VOSS Automate

Method of Procedure (MOP) for 21.4 Patch Bundle 4 Installation

Release 21.4-PB4

Mar 26, 2024

Contents

Dependencies

- Release 21.4, or;
- Release 21.4 Patch Bundle 1
- Release 21.4 Patch Bundle 2
- Release 21.4 Patch Bundle 3

The supported upgrade paths for this Patch Bundle Upgrade:

- `21.4` > `21.4-PB4`
- `21.4-PB1` > `21.4-PB4`
- `21.4-PB2` > `21.4-PB4`
- `21.4-PB3` > `21.4-PB4`

Patch Overview

- **Patch Name**: `21.4.PB4-Delta-Bundle-patch.script`
- **Features Included**: See release notes for detail.
- **SHA256 Checksum**: `fb34380ff59560308ad946daa38d397af1140d42b8e85296170512e59baee71e`

Important Information:

- We recommend taking snapshots of all nodes that are part of the cluster before applying the patch - to be used for rollback if needed. See *Rollback* in this document.
- Adaptations: We recommend verifying the compatibility of any installed adaptations with this patch bundle in a lab before installing in production.

  Some adaptations might need to be re-installed post patch bundle installation.
- If you have a Microsoft-only environment and an existing number inventory, a rebuild of the number inventory may be needed.
- If you have a Webex Calling environment and an existing number inventory, a rebuild of the number inventory may be needed.

  Contact VOSS to verify and assist in carrying out this step.

- It is recommended that commands in installation steps are run in a terminal opened with the **screen** command.
- Ensure that you perform any mandatory post-upgrade patch installs (if required) for all deployment types.

Download Location

The 21.4-PB4 Patch is available here:

- Server Name: https://voss.portalshape.com
- Path: **Downloads > VOSS Automate > 21.4 > Patches**
- Patch Directory: **Patch Bundle 4**
- Patch File: `21.4-PB4-Delta-Bundle-patch.script`

The Post-upgrade Patch for Single Sign-On Environments is available here:

- Server Name: https://voss.portalshape.com
- Path: **Downloads > VOSS Automate > 21.4 > Patches > Patch Bundle 4**
- Patch Directory: **EKB-18459-21.4-PB4_patch**
- Patch File: `EKB-18459-21.4-PB4_patch.script`

The MOP is available at https://documentation.voss-solutions.com/release_21.4/html/MOP-21.4-PB4-Delta-Bundle-patch.pdf

Install Procedure for a Unified Node Topology

5.1 Download Patch Script and Check

Note: It is recommended that the file download is done prior to the maintenance window.

Download the following file

- `21.4-PB4-Delta-Bundle-patch.script`

to the `media` folder on the primary *unified* node.

5.2 Verify SHA256 checksum

To verify SHA256 checksum for the patch, run the following command on the node the script was downloaded to:

- Command : `system checksum media/21.4-PB4-Delta-Bundle-patch.script`
- Expected: `fb34380ff59560308ad946daa38d397af1140d42b8e85296170512e59baee71e`

5.3 Pre-Installation, Version Check

To check the version pre-install:

1. Log in to the Admin Portal GUI.
2. Verify the information contained in the menu **About > Version > Release**.

   The release version should be either 21.4.0, or 21.4.1, or 21.4.2, or 21.4.3

5.4 Pre-Installation, Security and Health Steps

1. Turn off any scheduled imports to prevent syncs triggering part way through the upgrade.

   Note: Schedules can easily be activated and deactivated from the **Bulk Schedule Activation / Deactivation** menu which provides the **Choose Action** options: **Catalog and Deactivate Schedules** and **Activate Deactivated Catalog**. This menu is by default available on the `MVS-DataSync-LP` landing page which is a part of the set of enhanced menu layouts for Multi-Vendors - refer to the relevant topic in the Core Feature Guide.

   Two options are available:

   Individually for each job:

   a. Log in on the Admin Portal as a high level administrator above Provider level.

   b. Select the **Scheduling** menu to view scheduled jobs.

   c. Click each scheduled job. On the Base tab, uncheck the **Activate** check box.

