Upgrade Software on Headend and Branch

For supported software information, click here.

This article describes how to upgrade the software on the headend components—the Director, the Analytics, and the Controller nodes—and on Versa Operating System^{TM} (VOS^{TM}) branch devices.

When you upgrade the software on the headend components, you must ensure that at the end of the upgrade process, the same software version is running on all the headend components. The software running on VOS branch devices can be the same version as that running on the headend components, or it can be a lower (earlier) version.

To ensure that the software upgrade proceeds smoothly and to ensure minimum disruption to an operational network, perform a software upgrade in the following order. If you are upgrading the software on the headend components only and not on any of the VOS hub or branch devices, you can ignore the steps that apply to hub or branch VOS devices.

1. Upgrade the Director node—First, make a full backup of the Director node. Then upgrade the standalone node or the HA-enabled nodes.

Note: In Release 22.1.4, you must upgrade the Analytics node first, then upgrade the Director node.

2. Upgrade the Analytics node—Next, upgrade the Analytics node. Note that the Analytics log files are automatically archived.

Note: In Release 22.1.4, you must upgrade the Analytics node first, then upgrade the Director node.

3. Upgrade the Controller node—A Controller node is simply a VOS device acting as a Controller, so the Controller software upgrade procedure is the same as for upgrading a VOS device. In a multicontroller environment, start by upgrading only one of the Controller nodes.
4. For a hub-and-spoke topology, upgrade the active hub, following the VOS upgrade procedure.
5. For branch sites that have redundant (HA) VOS devices, upgrade the active VOS device at each site.
6. Upgrade the remaining Controller nodes.
7. For a hub-and-spoke topology, upgrade the remaining hubs.
8. Upgrade the remaining branch VOS devices.
9. Check that the upgrade Director node can connect to and manage branches that are running the same software version as the Director node.
10. Check that the upgraded Director node can connect to and manage existing branches that are running a software version that is older than the software running on the Director node.
11. Check that VOS devices whose software you have upgraded can communicate with the branches whose software

has not been upgraded.

Before you begin a software upgrade, check the release notes for the software release to which you are upgrading to determine whether you need to perform any additional steps before or during the upgrade. For example, for some upgrades you may need to install OS SPacks before beginning the upgrade.

To find the link to the latest software, go to the Versa Networks Customer Support website and then select the General > SD-WAN Software folder.

Note that to upgrade the software on headend components, you can upgrade from and to the same Ubuntu base operating system. That is, you can upgrade components running Ubuntu 18.04 (Bionic) to another Bionic image, and you can upgrade components running Ubuntu 14.04 (Trusty) to another Trusty image.

Note that if a power interruption occurs during the software upgrade process, the affected device may end up in an inconsistent state, and manual intervention would likely be required to recover. For assistance, you can contact Versa Networks Customer Support.

Upgrade a Standalone Director Node

This section describes how to upgrade the software on a standalone Director node. Before you upgrade the software, you must do the following:

- Perform a full backup of the Director node.
- Download the latest OS security packages (OS SPacks) to the Director node.
- Run an upgrade validation script to identify all the configuration discrepancies and fix them before the upgrade.

Then you upload the software image to the Director node and you upgrade the software.

To install or upgrade to the Director software for Releases 21.2 and later, the Director node, whether a virtual machine (VM) or a bare-metal server, must have a minimum of 150 GB of disk space.

Back Up the Director Node

Before you upgrade the Director software, make a full backup of the Director node:

```
admin@Director$ cli
admin@Director> request system recovery backup
admin@Director> exit
admin@Director$
```

Download the Latest OS SPacks

Before you upgrade to Release 21.2 or later, you must upgrade the OS security package (OS SPack) on the Director node to the latest version. You can find the latest OS SPacks at https://versanetworks.app.box.com/v/osspack or https://upload.versa-networks.com/index.php/s/nEkF9xOO3e7BA9Z. If you do not upgrade the OS SPack, the software upgrade may fail.

To install the OS SPack:

```
admin@Director$ chmod +x ./versa-director-osspack-date.bin
admin@Director$ sudo ./versa-director-osspack-date.bin
```

The following error may display when you upgrade from Release 16.1R2 to Release 21.2 or later from the Versa Director CLI:

```
admin@Director> request system package upgrade package-name
Will restart Versa Director (all processes). Are you sure? [no,yes] yes
Verify package checksum..
status Some of the packages on this system are not correctly installed, please resolve before upgrading Versa
Director
Desired=Unknown/Install/Remove/Purge/Hold| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-
aWait/Trig-pend|/ Err?=(none)/Reinst-required (Status,Err:uppercase=bad) ||/
Name  Version         Architecture                                     Description
================================================================================================
rc    amd64-microcode  3.20180524.1~ubuntu0.14.04.2+really20130710.1ubuntu1 amd64 Processor microcode
firmware for AMD CPUs
rc    intel-microcode  3.20180807a.0ubuntu0.14.04.1                     amd64 Processor microcode firmware for
Intel CPUs
```

To resolve this error, run the following commands to manually remove the offending packages from Linux shell before you attempt to upgrade the Director node from CLI again:

```
admin@Director$ sudo dpkg --purge amd64-microcode
admin@Director$ sudo dpkg --purge intel-microcode
```

Validate the Director Node Configuration

Before you upgrade to Release 20.2.2 or later, you must install a validation script on the Director node to identify all configuration discrepancies and fix them before you upgrade the Director node. To create the validation script, you download and run the versa-director-pre-upgrade-check.bin file, which creates the validation script, validate.py. Then, you run the validation script from the active Director node. (Note that in releases prior to Release 20.2.2, the versa-director-pre-upgrade-check.bin file was called versa-director-patch-*release*.bin.)

To install and run the upgrade validation script:

1. Download the versa-director-pre-upgrade-check.bin script from the Versa Director software release folder.
2. Run the script from the Director Linux shell. This script creates the validation script, validate.py, and places it in the /opt/versa/vnms/upgrade/scripts directory.

   ```
   admin@Director$ chmod +x ./versa-director-pre-upgrade-check.bin
   admin@Director$ sudo ./versa-director-pre-upgrade-check.bin
   ```

3. Run the validation script from the Director node. If you are upgrading to Release 22.1, issue the following command:

```
admin@Director$ sudo -E /opt/versa/vnms/upgrade/scripts/validate.py -n director-package.bin
```

If you are upgrading to an earlier release, issue the following command:

```
admin@Director$ sudo /opt/versa/vnms/upgrade/scripts/validate.py -f current-release -t new-release
```

For example, to upgrade from Release 21.1 to Release 21.2:

```
admin@Director$ sudo /opt/versa/vnms/upgrade/scripts/validate.py -f 21.1 -t 21.2
```

If the validation script is successful, the console shows the following output:

```
INFO - Pre-Upgrade Validation Initiated
INFO - Executing validation script: ha-pair-config-validation.py ...
INFO - Successfully executed ha-pair-config-validation.py
INFO - Executing validation script: auth-connector-validation.lua ...
INFO - Successfully executed auth-connector-validation.lua
INFO - Executing validation script: org-validation.py ...
INFO - Successfully executed org-validation.py
INFO - Executing validation script: ip-address-config-validation.py ...
INFO - Successfully executed ip-address-config-validation.py
```

If the validation script identifies incorrect configurations, the script displays error messages on the console and logs details to the /var/log/vnms/upgrade.log file. Fix all the incorrect configurations before you upgrade the software on the Director node.

The following sample console output shows error messages display because of a validation failure:

```
admin@Director$ sudo /opt/versa/vnms/upgrade/scripts/validate.py -f 20.2 -t 21.2
INFO - Pre-Upgrade Validation Initiated
Pre-Upgrade Validation Initiated
INFO - Executing validation script: auth-connector-validation.lua ...
Executing validation script: auth-connector-validation.lua ...
ERROR - Errors encountered during execution of auth-connector-validation.lua
Errors encountered during execution of auth-connector-validation.lua
INFO - Executing validation script: ha-pair-config-validation.py ...
Executing validation script: ha-pair-config-validation.py ...
INFO - Successfully executed ha-pair-config-validation.py
Successfully executed ha-pair-config-validation.py
INFO - Executing validation script: org-validation.py ...
Executing validation script: org-validation.py ...
INFO - Successfully executed org-validation.py
Successfully executed org-validation.py
INFO - Executing validation script: ip-address-config-validation.py ...
Executing validation script: ip-address-config-validation.py ...
INFO - Successfully executed ip-address-config-validation.py
Successfully executed ip-address-config-validation.py
ERROR - Validation failed for following scripts: auth-connector-validation.lua
Validation failed for following scripts: auth-connector-validation.lua
```

The following snippet from the /var/log/vnms/upgrade.log file explains the failure reported by the output above:

```
13-March-2021, 10:05:10 __main__ [INFO] Executing validation script: auth-connector-validation.lua ...
13-March-2021, 10:05:10 __main__ [DEBUG] Executing command su root -c "source /etc/profile.d/versa-profile.sh && /opt/versa/util/runlua -n confd -e confu /opt/versa/vnms/upgrade/validate/scripts/auth-connector-validation.lua"
13-March-2021, 10:05:10 __main__ [DEBUG] Command Output of auth-connector-validation.lua" is
13-March-2021, 10:05:12 __main__ [DEBUG] DEBUG badly formatted or nonexistent path - Bad path element "radius-server-details" after: /nms/provider/auth-connectors/auth-connector
13-March-2021, 10:05:12 __main__ [DEBUG] secret is not configured for authentication connector Name versaAuth Type radius
13-March-2021, 10:05:12 __main__ [DEBUG] Command exit status/return code is 1
13-March-2021, 10:05:12 __main__ [ERROR] Errors encountered during execution of auth-connector-validation.lua
```

The validation script runs automatically as the first step in the software upgrade. If the validation fails, the upgrade aborts immediately. If the following error is displayed while upgrading to Release 21.2 using Versa Director CLI, refer to the validation error mitigation guide or contact Versa Networks Customer Support:

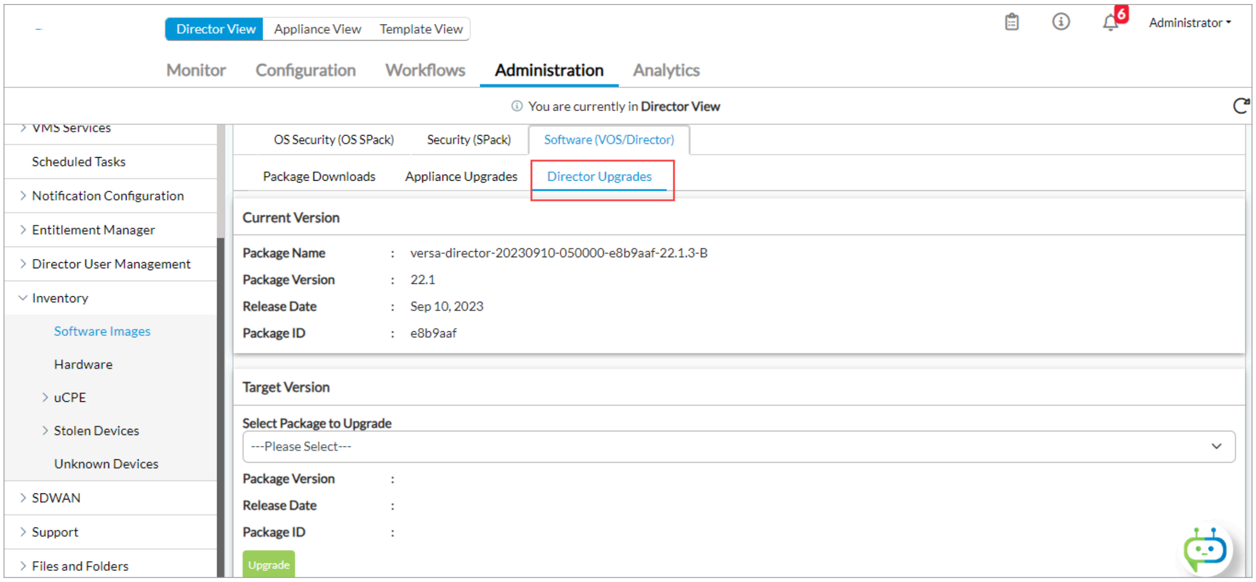
```
admin@Director> request system package upgrade package-name
Will restart Versa Director (all processes). Are you sure? [no,yes] yes
Pre-Upgrade Validation Initiated
Executing validation script: org-validation.py …
Successfully executed org-validation.py
Executing validation script: ip-address-config-validation.py …
Errors encountered during execution of ip-address-config-validation.py
Executing validation script: auth-connector-validation.lua …
Successfully executed auth-connector-validation.lua
Executing validation script: ha-pair-config-validation.py …
Successfully executed ha-pair-config-validation.py
Validation failed for following scripts: ip-address-config-validation.py
Pre-Upgrade-Validation Failed.
Please refer to /var/log/vnms/upgrade.log for more details.
```

Upgrade the Director Software

Note that if you are prompted to provide the username and password for the peer node while upgrading HA, you must provide credentials for a user with either the ProviderDataCenterSystemAdmin role, or any custom role with the HA_MANAGEMENT privilege and Update action. For standby IP address, use 127.0.0.1 when disabling HA on a standalone Director node; otherwise, use the HA management IP address of the standby Director node.

For Releases 22.1.1 and later, to upgrade a software image file on a Director node:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Inventory > Software Images in the left menu bar.
3. Select the Software (VOS/Director) tab, and then select the Director Upgrades tab. The Package Version column in the table displays information about the software package that is installed on the Director node.



Current Version

Package Name : versa-director-20230910-050000-e8b9aaf-22.1.3-B
Package Version : 22.1
Release Date : Sep 10, 2023
Package ID : e8b9aaf

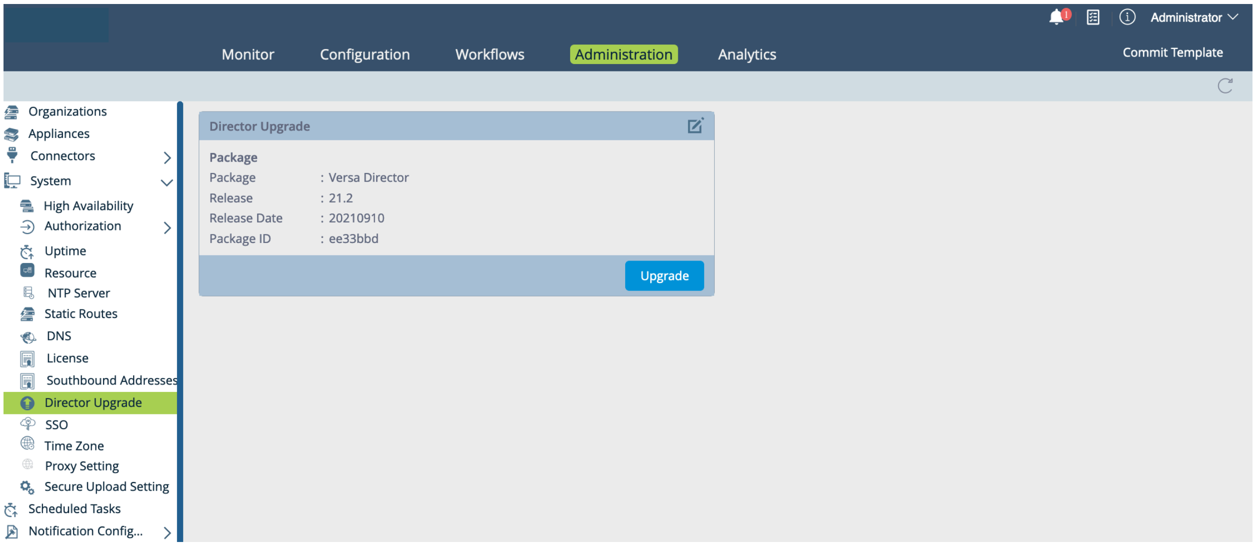
Target Version

Select Package to Upgrade
---Please Select---
Package Version :
Release Date :
Package ID :

4. In the Target Version box, in the Select Package to Upgrade field, select the package to which to upgrade the Director node.
5. Click Upgrade.

