



# Centralized License Manager

Release 25.8

## CLM User Guide

---

3HE-21489-AAAB-TQZZA  
Issue 1  
September 2025

© 2025 Nokia.

Use subject to Terms available at: [www.nokia.com/terms](http://www.nokia.com/terms)

---

**Legal notice**

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

---

This document includes Nokia proprietary and confidential information, which may not be distributed or disclosed to any third parties without the prior written consent of Nokia.

This document is intended for use by Nokia's customers ("You"/"Your") in connection with a product purchased or licensed from any company within Nokia Group of Companies. Use this document as agreed. You agree to notify Nokia of any errors you may find in this document; however, should you elect to use this document for any purpose(s) for which it is not intended, You understand and warrant that any determinations You may make or actions You may take will be based upon Your independent judgment and analysis of the content of this document.

Nokia reserves the right to make changes to this document without notice. At all times, the controlling version is the one available on Nokia's site.

No part of this document may be modified.

NO WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY OF AVAILABILITY, ACCURACY, RELIABILITY, TITLE, NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, IS MADE IN RELATION TO THE CONTENT OF THIS DOCUMENT. IN NO EVENT WILL NOKIA BE LIABLE FOR ANY DAMAGES, INCLUDING BUT NOT LIMITED TO SPECIAL, DIRECT, INDIRECT, INCIDENTAL OR CONSEQUENTIAL OR ANY LOSSES, SUCH AS BUT NOT LIMITED TO LOSS OF PROFIT, REVENUE, BUSINESS INTERRUPTION, BUSINESS OPPORTUNITY OR DATA THAT MAY ARISE FROM THE USE OF THIS DOCUMENT OR THE INFORMATION IN IT, EVEN IN THE CASE OF ERRORS IN OR OMISSIONS FROM THIS DOCUMENT OR ITS CONTENT.

Copyright and trademark: Nokia is a registered trademark of Nokia Corporation. Other product names mentioned in this document may be trademarks of their respective owners.

© 2025 Nokia.

# Contents

- About this document.....5**
- 1 Getting started.....7**
  - 1.1 Overview .....7
  - 1.2 Architecture .....8
  - 1.3 CLM UI overview.....9
  - 1.4 How do I access the CLM UI? .....9
  - 1.5 Pathway for typical CLM operator configuration .....10
- 2 Network pool keys.....11**
  - 2.1 Overview .....11
  - 2.2 How do I obtain a network pool key? .....12
  - 2.3 How do I upload a network pool key? .....12
  - 2.4 What does this network pool key upload error mean? .....12
  - 2.5 How do I delete a network pool key? .....13
  - 2.6 How do I view details of a network pool key? .....13
  - 2.7 How do I view allocated entitlements for a selected network pool key? .....14
  - 2.8 How do I download a usage report for a network pool key? .....14
  - 2.9 How do I download a network function inventory report? .....15
- 3 License repositories .....17**
  - 3.1 What is a license repository? .....17
  - 3.2 How do I configure a license repository? .....17
  - 3.3 How do I edit a license repository? .....18
  - 3.4 How do I delete a license repository? .....18
- 4 Network functions.....21**
  - 4.1 Requirements.....21
  - 4.2 How do I add a network function?.....21
  - 4.3 How do I copy an existing network function? .....23
  - 4.4 How do I bulk copy network functions?.....23
  - 4.5 How do I view network functions?.....25
  - 4.6 How do I edit a network function? .....25
  - 4.7 How do I upgrade a network function to a new major release? .....27
  - 4.8 How do I upgrade a network function to a new minor release? .....28
  - 4.9 How do I view an event log for a specific network function?.....28
  - 4.10 How do I delete a network function? .....29

---

- 4.11 How do I manually generate and deploy a license key? .....29
- 4.12 What does revoking a license key mean? .....31
- 4.13 How do I revoke a license key? .....31
- 4.14 How do I enable license key auto-renewal? .....31
- 4.15 How do I disable license key auto-renewal?.....33
- 4.16 How do I generate and download license keys?.....33
- 5 Notifications and events .....35**
  - 5.1 Overview .....35
  - 5.2 How do I sort or filter notifications? .....35
  - 5.3 What does this notification mean? .....35
  - 5.4 How do I configure notification thresholds? .....38
  - 5.5 How do I view the events history? .....38
  - 5.6 How do I view log details for an event? .....39
- 6 CLI commands .....41**
  - 6.1 Overview .....41
  - 6.2 CLI classic commands .....41
  - 6.3 Model-driven CLI commands .....41
- 7 CLM backup and restore .....43**
  - 7.1 Overview .....43
  - 7.2 How do I back up the CLM deployer host? .....43
  - 7.3 How do I restore the CLM deployer host? .....44
  - 7.4 How do I check CLM database synchronization? .....46
  - 7.5 How do I configure scheduled CLM backups? .....48
  - 7.6 How do I back up the CLM cluster databases? .....49
  - 7.7 How do I restore the Kubernetes etcd data in a CLM cluster? .....52
  - 7.8 How do I restore the CLM cluster databases? .....56
  - 7.9 How do I back up the CLM Kubernetes secrets? .....60
  - 7.10 How do I restore the CLM Kubernetes secrets? .....62

---

# About this document

## Purpose

The *CLM User Guide* describes how to configure and use the Centralized License Manager. This document applies to users of an independent CLM deployment as well as those who use a CLM deployment that is integrated with NSP.

## Safety information

For your safety, this document contains safety statements. Safety statements are given at points where risks of damage to personnel, equipment, and operation may exist. Failure to follow the directions in a safety statement may result in serious consequences.

## Document support

Customer documentation and product support URLs:

- [Documentation Center](#)
- [Technical support](#)

## How to comment

[Documentation Feedback](#)



---

# 1 Getting started

## 1.1 Overview

The Centralized License Manager (CLM) provides simplification of network function license management. With CLM, operators can flexibly control license entitlement and monitor license usage for their managed network functions which can be any processing function in a network; for example: a network element or a software instance running on hardware, or a virtualized function instantiated on a platform, such as on a cloud infrastructure. The CLM server communicates with the managed network as well as the license key repository that is used to store the license keys for network functions.



### CAUTION

#### Service Disruption

*A CLM instance is node-locked to the server where it is installed.*

*Network Pool Keys issued by Nokia are tied to a specific CLM instance by its UUID.*

*Resource and network parameters associated with the CLM server shall not be altered after Network Pool Keys are received for a specific CLM instance.*

*An operator may migrate a CLM instance within a VM environment only if the server resource and network characteristics remain constant.*



**Note:** The user profile of the user entered in the connection properties of the network function must be configured to use classic CLI for VSR-I, or classic or model-driven CLI for 7x50 SR/XRS.



**Note:** There are three types of CLM users defined by a system administrator during CLM installation:

- system administrators, who automatically have read/write access to CLM
- users with read-write access to CLM, as defined by the user access control function in Users and System Security.
- users with read-only access to CLM, as defined by the user access control function in Users and System Security.

See the *NSP System Administrator Guide* for more information about user access control.

CLM can be either deployed independently as a standalone product, or starting with CLM Release 25.4, integrated with NSP. The integrated deployment not only manages licenses for network functions but it also manages the NSP system license.

## 1.2 Architecture

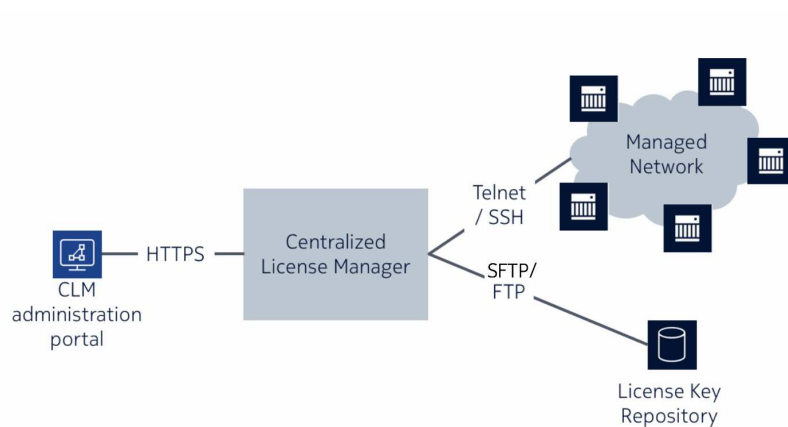
There are two deployment types of CLM:

- Independent - CLM can be used without NSP installed.
- Integrated - CLM is integrated with NSP.

An NSP-integrated deployment of CLM delivers the same functionality as the independent deployment. Additionally, you can use it to manage NSP license keys. The license key for NSP in an integrated deployment is called the NSP Routing key.

The following Figure shows the architecture of CLM.

Figure 1-1 CLM architecture



CLM consists of an administration portal and a server. The CLM administration portal is a user interface (UI) that allows an operator to perform administrative functions such as uploading licenses and viewing notifications.

The CLM server has the business logic for the license management of network functions as well as NSP, when integrated with NSP. The network license pool is maintained here for each network function type, as defined by the network pool key. A network pool key is a file that defines the quantity or pool of ASLs for a specific network function.

**Note:** The operator must acquire the network pool key for the specific network function type and version from your Nokia NSP product representative.

License entitlement for a network function involves license pool capacity reservation. The CLM server communicates with the managed network functions as well as the license key repository that is used to store the license keys used by the network functions. The CLM allows an operator to configure, manage, and monitor the license key deployment.



---

## 1.3 CLM UI overview

### 1.3.1 Overview

This section explains how to recognize and use common features of the CLM UI.

The main starting point for users is the default landing page, the **Network Map and Health** dashboard. Once you drill down from this default view, you start navigating in context.

