Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Tenant Portal Guide, Release 1.1

March 31, 2016

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Service Provider Segment
Cloud and Network Solutions
Cisco Cloud Architecture for the Microsoft Cloud Platform Solution

Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Tenant Portal Guide, Release 1.1

Part: CCAMCP-CNAP-Tenant1-1.1

CONTENTS

Preface

This document describes how to use the Tenant Portal of the Cisco Cloud Network Automation Provisioner (CNAP) for the Microsoft Cloud Platform (MCP).

Document Objective and Scope

This document is part of the Cisco Cloud Architecture for the Microsoft Cloud Platform (CCA MCP) documentation suite for Release 1, summarized in the following table.

Table 2-1 CCA MCP Documentation Suite

Document	Description
Release Notes for Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 1.1 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/CNAP-RNs/CNAP-Release-Notes.html	Describes caveats and other important information about Release 1.1.
Cisco Cloud Architecture for the Microsoft Cloud Platform: Infrastructure Foundation Guide, Release 1.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/Foundation/CCAMCP1_Foundation.html	Describes data center infrastructure setup and implementation to support CCA MCP based services.
Cisco Cloud Architecture for the Microsoft Cloud Platform: Zinc Container Configuration Guide, Release 1.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/IaaS_Zinc_Config/CCAMCP1_IaaS_Zinc_Config.html	Describes the Infrastructure as a Service (IaaS) model with per-tenant Cisco CSR 1000V-based router/firewall.

Table 2-1 CCA MCP Documentation Suite

Installing Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 1.1 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/CNAP-Install/CNAP-Install.html	Describes the procedures and initial configuration to install Cisco CNAP in a data center.
Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Admin Portal Guide, Release 1.1 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/CNAP-Admin/CNAP-Admin.html	Describes how the Cisco CNAP Admin Portal is used to create and manage network container plans.
Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Tenant Portal Guide, Release 1.1 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/CNAP-Tenant/CNAP-Tenant.html	Describes how the Cisco CNAP Tenant Portal is used to subscribe to network container plans and manage subscriptions.
Cisco Cloud Architecture for the Microsoft Cloud Platform: DBaaS Configuration Guide, Release 1.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/DBSQLaaS/CCAMCP1_DBaaS.html	Describes how Database as a Service (DBaaS) can be deployed over the CCA MCP solution.
Cisco Cloud Architecture for the Microsoft Cloud Platform: DRaaS Application Note, Release 1.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/DRaaS_Application_Note/DRaaS_ASR.html	Describes how Disaster Recovery as a Service (DRaaS) based on Microsoft Azure Site Recovery can be deployed over the CCA MCP architecture.
Cisco Cloud Architecture for the Microsoft Cloud Platform: Backup as a Service Implementation Guide, Release 1.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/BaaS/BaaS_CommVault.html	Describes how Backup as a Service (BaaS) based on Commvault Simpana software can be deployed over the CCA MCP architecture.

This document only describes the Cisco CNAP Tenant Portal. For information on using the Admin Portal of the Cisco CNAP for MCP, see the Admin Portal Guide listed in the table above.

CHAPTER 1

Introduction

The Cisco Cloud Architecture for Microsoft Cloud Platform (CCA for MCP) solution delivers IaaS, PaaS, and SaaS with integrated management software. The data center infrastructure is built with Cisco Application Centric Infrastructure (ACI) for the Data Center Fabric and Cisco UCS-based compute, Cisco Adaptive Security Appliance (ASA) firewall for security, and Cisco Aggregation Services Routers (Cisco ASR 9000 and Cisco ASR1000) data center edge routers. Additionally, Cisco virtualized network functions such as Cisco Cloud Services Router 1000V (CSR 1000V) are used to implement tenant services.

Microsoft Hyper-V Hypervisor is used as the virtualizing layer for compute to run tenant workloads. The Management Stack is based on Microsoft Windows Azure Pack (WAP), which allows service providers to create plans and tenant administrators to subscribe to those plans.

CCA for MCP enables service providers to offer network management services on top of a Cisco network infrastructure through Microsoft WAP. A Microsoft WAP administrator can use the Cisco Cloud Network Automation Provisioner (CNAP) for MCP Admin Portal to configure, manage, and administer Cisco Data Center Network resources. Cisco CNAP provides the capability to create tenant containers with sophisticated network services such as tenant edge routing, multiple security zones, firewalling, NAT, MPLS VPN access, and Server Load Balancing. The administrator uses the portal to define and set up the available plans that will be visible in the Tenant Portal and that can be consumed by tenants. Tenants consume resources by using the Tenant Portal to subscribe to an available plan. This allows service providers to offer differentiated plans that provide more value to tenants and generate more revenue for service providers, with the convenience of automation to deploy sophisticated containers for tenants.

For more information, see: http://www.cisco.com/go/cloud.

Tasks You Can Perform in the Tenant Portal

You can use the Tenant Portal to:

- Subscribe to plans
- Create containers for subscriptions
- View and modify information about containers, including:
  - View summary information about a container.
  - Delete a container.
  - View gateway information about a container, including remove a WAN gateway.
  - View and modify Shared Services information about a container.

- View and modify firewall information about a container, including add and modify a policy map for a service policy, modify and remove a class map instance, and modify and remove an access group (you can also add a rule to an Access Control List [ACL]).
- View and modify tier information about a container, including add a tier, change a tier (and update a segment), remove a tier, and remove a segment.
- View and modify load balancer information about a container, including View information about an existing load balancer, add a Citrix NetScaler VPX, add a load balancer, add a server, change a load balancer, change a server, remove a load balancer, remove a server, and remove a Citrix NetScaler VPX.

Understanding the Interrelationship of Tasks Performed in the Tenant Portal and by the Cloud Provider

Certain tasks performed in the Tenant Portal and by the cloud provider are interdependent in that tasks must be completed by one user before other tasks can be accomplished by the other user. For example:

- Base container plans must be created by the cloud provider before you can use the Tenant Portal to subscribe to them and create containers.
- In the Tenant Portal, after you subscribe to a plan and create a container, then the cloud provider can confirm that the newly-created tenant container is Active and configure the following for it:
  - WAN Gateway—When you are creating a container for a plan to which you have subscribed, you see a screen indicating whether the plan includes entitlement for a WAN Gateway (e.g., MPLS VPN). If it does, you see a message to contact your cloud provider. Once your container is active, the cloud provider can then configure the WAN Gateway.
  - Firewall—When you are creating a container for a plan to which you have subscribed, you specify the number of Workload Tiers for the container. Cisco CNAP will automatically set up a perimeter around each of the zones in the container, however the Tenant Firewall tab will not display any information until the WAN Gateway has been provisioned by the cloud provider. The firewall is automatically created with a base configuration during container creation. When the WAN gateway is created, another firewall zone is created for the WAN edge. You can configure a firewall in the Tenant Portal, however it can only be configured after you have created a container and the cloud provider has created a WAN Gateway.
  - Load Balancer—The cloud provider must acknowledge that the Citrix NetScaler VPX is licensed before you can set up a software load balancer (SLB).

Accessing the Tenant Portal

You access the Tenant Portal from the WAP Tenant Site.

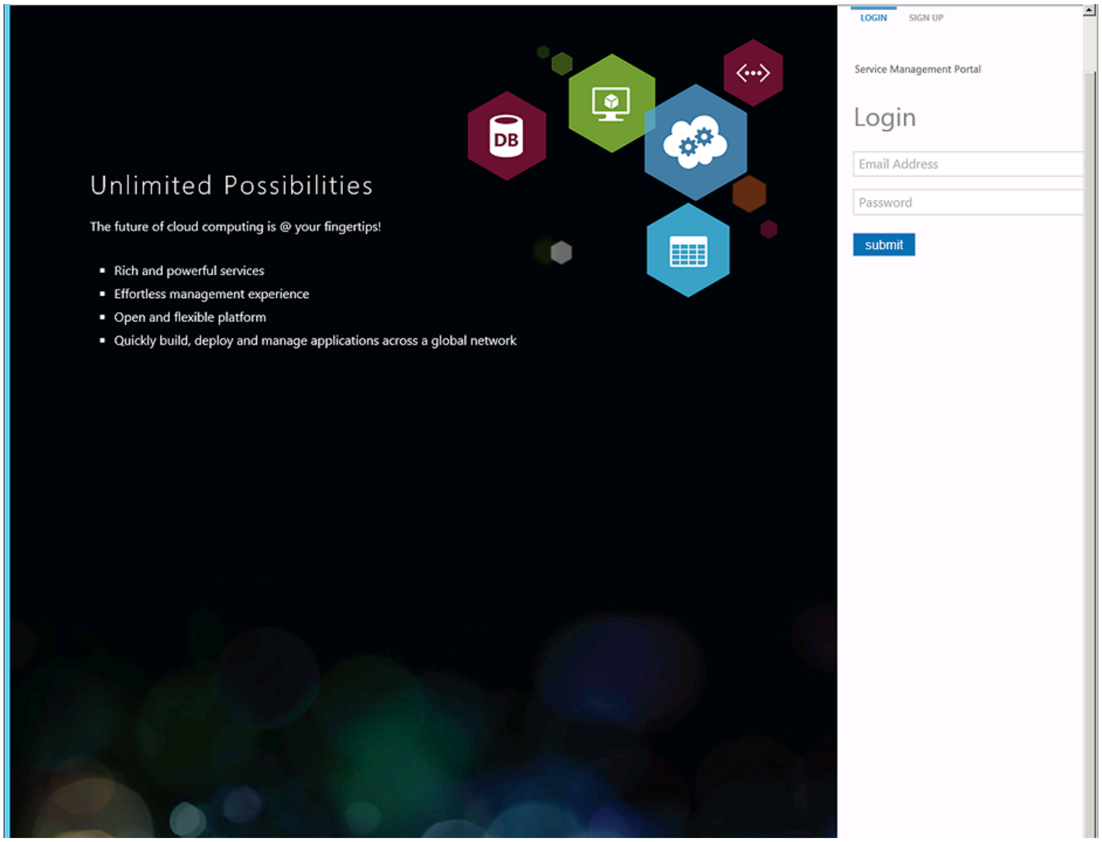
To access the Tenant Portal:

Step 1 Access WAP.

For information on accessing WAP, see the WAP documentation.

Step 2 You see the WAP Tenant Portal login scree, shown in the following screen.

Figure 1-1 WAP Tenant Portal Login Screen



Unlimited Possibilities

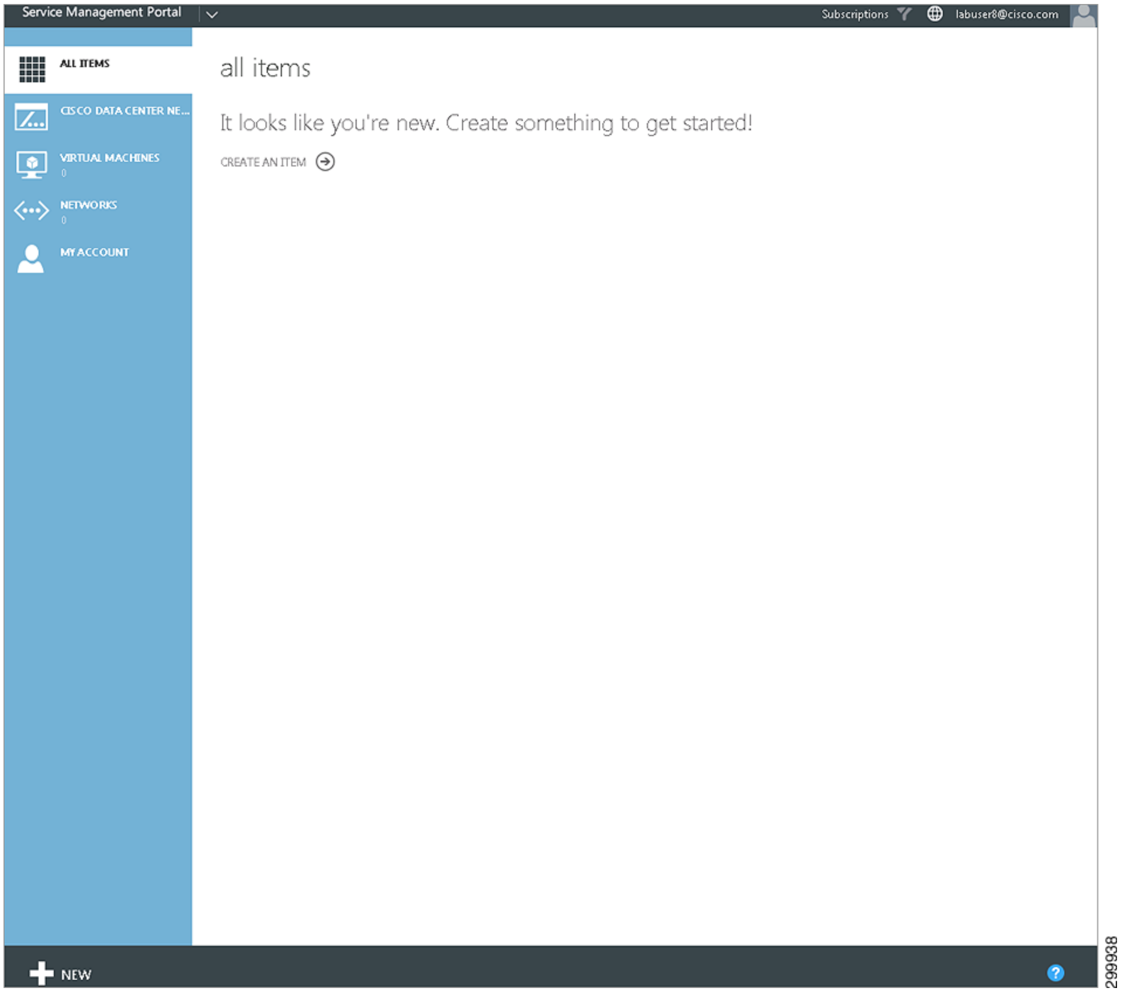
The future of cloud computing is @ your fingertips!

- Rich and powerful services
- Effortless management experience
- Open and flexible platform
- Quickly build, deploy and manage applications across a global network

Step 3 Enter your login credentials (email address and password) and click **submit**.

You see the main Tenant Portal screen, shown in the following screen.

Figure 1-2 Main Tenant Portal Screen



all items

It looks like you're new. Create something to get started!

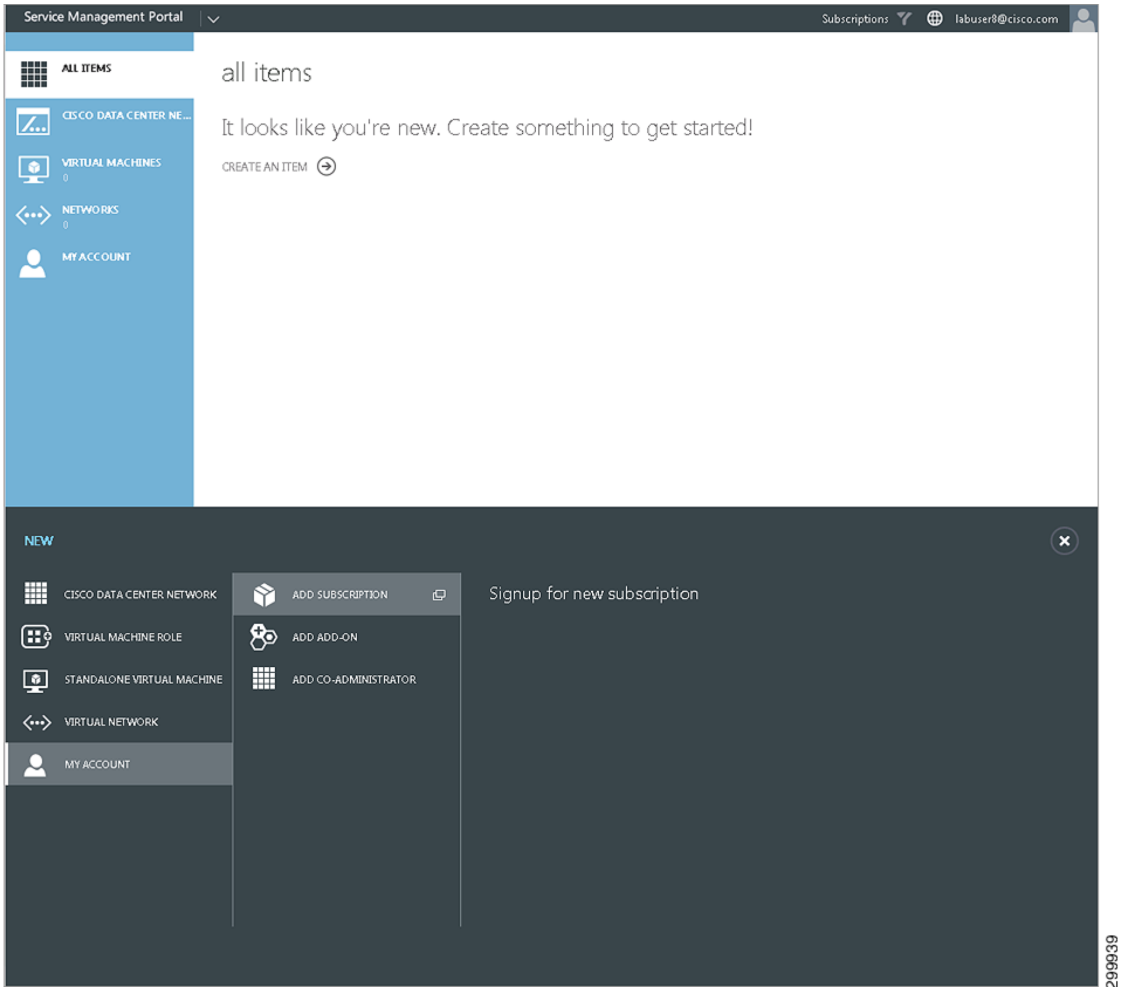
CREATE AN ITEM

Subscribing to a Plan

To subscribe to a plan:

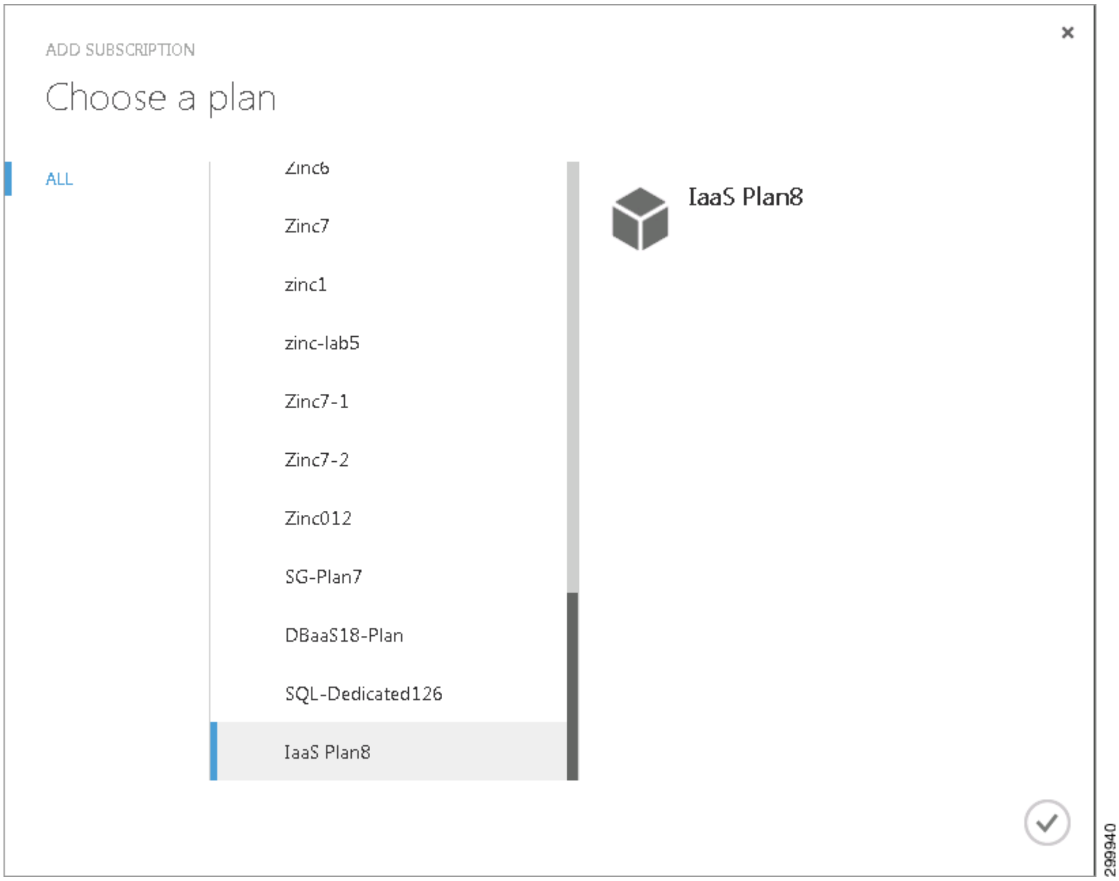
Step 1 On the main Tenant Portal screen, at the bottom, click **+ New** in the lower left corner, click **My Account**, then click **Add Subscription**, as shown in the following screen.

Figure 1-3 Add Subscription Screen



You see the Choose a Plan screen, as shown in the following screen.

Figure 1-4 Choose a Plan Screen



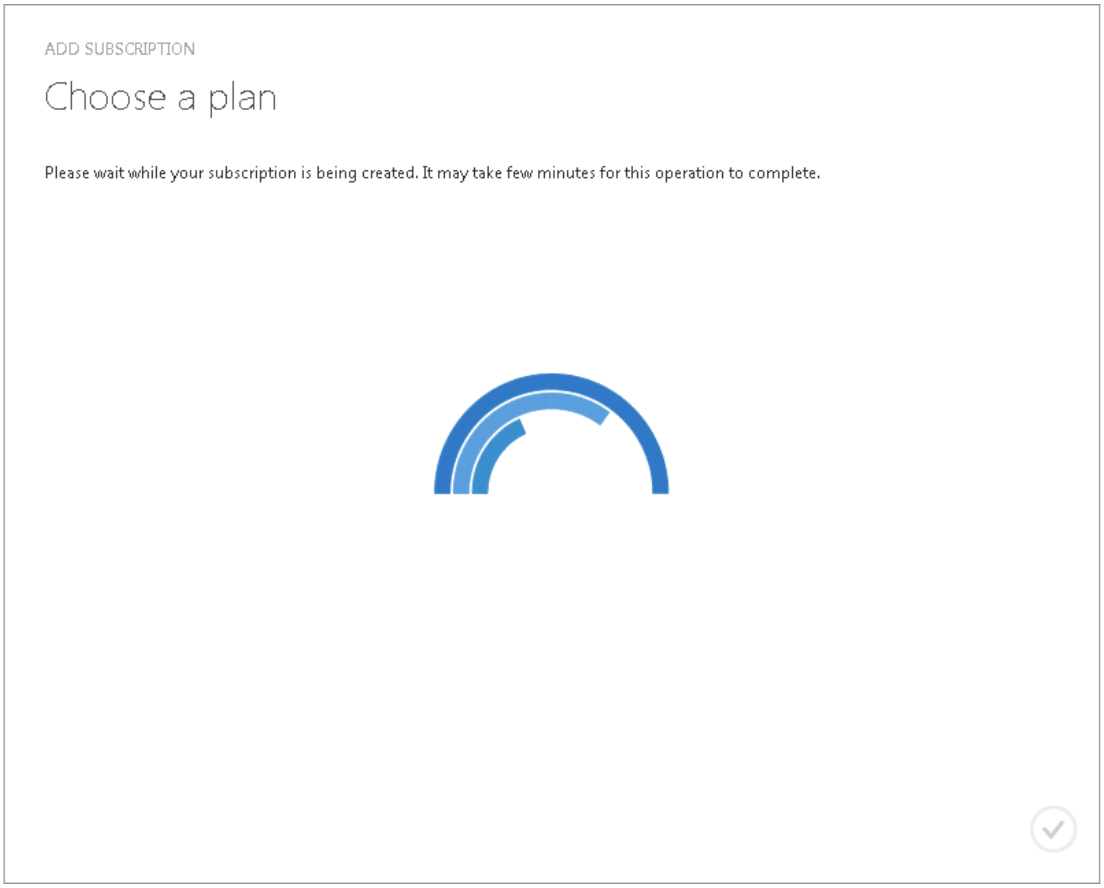
ADD SUBSCRIPTION

Choose a plan

Step 2 Click the plan to which you want to subscribe (in this example **IaaS Plan8**), then click the check mark.

You see the following screen while the subscription is being created.

Figure 1-5 ***Subscription Being Created Screen***



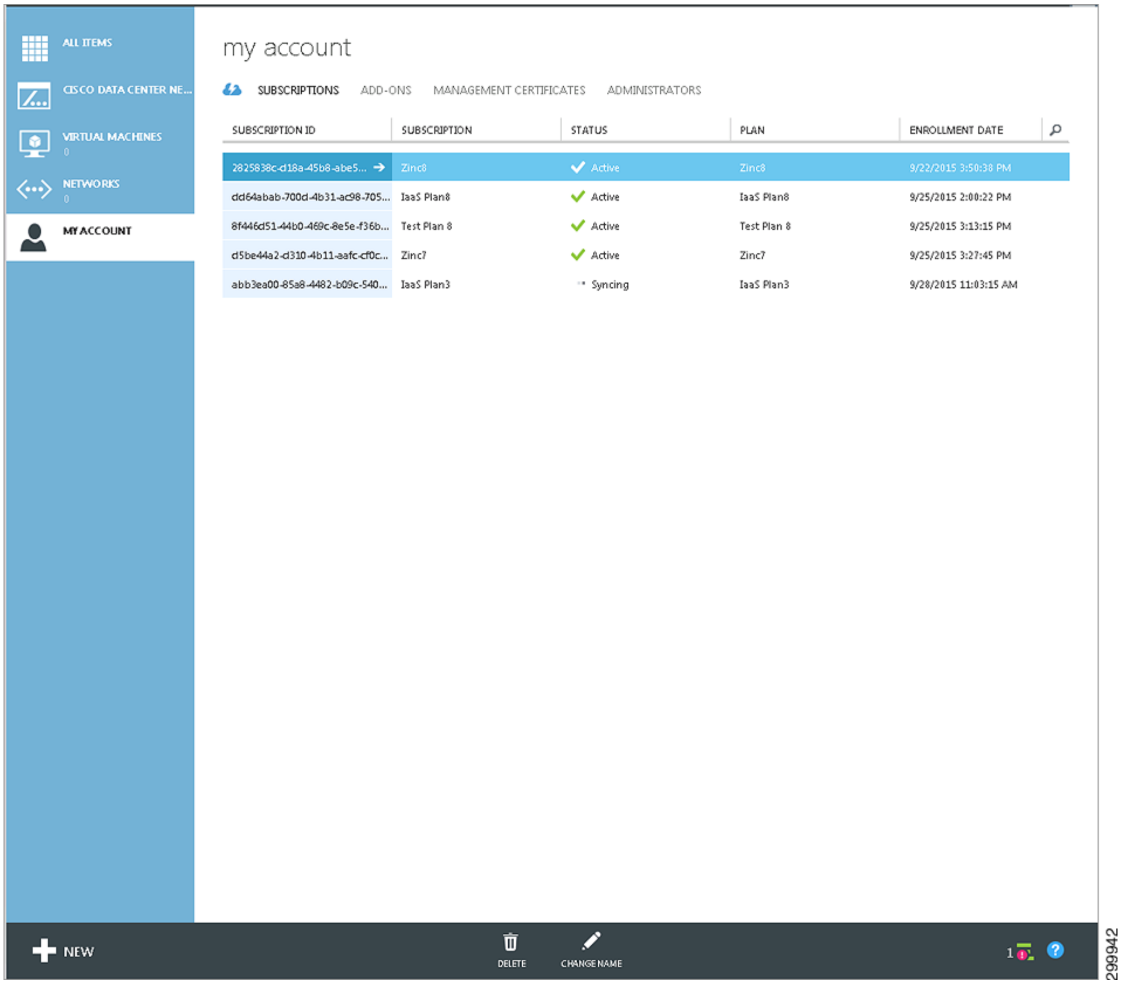
ADD SUBSCRIPTION

Choose a plan

Please wait while your subscription is being created. It may take few minutes for this operation to complete.

Next you see a screen showing the plan to which you subscribed with a Status of Syncing, as shown in the following screen.

Figure 1-6 Plan Subscription Syncing



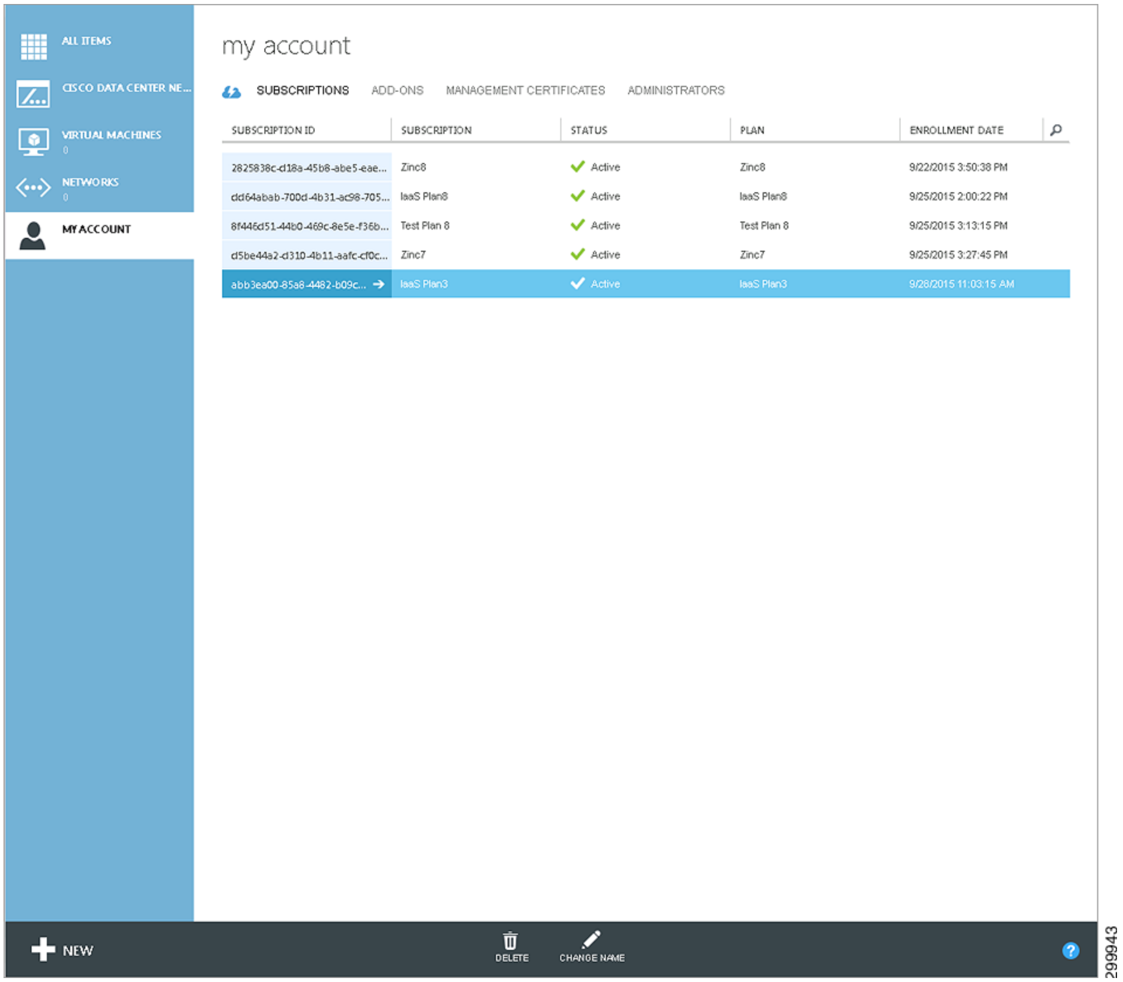
my account

SUBSCRIPTIONS ADD-ONS MANAGEMENT CERTIFICATES ADMINISTRATORS

SUBSCRIPTION ID	SUBSCRIPTION	STATUS	PLAN	ENROLLMENT DATE
2825838c-d18a-45b8-abe5...	Zinc8	✓ Active	Zinc8	9/22/2015 3:50:38 PM
dd64abab-700d-4b31-ac98-705...	IaaS Plan8	✓ Active	IaaS Plan8	9/25/2015 2:00:22 PM
8f446d51-44b0-469c-8e5e-f36b...	Test Plan 8	✓ Active	Test Plan 8	9/25/2015 3:13:15 PM
d5be44a2-d310-4b11-aafc-cf0c...	Zinc7	✓ Active	Zinc7	9/25/2015 3:27:45 PM
abb3ea00-85a8-4482-b09c-540...	IaaS Plan3	Syncing	IaaS Plan3	9/28/2015 11:03:15 AM

When the synchronization is complete, the subscription will show as Active, as shown in the following screen.

