Install Concerto

For supported software information, click here.

This article describes how to install a Concerto orchestrator node in standalone mode and in cluster mode.

Before You Begin

Before you install a Concerto node, you should set up the Versa Director, Controller, and Analytics (DCA) complex.

Note: Concerto Release 10.1.1 is supported with Release 21.1.2 and later versions of the Versa DCA complex. Concerto is also supported in Release 20.2.3 with an additional patch, which you can request from the Versa TAC.

To set up the Versa DCA complex:

1. Create and initialize a Versa Director node with or without high availability (HA). See Set Up Director in Perform Initial Software Configuration.
2. Create a provider organization. See Create Provider Organizations in Perform Initial Software Configuration.

Note: To have Concerto manage multiple DCA complexes, enure that the provider organization name and global ID are the same across all the DCA complexes.

3. Create and deploy the Controller nodes. See Set Up an SD-WAN Controller in Perform Initial Software Configuration.
4. Create an Analytics cluster. See Set Up Analytics in Perform Initial Software Configuration.

Install a Concerto Node in Standalone Mode

1. Install a Concerto node on bare metal servers using the ISO file, or create a virtual machine using the qcow2 or OVA file. Each node must have two network interfaces:
   - One interface for northbound communication, which allows access to the portal UI from the internet. On the northbound interface, configure firewalls to allow only TCP ports 80 and 443 to be used to access the portal UI from the internet.
   - One interface for southbound communication, which is used for docker overlay communications and for communication with Versa Director and Versa Analytics nodes.
2. Log in to the node with the username "admin" and password "versa123".
3. In the shell, configure the hostname of the Concerto node:

```
admin@concerto-1:~$ sudo hostnamectl set-hostname hostname
```

For example:

```
admin@concerto-1:~$ sudo hostnamectl set-hostname Concerto-1
```

4. Map that hostname to IP address 127.0.1.1 in the /etc/hosts file:

```
admin@concerto-1:~$ sudo vi /etc/hosts
```

For example:

```
127.0.1.1    Concerto-1

# The following lines are desirable for IPv6 capable hosts
::1     localhost ip6-localhost ip6-loopback
ff02::1 ip6-allnodes
ff02::2 ip6-allroutes
```

5. Configure the management IP address of the Concerto node and gateway in the /etc/network/interfaces file:

```
admin@concerto-1:~$ sudo vi /etc/network/interfaces
```

6. Initialize the Concerto node by issuing the **vsh cluster init** command and entering the required information. Enter the value to 1 in response to the "Enter the number of nodes needed for the cluster" prompt to set the Concerto node to run in standalone mode.

```
admin@concerto-1:~$ vsh cluster init

ARE YOU SURE, YOU WANT TO INITIALIZE THE CONCERTO SETUP? OLD CONFIGS WILL BE
DELETED - Y/N: y
Enter the number of nodes needed for the cluster: 1
--------------------------------------------------------------------------------
Enter the IP address for node 1: 10.40.159.181
Enter the Public/External IP address or FQDN for node 1 [Press enter to reuse the node IP]:
Enter the username for node 1: admin
Enter the password for node 1: *****
Enter the number of replicas of core services to run in the cluster [Press enter to use default settings]:
```

4. Start the Concerto services by issuing the **vsh start** command. It takes a few minutes for all the services to initialize.

Note: While you do not need to configure DNS (by default, Docker uses 8.8.8.8 as the DNS server), each DNS server configured in the/etc/resolv.conf file must be reachable from the Concerto node. If one or more of the DNS servers is not reachable from the node, the **vsh start** command takes a long time to complete.

```
admin@concerto-1:~$ vsh start
   __  __                  _____                                _
  \ \  / /__ _ __ ___  __ _  |  ___|___  _ __  ___ ___ _ __ | |_ ___
   \ \/ / _ \ '__/ __|/ _` | | |_  / _ \| '_ \/ __/ _ \ '__| __/ _ \
    \  /  __/ |  \__ \ (_| | |  _|| (_) | | | | (_|  __/ |  | || (_) |
     \/ \___|_|  |___/\__,_| |_|   \___/|_| |_|\___\___|_|   \__\___/

=> Initializing Docker Swarm
```

```
=> Creating Docker Networks
=> Deploying Traefik loadbalancer...
=> Deploying Zookeeper and Kafka...
=> Deploying Miscellaneous services...
=> Deploying PostgreSQL service...
=> Waiting for PostgreSQL to start...
=> Deploying Flyway service...
=> Flyway migration suceeded
=> Cleaning stale consumer groups in kafka...
=> Deploying Hazelcast cache service...
=> Deploying Solr search service...
=> Deploying System Monitoring service...
=> Deploying Concerto services...
```

5. Check the status of the Concerto services to ensure that they are all in the Running state.

```
admin@concerto-1:~$ vsh status
postgresql           is Running
zookeeper            is Running
kafka                is Running
solr                 is Running
glances              is Running
mgmt-service         is Running
web-service          is Running
cache-service        is Running
core-service         is Running
monitoring-service   is Running
traffic              is Running
```

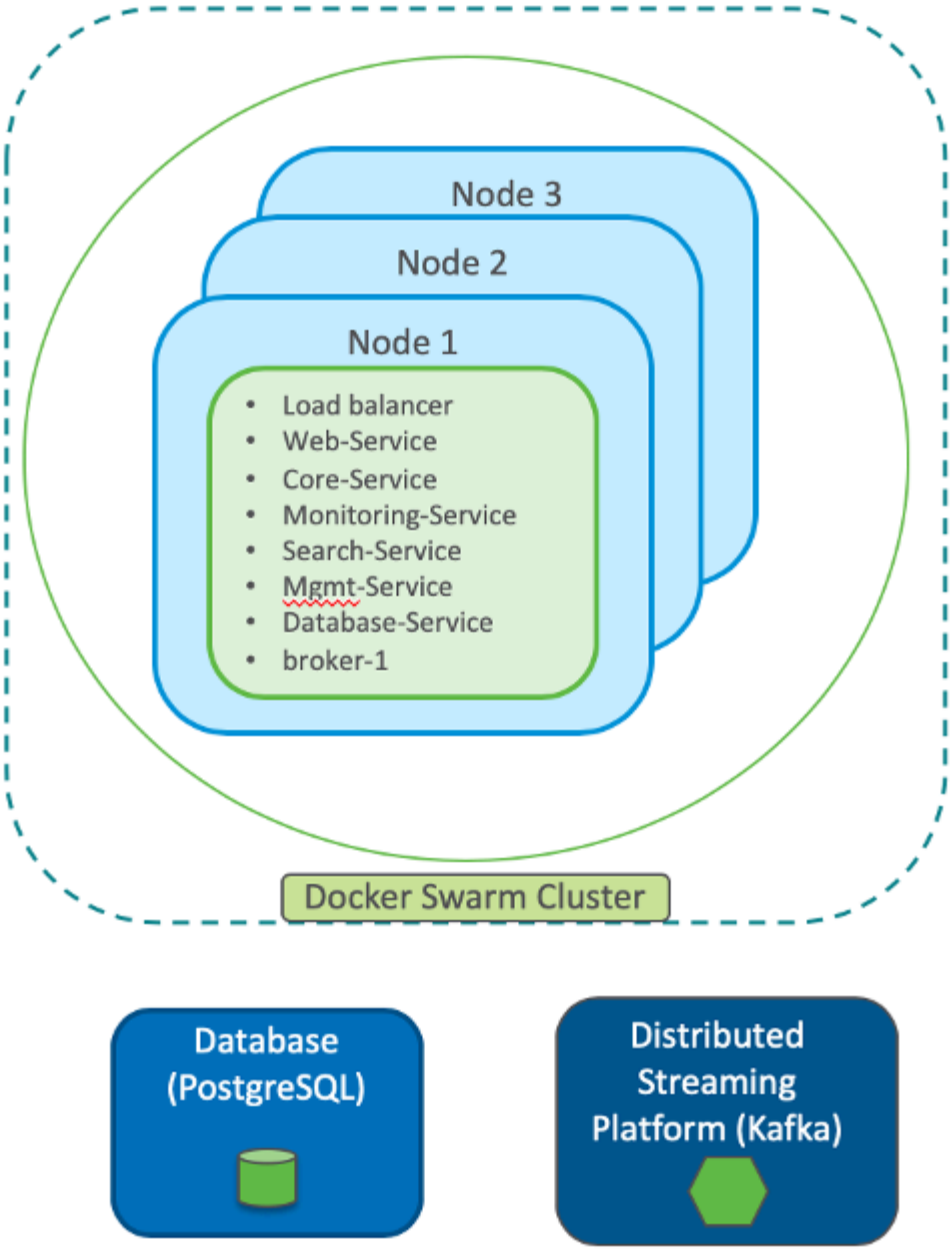
6. Display information about the Concerto node.

```
admin@concerto-1:~$ vsh cluster info

Concerto Cluster Status
-----------------------------------------------------
  Node Name:             concerto-1
  IP Address:            10.40.159.181
  Operational Status:    primary
  Configured Status:     primary
  Docker Node Status:    ready
  Node Reachability:     reachable
  GlusterFS Status:      good
```