The CLM UI uses breadcrumbs that orient you to your current main menu selection and allow you to navigate easily between different views. For example, you can navigate from **Centralized License Manager, Network Pool Keys** to a different view by clicking the view selector. This opens a drop-down menu of other CLM views. To return to the default view, click the breadcrumb **Centralized License Manager**.

Clicking the Nokia logo from any view will take you back to the default view, **Network Map and Health**.

### 1.3.2 Banner bar

In both deployment types, independent and integrated, the banner bar is accessible at the top of every view and comprises the following elements (left to right):

- [“Menu” \(p. 8\)](#)
- [“User menu” \(p. 9\)](#)
- [“Help button” \(p. 9\)](#)

#### Menu


The menu provides access to the **NSP ADMINISTRATION** areas that include, for example, **System Health, Users and System Security**, and **Centralized License Manager**. It is your primary navigation tool within the CLM UI.

To access the menu, click  on the top left corner of the Centralized License Manager banner bar.

#### User menu

The user menu provides access to release information and settings. Users can also change their password or sign out of CLM.

#### Help button

A  button on the right-hand side of the CLM banner bar gives you access to the user documentation. You can read Quick Help topics related to the current view, or click **OPEN HELP CENTER** at the bottom of the Quick Help menu to open the full Help Center in a new browser tab.

## 1.4 How do I access the CLM UI?

Both deployment types, independent and integrated, use a web-based UI in which the main menu is used for navigation.

- 
- 1 \_\_\_\_\_  
Launch the CLM in independent or integrated deployment:  
`https://Server_IP`  
where *Server\_IP* is the IP address of the CLM server or NSP
  - 2 \_\_\_\_\_  
Log into the system using your login credentials, then click **SIGN IN**.
  - 3 \_\_\_\_\_  
Enter your login credentials and click **SIGN IN**.
  - 4 \_\_\_\_\_  
From the main menu, select **Centralized License Manager**.

END OF STEPS \_\_\_\_\_

## 1.5 Pathway for typical CLM operator configuration

- 1 \_\_\_\_\_  
Obtain your network pool key(s) from your Nokia NSP product representative; see [2.2 “How do I obtain a network pool key?”](#) (p. 12).
- 2 \_\_\_\_\_  
Upload your network pool key(s); see [2.3 “How do I upload a network pool key?”](#) (p. 12).
- 3 \_\_\_\_\_  
Configure your customer license repositories; see [3.2 “How do I configure a license repository?”](#) (p. 17).
- 4 \_\_\_\_\_  
Define your network functions; see [4.2 “How do I add a network function?”](#) (p. 21). This is not applicable for the NSP Routing key.
- 5 \_\_\_\_\_  
Generate and deploy license keys; see [4.11 “How do I manually generate and deploy a license key?”](#) (p. 29) or [4.14 “How do I enable license key auto-renewal?”](#) (p. 31).

END OF STEPS \_\_\_\_\_

---

## 2 Network pool keys

### 2.1 Overview

Before entitlements can be associated with a network function, you need to first obtain a network pool key from Nokia. A network pool key is a file that contains details about the quantities and entitlements assigned to a specific release of a network function; for example, VSR-I Release 16.0. A network pool key contains an expiry date, after which time the ability to generate license keys for network functions is unavailable. The CLM provides a notification if the network pool key is nearing its expiry date. Network pool keys are digitally signed and the CLM rejects keys that have been tampered with. For more information about network pool keys, see [2.2 “How do I obtain a network pool key?”](#) (p. 12).

To generate license keys for network functions, you must first upload your network pool key(s) into the CLM. Your network pool key may come to you as a zip archive file from Nokia. You can upload the network pool keys you have received from Nokia; there is no need to unzip the file. See [2.3 “How do I upload a network pool key?”](#) (p. 12) for more information about uploading network pool keys.

Uploaded network pool keys are displayed in a list in the Network Pool Keys view. The list provides information about the product, entitlements, and release of each network pool key. Entitlements for each network pool key are grouped into categories. Expanding a category provides you with details for each entitlement, including the name of the entitlement, the initial release, and how many are licensed, consumed, and remaining. The network pool key list displays a warning icon, for example orange, if the network pool key is nearing its expiry date, or red, if all allocated entitlements have been consumed. When you click on a network pool key, the info panel to the right displays more information, including license type, product name, and activation date. For more information about network pool keys, see [2.6 “How do I view details of a network pool key?”](#) (p. 13).

You can download a report in CSV or text format with information about the current usage of a network pool key. The report can be generated for one network pool key at a time, and contains the following information:

- Report generation date/time
- Activation date
- Expiration date
- Number of network functions - this is not applicable for the NSP Routing key
- For each entitlement in the network pool key, numbers for: licensed, consumed, and remaining

See [2.8 “How do I download a usage report for a network pool key?”](#) (p. 14) for information about downloading a network pool key usage report.

The **Download NF Inventory Report (CVS)** menu option is available for all pool keys except for the NSP Routing key. The network inventory report includes a complete list of entitlements and how many are consumed. Network functions associated with a specific network pool key, including entitlements and consumed amounts. The report can be generated for one network pool key at a time. See [2.9 “How do I download a network function inventory report?”](#) (p. 15) for more information about downloading the network function inventory report.

---

## 2.2 How do I obtain a network pool key?

**i** **Note:** A network pool key is locked to a specific CLM installation.

1

Using the main menu, navigate to **Centralized License Manager, Configurations**. Then click **System Information**.

2

Click **Download** below **System Certificate Signing Request (CSR)**.

3

Email the downloaded zip file to your Nokia NSP product representative.

END OF STEPS

When Nokia receives the zip file containing the downloaded CSR and UUID information, a network pool key is provided back to you which can be uploaded on CLM.

## 2.3 How do I upload a network pool key?

**i** **Note:** If you have already uploaded a network pool key for the same product and license type, you will replace the currently uploaded network pool key with the new one. When you replace an uploaded network pool key, the network functions remain and do not need to be changed.

1

Using the main menu, navigate to **Centralized License Manager, Network Pool Keys**. Click **+ Pool Key**

2

Choose the file that contains the network pool key provided to you by Nokia and click **Upload**. A message appears confirming the upload was successful and a network pool key tile appears as a visual representation.

If an error message appears instead, see [2.4 "What does this network pool key upload error mean?"](#) (p. 12).

END OF STEPS

## 2.4 What does this network pool key upload error mean?

When you upload a network pool key, there are a number of errors that can occur. Contact Nokia to resolve any problems.

Common errors include:

Error	Cause
Invalid UUID	The UUID specified in the network pool key does not match the UUID of your CLM.
Invalid field: expiry date	The network pool key has expired and cannot be used.
Zip archive processing error	The zip file is corrupt.
Invalid signature	The network pool key has an invalid signature and might have been tampered with.
Parsing error	There was a problem parsing the network pool key.
Invalid pool key certificate	The network pool key was generated using a CSR from another CLM. This could happen if a user sends an older CSR after they have re-installed CLM.

## 2.5 How do I delete a network pool key?

After a pool key is no longer required, for example it has expired, you can delete the pool key from the CLM.

**i** **Note:** You receive an error message if you attempt to delete a network pool key that has associated network functions. You must first delete all network functions that reference the network pool key.

1 \_\_\_\_\_

Using the main menu, navigate to **Centralized License Manager, Network Pool Keys**.

To remove any of the network pool key tiles, click **⋮**, **Delete**.

A confirmation dialog box opens.

2 \_\_\_\_\_

Click **Delete**.

The network pool key is removed from the CLM.

END OF STEPS \_\_\_\_\_

## 2.6 How do I view details of a network pool key?

1 \_\_\_\_\_

Using the main menu, navigate to **Centralized License Manager, Network Pool Keys**.

---

2

Click on a network pool key. The info panel to the right displays the **Network Pool Key Details**.



**Note:** In most cases, the panel is expanded by default. If it isn't, it can be displayed with **<** or hidden with **>** .

END OF STEPS

---

## 2.7 How do I view allocated entitlements for a selected network pool key?

1

Using the main menu, navigate to **Centralized License Manager, Network Pool Keys**.

2

Click on a network pool key in the list to view entitlement categories. These can be expanded to view entitlement details.

- The **Initial Release** column displays release specific information for entitlements of network functions that have been upgraded. If no value is listed, the entitlement supports the original release of the network function. A range [x-y] specifies the release range that an entitlement is valid for. A [x+] value specifies the release an entitlement was introduced in.
- The **Licensed** column displays a count of the total number entitlement provided by the network pool key.
- The **Consumed** column displays how much of the entitlement has been allocated to your various network functions.
- The **Remaining** column shows how much of the entitlement remains for future use.
- A notification icon appears when an entitlement has approached or exceeded the set thresholds.

END OF STEPS

---

## 2.8 How do I download a usage report for a network pool key?

1

Using the main menu, navigate to **Centralized License Manager, Network Pool Keys**.

2

To download a usage report, click on the network pool key tile and choose one of the following download options:

- **Usage Report (CSV)**

- 
- **Usage Report (TEXT)**

END OF STEPS

---

## 2.9 How do I download a network function inventory report?

Network function inventory reports are available for all pool keys except for the NSP Routing key.

1

Using the main menu, navigate to **Centralized License Manager, Network Pool Keys**.

2

On the network pool key tile, click , **NF Inventory Report (CSV)**.

END OF STEPS

---





---


## 3 License repositories

### 3.1 What is a license repository?

A license repository contains information about the SFTP/FTP server that is used by your network functions (for example, VSR-I) to obtain their license key files. This information is used by the CLM to connect, log in, and manage license key files that the CLM generates and are referenced by the network functions. Once a license repository has been created in CLM, it can be assigned to network functions. When you generate and deploy a license key for a specific network function, the information defined in the license repository assigned to the network function is used for license key management.

