



# VMware Validated Design for Software-Defined Data Center

## 4.2 Release Notes

VMware Validated Design for Software-Defined Data Center 4.2 | 13 FEB 2018

Check for additions and updates to these release notes.

### What's in the Release Notes

The release notes cover the following topics:

- [About VMware Validated Design for Software-Defined Data Center 4.2](#)
- [VMware Software Components in the Validated Design](#)
- [What's New](#)
- [Internationalization](#)
- [Compatibility](#)
- [Installation](#)
- [Lifecycle of the VMware Software Components](#)
- [Caveats and Limitations](#)
- [Expanding a Consolidated SDDC with an NSX Advanced License to a Standard SDDC](#)
- [Known Issues](#)

### About VMware Validated Design for Software-Defined Data Center 4.2

VMware Validated Design provides a set of prescriptive documents that explain how to plan, deploy, and configure a Software-Defined Data Center (SDDC). The architecture, the detailed design, and the deployment guides provide instructions about configuring a dual-region SDDC.

VMware Validated Design is tested by VMware to ensure that all components and their individual versions work together, scale, and perform as expected. Unlike Reference Architectures which focus on an individual product or purpose, a VMware Validated Design is a holistic approach to design, encompassing many products in a full stack for a broad set of use case scenarios in an SDDC.

This VMware Validated Design supports a number of use cases, and is optimized for integration, expansion, Day-2 operations, as well as future upgrades and updates. As new products are introduced, and new versions of existing products are released, VMware continues to qualify the cross-compatibility and upgrade paths of VMware Validated Design. Designing with a VMware Validated Design ensures that future upgrade and expansion options are available and supported.

### VMware Software Components in the Validated Design

VMware Validated Design for Software-Defined Data Center 4.2 is based on a set of individual VMware products with different versions that are available in a common downloadable package.

The products included in VMware Validated Designs participate in the VMware's Customer Experience Improvement Program ("CEIP"). Join the CEIP because this program provides us with information used to improve VMware products and services, fix problems, and advise you on how best to deploy and use our products.

Details regarding the data collected through CEIP and the purposes for which it is used by VMware are set forth at the Trust & Assurance Center at <http://www.vmware.com/trustvmware/ceip.html>. To join or leave the CEIP for the products that are part of VMware Validated Design, see the documentation for each product.

VMware Software Components in VMware Validated Design 4.2

Product Group and Edition	Product Name	Product Version
VMware vSphere Enterprise Plus	ESXi	6.5 U1
	vCenter Server Appliance	6.5 U1

Product Group and Edition	Product Name	Product Version
VMware vSAN Standard or higher	vSAN	6.6.1
VMware NSX for vSphere Enterprise	NSX for vSphere	6.4
VMware Site Recovery Manager Enterprise	VMware Site Recovery Manager	6.5.1
VMware vSphere Replication	VMware vSphere Replication	6.5.1
VMware vRealize Automation Advanced or higher	vRealize Automation	7.3 *
	vRealize Orchestrator	7.3
VMware vRealize Business for Cloud Advanced	vRealize Business for Cloud	7.3.1
VMware vRealize Operations Manager Advanced or higher	vRealize Operations Manager	6.6.1
	vRealize Operations Management Pack for NSX for vSphere	3.5.1
	vRealize Operations Management Pack for Storage Devices	6.0.5
	vRealize Operations Management Pack for Site Recovery Manager	6.5.1.1
VMware vRealize Log Insight	vRealize Log Insight	4.5.1
	vRealize Log Insight Content Pack for NSX for vSphere	3.6
	vRealize Log Insight Content Pack for vRealize Automation 7	1.5
	vRealize Log Insight Content Pack for vRealize Orchestrator 7.0.1+	2.0
	vRealize Log Insight Content Pack for Microsoft SQL Server	3.1
	vRealize Log Insight Content Pack for Linux	1.0
	vRealize Log Insight Content Pack for Site Recovery Manager	1.2
	<b>New</b> VMware vRealize Suite Lifecycle Manager	vRealize Suite Lifecycle Manager

\* If you are already running VMware Validated Design 4.2, you must apply the patches in VMware Knowledge Base article [2151693](#).

If the communication in the vRealize Automation cluster is interrupted or is slow, the root partition of the vRealize Automation appliance can be filled up with log data. To prevent from having the space of the root partition of the vRealize Automation appliance exhausted, you must apply patches of the vRealize Automation 7.3 appliance and its Health Service. See VMware Knowledge Base article [2151693](#).

In this version of VMware Validated Design, the vRealize Automation servers in the cluster are `vra01svr01a.rainpole.local` and `vra01svr01b.rainpole.local`. Actual names vary according to your environment.

VMware makes available patches and releases to address critical security issues for several products. Verify that you are using the latest security patches for a given component when deploying VMware Validated Design.

