opentext™

Recon Appliance
R8000 and R8100 Models

Software Version: 24.2

Administrator's Guide to Hardware Appliances for ArcSight Recon

Legal Notices

Open Text Corporation

275 Frank Tompa Drive, Waterloo, Ontario, Canada, N2L 0A1

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.microfocus.com/support-and-services/documentation

Support

Contact Information

Phone	A list of phone numbers is available on the Technical Support Page: https://www.microfocus.com/en-us/contact-support/stackb
Support Web Site	https://www.microfocus.com/en-us/support
ArcSight Product Documentation	https://www.microfocus.com/documentation/arcsight/#gsc.tab=0

Contents

About this Guide 5
Intended Audience 5
Additional Documentation 5
Contact Information 6
Chapter 1: Overview 7
How the Recon Appliance Works 7
Appliances for Security, Compliance, and IT Applications 8
Chapter 2: Setting Up a Recon Appliance 9
Powering On the Recon Appliance 9
Setting Up the Appliance for Remote Access 10
Changing the iDRAC password on your Appliance 10
Encryption of SEDs 11
Initializing the Recon Appliance 11
First Boot Initialization of the Recon Appliance (Bootstrapping) 11
Regeneration of the First Login Token 14
Configuring Recon 14
Recon Configuration Failure 16
Appliance Licenses 17
Features Included with the License 17
Configuring a Recon Appliance 17
Storage Groups 18
Event Ingestion 18
Firewall 18
Chapter 3: Navigating the User Interface 19
Dashboard 19
Search 19
Insights 19
Configuration 20
Reports 20
ArcMC 21
Admin 22
Chapter 4: Backup and Restore Procedures 23
Appliance Configuration Backup and Restore 23
Appliance Backup Procedures 23
Restoring an Appliance to Factory Settings 23

Restoring an Appliance Using a USB Memory Stick 24
Image Burning 24
Restore Procedure: 24
Restoring an Appliance Using iDRAC Access 25
Restore Procedure: 25
ArcSight Database - Backup and Restore 26
Preparing the ArcSight Database Backup Host 27
Prerequisites 27
Estimating Backup Host Required Storage Space 28
Estimating 28
Freeing up space 28
Setting Up Passwordless SSH 29
29
Preparing the Backup Configuration File 29
Create your own copy of the vbr file 29
Available options 30
Example file 30
Backing Up the ArcSight Database 33
Backing Up the Database 33
Backing Up the Database Incrementally 34
Verifying the Integrity of the Backup 34
Managing ArcSight Database Backups 36
Viewing Available Backups 36
Deleting a Backup 36
ArcSight Database - Restore 36
Chapter 5: Managing the Recon Appliance 39
Restarting the Appliance 39
Publication Status 42
Send Documentation Feedback 43

About this Guide

This installation guide provides instructions on how to install and initialize the standalone Recon appliances:

- Recon R8000: which comprises **48 TB** of available event storage
- Recon R8100: which comprises **160 TB** of available event storage

For more information, see "How the Recon Appliance Works" on page 7.

Intended Audience

This book provides information for admins who need to install, initialize, and restore Recon appliances.

Additional Documentation

This documentation library includes the following resources, based on the product that you use.

ArcSight Platform

- ArcSight Platform 24.2 Release Notes, which provides information about the latest release.
- The Administrator's guide, which provides concepts, use cases, and guidance for installing, upgrade, managing, and maintaining the ArcSight Platform in your environment. See the guide corresponding to your deployment:
  - *Administrator's Guide for the ArcSight Platform 24.2 - Off-Cloud Deployment*
- Technical Requirements for ArcSight Platform 24.2, which provides information about the hardware and software requirements for installing ArcSight Platform and the deployed capabilities in your environment.
- *ArcSight Platform Upgrade Paths*, which provides information about the paths to upgrade to the latest release from your current release.
- *ArcSight Solutions and Compliance Insight Packages*, which provide a complete set of compliance and audit related packages and documentation.
- *Documentation* site for ArcSight Platform where you can discover documentation for multiple ArcSight products.

Contact Information

We want to hear your comments and suggestions about this book and the other documentation included with this product. You can use the comment on this topic link at the bottom of each page of the online documentation, or send an email to Documentation-Feedback@microfocus.com.

For specific product issues, contact OpenText Customer Care.

Chapter 1: Overview

ArcSight Recon provides a modern **log management and compliance** solution powered by a high-performance, column-oriented, clustered database. R8000 and R8100 are the hardware appliances custom built for ArcSight Recon.

Recon features include:

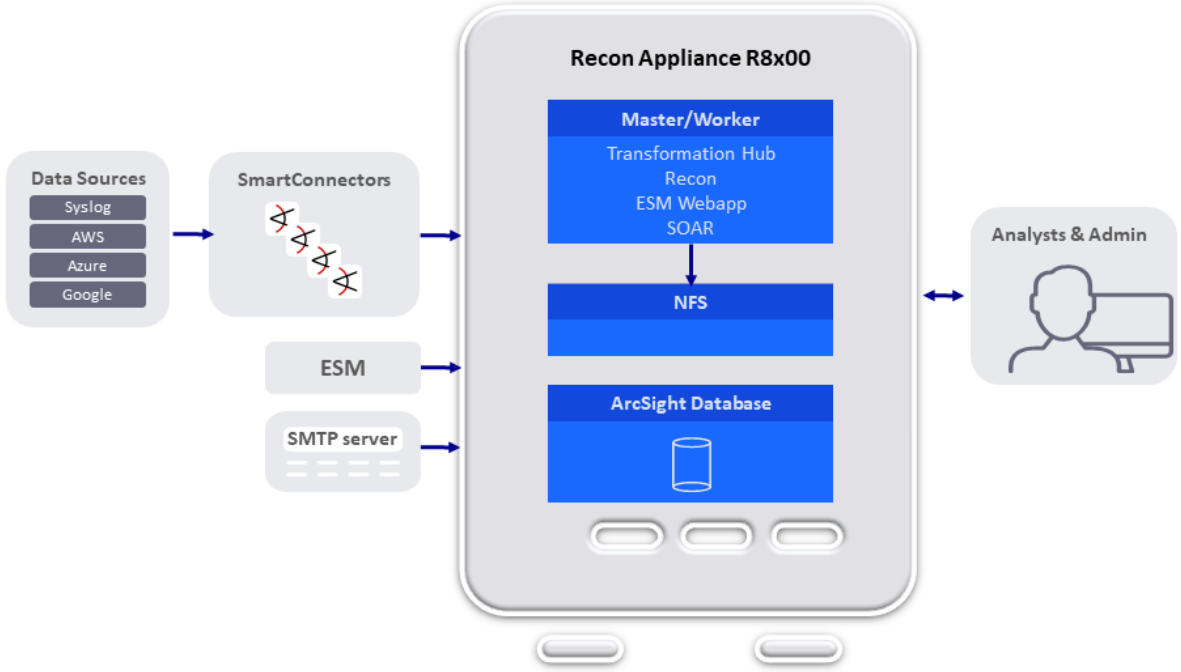
- Search, which helps you investigate security issues by viewing search results and identifying outlier events.
- The Reports Portal, which includes OWASP content, and enables you to hunt for undetected threats as well as create charts and dashboard to visualize filtered data with tables, charts, and gauges.
- Outlier Analytics, which allows you to identify anomalous behavior by comparing incoming event values to typical values for your environment.
- Ingestion, which is handled by SmartConnectors. Large amounts of heterogeneous raw event data are collected from security devices in an enterprise network, and SmartConnectors publish the events to Transformation Hub topics. Recon takes the events from Transformation Hub's Kafka cluster to perform the analysis.
- Event Integrity Check, which validates that the event information in your database matches the content sent from the SmartConnectors.
- ArcSight Database, which supports the searches and analysis capabilities. The database stores the collected events and enforces their immutability, ensuring that not even the most privileged database administrator can modify or delete an event. Combined with the existing Event Integrity Check, the database's ability to resist tampering provides an end-to-end, long-term solution for safeguarding events to ensure they are exactly as reported by the device where the activity was observed.
- Storage capacity, which allows the appliance to self-contain the ArcSight Database and the Recon functionalities. A Recon R8000 comprises a storage capacity of **48 TB**, and a Recon R8100 comprises a storage capacity of **160 TB**.