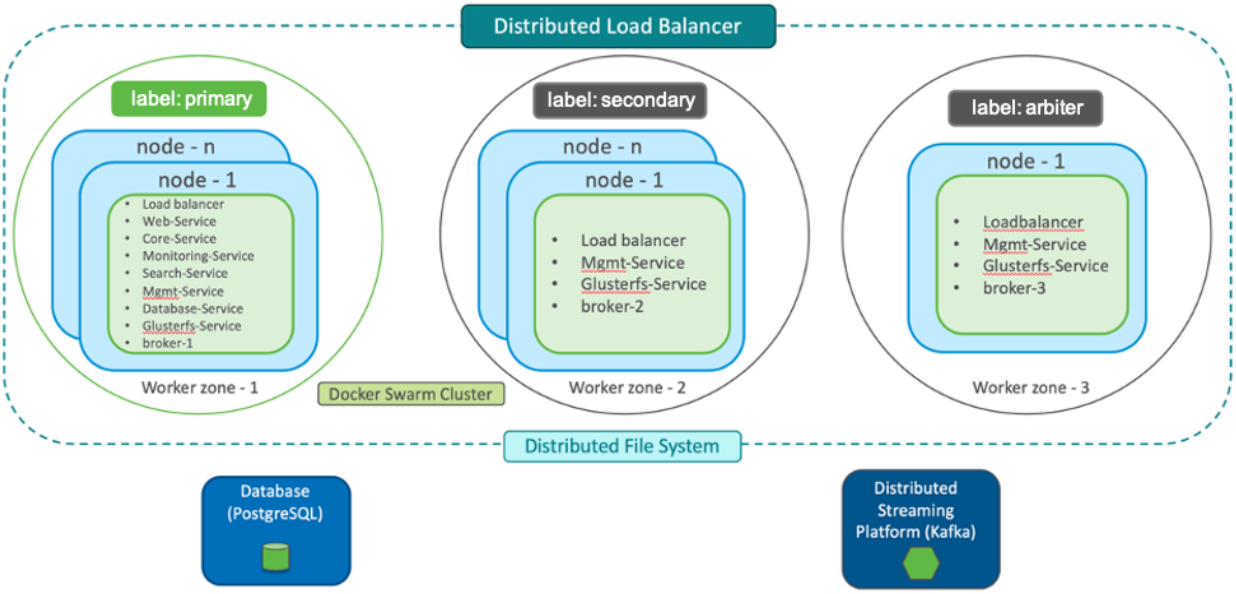
Install Concerto Nodes in Cluster Mode

You can deploy Concerto cluster nodes in two modes:

- All nodes in the cluster are of the same type and have the same role. This mode is recommended for deployments in which all the Concerto nodes are colocated in a single availability zone or data center, as shown in the following figure.



- Nodes are categorized as primary, secondary, and arbiter. This mode is recommended for deployments that require geographic redundancy and in which the nodes are spread across different availability zones or data centers, as shown in the following figure.



To install Concerto cluster nodes:

1. Create a Concerto instance for each of the nodes using the Concerto ISO or qcow2 image. Each node must have two network interfaces:
   - One interface for northbound communication, which allows access to the portal UI from the internet. On the northbound interface, configure firewalls to allow only TCP ports 80 and 443, which are used to access the portal UI from the internet.
   - One interface for southbound communication, which is used for Docker overlay communications and for communication with Versa Director and Versa Analytics nodes.
2. Initialize the cluster by logging into any of the Concerto nodes and then issuing the **vsh cluster init** command. The following table describes the prompts displayed by the **vsh cluster init** command.

Prompt	Description
Enter the number of nodes needed for the cluster	Enter the number of nodes in the cluster. In cluster mode, a minimum of three nodes are required. Setting the value to 1 sets the Concerto node to run in standalone mode.
Enter the Public/External IP address or FQDN for node *x*	If the Versa Director node communicates with the Concerto cluster using a public (external) IP address or FQDN, enter the IP address or FQDN.
Enter the username for node *x* Enter the password for node *x*	Enter the user credentials for SSH login to the node.
Select the node type: 1. Primary 2. Secondary 3. Arbiter Select the value:	Label each node for a particular role. For a simpler deployment, you can label all nodes as type Primary. For deployments requiring geographic redundancy, you label the nodes differently based on the role assigned to them. For example, in a deployment that has three availability zones (AZ-1, AZ-2, and AZ-3), you can assign two nodes as Primary node types (AZ-1), two nodes as Secondary node types (AZ-2), and one node as an Arbiter node type (AZ-3). Nodes of the same node type must be colocated in the same availability zone.
Enter the number of replicas of core services to run in the cluster	Determines the number of instances of core services, web services, and monitoring services to deploy in the cluster. All these attributes are included in the /var/versa/ecp/share/config/clusterconfig.json file.

Note: All nodes in a Concerto cluster must have a unique hostname. Otherwise, in multimode configurations, the service startup fails. Before you deploy a cluster, review the hostnames for all nodes in the cluster and update them if necessary. To add or update the hostname:

1. In the shell, configure a new hostname:

   admin@concerto-1:~$ **sudo hostnamectl set-hostname** *new-hostname*

2. Edit the /etc/hosts file, and replace any occurrences of the existing hostname with the new hostname:

   admin@concerto-1:~$ **sudo nano /etc/hosts**

Example: Create a Concerto Cluster Using the Same Node Type

The following example shows the creation of three nodes that are assigned the same node type, Primary.

```
admin@concerto-1:~$ vsh cluster init
ARE YOU SURE, YOU WANT TO INITIALIZE THE CONCERTO SETUP? OLD CONFIGS WILL BE DELETED -
 Y/N: y
Enter the number of nodes needed for the cluster: 3
--------------------------------------------------------------------------------
Enter the IP address for node 1: 10.48.7.81
Enter the Public/External IP address or FQDN for node 1 [Press enter to reuse the node IP]: concerto-1.versa-networks.com
Enter the username for node 1: admin
Enter the password for node 1: *****
Select the node type:
1. Primary
2. Secondary
3. Arbiter
Select the value: 1
--------------------------------------------------------------------------------
Enter the IP address for node 2: 10.48.7.82
Enter the Public/External IP address or FQDN for node 2 [Press enter to reuse the node IP]: concerto-2.versa-networks.com
Enter the username for node 2: admin
Enter the password for node 2: *****
Select the node type:
1. Primary
2. Secondary
3. Arbiter
Select the value: 1
--------------------------------------------------------------------------------
Enter the IP address for node 3: 10.40.30.80
Enter the Public/External IP address or FQDN for node 3 [Press enter to reuse the node IP]: concerto-3.versa-networks.com
Enter the username for node 3: admin
Enter the password for node 3: *****
Select the node type:
1. Primary
2. Secondary
3. Arbiter
Select the value: 1
Enter the number of replicas of core services to run in the cluster [Press enter to use default settings]:

admin@concerto-1:~$ vsh cluster info
Concerto Cluster Status
--------------------------------------------------
    Node Name:             concerto-3
    IP Address:            10.40.30.80
    Operational Status:    primary
    Configured Status:     primary
    Docker Node Status:    ready
    Node Reachability:     reachable
    GlusterFS Status:      good
```

```
Node Name:              concerto-1
IP Address:             10.48.7.81
Operational Status:     primary
Configured Status:      primary
Docker Node Status:     ready
Node Reachability:      reachable
GlusterFS Status:       good

Node Name:              concerto-2
IP Address:             10.48.7.82
Operational Status:     primary
Configured Status:      primary
Docker Node Status:     ready
Node Reachability:      reachable
GlusterFS Status:       good
-------------------------------------------------
```

Example: Creating a Concerto Cluster Using Different Node Types

The following example shows the creation of three nodes that are assigned the different node types, Primary, Secondary, and Arbiter.

