



DB8400 - SIEM Database Appliance 24.4

Software Version: 24.2.3

Administrator's Guide to the DB8400 - SIEM Database Appliance 24.4

Document Release Date: December, 2024

Software Release Date: December, 2024

Legal Notices

Open Text Corporation

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

Copyright Notice

Copyright 2024 OpenText

The only warranties for products and services of Open Text and its affiliates and licensors (“Open Text”) are as may be set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Open Text shall not be liable for technical or editorial errors or omissions contained herein. The information contained herein is subject to change without 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	5
Chapter 1: Overview	7
How the DB8400 appliance works	7
Appliances for security, compliance, and IT applications	8
Chapter 1: Set up the DB8400 appliance	8
Powering on the DB8400 appliance	9
Setting up the appliance for remote access	10
Changing the iDRAC password on your appliance	10
Encryption of SEDs	11
Initialize the DB8400 appliance	11
Bootstrapping the DB8400 appliance	11
Regeneration of the first login token	14
Chapter 2: Backup and restore procedures	15
Restoring an appliance to factory settings	15
Multinode Clusters	15
Restoring an appliance using a USB memory stick	16
Hardware Requirements	16
Image burning	16
Restore procedure:	16
Restoring an appliance using iDRAC access	17
Prerequisites:	17
Restore procedure:	17
Backing up and restoring the ArcSight database	18
Checklist: Backing up the ArcSight database	20
Backing up the ArcSight database	20
Understanding the database backup process	20
Backup overview	20
Backup terminology	21
Preparing the backup configuration file	21
Backing up the database	22

- Scheduling automatic backups 22
- Restoring the database 23
 - Prerequisites for restoring the database 23
 - Restoring a backup 23
- Managing your backups 24
 - Viewing available backups 25
 - Quick-check backup 25
 - Full-check backup 25
 - Deleting a backup 25
 - Disabling scheduled automatic backups 26
- Preparing for a database recovery 26
- Chapter 3: Manage the DB8400 appliance 28
 - Restarting the appliance 28
 - Stop data ingestion into the database temporarily 28
 - Start data ingestion into the database 28
 - Stop the database before an appliance restart 29
 - Publication status 30
- Send Documentation Feedback 31

About this guide

This installation guide provides instructions on how to install and initialize the *DB8400 - SIEM Database Appliance 24.4*; also referred as the DB8400 appliance in this guide for brevity.

For more information, see ["How the DB8400 appliance works" on page 7](#).

Intended Audience

This book provides information for admins who need to install, initialize, and restore the *DB8400 - SIEM Database Appliance 24.4*.

Additional Documentation

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

ArcSight Platform

- [DB8400 - SIEM Database Node Appliance 24.4 Release Notes](#) which provides information about the appliance 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 24.2.3 - Off-Cloud Deployment](#)
- [Technical Requirements for ArcSight Platform 24.2.3](#), 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

The DB8400 - SIEM Database Appliance 24.4 is one among the X-series of scalable appliances that provide scalable out-of-the-box computing capabilities for the ArcSight solution. It simplifies the deployment of the unified storage layer of the platform and works with the W8300 - SIEM Worker Node Appliance 24.4 only in a multi-node cluster. For example, if ArcSight Recon is installed on the W8300 appliance, the database is configured on the DB8400 appliance in the cluster. The DB8400 appliance acts as the database compute node and hosts the ArcSight database but with no event storage ability. Multiple DB8400 appliances may be distributed across a cluster to ensure high availability and redundancy and supports 15k EPS per node.

The ArcSight database stores all collected events and provides event searches and analysis capabilities. The database keeps the primary copy of your data in communal storage, and the local cache serves as the secondary copy. Communal storage is the database's centralized storage location, shared among the database nodes. It is based on an object store, such as Amazon's S3 service in the cloud or an S3-compatible object store in an Off-cloud deployment. The primary copy is not redistributed when nodes are added or removed.

