Monitoring and Alerting

27 MAR 2018
VMware Validated Design 4.2
VMware Validated Design for Software-Defined Data Center 4.2

vmware®

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

https://docs.vmware.com/

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

docfeedback@vmware.com

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

Contents

About 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 SDDC. This documentation also discusses enabling notifications about issues in your environment and operating a software-defined data center (SDDC) based on the VMware Validated Design™ for Software-Defined Data Center.

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 via SMTP for operations team notification.

The integration between vRealize Log Insight and vRealize Operations Manager allows for implementing the following cross-product event tracking:

- Sending alerts from vRealize Log Insight to vRealize Operations Manager, which automatically maps them to the target objects
- Launching in context from a vRealize Operations Manager object to the objects logs in vRealize Log Insight
- Launching 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 the 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. The alerts and queries are handled by the content packs for these products.

2 Enable the Alerts for vSphere Resources

Use the built-in problem and alert signatures in vRealize Log Insight for ESXi host and vCenter Server to enable alerts about issues in 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 to 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 in the SDDC 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 inbuilt 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 the 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. The alerts and queries are handled by the content packs for these products.

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	*vrli_admin_password*

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 ESXi host and vCenter Server to enable alerts about issues in 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 the vSphere components, use the following alerts:

Table 1-1. vSphere Alerts in vRealize Log Insight

Alert Name	Purpose	Severity
*** CRITICAL *** Hardware: Physical event detected	The purpose of this widget is to notify when the following physical hardware events have been detected, which indicates a hardware problem. Under most normal conditions, this widget should return no results. The following types of hardware events are returned ■ Advanced Programmable Interrupt Controller (APIC) ■ Machine Check Exception (MCE) ■ Non-Maskable Interrupt (NMI)	Critical
Hardware: Faulty memory detected	During the previous boot of an ESXi host faulty memory was detected. Unless a corresponding corrected message is seen, the memory should be replaced.	Critical
*** CRITICAL *** ESXi: Core dump detected	A core dump has been detected, which indicates the failure of a component in ESXi. This issue may lead to VM crashes and/or host PSODs.	Critical

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

Alert Name	Purpose	Severity
*** CRITICAL *** ESXi: Stopped logging	The purpose of this alert is to notify when an ESXi host has stopped sending syslog to a remote server.	Critical
*** CRITICAL *** ESXi: RAM disk / inode table is full	A root file system has reached its resource pool limit. Various administrative actions depend on the ability to write files to various parts of the root file system and might fail if the RAM disk and/or inode table is full.	Critical
ESXi: HA isolated events by hostname	During a health check, HA determined that a host was isolated. Depending on how HA is configured this may 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 the host(s) are marked as dead then VMs running on those hosts will be migrated to other systems.	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	*vrli_admin_password*

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)	*vsphere_alert_purpose* See Table 1-1.	*vsphere_alert_purpose* See Table 1-1.
Email	*Email address to send alerts to*	*Email address to send alerts to*
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)	*vsphere_alert_purpose* See Table 1-1.	*vsphere_alert_purpose* See Table 1-1.
Email	*Email address to send alerts to*	*Email address to send alerts to*
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 to 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 has become unavailable. Assuming other NICs are still online this 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 and/or the ESXi host may be possible.	Critical
Network: ESXi uplink redundancy lost	Only one physical NIC is currently connected, one more failure will result 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 virtual machine connectivity and may also lose connection with the vCenter Server. Other symptoms include: ■ 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.vMotions time-out ■ Restarting host management agents fail to complete 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	*vrli_admin_password*

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)	*networking_alert_purpose* See Table 1-6.	*networking_alert_purpose* See Table 1-6.
Email	*Email address to send alerts to*	*Email address to send alerts to*
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)	*networking_alert_purpose* See Table 1-6.	*networking_alert_purpose* See Table 1-6.
Email	*Email address to send alerts to*	*Email address to send alerts to*
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 indicates that one or more datastores is or was unavailable. As a result of this issue, VMs are or were unavailable and ESXi hosts may have been disconnected from vCenter Server. This issue requires immediate attention.	Critical
*** CRITICAL *** Storage: VSAN device offline	A Virtual SAN storage device that backs up the datastores might fail. This 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 failure. Virtual SAN automatically recovers data when new devices are added to the storage cluster, unless data lost is permanent.	Critical
Storage: NFS connectivity issue	The purpose of this alert is to notify when an NFS connectivity issue was detected. This means that an NFS datastore is or was unavailable. Do to this issue, one or more VMs may be unavailable.	Critical
Storage: NFS lock file issue	The purpose of this alert is to notify when an NFS lock file issue has been detected. Stale NFS lock files can prevent VMs from powering on.	Critical
Storage: SCSI Path dead	The purpose of this alert is to notify when a SCSI path has become unavailable. Assuming multiple paths are in use and the other paths are online this means reduced redundancy and performance. If all paths to a storage device become unavailable then VMs running on the storage device will become unavailable.	Critical
Storage: Snapshot consolidation required	The purpose of this alert is to notify when a snapshot consolidation is 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	*vrli_admin_password*