   Mass modify:

   a. On the Admin Portal, export scheduled syncs into a bulk load sheet.

   b. Modify the schedule settings to de-activate scheduled syncs.

   c. Import the sheet.

   Schedules enabled on the CLI:

   a. Run **schedule list** to check if any schedules exist and overlap with the maintenance window.

   b. For overlapping schedules, disable. Run **schedule disable <job-name>**.

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

   On the Primary Unified Node, run:

   ```
   database config
   ```

   This is to ensure that the node on which the installation will be initiated, has the:

   a. `stateStr` parameter set to **PRIMARY**

   b. *highest* `priority` **number** (highest priority number could vary depending on cluster layout).

   Example output

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

3. Validate the system health.

   On the primary unified node, run:

   `cluster status`

4. Verify network connectivity, disk status, NTP and that there are no pending Security Updates.

   On the primary unified node, run:

   `cluster check`

   `cluster run all diag disk`

   If there is any sign of the paths below are over 80% full, a clean-up is needed to avoid risk of for example full logs occurring during upgrade. Clean-up steps are indicated next to the paths:

```
/              (call support if over 80%)
/var/log       (run: log purge)
/opt/platform  (remove any unnecessary files from /media directory)
/tmp           (reboot)
```

   On the primary unified node, run:

   `cluster run all security check`

   If there are pending Security Updates, then:

   On the primary unified node, run:

   `cluster run all security update`

   Then reboot all nodes:

   `cluster run notme system reboot`

   (If node messages: `<node name> failed with timeout` are displayed, these can be ignored.)

   `system reboot`

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

5. Shutdown servers and take snapshots from VMWare or Azure VHD, as applicable.

   On the primary unified node, run:

   `cluster run notme system shutdown`

   Then after 1 minute: run:

   `system shutdown`

5.5 Patch Installation

On the primary unified node, run:

```
app install media/21.4-PB4-Delta-Bundle-patch.script
```

Note: Before the patch installation starts, the user is prompted to:

- Continue with the installation.

  Append the `--force` parameter to remove this prompt.
- Delete or keep the patch script in the `media` directory after installation.

  Append the `delete-on-success` parameter with a `yes|no` value to the command to remove this prompt.

To remove all prompts, use the command and parameters:

```
app install media/21.4-PB4-Delta-Bundle-patch.script delete-on-success yes --force
```

5.6 Post-Upgrade, Security and Health Steps

1. On the primary node, verify the cluster status:
   - `cluster status`
2. On each node verify security updates, network connectivity, disk status and NTP.
   - `cluster check`
3. If there are pending Security Updates, then run **security update** on all nodes. On the primary node, run:
   - `cluster run all security update`
4. Reboot all nodes:
   - `cluster run notme system reboot`

   (If node messages: `<node name> failed with timeout` are displayed, these can be ignored.)
   - `system reboot`

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

   Note: Schedules can easily be activated and deactivated from the **Bulk Schedule Activation / Deactivation** menu which provides the **Choose Action** options: **Catalog and Deactivate Schedules** and **Activate Deactivated Catalog**. This menu is by default available on the `MVS-DataSync-LP` landing page which is a part of the set of enhanced menu layouts for Multi-Vendors - refer to the relevant topic in the Core Feature Guide.

   Re-enable scheduled imports if any were disabled prior to the upgrade. Two options are available:

   Individually for each job:

   1. Log in to the Admin Portal as a high level administrator, above Provider level.
   2. Select the **Scheduling** menu to view scheduled jobs.

3. Click each scheduled job. On the Base tab, check the **Activate** check box.

Mass modify:

1. Modify the exported sheet of schedules to activate scheduled syncs.
2. Import the bulk load sheet.

Note: Select the **Skip next execution** option if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter.

Schedules enabled on the CLI:

1. For disabled schedules that were overlapping the maintenance window, enable.

   Run **schedule enable <job-name>**.