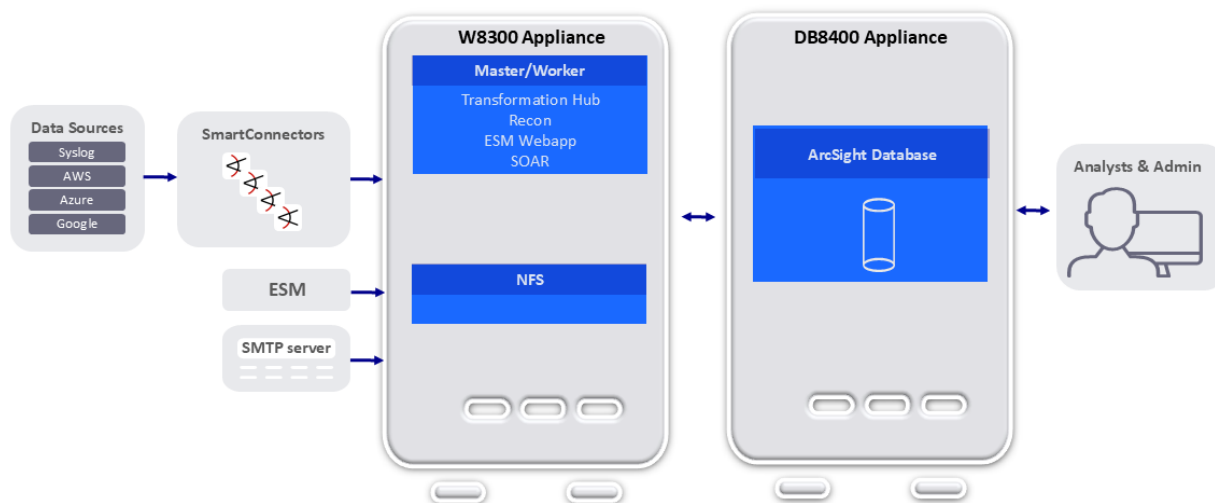
This shared storage model enables elasticity, it is both time and cost-effective to adapt the cluster resources to fit the usage pattern of the cluster. If a node goes down, other nodes are not impacted because of shared storage. Node restarts are fast and no recovery is needed. The database can bring the data to the cache on demand automatically and then move the data out when not in use. To expand communal storage, you can purchase additional storage devices rather than purchasing additional CPU and memory.



The purpose of this guide is to help you perform the initial configuration of your DB8400 - SIEM Database Appliance 24.4 appliance. For more information on the usage and settings of specific features, refer to the [User's Guide for ArcSight Platform CE 24.2](#)

How the DB8400 appliance works

The DB8400 appliance does not work standalone but requires a W8300 appliance alongside in the cluster. After you bootstrap the appliances, use the primary W8300 appliance node to add the DB8400 appliance and additional nodes, configure the database (including the S3 URL and related settings) and install the ArcSight Platform product. For additional nodes, they get the S3 location and other configurations automatically from the primary node. A cluster of more than three nodes automatically supports high availability. If you require more than one master W8300 appliance nodes, you can also configure three masters.



The appliance works with the ArcSight Database in **EON** mode. For more information, see **Architecture** in the [ArcSight Database 24.1 Guide](#).

Appliances for security, compliance, and IT applications

Although the DB8400 appliance's applicability alongside the W8300 appliance 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.




Chapter 1: Set up the DB8400 appliance

This section describes how to rack mount your DB8400 appliance. The appliance comes with software pre-installed. The following steps enable you to start using your appliance.



*Plan your cluster size for the EPS you are targeting, with a 10% buffer for possible growth. For general guidance on deployments, see the [Technical Requirements for ArcSight Platform 24.2 guide](#), [Examples of Deployment Scenarios](#). OpenText **strongly recommends** that you deploy all nodes at the same time. To add a new node after initial deployment, contact OpenText support.*

	Task	See
	1. Power on the Appliance	"Powering on the DB8400 appliance" on the next page

	2. Set up Remote Access	"Setting up the appliance for remote access" on the next page
	3. (Optional) Encrypt SEDs	"Encryption of SEDs" on page 11
	4. Initialize appliance	"Initialize the DB8400 appliance " on page 11

Powering on the DB8400 appliance

Before you begin:

The DB8400 appliance does not require a separate license. However you must redeem your license keys to access the features and functionalities on the DB8400 appliance and W8300 appliance respectively in a multi-node cluster, beyond the initial trial license period by following the instructions in the documents you received when purchasing. To redeem the license keys, complete the instructions provided in the document that you received when purchasing the product.