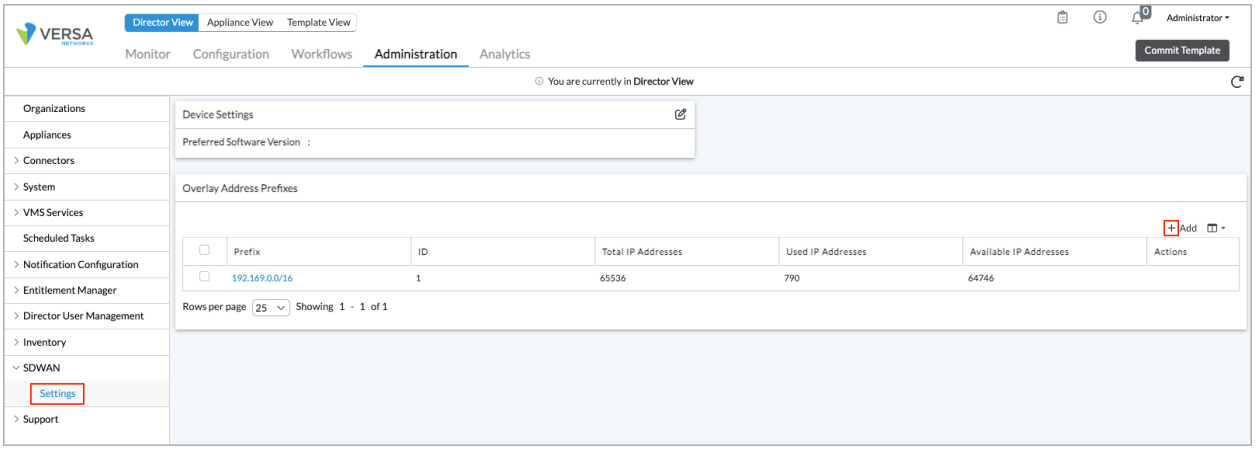
```
admin@concerto-1:~$ vsh cluster init
ARE YOU SURE, YOU WANT TO INITIALIZE THE CONCERTO SETUP? OLD CONFIGS WILL BE DELETED -
 Y/N: y
Enter the number of nodes needed for the cluster: 3
--------------------------------------------------------------------------------
Enter the IP address for node 1: 10.48.7.
81
Enter the Public/External IP address or FQDN for node 1 [Press enter to reuse the node IP]: concerto-1.versa-
networks.com
Enter the username for node 1: admin
Enter the password for node 1: *****
Select the node
type:
1. Primary
2.
Secondary
3. Arbiter
Select the value: 1
--------------------------------------------------------------------------------
Enter the IP address for node 2: 10.48.7.82
Enter the Public/External IP address or FQDN for node 2 [Press enter to reuse the node IP]: concerto-2.versa-
networks.com
Enter the username for node 2: admin
Enter the password for node 2: *****
Select the node type:
1.
Primary
2. Secondary
3.
```

```
Arbiter
Select the value: 2
--------------------------------------------------------------------------------
Enter the IP address for node 3: 10.40.30.80
Enter the Public/External IP address or FQDN for node 3 [Press enter to reuse the node IP]: concerto-3.versa-networks.com
Enter the username for node 3: admin
Enter the password for node 3:
*****
Select the node type:
1. Primary
2. Secondary
3. Arbiter
Select the value: 3
Enter the number of replicas of core services to run in the cluster [Press enter to use default settings]:

admin@concerto-1:~$ vsh cluster info
Concerto Cluster Status
--------------------------------------------------
    Node Name:             concerto-2
    IP Address:            10.48.7.82
    Operational Status:    secondary
    Configured Status:     secondary
    Docker Node Status:    ready
    Node Reachability:     reachable
    GlusterFS Status:      good

    Node Name:             concerto-1
    IP Address:            10.48.7.81
    Operational Status:    primary
    Configured Status:     primary
    Docker Node Status:    ready
    Node Reachability:     reachable
    GlusterFS Status:      good

    Node Name:             concerto-3
    IP Address:            10.40.30.80
    Operational Status:    arbiter
    Configured Status:     arbiter
    Docker Node Status:    ready
    Node Reachability:     reachable
    GlusterFS Status:      good

--------------------------------------------------
```

Attach a Concerto Portal to a Versa DCA Complex

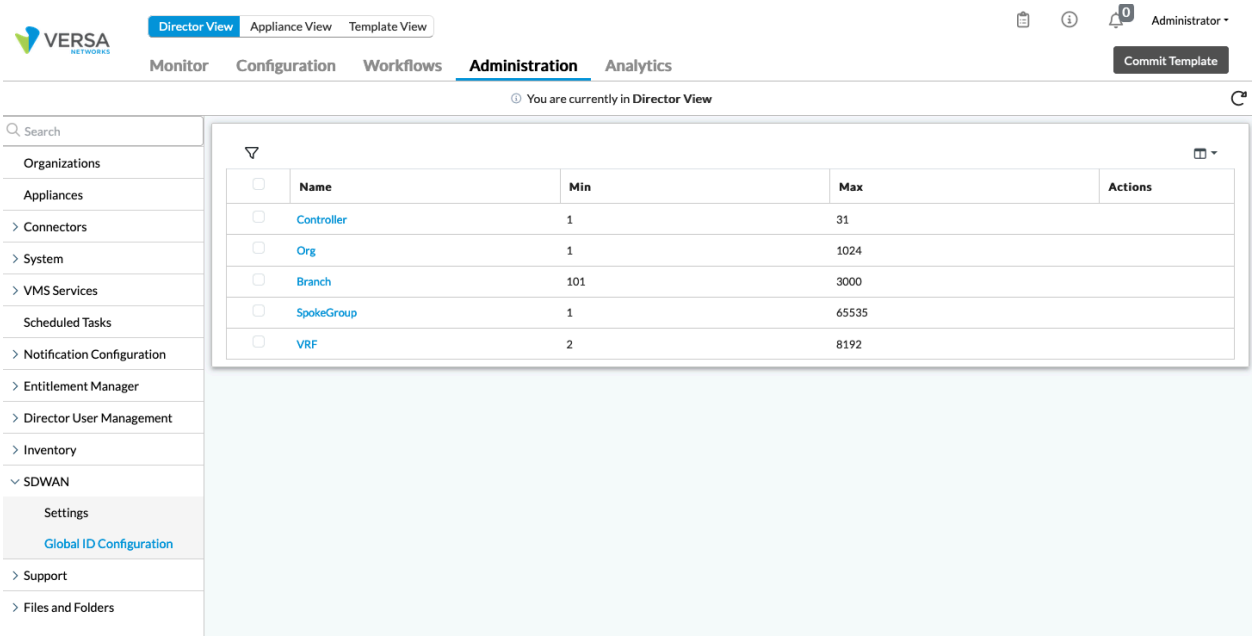
If multiple Versa Director complexes are attached to the same Concerto portal, configure each Director node with non-overlapping overlay address prefixes, device ID ranges, and Controller ID ranges after the Director nodes are installed but before any Controller nodes are created on the Director nodes.

1. In Director view, select the Administration tab in the top menu bar.
2. Select SD-WAN > Settings in the left menu bar. The Settings dashboard screen displays.

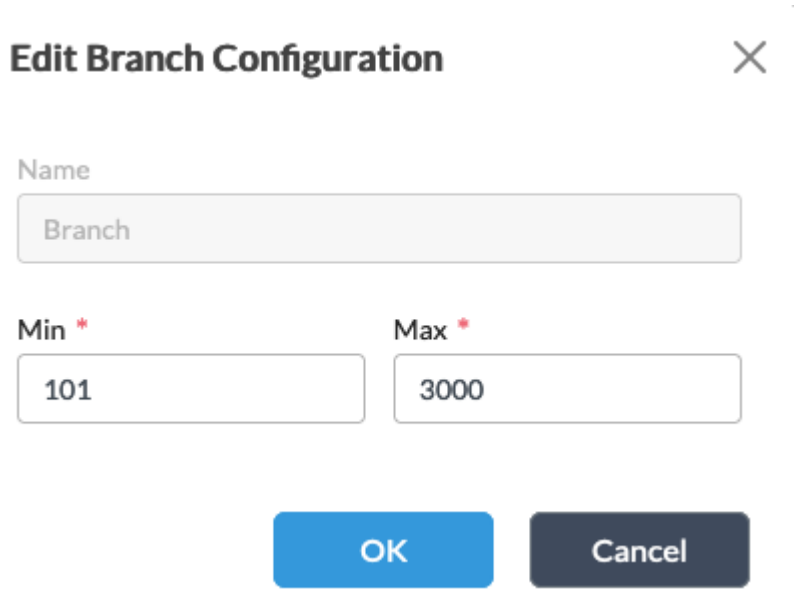


3. Click the Add icon in the Overlay Address Prefixes pane. The Overlay Address screen displays.

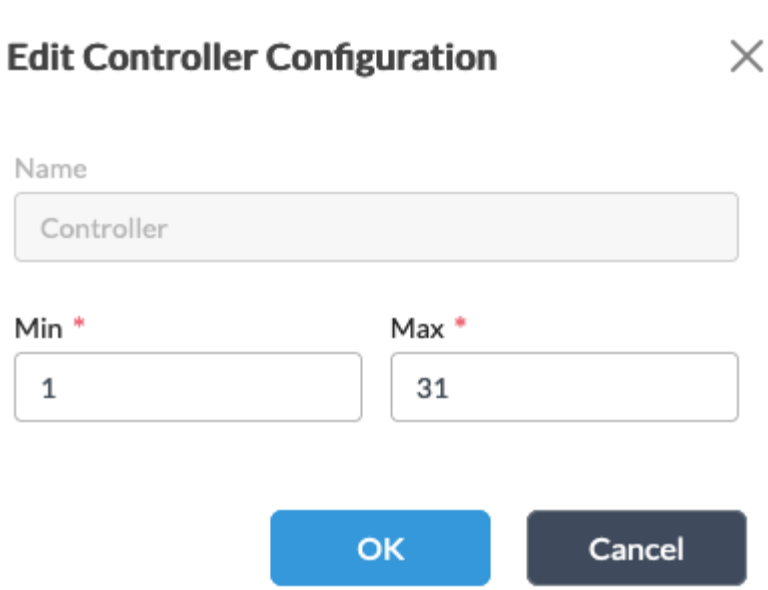
4. In the Prefix field, enter a non-overlapping overlay address prefix.
5. Click OK.
6. Select SD-WAN > Global ID Configuration in the left menu bar. The following screen displays.



7. To configure the device ID range on the Director node, click Branch in the main pane.
8. In the Edit Branch Configuration popup window, enter the Minimum and Maximum device ID range values.



9. Click OK.
10. To configure the Controller ID range on the Director node, click Controller in the main pane.
11. In the Edit Controller Configuration popup window, enter the Minimum and Maximum Controller ID range values.