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)	*storage_alert_purpose* See Table 1-11.	*storage_alert_purpose* See Table 1-11.
Email	*Email address to send alerts to*	*Email address to send alerts to*
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)	*storage_alert_purpose* See Table 1-11.	*storage_alert_purpose* See Table 1-11.
Email	*Email address to send alerts to*	*Email address to send alerts to*
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 will fire when the state of any SSD changes to unhealthy. The reason could be either because of permanent disk failure, disk decommissioning, node shutdown, etc.	Critical
VSAN - Configuration failure - Insufficient space	This alert indicates that we cannot create a configuration for a new object(VM) in the VSAN cluster because sufficient space is not available in the cluster. If we see this error, please check the error logs and try the provisioning operation after adding new hosts/disks.	Critical
VSAN - Device Offline	This alarm will trigger if a particular device goes offline. In this case, please check the device configuration and other cluster state.	Critical
VSAN - Object component state changed to degraded	This alert will be triggered when VSAN object state changes to 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	`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	*vrli_admin_password*

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)	*vsan_alert_purpose* See Table 1-16.	*vsan_alert_purpose* See Table 1-16.
Email	*Email address to send alerts to*	*Email address to send alerts to*
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: ■ 301501 - This is vsm side event if host failed to respond with in time-out window ■ 301503 - This is vsm side event if vsm failed while provisioning firewall rule ■ 301506 - This is vsm side event if vsm failed to send exclude list update ■ 301031 - Failed to receive/parse/Update firewall config. Key value will have context info like generation number and also other debugging info	Critical
VMW_NSX_VXLAN dataplane lost connection to controller	This alert indicates VXLAN dataplane lost connection to controller.	Critical
VMW_NSX_VXLAN configuration issue	This alert is generated when VXLAN configuration pushed to host before host was prep'ed - host must be rebooted to initialize configuration in correct order.	Critical
VMW_NSX_Manager - Host Communication Errors	This event will be generated when NSX Manager fails to receive 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	*vrli_admin_password*

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)	*nsx_alert_purpose* See Table 1-19.	*nsx_alert_purpose* See Table 1-19.
Email	*Email address to send alerts to*	*Email address to send alerts to*
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (VMs)	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)	*nsx_alert_purpose* See Table 1-19.	*nsx_alert_purpose* See Table 1-19.
Email	*Email address to send alerts to*	*Email address to send alerts to*
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (VMs)	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 in the SDDC 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	The purpose of this alert is to notify when vROPs instance is not able to get the data back from vCenter instance within the 5 minute interval and the metrics back up and get dropped with the error: Communication Error: com.integrien.adapter.vmware.VcCollector.collectMetrics - Vc stats query timed out (ms): 300377. This is usually due to intermittent connection issues with the vCenter and hosts or down to the network not able to handle the request and timing out.	Critical
vRops: Out of Memory errors occurred	This alert gets generated when OutOfMemoryError: Java heap space occurs. This could indicate memory issues and could 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	`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	*vrli_admin_password*

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)	*vrops_alert_purpose* See Table 1-24.	*vrops_alert_purpose* See Table 1-24.
Email	*Email address to send alerts to*	*Email address to send alerts to*
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (VMs)	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!	A vRA CAFE service has become unavailable. This may happen because: ■ A service has failed - if the service does not automatically restart, this may impact vRA's ability to function ■ A service is blocked and cannot response at the moment - this may indicate increased load within the environment ■ vRA 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	A vRA service has become unavailable. This may happen because: ■ A service has failed - if the service does not automatically restart, this may impact vRA's ability to function ■ A service is blocked and cannot response at the moment - this may indicate increased load within the environment ■ Management Agent - in an HA deployment, only ONE Management Agent instance should be running. If more than one is running, this will cause issues with normal functioning of the system.	Critical
*** CRITICAL *** vRA disk is full	Windows host(s) have disk that is at capacity. If disk space runs out completely, it will impact the Infrastructure services provided by IaaS component of vRA and the Infrastructure tab will become unavailable from the vRA UI.	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	*vrli_admin_password*