For a 7x50 SR/XRS network function, the preferred method of license key storage is local storage. See [4.2 “How do I add a network function?” \(p. 21\)](#) for information about setting local storage as the license repository.

### 3.2 How do I configure a license repository?

 **Note:** Create one license repository for each unique location that you want to store license keys. A location is unique if its server IP address and Full Directory Path are different than another license repository.

1

Using the main menu, navigate to **Centralized License Manager, Configurations**. Then click **License Repositories**.

2

Click **+ Repository**. The **Add License Repository** form opens.

3


Configure the required parameters, ensuring that:

- The **Name** is unique.
- The **Repository Type** is correct.
- The login credentials are correct.
- The directory specified by **Full Directory Path** exists and the user specified in the connection properties has read/write permissions to the directory.
- The directory is specified relative to root of the file system.

4

Click **Save**.

---

 **Note:** After you create a license repository, wait for a few minutes as the CLM automatically validates the connection.

END OF STEPS

---

### 3.3 How do I edit a license repository?

1 

---

Using the main menu, navigate to **Centralized License Manager, Configurations**. Then click **License Repositories**.

2 

---

Click  for the license repository you want to edit. The **Edit License Repository** form opens.

3 

---


Edit the parameters.

- The **Name** must be unique.
- You cannot change the **Full Directory Path** after you have associated network functions to the license repository.

4 

---


Click **Save**.

 **Note:** After you edit a license repository, wait for a few minutes as the CLM automatically validates the connection.

END OF STEPS

---

### 3.4 How do I delete a license repository?

 **Note:** You will receive an error message if you attempt to delete a license repository that has been assigned to one or more network functions.

1 

---

Using the main menu, navigate to **Centralized License Manager, Configurations**. Then click **License Repositories**.

2 

---

Un-assign the license repository from any network functions that are referencing it. Do this by editing a network function as described in [4.6 "How do I edit a network function?" \(p. 25\)](#). Then set the **License Repository** property to 'None'.

3 

---

Click  for the license repository you want to delete. A delete confirmation dialog box opens.

---

**4**

Click **Delete**.

**END OF STEPS**


---



---

## 4 Network functions

### 4.1 Requirements

 **Note:** Network functions cannot be created with NSP Routing keys.

Network functions have the following requirements:

- The UID must be the OAM IP or the Inband IP through which the network function is reachable. IPv4 and IPv6 addresses are supported.
- A network function must have a unique name.
- A network function for a given product type must have a unique UID within that product type.
- The user profile of the user entered in the connection properties of the network function must be configured to use classic CLI for VSR-I, or classic or model-driven CLI for 7x50 SR/XRS.
- See [Chapter 6, “CLI commands”](#) for the CLI commands that the user entered in the connection properties of the network function needs access to for each network function.
- When using dynamic licensing, the name of a VSR-I should only consist of ASCII characters and not contain the following characters: quote("), forward-slash(/), back-slash(\), asterix(\*), question mark(?).

### 4.2 How do I add a network function?

CLM allows you to assign entitlements to your network functions to enable specific features of the network function. An entitlement is a definition of the application-specific licenses for a specific network function.

1

Using the main menu, navigate to **Centralized License Manager, Network Pool Keys**.

2

In the network pool key list, click  , **Add Network Function**. The **Add Network Function** form opens.

3

If the network pool key supports more than one release of a network function, the **Version** parameter is displayed. Select the matching major release of the software running on the network function you are defining.

4

Configure the required parameters.

After you populate the **Name**, **UID**, **Connection Username** and **Connection Password** parameters, the **FETCH UID** button is enabled. Its color changes from light to dark gray.

---

Fetching the UUID, which auto-populates the UUID parameter(s), is only required if you are generating and downloading license keys. If you close the Define Network Function form when the CLM is retrieving the UUID(s), the process is cancelled.

For a 7x50 SR/XRS network function, the preferred setting for the **License Repository** parameter is **Local Storage**.

**i** **Note:** If you populate the UUID parameter(s) for a network function and if any one or both UUIDs do not match the network function, deployment will fail.

---

5

Apply one or more product standard templates, as required.

Certain network functions (for example, VSR-I) support standard sets of functionality that can be applied when creating or editing a network function. If a product supports the product standard templates, the **Apply Templates** button is enabled.

- Click **Apply Templates**.
- Select one or more product templates to apply.
- Select “Replace all existing entitlements” before applying the template(s).
- Click **Apply**.

---

6

Filter the entitlements, as required.

By default, all (licensed and unlicensed) entitlements are shown in the list. Disabling the **Show All Entitlements** toggle allows you to hide the entitlements that are not applicable to the network function you are creating or editing.

---

7

Allocate entitlements to the network function.

In the **Consumed** column of the **Entitlements** table, adjust the number of entitlements in one of the following ways:

- Choose “0” or “1” from the drop-down menu.
- Enter a value that does not exceed the remaining entitlements.

**i** **Note:** Creating the network function may result in an over-allocation of one or more entitlements. If the over-allocation of any single entitlement exceeds the amount configured in your network pool key, you will receive an error message and the network function is not created. You must either free up the listed entitlements from another network function, or order additional resources from Nokia.

---

8

Click **Add**.

---

END OF STEPS

---


### 4.3 How do I copy an existing network function?

You can define a network function based on an existing defined network function. All properties and entitlement allocations of the original network function are copied except for: **Name**, **UID** and the **UUID(s)**. Changes made to an entitlement allocation in the original network function after you complete the following procedure are not copied.

1 \_\_\_\_\_

Using the main menu, navigate to **Centralized License Manager, Network Functions**.

2 \_\_\_\_\_

Click on a network function from the list that you want to copy and click  (Table row actions), **Copy**. The **Define Network Function** form opens and is pre-populated with the information from the original network function.

3 \_\_\_\_\_

Edit the properties and entitlement allocations, as required, and click **Define**.

**END OF STEPS** \_\_\_\_\_

### 4.4 How do I bulk copy network functions?

Use this procedure to bulk copy multiple network functions based on an existing reference network function.

1 \_\_\_\_\_

Create a reference network function that allocates the common entitlements that you want to bulk copy to new network functions. See [4.2 "How do I add a network function?"](#) (p. 21).

2 \_\_\_\_\_

Create a CSV text file that contains a list of network functions with the following information:

- UID
- Name
- CLI credentials (only if different from the referenced network function)

The CSV must have a format of:

**Name, UID, Username, Password\n**

**<Name>, <UID>, [Username1], [Password1]\n**

**...**

**<Name>, <UIDN>, [UsernameN], [PasswordN]\n**

The lines can be terminated with \n or \r\n.

---

The Username and Password fields are optional. If they are not present, the values from the referenced network function are used. If an optional field is not present, it can be left empty (,,) or with white space (, ,). If there are no optional fields, then they can be omitted. For example, the following is a valid line.

**Name ,UID\n**

**3** \_\_\_\_\_

Using the main menu, navigate to **Centralized License Manager, Network Functions**.

**4** \_\_\_\_\_

Click on a network function from the list and then click  (Table row actions), **View Details**.

**5** \_\_\_\_\_

Click **+ Bulk Copy**.

**6** \_\_\_\_\_

Click **Choose File** and upload the CSV file.

**7** \_\_\_\_\_

Choose one of the following options:

- None - no license keys will be generated
- Deploy License Keys - a new license key will be deployed for each new network function.
- Enable Auto-Renewal License Keys - all of the new copied network functions will be auto-renew enabled as they are created.

**8** \_\_\_\_\_

Click **Upload**. A confirmation dialog appears for you to confirm this action.

CLM parses the list, and if successful, creates a new network function for each line in the file.

If an error is returned, no network functions are created. Troubleshoot the error and try again.

**END OF STEPS**

---

#### 4.4.1 Bulk Copy example in CSV format

**Name,UID, Username, Password**

**Name1,UID1**

**Name2,UID2, user, password**

**Name3,UID3**



---

## 4.5 How do I view network functions?

1

Using the main menu, navigate to **Centralized License Manager, Network Functions**. A list of network functions displays.

Use the column headings to sort the network functions, or the column fields to search for a specific network function.

The first column denotes the highest severity notification associated with the network function.

Notifications can be raised on network functions, for example, if:


- CLM cannot connect to the network function
- CLM fails to deploy a license key for a network function

The **License Expiry** column identifies the number of days before the license key will expire. The column will indicate Today or Expired as well.

The **Auto-renewal Status** column indicates if the CLM is automatically generating and deploying new license keys to the network function at periodic intervals.

The **Deployed Status** column identifies if network functions have deployed license keys on their referenced license repository. However, the network function may not actually be using the deployed key. If there are notifications, this may indicate that the network function did not accept the license key.

2

To view the entitlements that have been associated with the network function, click on a network function from the list and then click  (Table row actions), **View Details**.

END OF STEPS

---

## 4.6 How do I edit a network function?



**Note:** Editing a network function may result in an over-allocation of one or more entitlements. If the over-allocation of any single entitlement exceeds the amount configured in your network pool key, you receive an error message and the network function changes will not be saved. You must either free up the listed entitlements from another network function, or order additional resources from Nokia.




**Note:** You cannot edit a network function while a license key is being deployed or revoked. You will receive an error message stating that the object is busy and that you should re-try the operation.

1

Using the main menu, navigate to **Centralized License Manager, Network Functions**.

2

Click on a network function from the list that you want to modify and click  (Table row actions), **Edit**. The **Edit Network Function** form opens.

---

3


To change the release of the network function that you want to edit, click **Change Release**. The **Change Release** dialog box opens. Select a release and click **Apply**. The dialog box closes.