VMware Solution Exchange and in-product marketplace store only the latest versions of the management packs for vRealize Operations Manager and the content packs for vRealize Log Insight. The software components table contains the latest versions of

the packs that were available at the time this VMware Validated Design was validated. When you deploy the VMware Validated Design components, it is possible that the version of a management or content pack on VMware Solution Exchange and in-product marketplace is newer than the one used for this release.

For information on the lifecycle of the VMware software components in this VMware Validated Design, see [lifecycle of the VMware Software Components](#).

## What's New

VMware Validated Design for Software-Defined Data Center 4.2 provides a list of new features:

- Updated Bill of Materials that incorporates new product versions
- Guidance to design and implement a dual-region SDDC that has multiple availability zones  
By using a vSAN stretched cluster in the protected region, you can use synchronous replication between availability zones to prevent data loss if one of the zones goes offline.

In VMware Validated Design for Software-Defined Data Center 4.2, the design guidance on an SDDC with multiple availability zones is available in the *VMware Validated Design Architecture and Design* document. The step-by-step instructions about implementing a multi-zone SDDC are available as add-on documentation to *VMware Validated Design Deployment for Region A* and *VMware Validated Design Deployment for Region B*.

- Site Recovery Manager and vSphere Replication implementation is moved to a new SDDC layer for business continuity.
- An improved order of deployment to enable monitoring capabilities in the SDDC as early as possible during deployment. The operations management layer now comes before the cloud management platform layer.
- Metrics about Site Recovery Manager are now surfaced in vRealize Operations Manager and vRealize Log Insight
- New naming scheme for the tenant accounts in vRealize Automation for improved indication of the account purpose.
- Upgrade guidance to provide the best path to upgrade from VMware Validated Design 4.1.
- **New** The guidance about deploying VMware Validated Design Use Cases by using vRealize Suite Lifecycle Manager consists of three guides now, each guide discussing an individual use case.

For more information, see the [VMware Validated Design for Software-Defined Data Center](#) page.

## Internationalization

This VMware Validated Design release is available only in English.

## Compatibility

This VMware Validated Design guarantees that product versions in the VMware Validated Design for Software-Defined Data Center 4.1, and the design chosen, are fully compatible. Any minor known issues that exist are described in this release notes document.

## Installation

To install and configure an SDDC according to this validated design, follow the guidance in the VMware Validated Design for Software-Defined Data Center 4.2 documentation. For product download information, and guides access, see the [VMware Validated Design for Software-Defined Data Center](#) page.

## New Lifecycle of the VMware Software Components

This VMware Validated Design version is based on one or more VMware products whose versions eventually reach the End of Support Life (EOSL) stage as described by the [VMware Lifecycle Policies](#). Those versions are no longer generally supported by VMware. In such a case, upgrade to a later version by using the upgrade procedures in the *VMware Validated Design Upgrade* documentation.

If you are using an earlier version in your environment, upgrade your environment according to the following scenarios:

### Scenarios for Upgrade from a Version that Has Reached EOSL

Scenario	Upgrade Approach
The version of VMware Validated Design that you are using has already entered the EOSL stage but the next VMware Validated Design version is	Apply the <i>VMware Validated Design Upgrade</i> documentation to bring the VMware environment to a fully supported state

still supported.  
**Scenario**

## Upgrade Approach

The version of VMware Validated Design that you are using and the next version have both already entered the EOSL stage

Because the *VMware Validated Design Upgrade* documentation supports upgrade only from one release to the next one, the transition across multiple releases might be complex. Contact a VMware sales representative to plan and perform a custom upgrade procedure with the assistance of VMware Professional Services.

For more information about current and expired product releases, refer to the [VMware Lifecycle Product Matrix](#).

## Caveats and Limitations

To install vRealize Automation, you must open certain ports in the Windows firewall. This VMware Validated Design instructs that you disable the Windows firewall before you install vRealize Automation. It is possible to keep Windows firewall active and install vRealize Automation by opening only the ports that are required for the installation. This process is described in the [vRealize Automation Installation and Configuration](#) documentation.

## Expanding a Consolidated SDDC with an NSX Advanced License to a Standard SDDC

For easier expansion to a full-featured dual-region SDDC, use NSX universal objects. Using universal objects requires an NSX Enterprise license.

If you have an NSX Advanced license in the original Consolidated SDDC, deploy NSX global objects for distributed logical routers, transport zones, and virtual wires in any places where you must specify universal objects.

To expand the SDDC to a dual-region standard architecture, deploy new universal transport zones, universal distributed logical router, and universal virtual wires for the management component and manually migrate the Layer 3 networks and virtual machines to those new virtual wires. This migration would result in an outage to the management components on top of the virtual infrastructure layer (vRealize Automation, vRealize Orchestrator, vRealize Business, vRealize Operations Manager, and vRealize Log Insight) while the migration occurs.

