VOSS-4-UC
Installation Guide

Release 19.3.2

Apr 08, 2020

Legal Information

Please take careful note of the following legal notices:

Security Information

This product may contain cryptographic features that may be subject to state and local country laws that govern the import, export, transfer and use of such features. The provision of this software does not imply that third-party authorization to import, export, distribute or use encryption in your particular region has been obtained. By using this product, you agree to comply with all applicable laws and regulations within your region of operation. If you require further assistance, please contact your dedicated VOSS support person.

Contents

1 What’s New

2 Introduction

2.1. Overview

Note: For upgrade steps, refer to the Upgrade Guide.

This document provides an overview of the deployment of the VOSS-4-UC system on VMware.

The system can be deployed in either a test Standalone topology, or a multi-node cluster with High Availability and Disaster Recovery capabilities. It is aimed at Technical and Operational personnel responsible for the deployment of a VOSS-4-UC system.

This system supports various deployments/solutions - the document describes the product in general and is not specific to a particular deployment/solution. For cluster installations, also refer to the Health Checks for Cluster Installations Guide.

Information may vary slightly depending on the installation environment.

2.2. Command Conventions

For file transfers, either **sftp** or **scp** can be used. For example, either:

1. **sftp platform@<unified_node_hostname>**
2. **cd media**
3. **put <upgrade_template_file>**

or:

scp <upgrade_template_file> platform@<unified_node_hostname>:~/media

In this Guide, **scp** is used to show file transfer.

3 Deployment Topologies

3.1. Deployment Topologies

VOSS-4-UC is deployed either as a single node, 2 unified nodes, or a cluster of multiple nodes with High Availability (HA) and Disaster Recovery (DR) qualities.

Each node can be assigned one or more of the following functional roles:

- WebProxy - load balances incoming HTTP requests across unified nodes.
- Standalone - combines the Application and Database roles for use in a nonclustered environment.
- Unified - similar to the Standalone role Application and Database roles, but clustered with other nodes to provide HA and DR capabilities

The nginx web server is installed on the WebProxy, Standalone, and Unified node, but is configured differently for each role.

In a clustered environment containing multiple Unified nodes, a load balancing function is required to offer HA (High Availability providing failover between redundant roles).

VOSS-4-UC supports deployment of either the WebProxy node or a DNS load balancer. Here are some considerations in choosing a WebProxy node vs. DNS:

- The Proxy takes load off the Unified node to deliver static content (HTML/JAVA scripts). When using DNS or a third-party load balancer, the Unified node has to process this information.
- DNS does not know the state of the Unified node.
- The WebProxy detects if a Unified node is down or corrupt. In this case, the WebProxy will select the next Unified node in a round robin scheme.

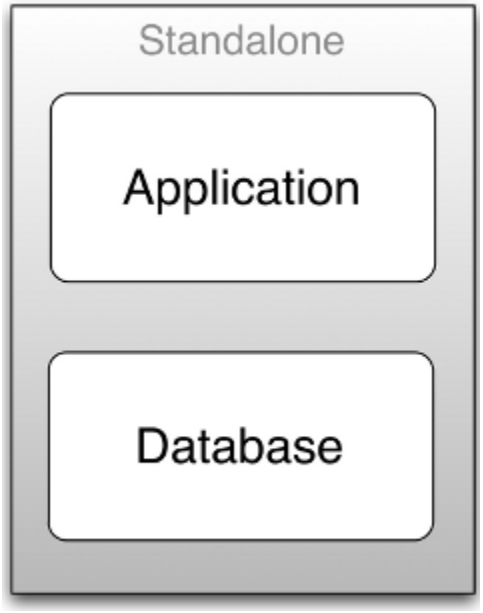
We recommend that you run no more than two Unified nodes and one WebProxy node on a physical server (VMware server). Also recommended is that the disk subsystems be unique for each Unified node.

The following deployment topologies are defined:

- Test or Small Production: a single, Standalone node with Application and Database roles combined. No High Availability/Disaster Recovery (HA/DR) is available.
- Production with Unified Nodes: in a clustered system, comprising:
  - 2, or 4 to 6 Unified nodes (each with combined Application and Database roles)
  - 0 to 4 (maximum 2 if 2 Unified nodes) WebProxy nodes offering load balancing. The WebProxy nodes can be omitted if an external load balancer is available.

3.2. Standalone Deployment

- No High Availability or Disaster Recovery capability is offered in this topology.



3.3. Multinode Cluster with Unified Nodes

In order to achieve Geo-Redundancy using the Unified nodes, you need the consider the following:

- Either four or six Unified nodes - each node combining Application and Database roles - are clustered and split over two geographically disparate locations.
- Two Web Proxy nodes to provide High Availability that ensure an Application role failure is gracefully handled. More may be added if Web Proxy nodes are required in a DMZ.

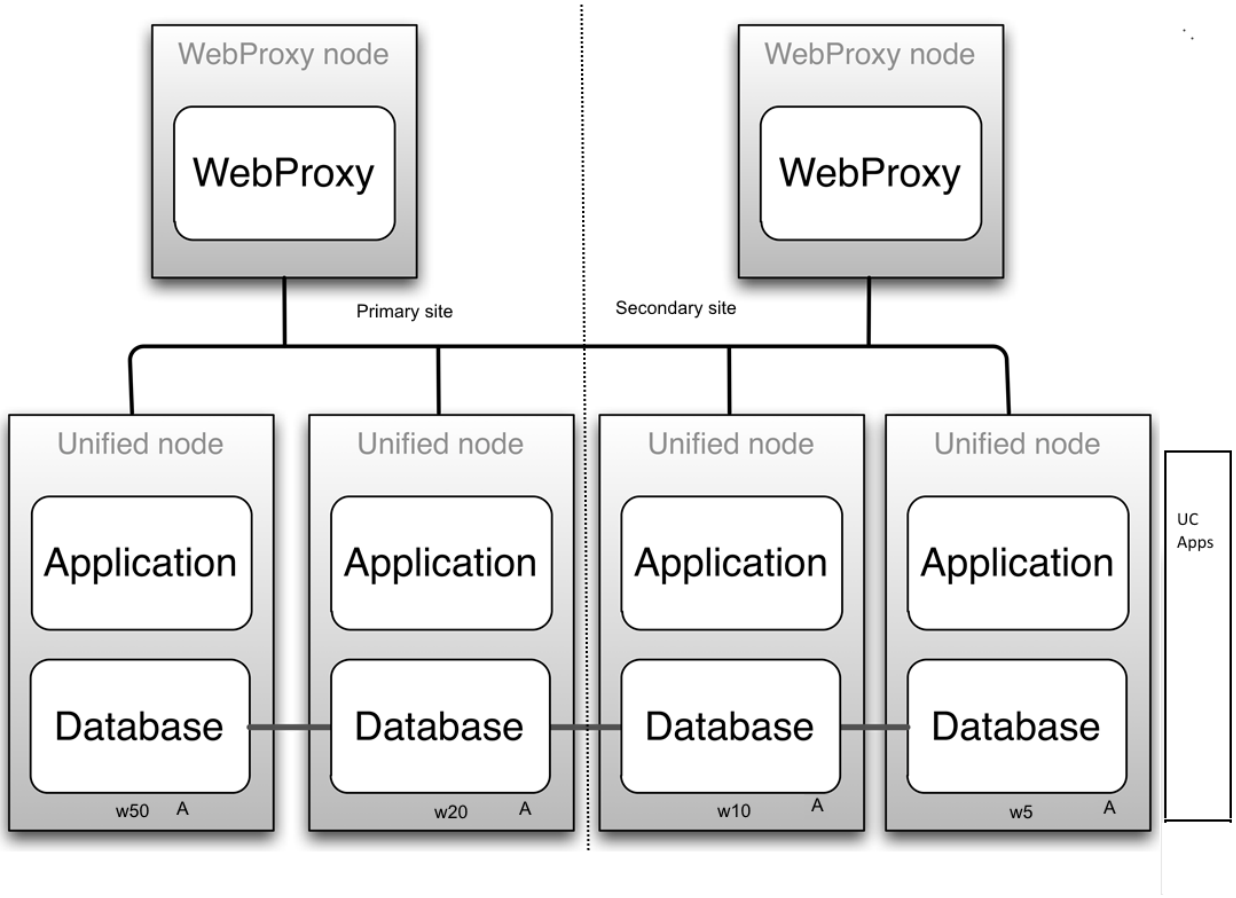
  It is strongly recommended *not* to allow customer end-users the same level of administrator access as the restricted groups of provider- and customer administrators. This is why Self-service web proxies as well as Administrator web proxies should be used.

