VOSS

# VOSS Automate
# Upgrade Guide with ISO and Template

Release 24.2

December 06, 2024

# Legal Information

DOCUMENT ID: 20241206153530

# Contents

**1 What’s New** **1**

1.1 Upgrade Guide with ISO and Template: Release 24.2 . . . . . . . . . . . . . . . . . . . . . . . 1

**2 Prepare for Upgrade** **2**

2.1 Before Upgrading . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 2

2.2 Upgrade and Data Migration . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

2.3 Using the `screen` command . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 4

2.4 VOSS Automate Hardware Specifications . . . . . . . . . . . . . . . . . . . . . . . . . . . 5

**3 Multinode Upgrade** **13**

3.1 Upgrade Unified Node Topology . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 13

3.2 Upgrade Modular Cluster Topology . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . 28

**4 Single Node Upgrade** **42**

4.1 Upgrade a Single Node Cluster Environment . . . . . . . . . . . . . . . . . . . . . . . . . 42

**Index** **55**

# 1. What's New

## 1.1. Upgrade Guide with ISO and Template: Release 24.2

- EKB-22058: Add delta sync capability to Insights syncs. See: *Before Upgrading*

  Added details on new delta-sync command

**Important:** This guide is *only* used to upgrade to a major version release, for example, 24.1, 24.2. For Patch Bundle upgrades, use the *Method of Procedure (MOP)* document.

# 2. Prepare for Upgrade

## 2.1. Before Upgrading

### 2.1.1. Dependencies

The supported upgrade paths to release 24.2 using this ISO upgrade:

- `21.4.x > 24.2`

### 2.1.2. Versions

Before starting with this upgrade, please read the following notes related to upgrades from earlier versions of the software.

#### Release 24.2 - Sync and Dashboard Management

- After upgrade to release 24.2, dashboard management is available after 30 minutes, since the scheduled `delta-sync` process initially carries out a *full sync* and thereafter an incremental resource sync. No manual sync is therefore required after upgrade. For details, see the Insights Analytics section of the Platform Guide.
- Ensure that:
  - An additional 70 GB disk is available for the Insights database
  - All application and database nodes memory allocation is 32 GB with 32 GB reservation

    See *Adding Hard Disk Space* in the Platform Guide and *VOSS Automate Hardware Specifications* in the Architecture and Hardware Specification Guide.

    This disk is needed to assign to the `insights-voss-sync:database` mount point. See *Mount the Insights Disk*.

### Release 24.1 onwards - Microsoft Teams, Deprecation of Basic Authentication

Starting with Automate 24.1, Microsoft PowerShell must be set up for app (application) registration for authentication.

See the following references:

- VOSS Automate 24.1 - Microsoft Customers, Upgrade Planning for App Registration
- Create MS Teams Service Account on Microsoft Cloud in the Core Feature Guide

### Release 24.1 onwards - Virtual Machine and ESXi Version Compatibility, and AVX Support

Before starting your upgrade, ensure that the hardware version of each of your virtual machines (VMs) is at least version 11, compatible with ESXi 6.0 and up, and that your host CPU supports AVX (Advanced Vector Extensions).

A `check cluster` command in the Automate pre-upgrade steps checks for AVX support. To ensure that AVX support is added to the VMs, you'll need to upgrade the compatibility of the VM in vCenter.

### Before upgrading to release 24.1:

- Install `EKB-21455-21.4.0_patch.script` first. Refer to `MOP-EKB-21455-21.4.0_patch.pdf`.
  - **Server Name**: https://voss.portalshape.com
  - **Path**: **Downloads > VOSS Automate > 24.1 > Upgrade > ISO**
  - **MOP**: MOP-EKB-21455-21.4.0_patch.pdf
  - **Patch File**: EKB-21455-21.4.0_patch.script

### Release 21.4 onwards - Product License Changes

From release 21.4 onwards, VOSS Automate allows for the registration and update of product licenses within the application. A licensing service is installed during installation or upgrade and a license token is associated with the platform on which it is installed.

## 2.1.3. Maintenance Windows and Upgrade Duration

**Note:** The standard **screen** command should be used where indicated. See: *Using the screen command*.

Normal operations will be interrupted during an upgrade. Perform the upgrade in a maintenance window. Refer to the type of upgrade for details on the upgrade duration.

Tasks that are marked **Prior to Maintenance Window** can be completed a few days prior to the scheduled maintenance window so that VOSS support can be contacted if needed and in order to allow for reduced downtime.

Ensure that sufficient time is allocated to the maintenance window. This may vary in accordance with your topology, number of devices and subscribers.

The information below serves as a guideline:

**Note:** Contact VOSS support if further guidance is required.

- Cluster upgrade: 4h
- Template install: 2.5h
- For a 500K Data User system (13Mil RESOURCE documents), the expected `upgrade_db` step is about 12h.
- For a 160K Data User system (2.5Mil RESOURCE documents), the expected `upgrade_db` step is about 2.5h.

You can follow the progress on the Admin Portal transaction list.

## 2.2. Upgrade and Data Migration

After the upgrade of the system with **app upgrade <file.ISO>** or **cluster upgrade <file.ISO>**, any changes and updates to core model schemas need to be added to the system database. It is recommended that this step is run in a terminal opened with the **screen** command.

This database upgrade is carried out from the Command Line Interface (CLI) by means of **voss upgrade_db**. It is recommended that this step is run in a terminal opened with the **screen** command.

From instructions in the newly upgraded ISO, the schemas of system core models are updated as required and existing data is migrated to these updated model schemas. Schema updates would include updated version numbers and may for example add or remove new model attributes to schemas and add new default data.

Migration instructions from existing model versions to new updated versions are used to create the updated model schemas and update data to be stored in the system database.

In the case of the installation of an updated template, the **app template <template_file>** command will also execute any migration instructions included in the template file to upgrade the database with the updated template data.

## 2.3. Using the `screen` command

The **screen** command is available to execute long-running commands (for example, when upgrading) in the background.

The following commands require the running of **screen**:

- **cluster provision**
- **cluster upgrade**
- **app template**
- **voss export type <args>**
- **voss export group <args>**
- **voss subscriber_data_export**

A message is displayed to indicate that **screen** should be run first:

```
This is a potentially long-running command and should be executed in a screen session
Run `screen` and then execute the command again
```

The use of **screen** is *not affected* by the use of the `--force` parameter with any of these commands.

The commands then run in a screen session that can be reconnected. The standard screen command parameters are available, in particular:

- **screen** - start a new session
- **screen -ls** - show sessions already available
- **screen -r [screen PID]** - reconnect to a disconnected session

The version of **screen** used in VOSS Automate also supports the creation of a log file. If long-running commands will be run, the log file captures screen console output up to the session timeout. A message shows:

```
timed out waiting for input: auto-logout
```

To create a screen log file:

1. Run **screen** and wait for screen to open.
2. Press **<Ctrl>-a** then **:** (colon). This will enter screen command mode at the bottom of the console.
3. Create your screen logfile in the `media/` directory:
   a. In screen command mode, type **logfile media/<screen-logfilename>.log**
   b. Press **<Enter>**
   c. Press **<Ctrl>-a** and then **H** to start writing to the log file
   d. Run your commands.

If the **screen** session times out, you can obtain console output from the log file, for example:

**$ sftp platform@<host>:media/<screen-logfilename>.log**

# 2.4. VOSS Automate Hardware Specifications

## 2.4.1. Overview

**Note:** For details around the open source software components used in Automate, see the *Open Source License Usage Guide*.

### Virtualized Hardware and Resource Oversubscription

It is recommended that no more than two Unified nodes and one Web Proxy node be run on a physical server (VMware server) and that the disk subsystems are unique for each Unified node.

VOSS Automate virtual machines should maintain a 1:1 ratio between virtual RAM and Disk hardware and physical hardware, in other words:

- 1 GB of virtual RAM (vRAM) must map to 1 GB of physical RAM
- 1 GB of virtual Disk (vDisk) storage must map to 1 GB of physical storage

For virtual CPU (vCPU), hyper-threading is supported.

## 2.4.2. Unified Node Hardware Specifications

### Single-node Cluster (cluster-of-one) Hardware Specification

This section provides the virtual machine specification for a single node cluster deployment topology in VOSS Automate.

| Node type | Quantity | VM | Memory | CPU | Disk | Network |
|---|---|---|---|---|---|---|
| Single node cluster | 1 | >= VMware 11 | 16 GB with 16 GB reservation | 4 vCPU @ 2 GHz with 4000 MHz reservation | 370 GB partitioned:<br>• 20 GB for OS<br>• 50 GB for application: 10 GB for logs, 40GB for our apps<br>• 50 GB for compressed backups<br>• 250 GB for database<br>70 GB database disk to be added after upgrade or installation. Refer to the Upgrade Guide with ISO and Template or Installation Guide. | 1 Gbit/s minimum |

For Memory and CPU, the Resource Allocation Reservation on VMware is indicated in the table. Hyper-threading is supported.

**Note:**

- From release 24.1, allowance should be made for an additional 70GB database disk to be added after upgrade or installation. This disk will be used for Insights sync.

  Refer to the Upgrade Guide with ISO and Template or Installation Guide and *Add Disks in the AWS or MS Azure Cloud Hosted Platform*.

- If memory allocations are customized, ensure that the memory reservation remains equal to the allocated memory in order to prevent possible negative side-effects due to memory reclamation.

For VMware details, refer to the VMware Support topic in the Compatibility Matrix.

The maximum number of users for a single node cluster is 50,000.

