Buchstabe O und die Zahl 0 (Null) gleichwertig behandelt.

Wenn Sie keinen Aktivierungsschlüssel für Ihre QRadar Risk Manager-Appliance erhalten haben, wenden Sie sich an die Kundenunterstützung (http://www.ibm.com/support).

Die Aktivierungsschlüssel für Software erfordern keine Seriennummern.

Vorgehensweise

1. Starten Sie Ihre QRadar Risk Manager-Appliance neu.
2. Wählen Sie **Factory re-install** (Factory-Neuinstallation) aus.
3. Geben Sie `flatten` ein, um fortzufahren. Die Festplatte wird partitioniert und neu formatiert, das Betriebssystem wird installiert und anschließend wird QRadar Risk Manager erneut installiert. Sie müssen warten, bis der Prozess 'flatten' abgeschlossen ist. Je nach System kann dieser Prozess einige Minuten dauern.
4. Geben Sie `SETUP` ein.
5. Melden Sie sich als Rootbenutzer bei QRadar Risk Manager an.
6. Lesen Sie die Informationen in dem Fenster. Mit der Leertaste können Sie jeweils um ein Fenster vorspringen, bis Sie zum Ende des Dokuments gelangen. Geben Sie `yes` (Ja) ein, um die Vereinbarung zu akzeptieren, und drücken Sie dann die Eingabetaste.
7. Geben Sie Ihren Aktivierungsschlüssel ein und drücken Sie die Eingabetaste.
8. Wählen Sie als Installationstyp **Normal** aus. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
9. Wählen Sie den Kontinent oder das Land Ihrer Zeitzone aus. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
10. Wählen Sie die Region Ihrer Zeitzone aus. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
11. Wählen Sie eine Internet Protocol-Version aus. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
12. Wählen Sie die Schnittstelle aus, die Sie als Verwaltungsschnittstelle angeben möchten. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
13. Geben Sie Informationen für Ihren Hostnamen, Ihre IP-Adresse, Ihre Netzmaske, Ihr Gateway, Ihr primäres und sekundäres Domänennamenssystem (Domain Name System, DNS) sowie für Ihr öffentliches IP und Ihren E-Mail-Server ein. Sie finden die Netzinformationen im Abschnitt „Informationen zu den Netzparametern für Internet Protocol Version 4 (IPv4)" auf Seite 6.
14. Geben Sie Ihr Kennwort ein, um das Rootkennwort für QRadar Risk Manager zu konfigurieren.
15. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
16. Geben Sie Ihr neues Kennwort zur Bestätigung erneut ein. Wählen Sie **Beenden** aus und drücken Sie die Eingabetaste. Dieser Prozess dauert in der Regel einige Minuten.
17. Drücken Sie die Eingabetaste, um OK auszuwählen.
18. Drücken Sie die Eingabetaste, um OK auszuwählen.

Nächste Schritte

Verwenden Sie den Implementierungseditor zum Hinzufügen von QRadar Risk Manager als verwalteten Host zu Ihrer QRadar SIEM-Konsole.

Kapitel 4. Netzeinstellungen ändern

Sie können die Netzeinstellungen einer IBM Security QRadar Risk Manager-Appliance, die einer IBM Security QRadar SIEM-Konsole zugeordnet wird, ändern.

Wenn Sie die Netzeinstellungen ändern müssen, müssen Sie die unten genannten Aufgaben in der folgenden Reihenfolge ausführen:

1. Entfernen Sie QRadar Risk Manager als verwalteten Host.
2. Ändern Sie die Netzeinstellungen.
3. Fügen Sie QRadar Risk Manager erneut als verwalteten Host hinzu.

Verwalteten Host entfernen

Sie können Ihren verwalteten IBM Security QRadar Risk Manager-Host zur Änderung von Netzeinstellungen oder bei einem Problem mit der Registerkarte **Risks** (Risiken) aus IBM Security QRadar SIEM entfernen.

Vorgehensweise

1. Öffnen Sie Ihren Web-Browser.
2. Geben Sie die URL `https://<IP-Adresse>` ein. Dabei steht <IP-Adresse> für die IP-Adresse der QRadar SIEM-Konsole.
3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.

