Deployment Scenarios

VMware Smart Assurance 10.1.0
You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/
## Contents

### 1 Deployment Scenarios 5
- VeloCloud SD-WAN Monitoring 5
  - Overview 6
  - Install and Configure 22
  - Troubleshooting Steps 35
- Virtual IMS Assurance 41
  - Overview 42
  - Install and Configure 54
  - Troubleshooting Steps 59
- VMware Integrated Openstack Management 60
  - Overview 60
  - Install and Configure 68
  - Troubleshooting Steps 70
- vCloud Director Management 72
  - Overview 72
  - Install and Configure 82
  - Troubleshooting Steps 87
- Cisco ACI SDN Monitoring 88
  - Overview 89
  - Install and Configure 94
  - Troubleshooting Steps 103
- vROps Alerts Subscription 105
  - SAM Configuration 105

### 2 Core Platform 107
- Data Store 107
  - Installing MongoDB 107
  - Installing Redis 108
  - Installing Elastic Search 114
- Messaging 117
  - Installing Kafka 117
- Data Management 125
  - Installing Data Collection Framework 125
  - Performing Upgrade 132
  - Data Collection Controller 134
  - KPI Engine (K4M) 136
- Domain Manager 145
  - Installation 145
UI Components 175
  Installing Global Console 175
  Installing Notification UI 175
  Installing Eventstore 176
  Installing cAPI 186
  Installing Smarts-UI 193
Deployment Scenarios

This chapter includes the following topics:

- VeloCloud SD-WAN Monitoring
- Virtual IMS Assurance
- VMware Integrated Openstack Management
- vCloud Director Management
- Cisco ACI SDN Monitoring
- vROps Alerts Subscription

VeloCloud SD-WAN Monitoring

This section provides end to end installation and configuration of VeloCloud Smart Assurance.
VeloCloud Architecture

Overview

VeloCloud is a cloud network service solution enabling sites to quickly deploy Enterprise grade access to legacy and cloud applications over both private networks and Internet broadband.

The following diagram shows the VeloCloud Software-defined WAN solution (SDWAN) components (in orange).
Discovery Flow

The Server Manager imports initial topology from the IP Availability Manager. After the topology is imported, Server Manager discovers domain-specific entities related to the features and creates additional topology objects for those features.

As a first step of discovery, VeloCloud Orchestrator (VCO) is discovered based on ICMP discovery. If the orchestrator device is not ICMP pingable, then workaround would be to add the device manually to the IP server. See Case 2 mentioned in the Installing SMARTS IP-AM section, to manually add the orchestrator device to IP server. On discovery of VeloCloud Orchestrator (Host) in SMARTS-IP domain manager, SMARTS ESM server imports the Host from IP Domain Manager and further does a complete discovery of Velocloud topology.

Monitoring Flow

For first time when discovery is initiated from SMARTS Domain Manager, DCF controller (part of the DCF framework) managing the lifecycle of the collectors instantiates and deploys the VeloCloud Discovery and Monitoring Collectors. The polling configuration applied to the VeloCloud Monitoring Collector polls VeloCloud Orchestrator based on specified polling cycle and frequency. The monitoring collector polls for the status attribute of the discovered Velocloud topology objects.

Topology

This section provides information on specific classes, attributes, relationships, and events related to VeloCloud.

VeloCloud versions 3.4.0 and 3.4.1 are supported.
<table>
<thead>
<tr>
<th>Class</th>
<th>Key Attributes</th>
<th>Key relationship</th>
<th>Problem and Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orchestrator</td>
<td>■ IsDiscoveryFailure</td>
<td>■ Supervises :: Tenant</td>
<td>■ DiscoveryFailure</td>
</tr>
<tr>
<td></td>
<td>■ IsMonitoringFailure</td>
<td>■ Orchestrate :: Vedge/VGateway</td>
<td>■ MonitoringFailure</td>
</tr>
<tr>
<td></td>
<td>■ IsManaged</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VEdge</td>
<td>■ IsActivated</td>
<td>■ ConnectedGateway :: VGateway</td>
<td>■ Down</td>
</tr>
<tr>
<td></td>
<td>■ IsInActiveStandByMode</td>
<td>■ ConnectedLink :: VGateway</td>
<td>■ VNFDOWN</td>
</tr>
<tr>
<td></td>
<td>■ IsHub</td>
<td>■ SpokeEdges :: VEdge</td>
<td>■ NotActivated</td>
</tr>
<tr>
<td></td>
<td>■ IsSpoke</td>
<td>■ HubEdges :: VEdge</td>
<td>■ HAReduced</td>
</tr>
<tr>
<td></td>
<td>■ StatusIsDown</td>
<td>■ OrchestratedBy :: Orchestrator</td>
<td>■ SpokeEdgeImpaired</td>
</tr>
<tr>
<td></td>
<td>■ IsHAReduced</td>
<td>■ ProvidesConnectivityTo :: Tenant</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ ProvidesApplicationConnectivityTo :: AppType</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VGateway</td>
<td>■ IsActivated</td>
<td>■ ConnectedVEdge :: VEdge</td>
<td>■ Down</td>
</tr>
<tr>
<td></td>
<td>■ StatusIsDown</td>
<td>■ ConnectedNonVCSite :: NonVCSiteRouter</td>
<td>■ VNFDOWN</td>
</tr>
<tr>
<td></td>
<td>■ ConnectedLinkNonVCSite :: NetworkConnection</td>
<td>■ OrchestratedBy :: Orchestrator</td>
<td>■ NotActivated</td>
</tr>
<tr>
<td></td>
<td>■ OrchestratedBy :: Orchestrator</td>
<td>■ ProvidesConnectivityTo :: Tenant</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ ProvidesApplicationConnectivityTo :: AppType</td>
<td></td>
<td></td>
</tr>
<tr>
<td>NonVCSiteRouter</td>
<td>■ IsAllGatewayDown</td>
<td>■ ConnectedGateway :: VGateway</td>
<td>■ ReducedConnectivity</td>
</tr>
<tr>
<td></td>
<td>■ IsAnyGatewayDown</td>
<td>■ ConnectedTunnel :: NetworkConnection</td>
<td>■ ConnectivityLost</td>
</tr>
<tr>
<td></td>
<td>■ IsAllTunnelDown</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ IsAnyTunnelDown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VEdgeRedundancyGroup</td>
<td>■ ComposedOf :: VEdge</td>
<td>■ ReducedRedundancy</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ AtRisk</td>
<td>■ AllComponentsDown</td>
<td></td>
</tr>
<tr>
<td>AppType/Tunnel/Tenant</td>
<td>■ Impaired</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Root Cause and Impact Analysis**

This section provides information on root cause and impact analysis for various events.

Below are the root-cause problem diagnosed and the impacted classes.
Table 1-1. Root-cause problems for VeloCloud classes

<table>
<thead>
<tr>
<th>Class</th>
<th>Root cause</th>
<th>Event (symptoms) of root cause</th>
<th>Impacted Class</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>VEdge</td>
<td>Down</td>
<td>VEdge ::VNFDown</td>
<td>VEdge</td>
<td>SpokeImpaired</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkConnection::Down</td>
<td>VEdge</td>
<td>VNFDOWN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OrFlapping</td>
<td>AppType</td>
<td>Impaired</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Tenant</td>
<td>Impaired</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NetworkConnection</td>
<td>DownOrFlapping</td>
</tr>
<tr>
<td>VGateway</td>
<td>Down</td>
<td>VGateway::VNFDown</td>
<td>VGateway</td>
<td>VNFDOWN</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkConnection::Down</td>
<td>NetworkConnection</td>
<td>DownOrFlapping</td>
</tr>
<tr>
<td></td>
<td></td>
<td>OrFlapping</td>
<td>Tenant</td>
<td>Impaired</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>NonVCSiteRouter</td>
<td>ConnectivityLost/ ReducedConnectivity</td>
</tr>
<tr>
<td>Interface</td>
<td>Down</td>
<td>Interface::DownOrFlapping</td>
<td>Tenant</td>
<td>Impaired</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkConnection::Down</td>
<td>NetworkConnection</td>
<td>DownOrFlapping</td>
</tr>
<tr>
<td>Router</td>
<td>Unresponsive</td>
<td>Router::Unresponsive</td>
<td>Tenant</td>
<td>Impaired</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NetworkConnection::Down</td>
<td>NetworkConnection</td>
<td>DownOrFlapping</td>
</tr>
</tbody>
</table>

**Note**  The Interface Down and Router Unresponsive root causes scenarios are for the MPLS PE router interface and the PE Router that an Edge connects.

**Root Cause and Impact Analysis – Edge Down**

VCO Reports:
- Edge as down
- Edge link as unstable

Smarts Notifies:
- VNFDOWN event and Down problem as the root cause.
- Impaired event for the tenant.
- Impaired event for the Application types in the profile that is applied for the edge.
- SpokeEdgeImpaired event for all the spoke edges (if this edge that is down is configured as hub).

The Down problem shows the Tenant, AppType, and SpokeEdge Impaired events as Impacts.
Root Cause and Impact Analysis – Edge HA StandBy Down

VCO Reports: The Standby Edge in Active/StandBy HA as down. The Active Edge is up.

Smarts Notifies: HAReduced event.

There is no root cause or impact for this events.
Root Cause and Impact Analysis – Edge HA (Active/Active)

VCO Reports: Some/All of the edges in the edge cluster (Active/Active HA) goes down.

Smarts Notifies: One of the below events on the redundancy group depending on the number of edges that are down.

- AtRisk
- ReducedRedundancy
- AllComponentsDown

The redundancy group event is shown as the impact for the edge down.
Root Cause and Impact Analysis – Edge Hub Down

VCO Reports: Edge that is configured as hub is down.

Smarts Notifies:

- VNFDOWN event and Down problem as the root cause for the Edge that is reported as down.
- SpokeEdgeImpaired event for all the spoke edges

The SpokeEdgeImpaired event is shown as the impact for the Edge down.
Root Cause and Impact Analysis – Edge WAN link goes down

VCO Reports: The Edge WAN link as down.

Smarts Notifies:

- DownOrFlapping event and Down problem for the NetworkConnection as the root cause.
- Impaired event for the tenants.

The Down problem shows the Tenant Impaired and Network Connection DownOrFlapping as Impacts.
Root Cause and Impact Analysis – Edge/Gateway Admin down

VCO Reports: Edge/Gateway is not provisioned.
Smarts Notifies: NotActivated event.
There is no root cause or impact for this events.
Root Cause and Impact Analysis – Gateway down

VCO Reports: Gateways is reported as down.

Smarts Notifies:

- VNFDOWN event and Down problem as the root cause for the Gateway.
- Impaired event for the impacted tenant.

The Impaired event is shown as the impact for the Gateway down.
Root Cause and Impact Analysis – All Gateways for an Edge is down

VCO Reports:
- All the Gateways for an Edge is reported as down.
- All NetworkConnection for the Edge is reported as Down.

Smarts Notifies:
- VNFDOWN event and Down problem as the root cause for the Gateway.
- Impaired event for the impacted tenant.
- NetworkConnection DownOrFlapping event for the Edge links.

The Impaired and the DownOrFlapping events are shown as the impact for the Gateway down. This will appear as impact in both the Gateway Down problem.
Root Cause and Impact Analysis – Non VC site Gateway down

VCO Reports: One of the Gateways connecting to Non VC Site router is down.

Smarts Notifies:

- VNFDown event and Down problem as the root cause for the Gateway.
- ReducedConnectivity event for the NonVCSiteRouter.
- Impaired event for the impacted tenant.

The Impaired and ReducedConnectivity events are shown as the impact for the Gateway down. Similar Impacts are shown when one of the NetworkConnections goes down with NetworkConnection Down as the root cause.
Root Cause and Impact Analysis – MPLS PE Router Down

VCO Reports: NetworkConnection Down.

Smarts Notifies:

- Router Down as root cause.
- NetworkConnection DownOrFlapping event.
- Impaired event for the impacted tenant.

The Impaired and DownOrFlapping events are shown as the impact for the Router down.

In this scenario, the VCO does not report Edge as down as it has a secondary link. But, if MPLS link is the only link then Edge VNFDOWN event will also come as impact. Edge Down will not be activated.

**Note** This scenario needs configuration to stitch VC and MPLS Edge topology.
Root Cause and Impact Analysis – MPLS PE Interface Down/Disabled

VCO Reports: NetworkConnection down

Smarts Notifies:
- Interface Down/Disabled.
- NetworkConnection DownOrFlapping event.
- Impaired event for the impacted tenant.

The Impaired and DownOrFlapping events are shown as the impact for the Interface Down/Disabled.

In this scenario, the VCO does not report Edge as down as it has a secondary link. But, if MPLS link is the only link then Edge VNFDOWN event will also come as impact. Edge Down will not be activated.

**Note**  This scenario needs configuration to stitch VC and MPLS Edge topology.
Root Cause and Impact Analysis – MPLS Core Network Router Down

Smarts Notifies:

- MPLS Core Router Down as root cause.
- Tunnel Impaired.

The Impaired event is as the impact for the Router Down.

**Note** This scenario needs configuration to stitch VC and MPLS Core topology. An Smarts MPLS server instance is also needed.
Root Cause and Impact Analysis – MPLS Core Network Interface Down

Smarts Notifies:

- Interface Down/Disabled
- Impaired event for the impacted Tunnel.

The Impaired event is shown as the impact for the Interface Down/Disabled.

**Note**  This scenario needs configuration to stitch VC and MPLS Core topology. An Smarts MPLS server instance is also needed.
Install and Configure

This section provides information on installation and configuration of open source and VSA components.

**Note** Perform the installation of the following VSA Components prior to further configurations.

**Messaging**
Refer, [Installing Kafka](#)

**SMARTS**
Refer, [Domain Manager](#)

**Data Management**
Refer, [Installing Data Collection Framework](#)
Refer, [Data Collection Controller](#)

**Notification UI**
Refer, [UI Components](#)

**Configuration**
This section provides information on custom configuration from Server Manager side.
The configuration to manage an VCO, falls in to four categories and three of these are configured using Device Access tab in the Polling & Threshold window of Global administrator console.

**Installing SMARTS IP-AM**

To install IP-AM, refer [Performing an Installation](#).

**Procedure**

1. No configuration is required in IP server specific for VeloCloud.

2. Discovery Steps for Velocloud Discovery:

   a. This has to be the final step that triggers the discovery of VeloCloud components in the ESM server. So, a prerequisite is that the ESM is installed and configured before executing this step.

   1. **Case 1**: ICMP is enabled on the VCO. The VeloCloud orchestrator needs to be discovered in IP domain which in turn trigger the ESM for VeloCloud specific discovery. If ICMP pings are enabled on VCO the VCO has to be discovered as an ICMPONLY device. Refer [Starting discovery from the console](#) or [Starting discovery from the command line](#).

   2. **Case 2**: ICMP is not enabled on the VCO. In this case, the VCO host needs to be created using the following `dmctl` command replacing the `<ip address>` with the VCO ip address:

```
create Host::<ip address>
create SNMPAgent::SNMPAgent-<ip address>
create IP::IP::<ip address>
insert Host::<ip address>::HostsServices SNMPAgent::SNMPAgent-<ip address>
insert Host::<ip address>::HostsAccessPoints IP::IP::<ip address>
put SNMPAgent::SNMPAgent-<ip address>::AgentAddress <ip address>
get SNMPAgent::SNMPAgent-<ip address>::LayeredOver
insert SNMPAgent::SNMPAgent-<ip address>::LayeredOver IP::IP::<ip address>
```

**Installing SMARTS ESM**

See the [Performing an Installation](#) for more information.

**Procedure**

1. See the #unique_20 and #unique_21 for DCF and Kafka configuration.

2. Optional: Correlating MPLS edge faults to VC faults or propagating MPLS core network faults to activate VC Tunnel fault events needs additional configuration. Refer, [MPLS Edge and Core Network stitching](#) for configuration.
Configuring Users and Tenant Filtering

Smarts can be configured to use one of the operator, MSP, or enterprise user for discovering and monitoring the VeloCloud orchestrator. Also, there is a flexibility to opt for only a subset of Tenants when using the MSP and operator user. When a subset of interested tenants is specified using a regex, the discovery and monitoring only deal with VeloCloud topology that belongs to these Tenants.

In summary Smarts provides:

- Support for operator, MSP, and enterprise user types.
- Enterprise filtering for operator and MSP users.

Table *Parameters and Descriptions* illustrates about the new parameters and their descriptions in the ESM file.

**Table 1-2. Parameters and Descriptions**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Descriptions</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCO_USERTYPE-&lt;Orchestrator_host_IP_address&gt;</td>
<td>Defines the VeloCloud user type.</td>
</tr>
<tr>
<td>operator</td>
<td>enterprise</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td>VCO_ENTERPRISE_FILTER-&lt;Orchestrator_host_IP_address&gt; &lt;REGEX FILTER&gt;</td>
<td>Defines the RegEx pattern for list of enterprises in the VeloCloud that ESM discovers and monitors. The regex pattern must confirm to patterns defined in java.util.regex documentation. This is an optional parameter. Default filter is .* (i.e discover all enterprises that belong to a specific user). For example, if ESM discovers two Tenants, &quot;A&quot; and &quot;B&quot;, then the parameter can be defined as &quot;A</td>
</tr>
<tr>
<td>VCO_HTTP_RESPONSE_TIMEOUT-&lt;Orchestrator_host_IP_address&gt; &lt;Time in Seconds&gt;</td>
<td>Defines the http timeout for response in seconds for VeloCloud discovery and monitoring collector while fetching Topology using REST API. This is an optional parameter. Minimum, Default, and Maximum values are; 120, 240 and 600 respectively.</td>
</tr>
<tr>
<td>VCO_DISCOVERY_TIMEOUT-&lt;Orchestrator_host_IP_address&gt; &lt;Time in Seconds&gt;</td>
<td>Defines the discovery collector timeout in seconds for VeloCloud discovery. This is an optional parameter. Minimum, Default, and Maximum values are; 3600, 15000 and 36000 respectively.</td>
</tr>
<tr>
<td>Parameters</td>
<td>Descriptions</td>
</tr>
<tr>
<td>------------</td>
<td>--------------</td>
</tr>
<tr>
<td>VCO_COLLECTOR_DISCOVERY_LOG_LEVEL-&lt;Orchestrator_host_IP_address&gt; &lt;LOGLEVEL&gt;</td>
<td>Defines the VeloCloud collector logging level for discovery. Valid debug levels are: WARNING, SEVERE, OFF, INFO, FINEST, FINER, FINE, CONFIG, ALL. This is an optional parameter and if not defined, the default loglevel value is INFO.</td>
</tr>
<tr>
<td>VCO_COLLECTOR_MONITORING_LOG_LEVEL-&lt;Orchestrator_host_IP_address&gt; &lt;LOGLEVEL&gt;</td>
<td>Defines the VeloCloud collector logging level for monitoring. Valid debug levels are: WARNING, SEVERE, OFF, INFO, FINEST, FINER, FINE, CONFIG, ALL. This is an optional parameter and if not defined, the default loglevel value is INFO.</td>
</tr>
<tr>
<td>VCO_COLLECTOR_MAX_HEAP_MEMORY-&lt;Orchestrator_host_IP_address&gt; &lt;MaxHeapSize&gt;</td>
<td>Defines the VeloCloud collectors maximum heap memory size (in Mega Bytes) for discovery and monitoring. This is an optional parameter. Minimum, Default, and Maximum values are; 64, 2048, and 4096 respectively.</td>
</tr>
<tr>
<td>VCO_KAFKA_ADAPTER_QUEUE_HIGH_WATERMARK &lt;integer value&gt;</td>
<td>By default, ESM reads all the available messages in the kafka bus. The read messages (discovery/monitoring) are stored in ESM process memory. If the processing of these message by ESM is slower than the message producer then it can result in higher memory footprint for ESM. This default behavior can be changed by setting a high and low water mark for the kafka adapter internal queue. Both high and low must be set in this case. VCO_KAFKA_ADAPTER_QUEUE_HIGH_WATERMARK parameter is for specifying the maximum size of the kafka adapter internal queue size at which the consumer is stopped to minimize the memory footprint of the ESM server. For example, VCO_KAFKA_ADAPTER_QUEUE_HIGH_WATERMARK 50000 can ensure that after beyond 50k messages being in the kafka adapter’s internal buffer the consumption of further messages from the kafka bus is stopped.</td>
</tr>
<tr>
<td>VCO_KAFKA_ADAPTER_QUEUE_LOW_WATERMARK &lt;integer value&gt;</td>
<td>Specifies the minimum size of the kafka adapter internal queue size at which the consumer is restarted. Refer the description of the VCO_KAFKA_ADAPTER_QUEUE_HIGH_WATERMARK. Both high and low water mark must be specified. By default, this is disabled and in this case the kafka adapter makes reads all the available messages from the kafka bus. For example, VCO_KAFKA_ADAPTER_QUEUE_LOW_WATERMARK 10000 restarts the message consumption from the kafka bus once the internal queue size drops below 10k.</td>
</tr>
</tbody>
</table>
Note  The following parameters must be modified in esm-param.conf file to discover a Topology having around 3500 Vedges, the parameters must be modified in esm-param.conf file based on user deployment:

- **MessagePollTimeoutPeriodInSeconds--<kafka_IP_Address> 2400**  
  When the latency between orchestrator and the DCF collector is higher, set the flag to a higher value. This flag dictate the timeout value for the ESM to wait for messages from kafka. If the timeout expires, then the discovery stops abruptly.
  Minimum, Default, and Maximum values are; 60, 1200 and 3000 respectively.

- **VCO_HTTP_RESPONSE_TIMEOUT--<Orchestrator IP> 240**  
  The timeout value for the http request that the DCF collector sends to the orchestrator. While configuring this value, the processing time of the orchestrator must also be considered into account as some of the REST API takes longer time to return.

- **VCO_DISCOVERY_TIMEOUT--<Orchestrator IP> 18000**  
  Increase the value of this parameter based on the topology size. This is the maximum time in seconds that the collector runs before stopping abruptly. This is a safeguard measure to prevent the collector from running under a false condition.

Configure Orchestrator credentials through GUI

To configure Server Manager to communicate with Orchestartor, specify the Orchestrator administrator credentials and the IP address of the Orchestrator host.

**Prerequisites**

For this task, when you use the console, you need to have Smarts administrator credentials to open the Configure menu where you specify the Orchestrator credentials.

**Procedure**

1. At BASEDIR/smarts/bin, type the following command:
   ```bash
   ./sm_edit conf/esm/esm-param.conf
   ```
2. Enter the following line for Orchestrator
   ```bash
   # If the Orchestrator is VELOCLOUD then usertype must be provided in the below format
   VCO_USERTYPE-xx.xx.xx.xx operator|enterprise|MSP
   ```
   For Example: VCO_USERTYPE-xx.xx.xx.xx operator
3. Restart the ESM server if it is already running to take above configuration changes into effect.
4. Open the **Service Assurance Manager Global Console** attached to the Server Manager (INCHARGE-ESM, by default).
In the **Topology Browser Console**, select **Configure > Domain Manager Administration Console**.

Right-click the ESM server in the left pane and select **Configure ESM credentials**.

In the **Configure ESM credentials** dialog box, select **Orchestrator** for the host type.

Type values in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>IP address of the Orchestrator host.</td>
</tr>
<tr>
<td>User ID</td>
<td>Orchestrator user name. The VeloCloud user can be an Operator user, MSP user, or Enterprise user. Only the operator user has the privilege to use the REST API that is used for discovery and monitoring.</td>
</tr>
<tr>
<td>Password</td>
<td>Orchestrator administrator password for respective User ID.</td>
</tr>
<tr>
<td>Port</td>
<td>Orchestrator port.</td>
</tr>
</tbody>
</table>

Click **Apply credential with testing**.

Verify that orchestrator credentials are accepted for the orchestrator by checking the status indicator in the **Configure ESM credentials** dialog box.

A green Passed test status indicates that the credentials are accepted. If the orchestrator credentials are not accepted, confirm that the credentials are correct and enter them again in the **Configure ESM credentials** dialog box. You can also check the log file to verify that Orchestrator credentials are accepted in the log file.

Click **Close**.

**Configuring Orchestrator credentials through clientConnect.conf file**

You need to specify the Orchestrator credentials in the clientConnect.conf file located in the Server Manager installation directory.

You can also configure the Orchestrator credentials through GUI, as mentioned in **Configure Orchestrator credentials through GUI**.

To specify credentials:

**Procedure**

1. At BASEDIR/smarts/bin, type the following command:
   
   ```
   ./sm_edit conf/clientConnect.conf
   ```

2. Enter the following line for each orchestrator instance:
   
   ```
   orchestrator:<orchestrator_IP_Address>:<orchestrator_Username>:<orchestrator_Password>:<Protocol>:<orchestrator_Port>
   ```
   
   You must add the line for orchestrator instance above the line for the Smarts admin user.
3. *:*::admin in the clientConnect.conf file.

For example:
orchestrator:10.106.14.29:username@VeloCloud.net:password:https:443

3. Save and close the file.

**Configuring TCO Edge Kafka/Kafka Cluster and TCO details**

You need to specify the TCO Edge Kafka Cluster and TCO credentials in the clientConnect.conf file and associate the Orchestrator, TCO Edge Kafka Cluster and TCO details in esm-param.conf file located in the Server Manager installation directory.

TCO Collector Manager APIs will be accessed using the details provided as part of TCO details.

To specify credentials:

**Procedure**

1. At BASEDIR/smarts/bin , type the following command:
   
   ./sm_edit conf/clientConnect.conf

2. Enter the following line for TCO Edge Kafka Cluster and TCO details:

   kafka:
   <kafka_IP_Address>:<kafka_Username>:<kafka_Password>:<port>:<Discovery_Topic>:<Monitoring_Topic>

   dcc: < tco_master_node_IP_Address>:
   <tco_Username>:<tco_Password>:<Protocol>:<Port>

   You must add the line for kafka and dcc instances above the line for smarts admin user

   "*:*:admin:<E-1.0>94689C5A7C826F05D8DE9F62284A68191EC739743EA25E5E1F76FE493337D558" in the clientConnect.conf file.

   For example:


   **Note** In case of TCO Edge Kafka Cluster add the details of any one Kafka broker (generally the IP of the Domain Managers node of TCO Deployment).

   **Note** server.conf file for the kafka installation has a property named “auto.create.topics.enable”. If this property is set then the discovery and monitoring topics are automatically created. If not, these topics need to be created manually.

3. Save and close the file.

4. At BASEDIR/smarts/bin , type the following command:
   
   ./sm_edit conf/esm/esm-param.conf
Enter the following line for Orchestrator, TCO Edge Kafka Cluster and TCO:

# For providing single broker instance use below format.
KAFKA-<Orchestrator_host_IP_address> <Kafka_broker_ip_address:port>

# For providing multiple broker instances of a kafka cluster use below format.
KAFKA-<Orchestrator_host_IP_address>
<Kafka_broker1_ip_address>:<port1>,<Kafka_broker2_ip_address>:<port2>,
......,<Kafka_broker[n]_ip_address>:<port[n]>

# For providing IP Address of TCO instance (Master Node) use below format
DCC- <orchestrator_IP_Address> tco_master_node_IP_Address

# For providing orchestrator instance use below format
ORCHESTRATOR- <orchestrator_IP_Address> VELOCLOUD

For Example:
KAFKA-xx.xx.xx.xx zz.zz.zz.zz:9092,zz.zz.zz.zz:9093, zz.zz.zz.zz:9094
DCC- xx.xx.xx.xx yy.yy.yy.yy

# For providing usertype when Orchestrator is VELOCLOUD use the below format
VCO_USERTYPE-xx.xx.xx.xx operator|enterprise|MSP
VCO_USERTYPE-xx.xx.xx.xx operator

Restart the Server Manager.

Configure ESM to send VCO Link Performance and Topology Data to MnR

The VeloCloud DCF collector collects and sends the topology and status monitoring information to Smart Assurance by default. User can configure the collector to collect and send topology and link performance data to MnR. User can use this data from MnR and can develop the report pack around this data.

Steps to configure ESM, so that it can provide VCO link performance and topology data to MnR:

Procedure

1. At BASEDIR/smarts/bin/ enter the command:
   
   .:/sm_edit conf/esm/esm-param.conf

2. For each orchestrator instance, enter the following line to send the data to MnR:
   
   VCO_PERFMETRIC_CONNECTOR-<orchestrator IP> <MnR Host>:<MnR backend port>

   For example,
   
   VCO_PERFMETRIC_CONNECTOR-10.102.124.111 10.102.122.111 10.102.122.113:2000

3. Save and close the conf file.
4 Restart the server to accomplish this configuration.

Alternatively, during the configuration of orchestrator, this configuration can be applied.

Refer "DCF and M&R Integration" for more details and the procedure for updating the collector without restarting ESM server.

**Edge Link Performance Statistics**

In VeloCloud SD-WAN feature the edge link performance statistics are reported by REST endpoint `monitoring/getAggregateEdgeLinkMetrics`, and the statistics reports for the edge links are available in MnR.

The performance statistics reported by REST endpoint `monitoring/getAggregateEdgeLinkMetrics` are:

- p1BytesRx
- p1BytesTx
- p1PacketsRx
- p1PacketsTx
- p2BytesRx
- p2BytesTx
- p2PacketsRx
- p2PacketsTx
- p3BytesRx
- p3BytesTx
- p3PacketsRx
- p3PacketsTx
- scoreRx
- scoreTx
- signalStrength
- bestJitterMsRx
- bestJitterMsTx
- bestLatencyMsRx
- bestLatencyMsTx
- bestLossPctRx
- bestLossPctTx
- bpsOfBestPathRx
- bpsOfBestPathTx
MPLS Edge and Core Network stitching

For some of the RCA scenarios to work, it is required that the Server Manager discovers the MPLS topology and relates the MPLS topology to VeloCloud overlay Tunnels and Edge. Smarts IP Manager and Smart MPLS Manager have capability to discover the MPLS physical and logical entities. Server Manager leverages this capability and import MPLS topology from IP and MPLS server.

Creating VEdge and MPLS PE router connection

A pre-requisite for creating this connection is that the IP server should discover the PE Routers and should also have MPLS discovery enabled. To enable MPLS discovery set DisableMPLSDiscovery to false in tpmgr-param.conf. In the Server Manager enable the parameter EnableMPLSTopologyImport in esm-param.conf file.

If the VeloCloud orchestrator REST API reports the PE Router IP Address as the MPLS gateway IP for an Edge then Server Manager with the imported topology from Smarts IP Manager be able form the Network Connection between Edge and the PE Router Interface. The VeloCloud orchestrator reports the PE Router IP address as the MPLS gateway IP if the Edge is directly connected to PE. If the edge connects to a CE which in turn connect to the MPLS PE router then the orchestrator REST API used for discovery may not report the MPLS PE IP address. In this case the user defined connection conf which is used to created Edge to Edge tunnel is also used to create the Edge to PE connection.

Creating VEdge to VEdge Tunnel and related MPLS core network

A tunnel between two VEdge instances can run through an MPLS core network. Smarts MPLS Manager has capability to discovery core MPLS physical/logical entities in the MPLS network. The Server manager can be configured to import this topology into Server Manager and create a VEdge to VEdge tunnel using a user defined configuration.

To configure a Smarts MPLS Manager for Server Manager run sm_edit conf/sdwan/esm-mpls.conf and specify the MPLS topology server details.

Note Type value must be MPLS, only one MPLS topology server can be configured for topology import.
To define user defined connection run `sm_edit conf/sdwan/user-defined-connection.conf`. The format of the file and an example is given below:

```
# Tunnel-A      Tunnel-Z       Tunnel-A-end    Tunnel-Z-end
#  -end-IP      -end-IP           -PE-IP       -PE-IP
#
# 10.166.12.1   10.166.13.1    10.166.12.2     10.166.13.2
```

For each of the Edge to Edge tunnel that goes over the MPLS network feed in the four IP address given above. Tunnel-A-end-IP is the IP address on the VEdge instance that connects to the PE Router. Tunnel-Z-end-IP is the other end where the Tunnel terminates. The Tunnel-A-End-PE-IP and Tunnel-Z-end-PE-IP are the A and Z End PE Router IP addresses. These IP addresses are the ones where the VRF are configured.

With the `esm-mpls.conf` and `user-defined-connection.conf` properly configured a Tunnel instance between two VEdge instances will be created. The Tunnel will have a LayeredOverIFs relationship through which all the MPLS core network Interfaces that are used to carry this Tunnel traffic are associated. Also, two NetworkConnection instances, for A and Z end, are created between the edge and PE Router. Whenever any of the MPLS LayeredOverIFs goes down or the device itself goes down an impact will be shown to the Velocloud Tunnel.

**10.1 upgrade procedure**

This section illustrates the 10.1 upgrade procedure.

**Prerequisites**

If VCO is already existing in the topology, run the following command to find all the VeloCloud instances:

```
<BASEDIR>/smarts/bin/dmctl -s <ESM-DOMAIN-NAME> invoke ICF_PersistentDataSet::VCOTopologyCollectorInstanceIds get
```

**Procedure**

1. Stop ESM server.
   
   Refer [VMware Smart Assurance Server Manager User and Configuration Guide](#).

2. Upgrade to DCF 10.1.x.
   
   Refer [Performing Upgrade](#) for more details.

3. If VeloCloud collector instances are already existing in DCF, recreate Kafka topics.
   
   To recreate Kafka topics:
   
   a. Ensure `/config/server.properties` file has `delete.topic.enable=true`
b Execute the following commands, and wait for one minute:

```
export KAFKA_OPTS="-Djava.security.auth.login.config=<KAFKA_HOME>/config/zookeeper_jaas.conf"
<KAFKA_HOME>/bin/kafka-topics.sh --zookeeper <KAFKA_CLUSTER_HOST1_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST2_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST3_IPADDRESS>:2181 --delete --topic <discovery topic name>
```

c Run the following command, and wait for one minute:

```
<KAFKA_HOME>/bin/kafka-topics.sh --zookeeper <KAFKA_CLUSTER_HOST1_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST2_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST3_IPADDRESS>:2181 --delete --topic <monitoring topic name>
```

d Execute the following command to ensure the successful deletion of the topics mentioned in steps b and d. The command does not list any topic if the deletion is successful.

```
<KAFKA_HOME>/bin/kafka-topics.sh --zookeeper <KAFKA_CLUSTER_HOST1_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST2_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST3_IPADDRESS>:2181 --list
```

e Execute the command:

```
export KAFKA_OPTS="-Djava.security.auth.login.config=<KAFKA_HOME>/config/kafka_server_jaas.conf"
```

f Run the command, and wait for 30 seconds:

```
<KAFKA_HOME>/bin/kafka-topics.sh --create --zookeeper <KAFKA_CLUSTER_HOST1_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST2_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST3_IPADDRESS>:2181 --replication-factor 3 --partitions 1 --topic <Discovery Topic Name>
```

- The value for --replication-factor must be equal to number of nodes in the cluster.
- At present, only 1 partition is supported per topic.

g Execute the command, and wait for 30 seconds:

```
<KAFKA_HOME>/bin/kafka-topics.sh --create --zookeeper <KAFKA_CLUSTER_HOST1_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST2_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST3_IPADDRESS>:2181 --replication-factor 3 --partitions 1 --topic <Monitoring Topic Name>
```

- The value for --replication-factor should be equal to number of nodes in the cluster.
- At present, only 1 partition is supported per topic.

4 Upgrade to ESM 10.1.x.

Refer VMware Smart Assurance Installation Guide for SAM, IP, ESM, MPLS, NPM, OTM, ACM, MCAST and VoIP Managers for upgrade details.
5 Start ESM.

6 Delete old collectors and run the following command for each of the collector ids reported in the `dmctl` command:

```bash
dmctl -s <ESM-DOMAIN-NAME> invoke ICF_PersistentDataSet::VCOTopologyCollectorInstanceIds get
curl -k --user <dcf-user>:<dcf-password> --request POST --url https://<dcf-host>:8443/dcc/v1/
runtime/blocks/<collector-id>/service/stop
curl -k --user <dcf-user>:<dcf-password> --request DELETE --url https://<dcf-host>:8443/dcc/v1/
catalog/blocks/<collector-id>
```

**Note**: Replace the `dcf-user`, `dcf-password`, `dcf-host`, `collector-id` (collect ids returned in the `dmctl` output) with proper value.

7 Go to following section, and perform the configuration:

```
#unique_21
#unique_20
#unique_34
```

8 In the **Domain Manager Administration Console**, select your ESM server, and select **Topology > Discover All**.

**Install and Configure Smarts Console for Discovery/Monitoring**

Refer, **Polling and Thresholds** for configuring polling and thresholds.

For Velocloud the polling group is called "**Orchestrator Polling Groups**". There is only one setting object called "**VCO Polling**". Currently only AnalysisMode and PollingInterval parameters are supported. The retries and timeout, though enabled, are not used.
Polling and Thresholds

You can configure polling interval defaults by using the Polling and Thresholds console of the Domain Manager Administrator Console.

Through the default polling groups for the Server Manager you control the polling of the VeloCloud orchestrator. The polled data serves as input to the Server Manager root-cause and impact analysis.

