IBM Security QRadar
Version 7.3.0

Upgrade Guide

IBM

Note

Before you use this information and the product that it supports, read the information in "Notices" on page 21.

Product information

This document applies to IBM® QRadar® Security Intelligence Platform V7.3.0 and subsequent releases unless superseded by an updated version of this document.

Contents

Introduction to upgrading QRadar software

Information about upgrading IBM Security QRadar applies to IBM Security QRadar SIEM and IBM QRadar Log Manager products.

Intended audience

System administrators who are responsible for upgrading IBM Security QRadar systems must be familiar with network security concepts and device configurations.

Technical documentation

To find IBM Security QRadar product documentation on the web, including all translated documentation, access the IBM Knowledge Center (http://www.ibm.com/support/knowledgecenter/SS42VS/welcome).

For information about how to access more technical 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 the Support and Download Technical Note (http://www.ibm.com/support/docview.wss?uid=swg21616144).

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 Security 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 Security QRadar.

Chapter 1. What's new when you upgrade to QRadar V7.3.0

IBM Security QRadar V7.3.0 introduces a shared license pool for managing EPS and FPM, and now uses Red Hat Enterprise Linux (RHEL) V7.3.

Shared license pool

You can adapt to workload changes by distributing events per second (EPS) and flows per minute (FPM) to any host in your deployment, regardless of which appliance the license is allocated to.

For example, you have a QRadar V7.2.8 distributed deployment that has two event processors, one with 7,500 EPS and the other with 15,000 EPS. When you upgrade to QRadar V7.3.0, each processor maintains the pre-upgrade EPS allocations, but the combined 22,500 EPS become part of the shared license pool. When the data volumes for the event processors change, or when you add a managed host, you can redistribute the EPS capacity.

For more information about managing the shared license pool, see the License Management chapter in the *IBM Security QRadar Administration Guide*.

RHEL V7.3 benefits

RHEL V7.3 makes QRadar more secure. RHEL V7.3 also supports Logical Volume Management (LVM).

Chapter 2. Preparing for the upgrade

To successfully upgrade an IBM Security QRadar system, verify your upgrade path, especially when you upgrade from older versions that require intermediate steps. You must also review the software, hardware, and high availability (HA) requirements.

Important: When you upgrade to QRadar V7.2.6 or later, the SSH keys on every managed host are replaced. If you are connecting to or from a QRadar managed host and you are using key-based authentication, do not remove or alter the SSH keys. Removing or altering the keys might disrupt communication between the QRadar Console and the managed hosts, and result in lost data.

Use the following checklist to make sure that you are prepared for an upgrade.

__ • Notify users of scheduled maintenance.

__ • Verify that running scans and reports are complete.

__ • Request that users close all QRadar sessions and **`screen`** sessions.

__ • Download the update ISO or SFS file. See the QRadar Release Notes (https://ibm.biz/qradarsoftware) for a download link.

__ • Verify the checksum of the update ISO or SFS.

__ • Get a CSV file that contains a list of IP addresses for each appliance in your deployment if you don't already have this information, but typing the following command:

```
/opt/qradar/support/deployment_info.sh
```

__ • Back up all third-party data, such as:

- scripts
- personal utilities
- important files or exports
- JAR files or interim fixes that were provided by QRadar support
- static route files for network interfaces

__ • If you have HA appliances in your deployment, verify that your primary appliances are in the Active state, and your secondary appliances are in the Standby state.

__ • Ensure that you have direct access to the command line on all appliances. If you are using IMM, iDRAC, Raritan, KVM, or other technology for command line access, ensure that they are configured and functional.

__ • Verify that the firmware is the latest version for your appliances. For more information about updating firmware, see Firmware update for QRadar (http://www-01.ibm.com/support/docview.wss?uid=swg27047121).