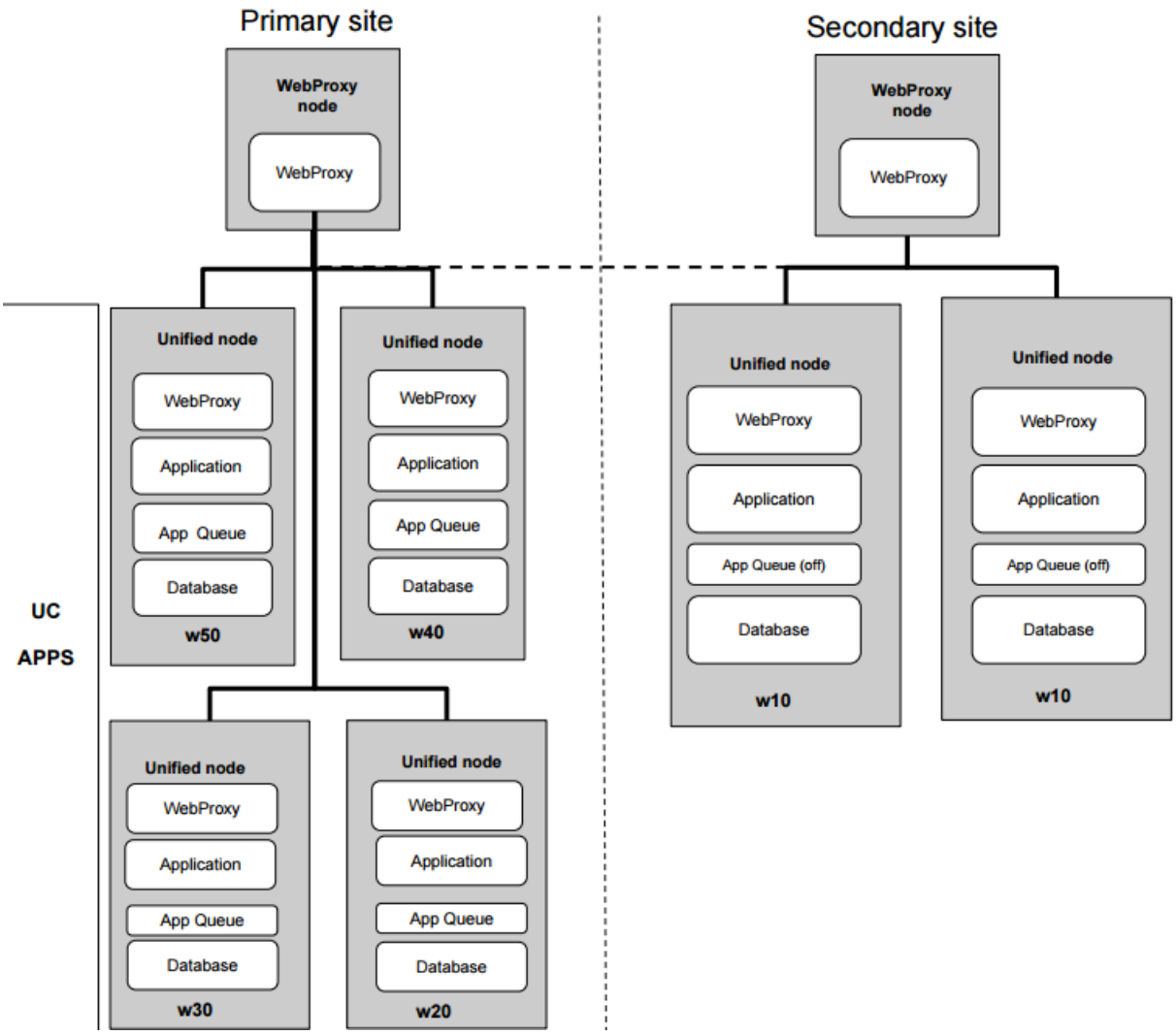
  Systems with Self-service only web proxies are *only* recommended where the system is customer facing, but where the customer does not administer the system themselves.
- Web Proxy and Unified nodes can be contained in separate firewalled networks.
- Database synchronization takes places between all Database roles, thereby offering Disaster Recovery and High Availability.
- For 6 unified nodes, all nodes in the cluster are active. For an 8 node cluster (with latency between data centers greater than 10ms) , the 2 nodes in the DR node are passive, in other words, the **voss workers 0** command has been run on the DR nodes.

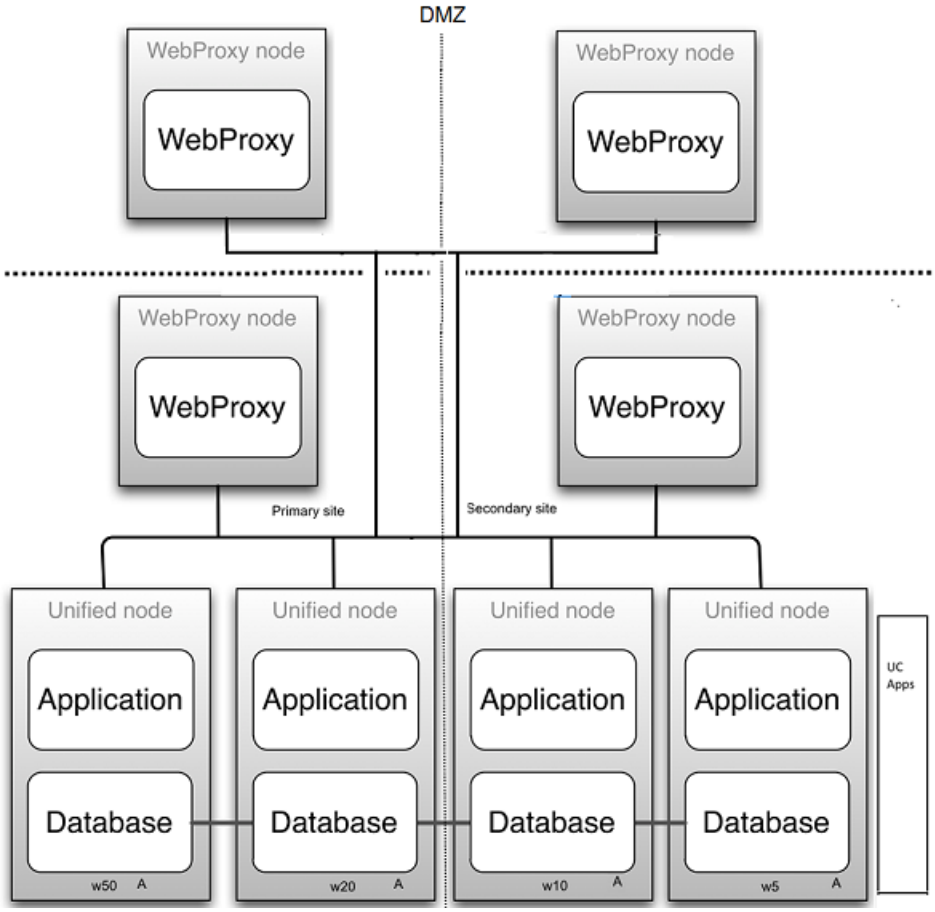
Primary and fall-back Secondary Database servers can be configured manually. Refer to the Platform Guide for further details.

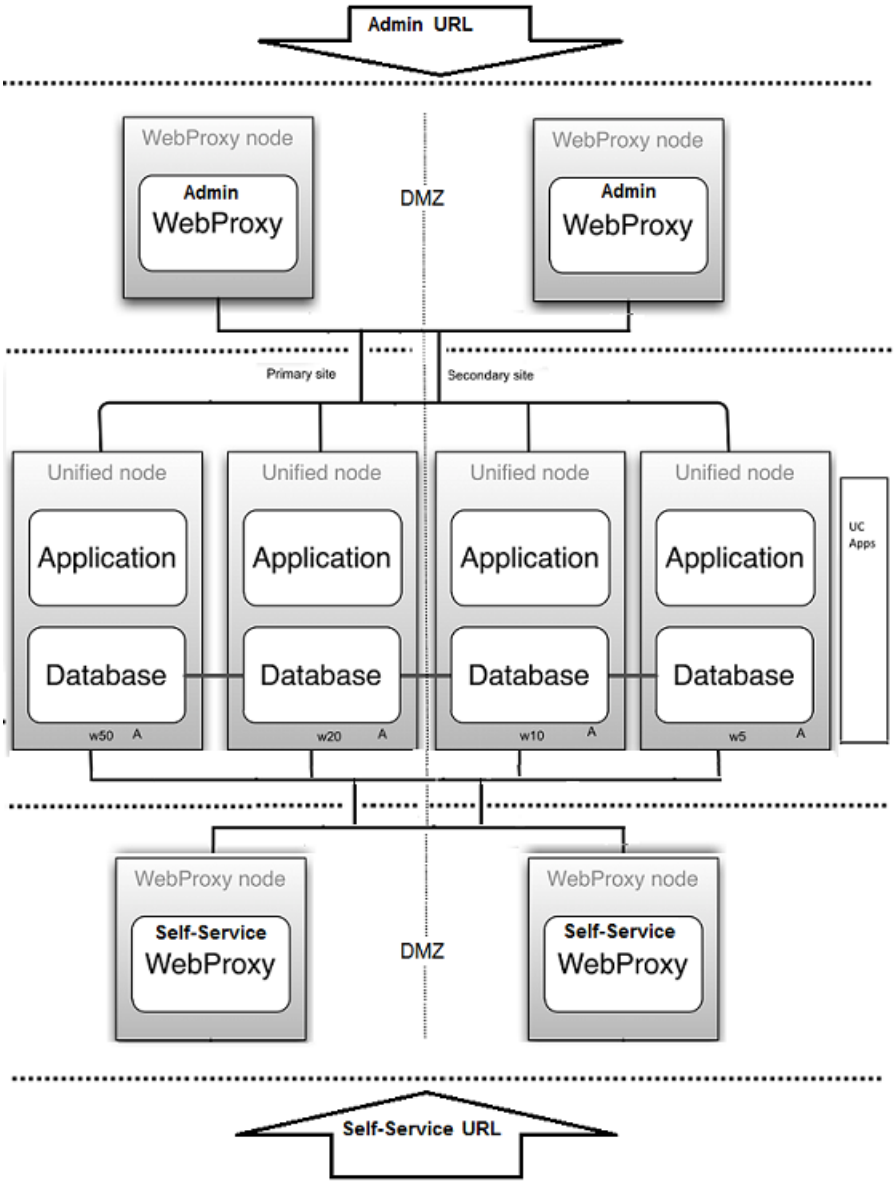
The diagrams in this section illustrate:

- the six node cluster
- the eight node cluster
- 2 Web Proxy nodes in a DMZ
- 4 (2 admin, 2 Self-service) Web Proxy nodes in a DMZ









3.4. Two-node Cluster with Unified Nodes

In order to achieve Geo-Redundancy using the Unified nodes, you need the consider the following:

- Two unified nodes - each node combining application and database roles - are clustered and optionally split over two geographically disparate locations.
- (Optional) Two web proxy nodes can be used. It may be omitted if an external load balancer is available.
- Web proxy and unified nodes can be contained in separate firewalled networks.
- Database synchronization takes place from primary to secondary unified nodes, thereby offering Disaster Recovery if the primary node fails.
- If the secondary unified node has *more than 10ms latency* with the primary unified node, it must be configured to be in the *same* geographical location.