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	VValue 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)	*vra_alert_purpose* See Table 1-27.	*vra_alert_purpose* See Table 1-27.
Email	*Email address to send alerts to*	*Email address to send alerts to*
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (VMs)	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 inbuilt 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	Error codes in this group will have severity levels 14 or 16. Login errors with severity level 14 would indicate security-related errors, such as permission denied. Login errors with severity 16 would indicate login error that can be rectified by user. The exact error message text appears in the line just after the error code and severity level. Detailed error description can be found on: http://technet.microsoft.com/en-us/library/cc645603%28v=sql.105%29.aspx	Critical
MS-SQL: Out of Memory (Resources)	Error codes in this group will have severity levels 17 or 16. 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 issues that can be addressed by the user. For further information on error codes falling in the category refer: http://technet.microsoft.com/en-us/library/cc645603%28v=sql.105%29.aspx	Critical
MS-SQL : Transaction Deadlocked	Transaction deadlock errors are usually characterized by severity level 13. This implies transaction was deadlocked on resources with another process and has been chosen as the deadlock victim. This signifies that you will have to re run the transaction. For further information on error codes falling in the category refer: http://technet.microsoft.com/en-us/library/cc645603%28v=sql.105%29.aspx	Critical
MS-SQL : Database Corruption	Database corruption is defined as a problem associated with the improper storage of the actual zeroes and ones needed to store you database data at the disk or IO sub-system level. Error codes in this group will have severity levels 20, 21, 22 or 23 or 16. You might need to check the logical and physical integrity of all the objects in the specified database. You can run DBCC CHECKDB to check for any database corruption. For more details on various error messages visit: http://technet.microsoft.com/en-us/library/cc645603%28v=sql.105%29.aspx For detailed information on MS SQL severity: http://msdn.microsoft.com/en-us/library/ms164086(v=sql.100).aspx	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	*vrli_admin_password*

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)	*mssql_alert_purpose* See Table 1-30.	*mssql_alert_purpose* See Table 1-30.
Email	*Email address to send alerts to*	*Email address to send alerts to*
Send to vRealize Operations Manager	Selected	Selected
Fallback Object (VMs)	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 Overview Dashboard

   This dashboard provides a summary of CPU, memory, and storage capacity provisioned, along with the resource reclamation opportunities available in all environments monitored by vRealize Operations Manager. Trend views within the dashboard allow you to predict running out of capacity.

2 Configure a Dashboard that Provides an Overview of SDDC Operation

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

SDDC Capacity Overview Dashboard

This dashboard provides a summary of CPU, memory, and storage capacity provisioned, along with the resource reclamation opportunities available in all environments monitored by vRealize Operations Manager. Trend views within the dashboard allow you to predict running out of capacity.

The Capacity Overview Dashboard provides you with a summary of the total physical capacity available across all your environments monitored by vRealize Operations Manager. The dashboard provides a summary of CPU, memory, and storage capacity provisioned as well as the resource reclamation opportunities available in those environments. Since capacity decisions are mostly tied to logical resource groups, the Capacity Overview dashboard allows you to assess capacity and utilization at each resource group level such as vCenter, datacenter, custom datacenter, or vSphere cluster. You can quickly select an object and view the total capacity and used capacity of the object. Capacity planning requires that you have visibility into the historical trends and future forecasts. The trend views within the dashboard provide you with this information to predict how soon you will run out of capacity.

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 **Home** page in the left pane of vRealize Operations Manager, click **Capacity Overview**.

3 You can use the **Capacity Overview** dashboard widgets in several ways.

a By using these widget categories, you can analyze the specific use cases and problems you are trying to resolve.

