Design and Deployment of VMware Skyline

28 MAY 2019
VMware Validated Design 5.0.1
About Deployment and Design of VMware Skyline

Deployment and Design of VMware Skyline provides details about the requirements for software, tools, and external services to implement VMware Skyline™ across an SDDC that is compliant with VMware Validated Design for Software-Defined Data Center.

Prerequisites

You must have VMware Validated Design for Software-Defined Data Center 5.0.1 deployed in at least a single-region deployment. See the VMware Validated Design documentation page.

Intended Audience

This design is intended for cloud architects, infrastructure administrators, and cloud administrators who want to use proactive support by VMware Technical Support and collect diagnostic data about the VMware vSphere®, VMware NSX® Data Center, and VMware vRealize® Operations Manager™ components by deploying VMware Skyline.

Required VMware Software

1. Deploy VMware Validated Design for Software-Defined Data Center 5.0.1.
2. Download VMware Skyline Collector 2.1.
Architecture and Design for VMware Skyline

The architecture of VMware Skyline supports collection of product usage telemetry at the location of the SDDC endpoints and analysis of the data in VMware Cloud Services. As part of the design, you determine the number and size of the required collector appliances, network configuration for the appliances, endpoint configuration and the number and permissions of the service accounts required for communication with the connected endpoints.

This chapter includes the following topics:

- VMware Skyline Architecture
- VMware Skyline Design

VMware Skyline Architecture

VMware Skyline gathers and aggregates product usage information such as configuration, feature, and performance data while listening for changes and events within the customer's environment, to provide proactive support recommendations.

Overview

VMware Skyline implements proactive support for VMware SDDC products. VMware Skyline uses automation to securely collect data and perform environment-specific analysis on configuration, feature, and performance data against best practices, VMware Knowledge Base articles, and Security Advisories. As a result, VMware can provide proactive, predictive, and prescriptive recommendations for improving the stability and reliability of the environment. In addition, VMware can resolve reactive support issues faster.

VMware Skyline collects diagnostic data about the vSphere, NSX for vSphere, and vRealize Operations Manager.

To use the proactive support capabilities of VMware Skyline, you must have an active Production Support or Premier Services contract.

Note  Product usage data might include customer identifiable information, such as ESXi host names, IP addresses, license keys, customer IDs, or entitlement account numbers. For information about data privacy and security, see VMware Skyline FAQ.
Customer Experience Improvement Program

Collection of product usage data by the Skyline Collector instances is a subject to acceptance in VMware’s Customer Experience Improvement Program (CEIP). The VMware Customer Experience Improvement Program (CEIP) provides information that helps VMware improve products and services, fix problems and advise you on how best to deploy and use VMware products. See CEIP home page.

Note  Skyline does not currently collect product log data.

Skyline Collector

A Skyline Collector instance is a Java-based application that is available as a pre-configured virtual appliance in OVA format. A Skyline Collector instance collects product usage data from compatible SDDC endpoints. The Skyline Collector instance also listens for certain changes and events, and sends them to the rules engine of VMware Skyline that is running in the cloud. To analyze inbound product information, the rules engine uses a library of support intelligence, product knowledge, and logic. After the analysis is complete, you can view your proactive findings and recommendations in Skyline Advisor.

The Skyline Collector UI is a VMware Clarity and Angular JS application that is hosted on Nginx. You use the Skyline Collector UI to register endpoints for collection of product usage data and manage the system status.

Before you use Skyline Collector, you must create an organization in VMware Cloud Services, associate it with your customer entitlement account in My VMware, and generate a registration token. When you log in to the collector for the first time, you connect the collector to your VMware Cloud Services organization. Then, the level of service that you receive is further managed according to the level of entitlement that you have.

Figure 2-1. Skyline Collector Architecture
Skyline Advisor

Skyline Advisor is a self-service, Web-based application that is available from the VMware Cloud services portal. You can view proactive findings and recommendations on-demand. Skyline Advisor shows each proactive finding as a card, with information on affected objects and recommendations. In addition, VMware Technical Support uses a similar view that contains more details on your environment and makes the resolution of service requests faster.

Skyline Log Assist

By using Skyline Log Assist, you can transfer log data from your environment to VMware. In Skyline Advisor, you or VMware Technical Support Engineers (TSEs) can initiate a log transfer from selected objects in the vCenter Server inventory. If a TSE initiates the log request, you must approve or deny the log transfer.

Skyline Collector Endpoints

To analyze telemetry information from vSphere, vSAN, NSX for vSphere, and vRealize Operations Manager, Skyline Collector instances can connect to vCenter Server, NSX Manager and vRealize Operations Manager endpoints.

Skyline Collector Authentication and Authorization

You can configure Skyline Collector to use the following user authentication and authorization models:

- Local administrator account
- Active Directory using anonymous LDAP operations.

Backup and Recovery of Skyline Collector

You back up a Skyline Collector virtual appliance by using traditional virtual machine backup solutions that are compatible with VMware vSphere Storage APIs – Data Protection (VADP).

Multi-Region Skyline Collector Deployment

You can use this design for both multiple regions and availability zones.

In a multi-region implementation, for endpoint registration you must deploy a Skyline Collector instance in each region. Each collector instance provides a separate localized collection of product usage data in each region of the SDDC. VMware aggregates information collected from multiple Skyline Collector instances. See VMware Skyline FAQ.

In a multi-availability zone implementation, which is a super-set of the multi-region design, Skyline Collector instances continue to collect product usage data in all regions of the SDDC. A Skyline Collector instance resides in Availability Zone 1 in Region A. If this zone becomes compromised, the Skyline Collector instance is brought up in Availability Zone 2.
VMware Skyline Design

VMware Skyline Collector integrates with the vSphere, NSX Data Center and vRealize Operations Manager components of the virtual infrastructure layer to provide proactive support recommendations.

Logical Design of VMware Skyline

To collect product usage data, each Skyline Collector instance communicates with SDDC endpoints for the management and workload domains in a region. The collector sends product usage data to VMware Skyline on VMware Cloud Services for analysis, proactive issue reporting, and support request research analysis. You can view the aggregated information from the collector instances by using Skyline Advisor.

Using a region-specific Skyline Collector instance supports localized collection of diagnostic data from adjacent endpoints.

Skyline Collector instances collect data from the following components.

- vSphere
- vSAN by using vSAN Support Insight
- NSX for vSphere
- vRealize Operations Manager
Physical Design of VMware Skyline

You deploy a Skyline Collector instance as a virtual appliance in the management cluster. After you deploy the appliance, you configure vCenter Server, NSX Manager and vRealize Operations Manager endpoints for collecting product usage data in the SDDC.

Deployment Model

You deploy a Skyline Collector virtual appliance in the management cluster collect data from the adjacent vCenter Server, NSX Manager, and vRealize Operations Manager endpoints in to the cloud. In a multi-region and multi availability zone SDDC, you deploy a Skyline Collector node in each region.

After you deploy the virtual appliance, the Skyline Collector services start automatically and you can configure the solution.

Table 2-1. Design Decisions on the Deployment Model for Skyline Collector

<table>
<thead>
<tr>
<th>Decision ID</th>
<th>Design Decision</th>
<th>Design Justification</th>
<th>Design Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDDC-SKY-001</td>
<td>In each region, deploy a Skyline Collector virtual appliance in the management cluster.</td>
<td>Supports collecting product usage data from endpoints in each region and in range of the Skyline Collector endpoint maximums.</td>
<td>None.</td>
</tr>
</tbody>
</table>
Sizing Compute and Storage Resource

Provide the compute and storage resources that are required for the operation of the solution.

Table 2-2. Resource Specification of the Skyline Collector Appliance

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virtual hardware version</td>
<td>Version 10</td>
</tr>
<tr>
<td>Number of CPUs</td>
<td>2 vCPUs</td>
</tr>
<tr>
<td>Memory</td>
<td>8 GB</td>
</tr>
<tr>
<td>Disk size</td>
<td>87 GB</td>
</tr>
<tr>
<td></td>
<td>1.1 GB initial if thin-provisioned.</td>
</tr>
<tr>
<td>Network adapters</td>
<td>1 VM NIC</td>
</tr>
</tbody>
</table>

Table 2-3. Design Decisions on the Compute and Storage Resources for Skyline Collector

<table>
<thead>
<tr>
<th>Decision ID</th>
<th>Design Decision</th>
<th>Design Justification</th>
<th>Design Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDDC-SKY-002</td>
<td>Deploy the Skyline Collector appliance with the default appliance sizing.</td>
<td>Accommodates the expected amount of product usage data from the endpoints in a region, up the endpoint maximum.</td>
<td>None.</td>
</tr>
</tbody>
</table>

Networking Design of VMware Skyline

The Skyline Collector virtual appliances are connected to the region-specific management VXLANs, Mgmt–RegionA01–VXLAN and Mgmt–RegionB01–VXLAN, for isolation and co-location with endpoint sources. The networking design also supports administrative access to the Skyline Collector instances and outbound access for each Skyline Collector instance to VMware for diagnostic data analysis.
**Application Virtual Network Design for Skyline Collector**

This networking design has the following features:

- Skyline Collector instances have routed access to the management network through the universal distributed logical router (UDLR) for the SDDC endpoints deployed in the management cluster.

- Routing to the management network and the external network is dynamic, and is based on the Border Gateway Protocol (BGP).

For more information about the networking configuration of the application virtual networks for Skyline Collector, see *Application Virtual Network and Virtual Network Design Example* in the *Architecture and Design* documentation of VMware Validated Design for Software-Defined Data Center.
Table 2-4. Design Decisions on the Application Virtual Network for the Skyline Collector Instances

<table>
<thead>
<tr>
<th>Decision ID</th>
<th>Design Decision</th>
<th>Design Justification</th>
<th>Design Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDDC-SKY-003</td>
<td>Deploy the Skyline Collector instances on the region-specific application virtual networks.</td>
<td>Ensures localized collection of diagnostic data per region if a cross-region network outage occurs.</td>
<td>You must use NSX to support this network configuration.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Avoids cross-region bandwidth usage for data collection.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provides a consistent deployment model for management applications.</td>
<td></td>
</tr>
</tbody>
</table>

IP Subnets for Skyline Collector

You can allocate the following example subnets to the Skyline Collector deployment.

Table 2-5. IP Subnets in the Application Virtual Networks of Skyline Collector

<table>
<thead>
<tr>
<th>Region</th>
<th>IP Subnet</th>
<th>VXLAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region A</td>
<td>192.168.31.0/24</td>
<td>Mgmt-RegionA01-VXLAN</td>
</tr>
<tr>
<td>Region B</td>
<td>192.168.32.0/24</td>
<td>Mgmt-RegionB01-VXLAN</td>
</tr>
</tbody>
</table>

DNS Records for Skyline Collectors

Skyline Collector virtual appliance name resolution uses a region-specific suffix, such as, sfo01.rainpole.local or lax01.rainpole.local according to the region deployment. The Skyline Collector instances in the two regions have the following fully qualified domain names registered in DNS.

Table 2-6. FQDNs for Skyline Collectors

<table>
<thead>
<tr>
<th>Region</th>
<th>FQDN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region A</td>
<td>sfo01sky01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>Region B</td>
<td>lax01sky01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

Table 2-7. Design Decision on the DNS Records for Skyline Collector

<table>
<thead>
<tr>
<th>Decision ID</th>
<th>Design Decision</th>
<th>Design Justification</th>
<th>Design Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDDC-SKY-004</td>
<td>Configure forward and reverse DNS records for each Skyline Collector virtual appliance.</td>
<td>Each Skyline Collector is accessible by using a fully qualified domain name instead of by using IP addresses only.</td>
<td>You must provide forward and reverse DNS records for each Skyline Collector virtual appliance.</td>
</tr>
</tbody>
</table>

External Connectivity

A Skyline Collector instance uses network connections to collect and transfer diagnostic data information securely.