12. Click OK.
13. (For releases 21.2.3 and earlier.) Configure the device and Controller ID ranges on the Director node using the CLI.
    a. To configure the device ID range, issue the following CLI command:

       admin@Director% **set nms sdwan global-config** *branch-id-range*

    b. To configure the Controller ID range, issue the following CLI command:

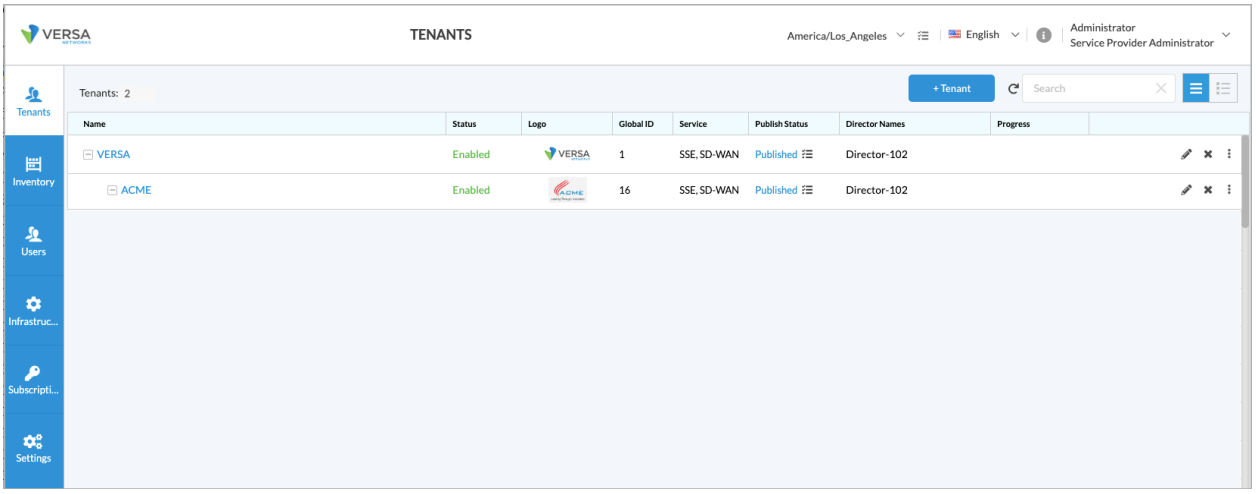
       admin@Director% **set nms sdwan global-config** *controller-id-range*

Create a Director Cluster

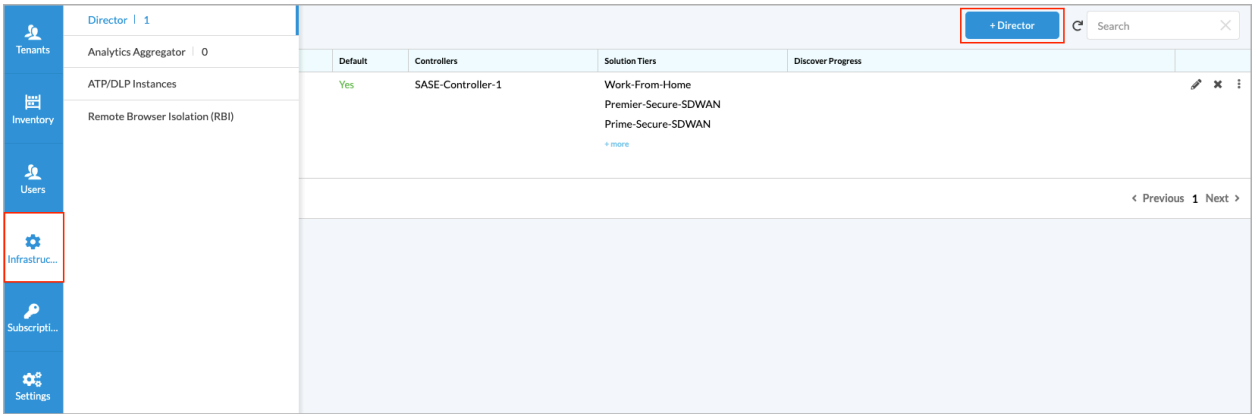
A Director cluster is a pair of Director nodes that are configured for HA. Each pair of Director nodes in a cluster operates in active–standby mode.

To add a Director cluster in the Concerto portal:

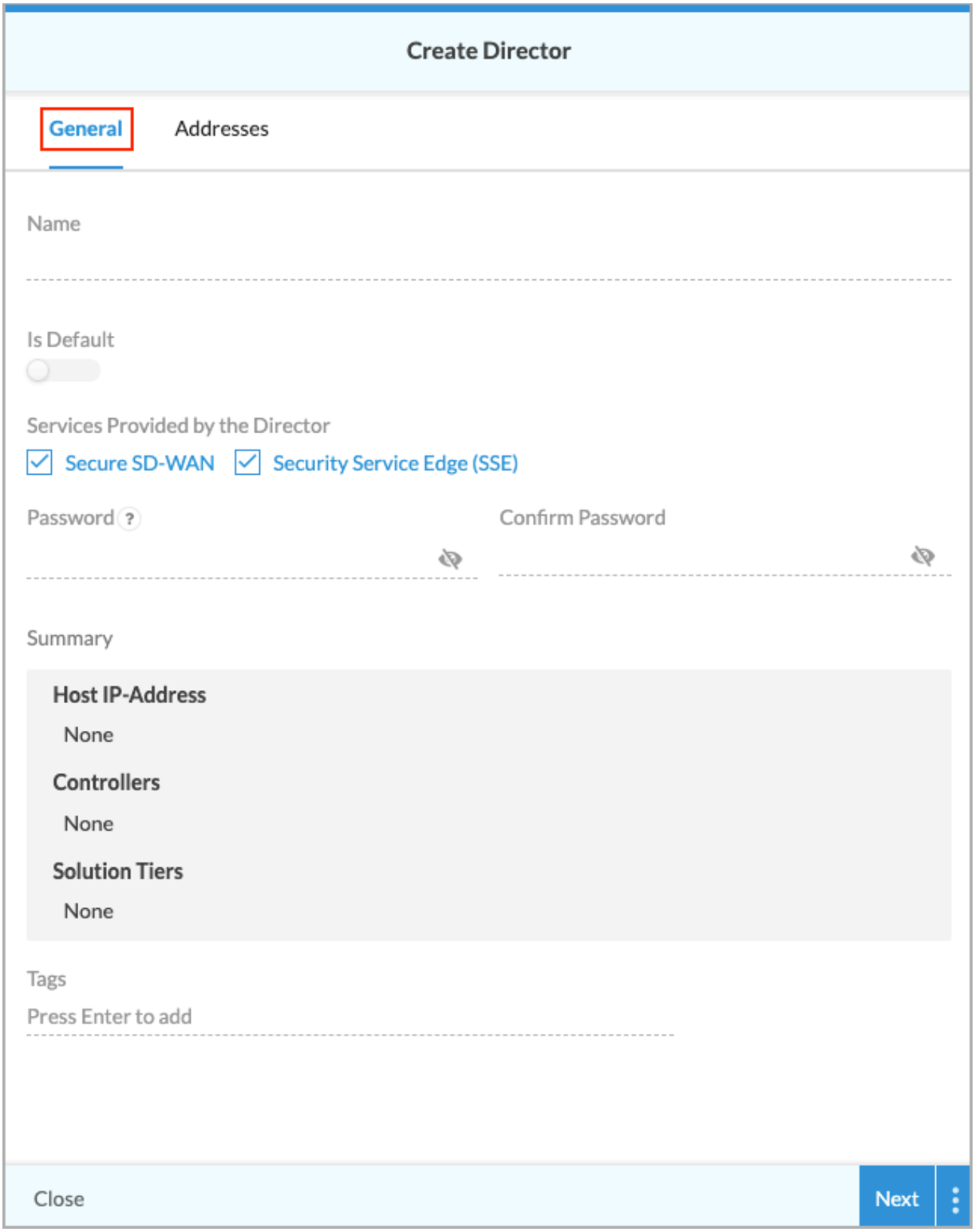
1. Log in to Concerto as an administrator. The Tenants home screen displays.



2. In the left menu bar, select Infrastructure.



3. Click +Director. In the Create Director screen, select the General tab, and then enter information for the following fields.