## Known Issues

The known issues are grouped as follows.

- [VMware Validated Design Content](#)
- [vSphere](#)
- [NSX for vSphere](#)
- [vSphere Update Manager Download Service](#)
- [vRealize Operations Manager](#)
- [vRealize Log Insight](#)
- [vRealize Automation and Embedded vRealize Orchestrator](#)
- [vRealize Business](#)
- [Site Recovery Manager and vSphere Replication](#)
- [vRealize Suite Lifecycle Manager](#)
- [VMware Validated Design Content](#)

### VMware Validated Design Content

- **Incorrect destination network is selected during deployment of the NSX Manager Appliance in VMware Validated Design for Workload and Management Consolidation**  
**New** In this Validated Design for Workload and Management Consolidation, when completing the [Assign an NSX Domain Service Account and Deploy the NSX Manager Appliance for Consolidated SDDC](#) procedure, in Step 18 you select the **sfo01-w01-vds01-management** destination network. This destination network is not correct and results in the the appliance being unable to communicate over the network.

Workaround: When deploying the NSX Manager Appliance for Validated Design for Workload and Management Consolidation, in Step 18 of the [Assign an NSX Domain Service Account and Deploy the NSX Manager Appliance for Consolidated SDDC](#) procedure, you select the **sfo01-w01-vds01-management-vm** network as the **Destination Network**.

### vSphere

- **If a host that runs the vCenter Server Appliance and is managed by the same vCenter Server instance fails, vCenter Server is not restarted on another host in the cluster as a part of the vSphere HA failover and thus becomes**

## inaccessible

vSphere HA does not restart the vCenter Server Appliance from the failed host. Because of a cluster reconfiguration or a race condition, the Fault Domain Manager (FDM) master can receive an empty compatibility data set about the vCenter Server virtual machine from vSphere DRS. To fill this data in, the master must contact the host that is running vCenter Server. Because the host has failed, the data set remains empty and vSphere HA does not have enough information to restart the vCenter Server virtual machine on another host.

Workaround:

- Recover the failed host which will restart the vCenter Server Appliance on the same host
- Manually re-register the vCenter Server virtual machine on another healthy host in the storage user interface in the vSphere Web Client and power it on. See VMware Knowledge Base article [2147569](#).
- **New You cannot access the vSphere Replication status in the vSphere Web Client in Region B**  
After the site pairing, when you log in to the vCenter Server instance in Region B by using the the vSphere Web Client and try to access vSphere Replication status, you receive the following error message:

```
interface com.vmware.vim.binding.hms.remote.SiteManager is not visible from class loader
```

Workaround: To access the status of vSphere Replication, log in to the vCenter Server instance in Region A by using the vSphere Web Client.

## NSX for vSphere

- **vCenter Server user with administrator role cannot assign an NSX for vSphere license**  
vCenter Server accepts an NSX for vSphere license when the account for registration of NSX Manager with vCenter Server is administrator@vsphere.local. Accounts that are not associated with vCenter Single Sign-On have no privileges to assign an NSX for vSphere license. When using an Active Directory service account such as svc-nsxmanager@rainpole.local to integrate NSX Manager with vCenter Server, you receive the following error "The following serial keys are invalid".

Workaround: See VMware Knowledge Base article <https://kb.vmware.com/s/article/52604>

- **In the vSphere Web Client, you can deploy NSX components only to the default folder**

During the deployment of NSX components like NSX Edge, NSX Controller, universal distributed logical router, or distributed logical router, the wizard does not show the virtual machine folders that are available in the vCenter Server inventory.

Workaround:

1. Complete the deployment of the NSX component without specifying a folder.
  2. From the Home menu, select VMs and Templates.
  3. In the Navigator pane, expand the data center where you created the NSX component.
  4. Expand the destination folder for the newly created NSX component VM.
  5. Drag the newly created NSX component VM to that folder.
- **When deploying distributed logical router (DLR) in the secondary NSX Manager, you cannot configure BGP and neighbors from the NSX interface.**  
BGP and neighbors options are greyed out when you deploy DLR for the NSX Manager in Region B.

Workaround: Use the NSX Rest API to update the configuration values for BGP.

See [https://docs.vmware.com/en/VMware-NSX-for-vSphere/6.4/nsx\\_64\\_api.pdf](https://docs.vmware.com/en/VMware-NSX-for-vSphere/6.4/nsx_64_api.pdf)

## vSphere Update Manager Download Service

- **New You cannot configure the Update Manager Download Service (UMDS) shared repository URL in Region B**  
When you log in to the vCenter Server instance in Region B by using the vSphere Web Client and try to configure the URL to the UMDS shared repository, you repeatedly see a vSphere Web Client restart dialog box, and you cannot set up the shared repository URL.

