Management Domain Implementation with VLAN-Backed Networks to Support Cloud Operations and Automation in the First Region

VMware Validated Design 6.0

VMware Validated Design for Software-Defined Data Center 6.0

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

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

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About Management Domain Implementation with VLAN-Backed Networks to Support Cloud Operations and Automation in the First Region

1

The *Management Domain Implementation with VLAN-Backed Networks to Support Cloud Operations and Automation in the First Region* documentation provides step-by-step instructions for installing and configuring the components required to deploy the vRealize Suite products by using VLAN-backed networks in a VMware Cloud Foundation instance.

Core networking functionality in an SDDC that is compliant with VMware Validated Design is on top of NSX-T Data Center. The VMware Validated Design uses the Border Gateway Protocol (BGP) as a method of dynamic routing. As an alternative, NSX-T supports the use of VLAN-backed network segments with static routes. This document provides the step-by-step instruction to set up VLAN-backed network segments that can be used to deploy the vRealize Suite products and Workspace ONE Access removing the need for BGP.

Intended Audience

The *Management Domain Implementation with VLAN-Backed Networks to Support Cloud Operations and Automation in the First Region* documentation is intended for cloud architects, infrastructure administrators, and cloud administrators who are familiar with and want to use VMware software to deploy in a short time and manage a software-defined data center (SDDC). You must also have a working knowledge of NSX-T Data Center.

Required VMware Software

The *Management Domain Implementation with VLAN-Backed Networks to Support Cloud Operations and Automation in the First Region* documentation is compliant and validated with certain product versions. See VMware Validated Design Release Notes.

Before You Apply This Guidance

The sequence of the documentation of this design follows the stages for implementing and maintaining an SDDC. See Guided Documentation Map for VMware Validated Design.

To use *Management Domain Implementation with VLAN-Backed Networks to Support Cloud Operations and Automation in the First Region*, you must be acquainted with the following guidance:

- *Introducing VMware Validated Designs*
- Optionally, *Architecture and Design for the Management Domain*
- *VMware Validated Design Planning and Preparation Workbook*

Prerequisites for the Management Domain Implementation with VLAN-Backed Networks in the First Region

2

Before you implement the management domain and configure VLAN-backed networks to support cloud operations and automation, you must ensure that certain prerequisites are met.

Before you implement the management domain, you must prepare the environment and deploy the Cloud Builder appliance. See:

1 Prepare the Environment for Deployment of the Management Domain in Region A

2 VMware Cloud Builder Implementation in Region A

3 Prerequisites for Management Domain Deployment in Region A

VLAN IDs and IP Subnets

The following VLANs and IP subnets must be available to the hosts in the Management domain vCenter Server.

The values in the following tables are example values used within this document. The procedure in this document uses an SDDC Manager deployment automation workflow to deploy and configure the NSX-T Data Center edge cluster and Tier-1 gateway. This workflow also deploys an NSX-T Data Center Tier-0 gateway with external network uplinks, which are not used as part of this procedure, however can be used for future dynamic routing use cases. Therefore, if you do not plan to use the Tier-0 gateway for other use cases, the VLAN IDs and IP addresses you enter for uplink networks do not need to exist in your environment.

Table 2-1. VLAN IDs and IP Subnets

Function	Description	VLAN ID	Subnet	Gateway
Uplink 01	First uplink to the external network	1617	172.16.17.0/24	172.16.17.253
Uplink 02	Second uplink to the external network	1618	172.16.18.0/24	172.16.18.253
NSX-T Edge Overlay	NSX-T edge cluster Overlay network	1619	172.16.19.0/24	172.16.19.253

Table 2-1. VLAN IDs and IP Subnets (continued)

Function	Description	VLAN ID	Subnet	Gateway
Region-Specific Components	Used for vRealize Log Insight and the region-specific Workspace ONE Access, and the vRealize Operations Manager remote collectors.	1631	172.16.31.0/24	172.16.31.253
Cross Region Capable Components	Used for vRealize Suite Lifecycle Manager, vRealize Operations Manager, vRealize Automation, and the cross-region Workspace ONE Access.	1632	172.16.32.0/24	172.16.32.253

