

Junos Space Connectivity Services Director Release Notes 2.1R1

16 August 2017

Contents

Introduction	3
Release Notes for Connectivity Services Director 2.1R1	3
Supported Platforms	4
Junos Space Network Management Platform Requirements for Connectivity Services Director 2.1R1	4
Installation and Upgrade Instructions	5
New Installation Instructions for Connectivity Services Director Release 2.1R1	5
Upgrading from Connectivity Services Director Release 2.0R2, 2.0R3, 2.0R4, or 2.0R5 to Connectivity Services Director Release 2.1R1	6
Upgrading from Connectivity Services Director Release 1.0R1 or Release 1.0R2 to Connectivity Services Director Release 2.1R1	7
Installing Junos Space Platform Hot Patch Release 15.2R2 v11	8
Upgrading from Services Activation Director Release 14.3R3 to Connectivity Services Director Release 2.1R1	9
Operational Notes	11
Installing and Uninstalling Red Hat Package Manager for Connectivity Services Director	13
Uninstalling Red Hat Package Manager for Connectivity Services Director	13
Installing Red Hat Package Manager for Connectivity Services Director	14
Installing and Uninstalling Red Hat Package Manager for Services Activation Director	15
Uninstalling Red Hat Package Manager for Services Activation Director	15
Installing Red Hat Package Manager for Services Activation Director	17
Accessing the Services Activation Director GUI	19
Junos Space DMI Schema Requirements for Junos Space Connectivity Services Director	19
Known Limitations	20

New and Changed Features	27
Known Issues	28
Resolved Issues	30
Finding More Information	31
Documentation Feedback	31
Requesting Technical Support	32
Self-Help Online Tools and Resources	32
Opening a Case with JTAC	32
Revision History	33

Introduction

These Release Notes accompany Release 2.1 of the Juniper Networks Junos Space Connectivity Services Director. They contain installation information, and they describe new and changed features, limitations, and known and resolved issues in the software.

Release Notes for Connectivity Services Director 2.1R1

Junos Space Connectivity Services Director, built to run on Junos Space Network Management Platform, is a robust and holistic application that facilitates automated design and provisioning of point-to-point services, virtual private LAN services (VPLS), Layer 3 VPN services, and RSVP-signaled label-switched path (LSP) services, configuration of quality-of-service (QoS) profiles, validation and monitoring of service performance, and management of timing or clock synchronization using Precision Time Protocol (PTP). Connectivity Services Director enables unified management of the ACX Series routers, M Series routers, MX Series routers, PTX Series routers, and TCA Series Timing Appliances in your network. It enables full network life cycle management by simplifying the discovery, configuration, visualization, monitoring, and administration of large networks containing physical and virtual devices.

Connectivity Services Director enables you to provision point-to-point and multipoint services across networks. You can also configure CoS (also called QoS) profiles to group a set of CoS parameters and apply the profiles to one or more interfaces of the devices that are managed by Connectivity Services Director. The Connectivity Services Director software application also contains the applications that were available in the Services Activation Director suite. Network Activate, Transport Activate, OAM Insight, and Sync Design are installed and presented with the same look-and-feel as Services Activation Director, after you install Connectivity Services Director.

The software images for Connectivity Services Director, Junos Space Management Platform, additional scripts, Connectivity Services Director API Reference documentation, and the release notes for Connectivity Services Director Release 2.1R1 are available at: [Junos Space and Junos Space Connectivity Services Director Download](#).

- [Supported Platforms on page 4](#)
- [Junos Space Network Management Platform Requirements for Connectivity Services Director 2.1R1 on page 4](#)
- [Installation and Upgrade Instructions on page 5](#)
- [Operational Notes on page 11](#)
- [Installing and Uninstalling Red Hat Package Manager for Connectivity Services Director on page 13](#)
- [Installing and Uninstalling Red Hat Package Manager for Services Activation Director on page 15](#)
- [Accessing the Services Activation Director GUI on page 19](#)
- [Junos Space DMI Schema Requirements for Junos Space Connectivity Services Director on page 19](#)

- [Known Limitations on page 20](#)
- [New and Changed Features on page 27](#)
- [Known Issues on page 28](#)
- [Resolved Issues on page 30](#)

Supported Platforms

[Table 1 on page 4](#) lists the supported platforms for Connectivity Services Director Release 2.1R1 and the corresponding qualified Junos OS releases.

Table 1: Supported Platforms and the Software Versions for Connectivity Services Director Release 2.1R1

Supported Platforms	Qualified Junos OS Release
ACX Series Universal Access Routers: <ul style="list-style-type: none"> • ACX500 router • ACX1000 router • ACX1100 router • ACX2000 router • ACX2100 router • ACX2200 router • ACX4000 router • ACX5000 router (ACX5048 and ACX5096) 	Release 12.3R1 through Release 12.3X54-D10 for ACX1000, ACX1100, ACX2000, ACX2100, ACX2200, and ACX4000 routers Release 15.1X54-D20 for ACX5000 routers Release 12.3X54-D20 for ACX500 routers Release 17.2R1
MX Series 3D Universal Edge Routers	Release 12.2R1 through Release 17.1R1 for MX80, MX104, MX240, MX480, and MX960 routers Release 13.3R1 through Release 17.1R1 for MX2010 and MX2020 routers
M Series Multiservice Edge Routers	Release 10.0 through Release 12.2R1.8 for M320 routers Release 10.0 through Release 14.2R1.12 for M7i and M10i routers
PTX Series Packet Transport Routers	Release 13.2R2.2 through Release 15.1F6 for PTX3000 routers Release 13.2R1.7 through Release 15.1F6 for PTX5000 routers
Virtual MX Series Routers (vMX)	Release 14.1R5 through Release 17.2R1

Junos Space Network Management Platform Requirements for Connectivity Services Director 2.1R1

You can install Connectivity Services Director in a Junos Space Virtual Appliance. The Junos Space Virtual Appliance can be deployed on a VMware ESX server. The Junos Space Virtual Appliance requires a VMware ESX server 4.0 or later or VMware ESXi server 4.0, 5.0, 5.1, or 5.5 that can support a virtual machine with the following configuration:

- 64-bit quad processor with at least 2.66-GHz speed
- 32-GB RAM

- One RJ-45 10/100/1000 Network Interface Connector
- 133-GB hard disk

Installation and Upgrade Instructions

Before you install Connectivity Services Director Release 2.1R1, ensure that the Junos Space Network Management Platform is of the required release number with the latest patch installed.



NOTE: We recommend that you restart the JBoss server after you install Connectivity Services Director Release 2.1R1.

The software image for Connectivity Services Director Release 2.1R1 enables you to install the Connectivity Services Director application. Also, Network Activate, Transport Activate, OAM Insight, and Sync Design are installed and presented in the same look-and-feel as the Services Activation Director GUI, after you install Connectivity Services Director. The Representational State Transfer (REST) APIs for Connectivity Services Director are installed along with the GUI.

When you install Connectivity Services Director, the single application package installs the capabilities for configuring network services, such as point-to-point, Layer 3 VPN, and VPLS; configuring MPLS and RSVP label-switched path (LSP) services; configuring Precision Time Protocol (PTP) and synchronous Ethernet services; configuring the Operations, Administration, and Maintenance (OAM) functionality; and configuring CoS profiles. For Connectivity Services Director Release 2.1R1, you can also access the Services Activation Director GUI to launch workspaces to configure functionalities that are not available in the Connectivity Services Director GUI. You need not separately install the different applications, such as Network Activate or Transport Activate, based on your deployment needs and device models to be managed, on a JA2500 Junos Space Appliance or a Junos Space Virtual Appliance that satisfies the hardware requirements.