You receive the following error message:

```
interface com.vmware.vim.binding.integrity.VcIntegrity is not visible from class loader .
```

Workaround: Log in to the vCenter Server instance in Region A by using the vSphere Web Client, and configure the <http://lax01umds01.lax01.rainpole.local> URL of the Region B shared repository.

## vRealize Operations Manager

- **The dashboards in vRealize Operations Manager indicate that no data is available although data is collected**  
The dashboards display "no data available" in vRealize Operations Manager. The settings of the dashboards are correct, the adapters collect metrics and the assigned license has enough capacity to collect data.

Workaround: Save the widgets that do not show data without making any changes.

- **After you perform a failover operation, the vRealize Operations Manager analytics cluster might fail to start because of an NTP time drift between the nodes**
  - The vRealize Operations Manager user interface might report that some of the analytics nodes are not coming online with the status message *Waiting for Analytics*.
  - The log information on the vRealize Operations Manager master or master replica node might contain certain NTP-related details.
    - The NTP logs in the `/var/log/` folder might report the following messages:

```
ntpd[9764]: no reply; clock not set
ntpd[9798]: ntpd exiting on signal 15
```

- The `analytics-wrapper.log` file in the `/storage/log/vcrops/logs/` folder might report the following message:  
INFO | jvm 1 | YYYY/MM/DD | >>> AnalyticsMain.run failed with error: IllegalStateException: time difference between servers is 37110 ms. It is greater than 30000 ms. Unable to operate, terminating...

**Note:** The time difference between servers is unique to the time drift between the vRealize Operations Manager nodes.

Workaround: See VMware Knowledge Base article [2151266](#).

- **Answers to Monitoring goals always show the default values**  
In the **Define Monitoring Goals** dialog box, your answers to the monitoring goals are not saved. Every time you open the dialog box, the default values for the answers appear.
- Workaround: None.
- **After you perform disaster recovery or planned migration of the vRealize Operations Manager or Cloud Management Platform virtual machines, the vRealize Automation Adapter might be failing to collect statistics**  
This issue might occur during both failover to Region B and failback to Region A of the Cloud Management Platform or the vRealize Operations Manager analytics cluster.

After you perform disaster recovery or planned migration of the Cloud Management Platform or virtual machines of the vRealize Operations Manager analytics cluster, the collection state of the vRealize Automation Adapter is *Failed* on the **Administration > Solutions** page of the vRealize Operations Manager user interface at <https://vrops01svr01.rainpole.local>.

Workaround: Click the **Stop Collecting** button and click the **Start Collecting** button to manually restart data collection in the vRealize Automation Adapter.

- **In the vRealize Operations Manager operations interface, the Storage Reclamation Opportunities widget of the vSAN Capacity Overview dashboard displays virtual machines that do not use vSAN**  
The **Storage Reclamation Opportunities** widget of the **vSAN Capacity Overview** dashboard shows statistics about virtual machines which store data non-vSAN storage.

Workaround: None.

- **New After you fail over the analytics cluster of vRealize Operations Manager to Region B, the option to bring the cluster back online is unavailable**  
You take the analytics cluster offline by using the administrator interface of vRealize Operations Manager and perform a disaster recovery or a planned migration of the cluster appliances to Region B by using Site Recovery Manager. According to this validated design, the remote collectors in Region A remain in the region. After you power on the analytics nodes, the option to bring the cluster back online is disabled because the remote collectors in Region A, previously connected to the analytics cluster, are inaccessible. As a result, you cannot complete the recovery of the vRealize Operations Manager deployment.

Workaround: To restore the operational state of the analytics cluster, perform either of the following workarounds:

- For a disaster recovery, see VMware Knowledge Base article [67280](#).
- For a planned migration, see VMware Knowledge Base article [67279](#).

## vRealize Log Insight

- **You see no logs from the vRealize Proxy Agent in vRealize Log Insight because these logs are located in a custom folder**  
In VMware Validated Design 4.4, the vRealize Proxy Agent has a custom name: `vRealize Agent 04`. As a result, the log data is

In VMware Validated Design 4.1, the vSphere Proxy Agent has a custom name vSphere-Agent-01. As a result, the log data is stored in the `log-insight-home-dir\vSphere-Agent-01\logs`, instead of in the default `log-insight-home-dir\vSphere\logs` folder.

Workaround: Configure the log agent on the vSphere Proxy Agents with the valid log directory.

1. Log in to the vRealize Log Insight instance in the region.

Region	vRealize Log Insight URL
Region A	https://vrli-cluster-01.sfo01.rainpole.local
Region B	https://vrli-cluster-51.lax01.rainpole.local

2. Click the **Configuration** drop-down menu icon and select **Administration**
3. Under **Management**, click **Agents**.
4. From the drop-down at the top, select **vRealize Automation 7 - Windows** from the **Available Templates** section.
5. Under **File Logs**, select **vra-agent-vcenter** and in the **Directory** text box enter the following value.

