IBM Security QRadar Incident Forensics
Version 7.3.0

QRadar Packet Capture-Benutzerhandbuch

Hinweis

Vor Verwendung dieser Informationen und des darin beschriebenen Produkts sollten Sie die Informationen unter „Bemerkungen" auf Seite 29 lesen.

Produktinformation

Die Informationen in diesem Dokument gelten für IBM QRadar Security Intelligence Platform V7.3.0 sowie für nachfolgende Releases, bis sie durch eine aktualisierte Version dieses Dokuments ersetzt werden.

Inhaltsverzeichnis

Informationen zum vorliegenden Packet Capture-Benutzerhandbuch

Das vorliegende Dokument enthält die für die Installation und Konfiguration von IBM® Security QRadar Packet Capture erforderlichen Informationen.

Zielgruppe

Die für die Installation von QRadar Packet Capture zuständigen Systemadministratoren müssen mit Netzsicherheitskonzepten und Gerätekonfigurationen vertraut sein.

Technische Dokumentation

Die Produktdokumentation für IBM Security QRadar in der QRadar-Produktbibliothek finden Sie unter Accessing IBM Security documentation (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. QRadar Packet Capture - Einführung

IBM Security QRadar Packet Capture ist eine Anwendung zum Aufzeichnen und Durchsuchen von Netzverkehrsdaten. Die Anwendung QRadar Packet Capture verfügt nur über einen Erfassungsport (DNA0), an dem Sie einen 10G- oder einen 1G-SFP-Transceiver installieren können.

Mit QRadar Packet Capture können Sie Netzpakete mit einer Rate von bis zu 10 Gb/s aus einer aktiven Netzschnittstelle aufzeichnen und Dateien ohne Paketverlust schreiben.

Mit QRadar Packet Capture können Sie aufgezeichneten Netzverkehr nach Zeitangabe und Paketenvelopdaten durchsuchen. Wenn ausreichend Appliance-Ressourcen und angepasste Suchvorgänge vorhanden sind, können Sie Suchdaten und Aufzeichnungsdaten gleichzeitig ohne Datenverlust verwenden.

QRadar Packet Capture-Appliances mit einem 10G-Transceiver unterstützen Cluster, die die Gesamtspeicherkapazität und die Rechenleistung gegenüber einem eigenständigen Einzelserver erhöhen. QRadar Packet Capture-Appliances mit einem 1G-Transceiver unterstützen keine Cluster.

QRadar Packet Capture - Leistungsmerkmale

Hier einige der Leistungsmerkmale von QRadar Packet Capture:

PCAP-Standarddateiformat
: Ein Dateiformat zum Speichern von Netzverkehr. Das Dateiformat erlaubt die Integration in bereits vorhandene Analysetools anderer Hersteller.

Leistungsstarke Aufzeichnung von Paketen auf Platte
: Erfassen Sie Netzpakete aus einem Livenetz.

Multi-Core-Unterstützung
: QRadar Packet Capture ist für Multi-Core-Architekturen konzipiert.

Direkter E/A-Zugriff auf Platten
: QRadar Packet Capture verwendet direkten E/A-Plattenzugriff, um einen maximalen Schreibdurchsatz auf der Platte zu ermöglichen.

Echtzeitindexierung
: QRadar Packet Capture kann während der Paketaufzeichnung automatisch einen Index erstellen. Dieser Index kann mithilfe einer BPF-ähnlichen Syntax (BPF = Berkeley Packet Filter) bzw. mit HTTP-Domänen- oder Basis-URL-Zeichenfolgen abgefragt werden und ermöglicht so den Abruf der gewünschten Pakete innerhalb eines angegebenen Zeitintervalls.

Clusterfähig zur Erhöhung der Speicherkapazität für Aufzeichnungsdaten (nur 10G-Edition).
: Sie können Datenknoten zum Erstellen eines Clusters für zusätzliche Speicherkapazität aktivieren.

Speicherformat

Aufzeichnungsdateien werden im PCAP-Standardformat mit Zeitmarken in Mikrosekundenauflösung gespeichert. Aufzeichnungsdateien werden der Größe nach ge-

speichert. Die Aufzeichnungsdateien werden in Verzeichnissen gespeichert. Wenn der Speicherplatz im Verzeichnis nicht mehr ausreicht, werden die Aufzeichnungsdateien basierend auf vorkonfigurierten Aufzeichnungsparametern überschrieben.

Aufzeichnungsgeschwindigkeit

Bei Paketaufzeichnungs-Appliances hängt die Geschwindigkeit der Aufzeichnung von Datenaustausch im Netz davon ab, ob Datenknoten an den Hauptknoten angehängt sind:

- Bei Paketaufzeichnungs-Appliances, bei denen keine Datenknoten angehängt sind, beträgt die maximale Aufzeichnungsgeschwindigkeit bis zu 7 Gb/s.
- Bei Paketaufzeichnungs-Appliances mit an den Hauptknoten angehängten Datenknoten erhöht sich die maximale Aufzeichnungsgeschwindigkeit auf bis zu 10 Gb/s.

Weitere Informationen zur Weiterleitung von Paketen an QRadar Packet Capture finden Sie im *IBM Security QRadar-Administrationshandbuch*.

Zugehörige Konzepte:

Kapitel 3, „Verwendung der Aufzeichnungsfunktion - Übersicht", auf Seite 9
Um Datenverkehr auf einer Platte zu erfassen, starten Sie die Aufzeichnungsanwendung. Die Aufzeichnungskomponente speichert die Netzverkehrsdaten in einem vorab konfigurierten Verzeichnis. Wenn der Speicherplatz im Verzeichnis nicht mehr ausreicht, werden vorhandene Dateien überschrieben.

Kapitel 2. QRadar Packet Capture - Setup

Vor der Verwendung von IBM Security QRadar Packet Capture sind einige grundlegende Konfigurationsschritte erforderlich.

Unterstützte Web-Browser

Folgende Web-Browser werden unterstützt:

- Google Chrome Version 44.0.2403.157 oder höher
- Mozilla Firefox Version 40.0.3 oder höher

Netz einrichten

Damit QRadar Packet Capture über Fernzugriff verfügbar ist, muss einem der Ethernet-Anschlüsse (in der Regel eth2, eth3 oder eth4) eine IP-Adresse zugewiesen werden. Standardmäßig ist das System für die Verwendung von Dynamic Host Configuration Protocol (DHCP) konfiguriert. Für die Erstkonfiguration müssen Sie u. U. einen VGA-kompatiblen Monitor anschließen.

