IBM QRadar
Version 7.3.2

Common Criteria for NIAP
Revision 1.4

Note

Before you use this information and the product that it supports, read the information in “Notices” on page 37.

Product information

This document applies to IBM® QRadar® Security Intelligence Platform V7.3.2 and subsequent releases unless superseded by an updated version of this document.

Contents

About this guide

This documentation includes the requirements and procedures for configuring Common Criteria on IBM QRadar.

Intended audience

The intended audience for this guide is:

- System administrators or developers who are configuring Common Criteria for IBM QRadar.
- NIAP certification personnel who are configuring and testing Common Criteria for IBM QRadar.

Technical documentation

To find IBM Security QRadar product documentation in the QRadar products library, see Accessing IBM Security Documentation Technical Note (www.ibm.com/support/docview.wss?rs=0&uid=swg21614644).

Contacting customer support

For information about contacting customer support, see QRadar Support – Assistance 101 (https://ibm.biz/qradarsupport).

Statement of good security practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Please Note:

Use of this Program may implicate various laws or regulations, including those related to privacy, data protection, employment, and electronic communications and storage. IBM QRadar may be used only for lawful purposes and in a lawful manner. Customer agrees to use this Program pursuant to, and assumes all responsibility for complying with, applicable laws, regulations and policies. Licensee represents that it will obtain or has obtained any consents, permissions, or licenses required to enable its lawful use of IBM QRadar.

Document control

The following table shows updates that were made to the *IBM QRadar V7.3.2 Common Criteria for NIAP* documentation.

Date	Revision	Updates
October 29, 2019	1.0	Initial version with document control.
November 19, 2019	1.1	The following topics are new: • *Logging out of QRadar* • *Configuring the DH parameters for Apache server* • *Configuring the inactivity time period* • *Configuring the local session timeout period* The following topics were updated: • *Configuration of Common Criteria on a QRadar All-in-one system* • *Logging in to QRadar* • *Configuring Java TLS ciphers* • *Verifying the event forwarding configuration* • *Configuring the password policy* • *QRadar self-test* • *Verifying secure updates*
December 9, 2019	1.2	The following topics were updated: • *Supported cipher suites* • *Limiting the cipher suites in use* The following topic was removed: • *Configuring the DH parameters for Apache server*
January 6, 2020	1.3	The following topics were added: • *Viewing the audit logs* The following topics were updated: • *Editing scripts to configure QRadar in STIG environments* • *Verifying secure updates*
January 20, 2020	1.4	The following topics were updated: • *Editing scripts to configure QRadar in STIG environments*

Chapter 1. Configuration of Common Criteria on a QRadar All-in-one system

The common criteria guide for IBM QRadar provides requirements and procedures for configuring Common Criteria by using prescribed NIAP methodology on a QRadar All-in-One system. The QRadar All-in-One system is a network device that detects potential threats through the review of event data and flow data that is collected from network sources.

What product is being evaluated?

The evaluated product is a QRadar 3129 (All-in-One) device that runs IBM QRadar SIEM.

The software identification for the evaluated product is IBM QRadar SIEM V7.3.2 NIAP.

QRadar consolidates log source event data from device endpoints and applications that are distributed throughout a network. QRadar performs normalization and correlation activities on this raw data and can forward data to another network server when event forwarding is configured. Communication with network peers for either inbound or outbound log event data is accomplished by using TLS protected communication channels. QRadar can authenticate inbound peers by using X.509v3 certificates, or by providing an X.509v3 certificate to authenticate itself as part of an outbound TLS connection.

The QRadar All-in-One is the Target of Evaluation (TOE). The TOE can be administered either locally or remotely. The QRadar product consolidates log source event data from multiple devices, endpoints, and applications distributed throughout a network.

NDcPP requirements

The following features are required for QRadar to satisfy NDcPP (Network Device Collaborative Protection Profile) requirements:

- Certificate Revocation is required for all certificates that are used by QRadar.
- TLS protection is needed for inbound and outbound audit or event log transmissions.
- QRadar must offer and demand X.509 certificate authentication for TLS protected communications.
- QRadar must be able to configure specific cryptographic cipher suites that are used with all TLS protected communications.
- QRadar must accept TLS connections only by using TLS version 1.1 or higher.
- QRadar must use a strong entropy source such as Jitter or HAVEGED.
- QRadar must have Cryptographic Algorithm Validation Program (CAVP) certificates for all cryptographic algorithms that are claimed in the security target (ST).

QRadar and Common Criteria acronyms

Several acronyms are used in this guide.

Acronyms

The following table lists the acronyms that are used in this guide.

Table 1. QRadar and Common Criteria acronyms

Acronym	Description
CC	Common Criteria
CCEVS	Common Criteria Evaluation and Validation Scheme

Table 1. QRadar and Common Criteria acronyms (continued)

Acronym	Description
EC	Event Collector
EP	Event Processor
NIAP	National Information Assurance Partnership
NTP	Network Time Protocol
TOE	Target of evaluation
TSF	TOE Security Functionality

Evaluated capabilities

An IBM QRadar All-in-One appliance is a single appliance that includes complete data collection, data processing, storage, monitoring, searching, reporting, and offense management capabilities. The appliance collects event and flow data from log sources in your network, then processes and stores the data, and makes it available for security monitoring and threat analysis.

The Common Criteria configuration adds support for security capabilities, such as protected transport of event audit data and secure communication by using TLS 1.1 or higher.

Supported cipher suites

During the STIG hardening, QRadar is configured to use TLS protocol version 1.1 and 1.2 and to use the supported cipher suites.

Before you evaluate QRadar in a test environment, we recommend that you configure TLS to support only the ciphers that are required to complete the evaluation.

The following TLS cipher suites are supported:

- TLS_RSA_WITH_AES_128_CBC_SHA

  This is the mandatory cipher.
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256

Chapter 2. QRadar installations for highly secure environments

This document provides guidance for implementing security standards for IBM QRadar deployments in highly secure environments, such as the federal government. These security standards meet the requirements set by the Defense Information Systems Agency (DISA).

Hardening of the operating system and QRadar hosts to implement the Security Technical Implementation Guide (STIG) standards is part of making QRadar deployments more secure. Some of the steps that are required to secure a QRadar deployment are not specified in the Red Hat Enterprise Linux STIG documents.

To configure the Target of Evaluation (TOE) machine into the common criteria evaluated configuration, you must complete the following steps:

1. Install the QRadar software.

   The STIG hardening scripts are included in the installation.
2. Create a non-root user.
3. Run the hardening script on the QRadar console.
4. Edit the QRadar configuration.
5. Modify the GRUB2 boot loader configuration.
6. Reboot the appliance and log in.

Installing QRadar in a STIG environment

Set up the Target of Evaluation (TOE) machine by installing QRadar on a IBM QRadar 3128-C (All-in-One) appliance.

Before you begin

Ensure that the following requirements are met:

- The required hardware is installed.
- A keyboard and monitor are connected by using the VGA connection.
- You have the required license key for your appliance. The temporary license key is good for 5 weeks.

Procedure

1. Install QRadar by following the steps in the *IBM QRadar Installation Guide*.

   Note: Select **Console All-in-One** as the appliance type.

   You can also watch this video to learn how to perform a clean install of IBM QRadar.
2. Configure the QRadar Console root user timeout by adding the following line in the `etc/profile` file:

```
[ $UID -eq 0 ] && TMOUT=600
```

What to do next

Create a non-root user.