Region	Directory Value
Region A	C:\Program Files (x86)\VMware\CAC\Agents\vSphere-Agent-01\logs\
Region B	C:\Program Files (x86)\VMware\CAC\Agents\vSphere-Agent-51\logs\

6. Click **Save Agent Group**.

- **The vRealize Log Insight user interface is inaccessible at its load-balanced URL https://sfo01vrli01.sfo01.rainpole.local and https://lax01vrli01.lax01.rainpole.local**

According to VMware Validated Design, vRealize Log Insight runs as a cluster of one master and two worker nodes behind the Integrated Load Balancer (ILB). When the load balancing role is transferred from one node to another, for example from the master to the second worker, the target node is unable to take over the 192.168.31.10 virtual IP (VIP) address.

vRealize Log Insight uses ARP requests between the nodes of the cluster to perform the election process and maintain quorum of the Integrated Load Balancer. The use of the IP discovery feature on the NSX logical switch for the region-local application virtual network actively performs ARP suppression. Thus, the deployment of vRealize Log Insight on an NSX logical switch can adversely affect the speed in which the election process completes, resulting in very long duration of failover between nodes.

In the user interface of the master node `sfo01vrli01a.sfo01.rainpole.local` or `lax01vrli01a.lax01.rainpole.local`, you might see the following message when the Integrated Load Balancer reports `Unavailable`:

```
{"Timestamp":"2017-07-20T09:08:34.746Z","Data":{"AlertId":"Cannot take over High Availability IP address 192.168.31.10 as it is already held by another machine (Host = vrli-wrkr-01.sfo01.rainpole.local)","Name":"Cannot take over High Availability IP address 192.168.31.10 as it is already held by another machine (Host = vrli-wrkr-01.sfo01.rainpole.local)","Description":"This notification was generated from Log Insight node (Host = vrli-wrkr-01.sfo01.rainpole.local, Node Identifier = 3eb6cbea-68ee-473b-b81e-a0296a20ae0b).\n\nLog Insight is unable to acquire the High Availability IP address 192.168.31.10 because another host within the same physical network is holding the IP address.\n\nLog data sent by the clients to the High Availability IP address 192.168.31.10 will not be received by Log Insight until either the IP address is free to be acquired by Log Insight, or the administrator changes the High Availability IP by visiting the vrli-mstr-01.sfo01.rainpole.local page.\n\nTo get more information about the current status of the IP address, the administrator can ping it, or run the following command from any machine within the same physical network:\n /sbin/arping -c 4 -I eth0 192.168.31.10 \n\nIf another host within the network still holds the IP address, this command will return the hardware address of that machine.\n\nThis message was generated by your Log Insight installation, visit the Documentation Center for more information."},"TriggerTime":"2017-07-20T09:08:34.740Z"},"AutoClearTimeoutSeconds":-1}
```

Workaround:

## vRealize Automation and Embedded vRealize Orchestrator

Task	Steps				
Locate the logical switch ID for each application virtual network	<ol style="list-style-type: none"> <li>1. Log in to vCenter Server by using the vSphere Web Client. <ol style="list-style-type: none"> <li>1. Open a Web browser and go to <code>https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client</code>.</li> <li>2. Log in using the <code>administrator@vsphere.local</code> user name and <code>vsphere_admin_password</code>.</li> </ol> </li> <li>2. Select <b>Home &gt; Networking &amp; Security</b>.</li> <li>3. In the <b>Navigator</b>, click <b>Logical Switches</b>.</li> <li>4. Select <b>172.16.11.65</b> from the <b>NSX Manager</b> drop-down menu.</li> <li>5. Locate the <code>Mgmt-RegionA01-VXLAN</code> and <code>Mgmt-RegionB01-VXLAN</code> logical switches and write down their Logical Switch ID. For example: <ul style="list-style-type: none"> <li>■ <code>Mgmt-RegionA01-VXLAN == universalwire-3</code></li> <li>■ <code>Mgmt-RegionB01-VXLAN == universalwire-4</code></li> </ul> </li> </ol>				
Disable IP discovery in each application virtual network by using	<ol style="list-style-type: none"> <li>1. Log in to the Windows host that has access to your data center.</li> <li>2. In a Chrome browser, start the Postman application and log in.</li> <li>3. Retrieve the features enabled on the application virtual networks by sending a request to NSX Manager.</li> </ol> <table border="1"> <thead> <tr> <th>Request Attribute or Response Attribute</th> <th>Value</th> </tr> </thead> <tbody> <tr> <td>AuthenticationType</td> <td>Basic Auth</td> </tr> </tbody> </table>	Request Attribute or Response Attribute	Value	AuthenticationType	Basic Auth
Request Attribute or Response Attribute	Value				
AuthenticationType	Basic Auth				

