opentext™

Open Enterprise Server 25.2
Cloud Integrated Storage Administration Guide

May 2025

Legal Notice

Copyright 2022 - 2025 Open Text

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.

About This Guide

This documentation describes how to install, configure and manage the Cloud Integrated Storage (CIS) for Open Enterprise Server (OES).

This document consists of the following chapters:

- Chapter 1, “Overview of Cloud Integrated Storage,” on page 9
- Chapter 2, “What’s New in CIS,” on page 17
- Chapter 3, “Planning Your Cloud Integrated Storage Server Environment,” on page 19
- Chapter 4, “Installing and Configuring CIS,” on page 21
- Chapter 5, “Updating (Patching) CIS Configured Server,” on page 43
- Chapter 6, “Upgrading CIS Server,” on page 45
- Chapter 7, “Management Tools for CIS,” on page 53
- Chapter 8, “Command Line Tools for CIS,” on page 71
- Chapter 9, “Migrating DST Volumes to Cloud,” on page 73
- Chapter 10, “Working with CIS Clients,” on page 77
- Chapter 11, “Scaling and Recovery of Infrastructure Node,” on page 83
- Chapter 12, “Troubleshooting CIS,” on page 85
- Chapter 13, “Best Practices and Common Questions,” on page 95
- Chapter 14, “Known Issues,” on page 101
- Appendix A, “Configuration and Log Files,” on page 103
- Appendix B, “Installing and Configuring MariaDB,” on page 105
- Appendix C, “Creating Certificates,” on page 107

Audience

This guide is intended for storage services administrators.

Feedback

We want to hear your comments and suggestions about this manual and the other documentation included with this product. Please use the `comment on this topic` link at the bottom of each page of the online documentation.

Additional Documentation

For documentation on other OES guides, see the OES 25.1 Documentation web site (https://www.microfocus.com/documentation/open-enterprise-server/24.4/).

Contents

About This Guide 3

1 Overview of Cloud Integrated Storage 9

1.1 Understanding Cloud Integrated Storage . . . 9
1.2 Benefits of Cloud Integrated Storage . . . 11
1.2.1 Reduce Total Cost of Ownership . . . 11
1.2.2 Transparent File Access for End Users . . . 11
1.2.3 Data Availability on Access . . . 11
1.2.4 Policy-Based Migration . . . 11
1.3 CIS Architecture Overview . . . 12
1.4 CIS Components . . . 12
1.4.1 Server . . . 13
1.4.2 Clients . . . 14
1.5 Services and Components Used by CIS . . . 14
1.5.1 Infrastructure Services . . . 14
1.5.2 Database . . . 15
1.6 Management Tools . . . 15
1.7 What's Next . . . 15

2 What's New in CIS 17

2.1 What's New in OES 25.2 . . . 17
2.2 What's New in OES 25.1 . . . 17
2.3 What's New in OES 24.4.1 . . . 17
2.4 What's New in OES 24.4 . . . 17

3 Planning Your Cloud Integrated Storage Server Environment 19

3.1 Open Enterprise Server . . . 19
3.2 Cloud Storage Requirements . . . 19
3.3 CIS Requirements . . . 19

4 Installing and Configuring CIS 21

4.1 Installing CIS . . . 21
4.2 Configuring CIS . . . 21
4.2.1 Accessing the CIS Configuration Console . . . 21
4.2.2 Deployment Types . . . 23
4.3 Verifying the CIS Configuration . . . 37
4.4 LUM Enabling CIS User and CIS Group . . . 39
4.4.1 Using Unified Management Console (UMC) . . . 39
4.4.2 Using Command Line Interface . . . 40
4.4.3 Using Script . . . 41

5 Updating (Patching) CIS Configured Server 43

5.1 Prerequisites . . . 43
5.2 Patching the Standalone or CIS Server . . . 43
5.3 Patching the CIS Infrastructure Servers . . . 44

6 Upgrading CIS Server 45

6.1 Upgrading Standalone CIS Server . . . 45
6.1.1 Prerequisites on Source Server . . . 45
6.1.2 Upgrading to OES 24.4 or OES 25.1 Server . . . 45
6.1.3 Data Transfer from Elasticsearch to OpenSearch . . . 46
6.2 Upgrading CIS in Multi-Server Environment . . . 47
6.2.1 Recommendations for Upgrading CIS . . . 48
6.2.2 Upgrading Infrastructure Servers from OES 24.3 to OES 24.4 or OES 25.1 . . . 48
6.2.3 Upgrading CIS Servers from OES 24.3 to OES 24.4 or OES 25.1 . . . 49
6.2.4 Upgrading Data Scale Server from OES 24.3 to OES 24.4 or OES 25.1 . . . 52

7 Management Tools for CIS 53

7.1 Managing CIS . . . 53
7.1.1 Insights . . . 55
7.1.2 OES Health . . . 55
7.1.3 Accounts . . . 56
7.1.4 Policies . . . 57
7.1.5 Tiers . . . 59
7.1.6 Dashboard . . . 64
7.1.7 Roles . . . 64
7.1.8 Agents . . . 65
7.1.9 Settings . . . 67
7.1.10 Data Servers . . . 69
7.1.11 Health Indicator . . . 69

8 Command Line Tools for CIS 71

9 Migrating DST Volumes to Cloud 73

10 Working with CIS Clients 77

10.1 CIS Client for Windows . . . 77
10.1.1 Prerequisites . . . 78
10.1.2 Installing CIS Client . . . 78
10.1.3 Reinstalling or Uninstalling CIS Client . . . 78
10.1.4 Log Details . . . 79
10.2 CIS Client for Mac . . . 79
10.2.1 Prerequisite . . . 79
10.2.2 Installing CIS Client . . . 79
10.2.3 Uninstalling CIS Client . . . 81
10.2.4 Log Details . . . 81

11 Scaling and Recovery of Infrastructure Node 83

11.1 Scaling Up of HA Nodes . . . 83

11.2 Disaster Recovery of CIS Infrastructure Nodes 84

12 Troubleshooting CIS 85

12.1 CIS Configuration Failure Issues 85
12.1.1 CIS Configuration Fails When Certificate Does Not Have SAN Name 86
12.1.2 Public Network Interface is not Added to Firewall Active Zone 87
12.1.3 CIS Configuration Fails When OES is Configured with BIOS Firmware 87
12.1.4 CIS Services Fails to Come Up 87
12.1.5 CIS Configuration Fails With an Error 87
12.1.6 Unable to Configure Kafka Service During CIS Configuration 88
12.2 Upgrade Issues 88
12.3 Changing Firewall State Causes Communication Failure 89
12.4 Default IP for the Docker0 Bridge Conflicts with Current Network 90
12.5 Default CIS Docker Subnet Conflicts with Current Network 90
12.6 Cloud Account Restart Causes CIS Data Services to Fail 90
12.7 Kafka Services Fail to Run on CIS Installed with ‘eth1’ 90
12.8 OES Health Page is not Displaying Status of Services 91
12.9 DST Migration From the Shadow Volume To Cloud Storage Causes High CPU Utilization 91
12.10 Scanning Volumes, Migrating and Recalling Data Fails 92
12.11 CIS Agents Stops Randomly During the Data Migration 92
12.12 Health Indicator on CIS Management Console Displays CIS Health as Not Healthy 92
12.13 Infrastructure Services Fails to Come Up After Cleaning Up the Disk Space in HA Node 93
12.14 /var/lib/docker/containers in Infrastructure Server Consumes More Disk Space 93
12.15 Agent is Not Being Listed During the Tier Creation 93
12.16 Agent Fails to Display the Volumes During Tier Configuration 93

13 Best Practices and Common Questions 95

13.1 Backup and Restore Options for Cloud Backed Volumes (CBV) 95
13.2 Client Recommendation 95
13.3 Recalling Files from the Cloud Storage to the Source NSS Volume 96
13.4 Log Level Settings 97
13.4.1 CIS Server 97
13.4.2 CIS Agents 97
13.4.3 Infrastructure Services 97
13.5 Scanner Settings 98
13.6 Using Distributed File Services (DFS) with Cloud Backed Volume 98

14 Known Issues 101

A Configuration and Log Files 103

B Installing and Configuring MariaDB 105

B.1 Installing MariaDB 105
B.2 Configuring MariaDB 105

C Creating Certificates 107

C.1 Creating Certificates for CIS using Identity Console 107

C.2 Creating Certificates for CIS using iManager 108
C.3 Reconfiguring Certificates 109

1 Overview of Cloud Integrated Storage

Cloud Integrated Storage (CIS) is a hybrid cloud solution that provides a secure gateway to store, manage, and access data across private or public cloud.

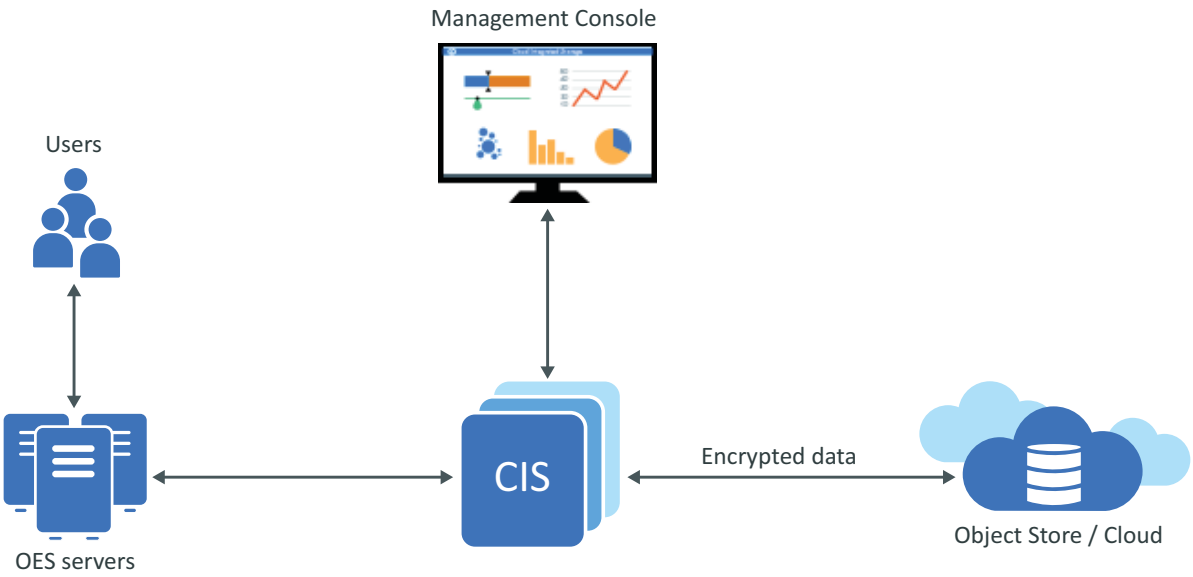
- Section 1.1, “Understanding Cloud Integrated Storage,” on page 9
- Section 1.2, “Benefits of Cloud Integrated Storage,” on page 11
- Section 1.3, “CIS Architecture Overview,” on page 12
- Section 1.4, “CIS Components,” on page 12
- Section 1.5, “Services and Components Used by CIS,” on page 14
- Section 1.6, “Management Tools,” on page 15
- Section 1.7, “What’s Next,” on page 15

1.1 Understanding Cloud Integrated Storage

A lot of our OES customers deal with huge storage (greater than TB) of data that is stored in the OES servers. As time grows, the data keeps increasing adding to the storage and maintenance cost. In the past few years, an object store or cloud has become very popular as a storage solution as it provides scalable storage and deployment with the total cost of ownership often being much less.

As the enterprise data continues to grow, the cold or inactive data keeps increasing and fills up the primary or expensive storage. This results in less space for hot or active data. Instead, you can move the cold data to cloud storage using pre-defined policies.

Keeping this in mind, we asked ourself how can we help our users take advantage of the benefits of an object store or cloud storage through OES and decided to offer a solution called Cloud Integrated Storage (CIS). CIS allows you to move and provision the enterprise data from the OES servers to object store or cloud storage by using pre-defined policies.



The three main objectives of CIS are:

- **Analyze:** A single view of data available across your organization. CIS performs adaptive scanning of the data on the OES servers and provides meaningful information such as:
  - Percentage of hot and cold data available based on the access time and modified time
  - Volumes with more cold data
  - Top file types available as part of cold data

  This information helps you to decide on how to manage the data effectively.
- **Migrate:** Based on your organizational needs, CIS helps you to create rich policies to decide what kind of data to be migrated. It offloads the cold data from highly expensive storage to much cheaper cloud storage while users still continue to seamlessly access the files.
- **Report:** Provides a rich dashboard to view the trends around the data movement. Generate reports on data migration and recall and also provides a graphical representation of the same for better understanding. You get to explicitly see how the data is moving within your organization.

Use the CIS Management console to perform the following major tasks:

- Configure your server
  - Configure cloud account, policies, and tiers
  - Create and manage roles for other users
  - Configure CIS and agents settings
- Monitor and manage your server's health
  - Overall status of the server
  - Monitor the status of individual services in the CIS server
- Data migration solution for DST volumes
- Securely transfer the data to the cloud using AES encryption

Cloud Integrated Storage is a network service that manages the data intelligently and reduces the total cost of ownership while improving flexibility.

The following video provides an introduction to Cloud Integrated Storage (CIS):

http://www.youtube.com/watch?v=6x9fdjlzFf4

1.2 Benefits of Cloud Integrated Storage

Cloud Integrated Storage has the following benefits:

- Section 1.2.1, “Reduce Total Cost of Ownership,” on page 11
- Section 1.2.2, “Transparent File Access for End Users,” on page 11
- Section 1.2.3, “Data Availability on Access,” on page 11
- Section 1.2.4, “Policy-Based Migration,” on page 11

1.2.1 Reduce Total Cost of Ownership

The active data (hot data) or frequently accessed data is stored on fast and high quality storage. The less accessed data (cold data) is placed on a cloud storage with relatively slower access. CIS policies helps you to partition the files based on last accessed time, size, type, name, and so on. You can move the less active data (cold data) from a higher performance storage to a lower performance storage, thus reserving the expensive storage for active data (hot data).

1.2.2 Transparent File Access for End Users

Users can seamlessly access the files through CIFS protocol. The user maps to the same logical path and is not aware of the physical location of the file. This allows the administrator to manage the data without disrupting the user’s view of the files. The files that are moved to cloud are represented with crossmark (x) symbol in Windows client and indicate that the files are in a offline state.

1.2.3 Data Availability on Access

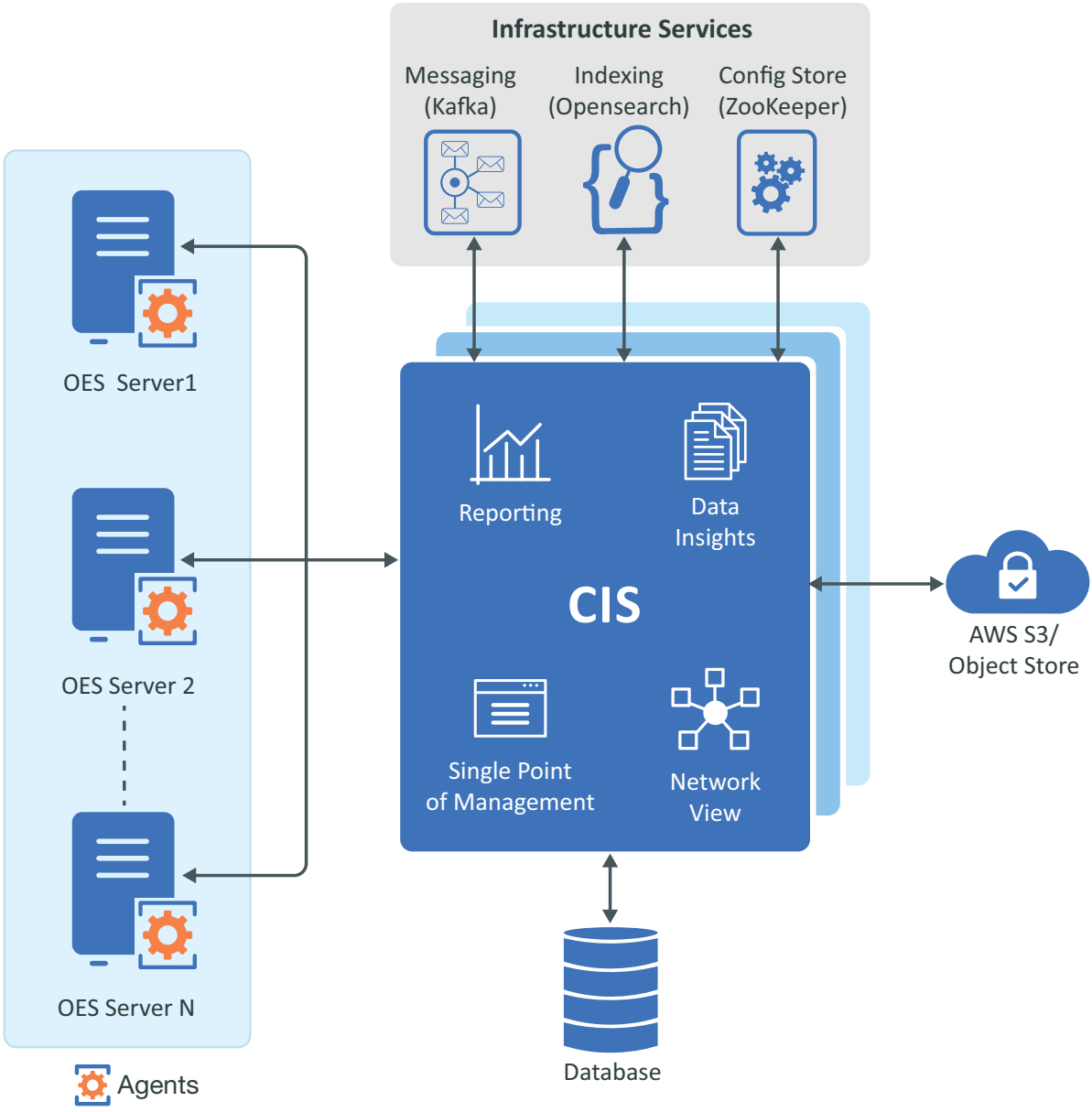
After moving the data to cloud, you still have access to the data. The access to the data available in the cloud storage is through secondary volumes called Cloud Backed Volumes (CBV). The CBV contains the metadata information of the data available in the cloud. When the data is accessed, they are brought back to the OES server.

1.2.4 Policy-Based Migration

Administrator can set policies to migrate the data from the primary volume to the cloud storage depending on the last accessed time, modified time, file type, size, and so on. To migrate the data, the policy can be run manually or automatically based on the scheduled time.

1.3 CIS Architecture Overview

Figure 1-1 *CIS Components Overview*



For detailed information about CIS and its infrastructure components, see Section 1.4, “CIS Components,” on page 12.

1.4 CIS Components

The following are the main components of Cloud Integrated Storage:

- Section 1.4.1, “Server,” on page 13
- Section 1.4.2, “Clients,” on page 14

1.4.1 Server

The CIS server requires multiple services to perform the overall operation. These services are built based on the concept of microservices. Microservices are a suite of independently deployable, small, modular services in which each service runs a unique process and communicates through a well-defined, lightweight mechanism to serve a business goal. All microservices run as an individual dockerized images.

The following are eleven microservices available for Cloud Integrated Storage:

- **Authentication:** Authenticates the agent and user. Also, facilitates token creation. The authentication service name is `cis-auth`.
- **Data:** Used for migration, recall, and communication of data with the target cloud. The data service name is `cis-data`.
- **Metadata:** Provides the capability to migrate, recall and maintain the metadata. The metadata service name is `cis-metadata`.
- **Policy:** It deals with the policies, agents, jobs, tiers, and schedule operation. The policy service name is `cis-policy`.
- **Management:** Handles all the management operations such as CIS account configuration, policy creation, tier configuration, assigning roles for other users, CIS server, and agent settings. The management service name is `cis-mgmt`.
- **OES Dashboard:** Displays status and health of all the OES services.
- **Collector and Aggregator:** Obtains the metadata information from the OES servers and performs calculations on the overall data and provides a meaningful information (hot and cold data) for the administrator. The collector and aggregator service names are `cis-collector` and `cis-aggregator`.
- **Collector and Aggregator for Reporting:** Obtains the information of files migrated to the cloud, files recalled from the cloud and then perform calculations on the overall migrated and recalled data and provides meaningful information. The collector and aggregator service names for reporting are `cis-repcollector` and `cis-repaggregator`.
- **Gateway:** It is the entry point to all services of CIS. It receives request from the OES servers and users and redirects it to the respective services. The gateway service name is `cis-gateway`.
- **Fluent Bit:** It is the logging framework used to collect the log information of all the CIS services at a common location. The logging service name is `cis-fluentbit`. The CIS services log information is located at `/var/opt/novell/log/cis/microservices`. Different log levels can be set for all the CIS services.