A Skyline Collector instance requires external network connectivity to VMware Skyline to upload diagnostic data. You can use an HTTP proxy server for outbound connectivity, but access to SDDC endpoints must be direct.
Table 2-8. Design Decision on Network Connectivity for Skyline Collector

<table>
<thead>
<tr>
<th>Decision ID</th>
<th>Design Decision</th>
<th>Design Justification</th>
<th>Design Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDDC-SKY-005</td>
<td>Provide direct or proxied HTTPS access to the external endpoints for Skyline Collector instances.</td>
<td>Skyline Collector instances require outbound network connectivity to the external VMware Skyline systems to upload diagnostic data.</td>
<td>You must provide the Skyline Collector instances with direct or proxied HTTPS access to the external VMware Skyline systems.</td>
</tr>
</tbody>
</table>

Endpoint Collection Design for VMware Skyline

You configure each Skyline Collector to collect data from the vCenter Server, NSX Manager, and vRealize Operations Manager endpoints for the management and workload domains in the region.

VMware Skyline monitors vSAN-enabled clusters in the management and workload domains by using vSAN Support Insight. Skyline matches the analyzed data from vSAN Support Insight to the monitored SDDC and includes the data in Skyline Advisor. VMware Technical Support can use the data to diagnose issues quickly and to reduce time-to-resolution during troubleshooting.

Table 2-9. Design Decisions on Endpoint Collection for VMware Skyline

<table>
<thead>
<tr>
<th>Decision ID</th>
<th>Design Decision</th>
<th>Design Justification</th>
<th>Decision Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>SDDC-SKY-006</td>
<td>Register the vCenter Server instance for the management cluster and shared edge and compute cluster with the Skyline Collector instance in the local region.</td>
<td>Enables collection of product usage data for the following operations:</td>
<td>You must manually register each vCenter Server endpoint with the Skyline Collector instance by using the UI.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Proactive identification of potential issues</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Research analysis for service requests that improve the stability and reliability of your VMware environment</td>
<td></td>
</tr>
<tr>
<td>SDDC-SKY-007</td>
<td>Enable vSAN Support Insight (vSAN Online Health) for each vSAN-enabled cluster.</td>
<td>Starts uploading vSAN health, performance, and configuration information to VMware Cloud Services on a regular cadence. In the cloud, the data it is analyzed and matched with VMware Skyline Collector product usage. By enabling vSAN Support Insight on each vSAN enabled cluster, you also enable CEIP.</td>
<td>You must enable vSAN Support Insight on each vSAN-enabled cluster.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ If the SDDC requires the use of firewall or proxy exceptions to connect to the Internet, then you must configure a firewall or proxy rule allowing outbound traffic through for <a href="https://vcsa.vmware.com:443/ph/oci/">https://vcsa.vmware.com:443/ph/oci/</a>* for each management and compute vCenter Server instance.</td>
<td></td>
</tr>
<tr>
<td>Decision ID</td>
<td>Design Decision</td>
<td>Decision Justification</td>
<td>Decision Implication</td>
</tr>
<tr>
<td>--------------</td>
<td>---------------------------------------------------------------------------------</td>
<td>----------------------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>
| SDDC-SKY-008 | Register the NSX Manager instance for the management cluster and shared edge and compute cluster with the Skyline Collector instance in the local region. | Enables collection of product usage data for the following operations:  
  ■ Proactive identification of potential issues  
  ■ Research analysis for service requests that improves the overall stability and reliability of your VMware environment | You must manually register each vCenter Server endpoint with the Skyline Collector instance by using the UI. |
| SDDC-SKY-009 | Register the vRealize Operations Manager instance in the management cluster with the Skyline Collector instance in the local region. | Enables collection of product usage data for the following operations:  
  ■ Proactive identification of potential issues  
  ■ Research analysis for service requests that improves the overall stability and reliability of your VMware environment | You must manually register vRealize Operations Manager with the Skyline Collector instance by using the UI. |

**Information Security and Access Control in VMware Skyline**

Protect Skyline Collector deployments by configuring secure communication and authentication with the other components in the SDDC. Use dedicated service accounts for communication between the Skyline Collector instance and the vCenter Server, NSX Data Center, and vRealize Operations Manager endpoints in the management cluster and shared edge and compute cluster.

**Encryption**

Access to Skyline Collector user interfaces requires an SSL connection. By default, the Skyline Collector appliance uses self-signed certificates for the application interface and the virtual appliance management interface (VAMI). To provide secure access to the Skyline Collector appliance and between the Skyline Collector instance and SDDC endpoints, replace the default self-signed certificates with a CA-signed certificate.

**Table 2-10. Design Decisions on Skyline Collector Encryption**

<table>
<thead>
<tr>
<th>ID</th>
<th>Design Decision</th>
<th>Design Justification</th>
<th>Design Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>SKY-SDDC-010</td>
<td>Replace the default self-signed certificates on the Skyline Collector virtual appliance with a CA-signed certificate.</td>
<td>Ensures that the communication to the user interface of the Skyline Collector instances and between the SDDC endpoints is encrypted.</td>
<td>Replacing the default certificates with a CA-signed certificate from a trusted certificate authority increases the deployment preparation time as certificate requests are generated and delivered.</td>
</tr>
</tbody>
</table>
Authentication and Authorization

Users can authenticate to a Skyline Collector instance in the following ways:

- **Local administrator Account**
  
  Skyline Collector performs local authentication for the default administrator account only. The admin account is the primary user account. You use this account to log in to the Skyline Collector administrative interface, register the application, and manage collection endpoints.

- **Active Directory**
  
  You can also enable authentication by using Active Directory for named user access. Active Directory users and groups can both be provided access to the Skyline Collector UI to perform administrative tasks, such as, monitoring system status and endpoint management. However, only the local default administrator account can perform Active Directory configuration tasks.

Configure service accounts for communication between the Skyline Collector instances and the SDDC endpoint instances. You define service accounts with only the minimum set of permissions to perform the collection of diagnostic data from the management cluster and shared edge and compute cluster.

<table>
<thead>
<tr>
<th>ID</th>
<th>Design Decision</th>
<th>Design Justification</th>
<th>Design Implication</th>
</tr>
</thead>
</table>
| SKY-SDDC-011  | Use local authentication for the Skyline Collector appliances.                    | Although Skyline Collector supports the use of Active Directory as an authentication source and access control, you must use anonymous LDAP operations to use the Active Directory integrate, which is non-default. | ▪ The accountability in tracking administrative interactions between the Skyline Collector and SDDC endpoints is limited.  
  ▪ You must control the access to the administrator account for Skyline Collector. |
<p>| SKY-SDDC-012  | Define a custom vCenter Server role for Skyline Collector that has the minimum privileges required to support the collection of data from the vSphere endpoints across the SDDC. | Skyline Collector instances access vSphere with the minimum set of permissions that are required to support the collection of diagnostic data from the management cluster and shared edge and compute clusters. | You must maintain the permissions required by the custom role. |</p>
<table>
<thead>
<tr>
<th>ID</th>
<th>Design Decision</th>
<th>Design Justification</th>
<th>Design Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>SKY-SDDC-013</td>
<td>Configure a service account in vCenter Server for application-to-application</td>
<td>Provides the following access control features:</td>
<td>You must maintain the lifecycle and availability of the service account outside of the SDDC stack.</td>
</tr>
<tr>
<td></td>
<td>communication from Skyline Collector to vSphere.</td>
<td>■ Skyline Collector instances access vSphere endpoints with the minimum set of required permissions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ If there is a compromised account, the accessibility in the destination application remains restricted.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ You can introduce improved accountability in tracking request-response interactions between the components of the SDDC.</td>
<td></td>
</tr>
<tr>
<td>SKY-SDDC-014</td>
<td>Assign global permissions to the Skyline Collector service account in vCenter Server by using the custom role.</td>
<td>■ Skyline Collector instances access vSphere with the minimum set of permissions.</td>
<td>All vCenter Server instances must be in the same vSphere domain.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Simplifies and standardizes the deployment of the service account across all vCenter Servers in the same vSphere domain.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>■ Provides a consistent authorization layer.</td>
<td></td>
</tr>
</tbody>
</table>
Table 2-11. Design Decisions on Authentication and Authorization to Skyline Collector (Continued)

<table>
<thead>
<tr>
<th>ID</th>
<th>Design Decision</th>
<th>Design Justification</th>
<th>Design Implication</th>
</tr>
</thead>
<tbody>
<tr>
<td>SKY-SDDC-015</td>
<td>Assign permissions for the Skyline Collector service account in the NSX Manager for the management cluster and shared edge and compute cluster for each region by using the default Auditor role.</td>
<td>Provides the following access control features: &lt;br&gt; - Skyline Collector instances access NSX endpoints with the minimum set of required permissions. &lt;br&gt; - If there is a compromised account, the accessibility in the destination application remains restricted. &lt;br&gt; - You can introduce improved accountability in tracking request-response interactions between the components of the SDDC.</td>
<td>You must maintain the lifecycle and availability of the service account outside of the SDDC stack.</td>
</tr>
<tr>
<td>SKY-SDDC-016</td>
<td>Assign permissions for the Skyline Collector service account in vRealize Operations Manager by using the default read-only role.</td>
<td>Provides the following access control features: &lt;br&gt; - Skyline Collector instances access vRealize Operations Manager endpoints with the minimum set of required permissions. &lt;br&gt; - If there is a compromised account, the accessibility in the destination application remains restricted. &lt;br&gt; - You can introduce improved accountability in tracking request-response interactions between the components of the SDDC.</td>
<td>You must maintain the lifecycle and availability of the service account outside of the SDDC stack.</td>
</tr>
</tbody>
</table>
Deployment of VMware Skyline

To connect the SDDC to VMware Skyline, first provide the required network, service account and certificate configuration and register with VMware Cloud Services. Then, proceed to deploying a Skyline Collector appliance in each region.

1 Before You Deploy the Skyline Collector Instances
Before you deploy the Skyline Collector nodes, you must create DNS records for the appliances, set up Active Directory service accounts in the solutions VMware Skyline can collect data from, create firewall rules, set up collector accounts in your VMware Cloud Services organization, and create certificates.

2 Deploy and Configure the Skyline Collector Instances
After preparing the environment, deploy the Skyline Collector appliances and connect them to VMware Cloud Services and to the solution endpoints in the SDDC.

Before You Deploy the Skyline Collector Instances

Before you deploy the Skyline Collector nodes, you must create DNS records for the appliances, set up Active Directory service accounts in the solutions VMware Skyline can collect data from, create firewall rules, set up collector accounts in your VMware Cloud Services organization, and create certificates.

Procedure

1 IP Address and Host Name Requirements for the Skyline Collector Instances
Before you deploy and configure the Skyline Collector instances in the SDDC, allocate the host names and IP addresses for their virtual appliances.

2 Configure User Access for Integration with VMware Skyline
Create service accounts for the Skyline Collector instances specifically for collecting usage data from vSphere, NSX for vSphere, and vRealize Operations Manager. Configure the service accounts with the minimum permissions that are required for connecting to and collecting data from the endpoints in the SDDC.

3 Configure the Distributed Firewall for the Skyline Collector Instances
Configuring a distributed firewall for use with your SDDC increases the security level of your environment by allowing only the network traffic that is required for running and operating the SDDC. To allow traffic to VMware Cloud Services and access to the Skyline Collector appliances, you configure additional policies on the distributed firewall for the management applications.
Prepare for Skyline Collector Registration with VMware Cloud Services
Before you register the Skyline Collector instances with VMware Cloud Services and start using VMware Skyline for proactive product support, you must create an organization on VMware Cloud Services and generate a registration token for the Skyline Collector instances.

Generate Certificates for the Skyline Collector Appliances
To generate certificates signed by the Microsoft certificate authority (MSCA) for the Skyline Collector appliances in a single operation, use the VMware Validated Design Certificate Generation Utility (CertGenVVD).

IP Address and Host Name Requirements for the Skyline Collector Instances
Before you deploy and configure the Skyline Collector instances in the SDDC, allocate the host names and IP addresses for their virtual appliances.