The purpose of this guide is to help you perform the initial configuration of your Recon appliance, so that you can start taking advantage of all its features. For more information on the usage and settings of specific features, please refer to the User's Guide for ArcSight Platform CE 24.2

How the Recon Appliance Works

Each appliance consists of a **single-node** version of Recon, such that the master node, worker node and database node are collocated. The nodes are pre-configured with labels to indicate the type of workload that can run on it. You don't need to modify any settings, such as labels, or add nodes, etc.

Being a single-node box, the Recon appliance doesn't support high availability



The appliance works with the ArcSight Database in **Enterprise** mode. For more information, see **Architecture** in the ArcSight Database 24.1 Guide.

Appliances for Security, Compliance, and IT Applications

Although Recon's applicability spans a wide array of industries, its search, reporting, and alerting capabilities are directly applicable to security and compliance reporting, and for IT operations search.

Recon ships with predefined content filters that define queries for commonly searched security, IT operations, and application development events. These include unsuccessful login attempts, the number of events by source, and SSH authentications on UNIX servers. Therefore, you do not need to define queries to search for many commonly searched events. You can also copy the predefined content filters and modify them to suit your needs, thus saving the time and effort required to start writing queries from scratch. In addition, Recon also contains predefined reports for common security and device monitoring use cases.

Chapter 2: Setting Up a Recon Appliance

This section describes how to rack mount your Recon R8000 and R8100 Appliances. You do not need to run an installer when setting up your appliance; the software comes pre-installed on it. These basic steps enable you to start using your Recon appliances.

	Task	See
❑	1. Power on the Appliance	"Powering On the Recon Appliance" below
❑	2. Set up Remote Access	"Setting Up the Appliance for Remote Access" on the next page
❑	3. (Optional) Encryption of SEDs	"Encryption of SEDs" on page 11
❑	4. Appliance Initialization	"Initializing the Recon Appliance " on page 11
❑	5. Appliance Licenses	"Appliance Licenses" on page 17
❑	6. Appliance Configuration	"Configuring a Recon Appliance" on page 17

Powering On the Recon Appliance

Before you Begin:

Redeem your license key by following the instructions in the documents you received when purchasing. Redeeming this key gets you the license that you need to access Recon functionality.

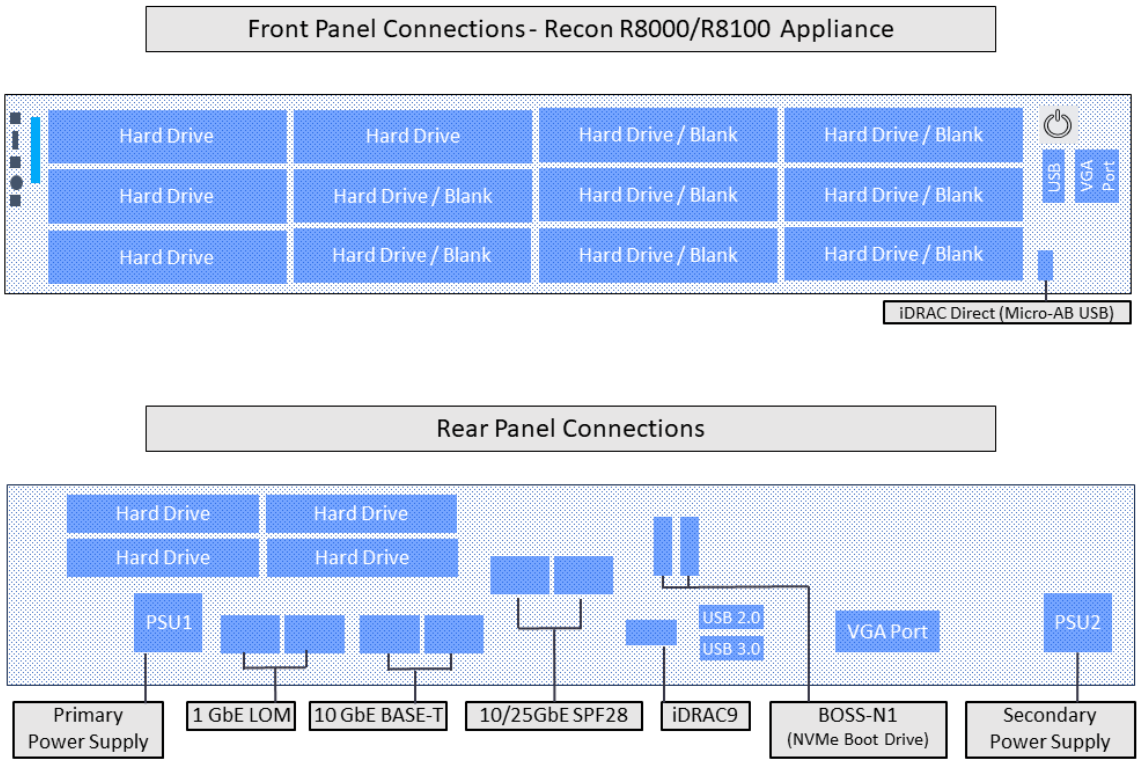
To install the appliance:

1. Unpack the appliance and its accompanying accessories.

   Note: Read carefully through the instructions, cautions, and warnings that are included with the appliance shipment. Failing to do so can result in bodily injury or appliance malfunction.

