

Monitoring and Alerting

30 OCT 2018

VMware Validated Design 4.3

VMware Validated Design for Software-Defined Data
Center 4.3



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

Copyright © 2016–2018 VMware, Inc. All rights reserved. [Copyright and trademark information.](#)

Contents

About VMware Validated Design Monitoring and Alerting	4
1 Enabling Alerts in vRealize Log Insight	5
View the Full List of Alerts for a Management Product	6
Enable the Alerts for vSphere Resources	7
Enable the Alerts for vSphere Networking	10
Enable the Alerts for Storage Resources	13
Enable the Alerts for vSAN	16
Enable the Alerts for NSX for vSphere	19
Enable the Alerts for vRealize Operations Manager	21
Enable the Alerts for vRealize Automation	23
Enable the Alerts for Microsoft SQL Server for vRealize Automation	26
2 Creating Custom SDDC vRealize Operations Dashboards	29
SDDC Capacity and Utilization Overview Dashboards	30
Configure a Dashboard That Provides an Overview of the SDDC Operation	31
Create Applications in vRealize Operations Manager for the SDDC Components	31
Collect the SDDC Objects in a Group	37
Configure a Dashboard That Provides an Overview of the SDDC State	38
3 Configure vRealize Operations Manager to Notify of SDDC Issues	43
Create Notifications in vRealize Operations Manager	43
List of Notifications for vRealize Operations Manager	44
4 Monitor VADP Based Backup Solution Jobs by Email	50
5 Configure vRealize Automation System Notification Events	51

About VMware Validated Design Monitoring and Alerting

VMware Validated Design Monitoring and Alerting provides step-by-step instructions about configuring vRealize Operations Manager and vRealize Log Insight for monitoring of the operations in the software-defined data center (SDDC). This documentation also discusses enabling notifications about issues in your environment and operating an SDDC based on the VMware Validated Design™ for SDDC.

After you deploy the Software-Defined Data Center from this VMware Validated Design, you can monitor the parameters that are most important for environment management by using a set of dashboards for alerts and log events.

Intended Audience

The *VMware Validated Design Monitoring and Alerting* documentation is intended for cloud architects, infrastructure administrators, cloud administrators, and cloud operators who are familiar with and want to use VMware software to deploy in a short time and manage an SDDC that meets the requirements for capacity, scalability, backup and restore, and extensibility for disaster recovery support.

Required VMware Software

VMware Validated Design Monitoring and Alerting is compliant and validated with certain product versions. See *VMware Validated Design Release Notes* for more information about supported product versions.

Enabling Alerts in vRealize Log Insight

1

Use the vRealize Log Insight known event signature engine to monitor key events. You can use a set of alerts to send to vRealize Operations Manager and through SMTP for operations team notification.

With the integration between vRealize Log Insight and vRealize Operations Manager you can implement the following cross-product event tracking:

- Send alerts from vRealize Log Insight to vRealize Operations Manager, which maps them to the target objects.
- Launch in context from a vRealize Operations Manager object to the objects logs in vRealize Log Insight.
- Launch in context from a vRealize Log Insight event to the objects in vRealize Operations Manager.

For applications that are failed over between regions, such as vRealize Automation and vRealize Operations Manager, configure alerting in both regions to avoid missing any alerts when applications move between regions.

Procedure

1 [View the Full List of Alerts for a Management Product](#)

Explore alerts and queries that are available in vRealize Log Insight for the management products in the SDDC such as vSphere, NSX for vSphere, vRealize Automation, and so on. Content packs for these products handle the alerts and queries.

2 [Enable the Alerts for vSphere Resources](#)

Use the built-in problem and alert signatures in vRealize Log Insight for an ESXi host and a vCenter Server to enable alerts for these components and map these alerts to the vRealize Operations Manager inventory. For each alert, you create one instance for the management data center and one instance for the shared edge and compute data center in each region.

3 [Enable the Alerts for vSphere Networking](#)

Use the in-built problem and alert signatures in vRealize Log Insight and create alerts for network-related events and map them to the vRealize Operations Manager inventory. For each alert, you create one instance for the management data center and one instance for the shared edge and compute data center in each region.

4 [Enable the Alerts for Storage Resources](#)

Use the built-in problem and alert signatures in vRealize Log Insight to create alerts about storage and map these alerts to the vRealize Operations Manager inventory. For each alert, you create one instance for the management data center and one instance for the shared edge and compute data center in each region.

5 [Enable the Alerts for vSAN](#)

Use the built-in problem and alert signatures in vRealize Log Insight to create alerts for vSAN monitoring and map them to the vRealize Operations Manager inventory. For each alert, you create one instance for the management data center in each region. This validated design uses vSAN only for the SDDC management components. If you use vSAN also for your tenant workloads, configure alerts accordingly.

6 [Enable the Alerts for NSX for vSphere](#)

Create alerts using the in-built problem and alert signatures in vRealize Log Insight for NSX for vSphere and direct them to the vRealize Operations Manager inventory. For each alert, you create one instance for the NSX Manager for the management cluster and one instance for the NSX Manager for the shared edge and compute cluster in the region.

7 [Enable the Alerts for vRealize Operations Manager](#)

Use the built-in problem and alert signatures in vRealize Log Insight for vRealize Operations Manager. You create one instance of each alert in Region A and in Region B because the vRealize Operations Manager instance works in the context of both management and compute resources in each region. The SDDC also contains one analytics cluster that is failed over to Region B and you receive alerts only about it.

8 [Enable the Alerts for vRealize Automation](#)

Use the in-built problem and alert signatures in vRealize Log Insight for vRealize Automation. You create one instance of each alert in Region A and in Region B because the vRealize Automation instance in the SDDC works in the context of the compute resources in each region. The environment also contains one vRealize Automation deployment that is failed over to Region B and you receive alerts only about it.

9 [Enable the Alerts for Microsoft SQL Server for vRealize Automation](#)

Use the built-in problem and alert signatures in vRealize Log Insight for the Microsoft SQL Server for vRealize Automation. For each alert, you create one instance for each region so that alerts are still available if the Microsoft SQL Server instance is failed over to Region B.

View the Full List of Alerts for a Management Product

Explore alerts and queries that are available in vRealize Log Insight for the management products in the SDDC such as vSphere, NSX for vSphere, vRealize Automation, and so on. Content packs for these products handle the alerts and queries.

Procedure

1 Open the vRealize Log Insight user interface.


a Open a Web browser and go to the following URL.

Region	vRealize Log Insight URL
Region A	https://sfo01vrli01.sfo01.rainpole.local
Region B	https://lax01vrli01.lax01.rainpole.local

b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vri_admin_password</i>

2 Locate the content pack for the management product.

a In the vRealize Log Insight user interface, click the configuration drop-down menu icon  and select **Content Packs**.

b Under **Installed Content Packs**, select any content pack.

c Click **Alerts** or **Queries** tab to view the full list of alerts or queries for the product.

Enable the Alerts for vSphere Resources

Use the built-in problem and alert signatures in vRealize Log Insight for an ESXi host and a vCenter Server to enable alerts for these components and map these alerts to the vRealize Operations Manager inventory. For each alert, you create one instance for the management data center and one instance for the shared edge and compute data center in each region.

For basic monitoring of the vSphere components, use the following alerts:

Table 1-1. vSphere Alerts in vRealize Log Insight

Alert Name	Purpose	Severity
*** CRITICAL *** ESXi: Core dump detected	This alert indicates the failure of a component in the ESXi host. This problem can lead to failing VMs and ESXi host PSODs.	Critical
*** CRITICAL *** Hardware: Physical event detected	This alert notifies when physical hardware events have been detected and that indicate a hardware problem. In normal conditions, this alert returns no results. The following types of hardware events are returned: <ul style="list-style-type: none"> ■ Advanced Programmable Interrupt Controller (APIC) ■ Machine Check Exception (MCE) ■ Non-Maskable Interrupt (NMI) 	Critical
Hardware: Faulty memory detected	During the previous start of an ESXi host, faulty memory was detected. You might replace the memory, unless you see a corresponding corrected message.	Critical

Table 1-1. vSphere Alerts in vRealize Log Insight (Continued)

Alert Name	Purpose	Severity
*** CRITICAL *** ESXi: Stopped logging	This alert notifies when an ESXi host has stopped sending syslog events to a remote server.	Critical
*** CRITICAL *** ESXi: RAM disk / inode table is full	A ESXi host root file system has reached its resource pool limit. Various administrative actions depend on the ability to write files to the root file system and can fail when the RAM disk or inode table is full.	Critical
ESXi: HA isolated events by hostname	During a health check, HA determined that an ESXi host was isolated. Depending on how HA is configured this alert can mean that VMs have been failed over from the isolated host.	Critical
vCenter Server: HA connection failure detected	A HA cluster has detected one or more unresponsive ESXi hosts. If any ESXi hosts get marked as dead, then VMs running on them are migrated to other hosts.	Critical


Procedure

- 1 Open the vRealize Log Insight user interface.
 - a Open a Web browser and go to the following URL.

Region	vRealize Log Insight URL
Region A	https://sfo01vrli01.sfo01.rainpole.local
Region B	https://lax01vrli01.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click **Interactive Analytics**.
- 3 Click the  icon and select **Manage Alerts**.
- 4 Select an alert that is related to vSphere resources.
 - a In the search box of the **Alerts** dialog box, enter the following alert name as a search phrase.

```
*** CRITICAL *** ESXi: Core dump detected
```

- b Select the alert from the search result and click the **Edit** icon next to the alert name.

5 Create an instance of the alert for each data center in the region.

a In the **New Alert** dialog box, click **Run Query**.

A query editor page opens.

b Click **Add Filter** and use the drop-down menus to define the following filter.

Table 1-2. Filters for vRealize Log Insight in Region A

Filter	Value for Management vSphere Alerts in Region A	Value for Compute vSphere Alerts in Region A
Object type	vmw_datacenter	vmw_datacenter
Operation	contains	contains
Object	sfo01-m01dc	sfo01-w01dc

Table 1-3. Filters for vRealize Log Insight in Region B

Filter	Value for Management vSphere Alerts in Region B	Value for Compute vSphere Alerts in Region B
Object type	vmw_datacenter	vmw_datacenter
Operation	contains	contains
Object	lax01-m01dc	lax01-w01dc

c Click on the **Search** icon.

d Click the  icon and select **Create Alert from Query**.

- e In the **New Alert** dialog box, configure the following alert settings and click **Save**.