Important:

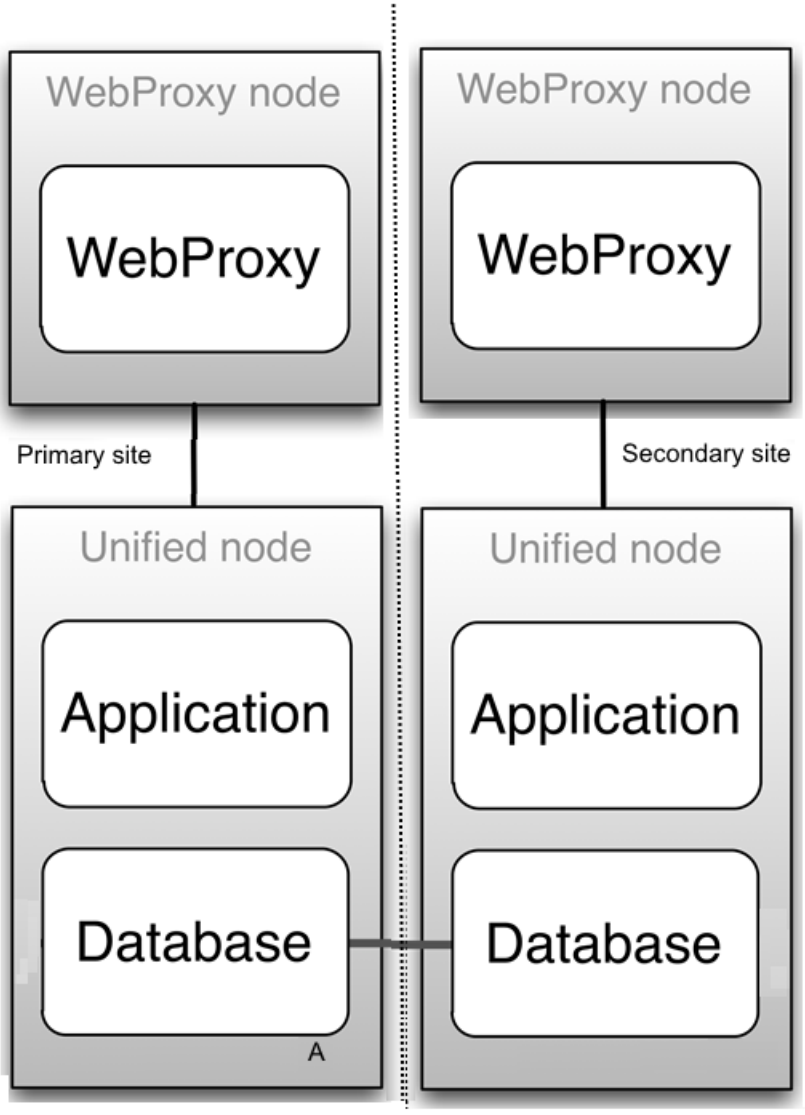
With only two Unified nodes, with or without Web proxies, there is no High Availability. The database on the primary node is read/write, while the database on the secondary is read only.

Only redundancy is available.

- If the primary node fails, a manual delete of the primary node on the secondary and a cluster provision will be needed.
- If the secondary node fails, it needs to be replaced.

Refer to the topic on DR Failover and Recovery in a 2 Node Cluster in the Platform Guide.

The diagram below illustrates the two node cluster:



3.5. Multi Data Center Deployments

Multinode clusters can be deployed in both Active/Active or Active/Standby configurations. Active/Active configurations have all the Unified nodes enabled for transaction processing. Active/Standby configurations have only the Unified nodes in the primary data center (the data center containing the Unified node with the primary database) enabled for transaction processing.

In order to run an Active/Active configuration, the latency (RTT) between data centers must not exceed 20ms. For higher latencies an Active/Standby configuration must be used.

To switch to an Active/Standby configuration, do the following on all Unified nodes in the secondary data center (the data center *not* containing the Unified node with the primary database):

1. log into platform:

   ssh platform@<ip_address>

2. set the worker count on the nodes in the secondary data center to zero:

   voss workers 0

   Setting the number of workers is persistent; in other words, this setting will still apply after upgrades and system restart.

For an Active/Standby configuration, the proxy server web weights should be set to the Unified nodes on the primary data center. This is done with the **web weight add** command.

The web weight specifies the routing and relative counts of the initial HTTP request from the Web Proxy to a Unified Node. The initial request could be a request such as a transaction, or for example a GET request. Consider web weights configuration as shown below:

```
172.0.0.158:443: 1
172.0.0.159:443: 1
172.0.0.161:443: 1
172.0.0.162:443: 1
173.0.0.163:443: 0
173.0.0.164:443: 0
```

This configuration means that the servers `173.0.0.163` and `173.0.0.164` serve as backup servers and requests are only routed to these if the other servers are not available. While the other servers are available, an equal number of requests are routed to them in a round-robin manner. Refer to the Best Practices Guide for more details on deployment models and web weight settings.

Consider an example where:

1. Primary data center has unified nodes with IP addresses and ports:
   - 172.0.0.158:443
   - 172.0.0.159:443
   - 172.0.0.161:443
   - 172.0.0.162:443
2. Secondary data center has unified nodes with IP addresses and ports:
   - 173.0.0.163:443
   - 173.0.0.164:443

The defaults of the **web weight list** command run on the proxy servers is as below:

1. Primary data center proxy server:

```
$ web weight list
Default service weights
    upstreamservers:
        selfservice:
            172.0.0.158:443: 1
            172.0.0.159:443: 1
            172.0.0.161:443: 1
            172.0.0.162:443: 1
            173.0.0.163:443: 0
            173.0.0.164:443: 0
        voss-deviceapi:
            172.0.0.158:443: 1
            172.0.0.159:443: 1
            172.0.0.161:443: 1
            172.0.0.162:443: 1
            173.0.0.163:443: 0
            173.0.0.164:443: 0
```

2. Secondary data center proxy server:

```
$ web weight list
Default service weights
    upstreamservers:
        selfservice:
            172.0.0.158:443: 0
            172.0.0.159:443: 0
            172.0.0.161:443: 0
            172.0.0.162:443: 0
            173.0.0.163:443: 1
            173.0.0.164:443: 1
        voss-deviceapi:
            172.0.0.158:443: 0
            172.0.0.159:443: 0
            172.0.0.161:443: 0
            172.0.0.162:443: 0
            173.0.0.163:443: 1
            173.0.0.164:443: 1
```

In order to ensure that the secondary data center is configured for a Standby mode, change the web weights to show `userweights` as seen in the output on the *secondary* data center proxy server below:

```
$ web weight list
Default service weights
    upstreamservers:
        selfservice:
            172.0.0.158:443: 0
            172.0.0.159:443: 0
            172.0.0.161:443: 0
            172.0.0.162:443: 0
            173.0.0.163:443: 1
            173.0.0.164:443: 1
        voss-deviceapi:
            172.0.0.158:443: 0
            172.0.0.159:443: 0
            172.0.0.161:443: 0
            172.0.0.162:443: 0
```

(continues on next page)

(continued from previous page)

```
            173.0.0.163:443: 1
            173.0.0.164:443: 1

Customized service weights
    userweights:
        172.0.0.158:443: 1
        172.0.0.159:443: 1
        172.0.0.161:443: 1
        172.0.0.162:443: 1
        173.0.0.163:443: 0
        173.0.0.164:443: 0
```

As can be seen, the load balancing web weights have been changed to the unified nodes on the *primary* data center.

3.6. Clustering Considerations

The cluster contains multiple nodes which can be contained in separate firewalled networks.

Network ports need to be opened on firewalls to allow inter-node communication – these are described in more detail in the Platform Guide.

All communication between nodes is encrypted.

Node type	Ports
WebProxy	22 (ssh & sftp), 80 (http), 161 & 162 (snmp), 443 & 8443 (https)
Unified	22 (ssh & sftp), 80 (http), 161 & 162 (snmp), 443 & 8443 (https), 27019, 27020 & 27030 (database)

- 22/ssh is used for remote administration
- 80 and 443 is used for the web server
- 161 and 162 are used for sending and receiving snmp
- 8443 is used for inter-cluster communication
- 27019, 27020 and 27030 is used for database queries and replication

3.7. Network Communications between Nodes within the Cluster

The cluster contains multiple nodes which can be contained in separate firewalled networks. Network ports need to be opened on firewalls to allow inter-node communication.