IP Addresses and Host Names for the NSX-T Components

Role	FQDN	IP Address
Edge Node 01	sfo-m01-en01.sfo.rainpole.local	■ 172.16.11.69 (Management) ■ 172.16.19.2 (Overlay) ■ 172.16.19.3 (Overlay) ■ 172.16.17.2 (Uplink 1) ■ 172.16.18.2 (Uplink 2)
Edge Node 02	sfo-m01-en02.sfo.rainpole.local	■ 172.16.11.70 (Management) ■ 172.16.19.4 (Overlay) ■ 172.16.19.5 (Overlay) ■ 172.16.17.3 (Uplink 1) ■ 172.16.18.3 (Uplink 2)
NSX-T Tier-1 Service Interface		172.16.32.253
Subnet Mask		255.255.255.0

VMware Cloud Foundation Management Domain Deployment Without Dynamic Routing

3

During the initial bring-up of the VMware Cloud Foundation management domain by using VMware Cloud Builder, you configure the bring-up process with a list of hosts which are pre-imaged and configured according to the requirements of VMware Cloud Foundation.

SDDC deployment supports the automated deployment and configuration of BGP-based networking. To perform a deployment without using BGP, follow this procedure.

Procedure

1. In the **Deployment Parameters Workbook for VMware Cloud Foundation**, navigate to the **Deploy Parameters** tab.
2. When asked **Do you want to deploy and configure Application Virtual Networks**, select **No**.
3. Run the Cloud Builder bring-up process.

What to do next

When the Cloud Builder bring-up process completes, follow the steps in this document to configure the NSX-T Data Center deployment to support VLAN-backed segments that are required for the management domain post-deployment steps, including the deployment of the region-specific Workspace ONE Access instance.

Configure NSX-T Data Center for VLAN-Backed Networking

4

You configure NSX-T Data Center in the management domain to support VLAN backed networks.

Procedure

1 Create an NSX-T Edge Cluster for the vRealize Suite Products by Using SDDC Manager

To support load-balancing services for the vRealize Suite products and Workspace ONE Access, you create a multi-node cluster of NSX-T Edge nodes. Deploy the NSX-T Edge cluster for the vRealize Suite products from the SDDC Manager API explorer by using a JSON specification. You take a sample JSON specification, enter the values for your environment, and use that specification for the deployment.

2 Create an NSX-T VLAN Transport Zone

An NSX-T VLAN Transport Zone is required for VLAN-based segments.

3 Add the VLAN Transport Zone to the Host Transport Nodes

To enable VLAN-backed segments, you must add the VLAN transport zone to the existing management domain transport nodes, that are the ESXi hosts.

4 Add the VLAN Transport Zone to the Edge Cluster Nodes

To enable VLAN-backed segments, you must add the VLAN transport zone to the management domain edge cluster nodes.

5 Create NSX-T Data Center VLAN Segments

NSX-T Data Center VLAN segments are required before you can deploy the vRealize Suite components.

6 Configure an NSX-T Data Center Tier-1 Gateway

Configure the NSX-T Tier-1 gateway to disconnect from the Tier-0 gateway, add a service interface, and set a static route for the vRealize Suite network.

Create an NSX-T Edge Cluster for the vRealize Suite Products by Using SDDC Manager

To support load-balancing services for the vRealize Suite products and Workspace ONE Access, you create a multi-node cluster of NSX-T Edge nodes. Deploy the NSX-T Edge cluster for the vRealize Suite

products from the SDDC Manager API explorer by using a JSON specification. You take a sample JSON specification, enter the values for your environment, and use that specification for the deployment.

Procedure

1 In a Web browser, log in to the SDDC Manager user interface.

Setting	Value
URL	https://sfo-vcf01.sfo.rainpole.io
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the navigation pane, click **Developer Center**.

3 On the **VMware Cloud Foundation Developer Center** page, click the **API Explorer** tab.

4 Retrieve the unique ID for the management cluster.

   a Expand **APIs for managing Clusters**, click **GET /v1/clusters**, and click **Execute**.

   b In the **Response** section, click **PageOfCluster** and click **Cluster (sfo-m01-cl01)**.

   c Save the *ID_of_the_cluster* to use it later.