Configure both forward and reverse DNS records with a fully qualified domain name (FQDN) and IP address.

Table 3-1. IP Addresses and Host Names for the Skyline Collector Instances

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value in Region A</th>
<th>Value in Region B</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>192.168.31.70</td>
<td>192.168.32.70</td>
</tr>
<tr>
<td>FQDN</td>
<td>sfo01sky01.sfo01.rainpole.local</td>
<td>lax01sky01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

Configure User Access for Integration with VMware Skyline
Create service accounts for the Skyline Collector instances specifically for collecting usage data from vSphere, NSX for vSphere, and vRealize Operations Manager. Configure the service accounts with the minimum permissions that are required for connecting to and collecting data from the endpoints in the SDDC.
Table 3-2. Application Service Accounts for the Skyline Collector Instances in the SDDC

<table>
<thead>
<tr>
<th>Username</th>
<th>Source</th>
<th>Destination</th>
<th>Description</th>
<th>Required Role</th>
</tr>
</thead>
<tbody>
<tr>
<td>svc-skyline-vsphere</td>
<td>Skyline Collectors</td>
<td>Management vCenter Server</td>
<td>A service account for collecting diagnostic data from vSphere endpoints in the SDDC.</td>
<td>Skyline Collector User (Custom vSphere role)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Compute vCenter Server</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>NSX Manager for the management cluster</td>
<td>A service account for collecting diagnostic data from NSX for the vSphere endpoints in the SDDC.</td>
<td>Auditor (Native NSX role)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>NSX Manager for the shared edge and compute cluster</td>
<td></td>
<td></td>
</tr>
<tr>
<td>svc-skyline-nsx</td>
<td>Skyline Collectors</td>
<td>vRealize Operations Manager</td>
<td>A service account for collecting diagnostic data from vRealize Operations Manager in the SDDC.</td>
<td>Read Only (Native vRealize Operations Manager role)</td>
</tr>
<tr>
<td>svc-skyline-vrops</td>
<td>Skyline Collectors</td>
<td>vRealize Operations Manager</td>
<td>A service account for collecting diagnostic data from vRealize Operations Manager in the SDDC.</td>
<td>Read Only (Native vRealize Operations Manager role)</td>
</tr>
</tbody>
</table>

Procedure

1. **Define a User Role in vSphere for the Skyline Collector Instances**
   To give the Skyline Collector instances rights to collect data from the vSphere endpoints, first create a user role with the required minimum privileges on the vCenter Server instances in the SDDC.

2. **Configure User Privileges in vSphere for the Skyline Collector Instances**
   To give the svc-skyline-vsphere service account rights for collecting product analytics data from all linked vCenter Server endpoints, assign global permissions to the account.

3. **Configure User Privileges in NSX for the Skyline Collector Instances**
   Configure the auditor privilege for the svc-skyline-nsx@rainpole.local service account only on the primary NSX Manager instances in Region A. The secondary NSX Manager instances in Region B automatically synchronize these privileges.

4. **Configure User Privileges in vRealize Operations Manager for the Skyline Collector Instances**
   To provide the Skyline Collector instances with access to vRealize Operations Manager, on vRealize Operations Manager, give only read-only privileges for the svc-skyline-vrops@rainpole.local service account.

**Define a User Role in vSphere for the Skyline Collector Instances**

To give the Skyline Collector instances rights to collect data from the vSphere endpoints, first create a user role with the required minimum privileges on the vCenter Server instances in the SDDC.
**Procedure**

1. Log in to vCenter Server by using the vSphere Client.
   a. Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.
   b. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. On the **Home** page of the vSphere Client, in the navigation pane, select **Administration**.

3. On the **Administration** page, select **Roles**.

4. Create a role for the Skyline Collector instances.
   a. From the **Roles provider** drop-down menu, select `sfo01m01vc01.sfo01.rainpole.local`.
   b. Select **Read-only** and click the **Clone role action** icon.

   You clone the Read-only role because it includes the `System.Anonymous`, `System.View`, and `System.Read` privileges. The Skyline Collector instances require these privileges to collect information from the vCenter Server endpoint in each workload domain and the vSphere infrastructure components.
   c. In the **Clone Role** dialog box, enter the name of the role and click **OK**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Role name</td>
<td>Skyline Collector User</td>
</tr>
</tbody>
</table>

5. To grant the Skyline Collector instances access to license data in vSphere, assign the **Global.Licenses** privilege to the role.
   a. From the list of **Roles**, select the **Skyline Collector User** role.
   b. Click the **Edit role action** icon.
   c. On the **Edit Role** dialog box, select **Global** in the left pane and select **Licenses** in the right pane.
   d. Click **Next** and click **Finish**.

   The Skyline Collector user role is propagated to the other linked vCenter Server instances.

**Configure User Privileges in vSphere for the Skyline Collector Instances**

To give the `svc-skyline-vsphere` service account rights for collecting product analytics data from all linked vCenter Server endpoints, assign global permissions to the account.
Procedure

1 Log in to vCenter Server by using the vSphere Client.
   a Open a Web browser and go to https://sfo01m01vc01.sfo01.rainpole.local/ui.
   b Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2 On the Home page of the vSphere Client, in the navigation pane, select Administration.

3 On the Administration page, under Access Control, select Global Permissions.

4 On the Global Permissions page, click the Add Permission icon.

5 In the Add Permission-Global Permissions Root dialog box, from the User drop-down menu, select rainpole.local.

6 In the search box, enter svc and press Enter.

7 From the list of users and groups, select the svc-skyline-vsphere user.

8 From the Role drop-down menu, select Skyline Collector User, select Propagate to children, and click OK.

Configure User Privileges in NSX for the Skyline Collector Instances

Configure the auditor privilege for the svc-skyline-nsx@rainpole.local service account only on the primary NSX Manager instances in Region A. The secondary NSX Manager instances in Region B automatically synchronize these privileges.

<table>
<thead>
<tr>
<th>Primary NSX Manager Instance in Region A</th>
<th>IP Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Manager instance for the management cluster</td>
<td>172.16.11.65</td>
</tr>
<tr>
<td>NSX Manager instance for the shared edge and compute cluster</td>
<td>172.16.11.66</td>
</tr>
</tbody>
</table>

Procedure

1 Log in to vCenter Server by using the vSphere Web Client.
   a Open a Web browser and go to https://sfo01m01vc01.sfo01.rainpole.local/vsphere-client/.
   b Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>
2 In the Networking & Security inventory, under System, select Users and Domains.

3 On the Users tab, from the NSX Manager drop-down menu, select 172.16.11.65.

4 Click the Add icon.

    The Assign Role wizard appears.

5 On the Identify User page, select the Specify a vCenter User radio button, enter svc-skyline-nsx@rainpole.local in the User text box, and click Next.

6 On the Select Roles page, select the Auditor radio button, and click Finish.

7 Repeat the procedure on the other NSX Manager instance in Region A.

Configure User Privileges in vRealize Operations Manager for the Skyline Collector Instances

To provide the Skyline Collector instances with access to vRealize Operations Manager, on vRealize Operations Manager, give only read-only privileges for the svc-skyline-vrops@rainpole.local service account.

Procedure

1 Log in to the vRealize Operations Manager master node by using the administration interface.
   a Open a Web browser and go to https://vrops01svr01a.rainpole.local.
   b Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>deployment_admin_password</td>
</tr>
</tbody>
</table>

2 On the main navigation bar, click Administration.

3 In the left pane of vRealize Operations Manager, expand Access and click Access Control.

4 On the Access Control page, click the User Accounts tab and click the Import Users icon.

5 On the Import Users page, import the svc-skyline-vrops@rainpole.local service account.
   a From the Import From drop-down menu, select Rainpole.local.
   b Select the Basic option for the search query.
   c In the Search String text box, enter svc-skyline-vrops and click Search.
      The search results contain the svc-skyline-vrops@rainpole.local user account.
   d Select svc-skyline-vrops@rainpole.local and click Next.
On the Assign Groups and Permissions page, click the Objects tab, assign the ReadOnly role to the svc-skyline-vrops@rainpole.local service account, and click Finish.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select Role</td>
<td>ReadOnly</td>
</tr>
<tr>
<td>Assign this role to the user</td>
<td>Selected</td>
</tr>
<tr>
<td>Allow access to all objects in the system</td>
<td>Selected</td>
</tr>
</tbody>
</table>

Configure the Distributed Firewall for the Skyline Collector Instances

Configuring a distributed firewall for use with your SDDC increases the security level of your environment by allowing only the network traffic that is required for running and operating the SDDC. To allow traffic to VMware Cloud Services and access to the Skyline Collector appliances, you configure additional policies on the distributed firewall for the management applications.

Prerequisites

- Implement the IP sets, security groups, and distributed firewall rules from VMware Validated Design for Software-Defined Data Center.

Procedure

1. Create an IP Set for the Skyline Collector Instances
   Create an IP set for the Skyline Collector appliances in the management cluster. You use the IP set later for creating a security group for use with the additional distributed firewall rules for Skyline Collector.

2. Configure Security Groups for the Skyline Collector Instances
   Create a new security group for the Skyline Collector appliances for configuring later a firewall rule specifically for access to the Skyline Collector user interface. Also update the existing VMware Appliances security group so that the you can access the collector appliances by using SSH and the virtual appliance management interface (VAMI). By adding the collector appliances to the VMware Appliances security group, you also control the access from a VMware vSphere Storage APIs - Data Protection (VADP) solution can back up the appliances.

3. Create a Distributed Firewall Rule for the Skyline Collector Instances
   For security reasons, only other solutions in the SDDC and approved administration IP addresses can directly communicate with individual management components including the Skyline Collector instances. To allow HTTPS access to the Skyline Collector, you create a rule in the distributed firewall.

Create an IP Set for the Skyline Collector Instances

Create an IP set for the Skyline Collector appliances in the management cluster. You use the IP set later for creating a security group for use with the additional distributed firewall rules for Skyline Collector.
Table 3-3. IP Set for the Skyline Collector

<table>
<thead>
<tr>
<th>Name</th>
<th>IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skyline Collector Virtual Appliances</td>
<td>Skyline-Collector-IPs</td>
</tr>
</tbody>
</table>

**Prerequisites**

**Procedure**

1. Log in to vCenter Server by using the vSphere Client.
   
   a. Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.
   
   b. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. In the **Networking and Security** inventory, select **Groups and Tags**.

3. On the **Groups and Tags** page, from the **NSX Manager** drop-down menu, select the **172.16.11.65**.

4. On the **IP Sets** tab, click **Add**.

5. In the **New IP Set** dialog box, configure the values for the IP set and click **Add**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Skyline Collectors</td>
</tr>
<tr>
<td>IP Addresses</td>
<td>192.168.31.70 192.168.32.70</td>
</tr>
<tr>
<td>Universal Synchronization</td>
<td>On</td>
</tr>
</tbody>
</table>

Configure Security Groups for the Skyline Collector Instances

Create a new security group for the Skyline Collector appliances for configuring later a firewall rule specifically for access to the Skyline Collector user interface. Also update the existing VMware Appliances security group so that you can access the collector appliances by using SSH and the virtual appliance management interface (VAMI). By adding the collector appliances to the VMware Appliances security group, you also control the access from a VMware vSphere Storage APIs - Data Protection (VADP) solution can back up the appliances.

You perform the security group configuration on the NSX Manager instance for the management cluster in Region A because this instance is primary for the management components in the SDDC.

Table 3-4. Security Groups for the Skyline Collector Instances in the SDDC

<table>
<thead>
<tr>
<th>Name</th>
<th>Object Type</th>
<th>Selected Object</th>
</tr>
</thead>
<tbody>
<tr>
<td>Skyline Collectors</td>
<td>IP Sets</td>
<td>Skyline Collectors</td>
</tr>
<tr>
<td>VMware Appliances</td>
<td>Security Groups</td>
<td>Skyline Collectors</td>
</tr>
</tbody>
</table>
Procedure

1. Log in to vCenter Server by using the vSphere Client.
   a. Open a Web browser and go to `https://sfo01m01vc01.sfo01.rainpole.local/ui`.
   b. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. In the Networking and Security inventory, select Groups and Tags.

