



# VMware Validated Design for Software-Defined Data Center 4.0 Release Notes

VMware Validated Design for Software-Defined Data Center 4.0.1 | 6 APR 2017

VMware Validated Design for Software-Defined Data Center 4.0 | 2 MAR 2017

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 4.0](#)
- [VMware Software Components in the Validated Design](#)
- [What's New](#)
- [Internationalization](#)
- [Compatibility](#)
- [Installation](#)
- [Lifecycle of the VMware Software Components](#)
- [Caveats and Limitations](#)
- [Resolved Issues](#)
- [Known Issues](#)

## About VMware Validated Design for Software-Defined Data Center 4.0

VMware Validated Designs provide 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 Designs are 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 the VMware Validated Designs. 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 4.0 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 VMware's Customer Experience Improvement Program ("CEIP"). VMware recommends that you join 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 VMware's CEIP for the products that are part of VMware Validated Designs, see the documentation for each product.

Product Group and Edition	Product Name	Product Version
VMware vSphere Enterprise Plus	ESXi	6.5 a
	vCenter Server Appliance	6.5 a
	vSphere Update Manager	6.5 a
VMware vSAN Standard or higher	vSAN	6.5
VMware vSphere Replication	VMware vSphere Replication	6.5
VMware Site Recovery Manager Enterprise	VMware Site Recovery Manager	6.5
VMware NSX for vSphere Enterprise	NSX for vSphere	6.3 * **
VMware vRealize Automation Advanced or higher	vRealize Automation	7.2
	vRealize Orchestrator	7.2
	vRealize Orchestrator Plug-in for NSX	1.0.4
VMware vRealize Business for Cloud Advanced	vRealize Business for Cloud	7.2
VMware vRealize Operations Manager Advanced or higher	vRealize Operations Manager	6.4
	vRealize Operations Management Pack for NSX for vSphere	3.5
	vRealize Operations Management Pack for vRealize Log Insight	1.0.1
	vRealize Operations Management Pack for vRealize Automation	2.1
	vRealize Operations Management Pack for Storage Devices	6.0.5
VMware vRealize Log Insight	vRealize Log Insight	4.0
	vRealize Log Insight Content Pack for NSX for vSphere	3.5
	vRealize Log Insight Content Pack for vSAN	2.0
	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 vRealize Operations Manager 6.x	1.7
	vRealize Log Insight Content Pack for Microsoft SQL Server	3.1
VMware vSphere Data Protection	vSphere Data Protection	6.1.3

\* Shortly before VMware Validated Designs 4.0 released, VMware released the NSX for vSphere 6.3.1 patch which includes an important hotfix. VMware Validated Designs supports this hotfix and VMware recommends that you apply it immediately

recommends that you apply it immediately.

**\*\* Important:** If you are running VMware Validated Design 4.0, you must apply the vCenter Server 6.5f patch. vCenter Server 6.5 has been updated to address the problems mentioned in VMware Knowledge Base article [000051124](#).

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. This 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.

## What's New

VMware Validated Design for Software-Defined Data Center 4.0 provides the following new features:

- Updated Bill of Materials that incorporates new product versions
- All new SDDC roles and personas guidance
- Platform Services Controllers in each region are now behind an NSX load balancer
- Use of host profiles to deploy ESXi on the hosts in the management and the shared edge and compute pods.
- New operational guidance for certificate replacement of the SDDC management cluster
- Support for SHA-2 Certificates
- NSX distributed logical router for the shared edge and compute cluster
- Improved free space recommendations for vSAN and NFS datastores
- Less nodes required for the analytics cluster of vRealize Operations Manager
- Now using syslog to send log data from vCenter Server and Platform Services Controller to vRealize Log Insight
- Implemented SSL for log forwarding
- Incorporated the use of vSphere Update Manager for upgrading ESXi hosts
- Adoption of service accounts for secure application-to-application communication
- **New** Remote Office and Branch Office (ROBO) guidance that extends the VMware Validated Design for Software-Defined Data Center with details about connecting smaller remote locations to primary data centers

VMware Validated Design for Software-Defined Data Center 4.0.1 updates the 4.0 guides to resolve issues with Platform Services Controller High Availability Load Balancer host name usage, Platform Services Controller Load Balancer deployment, and other technical points. You can find details on these changes in the *Updated Information* section of each guide that VMware modified for the 4.0.1 release.

