Installation and Configuration

Horizon Cloud with On-Premises Infrastructure 1.3
VMware Horizon Cloud Service

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.
You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com
## Contents

About Horizon Cloud with On-Premises Infrastructure Installation and Configuration  

1 Overview of a Horizon Cloud with On-Premises Infrastructure Installation 7  

2 Install Horizon Cloud with On-Premises Infrastructure on a vSAN Ready Node Cluster  
   Build the vSAN Ready Node Cluster 11  
   Deploy Horizon Air Link Into Your vSAN Ready Node Cluster 28  

3 Expanding the Existing vSAN Ready Node Cluster with Additional Nodes 35  
   Add vSAN Ready Nodes to Expand Capacity of an Existing vSAN Ready Node Cluster 35  
   Edit the Existing vSphere Cluster 37  
   Modify the HA Cluster Admission Criteria 37  

4 Installing Horizon Cloud with On-Premises Infrastructure on Dell EMC VxRail  
   Install Virtualization and Storage on Dell EMC VxRail 39  
   Deploy Horizon Air Link Into Your Dell EMC VxRail 39  

5 Configure One or More Horizon Cloud Nodes 41  

6 Configure the Environment for End-User Data, Settings, and Profile Persistence 45  

7 vSAN Ready Node Cluster Appendixes 47  
   Appendix A - Static IP Addresses and Host Names for vSAN Ready Node Cluster Setup 47  
   Appendix B - Active Directory Details for vSAN Ready Node Cluster Setup 50  

Index 51
About
Horizon Cloud with On-Premises Infrastructure
Installation and Configuration

This Horizon Cloud with On-Premises Infrastructure Installation and Configuration document describes the process of installing and configuring a Horizon Cloud with On-Premises Infrastructure environment.

This information serves as an example of a basic cluster configured using supported hyper-converged infrastructure hardware for use with VMware Horizon Cloud Service to create a Horizon Cloud with On-Premises Infrastructure environment. Discussions of the VMware vSAN software product are limited to this context. For more information about vSAN and related topics, see the Virtual SAN documentation page.

For information about how to use the product after you finish all the tasks outlined in this guide, see the Horizon Cloud with On-Premises Infrastructure Administration document.

Intended Audience

The information in this document is intended for experienced data center administrators with knowledge of VMware ESXi, VMware vSphere, and networking.

Also, you might find having a familiarity with VMware vCenter Server Appliance helpful.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, visit http://www.vmware.com/support/pubs.

Contacting VMware Support

Contact VMware Support when you need help with your Horizon Cloud with On-Premises Infrastructure environment.

- You can submit a support request to VMware Support online using your My VMware account or by phone.
- KB 2144012 Customer Support Guidelines provides details for getting support depending on the issue encountered.
- After you have configured your Horizon Cloud Node, you can submit a support request by logging in to the Administration Console and clicking > Support.
Overview of a Horizon Cloud with On-Premises Infrastructure Installation

Horizon Cloud with On-Premises Infrastructure is supported on specific hyper-converged infrastructure hardware.

The following hardware environments are supported.

<table>
<thead>
<tr>
<th>Hyper-Converged Infrastructure</th>
<th>Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>vSAN Ready Node</td>
<td>A minimum of four servers and two 10GBASE uplinks per server are required for a production deployment. Check with your vendor to determine models recommended for Horizon Cloud with On-Premises Infrastructure.</td>
</tr>
<tr>
<td>Dell EMC VxRail</td>
<td>A minimum of one hardware appliance containing four servers where each server has two 10GBASE uplinks is required.</td>
</tr>
</tbody>
</table>

Installation and configuration of Horizon Cloud with On-Premises Infrastructure involves the following steps.

- Install and configure vSphere and vSAN on supported hyper-converged infrastructure hardware.
  - For vSAN Ready Node, follow the steps in Chapter 2, “Install Horizon Cloud with On-Premises Infrastructure on a vSAN Ready Node Cluster,” on page 11.
  - For VxRail, follow the steps in Chapter 4, “Installing Horizon Cloud with On-Premises Infrastructure on Dell EMC VxRail,” on page 39.

- Deploy the Horizon Air Link virtual appliance to initiate a Horizon Cloud Node installation.
  - For vSAN Ready Node, follow the steps in “Deploy Horizon Air Link Into Your vSAN Ready Node Cluster,” on page 28.
  - For VxRail, follow the steps in “Deploy Horizon Air Link Into Your Dell EMC VxRail,” on page 39.

- Configure your Horizon Cloud Nodes by following the steps in Chapter 5, “Configure One or More Horizon Cloud Nodes,” on page 41.

- Configure the environment for persistence of end user data, settings, and profiles by following the steps in Chapter 6, “Configure the Environment for End-User Data, Settings, and Profile Persistence,” on page 45.

Networking Requirements

The following information about networks, addresses, host names, device names, and other items provides a consistent example for a vSAN Ready Node cluster. Use this information as both a guide for building this specific configuration and also as a reference or a blueprint when building clusters of increased size or resources.
See “Appendix A - Static IP Addresses and Host Names for vSAN Ready Node Cluster Setup,” on page 47 for a full list of static IP addresses, host names, and DNS domains used throughout the Horizon Cloud with On-Premises Infrastructure installation instructions.

When using a vSAN Ready Node cluster for your Horizon Cloud with On-Premises Infrastructure environment, ensure that cluster meets the following networking requirements.

**Switch Configuration**

- Two 10GBASE switch ports are required per vSAN Ready Node. The steps in this guide reflect this minimum requirement. Additional 10GBASE connections can be used as desired to complement cluster performance and redundancy.
- All switch ports used for the vSAN Ready Node cluster must have LACP disabled.
- All switch ports used for the vSAN Ready Node cluster must provide access to the VLANs listed in the table that follows.

**VLANs**

The following table of VLAN IDs, prefix lengths, and routers provides a consistent reference example that applies throughout this guide. You are not required to use the numbering scheme verbatim, only to provide a functionally equivalent configuration tailored to the site.

<table>
<thead>
<tr>
<th>VLAN</th>
<th>TYPE</th>
<th>PREFIX</th>
<th>ROUTER</th>
<th>USE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1000</td>
<td>routed</td>
<td>/24</td>
<td>172.16.0.1</td>
<td>Management network for the vSphere and Horizon Cloud with On-Premises Infrastructure infrastructure</td>
</tr>
<tr>
<td>1001</td>
<td>routed</td>
<td>/24</td>
<td>172.16.1.1</td>
<td>Desktop network used by the Horizon Cloud with On-Premises Infrastructure tenant software components and desktop virtual machines</td>
</tr>
<tr>
<td>4001</td>
<td>private</td>
<td>/24</td>
<td>none</td>
<td>vSAN The VLAN used for vSAN traffic requires IGMP snooping and IGMP querier enabled.</td>
</tr>
<tr>
<td>4002</td>
<td>private</td>
<td>/24</td>
<td>none</td>
<td>vSphere vMotion</td>
</tr>
</tbody>
</table>

**DNS**

- All systems on routed networks must use the FQDNs used during vSAN Ready Node cluster and Horizon Cloud with On-Premises Infrastructure configuration. Ensure that all host names resolve with forward and reverse lookups before proceeding.
- The appliances deployed for the Horizon Cloud with On-Premises Infrastructure environment, such as the Horizon Air Link, must be able to resolve external host names, such as cloud.horizon.vmware.com, to contact the cloud service environment, Horizon Cloud.

**NTP**

All vSphere and Horizon Cloud with On-Premises Infrastructure systems require time synchronization over NTP. An accurate time source must be present and reachable by all systems.

**Note** In the example commands documented here for configuring a vSAN Ready Node cluster, IP address 172.16.1.3 (host name vrndc1) is used as the address for the DNS and NTP server settings for the ESXi hosts in the cluster. When a Horizon Cloud with On-Premises Infrastructure environment is deployed in the cluster, the deployment relies on having an Active Directory Domain Controller that meets configuration requirements that correspond to the configured DNS and NTP server settings, as outlined in “Appendix B - Active Directory Details for vSAN Ready Node Cluster Setup,” on page 50. When you deploy the Horizon Cloud with On-Premises Infrastructure environment, ensure the Active Directory Domain Controller requirements are met.
Transparent Page Sharing

During deployment, Horizon Cloud with On-Premises Infrastructure enables the Transparent Page Sharing (TPS) configuration option in ESXi.

Deploying Horizon Cloud with On-Premises Infrastructure automatically changes the TPS configuration option in ESXi from the default setting of disabled to enabled. TPS is enabled to improve memory sharing between virtual machines, which increases the density of desktops per host. If you disable TPS, you might need to decrease the number of desktops you provision to the cluster to prevent a decrease in performance.

The Horizon Cloud with On-Premises Infrastructure capacity algorithms function with the assumption that TPS is enabled. If you disable TPS but deploy the full number of desktops recommended for provisioning, the host RAM might become overcommitted, resulting in poor desktop performance. Although RAM is often the limiting factor in virtual desktop infrastructure use cases, other factors, such as CPU and disk space, might limit the recommended desktop capacity. In such cases, disabling TPS might not impact the overall capacity of the node.

Therefore, you can disable TPS if necessary. See KB 2146823. However, Horizon Cloud with On-Premises Infrastructure performs best when TPS is enabled.
To install Horizon Cloud with On-Premises Infrastructure on a vSAN Ready Node cluster, you first build the vSAN Ready Node cluster itself and then you deploy the Horizon Air Link appliance into the cluster.

**IMPORTANT** Horizon Cloud with On-Premises Infrastructure is not supported for use in a vCenter Server environment that has more than one virtual data center configured in it. That data center is the vSAN Ready cluster. When you set up Horizon Cloud with On-Premises Infrastructure in the vCenter Server environment, ensure that the environment contains only one data center before deploying the Horizon Air Link into the environment.

**Procedure**

1. **Build the vSAN Ready Node Cluster** on page 11
   
   Building a vSAN Ready Node cluster involves installing ESXi on each server, followed by configuring initial networking on the resulting ESXi hosts and configuring them as a vSAN cluster.

2. **Deploy Horizon Air Link Into Your vSAN Ready Node Cluster** on page 28
   
   When using vSAN Ready Node cluster as the hyper-converged infrastructure for Horizon Cloud with On-Premises Infrastructure, use the vSAN Ready Node cluster vCenter to deploy the Horizon Air Link appliance OVA. After the appliance is deployed and powered on, you use it to connect with the VMware hosted service, Horizon Cloud, and begin the Horizon Cloud Node configuration process.