---

4

Modify the parameters, as required.

Fetching the UUID, which auto-populates the UUID parameter(s), is only required if you are generating and downloading license keys. If you close the Edit Network Function form when the CLM is retrieving the UUID(s), the process is cancelled.

 **Note:** If you populate the UUID parameter(s) for a network function and if any one or both UUIDs do not match the network function, deployment will fail.

 **Note:** If a network function has a deployed license key, one of the following occurs:

- If you changed the UUID(s) of the network function, the existing license key is revoked.
- If you changed which license repository the network function references, the license key is removed from the original license repository and a new license key is deployed to the new license repository.
- If you set the referenced license repository to 'none' the CLM revokes the license key from the original license repository.

---

5

Apply one or more product standard templates, as required.

Certain network functions (for example, VSR-I) support standard sets of functionality that can be applied when creating or editing a network function. If a product supports the product standard templates, the **Apply Templates** button is enabled.

- Click **Apply Templates**.
- Select one or more product templates to apply.
- Select "Replace all existing entitlements" before applying the template(s).
- Click **Apply**.

---

6


Filter the entitlements, as required.

By default, all (licensed and unlicensed) entitlements are shown in the list. Disabling the **Show All Entitlements** toggle allows you to hide the entitlements that are not applicable to the network function you are creating or editing.

---


7

Edit or assign new entitlements to the network function.

 **Note:** The **Save** button is enabled after you either press enter or click anywhere on the page to confirm the change.

---

If you remove or reduce an existing entitlement from a network function, a dialog box opens, confirming that you want to save the changes.

 **Note:** Certain network functions require that you apply configuration changes to them before deploying a new license key that reduces functionality. Consult the network functions operator guide.

8

---

Click **Save** to save your changes to the network function, or cancel the operation by clicking **X** in the upper right-hand corner of the edit form.

Changing the functionality of a network function may require a network function reboot for the new functionality to become active. The warning message returned by CLM will indicate if a reboot of the network function is required.

END OF STEPS

---

## 4.7 How do I upgrade a network function to a new major release?

When you want to upgrade a network function to a new major release with new features, and ensure seamless operation of the network function, you must first update the network function in CLM prior to the software upgrade.

1

---

To upgrade an existing network function to a new major software release, you must first obtain and upload a new network pool key from your Nokia NSP product representative that supports the product release into your CLM.

See [2.2 “How do I obtain a network pool key?” \(p. 12\)](#) and [2.3 “How do I upload a network pool key?” \(p. 12\)](#).

2

---

Change the release of the network function and edit or assign new entitlements. The displayed entitlements are valid for the new release.

For information about editing a network function, see [4.6 “How do I edit a network function?” \(p. 25\)](#).

3

---

Deploy a new license key file. The file will contain license keys for the network function releases supported by the network pool key.

See [4.11 “How do I manually generate and deploy a license key?” \(p. 29\)](#).

4

---

Upgrade the network function software to the new release.

---

See the appropriate node documentation.

END OF STEPS

---

## 4.8 How do I upgrade a network function to a new minor release?

When a new minor release of the network function software contains new entitlements that you want to use, perform this procedure to enable CLM to generate a license key that contains the new entitlements.

1

To upgrade an existing network function to a new minor software release, you may be required to first obtain and upload a new network pool key from your Nokia NSP product representative that supports the product release into your CLM.

See [2.2 “How do I obtain a network pool key?” \(p. 12\)](#) and [2.3 “How do I upload a network pool key?” \(p. 12\)](#).

2

Upgrade the network function software to the new minor release. The new network function minor release is able to operate with the existing network function license key.

3

Edit the network function and enable any of the new entitlements added in the minor release. See [4.6 “How do I edit a network function?” \(p. 25\)](#).

4

Deploy the new license key file.

See [4.11 “How do I manually generate and deploy a license key?” \(p. 29\)](#).

END OF STEPS


---

## 4.9 How do I view an event log for a specific network function?

1

Using the main menu, navigate to **Centralized License Manager, Network Functions**.

2

Click on the network function from the list for which you want to view an event log, and click  (Table row actions), **View Event Log**.

The Event Log lists all events that have occurred on the specified network function, including the date of each change and the user that applied each change.

END OF STEPS


---

## 4.10 How do I delete a network function?

You can delete a network function when it is no longer needed. Deleting a network function releases any entitlements assigned to it back to the pool of available entitlements.

If the network function you are deleting has a deployed license key, the CLM revokes the key from the license repository referenced by the network function.

1 \_\_\_\_\_  
Using the main menu, navigate to **Centralized License Manager, Network Functions**.

2 \_\_\_\_\_  
Click on a network function from the list that you want to delete and click  (Table row actions), **Delete**.  
A confirmation dialog box opens.


3 \_\_\_\_\_  
Click **Delete**.

END OF STEPS \_\_\_\_\_


## 4.11 How do I manually generate and deploy a license key?

### 4.11.1 Pre-requisite

- **Perform automated license key deployment?** is set to *true* in the network pool key details. To view details in the info panel, select the pool key in the **Network Pool Keys** view.

 **Note:** By default, this functionality is disabled. Contact your Nokia representative about how to enable this functionality.

The duration of any license manually generated and deployed is given by the **Manual License Key Duration in Days** of the network pool key details in the info panel.

 **Note:** Changing the functionality of a network function may require a network function reboot for the new functionality to become active. The CLM does not automatically reboot the network function.



### 4.11.2 Deployment steps for VSR-I/7x50 SR

Deploying a license key to the VSR-I/7x50 network functions consists of the following steps.

Step	Description
Validate connection	CLM will validate that it can connect to the network function using the UID and CLI credentials.

Step	Description
Check UUID	CLM will validate that all UUIDs of the network function match those as reported by the network function. If the network function UUID is not filled in, CLM will attempt to connect to the network function and populate the UUID field with the correct value from the network function. Otherwise, you can use CLI to look up the corresponding value on the network function. See the appropriate node documentation. <b>NOTE:</b> The UUID field corresponds to the Chassis Serial # for 7x50 SR.
Generate license key	CLM generates a unique license key file for the selected network function.
Upload license key to CLR	CLM places the license key file onto the license repository referenced by the network function. <b>NOTE:</b> For 7x50 SR/XRS network functions, the preferred method of license key storage is local storage on the 7x50 SR/XRS.
Activate license	CLM sets the network function to reference the license key file. For example, for a VSR-I, the BOF is set to reference the location of the license key file on the license repository

### 4.11.3 Procedure

- 1 \_\_\_\_\_  
Using the main menu, navigate to **Centralized License Manager, Network Functions**.
- 2 \_\_\_\_\_  
Click on a network function for which you want to deploy a license key and click  (Table row actions), **Deploy License Key**.  
A confirmation dialog box opens.
- 3 \_\_\_\_\_  
Click **Deploy**.  
The deploy license key operation is asynchronous and may take a few minutes depending on your network performance. Clicking  updates the data in the network function grid.  
The **Deployed Status** column of the network function grid indicates that the license key file has been deployed to the license repository. After deploying a license key:

- If the network function is not marked as Deployed, there will be notifications raised about problems communicating with the referenced license repository.
- If the network function is marked as Deployed, but there are notifications raised against it, the network function is not configured to use the new license key.

If a deploy operation fails, CLM raises a notification with the step, the CLI command CLM sent, and the CLI response received. You must address the problem indicated in the notification, and then choose the deploy license key operation again.

END OF STEPS

---

## 4.12 What does revoking a license key mean?

Revoking license keys is the process of removing the current license key for the network function from the license repository.

**i** **Note:** When the CLM revokes a license key, it only removes the license key file from the FTP server or network function local storage. It does not remove the reference to the license key from the BOF of the network function. This is done to ensure the network function remains functional for as long as the previous license was valid for, or until the network function is rebooted.

## 4.13 How do I revoke a license key?

1

---

Using the main menu, navigate to **Centralized License Manager, Network Functions**.

2

---

Click on a network function for which you want to revoke a license key and click **⋮** (Table row actions), **Revoke License Key**.

A confirmation dialog box opens.

3

---

Click **Revoke**.

END OF STEPS

---

## 4.14 How do I enable license key auto-renewal?

By enabling license key auto-renewal for a network function, the CLM will automatically generate and deploy license keys to the network function.

**i** **Note:** This functionality is not required for 7x50 SR/XRS network functions.

**i** **Note:** If you change the entitlements for a network function that has auto-renewal enabled, a new license key is not automatically generated when you save your edits. You must manually

---

deploy a new license key, and potentially restart the network function for the changed entitlements to take effect. If you do not perform this process, the network function may never apply your changes.

#### 4.14.1 Pre-requisite

- **Perform automated license key deployment?** is set to *true* in the network pool key details. To view details in the info panel, select the pool key in the **Network Pool Keys** view.

**i** **Note:** By default, this functionality is disabled. Contact your Nokia representative about how to enable this functionality.

The duration of an auto-renewal key is displayed by the **Auto-renewal License Key Duration in Days** of the network pool key details in the info panel.

#### 4.14.2 Procedure


1

---

Using the main menu, navigate to **Centralized License Manager, Network Functions**.

2

---

Click on a network function for which you want to configure automated license key deployment and click  (Table row actions), **Enable License Key Renewal**. A confirmation dialog box opens.

3

---

Click **Enable**.

The Auto-renewal Status column displays the new managed state.

The CLM attempts to generate a license key, deploy the license key to the appropriate license repository, and then set the BOF of the network function to use the new license key.

4

---

When a network function is first set to the auto-renewal managed state, you may be required to reboot the network function before it will use the new license key.