Task	Request Attribute or Response Attribute	Steps	Value
API of NSX Manager	Headers	Content-Type	application/xml
	Method	GET	
	URL	<ul style="list-style-type: none"> <li>https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/xvs/networks/universalwire-3/features</li> <li>https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/xvs/networks/universalwire-4/features</li> </ul>	
	Response Body		<?xml version="1.0" encoding="UTF-8"?> <networkFeatureConfig> <ipDiscoveryConfig> <enabled>true</enabled> </ipDiscoveryConfig> <macLearningConfig> <enabled>>false</enabled> </macLearningConfig> </networkFeatureConfig>

4. For each application virtual network, send a request to disable IP discovery.

Request Attribute	Value
AuthorizationType	Basic Auth
	Username admin
	Password <i>sfo01m01nsx01_admin_password</i>
Headers	Content-Type application/xml
Method	PUT
URL	<ul style="list-style-type: none"> <li>https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/xvs/networks/universalwire-3/features</li> <li>https://sfo01m01nsx01.sfo01.rainpole.local/api/2.0/xvs/networks/universalwire-4/features</li> </ul>
Request Body	<networkFeatureConfig> <ipDiscoveryConfig> <enabled>>false</enabled> </ipDiscoveryConfig> <macLearningConfig> <enabled>>false</enabled> </macLearningConfig> </networkFeatureConfig>

- Verify that IP discovery is disabled
- Log in to the vRealize Log Insight user interface.
    - Open a Web browser and go to <https://sfo01vrli01a.sfo01.rainpole.local>.
    - Log in using the admin user name and *vrli\_admin\_password* password.
  - Click the configuration drop-down menu icon and select **Administration**.
  - Under **Management**, click **Cluster**.
  - Under **Integrated Load Balancer**, verify that [sfo01vrli01.sfo01.rainpole.local](https://sfo01vrli01.sfo01.rainpole.local) is Available.

- Repeat for the application virtual network in the other region
- Get the Logical Switch ID and disable IP discovery on Mgmt-RegionB01-VXLAN under the 172.16.11.65 NSX Manager.
  - Log in to <https://lax01vrli01a.lax01.rainpole.local> and verify that [lax01vrli01.lax01.rainpole.local](https://lax01vrli01.lax01.rainpole.local) is Available.

**vRealize Automation Converged Blueprint with NSX routed networks fails with the error "Overlapping IP Addresses are not allowed for different addressGroups. Vnic xxx ip assignments overlaps xxx.xxx.xxx.xxx"**

Provisioning requests intermittently fail with the following error message:

Overlapping IP Addresses are not allowed for different addressGroups. Vnic xxx ip assignments overlaps xxx.xxx.xxx.xxx

Workaround: Perform the following steps:

- Login to NSX Manager and navigate to **NSX Edges**.

2. Locate the **Distributed Logical Router** under **Test**.
3. Navigate to **Manage > Settings > Interfaces** and delete the `Vnic_XXX` interface from the list of interfaces.

- **Manual installation of an IaaS Website component using the IaaS legacy GUI installer fails with a certificate validation error**

The error message appears when you click **Next** on the **IaaS Server Custom Install** page with the Website component selected. This error message is a false negative and appears even when you select the right option. The error prevents the installation of a vRealize Automation IaaS Website component.

Workaround: See Knowledge Base article [2150645](#).

- **Unable to log in to the vRealize Automation user interface and the embedded vRealize Orchestrator Control Center interface after configuring an authentication provider for the embedded vRealize Orchestrator.**

vRealize Automation user interface and the embedded vRealize Orchestrator control center interface become unavailable when the authentication settings in the embedded vRealize Orchestrator Control Center are configured with a non-existent tenant, for example, if you entered a tenant name with a typo.

Workaround: Resolve the issue by correcting the tenant and restarting the vRealize Orchestrator services on both vRealize Automation appliances.

1. Log in to the vRealize Orchestrator Control Center.
  1. Open a Web browser and go to `https://vra01svr01.rainpole.local:8283/org/vsphere.local`
  2. Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

2. Complete the authentication configuration with the correct tenant.
3. Wait for the control center to replicate the settings to all the vRO servers in the cluster
4. Restart the vRealize Orchestrator services on both vRealize Automation appliances.
  1. Open an SSH connection to `vra01svr01a.rainpole.local` and log in using the following credentials.

Setting	Value
User name	root
Password	vra_appA_root_password

2. Run the following command to restart the vRealize Orchestrator services.
  - `service vco-server restart`
3. Repeat the procedure for `vra01svr01b.rainpole.local`

- **Converged blueprint provisioning requests in vRealize Automation might fail in environments that have high workload churn rate**

In environments that have a high churn rate for tenant workloads, requests for provisioning converged blueprints in vRealize Automation might fail with one of the following error messages.