### Multinode Cluster Hardware Specification

Virtual machine requirements are specified in the table below.

| Node type | Quantity | VM | Memory | CPU | Disk | Network |
|---|---|---|---|---|---|---|
| Unified | 4 or 6 | >= VMware 11 | 32 GB with 32 GB reservation | 4 vCPU @ 2 GHz with 4000 MHz reservation | 370 GB partitioned:<br>• 20 GB for OS<br>• 50 GB for application: 10 GB for logs, 40GB for our apps<br>• 50 GB for compressed backups<br>• 250 GB for database<br>70 GB database disk to be added after upgrade or installation. Refer to the Upgrade Guide with ISO and Template or Installation Guide. | 1 Gbit/s minimum |
| WebProxy | 2 | >= VMware 11 | 4 GB with 4 GB reservation | 2 vCPU @ 2 GHz with no reservation | 70 GB partitioned:<br>• 20 GB for OS<br>• 50 GB for application | 1 Gbit/s minimum |

For Memory and CPU, the Resource Allocation Reservation on VMware is indicated in the table. Hyperthreading is supported.

**Note:**

- From release 24.1, allowance should be made for an additional 70GB database disk to be added after upgrade or installation. This disk will be used for Insights sync.

  Refer to the Upgrade Guide with ISO and Template or Installation Guide and *Add Disks in the AWS or MS Azure Cloud Hosted Platform*.

- If memory allocations are customized, ensure that the memory reservation remains equal to the allocated memory in order to prevent possible negative side-effects due to memory reclamation.

The OS disk requirement is fixed and logs are rotated to ensure that 10 GB is sufficient. 40 GB for applications is a generous allocation and does not scale with the number of users.

The Database storage partition is sized to support 250 K users. Database backups are compressed and the partition is sized to ensure that sufficient space available to support backup of 250 GB database.

**Note:** To change the TRANSACTION_LOG cap size to greater than 10GB at larger providers for operational reasons, for example for diagnostics and a longer transaction replay window, the **voss db_collection_cap TRANSACTION_LOG <10-50GB>** command can be used from the command line.

Refer to Database Commands in the Platform Guide for more details.

The resize operation will impact the usage on the disk size allocated for the database (typically, 250GB is reserved upon installation). Consider a larger database disk size allocation upon installation if a larger cap size is set.

The backup disk should be Thick Provisioned and Eager Zeroed for better performance immediately after installation.

Web Proxies are optional, but if Web Proxies are used, then they form part of the cluster to allow sharing of static data and other content as needed (for example, themes).

To set up the disk requirements, the disk should be set up on the VMware GUI Resources tab where a disk can be created. This task should be done after the OVA import but prior to the boot of the system.

For VMware details, refer to the VMware Support topic in the Compatibility Matrix.

### 2 Node Cluster Hardware Specification

Virtual machine requirements are specified in the table below.

| Node type | Quantity | VM | Memory | CPU | Disk | Network |
|---|---|---|---|---|---|---|
| Unified | = 2 | >= VMware 11 | 32 GB with 32 GB reservation | 4 vCPU @ 2 GHz with 4000 MHz reservation | 370 GB partitioned:<br>• 20 GB for OS<br>• 50 GB for application: 10 GB for logs, 40GB for our apps<br>• 50 GB for compressed backups<br>• 250 GB for database<br>70 GB database disk to be added after upgrade or installation. Refer to the Upgrade Guide with ISO and Template or Installation Guide. | 1 Gbit/s minimum |
| WebProxy | >= 0 | >= VMware 11 | 4 GB with 4 GB reservation | 2 vCPU @ 2 GHz with no reservation | 70 GB partitioned:<br>• 20 GB for OS<br>• 50 GB for application | 1 Gbit/s minimum |

For Memory and CPU, the Resource Allocation Reservation on VMware should correspond with these requirements.

**Note:**

- From release 24.1, allowance should be made for an additional 70GB database disk to be added after upgrade or installation. This disk will be used for Insights sync.

  Refer to the Upgrade Guide with ISO and Template or Installation Guide and *Add Disks in the AWS or MS Azure Cloud Hosted Platform*.

- If memory allocations are customized, ensure that the memory reservation remains equal to the allocated memory in order to prevent possible negative side-effects due to memory reclamation.

For VMware details, refer to the VMware Support topic in the Compatibility Matrix.

## 2.4.3. Modular Cluster Hardware Specifications

### Multinode Modular Cluster Hardware Specification

Virtual machine requirements are specified in the table below.

| Node type | Quantity | VM | Memory | CPU | Disk | Network |
|---|---|---|---|---|---|---|
| Application | 3 | >= VMware 11 | 32 GB with 32 GB reservation | 4 vCPU @ 2 GHz with 4000 MHz reservation | 80 GB partitioned:<br>• 20 GB for OS<br>• 50 GB for application: 10 GB for logs, 40GB for our apps | 1 Gbit/s minimum |
| Database | 3 | >= VMware 11 | 32 GB with 32 GB reservation | 4 vCPU @ 2 GHz with 4000 MHz reservation | 380 GB partitioned:<br>• 20 GB for OS<br>• 50 GB for compressed backups<br>• 50 GB for application:<br>– 10 GB for logs<br>– 40GB for our apps<br>• 250 GB for database<br>70 GB database disk to be added after upgrade or installation. Refer to the Upgrade Guide with ISO and Template or Installation Guide. | 1 Gbit/s minimum |
| WebProxy | 2 | >= VMware 11 | 4 GB with 4 GB reservation | 2 vCPU @ 2 GHz with no reservation | 70 GB partitioned:<br>• 20 GB for OS<br>• 50 GB for application | 1 Gbit/s minimum |

For Memory and CPU, the Resource Allocation Reservation on VMware is indicated in the table. Hyperthreading is supported.

**Note:**

- From release 24.1, allowance should be made for an additional 250GB database disk to be added after upgrade or installation. This disk will be used for Insights sync.

  Refer to the Upgrade Guide with ISO and Template or Installation Guide and *Add Disks in the AWS or MS Azure Cloud Hosted Platform*.

- If memory allocations are customized, ensure that the memory reservation remains equal to the allocated memory in order to prevent possible negative side-effects due to memory reclamation.

The OS disk requirement is fixed and logs are rotated to ensure that 10 GB is sufficient. 40 GB for an applications role node is a generous allocation and the size will not have to be increased with the number of users.

The Database storage partition is sized to support 250 K users. Database backups are compressed and the partition is sized to ensure that sufficient space is available to support backup of 250 GB database.

**Note:** To change the TRANSACTION_LOG cap size to greater than 10GB at larger providers for operational reasons, for example for diagnostics, the **voss db_collection_cap TRANSACTION_LOG <10-50GB>** command can be used from the command line.

Refer to Database Commands in the Platform Guide for more details.

The resize operation will impact the usage on the size of the disk allocated for the database (typically, 250GB is reserved upon installation). Consider a larger database disk size allocation upon installation if a larger cap size is set.

The backup disk should be Thick Provisioned and Eager Zeroed for better performance immediately after installation.

Web Proxies are optional, but if Web Proxies are used, then they form part of the cluster to allow sharing of static data and other content as needed (for example, themes).

To set up the disk requirements, the disk should be set up on the VMware GUI Resources tab where a disk can be created. This task should be done after the OVA import but prior to the boot of the system.

For VMware details, refer to the VMware Support topic in the Compatibility Matrix.

### 2.4.4. Add Disks in the AWS or MS Azure Cloud Hosted Platform

The steps below are required to add a disk that provides for the Insights database in release 24.1 - that should then be assigned to the `insights-voss-sync:database` mount point (refer to the final step in the *Upgrade Guide with ISO and Template* for your topology).

#### AWS

1. Create the EBS Volumes for each DB node in the Amazon EC2 console.

   Go to **EC2 > Volumes > Create volume**

   For **Volume settings**, enter:

   - Volume type: Provisioned IOPS SSD (io2)
   - Size (GiB): 70GB
   - IOPS: 750

   For **Availability Zone**:

   - Create 3 volumes in each of the zones (for example: us-east-1a, us-east-1b, us-east-1c)

2. Attach the newly created volumes to each of the database nodes.

   Go to **EC2 > Volumes > volume_id > Attach volume**

   - **Instance**: Select the database instance within the same corresponding az
   - **Device Name**: `/dev/sde` (This will display as `xvde` in drives list)

### Microsoft Azure

1. In the Microsoft Azure portal, search for Virtual Machines
   - Select each of the database nodes
   - Select **Disk** under **Properties**
2. Click **Create and attach a new disk**.
   - **LUN**: Next avaiable
   - **Disk Name**: Label according to your recommended naming convention
   - **Storage Type**: Premium SSD LRS
   - **Size**: 70GB
   - **Encryption**: Set according to your requirements
   - **Host Caching**: Read/Write

# 3. Multinode Upgrade

## 3.1. Upgrade Unified Node Topology

Read “Prepare for Upgrade” before proceeding.