**Build the vSAN Ready Node Cluster**

Building a vSAN Ready Node cluster involves installing ESXi on each server, followed by configuring initial networking on the resulting ESXi hosts and configuring them as a vSAN cluster.

**Procedure**

1. **Install VMware ESXi on Each Server** on page 12
   
   For each server that you are configuring for this vSAN Ready Node environment, install ESXi and perform its initial configuration. A minimum of four servers is required to meet the requirements for the vSAN cluster capabilities.

2. **Configure Initial Networking on ESXi Hosts** on page 12
   
   Configure the initial networking on ESXi hosts to prepare for the vSAN Ready Node cluster.

3. **Configure vSAN to Work with Horizon Cloud with On-Premises Infrastructure** on page 15
   
   Configuring vSAN to function with Horizon Cloud with On-Premises Infrastructure is a multi-step process. These steps must be performed in sequence.
Install VMware ESXi on Each Server

For each server that you are configuring for this vSAN Ready Node environment, install ESXi and perform its initial configuration. A minimum of four servers is required to meet the requirements for the vSAN cluster capabilities.

Procedure

1. Use the appropriate vendor-specific custom ESXi installer ISO to boot the ESXi installer ISO on the first server (esxi-01 in the example configuration) and use the defaults until you are asked to select the target device.
2. Select the storage device to use and select **Install ESXi, overwrite VMFS datastore**.
   This device is often an embedded SD card, USB storage, or other vendor-specific device type.
3. Use the defaults for the remaining questions and, when the installer finishes, reboot the system.
4. Repeat the steps on the other servers.

Configure Initial Networking on ESXi Hosts

Configure the initial networking on ESXi hosts to prepare for the vSAN Ready Node cluster.

Procedure

1. At the ESXi console, press F2, log in as root and enable the ESXi shell and SSH access under **Troubleshooting Options**.
2. Exit the ESXi console and log in as root to the ESXi shell (ALT-F1).
3. Determine the name of the two 10 GBASE NICs to use by checking the link status with ESXCLI.
   The following ESXCLI command output is condensed.
   ```bash
   [root@localhost:~] esxcli network nic list
   Name   PCI Device   Driver Admin Status Link Status Speed Duplex MAC Address
   ------ ------------ ------ ------------ ----------- ----- ------ ----------------
   vmnic4 0000:03:00.0 ixgbe  Up           Up          10000 Full   a0:36:9f:73:00:f8
   vmnic5 0000:03:00.1 ixgbe  Up           Up          10000 Full   a0:36:9f:73:00:fa
   ```
4. Determine the uplink on vSwitch0, and, if necessary, replace the current uplink on vSwitch0 with an active vmnic.
   ```bash
   [root@localhost:~] esxcli network vswitch standard list | grep Uplinks
   Uplinks: vmnic0
   [root@localhost:~] esxcli network vswitch standard uplink add --uplink-name=vmnic4 --vswitch-name=vSwitch0
   [root@localhost:~] esxcli network vswitch standard uplink remove --uplink-name=vmnic0 --vswitch-name=vSwitch0
   [root@localhost:~] esxcli network vswitch standard list | grep Uplinks
   Uplinks: vmnic4
   ```
5 Set vmk0 to use the static IP address for esxi-01 and set the default VMkernel gateway.

[root@localhost:~] esxcli network ip interface ipv4 set --interface-name=vmk0 --ipv4=172.16.0.11 --netmask=255.255.255.0 --type=static

[root@localhost:~] esxcli network ip interface ipv4 get

<table>
<thead>
<tr>
<th>Name</th>
<th>IPv4 Address</th>
<th>IPv4 Netmask</th>
<th>IPv4 Broadcast</th>
<th>Address Type</th>
<th>DHCP</th>
<th>DNS</th>
</tr>
</thead>
<tbody>
<tr>
<td>vmk0</td>
<td>172.16.0.11</td>
<td>255.255.255.0</td>
<td>172.16.0.255</td>
<td>STATIC</td>
<td>false</td>
<td></td>
</tr>
</tbody>
</table>

[root@localhost:~] esxcli network ip route ipv4 add --gateway=172.16.0.1 --network=default

[root@localhost:~] esxcli network ip route ipv4 list

<table>
<thead>
<tr>
<th>Network</th>
<th>Netmask</th>
<th>Gateway</th>
<th>Interface</th>
<th>Source</th>
</tr>
</thead>
<tbody>
<tr>
<td>default</td>
<td>0.0.0.0</td>
<td>172.16.0.1</td>
<td>vmk0</td>
<td>MANUAL</td>
</tr>
<tr>
<td>172.16.0.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>vmk0</td>
<td>MANUAL</td>
</tr>
</tbody>
</table>

6 Set the VLAN ID on the Management Network and VM Network port groups.

[root@localhost:~] esxcli network vswitch standard portgroup set --portgroup-name="Management Network" --vlan-id=1000

[root@localhost:~] esxcli network vswitch standard portgroup set --portgroup-name="VM Network" --vlan-id=1000

[root@localhost:~] esxcli network vswitch standard portgroup list

<table>
<thead>
<tr>
<th>Name</th>
<th>Virtual Switch</th>
<th>Active Clients</th>
<th>VLAN ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Management Network</td>
<td>vSwitch0</td>
<td>1</td>
<td>1000</td>
</tr>
<tr>
<td>VM Network</td>
<td>vSwitch0</td>
<td>0</td>
<td>1000</td>
</tr>
</tbody>
</table>

7 Connect to the host remotely with SSH and log in as root.

8 Set the hostname and domain name of the system and configure DNS.

[root@localhost:~] esxcli system hostname set --host=esxi-01 --domain=vrn.local

[root@esxi-01:~] esxcli system hostname get

Domain Name: vrn.local

Fully Qualified Domain Name: esxi-01.vrn.local

Host Name: esxi-01

[root@esxi-01:~] esxcli network ip dns server add --server=172.16.1.3

[root@esxi-01:~] esxcli network ip dns server list

DNS Servers: 172.16.1.3

[root@esxi-01:~] esxcli network ip dns search add --domain=vrn.local

[root@esxi-01:~] esxcli network ip dns search list

DNSSearch Domains: vrn.local
9 Configure and enable the NTP daemon, allow it a moment to start, and verify synchronization.

```
[root@esxi-01:] echo "server 172.16.1.3" >> /etc/ntp.conf
[root@esxi-01:] cat /etc/ntp.conf
restrict 127.0.0.1
restrict default kod nomodify notrap
driftfile /etc/ntp.drift
server 172.16.1.3
```

```
[root@esxi-01:] esxcli network firewall ruleset set --ruleset-id=ntpClient --enabled=true
[root@esxi-01:] chkconfig ntpd on
[root@esxi-01:] /etc/init.d/ntpd start
Starting ntpd
```

```
[root@esxi-01:] ntpq -p
```

```
remote  refid               st t when poll reach   delay   offset  jitter
==============================================================================
*vrn-dc1.vrn 172.16.100.100       4 u   18   64    3    2.425    0.089   7.999
```

10 Increase the number of hosts allowed in the vSAN cluster to a maximum of 64.

```
[root@esxi-01:] esxcli system settings advanced set --option=/VSAN/goto11 --int-value=1
[root@esxi-01:] esxcli system settings advanced list --option=/VSAN/goto11
```

Path: /VSAN/goto11
Type: integer
Int Value: 1
Default Int Value: 0
Min Value: 0
Max Value: 1
String Value:
Default String Value:
Valid Characters:
Description: Allow VSAN clusters to grow up to 64 nodes. (requires reboot)

11 Set TCP/IP heap size to 1024 MiB.

```
[root@esxi-01:] esxcli system settings advanced set --option=/Net/TcpipHeapMax --int-value=1024
[root@esxi-01:] esxcli system settings advanced list --option=/Net/TcpipHeapMax
```

Path: /Net/TcpipHeapMax
Type: integer
Int Value: 1024
Default Int Value: 512
Min Value: 32
Max Value: 1536
String Value:
Default String Value:
Valid Characters:
Description: Max megabytes the tcpip module heap can grow to. (REQUIRES REBOOT!)
12 Verify that CBRC cache size is 2048 MiB.

```
[root@esxi-01:] esxcli system settings advanced list --option=/CBRC/DCacheSize
```

Path: /CBRC/DCacheSize
Type: integer
Int Value: 2048
Default Int Value: 2048
Min Value: 2048
Max Value: 2048
String Value:
Default String Value:
Valid Characters:
Description: Size of CBRC Data Cache in MB. This cannot be changed if CBRC.Enable is set to 1.

13 Set CBRC cache mem reserved to 1024 MiB.

```
[root@esxi-01:] esxcli system settings advanced set --option=/CBRC/DCacheMemReserved --int-value=1024
```

```
[root@esxi-01:] esxcli system settings advanced list --option=/CBRC/DCacheMemReserved
```

Path: /CBRC/DCacheMemReserved
Type: integer
Int Value: 1024
Default Int Value: 400
Min Value: 100
Max Value: 2048
String Value:
Default String Value:
Valid Characters:
Description: Memory consumed by CBRC Data Cache (in MB)

14 If the SAS HBA of the system has a driver requirement, firmware requirement, or both for vSAN use, perform the updates according to the manufacturer’s documentation.

15 Enter maintenance mode, reboot the system, log in as root over SSH, and exit maintenance mode.

```
[root@esxi-01:] esxcli system maintenanceMode set --enable true
```

```
[root@esxi-01:] esxcli system shutdown reboot --reason=reasons
```

```
...
```

```
[root@esxi-01:] esxcli system maintenanceMode set --enable false
```

Configure vSAN to Work with Horizon Cloud with On-Premises Infrastructure

Configuring vSAN to function with Horizon Cloud with On-Premises Infrastructure is a multi-step process. These steps must be performed in sequence.

Procedure

1 Prepare Disks on page 16
   Ensure that all disks in the system intended for vSAN use are tagged as local.

2 Create vSAN Cluster on Node 1 on page 17
   Create and configure vSAN cluster on node 1.
3 **Install the vCenter Server Appliance on the ESXi Host (Node 1)** on page 18
   You install and configure the vCenter Server Appliance on the prepared ESXi host to create a virtual datacenter and vSphere cluster into which you can deploy the on-premises components. The vCenter Server Appliance installation is configured to use an embedded Platform Services Controller.