3. On the Groups and Tags page, from the NSX Manager drop-down menu, select the 172.16.11.65.

4. Create a security group for the Skyline Collector instances.
      The Create Security Group wizard appears.
   b. On the Name and description page, enter Skyline Collectors in the Name text box, click the Universal Synchronization toggle to On, and click Next.
   c. On the Select Objects to include page, from the Object Type drop-down menu, select IP Sets, add the Skyline Collectors IP set to the list of available objects, and click Next.
   d. On the Ready to Complete page, verify the configuration and click Finish.

5. Add the Skyline Collector appliances to the collective security group for the management appliances in the SDDC.
   a. On the Security Group page, select the group label VMware Appliances and click the Edit Security Group icon.
      The Edit Security Group wizard appears.
   b. On the Name and description page, click Next.
   c. On the Select objects to include page, from the Object Type drop-down menu, select Security Group, add the Skyline Collectors group to the list of available objects, and click Next.
   d. On the Ready to Complete page, verify the configuration values that you entered and click Finish.

Create a Distributed Firewall Rule for the Skyline Collector Instances

For security reasons, only other solutions in the SDDC and approved administration IP addresses can directly communicate with individual management components including the Skyline Collector instances.

To allow HTTPS access to the Skyline Collector, you create a rule in the distributed firewall.
Procedure

1. Log in to vCenter Server by using the vSphere Client.
   a. Open a Web browser and go to https://sfo01m01vc01.sfo01.rainpole.local/ui.
   b. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. In the Networking and Security inventory, select Firewall.

3. On the Firewall page, from the NSX Manager drop-down menu, select the 172.16.11.65.

4. Select the VMware Management Services section and click Add rule.

5. In the Name column of the new rule, enter Allow Skyline to admins.

6. Click the Edit icon in the Source column.

7. In the Specify Source dialog box, change the Object Type to Security Group, add Administrators to the Selected Objects list, and click Save.

8. In the Allow Skyline to admins rule, click the Edit icon in the Destination column.

9. In the Specify Destination dialog box, change the Object Type to Security Group, add Skyline Collectors to the Selected Objects list, and click Save.

10. Click the Edit icon in the Service column, enter HTTPS in the search filter, add HTTPS to the Selected Objects list, and click Save.

11. On the Firewall page, click the Publish button.

Prepare for Skyline Collector Registration with VMware Cloud Services

Before you register the Skyline Collector instances with VMware Cloud Services and start using VMware Skyline for proactive product support, you must create an organization on VMware Cloud Services and generate a registration token the Skyline Collector instances.

Procedure

1. Create an Organization on VMware Cloud Services
   To enable registration of your Skyline Collector instances, first create an organization on VMware Cloud Services.

2. Associate Support Entitlement with VMware Skyline on VMware Cloud Services
   Associate your Production Support or Premier Services Support Entitlement with Skyline so that you can connect the Skyline Collector instances to VMware Cloud and see product analytics data in Skyline Advisor.
3  Create a Token for Skyline Collector Registration with VMware Cloud Services

When you register a Skyline Collector instance with your VMware Cloud Services organization, you provide a registration token.

Create an Organization on VMware Cloud Services

To enable registration of your Skyline Collector instances, first create an organization on VMware Cloud Services.

Prerequisites

You must have an active VMware support entitlement. See VMware Skyline Architecture.

Procedure

1  Log in to the getting started page of VMware Skyline.
   a  Open a Web browser and go to https://skyline.vmware.com/get-started.
   b  Click Get started now.
   c  Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Email address registered with My VMware</td>
</tr>
<tr>
<td>Password</td>
<td>Password for My VMware</td>
</tr>
</tbody>
</table>

2  Click Create Your First Organization.

3  On the Set up your organization page, enter settings for your organization and click Continue.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization Name</td>
<td>Name of your organization on VMware Cloud Services</td>
</tr>
<tr>
<td>Organization Address</td>
<td>Country of your organization</td>
</tr>
<tr>
<td></td>
<td>Address of your organization</td>
</tr>
<tr>
<td></td>
<td>City where organization is located</td>
</tr>
<tr>
<td></td>
<td>State where your organization is located</td>
</tr>
<tr>
<td></td>
<td>Zip code of your organization's location</td>
</tr>
<tr>
<td>I agree to VMware Cloud Services Terms of Service</td>
<td>Selected</td>
</tr>
</tbody>
</table>

After you create the Organization on VMware Cloud Services, the Associate Support Entitlement to Skyline page appears.
**Associate Support Entitlement with VMware Skyline on VMware Cloud Services**

Associate your Production Support or Premier Services Support Entitlement with Skyline so that you can connect the Skyline Collector instances to VMware Cloud and see product analytics data in Skyline Advisor.

**Procedure**

1. Log in to the getting started page of VMware Skyline.
   a. Open a Web browser and go to [https://skyline.vmware.com/get-started](https://skyline.vmware.com/get-started).
   b. Click **Get started now**.
   c. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Email address registered with My VMware</td>
</tr>
<tr>
<td>Password</td>
<td>Password for My VMware</td>
</tr>
</tbody>
</table>

2. Click **Associate Support Entitlement**.

3. Click **Proceed to Next Step**.

**Create a Token for Skyline Collector Registration with VMware Cloud Services**

When you register a Skyline Collector instance with your VMware Cloud Services organization, you provide a registration token.

**Procedure**

1. Log in to the getting started page of VMware Skyline.
   a. Open a Web browser and go to [https://skyline.vmware.com/get-started](https://skyline.vmware.com/get-started).
   b. Click **Get started now**.
   c. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>Email address registered with My VMware</td>
</tr>
<tr>
<td>Password</td>
<td>Password for My VMware</td>
</tr>
</tbody>
</table>

2. Click **Step 4 - Register Skyline Collector**.

3. Click **Create New Token**, copy, and save the token.

A token for Skyline Collector registration is valid for 12 hours. If a token expires, you must generate a new one.
Generate Certificates for the Skyline Collector Appliances

To generate certificates signed by the Microsoft certificate authority (MSCA) for the Skyline Collector appliances in a single operation, use the VMware Validated Design Certificate Generation Utility (CertGenVVD).

For information about the VMware Validated Design Certificate Generation Utility, see VMware Knowledge Base article 2146215.

Prerequisites

- Provide a Window Server host that is part of the rainpole.local domain.
- Install a Certificate Authority server on the rainpole.local domain.

Procedure

1. Log in to a Windows host that has access to your data center.
2. Download the CertGenVVD-version.zip file of the Certificate Generation Utility from VMware Knowledge Base article 2146215 on the Windows host and extract the ZIP file to the C: drive.
3. In the C:\CertGenVVD-version folder, open the default.txt file in a text editor.
4. Verify that the following properties are configured:

```
ORG=Rainpole Inc.
OU=Rainpole.local
LOC=SFO
ST=CA
CC=US
CN=VMware_VVD
keysize=2048
```
5. Delete all files from C:\CertGenVVD-version\ConfigFiles.
6. Create the configuration files for the Skyline Collector appliances in the C:\CertGenVVD-version\ConfigFiles folder.

<table>
<thead>
<tr>
<th>Region</th>
<th>Configuration Filename</th>
<th>Common Name (CN)</th>
<th>Subject Alternative Name (SAN)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Region A</td>
<td>sky.sfo01.txt</td>
<td>sfo01sky01.sfo01.rainpole.local</td>
<td>sfo01sky01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>Region B</td>
<td>sky.lax01.txt</td>
<td>lax01sky01.lax01.rainpole.local</td>
<td>lax01sky01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

7. Insert the following content in each configuration file.

Set the FQDN of the collector appliances as the certificate common name in the [CERT] section and as a subject alternative name in the [SAN] section.
8 Open a Windows PowerShell prompt and navigate to the CertGenVVD folder.

```powershell
cd C:\CertGenVVD-version
```

9 Grant permissions to run third-party PowerShell scripts.

```powershell
Set-ExecutionPolicy Unrestricted
```

10 Validate if you can run the utility by using the configuration on the host and verify if VMware is included in the CA template policy in the command output.

```powershell
."\CertgenVVD-version.ps1 -validate
```

11 Generate the CA-signed certificates.

```powershell
."\CertGenVVD-version.ps1 -MSCASigned -attrib 'CertificateTemplate:VMware'
```

12 Verify that the C:\CertGenVVD-version folder contains the SignedByMSCACerts subfolder.

**Deploy and Configure the Skyline Collector Instances**

After preparing the environment, deploy the Skyline Collector appliances and connect them to VMware Cloud Services and to the solution endpoints in the SDDC.
Procedure

1. **Deploy the Skyline Collector Appliance in Region A**
   You deploy the Skyline Collector virtual appliance and configure storage, networking, and other key appliance attributes in Region A.

2. **Configure the Skyline Collector Instance in Region A**
   After deploying the Skyline Collector instance in Region A, proceed to the Skyline Collector configuration.

3. **Deploy the Skyline Collector Appliance in Region B**
   You deploy the Skyline Collector virtual appliance and configure storage, networking, and other key appliance attributes in Region B.

4. **Configure the Skyline Collector Instance in Region B**
   After you deploy the Skyline Collector appliance in Region B, proceed with the Skyline Collector configurations.

### Deploy the Skyline Collector Appliance in Region A

You deploy the Skyline Collector virtual appliance and configure storage, networking, and other key appliance attributes in Region A.

**Procedure**

1. Log in to vCenter Server by using the vSphere Client.
   a. Open a Web browser and go to [https://sfo01m01vc01.sfo01.rainpole.local/ui](https://sfo01m01vc01.sfo01.rainpole.local/ui).
   b. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. From the **Home** menu, select **Global Inventory Lists > vCenter Servers**.

3. Right-click **sfo01m01vc01.sfo01.rainpole.local** and select **Deploy OVF Template**.

4. On the **Select template** page, select **Local file**, browse to the location of the Skyline Collector OVA file, and click **Next**.

5. On the **Select name and location** page, enter the following information, and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>sfo01sky01</td>
</tr>
<tr>
<td>Datacenter</td>
<td>sfo01-m01dc</td>
</tr>
<tr>
<td>VM Folder</td>
<td>sfo01-m01fd-mgmt</td>
</tr>
</tbody>
</table>

6. On the **Select a resource** page, select **sfo01-m01-mgmt01** and click **Next**.
7 On the **Review details** page, review the virtual appliance details such as product, version, download size, and size on disk, and click **Next**.

8 On the **Accept license agreements** page, read and accept the End-User License Agreement, and click **Next**.

9 On the **Select storage** page, select the following parameters and click **Next**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select virtual disk format</td>
<td>Thin provision</td>
</tr>
<tr>
<td>VM storage policy</td>
<td>vSAN Default Storage Policy</td>
</tr>
<tr>
<td>Datastores</td>
<td>sfo01-m01-vsano1</td>
</tr>
</tbody>
</table>

10 On the **Select networks** page, select the distributed port group that ends with Mgmt-RegionA01-VXLAN from the **Destination Network** drop-down menu and click **Next**.

11 On the **Customize template** page, enter and confirm the root password for the virtual appliance in the **Application** section.

12 On the **Customize template** page, configure the following values in the **Networking Properties** section and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway</td>
<td>192.168.31.1</td>
</tr>
<tr>
<td>Domain Name</td>
<td>sfo01.rainpole.local</td>
</tr>
<tr>
<td>Domain Name Servers</td>
<td>172.16.11.5,172.16.11.4</td>
</tr>
<tr>
<td>Domain Search Path</td>
<td>sfo01.rainpole.local, rainpole.local</td>
</tr>
<tr>
<td>Network 1 IP Address</td>
<td>192.168.31.70</td>
</tr>
<tr>
<td>Network 1 Netmask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

13 On the **Ready to complete** page, click **Finish** and wait for the process to complete.

14 Power on the Skyline Collector virtual appliance.

   a From the **Home** menu, select **Hosts and Clusters**.

   b Expand the sfo01m01vc01.sfo01.rainpole.local tree.

   c Select the **sfo01sky01** virtual machine and from the **Actions** menu select **Power > Power on**.