Führen Sie für die Erstkonfiguration die folgenden Schritte aus:

1. Schalten Sie die QRadar Packet Capture-Appliance ein.
2. Verwenden Sie SSH und Port 4477, um sich als Rootbenutzer anzumelden.

   Der Standardbenutzername ist `root`. Das Standardkennwort ist `P@ck3t08.`

   Sie finden Informationen zur Änderung des Standardkennworts im Abschnitt „Kennwort des Betriebssystemkontos ändern" auf Seite 5.
3. Um sicherzustellen, dass Ihr System auf dem neuesten Stand ist, wenden Sie die Software-Fixes an, die in IBM Fix Central (www.ibm.com/support/fixcentral/) verfügbar sind.
4. Konfigurieren Sie eine statische IP-Adresse für Ihr eigenes Netz:
   a. Geben Sie folgenden Befehl ein, um die MAC-Adresse oder die eth2-Schnittstelle abzurufen:

      ```
      ifconfig | grep eth2
      ```

      Die Schnittstellen 'eth0' und 'eth1' sind nicht verfügbar. Verwenden Sie 'eth2' für M4 xSeries-Hardware.
   b. Notieren Sie sich die MAC-Adresse.
   c. Bearbeiten Sie die Einstellungen in der Datei `/etc/sysconfig/network-scripts/ifcfg-eth2`:
      - Fügen Sie als erste Zeile folgenden Text hinzu: `DEVICE=eth2`
      - Entfernen Sie die Kommentarzeichen für die MAC-Adresse des eth2-Anschlusses: `HWADDR=xx:xx:xx:xx:xx`
      - Stellen Sie sicher, dass die folgende Einstellung konfiguriert ist: `BOOTPROTO=static`
      - Stellen Sie sicher, dass Sie Informationen verwenden, die für Ihr Netz relevant sind. Die Ausgabe muss in etwa wie folgendes Beispiel für eine statische IP-Adresse aussehen:

        ```
        DEVICE=eth2
        #HWADDR=xx:xx:xx:xx:xx
        BOOTPROTO="static"
        BROADCAST="192.168.1.255"
        ```

```
DNS1="0.0.0.0"
DNS2="0.0.0.0"
GATEWAY="192.168.1.2"
IPADDR="192.168.1.1"
NETMASK="255.255.255.0"
NM_CONTROLLED="no"
ONBOOT="yes"
```

5. Speichern Sie die Datei.
6. Führen Sie folgenden Befehl aus, um die Einstellungen anzuwenden:
   `service network restart`
7. Überprüfen Sie Ihre Schnittstelleneinstellung mit folgendem Befehl:
   `ifconfig | more`

Zuweisung über DHCP - Beispiel: Bearbeiten Sie in CentOS6.2 in der Datei `/etc/sysconfig/network-scripts/ifcfg-eth0` oder `/etc/sysconfig/network-scripts/ifcfg-eth1` die folgenden Einstellungen:

```
BOOTPROTO="dhcp"
NM_CONTROLLED="no"
ONBOOT="yes"
```

Fernanmeldung

Nach Einrichtung einer lokalen IP-Adresse können Sie die Anwendung verwalten, indem Sie sich über Fernzugriff mithilfe von SSH an Port 4477 anmelden.

Lizenz konfigurieren

Vor der Verwendung von QRadar Packet Capture müssen Sie eine Lizenz für die QRadar Packet Capture-Appliance und die QRadar Packet Capture-Software konfigurieren.

Vorgehensweise

1. Führen Sie zur Konfiguration der Lizenzierung einer QRadar Packet Capture-Appliance, auf der ein SFP 1G-Transceiver installiert ist, die folgenden Schritte aus:
   a. Bitten Sie Ihren IBM Ansprechpartner um den Lizenzschlüssel für den Master-Knoten.
   b. Klicken Sie in QRadar Packet Capture auf **Help** > **Update Master License** (Hilfe > Masterlizenz aktualisieren).
   c. Zum Anwenden der erhaltenen Lizenz auf eine QRadar Packet Capture-Appliance fügen Sie den Wert in das Feld **License Key** (Lizenzschlüssel) ein.
   d. Fügen Sie die Werte für die System-ID und den Lizenzschlüssel in die entsprechenden Felder ein.
   e. Klicken Sie auf **Update Master License** (Masterlizenz aktualisieren), um die Änderungen anzuwenden.
2. Führen Sie zur Konfiguration der Lizenzierung einer QRadar Packet Capture-Appliance, auf der ein SFP+ 10G-Transceiver installiert ist, die folgenden Schritte aus:
   a. Bitten Sie Ihren IBM Ansprechpartner um einen Lizenzschlüssel für Ihre Datenknoten.
   b. Klicken Sie in QRadar Packet Capture zum Anwenden der Masterlizenz auf **Help** > **Update Master License** (Hilfe > Masterlizenz aktualisieren).

c. Fügen Sie die Werte für die System-ID und den Lizenzschlüssel in die entsprechenden Felder ein.
d. Klicken Sie auf **Update Master License** (Masterlizenz aktualisieren), um die Änderungen anzuwenden.
e. Danach klicken Sie, abhängig von der Anzahl der zu aktualisierenden Datenknoten in Ihrem Cluster, auf **Help** > **Node1** (Hilfe > Knoten1).
f. Fügen Sie zum Aktualisieren der Lizenz des Datenknotens die Werte für die System-ID und den Lizenzschlüssel in die entsprechenden Felder ein.
g. Klicken Sie zum Aktualisieren des Datenknotens auf **Update Node1 License** (Lizenz von Knoten1 aktualisieren), um die Änderungen anzuwenden.

Benutzer verwalten

Damit Benutzer auf IBM Security QRadar Packet Capture zugreifen und die Software verwenden können, müssen Sie die Benutzer hinzufügen, ihnen eine geeignete Rolle zuweisen und ihre Anmeldeberechtigungsnachweise konfigurieren.