Figure 1-7 Plan Subscription Active



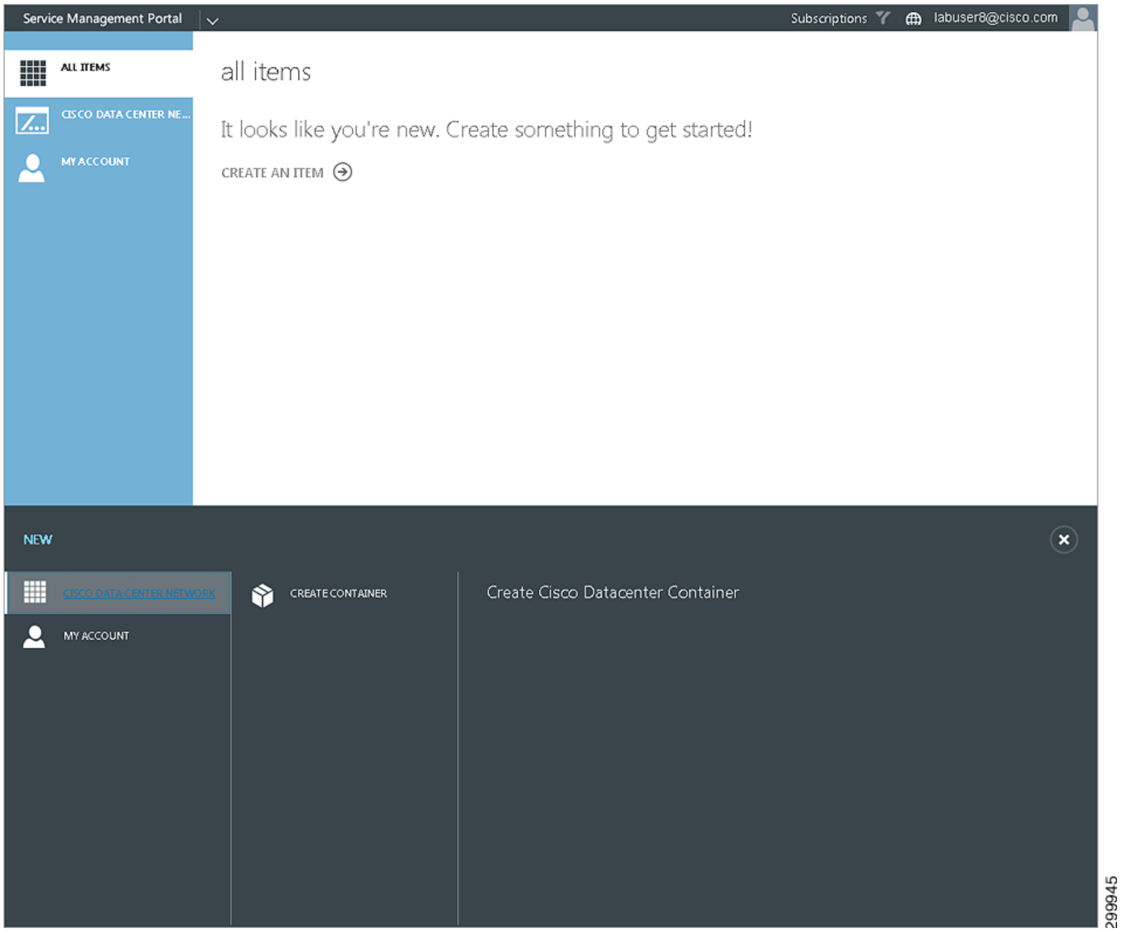
SUBSCRIPTION ID	SUBSCRIPTION	STATUS	PLAN	ENROLLMENT DATE
2825838c-d18a-45b8-abe5-eae...	Zinc8	✓ Active	Zinc8	9/22/2015 3:50:38 PM
dd64abab-700d-4b31-ac98-705...	IaaS Plan8	✓ Active	IaaS Plan8	9/25/2015 2:00:22 PM
8f446d51-44b0-469c-8e5e-f36b...	Test Plan 8	✓ Active	Test Plan 8	9/25/2015 3:13:15 PM
d5be44a2-d310-4b11-aafc-cf0c...	Zinc7	✓ Active	Zinc7	9/25/2015 3:27:45 PM
abb3ea00-85a8-4482-b09c... →	IaaS Plan3	✓ Active	IaaS Plan3	9/28/2015 11:03:15 AM

Creating a Container

To create a container:

Step 1 On the main Tenant Portal screen, click **+ New** in the lower left corner, then click **Cisco Datacenter Network**, then **Create Container**, as shown in the following screen.

Figure 1-8 Create New Container Screen

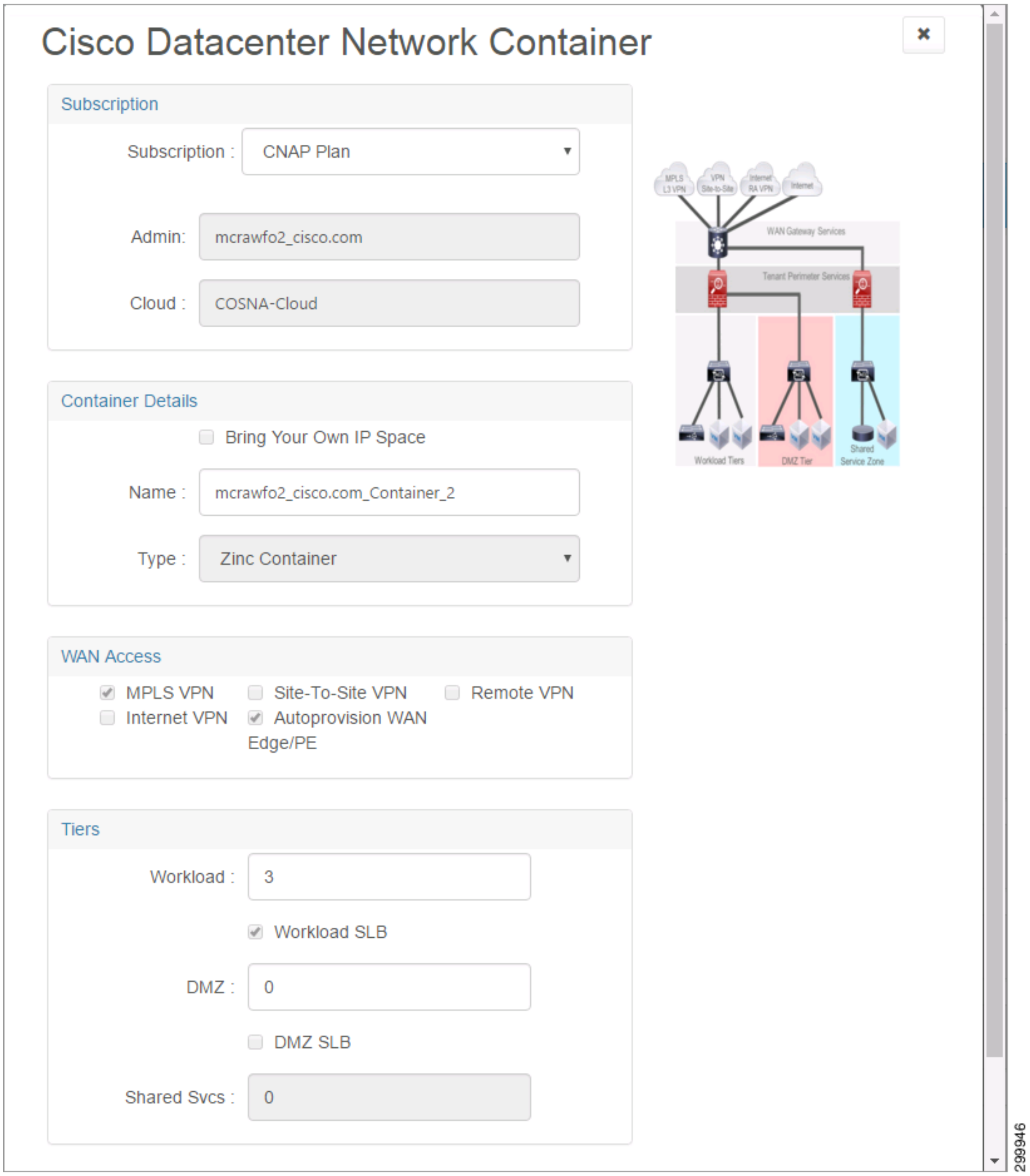


It looks like you're new. Create something to get started!

Create Cisco Datacenter Container

You see the following screen.

Figure 1-9 Container Creation Screen



Cisco Datacenter Network Container

Subscription

Subscription : CNAP Plan

Admin: mcrawfo2_cisco.com

Cloud : COSNA-Cloud

Container Details

□ Bring Your Own IP Space

Name : mcrawfo2_cisco.com_Container_2

Type : Zinc Container

WAN Access

☑ MPLS VPN □ Site-To-Site VPN □ Remote VPN
□ Internet VPN ☑ Autoprovision WAN Edge/PE

Tiers

Workload : 3

☑ Workload SLB

DMZ : 0

□ DMZ SLB

Shared Svcs : 0

Step 2 Some values are prepopulated based on what your cloud provider has defined. Complete the fields to create a network container:

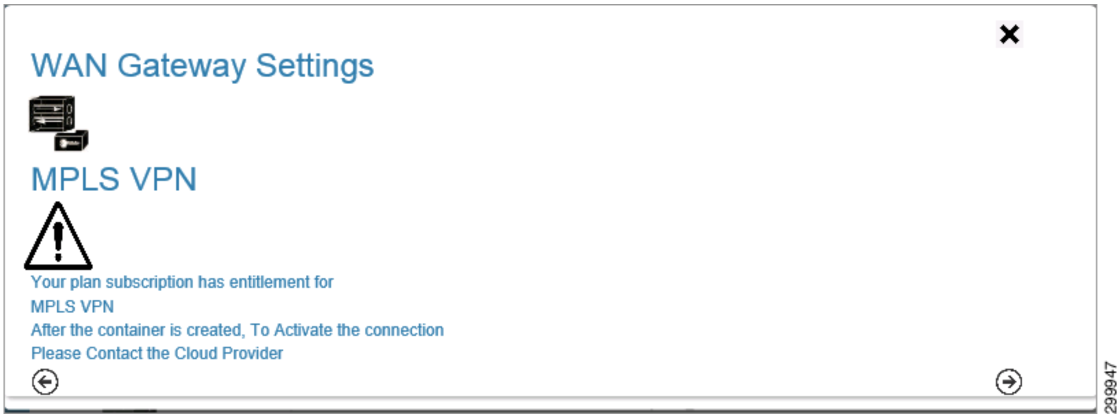
- Subscription:
  - Subscription:—Select the subscription for which you want to create a container.
  - Admin:—Preselected and cannot be changed.
  - Cloud:—Preselected and cannot be changed.
- Container Details:
  - Bring Your Own IP Space—Not supported in the current release.

  - Name:—Enter a name for the container.
  - Type:—Zinc is preselected.
- WAN Access (VPN):
  - MPLS is preselected (Site-to-Site, Remote Access, and Internet are not supported in the current release).
- Tiers:
  - Workload:—Number of tiers.
  - Workload SLB—Preselected based on plan.
  - DMZ:—Not supported in the current release.
  - DMZ SLB—Not supported in the current release.
  - Shared Svcs:—The Shared Services, such as Database as a Service (DBaaS), Disaster Recovery as a Service (DRaaS), etc., for the plan to which you have subscribed.

When you are finished, at the bottom of the screen, click the right arrow (–>).

You see the following screen.

Figure 1-10 WAN Gateway Screen



WAN Gateway Settings

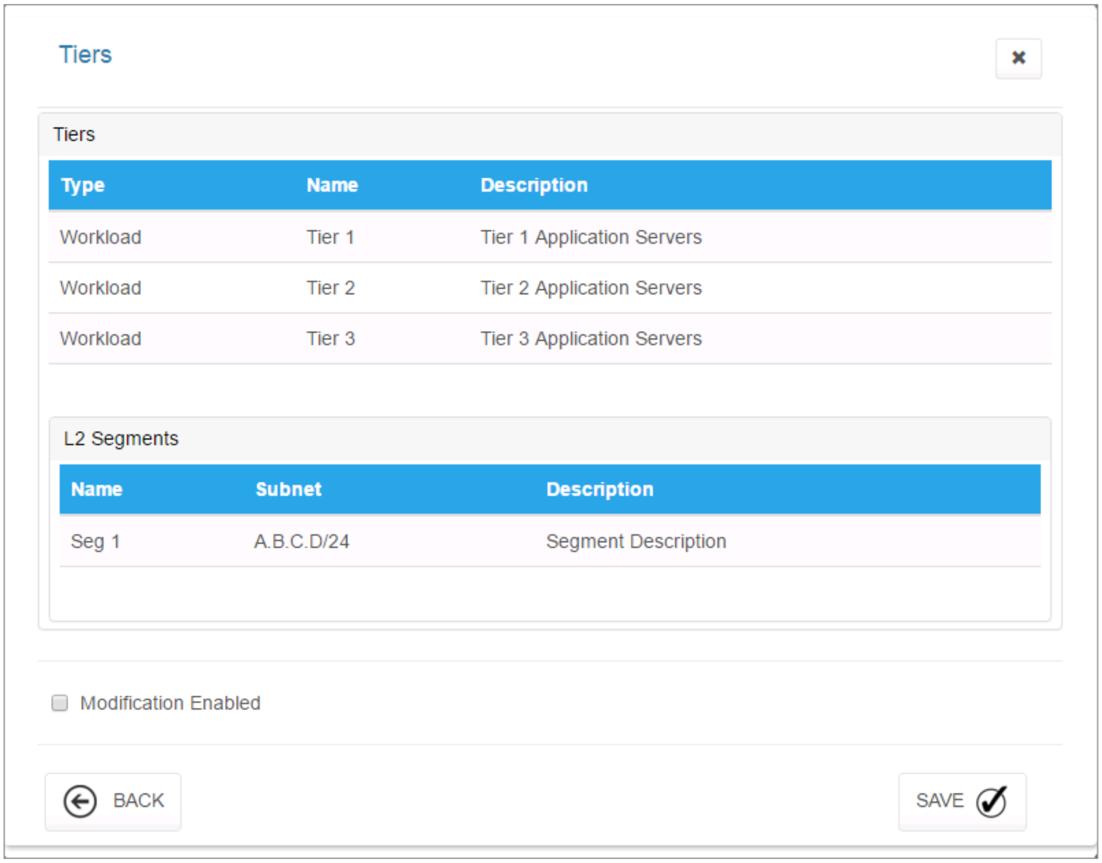
MPLS VPN

Your plan subscription has entitlement for
MPLS VPN
After the container is created, To Activate the connection
Please Contact the Cloud Provider

Step 3 Click the right arrow (–>).

You see the following screen.

Figure 1-11 Tiers and Layer 2 Segments Screen



Tiers

Tiers

Type	Name	Description
Workload	Tier 1	Tier 1 Application Servers
Workload	Tier 2	Tier 2 Application Servers
Workload	Tier 3	Tier 3 Application Servers

L2 Segments

Name	Subnet	Description
Seg 1	A.B.C.D/24	Segment Description

□ Modification Enabled

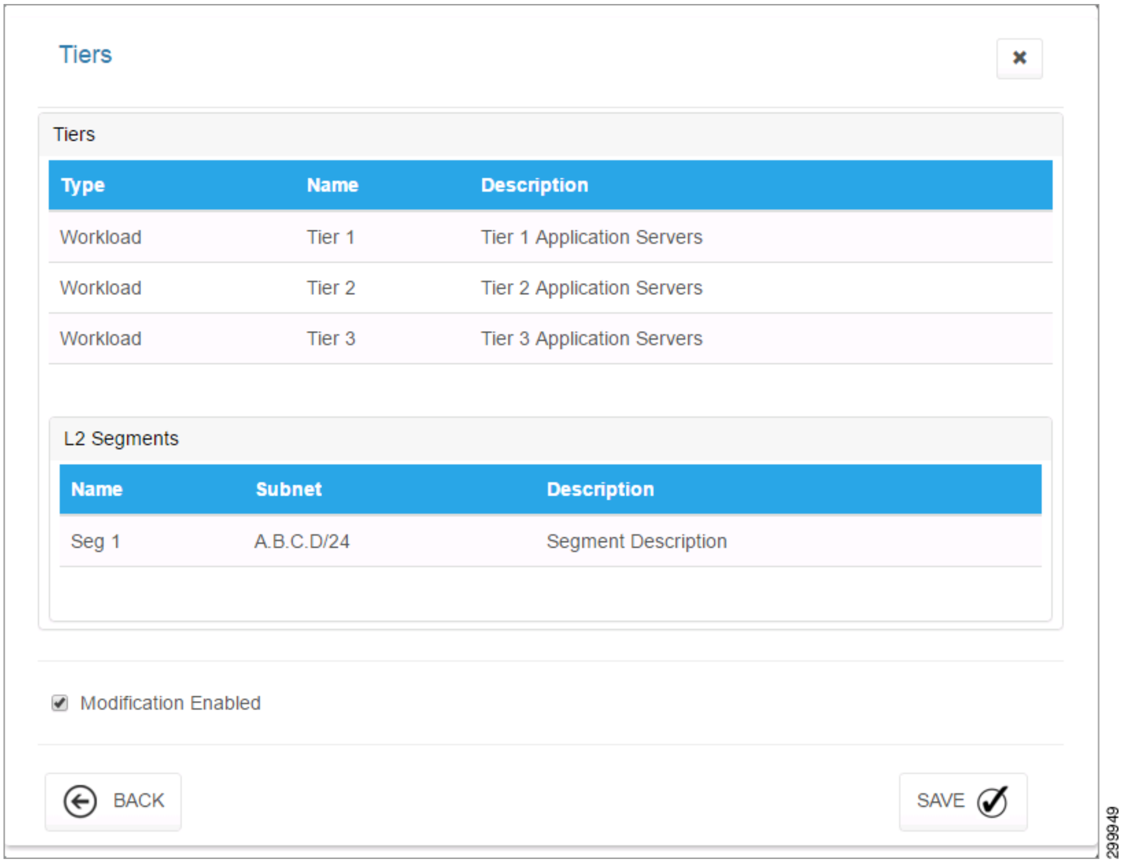
On the Container Creation screen we specified a Workload of 3 under Tiers, so this screen shows those structures already created.

This screen displays the following information:

- Tiers:
  - Type—Only Workload is supported in this release.
  - Name—Name of the tier.
  - Description—Description of the tier.
- L2 Segments:
  - Name—Name of the segment.
  - Subnet—Subnet the segment is in.
  - Description—Description of the segment.

Step 4 Click check box for **Modification Enabled** if you want to modify the names and descriptions of the tiers and segments. Click the check box and then click the tier you want to modify.

Figure 1-12 Modification Enabled Checked Screen



Tiers

Tiers

Type	Name	Description
Workload	Tier 1	Tier 1 Application Servers
Workload	Tier 2	Tier 2 Application Servers
Workload	Tier 3	Tier 3 Application Servers

L2 Segments

Name	Subnet	Description
Seg 1	A.B.C.D/24	Segment Description

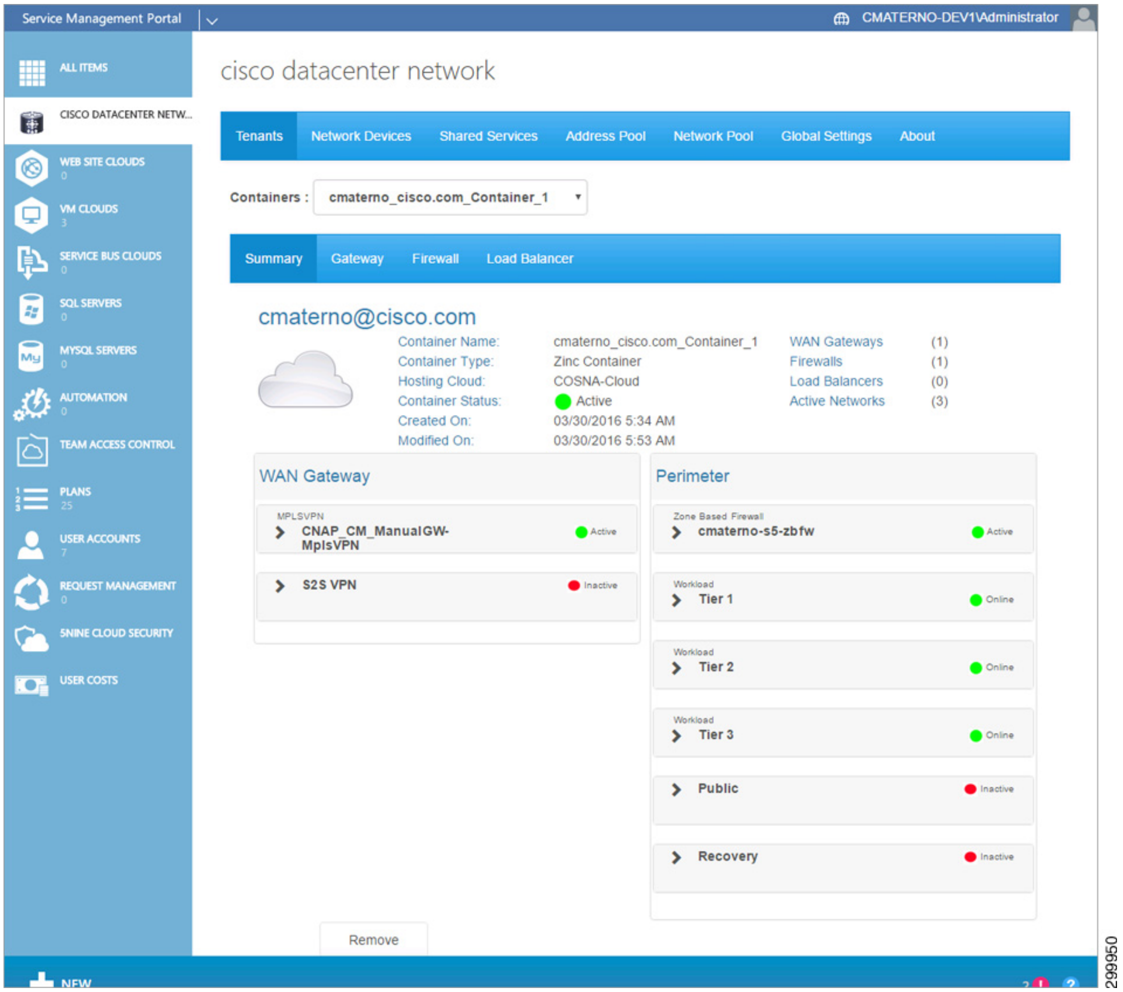
☑ Modification Enabled

Step 5 Click the check mark.

Step 6 Click **Cisco Datacenter Network**.

The container you created should be available in the Containers: pull-down menu at the top of the screen, as shown in the following screen.

Figure 1-13 Container Pull-down Menu Screen



Containers : cmaterno_cisco.com_Container_1

cmaterno@cisco.com

Container Name:	cmaterno_cisco.com_Container_1	WAN Gateways	(1)
Container Type:	Zinc Container	Firewalls	(1)
Hosting Cloud:	COSNA-Cloud	Load Balancers	(0)
Container Status:	● Active	Active Networks	(3)
Created On:	03/30/2016 5:34 AM		
Modified On:	03/30/2016 5:53 AM		

WAN Gateway

- MPLSVPN > CNAP_CM_ManualGW-MplsVPN ● Active
- > S2S VPN ● Inactive

Perimeter

- Zone Based Firewall > cmaterno-s5-zbfw ● Active
- Workload > Tier 1 ● Online
- Workload > Tier 2 ● Online
- Workload > Tier 3 ● Online
- > Public ● Inactive
- > Recovery ● Inactive

CHAPTER 2

Viewing and Modifying Information about Containers

You can view and modify a variety of information about containers, including:

- View summary information about a container
- Delete a container
- View gateway information about a container, including remove a WAN gateway
- View and modify access to Shared Services, including:
  - View information about Shared Services
  - Enable access to Shared Services for specific tiers
  - Change access to Shared Services for specific tiers
  - Disable access to Shared Services for specific tiers
- View and modify firewall information about a container, including:
  - View summary information about a firewall
  - View the hierarchy of information on the Firewall tab
  - Configure a firewall
  - Change the policy map for a service policy
  - Add a new class map
  - Change a class map
  - Create a new network Access Control List (ACL)
  - Change an Access Control List
  - Create a new object group
  - Change an object group
- View and modify tier information about a container, including:
  - Add a tier
  - Change a tier (and update a segment)
  - Remove a tier
  - Remove a segment
- View and modify load balancer information about a container, including:

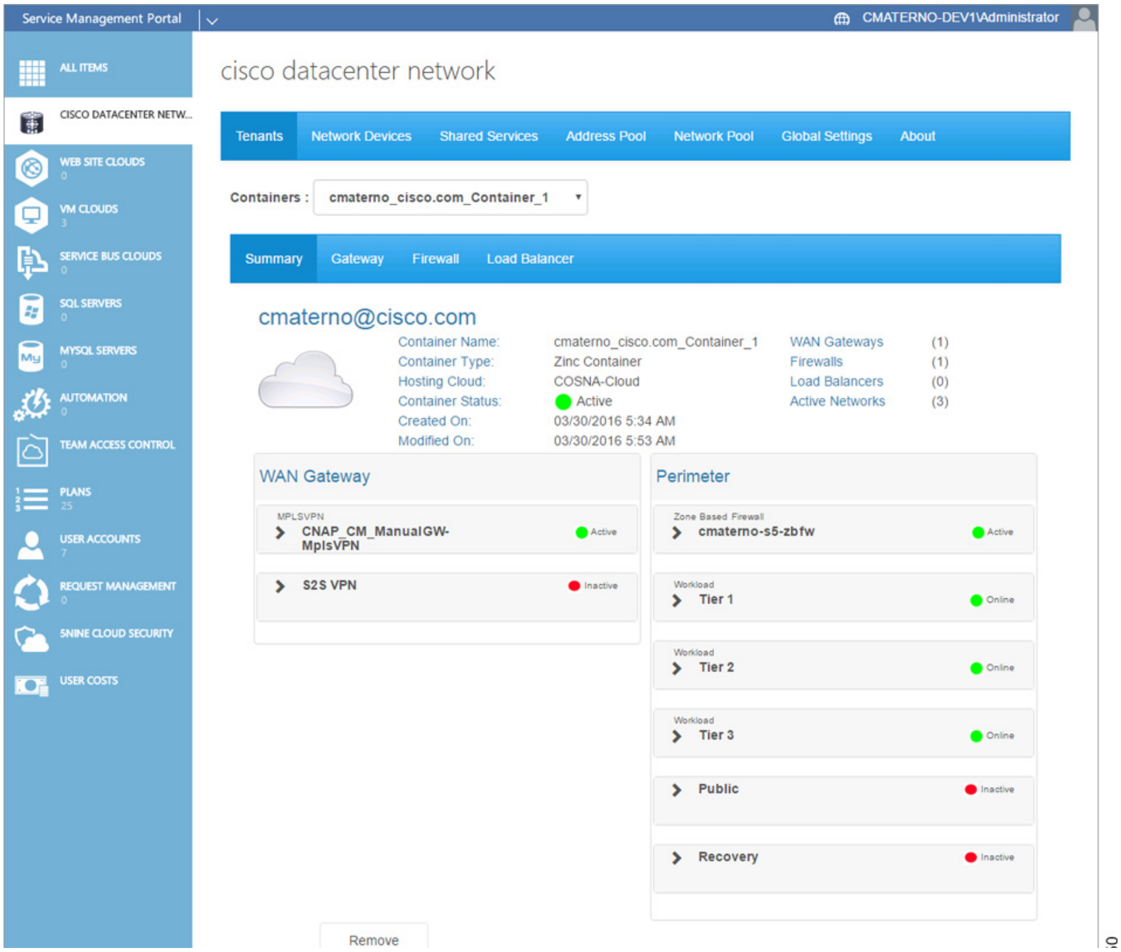
- – View information about an existing load balancer
- – Add a Citrix NetScaler VPX
- – Add a load balancer
- – Add a server
- – Change a load balancer
- – Change a server
- – Remove a load balancer
- – Remove a server
- – Remove a Citrix NetScaler VPX

Viewing Summary Information about a Container

Step 1 To display summary information about a specific container instance, click **Cisco Datacenter Network**.

You see the Tenant Summary Tab screen.

Figure 2-1 Tenant Summary Tab Screen



Containers : cmaterno_cisco.com_Container_1

cmaterno@cisco.com

Container Name:	cmaterno_cisco.com_Container_1	WAN Gateways	(1)
Container Type:	Zinc Container	Firewalls	(1)
Hosting Cloud:	COSNA-Cloud	Load Balancers	(0)
Container Status:	● Active	Active Networks	(3)
Created On:	03/30/2016 5:34 AM		
Modified On:	03/30/2016 5:53 AM		

WAN Gateway

MPLSVPN	CNAP_CM_ManualGW-MplsVPN	● Active
	S2S VPN	● Inactive

Perimeter

Zone Based Firewall	cmaterno-s5-zbfw	● Active
Workload	Tier 1	● Online
Workload	Tier 2	● Online
Workload	Tier 3	● Online
	Public	● Inactive
	Recovery	● Inactive

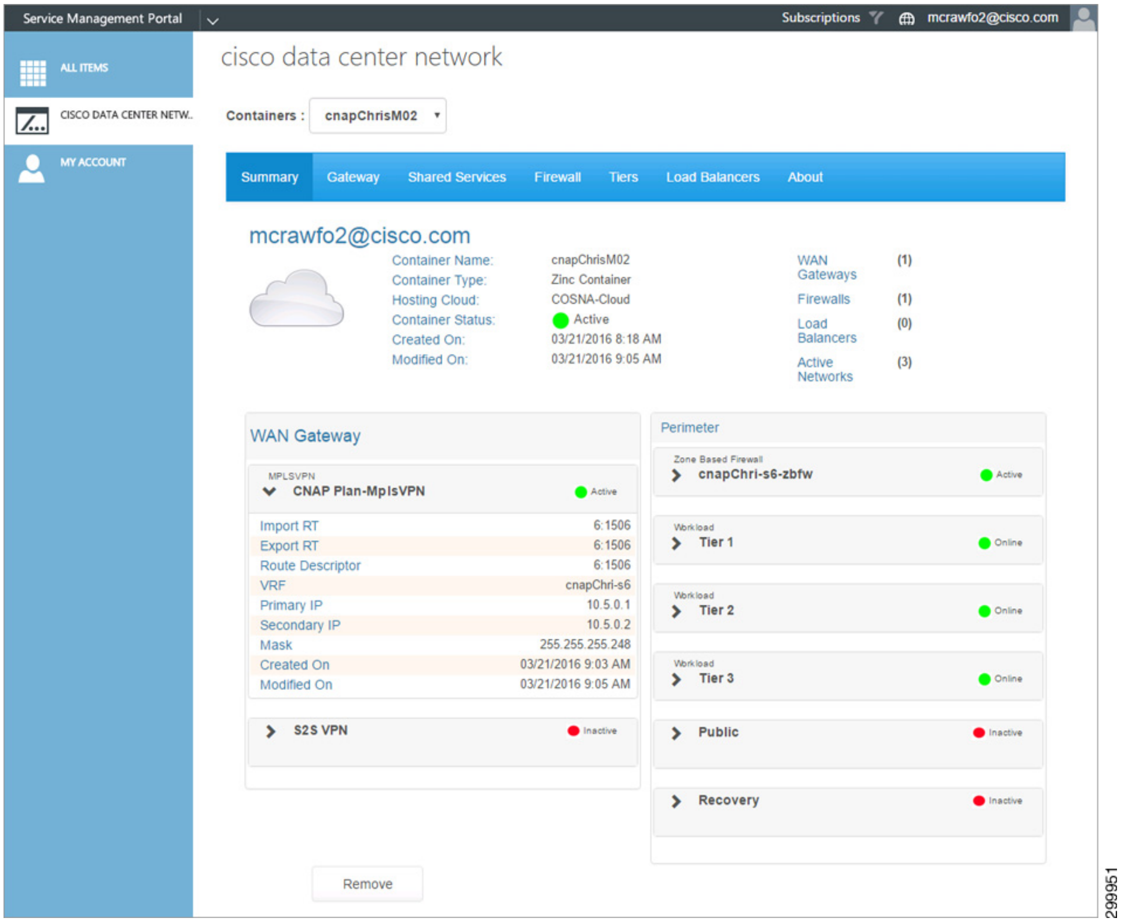
The Tenants Summary screen displays a list of all the WAN Gateway services configured in the container (MPLS VPN, Site-to-Site, Remote Access, and Internet) and a list of all the perimeter network services configured in the container (firewall, tiers, DMZ, etc.).