All these microservices communicate through the following default ports:

- **8343:** All requests from the OES server comes through this port.
- **8344:** All management operations are performed through this port.

1.4.2 Clients

The OES server acts as a client to the CIS server. The components that are available on the client side are as follows:

- **Core Agent:** Acts as a client to the CIS server. By default, agent communicates through port 8000. The OES agent name is `oes-core-agent.service`. The http communication is between CIS server and the OES Core agent. The other communications with migration agent, recall agent, scanner agent and the dashboard agent are taken care by the OES Core agent.
- **CIS Agent:** It performs the major operations such as volume listing, tier configuration, and so on. The CBV contains the metadata information of files that are migrated to the cloud. The CIS agent name is `oes-cis-agent.service`.
- **CIS Recall Agent:** Helps in recalling the data. When a request comes from a user for a specific file, the recall agent sends a request to the CIS server to retrieve the data from the cloud by using the metadata information. The CIS recall agent name is `oes-cis-recall-agent.service`.
- **CIS Scanner:** Scans the metadata on the NSS volumes of the OES server and sends it to CIS server. The CIS scanner name is `oes-cis-scanner.service`.
- **Dashboard Agent:** It is responsible for collecting health information of OES services and sending it to the CIS server. The Dashboard agent name is `oes-dashboard-agent.service`.

1.5 Services and Components Used by CIS

The services and components in this section are used by CIS.

- Section 1.5.1, “Infrastructure Services,” on page 14
- Section 1.5.2, “Database,” on page 15

1.5.1 Infrastructure Services

CIS infrastructure services includes the following:

- “OpenSearch (Indexing)” on page 14
- “ZooKeeper (Configuration Store)” on page 15
- “Kafka (Messaging)” on page 15

OpenSearch (Indexing)

CIS uses OpenSearch for the following benefits:

- Stores indexes and provides the capability for text search that enables faster discovery and deliver of relevant data.
- Analyze and aggregate the metadata obtained from the respective OES servers and enables CIS to query the information faster.

ZooKeeper (Configuration Store)

CIS uses ZooKeeper service for maintaining the configuration information.

Kafka (Messaging)

CIS uses Kafka for the following benefits:

- Good solution for large scale message processing applications.
- Asynchronous communication across services and to report event processing.

1.5.2 Database

CIS supports MariaDB and MS SQL database to store and retrieve the information. For example, OES server information, cloud information, CIS service related information, and information about the migrated data.

1.6 Management Tools

Cloud Integrated Storage policies, tiers, roles, agent settings, and cloud account configuration is managed in the CIS management console. For more information about using CIS management console, see Section 7.1, “Managing CIS,” on page 53.

1.7 What’s Next

For information about planning your CIS solution, see Chapter 3, “Planning Your Cloud Integrated Storage Server Environment,” on page 19.

For information about installing and configuring CIS, see Chapter 4, “Installing and Configuring CIS,” on page 21.

2 What's New in CIS

This section summarizes the new features and enhancements in Cloud Integrated Storage (CIS).

- Section 2.1, "What's New in OES 25.2," on page 17
- Section 2.2, "What's New in OES 25.1," on page 17
- Section 2.3, "What's New in OES 24.4.1," on page 17
- Section 2.4, "What's New in OES 24.4," on page 17

2.1 What's New in OES 25.2

Implemented enhanced security controls for containers aligned with the CIS Benchmarks, ensuring compliance with industry best practices.

For more information, see Section 4.4, "LUM Enabling CIS User and CIS Group," on page 39.

2.2 What's New in OES 25.1

CIS client for Mac 1.1.8 supports macOS 15 (Sequoia).

For more information, see Chapter 10, "Working with CIS Clients," on page 77.

2.3 What's New in OES 24.4.1

CIS client for Windows 1.0.12 supports Windows 11 24H2.

Additionally, CIS client is also compatible with Windows 10 22H2, Windows 11 22H2, and Windows 11 23H2.

For more information, see Chapter 10, "Working with CIS Clients," on page 77.

2.4 What's New in OES 24.4

- Improved security
- Improved CIS Integrity `(cisintegrity)` performance

3 Planning Your Cloud Integrated Storage Server Environment

This section describes the software requirements and configuration guidelines for installing and using Cloud Integrated Storage (CIS) on your Open Enterprise Server (OES) servers.

- Section 3.1, “Open Enterprise Server,” on page 19
- Section 3.2, “Cloud Storage Requirements,” on page 19
- Section 3.3, “CIS Requirements,” on page 19

3.1 Open Enterprise Server

Cloud Integrated Storage runs on OES servers with 64-bit processors. For information about installing and configuring OES, see the Installation Guide.

3.2 Cloud Storage Requirements

CIS supports the following:

- Amazon S3
- Object storage that is S3 compatible
- Azure Cloud Account
- Google Cloud Storage

3.3 CIS Requirements

Before you start configuring the Cloud Integrated Storage (CIS) or infrastructure services, ensure that the following prerequisites are met:

- Ensure that a minimum of 16 GB of RAM is configured for CIS or infrastructure services to function normally.
- Ensure that the number of CPU is 4 and Core per Socket is 1.
- The eDirectory schema for CIS must be extended so that the CIS server is successfully configured. If eDirectory schema is not extended for CIS, execute the `cis.sch` file on the OES server to enable the schema. For more information about how to run the script, see “CIS Configuration Fails With an Error” on page 87. If **OES Storage Service (NSS)** pattern is selected during installation, the eDirectory schema is automatically updated.
- Configure the IP address and FQDN with appropriate DNS entry so that the OES server, CIS, and its infrastructure services (OpenSearch, ZooKeeper, and Kafka) are mutually resolvable.
- The OES server certificate must include DNS name in the Subject Alternative Name (SAN).

4 Installing and Configuring CIS

This topic describes how to install and configure CIS in different environments.

- Section 4.1, “Installing CIS,” on page 21
- Section 4.2, “Configuring CIS,” on page 21
- Section 4.3, “Verifying the CIS Configuration,” on page 37
- Section 4.4, “LUM Enabling CIS User and CIS Group,” on page 39

4.1 Installing CIS

1. From the boot menu, select **Installation** and press enter, then continue with the installation as desired until you get to the Installation Settings page.

   For detailed instructions, see Installing OES as a New Installation in the Installation Guide.
2. On the **Installation Settings** page, click **Software** to open the Software Selection and System Tasks page.
3. Under **Open Enterprise Server**, select **Cloud Integrated Storage (CIS)** and continue with the installation process.

   The following additional services are automatically selected:

   - NetIQ eDirectory
   - OES Linux User Management (LUM)
   - OES Remote Manager (NRM)
   - OES Backup / Storage Management Services (SMS)
4. Continue with Section 4.2, “Configuring CIS,” on page 21.

4.2 Configuring CIS

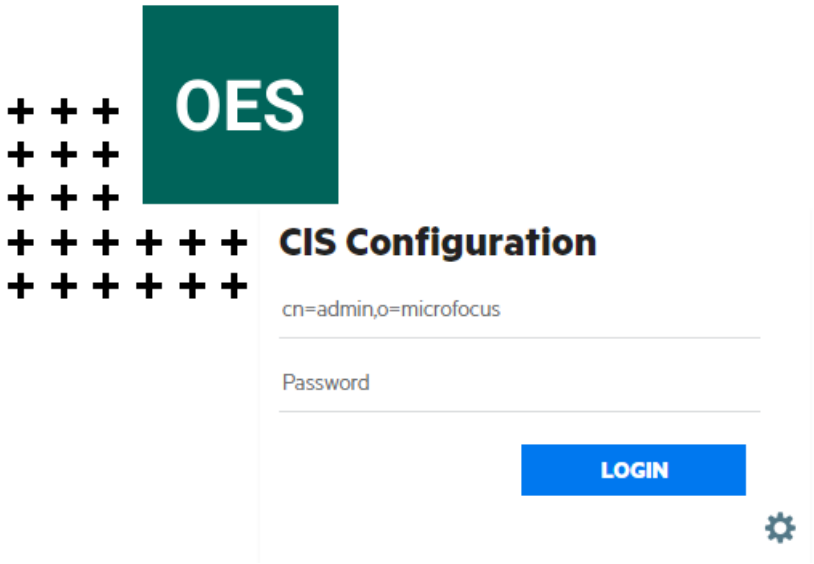
The Cloud Integrated Storage (CIS) provides a console to configure CIS and its infrastructure components.

NOTE: Before configuring CIS or infrastructure services on any server, ensure to select CIS pattern using the YaST configuration.

- Section 4.2.1, “Accessing the CIS Configuration Console,” on page 21
- Section 4.2.2, “Deployment Types,” on page 23

4.2.1 Accessing the CIS Configuration Console

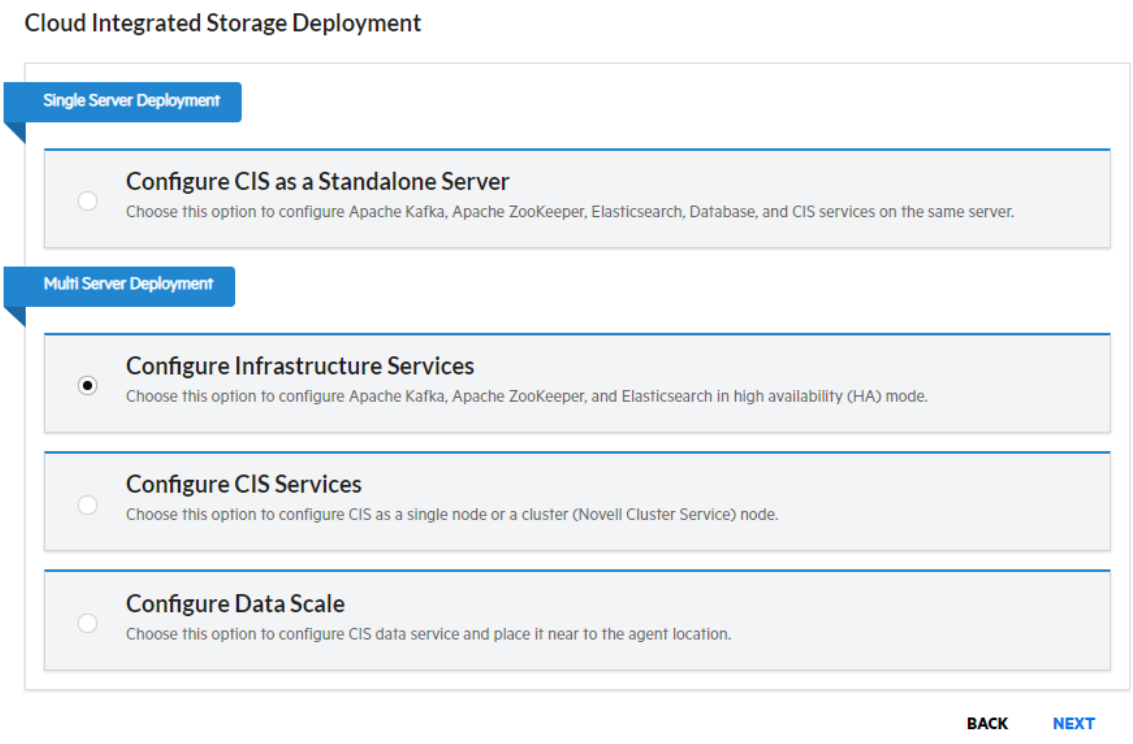
1. Point your browser to https://<*OES server IP address or the host name*>:8105.



2 Specify the user name or FQDN of the eDirectory administrator in the user name, specify the password, then click **Login**. For example, cn=admin,o=acme.

   The CIS Configuration welcome page explains the configuration flow of CIS components.

3 Review the flow, and then select the type of deployment as per your requirement.



IMPORTANT: Before configuring the CIS, ensure that there is sufficient disk space available on the root file system for CIS to function properly.

4.2.2 Deployment Types

It includes the following:

- "Configure CIS as a Standalone Server in Root (/) Path" on page 23
- "Configure CIS as a Standalone Server in NSS Media" on page 25
- "Configure Infrastructure Services" on page 29
- "Configure CIS Services" on page 30
- "Configure Data Scale" on page 35

Configure CIS as a Standalone Server in Root (/) Path

Choose this option to configure Apache Kafka, Apache ZooKeeper, OpenSearch, database and CIS services on the same server.

Prerequisites

- Before you start with CIS configuration, ensure to meet the requirements mentioned in Section 3.3, "CIS Requirements," on page 19 are met.
- A local database is created during CIS Standalone server configuration. Ensure that there is no database already configured on this server.
- If you prefer an external database ensure that the database is installed and configured. For information on how to install and configure MariaDB, see Appendix B, "Installing and Configuring MariaDB," on page 105. If you want to use already configured database (MariaDB or MS SQL) with CIS, ensure that the database is up and running.

Procedure

1. On the CIS deployment page, select **Configure CIS as a Standalone Server** deployment type and then click **Next**.
2. **Configuration Location:** Specify the following:
   - **Hostname / IP Address:** Specify the fully qualified domain name (FQDN) or IP address of the server where CIS will be configured. For example, `wdccisserver.labs.wdc.acme.com`.
   - **Configuration Path:** Specify the path to store CIS configuration files and log files. By default, the path is set to root (/).
3. **Database:** By default **Use external database** is disabled. In this case, you must specify the MariaDB password to configure the local database.

   If you prefer to Use external database, perform the following steps:

   1. Select either **MariaDB** or **MS SQL** database.
   2. Specify the database host name or IP address and port. By default, the database port for MariaDB is 3306 and MS SQL is 1433.
   3. Specify the user name and password for the database.
   4. **Use secure connection:** Enables or disables the database connection to be secure. By default, this option is disabled.

If **MariaDB** database is selected, ensure to meet the following prerequisites before proceeding in the GUI:

a. Ensure to copy MariaDB client certificates to the CIS server at `/etc/opt/novell/cis/db/certs`.

b. In the MySQL configuration file (`/etc/my.cnf`) under the `[mysqld]` section, update the following paths:

```
[mysqld]
ssl=1
ssl-ca=/etc/opt/novell/cis/db/certs/ca-cert.pem
ssl-cert=/etc/opt/novell/cis/db/certs/client-cert.pem
ssl-key=/etc/opt/novell/cis/db/certs/client-key.pem
```

- **Client CA Certificate file path:** Specify the path of client Certificate Authority (CA) file in `.pem` format.
- **Client Certificate file path:** Specify the path of the client certificate file in `.pem` format.
- **Client Key file path:** Specify the path of the key file associated with the client certificate in `.pem` format.

4 **Docker Network Setting:** The default subnet of cisnet docker is 172.16.0.0/16. If the default subnet conflicts with your current network, modify the subnet address.

For example: 192.168.0.0/16 or 10.10.0.0/16

NOTE: When creating a custom subnet with a mask, ensure that the host minimum and maximum subnet addresses do not overlap with existing subnet ranges. To accomplish this, choose a subnet address and mask combination that is compatible with your network topology, ensuring that the host range is outside of any existing subnet ranges.

---

5 **Infrastructure Server:** Specify the following:

- **ZooKeeper:** By default, it is configured with the CIS server IP and ZooKeeper port is 2181.
- **OpenSearch:** By default, it is configured with the CIS server IP and OpenSearch port is 9400.
- **Kafka:** By default, it is configured with the CIS server IP and Kafka port is 9092.

6 Click **Next**.

7 **Admin Context:** Specify the following:

- **CIS Admin Name with Context:** Specify the LDAP distinguished name (DN) of the user who administers the CIS server. For example, `cn=admin,o=acme`.
- **Admin Password:** Specify the password for the CIS administrator.
- **Agent Search Context:** Specify the LDAP distinguished name (DN) of the container object under which the NCP server objects of the OES server resides that connects to the CIS server. The OES server includes the agents that connects to the CIS server. The CIS admin user must have supervisory rights on this server context.

8 Click **Next**. Review the configuration summary and then click **Finish**.

9 Restart the agent services in all the servers connected under **Agent Search Context** for connecting to CIS server and displaying the status of the servers in the CIS Management Console.

```
systemctl restart oes-core-agent.service oes-dashboard-agent.service
oes-cis-agent.service oes-cis-recall-agent.service oes-cis-
scanner.service

systemctl status oes-core-agent.service oes-dashboard-agent.service
oes-cis-agent.service oes-cis-recall-agent.service oes-cis-
scanner.service
```

Configure CIS as a Standalone Server in NSS Media

Choose this option to configure Apache Kafka, Apache ZooKeeper, OpenSearch, database and CIS services on the same server.

Prerequisites

- Before you start with CIS configuration, ensure to meet the requirements mentioned in Section 3.3, “CIS Requirements,” on page 19 are met.
- A local database is created during CIS Standalone server configuration. Ensure that there is no database already configured on this server.
- If you prefer an additional database ensure that the database is installed and configured. For information on how to install and configure MariaDB, see Appendix B, “Installing and Configuring MariaDB,” on page 105. If you want to use already configured database (MariaDB or MS SQL) with CIS, ensure that the database is up and running.

Procedure

1. On the CIS deployment page, select **Configure CIS as a Standalone Server** deployment type and then click **Next**.
2. **Configuration Location:** Specify the following:
   - **Hostname / IP Address:** Specify the fully qualified domain name (FQDN) or IP address of the server where CIS will be configured. For example, `wdccisserver.labs.wdc.acme.com`.
   - **Configuration Path:** Specify the path `/media/nss/LOCAL_NSSVOLUME` or `/media/nss/CLUSTER_NSSVOLUME` to store CIS configuration files and log files depending on your requirement. Ensure the available space is equal or greater than 100 GB and you must LUM enable the `cisuser` and `cisgroup`. For more information, see Section 4.4, “LUM Enabling CIS User and CIS Group,” on page 39.

     If you are using `CLUSTER_NSSVOLUME` you need to modify the cluster resource to update the Load and Unload script with CIS service. For more information, see “Modifying the Load, Unload, and Monitor Scripts” on page 27.
3. **Database:** By default Use external database is disabled. In this case, you must specify the MariaDB password to configure the local database.

   If you prefer to use external database, perform the following steps:

   1. Select either **MariaDB** or **MS SQL** database.
   2. Specify the database host name or IP address and port. By default, the database port for MariaDB is 3306 and MS SQL is 1433.
   3. Specify the user name and password for the database.

4. **Use secure connection:** Enables or disables the database connection to be secure. By default, this option is disabled.

   If **MariaDB** database is selected, ensure to meet the following prerequisites before proceeding in the GUI:

   a. Ensure to copy MariaDB client certificates to the CIS server at `/etc/opt/novell/cis/db/certs`.

   b. In the MySQL configuration file (`/etc/my.cnf`) under the `[mysqld]` section, update the following paths:

   ```
   [mysqld]
   ssl=1
   ssl-ca=/etc/opt/novell/cis/db/certs/ca-cert.pem
   ssl-cert=/etc/opt/novell/cis/db/certs/client-cert.pem
   ssl-key=/etc/opt/novell/cis/db/certs/client-key.pem
   ```

   - **Client CA Certificate file path:** Specify the path of client Certificate Authority (CA) file in `.pem` format.
   - **Client Certificate file path:** Specify the path of the client certificate file in `.pem` format.
   - **Client Key file path:** Specify the path of the key file associated with the client certificate in `.pem` format.

4 **Docker Network Setting:** The default subnet of cisnet docker is 172.16.0.0/16. If the default subnet conflicts with your current network, modify the subnet address.

For example: 192.168.0.0/16 or 10.10.0.0/16

NOTE: When creating a custom subnet with a mask, ensure that the host minimum and maximum subnet addresses do not overlap with existing subnet ranges. To accomplish this, choose a subnet address and mask combination that is compatible with your network topology, ensuring that the host range is outside of any existing subnet ranges.

---

5 **Infrastructure Server:** Specify the following:

- **ZooKeeper:** By default, it is configured with the CIS server IP and ZooKeeper port is 2181.
- **OpenSearch:** By default, it is configured with the CIS server IP and OpenSearch port is 9400.
- **Kafka:** By default, it is configured with the CIS server IP and Kafka port is 9092.

6 Click **Next**.

7 **Admin Context:** Specify the following:

- **CIS Admin Name with Context:** Specify the LDAP distinguished name (DN) of the user who administers the CIS server. For example, cn=admin,o=acme.
- **Admin Password:** Specify the password for the CIS administrator.
- **Agent Search Context:** Specify the LDAP distinguished name (DN) of the container object under which the NCP server objects of the OES server resides that connects to the CIS server. The OES server includes the agents that connects to the CIS server. The CIS admin user must have supervisory rights on this server context.

8 Click **Next**. Review the configuration summary and then click **Finish**.

9 Restart the agent services in all the servers in the tree for displaying the status of the servers in CIS Management Console.

```
systemctl restart oes-core-agent.service oes-dashboard-agent.service
oes-cis-agent.service oes-cis-recall-agent.service oes-cis-
scanner.service
```

```
systemctl status oes-core-agent.service oes-dashboard-agent.service
oes-cis-agent.service oes-cis-recall-agent.service oes-cis-
scanner.service
```

Modifying the Load, Unload, and Monitor Scripts

1 Log in to iManager.

2 Under Roles and Tasks, select **Clusters > My Clusters**, then select the cluster.

If the cluster does not appear in your personalized list of clusters to manage, you can add it. Click **Add**, browse and select the cluster, then click **OK**. Wait for the cluster to appear in the list and report its status, then select the cluster.