Vorbereitende Schritte

Vergewissern Sie sich, dass Sie als Rootbenutzer (`root`) bei QRadar Packet Capture angemeldet sind. Als Alternative können Sie auch prüfen, ob Sie einen Benutzer mit dem Befehl `sudo` erstellen können.

Vorgehensweise

1. Führen Sie folgenden Befehl aus, um einen Benutzer zu erstellen:

   ```
   ./usr/local/nc/bin/nc_user_manager add <Benutzername> <Kennwort>
   <Admin|Guest>
   ```

   Falls der Benutzername <*Benutzername*> bereits vorhanden ist, schlägt dieser Befehl fehl.

   Wenn als Rolle weder eine Administratorrolle noch eine Gastrolle angegeben wird, schlägt dieser Befehl fehl.

   Wenn ein Benutzer hinzugefügt wird, können Sie für die Anmeldung beim Produkt und für die REST-API-Anmeldung denselben Benutzernamen und dasselbe Kennwort verwenden.
2. Führen Sie folgenden Befehl aus, um einen Benutzer zu löschen:

   ```
   ./usr/local/nc/bin/nc_user_manager delete <Benutzername> <Kennwort>
   ```

   Falls der Benutzername <*Benutzername*> bereits vorhanden ist, schlägt dieser Befehl fehl.

   Dieser Befehl schlägt fehl, wenn der <*Benutzername*> und das <*Kennwort*> nicht mit den Angaben übereinstimmen, die in QRadar Packet Capture aufgezeichnet sind.

   Wenn ein Benutzer gelöscht wird, können Sie für die Anmeldung beim Produkt und für die REST-API-Anmeldung denselben Benutzernamen und dasselbe Kennwort verwenden.

Kennwort des Betriebssystemkontos ändern

Ändern Sie nach der Konfiguration der Anwendung das Standard-Betriebssystemkennwort für IBM Security QRadar Packet Capture.

Um das Betriebssystemkonto zu ändern, müssen Sie als Rootbenutzer angemeldet sein.

Die Anwendungskennwörter für QRadar Packet Capture sind unabhängig von den Betriebssystemkennwörtern.

Vorgehensweise

1. Verwenden Sie SSH, um sich als `root`-Benutzer anzumelden.

   Das Standardkennwort für den Rootbenutzer ist `P@ck3t08..`
2. Zum Ändern des Kennworts für `root`-Benutzerkonten verwenden Sie den Befehl **`passwd`** *Benutzername*.

QRadar Packet Capture-Serverzeit mit der Systemzeit der QRadar-Konsole synchronisieren

Um sicherzustellen, dass die Zeiteinstellungen von IBM Security QRadar-Implementierungen konsistent sind, sodass Suchläufe und Funktionen in Zusammenhang mit Daten ordnungsgemäß arbeiten, müssen alle Appliances mit der als QRadar-Konsole fungierenden Appliance synchronisiert werden. Ein Administrator muss iptables auf der Appliance mit der QRadar-Konsole aktualisieren und anschließend so konfigurieren, dass eine rdate-Kommunikation an Port 37 möglich ist.

Vorbereitende Schritte

Die IP-Adresse bzw. der Hostname der QRadar-Konsole muss bekannt sein. Der Hostname muss mit dem Befehl 'nslookup' korrekt aufgelöst werden können.

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

Vorgehensweise

1. Melden Sie sich unter Verwendung von Secure Shell als `root`-Benutzer bei der QRadar Packet Capture-Appliance an.
2. Um den NTP-Service (Network Time Protocol) zu inaktivieren, geben Sie den Befehl `service ntpd stop` ein.
3. Um eine Überprüfung der Konfiguration auf NTP zu inaktivieren, geben Sie den Befehl `chkconfig ntpd off` ein.
4. Terminieren Sie die Synchronisierung als Cron-Job, indem Sie die Datei `crontab` (Cron-Tabelle) entsprechend bearbeiten.
   a. Geben Sie den Befehl `crontab -e` ein.
   b. Soll die Appliance alle 10 Minuten mit der QRadar-Konsole synchronisiert werden, müssen Sie den folgenden Befehl eingeben: `*/10 * * * * rdate -s` *`Konsolen-IP-Adresse`*`.`

      Geben Sie für die Variable *Konsolen-IP-Adresse* die IP-Adresse oder den Hostnamen ein.
   c. Speichern Sie die Konfigurationsänderungen.
   d. Aktivieren Sie 'crond', indem Sie die folgenden Befehle eingeben:

      ```
      service crond start
      chkconfig crond on
      ```
5. Aktualisieren Sie iptables auf der QRadar-Konsole, damit rdate-Datenverkehr aus QRadar Packet Capture-Einheiten akzeptiert wird.
   a. Melden Sie sich unter Verwendung von Secure Shell als `root`-Benutzer bei der Appliance mit der QRadar-Konsole an.
   b. Bearbeiten Sie die Datei `/opt/qradar/conf/iptables.pre`.

c. Geben Sie den folgenden Befehl ein:

```
-A QChain -m tcp -p tcp --dport 37 -j ACCEPT --src <PCAP_IP-Adresse>
```

Wenn mehrere QRadar Packet Capture-Appliances vorhanden sind, müssen die einzelnen IP-Adressen jeweils in einer eigenen Zeile stehen.

Beispiel:

```
QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.10
QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.11
QChain -m tcp -p tcp --dport 37 -j ACCEPT --src 100.100.1.12
```

d. Speichern Sie die Datei `iptables.pre`.

e. Aktualisieren Sie iptables auf der QRadar-Konsole, indem Sie den folgenden Befehl eingeben:

```
./opt/qradar/bin/iptables_update.pl
```

Zugehörige Konzepte:

Kapitel 3, „Verwendung der Aufzeichnungsfunktion - Übersicht”, auf Seite 9
Um Datenverkehr auf einer Platte zu erfassen, starten Sie die Aufzeichnungsanwendung. Die Aufzeichnungskomponente speichert die Netzverkehrsdaten in einem vorab konfigurierten Verzeichnis. Wenn der Speicherplatz im Verzeichnis nicht mehr ausreicht, werden vorhandene Dateien überschrieben.