Table 1-4. Alerts for vRealize Log Insight in Region A

Setting	Value for Management vSphere Alerts in Region A	Value for Compute vSphere Alerts in Region A
Name	*** CRITICAL *** ESXi: Core dump detected (sfo01-m01dc).	*** CRITICAL *** ESXi: Core dump detected (sfo01-w01dc).
Description (Recommendation)	<i>vsphere_alert_purpose</i> See Table 1-1 .	<i>vsphere_alert_purpose</i> See Table 1-1 .
Email	<i>Email address to send alerts to</i>	<i>Email address to send alerts to</i>
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (All Objects)	sfo01-m01dc	sfo01-w01dc
Criticality	critical	critical
Raise an alert	On any match	On any match

Table 1-5. Alerts for vRealize Log Insight in Region B

Setting	Value for Management vSphere Alerts in Region B	Value for Compute vSphere Alerts in Region B
Name	*** CRITICAL *** ESXi: Core dump detected (lax01-m01dc).	*** CRITICAL *** ESXi: Core dump detected (lax01-w01dc).
Description (Recommendation)	<i>vsphere_alert_purpose</i> See Table 1-1 .	<i>vsphere_alert_purpose</i> See Table 1-1 .
Email	<i>Email address to send alerts to</i>	<i>Email address to send alerts to</i>
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (All Objects)	lax01-m01dc	lax01-w01dc
Criticality	critical	critical
Raise an alert	On any match	On any match

- f Repeat the steps to create the alert instance for the other data center in the region.
- 6 Repeat *Step 3* to *Step 5* for the rest of the alerts, configuring two instances of each alert in the region.
- 7 Repeat the procedure in vRealize Log Insight to create the alerts for both data centers in the other region.

Enable the Alerts for vSphere Networking

Use the in-built problem and alert signatures in vRealize Log Insight and create alerts for network-related events and map them to the vRealize Operations Manager inventory. For each alert, you create one instance for the management data center and one instance for the shared edge and compute data center in each region.

For basic monitoring of the vSphere networking components, use the following alerts:

Table 1-6. vSphere Networking Alerts in vRealize Log Insight

Alert Name	Purpose	Severity
Network: ESXi physical NIC down	ESXi has reported that a physical NIC is unavailable. Assuming other NICs are online this alert indicates a lack of redundancy and a potential performance impact. If all physical NICs for a vSwitch/dvSwitch are unavailable, then communication problems to VMs or the ESXi host might be possible.	Critical
Network: ESXi uplink redundancy lost	Only one physical NIC is connected and one more failure results in a loss of connectivity.	Critical
Network: Out of Memory	ESXi 5.0 or later hosts with NetQueue enabled, run out of memory when using jumbo frames (MTU is 9000 bytes). The lack of memory for network packets leads to lost VM connectivity and might also lose the connection with the vCenter Server. Other symptoms include: <ul style="list-style-type: none"> ▪ Network performance of network card is substantially degraded. ▪ NFS datastores mounted and accessed through this card become unmounted or flap between connected and disconnected state. ▪ vMotion timeouts. ▪ Restarting host management agents fail to finish when they attempt to reinitialize. 	Critical


Procedure

- 1 Open the vRealize Log Insight user interface.
 - a Open a Web browser and go to the following URL.

Region	vRealize Log Insight URL
Region A	https://sfo01vrli01.sfo01.rainpole.local
Region B	https://lax01vrli01.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click **Interactive Analytics**.
- 3 Click the  icon and select **Manage Alerts**.
- 4 Select an alert that is related to vSphere networking.
 - a In the search box of the **Alerts** dialog box, enter the following alert name as a search phrase.

Network: ESXi physical NIC down

- b Select the alert from the search result and click the **Edit** icon next to the alert name.

5 Create an instance of the alert for each data center in the region.

a In the **New Alert** dialog box, click **Run Query**.

A query editor page opens.

b Click **Add Filter** and use the drop-down menus to define the following filter.

Table 1-7. Filters for vRealize Log Insight in Region A

Filter	Value for Management vSphere Networking Alerts in Region A	Value for Compute vSphere Networking Alerts in Region A
Object type	vmw_datacenter	vmw_datacenter
Operation	contains	contains
Object	sfo01-m01dc	sfo01-w01dc

Table 1-8. Filters for vRealize Log Insight in Region B

Filter	Value for Management vSphere Networking Alerts in Region B	Value for Compute vSphere Networking Alerts in Region B
Object type	vmw_datacenter	vmw_datacenter
Operation	contains	contains
Object	lax01-m01dc	lax01-w01dc

c Click on the **Search** icon.

d Click the  icon and select **Create Alert from Query**.

- e In the **New Alert** dialog box, configure the following alert settings and click **Save**.

Table 1-9. Alerts for vRealize Log Insight in Region A

Setting	Value for Management vSphere Networking Alert in Region A	Value for Compute vSphere Networking Alert in Region A
Name	Network: ESXi physical NIC down (sfo01-m01dc)	Network: ESXi physical NIC down (sfo01-w01dc)
Description (Recommendation)	<i>networking_alert_purpose</i> See Table 1-6 .	<i>networking_alert_purpose</i> See Table 1-6 .
Email	<i>Email address to send alerts to</i>	<i>Email address to send alerts to</i>
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (All Objects)	sfo01-m01dc	sfo01-w01dc
Criticality	critical	critical
Raise an alert	On any match	On any match

Table 1-10. Alerts for vRealize Log Insight in Region B

Setting	Value for Management vSphere Networking Alert in Region B	Value for Compute vSphere Networking Alert in Region B
Name	Network: ESXi physical NIC down (lax01-m01dc)	Network: ESXi physical NIC down (lax01-w01dc)
Description (Recommendation)	<i>networking_alert_purpose</i> See Table 1-6 .	<i>networking_alert_purpose</i> See Table 1-6 .
Email	<i>Email address to send alerts to</i>	<i>Email address to send alerts to</i>
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (All Objects)	lax01-m01dc	lax01-w01dc
Criticality	critical	critical
Raise an alert	On any match	On any match

- f Repeat the steps to create the alert instance for the other data center in the region.
- 6 Repeat *Step 3* to *Step 5* for the rest of the alerts, configuring two instances of each alert in the region.
- 7 Repeat the procedure in vRealize Log Insight to create the alerts for both data centers in the other region.

Enable the Alerts for Storage Resources

Use the built-in problem and alert signatures in vRealize Log Insight to create alerts about storage and map these alerts to the vRealize Operations Manager inventory. For each alert, you create one instance for the management data center and one instance for the shared edge and compute data center in each region.

For monitoring storage in the Software-Defined Data Center, you can use the following alerts in vRealize Log Insight:

Table 1-11. Storage Alerts in vRealize Log Insight

Alert Name	Purpose	Severity
*** CRITICAL *** Storage: All Paths Down (APD)	One or more datastores has experienced an All Paths Down (APD) outage situation. This alert indicates that one or more datastores is or was unavailable. As a result of this issue, VMs are or were unavailable and ESXi hosts might have been disconnected from vCenter Server. This alert requires immediate attention.	Critical
*** CRITICAL *** Storage: vSAN device offline	A Virtual SAN storage device that backs up the datastores might fail. This alert occurs due to a faulty device firmware, physical media, or storage controller or when certain storage devices are not readable or writeable. Typically, such failures are irreversible. In some instances, permanent data loss might also occur, especially when data is not replicated on other nodes before the failure. vSAN automatically recovers data when new devices are added to the storage cluster, unless data lost is permanent.	Critical
Storage: NFS connectivity issue	This alert means that an NFS datastore is or was unavailable. Due to this problem, one or more VMs might be unavailable.	Critical
Storage: NFS lock file issue	Stale NFS lock files can prevent VMs from powering on.	Critical
Storage: SCSI Path dead	If an SCSI path is unavailable, assuming multiple paths are in use and the other paths are online, then this alert means reduced redundancy and performance. If all paths to a storage device become unavailable then VMs running on the storage device become unavailable.	Critical
Storage: Snapshot consolidation required	A failed snapshot consolidation operation that is not manually addressed can lead to a full datastore.	Critical


Procedure

- 1 Open the vRealize Log Insight user interface.
 - a Open a Web browser and go to the following URL.

Region	vRealize Log Insight URL
Region A	https://sfo01vrli01.sfo01.rainpole.local
Region B	https://lax01vrli01.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vri_admin_password</i>

- 2 In the vRealize Log Insight user interface, click **Interactive Analytics**.
- 3 Click the  icon and select **Manage Alerts**.

- 4 Select the alerts that are related to storage.
 - a In the search box of the **Alerts** dialog box, enter the following alert name as a search phrase.

```
*** CRITICAL *** Storage: All Paths Down (APD)
```

- b Select the alert from the search result and click the **Edit** icon next to the alert name.
- 5 Create an instance of the alert for each data center in the region.
 - a In the **New Alert** dialog box, click **Run Query**.

A query editor page opens.


- b Click **Add Filter** and use the drop-down menus to define the following filter.

Table 1-12. Filters for vRealize Log Insight in Region A

Filter	Value for Management Storage Alerts in Region A	Value for Compute Storage Alerts in Region A
Object type	vmw_datacenter	vmw_datacenter
Operation	contains	contains
Object	sfo01-m01dc	sfo01-w01dc

Table 1-13. Filters for vRealize Log Insight in Region B

Filter	Value for Management Storage Alerts in Region B	Value for Compute Storage Alerts in Region B
Object type	vmw_datacenter	vmw_datacenter
Operation	contains	contains
Object	lax01-m01dc	lax01-w01dc

- c Click on the **Search** icon.
 - d Click the  icon and select **Create Alert from Query**.

- e In the **New Alert** dialog box, configure the following alert settings and click **Save**.