To install the appliance:

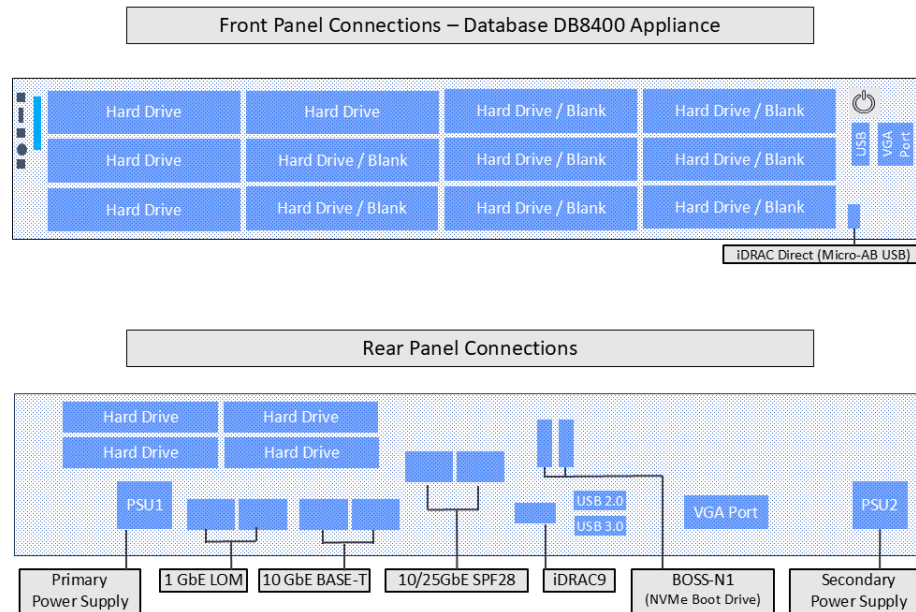
1. Unpack the appliance and its accompanying accessories.



Note: Read and follow 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 following diagram offers a general view of the basic connections:



4. Power on the appliance.

Setting up the appliance for remote access

This appliance is 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. This enables you or the Customer Support (with your permission and assistance) to remotely access the console of your appliance for troubleshooting, maintenance, and take 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, 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 DB8400 appliance supports 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, and 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, follow the steps to establish a [security key](#).

To apply the chosen passphrase to pre-existing virtual disks, follow the steps in [Secure a pre-existing virtual disk](#).

To change or disable a security key, follow the specific procedures listed under [this section](#).

Initialize the DB8400 appliance

The initialization of the DB8400 appliance consists of two parts: the first boot (bootstrapping) process through the console, and the database configuration through the W8300 appliance UI respectively.

Bootstrapping the DB8400 appliance



To successfully complete bootstrapping, make sure that the following network information is available:

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

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.
3. Using the local drive (NVMe), select the version of Red Hat you want to boot from.
4. Log in using the default username (otadmin and password (change_me)).

5. Change the password for otadmin:

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. Set passwords for both root and 'arcsight' users on the OpenText Appliance splash screen:

password for arcsight

Changing password for user root.

New password:

Retype new password:

passwd: all authentication tokens updated successfully



Passwords expire in 60 days. You must wait for at least a day before you can reset a newly set password.

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
```

```
*****
```

```
enxxxxnp0      UP      xx:xx:xx:xx:xx:xx      <BROADCAST, MULTICAST, UP, LOWER
```

```

enxxxxx          DOWN          xx:xx:xx:xx:xx:xx    <NO-CARRIER, BROADCAST, , MULTI
ensxxxxx        DOWN          xx:xx:xx:xx:xx:xx    <NO-CARRIER, BROADCAST, MULTICA

*****
Select one active connection to configure:
*****
1) enxxxxxnp0
#? 1

```

Select the number of active connections you want to configure.

8. Enter the following information to configure the network using a static IP address:

```

*****
Configure the network connection enxxxxxnp0 for device enxxxxxnp0:
*****
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. Specify the details of the NTP server to be configured:

```

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

Enter the NPT server for this appliance:

```

The console displays a summary of the network configuration and NTPserver configuration.

```

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

```

Press Y to confirm or Nto modify.

```

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

```

Specify the root password when prompted.