Kapitel 3. Verwendung der Aufzeichnungsfunktion - Übersicht

Um Datenverkehr auf einer Platte zu erfassen, starten Sie die Aufzeichnungsanwendung. Die Aufzeichnungskomponente speichert die Netzverkehrsdaten in einem vorab konfigurierten Verzeichnis. Wenn der Speicherplatz im Verzeichnis nicht mehr ausreicht, werden vorhandene Dateien überschrieben.

Fehlerbehebung: Falls Sie feststellen, dass keine Daten erfasst werden, vergewissern Sie sich, dass Datenverkehr über die Verbindungen fließt. Für die Erfassung des Datenverkehrs müssen Sie einen Tap- oder SPAN-Port (Spiegelport) verwenden. Wenn Sie einen SPAN-Port auf einem Switch verwenden und der Switch dem SPAN-Port eine niedrigere Priorität zuweist, werden manche Pakete möglicherweise gelöscht.

Erste Schritte

Nachdem Sie das System eingerichtet haben, melden Sie sich mit folgenden Schritten bei IBM Security QRadar Packet Capture an:

1. Öffnen Sie einen Web-Browser und geben Sie folgende URL ein:
   `https://`*`PCAP-IP-Adresse`*`:41390`
2. Melden Sie sich mit den folgenden Benutzerkontoinformationen an:
   Benutzer: `continuum`
   Kennwort: `P@ck3t08..`

Fehlerbehebung: Wenn ein Benutzer innerhalb von 10 Minuten fünf Mal hintereinander ein falsches Kennwort eingibt, ist er für 30 Minuten vom System ausgesperrt. Von einem Systemadministrator kann das Benutzerkonto allerdings manuell entsperrt werden.

Standardmäßig wird die Seite **Erfassungsstatus** angezeigt. Mit den Optionen **Erfassung starten** und **Erfassung stoppen** können Sie Aufzeichnungen steuern.

Erfassungsstatus

Auf der Seite **Erfassungsstatus** werden die folgenden Informationen bereitgestellt:

- **Erfassungsschnittstelle**
- **Erfassungsstatus**
- **Start-/Stoppzeit**
- **Dauer der Systemerfassung**
- **Durchsatzrate**
- **Aufgezeichnete Pakete**
- **Aufgezeichnete Bytes**
- **Gelöschte Pakete**
- **Verfügbarer Speicherplatz**

In einer Clusterkonfiguration wird die Speichernutzung für jeden aktivierten Datenknoten angezeigt. Wenn der QRadar Packet Capture-Datenknoten aufgrund eines Netzkonfigurationsproblems oder einer falschen Verbindung nicht erreichbar ist, wird anstelle der Speicherstatistik die folgende Nachricht angezeigt: `Slave node`

`is enabled but is currently unreachable.` (Untergeordneter Knoten ist aktiviert, aber derzeit nicht erreichbar).

Fehlerbehebung

Klicken Sie auf **Troubleshooting** (Fehlerbehebung), um die Systeminformationen zu den konfigurierten Aufzeichnungsschnittstellen anzuzeigen.

Serverinformationen

Klicken Sie auf **Server information** (Serverinformationen), um Informationen zum Serverspeicher anzuzeigen.

Netzbeschreibung

Zeigen Sie den Durchsatz des Netzes im grafischen Format an.

Der standardmäßige maximale Durchsatz der Aufzeichnung auf Platte beträgt 10 Gb/s.

Erfassungsprotokoll

Zeigen Sie das Protokoll der Paketaufzeichnungen an, die ausgeführt wurden oder in Bearbeitung sind.

Inlinekomprimierung

Zur Unterstützung von Forensics-Prüfungen können Sie den unformatierten Paketinhalt länger behalten. Hierfür müssen Sie die verfügbare Kapazität des virtuellen Speichers ohne Hinzufügen physischer Platten erhöhen. Sie können jetzt mithilfe der neuen Option für die Inlinekomprimierung mehr Daten auf der QRadar Packet Capture-Appliance speichern.

Die Komprimierungsmenge hängt mit dem Umfang des komprimierten Videoinhalts in den Nutzdaten zusammen. Wenn Ihre Nutzdaten beispielsweise 5 Prozent komprimiertes Videomaterial enthalten, wird die Komprimierung 13:1 verwendet. Das Verhältnis Komprimierung:Speicher ist das Verhältnis zwischen der nicht komprimierten Größe und der komprimierten Größe.

Tabelle 1. Inlinekomprimierungsverhältnisse

Prozentsatz (%) der komprimierten Videonutzdaten	**Verstärkungsverhältnis Komprimierung:Speicher**
0	17:1
5	13:1
10	6:1
20	4:1
40	2,4:1

Zugehörige Konzepte:

Kapitel 1, „QRadar Packet Capture - Einführung”, auf Seite 1
IBM Security QRadar Packet Capture ist eine Anwendung zum Aufzeichnen und Durchsuchen von Netzverkehrsdaten. Die Anwendung QRadar Packet Capture verfügt nur über einen Erfassungsport (DNA0), an dem Sie einen 10G- oder einen 1G-SFP-Transceiver installieren können.

Zugehörige Tasks:

„QRadar Packet Capture-Serverzeit mit der Systemzeit der QRadar-Konsole synchronisieren" auf Seite 6

Um sicherzustellen, dass die Zeiteinstellungen von IBM Security QRadar-Implementierungen konsistent sind, sodass Suchläufe und Funktionen in Zusammenhang mit Daten ordnungsgemäß arbeiten, müssen alle Appliances mit der als QRadar-Konsole fungierenden Appliance synchronisiert werden. Ein Administrator muss iptables auf der Appliance mit der QRadar-Konsole aktualisieren und anschließend so konfigurieren, dass eine rdate-Kommunikation an Port 37 möglich ist.

Kapitel 4. Cluster

Die QRadar Packet Capture-Appliance kann als eigenständiger Einzelserver oder in einem Servercluster verwendet werden.

10G-Editionen unterstützen Cluster, die die Gesamtspeicherkapazität und die Rechenleistung gegenüber einem eigenständigen Einzelserver erhöhen. Cluster enthalten Hauptknoten, auch als Mastersysteme bezeichnet. An jedem dieser QRadar Packet Capture-Mastersysteme können Sie bis zu zwei QRadar Packet Capture-Datenknoten anschließen.

Die Registerkarte **Cluster** zeigt zwei Datenknoten mit deren aktuellen Status an.

