IBM Security QRadar Incident Forensics
Version 7.3.0

QRadar Packet Capture - Kurzübersicht

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten die Informationen unter „Bemerkungen" auf Seite 7 gelesen werden.

Produktinformation

Dieses Dokument bezieht sich auf IBM QRadar Security Intelligence Platform V7.3.0 sowie auf nachfolgende Releases, sofern es nicht durch eine aktuellere Version ersetzt wurde.

Inhaltsverzeichnis

Informationen zu dieser Packet Capture-Kurzübersicht v

Kapitel 1. Upgrade von QRadar Packet Capture durchführen 1

Kapitel 2. QRadar Packet Capture - Kurzübersicht 3

Bemerkungen 7
Marken 8
Bedingungen für Produktdokumentation 8
IBM Online-Datenschutzerklärung 9

Informationen zu dieser Packet Capture-Kurzübersicht

In dieser Dokumentation finden Sie Informationen in einer Kurzübersicht, die für die Installation und Konfiguration von IBM® Security QRadar Packet Capture erforderlich sind. QRadar Packet Capture wird von IBM Security QRadar unterstützt.

Zielgruppe

Systemadministratoren, die für die Installation von QRadar Packet Capture zuständig sind, müssen mit Konzepten zur Netzsicherheit und mit der Gerätekonfiguration vertraut sein.

Technische Dokumentation

Die Produktdokumentation zu IBM Security QRadar in der QRadar-Produktbibliothek finden Sie unter 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 rechtmäßige Zwecke und auf rechtmäßige 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 erklärt, dass er die Zustimmung, Berechtigungen oder Lizenzen einholt bzw. einholen wird, die für die rechtmäßige Verwendung von IBM Security QRadar erforderlich sind.

Kapitel 1. Upgrade von QRadar Packet Capture durchführen

Um ein Upgrade von QRadar Packet Capture V7.2.8 auf V7.3.0 durchzuführen, installieren Sie ein kumulatives Software-Fixpack auf einer QRadar Packet Capture-Appliance. Die Softwareversion, die auf der Appliance installiert wird, muss Build 7.2.6.241 sein.

Vorgehensweise

1. Stellen Sie sicher, dass keine Paketaufzeichnungs- oder Suchaktivitäten in Bearbeitung sind.
2. Melden Sie sich über SSH als `root`-Benutzer bei Ihrem System an.
3. Laden Sie das Fixpack `7.3.0-QRadar-PCAP-build<build_number>.sfs` aus IBM Fix Central (http://www.ibm.com/support/fixcentral/) herunter.
4. Kopieren Sie das Fixpack in das `/tmp`-Verzeichnis.

   Falls der Speicherplatz im Verzeichnis `/tmp` begrenzt ist, kopieren Sie das Fixpack an einen anderen Speicherort, an dem ausreichend Speicherplatz vorhanden ist.
5. Erstellen Sie das Verzeichnis `/updates`, indem Sie den folgenden Befehl eingeben:

   ```
   mkdir -p /updates
   ```
6. Verwenden Sie den Befehl **cd**, um in das Verzeichnis zu wechseln, in das Sie die Fixpackdatei kopiert haben.

   ```
   cd /tmp
   ```
7. Geben Sie folgenden Befehl ein, um die Fixpackdatei an das Verzeichnis `/updates` anzuhängen:

   ```
   mount -o loop -t squashfs 7.3.0-QRadar-PCAP-build<Buildnummer>.sfs
   /updates
   ```
8. Um das Installationsprogramm für das Fixpack auszuführen, wechseln Sie in das Verzeichnis `/updates` und geben Sie folgenden Befehl ein:

   ```
   sh installer.sh
   ```
9. Starten Sie das System erneut.

Kapitel 2. QRadar Packet Capture - Kurzübersicht

Vor dem Aufzeichnen von Paketen müssen Sie zunächst die Netz- und Verbindungseinstellungen für IBM Security QRadar Packet Capture konfigurieren.