Specific information above the WAN Gateway and Perimeter tables includes:

- Container Name:—Displays the container name.
- Container Type:—Displays the container type name.
- Hosting Cloud:—Displays the Hosting Cloud name.
- Status:—Displays the container status. The icons indicate (icons are only meaningful on initial configuration as status is not routinely monitored):
  - Green—Container is Active.
  - Red—Container is Inactive.
  - Yellow—Container state is Creating.
- Created On:—Displays the date and time when the container was created.
- Modified On:—Displays the date and time when the container was last modified.
- WAN Gateways—Displays the total count of WAN gateways. For example, if MPLS VPN and Site-to-Site were part of the container, the displayed text would be WAN Gateways (2). The icon indicates the status of the WAN Gateway(s): Green, Red, and Gray (icons are only meaningful on initial configuration as status is not routinely monitored).
- Firewalls—Displays the total count of firewalls. For example, if one firewall was part of the container, the displayed text would be Firewalls (1). The icon indicates the status of the firewall(s): Green, Red, and Gray (icons are only meaningful on initial configuration as status is not routinely monitored).
- Load Balancers—Displays the total count of Load Balancers. For example, if two tiers have an SLB, the displayed text would be Load Balancers (2). The current release only supports one tier. The icon indicates the status of the load balancer(s): Green, Red, and Gray (icons are only meaningful on initial configuration as status is not routinely monitored).
- Active Networks—Displays the total count of active networks configured on the container. For example, if there were five total networks, the displayed text would be Active Networks (5).

You can collapse and expand the table information using the triangles, as shown in the following sample screen for the MPLS VPN WAN Gateway and Perimeter Tier 1.

Figure 2-2 Summary Tab—WAN Gateway MPLS VPN Details



Containers : cnapChrisM02

mcrawfo2@cisco.com

Container Name:	cnapChrisM02
Container Type:	Zinc Container
Hosting Cloud:	COSNA-Cloud
Container Status:	● Active
Created On:	03/21/2016 8:18 AM
Modified On:	03/21/2016 9:05 AM

WAN Gateways	(1)
Firewalls	(1)
Load Balancers	(0)
Active Networks	(3)

WAN Gateway

MPLSVPN
CNAP Plan-MplsVPN ● Active

Import RT	6:1506
Export RT	6:1506
Route Descriptor	6:1506
VRF	cnapChri-s6
Primary IP	10.5.0.1
Secondary IP	10.5.0.2
Mask	255.255.255.248
Created On	03/21/2016 9:03 AM
Modified On	03/21/2016 9:05 AM

S2S VPN ● Inactive

Perimeter

Zone Based Firewall
cnapChri-s6-zbfw ● Active

Workload
Tier 1 ● Online

Workload
Tier 2 ● Online

Workload
Tier 3 ● Online

Public ● Inactive

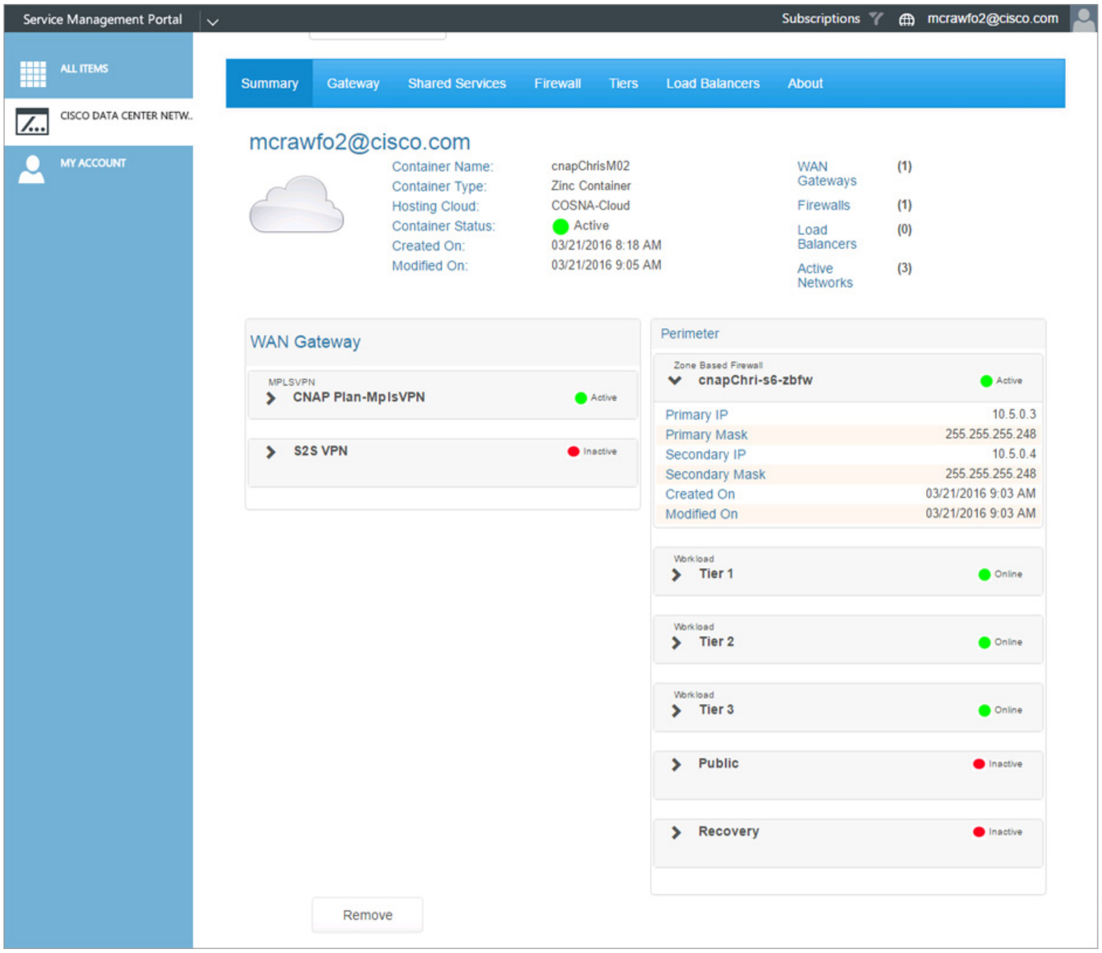
Recovery ● Inactive

Using MPLS VPN as an example, the information in the WAN Gateway table includes:

- MPLSVPN and name—Gateway type, name of the gateway, and an icon to indicate the status of the VPN (icons are only meaningful on initial configuration as status is not routinely monitored).
- Import RT—The configured RT for the WAN Gateway.
- Export RT—The configured RT for the WAN Gateway.
- Route Descriptor—The configured descriptor based on your cloud provider's network design.
- VRF—Generated by Cisco CNAP based on the abbreviation of the container ID.
- Primary IP—External PE IP Address in dotted format.
- Secondary IP—External PE IP Address in dotted format.
- Mask—External PE Mask in dotted format
- Created On:—Displays the date and time when the WAN Gateway was created.
- Modified On:—Displays the date and time when the WAN Gateway was last modified.

Information in the Perimeter table is based on the currently selected Cloud Service and includes information about firewalls and tiers (in the current release, public for backups and recovery for DMZ are not used).

Figure 2-3 Summary Tab—Perimeter Firewall Details



mcrawfo2@cisco.com

Container Name:	cnapChrisM02
Container Type:	Zinc Container
Hosting Cloud:	COSNA-Cloud
Container Status:	● Active
Created On:	03/21/2016 8:18 AM
Modified On:	03/21/2016 9:05 AM

WAN Gateways	(1)
Firewalls	(1)
Load Balancers	(0)
Active Networks	(3)

WAN Gateway

- MPLSVPN CNAP Plan-MplsVPN ● Active
- S2S VPN ● Inactive

Perimeter

Zone Based Firewall
cnapChri-s6-zbfw ● Active

Primary IP	10.5.0.3
Primary Mask	255.255.255.248
Secondary IP	10.5.0.4
Secondary Mask	255.255.255.248
Created On	03/21/2016 9:03 AM
Modified On	03/21/2016 9:03 AM

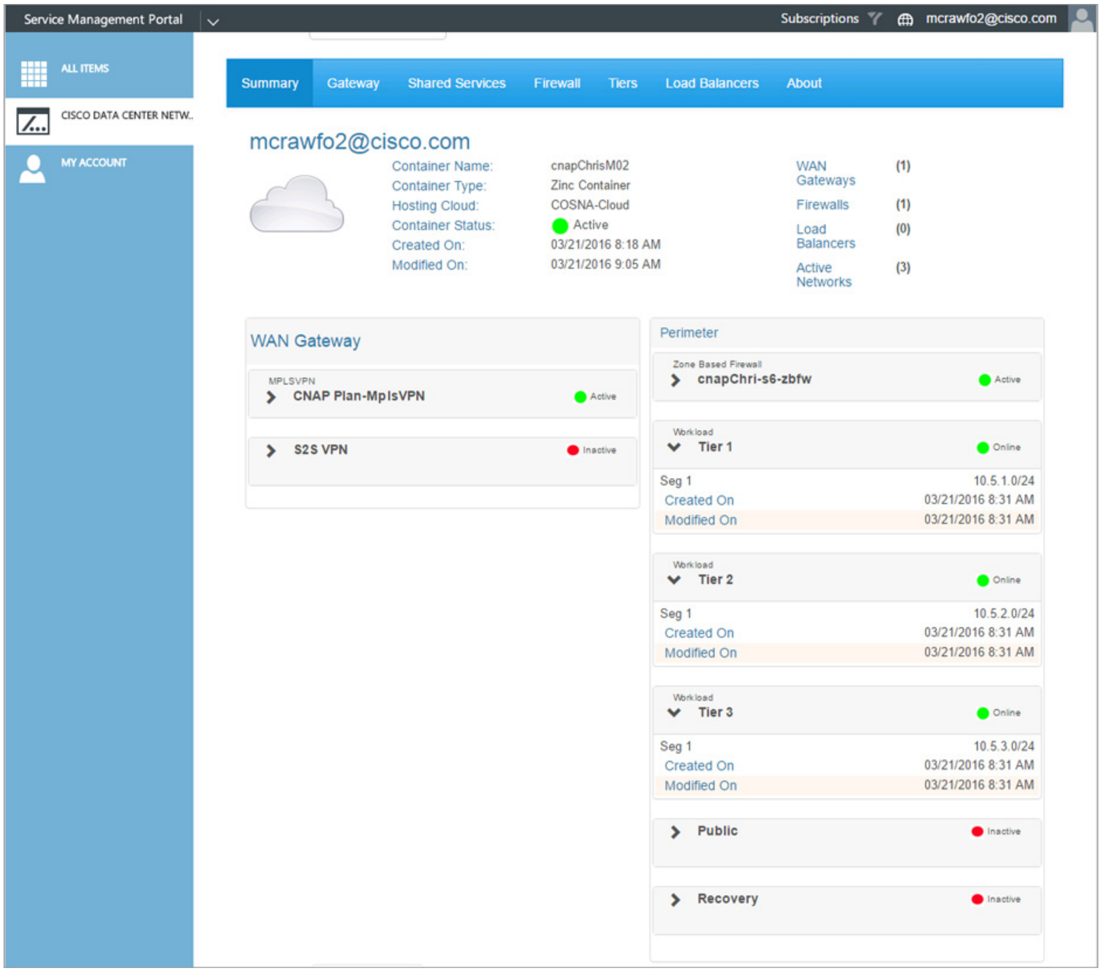
- Workload Tier 1 ● Online
- Workload Tier 2 ● Online
- Workload Tier 3 ● Online
- Public ● Inactive
- Recovery ● Inactive

299952

Using Zone Based Firewall as an example, the information in the Perimeter table includes:

- Zone Based Firewall and name—Firewall type, name of the firewall, and an icon to indicate the status of the firewall (icons are only meaningful on initial configuration as status is not routinely monitored).
- Primary IP—External PE IP Address
- Primary Mask—External PE Mask
- Secondary IP—External PE IP Address
- Secondary Mask—External PE Mask
- Created On:—Displays the date and time when the firewall was created.
- Modified On:—Displays the date and time when the firewall was last modified.

Figure 2-4 Summary Tab—Perimeter Tier Details



mcrawfo2@cisco.com

Container Name:	cnapChrisM02	WAN Gateways	(1)
Container Type:	Zinc Container	Firewalls	(1)
Hosting Cloud:	COSNA-Cloud	Load Balancers	(0)
Container Status:	● Active	Active Networks	(3)
Created On:	03/21/2016 8:18 AM		
Modified On:	03/21/2016 9:05 AM		

WAN Gateway

MPLSVPN
CNAP Plan-MplsVPN ● Active

S2S VPN ● Inactive

Perimeter

Zone Based Firewall
cnapChri-s6-zbfw ● Active

Workload
Tier 1 ● Online

Seg 1	10.5.1.0/24
Created On	03/21/2016 8:31 AM
Modified On	03/21/2016 8:31 AM

Workload
Tier 2 ● Online

Seg 1	10.5.2.0/24
Created On	03/21/2016 8:31 AM
Modified On	03/21/2016 8:31 AM

Workload
Tier 3 ● Online

Seg 1	10.5.3.0/24
Created On	03/21/2016 8:31 AM
Modified On	03/21/2016 8:31 AM

Public ● Inactive

Recovery ● Inactive

299953

Information in the Perimeter table for each Tier includes:

- Seg 1—IP Address of the tier segment.
- Created On:—Displays the date and time when Tier l was created.
- Modified On:—Displays the date and time when Tier 1 was last modified.

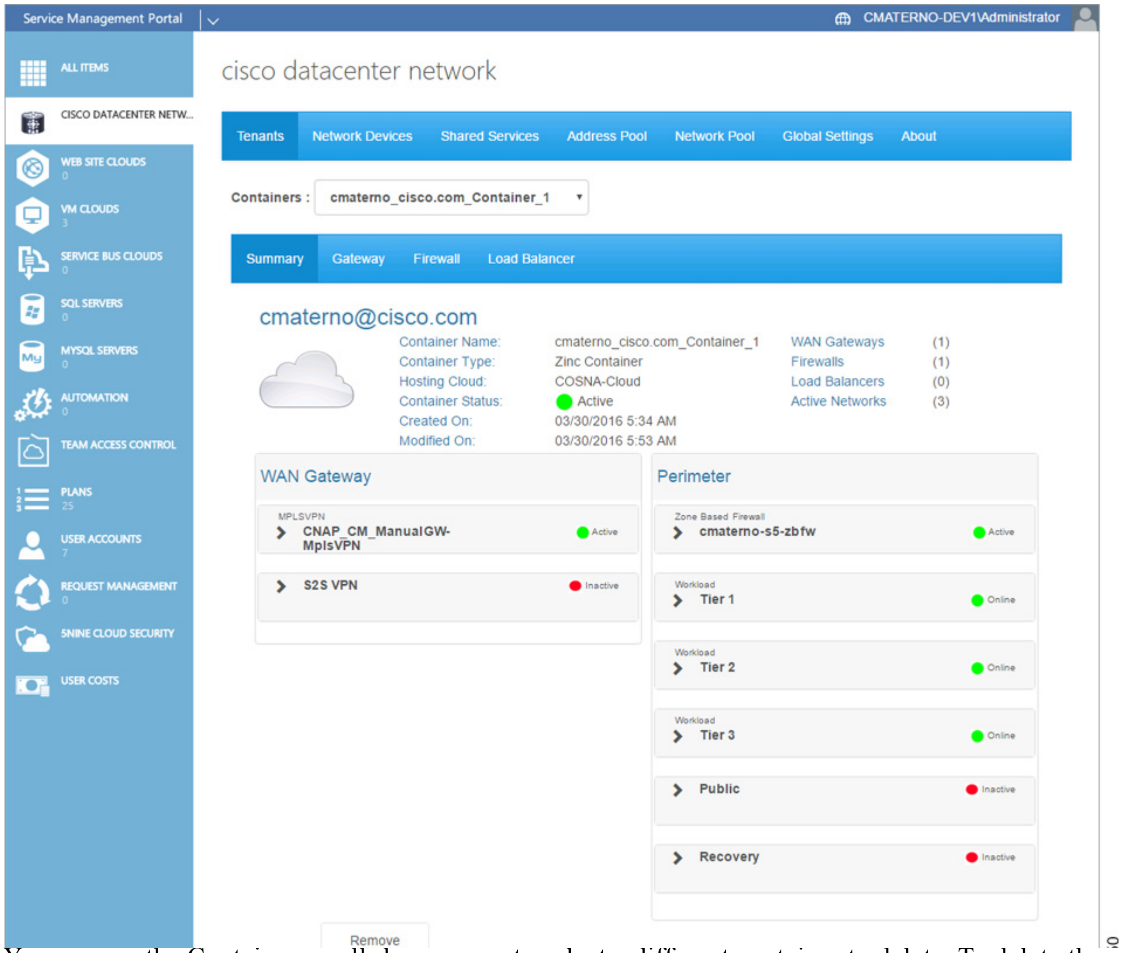
Deleting a Container

Note When you delete a container, all information about the container is deleted from the Cisco CNAP database and none of the deleted information can be recovered.

Step 1 To display summary information about a specific container instance, click **Cisco Datacenter Network**.

You see the Tenant Summary Tab screen.

Figure 2-5 Tenant Summary Tab Screen



Containers : cmaterno_cisco.com_Container_1

cmaterno@cisco.com

Container Name:	cmaterno_cisco.com_Container_1	WAN Gateways	(1)
Container Type:	Zinc Container	Firewalls	(1)
Hosting Cloud:	COSNA-Cloud	Load Balancers	(0)
Container Status:	● Active	Active Networks	(3)
Created On:	03/30/2016 5:34 AM		
Modified On:	03/30/2016 5:53 AM		

WAN Gateway

- MPLSVPN CNAP_CM_ManualGW-MplsVPN ● Active
- S2S VPN ● Inactive

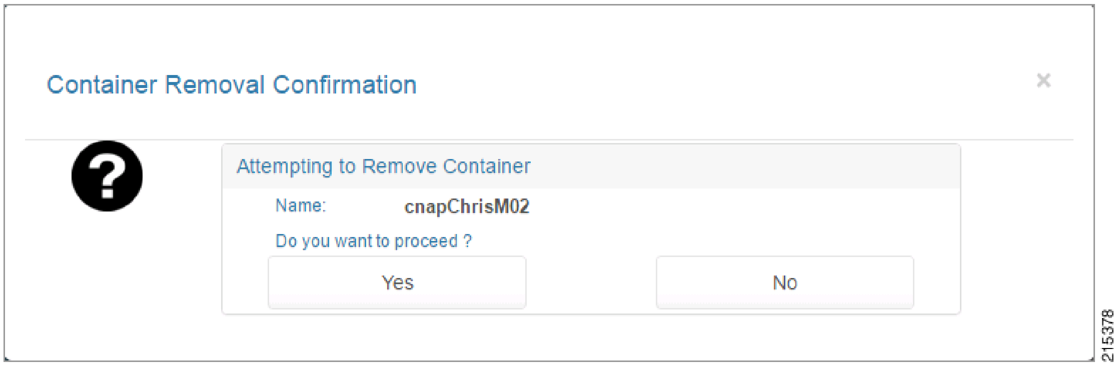
Perimeter

- Zone Based Firewall cmaterno-s5-zbfw ● Active
- Workload Tier 1 ● Online
- Workload Tier 2 ● Online
- Workload Tier 3 ● Online
- Public ● Inactive
- Recovery ● Inactive

Step 2 You can use the Containers: pull-down menu to select a different container to delete. To delete the selected container, at the bottom of the screen click **Remove**.

You see a screen asking you to confirm the deletion, as shown in the following screen.

Figure 2-6 Confirm Container Deletion



Container Removal Confirmation

Attempting to Remove Container

Name: cnapChrisM02

Do you want to proceed ?

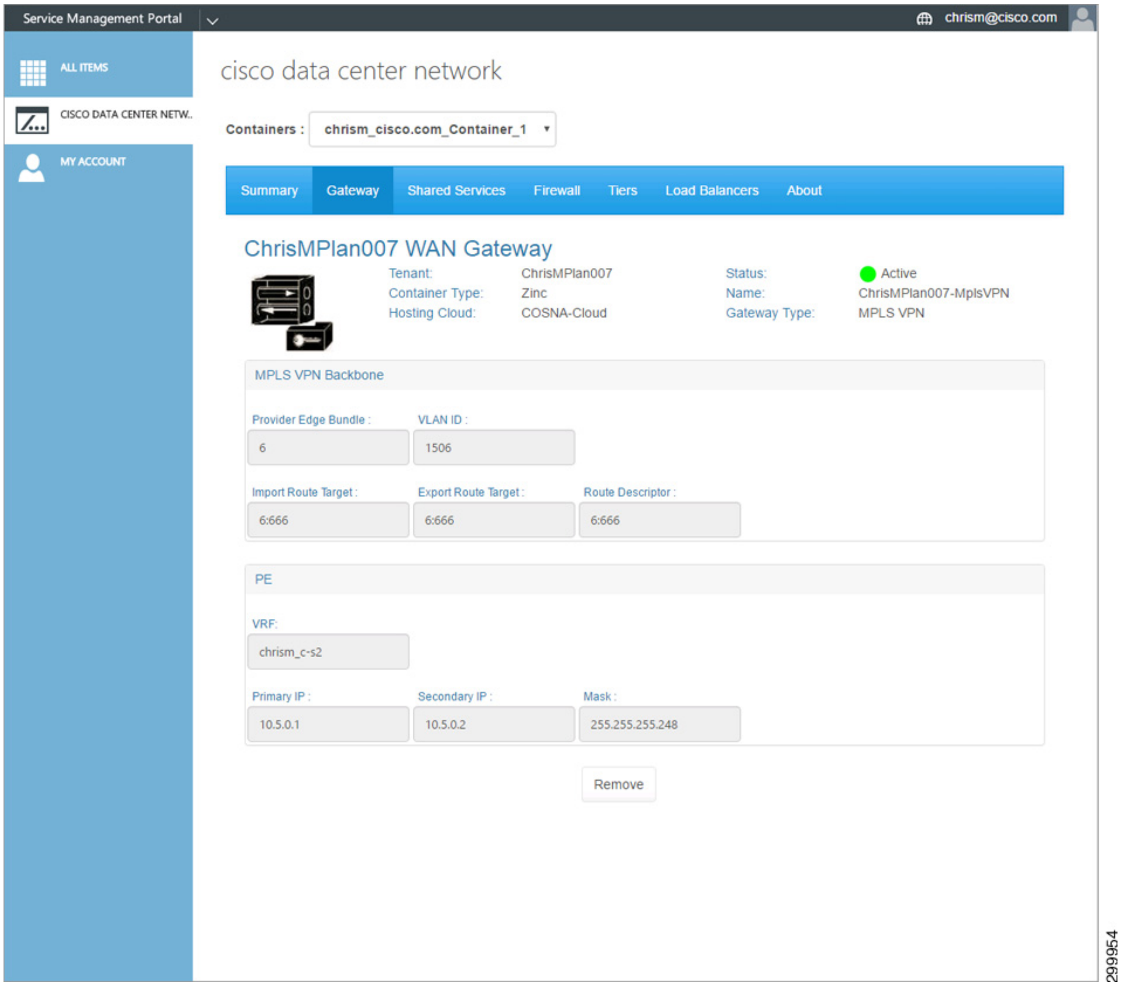
Step 3 Click **Yes** to delete the container or **No** to cancel the deletion.

Viewing Gateway Information about a Container

Step 1 To view gateway information for the currently selected container, click the **Gateway** tab.

You see the Tenant Gateway screen. The screen below shows an example for MPLS.

Figure 2-7 Tenant Gateway Tab Screen—MPLS



Containers : chrism_cisco.com_Container_1

ChrisMPlan007 WAN Gateway

Tenant: ChrisMPlan007
Container Type: Zinc
Hosting Cloud: COSNA-Cloud
Status: ● Active
Name: ChrisMPlan007-MplsVPN
Gateway Type: MPLS VPN

MPLS VPN Backbone

Provider Edge Bundle : 6
VLAN ID : 1506
Import Route Target : 6:666
Export Route Target : 6:666
Route Descriptor : 6:666

PE

VRF: chrism_c-s2
Primary IP : 10.5.0.1
Secondary IP : 10.5.0.2
Mask : 255.255.255.248

You can perform the following operation on the gateway screen:

- Remove Button—To remove a gateway, click **Remove**.

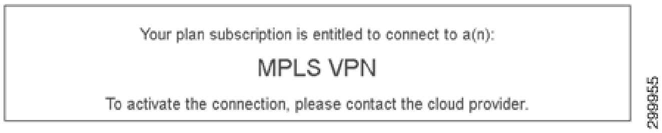
The screen displays the following information:

- Tenant:—Displays the tenant name.
- Container Type:—Displays the container type name, which in the current release is limited to Zinc.
- Hosting Cloud:—Displays the Hosting Cloud name.
- Status:—Displays the WAN Gateway status. The icons indicate (icons are only meaningful on initial configuration as status is not routinely monitored):
  - Green—WAN Gateway is Active.

  - Red—WAN Gateway is Inactive.
  - Yellow—WAN Gateway state is Creating.
- Name:—Displays the name in the form <abbreviation>-mpls-vpn.
- Gateway Type:—MPLS VPN
- Description:—Descriptive name.
- MPLS VPN Backbone:
  - Aut. System Number—The PEaciL2InterfacePrimary field from the global settings (contact your cloud provider for more information about this field).
  - Network ID—VLAN ID.
  - Import Route Target—Configured RT for the WAN Gateway.
  - Export Route Target—Configured RT for the WAN Gateway.
  - Route Descriptor—Configured descriptor based on your cloud provider's network design.
- PE:
  - VRF—Generated by Cisco CNAP based on the abbreviation of the container ID.
  - Primary IP—External PE IP Address in dotted format.
  - Secondary IP—External PE IP Address in dotted format.
  - Mask—External PE Mask in dotted format

Step 2 If the WAN Gateway has not been activated, you see the following screen.

Figure 2-8 Gateway Tab—WAN Gateway Not Activated



Your plan subscription is entitled to connect to a(n):

MPLS VPN

To activate the connection, please contact the cloud provider.

Step 3 Contact your cloud provider to have the WAN Gateway activated.

Removing a WAN Gateway

To remove a WAN Gateway, click **Remove**.

Viewing and Modifying Access to Shared Services

If your cloud provider has configured access to Shared Services, such as Database as a Service (DBaaS), Disaster Recovery as a Service (DRaaS), etc., those Shared Services will be displayed when you are creating a container for a plan to which you have subscribed.

On the Shared Services tab you can:

- View at information about Shared Services
- Enable access to Shared Services for specific tiers
- Change access to Shared Services for specific tiers

- Disable access to Shared Services for specific tiers

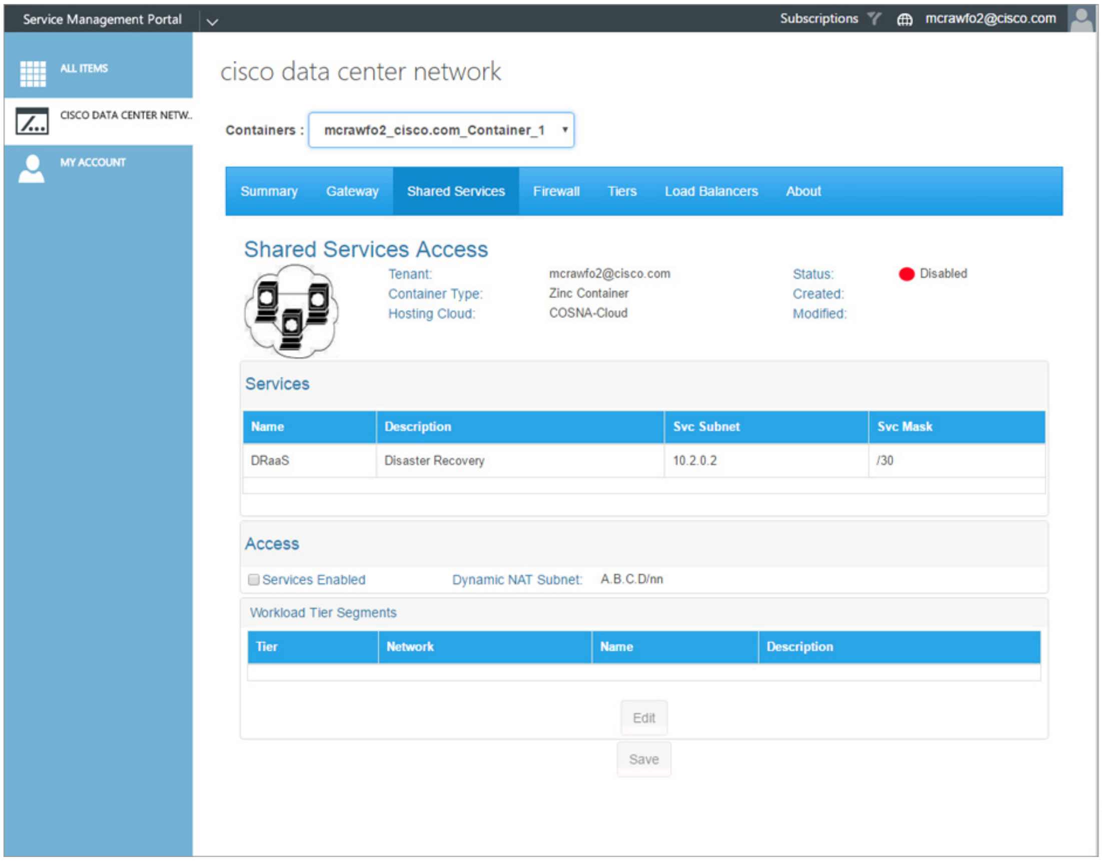
Viewing Information about Shared Services

To view information about Shared Services:

Step 1 Click the **Shared Services** tab.

You see the following screen.

Figure 2-9 Shared Services Tab



cisco data center network

Containers : mcrawfo2_cisco.com_Container_1

Shared Services Access

Tenant: mcrawfo2@cisco.com

Container Type: Zinc Container

Hosting Cloud: COSNA-Cloud

Status: ● Disabled

Created:

Modified:

Services

Name	Description	Svc Subnet	Svc Mask
DRaaS	Disaster Recovery	10.2.0.2	/30

Access

□ Services Enabled Dynamic NAT Subnet: A.B.C.D/nn

Workload Tier Segments

Tier	Network	Name	Description

This screen displays the following fields:

- Tenant:—Displays the tenant name.
- Container Type:—Displays the container type instance name.
- Hosting Cloud:—Displays the Hosting Cloud name.
- Status:—Displays the Shared Services Access status. The icons indicate (icons are only meaningful on initial configuration as status is not routinely monitored):
  - Green—Access is Enabled.
  - Red—Access is Disabled.
- Created:—Displays the date and time when access was activated in the form.

- Modified:—Displays the date and time when access was last modified in the form.
- Services:
  - Name— Name given to the Shared Service at the time the service was onboarded.
  - Description—Brief description of the Shared Service.
  - Svc Subnet— IP subnet (Public) on which the Shared Service is available.
  - Svc Mask— Subnet Mask associated with the Shared Service subnet.
- Access:
  - Services Enabled—Indicates whether Shared Services are enabled.
  - Dynamic NAT Subnet—The associated NAT subnet.
- Workload Tier Segments:
  - Tier—The Tier name.
  - Network—The Tier network.
  - Name—The segment name.
  - Description—The segment description.