Datenknoten sind jedoch standardmäßig eigenständig und nicht Teil eines Clusters. Deren Status lautet daher standardmäßig 'disabled' (inaktiviert).

Datenknoten aktivieren

Nachdem Sie eine physische Verbindung der IBM Security QRadar Packet Capture-Datenknoten mit dem QRadar Packet Capture-Hauptknoten hergestellt haben, müssen Sie die QRadar Packet Capture-Datenknoten aktivieren. Durch Aktivierung und Verbindung der QRadar Packet Capture-Datenknoten bilden Sie einen Cluster, der die Speicherkapazität und die Aufzeichnungsleistung gegenüber einem eigenständigen Einzelserver erhöht.

Weitere Informationen zum Verbinden der Appliances finden Sie in der *QRadar Packet Capture-Kurzübersicht*.

Vorbereitende Schritte

Vergewissern Sie sich, dass der Aufzeichnungsserver aktiv ist.

Vorgehensweise

1. Führen Sie zum Aktivieren der Datenknoten die folgenden Schritte aus:
   a. Wählen Sie auf der Registerkarte **Cluster** für jeden Datenknoten **Enable** (Aktivieren) aus. Der Status zeigt **Connected** (Verbunden) an.
   b. Starten Sie den Aufzeichnungsserver erneut. Die QRadar Packet Capture-Datenknoten sind jetzt aktiviert.

   Sobald die QRadar Packet Capture-Datenknoten verbunden sind und ausgeführt werden, wechselt ihr Status im Cluster in “connected” (Verbunden).

   Nachdem der Hauptknoten sich mit einem Datenknoten verbunden hat, schließt die komprimierte (virtuelle) Speichergröße, die auf dem Dashboard angezeigt wird, die Speichergröße der verbundenen Datenknoten ein.
2. Führen Sie zum Inaktivieren der Datenknoten die folgenden Schritte aus:
   a. Wählen Sie auf der Registerkarte **Cluster** für jeden Datenknoten **Disable** (Inaktivieren) aus. Der Status lautet nun **Disconnected** (Getrennt).
   b. Starten Sie den Aufzeichnungsserver erneut. Die QRadar Packet Capture-Datenknoten sind nun inaktiviert und nicht mehr mit dem Hauptknoten verbunden.

   Auf getrennten Datenknoten werden keine Daten mehr gespeichert.

Wenn auch der Hauptknoten inaktiviert ist, verringert sich die komprimierte (virtuelle) Speichergröße im Dashboard.

Wenn Datenknoten1 oder Datenknoten2 lizenziert ist, wird in der Lizenzspalte, je nach verwendeter Lizenz, **Permanent** oder **Evaluation** (Auswertung) angegeben.

Kapitel 5. QRadar Packet Capture-Diagramme

In IBM Security QRadar Packet Capture können Sie mittels Live- oder Langzeitdiagrammen Paketaufzeichnungsstatistiken visualisieren.

Live-Diagramm

Das Live-Diagramm erfasst die folgenden Statistiken zur aktuellen Paketaufzeichnung:

- Durchsatz in Gb/s (Gigabit pro Sekunde)
- Gesamtzahl der Pakete pro Sekunde
- TCP-Pakete pro Sekunde
- UDP-Pakete pro Sekunde
- Pakete pro Sekunde (Nicht-UDP-Datenverkehr)
- Anzahl der Systemereignisse
- Komprimierungsverhältnis der Pakete

Bewegen Sie den Mauszeiger über das Diagramm, um eine Statistik für diesen Diagrammpunkt anzuzeigen.

Wenn Sie auf einen Zeitpunkt im Diagramm klicken, wird die zugehörige Suchanforderung automatisch generiert. Außerdem können Sie über die Symbole für die Anzeigestile die Diagrammansicht ändern.

Langzeitdiagramm

Das Langzeitdiagramm gibt Ihnen einen Überblick über die Paketaufzeichnungsstatistiken über einen längeren Zeitraum. Sie können beispielsweise eine Statistik der letzten Stunde, des letzten Tages oder der letzten Woche anzeigen.

Bewegen Sie den Mauszeiger über das Diagramm, um eine Statistik für diesen Diagrammpunkt anzuzeigen.

Klicken Sie auf einen Zeitpunkt im Diagramm, um die zugehörige Suchanforderung automatisch zu generieren.

Kapitel 6. Pakete zu Diagnosetests innerhalb eines Zeitbereichs durchsuchen

Mit den während der Aufzeichnung erstellten Indexdaten wird eine Paketaufzeichnungsdatei (Packet Capture File, PCAP-Datei) erzeugt, in der die Pakete enthalten sind, die mit dem angegebenen Zeitbereich und den Metadateninformationen zu den Paketen übereinstimmen.

Einschränkung: Diese Suchvorgänge dienen nur zu Diagnosezwecken. Es ist eine manuelle Bereinigung erforderlich, um das Füllen der Partition für den Auszug zu vermeiden.

Vorgehensweise

1. Klicken Sie auf die Seite **Search** (Durchsuchen).

   Es sind bereits Standardwerte eingegeben.
2. Wählen Sie die Schnittstelle für den aufgezeichneten Datenverkehr aus, den Sie durchsuchen möchten.

   Wenn nur eine einzige Schnittstellenkonfiguration vorhanden ist, wird diese automatisch ausgewählt.
3. Geben Sie einen Wert an oder ändern Sie die Standardwerte für den Start- und den Endzeitpunkt des Zeitbereichs, der durchsucht werden soll.
4. Geben Sie einen Berkeley Packet Filter (BPF) an.

   Verwenden Sie die BPF-Syntax, um BPF-Filter anzugeben. Ein Ausdruck besteht aus mindestens einem Basiselement. Komplexe Filterausdrücke werden mithilfe der Operatoren AND, OR und NOT erstellt.