When subsequent license keys are automatically generated by the auto-renewal process, the network function does not need to be rebooted on installation of the new license key as long as you have not changed any entitlements (see Note at the beginning of this topic).

After enabling license key renewals:

- If errors are encountered during the deployment, notifications are raised.
- If an auto-renewal network function has notifications, at periodic intervals the CLM still attempts to generate and deploy a new license key to the network function to ensure the network function always has a valid license key. Once the problems that are causing the notification are resolved, the CLM will successfully deploy a new license key.

See [4.11 “How do I manually generate and deploy a license key?”](#) (p. 29) for information about the deployment steps and possible failure reasons.



---

**i** **Note:** If the CLM is reporting the 'LICENSE\_KEY\_DEPLOY\_NOT\_SET\_SR' notification for an auto-renewal network function, it means the BOF of the 7x50 SR/XRS network function is not pointing to the license key file CLM thinks it should, which could be caused by such things as:

- Rejected deploy due to Version mismatch
- An operator changing the BOF

If you encounter this notification for a network function, correct the BOF with the license file that has been deployed.

Select the 'Deploy License Key' option for the network function you had the original problem with.

These actions will cause the CLM to immediately generate and deploy a new license key to the network function. If the network function accepts the new license key, the notifications will disappear and the normal CLM auto-renewal process will resume.

END OF STEPS

---

## 4.15 How do I disable license key auto-renewal?

**i** **Note:** This functionality is not required for 7x50 SR/XRS network functions.

1

Using the main menu, navigate to **Centralized License Manager, Network Functions**.

2

Click on a network function for which you want to disable automated license key deployment and click **⋮** (Table row actions), **Disable License Key Renewal**. A confirmation dialog box opens.

3

Click **Disable**.

The Auto-renewal Status column no longer displays the network function as having auto-renewal enabled.

The CLM no longer auto-generates license keys for the network function. When a network function has auto-renewal disabled, the CLM leaves the existing license key on the license repository and set in the BOF of the network function.

END OF STEPS

---


## 4.16 How do I generate and download license keys?


**i** **Note:** This functionality is not required for 7x50 SR/XRS network functions.

The pool key associated with the network function may have permission to enable you to generate and download a license key file for a network function. If these permissions are present, the

---

**Perform license key generation and download?** value of the pool key details is set to *true*. To view details in the info panel, select the pool key in the **Network Pool Keys** view.

 **Note:** By default, this functionality is disabled. Contact your Nokia representative about how to enable this functionality.

 **Note:** The pool key would allow license download if specified during the network pool key acquisition process. Contact your Nokia representative to request a network pool key with permission to generate license key and download it.

When generating and downloading license keys, you must supply UUID(s) for the network function. Fetching the UUID auto-populates the UUID parameter(s).

1 \_\_\_\_\_

Using the main menu, navigate to **Centralized License Manager, Network Functions**.

2 \_\_\_\_\_

Click on a network function for which you want to generate and download a license key and click  (Table row actions), **Generate and Download License Key**.

Your browser downloads the license key file.

**END OF STEPS** \_\_\_\_\_


## 5 Notifications and events

### 5.1 Overview

Notifications alert an operator of configuration error of license repository, failed license deployment, or expiration of the pool key. Notifications are generated automatically by the CLM, and they are cleared when the condition has cleared.

**i** **Note:** Alarms related to the NSP Routing key are only generated in CLM integrated with NSP.

### 5.2 How do I sort or filter notifications?

- 1 \_\_\_\_\_  
Using the main menu, navigate to **Centralized License Manager, Notifications**. A list of notifications displays.
- 2 \_\_\_\_\_  
To sort or filter the notifications, use the column headings.
  - To sort, click on the column heading. The sort icon  appears, and the list of events is sorted by that column.
  - To filter, enter text in **Source Name**, **Type**, or **Message** text boxes. Only items that match the text in the filter text box are shown in the list.
  - To clear filters, remove the text from the filter text box.
- 3 \_\_\_\_\_  
You can also see notification icons on the Network Pool Key summary view list when thresholds are close to, or exceeding, thresholds.

END OF STEPS \_\_\_\_\_

### 5.3 What does this notification mean?

CLM Notification	Description
ENTITLEMENT_RESOURCE_ALERT	A specific entitlement is nearing, or has exceeded, its available allotment. When the allocation for an entitlement has been exceeded, CLM will not grant any more of the entitlement.

CLM Notification	Description
FAILED_CREATION_OF_NF_TEMP_LICENSE	CLM could not generate the temporary license key for a specific network function. The network function details are in the message. Try to manually regenerate a license key for the network function to troubleshoot why CLM cannot deploy a license key to the network function.
LICENSE_KEY_DEPLOY_FAILURE	The CLM failed to deploy a license key to the given network function during the given deployment step.
LICENSE_KEY_DEPLOY_NOT_ON_CLR	The CLM detected that a deployed license key that is in use by a network function is missing from the CLR. In the case of a 7x50 SR/XRS, if the network function reboots it will not find its license file. This is usually due to the accidental deletion of the file by another system. To rectify, you can manually deploy a new license key to the network function.
LICENSE_KEY_DEPLOY_NOT_SET_SR	The CLM found that the actual BOF license string on the 7x50 SR/XRS does not match the license file that the CLM has set. This can be caused by another system/operator changing the BOF after the CLM has deployed a license key. To clear this error, you can manually deploy a new license key to the 7x50 SR/XRS.
LICENSE_KEY_EXPIRY	The license key that is deployed on the specified network function is nearing or has expired. To rectify, manually deploy a new license key to the network function.
LICENSE_REPO_PATH_ERROR	There was an error accessing or creating the specific initial directory for the given license repository. Check that the directory is valid and that the specified user has permissions to read, write, and create directories on the license repository.
LICENSE_REPOSITORY_PROBLEM	There was a problem when communicating with the specific license repository. The parameters describe the cause of the error (i.e. TIMEOUT, AUTHENTICATION, etc.)

CLM Notification	Description
NF_COMMUNICATIONS_ERROR	The CLM is not able to communicate with the specific network function. The reason for the error is included in the notification (for example, TIMEOUT, AUTHENTICATION, etc.).
NF_CONFIGURATION_ERROR	The specified network function has an invalid configuration defined in the CLM which is preventing the CLM from deploying a license key. This is usually caused by the network function having a UUID defined in the CLM that is different from the actual UUID.
NF_REDUNDANCY_NOT_SET	The CLM detected that for a 7x50 SR/XRS node, standby is enabled but boot config redundancy is not set. To rectify, enable boot redundancy on the node.
NSP_LICENSE_KEY_NOT_FOUND	The NSP Routing license key is either missing or incompatible with the current NSP version. This alarm appears once every 2 hours. <b>Note:</b> This alarm only occurs for CLM integrated with NSP.
POOL_KEY_NEAR_EXPIRY	<p><b>Network pool keys</b></p> <p>The network pool license key is nearing expiry.</p> <p>This alarm appears once every 2 hours. Obtain a new network pool license key from Nokia.</p> <p><b>NSP Routing key</b></p> <p><b>Note:</b> This is only applicable for CLM integrated with NSP.</p> <p>The licence for the NSP Routing key is nearing expiry.</p> <p>This alarm appears once every 24 hours and has the following severities:</p> <ul style="list-style-type: none"> <li>• minor - alarm is issued daily, starting 180 prior to expiration</li> <li>• major - alarm is issued daily, starting 90 days prior to expiration</li> <li>• critical - alarm is issued daily, starting 7 days prior to expiration</li> </ul>

CLM Notification	Description
POOL_KEY_EXPIRED	The pool license key expiry date has passed. The pool key is no longer valid and you can no longer define new network functions or generate license keys. For network pool keys, this alarm appears once every 2 hours. For NSP Routing key, this alarm appears once every 24 hours. Obtain a new pool license key from Nokia.
POOL_KEY_REQUIRES_APP_UPDATE	The network pool license key supports a network function version that is not supported by the version of your CLM instance. You can still use the network pool license key, but you will not be able to define network functions for the unsupported versions. Upgrade your CLM installation if you need to use the newer network function versions.

## 5.4 How do I configure notification thresholds?

Perform this procedure to set thresholds for the percentage usage of an entitlement. For example, if you set the Warning Threshold to 75, the CLM raises a warning when an entitlement is 75% used.


- 1 \_\_\_\_\_  
Using the main menu, navigate to **Centralized License Manager, Configurations**. Then click **Notification Thresholds**.
- 2 \_\_\_\_\_  
Configure the parameters and click **Save**.

END OF STEPS \_\_\_\_\_

## 5.5 How do I view the events history?

Events provide a log of operations on CLM, listing all significant operator-initiated actions. It could be used as an audit log. After a year, events are deleted from the CLM.

- 1 \_\_\_\_\_  
Using the main menu, navigate to **Centralized License Manager, Events**. A list of events displays.
- 2 \_\_\_\_\_  
To sort or filter the events, use the column headings,

- 
- To sort, click on the column heading. The sort icon  appears, and the list of events is sorted by that column.
  - To filter, enter text in the **Type** or **Source ID** filter text box. Only events that match the text in the filter text box are shown in the list.
  - Clear filters by removing the text from the filter text box.

END OF STEPS

---

## 5.6 How do I view log details for an event?


1

---

Using the main menu, navigate to **Centralized License Manager, Events**. A list of events displays.

2

---

To view more details for an event, hover over the event and click  (Log Detail).

The **Event Info** dialog box opens, displaying information that includes, for instance, Properties, UUIDs, or associated pool keys.

3

---

Click **Close** when done.

The **Event Info** dialog box closes.

