VOSS-4-UC

Method of Procedure (MOP) for 19.3.4 Patch Bundle 2 Installation

Release 19.3.4-PB2

Apr 01, 2021

Contents

Dependencies 1

Patch Overview 2

Important Information: 2

Installation Procedure 2

Patch Script Upload 2

Checksum Verification 3

Pre-Installation, Version Check 3

Pre-Installation, Security and Health Steps 3

Patch Installation 4

Post-Upgrade, Security and Health Steps 5

Post-Checks 6

Dependencies

- Release 19.3.4

or

- Release 19.3.4 with 19.3.4 Patch Bundle 1

Patch Overview

- **Patch Name**: `19.3.4-PB2-Delta-Bundle-patch.script`
- **Features Included**: See release notes for detail.
- **SHA256 Checksum**: `468642fbaf676761e326d7f20f58cd45a4329b8c8dae5ad035185650e00a57c1`

Important Information:

- Release 19.3.4 Patch Bundle 2 is a *cumulative* patch bundle and also contains all the Release 19.3.4 Patch Bundle 1 patches.

  For details on 19.3.4 Patch Bundle 1, refer to the Release Notes for 19.3.4 Patch Bundle 1.
- 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.

Installation Procedure

The Patch and the MOP are available here:

- Server Name: https://voss.portalshape.com
- Path: **Downloads > VOSS-4-UC > 19.3.4 > Patches**
- Patch Directory: **Patch Bundle 2**
- Patch File: `19.3.4-PB2-Delta-Bundle-patch.script`
- MOP File (this file): `MOP-19.3.4-PB2-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.

Patch Script Upload

Upload the following file to the media folder on the PRIMARY NODE (or Standalone Node if running in Standalone):

- `19.3.4-PB2-Delta-Bundle-patch.script`

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

Checksum Verification

To verify SHA256 checksums for the patch, run the following command on the PRIMARY NODE:

- Command : `system checksum media/19.3.4-PB2-Delta-Bundle-patch.script`
- Expected: `468642fbaf676761e326d7f20f58cd45a4329b8c8dae5ad035185650e00a57c1`

Pre-Installation, Version Check

The release version should be 19.3.4 or 19.3.4-PB1:

- Log in on the GUI and check the information contained in the menu **About > Version**. The release version should be 19.3.4

or

- Log in on the GUI and check the information contained in the menu **About > Extended Version > Patches** and ensure that the 19.3.4 Patch Bundle number 1 is displayed.

Pre-Installation, Security and Health Steps

1. On the Primary Unified Node (or Standalone Node if running in Standalone) 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 a cluster: on the Primary Unified Node, run:

     `cluster status`
   - On a Standalone Node if running in Standalone, run:

     `app status`
3. Verify network connectivity, disk status, NTP and that there are no pending Security Updates.
   - On a cluster: on the Primary Unified Node run:

     `cluster check`
   - On a Standalone Node if running in Standalone, 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:

- For a multinode system, on the PRIMARY 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`

- For a standalone system, 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.

Patch Installation

Run the following command on the *PRIMARY NODE* (or Standalone Node if running in Standalone):

```
app install media/19.3.4-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/19.3.4-PB2-Delta-Bundle-patch.script delete-on-success yes
--force
```

Post-Upgrade, Security and Health Steps

10.1 On a cluster

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. If you are upgrading directly from 19.3.4 or if you have not carried out this step during the 19.3.4 Patch Bundle number 1 installation, run a manual summary attribute migration:

   `voss migrate_summary_attributes data/InterfaceBusinessAdminPortal`

10.2 On a standalone system

1. Verify Security Updates, network connectivity, disk status and NTP.
   - `app status`
   - `diag disk`
   - `security check`
2. If there are pending Security Updates, then run **security update**:
   - `security update`
3. Reboot:
   - `system reboot`

   Since all services will be stopped, this takes some time.
4. If you are upgrading directly from 19.3.4 or if you have not carried out this step during the 19.3.4 Patch Bundle number 1 installation, run a manual summary attribute migration:

   `voss migrate_summary_attributes data/InterfaceBusinessAdminPortal`

Post-Checks

Generic System Tests:

- Ensure all services are running on *all* nodes using `app status`.
- Log in to Administration Portal, go to **About > Extended Version > Patches** and ensure that the Patch Bundle number 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.
- 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).