   Bei diesen Beispielen handelt es sich um Basisfilter:

   ```
   ether host 00:11:22:33:44:55
   ether src host 00:11:22:33:44:55

   ip host 192.168.0.1
   ip dst host 192.168.0.1

   ip6 host 2001:0db8:85a3:0042:0000:8a2e:0371:7334
   ip6 src host 2001:0db8:85a3:0042:0000:8a2e:0371:7334

   ip net 192.168.1.0/24
   ip src net 192.168.1

   port 80
   udp port 9000
   tcp src port 80
   ```

   Bei diesen Beispielen handelt es sich um komplexe Filter:

   ```
   ip host 192.168.1.1 and 192.168.1.2
   ip src 192.168.1.1 and dst 192.168.1.2
   ip host 192.168.1.1 and tcp port (80 or 443)
   (ip host 192.168.1.1 or 192.168.1.2) and (port 80 or 443)
   ```
5. Geben Sie die Anzahl der Pakete an, die extrahiert werden sollen.

   Die standardmäßige maximale Anzahl von zu extrahierenden Paketen ist 10.000. Wenn Sie die Anzahl in 0 ändern, werden alle Pakete extrahiert, die mit dem Zeitplan und dem Filter übereinstimmen.
6. Klicken Sie auf **Start Search** (Suche starten).

7. Verwenden Sie in der Spalte **Action** (Aktion) der Suchseite die Option **Chunking**, um Suchanforderungen in kleinere Datensegmente aufzuteilen, sodass Sie auf die Ergebnisse zugreifen können, während noch ein Teil der Suchanforderung ausgeführt wird. Eine Suche fordern Sie an, indem Sie die PCAP-Dateinummer angeben und dann auf **Download PCAP File** (PCAP-Datei herunterladen) klicken.

   Datensegmente sind 128 MB groß und das letzte Datensegment kann eine beliebige Größe kleiner als 128 MB haben.
8. Um den Status der Suchwarteschlange zu sehen, zeigen Sie die **Search request queue** (Suchanforderungswarteschlange) an.
9. Um ein Protokoll aller abgeschlossenen Suchvorgänge zu sehen, zeigen Sie das **Request log** (Anforderungsprotokoll) an.
10. Bereinigen Sie die Suchvorgänge manuell, damit ausreichend Speicherbereich für die Prozesse der Forensics-Wiederherstellung vorhanden ist:
    a. Melden Sie sich als Rootbenutzer an.

       Benutzername: root

       Kennwort: P@ck3t08..
    b. Führen Sie den folgenden Befehl aus:

       `rm -r /extraction/<Name_der_Suche>`

       Bei der Variablen <*Name_der_Suche*> handelt es sich um die Namensspalte auf der Seite **Completed Searches** (Abgeschlossene Suchvorgänge).

Kapitel 7. Aufzeichnungsfilter konfigurieren

Aufzeichnungsfilter filtern den Netzverkehr, bevor die erfassten Daten auf die Platte geschrieben werden.

Vorgehensweise

1. Erstellen Sie einen Aufzeichnungsfilter.
   a. Klicken Sie auf das Menü **Pre capture filter** (Aufzeichnungsfilter).
   b. Geben Sie die Einstellungen für den Filternamen und den Suchfilter ein.

      Ein Aufzeichnungsfilter besteht aus primitiven Ausdrücken, die durch Konjunktionen (and/or) verbunden sind und denen optional ein 'not' vorangestellt ist.

      Im folgenden Beispiel wird sämtlicher Datenverkehr für Port 80 ausgefiltert:

      ```
      not dst port 80
      ```

      Im folgenden Beispiel wird nur der Datenverkehr für die beiden angegebenen Hosts aufgezeichnet; der restliche Datenverkehr wird ausgefiltert:

      ```
      host 1.2.3.4 or host 1.1.1.1
      ```

   c. Speichern Sie den Aufzeichnungsfilter, indem Sie auf **Add** (Hinzufügen) klicken. Der zuletzt hinzugefügte Aufzeichnungsfilter ist der aktive Filter. Darüber hinaus wird der Verlauf aller bisherigen Filter angezeigt.
2. Starten Sie den Aufzeichnungsserver erneut, damit der neu hinzugefügte Filter wirksam wird.
3. Mit **Delete** (Löschen) können Sie einen Aufzeichnungsfilter permanent löschen. Danach müssen Sie den Aufzeichnungsserver erneut starten.

Kapitel 8. Aktive Auslöser konfigurieren

Durch aktive Auslöser werden Sie bei bestimmten im Netz eintretenden Ereignissen gewarnt. Beispielsweise können Sie als Suchfilter eine IP-Adresse eingeben, damit Sie eine Warnung erhalten, wenn Datenverkehr mit dieser IP-Adresse aufgezeichnet wird.

Vorgehensweise

1. Erstellen Sie einen aktiven Auslöser.
   a. Klicken Sie auf das Menü **Active Trigger** (Aktiver Auslöser).
   b. Geben Sie die Einstellungen für den Auslösernamen und den Zeitrahmen ein.
   c. Speichern Sie den aktiven Auslöser, indem Sie auf **Add** (Hinzufügen) klicken.

   Einschränkung: Sie können bis zu fünf aktive Auslöser festlegen.
2. Die eingetretenen Auslöserereignisse können Sie im **Ereignisprotokoll** überprüfen. Wenn Sie auf ein aktives Auslöserereignis klicken, wird automatisch eine Suchanforderung für den festgelegten Zeitrahmen um das Auslöserereignis herum generiert. Dieses Suchzeitfenster beinhaltet (in Sekunden) sowohl die Zeit vor als auch die Zeit nach dem Ereignis.
3. Mit **Delete** (Löschen) können Sie ein konfiguriertes Auslöserereignis löschen.

Kapitel 9. Fehlersuche bei QRadar Packet Capture-Problemen

Die Fehlersuche ist ein systematischer Ansatz für die Lösung eines Problems. Das Ziel der Fehlersuche besteht darin, zu ermitteln, warum etwas nicht erwartungsgemäß funktioniert, und zu erklären, wie das Problem gelöst werden kann.

Ist die neueste Version der QRadar Packet Capture-Software installiert?

Führen Sie stets eine Aktualisierung auf die neueste Releaseversion der Software durch. Stellen Sie sicher, dass nach einem Software-Update oder einer Neuinstallation das System erneut gestartet wird, sodass die Änderungen wirksam werden. Stellen Sie weiter sicher, dass in Clusterkonfigurationen das Mastersystem sowie alle Datenknotensysteme auf dieselbe Version aktualisiert werden.

Steht Ihnen die empfohlene Firmware für den RAID-Controller und die Festplattenlaufwerke zur Verfügung?