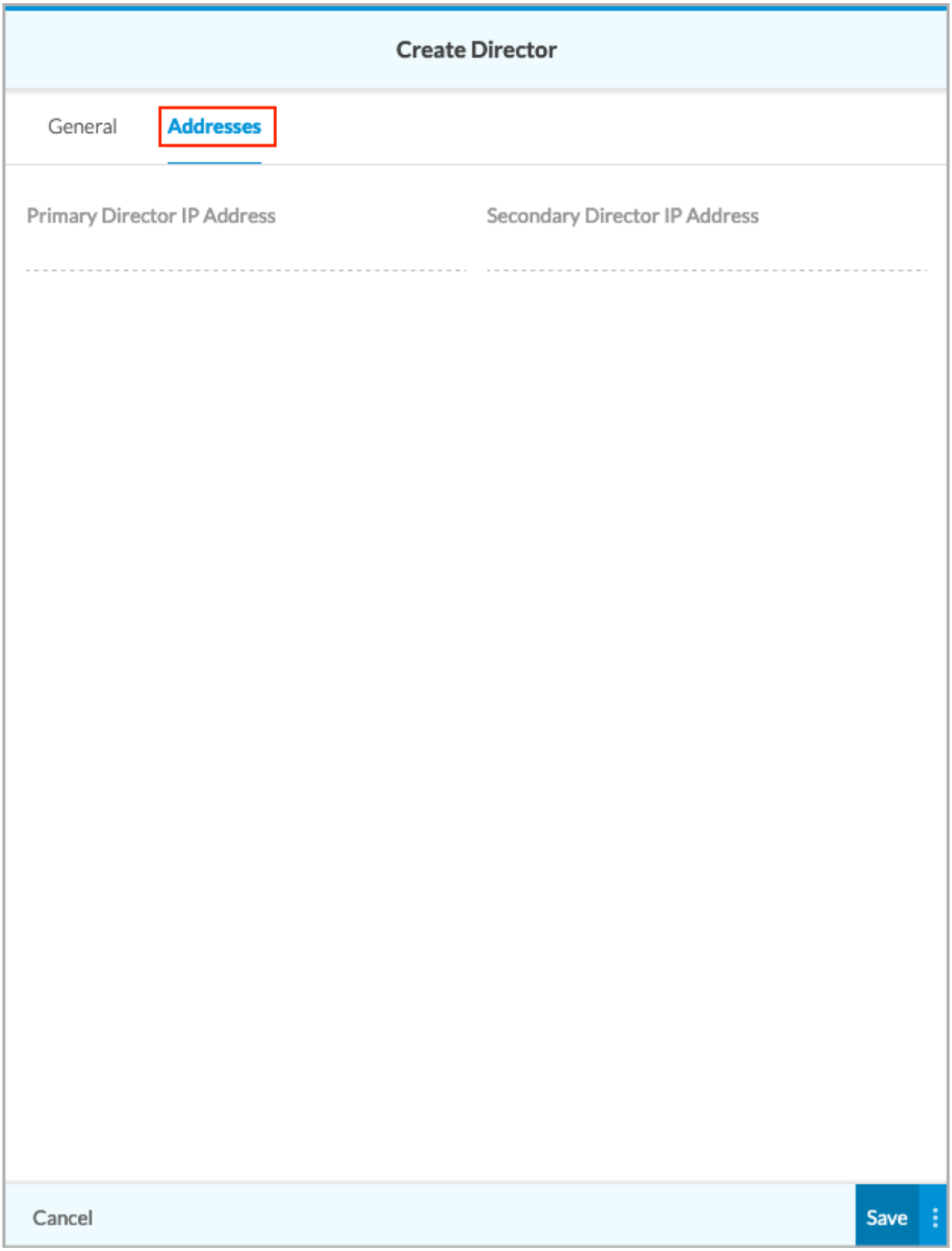


Field	Description
Name	Enter a name for the Director.

Field	Description
Is Default	Click the  Is Default slide bar to have the new Director node be the default Director node. The default Director node authenticates all Administrator users, whether the users are local or internal to the Director node.
Services Provided by Director	(For Releases 11.3.2 and later.) Select the services that the Director provides: ◦ Secure SD-WAN—Director supports only Secure SD-WAN gateways. ◦ Security Service Edge (SSE)—Director supports only Security Service Edge gateways. ◦ Secure SD-WAN and Security Service Edge (SSE)—Director supports both gateways. When you later create a tenant and select the services for that tenant, you can select only the Directors that support that service. For example, if you select only the Secure SD-WAN service for tenant and then select the Director or Directors for the tenant, only the Directors that support Secure SD-WAN are displayed.
Password	Enter a password that the Concerto orchestrator uses to enable server-to-server communication with the Director node using REST API calls. You can configure a separate password for each Director cluster. The password should have at least one uppercase character, one digit, and one special character. Note that this password is not the password for the Director cluster or for the Concerto orchestrator. It is used solely to enable communication between the Concerto orchestrator and the Director cluster.
Confirm Password	Re-enter the password.
Tags	Enter one or more tags to associate with the Director. A tag is an alphanumeric text descriptor with no spaces or special characters that is used for

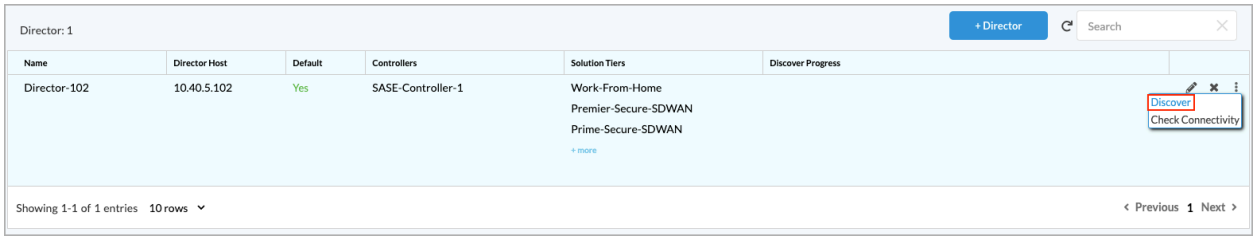
Field	Description
	searching objects.

4. Select the Addresses tab.

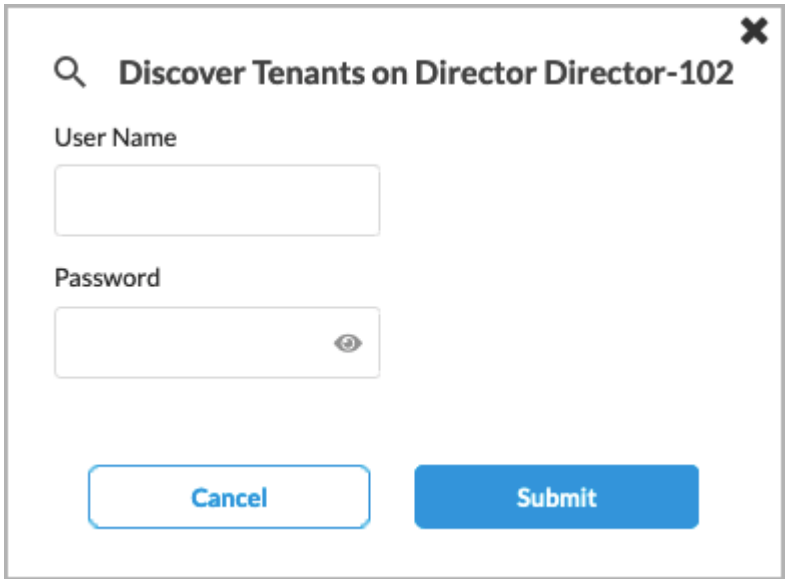


5. Enter the IP addresses of the primary and secondary Director nodes (if a secondary Director node exists). For a HA deployment, enter the IP addresses of both Director nodes.
6. Click Save. The Director cluster is created.

7. On the Infrastructure screen, click the three dots to the right of the new Director entry, and then select Discover to have the Concerto orchestrator discover the provider and subtenants, Controller nodes, and Analytics clusters.

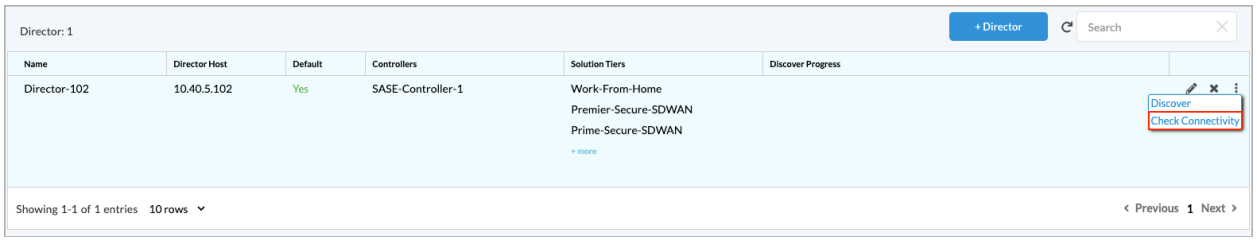


8. In the Discover Tenants popup window, enter the username and password for the ProviderDataCenterSystemAdmin. The screen then displays the discovered Controller nodes and the solution tiers for the new Director node.

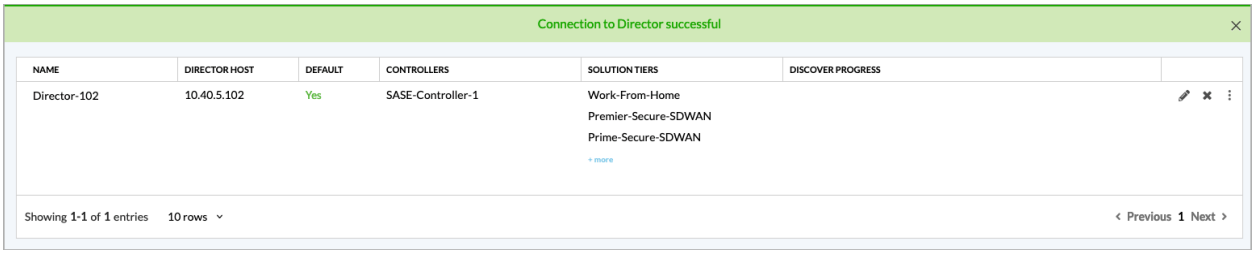


9. To verify that the tenants have been discovered, select Tenants in the left navigation bar and view the list of tenants.