- Timeout Customizing machine

Workaround: None.

- **After you perform disaster recovery of the Cloud Management Platform, the status of the shell-ui-app service might appear as Failed in the appliance management console of the vra01svr01b.rainpole.local node**

This issue might occur during both failover to Region B and failback to Region A of the Cloud Management Platform. After you perform disaster recovery of the Cloud Management Platform, you see the follow symptoms when you verify the overall state of the platform:

- In the appliance management console `https://vra01svr01b.rainpole.local:5480`, the status of the `shell-ui-app` service is Failed.
- The statistics about the `vra-svr-443` pool on the NSX load balancer shows that the `vra01svr01b` node is DOWN.
- Trying to access the `https://vra01svr01b.rainpole.local/vcac/services/api/health` URL results with following error message:

```
The service shell-ui-app was not able to register the service information with the Component Registry service! This might cause other dependent services to fail. Error Message: I/O error on POST request for "https://vra01svr01.rainpole.local:443/SAAS/t/vsphere.local/auth/oauth/token?grant_type=client_credentials": Read timed out; nested exception is java.net.SocketTimeoutException: Read timed out"
```

You can still log in to the vRealize Automation portal because the other vRealize Automation Appliance `vra01svr01a` can service your requests.

Workaround: Restart the `vcac-server` service on the `vra01svr01b.rainpole.local` node.

1. Open an SSH connection to the `vra01svr01b.rainpole.local` appliance and log in as the `root` user.
2. Restart the `vcac-server` service.

```
service vcac-server restart
```

- **After failover or failback during disaster recovery, login to the vRealize Automation Rainpole portal takes several minutes or fails with an error message**

This issue occurs during both failover to Region B and failback to Region A of the Cloud Management Platform when the root

This issue occurs during both failover to Region B and failback to Region A of the Cloud Management Platform when the root Active Directory is not available from the protected region. You see the following symptoms:

- Login takes several minutes or fails with an error  
When you log in to the vRealize Automation Rainpole portal at <https://vra01svr01.rainpole.local/vcac/org/rainpole> using the ITAC-TenantAdmin user, the vRealize Automation portal loads after 2 to 5 minutes.
- An attempt to log in to the vRealize Automation Rainpole portal fails with an error about incorrect user name and password.

Workaround: Perform one of the following workarounds according to the recovery operation type.

- Failover to Region B
  1. Log in to the vra01svr01a.rainpole.local appliance using SSH as the root user.
  2. Open the /usr/local/horizon/conf/domain\_krb.properties file in a text editor.
  3. Add the following list of the domain-to-host values and save the domain\_krb.properties file.  
Use only lowercase characters when you type the domain name.  
For example, as you have performed failover, you must map the rainpole.local domain to the controller in Region B:  
rainpole.local=dc51rpl.rainpole.local:389.
  4. Change the ownership of the domain\_krb.properties.  
chown horizon:www /usr/local/horizon/conf/domain\_krb.properties
  5. Open the /etc/krb5.conf file in a text editor.
  6. Update the realms section of the krb5.conf file with the same domain-to-host values that you configured in the domain\_krb.properties file, but omit the port number as shown in the following example.

```
[realms]
RAINPOLE.LOCAL = {
  auth_to_local = RULE:[1:$0$1](^RAINPOLE\.LOCAL\\.*)s/^RAINPOLE\.LOCAL/RAINPOLE/
  auth_to_local = RULE:[1:$0$1](^RAINPOLE\.LOCAL\\.*)s/^RAINPOLE\.LOCAL/RAINPOLE/
  auth_to_local = RULE:[1:$0$1](^SFO01\.RAINPOLE\.LOCAL\\.*)s/^SFO01\.RAINPOLE\.LOCAL/SFO01/
  auth_to_local = RULE:[1:$0$1](^LAX01\.RAINPOLE\.LOCAL\\.*)s/^LAX01\.RAINPOLE\.LOCAL/LAX01/
  auth_to_local = DEFAULT
  kdc = dc51rpl.rainpole.local
}
```
  7. Restart the workspace service.  
service horizon-workspace restart
  8. Repeat this procedure on the other vRealize Automation Appliance vra01svr01b.rainpole.local.

- Failback to Region A

If dc51rpl.rainpole.local becomes unavailable in Region B during failback, perform the steps for the failover case using dc01rpl.rainpole.local as the domain controller instead of dc51rpl.rainpole.local and restarting the services.

This workaround optimizes the synchronization with the Active Directory by pointing to a specific domain controller that is reachable from the vRealize Automation Appliance in the event of disaster recovery.