Default Polling Groups

Default polling group for the Server Manager for VeloCloud table lists the default polling group and the setting.

Table 1-3. Default polling group for the Server Manager for VeloCloud

<table>
<thead>
<tr>
<th>Polling Group</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Orchestrator Polling Groups</td>
<td>VCO Setting</td>
</tr>
</tbody>
</table>

Default Polling Settings

Default values for the VCO Settings table lists the VeloCloud relevant polling parameters.

Table 1-4. Default values for the VCO Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnalysisMode</td>
<td>ENABLED, DISABLED Default: ENABLED</td>
<td>Enables or Disables Polling.</td>
</tr>
<tr>
<td>PollingInterval</td>
<td>30 to 3600 seconds Default 1200</td>
<td>Time between successive polls.</td>
</tr>
</tbody>
</table>

Troubleshooting Steps

Some of the common troubleshooting steps are described here, which user must follow if discovery or monitoring is not working as expected.

Troubleshooting Methodologies -1

DCF Collector (Discovery & Monitoring)

- Getting Collector Id for a VCO:
  - Run “dmctl -s <server name> invoke ICF_PersistentDataSet::VCOTopologyCollectorInstanceIds get”
  - Returns two blocks for each VCO. Each block has a collector Id and a tag to indicate if it is discovery/monitoring collector.

- Logs and log locations:
  - Collector logs are located at /opt/DCF/Collecting/Collector-Manager/<collector Id>/logs/
Logging and troubleshooting:

- Edit /opt/DCF/Collecting/Collector-Manager/<collector Id>/conf/logging.properties to increase log level
- Change the default INFO level to one of – CONFIG, FINE, FINER & FINEST (lowest value)
- The new log level takes effect in the next discovery
- The kafka messages can also be configured to be written to file:
  - Edit /opt/DCF/Collecting/Collector-Manager/<collector Id>/conf/collecting.xml. Change enabled=true for file collector
    - <connector enabled="true" name="File" type="File-Connector" config="Collector-Manager/<collector Id>/conf/file-connector.xml" />

Troubleshooting Methodologies - 2

- Check if the /opt/DCF/Collecting/Stream-Collector/<Collector Id>/velo/conf/requests/context-vco.xml has proper values (username, password, port & protocol) for VeloCloud access.
- For specific discovery/monitoring issues use REST API to get the data directly from VCO to confirm VCO is returning proper value. The base URI for the REST API is https://<VCO IP>/portal/rest/

DCF Collector (Discovery & Monitoring)

Table 1-5. REST API used for Discovery and monitoring for different user types

<table>
<thead>
<tr>
<th>Topology/Status</th>
<th>REST API</th>
<th>Operator</th>
<th>MSP</th>
<th>Enterprise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login</td>
<td>/login/operatorLogin</td>
<td>Yes</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Login</td>
<td>/login/enterpriseLogin</td>
<td>Not Used</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Discovery</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Enterprises</td>
<td>/network/getNetworkEnterprises</td>
<td>Yes</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Enterprises</td>
<td>enterpriseProxy/getEnterpriseProxyEnterprises</td>
<td>NA</td>
<td>Yes</td>
<td>NA</td>
</tr>
<tr>
<td>Enterprises</td>
<td>enterprise/getEnterprise</td>
<td>Not used</td>
<td>Not used</td>
<td>Yes</td>
</tr>
<tr>
<td>Edge</td>
<td>/network/getNetworkEnterprises ( &quot;with&quot; : [&quot;edges&quot;])</td>
<td>Yes</td>
<td>NA</td>
<td>NA</td>
</tr>
<tr>
<td>Edge</td>
<td>/enterprise/getEnterpriseEdges</td>
<td>Not used</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Edge interfaces (WAN and LAN)</td>
<td>/edge/getEdgeConfigurationStack</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Edge links</td>
<td>/enterprise/getEnterpriseEdges</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Gateway</td>
<td>/network/getNetworkGatewayPools</td>
<td>Yes</td>
<td>Yes</td>
<td>NA</td>
</tr>
</tbody>
</table>
Table 1-5. REST API used for Discovery and monitoring for different user types (continued)

<table>
<thead>
<tr>
<th>Topology/Status</th>
<th>REST API</th>
<th>User Type</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td>GatewayPool</td>
<td>/network/getNetworkGatewayPools</td>
<td>Yes</td>
</tr>
<tr>
<td>Non VeloCloud Site and the Tunnels</td>
<td>/enterprise/getEnterpriseDataCenters</td>
<td>Yes</td>
</tr>
<tr>
<td>Edge and Gateway relationship</td>
<td>/network/getNetworkGatewayPools (connectedEdgeList field in the response)</td>
<td>Yes</td>
</tr>
<tr>
<td>Edge and Gateway relationship</td>
<td>gateway/getGatewayEdgeAssignments</td>
<td>Not used</td>
</tr>
<tr>
<td>Edge and Gateway relationship</td>
<td>/edge/getEdgeConfigurationStack</td>
<td>Not used</td>
</tr>
<tr>
<td>Edge Clusters</td>
<td>/edge/getEdgeConfigurationStack /enterprise/getEnterpriseEdgeServices /enterprise/getEnterpriseServices</td>
<td>Yes</td>
</tr>
<tr>
<td>Edge Hub and Spoke Relationship</td>
<td>/edge/getEdgeConfigurationStack /enterprise/getEnterpriseEdgeServices /enterprise/getEnterpriseServices</td>
<td>Yes</td>
</tr>
<tr>
<td>Monitoring</td>
<td></td>
<td>Operator</td>
</tr>
<tr>
<td>Edge Status</td>
<td>enterprise/getEnterpriseEdges</td>
<td>Yes</td>
</tr>
<tr>
<td>Edge link Status</td>
<td>enterprise/getEnterpriseEdges</td>
<td>Yes</td>
</tr>
<tr>
<td>Edge link Performance data</td>
<td>monitoring/getAggregateEdgeLinkMetrics</td>
<td>Yes</td>
</tr>
<tr>
<td>Gateway Status</td>
<td>network/getNetworkGatewayPools</td>
<td>Yes</td>
</tr>
<tr>
<td>Non VC site Tunnel Status</td>
<td>enterprise/getEnterpriseDataCenters</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Troubleshooting Methodologies -3

Smarts

- Logs and log locations:
  - Server logs are located at $INSTALL_DIR/smarts/local/logs
- Logging and troubleshooting:
  - Enable Discovery logging:
    - Run dmctl –s <server> put ESM_Manager::ESM-Manager::EnableVeloCloudDiscoveryDebug TRUE
    - Run dmctl –s <server> put ESM_Manager::ESM-Manager::IsDebug TRUE
    - Run dmctl –s <server> put ESM_Manager::ESM-Manager::LogLevel DEBUG

  **Note** This logs all the Kafka messages for all VCO.
Enable Monitoring Logging:

- Run `dmctl -s <server> put ESM_Manager::ESM-Manager::EnableVeloCloudMonitoringDebug TRUE`
- Run `dmctl -s <server> put ESM_Manager::ESM-Manager::LogLevel DEBUG`

**Note** This logs all the Kafka messages for all VCO.

Make sure VeloCloud feature is enabled (default enabled):

- Run `dmctl -s <server> get ESM_Manager::ESM-Manager::IsVC`

Smarts notifies DiscoveryFailure & MonitoringFailure event for the Orchestrator with the reason for failure set in the event details.

Log analysis:

- Discovery Kafka message:

  Sample:

  ```json
  {"groupName":"group","discoveryID":null,"jobID":"9999","type":"Tenant","timestamp":1554472776,"value":0.0,"action":"r","properties":
  {"Tenant-Orchestrator":"10.106.124.199","Tenant-name":"testTenant_1","source":"velocloud-sdwan4defedc886-41ac-a83f-9676c9014c4","type":"Tenant","Tenant-Id":"1","EnterpriseLogicalId":"c8cc3bc7-df6e-407c-ac30-352b4b3d93a"},"metrics":{"VCO-Req":{"properties":
  {"unit":"code","name":"VCO-Req"},"value":8080.0}},"relations":
  []},"initialized":true,"forceRefresh":true,"name":"testTenant_1"}

  Creates Tenant::testTenant_1
  Creates Orchestrator::VCO-a.b.c.d
  Establish relationship Tenant::testTenant_1 SupervisedBy Orchestrator::VCO-a.b.c.d

- Monitoring Kafka message:

  Sample:

  ```json
  {"groupName":"group","discoveryID":null,"jobID":"9999","type":"VGateway","timestamp":1554753805,"value":0.0,"action":"\\u0000","properties":
  {"instanceName":"GatewayName","attributes":"Status,IsActivated","source":"velocloud-sdwan048048cb-701e-440d-85e9-e46110965181","GatewayName":"VGateway-OneCloud-GW1-Bangalore","type":"VGateway","attributevalues":"OK,TRUE"},"metrics":{"VCO-Req":
  {"properties":{"unit":"code","name":"VCO-Req"},"value":0.0}},"relations":
  []},"initialized":true,"forceRefresh":false,"name":"VGateway-OneCloud-GW1-Bangalore"}

  VGateway::Vgateway-OneCloud-GW1-Bangalore is the instance name
  Status is OK
  IsActivated is TRUE

1 DCF Health Check

   a How does user know the Orchestrator not accepting ICMP pings?

   b Have the VeloCloud collectors deployed and Enabled?
c  Is the DCF connection to KAFKA alive?
d  Can DCF communicate to the Orchestrator?
e  Can UI communicate to DCF and Orchestrator?
f  Is DCF collecting data from the data source?
g  What is the last time SMARTS Discovery and monitoring has happened?
h  When is the last time DCF collected data from the data source?
i  When is the last time DCF has published data to KAFKA?

Logs contain all operational data. Specific Collector logs can be checked for all the
details <DCF_Install>/Collecting/Collector-Manager/<Collector-ID>/logs/collecting-0-0.log

2  KAFKA Health Check
   a  KAFKA Topics created
   b  KAFKA Messages not published from DCF, KPI engine
   c  KAFKA authentication issues
   d  KAFKA not reachable

Logs contain all operational data. Specific Collector logs can be checked for all the
details <DCF_Install>/Collecting/Collector-Manager/<Collector-ID>/logs/collecting-0-0.log

3  Smarts Domain Managers
   a  Getting Collector Id for a VCO:
       Run "dmctl -s <server name> invoke
       ICF_PersistentDataSet::VCOTopologyCollectorInstanceIds get"
       Returns two blocks for each VCO. Each block has a collector Id and a tag to indicate if it is
discovery/monitoring collector
       <connector enabled="true" name="File" type="File-Connector" config="Collector-
Manager/<collector Id>/conf/file-connector.xml" />
   b  DCF Logs and log locations:
       Collector logs are located at /opt/DCF/Collecting/Collector-Manager/<collector Id>/logs/
   c  DCF Logging and troubleshooting:
       Edit /opt/DCF/Collecting/Collector-Manager/<collector Id>/conf/logging.properties to
       increase log level
       Change the default INFO level to one of - CONFIG, FINE, FINER & FINEST (lowest value)
       The new log level takes effect in the next discovery.
   d  The kafka messages can also be configured to be written to file.
       Edit /opt/DCF/Collecting/Collector-Manager/<collector Id>/conf/collecting.xml.
Change enabled=true for file collector.

e Check if the /opt/DCF/Collecting/Stream-Collector/<Collector Id>/velo/conf/requests/context-vco.xml has proper values (username, password, port & protocol) for VeloCloud access.

f For specific discovery/monitoring issues use REST API to get the data directly from VCO to confirm VCO is returning proper value. The base URI for the REST API is https://<VCO IP>/portal/rest/. A REST client (e.g Postman, Insomnia & SoapUI) can be used to issue these REST queries.

Note The various VCO REST APIs used for discovery and monitoring for different user types are documented at the table REST API used for Discovery and monitoring for different user types.

g Smarts Logging:

1. Server logs are located at $INSTALL_DIR/smarts/local/logs
   a. Enable Discovery logging:
      1. Run `dmctl -s <server> put ESM_Manager::ESM-Manager::EnableVeloCloudDiscoveryDebug TRUE`
      2. Run `dmctl -s <server> put ESM_Manager::ESM-Manager::IsDebug TRUE`
      3. Run `dmctl -s <server> put ESM_Manager::ESM-Manager::LogLevel DEBUG`
   b. Enable Monitoring Logging:
      1. Run `dmctl -s <server> put ESM_Manager::ESM-Manager::EnableVeloCloudMonitoringDebug TRUE`
      2. Run `dmctl -s <server> put ESM_Manager::ESM-Manager::LogLevel DEBUG`

Note This logs all the Kafka messages for all VCO.

h Smarts Log analysis.

1. Discovery Kafka message:
   - Sample:
     ```json
     {"groupName":"group","discoveryID":null,"jobID":"9999","type":"Tenant","timestamp":1554472776,"value":0.0,"action":"r","properties":
      {"VelocloudOrchestrator":"10.106.124.199","Tenant-name":"testTenant_1","source":"velocloud-sdwan4ddefd0c-c8b6-41ac-a83f-96776c9001c4","type":"Tenant","Tenant-Id":"1","EnterpriseLogicalId":"c8cc3bc7-df6e-407c-ac30-352b4b3de93a"},"metrics":{"VCO-Req":{"properties":
       {"unit":"code","name":"VCO-Req"},"value":8080.0}},"relations":
       [{"type":"Orchestrator","element":"VCO-a.b.c.d","relationName":"SupervisedBy"}],"initialized":true,"forceRefresh":true,"name":"
       testTenant_1"}
     ```
Creates Tenant::testTenant_1
Creates Orchestrator::VCO-a.b.c.d
Establish relationship Tenant::testTenant_1 SupervisedBy Orchestrator::VCO-a.b.c.d

Monitoring Kafka message:
-Sample:
{"groupName":"group","discoveryID":null,"jobID":"9999","type":"VGateway","timestamp":1554753805,"value":0.0,"action":"\u0000","properties":
{"instanceName":"GatewayName","attributes":"Status,IsActivated","source":"velocloud-sdwan048048cb-701e-440d-85e9-e46110965181","GatewayName":"VGateway-OneCloud-GW1-Bangalore","type":"VGateway","attributevalues":"OK,TRUE"},"metrics":
{"VCO-Req":{"properties":{"unit":"code","name":"VCO-Req"},"value":0.0}},"relations":
[],"initialized":true,"forceRefresh":false,"name":"VGateway-OneCloud-GW1-Bangalore"}

VGateway::Vgateway-OneCloud-GW1-Bangalore is the instance name
Status is OK
IsActivated is TRUE

Feature is enabled (default enabled)

Run dmctl -s <server> get ESM_Manager::ESM-Manager::IsVC

Smarts ESM server raises a DiscoveryFailure/MonitoringFailure event on the Orchestrator instance when there is an internal error or communication failure between the components. The event has the reason for the failure set in the event details.

Virtual IMS Assurance

This section provides end to end installation and configuration of vIMS (Virtual IP Multimedia Subsystem).
vIMS (Clearwater) and Cloudify Architecture/Eco System

Overview

vIMS provides scalable deployment of IP Multimedia Subsystem (IMS) in virtualized and cloud environments for voice, video and messaging services.

IMS provides real-time multimedia sessions (voice session, video session, conference session, etc) and non-real-time multimedia sessions (Push to talk, Presence, instant messaging) over an all-IP network.

IMS converges services supplied by different types of networks: fixed, mobile, and internet. It allows the creation and deployment of IP-based multimedia services in the 5G networks.

The Server Manager provides vIMS management support for the following:

- vIMS components discovery using the Orchestrator (Cloudify) REST API
- Association of vIMS components (VNFs) with the virtual Infrastructure
- Root-cause and impact analysis.

Discovery Flow

The Server Manager discover various vIMS components using REST API interface of Cloudify Orchestrator.

The discovered vIMS components are:

- CallSessionControlFunction (P-CSCF & I/S-CSCF)
- HSSMirrorFunction (HSS/CDF)
- XMLDocumentManagementServer (XDMS)
Monitor vIMS Cloudify Orchestrator 4.5 is supported in Smart Assurance.

The monitored vIMS components are:

- CallSessionControlFunction (P-CSCF & I/S-CSCF)
- HSSMirrorFunction (HSS/CDF)
- XMLDocumentManagementServer (XDMS)
- VIMSApplicationService
- CallSessionControlFunctionsGroup
- HSSMirrorFunctionGroup
- XMLDocumentManagementServersGroup
- VIMSApplicationService Group
- Tenant
- IPMultimediaSubSystem (IMS)
- VNFManger
- Orchestrator

**Topology**

The Server Manager builds a topology of the deployed vIMS components. The topology objects represent the vIMS deployed VNFs, their relationships, and their association with tenants and virtual infrastructure.

**CallSessionControlFunction**

The Call Session Control Function (CSCF) in IMS comprises three distinct roles: the Proxy CSCF (P-CSCF), the Interrogating CSCF (I-CSCF), and the Serving CSCF (S-CSCF). The CSCF is implemented through servers using the SIP protocol to communicate with each other and application servers.

CallSessionControlFunction has the following relationships:

- **AvailedBy** with Tenant
- **PartOf** with CallSessionControlFunctionsGroup
- **vHostedBy** with VirtualMachine

**Table 1-6. Attributes for the CallSessionControlFunction objects**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>deploymentId</td>
<td>Indicates the deployment ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>hostId</td>
<td>Indicates the host ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>IPAddress</td>
<td>Indicates the host or VM IP address where application service is running.</td>
<td>String</td>
</tr>
<tr>
<td>networkID</td>
<td>Indicates network ID of the application service.</td>
<td>String</td>
</tr>
</tbody>
</table>
Table 1-6. Attributes for the CallSessionControlFunction objects (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>nodeId</td>
<td>Indicates node ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates type of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>Role</td>
<td>Indicates the role of CSCF.</td>
<td>String</td>
</tr>
</tbody>
</table>

**HSSMirrorFunction**

A primary user database that supports IMS network entities that actually handle calls.

HSSMirrorFunction has the following relationships:

- *AvailedBy* with Tenant
- *PartOf* with HSSMirrorFunctionGroup
- *vHostedBy* with VirtualMachine

**Table 1-7. Attributes for the HSSMirrorFunction objects**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>deploymentId</td>
<td>Indicates the deployment ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>hostId</td>
<td>Indicates the host ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>IPAddress</td>
<td>Indicates the host or VM IP address where application service is running.</td>
<td>String</td>
</tr>
<tr>
<td>networkID</td>
<td>Indicates network ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>nodeId</td>
<td>Indicates node ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates type of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>Role</td>
<td>Indicates the role of CSCF.</td>
<td>String</td>
</tr>
</tbody>
</table>

**XMLDocumentManagementServer**

Allows operators to maintain their subscriber's profile information in a central, secure and easy to access repository.

XMLDocumentManagementServer has the following relationships:

- *AvailedBy* with Tenant
- *PartOf* with XMLDocumentManagementServersGroup
- *vHostedBy* with VirtualMachine
### Table 1-8. Attributes for the XMLDocumentManagementServer objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>deploymentId</td>
<td>Indicates the deployment ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>hostId</td>
<td>Indicates the host ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>IPAddress</td>
<td>Indicates the host or VM IP address where application service is running.</td>
<td>String</td>
</tr>
<tr>
<td>networkID</td>
<td>Indicates network ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>nodeID</td>
<td>Indicates node ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates type of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>Role</td>
<td>Indicates the role of CSCF.</td>
<td>String</td>
</tr>
</tbody>
</table>

**VIMSApplicationService**

Represents vIMS application.

VIMSApplicationService has the following relationships:

- *AvailedBy* with Tenant
- *PartOf* with IPMultiMediaSubSystem
- *vHostedBy* with VirtualMachine

### Table 1-9. Attributes for the VIMSApplicationService objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>deploymentId</td>
<td>Indicates the deployment ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>hostId</td>
<td>Indicates the host ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>IPAddress</td>
<td>Indicates the host or VM IP address where application service is running.</td>
<td>String</td>
</tr>
<tr>
<td>networkID</td>
<td>Indicates network ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>nodeID</td>
<td>Indicates node ID of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates type of the application service.</td>
<td>String</td>
</tr>
<tr>
<td>Role</td>
<td>Indicates the role of CSCF.</td>
<td>String</td>
</tr>
</tbody>
</table>
CallSessionControlFunctionsGroup

CallSessionControlFunctionsGroup is a group of CallSessionControlFunction collectively provides redundancy.

CallSessionControlFunctionsGroup has the following relationships:

- **CollaboratedBy** with CallSessionControlFunctionsGroup
- **CollaborateWith** with HSSMirrorFunctionGroup
- **ComposedOf** with CallSessionControlFunction
- **PartOf** with IPMultiMediaSubSystem

<table>
<thead>
<tr>
<th>Table 1-10. Attributes for the CallSessionControlFunctionsGroup objects</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attribute</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>NumberOfComponents</td>
</tr>
</tbody>
</table>

HSSMirrorFunctionGroup

HSSMirrorFunctionGroup is a group of HSSMirrorFunction collectively provides redundancy.

HSSMirrorFunctionGroup has the following relationships:

- **CollaboratedBy** with CallSessionControlFunctionsGroup and VIMSApplicationServiceGroup
- **ComposedOf** with HSSMirrorFunction
- **PartOf** with IPMultiMediaSubSystem

<table>
<thead>
<tr>
<th>Table 1-11. Attributes for the HSSMirrorFunctionGroup objects</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Attribute</strong></td>
</tr>
<tr>
<td>Name</td>
</tr>
<tr>
<td>NumberOfComponents</td>
</tr>
</tbody>
</table>

XMLDocumentManagementServersGroup

XMLDocumentManagementServersGroup is a group of XMLDocumentManagementServer collectively provides redundancy.

XMLDocumentManagementServersGroup has the following relationships:

- **CollaboratedBy** with CallSessionControlFunctionsGroup and VIMSApplicationServiceGroup
- **ComposedOf** with XMLDocumentManagementServer
- **PartOf** with IPMultiMediaSubSystem
Table 1-12. Attributes for the XMLDocumentManagementServersGroup objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Indicates name of the object.</td>
<td>String</td>
</tr>
<tr>
<td>NumberOfComponents</td>
<td>Indicates total number of components in this group.</td>
<td>int</td>
</tr>
</tbody>
</table>

VIMSApplicationServiceGroup

Group of VIMSApplicationServiceGroup Processes that together provide a service.

VIMSApplicationServiceGroup has the following relationships:

- **CollaboratedBy** with CallSessionControlFunctionsGroup
- **CollaborateWith** with HSSMirrorFunctionGroup and XMLDocumentManagementServersGroup
- **ComposedOf** with VIMSApplicationService
- **PartOf** with IPMultiMediaSubSystem

Table 1-13. Attributes for the VIMSApplicationServiceGroup objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Indicates name of the object.</td>
<td>String</td>
</tr>
<tr>
<td>NumberOfComponents</td>
<td>Indicates total number of components in this group.</td>
<td>int</td>
</tr>
</tbody>
</table>

IPMultiMediaSubSystem

It is a framework for delivering IP multimedia service.

IPMultiMediaSubSystem has the following relationships:

- **ComposedOf** with CallSessionControlFunctionsGroup, HSSMirrorFunctionGroup, VIMSApplicationService, VIMSApplicationServiceGroup and XMLDocumentManagementServersGroup
- **LifecycleManagedBy** with VNFManager

Table 1-14. Attributes for the IPMultiMediaSubSystem objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Indicates name of the object.</td>
<td>String</td>
</tr>
</tbody>
</table>

VNFManager

VNF Manager provides the essential management and orchestration capabilities needed to deliver VNF-based network.

VNFManager has the following relationships:

- **ManagesLifecycleOf** with IPMultiMediaSubSystem
- **OrchestratedBy** with Orchestrator
Table 1-15. Attributes for the VNFManager objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Indicates name of the object.</td>
<td>String</td>
</tr>
</tbody>
</table>

Orchestrator

Orchestration is the automated configuration, coordination, and management of virtualized network components and software.

Orchestrator has the following relationships:

- *Orchestrates* with VNFManager
- *Supervises* with Tenant
- *HostedBy* with Host

Table 1-16. Attributes for the Orchestrator objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ManagementServiceAddress</td>
<td>Indicates management service access point of controller cluster used for accessing APIs.</td>
<td>String</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates type of the application service.</td>
<td>String</td>
</tr>
</tbody>
</table>

Tenant

User of cloud computing service, who shares resources and cost of underlying hardware resources like compute, storage and network with other users.

Tenant has the following relationships:

- *Avails* with CallSessionControlFunction, HSSMirrorFunction, VIMSApplicationService, and XMLDocumentManagementServer
- *SupervisedBy* with Orchestrator

Table 1-17. Attributes for the Tenant objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Indicates name of the object.</td>
<td>String</td>
</tr>
</tbody>
</table>

Root Cause and Impact Analysis

This section provides information on root cause and impact analysis for various events.
<table>
<thead>
<tr>
<th>Class</th>
<th>Root-Cause</th>
<th>Events (symptoms of root-cause)</th>
<th>Impacted system</th>
<th>Impacted system attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>VirtualMachine</td>
<td>Down</td>
<td>ServiceAffected</td>
<td>VIMSApplicationService</td>
<td>IsServiceAffected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VNFDown/ServiceAffected</td>
<td>CallSessionControlFunction</td>
<td>IsDown &amp; IsVMDown / IsServiceAffected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VNFDown/ServiceAffected</td>
<td>XMLDocumentManagementServer</td>
<td>IsDown &amp; IsVMDown / IsServiceAffected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VNFDown/ServiceAffected</td>
<td>HSSMirrorFunction</td>
<td>IsDown &amp; IsVMDown / IsServiceAffected</td>
</tr>
<tr>
<td>VirtualMachine</td>
<td>PoweredOff</td>
<td>ServiceAffected</td>
<td>VIMSApplicationService</td>
<td>IsServiceAffected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VNFDown/ServiceAffected</td>
<td>CallSessionControlFunction</td>
<td>IsDown &amp; IsVMDown / IsServiceAffected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VNFDown/ServiceAffected</td>
<td>XMLDocumentManagementServer</td>
<td>IsDown &amp; IsVMDown / IsServiceAffected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VNFDown/ServiceAffected</td>
<td>HSSMirrorFunction</td>
<td>IsDown &amp; IsVMDown / IsServiceAffected</td>
</tr>
<tr>
<td>Hypervisor</td>
<td>Down</td>
<td>ServiceAffected</td>
<td>VIMSApplicationService</td>
<td>IsServiceAffected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VNFDown/ServiceAffected</td>
<td>CallSessionControlFunction</td>
<td>IsDown &amp; IsVMDown / IsServiceAffected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VNFDown/ServiceAffected</td>
<td>XMLDocumentManagementServer</td>
<td>IsDown &amp; IsVMDown / IsServiceAffected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VNFDown/ServiceAffected</td>
<td>HSSMirrorFunction</td>
<td>IsDown &amp; IsVMDown / IsServiceAffected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReducedRedundancy/AllComponentsDown/AtRisk</td>
<td>VIMSApplicationServices Group</td>
<td>IsAllComponentsDown</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReducedRedundancy/AllComponentsDown/AtRisk</td>
<td>CallSessionControlFunctionGroup</td>
<td>IsAllComponentsDown</td>
</tr>
</tbody>
</table>

VMware, Inc.
<table>
<thead>
<tr>
<th>Class</th>
<th>Root-Cause</th>
<th>Events (symptoms of root-cause)</th>
<th>Impacted system</th>
<th>Impacted system attribute</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor Hosted by Host</td>
<td>Down</td>
<td>ServiceAffected</td>
<td>VIMSApplicationService</td>
<td>IsServiceAffected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VNFDown/ServiceAffected</td>
<td>CallSessionControlFunction</td>
<td>IsDown &amp; IsVMDown / IsServiceAffected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VNFDown/ServiceAffected</td>
<td>XMLDocumentManagementServerGroup</td>
<td>IsDown &amp; IsVMDown / IsServiceAffected</td>
</tr>
<tr>
<td></td>
<td></td>
<td>VNFDown/ServiceAffected</td>
<td>HSSMirrorFunction</td>
<td>IsDown &amp; IsVMDown / IsServiceAffected</td>
</tr>
<tr>
<td>ReducedRedundancy/AllComponentsDown/AtRisk</td>
<td>ReducedRedundancy/AllComponentsDown/AtRisk</td>
<td>XMLDocumentManagementServerGroup</td>
<td>IsAllComponentsDown/IsAnyComponentDown/IsEveryComponentDown</td>
<td></td>
</tr>
<tr>
<td>Class</td>
<td>Root-Cause</td>
<td>Events (symptoms of root-cause)</td>
<td>Impacted system</td>
<td>Impacted system attribute</td>
</tr>
<tr>
<td>-------</td>
<td>------------</td>
<td>---------------------------------</td>
<td>----------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReducedRedundancy/AllComponentsDown/AtRisk</td>
<td>HSSMirrorFunctionGroup</td>
<td>IsAllComponentsDown</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IsAnyComponentDown</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IsEveryComponentDown</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReducedRedundancy/AllComponentsDown/AtRisk</td>
<td>XMLDocumentManagementServerGroup</td>
<td>IsAllComponentsDown</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IsAnyComponentDown</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>IsEveryComponentDown</td>
</tr>
</tbody>
</table>

Host Down - Host Down impacting VNF Functions

![Notification Properties](image_url)
Hypervisor Down - Hypervisor Down impacting VNF Functions

VM Down - VM Down impacting VNF Functions
Install and Configure

This section provides information on installation and configuration of open source and VSA components for vIMS.

**Note** Perform the installation of the following VSA Components prior to further configurations.

**Messaging**
Refer, Installing Kafka

**SMARTS**
Refer, Domain Manager

**Data Management**
Refer, Installing Data Collection Framework
Refer, Data Collection Controller

**Notification UI**
Refer, UI Components

**VSA Configuration**
This section assists you with the information on custom configuration from Server Manager side.

**Configure Orchestrator credentials through GUI**
To configure Smarts Server Manager to communicate with Orchestartor, specify the Orchestartor administrator credentials and the IP address of the Orchestartor host.

**Prerequisites**
For this task, when you use the console, you need to have Smarts administrator credentials to open the Configure menu where you specify the Orchestartor credentials.

**Procedure**
1. Open the Service Assurance Manager Global Console attached to the Server Manager (INCHARGE-ESM, by default).
2. In the Topology Browser Console, select **Configure > Domain Manager Administration Console**.
3. Right-click the **ESM server** in the left pane and select **Configure ESM credentials**.
4. In the **Configure ESM credentials** dialog box, select **Orchestrator** for the host type.
5 Type values in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>IP address of the Orchestrator(Cloudify) host</td>
</tr>
<tr>
<td>User ID</td>
<td>Orchestrator(Cloudify) user name</td>
</tr>
<tr>
<td>Password</td>
<td>Orchestrator(Cloudify) password</td>
</tr>
<tr>
<td>Port</td>
<td>Orchestrator(Cloudify) port (Default value is 80)</td>
</tr>
</tbody>
</table>

6 Click **Apply credential with/without testing**.

7 Verify that orchestrator credentials are accepted for the orchestrator by checking the status indicator in the **Configure ESM credentials** dialog box.

   A green Passed test status indicates that the credentials are accepted for the orchestrator.

   If the orchestrator credentials are not accepted, confirm that the credentials are correct and enter them again in the Configure ESM credentials dialog box.

   You can also check the log file: `#unique_47`

8 Click **Close**.

9 In the **Domain Manager Administration Console**, select your IP Manager and select **Topology > Discover All to discover VIO and Orchestrator**. At the end of the IP Manager discovery process, the Server Manager discovery process is automatically started.

   **Note:** Configure Kafka/Kafka Cluster and DCF Controller details in clientConnect.conf and esm-param.conf, refer Configuring Edge Kafka/Edge Kafka Cluster and Telco Cloud Operator Data Collector.

   After the topology for your virtual network has been discovered, to continue to monitor and analyze your network, use the Service Assurance Global Console.

**Configuring Orchestrator credentials through clientConnect.conf file**

You need to specify the Orchestrator credentials in the clientConnect.conf file located in the Server Manager installation directory.

You can also configure the Orchestrator credentials through GUI, as mentioned in Configure Orchestrator credentials through GUI

**Procedure**

1 At BASEDIR/smarts/bin, type the following command:

   ```bash
   sm_edit ../conf/clientConnect.conf
   ```

2 Enter the following line for each orchestrator instance:

   ```bash
   ```

   You must add the line for orchestrator instance above:
" ::admin:<E-1.0>94689C5A7C826FD58DE9F62284A68191EC739743EA25E5E1F76FE493337D558 " in the clientConnect.conf file.


3 Save and close the file.

4 Restart the Server Manager.

Note: Configure Kafka/Kafka Cluster and DCF Controller details in clientConnect.conf and esm-param.conf. Refer Configuring Edge Kafka/Edge Kafka Cluster and Telco Cloud Operator Data Collector for more information.

Configuring Edge Kafka/Edge Kafka Cluster and Telco Cloud Operator Data Collector

You need to specify the Edge Kafka/Edge Kafka Cluster and Telco Cloud Operator Data Collector credentials in the clientConnect.conf file and specify the Orchestrator, Edge Kafka/ Edge Kafka Cluster and Telco Cloud Operator Data Collector details in esm-param.conf file located in the Server Manager installation directory.

To specify credentials:

Procedure

1 At BASEDIR/smarts/bin, type the following command:

   sm_edit ../conf/clientConnect.conf

2 Enter the following line for Kafka and DCC instance:

   kafka:<kafka_IP_Address>::<empty-string>::<empty-string>::<Port>::<Discovery_Topic>::<Monitoring_Topic>

   dcc:<TCOPs_Master_Node_IP_Address>::<Username>::<Password>::<Protocol>::<Port>

You must add the line for kafka and dcc instances above

   " ::admin:<E-1.0>94689C5A7C826FD58DE9F62284A68191EC739743EA25E5E1F76FE493337D558 " in the clientConnect.conf file.

For example:

   kafka:10.107.10.122:::9092:cloudify_disc:cloudify_mon
dcc:10.107.10.28:admin:<E-1.0>946F238CA85988759133A0E35B4600876574A26FE968414E1E3D295F7600BD:https:443

Note In case of Kafka Cluster add the details of any one Kafka broker.

Note Add the Kafka monitoring topic if user wants to collect the SNMP Performance metrics for vIMs VNF nodes.

3 Save and close the file.
4 At BASEDIR/smarts/bin, type the following command:
   sm_edit ../conf/esm/esm-param.conf

5 Enter the following line for Orchestrator, Kafka and DCF Controller:

   # For providing single broker instance use below format.
   KAFKA-<Orchestrator_host_IP_address> <Kafka_broker_ip_address:port>

   # For providing multiple broker instances of a kafka cluster use below format.
   KAFKA-<Orchestrator_host_IP_address>
   <Edge_Kafka_Broker_IP_Address>:<port1>,<Kafka_broker2_ip_address>:<port2>,
   ......,<Kafka_broker[n]_ip_address>:<port[n]>

   # For providing DCF Controller instance use below format
   DCC-<orchestrator_IP_Address> <TCOps Master Node IP_Address>

   # For providing orchestrator instance use below format
   ORCHESTRATOR-<orchestrator_IP_Address> CLOUDIFY

   For Example:
   KAFKA-xx.xx.xx.xx zz.zz.zz.zz:9092,zz.zz.zz.zz:9093, zz.zz.zz.zz:9094
   DCC- xx.xx.xx.xx yy.yy.yy.yy
   ORCHESTRATOR- xx.xx.xx.xx CLOUDIFY

6 Restart the Server Manager.

Configuring vIMS Clearwater details through clientConnect.conf file

You need to specify the vIMS (Clearwater) details in the clientConnect.conf file located in the Server Manager installation directory.

To specify details:

Procedure

1 At BASEDIR/smarts/bin, type the following command:
   sm_edit ../conf/clientConnect.conf

2 Enter the following line for each clearwater instance:
   snmp-vims:<vims_IP_Address>:<SNMP_Version>:<Community_String>:<SNMP_Port>

   You must add the line for vims instance above
   " ::admin:<E-1.0>94689C5A7C826FD58DDE9F62284A6A191EC739743EA25E5E1F76FE49 3337D558 "

   in the clientConnect.conf file.
For example:

```
```

3. **Save** and close the file.

4. Restart the Server Manager.

**Note**  This is required only if user wants to collect the SNMP Performance metrics for vIMS VNF nodes.

How to Update the Orchestrator Credentials for the Server Manager Configuration

If the Orchestrator administrator changed the administrator credentials, delete the Orchestrator credentials from the Service Manager configuration and re-add.

Follow the instructions in *Configuring Orchestrator for vIMS Discovery* and then perform a discovery (Topology > Discover All) from the Server Manager.

Deleting an Orchestrator Host

You can delete orchestrator Host and its components.

**Procedure**

1. Right-click the **ESM Domain Manager** and select **Configure ESM Credentials**.

2. In the **Configure ESM Credentials** window, select the credential that you intend to delete and click **Delete** selected credential.

3. In the **Delete confirmation** dialog box, click **yes** to confirm the deletion.

4. In the **ESM Domain Manager**, right-click the **Orchestrator** host instance and select **Delete**, to delete all the vIMS components discovered through this Orchestrator host.

