



# VOSS Automate Health Checks for Cluster Installations Guide

Release 24.2-PB2

March 19, 2025

## Legal Information

- Copyright © 2025 VisionOSS Limited.  
All rights reserved.
- This information is confidential. If received in error, it must be returned to VisionOSS ("VOSS"). Copyright in all documents originated by VOSS rests in VOSS. No portion may be reproduced by any process without prior written permission. VOSS does not guarantee that this document is technically correct or complete. VOSS accepts no liability for any loss (however caused) sustained as a result of any error or omission in the document.

DOCUMENT ID: 20250319064742

# Contents

<b>1</b>	<b>Introduction</b>	<b>1</b>
<b>2</b>	<b>Notification/SNMP setup</b>	<b>2</b>
<b>3</b>	<b>Check general cluster health</b>	<b>3</b>
3.1	Services . . . . .	3
3.2	Nodes in cluster . . . . .	3
3.3	Node communication . . . . .	4
3.4	NTP connectivity . . . . .	4
<b>4</b>	<b>Verify web proxy sanity</b>	<b>5</b>
<b>5</b>	<b>Verify database status</b>	<b>6</b>
5.1	Database health . . . . .	6
5.2	Primary database . . . . .	6
5.3	Database weights . . . . .	7
<b>6</b>	<b>Resource utilization checks</b>	<b>8</b>
6.1	Check disk space . . . . .	8
6.2	Check available RAM . . . . .	8
<b>7</b>	<b>VMWare checks</b>	<b>10</b>
7.1	Check VMWare disk space . . . . .	10
7.2	VMWare snapshots . . . . .	10
7.3	VMWare recommendations . . . . .	10
<b>8</b>	<b>Backup / export</b>	<b>11</b>
<b>9</b>	<b>Latency</b>	<b>12</b>
9.1	Transaction processing . . . . .	12
9.2	UC apps latency . . . . .	12
<b>10</b>	<b>Firewall configurations</b>	<b>13</b>
<b>11</b>	<b>Data collection for offline analysis</b>	<b>14</b>
11.1	Database data information . . . . .	14
11.2	Log collection . . . . .	14
11.3	Export installed patch information . . . . .	15

# 1. Introduction

This document serves as a brief checklist for VOSS Automate installation, deployment and maintenance.

For comprehensive details on the CLI commands, requirements, installation and maintenance procedures, please refer to the following guides:

- [Architecture and Hardware Specification Guide](#)
- [Installation Guide](#)
- [Platform Guide](#)
- [Multi-Cluster Deployments Technical Guide](#)

## 2. Notification/SNMP setup

It is recommended that SNMP and/or notifications should be proactively set up to monitor the system.

To setup:

1. Log in on any unified node (multinode unified topology) / application node (modular cluster topology), then run:  
`notify list`
2. For the warn and error sections, ensure that these are set up with valid details (mail/snmp), then run:  
`snmp list`
3. Ensure the query field has valid credentials for the customer's NMS system.

## 3. Check general cluster health

### 3.1. Services

If any services on the cluster are not running, it could indicate a problem in the system.

To check:

1. Log in on any unified node (multinode unified topology) / application node (modular cluster topology).
2. Run the following commands:  

```
cluster status
```

  
and  

```
cluster run all app status
```
3. Check for any anomalous output, for example, topped services or unknown nodes or mismatched service versions.
4. Resolve issues:
  - Start stopped services.
  - Resolve issues on non-responsive nodes.
  - Escalate unresolvable issues to VOSS L2 helpdesk.

### 3.2. Nodes in cluster

If all nodes in the cluster are not known to all other nodes, provisioning may fail.

1. Log in on any unified node (multinode unified topology) / application node (modular cluster topology).
2. Run the following command:  

```
cluster run database cluster list
```
3. Ensure all nodes list the correct number of nodes.
4. Resolve issues, if any:
  - If one or more nodes do not list all nodes, the nodes may need to be deleted and re-added, possibly from a different unified node. Add or delete nodes until all nodes show the same output of the `cluster list` command.
  - Escalate unresolvable issues to VOSS L2 helpdesk.

### 3.3. Node communication

Ensure the nodes in the cluster can freely communicate.

1. Log in on any unified node (multinode unified topology) / application node (modular cluster topology).
2. Run a cluster command across all nodes, for example:  

```
cluster run all network list
```
3. Verify that all nodes respond with the expected output.
4. To resolve issues, check the general health of the cluster.

### 3.4. NTP connectivity

Ensure NTP is accessible in order to prevent failures such as unexpected session timeout.

