VOSS Automate
Upgrade Guide with ISO and Template

Release 24.2-PB1

February 26, 2025

Legal Information

DOCUMENT ID: 20250226055210

Contents

1 Prepare for Upgrade **2**
1.1 Before upgrading . . . 2
1.2 Upgrade and data migration . . . 4
1.3 Using the `screen` command . . . 4
1.4 VOSS Automate Hardware Specifications . . . 5

2 Upgrade (all topologies) **13**
2.1 Upgrade Automate . . . 13

Index **29**

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.

1. Prepare for Upgrade

1.1. Before upgrading

1.1.1. Dependencies

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

- `21.4.x` > `24.2`

1.1.2. 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 `cluster check` 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.

1.1.3. 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.

1.2. 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.

1.3. 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

1.4. VOSS Automate Hardware Specifications

1.4.1. 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.

1.4.2. 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	At least VMware 11, compatible with ESXi 6.0 and up	32 GB with 32 GB reservation	4 vCPU @ 2 GHz with 4000 MHz reservation	Total: 440 GB as allocated below. 370 GB partitioned: • 20 GB for OS • 50 GB for application: – 10 GB for logs – 40 GB for our apps • 50 GB for compressed backups • 250 GB for database 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	At least VMware 11, compatible with ESXi 6.0 and up	32 GB with 32 GB reservation	4 vCPU @ 2 GHz with 4000 MHz reservation	Total: 440 GB as allocated below. 370 GB partitioned: • 20 GB for OS • 50 GB for application: – 10 GB for logs – 40 GB for our apps • 50 GB for compressed backups • 250 GB for database 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	At least VMware 11, compatible with ESXi 6.0 and up	4 GB with 4 GB reservation	2 vCPU @ 2 GHz with no reservation	70 GB partitioned: • 20 GB for OS • 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	At least VMware 11, compatible with ESXi 6.0 and up	32 GB with 32 GB reservation	4 vCPU @ 2 GHz with 4000 MHz reservation	Total: 440 GB as allocated below. 370 GB partitioned: • 20 GB for OS • 50 GB for application: – 10 GB for logs – 40 GB for our apps • 50 GB for compressed backups • 250 GB for database 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	At least VMware 11, compatible with ESXi 6.0 and up	4 GB with 4 GB reservation	2 vCPU @ 2 GHz with no reservation	70 GB partitioned: • 20 GB for OS • 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.

1.4.3. 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	At least VMware 11, compatible with ESXi 6.0 and up	32 GB with 32 GB reservation	4 vCPU @ 2 GHz with 4000 MHz reservation	70 GB partitioned: • 20 GB for OS • 50 GB for application: – 10 GB for logs – 40 GB for our apps	1 Gbit/s minimum
Database	3	At least VMWare 11, compatible with ESXi 6.0 and up	32 GB with 32 GB reservation	4 vCPU @ 2 GHz with 4000 MHz reservation	Total: 440 GB as allocated below. 370 GB partitioned: • 20 GB for OS • 50 GB for compressed backups • 50 GB for application: – 10 GB for logs – 40 GB for our apps • 250 GB for database 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	At least VMware 11, compatible with ESXi 6.0 and up	4 GB with 4 GB reservation	2 vCPU @ 2 GHz with no reservation	70 GB partitioned: • 20 GB for OS • 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.

1.4.4. 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 available
   - **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

2. Upgrade (all topologies)

2.1. Upgrade Automate

2.1.1. Overview

This section provides the steps for upgrading Automate with ISO and template, for all topologies. At each step in this procedure we've added labels to indicate the relevant topologies:

- Unified node topology: Unified Node
- Modular cluster topology: Modular Cluster
- Single node cluster topology: Single Node Cluster

You can find out more about the Automate deployment topologies in the *Automate Architecture and Hardware Specification Guide*.

2.1.2. Before you start

Unified Node Modular Cluster Single Node Cluster

Review section "Prepare for Upgrade" before proceeding.

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 `cluster check` 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.

For the target version, before starting this upgrade, verify VMWare, Cloud deployments, and application version compatibility, as indicated in the Compatibility Matrix.