5 Prepare a JSON specification to deploy an NSX-T Edge cluster.

a Copy and paste the following example JSON specification to a text editor.

```
{
   "edgeClusterName":"sfo-m01-ec01",
   "edgeClusterType":"NSX-T",
   "edgeRootPassword":"edge_root_password",
   "edgeAdminPassword":"edge_admin_password",
   "edgeAuditPassword":"edge_audit_password",
   "edgeFormFactor":"MEDIUM",
   "tier0ServicesHighAvailability":"ACTIVE_ACTIVE",
   "mtu":9000,
   "tier0RoutingType":"STATIC",
   "tier0Name": "sfo-m01-ec01-t0-gw01",
   "tier1Name": "sfo-m01-ec01-t1-gw01",
   "edgeClusterProfileType": "CUSTOM",
   "edgeClusterProfileSpec":
    {  "bfdAllowedHop": 255,
       "bfdDeclareDeadMultiple": 3,
       "bfdProbeInterval": 1000,
       "edgeClusterProfileName": "sfo-m01-ecp01",
       "standbyRelocationThreshold": 30
    },
   "edgeNodeSpecs":[
      {
         "edgeNodeName":"sfo-m01-en01.sfo.rainpole.io",
         "managementIP":"172.16.11.69/24",
         "managementGateway":"172.16.11.253",
         "edgeTepGateway":"172.16.19.253",
         "edgeTep1IP":"172.16.19.2/24",
         "edgeTep2IP":"172.16.19.3/24",
         "edgeTepVlan":"1619",
         "clusterId":"<!REPLACE WITH sfo-m01-cl01 CLUSTER ID !>",
         "interRackCluster": "false",
         "uplinkNetwork":[
            {
               "uplinkVlan":1617,
               "uplinkInterfaceIP":"172.16.17.2/24"
            },
            {
               "uplinkVlan":1618,
               "uplinkInterfaceIP":"172.16.18.2/24"
            }
         ]
      },
      {
         "edgeNodeName":"sfo-m01-en02.sfo.rainpole.io",
         "managementIP":"172.16.11.70/24",
         "managementGateway":"172.16.11.253",
         "edgeTepGateway":"172.16.19.253",
         "edgeTep1IP":"172.16.19.4/24",
         "edgeTep2IP":"172.16.19.5/24",
         "edgeTepVlan":"1619",
         "clusterId":"<!REPLACE WITH sfo-m01-cl01 CLUSTER ID !>",
```

```
         "interRackCluster": "false",
         "uplinkNetwork":[
            {
               "uplinkVlan":1617,
               "uplinkInterfaceIP":"172.16.17.3/24"
            },
            {
               "uplinkVlan":1618,
               "uplinkInterfaceIP":"172.16.18.3/24"
            }
         ]
      }
   ]
}
```

b Set the passwords by updating the `edgeRootPassword`, `edgeAdminPassword`, and `edgeAuditPassword` values.

c Set the *ID_of_the_cluster* for the management domain cluster that you previously saved by updating the `clusterId` value for the two NSX-T Edge nodes.

d Save the JSON specification to use it for the deployment of the NSX-T Edge cluster.

6 Validate your JSON specification.

a Expand **APIs for managing NSX-T Edge Clusters** and click **POST /v1/edge-clusters/validations**.

b In the **Value** text box, enter the content of your JSON specification file and click **Execute**.

c In the **Response** section, click **Validation UUID** and copy the `ID of the validation` value.

d Expand **APIs for managing NSX-T Edge Clusters** and click **POST /v1/edge-clusters/validations/{id}**.

e In the **Value** text box, paste the `ID of the validation` value and click **Execute**.

f In the **Response** section, click **Validation** and verify that the **resultStatus** is `SUCCEEDED`.

7 Run the workflow that deploys the NSX-T Edge cluster for the management domain in SDDC Manager.

a Expand **APIs for managing NSX-T Edge Clusters** and click **POST /v1/edge-clusters**.

b In the **Value** text box, paste the JSON specification that you prepared, click **Execute**, and wait for the task to complete.

You can see the task status in the SDDC Manager tasks pane.

Create an NSX-T VLAN Transport Zone

An NSX-T VLAN Transport Zone is required for VLAN-based segments.