Falls Zuverlässigkeits- oder Leistungsprobleme im Zusammenhang mit der Firmwareversion auftreten, die auf dem 3650 M4-RAID-Controller und den Festplattenlaufwerken installiert ist, stellen Sie sicher, dass Sie über die Mindestfirmwareversionen verfügen:

- Für den 3650 M4 ist dies die M5200-RAID-Controller-Firmwareversion 24.7.0-0052 vom 27. Mai 2015 oder neuer.

  Führen Sie die `.bin`-Dateien von der Red Hat Linux-Befehlszeile aus.
- Für IBM Lenovo ist dies die Version vom 15. Mai 2015 oder neuer.

  Führen Sie die `.bin`-Dateien von der Red Hat Linux-Befehlszeile aus.

Ist HyperThreading im BIOS aktiviert?

HyperThreading ist im BIOS standardmäßig aktiviert. Führen Sie den Befehl `lscpu` aus und vergewissern Sie sich in dessen Ausgabe, dass pro Kern zwei Threads festgelegt sind. Hier eine Beispielausgabe des Befehls für IBM 3650 M4:

```
[root@3650M4-001 bin]# lscpu
Architecture:          x86_64
CPU op-mode(s):        32-bit, 64-bit
Byte Order:            Little Endian
CPU(s):                40
On-line CPU(s) list:   0-39
Thread(s) per core:    2
Core(s) per socket:    10
Socket(s):             2
NUMA node(s):          2
Vendor ID:             GenuineIntel
CPU family:            6
Model:                 62
Stepping:              4
CPU MHz:               2800.000
BogoMIPS:              5592.04
Virtualization:        VT-x
L1d cache:             32K
L1i cache:             32K
L2 cache:              256K
L3 cache:              25600K
NUMA node0 CPU(s):     0-9,20-29
NUMA node1 CPU(s):     10-19,30-39
```

Ist der Erfassungsport ordnungsgemäß angeschlossen?

Die IBM Security QRadar Packet Capture-Einheit kann nur an der Schnittstelle 0 Erfassungen durchführen.

Ist die Ethernet-Netzverbindung ordnungsgemäß konfiguriert?

Um sicherzustellen, dass eine Ethernet-Schnittstelle einer IP-Adresse zugewiesen ist, führen Sie den Befehl `ifconfig` für die verbundene Schnittstelle aus.

Wenn keine Adresse konfiguriert ist, bearbeiten Sie die entsprechende Datei `ifcfg-eth*`, um eine Adresse zu konfigurieren.

- In diesem DHCP-Beispiel müssen Sie die folgenden Einstellungen in `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`* bearbeiten und *eth2* durch die entsprechende Einstellung ersetzen.

  ```
  BOOTPROTO="dhcp"
  NM_CONTROLLED="no"
  ONBOOT="yes"
  ```

- In diesem Beispiel für eine statische IP-Adresse müssen Sie die folgenden Einstellungen in `/etc/sysconfig/network-scripts/ifcfg-`*`eth2`* bearbeiten und *eth2* durch die entsprechende Einstellung ersetzen.

  ```
  BOOTPROTO="static"
  BROADCAST="192.168.1.255"
  DNS1="0.0.0.0"
  DNS2="0.0.0.0"
  GATEWAY="192.168.1.2"
  IPADDR="192.168.1.1"
  NETMASK="255.255.255.0"
  NM_CONTROLLED="no"
  ONBOOT="yes
  ```

Führen Sie nach Ihrer Änderung der Einstellungen den Befehl `ifconfig` aus, um die Netzschnittstelle zu konfigurieren.

Ist die Systemzeit ordnungsgemäß konfiguriert?

Die Systemzeit ist standardmäßig auf die koordinierte Weltzeit (UTC) eingestellt. Sie ist so konfiguriert, dass Network Time Protocol (NTP) verwendet wird und öffentliche Server die richtige Systemzeit beibehalten.

Bestehen Hardwareprobleme auf dem System?

1. Stellen Sie sicher, dass der Datenverkehr ordnungsgemäß generiert und von der Netzschnittstellenkarte (Network Interface Card, NIC) empfangen wird.

   Überprüfen Sie die Leuchtanzeigen direkt rechts neben dem Anschluss der Schnittstelle 0. Die unterste Leuchtanzeige muss dauerhaft leuchten, da dies auf eine Verbindung hinweist. Die oberste Leuchtanzeige muss blinken, da dies auf eine Datenverkehrsaktivität hinweist.

2. Führen Sie den Befehl `/usr/local/nc/bin/dpdk_nic_bind.py –status` aus.

   Das Ergebnis des Befehls muss ungefähr der folgenden Ausgabe entsprechen:

   ```
   Network devices using DPDK-compatible driver
   ============================================
   0000:0f:00.0 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
   unused=ixgbe
   0000:0f:00.1 '82599ES 10-Gigabit SFI/SFP+ Network Connection' drv=igb_uio
   unused=ixgbe
   Network devices using kernel driver
   ===================================
   0000:07:00.0 'I350 Gigabit Network Connection' if=eth2 drv=igb unused=igb_uio
   *Active*
   0000:07:00.1 'I350 Gigabit Network Connection' if=eth3 drv=igb unused=igb_uio
   0000:07:00.2 'I350 Gigabit Network Connection' if=eth4 drv=igb unused=igb_uio
   Other network devices
   =====================
   <none>
   ```

Erfasst das System den Datenverkehr?

Mit einer der folgenden Methoden können Sie prüfen, ob das System nach dem Start einer Erfassungssitzung tatsächlich Datenverkehr erfasst:

- Überprüfen Sie die Leuchtanzeigen direkt rechts neben dem Anschluss der Schnittstelle 0. Die oberste Leuchtanzeige muss blinken, da dies auf eine Datenverkehrsaktivität hinweist.
- Auf der Seite **Network Characterization** (Netzbeschreibung) sehen Sie die grafische Ausgabe.
- Führen Sie in der Befehlszeile den Befehl `du –h /storage0/int0` aus.