   Sie finden die Standardanmeldeinformationen im Abschnitt Tabelle 2 auf Seite 6.
4. Klicken Sie auf der Registerkarte **Verwaltung (Admin)** auf **Implementierungseditor**.
5. Klicken Sie auf die Registerkarte **Systemansicht**.
6. Klicken Sie mit der rechten Maustaste auf den verwalteten Host, den Sie löschen möchten, und wählen Sie **Löschen** aus. Wiederholen Sie diesen Vorgang für jeden verwalteten Host ohne Konsole, bis alle Hosts gelöscht sind.
7. Klicken Sie auf **Speichern**.
8. Schließen Sie den Implementierungseditor.
9. Klicken Sie auf der Registerkarte **Verwaltung (Admin)** auf **Änderungen implementieren**.

Netzeinstellungen ändern

Sie können die Netzeinstellungen einer IBM Security QRadar Risk Manager-Appliance, die einer IBM Security QRadar SIEM-Konsole zugeordnet wird, ändern.

Vorbereitende Schritte

Vor der Änderung der Netzeinstellungen müssen Sie den verwalteten QRadar Risk Manager-Host aus QRadar SIEM entfernen.

Vorgehensweise

1. Melden Sie sich unter Verwendung von Secure Shell (SSH) als Rootbenutzer bei QRadar Risk Manager an.
2. Geben Sie den Befehl `qchange_netsetup` ein.

3. Wählen Sie eine Internet Protocol-Version aus. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste. Je nach Ihrer Hardwarekonfiguration können im Fenster bis zu vier Schnittstellen angezeigt werden. Jede Schnittstelle mit einer physischen Verbindung ist durch ein Pluszeichen (+) gekennzeichnet.
4. Wählen Sie die Schnittstelle aus, die Sie als Verwaltungsschnittstelle angeben möchten. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
5. Geben Sie Informationen für Ihren Hostnamen, Ihre IP-Adresse, Ihre Netzmaske, Ihr Gateway, Ihr primäres und sekundäres Domänennamenssystem (Domain Name System, DNS) sowie für Ihr öffentliches IP und Ihren E-Mail-Server ein. Sie finden die Netzinformationen im Abschnitt „Informationen zu den Netzparametern für Internet Protocol Version 4 (IPv4)" auf Seite 6.
6. Geben Sie Ihr Kennwort ein, um das Rootkennwort für QRadar Risk Manager zu konfigurieren.
7. Wählen Sie **Weiter** aus und drücken Sie die Eingabetaste.
8. Geben Sie Ihr neues Kennwort zur Bestätigung erneut ein. Wählen Sie **Beenden** aus und drücken Sie die Eingabetaste. Dieser Prozess dauert in der Regel einige Minuten.

QRadar Risk Manager erneut als verwalteten Host hinzufügen

Sie können QRadar Risk Manager erneut als verwalteten Host hinzufügen, wenn er zuvor entfernt wurde.

Vorgehensweise

1. Öffnen Sie Ihren Web-Browser.
2. Geben Sie die URL `https://<IP-Adresse>` ein. Dabei steht <IP-Adresse> für die IP-Adresse der QRadar SIEM-Konsole.
3. Geben Sie Ihren Benutzernamen und Ihr Kennwort ein.

   Sie finden die Standardanmeldeinformationen im Abschnitt Tabelle 2 auf Seite 6.
4. Klicken Sie auf der Registerkarte **Verwaltung (Admin)** auf **Implementierungseditor**.
5. Klicken Sie auf die Registerkarte **Systemansicht**.
6. Wählen Sie im Menü nacheinander **Aktionen** > **Add a managed host** (Verwalteten Host hinzufügen) aus.
7. Klicken Sie auf **Weiter**.
8. Geben Sie im Fenster **Add new managed host** (Neuen verwalteten Host hinzufügen) die entsprechenden Werte ein.
9. Klicken Sie auf **Weiter**.
10. Klicken Sie auf **Beenden**. Es kann einige Minuten dauern, bis der QRadar Risk Manager hinzugefügt wurde.
11. Schließen Sie den Implementierungseditor.
12. Klicken Sie auf der Registerkarte **Verwaltung** auf **Änderungen implementieren**.