__ • Back up your custom content by typing the following command:

```
/opt/qradar/bin/contentManagement.pl --action export --content-type all
```

__ • Confirm that all appliances in your deployment are at the same software version by typing the following commands:

```
/opt/qradar/support/all_servers.sh -C -k /opt/qradar/bin/myver >
myver_output.txt
```

```
cat myver_output.txt
```

__ • Confirm that all previous updates are unmounted by typing the following commands:

```
/opt/qradar/support/all_servers.sh -k “umount /media/cdrom"
```

```
/opt/qradar/support/all_servers.sh -k “umount /media/updates"
```

__ • Confirm that the total size of the primary disk is greater than 130 gigabytes (GB) for all servers in your deployment by typing the following command:

```
/opt/qradar/support/all_servers.sh -k df -h /root /var/log |
tee diskchecks.txt
```

__ • Verify that the following file systems are mounted and available:

- `/store` - Stores event and flow data on each appliance.
- `/storetmp` - Stores configuration information on each appliance in QRadar 7.3.0 and later.
- `/store/tmp` - Stores configuration information on each appliance in QRadar 7.2.8 and earlier.
- `/transient` - Stores saved searches and index information in QRadar 7.3.0 and later.
- `/store/transient` - Stores saved searches and index information in QRadar 7.2.8 and earlier.

__ • If you have HA appliances in your deployment:

- Verify that the `/store` file system is mounted on the primary appliance and not mounted on the secondary appliance.
- Verify that the `/transient` file system is mounted on both the primary and secondary appliances.

__ • If the entire `/store` directory is mounted on offboard storage, run the following command to prepare the system for the upgrade:

```
/media/cdrom/post/prepare_offboard_storage_upgrade.sh
```

If you are not prompted to remount your offboard storage solution during the upgrade, remount the storage when the upgrade finishes.

For additional upgrade steps for iSCSI and Fibre Channel offboard storage solutions, and for information about remounting offboard storage, see the *Offboard Storage Guide*.

__ • Review system notifications for errors and warnings for the following messages before you attempt to update. Resolve these error and warning system notifications before you attempt to update:

- Performance or event pipeline degradation notifications
- Memory notifications
- TX sentry messages or process stopped notifications
- HA active or HA standby failure system notifications
- Disk failure system notifications
- Disk Sentry noticed one or more storage partitions are unavailable notifications
- Time synchronization system notifications
- Unable to execute a backup request notifications
- Data replication experiencing difficulty notifications
- RAID controller misconfiguration notifications

__ • Ensure that the QRadar Console doesn't have a QRadar Incident Forensics license allocated to it.

Upgrading a QRadar Console that uses a QRadar Incident Forensics license might cause the shared license pool to become over-allocated, and prevent you from using some features on the Log Activity and Network Activity tabs. To avoid this problem, remove the QRadar Incident Forensics license, and add it back after the upgrade is finished. For more information about managing licenses, see the *IBM Security QRadar Administration Guide*.

__ • Manually deploy changes in the user interface to verify that it completes successfully.

__ • Verify that the latest configuration backup completed successfully and download the file to a safe location.

__ • Resolve any issues with applications in an error state or not displaying properly.

Software version requirements for upgrades

To ensure that IBM Security QRadar upgrades without errors, ensure that you use only the supported versions of QRadar software:

- Ensure that QRadar V7.2.8 (20161118202122 and later) is installed. To learn more about QRadar versions, see the QRadar Master Software List.
- Check the software version in the software by clicking **Help** > **About**.

Important: Software versions for all IBM Security QRadar appliances in a deployment must be the same version and fix level. Deployments that use different QRadar versions of software are not supported.

Important: For a managed WinCollect deployment, you must use WinCollect V7.2.5 or later. If you are on an earlier version of WinCollect, you must upgrade to WinCollect V7.2.5 before you can apply the QRadar V7.3.0 upgrade. For more information on how to upgrade WinCollect agents, see http://www.ibm.com/support/docview.wss?uid=swg21999193. You might also find the WinCollect V7.2.5 Release Notes useful.

Memory and disk space requirements

Before you upgrade, ensure that IBM Security QRadar meets the minimum or suggested memory and disk space requirements.

QRadar memory requirements

The following table describes the minimum and suggested memory requirements for QRadar appliances. The minimum memory requirement defines the amount of memory that is required by the software features. The suggested memory requirements include the amount of memory that is required by the current software features and extra memory for possible future capabilities. Appliances that have less than the suggested appliance memory might experience performance issues during periods of excessive event and flow traffic.