All communication between nodes is encrypted.

The following details are all based on the default settings. These can vary depending on the application setup and network design (such as NAT) of the solution, so may need adjustment accordingly. Where a dependant is noted, this is fully dependant on the configuration with no default.

These communications are all related to communications between application nodes within the cluster. There are a few different deployment models so the details below cover the different models and relevant ports. So review and implement according to the deployment model in use.

Note that Standalone is only a single node so this section is not relevant for that deployment model.

- Proxy to Proxy Node

  This is relevant if the proxy node is present in the system.

Communication	Protocol	Port
Cluster Communications	HTTPS	TCP 8443 bi-directional

- Proxy to Unified/Application Node

  This is relevant if the proxy node is present in the system.

Communication	Protocol	Port
User access	HTTPS	TCP 443
Cluster Communications	HTTPS	TCP 8443 bi-directional

- Unified Node to Unified node

  This is relevant to the communications between the unified nodes (application and database combined). If the application and database nodes are split, then see the relevant application and database node details below. Database arbiters run on port 27030.

Communication	Protocol	Port
Database access	database	TCP 27020 and 27030 bi-directional
Cluster Communications	HTTPS	TCP 8443

- Application node to Application node

  This is relevant to the communications between application nodes nodes in the system. This is only relevant where the database node is separate from the application node (in other words, not Unified node).

Communication	Protocol	Port
Cluster communications	HTTPS	TCP 8443 bi-directional

- Application Node to Database node

  This is relevant to the communications between the application node and the database node. This is relevant if the database node is separate from the application node. Database arbiters run on port 27030.

Communication	Protocol	Port
Database access	database	TCP 27020 and 27030 bi-directional
Cluster Communications	HTTPS	TCP 8443

- Database Node to Database node

  This is relevant to the communications between the application node and the database node. This is relevant if the database node is separate from the application node. Database arbiters run on port 27030.

Communication	Protocol	Port
Database access	database	TCP 27020 and 27030 bi-directional
Cluster Communications	HTTPS	TCP 8443

3.8. Cluster Commands

The following Command Line Interface console display shows the available commands for clustering.

```
cluster add <ip>                          - add a new node to join the existing
                                            cluster
cluster backup <backup location>          - Run a backup across the cluster
cluster del <ip>                          - remove a node from the existing
                                            cluster
cluster job kill <pid>                    - Kill a detached job <pid>
cluster job list                          - List detached jobs in the cluster
cluster job reconnect <pid>               - Reconnect to a detached job <pid>
cluster list                              - display the list of nodes associated
                                            with the cluster
cluster prepnode                          - Prepares the system so that it can
                                            be joined to a cluster
cluster provision [datacentre             - perform cluster-wide provisioning
   <location>] [role <role>]
cluster run <where> <command>             - run the command on a particular
                                            host. <where> can either be a name
                                            prefix, ip, role, or 'all'
cluster status                            - display the status of the cluster
cluster upgrade <iso/url> [datacentre     - upgrade all applications from iso
   <location>] [backup <location>]          image <iso-name>. <iso-name> can
                                            be a URL for upgrading from a
                                            remote server.
cluster where <application>               - determine on which nodes the
                                            application is installed
```

3.9. Geo-redundancy/Redundancy And DR Synopsis

High Availability (HA) is an approach to IT system design and configuration that ensures VOSS-4-UC is operational and accessible during a specified time frame. This is achieved using redundant hardware and resources. If there is a failure, an automatic failover will occur to a second node.

Web server proxy nodes perform load-balancing between application roles, so that load is distributed. During provisioning, the web server proxy is provided with all the IP addresses of the application nodes. The web server software then does load balancing among these nodes, according to its configuration. If a node fails to respond in a set time, the proxy will send the transaction to another node. This means that in the event that an Application role is lost, the WebProxy will transparently bypass the faulty Application role.

The proxy web server that is configured to be located in the primary site normally load balances to the two unified nodes in the primary site. The proxy web server falls back to the two nodes in the Disaster Recovery site if the nodes in the primary site are down. The web proxy nodes in the secondary site defaults load balancing to the two unified nodes configured for the secondary site.

Data is replicated between Database roles, and role failure is recoverable. This is done using the database replication facility. Automatic failover between Database roles occurs while there is greater than 50% Database role availability. Once there is insufficient role availability, the system needs to be manually re-provisioned.

HA can be increased by adding nodes to the cluster. Application performance and availability can be increased by adding additional application role servers.

Backups can be scheduled to run automatically across the cluster. Backups include application data, configuration and software. Backups can take place to both local disk and remote network location. Every node upgrade is preceded by a snapshot backup which allows any upgrade to be rolled back. Refer to the Platform Guide for details.

4 Prepare to Install

4.1. Installation Prerequisites

Install VOSS-4-UC in the same domain as Cisco Hosted Collaboration Mediation Fulfillment.

Installation has the following prerequisites:

- HCM-F services are activated and running.
- Network connectivity is available between Unified CDM nodes and the HCM-F, UC application servers, and WebEx servers.

4.2. Standalone System Hardware Specification

Virtual machine requirements are specified in the table below.

Node type	Quantity	VM	Memory	CPU	Disk	Network
Standalone	1	>= VMware 5.1	16 GB with 16 GB reservation	4 vCPU @ 2 GHz with 4000 MHz reservation	370 GB partitioned: • 20 GB for OS • 50 GB for application: 10 GB for logs, 40GB for our apps • 50 GB for compressed backups • 250 GB for database	1 Gbit/s minimum

For Memory and CPU, the Resource Allocation Reservation on VMware is indicated in the table. Hyper-threading is supported.

The maximum number of users for a standalone node is 50,000.

4.3. Multinode Cluster Hardware Specification

Virtual machine requirements are specified in the table below.

Node type	Quantity	VM	Memory	CPU	Disk	Network
Unified	4 or 6	>= VMware 5.1	16 GB with 16 GB reservation	4 vCPU @ 2 GHz with 4000 MHz reservation	370 GB partitioned: • 20 GB for OS • 50 GB for application: 10 GB for logs, 40GB for our apps • 50 GB for compressed backups • 250 GB for database	1 Gbit/s minimum
WebProxy	2	>= VMware 5.1	4 GB with 4 GB reservation	2 vCPU @ 2 GHz with no reservation	70 GB partitioned: • 20 GB for OS • 50 GB for application	1 Gbit/s minimum

For Memory and CPU, the Resource Allocation Reservation on VMware is indicated in the table. Hyper-threading is supported.

The OS disk requirement is fixed and logs are rotated to ensure that 10 GB is sufficient. 40 GB for applications is a generous allocation and does not scale with the number of users.

The Database storage partition is sized to support 250 K users. Database backups are compressed and the partition is sized to ensure that sufficient space available to support backup of 250 GB database.

The backup disk should be Thick Provisioned and Eager Zeroed for better performance immediately after installation.

Web Proxies are optional, but if Web Proxies are used, then they form part of the cluster to allow sharing of static data and other content as needed (for example, themes).

To set up the disk requirements, the disk should be set up on the VMware GUI Resources tab where a disk can be created. This task should be done after the OVA import but prior to the boot of the system.

4.4. Two-node Cluster Hardware Specification

Virtual machine requirements are specified in the table below.

Node type	Quantity	VM	Memory	CPU	Disk	Network
Unified	= 2	>= VMware 5.1	16 GB with 16 GB reservation	4 vCPU @ 2 GHz with 4000 MHz reservation	370 GB partitioned: • 20 GB for OS • 50 GB for application: 10 GB for logs, 40GB for our apps • 50 GB for compressed backups • 250 GB for database	1 Gbit/s minimum
WebProxy	>= 0	>= VMware 5.1	4 GB with 4 GB reservation	2 vCPU @ 2 GHz with no reservation	70 GB partitioned: • 20 GB for OS • 50 GB for application	1 Gbit/s minimum

For Memory and CPU, the Resource Allocation Reservation on VMware should correspond with these requirements.

4.5. Network Docker Container Range

Important:

- If either:

  a. Installing the VOSS-4-UC platform release 19.2.1 for the first time

  or

  b. Upgrading to release 19.2.1 from CUCDM 11.5.3 / VOSS-4-UC 18.1 or older

  then the system will use the *new* IP address range `172.31.252.1/22` for each Docker container.
- Otherwise, users who upgrade to release 19.2.1 from 19.1.1 and later will retain either the default container host IP address range `172.17.0.0/16` or their modified range (as in steps below).
- Before installation, verify with your network administrator that this address range is not in use.

  If it is in use, modify the Private Address Space using the **network container range add <private IP>** command as described below.

RFC-1918 states that the following three blocks of the IP address space are reserved for private internets:

```
10.0.0.0        -   10.255.255.255  (10/8 prefix)
172.16.0.0      -   172.31.255.255  (172.16/12 prefix)
192.168.0.0     -   192.168.255.255 (192.168/16 prefix)
```

This subnet block address range may can be modified to another Private Address Space if needed.

Use the command **network container range list** to see the current Private Address Space.

For example:

```
$ network container range list
    range: 10.1.2.1/24
```

Use the command **network container range add <private IP>** to modify the Private Address Space.

Important: A valid Private Address IP is required as input.

The range `/24` is appended to the IP. For example, if `192.168.0.6` is used, the Private Address range `192.168.0.0/24` is used.