4 **Create a Virtual Data Center and Add a Distributed Virtual Switch and Distributed Port Groups** on page 23
   In the vCenter Server environment, you must create a virtual data center and create a distributed virtual switch and distributed port groups for that data center.

5 **Create the vSphere Cluster** on page 26
   To establish failover protection, create a vSphere Cluster.

### Prepare Disks
Ensure that all disks in the system intended for vSAN use are tagged as local.

**Note**: This procedure shows a system where only the vSAN disks are listed. Filter out extraneous devices, such as internal SD cards or a separate boot disk, as needed.

#### Procedure
1. Make note of a disk device that is marked as a boot volume so that the device can be avoided in subsequent steps.
   The command might not produce output.
   ```bash
   [root@esxi-01:~] esxcli --formatter=csv --format-param=fields="Devfs Path,Is Boot Device,Size" storage core device list | grep true
   /vmfs/devices/disks/naa.5000c500894625f3,true,286102,
   ```

2. Check for disk devices that are not tagged as local, making sure to remove boot volumes from the list that were identified in Step 1.
   ```bash
   [root@esxi-01:~] esxcli --formatter=csv --format-param=fields="Devfs Path,Is Local,Size" storage core device list | grep false | grep -v naa.5000c500894625f3
   /vmfs/devices/disks/naa.5000c5008f366e43,false,1144641,
   /vmfs/devices/disks/naa.5000c5008f3581f3,false,1144641,
   /vmfs/devices/disks/naa.5000c5008f35e103,false,1144641,
   /vmfs/devices/disks/naa.5000c5008f355c33,false,1144641,
   /vmfs/devices/disks/naa.5000c5008f353f7b,false,1144641,
   ```

3. Manually mark each device, one at a time, to set the value of the Is Local parameter to true.
   ```bash
   [root@esxi-01:~] esxcli storage nmp satp rule add --s VMW_SATP_LOCAL --option "enable_local" -d naa.5000c5008f366e43
   [root@esxi-01:~] esxcli storage core claiming unclaim --type device --device naa.5000c5008f366e43
   [root@esxi-01:~] esxcli storage core claimrule load
   [root@esxi-01:~] esxcli storage core claimrule run
   ```
4 Verify that the disk devices are all tagged as local, again avoiding any boot volumes that were identified.

```
[root@esxi-01:~] esxcli --formatter=csv --format-param=fields= "Devfs Path,Is Local,Size"
storage core device list | grep disks | grep false | grep -v naa.5000c500894625f3
```

**Create vSAN Cluster on Node 1**

Create and configure vSAN cluster on node 1.

**Procedure**

1 On Node 1, change the default vSAN storage policy.

```
[root@esxi-01:~] esxcli vsan policy setdefault -c vdisk -p "(("hostFailuresToTolerate" i1) ("forceProvisioning" i1))"
[root@esxi-01:~] esxcli vsan policy setdefault -c vmnamespace -p "(("hostFailuresToTolerate" i1) ("forceProvisioning" i1))"
```

2 On Node 1, use the system UUID to create the vSAN cluster.

```
[root@esxi-01:~] esxcli system uuid get
56a831ee-5a07-640f-b18e-a0369f730418
[root@esxi-01:~] esxcli vsan cluster join -u 56a831ee-5a07-640f-b18e-a0369f730418
```

3 On Node 1, verify that the vSAN cluster Local Node Type value is NORMAL, the Local Node State value is MASTER, and the Local Node Health State value is HEALTHY.

```
[root@esxi-01:~] esxcli vsan cluster get
Cluster Information
   Enabled: true
   Current Local Time: 2016-01-28T04:37:00Z
   Local Node UUID: 56a831ee-5a07-640f-b18e-a0369f730418
   Local Node Type: NORMAL
   Local Node State: MASTER
   Local Node Health State: HEALTHY
   Sub-Cluster Master UUID: 56a831ee-5a07-640f-b18e-a0369f730418
   Sub-Cluster Backup UUID:
   Sub-Cluster UUID: 56a831ee-5a07-640f-b18e-a0369f730418
   Sub-Cluster Membership Entry Revision: 0
   Sub-Cluster Member Count: 1
   Sub-Cluster Member UUIDs: 56a831ee-5a07-640f-b18e-a0369f730418
   Sub-Cluster Membership UUID: 299aa956-642c-3eb6-bff0-a0369f730418
```
4 On Node 1, assemble the vSAN disk groups.

**Note** The example vSAN Ready Node systems contain the minimum allowable configuration of three hard disk drives and one solid-state drive per disk group.

a List the solid-state drive (SSD) devices in the system and take note of one device name for the first disk group.

```
[root@esxi-01:/~] esxcli --formatter=csv --format-param=fields="Devfs Path,Is SSD,Size" storage
core device list | grep "disks/naa" | grep true
/vmfs/devices/disks/naa.5001e820028799a0,true,381554,
/vmfs/devices/disks/naa.5001e82002879c68,true,381554,
```

b List the hard disk drive (HDD) devices in the system, ensuring that the boot volume is not in the list, and take note of three device names for the first disk group.

```
[root@esxi-01:/~] esxcli --formatter=csv --format-param=fields="Devfs Path,Is SSD,Size" storage
core device list | grep "disks/naa" | grep false | grep -v naa.5000c5008f366e43
/vmfs/devices/disks/naa.5000c5008f366e43,false,1144641,
/vmfs/devices/disks/naa.5000c5008f3581f3,false,1144641,
/vmfs/devices/disks/naa.5000c5008f35a103,false,1144641,
/vmfs/devices/disks/naa.5000c5008f3e367,false,1144641,
/vmfs/devices/disks/naa.5000c5008f355c33,false,1144641,
/vmfs/devices/disks/naa.5000c5008f353f7b,false,1144641,
```

c Create additional disk groups, each containing one SSD and three HDD devices, starting with the devices noted in Step 4a and Step 4b.

```
[root@esxi-01:/~] esxcli vsan storage add -s naa.5001e820028799a0 -d naa.5000c5008f366e43 -d naa.5000c5008f3581f3
[root@esxi-01:/~] esxcli vsan storage add -s naa.5001e82002879c68 -d naa.5000c5008f3e367 -d naa.5000c5008f353f7b
```

**Install the vCenter Server Appliance on the ESXi Host (Node 1)**

You install and configure the vCenter Server Appliance on the prepared ESXi host to create a virtual datacenter and vSphere cluster into which you can deploy the on-premises components. The vCenter Server Appliance installation is configured to use an embedded Platform Services Controller.


**Note** These steps describe what to specify in the vCenter Server Appliance deployment for a successful Horizon Cloud with On-Premises Infrastructure setup. In general, you follow the on-screen instructions, advancing by clicking **Next** in each screen. The steps describe changes from the default values.

Some of the details in each step are slightly different depending on which version you are installing, 6.0.* or version 6.5.*. To see the precise details for step 6 for the version you are installing, you can see the following topics in the online vSphere Installation and Setup information at VMware vSphere 6 Documentation, specifically:

- For version 6.5.*, see the online topic **Stage 1 - Deploy the OVA File as a vCenter Server Appliance with an Embedded Platform Services Controller**.
- For version 6.0.*, see the online topic **Deploy the vCenter Server Appliance with an Embedded Platform Services Controller**.
Prerequisites

- Verify that you have obtained the ISO image for a version of vCenter Server Appliance that is supported by this Horizon Cloud with On-Premises Infrastructure release. The name of the ISO image file follows the pattern:

  VMware-VCSA-all-version_number-build_number.iso

  Where version_number and build_number are the vCenter Server Appliance version and build numbers, such as:

<table>
<thead>
<tr>
<th>ISO Image File</th>
<th>Version</th>
<th>Build</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware-VCSA-all-6.5.0-4944578.iso</td>
<td>6.5.0</td>
<td>4944578</td>
</tr>
<tr>
<td>VMware-VCSA-all-6.0.0-4637290.iso</td>
<td>6.0.0</td>
<td>4637290</td>
</tr>
</tbody>
</table>

  For a list of the supported versions for this version of Horizon Cloud with On-Premises Infrastructure, see the Release Notes. For the steps describing how to obtain the vCenter Server Appliance ISO image, see the Download and Mount the vCenter Server Appliance Installer topic in the vSphere Installation and Setup guide located at the vSphere Documentation page.

- Verify that the Windows system on which you are mounting the ISO image has the VMware Client Integration Plug-in installed on it, at the version that matches the ISO image's vCenter Server Appliance version. If the plug-in is not already installed, or is at a previous version, you can install the plug-in either by using its installer located in the ISO image's /vcsa directory or following the instructions in VMware knowledge base article 2145066.

Procedure

1. On a Windows system, mount the vCenter Server Appliance ISO image file.

2. (Optional) If the VMware Client Integration Plug-in is not already installed or if you want to upgrade it to the latest version that matches the ISO image’s vCenter Server Appliance version, install the VMware Client Integration Plug-in.

   The installer binary VMware-ClientIntegrationPlugin-6.n.n.exe is located in the /vcsa directory in the ISO image, for example:

<table>
<thead>
<tr>
<th>ISO Image File</th>
<th>Version</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMware-ClientIntegrationPlugin-6.5.0.exe</td>
<td>6.5.0</td>
<td>If you have the ISO image for vCenter Server Appliance version 6.5.n.</td>
</tr>
<tr>
<td>VMware-ClientIntegrationPlugin-6.0.0.exe</td>
<td>6.0.0</td>
<td>If you have the ISO image for vCenter Server Appliance version 6.0.n.</td>
</tr>
</tbody>
</table>

3. Depending on the version of vCenter Server Appliance you are installing, locate the appropriate file on the mounted image and start the installation wizard.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 6.5.n</td>
<td>Run the executable file at \vcsa-ui-installer\win32\installer.exe.</td>
</tr>
</tbody>
</table>
   | Version 6.0.n | Using a browser, open the vcsa-setup.html file located in the image's root directory.  
   |           | **Note** If prompted by a browser pop-up, accept the association of vmware-csd links to the plug-in and allow access to the system. This browser pop-up is a result of installing the Client Integration Plug-in in the previous step. |

4. Click Install.

5. Read and accept the license agreement, then click Next.
Specify the following information, depending on which vCenter Server Appliance version you are installing.