- [New Installation Instructions for Connectivity Services Director Release 2.1R1 on page 5](#)
- [Upgrading from Connectivity Services Director Release 2.0R2, 2.0R3, 2.0R4, or 2.0R5 to Connectivity Services Director Release 2.1R1 on page 6](#)
- [Upgrading from Connectivity Services Director Release 1.0R1 or Release 1.0R2 to Connectivity Services Director Release 2.1R1 on page 7](#)
- [Installing Junos Space Platform Hot Patch Release 15.2R2 v11 on page 8](#)
- [Upgrading from Services Activation Director Release 14.3R3 to Connectivity Services Director Release 2.1R1 on page 9](#)

[New Installation Instructions for Connectivity Services Director Release 2.1R1](#)

Before you start the installation, ensure the following:

- Connectivity Services Director is supported on a JA2500 Junos Space Appliance or a Junos Space Virtual Appliance that meets the hardware requirements specified in the Junos Space documentation. The Junos Space Appliance that suits your requirement is determined by the number of devices you plan to manage by using the network management application.
- Network Director or Edge Services Director cannot be installed on the same system as Connectivity Services Director. Uninstall Network Director or Edge Services Director before you install Connectivity Services Director on your system.
- When you back up the database of a Junos Space Appliance by using the Junos Space Network Application Platform database backup-and-restore facility, all the data maintained by the Junos Space Platform and installed Junos Space applications on the appliance is backed up. If your appliance contains a Junos Space application, such as Service Now, that you do not want to use in your network after upgrading to a different version of Junos Space Platform, you must ensure that you uninstall the application before you perform a backup. This is required because all the backed-up-data is restored when you use the restore utility to reapply the data after an upgrade operation. As a result, if your device was previously installed with a Junos Space application that you have not reinstalled after upgrading Junos Space Platform, restoring the backed up data causes undefined behavior because the backup in such a scenario also contains data of applications that you have not reinstalled.
- A prescribed order is always required for the installation or upgrade of Connectivity Services Director.

To perform a new installation of Connectivity Services Director Release 2.1R1:

1. Download and install Junos Space Platform Release 17.1R1.
2. Install Connectivity Services Director Release 2.1R1.
3. Restart the JBoss server.

The Connectivity Services Director Release 2.1R1 is installed.

Upgrading from Connectivity Services Director Release 2.0R2, 2.0R3, 2.0R4, or 2.0R5 to Connectivity Services Director Release 2.1R1

Before you start the upgrade, ensure that you have:

- Disabled monitoring for all categories on the Monitoring tab of the Preferences page. For more details, see [Disabling Data Collection for Monitors](#).
- Downloaded the Connectivity Services Director Release 2.1R1 software image to the hard disk or to an SCP server. The Connectivity Services Director software images are located at <http://www.juniper.net/support/downloads/space.html> .

To upgrade from Connectivity Services Director Release 2.0R2, 2.0R3, 2.0R4, or 2.0R5 to Release 2.1R1:

1. Upgrade Junos Space Platform to Release 16.1. See [Upgrading to Junos Space Network Management Platform Release 16.1R1](#) for instructions on installing Junos Space Platform Release 16.1R1.
2. Upgrade to Junos Space Platform to Release 17.1. See [Upgrading Junos Space Network Management Platform](#) for instructions on installing Junos Space Platform Release 17.1R1.
3. Upgrade Connectivity Services Director to Release 2.1R1.
4. Restart the JBoss server for the monitoring and fault features to work properly in standalone and cluster setups.

[Upgrading from Connectivity Services Director Release 1.0R1 or Release 1.0R2 to Connectivity Services Director Release 2.1R1](#)

Before you start the upgrade, ensure that you have:

- Disabled monitoring for all categories on the Monitoring tab of the Preferences page. For more details, see [Disabling Data Collection for Monitors](#).
- Junos Space Platform Release 15.2R2 running on your appliance. If your appliance is running an unsupported release of Junos Space, you must upgrade Junos Space before installing Connectivity Services Director.
- Downloaded the Connectivity Services Director Release 2.1R1 software image to the hard disk or to an SCP server. The Connectivity Services Director software images are located at <http://www.juniper.net/support/downloads/space.html>.

To upgrade from Connectivity Services Director Release 1.0R1 or 1.0R2 to Release 2.1R1:

1. Back up the Junos Space Platform database.
2. If you are running a version of Junos Space Platform earlier than Release 15.2R2, uninstall Red Hat Package Manager.

You can uninstall the Red Hat Package Manager manually, or you can run the `uninstall_rpm.sh` script to uninstall the Red Hat Package Manager.

For more information about uninstalling the Red Hat Package Manager manually, see [Installing and Uninstalling Red Hat Package Manager for Connectivity Services Director](#).

For more information about the script, contact the Juniper Networks Technical Assistance Center.
3. Upgrade Junos Space Platform to Release 15.2R2.



NOTE: You must not reboot Junos Space Platform on the Maintenance Mode Options page.

4. Install Red Hat Package Manager.

You can install the Red Hat Package Manager manually, or you can run the *install_rpm.sh* script to install the Red Hat Package Manager.

For more information about installing the Red Hat Package Manager manually, see [Installing and Uninstalling Red Hat Package Manager for Connectivity Services Director](#).

For more information about the script, contact the Juniper Networks Technical Assistance Center.

5. Reboot Junos Space Platform on the Maintenance Mode Options page.

6. Download the 15.2R2-hotpatch-v11.tgz patch to your local computer from the <https://www.juniper.net/support/downloads/?p=space#sw> location. See [Installing Junos Space Platform Hot Patch Release 15.2R2 v11](#) for more information.

7. Upgrade to Connectivity Services Director Release 2.0R6.

8. Upgrade Junos Space Platform to Release 16.1. See [Upgrading to Junos Space Network Management Platform Release 16.1R1](#) for instructions on installing Junos Space Platform Release 16.1R1.

9. Upgrade to Junos Space Platform to Release 17.1. See [Upgrading Junos Space Network Management Platform](#) for instructions on installing Junos Space Platform Release 17.1R1.

10. Upgrade to Connectivity Services Director Release 2.1R1.

11. Restart the JBoss server for the monitoring and fault features to work properly in standalone and cluster setups.

[Installing Junos Space Platform Hot Patch Release 15.2R2 v11](#)

To install Junos Space Platform hot patch release 15.2R2 v11:

1. Download the 15.2R2-hotpatch-v11.tgz patch to your local computer from the <https://www.juniper.net/support/downloads/?p=space#sw> location.

2. Log in to the Junos Space active VIP node as the admin user.

3. Transfer the patch to the Junos Space node by using Secure Copy Protocol (SCP). Save the file in a temporary location, such as /tmp/patch or /home/admin.
4. Navigate to the location on the node where you stored the patch.
5. Extract the patch by using the following command:


```
tar zxf 15.2R2-hotpatch-v11.tgz
```
6. Change to the extracted patch directory.


```
cd 15.2R2-hotpatch-v11
```
7. Type the following command and press Enter to install the patch:


```
sh patchme.sh
```
8. You are prompted to enter your password. Enter your CLI password.
The JBoss server is rebooted automatically.

Upgrading from Services Activation Director Release 14.3R3 to Connectivity Services Director Release 2.1R1



NOTE: We support migration only from Services Activation Director Release 14.3R3 running on Junos Space Platform Release 14.1R3.4. If you are running a version of Network Activate, Transport Activate, OAM Insight, or Sync Design earlier than 14.3R3, you must first upgrade to 14.3R3 or later before you can upgrade to Connectivity Services Director 2.1R1.

To upgrade from Network Activate Release 14.3R3, Transport Activate 14.3R3, OAM Insight 14.3R3 and Sync Design 14.3R3 to Connectivity Services Director Release 2.1R1:

1. Back up the Junos Space Platform database.
2. Upgrade Junos Space Platform to Release 15.1R1.
3. Reboot Junos Space Platform on the Maintenance Mode Options page.
4. Uninstall Red Hat Package Manager.