**Configure the Skyline Collector Instance in Region A**

After deploying the Skyline Collector instance in Region A, proceed to the Skyline Collector configuration.

**Procedure**

1 **Enable SSH on the Skyline Collector Appliance in Region A**

   You enable SSH on the Skyline Collector appliance in Region A before you enable NTP, change certificates, and enable logging.
2 Replace the Certificate for the Appliance Interface of the Skyline Collector Instance in Region A
To establish a trusted connection to the Skyline Collector instance in Region A, you replace the SSL certificate for the virtual appliance management interface (VAMI) with a custom certificate. The custom certificate is signed by the certificate authority available on the parent Active Directory or on the intermediate Active Directory.

3 Replace the Certificate for the Skyline Collector User Interface in Region A
To establish a trusted connection to the Skyline Collector user interface, you replace the SSL certificate for the Skyline Collector application with a custom certificate. The custom certificate is signed by the certificate authority available on the parent Active Directory or on the intermediate Active Directory.

4 Configure NTP on the Skyline Collector in Region A
Configure NTP on the Skyline Collector virtual appliance in Region A to keep it synchronized with the other SDDC components.

5 Connect Skyline Collector to vRealize Log Insight in Region A
Install and configure the vRealize Log Insight Linux Agent on the Skyline Collector virtual appliance in Region A to forward logs to the vRealize Log Insight Cluster in Region A.

6 Complete the Initial Configuration of the Skyline Collector in Region A
After you complete the deployment and appliance settings, perform the initial configuration of the Skyline Collector instance in Region A for the management cluster.

7 Register the Shared Edge and Compute Cluster with the Skyline Collector Instance in Region A
After completing the initial configuration for the management cluster, register the vCenter Server and NSX Manager endpoints with the Skyline Collector instance in Region A.

8 Disable SSH on the Skyline Collector Instance in Region A
After you complete the deployment and configuration, disable the SSH access on the Skyline Collector appliance in Region A for security reasons.

Enable SSH on the Skyline Collector Appliance in Region A
You enable SSH on the Skyline Collector appliance in Region A before you enable NTP, change certificates, and enable logging.

Procedure
1 Log in to vCenter Server by using the vSphere Client.
   a Open a Web browser and go to https://sfo01m01vc01.sfo01.rainpole.local/ui.
   b Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>
In the VMs and templates inventory, expand the sfo01m01vc01.sfo01.rainpole.local tree and expand the sfo01-m01dc data center.

In sfo01-m01fd-mgmt virtual machine folder, right-click the sfo01sky01 appliance and select Open Console.

In the console to the appliance, press Enter to switch to the command prompt.

At the command prompt, log in as the root user by using skyline_root_password password.

Open the SSH daemon configuration in the vi editor by running this command.

```
vi /etc/ssh/sshd_config
```

To permit SSH login for the root user, set the PermitRootLogin property to yes in the sshd_config file.

```
PermitRootLogin yes
```

Save the configuration and exit the vi editor.

Restart the SSH daemon on the virtual appliance by running this command.

```
systemctl restart sshd
```

To return to the original screen, run the exit command.

Close the virtual appliance console.

**Replace the Certificate for the Appliance Interface of the Skyline Collector Instance in Region A**

To establish a trusted connection to the Skyline Collector instance in Region A, you replace the SSL certificate for the virtual appliance management interface (VAMI) with a custom certificate. The custom certificate is signed by the certificate authority available on the parent Active Directory or on the intermediate Active Directory.

**Procedure**

1. On the Windows machine that you use to generate certificates, in the C:\CertGenVVD-version\SignedByMSCACerts folder, duplicate the files generated by using the VMware Validated Design Certificate Generation Utility under new file names.

<table>
<thead>
<tr>
<th>File Type</th>
<th>Original FileName</th>
<th>New FileName</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>sfo01sky01.2.chain.pem</td>
<td>nginx-selfsigned.crt</td>
</tr>
<tr>
<td>Key</td>
<td>sfo01sky01-orig.key</td>
<td>nginx-selfsigned.key</td>
</tr>
</tbody>
</table>
2  Log in to the Skyline Collector virtual appliance by using a Secure Shell (SSH) client.
   a  Open an SSH connection to sfo01sky01.sfo01.rainpole.local.
   b  Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_root_password</td>
</tr>
</tbody>
</table>

3  By using scp software such as WinSCP, copy and overwrite the existing nginx-selfsigned.crt and nginx-selfsigned.key files in the /usr/local/skyline/ui/ directory on the appliance with the generated certificate authority signed certificate files.

4  To update the certificate on the VAMI, restart the services of the Nginx and VAMI servers.
   a  Restart the Nginx and VAMI services by running the following commands.

      systemctl restart nginx
      /etc/init.d/vami-lighttp restart

   b  Check the status of the Nginx services by running the following command.

      systemctl status nginx

5  After restarting the services, verify that the certificate is updated on the VAMI.
   a  Close any open Web browser windows.
   b  Open a Web browser window, and go to https://sfo01sky01.sfo01.rainpole.local:5480.
   c  Verify that you see the new certificate in the Web browser.

### Replace the Certificate for the Skyline Collector User Interface in Region A

To establish a trusted connection to the Skyline Collector user interface, you replace the SSL certificate for the Skyline Collector application with a custom certificate. The custom certificate is signed by the certificate authority available on the parent Active Directory or on the intermediate Active Directory.

**Procedure**

1  On the Windows machine that you use to generate certificates, in the C:\CertGenVVD-version\SignedByMSCACerts folder, duplicate the files generated by using the VMware Validated Design Certificate Generation Utility under new file names.

<table>
<thead>
<tr>
<th>File Type</th>
<th>Original File Name</th>
<th>New File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>sfo01sky01.2.chain.pem</td>
<td>server.pem</td>
</tr>
</tbody>
</table>
2. Log in to the Skyline Collector virtual appliance by using a Secure Shell (SSH) client.
   a. Open an SSH connection to sfo01sky01.sfo01.rainpole.local.
   b. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_root_password</td>
</tr>
</tbody>
</table>

3. By using scp software such as WinSCP, copy and overwrite the existing server.pem file in the /opt/vmware/etc/lighttpd/ directory on the appliance with the generated CA-signed certificate file.

4. Restart the VAMI service by running the following command.

   ```
   /etc/init.d/vami-lighttp restart
   ```

5. After restarting the service, verify that the certificate is updated on the Skyline Collector user interface.
   a. Close any open Web browser windows.
   b. Open a Web browser window and go to https://sfo01sky01.sfo01.rainpole.local.
   c. Verify that you see the new certificate in the Web browser.

**Configure NTP on the Skyline Collector in Region A**

Configure NTP on the Skyline Collector virtual appliance in Region A to keep it synchronized with the other SDDC components.

**Procedure**

1. Log in to the Skyline Collector virtual appliance by using a Secure Shell (SSH) client.
   a. Open an SSH connection to sfo01sky01.sfo01.rainpole.local.
   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_root_password</td>
</tr>
</tbody>
</table>
2. Configure the NTP source for the Skyline Collector virtual appliance.
   a. Open the /etc/systemd/timesyncd.conf file for editing using a text editor such as vi.
   ```
   vi /etc/systemd/timesyncd.conf
   ```
   b. Remove the comment for the NTP configuration and add the following NTP settings.
   ```
   NTP=ntp.sfo01.rainpole.local ntp.lax01.rainpole.local
   ```

3. Enable the systemd-timesyncd service and verify the status.
   a. Run the following command to enable the network time synchronization.
   ```
   timedatectl set-ntp true
   ```
   b. Run the following command to enable the NTP synchronization.
   ```
   systemctl restart systemd-timesyncd
   ```
   c. Run the following command to verify the status of the service.
   ```
   timedatectl status
   ```

4. Log out of the session by entering logout.

**Connect Skyline Collector to vRealize Log Insight in Region A**

Install and configure the vRealize Log Insight Linux Agent on the Skyline Collector virtual appliance in Region A to forward logs to the vRealize Log Insight Cluster in Region A.

1. Install the vRealize Log Insight Linux Agent on the Skyline Collector Appliance in Region A
   To send log data from the Skyline Collector appliance to vRealize Log Insight, install the Linux log agent on the appliance in Region A.

2. Configure the vRealize Log Insight Linux Agent on the Skyline Collector in Region A
   After installation of the vRealize Log Insight Linux Agent, configure the agent on the Skyline Collector virtual appliance to collect and forward events to vRealize Log Insight in Region A.

**Install the vRealize Log Insight Linux Agent on the Skyline Collector Appliance in Region A**

To send log data from the Skyline Collector appliance to vRealize Log Insight, install the Linux log agent on the appliance in Region A.
Procedure

1. Log in to the vRealize Log Insight user interface.
   a. Open a Web browser and go to https://sfo01vrli01a.sfo01.rainpole.local.
   b. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>deployment_admin_passwordvrli_admin_password</td>
</tr>
</tbody>
</table>

2. Click the configuration drop-down menu icon and select Administration.


4. On the Agents page, click the Download Log Insight Agent Version link.

5. In the Download Log Insight Agent Version dialog box, click Linux RPM (32-bit/64-bit) and save the .rpm file.

6. By using an scp client such as WinSCP, copy the VMware-Log-Insight-Agent-4.6.0-xxxxxx.noarch_192.168.31.10.rpm file to the /tmp folder on the appliance.

7. Log in to the Skyline Collector virtual appliance by using a Secure Shell (SSH) client.
   a. Open an SSH connection to sfo01sky01.sfo01.rainpole.local.
   b. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_root_password</td>
</tr>
</tbody>
</table>

8. Install the vRealize Log Insight Linux agent by running the following command.

   ```bash
   rpm -i /tmp/VMware-Log-Insight-Agent-4.6.0-xxxxxx.noarch_192.168.31.10.rpm
   ```

9. Turn on auto-run by default for the vRealize Log Insight agent.

   ```bash
   chkconfig liagentd on
   ```

Configure the vRealize Log Insight Linux Agent on the Skyline Collector in Region A

After installation of the vRealize Log Insight Linux Agent, configure the agent on the Skyline Collector virtual appliance to collect and forward events to vRealize Log Insight in Region A.

On the Skyline Collector virtual appliance in Region A, to configure the agent with the location of the vRealize Log Insight deployment in the region, update the liagent.ini configuration file.
Procedure

1. Open an SSH connection to the Skyline Collector virtual appliance using the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>sfo01sky01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_root_password</td>
</tr>
</tbody>
</table>

2. Edit the `liagent.ini` file on Skyline Collector using a text editor such as `vi`.

   ```bash
   vi /var/lib/loginsight-agent/liagent.ini
   ```

3. Locate the `[server]` section, remove the comment for the following parameters and insert the following values.

   ```ini
   [server]
   ; Log Insight server hostname or ip address
   ; If omitted the default value is LOGINSIGHT
   hostname=sfo01vrli01.sfo01.rainpole.local
   ; Set protocol to use:
   ; cfapi - Log Insight REST API
   ; syslog - Syslog protocol
   ; If omitted the default value is cfapi
   proto=cfapi
   ; Log Insight server port to connect to. If omitted the default value is:
   ; for syslog: 512
   ; for cfapi without ssl: 9000
   ; for cfapi with ssl: 9543
   port=9000
   ; ssl - enable/disable SSL. Applies to cfapi protocol only.
   ; Possible values are yes or no. If omitted the default value is no.
   ssl=no
   ; Time in minutes to force reconnection to the server
   ; If omitted the default value is 30
   reconnect=30
   ```

4. Press Escape and enter `:wq!` to save the file.

5. Restart the vRealize Log Insight agent on the virtual appliance.

   ```bash
   /etc/init.d/liagentd restart
   ```

6. Verify that the vRealize Log Insight agent is running on the virtual appliance.

   ```bash
   /etc/init.d/liagentd status
   ```
Complete the Initial Configuration of the Skyline Collector in Region A

After you complete the deployment and appliance settings, perform the initial configuration of the Skyline Collector instance in Region A for the management cluster.