Install Procedure for a Modular Cluster Topology

6.1 Download Patch Script and Check

Note: It is recommended that the file download is done prior to the maintenance window.

Download the following file

- `21.4-PB4-Delta-Bundle-patch.script`

to the `media` folder on primary *application* node.

To check for this node:

1. Log in on a node in your modular cluster.
2. To find the *primary application node* in the cluster:

   ```
   $ cluster run all cluster primary role application
   ```

   Record the node entry where `is_primary: true`, for example:

   ```
   ---------- VOSS-UN-1, ip=192.168.100.3, role=webproxy,application, loc=cpt

      is_primary: true
   ```

6.2 Verify SHA256 checksum

To verify SHA256 checksum for the patch, run the following command on the node the script was downloaded to:

- Command : `system checksum media/21.4-PB4-Delta-Bundle-patch.script`
- Expected: `fb34380ff59560308ad946daa38d397af1140d42b8e85296170512e59baee71e`

6.3 Pre-Installation, Version Check

To verify the version pre-install:

1. Log in to the Admin Portal GUI.
2. Check the information contained in the menu **About > Version > Release**.

   The release version should be either 21.4.0, or 21.4.1, or 21.4.2, or 21.4.3

6.4 Pre-Installation, Security and Health Steps

1. Turn off any scheduled imports to prevent syncs triggering part way through the upgrade.

   Note: Schedules can easily be activated and deactivated from the **Bulk Schedule Activation** / **Deactivation** menu which provides the **Choose Action** options: **Catalog and Deactivate Schedules** and **Activate Deactivated Catalog**. This menu is by default available on the `MVS-DataSync-LP` landing page which is a part of the set of enhanced menu layouts for Multi-Vendors - refer to the relevant topic in the Core Feature Guide.

   Two options are available:

   Individually for each job:

   a. Log in on the Admin Portal as a high level administrator above Provider level.

   b. Select the **Scheduling** menu to view scheduled jobs.

   c. Click each scheduled job. On the Base tab, uncheck the **Activate** check box.

   Mass modify:

   a. On the Admin Portal, export scheduled syncs into a bulk load sheet.

   b. Modify the schedule settings to de-activate scheduled syncs.

   c. Import the sheet.

   Schedules enabled on the CLI:

   a. Run **schedule list** to check if any schedules exist and overlap with the maintenance window.

   b. For overlapping schedules, disable. Run **schedule disable <job-name>**.

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

   Have the IP address available of the node determined to be the primary database node. To find the *primary database node* in the cluster:

```
$ cluster run all cluster primary role database
```

Record the node entry IP where `is_primary: true`, for example:

```
---------- VOSS-UN-2, ip=192.168.100.4, role=database, loc=cpt


    is_primary: true
```

This IP address will be used in command parameters during upgrade.

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

On the primary application node, run:

cluster run <primary db IP> database config

From the output, ensure that the primary database node `stateStr` parameter is set to **PRIMARY** and it has the *highest* `priority:<number>` (highest priority number could vary depending on cluster layout).

Example output

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

3. Validate the system health.

   On the primary application node, run:

   `cluster status`

4. Verify network connectivity, disk status, NTP and that there are no pending Security Updates.

   On the primary application node, run:

   `cluster check`

   `cluster run all diag disk`

   If there is any sign of the paths below are over 80% full, a clean-up is needed to avoid risk of for example full logs occurring during upgrade. Clean-up steps are indicated next to the paths:

```
/              (call support if over 80%)
/var/log       (run: log purge)
/opt/platform  (remove any unnecessary files from /media directory)
/tmp           (reboot)
```

   On the primary application node, run:

   `cluster run all security check`

   If there are pending security updates, then:

   On the primary application node, run:

   `cluster run all security update`

   Then reboot all nodes:

   `cluster run notme system reboot`

(If node messages: `<node name> failed with timeout` are displayed, these can be ignored.)

```
system reboot
```

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

5. Shutdown servers and take snapshots from VMWare or Azure VHD, as applicable.

   On the primary application node, run:

   ```
   cluster run notme system shutdown
   ```

   Then after 1 minute: run:

   ```
   system shutdown
   ```

6.5 Patch Installation

On the primary application node, run:

```
app install media/21.4-PB4-Delta-Bundle-patch.script
```

Note: Before the patch installation starts, the user is prompted to:

- Continue with the installation.

