

Junos Space Connectivity Services Director Release 2.2R1 Release Notes

9 April, 2018

Contents

Introduction	2
Release Notes for Connectivity Services Director 2.2R1	2
Supported Platforms	2
Junos Space Network Management Platform Requirements for Connectivity Services Director 2.2R1	3
Operational Notes	4
Known Limitations	6
New and Changed Features	13
Known Issues	14
Resolved Issues	14
Finding More Information	17
Documentation Feedback	17
Requesting Technical Support	18
Self-Help Online Tools and Resources	18
Opening a Case with JTAC	18
Revision History	19

Introduction

These Release Notes accompany Release 2.2 of the Juniper Networks Junos Space Connectivity Services Director. They contain information about new and changed features, limitations, and known and resolved issues in the software.

Release Notes for Connectivity Services Director 2.2R1

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 2.2R1 are available at: [Junos Space and Junos Space Connectivity Services Director Download](#).

- [Supported Platforms on page 2](#)
- [Junos Space Network Management Platform Requirements for Connectivity Services Director 2.2R1 on page 3](#)
- [Operational Notes on page 4](#)
- [Known Limitations on page 6](#)
- [New and Changed Features on page 13](#)
- [Known Issues on page 14](#)
- [Resolved Issues on page 14](#)

Supported Platforms

[Table 1 on page 3](#) lists the supported platforms for Connectivity Services Director Release 2.2R1 and the corresponding qualified Junos OS releases.

Table 1: Supported Platforms and the Software Versions for Connectivity Services Director Release 2.2R1

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 Release 17.4R1
MX Series 3D Universal Edge Routers	Release 12.2R1 through Release 17.4R1.16 for MX80, MX104, MX240, MX480, and MX960 routers Release 13.3R1 through Release 17.4R1.16 for MX2010 and MX2020 routers Release 18.1R1 for MX10003, MX2008, MX204, and MX150 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 Release 15.1R6.7 for M10 routers
PTX Series Packet Transport Routers	Release 13.2R2.2 through Release 17.4R1 for PTX3000 routers Release 13.2R1.7 through Release 17.4R1 for PTX5000 routers
Virtual MX Routers (vMX)	Release 14.1R5 through Release 17.4R1.16

Junos Space Network Management Platform Requirements for Connectivity Services Director 2.2R1

You can install Connectivity Services Director in a Junos Space Virtual Appliance or the JA2500 Junos Space Appliance. The Junos Space Virtual Appliance can be deployed on a VMware ESXi server. The Junos Space Virtual Appliance requires a VMware ESXi server 5.5, 6.0, or 6.5 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
- 250-GB hard disk

For detailed information about deploying Junos Space Virtual Appliance, see [Junos Space Virtual Appliance Installation and Configuration Guide](#).

For detailed information about installing and upgrading CSD, see [Connectivity Services Director Quick Start Guide](#).

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.

- 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.

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.
- 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.
- 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 discover 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 Connectivity 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 point-to-point 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.
- Deletion of a decommissioned service order results in a 'ConstraintViolation' exception. The following error message is displayed:

An error occurred deleting this service order:

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

Workaround: Use the following command to manually delete the related EthernetUnis of the service order from the EthernetUni table in the database:

delete from EthernetUni



NOTE: Enter the **delete from EthernetUni** command at the shell prompt of the Junos Space Platform. To run shell commands on a Junos Space Virtual Appliance, enter 7 in the Junos Space Settings menu.

- 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

There are no new features in this release.

Known Issues

This section lists the known issues in Connectivity Services Director Release 2.2R1. For the most complete and latest information about known Junos Space Connectivity Services Director defects, use the Juniper Networks online [Problem Report Search application](#).

- While upgrading Connectivity Services Director Release 2.1, installed on Junos Space Platform Release 17.1R1, to Connectivity Services Director Release 2.2, installed on Junos Space Platform Release 17.2R1 or Release 18.1R1, the upgrade job goes to InProgress state and never completes. [PR 1345732]

Workaround: A timeout is introduced in the CSD installation script. As a result, the upgrade of Connectivity Services Director, from Release 2.1 to Release 2.2 is completed. However, you must restart jboss by executing the following commands after the upgrade job is completed:

Service jmp-watchdog stop

Service jboss-dc stop

Service jboss stop

Service jmp-watchdog start

Resolved Issues

This section lists the resolved issues in Connectivity Services Director Release 2.2R1. For the most complete and latest information about resolved Junos Space Connectivity Services Director defects, use the Juniper Networks online [Problem Report Search application](#).