This deployment uses the embedded Platform Services Controller option

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version 6.5.n</td>
<td>In version 6.5.n, the deployment of vCenter Server Appliance has two stages:</td>
</tr>
<tr>
<td></td>
<td>- Stage 1: Deploy the OVA file.</td>
</tr>
<tr>
<td></td>
<td>- Stage 2: Set up the newly deployed vCenter Server Appliance and start the services.</td>
</tr>
</tbody>
</table>

During Stage 1, make the following selections in the screens and advance to each screen by clicking Next. If an option is not explicitly stated here, retain the on-screen default value. After advancing through all screens and making the selections, click Finish to complete Stage 1.

- Deployment type: Keep the default selection vCenter Server with an Embedded Platform Services Controller.
- Target server: The target server is your node 1 ESXi host. Type the host's FQDN or IP address (esxi-01.vrn.local), the host's HTTPS port, the user name and password of a user with administrative privileges on that host, typically using the root user.
  
  **Note:** You must use the same password for all ESXi hosts.

  After clicking Next, verify that the certificate warning displays the SHA1 thumbprint of the host's SSL certificate and click Yes to accept the certificate thumbprint.

- Set up appliance: Type a name for the appliance (vcenter) and set a password for the appliance's root user.
  
  **Note:** vSphere has restrictions on what you can use for the appliance name and password. For the list of the characters you can use for those entries, see topic Stage 1 - Deploy the OVA File as a vCenter Server Appliance with an Embedded Platform Services Controller in the vSphere 6.5 online documentation.

- Deployment size: Select Small for the size and Default for the storage size.
- Datastore: Select vsanDatastore and select Enable Thin Disk Mode.
- Configure network settings. The following list shows example values. Customize these values according to the ESXi host configuration you performed in “Configure Initial Networking on ESXi Hosts,” on page 12.
  
  - Network: Select the network to which to connect the appliance.
    
    The networks displayed in the list come from the network settings of the target server (node 1 ESXi host).
  - IP version: IPv4
  - IP assignment: static
  - System name: vcenter.vrn.local
  - IP address: 172.16.0.10
  - Subnet mask or prefix length: 255.255.255.0
  - Default gateway: 172.16.8.1
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS servers</td>
<td>172.16.1.3</td>
</tr>
<tr>
<td>After you click Finish at the end of Stage 1, the system deploys the appliance. When the deployment activity is complete, click Continue to advance to Stage 2. During Stage 2, make the following selections in the screens and advance to each screen by clicking Next. If an option is not explicitly stated here, retain the on-screen default value. After advancing through all screens and making the selections, click Finish and then OK to complete stage 2.</td>
<td></td>
</tr>
<tr>
<td>Application configuration</td>
<td>Select Synchronize time with NTP servers, specify the NTP server (172.16.1.3 Use NTP servers), and enable SSH access.</td>
</tr>
<tr>
<td>SSO configuration</td>
<td>Type the domain name you want to use for the appliance’s SSO services (vsphere.local), type a user name and password for the SSO administrator account, and set the SSO site name as Default-First-Site. Note The SSO user name password is the one for the vCenter Single Sign-On administrator account. After the services are started, you can log in to vCenter Single Sign-On and to vCenter Server using the credentials as sso-user-name@sso-domain-name and the SSO password, for example, <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a>. vsphere has restrictions on what you can use for the SSO site name. For the list of the characters you can use, see topic Stage 2 - Set up the New Deployed vCenter Server Appliance with an Embedded Platform Services Controller in the vSphere 6.5 online documentation.</td>
</tr>
<tr>
<td>VMware Customer Experience Improvement Program (CEIP)</td>
<td>Decide whether to join the program and make the appropriate selection.</td>
</tr>
</tbody>
</table>

**Version 6.0.n**

When you deploy version 6.0.n of vCenter Server Appliance, make the following selections in the screens and advance to each screen by clicking Next. If an option is not explicitly stated here, retain the on-screen default value. After advancing through all screens and making the selections, click Finish to start the deployment and configuration process.

<p>| Target server                 | The target server is your node 1 ESXi host. Type the host's FQDN or IP address (esxi-01.vrn.local) and the user name and password of a user with administrative privileges on that host, typically using the root user. Note You must use the same password for all ESXi hosts in the cluster. |</p>
<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>After clicking <strong>Next</strong>, verify that the certificate warning displays the SHA1 thumbprint of the host’s SSL certificate and click <strong>Yes</strong> to accept the certificate thumbprint.</td>
<td></td>
</tr>
<tr>
<td>Virtual machine:</td>
<td>Type a name for the appliance (<strong>vcenter</strong>) and set a password for the appliance’s root user.</td>
</tr>
<tr>
<td><strong>Note</strong>: vSphere has restrictions on what you can use for the appliance name and password. For the list of the characters you can use for those entries, see topic <strong>Deploy the vCenter Server Appliance with an Embedded Platform Services Controller</strong> in the vSphere 6.0 online documentation.</td>
<td></td>
</tr>
<tr>
<td>Deployment type:</td>
<td>Keep the default selection <strong>vCenter Server with an Embedded Platform Services Controller</strong>.</td>
</tr>
<tr>
<td>SSO configuration:</td>
<td>Create a new single sign-on domain. Type the domain name you want to use for the appliance’s SSO services (<strong>vsphere.local</strong>), type a user name and password for the SSO administrator account, and set the SSO site name as <strong>Default-First-Site</strong>.</td>
</tr>
<tr>
<td><strong>Note</strong>: The SSO user name password is the one for the vCenter Single Sign-On administrator account. After the services are started, you can log in to vCenter Single Sign-On and to vCenter Server using the credentials as sso-user-name@sso-domain-name and the SSO password, for example, <a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a>. vSphere has restrictions on what you can use for the SSO site name. For the list of the characters you can use, see topic <strong>Deploy the vCenter Server Appliance with an Embedded Platform Services Controller</strong> in the vSphere 6.0 online documentation.</td>
<td></td>
</tr>
<tr>
<td>Appliance size:</td>
<td>Select <strong>Small</strong>.</td>
</tr>
<tr>
<td>Datstore:</td>
<td>Select <strong>vsanDatstore</strong> and select <strong>Enable Thin Disk Mode</strong>.</td>
</tr>
<tr>
<td>Database:</td>
<td>Accept the default of using an embedded database (<strong>PostgreSQL</strong>).</td>
</tr>
<tr>
<td>Configure network settings. The following list shows example values. Customize these values according to the ESXi host configuration you performed in “Configure Initial Networking on ESXi Hosts,” on page 12.</td>
<td></td>
</tr>
<tr>
<td>Network: Select the network to which to connect the appliance. The networks displayed in the list come from the network settings of the target server (node 1 ESXi host).</td>
<td></td>
</tr>
<tr>
<td><strong>Network address family</strong>: IPv4</td>
<td></td>
</tr>
<tr>
<td><strong>Network type</strong>: static</td>
<td></td>
</tr>
<tr>
<td><strong>Network address</strong>: 172.16.0.10</td>
<td></td>
</tr>
<tr>
<td><strong>System name</strong>: vcenter.vrn.local</td>
<td></td>
</tr>
<tr>
<td><strong>Subnet mask</strong>: 255.255.255.0</td>
<td></td>
</tr>
<tr>
<td><strong>Network gateway</strong>: 172.16.0.1</td>
<td></td>
</tr>
<tr>
<td><strong>Network DNS servers</strong>: 172.16.1.3</td>
<td></td>
</tr>
<tr>
<td><strong>Configure time sync</strong>: 172.16.1.3 (Use NTP servers)</td>
<td></td>
</tr>
<tr>
<td><strong>Enable SSH</strong> (set enabled)</td>
<td></td>
</tr>
<tr>
<td>VMware Customer Experience Improvement Program (CEIP): Decide whether to join the program and make the appropriate selection.</td>
<td></td>
</tr>
</tbody>
</table>

7 When the installation process is finished, exit the installation wizard and unmount the ISO image.
Create a Virtual Data Center and Add a Distributed Virtual Switch and Distributed Port Groups

In the vCenter Server environment, you must create a virtual data center and create a distributed virtual switch and distributed port groups for that data center.

**Important** Horizon Cloud with On-Premises Infrastructure is not supported for use in a vCenter Server environment that has more than one virtual data center configured in it. That data center is the vSAN Ready cluster. When you set up Horizon Cloud with On-Premises Infrastructure in the vCenter Server environment, ensure that the environment contains only one data center before deploying the Horizon Air Link into the environment.

**Procedure**

1. In the vSphere Web Client, create a single data center named VRN-DC.

2. Add hosts to the data center.
   a. Under datacenters, select VRN-DC and Add Host.
   b. Add esxi-01.vrn.local followed by all remaining hosts to the VDC using defaults.

   **Note** You must use FQDNs when you add the ESXi hosts.

3. Create a single distributed switch named dvSwitch0 for the data center VRN-DC and configure the switch settings.

   The distributed switch version you use depends on the version of vCenter Server Appliance you are using.

<table>
<thead>
<tr>
<th>dvSwitch0 Option</th>
<th>vCenter Server Appliance Version 6.5.n</th>
<th>vCenter Server Appliance Version 6.0.n</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>6.5.n</td>
<td>6.0.n</td>
</tr>
<tr>
<td>Number of uplinks</td>
<td>Two</td>
<td>Two</td>
</tr>
<tr>
<td>Create default port group</td>
<td>Deselect this option.</td>
<td>Deselect this option.</td>
</tr>
</tbody>
</table>

4. Under dvSwitch0, select Add and Manage Hosts and perform the following steps.
   a. Select task > Add hosts.
   b. Select New hosts then select all of the hosts listed.
   c. Select network adapter tasks > Manage physical adapters.
   d. Manage physical adapters - for each ESXi host, select the vmnic that is not in use, select Assign uplink, and use Uplink 2.

5. Under dvSwitch0, select Distributed Port group > New Distributed Port Group.

6. Add the following port groups to dvSwitch0, using defaults except for setting the VLAN ID.

<table>
<thead>
<tr>
<th>PORTGROUP</th>
<th>VLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>dvpg-vmk0-management</td>
<td>1000</td>
</tr>
<tr>
<td>dvpg-vmk1-VSAN</td>
<td>4001</td>
</tr>
<tr>
<td>dvpg-vmk2-vMotion</td>
<td>4002</td>
</tr>
<tr>
<td>dvpg-management</td>
<td>1000</td>
</tr>
<tr>
<td>dvpg-tenant</td>
<td>1001</td>
</tr>
</tbody>
</table>
7 Migrate VMkernel interfaces to the DVS.
   a In the vSphere Web Client, under Distributed Switches, select Add and Manage Hosts.
   b Select task > Manage host networking.
   c Select Attached hosts then select all of the attached hosts.
   d Select network adapter tasks > Manage VMkernel adapters.
   e Manage VMKernel network adapters - for each ESXi host, select vmk0, then select Assign port group > dvpg-vmk0-management.