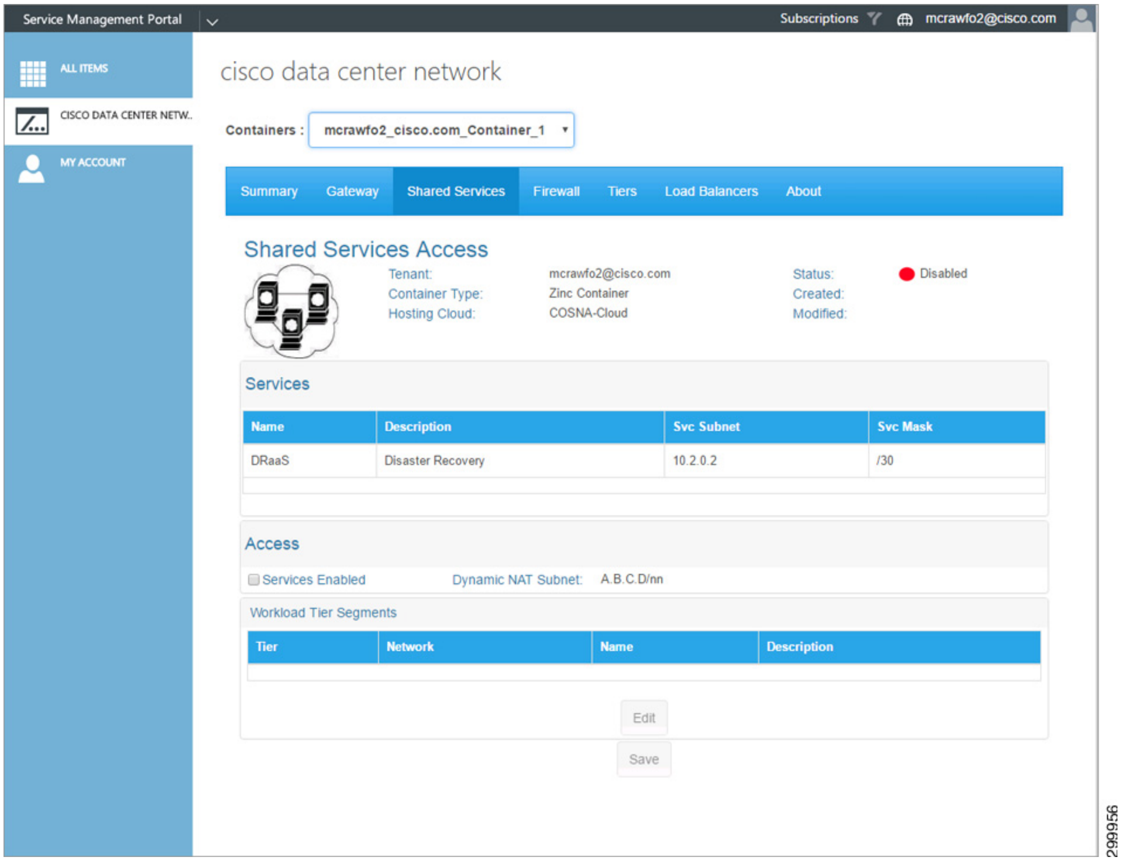
Enabling Access to Shared Services

To enable access to Shared Services:

Step 1 Click the **Shared Services** tab.

You see the following screen, which lists the available Shared Services.

Figure 2-10 Enabling Access to Shared Services



Containers : mcrawfo2_cisco.com_Container_1

Shared Services Access

Tenant: mcrawfo2@cisco.com
Container Type: Zinc Container
Hosting Cloud: COSNA-Cloud
Status: ● Disabled
Created:
Modified:

Services

Name	Description	Svc Subnet	Svc Mask
DRaaS	Disaster Recovery	10.2.0.2	/30

Access

□ Services Enabled Dynamic NAT Subnet: A.B.C.D/nn

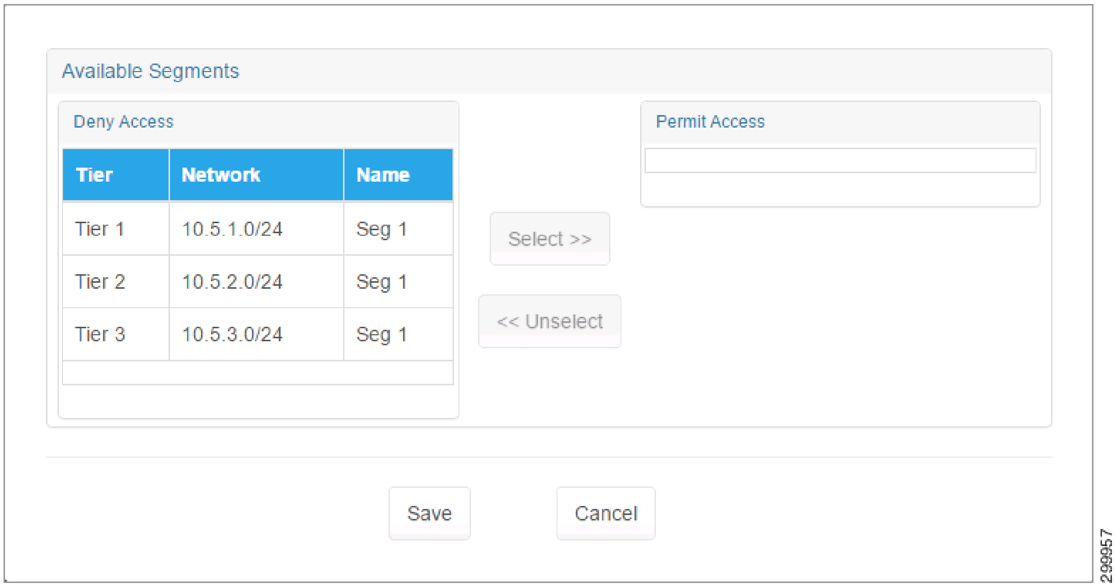
Workload Tier Segments

Tier	Network	Name	Description

Step 2 Click the check box next to **Services Enabled** and click **Edit**.

You see the following screen.

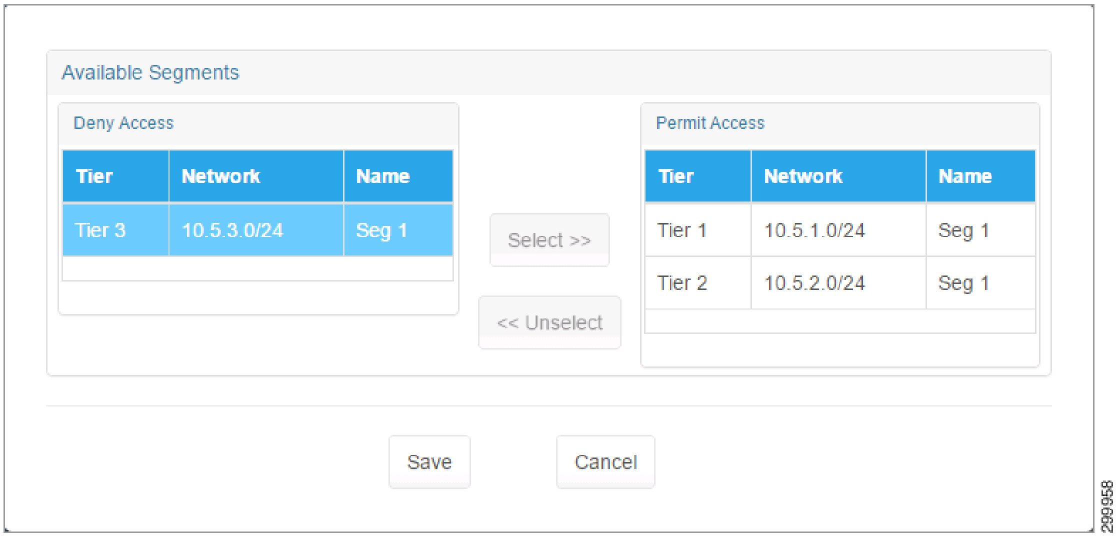
Figure 2-11 ***Select Tier Segments with Access to Shared Services***



Tier	Network	Name
Tier 1	10.5.1.0/24	Seg 1
Tier 2	10.5.2.0/24	Seg 1
Tier 3	10.5.3.0/24	Seg 1

Step 3 Click a tier segment you want to have access to Shared Services, then click **Select>>**. Select additional tier segments in the same way, as shown in the following screen.

Figure 2-12 ***Tier Segments Selected***



Deny Access

Tier	Network	Name
Tier 3	10.5.3.0/24	Seg 1

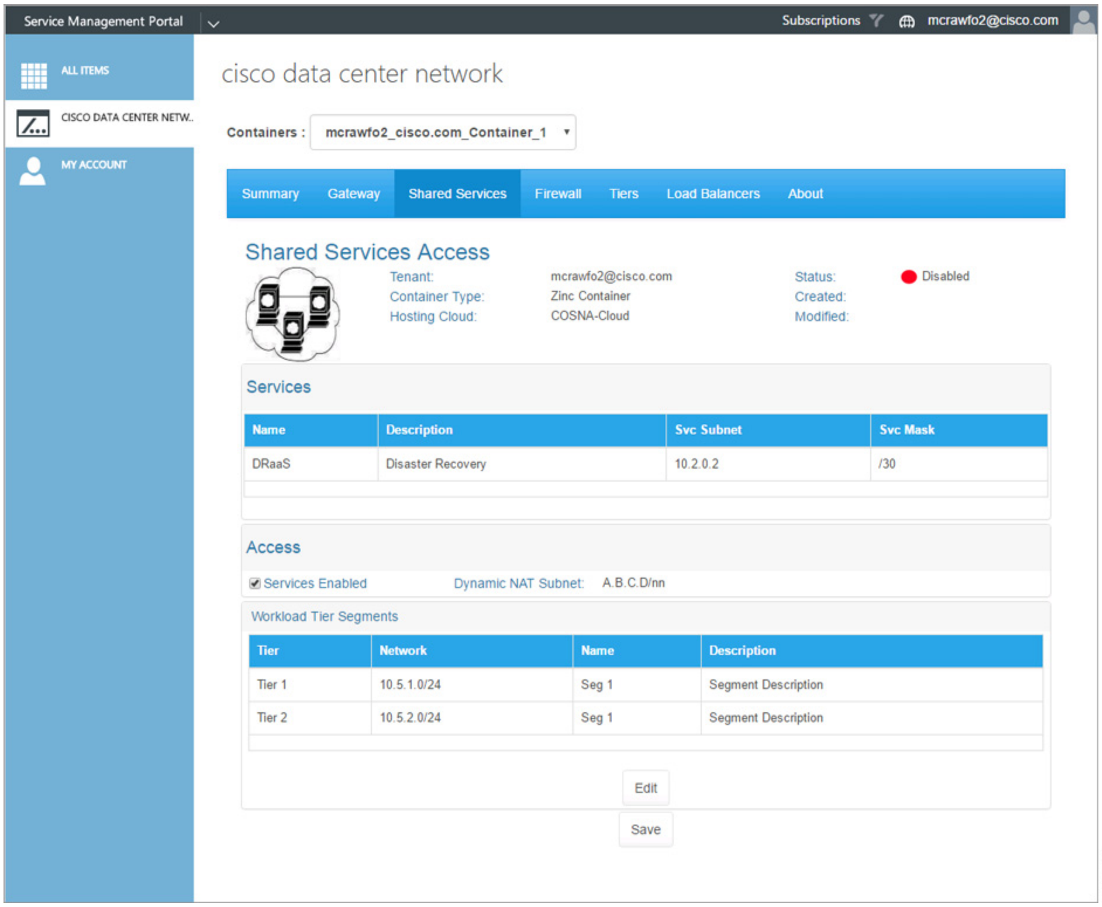
Permit Access

Tier	Network	Name
Tier 1	10.5.1.0/24	Seg 1
Tier 2	10.5.2.0/24	Seg 1

Step 4 When you are finished selecting tier segments, click **Save**.

You return to the Shared Service tab screen with the selected tiers displayed under Workload Tier Segments, as shown in the following screen.

Figure 2-13 Shared Services Tab with Access Enabled for Tier Segments



Containers : mcrawfo2_cisco.com_Container_1

Shared Services Access

Tenant: mcrawfo2@cisco.com
Container Type: Zinc Container
Hosting Cloud: COSNA-Cloud
Status: ● Disabled
Created:
Modified:

Services

Name	Description	Svc Subnet	Svc Mask
DRaaS	Disaster Recovery	10.2.0.2	/30

Access

☑ Services Enabled Dynamic NAT Subnet: A.B.C.D/nn

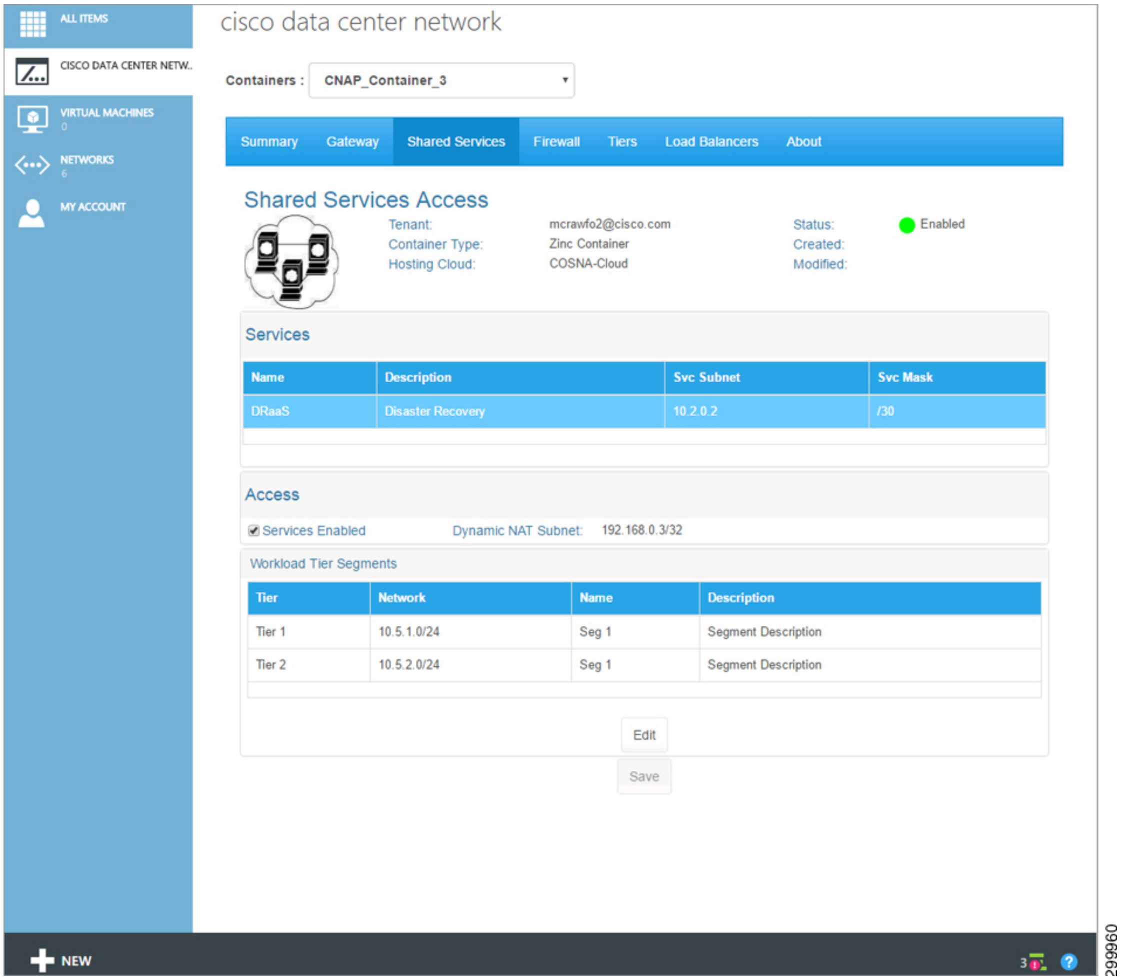
Workload Tier Segments

Tier	Network	Name	Description
Tier 1	10.5.1.0/24	Seg 1	Segment Description
Tier 2	10.5.2.0/24	Seg 1	Segment Description

Step 5 The tier segments do not have access until you click **Save**.

The configuration takes a few moments. When you refresh the screen, you see that the Status: is now Enabled. If you click on a specific Shared Services, the Dynamic NAT Subnet: field will update, as shown in the following screen. The Dynamic NAT Subnet is configured by your cloud provider.

Figure 2-14 Shared Services Access Enabled



Containers : CNAP_Container_3

Shared Services Access

Tenant: mcrawfo2@cisco.com
Container Type: Zinc Container
Hosting Cloud: COSNA-Cloud
Status: ● Enabled
Created:
Modified:

Services

Name	Description	Svc Subnet	Svc Mask
DRaaS	Disaster Recovery	10.2.0.2	/30

Access

☑ Services Enabled Dynamic NAT Subnet: 192.168.0.3/32

Workload Tier Segments

Tier	Network	Name	Description
Tier 1	10.5.1.0/24	Seg 1	Segment Description
Tier 2	10.5.2.0/24	Seg 1	Segment Description

Changing Access to Shared Services

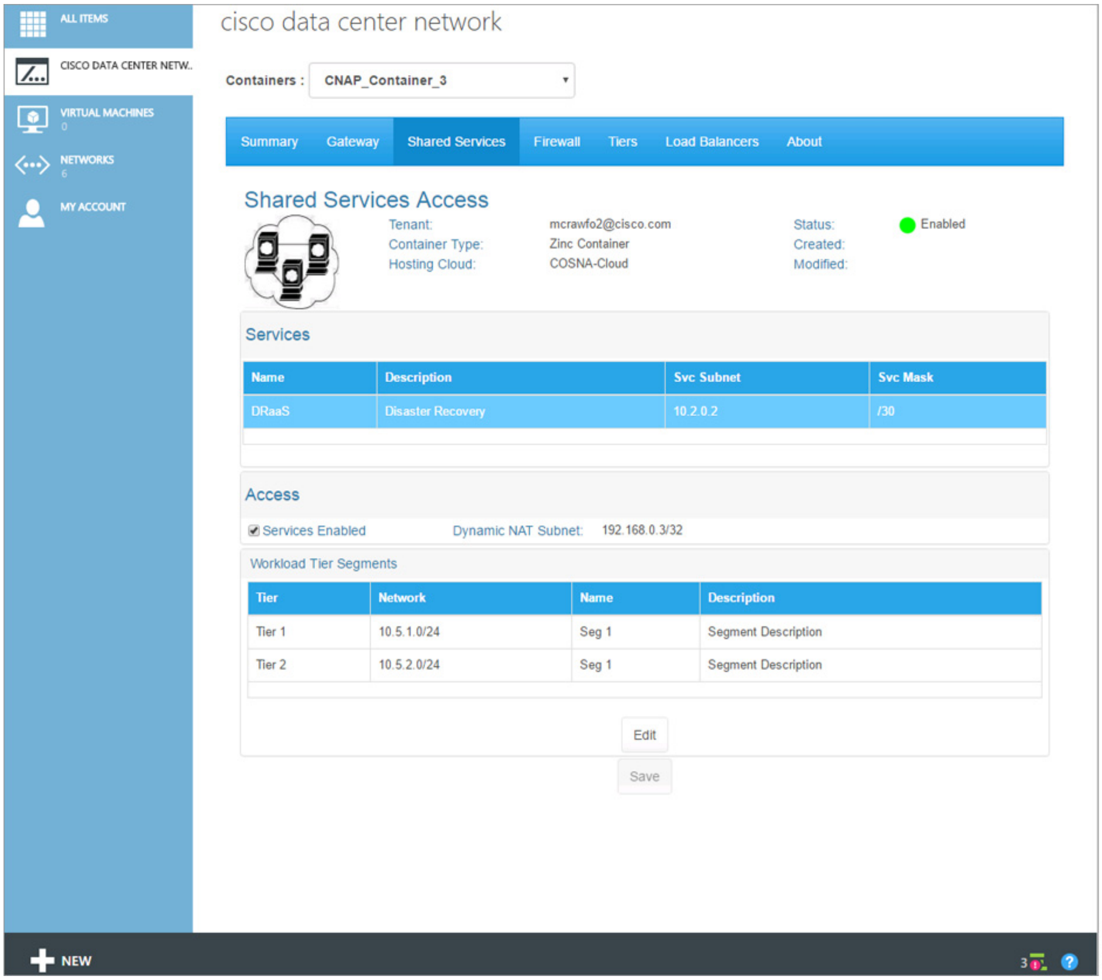
You can change and add access rights for tier segments.

To change access to Shared Services:

Step 1 Click the **Shared Services** tab.

You see the following screen, which lists the available Shared Services.

Figure 2-15 Changing Access to Shared Services



Containers : CNAP_Container_3

Shared Services Access

Tenant: mcrawfo2@cisco.com

Container Type: Zinc Container

Hosting Cloud: COSNA-Cloud

Status: ● Enabled

Created:

Modified:

Services

Name	Description	Svc Subnet	Svc Mask
DRaaS	Disaster Recovery	10.2.0.2	/30

Access

☑ Services Enabled Dynamic NAT Subnet: 192.168.0.3/32

Workload Tier Segments

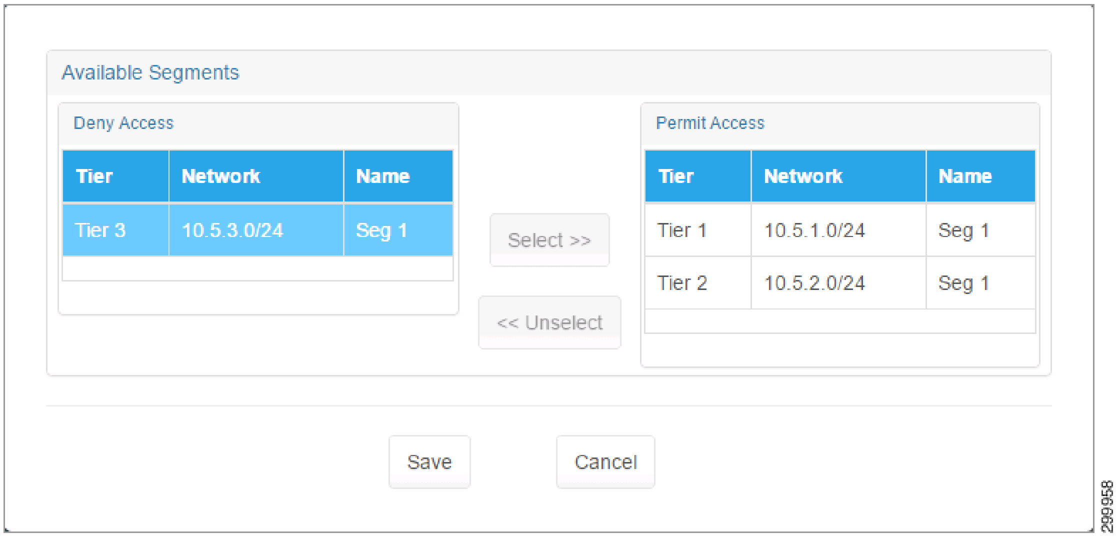
Tier	Network	Name	Description
Tier 1	10.5.1.0/24	Seg 1	Segment Description
Tier 2	10.5.2.0/24	Seg 1	Segment Description

299960

Step 2 Click **Edit**.

You see the following screen.

Figure 2-16 Tier Segments with Access to Shared Services



Available Segments

Deny Access

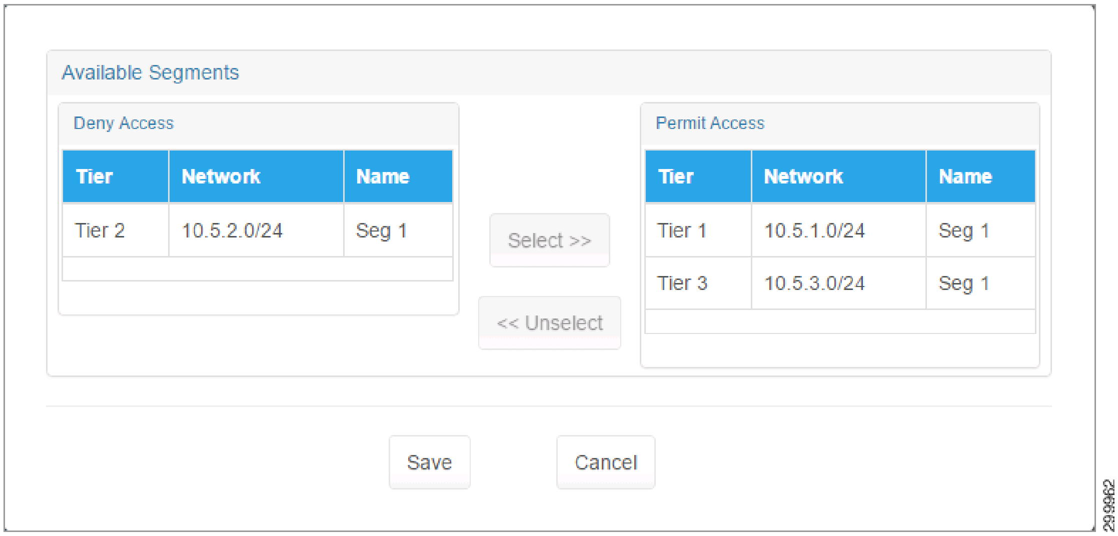
Tier	Network	Name
Tier 3	10.5.3.0/24	Seg 1

Permit Access

Tier	Network	Name
Tier 1	10.5.1.0/24	Seg 1
Tier 2	10.5.2.0/24	Seg 1

Step 3 You can remove and add access to tier segments by clicking a tier segment then clicking **Select>>** or **<<Unselect** to move tier segments between Deny Access and Permit Access. In the following screen, Tier 2 has been moved to Deny Access and Tier 3 to Permit Access.

Figure 2-17 Tier Segments Selected and Access Rights Changed



Available Segments

Deny Access

Tier	Network	Name
Tier 2	10.5.2.0/24	Seg 1

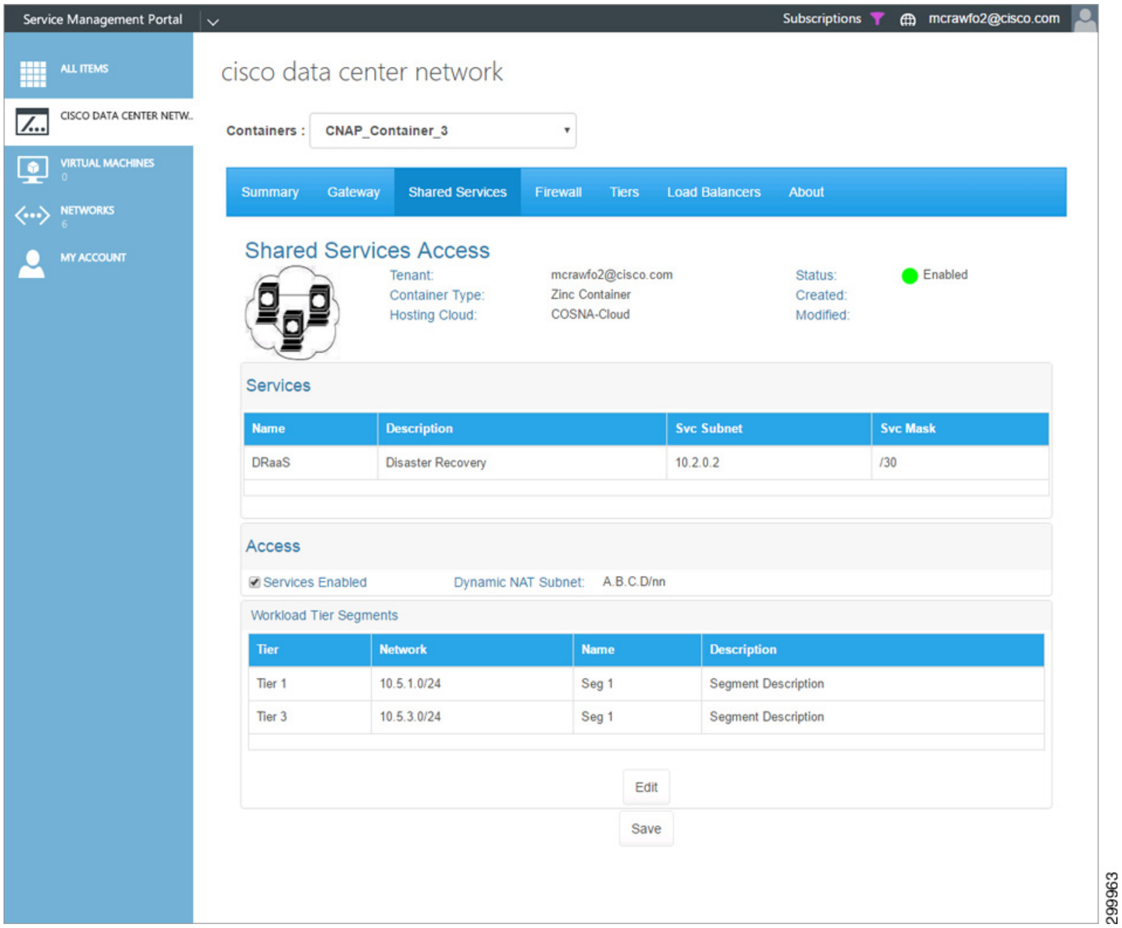
Permit Access

Tier	Network	Name
Tier 1	10.5.1.0/24	Seg 1
Tier 3	10.5.3.0/24	Seg 1

Step 4 When you are finished selecting tier segments, click **Save**.

You return to the Shared Service tab screen with the tiers displayed under Workload Tier Segments, as shown in the following screen.

Figure 2-18 Shared Services Tab with Access Changed for Tier Segments



Containers : CNAP_Container_3

Shared Services Access

Tenant: mcrawfo2@cisco.com
Container Type: Zinc Container
Hosting Cloud: COSNA-Cloud
Status: ● Enabled
Created:
Modified:

Services

Name	Description	Svc Subnet	Svc Mask
DRaaS	Disaster Recovery	10.2.0.2	/30

Access

☑ Services Enabled Dynamic NAT Subnet: A.B.C.D/nn

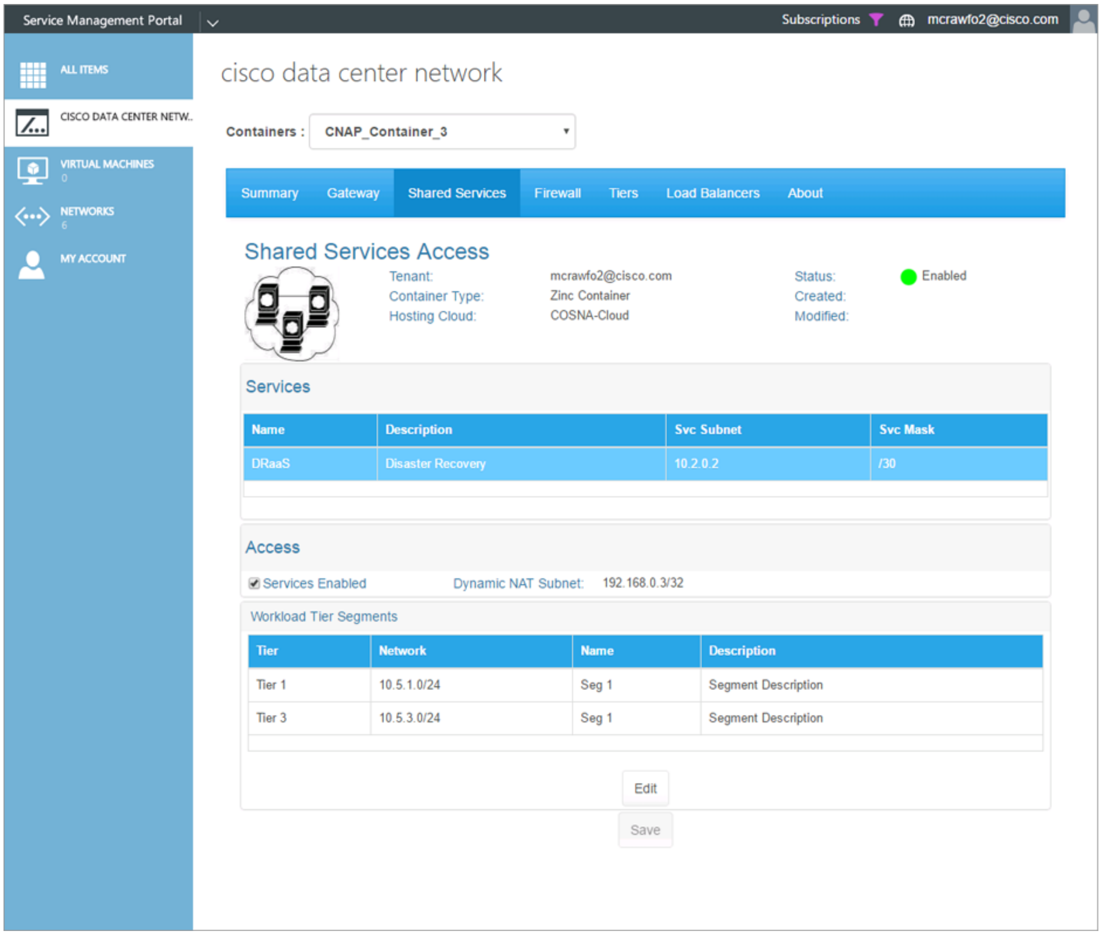
Workload Tier Segments

Tier	Network	Name	Description
Tier 1	10.5.1.0/24	Seg 1	Segment Description
Tier 3	10.5.3.0/24	Seg 1	Segment Description

Step 5 The changes to the tier segments are not effective until you click **Save**.