Procedure

1. Log in to the Skyline Collector user interface.
   a. Open a Web browser and go to https://sfo01sky01.sfo01.rainpole.local.
   b. Log in by using the default credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>default</td>
</tr>
</tbody>
</table>

2. On the You must change your password on first login page, use the following credentials and click Change.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Old Password</td>
<td>default</td>
</tr>
<tr>
<td>Enter New Password</td>
<td>skyline_admin_password</td>
</tr>
<tr>
<td>Reenter New Password</td>
<td>skyline_admin_password</td>
</tr>
</tbody>
</table>

3. Click Login Again.

4. Log in to the Skyline Collector user interface by using the new credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_admin_password</td>
</tr>
</tbody>
</table>

The Initial Configuration wizard appears displaying the Network Connectivity page.

5. Configure the network connectivity of the virtual appliance.
   a. If your organization requires the use of an HTTPS Proxy, toggle Use a Proxy Server to Yes and input the configuration.
   b. Click Test Connectivity.
   c. After the Connection was successful! message appears, click Continue.

6. On the Customer Experience Improvement Program (CIEP) page, review the information and click Agree and Continue.
7 On the **Collector Registration** page, connect the Skyline Collector instance with your VMware Cloud Services organization.
   a In the **Collector Registration Token** box, enter the token you generated in the VMware Cloud Services portal.
   b Click **Register Collector** and click **Continue**.

8 On the **Continue Configuration** page, click **Continue**.

9 On the **Collector Name** page, configure the friendly name of the collector.
   a Enter `sfo01sky01.sfo01.rainpole.local` in the **Friendly Name** text box and click **Set Friendly Name**
   b After the Collector Friendly Name successfully configured! message appears, click **Continue**.

10 On the **Auto-Upgrade** page, to accept **No** as the default selection for **Enable Collector Auto-Upgrade**, click **Continue**.

11 On the **Configure vCenter** page, register the Management vCenter Server as an endpoint.
   a In the **Configure vCenter** section, enter the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Host Address</td>
<td>sfo01m01vc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>vCenter Read-Only Account</td>
<td><a href="mailto:svc-skyline-vsphere@rainpole.local">svc-skyline-vsphere@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-skyline-vsphere_password</td>
</tr>
</tbody>
</table>

   b In the **SSO Config** section, enter the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Custom SSO Configuration</td>
<td>Yes</td>
</tr>
<tr>
<td>PSC/SSO Host Address</td>
<td>sfo01psc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>SSO Admin URL</td>
<td><a href="https://sfo01psc01.sfo01.rainpole.local">https://sfo01psc01.sfo01.rainpole.local</a> /sso-adminserver/sdk/vsphere.local</td>
</tr>
<tr>
<td>SSO STS URL</td>
<td><a href="https://sfo01psc01.sfo01.rainpole.local">https://sfo01psc01.sfo01.rainpole.local</a> /sts/STSService/vsphere.local</td>
</tr>
<tr>
<td>Lookup Service URL</td>
<td><a href="https://sfo01psc01.sfo01.rainpole.local">https://sfo01psc01.sfo01.rainpole.local</a> /lookupservice/sdk/vsphere.local</td>
</tr>
</tbody>
</table>

   c In the **Data Collection** section, leave **Collect from All Datacenters** as **Yes** and click **Add**.
   d Accept the certificate from the vCenter Server instance by clicking **Continue**.
   e After the Your new vCenter has been configured successfully! message appears, click **Continue**.
On the **Configure NSX (optional)** page, register the Skyline Collector instance with the NSX Manager instance for the management cluster.

a. Enter the following and click **Add**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Address/IP</td>
<td>sfo01m01nsx01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:svc-skyline-nsx@rainpole.local">svc-skyline-nsx@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-skyline-nsx_password</td>
</tr>
</tbody>
</table>

b. Accept the certificate from the NSX Manager instance by clicking **Continue**.

c. After the Successful connection to NSX Manager sfo01m01nsx01.sfo01.rainpole.local. message appears, click **Continue**.

On the **Configure vRealize Operations (optional)** page, register the Skyline Collector instance with vRealize Operations Manager.

a. Enter the following and click **Add**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vROps Manager Host</td>
<td>vrops01svr01.rainpole.local</td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:svc-skyline-vrops@rainpole.local">svc-skyline-vrops@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-skyline-vrops_password</td>
</tr>
</tbody>
</table>

On the **Final Step** page, review the configuration and click **Finish**.

On the **System Status** page, under **Collector Overview**, verify that the status of the collector is **Your collector is running**.

On the **System Status** page, under **System Overview**, verify the status for each of the sfo01m01vc01.sfo01.rainpole.local, sfo01m01nsx01.sfo01.rainpole.local and vrops01svr01.rainpole.local endpoints is **Endpoints Working**.

**Register the Shared Edge and Compute Cluster with the Skyline Collector Instance in Region A**

After completing the initial configuration for the management cluster, register the vCenter Server and NSX Manager endpoints with the Skyline Collector instance in Region A.

Procedure

1. **Register the Compute vCenter Server with the Skyline Collector Instance in Region A**

   After completing initial configuration of the Skyline Collector instance in Region A for the management cluster, add the vCenter Server instance for the shared edge and compute cluster in Region A.
Register the NSX Manager Instance for the Shared Edge and Compute Cluster with the Skyline Collector in Region A

After completing initial configuration of the Skyline Collector in Region A for the management cluster, add the NSX Manager instance for the shared edge and compute cluster in Region A.

Register the Compute vCenter Server with the Skyline Collector Instance in Region A

After completing initial configuration of the Skyline Collector instance in Region A for the management cluster, add the vCenter Server instance for the shared edge and compute cluster in Region A.

Procedure

1. Log in to the Skyline Collector user interface.
   - a. Open a browser and go to https://sfo01sky01.sfo01.rainpole.local.
   - b. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_admin_password</td>
</tr>
</tbody>
</table>

2. Select Configuration.

3. On the vCenter section, click + Add vCenter.

4. On the Enhanced Customer Experience Improvement Program ("CEIP") page, review the information and click Continue.
5 On the Add vCenter page, enter the settings for connecting to vCenter Server to collect usage data and to the Platform Services Controller pair over vCenter Single Sign-On.

   a In the Configure vCenter section, enter the following.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Host Address</td>
<td>sfo01w01vc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>vCenter Read-Only Account</td>
<td><a href="mailto:svc-skyline-vsphere@rainpole.local">svc-skyline-vsphere@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-skyline-vsphere_password</td>
</tr>
</tbody>
</table>

   b In the SSO Config section, enter the following.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Custom SSO Configuration</td>
<td>On</td>
</tr>
<tr>
<td>PSC/SSO Host Address</td>
<td>sfo01psc01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>SSO Admin URL</td>
<td><a href="https://sfo01psc01.sfo01.rainpole.local">https://sfo01psc01.sfo01.rainpole.local</a> /ssoadminserver/sdk/vsphere.local</td>
</tr>
<tr>
<td>SSO STS URL</td>
<td><a href="https://sfo01psc01.sfo01.rainpole.local">https://sfo01psc01.sfo01.rainpole.local</a> /sts/STSService/vsphere.local</td>
</tr>
<tr>
<td>Lookup Service URL</td>
<td><a href="https://sfo01psc01.sfo01.rainpole.local">https://sfo01psc01.sfo01.rainpole.local</a> /lookupservice/sdk/vsphere.local</td>
</tr>
</tbody>
</table>

   c Leave Collect from All Datacenter to Yes.

   d In the Data Collection section, click Add.

   e To accept the certificate provided by the sfo01w01vc01.sfo01.rainpole.local vCenter Server, click Continue.

   f After the Your new vCenter has been configured successfully! message appears, click Finish.

6 In the vCenter section, verify that sfo01w01vc01.sfo01.rainpole.local appears as endpoint and the status for it is Endpoints Working.

Register the NSX Manager Instance for the Shared Edge and Compute Cluster with the Skyline Collector in Region A

After completing initial configuration of the Skyline Collector in Region A for the management cluster, add the NSX Manager instance for the shared edge and compute cluster in Region A.
Procedure

1 Log in to the Skyline Collector user interface.
   a Open a browser and go to https://sfo01sky01.sfo01.rainpole.local.
   b Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_admin_password</td>
</tr>
</tbody>
</table>

2 Select Configuration.

3 Click NSX Managers.

4 In the NSX Managers section, click + Add NSX Manager.

5 On the Enhanced Customer Experience Improvement Program ("CEIP") page, review the information and click Continue.

6 On the Add NSX Manager page, connect to the NSX Manager instance.
   a In the NSX Manager section, enter the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Address/IP</td>
<td>sfo01w01nsx01.sfo01.rainpole.local</td>
</tr>
<tr>
<td>User name</td>
<td><a href="mailto:svc-skyline-nsx@rainpole.local">svc-skyline-nsx@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-skyline-nsx_password</td>
</tr>
</tbody>
</table>

   b To accept the certificate provided by the sfo01w01nsx01.sfo01.rainpole.local NSX Manager, click Continue.

   c After the Successful connection to NSX Manager sfo01w01nsx01.sfo01.rainpole.local message appears, click Finish.

7 In the NSX Managers section, verify that sfo01w01nsx01.sfo01.rainpole.local appears as an endpoint and that its status is Endpoints Working.

Disable SSH on the Skyline Collector Instance in Region A

After you complete the deployment and configuration, disable the SSH access on the Skyline Collector appliance in Region A for security reasons.
Procedure

1. Log in to vCenter Server by using the vSphere Client.
   a. Open a Web browser and go to [https://sfo01m01vc01.sfo01.rainpole.local/ui](https://sfo01m01vc01.sfo01.rainpole.local/ui).
   b. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. In the *VMs and templates* inventory, expand the `sfo01m01vc01.sfo01.rainpole.local` tree and expand the `sfo01-m01dc` data center.

3. In `sfo01-m01fd-mgmt` virtual machine folder, right-click the `sfo01sky01` virtual appliance and select Open Console.

4. In the console to the appliance, press Enter to switch to the command prompt.

5. At the command prompt, log in as the *root* user by using `skyline_root_password` password.

6. Open the SSH daemon configuration in the *vi* editor by running this command.

   ```
   vi /etc/ssh/sshd_config
   ```

7. To disable SSH login for the *root* user, set the *PermitRootLogin* property to *no* in the `sshd_config` file.

   ```
   PermitRootLogin no
   ```

8. Save the configuration file and exit the *vi* editor.

9. Save the configuration and exit the *vi* editor.

10. Restart the SSH daemon on the virtual appliance by running this command.

   ```
   systemctl restart sshd
   ```

11. To return to the original screen, run the `exit` command.

12. Close the virtual appliance console.

**Deploy the Skyline Collector Appliance in Region B**

You deploy the Skyline Collector virtual appliance and configure storage, networking, and other key appliance attributes in Region B.
Procedure

1. Log in to vCenter Server by using the vSphere Client.
   a. Open a Web browser and go to https://lax01m01vc01.lax01.rainpole.local/ui.
   b. Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2. From the Home menu, select Global Inventory Lists > vCenter Servers.

3. Right-click lax01m01vc01.lax01.rainpole.local and select Deploy OVF Template.

4. On the Select template page, select Local file, browse to the location of the Skyline Collector OVA file, and click Next.

5. On the Select name and location page, enter the following information, and click Next.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>lax01sky01</td>
</tr>
<tr>
<td>Datacenter</td>
<td>lax01-m01dc</td>
</tr>
<tr>
<td>VM Folder</td>
<td>lax01-m01fd-mgmt</td>
</tr>
</tbody>
</table>

6. On the Select a resource page, select lax01-m01-mgmt01 and click Next.

7. On the Review details page, review the virtual appliance details such as product, version, download size, and size on disk, and click Next.