For Releases 21.2 and earlier, to upgrade a software image file on a Director node:

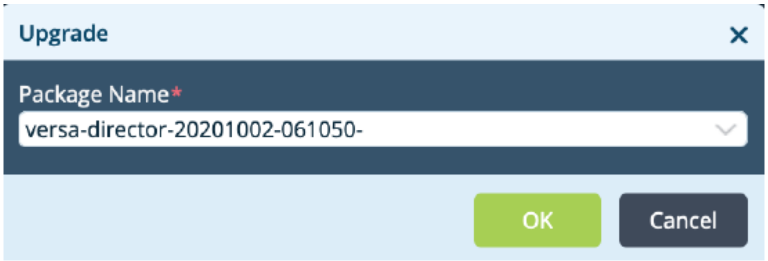
1. In Director view, select the Administration tab in the top menu bar
2. Select System > Director Upgrade in the left menu bar. The main pane display the Director Upgrade pane.



Director Upgrade

Package
Package : Versa Director
Release : 21.2
Release Date : 20210910
Package ID : ee33bbd

3. Click the Edit icon. In the Upgrade popup window, select the software package name:


Upgrade

Package Name*

versa-director-20201002-061050-

4. Click OK.
5. Click Upgrade.

Upgrade from the Director CLI

1. Upload the software image to the Director repository. You can do this from the Director CLI or manually.

   - To use the Director CLI, issue the following command.

     > admin@Director> **request system package fetch uri** *url*

     For example:

     > admin@Director> **request system package fetch uri http://10.167.57.1/Builds/VOAE/21.2.2/versa-director-20151126-094545-a532d5d-21.2.2.bin**
     > status
     > Package Saved

   - To upgrade manually:

     a. Upload the Director image using the **scp** (**ssh**) command from your Linux or Mac device.

        > **scp versa-director-20***xxxxxxxxx***.bin Administrator@***director-ip-address***:**

        For example:

        > **scp versa-director-2020240208-092811-0583692-22.1.3-B.bin Administrator@1.2.3.4:**

     b. Move the image to the directory that contains the Versa Director images. For example:

        > **mv versa-director-20240208-092811-0583692-22.1.3-B.bin /var/versa/packages/vnms/**

2. Verify that the software image has been uploaded:

   > admin@Director> **request system package list**

   For example:

   > admin@Director> **request system package list**

```
packages
{
   name versa-director-20151126-002132-0ebe99d-21.2.2.bin
}
packages
{
   name versa-director-20151126-094545-a532d5d-21.2.2.bin
}
```

3. Upgrade the software:

   ```
   admin@Director> request system upgrade package image-filename
   Will restart Director (all processes). Are you sure? [no,yes] yes
   ```

   For example:

   ```
   admin@Director> request system upgrade package
   versa-director-20151126-094545-a532d5d-21.2.2.bin
   Will restart Director (all processes). Are you sure? [no,yes] yes
   ```

To monitor the progress of the software upgrade, issue the following command:

```
admin@Director$ tail -f /var/log/vnms/upgrade.log
```

Note: While the upgrade is in progress, you may see a message that a system reboot is required. You must wait until the upgrade process is completed before you reboot the system. When the upgrade is completed, the screen output displays a message that the upgrade was successful, as shown in the following sample output:

```
27–April-2024, 10:05:12 __main__ [INFO] Upgrade to director-director-201210910-171209.bin successful!
```

When the upgrade is completed, reboot the standalone Director node.

Upgrade HA-Enabled Director Nodes

This section describes how to upgrade HA-enabled Director nodes. Before you update the Versa Director software on HA-enabled nodes, you must perform the following tasks:

- Perform a full backup of the Director software.
- Verify that the primary (active) and standby Director nodes are operating in the proper mode and that HA is enabled.
- Download the latest OS security packages (OS SPacks) on the primary and standby Director nodes.
- Run an upgrade validation script to identify all the configuration discrepancies and fix them before the upgrade.

Note: When you upgrade HA-enabled Director nodes, if you see the message, "Disable HA before upgrading director to 22.1.*x*", you must disable HA and then re-enable it after the upgrade of both the active and standby Director nodes.

To install or upgrade to the Director software for Releases 21.2 and later, each Director node, whether a virtual machine

(VM) or a bare-metal server, must have a minimum of 150 GB of disk space.

Back Up the Director Node

Before you upgrade the Director software, make a full backup of the Director node:

```
admin@Director1> request system recovery backup
```

Verify the Director Node Operating Mode

To verify that the primary (active) and standby Director noes are operating in the proper modes and that HA is enabled:

1. Ensure that the same software version is running on the primary and standby Director nodes:

   ```
   admin@Director1> show system package-info

   admin@Director2> show system package-info
   ```

2. Check that the primary Director node is in master mode. In the following example, the line "mode master" under "vnmsha-details" indicates that the primary Director is in master mode. (The "mode slave" line under "peer-vnmsha-details" shows the mode for the peer Director node, which is the standby.)

   ```
   admin@Director1> request vnmsha actions get-vnmsha-details fetch-peer-vnmsha-details true
   status SUCCESS
   vnmsha-details {
       mgmt-ip-address 10.192.36.170
       enabled true
       designated-master true
       mode master
       peer-vnmsha-details {
          peer-vnmsha-detail {
              mgmt-ip-address 10.192.36.171
              enabled true
              designated-master false
              mode slave
          }
       }
   }
   ```

   You can also check the Director mode by issuing the following command:

   ```
   admin@Director1> request vnmsha actions get-vnmsha-postgres-status
   ```

   The Role column in the command output shows "primary" for the primary Director node. For example:

   ```
   admin@Director1> request vnmsha actions get-vnmsha-postgres-status

   status ID | Name              | Role      | Status      | Upstream        | Location | Connection string
   ----------+-------------------+-----------+-------------+-----------------+----------+--------------------------------------------
   1         | director-node1    | primary   | * running   |                 | default  | host=10.192.36.170 user=repmgr
   ```

```
dbname=repmgr
2        | director-node2    | standby   | running     | director-node1  | default  | host=10.192.36.171
user=repmgr dbname=repmgr
```

3. Check that the standby Director node is in slave mode. In the following example, the line "mode slave" under "vnmsha-details" indicates that the standby Director node is in slave mode. (The "mode master" line under "peer-vnmsha-details" shows the mode for the peer Director node, which is the primary.)

   ```
   admin@Director2> request vnmsha actions get-vnmsha-details fetch-peer-vnmsha-details true
   status SUCCESS
   vnmsha-details {
       mgmt-ip-address 10.192.36.171
       enabled true
       designated-master false
       mode slave
       peer-vnmsha-details {
           peer-vnmsha-detail {
               mgmt-ip-address 10.192.36.170
               enabled true
               designated-master true
               mode master
           }
       }
   }
   ```

   You can also check the Director mode by issuing the following command:

   ```
   admin@Director2> request vnmsha actions get-vnmsha-postgres-status
   ```

   The Role column in the command output shows "standby" for the standby Director node. For example:

   ```
   admin@Director2> request vnmsha actions get-vnmsha-postgres-status

   status ID | Name           | Role    | Status     | Upstream       | Location | Connection string
   ----------+----------------+---------+-----------+----------------+----------+---------------------------------------------
   1        | director-node1 | primary | * running |                | default  | host=10.192.36.170 user=repmgr
   dbname=repmgr
   2        | director-node2 | standby |   running | director-node1 | default  | host=10.192.36.171 user=repmgr
   dbname=repmgr
   ```

4. Verify that the primary and standby Director nodes are synchronized:

   ```
   admin@Director1> request vnmsha actions check-sync-status
   postgres-status  IN_SYNC
   ncs-status  IN_SYNC

   admin@Director2> request vnmsha actions check-sync-status
   postgres-status  IN_SYNC
   ncs-status  IN_SYNC
   ```

Download the Latest OS SPacks

Before you upgrade to Release 21.2 or later, you must upgrade the OS security packages (OS SPacks) on all Director nodes to the latest version. You can find the latest OS SPacks at https://versanetworks.app.box.com/v/osspack or https://upload.versa-networks.com/index.php/s/nEkF9xOO3e7BA9Z. If you do not upgrade the OS SPacks, the software upgrade may fail.

To install the OS SPack:

```
admin@Director1$ chmod +x ./versa-director-osspack-date.bin
admin@Director1$ sudo ./versa-director-osspack-date.bin
```

The following error may display when you upgrade from Release 16.1R2 to Release 21.2 or later from the Versa Director CLI:

```
admin@Director1> request system package upgrade package-name
Will restart Versa Director (all processes). Are you sure? [no,yes] yes
Verify package checksum..
status Some of the packages on this system are not correctly installed, please resolve before upgrading Versa
Director
Desired=Unknown/Install/Remove/Purge/Hold| Status=Not/Inst/Conf-files/Unpacked/halF-conf/Half-inst/trig-
aWait/Trig-pend|/ Err?=(none)/Reinst-required (Status,Err:uppercase=bad) ||/
Name  Version         Architecture                                  Description
===============================================================================================
rc    amd64-microcode  3.20180524.1~ubuntu0.14.04.2+really20130710.1ubuntu1 amd64 Processor microcode
firmware for AMD CPUs
rc    intel-microcode  3.20180807a.0ubuntu0.14.04.1                       amd64 Processor microcode firmware for
Intel CPUs
```

To resolve this error, run the following commands to manually remove the offending packages from Linux shell before you attempt to upgrade the Director node from CLI again:

```
admin@Director1$ sudo dpkg --purge amd64-microcode
admin@Director1$ sudo dpkg --purge intel-microcode
```

Validate the Director Node Configuration

Before you upgrade to Release 20.2.2 or later, you must install a validation script on both the active and standby Director nodes to identify all configuration discrepancies and fix them before you upgrade the Director nodes. To create the validation script, you download and run the versa-director-pre-upgrade-check.bin file, which creates the validation script, validate.py. Then, you run the validation script from the active Director node. (Note that in releases prior to Release 20.2.2, the versa-director-pre-upgrade-check.bin file was called versa-director-patch-*release*.bin.)

To install and run the upgrade validation script:

1. Download the versa-director-pre-upgrade-check.bin script from the Versa Director software release folder.
2. Run the script from the Director Linux shell. This script creates the validation script, validate.py, and places it in the /opt/versa/vnms/upgrade/scripts directory.

```
admin@Director1$ chmod +x ./versa-director-pre-upgrade-check.bin
admin@Director1$ sudo ./versa-director-pre-upgrade-check.bin

admin@Director2$ chmod +x ./versa-director-pre-upgrade-check.bin
admin@Director2$ sudo ./versa-director-pre-upgrade-check.bin
```

3. Run the validation script from the active Director node (here, Director1). If you are upgrading to Release 22.1, issue the following command:

   ```
   admin@Director$ sudo -E /opt/versa/vnms/upgrade/scripts/validate.py -n director-package.bin
   ```

   If you are upgrading to an earlier release, issue the following command:

   ```
   admin@Director$ sudo /opt/versa/vnms/upgrade/scripts/validate.py -f current-release -t new-release
   ```

   For example, to upgrade from Release 21.1 to Release 21.2:

   ```
   admin@Director1$ sudo /opt/versa/vnms/upgrade/scripts/validate.py -f 21.1 -t 21.2
   ```

If the validation script is successful, the console shows the following output:

```
INFO - Pre-Upgrade Validation Initiated
INFO - Executing validation script: ha-pair-config-validation.py ...
INFO - Successfully executed ha-pair-config-validation.py
INFO - Executing validation script: auth-connector-validation.lua ...
INFO - Successfully executed auth-connector-validation.lua
INFO - Executing validation script: org-validation.py ...
INFO - Successfully executed org-validation.py
INFO - Executing validation script: ip-address-config-validation.py ...
INFO - Successfully executed ip-address-config-validation.py
```

If the validation script identifies incorrect configurations, the script displays error messages on the console and logs details to the /var/log/vnms/upgrade.log file. Fix all the incorrect configurations before you upgrade the software on the Director nodes.

The following sample console output shows error messages display because of a validation failure:

```
admin@Director2$ sudo /opt/versa/vnms/upgrade/scripts/validate.py -f 20.2 -t 21.2
INFO - Pre-Upgrade Validation Initiated
Pre-Upgrade Validation Initiated
INFO - Executing validation script: auth-connector-validation.lua ...
Executing validation script: auth-connector-validation.lua ...
ERROR - Errors encountered during execution of auth-connector-validation.lua
Errors encountered during execution of auth-connector-validation.lua
INFO - Executing validation script: ha-pair-config-validation.py ...
Executing validation script: ha-pair-config-validation.py ...
INFO - Successfully executed ha-pair-config-validation.py
Successfully executed ha-pair-config-validation.py
INFO - Executing validation script: org-validation.py ...
Executing validation script: org-validation.py ...
INFO - Successfully executed org-validation.py
Successfully executed org-validation.py
```

```
INFO - Executing validation script: ip-address-config-validation.py ...
Executing validation script: ip-address-config-validation.py ...
INFO - Successfully executed ip-address-config-validation.py
Successfully executed ip-address-config-validation.py
ERROR - Validation failed for following scripts: auth-connector-validation.lua
Validation failed for following scripts: auth-connector-validation.lua
```

The following snippet from the /var/log/vnms/upgrade.log file explains the failure reported by the output above:

```
13-March-2021, 10:05:10 __main__ [INFO] Executing validation script: auth-connector-validation.lua ...
13-March-2021, 10:05:10 __main__ [DEBUG] Executing command su root -c "source /etc/profile.d/versa-profile.sh && /opt/versa/util/runlua -n confd -e confu /opt/versa/vnms/upgrade/validate/scripts/auth-connector-validation.lua"
13-March-2021, 10:05:10 __main__ [DEBUG] Command Output of auth-connector-validation.lua" is
13-March-2021, 10:05:12 __main__ [DEBUG] DEBUG badly formatted or nonexistent path - Bad path element "radius-server-details" after: /nms/provider/auth-connectors/auth-connector
13-March-2021, 10:05:12 __main__ [DEBUG] secret is not configured for authentication connector Name versaAuth Type radius
13-March-2021, 10:05:12 __main__ [DEBUG] Command exit status/return code is 1
13-March-2021, 10:05:12 __main__ [ERROR] Errors encountered during execution of auth-connector-validation.lua
```

The validation script runs automatically as the first step in the software upgrade. If the validation fails, the upgrade aborts immediately. If the following error is displayed while upgrading to Release 21.2 using Versa Director CLI, refer to the validation error mitigation guide or contact Versa Networks Customer Support:

```
admin@Director> request system package upgrade package-name
Will restart Versa Director (all processes). Are you sure? [no,yes] yes
Pre-Upgrade Validation Initiated
Executing validation script: org-validation.py …
Successfully executed org-validation.py
Executing validation script: ip-address-config-validation.py …
Errors encountered during execution of ip-address-config-validation.py
Executing validation script: auth-connector-validation.lua …
Successfully executed auth-connector-validation.lua
Executing validation script: ha-pair-config-validation.py …
Successfully executed ha-pair-config-validation.py
Validation failed for following scripts: ip-address-config-validation.py
Pre-Upgrade-Validation Failed.
Please refer to /var/log/vnms/upgrade.log for more details.
```

Upgrade the Director Software

To upgrade the software on HA-enabled Director nodes, you first upgrade the standby Director node, and then the primary (active) Director node.

Note that if you are prompted to provide the username and password for the peer node while upgrading HA, you must provide credentials for a user with either the ProviderDataCenterSystemAdmin role, or any custom role with the HA_MANAGEMENT privilege and Update action. For standby IP address, use 127.0.0.1 when disabling HA on a standalone Director node; otherwise, use the HA management IP address of the standby Director node.

To upgrade the software on HA-enabled Director nodes:

1. On the primary Director node, upload the software image:

   ```
   admin@Director1> request system package fetch uri url
   ```

   For example:

   ```
   admin@Director1> request system package fetch uri http://10.167.57.1/Builds/VOAE/21.2.2/director-201210910-171209.bin
   status
   Package Saved
   ```

   After you upload the software image, it is copied to the standby Director node.