Table 1. Minimum and optional memory requirements for QRadar appliances

Appliance	Minimum memory requirement	Suggested memory requirement
QFlow Collector 1201	6 GB	6 GB
QFlow Collector 1202	6 GB	6 GB
QFlow Collector Virtual 1299 without QRadar Vulnerability Scanner	2 GB	2 GB
QFlow Collector Virtual 1299 with QRadar Vulnerability Scanner	6 GB	6 GB
QFlow Collector 1301	6 GB	6 GB
QFlow Collector 1310	6 GB	6 GB
QRadar Event Collector 1501	12 GB	16 GB
QRadar Event Collector Virtual 1599	12 GB	16 GB
QRadar Event Processor 1601	12 GB	48 GB
QRadar Event Processor 1605	12 GB	48 GB
QRadar Event Processor 1624	64 GB	64 GB
QRadar Event Processor 1628	128 GB	128 GB

Table 1. Minimum and optional memory requirements for QRadar appliances (continued)

Appliance	Minimum memory requirement	Suggested memory requirement
QRadar Event Processor Virtual 1699	12 GB	48 GB
QRadar Flow Processor 1701	12 GB	48 GB
QRadar Flow Processor 1705	12 GB	48 GB
QRadar Flow Processor 1724	64 GB	64 GB
QRadar Flow Processor 1728	128 GB	128 GB
QRadar Flow Processor Virtual 1799	12 GB	48 GB
QRadar Event and Flow Processor 1805	12 GB	48 GB
QRadar Event and Flow Processor 1824	64 GB	64 GB
QRadar Event and Flow Processor 1828	128 GB	128 GB
QRadar SIEM 2100	24 GB	24 GB
QRadar SIEM 2100 Light	24 GB	24 GB
QRadar SIEM 3100	24 GB	48 GB
QRadar SIEM 3105	24 GB	48 GB
QRadar SIEM 3124	64 GB	64 GB
QRadar SIEM 3128	128 GB	128 GB
QRadar SIEM Virtual 3199	24 GB	48 GB
QRadar xx48	128 GB	128 GB
QRadar Network Packet Capture	128 GB	128 GB
QRadar Network Insights	128 GB	128 GB
QRadar xx48	128 GB	128 GB
QRadar Log Manager 1605	12 GB	48 GB
QRadar Log Manager 1624	64 GB	64 GB
QRadar Log Manager 1628	128 GB	128 GB
QRadar Log Manager 2100	24 GB	24 GB
QRadar Log Manager 3105	24 GB	48 GB
QRadar Log Manager 3124	64 GB	64 GB
QRadar Log Manager 3128	128 GB	128 GB
QRadar Log Manager 3199	24 GB	48 GB

Other memory requirements

If the following conditions are met, extra memory requirements might be required:

- If you plan to enable payload indexing, your system requires a minimum of 24 GB of memory. However, 48 GB of memory is suggested.
- If you install QRadar software on your own hardware, your system requires a minimum of 24 GB of memory.

Disk space requirements

Before you upgrade to QRadar V7.3.0, ensure that the total size of the primary disk is at least 130 gigabytes (GB).

The upgrade pretest determines whether a partition includes enough free space to complete an upgrade. Before you can upgrade, you must free up sufficient disk space on the partition that is defined in the pretest error message.

Upgrade sequence in distributed deployments

When you upgrade IBM Security QRadar systems, you must complete the upgrade process on your QRadar Console first. You must be able to access the user interface on your desktop system before you upgrade your secondary QRadar Console and managed hosts.

Upgrade your QRadar systems in the following order:

1. Console
2. The following QRadar systems can be upgraded concurrently:
   - Event Processors
   - QRadar Event Collectors
   - Flow Processors
   - QFlow Collectors

Upgrading high-availability deployments

Before you upgrade the IBM Security QRadar in a high-availability (HA) deployment, the primary host must be the active system in your deployment. The primary host must be upgraded before you manually upgrade the secondary host.

Before you upgrade the secondary host, copy the following file from the upgraded primary HA host to the secondary HA host to ensure that the management interfaces match between the two hosts after the upgrade finishes:

```
scp /opt/qradar/conf/capabilities/map_localhost_interfaces.txt.bak
root@<secondary_ip>:/opt/qradar/ha/map_localhost_interfaces.txt
```

If the HA cluster is disconnected, or you want to add a new secondary HA host, you must reinstall QRadar on the secondary HA. For more information about reinstalling software, see the *Installation Guide* for your system. After you reinstall the secondary HA host, log in to the user interface to reconnect or to create a new HA cluster.

Before you upgrade a disconnected HA cluster, copy the following file from the primary to the secondary HA host to ensure that the management interfaces match between the two hosts after the upgrade finishes:

```
scp /opt/qradar/conf/capabilities/map_localhost_interfaces.txt.bak
root@<secondary_ip>:/opt/qradar/ha/map_localhost_interfaces.txt
```

Important: Disk replication and failover are disabled until the primary and secondary hosts synchronize and the `needs upgrade` or `failed` status is cleared from the secondary host.

