VOSS-4-UC

Method of Procedure (MOP) for 19.3.4 Patch Bundle 1 Installation

Release 19.3.4-PB1

Mar 18, 2021

Contents

Dependencies

Release 19.3.4

Patch Overview

- **Patch Name**: `19.3.4-PB1-Delta-Bundle-patch.script`

- **Features Included**: See release notes for detail.

- **SHA256 Checksum**: `03126ee292b496527546955b065639a7b145824a2475f37f2011dca3247ce799`

Important Information 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 the Phone Based registration Feature is installed, ensure that version *19.3.4* is installed *before* running this patch bundle.

Run: `app status`. The output should contain `v19.3.4`, for example:

```
phone-based-registration v19.3.4 (2020-11-11 07:46)
   |-nodeservice         running
```

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 1**

- Patch File: `19.3.4-PB1-Delta-Bundle-patch.script`

- MOP File (this file): `MOP-19.3.4-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.

Patch Script Upload

Upload the following file to the media folder on the PRIMARY NODE:

- `19.3.4-PB1-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-PB1-Delta-Bundle-patch.script`
- Expected: `03126ee292b496527546955b065639a7b145824a2475f37f2011dca3247ce799`

Pre-Installation, Version Check

The release version should be 19.3.4.

Log in on the GUI and check the information contained in the menu **About > Version**.

Pre-Installation, Security and Health Steps

1. 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, verify cluster connectivity:

   ```
   cluster status
   ```

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

   ```
   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)
   ```

4. Shutdown servers and take snapshots from VMWare.

Patch Installation

Run the following command on the *primary node*:

```
app install media/19.3.4-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/19.3.4-PB1-Delta-Bundle-patch.script delete-on-success yes
--force
```

Post-Upgrade, Security and Health Steps

10.1   On a cluster

1. On the primary unified node, verify the cluster status:
   - `cluster status`
2. On each node verify network connectivity, disk status and NTP.
   - `cluster check`
3. Run a manual summary attribute migration:

   ```
   voss migrate_summary_attributes data/InterfaceBusinessAdminPortal
   ```

10.2   On a standalone system

1. Verify the status:
   - `diag health`
2. 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 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).