### 3.1.1. Prior to Maintenance Window

#### Download Files and Check

**Note:** Ensure that the `.iso` file is available on *all* nodes.

| Description and Steps | Notes and Status |
|---|---|
| VOSS files:<br>**https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade**<br>Download `.iso` and `.template` files, where XXX matches the release.<br>• Transfer the `.iso` file to the `media/` folder of all nodes.<br>• Transfer the `.template` file to the `media/` folder of the primary node.<br>Two transfer options:<br>Either using SFTP:<br>`sftp platform@<unified_node_hostname>`<br>`cd media`<br>`put <upgrade_iso_file>`<br>`put <upgrade_template_file>`<br>Or using SCP:<br>`scp <upgrade_iso_file> platform@<unified_node_ip_address>:~/media`<br>`scp <upgrade_template_file> platform@<unified_node_ip_address>:~/media`<br>Verify that the `.iso` image and `.template` file copied:<br>`ls -l media/`<br>Verify that the original `.sha256` checksums on the Download site server match.<br>• `system checksum media/<upgrade_iso_file>`<br>`Checksum: <SHA256>`<br>• `system checksum media/<upgrade_template_file>`<br>`Checksum: <SHA256>` | |

### Version Check

Verify VMWare, Cloud Deployments, and Application version compatibility as indicated in the Compatibility Matrix, then:

| Description and Steps | Notes and Status |
|---|---|
| **Customized ``data/Settings``**<br>If `data/Settings` instances have been modified, record these or export them as JSON. The modifications can be re-applied or exported JSON instances can be merged following the upgrade. See: *Post Template Upgrade Tasks*.<br>**Version**<br>Record the current version information. This is required for upgrade troubleshooting.<br>• Log in on the Admin Portal and record the information contained in the menu: **About > Version** | |

## 3.1.2. Maintenance Window

### Security and Health Check Steps

| Description and Steps | Notes and Status |
|---|---|
| **Choose an option:**<br>• **If you're upgrading from: [21.4-PB4, 21.4-PB5]**<br>Place the system in maintenance mode to suspend any scheduled transactions. Scheduled transactions that are in progress will be allowed to complete, or otherwise, cancel data sync transactions that are in progress on the GUI. Refer to the Core Feature Guide. For details, refer to the System Maintenance Mode topic in the Platform Guide.<br>On an application node of the system, run:<br>`cluster maintenance-mode start`<br>You can verify the maintenance mode status with:<br>`cluster maintenance-mode status`<br>• **If you're upgrading from: [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]**<br>Turn off any scheduled imports to prevent syncs triggering part way through the upgrade.<br>**Note:** Schedules can easily be activated and deactivated from the **Bulk Schedule Activation** / **Deactivation** menu available on the available on the `MVS-DataSync-Dashboard`.<br>Two options are available:<br>Individually for each job:<br>1. Log in on the Admin Portal as a high level administrator above Provider level.<br>2. Select the **Scheduling** menu to view scheduled jobs.<br>3. Click each scheduled job. On the Base tab, uncheck the **Activate** check box.<br>Mass modify:<br>1. On the Admin Portal, export scheduled syncs into a bulk load sheet.<br>2. Modify the schedule settings to de-activate scheduled syncs.<br>3. Import the sheet.<br>Schedules enabled on the CLI:<br>1. Check if any schedules exist and overlap with the maintenance window:<br>`schedule list`<br>2. For overlapping schedules, disable. Run:<br>`schedule disable <job-name>`<br>Verify that the primary node is the active primary node at the time of upgrade:<br>`database config`<br>Ensure that the node on which the installation will be initiated has the `stateStr` parameter set to **PRIMARY** and has the **highest** `priority` **number** (highest priority number could vary depending on cluster layout).<br>Example output<br>`<ip address>:27020:`<br>`  priority: <number>`<br>`  stateStr: PRIMARY`<br>`  storageEngine: WiredTiger` | |

| Description and Steps | Notes and Status |
|---|---|
| The following step is needed if own private certificate and generated SAN certificates are required and the `web cert gen_csr` command was run. For details, refer to the Web Certificate Setup Options topic in the Platform Guide.<br>The steps below are needed to check if a CSR private key exists but no associated signed certificate is available.<br>Request VOSS support to run the following command (displayed for information only):<br>`for LST in /opt/platform/apps/nginx/config/csr/*;`<br>`do openssl x509 -in $LST -text -noout >/dev/null`<br>`2>&1 && SIGNED="$LST"; done`<br><br>`echo $SIGNED`<br>If the `echo $SIGNED` command output is blank, back up the `csr/` directory with for example the following command:<br>`mv /opt/platform/apps/nginx/config/csr/ /opt/platform/apps/nginx/config/csrbackup` | |

### Validate System Health

**Important:**

- Before starting the upgrade, ensure that the hardware version of each of your virtual machines (VMs) is at least version 11, compatible with ESXi 6.0 and up, and that your host CPU supports AVX (Advanced Vector Extensions).

  A `check cluster` command in the Automate pre-upgrade steps checks for AVX support. To ensure that AVX support is added to the VMs, you'll need to upgrade the compatibility of the VM in vCenter.

- Follow all of the steps in the table, in the order presented.

| Description and Steps | Notes and Status |
|---|---|
| Perform these steps:<br>1. Mount upgrade ISO:<br>`system mount`<br>2. Install the new version of the `cluster check` command:<br>`app install check_cluster`<br>For details, see the "Cluster Check" topic in the Platform Guide.<br>3. Inspect the output of this command for warnings and errors.<br>`cluster check`<br>You can also use `cluster check verbose` to see more details.<br>Verify that `avx` is enabled.<br>Review and resolve any warnings or errors before proceeding with the upgrade.<br>Contact VOSS Support for assistance, if required.<br>For troubleshooting and resolutions, also refer to the *Health Checks for Cluster Installations Guide* and *Platform Guide*.<br>If there is any sign that the paths below are over 80% full, a clean-up is needed, for example to avoid risk of full logs occurring during upgrade. Clean-up steps are indicated next to the paths:<br>`/               (call support if over 80%)`<br>`/var/log        (run: log purge)`<br>`/opt/platform   (remove any unnecessary files from /media directory)`<br>`/tmp            (reboot)`<br>On the Primary Unified Node, verify there are no pending Security Updates on any of the nodes.<br>**Note:** If you run `cluster status` after installing the new version of `cluster check`, any error message regarding a failed command can be ignored. This error message will not show after upgrade. | |

### Pre-Upgrade Steps

| | |
|---|---|
| As part of the rollback procedure, ensure that a suitable restore point is obtained prior to the start of the activity, as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed.<br>Optional: If a backup is also required, use:<br>`backup add <location-name>`<br>and<br>`backup create <location-name>`<br>For details, refer to the *Platform Guide*. | |

<table>
<thead>
<tr><th>Description and Steps</th><th>Notes and Status</th></tr>
</thead>
<tbody>
<tr><td>

After restore point creation and before upgrading: validate system health and check all services, nodes and weights for the cluster:

- `cluster run application cluster list`<br>Make sure all application nodes show 4 or 6 nodes.
- Inspect the output of this command for warnings and errors:<br>`cluster check`<br>You can also use `cluster check verbose` to see more details.
  - Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on the fresh unified nodes.
  - Check that the database weights are set. It is *critical* to ensure the weights are set before upgrading a cluster. Example output:

```
172.29.21.240:
    weight: 80
172.29.21.241:
    weight: 70
172.29.21.243:
    weight: 60
172.29.21.244:
    weight: 50
```

  - Verify the primary node in the primary site and ensure no nodes are in the 'recovering' state (`stateStr` is not `RECOVERING`). On the primary node:

</td><td></td></tr>
</tbody>
</table>

### Upgrade

**Note:**

- By default, the cluster upgrade is carried out in parallel on all nodes and without any backup in order to provide a fast upgrade.
- For systems *upgrading to 24.2 from 21.4.0 - 21.4-PB5*:
  - The VOSS platform maintenance mode will be started automatically when the `cluster upgrade` command is run. This prevents any new occurrences of scheduled transactions, including the 24.2 database syncs associated with `insights sync`. For details on `insights sync`, see the *Insights Analytics* topic in the Platform Guide.
  - The `cluster maintenance-mode stop` command must however be run manually after the maintenance window of the upgrade: *End of the Maintenance Window and Restoring Schedules*.

For details on the VOSS platform maintenance mode, see the *Maintenance Mode* topic in the Platform Guide.

| Description and Steps | Notes and Status |
|---|---|
| It is recommended that the upgrade steps are run in a terminal opened with the `screen` command.<br>Verify that the ISO has been uploaded to the `media/` directory on each node. This will speed up the upgrade time.<br>On the primary unified node:<br>• `screen`<br>• `cluster upgrade media/<upgrade_iso_file>`<br>Note: If the system reboots, do not carry out the next manual reboot step.<br>Manual reboot *only if needed*:<br>• `cluster run notme system reboot`<br>If node messages: `<node name> failed with timeout` are displayed, these can be ignored.<br>• `system reboot`<br>Since all services will be stopped, this takes some time.<br>Close `screen`:<br>• **Ctrl** + `a`, then: `\`<br>• Log in on the primary database node, then run:<br>`cluster run database app status`<br>If the report shows `insights-voss-sync:realtime stopped` on some database contact VOSS Support for assistance to perform the following on the primary database node (displayed for information only):<br>1. Run `/opt/platform/mags/insights-voss-sync-mag-script install database`<br>The output should be: `Configured Postgres secrets`<br>2. Verify that the database nodes now all have the correct mongo info:<br>`cluster run database diag config app insights-voss-sync /mongo`<br>All nodes should have the password/port/user shown as below:<br>`mongo:`<br>`   password: ********`<br>`   port: 27020`<br>`   user: insights-platform`<br>3. Restart the `insights-voss-sync:real-time` service on all database nodes:<br>`cluster run database app start insights-voss-sync:real-time` | |

All unused docker images except `selfservice` and `voss_ubuntu` images will be removed from the system at this stage.