For more information, see the [VMware Validated Design for Software-Defined Data Center 4.0](#) 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 4.0, 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 4.0 documentation. For product download information, and guides access, see the [VMware Validated Design for Software-Defined Data Center 4.0](#) 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 still supported.	Apply the <i>VMware Validated Design Upgrade</i> documentation to bring the VMware environment to a fully supported state
The version of VMware Validated Design that you are using and the next version have both already entered the EOSL stage	Because the <i>VMware Validated Design Upgrade</i> 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.

## Resolved Issues

The resolved issues are grouped as follows.

- [VMware Validated Design Content](#)

### VMware Validated Design Content

- **Some documents incorrectly use the name LAX01PSC01 for the Platform Services Controller High Availability Load Balancer name**

Some VMware Validated Design for Software-Defined Data Center documents instruct you to use a fully qualified domain name (FQDN) of lax01psc01.lax01.rainpole.local and a NSX Load Balancer name of LAX01PSC01.

Note: Because this usage was prevalent in the Deployment for Region B guide VMware has removed this guide temporarily.

Where you see LAX01PSC01.lax01.rainpole.local or LAX01PSC01 in the documentation, replace it with an FQDN of lax01psc51.lax01.rainpole.local and an NSX Load Balancer of LAX01PSC51.

- **Documentation incorrectly instructs you to deploy an NSX Load Balancer in Region B to the Region A's vSAN datastore**

Some VMware Validated Design for Software-Defined Data Center documents instruct you to use the Management vSAN datastore SFO01A-VSAN01-MGMT01, located in Region A, to deploy the NSX Load Balancer for Platform Services Controller High Availability residing in Region B.

Where you see the vSAN datastore SFO01A-VSAN01-MGMT01 in the context of deploying the NSX Load Balancer for Platform Services Controller High Availability residing in Region B replace it with vSAN datastore LAX01A-VSAN01-MGMT01.

- **Documentation incorrectly instructs you to use a tool other than CertGenVVD to generate certificates**

The topic "Generate Certificates for the Cloud Management Platform in Region A" in the *VMware Validated Design Deployment for Region A* documentation instructs you to use the vRealize Certificate Generation Tool (certgen.sh) to generate certificates for vRealize Automation, vRealize Orchestrator and vRealize Business. The script is also referenced in the topic "VMware Scripts and Tools" in the *VMware Validated Design Planning and Preparation* documentation.

The preferred tool with which to generate certificates for these components is the VMware Validated Design Certificate Generation Utility (CertGenVVD). While you can follow the "Generate Certificates for the Cloud Management Platform in Region A" procedure, using certgen.sh to generate certificates, with no defect in the deployment or operation of this VMware Validated Design, we encourage you to use the CertGenVVD, which is the preferred tool to use when deploying this VMware Validated Design.

Workaround: Use CertGenVVD to generate Certificate Signing Request (CSR), OpenSSL CA-signed certificates, and Microsoft CA-signed certificates for all VMware products included in the VMware Validated Design. In the context of this VMware Validated Design, you use the CertGenVVD tool to save time in creating signed certificates. To learn more about the VMware Validated Design Certificate Generation Utility, see VMware Knowledge Base article [2146215](#).

## Known Issues

The known issues are grouped as follows.

- [vSphere](#)
- [NSX for vSphere](#)
- [vRealize Automation](#)
- [vRealize Orchestrator](#)
- [vRealize Operations Manager](#)
- [vRealize Log Insight](#)
- [vSphere Data Protection](#)
- [VMware Validated Design Content](#)
- [VMware Validated Design for Remote Office and Branch Office](#)

## vSphere

- **New** When you apply a host profile that has the vMotion TCP/IP stack configured, the **VMkernel gateway for the vMotion TCP/IP stack on the target ESXi hosts is not configured**  
After you modify the vMotion TCP/IP stack on a management or compute ESXi host in Region A and Region B at installation or upgrade to vSphere 6.5, you extract a host profile from this host. When you apply the profile on the hosts in the management clusters and shared edge and compute clusters in both regions, the VMkernel gateway for the vMotion stack is not configured on the hosts. The **Host Compliance** state is Not Compliant and you see the following description:

IP route configuration doesn't match the specifications  
Number of IPv4 routes did not match

Workaround: Update manually the VMkernel gateway for the vMotion TCP/IP stack on each of the hosts in the management clusters and the shared edge and compute clusters.