Table 1-14. Alerts for vRealize Log Insight in Region A

Setting	Value for Management Storage Alert in Region A	Value for Compute Storage Alert in Region A
Name	*** CRITICAL *** Storage: All Paths Down (APD) (sfo01-m01dc)	*** CRITICAL *** Storage: All Paths Down (APD) (sfo01-w01dc)
Description (Recommendation)	<i>storage_alert_purpose</i> See Table 1-11 .	<i>storage_alert_purpose</i> See Table 1-11 .
Email	<i>Email address to send alerts to</i>	<i>Email address to send alerts to</i>
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (All Objects)	sfo01-m01dc	sfo01-w01dc
Criticality	critical	critical
Raise an alert	On any match	On any match

Table 1-15. Alerts for vRealize Log Insight in Region B

Setting	Value for Management Storage Alert in Region B	Value for Compute Storage Alert in Region B
Name	*** CRITICAL *** Storage: All Paths Down (APD) (lax01-m01dc)	*** CRITICAL *** Storage: All Paths Down (APD) (lax01-w01dc)
Description (Recommendation)	<i>storage_alert_purpose</i> See Table 1-11 .	<i>storage_alert_purpose</i> See Table 1-11 .
Email	<i>Email address to send alerts to</i>	<i>Email address to send alerts to</i>
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (All Objects)	lax01-m01dc	lax01-w01dc
Criticality	critical	critical
Raise an alert	On any match	On any match

- f Repeat the steps to create the alert instance for the other data center in the region.
- 6 Repeat *Step 3* to *Step 5* for the rest of the alerts, configuring two instances of each alert in the region.
- 7 Repeat the procedure in vRealize Log Insight to create the alerts for both data centers in the other region.

Enable the Alerts for vSAN

Use the built-in problem and alert signatures in vRealize Log Insight to create alerts for vSAN monitoring and map them to the vRealize Operations Manager inventory. For each alert, you create one instance for the management data center in each region. This validated design uses vSAN only for the SDDC management components. If you use vSAN also for your tenant workloads, configure alerts accordingly.

For monitoring vSAN in the Software-Defined Data Center, you can use the following alerts in vRealize Log Insight:

Table 1-16. vSAN Alerts in vRealize Log Insight

Alert Name	Purpose	Severity
vSAN - SSD health change to unhealthy state	This alert triggers when the state of any SSD changes to unhealthy. The reasons might be a permanent disk failure, disk decommissioning, node shutdown, and so on.	Critical
vSAN - Configuration failure - Insufficient space	This alert triggers when a configuration for a new object (VM) in the vSAN cluster cannot be created due to not enough space being available in the cluster. Check the error logs and try the provisioning operation again after adding new hosts or disk drives.	Critical
vSAN - Device Offline	This alert triggers if a particular device goes offline. Check the device configuration and other cluster state.	Critical
vSAN - Object component state changed to degraded	This alert triggers when a vSAN object state changes to a degraded state. Check the state of the adapters, disks, and network settings associated with the vSAN cluster.	Critical


Procedure

- 1 Open the vRealize Log Insight user interface.
 - a Open a Web browser and go to the following URL.

Region	vRealize Log Insight URL
Region A	<code>https://sfo01vrli01.sfo01.rainpole.local</code>
Region B	<code>https://lax01vrli01.lax01.rainpole.local</code>

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<code>vrli_admin_password</code>

- 2 In the vRealize Log Insight user interface, click **Interactive Analytics**.
- 3 Click the  icon and select **Manage Alerts**.
- 4 Select an alert that is related to vSAN storage.
 - a In the search box of the **Alerts** dialog box, enter the following alert name as a search phrase.

VSAN – SSD health change to unhealthy state

- b Select the alert from the search result and click the **Edit** icon next to the alert name.

5 Create an instance of the alert for each data center in the region.

- a In the **New Alert** dialog box, click **Run Query**.

A query editor page opens.

- b Click **Add Filter** and use the drop-down menus to define the following filter.

Table 1-17. Filters for vRealize Log Insight

Filter	Value for Management vSAN Alerts in Region A	Value for Management vSAN Alerts in Region B
Object type	vmw_datacenter	vmw_datacenter
Operation	contains	contains
Object	sfo01-m01dc	lax01-m01dc

- c Click on the **Search** icon.

- d Click the  icon and select **Create Alert from Query**.

- e In the **New Alert** dialog box, configure the following alert settings and click **Save**.

Table 1-18. Alerts for vRealize Log Insight

Setting	Value for Management vSAN Alert in Region A	Value for Management vSAN Alert in Region B
Name	vSAN - SSD health change to unhealthy state (sfo01-m01dc)	vSAN - SSD health change to unhealthy state (lax01-m01dc)
Description (Recommendation)	<i>vsan_alert_purpose</i> See Table 1-16 .	<i>vsan_alert_purpose</i> See Table 1-16 .
Email	<i>Email address to send alerts to</i>	<i>Email address to send alerts to</i>
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (All Objects)	sfo01-m01dc	lax01-m01dc
Criticality	critical	critical
Raise an alert	On any match	On any match

- f If you use a vSAN datastore in the shared edge and compute cluster in both regions, repeat the steps to create an alert instance for the compute data centers.

6 Repeat *Step 3* to *Step 5* for the rest of the alerts in the region.

7 Repeat the procedure in vRealize Log Insight to create the alerts for the management data center in the other region.

Enable the Alerts for NSX for vSphere

Create alerts using the in-built problem and alert signatures in vRealize Log Insight for NSX for vSphere and direct them to the vRealize Operations Manager inventory. For each alert, you create one instance for the NSX Manager for the management cluster and one instance for the NSX Manager for the shared edge and compute cluster in the region.

For monitoring the NSX for vSphere configuration in the Software-Defined Data Center, you can use the following alerts in vRealize Log Insight:

Table 1-19. NSX Alerts in vRealize Log Insight

Alert Name	Purpose	Severity
VMW_NSX_Firewall critical errors	Firewall critical events: <ul style="list-style-type: none"> ■ 301501 - This alert is a VSM side event if a host failed to respond within the time-out window. ■ 301503 - This alert is a VSM side event if VSM failed while provisioning a firewall rule. ■ 301506 - This alert is a VSM side event if VSM failed to send an exclude list update. ■ 301031 - Failed to receive, parse, or update firewall configuration. The key value has contextual information like generation number and other debugging information. 	Critical
VMW_NSX_VXLAN data plane lost connection to controller	This alert indicates that the VXLAN data plane lost connection to the controller.	Critical
VMW_NSX_VXLAN configuration issue	This alert is generated when VXLAN configuration is pushed to a host before the host was prepared. The host must be rebooted to initialize the configuration in the correct order.	Critical
VMW_NSX_Manager - Host Communication Errors	This event is generated when NSX Manager fails to receive a heartbeat from UserWorld Agent on the host within the threshold period. The output is grouped by host-id. The host-id can be found from vCenter.	Critical


Procedure

- 1 Open the vRealize Log Insight user interface.
 - a Open a Web browser and go to the following URL.

Region	vRealize Log Insight URL
Region A	https://sfo01vrli01.sfo01.rainpole.local
Region B	https://lax01vrli01.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click **Interactive Analytics**.
- 3 Click the  icon and select **Manage Alerts**.
- 4 Select an alert that is related to NSX .
 - a In the search box of the **Alerts** dialog box, enter the following alert name as a search phrase.

```
VMW_NSX_Firewall critical errors
```


- b Select the alert from the search result and click the **Edit** icon next to the alert name.
- 5 Create an instance of the alert for each NSX Manager in the region using the name of the NSX Manager virtual machine in the query filter.
 - a In the **New Alert** dialog box, click **Run Query**.
A query editor page opens.
 - b Click **Add Filter** and use the drop-down menus to define the following filter.

Table 1-20. Filters for vRealize Log Insight in Region A

Filter	Value for Management NSX Alerts in Region A	Value for Compute NSX Alerts in Region A
Object type	vc_vm_name	vc_vm_name
Operation	contains	contains
Object	sfo01m01nsx01	sfo01w01nsx01

Table 1-21. Filters for vRealize Log Insight in Region B

Filter	Value for Management NSX Alerts in Region B	Value for Compute NSX Alerts in Region B
Object type	vc_vm_name	vc_vm_name
Operation	contains	contains
Object	lax01m01nsx01	lax01w01nsx01

- c Click on the **Search** icon.
 - d Click the  icon and select **Create Alert from Query**.

- e In the **New Alert** dialog box, configure the following alert settings and click **Save**.

Table 1-22. Alerts for vRealize Log Insight in Region A

Setting	Value for Management NSX Alert in Region A	Value for Compute NSX Alert in Region A
Name	VMW_NSX_Firewall critical errors (sfo01m01nsx01)	VMW_NSX_Firewall critical errors (sfo01w01nsx01)
Description (Recommendation)	<i>nsx_alert_purpose</i> See Table 1-19 .	<i>nsx_alert_purpose</i> See Table 1-19 .
Email	<i>Email address to send alerts to</i>	<i>Email address to send alerts to</i>
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (Active Objects)	sfo01m01nsx01	sfo01w01nsx01
Criticality	critical	critical
Raise an alert	On any match	On any match

Table 1-23. Alerts for vRealize Log Insight in Region B

Setting	Value for Management NSX Alert in Region B	Value for Compute NSX Alert in Region B
Name	VMW_NSX_Firewall critical errors (lax01m01nsx01)	VMW_NSX_Firewall critical errors (lax01w01nsx01)
Description (Recommendation)	<i>nsx_alert_purpose</i> See Table 1-19 .	<i>nsx_alert_purpose</i> See Table 1-19 .
Email	<i>Email address to send alerts to</i>	<i>Email address to send alerts to</i>
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (Active Objects)	lax01m01nsx01	lax01w01nsx01
Criticality	critical	critical
Raise an alert	On any match	On any match

- f Repeat the steps to create the alert instance for the other NSX Manager in the region.
- 6 Repeat *Step 3* to *Step 5* for the rest of the alerts, configuring two instances of each alert in the region.
- 7 Repeat the procedure in vRealize Log Insight to create the alerts for both instances of NSX Managers in the other region.

Enable the Alerts for vRealize Operations Manager

Use the built-in problem and alert signatures in vRealize Log Insight for vRealize Operations Manager. You create one instance of each alert in Region A and in Region B because the vRealize Operations Manager instance works in the context of both management and compute resources in each region. The SDDC also contains one analytics cluster that is failed over to Region B and you receive alerts only about it.

For monitoring the vRealize Operations Manager deployment in the Software-Defined Data Center, you can use the following alerts in vRealize Log Insight:

Table 1-24. vRealize Operations Manager Alerts in vRealize Log Insight

Alert Name	Purpose	Severity
vRops: VC stats query timed out occurred	This alert notifies when vRealize Operations Manager instance is not able to get data from the vCenter instance within a 5 minute interval and the metrics back up and get dropped with the error: <code>Communication Error: com.integrien.adapter.vmware.VcCollector.collectMetrics - Vc stats query timed out (ms): 300377</code> . This error is due to intermittent connection issues with the vCenter and hosts or down to the network that is not able to handle the requests and is timing out.	Critical
vRops: Out of Memory errors occurred	This alert is generated when <code>OutOfMemoryError: Java heap space</code> occurs. This error might indicate memory problems and might lead to degradation in performance.	Critical


Procedure

- 1 Open the vRealize Log Insight user interface.
 - a Open a Web browser and go to the following URL.