For each node:

1. Log in as root.
2. Run the following command:  

```
ntpq -p
```
3. The output displays a result for the **reach** metric. A value of 377 indicates that there has been no packet loss, while a value less than 377 shows that there was some packet loss. A value of zero will need to be resolved.
4. Resolve issues:
  - If the **reach** parameter returns with a value of zero (0), restart the time service using the following command:  

```
app start services:time --force
```
  - Repeat the procedure. If the problem persists, contact VOSS L2 Helpdesk.

## 4. Verify web proxy sanity

To prevent cluster processes from failing silently due to a misconfigured cluster, a web proxy should not have any database or VOSS application services present or running.

1. Log in on all webproxy nodes.
2. Run the following command:  

```
app status | grep "voss-deviceapi\|selfservice\|mongodb"
```
3. Check for any output from the command. A healthy node should simply return to the command prompt with no output from the command.
4. If there are problems identified on any of the webproxy nodes, contact VOSS L2 helpdesk.



## 5. Verify database status

### 5.1. Database health

This procedure ensures that the database is in a healthy state.

1. Log in on any unified node (multinode unified topology) / database node (modular cluster topology).
2. Run the following command:  
`database config`
3. Verify that the **stateStr** of each node is one of the following values:
  - stateStr: PRIMARY
  - stateStr: ARBITER
  - stateStr: SECONDARY
4. If any node has a **stateStr** not listed above, contact VOSS L2 helpdesk.

---

**Important:** Provisioning must not take place if any of the database nodes are in the following states:

- STARTUP
  - STARTUP2
  - RECOVERING
- 

### 5.2. Primary database

This procedure ensures that the primary database is the correct node

1. Log in on any unified node (multinode unified topology) / database node (modular cluster topology).
2. Run the following commands:  
`database primary`  
and  
`cluster run database database primary`
3. Ensure the IP address matches the intended primary database expected.
4. If a failover has occurred for any reason and the primary database has changed from what is expected, refer to the “Check General Cluster Health” section.

## 5.3. Database weights

Database weights are used to determine how a new primary node is elected in the event of database primary node failover. Although any values can be used, recommended weights are:

- For 4 database nodes: weight of 40/30/20/10
- For 6 database nodes: weight of 60/50/40/30/20/10

These weight numbers ensure that if a re-provision occurs (when the primary data center goes offline for an indeterminate time), the remaining nodes have weights that will allow a new primary to be chosen.

1. Log in on any unified node (multinode unified topology) / database node (modular cluster topology).
2. Run the following commands:  

```
database config
```
3. Verify that weights are set with highest numbers in primary Data Center (DC), and lesser weights in secondary DC.
4. To resolve any issues, fix database weights to have the highest numbers at primary DC.

## 6. Resource utilization checks

### 6.1. Check disk space

This procedure checks that there is enough disk space.

1. Login to all nodes.
2. Run the following command:  
`diag disk`
3. Verify that the following disks are not over 85%:

```
/
/opt/platform
/tmp
/var/log
/opt/platform/apps/mongodb/chroot/dbroot
(this is only on:

unified nodes for multinode unified topology
database nodes for modular cluster topology)
```

4. If any node is above the threshold, please clean if possible, else contact VOSS L2 support.

### 6.2. Check available RAM

This procedure ensures that the RAM available per node aligns with the scale of the platform.

- Multinode unified topology: unified nodes must be allocated a minimum of 16GB.
  - Modular cluster topology: application nodes must be allocated a minimum of 16GB.
  - Modular cluster topology: database nodes must be allocated a minimum of 32GB.
  - Each WebProxy should have a minimum of 4GB RAM.
1. Login to one node as platform.
  2. Run the following command:  
`cluster run all diag free`

3. Verify that total RAM aligns with the scale of the platform.

---

**Note:** The command above shows RAM in kilobytes.

---

4. If any node is below the threshold, please allocate more RAM to the virtual machine.

## 7. VMWare checks

### 7.1. Check VMWare disk space

This procedure ensures that the datastore(s) the cluster is using is sufficient for the cluster.

1. Log into the VMWare server(s) hosting the cluster nodes.
2. Identify the Datastore each node is using.
3. Ensure there is sufficient space for all systems.
4. If there is any doubt that datastore space may not be sufficient, contact your VMWare administrator.

### 7.2. VMWare snapshots

VMWare snapshot management is vital to ensure optimal performance.

1. Log in on one VMWare host(s)
2. Ensure that there is no more than one snapshot, if possible. Delete any old snapshots.

### 7.3. VMWare recommendations

It is recommended that there be a 1-to-1 mapping for memory and CPU in VMWare.