Dashboard Widget	Purpose/Usage
Total Environment Capacity	Use this widget to view the total available capacity in the environment, including information about the number of hosts and datastores. You can also view storage, memory, and CPU capacity, and the number of physical CPUs.
Select an Environment	Use this widget to select a data center, a cluster compute resource, or a vCenter Server. You can use the filter to narrow your list based on several parameters. After you identify the data center you want to view, select it. The dashboard is populated with the relevant data.
Total Reclamation Opportunity	Use this widget to view the reclaimable resources in the environment.
Total Capacity	Use this widget to view the total physical capacity of the environment, including capacity assigned as High Availability (HA). The actual capacity is less than the total capacity displayed when you consider HA and a buffer.
Used Capacity	Use this widget to view the capacity that has been used in your environment
Memory Capacity Utilization Trend (TB)	Use this widget to view the overall memory capacity trend. This widget displays the total physical resources you have. The physical resources include a HA buffer and a utilization buffer. This widget also displays the total memory you have allocated to VMs. If the number is close to the total physical capacity, the VMs may contend for memory. Ensure that the contention level is lower than what you promise to your customers. The chart also includes the actual utilization of memory capacity. The actual utilization is based on the active memory and hence it tends to be lower, as VMs do not normally access most of their RAM at any given moment.
CPU Capacity Utilization Trend (GHz)	Use this widget to view the overall CPU capacity trend. This widget displays the total physical resources you have. The physical resources include an HA buffer and a utilization buffer, which reflects the total capacity. This widget also displays the total CPU capacity you have allocated to VMs. If the number is close to the total physical capacity, the VMs may contend for CPU. Ensure that the contention level is lower than what you promise to your customers. The chart also includes the actual utilization of CPU. The actual utilization is based on the CPU demand counter, which takes into account the CPU used to perform I/O on behalf of the VM. The ESXi host performs storage I/O and network I/O on behalf of the VM, and this may be performed on a core that is different from the one on which the VM runs. As a result, CPU demand is a more accurate reflection of the VM CPU usage.
Disk Space Capacity Utilization Trend	Use this widget to view the amount of disk space allocated to a VM and the amount that is actually used. This information is helpful when you plan for thin provisioning
Cluster Capacity Details	Use this widget to view the capacity of each cluster in the environment. You can view details such as the number of VMs, hosts, datastores, and CPUs in each cluster. You can also view details such as the total CPU capacity and the provisioned CPU capacity, the total memory, and the provisioned memory in each cluster

b If you plan to report the current capacity situation to others within your organization, you can edit the **Cluster Capacity Details** widget on this dashboard and export this as a report for sharing purposes.

Configure a Dashboard that Provides an Overview of SDDC Operation

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

Procedure

1 Create an Application for vRealize Log Insight

Create an application in vRealize Operations Manager to group the monitoring data about the virtual machines of vRealize Log Insight.

2 Create an Application for VMware Site Recovery Manager

Create an application in vRealize Operations Manager to group the monitoring data about the virtual machines of VMware Site Recovery Manager.

3 Create an Application for VMware vSphere Replication

Create an application in vRealize Operations Manager to group the monitoring data about the virtual machines of VMware vSphere Replication.

4 Create an Application for VMware vRealize Operations Manager

Create an application in vRealize Operations Manager to group the monitoring data for the virtual machines of VMware vRealize Operations Manager.

5 Create an Application for VADP Based Backup Solution

Create an application in vRealize Operations Manager to group the monitoring data collected from your vSphere Storage APIs for Data Protection (VADP) based Backup Solution vitrual machines.

6 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)

7 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.

8 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 an Application for vRealize Log Insight

Create an application in vRealize Operations Manager to group the monitoring data about the virtual machines of vRealize Log Insight.

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 of the components.

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	*vrops_admin_password*

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

Create an application in vRealize Operations Manager to group the monitoring data about the virtual machines of VMware Site Recovery Manager.

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	*vrops_admin_password*

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

Create an application in vRealize Operations Manager to group the monitoring data about the virtual machines of VMware vSphere Replication.

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 for each application 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	*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 **`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

Create an application in vRealize Operations Manager to group the monitoring data for the virtual machines of VMware vRealize Operations Manager.

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	*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 **`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 **`vrops01`** 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

Create an application in vRealize Operations Manager to group the monitoring data collected from your vSphere Storage APIs for Data Protection (VADP) based Backup Solution vitrual machines.