After you upgrade the secondary host, you might need to restore the configuration of the secondary host. For more information about restoring a failed host, see the *Administration Guide* for your product.

Chapter 3. Upgrading QRadar appliances

You must upgrade all of the IBM Security QRadar products in your deployment to the same version. During the upgrade, the version of Red Hat Enterprise Linux is upgraded to V7.3.

About this task

Important: You must have QRadar v7.2.8 -QRFULL- 20161118202122 fix pack or later installed before you can upgrade to QRadar V7.3.1. Click **Help** > **About** to view the QRadar version. Download the software fix (https://www-945.ibm.com/support/fixcentral/swg/selectFixes?product=ibm%2FOther +software%2FIBM+Security+QRadar+Risk+Manager&fixids=7.2.8-QRADAR-QRSIEM-20161118202122&source=dbluesearch&function=fixId&parent=IBM%20Security).

Upgrade your QRadar Console first, and then upgrade each managed host. In high-availablity (HA) deployments, upgrade the HA primary host first, and then upgrade the HA secondary host.

Important: Upgrading the QRadar Console to V7.3.1 takes approximately 3 hours. Upgrading managed hosts takes approximately 1 ½ hours. If you experience extended upgrade times, contact support to review the progress of the upgrade.

Procedure

1. If you are not on QRadar V7.2.8.2 or later, perform the following steps to update to the minimum QRadar software version patch required for the QRadar V7.3.1 upgrade. Otherwise skip to step 2.

   Note: Ensure that the console is upgraded before upgrading any attached managed hosts or HA secondary appliances.

   a) Download the *<QRadar_patchupdate>*.sfs file from Fix Central (www.ibm.com/support/fixcentral).

   b) Use SSH to log in to your system as the root user.

   c) Copy the patch file to the `/root` or `/var/log` directory or to another location that has sufficient disk space.

      Important: Do not copy the file to an existing QRadar system directory, such as `/store`.

   d) To create the `/media/updates` directory, type the following command:

      ```
      mkdir -p /media/updates
      ```

   e) Change to the directory where you copied the patch file.

   f) To mount the patch file to the `/media/updates` directory, type the following command:

      ```
      mount -o loop -t squashfs <QRadar_patchupdate>.sfs /media/updates
      ```

   g) To run the patch installer, type the following command:

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

      Tip: The first time that you run the patch installer script, there might be a delay before the first patch installer menu is displayed.

   h) Provide answers to the pre-patch questions based on your QRadar deployment.

   i) Using the patch installer, apply the software fix to all systems in your deployment.

      The patch installer menu lists the following options.

      - Console
      - All

      If you select **All**, the software fix is applied to the QRadar Console first, and then to all managed hosts. If you select **Console**, the software fix is applied only to the QRadar Console. After the software fix is applied to the QRadar Console, the menu lists the remaining managed hosts, and the **All** option.

If your SSH session is disconnected while the patching is in progress, the patching continues. When you reopen your SSH session and rerun the installer, the installation resumes.

j) After the patch is complete, unmount the software update by using the following command:

```
umount /media/updates
```

k) Now that you have updated to the minimum fix pack required for V7.2.8, use the following sequence to upgrade to QRadar V7.3.1.

2. To upgrade, download the *<QRadar>*.iso file from Fix Central (www.ibm.com/support/fixcentral).

   a) Use SSH to log in to your system as the root user.

   b) Copy the ISO file to the `/root` or `/var/log` directory or to another location that has sufficient disk space.

   Important: Don't copy the file to an existing QRadar system directory, such as `/store`.

   c) To create the `/media/cdrom` directory, type the following command:

   ```
   mkdir -p /media/cdrom
   ```

   d) Change to the directory where you copied the ISO file.

   e) To mount the ISO file to the `/media/cdrom` directory, type the following command:

   ```
   mount -o loop <QRadar>.iso /media/cdrom
   ```

   f) Pretest the installation by typing the following command:

   ```
   /media/cdrom/setup -t
   ```

   g) Review the pretest output and, if your deployment fails any pretests, take any of the suggested actions.

   h) To run the installer, type the following command:

   ```
   /media/cdrom/setup
   ```

   Important: The SSH connection pauses for 20 minutes because the system restarts. Monitor the console screen to confirm when the SSH becomes available after the system restart.

   i) If your deployment includes offboard storage, see the *IBM Security QRadar Offboard Storage Guide* for steps to reconnect and remount offboard storage types.