8 Migrate the vCenter Server Server appliance to the DVS.
   a In the vSphere Web Client, under Distributed Switches, select Add and Manage Hosts.
   b Select task > Manage host networking.
   c Select Attached hosts then select all attached hosts.
   d Select network adapter tasks > Migrate virtual machine networking.
   e Manage VM networking - under esxi-01.vrn.local, select vcenter, then select Assign port group > dvpg-management.

9 Remove vSwitch0 from all nodes.
   [root@esxi-01:~] esxcli network vswitch standard portgroup remove --portgroup-name="VM Network" --vswitch-name=vSwitch0
   [root@esxi-01:~] esxcli network vswitch standard uplink remove --uplink-name=vmnic4 --vswitch-name=vSwitch0
   [root@esxi-01:~] esxcli network vswitch standard remove --vswitch-name=vSwitch0

10 Add a second physical network adapter to the DVS.
   a In the vSphere Web Client, under Distributed Switches, select Add and Manage Hosts.
   b Select task > Manage host networking.
   c Select Attached hosts then select all attached hosts.
   d Select network adapter tasks > Manage physical adapters.
   e Manage physical network adapters. For each ESXi host, select the vmnic that is not in use, then select Assign uplink and use Uplink 1.

11 Add VMkernel adapters for vSphere vMotion and vSAN.
   a In the vSphere Web Client, under Distributed Switches, select Add and Manage Hosts.
   b Select task > Manage host networking.
   c Select Attached hosts and then select all the attached hosts.
   d Select network adapter tasks > Manage VMKernel adapters.
Configure the network adapters under Manage VMkernel network adapters.

1. Repeat this procedure for all hosts.
2. On esxi-01.vrn.local, select New adapter.
3. Select target device - Select an existing network and select dvpg-vmk1-VSAN.
4. Port properties - enable Virtual SAN traffic only.
5. IPv4 settings - Set the static IP address to 192.168.1.11 and netmask to 255.255.255.0.
7. Select target device - Select an existing network and select dvpg-vmk2-vMotion.
8. Port properties - enable vMotion traffic only.
9. IPv4 settings - Set the static IP address to 192.168.2.11 and netmask to 255.255.255.0.

Follow the prompts and click Finish.

The following image is an example of the Manage VMkernel network adapters page.

The following image is an example of the topology page for dvSwitch0 in a vSAN Ready Node cluster environment.
12 Balance VMkernel traffic across physical network adapters.
   a In the vSphere Web Client, under Distributed Switches, select Distributed Port group > Manage Distributed Port Groups.
   b Select Teaming and failover, and port group dvpg-vmk1-VSAN.
   c Set Uplink 1 to Standby and Uplink 2 to Active.
   d Apply the settings and return to Distributed Port Group management.
   e Select Teaming and failover, then select all of the remaining port groups, which are non-virtual SAN traffic.
   f Set Uplink 1 to Active and Uplink 2 to Standby.
   g Apply the settings and return to Distributed Port Group management.
   h Select Traffic shaping, then select port group dvpg-vmk2-vMotion.
   i Enable both Ingress and Egress traffic shaping and set the following values for both Ingress and Egress.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Average bandwidth in Kbps</td>
<td>4294967</td>
</tr>
<tr>
<td>Peak bandwidth in Kbps</td>
<td>4294967</td>
</tr>
<tr>
<td>Burst size in KB</td>
<td>102400</td>
</tr>
</tbody>
</table>

**Create the vSphere Cluster**

To establish failover protection, create a vSphere Cluster. These steps are performed using the vSphere Web Client.

**Procedure**

1 Create a cluster with the name VRN-CLUSTER.
2 Select VRN-DC as the cluster location.

3 Select **Turn ON** for vSAN, leave **Add disks to storage** set to Automatic, and click **OK**.

4 Under VRN-CLUSTER, select **Move Hosts into Cluster**, select **esx-01** only, and move it to the cluster.

5 Return to **Move Hosts into Cluster**, select the remaining hosts, and move them to the cluster.

**NOTE** The tasks performed by vCenter to move the remaining hosts to the cluster might take several minutes to finish. Some vSAN Health Alarms might appear in the vSphere Web Client. You can safely dismiss these alerts.

6 Verify vSAN cluster configuration.

   a Under Datastores, navigate to the device backing location, following the steps appropriate for the vCenter Server Appliance version you are using

<table>
<thead>
<tr>
<th><strong>Option</strong></th>
<th><strong>Description</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Version 6.5.n</strong></td>
<td>Select vsanDatastore &gt; Configure &gt; Device Backing.</td>
</tr>
<tr>
<td><strong>Version 6.0.n</strong></td>
<td>Select vsanDatastore &gt; Manage &gt; Device Backing.</td>
</tr>
</tbody>
</table>

   b Verify that all ESXi hosts have a state of Connected/Healthy.

   c Verify that all disk groups have a state of Mounted/Healthy.

   d Verify that all ESXi hosts have the same Network Partition Group.

7 Enable DRS on the cluster VRN-CLUSTER.

   a Under Clusters, select **VRN-CLUSTER > Manage > Settings**.

   b Under Services, select **vSphere DRS** and **Edit**.

   c Select the option **Turn ON vSphere DRS**, keep the default value for all configuration options.

   d Save your choices by clicking **OK**.
8 On the cluster’s **Manage** tab, under **Settings**, enable HA on the cluster by following the steps according to the vCenter Server Appliance version you are using.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Version 6.5.n** | a Select vSphere Availability and click Edit.  
 b Click Turn ON vSphere HA to select it.  
 c Click the Failure and Response tab.  
 d Change Response for Host Isolation to Power off and restart VMs.  
 e Click the Admission Control tab.  
 f To set single host redundancy, set Host failures cluster tolerates to 1.  
 g Verify that Define host failover capacity is set to Cluster resource percentage, and adjust it if not.  
 h Keep the default values for all other settings and click OK to apply changes. |

| **Version 6.0.n** | a Select vSphere HA then select the option Turn ON vSphere HA.  
 b Expand Failure conditions and VM response.  
 c Change Response for Host Isolation to Power off and restart VMs.  
 d Expand Admission Control.  
 e Select Define failover capacity by reserving a percentage of the cluster resources and set the percentages for Reserved failover CPU capacity and Reserved failover Memory capacity.  
 To determine the percentage of cluster resources to reserve in order to provide single redundancy in a cluster of N identical hosts, calculate \((1/N)\times100\), where N is the number of hosts. For this four-node cluster, the percentage equals \((1/4)\times100\) or 25%.  
 f Keep the default value for all other settings and click OK to apply changes. |

---

**Deploy Horizon Air Link Into Your vSAN Ready Node Cluster**

When using vSAN Ready Node cluster as the hyper-converged infrastructure for Horizon Cloud with On-Premises Infrastructure, use the vSAN Ready Node cluster vCenter to deploy the Horizon Air Link appliance OVA. After the appliance is deployed and powered on, you use it to connect with the VMware hosted service, Horizon Cloud, and begin the Horizon Cloud Node configuration process.

**IMPORTANT** Horizon Cloud with On-Premises Infrastructure is not supported for use in a vCenter Server environment that has more than one virtual data center configured in it. That data center is the vSAN Ready cluster. When you set up Horizon Cloud with On-Premises Infrastructure in the vCenter Server environment, ensure that the environment contains only one data center before deploying the Horizon Air Link into the environment.

**Procedure**

1. Download the Horizon Air Link OVA file from the **My VMware® Horizon Cloud with On-Premises Infrastructure** download page.

2. In the vSphere Web Client, navigate to the vCenter server where you are installing the Horizon Air Link.
3 Right-click your cluster and select **deploy OVF Template**.

4 Browse to the local file you downloaded and click **Next**.
   The page displays basic information about the OVF template.
5 Click Next.

6 Enter a name for the virtual machine, select the virtual data center you previously configured, and then click Next.
7 Select vsanDatastore and click Next.

8 On the Setup Networks tab, select dvpg-management and click Next.
In the **Authentication** section, you can provide a new root password for the appliance.

**Note** The password is not required and defaults to `Passw0rd`! unless you change it to a password of your own during deployment.

In the **Networking** section, if you want to configure the appliance using DHCP, leave the **IP address**, **Netmask**, **Default Gateway**, and **DNS Servers** text boxes blank. Otherwise, provide values for the text boxes to statically configure the values.

For the DHCP option, confirm that DHCP is configured on the network you are deploying to.

If your deployment requires you to configure a proxy server for outbound Internet access, in the **Internet Proxy** section, enter values in the **Proxy Server**, **Proxy Port**, **Proxy Username**, and **Proxy Password** text boxes. If your deployment does not require you to configure a proxy server, leave the text boxes blank.

Click **Next**.

Select the **Power on after deployment** check box and click **Finish**.

After a few minutes, the appliance deploys.
Open the console for the virtual machine.

The console window displays the management URL. The link is in the format of https://HAL-IP-address:8443, where HAL-IP-address represents the IP address of your Horizon Air Link appliance.

The Horizon Air Link appliance is ready to start the Horizon Cloud Node setup process.

What to do next

Continue setting up this Horizon Cloud Node by:

1. Using a browser and navigating to the URL displayed in the Horizon Air Link appliance, such as https://HAL-IP-address:8443, using the IP address of the appliance.

2. Following the steps as described in Chapter 5, “Configure One or More Horizon Cloud Nodes,” on page 41.
Expanding the Existing vSAN Ready Node Cluster with Additional Nodes

To add ESXi hosts to an existing data center, you must repeat several previous installation steps as prerequisites, such as the ESXi installation steps.

These instructions describe how to expand the cluster you created earlier, as described in Chapter 2, “Install Horizon Cloud with On-Premises Infrastructure on a vSAN Ready Node Cluster,” on page 11.