3 On the Cluster Manager page or Cluster Options page, select the cluster resource to view its properties, then click the **Scripts** tab.

4 Click the **Load Script, Unload,** or **Monitor Script** links to view or modify the scripts. If you modify a script, click **Apply** to save your changes before you leave the page.

Changes do not take effect until you take the resource offline, and bring it online again.

4a Edit the load script for the Cluster Pool. Add the following lines to the existing load script before the `exit 0` statement.

```
# start CIS services
exit_on_error /usr/bin/systemctl start oes-cis-fluentbit.service
exit_on_error /usr/bin/systemctl start oes-cis-
configuration.service

# start CIS infra services
exit_on_error /usr/bin/systemctl start oes-cis-zk.service
exit_on_error /usr/bin/systemctl start oes-cis-opensearch.service
exit_on_error /usr/bin/systemctl start oes-cis-kafka.service

# start CIS core services
exit_on_error /usr/bin/systemctl start oes-cis-auth.service
exit_on_error /usr/bin/systemctl start oes-cis-data.service
exit_on_error /usr/bin/systemctl start oes-cis-metadata.service
exit_on_error /usr/bin/systemctl start oes-cis-policy.service
exit_on_error /usr/bin/systemctl start oes-cis-mgmt.service
exit_on_error /usr/bin/systemctl start oes-dashboard.service
exit_on_error /usr/bin/systemctl start oes-cis-aggregator.service
exit_on_error /usr/bin/systemctl start oes-cis-collector.service
exit_on_error /usr/bin/systemctl start oes-cis-
repaggregator.service
exit_on_error /usr/bin/systemctl start oes-cis-repcollector.service
exit_on_error /usr/bin/systemctl start oes-cis-gateway.service

# check the services
exit_on_error /usr/bin/systemctl is-active oes-cis-
fluentbit.service
```

```
exit_on_error /usr/bin/systemctl is-active oes-cis-
configuration.service
exit_on_error /usr/bin/systemctl is-active oes-cis-zk.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
opensearch.service
exit_on_error /usr/bin/systemctl is-active oes-cis-kafka.service
exit_on_error /usr/bin/systemctl is-active oes-cis-auth.service
exit_on_error /usr/bin/systemctl is-active oes-cis-data.service
exit_on_error /usr/bin/systemctl is-active oes-cis-metadata.service
exit_on_error /usr/bin/systemctl is-active oes-cis-policy.service
exit_on_error /usr/bin/systemctl is-active oes-cis-mgmt.service
exit_on_error /usr/bin/systemctl is-active oes-dashboard.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
aggregator.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
collector.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
repaggregator.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
repcollector.service
exit_on_error /usr/bin/systemctl is-active oes-cis-gateway.service

# restart firewall if its running
systemctl status firewalld.service
if [ $? -eq 0 ]; then
    ignore_error systemctl restart firewalld.service
fi
```

4b Edit the unload script for the Cluster Pool. Add the following lines to the existing unload script after the `/opt/novell/ncs/lib/ncsfuncs` statement:

```
# stop cis services
ignore_error /usr/bin/systemctl stop oes-cis-fluentbit.service
ignore_error /usr/bin/systemctl stop oes-cis-auth.service
ignore_error /usr/bin/systemctl stop oes-cis-data.service
ignore_error /usr/bin/systemctl stop oes-cis-metadata.service
ignore_error /usr/bin/systemctl stop oes-cis-policy.service
ignore_error /usr/bin/systemctl stop oes-cis-mgmt.service
ignore_error /usr/bin/systemctl stop oes-dashboard.service
ignore_error /usr/bin/systemctl stop oes-cis-aggregator.service
ignore_error /usr/bin/systemctl stop oes-cis-collector.service
ignore_error /usr/bin/systemctl stop oes-cis-repaggregator.service
ignore_error /usr/bin/systemctl stop oes-cis-repcollector.service
ignore_error /usr/bin/systemctl stop oes-cis-gateway.service
ignore_error /usr/bin/systemctl stop oes-cis-configuration.service

# stop infra services
ignore_error /usr/bin/systemctl stop oes-cis-kafka.service
ignore_error /usr/bin/systemctl stop oes-cis-opensearch.service
ignore_error /usr/bin/systemctl stop oes-cis-zk.service
```

4c Edit the monitor script for the Cluster Pool. Add the following lines to the existing monitor script before the `exit 0` statement.

```
exit_on_error /usr/bin/systemctl is-active oes-cis-
fluentbit.service
exit_on_error /usr/bin/systemctl is-active oes-cis-zk.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
opensearch.service
exit_on_error /usr/bin/systemctl is-active oes-cis-kafka.service
exit_on_error /usr/bin/systemctl is-active oes-cis-auth.service
exit_on_error /usr/bin/systemctl is-active oes-cis-data.service
exit_on_error /usr/bin/systemctl is-active oes-cis-metadata.service
exit_on_error /usr/bin/systemctl is-active oes-cis-policy.service
exit_on_error /usr/bin/systemctl is-active oes-cis-mgmt.service
exit_on_error /usr/bin/systemctl is-active oes-dashboard.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
aggregator.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
collector.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
repaggregator.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
repcollector.service
exit_on_error /usr/bin/systemctl is-active oes-cis-gateway.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
configuration.service
```

Configure Infrastructure Services

Choose this option to configure Apache Kafka, Apache ZooKeeper, and OpenSearch in high availability (HA) mode.

A multi node high availability configuration of infrastructure server helps to increase the efficiency and availability of the infrastructure server. It is mandatory to configure atleast three HA nodes. You can configure up to seven nodes.

Prerequisites

- Before you start with infrastructure services configuration, ensure that the requirements mentioned in Section 3.3, “CIS Requirements,” on page 19 are met.
- Ensure that you allocate sufficient disk space for the infrastructure server.

Procedure

1. To automatically make the server HA ready, click **Start**.

   After successful configuration, click **OK**. Re-login to the console to view the steps to complete the Infrastructure service configuration (using CLI).

2. (Using CLI) To setup the K3s cluster, perform the following on the terminal console of this server:

   2a Open a terminal console, then log in as a `root` user.

   2b Initialize a K3s cluster.

```
cis_ext_service.sh enableha <first_node_ip>
```

2c Add a manager to an existing K3s cluster.

```
cis_ext_service.sh enableha <first_node_ip> <node_ip>
```

NOTE: Repeat this step on every Infrastructure server node.

2d On the last HA node, start the Infrastructure services.

```
cis_ext_service.sh start
```

After successful configuration of Infrastructure services, continue with "Configure CIS Services" on page 30.

Configure CIS Services

Choose this option to configure CIS as a single node or a NCS (OES Cluster Services) cluster resource.

Prerequisites

- Before you start with CIS configuration, ensure that the requirements mentioned in Section 3.3, "CIS Requirements," on page 19 are met.
- Ensure that the infrastructure services (in high availability mode) is configured.
- For CIS server to function in a cluster environment, ensure that all nodes are configured with OES 25.1. Novell Cluster Services must be installed and running on the servers that have CIS installed. For information, see Installing, Configuring, and Repairing OES Cluster Services in the OES Cluster Services for Linux Administration Guide.
- Create a dedicated pool resource and volume to run the CIS service. Ensure to cluster-enable the pool resource.
- You must LUM enable the `cisuser` and `cisgroup` in all the server where CIS services will be used. For more information, see Section 4.4, "LUM Enabling CIS User and CIS Group," on page 39.

- Ensure that the database is installed and configured. For information on how to install and configure MariaDB, see Appendix B, "Installing and Configuring MariaDB," on page 105. If you want to use already configured database (MariaDB or MS SQL) with CIS, ensure that the database is up and running.

Procedure

1 **Configuration Location:** Specify the following:

Configure CIS as a NCS cluster resource: Configures CIS in a cluster environment. By default, this option is enabled.

- **Hostname / IP address:** Specify the server address for standalone and resource or virtual IP address or hostname of the NCS cluster resource where the CIS server is part of.

NOTE: All IP addresses used by the master cluster IP address, its cluster servers, and its cluster resources must be on the same IP subnet. They do not need to be contiguous addresses.

- **Configuration Path:** Specify the NSS media path to store CIS configuration files and log files. For example, /media/nss/CISVOL.

2 **Database:** Specify the following:

2a Select either **MariaDB** or **MS SQL** database.

2b Specify the database host name or IP address and port. By default, the database port for MariaDB is 3306 and MS SQL is 1433.

2c Specify the user name and password for the database.

2d **Connection Parameters:** If your MS SQL is configured with connection parameters, specify the value.This is not a mandatory field.

2e **Use secure connection:** Enables or disables the database connection to be secure. By default, this option is disabled.

If **MariaDB** database is selected, ensure to meet the following prerequisites before proceeding in the GUI:

1. Ensure to copy MariaDB client certificates to the CIS server at `/etc/opt/novell/cis/db/certs`.
2. In the MySQL configuration file (`/etc/my.cnf`) under the `[mysqld]` section, update the following paths:

```
[mysqld]
ssl=1
ssl-ca=/etc/opt/novell/cis/db/certs/ca-cert.pem
ssl-cert=/etc/opt/novell/cis/db/certs/client-cert.pem
ssl-key=/etc/opt/novell/cis/db/certs/client-key.pem
```

- **Client CA Certificate file path:** Specify the path of client Certificate Authority (CA) file in .pem format.
- **Client Certificate file path:** Specify the path of the client certificate file in format.
- **Client Key file path:** Specify the path of the key file associated with the client certificate in `.pem` format.

3 **Docker Network Setting:** The default subnet of cisnet docker network is 172.16.0.0/16. If the default subnet conflicts with your current network, modify the subnet address.

For example: 192.168.0.0/16 or 10.10.0.0/16

NOTE: When creating a custom subnet with a mask, ensure that the host minimum and maximum subnet addresses do not overlap with existing subnet ranges. To accomplish this, choose a subnet address and mask combination that is compatible with your network topology, ensuring that the host range is outside of any existing subnet ranges.

---

4 **Infrastructure Server Host name / IP address:** Specify the host name or IP address of all the configured infrastructure server HA nodes. Separate multiple entries with a comma.

5 Click **Validate**. If there are errors, ensure to resolve them before you proceed.

6 **CIS Admin Name with Context:** Specify the LDAP distinguished name (DN) of the user who administers the CIS server. For example, `cn=admin,o=acme`.

7 **Admin Password:** Specify the password for the CIS administrator.

8 **Agent Search Context:** Specify the LDAP distinguished name (DN) of the container object under which the NCP server objects of the OES server resides that connects to the CIS server. The OES server includes the agents that connects to the CIS server. The CIS admin user must have supervisory rights on this server context.

9 Click **Next**. Review the configuration summary and then click **Finish**.

10 When CIS is configured with cluster resource IP or hostname, you must replace the certificates in `/etc/opt/novell/cis/certs` with the certificate that you have created manually for CIS. To create the certificates, see Appendix C, “Creating Certificates,” on page 107.

11 Modify the Load, Unload and Monitor script.

11a Log in to iManager.

11b Under Roles and Tasks, select **Clusters > My Clusters**, then select the cluster.

If the cluster does not appear in your personalized list of clusters to manage, you can add it. Click **Add**, browse and select the cluster, then click **OK**. Wait for the cluster to appear in the list and report its status, then select the cluster.

11c On the Cluster Manager page or Cluster Options page, select the CIS cluster resource to view its properties, then click the **Scripts** tab.

11d Click the **Load Script, Unload,** or **Monitor Script** links to view or modify the scripts. If you modify a script, click **Apply** to save your changes before you leave the page.

Changes do not take effect until you take the resource offline, and bring it online again.

11d1 Edit the load script for the Cluster Pool. Add the following lines to the existing load script before the `exit 0` statement.

```
# update the links

/bin/bash /opt/novell/cis/bin/update_cislinks.sh cis <New media
path>

# Verify the cis subnet address
/bin/bash /opt/novell/cis/bin/update_docker_subnet.sh


# start the services

exit_on_error /usr/bin/systemctl start oes-cis-fluentbit.service
exit_on_error /usr/bin/systemctl start oes-cis-
configuration.service
exit_on_error /usr/bin/systemctl start oes-cis-auth.service
exit_on_error /usr/bin/systemctl start oes-cis-data.service
exit_on_error /usr/bin/systemctl start oes-cis-metadata.service
exit_on_error /usr/bin/systemctl start oes-cis-policy.service
exit_on_error /usr/bin/systemctl start oes-cis-mgmt.service
exit_on_error /usr/bin/systemctl start oes-dashboard.service
exit_on_error /usr/bin/systemctl start oes-cis-
aggregator.service
exit_on_error /usr/bin/systemctl start oes-cis-collector.service
exit_on_error /usr/bin/systemctl start oes-cis-
repaggregator.service
exit_on_error /usr/bin/systemctl start oes-cis-
repcollector.service
exit_on_error /usr/bin/systemctl start oes-cis-gateway.service
```

```
# wait before checking their status

sleep 5

# check the services

exit_on_error /usr/bin/systemctl is-active oes-cis-
fluentbit.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
configuration.service
exit_on_error /usr/bin/systemctl is-active oes-cis-auth.service
exit_on_error /usr/bin/systemctl is-active oes-cis-data.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
metadata.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
policy.service
exit_on_error /usr/bin/systemctl is-active oes-cis-mgmt.service
exit_on_error /usr/bin/systemctl is-active oes-dashboard.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
aggregator.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
collector.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
repaggregator.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
repcollector.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
gateway.service

# restart firewall if its running

systemctl status firewalld.service

if [ $? -eq 0 ]; then

    ignore_error systemctl restart firewalld.service

fi
```

11d2 Edit the unload script for the Cluster Pool. Add the following lines to the existing unload script after the `/opt/novell/ncs/lib/ncsfuncs` statement:

```
ignore_error /usr/bin/systemctl stop oes-cis-fluentbit.service
ignore_error /usr/bin/systemctl stop oes-cis-auth.service
ignore_error /usr/bin/systemctl stop oes-cis-data.service
ignore_error /usr/bin/systemctl stop oes-cis-metadata.service
ignore_error /usr/bin/systemctl stop oes-cis-policy.service
ignore_error /usr/bin/systemctl stop oes-cis-mgmt.service
ignore_error /usr/bin/systemctl stop oes-dashboard.service
ignore_error /usr/bin/systemctl stop oes-cis-aggregator.service
ignore_error /usr/bin/systemctl stop oes-cis-collector.service
ignore_error /usr/bin/systemctl stop oes-cis-
repaggregator.service
ignore_error /usr/bin/systemctl stop oes-cis-
repcollector.service
ignore_error /usr/bin/systemctl stop oes-cis-gateway.service
ignore_error /usr/bin/systemctl stop oes-cis-
configuration.service
```

11d3 Edit the monitor script for the Cluster Pool. Add the following lines to the existing monitor script before the `exit 0` statement.

```
exit_on_error /usr/bin/systemctl is-active oes-cis-
fluentbit.service
exit_on_error /usr/bin/systemctl is-active oes-cis-auth.service
exit_on_error /usr/bin/systemctl is-active oes-cis-data.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
metadata.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
policy.service
exit_on_error /usr/bin/systemctl is-active oes-cis-mgmt.service
exit_on_error /usr/bin/systemctl is-active oes-dashboard.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
aggregator.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
collector.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
repaggregator.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
repcollector.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
gateway.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
configuration.service
```

12 Restart the agent services in all the servers connected under **Agent Search Context** for connecting to CIS server and displaying the status of the servers in the CIS Management Console.

```
systemctl restart oes-core-agent.service oes-dashboard-agent.service
oes-cis-agent.service oes-cis-recall-agent.service oes-cis-
scanner.service
```

```
systemctl status oes-core-agent.service oes-dashboard-agent.service
oes-cis-agent.service oes-cis-recall-agent.service oes-cis-
scanner.service
```

13 To add a new node to this cluster:

13a Ensure that the CIS pattern is installed and updated with the latest patches.

13b Ensure this node is part of the same cluster.

13c Migrate the CIS resource to the new node.

Configure Data Scale

Choose this option to improve the latency of the data access.

Prerequisite

Before you start with CIS configuration, ensure that the requirements mentioned in Section 3.3, “CIS Requirements,” on page 19 are met.

Data and Gateway

Choose this option to configure the data and gateway service on this server. It is recommended to select this option if this is the first data scale server getting configured, because the gateway service provides load balancing on the data service.

1 **Host names:** Specify the following:

1a **Data Server:** Displays the host name or IP address of the local server.

1b **Configure gateway as a NCS cluster resource:** Enables or disables the gateway as a NCS cluster resource. By default, this option is enabled.

- If this option is enabled, specify the IP address of the NCS cluster resource where gateway is configured.

  NOTE: All IP addresses used by the master cluster IP address, its cluster servers, and its cluster resources must be on the same IP subnet. They do not need to be contiguous addresses.

- If this option is disabled, the host name or IP address of the local server is displayed.

NOTE: It is recommended to configure gateway as a cluster to avoid interruption of the service.

2 **General:** Specify the following:

2a **CIS Server Address:** Specify the host name or IP address where the CIS server is configured.

2b **Infrastructure Server Host name:** Specify the host name or IP address of all the configured HA nodes. Separate multiple entries with a comma.

3 **Certificates:** Specify the following:

3a **eDirectory Server:** Displays the CIS server host name and port where the eDirectory server is configured. By default, eDirectory server port is 524.

3b **Cluster Resource Host name:** Specify the fully qualified domain name (FQDN) of a NCS cluster resource where the CIS server is part of. Separate multiple entries with a comma.

3c **Cluster Resource IP Address:** Specify the virtual IP address of the NCS cluster resource where the CIS server is part of. Separate multiple entries with a comma.

4 Click **Next**. Review the configuration summary and then click **Finish**.

Data

Choose this option to configure the server as a standalone data server or connect the data server to an existing gateway server.

1 **Host names:** Specify the following:

1a **Connect to Gateway server:** Enables or disables the data server to connect to gateway. By default, this option is enabled.

- If this option is enabled, displays the host name or IP address of the local server that will be connected to gateway.

  Gateway: Specify the host name or IP address of the server where gateway service is configured.

- If this option is disabled, the host name or IP address of the local server is displayed.

2 **General:** Specify the following:

2a **CIS Server Address:** Specify the host name or IP address of the server that is configured with CIS.

2b **Infrastructure Server Host name:** Specify the host name or IP address of all the configured HA nodes. Separate multiple entries with a comma.

3 **Certificates:** Specify the following:

3a **eDirectory Server:** Displays the CIS server host name and port where the eDirectory server is configured. By default, eDirectory server port is 524.

3b **Cluster Resource Host name:** Specify the fully qualified domain name (FQDN) of a NCS cluster resource where the CIS server is part of. Separate multiple entries with a comma.

3c **Cluster Resource IP Address:** Specify the virtual IP address of the NCS cluster resource where the CIS server is part of. Separate multiple entries with a comma.

4 Click **Next**. Review the configuration summary and then click **Finish**.

Gateway

Choose this option to configure only the gateway service on this server. You can connect multiple data servers to this gateway server for load balancing between the OES agents and data services.

1 **Host names:** Specify the following:

   1a **Configure gateway as a NCS cluster resource:** Enables or disables the gateway as a NCS cluster resource. By default, this option is enabled.

   - If this option is enabled, specify the IP address of the NCS cluster resource where the gateway is configured.
   - If this option is disabled, the host name or IP address of the local server is displayed.

2 **General:** Specify the following:

   2a **CIS Server Address:** Specify the host name or IP address where the CIS server is configured.

   2b **Infrastructure Server Host name:** Specify the host name or IP address of all the configured HA nodes. Separate multiple entries with a comma.

3 **Certificates:** Specify the following:

   3a **eDirectory Server:** Displays the CIS server host name and port where the eDirectory server is configured. By default, eDirectory server port is 524.

   3b **Cluster Resource Host name:** If gateway is configured as a NCS clustered resource, specify the fully qualified domain name (FQDN) of a NCS cluster resource where the gateway server is configured. Separate multiple entries with a comma.

   Host name: Specify the fully qualified domain name (FQDN) of the local server. Separate multiple entries with a comma.

   3c **Cluster Resource IP Address:** If gateway is configured as a NCS clustered resource, specify the virtual IP address of a NCS cluster resource where the gateway server is configured. Separate multiple entries with a comma.