END OF STEPS

---





## 6 CLI commands

### 6.1 Overview

CLM uses the classic CLI engine for VSR-I and 7x50 SR/XRS network functions. CLM also uses the model-driven CLI engine for 7x50 SR/XRS, Release 20.10 and later. CLM auto-detects the correct CLI engine to use.

### 6.2 CLI classic commands

The following table lists the CLI classic commands used by the CLI user specified for each network function.

Table 6-1 CLI classic commands support

CLI classic command	VSR-I	7x50 SR/XRS
admin system license activate	✓	✓
admin system license validate		✓
bof license-file	✓	✓
bof save	✓	✓
environment no more	✓	✓
show bof	✓	✓
show redundancy synchronization		✓
show system information	✓	✓
show system license	✓	✓

### 6.3 Model-driven CLI commands

The following list of model-driven commands are used for 7x50 SR/XRS, Release 20.10 and later.

- // — to switch the CLI engine
  - This command is used depending on the current Model Interface Configuration Mode (MICM) used by the 7x50 SR/XRS, and the default CLI engine of the user entered in the connection properties of the network function. The switch CLI engine command is executed if:
    - The MICM is classic, but the default CLI engine is md-cli
    - The MICM is model-driven, but the default CLI engine is classic-cli
- admin show configuration bof json
- admin system license activate
- bof exclusive

- 
- commit
  - discard
  - environment more false
  - exit
  - license primary-location
  - show redundancy synchronization
  - show system information
  - show system license

---

## 7 CLM backup and restore

### 7.1 Overview

This chapter describes the procedures that must be performed in order to preserve crucial system data in the case of a catastrophic failure.

### 7.2 How do I back up the CLM deployer host?

#### 7.2.1 Purpose

Perform the following steps to back up the CLM deployer host in a CLM cluster. A CLM deployer host backup is crucial for the recovery of the CLM deployer host in the event of a failure.

**i** **Note:** The steps describe how to back up a CLM deployer host in a KVM virtualization environment; for OpenStack or VMware ESXi, see the RHEL or VMware documentation for information about how to restore a VM.

#### 7.2.2 Steps

- 1 \_\_\_\_\_  
Log in as the root user on the station that hosts the CLM deployer host VM.
- 2 \_\_\_\_\_  
Open a console window.
- 3 \_\_\_\_\_  
Enter the following to stop the VM:  

```
# virsh destroy VM ↵
```

where *VM* is the VM name
- 4 \_\_\_\_\_  
Enter the following to convert the CLM deployer host VM image in qcow2 format to conserve disk space:  

```
# qemu-img convert -f raw -O qcow2 sparse_current_image raw_backup_image.qcow2 ↵
```

where  
*sparse\_current\_image* is the name of the current VM image in sparse format  
*raw\_backup\_image* is the name to assign to the backup VM image in raw format
- 5 \_\_\_\_\_  
Enter the following to start the VM:

---

```
# virsh start VM ↵
```

where *VM* is the VM name  
The VM starts.

6 \_\_\_\_\_  
Store the *raw\_backup\_image.qcow2* file in a location separate from the CLM system and preferably in a remote facility.

7 \_\_\_\_\_  
Close the open console windows.

END OF STEPS \_\_\_\_\_

## 7.3 How do I restore the CLM deployer host?

### 7.3.1 Purpose

The following steps describe how to restore the CLM deployer host in a CLM cluster, for example, if the deployer host VM fails and must be recreated.

**i** **Note:** The steps describe how to restore a CLM deployer host in a KVM virtualization environment; for OpenStack or VMware ESXi, see the RHEL or VMware documentation for information about how to restore a VM.

**i** **Note:** In order to perform the procedure, you require a backup of the CLM deployer host configuration. A backup is created during CLM system deployment or reconfiguration, and also by performing [7.2 “How do I back up the CLM deployer host?”](#) (p. 43).

### 7.3.2 Steps

1 \_\_\_\_\_  
Log in as the root user on the station that hosts the CLM deployer host VM.

2 \_\_\_\_\_  
Open a console window.

3 \_\_\_\_\_  
Create a temporary local directory.

**i** **Note:** The directory must be empty.

4 \_\_\_\_\_  
Enter the following:

```
# cd directory ↵
```

---

where *directory* is the temporary directory created in [Step 3](#).

5

---

Copy the CLM deployer host backup file set to the temporary directory.

6

---

Enter the following to convert the backup CLM deployer host qcow2 image to raw format:

```
# qemu-img convert -f qcow2 backup_image.qcow2 -O raw new_image.img ↵
```

where

*backup\_image* is the backup image file name

*new\_image* is a name to assign to the new image file

7

---

If the CLM deployer host is running, enter the following to stop the VM:


```
# virsh destroy VM ↵
```

where *VM* is the VM name

8

---

Enter the following to deploy the VM:

 **Note:** One “--network bridge=*bridge\_name*” entry is required for each VM interface that you intend to configure.

```
# virt-install --connect qemu:///system --ram RAM --vcpu=vCPUs -n instance --os-type=linux --os-variant=rhel7 --disk path="new_image", device=disk,bus=virtio,format=raw,io=native,cache=none --network bridge=bridge_name --import & ↵
```

where

*RAM* is the required amount of VM RAM in Mbytes; for example, 64 Gbytes is expressed as 65536, which is 64 x 1024 Mbytes

*vCPUs* is the required number of vCPU threads

*instance* is the name to assign to the VM

*new\_image* is the name of the disk image created in [Step 6](#)

*bridge\_name* is the name of the network bridge for a VM interface

9

---

When the VM creation is complete, enter the following:

```
# virsh domiflist deployer_host | awk '{print $5}' ↵
```

where *deployer\_host* is the instance name assigned to the VM

The CLM deployer host MAC address is displayed.

- 
- 10** \_\_\_\_\_  
Record the MAC address for use in a later step.
- 11** \_\_\_\_\_  
Enter the following to open a console session as the root user on the CLM deployer host:  
`# virsh console deployer_host ↵`
- 12** \_\_\_\_\_  
Open the following file with a plain-text editor such as vi:  
`/etc/sysconfig/network-scripts/ifcfg-ethn`  
where  
*n* is the Ethernet interface number; for example, eth0 is the first interface
- 13** \_\_\_\_\_  
Edit the following line as shown below:  
`HWADDR=MAC_address`  
where *MAC\_address* is MAC address recorded in [Step 9](#)
- 14** \_\_\_\_\_  
Save and close the file.
- 15** \_\_\_\_\_  
Enter the following:  
`# init 6 ↵`  
The CLM deployer host station reboots, and the CLM deployer host is restored.
- 16** \_\_\_\_\_  
Close the console window.
- END OF STEPS** \_\_\_\_\_

## 7.4 How do I check CLM database synchronization?

### 7.4.1 Purpose

Perform this procedure to check the synchronization status of the database instances in the redundant CLM clusters of a DR deployment. You can check the synchronization status from the CLM UI, or using a CLI.

---

## 7.4.2 Steps

### Check database synchronization from the CLM UI

1

As a CLM administrator, choose **System Health** from the main menu.

2

View the information in the **Database Synchronization Status** tile, which lists the synchronization completion percentage for postgres—PostgreSQL database.

To view expanded details for the database listed on the tile, click , **Expand size**.

END OF STEPS

---

## 7.4.3 Steps

### Check database synchronization using a CLI

1

Log in as the root or CLM admin user on the CLM cluster host in the primary data center.

2

Open a console window.

3

Enter the following:

```
# kubectl exec -n $(kubectl get pods -A | awk '/nspos-asm/ {print $1;exit}') -it $(kubectl get pods -A | awk '/nspos-asm/ {print $2;exit}') -c nspos-asm-app -- /opt/nsp/os/asm/bin/report.py ↵
```

4

Database synchronization data is returned in the following format:

```
{
  "message": "Data retrieved",
  "data":
  [
    {
      "dcName": "string",
      "dbName": "string", // postgres|neo4j
      "podName": "string",
```

---

```
"role": "string", // PRIMARY|STANDBY for postgres,
LEADER|FOLLOWER|READ_REPLICA for neo4j
"activeSize": "string",
"sizeUnit": "string", // Bytes for postgres, Commits for neo4j
"isInRecovery": null, // or boolean for postgres
"isReplayPaused": null, // or boolean for postgres
"receivedSize": null, // or string for postgres
"replaySize": null, // or string for non primary/leader instances
"lastReplayTimeStamp": null, // or timestamp string for postgres
"missingSize": null, // or string for non primary pg instances
"dataToTransfer": null, // or string for non primary pg instances
"dataToProcess": null, // or string for non primary/leader instances
"syncPercentage": double // real number 0-100
},
],
"status": "success"
}
```

5 \_\_\_\_\_  
Review the information.

6 \_\_\_\_\_  
Close the console window.

END OF STEPS \_\_\_\_\_

## 7.5 How do I configure scheduled CLM backups?

### 7.5.1 Purpose

Perform this procedure to configure scheduled backups of the following CLM cluster databases:

- Kubernetes etcd data
- PostgreSQL

Scheduled backups are enabled by default, and scheduled to run daily at 12:30 AM UTC.

**i** **Note:** By default, the CLM retains the three most recent scheduled backups.

**i** **Note:** *release-ID* in a file path has the following format:

*R.r.p-rel.version*

where

*R.r.p* is the CLM release, in the form *MAJOR.minor.patch*



---

*version* is a numeric value

## 7.5.2 Steps

- 1 \_\_\_\_\_  
Log in as the root or CLM admin user on the CLM deployer host.
- 2 \_\_\_\_\_  
Open the following file with a plain-text editor such as vi:  
`/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/config/nsp-config.yml`
- 3 \_\_\_\_\_  
Locate the section that begins with the following:  

```
backups:
```
- 4 \_\_\_\_\_  
Configure the following parameters:  
**i** **Note:** If the schedule value is an empty string, no scheduled backup is performed.  
**i** **Note:** See the RHEL cron man page for information about defining a crontab schedule.  

```
schedule: "definition"  
retained: n
```

where  
*definition* is a UNIX crontab schedule definition; for example, "30 0 \* \* \*" specifies the default backup schedule of 12:30 a.m. daily  
*n* is the number of backups to retain
- 5 \_\_\_\_\_  
Save and close the file.