### Post-Upgrade, Security and Health Steps

| Description and Steps | Notes and Status |
|---|---|
| Check for needed security updates. On the primary node, run:<br>• `cluster run all security check`<br>If one or more updates are required for any node, run on the primary Unified node:<br>• `cluster run all security update`<br>If upgrading a cloud deployment (MS Azure / AWS), run:<br>`cluster check`<br>If an error shows at each node:<br>`grub-pc:  package in an undesired state`<br>then request assistance from VOSS Support in order to run the command on each node (displayed for information only):<br>`dpkg --configure -a`<br>A text user interface opens and you will be prompted:<br>– “GRUB install devices:”- Do *not* select any device. Press <Tab> to highlight <Ok> and press <Enter>.<br>– At “Continuing without installing GRUB?”, press <Yes><br>– Run `cluster check` again and verify the error does not show.<br>Note: *if the system reboots, do not carry out the next manual reboot step*.<br>Manual reboot *only if needed*:<br>• `cluster run notme system reboot`<br>If node messages: `<node name> failed with timeout` are displayed, these can be ignored.<br>• `system reboot`<br>Since all services will be stopped, this takes some time. | |
| On the primary unified node, verify the cluster status:<br>• `cluster check`<br>• If any of the above commands show errors, check for further details to assist with troubleshooting:<br>`cluster run all diag health` | |
| To remove a mount directory `media/<iso_file basename>` on nodes that may have remained after for example an upgrade, run:<br>`cluster run all app cleanup` | |

| Description and Steps | Notes and Status |
|---|---|
| If upgrade is successful, the screen session can be closed by typing `exit` in the screen terminal. If errors occurred, keep the screen terminal open for troubleshooting purposes and contact VOSS support. | |

### Database Schema Upgrade

| Description and Steps | Notes and Status |
|---|---|
| It is recommended that the upgrade steps are run in a terminal opened with the `screen` command.<br>On the primary unified node:<br>• `screen`<br>• `voss upgrade_db`<br>Check cluster status<br>• `cluster check` | |

### Template Upgrade

| Description and Steps | Notes and Status |
|---|---|
| It is recommended that the upgrade steps are run in a terminal opened with the `screen` command.<br>On the primary unified node:<br>• `screen`<br>• `app template media/<VOSS Automate.template>` | |

The following message appears:

```
Running the DB-query to find the current environment's
existing solution deployment config...
```

- Python functions are deployed
- System artifacts are imported.

> **Note:** In order to carry out fewer upgrade steps, the updates of instances of some models are skipped in the cases where:
>
> - `data/CallManager` instance does not exist as instance in `data/NetworkDeviceList`
> - `data/CallManager` instance exists, but `data/NetworkDeviceList` is empty
> - Call Manager AXL Generic Driver and Call Manager Control Center Services match the `data/CallManager` IP

The template upgrade automatically detects the deployment mode: “Enterprise” or “Provider”

A message displays according to the selected deployment type. Check for one of the messages below:

```
Importing EnterpriseOverlay.json

Importing ProviderOverlay.json ...
```

The template install automatically restarts necessary applications. If a cluster is detected, the installation propagates changes throughout the cluster.

<table>
<tr><th>Description and Steps</th><th>Notes and Status</th></tr>
<tr><td>

Review the output from the `app template` command and confirm that the upgrade message appears:

```
Deployment summary of PREVIOUS template solution
(i.e. BEFORE upgrade):
------------------------------------------------


Product: [PRODUCT]
Version: [PREVIOUS PRODUCT RELEASE]
Iteration-version: [PREVIOUS ITERATION]
Platform-version: [PREVIOUS PLATFORM VERSION]
```

This is followed by updated product and version details:

```
Deployment summary of UPDATED template solution
(i.e. current values after installation):
----------------------------------------------

Product: [PRODUCT]
Version: [UPDATED PRODUCT RELEASE]
Iteration-version: [UPDATED ITERATION]
Platform-version: [UPDATED PLATFORM VERSION]
```

</td><td></td></tr>
</table>

| Description and Steps | Notes and Status |
|---|---|
| • If no errors are indicated, create a restore point.<br>This restore point can be used if post-upgrade patches that may be required, fail. As part of the rollback procedure, ensure that a suitable restore point is obtained prior to the start of the activity, as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed. | |
| For an unsupported upgrade path, the install script stops with the message:<br>`Upgrade failed due to unsupported upgrade path.`<br>`Please log in as sysadmin`<br>`and see Transaction logs for more detail.`<br>You can roll back as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed. | |
| If there are errors for another reason, the install script stops with a failure message listing the problem. Contact VOSS support. | |
| Verify the `extra_functions` have the *same checksum* across the cluster.<br>• `cluster run application voss get_extra_functions_version -c` | |
| Post upgrade migrations:<br>On a single node of a cluster, run:<br>• `voss post-upgrade-migrations` | |

Data migrations that are not critical to system operation can have significant execution time at scale. These need to be performed after the primary upgrade, allowing the migration to proceed whilst the system is in use - thereby limiting upgrade windows.

A transaction is queued on VOSS Automate and its progress is displayed as it executes.

| Description and Steps | Notes and Status |
|---|---|
| Check cluster status and health<br>• `cluster status` | |

### Post Template Upgrade Tasks

| Description and Steps | Notes and Status |
|---|---|
| **Verify the upgrade**<br>Log in on the Admin Portal and check the information contained in the **About > Version** menu. Confirm that versions have upgraded.<br>• **Release** should show `XXX`<br>• **Platform Version** should show `XXX`<br>where `XXX` corresponds with the release number of the upgrade. | |
| • Check themes on all roles are set correctly | |
| • For configurations that make use of the Northbound Billing Integration (NBI), please check the service status of NBI and restart if necessary. | |

### Log Files and Error Checks

| Description and Steps | Notes and Status |
|---|---|
| Inspect the output of the command line interface for upgrade errors, for example `File import failed!` or `Failed to execute command.`<br>Use the `log view` command to view any log files indicated in the error messages, for example, run the command if the following message appears:<br>`For more information refer to the execution log file with`<br>`'log view platform/execute.log'`<br>For example, if it is required send all the install log files in the `install` directory to an SFTP server:<br>• `log send sftp://x.x.x.x install` | |
| Log in on the Admin Portal as system level administrator, go to **Administration Tools > Transaction** and inspect the transactions list for errors. | |

### 3.1.3. Post Maintenance Window

#### End of the Maintenance Window and Restoring Schedules

| Description and Steps | Notes and Status |
|---|---|
| On the CLI:<br>Run the **cluster maintenance-mode stop** command to end the VOSS maintenance mode when upgrading to 24.2 from 21.4 or 21.4.-PBx.<br>This will allow scheduled data sync transactions to resume, including **insights sync** operations added in 24.1.<br>For details on the VOSS platform maintenance mode, see the *Maintenance Mode* topic in the Platform Guide.<br>• **If you're upgrading from: [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]**<br>Restore Schedules<br>**Note:** Schedules can easily be activated and deactivated from the **Bulk Schedule Activation / Deactivation** menu available on the available on the `MVS-DataSync-Dashboard`.<br>Re-enable scheduled imports if any were disabled prior to the upgrade.<br>Individually for each job:<br>1. Log in on the Admin Portal as a high level administrator above Provider level.<br>2. Select the **Scheduling** menu to view scheduled jobs.<br>3. Click each scheduled job. On the Base tab, check the **Activate** check box.<br>Mass modify:<br>1. Modify the exported sheet of schedules to activate scheduled syncs.<br>2. Import the sheet.<br>**Note:** Select the **Skip next execution** option if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter.<br>Schedules enabled on the CLI:<br>For disabled schedules that were overlapping the maintenance window, enable.<br>Run **schedule enable <job-name>**. | |

### Licensing (outside, after Maintenance Window)

| Description and Steps | Notes and Status |
|---|---|
| From release 21.4 onwards, the deployment needs to be licensed. After installation, a 7-day grace period is available to license the product. Since license processing is only scheduled every hour, if you wish to license immediately, first run **voss check-license** from the primary unified node CLI.<br>1. Obtain the required license token from VOSS.<br>2. Steps for GUI and CLI:<br>a. To license through the GUI, follow steps indicated in Product License Management in the Core Feature Guide.<br>b. To license through the CLI, follow steps indicated in Product Licensing in the Platform Guide. | |

### Mount the Insights disk

<table>
<tr><th>Description and Steps</th><th>Notes and Status</th></tr>
<tr><td>

*On each unified node*, assign the `insights-voss-sync:database` mount point to the drive added for the Insights database prior to upgrade.
For example, if `drives list` shows the added disk as:

```
Unused disks:
sde
```

then run the command
`drives add sde insights-voss-sync:database`
on each unified node where the drive has been added.
Sample output (the message below can be ignored on release 24.2:

> `WARNING: Failed to connect to lvmetad. Falling back to device scanning.`)

```
$ drives add sde insights-voss-sync:database
Configuration setting "devices/scan_lvs" unknown.
Configuration setting "devices/allow_mixed_block_sizes" unknown.
WARNING: Failed to connect to lvmetad. Falling back to device scanning.
71ad98e0-7622-49ad-9fg9-db04055e82bc
Application insights-voss-sync processes stopped.
Migrating data to new drive - this can take several minutes
Data migration complete - reassigning drive
Checking that /dev/sde1 is mounted
Checking that /dev/dm-0 is mounted
/opt/platform/apps/mongodb/dbroot
Checking that /dev/sdc1 is mounted
/backups

Application services:firewall processes stopped.
Reconfiguring applications...
Application insights-voss-sync processes started.
```

With release 24.2, the initial management of dashboards on the GUI and use of VOSS Wingman is available after the first scheduled `delta-sync` of data - which is scheduled to run every 30 minutes. No manual sync is therefore required after upgrade.
For details, see the Insights Analytics section of the Platform Guide.

</td><td></td></tr>
</table>

# 3.2. Upgrade Modular Cluster Topology

Read “Prepare for Upgrade” before proceeding.