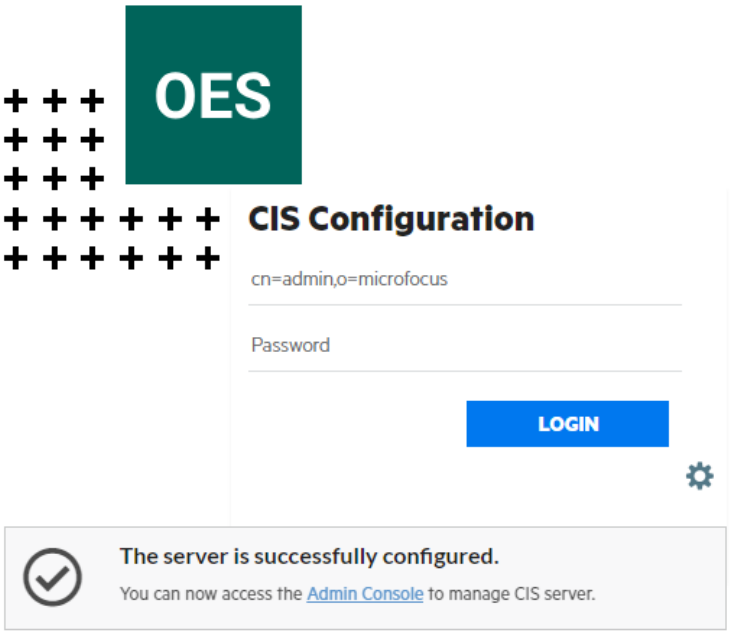
   IP Address: Specify the IP address of the local server. Separate multiple entries with a comma.

4 Click **Next**. Review the configuration summary and then click **Finish**.

4.3 Verifying the CIS Configuration

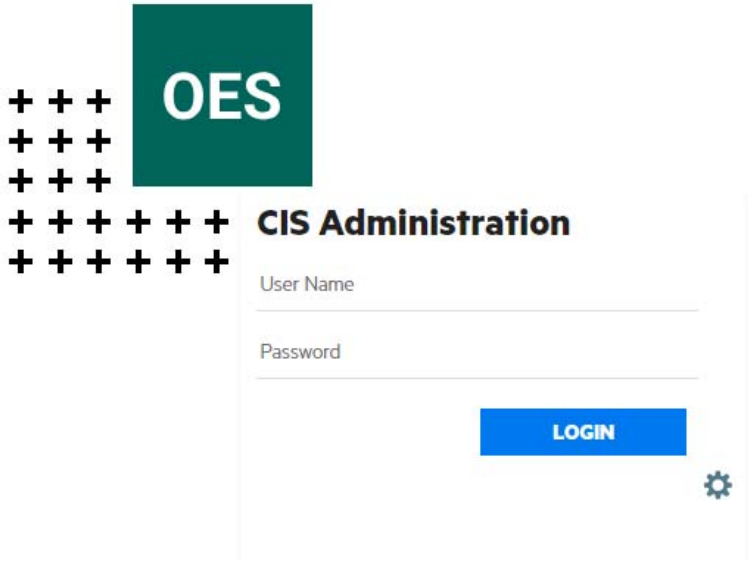
After successful configuration of CIS and its infrastructure services, perform any one of the following:

- Point your browser to https://<*OES server IP address or host name*>:8105 and click **Admin Console** link to go to CIS Administration login page.



OR

- Point your browser to https://<*OES server IP address or host name*>:8344.



- To verify the type of server configuration, run the following command:

  `cat /etc/opt/novell/cis/configurationStatus.json`

  The `configType` parameter displays the following:

  - `"configType":"infraHA"` - This is an Infrastructure server.
  - `"configType":"core"` - This is a CIS server.

- `"configType":"scale"` - This is a Data Scale server.
- `"configType":"standalone"` - This is a Standalone server.

4.4 LUM Enabling CIS User and CIS Group

Choose one of the methods to enable Linux User Management (LUM) for CIS user (`cisuser`) and CIS group (`cisgroup`), followed by assigning rights to the volume:

- Section 4.4.1, “Using Unified Management Console (UMC),” on page 39
- Section 4.4.2, “Using Command Line Interface,” on page 40
- Section 4.4.3, “Using Script,” on page 41

4.4.1 Using Unified Management Console (UMC)

If the CIS configuration is core and located in the cluster volume, delete the `cisgroup` and `cisuser` accounts on the workstations at each cluster node assigned to the CIS server resource before creating the LUM-enabled `cisgroup` and `cisuser`.

NOTE: Beginning with OES 24.4.1, you can LUM enable `cisuser` and `cisgroup` using UMC.

---

1. Delete the local CIS user.

   ```
   userdel cisuser
   ```

2. Verify if the CIS user is deleted.

   ```
   cat /etc/passwd | grep "cisuser"
   ```

3. Delete the local CIS group.

   ```
   groupdel cisgroup
   ```

4. Verify if the CIS group is deleted.

   ```
   cat /etc/group | grep "cisgroup"
   ```

5. Create `cisuser` using Identity Console (IC). See, Creating a User in Identity Console (https://www.netiq.com/documentation/identity-console/identity_console-admin/data/t491gw6muco1.html).
6. Create and LUM-enable `cisgroup` only once, on any one cluster node. See, How to create and enable LUM for groups? in Unified Management Console.
7. Enable `cisuser` using UMC. See, How to add and enable a user for LUM? in Unified Management Console.
8. Assign the following rights to the NSS volume that stores the CIS configuration:
   - Read
   - Write
   - Create
   - Erase

- Modify
- File scan

See, How to add trustee(s) for a volume, file, or folder? in Unified Management Console.

9 (**Conditional**) If the CIS configuration is core and configured in the cluster volume, enable `cisgroup` and `cisuser` on the workstation at each cluster node assigned to the CIS server resource. See, How to enable existing groups or users for LUM? in Unified Management Console.

4.4.2 Using Command Line Interface

If the CIS configuration is core and configured in the cluster volume, enable `cisgroup` and `cisuser` on the workstation at each cluster node assigned to the CIS server resource.

1 Delete the local CIS user.

```
userdel cisuser
```

2 Verify if the CIS user is deleted.

```
cat /etc/passwd | grep "cisuser"
```

3 Delete the local CIS group.

```
groupdel cisgroup
```

4 Verify if the CIS group is deleted.

```
cat /etc/group | grep "cisgroup"
```

5 Create a LUM-enabled `cisgroup` object for all cluster nodes assigned to the CIS server resource.

```
namgroupadd [-a adminFDN] - x group_context -W workstation_name
group_name
```

Example for single UNIX workstation:

```
namgroupadd -a cn=admin,o=microfocus -x o=microfocus cisgroup -W
server1
```

Example for multiple UNIX workstation:

```
namgroupadd -a cn=admin,o=microfocus -x o=microfocus cisgroup -W
server1,server2,server3
```

6 Create a Linux user object.

```
namuseradd [-a adminFDN] -x user_context [-c comment] -g
primary_groupFDN [-s shell] login_name
```

```
namuseradd -a cn=admin,o=microfocus -x o=microfocus -c cisuser -g
cn=cisgroup,o=microfocus -s /sbin/nologin cisuser
```

7 Refresh the `namcd` cache immediately or restart the `namcd` service on all cluster nodes assigned to the CIS server resource.

```
namconfig cache_refresh
```

or

```
systemctl restart namcd.service
```

8 Verify if `cisgroup` and `cisuser` have been successfully LUM-enabled at each cluster node.

```
namuserlist cisuser
```

```
namgrouplist cisgroup
```

9 Provide rights to the configuration and log folder.

```
rights -f /media/nss/CISVOLUME -r rwfcem trustee
cisuser.microfocus.oes_tree
```

10 (**Conditional**) If the CIS configuration is core and configured in the cluster volume, enable `cisgroup` and `cisuser` on the workstation at each cluster node assigned to the CIS server resource.

You can do this by running the following commands on one of the cluster nodes. These commands will automatically run on all other nodes or servers:

```
cluster exec "/usr/sbin/userdel cisuser"
```

```
cluster exec "/usr/sbin/groupdel cisgroup"
```

```
cluster exec "/usr/bin/namgroupadd -a cn=admin,o=microfocus -x
o=microfocus cisgroup -W server1,server2,server3"
```

```
cluster exec "/usr/bin/namconfig cache_refresh"
```

```
cluster exec "/usr/bin/systemctl restart nscd"
```

4.4.3 Using Script

Beginning with OES 25.2, you can run `cis_enable_lum_user.sh` script to enable LUM for CIS user (`cisuser`) and CIS group (`cisgroup`), then assign rights to the volume.

1 Run this script where CIS cluster resource is running.

```
sh /opt/novell/cis/bin/cis_enable_lum_user.sh -a adminFDN -x
user_context -v CIS_volume_name -t TREENAME
```

2 (**Conditional**) If the CIS configuration is core and configured in the cluster volume, run the following script on the other nodes where you migrate the cluster volume.

```
sh /opt/novell/cis/bin/cis_enable_lum_user.sh -a adminFDN -x
user_context -t TREENAME
```

5 Updating (Patching) CIS Configured Server

The instruction in this chapter are for updating or patching the CIS configured servers.

Type of Server

To find out whether the server is a standalone, infrastructure, CIS, or data scale, execute the following command:

```
cat /etc/opt/novell/cis/configurationStatus.json
```

The `configType` parameter displays the following:

- `"configType": "standalone"` - This is an Standalone server.
- `"configType":"infraHA"` - This is an Infrastructure server.
- `"configType":"core"` - This is a CIS server.
- `"configType":"scale"` - This is a Data Scale server.

5.1 Prerequisites

This prerequisites only applies if you are updating to CIS 25.2.

- If CIS is configured in NSS media or NCS cluster resource, enable LUM for CIS user (`cisuser`) and CIS group (`cisgroup`), followed by assigning rights to the volume.
- For more information, see Section 4.4, “LUM Enabling CIS User and CIS Group,” on page 39.

5.2 Patching the Standalone or CIS Server

1. Remove old docker images.

   ```
   sh /opt/novell/cis/bin/cis_image_cleanup.sh
   ```

2. (Conditional) If the CIS server has been configured on the NSS media volume, then copy the newly updated files from the `cis_local` location to the media path (`/media/nss/CISVOL`).

   ```
   sh /opt/novell/cis/bin/copy_upgraded_files.sh
   ```

3. Restart the CIS services.

   ```
   systemctl restart oes-cis-zk.service oes-cis-kafka.service oes-cis-opensearch.service
   ```

   ```
   systemctl restart oes-cis-server.target
   ```

5.3 Patching the CIS Infrastructure Servers

1. Stop the infrastructure services on any one of the node.

   ```
   cis_ext_service.sh stop
   ```

2. Verify that infrastructure services are stopped.

   ```
   cis_ext_service.sh status
   ```

   The output displays, "**nothing found in stack: cis**".

3. Ensure that all the infrastructure nodes are on OES 25.1. Upgrade the service on all the infrastructure nodes (3/ 5/ 7 - based on the configuration).

   ```
   cis_ext_service.sh upgrade
   ```

   The output displays, "**Upgrade completed successfully.**"

4. Start the infrastructure service on any one of the node.

   ```
   cis_ext_service.sh start
   ```

6 Upgrading CIS Server

This topic describes steps to upgrade from OES 2023 or OES 23.4 CIS configured server to OES 24.4 or OES 25.1.

- Section 6.1, “Upgrading Standalone CIS Server,” on page 45
- Section 6.2, “Upgrading CIS in Multi-Server Environment,” on page 47

6.1 Upgrading Standalone CIS Server

- Section 6.1.1, “Prerequisites on Source Server,” on page 45
- Section 6.1.2, “Upgrading to OES 24.4 or OES 25.1 Server,” on page 45
- Section 6.1.3, “Data Transfer from Elasticsearch to OpenSearch,” on page 46

The detailed instructions for upgrading a standalone CIS server are provided in the following video:

http://www.youtube.com/watch?v=GBpYruXiOA8

6.1.1 Prerequisites on Source Server

- **Source Server:** OES 2023 or OES 24.3
- **CIS server:** OES 25.1
- **Certificates:** Backup certificates available in this path: `/etc/opt/novell/cis/certs`

6.1.2 Upgrading to OES 24.4 or OES 25.1 Server

1. Follow the step-by-step instructions for upgrading to OES 24.4 or OES 25.1 server. For more information, see Upgrading OES in the Installation Guide.
2. If CIS is configured on `/root`, `/home or /media/nss/VOL1` (non-clustered), the path is mounted.

   If CIS is configured on a cluster volume (for example, `/media/nss/CLUS_VOL`), then verify if the cluster volume is mounted. If not, then mount the cluster volume manually.
3. Verify if key-value pair `"cisConfigSuccess": true` is present in the `/etc/opt/novell/cis/configurationStatus.json` file.

   Do not proceed if this is not available and contact OpenText for further information.
4. Execute the following command to upgrade the CIS services:

   ```
   sh /opt/novell/cis/bin/cis_upgrade.sh
   ```

   On successful execution of upgrade script, a few of the CIS services are stopped.
5. Ensure that the database configured for CIS is up and running.

   5a If it is a local database, verify the status of the database service:

```
systemctl status mysql.service
```

5b If the database is down, then enable and restart it:

```
systemctl enable mysql.service
systemctl restart mysql.service
```

6 Verify the status of the CIS Infra services. If not running, then start the services.

/root or /home or /media/nss/VOL1 (non clustered):

```
systemctl status oes-cis-zk.service oes-cis-opensearch.service oes-cis-kafka.service
```

Start the logging and configuration services.

```
systemctl start oes-cis-fluentbit.service oes-cis-configuration.service
```

Start the Core services.

```
systemctl restart oes-cis-server.target
```

7 Ensure all the CIS services are running, by executing the following command:

```
docker ps -a
```

This displays the status of all the CIS services.

8 Verify the health of the CIS server.

```
cishealth
```

When the status displays “Healthy”, then the CIS server is successfully upgraded.

NOTE: The upgrade takes time to complete depending on the size of the database getting migrated from the earlier version of OES server. During this phase, the CIS health might display the status of some services as “Not Healthy” because the scanned data is getting updated. On completing the update, the health status changes to “Healthy”.

---

9 Restart the agent services.

```
systemctl restart oes-core-agent.service oes-dashboard-agent.service oes-cis-agent.service oes-cis-recall-agent.service oes-cis-scanner.service
```

```
systemctl status oes-core-agent.service oes-dashboard-agent.service oes-cis-agent.service oes-cis-recall-agent.service oes-cis-
```

```
scanner.service
```

6.1.3 Data Transfer from Elasticsearch to OpenSearch

If you upgrade from OES 2023, the CIS Admin Console's **Insights and Dashboard** pages will not display any data because elasticsearch stores the data for these pages.

To transfer the data from Elasticsearch to OpenSearch, follow these steps:

1 Ensure to have completed procedure mentioned in Section 6.1.2, “Upgrading to OES 24.4 or OES 25.1 Server,” on page 45.

NOTE: (Conditional) If CIS is configured on a cluster volume (for example, `/media/nss/CLUS_VOL`), then verify if the cluster volume is mounted. If not, then mount the cluster volume manually.

2 Verify the status of the Elasticsearch. If not running, restart the service.

```
systemctl status oes-cis-elastic.service
```

```
systemctl restart oes-cis-elastic.service
```

3 Verify the health of CIS.

```
cishealth
```

Before proceeding ensure CIS is healthy.

4 Move data from the Elasticsearch to OpenSearch:

```
sh /opt/novell/cis/bin/elastic_move_data.sh migrate
```

You can verify the logs at

```
/var/opt/novell/log/cis/cis_opensearch_move__<timestamp>.log
```

NOTE: The duration of the migration can be prolonged depending on the data saved in Elasticsearch.

5 Verify the data migration count.

```
sh /opt/novell/cis/bin/elastic_move_data.sh verify
```

6 On successfully transferring the data, the Insights and Dashboard pages of the CIS Admin Console will populate the existing data.

7 Cleanup the Elasticsearch data.

```
sh /opt/novell/cis/bin/elastic_move_data.sh cleanup
```

/media/nss/CLUS_VOL (clustered volumes): Replace the `oes-cis-elastic.service` with the `oes-cis-opensearch.service` in the Load, Unload, and Monitor script. For more information, see "Modifying the Load, Unload, and Monitor Scripts" on page 27. This ensures all the required services start on bringing the resource online.

6.2 Upgrading CIS in Multi-Server Environment

If you are upgrading from OES 23.4 or earlier release, see OES 23.4: CIS Administration Guide.

If you are upgrading from OES 24.3 to OES 24.4 or OES 25.1 then ensure that CIS multi-server with Docker Swarm configuration is moved to K3s.

- Section 6.2.1, "Recommendations for Upgrading CIS," on page 48
- Section 6.2.2, "Upgrading Infrastructure Servers from OES 24.3 to OES 24.4 or OES 25.1," on page 48
- Section 6.2.3, "Upgrading CIS Servers from OES 24.3 to OES 24.4 or OES 25.1," on page 49
- Section 6.2.4, "Upgrading Data Scale Server from OES 24.3 to OES 24.4 or OES 25.1," on page 52

6.2.1 Recommendations for Upgrading CIS

You must backup certificates available in this path: `/etc/opt/novell/cis/certs` and ensure to follow this sequence when upgrading CIS:

1. Infrastructure servers
2. CIS servers
3. Data Scale servers

Type of Server

To find out whether the server is an Infrastructure or CIS or Data Scale, execute the following command on the server:

```
cat /etc/opt/novell/cis/configurationStatus.json
```

The `configType` parameter displays the following:

- `"configType":"infraHA"` - This is an Infrastructure server.
- `"configType":"core"` - This is a CIS server.
- `"configType":"scale"` - This is a Data Scale server.

6.2.2 Upgrading Infrastructure Servers from OES 24.3 to OES 24.4 or OES 25.1

Procedure

1. Stop the infrastructure services on any one of the node with the following command:

   ```
   cis_ext_service.sh stop
   ```

2. To verify that infrastructure services are stopped, run the following command:

   ```
   cis_ext_service.sh status
   ```

   The output displays, "**nothing found in stack: cis**".

3. Ensure that all the infrastructure nodes are on OES 25.1. Run the following command on all the infrastructure nodes (3/ 5/ 7 - based on the configuration) to upgrade the service:

   ```
   cis_ext_service.sh upgrade
   ```

   The output displays, "**Upgrade completed successfully.**"

4. Run the following command on any one of the node to start the infrastructure service:

   ```
   cis_ext_service.sh start
   ```

5. Run the following command to display the status of all the CIS services:

   ```
   kubectl get pods
   ```

6.2.3 Upgrading CIS Servers from OES 24.3 to OES 24.4 or OES 25.1

1 On node 1, upgrade the CIS server to OES 24.4 or OES 25.1.

1a If CIS servers are configured with OES Cluster Services (NCS), then migrate the cluster resource to the upgraded node 1. Cluster resource will be up and running or might go to comatose because the CIS services are not updated with the latest changes that are done with OES 24.4.

1b Make the CIS cluster resource offline and manually mount the volumes (where CIS is configured).

1c Upgrade CIS by running the following script:

```
sh /opt/novell/cis/bin/cis_upgrade.sh
```

2 Modify the Load, Unload and Monitor script.

2a Log in to iManager.

2b Under Roles and Tasks, select **Clusters > My Clusters**, then select the cluster.

If the cluster does not appear in your personalized list of clusters to manage, you can add it. Click **Add**, browse and select the cluster, then click **OK**. Wait for the cluster to appear in the list and report its status, then select the cluster.

2c On the Cluster Manager page or Cluster Options page, select the CIS cluster resource to view its properties, then click the **Scripts** tab.

2d Click the **Load Script, Unload,** or **Monitor Script** links to view or modify the scripts. If you modify a script, click **Apply** to save your changes before you leave the page.