2.1.3. Prior to maintenance window

Prior to the maintenance window, you will need to complete the following tasks:

1. Verify the primary database node and application node
2. Download and check files
3. Check the version

Verify the primary database node and application node

Unified Node Modular Cluster

Note: This task is **optional** for a **single node cluster** topology.

---

1. Verify the primary application node, run the following command on the node:

   ```
   cluster primary role application
   ```

   Note:

   - In a **modular cluster** topology, the application and database are on separate nodes.
   - In a **unified node** topology you will need to ensure that the database and application status is primary on the same node (the node configured as "primary"). In this case (**unified node**), you'll need to run the command on each node until you find the "primary" node. For example, the database node with the highest "weight" is "primary".

   The output should be true, for example:

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

2. Verify the primary database node, run the following command on the node:

   ```
   cluster primary role database
   ```

   Note:

   - In a **modular cluster** topology, the application and database are on separate nodes.
   - In a **unified node** topology you will need to ensure that the database and application status is "primary" on the same node (the node configured as "primary"). In this case (**unified node**), you'll need to run the command on each node until you find the "primary" node. For example, the database node with the highest "weight" is "primary".

   The output should be true, for example:

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

Download and check files

Unified Node | Modular Cluster | Single Node Cluster

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

1. Go to the download location for VOSS files (where XXX is the major version in your upgrade path requirement, for example, 24.2, if you're upgrading to 24.2-PB1):

   https://voss.portalshape.com > Downloads > VOSS Automate > XXX > Upgrade

2. Download **.iso** and **.template** files.
3. Transfer the files to the **media**/ folder, using either SFTP or SCP:
   - Transfer the **.iso** file to the **media**/ folder of all nodes.
   - Transfer the **.template** file to the **media**/ folder of the primary application node.

   Transfer using SFTP:

For all nodes	`sftp platform@<node_hostname>`
	`cd media`
	`put <upgrade_iso_file>`

For primary application node	`sftp platform@<application_node_hostname>`
	`cd media`
	`put <upgrade_template_file>`

   Transfer using SCP:

For all nodes	`scp <upgrade_iso_file> platform@<node_ip_address>:~/media`
For primary application node	`scp <upgrade_template_file> platform@<application_node_ip_address>:~/media`

4. Verify that the **.iso** image and **.template** file copied: `ls -l media/`
5. Verify that the original **.sha256** checksums on the Download site match:

   On any node, run:

   `cluster run all system checksum media/<upgrade_iso_file>`

   Note: If you have multiple nodes, run this command on only one node.

   The output should be:

```
Checksum: <SHA256>
```

   On the primary application node, run: `system checksum media/<upgrade_template_file>`

   The output should be:

```
Checksum: <SHA256>
```

Version check

Unified Node | Modular Cluster | Single Node Cluster

1. If you have customized data settings (data/Settings), record these or export as JSON. Customizations can be re-applied or the exported JSON instances can be merged following the upgrade. See *Post-template upgrade*.
2. Record current version information for upgrade troubleshooting:
   a. Log in to the Admin Portal.
   b. Go to **About > Version**.
   c. Make a note of the system version information.

2.1.4. Maintenance window

In the maintenance window, you will need to complete the following tasks:

1. Perform security and health checks
2. Validate system health
3. Perform pre-upgrade steps
4. Upgrade
5. Perform post-upgrade and health check steps
6. Perform database schema upgrade
7. Perform template upgrade
8. Perform post-template upgrade steps
9. Inspect the log files and check for errors

Security and health checks

1. Unified Node | Modular Cluster | Single Node Cluster

   If upgrading from [21.4-PB4, 21.4-PB5]:

   Place the system in maintenance mode and suspend any scheduled transactions:

   a. On an application node of the system, place the system in maintenance mode:

      ```
      cluster maintenance-mode start
      ```

      Scheduled transactions that are in progress will be allowed to complete, else, cancel data sync transactions that are in progress on the GUI. Refer to the Core Feature Guide. For details, see System Maintenance Mode in the Platform Guide.

b. Verify maintenance mode status:

```
cluster maintenance-mode status
```

c. Turn off scheduled imports:

If upgrading from [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]:

Turn off any scheduled imports to prevent syncs triggering part way through the upgrade, either individually for each job, or mass modify:

Note: Schedules can easily be activated and deactivated via the Bulk Schedule Activation / Deactivation menu (available on the MVS-DataSync-Dashboard).