END OF STEPS \_\_\_\_\_

## 7.6 How do I back up the CLM cluster databases?

### 7.6.1 Purpose

Perform this procedure to manually create a backup of one or more of the following in a CLM cluster:

- Kubernetes etcd data
- CLM Kubernetes secrets
- PostgreSQL

---

**i** **Note:** *release-ID* in a file path has the following format:

*R.r.p-rel.version*

where

*R.r.p* is the CLM release, in the form *MAJOR.minor.patch*

*version* is a numeric value

## 7.6.2 Steps

1

Log in as the root or CLM admin user on the CLM deployer host.

2

Open a console window.

3

If a common backup storage location is defined in the CLM configuration, go to [Step 7](#).

4

Open the following file with a plain-text editor such as vi:

```
/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/config/nsp-config.yml
```

5

If required, configure the backups to be stored on an NFS server.

1. Locate the section that begins with the following:

```
backups:
```

2. Configure the following parameters in the following subsection:

```
nfs:
  server: "server"
  path: "path"
```

where

*server* is the NFS server IP address

*path* is the path of the exported file system on the server

6

If you made any changes to the `nsp-config.yml` file in [Step 5](#), enter the following to apply the changes to the cluster:



**Note:** If the CLM cluster VMs do not have the required SSH key, you must include the `--ask-pass` argument in the `nspdeployerctl` command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:

```
nspdeployerctl --ask-pass install --config --deploy
```

---

```
# /opt/nsp/NSP-CN-DEP-release-ID/bin/nspdeployerctl install --config  
--deploy ↵
```

7

Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/database ↵
```

8

Enter one or more of the following, as required, to back up system data and databases:

**i** **Note:** It is recommended that you back up all system data and databases.

**i** **Note:** You must not proceed to the next step until each backup job is complete.

a. To back up the CLM Kubernetes etcd data:

```
# ./nspos-db-backup-k8s.sh nsp-etcd backup_dir ↵
```

b. To back up the CLM PostgreSQL database:

```
# ./nspos-db-backup-k8s.sh nspos-postgresql backup_dir ↵
```

where *backup\_dir* is the directory in which to store the backup

The backup script displays messages like the following as a backup job proceeds:

```
----- BEGIN : Backing up database-backup -----  
job.batch/backup_job created  
timestamp LOG: Waiting for job backup_job at namespace namespace to  
finish...  
timestamp LOG: backup done successfully  
timestamp LOG: Removing job backup_job at namespace namespace  
job.batch "backup_job" deleted  
timestamp LOG: Job backup_job at namespace namespace deleted  
----- END : Backing up database_backup -----  
----- BEGIN : Fetching backup database -----  
timestamp LOG: Fetching database backup from pod nsp-backup-storage-0  
at namespace namespace  
timestamp LOG: Latest database backup is database_backup_timestamp.  
tar.gz  
tar: removing leading '/' from member names  
timestamp LOG: Latest database backup fetched successfully  
----- END : Fetching backup database -----
```

A backup filename has the following format:

```
database_backup_timestamp.tar.gz
```

where

---

*database* is the database name, for example, nspos-neo4j  
*timestamp* is the start time of the database backup

## Safeguard backup files

9

Transfer the files in *backup\_dir* to a secure location for safekeeping.



**Note:** It is strongly recommended that you transfer each backup file to a secure facility that is outside the local data center.

10

Close the console window.

END OF STEPS

---

## 7.7 How do I restore the Kubernetes etcd data in a CLM cluster?

### 7.7.1 Purpose



#### CAUTION

#### System Data Corruption

*Attempting to restore the etcd data from one CLM cluster to a different CLM cluster causes the restore to fail, and renders the CLM cluster unrecoverable.*

*You must restore only an etcd data backup from the same CLM cluster; you cannot move a CLM cluster configuration to a different cluster, or restore a cluster configuration in a new cluster.*

An etcd data backup, called a snapshot, captures all Kubernetes objects and associated critical information. A scheduled etcd data snapshot is performed daily. The following procedure describes how to recover a failed CLM cluster by restoring the etcd data from a snapshot.

### 7.7.2 Steps

#### Obtain and distribute snapshot

1

Log in as the root or CLM admin user on the CLM cluster host.

2

Enter the following to identify the namespace of the nsp-backup-storage pod:

```
# kubectl get pods -A | grep nsp-backup ↵
```

---

The leftmost entry in the output line is the namespace, which in the following example is nsp-psa-restricted:

```
nsp-psa-restricted    nsp-backup-storage-0    1/1    Running    0    5h16m
```

3

---

Record the namespace value.

4

---

Enter the following to identify the etcd snapshot to restore:

```
# kubectl exec -n namespace nsp-backup-storage-0 - ls -la /tmp/backups/nsp-etcd/ ↵
```

where *namespace* is the namespace value recorded in [Step 3](#)

The directory contents are listed; the filename format of an etcd snapshot is:

```
nsp-etcd_backup_timestamp.tar.gz
```

where *timestamp* is the snapshot creation time

5

---

Record the name of the snapshot file that you need to restore.

6

---

Enter the following to copy the snapshot file from the backup pod to an empty directory on the local file system:

```
# kubectl cp namespace/nsp-backup-storage-0: /tmp/backups/nsp-etcd/snapshot_file_path/snapshot_file ↵
```

where

*namespace* is the namespace value recorded in [Step 3](#)

*path* is an empty local directory

*snapshot\_file* is the snapshot file name recorded in [Step 5](#)

7

---

Enter the following:

**i** **Note:** The file lists either one member, or three, depending on the deployment type.

```
# grep ETCD_INITIAL /etc/etcd.env ↵
```

Output like the following is displayed.

```
ETCD_INITIAL_ADVERTISE_PEER_URLS=https://local_address:port
```

```
ETCD_INITIAL_CLUSTER_STATE=existing
```

```
ETCD_INITIAL_CLUSTER_TOKEN=k8s_etcd
```

```
ETCD_INITIAL_CLUSTER=etcd1=https://address_1:port,etcd2=https://address_2:port,etcd3=https://address_3:port
```

---

where  
*local\_address* is the IP address of the etcd cluster member you are operating from  
*address\_1*, *address\_2*, and *address\_3* are the addresses of all etcd cluster members  
*port* is a port number

8 

---

 Perform the following on each etcd cluster member.

**i** **Note:** After this step, the etcd cluster is unreachable until the restore is complete.

1. Log in as the root or CLM admin user.
2. Enter the following:  

```
# systemctl stop etcd ↵
```

The etcd service stops.
3. Transfer the snapshot file obtained in [Step 7](#) to the cluster member.

## Restore database on etcd cluster members

9 

---

 Perform [Step 11](#) to [Step 19](#) on each etcd cluster member.

10 

---

 Go to [Step 20](#).

11 

---

 Log in as the root or CLM admin user.

12 

---

 Navigate to the directory that contains the transferred snapshot file.

13 

---

 Enter the following:  

```
# tar xzf path/nsp-etcd_backup_timestamp.tar.gz ↵
```

where  
*path* is the absolute path of the snapshot file  
*timestamp* is the snapshot creation time  
The snapshot file is uncompressed.

14 

---

 Enter the following:  

```
# ETCDCCTL_API=3 etcdctl snapshot restore etcd.db --name member  
--initial-cluster initial_cluster --initial-cluster-token token
```

---

```
--initial-advertise-peer-urls URL ↵
```

where

*member* is the name of the cluster member you are working on, for example, etcd2

*initial\_cluster* is the ETCD\_INITIAL\_CLUSTER list of cluster members recorded in [Step 7](#)

*token* is the ETCD\_INITIAL\_CLUSTER\_TOKEN value recorded in [Step 7](#)

*URL* is the URL of the cluster member you are working on; for example, the etcd2 cluster member URL shown in [Step 7](#) is `https://address_2:port`

The etcd database is restored.

---

15

Enter the following to create a directory in which to store the previous database:

```
# mkdir path/old_etcd_db ↵
```

where *path* is the absolute path of the directory to create

---

16

Enter the following to move the previous database files to the created directory:

```
# mv /var/lib/etcd/* path/old_etcd_db ↵
```

where *path* is the absolute path of the directory created in [Step 15](#)

---

17

Enter the following:

```
# mv ./member.etcd/* /var/lib/etcd/ ↵
```

where *member* is the member name specified in [Step 14](#)

The backup files move to the `/var/lib/etcd` directory.

---

18

Enter the following:

```
# systemctl start etcd ↵
```

The etcd service starts.

---

19

Enter the following:

```
# systemctl status etcd ↵
```

The etcd service status is displayed.

The service is up if the following is displayed:

```
Active: active (running)
```

---

20

When the etcd service is up, close the open console windows.

END OF STEPS

---

## 7.8 How do I restore the CLM cluster databases?

### 7.8.1 Purpose

Perform this procedure to restore one or more of the following in each CLM cluster:

- CLM Kubernetes secrets
- PostgreSQL database

**i** **Note:** If you are performing the procedure as part of a system conversion, migration, or upgrade procedure in a DR deployment, you must perform the procedure only in the new primary CLM cluster.

**i** **Note:** You can specify a local backup file path, or a remote path, if the remote server is reachable from the CLM deployer host and from the CLM cluster host.

To specify a remote path, use the following format for the *backup\_file* parameter in the command, where *user* has access to *backup\_file* at the *server* address:

```
user@server:/backup_file
```

**i** **Note:** If root access for remote operations is disabled in the CLM configuration, remote operations such as SSH and SCP as the root user are not permitted within a CLM cluster. Steps that describe such an operation as the root user must be performed as the designated non-root user with sudoer privileges.

For simplicity, such steps describe only root-user access.

**i** **Note:** *release-ID* in a file path has the following format:

*R.r.p-rel.version*

where

*R.r.p* is the CLM release, in the form *MAJOR.minor.patch*

*version* is a numeric value

### 7.8.2 Steps

#### Prepare to restore databases

1

---

Log in as the root or CLM admin user on the CLM deployer host.

2

---

Open a console window.



---

### 3

If you are restoring the data on new CLM cluster VMs, create and distribute an SSH key for password-free CLM deployer host access to each CLM cluster VM.

1. Enter the following:

```
# ssh-keygen -N "" -f path -t rsa ↵
```

where *path* is the SSH key file path, for example, */home/user/.ssh/id\_rsa*

An SSH key is generated.

2. Enter the following for each CLM cluster VM to distribute the key to the VM.