You can uninstall the Red Hat Package Manager manually, or you can run the *uninstall_rpm.sh* script to uninstall the Red Hat Package Manager.

For more information about uninstalling the Red Hat Package Manager manually, see *Installing and Uninstalling Red Hat Package Manager for Services Activation Director*.

For more information about the script, contact the Juniper Networks Technical Assistance Center.

5. Upgrade Junos Space Platform to Release 15.2R2.



NOTE: You must not reboot Junos Space Platform on the Maintenance Mode Options page.

6. Install Red Hat Package Manager.

You can install the Red Hat Package Manager manually, or you can run the `install_rpm.sh` script to install the Red Hat Package Manager.

For more information about installing the Red Hat Package Manager manually, see [Installing and Uninstalling Red Hat Package Manager for Services Activation Director](#).

For more information about the script, contact the Juniper Networks Technical Assistance Center.

7. Reboot Junos Space Platform on the Maintenance Mode Options page.
8. Upgrade Junos Space Platform to Release 16.1. See [Upgrading to Junos Space Network Management Platform Release 16.1R1](#) for instructions on installing Junos Space Platform Release 16.1R1.
9. Upgrade to Junos Space Platform to Release 17.1. See [Upgrading Junos Space Network Management Platform](#) for instructions on installing Junos Space Platform Release 17.1R1.
10. Install Connectivity Services Director Release 2.1R1.
11. Uninstall other applications (such as Junos Space QoS Design or Junos Space Transport Activate) as needed before you uninstall Network Activate.
12. Uninstall NetworkAppsApi.
13. Uninstall Network Activate.
14. Restart the JBoss server.



NOTE: QoS Design cannot be installed on the same system as Connectivity Services Director. After the uninstallation of the legacy applications, such as Network Activate 14.3R1, Transport Activate 14.3R1, Sync Design 14.3R1, or OAM Insight 14.3R1, wait until the applications are removed from the Applications page of the Junos Space Platform application. After all the applications are uninstalled, restart the JBoss server. Connectivity Services Director does not work correctly if the JBoss server is not rebooted.

Operational Notes

The following are the operational notes for Connectivity Services Director:

- The minimum supported screen resolution is 1280 x 1024. If your screen resolution is less than the supported resolution, the Connectivity Services Director UI might not be displayed properly. For example, icons might not be displayed on the Connectivity Services Director banner, pages might appear truncated, or scroll bars might not work correctly.
- The supported Web browsers are Google Chrome 17 and later, Mozilla Firefox 14.0 and later, and Microsoft Internet Explorer 9.0, 10.0, and 11.0.
- If you have been logged in to Connectivity Services Director for a long period of time, the connection to the server might time out. Monitoring pages might go blank or you might not be able to access tasks. To resolve this, log out of Connectivity Services Director and then log in again.
- If you receive a Java exception error message when you perform an operation, retry the operation. The error condition is usually temporary and harmless.
- Only user accounts with administrator (admin) privileges can use the Connectivity Services Director API.
- For Connectivity Services Director to be able to discover and manage devices, the following protocol ports must be open between the Junos Space Platform server and the devices:
 - Port 22 for SSH connections. If you have changed the SSH port to a port other than port 22 on your Junos Space Platform, you must change the SSH ports on your managed devices to the port that the Junos Space Platform is using.
 - Port 10162 for device-level SNMP traps. Connectivity Services Director receives traps from managed devices on this port. (After you install Connectivity Services Director, use Connectivity Services Director to configure SNMP on your devices to send traps to Connectivity Services Director on this port.)
 - Port 162 for service-level SNMP traps. Connectivity Services Director uses OpenNMS for SNMP trap collection and correlation.
 - Port 21 (TCP) and port 69 (UDP) for uploading the software image and configuration file to the FTP server.
- When a switchover from the active Junos Space server to the standby server occurs in a clustered Junos Space appliance environment, cleared alarms are not notified to the Junos Space server, although OpenNMS receives the clear-alarm notification. To work around this problem, you must manually clear the appropriate alarm from the Alarm Detail monitor in Fault mode of Service view of the Connectivity Services Director GUI.
- Sometimes, it is observed that the View Pending Configuration REST API call fails due to a timeout. To prevent this problem, the timeout has been increased to one minute from the default value of 30 seconds.

- If OpenNMS is restarted, the OpenNMS service loses all the data in its cache repository and the multisite alarm status calculation goes wrong. In such a scenario, you must manually analyze the network and take corrective actions, as necessary, on the alarms.
- When you add or delete a Fault Monitoring and Performance Monitoring (FMPM) node to a Junos Space cluster, the following message is displayed:

Adding/Deleting FMPM specialized node involves optimization and readjustment of memory used for various software components. Space servers must be rebooted in order to operate under this new setting

You must restart all the Junos Space nodes in such a scenario.

- After a device is prestaged in Connectivity Services Director, the prestaging job is not initiated on the same device again. When a device notification is received by the application, Connectivity Services Director synchronizes the prestaging database on the user-to-network interfaces (UNI). If a mismatch is detected in the UNI status of the interface in the Connectivity Services Director database and the UNI status of the interface on the device (caused by the application being down or network accessibility problems), the synchronization of the UNI interface might not occur. In such a case, the synchronization operation occurs when a configuration-commit on the device is performed the next time. To manually resolve this discrepancy in the UNI status of the interface, you can unassign the UNI role of the interface, which causes prestaging to perform a synchronization.
- In a scaled environment, you can disable the monitoring functionality, which causes the Connectivity Services Director application to poll the specified devices and retrieve details to be displayed in the widgets in Monitor mode of Service view. You might require the monitoring functionality to be disabled to prevent the slowness in loading the GUI pages. To disable the monitoring mechanism, you can run a script on the Junos Space Appliance. You must stage the script on the device with administrative and execute permissions for the script file before executing the script.

To enable or disable monitoring, enter the following command at the shell prompt (To run shell commands, from the Junos Space Appliance Settings menu, enter **7** at the prompt):

```
EnableDisableCollector.sh <db_user_name> <db_password> <collectorName>  
<enable/disable>
```

where:

- **db_user_name** is the username of the user for the Connectivity Services Director database.
- **db_password** is the password of the user for the database.
- **collectorName** is the name of the collector for which you want to enable or disable retrieval of statistics. You can enter one of the following collector names:
 - ProvisioningMonitorInterfaceStatusCollector—Defines the polling interval for monitoring the interface status
 - ProvisioningMonitorInterfaceStatsCollector—Defines the polling interval for monitoring the interface statistics

- `ProvisioningMonitorServiceStatusCollector`—Defines the polling interval for monitoring the service status
- `ProvisioningMonitorLDPStatsCollector`—Defines the polling interval for monitoring the LDP statistics
- `ProvisioningMonitorY1731PMCollector`—Defines the polling interval for monitoring the performance management or Y.1731 statistics
- `ProvisioningMonitorLSPStatsCollector`—Defines the polling interval for monitoring the LSP statistics
- `EquipmentMonitorDeviceStatusCollector`—Defines the polling interval for monitoring the status of a device

The ***collectorName*** parameter is optional. If you do not specify a collector name, monitoring is enabled or disabled for all the collectors. If you enter an incorrect collector name, the list of collector names is displayed and you are prompted to select from the list.

- **enable** is the keyword to enable the monitoring functionality and collection of statistics.
- **disable** is the keyword to disable the monitoring functionality and collection of statistics.

We recommend that you use the script to disable the monitoring functionality only with the assistance of a Juniper Technical Assistance Center (JTAC) representative.

- Although SRX Series Services Gateways are not displayed in the Device view of Connectivity Services Director, if the configuration of such devices matches the prestaging rules, SRX Series devices are prestaged and displayed as network-provider edge (N-PE) devices in the Prestage Devices window.
- For Layer 3 VPN services, data plane validation is not performed when you run functional audit for a service that does not contain the ***vrf-table-label*** attribute, which maps the inner label of a packet to a specific VRF instance. The Functional Audit Results window displays a message about the ***vrf-table-label*** configuration attribute not enabled in the service in such a scenario.