Creating a non-root user in a STIG-compliant environment

You can't log in remotely as the root user in a STIG-compliant environment.

Create a non-root user who has **sudo** access and choose a non-root user name such as *stiguser*.

Procedure

1. To create the non-root user, type the following commands:

```
useradd -c 'Admin User' -d /home/stiguser -m -s /bin/bash stiguser
```

```
passwd stiguser
```

   The password must follow these guidelines:

   - Consist of 15 or more characters.
   - Not repeat the same character consecutively more than two times.
   - Not repeat the same character type consecutively more than two times.
   - Have at least one uppercase character.
   - Have at least one numerical character.
   - Have at least one special character.

   Tip: These new password requirements are enforced when the STIG script is run. If your root password doesn't meet these requirements, you can change it now.

2. Edit the `/etc/sudoers` file.
   a) At the end of the file, type the following line:

      `stiguser ALL=(ALL) ALL`

      Note: It is conventional to use tabs for white space but it's not a requirement; for example:

      `stiguser ALL=(ALL) ALL`

   b) Use the *#* symbol to comment out any lines that contain `NOPASSWD`.

      Tip: If you use the Vim text editor, type **`:/NOPASSWD`** in command mode to search for any instances of `NOPASSWD`.

3. Verify that the new user can log in from a remote host and use the **sudo** command to become a root user.

   For example, use an SSH client such as PuTTY to log in to IBM QRadar as *stiguser*, and then run a command by using **sudo**.

```
sudo cat /etc/shadow
```

What to do next

Run the hardening script on the QRadar console.

Running the hardening script on the Console

To help secure the system, you must run hardening scripts on the IBM QRadar Console.

Before you begin

Before you run the hardening script, verify that the *stiguser* can log in remotely.

Procedure

1. Go to the STIG directory by typing the following command:

   ```
   cd /opt/qradar/util/stig/bin
   ```

2. Run the STIG hardening script by typing the following command:

   ```
   ./stig_harden.sh -h
   ```

   Type `yes` at the following prompt: **Do you want to continue (yes/no)?**

   Note: You must run the script only once.

3. Restart the QRadar appliance.
4. While you are logged in as an administrator, verify that the `stiguser` can log in remotely at the same time that you (as administrator) are logged in as a root user.

   Change the root user's password to meet the password requirements. Ensure that the root authentication works locally.

What to do next

Edit the QRadar configuration.

Editing scripts to configure QRadar in STIG environments

Extra configuration tasks, such as configuring the mail server, disabling the DHCP client, updating iptables, and changing the backup log directory location are required when you configure QRadar in STIG environments.

Procedure

1. To ensure that the mail server on each host is listening on local interfaces.
   a) Make a backup copy of the `/etc/postfix/main.cf` file.
   b) Edit the `/etc/postfix/main.cf` file and verify that the `inet_interfaces` line is similar to one of the following examples:
      - `inet_interfaces = localhost`.
      - `inet_interfaces = loopback-only`.
2. Verify that the **BOOTPROTO** parameter is set to **none** or **`static`** in the configuration files.
   a) Type the following command:

      ```
      grep –rl BOOTPROTO /etc/sysconfig/network-scripts/ifcfg*
      ```

   b) For each interface configuration file that is returned, where **BOOTPROTO** does not equal **none** or **`static`**, change the **BOOTPROTO** value to **none**.

      Example:

      ```
      DEVICE=eth0
      ONBOOT=yes
      BOOTPROTO=none
      IPADDR=192.168.122.254
      IPADDR=192.168.122.254
      ```

3. Change `IPtables` and set the default INPUT policy to *DROP*.
   a) Make a backup copy of the `/opt/qradar/bin/iptables_update.pl` file.
   b) Edit the `/opt/qradar/bin/iptables_update.pl` file and change `INPUT ACCEPT [0:0]` to `INPUT DROP [0:0]`.
   c) Run the `/opt/qradar/bin/iptables_update.pl` script.
4. Add the following line to the `/etc/hosts.allow` file on the QRadar Console:

```
time: ALL
```

5. Change the backup log directory.
   a) Search for the `/var/log/backup.log` log file and if it exists, move the file to `/store/LOGS`.

      Note: The `/var/log/backup.log` does not exist on a fresh installation.

   b) Make a backup copy of the `/opt/qradar/bin/backup.sh` file.
   c) Edit the `/opt/qradar/bin/backup.sh` file and change this text:

```
InitLog @syslog:local1.info || ErrorExit 'Failed to initialize logging'
```

      To this text:

```
InitLog /store/LOGS/$(basename ${0} .sh).log || ErrorExit 'Failed to initialize logging'
```

6. Create an AIDE baseline and schedule integrity checks. Then, after you make the configuration changes, perform aide updates.
   a) As root user, initialize the AIDE database by typing the following command:

```
aide --init
mv -f /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

   b) To reduce the system startup time, schedule the AIDE integration check to run at daily intervals. For example, to schedule the AIDE checks to run at 4:20 AM every day, log in as the root user and edit `/etc/crontab` by adding `20 4 * * * root /usr/sbin/aide --check`.

      Scheduling daily interval checking ensures that the checks are run more frequently. The administrator can change the schedule later if a different time period or interval is required.

   c) To view the scheduled AIDE output, type the following command:

```
sudo less /var/log/aide/aide.log
```

      If there are unapproved changes, the system might be compromised. The administrator should perform a factory installation. For more information, see Chapter 2, “QRadar installations for highly secure environments,” on page 3.

   d) After reviewing the changes, create a new baseline:

```
aide --update
mv -f /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

   e) Run the aide update after you install, uninstall, change the system configuration, or run a QRadar deployment action.

```
aide --update
mv -f /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

What to do next

Modify the GRUB2 boot loader configuration.

Changing the boot loader configuration

You must update the GRUB2 configuration to configure the non-root user for the STIG environment, and for the changes that were made by the hardening script to be effective. You must update the GRUB2 configuration on the QRadar Console, event processors, and flow processors.

Procedure

1. Make a backup of the following GRUB2 configuration folders:

- /etc/grub.d
- /etc/default/grub
- /boot/grub2

2. Enter the following command to back up the GRUB 2 configuration files:

   ```
   tar -cvf /root/grub2backup.tar /etc/grub.d /etc/default/grub /boot/grub2
   ```

3. Run the following script to generate a password hash for the boot loader.

   ```
   grub2-mkpasswd-pbkdf2
   ```

   The generated hash value might look similar to the following example. Take note of it because you will need to use it later.

   ```
   grub.pbkdf2.sha512.10000.51A734C16CD93009EED3814937CCBABAF
   70256B5EB67BE6B6D96138A110B3092722248605923588F143375E09149520ADE32
   5EB4791DA08C74F0E48A2A1CD3F8.D1B528BD41790DAFF9479A511FD95EF03B4F4A
   583EF6DA53AA2DFE10941A028F15AA9ADEEEE0E3398F5734516655820C836BBBA86
   5911282D326C5B7EA2FEC1A
   ```

   Tip: If you complete this step remotely by using the *stiguser* user account, you can copy the generated hash value so that you can paste it later.

4. Edit or create the /etc/grub.d/01_users file that contains a user name and the password hash.

   For example, the file might look similar to the following code snippet. The line that starts with grub.pbkdf2 is one continuous line.

   ```
   set superusers= stiguser>
   password_pbkdf2  stiguser>
   grub.pbkdf2.sha512.
   10000.19074739ED80F115963D984BDCB35AA671C24325755377C3
   E9B014D862DA6ACC77BC110EED41822800A87FD3700C037320E51E9326188D53247EC0722
   DDF15FC.C56EC0738911AD86CEA55546139FEBC366A393DF9785A8F44D3E51BF09DB980BA
   FEF85281CBBC56778D8B19DC94833EA8342F7D73E3A1AA30B205091F1015A85
   ```

5. Edit the /boot/grub2/grub.cfg file.

   a) Locate the following line:

   ```
   ### END /etc/grub.d/00_header ###
   ```

   b) Using the following as an example, replace the text between label 1 and label 2 with the generated hash value from the earlier step.

   ```
   ### END /etc/grub.d/00_header ###
   set superusers=<stiguser>
   password_pbkdf2=<stiguser>
    1 grub.pbkdf2.sha512.10000.51A734C16CD93009EED3814937CCBABAF
   70256B5EB67BE6B6D96138A110B3092722248605923588F143375E09149520ADE32
   5EB4791DA08C74F0E48A2A1CD3F8.D1B528BD41790DAFF9479A511FD95EF03B4F4A
   583EF6DA53AA2DFE10941A028F15AA9ADEEEE0E3398F5734516655820C836BBBA86
   5911282D326C5B7EA2FEC1A 2
   ### BEGIN /etc/grub.d/10_linux ###
   ```

   c) Edit every line that begins with menuentry so that --class os is followed by --users stiguser.

   For example, the menuentry might look similar to this:

   ```
   ### BEGIN /etc/grub.d/10_linux
   ### menuentry 'Red Hat Enterprise Linux Server'
   --class gnu-linux --class gnu --class os --users stiguser
   $menuentry_id_option 'gnulinux-simple-f804409d-9e87-4e19-a321-a26b55a66fd9'
   { load_video set gfxpayload=keep
   ```

   Tip: If you use the Vim text editor, type **:/menuentry** to search for any instances of menuentry.

   Note: If --class os is followed by --unrestricted, replace --unrestricted with --users *stiguser*.

6. Optional: The following command is used to update the GRUB 2 configuration.

   `grub2-mkconfig -o /boot/grub2/grub.cfg`

   Note: If you use this command to update `grub.cfg`, then you need to repeat the previous steps to restore password protection.
7. Type the following commands to set read and write permissions for the listed files:
   - `chmod 600 /etc/grub.d/*`
   - `chmod 600 /etc/default/grub`

What to do next
Reboot the appliance and log in.

Logging in to QRadar

Only security administrators can login to the Target of Evaluation (TOE) system via its command line or Web GUI interfaces. This restricts access to all management functions, including management of X.509 certificates. To access the web interface on your IBM QRadar appliance, log in remotely using your web browser.

About this task

IBM QRadar is a web-based application. For the features to work properly, you must use a supported web browser.

Table 2. Supported web browsers for QRadar products

Web browser	Supported versions
64-bit Mozilla Firefox	45.8 Extended Support Release and later
64-bit Microsoft Internet Explorer with Microsoft Edge mode enabled.	11.0, Edge 38.14393 and later
64-bit Google Chrome	Latest

Procedure

1. In your browser window, type `https://<QRadar_IP_Address>`.

   To log in to QRadar in an IPv6 or mixed environment, wrap the IP address in square brackets: `https://[<QRadar_IP_Address>]`.
2. Type the log in credentials:
   - User name: admin
   - Password: *<Password that was created during the installation process>*

   The default license key provides you access to the system for 5 weeks.

   Note: To access the command-line interface on your IBM QRadar appliance, type the following command in a terminal on a remote system:

   `ssh stiguser@<QRadar_IP>`

Logging out of QRadar

To log out of the QRadar administrative session, follow these steps:

Procedure

1. To log out of the web interface, click the user icon in the top-right corner of the page, and then click **Log out**.
2. To log out of the remote SSH session, type `exit`.
3. To log out of the local session, type `logout`.

Chapter 3. Secure communication configuration

After you've hardened the QRadar system by using the STIG scripts, you must prepare for configuring TLS secure communication.

1. “Disabling auto updates for configuration files” on page 11.
2. Configure SSH to use public key authentication only.
3. Configure the SSHD_config file.
4. “Configuring Java TLS ciphers” on page 12.
5. Limit the cipher suites in use.

Disabling auto updates for configuration files

Configure QRadar so that it does not automatically apply updates to the configuration files.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration** > **Auto update**.
3. Click **Change settings**.
4. In the **Update types** section, under **Configuration updates**, change the **Update type** to **Disable**.

Configuring SSH to use public key authentication only

Configure SSH authentication on the IBM QRadar 3128-C (All-in-One) appliance to accept only public key authentication and RSA authentication.

Before you begin

On the remote computer that is used to connect to QRadar, locate the SSH public key. Copy the key to the `~/.ssh/authorized_keys` folder on the IBM QRadar 3128-C (All-in-One) appliance.

Procedure

1. At the command line on the QRadar 3128-C (All-in-One), edit the `sshd_config` file by typing the following command:

   ```
   vi /etc/ssh/sshd_config
   ```

2. Set `PubkeyAuthentication` to `Yes`.
3. Set `PasswordAuthentication` to `No`.
4. Restart SSHD by typing the following command:

   ```
   service sshd restart
   ```

Configuring the SSHD_config file

Edit the /etc/ssh/sshd_config file to control the ciphers that are available.

Procedure

1. In the /etc/ssh/sshd_config file, uncomment the HostKey line that references the RSA key. Leave the other HostKey lines commented out.

   Note: The supported TLS cipher suites include the sha-1 and sha-256 algorithms.

   The following example shows what the file looks like when you uncomment the HostKeys line that references the RSA key.

   ```
   # HostKey for protocol version 1
   ```

   ```
   # HostKey /etc/ssh/ssh_host_key
   ```

   ```
   # HostKeys for protocol version 2
   ```

   ```
     HostKey /etc/ssh/ssh_host_rsa_key
   ```

   ```
   # HostKey /etc/ssh/ssh_host_dsa_key
   ```

2. Replace the Ciphers aes128-ctr,aes192-ctr,aes256-ctr line near the bottom of the file with the following two lines:

   ```
   Ciphers aes128-cbc,aes256-cbc
   ```

   ```
   KexAlgorithms diffie-hellman-group14-sha1,diffie-hellman-group14-sha256
   ```

3. Type the following command to restart the service:

   ```
   service sshd restart
   ```

   Note: The SSH session rekey is hardcoded to rekey after one hour or following the exchange of one GB of data, whichever comes first.

Configuring Java TLS ciphers

Follow these steps to exclude cipher suites from the Java security policy file.

Procedure

1. Type the following command:

   ```
   sudo cp /opt/ibm/java-x86_64-80/jre/lib/security/policy/unlimited/local_policy.jar
   /opt/ibm/java-x86_64-80/jre/lib/security/
   ```

2. Type this command to edit the configuration file:

   ```
   sudo vim /opt/ibm/java-x86_64-80/jre/lib/security/java.security
   ```

3. Replace this line of text:

   ```
   jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, DSS, DH_anon, ECDH, ECDHE, GCM, MD5, MD5withRSA,
   DH keySize < 2048, NULL, DESede, \
   EC keySize < 224, 3DES_EDE_CBC
   ```

with this text:

```
jdk.tls.disabledAlgorithms=SSLv3, RC4, DES, DSS, DH_anon, ECDH, ECDHE, GCM, MD5, MD5withRSA,
DH keySize < 1024, NULL, DESede, \
EC keySize < 224, 3DES_EDE_CBC
```

4. Reboot the appliance.

Limiting the cipher suites in use

Configure QRadar to use only those cipher suites that are required for the evaluation.

Procedure

1. Type the following command to edit the `ssl.conf` file:

```
vim /etc/httpd/conf.d/ssl.conf
```

2. Replace the `SSLCipherSuite` line with the following text:

```
SSLCipherSuite AES128-SHA:AES256-SHA:AES256-SHA256:!aNULL:!eNULL:!EXPORT:!DES:!MD5:!PSK:!RC4
```

3. Type the following command to restart the service:

```
service httpd restart
```

Enable usage checking for certificates

The certificate includes information in the Key Usage field that identifies what the certificate can be used for.

Enable usage checking of the certificate to verify that the claimed purpose of the imported certificate matches the intended usage. Usage checking also verifies that the issuers of the certificate revocation lists (CRL) files for a certificate have the CRLSign usage.

Procedure

1. Edit the `frameworks.properties` file in the `/store/configservices/staging/globalconfig` directory.
2. Set `trustmanager.checkusage=true`.
3. On the **Admin** tab, deploy the change.
4. Restart the system.

Chapter 4. Certificate generation and verification

Creating a CSR request by using a 2048-bit RSA key

Generate an SSL certificate request from your IBM QRadar Console.

Procedure

1. Use an SSH client to log in to QRadar Console.
2. Generate a 2048-bit RSA private key file by typing the following command.

```
openssl genrsa -out qradar.key 2048
```

   The `qradar.key` file is created in the current directory.
3. Generate the certificate signing request (CSR) file by using the command:

```
openssl req -new -key qradar.key -out qradar.csr
```

   The `qradar.csr` file is created for the certificate authority (CA) to use.
4. When prompted in the command line, provide the following information:

```
Country Name (2 letter code) [XX]:CA
State or Province Name (full name) []:NB
Locality Name (eg, city) [Default City]:Fredericton
Organization Name (eg, company) [Default Company Ltd]:IBM
Organizational Unit Name (eg, section) []:SI
Common Name (eg, your name or your server's hostname) []:myhostname
Email Address []:username@example.com
```

   If the command line asks for more properties, leave the fields empty.

   Note: If you enter a password for the `Challenge Password` property and you forget the entry, you might not be able to use the CSR. The CA might not support a challenge password.
5. Before you send the CSR, verify the information by typing the following command:

```
openssl req -noout -text -in qradar.csr
```

6. Use Secure File Transfer Protocol or another program to securely copy the CSR file to your computer.
7. Submit the CSR to the certificate authority.

   The CSR is identified as a certificate in Apache format.

Certification Revocation List

The IBM QRadar cryptographic system uses OpenSSL to generate a Certificate Revocation List (CRL), which lists digital certificates that are revoked by the issuing certificate authority (CA) before their scheduled expiration date. Any certificates that are listed in the CRL are not trusted.

The cryptographic system determines the certificate revocation status by using one or more CRL Distribution Points (CRLDP) that are embedded within the certificate that is checked. The trust manager compares a certificate ID with the list of IDs in the CRL to determine whether and why the certificate was revoked.

Verifying the CA certificates

Verify that the certificates are issued by a trusted certificate authority (CA).

Certificates from a well-known public CA

For certificates that are issued from a well-known public CA, you can verify the certificate by using the Red Hat Enterprise Linux (RHEL) built-in CA store. Run the following command to verify the certificate:

```
openssl verify -verbose -x509_strict cert_chain.pem
```

The `cert_chain.pem` file contains the certificate bundle that is returned from the CA.

Certificates from a private CA

For certificates that are issued by a private CA where the root CA certificate must be installed for QRadar, use the following command:

```
openssl verify -verbose -x509_strict -CAfile /opt/qradar/conf/trusted_certificates/ca.pem -
CApath nosuchdir cert_chain.pem
```

The `ca.pem` file is the root CA certificate that is installed previously in `trusted_certificates`, and the `cert_chain.pem` file is the certificate bundle that is returned from the CA.

Chapter 5. Configure TLS syslog for inbound data

Importing the root CA of the TLS client

If the root CA certificate of the TLS client is not a well-known root CA that has been pre-installed with Red Hat v7.5, you must use a 3rd party REST API client tool to call the QRadar REST API endpoints to import it.

Procedure

1. Create a HTTPS request with the following settings:

Setting	Value
URL	`https://<QRadar_IP_Address>/api/staged_config/ca_certs`
Protocol	POST
Header	“allow-hidden: true”
Content-type	multipart/form-data
Authorization	Basic Username: admin Password: *<Admin user password>*
multipart/form-data:	filename="*<root ca filename>*" where <filename> is the name of the root CA file, in PEM format.

2. Send the request and verify that the returned JSON shows correct information about the root CA of the TLS server certificate.
3. On **Admin** tab, in the deployment banner, click **Deploy Changes**.

Related concepts

“Verifying the CA certificates” on page 16
Verify that the certificates are issued by a trusted certificate authority (CA).

Importing the TLS server certificates

Use a 3rd party REST API client tool to call the QRadar REST API endpoints to import the certificate files.

Procedure

1. If the root CA of the server certificate is different than the root CA of the TLS client certificate, you must import it.
   a) Create an HTTPS request with the following settings:

Setting	Value
URL	`https://<QRadar_IP_Address>/api/staged_config/ca_certs`
Protocol	POST
Header	“allow-hidden: true”

Setting	Value
Content-type	multipart/form-data
Authorization	Basic Username: admin Password: *<Admin user password>*
multipart/form-data:	filename="*<root ca filename>*" where <filename> is the name of the root CA file, in PEM format.

b) Send the request and verify that the JSON response shows correct information about the root CA of the server certificate.

c) On **Admin** tab, in the deployment banner, click **Deploy Changes**.

2. Create a certificate resource.

a) Create an HTTPS request with the following settings:

Setting	Value
URL	`https://<QRadar_IP_Address>/api/staged_config/certificates`
Protocol	POST
Header	“allow-hidden: true”
Header	'Accept: application/json'
Content-type	application/json
Authorization	Basic Username: admin Password: *<Admin user password>*
body	`{ "component_id": 4, "name": "yourCertFriendlyName", "purpose": "SERVER" }`

b) Record the ID that is returned in the JSON response.

3. Import the key file.

a) Create an HTTPS request with the following settings:

Setting	Value
URL	`https://<QRadar_IP_Address>/api/staged_config/certificates/<ID>/key_file` where *<ID>* is the value that you recorded when you created the certificate resource.
Protocol	PUT
Header	“allow-hidden: true”
Content-type	application/json
Authorization	Basic Username: admin Password: *<Admin user password>*

Setting	Value
body	{"private_key": "-----BEGIN PRIVATE KEY —— <*key file content PEM encoded and in PKCS8 format*> -----END PRIVATE KEY——“

b) Verify that the HTTP response code is 204.

4. Import the intermediate file.

a) Create an HTTPS request with the following settings:

Setting	Value
URL	https://<*QRadar_IP_Address*>/api/staged_config/certificates/<*ID*>/ca_chain_file where <*ID*> is the value that you recorded when you created the certificate resource.
Protocol	PUT
Header	“allow-hidden: true”
Content-type	text/plain
Authorization	Basic Username: admin Password: <*Admin user password*>
body	:-----BEGIN CERTIFICATE----- <*your intermediate file content in pem format*> -----END CERTIFICATE——

b) Verify that the HTTP response code is 204.

5. Import the certificate file.

a) Create an HTTPS request with the following settings:

Setting	Value
URL	https://<*QRadar_IP_Address*>/api/staged_config/certificates/<*ID*>/cert_file where <*ID*> is the value that you recorded when you created the certificate resource.
Protocol	PUT
Header	“allow-hidden: true”
Content-type	text/plain
Authorization	Basic Username: admin Password: <*Admin user password*>
body	:-----BEGIN CERTIFICATE----- <*your intermediate file content in pem format*> -----END CERTIFICATE——

b) Verify that the HTTP response code is 204.

6. On **Admin** tab, in the deployment banner, click **Deploy Changes**.

Adding a log source

Add a log source to receive events from your network devices or appliances.

Procedure

1. On the **Admin** tab, click **Data Sources**, and then click the **Log Sources** icon.
2. On the toolbar, click **Add** and provide a name, description, and type of the log source.
3. In the **Log Source Type** field, select **Universal DSM**.
4. In the **Protocol Configuration** list, select **TLS Syslog** .
5. In the **Log Source Identifier** field, enter the IPv4 address or host name of the log source.
6. In the **TLS Listen Port** field, add a port, or leave the default port entry of 6514.
7. In the **Authentication Mode** field, select **TLS And Client Authentication**.
8. In the **Client Certificate Issuer ID** field, type the **Authority Key Identifier** of the client certificate.

   This is the ID of the certificate that issued the client certificate.
9. In the **Certificate CN Whitelist** field, type a comma-separated list of the client certificates' common names.
10. In the **Certificate Type** field, select **Provide Certificate**.
11. Select **Check Client Certificate Revocation**.
12. Select **Check Client Certificate Self Signed**.
13. Select **Check Client Certificate Usage**.
14. In the **Server Certificate Resource ID** field, type the ID that was returned from the RestAPI call that created the client certificate resource.
15. In the **Maximum Connections** field, enter the number of maximum connections that are allowed.
16. In the **TLS Protocols** list, select **TLS 1.2 and above**
17. Select the **Enabled** check box.

    When this option is not enabled, the log source does not collect events and the log source is not counted in the license limit.
18. In the **Credibility** list, select a credibility level.

    Credibility is a representation of the integrity or validity of events that are created by a log source.
19. From the **Target Event Collector** menu, leave as the default setting.
20. To coalesce events, select the **Coalescing Events** check box.

    When this check box is clear, events are viewed individually and events are not bundled.
21. To store the event payload, select the **Store Event Payload** check box.
22. Click **Save**.
23. On the **Admin** tab, click **Deploy Changes**.

Verifying the TLS syslog configuration

Follow these steps to verify the TLS syslog configuration.

Before you begin

You must have the client certificate and the intermediate certificate that issued the client certificate. Both the client certificate and intermediate certificate should be issued by the root CA certificate that you imported earlier.

Procedure

1. On a remote host, run the following command to print the certificate of the TLS syslog server and opens a TLS connection:

   ```
   openssl s_client -connect <QRadar_IP_address>:6514
   -cert client.crt -key client.key -CAfile intermediate.crt
   ```

2. In the open connection session, type some messages.

   The messages are collected by the QRadar TLS log server. You can view the messages on the **Log Activity** tab.

3.

Chapter 6. Configure event forwarding for outbound data

You can configure IBM QRadar systems to forward data to one or more vendor systems, such as ticketing or alerting systems. You can also forward normalized data to other QRadar systems. The target system that receives the data from QRadar is known as a *forwarding destination*.

The TLS event forwarding connections in QRadar are capable of using X.509 validation.

Follow these steps to configure QRadar to use TLS and full X.509 validation:

1. Import the root CA of the TLS server.
2. Import the TLS client certificates.
3. Create a forwarding destination.
4. Configure a routing rule to forward events to the target device.
5. “Verifying the event forwarding configuration” on page 29

Importing the root CA of the TLS server

If the root CA certificate of the remote TLS server is not a well-known root CA that has been pre-installed with Red Hat v7.5, use a 3rd party REST API client tool to call the QRadar REST API endpoints to import it.

Procedure

1. Create a HTTPS request with the following settings:

Setting	Value
URL	`https://<QRadar_IP_Address>/api/staged_config/ca_certs`
Protocol	POST
Header	“allow-hidden: true”
Content-type	multipart/form-data
Authorization	Basic Username: admin Password: *<Admin user password>*
multipart/form-data:	filename="*<root ca filename>*" where <filename> is the name of the root CA file, in PEM format.

2. Send the request and verify that the returned JSON shows correct information about the root CA of the TLS server certificate.
3. On **Admin** tab, in the deployment banner, click **Deploy Changes**.

Related concepts

“Verifying the CA certificates” on page 16

Verify that the certificates are issued by a trusted certificate authority (CA).

Importing the TLS client certificates

To import the certificate files for the TLS client, use a 3rd party REST API client tool to call the QRadar REST API endpoints.

Procedure

1. If the root CA of the client certificate is different than the root CA of the TLS server certificate, you must import it.
   a) Create an HTTPS request with the following settings:

Setting	Value
URL	`https://<QRadar_IP_Address>/api/staged_config/ca_certs`
Protocol	POST
Header	“allow-hidden: true”
Content-type	multipart/form-data
Authorization	Basic Username: admin Password: *<Admin user password>*
multipart/form-data:	filename="*<root ca filename>*" where <filename> is the name of the root CA file, in PEM format.

   b) Send the request and verify that the JSON response shows correct information about the root CA of the client certificate.
   c) On **Admin** tab, in the deployment banner, click **Deploy Changes**.
2. Create a certificate resource.
   a) Create an HTTPS request with the following settings:

Setting	Value
URL	`https://<QRadar_IP_Address>/api/staged_config/certificates`
Protocol	POST
Header	“allow-hidden: true”
Header	'Accept: application/json'
Content-type	application/json
Authorization	Basic Username: admin Password: *<Admin user password>*
body	`{ "component_id": 4, "name": "yourCertFriendlyName", "purpose": "CLIENT" }`

   b) Record the ID that is returned in the JSON response.
3. Import the key file.