  Das Ergebnis ähnelt der folgenden Ausgabe:

  ```
  4.4G /storage0/int0/1_0
  4.9G /storage0/int0/2_0
  6.4G /storage0/int0/3_0
  4.9G /storage0/int0/4_0
  4.9G /storage0/int0/5_0
  4.9G /storage0/int0/6_0
  .
  .
  .
  1.4T /storage0/int0/
  ```

  Wenn Sie diesen Befehl wiederholt ausführen, erhöhen sich die zurückgegebene Anzahl der Unterverzeichnisse und der Wert für die Reservierungsmenge.

Ist der QRadar Packet Capture-Datenknoten aktiviert?

Wenn der QRadar Packet Capture-Datenknoten physisch mit dem Masterknoten verbunden ist, müssen Sie auch sicherstellen, dass er in der Benutzerschnittstelle für die Arbeit mit dem Master-Server aktiviert ist. Das System unterstützt zurzeit bis zu zwei QRadar Packet Capture-Datenknoten.

Wenn auf der Registerkarte **Cluster** angezeigt wird, dass die QRadar Packet Capture-Datenknoten verbunden und aktiviert sind, und in der Anzeige **Update Node(n) License** (Knoten(n)-Lizenz aktualisieren) auf der Registerkarte **Admin** die Einstellung **System ID** fehlt, müssen Sie sicherstellen, dass auf dem betreffenden QRadar Packet Capture-Datenknoten die gleiche Version der QRadar Packet Capture-Datenknotensoftware installiert ist wie auf dem Master-Knoten. Stellen Sie sicher, dass diese Anforderung auch nach der Aktualisierung auf die neueste Softwareversion erfüllt wird.

Führen Sie als Benutzer `root` folgenden Befehl aus, um die Softwareversion zu überprüfen, die auf dem QRadar Packet Capture-Datenknoten und -Master-Knoten installiert ist:

```
cat /root/version.txt
```

Die Softwareversion des QRadar Packet Capture-Datenknotens muss dieselbe sein wie die auf dem Master-Knoten installierte Version.

Wie wird eine Lizenz für den QRadar Packet Capture-Datenknoten über die Befehlszeile angewendet?

Führen Sie als Benutzer `root` folgenden Befehl aus, um sicherzustellen, dass Sie sich im QRadar Packet Capture-Datenknoten befinden:

```
cat /root/version.txt
```

Überprüfen Sie, ob Sie mit dem QRadar Packet Capture-Datenknoten verbunden sind, indem Sie nach einem D suchen, das an das Ende der Versionsnummer angehängt ist, z. B. 7.2.7.256D.

Führen Sie als Benutzer `root` folgendes Script aus, um die Lizenz auf den QRadar Packet Capture-Datenknoten anzuwenden: `nc_set_license.sh`.

Hinweise:

- Damit die neue Lizenz wirksam wird, müssen Sie den QRadar Packet Capture-Datenknoten erneut starten.
- Wenn der QRadar Packet Capture-Datenknoten bereits zum Zeitpunkt der Fertigung lizenziert wurde, müssen Sie das Script nicht ausführen. Die Lizenz wird wirksam, sobald das System gestartet wird.

Falls die angewendete Lizenz ungültig ist, wird folgende Fehlernachricht angezeigt:

`Warning: LicenseKey is *NOT* valid.` (Warnung: Lizenzschlüssel *NICHT* gültig.)

Was ist das Protokollierungsformat LEEF 2.0?

Die LEEF-Nachrichten (Log Event Extended Format) werden in folgendem Format zur Datei `/var/log/messages` hinzugefügt:

```
<Datum/Zeit> <Server-IP> LEEF: 2.0|IBM|QRadar Packet
Capture|7.2.7.256|<ID>|cat=<Kategorie> msg=<Nachricht>
```

Wird beispielsweise der Paketaufzeichnungsserver auf einem System mit der IP-Adresse 10.91.170.20 gestartet, wird folgende LEEF-Nachricht zur Datei `/var/log/messages` hinzugefügt:

```
May 24 22:27:49 IP_10_91_170_20 LEEF: 2.0|IBM|QRadar Packet
Capture|7.2.7.256|Started|cat=PacketCapture
```

Warum gibt die Anforderung Create Search (Suche erstellen) einen `NoSpace`-Fehler zurück?

Wenn Sie eine Suche erstellen und das Verzeichnis `/extraction` voll ist, gibt der Server den Fehler `NoSpace` (Kein Speicherplatz) zurück.

Was passiert beim Anhalten einer Suche?

Eine Suche wird angehalten, wenn der belegte Speicherplatz im Verzeichnis `/extraction` die Größe von 6,7 GB überschreitet. Es wird eine LEEF-Nachricht an `Syslog` gesendet mit der Information, dass die Suche angehalten wurde. Im Ereignisprotokoll wird eine Warnung wie die folgende angezeigt:

`!WARNING: Extraction Storage Full! Search cannot proceed!!` (Warnung: Extraktionsspeicher voll! Suche kann nicht fortgesetzt werden!!)

Um sicherzustellen, dass eine angehaltene Suche wiederaufgenommen wird, müssen Sie Speicherplatz freigeben, indem Sie ältere, bereits beendete Suchen löschen. Gehen Sie zum Löschen einer alten Suche wie folgt vor:

1. Klicken Sie im Hauptmenü auf **Suche**.
2. Löschen Sie im Rahmen **Search Request Log** (Suchanforderungsprotokoll) ältere Suchen, indem Sie auf **Delete Search** (Suche löschen) klicken.

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 Produkte, Programme oder Services 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 Leistungsdaten und Kundenbeispiele dienen allein der Veranschaulichung. Die tatsächliche Leistung ist 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 und Absichten von IBM unterliegen Änderungen oder können zurückgenommen werden und repräsentieren nur die Ziele von IBM.

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

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

Marken

IBM, das IBM Logo und ibm.com sind Marken oder eingetragene Marken der International Business Machines Corp. in den USA und/oder anderen Ländern. Weitere Produkt- und 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.

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

Nutzungsbedingungen 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 Rechten 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 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 implementiert wurden, ist es möglich, dass dieses Softwareangebot Sitzungscookies zum Erfassen der Sitzungs-IDs einzelner Benutzer für die Sitzungsverwaltung und die Authentifizierung verwendet. 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 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 unter "IBM Software Products and Software-as-a-Service Privacy Statement" (http://www.ibm.com/software/info/product-privacy).

Gedruckt in Deutschland