2. Follow the rack installation instructions to securely mount it.

3. Make the front and rear panel connections. The diagram below offers a general view of the basic connections:



4. Power on the appliance.

Setting Up the Appliance for Remote Access

All appliances are equipped with an `iDRAC Service Module (iSM)` for remote access. OpenText strongly recommends setting up and configuring your appliance for out-of-band remote access. Doing so ensures that you or Customer Support (with your permission and assistance) can remotely access the console of your appliance for troubleshooting, maintenance, and control over the powering on and off of the box.

Changing the `iDRAC` password on your Appliance

Appliance boxes come with a random `iDRAC` password. For information on how to locate the password, see Secure Default Password.

This is a unique password, which will be required the first time `iDRAC` is accessed. The appliance then will prompt for a new password to be chosen. For security reasons, OpenText recommends to change this password as soon as possible.

To set up your appliance for remote access, follow the instructions in the EMC iDRAC Service Module.

Encryption of SEDs

The Recon Appliances support FIPS enabled self-encrypting disks (SEDs).

A SED is a data storage device with built-in cryptographic processing to encrypt and decrypt the data it contains. This process occurs within the device itself, independent of any connected information system, and it provides data protection against the loss or theft of the disks, as well as certain levels of hacking attempts.

This protection consists of setting up passphrase-access-only.

The SEDs ship without the passphrase, allowing you to chose your own. To set up a passphrase, first follow the steps to establish a security key.

The chosen passphrase can then be applied to pre-existing virtual disks by following the steps in Secure a pre-existing virtual disk.

To change or disable a security key, please follow the specific procedures listed under this section.

Initializing the Recon Appliance

The initialization of a Recon appliance consists of two parts: the first boot (bootstrapping) of the process through the console, and the installation of the software through the appliance UI.

First Boot Initialization of the Recon Appliance (Bootstrapping)

Tip: Be aware that this process will require network information for the appliance, such as:

- Static IP address
- Resolvable FQDN hostname
- NTP server that's both accessible and running

All of this information must be available to successfully complete the bootstrapping.

1. Log into your appliance using iDRAC (see "Setting Up the Appliance for Remote Access" on the previous page for instructions), and launch the Virtual Console.
2. Turn on the appliance using the Power Controls option, in case the appliance is off.

3. Using the local drive (NVMe), select from the menu the version of Red Hat you want to boot from.
4. From the console, login using your default username (arcsight) and password (change_me).
5. Once the default credentials are entered, you will be asked to change the password for arcsight:

```
You are required to change your password immediately (administrator
enforced).
Current password:
New password:
Retype new password:
```

> **Note:** The STIG-compliant password policy rules for both the arcsight and the root password require:
>
> - A minimum of 15 characters
> - A minimum of 1 number
> - A minimum of 1 lowercase character
> - A minimum of 1 uppercase character
> - A minimum of 1 special character
> - A maximum of 2 consecutive repeating characters
> - A maximum of 4 consecutive repeating characters of the same class
> - A minimum of 8 different characters
> - To not be a word from the dictionary
> - To be different from the last seven passwords

6. The **OpenText Appliance** splash screen will appear, with the **User must set 'root' password to proceed** message. You will be required to enter the arcsight user password you just reset to make the change to the root password:

```
password for arcsight
Changing password for user root.
New password:
Retype new password:
passwd: all authentication tokens updated successfully
```

> Once your passwords have been set, you will need to wait for at least one day to update to a different one. And the maximum expiration period for a password is 60 days.

7. Complete the **Network Configuration**. The screen will display a list of network interfaces and their status:

```
**********************************************************************
Network Configuration
**********************************************************************
WARNING: You must specify static IP address and resolvable hostname
(FQDN).
**********************************************************************
List of network interfaces
**********************************************************************
enoxxxxnp0      UP             xx:xx:xx:xx:xx:xx       <BROADCAST, MULTICAST, UP, LOWER
enoxxxx         DOWN            xx:xx:xx:xx:xx:xx       <NO-CARRIER, BROADCAST, , MULTI
ensxxxx         DOWN            xx:xx:xx:xx:xx:xx       <NO-CARRIER, BROADCAST, MULTICA

**********************************************************************
Select one active connection to configure:
**********************************************************************
1) enoxxxxnp0
#? 1
```

Select the number of the active connection you want to configure.

8. Configure the network using a static IP address by providing this information:

```
**********************************************************************
Configure the network connection enoxxxxnp0 for device enoxxxxnp0:
**********************************************************************
Enter the hostname (FQDN) for this appliance: your_appliance_host_fqdn

Configure network using static IP address:
Enter static IPv4 address:
Enter IPv4 prefix (1-32):
Enter IPv4 gateway:
Enter IPv4 Primary DNS server:
Enter IPv4 Secondary DNS server (optional):
Enter spaced separated IPv4 DNS search domains: your_appliance_domain
```

9. Next, the NTP server must be configured:

```
**********************************************************************
NTP Server Configuration
**********************************************************************
WARNING: You must specify an accessible NTP server

Enter the NPT server for this appliance:
```

Once all this information has been provided, the console will display a summary of the network configuration and NTP server configuration, and will ask you to verify by entering Y:

```
Do you want to configure network settings and NTP services using above
configuration? (Y/N)
```

If you need to correct the information, enter `N`, and the process will ask you for each item again. If you enter `Y`, the process will continue:

```
Generate self-signed certificate and first time login token...
```

To proceed, you will be asked for the `root` password again, as confirmation.

10. If the configuration ends successfully, you will see the following message:

```
**********************************************************************
The appliance network and NTP server have been setup successfully
**********************************************************************
Go to https://<your_appliance_host_fqdn>:6443 to install Recon product
IMPORTANT: You will need the token to login for the first time:
xxxxxxxx
**********************************************************************
```

> ✔ The console will not allow you to copy the token, which you will need for your first login to the **Recon Installer Web App**. Access the URL provided above in your browser, and type the token manually as shown in the console.