2. On the primary Director node, confirm that the software image was uploaded:

   ```
   admin@Director1> request system package list
   ```

   For example:

   ```
   admin@Director1> request system package list
   packages {
      name *.deb
   }
   packages {
      name director-20210411-162626-6ede038-21.2.2S1.bin
   11}
   packages {
      name versa-director-20210910-054900-f009649-21.2.2S2.bin
   }
   ```

3. If proxy is enabled, you must add the northbound and southbound IP addresses of both the primary and standby Director nodes in the Exception IP list. For more information, see Configure Proxy Settings.
4. Ensure that you have installed the latest OS SPack on the standby Director node, as described in Download the Latest OS SPacks, above.
5. From the standby Director node, upgrade the software on the standby Director node:

   ```
   admin@Director2> request system package upgrade image-filename
   ```

   Ensure that the *image-filename* that you specify is the same image you used on the primary Director node.

   For example:

   ```
   admin@Director2> request system package upgrade director-20210910-171209.bin
   ```

5. After the upgrade completes, check that the services on the standby Director node have restarted and are running:

   ```
   admin@Director2$ vsh status
   ```

6. After the services on the standby Director node have restarted, verify that the correct software image is running on

the standby Director node:

```
admin@Director2> show system package-info
```

For example:

```
admin@Director2> show system package-info
Package        Director Software
Release        21.2.2
Build          S2
Release date   20210910
Package id     f009649
UI Package id  8c68b16
Package name   director-20210910-171209-21.2.2
Branch         21.2.2
```

7. Stop the services on the standby Director node:

```
admin@Director2$ vsh stop
```

8. Ensure that you have installed the latest OS SPack on the primary Director node, as described in Download the Latest OS SPacks, above.
9. From the primary Director node, upgrade the software on the primary Director node:

```
admin@Director1> request system package upgrade image-filename
```

image-filename is the name of the file that you uploaded in Step 1.

For example:

```
admin@Director1> request system package upgrade director-director-201210910-171209.bin
```

Note: While the upgrade is in progress, you may see a message that a system reboot is required. You must wait until the upgrade process is completed before you reboot the system. When the upgrade is completed, the screen output displays a message that the upgrade was successful, as shown in the following sample output:

```
27–April-2024, 10:05:12 __main__ [INFO] Upgrade to director-director-201210910-171209.bin successful!
```

When the upgrade is completed, reboot the standalone Director node.

10. After the upgrade completes, check that the services on the primary Director node have restarted and are running:

```
admin@Director1$ vsh status
```

11. After the services on the primary Director node have restarted, verify that the correct software image is running on the primary Director node:

```
admin@Director1> show system package-info
```

For example:

```
admin@Director1> show system package-info
Package        Director Software
Release        21.2.2
Build          S2
Release date   20210910
Package id     f009649
UI Package id  8c68b16
Package name   director-20210910-171209-21.2.2
Branch         21.2.2
```

12. Restart the services on the standby Director node:

```
admin@Director2$ vsh start
```

13. To verify that the primary and standby Director nodes are synchronized for their HA roles, issue the **request vnmsha actions status** command from either the primary or standby Director node.
14. Confirm that the primary Director node is running and has the "primary" role. For example:

```
admin@Director1> request vnmsha actions get-vnmsha-postgres-status

status ID | Name             | Role      | Status      | Upstream        | Location | Connection string
----------+------------------+-----------+-------------+-----------------+----------+--------------------------------------------
1         | director-node1    | primary   | * running   |                 | default  | host=10.192.36.170 user=repmgr
dbname=repmgr
2         | director-node2    | standby   |   running   | director-node1  | default  | host=10.192.36.171
user=repmgr dbname=repmgr
```

15. Confirm that the standby Director node is running has has the "standby" role. For example:

```
admin@Director2> request vnmsha actions get-vnmsha-postgres-status

status ID | Name           | Role    | Status    | Upstream       | Location | Connection string
----------+----------------+---------+-----------+----------------+----------+---------------------------------------------
1         | director-node1 | primary | * running |                | default  | host=10.192.36.170 user=repmgr
dbname=repmgr
2         | director-node2 | standby |   running | director-node1 | default  | host=10.192.36.171 user=repmgr
dbname=repmgr
```

16. Check that the primary and standby Director node are synchronized. Note that this command is available in Release 16.1R2.S8 and later.

```
admin@Director1> request vnmsha actions check-sync-status
postgres-status  IN_SYNC
ncs-status  IN_SYNC

admin@Director2> request vnmsha actions check-sync-status
postgres-status  IN_SYNC
ncs-status  IN_SYNC
```

Upgrade Analytics Nodes

Before you upgrade the Analytics software, archive the Analytics log files. By default, archiving of log files is enabled when you install the Analytics software.

If you have disabled the automatic log file archiving or if you want to manually archive the log files, run the following script to archive the log files at the specified time interval:

```
admin@Analytics$ /opt/versa/scripts/van-scripts/log-archive-start source-directory destination-directory
(hourly | daily | weekly)
```

The archive debug logs are in the file /var/log/versa/versa-log-archive.log.

To disable the manual archiving of log files:

```
admin@Analytics$ /opt/versa/scripts/van-scripts/log-archive-stop
```

Note: If you are upgrading the nodes in an Analytics cluster, upgrade the analytics nodes before you upgrade the search nodes.

Download the Software Image to the Analytics Node

1. Copy the software image file to the /home/versa/packages directory:

   ```
   admin@Analytics> request system package fetch uri url filename.bin
   ```

   Note that after you upload the software image file, existing configuration-related files, such as /etc/hosts, /etc/network/interfaces, and vansetup.conf, remain unchanged on the Analytics node.

2. Confirm that the software image was uploaded:

   ```
   admin@Analytics> request system package list
   ```

Upgrade a Standalone Analytics Node

If you are using a single Analytics node to perform both analysis and search:

1. Run the software image binary file. Note that upgrading the software image restarts the Analytics node.

   ```
   admin@Analytics> request system package upgrade filename.bin
   ```

2. Check that the services on the Analytics node have restarted:

   ```
   admin@Analytics$ vsh status
   versa-confd            is Running
   versa-lced             is Running
   versa-analytics-driver is Running
   versa-analytics-app    is Running
   ```

```
versa-monit           is Running
```

3. If the services are not started, issue the following command from the shell:

   ```
   admin@Analytics$ vsh start
   ```

Upgrade an Analytics Cluster

Upgrade the Analytics cluster nodes one at a time. Upgrade the nodes containing the noSQL database first, and then upgrade nodes containing the Analytics search engine.

To upgrade nodes in an Analytics cluster:

1. Upgrade a node whose personality is Analytics. Issue the following command from the CLI:

   ```
   admin@Analytics> request system package upgrade filename.bin
   ```

2. Check that the services on the Analytics node have restarted. Issue the following command from the shell:

   ```
   admin@Analytics$ vsh status
   versa-confd           is Running
   versa-lced            is Running
   versa-analytics-driver is Running
   versa-analytics-app    is Running
   versa-monit           is Running
   ```

   Note: If the output of **vsh status** command recommends a reboot, reboot the nodes only after the entire cluster is upgraded. For more information, see Step 7.

3. Repeat Steps 1 and 2 for all Analytics node whose personality is Analytics.
4. Upgrade a node whose personality is Search:

   ```
   admin@Analytics2> request system package upgrade filename.bin
   ```

5. Check that the services on the Analytics node have restarted:

   ```
   admin@Analytics2$ vsh status
   versa-confd           is Running
   versa-lced            is Running
   versa-analytics-driver is Running
   versa-analytics-app    is Running
   versa-monit           is Running
   ```

   Note: If the output of **vsh status** command recommends a reboot, reboot the nodes only after the entire cluster is upgraded. For more information, see Step 7.

6. Repeat Steps 4 and 5 for all Analytics node whose personality is Search.
7. In some cases after an upgrade, the output of the **vsh status** command recommends a reboot of the node, for example, after a kernel upgrade.

If a reboot is recommended, reboot the nodes only after the entire cluster is upgraded. You can reboot these nodes one by one in the same order that you upgraded them. The reboot command varies, depending on the type of Analytics node.

For Analytics-type nodes, reboot by issuing the following command:

```
admin@Analytics$ sudo nodetool drain && sudo reboot
```

For nodes with personality other than Analytics, reboot by issuing the following command:

```
admin@Search$ sudo reboot
```

8. Check that all nodes in the Analytics cluster are connected.
    a. Identify whether the node is running the DSE or Fusion platform.

```
admin@Analytics$ dse -v
dse: command not found
```

If the command returns returns a version number, such as 4.5 or 4.8, then the node is running the DSE platform. If the command returns an error message, then the platform is Fusion.

    b. On the DSE platform, issue the command below and verify that the nodes display status UN (Up and Normal).

```
admin@Analytics$ nodetool status
```

For example:

```
admin@Analytics$ nodetool status
[sudo] password for Administrator:
Note: Ownership information does not include topology; for complete information, specify a keyspace
Datacenter: Search
==============================================================================
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
--  Address      Load       Tokens   Owns   Host ID                              Rack
UN  10.51.24.34  9.73 GB    256      25.8%  d640f8d5-45e3-4152-bd9a-1e280973b22b  RAC1
UN  10.51.24.33  9.88 GB    256      22.1%  dd79fab5-e480-4e84-b8f6-dda4f631de8e  RAC1
Datacenter: Analytics
=================================================================================
Status=Up/Down
|/ State=Normal/Leaving/Joining/Moving
--    Address      Load       Tokens    Owns    Host ID                              Rack
UN  10.51.24.43   25.77 GB    256       24.2%   666f6173-1ffc-41e2-a86d-b64b4058a439  RAC1
UN  10.51.24.44   25.76 GB    256       27.9%   2dfb1545-ddea-4a28-adc6-88ae5d16a4e7  RAC1
```

    c. On the Fusion platform, issue the following command to verify that the nodes display status UN (Up and Normal).

```
admin@Analytics$ vsh dbstatus
```

Checks To Perform after an Analytics Upgrade

In Releases 21.2. and later, you cannot access the Versa Analytics application using port 8080, to avoid any security vulnerabilities. By default, only secure ports 443 and 8443 are enabled in Analytics, and port 8443 is used for communication between the Director and Analytics nodes. When you upgrade to Releases 21.2 and. later on Director nodes, the upgrade process automatically changes the northbound interface port number 8080 to 8443, and it automatically synchronizes the certificates required for SSL communication between the Analytics and Director nodes.

If there is no communication between the Versa Director and Versa Analytics nodes, perform the following steps:

1. Check whether any firewall rule is blocking Versa Director to Versa Analytics communication on port 8443.
2. Connect to Versa Analytics directly using https://*analytics-ip-address*:8443 to determine whether the portal is accessible. This ensures that the application is reachable using a secure port and that the SSL certificate is valid.
3. Log in to the Versa Analytics node using the same username and password as the Versa Director node. If the login is successful, this means that RBAC between the Analytics and Director nodes is working using a secure connection. If the login is not successful, install Versa Director certificates on Versa Analytics nodes as described in https://support.versa-networks.com/a/solutions/articles/23000010418.
4. Log in to the Versa Director shell and issue the following commands to check whether the Versa Analytics truststore has been created on Versa Director:

```
admin@Director$ cd /var/versa/vnms/data/certs
admin@Director$ ls -tlr versa_analytics_truststore.ts
-rw-rw---- 1 versa versa 1274 Jul 30 05:42 versa_analytics_truststore.ts
```

5. If the truststore file does not exist or if the Versa Analytics certificates were regenerated, resynchronize and import the Versa Analytics certificates by running the vd-van-cert-upgrade.sh script in the active Director shell. This script transfers the Versa Analytics certificates from each of the Analytics nodes configured under the connectors and then imports them. You must restart Versa Director for the certificate to take effect.

```
admin@Director$ sudo su – versa
versa@Director$ /opt/versa/vnms/scripts/vd-van-cert-upgrade.sh --pull
```

For example:

```
versa@Director$ /opt/versa/vnms/scripts/vd-van-cert-upgrade.sh --pull
Pulling Analytics certificates to Director key store
Checking previous version config path
Changing port for [Analytics]
No modifications to commit.
Port Migration completed
VAN Clusters IPs: [ 10.48.189.23 ]
Removing previous analystics cert store
Getting Certificate for : 10.48.189.23
depth=0 C = US, ST = California, L = Santa Clara, O = versa-networks, OU = VersaAnalytics, CN = versa-
analytics
verify error:num=18:self signed certificate
verify return:1
depth=0 C = US, ST = California, L = Santa Clara, O = versa-networks, OU = VersaAnalytics, CN = versa-
analytics
verify return:1
```

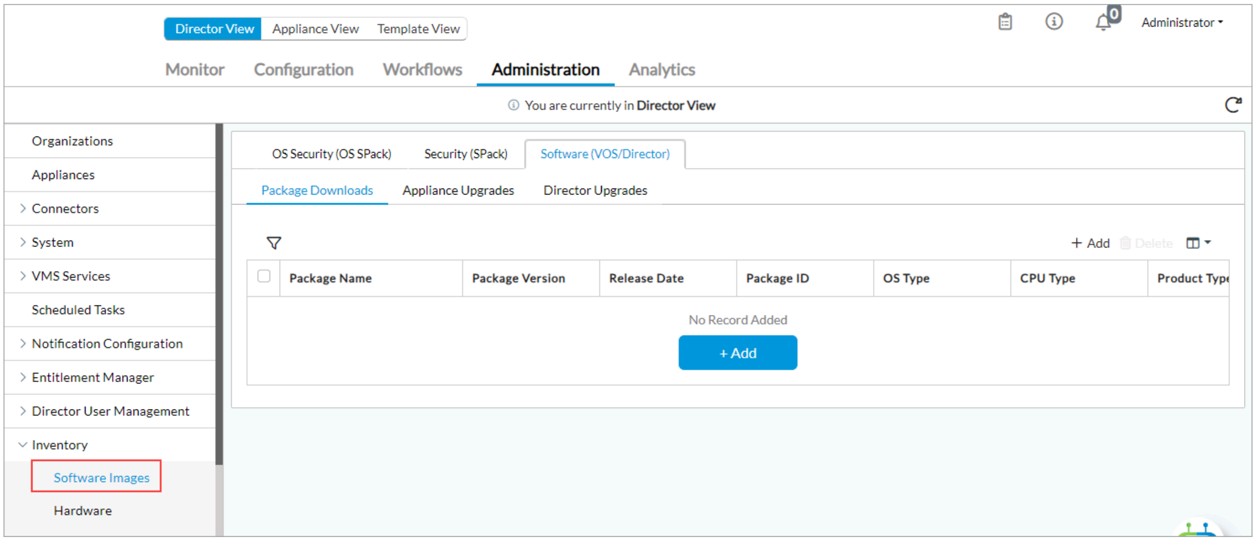
```
DONE
Importing Certificate for : 10.48.189.23
Certificate was added to keystore
Certificates Imported... Requires restart.. Do you want to postpone restart (y/N): N
[sudo] password for versa:
Stopping VNMS service
------------------------------------
Stopping TOMCAT................[Stopped]
Stopping REDIS.................[Stopped]
Stopping NETBOX-IPAM...........[Stopped]
Stopping POSTGRE...............[Stopped]
Stopping SPRING-BOOT...........[Stopped]
Stopping SPACKMGR..............[Stopped]
Stopping NCS...................[Stopped]
* Stopping daemon monitor monit
Starting VNMS service
------------------------------------
Starting NCS...................[Started]
Starting POSTGRE...............[Started]
Starting NETBOX-IPAM...........[Started]
Starting SPRING-BOOT.......... [Started]
Starting REDIS.................[Started]
Starting TOMCAT................[Started]
```

Download Controller and VOS Software Image to Director Node

Before you can upgrade the VOS software on a Director node, on VOS devices, and on Controllers nodes, which are simply VOS devices acting in the role of a controller, you download the VOS software image file to the Director node.