   If you delete the Orchestrator Host in the IP server and then triggers discover-all in the IP server. The Orchestrator components are not deleted in ESM server, only host is deleted.

vIMS Discovery using Cloudify as Orchestrator

This sections provides information on how to discover vIMS using Cloudify as Orchestrator.

**Pre-requisite**

All the servers including IP, SAM, and ESM should up and running.

**Discovery Steps for vIMS:**
Depending on the customer environment there are 2 cases:

1. This has to be the final step that trigger the discovery of Cloudify components in the ESM server. So a prerequisite is that the ESM is installed and configured before executing this step.

   - **Case 1:** ICMP is enabled on the Cloudify. The Cloudify orchestrator need to be discovered in IP domain which in turn trigger the ESM for Cloudify specific discovery. If ICMP pings are enabled on Cloudify the Cloudify has to be discovered as an ICMPONLY device. Refer IP Manager user guide Chapter 11 "Discovery", subsection "Starting discovery".

   - **Case 2:** ICMP is not enabled on the Cloudify. In this case the Cloudify host needs to be created using the following dmctl command replacing the "<ip address>" with the Cloudify ip address:

     ```
     create Host::<ip address>
     create SNMPAgent::SNMPAgent-<ip address>
     create IP::IP-<ip address>
     insert Host::<ip address>::HostsServices SNMPAgent::SNMPAgent-<ip address>
     insert Host::<ip address>::HostsAccessPoints IP::IP-<ip address>
     put SNMPAgent::SNMPAgent-<ip address>::AgentAddress <ip address>
     get SNMPAgent::SNMPAgent-<ip address>::LayeredOver
     insert SNMPAgent::SNMPAgent-<ip address>::LayeredOver IP::IP-<ip address>
     ```

**Troubleshooting Steps**

Some of the common troubleshooting steps are given below, which user must follow if discovery or monitoring is not working.

**Debug flags for vlMS feature (ESM.import file) in ESM**

- EnableCloudifyDiscoveryDebug = TRUE (Default value : FALSE)
- LogLevel = ALL (Default value : ERR)
- IsDebug = TRUE (Default value is FALSE)

**Log file in ESM:**

vlMS discovery logs will be dumped in the generic INCHARGE-ESM log file under local/logs directory.

**Logs in DCF**

Collector logs are located at <DCF_INSTALL_LOCATION>/Collecting/Collector-Manager/<collector Id>/logs/

**Enabling Debug Logs for Collector in DCF**

1. Edit <DCF_INSTALL_LOCATION>/Collecting/Collector-Manager/<collector Id>/conf/logging.properties to increase log level
2 Change the default INFO level to one of – CONFIG, FINE, FINER & FINEST (lowest value).
3 The new log level takes effect in the next discovery.
4 The kafka messages can also be configured to be written to file by editing
   <DCF_INSTALL_LOCATION>/Collecting/Collector-Manager/<collector Id>/conf/
   collecting.xml. Change enabled=true for file collector
   
   <connector enabled="true" name="File" type="File-Connector" config="Collector-
   Manager/<collector Id>/conf/file-connector.xml" />

Discovery can fail due to following reasons:

Orchestrator Credentials are incorrect

Error in the log:
SAM GUI Test Credentials fails.

DCC not responding

Error in the log:

[April 30, 2019 4:35:46 AM EDT +968ms] t027232000 Discovery #1

NV_MESSAGE-*-NV_GENERIC-MSG ERR : [Thread-7 DCCRestClientImpl]:Error occurred while
sending a request to the DCC API
Connection refused (Connection refused)

Kafka Credentials are incorrect

Errors in the log:

[April 30, 2019 4:43:59 AM EDT +481ms] t02223998720 Discovery #1

NV_MESSAGE-*-NV_GENERIC-MSG ERR : [Thread-7 DiscoveryManager]:Error while starting
discovery consumer thread.Timeout expired while fetching topic metadata (invalid
Kafka login credentials may trigger this error)

[April 30, 2019 4:43:59 AM EDT +481ms] t03325163264 platform

Thread-7 Kafka listener start error: Timeout expired while fetching topic metadata
(invalid Kafka login credentials may trigger this error)

VMware Integrated Openstack Management

This section provides end to end installation and configuration of VMware Integrated Openstack
Management.

Overview

VMware Integrated OpenStack (VIO) is a VMware supported OpenStack distribution that makes it
easy for IT to run and manage an enterprise-grade OpenStack cloud on top of VMware
Infrastructure. The VMware Integrated OpenStack architecture connects various virtual resources to the OpenStack Nova, Neutron, Cinder, Identity and Horizon services.

**Nova:** OpenStack Nova service interacts with the VMwareVCDriver (compute driver) to connect OpenStack Compute with vCenter. This driver enables Nova to communicate with a VMware vCenter server managing one or more clusters of ESXi hosts. The nova-compute service communicates, through the vCenter APIs, to a vCenter Server, which handles management of one or more ESXi clusters. The nova-compute service runs on a Linux server (OpenStack compute node) which acts as a proxy that uses the VMwareVCDriver to translate nova API calls to vCenter API calls and relates them to a vCenter server for processing. Hence, when a Nova API call is made to create a VM, Nova compute schedules where the VM is created. If the VM is to be created on a vSphere cluster, Nova compute hands that request off to the vCenter server which then schedules where in the cluster the VM will be created.

**Neutron:** OpenStack Neutron service interacts with the NSX Manager via a plugin for better network management and automating the network components.

VMware Integrated OpenStack offers three types of deployments:

- High Availability Mode
- Compact Mode
- Tiny Mode

The Server Manager provides VMware hypervisor management support for the following:

- VMware Integrated OpenStack compute support (using NOVA API).
- VMware hypervisor and virtual machine discovery via VMware Integrated OpenStack.
- VMware hypervisor and virtual machine monitoring.
- Monitor hypervisor status.
- Monitor virtual machine status.
- VM addition and deletion.
- Tracks virtual machine mobility (VM migration).
- VMware Integrated OpenStack block storage support (using CINDER API).
- Logical volume discovery and monitoring via OpenStack.
- VMware Integrated OpenStack network support (using Neutron API).
- Virtual interface discovery and monitoring via OpenStack
- vRouter discovery and monitoring via VMware Integrated OpenStack.
- VMware Integrated OpenStack service discovery and monitoring.
- Root-cause and impact analysis.
Discovery Flow

The Server Manager discover various VIO components.

The discovered VIO components are:

- ClusterManager
- ControllerService
- ControllerServiceCluster
- ComputeService

KVM logical volume discovery via OpenStack

The Server Manager:

- Discovers all logical volumes associated with virtual machines.
- Displays the relationship of logical volume with tenant, virtual machines, and ScsiLun.
- Generates notifications and provide impact analysis when a KVM logical volume is down.

Virtual interface discovery via OpenStack

The Server Manager:

- Discovers all virtual interfaces.
- Displays the relationship of virtual interface with network adapter, virtual network, and vRouter.
- Generates notifications and provide impact analysis when a virtual interface is down.
vRouter discovery via OpenStack
The Server Manager:
- Discovers all vRouters.
- Displays the relationship of vRouter with virtual network, tenant, and network adapter.
- Generates notifications and provide impact analysis when vRouter is down.

Open vSwitch discovery via OpenStack
The Server Manager:
- Discovers all Open vSwitches.
- Displays the relationship of Open vSwitch with virtual network, interface, OVSApplicationServiceGroup, and host.

OpenStack service discovery
The Server Manager:
- Discovers all OpenStack components (services running on hosts).

Monitoring Flow
This section provides information on the classes which are monitored as part of VIO monitoring.
The monitored VIO components are:
- ClusterManager
- ControllerService
- ControllerServiceCluster
- ComputeService
The Server Mangers also monitors:
- The KVM logical volume status by periodically polling the CINDER API in OpenStack.
- All the virtual interface status.
- All the vRouter status.
- All the all OpenStack services status.

Topology
The Server Manager discovers the topology of the managed VIO eco system. The topology objects represent the managed VIO elements and their relationships among other components.
VIO topology objects include:
- **ClusterManager**: Represent the OpenStack Management Server of the VIO eco system
- **ComputeService**: Represents the Compute Service of the VIO eco system.
- **ControllerService**: Represents the Controller Service of the VIO eco system.
- **ControllerServiceCluster**: Represents the Controller Services as cluster on the ESM topology.

### ClusterManager attributes

ClusterManager has the following relationships:

- *Administrates* with CloudController, ComputeService, and ControllerServiceCluster
- *RunningOn* with VirtualMachine

#### Table 1-18. Attributes for the ClusterManager objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>cloudControllerVIP</td>
<td>Indicates virtual IP address of the CloudController which is administrated by the ClusterManager.</td>
<td>String</td>
</tr>
<tr>
<td>vcName</td>
<td>Indicates name or IPaddress of the vCenter which manages the OpenStack Management Server</td>
<td>String</td>
</tr>
<tr>
<td>vmName</td>
<td>Indicates name or IPaddress of the virtual machine where the OpenStack Management Server is running</td>
<td>String</td>
</tr>
</tbody>
</table>

### ComputeService attributes

ComputeService attributes has the following relationships:

- *AdministratedBy* with ClusterManager
- *Maps* with VMwareCluster
- *ProvideServiceBy* with Hypervisor
- *RunningOn* with VirtualMachine

#### Table 1-19. Attributes for the ComputeService objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>hypervisorName</td>
<td>Indicates the name or IPaddress of the Hypervisor where the ComputeService is running.</td>
<td>String</td>
</tr>
<tr>
<td>vcName</td>
<td>Indicates the name or IPaddress of the vCenter which manages the ComputeService</td>
<td>String</td>
</tr>
<tr>
<td>vmName</td>
<td>Indicates the name or IPaddress of the virtual machine where the ComputeService is running</td>
<td>String</td>
</tr>
</tbody>
</table>

### ControllerService attributes

ControllerService attributes has the following relationships:
Table 1-20. Attributes for the ControllerService objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>hypervisorName</td>
<td>Indicates the name or IP address of the Hypervisor where the ControllerService is running.</td>
<td>String</td>
</tr>
<tr>
<td>vcName</td>
<td>Indicates the name or IP address of the vCenter which manages the ControllerService.</td>
<td>String</td>
</tr>
<tr>
<td>vmName</td>
<td>Indicates the name or IP address of the virtual machine where the ControllerService is running.</td>
<td>String</td>
</tr>
</tbody>
</table>

ControllerServiceCluster attributes

ControllerServiceCluster has the following relationships:

- *AdministratedBy* with ClusterManager
- *ComposedOf* with ControllerService

Table 1-21. Attributes for the ControllerServiceCluster objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>CreationClassName</td>
<td>Indicates the creation class Name of the ControllerServiceCluster.</td>
<td>String</td>
</tr>
<tr>
<td>Name</td>
<td>Indicates the name of the ControllerServiceCluster</td>
<td>String</td>
</tr>
</tbody>
</table>

Root Cause and Impact Analysis

This section provides information on root cause and impact analysis for various events.

Following table lists the root-cause problem diagnosed and the impacted classes.

Table 1-22. Root-cause problems for VIO management classes

<table>
<thead>
<tr>
<th>Class</th>
<th>Root Cause</th>
<th>Event (symptoms) of root cause</th>
<th>Impacted System</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Down</td>
<td>Down</td>
<td>Hypervisor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>DownOrImpaired</td>
<td>VirtualMachines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Unresponsive</td>
<td>Host</td>
</tr>
<tr>
<td></td>
<td></td>
<td>InterfaceLostConnection</td>
<td>Interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ServiceAffected</td>
<td>ControllerService</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ComputeService</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AtRisk</td>
<td>ControllerServiceCluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReducedRedendancy</td>
<td></td>
</tr>
<tr>
<td>Hypervisor</td>
<td>Down</td>
<td>DownOrImpaired</td>
<td>VirtualMachines</td>
</tr>
</tbody>
</table>
Table 1-22. Root-cause problems for VIO management classes (continued)

<table>
<thead>
<tr>
<th>Class</th>
<th>Root Casue</th>
<th>Event (symptoms) of root cause</th>
<th>Impacted System</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>HostLostConnection</td>
<td>Hypervisor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerOff</td>
<td>Hypervisor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>InterfaceLostConnection</td>
<td>Interface</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ServiceAffected</td>
<td>ControllerService</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ComputeService</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AtRisk</td>
<td>ControllerServiceCluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReducedRedendancy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AllComponentsDown</td>
<td></td>
</tr>
<tr>
<td>VirtualMachine</td>
<td>Down</td>
<td>DownOrImpaired</td>
<td>VirtualMachine</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ServiceAffected</td>
<td>ControllerService</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>ComputeService</td>
</tr>
<tr>
<td></td>
<td></td>
<td>AtRisk</td>
<td>ControllerServiceCluster</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ReducedRedendancy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AllComponentsDown</td>
<td></td>
</tr>
</tbody>
</table>

The Server Manager provides:

- Impact analysis and diagnosis when a hypervisor server is down. For example, it diagnoses when a VMware hypervisor host goes down (Host Down) and identifies the impact to a virtual machine (Down).

- Impact analysis and diagnosis when a physical switch is down. For example, it diagnoses when a physical switch goes down and identifies the impact to the hypervisor and virtual machines.

- Impact analysis and diagnosis when a hypervisor server is down. For example, it diagnoses when a hypervisor host goes down (Host Down) and identifies the impact to ComputeService or ControllerService (Service Affected).

- Impact analysis and diagnosis when a Virtual Machine is down. For example, it diagnoses when a Virtual Machine goes down (Host Down) and identifies the impact to ComputeService or ControllerService (Service Affected).

- Impact analysis and diagnosis when a Virtual Machine is down. For example, it diagnoses when a Virtual Machine goes down (Host Down) and identifies the impact to ClusterManager (Service Affected).

- Impact analysis and diagnosis when a logical/tap interface is down. For example, it diagnoses when a logical interface goes down (Interface Down) and identifies the impact to a virtual machine (VMLostConnection).

- Impact analysis and diagnosis when a vRouter is down. For example, it diagnoses when a vRouter goes down and identifies the impact to a virtual machine.
Impact analysis and diagnosis when a virtual interface is down. For example, it diagnoses when the virtual interface of a vRouter or virtual machine goes down and identifies the impact to a virtual machine.

Impact analysis and diagnosis when the physical interface of the hypervisor is down. For example, it diagnoses when a physical interface goes down and identifies the impact to a virtual machine.

Impact analysis and diagnosis when a host hosting OpenStack service is down. For example, it diagnoses when a host hosting OpenStack service goes down and identifies the impact to CloudController and VMs.

### Physical Hypervisor hosting Host Down

![Physical Hypervisor hosting Host Down]

### Hypervisor Down

![Hypervisor Down]
Compute VirtualMachine PoweredOff

Install and Configure

This section provides information on installation and configuration of open source and VSA components.

**Note**  Perform the installation of the following VSA Components prior to further configurations.

**SMARTS**

Refer, Domain Manager

**Notification UI**

Refer, UI Components

**Configuration**

This section provides information on custom configuration from Server Manager side.

**Configuring VIO Credentials**

To configure Server Manager to communicate with VIO, specify the Virtual IP address credentials of the Keystone Service.

**Prerequisites**

For this task, when you use the console, you need to have Smart administrator credentials to open the Configure menu where you specify the Openstack credentials.

**Procedure**

1. Open the **Service Assurance Manager Global Console** attached to the Server Manager (INCHARGE-ESM, by default).
In the **Topology Browser Console**, select **Configure > Domain Manager Administration Console**.

Right-click the ESM server in the left pane and select **Configure ESM credentials**.

In the **Configure ESM credentials** dialog box, select **Openstack** for the host type.

Type values in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Virtual IP address of KeyStone Service</td>
</tr>
<tr>
<td>User ID</td>
<td>VIO administrator user name</td>
</tr>
<tr>
<td>Password</td>
<td>VIO administrator password</td>
</tr>
<tr>
<td>Domain</td>
<td>VIO domain. Value is default if not provided.</td>
</tr>
<tr>
<td>Port</td>
<td>Port number for the keystone service. Default is: 5000.</td>
</tr>
</tbody>
</table>

Click **Apply credential with testing**.

Verify that your Openstack credentials are accepted by checking the status indicator in the **Configure ESM credentials** dialog box.

A green Passed test status indicates that the credentials are accepted.

If the Openstack credentials are not accepted, confirm that the credentials are correct and enter them again in the **Configure ESM credentials** dialog box.

Click **Close**.

In the **Domain Manager Administration Console**, select your IP Manager and select **Topology > Discover All** to discover VIO. At the end of the IP Manager discovery process, the Server Manager discovery process is automatically started.

Verify that VIO credentials are accepted in the log file

Verify that your VIO credentials are accepted by checking your log file.

**Procedure**

1. Open the Server Manager log file in the `opt/InCharge/ESM/smarts/local/logs` directory.
2. Locate the credential messages.

**Example**

For example, the following messages indicate the Openstack credentials are accepted:

```
[February 2, 2019 6:42:20 PM GMT+05:30 +251ms] t@7336 ESM-SYNC-DRIVER DISC-*=CAL_FR-Credential_Util::addCredential : was called for credential: OPENSTACK-10.31.119.21
[February 2, 2019 6:42:20 PM GMT+05:30 +251ms] t@7336 ESM-SYNC-DRIVER DISC-*=CAL_FR-Credential_Util::addCredential : was called for credential: OPENSTACK-10.31.119.21
```

VMware, Inc.
VMware Integrated OpenStack Consolidation in presence of VMware vSphere

With only VMware Integrated OpenStack discovered the Virtual Machine are associated with the Hypervisor that are part of the VIO.

When user discovers VMware Integrated OpenStack and the associated VMware Virtual Center servers together, the VirtualMachine are replaced with the VMware Virtual Center VM and gets disassociated with the Hypervisors that are discovered as part of VIO discovery.

VMware Integrated OpenStack Consolidation in presence of NSX-T

When user discovers both VMware Integrated OpenStack and the associated NSX-T Manager together on Server Manager Topology, the following relationships are formed between topology objects as part of the consolidation:

- vRouter Manifests LogicalRouter
- VirtualNetwork Manifests LogicalSwitch

Troubleshooting Steps

Some of the common troubleshooting steps are given below, which user must follow if discovery or monitoring is not working.

Debug flags for VIO Feature

- Logging and troubleshooting:
  - Debug flags for OpenStack feature are present under $SM_HOME/conf/esm/ESM.import file.
  - Modify the file using sm_edit utility.
  - Update EnableOpenStackDiscoveryDebug = TRUE (Default value : FALSE) for enabling the discovery related logging.
  - Update EnableOpenStackMonitoringDebug = TRUE (Default value : FALSE) for enabling the monitoring related logging.
  - Change LogLevel = DEBUG (Default value : ERR) to increase logging levels if required.
  - No restart is required.

- Logs and log locations:
  - ESM server logs can be found under $SM_HOME/local/log directory.
VIO errors and logging for troubleshooting

- Scenario 1- Errors observed due to Controller/OpenStack ManagementServer Down:

  [April 20, 2019 4:44:48 PM GMT+05:30 +436ms] t@3682531072 Discovery #14
  NV_MESSAGE-*-NV_GENERIC-MSG ERR : [Thread-2365 OpenStackDiscoveryProbe]:Exception in OpenStack Discovery
  [April 20, 2019 4:44:48 PM GMT+05:30 +436ms] t@446584576 platform
  MAIN_MSG-*-STDFD_ERR-stderr: java.lang.Exception: Could not retrieve credentials for OpenStack : 10.234.61.189
  at com.emc.asd.openstack.OpenStackDiscoveryProbe.invoke(OpenStackDiscoveryProbe.java:321)
  at com.smarts.java_probe.ProbeRunner.invoke(ProbeRunner.java:69)

  [April 20, 2019 4:44:48 PM GMT+05:30 +763ms] t@3682531072 Discovery #14
  TM-W-EPROBE-Probe driver failed when probing element 'SNMPAgent=10.234.61.189'. Discovery error is 'java.lang.Exception: Could not retrieve credentials for OpenStack : 10.234.61.189'

- Scenario 2- Errors observed due to NSX Manager Down

  [April 20, 2019 4:21:32 PM GMT+05:30 +943ms] t@446584576 platform
  MAIN_MSG-*-STDFD_ERR-stderr: java.lang.Exception: Could not retrieve credentials for NSX-T : 10.234.24.70
  at com.emc.asd.nsx.NSXTDiscoveryProbe.invoke(NSXTDiscoveryProbe.java:166)
  at com.smarts.java_probe.ProbeRunner.invoke(ProbeRunner.java:69)
  [April 20, 2019 4:21:33 PM GMT+05:30 +180ms] t@3686733568 Discovery #9
  TM-W-EPROBE-Probe driver failed when probing element 'SNMPAgent=10.234.24.70'. Discovery error is 'java.lang.Exception: Could not retrieve credentials for NSX-T : 10.234.24.70'

- Scenario 3- Errors observed due to VIO vCenter Down

  ASL-W-ERROR_RULE_SOURCE-While executing rule set '/opt/INCHARGE10/ESM/smarts/rules/nv/openstack-post.asl'
  ASL-ERROR_ACTION-While executing action at:
  ASL-CALL_STACK_RULE- RuleName: VMWARE_VIO_MAP_CLUSTER_MANAGER_TO_VM, Line: 675
  ASL-CALL_STACK_RULE- RuleName: VMWARE_VIO_MAP_SERVICES_CLUSTER_MANAGER_TO_VM, Line: 662
  ASL-CALL_STACK_RULE- RuleName: START, Line: 54
  ASL-ERROR_RESULT_ASSIGNMENT-While assigning to the variable 'mgmtVM' in rule 'VMWARE_VIO_MAP_CLUSTER_MANAGER_TO_VM'
  ASL-UNDEFINED_INTERMEDIATE-Function 'GET_MGMT_SRV_VM_OBJ' failed to return a value

  MAIN_MSG-*-STDFD_ERR-stderr: java.net.UnknownHostException: compute01: Name or service not known
  at java.net.Inet6AddressImpl.lookupAllHostAddr(Native Method)
  at java.net.InetAddress$2.lookupAllHostAddr(InetAddress.java:928)
  at java.net.InetAddress.getAddressesFromNameService(InetAddress.java:1323)
  at java.net.InetAddress.getAllByName0(InetAddress.java:1276)
  at java.net.InetAddress.getAllByName(InetAddress.java:1192)
  at java.net.InetAddress.getByName(InetAddress.java:1126)
  at java.net.InetAddress.getByName(InetAddress.java:1076)
  at com.emc.asd.common.Utils.getFQDNFromName(Utils.java:116)
  at com.emc.asd.factory.dmt.DmtObjectFactory.getHostNameByName(DmtObjectFactory.java:1280)
vCloud Director Management

This section provides end to end installation and configuration of vCD (vCloud Director) Smart Assurance.

Overview

VMware vCloud Director (vCD) is a software product that provides the ability to build secure, multi-tenant clouds by pooling virtual infrastructure resources into virtual datacenters and exposing them to users through Web-based portals and programmatic interfaces as a fully-automated, catalog-based service.

vCloud Director relies on vSphere resources to provide CPU and memory to run virtual machines. In addition, vSphere datastores provide storage for virtual machine files and other files necessary for virtual machine operations. vCloud Director also utilizes vSphere distributed switches and vSphere port groups to support virtual machine networking.

vSphere resources are used to create cloud resources. Cloud resources are an abstraction of their underlying vSphere resources. They provide the compute and memory resources for vCloud Director virtual machines and vApps. Cloud resources also provide access to storage and network connectivity. Cloud resources include provider and organization virtual datacenters, external networks, organization vDC networks, and network pool.

vCloud Director introduces a number of logical components to support the notion of a VDC and multi-tenancy that is presented to end users. The following are the main logical components:

Provider Virtual Datacenter: A provider VDC is a logical grouping of compute and storage resources. The provider VDC groups together a set of vSphere hosts and a set of one or more associated datastores. This logical grouping is then made available for consumption by organizations.

Organizations: One of the key capabilities of a vCloud Director private cloud is secure multitenancy. The organization concept is one of the key building blocks of this. A vCloud Director organization is a unit of administration that represents a Collection of users and user groups. An organization also serves as a security boundary, because users from a particular organization have visibility only to other users and resources allocated to that organization.

Organization Virtual Datacenter: An organization VDC is a logical grouping of resources from one or more provider VDCs that an organization is allowed to access. Depending on back-end (provider VDC) configuration and needs of the organization, one or more sets of resources backed by different provider VDCs might be present. This enables different performance, SLA or cost options to be available to organization users when deploying a workload.
**vApps:** A VMware vSphere vApp is an abstraction that encapsulates all of the virtual machine and internetworking needs of an application. vApps can be as simple as a single virtual machine or as complex as a multitier business application. Templates can be created from a vApp to enable one to be easily redeployed multiple times by an organization’s users.

The Server Manager provides vCloud Director management support for the following:

- vCloud Director components discovery using REST API
- Association of vCD components with the virtual infrastructure discovered through vCenter and NSX.
- Root-cause and Impact analysis.

**Discovery Flow**

The Server Manager discovers and monitors various vCloud Director components via REST API.

The Server Manager imports initial topology from the IP Availability Manager. After the topology is imported, Server Manager discovers domain-specific entities related to the features and creates additional topology objects for those features.

As a first step of discovery, vCD (vCloud Director) is discovered based on ICMP discovery. On discovery of vCloud Director (Host) in SMARTS-IP domain manager, SMARTS ESM server imports the Host from IP Domain Manager and further does a complete discovery of vCloud Director topology.

**vCloud Director (vCD) Discovered Components are:**

- Cloud Controller
- Organization (Tenant)
- Organization vDC
- Provider vDC
- vApp (Virtual Appliance)
vCD components table summarizes list of the vCD components used in Server Manager.

**Table 1-23. vCD components**

<table>
<thead>
<tr>
<th>vCD Components</th>
<th>Smarts Model Representation of vCD Components in ESM</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCloud Director</td>
<td>CloudController</td>
</tr>
<tr>
<td>Organization</td>
<td>Tenant</td>
</tr>
<tr>
<td>OrganizationVDC</td>
<td>OrganizationVDC</td>
</tr>
<tr>
<td>ProviderVDC</td>
<td>ProviderVDC</td>
</tr>
<tr>
<td>vApp</td>
<td>VirtualAppliance</td>
</tr>
</tbody>
</table>

**Monitoring Flow**

This section provides information on the classes which are monitored as part of vCD monitoring.

For first time when discovery is initiated from SMARTS Domain Manager, DCF controller (part of the DCF framework) instantiates and deploys the vCloud Director discovery and monitoring collectors. The vCloud Director monitoring collector, polls vCloud Director based on specified polling cycle and frequency. The monitoring collector polls for the monitored attributes of the discovered vCloud Director topology objects.
vCloud Director (vCD) monitored components are:

- Organization vDC
- Virtual Appliance

**Topology**

The Server Manager builds a topology of the deployed vCD components. The topology objects represent the vCD deployed components, their relationships, and their association with tenants and virtual infrastructure.

vCloud Director (vCD) version 9.5 is supported in Smart Assurance 10.1.

vCD topology objects include:

- **VirtualAppliance**: A vApp is an application container containing one or more virtual machines.
- **OrganizationVDC**: Organization vDC allocates resources to organization. An organization vDC is partitioned from a provider vDC.
- **ProviderVDC**: A Provider VDC is a collection of compute, memory, and storage resources from one vCenter server. A Provider VDC provides resources to organization VDCs.
- **Tenant**: User of cloud computing service, who shares resources and cost of underlying hardware resources like compute, storage and network with other users.
- **CloudController**: Represents vCloud Director, which is deployment, automation and management software for virtual infrastructure resources in multi-tenant cloud environments.

**VirtualAppliance relationships and attributes**

VirtualAppliance has the following relationships:

- **Contains** with VirtualMachine
- **PartOf** with OrganizationVDC

**Table 1-24. Attributes for the VirtualAppliance objects**

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllocatedCPU</td>
<td>Indicates the CPU allocated to this vApp in MHZ.</td>
<td>String</td>
</tr>
<tr>
<td>AllocatedMemory</td>
<td>Indicates the memory allocated to this vApp in MB.</td>
<td>String</td>
</tr>
<tr>
<td>AllocatedStorage</td>
<td>Indicates the Storage Allocated to this vApp in KB.</td>
<td>String</td>
</tr>
<tr>
<td>IsApplianceDown</td>
<td>Indicates the Appliance is down or not.</td>
<td>Boolean</td>
</tr>
<tr>
<td>numberOfCpus</td>
<td>Indicates the number of CPUs of the vApp.</td>
<td>String</td>
</tr>
<tr>
<td>numberOfVMs</td>
<td>Indicates the number of VMs in this vApp.</td>
<td>String</td>
</tr>
</tbody>
</table>
### Table 1-24. Attributes for the VirtualAppliance objects (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>OrgVDCId</td>
<td>Id of the Organization VDC this vApp belongs to.</td>
<td>String</td>
</tr>
<tr>
<td>OrgVDCName</td>
<td>Name of the Organization VDC this vApp belongs to.</td>
<td>String</td>
</tr>
<tr>
<td>Status</td>
<td>Represents the status of the vCloud Director managed vApp.</td>
<td>Enum</td>
</tr>
<tr>
<td>vAppId</td>
<td>Indicates Id of the vApp.</td>
<td>String</td>
</tr>
<tr>
<td>vmIPAddressList</td>
<td>Comma separated list of Virtual Machine IP Addresses.</td>
<td>String</td>
</tr>
<tr>
<td>vmMACAddressList</td>
<td>Comma separated list of Virtual Machine/Interface MAC Addresses.</td>
<td>String</td>
</tr>
</tbody>
</table>

### OrganizationVDC relationships and attributes

OrganizationVDC has the following relationships:

- **ComposedOf** with VirtualAppliance
- **OwnedBy** with Tenant
- **ResourcesProvidedBy** with ProviderVDC
- **AccessesNetwork** with LogicalSwitch

### Table 1-25. Attributes for the OrganizationVDC objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>AllocationModel</td>
<td>Defines how resources are allocated from the Provider VDC.</td>
<td>String</td>
</tr>
<tr>
<td>FreeMemory</td>
<td>The free memory units in MB as reported by vCloud Director Rest API.</td>
<td>Int</td>
</tr>
<tr>
<td>FreeMemoryPct</td>
<td>The percentage of free memory of the total memory.</td>
<td>Double</td>
</tr>
<tr>
<td>FreeMemoryThreshold</td>
<td>The threshold for minimum amount of free memory expressed as a percentage of total amount of memory.</td>
<td>Unsigned-int</td>
</tr>
<tr>
<td>networkQuota</td>
<td>Network Quota allocated to this Organization VDC</td>
<td>String</td>
</tr>
<tr>
<td>nicQuota</td>
<td>Nic Quota allocated to this Organization VDC</td>
<td>String</td>
</tr>
<tr>
<td>orgVDCId</td>
<td>Unique Identifier for the Organization VDC.</td>
<td>String</td>
</tr>
</tbody>
</table>
### Table 1-25. Attributes for the OrganizationVDC objects (continued)

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProcessorUtilizationThreshold</td>
<td>The upper threshold for processor utilization expressed as a percentage of the total capacity of the processor.</td>
<td>Unsigned-int</td>
</tr>
<tr>
<td>TotalCPU</td>
<td>The total Allocated CPU/Processor in MHZ as reported by vCloud Director Rest API.</td>
<td>Int</td>
</tr>
<tr>
<td>TotalMemory</td>
<td>The total Allocated memory in MB as reported by vCloud Director Rest API.</td>
<td>Int</td>
</tr>
<tr>
<td>UsedCPU</td>
<td>The utilized CPU/Processor in MHZ as reported by vCloud Director Rest API.</td>
<td>Int</td>
</tr>
<tr>
<td>UsedCpuPct</td>
<td>The percentage of used CPU/Processor of the total allocated CPU/Processor</td>
<td>Double</td>
</tr>
<tr>
<td>vmQuota</td>
<td>VM Quota allocated to this Organization VDC.</td>
<td>String</td>
</tr>
</tbody>
</table>

### ProviderVDC relationships and attributes

ProviderVDC has the following relationships:

- **AssociatedVC** with VirtualCenter
- **ProvidesResourcesTo** with OrganizationVDC
- **VDCManagedBy** with CloudController

### Table 1-26. Attributes for the ProviderVDC objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>providerVDCId</td>
<td>Unique Identifier for the Provider VDC.</td>
<td>String</td>
</tr>
<tr>
<td>vimServerID</td>
<td>Unique identifier of the vCenter this ProviderVDC uses resources.</td>
<td>String</td>
</tr>
<tr>
<td>vimServerIPAddress</td>
<td>IP address of the vCenter this ProviderVDC uses resources.</td>
<td>String</td>
</tr>
</tbody>
</table>

### Tenant relationships and attributes

Tenant has the following relationships:

- **Owns** with OrganizationVDC
- **ConsistsOf** VirtualMachine
- **SupervisedBy** with CloudController
### Table 1-27. Attributes for the Tenant objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPAddress</td>
<td>IP Address of the OpenStack management Server.</td>
<td>String</td>
</tr>
<tr>
<td>NumberOfVirtualMachine</td>
<td>Number of Virtual machine used by this Tenant.</td>
<td>Int</td>
</tr>
<tr>
<td>UUID</td>
<td>Unique identifier of this Tenant.</td>
<td>String</td>
</tr>
<tr>
<td>VirtualMachinesTotal</td>
<td>The total number of Virtual Machines that belong to this tenant.</td>
<td>Float</td>
</tr>
</tbody>
</table>

### CloudController relationships and attributes

CloudController has the following relationships:

- *ManagesVDC* with *ProviderVDC*
- *Supervises* with *Tenant*
- *HostedBy* with *Host*

### Table 1-28. Attributes for the CloudController objects

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
<th>Allowed values</th>
</tr>
</thead>
<tbody>
<tr>
<td>IPAddress</td>
<td>IP Address of the OpenStack management Server.</td>
<td>String</td>
</tr>
<tr>
<td>SystemName</td>
<td>The Name of the ICIM_System hosting this service.</td>
<td>String</td>
</tr>
<tr>
<td>SystemVendor</td>
<td>The name of the System's supplier.</td>
<td>String</td>
</tr>
<tr>
<td>Vendor</td>
<td>The name of the Application's supplier.</td>
<td>String</td>
</tr>
<tr>
<td>Version</td>
<td>Version of the CloudController Instance.</td>
<td>String</td>
</tr>
</tbody>
</table>

### Root-cause Analysis

This section provides information on root cause and impact analysis for various events.

Following table lists the root-cause problem diagnosed and the impacted classes.

### Table 1-29. Root-cause problems for VCD classes

<table>
<thead>
<tr>
<th>Class</th>
<th>Root Cause</th>
<th>Event (symptoms) of root cause</th>
<th>Impacted Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>Down</td>
<td>Down</td>
<td>Hypervisor</td>
</tr>
<tr>
<td></td>
<td>DownOrImpaired</td>
<td>DownOrImpaired</td>
<td>VirtualMachines</td>
</tr>
<tr>
<td></td>
<td>Unresponsive</td>
<td>Unresponsive</td>
<td>Host</td>
</tr>
<tr>
<td></td>
<td>InterfaceLostConnection</td>
<td>InterfaceLostConnection</td>
<td>Interface</td>
</tr>
</tbody>
</table>
Table 1-29. Root-cause problems for VCD classes (continued)

<table>
<thead>
<tr>
<th>Class</th>
<th>Root Cause</th>
<th>Event (symptoms) of root cause</th>
<th>Impacted Systems</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hypervisor</td>
<td>Down</td>
<td>DownOrImpaired</td>
<td>VirtualMachines</td>
</tr>
<tr>
<td></td>
<td></td>
<td>HostLostConnection</td>
<td>Hypervisor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>PowerOff</td>
<td>Hypervisor</td>
</tr>
<tr>
<td></td>
<td></td>
<td>InterfaceLostConnection</td>
<td>Interface</td>
</tr>
<tr>
<td>VirtualMachine</td>
<td>Down</td>
<td>DownOrImpaired</td>
<td>VirtualMachine</td>
</tr>
</tbody>
</table>

The Server Manager provides:

- Impact analysis when a hypervisor server is down. For example, it diagnoses when a VMware hypervisor host goes down (Host Down) and identifies the impact to a virtual machine (Down).
- Impact analysis when a physical switch is down. For example, it diagnoses when a physical switch goes down and identifies the impact to the hypervisor and virtual machines.
- Impact analysis when a logical/tap interface is down. For example, it diagnoses when a logical interface goes down (Interface Down) and identifies the impact to a virtual machine (VMLostConnection).
- Impact analysis when the physical interface of the hypervisor is down. For example, it diagnoses when a physical interface goes down and identifies the impact to a virtual machine.
- Impact analysis and diagnosis when a host hosting vCloud Director is down. For example, it diagnoses when a host hosting vCloud Director goes down and identifies the impact to CloudController.

