VOSS Automate

Method of Procedure (MOP) for 24.1-PB2 Installation

Release 24.1-PB2

Oct 04, 2024

Contents

Dependencies

- Release 24.1

  To upgrade to release 24.1, refer to the Release 24.1 Upgrade Guide with ISO and Template

  If you are upgrading from release 24.1 on either AWS or the MS Azure cloud platform, then install `EKB-21407-24.1.0_patch.script` first:

  - **Server Name**: https://voss.portalshape.com
  - **Path**: **Downloads > VOSS Automate > 24.1 > Patches**
  - **Patch Directory**: EKB-21407-24.1.0_patch
  - **Patch File**: EKB-21407-24.1.0_patch.script

The supported upgrade paths for this Patch Bundle Upgrade:

- `24.1` > `24.1-PB2`
- `24.1-PB1` > `24.1-PB2`

Patch Overview

- **Patch Name**: `24.1.PB2-Delta-Bundle-patch.script`
- **SHA256 Checksum**: The value in `24.1-PB2-Delta-Bundle-patch.script.sha` available in the download location.
- **Features Included**: See release notes for detail.

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.
- Maintenance mode: ensure that you place the system in maintenance mode prior to upgrading and end the maintenance mode when done. The **cluster maintenance-mode** command is indicated at the relevant steps below. For details on this command, refer to the System Maintenance Mode topic in the Platform Guide.
- **EKB-21316: Subscriber from profile filtering with hierarchy limit, like Quick Add Groups.**: Ensure that any subscriber profiles in use have been cloned to the required hierarchy level after upgrading to release 24.1-PB2.

  For details on this command, refer to the System Maintenance Mode topic in the Platform Guide.

Download Location

The 24.1-PB2 Patch is available here:

- Server Name: https://voss.portalshape.com
- Path: **Downloads > VOSS Automate > 24.1**
- Folder: **24.1-PB2**
- Patch File: `24.1-PB2-Delta-Bundle-patch.script`
- SHA file: `24.1-PB2-Delta-Bundle-patch.script.sha`

The MOP is available at https://documentation.voss-solutions.com/release_24.1-PB2/html/MOP-24.1-PB2-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

- `24.1-PB2-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/24.1-PB2-Delta-Bundle-patch.script`
- Expected: The value in `24.1-PB2-Delta-Bundle-patch.script.sha` available in the download location.

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 24.1.x

5.4 Pre-Installation, Security and Health Steps

1. Place the system in maintenance mode to suspend any scheduled transactions. Scheduled transactions that are in progress, will be allowed to complete.

   For details on this command, refer to the System Maintenance Mode topic in the Platform Guide.

   On an application node of the system, run:

   ```
   cluster maintenance-mode start
   ```

   You can verify the maintenance mode status with:

   ```
   cluster maintenance-mode status
   ```

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`

   Monitor the power state of the nodes in VSphere until they are powered off, then press `Ctrl-c` and run:

   `system shutdown`

5.5 Patch Installation

On the primary unified node, run:

- `screen`
- `app install media/24.1-PB2-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/24.1-PB2-Delta-Bundle-patch.script delete-on-success yes --force
```

- Close **screen**: `Ctrl-a \`

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, reboot, 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. End the system maintenance mode.

   On an application node of the system, run:

   ```
   cluster maintenance-mode stop
   ```

   You can verify the maintenance mode status with:

   ```
   cluster maintenance-mode status
   ```

   For details on this command, refer to the System Maintenance Mode topic in the Platform Guide.

5.7 FIPS

If FIPS is enabled, FIPS proxy configuration has been included in this release. To apply this package, please run the command *security update* on each FIPS enabled node in the cluster after the upgrade has been completed. No reboot is required.

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

- `24.1-PB2-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 application 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/24.1-PB2-Delta-Bundle-patch.script`
- Expected: The value in `24.1-PB2-Delta-Bundle-patch.script.sha` available in the download location.

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 24.1

6.4 Pre-Installation, Security and Health Steps

1. Place the system in maintenance mode to suspend any scheduled transactions. Scheduled transactions that are in progress, will be allowed to complete.

   For details on this command, refer to the System Maintenance Mode topic in the Platform Guide.

   On an application node of the system, run:

   `cluster maintenance-mode start`

   You can verify the maintenance mode status with:

   `cluster maintenance-mode status`

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 database 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

   Upgrade 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:

- `screen`
- `app install media/24.1-PB2-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/24.1-PB2-Delta-Bundle-patch.script delete-on-success yes --force`

- Close **screen**: `Ctrl-a \`

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, reboot, 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. End the system maintenance mode. On an application node of the system, run:

   `cluster maintenance-mode stop`

   You can verify the maintenance mode status with:

   `cluster maintenance-mode status`

   For details on this command, refer to the System Maintenance Mode topic in the Platform Guide.

6.7 FIPS

If FIPS is enabled, FIPS proxy configuration has been included in this release. To apply this package, please run the command *security update* on each FIPS enabled node in the cluster after the upgrade has been completed. No reboot is required.

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

- `24.1-PB2-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/24.1-PB2-Delta-Bundle-patch.script`
- Expected: The value in `24.1-PB2-Delta-Bundle-patch.script.sha` available in the download location.

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 24.1

7.4 Pre-Installation, Security and Health Steps

1. Place the system in maintenance mode to suspend any scheduled transactions. Scheduled transactions that are in progress, will be allowed to complete.

   For details on this command, refer to the System Maintenance Mode topic in the Platform Guide.

   On an application node of the system, run:

   ```
   cluster maintenance-mode start
   ```

   You can verify the maintenance mode status with:

   ```
   cluster maintenance-mode status
   ```

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:

- `screen`
- `app install media/24.1-PB2-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/24.1-PB2-Delta-Bundle-patch.script delete-on-success yes --force
```

- Close **screen**: `Ctrl-a \`

7.6 Post-Upgrade, Security and Health Steps

Verify Security Updates, reboot, 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.

- End the system maintenance mode. On the application node of the system, run:

  `cluster maintenance-mode stop`

  You can verify the maintenance mode status with:

  `cluster maintenance-mode status`

  For details on this command, refer to the System Maintenance Mode topic in the Platform Guide.

7.7 FIPS

If FIPS is enabled, FIPS proxy configuration has been included in this release. To apply this package, please run the command *security update* on each FIPS enabled node in the cluster after the upgrade has been completed. No reboot is required.

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 '24.1 Delta Bundle 2' 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.

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.