8. On the Accept license agreements page, read and accept the End-User License Agreement, and click Next.

9. On the Select storage page, select the following parameters and click Next.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select virtual disk format</td>
<td>Thin provision</td>
</tr>
<tr>
<td>VM storage policy</td>
<td>vSAN Default Storage Policy</td>
</tr>
<tr>
<td>Datastores</td>
<td>lax01-m01-vsan01</td>
</tr>
</tbody>
</table>

10. On the Select networks page, select the distributed port group that ends with Mgmt–RegionB01–VXLAN from the Destination Network drop-down menu and click Next.

11. On the Customize template page, enter and confirm the root password for the virtual appliance in the Application section.
12. On the **Customize template** page, configure the following values in the **Networking Properties** section and click **Next**.

<table>
<thead>
<tr>
<th>Option</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Gateway</td>
<td>192.168.32.1</td>
</tr>
<tr>
<td>Domain Name</td>
<td>lax01.rainpole.local</td>
</tr>
<tr>
<td>Domain Name Servers</td>
<td>172.17.11.5,172.17.11.4</td>
</tr>
<tr>
<td>Domain Search Path</td>
<td>lax01.rainpole.local,rainpole.local</td>
</tr>
<tr>
<td>Network 1 IP Address</td>
<td>192.168.32.70</td>
</tr>
<tr>
<td>Network 1 Netmask</td>
<td>255.255.255.0</td>
</tr>
</tbody>
</table>

13. On the **Ready to complete** page, click **Finish** and wait for the process to complete.

   a. From the **Home** menu, select **Hosts and Clusters**.
   b. Expand the lax01m01vc01.lax01.rainpole.local tree.
   c. Select the **lax01sky01** virtual machine and from the **Actions** menu select **Power > Power on**.

**Configure the Skyline Collector Instance in Region B**

After you deploy the Skyline Collector appliance in Region B, proceed with the Skyline Collector configurations.

### Procedure

1. **Enable SSH on the Skyline Collector Instance in Region B**
   
   You enable SSH on the Skyline Collector appliance in Region B before enabling NTP, changing certificates, and enabling logging.

2. **Replace Certificate for the Appliance Interface of the Skyline Collector Instance in Region B**
   
   To establish a trusted connection to the Skyline Collector instance in Region B, you replace the SSL certificate on the virtual appliance management interface (VAMI) with a custom certificate signed by a certificate authority that is available on the parent Active Directory or on the intermediate Active Directory.

3. **Replace the Certificate for the Skyline Collector User Interface in Region B**
   
   To establish a trusted connection to the user Skyline Collector user interface in Region B, you replace the SSL certificate for the Skyline Collector application with a custom certificate. The custom certificate is signed by the certificate authority available on the parent Active Directory or on the intermediate Active Directory.

4. **Configure NTP on the Skyline Collector in Region B**
   
   Configure NTP on the Skyline Collector virtual appliance in Region B to keep it synchronized with the other SDDC components.
5 Connect Skyline Collector to vRealize Log Insight in Region B
   Install and configure the vRealize Log Insight Linux Agent on the Skyline Collector virtual appliance in Region B to forward logs to the vRealize Log Insight Cluster in Region B.

6 Complete the Initial Configuration of the Skyline Collector Instance in Region B
   After you complete the deployment and appliance settings, perform the initial configuration of the Skyline Collector in Region B to the management cluster.

7 Register the Shared Edge and Compute Cluster with Skyline Collector in Region B
   After completing the initial configuration for the management cluster, register the vCenter Server and NSX Manager endpoints with the Skyline Collector instance in Region B.

8 Disable SSH on the Skyline Collector Instance in Region B
   After you complete the deployment and configuration, you disable SSH on the Skyline Collector virtual appliance in Region B for security reasons.

Enable SSH on the Skyline Collector Instance in Region B
You enable SSH on the Skyline Collector appliance in Region B before enabling NTP, changing certificates, and enabling logging.

Procedure
1 Log in to vCenter Server by using the vSphere Client.
   a Open a Web browser and go to https://lax01m01vc01.lax01.rainpole.local/ui.
   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2 In the VMs and templates inventory, expand the lax01m01vc01.lax01.rainpole.local tree and expand the lax01-m01dc data center.

3 In lax01-m01fd-mgmt virtual machine folder, right-click the lax01sky01 appliance and select Open Console.

4 In the console to the appliance, press Enter to switch to the command prompt.

5 At the command prompt, log in as the root user by using skyline_root_password password.

6 Open the SSH daemon configuration in the vi editor by running this command.

   vi /etc/sshd/sshd_config

7 To permit SSH login for the root user, set the PermitRootLogin property to yes in the sshd_config file.

   PermitRootLogin yes
8  Save the configuration and exit the vi editor.
9  Restart the SSH daemon on the virtual appliance by running this command.
   ```
   systemctl restart sshd
   ```
10 To return to the original screen, run the exit command.
11 Close the virtual appliance console.

**Replace Certificate for the Appliance Interface of the Skyline Collector Instance in Region B**

To establish a trusted connection to the Skyline Collector instance in Region B, you replace the SSL certificate on the virtual appliance management interface (VAMI) with a custom certificate signed by a certificate authority that is available on the parent Active Directory or on the intermediate Active Directory.

**Procedure**

1  On the Windows machine that you use to generate certificates, in the `C:\CertGenVVD\version\SignedByMSCACerts` folder, duplicate the files generated by using the VMware Validated Design Certificate Generation Utility under new file names.

<table>
<thead>
<tr>
<th>File Type</th>
<th>Original File Name</th>
<th>New File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>lax01sky01.2.chain.pem</td>
<td>nginx-selfsigned.crt</td>
</tr>
<tr>
<td>Key</td>
<td>lax01sky01-orig.key</td>
<td>nginx-selfsigned.key</td>
</tr>
</tbody>
</table>

2  Log in to the Skyline Collector virtual appliance by using a Secure Shell (SSH) client.
   a  Open an SSH connection to lax01sky01.lax01.rainpole.local.
   b  Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_root_password</td>
</tr>
</tbody>
</table>

3  By using SCP software such as WinSCP, copy and overwrite the existing nginx-selfsigned.crt and nginx-selfsigned.key files in the `/usr/local/skyline/ui/` directory on the appliance with the generated certificate authority signed certificate files.
4  To update the certificate on the VAMI, restart the services of the Nginx and VAMI servers.
   a  Restart the Nginx and VAMI services by running the following commands.

   ```
   systemctl restart nginx
   /etc/init.d/vami-lighttp restart
   ```

   b  Check the status of the Nginx services by running the following command.

   ```
   systemctl status nginx
   ```

5  After you restart the services, verify that the certificate is updated on the VAMI.
   a  Close any opened Web browser windows.
   b  Open a Web browser window, and go to https://lax01sky01.lax01.rainpole.local:5480.
   c  Verify that you see the new certificate in the Web browser.

**Replace the Certificate for the Skyline Collector User Interface in Region B**

To establish a trusted connection to the user Skyline Collector user interface in Region B, you replace the SSL certificate for the Skyline Collector application with a custom certificate. The custom certificate is signed by the certificate authority available on the parent Active Directory or on the intermediate Active Directory.

**Procedure**

1  On the Windows machine that you use to generate certificates, in the C:\CertGenVVD-version\SignedByMSCACerts folder, duplicate the files generated by using the VMware Validated Design Certificate Generation Utility under new file names.

<table>
<thead>
<tr>
<th>File Type</th>
<th>Original File Name</th>
<th>New File Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate</td>
<td>lax01sky01.2.chain.pem</td>
<td>server.pem</td>
</tr>
</tbody>
</table>

2  Log in to the Skyline Collector virtual appliance by using a Secure Shell (SSH) client.
   a  Open an SSH connection to lax01sky01.lax01.rainpole.local.
   b  Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_root_password</td>
</tr>
</tbody>
</table>

3  By using SCP software such as WinSCP, copy and overwrite the existing server.pem file in the /opt/vmware/etc/lighttpd/ directory on the appliance with the generated CA-signed certificate file.
4  Restart the VAMI service by running the following command.

/etc/init.d/vami-lighttp restart

5  After restarting the service, verify that the certificate is updated on the Skyline Collector user interface.
   a  Close any open Web browser windows.
   b  Open a Web browser window and go to https://lax01sky01.lax01.rainpole.local.
   c  Verify that you see the new certificate in the Web browser.

Configure NTP on the Skyline Collector in Region B

Configure NTP on the Skyline Collector virtual appliance in Region B to keep it synchronized with the other SDDC components.

Procedure

1  Log in to the Skyline Collector virtual appliance by using a Secure Shell (SSH) client.
   a  Open an SSH connection to lax01sky01.sfo01.rainpole.local.
   b  Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_root_password</td>
</tr>
</tbody>
</table>

2  Configure the NTP source for the Skyline Collector virtual appliance.
   a  Open the /etc/systemd/timesyncd.conf file for editing using a text editor such as vi.

   vi /etc/systemd/timesyncd.conf

   NTP=ntp.lax01.rainpole.local ntp.sfo01.rainpole.local
3  Enable the systemd-timesyncd service and verify the status.
   a  Run the following command to enable the network time synchronization.
      ```
      timedatectl set-ntp true
      ```
   b  Run the following command to enable the NTP synchronization.
      ```
      systemctl restart systemd-timesyncd
      ```
   c  Run the following command to verify the status of the service.
      ```
      timedatectl status
      ```

4  Log out of the session by entering `logout`.

Connect Skyline Collector to vRealize Log Insight in Region B

Install and configure the vRealize Log Insight Linux Agent on the Skyline Collector virtual appliance in Region B to forward logs to the vRealize Log Insight Cluster in Region B.

1  Install vRealize Log Insight Linux Agent on the Skyline Collector Appliance in Region B
   To send log data from the Skyline Collector appliance to vRealize Log Insight, install the Linux log agent on the appliance in Region B.

2  Configure the vRealize Log Insight Linux Agent on the Skyline Collector in Region B
   After installation of the vRealize Log Insight Linux Agent, configure the agent on the Skyline Collector virtual appliance to collect and forward events to vRealize Log Insight in Region B.

Install vRealize Log Insight Linux Agent on the Skyline Collector Appliance in Region B

To send log data from the Skyline Collector appliance to vRealize Log Insight, install the Linux log agent on the appliance in Region B.

Procedure

1  Log in to the vRealize Log Insight user interface.
   a  Open a Web browser and go to `https://lax01vrli01.lax01.rainpole.local`.
   b  Log in using the following credentials.
      | Setting   | Value         |
      |-----------|---------------|
      | User name | admin         |
      | Password  | vrl_admin_password |

2  Click the configuration drop-down menu icon  and select Administration.

3  Under Management, click Agents.

4  On the Agents page, click the Download Log Insight Agent Version link.
5 In the Download Log Insight Agent Version dialog box, click Linux RPM (32-bit/64-bit) and save the .rpm file.

6 By using an scp client such as WinSCP, copy the VMware-Log-Insight-Agent-4.6.0-xxxxxx.noarch_192.168.32.10.rpm file to the /tmp folder on the appliance.

7 Log in to the Skyline Collector virtual appliance by using a Secure Shell (SSH) client.
   a Open an SSH connection to lax01sky01.lax01.rainpole.local.
   b Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_root_password</td>
</tr>
</tbody>
</table>

8 Install the vRealize Log Insight Linux agent by running the following command.

   ```shell
   rpm -i /tmp/VMware-Log-Insight-Agent-4.6.0-xxxxxx.noarch_192.168.32.10.rpm
   ```

9 Turn on auto-run by default for the vRealize Log Insight agent.

   ```shell
   chkconfig liagentd on
   ```

**Configure the vRealize Log Insight Linux Agent on the Skyline Collector in Region B**

After installation of the vRealize Log Insight Linux Agent, configure the agent on the Skyline Collector virtual appliance to collect and forward events to vRealize Log Insight in Region B.