Regeneration of the First Login Token

In case there's a need to obtain a First Login Token again (other than with the preceding procedure), you can regenerate it by running the following command in the console:

```
# /var/opt/arcsight/appliance_scripts/generate_first_login_token.sh
```

You will be prompted for the `arcsight` password, and after providing it, the First Login Token will be generated again:

```
================================================================
Go to https://<your_appliance_host_fqdn>:6443 to install Recon product
IMPORTANT: You will need the token to login for the first time:
xxxxxxxx
================================================================
```

Configuring Recon

The first time you connect to the appliance, you will need to accept the end user license agreements, and provide basic setup information.

Follow these steps to configure your Recon appliance the first time:

All through this process, you might see confirmation pop-ups, letting you know that the operation has concluded or started successfully.

1. Open a browser to access the following URL:

   ```
   https://<your_hostname>:6443
   ```

2. At the **Welcome** screen, set up your **Username** and **Password**, and provide your **Token** (which you obtained at the end of the "First Boot Initialization of the Recon Appliance (Bootstrapping)" on page 11 procedure), to begin the process.

   Click the Create User button to proceed.

3. The next screen will require your newly created **Username** and **Password** retyped. Click the Log in button to proceed.

4. The Recon Appliance Set up Wizard will guide you through the installation process. The first screen will display the **OpenText End User License Agreement**. You must scroll down to the end of the agreement and click the I have read and agree with the end user license agreements for the Next button to allow you to proceed.

   Every screen in this process will also have a Log out button on the right upper corner. Logging out will bring up the initial Login screen, but if you had already initiated a process (install or uninstall), the process will proceed behind the scenes even if you log out.

5. The second screen will display the **Red Hat End User License Agreement** for your perusal. You must scroll down to the end of the agreement, and click the I have read and agree with the end user license agreements for the Next button to allow you to proceed.

6. Next, the Application Setup screen will prompt you for the following information:

   - `Application administrator username`: this is a hardcoded value for the `OPTIC Management Toolkit (OMT)` username (`admin`).
   - Password for the application admin: your password for the `Admin` OMT username. The password requirements will be listed under the password box. Confirm the password by reentering it.
   - `Database administrator username`: this is the value for the ArcSight Database username (`dbadmin` user).
   - DB admin password: your password for the `dbadmin` database username. Confirm the password by reentering it.

   Click Next.

   The next screen will present the information you just provided, for review. Click the Submit information button if everything looks correct, or the Previous button for corrections.

7. The setup process will proceed without any more user intervention, and it will take around 20 minutes to complete. You can select for the setup to proceed with or without on-screen logs.

   If the installation fails, you will need to reboot the machine to restart the process. Follow these instructions in case of an installation failure.

8. Once the process is completed successfully, you will arrive at a screen with the following message: **You have successfully set up your appliance. Use the URL below to log into the ArcSight Platform application**.

   Click the Copy URL button and paste the URL into your browser to start using your appliance.

9. The URL you obtained from the process will bring you to the start screen, where you must provide your:

   - First Name
   - Last Name
   - Email
   - Password

   This information is used to establish your `admin user`. Click the Create System Admin button to proceed.

Recon Configuration Failure

A configuration failure is highly unlikely, but if it should happen, follow this procedure to attempt it again.

1. If the configuration fails, you will land on a screen that shows the next message:

   ```
   The appliance setup was unsuccessful.  The logs below contain information
   about this failure.
   Please click the Uninstall button to revert the installation.
   ```

   Click the Uninstall button to proceed to the Uninstalling screen.

2. The uninstalling process can have two outcomes:

   - Success, which will take you to a screen with the following message:

     ```
     The uninstalling process has concluded successfully. Click the Reboot
     Appliance button to attempt the installation again (rebooting will take
     around 3 minutes)
     ```

     Clicking the Reboot Appliance button will take you to the Reboot in process… please hold! screen. Wait for around 5 minutes, and refresh your browser.

Once the reboot is done, you will return to the Review Information screen, which has preserved all the configuration information you have provided.

Click the Submit information button and go back to the configuring procedure.

- Failure, which will take you to a screen with the following message:

```
The appliance setup was unsuccessful.  The logs below contain
information about this failure.
Please click the Retry Uninstall button to revert the installation.
```

Clicking the Retry Uninstall button will repeat the procedure described in this page. The repeated process can have the same outcomes, success or failure.

If the uninstalling process fails after several tries, you will land on a screen with this message:

```
The appliance installation has failed 3 times, the maximum number of
allowed attempts.
Please contact OpenText tech support for assistance:
https://www.microfocus.com/en-us/support/contact-support/
```

Appliance Licenses

Redeem your license on the Software Entitlements Portal, then download the license file to a computer from which you can connect to Recon. For more information, refer to the software delivery confirmation email you received from OpenText.

For instructions on how to install your license key, see:

Installing Your License Key

Features Included with the License

For more information regarding what's included in your license refer to the following topics:

Understanding the Types of Licenses

How Your License Affects Data Storage Policies

Configuring a Recon Appliance

The links provided for each feature are meant as a starting point, and not meant to be exhaustive. You will find more in depth information in the User's Guide for ArcSight Platform CE 24.2.

The installation and initialization process sets up your appliance with an initial configuration described in the sections below. You can perform additional configuration on the appliance to adapt to your environment needs.

If you have installed multiple Recon appliances, connect to and configure each one separately.

Storage Groups

In a Recon appliance, Storage Groups allow you to divide data into categories, each supporting different retention policies.

For more information see:

- Use Storage Groups to Organize and Retain Data
- Configure Retention Policies for Your Data

You can monitor the storage utilization with the Health and Performance Monitoring Dashboard. If the storage utilization reaches 90%, the watchdog script will automatically drop the oldest partition to ensure that the appliance can continue ingesting new events.

Event Ingestion

The Recon appliance harnesses the Transformation Hub capabilities to receive events from SmartConnectors.

See Producing Events with SmartConnectors for more information.

Firewall

The firewall for the Recon appliance comes pre-configured, with the following ports open by default to facilitate the initial setup:

Port	Protocol	Description
22	HTTPS	Used by the appliance installer
6443	HTTPS	Used by the appliance installer

The rest of the ports required for the appliance's normal functions (such as for infrastructure, capabilities and supported components), are listed here.

Chapter 3: Navigating the User Interface

A menu on the left side of the user interface allows you to access all the available Recon options:

Dashboard

The Dashboard is where you land after logging into the Recon appliance. It displays a list of dashboards, indicating **NAME**, **SHARING** (whether it's private or shared) and **OWNER** for each.

For more information see:

- Creating and Using ArcSight Dashboards
- Viewing a Dashboard

Search

The Search tab allows you to set up queries to probe through your data.

For more information see:

- Searching for Events
- Understanding Search
- Creating and Saving Searches
- Viewing and Managing Your Searches
- Scheduling Regular Runs of a Search

Insights

The Insights tab provides detailed information gathered about your data.