In a clustered environment, you could use **cluster run all network container range add <private IP>**, but if required, the Private Address Space can be also set to be different on each node by running the **add** command on each individual node.

For example:

```
$ network container range add 192.168.2.3
You are about to restart all services. Do you wish to continue?y
Application processes stopped.  (note this line changes dynamically)

Reconfiguring applications....
Application  processes started. (note this line changes dynamically)
```

4.6. Backup Size Considerations

The default backup partition size is 50GB for the default 250GB database partition size. These are the default partition installation sizes. It is recommended that a 250GB backup partition size be used if the database size is 50GB.

To determine the required space for a specific backup partition, carry out and consider the following:

1. Run **backup create <name>** from the CLI. The command output indicates the required space needed to do the backup and the command can be canceled to cancel the actual backup, if needed. If the current backup partition size is too small, the command will fail and suggest the size of the partition required. If there is sufficient space but only a size check is required, the backup command can be canceled (Ctrl-C), if needed.
2. Run **voss db_collection_stats all** to show the size of the current database. This command validates the size of the database. This total will be smaller than the suggested backup backup size.

- A local backup requires a partition of at lease twice the size of the database. Preferably add another +30% of this. For remote backups, the size should be a partition of the size of the database plus an additional 30% of this.
- Database growth over time needs to be considered and allowed for in the backup partition size.
- Space for multiple local backups also needs to be considered and added to the calculated backup partition size.

5 Install VOSS-4-UC

5.1. Installation Process

The installation process is divided into:

1. The VMWare installation of a node (*Create a New VM Using the Platform-Install OVA*).
2. Node setup for standalone or multinode installations (*Multinode Installation* and *Standalone Installation*).

The node setup stage requires one or more prerequisite VMWare node installations.

5.2. Create a New VM Using the Platform-Install OVA

The steps below show the common setup of a *single node* from the OVA file - either for the purposes of:

- a standalone installation
- a node installation during multinode installation - see *Notes on Multi-Node Installation*
- or during a failover recovery

The steps will therefore be followed either once or multiple times during installation - in accordance with the required topology.

The downloaded OVA file is imported into VMware vCenter Server. Only one OVA file is used to deploy all the functional roles. You choose the specific node *role* when the installation wizard is run.

1. Log in to vSphere to access the ESXi Host.
2. Choose **File > Deploy OVF Template**.
3. Choose Source, browse to the location of the .ova file, and click **Next**.
4. On the Name and Location page, enter a Name for this server.
5. On the Deployment Configuration page, select the appropriate node type.
6. Choose the resource pool in which to locate the VM.
7. Choose the data store you want to use to deploy the new VM.
8. Choose the disk format to use when deploying the new VM.

   In production environments, “thick provisioning” is mandatory.

   Thick Provision Eager Zeroed is recommended.
9. On the Network Mapping, choose your network on which this VM will reside.

10. Do not select Power on after deployment.
11. On the Ready to Complete page, click **Finish** to start the deployment.
12. After the VM is created, select the CD ROM configuration and verify the **Connect at Power On** check box is enabled. Also, verify the memory, CPU, and disk settings against the requirements shown in either the Standalone System Hardware Specification or Multinode Cluster Hardware Specification section in the Install Guide.
13. Power on the VM.
14. Configure the options in the installation wizard:

Option	Option name	Description
1	IP	The IP address of the server.
2	netmask	The network mask for the server.
3	gateway	The IP address of the network gateway.
4	DNS	The DNS server is optional. Ensure that the DNS server is capable of looking up all hostnames referred to, including NTP server and remote backup locations.
5	NTP	The NTP server is mandatory to ensure that time keeping is accurate and synchronized among nodes in the same cluster.
6	boot password	Enable boot loader configuration password. See the example below.
7	hostname	The hostname, not the fully qualified domain name (FQDN).
8	role	• A WebProxy role installs only the front-end web server together with ability to distribute load among multiple middleware nodes. • An Application node is the main transaction processing engine and includes a web server which can operate by itself, or route transactions from a web node. • A Database node provides persistent storage of data. • A Standalone node consists of the Web, Application, and Database roles on one node. • A Unified node consists of the Web, Application, and Database roles on one node. On installation, the system needs to be clustered with other nodes and the cluster provisioned.
9	data center	The system's geographic location (data center name, city, country that a customer can use to identify the system location). You cannot change this setting once set.
10	platform password	Platform password must be at least eight characters long and must contain both uppercase and lowercase letters and at least one numeric or special character.

Note: On a fresh installation, if you run the install on a network with a DHCP server and encounter an error:

"Error: DNS server <DNS server> is either invalid or cannot be reached on the network"

you can enter a valid DNS server address to continue the installation.

Once all details are entered, installation will commence. When installation is complete, the system will reboot. Since all services will be stopped, this takes some time.

5.2.1. Notes on Passwords and Security

The default security protocol for the web server is TLSv1.2.

Password protection can be enabled on the VOSS-4-UC boot loader configuration from the install wizard upon first install and also from the CLI - see the topic on System Boot Passwords in the Platform Guide for commands to enable, disable or reset the boot password.

Important: The boot password is non-recoverable.

The console example below shows the `boot password` configuration output:

```
(1)              ip    (199.29.21.89)
(2)         netmask    (255.255.255.0)
(3)         gateway    (199.29.21.1)
(4)             dns    (199.29.88.56)
(5)             ntp    (199.29.88.56)
(6)   boot password    (disabled)
(7)        hostname    (atlantic)
(8)            role    (UNDEFINED)
(9)     data centre    (earth)
(10) platform password (UNDEFINED)
Select option ? 6
Valid passwords must contain:
   at least one lower- and one upper-case letter,
   at least one numeric digit
   and a special character eg. !#@$%&^*
Password: Please enter platform user password:
 Please re-enter password
Password:
NOTE: The system boot password is now set for user platform.
```

When the boot password is set, the wizard will show:

```
(6)   boot password    (*****)
```

5.2.2. Notes on Multi-Node Installation

According to the multi-node deployment topology and specification, the *role* of each VM installation is as indicated below.

- For each WebProxy instance, create a new VM using the platform-install OVA. For *role*, select **(3) WebProxy**. Specify the appropriate data center (Primary/DR site) for each WebProxy instance.
- For each Unified instance, create a new VM using the platform-install OVA. For *role*, select **(2) Unified**. Specify the appropriate data center (Primary/DR Site) for each Unified instance.

  The following Unified nodes are required in the cluster:

- One Unified node as the Primary node at the Primary site
- One Unified node as the Secondary node at the Primary site
- Two Unified nodes as the Secondary nodes at the Disaster Recovery (DR) site

Note:

- For a six Node Multi Cluster deployment there are; two Unified nodes (one Primary and one Secondary) and one WebProxy node at the Primary site, and two Unified nodes (both Secondary) and one WebProxy node at the DR site.
- For an eight Node Multi Cluster deployment, there are four Unified nodes (one Primary and three Secondary) and one WebProxy node at the Primary site. Two Unified nodes (both Secondary) and one WebProxy node are at the DR site.

Also refer to Multinode Installation section in the Install Guide.

Detailed configuration can be applied from the Command Line Interface (CLI). Use **network help** or **network** for details. For example, domain can be configured using **network domain add <domain-name>**. For a geo-redundant deployment, the `data center` information entered in the wizard is equivalent to the location information.

5.2.3. Finalize the Installation

When the installation of the OVA is complete, a sign-in prompt for the platform user is displayed. The system is ready for use.

Connect to newly deployed server CLI as the platform user.

The login message would for example looks the same as below:

```
Last login: Wed Nov  2 11:12:45 UTC 2016 from thwh on pts/6
Last failed login: Wed Nov  2 11:19:53 UTC 2016 from iza on ssh:notty
There were 2 failed login attempts since the last successful login.

host: dev-test, role: webproxy,application,database, load: 0.21, USERS: 3
date: 2016-11-02 11:19:57 +00:00, up: 14:19
network: 172.29.253.14, ntp: 172.29.1.15
HEALTH: NOT MONITORED
database: 31Gb
Failed logins: 2 since Wed Nov 02 11:19:53 2016 from iza

    mail - local mail management          keys - ssh/sftp credentials
 network - network management           backup - manage backups
    voss - voss management tools           log - manage system logs
database - database management          notify - notifications control
schedule - scheduling commands        selfservice - selfservice management
    diag - system diagnostic tools      system - system administration
    snmp - snmp configuration             user - manage users
 cluster - cluster management           drives - manage disk drives
     web - web server management           app - manage applications
security - security update tools
```

If the user failed to log in prior to a successful login, the count, date and origin of the attempts are shown as `Failed logins`. A successful login resets this login count.

Note: Return to Multinode Installation, Standalone Installation or Failover step to complete the overall installation or failover recovery procedure.

5.3. Multinode Installation

5.3.1. Before You Begin

Before continuing, you should have followed the OVA installation on each node according to the steps and preliminary requirements specified in: *Create a New VM Using the Platform-Install OVA* and according to the node roles as indicated in *Notes on Multi-Node Installation*.

Optionally download or extract language pack template files to support languages other than English.

Note:

- For geo-redundant Multinode Cluster deployment with six Unified Nodes, there are four Unified nodes in the Primary Site and two Unified nodes in the Disaster Recovery (DR) Site in active-standby setup.

