# VOSS Automate

# Method of Procedure (MOP) for 21.3 Patch Bundle 1 Installation

Release 21.3-PB1

Sep 14, 2022



## Contents

# Dependencies

- Release 21.3

# Patch Overview

- **Patch Name**: `21.3.PB1-Delta-Bundle-patch.script`
- **Features Included**: See release notes for detail.
- **SHA256 Checksum**: `41f9444a270137c2b4e12156745cff425c03e65ef2f57e23078c89e0fa616d26`

# Important Information: PowerShell Proxy Teams Module Update

### To upgrade any PowerShell proxies that have already been deployed, perform these steps:

Starting with VOSS Automate version 21.3-PB1, the requirement is MS Teams PowerShell module v4.3.0. If you are upgrading existing PowerShell proxy servers, perform the following steps (on each PowerShell proxy server) to use the supported version of the MS Teams module (v4.3.0).

1. Exit any existing PowerShell and PowerShell ISE windows.
2. From an elevated (run as Administrator) PowerShell window:

```
Stop-Service WinRM
Uninstall-Module MicrosoftTeams
Install-Module MicrosoftTeams -RequiredVersion 4.3.0 -AllowClobber
Start-Service WinRM
```

3. Verify

```
Get-Module -ListAvailable -Name MicrosoftTeams
```

   The output should show version 4.3.0

```
$cred = Get-Credential
```

   Enter MS Teams tenant admin credentials in the pop-up.

```
Connect-MicrosoftTeams -Credential $cred
Get-CsOnlineUser -ResultSize 1
```

   The output should display the details for one random user.

**To install MS Teams PowerShell module on a new PowerShell proxy, perform this step:**

1. From an elevated PowerShell session issue the following command:

```
Install-Module MicrosoftTeams -RequiredVersion 4.3.0
```

# Download Location

The Patch and the MOP are available here:

- Server Name: https://voss.portalshape.com
- Path: **Downloads > VOSS Automate > 21.3 > Patches**
- Patch Directory: **Patch Bundle 1**
- Patch File: `21.3-PB1-Delta-Bundle-patch.script`
- MOP File (this file): `MOP-21.3-PB1-Delta-Bundle-patch.pdf`

---

**Important:**

- We recommend taking snapshots of all nodes that are part of the cluster before applying the patch - to be used for rollback if needed.
- About 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 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.

---

# 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

- `21.3-PB1-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/21.3-PB1-Delta-Bundle-patch.script`
- Expected: `41f9444a270137c2b4e12156745cff425c03e65ef2f57e23078c89e0fa616d26`

## 5.3 Pre-Installation, Version Check

The release version should be 21.3:

- Log in on the GUI and check the information contained in the menu **About > Version > Release**. The release version should be 21.3

## 5.4 Pre-Installation, Security and Health Steps

1. 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
   ```

2. Validate the system health.

   On the primary unified node, run:

   `cluster status`

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

   On the primary unified node, run:

   `cluster check`

   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)
   ```

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.

4. Shutdown servers and take snapshots from VMWare.

## 5.5 Patch Installation

On the primary unified node, run:

`app install media/21.3-PB1-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/21.3-PB1-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. On the primary node, run:
    - `voss migrate_summary_attributes data/InternalNumberInventory`

# 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

- `21.3-PB1-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/21.3-PB1-Delta-Bundle-patch.script`
- Expected: `41f9444a270137c2b4e12156745cff425c03e65ef2f57e23078c89e0fa616d26`

## 6.3 Pre-Installation, Version Check

The release version should be 21.3:

- Log in on the GUI and check the information contained in the menu **About > Version > Release**. The release version should be 21.3

## 6.4 Pre-Installation, Security and Health Steps

1. 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
   ```

2. Validate the system health.

   On the primary application node, run:

   ```
   cluster run all cluster status
   ```

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

   On the primary application node, run:

   ```
       cluster run all security check
   ```

   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)
   ```

   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.

4. Shutdown servers and take snapshots from VMWare.

## 6.5 Patch Installation

On the primary application node, run:

```
app install media/21.3-PB1-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/21.3-PB1-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. On the primary application node, run:

- `voss migrate_summary_attributes data/InternalNumberInventory`

# 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

- `21.3-PB1-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/21.3-PB1-Delta-Bundle-patch.script`
- Expected: `41f9444a270137c2b4e12156745cff425c03e65ef2f57e23078c89e0fa616d26`

## 7.3 Pre-Installation, Version Check

The release version should be 21.3:

- Log in on the GUI and check the information contained in the menu **About > Version > Release**. The release version should be 21.3

## 7.4 Pre-Installation, Security and Health Steps

1. 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
```

2. Validate the system health.

   On the single node, run:

   `app status`

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

   On the single node, run:

   `diag disk` and then `security check`

   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)
```

   If there are pending Security Updates, then run:

   `security update`

   Then reboot:

   `system reboot`

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

4. Shutdown servers and take snapshots from VMWare.

## 7.5 Patch Installation

On the single node, run:

`app install media/21.3-PB1-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/21.3-PB1-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.

On the single node, run:

- `voss migrate_summary_attributes data/InternalNumberInventory`

## 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 > Patch Bundle** and ensure that the Patch Bundle number 1 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 steps for Microsoft Environments

**Note:** These steps do not have to be carried out in a maintenance window.

1. Do a full MS Teams sync. When carrying out the sync, ensure that:
   - The **Refresh Existing (Changed) Data** option is enabled.
   - The **Force Refresh Of Data** option is enabled.
   - Check that there are no disabled actions on the sync.

- Check that the sync is not ignoring the removal of old instances which no longer exist on the device due to a `PULL_SYNC_DELETE_THRESHOLD_` macro.

This is needed to pull in the data from Teams for the updates drivers and schemas due to the PowerShell 4 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 21.3 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.