Installing and Uninstalling Red Hat Package Manager for Connectivity Services Director

These topics provide step by step instructions to uninstall and install Red Hat Package Manager for Connectivity Services Director.

- [Uninstalling Red Hat Package Manager for Connectivity Services Director on page 13](#)
- [Installing Red Hat Package Manager for Connectivity Services Director on page 14](#)

Uninstalling Red Hat Package Manager for Connectivity Services Director

To uninstall the Red Hat Package Manager for Connectivity Services Director:



NOTE: If your Junos Space setup contains more than one node, you must perform these steps for all nodes in the fabric.

1. Connect to the Junos Space VIP node (by using SSH) and log in (as the **admin** user) to access the Junos Space CLI.

The Junos Space Settings Menu appears.

2. Type **6** (if the node is a hardware appliance) or **7** (if the node is a virtual appliance) to open a debug (command) prompt.

You are prompted to enter your password.

3. Type the password for the **admin** user and press Enter.

You are taken to the shell.

4. Run the **rpm -qa|grep jmp-csd** command to determine Connectivity Services Director Red Hat Package Manager to uninstall. A sample output is as follows:

```
[root@host ~]# rpm -qa|grep jmp-csd
jmp-csd-1.0-367423
```

5. Run the **rpm -e --nodeps rpm-name** command to uninstall the Red Hat Package Manager, where *rpm-name* is the name of the Red Hat Package Manager obtained in the preceding step.
6. Run the **rpm -qa|grep jmp-csd** command to confirm that the Red Hat Package Manager was uninstalled successfully. The command produces no output if the Red Hat Package Manager was uninstalled successfully.
7. Exit the shell and log out of the Junos Space VIP node.

Installing Red Hat Package Manager for Connectivity Services Director

To install Red Hat Package Manager for Connectivity Services Director:



NOTE: If your Junos Space setup contains more than one node, you must perform these steps for all nodes in the fabric.

1. Log in to the Junos Space CLI on the VIP node and access the shell.
2. Run the **/usr/bin/extract_image.sh -i /var/cache/jboss/jmp/Connectivity-Services-Director.1.0R2.6/Connectivity-Services-Director.1.0R2.6.img -s /etc/pki/jmp-softwareManager/certs/JunosSpaceSoftwareCA_v1.pem -t /etc/pki/jmp-softwareManager/certs/JunosSpaceTrusted_CAs.pem -d /home/admin/**

command to extract the Connectivity Services Director Red Hat Package Manager that you previously uninstalled from the Connectivity Services Director software image.

The Red Hat Package Manager is extracted to the `/home/admin/Connectivity-Services-Director.1.0R2.6` directory.

- Run the `rpm -ivh --force jmp-csd-1.0-367423.x86_64.rpm` command to install the Connectivity Services Director Red Hat Package Manager. A sample output follows.

```
[root@host ~]# rpm -ivh --force jmp-csd-1.0-367423.x86_64.rpm
Preparing... #####
[100%]
  1: jmp-csd #####
[100%]
File exists so just check for the strings      modprobe ip_contrack_ftp
present
modprobe ip_contrack_tftp present
File exists so just check for the strings
string present - so just replace the value
```

- Exit the shell and log out of the Junos Space VIP node.

Installing and Uninstalling Red Hat Package Manager for Services Activation Director

These topics provide step by step instructions to uninstall and install Red Hat Package Manager for Services Activation Director.

- [Uninstalling Red Hat Package Manager for Services Activation Director on page 15](#)
- [Installing Red Hat Package Manager for Services Activation Director on page 17](#)

Uninstalling Red Hat Package Manager for Services Activation Director

To uninstall the Red Hat Package Manager for Services Activation Director:



NOTE: If your Junos Space setup contains more than one node, you must perform these steps for all nodes in the fabric.

- Connect to the Junos Space VIP node (by using SSH) and log in (as the **admin** user) to access the Junos Space CLI.

The Junos Space Settings Menu appears.

- Type **6** (if the node is a hardware appliance) or **7** (if the node is a virtual appliance) to open a debug (command) prompt.

You are prompted to enter your password.

- Type the password for the **admin** user and press Enter.

You are taken to the shell.

4. Run the `rpm -qa | grep jmp-provisioning` command to determine which Network Activate Red Hat Package Manager to uninstall. A sample output is as follows:

```
[root@host ~]# rpm -qa | grep jmp-provisioning
jmp-provisioning-14.3-167423
```

5. Run the `rpm -e --nodeps rpm-name` command to uninstall the Red Hat Package Manager, where *rpm-name* is the name of the Red Hat Package Manager obtained in the preceding step.

6. Run the `rpm -qa | grep jmp-provisioning` command to confirm that the Network Activate Red Hat Package Manager was uninstalled successfully. The command produces no output if the Red Hat Package Manager was uninstalled successfully.

7. Run the `rpm -qa | grep jmp-timing` command to determine which Sync Design Red Hat Package Manager to uninstall. A sample output is as follows:

```
[root@host ~]# rpm -qa | grep jmp-timing
jmp-timing-14.3-167423
```

8. Run the `rpm -e --nodeps rpm-name` command to uninstall the Red Hat Package Manager, where *rpm-name* is the name of the Red Hat Package Manager obtained in the preceding step.

9. Run the `rpm -qa | grep jmp-timing` command to confirm that the Sync Design Red Hat Package Manager was uninstalled successfully. The command produces no output if the Red Hat Package Manager was uninstalled successfully.

10. Run the `rpm -qa | grep jmp-oam` command to determine which OAM Insight Red Hat Package Manager to uninstall. A sample output is as follows:

```
[root@host ~]# rpm -qa | grep jmp-oam
jmp-oam-14.3-167423
```

11. Run the `rpm -e --nodeps rpm-name` command to uninstall the Red Hat Package Manager, where *rpm-name* is the name of the Red Hat Package Manager obtained in the preceding step.

12. Run the `rpm -qa | grep jmp-oam` command to confirm that the OAM Insight Red Hat Package Manager was uninstalled successfully. The command produces no output if the Red Hat Package Manager was uninstalled successfully.

13. Exit the shell and log out of the Junos Space VIP node.

Installing Red Hat Package Manager for Services Activation Director

To install Red Hat Package Manager for Services Activation Director:



NOTE: If your Junos Space setup contains more than one node, you must perform these steps for all nodes in the fabric.

1. Log in to the Junos Space CLI on the VIP node and access the shell.
2. Run the `/usr/bin/extract_image.sh -i /var/cache/jboss/jmp/Network-Activate.$appVersion/Network-Activate.$appVersion.img -s /etc/pki/jmp-softwareManager/certs/JunosSpaceSoftwareCA_v1.pem -t /etc/pki/jmp-softwareManager/certs/JunosSpaceTrusted_CAs.pem -d /home/admin/` command to extract Network Activate Red Hat Package Manager that you previously uninstalled from the Network Activate software image.

The Red Hat Package Manager is extracted to the `/home/admin/Network-Activate.$appVersion` directory.



NOTE: Before you execute the command, you must specify the release version for `$appVersion`, for example, `Network-Activate.14.3R3.1.img`.

3. In the `/home/admin/Network-Activate.$appVersion` directory, run the `rpm -ivh -force jmp-provisioning*` command to install the Network Activate Red Hat Package Manager. A sample output follows.

```
[root@host ~]# rpm -ivh -force jmp-provisioning*
Preparing... #####
[100%]
 1: jmp-provisioning ##### [100%]

File exists so just check for the strings      modprobe ip_contrack_ftp
present
modprobe ip_contrack_tftp present
File exists so just check for the strings
string present - so just replace the value
```

4. Run the `/usr/bin/extract_image.sh -i /var/cache/jboss/jmp/OAMInsight.$appVersion/OAMInsight.$appVersion.img -s /etc/pki/jmp-softwareManager/certs/JunosSpaceSoftwareCA_v1.pem -t /etc/pki/jmp-softwareManager/certs/JunosSpaceTrusted_CAs.pem -d /home/admin/` command to extract OAM Insight Red Hat Package Manager that you previously uninstalled from OAM Insight software image.