The following topics provide information to understand the Insights for Outliers:

- Analyzing Anomalous Data with Outlier Analytics
- Generating Models to View Anomalous Data

The following topics provide information to understand the Insights for Data Quality:

- Managing the Quality of Your Data
- Understanding the Data Quality Insights
- Understanding How Data Quality is Calculated
- Analyzing Data Quality

Configuration

The Configuration tab allows you to change the settings for the following Recon features:

- Outlier Configuration

  For more information see:

  - Define and Build a Model
  - Score a Model
- Storage Information

  For more information see:

  - Managing Your Stored Data
  - Use Storage Groups to Organize and Retain Data
- Event Integrity

  For more information see:

  - Checking the Integrity of Event Data
  - Understand the Event Integrity Check
- Import Logger Data

  For more information see:

  - Migrating Logger Data to the ArcSight Database
  - Importing Event Data From Logger
  - Importing Logger Data to the ArcSight Database (non-SaaS)

Reports

The Reports tab contains the following sections:

- Portal: To access all available reports and dashboards

  For more information see:

    - Accessing Reports and Dashboards in the Reports Portal
    - Specify Your Default Dashboards for the Reports Portal
- Dashboard Designer: To create interactive dashboards

  For more information see:
    - Create Additional Dashboards and Reports
      - Customize Your Dashboards
- Report Designer: To create reports

  For more information see:
    - Designing Reports for Data Analysis
    - Create a Simple Report
- Scheduler: To create and managed scheduled reports

  For more information see:
    - Create a Simple Scheduled Report
    - Scheduling Report Generation
- Content: To import and export report content

  For more information see:
    - Adding and Removing Reports Content
    - Import and Export Content

Each of these features opens in a new browser tab, with their own options.

ArcMC

The ArcMC tab contains the following sections:

- ArcMC: View the health and status of products managed by ArcMC

  For more information see:
    - Accessing ArcMC
    - Accessing ArcMC Dashboards
- Bulk Operations: Manage multiple host systems

  For more information see:
    - Accessing Bulk Operations

Admin

The Admin tab contains the following sections:

- Users and groups:

  For more information see:

  - Managing Users and Groups of Users
  - View a User's Profile
- Roles and Permissions:

  For more information see:

  - Review Your Roles and Permissions
  - Assigning Permissions to Roles

Chapter 4: Backup and Restore Procedures

OpenText recommends to perform backups of the information and configuration of a Recon appliance to ensure you can recover your data in case of loss.

Components should be backed up on a regular schedule, as well as before you upgrade your environment.

Appliance Configuration Backup and Restore

Appliance Backup Procedures

The following procedures will create a backup of each specific appliance component:

- Backing Up and Restoring Core Secrets
- Backing Up and Restoring Kubernetes Data for Off-Cloud Deployments
- Backing Up and Restoring Configuration Data for Deployed Capabilities
- Backing Up and Restoring the Postgres Database

Restoring an Appliance to Factory Settings

You can restore appliances to their original factory settings by using the procedures detailed here. To perform a restore procedure, you will require:

- An `.iso` image file containing the factory settings for the version of Recon you are restoring. Find the name of the file in the **Downloading the ArcSight Platform Installation Files** section of the ArcSight Platform 24.2 Release Notes.

  Once you have acquired the image file, please refer to the signature verification instructions, and perform the verification steps before starting the procedure below

The restore procedure can be conducted in two ways:

- If you have physical access to the appliance, use the "Restoring an Appliance Using a USB Memory Stick" on the next page method
- If you have only `iDRAC` access to the appliance, use the "Restoring an Appliance Using iDRAC Access" on page 25 method

Restoring an Appliance Using a USB Memory Stick

This method will require the following external hardware:

- A 32 GB or higher USB memory stick (the faster type available, but at least USB 2.0 or 3.x)
- A Linux machine to perform the burning of the .iso image into the USB memory stick

Image Burning

1. Connect the USB memory stick to one of the ports of the Linux machine.
2. From the command line, execute the following command to burn the `.iso` image into the USB memory stick:

   ```
   dd if=<iso_image_file_name>.iso status=progress oflag=sync of=/dev/sdb
   bs=1M
   ```

   Where `<iso_image_file_name>` is the name of the image file downloaded here.

   And wait until the progress has reached 100%.
3. Turn your appliance off and connect the bootable USB stick you just created to one of its ports. Reboot the appliance.

Restore Procedure:

1. Access the remote console of the appliance through `iDRAC`.

   If you already used the remote access, use the password you setup the first time you connected. Otherwise, for instructions see:

   "Setting Up the Appliance for Remote Access" on page 10
2. From the `iDRAC` **Dashboard**, select the **Virtual Console** on the right lower corner.
3. Click the **BOOT** button on the upper right hand corner and select the **BIOS Boot Manager** option.

   A pop-up window will request to **Confirm Boot Action**, setting a new device to boot from. Select **Yes**.
4. The previous step will not initiate the reboot automatically. For that, you will need to click the **POWER** button, and from the **Power Control** pop-up window, choose the **Reset System (warm boot) option**.

   A pop-up window will request to **Confirm Power Action**. Select **Yes**.
5. The booting process will prompt a selection from the **Boot Manager**. Choose **One-shot UEFI Boot Menu**.
6. From the **Select UEFI Boot Option**, select your USB stick (its name will depend on brand and model, but it will start with **Disk connected to back USB**).

7. The appliance will boot from the selected USB stick.

   The restore process will start automatically if you allow it some time, or you can click on the **ArcSight User Image RECON-R7615-R8X00-RH92-FIPS-STIG-XXXXXX.iso** option at the top to start right away.

   Twice during this process you will receive a warning about all the data in the partition or hard disk being overwritten. You must enter `Y` to proceed both times:

   ```
   Are you sure you want to continue? (y/n)
   ```

8. Different screens will follow each other, some of them with progress bars, indicating the restoring progress of a specific system portion. None of these require user intervention, and the whole process takes approximately 10 minutes. Once the restore process has reached this point:

   ```
   realtime =none
   The next step: true
   Now run: true
   ```

   Your input will be required to reboot the appliance:

   ```
   reboot
   ```

9. Once the reboot process is finished, follow the instructions listed in:

   "Initializing the Recon Appliance " on page 11

Restoring an Appliance Using iDRAC Access

When using the `iDRAC` Remote File Share feature to perform the restore procedure, make sure there is no USB drive connected to the appliance ports, since its presence may interfere with the restore process.