## vRealize Business

- **When you power on the vRealize Business appliance, the following question appears in the vSphere Web Client: "Cannot connect the virtual device IDE0:0 because no corresponding device is available on the host. Do you want to try to connect this virtual device every time you power on the virtual machine?"**

By default, the virtual CD/DVD drive of the vRealize Business appliance is set to connect at power on. When the appliance is unable to find media at bootup, the question that is described in the symptom appears.

Workaround: See VMware Knowledge Base article [2151287](#).

## Site Recovery Manager and vSphere Replication

- **After you add a second or third NIC adapter with a static IP address to the vSphere Replication appliance, the VAMI interface indicates that the IPv4 Default Gateway for the NIC adapters is incorrect.**

After adding a second NIC adapter (eth1) with a configuration containing a static IP address to the vSphere Replication appliance and restarting the appliance, the VAMI interface of the appliance displays the IPv4 Default Gateway of the original NIC adapter (eth0) as empty and the IPv4 Default Gateway of the new NIC adapter (eth1) as the original default gateway of eth0.

Adding a third NIC adapter (eth2) with a configuration containing a static IP address to the vSphere Replication appliance and restarting the appliance, the VAMI interface displays the IPv4 Default Gateway of both eth0 and eth1 as empty, while the IPv4 Default Gateway of the new NIC adapter eth2 is set to the original default gateway of eth0.

Workaround: Do not change the IPv4 Default Gateway field of both NIC adapters. This is a VAMI display issue.

## vRealize Suite Lifecycle Manager

- **New Use case deployment using vRealize Suite Lifecycle Manager results in deploying vRealize Business, vRealize Operations Manager, and vRealize Log Insight virtual appliances with incorrect size.**

When you deploy the IT Automating IT, Intelligent Operations, or Micro-Segmentation uses case by using vRealize Suite Lifecycle Manager, vRealize Suite Lifecycle Manager does not respect the deployOption setting for the size of the virtual appliances. All appliances are deployed as large-size. The issue appears in both cases, using the UI wizard and using a JSON configuration file.

Workaround: Manually resize the memory and vCPU to their sizes in VMware Validated Design as follows:

Node Type	New Amount of Memory	New Number of vCPUs
vRealize Business Remote Data Collector	2 GB	4
vRealize Operations Manager Master, Replica, and Data Nodes	32 GB	8
vRealize Operations Manager Remote Collector Nodes	4 GB	2
vRealize Log insight Master and Worker Nodes	16 GB	8

## VMware Validated Design Content

- **New BGP configuration values are not available when you configure NSX for vSphere in Region A.**

BGP configuration values are not present in Step 6b in [Configure the Distributed Logical Router for Dynamic Routing in Shared Edge and Compute Cluster in Region A](#).

Workaround: Use the following values:

Setting	Value
Enable BGP	Selected
Enable Graceful Restart	Selected
Local AS	65000

- **New Segment ID allocation values are not available when you configure NSX logical network in Region B**

Segment ID allocation values are not present in Step 2d in [Configure the NSX Logical Network for the Management Cluster in Region B](#).

Workaround: Use the following values:

Setting	Value
Segment ID pool	6000-6200
Enable Multicast addressing	Selected
Multicast addresses	239.5.0.0-239.5.255.255

**Note:** Universal Segment ID pool automatically populates from the primary NSX Manager.

- **New Reconnecting vRealize Orchestrator with vRealize Automation when replacing certificates for the Cloud Management Platform in Region A is no longer necessary.**

Step 1 in procedure [Update the vRealize Automation Certificate on vRealize Orchestrator and vRealize Business in Region A](#) is no longer required.

Workaround: Skip Step 1 in procedure [Update the vRealize Automation Certificate on vRealize Orchestrator and vRealize Business in Region A](#).

- **New The minimum requirements for the vRealize Automation 7.3 IaaS Windows Servers in this version of VMware Validated Design are different from the official vRealize Automation requirements.**

The minimum memory requirements for the vRealize Automation IaaS Windows Servers in the *Architecture and Design* and *Planning and Preparation* documents are 4 GB for the IaaS Web Server, IaaS Manager Server, and Proxy Agent nodes, and 6 GB for the IaaS DEM Worker nodes. According to the official vRealize Automation product documentation, you must allocate 8 GB memory to each vRealize Automation Windows Server node. See <http://docs.vmware.com/en/vRealize-Automation/7.3/com.vmware.vra.install.upgrade.doc/GUID-47F45416-D297-4C38-A1C0-06E6DFC1EBB5.html>.

Workaround: When you deploy the vRealize Automation IaaS Windows Servers for a new environment, set the minimum memory for each IaaS Windows Server to 8 GB of memory.

When you upgrade from an earlier release, update the memory for each IaaS Windows Server to 8 GB.