  The worker count (**voss workers** command) needs to be set on the DR nodes. Refer to:

  - *Multinode Cluster with Unified Nodes*
  - *Multi Data Center Deployments*
- For 2 node cluster deployment there are 2 unified nodes.
- Template installation and upgrade takes approximately two hours. You can follow the progress on the GUI transaction list.
- It is strongly recommended *not* to allow customer end-users the same level of administrator access as the restricted groups of provider- and customer administrators. This is why Self-service web proxies as well as Administrator web proxies should be used.

  Systems with Self-service only web proxies are *only* recommended where the system is customer facing, but where the customer does not administer the system themselves.
- For cluster installations, also refer to the Health Checks for Cluster Installations Guide.
- If it is necessary to change an IP address of a node in a cluster, first remove it from the cluster by running the command below *on the node to be changed*:

  cluster del <IP address of node to be changed>
- Refer to *Installation Logs* for troubleshooting logs during an installation.

The standard **screen** command should be used where indicated, and the *reconnect* parameter is available if needed:

- **screen** - start a new session
- **screen -ls** - show sessions already available
- **screen -r [screen PID]** - reconnect to a disconnected session

We recommend using the **screen** command to avoid failures if the connection is interrupted whilst running the command. If the connection is interrupted whilst running the command in `screen` then the session can be retrieved by first listing the sessions PID currently running in screen: **screen -ls**, and then reconnecting to the session using **screen -r [screen PID]**.

The version of **screen** used in VOSS-4-UC also supports the creation of a log file. If long-running commands will be run, the log file captures screen console output up to the session timeout. A message shows:

```
timed out waiting for input: auto-logout
```

To create a screen log file:

1. Run **screen** and wait for screen to open.
2. Press **<Ctrl>-a** then **:** (colon). This will enter screen command mode at the bottom of the console.
3. Create your screen logfile in the `media/` directory:
    a. In screen command mode, type **logfile media/<screen-logfilename>.log**
    b. Press **<Enter>**
    c. Press **<Ctrl>-a** and then **H** to start writing to the log file
    d. Run your commands.

If the **screen** session times out, you can obtain console output from the log file, for example:

$ sftp platform@<host>:media/<screen-logfilename>.log

5.3.2. Procedure

1. Install VMware tools on each node.
    a. Log in to each node and run **app install vmware**.
    b. Verify that vmware is running: **app list**.
2. Prepare each node to be added to the cluster:
    a. Select a primary Unified node that will become the primary database node. The designation of primary unified node is arbitrary. The deploying administrator can pick any unified node that they see fit.
    b. On each WebProxy and Unified node, *excluding the primary node*, run **cluster prepnode**.
3. Add nodes to the cluster.
    a. Log in to the selected primary Unified node.
    b. Add the Unified and WebProxy nodes to the cluster: **cluster add <ip_addr>**.

    Note that you do not have to add the selected primary node to the cluster. It will autmatically be added to the cluster.

    c. Verify the list of nodes in the cluster: **cluster list**.
4. Add the network domain (optional if a domain name is needed). From the selected primary Unified node:
    a. Configure the domain: **cluster run all network domain <domain_name>**.
    b. Verify the configured network domain: **cluster run all network domain**. Each node shows the domain that you configured.

5. Check the network:
   a. Verify the status of the cluster with: **cluster status**.
   b. Run **cluster check** on each node to verify network connectivity, disk status and NTP.
   c. Verify the DNS configuration: **cluster run all network dns**. Each node responds with the DNS server address.
6. (Optional) From the selected primary Unified node, run **cluster run notme system shutdown**. From the selected primary Unified node, run **system shutdown**.

   Take a snapshot of each node. Restart each node.
7. Configure the cluster.
   a. Provide a weight for each database server with the **database weight add <database_ip> <priority>** command.
      - Weights of 40, 30 are recommended for two Unified nodes
      - Weights of 40, 30, 20, and 10 are recommended for four Unified nodes
      - Weights of 60, 50, 40, 30, 20, and 10 are recommended for six Unified nodes

      The higher the value, the more priority.

      For Multinode Cluster deployment with four Unified Nodes in a geo-redundant system containing two data center infrastructures in two physical locations the following weights are used:
      - Specify a weight of 40 for the Primary node at the Primary site
      - Specify a weight of 30 for the Secondary node at the Primary site
      - Specify weights of 20 and 10 for the Secondary nodes at the DR site

      For Multinode Cluster deployment with six Unified Nodes in a geo-redundant system containing two data center infrastructures in two physical locations the following weights are used:
      - Specify a weight of 60 for the Primary node at the Primary site
      - Specify a weight of 50 for the Secondary node at the Primary site
      - Specify a weight of 40 for the Secondary node at the Primary site
      - Specify a weight of 30 for the Secondary node at the Primary site
      - Specify weights of 20 and 10 for the Secondary nodes at the DR site
   b. From the selected primary Unified node, now set it up as the primary Unified node. It is recommended that this step is run in a terminal opened with the **screen** command.
      i. Run **screen**.
      ii. Run **cluster provision primary <IP address of primary database node>**

      Allow approximately 2 hours for the operation to complete for two WebProxy and four Unified nodes.
   c. When provisioning is complete, check that each node is contactable and that the time server is running on each with **cluster check**.

      If a service is down, run **cluster run <node_ip> app start** to restart the service.

      If provisioning is successful, the screen session can be closed by typing **exit** in the screen terminal. If errors occurred, keep the screen terminal open for troubleshooting purposes and contact VOSS support.

d. (Optional) If required, set the web weights configurations (Active-Active, Active-Standby, Standalone). From the primary Unified node, run the required **web weight** commands for the Web Proxy nodes. For details, refer to *Multi Data Center Deployments* and the VOSS-4-UC Best Practices Guide.

e. (Optional) If required, enable or disable Self-service or admin web services on the web proxy nodes. This may for example be needed for security purposes.

The commands must be run on the relevant web proxy node. It is not recommended that the commands be run on a standalone system, but only on a cluster. The commands will automatically reconfigure and restart the nginx process, so some downtime will result. Request URLs to a disabled service will redirect the user to the active service.

- To disable or enable admin or Self-service web services on the web proxy node:

  web service disable <selfservice|admin>

  web service enable <selfservice|admin>

- To list web services on the web proxy node:

  web service list

8. (Optional) Shut down all the nodes gracefully, snapshot and restart:
   a. From the selected primary Unified node, run **cluster run notme system shutdown**.
   b. From the selected primary Unified node, run **system shutdown**.
   c. Take a VMWare snapshot of each node and then remove any previous snapshot.
   d. Restart each node.
9. Initialize the database and clear all data. On the primary Unified node, run **voss cleardown**.

   Note that this step may take some time. You can follow the process by running **log follow upgrade_db.log** or **log follow voss-deviceapi/app.log** in a separate console on the primary Unified node.
10. Import the templates.
    a. Copy the VOSS-4-UC template file to the primary Unified node with the command:

       scp <VOSS-4-UC_template_file> platform@<unified_node_ip_address>:~/media

    b. Log in to the primary Unified node and and install the template. It is recommended that this step is run in a terminal opened with the **screen** command.
       i. Run **screen**.
       ii. Run **app template media/<VOSS-4-UC_template_file>**
       - The console will display a message:

       ```
       Deploying the template-product for VOSS-4-UC <<RELEASE_VERSION>> ...
       ```

    c. When prompted to select the product deployment type, provide and confirm the deployment type:
       - `Enterprise`
       - `Provider without HCM-F`
       - `Provider with HCM-F`

       In accordance with the selected deployment type, you are prompted to enter and verify a top-level administrator password:

- `Enterprise : Please enter a password for "entadmin@sys.hcs"`
- `Provider : Please enter a password for "hcsadmin@sys.hcs"`

Upon installation, the password length should be at least 8 characters.

Deployment-specific artifacts are installed according to the selected type of product deployment. A message displays according to the selected deployment type - one of:

```
"Importing EnterpriseOverlay.json"

"Importing ProviderOverlay_Hcmf.json ..."

"Importing ProviderOverlay_Decoupled.json ..."
```

Deployment specific system artifacts are imported and a message is displayed:

```
Deployment-specific Overlay artifacts successfully imported.
```

i. Python functions are deployed

ii. System artifacts are imported.

iii. You are prompted to provide administrator passwords.

The template install automatically restarts necessary applications. If a cluster the installation propagates changes throughout the cluster.

11. Review the output from the **app template** commands and confirm that the install message appears:

```
Deployment summary of UPDATED template solution (i.e. current values after␣
↪installation):
--------------------------------------------------------------------------------
↪-------

Product: [PRODUCT]
Version: [UPDATED PRODUCT RELEASE]
Iteration-version: [UPDATED ITERATION]
Platform-version: [UPDATED PLATFORM VERSION]
```

You can also monitor the template installation from the GUI transaction list.

- If there are no errors indicated, we recommend that you make a snapshot:
  i. From the selected primary Unified node, run **cluster run notme system shutdown**.
  ii. From the selected primary Unified node, run **system shutdown**.
  iii. Take a VMWare snapshot of each node and then remove any previous snapshot.
  iv. Restart each node.
- If there was an error, the install script stops with a failure message listing the problem. Contact VOSS Support.

12. Check for needed security updates by running the **cluster run all security check** command on the primary node. If at least one update is required for any node, run the **cluster run all security update** command on the primary Unified node.

    After the security update is successful, reboot the cluster:

    a. From the selected primary Unified node, run **cluster run notme system reboot**. Since all services will be stopped, this takes some time.

b. From the selected primary Unified node, run **system reboot**. Since all services will be stopped, this takes some time.