Individually for each job	• Log in on the Admin Portal as a high level admin (above Provider). • Select the **Scheduling** menu to view scheduled jobs. • For each scheduled job, on the **Base** tab, clear the **Activate** checkbox to disable this setting.
Mass modify	• In the Admin Portal, export scheduled syncs into a bulk load sheet. • Modify schedule settings to de-activate scheduled syncs. • Import the sheet.

d. Turn off schedules enabled on the CLI:

- Check if any schedules exist and overlap with the maintenance window: `schedule list`
- Disable overlapping schedules: `schedule disable <job-name>`

2. Unified Node Modular Cluster

Note: This step is not relevant when upgrading a **Single Node Cluster** topology.

Verify that the primary database node is the active primary node at the time of upgrade:

```
database config
```

Note: A **unified node** topology will have the primary and database on the same node.

---

3. Unified Node Modular Cluster

Note: This step is not relevant when upgrading a **Single Node Cluster** topology.

Ensure that the primary database 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
```

```
<ip address>:27020:
    priority: 70.0
    stateStr: PRIMARY
    storageEngine: WiredTiger
<ip address>:27030:
    priority: 0.0
    stateStr: ARBITER
    storageEngine: WiredTiger
<ip address>:27020:
    priority: 50.0
    stateStr: SECONDARY
    storageEngine: WiredTiger
<ip address>:27030:
    priority: 0.0
    stateStr: ARBITER
    storageEngine: WiredTiger
<ip address>:27020:
    priority: 30.0
    stateStr: SECONDARY
    storageEngine: WiredTiger
```

Validate system health

Unified Node | Modular Cluster | Single Node Cluster

1. Verify that there are no pending security updates: `security check`

   If any security updates are required, run `security update`

2. Mount upgrade ISO: `system mount`

3. Install the new version of the cluster check command: `app install check_cluster`

   For details, see **Cluster Check**.

4. Run `cluster check`.

   Inspect the output for warnings and errors. You can also use `cluster check verbose` to see 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.

   For troubleshooting and resolutions, also refer to the *Health Checks for Cluster Installations Guide* and the *Platform Guide*.

   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 during upgrade. Recommended steps to resolve are indicated at each path:

Path	Resolution
/	Contact VOSS Support if over 80%
/var/log	Run `log purge`
/opt/platform	Remove any unnecessary files from /**media** directory
/tmp	Reboot

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.
- Adaptation checks - if the **GS SME Adaptation** is installed, check for duplicate instances of of **GS_SMETemplateData_DAT** and delete any duplicates before upgrading to 24.2.

Pre-upgrade

Unified Node | Modular Cluster | Single Node Cluster

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).

   Important: All nodes must be powered off prior to creating the restore point, and must be powered back on again when the restore point is complete.

   Optionally, if a backup is also required, use the following commands on the primary database node:

   `backup add <location-name>`

   `backup create <location-name>`

   For details, see the *Platform Guide*.

2. Validate system health and check all services, nodes, and weights for the cluster:

   A. Run `cluster run application cluster list`, and ensure that all application nodes show.

   B. Run `cluster check`, then inspect the output of this command for warnings and errors. You can use the `cluster check verbose command` to see more details.

   C. Ensure that no services are stopped or broken: `app status`

   The following message is normal on fresh database nodes:

   ```
   suspended waiting for mongo ...
   ```

   D. **Important**! Check that the database weights are set before upgrading a cluster. Example output:

   ```
   <ip address>:
        weight: 80
    <ip address>:
   ```

(continues on next page)

(continued from previous page)