What to do next

1. Perform an automatic update to ensure that your configuration files contain the latest network security information. For more information, see the *IBM Security QRadar SIEM Administration Guide*.
2. Delete the patch file to free up space on the partition.
3. Clear your web browser cache. After you upgrade QRadar, the **Vulnerabilities** tab might not be displayed. To use QRadar Vulnerability Manager after you upgrade, you must upload and allocate a valid license key. For more information, see the *Administration Guide* for your product.

Clearing the web browser cache after upgrades

After you upgrade, clear the web browser cache before you log in to IBM Security QRadar.

Procedure

1. To clear your web browser cache, ensure that you have only one instance of your web browser open, and then clear the cache.
2. Log in to QRadar by typing the IP address of the QRadar system into a web browser:

   ```
   https://IP Address
   ```

   The default user name is `admin`.

Chapter 4. Upgrading QRadar software installations

Upgrade IBM Security QRadar V7.2.8 to V7.3.0 on your own appliance with a QRadar software installation. A software installation includes custom Red Hat Enterprise Linux (RHEL) partitions that are already configured.

Important: You must have QRadar v7.2.8 -QRFULL- 20161118202122 fixpack and later installed before you can upgrade to QRadarV7.3.0. Click **Help** > **About** to view the QRadar version. Download the software fix (https://www-945.ibm.com/support/fixcentral/swg/selectFixes?product=ibm%2FOther+software%2FIBM+Security+QRadar+Risk+Manager&fixids=7.2.8-QRADAR-QRSIEM-20161118202122&source=dbluesearch&function=fixId&parent=IBM%20Security).

You must complete these tasks to upgrade QRadar with customer RHEL partitions:

1. Copy the required files to your appliance and start the upgrade.
2. Install RHEL V7.3 and configure partitions.
3. Follow the installation wizard to complete the QRadar installation.

Important: Upgrading the QRadar Console to V7.3.0 should take approximately 3 hours. Upgrading managed hosts should take approximately 1 ½ hours. If you experience extended upgrade times, please contact support to review the progress of the upgrade.

Copying the required files

Copy the files to the host where you want to upgrade IBM Security QRadar, and begin the setup process.

Before you begin

- Download the QRadar release ISO file from Fix Central (https://www-945.ibm.com/support/fixcentral).
- Obtain the Red Hat Enterprise Linux V7.3 ISO.
- Confirm that your appliance meets the minimum requirements for QRadar. For more information about system requirements, see "Memory and disk space requirements" on page 5.
- Upgrade all managed hosts before you deploy changes.
- Disconnect high-availablity (HA) hosts before the upgrade if the entire `/store` directory is mounted on offboard storage. For more information about disconnecting an HA cluster, see the *IBM Security QRadar High Availability Guide*.
- Ensure that the order of mount points in the `/etc/fstab` file matches on both the primary and secondary HA host:
  - `/store`
  - `/store/tmp`
  - `/store/transient`
  - Any subdirectory of `/store` if the partition is mounted on offboard storage

  Restart the system after any updates to the `/etc/fstab` file.
- If the entire `/store` directory is mounted on offboard storage, run the following command to prepare the system for the upgrade:

  ```
  /media/cdrom/post/prepare_offboard_storage_upgrade.sh
  ```
- If you are not prompted to remount your offboard storage solution during the upgrade, remount the storage when the upgrade finishes.

  For additional upgrade steps for iSCSI and Fibre Channel offboard storage solutions, and for information about remounting offboard storage, see the *Offboard Storage Guide*.

Procedure

1. Copy the Red Hat Enterprise Linux operating system DVD ISO to one of the following portable storage devices:
    - Digital Versatile Disk (DVD)
    - Bootable USB flash drive
2. Using a Secure File Transfer Protocol (SFTP) program, such as WinSCP, copy the QRadar ISO to the host where you want to install QRadar.
3. Use SSH to log in to the system as the root user.
4. Create the installation directory by typing the following command:

    ```
    mkdir -p /media/cdrom
    ```

5. Mount the QRadar ISO by typing the following command:

    ```
    mount -o loop <QRadar_ISO> /media/cdrom
    ```

6. Start the QRadar setup by typing the following command:

    ```
    /media/cdrom/setup
    ```

Partition requirements and recommendations

During the upgrade process, partition requirements and recommendations are generated. If those instructions don't work, you can configure the partition manually.