On the Skyline Collector virtual appliance in Region B, to configure the agent with the location of the vRealize Log Insight deployment in the region, update the liagent.ini configuration file.

**Procedure**

1 Open an SSH connection to the Skyline Collector virtual appliance using the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname</td>
<td>lax01sky01.lax01.rainpole.local</td>
</tr>
<tr>
<td>User name</td>
<td>root</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_root_password</td>
</tr>
</tbody>
</table>

2 Edit the liagent.ini file on Skyline Collector using a text editor such as vi.

   ```shell
   vi /var/lib/loginsight-agent/liagent.ini
   ```
3 Locate the [server] section, remove the comment for the following parameters and insert the following values.

```
[server]
; Log Insight server hostname or ip address
; If omitted the default value is LOGINSIGHT
hostname=lax01vrli01.lax01.rainpole.local
; Set protocol to use:
; cfapi - Log Insight REST API
; syslog - Syslog protocol
; If omitted the default value is cfapi
proto=cfapi
; Log Insight server port to connect to. If omitted the default value is:
; for syslog: 512
; for cfapi without ssl: 9000
; for cfapi with ssl: 9543
port=9000
; ssl - enable/disable SSL. Applies to cfapi protocol only.
; Possible values are yes or no. If omitted the default value is no.
ssl=no
; Time in minutes to force reconnection to the server
; If omitted the default value is 30
; reconnect=30
```

4 Press Escape and enter `:wq!` to save the file.

5 Restart the vRealize Log Insight agent on the virtual appliance.

```
/etc/init.d/liagentd restart
```

6 Verify that the vRealize Log Insight agent is running on the virtual appliance.

```
/etc/init.d/liagentd status
```

**Complete the Initial Configuration of the Skyline Collector Instance in Region B**

After you complete the deployment and appliance settings, perform the initial configuration of the Skyline Collector in Region B to the management cluster.

**Procedure**

1 Log in to the Skyline Collector user interface.
   a Open a browser and go to `https://lax01sky01.lax01.rainpole.local`.
   b Log in by using the default credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>default</td>
</tr>
</tbody>
</table>
2. On the **You must change your password on first login** page, use the following credentials and click **Change**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enter Old Password</td>
<td>default</td>
</tr>
<tr>
<td>Enter New Password</td>
<td>skyline_admin_password</td>
</tr>
<tr>
<td>Re-enter New Password</td>
<td>skyline_admin_password</td>
</tr>
</tbody>
</table>

After you submit the change, the *Your password was changed successfully!* message appears.

3. Click **Login Again**.

4. Log in to the Skyline Collector user interface by using the new credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_admin_password</td>
</tr>
</tbody>
</table>

The **Initial Configuration** wizard appears displaying the **Network Connectivity** page.

5. Configure the network connectivity of the virtual appliance.
   
a. If your organization requires the use of an HTTPS Proxy, toggle **Use a Proxy Server** to **Yes** and input the configuration.
   
b. Click **Test Connectivity**.
   
c. After the **Connection was successful!** message appears, click **Continue**.

6. On the **Customer Experience Improvement Program (CIEP)** page, review the information displayed and click **Agree and Continue**.

7. On the **Collector Registration** page, connect the Skyline Collector instance with your VMware Cloud Services organization.
   
a. In the **Collector Registration Token** box, enter the token you generated in the VMware Cloud Services portal.
   
b. Click **Register Collector** and click **Continue**.

8. On the **Continue Configuration** page, click **Continue**.

9. On the **Collector Name** page, configure the friendly name of the collector.
   
a. Enter `sfo01sky01.sfo01.rainpole.local` in the **Friendly Name** box and click **Set Friendly Name**
   
b. After the Collector Friendly Name successfully configured! message appears, click **Continue**.

10. On the **Auto-Upgrade** page, to keep **Enable Collector Auto-Upgrade** set to **No**, click **Continue**.
11 On the **Configure vCenter** page, connect the Skyline Collector instance to the Management vCenter Server.

   a In the **Configure vCenter** section, enter the following.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Host Address</td>
<td>lax01m01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>vCenter Read-Only Account</td>
<td><a href="mailto:svc-skyline-vsphere@rainpole.local">svc-skyline-vsphere@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-skyline-vsphere_password</td>
</tr>
</tbody>
</table>

   b In the **SSO Config** section, enter the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Custom SSO Configuration</td>
<td>On</td>
</tr>
<tr>
<td>PSC/SSO Host Address</td>
<td>lax01psc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>SSO Admin URL</td>
<td><a href="https://sfo01psc01.sfo01.rainpole.local">https://sfo01psc01.sfo01.rainpole.local</a> /sso-adminserver/sdk/vsphere.local</td>
</tr>
<tr>
<td>SSO STS URL</td>
<td><a href="https://sfo01psc01.sfo01.rainpole.local">https://sfo01psc01.sfo01.rainpole.local</a> /sts/STSService/vsphere.local</td>
</tr>
<tr>
<td>Lookup Service URL</td>
<td><a href="https://sfo01psc01.sfo01.rainpole.local">https://sfo01psc01.sfo01.rainpole.local</a> /lookupservice/sdk/vsphere.local</td>
</tr>
</tbody>
</table>

   c In the **Data Collection** section, leave **Collect from All Datacenters** as **Yes** and click **Add**.

   d Accept the certificate from the vCenter Server instance by clicking **Continue**.

   e After the **Your new vCenter has been configured successfully!** message appears, click **Continue**.

12 On the **Configure NSX (optional)** page, connect the Skyline Collector instance with the NSX Manager instance for the management cluster.

   a Enter the following and click **Add**.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Address/IP</td>
<td>lax01m01nsx01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:svc-skyline-nsx@rainpole.local">svc-skyline-nsx@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-skyline-nsx_password</td>
</tr>
</tbody>
</table>

   b Accept the certificate from the NSX Manager instance by clicking **Continue**.

   c After the **Successful connection to NSX Manager lax01m01nsx01.lax01.rainpole.local. message appears, click **Continue**.

13 On the **Final Step** page, review the configuration and click **Finish**.
On the **System Status** page, under **Collector Overview**, verify that the status of the collector is **Your collector is running**.

On the **System Status** page, under **System Overview**, verify that the status for each of the `lax01m01vc01.lax01.rainpole.local` and `lax01m01nsx01.lax01.rainpole.local` endpoints is **Endpoints Working**.

**Register the Shared Edge and Compute Cluster with Skyline Collector in Region B**

After completing the initial configuration for the management cluster, register the vCenter Server and NSX Manager endpoints with the Skyline Collector instance in Region B.

**Procedure**

1. **Register the Compute vCenter Server with the Skyline Collector Instance in Region B**
   After completing initial configuration of the Skyline Collector in Region B for the management cluster, add the vCenter Server instance for the shared edge and compute cluster in Region B.

2. **Register the NSX Manager Instance for the Shared Edge and Compute Cluster with the Skyline Collector Instance in Region B**
   After completing initial configuration of the Skyline Collector in Region B for the management cluster, add the NSX Manager instance for the shared edge and compute cluster in Region B.

**Register the Compute vCenter Server with the Skyline Collector Instance in Region B**

After completing initial configuration of the Skyline Collector in Region B for the management cluster, add the vCenter Server instance for the shared edge and compute cluster in Region B.

**Procedure**

1. Log in to the Skyline Collector user interface.
   a. Open a browser and go to `https://lax01sky01.lax01.rainpole.local`.
   b. Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td><code>skyline_admin_password</code></td>
</tr>
</tbody>
</table>

2. Select **Configuration**.

3. In the **vCenter** section, click **+ Add vCenter**.

4. On the **Enhanced Customer Experience Improvement Program ("CEIP")** page, review the information and click **Continue**.
5 On the **Add vCenter** page, enter the settings for connecting to vCenter Server to collect usage data and to the Platform Services Controller pair over vCenter Single Sign-On.

   a In the **Configure vCenter** section, enter the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>vCenter Host Address</td>
<td>lax01w01vc01.lax01.rainpole.local</td>
</tr>
<tr>
<td>vCenter Read-Only Account</td>
<td><a href="mailto:svc-skyline-vsphere@rainpole.local">svc-skyline-vsphere@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-skyline-vsphere_password</td>
</tr>
</tbody>
</table>

   b In the **SSO Config** section, enter the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Custom SSO Configuration</td>
<td>On</td>
</tr>
<tr>
<td>PSC/SSO Host Address</td>
<td>lax01psc01.lax01.rainpole.local</td>
</tr>
</tbody>
</table>

   c For **Collect from All Datacenter**, retain the default selection **Yes**.

   d In the **Data Collection** section, click **Add**.

   e To accept the certificate provided by the lax01w01vc01.lax01.rainpole.local vCenter Server, click **Continue**.

   f After the Your new vCenter has been configured successfully! message appears, click **Finish**.

6 In the **vCenter** section, verify that lax01w01vc01.lax01.rainpole.local appears as an endpoint and that its status is **Endpoints Working**.

**Register the NSX Manager Instance for the Shared Edge and Compute Cluster with the Skyline Collector Instance in Region B**

After completing initial configuration of the Skyline Collector in Region B for the management cluster, add the NSX Manager instance for the shared edge and compute cluster in Region B.

**Procedure**

1 Log in to the Skyline Collector user interface.

   a Open a Web browser and go to https://lax01sky01.lax01.rainpole.local.

   b Log in by using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td>admin</td>
</tr>
<tr>
<td>Password</td>
<td>skyline_admin_password</td>
</tr>
</tbody>
</table>

2 Select **Configuration**.

3 Click **NSX Managers**.

4 In the **NSX Managers** section, click **+ Add NSX Manager**.
5 On the Enhanced Customer Experience Improvement Program ("CEIP") page, review the information and click Continue.

6 On the Add NSX Manager page, connect to the NSX Manager instance.
   a In the NSX Manager section, enter the following settings.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>NSX Address/IP</td>
<td>lax01w01nsx01.lax01.rainpole.local</td>
</tr>
<tr>
<td>Username</td>
<td><a href="mailto:svc-skyline-nsx@rainpole.local">svc-skyline-nsx@rainpole.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>svc-skyline-nsx_password</td>
</tr>
</tbody>
</table>

   b To accept the certificate provided by the lax01w01nsx01.lax01.rainpole.local NSX Manager, click Continue.

   c After the Successful connection to NSX Manager lax01w01nsx01.lax01.rainpole.local message appears, click Finish.

7 In the NSX Managers section, verify that lax01w01nsx01.lax01.rainpole.local appears as an endpoint and that its status is Endpoints Working.

Disable SSH on the Skyline Collector Instance in Region B

After you complete the deployment and configuration, you disable SSH on the Skyline Collector virtual appliance in Region B for security reasons.

Procedure

1 Log in to vCenter Server by using the vSphere Client.
   a Open a Web browser and go to https://lax01m01vc01.lax01.rainpole.local/ui.
   b Log in using the following credentials.

<table>
<thead>
<tr>
<th>Setting</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>User name</td>
<td><a href="mailto:administrator@vsphere.local">administrator@vsphere.local</a></td>
</tr>
<tr>
<td>Password</td>
<td>vsphere_admin_password</td>
</tr>
</tbody>
</table>

2 In the VMs and templates inventory, expand the lax01m01vc01.lax01.rainpole.local tree and expand the lax01-m01dc data center.

3 In lax01-m01fd-mgmt virtual machine folder, right-click the lax01sky01 appliance and select Open Console.

4 In the console to the appliance, press Enter to switch to the command prompt.

5 At the command prompt, log in as the root user by using skyline_root_password password.

6 Open the SSH daemon configuration in the vi editor by running this command.

   vi /etc/ssh/sshd_config
7 To disable SSH login for the root user, set the PermitRootLogin property to no in the sshd_config file.

    PermitRootLogin no

8 Save the configuration and exit the vi editor.

9 Restart the SSH daemon on the virtual appliance by running this command.

    systemctl restart sshd

10 To return to the original screen, run the exit command.

11 Close the virtual appliance console.