Region	vRealize Log Insight URL
Region A	<code>https://sfo01vrli01.sfo01.rainpole.local</code>
Region B	<code>https://lax01vrli01.lax01.rainpole.local</code>

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<code>vrij_admin_password</code>

- 2 In the vRealize Log Insight user interface, click **Interactive Analytics**.
- 3 Click the  icon and select **Manage Alerts**.
- 4 Select an alert that is related to vRealize Operations Manager resources.
 - a In the search box of the **Alerts** dialog box, enter the following alert name as a search phrase.

```
vRops: VC stats query timed out occurred
```

- 5 Create an alert for vRealize Operations Manager in the region using the name of the master virtual machine in the query filter.
 - a In the **New Alert** dialog box, click **Run Query**.
A query editor page opens.
 - b Click **Add Filter** and use the drop-down menus to define the following filter.

Table 1-25. Filters for vRealize Log Insight

Filter	Value for vRealize Operations Manager in Region A	Value for vRealize Operations Manager in Region B
Object type	vc_vm_name	vc_vm_name
Operation	contains	contains
Object	vrops01svr01a	vrops01svr01a


- c Click on the **Search** icon.
- d Click the  icon and select **Create Alert from Query**.
- e In the **New Alert** dialog box, configure the following alert settings and click **Save**.

Table 1-26. Alerts for vRealize Log Insight

Setting	Value for vRealize Operations Manager in Region A	Value for vRealize Operations Manager in Region B
Name	vRops: VC stats query timed out (vrops01svr01a)	vRops: VC stats query timed out (vrops01svr01a)
Description (Recommendation)	<i>vrops_alert_purpose</i> See Table 1-24 .	<i>vrops_alert_purpose</i> See Table 1-24 .
Email	<i>Email address to send alerts to</i>	<i>Email address to send alerts to</i>
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (Active Objects)	vrops01svr01a	vrops01svr01a
Criticality	critical	critical
Raise an alert	On any match	On any match

- 6 Repeat *Step 3* to *Step 5* for the rest of the alerts in the region.
- 7 Repeat the procedure in vRealize Log Insight to create the alerts for the vRealize Operations Manager master virtual machine in the other region.

Enable the Alerts for vRealize Automation

Use the in-built problem and alert signatures in vRealize Log Insight for vRealize Automation. You create one instance of each alert in Region A and in Region B because the vRealize Automation instance in the SDDC works in the context of the compute resources in each region. The environment also contains one vRealize Automation deployment that is failed over to Region B and you receive alerts only about it.

For monitoring the vRealize Automation deployment in the Software-Defined Data Center, you can use the following alerts in vRealize Log Insight.

Table 1-27. vRealize Automation Alerts in vRealize Log Insight

Alert Name	Purpose	Severity
*** CRITICAL *** vRA CAFE service unavailable!	vRealize Automation CAFE service is not available because: <ul style="list-style-type: none"> ■ A service has failed and if the it does not automatically restart this might impact the vRealize Automation ability to function. ■ A service is blocked and does not respond. This problem might indicate an increased load within the environment. ■ vRealize Automation is starting and certain dependencies of the component are not available yet - this issue should clear automatically as all services come online. 	Critical
*** CRITICAL *** vRA IaaS Services Stopped	vRealize Automation service is not available because: <ul style="list-style-type: none"> ■ A service has failed and if the it does not automatically restart this may impact vRealize Automation ability to function. ■ A service is blocked and does not respond - this might indicate an increased load within the environment. ■ Management Agent - In an HA deployment, only one Management Agent instance can be running. If more than one instance of Management Agent is running, this can cause issues with the normal operation of the system. 	Critical
*** CRITICAL *** vRA disk is full	Windows hosts have disk that reached its capacity. If disk space runs out completely, it will impact the Infrastructure services provided by the IaaS component of vRealize Automation and the Infrastructure tab will become unavailable in the vRealize Automation user interface.	Critical


Procedure

- 1 Open the vRealize Log Insight user interface.
 - a Open a Web browser and go to the following URL.

Region	vRealize Log Insight URL
Region A	https://sfo01vrli01.sfo01.rainpole.local
Region B	https://lax01vrli01.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click **Interactive Analytics**.
- 3 Click the  icon and select **Manage Alerts**.

- 4 Select an alert that is related to vRealize Automation.
 - a In the search box of the **Alerts** dialog box, enter the following alert name as a search phrase.

```
*** CRITICAL *** vRA CAFE service unavailable!
```

- b Select the alert from the search result and click the **Edit** icon next to the alert name.
- 5 Create an alert for vRealize Automation in the region using the name of the primary vRealize Automation Appliance in the query filter.

- a In the **New Alert** dialog box, click **Run Query**.

A query editor page opens.

- b Click **Add Filter** and use the drop-down menus to define the following filter.

Table 1-28. Filters for vRealize Log Insight

Filter	Value for vRealize Automation Alerts in Region A	Value for vRealize Automation Alerts in Region B
Object type	vc_vm_name	vc_vm_name
Operation	contains	contains
Object	vra01svr01a	vra01svr01a


- c Click on the **Search** icon.
 - d Click the  icon and select **Create Alert from Query**.
 - e In the **New Alert** dialog box, configure the following alert settings and click **Save**.

Table 1-29. Alerts for vRealize Log Insight

Setting	Value for vRealize Automation Alert in Region A	Value for vRealize Automation Alert in Region B
Name	*** CRITICAL *** vRA CAFE service unavailable! (vra01svr01a)	*** CRITICAL *** vRA CAFE service unavailable! (vra01svr01a)
Description (Recommendation)	<i>vra_alert_purpose</i> See Table 1-27 .	<i>vra_alert_purpose</i> See Table 1-27 .
Email	<i>Email address to send alerts to</i>	<i>Email address to send alerts to</i>
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (Active Objects)	vra01svr01a	vra01svr01a
Criticality	critical	critical
Raise an alert	On any match	On any match

- 6 Repeat *Step 3* to *Step 5* for the rest of the alerts in the region.
- 7 Repeat the procedure in vRealize Log Insight to create the alerts for the primary vRealize Automation Appliance in the other region.

Enable the Alerts for Microsoft SQL Server for vRealize Automation

Use the built-in problem and alert signatures in vRealize Log Insight for the Microsoft SQL Server for vRealize Automation. For each alert, you create one instance for each region so that alerts are still available if the Microsoft SQL Server instance is failed over to Region B.

For monitoring the health of the Microsoft SQL Server installation in the Software-Defined Data Center, you can use the following alerts in vRealize Log Insight:

Table 1-30. Microsoft SQL Server Alerts in vRealize Log Insight

Alert Name	Purpose	Severity
MS-SQL: Failed login attempt	<p>Error codes in this group have severity levels 14 or 16.</p> <ul style="list-style-type: none"> Severity level 14 indicates security-related login errors, such as permission denied. Severity level 16 indicates login errors that are addressable by user. The exact error message text appears in the line just after the error code and severity level. 	Critical
MS-SQL: Out of Memory (Resources)	<p>Error codes in this group have severity levels 17 or 16.</p> <ul style="list-style-type: none"> Severity level 17 indicates that the statement caused SQL Server to run out of resources such as memory, locks, or disk space for the database, or to exceed some limit set by the system administrator. Severity level 16 indicates problems that are addressable by the user. The exact error message text appears in the line just after the error code and severity level. 	Critical
MS-SQL : Transaction Deadlocked	<ul style="list-style-type: none"> Severity level 13 indicates transaction deadlock errors. This error means that a transaction was deadlocked on resources with another process and has been selected as the deadlock victim. Run the transaction again. 	Critical
MS-SQL : Database Corruption	<p>Error codes in this group have severity levels 20, 21, 22 or 23 or 16.</p> <p>Database corruption is defined as a problem associated with the improper storage of the actual zeroes and ones that store your database data at the disk or IO subsystem level.</p> <p>You might need to check the logical and physical integrity of all the objects in the specified database.</p> <p>You can run DBCC CHECKDB to check for any database corruption.</p>	Critical

For detailed information on Microsoft SQL severity levels: [https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008/ms164086\(v=sql.100\)](https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008/ms164086(v=sql.100))

For further information on the error codes: [https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/cc645603\(v=sql.105\)](https://docs.microsoft.com/en-us/previous-versions/sql/sql-server-2008-r2/cc645603(v=sql.105))

Procedure

- 1 Open the vRealize Log Insight user interface.

- a Open a Web browser and go to the following URL.

Region	vRealize Log Insight URL
Region A	https://sfo01vrli01.sfo01.rainpole.local
Region B	https://lax01vrli01.lax01.rainpole.local

- b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrli_admin_password</i>

- 2 In the vRealize Log Insight user interface, click **Interactive Analytics**.

- 3 Click the  icon and select **Manage Alerts**.

- 4 Select an alert that is related to Microsoft SQL for vRealize Automation.

- a In the search box of the **Alerts** dialog box, enter the following alert name as a search phrase.

MS-SQL: Failed login attempt

- b Select the alert from the search result and click the **Edit** icon next to the alert name.

- 5 Create an alert for the Microsoft SQL Server for vRealize Automation in Region A using the name of the virtual machine in the query filter.

- a In the **New Alert** dialog box, click **Run Query**.

A query editor page opens.

- b Click **Add Filter** and use the drop-down menus to define the following filter.

Table 1-31. Filters for vRealize Log Insight

Filter	Value for Microsoft SQL for vRealize Automation Alerts in Region A	Value for Microsoft SQL for vRealize Automation Alerts in Region B
Object type	vc_vm_name	vc_vm_name
Operation	contains	contains
Object	vra01mssql01	vra01mssql01

- c Click on the **Search** icon.

- d Click the  icon and select **Create Alert from Query**.
- e In the **New Alert** dialog box, configure the following alert settings and click **Save**.