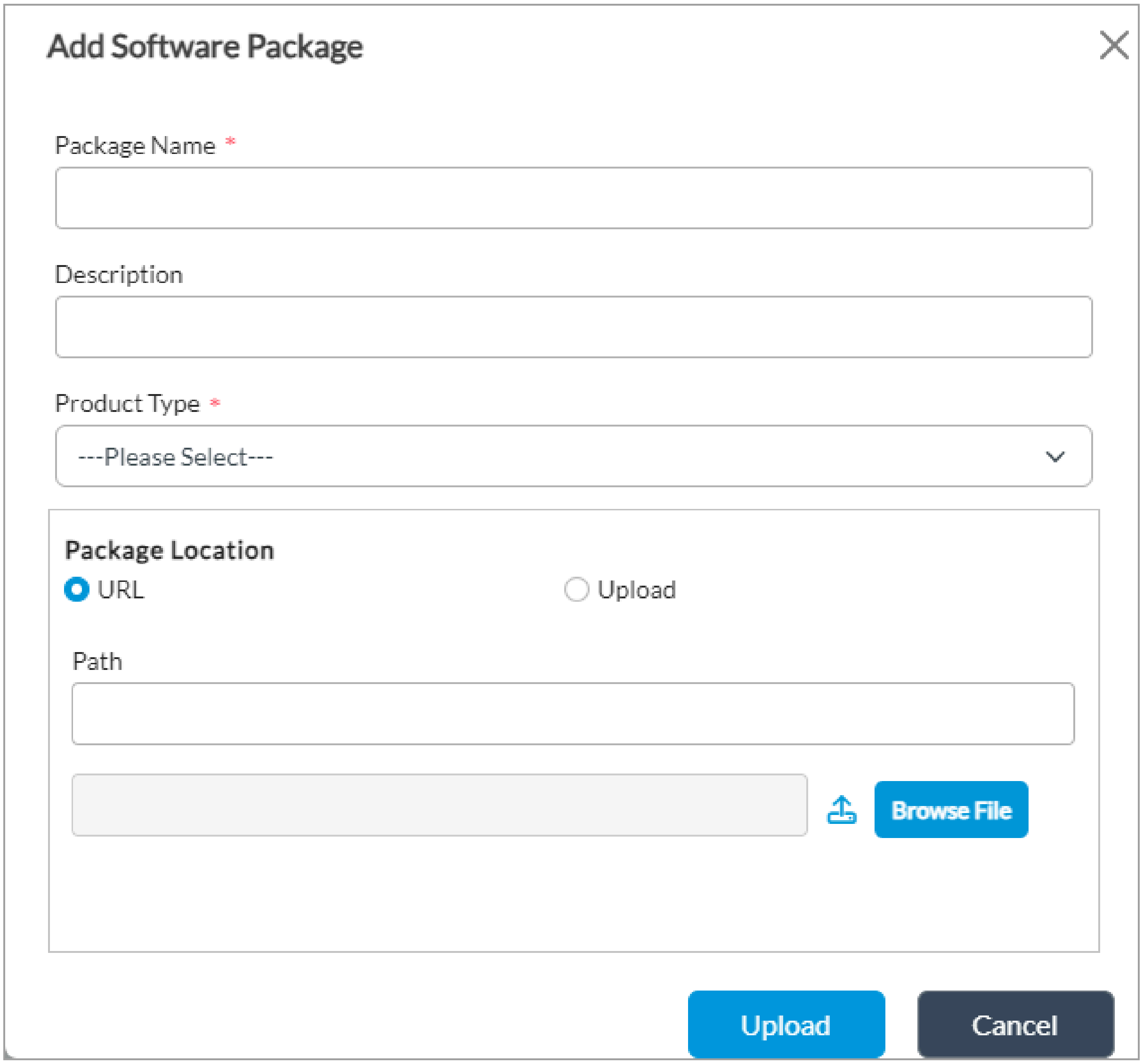
For Releases 22.1.1 and later, to download the VOS software image file from the Director software image repository:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Inventory > Software Images in the left menu bar.
3. Select the Software (VOS/Director) tab, and then select the Package Downloads tab. The following screen displays.



□	Package Name	Package Version	Release Date	Package ID	OS Type	CPU Type	Product Type

4. Click the + Add icon. In the Add Software Package popup window, enter information for the following fields.



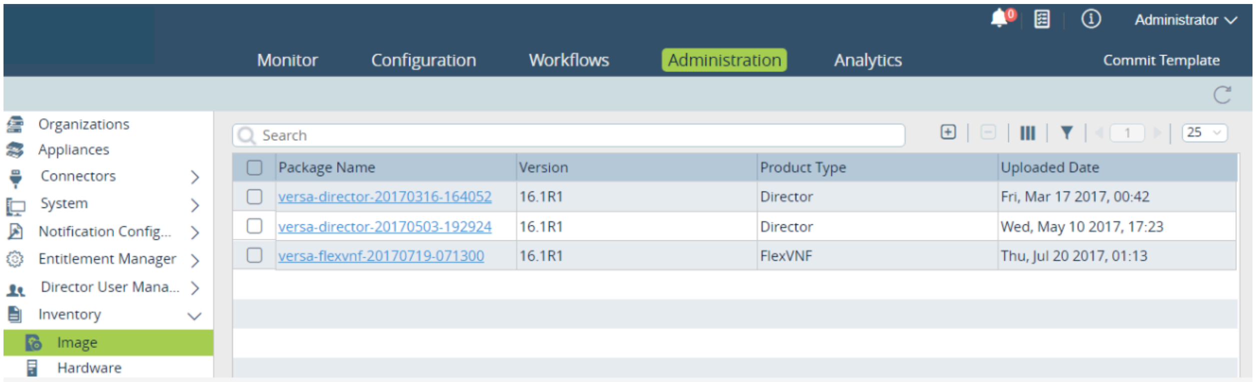
Field	Description
Package Name (Required)	Enter the name of the software package.
Description	Enter a text description for the software package.
Product Type (Required)	Select the product type: ◦ Director—Select for a Director node. ◦ FlexVNF —Select for a VOS device or Controller node.

Package Location (Group of Fields)	Select the location of the software package.
◦ URL	Click, and then enter the URL in the Path field from which to download th
◦ Upload	Click Browse, and then select the software package file.

5. Click Upload.

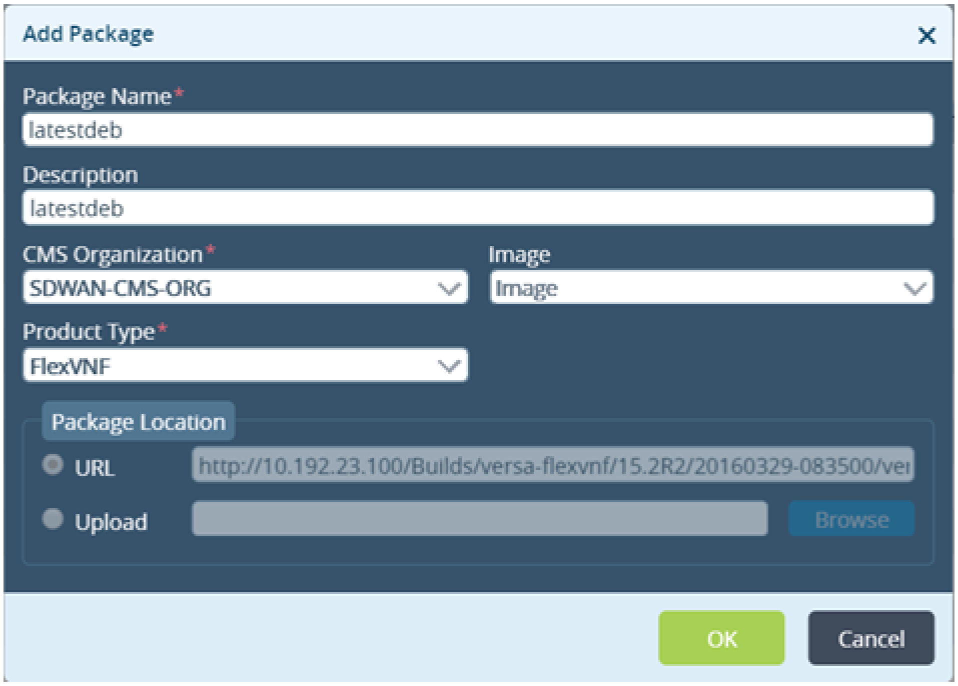
For Releases 21.2 and earlier, to download the VOS software image file to the Director software image repository:

1. In Director mode, select the Administration tab in the top menu bar.
2. Select Inventory > Images in the left menu bar. The following screen displays.



☐	Package Name	Version	Product Type	Uploaded Date
☐	versa-director-20170316-164052	16.1R1	Director	Fri, Mar 17 2017, 00:42
☐	versa-director-20170503-192924	16.1R1	Director	Wed, May 10 2017, 17:23
☐	versa-flexvnf-20170719-071300	16.1R1	FlexVNF	Thu, Jul 20 2017, 01:13

3. Click the ⊞ Add icon. In the Add Package popup window, enter information for the following fields:



Add Package

Package Name* latestdeb

Description latestdeb

CMS Organization* SDWAN-CMS-ORG

Image Image

Product Type* FlexVNF

Package Location

URL http://10.192.23.100/Builds/versa-flexvnf/15.2R2/20160329-083500/ver

Upload

Field	Description
Package Name (Required)	Enter the name of the software package.
Description	Enter a text description for the software package.
CMS Organization	Select the name of the organization to which the Director node belong
Image	Select Image as the package type.
Product Type (Required)	Select the product type: ◦ Director—Select for a Director node. ◦ FlexVNF —Select for a VOS device or Controller node.
Package Location	Click URL to enter the URL from which to download the software pack Click Upload to browse for and select the software package file.
Package Location (Group of Fields)	Select the location of the software package.

◦ URL	Click, and then enter the URL in the Path field from which to download
◦ Upload	Click Browse, and then select the software package file.

4. Click OK.

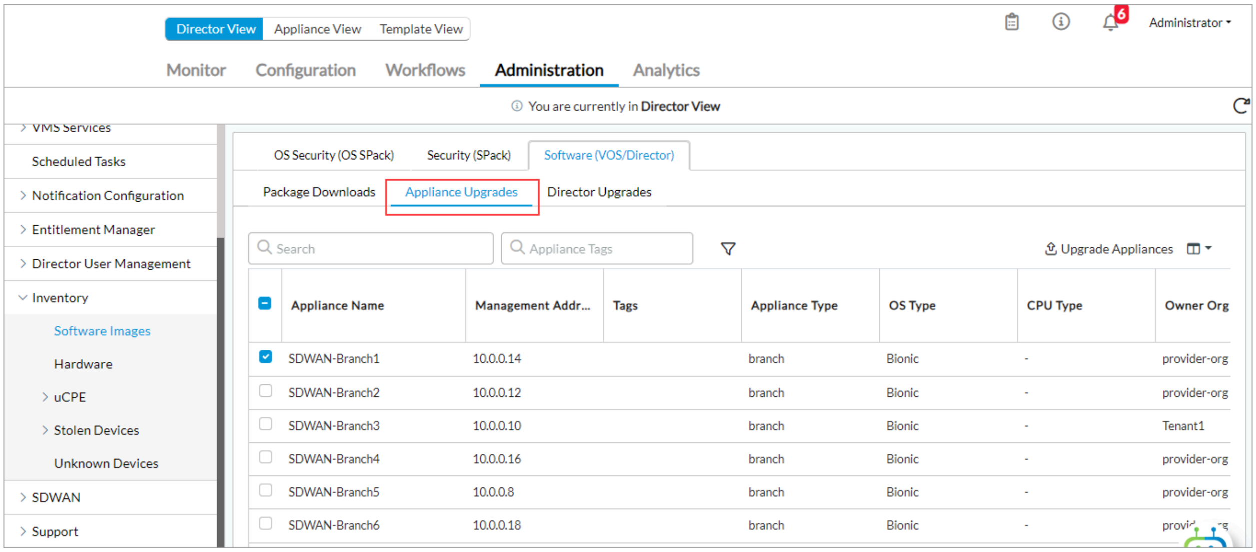
Upgrade a Software Image on a VOS Device

For Releases 22.1.1 and later.

You can upgrade the software image on a VOS device from the Inventory > Software Images option as described in this section. You can also upgrade the VOS device software image from the Appliance option, as described in Upgrade the Remaining Controller Nodes, below.

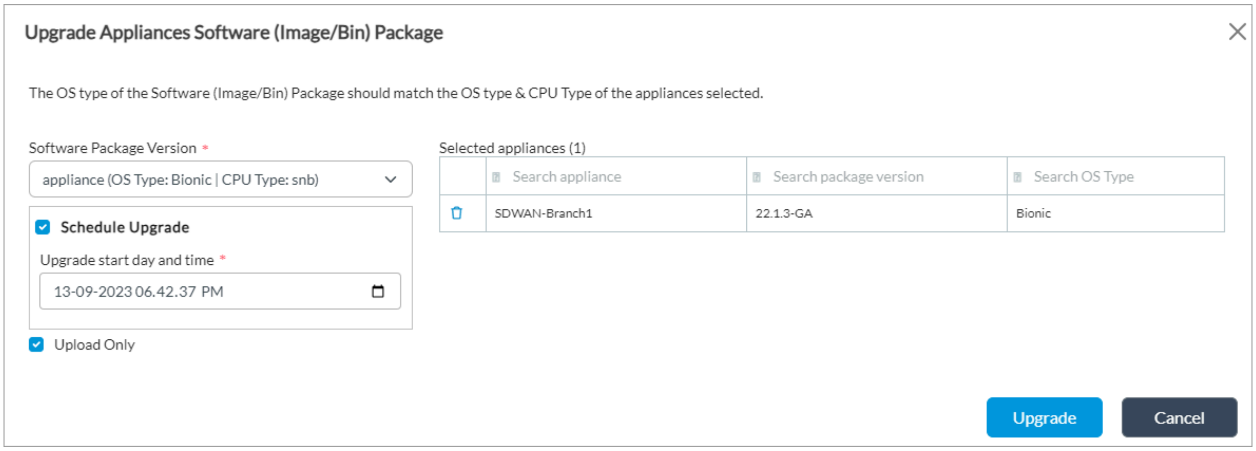
To upgrade a software image on a VOS device:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Inventory > Software Images in the left menu bar.
3. Select the Software (VOS/Director) tab, and then select the Appliance Upgrades tab.



☑	Appliance Name	Management Addr...	Tags	Appliance Type	OS Type	CPU Type	Owner Org
☑	SDWAN-Branch1	10.0.0.14		branch	Bionic	-	provider-org
□	SDWAN-Branch2	10.0.0.12		branch	Bionic	-	provider-org
□	SDWAN-Branch3	10.0.0.10		branch	Bionic	-	Tenant1
□	SDWAN-Branch4	10.0.0.16		branch	Bionic	-	provider-org
□	SDWAN-Branch5	10.0.0.8		branch	Bionic	-	provider-org
□	SDWAN-Branch6	10.0.0.18		branch	Bionic	-	provider-org

4. Select the VOS device or devices on which to upgrade the software, or select the box next to the Appliance Name column to select all devices. The Package Version column in the table displays the current software version installed on the device.
5. Click Upgrade Appliances. The Upgrade Appliances Software (Image/Bin) Package popup window displays. Enter information for the following fields.



Upgrade Appliances Software (Image/Bin) Package

The OS type of the Software (Image/Bin) Package should match the OS type & CPU Type of the appliances selected.