If a node does not properly reboot but the console shows that all processes have terminated, you can manually reboot the node without any system corruption.

13. (Optional) Install language templates for languages other than English.
    a. Copy the language template file to the primary Unified node with the command:

       scp <language_template_file> platform@<unified_node_ip_address>:~/media

    b. Log in to the primary Unified node and install the template with the command:

       app template media/<language_template_file>

       For example, to install French:

       app template media/VOSS-4-UCLanguagePack_fr-fr.template

       There is no need to run this command on all nodes.
14. (Optional) If the VOSS-4-UC Phone Based Registration Add-on is required, follow the installation instructions in the Appendix of your Core Feature Guide:

    "Install the Phone Based Registration Web Service"

5.4. Standalone Installation

5.4.1. Before You Begin

Before continuing, you should have followed the OVA installation according to the steps and preliminary requirements specified in: *Create a New VM Using the Platform-Install OVA*

Note:

- Template installation and upgrade takes approximately two hours. You can follow the progress on the GUI transaction list.

The standard **screen** command should be used where indicated, and the *reconnect* parameter is available if needed:

- **screen** - start a new session
- **screen -ls** - show sessions already available
- **screen -r [screen PID]** - reconnect to a disconnected session

We recommend using the **screen** command to avoid failures if the connection is interrupted whilst running the command. If the connection is interrupted whilst running the command in `screen` then the session can be retrieved by first listing the sessions PID currently running in screen: **screen -ls**, and then reconnecting to the session using **screen -r [screen PID]**.

The version of **screen** used in VOSS-4-UC also supports the creation of a log file. If long-running commands will be run, the log file captures screen console output up to the session timeout. A message shows:

```
timed out waiting for input: auto-logout
```

To create a screen log file:

1. Run **screen** and wait for screen to open.
2. Press **<Ctrl>-a** then **:** (colon). This will enter screen command mode at the bottom of the console.
3. Create your screen logfile in the `media/` directory:
   a. In screen command mode, type **logfile media/<screen-logfilename>.log**
   b. Press **<Enter>**
   c. Press **<Ctrl>-a** and then **H** to start writing to the log file
   d. Run your commands.

If the **screen** session times out, you can obtain console output from the log file, for example:

$ sftp platform@<host>:media/<screen-logfilename>.log

5.4.2. Procedure

1. Install VMware tools:
   a. Log in to the node as the platform user and run the **app install vmware** command.
   b. Verify that vmware is running: **app list**.
2. Check that the time server is running with **app status services:time**.
3. Initialize the database and clear all data with the **voss cleardown** command.

   Note that this step may take some time. You can follow the process by running **log follow upgrade_db.log** or **log follow voss-deviceapi/app.log**.
4. Issue the **network domain <your_domain>** command.
5. Issue the **security check** command, followed by **security update**.
6. Issue the **system reboot** command. Since all services will be stopped, this takes some time.
7. Import the templates:
   a. Use **scp** to transfer the template files to the platform user's media directory server.

      scp <template_file> platform@<unified_node_ip_address>:~/media
   b. Install the VOSS-4-UC template. It is recommended that this step is run in a terminal opened with the **screen** command.
      i. Run **screen**.
      ii. Run **app template media/<VOSS-4-UC_template_file>**

      The following message appears:

      ```
      Deploying the template-product for VOSS-4-UC ....
      ```

      The template detects the deployment mode of the system as a New/Fresh installation.
   c. When prompted to select the product deployment type, provide and confirm the deployment type:
      - `Enterprise`
      - `Provider without HCM-F`
      - `Provider with HCM-F`

In accordance with the selected deployment type, you are prompted to enter and verify a top-level administrator password:

- `Enterprise : Please enter a password for "entadmin@sys.hcs"`
- `Provider : Please enter a password for "hcsadmin@sys.hcs"`

Upon installation, the password length should be at least 8 characters.

Deployment-specific artifacts are installed according to the selected type of product deployment. A message displays according to the selected deployment type - one of:

```
"Importing EnterpriseOverlay.json"

"Importing ProviderOverlay_Hcmf.json ..."

"Importing ProviderOverlay_Decoupled.json ..."
```

Deployment specific system artifacts are imported and a message is displayed:

```
Deployment-specific Overlay artifacts successfully imported.
```

i. Python functions are deployed

ii. System artifacts are imported.

iii. You are prompted to provide administrator passwords.

The template install automatically restarts necessary applications. If a cluster is detected, the installation propagates changes throughout the cluster.

8. Review the output from the app template commands and confirm that the install message appears:

```
Deployment summary of UPDATED template solution (i.e. current values after␣
↪installation):
--------------------------------------------------------------------------------
↪-------

Product: [PRODUCT]
Version: [UPDATED PRODUCT RELEASE]
Iteration-version: [UPDATED ITERATION]
Platform-version: [UPDATED PLATFORM VERSION]
```

- If there are no errors indicated, make a backup or snapshot.
- If there was an error, the install script has stopped with a failure message listing the problem. Resolve the problem and retry the installation.

9. Issue the **system reboot** command. Since all services will be stopped, this takes some time.
10. (Optional) Install language templates for languages other than English.
    a. Copy the language template file to the primary Unified node with the command:

    scp <language_template_file> platform@<unified_node_ip_address>:~/media

    b. Log in to the primary Unified node and install the template with the command:

    app template media/<language_template_file>

    For example, to install French:

    app template media/VOSS-4-UCLanguagePack_fr-fr.template

11. (Optional) If the VOSS-4-UC Phone Based Registration Add-on is required, follow the installation instructions in the Appendix of your Core Feature Guide:

    "Install the Phone Based Registration Web Service"

5.5. View Installation and Upgrade Transactions

Use this procedure to view transactions from a VOSS-4-UC installation or upgrade.

5.5.1. Procedure

1. Log in as sysadmin administrator.
2. Select **Administration Menu > Transactions**.
3. To view details on a transaction, click the transaction.

5.6. Installation Quick Reference

Note:

- These steps are described in depth in the VOSS-4-UC Install Guide.
- From VOSS-4-UC 18.1 or CUCDM 11.5.3 onwards, the standard **screen** command should be used where indicated, and the *reconnect* parameter is available if needed:
  - **screen** - start a new session
  - **screen -ls** - show sessions already available
  - **screen -r [screen PID]** - reconnect to a disconnected session

  VOSS recommends to use the **screen** command to avoid failures if the connection is interrupted whilst running the command. If the connection is interrupted whilst running the command in `screen` then the session can be retrieved by first listing the sessions PID currently running in screen: **screen -ls**, and then reconnecting to the session using **screen -r [screen PID]**.

5.6.1. General Steps

1. Download VOSS-4-UC install and patch media from:

   `sftp://secure.voss-solutions.com`
2. Review sizing requirements and define the deployment model:
   - Standalone (Lab Only)
   - MicroCluster (Two Unified nodes clustered)
   - Cluster (4 Unified Nodes and 2 Web Proxies)
   - DR Cluster (6 Unified Nodes and 2 Web Proxies)

3. Define VMHost space on VMWare servers
4. Deploy the VOSS-4-UC OVA to VMHost(s)
5. After the VM is created, select the CD ROM configuration and verify the **Connect at Power On** check box is enabled.
6. Power on the VM.
7. Configure the options in the installation wizard.
8. Install VMWare Tools from VOSS-4-UC CLI as platform user:

   command: **app install vmware**
9. Continue below to chosen deployment model.

5.6.2. Standalone Deployment

1. Connect to newly deployed servers CLI via SSH as the platform user.
2. Cleardown (initialize) the VOSS-4-UC database via SSH CLI:

   command: **voss cleardown**
3. (Optional) Set VOSS-4-UC Network Domain:

   command: **network domain <yourdomain>**
4. SFTP the install templates to the VOSS-4-UC server `media` directory
5. Install VOSS-4-UC Templates via VMWare Console CLI. From VOSS-4-UC 18.1 or CUCDM 11.5.3 onwards, VOSS recommends that this step is run in a terminal opened with the **screen** command, or on the VMWare console.
   a. Run **screen**.
   b. Run **app template media/<VOSS-4-UC_Template_Name>**.

   - A Deployment Type choice must be made during the template install execution. Choose one of:
     - Enterprise
     - Provider without HCM-F
     - Provider with HCM-F

     In accordance with the selected deployment type, you are prompted to enter and verify a top-level administrator password:
     - `Enterprise : Please enter a password for "entadmin@sys.hcs"`
     - `Provider : Please enter a password for "hcsadmin@sys.hcs"`

     Upon installation, the password length should be at least 8 characters.

5.6.3. Multi Node Deployment

All of the following commands will be run on the primary node via the SSH CLI until specified to use ESX Console CLI. The designation of primary unified node is arbitrary. The deploying administrator can pick any unified node that they see fit.

1. On each node that is not the designated primary unified node. prepare the servers for cluster command via the SSH CLI:

   command: **cluster prepnode**

2. Add all of the other nodes to the cluster:

   command: **cluster add <non-primary-node_ip-address>**

   Repeat this command for each other node - binding each individual node IP Address to the cluster. This command does not need to be run for the primary unified node.