Table 1-32. Alerts for vRealize Log Insight

Setting	Value for Microsoft SQL for vRealize Automation Alert in Region A	Value for Microsoft SQL for vRealize Automation Alert in Region B
Name	MS-SQL: Failed login attempt (vra01mssql01)	MS-SQL: Failed login attempt (vra01mssql01)
Description (Recommendation)	<i>mssql_alert_purpose</i> See Table 1-30 .	<i>mssql_alert_purpose</i> See Table 1-30 .
Email	<i>Email address to send alerts to</i>	<i>Email address to send alerts to</i>
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (Active Objects)	vra01mssql01	vra01mssql01
Criticality	critical	critical
Raise an alert	On any match	On any match

- 6 Repeat *Step 3* to *Step 5* for the rest of the alerts in the region.
- 7 Repeat the procedure in vRealize Log Insight to create the alerts for the Microsoft SQL Server for vRealize Automation virtual machine in the other region.

Creating Custom SDDC vRealize Operations Dashboards

2

Monitoring the SDDC is critical to the health of the environment. You create custom vRealize Operations Manager dashboards to provide centralized SDDC dashboards. Using such dashboards simplifies monitoring the health of the SDDC as opposed to having to switch between multiple product-specific dashboards.

To create custom dashboards, verify that you have deployed vRealize Operations Manager according to implementation guides. You must have the following management packs installed and configured:

- vRealize Operations Manager Management Pack for VMware vSphere
- vRealize Operations Manager Management Pack for VMware vSAN
- vRealize Operations Manager Management Pack for VMware vRealize Log Insight
- vRealize Operations Manager Management Pack for VMware vRealize Business for Cloud
- vRealize Operations Manager Management Pack for VMware vRealize Automation
- vRealize Operations Manager Management Pack for NSX-vSphere
- vRealize Operations Manager Management Pack for Storage Devices
- vRealize Operations Manager Management Pack for Site Recovery Manager

Procedure

1 [SDDC Capacity and Utilization Overview Dashboards](#)

The dashboards in the **Capacity and Utilization** category cater to the teams responsible for tracking the use of the provisioned capacity in their virtual infrastructure. The dashboards within this category allow you to take capacity procurement decisions, reduce wastage through reclamation, and track usage trends to avoid performance problems due to capacity shortfalls.

2 [Configure a Dashboard That Provides an Overview of the SDDC Operation](#)

Create a dashboard in vRealize Operations Manager where you can monitor the objects of the SDDC management stack.

SDDC Capacity and Utilization Overview Dashboards

The dashboards in the **Capacity and Utilization** category cater to the teams responsible for tracking the use of the provisioned capacity in their virtual infrastructure. The dashboards within this category allow you to take capacity procurement decisions, reduce wastage through reclamation, and track usage trends to avoid performance problems due to capacity shortfalls.

Key questions that these dashboards aim to answer are:

- How much capacity exists, how much capacity is used, and what are the use trends for a specific vCenter, data center, or cluster?
- How much disk, vCPU, or memory you can reclaim from large VMs in your environment to reduce wastage and improve performance?
- Which clusters have the largest resource demands?
- Which hosts are being heavily used and what is the cause?
- Which datastores are running out of disk space and what are the top consumers of disk space?
- The storage capacity and use of your vSAN environment with the savings achieved by enabling deduplication and compression.

Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
 - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 Click **Dashboards** and click the **All Dashboards** drop-down menu.
- 3 Use the following predefined dashboards in **Capacity & Utilization** according to the following scenarios.

Dashboard	Dashboard Use
Capacity Allocation Overview	This dashboard provides an overview of allocation ratios for virtual machines, vCPUs, and memory for a specific data center or cluster.
Cluster Utilization	This dashboard shows vSphere clusters that are extensively consumed from a CPU, memory, disk, and network perspective.
Datastore Utilization	This dashboard shows storage provisioning and use patterns in the virtual infrastructure.
Heavy Hitter VMs	This dashboard shows VMs which are consistently consuming a large amount of resources from the virtual infrastructure. In heavily over-provisioned environments, this might create resource bottlenecks resulting in potential performance issues.

Dashboard	Dashboard Use
Host Utilization	This dashboard shows ESXi hosts that are extensively consumed from a CPU, memory, disk, and network perspective.
Utilization Overview	This dashboard shows the available capacity in the virtual infrastructure.
VM Utilization	This dashboard provides a capture of the use trends for any VM in the virtual infrastructure. You can list the key properties of a VM and the resource use trends for a specific time period.
vSAN Capacity Overview	This dashboard provides an overview of vSAN storage capacity and savings achieved by enabling deduplication and compression across all vSAN clusters.

Configure a Dashboard That Provides an Overview of the SDDC Operation

Create a dashboard in vRealize Operations Manager where you can monitor the objects of the SDDC management stack.

Procedure

1 [Create Applications in vRealize Operations Manager for the SDDC Components](#)

Use applications in vRealize Operations Manager to group the monitoring data about the virtual machines of the SDDC management components.

2 [Collect the SDDC Objects in a Group](#)

Create a custom group for each management application to monitor the health of the entire application stack as opposed to individual virtual machine health.

3 [Configure a Dashboard That Provides an Overview of the SDDC State](#)

Create a central dashboard that you can use to track the overall state of the SDDC.

Create Applications in vRealize Operations Manager for the SDDC Components

Use applications in vRealize Operations Manager to group the monitoring data about the virtual machines of the SDDC management components.

vRealize Operations Manager builds an application to determine how your environment is affected when one or more components in an application experience problems. You can also monitor the overall health and performance of the application.

vRealize Operations Manager collects data from the components in the application and displays the results in a summary dashboard with a real-time analysis for any or all the components.

- [Create an Application for vRealize Suite Lifecycle Manager](#)

Group the monitoring data about the virtual machine of vRealize Suite Lifecycle Manager by creating an application in vRealize Operations Manager.

- [Create an Application for vRealize Log Insight](#)

Group the monitoring data about the virtual machines of vRealize Log Insight by creating an application in vRealize Operations Manager.

- [Create an Application for VMware Site Recovery Manager](#)
Group the monitoring data about the virtual machines of VMware Site Recovery Manager by creating an application in vRealize Operations Manager.
- [Create an Application for VMware vSphere Replication](#)
Group the monitoring data about the virtual machines of VMware vSphere Replication by creating an application in vRealize Operations Manager.
- [Create an Application for VMware vRealize Operations Manager](#)
Group the monitoring data for the virtual machines of VMware vRealize Operations Manager by creating an application in vRealize Operations Manager.
- [Create an Application for VADP Based Backup Solution](#)
Group the monitoring data collected from your vSphere Storage APIs for Data Protection (VADP) based backup solution VMs by creating an application in vRealize Operations Manager.
- [Create an Application for VMware vSphere Update Manager Download Service](#)
Create an application in vRealize Operations Manager to group the monitoring data about the virtual machines of VMware vSphere Update Manager Download Service (UMDS)

Create an Application for vRealize Suite Lifecycle Manager

Group the monitoring data about the virtual machine of vRealize Suite Lifecycle Manager by creating an application in vRealize Operations Manager.

Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
 - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Environment** menu and click the **Applications** tab.
- 3 On the **Applications** tab, click the **Add** icon to add an application.
- 4 In the **Add Application** dialog box, select **Custom** and click **OK**.
- 5 In the **Application Management** dialog box, in the **Application** text box enter **vRealize Suite Lifecycle Manager**.
- 6 In the **Tiers** pane, click **Add Tier**, enter **vRSLCM VMs** as the **Tier Name**, and click **Update**.
- 7 In the objects list underneath, enter **vrs1cm** in the search box, and press **Enter**.

- 8 Select the Virtual Machine object of **vRealize Suite Lifecycle Manager** and drag it to the **Tier Objects** pane.

vrslcm01svr01a

- 9 Click **Save**.

Create an Application for vRealize Log Insight

Group the monitoring data about the virtual machines of vRealize Log Insight by creating an application in vRealize Operations Manager.

Because the Management Pack for vRealize Log Insight does not collect monitoring data about the virtual machines of the vRealize Log Insight deployment, you create an application to watch their state.

Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
 - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Environment** menu and click the **Applications** tab.
- 3 On the **Applications** tab, click the **Add** icon to add an application.
- 4 In the **Add Application** dialog box, select **Custom** and click **OK**.
- 5 In the **Application Management** dialog box, in the **Application** text box enter **vRealize Log Insight**.
- 6 In the **Tiers** pane, click **Add Tier**, enter **Log Insight VMs** as the **Tier Name**, and click **Update**.
- 7 In the objects list underneath, enter **vrli01** in the search box, and press **Enter**.
- 8 Select the Virtual Machine objects of vRealize Log Insight and drag them to the **Tier Objects** pane.

vRealize Log Insight Region A VMs	vRealize Log Insight Region B VMs
sfo01vrli01a	lax01vrli01a
sfo01vrli01b	lax01vrli01b
sfo01vrli01c	lax01vrli01c

- 9 Click **Save**.

Create an Application for VMware Site Recovery Manager

Group the monitoring data about the virtual machines of VMware Site Recovery Manager by creating an application in vRealize Operations Manager.

Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
 - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click **Environment** menu and click the **Applications** tab.
- 3 On the **Applications** tab, click the **Add** icon to add an application.
- 4 In the **Add Application** dialog box, select **Custom** and click **OK**.
- 5 In the **Application Management** dialog box, in the **Application** text box enter **Site Recovery Manager**.
- 6 In the **Tiers** pane, click **Add Tier**, enter **SRM VMs** as the **Tier Name**, and click **Update**.
- 7 In the objects list underneath, enter **srm** in the search box, and press **Enter**.
- 8 Select the Virtual Machine objects of Site Recovery Manager and drag them to the **Tier Objects** pane.

VMware Site Recovery Manager Region A VMs	VMware Site Recovery Manager Region B VMs
sfo01m01srm01	lax01m01srm01

- 9 Click **Save**.

Create an Application for VMware vSphere Replication

Group the monitoring data about the virtual machines of VMware vSphere Replication by creating an application in vRealize Operations Manager.

Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
 - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click the **Environment** menu and click the **Applications** tab.
- 3 On the **Applications** tab, click the **Add** icon to add an application.
- 4 In the **Add Application** dialog box, select **Custom** and click **OK**.

- 5 In the **Application Management** dialog box, in the **Application** text box enter **vSphere Replication**.
- 6 In the **Tiers** pane, click **Add Tier**, enter **vSphere Replication VMs** as the **Tier Name** and click **Update**.
- 7 In the objects list underneath, enter **vrms** in the search box, and press **Enter**.
- 8 Select the Virtual Machine objects of vSphere Replication and drag them to the **Tier Objects** pane.