The Red Hat Package Manager is extracted to the `/home/admin/OAMInsight.$appVersion` directory.



NOTE: Before you execute the command, you must specify the release version for *\$appVersion*, for example, OAMInsight.14.3R3.1.img.

- Run the `rpm -ivh -force jmp-oam*` command to install the OAM Insight Red Hat Package Manager. A sample output follows.

```
[root@host ~]# rpm -ivh -force jmp-oam*
Preparing... #####
[100%]
1: jmp-oam #####
[100%]
File exists so just check for the strings      modprobe ip_contrack_ftp
present
modprobe ip_contrack_tftp present
File exists so just check for the strings
string present - so just replace the value
```

- Run the `/usr/bin/extract_image.sh -i /var/cache/jboss/jmp/SyncDesign.$appVersion/SyncDesign.$appVersion.img -s /etc/pki/jmp-softwareManager/certs/JunosSpaceSoftwareCA_v1.pem -t /etc/pki/jmp-softwareManager/certs/JunosSpaceTrusted_CAs.pem -d /home/admin/` command to extract Sync Design Red Hat Package Manager that you previously uninstalled from Sync Design software image.

The Red Hat Package Manager is extracted to the `/home/admin/SyncDesign.$appVersion` directory.



NOTE: Before you execute the command, you must specify the release version for *\$appVersion*, for example, SyncDesign.14.3R3.1.img.

- Run the `rpm -ivh -force jmp-timing*` command to install the Sync Design Red Hat Package Manager. A sample output follows.

```
[root@host ~]# rpm -ivh -force jmp-timing*
Preparing... #####
[100%]
1: jmp-timing #####
[100%]
File exists so just check for the strings      modprobe ip_contrack_ftp
present
modprobe ip_contrack_tftp present
File exists so just check for the strings
string present - so just replace the value
```

- Exit the shell and log out of the Junos Space VIP node.

Accessing the Services Activation Director GUI

In Connectivity Services Director Release 2.1R1, you can also access the Services Activation Director GUI to launch workspaces to configure functionalities. You must install Junos Space Platform before trying to access the Services Activation Director GUI.

To access the Services Activation Director GUI:

1. Install Connectivity Services Director using the Junos Space Platform GUI.

The JBoss server restarts automatically after the installation.

2. Close your browser window and open a new browser window.

3. Log in to Junos Space by using the following URL:

```
https://<n.n.n.n>/mainui
```

where *n.n.n.n* is the IP address of the Junos Space Platform GUI.

The Junos Space login page appears.

4. Enter your username and password and click **Log In**.

The Junos Space Platform GUI is displayed.

5. Select **Services Activation Director** from the Applications list on the left pane of the Junos Space Platform GUI.

The Services Activation Director GUI is launched.



NOTE: If you select **Connectivity Services Director** from the Applications list on the left pane of the Junos Space Platform GUI, the Connectivity Services Director GUI is launched.

Alternatively, in the Address field of your browser, enter the following URL:

```
https://<n.n.n.n>/csd/
```

where *n.n.n.n* is the IP address of the Junos Space GUI. You can bookmark the login page for future use.

Junos Space DMI Schema Requirements for Junos Space Connectivity Services Director

In most installations, Junos Space automatically matches DMI schemas to device families. But there might be situations where your network uses a device for which Junos Space does not have the latest or supported schema available. In such situations, you must obtain and upload the requisite schema and set it as the default DMI schema for each device family. For the different devices, you can set a default DMI schema for each device family to enable Junos Space to apply an appropriate schema to a device family.

We recommend that you use the JUNOS 14.2R2.8 schema for Connectivity Services Director Release 2.1R1.



NOTE: See [Setting a Default DMI Schema](#) for detailed steps to set a default schema.

Known Limitations

This section lists the known limitations in Connectivity Services Director:

- Job details displayed on the **Config Deployment Jobs Status** page do not contain complete information about failed jobs. To get complete information about failed jobs, including the reason for job failure, you need to verify the server logs stored on the server.
- Connectivity Services Director supports role-based access control (RBAC) only at the task category level. There is no support for object-level or task-level access control.
- If an interface or the logical unit of an interface is deactivated, the configuration audit operation fails and a message about a mismatch between the interface configuration on the device and the interface configuration in the Connectivity Services Director database is displayed under the Show Results tab of the Configuration Audit dialog box. However, configuration audit is successful if you deactivate the interface at the **[edit interfaces *interface-name* unit *logical-unit-number* family *vpls*]** hierarchy level of the CLI configuration.

When you disable an interface from the CLI, a new tag, **<disable>**, is added to the configuration on the device. When you perform a configuration audit, Connectivity Services Director sends the list of XPath attributes to be verified in the XML configuration present on the device before the configuration changes are propagated to the device. Because the **<disable>** attribute is not one of the tags that are sent to the device, the Connectivity Services Director application cannot determine whether the tag has been added to the XML configuration. As a result, a configuration audit is successful in such a scenario.

- When you edit a service order, the auto-pick option that you enabled during the creation of the service order that is associated with a service definition is not preserved. Also, the parameters for which you enabled automatic selection by the system, such as Unit ID and Route Target, require you to enter values, and the Autopick check boxes do not remain selected.
- When you edit an existing service order by clicking the Edit button on the Manage Network Services or Manage Service Deployment pages in Deploy mode of the Service view on the Connectivity Services Director GUI, a fresh service order is created with the name you specified. Only the changed node details are stored in the new service order and the previous details are lost.

This is an expected behavior because only a subset of the configuration settings are required to be propagated to a device from Connectivity Services Director, whenever a service order is modified. As a result, an existing service order is not saved when you modify it; instead, a fresh service order is created. Also, a service order related to a

failed or invalid modified service cannot be modified. You need to delete the failed or invalid service order and modify the service again.

- Sometimes, the validation of a point-to-point service order fails with an error message stating that a duplicate virtual circuit ID exists, even when you have selected the option to automatically assign a VC ID from the VC ID pool in the service order. This condition occurs because of a resource pool allocation failure—that is, when the same device is managed by more than one Junos Space Platform application. Consider a device that is added and discovered by two Junos Space Platform servers. Assume that on one server running Junos Space Platform, Connectivity Services Director is also installed. The resource pool management functionality on that server reserves resources for devices that are managed only by using that server. If a resource, such as an IP address pool, VLAN ID, or a route target is reserved by both the Junos Space Platform servers, the reservation on one server is not reflected in the other server. If the same resource is marked for use in a service by multiple Junos Space instances or servers that manage the same device, you must perform a service recovery operation. This operation recovers services that are present on devices that Junos Space is not managing. Auto-discovery of services is not supported; therefore, resources used by other Junos Space servers or modified on a managed device using the CLI are not reserved and displayed in the resource pool. The device configuration must be validated to check for duplicate resources before deploying or validating a service.
- When you launch the Chassis view of a device, device labels are missing from the Google Chrome browser. The interface numbers are not displayed beneath the ports and the device name is not shown in the front view of the chassis image. Also, when you click the Perspective button to view the three-dimensional, advanced view of the chassis, the quality of the chassis image displayed is reduced slightly. This behavior with image quality is expected in the Google Chrome browser.
- In Monitor mode of the Service view, for the Service Monitoring Summary page, the Traffic Trend data is displayed without a unit of measurement (UOM), a tooltip, or an option to zoom in or zoom out.
- When you select the Service Traffic tab in Monitor mode for a specific point-to-point LDP resiliency service, the connection status between the source device and other devices is denoted as NA (not available) in the Service Traffic monitor if any of the following conditions occur:
 - The device does not have Layer 2 circuit data.
 - Remote procedure call (RPC) commands are failing.
 - The NETCONF connection fails to be established.