Intel SFP+- und SFP-Kompatibilitätsliste

Die QRadar Packet Capture-Appliance verfügt über nur einen Erfassungsport (DNA0). Die QRadar Packet Capture-Appliance ist nicht mit einem SFP-Transceiver ausgestattet, daher müssen Sie entweder ein SFP+ 10G oder SFP 1G (Copper RJ45) im Erfassungsport installieren.

Zum Kauf von SFP-Modulen für Ihre QRadar Packet Capture-Appliance siehe folgende Anbieterwebsites:

- Website von Digi-Key (http://www.digikey.com)
- Website von Mouser Electronics (http://www.mouser.com)
- Website von CDW (http://www.cdw.com)
- Website von Newegg (https://www.newegg.com)
- Website von Amazon (http://amazon.com)

Wenn SFP 1G installiert ist, kürzt es die Erfassungsrate auf 1 Gb/s.

Um mehrere 1G-Verbindungen zu erhalten, können Sie einen Switch oder einen Aggregator an der Stelle platzieren, an der der 10G-Port für abgehende Daten in den QRadar Packet Capture-SFP+-10G-Port übergeht. Als Ergebnis können Sie mehrere 1Gb-Ports in die QRadar Packet Capture-10G-SFP+-Schnittstelle aggregieren.

In der folgenden Liste werden die SFP+- und SFP-Modulanforderungen beschrieben:

Teilenummer	**Beschreibung**
E10GSFPSR	Dual Rate 10GBASE-SR/1000BASE-SX, Intel Ethernet SFP+ SR Optical
E10GSFPLR	Dual Rate 10GBASE-LR/1000BASE-LX, Intel Ethernet SFP+ LR Optical
FCLF8522P2BTL	1000BASE-T, Finisar Gigabit Ethernet Transceiver
453153-001	HP Gigabit SX Transceiver

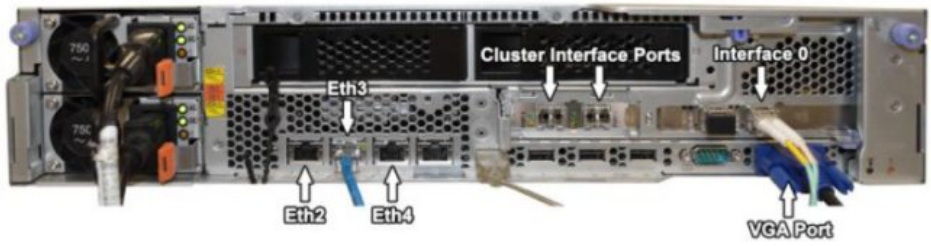
Netzkonfiguration

Bei der Erstkonfiguration des Netzes sind ein Bildschirm, eine Tastatur und eine Ethernet-Verbindung zu einem Onboard-Port erforderlich. Das System verfügt standardmäßig über aktive DHCP-Ports.

Wenn Sie die IP-Adresse des aktiven Ethernet-Ports kennen, fahren Sie mit Start recording (Aufzeichnung starten) fort.

1. Stellen Sie eine Netzverbindung für den Fernzugriff auf den Server bereit.

   Stellen Sie eine Ethernet-Verbindung für einen der integrierten Ehternet-Ports (eth2, eth3 oder eth4) bereit, wie im folgenden Diagramm gezeigt wird.



2. Geben Sie eine Netzverbindung für die Netzaufzeichnung an.

   Stellen Sie mit den im folgenden Diagramm gezeigten Ports der Schnittstelle 0 10G-Glasfaserverbindungen bereit.

   Wichtig: Stellen Sie sicher, dass Daten über die Verbindungen übertragen werden. Für die Aufzeichnung des Datenverkehrs muss ein TAP-Port oder ein SPAN-Port (Spiegelport) verwendet werden. Wenn Sie einen SPAN-Port auf einem Switch verwenden und der Switch diesem SPAN-Port eine niedrige Priorität zuweist, gehen einige Pakete unter Umständen verloren.