2d1 Edit the load script for the Cluster Pool as shown below:

```
# update the links

/bin/bash /opt/novell/cis/bin/update_cislinks.sh cis <New media
path>

# Verify the cis subnet address
/bin/bash /opt/novell/cis/bin/update_docker_subnet.sh

# start the services

exit_on_error /usr/bin/systemctl start oes-cis-fluentbit.service
exit_on_error /usr/bin/systemctl start oes-cis-
configuration.service
exit_on_error /usr/bin/systemctl start oes-cis-auth.service
exit_on_error /usr/bin/systemctl start oes-cis-data.service
exit_on_error /usr/bin/systemctl start oes-cis-metadata.service
exit_on_error /usr/bin/systemctl start oes-cis-policy.service
exit_on_error /usr/bin/systemctl start oes-cis-mgmt.service
exit_on_error /usr/bin/systemctl start oes-dashboard.service
exit_on_error /usr/bin/systemctl start oes-cis-
aggregator.service
exit_on_error /usr/bin/systemctl start oes-cis-collector.service
exit_on_error /usr/bin/systemctl start oes-cis-
repaggregator.service
exit_on_error /usr/bin/systemctl start oes-cis-
repcollector.service
```

```
exit_on_error /usr/bin/systemctl start oes-cis-gateway.service

# wait before checking their status

sleep 5

# check the services

exit_on_error /usr/bin/systemctl is-active oes-cis-
fluentbit.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
configuration.service
exit_on_error /usr/bin/systemctl is-active oes-cis-auth.service
exit_on_error /usr/bin/systemctl is-active oes-cis-data.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
metadata.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
policy.service
exit_on_error /usr/bin/systemctl is-active oes-cis-mgmt.service
exit_on_error /usr/bin/systemctl is-active oes-dashboard.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
aggregator.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
collector.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
repaggregator.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
repcollector.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
gateway.service

# restart firewall if its running

systemctl status firewalld.service

if [ $? -eq 0 ]; then

    ignore_error systemctl restart firewalld.service

fi
```

2d2 Edit the unload script for the Cluster Pool as shown below:

```
ignore_error /usr/bin/systemctl stop oes-cis-fluentbit.service
ignore_error /usr/bin/systemctl stop oes-cis-auth.service
ignore_error /usr/bin/systemctl stop oes-cis-data.service
ignore_error /usr/bin/systemctl stop oes-cis-metadata.service
ignore_error /usr/bin/systemctl stop oes-cis-policy.service
ignore_error /usr/bin/systemctl stop oes-cis-mgmt.service
ignore_error /usr/bin/systemctl stop oes-dashboard.service
ignore_error /usr/bin/systemctl stop oes-cis-aggregator.service
ignore_error /usr/bin/systemctl stop oes-cis-collector.service
ignore_error /usr/bin/systemctl stop oes-cis-
repaggregator.service
ignore_error /usr/bin/systemctl stop oes-cis-
repcollector.service
ignore_error /usr/bin/systemctl stop oes-cis-gateway.service
ignore_error /usr/bin/systemctl stop oes-cis-
configuration.service
```

2d3 Edit the monitor script for the Cluster Pool as shown below:

```
exit_on_error /usr/bin/systemctl is-active oes-cis-
fluentbit.service
exit_on_error /usr/bin/systemctl is-active oes-cis-auth.service
exit_on_error /usr/bin/systemctl is-active oes-cis-data.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
metadata.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
policy.service
exit_on_error /usr/bin/systemctl is-active oes-cis-mgmt.service
exit_on_error /usr/bin/systemctl is-active oes-dashboard.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
aggregator.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
collector.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
repaggregator.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
repcollector.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
gateway.service
exit_on_error /usr/bin/systemctl is-active oes-cis-
configuration.service
```

Changes do not take effect until you take the resource offline, and bring it online again.

3 Verify the CIS services are successfully upgraded by using the following command:

```
cishealth
```

When the status displays “Healthy”, then the CIS server is successfully upgraded.

4 Restart the agent services.

```
systemctl restart oes-core-agent.service oes-dashboard-agent.service
oes-cis-agent.service oes-cis-recall-agent.service oes-cis-
scanner.service
```

```
systemctl status oes-core-agent.service oes-dashboard-agent.service
oes-cis-agent.service oes-cis-recall-agent.service oes-cis-
scanner.service
```

6.2.4 Upgrading Data Scale Server from OES 24.3 to OES 24.4 or OES 25.1

Prerequisite:

After upgrading to OES 24.4 or OES 25.1, ensure to check the `gatewayforscale` (8346) and `dataatscale` (8347) port on the configured server, and if the port number is missing in the firewall, add it.

Procedure:

1. Restart the services.

   If both `gatewayforscale` and `dataatscale` services are available in the same server then you must start the `gatewayforscale` service first followed by `dataatscale` service.

   ```
   systemctl status oes-cis-gatewayforscale.service
   ```

   ```
   systemctl status oes-cis-dataatscale.service
   ```

2. Verify the status of the service.

   ```
   systemctl restart oes-cis-gatewayforscale.service
   ```

   ```
   systemctl restart oes-cis-dataatscale.service
   ```

7 Management Tools for CIS

This section provides an overview of the management tools for Cloud Integrated Storage (CIS) in Open Enterprise Server (OES).

- Section 7.1, “Managing CIS,” on page 53

7.1 Managing CIS

Cloud Integrated Storage (CIS) management console allows you to move the NSS data to cloud storage. It also allows you to define policies for data migration and view statistic information on migration, files migrated and recalled.

IMPORTANT: The CIS management login page (https://<*OES server IP address or the host name*>:8344) works only if CIS is configured.

Prerequisites

Before you start using the CIS management console, ensure that the following prerequisites are met:

- Supported web browsers:
  - Mozilla Firefox
  - Google Chrome
  - Microsoft Edge
  - Apple Safari
- Ensure that a cloud account is created and you have details of the access key and secret key.
- If you use cloud account with SSL support and create certificate signed by different CA (other than eDirectory CA), copy the CA bundle (.pem format) in `/etc/opt/novell/cis/certs/rootCAs` and add the CA bundle file name in `CLOUD_CA_BUNDLE_NAME` in the `/etc/opt/novell/cis/config` file.

  For example:

  ```
  CLOUD_CA_BUNDLE_NAME="Cloud1-CA.pem"
  ```

  NOTE: If you have multiple cloud accounts with SSL support, concatenate CAs (.pem format) of the cloud accounts and add the concatenated CA bundle name in `CLOUD_CA_BUNDLE_NAME` in the `/etc/opt/novell/cis/config` file.

  After configuring the `/etc/opt/novell/cis/config` file, ensure to restart the data service using the following command:

  ```
  systemctl restart oes-cis-data.service
  ```

  In data scale scenario, repeat the same steps on all the servers where data service is running. The `config` file path in data scale is `/etc/opt/novell/cis-scale`.

After configuring the `/etc/opt/novell/cis-scale/config` file, ensure to restart the data scale service using the following command:

```
systemctl restart oes-cis-dataatscale.service
```

NOTE: This prerequisite is not applicable in AWS S3, as secure communication is taken care without the `CLOUD_CA_BUNDLE_NAME` parameter.

- Ensure that all the CIS services and its infrastructure services are up and running.
- Verify whether the CIS agents are up and running. The CIS agents includes the following:

  ```
  oes-core-agent.service
  ```

  ```
  oes-dashboard-agent.service
  ```

  ```
  oes-cis-agent.service
  ```

  ```
  oes-cis-recall-agent.service
  ```

  ```
  oes-cis-scanner.service
  ```

  For example,

  ```
  blr7-user1:/lib/modules/4.4.21-69-default/kernel # systemctl status
  oes-cis-agent.service
  oes-cis-agent.service - CIS agent for OES
     Loaded: loaded (/usr/lib/systemd/system/oes-cis-agent.service;
  enabled; vendor preset: disabled)
    Active: active (running) since Wed 2017-06-14 19:01:09 IST; 1 day 23h
  ago
   Main PID: 17177 (cisagents)
      Tasks: 107 (limit: 512)
     CGroup: /system.slice/oes-cis-agent.service
             └─17177 /opt/novell/cis/bin/cisagents

  Jun 16 10:53:43 blr7-user1 cisagents[17177]: Entry name = /media/nss/
  TEST1/DESKTOP.AFP/ICON/736F646D5458455
  Jun 16 10:53:43 blr7-user1 cisagents[17177]: Entry name = /media/nss/
  TEST1/DESKTOP.AFP/ICON/736F646D666C726
  Jun 16 10:53:43 blr7-user1 cisagents[17177]: Entry name = /media/nss/
  TEST1/~DFSINFO.8-P
  Jun 16 11:07:26 blr7-user1 cisagents[17177]: 2017/06/16 11:07:26 Number
  of Components: 3
  Jun 16 11:07:26 blr7-user1 cisagents[17177]: Entry name = /media/nss/
  TEST1/BB/krb5.conf
  Jun 16 11:07:26 blr7-user1 cisagents[17177]: Entry name = /media/nss/
  TEST1/DESKTOP.AFP/ICON/736F646D414E494
  Jun 16 11:07:26 blr7-user1 cisagents[17177]: Entry name = /media/nss/
  TEST1/DESKTOP.AFP/ICON/736F646D4C50504
  Jun 16 11:07:26 blr7-user1 cisagents[17177]: Entry name = /media/nss/
  TEST1/DESKTOP.AFP/ICON/736F646D5458455
  Jun 16 11:07:26 blr7-user1 cisagents[17177]: Entry name = /media/nss/
  TEST1/DESKTOP.AFP/ICON/736F646D666C726
  Jun 16 11:07:26 blr7-user1 cisagents[17177]: Entry name = /media/nss/
  TEST1/~DFSINFO.8-P
  ```

  Similarly, verify the status of other two CIS agents.

  If CIS agents are not running, restart all 3 agents by entering the following command:

```
systemctl start oes-cis-agent.service
systemctl start oes-cis-recall-agent.service
systemctl start oes-cis-scanner.service
```

- Enable the `ListXattrNWMetadata` option on the NSS filesystem to display the trustees for a file or directory when performing scan or migration.For more information on enabling the option, see ListXattrNWmetadata Option in the Storage Services File System (NSS) Administration Guide for Linux.

Data Migration Using CIS Management Console

1. Configure the cloud account. For more information, see Section 7.1.3, “Accounts,” on page 56.
2. Create a policy. For more information, see Section 7.1.4, “Policies,” on page 57.
3. Configure the tier. For more information, see Section 7.1.5, “Tiers,” on page 59.
4. View the status of data migration. For more information, see Section 7.1.6, “Dashboard,” on page 64.

7.1.1 Insights

The CIS welcome page provides the network level view of total number of volumes available on the OES servers that is configured with CIS, total number of files available, and total space used by those files. Based on the access time or modification time, the **Data Summary** section displays the percentage of hot and cold data available on all the volumes and lets you do the following:

- View the percentage of hot and cold data (based on access time or modification time) by moving the data slider.
- Set the age of the hot and cold data (based on access time and modification time) by moving the time slider.

Click to view the updated scan details of all the CIS agents. You can use this page to discover the top five volumes that contain more cold data, the top five users with more cold data, and the top five file types available as part of that cold data. Overall, this page provides the user with the insights of data available in their organization and use this information to create policies.

Click any volume in **Top Cold Volumes** or the HOT/COLD chart to view the volume specific summary. Click on volumes count at the top to go to volume summary information page.

7.1.2 OES Health

Provides a rich dashboard to monitor the health of all the servers (and its services) that are child nodes installed below the CIS context in the same eDirectory tree.

On visiting this tab, this server contacts all the servers to provide a real-time health status. The **Scan triggered at** option displays the time all the servers were contacted to collect the data.

On clicking the server on right-side a list of services with their health are displayed on the left-side. The health indicators are:

- **Good:** Displays all the services are in good health.

- **Partially Unhealthy:** One or more service has a minor problem while the rest all services are in good health. You should refer to the service log for more information.
- **Bad:** One or more service has a critical problem. You should refer to the service log for more information.
- **No Connection:** Unable to contact the server for its status.

7.1.3 Accounts

Configure and manage the cloud account to which you are planning to migrate the data.

- "Configuring Cloud Account" on page 56
- "Managing Cloud Accounts" on page 57

Configuring Cloud Account

Click the **Accounts** tab, the **Cloud Accounts** page is displayed.

1 Click + to configure the cloud account.

2 Specify the following:

2a **Account Name:** Specify the name of the cloud account.

2b **Account Type:** Select one of the following:

- AWS S3
- S3 Compatible

  Endpoint: Specify the URL of the cloud server. This parameter is displayed only if you select Account Type as S3 Compatible.
- Azure

  Storage Account Name: Specify the account name of the Azure cloud account. This parameter is displayed only if you select the Account Type as Azure.

  NOTE: CIS supports Azure Blob storage service and Azure account types with the Access key authentication method.

- Google Cloud Storage

  Upload Service Account File: This parameter is displayed only if you select the Account Type as Google Cloud Storage.

2c **Region:** Select the region name where the cloud server is available.

2d **Access Key:** Specify the access key of the cloud account.

2e **Secret Key:** Specify the secret key of the cloud account.

3 Click **SAVE**.

Managing Cloud Accounts

Click the **Accounts** tab to view all the configured cloud accounts.

- To modify the cloud account information:
  1. Click on the cloud account you want to modify.
  2. Click **UPDATE**.
- To delete the cloud account:
  1. Click on the cloud account you want to delete.

     NOTE: You cannot delete the account on which the data migration is already performed.
  2. Click **OK**.

7.1.4 Policies

The data is migrated using the policies that are created based on the last accessed time, modified time, file type, file size, and so on.

- "Creating a Policy" on page 57
- "Managing Policies" on page 59

Creating a Policy

Click the **Policies** tab, the **Policies** page is displayed.

1 Click to create a policy.

2 Specify the name and description for the policy.

3 Select the required rule.

Sample use cases:

- **Use Case 1:** To migrate data that is not accessed for more than 120 days.

Rules	Value	Unit	Operation
Files not accessed since	120	days	End

OR

Rules	Value	Unit	Operation
Files not accessed since	4	months	End

- **Use Case 2:** To migrate data that is not modified for the last two years.

Rules	Value	Unit	Operation
Files not modified since	2	years	End

- **Use Case 3:** To migrate all the files with `.doc` and `.pdf` extension.

Rules	Value	Operation
File name matches	*.doc,*.pdf	End

- **Use Case 4:** Consider you have six files with names data, user1_data, 2017_data, 16-may_data, may-17_data, and data32. To migrate files with file names containing a matching string.

Rules	Value	Operation
File name matches	*data*	End

After running this policy, all the six files are successfully migrated.

- **Use Case 5:** To migrate all the files that are less than 1 MB in size.

Rules	Value	Unit	Operation
File size is less than	1	MB	End

- **Use Case 6:** To migrate all the files and folders that are available in a specific file path.

Rules	Value	Operation
File path contains	/data1/secret	End

- **Use Case 7:** To migrate or recall all the files and folders starting from the given directory path.

Rules	Value	Operation
Directory path is equal to	/data2/secret	End

The entire volume will be examined if any other rules are added along with the **Or** operation.

NOTE: Ensure that the path provided is from the root of the volume.

4 (Optional) Create multiple rules for the same policy using the following:

- **And:** Performs **And** operation between the selected and next rule.
- **Or:** Performs **Or** operation between the selected and next rule.

- **New group:** Adds a new group and use **And** or **Or** option between these two groups. You can create any number of groups and add multiple rules for the same group.
- **Delete:** Deletes the selected rule.
- **End:** Deletes all the rules that follows the selected rule.

For example, to migrate all the data except PDF files larger than 10 MB and less than 6 months old:

Rule	Value	Unit	Operation
File not accessed since	6	months	And
File size is less than	10	MB	And
File name does not match	*.pdf	-	And

5 Click **SAVE**.

Managing Policies

Click the **Policies** tab to view all the policies.

- To modify the policy:
  1. Click policy name or on the policy you want to modify.
  2. Click **UPDATE**.
- To delete the policy:
  1. Click on the policy you want to delete.

     NOTE: You cannot delete the policy that you have used to migrate data.
  2. Click **OK**.

7.1.5 Tiers

It includes:

- "Tiers" on page 59
- "Migrate from DST" on page 62

Tiers

By configuring the cloud tier, you are associating the primary storage (data on OES server) and cloud storage to perform the data migration. Using tier configuration, you can run the policy at a scheduled time.

- "Configuring Cloud Tiers" on page 60
- "Managing Cloud Tiers" on page 60

Configuring Cloud Tiers

Click the **Tiers** tab, then click **Tiers**.

1 Click + to configure the tier.

2 Specify the following:

2a **Server:** Select the OES server. This lists the OES servers that are configured with CIS server where agent is running and also includes the cluster resources.

2b **Volume:** Select a volume.

2c **Endpoint:** Select the required cloud account name.

2d **Bucket Name:** Specify the bucket name used to store the migrated data for account. You can access your AWS and S3 cloud account to find the bucket name.

2e **Container Name:** Specify the container name used to store the migrated data for Azure cloud account. You can access your Azure cloud account to find the container name.

2f **Region:** Select the region where the specified bucket name is available.

2g **Encryption:** Configure the encryption settings to enable this parameter. If enabled, encrypts the migrated data in the cloud storage.

For more information on encryption settings, see "Encryption" on page 68.

2h **Policy:** Select the required policy to be applied.

2i **Schedule:** Select the schedule type based on how frequently the policy should be run for the tier. It includes the following: Daily, Weekly, Monthly, Once, and None.

As a best practice, you can limit the duration of run to four hours everyday or run during the weekend to minimize the load on the OES servers. It is recommended that you do not migrate the data when users are accessing the data.

To limit the duration of the schedule run, select **Time duration for the schedule run** option and specify the time duration.

3 Click **SAVE**.

NOTE: The secondary volume or CBV (Cloud Backed Volume) is automatically created after the tier configuration.

Managing Cloud Tiers

Click the **Tiers** tab to view all the cloud tiers. Before to estimate the total migrate or recall data before the actual run.

- If the schedule type is **None**, click ▶ to start the data migration.
- To stop the data migration, click the rotating icon ⟳.

  The next time, you start the data migration process for the same tier, the remaining data is migrated to the cloud storage.
- To rerun the policy for the tier, click ⟳.
- To view statistics for the tier:

  1. Click 📈.

Displays information of the migrated files from the previous job run (each time the schedule starts at a specified time, a new job run is created). The statistic information includes:

- **Status:** Provides the status of data migration.
- **Start Time:** Provides the data migration start time.
- **End Time:** Provides the data migration completion time.
- **Files Migrated:** The total number of files migrated.
- **Data Size:** Lists the overall size of the data migrated for each volume.

For more information on detailed reports, see "Dashboard" on page 64.

2. If no files are migrated, click **Last Run** to view the statistic information for the previous job run.

- To modify the tier:

1. Click on the tier you want to modify.
2. Select the policy type for tier run. It includes:
   - **Migration Policy:** Migrates the data (that satisfies the policy selected) to the cloud.
   - **Recall Policy:** Recalls the data (that satisfies the policy selected) from the cloud.
   - **Free Space Calculation:** Calculates (dry run) the amount of data that will be migrated to the cloud. Before performing the migration, ensure that enough space is available on the cloud.
   - **Recall Space Estimation:** Calculates (dry run) the amount of data that will be recalled from the cloud to your Primary volume. Before performing the recall, ensure that enough space is available on your Primary volume.
3. Click **UPDATE**.

- To delete the tier:

1. Click on the tier you want to delete.

   If data migration is not performed on this tier, click **OK** to delete.

   If data migration is performed on this tier, select the desired action.
   - **Recall files and delete:** This recalls all files (migrated as part of this tier) from the cloud and automatically deletes the tier.
   - **Force delete:** This deletes the tier and CBV volume associated with this tier without recalling files. The data (migrated as part of this tier) is lost and cannot be recovered.
2. If you select the **Recall files and delete** action, choose the schedule to recall files and then click **Recall**.

   OR

   If you select the **Force delete** action, click **Delete**.

Migrate from DST

Based on the DST migrate tier details, the data is migrated from the DST shadow volume to the cloud storage. By default, an internal policy is applied to migrate all files in the DST shadow volume.

- "Prerequisites" on page 62
- "Configuring DST Migrate Tier" on page 62
- "Managing DST Migrate Tiers" on page 63

Prerequisites

Create a policy to perform switch operation for moving the DST tier to cloud tier. For more information, see Section 7.1.4, "Policies," on page 57.

Configuring DST Migrate Tier

Click the **Tiers** tab, then click **Migrate from DST**.

NOTE: Before configuring the DST tier, ensure to disable the DST policies. For more information, see Chapter 9, "Migrating DST Volumes to Cloud," on page 73.

---

1 Click + to configure the tier.

2 Specify the following:

2a **Server:** Select the OES server. This lists the OES servers that are configured with CIS server where agent is running and also includes the cluster resources.

2b **Volume:** Select a volume.

2c **Endpoint:** Select the required cloud account name.

2d **Bucket Name:** Specify the bucket name used to store the migrated data. The bucket name can be obtained from your cloud account.

2e **Region:** Select the region where the specified bucket name is available.

2f **Encryption:** To enable this parameter, configure the encryption settings. If enabled, encrypts the migrated data in the cloud storage.

For more information on encryption settings, see "Encryption" on page 68.

2g **Schedule:** Select the schedule type based on how frequently the policy should be run for the tier. It includes the following: Daily, Weekly, Monthly, Once, and None.

As a best practice, you can limit the duration of run to four hours everyday or run during the weekend to minimize the load on the OES servers. It is recommended that you do not migrate the data when users are accessing the data.

To limit the duration of the schedule run, select **Time duration for the schedule run** option and specify the time duration.

3 Click **SAVE**.

NOTE: ◆The secondary volume or CBV (Cloud Backed Volume) is automatically created after the tier configuration.

- If the primary volume is AD enabled, ensure that the CBV created for the corresponding primary volume is also AD enabled using NSS tools or utilities.

Managing DST Migrate Tiers

Click the **Tiers** tab to view all the DST migrate tiers.

- If the schedule type is **None**, click to start the DST migration.
- To stop the DST migration, click the rotating icon.

  The next time, you start the DST migration process for the same tier, the remaining data is migrated to the cloud storage.
- To rerun the policy for the DST tier, click.
- To view statistics for the DST tier:
  1. Click.