- You cannot navigate to the Site Settings page when modifying a Layer 3 VPN service, if policies are attached to the nodes. [PR 1256023]
- While trying to delete the customer IP address pool, the **Delete** button is not getting enabled. [PR 1303698]
- Different policy attributes are added to the same term, even when the term names are different. [PR 1306215]
- The **VLAN** field is not retained in the Site Settings page when the **OK** button is clicked. [PR 1312862]
- A template created in Services Activation Director cannot be deployed to a device from Connectivity Services Director because of a limitation of the Route Preference value. [PR 1314776]
- A service created in one Connectivity Services Director server cannot be recovered from another Connectivity Services Director server. [PR 1314903]
- While creating a VPLS service order by using a default VPLS Service Definition, the **Instance Type** and **Protocol** fields have no default values specified. [PR 1316632]

- When creating a service order, Connectivity Services Director does not accept the device configuration if at least one Juniper Networks device is not defined as a hub. [PR 1324706]
- The Tag Protocol Identifier (TPID) is associated with an endpoint even after the TPID is removed from a VPLS service definition. [PR 1329037]
- You cannot create a service order with an integrated routing and bridging interface and static protocol route. [PR 1331545]
- API queries for the number of interfaces used in a Layer 3 VPN service return inconsistent results. [PR 1337575]
- You cannot deactivate a VPLS service that has an interface with a different unit and VLAN ID. [PR 1340453]
- The class-of-service profile configuration is removed from a site on which BGP service is configured with hub and spoke roles, when the site type is changed from hub to spoke or vice versa. [PR 1341499]
- While creating a VPLS service, the VLAN ID cannot be edited from the Site Settings page. Instead, the existing VLAN ID is deleted if the description is updated. [PR 1344037]
- While creating a Layer 3 VPN service with policy, a new term cannot be inserted above a selected policy term. [PR 1313422]
- While creating a Layer 3 VPN service, the service name is not displayed on the Service View pane. [PR 1335873]
- When a device is deleted, the services associated with that device are not deleted. [PR 1341350]
- You cannot create a VPLS service with an IRB interface. [PR 1344115]
- While modifying a VPLS service with TPID configured, the **inner TPID** and **outer TPID** fields are editable. [PR 1345103]
- After modifying an LSP service, only the modified endpoints are listed on the LSP Service Details page. [PR 1345431]
- After an LSP service is modified, the LSP Modify page displays only the last updated egress nodes. [PR 1345444]
- When a service is created by using a customer-specific service definition, all the required configurations are not sent to the device. [PR 1301386]
- The VLAN maps are applied to point-to-point services even though the **VLAN maps for P2P services** option is not selected. [PR 1321984]
- While creating an L2 or L3 service, duplicate UNIs are created on devices. [PR 1330735]
- While creating an LSP service, the name of a decommissioned service cannot be assigned to the new service. [PR 1343812]
- Connectivity Services Director incorrectly allows users to select SRX Series devices during provisioning of LSP services. [PR 1344119]
- Connectivity Services Director should allow a minimum packet size of 100 bytes instead of 1 byte for MPLS LSP ping. [PR 1344124]

- When a point-to-multipoint service is modified by deleting a node and adding another node, the service order details show only the newly added node. Existing nodes in the service are not displayed. [PR 1343805]
- Connectivity Services Director accepts values for the Adjust Interval parameter only up to 2,147,483,647, while devices accept values up to 315,360,000. [PR 1340156]
- While creating a VPLS service order, when the 802.1Q tagging is selected, the **Inner TPID** field should not be editable. [PR 1342523]
- All the discovered devices listed on the Node Settings page are not listed on the Prestage Devices page while creating a service. Also, the devices qualified for the N_PE role are shown as qualified for the P role. [PR 1344033]
- Functional Audit fails for a Layer 3 VPN Service if VRF table label and Enable Auto export routes options are set to **Editable in service order** in an L3 VPN service definition. [PR 1344995]
- No results are displayed under the **Audit Results** tab in the Configuration Audit window, when point-to-point spoke is associated with neighbor and backup neighbor in a hub-and-spoke BGP service. [PR 1343143]
- A term or clause cannot be deleted from a Layer 3 VPN service policy. [PR 1313419]
- On the Create Service Definition page, the upper limit of MTU is 9216. [PR 1241543]
- While modifying a VPLS service, you cannot search on the Site Settings page for an endpoint that is not associated with the service. [PR 1248119]
- An Ethernet interface, which is a part of an aggregated Ethernet, is listed as a user-to-network interface (UNI). [PR 1255682]
- For a modified RSVP LSP service, the View Configuration Change page displays only the modified configuration instead of displaying the entire configuration. [PR 1259449]
- 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. [PR 1255005]
- You cannot modify a service without modifying at least one endpoint. [PR 1282178]
- In a 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. [PR 1257293]
- Service templates are not recovered if they do not contain the complete hierarchy for the attributes or statements that are configured. [PR 1287027]
- Some interfaces are listed incorrectly in both NNI and UNI tabs. [PR 1290708]
- 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. [PR 1294235]
- If you allocate an IP address with a suffix less than 18 to a site in a Layer 3 VPN service, then IP address allocation is not done properly.

For IP addresses to be assigned properly, you must allocate an IP address suffix that is greater than 18. [PR 1295268]

- If nodes having the same route distinguisher value are deleted from a service, then the route distinguisher value is not deleted from the service. [PR 1298805]
- 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. [PR 1299605]
- **vlan-list** configuration is not pushed to devices that have VLAN normalization configured. [PR 1299976]
- The ACX5000 line of routers do not support the **vlan-id all** configuration. [PR 1299969]
- 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. [PR 1300966]

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

Revision History

9 April, 2018—Revision 1—Junos Space Connectivity Services Director 2.2R1.

Copyright © 2018 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.