3. Melden Sie sich über die Secure Shell (SSH) und Port 4477 als Rootbenutzer an.

   Der standardmäßige Benutzername lautet `root`. Das Standardkennwort ist: `P@ck3t08..`

4. Schreiben Sie die IP-Adresse auf.

   Öffnen Sie nach der Anmeldung ein Terminal und geben Sie den folgenden Befehl ein: `#ifconfig -a`

   Mit diesem Befehl wird die IP-Adresse des Ethernet-Ports bereitgestellt, zu dem eine Verbindung hergestellt ist.

   Anmerkung: Weitere Informationen zum Einrichten einer statischen IP-Adresse finden Sie im *IBM Security QRadar Packet Capture User Guide.*

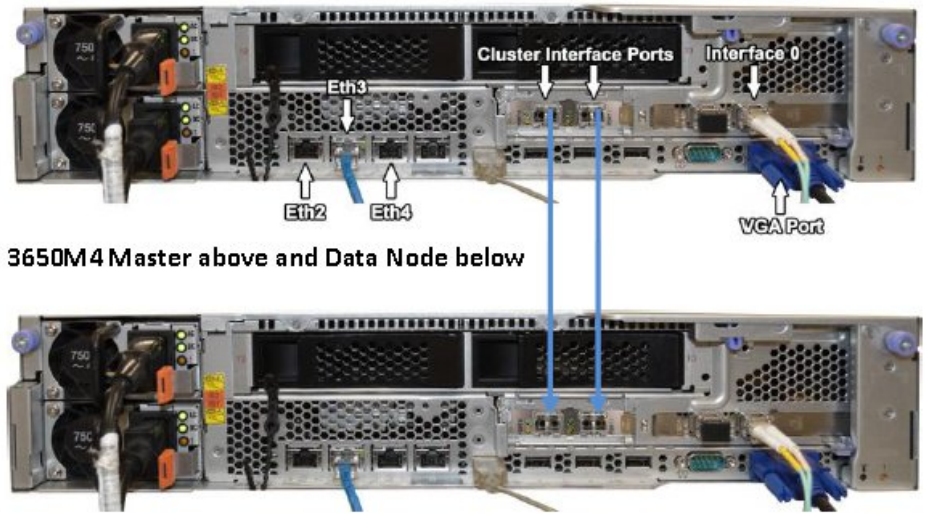
5. Testen Sie die Verbindung.

   Zum Testen der Verbindung überprüfen Sie Ihr internes Netz mit einem Pingsignal oder melden sich mithilfe von SSH über Fernzugriff an Port 4477 an. Stellen Sie vor dem Fortfahren sicher, dass eine Verbindung erfolgreich hergestellt ist.

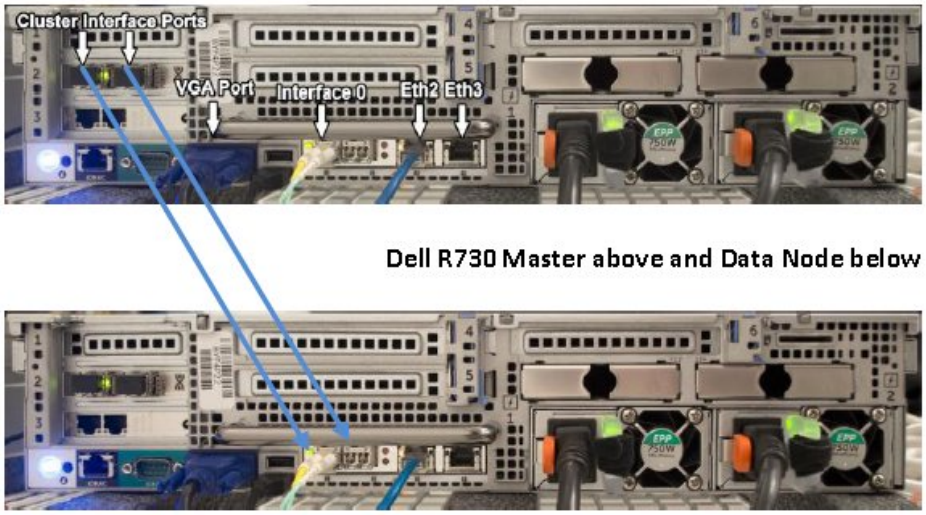
Verbindung zum Cluster herstellen

Nachdem Sie die Verbindung vom Netz zum eigenständigen System oder dem Mastersystem erfolgreich hergestellt haben, verbinden Sie die Master-Paketaufzeichnungseinheit mit den Appliances des QRadar Packet Capture-Datenknotens. Wenn Sie nur ein eigenständiges Paketaufzeichnungssystem verwenden, ist dieser Schritt nicht erforderlich.