On the pseudowire graph in the Service Traffic monitor, a gray line is displayed for the NA state. After the next polling cycle, the monitoring mechanism of Connectivity Services Director marks the connections status as NA for all connections from the endpoints on which the Layer 2 circuit configuration is deleted.

The connection status value in the Service Traffic monitor is refreshed depending on the polling interval configured on the Monitoring tab of the Preferences page (which you can launch by clicking the down arrow beside the System button on the Connectivity Services Director banner and selecting Preferences).

- On the Service Monitoring Summary page that is displayed when you select a service from the Network Services > Connectivity > P2P Services tree, Network Services > Connectivity > L3VPN Services tree, or Network Services > Connectivity > VPLS Services tree in the Tasks pane, and select the Service Traffic tab in Monitor mode of Service view, the Traffic Trend (bps) column displays only the rate of egress traffic in the form of a line graph. The rate at which ingress packets are received is not displayed.
- When you attempt to validate or provision a service order, the "Service Order Deployed OK" pop-up message is displayed, regardless of the result of the action. This is an incorrect behavior. The same message is displayed even if the validation and provisioning attempts fail. A job ID with a link must be displayed that you can click to navigate to the Job Management page for the results.

The status of the service order that you validated or provisioned does not change from Scheduled to Validated or Deployed. When a subsequent action is triggered on the service order, a status change is reflected. After the service order is deployed, you are not taken back to the Services landing page in Deploy mode of the Service view.

- When a configuration audit is performed, the XPath attributes in the service configuration are used. Only the addition, modification, and deletion of the XPath attributes are detected, but the creation of a new attribute (child XPath) on a device is ignored. This behavior is expected because Junos Space Platform audits only the settings in a user template. If the template has a container, Junos Space Platform audits only to determine whether the device is configured with this container. If you want to audit any container child, you need to add it into the template. This scenario is similar to an out-of-band configuration change on the device, which Junos Space Platform can determine only whether System of Record mode is set for Junos Space Platform.
- In a scaled environment, the VLAN ID resource pool is not properly considered during the deployment of a Layer 3 VPN service. After being deployed, the service moves to the invalid state because the service generates the same VLAN ID for different interfaces. This problem can arise when the device already contains a service with a VLAN ID and you select the auto-pick option for VLAN ID configuration in the service provisioning workflow for the same device. In such a scenario, the Connectivity Services Director application can generate the VLAN ID, which is already available as part of some other service on the device. At the time of validation, an error message is generated and the service order moves to the invalid state.

Workaround: Select the option to configure the VLAN ID manually (and enter a VLAN ID that is not present as part of any service in the device), instead of selecting the auto-pick option.

- Several **delete** statements are observed in the service settings on the Service Configuration tab of the Configuration dialog box. The **delete** statements indicate deleted policy attributes from a corresponding service on a device. When a service is created or modified, its policy options are deleted from the device to prevent the previously existing policies from interfering with the service. The presence of the **delete** statements is an expected behavior and does not indicate any incorrect service configuration.

- You cannot view details of a device prestaging job on the Job Management page. You need to view the Prestage Devices page in Build mode to view the device prestaging details.
- When you modify a Layer 3 VPN service order for which multicast VPN has been enabled during the creation of the service order, the MVPN check box is disabled on the Service Parameters page of the Layer 3 VPN service modification wizard. You cannot modify MVPN settings during the editing of a service order if MVPN is already enabled in the service order.
- You cannot select a multihomed group on the Node Settings page of the VPLS service order creation wizard with the signaling type as BGP.
- On the Manage Network Services page, you can search for services using only the service name. For the other fields displayed on this page, the search utility is not supported. You can filter the table by clicking the arrow to display the column drop-down menu in the table and selecting the Filters option.
- The search function is supported only for the elements of the tree that are displayed on the page; the global search facility that analyzes all configured elements in the database is not supported.
- While prestaging a device, you cannot modify a loopback address or add multiple loopback addresses.
- At times, when you attempt to validate a VPLS service, an error message is displayed stating that the route target is not in the prescribed format of x:y. This error occurs when an autonomous system (AS) number is defined in the device or when the routing options table does not have the AS number of the device stored in it (that is, the AS number is not synchronized properly).
- In a scaled environment, thousands of services, each assigned to a different virtual circuit ID (VC ID), the Resource Allocation Details page from the Prestage Devices workspace in Build mode of the Service view contains too many details. It is difficult to determine whether a VC ID has been assigned to a device or not. This is because VC IDs are sorted on the basis of strings and not numbers.
- You cannot view the pending service order configuration for an invalid service order.
- The Decommissioned Service Orders option is available on the Tasks pane only when you select the Connectivity node or the Tunnel node from the Network Services tree on the View pane. This option is not available if you select the Network Services node on the View pane. Also, this option is not available if you expand the Connectivity tree and select P2P Services, VPLS Services, or L3VPN Services, or if you expand the Tunnel tree and select RSVP LSPs.
- From the Service Monitoring Summary page, which is displayed if you do not select a particular service from the Service view pane and select the Network Services, Connectivity, P2P Services, L3VPN Services, or VPN Services node on the Service view pane and you want to navigate to the Service Summary page of a specific service, select the corresponding service from the Network Services > Connectivity tree on the View pane.
- When you perform a functional audit with the DMI schema as JUNOS 13.2 on the Junos Space Platform server that is running Connectivity Services Director, the functional

audit job fails because the configuration is propagated to devices without the accept and reject tags, which prevents the routes from coming up.

Workaround: Upgrade the DMI schema to JUNOS 14.2, which causes functional audit to succeed and the routes to come up properly.

- Sometimes, when you attempt to discovery devices from the Connectivity Services Director GUI after the installation of a new image, the "Service is not available due to resource loading, please retry later." message is displayed. This condition occurs because it takes more time than expected for the resources and schema to be loaded from Junos Space Platform. As a result, adequate resources are not available to initiate the discovery of devices.
- For each VPLS service order, multiple entries are created in the Edge Services Director database. This behavior is expected because a service with "n" endpoints creates "n" entries in the ELANVplsConnectivity table of the database and for each endpoint, data is saved separately with different route distinguishers.
- For some fields, such as Interface and LSP Status, that are displayed in the different widgets on the Service Traffic, Service Transport, and Service Summary pages in Monitor mode of the Service view, the values or statuses that are shown are updated based on the polling interval for retrieving data from the devices. As a result, the values or statuses for such fields are reflected in the widgets of the monitoring pages with a delay of a few minutes.
- Tags, which enable you to categorize and organize managed devices, are not supported in Connectivity Services Director. Because tags are not supported, you cannot use tags for provisioning LSPs in cases where an ingress device is a router and an egress device is a device tag, which denotes multiple spokes in a full-mesh or hub-and-spoke topology.
- In a scaled environment with approximately 3000 services configured, it is observed that the size of the file descriptor increases to the range of 16,000 to 17,000 and remains within this range.
- When you edit a service order, you cannot modify the parameters of the MAC Settings and Advanced Settings sections of the service order wizard.
- When you edit a VPLS service order, you cannot modify the device roles. For example, you cannot modify a VPLS spoke to be a P2P spoke.
- You must clear the browser cache when you need to view and work with the VPLS service order pages. Otherwise, the webpage is not loaded properly.
- To view only MX Series routers on the Assign Quick Templates page, you select **MX** from the Device Family list. However, you do not have an option to view only ACX Series routers on the Assign Quick Templates page. You select **Common** from the Device Family list to display all device families, which also includes ACX Series routers.
- The deletion of a service order that is in the decommissioned state fails with the following error message:

An error occurred deleting this service order:

Bad Request org.hibernate.exception.ConstraintViolationException: could not delete: [net.juniper.jmp.provisioning.jpaservices.ServiceElementEntity#1311450

To correct this problem, enter the following commands at the shell prompt to delete the service order on the device associated with the service order (To run shell commands, from the Junos Space Appliance Settings menu, enter **7** at the prompt):

delete from EthernetUni where the service order ID is in the range 1311440–1311445

delete from EthernetUni where the service order ID is in the range 1311466–1311471

- For the discovery of LSPs, Connectivity Services Director creates router profiles on CSD-Topology. Connectivity Services Director uses the same username that it uses to discover devices to discover LSPs. If the user account has privileges for shell access, LSP discovery fails on CSD-Topology. This failure occurs because the CSD-Topology requires the user account to have only CLI-access privilege and not shell-access privilege. Also, if Connectivity Services Director has discovered devices using the root account (with native access), LSP discovery fails on CSD-Topology.