**Prerequisites**

- To prepare for the expansion of the vSAN Ready Node cluster capacity, allocate new IP addresses for each node that you plan to add to the vSAN, vSphere vMotion, and management networks. See Chapter 1, “Overview of a Horizon Cloud with On-Premises Infrastructure Installation,” on page 7 for information helpful in creating a plan for adding IP addresses. For example, you must properly configure DNS entries for hosts in routed networks, such as the management network.
- Install additional ESXi hosts. See “Install VMware ESXi on Each Server,” on page 12.
- Configure initial networking on the additional ESXi hosts. See “Configure Initial Networking on ESXi Hosts,” on page 12.
- Prepare disks. See “Prepare Disks,” on page 16.

**Procedure**

1. **Add vSAN Ready Nodes to Expand Capacity of an Existing vSAN Ready Node Cluster** on page 35
   The procedures for expanding cluster capacity with additional vSAN Ready Node hardware are similar to the procedures performed initially to build the cluster.

2. **Edit the Existing vSphere Cluster** on page 37
   You must move the newly created hosts into the existing vSphere cluster.

3. **Modify the HA Cluster Admission Criteria** on page 37
   Update the HA cluster admission criteria to maintain the current level of cluster-node redundancy.

**Add vSAN Ready Nodes to Expand Capacity of an Existing vSAN Ready Node Cluster**

The procedures for expanding cluster capacity with additional vSAN Ready Node hardware are similar to the procedures performed initially to build the cluster.

**Prerequisites**

Verify that you have met the prerequisites described in Chapter 3, “Expanding the Existing vSAN Ready Node Cluster with Additional Nodes,” on page 35.
Procedure

1. In the vSphere Web Client, select VRN-DC and Add Host.

2. Add the new ESXi hosts to the data center.

   **Note** FQDNs must be used when adding the ESXi hosts.

3. Under dvSwitch0, select Add and Manage Hosts and perform the following steps.
   
   a. Select task > Add hosts.
   
   b. Select New hosts and then select all hosts listed.
   
   c. Select network adapter tasks > Manage physical adapters.
   
   d. Manage physical adapters - for each ESXi host, select the vmnic that is not in use, select Assign uplink, and use Uplink 2.

4. Migrate VMkernel interfaces to the DVS.
   
   a. In the vSphere Web Client, under Distributed Switches select Add and Manage Hosts.
   
   b. Select task > Manage host networking.
   
   c. Select Attached hosts and then select all the newly created attached hosts.
   
   d. Select network adapter tasks > Manage VMkernel adapters.
   
   e. Manage VMkernel network adapters - for each ESXi host, select vmk0, then select Assign port group > dvpg-vmk0-management.

5. On the newly created hosts, remove vSwitch0 from all nodes

   [root@esxi-01:] esxcli network vswitch standard portgroup remove --portgroup-name="VM Network" --vswitch-name=vSwitch0
   
   [root@esxi-01:] esxcli network vswitch standard uplink remove --uplink-name=vmnic4 --vswitch-name=vSwitch0
   
   [root@esxi-01:] esxcli network vswitch standard remove --vswitch-name=vSwitch0

6. On the newly created hosts, add a second physical network adapter to the DVS.
   
   a. In the vSphere Web Client, under Distributed Switches, select Add and Manage Hosts.
   
   b. Select task > Manage host networking.
   
   c. Select Attached hosts and then select all attached hosts.
   
   d. Select network adapter tasks > Manage physical adapters.
   
   e. Manage physical network adapters - for each ESXi host, select the vmnic that is not in use, then select Assign uplink and use Uplink 1.

7. On the newly created hosts, add VMkernel adapters for vSphere vMotion and vSAN.
   
   a. In the vSphere Web Client, under Distributed Switches, select Add and Manage Hosts.
   
   b. Select task > Manage host networking.
   
   c. Select Attached hosts and then select the newly attached hosts.
   
   d. Select network adapter tasks > Manage VMkernel adapters.
Under Manage VMkernel network adapters, perform the following tasks.

1. On the first new ESXi host, select **New adapter**.
2. Select **target device - Select an existing network** and select **dvpg-vmk1-VSAN**.
3. **Port properties** - enable **Virtual SAN traffic** only.
4. **IPv4 settings** - Set the static IP address to match that of the new host and set the netmask to **255.255.255.0**.

   **NOTE**  This action applies to the recently added vSAN IPv4 address and vSphere vMotion addresses, respectively.

5. Select **New adapter** again.
6. Select **target device - Select an existing network** and select **dvpg-vmk2-vMotion**.
7. **Port properties** - enable **vMotion traffic** only.
8. **IPv4 settings** - Set the static IP address to match that of the new host and set the netmask to **255.255.255.0**.

   **NOTE**  This action applies to the recently added vSAN IPv4 address and vSphere vMotion, respectively.

9. Repeat the preceding instructions for all remaining hosts.

f. Click **Next** on the following pages and then click **Finish**.

---

**Edit the Existing vSphere Cluster**

You must move the newly created hosts into the existing vSphere cluster.

**Procedure**

1. In the vSphere Web Client, under VRN-CLUSTER, select **Move Hosts into Cluster**, select the newly created hosts, and move them to the cluster.

   **NOTE**  The tasks performed by vCenter to move the new hosts into the cluster might take several minutes to finish and some vSAN health alarms might appear in the vSphere Web Client. You can safely dismiss these alarms.

2. Verify the vSAN cluster configuration.
   a. In the vSphere Web Client, under Datastores, select **vsanDatastore > Manage > Device Backing**.
   b. Verify that all ESXi hosts have a state of Connected/Healthy.
   c. Verify that all disk groups have a state of Mounted/Healthy.
   d. Verify that all ESXi hosts have the same Network Partition Group.

---

**Modify the HA Cluster Admission Criteria**

Update the HA cluster admission criteria to maintain the current level of cluster-node redundancy.

The method for determining HA admission criteria is identical to the method previously provided. The method requires that the hardware used across the hosts in the cluster is identical.

**Procedure**

1. In the vSphere Web Client, under Clusters, select **VRN-CLUSTER > Settings**.
2. Expand the Admission Control section.
3 Select **Define failover capacity by reserving a percentage of the cluster resources.**

4 Determine and apply HA admission criteria.

5 To determine the percentage of cluster resources to reserve to provide single-redundancy in a cluster of N identical hosts, calculate (1/N)*100, where N is the number of hosts.

   For a four-node cluster, the percentage equals (1/4)*100, or 25 percent.

6 Apply this value to **Reserved failover CPU capacity** and **Reserved failover Memory capacity.**

7 Leave all other settings at defaults.

8 Select **OK** to apply changes.
Installing
Horizon Cloud with On-Premises Infrastructure on Dell EMC VxRail

To install Horizon Cloud with On-Premises Infrastructure on Dell EMC VxRail, you first configure a cluster on that hardware. Then you deploy the Horizon Air Link appliance into the cluster.

This chapter includes the following topics:

- “Install Virtualization and Storage on Dell EMC VxRail,” on page 39
- “Deploy Horizon Air Link Into Your Dell EMC VxRail,” on page 39

Install Virtualization and Storage on Dell EMC VxRail

Use Dell EMC VxRail to build a cluster and configure the cluster by following the appropriate documentation.

After obtaining your Dell EMC VxRail from your provider, follow the applicable Dell EMC VxRail documentation to configure the deployment, applying the Horizon Cloud with On-Premises Infrastructure networking guidelines as appropriate. See Chapter 1, “Overview of a Horizon Cloud with On-Premises Infrastructure Installation,” on page 7.

Deploy Horizon Air Link Into Your Dell EMC VxRail

When you use Dell EMC VxRail as the hyper-converged infrastructure for your Horizon Cloud with On-Premises Infrastructure deployment, you can use the Dell EMC VxRail marketplace to install and configure the Horizon Air Link appliance. When the appliance is deployed and powered on, you use it to connect to the VMware hosted service, Horizon Cloud, and begin the Horizon Cloud Node configuration process.

Procedure

1. In VxRail Manager Extension, click Configuration.
2. Click Market.
3. Click Install in the Horizon Cloud with On-Premises Infrastructure option.
   If necessary, use the filter and scroll function to locate the option.
4. Finish the Install Horizon Cloud with On-Premises Infrastructure form.
   a. In the Virtual machine name text box, enter a name for the Horizon Air Link instance.
   b. In the Network drop-down menu, select vCenter Server Network.
c Complete the text boxes in the form specific to the vCenter Server instance.

- If you use DHCP to configure the Horizon Air Link, leave the **IP address**, **Netmask**, **Default Gateway**, and **DNS Server** text boxes blank. If a proxy server is required to reach the Internet, provide the proxy server settings.

d Click **Install**.

A Horizon Air Link instance is installed and the name you provided for it is listed on the Market page under the Horizon Cloud with On-Premises Infrastructure option.

5 Click **Manage** for the new application.

The Horizon Air Link appliance is ready to start the Horizon Cloud Node setup process.

**What to do next**

Continue setting up this Horizon Cloud Node by:

1 Using a browser and navigating to the URL displayed in the Horizon Air Link appliance, such as `https://HAL-IP-address:8443`, using the IP address of the appliance.

2 Following the steps as described in Chapter 5, “Configure One or More Horizon Cloud Nodes,” on page 41.
Configure One or More Horizon Cloud Nodes

After deploying the Horizon Air Link appliance, you use the Horizon Cloud Node Setup user interface to provide the networking and other information required to configure the Horizon Cloud Node. You configure a Horizon Cloud Node using a Web browser to open the Setup user interface. You must log in using My VMware credentials.

You must perform this procedure for each Horizon Cloud Node that you want to pair with Horizon Cloud for a Horizon Cloud with On-Premises Infrastructure deployment.

Managing multiple Horizon Cloud Nodes is advantageous in the following situations.

- If you operate in multiple geographical locations, having one node physically located in each office can lower the latency.
- You can use a second Horizon Cloud Node as a test environment, where you can test images and applications outside of the production environment.
- If you scale beyond the current limits of the hardware, you can add nodes to additional hardware to meet the demand.

**Prerequisites**

For each Horizon Cloud Node that you want to set up, verify that you have the following items:

- A deployed Horizon Air Link appliance, as described in “Deploy Horizon Air Link Into Your vSAN Ready Node Cluster,” on page 28 and “Deploy Horizon Air Link Into Your Dell EMC VxRail,” on page 39.

- The IP address for the deployed Horizon Air Link appliance.