1. Weitere Informationen finden Sie im Hardwarediagramm zu Ihrer Paketaufzeichnungseinheit.
   - IBM System x3650 M4-Master-Paketaufzeichnungseinheit und QRadar Packet Capture Data Node-Verbindung



   - Dell R730-Paketaufzeichnungseinheit und QRadar Packet Capture Datenknoten



2. Verbinden Sie auf der Rückseite der Paketaufzeichnungseinheit den linken Port für die Schnittstelle des Clusters auf dem Mastersystem mit dem linken Port für die Schnittstelle des Clusters im ersten Datenknoten, wie durch die Pfeile in den vorherigen Diagrammen angezeigt wird.
3. Wenn ein zweiter Datenknoten vorhanden ist, verbinden Sie den rechten Port für die Schnittstelle des Clusters auf dem Mastersystem mit dem rechten Port für die Schnittstelle auf dem zweiten Datenknoten.
4. Überprüfen Sie die Verbindungen aus einem Terminal auf dem Mastersystem mithilfe eines Pingtests:

```
ping 1.1.1.2
ping 2.2.2.2
```

5. Wenn Sie keine Antwort vom Pingsignal empfangen, tauschen Sie die Kabelverbindungen nur auf den Schnittstellen des Datenknotens.

- Wenn nur ein Datenknoten angeschlossen ist, muss nur ein Pingsignal erfolgreich antworten.
- Wenn nach dem Tausch der Kabel noch immer keine Antwort vom Pingsignal empfangen wird, tauschen Sie die Kabel auf der Netzschnittstellenkarte des Datenknotens mit der zweiten installierten Netzschnittstellenkarte des optischen Ethernets (falls vorhanden) und wiederholen den Pingtest.

Aufzeichnung starten

Nachdem eine erfolgreiche Netzverbindung mit dem System hergestellt wurde, können Sie mit dem Aufzeichnen von Netzpaketen auf einem Datenträger und der Anzeige von Statistikdaten zum Datenverkehr in einem Netz starten.

1. Öffnen Sie einen Web-Browser und greifen Sie auf die Einheit zu:

   `https://`*`PCAP-IP-Adresse`*`:41390`
2. Melden Sie sich mit folgenden Benutzerinformationen an:

   Benutzer: `continuum`

   Kennwort: `P@ck3t08..`
3. Aktivieren Sie jeden Datenknoten (Slave), für den eine physische Verbindung hergestellt wurde.
4. Starten Sie die Aufzeichnung.

   Nach dem Anmelden und der Aktivierung der Datenknoten wechseln Sie auf die Seite **Capture State** (Aufzeichnungsstatus) und klicken auf **Start Capture** (Aufzeichnung starten).

   Anmerkung: Nach dem Start der Aufzeichnung wird ein Fenster mit Statistikdaten angezeigt, in dem alle Einzelheiten zur Datenerfassung enthalten sind.

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 die in diesem Handbuch beschriebenen 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 gezeigten Leistungsdaten und Clientbeispiele dienen lediglich Darstellungszwecken. Die tatsächlichen Leistungsdaten sind von der jeweiligen Konfiguration und den Betriebsbedingungen abhängig.

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

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

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

Bedingungen für Produktdokumentation

Die Berechtigung zur Nutzung dieser Veröffentlichungen wird 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 weder weitergeben oder anzeigen noch 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.

Berechtigung

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

IBM behält sich das Recht vor, die hierin 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 Informationen. 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 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 Datenschutzerklärung, Schwerpunkte" 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"
(http://www.ibm.com/software/info/product-privacy).

Gedruckt in Deutschland