```
# ssh-copy-id -i key_file user@address ↵
```

where

*user* is the designated CLM ansible user, if root-user access is restricted; otherwise, *user@* is not required

*key\_file* is the SSH key file, for example, */home/user/.ssh/id\_rsa.pub*

*address* is the CLM cluster VM IP address

---

### 4

Perform one of the following.

**i** **Note:** You must not proceed to the next step until the cluster is ready.

- a. If both of the following are true, you must stop each cluster and remove all existing cluster data:

- You are restoring the data in an existing CLM cluster, rather than on new CLM cluster VMs.
- You are restoring all CLM databases.

Perform the following steps on the CLM deployer host in each CLM cluster.

**i** **Note:** In a DR deployment, you must perform the steps first on the standby cluster.

1. Log in as the root or CLM admin user.
2. Open the following file with a plain-text editor such as vi:  
*/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/config/nsp-config.yml*
3. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

```
deleteOnUndeploy:true
```

4. Save and close the file.
5. Enter the following:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

6. Enter the following:

```
# ./nspdeployerctl uninstall --undeploy ↵
```

The CLM cluster is undeployed, and the existing data is removed.

- b. If you are not restoring all databases, you must delete only the existing data in each database that you are restoring.

Perform the following steps on the CLM deployer host in each CLM cluster.

**i** **Note:** In a DR deployment, you must perform the steps first on the CLM cluster that you want to start as the standby cluster.

1. Log in as the root or CLM admin user.
2. Open the following file using a plain-text editor such as vi:  
`/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/config/nsp-config.yml`
3. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

```
deleteOnUndeploy:false
```

4. Save and close the file.
5. On the CLM cluster host, enter the following to determine which node the backup files are on:

```
# kubectl get pods -o wide -A | grep backup | awk '{print $8}' ↵
```

6. Log in on the CLM cluster node where the backup files are.

7. On the node, enter the following for each database that you are restoring:

**Note:** Database instances are dynamically allocated to CLM cluster nodes, so some nodes may not have an instance of a specific database. If a database instance is not present on a node; the command returns an error message that you can safely ignore.

```
# rm -rf /opt/nsp/volumes/db_name/* ↵
```

where *db\_name* is the database name, and is one of:

- nsp-file-service
- nspos-postgresql

## Enable CLM restore mode

5

Enter the following on the CLM deployer host:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

6

Enter the following to enter restore mode:

**i** **Note:** If the CLM cluster VMs do not have the required SSH key, you must include the `--ask-pass` argument in the `nspdeployerctl` command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:

```
nspdeployerctl --ask-pass install --config --restore
```

```
# ./nspdeployerctl install --config --restore ↵
```

---

7

The following CLM cluster pod must be operational before the restore begins:

- `nspos-postgresql-primary-n`


Enter the following periodically to list the pods; the cluster is ready for the restore when each required pod is in the Running state:

```
# kubectl get pods -A ↵
```

---

8

If any required pod is not Running, return to [Step 7](#).

 **Note:** A restore attempt fails unless each required pod is Running.

## Restore data

---

9


Enter the following on the CLM deployer host:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/tools/database ↵
```

---

10

Enter one or more of the following to restore system data and the database:

 **Note:** In a DR deployment, you must perform the steps first in the data center that you want to start as the primary data center.

To restore the CLM PostgreSQL database:

```
# ./nspos-db-restore-k8s.sh nspos-postgresql backup_dir/backup_file ↵
```

where

*backup\_dir* is the directory that contains the backup file


*backup\_file* is the backup file name, for example, for PostgreSQL, the name is `nspos-postgresql_backup_timestamp.tar.gz`


## Start CLM clusters

---

11

Perform the following steps in each data center.

 **Note:** In a DR deployment, you must perform the steps first in the data center that you want to start as the primary data center.

 **Note:** If the CLM cluster VMs do not have the required SSH key, you must include the `--ask-pass` argument in the `nspdeployerctl` command, as shown in the following example, and are subsequently prompted for the root password of each cluster member:

---

```
nspdeployerctl --ask-pass uninstall --undeploy OR nspdeployerctl
--ask-pass uninstall --undeploy
```

1. Log in as the root or CLM admin user on the CLM deployer host.
2. Open a console window.
3. Open the following file with a plain-text editor such as vi:  
`/opt/nsp/NSP-CN-DEP-release-ID/NSP-CN-release-ID/config/nsp-config.yml`
4. Edit the following line in the **platform** section, **kubernetes** subsection to read as shown below:

```
deleteOnUndeploy:false
```

5. Save and close the file.
6. Enter the following:  

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```
7. Enter the following to exit restore mode and terminate the restore pods:  

```
# ./nspdeployerctl uninstall --undeploy ↵
```

8. Open a CLI on the CLM cluster host.

9. Enter the following:

```
# kubectl get pods -A ↵
```

The pods are listed.

10. If the following restore pod is listed, the pod is not terminated; return to substep 9.

- `nspos-postgresql-primary-n`

**Note:** You must not proceed to the next step if a restore pod is listed.

11. On the CLM deployer host, enter the following:

```
# ./nspdeployerctl install --deploy ↵
```

The CLM initializes using the restored data.

12. Enter the following periodically on the CLM cluster host to display the cluster status:

```
# kubectl get pods -A ↵
```

The cluster is operational when the status of each pod is Running.

12

---

Close the open console windows.

END OF STEPS

---

## 7.9 How do I back up the CLM Kubernetes secrets?

### 7.9.1 Steps

Perform the following steps in each data center to back up the Kubernetes secrets.

- 
- 1 \_\_\_\_\_  
Log in as the root or CLM admin user on the CLM deployer host.
  - 2 \_\_\_\_\_  
Open a console window.
  - 3 \_\_\_\_\_  
Enter the following on the CLM deployer host:  

```
# cd /opt/nsp/nsp-CN-DEP-release-ID/bin ↵
```
  - 4 \_\_\_\_\_  
Enter the following:  

```
# ./nspdeployerctl secret -o backup_file backup ↵
```

where *backup\_file* is the absolute path and name of the backup file to create

As the secrets are backed up, messages like the following are displayed for each Kubernetes namespace:

```
Backing up secrets to /opt/backupfile...  
Including secret namespace:ca-key-pair-external  
Including secret namespace:ca-key-pair-internal  
Including secret namespace:nsp-tls-store-pass
```

When the backup is complete, the following prompt is displayed:

```
Please provide an encryption password for backup_file  
enter aes-256-ctr encryption password:
```
  - 5 \_\_\_\_\_  
Enter a password.  
The following prompt is displayed:  

```
Verifying - enter aes-256-ctr encryption password:
```
  - 6 \_\_\_\_\_  
Re-enter the password.  
The backup file is encrypted using the password.
  - 7 \_\_\_\_\_  
Record the password for use when restoring the backup.
  - 8 \_\_\_\_\_  
Record the name of the data center associated with the backup.

- 
- 9 \_\_\_\_\_  
Copy *backup\_file* to a backup directory.

END OF STEPS \_\_\_\_\_

## 7.10 How do I restore the CLM Kubernetes secrets?

### 7.10.1 Steps

**i** **Note:** Ensure that you restore each backup file on the correct CLM cluster; a CLM secrets backup is specific to a CLM cluster.

Perform the following steps in each data center to restore the CLM Kubernetes secrets.

- 1 \_\_\_\_\_  
Log in as the root or CLM admin user on the CLM deployer host.

- 2 \_\_\_\_\_  
Open a console window.

- 3 \_\_\_\_\_  
Enter the following on the CLM deployer host:

```
# cd /opt/nsp/NSP-CN-DEP-release-ID/bin ↵
```

- 4 \_\_\_\_\_  
Enter the following:

```
./nspdeployerctl secret -i backup_file restore ↵
```

where *backup\_file* is the absolute path and filename of the secrets backup file to restore

The following prompt is displayed:

```
Please provide the encryption password for /opt/backupfile  
enter aes-256-ctr decryption password:
```

- 5 \_\_\_\_\_  
Enter the password recorded during the backup creation.

As the secrets are restored, messages like the following are displayed for each Kubernetes namespace:

```
Restoring secrets from backup_file...  
secret/ca-key-pair-external created  
  Restored secret namespace:ca-key-pair-external  
secret/ca-key-pair-internal created  
  Restored secret namespace:ca-key-pair-internal  
secret/nsp-tls-store-pass created
```

---

Restored secret `namespace:nsp-tls-store-pass`

**END OF STEPS**

---