Software Package Version *

appliance (OS Type: Bionic | CPU Type: snb)

☑ Schedule Upgrade

Upgrade start day and time *

13-09-2023 06.42.37 PM

☑ Upload Only

Selected appliances (1)

	Search appliance	Search package version	Search OS Type
	SDWAN-Branch1	22.1.3-GA	Bionic

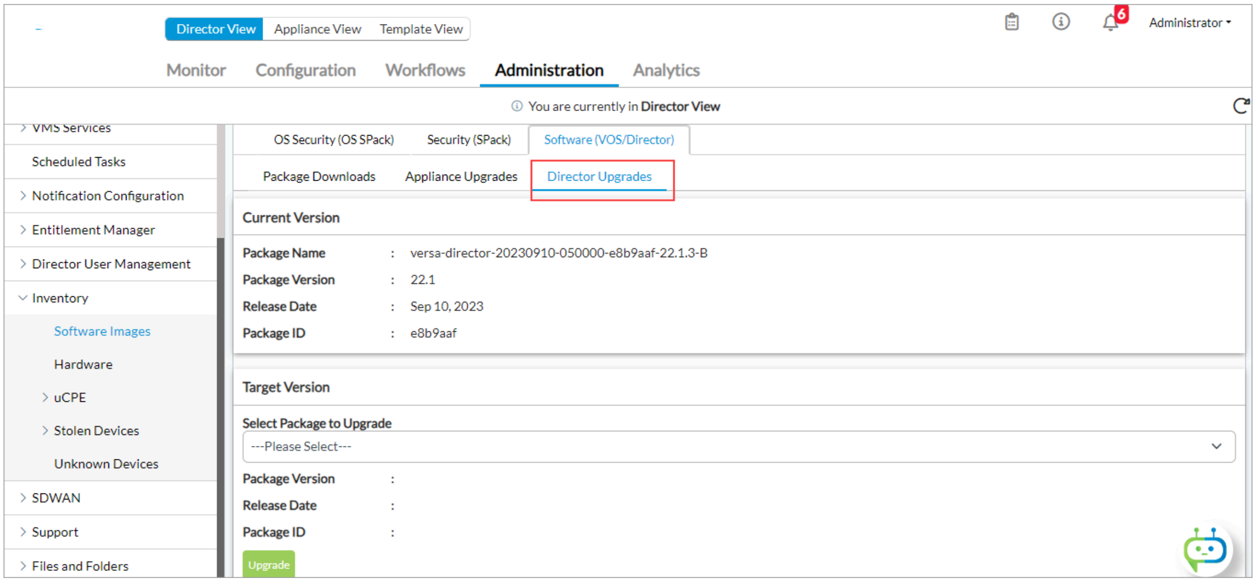
Field	Description
Software Package Version (Required)	Select the software package from the list of downloaded software packages.
Schedule Upgrade (Required)	Click to schedule a date and time for the upgrade to occur. Enter the date in the format *mm/dd/yyyy* (month/date/year), and enter the time in the format *hh*:*mm*:*ss* (hours:minutes:seconds, using 24-hour format for the hours).
Upload Only	Click to upload the software package without upgrading it.
Selected Appliances	Displays the device or devices you selected to upgrade

6. Click Upgrade. If you have not set a schedule for upgrade, the software package is upgraded immediately.

Upgrade a Software Image on a Director Node

For Releases 22.1.1 and later, to upgrade a software image file on a Director node:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Inventory > Software Images in the left menu bar.
3. Select the Software (VOS/Director) tab, and then select the Director Upgrades tab. The Package Version column in the table displays information about the software package that is installed on the Director node.



Current Version

Package Name : versa-director-20230910-050000-e8b9aaf-22.1.3-B
Package Version : 22.1
Release Date : Sep 10, 2023
Package ID : e8b9aaf

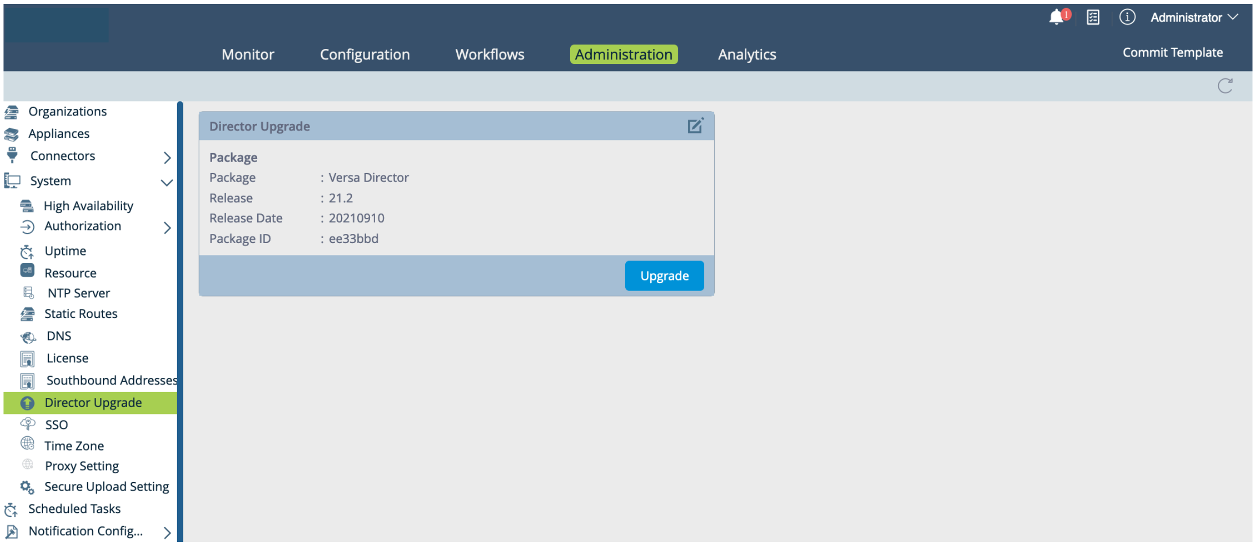
Target Version

Select Package to Upgrade
---Please Select---
Package Version :
Release Date :
Package ID :

4. In the Target Version box, in the Select Package to Upgrade field, select the package to which to upgrade the Director node.
5. Click Upgrade.

For Releases 21.2 and earlier, to upgrade a software image file on a Director node:

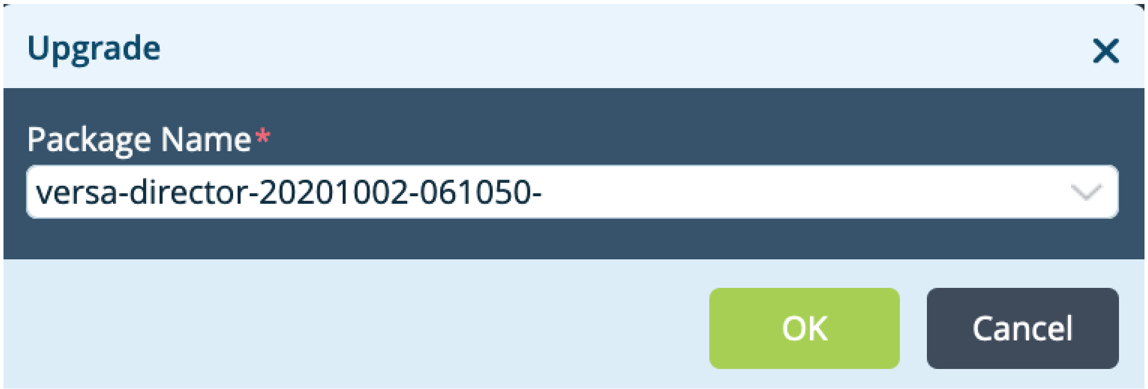
1. In Director view, select the Administration tab in the top menu bar
2. Select System > Director Upgrade in the left menu bar. The main pane display the Director Upgrade pane.



Director Upgrade

Package
Package : Versa Director
Release : 21.2
Release Date : 20210910
Package ID : ee33bbd

3. Click the Edit icon. In the Upgrade popup window, select the software package name.



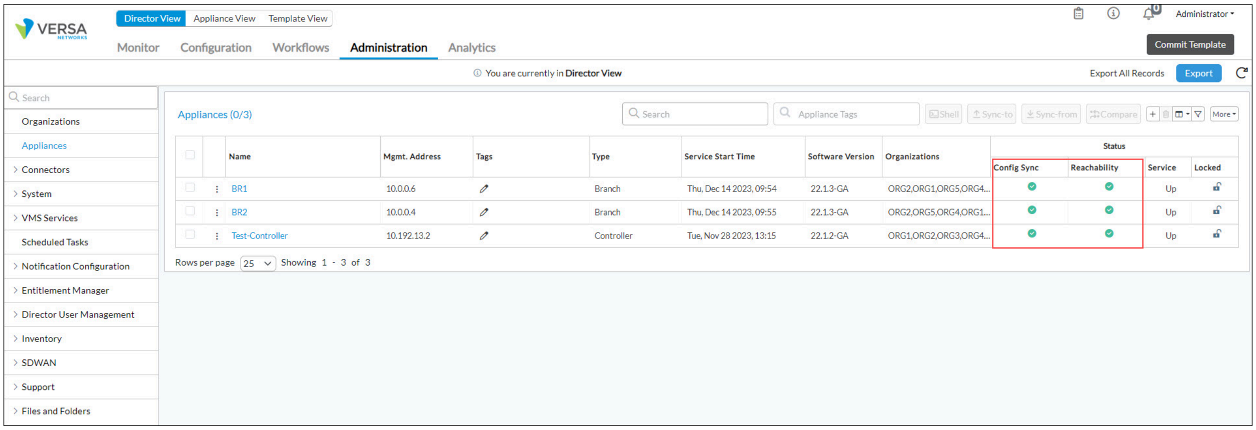
versa-director-20201002-061050-

4. Click OK.
5. Click Upgrade.

Upgrade the First Controller Node

For Releases 22.1.1 and later, to upgrade the first Controller node:

1. Check that the Controller node (or VOS device) status is synchronized and reachable:
   a. In Director view, select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Check the values in the Status columns in the main pane. Note that you cannot update a device whose state is error or unreachable.



You are currently in **Director View**

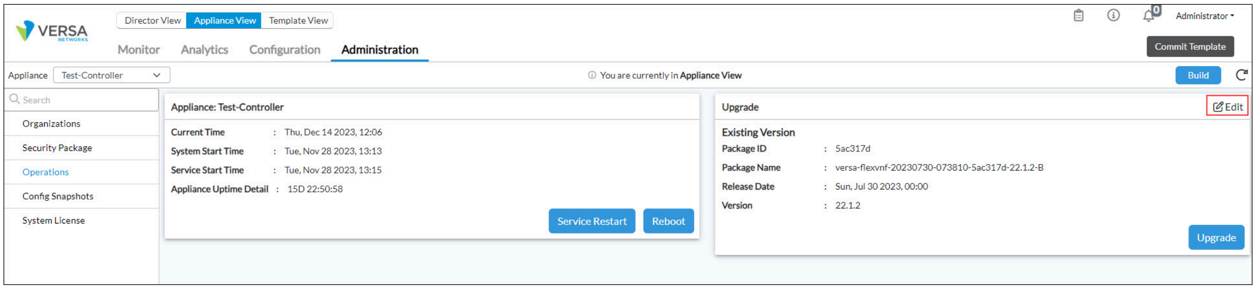
Appliances (0/3)

Name	Mgmt. Address	Tags	Type	Service Start Time	Software Version	Organizations	Status			
							Config Sync	Reachability	Service	Locked
BR1	10.0.0.6		Branch	Thu, Dec 14 2023, 09:54	22.1.3-GA	ORG2,ORG1,ORG5,ORG4...	✓	✓	Up	
BR2	10.0.0.4		Branch	Thu, Dec 14 2023, 09:55	22.1.3-GA	ORG2,ORG5,ORG4,ORG1...	✓	✓	Up	
Test-Controller	10.192.13.2		Controller	Tue, Nov 28 2023, 13:15	22.1.2-GA	ORG1,ORG2,ORG3,ORG4...	✓	✓	Up	

Rows per page 25 Showing 1 - 3 of 3

2. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select a Controller node (or VOS device) from the main pane. The view changes to Appliance view.

3. Select Operations in the left menu bar, and click the ✎ Edit icon in the Upgrade box.



Appliance Test-Controller

You are currently in Appliance View

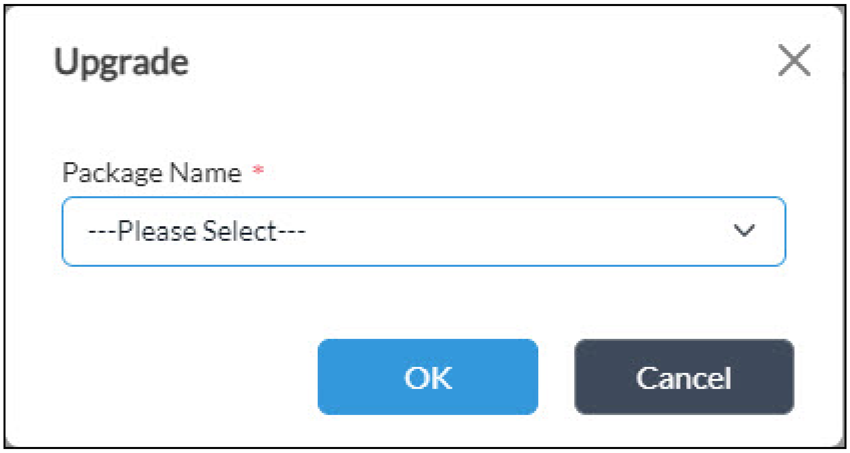
Appliance: Test-Controller

Current Time : Thu, Dec 14 2023, 12:06
System Start Time : Tue, Nov 28 2023, 13:13
Service Start Time : Tue, Nov 28 2023, 13:15
Appliance Uptime Detail : 15D 22:50:58

Upgrade

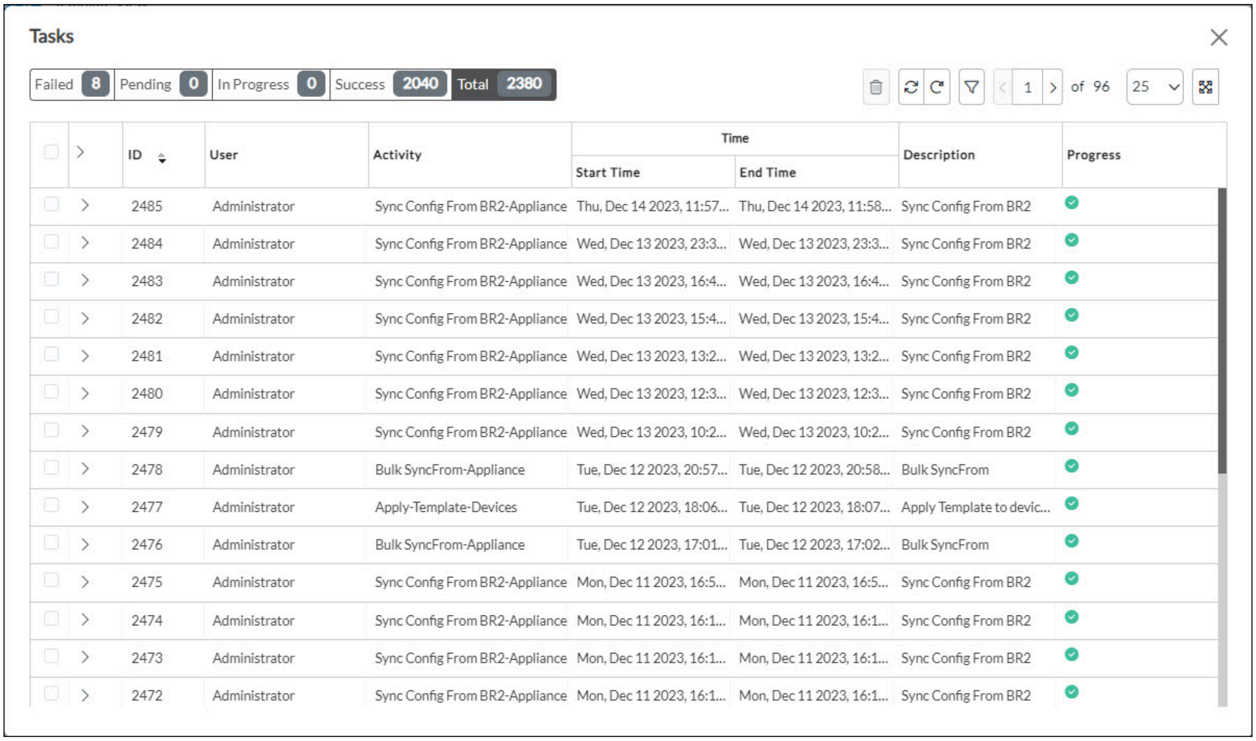
Existing Version
Package ID : 5ac317d
Package Name : versa-flexvnf-20230730-073810-5ac317d-22.1.2-B
Release Date : Sun, Jul 30 2023, 00:00
Version : 22.1.2