  You use the appliance’s IP address to display the setup login page by browsing to a URL of the form https://<Horizon Air Link appliance IP>:8443, where <Horizon Air Link appliance IP> is the IP address of the deployed appliance. If you do not know the IP address of the Horizon Air Link appliance, use the vSphere Web Client to connect to the virtual data center in which the appliance is deployed and navigate to the summary page for the Horizon Air Link appliance. The IP address appears on the summary page.

- The My VMware credentials you used when you registered for the Horizon Cloud with On-Premises Infrastructure service.

- The single sign-on credentials for the vCenter Server cluster in which the Horizon Air Link appliance is deployed.

- The fully qualified domain name of the vCenter Server instance.

**IMPORTANT** You enter the vCenter Server instance’s fully qualified domain name as part of the setup process. If you use an IP address, the setup process will fail.
The password for the ESXi hosts in the cluster.

During node configuration, the bottom of the page displays a link to Support Bundle. If something occurs that requires you to send support logs to VMware for review, click the link. A ZIP file containing the logs is downloaded to your browser. Contact VMware Support as described in KB 2144012.

Procedure

1. Using a browser, navigate to https://<Horizon Air Link appliance IP>:8443, where <Horizon Air Link appliance IP> is the IP address of the deployed appliance.

   The Setup page appears with the login fields.

2. At the Horizon Cloud Node Setup page, log in using the My VMware credentials that you used to register for the Horizon Cloud with On-Premises Infrastructure service.

3. Click Login.

4. If prompted either to review the End User License Agreement or to respond to offline nodes, take the appropriate action.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Offline Nodes</td>
<td>The Offline Nodes dialog box appears when you attempt to onboard a node and the system detects that one or more existing nodes associated with your logged-in My VMware credentials are in an offline state. This dialog gives you the opportunity to delete the offline nodes. If you are absolutely certain that you want to delete an offline node, click Yes, then click + to continue the configuration of the node you started.</td>
</tr>
<tr>
<td>End User License Agreement</td>
<td>The license agreement appears when you configure your first Horizon Cloud Node using the logged-in My VMware credentials. Select the check box to accept and click Next. The license agreement does not appear when you configure subsequent nodes.</td>
</tr>
</tbody>
</table>

5. Enter the virtual infrastructure information for the cluster in which the Horizon Air Link appliance is deployed.

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter address</td>
<td>Type the vCenter Server instance’s fully qualified domain name. IMPORTANT You must use the fully qualified domain name. If you use an IP address, the setup process will fail.</td>
</tr>
<tr>
<td>vCenter username</td>
<td>Type the single sign-on name in the form of <a href="mailto:username@example.com">username@example.com</a>.</td>
</tr>
<tr>
<td>vCenter password</td>
<td>Type the single sign-on password.</td>
</tr>
<tr>
<td>ESXi password</td>
<td>Type the password used by the ESXi hosts.</td>
</tr>
</tbody>
</table>

6. Click Next.

7. If a certificate was loaded to the vCenter Server environment that cannot be automatically validated, review and verify the displayed certificate details in the vCenter Server Certificate section and click Next.
8 Enter the hardware description and network information.

<table>
<thead>
<tr>
<th>Option</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware Description</td>
<td>Enter the hardware and data center information. For example, the name of the Horizon Cloud Node, location, and optional description. You can also create a data center location or edit an existing one.</td>
</tr>
</tbody>
</table>
| Management Network  | a Select a network from the drop-down menu, such as dvpg-management.  
                          Note The selected network must be configured to allow outbound access to the Internet, to allow management of the Horizon Cloud Node by the Horizon Cloud service. As an example, typically you select the same management network that the Horizon Air Link appliance is connected to.  
                          b Type the selected network’s gateway IP address and a subnet mask.  
                          c In the IP Range Min and IP Range Max text boxes, assign at least five (5) contiguous IP addresses from the selected management network. |
| Desktop Network     | Enter the network information, including an assigned range of three (3) contiguous IP addresses in the same subnet as the gateway.  
                          The subnet must include the desktop IP addresses for end-user desktops, which get IP addresses from DHCP.  
                          The subnet must be large enough to contain all end-user desktops and DHCP must be configured to serve IP addresses to those desktops. |
| Additional Information| Enter IP addresses for NTP and DNS servers.                                                                                                                                 |

9 Click Next.

The system begins downloading binaries from the cloud. The download time varies based on location and network conditions. Typically, the download finishes in less than 45 minutes. You can close the browser now.

After the download process finishes, the system builds the virtual machines required by the Horizon Cloud Node environment, which takes approximately 30–45 minutes. After the virtual machines are built, a check is done to confirm that a connection exists to the Horizon Cloud service.

10 If the confirmation page remains open for more than a few seconds, click More Information to determine which IP addresses need outbound access.

11 To receive an email when the process finishes, enter your email address and click Submit.

12 (Optional) If you close the browser and want to reconnect to check the progress, repeat Step 1 and reauthenticate using your My VMware credentials.

A congratulations page appears when the Horizon Cloud Node configuration is successfully completed.

What to do next

Log in to Horizon Cloud at https://cloud.horizon.vmware.com and register your Active Directory domain with this Horizon Cloud Node. Registering Active Directory is the next required step. After registering the domain, you continue management of this Horizon Cloud Node from https://cloud.horizon.vmware.com.

Note If the Setup congratulations page is still open in your browser, you can click Get Started! to open the Horizon Cloud login page at https://cloud.horizon.vmware.com.

For detailed steps, see Horizon Cloud with On-Premises Infrastructure Administration.

If you have additional Horizon Cloud Nodes to onboard, you can configure them by repeating the steps using the IP addresses for the Horizon Air Link appliances in those clusters.
Configure the Environment for End-User Data, Settings, and Profile Persistence

An optimal Microsoft Windows desktop experience provides persistence of user data, settings, and profiles in the end users’ virtual desktops. To provide this persistence in the end-user virtual desktops delivered by a Horizon Cloud with On-Premises Infrastructure environment, you must deploy and configure VMware User Environment Manager™ software. Then you use the User Environment Manager™ capabilities with folder redirection to achieve this persistence.

A Horizon Cloud with On-Premises Infrastructure environment uses the VMware next-generation desktop and application delivery platform known as JMP (Just-in-Time Management Platform). JMP is a set of VMware technologies that deliver Just-in-Time desktops and applications. The JMP technologies applicable in a Horizon Cloud with On-Premises Infrastructure environment are:

- VMware Instant Clone Technology, providing fast desktop provisioning for your environment’s virtual desktops
- App Volumes, providing real-time application delivery into those desktops
- User Environment Manager, providing contextual policy management

User Environment Manager provides various options for achieving the persistence of end-user data, settings, and profiles of virtual desktops. For a Horizon Cloud with On-Premises Infrastructure environment, the best practice is using User Environment Manager with folder redirection. A pre-defined configuration is available from VMware. For details about this pre-defined configuration along with the best practices for using App Volumes and User Environment Manager with your environment, see the document titled VMware App Volumes with Horizon Cloud Application Delivery Best Practices and Operations Procedures at vmware.com. This document also includes detailed information on the installation and setup of User Environment Manager for use with Horizon Cloud with On-Premises Infrastructure.

You install User Environment Manager on premises. User Environment Manager is straightforward to set up, requiring the installation of management console software, creation of two network file shares, and configuration of group policy objects (GPOs) on the user organizational unit (OU). You can download the software from the Horizon Cloud with On-Premises Infrastructure downloads page at vmware.com. The management console runs on Windows. You can install it on a Windows VM running on your Horizon Cloud Node or on a Windows VM or machine from which you want to manage User Environment Manager.

In addition to the best practices white paper, other useful sources of information about User Environment Manager are:

- VMware User Environment Manager Deployed in 60 Minutes or Less VMware blog article.
- User Environment Manager product documentation
- User Environment Manager Deployment Considerations white paper
You must use the appendixes to install and configure Horizon Cloud with On-Premises Infrastructure on a vSAN Ready Node.

This chapter includes the following topics:

- “Appendix A - Static IP Addresses and Host Names for vSAN Ready Node Cluster Setup,” on page 47
- “Appendix B - Active Directory Details for vSAN Ready Node Cluster Setup,” on page 50

Appendix A - Static IP Addresses and Host Names for vSAN Ready Node Cluster Setup

The reference network configuration described in Horizon Cloud with On-Premises Infrastructure Installation and Configuration uses the specific static IP addresses, host names, and DNS domains described here. Use these examples to determine the deployment settings appropriate for your organization’s needs.

DNS and Your Horizon Cloud with On-Premises Infrastructure Environment

Deploying and configuring a Horizon Cloud with On-Premises Infrastructure environment involves deploying several virtual instances (virtual machines and virtual appliances) in an on-premises virtual infrastructure environment. These virtual instances get assigned static IP addresses. For proper configuration, some of the components also use a system name or hostname, and the best practice is to use a fully qualified domain name (FQDN) as the system name. The FQDN must be resolvable by your specified DNS server.

Examples:

- Each ESXi host in the vSAN Ready Node cluster has a hostname and must have a fully qualified domain name (FQDN), because the hosts must be registered with the deployed vCenter Server Appliance instance using their FQDNs.
- During installation of the vCenter Server Appliance, you specify the network address and system name in the network settings step of the installation screens. When you specify the network address as IP address 172.16.0.10 and the system name as vcenter.vrn.local, the virtual appliance is deployed with IP address 172.16.0.10 allocated to it and the system name is set to that vcenter.vrn.local FQDN.
- When the Horizon Air Link deploys and configures the Horizon Cloud Node virtual appliance, it allocates an IP address from the desktop network IP addresses that you entered in the Horizon Cloud Node Setup user interface. This IP address is used for brokering the end-user connection from the end user's client device or browser and the pool of virtual desktops. For ease of use, rather than using a
numeric IP address in the client device, the best practice is to match a memorable name, like desktops.example.com, to the numeric IP address, and provide that memorable name to your end users. You configure your organization’s DNS records to match the memorable name to the numeric IP address.

For environments other than proof-of-concepts or labs, the general best practice is to update your organization’s DNS configuration with records that associate an FQDN name with the allocated network IP address.

**Example Configuration Values**

Note The Horizon Cloud Node virtual appliance is listed in both of these networking tables for the management network and desktop network reference values. When the Horizon Air Link deploys and configures the virtual appliance, two IP addresses are assigned to the appliance: one from the management network and one from the desktop network. The IP address from the management network is used for the component that connects the virtual appliance to the cloud management plane. The IP address from the desktop network is used to broker the end-user connections to the pool of virtual desktops.