CloudController Monitoring Failure Event

Monitoring failure shows details like “error in reading kafka messages” due to which monitoring failed. This may be due to Cloud Controller down or Kafka down.
CloudController Unreachable Event

CloudController Unreachable event indicates vCD (vCloud Director) is not reachable or down. Which is caused-by VM or Host which is hosting vCloud Director is down or Unresponsive.

OrganizationVDC HighMemoryUtilization Event

This event indicates that Memory for that Organization VDC is getting utilized more than the configured threshold. Details tab in notification window shows the FreeMemoryThreshold, FreeMemory, FreeMemoryPct and TotalMemory.
VirtualAppliance StoppedPartiallyRunningOrSuspended Event

This event indicates that one or many VMs that are part of that VirtualAppliance is either stopped or suspended or powered-off.

VM down event impacting cloud-controller

This VM down problem show Host Unresponsive and CloudController down events as impacts.
Install and Configure

This section provides information on installation and configuration of open source and VSA components.

**Note**  Perform the installation of the following VMware Smart Assurance Components prior to further configurations.

**Messaging**
Refer, Installing Kafka

**SMARTS**
Refer, Domain Manager

**Data Management**
Refer, Installing Data Collection Framework
Refer, Data Collection Controller

**Notification UI**
Refer, UI Components

**Configuration**

This section provides information on custom configuration for vCD (vCloud Director) from Server Manager side.

**Enabling and Disabling VCD discovery**

By default, vCD discovery is enabled (The IsVCD parameter is set to True) in the ESM.import file.
If you need to disable vCD discovery:

Procedure
1. At BASEDIR/smarts/bin, type the following command:
   ```
   sm_edit conf/esm/ESM.import
   ```
2. Change the IsVCD value to False:
   ```
   IsVCD = False
   ```
3. Save and close the file.
4. Restart the Server Manager to load the changed values in ESM.import file.

Configuring IP/ESM Domain for vCloud Director Discovery

For Discovery of vCD:
- Discover vCenter host in IP used for vCloud Director to provide resources.
- Configure vCenter credentials in ESM server for vCenter discovery. Refer, chapter VMware Management, in VMware Smart Assurance Server Manager User and Configuration Guide for more information.
- Discover NSX host in IP used for vCloud Director to enable network resources. Refer, chapter Software-Defined Networks Management, in VMware Smart Assurance Server Manager User and Configuration Guide for more information.
- Configure NSX credentials in ESM for NSX discovery.
- Discover vCloud Director as host in IP using ICMP-Only mode.

Configure vCloud Director through GUI

To configure Smarts Server Manager to communicate with vCloud Director, specify the vCloud Director administrator credentials and the IP address of the vCloud Director host.

Prerequisites

For this task, when you use the console, you need to have Smarts administrator credentials to open the Configure menu where you specify the vCloud Director credentials.

Procedure
1. Open the Service Assurance Manager Global Console attached to the Server Manager (INCHARGE-ESM, by default).
2. In the Topology Browser Console, select Configure > Domain Manager Administration Console.
3. Right-click the ESM server in the left pane and select Configure ESM credentials.
4. In the Configure ESM credentials dialog box, select vCloud Director for the host type.
5 Type values in the following fields:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host</td>
<td>IP address of the vCloud Director host.</td>
</tr>
<tr>
<td>User ID</td>
<td>vCloud Director user name.</td>
</tr>
<tr>
<td>Password</td>
<td>vCloud Director administrator password</td>
</tr>
<tr>
<td>Port</td>
<td>vCloud Director port (default value is 443)</td>
</tr>
</tbody>
</table>

6 Click **Apply credential with testing**.

7 Verify that vCloud Director credentials are accepted for the vCloud Director by checking the status indicator in the **Configure ESM credentials** dialog box.

A green Passed test status indicates that the credentials are accepted. If the orchestrator credentials are not accepted, confirm that the credentials are correct and enter them again in the **Configure ESM credentials** dialog box.

8 Click **Close**.

**Note** Configure Kafka/Kafka Cluster and DCF Controller details in clientConnect.conf and esm-param.conf, refer Configuring Kafka/Kafka Cluster and Data Collection Framework(DCF) Controller details for vCD.

### Configuring vCloud Director credentials through clientConnect.conf file

You need to specify the vCloud Director credentials in the clientConnect.conf file located in the Server Manager installation directory.

You can also configure the vCloud Director credentials through GUI, as mentioned in Configure vCloud Director through GUI.

To specify credentials:

**Procedure**

1 At BASEDIR/smarts/bin, type the following command:
   ```
   sm_edit conf/clientConnect.conf
   ```

2 Enter the following line for each vCloud Director instance:
   ```
   clouddirector:<vCloudDirector_IP_Address>:<vCloudDirector_Username>:<vCloudDirector_Password>:<Protocol>:<vCloudDirector_Port>
   ```

   You must add the line for vCloud Director instance above the line for the Smarts admin user.

   “::admin:<E-1.0>94689C5A7C826FD58DDE9F62284A68191EC739743EA25E5E1F76FE493337D558” in the clientConnect.conf file.

   For example:
   ```
   ```
3  Save and close the file.
4  Restart the Server Manager.

**Note**  Configure Kafka/Kafka Cluster and DCF Controller details in clientConnect.conf and esm-param.conf, refer [Configuring Kafka/Kafka Cluster and Data Collection Framework(DCF) Controller details for vCD](#).

### Configuring Kafka/Kafka Cluster and Data Collection Framework(DCF) Controller details for vCD

You need to specify the Kafka/Kafka Cluster and DCF Controller credentials in the clientConnect.conf file and specify the VCloud Director, Kafka/Kafka Cluster and DCF Controller details in esm-param.conf file located in the Server Manager installation directory.

To specify credentials:

**Procedure**

1  At BASEDIR/smarts/bin , type the following command:
   ```
   sm_edit conf/clientConnect.conf
   ```
2  Enter the following line for Kafka and DCC instance:
   ```
   kafka:<kafka_IP_Address>:<kafka_Username>:<kafka_Password>:<Discovery_Topic>:<Monitoring_Topic>
   dcc:<dcf_controller_IP_Address>:<dcf_controller_Username>:<dcf_controller_Password>:<Protocol>:<Port>
   ```
   You must add the line for kafka and dcc instances above the line for smarts admin user “::admin:<E-1.0>94689C5A7C826FD58DDE9F62284A68191EC739743EA25E5E1F76FE493337D558” in the clientConnect.conf file.
   For example:
   ```
   ```
   **Note**  In case of Kafka Cluster add the details of any one Kafka broker.
3  Save and close the file.
4  At BASEDIR/smarts/bin , type the following command:
   ```
   sm_edit conf/esm/esm-param.conf
   ```
5  Enter the following line for vCloud Director, Kafka and DCF Controller
   ```
   # For providing single broker instance use below format.
   KAFKA-<vCloudDirector_host_IP_address> <Kafka_broker_ip_address:port>
   ```
   ```
   # For providing multiple broker instances of a kafka cluster use below format.
   ```
KAFKA-<vCloudDirector_host_IP_address>
<Kafka_broker1_ip_address>:<port1>,<Kafka_broker2_ip_address>:<port2>,
......,<Kafka_broker[n]_ip_address>:<port[n]>

# For providing DCF Controller instance use below format
DCC- <vCloudDirector_IP_Address> dcf_controller_IP_Address

For Example:
KAFKA-xx.xx.xx.xx zz.zz.zz.zz:9092,zz.zz.zz.zz:9093, zz.zz.zz.zz:9094
DCC- xx.xx.xx.xx yy.yy.yy.yy

6 Restart the Server Manager.

Polling and Thresholds
You can configure polling interval defaults by using the Polling and Thresholds console of the
Domain Manager Administrator Console.

Through the default polling groups for the Server Manager you control the polling of the vCloud
Director. The polled data serves as input to the Server Manager root-cause and impact analysis.

Default Polling Groups
Default polling group for the Server Manager for vCD table, lists the default polling group and the
setting.

Table 1-30. Default polling group for the Server Manager for vCD

<table>
<thead>
<tr>
<th>Polling Group</th>
<th>Default Setting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCD Polling Groups</td>
<td>vCloud Director Polling</td>
</tr>
</tbody>
</table>

Default Polling Settings
Default values for the VCD Settings table lists the VCD relevant polling parameters.

Table 1-31. Default values for the VCD Settings

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Default Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AnalysisMode</td>
<td>ENABLED, DISABLED</td>
<td>Enables or Disables Polling.</td>
</tr>
<tr>
<td>PollingInterval</td>
<td>30 to 3600 seconds, Default 1200</td>
<td>Time between successive polls.</td>
</tr>
</tbody>
</table>

Updating the vCloud Director Credentials for the Server Manager Configuration
If the vCloud Director administrator changed the administrator credentials, delete the vCloud
Director credentials from the Service Manager configuration and re-add.

Follow the instructions in ,Configure vCloud Director through GUI and then perform a discovery
(Topology > Discover All) from the Server Manager.
Deleting a vCloud Director Host

To delete vCloud Director Host and its components:

1. Right-click the ESM Domain Manager and select Configure ESM Credentials.
2. In the Configure ESM Credentials window, select the credential that you intend to delete and click Delete selected credential.
3. In the Delete confirmation dialog box, click yes to confirm the deletion.
4. In the ESM Domain Manager, right-click the vCloud Director host instance and select Delete, to delete all the components discovered through this vCloud Director host.

If you delete the vCloud Director Host in the IP server and then triggers discover-all in the IP server. The vCloud Director components will not be deleted in ESM server, only host will be deleted.

Troubleshooting Steps

Some of the common troubleshooting steps are given below, which user must follow if discovery or monitoring is not working.

Debug flags for vCD feature (ESM.import file) in ESM

- EnableVCDDiscoveryDebug = TRUE (Default value : FALSE)
- EnableVCDMonitoringDebug = TRUE (Default value : FALSE)
- LogLevel = ALL (Default value : ERR)
- IsDebugEnabled = TRUE (Default value is FALSE)

Log file in ESM:

vCD discovery logs will be dumped in the generic INCHARGE-ESM log file under local/logs directory.

Logs in DCF

Collector logs are located at <DCF_INSTALL_LOCATION>/Collecting/Collector-Manager/<collector Id>/logs/

Enabling Debug Logs for Collector in DCF

1. Edit <DCF_INSTALL_LOCATION>/Collecting/Collector-Manager/<collector Id>/conf/logging.properties to increase log level
2. Change the default INFO level to one of – CONFIG, FINE, FINER & FINEST (lowest value).
3. The new log level takes effect in the next discovery.
4. The kafka messages can also be configured to be written to file by editing <DCF_INSTALL_LOCATION>/Collecting/Collector-Manager/<collector Id>/conf/collecting.xml. Change enabled=true for file collector
Discovery can fail due to following reasons:

**CloudController Credentials are incorrect**

Error in the log:

SAM GUI Test Credentials fails.

**DCC not responding**

Error in the log:

[April 30, 2019 4:35:46 AM EDT +968ms] t@27232000 Discovery #1

NV_MESSAGE-*--NV_GENERIC-MSG ERR : [Thread-7 DCCRestClientImpl]:Error occurred while sending a request to the DCC API Connection refused (Connection refused)

**Kafka Credentials are incorrect**

Errors in the log:

[April 30, 2019 4:43:59 AM EDT +481ms] t@2223998720 Discovery #1

NV_MESSAGE-*--NV_GENERIC-MSG ERR : [Thread-7 DiscoveryManager]:Error while starting discovery consumer thread. Timeout expired while fetching topic metadata (invalid Kafka login credentials may trigger this error)

[April 30, 2019 4:43:59 AM EDT +481ms] t@3325163264 platform

MAIN_MSG-*--STDFD_OUT-stdout: 2019-04-30 04:43:59,478 FATAL StringKafkaListenerThread-7 Kafka listener start error: Timeout expired while fetching topic metadata (invalid Kafka login credentials may trigger this error)

**Cisco ACI SDN Monitoring**

This section illustrates end to end installation and configuration of Cisco ACI SDN monitoring in Smart Assurance.
Overview

Cisco Application Centric Infrastructure (ACI) is a software-defined networking solution, which facilitates application agility and data center automation.

The entire application deployment life cycle can be simplified, optimized, and accelerated with the help of this architecture. The following diagram shows a typical Cisco ACI SDN deployment.
Discovery Flow

Smart Assurance IP Availability and Performance Manager discovers domain-specific entities related to the features of Cisco ACI SDN and creates topology objects for those features.

As a first step of discovery, Cisco ACI Controller (APIC) is discovered through the ICMP discovery. On the discovery of APIC as a Host in Smart Assurance IP Domain Manager, it communicates with the DCF controller which provisons a discovery collector. The discovery collector runs REST APIs which are required to create a topology representation in the Smart Assurance IP domain manager.

Below diagram showcases how a typical Cisco ACI topology looks like after discovery.
Monitoring Flow

When discovery completes, the domain manager creates a Monitoring Collector for each discovered Cisco ACI Control-cluster, which runs REST APIs for every polling interval. The monitoring collector essentially polls for the status and performance data of the discovered Cisco ACI topology objects. The polling interval, fetched from the polling configuration is applied to Cisco ACI in Smart Assurance IP Domain Manager.

Topology

This section provides information on specific classes, attributes, relationships, and events related to topology objects created to represent Cisco ACI.

Cisco ACI version 4.1 is supported in Smart Assurance 10.1.
Following Logical entities are created on the top of existing physical fabric:

<table>
<thead>
<tr>
<th>Class</th>
<th>Key Attributes</th>
<th>Key relationship</th>
<th>Problem and Event</th>
</tr>
</thead>
<tbody>
<tr>
<td>ControlCluster</td>
<td>IsAnyComponentDown</td>
<td>ComposedOf</td>
<td>AllComponentsDown</td>
</tr>
<tr>
<td></td>
<td>IsClusterDown</td>
<td>Manages</td>
<td>AtRisk</td>
</tr>
<tr>
<td></td>
<td>IsEveryComponentDown</td>
<td>ProvidesClientServiceTo</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>NumberOfComponent</td>
<td></td>
<td>ReducedRedundancy</td>
</tr>
<tr>
<td></td>
<td>NumberOfFaultyComponents</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ControllerNode</td>
<td>Status</td>
<td>HostedBy</td>
<td>Down</td>
</tr>
<tr>
<td></td>
<td>IsControllerDown</td>
<td>PartOf</td>
<td></td>
</tr>
<tr>
<td>Tenant</td>
<td>NumberOfEPGs</td>
<td>ClientServiceProvidedBy</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Owns</td>
<td></td>
</tr>
<tr>
<td>BridgeDomain</td>
<td>Name</td>
<td>Associates</td>
<td>None</td>
</tr>
<tr>
<td>EndPointGroup</td>
<td>Name</td>
<td>AssociatedWith</td>
<td>None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>ComposedOf</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>OwnedBy</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Uses</td>
<td></td>
</tr>
<tr>
<td>Contracts</td>
<td>Name</td>
<td>UsedBy</td>
<td>None</td>
</tr>
</tbody>
</table>

Refer VMware Smart Assurance IP Domain Manager User Guide for existing physical fabric.

The table Support of Cisco ACI Components in IP describes the components which are discovered as a part of Cisco ACI

Table 1-32. Support of Cisco ACI Components in IP

<table>
<thead>
<tr>
<th>ClassName</th>
<th>Component Name</th>
<th>Discovery</th>
<th>Monitoring</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>AggregatePort</td>
<td>Aggregate Port / Port Channel</td>
<td>YES</td>
<td>YES</td>
<td>Only AdminStatus are monitored.</td>
</tr>
<tr>
<td>BridgeDomain</td>
<td>Bridge Domain</td>
<td>YES</td>
<td>NO</td>
<td>BridgeDomains which are not associated to any EPG are not discovered.</td>
</tr>
<tr>
<td>Cable</td>
<td>Cable</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Card</td>
<td>Line Card, Supervisory Card</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Chassis</td>
<td>Chassis</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Contract</td>
<td>Contract</td>
<td>YES</td>
<td>YES</td>
<td>Contracts which are not associated to any EPG are not discovered.</td>
</tr>
<tr>
<td>ControlCluster</td>
<td>APIC Cluster</td>
<td>YES</td>
<td>NO</td>
<td>Events are raised based on ControllerNode monitoring.</td>
</tr>
<tr>
<td>ControllerNode</td>
<td>APIC</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>EndPointGroup</td>
<td>End Point Group (EPG)</td>
<td>YES</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>Fan</td>
<td>Fabric Switch Fan</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Interface</td>
<td>APIC interfaces</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>ClassName</td>
<td>Component Name</td>
<td>Discovery</td>
<td>Monitoring</td>
<td>Comments</td>
</tr>
<tr>
<td>-----------</td>
<td>--------------------------------------------</td>
<td>-----------</td>
<td>------------</td>
<td>--------------------------------------------------------------------------</td>
</tr>
<tr>
<td>IP</td>
<td>IP Address</td>
<td>YES</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>IPNetwork</td>
<td>IP Subnetwork</td>
<td>YES</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>MAC</td>
<td>MAC Address</td>
<td>YES</td>
<td>NO</td>
<td>Created only for a network Connection, but not associated to a Port.</td>
</tr>
<tr>
<td>Memory</td>
<td>Fabric Switch Memory</td>
<td>YES</td>
<td>YES</td>
<td>Only Free Memory monitored.</td>
</tr>
<tr>
<td>Partition</td>
<td>Partition</td>
<td>YES</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>Port</td>
<td>Fabric Switch Port</td>
<td>YES</td>
<td>YES</td>
<td>Port utilization, error, and discard rate are monitored along with fault monitoring.</td>
</tr>
<tr>
<td>PowerSupply</td>
<td>Fabric Switch Power supply</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Processor</td>
<td>Fabric Switch Processor</td>
<td>YES</td>
<td>NO</td>
<td>Cisco does not expose APIs to monitor Processor usage.</td>
</tr>
<tr>
<td>Switch</td>
<td>Fabric Switch (Leaf and Spine)</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>TemperatureSensor</td>
<td>Fabric Switch Temperature Sensor</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Tenant</td>
<td>Cisco ACI Tenant</td>
<td>YES</td>
<td>NO</td>
<td>Tenants which are not associated to any EPG are not discovered.</td>
</tr>
<tr>
<td>TrunkCable</td>
<td>Connection between Leaf to Spine, Leaf to Ext Switch, Spine to Ext Switch</td>
<td>YES</td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>vAggregatePort</td>
<td>Virtual Port Channel</td>
<td>YES</td>
<td>NO</td>
<td></td>
</tr>
<tr>
<td>VLAN</td>
<td>VLAN</td>
<td>YES</td>
<td>NO</td>
<td></td>
</tr>
</tbody>
</table>

**Note** Kafka_Service object is created to support fail-over as a part of discovery, for internal purposes. The fields, **DiscoveryTopic** and **Monitoring Topic** are empty and must not be populated as they have no effect on either discovery or monitoring of Cisco ACI fabric.

**Root Cause and Impact Analysis**

This section provides information on the root cause and impact analysis for newly introduced classes on top existing ones, in Smart Assurance IP Availability and Performance Manager.

The table **Events Introduced for Cisco ACI** illustrates the class, event, and the description of events.
Table 1-33. Events Introduced for Cisco ACI

<table>
<thead>
<tr>
<th>Class</th>
<th>Event</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ControlCluster</td>
<td>AtRisk</td>
<td>Indicates that the number of functioning ControllerNode components is below the AtRiskThreshold.</td>
</tr>
<tr>
<td></td>
<td>ReducedRedundancy</td>
<td>Indicates at least one ControllerNode component is not functioning but the total number of functioning components is above AtRiskThreshold.</td>
</tr>
<tr>
<td></td>
<td>Down</td>
<td>Cluster is completely down.</td>
</tr>
<tr>
<td>ControllerNode</td>
<td>Down</td>
<td>Indicates that ControllerNode is down.</td>
</tr>
<tr>
<td>EndPointGroup</td>
<td>EPGImpacted</td>
<td>EPGImpacted event is generated when a virtual machine, part of an EndPointGroup is powered off or unreachable.</td>
</tr>
<tr>
<td>Tenant</td>
<td>TenantImpacted</td>
<td>TenantImpacted event is generated when a virtual machine, part of an EndPointGroup owned by a Tenant is powered off or unreachable.</td>
</tr>
</tbody>
</table>

The Table RCA Introduced for Cisco ACI provides the details about the class, RCA event, impacted class, and the events.

Table 1-34. RCA Introduced for Cisco ACI

<table>
<thead>
<tr>
<th>Class</th>
<th>RCA Event</th>
<th>Impacted Class</th>
<th>Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>ControllerNode</td>
<td>APIServerDown</td>
<td>ControlCluster</td>
<td>AtRisk/ReducedRedundancy/ Down</td>
</tr>
</tbody>
</table>

Install and Configure

This section provides information on installation and configuration of open source and VMware Smart Assurance components.

**Note**  Perform the installation of the following VMware Smart Assurance Components prior to further configurations.

Kafka

Refer, Installing Kafka

SMARTS

Refer, Domain Manager

Data Collection Framework

Refer, Installing Data Collection Framework
Notification UI
Refer, UI Components

Configuration

Discovery of Cisco ACI
This section details the necessary configuration of the files and components in the Smart Assurance IP Availability and Performance Manager to discover Cisco ACI fabric.

For the Discovery of Cisco ACI:

- Before starting the Smart Assurance IP Availability and Performance Manager, change the value of flag DisableJAVAProbe to FALSE in the discovery.conf file.
  
  Execute the command:
  
  ```bash
  sm_edit ../conf/discovery/discovery.conf
  ```
  
  The VMware Smart Assurance System Administration Guide provides additional information about the sm_edit utility.

- Update Device Access Setting for Cisco ACI.
- Update Device Access Setting for DCF.
- Update Device Access Setting for Kafka.

Note Make the necessary changes for Cisco ACI Access Group, Kafka Bus Access Group, and Data Collector Access Group setting from the Smart Assurance IP Availability and Performance Manager directly as setting changes cannot be applied from the Configuration Manager.

Update Device Access Setting for Cisco ACI
This section describes the procedure of updating device access settings for Cisco ACI in Smart Assurance IP Availability and Performance Manager.

To update Cisco ACI in Smart Assurance IP Availability and Performance Manager:

Procedure

1. Click Device Access tab at the bottom of the Polling and Thresholds window.
2. Right Click Cisco ACI Group.
3. Copy the Cisco ACI group.
4. Give a new group name.
5. Change the priority of the new group name, so that, it appears at the top of the default Cisco ACI Group.
6. Click New Group Name.
7. Click Matching Criteria tab.
8 Select any matching criteria, so that, the setting is associated with the APIC host.

Set the matching criteria is for the first APIC host. **SNMPAddress** is the most preferred criteria considering its uniqueness.

For Example, if apic1, apic2, and apic3 are three controller nodes running in Cluster mode, provide only apic1 details in the matching criteria. To monitor multiple APIC clusters, provide matching criteria which matches the APIC host of each cluster.

Example:

```
SNMPAddress – <apic1-controlcluster1>|<apic1-controlcluster2>
```

Here, apic1-controlcluster1 is first controller node IPaddress of the APIC cluster1 and apic1-controlcluster2 is the first controller node IPAddress of the second APIC cluster.

**Note** Even though **SNMPAddress** is used for matching criteria but SNMP is not used to either discover or monitor, it is an existing attribute which has been used.

9 Expand **Cisco ACI Access Group > Settings**

10 Click **Cisco ACI Access Setting**.

11 Select **Cisco ACI device access protocol**.

Default is HTTPS.

12 Enter Hostname/IPAddress of the machine where DCF is installed.

13 Enter comma-separated Kafka Cluster Hostname/IPAddress and Port.

14 Enter Cisco ACI device user name and password.

15 Confirm the password for Cisco ACI device.

16 Enter the Cisco ACI port number.

17 Click **Apply** to apply the settings.
18  Click **Reconfigure** to complete the applied settings on the server.

---

**Update Device Access Setting for DCF**

This section describes the procedure, how to update device access settings for DCF in Smart Assurance IP Availability and Performance Manager.

To update device access setting for DCF in Smart Assurance IP Availability and Performance Manager:
Prerequisites

DCF 10.1 must be installed.

Refer Installing Data Collection Framework.

Procedure

1. Click Device Access tab at the bottom of Polling and Thresholds window.
2. Expand Data Collector Access Group > Settings.
3. Click Data Collector Access Setting.
5. Enter Hostname/IPAddress of the machine where DCF is installed.
6. Enter username and password for DCF.
7. Confirm password for DCF.
8. Enter Port number for DCF.
   Default port is 8443
9. Click Apply to apply the settings.
10. Click Reconfigure to complete the configuration on the server.

Update Device Access Setting for Kafka

This section illustrates the procedure of updating device access settings for kafka in Smart Assurance IP Availability and Performance Manager.

To configure Device Access Settings for Kafka in Smart Assurance IP Availability and Performance Manager:
Prerequisites

- 3 node Kafka Cluster must be up and running.
- Kafka Cluster must have SASL/PLAINTEXT authentication enabled.
  Refer [Kafka Setup](#) for more information.

Procedure

1. Click **Device Access tab** at the bottom of **Polling and Thresholds** window.
2. Expand **Kafka Bus Access Group > Settings**.
3. Click **Kafka Access Setting**.
4. Enter comma separated Kafka Cluster Hostname/IPAddress and Port.
5. Enter username and password for Kafka.
6. Confirm password for Kafka.
7. Enter any name for Discovery topic.
   Default is dctopo.
8. Enter any name for Monitoring topic.
   Default is dcfmon.
9. Click **Apply** to apply the settings.
10. Click **Reconfigure** to accept the configuration on the server.

Discover Cisco ACI Fabric

This Section describes the discovery of Cisco ACI fabric.
Cisco ACI fabric can be discovered in the following three ways:

- **Discover Cisco ACI Using GUI**
- **Discover Cisco ACI using sm_tpmgr Command Line Interface**
- **Discover Cisco ACI using Seed File**

**Discover Cisco ACI Using GUI**

To discover Cisco ACI fabric using Domain Manager Administration Console, follow the procedure:

**Procedure**

1. Click **Topology** in Domain Manager Administration Console.
2. Select **Add agent**.
3 Enter IPAddress or Hostname of the Cisco ACI APIC host.

4 Click **Advanced Options** check box.

5 Select Access Mode as **REST**.

6 Click **OK**.

**Discover Cisco ACI using sm_tpmgr Command Line Interface**

To discover Cisco ACI fabric using `sm_tpmgr` command-line interface, run the command:

```
<IP Install Dir>/IP/smarts/bin/sm_tpmgr -b <Broker:Port> -s <Server Name> --add-agent=<Cisco ACI IP/Hostname> --source_type=TM_REST --snmp_mode=TM_NONSNMP
```

**Discover Cisco ACI using Seed File**

The format of the seed file for Cisco ACI fabric discovery must be:

```
<Cisco ACI ControllerNode IP/Hostname> SNMPSTATE=TM_NONSNMP SOURCETYPE=TM_REST ACCESSMODE=ICMPONLY
```

**Example**

```
10.106.124.155 SNMPSTATE=TM_NONSNMP SOURCETYPE=TM_REST ACCESSMODE=ICMPONLY
```

Refer *VMware Smart Assurance IP Manager User Guide* for further details about discovery using seed file.

**Deleting an Unused Collector from DCF**

This section describes how to delete an unused collector from DCF. To enable logs for a particular collector used for discovery/monitoring in DCF, first find the corresponding collector IDs.

If any Cisco ACI fabric is monitored and the Smart Assurance IP service is restarted with **--norestore** option, it is essential to delete the corresponding collectors in DCF manually. For every discovered Cisco ACI fabric, two collectors are created, run the following command to obtain information about them:

```
dmctl -s <domain name> -b <broker> invoke ICF_PersistentDataSet::ACICollectorIDs get
```

Once the Collector IDs are obtained, delete monitoring and discovery collectors using the command:

```
```

**Example**

```
curl -k --user admin:changeme -X DELETE -H 'Content-Type: application/json' https://127.0.0.1:8443/dcc/v1/catalog/blocks/cisco-aci01201478-f531-49d1-9479-0570069b5186
```
Deleting a Cisco ACI Controller

This section describes how to delete a Cisco ACI Controller and its components.

Perform these steps in Smart Assurance IP Availability and Performance Manager to delete Cisco ACI controller and its components:

**Procedure**

1. Right-click **ControlCluster** instance.
2. Click **Delete**.

Polling and Threshold

Polling of Cisco ACI Devices

A new polling group “ACI Polling Groups” has been introduced in Smart Assurance IP Availability and Performance Manager to poll Cisco ACI devices.

To change the polling interval for Cisco ACI devices, perform these steps:

**Procedure**

1. Click **Polling** tab at the bottom of the **Polling and Thresholds** window.
2. Expand **ACI Polling Groups > Control Cluster > Settings**.
3. Click **Polling Setting for Cisco ACI**.
4. Set a value for the new polling interval on the right side window.
   
   Default value is 240 seconds.
5. Click **Apply** to apply the changes.
6. Click **Reconfigure** to complete the applied settings on the IP server.

**Note**  All components which are discovered through Cisco APIC controllers, like ControllerNodes, Fabric Switch and its components use the polling interval, defined by ACI Polling Groups. However, for threshold existing settings are used. Example, for Fabric Switch, regular Switch thresholds are applied.
Troubleshooting Steps

This section describes about some common troubleshooting steps, which user can follow in case either discovery or monitoring feature for Cisco ACI SDN is not working as expected.

**Troubleshooting Cisco ACI Discovery and Monitoring feature:**

Domain Manager logs are located at $INSTALL_DIR/smarts/local/logs

**Enable Discovery and Monitoring logs in Smart Assurance IP Availability and Performance Manager:**

Run `dmctl <domain name> -b <broker> put ICF_TopologyManager::ICF-TopologyManager::DebugEnabled TRUE`

Run `dmctl -s <domain name> -b <broker> invoke ICF_TopologyManager::ICF-TopologyManager insertParameter DebugReconfigure TRUE`

**Enable Debug Logs for DCF Collectors**

**DCF Collector (Discovery & Monitoring)**

To enable logs for a particular Collector used for discover/monitoring in DCF, first get the corresponding collector ID.

To get Collector Id:

Run `dmctl -s <domain name> -b <broker> invoke ICF_PersistentDataSet::ACICollectorIDs get`

The above command returns two entries for each ACI. ACI Controller is associated to two Collectors, one is for discovery and another one is for monitoring, output of the command indicates the same.
Steps to enable logs:

1. To increase the log level, edit `/opt/DCF/Collecting/Collector-Manager/<collector Id>/conf/logging.properties`
2. Change the default INFO level to one of – CONFIG, FINE, FINER & FINEST (lowest value).
3. The new log level takes effect in the next discovery/monitoring cycle.

**Enable file connector logs for a collector:**

Edit `/opt/DCF/Collecting/Collector-Manager/<collector Id>/conf/collecting.xml`. Change `enabled=true` for the file collector.

```xml
<connector enabled="true" name="File" type="File-Connector" config="Collector-Manager/<collector Id>/conf/file-connector.xml"/>
```

Following table describes some common reasons for Cisco ACI fabric discovery failure.

<table>
<thead>
<tr>
<th>Comment</th>
<th>Description</th>
<th>Troubleshooting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kafka consumer has failed!</td>
<td>The Kafka cluster is not configured correctly.</td>
<td>Refer to Troubleshooting Methodologies -1</td>
</tr>
<tr>
<td>Cannot find Matching kafka Broker Settings.</td>
<td>The Kafka cluster is configured in Cisco ACI Access setting does not have a corresponding Kafka Bus Access setting.</td>
<td>Refer to Troubleshooting Methodologies -2</td>
</tr>
<tr>
<td>Cannot find Matching DCC Settings.</td>
<td>The Data Collector is configured in Cisco ACI Access setting does not have a corresponding Data Collector Access setting.</td>
<td>Refer to Troubleshooting Methodologies -2</td>
</tr>
<tr>
<td>Timeout - Messages not received from DCF.</td>
<td>The Data Collector does not push the Messages consistently.</td>
<td>Refer to Troubleshooting Methodologies -3</td>
</tr>
<tr>
<td>Not able to connect to Cisco ACI Controller.</td>
<td>HTTP Connection with Cisco ACI Controller is not properly established.</td>
<td>Refer to Troubleshooting Methodologies -4</td>
</tr>
<tr>
<td>Controller Failed to create block for [apicIp/Name].</td>
<td>The Collection block in Data Collector cannot be created.</td>
<td>Refer to Troubleshooting Methodologies -5</td>
</tr>
<tr>
<td>Controller Failed to getConfig for Collector instance [apicIp/Name].</td>
<td>The configurations of a collection block in Data Collector cannot be fetched.</td>
<td>Refer to Troubleshooting Methodologies -5</td>
</tr>
<tr>
<td>Controller Failed to set configurations for [apicIp/Name].</td>
<td>The configurations of a collection block in Data Collector cannot be set.</td>
<td>Refer to Troubleshooting Methodologies -5</td>
</tr>
</tbody>
</table>

**Troubleshooting Methodologies -1**

If the error message “Discovery Error [kafka consumer has failed!]” appears during discovery:

- Check kafka credentials and port details.
- Check if the kafka process is running on the server.
- Check if kafka topic name is configured.
Troubleshooting Methodologies -2
If the error message "Cannot find Matching kafka Broker Settings" appears during discovery:

- Check Device Access Setting for the Cisco ACI kafka Broker detail matches with the Device Access Setting for kafka Broker detail.

If the error message "Cannot find Matching DCC Settings" appears during discovery:

- Check Device Access Setting for Cisco ACI Data Collector address detail matches with Device Access Setting for Data Collector Access Setting Hostname detail.

Troubleshooting Methodologies -3
In case discovery fails with the error message “Timeout - Messages not received from DCF”:

- Check if the DCF collector corresponding to this discovery has started.
  - A quick way is to check the timestamp of the discovery failure message and then comparing it with last update in the logs of the corresponding collector.
- In case the collector does not start, contact to Smart Assurance Support.

Troubleshooting Methodologies -4
In case discovery fails with the error message “Not able to connect to Cisco ACI Controller”:

- Check if all the information provided in Cisco ACI Device Access settings is proper. Generally, incorrect Cisco ACI port or username/password is the reason.

Troubleshooting Methodologies -5
In case the discovery fails with error message “Controller Failed”:

- Retry discovery as it mostly causes due to a huge number of requests sent to DCF, in case the issue persists contact Smart Assurance support.

vROps Alerts Subscription

This chapter describes about the collection of alert notifications from vRealize Operations into VMware Smart Assurance.

SAM Configuration

You can configure SAM (Service Assurance Manager), to get alert notifications from vRealize Operations.

To get vROPS alerts in SAM, follow the procedure:

Prerequisites

Install and configure the vROPS alerts collector, refer VMware Smart Assurance UI Platform User and Configuration Guide, chapter VMware vROPs Alerts collector.
Procedure

   
   a. Set `EnableKafkaSubscription` to `TRUE`.
   
   b. Set `BrokerInfo` to `<KAFKA BROKER IP>:<KAFKA BROKER PORT>`.
   
   c. Set `Topic` to the topic that was configured in the vROPS alerts collector. For example, topic name can be `vrops-alerts`.

2. Type the following command to go to bin directory:
   ```
   cd /opt/InCharge/SAM/smarts/bin
   ```

   
   a. Add the following line just before the admin password:
   ```
   kafka:<kafka broker ip>:<Kafka admin user>:<Kafka admin password
   ```
   
   b. Restart OI server.

   **Note** The OI server automatically connects to Kafka, if `EnableKafkaSubscription` is set to `TRUE`. 
Core Platform

This section describes steps to install and configure each core platform components.

This chapter includes the following topics:

- Data Store
- Messaging
- Data Management
- Domain Manager
- UI Components

Data Store

Installing MongoDB

MongoDB is a cross-platform document-oriented database program. MongoDB is required for DCF and K4M. It is classified as a NoSQL database program, MongoDB uses JSON-like documents with schemata. MongoDB is developed by MongoDB Inc.

You can install MongoDB in the following three ways:

1. Use MongoDB documentation to install the MongoDB.
2. Use MongoDB install script to install MongoDB, which has below procedure automated in the script. You can refer KB article from https://kb.vmware.com/s/article/70718 to download the script.
3. Use below manual procedure to install MongoDB.

Procedure

1. Stop firewall on the server where MongoDB will be installed or open port 27017.
Create a file `/etc/yum.repos.d/mongodb-org-4.0.repo` with the following content:

```
[mongodb-org-4.0]
name=MongoDB Repository
baseurl=https://repo.mongodb.org/yum/redhat/$releasever/mongodb-org/4.0/x86_64/
gpgcheck=1
enabled=1
gpgkey=https://www.mongodb.org/static/pgp/server-4.0.asc
```

Install MongoDB, by invoking the command:

```
yum install -y mongodb-org-4.0.4 mongodb-org-server-4.0.4 mongodb-org-shell-4.0.4
mongodb-org-mongos-4.0.4 mongodb-org-tools-4.0.4
```

Start MongoDB service:

```
service mongod start
```

Create first user in MongoDB, by invoking the command:

```
mongo admin --eval 'db.createUser({user: "admin",pwd: "changeme",roles: [ { role: "root", db: "admin" } ]})'
```

Enable authentication in MongoDB, by invoking the command:

```
vi /etc/mongod.conf
security:
  authorization: "enabled"
```

Restart MongoDB, by invoking command:

```
service mongod restart
```

## Installing Redis

This section describes how to deploy three node Redis Cache 5.0.5 Cluster Deployment. Execute all the steps in each node to install Redis Cache in cluster mode. Redis Cluster setup require atleas three primary nodes.