VMware vSphere Replication Region A VMs	VMware vSphere Replication Region B VMs
sfo01m01vrms01	lax01m01vrms01

- 9 Click **Save**.

Create an Application for VMware vRealize Operations Manager

Group the monitoring data for the virtual machines of VMware vRealize Operations Manager by creating an application in vRealize Operations Manager.

Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
 - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click the **Environment** menu and click the **Applications** tab.
- 3 On the **Applications** tab, click the **Add** icon to add an application.
- 4 In the **Add Application** dialog box, select **Custom** and click **OK**.
- 5 In the **Application Management** dialog box, in the **Application** text box enter **vRealize Operations Manager**.
- 6 In the **Tiers** pane, click **Add Tier**, enter **vRealize Operations Manager VMs** as the **Tier Name** and click **Update**.
- 7 In the objects list underneath, enter **vrops01svr** in the search box and press **Enter**.
- 8 Select the Virtual Machine objects of vRealize Operations Manager Cluster and drag them to the **Tier Objects** pane.
 - vrops01svr01a
 - vrops01svr01b
 - vrops01svr01c

- 9 Click **Save**.

Create an Application for VADP Based Backup Solution

Group the monitoring data collected from your vSphere Storage APIs for Data Protection (VADP) based backup solution VMs by creating an application in vRealize Operations Manager.

Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
 - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click the **Environment** menu and click the **Applications** tab.
- 3 On the **Applications** tab, click the **Add** icon to add an application.
- 4 In the **Add Application** dialog box, select **Custom** and click **OK**.
- 5 In the **Application Management** dialog box, in the **Application** text box enter **Backup Solution**.
- 6 In the **Tiers** pane, click **Add Tier**, enter **Backup Solution VMs** as the **Tier Name** and click **Update**.
- 7 In the objects list underneath, enter **virtual machines for backup solution** in the search box, and press **Enter**.
- 8 Select the Virtual Machine objects of backup solution and drag them to the **Tier Objects** pane.

Backup Solution Region A VMs	Backup Solution Region B VMs
VMs for the backup solution in Region A	VMs for the backup solution in Region B

- 9 Click **Save**.

Create an Application for VMware vSphere Update Manager Download Service

Create an application in vRealize Operations Manager to group the monitoring data about the virtual machines of VMware vSphere Update Manager Download Service (UMDS)

vRealize Operations Manager builds an application to determine how your environment is affected when one or more components in an application experiences problems. You can also monitor the overall health and performance of the application.

vRealize Operations Manager collects data from the components in the application and displays the results in a summary dashboard with a real-time analysis for any or all of the components.

Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
 - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click the **Environment** menu and click the **Applications** tab.
- 3 On the **Applications** tab, click the **Add** icon to add an application.
- 4 In the **Add Application** dialog box, select **Custom** and click **OK**.
- 5 In the **Application Management** dialog box, in the **Application** text box enter **vSphere UMDS**.
- 6 In the **Tiers** pane, click **Add Tier**, enter **UMDS VMs** as the **Tier Name** and click **Update**.
- 7 In the objects list underneath, enter **umds** in the search box, and press **Enter**.
- 8 Select the Virtual Machine objects of vSphere Update Manager Download Service and drag them to the **Tier Objects** pane.

VMware vSphere UMDS Region A VMs	VMware vSphere UMDS Region B VMs
sfo01umds01	lax01umds01

- 9 Click **Save**.

Collect the SDDC Objects in a Group

Create a custom group for each management application to monitor the health of the entire application stack as opposed to individual virtual machine health.

Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
 - a Open a Web browser and go to **https://vrops01svr01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vrops_admin_password</i>

- 2 On the main navigation bar, click the **Environment** menu and click the **Custom Groups** tab.
- 3 On the **Custom Groups** tab, click the **Add** icon to add a custom group.
- 4 In the **New group** dialog box, enter **SDDC Management** in the **Name** text box.

- 5 From the **Group Type** drop-down menu, select **Function**.
- 6 Expand the **Define membership criteria** section.
- 7 To add the vRealize Automation objects, from the **Select the Object Type that matches all of the following criteria** drop-down menu, select **vRealize Automation Adapter > vRealize Automation MP Instance**.
- 8 Click **Add another criteria set** and repeat [Step 7](#) to add each of the following object types representing the other management applications in the SDDC.
 - **vRBC Adapter > vRBC Adapter Instance**
 - **vCenter Adapter > vSphere World**
 - **NSX-vSphere Adapter > NSX-vSphere Environment**
- 9 Expand the **Objects to always include** section.
- 10 Add the following application objects.
 - a Under **Filtered objects**, expand **Custom Groups** and select **Applications**.
 - b Select **vRealize Log Insight**, click the **Add** button to add the application objects to **Objects to always include** list on the right.
 - c Add the rest of application objects.
 - **Site Recovery Manager**
 - **vRealize Log Insight**
 - **vRealize Operations Manager**
 - **vRealize Suite Lifecycle Manager**
 - **vSphere Replication**
 - **vSphere UMDS**
 - **Backup Solution**
- 11 Click **OK**.

Configure a Dashboard That Provides an Overview of the SDDC State

Create a central dashboard that you can use to track the overall state of the SDDC.

The SDDC overview dashboard shows:

- The main indicators for the state of CPU, memory, connectivity, and storage in the management cluster that hosts the management applications.
- The overall state of the management applications in the SDDC. You use the SDDC management custom group that represents a common object for all management applications.

The SDDC overview dashboard consists of the following widgets:

- One Health Chart widget.
- Twelve Heatmap widgets showing heatmaps of the compute resources in the SDDC. You arrange the heatmap widgets in three rows and four columns. Heatmap widgets are labeled Heatmap *X.Y* where *X* is the row number and *Y* is the column number in the dashboard.

Table 2-1. Configuration of the Heatmap Widgets in the First Row of the SDDC Overview Dashboard

Widget Setting	Heatmap 1.1	Heatmap 1.2	Heatmap 1.3	Heatmap 1.4
Title	Physical CPU Time Remaining	Physical Memory Time Remaining	Management VM CPU Used	Management VM CPU Contention
Refresh Content	On	On	On	On
Refresh Interval	300 s	300 s	300 s	300 s
Name	Management Hosts	Management Hosts	Management VMs	Management VMs
Group by	vCenter Adapter > Datacenter	vCenter Adapter > Datacenter	vCenter Adapter > Datacenter	vCenter Adapter > Datacenter
Then by	-	-	-	-
Focus on Groups	Selected	Selected	Selected	Selected
Mode	Instance	Instance	Instance	Instance
Object Type	vCenter Adapter > Host System	vCenter Adapter > Host System	vCenter Adapter > Virtual Machine	vCenter Adapter > Virtual Machine
Attribute Type	Capacity Analytics Generated > CPU > Demand > Time Remaining (Day(s))	Capacity Analytics Generated > Memory > Demand > Time Remaining (Day(s))	CPU > Usage (%)	CPU > CPU Contention (%)
Min Value (Color)	0 (red)	0 (red)	80 (green)	0 (green)
Max Value (Color)	1 (green)	1 (green)	100 (red)	2 (red)
Filter	-	-	<ul style="list-style-type: none"> ■ Adapter Instances > vCenter Server > sfo01m01vc01 ■ Adapter Instances > vCenter Server > lax01m01vc01 	<ul style="list-style-type: none"> ■ Adapter Instances > vCenter Server > sfo01m01vc01 ■ Adapter Instances > vCenter Server > lax01m01vc01

Table 2-2. Configuration of the Heatmap Widgets in the Second Row of the SDDC Overview Dashboard

Widget Setting	Heatmap 2.1	Heatmap 2.2	Heatmap 2.3	Heatmap 2.4
Title	Physical Disk Space Time Remaining	Physical Dropped Packets	Management VM Memory Used	Management VM Swap Rate
Refresh Content	On	On	On	On
Refresh Interval	300 s	300 s	300 s	300 s
Name	Management Hosts	Management Hosts	Management VMs	Management VMs

Table 2-2. Configuration of the Heatmap Widgets in the Second Row of the SDDC Overview Dashboard (Continued)

Widget Setting	Heatmap 2.1	Heatmap 2.2	Heatmap 2.3	Heatmap 2.4
Group by	vCenter Adapter > Datacenter	vCenter Adapter > Datacenter	vCenter Adapter > Datacenter	vCenter Adapter > Datacenter
Then by	-	-	-	-
Focus on Groups	Selected	Selected	Selected	Selected
Mode	Instance	Instance	Instance	Instance
Object type	vCenter Adapter > Host System	vCenter Adapter > Host System	vCenter Adapter > Virtual Machine	vCenter Adapter > Virtual Machine
Attribute type	Capacity Analytics Generated > Disk Space > Demand > Time Remaining (Day(s))	Network > Packets Dropped %	Memory > Usage (%)	Memory > Swapped (KB)
Min Value (Color)	0 (red)	0 (green)	50 (green)	0 (green)
Max Value (Color)	1 (green)	1 (red)	90 (red)	1 (red)
Filter	-	-	<ul style="list-style-type: none"> ■ Adapter Instances > vCenter Server > sfo01m01vc01 ■ Adapter Instances > vCenter Server > lax01m01vc01 	<ul style="list-style-type: none"> ■ Adapter Instances > vCenter Server > sfo01m01vc01 ■ Adapter Instances > vCenter Server > lax01m01vc01

Table 2-3. Configuration of the Heatmap Widgets in the Third Row of the SDDC Overview Dashboard

Widget Setting	Heatmap 3.1	Heatmap 3.2	Heatmap 3.3	Heatmap 3.4
Title	Storage vSAN Latency	Storage NFS Latency	Management VM Storage Latency	Management VM Disk Space Time Remaining
Refresh Content	On	On	On	On
Refresh Interval	300 s	300 s	300 s	300 s
Name	Datstores	Datstores	Management VMs	Management VMs
Group by	Storage Devices > VirtualSAN Datastore	Storage Devices > NFS Volume	vCenter Adapter > Datacenter	vCenter Adapter > Datacenter
Then by	-	-	-	-
Focus on Groups	Selected	Selected	Selected	Selected
Mode	Instance	Instance	Instance	Instance
Object type	Storage Devices > VirtualSAN Datastore	Storage Devices > NFS Volume	vCenter Adapter > Virtual Machine	vCenter Adapter > Virtual Machine
Attribute type	Host Specific Metrics > Write Latency (ms)	Derived Statistics > Inferred Latency	Virtual Disk > Read Latency (ms)	Capacity Analytics Generated > Disk Space > Time Remaining (Day(s))