Workaround: Perform the following steps for CSD-Topology to successfully discover LSPs:

1. Initiate an SSH or Telnet session to the CSD-Topology VM external IP address.
2. Modify the following CLI command files to be executed to add the **cli** command before any other command is executed so that access to the CLI shell is obtained. This modification does not impact non-root (non-superuser accounts) because the output of the additional command is ignored. For root users, the CLI shell is invoked first and all other commands (such **show configuration** and **show mpls lsp**) are executed correctly:

```
[root@hostname ~]# /opt/pcs/db/command/juniper.config
[root@hostname ~]# /opt/pcs/db/command/juniper.interface
[root@hostname ~]# /opt/pcs/db/command/juniper.tunnel_path
[root@hostname ~]# /opt/pcs/db/command/juniper.transit_tunnel
```

The contents of the preceding files have the CLI command to be executed on the routers. For example, the original contents of **juniper.config** file are as follows:

```
!Silent
set cli screen-width 0
show config|display inheritance|no-more
```

You must modify this file as follows to include the **cli** command:

```
@P
cli
!P
!Silent
set cli screen-width 0
show config|display inheritance|no-more
```

- In a scaled environment, the Connectivity Services Director application may allow multiple users to modify a large service at the same time from different browsers or machines. As a result you may see more than one instances of a single validated service order.
- On the Service Summary page for VPLS services, the Connections matrix does not show the exact VPLS connection present on the device for all endpoints. This problem

occurs because the remote procedure calls and CLI commands do not return the remote device IP address when the connection is down.

- The monitoring framework polls data from devices based on the serial number of the chassis, rather than the hostname or IP address of the device, which is unique in a network deployment. With the existing monitoring mechanism, when a chassis contains a new serial number, the device chassis is considered a different entity and all historical data (collected for the same host or IP address of the chassis) saved is lost.
- The outer and inner tag protocol IDs that you want to configure in a service definition must be preconfigured on the device associated with the service definition for a successful validation and provisioning of the service order.
- In certain scenarios, such as after an upgrade from Services Activation Director 14.3R1 to Connectivity Services Director Release 1.0, you might observe that alarms related to services are not properly cleared on the Connectivity Services Director GUI. This problem occurs because of the manner in which alarms are transmitted from OpenNMS to Junos Space Platform.

Workaround: Manually clear the appropriate alarm from the Alarm Details page in Fault mode of Service view after examining the alarm and associated events, and taking any action needed to resolve the condition that triggered the event on the corresponding device.

- During creation of a set of a point-to-point service with pseudowires, which are doubly tagged on the ingress router and singly tagged on the egress router, it is observed that an additional VLAN swap operation occurs on the Z side. This is effectively a null operation because both the input and output VLAN IDs are set as 133 in this case. This behavior also occurs with a local-switching service.
- If you attempt to create a service order with a point-to-point LDP service definition, you cannot view the non-editable parameters in service template during service deployment. This problem occurs when you create and publish the service definition with local-stitching by associating it with a service template that contains the circuit cross-connect (CCC) family set, such as **set interfaces xe-0/2/0 unit 0 family ccc**.
- The ILA adapter fails to upgrade if you install the Connectivity Services Director application in a setup where an ILA adapter already exists.

Workaround: Before you install the Connectivity Services Director application you must delete the existing ILA adapter. You can delete the existing ILA adapter at Network Management Platform > Devices > Device Adapter.

- If you migrate from Services Activation Director to Connectivity Services Director Release 2.0R3 or earlier, **Enable Tunnel services** and **Enable Local Switching** parameters cause functional issues.

In order to overcome these issues and maintain consistency across products, in Connectivity Services Director Release 2.0R4, **Enable Tunnel services** and **Enable Local Switching** parameters are renamed **Disable Tunnel services** and **Disable Local Switching** respectively.

As a result of this renaming, you may encounter issues when you are migrating from Connectivity Services Director Release 2.0R2 to Connectivity Services Director Release 2.0R4.

Workaround: Use the Modify Service workflow to modify the service according to the new naming convention. For example, if you prefer to enable tunnel services while modifying the existing service, clear the **Disable Tunnel services** check box.

- In specific cases, in a VPLS service, multiple sites might have same interface, UnitID, and VLAN ID. Any subsequent addition of a site results in a redundant site addition along with the original site. Though deployment is successful extra redundant configuration is pushed to the devices.

Workaround: Perform the following steps:

1. Disable deploy to device.
2. Delete one UNI which is duplicate and deploy the service order.
3. Delete the other UNI and deploy again.
4. Add the required UNI and deploy.
5. Enable deploy to device.

New and Changed Features

This section lists the new features in Connectivity Services Director, Release 2.1R1.

- **Support for configuring both BGP and OSPF protocols in a single service**—Starting with Connectivity Services Director Release 2.1R1, you can configure both BGP and OSPF protocols in a single service. In earlier releases, you can choose either BGP or OSPF for a single service.

To configure BGP and OSPF protocols on the service order, select the **BGP/OSPF/Static** option from the Routing Protocol list while creating the service definition. You can see both BGP and OSPF configuration settings in the Service Settings page of the Create Layer 3 VPN service order wizard. You can configure these protocols on the Node Settings page and Site Settings page.

- **Enhancements to service recovery feature**—In Connectivity Services Director Release 2.1R1, you can use the Force Upload feature to overwrite the service definitions that were recovered using the service recovery feature and do not contain the changes made through CLI configuration or through templates. You do this by creating a service definition containing templates that matches the configuration, and uploading it to the Connectivity Services Director application.

In Connectivity Services Director Release 2.0 and earlier, you cannot recover changes made to service definitions through CLI configuration or through templates.

- **Community support for static routes**—In Connectivity Services Director Release 2.1R1, you can configure static routes by adding **next-table** and **community** as option types. You use the community option type to advertise a static route. In earlier releases, you can configure static routes only by adding the next-hop option type.

You can configure a static route while creating a service order by adding either a next-hop or a next-table option type, and a community option type on the Node Settings page.

- **IP address block size restriction removed**—In Connectivity Services Director Release 2.1R1, you can configure the block size using a much wider range from 1 through 32. In earlier releases, you can allocate an IP address block size only in the range 24 through 32.

You can set an IP address block size when you add a new IP pool.

- **Support for 4-byte AS number**—Connectivity Services Director Release 2.1R1 supports a mix of both 2-byte and 4-byte AS numbers. In earlier releases, you can set only a 2-byte AS number that provides a pool of 65,536 AS numbers. With this enhancement, you can either use the **Auto Pick Route Target** check box to automatically pick a route target, or manually enter an AS number in the **Route Target** field in the range 1 through 4,294,967,296.
- **Managing resources based on pool type**—Starting in Connectivity Services Director Release 2.1R1, you can view and manage a particular pool of resources by selecting an option from the **Pool Type** list. The **Manage Resource** page displays the list of resource pools that can be configured. You can filter the resources displayed on this page by device name, by interface name, or by customer. The page also displays the status of various other resources such as VLAN IDs, virtual circuit IDs, route distinguisher, and route targets that are created for utilization in services.