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 for each application 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	*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 name of **`<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	*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 **`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	*vrops_admin_password*

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**
- **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 has the following two aspects:

- Display the main indicators for the state of CPU, memory, connectivity, and storage in the management cluster that hosts the management applications.
- Show 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 dashboard consists of the following widgets:

- 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.
- One Health Chart widget

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

Widget Setting	Heatmap 1.1	Heatmap 1.2	Heatmap 1.3	Heatmap 1.4
Title	Physical CPU Remaining	Physical Memory Remaining	Management VM CPU Used	Management VM CPU Contention
Refresh Content	On	On	On	On
Refresh Interval	300s	300s	300s	300s
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	-	-	-	-
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	CPU > Capacity Remaining (%)	Memory > Capacity Remaining (%)	CPU > Usage (%)	CPU > CPU Contention (%)
Min Value (Color)	0 (red)	0 (red)	80 (green)	0 (green)
Max Value (Color)	25 (green)	25 (green)	100 (red)	2 (red)
Filter	-	-	■ Adapter Instances > vCenter Server > sfo01m01vc01 ■ Adapter Instances > vCenter Server > lax01m01vc01	■ 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 Dashboard

Widget Setting	Heatmap 2.1	Heatmap 2.2	Heatmap 2.3	Heatmap 2.4
Title	Physical Network I/O	Physical Dropped Packets	Management VM Memory Used	Management VM Swap Rate
Refresh Content	On	On	On	On
Refresh Interval	300s	300s	300s	300s
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	-	-	-	-

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

Widget Setting	Heatmap 2.1	Heatmap 2.2	Heatmap 2.3	Heatmap 2.4
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	Network I/O > Demand (%)	Network I/O > Packets Dropped	Memory > Usage (%)	Memory > Swapped (KB)
Min Value (Color)	80 (green)	0 (green)	50 (green)	0 (green)
Max Value (Color)	100 (red)	1 (red)	90 (red)	1 (red)
Filter	-	-	■ Adapter Instances > vCenter Server > sfo01m01vc01 ■ Adapter Instances > vCenter Server > lax01m01vc01	■ 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 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 Free
Refresh Content	On	On	On	On
Refresh Interval	300s	300s	300s	300s
Name	Datastores	Datastores	Management VMs	Management VMs
Group by	Storage Devices > VirtualSAN Datastore	Storage Devices > NFS Volume	vCenter Adapter > Datacenter	vCenter Adapter > Datacenter
Then by	-	-	-	-
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)	Disk Space > Capacity Remaining (%)
Min Value (Color)	0 (green)	0 (green)	0 (green)	5 (red)
Max Value (Color)	30 (red)	30 (red)	30 (red)	20 (green)
Filter	-	-	■ Adapter Instances > vCenter Server > sfo01m01vc01 ■ Adapter Instances > vCenter Server > lax01m01vc01	■ Adapter Instances > vCenter Server > sfo01m01vc01 ■ Adapter Instances > vCenter Server > lax01m01vc01

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

Health Widget Setting	Value
Title	Management Applications
Refresh Content	On
Refresh Interval	300s
Self Provider	On
Mode	Children
Order By	Value Asc
Pagination number	15
Period Length	Last 6 hours
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 **Dashboard**.

3 Select **Create Dashboard** from the **Actions** menu.

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 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 **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 the SDDC operators know 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 the SDDC operators know 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://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 **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	Virtual machine is projected to run out of disk space
Method	Standard Email Plugin
Instance	SMTP Alert Mail Relay
Recipient(s)	*Email address to send alerts to*
Filtering Criteria	
Scope	Object Type
Object Type	**vCenter Adapter > Virtual Machine**

5 Configure the trigger for the notification.

a In the **Filtering Criteria** section of the **Add Rule** dialog box, select **Alert Definition** from the **Notification Trigger** drop-down menu.

b Click the **Select an Alert Definition** button.

c In the **Quick filter (Name)** text box of the **Alert Definitions** dialog, enter **`disk space`** and press Enter.

d Select the **Virtual machine is projected to run out of disk space** alert definition and click **Select**.