## 3.2.1. Prior to Maintenance Window

### Verify Primary Database Node and Application Node

1. To verify the *primary application node* (UN2), run the following command on the node:

   ```
   cluster primary role application
   ```

   The output should be *true*, for example:

   ```
   platform@UN2:~$ cluster primary role application
   is_primary: true
   ```

2. To verify the *primary database node* (UN1), run the following command on the node:

   ```
   cluster primary role database
   ```

   The output should be *true*, for example:

   ```
   platform@UN1:~$ cluster primary role database
   is_primary: true
   ```

### Download and Check Files

Ensure that the `.iso` file is available on *all* nodes.

| Steps | Status |
|---|---|
| 1. Go to the download location for VOSS files (where *XXX* is the release number): **https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade**<br>2. Download the relevant `.iso` and `.template` files.<br>3. Transfer the files, using *either* SFTP or SCP:<br>• Transfer the `.iso` file to the `media/` folder of all nodes.<br>• Transfer the `.template` file to the `media/` folder of the primary application node.<br>Transfer using SFTP:<br>`sftp platform@<unified_node_hostname>`<br>`cd media`<br>`put <upgrade_iso_file>`<br>`put <upgrade_template_file>`<br>Transfer using SCP:<br>`scp <upgrade_iso_file> platform@<unified_node_ip_address>:~/media`<br>`scp <upgrade_template_file> platform@<unified_node_ip_address>:~/media`<br>4. Verify that the `.iso` image and `.template` file copied:<br>`ls -l media/`<br>5. Verify that the original `.sha256` checksums on the Download site match:<br>• Primary database node, run: `system checksum media/<upgrade_iso_file>`<br>`Checksum: <SHA256>`<br>• Primary application node, run: `system checksum media/<upgrade_template_file>`<br>`Checksum: <SHA256>` | |

## Version Check

In this step you'll verify and make a note for the current version information, which is required for upgrade troubleshooting.

**Note:** Also verify VMWare, Cloud Deployments, and Application version compatibility, as indicated in the Compatibility Matrix.

| Steps | Status |
|---|---|
| 1. Log in to the Admin Portal.<br>2. Go to **About > Version**.<br>3. Make a note of the system version information. | |

### 3.2.2. Maintenance Window

#### Security and Health Check

| Steps | Status |
|---|---|
| 1. Choose an option:<br>**If upgrading from [21.4-PB4, 21.4-PB5]**:<br>Place the system in maintenance mode and suspend any scheduled transactions. On an application node of the system, run the following command:<br>`cluster maintenance-mode start`<br>In-progress scheduled transactions will be allowed to complete, else, cancel data sync transactions that are in progress on the GUI. See *System Maintenance Mode* in the Platform Guide.<br>Verify maintenance mode status: `cluster maintenance-mode status`<br>**If upgrading from [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]**:<br>Turn off any scheduled imports to prevent syncs triggering part way through the upgrade, either *individually for each job*, or *mass modify*:<br>**Note:** Schedules can easily be activated and deactivated via the **Bulk Schedule Activation** / **Deactivation** menu (available on the `MVS-DataSync-Dashboard`).<br>• Individually for each job:<br>a. Log in on the Admin Portal as a high level admin (above Provider).<br>b. Select the **Scheduling** menu to view scheduled jobs.<br>c. **For each scheduled job, on the Base tab, clear the Activate checkbox to** disable this setting.<br>• Mass modify:<br>a. In the Admin Portal, export scheduled syncs into a bulk load sheet.<br>b. Modify schedule settings to de-activate scheduled syncs.<br>c. Import the sheet.<br>Turn off schedules enabled on the CLI:<br>• Run `schedule list` to check if any schedules exist and overlap with the maintenance window.<br>• For overlapping schedules run `schedule disable <job-name>` to disable. | |

| Steps | Status |
|---|---|

2. Verify that the primary database node is the active primary node at the time of upgrade: `database config`
3. Ensure that the node on which installation will be initiated has the `stateStr` parameter set to **PRIMARY** and has the **highest** `priority` **number**.
   The highest priority number could vary depending on cluster layout.
   Example output

   ```
   <ip address>:27020:
   priority: <number>
   stateStr: PRIMARY
   storageEngine: WiredTiger
   ```

4. This step checks if a CSR private key exists but no associated signed certificate is available. This step is required *ONLY* if own private certificate and generated SAN certificates are required and the `web cert gen_csr` command was run. For details, see *Web Certificate Setup Options* in the Platform Guide.

The steps below are needed to check if a CSR private key exists but no associated signed certificate is available.
Request VOSS support to run the following command (displayed for information only):

```
if [ -d /opt/platform/apps/nginx/config/csr/ ] ;
then
  for LST in /opt/platform/apps/nginx/config/csr/*;
  do
    openssl x509 -in $LST -text -noout >/dev/null 2>&1 && SIGNED="$LST";
  done;
  echo $SIGNED;
else:
  echo "No further action required";
fi
```

If the `echo $SIGNED` command output is blank, back up the `csr/` directory with for example the following command:
`mv /opt/platform/apps/nginx/config/csr/ /opt/platform/apps/nginx/config/csrbackup`

### Validate System Health

**Important:** Before starting the upgrade, ensure that the hardware version of each of your virtual machines (VMs) is at least version 11, compatible with ESXi 6.0 and up, and that your host CPU supports AVX (Advanced Vector Extensions).

A `check cluster` command in the Automate pre-upgrade steps checks for AVX support. To ensure that AVX support is added to the VMs, you'll need to upgrade the compatibility of the VM in vCenter.

| Steps | Status |
|---|---|
| 1. Mount upgrade ISO: `system mount`<br>2. Install the new version of the cluster check command: `app install check_cluster`<br>See *Cluster Check* in the Platform Guide.<br>3. Inspect the output of this command for warnings: `cluster check`<br>You can also use `cluster check verbose` for more details for example, to check that `avx` is enabled. Review and resolve any warnings or errors before proceeding with the upgrade. Contact VOSS Support for assistance, if required.<br>For troubleshooting and resolutions, also see the *Health Checks for Cluster Installations Guide* and the *Platform Guide*.<br>If there is any sign that the paths below are over 80% full, a clean-up is required, for example, to avoid the risk of full logs occurring during upgrade:<br>• `/` - Contact VOSS Support if over 80%<br>• `/var/log` - Run `log purge`<br>• `/opt/platform` - Remove any unnecessary files from `/media` directory<br>• `/tmp` - Reboot<br>4. On the primary application node, verify that there are no pending security updates on any of the nodes.<br>If you run `cluster status` after installing the new version of `cluster check`, any error message regarding a failed command can be ignored. This error message will not show after upgrade. | |

### Pre-Upgrade

| Steps | Status |
|---|---|
| 1. Obtain a suitable restore point as part of the rollback procedure (as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed)<br>Optionally, if a backup is also required, use the following commands on the primary database node:<br>`backup add <location-name>`<br>`backup create <location-name>`<br>For details, see the *Platform Guide*<br>2. Validate system health and check all services, nodes, and weights for the cluster:<br>• Run `cluster run application cluster list`, and ensure that all application nodes show.<br>• Run `cluster check`, then inspect the output of this command for warnings and errors.<br>You can use the `cluster check verbose` command to see more details.<br>– Ensure that no services are stopped/broken. Note that the following message is normal on fresh database nodes: “suspended waiting for mongo”<br>– *Important*! Check that the database weights are set before upgrading a cluster.<br>Example output:<br>`172.29.21.240:`<br>`    weight: 80`<br>`172.29.21.241:`<br>`    weight: 70`<br>`172.29.21.243:`<br>`    weight: 60`<br>`172.29.21.244:`<br>`    weight: 50`<br>• Verify the primary node in the primary site and ensure no nodes are in the *recovering* state (`stateStr` is not `RECOVERING`).<br>3. On the primary application node, run the following command to verify that there are no pending security updates on any of the nodes:<br>`cluster run all security check` | |

### Upgrade

It is recommended that the upgrade steps are run in a terminal opened with the `screen` command.

By default, the cluster upgrade is carried out in parallel on all nodes and without any backup in order to provide a fast upgrade.

**Note:** For systems upgrading to 24.2 from 21.4.0 - 21.4-PB5, the VOSS platform maintenance mode starts automatically when running `cluster upgrade`. This prevents any new occurrences of scheduled transactions, including the 24.2 database syncs associated with `insights sync`. For details, see *Insights Analytics* in the Platform Guide.

The `cluster maintenance-mode stop` command must however be run manually after the maintenance window of the upgrade: *End of Maintenance Window and Restore Schedules*.

For details on the VOSS platform maintenance mode, see *Maintenance Mode* in the Platform Guide.

| Steps | Status |
|---|---|
| 1. Verify that the ISO has been uploaded to the `media/` directory on each node. This speeds up the upgrade time.<br>On the primary database node, run the following commands:<br>`screen`<br>`cluster upgrade media/<upgrade_iso_file>`<br>2. **Ctrl** + `a`, then \ to close `screen`.<br>3. Log in on the primary database node, then run:<br>`cluster run database app status`<br>If the report shows `insights-voss-sync:realtime stopped` on some database contact VOSS Support for assistance to perform the following on the primary database node (displayed for information only):<br>1. Run `/opt/platform/mags/insights-voss-sync-mag-script install database`<br>The output should be: `Configured Postgres secrets`<br>2. Verify that the database nodes now all have the correct mongo info:<br>`cluster run database diag config app insights-voss-sync /mongo`<br>All nodes should have the password/port/user shown as below:<br>`mongo:`<br>`   password: ********`<br>`   port: 27020`<br>`   user: insights-platform`<br>3. Restart the `insights-voss-sync:real-time` service on all database nodes:<br>`cluster run database app start insights-voss-sync:real-time` | |

**Note:** All unused docker images except `selfservice` and `voss_ubuntu` images will be removed from the system at this stage.