4. In the Upgrade popup window, select the software image package name.



Package Name *
---Please Select---

5. Click OK.
6. In the Upgrade box, verify the information about the existing and new VOS software packages.
7. Click the Upgrade Upgrade button.
8. Select the name of the software package to which you are upgrading.
9. Click OK.
10. To track the progress of the software upgrade, click the Tasks icon. The Tasks screen displays:

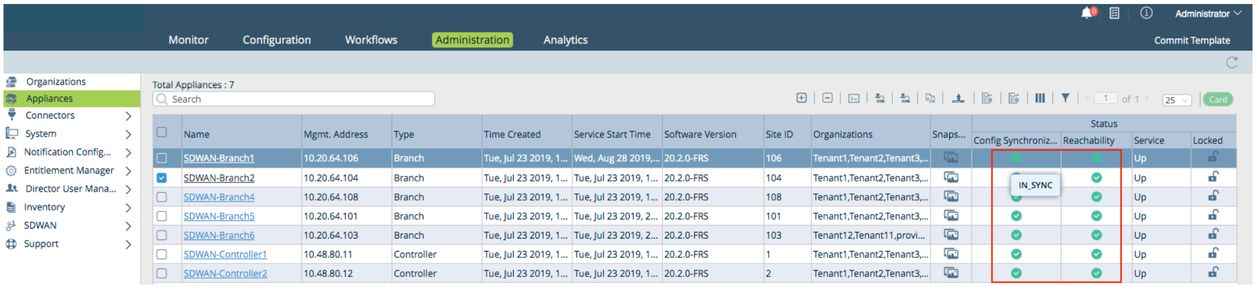


ID	User	Activity	Time Start Time	 End Time	Description	Progress
2485	Administrator	Sync Config From BR2-Appliance	Thu, Dec 14 2023, 11:57...	Thu, Dec 14 2023, 11:58...	Sync Config From BR2	✓
2484	Administrator	Sync Config From BR2-Appliance	Wed, Dec 13 2023, 23:3...	Wed, Dec 13 2023, 23:3...	Sync Config From BR2	✓
2483	Administrator	Sync Config From BR2-Appliance	Wed, Dec 13 2023, 16:4...	Wed, Dec 13 2023, 16:4...	Sync Config From BR2	✓
2482	Administrator	Sync Config From BR2-Appliance	Wed, Dec 13 2023, 15:4...	Wed, Dec 13 2023, 15:4...	Sync Config From BR2	✓
2481	Administrator	Sync Config From BR2-Appliance	Wed, Dec 13 2023, 13:2...	Wed, Dec 13 2023, 13:2...	Sync Config From BR2	✓
2480	Administrator	Sync Config From BR2-Appliance	Wed, Dec 13 2023, 12:3...	Wed, Dec 13 2023, 12:3...	Sync Config From BR2	✓
2479	Administrator	Sync Config From BR2-Appliance	Wed, Dec 13 2023, 10:2...	Wed, Dec 13 2023, 10:2...	Sync Config From BR2	✓
2478	Administrator	Bulk SyncFrom-Appliance	Tue, Dec 12 2023, 20:57...	Tue, Dec 12 2023, 20:58...	Bulk SyncFrom	✓
2477	Administrator	Apply-Template-Devices	Tue, Dec 12 2023, 18:06...	Tue, Dec 12 2023, 18:07...	Apply Template to devic...	✓
2476	Administrator	Bulk SyncFrom-Appliance	Tue, Dec 12 2023, 17:01...	Tue, Dec 12 2023, 17:02...	Bulk SyncFrom	✓
2475	Administrator	Sync Config From BR2-Appliance	Mon, Dec 11 2023, 16:5...	Mon, Dec 11 2023, 16:5...	Sync Config From BR2	✓
2474	Administrator	Sync Config From BR2-Appliance	Mon, Dec 11 2023, 16:1...	Mon, Dec 11 2023, 16:1...	Sync Config From BR2	✓
2473	Administrator	Sync Config From BR2-Appliance	Mon, Dec 11 2023, 16:1...	Mon, Dec 11 2023, 16:1...	Sync Config From BR2	✓
2472	Administrator	Sync Config From BR2-Appliance	Mon, Dec 11 2023, 16:1...	Mon, Dec 11 2023, 16:1...	Sync Config From BR2	✓

11. If you are upgrading a Controller node, wait for services to come up on the node. Then verify that the Controller has connected to the other Controllers, to all branches, and to all hubs if there are any in the network.

For Releases 21.2 and earlier, to upgrade the first Controller node:

1. Check that the Controller node (or VOS device) status is synchronized and reachable:
   a. In Director view, select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Check the values in the Status columns in the main pane. Note that you cannot update a device whose state is error or unreachable.

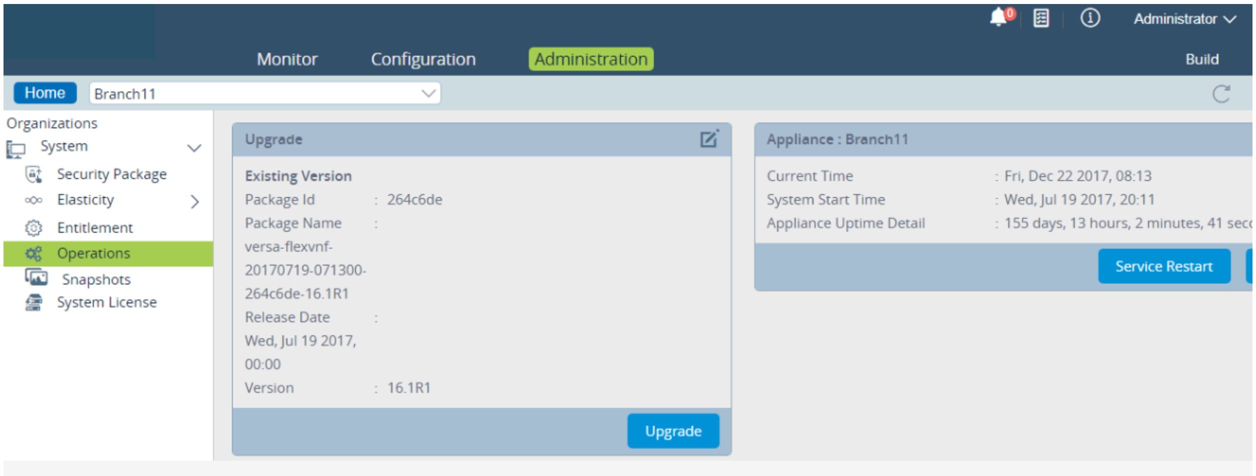


Total Appliances : 7

	Name	Mgmt. Address	Type	Time Created	Service Start Time	Software Version	Site ID	Organizations	Snaps...	Status Config Synchroniz...	 Reachability	 Service	 Locked
□	SDWAN-Branch1	10.20.64.106	Branch	Tue, Jul 23 2019, 1...	Wed, Aug 28 2019,...	20.2.0-FRS	106	Tenant1,Tenant2,Tenant3,...		✓	✓	Up	
☑	SDWAN-Branch2	10.20.64.104	Branch	Tue, Jul 23 2019, 1...	Tue, Jul 23 2019, 1...	20.2.0-FRS	104	Tenant1,Tenant2,Tenant3,...		✓	✓	Up	
□	SDWAN-Branch4	10.20.64.108	Branch	Tue, Jul 23 2019, 1...	Tue, Jul 23 2019, 1...	20.2.0-FRS	108	Tenant1,Tenant2,Tenant3,...		✓	✓	Up	
□	SDWAN-Branch5	10.20.64.101	Branch	Tue, Jul 23 2019, 1...	Tue, Jul 23 2019, 2...	20.2.0-FRS	101	Tenant1,Tenant2,Tenant3,...		✓	✓	Up	
□	SDWAN-Branch6	10.20.64.103	Branch	Tue, Jul 23 2019, 1...	Tue, Jul 23 2019, 2...	20.2.0-FRS	103	Tenant12,Tenant11,provi...		✓	✓	Up	
□	SDWAN-Controller1	10.48.80.11	Controller	Tue, Jul 23 2019, 1...	Tue, Jul 23 2019, 1...	20.2.0-FRS	1	Tenant1,Tenant2,Tenant3,...		✓	✓	Up	
□	SDWAN-Controller2	10.48.80.12	Controller	Tue, Jul 23 2019, 1...	Tue, Jul 23 2019, 1...	20.2.0-FRS	2	Tenant1,Tenant2,Tenant3,...		✓	✓	Up	

2. In Director view:
   a. Select the Configuration tab in the top menu bar.
   b. Select Devices > Devices in the left menu bar.
   c. Select an organization in the left menu bar.
   d. Select a Controller node (or VOS device) from the main pane. The view changes to Appliance view.

3. Select System > Operations in the left menu bar.



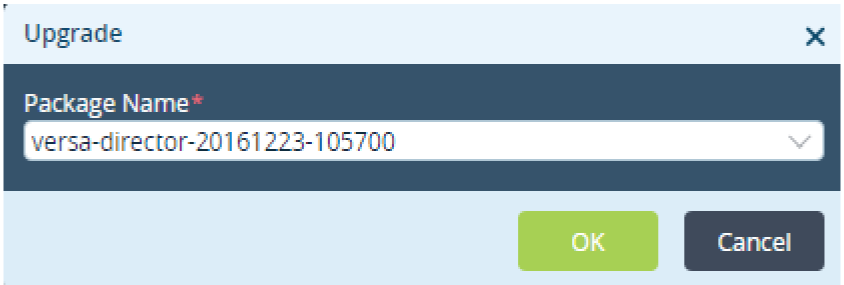
Upgrade

Existing Version
Package Id : 264c6de
Package Name : versa-flexvnf-20170719-071300-264c6de-16.1R1
Release Date : Wed, Jul 19 2017, 00:00
Version : 16.1R1

Appliance : Branch11

Current Time : Fri, Dec 22 2017, 08:13
System Start Time : Wed, Jul 19 2017, 20:11
Appliance Uptime Detail : 155 days, 13 hours, 2 minutes, 41 seco

4. Click the Edit icon in the Upgrade box.
5. In the Upgrade popup window, select the software image package name.

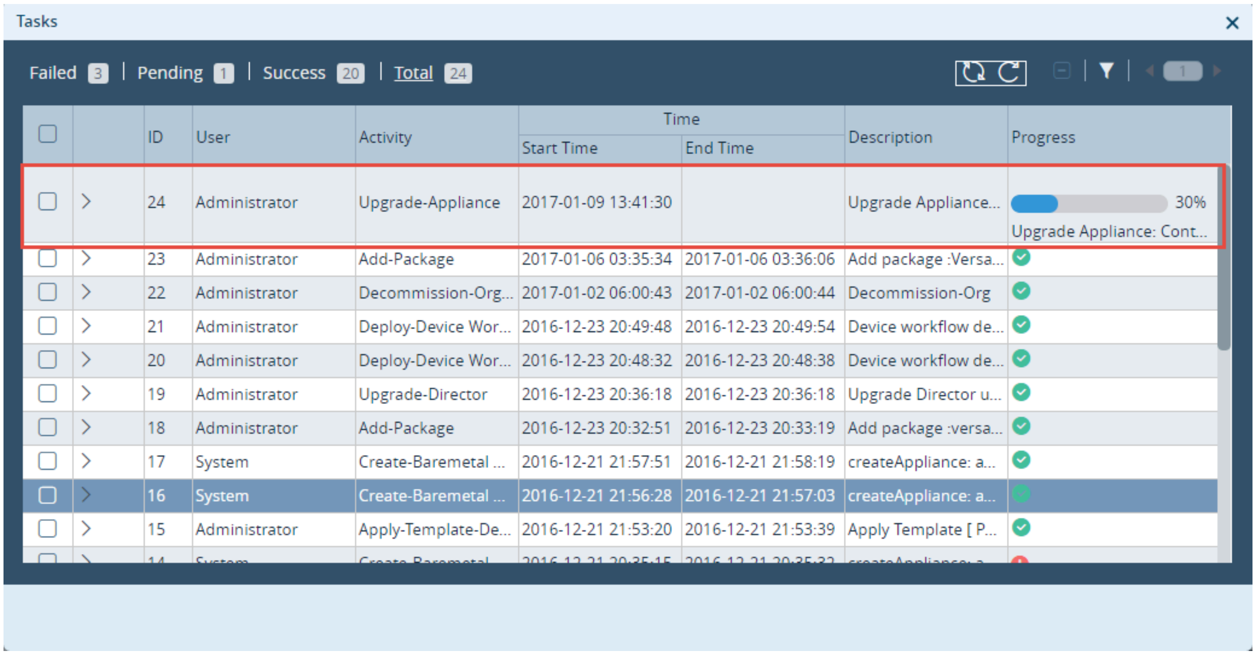


Package Name* versa-director-20161223-105700

6. Click OK.
7. In the Upgrade box, verify the information about the existing and new VOS software packages.

8. Click the Upgrade Upgrade button.
9. Select the name of the software package to which you are upgrading.
10. Click OK.

11. To track the progress of the software upgrade, click the Tasks icon. The Tasks screen displays:



Tasks

Failed 3 | Pending 1 | Success 20 | Total 24

☐		ID	User	Activity	Time		Description	Progress
					Start Time	End Time		
☐	>	24	Administrator	Upgrade-Appliance	2017-01-09 13:41:30		Upgrade Appliance...	30% Upgrade Appliance: Cont...
☐	>	23	Administrator	Add-Package	2017-01-06 03:35:34	2017-01-06 03:36:06	Add package :Versa...	✓
☐	>	22	Administrator	Decommission-Org...	2017-01-02 06:00:43	2017-01-02 06:00:44	Decommission-Org	✓
☐	>	21	Administrator	Deploy-Device Wor...	2016-12-23 20:49:48	2016-12-23 20:49:54	Device workflow de...	✓
☐	>	20	Administrator	Deploy-Device Wor...	2016-12-23 20:48:32	2016-12-23 20:48:38	Device workflow de...	✓
☐	>	19	Administrator	Upgrade-Director	2016-12-23 20:36:18	2016-12-23 20:36:18	Upgrade Director u...	✓
☐	>	18	Administrator	Add-Package	2016-12-23 20:32:51	2016-12-23 20:33:19	Add package :versa...	✓
☐	>	17	System	Create-Baremetal ...	2016-12-21 21:57:51	2016-12-21 21:58:19	createAppliance: a...	✓
☐	>	16	System	Create-Baremetal ...	2016-12-21 21:56:28	2016-12-21 21:57:03	createAppliance: a...	✓
☐	>	15	Administrator	Apply-Template-De...	2016-12-21 21:53:20	2016-12-21 21:53:39	Apply Template [P...	✓
☐	>	14	System	Create-Baremetal ...	2016-12-21 20:35:15	2016-12-21 20:35:32	createAppliance: a...	●

12. If you are upgrading a Controller node, wait for services to come up on the node. Then verify that the Controller has connected to the other Controllers, to all branches, and to all hubs if there are any in the network.

Upgrade Active Hub Devices

If you are not upgrading the software image on VOS hub devices, you can skip this section.

If you are using a hub-and-spoke topology, and if you have deployed the hub in an active-standby HA pair, upgrade the software on the active hub of the HA pair. Follow the procedure in Upgrade the First Controller Node, above. Then follow the same procedure to upgrade the standby hub.

Upgrade Active HA VOS Branch Devices

If you are not upgrading the software image on VOS devices, you can skip this section.

If any branches have two VOS devices that use an interchassis HA deployment, in which one branch VOS device is the active device and a second is the standby device, upgrade the software on the active VOS devices. Follow the procedure in Upgrade the First Controller Node, above. Then follow the same procedure to upgrade the standby VOS branch device.