```
    weight: 70
<ip address>:
    weight: 60
<ip address>:
    weight: 50
```

E. Verify the primary node in the primary site and ensure no nodes are in the recovering state (**stateStr** is not "RECOVERING").

3. On the primary application node, verify that there are no pending security updates on any of the nodes:

   `cluster run all security check`

   If any security updates are required, run: `security update`

Upgrade

Unified Node | Modular Cluster | Single Node Cluster

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.

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*.

1. Verify that the ISO has been uploaded to the **media**/ directory on each node. This speeds up the upgrade time.

   On the primary database node (**modular cluster**) or primary unified node (**unified node** and **single node cluster**), run the following commands:

   `screen`

   `cluster upgrade media/<upgrade_iso_file>`

2. To remove a mount directory **media/<iso_file basename>** on nodes that may have remained after, for example, an upgrade, run:

   `cluster run all app cleanup`

3. The system should reboot automatically. If it does not, perform manual reboot:

Topology	Command
Unified Node Modular Cluster	`cluster run notme system reboot` When all other nodes have rebooted, run `system reboot` on the local node.
Single Node Cluster	`system reboot`

   If the following node messages display, these can be ignored:

```
<node name> failed with timeout
```

Since all services will be stopped, this takes some time.

4. Press **Ctrl + a**, then \ to close screen.

Post-upgrade and health check

Unified Node | Modular Cluster | Single Node Cluster

1. Check for required security updates. On the primary application node, run:

   `cluster run all security check`

2. If security updates are required on any nodes, run the following on the primary application node:

   `cluster run all security update`

   If upgrading a Cloud deployment (Microsoft Azure or AWS), run: `cluster check`

Note: Contact VOSS Support for assistance if the following message displays at each node:

```
grub-pc: package in an undesired state
```

To resolve, VOSS Support runs the following command on each node (displayed for informational purposes only):

`dpkg --configure -a`

Following this command, prompts display in the text window. VOSS Support then performs the following (displayed for informational purposes only):

- At **GRUB install devices**, do not select any device. Press **<Tab>** to highlight, then **<Ok>**, and then press **<Enter>**.
- At **Continuing without installing GRUB?**, press **<Yes>**.
- Run `cluster check` again, and verify the error no longer displays.

3. If the system does not automatically reboot and you need to reboot manually - this takes some time as all services are stopped:

   The system should reboot automatically. If it does not, perform manual reboot:

Topology	Command
Unified Node Modular Cluster	`cluster run notme system reboot` When all other nodes have rebooted, run `system reboot` on the local node.
Single Node Cluster	`system reboot`

You can ignore the following node messages:

```
<node name> failed with timeout
```

4. Log in on the primary database node, then run:

   `cluster run database app status`

   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):

   - Run `/opt/platform/mags/insights-voss-sync-mag-script install database`

     The output should be:

     ```
     Configured Postgres secrets
     ```

   - Verify that the database nodes now all have the correct mongo info:

     `cluster run database diag config app insights-voss-sync /mongo`

     All nodes should have the password/port/user shown as below:

     ```
     mongo:
       password: ********
       port: 27020
       user: insights-platform
     ```

   - Restart the *insights-voss-sync:real-time service* on all database nodes:

     `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.

   ---

5. Verify cluster status. On the primary node, run: `cluster check`
6. If there are any errors, for details that may help with troubleshooting, run the following:

   `cluster run all diag health`

7. 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`

8. If the upgrade succeeds, type **exit** in the terminal to close the screen session.

   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.

Unified Node | Modular Cluster | Single Node Cluster

1. On the primary application node, run the following:

   ```
   screen
   voss upgrade_db
   voss upgrade_db
   ```

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.

Unified Node | Modular Cluster | Single Node Cluster

1. On the primary application node, run the following commands:

   ```
   screen
   app template media/<VOSS Automate.template>
   ```

2. View the message that displays:

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

3. View progress:
   - Python functions are deployed
   - System artifacts are imported

   Note: To perform fewer upgrade steps, updates of instances of some models are skipped, 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 system message displays for the selected deployment mode, for example:

     On Enterprise deployment:

     ```
     Importing EnterpriseOverlay.json
     ```

     On Provider deployment:

     ```
     Importing ProviderOverlay.json
     ```

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

4. Run `app template`, then review the output to verify 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]
```

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.