This method will require the following preparation:

- Store your `.iso` image in a location that is accessible to the `iDRAC` network. For more information, see the iDRAC documentation.
- Configure the `iDRAC` Remote File Share option in the Virtual Media tab using shared the `.iso` image downloaded here.

Restore Procedure:

1. Access the remote console of the appliance through `iDRAC`.

   If you already used the remote access, use the password you setup the first time you connected. Otherwise, for instructions see:

   "Setting Up the Appliance for Remote Access" on page 10

2. From the iDRAC **Dashboard**, select the **Virtual Console** on the right lower corner.
3. Click the **BOOT** button on the upper right hand corner and select the **BIOS Boot Manager** option.

   A pop-up window will request to **Confirm Boot Action**, setting a new device to boot from. Select **Yes**.
4. The previous step will not initiate the reboot automatically. For that, you will need to click the **POWER** button, and from the **Power Control** pop-up window, choose the **Reset System (warm boot) option**.

   A pop-up window will request to **Confirm Power Action**. Select **Yes**.
5. The booting process will prompt a selection from the **Boot Manager**. Choose **One-shot UEFI Boot Menu**.
6. From the **Select UEFI Boot Option**, select **Virtual Optical Drive**.
7. The appliance will boot from the .iso image in the Remote File Share.

   The restore process will start automatically if you allow it some time, or you can click on the **ArcSight User Image RECON-R7615-R8X00-RH92-FIPS-STIG-XXXXXX.iso** option at the top to start right away.

   Twice during this process you will receive a warning about all the data in the partition or hard disk being overwritten. You must enter Y to proceed both times:

   ```
   Are you sure you want to continue? (y/n)
   ```
8. Different screens will follow each other, some of them with progress bars, indicating the restoring progress of a specific system portion. None of these require user intervention, and the whole process takes approximately 10 minutes. Once the restore process has reached this point:

   ```
   realtime =none
   The next step: true
   Now run: true
   ```

   Your input will be required to reboot the appliance:

   ```
   reboot
   ```
9. Once the reboot process is finished, follow the instructions listed in:

   "Initializing the Recon Appliance " on page 11

ArcSight Database - Backup and Restore

The **Enterprise** Mode of the ArcSight Database stores data in the appliance's file system, optimizing it for analytic speed.

The appliance's ArcSight Database is self-contained, and cannot be expanded.

For more information, see **Architecture** in the ArcSight Database 24.1 Guide.

As a best practice, you should routinely back up the ArcSight Database data.

Preparing the ArcSight Database Backup Host

The recommendation for each backup host size depends on your version of the Recon appliance:

- For an R8000 appliance, assuming that the maximum database size is 80% of the available disk storage, you will need at a minimum 77 TB of disk storage on the backup host (that amount represents twice the size of a database occupying 80% of the available storage).
- For an R8100 appliance, you will need 258 TB at a minimum.

You can perform backups on `ext3`, `ext4`, and XFS file systems.

	Task	See
❑	1. Prerequisites	"Prerequisites" below
❑	2. Estimate the Required Storage Space	"Estimating Backup Host Required Storage Space" on the next page
❑	3. Setup Passwordless SSH	"Setting Up Passwordless SSH" on page 29
❑	4. Prepare the Backup Configuration File	"Preparing the Backup Configuration File" on page 29

Prerequisites

Consider the following when backing up and restoring the ArcSight Database:

- The backup process can consume additional storage. The amount of space that the backup consumes depends on the size of your catalog and any objects (tables or schemas) you decide to exclude from the backup. The backup process releases this storage after the backup is complete.

  See [misc] in the ArcSight Database 24.1 Guide for more information on the inclusion or exclusion of database objects during a backup.

- The ArcSight Database supports restoration to a database that is no more than one minor version higher than the current database version. For example, you can restore objects from a `23.3` database to a `24.1` database, but not to a database version higher than that.
- You can perform backups on `ext3`, `ext4`, and `XFS` file systems.

Estimating Backup Host Required Storage Space

When saving data backups, consider the disk requirements for historical backups at your site. Multiple archives potentially require more disk space than a single archive. It is recommended for each backup host to have enough space for at least twice the database node footprint size.

Appliance model	Available Event storage space	Backup storage space needed for 80% event storage	Backup storage space needed for 90% event storage (maximum allowed)
R8000	48 TB	77 TB	87 TB
R8100	160 TB	258 TB	290 TB

Estimating

To estimate the database size, use the `used_bytes` column of the `storage_containers` system table as in the following example:

```
=> SELECT SUM(used_bytes) FROM storage_containers WHERE node_name='v_fusiondb_
node0001';
```

Example output:

```
total_size
------------------
302135743
(1 row)
```

If you are storing more than one archive or keeping many restore points, the required storage space will increase.

Freeing up space

If you are running out of disk storage on the backup host, you can review the available backups and delete some of them to free up space. For more information, see "Deleting a Backup" on page 36.

Setting Up Passwordless SSH

Remote backup hosts must have SSH access, and you must setup passwordless SSH on the remote backup host for the `dbadmin` user to access the remote backup host from the ArcSight Database.

1. Log in to the backup server.
2. Create the `$dbadmin` user, to be the database administrator.
3. Ensure that `$dbadmin` has write permission to the dedicated directory where you will store the backup.
4. Copy the `authorized_keys` from the database server:

   ```
   /home/dbadmin/.ssh/authorized_keys*
   ```

   To the backup_server:

   ```
   /home/dbadmin/.ssh/
   ```

5. Ensure that the backup server `authorized_keys` (`/home/dbadmin/.ssh/authorized_keys*`) have identical ownership as the database server's `authorized_keys` (`/home/dbadmin/.ssh/authorized_keys*`).

Preparing the Backup Configuration File

The ArcSight Database includes sample configuration files that you can copy, edit, and deploy for your various *vbr* tasks.

The database automatically installs these files at:

```
/opt/vertica/share/vbr/example_configs
```

For more information, see **Sample vbr configuration files** in the ArcSight Database 24.1 Guide.

For a database configuration backup and restore procedure, the sample configuration file to be used is `backup_restore_full_external.ini`.

Create your own copy of the `vbr` file

Execute these commands from the database node:

```
su - $dbadmin
```

```
cp /opt/vertica/share/vbr/example_configs/backup_restore_full_external.ini db_
backup.ini
```

```
vi db_backup.ini
```

You must save a copy of `db_backup.ini` for future tasks.

Available options

The following options are available for the backup configuration file:

- The default for the number of restore points is 52, assuming a weekly backup for one year. Using multiple restore points gives you the option to recover from one of several backups. For example, if you specify 3, you have 1 current backup and 3 backup archives. The Database stores the value you enter as the `restorePointLimit` parameter in the `vbr` configuration file.
- To avoid prompting in the future, the backup configuration can save the `$dbadmin` password.
- Advanced options allow additional security measures, but our recommendation is to use the default options.