     Displays information of the migrated files from the previous job run (each time the schedule starts at a specified time, a new job run is created). The statistic information includes:

     - **Status:** Provides the status of data migration.
     - **Start Time:** Provides the data migration start time.
     - **End Time:** Provides the data migration completion time.
     - **Files Migrated:** The total number of files migrated.
     - **Data Size:** Lists the overall size of the data migrated for each volume.

     For more information on detailed reports, see "Dashboard" on page 64.
  2. If no files are migrated, click **Latest Migration** to view the statistic information for the previous job run.
- To modify the DST tier:
  1. Click on the DST tier you want to modify.
  2. Click **UPDATE**.
- To move the DST tier to cloud tier, perform the following:
  1. After migrating all the files to cloud, remove the DST pair. For more information, see Chapter 9, "Migrating DST Volumes to Cloud," on page 73.
  2. Click on the DST tier.
  3. Select the required policy and click **MIGRATE**.

     The DST tier is no longer listed in **Migrate from DST**. Instead, it is listed in **Tiers**.
- To delete the DST tier:
  1. Click on the DST tier you want to delete.
  2. Click **OK**.

7.1.6 Dashboard

The **Dashboard** page displays the following:

- **File Size:** Total size of files migrated and recalled.
- **File Count:** Total number of files migrated and recalled.
- **Graphical Representation of Files Migrated and Recalled:** Displays a line graph for both files migrated and recalled. The horizontal axis (x-axis) represents the migrated or recalled time, whereas the vertical axis (y-axis) represents the data size. Click on the files migrated or recalled value and zoom in to view the exact time the individual files are moved.
- **Select Date:** Click on date icon at the top right corner to select a date and to view the information of files migrated and recalled on the selected dates. The date selection option is available on **Dashboard** and **Statistics** page.

Click the file size or file count to go to **Volumes** page. The **Volumes** page displays the total size of files migrated, recalled, and a graphical representation of the same in the form of pie graph for each volume.

Click on a volume or pie graph to go to **Statistics** page. The **Statistics** page displays the file size, file count, and a graphical representation of files migrated and recalled for a specific volume. Click **More Details** to view the detailed information of files migrated and recalled. The migrated files are displayed based on the run ID (ID generated for every policy/job run on each tier). Select the run ID to view the information of migrated files for a specific job (policy run for a specific volume).

7.1.7 Roles

Configure roles for the user or group objects that belongs to eDirectory to manage CIS.

NOTE: Active Directory user or group objects are not supported.

- "Configuring Roles" on page 64
- "Managing Roles" on page 65

Configuring Roles

NOTE: Before configuring the Roles, create a proxy user using iManager and specify that user in **Proxy User Name** under the **Settings** > **Proxy User and Context** tab. For more information, see "Proxy User and Context" on page 67.

Click the **Roles** tab, the **Roles** page is displayed.

1. Click + to configure the role.
2. Specify the following:
   - 2a **Name:** Specify the eDirectory object name.
   - 2b **Type:** Select either User or Group.

2c **Role:** Select the required access:

- **Read Admin:** The user or group objects can only view the cloud account, policy and tier information.
- **Execute Admin:** The user or group objects can configure cloud account, create policy, and configure cloud tier.
- **Root Admin:** The user or group objects can configure cloud account, create policy, configure cloud tier, configure roles and modify the CIS server and agent settings.

3 Click **SAVE**.

Managing Roles

Click the **Roles** tab to view all the roles configured.

- To modify the role:
  1. Click on the role you want to modify.
  2. Click **UPDATE**.
- To delete the role:
  1. Click on the role you want to delete.
  2. Click **OK**.

7.1.8 Agents

This page allows you to set the configuration for OES server agents and scanners. Click the **Agents** tab, the **Agent Settings** page is displayed. It includes:

- "Global Configuration for All Agents" on page 65
- "Configuration for Each Agent" on page 66
- "Global Configuration for All Scanners" on page 67
- "Configuration for Each Scanner" on page 67

Global Configuration for All Agents

This section lists the common configuration for all the CIS agents on OES servers that is connected to CIS server. It includes the following:

- **Port:** Specify the port through which all the CIS agents on OES servers communicate to CIS server. The default value is 8000.

  NOTE: If you are modifying the port, ensure to close the existing port.

- **Log Level:** Select the log level for all the CIS agents. The options are: Panic, Fatal, Error, Warn, Info, and Debug. The default log level is Info.

- **Throttling:** Click toggle button (On) to regulate the data transfer rate of the recalled files. By default, it is Off. It includes:
  - **Duration:** Specify the time interval in seconds within which the specified number of files in **File Limit** should be recalled. The default value is 60 seconds.
  - **File Limit:** Specify the total number of files to be recalled within the specified **Duration**. The default value is 100.

  For example, consider a scenario where the **Duration** as 30 seconds and **File Limit** as 60, which indicates maximum 60 files can be recalled at any given point in time depending on the file size and network bandwidth. Assuming that if 60 files are recalled in first 10 seconds, then the time taken to recall the remaining files is based on the following rule:

  Recall rate per file = Duration/File Limit = "n" seconds, which means 30/60 = 0.5 seconds.

  NOTE: Ensure to restart the recall agent for throttling changes to take effect.

- **Online/Offline:** Enables or disables the data recall on all the CIS agents. By default, it is set to **Online**.
- **Enabled/Disabled:** Enables or disables the data migration and recall on all the CIS agents on OES server that is connected to CIS. By default, it is **Enabled**.

  If disabled, it brings down all the CIS agents. To enable the CIS agents again, set toggle button to **Enabled**, click **SAVE** and then manually login to the OES servers and restart the CIS agent service

After setting the global configuration, click **SAVE**.

Configuration for Each Agent

This section lists all the CIS agents on OES server that is connected to the CIS server. It provides the setting parameters for individual CIS agent.

NOTE: The agents in the highlighted rows will be configured with the global agent configuration.

- **Agent Name:** Displays the CIS agent name on OES server that is connected to CIS.
- **Data Server:** Select the required CIS data server URI through which the CIS agent should communicate to. By default, the CIS server URI is displayed
- **Port:** Specify the port through which the CIS agent on OES server should communicate to CIS data server. The default value is 8000.

  NOTE: If you are modifying the port, ensure to close the existing port.

- **Log Level:** Select the log level for the CIS agent. The options are: Panic, Fatal, Error, Warn, Info, and Debug. The default log level is Info.
- **Agent State:** This includes the following:
  - **Online/Offline:** Enables or disables the data recall on that CIS agent. By default, it is set to **Online**.

- **Enabled/Disabled:** Enables or disables the data migration and recall on that CIS agent. By default, it is **Enabled**.

  If disabled, it brings down the CIS agent. To enable the CIS agent again, set toggle button to **Enabled**, click **SAVE** and then manually login to the OES server and restart the CIS agent service.

After setting the agent configuration, click **SAVE**.

Global Configuration for All Scanners

This section lists the common configuration for all the CIS scanners on OES servers that is connected to CIS server. It includes the following:

- **Schedule:** Select the schedule type based on how frequently the scanner should run on OES servers. It includes the following: Daily, Weekly, Monthly, Once, and None.

  To limit the duration of the schedule run, select **Time duration for the schedule run** option and specify the time duration.
- **Incremental Scanning:** Allows you to perform a full scan or a incremental scan on the OES volumes. By default, it is **Disabled**. If enabled, performs the differential scan from the previous full scan on the OES volumes.

After setting the global configuration, click **SAVE**.

Configuration for Each Scanner

This section lists all the CIS scanners on the OES servers that is connected to the CIS server. It provides the setting parameters for individual CIS scanner.

- To immediately trigger a file scan, go to specific OES server and click .
- To modify the scheduled scan:
  1. Click on the OES server you want to modify.
  2. Select the schedule type.
  3. Click **UPDATE**.

After setting the agent configuration, click **SAVE**.

7.1.9 Settings

This page allows you to set the configuration for CIS server. Click the **Settings** tab, the **CIS settings** page is displayed. It includes:

- "Proxy User and Context" on page 67
- "General" on page 68
- "Encryption" on page 68

Proxy User and Context

Includes the following:

IMPORTANT: The root admin must have the following rights:

- Rights to modify the `cishost-info` attribute on the server context.
- Supervisory rights on the proxy user of eDirectory object, if root admin needs to update the proxy DN.

- **CIS Server Context:** By default, it is obtained from the CIS configuration. Displays the fully distinguished name of the context under which the OES server objects that can connect to the CIS server reside. For example, ou=wdc,o=acme is set as context indicates that any server within this context can connect to CIS.
- **Administrator Search Context:** Specify the context of the administrator user or group object where you can configure roles for a specific user or group. For example, if o=acme is set as search context, the authentication object is searched only within this context.
- **Proxy User Name:** Specify the proxy user used by the CIS server for users or groups lookup. The proxy user should have read and compare permissions for CN attribute on the **Administrator Search Context** configured. The proxy user password is reset and maintained by the CIS server. This proxy user should be used to manage only CIS.

After configuring the context settings, click **SAVE**.

General

Includes the following:

- **Secondary Volume Suffix Pattern:** Specify the name that needs to be suffixed with the secondary volume name. The default value is _CBV. For example, if the primary volume name is VOL1, the secondary volume name is VOL1_CBV.
- **Log Level:** Select the log level for CIS services. The options are: Panic, Fatal, Error, Warn, Info, and Debug. The default log level is Info.

After configuring the general settings, click **SAVE**.

Encryption

CIS supports pool-based encryption and generates a pool of keys for data encryption. It includes the following:

- **Key Size:** Select the AES encryption key size based on your requirement.
- **Pool Size:** Specify a valid integer. Based on the specified value, the corresponding pool of keys are generated and used for data encryption. The minimum pool size value is 127.

After configuring the encryption settings, click **SAVE** to generate the pool of keys. To again generate a new pool of keys for a different **Pool Size** values, click **REGENERATE**.

7.1.10 Data Servers

The data servers page displays the following:

- Lists all the gateway servers and the data servers that are connected to the individual gateway server. It also displays the corresponding CIS agents configured for all the gateway servers.
- Lists all the standalone data servers and corresponding CIS agents configured to a standalone data server.

7.1.11 Health Indicator

The CIS health indicator shows the current server health status as healthy, partially healthy, or not healthy. Click the server health icon at the top right corner to display the **CIS Health Status** window.

The CIS health status displays the status of the following:

- **Summary:** Displays the overall status of the CIS server.
- **Services:** Displays the status of all the CIS services.
- **Gateway:** Displays the connection status between the CIS gateway and CIS services.
- **Infrastructure:** Displays the status of ZooKeeper, OpenSearch, Kafka, and Database.
- **Configuration:** Displays the status of docker daemon, docker network for CIS, CIS network in iptables - Firewall, network masquerading for CIS, CIS ports, and logging service.

If the server health status is not good, click **FIX** to fix the issues. Similarly, to get the updated health status of CIS server, click **REFRESH**.

8 Command Line Tools for CIS

This section provides an overview of the command line tools for Cloud Integrated Storage (CIS) in Open Enterprise Server (OES).

CIS Integrity `(cisintegrity)` is a command line utility that offers a variety of validation options to verify the integrity of migrated objects in the cloud storage and database. This utility identifies the orphan objects and deletes them from cloud storage. As a result, unused space is reclaimed from orphaned objects.

Syntax

`cisintegrity <CISOPTION> [OPTION]`

You can execute `cisintegrity` command on the following servers:

- Standalone Server: `"configType":"standalone"`
- CIS Core Server: `"configType":"core"`

For a list of available options, see the `cisintegrity` man page.

9 Migrating DST Volumes to Cloud

This section describes how to migrate DST local and cluster volumes to cloud storage.

The following video demonstrates how to migrate DST cluster volumes to the cloud using CIS:

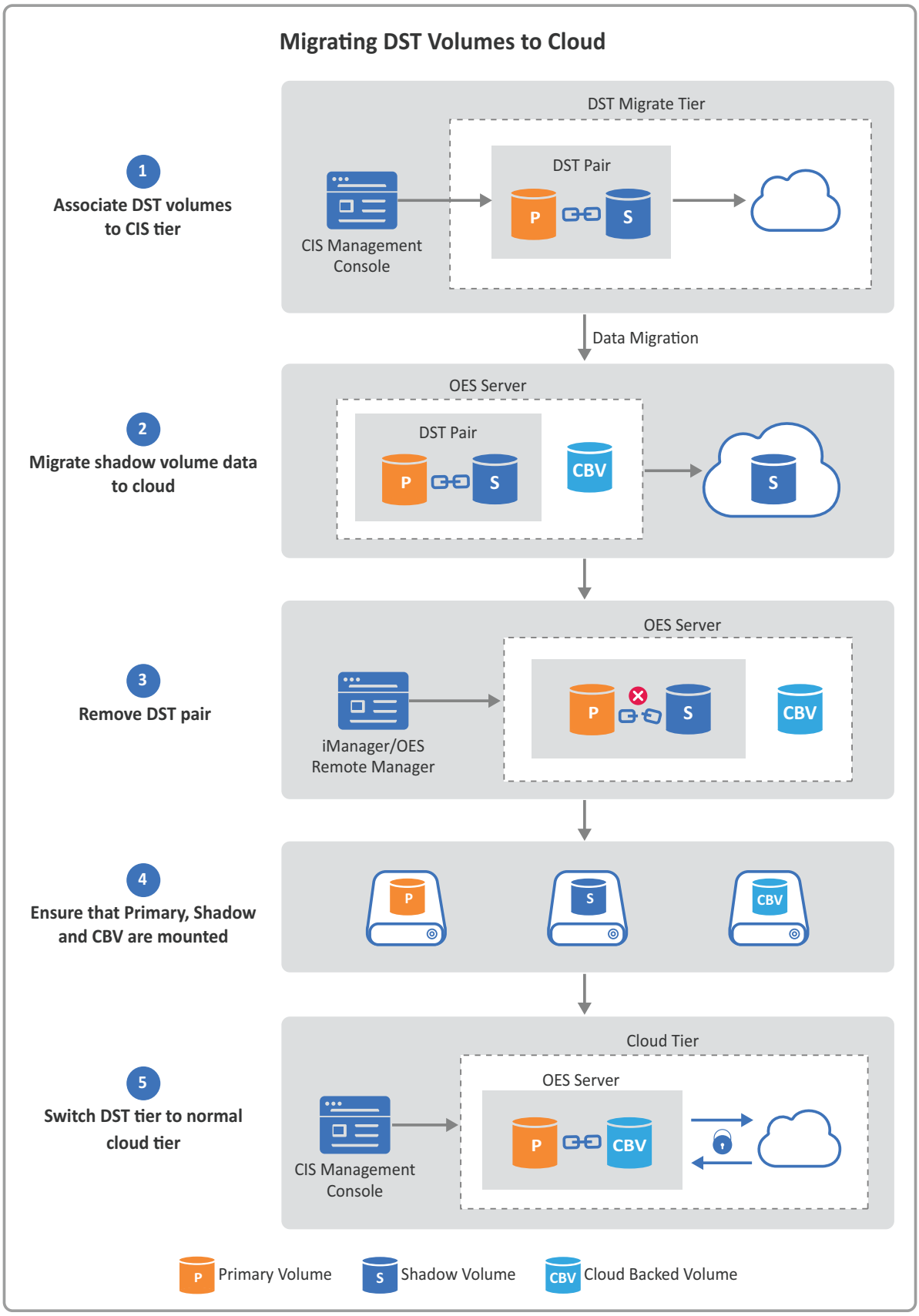
http://www.youtube.com/watch?v=3-A9wYtUQt8

Prerequisites

- Salvage the required files available in the DST shadow volume. Otherwise, the salvageable files are not migrated to cloud during the tier run.
- It is recommended to take a backup of the DST shadow volume before performing the DST migration.
- Ensure that all the active and running DST policies are completed or stopped.
- In OES Remote Manager, under **Manage NCP Services > Manage Server**, set the DST parameter information as follows:

```
REPLICATE_PRIMARY_TREE_TO_SHADOW: 1
SHIFT_ACCESSED_SHADOW_FILES: 0
SHIFT_DAYS_SINCE_LAST_ACCESS: 0
SHIFT_MODIFIED_SHADOW_FILES: 1
DUPLICATE_SHADOW_FILE_ACTION: 0
DUPLICATE_SHADOW_FILE_BROADCAST: 0
```

Figure 9-1 *Migrating DST Volumes to Cloud*



Procedure

1. Using CIS management console, associate the DST volumes to CIS tier. For more information, see “Migrate from DST” on page 62.
2. Migrate the DST shadow volume data to cloud.
3. Remove the DST pair.
   - **3a** To remove the shadow relationship for local DST volume pair, see Removing the Shadow Relationship for a Non-Clustered DST Shadow Volume in the Dynamic Storage Technology Administration Guide.
   - **3b** To remove the shadow relationship for clustered DST volume pair, perform the following:
     - **3b1** Remove the shadow definition for the DST shadow volume pair and NCP bindings exclusion for the secondary volume on each node. For more information, see Removing the Shadow Definition and NCP/NSS Bindings Exclusion on All Nodes in the Dynamic Storage Technology Administration Guide.
     - **3b2** In the primary pool cluster resource scripts, remove (or comment out) the lines for the management of the secondary pool and secondary volume. For more information, see Preparing the Primary Pool Cluster Resource for Independent Use in the Dynamic Storage Technology Administration Guide.
     - **3b3** Online the pool with shadow volume. For more information, see Modifying the Secondary Pool Cluster Resource in the Dynamic Storage Technology Administration Guide.
4. Ensure that the primary volume, shadow volume, and CBV are mounted.
5. Using CIS management console, perform switch operation to move the DST tier to cloud tier. For more information, see “Managing DST Migrate Tiers” on page 63.

10 Working with CIS Clients

Users can seamlessly access their files (on-premise or cloud) through the file explorer (Windows) or the Finder (Mac). In the background, the CIS client integrates with the explorer/finder to provide this functionality through the CIFS protocol. The benefits are:

- Access to the files uploaded to the cloud (Windows and Mac workstations).
- Displays the cloud overlay icon on the files uploaded to the cloud (Windows workstation).

To enjoy the above benefits,

- Users need to install the CIS client on their workstation. If the client is not installed, then you will not be able to access the files uploaded to the cloud.
- An administrator needs to enable the `--block-unmanaged-cis-reads` option on the OES server by using the `novcifs` utility.

CIS Client Support Matrix

The following are the requirements for installing and running the CIS client on Windows and Mac workstations:

- **Windows:** Windows 11 and Windows 10
- **Mac:** macOS 14 (Sonoma) and macOS 15 (Sequoia)

Accessing and Installing CIS Client

On the OES Welcome page (http://*<OES server IP Address or the host name>*/welcome/client-software.html) download the CIS client based on your operating system. It includes:

- Section 10.1, “CIS Client for Windows,” on page 77
- Section 10.2, “CIS Client for Mac,” on page 79

10.1 CIS Client for Windows

The CIS client on Windows allows users to access the files uploaded to the cloud. This client also provides an enhancement to the overlay icon on the files uploaded to the cloud. This overlay icon helps to differentiate the local files from the files uploaded to the cloud.

- Section 10.1.1, “Prerequisites,” on page 78
- Section 10.1.2, “Installing CIS Client,” on page 78
- Section 10.1.3, “Reinstalling or Uninstalling CIS Client,” on page 78
- Section 10.1.4, “Log Details,” on page 79

10.1.1 Prerequisites

- The CIS client is built on the Microsoft .NET Framework 4.5, so make sure to update your Windows version with the latest patches.
- Use the `novcifs` command line utility to set `--block-unmanaged-cis-reads` option to "`yes`".

NOTE: Only administrators can modify this option on the OES server.

10.1.2 Installing CIS Client

The steps to install the CIS client on a Windows workstation are as follows:

1. Run the `CISClient.msi` installer to launch the setup.
2. Read the introduction, then click **Next**.
3. Read and accept the end-user license agreement, then click **Next**.
4. On the Features window page, click **Next**.

   The following features will be installed:

   - Use the Overlay Icon

     Displays the overlay icon on the files that are uploaded to the cloud. The overlay icon helps to differentiate the local files from the files uploaded to the cloud.

   - Access Files Uploaded to the Cloud

     Allows the user to access the files uploaded to the cloud.
5. Click **Install** to begin the installation.

   In a few seconds, the client is successfully installed.
6. Click **Finish** to exit the installer.

   A pop-up message is displayed to restart the workstation for the configuration changes made to the CIS client to take effect.

10.1.3 Reinstalling or Uninstalling CIS Client

To reinstall or uninstall the CIS client on a Windows workstation, follow these steps:

1. Run the `CISClient.msi` installer to launch the setup.
2. Read the introduction, then click **Next**.
3. Select the required action to perform:

   - **Repair**

     To install any missing components, the installation program detects the previously installed components and reinstalls them.

   - **Remove**

     To uninstall the CIS client.