6. On the primary application node, run the following command to verify that the *extra_functions* have the same checksum across the cluster:

Topology	Command
Unified Node Modular Cluster	`cluster run application voss get_extra_functions_version -c`
Single Node Cluster	`cluster run voss get_extra_functions`

7. For post-upgrade migrations, run the following command on a single application node of a cluster:

   `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 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.
9. On the primary database node, check cluster status and health: `cluster status`

Post-template upgrade

Unified Node | Modular Cluster | Single Node Cluster

1. Verify the upgrade:
   a. Log in on the Admin Portal, and check version details in **About > Version**.

      If your web browser can't open the user interface, clear your browser cache before trying to open the interface again.

   b. Confirm that versions are upgraded (where *XXX* is the release version).
      - Release should display XXX
      - Platform version should display XXX
2. Check that themes on all roles are set correctly.
3. For configurations using Northbound Billing Integration (NBI), check the service status of NBI, and restart if necessary.

Log files and error checks

Unified Node | Modular Cluster | Single Node Cluster

1. Inspect the output of the command line interface for upgrade errors, for example, "File import failed!" or "Failed to execute command".
2. If there are any errors referring to log files, for example:

   ```
   For more information refer to the execution log file with ``log view platform/
   ↪execute.log``
   ```

   Then run the `log view` command on the primary application node command to view any log files indicated in the error messages.

   If required, send all the install log files in the install directory to an SFTP server:

   `log send sftp://x.x.x.x install`
3. Log in on the Admin Portal as system level admin, then go to **Administration Tools > Transaction**, and inspect the transaction list for errors.

2.1.5. Post-maintenance window

In the post-maintenance part of the upgrade you will need to perform the following tasks:

1. End the maintenance window and restore schedules
2. Apply the license
3. Mount the Insights disk

End maintenance window and restore schedules

Unified Node | Modular Cluster | Single Node Cluster

1. If you're upgrading from 21.4 or 21.4.-PBx to 24.2, then, on the CLI, run the following command to end the VOSS maintenance window:

   ```
   cluster maintenance-mode stop
   ```

   Scheduled data sync transactions can now resume, including insights sync operations added in 24.1. For details, see *Maintenance Mode* in the *Platform Guide*.

2. Restore schedules.

   Schedules can easily be activated and deactivated from the Bulk Schedule Activation / Deactivation menu available on the MVS-DataSync-Dashboard.

   If upgrading from [21.4, 21.4-PB1, 21.4-PB2, 21.4-PB3]:

   a. Re-enable scheduled imports if any were disabled prior to the upgrade - either individually for each job, or mass modify:

Individually for each job	• Log in on the Admin Portal as a high level admin (above Provider). • Select the **Scheduling** menu to view scheduled jobs. • Click each scheduled job, and on the **Base** tab, select the **Activate** checkbox.
Mass modify	• Modify the exported sheet of schedules to activate scheduled syncs. • Import the sheet. If you don't want to execute schedules overlapping the maintenance window but only execute afterwards, select **Skip next execution**.

   b. For schedules enabled on the CLI, enable any disabled schedules that were overlapping the maintenance window:

   ```
   schedule enable <job-name>
   ```

Licensing

Unified Node | Modular Cluster | Single Node Cluster

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.

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

Mount the Insights disk

Unified Node | Modular Cluster | Single Node Cluster

1. On each database/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 following command on each database/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.
   ```

The following message can be ignored on release 24.1:

```
Warning: Failed to connect to lvmetad. Falling back to device scanning.
```

Note: On Automate 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 (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*.

Index

A

app
    app cleanup, 13
    app template, 4

C

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

D

database
    database convert_drive, 13

S

screen, 4, 13

V

voss
    voss db_collection_cap, 7
    voss upgrade_db, 4
voss export
    voss export group, 4
    voss export type, 4
voss subscriber_data_export, 4