The configuration takes a few moments. When you refresh the screen, you see that the Status: is now Enabled. If you click on a specific Shared Services, the Dynamic NAT Subnet: field will update, as shown in the following screen.

Figure 2-19 Changed Shared Services Access Enabled



cisco data center network

Containers : CNAP_Container_3

Shared Services Access

Tenant: mcrawfo2@cisco.com
Container Type: Zinc Container
Hosting Cloud: COSNA-Cloud
Status: ● Enabled
Created:
Modified:

Services

Name	Description	Svc Subnet	Svc Mask
DRaaS	Disaster Recovery	10.2.0.2	/30

Access

☑ Services Enabled   Dynamic NAT Subnet: 192.168.0.3/32

Workload Tier Segments

Tier	Network	Name	Description
Tier 1	10.5.1.0/24	Seg 1	Segment Description
Tier 3	10.5.3.0/24	Seg 1	Segment Description

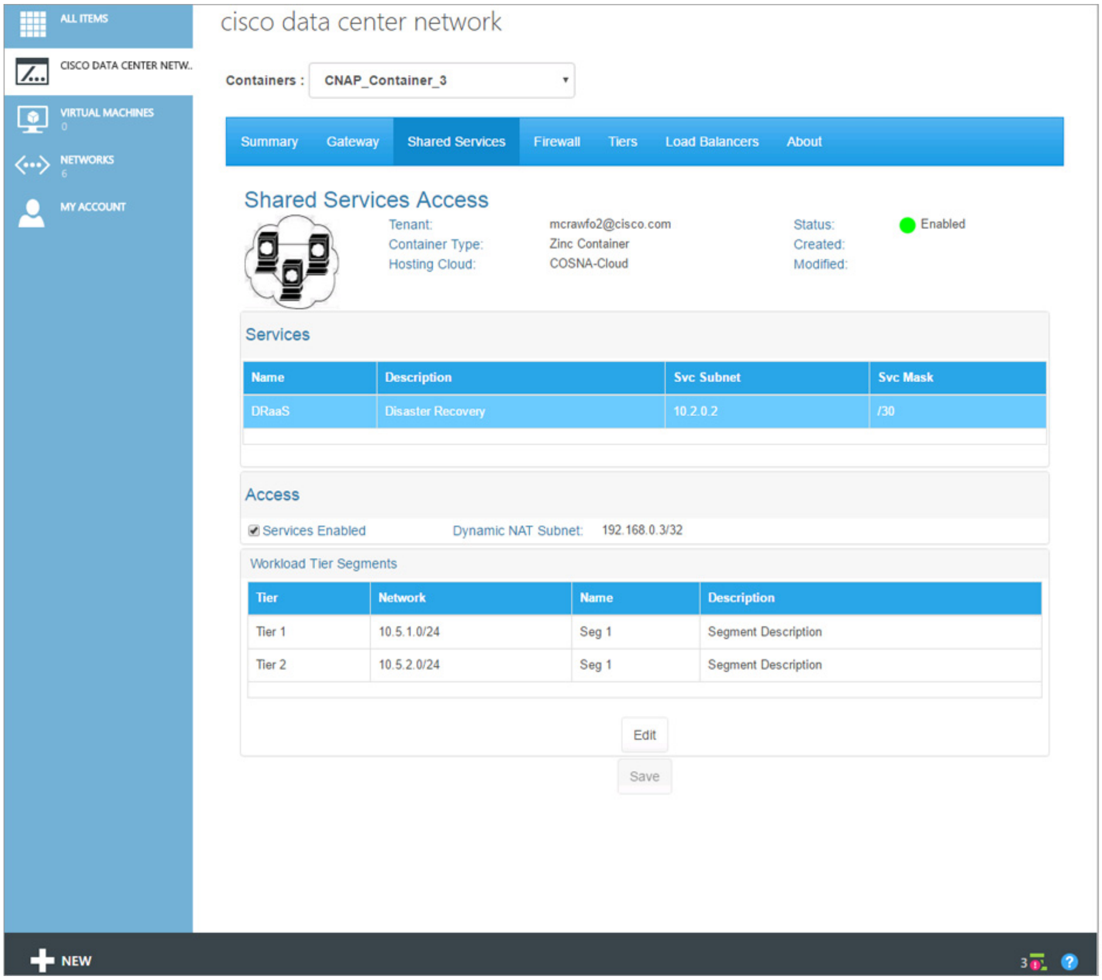
Disabling Access to Shared Services

To disable access to Shared Services:

Step 1 Click the **Shared Services** tab.

You see the following screen, which lists the available Shared Services.

Figure 2-20 Access to Shared Services



Containers : CNAP_Container_3

Shared Services Access

Tenant: mcrawfo2@cisco.com
Container Type: Zinc Container
Hosting Cloud: COSNA-Cloud
Status: ● Enabled
Created:
Modified:

Services

Name	Description	Svc Subnet	Svc Mask
DRaaS	Disaster Recovery	10.2.0.2	/30

Access

☑ Services Enabled Dynamic NAT Subnet: 192.168.0.3/32

Workload Tier Segments

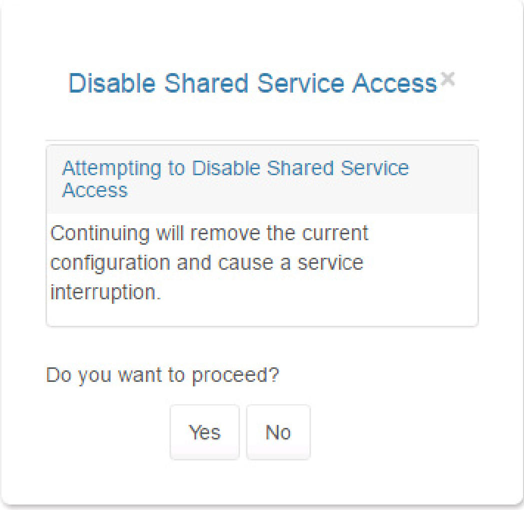
Tier	Network	Name	Description
Tier 1	10.5.1.0/24	Seg 1	Segment Description
Tier 2	10.5.2.0/24	Seg 1	Segment Description

Step 2 You can disable access to Shared Services in two ways:

- Click **Edit**. On the pop-up menu, select the tier segments under Permit Access and use the **<<Unselect** button to move them all to Deny Access, then click **Save**. Also click **Save** on the main Shared Services tab screen.
- On the main Shared Services tab screen, remove the check mark from **Service Enabled**, then click **Save**.

You see the following screen.

Figure 2-21 Confirm Disable Access to Shared Services



Disable Shared Service Access

Attempting to Disable Shared Service Access

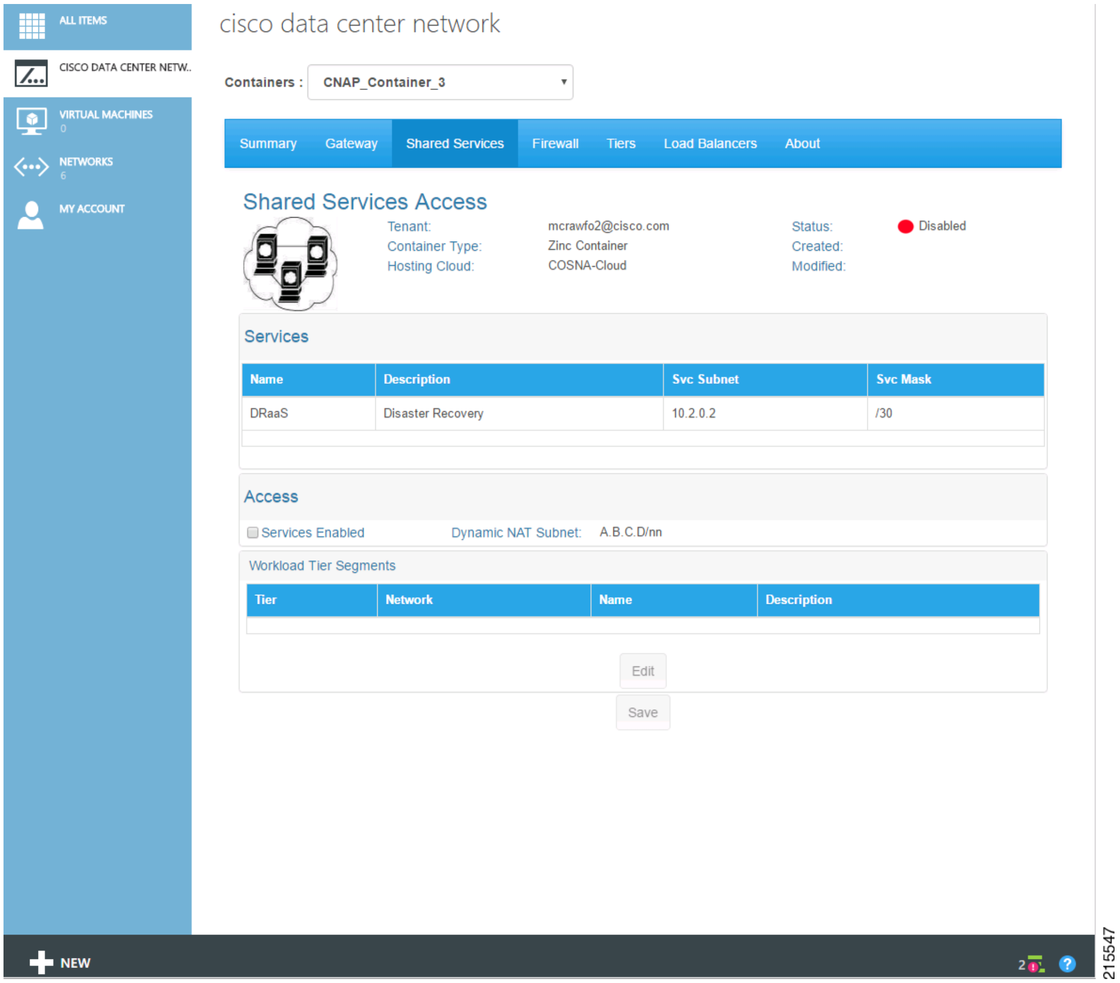
Continuing will remove the current configuration and cause a service interruption.

Do you want to proceed?

Step 3 Click **Yes**.

The configuration takes a few moments. When you refresh the screen, you see that the Status: is now Disabled and the tiers no longer display under Workload Tier Segments, as shown in the following screen.

Figure 2-22 Shared Services Access Disabled



Containers : CNAP_Container_3

Shared Services Access

Tenant: mcrawfo2@cisco.com

Container Type: Zinc Container

Hosting Cloud: COSNA-Cloud

Status: ● Disabled

Created:

Modified:

Services

Name	Description	Svc Subnet	Svc Mask
DRaaS	Disaster Recovery	10.2.0.2	/30

Access

□ Services Enabled Dynamic NAT Subnet: A.B.C.D/nn

Workload Tier Segments

Tier	Network	Name	Description

Viewing and Modifying Firewall Information about a Container

On the Firewall tab, you can:

- View summary information about a firewall
- View the hierarchy of information on the Firewall tab
- Configure a firewall
- Change the policy map for a service policy
- Add a new class map
- Change a class map
- Create a new network ACL
- Change an ACL
- Create a new object group

- Change an object group

Understanding Firewall Creation

A firewall is created by default the moment your cloud provider creates a WAN Gateway. Cisco CNAP will automatically set up a perimeter around each of the zones in your container. Each Tier is considered a zone, as is the Layer 3 VPN as well as any other external access such as Site-to-Site VPN, Internet access, etc. The Firewall tab will not display any information until the WAN Gateway has been provisioned, since there is no point in showing how traffic is going to be regulated if you cannot access the container from the "outside".

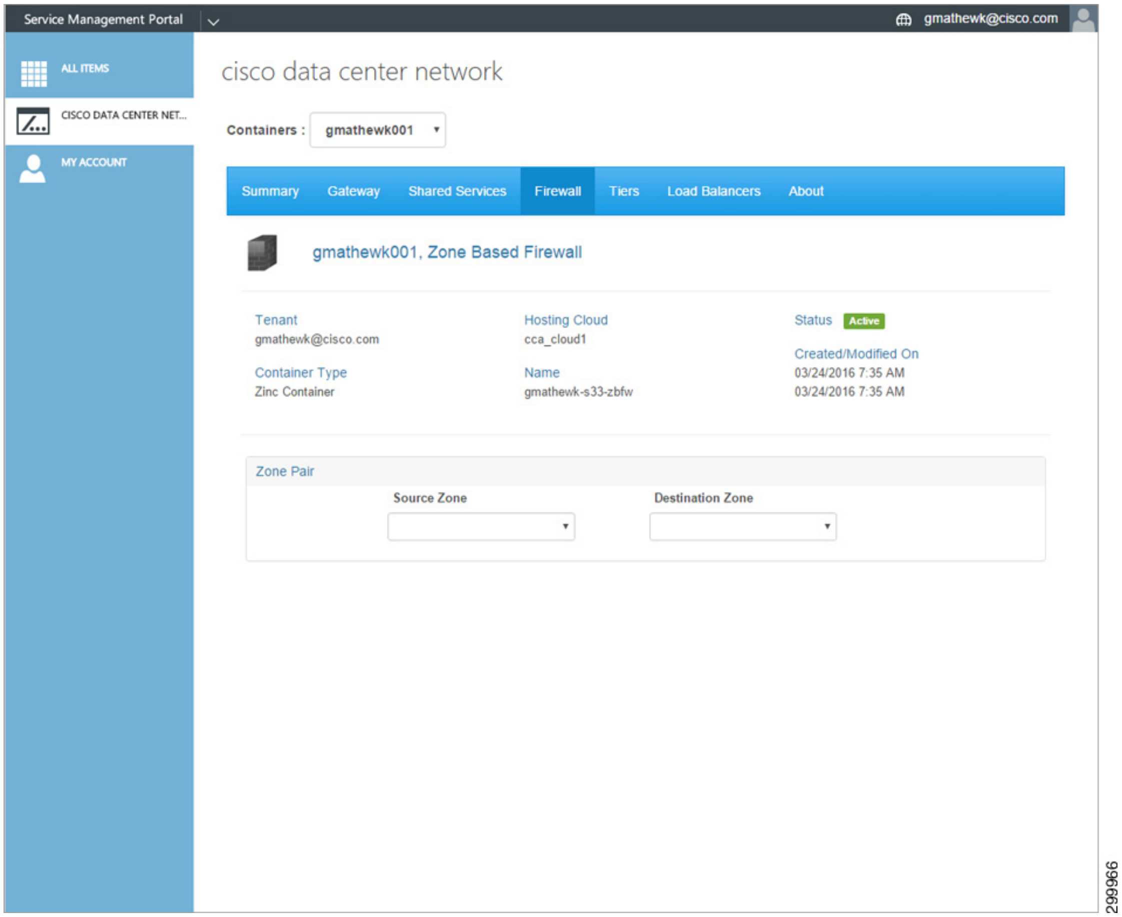
For detailed information on the base firewall configuration, see: *Cisco Cloud Architecture for the Microsoft Cloud Platform: Zinc Container Configuration Guide, Release 1.0* http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/1-0/IaaS_Zinc_Config/CCAMCP1_IaaS_Zinc_Config.html

Viewing Summary Information about a Firewall

Step 1 To view firewall information, click the **Firewall** tab.

You see the following screen.

Figure 2-23 Firewall Tab



Containers : gmathewk001

gmathewk001, Zone Based Firewall

Tenant
gmathewk@cisco.com

Container Type
Zinc Container

Hosting Cloud
cca_cloud1

Name
gmathewk-s33-zbfw

Status Active

Created/Modified On
03/24/2016 7:35 AM
03/24/2016 7:35 AM

Zone Pair

Source Zone

Destination Zone

The screen displays the following information:

- Tenant:—Displays the tenant name.
- Container Type:—Displays the container type instance name.
- Hosting Cloud:—Displays the Hosting Cloud name.
- Modified:—Displays the date and time when the firewall was last modified.
- Status:—Displays the firewall status. The icons indicate (icons are only meaningful on initial configuration as status is not routinely monitored):
  - Green—Firewall is Active.
  - Red— Firewall is Inactive.
  - Yellow—Firewall state is Creating.
- Name:—Displays the name in the form <*abbreviation*>-fw.
- Created:—Displays the date and time when the firewall was created.
- Zone Pair—Source Zone and Destination Zone are the zones between which the firewall is configured.

Viewing the Hierarchy of Information on the Firewall Tab

You use the Firewall Tab to view the various layers of information about firewalls, including:

- Service Policy with its associated Policy Map for a particular Source Zone and Destination Zone

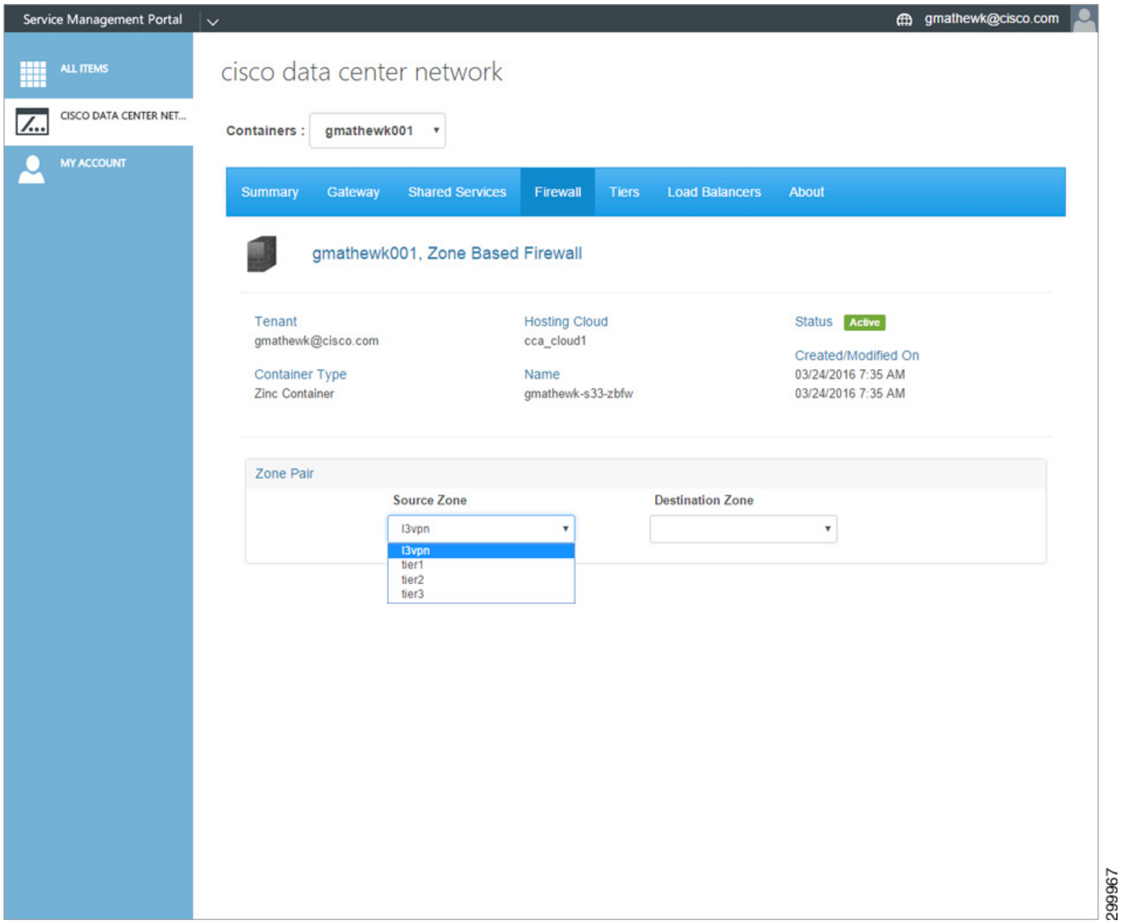
Note To change the Policy Map associated with a Source and Destination Zone pair, you have to define a new Policy Map, which replaces the existing one.

- Class Maps in a Service Policy
- Access Control Lists within a Class Map
- Rules in an Access Control List
- Object Groups of a Rule

To display the various tiers of information about a firewall:

Step 1 Use the Source Zone: and Destination Zone: pull-down menus to select the relevant zones, as shown in the following screens.

Figure 2-24 Firewall Source Zone Pull-down Menu



Containers : gmathewk001

gmathewk001, Zone Based Firewall

Tenant: gmathewk@cisco.com

Hosting Cloud: cca_cloud1

Status: Active

Created/Modified On: 03/24/2016 7:35 AM, 03/24/2016 7:35 AM

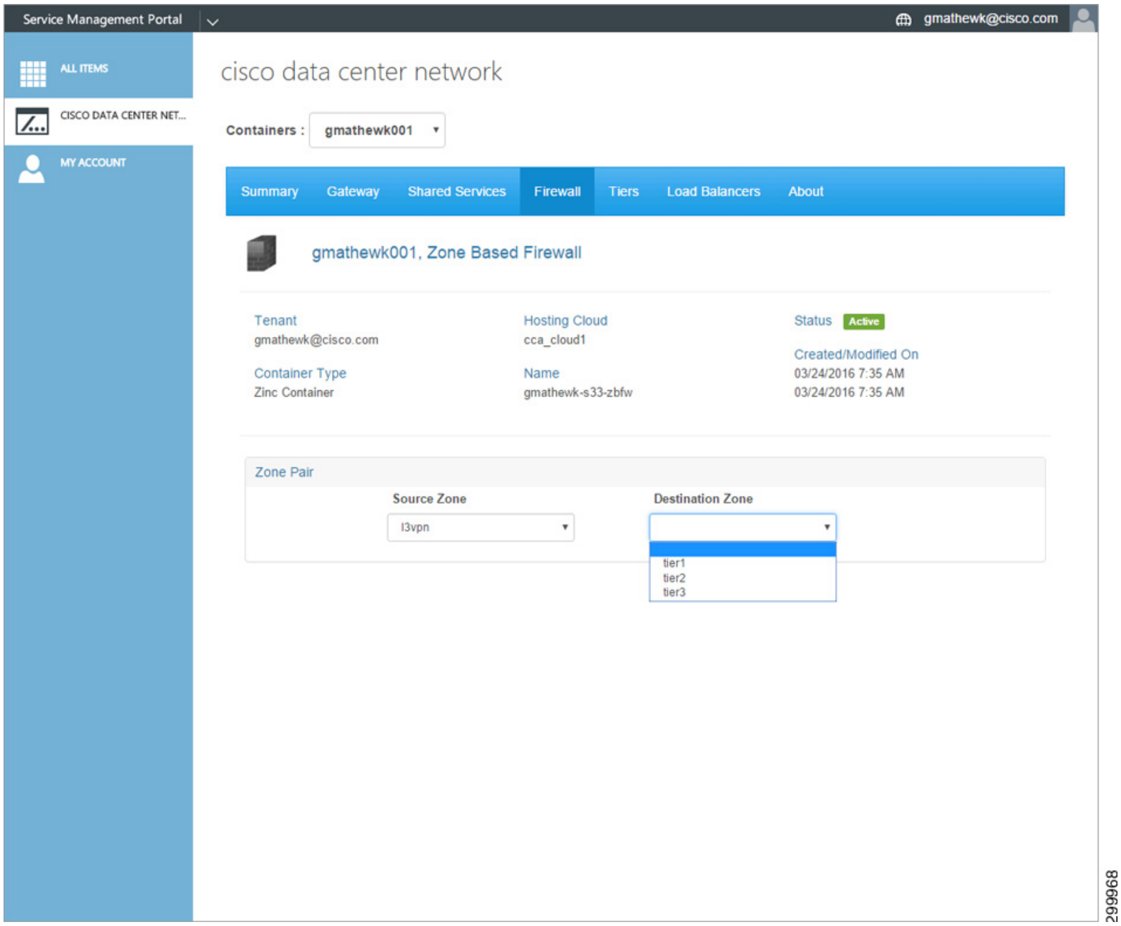
Container Type: Zinc Container

Name: gmathewk-s33-zbfw

Source Zone: l3vpn

Destination Zone:

Figure 2-25 Firewall Destination Zone Pull-down Menu



cisco data center network

Containers : gmathewk001

gmathewk001, Zone Based Firewall

Tenant
gmathewk@cisco.com

Hosting Cloud
cca_cloud1

Status Active

Created/Modified On
03/24/2016 7:35 AM
03/24/2016 7:35 AM

Container Type
Zinc Container

Name
gmathewk-s33-zbfw

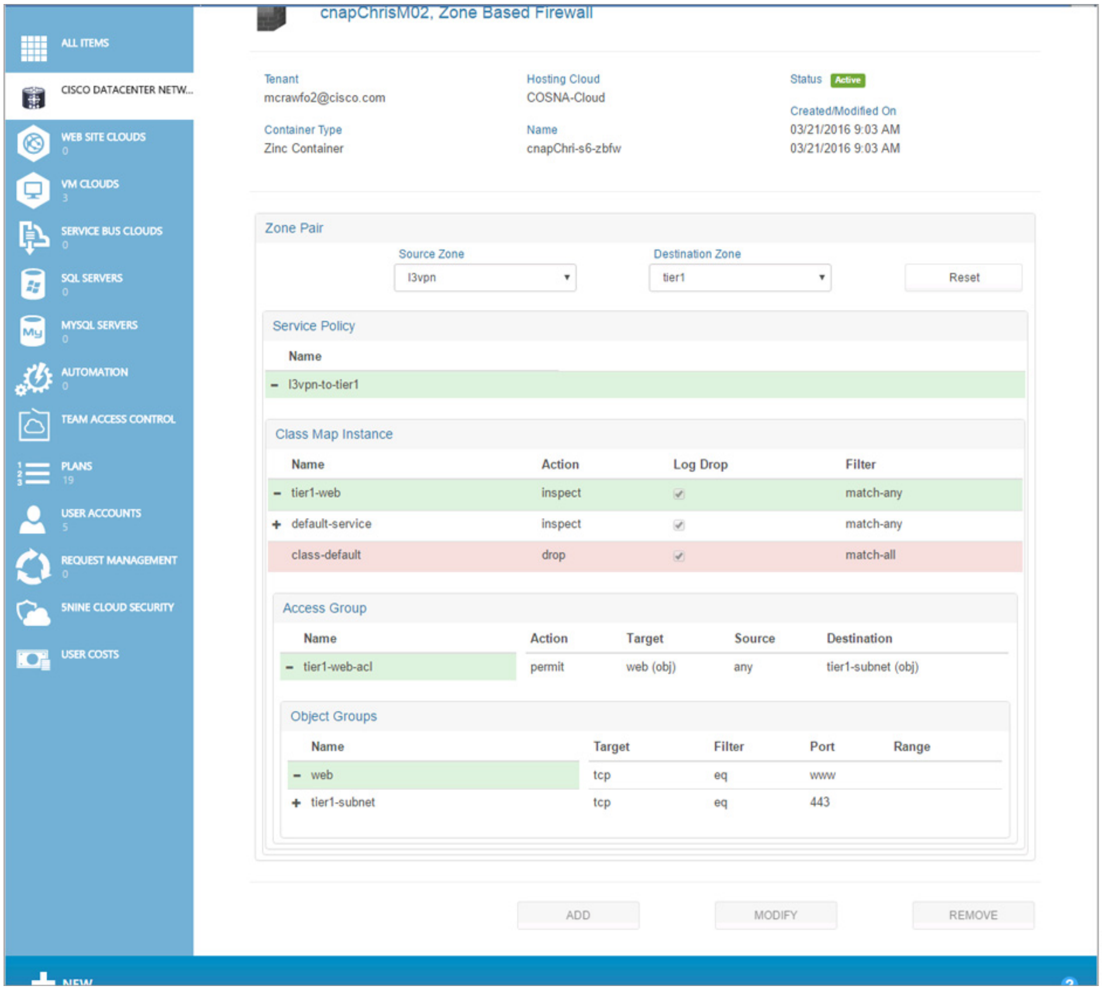
Zone Pair

Source Zone
l3vpn

Destination Zone
tier1
tier2
tier3

After you select the Source and Destination Zones, the screen populates with a variety of information, as shown in the following screen.

Figure 2-26 Firewall Zones Selected Screen—Detailed Firewall Information Displayed



cnapChrisM02, Zone Based Firewall

Tenant mcrawfo2@cisco.com	Hosting Cloud COSNA-Cloud	Status Active
		Created/Modified On
Container Type Zinc Container	Name cnapChri-s6-zbfw	03/21/2016 9:03 AM 03/21/2016 9:03 AM

Zone Pair

Source Zone: l3vpn ▾ Destination Zone: tier1 ▾

Service Policy

	Name
–	l3vpn-to-tier1

Class Map Instance

	Name	Action	Log Drop	Filter
–	tier1-web	inspect	✓	match-any
+	default-service	inspect	✓	match-any
	class-default	drop	✓	match-all

Access Group

	Name	Action	Target	Source	Destination
–	tier1-web-acl	permit	web (obj)	any	tier1-subnet (obj)

Object Groups

	Name	Target	Filter	Port	Range
–	web	tcp	eq	www	
+	tier1-subnet	tcp	eq	443	

The various operations you can perform on this screen are described in the following section, Configuring a Firewall.

Step 2 If you click an element on the screen to bring it into focus, it changes to blue. For the element in focus:

- The **Remove** button de-couples the entity in focus, for example the Class Map Instance tier1-web, from the parent entity marked, for example the Policy Map l3vpn-to-tier1 for the Service Policy.

  The **Remove** button may be used to remove a:

  - Class Map Instance from a Policy Map
  - Access List from a Class Map
  - Rule from an Access List

Note In the current release, Cisco CNAP allows and requires you to associate only one Policy Map with any given zone pair. Consequently, the **Remove** button is deactivated when you drill down to the Policy Map, but not further.

- The **Modify** button displays the change screen for the element currently in focus.