10. To check connectivity to the Director, click the three dots to the right of the new Director entry, and then select Check Connectivity.



The following screen confirms that the connection to the Director was successful.



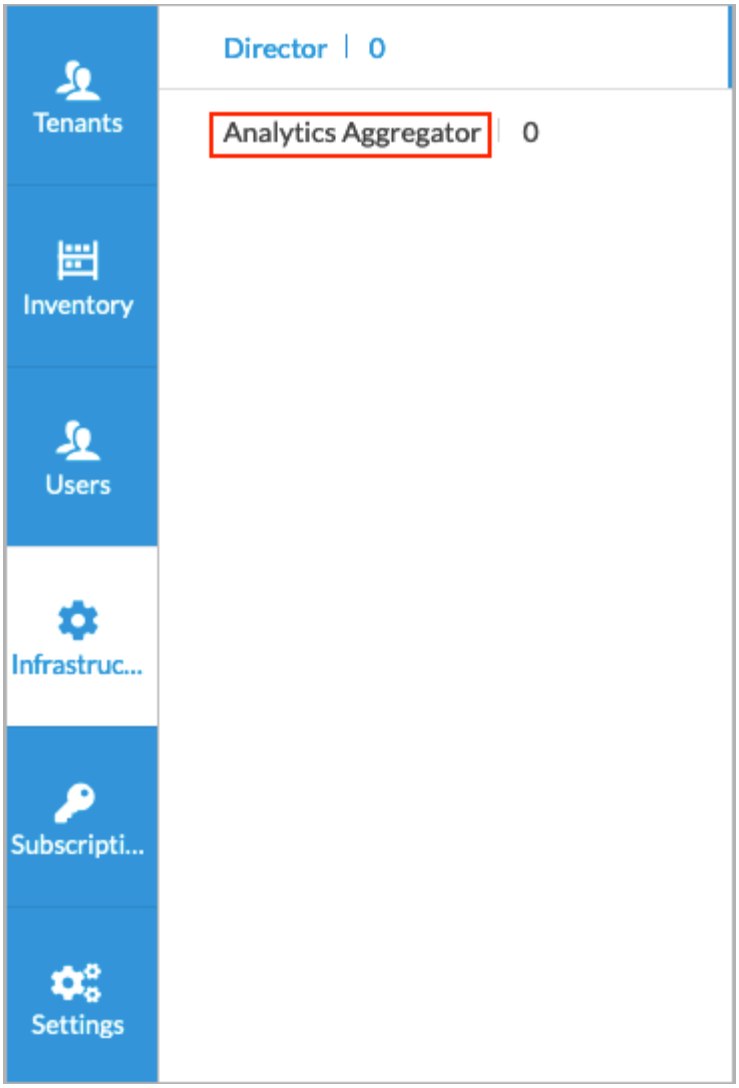
Add an Analytics Aggregator Cluster

For Releases 11.4.1 and later.

An Analytics aggregator cluster consists of one or more aggregator nodes that combine tenant log data from multiple Analytics clusters into single reports. In Concerto, you add aggregator clusters of one or more nodes. Each aggregator node operates independently to aggregate data from the same source. Because the underlying data is the same, each aggregator node presents the same reports. If one node fails, other nodes can produce the same reports to provide redundancy. For more information about aggregator nodes, see Configure Analytics Aggregator Nodes.

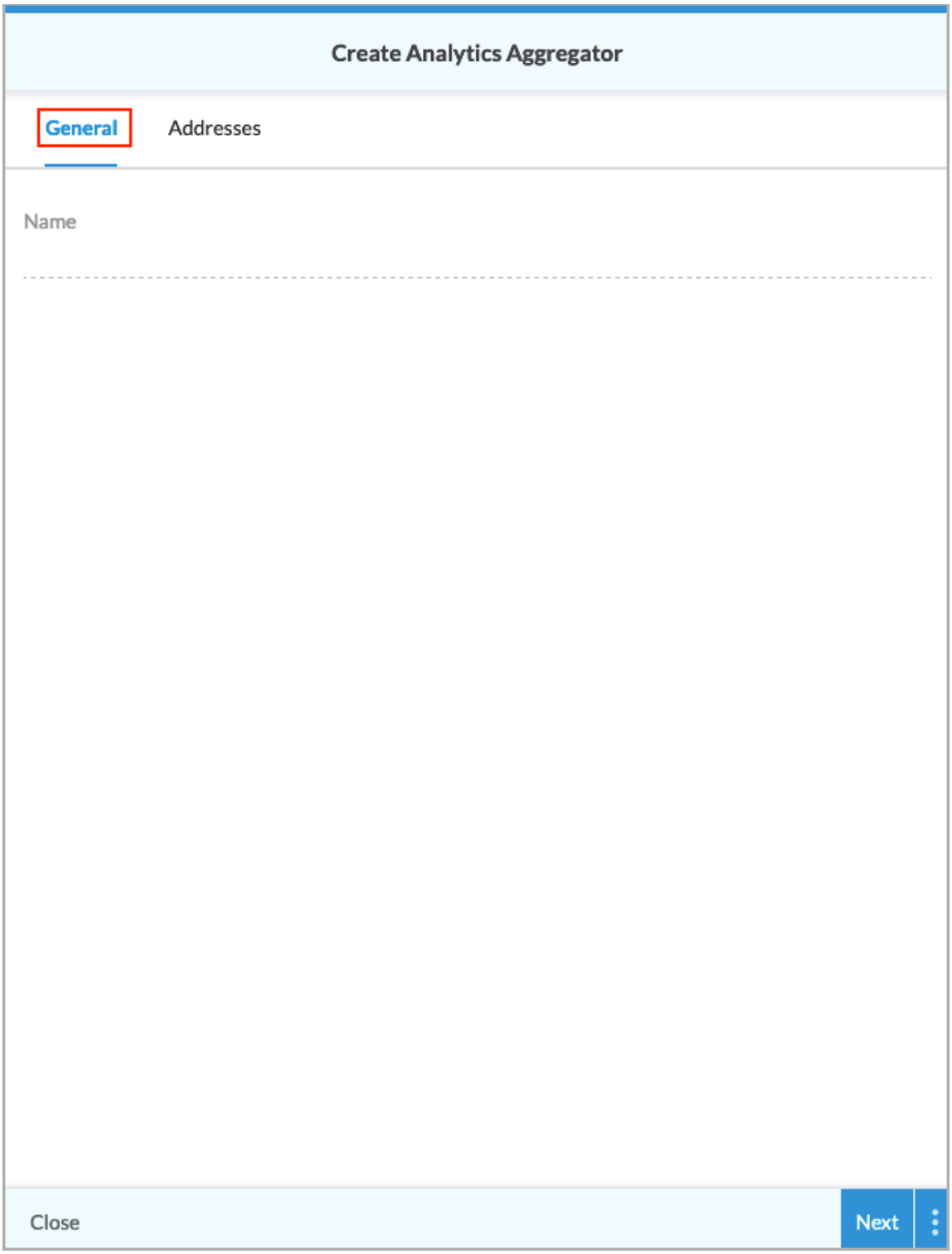
To configure an Analytics aggregator cluster:

1. Go to Infrastructure > Analytics Aggregator.

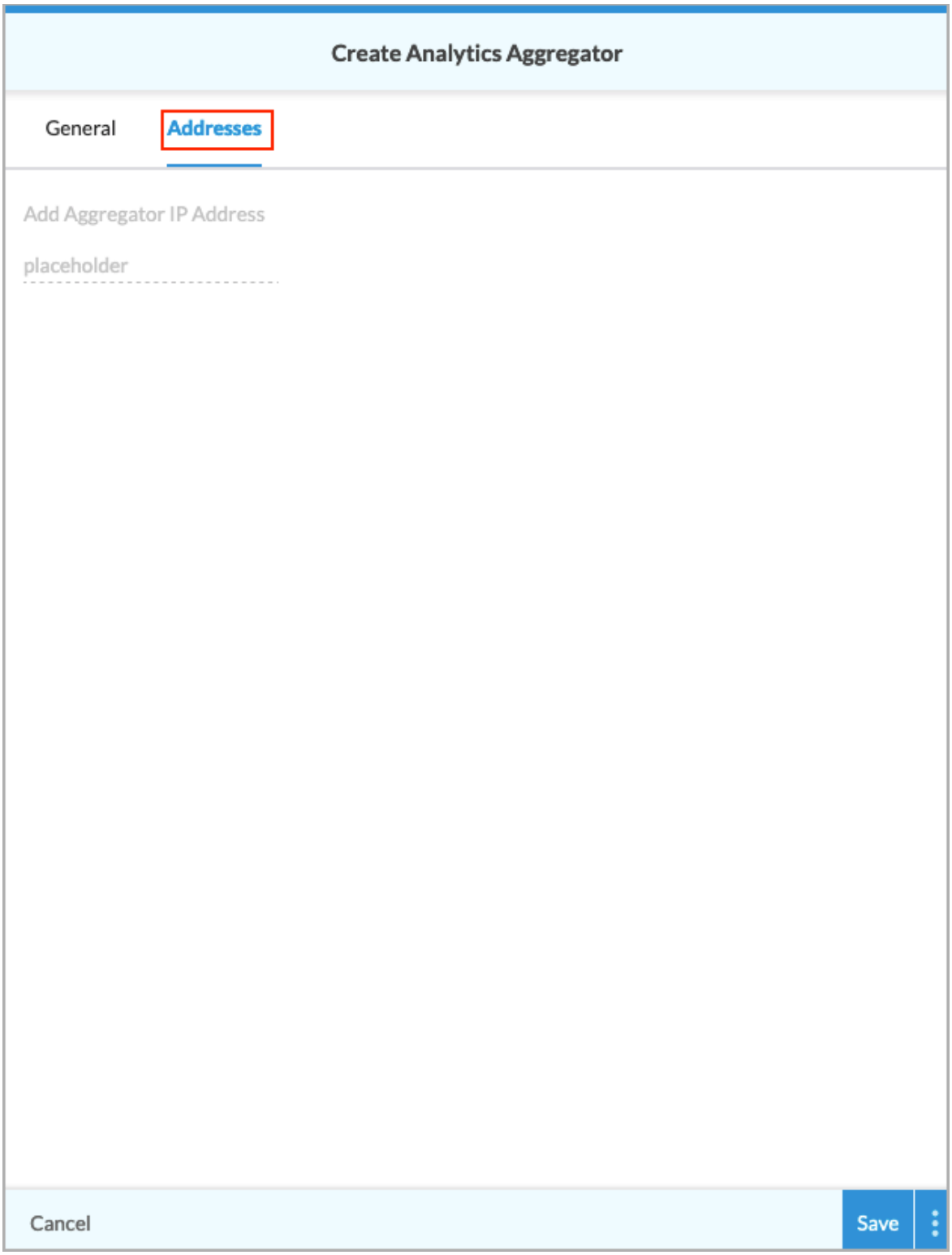


The Analytics Aggregator screen displays.

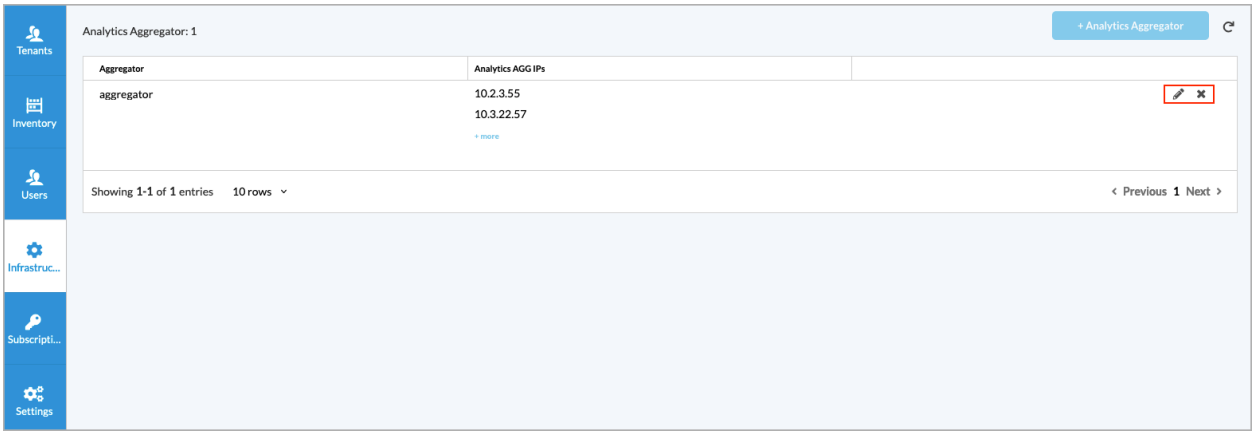
2. Click + Analytics Aggregator to add a new aggregator cluster. The Create Analytics Aggregator screen displays. Note that if you have already configured an Analytics aggregator cluster, you cannot configure a second cluster, and the + Analytics Aggregator button is grayed out.



3. Select the General tab, and then enter a name for Analytics aggregator cluster in the Name field.
4. Select the Addresses tab. The following screen displays.



5. Enter the IP address for the first Analytics aggregator node, and then press Enter.
6. Optionally, enter the IP address for one or more additional Analytics aggregator nodes, pressing Enter after entering each IP address.
7. Click Save to create the Analytics aggregator cluster. The main Analytics Aggregator screen shows the configured cluster.



8. To edit the Analytics Aggregator, click the Edit icon. To delete it, click the Delete icon.

Add an ATP/DLP Instance

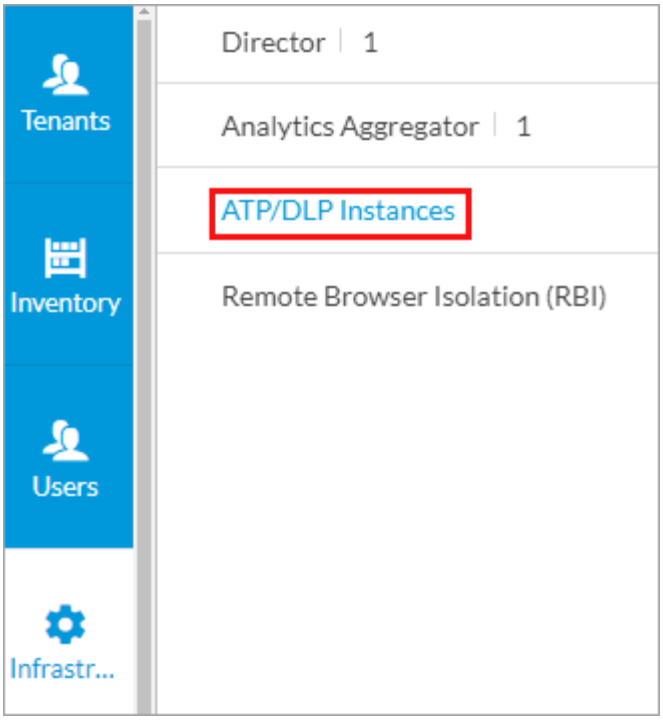
For Releases 12.1.1 and later.

Configuring an advanced threat protection (ATP) or data loss prevention (DLP) cloud instance provides credentials to the Versa Cloud Gateway (VCG), which allows the VCG to connect to the cloud sandboxing service. For more information, see Configure Advanced Threat Protection and Configure Data Loss Prevention.

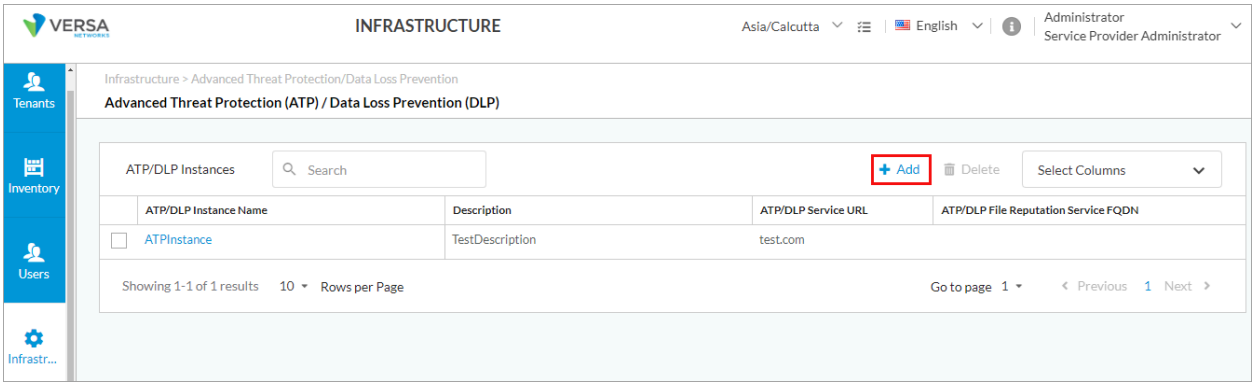
You use the ATP/DLP instances while configuring tenants. For more information, see Configure SASE Tenants.

To configure an ATP/DLP instance:

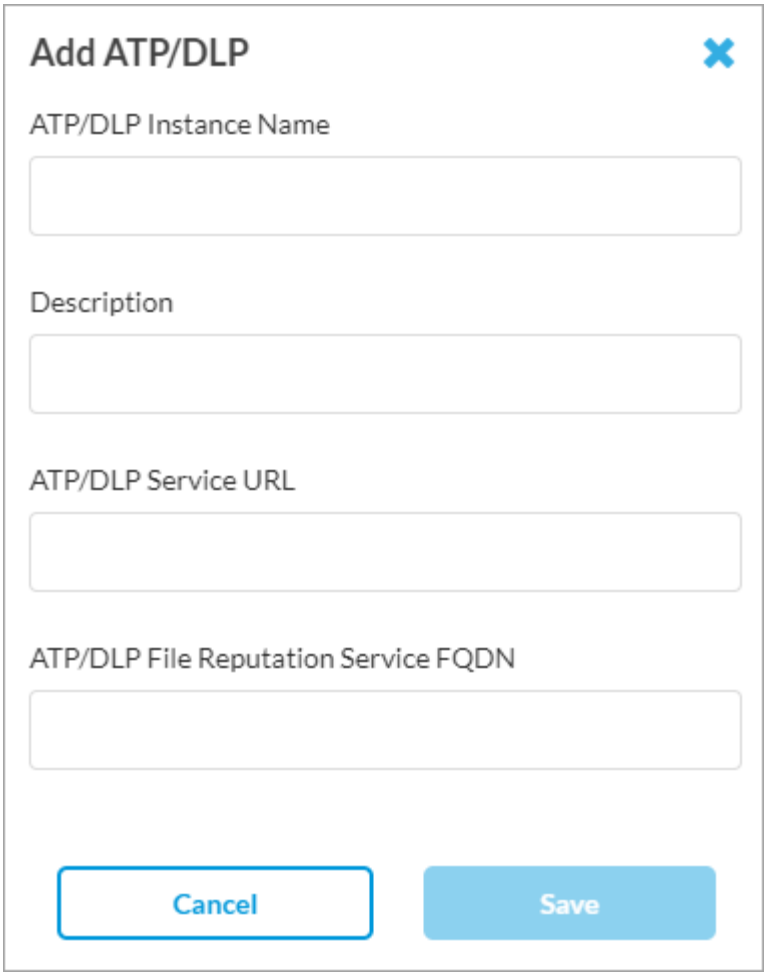
1. Go to Infrastructure > ATP/DLP Instances.