Example file

The following is an example to be used for reference only. The values for the node (`v_fusiondb_node0001`) and the database (`dbName`) are hardcoded.

```
; This sample vbr configuration file shows full or object backup and restore
to a separate remote backup-host for each respective database host.
; Section headings are enclosed by square brackets.
; Comments have leading semicolons (;) or pound signs (#).
; An equal sign separates options and values.
; Specify arguments marked '!!Mandatory!!' explicitly.
; All commented parameters are set to their default value.

; ----------------------------------------- ;
;;; BASIC PARAMETERS ;;;
; ----------------------------------------- ;

[Mapping]
; !!Mandatory!! This section defines what host and directory will store the
backup for each node.
; node_name = backup_host:backup_dir
; In this "parallel backup" configuration, each node backs up to a distinct
external host.
```

```
; To backup all database nodes to a single external host, use that single
hostname/IP address in each entry below.
v_fusiondb_node0001 = 192.168.1.1:/opt/dbadmin/backups

[Misc]
; !!Recommended!! Snapshot name.  Object and full backups should always have
different snapshot names.
; Backups with the same snapshotName form a time sequence limited by
restorePointLimit.
; SnapshotName is used for naming archives in the backup directory, and for
monitoring and troubleshooting.
; Valid characters: a-z A-Z 0-9 - _
snapshotName = backup_snapshot

[Database]
; !!Recommended!! If you have more than one database defined on this Vertica
cluster, use this parameter to specify which
database to backup/restore.
dbName = fusiondb

; If this parameter is True, vbr prompts the user for the database password
every time.
; If False, specify the location of password config file in 'passwordFile'
parameter in [Misc] section.
dbPromptForPassword = True

; If true, vbr attempts to connect to the database using a local connection.
; dbUseLocalConnection = False

; ---------------------------------------- ;
;;; ADVANCED PARAMETERS ;;;
; ---------------------------------------- ;

[Misc]
; The temp directory location on all database hosts.
; The directory must be readable and writeable by the dbadmin, and must
implement POSIX style fcntl lockf locking.
tempDir = /tmp

; Specifies the number of historical backups to retain in addition to the most
recent backup.
; 1 current + n historical backups
restorePointLimit = 52

; Full path to the password configuration file
; Store this file in directory readable only by the dbadmin
; (no default)
```

```
# passwordFile = /home/dbadmin/vbr/pw.txt

; When enabled, Vertica confirms that the specified backup locations contain
; sufficient free space and inodes to allow a successful backup. If a backup
; location has insufficient resources, Vertica displays an error message
explaining the shortage and
; cancels the backup. If Vertica cannot determine the amount of available
space
; or number of inodes in the backupDir, it displays a warning and continues
; with the backup.
enableFreeSpaceCheck = True

[Transmission]
; Specifies the default port number for the rsync protocol.
port_rsync = 50000

; Total bandwidth limit for all backup connections in KBPS, 0 for unlimited.
Vertica distributes
; this bandwidth evenly among the number of connections set in concurrency_
backup.
total_bwlimit_backup = 0

; The maximum number of backup TCP rsync connection threads per node.
; Optimum settings depend on your particular environment.
; For best performance, experiment with values between 2 and 16.
concurrency_backup = 2

; The total bandwidth limit for all restore connections in KBPS, 0 for
unlimited
total_bwlimit_restore = 0

; The maximum number of restore TCP rsync connection threads per node.
; Optimum settings depend on your particular environment.
; For best performance, experiment with values between 2 and 16.
concurrency_restore = 2

; The maximum number of delete TCP rsync connection threads per node.
; Optimum settings depend on your particular environment.
; For best performance, experiment with values between 2 and 16.
concurrency_delete = 16

[Database]
; Vertica user name for vbr to connect to the database.
; This setting is rarely needed since dbUser is normally identical to the
database administrator
dbUser = dbadmin
```

Backing Up the ArcSight Database

The database backup server and database server must be on the same OS.

The backup procedure must be performed by the `$dbadmin` user.

	Task	See
❑	1. Database Backup	"Backing Up the Database" below
❑	2. Incremental Database Backup	"Backing Up the Database Incrementally" on the next page
❑	3. Verify the Integrity of the Backup	"Verifying the Integrity of the Backup" on the next page

Backing Up the Database

1. Log into the database node as `root`.
2. Initialize the backup locations:

```
su - $dbadmin
```

```
/opt/vertica/bin/vbr --task init --config-file db_backup.ini
```

3. To back up the data, run the following commands:

```
su -l $dbadmin
/opt/vertica/bin/vbr --task backup --config-file db_backup.ini
Enter the vertica password:
Starting backup of database fusiondb.
Participating nodes: v_fusiondb_node0001.
Snapshotting database.
Snapshot complete.
Approximate bytes to copy: 3206846934901 of 3206846934901 total.
[==================================================.] 99%Copying backup
metadata.
Finalizing backup.
[==================================================] 100%
Backup complete!
```

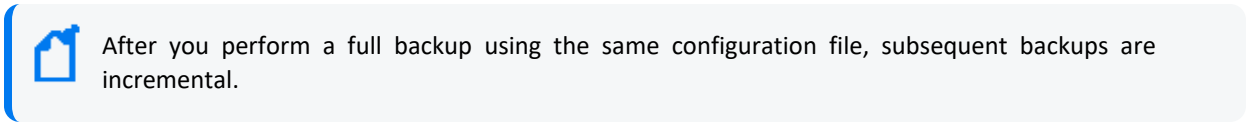
4. Verify that the backup files were written to the backup location by running the following commands:

```
ssh backup server
su - dbadmin
cd /opt/dbadmin/backups
ls -l
```

Example output:

```
-rw-------.   x dbadmin dbadmin x xxx  x xx:xx backup_manifest
drwx------.   x dbadmin dbadmin x xxx  x xx:xx Objects
drwx------.   x dbadmin dbadmin x xxx  x xx:xx Snapshots
```

Backing Up the Database Incrementally



After you perform a full backup using the same configuration file, subsequent backups are incremental.

Incremental backups use the same setup as a full backup and only back up what changed from the previous full backup.

When you start an incremental backup, the `vbr` tool displays a backup size that is a portion of the total backup size. This portion represents the delta changes that will be backed up during the incremental backup.