  Append the `--force` parameter to remove this prompt.

- Delete or keep the patch script in the `media` directory after installation.

  Append the `delete-on-success` parameter with a `yes|no` value to the command to remove this prompt.

To remove all prompts, use the command and parameters:

```
app install media/21.4-PB4-Delta-Bundle-patch.script delete-on-success yes --force
```

6.6 Post-Upgrade, Security and Health Steps

1. On the primary application node, verify the cluster status:
   - `cluster status`
2. On each node verify Security Updates, network connectivity, disk status and NTP.
   - `cluster check`
3. If there are pending Security Updates, then run **security update** on all nodes. On the primary application node, run:
   - `cluster run all security update`
4. Reboot all nodes:
   - `cluster run notme system reboot`

   (If node messages: `<node name> failed with timeout` are displayed, these can be ignored.)
   - `system reboot`

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

5. Restore Schedules

Note: Schedules can easily be activated and deactivated from the **Bulk Schedule Activation** / **Deactivation** menu which provides the **Choose Action** options: **Catalog and Deactivate Schedules** and **Activate Deactivated Catalog**. This menu is by default available on the `MVS-DataSync-LP` landing page which is a part of the set of enhanced menu layouts for Multi-Vendors - refer to the relevant topic in the Core Feature Guide.

Re-enable scheduled imports if any were disabled prior to the upgrade. Two options are available:

Individually for each job:

1. Log in on the Admin Portal as a high level administrator above Provider level.
2. Select the **Scheduling** menu to view scheduled jobs.
3. Click each scheduled job. On the Base tab, check the **Activate** check box.

Mass modify:

1. Modify the exported sheet of schedules to activate scheduled syncs.
2. Import the bulk load sheet.

Note: Select the **Skip next execution** option if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter.

Schedules enabled on the CLI:

1. For disabled schedules that were overlapping the maintenance window, enable.

   Run **schedule enable <job-name>**.

Install Procedure for a Single Node Cluster Environment

7.1 Download Patch Script and Check

Note: It is recommended that the file download is done prior to the maintenance window.

Download the following file

- `21.4-PB4-Delta-Bundle-patch.script`

to the `media` folder on the single node.

7.2 Verify SHA256 checksum

To verify SHA256 checksum for the patch, run the following command on the node the script was downloaded to:

- Command : `system checksum media/21.4-PB4-Delta-Bundle-patch.script`
- Expected: `fb34380ff59560308ad946daa38d397af1140d42b8e85296170512e59baee71e`

7.3 Pre-Installation, Version Check

To check the version pre-install:

1. Log in to the Admin Portal GUI.
2. Check the information contained in the menu **About > Version > Release**.

   The release version should be either 21.4.0, or 21.4.1, or 21.4.2, or 21.4.3

7.4 Pre-Installation, Security and Health Steps

1. Turn off any scheduled imports to prevent syncs triggering part way through the upgrade.

   Note: Schedules can easily be activated and deactivated from the **Bulk Schedule Activation / Deactivation** menu which provides the **Choose Action** options: **Catalog and Deactivate Schedules** and **Activate Deactivated Catalog**. This menu is by default available on the `MVS-DataSync-LP` landing page which is a part of the set of enhanced menu layouts for Multi-Vendors - refer to the relevant topic in the Core Feature Guide.

   Two options are available:

   Individually for each job:

   a. Log in on the Admin Portal as a high level administrator above Provider level.

   b. Select the **Scheduling** menu to view scheduled jobs.

   c. Click each scheduled job. On the Base tab, uncheck the **Activate** check box.