The following partitions must be preserved and must not be reformatted:

Table 2. Requirements (preserve and do not reformat these partitions).

Partition	Description
/store	Stores data files.
/storetmp	Stores configuration files.
/transient	Stores saved searches.

Table 3. Requirements (minimum partition sizes for Red Hat V7.3 & QRadar V7.3.0 Upgrade)

Partition	Size(MiB)	Device Type	Volume Group	File System Type
/boot	100 MiB **Note:** Suggested size is at least 200 MiB. Ideal size is 1024 MiB.	Standard Partition	N/A	XFS

Table 3. Requirements (minimum partition sizes for Red Hat V7.3 & QRadar V7.3.0 Upgrade) (continued)

Partition	Size(MiB)	Device Type	Volume Group	File System Type
/	5000 MiB (Normally 1000 MiB, but /store requires 4000 MiB.) **Note:** `/store` needs to be unmounted when you are installing QRadar V7.3.0 for the upgrade, so the requirement falls to /.	LVM	rootrhel	XFS
/opt	6000 MiB	LVM	rootrhel	XFS
/var	500 MiB	LVM	rootrhel	XFS
/home	1 MiB	LVM	rootrhel	XFS
/tmp	500 MiB	LVM	rootrhel	XFS
/var/log	1000 MiB	LVM	varlogrhel	XFS
/var/log/audit	1000 MiB	LVM	varlogrhel	XFS

Recommendations:

- Keep and reformat `/boot/efi` partition if it exists in the existing partition layout. Otherwise, it does not need to be created.
- Delete and re-create `/boot` with size 1024 MiB by taking space from `swap` or / if possible. Else, re-create `/boot` with original size.

  Note: If there is no `/boot/efi` partition, take 1 MiB away from `/boot` size and create a `biosboot` mount point with size 1 MiB.
- Delete the preexisting / partition and re-create as LVM. Ensure that you use `rootrhel` as the volume group name. The file system type must be XFS, and the device type must be LVM.
- Break down as:

  If space was taken for `/boot`, remove that amount from here.

  4 MiB for LVM metadata.
- Break down remaining based on percentage. You can use the following formula for calculating partition size.

  File System Type: XFS

  Device Type: LVM

  / 36%

  `/opt` 36%

  `/var` 14%

  `/home` 2%

  `/tmp` 8%
- Formula for calculating partition size:

Preexisting / is 20000 MiB, and size for /boot is taken from /. Thus, 20000 - 4 - 1024 = 18972.

/ = 18972 * 36 / 100 = 6829.92. Round to 6829.

/opt = 18972 * 36 / 100 = 6829.92. Round to 6829.

/var = 18972 * 14 / 100 = 2656.08. Round to 2656.

/home = 18972 * 2 / 100 = 379.44. Round to 379.

/tmp = 18972 * 8 / 100 = 1517.76. Round to 1517.

- Delete preexisting /var/log partition and re-create as LVM. Ensure that you use rootrhel as the volume group name. The file system type must be XFS, and the device type must be LVM.
- Break down as:

  4 MiB for LVM metadata.
- Break down remaining based on percentage. You can use the following formula for breaking down the existing partition into LVM:

  /var/log 83%

  /var/log/audit 17%
- Formula for breaking down existing partition into LVM with new volumes:

  (Total size from preexisting partition - 4 MiB for LVM metadata - size for /boot) * percentage / 100

Installing RHEL V7.3 and configuring partitions

When you initiate an IBM Security QRadar upgrade on a host that has custom RHEL partitions configured, a message appears stating that a RHEL Software Installation exists. Copy the recommendations for sizing your existing partitions for RHEL V7.3 to use later in the procedure.

Procedure

1. Insert the portable storage device into your appliance and restart your appliance.
2. From the starting menu, select one of the following options:
   - Select the USB or DVD drive as the boot option.
   - To install on a system that supports Extensible Firmware Interface (EFI), you must start the system in legacy mode.
3. Follow the instructions in the installation wizard to begin the installation:

   a) Set the language to English (US).

   b) Click **Date & Time** and set the time for your deployment.

   c) Click **Installation Destination** and select the **I will configure partitioning** option, and then click **Done**.
4. Adjust the partition sizes according to the recommendations for your deployment that is listed in the installation window.