1. Log into the VMWare console, select the VOSS nodes one by one.
2. Ensure that the system has a 1 to 1 mapping for memory and CPU. For example, if the system is set to 16GB, there is 16GB RAM reserved, and if CPU is set to 4 cores, that the VMWare host has 4 cores available.

## 8. Backup / export

It is recommended best practice for customers to regularly run a backup.

---

**Note:** To perform these tasks on a multinode unified node topology or on a modular cluster topology, log in on the database node with the second highest weight.

---

1. Create a localbackup with:

```
backup create localbackup
```

2. Add a remote location for the export with:

```
backup add <remotename> sftp://<sftpusername>:<sftppassword>@<IP address>
```

3. Export the local backup with:

```
backup export localbackup <remotename> <timestamp>
```

(<timestamp> seen with the `backup list` command)

4. Ensure that the backup gets run regularly, using the `schedule` commands.

---

**Note:** For more details and examples on backup and restore, refer to the Backup and Import topic in the Platform Guide.

---

## 9. Latency

### 9.1. Transaction processing

Transactions should not be run by nodes over a high latency network, if possible.

1. Log in on any unified node (multinode unified topology) / application node (modular cluster topology).
2. Run the following for all the other nodes:  
`diag ping <IP>`
3. If any of the average round trip time is higher than 10ms, it is recommended that the nodes in the secondary DC should have **voss workers** set to zero (0) on version 11.5.3 and later, or the command `app stop voss-queue` is run on older versions.

---

**Note:** For software versions *pre* 11.5.3, the `app stop voss-queue` command needs to be run after every service restart or server reboot.

---

### 9.2. UC apps latency

Latency between unified nodes and UC apps impacts overall provisioning times against the UC apps. This check is done as part of diagnosis of provisioning performance problems.

For each data center:

1. Log in on any unified node (multinode unified topology) / application node (modular cluster topology).
2. Run the following command for all the UC apps under investigation:  
`diag ping <IP>`
3. Record the output, then send the file with VOSS L2 support.

## 10. Firewall configurations

Incorrect firewall rules can cause outages and make it difficult to resolve issues. These need to be verified by the customer's network/firewall team.

1. Ensure that the connectivity between all VOSS nodes allows bidirectional traffic for ports 80, 443 and 8443. For example, to test platform API connectivity on port 8443 from all other hosts back to a node with an IP address of `10.0.0.10`:
  - a. SSH to `10.0.0.10`
  - b. Run `cluster run all diag test_connection 10.0.0.10 8443 --force` to test connectivity **from** the other hosts in the cluster.
2. Ensure that ports 27020 and 27030 are bidirectionally open between:
  - unified nodes (multinode unified topology)
  - database nodes (modular cluster topology)
  - database and application nodes (modular cluster topology)

For example, to test connectivity from all unified to the arbiter running on a primary node with IP address `10.0.0.10`:

- a. SSH to `10.0.0.10`
  - b. Run `cluster run database diag test_connection 10.0.0.10 27030 --force` to test connectivity from the unified hosts (multinode unified topology) or database nodes (modular cluster topology) in the cluster.
3. From VOSS unified nodes (multinode unified topology) / application and database nodes (modular cluster topology), ensure that all Cisco equipment managed by VOSS is accessible on the relevant ports. For example, to test connectivity from a VOSS Automate cluster to a CUC on `172.16.0.10`:
  - a. SSH to the primary unified node (multinode unified topology) / application node (modular cluster topology).
  - b. Run `cluster run application diag test_connection 172.16.0.10 443` to test HTTPS connectivity to a remote host.



# 11. Data collection for offline analysis

## 11.1. Database data information

Collect information relating to actual database data size usage and index configuration.

1. Log in on the primary unified node.
2. Run the following commands, and save the output to a file:

```
voss db_collection_stats  
and  
voss db_index_stats
```

3. Send the file with the output to VOSS L2.

## 11.2. Log collection

Logs must be extracted to enable offline performance analysis of a platform.

For each node:

1. Log in as platform.
2. Run the following command:

```
log collect start YYYY-MM-DD end YYYY-MM-DD
```

---

**Note:** The **start** and **end** parts of this command must cover the period over which performance analysis is required.

---

3. Send the output files from each node to VOSS L2.

## 11.3. Export installed patch information

Ensures platform has all recommended patches installed.

1. Log into Automate Admin Portal.
2. Navigate to **About > Extended Version** menu.
3. Open **Patches** tab.
4. Export to JSON (via Actions button top right).
5. Send the output files from each node to VOSS L2.