Procedure

1 In a Web browser, log in to NSX-T Manager for the Management domain by using the user interface.

Setting	Value
URL	https://sfo-m01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

2 Navigate to **System** > **Fabric** > **Transport Zones**

3 Under **Transport Zones**, click **Add**, enter the following values, and click **Add**.

Setting	Value
Name	sfo-m01-tz-vlan02
Description	VLAN Transport Zone for vRealize Suite Components
Traffic Type	VLAN

Add the VLAN Transport Zone to the Host Transport Nodes

To enable VLAN-backed segments, you must add the VLAN transport zone to the existing management domain transport nodes, that are the ESXi hosts.

Procedure

1 In a Web browser, log in to NSX-T Manager for the Management domain by using the user interface.

Setting	Value
URL	https://sfo-m01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

2 Navigate to **System** > **Fabric** > **Nodes** > **Host Transport Nodes**

3 From the **Managed By** drop-down menu, select **sfo-m01-vc01.sfo.rainpole.io**.

4 Expand **sfo-m01-cl01**, select the check box for each of the hosts in the management domain cluster, and click **Actions** > **Manage Transport Zones**.

Note Do not select the cluster check box, because this option prevents adding the transport zone to multiple hosts simultaneously.

5 From the **Transport Zone** drop-down menu, select **sfo-m01-tz-vlan02** and click **Add**.

Add the VLAN Transport Zone to the Edge Cluster Nodes

To enable VLAN-backed segments, you must add the VLAN transport zone to the management domain edge cluster nodes.

Procedure

1 In a Web browser, log in to NSX-T Manager for the Management domain by using the user interface.

Setting	Value
URL	https://sfo-m01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

2 Navigate to **System** > **Fabric** > **Nodes** > **Edge Transport Nodes**.

3 Select the check box for each of the edge transport nodes in the management domain cluster and click **Actions** > **Manage Transport Zones**.

4 From the **Transport Zone** drop-down menu, select **sfo-m01-tz-vlan02** and click **Add**.

Create NSX-T Data Center VLAN Segments

NSX-T Data Center VLAN segments are required before you can deploy the vRealize Suite components.

Procedure

1 In a Web browser, log in to NSX-T Manager for the Management domain by using the user interface.

Setting	Value
URL	https://sfo-m01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

2 Navigate to **Networking** > **Segments**.

3 Click **Add Segment**, enter the following values for each segment, and click **Save**.

Setting	Value for Region A Segment	Value for Cross-Region Segment
Segment Name	sfo-m01-seg01	xreg-m01-seg01
Connectivity	None	None
Transport Zone	sfo-m01-tz-vlan02	sfo-m01-tz-vlan02
VLAN	1631	1632

4 In the **Want to continue configuring this Segment?** dialog box, click **No**.

Configure an NSX-T Data Center Tier-1 Gateway

Configure the NSX-T Tier-1 gateway to disconnect from the Tier-0 gateway, add a service interface, and set a static route for the vRealize Suite network.

Procedure

1 In a Web browser, log in to NSX-T Manager for the Management domain by using the user interface.

Setting	Value
URL	https://sfo-m01-nsx01.sfo.rainpole.io/login.jsp?local=true
User name	admin
Password	*nsx-t_admin_password*

2 Navigate to **Networking** > **Tier-1 Gateways**.

3 Click the vertical ellipsis for **sfo-m01-ec01-t1-gw01** and select **Edit**.

4 Under **Linked Tier-0 Gateway**, click **x** to remove the linked Tier-0 gateway and click **Save**.

Note To use the Tier-1 gateway for load-balancing services, it must not be linked to a Tier-0 gateway. The Tier-0 gateway that was created as part of the automation can be reused for future dynamic routing use cases.