Kapitel 5. Sicherung und Wiederherstellung von Daten

Mithilfe eines Scripts, das in der Befehlszeilenschnittstelle (Command-Line Interface, CLI) ausgeführt wird, können Sie die auf verwalteten IBM Security QRadar SIEM-Hosts gespeicherten Daten sichern.

Mit dem CLI-Script können Sie IBM Security QRadar Risk Manager nach einem Datenfehler oder Hardwareausfall auf der Appliance wiederherstellen.

QRadar Risk Manager umfasst ein Sicherungsscript, dessen Ausführung mit crontab geplant werden kann. Das Script erstellt automatisch jeden Tag um 3 Uhr morgens ein Archiv der QRadar Risk Manager-Daten. QRadar Risk Manager speichert standardmäßig die letzten fünf Sicherungen. Falls Sie über einen Netzspeicher oder angehängten Speicher verfügen, müssen Sie einen cron-Job erstellen, um die Sicherungsarchive an Ihren Netzspeicherort zu kopieren.

Das Sicherungsarchiv schließt die folgenden Daten ein:

- QRadar Risk Manager-Einheitenkonfigurationen
- Verbindungsdaten
- Topologiedaten
- Fragen aus der Richtlinienüberwachung
- QRadar Risk Manager-Datenbanktabellen

Sie finden Informationen zur Migration von QRadar Risk Manager Maintenance Release 5 auf dieses aktuelle Release im *IBM Security QRadar Risk Manager Migrationshandbuch*.

Voraussetzungen für die Sicherung und Wiederherstellung von Daten

Machen Sie sich vor der Sicherung und Wiederherstellung Ihrer Daten eingehend damit vertraut, wie Daten gesichert, gespeichert und archiviert werden.

Speicherort der Datensicherung

Die Daten werden im lokalen Verzeichnis `/store/qrm_backups` gesichert. Möglicherweise wurde auf Ihrem System über eine Mountoperation das Verzeichnis `/store/backup` aus einem externen SAN- oder NAS-Service zugeordnet. Externe Services stellen eine langfristige Offline-Aufbewahrung der Daten zur Verfügung. Die Langzeitspeicherung kann erforderlich sein, damit Konformitätsregelungen (zum Beispiel PCI-Standards aus der Kreditkartenbranche) eingehalten werden können.

Version der Appliance

Es wird die Version der Appliance gespeichert, von der die Sicherung im Archiv erstellt wurde. Eine Sicherung kann nur dann in einer QRadar Risk Manager-Appliance wiederhergestellt werden, wenn dieselbe Version verwendet wird.

Häufigkeit der Datensicherung und Archivierungsinformationen

Datensicherungen werden täglich um 3 Uhr morgens erstellt. Nur die letzten fünf Sicherungsdateien werden gespeichert. Falls genügend freier Speicherplatz in QRadar Risk Manager verfügbar ist, wird ein Sicherungsarchiv erstellt.

Format der Sicherungsdateien

Verwenden Sie beim Speichern von Sicherungsdateien folgendes Format:
`backup-<Zieldatum>-<Zeitmarke>.tgz`

Dabei gilt Folgendes:

`<Zieldatum>` ist das Datum, an dem die Sicherungsdatei erstellt wurde.

Das Format des Zieldatums lautet `<Tag>_<Monat>_<Jahr>`. `<Zeitmarke>` gibt die Uhrzeit an, zu der die Sicherungsdatei erstellt wurde. Das Format der Zeitmarke lautet `<Stunde>_<Minute>_<Sekunde>`.

Daten sichern

Jeden Tag wird um 3 Uhr morgens eine automatische Sicherung durchgeführt. Sie können den Sicherungsprozess jedoch auch manuell starten.