Table 2-3. Configuration of the Heatmap Widgets in the Third Row of the SDDC Overview Dashboard (Continued)

Widget Setting	Heatmap 3.1	Heatmap 3.2	Heatmap 3.3	Heatmap 3.4
Min Value (Color)	0 (green)	0 (green)	0 (green)	0 (red)
Max Value (Color)	30 (red)	30 (red)	30 (red)	1 (green)
Filter	-	-	<ul style="list-style-type: none"> ■ Adapter Instances > vCenter Server > sfo01m01vc01 ■ Adapter Instances > vCenter Server > lax01m01vc01 	<ul style="list-style-type: none"> ■ Adapter Instances > vCenter Server > sfo01m01vc01 ■ Adapter Instances > vCenter Server > lax01m01vc01

Table 2-4. Configuration of the Health Chart Widget in the SDDC Overview Dashboard

Health Widget Setting	Value
Title	Management Applications
Refresh Content	On
Refresh Interval	300 s
Self Provider	On
Mode	Children
Order By	Value Ascending
Pagination number	15
Metric	Health

Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
 - a Open a Web browser and go to <https://vrops01svr01.rainpole.local>.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	vrops_admin_password

- 2 On the main navigation bar, click **Dashboards**.
- 3 From the **Actions** menu, select **Create Dashboard**.
- 4 In the **Dashboard Configuration** section of the **New Dashboard** dialog box, configure the following settings.

Dashboard Setting	Value
Name	SDDC Overview
Is default	Yes

5 Add widgets to the dashboard.

- a Expand the **Widget List** section.
- b Drag the 12 Heatmap widgets to the layout pane on the right, make three rows with four columns, and align them so that they are all approximately equal in size.
- c Drag a Health Chart widget to the layout pane on the right.

6 Configure the Heatmap widgets.

- a In the upper-right corner of each widget, click the **Edit Widget** icon and configure the widget.
- b In the **Edit Heatmap** dialog box, configure the settings of the heatmap widget and click **Save**.

7 Configure the Health Chart widget.

- a In the upper-right corner of the widget, click the **Edit Widget** icon and configure the widget.
- b In the **Edit Health Chart** dialog box, configure the settings of the Health Chart widget .
- c From the objects list at the bottom, expand **Function** and select the **SDDC Management** custom group and click **Save**.

8 In the **New Dashboard** dialog box, click **Save**.

The **SDDC Overview** dashboard becomes available in the **Dashboards** list of the vRealize Operations Manager user interface.



Configure vRealize Operations Manager to Notify of SDDC Issues

3

Create a set of notifications in vRealize Operations Manager so that data center operators receive alerts about issues in the SDDC main functions.

- [Create Notifications in vRealize Operations Manager](#)
Create email notifications in vRealize Operations Manager so that it informs the SDDC operators of issues in the main monitoring parameters of the environment.
- [List of Notifications for vRealize Operations Manager](#)
Configure vRealize Operations Manager to send email notifications about important alerts in the SDDC.

Create Notifications in vRealize Operations Manager

Create email notifications in vRealize Operations Manager so that it informs the SDDC operators of issues in the main monitoring parameters of the environment.

You create a set of notifications of important alerts in the SDDC. See [List of Notifications for vRealize Operations Manager](#).

Procedure

- 1 Log in to vRealize Operations Manager by using the operations interface.
 - a Open a Web browser and go to **https://vroops01svr01.rainpole.local**.
 - b Log in using the following credentials.

Setting	Value
User name	admin
Password	<i>vroops_admin_password</i>

- 2 On the main navigation bar, click **Alerts**.
- 3 In the **Navigator**, expand **Alert Settings** and click **Notifications Settings**.

- 4 On the **Notification Settings** page, click the **Add** icon and configure the following notification settings in the **Add Rule** dialog box.

Notification Setting	Value
Name	One or more virtual machine guest file systems are running out of disk space.
Method	Standard Email Plugin
Instance	SMTP Alert Mail Relay
Recipients	<i>Email address to send alerts to</i>
Filtering Criteria	
Scope	Object Type > vCenter Adapter > Virtual Machine
Notification Trigger	Alert Definition

- 5 Configure the trigger for the notification.
- Click the **Select an Alert Definition** button.
 - In the **Quick filter (Name)** text box of the **Alert Definitions** dialog box, enter **disk space** and press Enter.
 - Select the **One or more virtual machine guest file systems are running out of disk space** alert definition and click **Select**.
- 6 In the **Add Rule** dialog box, click **Save**.
- 7 Repeat the steps to create the remaining SDDC notifications.

List of Notifications for vRealize Operations Manager

Configure vRealize Operations Manager to send email notifications about important alerts in the SDDC.

You define notifications from the **Alerts > Alert Settings > Notification Settings** page in vRealize Operations user interface. See [Create Notifications in vRealize Operations Manager](#).

Notification Delivery Properties

When you define notifications from vRealize Operations Manager, use the following properties to send them by email to the operations team in your organization.

Table 3-1. Delivery Properties of vRealize Operations Manager Notifications

Notification Delivery Property	Value
Method	Standard Email Plugin
Instance	SMTP Alert Mail Relay
Recipients	<i>Email address to send alerts to</i>

Virtual Machine and Host Notifications

Create notifications for important virtual machines and ESXi host issues.

Table 3-2. VM and Host Notifications in SDDC

Name	Scope	Notification Trigger	Alert Definition
One or more virtual machine guest file systems are running out of disk space	1 Object Type 2 vCenter Adapter > Virtual Machine	Alert Definition	One or more virtual machine guest file systems are running out of disk space
Virtual machine has CPU contention due to multi-vCPU scheduling issues (co-stop) caused by too many vCPUs	1 Object Type 2 vCenter Adapter > Virtual Machine	Alert Definition	Virtual machine has CPU contention due to multi-vCPU scheduling issues (co-stop) caused by too many vCPUs
Virtual machine has CPU contention due to memory page swapping in the host	1 Object Type 2 vCenter Adapter > Virtual Machine	Alert Definition	Virtual machine has CPU contention due to memory page swapping in the host
Virtual machine has memory contention caused by swap wait and high disk read latency	1 Object Type 2 vCenter Adapter > Virtual Machine	Alert Definition	Virtual machine has memory contention caused by swap wait and high disk read latency
Virtual machine has unexpected high disk I/O workload	1 Object Type 2 vCenter Adapter > Virtual Machine	Alert Definition	Virtual machine has unexpected high disk I/O workload
Virtual machine has disk I/O latency problem caused by snapshots	1 Object Type 2 vCenter Adapter > Virtual Machine	Alert Definition	Virtual machine has disk I/O latency problem caused by snapshots
Virtual machine has CPU contention due to multi-vCPU scheduling issues (co-stop) caused by snapshots	1 Object Type 2 vCenter Adapter > Virtual Machine	Alert Definition	Virtual machine has CPU contention due to multi-vCPU scheduling issues (co-stop) caused by snapshots
Not enough resources for vSphere HA to start the virtual machine	1 Object Type 2 vCenter Adapter > Virtual Machine	Alert Definition	Not enough resources for vSphere HA to start the virtual machine
vSphere HA cannot perform a failover operation for the virtual machine	1 Object Type 2 vCenter Adapter > Virtual Machine	Alert Definition	vSphere HA cannot perform a failover operation for the virtual machine
Standalone host has CPU contention caused by overpopulation of virtual machines	1 Object Type 2 vCenter Adapter > Host System	Alert Definition	Standalone host has CPU contention caused by overpopulation of virtual machines
Standalone host has memory contention caused by overpopulation of virtual machines	1 Object Type 2 vCenter Adapter > Host System	Alert Definition	Standalone host has memory contention caused by overpopulation of virtual machines
vSphere DRS enabled cluster has CPU contention caused by overpopulation of virtual machines	1 Object Type 2 vCenter Adapter > Cluster Compute Resource	Alert Definition	Fully-automated DRS-enabled cluster has CPU contention caused by overpopulation of virtual machines

Table 3-2. VM and Host Notifications in SDDC (Continued)

Name	Scope	Notification Trigger	Alert Definition
vSphere DRS enabled cluster has high CPU workload	1 Object Type	Alert Definition	Fully-automated DRS-enabled cluster has high CPU workload
	2 vCenter Adapter > Cluster Compute Resource		
vSphere DRS enabled cluster has memory contention caused by overpopulation of virtual machines	1 Object Type	Alert Definition	Fully-automated DRS-enabled cluster has memory contention caused by overpopulation of virtual machines
	2 vCenter Adapter > Cluster Compute Resource		
vSphere DRS enabled cluster has high memory workload and contention	1 Object Type	Alert Definition	Fully-automated DRS-enabled cluster has high memory workload and contention
	2 vCenter Adapter > Cluster Compute Resource		
vSphere HA failover resources are insufficient	1 Object Type	Alert Definition	vSphere High Availability (HA) failover resources are insufficient
	2 vCenter Adapter > Cluster Compute Resource		

Network-Related Notifications

Create notifications for important network-related issues in distributed switches and NSX components.

Table 3-3. Network-Related Notifications in SDDC

Name	Scope	Notification Trigger	Alert Definition
Distributed switch configuration is out of sync	1 Object Type	Alert Definition	Distributed Switch configuration is out of sync
	2 vCenter Adapter > vSphere Distributed Switch		
Host's NSX messaging infrastructure is reporting an issue	1 Object Type	Alert Definition	Host's NSX messaging infrastructure is reporting an issue
	2 vCenter Adapter > Host System		
NSX Manager resource usage is high	1 Object Type	Alert Definition	Manager resource usage is high
	2 NSX-vSphere Adapter > NSX-vSphere Manager		
NSX Manager API calls are failing	1 Object Type	Alert Definition	Manager API calls are failing
	2 NSX-vSphere Adapter > NSX-vSphere Manager		
VXLAN segment range has been exhausted	1 Object Type	Alert Definition	VXLAN segment range has been exhausted
	2 NSX-vSphere Adapter > NSX-vSphere Manager		
Less than three NSX Controllers are active	1 Object Type	Alert Definition	Less than three controllers are active
	2 NSX-vSphere Adapter > NSX-vSphere Controller Cluster		

Table 3-3. Network-Related Notifications in SDDC (Continued)

Name	Scope	Notification Trigger	Alert Definition
Edge resource usage is high	1 Object Type 2 NSX-vSphere Adapter > NSX-vSphere Edge	Alert Definition	Edge resource usage is high
High Availability is not configured correctly on the Edge	1 Object Type 2 NSX-vSphere Adapter > NSX-vSphere Edge	Alert Definition	High Availability is not configured correctly on the Edge
Edge VM is not responding to health check	1 Object Type 2 NSX-vSphere Adapter > NSX-vSphere Edge	Alert Definition	Edge VM is not responding to health check
One or more Load Balancer pool members are down	1 Object Type 2 NSX-vSphere Adapter > NSX-vSphere Edge	Alert Definition	One or more Load Balancer pool members are down

Storage Notifications

Create notifications for important storage issues.