   Mass modify:

   a. On the Admin Portal, export scheduled syncs into a bulk load sheet.

   b. Modify the schedule settings to de-activate scheduled syncs.

   c. Import the sheet.

   Schedules enabled on the CLI:

   a. Run **schedule list** to check if any schedules exist and overlap with the maintenance window.

   b. For overlapping schedules, disable. Run **schedule disable <job-name>**.

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

   On the single node, run:

   ```
   database config
   ```

This is to ensure that the node on which the installation will be initiated, has the:

a. `stateStr` parameter set to **PRIMARY**

b. *highest* `priority` **number** (highest priority number could vary depending on cluster layout).

Example output

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

3. Validate the system health.

   On the single node, run:

   ```
   app status
   ```

4. Verify network connectivity, disk status, NTP and that there are no pending Security Updates.

   On the single node, run:

   ```
   diag disk
   ```

   If there is any sign of the paths below are over 80% full, a clean-up is needed to avoid risk of for example full logs occurring during upgrade. Clean-up steps are indicated next to the paths:

   ```
   /              (call support if over 80%)
   /var/log       (run: log purge)
   /opt/platform  (remove any unnecessary files from /media directory)
   /tmp           (reboot)
   ```

   On the single node, run:

   ```
   security check
   ```

   If there are pending Security Updates, then run:

   ```
   security update
   ```

   Then reboot:

   ```
   system reboot
   ```

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

5. Shutdown servers and take snapshots from VMWare or Azure VHD, as applicable.

   Run:

   ```
   system shutdown
   ```

7.5 Patch Installation

On the single node, run:

```
app install media/21.4-PB4-Delta-Bundle-patch.script
```

Note: Before the patch installation starts, the user is prompted to:

- Continue with the installation.

  Append the `--force` parameter to remove this prompt.
- Delete or keep the patch script in the `media` directory after installation.

  Append the `delete-on-success` parameter with a `yes|no` value to the command to remove this prompt.

To remove all prompts, use the command and parameters:

```
app install media/21.4-PB4-Delta-Bundle-patch.script delete-on-success yes --force
```

7.6 Post-Upgrade, Security and Health Steps

Verify Security Updates, network connectivity, disk status and NTP.

On the single node, run:

- `app status`
- `diag disk`
- `security check`

If there are pending Security Updates, then run **security update**.

On the single node, run:

- `security update`

Reboot.

On the single node, run:

- `system reboot`

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

Restore Schedules

Note: Schedules can easily be activated and deactivated from the **Bulk Schedule Activation** / **Deactivation** menu which provides the **Choose Action** options: **Catalog and Deactivate Schedules** and **Activate Deactivated Catalog**. This menu is by default available on the `MVS-DataSync-LP` landing page which is a part of the set of enhanced menu layouts for Multi-Vendors - refer to the relevant topic in the Core Feature Guide.

Re-enable scheduled imports if any were disabled prior to the upgrade. Two options are available:

Individually for each job:

1. Log in on the Admin Portal as a high level administrator above Provider level.

2. Select the **Scheduling** menu to view scheduled jobs.
3. Click each scheduled job. On the Base tab, check the **Activate** check box.

Mass modify:

1. Modify the exported sheet of schedules to activate scheduled syncs.
2. Import the bulk load sheet.

Note: Select the **Skip next execution** option if you do not wish to execute schedules overlapping the maintenance window, but only execute thereafter.

Schedules enabled on the CLI:

1. For disabled schedules that were overlapping the maintenance window, enable.

   Run **schedule enable <job-name>**.

Post-Checks

Generic System Tests:

- Ensure all services are running on *all* nodes using `app status`.
- Log in to Administration Portal, go to **About > Version > Patches** and ensure that '21.4 Delta Bundle 4' is displayed.
- Log in to the Administration Portal of all the nodes using an administrator account.
- Log in to the Self-service Portal of all the nodes using a Self-service account.
- Log in to the Business Admin Portal on all nodes using an administrator account with a Role configured for access to the Business Admin Portal and verify functionality. (For Role Configuration, please refer to the Business Admin Portal Quickstart Guide).