Redis Cluster becomes nonoperational if any one redis primary process goes down. For primary failover, additional 3 redis replica processes can be configured.

You can install Redis in the following three ways:

1. Use Redis documentation to install Redis.
2. Use Redis install script to install Redis, which has below procedure automated in the script.
   You can refer KB article from [https://kb.vmware.com/s/article/70718](https://kb.vmware.com/s/article/70718).
3. Use below manual procedure to install Redis.

**Procedure**

1. Stop firewall on all 3 nodes or open ports 6379, 16379, 6380 and 16380 on all 3 nodes.
2 Set the system configuration parameters by executing below commands:
   a echo 'sysctl -w net.core.somaxconn=65535' >> /etc/rc.local
   b sysctl -w net.core.somaxconn=65535
   c echo never > /sys/kernel/mm/transparent_hugepage/enabled
   d echo 'echo never > /sys/kernel/mm/transparent_hugepage/enabled' >> /etc/rc.local
   e chmod +x /etc/rc.local
   f echo 'vm.overcommit_memory = 1' >> /etc/sysctl.conf
   g sysctl vm.overcommit_memory=1

3 Install Epel-Release, by invoking below command:
     -- for RHEL 7.5 or 7.6
     -- for RHEL 6.9, 6.10

4 Install Yum utilities, by invoking below command:
   yum install -y yum-utils

5 Install Remi release, by using below commands:
   - yum install -y http://rpms.remirepo.net/enterprise/remi-release-7.rpm
     -- for RHEL 7.5 or 7.6
   - yum install -y http://rpms.remirepo.net/enterprise/remi-release-6.rpm
     -- for RHEL 6.9, 6.10

6 Enable Remi, using below command:
   yum-config-manager --enable remi

7 Install Redis, by invoking below command:
   yum install -y redis

8 Verify the Redis version is 5.0.5, by using below command:
   redis-server --version

9 Copy redis.conf under /etc directory as redis-6379.conf, by using below command:
   cp /etc/redis.conf /etc/redis-6379.conf

10 Change Owner of /etc/redis-6379.conf to redis, by using below command:
    chown redis:root /etc/redis-6379.conf

11 Edit /etc/redis-6379.conf file with below configurations:
   a Change "bind 127.0.0.1" to "bind <IPAddress>"
b Change "port 6379" to "port 6379"

c Change 'logfile "'' to 'logfile /var/log/redis/redis-6379.log'

d Change "dbfilename dump.rdb" to "dbfilename dump-6379.rdb"

e Change '# cluster-enabled yes' to 'cluster-enabled yes'

f Change '# cluster-config-file nodes-6379.conf' to 'cluster-config-file redis-6379.conf'

g Change '# cluster-node-timeout 15000' to 'cluster-node-timeout 5000'

h Change '#requirepass' to 'requirepass <password>'

i Change '# masterauth <master-password>' to 'masterauth <password>'

**Note** Password for masterauth must be same as requirepass.

---

12 For RHEL 7.5 or 7.6, create /usr/lib/systemd/system/redis-6379.service file:


b Replace 'ExecStart=/usr/bin/redis-server /etc/redis.conf --supervised systemd' with 'ExecStart=/usr/bin/redis-server /etc/redis-6379.conf --supervised systemd'

c Replace 'ExecStop=/usr/libexec/redis-shutdown' with 'ExecStop=/usr/libexec/redis-shutdown redis-6379'

For RHEL 6.9 or 6.10, create /etc/init.d/redis-6379 service file:

a Copy /etc/init.d/redis to /etc/init.d/redis-6379 and, edit /etc/init.d/redis-6379 file.

b Replace 'shut="/usr/libexec/redis-shutdown"' with 'shut="/usr/libexec/redis-shutdown redis-6379"

c Replace 'pidfile="/var/run/redis/redis.pid"' with 'pidfile="/var/run/redis/redis-6379.pid"'

d Replace 'REDIS_CONFIG="/etc/redis.conf"' with 'REDIS_CONFIG="/etc/redis-6379.conf"

e Replace '[[ -e /etc/sysconfig/redis ] && . /etc/sysconfig/redis' with '[[ -e /etc/sysconfig/redis-6379 ] && . /etc/sysconfig/redis-6379'

f Replace 'lockfile=/var/lock/subsys/redis' with 'lockfile=/var/lock/subsys/redis-6379'

g Replace '[[ -x $shut ] && $shut' with '$shut'

13 Enable the service:

- For RHEL 7.5 or 7.6 command is: systemctl enable redis-6379
For RHEL 6.9 or 6.10 command is:

```
chkconfig --add redis-6379
chkconfig redis-6379 on
```

14 Start the service:

- For RHEL 7.5 or 7.6 command is: `systemctl start redis-6379`
- For RHEL 6.9 or 6.10 command is: `service redis-6379 start`

15 Verify service status:

- For RHEL 7.5 or 7.6 command is: `systemctl status redis-6379` (service should be running)
- For RHEL 6.9 or 6.10 command is: `service redis-6379 status` (service should be running)

16 Check the redis logs `/var/log/redis/redis-6379.log`. The log must contains "Ready to accept connections".

17 Execute step 1 to 15 on all 3 cluster nodes.

18 Create redis cluster without replication by executing below command from any one cluster node:

```
redis-cli -a <password> --cluster create <IP1>:6379 <IP2>:6379 <IP3>:6379
```

Enter "Yes" when prompted
Expected output: "[OK] All 16384 slots covered."

19 Validate Redis cluster by running below command:

```
redis-cli -a <password> -h <IP> -p 6379 cluster nodes
```

Output: Should show all primary nodes

What to do next

You must create atleast 1 replica for each primary for failover.

Creating Replica for Each Primary Node for Failover

It is important to create atleast 1 replica for each Redis primary node for failover. Execute all steps on all 3 cluster nodes to create one replica for each primary node.

Procedure

1 Copy redis.conf file under /etc directory as redis-6380.conf, by invoking below command:

```
cp /etc/redis.conf /etc/redis-6380.conf
```

2 Change owner of /etc/redis-6380.conf to redis by using command:

```
chown redis:root /etc/redis-6380.conf
```
3 Edit /etc/redis/redis-6380.conf file with below configurations:
   a Change "bind 127.0.0.1" to "bind <IPAddress>"
   b Change "port 6379" to "port 6380"
   c Change 'logfile /var/log/redis/redis.log' to 'logfile /var/log/redis/redis-6380.log'
   d Change "dbfilename dump.rdb" to "dbfilename dump-6380.rdb"
   e Change "pidfile /var/run/redis_6379.pid" to "pidfile /var/run/redis_6380.pid". Change only in RHEL 7.5 or 7.6.
   f Change '# cluster-enabled yes' to 'cluster-enabled yes'
   g Change '# cluster-config-file nodes-6379.conf' to 'cluster-config-file redis-6380.conf'
   h Change '# cluster-node-timeout 15000' to 'cluster-node-timeout 5000'
   i Change 'requirepass' to 'requirepass <password>'
   j Change '# masterauth <master-password>' to 'masterauth <password>'

4 For RHEL 7.5 or 7.6, create /usr/lib/systemd/system/redis-6380.service file:
   b Replace 'ExecStart=/usr/bin/redis-server /etc/redis.conf --supervised systemd' with 'ExecStart=/usr/bin/redis-server /etc/redis-6380.conf --supervised systemd'
   c Replace 'ExecStop=/usr/libexec/redis-shutdown' with 'ExecStop=/usr/libexec/redis-shutdown redis-6380'

For RHEL 6.9 or 6.10, create /etc/init.d/redis-6380 service file:
   a Copy /etc/init.d/redis to /etc/init.d/redis-6380 and, edit /etc/init.d/redis-6380 file
   b Replace 'shut="/usr/libexec/redis-shutdown"' with 'shut="/usr/libexec/redis-shutdown redis-6380"
   c Replace 'pidfile="/var/run/redis/redis.pid"' with 'pidfile="/var/run/redis/redis-6380.pid"
   d Replace 'REDIS_CONFIG="/etc/redis.conf"' with 'REDIS_CONFIG="/etc/redis-6380.conf"
   f Replace 'lockfile=/var/lock/subsys/redis' with 'lockfile=/var/lock/subsys/redis'
g Replace `'[ -x $shut ] && $shut'` with `'$shut'

5 Enable the service:

- For RHEL 7.5 or 7.6 command is: `systemctl enable redis-6379`
- For RHEL 6.9 or 6.10 command is:
  
  ```
  chkconfig --add redis-6379
  chkconfig redis-6379 on
  ```

6 Start the service:

- For RHEL 7.5 or 7.6 command is: `systemctl start redis-6379`
- For RHEL 6.9 or 6.10 command is: `service redis-6379 start`

7 Verify service status:

- For RHEL 7.5 or 7.6 command is: `systemctl status redis-6379` (service should be running)
- For RHEL 6.9 or 6.10 command is: `service redis-6379 status` (service should be running)

8 Check the redis logs `/var/log/redis/redis-6379.log`. The log must contains "Ready to accept connections".

9 Execute step 1 to 8 on all 3 cluster nodes.

10 Add each redis process running on 6380 port as replicas to each primary running on 6379 port, by using commands:

  ```
  redis-cli -a <password> --cluster add-node <IP2>:6380 <IP1>:6379 --cluster-slave
  redis-cli -a <password> --cluster add-node <IP3>:6380 <IP2>:6379 --cluster-slave
  redis-cli -a <password> --cluster add-node <IP1>:6380 <IP3>:6379 --cluster-slave
  ```

  **Note** Before executing above command, ensure that steps 1-9 are executed on each node in the cluster. Above commands can be executed from any one cluster node.

  Expected output after executing each command:

  `[OK] New node added correctly`.  

11 Validate redis primary and replication nodes by running below command:

  ```
  redis-cli -a <password> --cluster nodes -h <IP> -p 6379
  ```

  **Output:** Must show both the primary and secondary nodes along with primary to secondary mapping information.

  Other useful commands:

  a Command to list all keys in redis cluster: `redis-cli -a <password> --cluster nodes -h <IP1/IP2/IP3> -p <6379/6380> keys "*"`
b Command to see content/value of any particular keys: `redis-cli -a <password> -h <IP1/IP2/IP3> -p <6379/6380> HGETALL "key"

c Command to reset redis cluster:

```
redis-cli -a <password> -h <IP1/IP2/IP3> -p <6379/6380>
IP:Port> flushall
IP:Port> cluster reset
IP:Port> exit
```

## Installing Elastic Search

This section provides information on how to deploy three node Elastic Search cluster. Execute all the steps in each node to install elastic search in cluster mode.

You can install Elastic Search in the following three ways:

1. Use Elastic Search documentation to install Elastic Search.
2. Use Elastic Search install script to install Elastic Search, which has below procedure automated in the script. You can refer KB article from [https://kb.vmware.com/s/article/70718](https://kb.vmware.com/s/article/70718).
3. Use below manual procedure to install Elastic Search.

### Procedure

1. Stop firewall on all 3 nodes or open ports 9200 and 9300 on all 3 nodes.
2. Verify Java 1.8, by invoking command:
   ```
yum install -y java-1.8.0-openjdk.x86_64
   ```
   If not installed, install java 1.8.
3. If operating system is RHEL 6.9 or 6.10, then edit `/etc/security/limits.d/90-nproc.conf` file:
   ```
   Change "* soft nproc 1024" to "* soft nproc 4096"
   ```
   Save and close the file.
4. Download elastic search 6.4.2 rpm from [https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-oss-6.4.2.rpm](https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-oss-6.4.2.rpm) and install it using command:
   ```
rpm -ivh elasticsearch-oss-6.4.2.rpm
   ```
5. Run below command to search for elastic search rpm:
   ```
rpm -qa | grep elasticsearch
   ```
6. Run below command to enable elasticsearch service in RHEL 7.5 or 7.6:
   ```
   systemctl enable elasticsearch
   ```
   Run below command to enable elasticsearch service in RHEL 6.9 or 6.10:
   ```
   chkconfig --add elasticsearch
   chkconfig elasticsearch on
   ```
7 Download Readonlyrest Elastic Search plugin from the given link to enable security (Authentication) in Elastic Search – https://readonlyrest.com/download/

**Note** On the download page, select Product as "Elastic Search Plugin (Free)", Elastic Search Version as "6.4.2" and Send to email as "Your email". A link to the latest readonlyrest plugin will be sent to your inbox from which you can download the zip file.

8 Install the plugin using below command:

```
/usr/share/elasticsearch/bin/elasticsearch-plugin install file:///path to downloaded zip file>
```

For example: /usr/share/elasticsearch/bin/elasticsearch-plugin install file:///root/readonlyrest-1.16.28_es6.4.2.zip

**Note** Press 'y' when prompted to "continue with installation'

9 List all installed plugins, using command:

```
/usr/share/elasticsearch/bin/elasticsearch-plugin list
```

Create a new file "readonlyrest.yml" under /etc/elasticsearch with below contents:

```yaml
readonlyrest:
  access_control_rules:
  - name: Accept GET,POST requests from user
    auth_key_unix: Test:$6$rounds=65635$koKsfnc$4iZfsaq9mzYcRMSXy1Da2T/mPWhh/WWnqI7lm.2hdXC1x5cVJJY8NiSNrRUXPc5F8x5VYGvs70RVzAayJexq/
```

**Note**

a Ensure the indentation while creating readonlyrest.yml file is maintained as shown above.

b The above readonlyrest.yml content will create a user with name "test" and password "test".


10 Edit /etc/elasticsearch/elasticsearch.yml file:

a Change "#cluster.name: my-application" to "cluster.name: <YourClusterName>"

**Note** Ensure <YourClusterName> is same across all 3 nodes.

b Change "#node.name: node-1" to "node.name: <FQDN>"

**Note** node.name must be unique accross the cluster.

c Add below two lines after line "#node.attr.rack: r1":

```yaml
node.master: true
node.data: true
```
d. Change "#network.host: to network.host: _local_, _site_

e. Change "#http.port: 9200" to "http.port: <port number>". This step is optional and required if you want to start elastic search on any other port other than 9200.

f. Change "#discovery.zen.ping.unicast.hosts: ['host1', 'host2']" to "discovery.zen.ping.unicast.hosts: ['<FQDN/IP Of Host1>', '<FQDN/IP Of Host2>']"

g. Change "discovery.zen.minimum_master_nodes:2" to "discovery.zen.minimum_master_nodes: 2"

h. Add a new line "bootstrap.system_call_filter: false" if operating system is Linux 6.9 or 6.10.

i. Save and close the file.

11 Edit /etc/elasticsearch/jvm.options. (Optional: If needed to increase java heap size. By default 1 GB heap space is allocated to ES):

   a. Change "-Xms1g" to "-Xms2g".

   b. Change "-Xmx1g" to "-Xmx2g"

12 Start Elastic Search Service after executing steps from 1-11 on all 3 hosts.

13 Verify Elastic Search Service status and it must be running on all 3 machines.

14 Validate successful Elastic Search Cluster setup by executing below commands:

   a. curl -u username:password http://<ES FQDN/IP>:9200/ (The output must contain version as 6.4.2 and clustername as set in elasticsearch.yml file).


15 Enable HTTPS in Elastic Search (Optional):

   a. Run cd /etc/elasticsearch


   d. Edit /etc/elasticsearch/readonlyrest.yml file and add below line:

        ssl:
        keystore_file: "keystore.jks"
        keystore_pass: readonlyrest
        key_pass: readonlyrest

   e. Restart Elastic Search service.
Other useful commands:

Get all indices in ES:
```
```

Delete all data events indices:
```
curl -u user:password -X DELETE http://<ES FQDN/IP>:9200/events
```

Cluster Health:
```
curl -u user:password http://<ES FQDN/IP>:9200/_cluster/health
```

Monitor shard sizes:
```
curl -u user:password http://<ES FQDN/IP>:9200/_cat/shards
```

### Messaging

#### Installing Kafka

Apache Kafka is publish-subscribe based fault tolerant messaging system. It is fast, scalable and distributed by design.

You can install Kafka in the following three ways:

1. Use Kafka documentation to install the Kafka.
2. Use Kafka install script to install Kafka, which has below procedure automated in the script. You can refer KB article from [https://kb.vmware.com/s/article/70718](https://kb.vmware.com/s/article/70718) to download the script.
3. Use below manual procedure to install Kafka.

#### Pre-Install Steps

You need to follow the pre-install steps to install Kafka.

**Procedure**

1. Stop firewall on all 3 nodes or open ports 2181, 3181, 4181 and 9092 on all 3 nodes.
2. Check for java 1.8. If not installed, install java 1.8:
   ```
   yum install -y java-1.8.0-openjdk.x86_64
   ```
3. Download Kafka 2.0.0 from [https://archive.apache.org/dist/kafka/2.0.0/kafka_2.11-2.0.0.tar.gz](https://archive.apache.org/dist/kafka/2.0.0/kafka_2.11-2.0.0.tar.gz), to any directory (for example /root or /opt)
4. Run below command to untar and deploy Kafka:
   ```
   tar -xvf kafka_2.11-2.0.0.tar.gz
   ```

#### Zookeeper Setup
Procedure

1. Create a file `/var/zookeeper/myid` on each cluster node with unique value (for example 1,2,3) on each node.

   ```bash
   mkdir -p /var/zookeeper
   echo "1" > /var/zookeeper/myid
   ```

2. Edit `zookeeper.properties` file under `<KAFKA_HOME>/config` directory.

   ```properties
   dataDir=/var/zookeeper
   clientPort=2181
   maxClientCnxns=0
   tickTime=2000
   initLimit=5
   syncLimit=10
   dataLogDir=/var/log/zookeeper
   server.1=<KAFKA_CLUSTER_HOST1_IPADDRESS>:3181:4181
   server.2=<KAFKA_CLUSTER_HOST2_IPADDRESS>:3181:4181
   server.3=<KAFKA_CLUSTER_HOST3_IPADDRESS>:3181:4181
   authProvider.1=org.apache.zookeeper.server.auth.SASLAuthenticationProvider
   authProvider.2=org.apache.zookeeper.server.auth.SASLAuthenticationProvider
   authProvider.3=org.apache.zookeeper.server.auth.SASLAuthenticationProvider
   requireClientAuthScheme=sasl
   ```

   **Note** 2181 is the port on which Zookeeper will listen for connections. Instead of 3181 and 4181, any port number can be used, but ensure same ports are used across all 3 nodes.

3. Create a new `zookeeper_jaas.conf` file under `<KAFKA_HOME>/config` directory with below content:

   ```properties
   Server {
   org.apache.zookeeper.server.auth.DigestLoginModule required
   user_super="zookeeper"
   user_kafka="zoo-pwd";
   }
   ```

   **Note** The file `zookeeper_jaas.conf` is used for authentication.

   **Note** `user_super`: superuser will have automatically administrator privileges.

   **Note** `user_kafka`: kafka is the username and password is zoo-pwd. The user kafka and password can be anything.

4. Start Zookeeper server by running below command:

   ```bash
   KAFKA_OPTS="-Djava.security.auth.login.config <KAFKA_HOME>/config/zookeeper_jaas.conf" <KAFKA_HOME>/bin/zookeeper-server-start.sh -daemon <KAFKA_HOME>/config/zookeeper.properties
   ```
5 Check the status of Zookeeper service by running any the below command:

   a. `ps -aef | grep zookeeper` or `ps -aef | grep zookeeper.properties`
   b. `lsof -i:2181`
   c. `netstat -tnlup | grep 2181`

Kafka Setup

Three Node Kafka cluster deployment. Execute all below steps in each node to install Kafka in cluster mode.

Procedure

1 Edit `server.properties` file under `<KAFKA_HOME>/config` directory.

   ```
   broker.id=1
   delete.topic.enable=true
   auto.create.topics.enable=true
   default.replication.factor=3
   security.inter.broker.protocol=SASL_PLAINTEXT
   sasl.mechanism.inter.broker.protocol=PLAIN
   sasl.enabled.mechanisms=PLAIN
   authorizer.class.name=kafka.security.auth.SimpleAclAuthorizer
   allow.everyone.if.no.acl.found=true
   listeners=SASL_PLAINTEXT://<KAFKA_CLUSTER_HOST1_IPADDRESS>:9092
   advertised.listeners=SASL_PLAINTEXT://<KAFKA_CLUSTER_HOST1_IPADDRESS>:9092
   zookeeper.connect=<KAFKA_CLUSTER_HOST1_IPADDRESS>:2181,<KAFKA_CLUSTER_HOST2_IPADDRESS>:2181,<KAFKA_CLUSTER_HOST3_IPADDRESS>:2181
   ```

   **Note**  broker.id value should be unique across all cluster nodes. And, 9092 is Kafka broker/server port and can be anything.

2 Create a new `kafka_server_jaas.conf` file under `<KAFKA_HOME>/config` directory with below content.

   ```
   KafkaServer {
   org.apache.kafka.common.security.plain.PlainLoginModule required
   username="kafkaadmin"
   password="kafka-pwd"
   user_kafkaadmin="kafka-pwd";
   };
   Client {
   org.apache.zookeeper.server.auth.DigestLoginModule required
   username="kafka"
   password="zoo-pwd";
   }
   ```

   a The file `kafka_server_jaas.conf` is used for authentication.
   b username="kafkaadmin": kafkaadmin is the username and can be any username.
   c password="kafka-pwd": kafka-pwd is the password and can be any password.
d Both username="kafkaadmin" and password="kafka-pwd" is used for inter broker communication.

e user_kafkaadmin="kafka-pwd": kafkaadmin and kafka-pwd are username and passwords used for server client communication and can be anything.

f Under Client section, the username="kafka" and password="zoo-pwd" should match username and password provided in zookeeper_jaas.conf file.

3 Edit consumer.properties file under <KAFKA_HOME>/config directory and the following configurations.

```
security.protocol=SASL_PLAINTEXT
sasl.mechanism=PLAIN
```

4 Edit producer.properties file under <KAFKA_HOME>/config directory and the following configurations.

```
security.protocol=SASL_PLAINTEXT
sasl.mechanism=PLAIN
bootstrap.servers=<KAFKA_CLUSTER_HOST1_IPADDRESS>:9092,<KAFKA_CLUSTER_HOST2_IPADDRESS>:9092,<KAFKA_CLUSTER_HOST3_IPADDRESS>:9092
compression.type=none
```

5 Create a new kafka_client_jaas.conf file under <KAFKA_HOME>/config directory with below content.

```
KafkaClient {
    org.apache.kafka.common.security.plain.PlainLoginModule required
    username="kafkaadmin"
    password="kafka-pwd";
};
Client {
    org.apache.zookeeper.server.auth.DigestLoginModule required
    username="kafka"
    password="zoo-pwd";
};
```

a Under KafkaClient section, the username="kafkaadmin" and password="kafka-pwd" should match username and password provided in kafka_server_jaas.conf file.

b Under Client section, the username="kafka" and password="zoo-pwd" should match username and password provided in zookeeper_jaas.conf file.

6 Start Kafka broker by running below command:

```
KAFKA_OPTS="-Djava.security.auth.login.config=<KAFKA_HOME>/config/kafka_server_jaas.conf" <KAFKA_HOME>/bin/kafka-server-start.sh -daemon <KAFKA_HOME>/config/server.properties
```

7 Check the status of kafka broker service by running any one of below 3 commands:

- `ps -aef | grep -v zookeeper | grep kafka` or `ps -aef | grep server.properties`
- lsof -i:9092
- netstat -tnlup | grep 9092

8 Create a topic after executing steps from 1 to 7 on all 3 cluster nodes. The command to create topic can be executed from any one cluster node.

<KAFKA_HOME>/bin/kafka-topics.sh --create --zookeeper <KAFKA_CLUSTER_HOST1_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST2_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST3_IPADDRESS>:2181 --replication-factor 3 --partitions 1 --topic <Topic Name>

   a The value for --replication-factor should be equal to number of nodes in the cluster.
   b At present, only 1 partition is supported per topic.

9 Command to list/verify topic:

<KAFKA_HOME>/bin/kafka-topics.sh --list --zookeeper <KAFKA_CLUSTER_HOST1_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST2_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST3_IPADDRESS>:2181

10 Command to start consumer and attach to topic. This command should be used only for debugging purpose to read the content of the topic from beginning. The output can be redirected to a file.

<KAFKA_HOME>/bin/kafka-console-consumer.sh --bootstrap-server <KAFKA_CLUSTER_HOST1_IPADDRESS>:9092 <KAFKA_CLUSTER_HOST2_IPADDRESS>:9092 <KAFKA_CLUSTER_HOST3_IPADDRESS>:9092 --topic <Topic Name> --from-beginning --consumer.config=<KAFKA_HOME>/config/consumer.properties

Enabling SSL In Kafka (Optional)

Procedure

1 Stop all zookeepers in the cluster.
   a Run zookeeper-server-stop.sh under <KAFKA_HOME>/bin directory to stop kafka server. If it doesn't work, then run step b & c.
   b Get the pid by running the command "netstat -tnlup | grep 2181"
   c kill -9 <pid>

2 Delete the topic by executing below command from any one cluster node (Optional):

<KAFKA_HOME>/bin/kafka-topics.sh --delete --topic <Topic Name> --zookeeper <KAFKA_CLUSTER_HOST1_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST2_IPADDRESS>:2181 <KAFKA_CLUSTER_HOST3_IPADDRESS>:2181

3 Create Kafka Keystore and Truststore on all nodes in the cluster by executing below command:
   a Create CA Cert and CA Key by executing below command on any linux machine.
openssl req -new-x509 -keyout ca-key -out ca-cert -days365-subj'/CN=<fqdn>''-extensions san -config <(echo'
[req]
subjectAltName = DNS:localhost, IP:127.0.0.1, DNS:<hostname>, IP:<ip-address>

[san]
subjectAltName = DNS:localhost, IP:127.0.0.1,DNS:<hostname>, IP:<ip-address>
')

b Enter the passphrase(changeit) when prompted. Make a note of this passphrase.
c Copy ca-key and ca-cert files to any location on all 3 cluster nodes.
d Create server keystore file by executing below command on all 3 cluster nodes:

```
Change directory to <KAFKA_HOME>/config
```
e Import ca-cert file into server truststore on all 3 cluster nodes by executing below command:

```
<JREHome>/bin/keytool -keystore server.truststore.jks -alias CARoot -import-file ca-cert
```
f Import ca-cert file into client truststore on all 3 cluster nodes by executing below command:

```
<JREHome>/bin/keytool -keystore client.truststore.jks -alias CARoot -import-file ca-cert
```
g Export the unsigned certificate from server keystore by executing below command on all 3 cluster nodes:

```
<JREHome>/bin/keytool -keystore server.keystore.jks -alias <alias> -certreq -file cert-file -ext SAN=DNS:<hostname>,DNS:localhost,IP:<ip-address>,IP:127.0.0.1
```
h Sign the unsigned certificate cert-file using CA certificate & key ca-cert and ca-key on all 3 cluster nodes by executing below command:

```
openssl x509 -req -extfile <(printf"subjectAltName = DNS:localhost, IP:127.0.0.1,DNS:<fqdn>, IP:<ip-address>"),CA ca-cert -CAkey ca-key -in cert-file -out cert-signed -days365-CAcreateserial -passin pass:<password>
```
i Import ca-cert file into server keystore on all 3 cluster nodes by running below command:

```
<JREHome>/bin/keytool -keystore server.keystore.jks -alias CARoot -import-file ca-cert
```
j Import signed cert file cert-signed into server keystore on all 3 cluster nodes by running below command:

```
<JREHome>/bin/keytool -keystore server.keystore.jks -alias <alias> -import-file cert-signed
```
4 Edit `server.properties` file under `<KAFKA_HOME>/config` directory and add/edit the following configurations:

```java
security.inter.broker.protocol=SASL_SSL
listeners= SASL_SSL://<KAFKA_CLUSTER_HOST_IPADDRESS>:9092
advertised.listeners=SASL_SSL://<KAFKA_CLUSTER_HOST_IPADDRESS>:9092
ssl.keystore.location=<KAFKA_HOME>/config/kafka.server.keystore.jks
ssl.keystore.password=changeit
ssl.key.password=changeit
ssl.truststore.location=<KAFKA_HOME>/config/kafka.server.truststore.jks
ssl.truststore.password=changeit
```

5 Edit `consumer.properties` file under `<KAFKA_HOME>/config` directory and add/edit the following configurations:

```java
security.protocol=SASL_SSL
sasl.mechanism=PLAIN
ssl.truststore.location=<KAFKA_HOME>/config/kafka.client.truststore.jks
ssl.truststore.password=changeit
```

6 Edit `producer.properties` file under `<KAFKA_HOME>/config` directory and add/edit the following configurations:

```java
sasl.mechanism=PLAIN
security.protocol=SASL_SSL
sasl.jaas.config=org.apache.kafka.common.security.plain.PlainLoginModule required
username="admin"
password="admin-secret";
ssl.truststore.location= <KAFKA_HOME>/config/client.truststore.jks
ssl.truststore.password=<password>
```

7 Start Kafka broker on all 3 servers.

8 Create the topic (If the topic is not deleted in step 2).

**Kafka SASL_PLAIN Authentication Configuration**

This section describes the configuration of Kafka SASL_PLAIN authentication.

**Procedure**

1 Add/Update the below files in `/KAFKA_HOME/config` directory.

a **server.properties**

```java
security.inter.broker.protocol=SASL_PLAINTEXT
sasl.mechanism.inter.broker.protocol=PLAIN
sasl.enabled.mechanisms=PLAIN
authorizer.class.name=kafka.security.auth.SimpleAclAuthorizer
allow.everyone.if.no.acl.found=true
auto.create.topics.enable=true
listeners=SASL_PLAINTEXT://<IP Address>:9092
advertised.listeners=SASL_PLAINTEXT://<IP Address>:9092
```
### Deployment Scenarios

#### b. zookeeper.properties

```properties
authProvider.1=org.apache.zookeeper.server.auth.SASLAuthenticationProvider
requireClientAuthScheme=sasl
jaasLoginRenew=3600000
```

#### c. consumer.properties

```properties
security.protocol=SASL_PLAINTEXT
sasl.mechanism=PLAIN
```

#### d. zookeeper_jaas.conf

```properties
Server {
    org.apache.zookeeper.server.auth.DigestLoginModule required
        user_super="zookeeper"
        user_admin="admin-secret";
}
```

#### e. kafka_server_jaas.conf

```properties
KafkaServer {
    org.apache.kafka.common.security.plain.PlainLoginModule required
        username="admin"
        password="admin-secret"
        user_admin="admin-secret";
}
Client {
    org.apache.zookeeper.server.auth.DigestLoginModule required
        username="admin"
        password="admin-secret";
}
```

2. Add the zookeeper_jaas.conf file to the environment variable KAFKA_OPTS before starting zookeeper.

```bash
$ export KAFKA_OPTS="-Djava.security.auth.login.config=/KAFKA_HOME/config/zookeeper_jaas.conf"
$ bin/zookeeper-server-start.sh -daemon config/zookeeper.properties
```

3. Add the kafka_server_jaas.conf file to the environment variable KAFKA_OPTS before starting kafka server.

```bash
$ export KAFKA_OPTS="-Djava.security.auth.login.config=/KAFKA_HOME/config/kafka_server_jaas.conf"
$ bin/kafka-server-start.sh -daemon config/server.properties
```
Configuring the producer.

**producer.properties**

```properties
security.protocol=SASL_PLAINTEXT
sasl.mechanism=PLAIN
bootstrap.servers=localhost:9092
compression.type=none
```

**kafka_client_jaas.conf.**

---

**Note**  Console operations [for testing purpose only].

```java
KafkaClient {
   org.apache.kafka.common.security.plain.PlainLoginModule required
   username="admin"
   password="admin-secret";
};
Client {
   org.apache.zookeeper.server.auth.DigestLoginModule required
   username="admin"
   password=\"admin-secret\";
};
$ export KAFKA_OPTS="-
Djava.security.auth.login.config=/KAFKA_HOME/config/kafka_client_jaas.conf"
$ ./bin/kafka-console-consumer.sh --topic test-topic --from-beginning --
   consumer.config=config/consumer.properties --bootstrap-server=localhost:9092
$ export KAFKA_OPTS="-
Djava.security.auth.login.config=/KAFKA_HOME/config/kafka_client_jaas.conf"
$ ./bin/kafka-console-producer.sh --broker-list localhost:9092 --topic test-topic
   --producer.config=config/producer.properties
```

---

**Data Management**

**Installing Data Collection Framework**

This section describes how to install DCF.

DCF Default Properties:
In DCF installation (Console or GUI mode), by default following values are used for respective variables, which are not prompts for user inputs:

```
CTRL_URI_1=8443
CTRL_UN=admin
CTRL_PWD=changeme
MDB_URI=127.0.0.1:27017
MDB_UN=admin
MDB_PWD=changeme
```

**Note** User can modify any of the above values, by creating a file named `dcf-installer.properties` file with exactly same variable names and modified values, inside the same folder where binary is available for installation. The installer then automatically picks values defined in `dcf-installer.properties` file, if the file exists.

**Note** Make sure the URI, Username, and Password for MongoDB are same as the credentials created during MongoDB setup. If credentials are mismatched, installer displays a validation error and exits.

**Note** If you are providing special characters password in the `dcf-installer.properties`, then you must specify the password in double quotes ("password$").

### Install DCF using Console Mode

DCF can be installed on the platform of supported Linux hosts. This procedure specifically uses the Linux installation procedure as an example.

**Prerequisites**

Fulfill the following prerequisites before starting the installation:

1. Installation server must have bash installed.
2. Installation server must have zip installed.
3. Installation server must have installed curl utility.
4. MongoDB must be already installed along with first MongoDB user.
   - Refer, [Installing MongoDB](#) for more information.
5. When you install DCF on a Linux Platform, assign executable permissions to the installation script.
6. Ensure that you have a login with root privileges to run the installer.
7. Download the installation file from [http://support.vmware.com](http://support.vmware.com) and place it in a temporary location on the server.

**Procedure**

1. Login server as root.
2 Type "./SA-10.1-dcf-1.0.1.0-111.bin -i console" to run the installer in the console-based installer mode, press **Enter**.

   The introduction command prompt screen appears.

3 Press **Enter** to continue.

   License agreement appears.

4 PRESS ANY KEY TO CONTINUE TO READ LICENSE AGREEMENT OR PRESS '0' to ADVANCE TO END. Press **Enter**.

5 Type **Y** and press **Enter** to accept the license agreement.

6 Specify the directory to install DCF when installer prompts, or else press **Enter** to accept the default folder.

   Default Install Folder: /opt/DCF

   **Note**  If the target directory already contains an existing DCF installation, then it upgrades (patch or full), else fresh installation takes place.

7 Press **Enter** to continue when pre-install summary displays.

   Installation continues.

   **Note**  Installer triggers rollback action on any kind of failure. Except DCF_Logs, all files and folders gets uninstalled. Errors can be seen inside DCF_Logs/INSTALL_ERR.log

8 Press **Enter** to exit the installer when Install completed message displays.

What to do next

After successful DCF installation, Install **VMware Smarts Notification Collector** to pull all the events from Smarts Presentation SAM and publish the same to KAFKA for consumption.

   **Note**  If you shutdown or stop IP/ESM server which has Cisco ACI / VCD / Velocloud / vIMS / Cloudify discovered and restart the server with the same repos / topology using --ignore-restore-errors or --clean-topology then no issues. However if you shutdown ESM server and restart with --norestore option then old monitoring collectors for Cisco ACI / VCD / Velocloud / vIMS / Cloudify will be running and those need to be stopped manually.

Install DCF using Graphical Mode

This installation procedure describes the steps of DCF installation in the Graphical Interface.

Prerequisites

1 Ensure that you have a login with root privileges to run the installer.

2 Download the installer file from [http://support.vmware.com](http://support.vmware.com) and place it in a temporary location on the server.
Procedure

1. Login to the server as root.
2. Type `. /SA-10.1-dcf-1.0.1.0-111.bin -i gui` to run the installer in the graphical installer mode, press Enter.
   Installer introduction appears.
3. Click Next to continue.
   License agreement appears.
4. Select the checkbox I agree to the terms of the License agreement and click Next.
   Installer prompts to choose an install folder.
5. Specify the directory to install DCF when installer prompts, or else press Enter to accept the default folder.
   Default Install folder: `/opt/DCF`.
   Note If the target directory already contains an existing DCF installation, then it upgrades (patch or full), else fresh installation takes place.
6. Click Next to continue when pre-install summary displays.
   Note Installer triggers rollback action on any kind of failure. Except DCF_Logs, all files and folders gets uninstalled. Errors can be seen inside DCF_Logs/INSTALL_ERR.log
7. Click Done to exit the installer when Install Completed message displays.
   DCF installation is completed.

What to do next

After successful DCF installation, install VMware Smarts Notification Collector to pull all the events from Smarts Presentation SAM and publish the same to KAFKA for consumption.