1. Log in to vCenter Server.
  1. Open a Web browser and go to <https://mgmt01vc01.sfo01.rainpole.local>.
  2. Log in using the following credentials.

Setting	Value
User name	administrator@vsphere.local
Password	vsphere_admin_password

2. In the **Navigator**, click **Hosts and Clusters**.
3. Expand each vCenter Server instance and navigate to the cluster.
  - mgmt01vc01.sfo01.rainpole.local > SFO01 > SFO01-Mgmt01
  - comp01vc01.sfo01.rainpole.local > SFO01 > SFO01-Comp01
  - mgmt01vc51.lax01.rainpole.local > LAX01 > LAX01-Mgmt01
  - comp01vc51.lax01.rainpole.local > LAX01 > LAX01-Comp01
4. Select a ESXi host in the cluster.
5. On the **Configure** tab, select **TCP/IP configuration > vMotion** and click **Edit**.
6. In the **Edit TCP/IP Stack Configuration** dialog box, click **Routing**, enter the following IP address in the **VMkernel gateway** text box and click **OK**.

Cluster	VMkernel Gateway IP Address
mgmt01vc01.sfo01.rainpole.local > SFO01 > SFO01-Mgmt01	172.16.12.253
comp01vc01.sfo01.rainpole.local > SFO01 > SFO01-Comp01	172.16.32.253
mgmt01vc51.lax01.rainpole.local > LAX01 > LAX01-Mgmt01	172.17.12.253
comp01vc51.lax01.rainpole.local > LAX01 > LAX01-Comp01	172.17.32.253

7. Repeat this procedure on each of the other ESXi hosts in clusters in both regions.

## NSX for vSphere

- **Auto-redirect from the HTTP to HTTPS login page of the vRealize Operations Manager analytics cluster does not work**

When you log in to <http://vrops-cluster-01.rainpole.local>, the NSX load balancer does not redirect you to the HTTPS URL <https://vrops-cluster-01.rainpole.local> and you see the This site cannot be reached error.

Workaround: On the SFOMGMT-LB01 and LAXMGMT-LB01 NSX load balancers, create an empty load balancer pool and assign it as **Default Pool** to the VROPS\_REDIRECT virtual server that handles the HTTP-to-HTTPS redirects.

## vRealize Automation

- **After failover or failback during disaster recovery, login to the vRealize Automation Rainpole portal takes several minutes and an attempt for test login to vRealize Orchestrator fails**

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 times out
  - 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 for a Test Login to vRealize Orchestrator from the vRealize Orchestrator Control Center at <https://vra01vro01a.rainpole.local:8283/vco-controlcenter/> by using the svc-vra user account fails with the following error message:

Error: I/O error on POST request for "https://vra01svr01.rainpole.local:443/SAAS/t/rainpole/auth/oauth/token?grant\_type=password": Read timed out; nested exception is java.net.SocketTimeoutException: Read timed out

- Login 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 file `/usr/local/horizon/conf/domain_krb.properties` 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:  
`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 file `/etc/krb5.conf` 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 vRealize Automation appliance in the event of disaster recovery.

- **vRealize Automation Converged Blueprint with NSX routed networks fails with the error "I/O error on GET request for https://vra01vro01.rainpole.local:8281/vc/api/catalog/NSX/Nic/ : read timed out;nested exception is java.net.SocketTimeoutException: Read timed out"**

All subsequent provisioning requests 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:

1. 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.

- **Converged blueprint provisioning requests in vRealize Automation may fail in high workload churn environments**

In very high workload churn environments, converged blueprint provisioning requests in vRealize Automation may fail with one of the following error messages.