Known Issues

The following are the known issues in Connectivity Services Director Release 2.1R1. For each entry, the identifier in the PR Number column of [Table 2 on page 28](#) is the tracking number in the Juniper Networks problem report (PR) tracking system.

Table 2: Known Issues in Connectivity Services Director Release 2.1R1

PR Number	Problem Description
1241543	On the Create Service Definition page, the upper limit of MTU is limited to 9216. Workaround: None at present.
1248119	While you are modifying a VPLS service, you cannot search on the Site Settings page for an endpoint that is not associated with the service. Workaround: None at present.
1255682	An Ethernet interface, which is a part of an aggregated Ethernet, is listed as user-to-network interface (UNI). Workaround: None at present.
1259449	For a modified RSVP LSP service, the View Configuration Change page displays only the modified configuration instead of the displaying the entire configuration. Workaround: To view the entire configuration, you must force-deploy the RSVP LSP service.

Table 2: Known Issues in Connectivity Services Director Release 2.1R1 (*continued*)

PR Number	Problem Description
1255005	<p>If a service template has multiple MD5 key-value rows with different default values and if you attach this service template to a Layer 3 VPN service, the Template Configuration page displays the same default value for each MD5 key-value row.</p> <p>Workaround: While you are creating a service you can modify the default values for each MD5 key-value row.</p>
1282178	<p>You cannot modify a service without modifying at least one endpoint.</p> <p>Workaround: From the Service Settings tab, modify the comment and UNI description of any of the endpoint and deploy the service.</p>
1257293	<p>In VPLS Service, you cannot search a service by its description. This is because the Connectivity Services Director application does not support searching a service by service description. There is currently no workaround.</p>
1287027	<p>Service templates are not recovered if they do not contain the complete hierarchy for the attributes or statements that are configured.</p> <p>Workaround: Re-create the templates by providing the complete hierarchy. The Connectivity Services Director application needs this information to recover and manage the templates.</p>
1290708	<p>Some interfaces are listed incorrectly in both NNI and UNI tabs. There is currently no workaround.</p>
1294235	<p>The service recovery process does not recover unmanaged device details such as loopback IP address and UNI interface if one of the endpoints is configured as unmanaged. There is currently no workaround.</p>
1295268	<p>If you allocate an IP address with a suffix less than 18 to a site in an Layer 3 VPN service, then IP address allocation is not done properly.</p> <p>For IP addresses to be assigned properly, you must allocate an IP address suffix that is greater than 18.</p> <p>There is currently no workaround.</p>
1298805	<p>If nodes having the same route distinguisher value are deleted from a service, then the route distinguisher value is not deleted from the service. There is currently no workaround.</p>
1299605	<p>If a new node along with path is added during modification of an RSVP full mesh service definition that has a custom pattern, then an additional LSP configuration is added to the newly added device.</p> <p>Workaround: Modify the RSVP full mesh service and add a new node without path information. Modify the service and add the path information.</p>
1299976	<p>vlan-list configuration is not pushed to devices that has VLAN normalization configured.</p> <p>Workaround: Use templates to configure vlan-list instead of vlan-range.</p>
1299969	<p>The ACX5000 line of routers do not support the vlan-id all configuration. There is currently no workaround.</p>

Table 2: Known Issues in Connectivity Services Director Release 2.1R1 (*continued*)

PR Number	Problem Description
1300966	<p>If you try to create a Layer 3 VPN service order with loopback configuration on Junos Space Platform Release 16.1, 17.1, or 17.2, then the service order creation job fails.</p> <p>Workaround: When you deploy a loop back interface, attach a template containing loop back configuration to the service order.</p>

Resolved Issues

The following issues are resolved in Connectivity Services Director Release 2.1R1. For each entry, the identifier in the PR Number column of [Table 3 on page 30](#) is the tracking number in the Juniper Networks problem report (PR) tracking system.

Table 3: Resolved Issues in Connectivity Services Director Release 2.1R1

PR Number	Problem Description
1262213	Transit service applied BGP prefix limit to the BGP protocol instead of applying it to the peer group.
1262216	You cannot specify a BGP authentication key for a peer having an IPv4 or an IPv6 address from the Connectivity Services Director application.
1262678	The OSPF domain ID is rejected with the message Value does not contain a valid AS number prefix of range 1 - 65536.
1263598	<p>Connectivity Services Director displayed the following error message when an existing P2P service order is modified and submitted:</p> <p>Provider VlanId not modifiable in Service. Interface xe-0/2/8(3866879).</p>
1264686	The CoS template created from Connectivity Services Director 2.0R5 was not applied on all devices on Layer 3 VPN.
1264687	The status of services is displayed as Down for all services on the Service Summary page.
1267718	The routing instance configuration is present on devices even after the services are removed.
1272976	Connectivity Services Director Release 2.0R4 identifies NNI as UNI a during prestage job.
1274579	The View Physical Inventory page incorrectly shows the slots in MX104 router as empty.
1275828	If you try to select endpoints to set up services on an MX104 router, the interface are unavailable.
1280320	The device status in Junos Space Network Management Platform appears as In-Sync, while the devices in Connectivity Services Director display the status as Out Of Sync.
1271581	If a service order decommission job in Scheduled state is canceled following a server restart, then the service order cannot be deleted from the system.

Table 3: Resolved Issues in Connectivity Services Director Release 2.1R1 (*continued*)

PR Number	Problem Description
1247227	A generic error message is displayed if the deployment of a VPLS service with Traffic Type as Transport VLAN fails. The generic error message must be replaced with the following appropriate error message: Specify CVLAN start and CVLAN end values.
1238027	Connectivity Services Director fails to recover a service if the Route Target or Route Distinguisher values contain the letter L".
1244763	In the Topology view, the status of Layer 3 links is not dynamically updated.
1258324	In the Topology view, optical inline amplifiers (ILAs) are displayed on optical links only after a delay of 15 seconds.
1257863	While modifying a Layer 3 VPN service, if you select a device to associate a policy with it, the policy is listed only if you have associated the policy with a device at the time of policy creation.
1243315	A device you deleted while modifying a Layer 3 VPN service appears on the Create Policy page.
1250579	If you modify the ASN value on a device, then the new ASN value is not updated in the Connectivity Services Director application.

Finding More Information

For the latest, most complete information about known and resolved issues with Junos Space Network Management Platform and Junos Space Management Applications, see the Juniper Networks Problem Report Search application at: <http://prsearch.juniper.net>.

Juniper Networks Feature Explorer is a Web-based application that helps you to explore and compare Junos Space Network Management Platform and Junos Space Management Applications feature information to find the correct software release and hardware platform for your network. Find Feature Explorer at: <http://pathfinder.juniper.net/feature-explorer/>.

Juniper Networks Content Explorer is a Web-based application that helps you explore Juniper Networks technical documentation by product, task, and software release, and download documentation in PDF format. Find Content Explorer at: <http://www.juniper.net/techpubs/content-applications/content-explorer/>.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation. You can provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience.

Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.

- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software version (if applicable).

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or Partner Support Service support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at <http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf>.
- Product warranties—For product warranty information, visit <http://www.juniper.net/support/warranty/>.
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <https://prsearch.juniper.net/>
- Find product documentation: <http://www.juniper.net/documentation/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>
- Search technical bulletins for relevant hardware and software notifications: <http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum: <http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: <https://entitlementsearch.juniper.net/entitlementsearch/>

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at <http://www.juniper.net/cm/>.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see <http://www.juniper.net/support/requesting-support.html>.

Revision History

16 August, 2017—Revision 1—Junos Space Connectivity Services Director 2.1R1.

Copyright © 2017 Juniper Networks, Inc. All rights reserved.

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. and/or its affiliates in the United States and other countries. All other trademarks may be property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.