### Post-Upgrade and Health Steps

| Steps | Status |
|---|---|
| 1. Check for required security updates. On the primary application node, run `cluster run all security check`<br>2. If security updates are required on any nodes, run the following on the primary application node: `cluster run all security update`<br>If upgrading a Cloud deployment (Microsoft Azure or AWS), run `cluster check`.<br>**Note:** If the `grub-pc:  package in an undesired state` error displays at each node, contact VOSS Support for assistance. Support runs the following command on each node (displayed for informational purposes only):<br>`dpkg --configure -a`<br>Follow the prompts that display in the text window:<br>a. At `GRUB install devices`, do *not* select any device. Press **<Tab>** to highlight, then **<Ok>**, and then press **<Enter>**.<br>b. At `Continuing without installing GRUB?`, press **<Yes>**.<br>c. Run `cluster check` again, and verify the error no longer displays.<br>3. If the system does not automatically reboot and you need to reboot manually:<br>a. Run `cluster run notme system reboot`. You can ignore the following node messages: `<node name> failed with timeout`.<br>b. Run `system reboot`. This takes some time because all services are stopped.<br>4. Verify cluster status. On the primary node, run `cluster check`.<br>5. If any errors display, run `cluster run all diag health` for details that may help with troubleshooting.<br>6. To remove a mount directory (`media/<iso_file basename>`) on nodes that may have remained, after an upgrade for example, run the following on the primary database node: `cluster run all app cleanup`<br>7. If the upgrade succeeds, type `exit` in the terminal to close the `screen` session.<br>If there are errors, keep the `screen` terminal open for troubleshooting and contact VOSS Support. | |

### Database Schema Upgrade

It is recommended that the upgrade steps are run in a terminal opened with the `screen` command.

| Steps | Status |
|---|---|
| 1. On the primary application node, run the following:<br>`screen`<br>`voss upgrade_db`<br>• **voss upgrade_db**<br>2. Check cluster status: `cluster check` | |

### Template Upgrade

It is recommended that the upgrade steps are run in a terminal opened with the `screen` command.

| Steps | Status |
|---|---|
| 1. On the primary application node, run the following commands:<br>`screen`<br>`app template media/<VOSS Automate.template>`<br>2. View the message that displays:<br>`Running the DB-query to find the current environment's`<br>`existing solution deployment config ...`<br>3. View progress:<br>• Python functions are deployed.<br>• System artifacts are imported.<br>**Note:** To perform fewer upgrade steps, updates of instances of some models are skipped, where:<br>• `data/CallManager` instance does not exist as instance in `data/NetworkDeviceList`<br>• `data/CallManager` instance exists, but `data/NetworkDeviceList` is empty<br>• Call Manager AXL Generic Driver and Call Manager Control Center Services match the `data/CallManager` IP<br>• The template upgrade automatically detects the deployment mode, *Enterprise* or *Provider*. A system message displays for the selected deployment mode:<br>`Importing EnterpriseOverlay.json`<br>`Importing ProviderOverlay.json`<br>• The template install automatically restarts necessary applications. If a cluster is detected, the installation propagates changes throughout the cluster. | |

<table>
<tr><th>Steps</th><th>Status</th></tr>
<tr><td>

4. Review the output from the `app template` command and confirm that the upgrade message displays:

```
Deployment summary of PREVIOUS template solution
(i.e. BEFORE upgrade):
-------------------------------------------------

Product: [PRODUCT]
Version: [PREVIOUS PRODUCT RELEASE]
Iteration-version: [PREVIOUS ITERATION]
Platform-version: [PREVIOUS PLATFORM VERSION]
```

This is followed by updated product and version details:

```
Deployment summary of UPDATED template solution
(i.e. current values after installation):
-----------------------------------------------

Product: [PRODUCT]
Version: [UPDATED PRODUCT RELEASE]
Iteration-version: [UPDATED ITERATION]
Platform-version: [UPDATED PLATFORM VERSION]
```

</td><td></td></tr>
<tr><td>

5. If no errors are indicated, create a restore point.
As part of the rollback procedure, ensure that a suitable restore point is obtained prior to the start of the activity, as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed.
For unsupported upgrade paths, the install script stops with the message:

```
Upgrade failed due to unsupported upgrade path.
Please log in as sysadmin and see Transaction logs for more detail.

You can roll back as per the guidelines for the infrastructure on␣
↪which the
VOSS Automate platform is deployed.
```

If there are errors for another reason, the install script stops with a failure message listing the problem. Contact VOSS Support.

</td><td></td></tr>
</table>

| Steps | Status |
|---|---|
| 6. On the primary application node, run the following command to verify that the `extra_functions` have the *same checksum* across the cluster:<br>`cluster run application voss get_extra_functions_version -c`<br>7. For post-upgrade migrations, run the following command on a single application node of a cluster:<br>`voss post-upgrade-migrations`<br>Data migrations that are not critical to system operation can have significant execution time at scale. These need to be performed after the primary upgrade, allowing the migration to proceed while the system is in use - thereby limiting upgrade windows. | |
| 8. View transaction progress. A transaction is queued on VOSS Automate and its progress displays as it executes.<br>9. On the primary database node, check cluster status and health:<br>`cluster status` | |

### Post Template Upgrade

| Steps | Status |
|---|---|
| 1. Verify the upgrade:<br>• Log in on the Admin Portal, and check version details in **About > Version**.<br>• Confirm that versions are upgraded (where "XXX" is the release version).<br>– **Release** should display `XXX`<br>– **Platform Version** should display `XXX`<br>2. Check that themes on all roles are set correctly.<br>3. For configurations using Northbound Billing Integration (NBI), check the service status of NBI, and restart if necessary. | |

### Log Files and Error Checks

| Steps | Status |
|---|---|
| 1. Inspect the output of the command line interface for upgrade errors, for example, `File import failed!` or *Failed to execute command*.<br>2. On the primary application node, use the `log view` command to view any log files indicated in the error messages. For example, run this command if the following message displays:<br>For more information refer to the execution log file with ``log view platform/execute.log``<br>If required, send all the install log files in the `install` directory to an SFTP server:<br>`log send sftp://x.x.x.x install`<br>3. Log in on the Admin Portal as system level admin, then go to **Administration Tools > Transaction**, and inspect the transaction list for errors. | |

## 3.2.3. Post Maintenance Window

### End of Maintenance Window and Restore Schedules

| Steps | Status |
|---|---|
| 1. On the CLI, when upgrading to 24.2 from 21.4 or 21.4.-PBx., run the following command to end the VOSS maintenance mode:<br>`cluster maintenance-mode stop`<br>Scheduled data sync transactions can now resume, including `insights sync` operations added in 24.1. For details on the VOSS platform maintenance mode, see *Maintenance Mode* in the Platform Guide.<br>2. Restore schedules:<br>Schedules can easily be activated and deactivated from the **Bulk Schedule Activation** / **Deactivation** menu available on the **MVS-DataSync-Dashboard**.<br>If you're upgrading from [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]:<br>Re-enable scheduled imports if any were disabled prior to the upgrade. There are two ways to do this, either individually for each job, or mass modify:<br>• Individually for each job:<br>1. Log in on the Admin Portal as a high level admin (above Provider level).<br>2. Select the **Scheduling** menu to view scheduled jobs.<br>3. Click each scheduled job, and on the **Base** tab, select the **Activate** checkbox.<br>• Mass modify:<br>1. Modify the exported sheet of schedules to activate scheduled syncs.<br>2. Import the sheet.<br>If you don't want to execute schedules overlapping the maintenance window but only execute afterwards, select **Skip next execution**.<br>For schedules enabled on the CLI, enable any disabled schedules that were overlapping the maintenance window:<br>`schedule enable <job-name>` | |

### Licensing

The Automate deployment requires a license. After installation, a 7-day grace period is available to license the product.

Since license processing is only scheduled every hour, if you wish to license immediately, first run `voss check-license` from the primary application node CLI.

| Steps | Status |
|---|---|
| 1. Obtain the required license token from VOSS.<br>2. Apply the license:<br>• If applying a license via the GUI, follow the steps indicated in the *Product License Management* section of the Core Feature Guide.<br>• If applying a license through the CLI, follow the steps indicated in *Product Licensing* in the Platform Guide. | |

### Mount the Insights Disk

| Steps | Status |
|---|---|

1. On each database node, assign the *insights-voss-sync:database* mount point to the drive added for the Insights database prior to upgrade.
   For example, if `drives list` shows the added disk as . . .

   ```
   Unused disks:
   sde
   ```

   Then run the following command on each unified node where the drive has been added:
   `drives add sde insights-voss-sync:database`
   Sample output:

   ```
   $ drives add sde insights-voss-sync:database
   Configuration setting "devices/scan_lvs" unknown.
   Configuration setting "devices/allow_mixed_block_sizes" unknown.
   WARNING: Failed to connect to lvmetad. Falling back to device scanning.
   71ad98e0-7622-49ad-9fg9-db04055e82bc
   Application insights-voss-sync processes stopped.
   Migrating data to new drive - this can take several minutes
   Data migration complete - reassigning drive
   Checking that /dev/sde1 is mounted
   Checking that /dev/dm-0 is mounted
   /opt/platform/apps/mongodb/dbroot
   Checking that /dev/sdc1 is mounted
   /backups

   Application services:firewall processes stopped.
   Reconfiguring applications...
   Application insights-voss-sync processes started.
   ```

   **Note:** The following message can be ignored on release 24.1: *Warning: Failed to connect to lvmetad. Falling back to device scanning.*

2. With release 24.2, the initial management of dashboards on the GUI and use of VOSS Wingman is available after the first scheduled `delta-sync` of data - which is scheduled to run every 30 minutes. No manual sync is therefore required after upgrade.
   For details, see the Insights Analytics section of the Platform Guide.

# 4. Single Node Upgrade

## 4.1. Upgrade a Single Node Cluster Environment

Read “Prepare for Upgrade” before proceeding.