   Example: The following steps are an example of adjusting partition sizes to upgrade a deployment with a /root partition that is 20,000 MB.

   In the **Red Hat Enterprise Linux Server Linux V6.8 for x86_64** section, modify the following partitions:

   a. Select **Swap**, and select the **Reformat** option.

   b. Select **/store**, and enter **/store** in the **Mount Point** field.

   Important: This option is not available in high-availability (HA) deployments.

   c. Select **/storetmp**, and enter **/storetmp** in the **Mount Point** field.

d. Select **/transient**, and enter **/transient** in the **Mount Point** field.

e. Select **/boot**, and enter the new value of **/bootold** in the **Mount Point** field.

f. Delete **/**.

In the **New Red Hat Linux Enterprise V7.X Installation** section, click **+** to create the new RHEL V7.3 partitions:

Important: Click **Update Settings** after you create each partition.

a. Create a `/boot` mount point that is `1024 MiB` in size, with **XFS** for a file system, and **Standard Partition** for the device type.

b. Create a / mount point that is `6672 MiB` in size, with **XFS** for a file system, and **LVM** for the device type.

c. With the **/** partition still selected, click **Modify** under the **Volume Group** button to create a **rootrhel** volume group, and select **Size Policy** > **As large as possible**.

d. Create a `/var` mount point that is `2594 MiB` in size, with **XFS** for a file system, and **LVM** for the device type. Ensure that **rootrhel** is selected for the **Volume Group**.

e. Create a `/opt` mount point that is `6672 MiB` in size, with **XFS** for a file system, and **LVM** for the device type. Ensure that **rootrhel** is selected for the **Volume Group**.

f. Create a `/tmp` mount point that is `1482 MiB` in size, with **XFS** for a file system, and **LVM** for the device type. Ensure that **rootrhel** is selected for the **Volume Group**.

g. Create a /home mount point that is `370 MiB` in size, with **XFS** for a file system, and **LVM** for the device type. Ensure that **rootrhel** is selected for the **Volume Group**.

h. Delete the `/var/log` partition in the **Red Hat Enterprise Linux Server Linux V6.8 for x86_64** section.

Note: Do not select the **Delete all other file systems in the Red Hat Enterprise Linux Server Linux V6.8 for x86_64 root as well** option.

i. Create a new `/var/log` mount point that is `8063 MiB` in size, with **XFS** for a file system, and **LVM** for the device type.

j. With the `var/log` partition still selected, click **Modify** under the **Volume Group** button to create a **varlogrhel** volume group, and select **Size Policy** > **As large as possible**.

k. Create a `/var/log/audit` mount point that is `1651 MiB` in size, with **XFS** for a file system, and **LVM** for the device type. Ensure that **varlogrhel** is selected for the **Volume Group**.

l. Delete the `/bootold` partition in the **Red Hat Enterprise Linux Server Linux V6.8 for x86_64** section. Only three partitions are now listed for RHEL V6.8: `/store`, `/storetmp`, and `/transient`.

m. Create a `biosboot` mount point and accept the default settings.

5. Click **Done** on the **Manual Partitioning** window.
6. Follow the instructions in the wizard to complete the installation:

a) Click **Network & Host Name**.

b) Enter the host name for your appliance.

c) Select the interface in the list, move the switch to the **ON** position, and click **Configure**.

d) On the **General** tab, select the **Automatically connect to this network when it is available** option.

e) On the **IPv4 Settings** tab, in the **Method** list, select **Manual**.

f) Click **Add** to enter the IP address, Netmask, and Gateway for the appliance in the **Addresses** field.

g) Add two DNS servers.

h) Click **Save**, click **Done**, and then click **Begin Installation**.

7. Set the root password, and then click **Finish configuration**.
8. Restart the host after the RHEL V7.3 installation finishes.

Completing the QRadar installation

After you configure RHEL V7.3, complete the IBM Security QRadar installation by preparing for the QRadar installation wizard.