The Advanced Threat Protection (ATP)/Data Loss Prevention (DLP) screen displays.



2. Click + Add. In the Add ATP/DLP popup window, enter information for the following fields.



Field	Description
ATP/DLP Instance Name	Enter a name for the ATP/DLP cloud instance.
Description	Enter a text description for the ATP/DLP instance.
ATP/DLP Service URL	Enter the URL for the VCG to use for the ATP/DLP cloud instance;
ATP/DLP File Reputation Service FQDN	Enter the FQDN for the VCG to use for the ATP/DLP cloud instance.

3. Click Save.

Add an RBI Instance

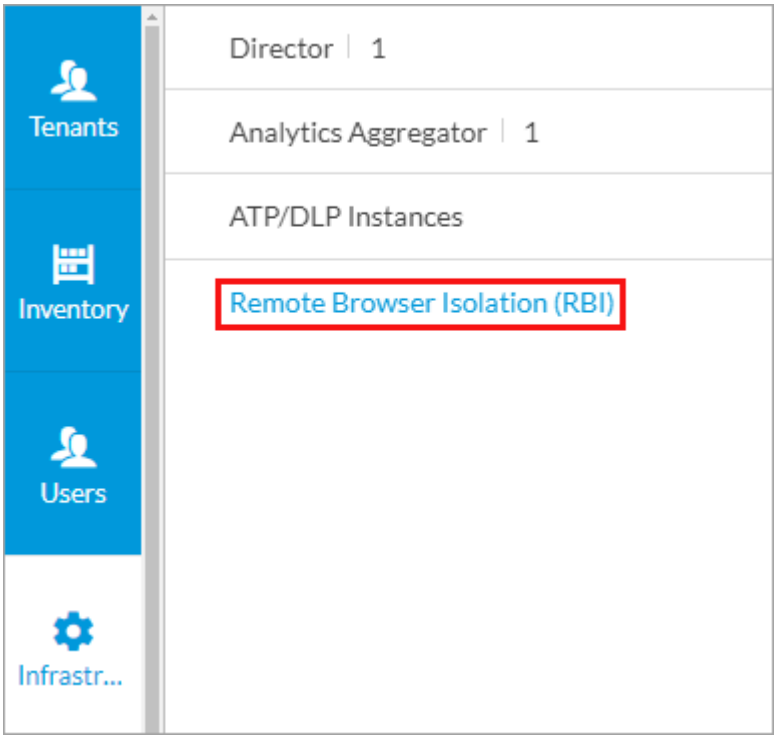
For Releases 12.1.1 and later.

The Versa remote browser isolation (RBI) is a cloud-based solution that provides zero-trust access to browser-based applications. Configuring an RBI cloud instance provides the VCG the credentials to connect to the cloud RBI service. For more information, see Configure Remote Browser Isolation.

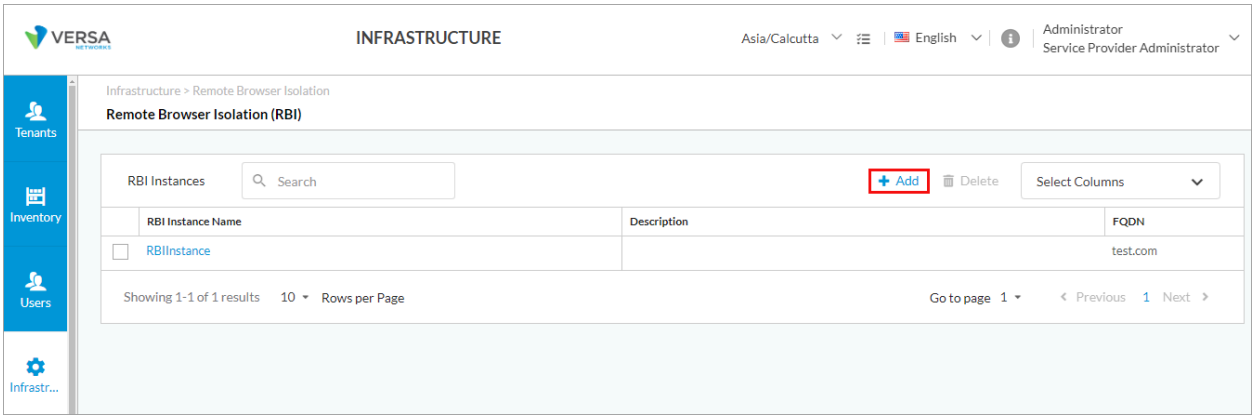
You use RBI instances while configuring tenants. For more information, see Configure SASE Tenants.

To configure an RBI instance:

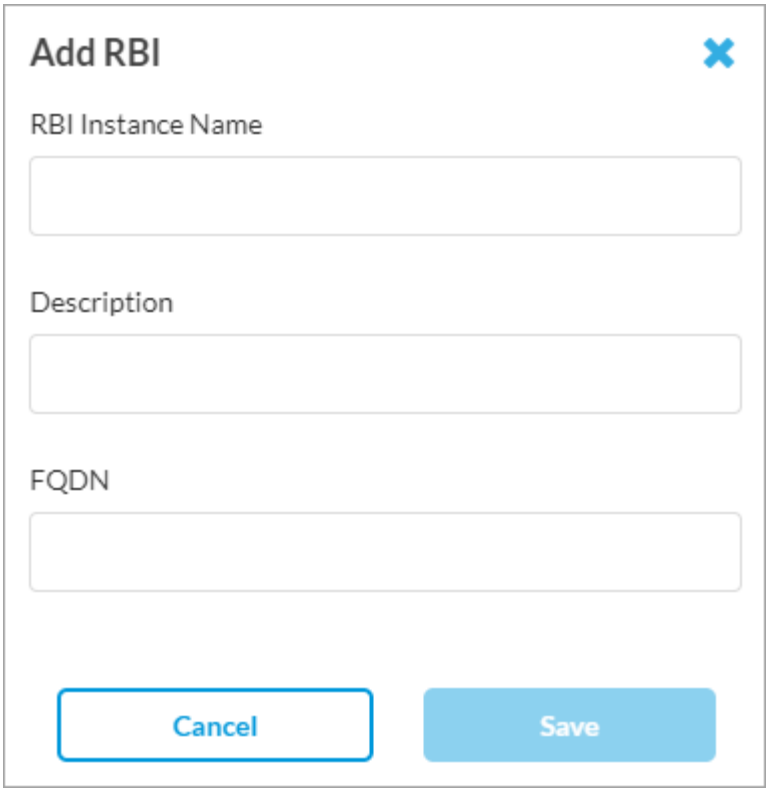
1. Go to Infrastructure > Remote Browser Isolation (RBI).



   The Remote Browser Isolation (RBI) screen displays.



2. Click + Add. In the Add RBI popup window, enter information for the following fields.



Field	Description
RBI Instance Name	Enter a name for the RBI instance.
Description	Enter a text description for the RBI instance.
FQDN	Enter the FQDN for the VCG to connect to the cloud service.

3. Click Save.

Install a CA Certificate

You can upload a certificate to a web server so that Concerto can establish a secure connection with a valid certificate.

To upload and install a CA certificate:

1. Combine the certificate and the CA chain into a single file, and name the file ecp.crt.
2. Ensure that the private key for the certificate is named ecp.key.
3. On any one of the Concerto cluster nodes, upload the two files to the /var/versa/ecp/share/certs folder.
4. Update the file ownership and permissions.

```
sudo chmod 775 /var/versa/ecp/share/certs ecp.*
sudo chown versa:versa /var/versa/ecp/share/certs ecp.*
```

5. Restart the Versa services.

```
vsh restart
```

Supported Software Information

Releases 10.1.1 and later support all content described in this article, except:

- Release 10.2.1 supports the **vsh start**, **vsh status**, and **vsh cluster init** commands to install Concerto standalone and cluster nodes.
- Release 11.1.1 supports the automatic configuration of Kafka from Concerto.
- Release 11.3.2 allows you to choose which services a Director supports.
- Release 11.4.1 adds the User Settings screen for each Versa Director in a Director cluster; adds support for Analytics aggregator nodes.
- Release 12.1.1 allows you to add instances for ATP/DLP and RBI.

Additional Information

Configure Analytics Aggregator Nodes
Perform Initial Software Configuration