Configuring a Firewall

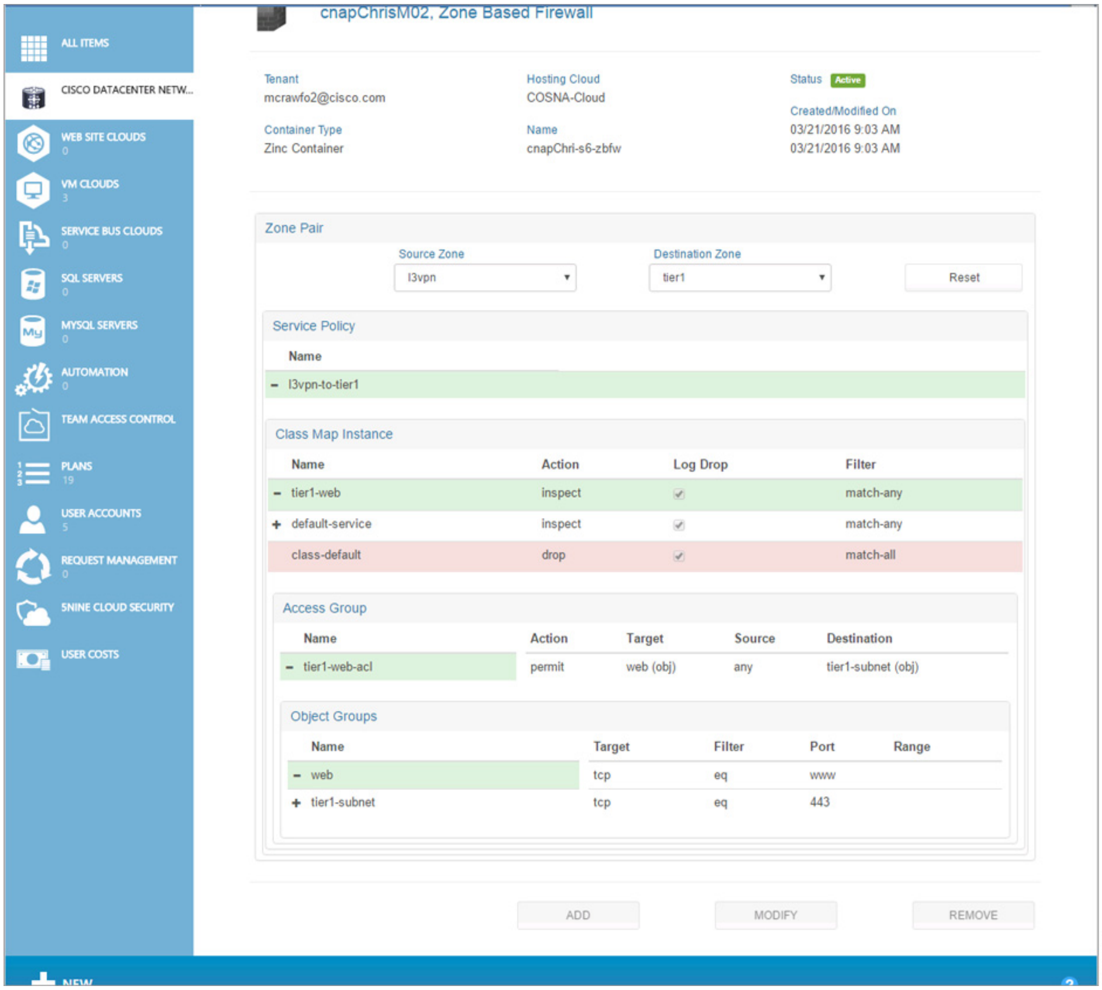
Note You can only configure a firewall after you have created a container and your cloud provider has created a WAN Gateway. The firewall is automatically created with a base configuration either during container creation if the container has multiple tiers or when the WAN gateway is created. For more information, see the section Understanding Firewall Creation.

Firewalls are configurable on a per-Tier basis. You configure one firewall per container (not per tier) and you specify policy rules between zones. Firewall policies are specified between each of the workload Tiers and outside interfaces and in each direction independently. That is, a policy needs to be specified for L3VPN to Tier 1 and Tier 1 to L3VPN, and so on for each tier.

To configure a firewall for a container:

Step 1 Use the Source Zone: and Destination Zone: pull-down menus to select the relevant zones. After you select the zones, the screen populates with a variety of information, as shown in the following screen.

Figure 2-27 Firewall Zones Selected Screen—Detailed Firewall Information Displayed



cnapChrisM02, Zone Based Firewall

Tenant: mcrawfo2@cisco.com

Hosting Cloud: COSNA-Cloud

Status: Active

Container Type: Zinc Container

Name: cnapChri-s6-zbfw

Created/Modified On: 03/21/2016 9:03 AM 03/21/2016 9:03 AM

Zone Pair

Source Zone: l3vpn ▾

Destination Zone: tier1 ▾

Reset

Service Policy

Name
− l3vpn-to-tier1

Class Map Instance

Name	Action	Log Drop	Filter
− tier1-web	inspect	✓	match-any
+ default-service	inspect	✓	match-any
class-default	drop	✓	match-all

Access Group

Name	Action	Target	Source	Destination
− tier1-web-acl	permit	web (obj)	any	tier1-subnet (obj)

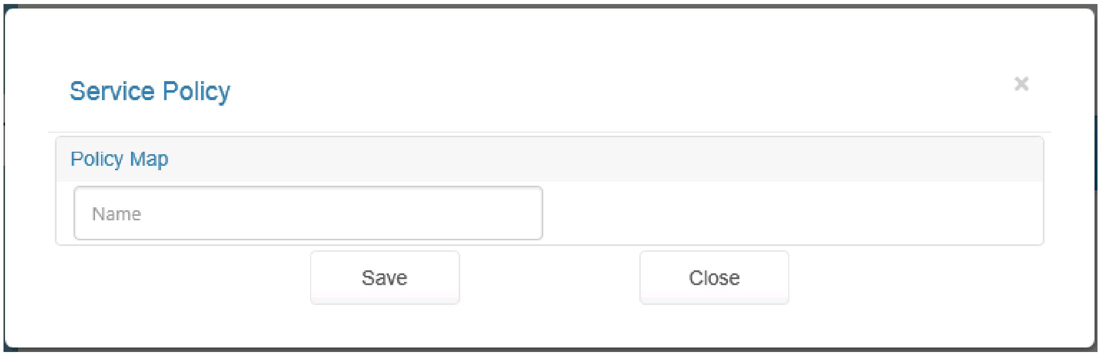
Object Groups

Name	Target	Filter	Port	Range
− web	tcp	eq	www	
+ tier1-subnet	tcp	eq	443	

ADD MODIFY REMOVE

Step 2 To add a Policy Map, click the Policy Map under Service Policy, then click the **Add** button. You see the following screen.

Figure 2-28 Add Policy Map for Service Policy Screen



Service Policy

Policy Map

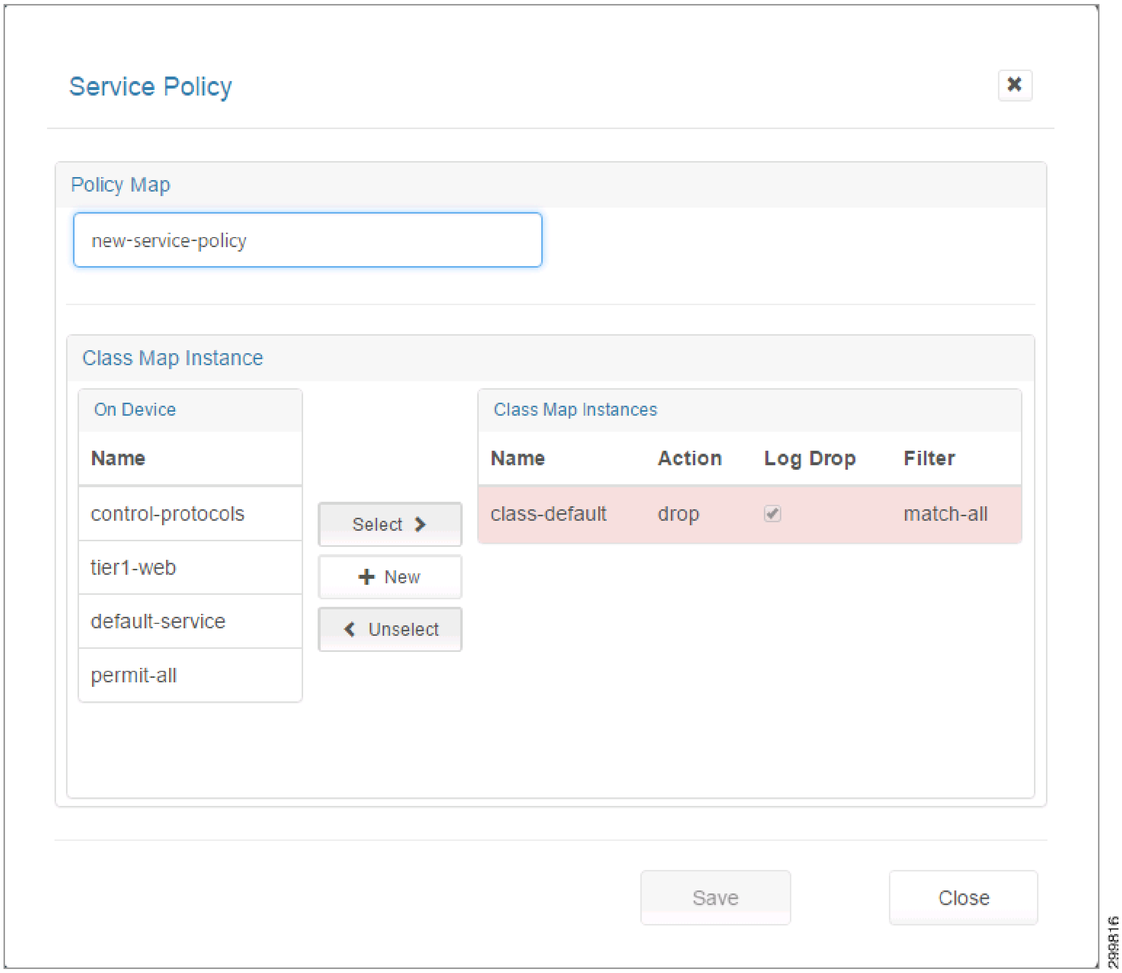
Name

Save Close

Step 3 Enter a name.

As you begin entering a name, the screen expands to display the following screen where you can associate class maps with the new Policy Map.

Figure 2-29 New Policy Map—Class Maps Screen



Service Policy

Policy Map

new-service-policy

Class Map Instance

On Device
Name
control-protocols
tier1-web
default-service
permit-all

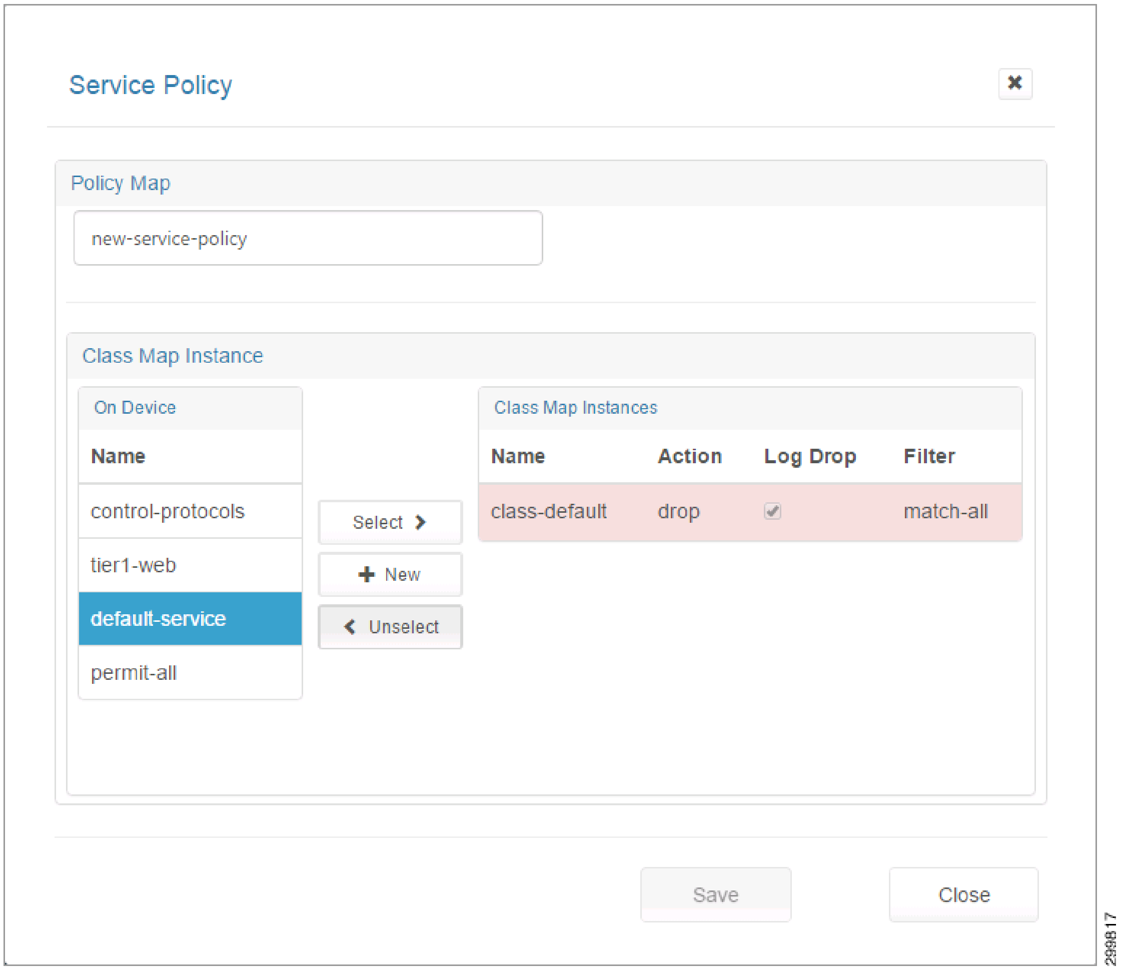
Class Map Instances			
Name	Action	Log Drop	Filter
class-default	drop	☑	match-all

Step 4 Associate class maps with the new Policy Map:

- Name—Enter a descriptive name for the Policy Map.
- On Device—Lists all the Class Maps available on the device.
- Class Map Instances—Lists the class maps associated with this Policy Map.
- **Select>>** button—Click to select one or more Class Maps available "On Device"'. Clicking **Select** associates them to the current Policy Map.
- <<**Unselect** button—Click to select one or more Class Map Instances associated with the current Service Policy. Clicking **Unselect** disassociates them from the current Policy Map.
- +**New** button—Click the +**New** button to create a new Class Map.
- Ordering the Class Maps—The Class Map Instances get added to the top of the list. You can reorder them by clicking <<**Unselect** and **Select**>> on the Class Maps in the desired order.

Note The class-default shown in the following screen cannot be de-coupled from the policy.

Figure 2-30 Class Map Instance class-default Screen



Policy Map

new-service-policy

Name
control-protocols
tier1-web
default-service
permit-all

Class Map Instances

Name	Action	Log Drop	Filter
class-default	drop	☑	match-all

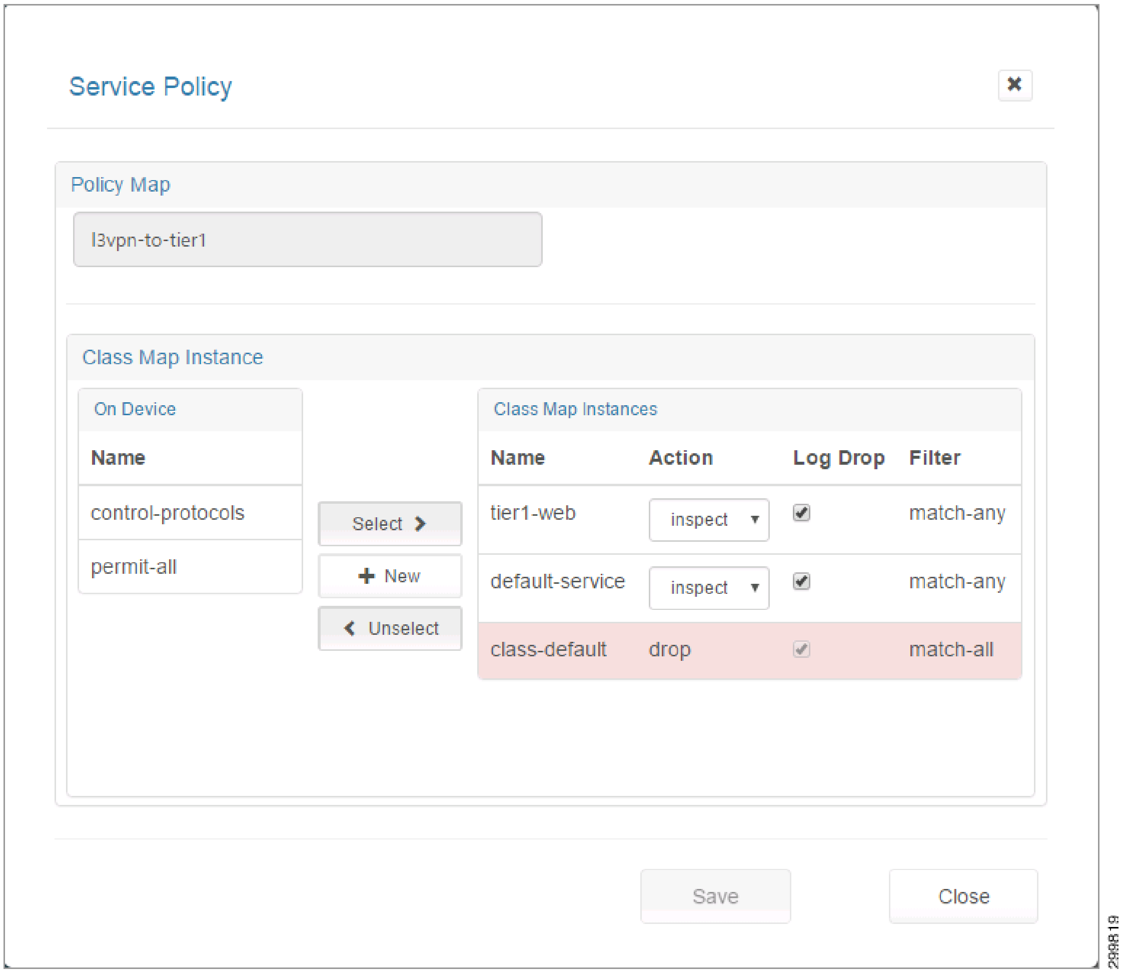
Step 5 When you are finished, click **Save**.

Changing a Policy Map for a Service Policy

Step 1 Click a Policy Map to select it (mark it blue).

Step 2 Click the **Modify** button to display the Policy Map pop-up.

Figure 2-31 Policy Map Pop-up Screen



Policy Map

l3vpn-to-tier1

Class Map Instance

On Device

Name
control-protocols
permit-all

Class Map Instances

Name	Action	Log Drop	Filter
tier1-web	inspect ▾	☑	match-any
default-service	inspect ▾	☑	match-any
class-default	drop	☑	match-all

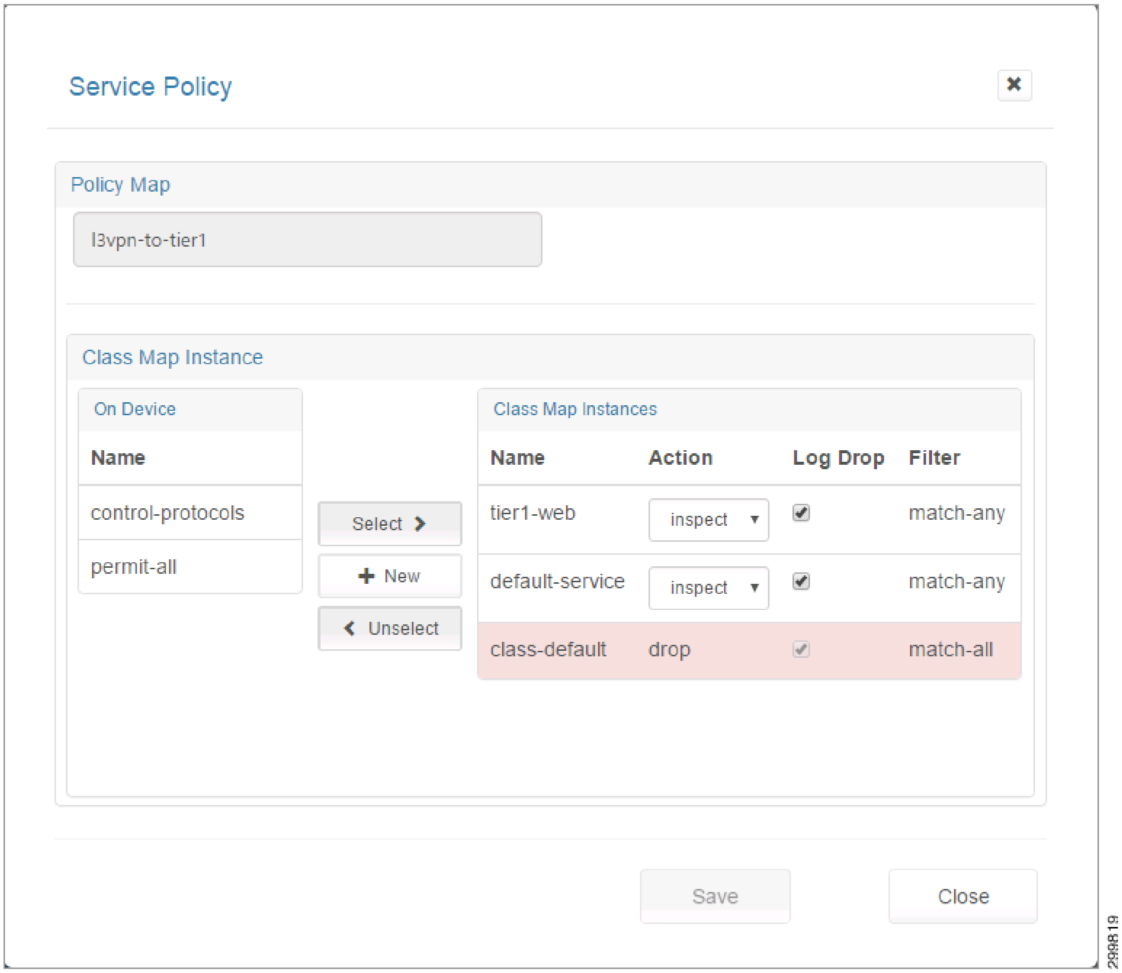
This is the same as the Create Service Policy page, but with the name field deactivated. You can click:

- **Select>>** to select Class Maps available on the device.
- <<**Unselect** to unselect Class Map Instances associated with the Policy Map.
- +**New** to create a new Class Map.

Adding a New Class Map

Step 1 Click +**New** in the Class Map Instance section on the Policy Map screen shown below.

Figure 2-32 Class Map Instance Screen—Click +New



Policy Map

l3vpn-to-tier1

Class Map Instance

On Device

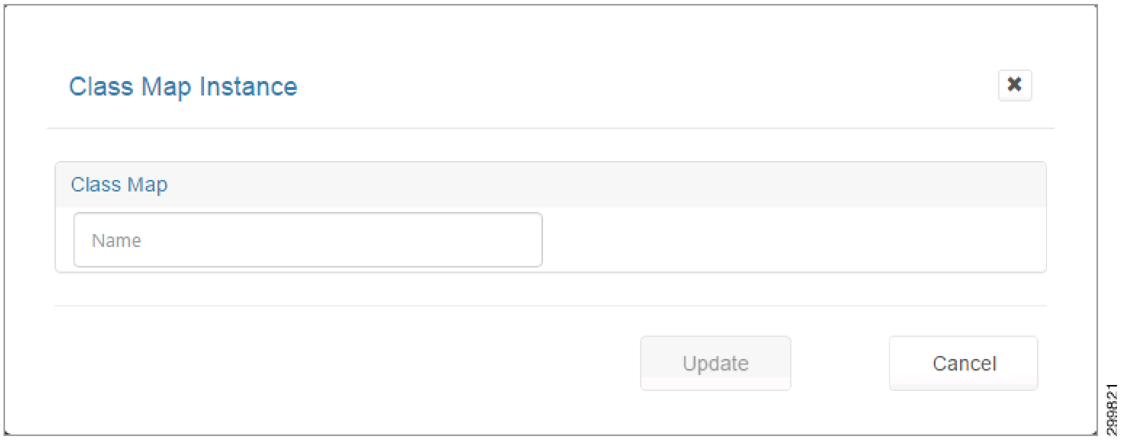
Name
control-protocols
permit-all

Class Map Instances

Name	Action	Log Drop	Filter
tier1-web	inspect ▾	☑	match-any
default-service	inspect ▾	☑	match-any
class-default	drop	☑	match-all

You see the following screen.

Figure 2-33 New Class Map Instance Screen



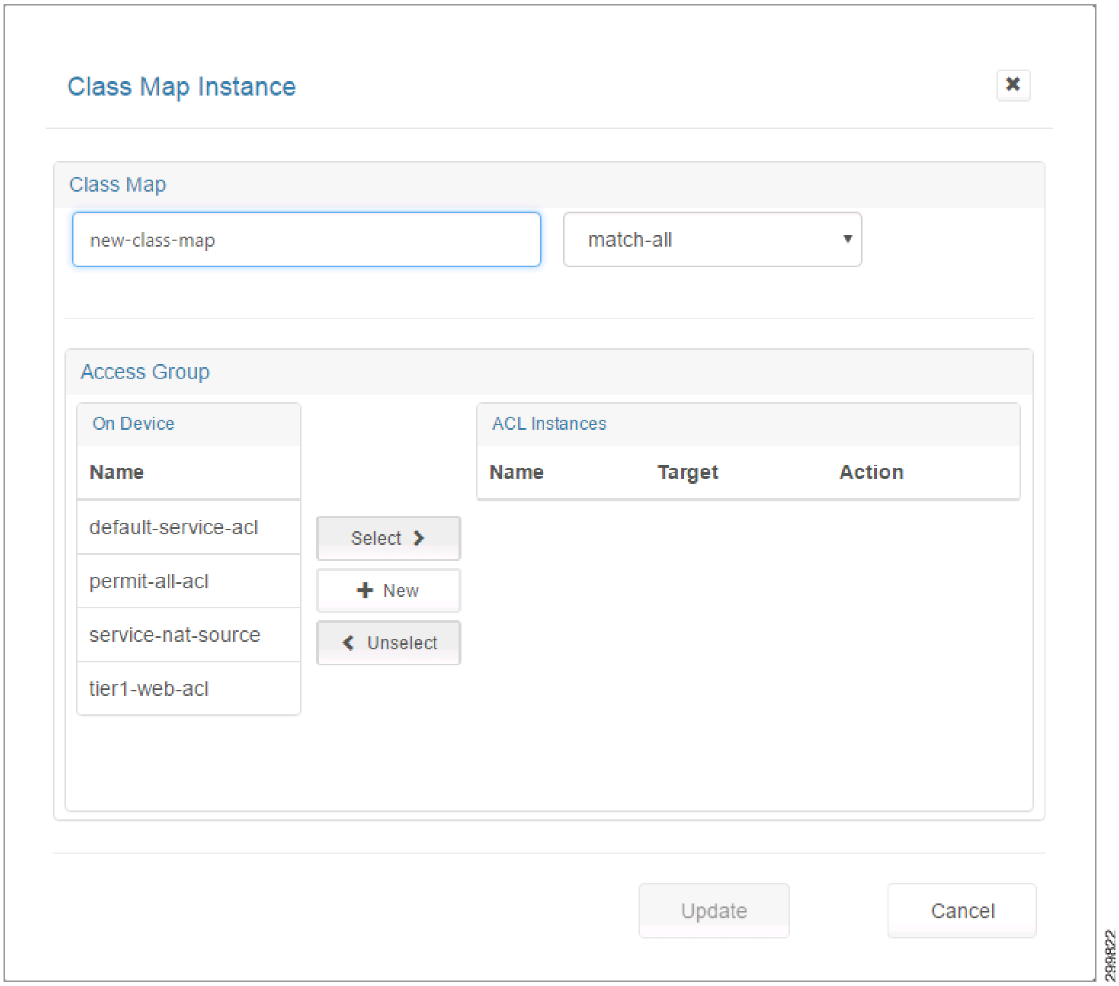
Class Map

Name

Step 2 In the Name field, enter a descriptive name for your new Class Map.

This expands the screen to display the following screen.

Figure 2-34 New Class Map Instance Details Screen



Class Map Instance

Class Map

new-class-map

match-all

Access Group

On Device

Name
default-service-acl
permit-all-acl
service-nat-source
tier1-web-acl

ACL Instances

Name	Target	Action

The fields on this screen are:

- match-all/match-any—This pull-down menu identifies the criteria used to match access groups in the map.
- On Device—Lists all the ACLs available for use on the device.
- ACL Instances—Lists the ACLs associated with this Class Map.
- **Select>>**, +**New**, and <<**Unselect**—These buttons work the same as on the Service Policy screen.

Step 3 When you are finished associating ACLs to this Class Map, click **Update** to return to the Service Policy screen.

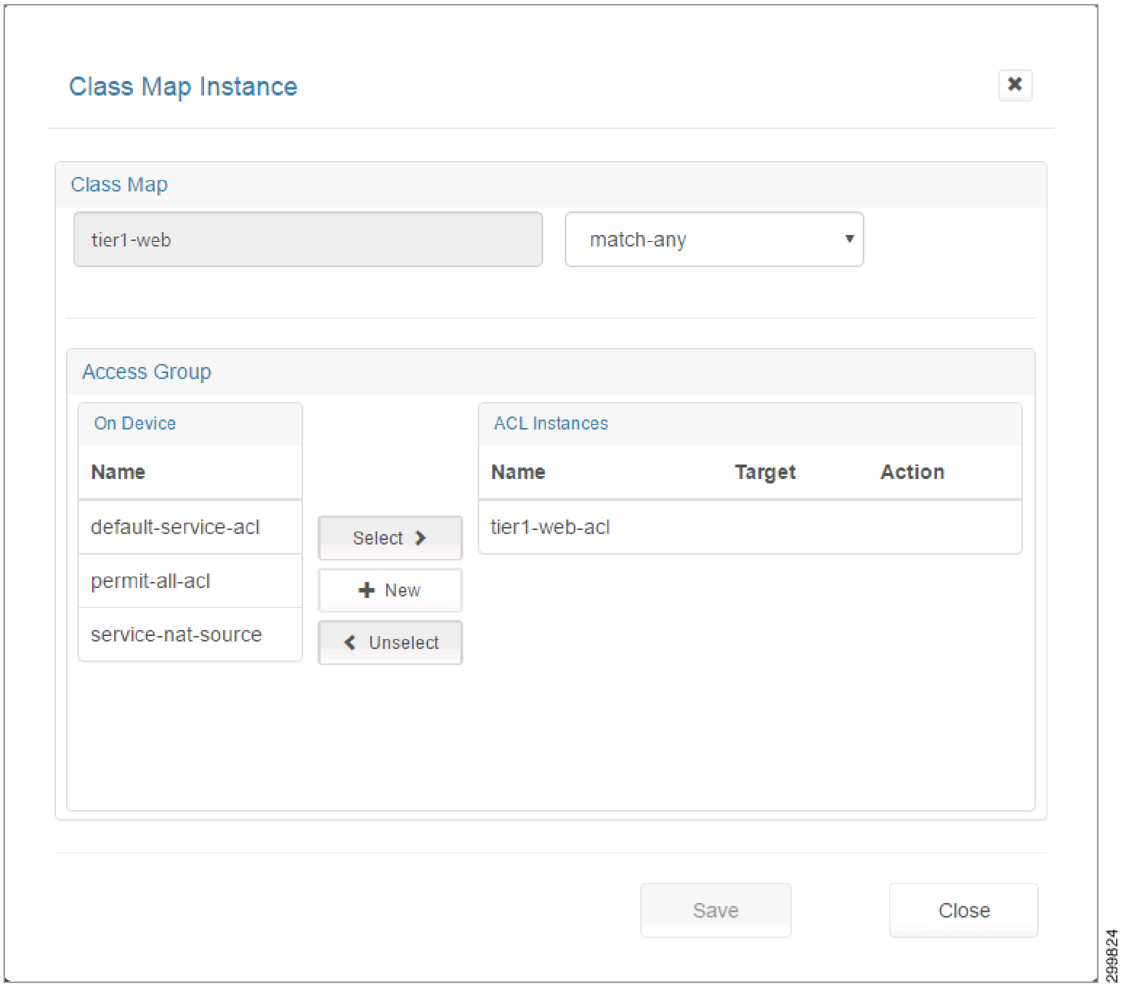
Changing a Class Map

Step 1 Select the desired Class Map on the Firewall tab.

Step 2 Click **Modify**.

You see the following screen.

Figure 2-35 Class Map Instance Screen



Class Map Instance

Class Map

tier1-web | match-any

Access Group

On Device

Name
default-service-acl
permit-all-acl
service-nat-source

ACL Instances

Name	Target	Action
tier1-web-acl		

This screen is identical to the Create Class Map pop up, but with the Name field deactivated.