Note If you shutdown or stop IP/ESM server which has Cisco ACI / VCD / Velocloud / vIMS / Cloudify discovered and restart the server with the same repos / topology using --ignore-restore-errors or --clean-topology then no issues. However if you shutdown ESM server and restart with --norestore option then old monitoring collectors for Cisco ACI / VCD / Velocloud / vIMS / Cloudify will be running and those need to be stopped manually.

Install DCF in Silent Mode

A DCF silent installation is an installation procedure that continues without user interaction.

Table 2-1. Variables Properties and Description

<table>
<thead>
<tr>
<th>Properties</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER_INSTALL_DIR</td>
<td>Choose Install Folder, =/opt/DCF.</td>
</tr>
<tr>
<td>CTRL_URI_1</td>
<td>Controller Details, Controller Port, = 8443.</td>
</tr>
</tbody>
</table>
Table 2-1. Variables Properties and Description (continued)

<table>
<thead>
<tr>
<th>Properties</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CTRL_UN</td>
<td>Controller Username.</td>
</tr>
<tr>
<td>CTRL_PWD</td>
<td>Controller Password.</td>
</tr>
<tr>
<td>MDB_URI</td>
<td>MongoDB URL.</td>
</tr>
<tr>
<td></td>
<td>MDB_URI=127.0.0.1:27017.</td>
</tr>
<tr>
<td>MDB_UN</td>
<td>MongoDB Username.</td>
</tr>
<tr>
<td>MDB_PWD</td>
<td>MongoDB Password.</td>
</tr>
</tbody>
</table>

Prerequisites

Create a configuration file for the installer to execute the installation. To create configuration file:

1. Copy the sample configuration file from the distribution (SA-10.1-dcf-1.0.1.0-111-silent-installer.properties) to a directory on the server where you are installing DCF.

2. Use any editor (vi/vim) to modify this file.

3. Define each of the properties in this file for server type, according to Table Variables Properties and Description. Save the changes to the file.

Sample content for installer.properties file:

```plaintext
# Replay feature output
# ____________________________
# This file was built by the Replay feature of InstallAnywhere.
# It contains variables that were set by Panels, Consoles or Custom Code.

# Choose Install Folder
# _________________________
USER_INSTALL_DIR=/opt/DCF

# Controller Details
# __________________
# Controller Port
CTRL_URI_1=8443

# Controller Username
CTRL_UN=admin

# Controller Password
CTRL_PWD=changeme

# MongoDB Details
# _________________
# MongoDB URL
MDB_URI=127.0.0.1:27017
```

Deployment Scenarios
**MDB_UN=admin**

**#MongoDB Password**

**MDB_PWD=changeme**

**Procedure**

1. Login to server as **root**.

2. Type `./SA-10.1-dcf-1.0.1.0-111.bin -i silent -f SA-10.1-dcf-1.0.1.0-111-silent-installer.properties` to run the installer in the silent installer mode, press **Enter**.

   **Note** Any user interaction is not required for this installer. Once it completes, a message displays indicating that installation is completed, and you are returned to the shell prompt. Logs are available at `<DCF_INSTALL_DIRECTORY>/DCF_Logs`.

   **Note** In case, both files (`dcf-installer.properties` and `SA-10.1-dcf-1.0.1.0-111-silent-installer.properties`) are present with different values to same variables then `dcf-installer.properties` file will get the precedence.

   **Note** If you are providing special characters password in the `SA-10.1-dcf-1.0.1.0-111-silent-installer.properties`, then you must specify the password in double quotes ("password$").

**What to do next**

After successful DCF installation, Install **VMware Smarts Notification Collector** to pull all the events from Smarts Presentation SAM and publish the same to KAFKA for consumption.

**Note** If you shutdown or stop IP/ESM server which has Cisco ACI / VCD / Velocloud / vIMS / Cloudify discovered and restart the server with the same repos / topology using --ignore-restore-errors or --clean-topology then no issues. However if you shutdown ESM server and restart with --norestore option then old monitoring collectors for Cisco ACI / VCD / Velocloud / vIMS / Cloudify will be running and those need to be stopped manually.

**DCF and M&R Integration**

This section helps you to integrate DCF with M&R. Kafka Messaging bus is used by VSA to fetch data from DCF and build topology and performance monitoring as well for the devices managed. The data collected by DCF which is pushed to Kafka is pushed to M&R backend where this can be leveraged to build reports for analysis.
To integrate DCF with M&R, run the script as mentioned in the knowledge base article *Integrate DCF with M&R* or perform the following steps:

**Procedure**

1. Go to the `bin` directory of DCF installation `/opt/DCF/bin`.
2. Update the required module to provide the details about the M&R backend host and port using the following command:
   
   `./manage-modules.sh update <module-name> <module instance-name>`

3. Enter ‘Y’, when prompt appears to modify the module configuration and process ahead.

   Do you want to modify the module configuration? (yes/no) [n] > y

4. Enter the details when prompted to forward the data to M&R. Enter ‘Y’ and enter the M&R backend Hostname and Port Number when prompted.

   ? Do you want data to be forwarded to M&R? (yes/no) [y] > y

**Results**

After the above integration you can see that the data is available in M&R.

**Note** In the M&R database, performance data is only available for VeloCloud SD-WAN Monitoring, Cisco ACI SDN Monitoring, and vCloud Director Management. You can create custom reports manually based on the requirements, reports are not available by default.
Performing Upgrade
This chapter illustrates the upgradation procedure.

Upgrading DCF using CLI Mode
This section describes the procedure of DCF upgradation in Console Mode.

Prerequisites
1. Download the installer package SA-10.1-dcf-1.0.1.0-111.bin from http://support.vmware.com
2. Ensure to stop all programs before you start the installation.

Procedure
1. To run the installer in console based installer mode, execute the command:
   
   ./SA-10.1-dcf-1.0.1.0-111.bin -i console

2. Press Enter to continue.

   License agreement prompt appears.

3. Press any key to continue reading the license agreement or press 0 to advance to end. Type Y and press Enter to accept the license agreement.

4. Specify the directory to install DCF when installer prompts, or else press Enter to accept the default folder.

   Default Install Folder: /opt/DCF

   **Note**  If the target directory already contains an existing DCF installation, then it upgrades, else fresh installation takes place.

5. Verify Pre-Installation Summary before moving ahead with the installation.

6. Press Enter to continue the installation.

   Installation complete message displays.

7. Press Enter to exit the installer.

Upgrading DCF using GUI Mode
This section details about the upgradation procedure of DCF in Graphical Mode.

Prerequisites
1. Download the installer package SA-10.1-dcf-1.0.1.0-111.bin from http://support.vmware.com
2. Ensure to stop all programs before you start the installation.
**Procedure**

1. To run the installer in console based installer mode, type the command.
   
   ```
   ./SA-10.1-dcf-1.0.1.0-111.bin -i gui
   ```

2. Press **Enter** to continue.

   License agreement prompt appears.

3. Select the checkbox **I agree to the terms of the License agreement** and click **Next**.

   Installer prompts to choose an install folder.

4. Specify the directory to install DCF when installer prompts, or else press **Enter** to accept the default folder.

   Default installation folder is `/opt/DCF`

   **Note**  If the target directory already contains an existing DCF installation, then it upgrades, else fresh installation takes place.

5. Verify Pre-Installation Summary before moving ahead with the installation.

6. Click **Done** to exit the installer when Install Completed message displays.

**Upgrading DCF using Unattended (Silent) Mode**

This section illustrates the DCF upgradation procedure in unattended (Silent) mode that is upgradation without user input.

**Procedure**

1. When DCF base install location is `/opt/DCF`, type the setup command syntax:
   
   ```
   ./SA-10.1-dcf-1.0.1.0-111.bin -i silent
   ```

   and press **Enter**.

2. If the base install location is different from `/opt/DCF`, specify the location of the product suite to be upgraded in properties file.

   For example, specify the directory as:
   ```
   USER_INSTALL_DIR=/opt/DCF1 in “SA-10.1-dcf-1.0.1.0-111-silent-installer.properties”.
   ```

3. To create `installer.properties` file, execute the command:

   ```
   echo "USER_INSTALL_DIR=<DCF_Install_DIRECTORY>" > SA-10.1-dcf-1.0.1.0-111-silent-installer.properties
   ```
Provide the path to SA-10.1-dcf-1.0.1.0-111-silent-installer.properties file.

**Note** If it is not present in the DCF binary location, execute the command:

```
Product Name: DCF
Install Folder: /opt/DCF
./SA-10.1-dcf-1.0.1.0-111.bin -i silent -f SA-10.1-dcf-1.0.1.0-111-silent-installer.properties
```

**Note** Ensure to update the SA-10.1-dcf-1.0.1.0-111-silent-installer.properties file with DCF base directory `<DCF_Install_DIRECTORY>` correctly. Else a fresh installation will take place at the new location causing two DCF instances.

### Data Collection Controller

Data Collection Controller (DCC) is a REST-based orchestrator that takes requests from users to deploy and manage data collection blocks. Data Collection Blocks (usually called 'block') collect data from specified devices, transform, filter, and publish them via multiple interfaces. Currently, a block defines a pipeline that may contain one or more components that will collect, process, and publish data.

#### Main components of DCC

1. **Web server**: Gunicorn 'Green Unicorn' is a Python WSGI HTTP Server for UNIX. It's a pre-fork worker model. The Gunicorn server is broadly compatible with various web frameworks, simply implemented, light on server resources, and fairly speedy.

2. **MongoDB**: MongoDB is a cross-platform document-oriented database program. It is a dependency of the DCC. It is classified as a NoSQL database program. MongoDB uses JSON-like documents with schemata. MongoDB is developed by MongoDB Inc.

3. **Data Collector Framework core**: DCF core technology software delivers enterprise and carrier-class cross-domain performance and service level management which transforms data into actionable information, helping assure the delivery of business services.

   DCC interacts with DCF core via its Web Service Gateway, a SOAP-based API that provides a programmable interface to DC Core features.

DCC endpoints: DCC has two main endpoints:

1. **Catalog**: Catalog is responsible for block provisioning, configuration, available blocks, and packages.

2. **Runtime**: Runtime is responsible for operations with blocks, such as start, stop, restart, manage, and un-manage configuration of variable handling filter (VHF).
How authentication works

DCC is configured to be the only entry point of DCF. Once you install it, it allows you to provision and orchestrate any available block in DCF.

Most of the DCC configuration is done through properties in dc_controller/server/config.py.

This is typically where an administrator would change the protocol (http/https), the listening address, the listening port, secret key parameters, and a few other advanced settings.

DCC communication is encrypted using HTTPS. The client issues a request using Basic authentication through a HTTPS channel. Therefore, a certificate needs to be generated during the installation process.

DCC logs

DCC logs are present at directory <Path_to_DCF_Installation>/Tools/Controller/Default/logs/

The log file under above directory structure : apg-controller-default.out - contains controller startup related errors.

Another log file under above directory structure : dcf.log - contains controller functionality errors.

DCC configuration

The configuration file dc_controller/server/config.py contains all the parameters of DCC.

It contains information about:

1. DCC internal credentials, secret key, and path to client certificate.
2. MongoDB location and credentials, DC Core location and credentials, maximum number of clients interacting with web service gateway, DCC location, and type of deployment (i.e. Bare metal or virtualized).

This file will be generated as result of the 'create first user' script execution:

```python
MONGODB_URI='127.0.0.1:27017'
MONGODB_USERNAME='admin'
MONGODB_PASSWORD='ENCRYPTED_PASSWORD'
MONGODB_DATABASE='admin'
DEPLOYMENT_TYPE='BAREMETAL'
MNR_HOST='127.0.0.1'
MNR_PORT='48443'
MNR_USER='admin'
MNR_PASSWORD='ENCRYPTED_PASSWORD'
MNR_MAX_THREADS=2
SECRET_KEY='SECRET_KEY'
CERTIFICATE_PATH="/opt/DCF/Tools/Controller/Default"
DCF_HOST='0.0.0.0'
DCF_PORT='8443'
USERNAME='admin'
PASSWORD='ENCRYPTED_PASSWORD'
LOG_LEVEL='INFO' # 'DEBUG', 'ERROR', 'CRITICAL', 'WARNING'
```
# The following properties are passed to the DCC web server (Gunicorn)
bind='0.0.0.0:8443' # Gunicorn bind socket
workers='4' # Number of async workers
worker_class='gthread' # Gunicorn mode
certfile='/opt/DCF/Tools/Controller/Default/conf/controller-cert.pem'
keyfile='/opt/DCF/Tools/Controller/Default/conf/controller-key.pem' preload_app='True'

# The following is a Gunicorn server hook, called just after the server is started.
def when_ready(server):
    import dc_controller.wsgi as dcfControllerApp
dcfControllerApp.create_default_template()

The 'config.py' file can be regenerated using below command:

```
python3.6 <DCF_Installation_path>/Tools/Controller/Default/dc_controller/utils/create-first-user.py
<DEPLOYMENT_TYPE> <MongoDB_USERNAME> <MongoDB_PASSWORD> <MONGODB_URI> <MNR_HOST><MNR_PORT>
<MNR_USERNAME> <MNR_PASSWORD> <MNR_MAX_THREADS> <OUTPUT_CONFIG_FILE>
<CERTIFICATE_PATH><KEY_FILE_PATH> <DCF_HOST> <DCF_PORT> <DCF_HOST:DCF_PORT>
<DCF_USERNAME><DCF_PASSWORD>
```

### KPI Engine (K4M)

This section provides information on how to install K4M.

K4M comprises the following components:

- K4M REST Service
- KPI Engine
- KPI Configuration Store
- KPI Designer Graphical User Interface (GUI)

Installation, configuration and verification of all above components except the KPI Designer GUI is described here.

The KPI Designer GUI is included in the VMware Smart Assurance UI. Refer to the VMware Smart Assurance UI documentation for details. K4M will integrate with VMware Smart Assurance (VSA) via a Kafka broker.

### System Requirements

VMware K4M must be installed on a single host/node. You can refer to this host as **K4M_HOST** and the host the K4M Designer GUI is installed as the **KPI_GUI_HOST**.

1. **Minimum System Requirements:**
   
   a. Operating system: Red Hat Enterprise Linux (RHEL) or CentOS 6.9, 6.10, 7.5 or 7.6. A fresh installation of the operating system is recommended to avoid conflict with previously installed packages.
   
   b. CPU: 2.0 GHz.
   
   c. Memory: 16GB.
Hard disk space recommended: 100GB.

VMware K4M creates a separate user account "k4m" during installation. This should be used primarily for all operations. Root access is required for few steps, which are specified below.

MongoDB version 4.0.4. This guide assumes that MongoDB is running on the same host as VMware K4M. Modify the instructions accordingly if it is on a different host. Refer installing MongoDB for more detail.

Internet connectivity, to download dependent packages and software.

Connectivity to Kafka broker used by VMware Smart Assurance. Ensure that DNS is configured in your environment, or that you have statically configured the Fully Qualified Domain Name (FQDN) of the Kafka broker on your K4M_HOST (in the /etc/hosts file).

Required ports - K4M services run on the ports listed below. Ensure these ports are accessible in case you have a firewall.

<table>
<thead>
<tr>
<th>Port</th>
<th>K4M Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>8083</td>
<td>K4M REST Service</td>
</tr>
<tr>
<td>8081</td>
<td>KPI Engine (Flink)</td>
</tr>
<tr>
<td>27017</td>
<td>KPI Configuration Store</td>
</tr>
</tbody>
</table>

Assuming firewall is installed on your host, login as root and use the following commands to open the ports. Since your host's version of firewalld or configuration may vary, refer to your host-specific firewall documentation for the exact commands.

```
$ firewall-cmd --zone=public --add-port=8083/tcp --permanent
$ firewall-cmd --zone=public --add-port=8081/tcp --permanent
$ firewall-cmd --zone=public --add-port=27017/tcp --permanent
$ firewall-cmd -reload
```

Installing K4M

This section helps you to install K4M.

Procedure to install K4M:

Procedure

1. Login as root
2. Copy installer file "vmware-k4m-VERSION-nogui-installer.bin" to host. This location is INSTALLER_DIR.
3. Change to INSTALLER_DIR and modify permissions:

```
$ chmod +x vmware-k4m-VERSION-nogui-installer.bin
```
4 Launch the installer and follow the prompts on the terminal till the installer completes installation:

$ ./vmware-k4m-VERSION-nogui-installer.bin

5 By default, VMware K4M is installed under /opt. Can be modified, must enter the absolute path to your location and modify scripts as mentioned in subsequent steps. Recommend to use default.

6 Installation finished, with messages as displayed below:

Congratulations. VMware K4M <VERSION> has been successfully installed at:
/opt/vmware-k4m
PRESS <ENTER> TO EXIT THE INSTALLER:

Product is extracted to /opt/vmware-k4m (or your_location/vmware-k4m). You can refer to this location as VMWARE_K4M_HOME.

7 VMWARE_K4M_HOME contains:
   - config
   - examples
   - k4m-rest-VERSION.tar.gz
   - license
   - scripts

   **Note** Installation process and creates logs under INSTALLER_DIR/_VMware K4M_installer/logs. The .log file has the installation process details and the .txt file has information about the installer.

**Setup and Configure K4M**

This section helps you in setting-up, configuring and launching VMware K4M.

**Procedure**

1 Modify files (Optional):

   If VMware K4M has been installed under default location /opt, you may skip this step. Otherwise replace occurrence of /opt with the full path to the parent folder of your VMware K4M installation in the following files:
   a All scripts under VMWARE_K4M_HOME/scripts.
   b VMWARE_K4M_HOME/config/k4m-rest-application.properties

2 Configure system settings, download system and open-source packages:

   Change to VMWARE_K4M_HOME/scripts. Run the script "step-1-as-root.sh" and follow prompts.
$ ./step-1-as-root.sh

This will:

a  Create the user **k4m** and give it ownership of the installation under VMWARE_K4M_HOME. The default password is "**k4m**".

b  Download and install system packages including OpenJDK.

c  Configure SSHD.
d Add the following entry into /etc/hosts file such that k4m01 refers to the localhost. k4m01 is referred in other scripts.

```
127.0.0.1 k4m01
```

**Note**

1. On RHEL and CentOS 6.9 and 6.10, when the script finishes you will see the following. This can be ignored as necessary configuration is made by the OS by default. / step-1-as-root.sh: line 64: sshd-keygen: command not found

2. The script uses the yum command to install dependencies. Rarely, installation of some dependent system package may fail, because of the specific configuration of your OS. When something fails to install you can try these steps:
   a. Based on the error on your terminal, identify the dependency package. Open the script and note down the exact name and version.
   b. If using RHEL, ensure your host is subscribed to the Red Hat Subscription Service (refer to Red Hat documentation) so you can download the dependency. Then re-run the command to install the package as follows:

```
$ yum install -y REQUIRED_PACKAGE_NAME
```

c. Sometimes a package may fail to install due to another existing dependency's version. In that case update that existing package or even all your system software and then re-run the command to install the required dependency.

```
$ yum update EXISTING_PACKAGE
OR
$ yum update
```

then

```
$ yum install -y REQUIRED_PACKAGE_NAME
```

3. jq package manual installation: The jq package is installed in script "step-1-as-root.sh" as well using yum and can fail to install due to the reasons mentioned above in 2. If the steps to rectify mentioned above do not work, one should manually install the package as follows. Login as root and navigate to the /opt. There run the following:

```
$ wget -O jq https://github.com/stedolan/jq/releases/download/jq-1.6/jq-linux64
$ chmod +x ./jq
$ cp jq /usr/bin
```

The jq package is used later in the automated health check script to verify that K4M is installed correctly.
3 Configure MongoDB [1]

**Note** It is assumed that the reader is familiar with MongoDB administration.

a Create a database “k4m-rest” and user “k4m” in your MongoDB instance. A script has been provided with the configuration viz. VMWARE_K4M_HOME/config/mongo-config.js as shown below:

```javascript
db.createUser(
    {
        user: "k4m",
        pwd: "k4m",
        roles: [{ role: "readWrite", db: "k4m-rest" }]
    }
)
```

One may change the database name (db) and user name (user), and if you do so, you must follow the steps below to make corresponding changes in other places. Recommend to use the default settings. Change to VMWARE_K4M_HOME/config folder and run the MongoDB Admin command line tool to execute the script as shown below:

```bash
$ mongo --host MONGODB_HOST --port MONGODB_PORT --username ADMIN_USERNAME --password ADMIN_PASSWORD admin mongo-config.js
```

where

- MONGODB_HOST and MONGODB_PORT need to be specified only if your MongoDB instance is running on a remote host. If MongoDB is running locally then you don't need --host and --port options. Default host is localhost and port is 27017.
- ADMIN_USERNAME and ADMIN_PASSWORD are your MongoDB instance administrative account credentials
- The "admin" database is specified to store the user "k4m" being created.

On running the above command machine displays:

```
MongoDB shell version v4.0.9
connecting to: mongodb://127.0.0.1:27017/admin?gssapiServiceName=mongodb
Implicit session: session { "id" : UUID("d1e1b971-12f0-4aa7-a12f-64236138785d") }
MongoDB server version: 4.0.9
Successfully added user: {
    "user" : "k4m",
    "roles" : [ {
        "role" : "readWrite",
        "db" : "k4m-rest"
    } ]
}
```
You can also verify by logging into the Mongo Shell, then switching to the admin database and listing the users as shown below. Notice that the k4m user is created in the admin db but has privileges for the k4m-rest db as it should be.

```
$ mongo HOST:PORT --username ADMIN_USERNAME --password ADMIN_PASSWORD
> use admin
switched to db admin
> show users
{
  "_id" : "admin.admin",
  "userId" : UUID("437b6bea-e8db-4d1d-b244-3464e75b682f"),
  "user" : "admin",
  "db" : "admin",
  "roles" : [
    {
      "role" : "root",
      "db" : "admin"
    },
    {
      "mechanisms" : [
        "SCRAM-SHA-1",
        "SCRAM-SHA-256"
      ]
    }
  ],
  "mechanisms" : [
    "SCRAM-SHA-1",
    "SCRAM-SHA-256"
  ]
}
{
  "_id" : "admin.k4m",
  "userId" : UUID("c4ff7994-ba17-4709-927e-96c103cc814d"),
  "user" : "k4m",
  "db" : "admin",
  "roles" : [
    {
      "role" : "readWrite",
      "db" : "k4m-rest"
    },
    {
      "mechanisms" : [
        "SCRAM-SHA-1",
        "SCRAM-SHA-256"
      ]
    }
  ],
  "mechanisms" : [
    "SCRAM-SHA-1",
    "SCRAM-SHA-256"
  ]
}
```

b) Modify the VMWARE_K4M_HOME/config/k4m-rest-application.properties file as follows:

1. The database connection details should be updated according to your MongoDB instance's details. The K4M REST Service uses these details to connect to the KPI Configuration Store. The defaults are as follows:

```
spring.data.mongodb.uri=mongodb://k4m:k4m@k4m01:27017
spring.data.mongodb.database=k4m-rest
```

where

- k4m:k4m is the database user and password created in the step above. Recommend default.
4 Install Flink and the K4M REST Service:

Become k4m user:

$ su k4m

Run the script "step-2-as-k4m.sh". This will:

a Configure SSH keys
b Download and install Flink. Flink is extracted into folder "flink-VERSION", created under the same directory that vmware-k4m is installed. By default, it is under /opt or the path specified by you when modifying the scripts in step 1 above. We will refer to this complete path as FLINK_HOME (also set as environment variable).

c Install the K4M REST Service:

$ ./step-2-as-k4m.sh

5 Start the Flink cluster and K4M REST Service:

Run the script "step-3-as-k4m.sh"

$ ./step-3-as-k4m.sh

Verifying K4M Installation

This section describes tasks for confirming proper installation of the VMware K4M Installation.

Verification by script:

1 Checks message flow to Kafka broker by publishing and subscribing to test message. For this, the script downloads a Kafka distribution under the /scripts folder and runs the console producer and consumer.

2 Queries the VMware K4M http://<K4M_HOST_IP>:8083/v1/health REST endpoint to verify all services are running.

   For example, if the Host IP is 10.118.233.41. Then the URL will be http://10.118.233.41:8083/v1/health.

Note In this release, the verification script checks only one Kafka broker and VMware K4M monitors its status. This is applicable for either a single-broker or a Kafka cluster. If you are running a Kafka cluster please provide any one broker and port as mentioned in the steps below, so the script can verify connectivity to at least one broker in the cluster.
Prerequisites

Confirms all services are installed correctly and communicate with each other including VSA Kafka broker. Monitors status of following services:

1. K4M Rest Service
2. KPI Engine (based on Flink)
3. KPI Configuration store (MongoDB)
4. Ensure Kafka broker for the VSA solution is running and accessible.

Procedure

1. Become k4m user by modifying the script "step-4-as-k4m.sh" by setting values for the variables shown below:

```
# Set to Kafka broker
KAFKA_HOST=kafka_broker_ip
KAFKA_PORT=kafka_broker_port
KAFKA_USER=kafka_user
KAFKA_PASSWORD=kafka_password
# Set to Zookeeper
ZOOKEEPER_HOST=zookeeper_ip
ZOOKEEPER_PORT=zookeeper_port
```

   **Note** Use the advertised Kafka broker IP found in your broker’s server.properties. If secured access to Kafka broker is not required, the Kafka username and password should be left blank.

2. Kafka status is monitored via JMX so the Kafka broker must have JMX port enabled. This must be done when installing Kafka and in a manner so it is permanent (for example add to .bash_profile). Refer Installing Kafka for the procedure. If not done during Kafka installation, follow the steps to enable the port and restart Kafka.

   **Note** Setting the JMX port is required only to monitor Kafka status and not required to run K4M. So it can be an optional step. If you skip this step you can also skip the next command. $ export JMX_PORT=kafka_broker_jmx_port

3. Only if you have completed step 2 above, then set the same JMX port from step 2 in the script "step-4-as-k4m.sh": The script creates a service entry in VMware K4M for the Kafka broker using ip, port, JMX port. VMware K4M monitors Kafka and updates the status of the service.

```
KAFKA_JMX_PORT=kafka_broker_jmx_port
```
4 Run the script "step-4-as-k4m.sh" and if everything is running correctly, screen displays:

```
$ ./step-4-as-k4m.sh
Verifying installation of VMware K4M services....
.....
VMware K4M services ready
```

You can also verify that all the services are online by visiting the REST API endpoint at http://<K4M_HOST_IP>:8083/v1/health.

**Note** Without enabling the JMX port on the Kafka host, VMware K4M is not able to monitor Kafka. However, this does not affect the working of VMware K4M. The script reports that JMX is not enabled.

**Monitoring K4M health**

You can monitoring K4M health subsequently.

The status of all K4M services and the Kafka broker it is connected to can be monitored at any time after installation in one the following ways:

1. Running the `VMWARE_K4M_HOME/scripts/step-4-as-k4m.sh` as described in the Verify Installation section.
2. Visiting the `http://<K4M_HOST_IP>:8083/v1/health` REST endpoint to view the status details.

For example, if the Host IP is 10.118.233.41. Then the URL will be `http://10.118.233.41:8083/v1/health`.

**Domain Manager**

**Installation**

This section describes how to install and configure IP, SAM and ESM.

**Prerequisite**

Ensure that following components are up and running:

- DCF
- MongoDB
- Kafka

**Installing SMARTS SAM**

1. To install SAM, refer Performing an Installation.
2. To attach the IP and ESM server as the underlying server for a SAM server, refer Configuring Domains.
3. To install SAM Global Console, refer to Install using Wizard mode for SAM Console (Windows only).

**Note**: For opening Global Console, refer to Procedure for opening the Global Console.

Performing an Installation

Installation overview

The installation flow is shown in New installation flowchart. A new installation installs a new version of a product on a host system that either has no software installed or has a previous version of the software installed.

Figure 2-1. New installation flowchart

![New installation flowchart](image)

Installation prerequisites

Fulfill the following prerequisites before starting the installation:

- Ensure that you have superuser (User ID 0) or administrative privileges on the target host. The installation program will halt if you do not have the appropriate privileges.
Ensure that the required operating system patches have been installed. Clicking More Information during the installation process will launch the System Information window and the Pass/Fail status of the operating system patches. The VMware Smart Assurance Support Matrix provides information on operating system patches.

Determine the location of the VMware Smart Assurance Broker.

You must specify the location of the Broker during a new installation of VMware Smart Assurance software. Typically, this location is chosen during the design of the VMware Smart Assurance software deployment and before any installation begins. Consult with your deployment planner or check the build guide that documents your deployment to determine the name of the host where the Broker was installed and the port that the Broker uses.

If the location is the same host where you are installing this product, the installation program will automatically install the Broker if it is not already on the host.

(Service Assurance Manager only) Decide whether your operators will use the Service Assurance Manager Notification Console (classic SAM functionality).

Install the product

You acquire the software for the VMware Smart Assurance Service Assurance Manager, VMware Smart Assurance IP Manager, VMware Smart Assurance MPLS Management Suite, VMware Smart Assurance Server Manager, and VMware Smart Assurance Network Protocol Management Suite in one of two ways:

From the installation CD/DVD-ROM.

Insert the CD/DVD-ROM into the optical drive of the host system.

When you insert the installation CD/DVD, several minutes might pass between the InstallAnywhere preparation screen and the VMware Smart Assurance splash screen/installation dialog boxes. Be patient. Do not eject/reinsert the CD/DVD to start a second install process.

From the VMware online support website.

Go to the VMware online support website and download the installation file that is specific to your platform.

You install each product in one of three ways: Wizard mode, CLI mode, or Unattended mode.

Install using CLI mode

CLI mode provides a text-based method for invoking the installation program. This mode is intended for UNIX platforms with non-graphics consoles. The CLI mode follows the same process flow as the Wizard mode but uses text rather than graphics.

Running CLI mode
### Table 2-2. Setup command syntax for CLI mode

<table>
<thead>
<tr>
<th>Product</th>
<th>Operating system</th>
<th>Executable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Assurance Manager Server</td>
<td>Linux</td>
<td>./setup-SAM-10_0_0_0-linux64.bin</td>
</tr>
<tr>
<td>Service Assurance Manager Console</td>
<td>Linux</td>
<td>./setup-CONSOLE-10_0_0_0-linux.bin</td>
</tr>
<tr>
<td>IP Manager</td>
<td>Linux</td>
<td>./setup-IP-10_0_0_0-linux64.bin</td>
</tr>
<tr>
<td>MPLS Management Suite</td>
<td>Linux</td>
<td>./setup-MPLS-10_0_0_0-linux64.bin</td>
</tr>
<tr>
<td>Server Manager</td>
<td>Linux</td>
<td>./setup-ESM-10_0_0_0-linux64.bin</td>
</tr>
<tr>
<td>Network Protocol Management Suite</td>
<td>Linux</td>
<td>./setup-NPM-10_0_0_0-linux64.bin</td>
</tr>
</tbody>
</table>

**User selections and navigation in CLI mode**

During the installation and uninstallation processes, you are prompted with a series of steps and menus:

- For prompts, accept the default value or select another choice. The default values are indicated in brackets. To accept the default value, press **Enter**. To reply “yes,” enter **y** or **Y**; to reply “no,” enter **n** or **N**. Do not press **Delete** because doing so will cause the process to terminate with an error message.

- For selections in menus, accept the default selections or type the number of the item and press **Enter**.

  If you incorrectly type an entry, press **back** to repeat the prompt and select the correct value. Arrow keys and the Backspace key are not supported.

If your product is part of a deployment that requires the Federal Information Processing Standard (FIPS) Publication 140-2, a U.S. government computer security standard governing cryptographic modules, follow the instructions in *Support for FIPS 140-2 for Smart Assurance products*.

**Install using Unattended mode**

Unattended mode reads the selections and settings for the installation from a user-modifiable response file, which enables you to easily duplicate the installation on many computer systems. Manual intervention is not necessary after you execute the setup command.

The response file, named `<product>-response.txt`, is located on the CD/DVD-ROM in the `/utils` directory. The file provides instructions and examples of command line options that are passed to the installation program in Unattended mode. The command line options are organized by process flow, which is almost identical to that of Wizard mode or CLI mode.

**Modifying the response file**

To modify the response file:

1. Copy the response file from the CD/DVD’s /utils directory to a directory on your host, for example, to the /tmp directory.

2. Using a text editor, modify the values for the command line options in the response file:
   - Specify the target directory.
b Select a directory for the process log file.

c Select the products to install. Ensure that the property value for the product is set to true.

d Select the products to start as services. Ensure that the property value for the product is set to true.

e Specify the location of the Broker. By default, the location is set to localhost at port 426.

3 Save the file.

Running Unattended mode

To start the Unattended mode, invoke the setup command with the -options command-line option, followed by the full path to the response file as described in the below table.

Table 2-3. Setup command syntax for Unattended mode

<table>
<thead>
<tr>
<th>Product</th>
<th>Operating system</th>
<th>Executable</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Assurance Manager Server</td>
<td>Linux</td>
<td>./setup-SAM-10_0_0_0-linux64.bin -i silent -f &lt;path&gt;/&lt;product&gt;-response.txt</td>
</tr>
<tr>
<td>Service Assurance Manager Console</td>
<td>Linux</td>
<td>./setup-CONSOLE-10_0_0_0-linux64.bin -i silent -f &lt;path&gt;/&lt;product&gt;-response.txt</td>
</tr>
<tr>
<td>IP Manager</td>
<td>Linux</td>
<td>./setup-IP-10_0_0_0-linux64.bin -i silent -f &lt;path&gt;/&lt;product&gt;-response.txt</td>
</tr>
<tr>
<td>MPLS Management Suite</td>
<td>Linux</td>
<td>./setup-MPLS-10_0_0_0-linux64.bin -i silent -f &lt;path&gt;/&lt;product&gt;-response.txt</td>
</tr>
<tr>
<td>Server Manager</td>
<td>Linux</td>
<td>./setup-ESM-10_0_0_0-linux64.bin -i silent -f &lt;path&gt;/&lt;product&gt;-response.txt</td>
</tr>
<tr>
<td>Network Protocol Management Suite</td>
<td>Linux</td>
<td>./setup-NPM-10_0_0_0-linux64.bin -i silent -f &lt;path&gt;/&lt;product&gt;-response.txt</td>
</tr>
</tbody>
</table>

where <path> is the fully qualified path to the response file and <product> is the product name, for example, IP_NETWORK_SUITE, MPLS_SUITE, or SAM_SUITE.

For example for MPLS Management Suite, to start the Unattended mode of installation on Linux when the response file is located in /opt/home, enter:

```
./setup-MPLS-10_0_0_0-linux64.bin -i silent -f <path>/<product>-response.txt
```

If your product is part of a deployment that requires the Federal Information Processing Standard (FIPS) Publication 140-2, a U.S. government computer security standard governing cryptographic modules, follow the instructions in Support for FIPS 140-2 for Smart Assurance products.

**Note**  SAM and SAM-Console Custom feature is removed. Now, all the features are available as a complete installation in both fresh installation and upgrade from older products.
Support for FIPS 140-2 for Smart Assurance products

The Federal Information Processing Standard (FIPS) Publication 140-2 is a U.S. government computer security standard governing cryptographic modules. FIPS 140 is required for any software purchased by the U.S government and U.S military. This release specifically addresses U.S Government accounts which require FIPS 140 compliance.

A configuration parameter, SM_FIPS140, has been introduced for FIPS 140 in the runcmd_env.sh file. The SAM or VMware Smart Assurance administrator can enable or disable this parameter as required. The default value of this parameter is FALSE.

FIPS 140 mode allows you to use SNMP V1, SNMPV2C, SNMP V3, with SHA and AES 128 protocols. FIPS 140 does not support the DES privacy protocol or the MD5 authentication protocol. When you discover an SNMPv3 device, you need to select the option “V3” in the “Add Agent” window. The “Authentication Protocol” option lists only SHA and not MD5, and the “Privacy Protocol” option lists only AES and not DES. This is because MD5 and DES are not supported in FIPS 140 mode. When you discover SNMPv3 devices with MD5 and DES protocol as seed, the devices go to the Pending List and display as “Invalid” or “Unsupported SNMP V3 protocol.”

Note  FIPS 140 mode cannot be enabled or disabled after a server is started. FIPS 140-enabled Domain Managers such as MPLS Management Suite, IP Manager, Service Assurance Manager, and Server Manager can work only with the SAM Global Console 9.x or later for FIPS 140-2 mode.

A non-FIPS 140 mode Broker will not be able to communicate with a FIPS 140-enabled Manager (IP server, SAM server, or Domain Manager). Trying to establish such a connection will result in the enabled Manager going into a DEAD state after couple of minutes. Communication should always happen between FIPS 140-enabled Brokers and Managers.

Inter-domain and FIPS 140 Broker communication happens only when the Broker, Managers, and the SAM Console are all in FIPS 140 mode, else the application will not be operational. Enabling FIPS 140 mode on a new installation

When you install a 10.0.0 product, FIPS 140 is not enabled by default. You must enable FIPS 140 on a clean installation or an upgrade, before the servers are started, using the following procedure:

Procedure

1. Back up the imk.dat, brokerConnect.conf, serverConnect.conf and clientConnect.conf files from the existing installation. These files are located in the BASEDIR/local/conf folder.