Upgrade the Remaining Controller Nodes

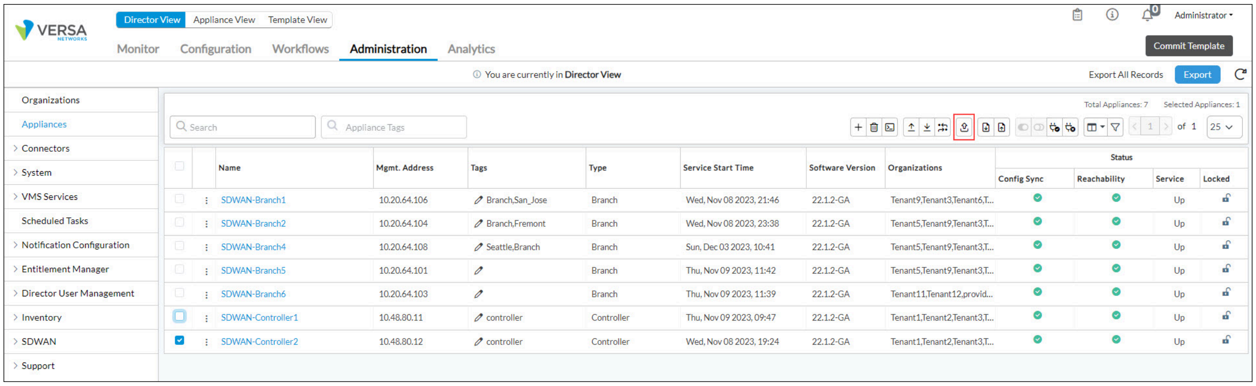
To upgrade the remaining Controller nodes (or VOS devices) one at a time, follow the procedure in Upgrade the First Controller Node, above.

If your network has more than two Controller nodes (or more than two VOS devices), you can choose to upgrade them all at once.

For Releases 22.1.1 and later, to upgrade the remaining Controller nodes:

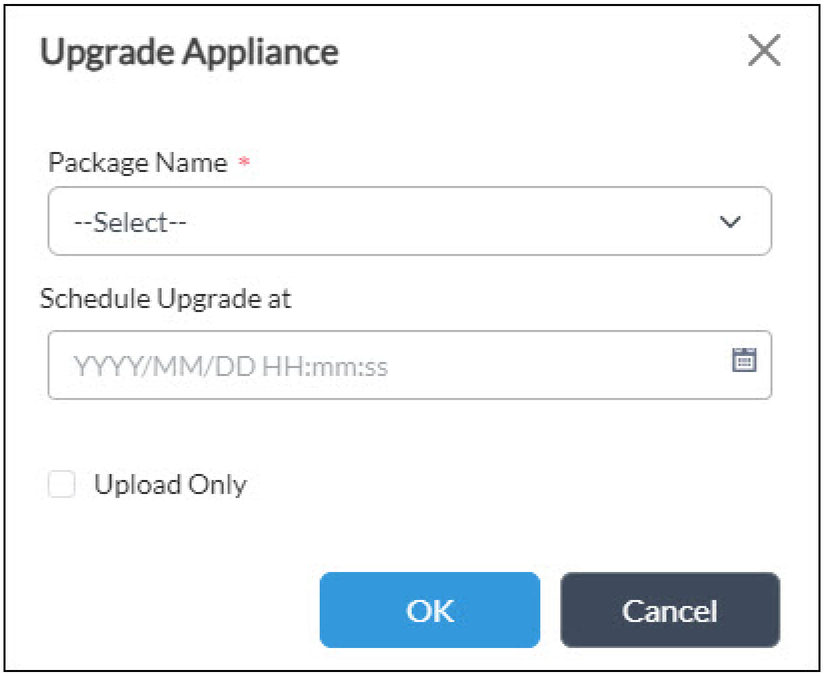
1. Check that the Controller or VOS status is synchronized and reachable:
   a. In Director view, select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Check the values in the Status columns in the main pane. Note that you cannot update a device whose state is error or unreachable.
2. In Director view:
   a. Select the Administration tab in the top menu bar.
   b. Select Appliances in the left menu bar.
   c. Select an organization in the left menu bar.

3. Select one or more Controller nodes (or VOS devices) in the main pane, and click the Upgrade Selected Appliances icon.



☐		Name	Mgmt. Address	Tags	Type	Service Start Time	Software Version	Organizations	Status			
									Config Sync	Reachability	Service	Locked
☐	⋮	SDWAN-Branch1	10.20.64.106	Branch,San_Jose	Branch	Wed, Nov 08 2023, 21:46	22.1.2-GA	Tenant9,Tenant3,Tenant6,T...	✓	✓	Up	🔓
☐	⋮	SDWAN-Branch2	10.20.64.104	Branch,Fremont	Branch	Wed, Nov 08 2023, 23:38	22.1.2-GA	Tenant5,Tenant9,Tenant3,T...	✓	✓	Up	🔓
☐	⋮	SDWAN-Branch4	10.20.64.108	Seattle,Branch	Branch	Sun, Dec 03 2023, 10:41	22.1.2-GA	Tenant5,Tenant9,Tenant3,T...	✓	✓	Up	🔓
☐	⋮	SDWAN-Branch5	10.20.64.101		Branch	Thu, Nov 09 2023, 11:42	22.1.2-GA	Tenant5,Tenant9,Tenant3,T...	✓	✓	Up	🔓
☐	⋮	SDWAN-Branch6	10.20.64.103		Branch	Thu, Nov 09 2023, 11:39	22.1.2-GA	Tenant11,Tenant12,provid...	✓	✓	Up	🔓
☐	⋮	SDWAN-Controller1	10.48.80.11	controller	Controller	Thu, Nov 09 2023, 09:47	22.1.2-GA	Tenant1,Tenant2,Tenant3,T...	✓	✓	Up	🔓
☑	⋮	SDWAN-Controller2	10.48.80.12	controller	Controller	Wed, Nov 08 2023, 19:24	22.1.2-GA	Tenant1,Tenant2,Tenant3,T...	✓	✓	Up	🔓

4. In the Upgrade Appliance popup window, enter information for the following fields:



Field	Description
Package Name (Required)	Select the name of the software image package.
Schedule Upgrade at	Select the date and time to run the automatic appliance upgrade.
Upload Only	To upload the software image package only but not upgrade the software, sele Leave the box unchecked to upgrade the software image.

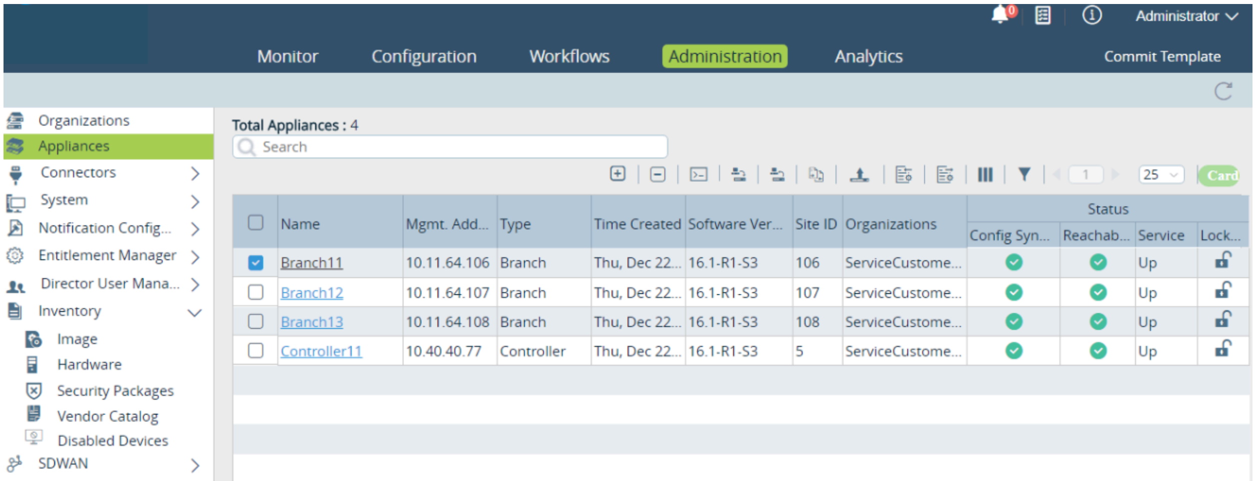
5. To view the progress of the upgrade process, click the 📋 Tasks icon.
6. If you are upgrading Controller nodes, wait for services to come up on the nodes. Then verify that each Controller has connected to the other Controllers, to all branches, and to all hubs if there are any in the network.

For Releases 21.2 and earlier, to upgrade the remaining Controller nodes:

1. Check that the Controller or VOS status is synchronized and reachable:
    a. In Director view, select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.
    c. Check the values in the Status columns in the main pane. Note that you cannot update a device whose state is error or unreachable.
2. In Director view:
    a. Select the Administration tab in the top menu bar.
    b. Select Appliances in the left menu bar.

   c. Select an organization in the left menu bar.

3. Select one or more Controller nodes (or VOS devices) in the main pane, and click the Upgrade Selected Appliances icon.

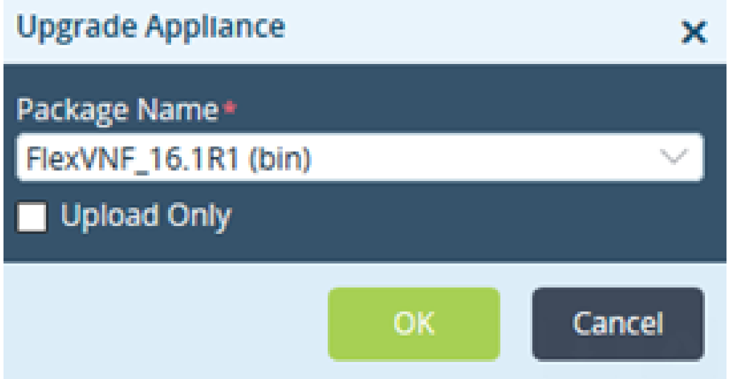


Total Appliances : 4

☐	Name	Mgmt. Add...	Type	Time Created	Software Ver...	Site ID	Organizations	Status			
								Config Syn...	Reachab...	Service	Lock...
☑	Branch11	10.11.64.106	Branch	Thu, Dec 22...	16.1-R1-S3	106	ServiceCustome...	✓	✓	Up	🔓
☐	Branch12	10.11.64.107	Branch	Thu, Dec 22...	16.1-R1-S3	107	ServiceCustome...	✓	✓	Up	🔓
☐	Branch13	10.11.64.108	Branch	Thu, Dec 22...	16.1-R1-S3	108	ServiceCustome...	✓	✓	Up	🔓
☐	Controller11	10.40.40.77	Controller	Thu, Dec 22...	16.1-R1-S3	5	ServiceCustome...	✓	✓	Up	🔓

4. Click the Upgrade Selected Appliances icon.

5. In the Upgrade Appliance popup window, enter information for the following fields:



Package Name*

FlexVNF_16.1R1 (bin)

☐ Upload Only

Field	Description
Package Name (Required)	Select the name of the software image package.
Upload Only	To upload the software image package only but not upgrade the software, s box unchecked.

6. Click OK.

7. To view the progress of the upgrade process, click the Tasks icon.

8. If you are upgrading Controller nodes, wait for services to come up on the nodes. Then verify that each Controller

node has connected to the other Controller nodes, to all branches, and to all hubs if there are any in the network.

Upgrade the Remaining Hub Devices

If you are not upgrading the software image on VOS hub devices, you can skip this section.

If you are using a hub-and-spoke topology, and if you have deployed the hub in an active-standby HA pair, upgrade the software on the standby hub of the HA pair.

To upgrade the standby hub of the HA pair, or to upgrade hubs one at a time if you have more than two hubs, follow the procedure in Upgrade the First Controller Node, above.

To upgrade the hubs all at once if you have more than two hubs, follow the procedure in Upgrade the Remaining Controller Nodes, above.

Upgrade the Remaining VOS Branch Devices

If you are not upgrading the software image on VOS devices, you can skip this section.

If any branches have two VOS devices that use an interchassis HA deployment, where one branch VOS device is the active device and a second is the standby device, upgrade the software on the standby VOS device.

To upgrate the standby VOS device in an interchassis HA deployment, or to upgrade VOS branch devices one at a time if you have more than two VOS devices. follow the procedure in Upgrade the First Controller Node, above.

To upgrade the VOS branch devices all at once if you have more than two VOS devices, follow the procedure in Upgrade the Remaining Controller Nodes, above.

Check Connectivity Between the Director Nodes and VOS Devices

Check that the upgrade Director node can connect to and manage branches that are running the same software version as the Director node.

Check that the upgraded Director node can connect to and manage existing branches that are running a software version that is older than the software running on the Director node.

Check that VOS devices whose software you have upgraded can communicate with the branches whose software has not been upgraded.

To check communication between the Director node and VOS devices, start by selecting the Monitor tab in the Director top menu bar and selecting a VOS device in the left menu bar.

Schedule Automatic Software Upgrade

For Releases 21.1.0 and later.

On a Director node, you can schedule software upgrade tasks to occur automatically. In a software upgrade tasks, you can download or upload software to one or more VOS devices at the same time, and you can commit tenant-specific templates. In a single scheduled upgrade task, you can have multiple appliances for an individual job type.

You can edit or cancel an automatic software upgrade at any time. When you edit the task, the changes apply to all the VOS devices in the list of tasks that are in the queue.

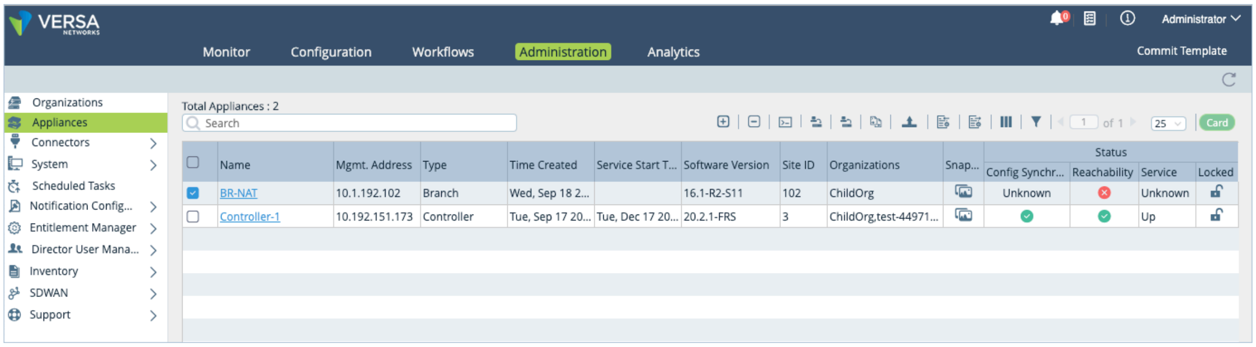
The ability to schedule automatic software upgrades uses role-based access control (RBAC), so only users with the authorized role can configure schedule modification. If a scheduling job affects multiple devices and if each device owner tenant is in a different organization, the task is visible only to the owner who has RBAC access to all the devices.

You typically schedule automatic software upgrades during a maintenance window. If a VOS device is not reachable at that time, you can configure pending tasks to resume when the device becomes reachable. If you apply (commit) a template to multiple devices, the prevalidation for the schedule job can take a few minutes to several hours.

If a scheduled software upgrade is in process and a Director HA failover occurs, the scheduled software upgrade fails.