a) Create an HTTPS request with the following settings:

Setting	Value
URL	`https://<QRadar_IP_Address>/api/staged_config/certificates/<ID>/key_file` where *<ID>* is the value that you recorded when you created the certificate resource.
Protocol	PUT
Header	“allow-hidden: true”
Content-type	application/json
Authorization	Basic Username: admin Password: *<Admin user password>*
body	`{"private_key": "-----BEGIN PRIVATE KEY ——` *<key file content PEM encoded and in PKCS8 format>* `-----END PRIVATE KEY——“`

b) Verify that the HTTP response code is 204.

4. Import the intermediate file.

a) Create an HTTPS request with the following settings:

Setting	Value
URL	`https://<QRadar_IP_Address>/api/staged_config/certificates/<ID>/ca_chain_file` where *<ID>* is the value that you recorded when you created the certificate resource.
Protocol	PUT
Header	“allow-hidden: true”
Content-type	text/plain
Authorization	Basic Username: admin Password: *<Admin user password>*
body	`:-----BEGIN CERTIFICATE-----` *<your intermediate file content in PEM format>* `-----END CERTIFICATE——`

b) Verify that the HTTP response code is 204.

5. Import the certificate file.

a) Create an HTTPS request with the following settings:

Setting	Value
URL	`https://<QRadar_IP_Address>/api/staged_config/certificates/<ID>/cert_file`

Setting	Value
	where *<ID>* is the value that you recorded when you created the certificate resource.
Protocol	PUT
Header	“allow-hidden: true”
Content-type	text/plain
Authorization	Basic Username: admin Password: *<Admin user password>*
body	:-----BEGIN CERTIFICATE----- *<your intermediate file content in PEM format>* -----END CERTIFICATE——

b) Verify that the HTTP response code is 204.

6. On **Admin** tab, in the deployment banner, click **Deploy Changes**.

Adding forwarding destinations to QRadar

Before you can configure bulk or selective data forwarding, you must add forwarding destinations on the QRadar console.

Procedure

1. On the **Admin** tab, click **System Configuration**.
2. Click the **Forwarding Destinations** icon.
3. On the toolbar, click **Add**.
4. In the **Name** field, type a descriptive name for the forwarding destination.
5. In the **Destination Address**, type the host name of the vendor system that you want to forward data to.

   Note: The host name must match an entry in the subject alternative names (SAN) in the server certificate of the remote TLS server.
6. In the **Event Format** list, select **Payload**.
7. In the **Destination Port**, type the port number.
8. In the **Protocol** list, select **TCP over TLS 1.1 or above**.
9. Select the **Enable hostname verification** check box.
10. Select the **Enable client authentication** check box.
11. In the **Client Certificate** list, select the client certificate that you want to use for the forwarding destination.

    Note: The list contains only those certificates that are used for event forwarding through TLS 1.1 or above. To import a new certificate, see “Importing the TLS client certificates” on page 24.
12. Select the **Prefix a syslog header if it is missing or invalid** check box.

    Note: When QRadar forwards syslog messages, the outbound message is verified to ensure that it has a valid syslog header.

    If a valid syslog header is not detected on the original syslog message and this check box is selected, the prefixed syslog header includes the originating IP address from the packet that QRadar received

in the **Hostname** field of the syslog header. If this check box is not selected, the data is sent unmodified.

13. Click **Save**.

Configuring routing rules for event forwarding

After you added one or more forwarding destinations, you can create filter-based routing rules to forward event data.

About this task

You can configure routing rules to forward data in either online or offline mode:

- In **Online** mode, your data remains current because forwarding is performed in real time. If the forwarding destination becomes unreachable, data can potentially be lost.
- In **Offline** mode, all data is stored in the database and then sent to the forwarding destination. This assures that no data is lost, however, there might be delays in data forwarding.

The following table describes some of the **Routing Rules** parameters

*Table 3. **Routing Rules** window parameters*

Parameter	Description
Forwarding Event Collector	This option is displayed when you select the **Online** option. Specifies the Event Collector that you want this routing rule to process data from.
Forwarding Event Processor	This option is displayed when you select the **Offline** option. Specifies the Event Processor that you want this routing rule process data from. **Restriction:** This option is not available if **Drop** is selected from the **Routing Options** pane.

*Table 3. **Routing Rules** window parameters (continued)*	
Parameter	**Description**
Routing Options	• The **Forward** option specifies that data is forwarded to the specified forwarding destination. Data is also stored in the database and processed by the Custom Rules Engine (CRE). • The **Drop** option specifies that data is dropped. The data is not stored in the database and is not processed by the CRE. This option is not available if you select the **Offline** option. • The **Bypass Correlation** option specifies that data bypasses CRE, but it is stored in the database. This option is not available if you select the **Offline** option. You can combine two options: • **Forward** and **Drop** Data is forwarded to the specified forwarding destination. Data is not stored in the database and is not processed by the CRE. • **Forward** and **Bypass Correlation** Data is forwarded to the specified forwarding destination. Data is also stored in the database, but it is not processed by the CRE. The CRE at the forwarded destination processes the data. If data matches multiple rules, the safest routing option is applied. For example, if data that matches a rule that is configured to drop and a rule to bypass CRE processing, the data is not dropped. Instead, the data bypasses the CRE and is stored in the database. All events are counted against the EPS license.

Procedure

1. On the **Admin** tab, click **System Configuration**.
2. Click the **Routing Rules** icon, and click **Add**.
3. Type a name and description for your routing rule.
4. In the **Mode** field, select either **Online** or **Offline**.

   QRadar uses an Event Collector for **Online** mode, and an Event Processor for **Offline** mode.
5. In the **Forwarding Event Collector** or **Forwarding Event Processor** list box, select the appliance from which you want to forward data.
6. In the **Data Source** field, select **Events**.
7. In the **Event Filters** box, specify the filter criteria:
   a) To forward all incoming data, select the **Match All Incoming Events** check box.

      Restriction: If you select this check box, you cannot add a filter.
   b) To add a filter, specify the filter criteria and click **Add Filter**.
   c) Repeat the steps for each filter that you want to add.

8. In the **Routing Options** box, specify the routing options to apply to the forwarded data:
   a) If you want to edit, add, or delete a forwarding destination, click the **Manage Destinations** link.
   b) To forward log data that matches the specified filters, select the **Forward** check box and then select the check box for each forwarding destination.

      Restriction: If you select the **Forward** check box, you can select only one of these check boxes: **Drop**, **Bypass Correlation**, or **Log Only**.

      Learn more about routing options:

      - The **Forward** option specifies that data is forwarded to the specified forwarding destination. Data is also stored in the database and processed by the Custom Rules Engine (CRE).
      - The **Drop** option specifies that data is dropped. The data is not stored in the database and is not processed by the CRE. This option is not available if you select the **Offline** option. Any events that are dropped are credited back 100% to the license.
      - The **Bypass Correlation** option specifies that data bypasses CRE, but it is stored in the database. This option is not available if you select the **Offline** option.
      - The **Log Only (Exclude Analytics)** option specifies that events are stored and flagged in the database as Log Only and bypass CRE. These events are not available for historical correlation, and are credited back 100% to the license. This option is not available for flows.

        Note: The **Log Only** option requires a license for QRadar Data Store. After the license is applied and the **Log Only** option is selected, events that match the routing rule will be stored to disk and will be available to view and for searches. The events bypass the custom rule engine and no real-time correlation or analytics occur. The events can't contribute to offenses and are ignored when historical correlation runs. Some apps will also ignore Log Only events (https://www-ibm.com/support/docview.wss?uid=swg22009471).

      You can combine three options:

      - **Forward** and **Drop**

        Data is forwarded to the specified forwarding destination. Data is not stored in the database and is not processed by the CRE.
      - **Forward** and **Bypass Correlation**

        Data is forwarded to the specified forwarding destination. Data is also stored in the database, but it is not processed by the CRE. The CRE at the forwarded destination processes the data.
      - **Forward** and **Log Only (Exclude Analytics)**

        Events are forwarded to the specified forwarding destination in online mode. Events are stored and flagged in the database as Log Only and bypass CRE. These events are not available for historical correlation, and are credited back 100% to the license. This option is not available in offline mode.

      If data matches multiple rules, the safest routing option is applied. For example, if data that matches a rule that is configured to drop and a rule to bypass CRE processing, the data is not dropped. Instead, the data bypasses the CRE and is stored in the database.
9. Click **Save**.

Verifying the event forwarding configuration

Follow these steps to verify the event forwarding configuration.

Before you begin
On a remote system, gather the server certificate, the intermediate certificate, and the root CA that issued the server certificate.

If the intermediate certificate and the root CA for the client are different from those of the server, you will also need to gather the client intermediate certificate and root CA.

Combine all the certificate files into a single CA file.

Procedure

On a remote host, run the following command to start the TLS server:

```
openssl s_server -cert server.crt -key server.key -CAfile <CA_file>
-verify 3 -accept <Port_Defined_In_Forwarding_Dest>  -Verify on -verify_return_error
```

Results

The TLS server starts and opens a session. If there are events that meet the criteria that is defined in the routing rule, QRadar forwards those events to this TLS server and they are printed out in the opened session.

Note: When a connection to the remote TLS server is disconnected unintentionally, QRadar tries to re-establish the connection automatically.

Chapter 7. QRadar system configuration

You need to configure some system settings and follow the guidelines that are provided

Complete the following tasks:

- Configure time settings.
- Create a login banner.
- Login using the different system access methods.
- Follow the guidelines for password creation.
- Complete a QRadar self-test.

Configuring system time

Set the *system time* on your IBM QRadar Console manually.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System and License Management**.
3. In the **Display** list, select **Systems**.
4. Select the host for which you want to configure the system time settings.
5. From the **Actions** menu, click **View and Manage System**.
6. Click the **System Time** tab.
7. To configure time on the QRadar Console, follow these steps:
   a) In the **Time Zone** list, select the time zone that applies to the QRadar Console.
   b) To manually configure the time, click **Set time manually:**, and then set the date and time for the console.

      Note: If you set the system time to a future date that is affected by Daylight Saving Time (DST) changes, the time you set is adjusted by 1 hour. For example, on 4 July 2016 in the U.S.A, you set the date to December 16, 2016 and the time to 8:00 PM. The time that you set ignores the DST change and is adjusted to 7:00 PM.
8. Click **Save**.
9. Click **OK** to accept that services are restarted, or **Cancel** to cancel the changes.

Adding or editing a QRadar login message

Create a new login message or edit an existing login message on your IBM QRadar Console.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System Settings**.
3. Click **Authentication Settings**.
4. To edit the login message, click **Edit** in the **Login Message** field.
   a) Type your message in the **Edit Login Message** window.
   b) To force users to consent to the login message before they can log in, select the check box.
   c) Click **Save**.

The login message is saved in the `opt/qradar/conf/loginMessage.txt` file.

Note: You can also upload the `loginMessage.txt` file to the `opt/qradar/conf/` directory.

5. On the **Admin** tab, click **Deploy Changes**.
6. To see your changes, log out of QRadar.

Administrative logins

When you initially configure IBM QRadar, you must create user accounts for all users that require access to the system. You can use the **User Management** feature on the **Admin** tab to define user roles, security profiles, and user accounts to control who has access to the system, which tasks they can perform, and which data they have access to.

You can configure QRadar to block login requests from a user account for a configurable period of time after a configurable number of failed login attempts

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System Settings**.
3. Click **Authentication settings** and configure the following settings:
   - In the **Maximum Login Attempts** field, specify the number of times a login attempt can fail.
   - In the **Login Failure Attempt Window (in minutes)** field, specify the length of time during which a maximum number of login failures can occur before the system is locked.
   - In the **Login Failure Block Time (in minutes)** field, specify the length of time that the system is locked if the maximum login failures value is exceeded.

   When the configured **Maximum Login Attempts** per account is reached within the number of minutes set in the **Login Failure Attempt Window (in minutes)**, the user account will be locked out.
4. On the **Admin** tab, select **Advanced** > **Deploy Full Configuration**.

   Note: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

Configuring the password policy

You can configure the password policy settings that apply to local user accounts. When the policy is updated, users are prompted to change their password if they log in with a password that does not meet the new requirements.

About this task

Users should be encouraged to follow these guidelines when setting their password:

- Use a password that is significantly different from previous passwords.

  Do not append a symbol or character to a previously used password because this change is not sufficiently different.
- Use a minimum of 15 characters.
- Do not use complete words that are listed in a dictionary.
- Use a mixture of uppercase letters, lowercase letters, digits, and symbols.
- Do not use personal information that is known about you, for example, pets names, your name, kids names, or any information that is available in the public domain.

Procedure

1. Click the **Admin** tab.
2. On the navigation menu, click **System Configuration** > **User Management** > **Authentication**.
3. Click **Local Passsword Policy Configuration**.
4. Specify the password policy configuration that you want to enforce.
5. On the **Admin** tab menu, select **Advanced** > **Deploy Full Configuration**.

Configuring the inactivity time period

Configure the number of minutes of inactivity after which IBM QRadar logs the user out and terminates the session.

Procedure

1. On the navigation menu (☰), click **Admin**.
2. In the **System Configuration** section, click **System Settings**.
3. Click **Authentication settings**.
4. In the **Inactivity Timeout** field, specify the number of minutes of inactivity before QRadar logs the user out.
5. Click **Save**.
6. On the **Admin** tab, select **Advanced** > **Deploy Full Configuration**.

   Note: QRadar continues to collect events when you deploy the full configuration. When the event collection service must restart, QRadar does not restart it automatically. A message displays that gives you the option to cancel the deployment and restart the service at a more convenient time.

Configuring the local session timeout period

You can configure the TMOUT environment variable to automatically log users out after a specified period of inactivity.

Procedure

1. Use SSH to log in to your QRadar Console.
2. Type `vim /etc/profile` to edit the configuration file.
3. Change the TMOUT value to the number of seconds that you want to wait before a user is automatically logged out.
4. Save the file.

Accessing QRadar RESTful API

Use the representational state transfer (REST) application programming interface (API) to make HTTPS queries and integrate IBM QRadar with other solutions. REST API communication is protected by using TLS via the Apache server, where each request is authenticated individually.

The QRadar API doc page can be used to call most QRadar APIs, but you cannot use it to upload files such as the root CA certificate. You must use a third-party API tool, such as Insomnia, to do import the certificates.

Procedure

1. Enter the following URL in your web browser to access the technical documentation interface: `https://QRadar_All_in_one_IPaddress/api_doc`.

   ```
   https://<QRadar_IP_address>/api_doc
   ```

2. Click the header for the API that you want to access; for example, `/ariel`.
3. Click the subhead for the endpoint that you want to access, for example, `/databases`.
4. Click **Try it out** to receive properly formatted HTTPS responses.
5. Review and gather the information that you need to implement in your third-party solution.

QRadar self-test

QRadar runs cryptographic "known answer" self-tests during startup.

With exception of the Digital Signature Algorithm (DSA), each cryptographic algorithm provided by the Linux Kernel Crypto API is tested using a “known answer” test to verify the correct operation of the algorithm.

A failure of any of the power-up self-tests panics the module. The only recovery is to reboot. If a reboot cannot solve the problem, the system may be compromised, and QRadar must be reinstalled on the system.

Verifying secure updates

Administrators need to manually apply QRadar secure updates when they are released. Secure updates are signed by QRadar Security Keys.

Procedure

1. Download the QRadar V7.3.2 Common Criteria update from https://www-945.ibm.com/support/fixcentral.
2. Copy the update file to the system by typing the following command:

   `scp <732_QRadar_patchupdate-7.3.2-xxxxxxxx.sh> stiguser@qradar_IP:/home/stiguser`
3. Type the following command, that uses the file name of the update that you want to install:

   ```
   sudo chmod 755 <732_QRadar_patchupdate-7.3.2-xxxxxxxx.sh>
   ```

   ```
   sudo <732_QRadar_patchupdate-7.3.2-xxxxxxxx.sh>
   ```

   This command verifies the update’s signature with the preinstalled IBM Security public key. It then creates a regular QRadar update file; For example, `732_QRadar_patchupdate-7.3.2-xxxxxxxx.sh.sfs`.

   When the signature is successfully verified, the following message appears:
4. Review the status of the signature verification.

   a) When the verification is successful, the following message is shown:

   ```
   The signature for 732_QRadar_patchupdate-7.3.2.xxxxx.sfs is valid.
   Proceed with the install by mounting the 732_QRadar_patchupdate-7.3.2.xxxxx.sfs
   file and executing the embedded setup script.