- Timeout Customizing machine
- Failed while updating distributed router interfaces on controller for edge
- The following component requests failed: [Error code: 44010 ] - [Error Msg: Error executing vRealize Orchestrator workflow [VSM response error (836): A controller is not available for this operation. (Workflow: Create logical switch / Scriptable task (item1)#4)]]
- java.lang.RuntimeException: Failed to perform operation connectEdgeInterface after 5 retries. Aborting.  
(Workflow:Connect logical switch to router / Scriptable task (item1)#23)

Workaround: None

- **vRealize Automation multi-machine VM provisioning request fails with an exception "java.lang.IllegalArgumentException: Error updating virtual wire backings"**

A Converged blueprint provisioning request in vRealize Automation fails with the following error message:

java.lang.IllegalArgumentException: Error updating virtual wire backings: the input list of network ids [dvportgroup-4659] of length 1 does not match the length 0 of the workflow output array

Workaround: See VMware Knowledge Base article [2148946](#).

- **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 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
```

## vRealize Orchestrator

- **vRealize Orchestrator nodes show a Not Responding status**

Loss of network connectivity between vRealize Orchestrator and vRealize Log Insight might cause the vRealize Orchestrator nodes to become unresponsive.

The /var/log/vmware/vco/app-server/catalina.out log file reports the following messages:

```
log4j:ERROR Attempted to append to closed appender named [SOCKET]. tcp: DOWN
(org.productivity.java.syslog4j.SyslogRuntimeException: java.net.NoRouteToHostException: No route to host)
INFO <134>Aug 19 15:00:00 vra01vro01b.rainpole.local vco: ae21b98e-1cff-4142-9ecc-9eb1f2f4ee52 prio:INFO
```

The /var/log/vmware/vco/app-server/server.log log file reports the following messages:

```
9444 2016-09-15 01:49:49.123+0000 [Shared Factory release pool] DEBUG {} [VSOFactoryClient] << Disconnecting Shared
Factory !
9445 2016-09-15 01:49:49.123+0000 [Shared Factory release pool] DEBUG {} [VSOFactoryClient] Disconnect from server
9446 2016-09-15 01:49:35.777+0000 [http-nio-0.0.0.0-8281-exec-313] DEBUG {} [TokenAuthenticationFilter] Token
Authentication Authorization header found for user 'cafe-PCZ_HVulmA@vsphere.local'
9447 2016-09-15 01:47:14.194+0000 [Heartbeat] WARN {} [HeartBeatServiceImpl] Unable to send heartbeat signal:
9448 org.springframework.jdbc.CannotGetJdbcConnectionException: Could not get JDBC Connection; nested exception is
org.apache.tomcat.jdbc.pool.PoolExhaustedException: [Heartbeat] Timeout: Pool empty. Unable to fetch a connection in 30
seconds, none available[size:1; busy:1; idle:0; lastwait:30000].
```

Workaround: After you restore the network connectivity between vRealize Orchestrator and vRealize Log Insight, restart the unresponsive vRealize Orchestrator nodes. After nodes are running again, log in to a Control Center and verify the the current status of the Orchestrator server service is Running for all nodes.

## 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.

- **vRealize Operations Manager health badges might be unavailable in the vSphere Web Client**  
When vCenter Server is registered in vRealize Operations Manager using its fully-qualified domain name (FQDN) and not using its IP address, the health badges are missing from the **Summary** and **Monitor** tabs for the inventory objects in vSphere Web Client. You cannot see the health status of

**Monitor** tabs for the inventory objects in vSphere Web Client. You cannot see the health status of vCenter Server, clusters, ESXi hosts, virtual machines, and so on.

Workaround: Use one of the following approaches:

- To be able to view the health badges in the vSphere Web Client, see VMware Knowledge Base article [2145264](#).
- To proceed with monitoring your environment until the health badges become available in the vSphere Web Client, log in to vRealize Operations Manager at <https://vroops-cluster-01.rainpole.local>.

- **You might not be able to access vRealize Operations Manager from the vSphere Web Client in the case of many simultaneous requests for access**

vRealize Operations Manager does not register with vCenter Server with the Virtual IP (VIP) address that is allocated on the load balancer but with the address of an individual node from the analytics cluster. As a result, when you start the vRealize Operations Manager user interface from the vSphere Web Client, the vSphere Web Client redirects you to this node instead of to the load-balanced VIP. The access to the vRealize Operations Manager user interface is not balanced if you launch it from the vSphere Web Client. The node, where the vSphere Web Client redirects you, might become overloaded and you might not be able to access vRealize Operations Manager.

Workaround: Log in to vRealize Operations Manager directly at the VIP address <https://vroops-cluster-01.rainpole.local> instead of from the vSphere Web Client.

- **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/vcroops/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: Perform the following tasks:

- Ensure that all NTP servers that are used by both the analytics and remote collector nodes are accessible.
- Update the `ntp.conf` file with new NTP servers on each vRealize Operations Manager node if the original NTP servers are no longer available.

- **Answers to Monitoring goals always show the default values**

In the Define Monitoring Goals dialog box, the answers for Monitoring goals are not retained if you change them. Every time you reload the page, 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 failovers to Region B and failbacks to Region A of the Cloud

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 the vRealize Operations Manager virtual machines, the collection state of the vRealize Automation Adapter is Failed on the **Administration > Solutions** page of the vRealize Operations Manager user interface at <https://vrops-cluster-01.rainpole.local>.

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

## vRealize Log Insight

- **vRealize Automation Content Pack for vRealize Log Insight pulls no events from the vRealize Automation vSphere Proxy Agents because of invalid event marker**

In the vRealize Automation Log Insight Windows agent configuration, the default regular expression of the event marker for the `vra-agent-vcenter` log file is incorrect. As a result, the vRealize Log Insight agent does not locate events of interest in this log file and does not forward log information to vRealize Log Insight.

Workaround: Apply a valid event marker for vSphere Proxy Agent events by performing the following steps:

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

Region	vRealize Log Insight URL
Region A	<a href="https://vrli-cluster-01.sfo01.rainpole.local">https://vrli-cluster-01.sfo01.rainpole.local</a>
Region B	<a href="https://vrli-cluster-51.lax01.rainpole.local">https://vrli-cluster-51.lax01.rainpole.local</a>

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 enter the following value in the **Event Marker** text box.  
`^d{4}-d{1,2}-d{1,2}T\d{1,2}:\d{1,2}:\d{1,2}.\d{1,3}Z4`
6. Click **Save Agent Group**.

- **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 4.0, 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	<a href="https://vrli-cluster-01.sfo01.rainpole.local">https://vrli-cluster-01.sfo01.rainpole.local</a>
Region B	<a href="https://vrli-cluster-51.lax01.rainpole.local">https://vrli-cluster-51.lax01.rainpole.local</a>

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

6. Click **Save Agent Group**.

- **After you upgrade the vRealize Log Insight agent on an SDDC management component, the agent might fail to connect to the vRealize Log Insight cluster**

After you upgrade the vRealize Log Insight and the vRealize Log Insight agent on an SDDC management component, the agent does not send log information to the cluster. On the

**Administration > Agents** of the vRealize Log Insight user interface, the report about the agent instance shows a Last Active time greater than 5 minutes.

In vRealize Log Insight 4.0, the SSL connection between cluster and agents is enabled by default even if the **Administration > Configuration > SSL > API Server SSL > Require SSL**

**Connection** is disabled. Because of a mismatch in the SSL port configuration on the cluster and on the agent, the agent is not able to connect to the cluster and send log data.

Workaround: See VMware Knowledge Base article [2148837](#).

## vSphere Data Protection

- **The vSphere Data Protection appliance is disconnected while backing virtual machines up, or the backup job or restore job for them shows no progress beyond 92%**

When you back up virtual machines with multiple VMDKs on a vSAN datastore, such as the vRealize Log Insight nodes, vSphere Data Protection stops responding, or the backup job or restore job remains at 92% for days.

Workaround: Deploy an external vSphere Data Protection proxy on the vSAN datastore and disable the SAN mode check on the proxy. See VMware Knowledge Base article [2149101](#).

- **After you restore a Platform Services Controller appliance, you might not be able to enable the Bash shell or some services might not be started**

After you restore a Platform Services Controller appliance, you might encounter one or more of the following issues:

- If you run the `shell.set --enabled True` command to enable the Bash shell on a restored Platform Services Controller virtual appliance, the following error might appear:

```
Command> shell.set --enabled True
Unknown command: 'shell.set'
Command> shell
Shell is disabled
```

- Running the `psc_restore` script fails to restore the Platform Services Controller. Not all services of Platform Services Controller start, synchronization with the partner Platform Services Controller fails, and so on.

Workaround: Restore the Platform Services Controller from another restore point in vSphere Data Protection.

- **An error message is reported during backup of the vRealize Automation VMs by using vSphere Data Protection**

During backup of the vRealize Automation VMs, the following error message appears in the vSphere Events section:

Failed to add disk scsi0:4.

Regardless of the error message, the backup job completes successfully. If you restore the VMs from the backup, the process completes and validates successfully.

Workaround: None.

- **New Attempting to configure vSphere Data Protection with vCenter Server fails on allocating storage and CPU and memory.**

Errors appear when you perform the following deployment tasks:

1. Deploy the vSphere Data Protection appliance.
2. Replace the default certificate on the appliance in Region A or in Region B.
3. Try to configure the resources of the appliance and register it with the Management vCenter Server.

During the device allocation and CPU and Memory phases, the following errors appear and you cannot complete the configuration:

On the Device Allocation page	On the CPU and Memory page
Failed to retrieve the list of datastores.	Failed to retrieve the current hardware configuration.
Failed to compare the current resource settings with the minimum hardware requirements.	Failed to retrieve the hardware information.
The list of available datastores is empty.	The list of Virtual CPUs and Memory allocated are both 0.

On the vSphere Data Protection appliance, the `/space/vdp/logs/vdp_logs/vdr/server_logs/vdr-configure.log` file contains the following entries:

```
2017-04-10 09:04:17,623 INFO [http-nio-8543-exec-7]-network.NetworkInfoApi: Found IP Address: [172.18.11.81] link local? [false], site local? [true], loopback? [false]
2017-04-10 09:04:17,624 INFO [http-nio-8543-exec-7]-network.NetworkInfoApi: Found IP Address: 172.18.11.81
2017-04-10 09:04:18,255 ERROR [http-nio-8543-exec-8]-vi.ViJavaAccess: getPoweredOnVmByIpAddr(): Did not find powered on AVE virtual machine with IP Address [172.18.11.81]
2017-04-10 09:04:18,308 ERROR [http-nio-8543-exec-8]-storage.VirtualMachineServiceImpl: Unable to collect the correct hardwareinfo values java.lang.NullPointerException
    at com.emc.vdp2.common.storage.VirtualMachineServiceImpl.getMaxVcpuForVM(VirtualMachineServiceImpl.java:551)
    at
com.emc.vdp2.common.storage.VirtualMachineServiceImpl.getMinimumHardwareInfo(VirtualMachineServiceImpl.java:1349)
    at com.emc.vdp2.config.services.StorageService.getHotswapCheckResult(StorageService.java:323)
    at com.emc.vdp2.config.services.StorageService.hotswapCheck(StorageService.java:307)
    at sun.reflect.NativeMethodAccessorImpl.invoke0(Native Method) at
sun.reflect.NativeMethodAccessorImpl.invoke(Unknown Source)
    at sun.reflect.DelegatingMethodAccessorImpl.invoke(Unknown Source)
    at java.lang.reflect.Method.invoke(Unknown Source)
```

Workaround: See <http://support.emc.com/kb/501443>. You must log in to the EMC Knowledge Base system.

- **Backup of a VM that requires disk consolidation fails**

If you try to back up a VM that requires disk consolidation, the job fails due to a disk lock error. vSphere Data Protection can not release the lock and perform backup. If you try to power on the VM

or consolidate its disks, the same error occurs.

Workaround: Perform either of the following workarounds:

- Migrate the VM that experiences the issue to a different ESXi host and consolidate the disk manually. After successful consolidation, back up the VM.
- Migrate the VM that experiences the issue to a different datastore and consolidate the disk manually. After successful consolidation, back up the VM.

## VMware Validated Design Content

- **New You cannot directly replace the certificate of the vSphere Data Protection appliances following VMware Validated Design Deployment in Region A and VMware Validated Design Deployment in Region B because SSH is not enabled**

You cannot install the certificate for vSphere Data Protection in Region A and Region B during deployment following the instructions in *Install a CertGenVVD-Generated Certificate on vSphere Data Protection in Region A* and *Install a CertGenVVD-Generated Certificate on vSphere Data Protection in Region B* because Secure Shell (SSH) is not enabled in the appliances. The documentation is missing the instructions about turning SSH on after you deploy the appliances.

Workaround: Before you replace the certificate of vSphere Data Protection, enable SSH in the following way:

1. Open the remote console to the mgmt01vdp01 and mgmt01vdp51 appliance from the vSphere Web Client.
2. Edit the sshd\_config file.
  1. Open the file in the vi editor.