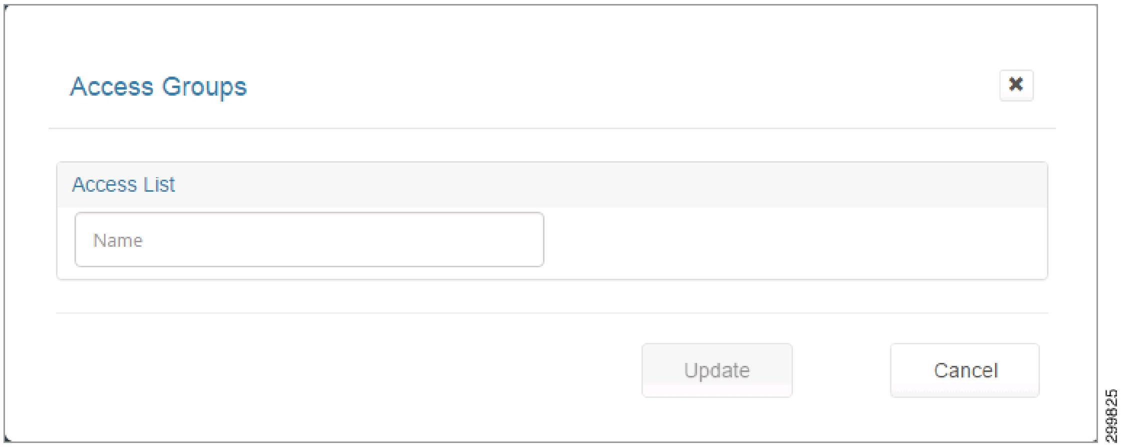
Step 3 You can:

- **Select>>** ACLs from the list of ACLs available on the device.
- <<**Unselect** ACLs associated with the Class Map.
- Create a +**New** ACL on the device and have it associated with the Class Map.

Creating a New Network Access Control List

Step 1 Click **New** on the Class Map Instance screen shown above, which displays the Access Group screen shown below.

Figure 2-36 Access Groups Screen

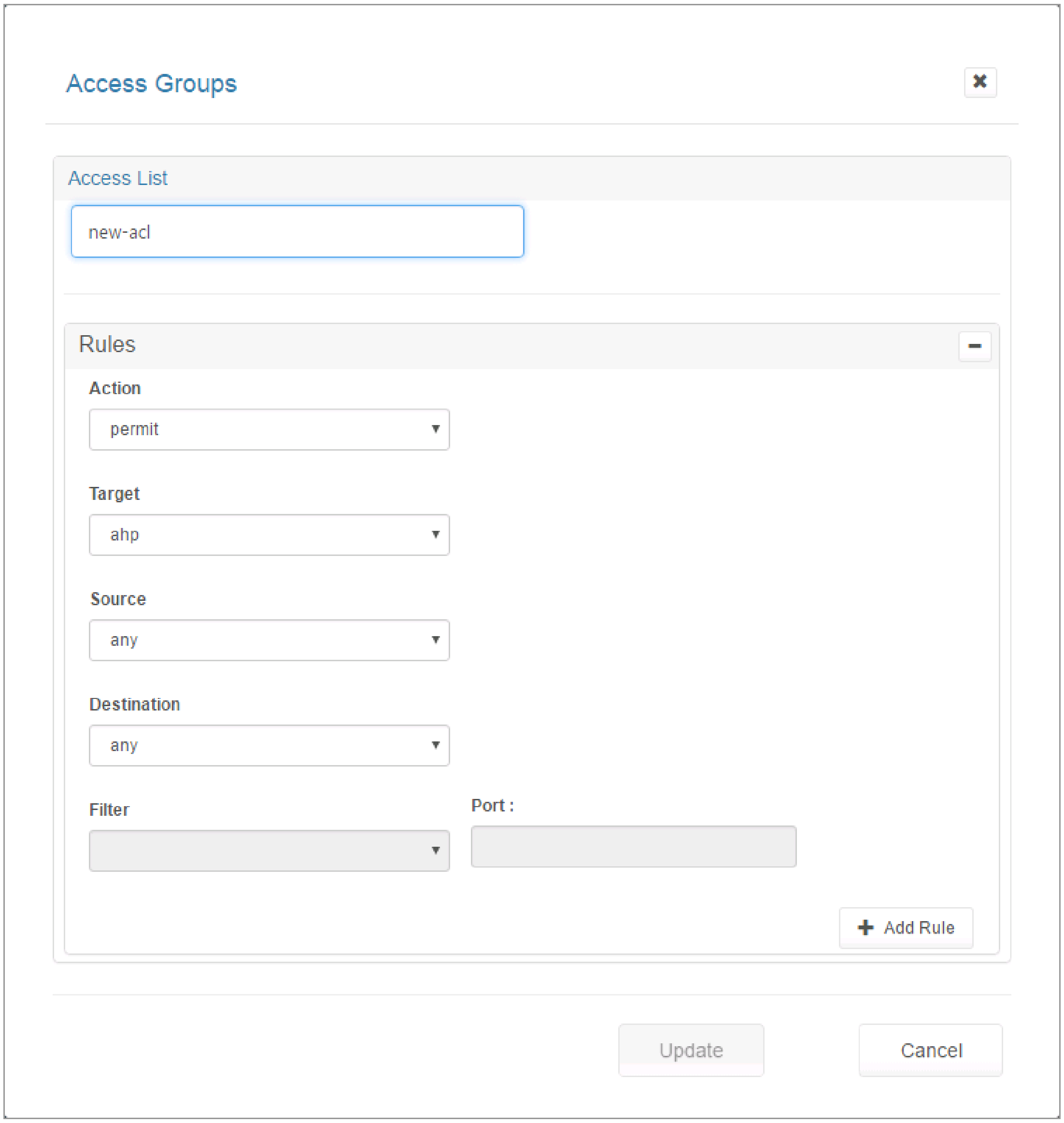


Access Groups

Access List

Step 2 When you enter a name for the Access List, the screen expands to display the Rules section. Since this is a new ACL, the screen expands in the Add Rule mode as shown below.

Figure 2-37 Access Groups Details Screen



Access Groups

Access List

new-acl

Rules

Action

permit

Target

ahp

Source

any

Destination

any

Filter

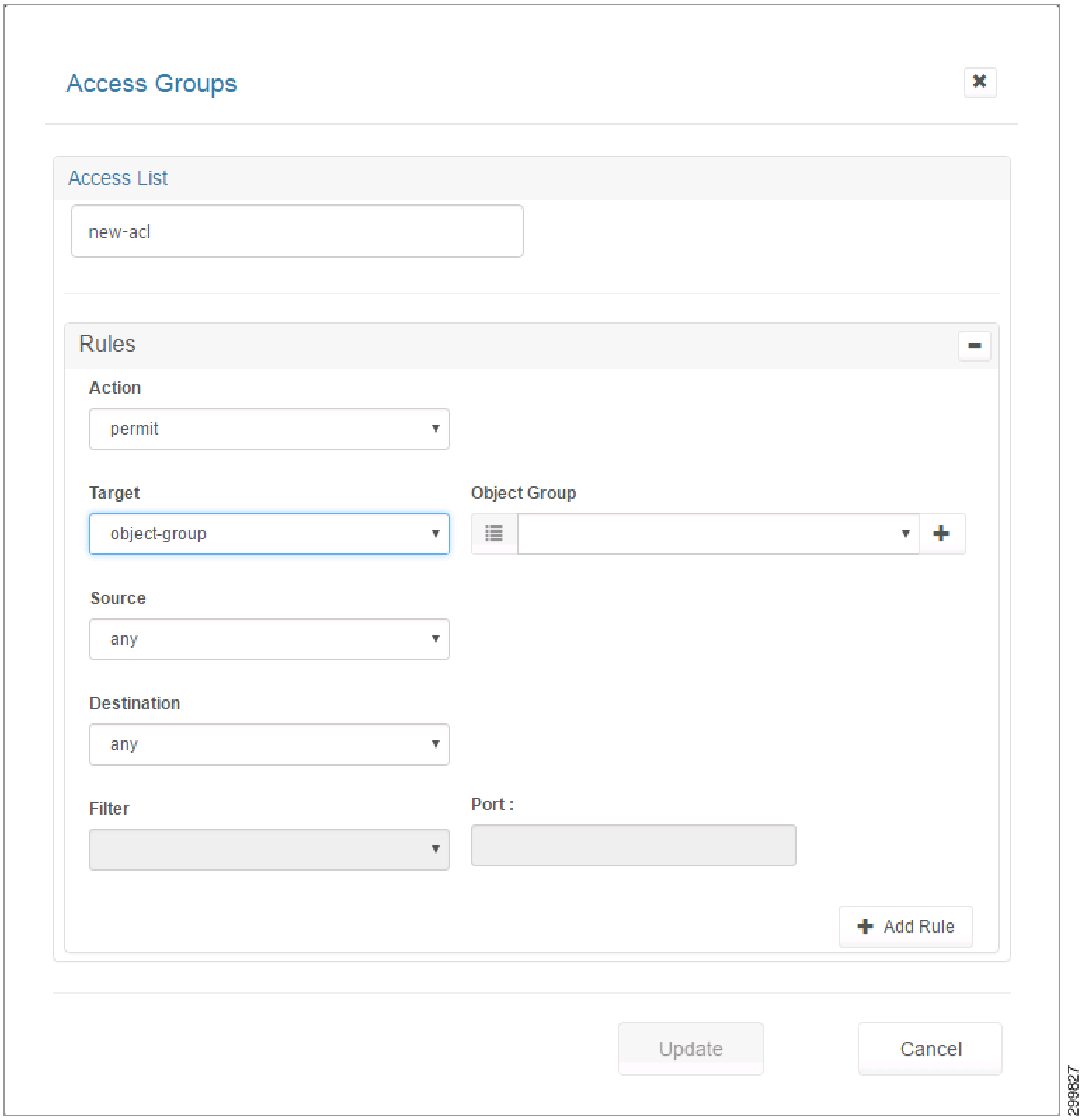
Port :

Step 3 The fields you can complete include:

- Action—Indicates weather traffic is permitted or denied by the rule.
- Target—A valid protocol or object group.
- Source—Network entity identified as the traffic source.
- Destination—Network entity identified as the traffic destination.

Step 4 If you select **Object-Group** in the drop-down menu for Target, the Source or Destination menus allow you to choose from object groups existing on the device or create new ones, as shown in the following screen.

Figure 2-38 Access Groups Screen—Object Group Selected



Access Groups

Access List

new-acl

Rules

Action: permit

Target: object-group

Object Group:

Source: any

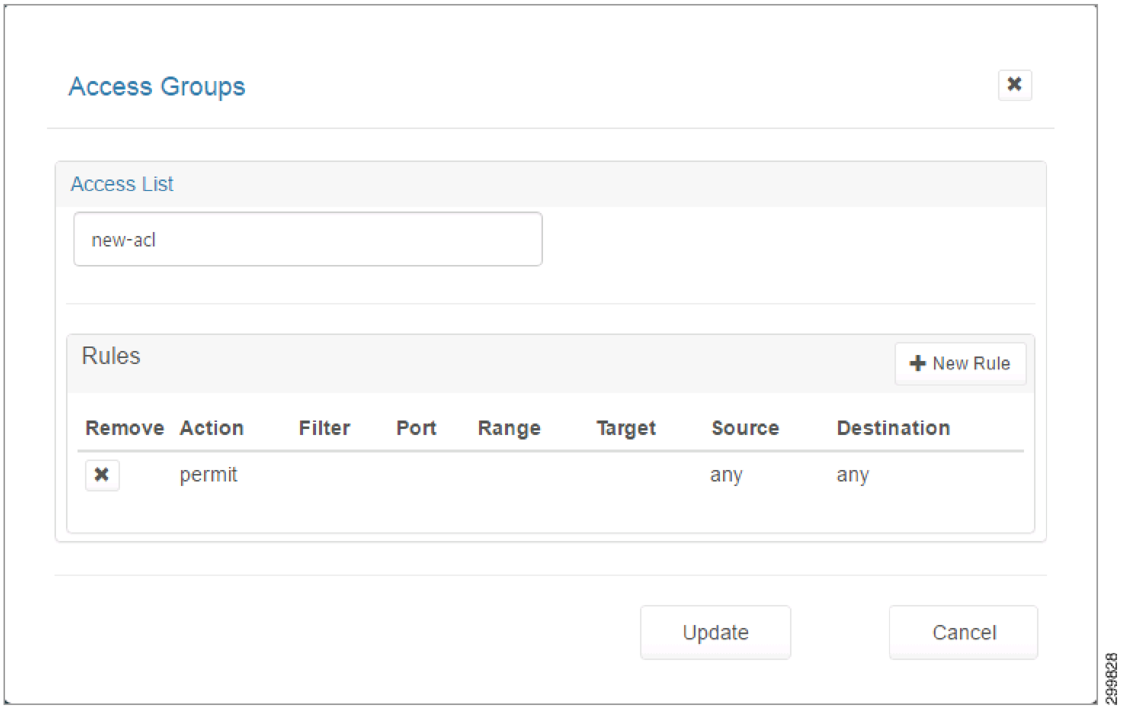
Destination: any

Filter:

Port :

Step 5 Click the **+Add Rule** button to add the current rule being built to the ACL.

Figure 2-39 Rule Added to ACL Screen



Access Groups

Access List: new-acl

Rules

Remove	Action	Filter	Port	Range	Target	Source	Destination
✖	permit					any	any

Step 6 Click **+New Rule** to add more rules.

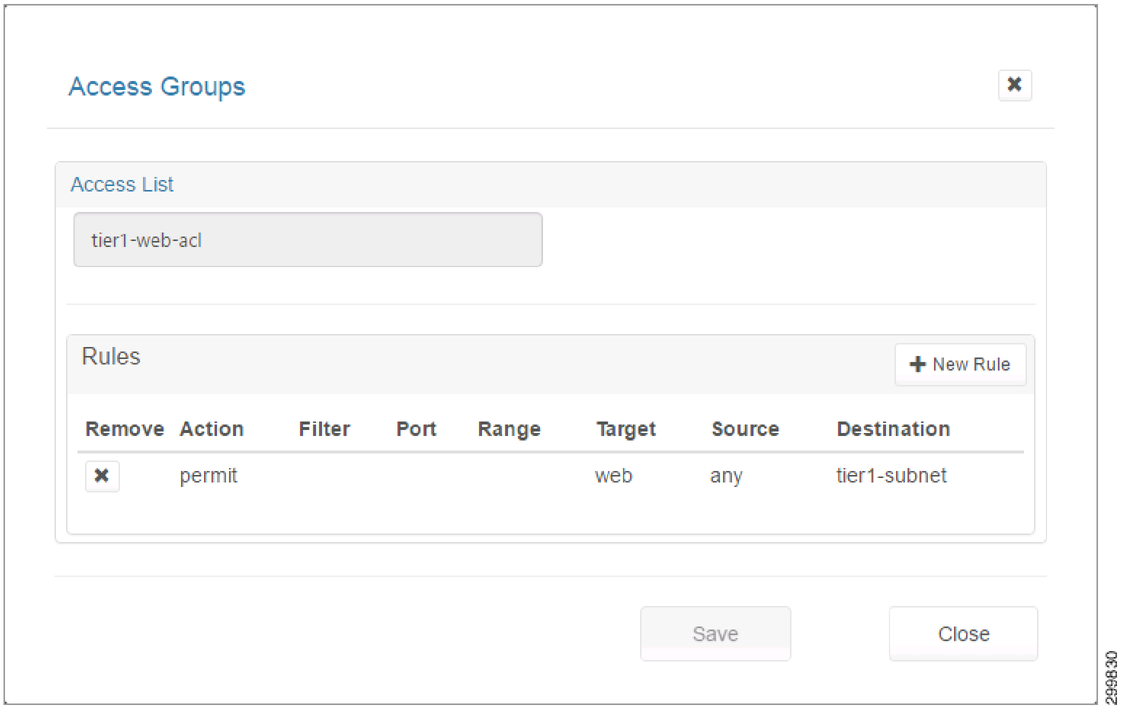
Step 7 Click the **Update** button to exit the Add Rule mode and show the list of all rules in the ACL.

Changing an Access List

Step 1 Select the desired Access List on the Firewall tab.

Step 2 Click **Modify** to display the Access List pop-up screen, as shown below.

Figure 2-40 Access List Pop-up Screen



Access Groups

Access List

tier1-web-acl

Rules

Remove	Action	Filter	Port	Range	Target	Source	Destination
✖	permit				web	any	tier1-subnet

Step 3 You can add and remove rules as explained in Creating a New Network Access Control List.

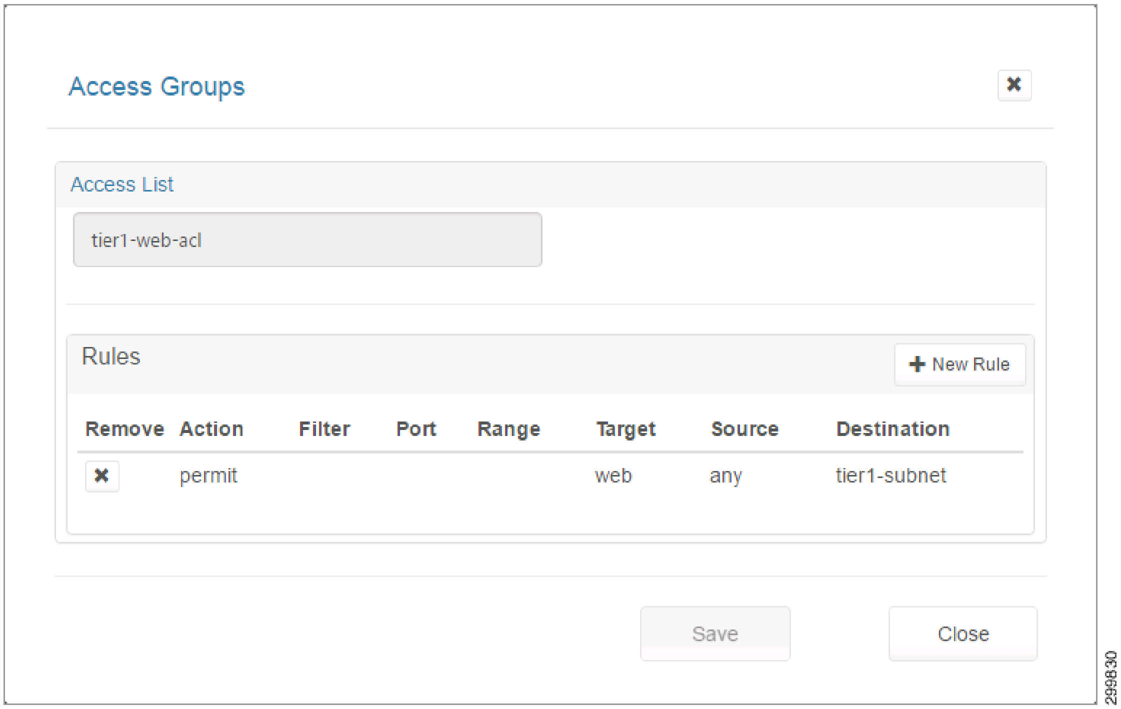
Step 4 If you make any changes to the list of Rules, the **Save** button is activated and you can click it to save the changes.

Creating a New Object Group

Step 1 Select the desired Access List on the Firewall tab.

Step 2 Click **Modify** to display the Access List pop-up screen, as shown in the following screen.

Figure 2-41 Access List Pop-up Screen



Access Groups

Access List

tier1-web-acl

Rules

Remove	Action	Filter	Port	Range	Target	Source	Destination
✖	permit				web	any	tier1-subnet

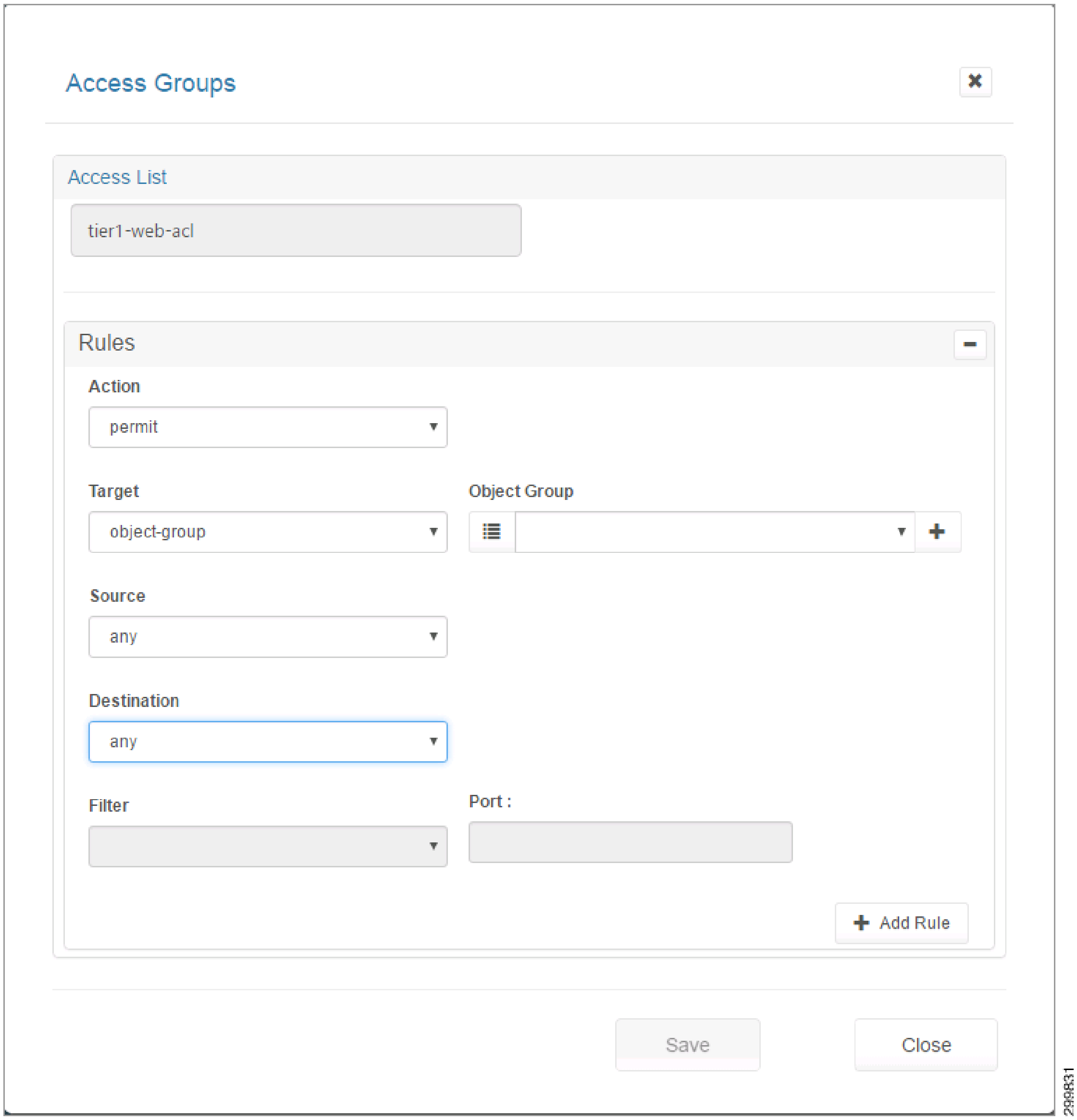
Step 3 Click the **+New Rule** button.

On the Access Groups screen, the **Target**, **Source**, and **Destination** drop-down menus have an **object-group** option which when selected displays the **Object Group:** fields with drop-down menus with a list of *compatible* object groups and + buttons that launch a page where you can create a new compatible Object Group.

- The Object Group drop-down menu for **Target** would only show Service type Object Groups (groups of objects having the Target, filter, and port fields or having the Target and Range fields).
- The Object Group drop down for **Source** and **Destination** would only show Network type Object Groups (groups of objects having a Host field or having the Subnet and mask fields).
- The + buttons are contextual. Clicking the + button for the **Target** of the ACL Rule launches a page to create an Object Group with Service type objects.
- Clicking the + button for the Source or Destination of the ACL Rule launches a page to create an Object Group with Network type objects.

Step 4 Click the + button as shown in the following screen.

Figure 2-42 Access Groups Screen—Object Group Selected



Access Groups

Access List

tier1-web-acl

Rules

Action: permit

Target: object-group

Object Group:

Source: any

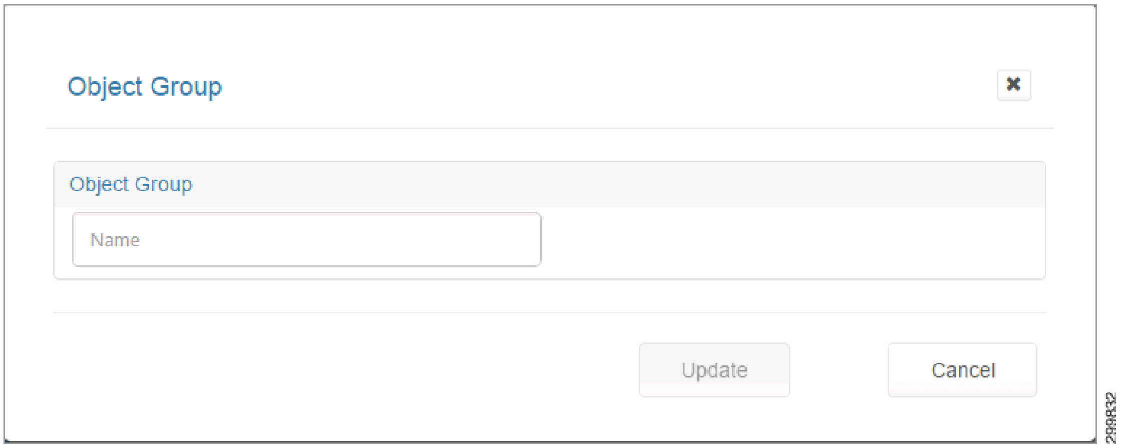
Destination: any

Filter:

Port :

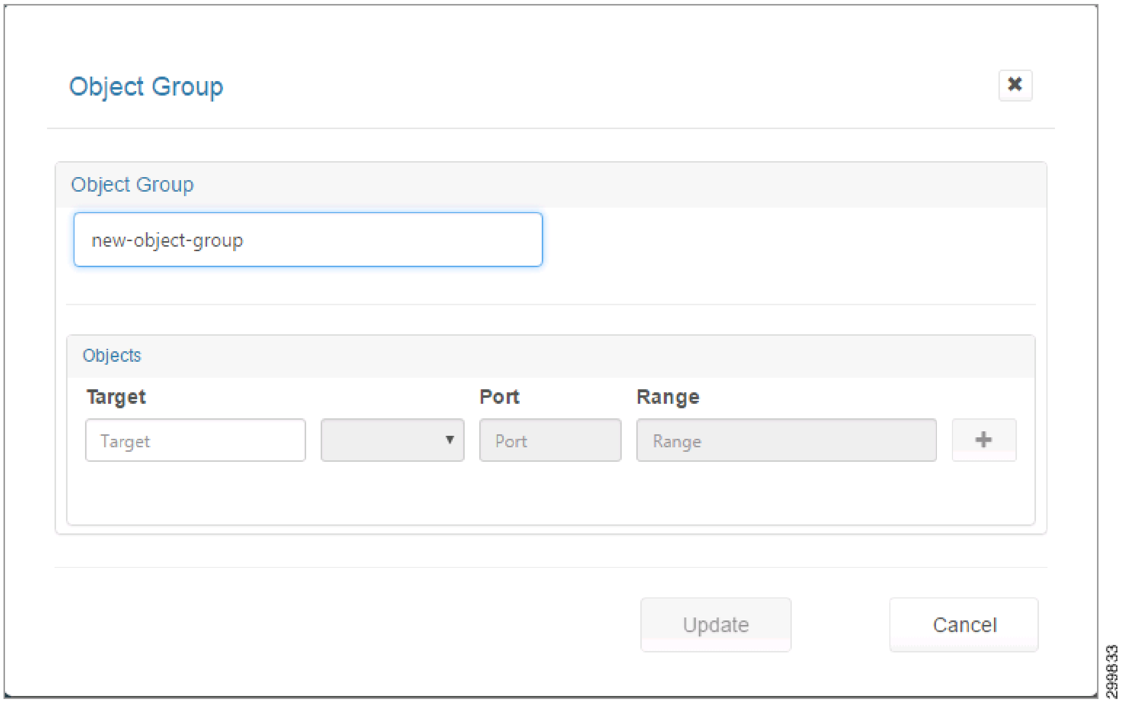
You see the following screen.

Figure 2-43 Object Group Screen



Step 5 When you enter a name, you see the Add Object screen, as shown below.

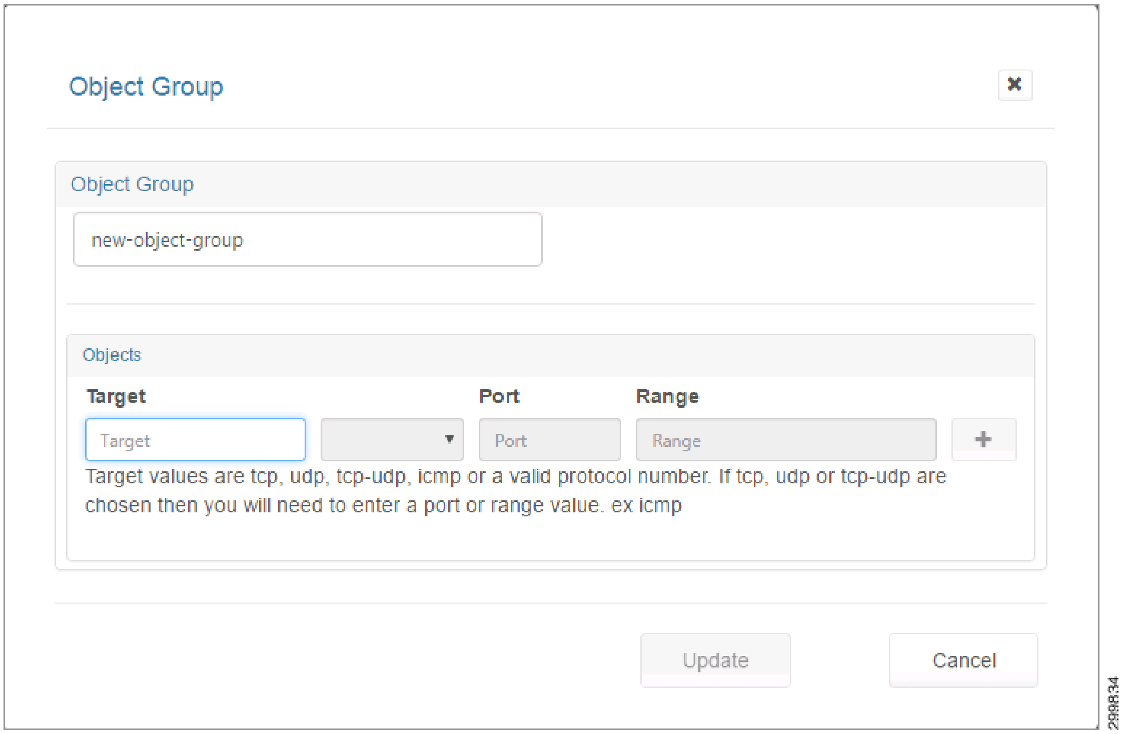
Figure 2-44 Add Object Screen



Object Group: new-object-group

Step 6 When you click a field, you see information about allowable values, as shown in the following screen.

Figure 2-45 Add Object Screen—Possible Field Values Displayed



new-object-group

Target values are tcp, udp, tcp-udp, icmp or a valid protocol number. If tcp, udp or tcp-udp are chosen then you will need to enter a port or range value. ex icmp

Step 7 You can enter information for the following fields:

- Target—A valid protocol {ahp, esp, gre, icmp, ip, tcp, udp, number [0,255]}.
- Filter—eq (equals), gt (greater than), or lt (less than). The Filter indicates the criteria to match packets based on the port number. If “filter” is present, then “port” **must** be present.
- Port—IP port [0,65535]
- Range—*<port-number1>*-*<port-number2>*. Must be entered from low to high, e.g., 20-90. Match only packets in the range of the port numbers.