### Table 7-1. Management Network for VLAN 1000

<table>
<thead>
<tr>
<th>Host Name or System Name</th>
<th>IP Address</th>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan1000gw</td>
<td>172.16.0.1</td>
<td>vrn.local</td>
<td>Your gateway used for this management network and VLAN 1000.</td>
</tr>
<tr>
<td>horizon-air-link</td>
<td>172.16.0.5</td>
<td>vrn.local</td>
<td>The Horizon Air Link virtual appliance deployed in the vSAN cluster. In this example, the instance has an FQDN of horizon-air-link.vrn.local and an IP address of 172.16.0.5 assigned to one of the appliance’s network interfaces, typically eth0. You provide the IP address when you deploy the OVA into the vSAN Ready Node cluster.</td>
</tr>
<tr>
<td>loghost</td>
<td>172.16.0.9</td>
<td>vrn.local</td>
<td>A network server to which you configure the ESXi Dump Collector and vSphere Syslog Collector on each ESXi host to redirect ESXi memory dumps and system logs. As described in the VMware vSAN documentation, it is a best practice to configure the ESXi Dump Collector and vSphere Syslog Collector to redirect ESXi memory dumps and system logs to a network server. Having this <code>loghost</code> destination avoids potential loss of log information for systems where you might not have enough local storage or datastore space left for persistent logging. See the vSphere Installation and Setup Guide at the vSphere 6 documentation page for steps on how to configure the redirection of ESXi memory dumps and system logs to a network server.</td>
</tr>
<tr>
<td>vcenter</td>
<td>172.16.0.10</td>
<td>vrn.local</td>
<td>The vCenter Server Appliance instance deployed in the vSAN Ready Node environment. In this example, the instance has a system name that is an FQDN (vcenter.vrn.local) and an IP address of 172.16.0.10 from the management network.</td>
</tr>
<tr>
<td>esxi-01</td>
<td>172.16.0.11</td>
<td>vrn.local</td>
<td>The first ESXi host in the vSAN cluster. In this example, the ESXi host has an FQDN of esxi-01.vrn.local and its vmk0 interface has IP address 172.16.0.11. This ESXi host is also called Node 1 in Horizon Cloud with On-Premises Infrastructure Installation and Configuration.</td>
</tr>
<tr>
<td>esxi-02</td>
<td>172.16.0.12</td>
<td>vrn.local</td>
<td>The second ESXi host in the vSAN cluster. In this example, the ESXi host has an FQDN of esxi-02.vrn.local and its vmk0 interface has IP address 172.16.0.12.</td>
</tr>
<tr>
<td>esxi-03</td>
<td>172.16.0.13</td>
<td>vrn.local</td>
<td>The third ESXi host in the vSAN cluster. In this example, the ESXi host has an FQDN of esxi-03.vrn.local and its vmk0 interface has IP address 172.16.0.13.</td>
</tr>
<tr>
<td>esxi-04</td>
<td>172.16.0.14</td>
<td>vrn.local</td>
<td>The fourth ESXi host in the vSAN cluster. In this example, the ESXi host has an FQDN of esxi-04.vrn.local and its vmk0 interface has IP address 172.16.0.14.</td>
</tr>
</tbody>
</table>
## Table 7-1. Management Network for VLAN 1000 (Continued)

<table>
<thead>
<tr>
<th>Host Name or System Name</th>
<th>IP Address</th>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>smartnode-sm1</td>
<td>172.16.0.28</td>
<td>vrn.local</td>
<td>The Horizon Cloud Node virtual appliance deployed in the vSAN cluster. The Horizon Air Link virtual appliance automatically creates, deploys, and configures this virtual appliance in the cluster. The deployed appliance has a host name that is generated by the system automatically by default. You can use the vSphere Web Client to connect to your vCenter Server environment and see the host name of the Horizon Cloud Node virtual appliance deployed in your environment. When deployed, this virtual appliance is assigned two IP addresses: one from the range of management network IP addresses and one from the range of desktop network addresses that you entered in the Horizon Cloud Node Setup user interface. Additionally, the Horizon Air Link reserves another of the IP addresses from the set of management network IP addresses to later use for update purposes. That reserved IP address is listed here with braces, for example {172.16.0.29}. For information about the update process, see the Horizon Cloud with On-Premises Infrastructure Administration guide.</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>vrn-01-ipmi</td>
<td>172.16.0.41</td>
<td>vrn.local</td>
<td>The first ESXi host’s IPMI connection.</td>
</tr>
<tr>
<td>vrn-02-ipmi</td>
<td>172.16.0.42</td>
<td>vrn.local</td>
<td>The second ESXi host’s IPMI connection.</td>
</tr>
<tr>
<td>vrn-03-ipmi</td>
<td>172.16.0.43</td>
<td>vrn.local</td>
<td>The third ESXi host’s IPMI connection.</td>
</tr>
<tr>
<td>vrn-04-ipmi</td>
<td>172.16.0.44</td>
<td>vrn.local</td>
<td>The fourth ESXi host’s IPMI connection.</td>
</tr>
</tbody>
</table>

## Table 7-2. Tenant or Desktop Network for VLAN 1001

<table>
<thead>
<tr>
<th>Host Name or System Name</th>
<th>IP Address</th>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>vlan1001.gw</td>
<td>172.16.1.1</td>
<td>vm.local</td>
<td>Your gateway used for this desktop network and VLAN 1001.</td>
</tr>
<tr>
<td>vrn-dcl</td>
<td>172.16.1.3</td>
<td>vm.local</td>
<td>The DNS and NTP server.</td>
</tr>
<tr>
<td>unified-access-gw-app</td>
<td>172.16.1.9</td>
<td>vm.local</td>
<td>The Unified Access Gateway appliance deployed when you install the Unified Access Gateway product. A best practice is to use Unified Access Gateway with a Horizon Cloud with On-Premises Infrastructure environment to provide end users with seamless HTML access to their desktops. For more information, see the Horizon Cloud with On-Premises Infrastructure Administration guide and the Unified Access Gateway documentation page.</td>
</tr>
<tr>
<td>smartnode-sm1</td>
<td>172.16.1.11</td>
<td>vm.local</td>
<td>The Horizon Cloud Node virtual appliance deployed in the vSAN cluster. The Horizon Air Link virtual appliance automatically creates, deploys, and configures this virtual appliance in the cluster. The deployed appliance has a host name that is generated by the system automatically by default. You can use the vSphere Web Client to connect to your vCenter Server environment and see the host name of the Horizon Cloud Node virtual appliance deployed in your environment. When deployed, this virtual appliance is assigned two IP addresses: one from the range of management network IP addresses and one from the range of desktop network addresses that you entered in the Horizon Cloud Node Setup user interface. The IP address here from the desktop network is used to broker the end-user connections to the pool of virtual desktops.</td>
</tr>
<tr>
<td>(DHCP start)</td>
<td>172.16.1.16</td>
<td>vm.local</td>
<td>Start of the IP address range used for the end-user virtual desktops provided by this Horizon Cloud Node.</td>
</tr>
<tr>
<td>(DHCP end)</td>
<td>172.16.1.254</td>
<td>vm.local</td>
<td>End of the IP address range used for the end-user virtual desktops provided by this Horizon Cloud Node.</td>
</tr>
</tbody>
</table>

## Table 7-3. vSAN Private Network for VLAN 4001

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Node / ESXi Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.11</td>
<td>vrn-01</td>
</tr>
<tr>
<td>192.168.1.12</td>
<td>vrn-02</td>
</tr>
</tbody>
</table>
### Table 7-3. vSAN Private Network for VLAN 4001 (Continued)

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Node / ESXi Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.13</td>
<td>vrn-03</td>
</tr>
<tr>
<td>192.168.1.14</td>
<td>vrn-04</td>
</tr>
</tbody>
</table>

### Table 7-4. vSphere vMotion Private Network for VLAN 4002

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Node / ESXi Host</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.2.11</td>
<td>vrn-01</td>
</tr>
<tr>
<td>192.168.2.12</td>
<td>vrn-02</td>
</tr>
<tr>
<td>192.168.2.13</td>
<td>vrn-03</td>
</tr>
<tr>
<td>192.168.2.14</td>
<td>vrn-04</td>
</tr>
</tbody>
</table>

### Appendix B - Active Directory Details for vSAN Ready Node Cluster Setup

You must use specific services to configure the Active Directory Domain Controller.

<table>
<thead>
<tr>
<th>Server Role</th>
<th>Use</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP Server</td>
<td>Desktops on VLAN 1001</td>
</tr>
<tr>
<td>Domain Services</td>
<td>Active Directory Domain vrn.local</td>
</tr>
<tr>
<td>DNS Server</td>
<td>vrn.local, 0.16.172.in-addr.arpa, and 1.16.172.in-addr.arpa zones</td>
</tr>
<tr>
<td>NTP Server</td>
<td>w32tm peered to accurate time sources</td>
</tr>
<tr>
<td>Certificate Authority</td>
<td>LDAPS during domain bind</td>
</tr>
</tbody>
</table>
Index

A
Active Directory 50

C
CBRC 12
configure a Horizon Cloud Node 41

datacenter, pre-existing 35
Dell EMC VxRail 39
disk device 16
DNS domain 47
DNS server 7

E
ESXCLI 12
ESXi
additional hosts 35
host 26
ESXi networking 12

F
failover 37

G
glossary 5

H
HA cluster 37
HBA 12
HDD 17
high availability 26, 37
Horizon Air Link 28, 39
Horizon Cloud Node, configuring 41
host name 47

I
IGMP querier 7
IGMP snooping 7
intended audience 5
IP address 7, 47

M
MAC address 12

N
network adapter 12
networking 39
NIC 12
node 1 17

O
OVA 28, 39

P
PCI device 12
persistence of user data, settings, and profiles 45
physical network adapter 23
port groups 23

S
SAS 12
SSD device 17
storage policy 17

T
TCP/IP 12

V
vCenter Server Appliance 18
virtual datacenter 23
Virtual SAN
cluster 26
Ready Node cluster 47
Virtual SAN cluster 7
virtual switch 12, 23
Virtual SAN Ready Node, cluster 11
VLAN 7
VMkernel traffic 23
vMotion 23
vSAN
cluster 17
configure 15
disk group 17
Ready Node cluster 50
vSAN Ready Node, installing on 11
vSphere cluster 26, 37
VxRail 39