   Note  The backup is necessary in case you need to disable FIPS 140 mode and remove FIPS 140-2 encryption.

2. Run the following command at the command line prompt:

   sm_rebond --upgrade --basedir=<BASEDIR>/smarts sm_rebond --upgrade --basedir=C:\InCharge\SAM\smarts
3. When prompted, type a password to regenerate the imk.dat file. The default password is Not a secret.

4. Set the value for the parameter SM_FIPS140 to TRUE in the runcmd_env.sh file. The file is located under the BASEDIR/smarts/local/conf directory.

Enabling FIPS 140 mode on SAM Web Console

Procedure
1. Perform steps 1 - 3 as described in the section, Enabling FIPS 140 mode on a new installation.
2. Go to the <BASEDIR>/smarts/jre/lib/security folder, and in the java.security file, change:
   “sun.security.rsa.SunRsaSign” to “com.rsa.jsafe.provider.JsafeJCE” and
3. Set the value for the parameter SM_FIPS140 to TRUE in the runcmd_env.sh file. This file is located under the <BASEDIR>/CONSOLE/smarts/local/conf folder of your Global Console installation.
   or
   Use "-Dcom.smarts.fips_mode=true" as a command line parameter for the sm_gui command.

Enabling FIPS 140 mode on SAM Dashboard

Procedure
1. Perform steps 1 - 3 as described in the section, Enabling FIPS 140 mode on a new installation.
2. Set the value for the com.smarts.fips_mode to TRUE in the corresponding webconsole.properties file (located under <BASEDIR>/InCharge/CONSOLE/smarts/tomcat/webapps/webconsole folder)
   or
   dashboard.properties file (located under <BASEDIR>/InCharge/CONSOLE/smarts/tomcat/webapps/templates).
3. Set the value for the parameter SM_FIPS140 to TRUE in the runcmd_env.sh file. This file is located under the <BASEDIR>/CONSOLE/smarts/local/conf folder of your Global Console installation.
   or
   Use "-Dcom.smarts.fips_mode=true" as a command line parameter for the sm_gui command.

Enabling FIPS 140 mode on SAM NOTIF

Procedure
1. Perform steps 1 - 3 as described in the section, Enabling FIPS 140 mode on a new installation.

Set the value for the parameter SM_FIPS140 to TRUE in the runcmd_env.sh file. This file is located under the `<BASEDIR>/CONSOLE/smarts/local/conf` folder of your Global Console installation.

or

Use "-Dcom.smarts.fips_mode=true" as a command line parameter for the sm_gui command.

**Note** If you install the servers as a service on Linux platforms, the services will start automatically after you issue the sm_rebond command. First stop the services, modify SM_FIPS140=TRUE in the runcmd_env.sh file, and then manually start the services.

After enabling FIPS 140 mode, when you start the broker and the SAM server, you may see the following message in the server log:

“CI-W-NOCGSS-No certificate loaded for INCHARGE-AM, generating self-signed certificate.”

This message is generated because FIPS 140 requires secure communication, which can be achieved using SSL. If this certificate is not available, the SAM Manager generates a self-signed certificate. This message is benign in nature and does not impact functionality.

Disabling FIPS 140 mode
To disable FIPS 140, follow the procedure.

**Procedure**

1. Replace the `imk.dat`, `brokerConnect.conf`, `serverConnect.conf` and `clientConnect.conf` files in the `BASEDIR/local/conf` folder, with the copies saved from prior to Enabling FIPS 140 mode on a new installation. If you do not have a copy of these files saved, contact Technical Support.

2. Set the value for the **SM_FIPS140** parameter to **FALSE** in the `runcmd_env.sh` file. This file is located under `BASEDIR/smarts/local/conf/runcmd_env.sh`.

3. Restart all processes, such as the Broker, Domain Managers, SAM Global Manager, and Global Console.

**Note** RPS files started under FIPS mode cannot be re-used in non-FIPS mode. Domains will need to be started either from scratch or pre-FIPS RPS files can be used in cases where topologies have not changed. Restoring from older RPS files may not be productive as it will not contain any recent topology.

Install using Wizard mode for SAM Console (Windows only)
Wizard mode provides a graphical user interface to the installation program for Windows platforms.

Microsoft Windows Server 2012 and Microsoft Windows Server 2016, operating system are only supported.

Users who display Business Dashboard viewlets in a web browser, or want to use the Web Console, require the following software:

- Google Chrome
- Internet Explorer
- Mozilla Firefox
- Safari.

At the start of the installation, the installation program detects and stops all services, scheduled jobs, and processes that use programs or libraries that are running from the previous installation. It also stops the service daemon, sm_serviced, if it is running.

Be aware that in some cases, on Windows, services cannot be stopped by the installation program because multiple threads are locking the services. In those cases, use the Windows Control Panel to stop the services manually.

**Running Wizard mode**

1. Run the setup command that is appropriate for the operating system as shown in *Server setup command syntax for Wizard mode*.

   **Table 2-4. Server setup command syntax for Wizard mode**

<table>
<thead>
<tr>
<th>Product</th>
<th>Operating system</th>
<th>Setup command</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Assurance Manager Server</td>
<td>Windows</td>
<td>setup-CONSOLE-10_1_0_0-win.exe. To setup, double click the executable file.</td>
</tr>
</tbody>
</table>

   **Note**: The InstallAnywhere wizard dialog box appears and closes. The *Shutdown Programs* dialog box and the *Welcome* screen appear.

1. Click **OK** in the *Warning* dialog box.
   
   If stopping services is necessary, you will be prompted with specific instructions later in the installation process.

2. Click **Next** in the *Welcome* screen.

3. Read and accept the end user license agreement and click **Next**.

4. If the installation program detects an existing installation of the same product, the *Upgrade or Install* screen appears. In the *Upgrade or Install* screen, select *Install products to a new directory*.

5. Click **Next** to accept the default installation directory or type your preferred directory and click **Next**.
The default installation directory is:

If you specify a directory, the directory name cannot contain spaces. If the specified directory does not exist, it will be created. If you do not have write privileges, an error message appears.

6 Click **Next**.

7 In the **Services Selection** screen, select the products that you want to install as services and click **Next**. If you do not install services at this point, you will need to install them manually later.

For Service Assurance Manager services, you have two choices:

- Select **VMware Smart Assurance Servelet Engine** if you plan to run only the `ic-business-dashboard` service.

8 In the **Broker Specification** screen, specify the VMware Smart Assurance Broker.

- If you are installing the Broker as a service or server way, specify the port and hostname.
  
  - If the Broker is already running on this host, keep the default values.
  
  - If the Broker is running on another host, specify the hostname of that system and the port that the Broker uses.

  Click **Next** to continue.

9 The **Installation Criteria** screen appears. Review the list of products that will be installed and the target installation directory. At the bottom of the list, the total amount of disk space that is required for the selected products is provided so that you can verify that adequate disk space is available. To install the products, click **Next** and the **Installation Progress** screen appears.

10 Upon completion, the **Installation Summary** shows informational messages such as successful confirmations, error messages, and warnings. Investigate any errors or warnings.

If **Next** appears, your system needs to be rebooted because one or both of the following tasks are pending on the system:

- A system-protected file was replaced during the installation and requires a restart.
- A pending restart was triggered by another application or by an operating system patch installation.

Click **Next** and then reboot your system. Otherwise, click **Finish** to exit the installation.

The installation program writes an install log file to the `BASEDIR/smarts/setup/logs` directory, unless the installation fails at the very start, in which case the installation program writes the log file to the `/tmp` directory. The log file is a text file with the naming convention `Install.<product>.<productversionNumber>.log`. 
If your product is part of a deployment that requires the Federal Information Processing Standard (FIPS) Publication 140-2, a U.S. government computer security standard governing cryptographic modules, follow the instructions in “Support for FIPS 140-2 for 9.5.1 products” on page 34.

Next steps on page 38 provides post-installation tasks.

Configuring Domains
Configuring domains
This section provides detailed information on configuring domains and includes the following topics:

- Creating a domain
- Modifying domains
- Deleting domains

Available domains defines the domains available.

Note The domains will be available in the Console only if SAM is started without an RPS file. For domains with existing RPS files, the domains will not be available. The INCHARGE-AM domain is enabled by default. All other domains are disabled.

<table>
<thead>
<tr>
<th>Domain</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INCHARGE-AM-PM</td>
<td>Availability and Performance Manager</td>
</tr>
<tr>
<td>INCHARGE-AM</td>
<td>Availability Manager</td>
</tr>
<tr>
<td>INCHARGE-DISCMGR</td>
<td>Discovery Manager</td>
</tr>
<tr>
<td>INCHARGE-MPLS-ANALYSIS</td>
<td>Analysis Server for MPLS 2.0</td>
</tr>
<tr>
<td>INCHARGE-MPLS-MONITORING</td>
<td>Monitoring Server for MPLS 2.0</td>
</tr>
<tr>
<td>INCHARGE-MPLS-TOPOLOGY</td>
<td>Topology Server for MPLS 2.0</td>
</tr>
<tr>
<td>INCHARGE-OI</td>
<td>Adapter Platform</td>
</tr>
<tr>
<td>INCHARGE-PM</td>
<td>Performance Manager</td>
</tr>
<tr>
<td>INCHARGE-MBIM</td>
<td>MBIM Manager</td>
</tr>
<tr>
<td>NCM</td>
<td>Network Connectivity Monitor</td>
</tr>
</tbody>
</table>

Note You can use sm_config utility to import domain configurations. However, VMware Corporation recommends that you create and modify domains using the Domain Creation Wizard and the Global Manager Administration Console. Creating a domain and Modifying domains provide detailed information.
To create a domain:

1. From the **Global Manager Administration Console**, click **Edit > New Domain**.
   The **Domain Creation Wizard** appears.

2. Type the name of the domain server in the **Domain Name** field.

3. Type the description of the domain in the **Domain Description** field, and click **Next**.
   
   **Note** To create a domain using the Copy Existing option, select an existing domain server from the **Copy Existing** list, type a **Domain Name**, and click **Finish**.

4. Click the domain type. Available options include:
   
   - **Use Default Type**
     
     **Note** This option is available only when copying an existing domain.
   
   - **Create New Type**
     
     If this option is selected, type the name of the domain type in the **Type Name** field.
     
     To copy an existing domain type, select an existing domain type from the **Copy Existing** list.
   
   - **Select Existing Type**
     
     If this option is selected, select a domain type from the **Select Type** list.

5. Click **Next**.

6. Type the tag string in the **Tag String** field.
   
   **Note** If a tag string is not specified, go to step 12.

7. Click **Next**.

8. Click the appropriate option. Available options include:
   
   - **Use Default Tag**
     
     **Note** This option only appears when a copied domain is selected or when the selected domain has an assigned tag.
   
   - **Create New Tag**
     
     Type a name in the **Tag Type Name** field. To copy an existing tag, select a tag from the **Copy Existing** list.
   
   - **Select Existing Tag**
     
     Select a tag from the **Select Tag** list.

9. Click **Next**.

10. Type description in the **Tag Description** field.

11. Type a matching tag pattern in the **Matching Pattern** field.
12 Click Next.

13 Select the groups this domain belongs to from the Available Groups list.

14 Click the group’s role. Available options include:
   - Topology Server
   - Monitoring Server
   - Analysis Server

   **Note** This step is only required if configured groups exist.

15 Click Add to move the group to the Selected Groups list.

16 Click Next.

   The instance that will be created when the domain creation process is complete is displayed.

   **Note** By default, the domain is enabled. If the domain is part of a domain group, it is only enabled if the domain group it belongs to is enabled. To disable the domain, clear its checkbox.

17 Click Finish.

Modifying domains

To modify a domain:

1 Open the Global Manager Administration Console.

2 From the Manager List, select the SAM Manager.

3 Expand ICS Configuration.

4 Expand IC Domain Configuration.

5 Expand Domains.

6 Click the appropriate domain.

   The Configure Domain interface appears, as illustrated in Figure 2-2. Global Manager Administration Console—Configure Domain interface.
Figure 2-2. Global Manager Administration Console—Configure Domain interface

7 Type the appropriate configurations.

Domain parameters describes the available Domain parameters.

Table 2-6. Domain parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Enables the domain.</td>
</tr>
<tr>
<td>Domain Description</td>
<td>Provides a description of the domain.</td>
</tr>
<tr>
<td>Domain Type</td>
<td>Defines the domain type.</td>
</tr>
<tr>
<td>Show Type Details</td>
<td>Displays the domain type information.</td>
</tr>
<tr>
<td>Tag Type</td>
<td>Defines the tag type.</td>
</tr>
</tbody>
</table>
Table 2-6. Domain parameters (continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag String</td>
<td>Defines the tag string.</td>
</tr>
<tr>
<td>Domain Groups</td>
<td>Defines the domain groups in which the domain is included. The table includes the following columns:</td>
</tr>
<tr>
<td></td>
<td>- T — Topology</td>
</tr>
<tr>
<td></td>
<td>- M — Monitoring</td>
</tr>
<tr>
<td></td>
<td>- A — Analysis</td>
</tr>
</tbody>
</table>

**Note** Click Add New to display the Add Domain Group dialog box. Select a Domain Group and click Delete Selected to remove a domain group.

1. Click the **Apply**.
2. Click **Reconfigure**.

**Note** Configuration changes are not applied until the **Reconfigure** button has been clicked. Clicking the **Reconfigure** button starts the data synchronization process. Click the **Reconfigure** button only after all updates to domains, domain tags, domain groups, and domain types have been made.

Deleting domains

To delete domains:

1. Open the **Global Manager Administration Console**.
2. From the Manager list, select the SAM Manager.
3. Expand **ICS Configuration**.
4. Expand **IC Domain Configuration**.
5. Expand **Domain**.
6. Click the appropriate domain.
7. Select **Edit > Delete**.

The selected domain is deleted.

**Note** Domains that refer to other domains cannot be deleted.

Configuring domain groups

A typical domain group comprises three servers—a topology server, an analysis server, and a monitoring server.

**Note** For more complex deployments, contact Custom Engineering.
The Configure Domain Group interface consists of a description of the domain group and three sections listing the topology servers, monitoring servers, and analysis servers. A typical MPLS deployment includes one of each type of server. The pane included on the left of the interface displays the default configuration of the Service Assurance Manager (SAM) server.

**Note** Most domain objects included in the default configuration are disabled (except INCHARGE-AM). The MPLS Group is disabled by default.

This section includes the following topics:

- Creating domain groups
- Modifying domain groups
- Deleting domain groups

### Creating domain groups

Use the Domain Groups Creation Wizard to create a new domain group. Using the wizard, you can:

- Copy an existing domain group and type a name for the new group. The wizard automatically creates the domains in the group.
- Manually create the component domains from within the wizard.

### Modifying domain groups

To modify a domain group:

1. Open the **Global Manager Administration Console**.
2. From the **Manager** list, select the SAM Manager.
3. Expand **ICS Configuration**.
4. Expand **IC Domain Configuration**.
5. Expand **Domain Groups**.
6. Click **INCHARGE-MPS**. The **Configure Domain Group** interface appears, as illustrated in Figure 2-3. Global Manager Administration Console—Configure Domain Group interface.
7 Type the appropriate configurations.

Domain Group parameters describes the available Domain Group parameters.

Table 2-7. Domain Group parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable</td>
<td>Enables the domain group. Enabling a domain group enables all the domains within it. Disabling the group disables domains included in the group as long as the domains are not members of any other enabled group. Disabling or enabling a domain, however, has no effect on groups of which that domain is a member.</td>
</tr>
<tr>
<td>Group Description</td>
<td>Provides a description of the domain group.</td>
</tr>
<tr>
<td>Topology Servers</td>
<td>Defines the topology servers.</td>
</tr>
<tr>
<td>Monitoring Servers</td>
<td>Defines the monitoring servers.</td>
</tr>
<tr>
<td>Analysis Servers</td>
<td>Defines the analysis servers.</td>
</tr>
</tbody>
</table>

**Note**  Click the Modify List button to display the Modify List of Topology Services dialog box. To remove a server from a list, select the server in the list and click the Removed Selected button.

1 Click the Apply.
2 Click **Reconfigure**.

**Note** Configuration changes are not applied until the **Reconfigure** button has been clicked. Clicking the **Reconfigure** button starts the data synchronization process. Click the **Reconfigure** button only after all updates to domains, domain tags, domain groups, and domain types have been made.

Deleting domain groups

To delete domain groups:

1 Open the **Global Manager Administration Console**.
2 From the **Manager** list, select the SAM Manager.
3 Expand **ICS Configuration**.
4 Expand **IC Domain Configuration**.
5 Expand **Domain Groups**.
6 Click the appropriate domain group.
7 Select **Edit > Delete**.

The selected domain group is deleted.

**Note** Domain groups that refer to other domains cannot be deleted.

Configuring domain types

A domain type is a configuration object that captures all the settings relevant to a particular type of domain with which the Service Assurance Manager server connects. One domain type exists for each class of server communicating; for example, AM, NPM, MPLS, and SIA.

Properties of a domain type include:

- DXA file
- Hook scripts
- Minimum certainty
- Smoothing intervals

**Note** The domain type does not instantiate a domain object.

*Default domain types* defines the default domain types.

<table>
<thead>
<tr>
<th>Domain type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INCHARGE-AM-PM-SUITE</td>
<td>Availability and Performance Manager</td>
</tr>
<tr>
<td>INCHARGE-AM-SUITE</td>
<td>Availability Manager</td>
</tr>
<tr>
<td>INCHARGE-DISCMGR-SUITE</td>
<td>Discovery Manager</td>
</tr>
</tbody>
</table>
Table 2-8. Default domain types (continued)

<table>
<thead>
<tr>
<th>Domain type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>INCHARGE-MPLS-ANALYSIS-SUITE</td>
<td>Analysis Server for MPLS 2.0</td>
</tr>
<tr>
<td>INCHARGE-MPLS-MONITORING-SUITE</td>
<td>Monitoring Server for MPLS 2.0</td>
</tr>
<tr>
<td>INCHARGE-MPLS-TOPOLOGY-SUITE</td>
<td>Topology Server for MPLS 2.0</td>
</tr>
<tr>
<td>INCHARGE-OI-SUITE</td>
<td>Open Integration Server</td>
</tr>
<tr>
<td>INCHARGE-PM-SUITE</td>
<td>Performance Manager</td>
</tr>
<tr>
<td>INCHARGE-SAM-MBIM-SUITE</td>
<td>Maintenance and Business Impact Manager</td>
</tr>
<tr>
<td>NCM-SUITE</td>
<td>NCM OEM</td>
</tr>
</tbody>
</table>

**Note**  Additional domain types previously configured in the ics.conf file are available as separately loadable XML files located in the conf/ics directory.

The following topics are included in this section:

- Creating domain types
- Modifying domain types
- Deleting domain types

Creating domain types

To create a domain type using the Domain Groups Creation Wizard:

1. From the **Global Manager Administration Console**, click **Edit > New Domain Type**. The **Domain Groups Creation Wizard** appears.

2. Select a type to be copied from the **Copy Existing** list.

3. Type a name in the **Type Name** field.

4. Type a description in the **Type Description** field.

5. Click **Next**.

6. Edit the domain type settings, and click **Next**.

**Domain type settings** defines the available domain type settings.

Table 2-9. Domain type settings

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>DXA File</td>
<td>Defines the DXA configuration file.</td>
</tr>
<tr>
<td>Hook Script: Enable</td>
<td>Enables the hook script.</td>
</tr>
</tbody>
</table>

**Note**  If the hook script is enabled, type the path for the hook script in the field.
Table 2-9. Domain type settings (continued)

<table>
<thead>
<tr>
<th>Option</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Certainty</td>
<td>Defines the minimum certainty. Default value: 0.01</td>
</tr>
<tr>
<td>Smoothing Interval</td>
<td>Defines the smoothing interval. Default value: 65</td>
</tr>
</tbody>
</table>

1. Select the servers from the **Available Domains** list.
2. Click **Add** to move the server to the **Selected Domains** list.
   
   This defines the servers associated with the new domain type.

   **Note**  Domains cannot be removed from a domain type—they can only be reassigned to another domain type. By adding domains, you are only reassigning the domains to a different domain type. Newly added domains display in green text. You can only delete domains displayed in green text. After clicking **Apply**, the domains cannot be deleted.

3. Click **Next**.
4. Click **Finish**. The configuration objects are created in the server.

Modifying domain types

To modify a domain type:

1. Open the **Global Manager Administration Console**.
2. From the **Manager** list, select the SAM Manager.
3. Expand **ICS Configuration**.
4. Expand **IC Domain Configuration**.
5. Expand **Domain Types**.
6. Click the appropriate **INCHARGE Domain Type**. The **Configure Domain Type** interface appears, as illustrated in Figure 2-4. **Global Manager Administration Console—Configure Domain Type interface**.
7 Type the appropriate configurations.

**Domain type configuration parameters** defines the available domain type configuration parameters.

**Table 2-10. Domain type configuration parameters**

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type Description</strong></td>
<td>Defines the domain type.</td>
</tr>
<tr>
<td><strong>DXA Configuration File</strong></td>
<td>Defines the DXA configuration file.</td>
</tr>
<tr>
<td><strong>Hook Script: Enable</strong></td>
<td>Enables the hook script.</td>
</tr>
<tr>
<td><strong>Minimum Certainty</strong></td>
<td>Defines the minimum certainty.</td>
</tr>
</tbody>
</table>

**Note** If the hook script is enabled, type the path for the hook script in the field.

**Default value:** 0.01
### Table 2-10. Domain type configuration parameters (continued)

<table>
<thead>
<tr>
<th>Parameters</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Smoothing Interval</td>
<td>Defines the smoothing interval. Default value: 65</td>
</tr>
<tr>
<td>Domains</td>
<td>Defines the domains associated with the domain type.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Click Modify List to add domains, select a domain from the list and click Remove Selected to remove domains, and click Restore to restore previously configured domains. Domains cannot be removed from a domain type, they can only be reassigned to another domain type.</td>
</tr>
</tbody>
</table>

1. Click **Apply**.
2. Click **Reconfigure**.
   **Note** Configuration changes are not applied until the **Reconfigure** button has been clicked. Clicking the **Reconfigure** button starts the data synchronization process. Click the **Reconfigure** button only after all updates to domains, domain tags, domain groups, and domain types have been made.

#### Deleting domain types

To delete domain tags:
1. Open the **Global Manager Administration Console**.
2. From the **Manager** list, select the SAM Manager.
3. Expand **ICS Configuration**.
4. Expand **IC Domain Configuration**.
5. Expand **Domain Types**.
6. Click the appropriate domain type.
7. Select **Edit > Delete**.
   The selected domain type is deleted.

**Note** Domain types that refer to other domains cannot be deleted.

#### Managing overlapping elements from separate underlying domains

A collects topology information from multiple underlying domains. In some cases, two or more of these domains can manage elements with the same name. Two such examples are IP networks, which are named using the network address, and partitions which are assigned names by the underlying domain.

For example, a service provider might use a private IP network address, such as 10.0.0.0, to provide IP addresses to different customers. When the same range of IP addresses are assigned to multiple customers, different topology elements may have the same IP address, and thus the same name.
Partitions are created and named by . All s use the same convention to name partitions. If the topologies of two domain managers each include partitions, it is possible that one or more of the partitions have the same name, as defined by the Name attribute. The provides more information about partitions.

By default, the treats elements with the same name from different underlying domains as a single instance, consolidating the relationships and attributes of the two elements to a single topological instance. The values for the attributes are taken from the underlying domain that performs the most recent topology synchronization.

You can, however, configure the to manage elements of the same name from different domains as distinct elements. By specifying a tag for one or both of the underlying domains, the will create two separate topology elements, each containing the attributes and relationships of the respective objects in the underlying domains. The tag that you specify is appended to the name of the objects in the tagged domain and displayed in the Global Console.

To tag managed elements, you need to complete two tasks:

- Specify a tag.
- Specify a matching pattern that will match the IP addresses and partitions to be tagged.

**Configuring domain tagging**

Domain tags allow to tag a subset of the topology of a given domain. Domain tags distinguish a topology subset from topology from an underlying domain which may have instance names that overlap but represent unique instances in the network topology.

A domain tag consists of a unique identifier and a wildcard expression that identifies matching instances.

The following topics are included in this section:

- Creating domain tags
- Modifying domain tags
- Deleting domain tags

Creating domain tags

To create a domain tag:

1. From the Global Manager Administration Console, click Edit > New Domain Tag.

   The Domain Tag Creation Wizard appears.

2. Type a name in the Tag Type Name field.

3. Type a description in the Tag Description field.

   **Note** To copy an existing tag, select a tag from the Copy Existing list.

4. Click Next.

5. Type a matching pattern for the domain tag in the Matching Pattern text box.
6 Click Next.

7 From the Available Domains list, select domains for which the domain tag applies.

**Note** For each domain selected, type a tag string in the Tag String field. If a domain has a tag string already associated with it, you can replace the domain tag associated with the tag string with this new one.

8 Click the Add button to move the selected domains to the Selected Domains list.

9 Click Next.

Instances that will be created when the create domain tag process is completed appear in this screen.

10 Click Finish.

Modifying domain tags

To modify domain tags:

1 Open the Global Manager Administration Console.

2 From the Manager list, select the SAM Manager.

3 Expand ICS Configuration.

4 Expand IC Domain Configuration.

5 Expand Domain Tags.

6 Click the appropriate domain tag.

The Configure Domain Tag interface appears, as illustrated by Figure 2-5. Global Manager Administration Console—Configure Domain Tag interface.
7 Type the appropriate configurations.

Domain Tag parameters describes the available Domain Tag parameters.

Table 2-11. Domain Tag parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Tag Description</td>
<td>Provides a description of the domain tag.</td>
</tr>
<tr>
<td>Matching Pattern</td>
<td>Defines the domain tag matching pattern.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Wildcard expressions are valid.</td>
</tr>
<tr>
<td>Domains</td>
<td>Defines the domains with which the domain tag is associated.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Click Add New to display the Add New Domain dialog box. Select a domain and click Edit Selected to display the Edit Domain dialog box. Select a domain and click Delete Selected to delete the selected domain.</td>
</tr>
</tbody>
</table>

1 Click **Apply**.
2 Click **Reconfigure**.

**Note**  
Configuration changes are not applied until the **Reconfigure** button has been clicked. Clicking the **Reconfigure** button starts the data synchronization process. Click the **Reconfigure** button only after all updates to domains, domain tags, domain groups, and domain types have been made.

Deleting domain tags

To delete domain tags:

1 Open the **Global Manager Administration Console**.
2 From the **Manager** list, select the SAM Manager.
3 Expand **ICS Configuration**.
4 Expand **IC Domain Configuration**.
5 Expand **Domain Tags**.
6 Click the appropriate domain tag.
7 Select **Edit > Delete**.

The selected domain tag is deleted.

**Note**  
Domain tags that refer to other domains cannot be deleted.

Reconfiguring the server

Any modifications to domains, domain groups, domain tags, and domain types are not implemented until the server has been reconfigured. You should reconfigure the server only after all modifications have been applied—not after each individual modification. When you click the **Launch Server Reconfiguration** toolbar button, the reconfigure process begins.

Click **View > Message Log** to display the Manager Message Log window. Configuration errors are displayed in this window.

**Note**  
The Service Assurance Manager server applies all reconfigurations during the restart process.

To reconfigure the server:

From the Global Manager Administration Console, click the **Launch Server Reconfiguration** toolbar button.

**Note**  
Click the **Launch Server Reconfiguration** toolbar button only after all modifications have been applied.

Procedure for opening the Global Console

This section explains how to open the Global Console in Windows and Unix platform.

To open the Global Console:
Procedure

1 Start the **Global Console**.

- On a Windows system, select **Start > Programs > InCharge > VMware Smart Assurance Global Console**.

  **To use timeout feature in Windows:**

  You can run the command `<BASEDIR>/smarts/bin/sm_gui.exe -Dsmarts.inactivityTimeout=<Time Duration in seconds>` on the command prompt, to set the timeout. If there is no activity on the console window for the time defined by the user, then the domain session will get disconnected from the console.

  For example: Run `<BASEDIR>/smarts/bin/sm_gui.exe -Dsmarts.inactivityTimeout=20`. This command disconnects the domain session after 20 seconds, if there is no activity on the console.

- On a UNIX system, go to the BASEDIR/smarts/bin directory in the Service Assurance Manager (Global Manager) installation area and type:

  `sm_gui`

  **To use timeout feature in Unix:**

  Run `<BASEDIR>/smarts/bin/sm_gui -Dsmarts.inactivityTimeout=<Time Duration in seconds>`, to set the timeout. If there is no activity on the console window for the time defined by the user, then the domain session will get disconnected from the console.

  For example: Run `<BASEDIR>/smarts/bin/sm_gui -Dsmarts.inactivityTimeout=20`. This command disconnects the domain session after 20 seconds, if there is no activity on the console.

  Press **Enter**.

**Note** In order to use the timeout feature in webconsole, you need to add `smarts.inactivityTimeout = number of seconds` in `<BASE-DIR>\CONSOLE\smarts\tomcat \webapps\webconsole\webconsole.properties` file. And, start or restart the Tomcat Server.

The Attach Manager dialog box opens, as shown in Figure **Attach Manager dialog box**.
In the dialog box:

a. Ensure that the VMware Smart Assurance Broker for your deployment appears in the **Broker** text box.

b. Click the **Manager** list box or the **Browse** button to display a list of active (running) Managers, and from that list select a Domain Manager (for example, **INCHARGE-AM**) or a Global Manager (for example, **INCHARGE-SA**) in your deployment as the Manager to which you want to connect.

c. Type your login username and password.

d. Click **OK**.

A console view opens.

**Results**

What console view opens at this point depends on whether you selected a Domain Manager or a Global Manager application.

If you selected a Domain Manager, a Topology Browser Console view of the Global Console will open by default, an example of which is shown in Figure *Topology Browser Console*. In the example display, the Topology Browser Console is attached to a Domain Manager named INCHARGE-AM.
If you selected a Global Manager, a Notification Log Console view of the Global Console will open by default, an example of which is shown in Figure Notification Log Console. In the example display, the Notification Log Console is attached to a Global Manager application named INCHARGE-SA.
The VMware Smart Assurance Service Assurance Manager Operator Guide provides detailed instructions on using the Global Console.

Installing SMARThS IP-AM

To install IP-AM, refer Performing an Installation.

Starting discovery from the console

From a Domain Manager Administration Console that is attached to the, you can use any of the following methods to manually invoke a discovery:

- To discover all managed systems, including those on the Pending Devices list, select Topology > Discover All.
- To discover all systems on the Pending Devices list, select
- Topology > Discover Pending.
- To discover a single system on the Pending Devices list, right-click the system on the Pending Devices list and then select Rediscover from the pop-up menu.
- To rediscover a single system in the topology tree, click the system and then select Topology > Rediscover.

You can also rediscover a system by right-clicking it and selecting Rediscover from the pop-up menu.
Starting discovery from the command line

From the command line, you can invoke a full discovery or a pending discovery by using the `dmctl` or `sm_tpmgr` utility. Doing so is useful if you want to schedule a full or pending discovery at a specific time by using batch processing or the `sm_sched` utility.

The `dmctl` and `sm_sched` utilities are described in the HTML pages that are located in the BASEDIR/smarts/doc/html/usage directory of any installation area.

Installing SMARTS ESM

To install ESM, refer to [Performing an Installation].

UI Components

Installing Global Console

This section describes how to install SAM Global console on Windows.

Procedure

1. To install SAM Global Console, refer to [Install using Wizard mode for SAM Console (Windows only)].
2. For launching SAM Global Console, refer to [Procedure for opening the Global Console].

Installing Notification UI

This section describes installation and configuration of VSA Notification UI component for Smarts SAM and Domain Managers.

MongoDB Installation

Refer to [Installing MongoDB].

Redis Installation

Refer to [Installing Redis].

Elastic Search

Refer to [Installing Elastic Search].

Kafka Installation

Refer to [Installing Kafka].

DCF Installation

Refer to [Installing Data Collection Framework].
Eventstore Installation
Refer, Installing Eventstore

viDM Installation
Refer Installing and Configuring VMware Identity Manager for Linux.

cAPI Installation
Refer, Installing cAPI

K4M Installation
Refer, Installing K4M.

Smarts UI Installation
Refer, Installing Smarts-UI

Installing Eventstore
This section describes how to install Eventstore.

Install Eventstore using Console Mode
You can install the Eventstore on the platform of supported Linux hosts. One server can support only one instance of Eventstore installation.

Prerequisites
Fulfill the following prerequisites before starting the installation:

1. Installation server must have java version 1.8+ installed.
   If not installed, type `yum install -y java-1.8.0-openjdk.x86_64` to install java 1.8.

2. Installation server must support bash, sed and curl utility.

3. Elastic Search - version 6.4.2 must be installed. Refer, Installing Elastic Search for more information.
   Download free Open Source Elastic Search 6.4.2 rpm from https://artifacts.elastic.co/downloads/elasticsearch/elasticsearch-oss-6.4.2.rpm.
   a. User name and password authentication must be enabled for Elastic Search.
   b. Minimum 3 node Elastic Search Cluster is required for high availability.

4. Redis - version 5.0.5 must be installed and running. Refer, Installing Redis for more information.
   a. Password Authentication must be enabled for Redis.
   b. For Redis minimum 6 node (3 Primary, 3 Secondary) cluster is required which can be deployed over 3 machines.
Kafka - version 2.0.0 must be installed and running. Refer, Installing Kafka for more information.

a. SASL/PlainText based authentication must be enabled in kafka.

b. A topic must be created with 1 partition.

c. Zookeeper must be running.

d. Minimum 3 node Kafka Broker is required for high availability. In Cluster mode, it is recommended to create a topic with 1 partition and 3 replication factor.

e. Optional: Enabling SSL (encryption) using SASL/SSL mechanism between Kafka Broker and Clients with 1-way authentication is also supported.

Smarts Presentation SAM must be already running.

a. EDAA must be enabled and-smarts tomcat service must be running.

b. Optional: Enabling HTTPS in EDAA is also supported.

Copy the `eventstore-install.bin` installer to any directory on the server where Eventstore can be installed.

Ensure that you have a login with root privileges to run the installer.

Download the installation file from support.vmware.com and place it in a temporary location on the server.

Procedure

1. Login to the server as root.

2. Type `bash eventstore-install.bin -i console` to run the installer in the console-based installer mode and hit Enter.

   The command prompt screen appears.

3. Press Enter.

   Installer introduction continues.

4. Press Enter to accept the default location when Installer prompts to choose an Install folder or provide the desired location.

   This is the location where you can find Eventstore is installed.

5. If the Install folder already contains Eventstore folder, installer prompts for the below selections.

   - Enter 1 to override the already installed folder and Press Enter to continue.
   - or Enter 2 to choose a new installation directory and Press Enter to continue.
   - or Enter 3 to cancel the installation and Press Enter.
6 Press Enter to continue when installer prompts to enter the Eventstore port.

This is the port in which Eventstore service starts. Port number must be between 1 to 65535. If wrong port number is entered, Installer will throw a validation error and redirect to re-enter the Port details. Default port is 8080.

7 The installer prompts to choose the protocol for communication:

- Choose option 1 for https communication and Press Enter to continue.
  
  or
  
- Choose option 2 for http communication Press Enter to continue.

**Note** 1. Default is http. For “https” you must ensure that “esdb.crt” file is available in “/opt/ssl”. For configuring https in Elastic Search refer section Enabling HTTPS In Elastic Search.

**Note** 2. The certificate file esdb.crt must contain certificates from all elastic search instances in a cluster.

8 Installer prompts for Elastic Search Configurations.

- Enter the Elastic search IP or FQDN or Hostname in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>. In case of cluster enter the comma separated IP or FQDN or Hostname address.

- Type the Elastic Search Username and press Enter to continue.

  (To enable ES authentication refer Elasticsearch Authentication).

9 Enter the Elastic Search Password when prompted and confirm Elastic Search Password when prompted for confirmation.

If Passwords are mismatched, installer throws a validation error and redirect to re-enter the password. Verify if any fields are blank to avoid the installer validation error and redirection of step 8.

Also verify if the first IP/fqdn/hostname address of Elastic Search entered, is reachable from Installation server. Otherwise, installer will throw a connectivity error, and redirect to at the beginning of step 8.

10 Provide Redis IP Address and press Enter to continue when installer prompts to enter Redis configuration.

  In case of Redis cluster enter the Comma separated IP in the format
  
  <IP-ADDRESS>:<PORT>

  Default is 127.0.0.1:6379
(For redis authentication refer *Redis Cluster Authentication*).

**Note** 1. Eventstore supports only Redis Cluster with 3 Redis primary instance. A single non-cluster redis instance is not supported.

**Note** 2. Verify if you have entered the IP address in a correct format. Otherwise, installer throws a validation error and redirects to this step again.

11 Enter **Redis Password** and confirm **Redis Password** again when installer prompts. Press Enter to continue.

**Note** Installer throws a validation error and redirect to the beginning of step 11 if the passwords are mismatching.

12 Installer prompts to enter the Kafka SASL configuration. You can choose SASL_PLAINTEXT or SASL_SSL for Kafka communication.