IMPORTANT: After uninstalling the CIS client, ensure to restart the Windows workstation. Otherwise, the workstation would still behave as a managed CIS client (accessing the files uploaded to the cloud).

4 Follow the installation wizard to complete the setup.

10.1.4 Log Details

The CIS client log information is available at `C:\Users\<username>\AppData\Local\OES\CISClient\logs\cisclient.log`. To configure the log level, do the following:

1 In the Start menu, in the Run box or the Search box, type `regedit`, and press Enter.

2 Select **HKEY_CURRENT_USER > Software > OES > CISClient > LogLevel**.

3 Right-click and select **Modify**. Specify the required value under 'Value data' and click **OK**.

Example:

Value data = 0 (displays all logs)

4 After setting the log level, restart the Windows workstation to view the log information.

10.2 CIS Client for Mac

The CIS client on Mac allows users to preview the files uploaded to the cloud instead of the earlier issue of downloading them to the local storage.

- Section 10.2.1, “Prerequisite,” on page 79
- Section 10.2.2, “Installing CIS Client,” on page 79
- Section 10.2.3, “Uninstalling CIS Client,” on page 81
- Section 10.2.4, “Log Details,” on page 81

10.2.1 Prerequisite

- Use the `novcifs` command line utility to set `--block-unmanaged-cis-reads` option to “`yes`”.
- To install the latest version of CIS Client for Mac 1.1.8, you must uninstall the earlier version of CIS Client for Mac. Section 10.2.3, “Uninstalling CIS Client,” on page 81.

10.2.2 Installing CIS Client

- “macOS Sonoma” on page 80
- “macOS Sequoia” on page 80

macOS Sonoma

To install the CIS client on a macOS Sonoma workstation:

1. Open the `CISClient.pkg` installer to launch the package.
2. Follow the prompt, read the agreement and click **Agree** to accept the end-user license agreement.
3. Click **Install**. The system prompts for administrator credentials; enter the password and click **Install Software** > **OK** to begin the installation.

   The CIS client successfully installs within a few seconds.
4. Click **Open System Settings** when the system prompts o use a new network extension for **CisAgent**.
5. Navigate to **Privacy & Security** > **Details,** which prompts for the system password. Specify the password and click **Modify Settings**.
6. Turn on the **CisAgent** switches and click **OK**.
7. Click **Allow** when the system prompts to enable network filtering.
8. In the **Privacy & Security** tab, click **Full Disk Access**.
9. Turn on the **EndpointSecurityExtension** and **CisAgent** switches to provide full disk access.

   Click the **+** button if you do not see **CisAgent** listed.
10. Click **Restart** to complete the CIS client installation.

macOS Sequoia

To install the CIS client on a macOS Sequoia workstation:

1. Open the `CISClient.pkg` installer to launch the package.
2. Follow the prompt, read the agreement and click **Agree** to accept the end-user license agreement.
3. Click **Install**. The system prompts for administrator credentials; enter the password and click **Install Software** > **OK** to begin the installation.

   The CIS client successfully installs within a few seconds.
4. Click **Open System Settings** when the system prompts to use a new network extension for **CisAgent**.
5. Turn on the **CisAgent.app** switch to enable the new network extension.
6. Navigate to **System Settings > General > Login Items & Extensions > Endpoint Security Extensions** and turn on the **CisAgent.app** switch to enable endpoint security extension.
7. In the **Privacy & Security** tab, click **Full Disk Access**.
8. Turn on the **CisAgent** and **EndpointSecurityExtension** switches to provide full disk access.

   Click the **+** button if you do not see **CisAgent** listed.
9. Click **Restart** to complete the CIS client installation.

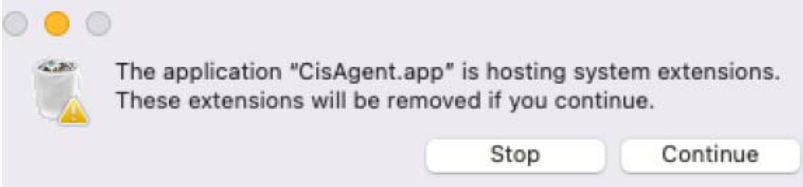
10.2.3 Uninstalling CIS Client

The steps to uninstall the CIS client on a Mac workstation are as follows:

1. Run the command:

   ```
   sudo sh /Applications/CisAgent.app/Contents/Resources/Uninstall.sh
   ```

2. Restart the Mac workstation.
3. On restarting the machine, go to **Application** > right-click on **CisAgent** > **Move to Bin**. This prompts for a password. On specifying the password, a confirmation message to remove the system extensions is displayed, click **Continue**. This cleans up the workstation and uninstalls the CIS client.



4. After uninstalling the CIS client, ensure to restart the Mac workstation. Otherwise, the workstation would still behave as a managed CIS client (accessing and previewing the files uploaded to the cloud).

10.2.4 Log Details

To view the log messages or activities, do one of the following:

In the console of MAC, search for cisagent.

OR

In the Terminal > enter the following command:

```
log show --predicate 'processImagePath CONTAINS "CisAgent"' --last 1d >
cisclient.log
```

This saves the past 24 hours of log messages and activities to the `cisclient.log` file. The `--last` parameter is customizable, if this parameter is not specified, then all the CIS client log messages and activities are saved to the `cisclient.log` file.

11 Scaling and Recovery of Infrastructure Node

This topic describes how to scale up the infrastructure high availability nodes and how to recover them if corrupted.

- Section 11.1, “Scaling Up of HA Nodes,” on page 83
- Section 11.2, “Disaster Recovery of CIS Infrastructure Nodes,” on page 84

11.1 Scaling Up of HA Nodes

Additional nodes can be added to the multi node high availability configuration of the infrastructure server. You can increase the number of nodes from three to five, three to seven, or five to seven.

To add new HA nodes:

1. Install CIS pattern on the new servers you want to add as a HA node.
2. In the CIS Configuration Console, select **Configure Infrastructure Services**, click **Prepare this Node to be HA Ready**, and then click **OK** to confirm.
3. To join the new HA nodes to the existing K3s cluster, run the following command:

   ```
   cis_ext_service.sh enableha <first_node_ip> <node_ip>
   ```
4. To synchronize data between the existing HA nodes and the new HA nodes added, run the following scripts sequentially on any node:

   ```
   cis_ext_service.sh stop
   ```

   ```
   cis_ext_service.sh start
   ```

   The infrastructure services starts on all the HA nodes (existing and new).
5. To synchronize all the HA nodes, run the following command on the core CIS server:

   ```
   /opt/novell/cis/bin/infra-reconfigure --add -infra <FQDN of new infra node> -infra <FQDN of new infra node>
   ```

   The information of the new HA nodes are added to the configuration page.
6. Verify the addition of new HA nodes on the core server in the following files:

   Configuration file: `/etc/opt/novell/cis/configurationStatus.json`

   Config file: `/etc/opt/novell/cis/config`

   The FQDN of the new HA nodes added are also listed in these files along with the FQDN of the existing HA nodes.

11.2 Disaster Recovery of CIS Infrastructure Nodes

All HA nodes must run for the CIS to work properly. If any of the nodes is corrupted, you can replace it with a new recovery server. At least one healthy node must be available to recover the corrupted nodes.

To replace an infrastructure node:

1. On the new node that you are adding to replace the corrupted node, perform Step 1 to Step 5 of Section 11.1, “Scaling Up of HA Nodes,” on page 83.
2. On the CIS core server, run the following command:

   ```
   /opt/novell/cis/bin/infra-reconfigure -replace -new <FQDN of new infra node> -old <FQDN of old infra node>
   ```

3. Verify the replacement of node on the core server in the following files:

   Configuration file: `/etc/opt/novell/cis/configurationStatus.json`

   Config file: `/etc/opt/novell/cis/config`

   The FQDN of the new node is listed instead of the FQDN of the old node in these files.

12 Troubleshooting CIS

This section describes some issues you might experience with Cloud Integrated Storage and provides suggestion for resolving or avoiding them.

- Section 12.1, “CIS Configuration Failure Issues,” on page 85
- Section 12.2, “Upgrade Issues,” on page 88
- Section 12.3, “Changing Firewall State Causes Communication Failure,” on page 89
- Section 12.4, “Default IP for the Docker0 Bridge Conflicts with Current Network,” on page 90
- Section 12.5, “Default CIS Docker Subnet Conflicts with Current Network,” on page 90
- Section 12.6, “Cloud Account Restart Causes CIS Data Services to Fail,” on page 90
- Section 12.7, “Kafka Services Fail to Run on CIS Installed with ‘eth1’,” on page 90
- Section 12.8, “OES Health Page is not Displaying Status of Services,” on page 91
- Section 12.9, “DST Migration From the Shadow Volume To Cloud Storage Causes High CPU Utilization,” on page 91
- Section 12.10, “Scanning Volumes, Migrating and Recalling Data Fails,” on page 92
- Section 12.11, “CIS Agents Stops Randomly During the Data Migration,” on page 92
- Section 12.12, “Health Indicator on CIS Management Console Displays CIS Health as Not Healthy,” on page 92
- Section 12.13, “Infrastructure Services Fails to Come Up After Cleaning Up the Disk Space in HA Node,” on page 93
- Section 12.14, “/var/lib/docker/containers in Infrastructure Server Consumes More Disk Space,” on page 93
- Section 12.15, “Agent is Not Being Listed During the Tier Creation,” on page 93
- Section 12.16, “Agent Fails to Display the Volumes During Tier Configuration,” on page 93

12.1 CIS Configuration Failure Issues

- Section 12.1.1, “CIS Configuration Fails When Certificate Does Not Have SAN Name,” on page 86
- Section 12.1.2, “Public Network Interface is not Added to Firewall Active Zone,” on page 87
- Section 12.1.3, “CIS Configuration Fails When OES is Configured with BIOS Firmware,” on page 87
- Section 12.1.4, “CIS Services Fails to Come Up,” on page 87
- Section 12.1.5, “CIS Configuration Fails With an Error,” on page 87
- Section 12.1.6, “Unable to Configure Kafka Service During CIS Configuration,” on page 88

12.1.1 CIS Configuration Fails When Certificate Does Not Have SAN Name

The following procedure describes about how to create a sample Server Certificate, Server Key and CA Certificate files with SAN name:

1. Create a `temp` folder.
2. Generate CSR (Certificate Signing Request) file.

   The sample csr_detail_file.txt file is as follows:

   ```
   [req]
   default_bits = 2048
   prompt = no
   default_md = sha256
   req_extensions = req_ext
   distinguished_name = dn

   [ dn ]
   O= <Organization Name>
   CN= <Hostname or DNS Name>

   [ req_ext ]
   subjectAltName = @alt_names

   [ alt_names ]
   DNS.1 = oes_doc.labs.wdc.acme.com
   IP = 192.168.0.1
   ```

   The attribute details is as follows:

   - **CN:** Host name of a OES server where CIS server is installed.
   - **DNS.<value>:** DNS name of a OES server where CIS server is installed.

     If DNS name is provided for Gateway Server Address during CIS configuration, ensure that the same DNS name is configured. For more information, see "Configure CIS as a Standalone Server in NSS Media" on page 25.
   - **IP:** IP address of the OES server where CIS is configured.
3. Create the .csr file using the following command:

   ```
   openssl req -new -sha256 -nodes -out csrfilename.csr -newkey rsa:2048 -keyout serverkey.pem -config <csr_detail_file name>
   ```
4. Generate the public certificate using the .csr file and eDirectory.

   4a Go to **iManager > Netiq Certificate Server > Issue Certificate**.

   4b Click **Choose File** to select the .csr file and click **Next**.

   4c Select **Key type** as `SSL or TLS` and **Extended key usage** as `Server authentication` and `User authentication`, then click **Next**.

   4d Select **Certificate Type** as `End Entity` and follow the wizard to continue.

   4e Click **Download the issued certificate** link.
5. Copy the generated server certificate to the `temp` folder.

6 Convert the generated certificate from .der to .pem format.

```
openssl x509 -inform der -in <.der file name> -out <servercert.pem>
```

12.1.2 Public Network Interface is not Added to Firewall Active Zone

When the OES server is installed with firewall disabled, it is set to the default zone. Thus, the public network interface is not added to the firewall active zone.

Before configuring CIS, you must first change the zone from default to public.

1. Open Yast2 Firewall window using `yast2 firewall` command.
2. Select the required ethernet device and then click **Change Zone** > **public**.

12.1.3 CIS Configuration Fails When OES is Configured with BIOS Firmware

When CIS is installed during the OES installation and if OES is configured with BIOS Firmware, some of the CIS service configuration fails. To avoid this issue, restart the server after the installation and then proceed with CIS configuration either using the FQDN or the IP address of the server. However, it can be configured using the IP address without requiring a restart of the server.

12.1.4 CIS Services Fails to Come Up

When you execute `docker ps` command to verify the CIS server configuration, the command does not list any of the CIS services or lists only the collector and aggregator service.

To resolve this issue, perform the following:

- Ensure that the MariaDB and OpenSearch service are up and running with the CIS service that is configured with.
- If firewall is running, ensure that the MariaDB port 3306 and OpenSearch port 9400 is open.

12.1.5 CIS Configuration Fails With an Error

If CIS is the first server installed on the tree, the schema is not updated. Therefore, while configuring CIS an "Undefined Attribute Type" error is displayed. To resolve this issue, extend the eDirectory schema for the CIS server.

To extend the eDirectory schema, perform the following:

- If eDirectory and CIS is installed on the same server, run the following command:

  ```
  /opt/novell/eDirectory/bin/ndssch -h <IP address or hostname where eDirectory or CIS is running> 'cn=admin.o=novell' <file path of cis.sch>
  ```

  For example,

  ```
  /opt/novell/eDirectory/bin/ndssch -h 192.168.0.1 'cn=admin.o=novell' /opt/novell/cis/schema/cis.sch
  ```

OR

- If eDirectory and CIS is installed on different servers, perform the following:
  1. Copy the `cis.sch` file from `/opt/novell/cis/schema` to eDirectory server.
  2. Run the following command:

     `/opt/novell/eDirectory/bin/ndssch -h <IP address or hostname where eDirectory is running> 'cn=admin.o=novell' <file path of cis.sch>`

     For example,

     ```
     /opt/novell/eDirectory/bin/ndssch -h 192.168.0.1
     'cn=admin.o=novell' /root/cis.sch
     ```

12.1.6 Unable to Configure Kafka Service During CIS Configuration

CIS configuration fails with an error "Kafka configuration failed: ErrInternalError: eth0: error fetching interface information: Device not found" while configuring Kafka service. This is because the server has a network device with 'em0' as identifier instead of 'eth0'.

To avoid this issue, perform the following:

1. Login to the server as a `root` user.
2. Run the following command:

   ```
   yast2 lan
   ```
3. On **Network Settings** page under **Overview** tab, select a network device with em0 and click **Edit**.
4. On **Network Card Setup** page under **Hardware** tab, click **Change** and rename the **Device Name** to 'eth0' from 'em0'.
5. Click **Next** and then click **OK**.

12.2 Upgrade Issues

After upgrading OES 2015 SP1 or older OES versions to OES 2018 SP1 or later, during tier creation in CIS management console, the server option fails to list the OES server and displays an error, “Certificate is not valid for any names, but tried to match with <host>”. Because the eDirectory certificates in OES 2015 SP1 and older versions do not add DNS name in the Subject Alternative Name (SAN).

Verify the Certificate

To view the certificate details, run the following command:

```
openssl x509 -in /etc/ssl/servercerts/servercert.pem  -noout -text
```

The output:

```
X509v3 Subject Alternative Name:
IP Address:192.168.2.33, DNS:blr-2-33.example.com
```

If the Subject Alternative Name (SAN) value does not display the IP Address and DNS entries, you must repair the eDirectory certificate.

To repair the eDirectory certificates on the upgraded CIS server:

1. Log in to iManager as Admin.
2. Go to **Roles and Tasks > NetIQ Certificate Server > Repair Default Certificates**.
3. Select the server(s) that own the certificates and click **Next**.
4. Choose the default certificate options and then click **Next**.
   - **4a** Select **Yes All Default Certificates will be overwritten**.
   - **4b** Select **Create SSL CertificateIP** and click the other option to specify the IP address you want to use.
   - **4c** Under **Default DNS Address**, click the other option to specify the DNS address you want to use.
5. Review the tasks to be performed and select **Finish**.
6. Restart eDirectory service.
7. Restart the following services:

   CIS Agent: `systemctl restart oes-cis-agent.service`

   Scanner: `systemctl restart oes-cis-scanner.service`

   Recall Agent: `systemctl restart oes-cis-recall-agent.service`

For more information on repairing server certificates, see OpenText knowledge base article 7013080.

NOTE: Micro Focus is now OpenText.

12.3 Changing Firewall State Causes Communication Failure

If you modify the firewall state on any one of the nodes, the OpenSearch service communication between the infrastructure HA nodes may fail.

To resolve this issue, complete the following steps on any of the nodes:

1. Stop the infrastructure services.

   ```
   cis_ext_services.sh stop
   ```

2. Ensure the infrastructure state is down.

   ```
   cis_ext_services.sh status
   ```

3. Start the infrastructure service.

   ```
   cis_ext_services.sh start
   ```

12.4 Default IP for the Docker0 Bridge Conflicts with Current Network

The default IP address for the docker0 network is 172.17.0.0/16. If the default docker0 network conflicts with your current network, modify the docker0 bridge.

To resolve this issue, complete the following steps:

1. Change the default IP for the docker0 bridge. For more information, see SUSE Support Page (https://www.suse.com/support/kb/doc/?id=000018916).
2. If CIS is configured on the same server, update the new subnet address.

   ```
   /opt/novell/cis/bin/update_docker_bridge.sh
   ```

12.5 Default CIS Docker Subnet Conflicts with Current Network

The default subnet address for CIS docker subnet network is 172.17.0.0/16. If CIS is configured and the default CIS docker subnet conflicts with your current network, modify the subnet address.

To resolve this issue, run the following command:

```
/opt/novell/cis/bin/docker_change_cisnet.sh --subnet "<new subnet address>"
```

For example:

```
/opt/novell/cis/bin/docker_change_cisnet.sh --subnet "10.0.0.0/16"
```

12.6 Cloud Account Restart Causes CIS Data Services to Fail

If the Cloud Account (Amazon/S3) gets restarted for any reason, CIS data migration and recall fails. This is because of the data services signature mismatch. You must provide the key for the Cloud Account again to establish communication between the CIS and the cloud storage.

1. In the CIS Management Console, click **ACCOUNTS**.
2. Click the Cloud Account name and enter the **Access Key** and **Secret Key**.
3. Click **UPDATE**.

12.7 Kafka Services Fail to Run on CIS Installed with ‘eth1’

If you try to configure CIS on OES 25.1 with ‘eth1’ FQDN address, the Kafka services does not come up because of an error in resolving the domain address. To avoid this, configure CIS using the IP address instead of using FQDN of the server.

12.8 OES Health Page is not Displaying Status of Services

On installing an OES service, the `core agent` and `dashboard agent` service will be installed on the OES system. These agent services will try to contact the CIS server and if not available the agent services will stop. Ensure that these services are always running else the communication failure results in an empty page.

To view the health of the services, do the following:

1. On the OES server, restart the Core agent service.

   ```
   systemctl restart oes-core-agent.service
   ```

2. On the OES server, restart the Dashboard agent service.

   ```
   systemctl restart oes-dashboard-agent.service
   ```

3. When the core and dashboard agents are running successfully, then the OES Health page displays the health of the OES servers.

12.9 DST Migration From the Shadow Volume To Cloud Storage Causes High CPU Utilization

Performing DST migration from the Shadow volume to the cloud storage might also cause the OES server to hang or the client connections to drop.

To ensure the CPU is not loaded, the DST migration process is divided in two phases. In phase 1, data is migrated and in phase 2 the attributes of the files and folders are copied from shadow volume to cloud. To perform the migration, do the following:

1. Patch the OES servers with the latest patches.
2. On the OES server where DST migration is planned, do the following:
   - **2a** In the `/etc/opt/novell/cisagent/config` file change the value of the parameter "`TWO_PASS_MIGRATION`" to "`true`".
   - **2b** Restart the agent services: `systemctl restart oes-cis-agent.service`
3. Using CIS management console, migrate the DST shadow volume data to cloud. For more information, see Chapter 9, "Migrating DST Volumes to Cloud," on page 73.
4. In the CIS management console, click the **Tiers** > **Migrate from DST** to view the DST migrated tier.

   Click to view the status of DST migration. If the status displays `Completed`, then migrate the attributes of files and folders.

   - **4a** To migrate the attributes, run the following command on the OES server:

     ```
     copyattr -shadow DSTS -cbv VOL1_CBV
     ```

     where DSTS is the DST shadow volume and VOL1_CBV is the Cloud Backed up volume.

     The `copyattr.log` file is located at `/var/opt/novell/log/cisagent`.
5. Remove the DST pair. For more information, see Chapter 9, "Migrating DST Volumes to Cloud," on page 73.