10. If the configuration is successful, the following message is displayed:

```

*****
The appliance network and NTP server have been setup successfully
*****
Go to https://<your_appliance_host_fqdn>:6443 to install ArcSight Platform

```

```
product.  
IMPORTANT: You will need the token to login for the first time:  
XXXXXXXXXX  
*****
```

Regeneration of the first login token

To regenerate the First Login Token, run the following command in the console:

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

Specify the arcsightpassword when prompted to regenerate the First Login Token:

```
=====  
Go to https://<your_appliance_host_fqdn>:6443 to install ArcSight Platform  
product.  
IMPORTANT: You will need the token to login for the first time:  
XXXXXXXXXX  
=====
```

Chapter 2: Backup and restore procedures

To enable data recovery when needed, OpenText recommends that database backups of the DB8400 appliance components must be performed regularly and every time before you upgrade your environment.

Restoring an appliance to factory settings

Follow the instructions in this section to restore the DB8400 appliance in a cluster to factory settings.

To perform a restore procedure, you will require:

- An .iso image file containing the factory settings for the version of DB8400 - SIEM Database Appliance 24.4 you are restoring. Find the name of the file in the **Downloading Your Factory Restore Image Files** section of the [DB8400 - SIEM Database Node Appliance 24.4 Release Notes](#)



After you have acquired the image file, please refer to the [signature verification](#) instructions, and perform the verification steps before starting the following procedure.

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 17](#) method

Multinode Clusters

In a multinode cluster configured for high-availability, the HA quorum may be spoiled by bringing down a single node for restoration. In this case, all nodes in the cluster will need to be restored to their factory settings. For example, in a 3 - node highly-available W8300 appliance and DB8400 appliance cluster, to restore a single W8300 appliance node to factory settings, the complete process for each node is as follows:

1. Remove the impacted node from the Kubernetes cluster.
For more information, see [Restarting or shutting nodes in a Kubernetes cluster](#).
2. Restore to factory settings as detailed in the [previous section](#).
3. Bootstrap the [W8300 appliance node](#) or [DB8400 appliance node](#).
4. [Add the node back to the cluster](#).

Restoring an appliance using a USB memory stick

Hardware Requirements

- A USB 2.0 or higher memory stick with 32 GB or more capacity
- A Linux machine to burn 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 lower right corner.
3. Click the **BOOT** button on the top right corner and select the **BIOS Boot Manager** option.
Select Yes in the pop-up window to confirm boot action to set a new device from which to boot.
4. Click the **POWER** button, and from the **Power Control** pop-up window, choose the **Reset System (warm boot) option**.
Select Yes to confirm the power action.
5. When prompted 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**).
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 ARST-C6615-DB8400-RH94-FIPS-STIG-CIS2-24.4-1.iso** option.

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)
```

- The restore screens progress without any user input. The process takes about 10 minutes to complete. After 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
```

- After the reboot process is complete, follow the instructions listed in the following section to initialize the appliance:

["Initialize the DB8400 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.

Prerequisites:

- 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 the shared .iso image downloaded [here](#).

Restore procedure:

- 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](#)
- From the iDRAC **Dashboard**, select the **Virtual Console** on the lower right corner.

3. Click the **BOOT** button on the top right corner and select the **BIOS Boot Manager** option.
Select Yes in the pop-up window to confirm boot action to set a new device from which to boot.
4. Click the **POWER** button, and from the **Power Control** pop-up window, choose the **Reset System (warm boot) option**.
Select Yes to confirm the power action.
5. When prompted choose **One-shot UEFI Boot Menu**.
6. From the **Select UEFI Boot Option**, select **Virtual Optical Drive**.
The appliance will boot from the .iso image in the Remote File Share.
7. The restore process will start automatically if you allow it some time, or you can click on the **ArcSight User Image ARST-C6615-DB8400-RH94-FIPS-STIG-CIS2-24.4-1.iso** option.
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. The restore screens progress without any user input. The process takes about 10 minutes to complete. After 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. After the reboot process is complete, follow the instructions listed in the following section to initialize the appliance:

["Initialize the DB8400 appliance " on page 11](#)

Backing up and restoring the ArcSight database

You can configure automatic backups of the ArcSight database on a DB8400 appliance to protect against data loss or corruption. The backed up data can be restored anytime to the same or separate system as per your requirement. When you perform a backup, data gets copied to a backup communal storage location that replicates the live communal storage.