   E.g.
   mount -o loop 732_QRadar_patchupdate-7.3.2.xxxxx.sfs  /mnt
   /mnt/installer

   Done.
   ```

The successful verification is tracked in the `/var/log/audit.log` file.

b) When the signature verification fails, the following message is shown:

```
Signature invalid! 732_QRadar_patchupdate-7.3.2.xxxxx.sfs.
Check with your vendor to ensure that you receive only valid, signed packages.
```

The failed verification is tracked in the `/var/log/audit.log` file.

5. Run the updates by typing the following commands:

```
sudo mkdir /media/updates
```

```
sudo mount -o loop ./732_QRadar_patchupdate-7.3.2-xxxxxxxx.sfs /media/updates
```

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

6. Type the following command to verify the QRadar patch version:

```
sudo /opt/qradar/bin/myver -v
```

Viewing the audit logs

Changes that are made by IBM QRadar users are recorded in the audit logs. You can use Secure Shell (SSH) to review the audit logs and monitor changes to your system.

About this task

All audit logs are stored in plain text and are archived and compressed when the audit log file reaches 200 MB. The current log file is named `audit.log`. When the file reaches 200 MB, the file is compressed and renamed to `audit.log.1.gz`. The file number increments each time that a log file is archived. QRadar retains up to 50 archived log files.

The Target of Evaluation (TOE) system displays the following warning message before the local storage space for the audit log is full:

```
Audit log rotation event.
The audit.log file has reached maximum capacity and will be overwritten.
```

Procedure

1. Using SSH, log in to QRadar as the root user:
   - **User Name:** `root`
   - **Password:** *password*
2. Review the following audit logs:
   - `/var/log/audit/audit.log`
   - `/var/log/qradar.log`
   - `/var/log/secure`
   - `/var/log/qradar.error`
   - `/var/log/<patch_reference>/patches.log`

What to do next

For more information about the format of the audit log entries and the actions that are logged, see the *Audit Logs* document (`732niap_audit_logs.docx`) that was provided.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785 U.S.A.

For license inquiries regarding double-byte character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some jurisdictions do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM websites are provided for convenience only and do not in any manner serve as an endorsement of those websites. The materials at those websites are not part of the materials for this IBM product and use of those websites is at your own risk.

IBM may use or distribute any of the information you provide in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Director of Licensing
IBM Corporation
North Castle Drive, MD-NC119
Armonk, NY 10504-1785
US

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

The performance data and client examples cited are presented for illustrative purposes only. Actual performance results may vary depending on specific configurations and operating conditions..

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

Statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to actual people or business enterprises is entirely coincidental.

Trademarks

IBM, the IBM logo, and ibm.com® are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Terms and conditions for product documentation

Permissions for the use of these publications are granted subject to the following terms and conditions.

Applicability

These terms and conditions are in addition to any terms of use for the IBM website.

Personal use

You may reproduce these publications for your personal, noncommercial use provided that all proprietary notices are preserved. You may not distribute, display or make derivative work of these publications, or any portion thereof, without the express consent of IBM.

Commercial use

You may reproduce, distribute and display these publications solely within your enterprise provided that all proprietary notices are preserved. You may not make derivative works of these publications, or reproduce, distribute or display these publications or any portion thereof outside your enterprise, without the express consent of IBM.

Rights

Except as expressly granted in this permission, no other permissions, licenses or rights are granted, either express or implied, to the publications or any information, data, software or other intellectual property contained therein.

IBM reserves the right to withdraw the permissions granted herein whenever, in its discretion, the use of the publications is detrimental to its interest or, as determined by IBM, the above instructions are not being properly followed.

You may not download, export or re-export this information except in full compliance with all applicable laws and regulations, including all United States export laws and regulations.

IBM MAKES NO GUARANTEE ABOUT THE CONTENT OF THESE PUBLICATIONS. THE PUBLICATIONS ARE PROVIDED "AS-IS" AND WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING BUT NOT LIMITED TO IMPLIED WARRANTIES OF MERCHANTABILITY, NON-INFRINGEMENT, AND FITNESS FOR A PARTICULAR PURPOSE.

IBM Online Privacy Statement

IBM Software products, including software as a service solutions, (“Software Offerings”) may use cookies or other technologies to collect product usage information, to help improve the end user experience, to tailor interactions with the end user or for other purposes. In many cases no personally identifiable information is collected by the Software Offerings. Some of our Software Offerings can help enable you to collect personally identifiable information. If this Software Offering uses cookies to collect personally identifiable information, specific information about this offering’s use of cookies is set forth below.

Depending upon the configurations deployed, this Software Offering may use session cookies that collect each user’s session id for purposes of session management and authentication. These cookies can be disabled, but disabling them will also eliminate the functionality they enable.

If the configurations deployed for this Software Offering provide you as customer the ability to collect personally identifiable information from end users via cookies and other technologies, you should seek your own legal advice about any laws applicable to such data collection, including any requirements for notice and consent.

For more information about the use of various technologies, including cookies, for these purposes, See IBM’s Privacy Policy at http://www.ibm.com/privacy and IBM’s Online Privacy Statement at http://www.ibm.com/privacy/details the section entitled “Cookies, Web Beacons and Other Technologies” and the “IBM Software Products and Software-as-a-Service Privacy Statement” at http://www.ibm.com/software/info/product-privacy.

General Data Protection Regulation

Clients are responsible for ensuring their own compliance with various laws and regulations, including the European Union General Data Protection Regulation. Clients are solely responsible for obtaining advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulations that may affect the clients’ business and any actions the clients may need to take to comply with such laws and regulations. The products, services, and other capabilities described herein are not suitable for all client situations and may have restricted availability. IBM does not provide legal, accounting or auditing advice or represent or warrant that its services or products will ensure that clients are in compliance with any law or regulation.

Learn more about the IBM GDPR readiness journey and our GDPR capabilities and Offerings here: https://ibm.com/gdpr