Vorgehensweise

1. Melden Sie sich unter Verwendung von Secure Shell (SSH) als Rootbenutzer bei Ihrer QRadar SIEM-Konsole an.
2. Melden Sie sich unter Verwendung von Secure Shell (SSH) von der QRadar SIEM-Konsole aus als Rootbenutzer bei QRadar Risk Manager an.
3. Starten Sie eine QRadar Risk Manager-Sicherung, indem Sie `/opt/qradar/bin/dbmaint/risk_manager_backup.sh` eingeben.

Ergebnisse

Es kann einige Minuten dauern, bis das Script für den Start des Sicherungsprozesses gestartet wird.

Nachdem das Script den Sicherungsprozess abgeschlossen hat, wird folgende Nachricht angezeigt:

```
Tue Sep 11 10:14:41 EDT 2012
- Risk Manager Backup complete,
wrote /store/qrm_backups/backup-2012-09-11-10-14-39.tgz
```

Daten wiederherstellen

Mithilfe eines Wiederherstellungsscripts können Sie Daten aus einer QRadar Risk Manager-Sicherung wiederherstellen.

Vorbereitende Schritte

Die QRadar Risk Manager-Appliance und das Sicherungsarchiv müssen dieselbe Version von QRadar Risk Manager aufweisen. Falls das Script eine Versionsabweichung zwischen dem Archiv und dem verwalteten QRadar Risk Manager-Host findet, wird ein Fehler angezeigt.

Informationen zu diesem Vorgang

Verwenden Sie das Wiederherstellungsscript für die Angabe des Archivs, das Sie in QRadar Risk Manager wiederherstellen möchten. Für diesen Prozess müssen Sie die Services in QRadar Risk Manager stoppen. Durch das Stoppen der Services werden alle QRadar Risk Manager-Benutzer abgemeldet und mehrere Prozesse gestoppt.

In der folgenden Tabelle werden die Parameter beschrieben, die Sie für die Wiederherstellung eines Sicherungsarchivs verwenden können.

Tabelle 3. Für die Wiederherstellung eines Sicherungsarchivs in QRadar Risk Manager verwendete Parameter

Option	Beschreibung
-f	Überschreibt alle vorhandenen QRadar Risk Manager-Daten auf Ihrem System mit den Daten in der Wiederherstellungsdatei. Wenn Sie diesen Parameter auswählen, kann das Script alle vorhandenen Einheitenkonfigurationen in der Konfigurationsquellenverwaltung mit den Einheitenkonfigurationen aus der Sicherungsdatei überschreiben.
-w	Vor der Wiederherstellung der QRadar Risk Manager-Daten werden keine Verzeichnisse gelöscht.
-h	Der Hilfetext für das Wiederherstellungsscript.

Vorgehensweise

1. Melden Sie sich unter Verwendung von Secure Shell (SSH) als Rootbenutzer bei Ihrer QRadar SIEM-Konsole an.
2. Melden Sie sich unter Verwendung von Secure Shell (SSH) von der QRadar SIEM-Konsole aus als Rootbenutzer bei QRadar Risk Manager an.
3. Stoppen Sie den Hostkontext, indem Sie `service hostcontext stop` eingeben.
4. Geben Sie folgenden Befehl ein, um ein Sicherungsarchiv in QRadar Risk Manager wiederherzustellen: `/opt/qradar/bin/risk_manager_restore.sh -r /store/qrm_backups/<Sicherung>`. Dabei steht `<Sicherung>` für das QRadar Risk Manager-Archiv, das Sie wiederherstellen möchten.

   Beispiel: backup-2012-09-11-10-14-39.tgz.
5. Starten Sie den Hostkontext, indem Sie `service hostcontext start` eingeben.

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 Defense
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 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 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).

Adobe und Acrobat sowie alle auf Adobe basierenden Marken sind eingetragene Marken oder Marken von Adobe Systems Incorporated in den USA und/oder anderen Ländern.

Java und alle auf Java basierenden Marken und Logos sind Marken oder eingetragene Marken von Sun Microsystems, Inc. in den USA und/oder anderen Ländern.

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

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

GC12-5039-00