SASL_PLAINTEXT: User name and Password authentication without encryption of data.

SASL_SSL: User name and Password authentication with SSL encryption.

For SSL encrypted communication ensure that "kafka.crt" file is available in "/opt/ssl". Default is SASL_SSL.

- Choose 1 for SASL_PLAINTEXT, press Enter to continue.
  
  (For Enabling Kafka authentication using SASL/PLAINTEXT, refer Kafka SASL_PLAIN Authentication Configuration).

  or

- Choose 2 for SASL_SSL Enter the KAKFA TOPIC, press Enter to continue.
  
  (For Enabling Kafka authentication with SSL Encryption using SASL/SSL, refer Kafka SASL_SSL Authentication Configuration).

13 Installer prompts to enter the kafka configuration:

a Enter **KAKFA ADDRESS**.

Kafka IP/fqdn/hostname address must be in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>.

For Kafka cluster enter the comma separated address.

b Enter **KAKFA TOPIC**. Default is sam_notification.

**Note** The topic must be already created with 1 partition only.

c Enter **KAFKA Username**, press Enter to continue.
14 Enter the **Kafka Password** and Confirm **Kafka Password** when Installer prompts for confirmation.

If Passwords are mismatched, installer throws a validation error and redirect to the beginning of step 14.

15 Installer prompts for the choice of communication protocol https and default (http)

- Enter 1 for https and press Enter to continue. For **https**, ensure that “sam.crt” is available in “/opt/ssl”.

  To import the SAM certificate refer [Enabling HTTPS in SAM](#).

  or

- Enter 2 for **http** and press Enter to continue. Http is default.

16 Enter the presentation **SAM configuration details** when Installer prompts. Enter the IP/fqdn/hostname address for SAM in the format `<IP-ADDRESS/FQDN/HOSTNAME>:<PORT>`). Press Enter to continue.

If any input fields are empty, installer throws a validation error and redirects to the beginning of this step 16.

**Note** In SAM, Port 8080 is enabled in http mode and Port 8443 is enabled in https mode.

17 Press Enter to continue when Pre install summary is displayed.

Installation continues.

18 Press Enter to exit the installer.

Install Completed message is displayed.

**What to do next**

After successful EventStore installation, install 3 elastic search plugins on all elastic search instances in the cluster by following these steps:

1 Copy the plugins directory containing "ChainingSupport-6.4.2.zip, elasticsearch-arrayformat-6.4.2.zip and elasticsearch-userprofile-6.4.2.zip" from "<EventStore_INSTALL_DIR>/evenstore/plugins/" to the `<PLUGIN-DIRECTORY>` where Elastic Search is running. Here `<PLUGIN-DIRECTORY>` can be any directory.

2 After copying run the following command to install each plugin:

   1. `/path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN DIRECTORY>/plugins/ChainingSupport-6.4.2.zip`
   2. `/path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN DIRECTORY>/plugins/elasticsearch-arrayformat-6.4.2.zip`
   3. `/path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN DIRECTORY>/plugins/elasticsearch-userprofile-6.4.2.zip`
3 After installing all the plugins restart the **Elastic Search Service** on all cluster nodes.

**Install Eventstore using Graphical Mode**

This installation procedure describes the steps of Eventstore installation in the Graphical Interface. One server can support only one instance of Eventstore installation.

**Prerequisites**

- Ensure that you have a login with root privileges to run the installer.
- Download the installation file from [support.vmware.com](http://support.vmware.com) and place it in a temporary location on the server.

**Procedure**

1. Log in to the server as root.
   
   Logged in with root privileges.

2. Type `bash eventstore-install.bin -i gui` to run the installer in the graphical installer mode, and press **Enter**.
   
   Installer introduction appears.

3. Click **Next**.
   
   Installer introduction continues.

4. Installer prompts to choose an install folder, click **Next** to continue with the Default folder.
   
   Default is `/opt/eventstore`.

5. If the install folder already contains eventstore folder you can choose appropriate options from any of the following:
   
   - Click **Yes** to override the already installed folder.
   
   or
   
   - Click **No** to choose a new installation directory.
   
   or
   
   - Click **Cancel** to cancel the installation.

6. Click **Next** to continue when installer prompts to enter the eventstore port.
   
   This is the port in which eventstore service starts. Port number must be between 1 to 65535. If wrong port number is entered, installer will throw a validation error and redirect to re-enter the Port details. Default port is 8080.

7. The Installer prompts you to choose any of the below protocol for communication.
   
   - Click “https” radio button for https communication and click **Next** to continue.
   
   or
- Click “http” radio button for http communication and click **Next** to continue.

**Note** 1. For “https” communication ensure that “esdb.crt” file is available in “/opt/ssl”. (For configuring https in elastic search refer [Enabling HTTPS In Elastic Search](#)).

**Note** 2. The certificate file esdb.crt should contain certificates from all elastic search instances in a cluster.

8 Installer prompts for Elastic Search Configurations:

a  Enter the Elastic search IP or FQDN or Hostname in the format `<IP-ADDRESS/FQDN/HOSTNAME>:<PORT>`. In case of cluster enter the comma separated IP or FQDN or Hostname address.

b  Type the **Elastic Search Username** and click **Next** to continue. (To enable ES authentication refer [#unique_185](#)).

9 Enter the **Elastic Search Password** when installer prompted and click **Next** to continue.

Password confirmation prompt appears.

10 Enter **Elastic Search Password** again when prompts for confirmation and click **Next** to continue.

Installer throws a validation error and redirects to the beginning of step 9 if the password mismatches. Verify if any fields are blank to avoid the installer validation error and redirects to step 8.

Also verify if the first IP/fqdn/hostname address of Elastic Search entered, is reachable from Installation server. Otherwise, installer will throw a connectivity error, and redirects to the beginning of step 8.

11 Enter **Redis IP address** when installer prompts for Redis configurations and click **Next** to continue.

For Redis cluster enter the Comma separated IP in the format `<IP-ADDRESS>:<PORT>` Default is 127.0.0.1:6379 (For redis authentication refer [Redis Authentication](#)).

**Note** 1. Eventstore supports only Redis Cluster with 3 Redis primary instance. A single non-cluster redis instance is not supported.

**Note** 2. Verify if you have entered the IP address in a correct format. Otherwise, installer throws a validation error and redirects to this step again.

12 Enter the **Redis Password** when installer prompts and click **Next** to continue.

Installer prompts for password confirmation.

13 Enter **Redis Password** when prompts for confirmation and click **Next** to continue.

Installer throws a validation error and redirects to the beginning of step 12 if the passwords are mismatched.
14 Installer prompts to enter Kafka SASL Configuration. You can choose SASL_PLAINTEXT or SASL_SSL for Kafka communication.

SASL_PLAINTEXT: User name and Password authentication without encryption of data.
SASL_SSL: User name and Password authentication with SSL encryption.

For SSL encrypted communication ensure that "kafka.crt" file is available in "/opt/ssl". Default is SASL_SSL.

a Click SASL_PLAINTEXT radio button for SASL_PLAINTEXT, click Next to continue.
   (For Enabling Kafka authentication using SASL/PLAINTEXT, refer Kafka SASL_PLAIN Authentication Configuration).

or

b Click SASL_SSL radio button for SASL_SSL, click Next to continue.
   (For Enabling Kafka authentication with SSL Encryption using SASL/SSL, refer Kafka SASL_SSL Authentication Configuration).

15 Installer prompts to enter the kafka configuration.

a Enter KAKFA ADDRESS. Kafka IP/fqdn/hostname address must be in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>. For Kafka cluster enter the comma separated address.

b Enter KAKFA TOPIC. Default is sam_notification.

   Note The topic must be already created with 1 partition only.

c Enter KAFKA Username, click Next to continue.

   Note Installer throws a validation error if any input fields are empty and redirects to the beginning of this step 15.

16 Enter the KAFKA Password when installer prompts and click Next to continue.

   Installer prompts for password confirmation.

17 Enter KAFKA Password again when prompts for confirmation and click Next to continue.

   Installer throws a validation error and redirects to the beginning of step 12 if the passwords are mismatched.

18 Installer prompts to choose the communication protocol for presentation SAM. Default is http.

   - Click https radio button for https communication and Click Next to continue.
     For https, ensure that “sam.crt” is available in /opt/ssl. To import the SAM certificate refer Enabling HTTPS in SAM.

   or

   - Click http radio button for http communication and Click Next to continue.
19 Enter the presentation **SAM configuration details** when Installer prompts. Enter the IP/fqdn/hostname address for SAM in the format `<IP-ADDRESS/FQDN/HOSTNAME>:<PORT>)`. Click **Next** to continue.

Installer throws a validation error if any input fields are empty and redirects to the beginning of this step 19.

**Note** In SAM Port 8080 is enabled in http mode and Port 8443 is enabled in https mode.

20 Click **Next** to continue when Pre install summary is displayed.

Installation continues.

21 Click **Done** to exit the Installer.

Install Completed message is displayed.

**What to do next**

After successful EventStore installation, install 3 elastic search plugins on all elastic search instances in the cluster by following these steps:

1 Copy the plugins directory containing "ChainingSupport-6.4.2.zip, elasticsearch-arrayformat-6.4.2.zip and elasticsearch-userprofile-6.4.2.zip" from "<EventStore_INSTALL_DIR>/evenstore/plugins/" to `<PLUGIN-DIRECTORY> where Elastic Search is running.

Here `<PLUGIN-DIRECTORY>` can be any directory.

2 After copying Run the following command to install each plugin:

   1. `/path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN DIRECTORY>/plugins/ChainingSupport-6.4.2.zip`
   2. `/path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN DIRECTORY>/plugins/elasticsearch-arrayformat-6.4.2.zip`
   3. `/path/to/elasticsearch/bin/elasticsearch-plugin install file:///<PLUGIN DIRECTORY>/plugins/elasticsearch-userprofile-6.4.2.zip`

3 After installing all the plugins Restart the **Elastic Search Service** on all cluster nodes.

**Install Eventstore in Silent Mode**

A silent installation is an installation procedure that continues without user interaction. It requires no user intervention from start to finish. This installation is performed using a user-modifiable response file, which enables you to easily duplicate the installation on many computer systems.
<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER_INSTALL_DIR</td>
<td>Install directory for eventstore.</td>
</tr>
<tr>
<td>ES_PROTOCOL</td>
<td>Choose the protocol (http/https) for Elastic Search communication.</td>
</tr>
<tr>
<td></td>
<td>For https communication ensure that &quot;esdb.crt&quot; certificate is available on &quot;/opt/ssl&quot;.</td>
</tr>
<tr>
<td></td>
<td>For https set ES_PROTOCOL to &quot; https&quot;.</td>
</tr>
<tr>
<td></td>
<td>For http set ES_PROTOCOL to &quot; http &quot;.</td>
</tr>
<tr>
<td>ES_CERT_FILE</td>
<td>If https is enabled for ES then set the CERT FILE location else leave it blank.</td>
</tr>
<tr>
<td></td>
<td>For example, ES_CERT_FILE=/opt/ssl/esdb.crt.</td>
</tr>
<tr>
<td>EVENTSTORE_PORT_NO</td>
<td>Event Store Port.</td>
</tr>
<tr>
<td></td>
<td>Enter the port number in which you want to start the Event Store.</td>
</tr>
<tr>
<td>ES_ADDRESS</td>
<td>Elastic search IP/fqdn/hostname address in the format &lt;IP-ADDRESS/FQDN/HOSTNAME&gt;:&lt;PORT&gt;</td>
</tr>
<tr>
<td></td>
<td>For Elastic search cluster, enter the comma separated address.</td>
</tr>
<tr>
<td>ES_USER_NAME</td>
<td>Elastic search user name.</td>
</tr>
<tr>
<td>ES_PASSWORD</td>
<td>Elastic Search Password.</td>
</tr>
<tr>
<td>REDIS_IP_ADDRESS</td>
<td>REDIS IP ADDRESS.</td>
</tr>
<tr>
<td></td>
<td>Example: 127.0.0.1:6379</td>
</tr>
<tr>
<td></td>
<td>For Redis cluster, enter the comma separated IP in the format &lt;IP-ADDRESS&gt;:&lt;PORT&gt;.</td>
</tr>
<tr>
<td>REDIS_PASSWORD</td>
<td>Redis Password.</td>
</tr>
<tr>
<td>KAFKA_SASL_PROTOCOL</td>
<td>Kafka SASL Configuration.</td>
</tr>
<tr>
<td></td>
<td>For SSL encrypted communication, ensure that &quot;kafka.crt&quot; file is available in &quot;/opt/ssl&quot;.</td>
</tr>
<tr>
<td></td>
<td>Set KAFKA_SASL_PROTOCOL to SASL_PLAINTEXT or SASL_SSL.</td>
</tr>
<tr>
<td></td>
<td>SASL_PLAINTEXT : User name and Password authentication without encryption of data.</td>
</tr>
<tr>
<td></td>
<td>SASL_SSL: User name and Password authentication with SSL encryption.</td>
</tr>
<tr>
<td></td>
<td>Example: KAFKA_SASL_PROTOCOL=SASL_SSL</td>
</tr>
<tr>
<td>KAFKA_ADDRESS</td>
<td>KAFKA IP ADDRESS.</td>
</tr>
<tr>
<td></td>
<td>For Kafka cluster, enter the comma separated IP/fqdn/hostname in the format &lt;IP-ADDRESS/FQDN/HOSTNAME&gt;:&lt;PORT&gt;.</td>
</tr>
<tr>
<td>KAFKA_TOPIC</td>
<td>KAFKA Topic.</td>
</tr>
<tr>
<td></td>
<td>Example: KAFKA_TOPIC =sam_notification.</td>
</tr>
<tr>
<td>KAFKA_USER_NAME</td>
<td>KAFKA User Name.</td>
</tr>
<tr>
<td>KAFKA_PASSWORD</td>
<td>Kafka Password.</td>
</tr>
<tr>
<td>SAM_PROTOCOL</td>
<td>Choose the protocol ( http/https) for SAM communication.</td>
</tr>
<tr>
<td></td>
<td>For https communication, ensure that &quot; sam.crt&quot; certificate is available on &quot;/opt/ssl&quot;.</td>
</tr>
<tr>
<td></td>
<td>For https set SAM_PROTOCOL to &quot; https&quot;.</td>
</tr>
<tr>
<td></td>
<td>For http set SAM_PROTOCOL to &quot; http &quot;.</td>
</tr>
<tr>
<td>SAM_CERT_FILE</td>
<td>If https is enabled for SAM then set the CERT FILE location else leave it blank.</td>
</tr>
<tr>
<td></td>
<td>Example: SAM_CERT_FILE =/opt/ssl/sam.crt.</td>
</tr>
<tr>
<td>SAM_ADDRESS</td>
<td>SAM IP ADDRESS.</td>
</tr>
<tr>
<td></td>
<td>Enter the the IP/fqdn/hostname address in the format &lt;IP-ADDRESS/FQDN/HOSTNAME&gt;:&lt;PORT&gt;.</td>
</tr>
</tbody>
</table>
Prerequisites

Create a configuration file for the installer to execute the installation. To create configuration file:

1. Copy the sample configuration file from the distribution eventstore-installer.properties to a directory on the server where you are installing eventstore.
2. Use any editor (vi/vim) to modify this file.
3. Define each of the properties in this file, according to Table - Variables Property and Description.
4. Save the changes to the file.

Procedure

1. Login to the server as root.
2. Type `bash eventstore-install.bin -f <response file location> -i silent` and press Enter.

   **Note** Any user interaction is not required for this installer. Once it completes, a message displays indicating that installation is completed, and you are returned to the shell prompt. If the installer is unable to complete the installation, an error message is saved in the [Product directory]/eventstore_logs.

What to do next

After successful EventStore installation, install 3 elastic search plugins on all elastic search instances in the cluster by following these steps:

1. Copy the plugins directory containing "ChainingSupport-6.4.2.zip, elasticsearch-arrayformat-6.4.2.zip and elasticsearch-userprofile-6.4.2.zip" from "<EventStore_INSTALL_DIR>/evenstore/plugins/" to <PLUGIN-DIRECTORY> where Elastic Search is running.
   
   Here <PLUGIN-DIRECTORY> can be any directory.
2. After copying Run the following command to install each plugin:

<table>
<thead>
<tr>
<th>Path</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. /path/to/elasticsearch/bin/elasticsearch-plugin install file:///&lt;PLUGIN DIRECTORY&gt;/ plugins/ChainingSupport-6.4.2.zip</td>
</tr>
<tr>
<td>2. /path/to/elasticsearch/bin/elasticsearch-plugin install file:///&lt;PLUGIN DIRECTORY&gt;/ plugins/elasticsearch-arrayformat-6.4.2.zip</td>
</tr>
<tr>
<td>3. /path/to/elasticsearch/bin/elasticsearch-plugin install file:///&lt;PLUGIN DIRECTORY&gt;/ plugins/elasticsearch-userprofile-6.4.2.zip</td>
</tr>
</tbody>
</table>

3. After installing all the plugins Restart the Elastic Search Service on all cluster nodes.

Installing cAPI

This section provides information on how to install cAPI.
Install cAPI using Console Mode

You can install cAPI on supported Linux Platform. Console mode provides a text-based method for invoking the installation program. This mode is intended for Linux platforms with non-graphics consoles.

Prerequisites

Fulfill the following prerequisites before starting the installation:

1. Ensure Event store is installed already.
2. Ensure that minimum 3 node elastic search cluster is already installed.
3. Ensure java version 1.8+ is already installed.
4. Ensure bash and curl utility are already installed and installation server is compatible with "sed" command.
5. Create Client Id and Shared Secret in VIDM for cAPI.
   Refer the #unique_188.
6. Copy the "cAPI-install.bin " installer to any directory on the server where cAPI will be installed.
7. Ensure that you have a login with root privileges to run the installer.
8. Download the installation file from support.vmware.com and place it in a temporary location on the server.

Procedure

1. Login to the server as root.
   Logged in with root privileges.

2. Type bash cAPI-install.bin  -i console to run the installer in the console-based installer mode, press Enter.
   Installer introduction appears.

3. Press Enter to continue.
   Installer Prompts to choose an install folder.

4. Press Enter to continue.
   This is the location where cAPI will be installed. Default is /opt/cAPI.

5. If install folder already contains cAPI folder, choose from the following options
   - Enter 1 to override the already installed folder.
   or
   - Enter 2 to choose a new installation directory.
   or
Enter 3 to cancel the installation.

6 Installer prompts for cAPI configuration.
   a Enter cAPI ADMIN port. Default port 9901.
   b Enter cAPI Listener port. Default port 10000.
   c Press Enter to continue.

   Note  The port number must be between 1 to 65535. Otherwise, installer throws validation
   error and redirects to this step to re-enter the port details.

7 Installer prompts to enter the cAPI configuration.
   a Enter VIDM HOST NAME. Default is identitymanager.eng.vmware.com.
   b Enter the VIDM IP ADDRESS. Default is 127.0.0.1
   c Enter the VIDM PORT. Default port is 443.
   d Press Enter to continue.

   Note  If the IP address is wrong or the Port is invalid, installer throws validation error and
   redirects to the beginning of this step to enter the configurations.

8 Choose the Elastic Search https Configuration when installer prompts. Default is http.
   a Choose 1 for https and Press Enter to continue.
      or
   b Choose 2 for http and Press Enter to continue.

   Note  1. For https communication in Elastic search ensure that "esdb.crt" file is available in
   
   Note  2. The certificate file esdb.crt should contain certificates from all elastic search
   instances in a cluster.

9 Installer prompts for Elastic Search configurations.
   a Enter the Elastic search IP/fqdn/hostname in the format <IP-ADDRESS/FQDN/HOSTNAME>:<PORT>. In case of cluster, enter the comma separated IP/fqdn/hostname
   address.
   b Enter Elastic Search User name and press Enter to continue.
      To enable ES authentication, refer #unique_185.

   Note  Installer throws validation error and redirects to the beginning of this step to enter the
   configurations if any input fields are left blank.

10 Enter the Elastic Search Password when installer prompts, press Enter to continue.

   Installer prompts for password confirmation.
11 Press Enter to continue.

If the passwords are mismatched, installer throws a validation error and redirects to re-enter the password at step 10.

12 Enter EventStore configuration when installer prompts.
   a Enter Event Store IP Address. Default is 127.0.0.1.
   b Enter Event Store Port. Default is 8080.
   c Press Enter to continue.

   Note  If the IP address is wrong or the Port is invalid, installer throws validation error and redirects to the beginning of this step to enter the configurations.

13 Installer prompts to enter the Client Registration configuration.
   a Provide Client ID. Default is capi_client.
   b Provide Secret and press Enter to continue.

   Note  Client ID and Secret is a one-time configuration of an Oauth2 client that supports password grant on VIDM.

   Refer #unique_188 for configuration details.

   Installer throws an error and redirects to the beginning of this step to enter the configurations if any input filed left blank.

14 Press Enter to continue the installation when installer shows the pre-install summary.

   Installation continues.

15 Press Enter to exit the installer when installer shows the installation is completed.

   cAPI is installed.

Install cAPI using Graphical Mode
This installation procedure describes the steps of cAPI installation in the Graphical Interface.

Prerequisites
- Ensure that you have a login with root privileges to run the installer.
- Download the installation file from support.vmware.com and place it in a temporary location on the server.

Procedure
1 Log in to the server as root.
   Logged in with root privileges.
2 Type `bash cAPI-install.bin -i gui` to run the installer in the graphical mode, press **Enter**. Introduction to the installer appears.

3 Click **Next** to continue.

4 Click **Choose**.

   This is the location where cAPI will be installed. Default is /opt/cAPI.

5 Click **Next** to continue.

   Installer checks if any cAPI folder existing inside install folder.

6 If install folder already contains cAPI folder, choose from the following options:
   - Click **Yes** to override the already installed folder.
   - Click **No** to choose a new Installation directory.
   - Click **Cancel** to cancel the Installation.

7 Installer prompts for cAPI configuration.
   a Enter **cAPI ADMIN port**. Default port 9901.
   b Enter **cAPI Listener port**. Default port 10000.
   c Click **Next** to continue.

   **Note** The port number must be between 1 to 65535. Otherwise, installer throws validation error and redirects to this step to re-enter the port details.

8 Installer prompts to enter the cAPI configuration.
   a Enter **VIDM HOST NAME**. Default is identitymanager.eng.vmware.com.
   b Enter the **VIDM IP ADDRESS**. Default is 127.0.0.1.
   c Enter the **VIDM PORT**. Default port number is 443.
   d Click **Next** to continue.

   **Note** If the IP address is wrong or the Port is invalid, installer throws validation error and redirects to the beginning of this step to enter the configurations.

9 Choose the Elastic Search https Configuration when installer prompts. Default is http.
   - Click **https** radio button for https communication and Click **Next** to continue.
   or
- Click **http** radio button for http communication and Click **Next** to continue.

**Note** 1. For https communication in Elastic search ensure that "esdb.crt" file is available in "/opt/ssl". For configuring https refer Enabling HTTPS In Elastic Search.

**Note** 2. The certificate file esdb.crt should contain certificates from all elastic search instances in a cluster.

**10** Installer prompts for Elastic Search configurations.

a  Enter the Elastic search IP/fqdn/hostname in the format `<IP-ADDRESS/FQDN/HOSTNAME>:<PORT>`. In case of cluster enter the comma separated IP/fqdn/hostname address.

b  Enter Elastic Search **User name** and click **Next** to continue.

To enable ES authentication refer the **#unique_185**.

**Note** Installer throws validation error and redirects to the beginning of this step to enter the configurations if any input filed left blank.

**11** Enter the **Elastic Search Password** when installer prompts, click **Next** to continue.

Installer prompts for password confirmation.

**12** Confirm **Elastic Search Password** when installer prompts for confirmation, click **Next** to continue.

If the passwords are mismatched, installer throws a validation error and redirects to re-enter the password at step 11.

**13** Enter EventStore configuration when installer prompts.

a  Enter **Event store IP address**. Default is 127.0.0.1.

b  Enter **Event store port**. Default is 8080.

c  Click **Next** to continue.

If the IP address is wrong or the Port is invalid, installer throws validation error and redirects to the beginning of this step to enter the configurations.

**14** Installer prompts to enter the Client Registration configuration.

a  Provide Client ID. Default is capi_client.

b  Provide **Secret** and click **Next** to continue.

**Note** Client ID and Secret is a one-time configuration of an Oauth2 client that supports password grant on VIDM. Refer **#unique_188** for configuration details.

Installer throws an error and redirects to the beginning of this step to enter the configurations if any input filed is left blank.
15 Click **Install** to continue the installation when displays pre-install summary.

   Installation continues.

16 Click **Done** to exit the installer.

   Installer displays installation is completed.

**Install cAPI in Silent Mode**

A silent installation is an installation procedure that continues without user interaction. It requires no user intervention from start to finish. This installation is performed using a user-modifiable response file, which enables you to easily duplicate the installation on many computer systems.

**Table 2-13. Variables Property and Description**

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER_INSTALL_DIR</td>
<td>Install directory for cAPI.</td>
</tr>
<tr>
<td>ADMIN_PORT</td>
<td>Admin Port: cAPI admin port.</td>
</tr>
<tr>
<td>LISTENER_PORT</td>
<td>Listener Port: cAPI client port, where cAPI listens incoming request.</td>
</tr>
<tr>
<td>VIDM_HOST_NAME</td>
<td>VIDM Host Name. Example: identitymanager.eng.vmware.com.</td>
</tr>
<tr>
<td>VIDM_IP_ADDRESS</td>
<td>VIDM IP Address (example: 127.0.0.1)</td>
</tr>
<tr>
<td>VIDM_PORT</td>
<td>VIDM Port</td>
</tr>
<tr>
<td>ES_PROTO</td>
<td>Choose the protocol for communication. For https communication ensure that &quot;esdb.crt&quot; certificate is available on &quot;/opt/ssl&quot;. For https set ES_PROTO to &quot;https&quot;. For http set ES_PROTO to &quot;http&quot;.</td>
</tr>
<tr>
<td>ES_ADDRESS</td>
<td>Elastic Search IP Address. For Elastic search cluster, please use the comma separated IP/fqdn/hostname in the format: &lt;IP-ADDRESS/FQDN/HOSTNAME&gt;:&lt;PORT&gt;.</td>
</tr>
<tr>
<td>ES_USER_NAME</td>
<td>Elastic Search User Name.</td>
</tr>
<tr>
<td>ES_PASSWORD</td>
<td>Elastic Search Password.</td>
</tr>
<tr>
<td>EVENTSTORE_IP_ADDRESS</td>
<td>EventStore IP Address.</td>
</tr>
<tr>
<td>EVENTSTORE_PORT</td>
<td>EventStore Port.</td>
</tr>
<tr>
<td>CLIENT_ID</td>
<td>Client ID.</td>
</tr>
</tbody>
</table>

**Note** Client registration configuration. ClientID and Secret is onetime configuration of an Oauth2 client that supports password grant on vIDM.

| SECRET               | Secret.                                                                     |
Prerequisites

Create a configuration file for the installer to execute the installation. To create configuration file:

1. Copy the sample configuration file from the distribution `cAPI-installer.properties` to a directory on the server where you are installing `cAPI`.
2. Use any editor (vi/vim) to modify this file.
3. Define each of the properties in this file, according to Table - Variables Property and Description.
4. Save the changes to the file.

Procedure

1. Log in to the server as root.
2. Type `bash cAPI-install.bin -f <response file location> -i silent` and press Enter.

   **Note** Any user interaction is not required for this installer. Once it completes, a message displays indicating that installation is completed, and you are returned to the shell prompt. If the installer is unable to complete the installation, an error message is saved in the `[Product directory]/cAPI_logs`.

Installing Smarts-UI

Install Smarts-UI using Console Mode

You can install Smarts-UI on supported Linux Platform. This procedure describes Smarts-UI installation in Console Mode.

Prerequisites

Fulfill the following prerequisites before starting the installation:

1. Ensure Eventstore and `cAPI` are already installed on the Installation server.
2. Ensure java version 1.8+ is already installed on the Installation server.
3. Ensure bash is already installed on the Installation server.
4. Ensure bash and curl utility are already installed and installation server is compatible with "sed" command.
5. SE Linux must be disabled in installation server.
6. Create Client Id and Shared Secret in VIDM for smarts-ui installation. Refer `#unique_192`.
7. Copy the "`smartsui-install.bin`" installer to any directory on the server where smarts-ui will be installed.
8. KPI should be installed and running. For KPI installation refer to VMware-K4M-1.0.0.0-Installation-and-Administration-Guide.
9 Installation server must have httpd and mod-ssl installed.

10 When you install Smart-UI on a Linux Platform, assign executable permissions to the installation script.

11 Ensure that you have a login with root privileges to run the installer.

12 Download the installation file from support.vmware.com and place it in a temporary location on the server.

Procedure

1 Login the server as root.

2 Type `bash smartsui-install.bin -i console` to run the installer in the console-based installer mode, press **Enter**.

   Introduction to the installer appears.

3 Press **Enter** to continue.

   Installer prompts to choose an install folder.

4 Press **Enter** to continue.

   This is the location where smarts-ui will be installed. Default is /opt/smarts-ui.

5 If install folder already contains smarts-ui folder, choose from the following options.
   - Enter 1 to override the already installed folder.
     or
   - Enter 2 to choose a new Installation directory.
     or
   - Enter 3 to cancel the Installation.

6 Installer prompts for VIDM configuration.
   a Enter the **client ID**.
   b Enter the **Shared Secret**.
   c Enter **VIDM Host Name**. Default is identitymanager.eng.vmware.com.
   d Enter the **Auth application Port**. Default port is 8082. This is the port where auth application will start.
   e Press **Enter** to continue.

   **Note**. Installer throws validation error and redirects to the beginning of this step to enter the configurations if any input field is left blank.

   For VIDM configuration, refer [#unique_192](#unique_192).
7 Installer prompts to enter the cAPI configuration. Enter cAPI IP Address in the format <IP-ADDRESS:PORT> and Press Enter to continue.

Default value for this fields is 127.0.0.1:10000. The port number is cAPI listener port provided during cAPI installation. If the input is in wrong format, installer throws validation error and redirects to the beginning of this step to enter the configurations.

8 Enter ssl.conf directory and Press Enter to continue when installer prompts to choose the ssl.conf folder location.

Default value is /etc/httpd/conf.d. If ssl.conf is not existing on the directory, Installer throws an error and redirects to the beginning of step 8 to re-enter the configuration.

9 Make your selection to enable or disable KPI Designer in UI.

Choose option 1 to enable KPI Designer in UI

**Note** If you choose option 1, ensure K4M is installed.

or

Choose option 2 to disable KPI Designer in UI.

**Note** If you choose option 2, refer "Enabling KPI Designer in UI" section to enable KPI manually.

10 Installer prompts to enter KPI REST API IP and PORT if you choose option 1 in step 9. Provide KPI REST API IP and PORT and press Enter to continue.

Default value is 127.0.0.1:8083. This is the address where KPI is running.

**Note** Installer throws validation error and redirects to the beginning of this step to enter IP Address if IP Address input filed left blank.

11 Press Enter to continue the installation when installer shows the pre-install summary.

Installer continues the installation.

12 Press Enter to exit the installer when installer shows the installation is completed.

**What to do next**

After successful Smart-UI installation, follow the steps provided in Export VIDM Certificate section to export and import VIDM certificates.

**Install Smarts-UI using Graphical Mode**

This installation procedure describes the procedure of Smarts-UI installation in the Graphical Interface.

**Prerequisites**

1 Ensure that you have a login with root privileges to run the installer.
2 Download the installation file from support.vmware.com and place it in a temporary location on the server.

Procedure

1 Login to the server as root.

2 Type `bash smartsui-install.bin -i` to gui to run the installer graphical mode, press Enter.

3 Click Next to continue when introduction to the installer appears.

   Installer prompts to choose an install folder.

4 Choose a location and click Next to continue.

   This is the location where smarts-ui will be installed. Default is /opt/ smarts-ui.

5 If install folder already contains smarts-ui folder, choose from the following options:

   - Click Yes to override the already installed folder.
     or
   - Click No to choose a new Installation directory.
     or
   - Click Cancel to cancel the Installation.

6 Installer prompts for VIDM configuration.

   a Enter the **Client ID**.
   
   b Enter the **Shared Secret**.
   
   c Enter **VIDM Host Name**. Default is identitymanager.eng.vmware.com.
   
   d Enter the **Auth application Port**. Default port is 8082. This is the port where auth application starts.
   
   e Click Next to continue.

   For VIDM configuration refer vidm.docx.

   Installer throws validation error and redirects to the beginning of this step to enter the configurations if any input filed left blank.

7 Installer prompts to enter the **cAPI configuration**. Enter cAPI IP Address in the format `<IP-ADDRESS:PORT>` and click Next to continue.

   Default value for this fields is 127.0.0.1:10000. The port number is cAPI listener port provided during cAPI Installation.

   If the input is in wrong format, installer throws validation error and redirects to the beginning of this step to enter the configurations.
Choose ssl.conf directory and click **Next** to continue when installer prompts to choose the ssl.conf folder location.

Default value is /etc/httpd/conf.d

**Note** If ssl.conf is not existing on the directory, installer throws an error and redirects to the beginning of step 8 to re-enter the configuration.

Choose from the selections (Yes/No) to enable or disable KPI Designer in UI when Installer prompts to enable KPI.

Select **Yes** to enable KPI Designer in UI.

**Note** If you select Yes, ensure that K4M is already installed.

or

Select **No** to disable KPI Designer in UI.

**Note** If you select No, refer "Enabling KPI Designer in UI" section to enable KPI manually

Installer prompts to enter **KPI REST API IP** and **PORT** if you select Yes in step 9. Provide **KPI REST API IP** and **PORT** and click **Next** to continue.

Default value is 127.0.0.1:8083. This is the address where KPI is running.

Installer throws validation error and redirects to the beginning of this step to enter IP Address if IP Address input field left blank.

Click **Install** to continue the installation when installer shows the pre-install summary.

Installation continues.

Click **Done** to exit the installer when installer displays as completed.

Installation is completed.

**What to do next**

After successful Smart-UI installation, follow the steps provided in Export VIDM Certificate section to export and import VIDM certificates.

**Install Smarts-UI in Silent Mode**

A silent installation is an installation procedure that continues without user interaction. It requires no user intervention from start to finish. This installation is performed using a user-modifiable response file, which enables you to easily duplicate the installation on many computer systems.
Table 2-14. Variables Property and Description

<table>
<thead>
<tr>
<th>Property</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>USER_INSTALL_DIR</td>
<td>Install directory for smarts-ui.</td>
</tr>
<tr>
<td>CLIENT_ID</td>
<td>Client ID.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Use the created remote access token for Auth App for VIDM Authentication. Get the values of client ID, shared secret and VIDM host name from VIDM authentication server.</td>
</tr>
<tr>
<td>SECRET</td>
<td>Shared Secret.</td>
</tr>
<tr>
<td>VIDM_HOST_NAME</td>
<td>VIDM Host Name.</td>
</tr>
<tr>
<td>AUTH_PORT</td>
<td>Auth Application Port.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Port where Auth application will start.</td>
</tr>
<tr>
<td>CAPI_IP_ADDRESS</td>
<td>cAPI IP Address.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Enter the cAPI address in the format <a href="">IP:PORT</a></td>
</tr>
<tr>
<td></td>
<td>Example: 127.0.0.1:10000.</td>
</tr>
<tr>
<td>SSL_CONF_DIR</td>
<td>Enter the ssl.conf location folder.</td>
</tr>
<tr>
<td></td>
<td>For example, /etc/httpd/conf.d</td>
</tr>
<tr>
<td>KPI_ENABLED</td>
<td>To enable KPI set KPI_ENABLED to &quot;Yes&quot; else set to &quot;No&quot;.</td>
</tr>
<tr>
<td>KPI_REST_API_URL</td>
<td>KPI REST API URL.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Enter the KPI REST API URL in the format <a href="">IP-ADDRESS:PORT</a> if KPI_ENABLED flag is set to Yes.</td>
</tr>
<tr>
<td></td>
<td>For example, KPI_REST_API_URL=127.0.0.1:8083. Or Else do not set the KPI_REST_API_URL, For example KPI_REST_API_URL=</td>
</tr>
</tbody>
</table>

Prerequisites

Create a configuration file for the installer to execute the installation. To create configuration file:

1. Copy the sample configuration file from the distribution (smartsui-installer.properties) to a directory on the server where you are installing smarts-ui.
2. Use any editor (vi/vim) to modify this file.
3. Define each of the properties in this file, according to the Table - Variables Property and Description. Save the changes to the file.

Procedure

1. Log in to the server as root.
2. Type `bash smartsui-install.bin -f <response file location> -i silent, press Enter`. **Note** Any user interaction is not required for this installer. Once it completes, a message displays indicating that installation is completed, and you are returned to the shell prompt. If the installer is unable to complete the installation, an error message is saved in the [Product directory]/smarts-ui_logs.
What to do next

After successful Smart-UI installation, follow the steps provided in Export VIDM Certificate section to export and import VIDM certificates.