### 4.1.1. Prior to Maintenance Window

#### Download Files and Check

| Description and Steps | Notes and Status |
|---|---|
| VOSS files:<br>**https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade**<br>Download `.iso` and `.template` files, where XXX matches the release. Transfer the file to the `media/` folder. Two options:<br>Either using SFTP:<br>`sftp platform@<unified_node_hostname>`<br>`cd media`<br>`put <upgrade_iso_file>`<br>`put <upgrade_template_file>`<br>Or using SCP:<br>`scp <upgrade_iso_file> platform@<unified_node_ip_address>:~/media`<br>`scp <upgrade_template_file> platform@<unified_node_ip_address>:~/media`<br>Verify that the `.iso` image and `.template` file copied:<br>• `ls -l media/`<br>Verify that the original `.sha256` checksums on the Download site match.<br>• `system checksum media/<upgrade_iso_file>`<br>`Checksum: <SHA256>`<br>• `system checksum media/<upgrade_template_file>`<br>`Checksum: <SHA256>` | |

### Security and Health Steps Single Node Cluster

<table>
<tr><th>Description and Steps</th><th>Notes and Status</th></tr>
<tr><td>

The following step is needed if own private certificate and generated SAN certificates are required and the `web cert gen_csr` command was run. For details, refer to the Web Certificate Setup Options topic in the Platform Guide.<br>
The steps below are needed to check if a CSR private key exists but no associated signed certificate is available.<br>
The steps below are needed to check if a CSR private key exists but no associated signed certificate is available.<br>
Request VOSS support to run the following command (displayed for information only):

```
if [ -d /opt/platform/apps/nginx/config/csr/ ] ;
then
  for LST in /opt/platform/apps/nginx/config/csr/*;
  do
    openssl x509 -in $LST -text -noout >/dev/null 2>&1 && SIGNED="$LST";
  done;
  echo $SIGNED;
else:
  echo "No further action required";
fi
```

If the `echo $SIGNED` command output is blank, back up the `csr/` directory with for example the following command:<br>
`mv /opt/platform/apps/nginx/config/csr/ /opt/platform/apps/nginx/config/csrbackup`

</td><td></td></tr>
</table>

### Validate System Health

**Important:**

- Before starting the upgrade, ensure that the hardware version of each of your virtual machines (VMs) is at least version 11, compatible with ESXi 6.0 and up, and that your host CPU supports AVX (Advanced Vector Extensions).

  A `check cluster` command in the Automate pre-upgrade steps checks for AVX support. To ensure that AVX support is added to the VMs, you'll need to upgrade the compatibility of the VM in vCenter.

- Follow all of the steps in the table, in the order presented.

| Description and Steps | Notes and Status |
|---|---|
| 1. Verify there are no pending Security Updates:<br>`security check` | |
| 2. Mount upgrade ISO:<br>`system mount`<br>3. Install the new version of the `cluster check` command:<br>`app install check_cluster`<br>For details, refer to the "Cluster Check" topic in the Platform Guide.<br>4. Inspect the output of the command below for warnings and errors. You can also use `cluster check verbose` to see more details.<br>`cluster check`<br>Review and resolve any warnings or errors before proceeding with the upgrade. Contact VOSS Support for assistance, if required.<br>For troubleshooting and resolutions, also refer to the *Health Checks for Cluster Installations Guide* and *Platform Guide*.<br>If there is any sign of the paths below are over 80% full, a clean-up is needed, for example to avoid risk of full logs occurring during upgrade. Clean-up steps are indicated next to the paths:<br>`/              (call support if over 80%)`<br>`/var/log       (run: log purge)`<br>`/opt/platform  (remove any unnecessary files from /media directory)`<br>`/tmp           (reboot)`<br>Verify there are no pending Security Updates.<br>**Note:** If you run `cluster status` after installing the new version of `cluster check`, any error message regarding a failed command can be ignored. This error message will not show after upgrade.<br>• **Adaptation check** - if the *GS SME Adaptation* is installed, check for duplicate instances of of `GS_SMETemplateData_DAT` and deleted any duplicates before upgrading to 24.2. | |

### Version Check

Also verify VMWare, Cloud Deployments, and Application version compatibility as indicated in the Compatibility Matrix.

| Description and Steps | Notes and Status |
|---|---|
| **Customized ``data/Settings``**<br>If `data/Settings` instances have been modified, record these or export them as JSON. The modifications can be re-applied or exported JSON instances can be merged following the upgrade. See: *Post Template Upgrade Tasks single node cluster*.<br>**Version**<br>Record the current version information. This is required for upgrade troubleshooting.<br>• Log in on the Admin Portal and record the information contained in the **About > Extended Version** | |

## 4.1.2. Maintenance Window

### Pre-Upgrade Steps single node cluster

| Description and Steps | Notes and Status |
|---|---|
| **Choose an option:**<br>• **If you're upgrading from: [21.4-PB4, 21.4-PB5]**<br>Place the system in maintenance mode to suspend any scheduled transactions. Scheduled transactions that are in progress will be allowed to complete, or otherwise, cancel data sync transactions that are in progress on the GUI. Refer to the Core Feature Guide. For details, refer to the System Maintenance Mode topic in the Platform Guide.<br>Run:<br>`cluster maintenance-mode start`<br>You can verify the maintenance mode status with:<br>`cluster maintenance-mode status`<br>• **If you're upgrading from: [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]**<br>Turn off any scheduled imports to prevent syncs triggering part way through the upgrade.<br>**Note:** Schedules can easily be activated and deactivated from the **Bulk Schedule Activation** / **Deactivation** menu available on the available on the `MVS-DataSync-Dashboard`.<br>Two options are available:<br>Individually for each job:<br>1. Log in on the Admin Portal as a high level administrator above Provider level.<br>2. Select the **Scheduling** menu to view scheduled jobs.<br>3. Click each scheduled job. On the Base tab, uncheck the **Activate** check box.<br>Mass modify:<br>1. On the Admin Portal, export scheduled syncs into a bulk load sheet.<br>2. Modify the schedule settings to de-activate scheduled syncs.<br>3. Import the sheet.<br>Schedules enabled on the CLI:<br>1. Run `schedule list` to check if any schedules exist and overlap with the maintenance window.<br>2. For overlapping schedules, disable. Run:<br>`schedule disable <job-name>`<br>Create a restore point and then restart server.<br>As part of the rollback procedure, ensure that a suitable restore point is obtained prior to the start of the activity, as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed. If you cannot restore the application from a restore point, your only recourse is to reinstall the application. When the backup is complete and you do not need the restore point for restore activities, you can remove it.<br>After the restore point has been created, restart.<br>Optional: If a backup is required in addition to the restore point, use the commands:<br>`backup add <location-name>`<br>and<br>`backup create <location-name>`<br>For details, refer to the *Platform Guide*. | |

| Description and Steps | Notes and Status |
|---|---|
| Before upgrading, check all services:<br>Make sure no services are stopped/broken. The message 'suspended waiting for mongo' is normal on a fresh node.<br>• `app status`<br>Verify the node is not in the 'recovering' state (`stateStr` is not `RECOVERING`)<br>• `database config` | |

### Upgrade single node cluster

**Note:**

- By default, the cluster upgrade is carried out in parallel on all nodes and without any backup in order to provide a fast upgrade.
- For systems *upgrading to 24.2 from 21.4.0 - 21.4-PB5*:
  - The VOSS platform maintenance mode will be started automatically when the `cluster upgrade` command is run. This prevents any new occurrences of scheduled transactions, including the 24.2 database syncs associated with `insights sync`. For details on `insights sync`, see the *Insights Analytics* topic in the Platform Guide.
  - The `cluster maintenance-mode stop` command must however be run manually after the maintenance window of the upgrade: *End of the Maintenance Window and Restoring Schedules*.

For details on the VOSS platform maintenance mode, see the *Maintenance Mode* topic in the Platform Guide.

| Description and Steps | Notes and Status |
|---|---|
| It is recommended that the upgrade steps are run in a terminal opened with the `screen` command.<br>On the primary unified node:<br>• `screen`<br>• `cluster upgrade media/<upgrade_iso_file>`<br>All unused docker images except `selfservice` and `voss_ubuntu` images will be removed from the system at this stage.<br>Note: If the system reboots, do not carry out the next manual reboot step.<br>To remove a mount directory `media/<iso_file basename>` on nodes that may have remained after for example an upgrade, run:<br>`cluster run all app cleanup`<br>Manual reboot *only if needed*:<br>• `system reboot`<br>If node messages: `<node name> failed with timeout` are displayed, these can be ignored.<br>Since all services will be stopped, this takes some time.<br>Close `screen`: **Ctrl** + `a`, then: `\`<br>Log in on the primary database node and run:<br>`cluster run database app status`<br>If the report shows `insights-voss-sync:realtime stopped` on some database nodes, request assistance from VOSS support in order to carry out the following on the primary database node (displayed for information only):<br>1. Run the command:<br>`/opt/platform/mags/insights-voss-sync-mag-script install database`<br>This should return: `Configured Postgres secrets`.<br>2. Verify that the database nodes now all have the correct mongo info:<br>`cluster run database diag config app insights-voss-sync /mongo`<br>All nodes should have the password/port/user shown as below:<br>`mongo:`<br>`    password: ********`<br>`    port: 27020`<br>`    user: insights-platform`<br>3. Restart the `insights-voss-sync:real-time` service on all database nodes:<br>`cluster run database app start insights-voss-sync:real-time` | |

**Note:** In order to carry out fewer upgrade steps, the updates of instances of some models are skipped in the cases where:

- `data/CallManager` instance does not exist as instance in `data/NetworkDeviceList`
- `data/CallManager` instance exists, but `data/NetworkDeviceList` is empty
- Call Manager AXL Generic Driver and Call Manager Control Center Services match the `data/CallManager` IP

### Post-Upgrade, Security and Health Steps single node cluster

| Description and Steps | Notes and Status |
|---|---|
| Verify the status:<br>• `cluster check`<br>• If any of the above commands show errors, check for further details to assist with troubleshooting:<br>`cluster run all diag health`<br>For a cloud deployment (MS Azure / AWS), also refer to the steps below. | |
| If upgrade is successful, the screen session can be closed by typing `exit` in the screen terminal. If errors occurred, keep the screen terminal open for troubleshooting purposes and contact VOSS support. | |
| Complete all the security updates:<br>• `security update`<br>If upgrading a cloud deployment (MS Azure / AWS), run **cluster check**. If an error shows at each node:<br>`grub-pc:  package in an undesired state`<br>then request assistance from VOSS Support in order to run the command on each node (displayed for information only):<br>`dpkg --configure -a`<br>A text user interface opens and you will be prompted:<br>– “GRUB install devices:”- Do *not* select any device. Press <Tab> to highlight <Ok> and press <Enter>.<br>– At “Continuing without installing GRUB?”, press <Yes><br>– Run `cluster check` again and verify the error does not show.<br>The docker images `selfservice` and `voss_ubuntu` will be removed from the system at this stage.<br>Note: If the system reboots, do not carry out the next manual reboot step .<br>Manual reboot *only if needed*:<br>• `system reboot` | |

### Database Schema Upgrade single node cluster

| Description and Steps | Notes and Status |
|---|---|
| It is recommended that the upgrade steps are run in a terminal opened with the `screen` command.<br>• `screen`<br>• `voss upgrade_db` | |

### Template Upgrade single node cluster

| Description and Steps | Notes and Status |
|---|---|
| It is recommended that the upgrade steps are run in a terminal opened with the `screen` command.<br>• `screen`<br>• `app template media/<VOSS Automate.template>` | |

The following message appears:

```
Running the DB-query to find the current environment's
existing solution deployment config...
```

- Python functions are deployed
- System artifacts are imported.

The template upgrade automatically detects the deployment mode, either "Enterprise" or "Provider". A message displays according to the selected deployment type. Check for one of the messages below:

```
Importing EnterpriseOverlay.json

Importing ProviderOverlay.json ...
```

The template install automatically restarts necessary applications.

| Description and Steps | Notes and Status |
|---|---|
| Review the output from the `app template` command and confirm that the upgrade message appears:<br>`Deployment summary of PREVIOUS template solution`<br>`(i.e. BEFORE upgrade):`<br>`-------------------------------------------------`<br><br>`Product: [PRODUCT]`<br>`Version: [PREVIOUS PRODUCT RELEASE]`<br>`Iteration-version: [PREVIOUS ITERATION]`<br>`Platform-version: [PREVIOUS PLATFORM VERSION]`<br>This is followed by updated product and version details:<br>`Deployment summary of UPDATED template solution`<br>`(i.e. current values after installation):`<br>`-----------------------------------------------`<br><br>`Product: [PRODUCT]`<br>`Version: [UPDATED PRODUCT RELEASE]`<br>`Iteration-version: [UPDATED ITERATION]`<br>`Platform-version: [UPDATED PLATFORM VERSION]` | |

| Description and Steps | Notes and Status |
|---|---|
| • If no errors are indicated, make a backup or restore point as per the guidelines for the infrastructure on which the VOSS Automate platform is deployed.<br>This restore point can be used if post-upgrade patches that may be required, fail. | |
| For an unsupported upgrade path, the install script stops with the message:<br>`Upgrade failed due to unsupported upgrade path.`<br>`Please log in as sysadmin`<br>`and see Transaction logs for more detail.`<br>You can restore to the backup or rollback/revert to the restore point made before the upgrade. | |
| If there are errors for another reason, the install script stops with a failure message listing the problem. Contact VOSS support. | |
| Post upgrade migrations:<br>• `voss post-upgrade-migrations`<br>Data migrations that are not critical to system operation can have significant execution time at scale. These need to be performed after the primary upgrade, allowing the migration to proceed whilst the system is in use - thereby limiting upgrade windows.<br>A transaction is queued on VOSS Automate and its progress is displayed as it executes. | |

| Description and Steps | Notes and Status |
|---|---|
| Check status and health<br>• `diag health`<br>• `app status` | |

### Post Template Upgrade Tasks single node cluster

| Description and Steps | Notes and Status |
|---|---|
| Verify the upgrade:<br>Log in on the Admin Portal and check the information contained in the **About > Version** menu. Confirm that versions have upgraded.<br>• **Release** should show `XXX`<br>• **Platform Version** should show `XXX`<br>where `XXX` corresponds with the release number of the upgrade.<br>If your web browser cannot open the user interface, clear your browser cache before trying to open the interface again. | |
| • Check themes on all roles are set correctly | |

### Log Files and Error Checks single node cluster

| Description and Steps | Notes and Status |
|---|---|
| Inspect the output of the command line interface for upgrade errors, for example `File import failed!` or `Failed to execute command`.<br>Use the `log view` command to view any log files indicated in the error messages, for example, run the command if the following message appears:<br>`For more information refer to the execution log file with 'log view platform/execute.log'`<br>For example, if it is required send all the install log files in the `install` directory to an SFTP server:<br>• `log send sftp://x.x.x.x install` | |
| Log in on the Admin Portal as system level administrator, go to **Administration Tools > Transaction** and inspect the transactions list for errors. | |

## 4.1.3. Post Maintenance Window

### End of the Maintenance Window and Restoring Schedules

| Description and Steps | Notes and Status |
|---|---|
| On the CLI:<br>Run the `cluster maintenance-mode stop` command to end the VOSS maintenance mode when upgrading to 24.2 from 21.4 or 21.4.-PBx.<br>This will allow scheduled data sync transactions to resume, including `insights sync` operations added in 24.1.<br>For details on the VOSS platform maintenance mode, see the *Maintenance Mode* topic in the Platform Guide.<br>• **If you're upgrading from: [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]**<br>Restore Schedules<br>**Note:** Schedules can easily be activated and deactivated from the **Bulk Schedule Activation / Deactivation** menu available on the available on the `MVS-DataSync-Dashboard`.<br>Re-enable scheduled imports if any were disabled prior to the upgrade.<br>Individually for each job:<br>1. Log in on the Admin Portal as a high level administrator above Provider level.<br>2. Select the **Scheduling** menu to view scheduled jobs.<br>3. Click each scheduled job. On the Base tab, check the **Activate** check box.<br>Mass modify:<br>1. Modify the exported sheet of schedules to activate scheduled syncs.<br>2. Import the sheet.<br>**Note:** Select the **Skip next execution** option if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter.<br>Schedules enabled on the CLI:<br>For disabled schedules that were overlapping the maintenance window, enable.<br>Run `schedule enable <job-name>` | |

### Licensing

| Description and Steps | Notes and Status |
|---|---|
| From release 21.4 onwards, the deployment needs to be licensed. After installation, a 7-day grace period is available to license the product. Since license processing is only scheduled every hour, if you wish to license immediately, first run `voss check-license` on the CLI.<br>1. Obtain the required license token from VOSS.<br>2. To license:<br>a. Through the GUI, follow steps indicated in Product License Management in the Core Feature Guide.<br>b. Through the CLI, follow steps indicated in Product Licensing in the Platform Guide. | |

### Mount the Insights disk

| Description and Steps | Notes and Status |
|---|---|
| *On the primary unified node*, assign the `insights-voss-sync:database` mount point to the drive added for the Insights database prior to upgrade.<br>For example, if `drives list` shows the added disk as:<br>`Unused disks:`<br>`sde`<br>then run the command below on each unified node where the drive has been added:<br>`drives add sde insights-voss-sync:database`<br>The message below can be ignored on release 24.2:<br>`WARNING: Failed to connect to lvmetad. Falling back to device scanning.`<br>Sample output:<br>`$ drives add sde insights-voss-sync:database`<br>`Configuration setting "devices/scan_lvs" unknown.`<br>`Configuration setting "devices/allow_mixed_block_sizes" unknown.`<br>`WARNING: Failed to connect to lvmetad. Falling back to device scanning.`<br>`71ad98e0-7622-49ad-9fg9-db04055e82bc`<br>`Application insights-voss-sync processes stopped.`<br>`Migrating data to new drive - this can take several minutes`<br>`Data migration complete - reassigning drive`<br>`Checking that /dev/sde1 is mounted`<br>`Checking that /dev/dm-0 is mounted`<br>`/opt/platform/apps/mongodb/dbroot`<br>`Checking that /dev/sdc1 is mounted`<br>`/backups`<br><br>`Application services:firewall processes stopped.`<br>`Reconfiguring applications...`<br>`Application insights-voss-sync processes started.`<br>With release 24.2, the initial management of dashboards on the GUI and use of VOSS Wingman is available after the first scheduled `delta-sync` of data - which is scheduled to run every 30 minutes. No manual sync is therefore required after upgrade.<br>For details, see the Insights Analytics section of the Platform Guide. | |

# Index

## A

app

- app cleanup, 13, 28, 42
- app template, 4

## C

cluster

- cluster check, 13, 28
- cluster maintenance-mode, 13, 28, 42
- cluster provision, 4
- cluster upgrade, 4, 13, 28

## D

database

- database convert_drive, 13, 28, 42

## S

screen, 4, 13, 28, 42

## V

voss

- voss db_collection_cap, 7
- voss post-upgrade-migrations, 42
- voss upgrade_db, 4

voss export

- voss export group, 4
- voss export type, 4

voss subscriber_data_export, 4