Post-upgrade Patch Install for Single Sign-On Environments

Important: For environments that make use of Single Sign-On, the following patch must be installed after upgrading to Automate 21.4-PB4: `EKB-18459-21.4-PB4_patch.script`

Failure to install the patch after upgrading will result in a blank screen shown to users who access the Admin Portal SSO login URL, once authenticated.

Post-upgrade Steps for Webex Environments

Important:

1. Run a Webex sync of Licenses and Users

   Automate 21.4-PB4 includes changes to certain license names introduced by Webex in November 2024. If this sync was already performed on Automate 21.4-PB3, there is no need to perform the sync again after upgrading to Automate 21.4-PB4.

2. *For Webex Calling environments*:

   If you have a Webex Calling environment, and specifically, an inventory containing numbers in the non-"\+" format, an inventory rebuild may be required. Contact VOSS to verify and assist in carrying out this step.

Post-upgrade Steps for Microsoft Environments

Note:

- Upon upgrade to release 21.4-PB3 or above, the Microsoft Teams Windows PowerShell Proxy module should be updated to version 5.6.0. Refer to the *Set up PowerShell Proxy* topic in the Core Feature Guide for details.
- Upon upgrade to release 21.4-PB3 or above, the Microsoft Exchange Online Management module should be updated to version 3.2.0. Refer to the *Set up Exchange Online* topic in the Core Feature Guide for details.
- Upon upgrade to release 21.4-PB2 or above, attributes of `device/msteamsonline/CsOnlineUser` and `device/msgraph/MsolUser` have been added to the default Global Settings *allowlist* for Data sync, so that *only* the attributes in this list are synced. The denylists for these models have been removed.

  After upgrading to this release, ensure the lists for these models correspond with the defaults. Refer to the *Data Sync Allow list and Deny list* topic in the Advanced Configuration Guide.
- Upon upgrade to release 21.4-PB1 or above, communication between VOSS Automate and the Windows PowerShell Proxy will be encrypted by default using HTTPS, as recommended by Microsoft. The port used for secure communication is TCP 5986 instead of TCP 5985 which is used for insecure HTTP . To revert back to using insecure HTTP communication post upgrade, a new driver parameter: `winrm_transport` can be manually added to the `data/MSTeamsOnline` instance with a value of `plaintext`. Reverting back to insecure communication is only recommended as a temporary measure while the PowerShell Proxy is being configured for secure communication.
- Refer to the Best Practices Guide for important changes related to Quick Import setting on MS Data syncs and the section on "Limiting 'Update User' Workflows for MS Data Syncs".
- If the below full sync was done after a previous 21.4.X upgrade, then it is NOT needed again after upgrading to 21.4 PB1 and later versions. (These steps do NOT have to be carried out in a maintenance window)

1. Do a full MS Teams sync.

This is needed to pull in the data from Teams for the updates drivers and schemas due to the PowerShell 4/5 changes. This applies specifically to changes on CSOnlineUser as well as new policies, emergency, etc.

If you have custom MTLs or syncs, review these for inclusion of new elements supporting in this release. For details on new elements, refer to the *Upgrade Notes for VOSS Automate 21.4* and *Upgrade Notes for VOSS Automate 21.4 Patch Bundle 1*.

Alternatively, use no MTL for a full sync.

Important: This sync should be run on *all* tenants in the system.

---

2. *For Microsoft-only environments*:

   If you have a Microsoft-only environment and in particular an inventory containing numbers in the non-"\+" format, an inventory rebuild may be needed. Contact VOSS to verify and assist in carrying out this step.

Rollback

A VMWare or Azure VHD snapshot of Automate instance is taken under the maintenance window, just before the upgrade activities start. If rollback is needed during the same change window as the upgrade, use the VMware snapshot to revert Automate to its original state and bring the services back.