- [Checklist: Backing up the database](#)
- [Backing up the database](#)
- [Restoring the database](#)

- [Managing your backups](#)
- [Preparing for a database recovery](#)

Checklist: Backing up the ArcSight database

	Task	See
<input type="checkbox"/>	1. Database backup	"Backing up the ArcSight database" below
<input type="checkbox"/>	2. Incremental database backup	Backing up the database incrementally
<input type="checkbox"/>	3. Verify the integrity of the backup	Verifying the integrity of the backup

Backing up the ArcSight database

You can manually create or automatically schedule a database backup before upgrading the DB8400 appliance. Follow this section to successfully back up the database.

- [Understanding the database backup process](#)
- [Preparing the backup configuration File](#)
- [Backing up the database](#)
- [Scheduling automatic backups](#)

Understanding the database backup process

This section provides an introduction to the backup process:

- [Backup overview](#)
- [Backup terminology](#)

Backup overview

You can perform a full backup, which is a complete copy of the database catalog, its schemas, tables, and other objects. It provides a snapshot of the database at the time of backup. You can use it for disaster recovery or to restore a damaged or an incomplete database. You can also restore individual objects from a full backup.

If a full backup already exists, then the database backup utility tool backs up new or changed data from the time the full backup was created. You can specify the number of backup snapshots to retain.

Backup terminology

- Backups are stored in the following folders in the backup location:
 - **Object Folder:** Consists of database objects files, which contain the actual data stored in the database. Repeated backups copy the new objects that are not in the backup location.
 - **Snapshot folder:** Contains a snapshot of the full catalog of the database at the time of the backup. Catalog contains metadata which is smaller in size than the actual data in the database. Catalog keeps track of all the database objects that were present in the database at the time of the backup snapshot. Many Catalog snapshots will refer to the same object files as the backups are performed more often than the lifespan of the object file. This avoids storing duplicates of object files for each backup. The backup_snapshot portion is defined by the .ini file and the date time strings are automatically appended by the database backup process.
- **Restore point:** Each backup operation records the state of the database at the time of the backup and stores it in the backup archive as a restore point. You can restore to a specific restore point using the `-archive` argument.
- **Restore point limit:** Specifies the number of previous backups that you want to retain in addition to the most recent backup.
- In the backup utility configuration file, you can specify the number of backup snapshots to be retained using **Specify the number of historical backups to retain in addition to the most recent backup**, so that the expired snapshots can be groomed out. When a backup snapshot is groomed out, all associated object files that was being referenced by the snapshot will also be groomed out.

Preparing the backup configuration file

A database backup utility is used to perform backup and restore procedures. You must configure this utility before using it to perform the complete lifecycle of scheduling backups, backup on-demand, manage the backup archive, and restore from backup.



You must create an S3 bucket or a Blob storage backup folder before configuring the database backup utility.



Run this tool as a root user.

1. On database node1, execute the following command from the database scripts directory, located by default at `/opt/arcsight-db-tools/scripts`:

```
./db_backup.sh config
```

2. Select the communal storage.
3. Specify the values for the fields based on your storage type.
 - For S3 storage:

Scenario	Fields
Using IAM role	<ol style="list-style-type: none"> a. Specify your S3 server: b. Specify S3 server port [443]: c. Is TLS enabled(y/n): d. Specify your S3 backup bucket: e. Specify your S3 backup folder path: f. Specify your locking system path [/tmp]: g. Specify temp directory path [/tmp/vbr]: h. Specify the number of historical backups to retain in addition to the most recent backup: Are the values correct? (y/n):

Backing up the database

To back up the database, complete the following steps:

1. [Prepare the backup configuration file.](#)
2. Run the following command from the database scripts directory, located by default at `/opt/arcsight-db-tools/scripts`:

```
./db_backup.sh backup
```

Scheduling automatic backups

OpenText recommends that you schedule backups to run every hour. To schedule a backup, use the following command from the database scripts directory, located by default at `/opt/arcsight-db-tools/scripts`:

```
./db_backup.sh schedule '<crontab_expression>'
```

where `<crontab_expression>` represents the time that you want to set for the scheduled backup.