Table 3-4. Storage Notifications in SDDC

Name	Scope	Notification Trigger	Alert Definition
Datastore is running out of disk space	1 Object Type 2 vCenter Adapter > Datastore	Alert Definition	Datastore is running out of disk space
Datastore has unexpected high Disk I/O workload	1 Object Type 2 vCenter Adapter > Datastore	Alert Definition	Datastore has unexpected high Disk I/O workload
Datastore has lost connectivity to a storage device	1 Object Type 2 vCenter Adapter > Datastore	Alert Definition	Datastore has lost connectivity to a storage device
After one additional host failure, vSAN Cluster will not have enough resources to rebuild all objects	1 Object Type 2 vSAN Adapter > vSAN Cluster	Alert Definition	After one additional host failure, vSAN Cluster will not have enough resources to rebuild all objects
vSAN Cluster Overall Health is Red	1 Object Type 2 vSAN Adapter > vSAN Cluster	Alert Definition	vSAN Cluster Overall Health is Red
vSAN Cluster flash read cache reservation is approaching capacity	1 Object Type 2 vSAN Adapter > vSAN Cluster	Alert Definition	vSAN Cluster flash read cache reservation is approaching capacity

Notifications for Site Recovery

Create notifications for important issues in Site Recovery.

Table 3-5. Site Recovery Notifications in SDDC

Name	Scope	Notification Trigger	Alert Definition
Protection Group is Not Configured	1 Object Type 2 SrmAdapter > Protection Groups	Alert Definition	Protection Group is Not Configured
Protection Group is Partially Recovered	1 Object Type 2 SrmAdapter > Protection Groups	Alert Definition	Protection Group is Partially Recovered
Protection Group is Recovering	1 Object Type 2 SrmAdapter > Protection Groups	Alert Definition	Protection Group is Recovering
Protection Group is Testing	1 Object Type 2 SrmAdapter > Protection Groups	Alert Definition	Protection Group is Testing
Recovery Plan Has Errors	1 Object Type 2 SrmAdapter > Recovery Plans	Alert Definition	Recovery Plan Has Errors
Recovery Plan Has Warnings	1 Object Type 2 SrmAdapter > Recovery Plans	Alert Definition	RecoveryPlan Has Warnings .
Is Pair Site Not Connected	1 Object Type 2 SrmAdapter > SRM Site	Alert Definition	Is Pair Site Not Connected
Site Not Paired	1 Object Type 2 SrmAdapter > SRM Site	Alert Definition	Site Not Paired
SRM Site Has Object(s) With Issues	1 Object Type 2 SrmAdapter > SRM Site	Alert Definition	SRM Site Has Object(s) With Issues

Notifications for vRealize Operations Manager

Create notifications for important issues in the operation of vRealize Operations Manager.

Table 3-6. Notifications for vRealize Operations Manager Issues

Name	Scope	Notification Trigger	Alert Definition
One or more vRealize Operations services on a node are down	1 Object Type 2 vRealize Operations Adapter > vRealize Operations Node	Alert Definition	One or more vRealize Operations services on a node are down
Disk space on a vRealize Operations Manager node is low	1 Object Type 2 vRealize Operations Adapter > vRealize Operations Node	Alert Definition	Disk space on node is low
Node processing queue is backing up	1 Object Type 2 vRealize Operations Adapter > vRealize Operations Node	Alert Definition	Node processing queue is backing up
FSDB failed to repair corrupted files	1 Object Type 2 vRealize Operations Adapter > vRealize Operations FsdB	Alert Definition	FsdB failed to repair corrupted files

Table 3-6. Notifications for vRealize Operations Manager Issues (Continued)

Name	Scope	Notification Trigger	Alert Definition
FSDB overload	1 Object Type 2 vRealize Operations Adapter > vRealize Operations FsdB	Alert Definition	FsdB high load
Number of objects being monitored by this vRealize Operations Manager node exceeds the configured limit. Possible loss of data	1 Object Type 2 vRealize Operations Adapter > vRealize Operations Analytics	Alert Definition	Number of Objects being monitored by this vRealize Operations Node exceeds the configured limit. Possible loss of data
One or more vRealize Operations services on a remote collector are down	1 Object Type 2 vRealize Operations Adapter > vRealize Operations Remote Collector	Alert Definition	One or more vRealize Operations services on a remote collector are down
Remote Collector not reporting correct number of services	1 Object Type 2 vRealize Operations Adapter > vRealize Operations Remote Collector	Alert Definition	Remote Collector not reporting correct number of services
vRealize Operations Cluster processes might be out of memory	1 Object Type 2 vRealize Operations Adapter > vRealize Operations Cluster	Alert Definition	vRealize Operations Cluster processes may not have enough memory

Monitor VADP Based Backup Solution Jobs by Email

4

It is recommended that your vSphere Storage APIs for Data Protection (VADP) Based Backup Solution support email notifications. Ensure that your backup solution has been configured to email, at a minimum, notifications about the status of backup jobs. This should be included in your daily monitoring activities to ensure that all management objects within the SDDC have successful backup images.

Configure vRealize Automation System Notification Events

5

You can receive automatic notifications for several types of events, such as the successful completion of a catalog request or a required approval.

System administrators can configure global email servers that handle email notifications.

Tenant administrators can override the system default servers, or add their own servers if no global servers are specified. Tenant administrators select which events, also known as notification scenarios. Each component, such as the service catalog or IaaS, can define events that can trigger notifications.

Each user can choose whether to receive notifications. Users either receive all notifications configured by the tenant administrator or no notifications, they do not have control over which notifications to receive.

Prerequisites

Verify that vRealize Automation has the inbound and outbound email servers configured. See *Configure the Default Email Servers in Region A* in *VMware Validated Design Deployment Guide for Region A*.

Procedure

- 1 Log in to the vRealize Automation Rainpole portal.
 - a Open a Web browser and go to **https://vra01svr01.rainpole.local/vcac/org/rainpole**.
 - b Log in using the following credentials.

Setting	Value
User name	vra-admin-rainpole
Password	vra-admin-rainpole_password
Domain	rainpole.local

- 2 On the **Home** page of the vRealize Automation management console, click the **Administration** tab and click **Notifications**.

- 3 Configure the scenarios to receive notifications about. NOTE: By default all scenarios are active.
 - a In the **Navigator**, click **Scenarios**.
 - b If you do not want to be alerted on a scenario, select it and click the **Suspend** button.
 - c Verify that each of the scenarios you want to receive notifications about has **Status** - Active.

The screenshot shows the 'Notification Scenarios' page in the Infrastructure Service Portal. The page title is 'Notification Scenarios' and it includes a sub-header: 'Select the scenarios for which to send notifications. To receive notifications, users must subscribe to notifications in their user preferences.' Below this is a table with columns for 'Source', 'Scenario', and 'Status'. The table lists various scenarios, all of which have a status of 'Active'. At the top of the table, there are 'Activate' and 'Suspend' buttons. The footer of the page contains copyright information and version details.

Source	Scenario	Status
Infrastructure Service	Alert on Host Reservation	Active
Infrastructure Service	Archive Period Expired	Active
Infrastructure Service	Custom Notification	Active
Infrastructure Service	EPI Register	Active
Infrastructure Service	EPI Unregister	Active
Infrastructure Service	Lease About To Expire (Manager)	Active
Infrastructure Service	Lease Expired (Manager)	Active
Infrastructure Service	Reclamation Expired Lease Modified (Manager)	Active
Infrastructure Service	Reclamation Forced Lease Modified (Manager)	Active
Infrastructure Service	Reclamation Expired Lease Modified	Active
Infrastructure Service	Reclamation Forced Lease Modified	Active
Infrastructure Service	VDI Register	Active
Infrastructure Service	VDI Unregister	Active
Catalog Service	Service Catalog Request Approved	Active
Catalog Service	Service Catalog Request Cancelled	Active
Catalog Service	Service Catalog Request Failed	Active
Catalog Service	Service Catalog Request Rejected	Active
Catalog Service	Service Catalog Request Submission	Active
Catalog Service	Service Catalog Request Successful	Active
Catalog Service	Resource Activated	Active
Catalog Service	Resource Archived	Active
Catalog Service	Resource Disposed	Active
Catalog Service	Resource Lease Pre-Expiration Notification	Active
Catalog Service	Resource Lease Enforcement Pending	Active
Catalog Service	Resource Lease Modified	Active
Catalog Service	Resource Owners Changed	Active
Catalog Service	Service Catalog Request Approved (Manager)	Active
Catalog Service	Service Catalog Request Failed (Manager)	Active
Catalog Service	Service Catalog Request Rejected (Manager)	Active
Catalog Service	Service Catalog Request Successful (Manager)	Active
Catalog Service	Resource Activated (Manager)	Active
Catalog Service	Resource Archived (Manager)	Active
Catalog Service	Resource Disposed (Manager)	Active
Catalog Service	Resource Lease Expiration Reminder (Manager)	Active
Catalog Service	Resource Lease Enforcement Pending (Manager)	Active
Catalog Service	Resource Lease Modified (Manager)	Active
Catalog Service	Resource Owners Changed (Manager)	Active
WorkItem Service	Reclamation Request	Active
WorkItem Service	Approval	Active
WorkItem Service	Manual User Action	Active

- 4 Subscribe to notifications from vRealize Automation.
 - a Click **Preferences** next to the **vra-admin-rainpole** user name on the top banner.
 - b Under **Notifications**, select **English (United States)** from the **Language** drop-down menu.
 - c Select **Enabled** next to the Email protocol, click **Apply** and click **Close**.

Notifications are now enabled for the **vra-admin-rainpole** account.