Procedure

1. Use SSH to log in to the system as a root user.
2. Modify the SELINUX value in the `/etc/selinux/config` file to `SELINUX=disabled`, and restart the host.
3. Use SSH to log back in to the system as the root user.
4. Confirm that the `/store` partition is not mounted by typing the following command:

   ```
   mount
   ```

   If the `/store` partition is mounted, unmount the partition by typing the following command:

   ```
   umount /store
   ```

5. Confirm that the `/storetmp` partition is mounted by typing the following command:

   ```
   mount /storetmp
   ```

6. Create the `/media/cdrom` directory by typing the following command:

   ```
   mkdir /media/cdrom
   ```

7. Mount the QRadar ISO by typing the following command:

   ```
   mount /storetmp/731/<QRadar>.iso /media/cdrom
   ```

8. Type the following command to begin the QRadar upgrade:

   ```
   /media/cdrom/setup
   ```

   Note: A new kernel might be installed as part of the upgrade, which requires a system restart. Repeat the commands in steps 4 - 8 after the system restart to continue the upgrade.
9. After the installation finishes, delete the ISO file and clear your browser cache.

What to do next

Log in to QRadar by typing the IP address of the QRadar system into a web browser:

```
https://IP Address
```

The default user name is `admin`.

Chapter 5. Upgrading QRadar on Amazon Web Services

Upgrade IBM Security QRadar V7.2.8 to V7.3.0 on an Amazon Web Services (AWS) instance.

Before you begin

- Download the AWS QRadar Install Helper script from Fix Central (www.ibm.com/support/fixcentral/).
  1. Go to the **Select product** tab.
  2. Set **Product Group** to **IBM Security**.
  3. Set **Select from IBM Security** to **IBM Security QRadar SIEM**.
  4. Set **Installed Version** to **7.3.0** and click **Continue**.
  5. Select **Browse for fixes** and click **Continue**.
  6. Click **SCRIPT**.
  7. Select the AWS QRadar Install Helper script.
- Download the QRadar release ISO file from Fix Central (www.ibm.com/support/fixcentral/).
- Note the private IP and subnet of the V7.2.8 instance.

About this task

Important: You must have QRadar v7.2.8 -QRFULL- 20161118202122 fixpack and later installed before you can upgrade to QRadarV7.3.0. Click **Help** > **About** to view the QRadar version. Download the software fix (https://www-945.ibm.com/support/fixcentral/swg/selectFixes?product=ibm%2FOther+software%2FIBM+Security+QRadar+Risk+Manager&fixids=7.2.8-QRADAR-QRSIEM-20161118202122&source=dbluesearch&function=fixId&parent=IBM%20Security).

Procedure

1. To copy the ISO image to the device, type the following command:

```
scp -i <key.pem> <qradar.iso> ec2-user@<public_IP_address>:
```

2. To mount the ISO image, type the following command:

```
sudo mount -o loop /home/ec2-user/<qradar.iso> /media/cdrom
```

3. Type the following command:

```
sudo sed -i -e 's/plugins=1/plugins=0/' /etc/yum.conf
```

4. To start the setup program, type the following command:

```
sudo /media/cdrom/setup
```

5. When prompted by the setup program:
   a) At rc.local prompt select **2 - Continue and LEAVE rc.local as is**.
   b) When prompted to check users, type Y to delete the user.
6. Stop the instance.
7. Note where any extra (non-root) EBS volumes are mounted, then detach the extra EBS volumes and take a snapshot
8. Terminate the instance.

9. Launch a new RHEL 7.3 instance by using the private IP address and subnet that you noted earlier. Use AMI RHEL-7.3_HVM_GA-20161026-x86_64-1-Hourly2-GP2. Give 100 GB to the root device. No other volumes need be created.
10. Reattach any extra EBS volumes in the same locations that you noted in step 7.
11. To copy the script that prepares the AWS partitions and configuration options to the AWS instance, type the following command:

    ```
    scp -i <key.pem> aws_qradar_prep.sh ec2-user@<public_IP_address>:
    ```

12. To run the script to prepare the AWS partitions and configuration options, type the following command:

    ```
    sudo bash +x ./aws_qradar_prep.sh --upgrade
    ```

    The AWS instance restarts after the script runs.
13. After the restart, make sure that `/storetmp` is mounted, and that `/store` is not mounted.

    If `/store` is mounted, run:

    ```
    sudo umount /store
    ```

14. To mount the ISO image, type the following command:

    ```
    sudo mount -o loop /home/ec2-user/<qradar.iso> /media/cdrom
    ```

15. Run the setup program again by typing the following command:

    ```
    sudo /media/cdrom/setup
    ```

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.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

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

IBM®