6 In the **Add Rule** dialog, click **Save**.

7 Repeat the steps to create the other 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	*Email address to send alerts to*

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
Virtual machine is projected to run out of disk space	1 Object Type 2 **vCenter Adapter > Virtual Machine**	Alert Definition	Virtual machine is projected to run out of disk space
Virtual machine has CPU contention caused by co-stop	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 unexpected high CPU workload	1 Object Type 2 **vCenter Adapter > Virtual Machine**	Alert Definition	Virtual machine has unexpected high CPU workload
Virtual machine has unexpected high memory workload	1 Object Type 2 **vCenter Adapter > Virtual Machine**	Alert Definition	Virtual machine has unexpected high memory 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 is running out of disk space	1 Object Type 2 **vCenter Adapter > Virtual Machine**	Alert Definition	Virtual Machine is running out of disk space
Virtual machine has large disk snapshots	1 Object Type 2 **vCenter Adapter > Virtual Machine**	Alert Definition	Virtual machine has large disk 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 2 **vCenter Adapter > Cluster Compute Resource**	Alert Definition	Fully automated DRS-enabled cluster has high CPU workload
vSphere DRS enabled cluster has memory contention caused by overpopulation of virtual machines	1 Object Type 2 **vCenter Adapter > Cluster Compute Resource**	Alert Definition	Fully automated DRS-enabled cluster has memory contention caused by overpopulation of virtual machines
vSphere DRS enabled cluster has high memory workload and contention	1 Object Type 2 **vCenter Adapter > Cluster Compute Resource**	Alert Definition	Fully automated DRS-enabled cluster has high memory workload and contention
vSphere HA failover resources are insufficient	1 Object Type 2 **vCenter Adapter > Cluster Compute Resource**	Alert Definition	vSphere High Availability (HA) failover resources are insufficient

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

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

Name	Scope	Notification Trigger	Alert Definition
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 is projected to run out of disk space	1 Object Type 2 **vCenter Adapter > Datastore**	Alert Definition	Datastore is projected to run out of disk space
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 health checks are reporting issues	1 Object Type 2 **vSAN Adapter > vSAN Cluster**	Alert Definition	vSAN cluster health checks are reporting issues
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

Table 3-5. Site Recovery Notifications in SDDC (Continued)

Name	Scope	Notification Trigger	Alert Definition
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
FSDB overload	1 Object Type 2 **vRealize Operations Adapter > vRealize Operations Fsdb**	Alert Definition	Fsdb high load

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

Name	Scope	Notification Trigger	Alert Definition
Number of objects 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 monitored by this vRealize Operations Node exceeds the configured limit. Possible loss of data
Remote Collector one or more vRealize Operations services 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

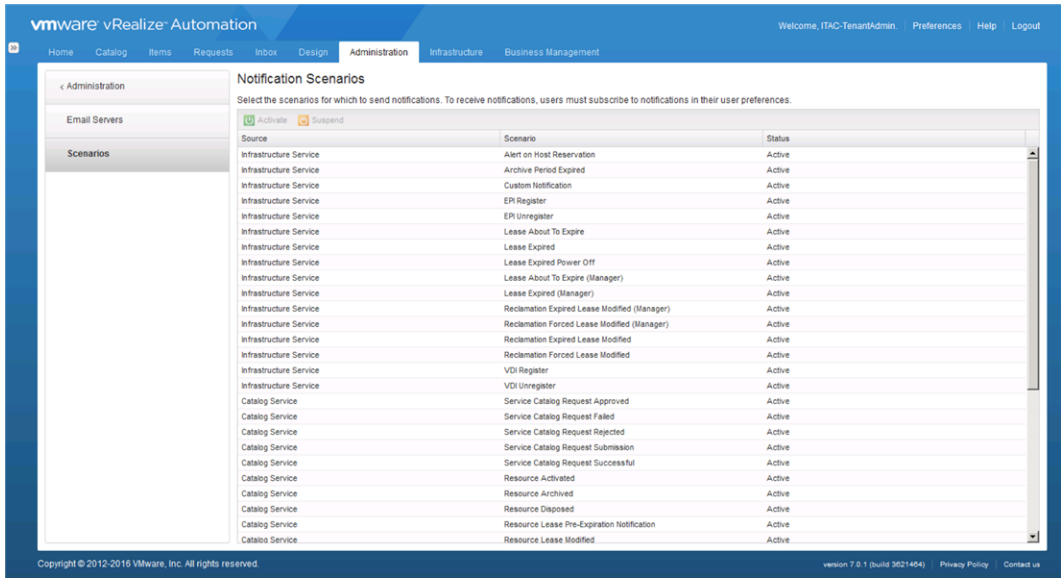
2 On the **Home** page of the vRealize Automation management console, click the **Administration** tab and click **Notifications**.

3 Configure the scenarios to receive notifications about. NOTE: By default all scenarios are active.

a In the **Navigator**, select **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`.



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.