3. Verify all nodes are members of the cluster:

   command: **cluster list**

4. (Optional) Set VOSS-4-UC Network Domain:

   command: **cluster run all network domain <yourdomain>**

5. Set each unified node's database weight:

   command: **database weight <un-node_ip-address> <priority_weight>**

   - This command must be run for all unified nodes primary and secondary.
   - Priority weights of 40, 30 are recommended for *two* Unified nodes.
   - Priority weights of 40, 30, 20, and 10 are recommended for *four* Unified nodes
   - Priority weights of 60, 50, 40, 30, 20, and 10 are recommended for *six* Unified nodes.

6. Provision the VOSS-4-UC cluster database. From VOSS-4-UC 18.1 or CUCDM 11.5.3 onwards, VOSS recommends that this step is run in a terminal opened with the **screen** command, or on the VMWare console.

   a. Run **screen**.

   b. command: **cluster provision primary <ip_address_of_primary_database_node>**.

7. Check cluster application status:

   command: **cluster status**

   - Should any services be in a down state, restart all services on that affected node:

     command: **cluster run <node_ip> app start**

8. Run the command: **voss cleardown**.

9. SFTP the install templates to the VOSS-4-UC server `media` directory of the primary unified node.

10. Install VOSS-4-UC Templates via VMWare Console CLI of primary unified node. From VOSS-4-UC 18.1 or CUCDM 11.5.3 onwards, VOSS recommends that this step is run in a terminal opened with the **screen** command, or on the VMWare console.

    a. Run **screen**.

    b. Run **app template media/<VOSS-4-UC_Template_Name>**

11. A Deployment Type choice must be made during the template install execution. Choose one of:

    - Enterprise
    - Provider without HCM-F
    - Provider with HCM-F

In accordance with the selected deployment type, you are prompted to enter and verify a top-level administrator password:

- `Enterprise : Please enter a password for "entadmin@sys.hcs"`
- `Provider : Please enter a password for "hcsadmin@sys.hcs"`

Upon installation, the password length should be at least 8 characters.

5.6.4. Post Deployment

1. Access the VOSS-4-UC web interface via any web browser:

   `https://<ip_address_or_dns_name_of_VOSS-4-UC_PrimaryUN_or_WebProxy>`

2. Run the following security commands:
   - **security check**
   - **security update**.

5.7. Migrating from a 6 Node to 8 Node System

To migrate a clustered 6 node system (4 unified nodes and 2 WebProxy nodes) to a clustered 8 node system (6 unified nodes and 2 WebProxy nodes), the considerations and steps below are required.

1. Check and snapshot the clustered 6 node system *before* adding the nodes:
   a. Run **cluster list** to ensure the node count is correct.
   b. Run **cluster status** to check all nodes are online and services reported as running.
   c. Run **cluster run database cluster list** to make sure all unified nodes are aware of the current cluster nodes.
   d. Run **cluster run all app status** to make sure all services are running on all nodes.
   e. Snapshot the entire 6 node cluster
2. Add the 2 unified nodes:
   a. Create the new unified node - see: *Create a New VM Using the Platform-Install OVA*.
   b. An extra functions file (`extra_functions.py`) that is installed on the existing cluster needs to be re-installed *on each added unified node*. Request the `deploy_extra_functions_<version>.template` file from VOSS Level 2 support and run the command **app template deploy_extra_functions_<version>.template**.
   c. Run **cluster prepnode** *on all nodes*, including new nodes.
   d. From the primary unified node, run **cluster add <ip>** for new nodes, excluding itself.
3. Reset the cluster database weights. When nodes are removed from and added to a cluster, remove all database weights completely and add them back in *before provisioning* to reset the configuration.
   a. Delete all database weights in the cluster. For each IP, run **database weight del <IP>**.
   b. To add database weights in, you set the weight of the intended primary, but must always specify the current primary (using **database primary**), regardless of whether the new intended primary is

the same node or not. During the provision process, the role of primary will then be transferred from the existing primary to the node with the highest weight.

Determine the current primary database node with **database primary**.

4. Run the command **database weight add <IP> <numeric>** on the primary database node for each IP, making the value of the intended primary database node the highest value.
5. Check the cluster before provisioning:
   a. Run **cluster list** to ensure the node count is correct.
   b. Run **cluster status** to check all nodes are online and services reported as running.
   c. Run **cluster run database cluster list** to make sure all unified nodes are aware of the current cluster nodes.
   d. Run **cluster run all app status** to make sure all services are running on all nodes. Fresh nodes that have not been provisioned will show a message: `suspended waiting for mongo`.
6. Run **cluster provision primary <primary IP>** to provision the cluster.
7. After a successful migration, the snapshot made in step 1. can be removed.

5.8. Installation Logs

To troubleshoot an installation, log files can be inspected. For example, detailed platform commands show in the `execute.log` file. Here, log entries for the command execution have a `ui` column. Log entries that follow these show related commands.

To only see the commands in `execute.log` example, you can open a new console and run:

log follow execute.log | grep " ui "

Note: Logs are rotated and install commands may not show after log rotation.

The list below shows examples of installation commands and corresponding `ui` and following entries in `execute.log`.

- **app install vmware**.

  `execute.log`:

```
<timestmp><user><execnum>: ui - /opt/platform/bin/scripts.py install 'vmware'
```

- **app list**.

  `execute.log`:

```
<timestmp><user><execnum>: ui - /opt/platform/bin/execute get /scripts/
<timestmp><user><execnum>: run: /opt/platform/bin/execute get /scripts/
<timestmp><user><execnum>: run: /opt/platform/bin/scripts.py list
```

- **database config**

  `execute.log`:

```
<timestmp><user><execnum>: ui - /opt/platform/apps/mongodb/bin/database_
↪helper.py config
<timestmp><user><execnum>: run: /opt/platform/apps/mongodb/bin/database_
↪helper.py config
<timestmp><user><execnum>: run: /opt/platform/apps/mongodb/bin/database_
↪helper.py config returned 0
```

- **cluster list**.

  execute.log:

```
<timestmp><user><execnum>: ui - /opt/platform/bin/execute get /apps/cluster/
↪engine/list
<timestmp><user><execnum>: run: /opt/platform/bin/execute get /apps/cluster/
↪engine/list
<timestmp><user><execnum>: run: /opt/platform/bin/execute --app=cluster   get /
↪list
<timestmp><user><execnum>: run: /opt/platform/apps/cluster/cluster.py list
<timestmp><user><execnum>: run: /opt/platform/apps/cluster/cluster.py list␣
↪returned 0
```

- **cluster status**.

  execute.log:

```
<timestmp><user><execnum>: ui - /opt/platform/bin/execute get /apps/
↪cluster/engine/status
<timestmp><user><execnum>: run: /opt/platform/bin/execute get /apps/
↪cluster/engine/status
<timestmp><user><execnum>: run: /opt/platform/bin/execute --app=cluster  ␣
↪get /status
<timestmp><user><execnum>: run: /opt/platform/apps/cluster/cluster.py␣
↪status
```

- **web service list**

  execute.log:

```
<timestmp><user><execnum>: ui - /opt/platform/bin/execute get /apps/nginx/
↪engine/disable
<timestmp><user><execnum>: run: /opt/platform/bin/execute get /apps/nginx/
↪engine/disable
<timestmp><user><execnum>: run: /opt/platform/bin/execute --app=nginx  ␣
↪get /disable
<timestmp><user><execnum>: run: /opt/platform/bin/config.py get --
↪app=nginx disable
<timestmp><user><execnum>: run: /opt/platform/bin/config.py get --
↪app=nginx disable returned 0
```

- **log follow upgrade_db.log**

  execute.log:

```
<timestmp><user><execnum>: ui - /opt/platform/bin/execute post /apps/services/
↪process/log/engine/log/follow '{"follow":"upgrade_db.log"}'
<timestmp><user><execnum>: run: /opt/platform/bin/execute post /apps/services/
↪process/log/engine/log/follow '{"follow":"upgrade_db.log"}' --method=os.system
<timestmp><user><execnum>: run: /opt/platform/bin/execute --app=services:log  ␣
↪post /log/follow '{"follow":"upgrade_db.log"}' --method=os.system
```

(continues on next page)

(continued from previous page)

```
<timestmp><user><execnum>: run: /opt/platform/apps/services/logviewer.sh follow␣
↪upgrade_db.log
```

- **app template media/<VOSS-4-UC_template_file>**

  execute.log:

```
<timestmp><user><execnum> ui - /opt/platform/apps/template_runner/template media/
↪install.template platform
[...]
<timestmp><user><execnum> ui - /opt/platform/bin/execute --app=template_runner␣
↪post /methods/import
    '{"filename":"DummyTestImport.json","import":"DummyTestImport.json"}'


Please enter a password for ...

<timestmp><user><execnum>  ui - /usr/bin/docker exec -it voss-wsgi /opt/voss-
↪deviceapi/bin/python
   /opt/voss-deviceapi/src/deviceapi/utils/get_user_password.py set_details␣
↪sysadmin@sys

[...]

<timestmp><user><execnum>: ui - /opt/platform/bin/execute --app=template_runner␣
↪post /methods/import
'{"filename":"UpgradeChecks.json","import":"UpgradeChecks.json -p sys"}'

[...]

'{"filename":"EndToEnd.application.json","import":"EndToEnd.application.json -p␣
↪sys"}'
'{"filename":"SYS.json","import":"SYS.json -p sys"}'
'{"filename":"SYSnoPKG.json","import":"SYSnoPKG.json -p sys"}'
'{"filename":"SYSdotHCS_with_hcmf.json","import":"SYSdotHCS_with_hcmf.json -p sys.
↪hcs"}'

[...]
```

Index