For example:

```
./db_backup.sh schedule '0 * * * *'
```

Restoring the database

You can use the following information to restore a backed up database. This section has the following topics:

- [Prerequisites for restoring the database](#)
- [Restoring a backup](#)

Prerequisites for restoring the database

Before restoring a backup, make a note of the following requirements:

- The database name must match the database name in the backup.
- The number of nodes in the primary subcluster must be equal to the number of nodes that were present in the primary subcluster at the time the backup was taken.
- Database node names must match the names of nodes in the backup.
- Use the same catalog directory location that was used in the database when the backup was taken.
- Use the same port numbers that were used by the database when the backup was taken.
- For object restore, have the same shard subscriptions. If the shard subscriptions have changed, then you can only perform full restore. Shard subscriptions can change when you add or remove nodes or rebalance the cluster.
- The database cannot be restored while it is still running. Run `db_installer stop-db` to stop the database. If you must stop the database, also run `./scripts/watchdog.sh disable` to disable the watchdog.



You must stop the database before you perform a full restore. Run `db_installer stop-db` to stop the database. However, the database must be running to perform an object restore. Run `db_installer start-db` to start the database.




Restoring a backup

You can restore a full or object backup of a database that has primary and secondary subclusters to a new (target) database. The target database can have both primary and secondary subclusters. However, the backup is restored only to the primary subclusters of the target database.

To restore a backup, use following command from the database scripts path (`/opt/arcsight-db-tools/scripts`):

```
./db_backup.sh restore
```

You can use the following parameters:

<code>--archive=<timestamp_value></code>	To specify a timestamp of the backup that you want to restore. For example: <code>./db_backup.sh restore --archive=20211006_205934</code>
<code>--restore-objects=<objects></code>	To specify the individual objects you want to restore from a full or object-level backup. If you are using wildcards, then use <code>--include-objects</code> and <code>--exclude-objects</code> instead. For example: <code>./db_backup.sh restore --restore-objects=default_secops_adm</code>  This parameter is invalid in combination with parameters <code>--include-objects</code> and <code>--exclude-objects</code> .
<code>--include-objects=<objects></code>	To specify database objects or pattern of objects to restore from a full or object-level backup. Use comma to delimit multiple objects and wildcard patterns. For example: <code>./db_backup.sh restore --include-objects=default_secops_adm</code>  You cannot use this parameter with <code>--restore-objects</code> parameter.
<code>--exclude-objects=<objects></code>	Used along with <code>--include-objects</code> option, to specify database objects or pattern of objects you want to remove from the set. Use comma to delimit multiple objects and wildcard patterns. For example: <code>./db_backup.sh restore --include-objects=default_adm --exclude-objects=default_secops_adm</code>  You cannot use this parameter with <code>--restore-objects</code> parameter.

After restore completes, execute the restart commands:

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

```
./kafka_scheduler start
```

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



After the database is restored, it takes some time before all data is populated in the (missing or bad snippet) dashboard.

Managing your backups

You can use the following information to manage your backups. This section has the following topics:

- [Viewing available backups](#)
- [Quick-check backup](#)
- [Full-check backup](#)

- [Deleting a backup](#)
- [Disabling scheduled automatic backups](#)

Viewing available backups

To view all the available backups, use the following command from the database scripts path (/opt/arcsight-db-tools/scripts):

```
./db_backup.sh list
```

Quick-check backup

You can collect all backup metadata from the backup location specified in the configuration file and compare that metadata to the backup manifest using the following command from the database scripts path (/opt/arcsight-db-tools/scripts):

```
./db_backup.sh quick-check
```

Full-check backup

Verify all objects listed in the backup manifest against the filesystem metadata using the following command from the database scripts path (/opt/arcsight-db-tools/scripts):

```
./db_backup.sh full-check
```

Available options:

```
--report-file=<path or a file name>
```



Full-Check also includes the steps of Quick-Check.