Run the following command to perform an incremental backup:

```
/opt/vertica/bin/vbr --task backup --config-file db_backup.ini
```

Using the `restorePointLimit` argument will define the number of earlier backups to retain with the most recent backup. If the value is not provided, the default value of 1 means that the ArcSight Database will maintain two backups: the latest backup and the one before it.

Verifying the Integrity of the Backup

Use the `full-check` option to verify the integrity of the Database backup.

The option reports the following:

- Incomplete restore points
- Damaged restore points
- Missing backup files
- Unreferenced files

To verify the backup integrity, run the following command:

```
/opt/vertica/bin/vbr --task full-check --config-file db_backup.ini
```

Example output:

```
Enter vertica password:
```

```
Checking backup consistency.
List all snapshots in backup location:
Snapshot name and restore point: backup_snapshot_2024_20240405_193836, nodes:
['v_fusiondb_node001'].
Snapshot name and restore point: backup_snapshot_2024_20240408_090856, nodes:
['v_fusiondb_node001'].
Snapshots that have missing objects(hint: use 'vbr --task remove' to delete
these snapshots):
Backup locations have 0 unreferenced objects
Backup locations have 0 missing objects
Backup consistency check complete.
```

Managing ArcSight Database Backups

This section describes how to view and delete backups.

- "Viewing Available Backups" below
- "Deleting a Backup" below

Viewing Available Backups

To view the available backups, run the following command:

```
/opt/vertica/bin/vbr --task listbackup --config-file db_backup.ini
```

Example output:

```
Enter vertica password:
backup                              backup_type   epoch   objects   include_
patterns   exclude_patterns   nodes(hosts)                              version
 file_system_type
backup_snapshot_20240416_063830   full          4998
                         v_fusiondb_node0001(15.214.141.242)   v23.4.0-4
[Linux]
backup_snapshot_20240416_063714   full          4992
                         v_fusiondb_node0001(15.214.141.242)   v23.4.0-4
[Linux]
```

The backup file name includes the backup timestamp.

Deleting a Backup

To delete a backup, run the following command:

```
# /opt/vertica/bin/vbr --task remove --config-file db_backup.ini --archive
20180104_142326
```

Example output:

```
# 20180104_142326 is the backup timestamp
Enter vertica password:
Removing restore points: 20180104_142326
Remove complete!
```

ArcSight Database - Restore

The restore process must be performed by the `$dbadmin` user.

1. Log into the database node and stop the database with the following command:

```
cd <arcsight_database_installation_directory>
./vertica_installer stop-db
```

2. Stop the database watchdog service by running the following command:

```
crontab -l | sed '/^[^#].*scripts.watchdog/s/^/#/' | crontab -
```

3. Change to the $dbadmin user by running the following command:

```
su -l $dbadmin
```

4. Restore the backup data by running the following command:

```
/opt/vertica/bin/vbr --task restore --config-file db_backup.ini
```

Example output:

```
Enter vertica password:
Starting full restore of database Recon.
Participating nodes: v_fusiondb_node0001.
Restoring from restore point: Vertica_backup-April_2024_20240408_172524
Determining what data to restore from backup.
[==================================================] 100%
Approximate bytes to copy: 1086978980 of 3206846934901 total.
Syncing data from backup to cluster nodes.
[==================================================] 100%
Restoring catalog.
Restore complete!
```

5. Start the database by running the following command:

```
exit
./db_installer start-db
```

Example output:

```
Start database: fusiondb
Going with traditional slower startup
       Starting nodes:
               v_fusiondb_node0001 (15.214.136.201)
       Starting Vertica on all nodes. Please wait, database with a large catalog
may take a while to initialize.
       Node Status: v_fusiondb_node0001: (DOWN)
       Node Status: v_fusiondb_node0001: (DOWN)
       Node Status: v_fusiondb_node0001: (DOWN)
       Node Status: v_fusiondb_node0001: (UP)
Syncing catalog on fusiondb with 2000 attempts
Database fusiondb: Startup suceeded. All nodes are UP
```

6. Start the Kafka scheduler by running the following command:

```
./kafka_scheduler start
```

7. Start the database watchdog service by running the following command:

```
/opt/arcsight-db-tools/scripts/watchdog.sh enable
```

Chapter 5: Managing the Recon Appliance

Restarting the Appliance

The following steps are required to stop the appliance's processes, which would be required to perform maintenance, or when updating the OS.

The following commands must be executed as the `root` user.

1. Check that kubernetes is in running status:

   ```
   kubectl get pods -A
   ```

   In the output, all pods must be in **Running** or **Completed** state.
2. Check the status of the ArcSight Database kafka scheduler:

   ```
   cd /opt/arcsight-db-tools
   ```

   ```
   ./kafka_scheduler status
   ```

   The scheduler must be in a running status, without exception.
3. (If Multi-Tenancy is enabled) Check the event flow for each tenant:

   ```
   ./kafka_scheduler events -t $tenant
   ```

   The event flow must be running well.
4. Stop kubernetes with the following commands:

```
cd /opt/arcsight/kubernetes/bin
```

```
./kube-stop.sh
```

The operation must succeed without exception.

5. Stop the database with these commands:

```
cd /opt/arcsight-db-tools
```

```
scripts/watchdog.sh disable
```

The operation must succeed without exception.

```
./db_installer stop-db
```

The command should have the following output:

```
Database fusiondb stopped successfully
```

6. You can now perform the planned operation on the appliance.

If a reboot is needed, you can execute it at this point.

7. (Conditional) If the appliance has not been rebooted, execute these steps to resume operations:

```
cd /opt/arcsight/kubernetes/bin
```

```
./kube-start.sh
```

The operation must succeed without exception.

8. Check the kubernetes status:

```
kubectl get pods -A
```

In the output, all pods must be in **Running** or **Completed** state.

9. Start the ArcSight Database with these commands:

```
cd /opt/arcsight-db-tools
```

```
./db_installer start-db
```

The command should have the following output:

```
Database fusiondb: Startup Succeeded.  All Nodes are UP
```

10. Start the scheduler with this command:

```
./kafka_scheduler start
```

The operation must succeed without exception.

11. Start the watchdog:

```
scripts/watchdog.sh enable
```

The operation must succeed without exception.

12. Check the status of the database kafka scheduler:

```
./kafka_scheduler status
```

The scheduler must be running without exception.

13. (If Multi-Tenancy is enabled) Check the event flow for each tenant:

```
./kafka_scheduler events -t $tenant
```

The event flow must be running well.

Publication Status

Released: Wednesday, June 5, 2024

Updated: Monday, June 3, 2024

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Administrator's Guide to Hardware Appliances for ArcSight Recon (8000 Appliance 24.2)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to documentation-feedback@microfocus.com.

We appreciate your feedback!