5 Expand **Service Interfaces** and click **Set**.

6 Click **Add Interface**, enter the following values for the cross-region segment, click **Save**, and click **Close**.

Setting	Value
Name	sfo-m01-ec01-t1-lb01-si01
IP Address / Mask	172.16.32.2/24
Connected To(Segment)	xreg-m01-seg01
MTU	9000

7 Expand **Static Routes** and click **Set**.

8 Click **Add Static Route** and enter the following values.

Setting	Value
Name	default
Network	0.0.0.0/0

9 Click **Set Next Hops**.

10 Click **Add Next Hop**, enter the following values, click **Add**, and click **Apply**.

Setting	Value
IP Address	172.16.32.253
Admin Distance	1
Scope	xreg-m01-seg01

11 Click **Save**, and click **Close**.

12 Click **Close Editing**.

What to do next

Before you enable the vRealize Suite Lifecycle Manager deployment in SDDC Manager, enable the load-balancer service that is required for Workspace ONE Access, vRealize Operations Manager, and vRealize Automation. See Enable the Load Balancer Service on the Tier-1 Gateway in Region A.

Enable the vRealize Suite Lifecycle Manager Deployment in SDDC Manager

5

To enable the deployment of vRealize Suite Lifecycle Manager on a VLAN-backed network, you must update SDDC Manager.

Procedure

1 Log in to SDDC Manager by using a Secure Shell (SSH) client.

Setting	Value
URL	sfo-vcf01.sfo.rainpole.io
User name	vcf
Password	*vcf_password*

2 Enter **su** to elevate to **root** and enter the ***root_password***.

3 Enter the following and commands and press Enter.

```
cd /home/vcf
echo "feature.vcf.avn.greenfield=false" >> feature.properties
chown vcf:vcf feature.properties
chmod 644 feature.properties
/opt/vmware/vcf/operationsmanager/scripts/cli/sddcmanager_restart_services.sh
```

4 Enter **Y** to confirm.

Results

The SDDC Manager services restart. This process can take up to 5 minutes to complete.

What to do next

Before you deploy vRealize Suite Lifecycle Manager, Download the vRealize Suite Lifecycle Manager Install Bundle.

Deploy vRealize Suite Lifecycle Manager

6

vRealize Suite Lifecycle Manager is required to deploy, configure and perform life cycle operations of Workspace ONE Access, vRealize Operations Manager, and vRealize Automation. vRealize Suite Lifecycle Manager is deployed by using SDDC Manager.

Procedure

1 In a Web browser, log in to the SDDC Manager user interface.

Setting	Value
URL	https://sfo-vcf01.sfo.rainpole.io
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 Navigate to **Administration** > **vRealize Suite**.

3 Under **vRealize Suite Lifecycle Manager**, click **Deploy**.

4 Review the **vRealize Suite Lifecycle Manager Installation Prerequisites**, select the **Select All** check box, and click **Begin**.

5 On the **Network Settings** page, enter the following values and click **Next**.

Setting	Value
VLAN ID	1632
Subnet Mask	255.255.255.0
Gateway	172.16.32.253

6 On the **Virtual Appliance Settings** page, enter the following values, click **Next**, and click **Finish**.

Section	Setting	Value
Virtual Appliance	FQDN	xreg-vrslcm01.rainpole.io
System Administrator	Create Password	*admin_password*
	Confirm Password	*admin_password*
SSH Root Account	Create Password	*root_password*
	Confirm Password	*root_password*

Migrate vRealize Lifecycle Manager to the Cross-Region NSX-T VLAN Segment

7

vRealize Suite Lifecycle Manager is deployed on a standard vSphere Distributed Switch port group. To enable NSX-T distributed firewall rules and co-location on the same network as the components it will manage, you migrate the vRealize Suite Lifecycle Manager appliance to the cross-region NSX-T VLAN segment.

Procedure

1 In a Web browser, log in to vCenter Server by using the vSphere Client.

Setting	Value
URL	https://sfo-m01-vc01.sfo.rainpole.io/ui
User name	administrator@vsphere.local
Password	*vsphere_admin_password*

2 In the **VMs and Templates** inventory, right-click the **xreg-vrslcm01** VM and select **Edit Settings**.

3 From the **Network Adapter 1** drop-down menu, select **Browse**.

4 Select **xreg-m01-seg01** and click **OK**.

5 Click **OK** to save the change.

6 Verify connectivity to the vRealize Suite Lifecycle Manager user interface in a browser.

What to do next

1 Perform the Post-Deployment Management Domain Configuration in Region A.

2 Deploy, configure, and perform life cycle operations of Workspace ONE Access, vRealize Operations Manager and vRealize Automation. See Deployment of Cloud Operations and Automation in the First Region.