6 Ensure that the primary volume, shadow volume, and CBV are mounted.

7 Using CIS management console, perform switch operation to move the DST tier to cloud tier. For more information, see “Managing DST Migrate Tiers” on page 63.

12.10 Scanning Volumes, Migrating and Recalling Data Fails

To scan volumes, migrate data to cloud or recall data from cloud, the services that communicate with CIS server are Core Agent, Scanner, CIS agent, and Recall Agent. Ensure that these services are always running else the respective operations fails. Restart the services for performing the operations successfully:

Core agent service: `systemctl restart oes-core-agent.service`

Scan Volumes: `systemctl restart oes-cis-scanner.service`

Migrate Data to Cloud: `systemctl restart oes-cis-agent.service`

Recall Data from Cloud: `systemctl restart oes-cis-recall-agent.service`

12.11 CIS Agents Stops Randomly During the Data Migration

When migrating the data to cloud, CIS agents stops randomly with an error "socket: too many open files". This is because the `Max open files` resource is set with the lower 'soft limit' and 'hard limit' values. In SLES 15, the default values of 'soft limit' and 'hard limit' for `Max open files` resource are 1024 and 4096 respectively.

To resolve this issue, increase the 'soft limit' and 'hard limit' values for `Max open files` resource:

1 Login to the server as a `root` user.

2 Obtain CIS agents process ID using the following command:

```
pgrep cisagents
```

3 For `Max open files` resource, set the 'soft limit' and 'hard limit' values to 65535 using the following command:

```
prlimit --pid <pid_of_cisagent_obtained_in_step2> --nofile=65535:65535
```

4 Verify the 'soft limit' and 'hard limit' values using the following command:

```
cat /proc/<pid_of_cisagent_obtained_in_step2>/limits | grep "open
files"
```

12.12 Health Indicator on CIS Management Console Displays CIS Health as Not Healthy

After successfully configuring CIS in a cluster environment, the health indicator icon on CIS management console displays the CIS health status as not healthy.

To resolve this issue, restart the CIS configuration service on OES server using the following command:

```
systemctl restart oes-cis-configuration.service
```

12.13 Infrastructure Services Fails to Come Up After Cleaning Up the Disk Space in HA Node

After cleaning up all the container data on the infrastructure HA nodes where there was no free disk space available, the infrastructure services on that node still does not come up. This is because the docker services are not running.

To resolve this issue, perform the following on all HA nodes where the issue occurs:

1. Open a terminal console, then log in as a `root` user.
2. Cleanup the old container data using the following command:

   ```
   docker system prune -a -f
   ```
3. On any HA node, execute the following command:

   ```
   sh /opt/novell/cis/bin/cis_ext_service.sh prepare
   ```

For more information on this issue, see https://github.com/moby/moby/issues/31254.

12.14 /var/lib/docker/containers in Infrastructure Server Consumes More Disk Space

The `/var/lib/docker/containers` path in Infrastructure server configured in high availability (HA) consumes more space which results in disk getting filled. For more information, see https://github.com/docker/distribution/blob/master/ROADMAP.md#deletes.

To avoid this issue, ensure to provide sufficient disk space while deploying the Infrastructure server in HA.

12.15 Agent is Not Being Listed During the Tier Creation

In CIS Management Console, during the tier creation the **Server** parameter does not display the OES servers that are configured with CIS server.

To resolve this issue, ensure that the agent is up and running. Also, if firewall is enabled, ensure that the agent port 8000 is open.

12.16 Agent Fails to Display the Volumes During Tier Configuration

During the tier configuration, agent does not display the list of volumes when you click on drop-down menu on the **Volume** parameter in the CIS management console.

To resolve this issue, ensure that the `/etc/resolv.conf` is configured with the appropriate DNS entry so that the OES server and CIS server are mutually resolvable.

13 Best Practices and Common Questions

This section contains recommendations about the following topics.

- Section 13.1, “Backup and Restore Options for Cloud Backed Volumes (CBV),” on page 95
- Section 13.2, “Client Recommendation,” on page 95
- Section 13.3, “Recalling Files from the Cloud Storage to the Source NSS Volume,” on page 96
- Section 13.4, “Log Level Settings,” on page 97
- Section 13.5, “Scanner Settings,” on page 98
- Section 13.6, “Using Distributed File Services (DFS) with Cloud Backed Volume,” on page 98

13.1 Backup and Restore Options for Cloud Backed Volumes (CBV)

If OES Storage Management Service (SMS) or third-party backup software based on SMS is used to backup and restore, it takes care of backing up only the metadata information of the files that are migrated to cloud storage or object store without recalling the actual file data. If third-party backup software that supports the standard Linux Extended Attributes (xattr) is used, ensure that on CBV you backup only metadata for the cloud migrated files. However, if third-party backup software does not provide any option to backup only metadata for the cloud migrated files, then perform the following to disallow recall of migrated files from cloud storage:

1. Open a terminal console, then log in as a `root` user.
2. Add the `RECALL_OFFLINEMODE` environment variable and set to `TRUE` in `/usr/lib/systemd/system/oes-cis-recall-agent.service` on all the agents.

   For example, add the following in `oes-cis-recall-agent.service`.

   ```
   Environment="RECALL_OFFLINEMODE=TRUE"
   ```
3. To ensure system has read any changes, run the following command:

   ```
   systemctl daemon-reload
   ```
4. Restart the recall agent on all OES servers where backup and restore need to be done.

   ```
   systemctl restart oes-cis-recall-agent.service
   ```

13.2 Client Recommendation

For CIS agents to scale up during the data migration, it is recommended to increase the 'soft limit' and 'hard limit' values for `Max open files` resource. For more information, see Section 12.11, “CIS Agents Stops Randomly During the Data Migration,” on page 92.

13.3 Recalling Files from the Cloud Storage to the Source NSS Volume

You can control how files in the cloud storage are recalled automatically to the source NSS volume. When a file is migrated to cloud storage and replaced with a CBV file on the source NSS volume, the CBV file should look and behave like the original file. The size on the disk for the CBV file will be in KBs. File recall is the process by which the user clicks the CBV file and quickly accesses the original file available in the cloud storage.

The CBV file contains the information required to find the original file. When a user attempts to read the CBV file, NSS sends a recall request to CIS, which then executes the recall and passes the file to the NSS.

Use Cases for Recalling Files from the Cloud

Table 13-1 describes use cases for recalling files based on the user access.

Table 13-1 *Recall Behaviors for Files in the Cloud*

	Source NSS Volume	Cloud Storage
When the file is modified	The file gets recalled from the cloud storage and will be available for the duration based on the value configured in the `MOVE_ON_MODIFY_DURATION` parameter. After that duration, the file retains in the NSS volume.	A copy of the file is available on the cloud for the duration based on the value configured in the `MOVE_ON_MODIFY_DURATION` parameter. After that duration, the file copy gets deleted, and it is no longer available.
When the file is accessed but not modified	The file gets recalled from the cloud storage and will be available for the duration based on the value configured in the `MOVE_ON_MODIFY_DURATION` parameter. After that duration, a new CBV file is created, and the recalled file gets deleted to free up space.	A copy of the file is available on the cloud for the duration based on the value configured in the `MOVE_ON_MODIFY_DURATION` parameter. After that duration, the file copy retains in the cloud.

The recalled files are available on both the source NSS volume and cloud storage for a specific time duration based on the value configured in the `MOVE_ON_MODIFY_DURATION` parameter. To modify this time duration, perform the following on the CIS server:

1. Open a terminal console, then log in as a `root` user.
2. Go to the `/etc/opt/novell/cis/config` file and configure the `MOVE_ON_MODIFY_DURATION` parameter with the required time duration. The default value is 3 days. The available range is 1 to 3 days.

   For example:

   ```
   MOVE_ON_MODIFY_DURATION=1
   ```
3. Restart the metadata service.

   ```
   systemctl restart oes-cis-metadata.service
   ```

13.4 Log Level Settings

It includes following sections:

- Section 13.4.1, “CIS Server,” on page 97
- Section 13.4.2, “CIS Agents,” on page 97
- Section 13.4.3, “Infrastructure Services,” on page 97

13.4.1 CIS Server

The CIS services log level is configured using CIS management console. For more information, see “General” on page 68.

13.4.2 CIS Agents

The CIS agents log level can be set at global configuration (all OES server agents) and individual OES server agents using CIS management console. For more information, see Section 7.1.8, “Agents,” on page 65.

13.4.3 Infrastructure Services

The infrastructure services includes ZooKeeper, OpenSearch, and Kafka services configured in high availability nodes. You must login to all the nodes and then configure the log level for each infrastructure services separately.

1. Open a terminal console, then log in as a `root` user.
2. Configure log level for the following infrastructure services:
   - **ZooKeeper:** Go to `/etc/opt/novell/cis/zk/log4j.properties` and configure the required log level in `rootLogger.level` parameter.

     For example, to set `Debug` log level for ZooKeeper, add the following in `/etc/opt/novell/cis/zk/log4j.properties`.

     ```
     zookeeper.root.logger=DEBUG, CONSOLE
     zookeeper.console.threshold=WARN
     ```
   - **OpenSearch:** Go to `/etc/opt/novell/cis/es/log4j2.properties` and configure the required log level in `rootLogger.level` parameter.

     For example, to set `Debug` log level for OpenSearch, add the following in `/etc/opt/novell/cis/es/log4j2.properties`.

     ```
     rootLogger.level = debug
     ```
   - **Kafka:** Go to `/etc/opt/novell/cis/kafka/log4j.properties` and configure the required log level in `log4j.rootLogger` parameter.

     For example, to set `Debug` log level for Kafka, add the following in `/etc/opt/novell/cis/kafka/log4j.properties`.

     ```
     log4j.rootLogger=DEBUG, stdout
     ```

   The log levels supported are: Trace, Debug, Info, Warn, and Error. The default value is Warn.

3 Restart docker services on all the infrastructure HA nodes using the following command:

```
systemctl restart docker.service
```

13.5 Scanner Settings

After configuring the CIS server, the scanner agent associated to CIS server scans all the volumes. To rescan the OES server at a scheduled time, add the environment variable in `oes-cis-scanner.service` on all the OES server agents. Based on the value configured, the scanner scans the OES server to get the updated volumes information. The default value is 7 days.

This settings are applicable to all OES servers that are configured before OES 2018 SP3. To configure the scanner settings on OES 25.1 servers, see Section 7.1.8, “Agents,” on page 65.

To set the configuration to scan OES server volumes, perform the following:

1 Configure the `SCAN_INTERVAL_DAYS` environment variable in `/usr/lib/systemd/system/oes-cis-scanner.service` on all the agents.

For example, add the following in `oes-cis-scanner.service`.

```
Environment="SCAN_INTERVAL_DAYS=2"
```

2 To ensure system has read any changes, run the following command:

```
systemctl daemon-reload
```

3 Restart the scanner agent.

```
systemctl restart oes-cis-scanner.service
```

13.6 Using Distributed File Services (DFS) with Cloud Backed Volume

Distributed File Services (DFS) is installed automatically as part of the NSS file system. Cloud Integrated Storage supports using DFS junctions on the primary NSS volume. The primary volume can also be the target of a junction. Primary NSS volumes that contain DFS junctions or are junction targets can reside in a OES Cluster Services cluster.

DST does not support using DFS junctions on the CBV. The CBV cannot be the junction target.

Table 13-2 on page 99 summarizes the supported CIS configurations for use with DFS:

Table 13-2 *CIS support for DFS Features*

DFS Features	Primary NSS Volume	Cloud Backed Volume	Cluster	File Access Protocol
Junctions	Yes	No	Yes	NCP Novell CIFS. DFS support must be enabled in CIFS. See DFS Junction Support in CIFS Linux in the OES CIFS for Linux Administration Guide. Linux Samba does not support DFS junctions for NSS volumes.
Junction targets	Yes	No	Yes	Not applicable
Move/split volumes	No	No	No	Not applicable

14 Known Issues

This section lists the known issues in Cloud Integrated Storage.

- CIS clients do not support Windows 11 24h2 and macOS Sequoia 15.1.
- CIS works only with the default NSS mount volume path.
- If the MS SQL server is configured in a timezone that is different from the CIS server, then the migration time stamp on the CIS **Dashboard** page is synchronized with MS SQL server.

A Configuration and Log Files

This section provides information on all CIS and infrastructure components configuration and log files location.

Table A-1 *CIS Configuration Files*

Path	Description
/etc/opt/novell/cis/config	CIS server configuration
/etc/opt/novell/cis/fluentbit/config	CIS server log configuration
/etc/opt/novell/cis/fluentbit/fluentd.conf	Fluent Bit configuration for CIS server
/etc/opt/novell/cis/certs/rootCAs	If secure communication is used with the target cloud or object store, copy the CA bundle in PEM format to this location.

Table A-2 *CIS Log Files*

Path	Description
/var/log/messages	CIS server logs
/var/opt/novell/log/cis/microservices	Common log location of all the CIS services
/var/opt/novell/log/coreagent/coreagent.log	Contains log messages of OES Core agent
/var/opt/novell/log/cisagent/agent.log	Contains log messages of OES server agent
/var/opt/novell/log/cisagent/recallagent.log	Contains log messages of OES server recall agent
/var/opt/novell/log/cisagent/cisscanner.log	Contains log messages of OES server scanner
/var/opt/novell/log/dashboardagent/dashboardagent.log	Contains log messages of OES dashboard agent
/var/log/mysql/mysqld.log	MariaDB server logs
/var/log/opensearch/opensearch.log	OpenSearch logs

B Installing and Configuring MariaDB

This section describes how to install and configure the MariaDB database to use with CIS.

- Section B.1, “Installing MariaDB,” on page 105
- Section B.2, “Configuring MariaDB,” on page 105

B.1 Installing MariaDB

1. Ensure you have access to your operating system installation media.
2. In YaST, click **Software > Software Management**.
3. In the **Search** field, type `mariadb`, then click **Search**.
4. Select **mariadb**, then click **Accept**.

   The MariaDB is successfully installed.
5. Continue with Section B.2, “Configuring MariaDB,” on page 105.

B.2 Configuring MariaDB

When MariaDB is initially installed, it is not configured with an administrator password, nor is it configured to start automatically. To set up the MariaDB database server for use with CIS, perform the following:

1. In a terminal window, become the root user.
2. To start the database server, run the following command:

   ```
   systemctl restart mysql.service
   ```
3. To enable the database server, run the following command:

   ```
   systemctl enable mysql.service
   ```
4. To verify the database server has started, run the following command:

   ```
   systemctl status mysql.service
   ```
5. To set the root password and enable root access from remote machines, run the following command:

   ```
   mysql_secure_installation
   ```

   5a It prompts for `current password for root user`, press 'Enter' to continue.

   5b It prompts to `Set root password?`, enter 'y' to continue and then enter password.

   The password is updated successfully.

   5c It prompts to `Remove anonymous users?`, press 'Enter' to continue with the default configuration.

   5d It prompts to `Disallow root login remotely?`, enter 'n' to continue.

5e It prompts to `Remove test database and access to it?`, press 'Enter' to continue with the default configuration.

5f It prompts to `Reload privilege tables now?`, enter 'y' to continue.

6 Login to MariaDB.

```
mysql -u root -p
```

It prompts for password.

7 To grant permissions for the superuser account, run the following commands:

```
> GRANT ALL PRIVILEGES ON *.* TO '<username>'@'%' IDENTIFIED BY
'<password>';
```

```
> FLUSH PRIVILEGES;
```

For example:

```
GRANT ALL PRIVILEGES ON *.* TO 'root'@'%' IDENTIFIED BY 'password';
```

8 To enable the firewall, run the following command:

```
yast2 firewall
```

The **Firewall Configuration: Start-Up** window is displayed.

9 In the left menu, click **Allowed Services** and then click **Advanced** option.

The **Additional Allowed Ports** window is displayed.

10 Add 3306 port under the **TCP Ports** and then click **OK**.

11 Click **Next** and **Finish**.

C Creating Certificates

When CIS is configured on a clustered NSS volume, you must use the cluster resource IP for CIS configuration, thus a server certificate with the cluster IP and SAN name is required.

- Section C.1, “Creating Certificates for CIS using Identity Console,” on page 107
- Section C.2, “Creating Certificates for CIS using iManager,” on page 108
- Section C.3, “Reconfiguring Certificates,” on page 109

C.1 Creating Certificates for CIS using Identity Console

To create a sample Server Certificate, Server Key, and CA Certificate files using Identity Console complete the following steps:

1. Create a `temp` folder.
2. Generate CSR (Certificate Signing Request) file.

   The sample `csr_detail_file.txt` file is as follows:

   ```
   [req]
   default_bits = 2048
   prompt = no
   default_md = sha256
   req_extensions = req_ext
   distinguished_name = dn

   [ dn ]
   O= <Organization Name>
   CN= <Hostname or DNS Name>

   [ req_ext ]
   subjectAltName = @alt_names

   [ alt_names ]
   DNS.1 = oes_doc.labs.wdc.acme.com
   IP = 192.168.0.1
   ```

   The attribute details is as follows:

   - **CN:** Host name of a gateway cluster resource.
   - **DNS.<value>:** DNS name of a gateway cluster resource.

     If DNS name is provided for Gateway Server Address during CIS configuration, ensure that the same DNS name is configured. For more information, see “Configure CIS Services” on page 30.
   - **IP:** IP address of the cluster gateway resource IP.
3. Create the `.csr` file using the following command:

```
openssl req -new -sha256 -nodes -out csrfilename.csr -newkey rsa:2048 -
keyout serverkey.pem -config <csr_detail_file name>
```

4 Perform the following steps to generate the public certificate:

4a Go to **Identity Console > Certificate Server > Issue Certificates**.

4b Browse and select a CSR file.

4c Select **Key type** as `SSL or TLS` under **Key Usage Specifications**.

4d Select `Server authentication` and `User authentication` under **Extended key usage**.

4e Select `End Entity` certificate type under **Basic Constraints**.

4f Specify the following parameters:

- **Subject Name**: `O=Organization Name; CN=oes_doc.labs.wdc.acme.com`
- **Subject Alternative Names:** IP and DNS name

4g Click **Download the issued certificate** link.

For more information, see *Issuing a Public Key Certificate using Identity Console* (https://www.netiq.com/documentation/identity-console/identity_console-admin/data/t4di8qw40pg7.html).

5 Copy the generated server certificate to the `temp` folder.

6 Convert the generated certificate from `.der` to `.pem` format.

```
openssl x509 -inform der -in <.der file name> -out <servercert.pem>
```

C.2 Creating Certificates for CIS using iManager

To create a sample Server Certificate, Server Key and CA Certificate files using iManager complete the following steps:

1 Create a `temp` folder.

2 Generate CSR (Certificate Signing Request) file.

The sample csr_detail_file.txt file is as follows:

```
[req]
default_bits = 2048
prompt = no
default_md = sha256
req_extensions = req_ext
distinguished_name = dn

[ dn ]
O= <Organization Name>
CN= <Hostname or DNS Name>

[ req_ext ]
subjectAltName = @alt_names

[ alt_names ]
DNS.1 = oes_doc.labs.wdc.acme.com
IP = 192.168.0.1
```

The attribute details is as follows:

- **CN:** Host name of a gateway cluster resource.
- **DNS.<value>:** DNS name of a gateway cluster resource.

  If DNS name is provided for Gateway Server Address during CIS configuration, ensure that the same DNS name is configured. For more information, see "Configure CIS Services" on page 30.
- **IP:** IP address of the cluster gateway resource IP.

3 Create the `.csr` file using the following command:

```
openssl req -new -sha256 -nodes -out csrfilename.csr -newkey rsa:2048 -keyout serverkey.pem -config <csr_detail_file name>
```

4 Perform the following steps to generate the public certificate:

4a Go to **iManager > Netiq Certificate Server > Issue Certificate**.

4b Click **Choose File** to select the .csr file and click **Next**.

4c Select **Key type** as `SSL or TLS` and **Extended key usage** as `Server authentication` and `User authentication`, then click **Next**.

4d Select **Certificate Type** as `End Entity` and follow the wizard to continue.

4e Click **Download the issued certificate** link.

5 Copy the generated server certificate to the `temp` folder.

6 Convert the generated certificate from `.der` to `.pem` format.

```
openssl x509 -inform der -in <.der file name> -out <servercert.pem>
```

C.3 Reconfiguring Certificates

Centralized certificate management helps administrators in managing the certificate lifecycle. The features are:

- Mail notifications notify the administrator and the root user of the certificates' impending expiration.
- Indicates where each service's certificates can be found.
- Indicates the certificate's type, such as whether it is self-signed or CA-signed.
- Indicates whether the certificates are still valid.
- Reconfigures the OES services to use a new certificate when certificates are invalid, corrupted or expired.
- A browser-based tool (Unified Management Console, or UMC) that enables remote management of certificates across servers will be available in the upcoming releases.

For more information about reconfiguring CIS certificates, see Example - Replacing Expired or Corrupted Certificate of CIS Server in Installation Guide.