Deleting a backup

To delete a backup, use the following command from the database scripts path (/opt/arcsight-db-tools/scripts):

```
./db_backup.sh remove --archive=<timestamp>
```

Required parameter:

--archive=<timestamp>: To specify a timestamp of the backup you want to remove. Replace <timestamp> with the timestamp of the archive.

For example:

```
./db_backup.sh remove --archive=20211006_205934
```

Required options:

Disabling scheduled automatic backups

To remove a job that runs scheduled backup, use following command from the database scripts path (/opt/arcsight-db-tools/scripts):

```
./db_backup.sh unschedule
```

Preparing for a database recovery

In the event your database is lost, you must work with a Support Technician to recover the DB8400 appliance. Before doing so, you must prepare your environment for the recovery process. This process is different from [restoring the database](#) as you are preparing to rebuild the database in this scenario.

NOTE: You must complete this process with the ArcSight Platform Installer. If you use a manual install, it will be difficult to access the necessary files needed in this process.

1. To install the database, [run the ArcSight Platform Installer](#).
NOTE: The following installation commands must be completed with no exceptions:
 - `./arcsight-install -c /opt/my-install-config.yaml --cmd preinstall`
 - `./arcsight-install -c /opt/my-install-config.yaml --cmd install`
 - `./arcsight-install -c /opt/my-install-config.yaml --cmd postinstall`
2. After installation is complete, ensure that the events collected by [SmartConnectors](#) can be copied to the database.
This step ensures that the events are flowing properly into the database and that the installation was successful.
3. Configure the [database backup](#). This process generates the following backup-related file:
 - `/opt/arcsight-db-tools/scripts/db_backup.sh config`
4. Perform a [backup of the database](#). This process generates the following backup-related file:
`./opt/arcsight-db-tools/scripts/db_backup.sh backup`
This steps ensures that the backup process is working without error.
5. Execute the following commands on database node1 to create separate directories:
 - `mkdir /opt/db-saved`
 - `mkdir /opt/db-saved/db-cert`
 - `mkdir /opt/db-saved/db-config`
6. Execute the following commands on database node1:

- `cd /opt/arcsight-db-tools`
 - `cp db-remote-install.properties /opt/db-saved`
 - `cp cert/* /opt/db-saved/db-cert`
 - `cd /opt/arcsight-db-tools/config`
 - `cp db_credentials_default.properties /opt/db-saved/db-config`
 - `cp db_user.properties /opt/db-saved/db-config`
 - `cp backup_restore_cloud_storage.ini /opt/db-saved/db-config`
 - `cp backup_restore_cloud_storage_test.ini /opt/db-saved/db-config`
 - `cp db_backup.properties /opt/db-saved/db-config`
 - `cp password.ini /opt/db-saved/db-config`
7. Save the `/opt/db-saved` directory from [step 7](#) to a location outside of the database.
 8. Save the following S3 storage credentials to a location outside of the database:
 - AWS: Access key | Secret
 - minIO: MINIO_ROOT_USER | MINIO_ROOT_PASSWORD
 - S3 certs/keys, if available

Chapter 3: Manage the DB8400 appliance

Restarting the appliance

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

Stop data ingestion into the database temporarily

1. Log in to the DB8400 appliance:

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

2. Disable the watchdog so that the scheduler does not start automatically:

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

3. Stop the scheduler:

```
./kafka_scheduler stop
```

Start data ingestion into the database

If you had stopped data ingestion into the database, you can restart by following these steps -

1. Start the scheduler:

```
./kafka_scheduler start
```

The operation must succeed without exception.

2. Start the watchdog:

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

Stop the database before an appliance restart

1. 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
```

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



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

Publication status

Released: Tuesday, December 17th, 2024

Updated: Friday, December 20, 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 the DB8400 - SIEM Database Appliance 24.4 (8000 Appliance 24.2.3)

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!