```
vi /etc/ssh/sshd_config
```
  2. Remove the # comment from the beginning of the line `#PermitRootLogin yes`.
  3. Save the changes.

```
:wq!
```
3. Restart the SSH service to apply the configuration.

```
/etc/init.d/sshd restart
```
4. Log out and close the console of the appliance in the vSphere Web Client.

## VMware Validated Design for Remote Office and Branch Office

- **New After you register the ROBO vCenter Server with vRealize Operations Manager in the hub, the vSphere Web Client does not show the health badges for the inventory objects of the ROBO vCenter Server**

After you connect vRealize Operations Manager in the hub to the ROBO vCenter Server, the health badges for the inventory objects of the ROBO vCenter Server are missing from the **Summary** and **Monitor** tabs in the vSphere Web Client. You cannot see the health status of the ROBO vCenter Server, its clusters, managed ESXi hosts and virtual machines, and so on, in the vSphere Web Client.

Workaround: None.

- **New vRealize Orchestrator becomes unresponsive if you add many vCenter Server instances simultaneously or concurrently**

vRealize Orchestrator becomes unresponsive if you run a workflow that uses a REST host. An attempt to run the REST host workflow fails with an error that is similar to:

Uninitialized keystorejava.security.KeyStoreException: Uninitialized keystore Uninitialized keystore exception

This situation might occur when you add multiple vCenter Server instances to a vRealize

Orchestrator instance simultaneously by using the Add vCenter Server workflow causing corruption of the keystore.

Workaround: Consult VMware Global Support Services.

- **New Performance, Cost, and Network and Security tabs are missing from the vRealize Automation Data Collection page on faulty installation**

This situation can occur when you uninstall and then re-install vRealize Automation using a new name for the data collection agent. The new agent collects data from the same endpoint using the new name to record information to the database. However, the name of the original agent still exists in the database, causing records to be stored using two different names.

Workaround: Consult VMware Global Support Services.

- **New Logging in using Active Directory credentials to the vRealize Automation Tenant Portal or the vRealize Orchestrator Java Client takes an exponentially long time to authenticate**

The vRealize Automation Appliance's Domain Name System (DNS) Service records (SRV record) point to rainpole.local, which includes all domain controllers in the environment, including the geographically remote or slow linked domain controllers located in the remote office or branch office (ROBO) site. This results in user login sessions using non-optimized paths in order to reach the Active Directory Domain Controllers, resulting in the system timing out before successfully authenticating. You may observe the following symptoms when the environment is not optimized:

- The vRealize Automation Converged Blueprint deployments fail with the following exception:  
Read timed out; nested exception is --java.net.SocketTimeoutException: Read timed out
- Logging into the vRealize Automation Tenant Portal takes longer than usual.
- Logging into the vRealize Orchestrator Java client, with vRealize Orchestrator configured to use vRealize Automation as its authentication source, takes longer than usual.

Workaround:

1. Edit the configuration file `/etc/krb5.conf` on both vRealize Automation nodes to include the following entry in the `[realms]` section, adjusted to use the domain name in use by your environment: `kdc = dc01rpl.rainpole.local`
2. Restart the Horizon Workspace service on the vRealize Automation nodes using the following command.  
`service horizon-workspace restart`

For more information, see "[About Domain Controller Selection](#)" in *vRealize Automation Information*, and VMware Knowledge Base article [2144953](#).