To schedule automatic software upgrade:

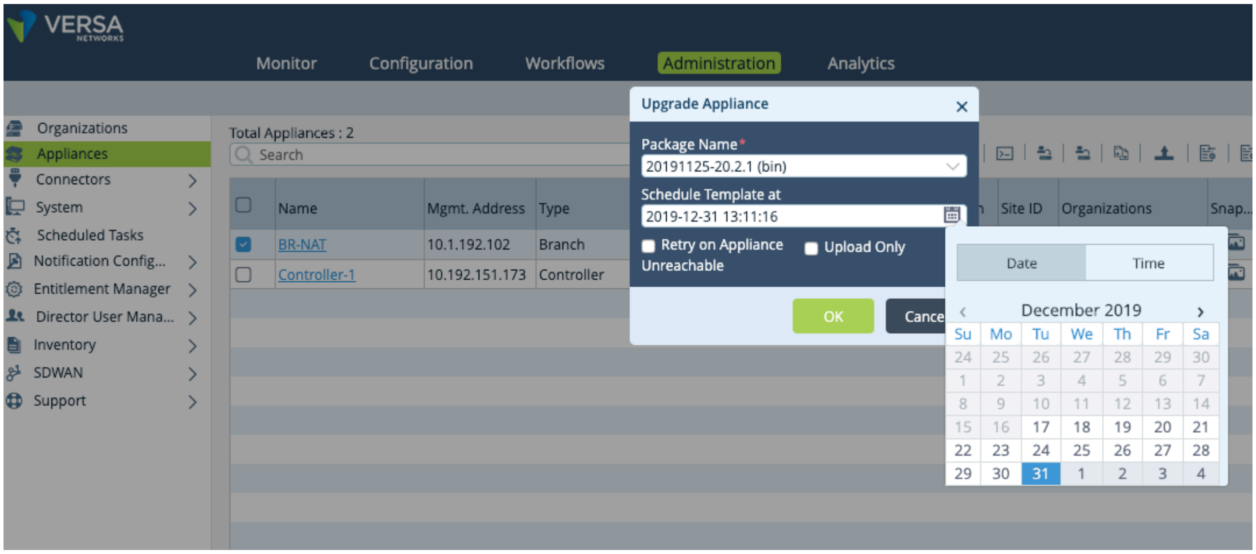
1. In Director view, select the Administration tab in the top menu bar.
2. Select Appliances in the left menu bar.
3. Select one or more Controller nodes or VOS devices in the main pane. Note that you can schedule a software upgrade on multiple Controller nodes or multiple VOS devices in a single job, but you cannot upgrade Controller and VOS devices in the same job.



Total Appliances : 2

☐	Name	Mgmt. Address	Type	Time Created	Service Start T...	Software Version	Site ID	Organizations	Snap...	Status			
										Config Synchr...	Reachability	Service	Locked
☑	BR-NAT	10.1.192.102	Branch	Wed, Sep 18 2...		16.1-R2-S11	102	ChildOrg		Unknown	✗	Unknown	
☐	Controller-1	10.192.151.173	Controller	Tue, Sep 17 20...	Tue, Dec 17 20...	20.2.1-FRS	3	ChildOrg,test-44971...		✓	✓	Up	

4. Click the Upgrade Selected Appliances icon.
5. In the Upgrade Appliance popup window, enter information for the following fields.



Total Appliances : 2

☐	Name	Mgmt. Address	Type
☑	BR-NAT	10.1.192.102	Branch
☐	Controller-1	10.192.151.173	Controller

Upgrade Appliance

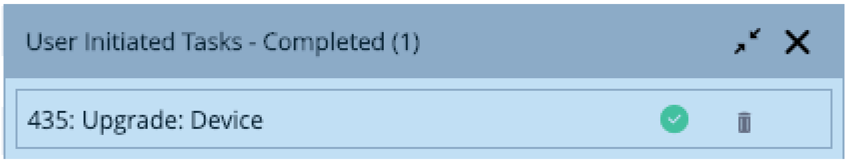
Package Name* 20191125-20.2.1 (bin)

Schedule Template at 2019-12-31 13:11:16

☐ Retry on Appliance Unreachable ☐ Upload Only

Field	Description
Package Name (Required)	Select the name of the software image package.
Schedule Template	Select the date and time to run the automatic software update.
Retry on Appliance Unreachable	Click to retry the software update if the device is not reachable at the scheduled time.
Upload Only	Click to upload the software image package only, but not upgrade the software. To upgrade the software image, leave the box unchecked.

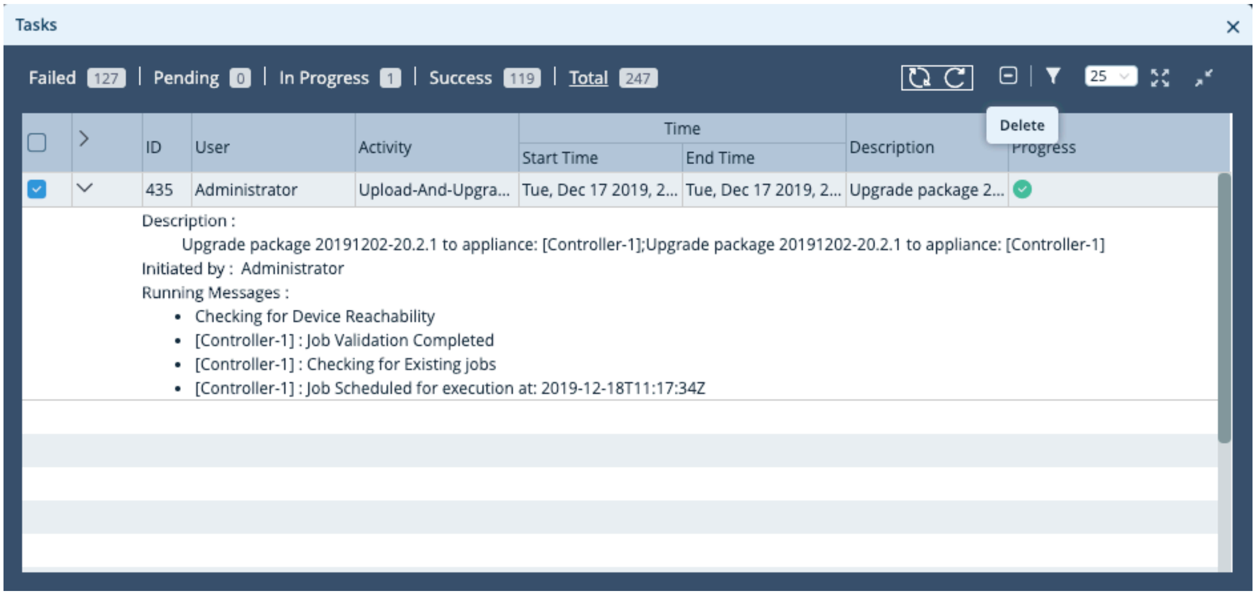
6. Click OK. A popup window confirms the user-initiated task.



User Initiated Tasks - Completed (1)

435: Upgrade: Device

7. Click the Upgrade: Device bar to open the Tasks status window.
8. To view scheduled software upgrade status, select a task.
9. To cancel the scheduled software upgrade, click the Delete icon.



Tasks
Failed 127 | Pending 0 | In Progress 1 | Success 119 | Total 247
25
Delete

☐	>	ID	User	Activity	Time		Description	Progress
					Start Time	End Time		
☑	⌄	435	Administrator	Upload-And-Upgra...	Tue, Dec 17 2019, 2...	Tue, Dec 17 2019, 2...	Upgrade package 2...	✓

Description :
Upgrade package 20191202-20.2.1 to appliance: [Controller-1];Upgrade package 20191202-20.2.1 to appliance: [Controller-1]

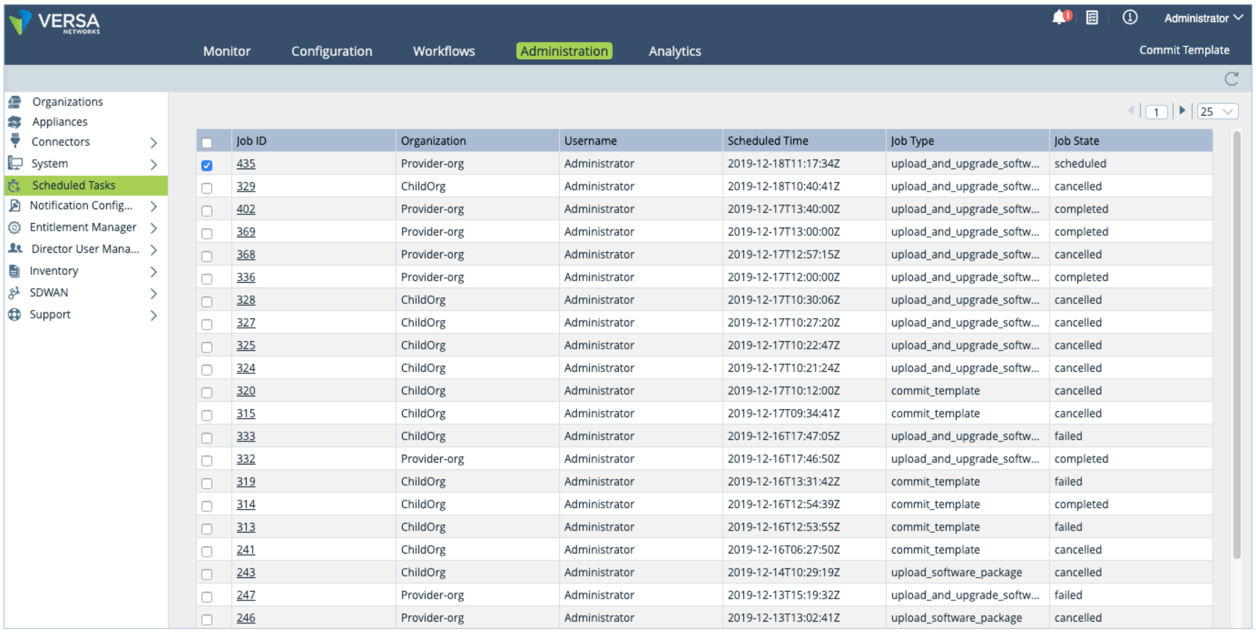
Initiated by : Administrator

Running Messages :

- Checking for Device Reachability
- [Controller-1] : Job Validation Completed
- [Controller-1] : Checking for Existing jobs
- [Controller-1] : Job Scheduled for execution at: 2019-12-18T11:17:34Z

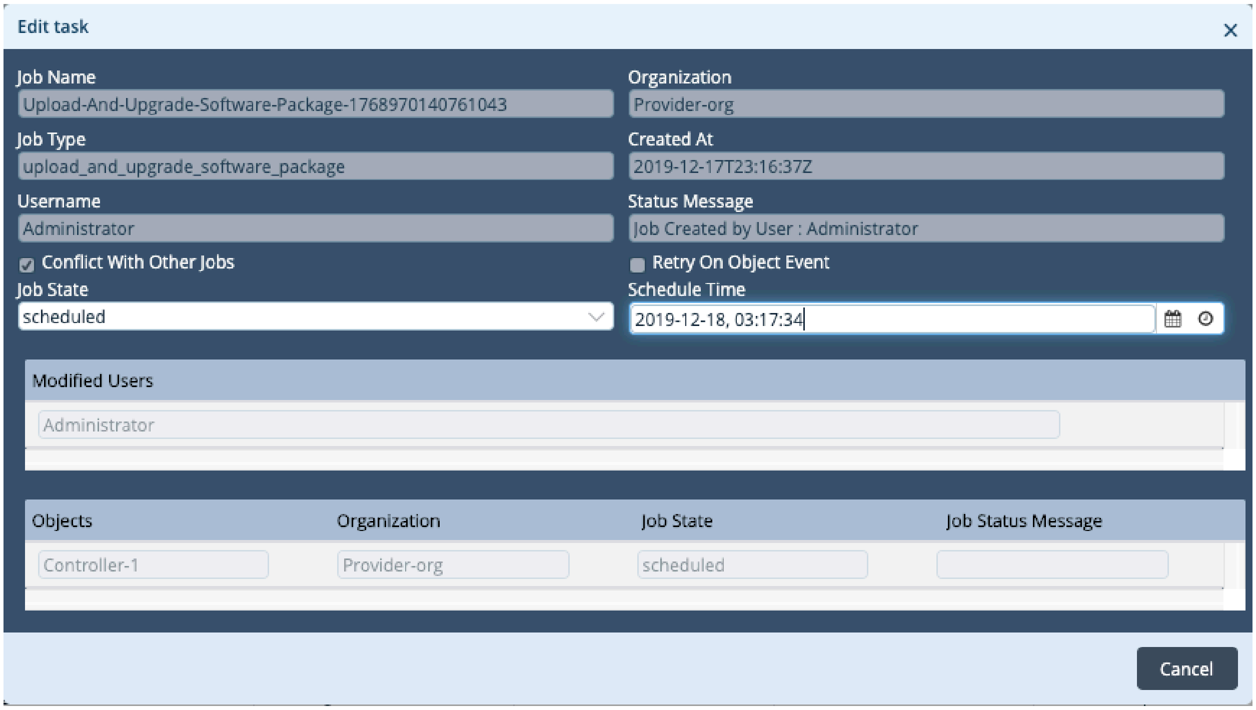
To view, edit, or delete a scheduled task:

1. In Director view, select the Administration tab in the top menu bar.
2. Select Scheduled Tasks in the left menu bar. The table in the main pane displays the scheduled tasks, including job type and job state.



☐	Job ID	Organization	Username	Scheduled Time	Job Type	Job State
☑	435	Provider-org	Administrator	2019-12-18T11:17:34Z	upload_and_upgrade_softw...	scheduled
☐	329	ChildOrg	Administrator	2019-12-18T10:40:41Z	upload_and_upgrade_softw...	cancelled
☐	402	Provider-org	Administrator	2019-12-17T13:40:00Z	upload_and_upgrade_softw...	completed
☐	369	Provider-org	Administrator	2019-12-17T13:00:00Z	upload_and_upgrade_softw...	completed
☐	368	Provider-org	Administrator	2019-12-17T12:57:15Z	upload_and_upgrade_softw...	cancelled
☐	336	Provider-org	Administrator	2019-12-17T12:00:00Z	upload_and_upgrade_softw...	completed
☐	328	ChildOrg	Administrator	2019-12-17T10:30:06Z	upload_and_upgrade_softw...	cancelled
☐	327	ChildOrg	Administrator	2019-12-17T10:27:20Z	upload_and_upgrade_softw...	cancelled
☐	325	ChildOrg	Administrator	2019-12-17T10:22:47Z	upload_and_upgrade_softw...	cancelled
☐	324	ChildOrg	Administrator	2019-12-17T10:21:24Z	upload_and_upgrade_softw...	cancelled
☐	320	ChildOrg	Administrator	2019-12-17T10:12:00Z	commit_template	cancelled
☐	315	ChildOrg	Administrator	2019-12-17T09:34:41Z	commit_template	cancelled
☐	333	ChildOrg	Administrator	2019-12-16T17:47:05Z	upload_and_upgrade_softw...	failed
☐	332	Provider-org	Administrator	2019-12-16T17:46:50Z	upload_and_upgrade_softw...	completed
☐	319	ChildOrg	Administrator	2019-12-16T13:31:42Z	commit_template	failed
☐	314	ChildOrg	Administrator	2019-12-16T12:54:39Z	commit_template	completed
☐	313	ChildOrg	Administrator	2019-12-16T12:53:55Z	commit_template	failed
☐	241	ChildOrg	Administrator	2019-12-16T06:27:50Z	commit_template	cancelled
☐	243	ChildOrg	Administrator	2019-12-14T10:29:19Z	upload_software_package	cancelled
☐	247	Provider-org	Administrator	2019-12-13T15:19:32Z	upload_and_upgrade_softw...	failed
☐	246	Provider-org	Administrator	2019-12-13T13:02:41Z	upload_software_package	cancelled

3. Select a task from the Job ID column, and then click the task number to open the Edit Task window.



Edit task

Job Name: Upload-And-Upgrade-Software-Package-1768970140761043

Organization: Provider-org

Job Type: upload_and_upgrade_software_package

Created At: 2019-12-17T23:16:37Z

Username: Administrator

Status Message: Job Created by User : Administrator

☑ Conflict With Other Jobs

□ Retry On Object Event

Job State: scheduled

Schedule Time: 2019-12-18, 03:17:34

Modified Users
Administrator

Objects	Organization	Job State	Job Status Message
Controller-1	Provider-org	scheduled	

4. Edit information in the following fields:
   - Job State—Select Cancel to delete the scheduled task.
   - Schedule Time—Click the Calendar and Clock icons to reschedule the task.
5. Click OK.
6. Click Confirm.

Supported Software Information

Releases 20.2 and later support all content described in this article, except:

- Release 21.1.0 adds support for the scheduling automatic software upgrades.

Additional Information

Configure Maintenance Mode