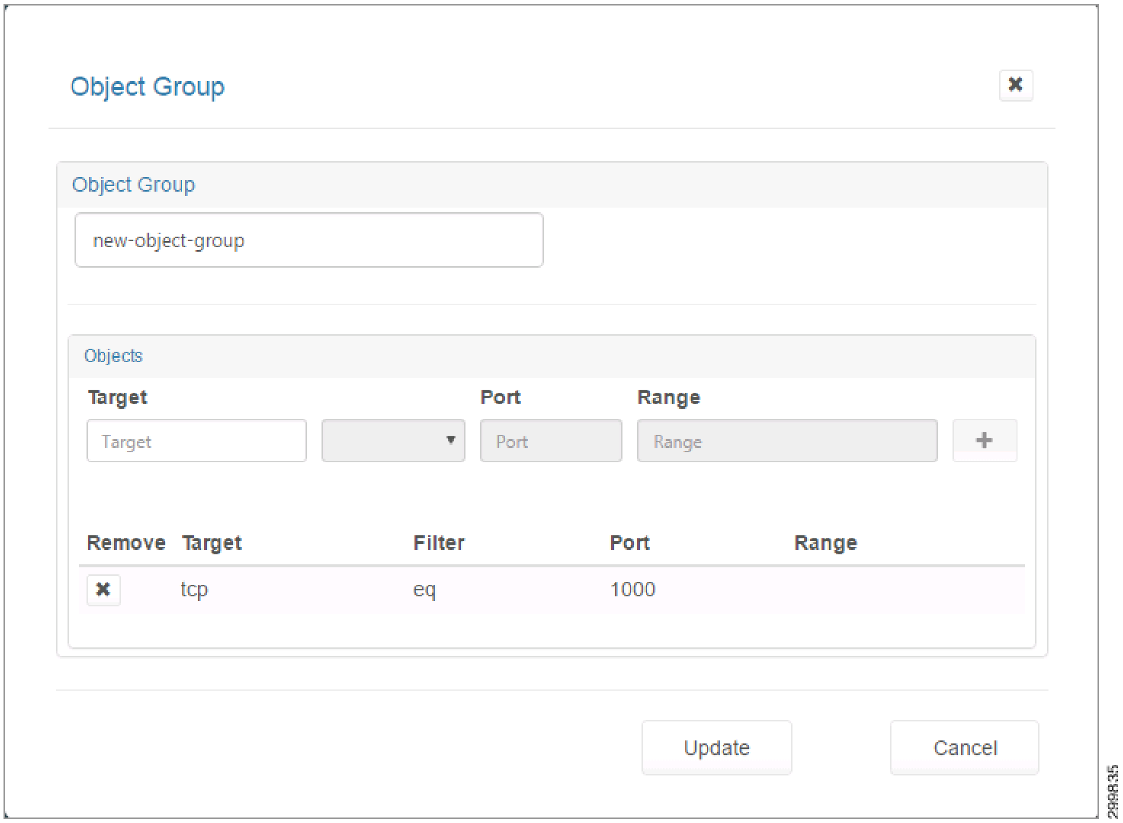
Note If “range” is present, the “filter” and “port” properties are ignored.

Step 8 You can create Network or Service type objects and click + to include the object in the group.

A Group **must** be homogeneous; i.e., it must contain objects of only one type (Network or Service)

Step 9 When you click +, you see the following screen.

Figure 2-46 Object Added to Group Screen



Object Group

new-object-group

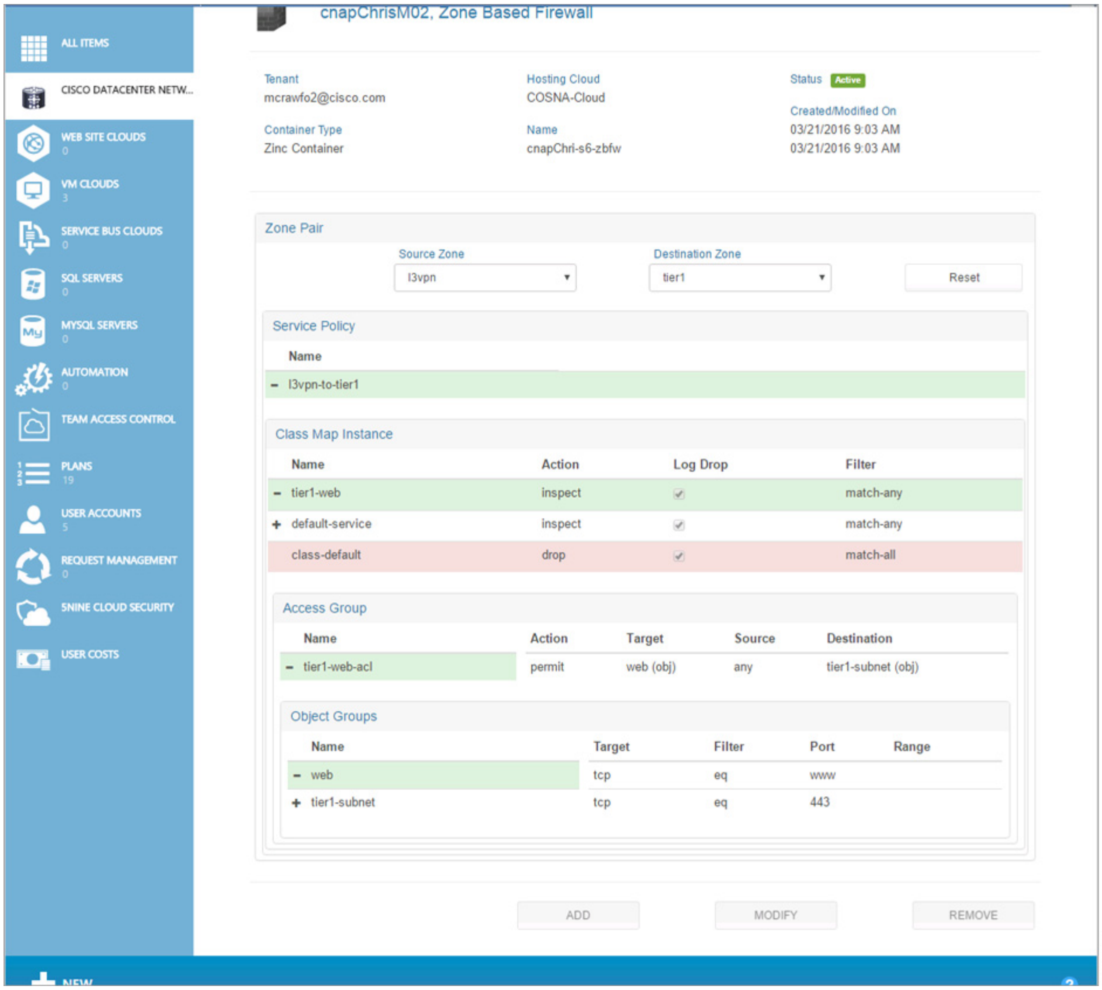
Remove	Target	Filter	Port	Range
✖	tcp	eq	1000	

Step 10 Click the **X** under **Remove** to remove an object from the group.

Changing an Object Group

Step 1 On the screen shown below, select the object group you want to change, then click **Modify**.

Figure 2-47   Firewall Zones Selected Screen—Select Object Group



cnapChrisM02, Zone Based Firewall

Tenant
mcrawfo2@cisco.com

Hosting Cloud
COSNA-Cloud

Status Active

Container Type
Zinc Container

Name
cnapChri-s6-zbfw

Created/Modified On
03/21/2016 9:03 AM
03/21/2016 9:03 AM

Zone Pair

Source Zone: l3vpn ▾

Destination Zone: tier1 ▾

Reset

Service Policy

	Name
−	l3vpn-to-tier1

Class Map Instance

	Name	Action	Log Drop	Filter
−	tier1-web	inspect	✓	match-any
+	default-service	inspect	✓	match-any
	class-default	drop	✓	match-all

Access Group

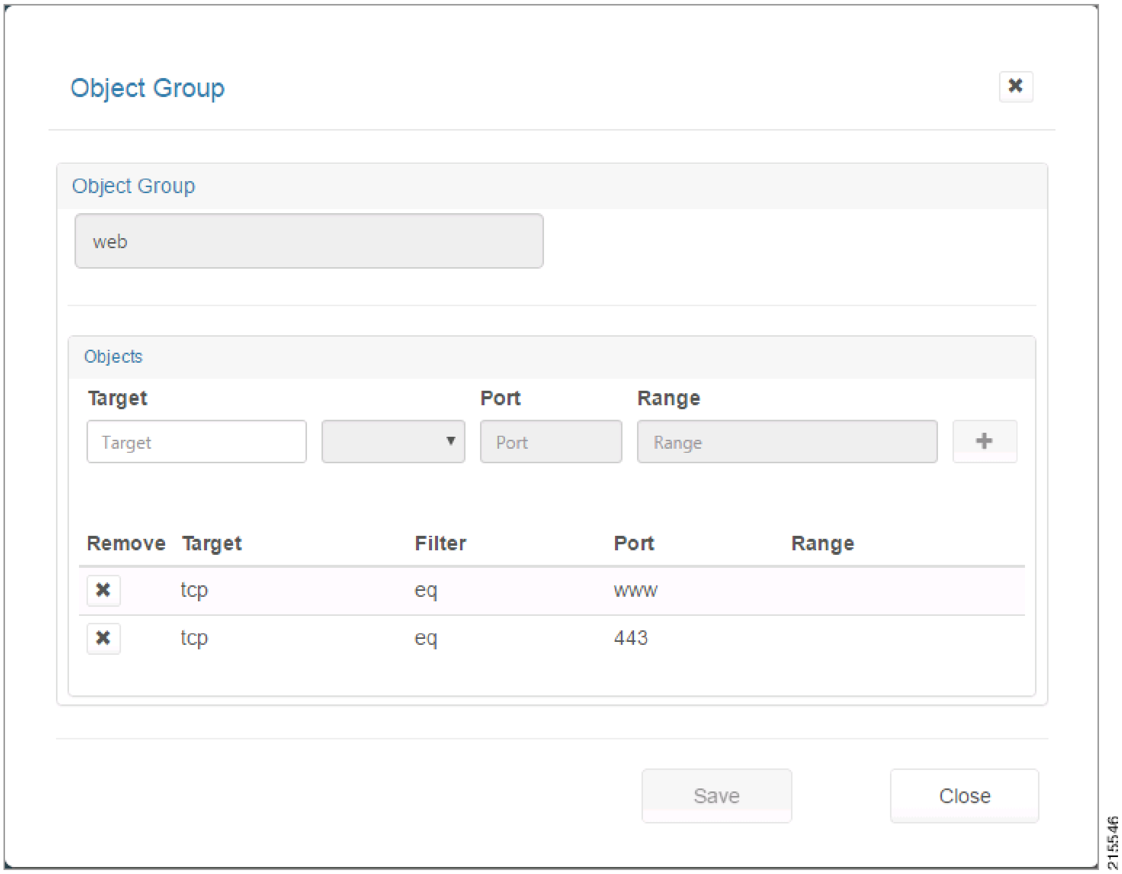
	Name	Action	Target	Source	Destination
−	tier1-web-acl	permit	web (obj)	any	tier1-subnet (obj)

Object Groups

	Name	Target	Filter	Port	Range
−	web	tcp	eq	www	
+	tier1-subnet	tcp	eq	443	

You see the following screen.

Figure 2-48 ***Modify Object Group Screen***



Object Group: web

Remove	Target	Filter	Port	Range
✖	tcp	eq	www	
✖	tcp	eq	443	

Step 2 You can enter information for the following fields:

- Target—A valid protocol {ahp, esp, gre, icmp, ip, tcp, udp, number [0,255]}.
- Filter—eq (equals), gt (greater than), or lt (less than). The Filter indicates the criteria to match packets based on the port number. If “filter” is present, then “port” **must** be present.
- Port—IP port [0,65535]
- Range—<*port-number1*>-<*port-number2*>. Must be entered from low to high, e.g., 20-90. Match only packets in the range of the port numbers.

Note If “range” is present, the “filter” and “port” properties are ignored.

Step 3 You can create Network or Service type objects and click + to include the object in the group.

A Group **must** be homogeneous; i.e., it must contain objects of only one type (Network or Service)

Step 4 When you click +, the object is added to the group. Click the **X** under **Remove** to remove an object from the group. When you are done, click **Save** to save your changes or **Close** to exit without saving them.

Viewing and Modifying Tier Information about a Container

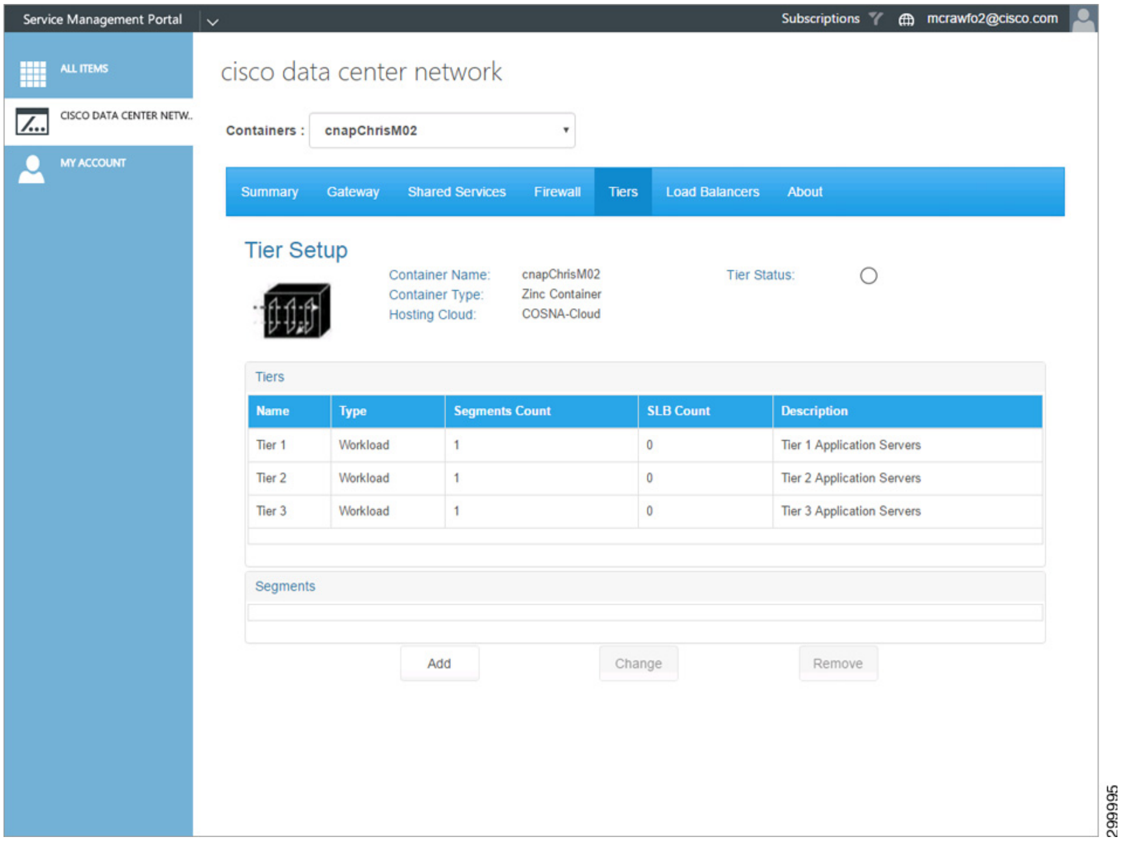
On the Tier tab, you can:

- Add a tier
- Change a tier, including update a segment
- Remove a tier
- Remove a segment

Step 1 To view tier information, click the **Tiers** tab.

You see the following screen.

Figure 2-49 Tiers Tab



Containers : cnapChrisM02

Tier Setup

Container Name: cnapChrisM02

Container Type: Zinc Container

Hosting Cloud: COSNA-Cloud

Tier Status: ○

Tiers

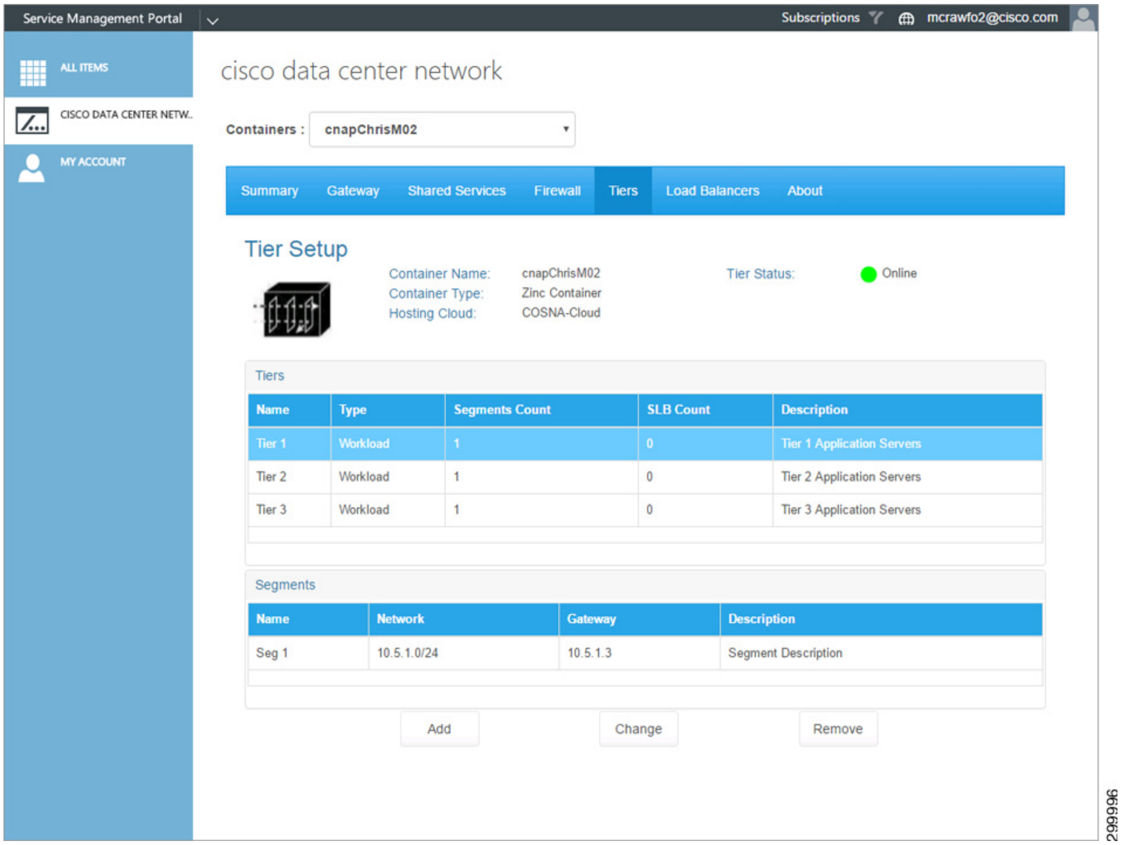
Name	Type	Segments Count	SLB Count	Description
Tier 1	Workload	1	0	Tier 1 Application Servers
Tier 2	Workload	1	0	Tier 2 Application Servers
Tier 3	Workload	1	0	Tier 3 Application Servers

Segments

Step 2 To view segment information about a specific tier, click the tier name.

You see the following screen.

Figure 2-50 Tiers Screen—Tier Selected and Segment(s) Visible



Containers : cnapChrisM02

Tier Setup

Container Name: cnapChrisM02
Container Type: Zinc Container
Hosting Cloud: COSNA-Cloud

Tier Status: ● Online

Tiers

Name	Type	Segments Count	SLB Count	Description
Tier 1	Workload	1	0	Tier 1 Application Servers
Tier 2	Workload	1	0	Tier 2 Application Servers
Tier 3	Workload	1	0	Tier 3 Application Servers

Segments

Name	Network	Gateway	Description
Seg 1	10.5.1.0/24	10.5.1.3	Segment Description

The screen displays the following information:

- Container Name:—Displays the container name.
- Container Type:—Displays the container type instance name.
- Hosting Cloud:—Displays the Hosting Cloud name.
- Name:—Name of the tier.
- Description:—Description of the tier.
- Status:—Displays the Tiers status. The icons indicate (icons are only meaningful on initial configuration as status is not routinely monitored):
  - Green—Tier is Active.
  - Red—Tier is Inactive.
- Num Segments:—The number of segments in the tier.
- Tiers:
  - Name—Name given to the tier. The System assigns Tier <*space*><*number*> during container creation.
  - Type—It specifies the type of container to which the tier belongs.
  - Num Segments—Tiers can contain multiple segments.
  - Num SLB—Number of Server Load Balancers

  - Description—A brief description of the tier (what the user intends to use it for, what services are hosted in it, etc.)
- Segments:
  - Name—Name given to the segment. The System assigns Segment <*space*><*number*> during container creation.
  - Network—The subnet address of this segment.
  - Gateway—The default gateway to access this segment.
  - Description—A brief description of the segment (what the user intends to use it for, what services are hosted in it, etc.).

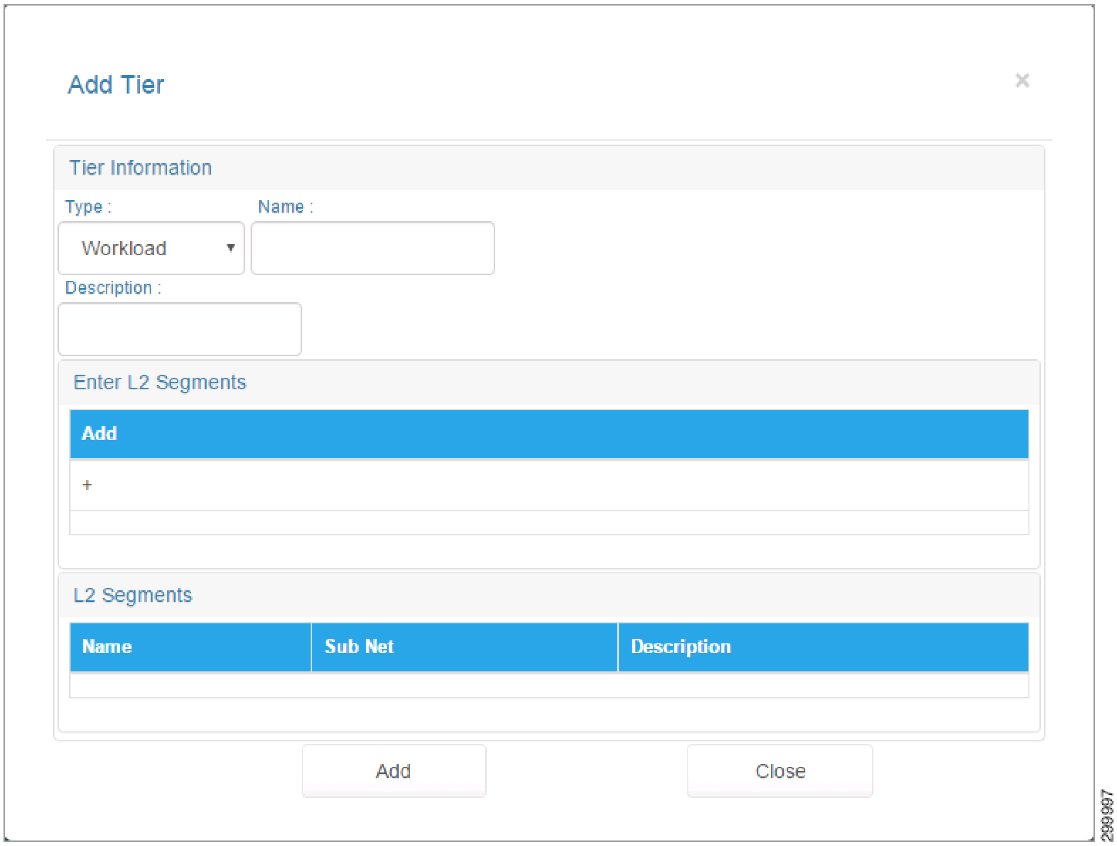
Adding a Tier

To add a tier:

Step 1 On the Tiers Tab screen, click **Add**.

You see the following screen.

Figure 2-51 Add a Tier Screen



Type : Workload

The screen displays the following information:

- Type:—Only Workload is supported in the current release.
- Name:—Enter a name for the tier.
- Description:—Enter a description for the tier.
- Enter L2 Segments—
  - Add—Add a segment. For more information, see the next section.
- L2 Segments—
  - Name—Name of the Layer 2 segment.
  - Sub Net—Subnet of the Layer 2 segment.
  - Description—Description of the Layer 2 segment.

Step 2 When you are finished, click **Add**.

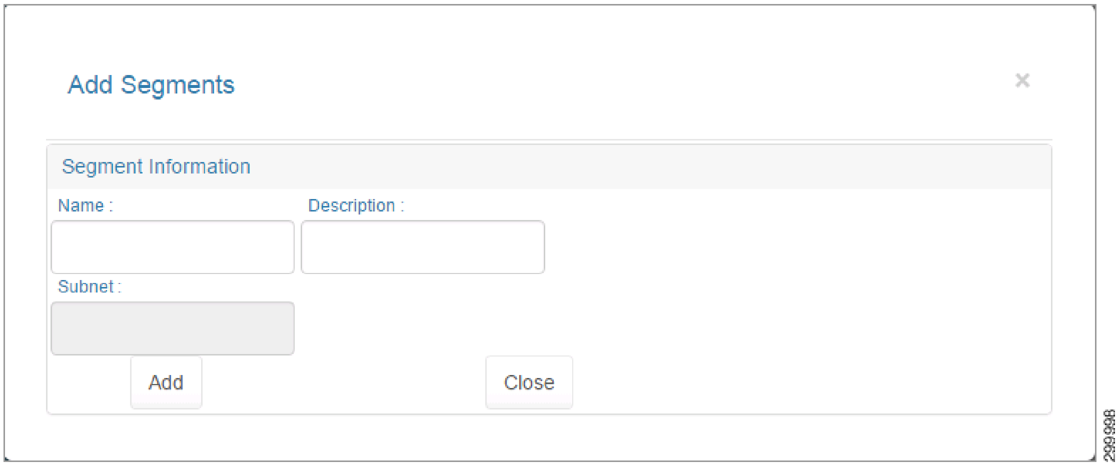
Adding a Segment

When you are adding a tier, you must add a segment:

Step 1 On the Add Tier screen shown in the previous section, under Enter L2 Segments, click the addition symbol (+).

You see the following screen.

Figure 2-52 Add Segment Screen



Enter information about the segment:

- Name—Name of the segment.
- Description—Description of the segment.
- Subnet—Subnet of the segment.

Step 2 When you are finished, click **Add**.

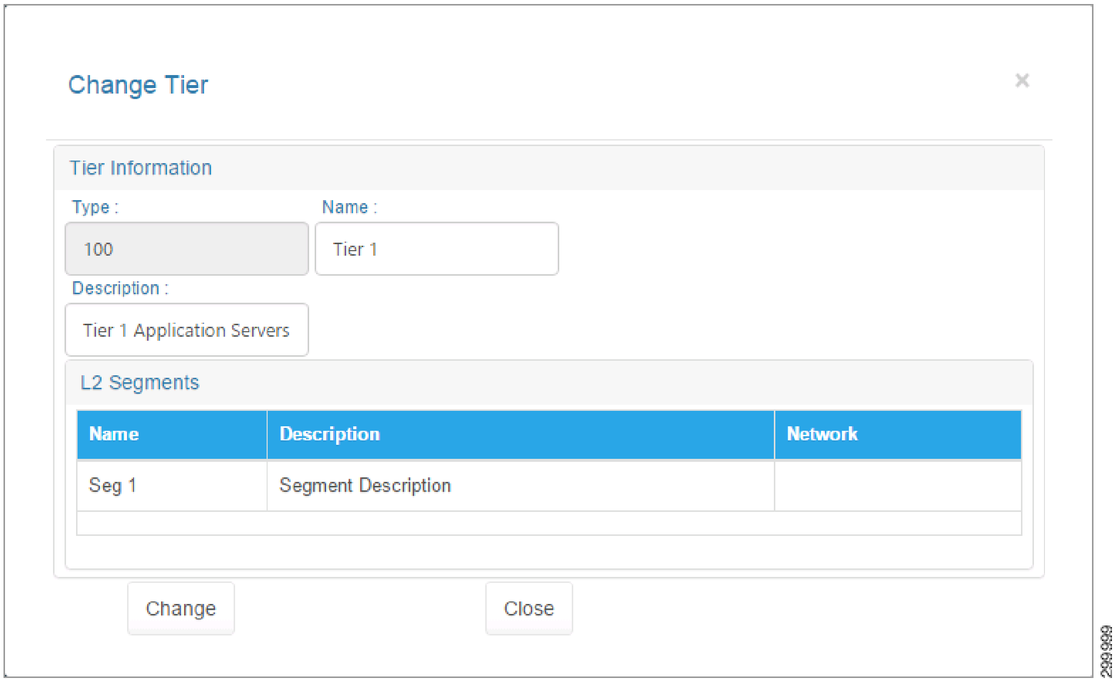
Changing a Tier

To change a tier:

Step 1 On the Tiers Tab screen, click the tier you want to change, then click **Change** (when you click a tier, you see segment information about the selected tier).

You see the following screen.

Figure 2-53 Change a Tier Screen



Change Tier

Tier Information

Type : 100

Name : Tier 1

Description : Tier 1 Application Servers

L2 Segments

Name	Description	Network
Seg 1	Segment Description	

The screen displays the following information, some of which you can change:

- Tier Information:
  - Type:—Prepopulated
  - Name:—You can edit the name.
  - Description:—You can edit the description.
- L2 Segments—
  - Name—Name of the Layer 2 segment.
  - Description—Description of the Layer 2 segment.
  - Network—The network of the Layer 2 segment.

You can click a specific segment under L2 Segments to update it. For more information, see the next section.

Step 2 When you are finished, click **Change**.

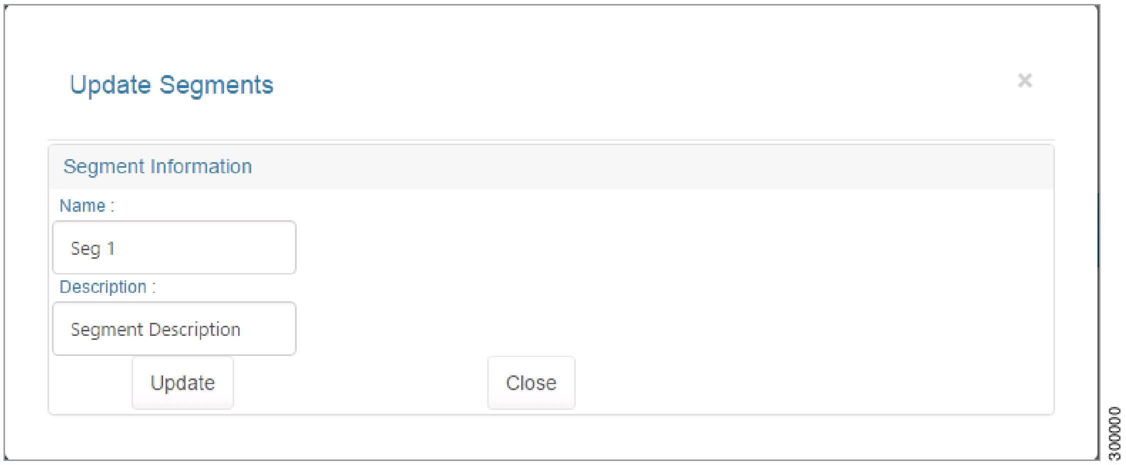
Updating a Segment

When you are changing a tier, you can update a segment:

Step 1 On the Change Tier screen shown in the previous section, under L2 Segments, click the segment you want to update.

You see the following screen.

Figure 2-54 Update Segments Screen



Update Segments

Segment Information

Name : Seg 1

Description : Segment Description

You can change:

- Name:—You can edit the name of the segment
- Description:—You can edit the description of the segment.

Step 2 When you are finished, click **Update**.

You return to the previous screen.

Removing a Tier

To remove a tier, on the Tiers Tab screen, click the tier you want to remove, then click **Remove**. In the current release, you must return to the Tiers tab to force a reload and consequent fetch from the backend.

Viewing and Modifying Load Balancer Information about a Container

On the Load Balancer tab, you can:

- View information about an existing load balancer
- Add a Citrix NetScaler VPX
- Add a load balancer
- Add a server
- Change a load balancer

- Change a server
- Remove a load balancer
- Remove a server
- Remove a Citrix NetScaler VPX

Understanding the Load Balancer Creation Procedure

Creating a load balancer involves three steps:

1. Add a Citrix NetScaler VPX.
2. Contact your cloud provider to license the Citrix NetScaler VPX you added.
3. Configure a load balancer.

These steps are described below.

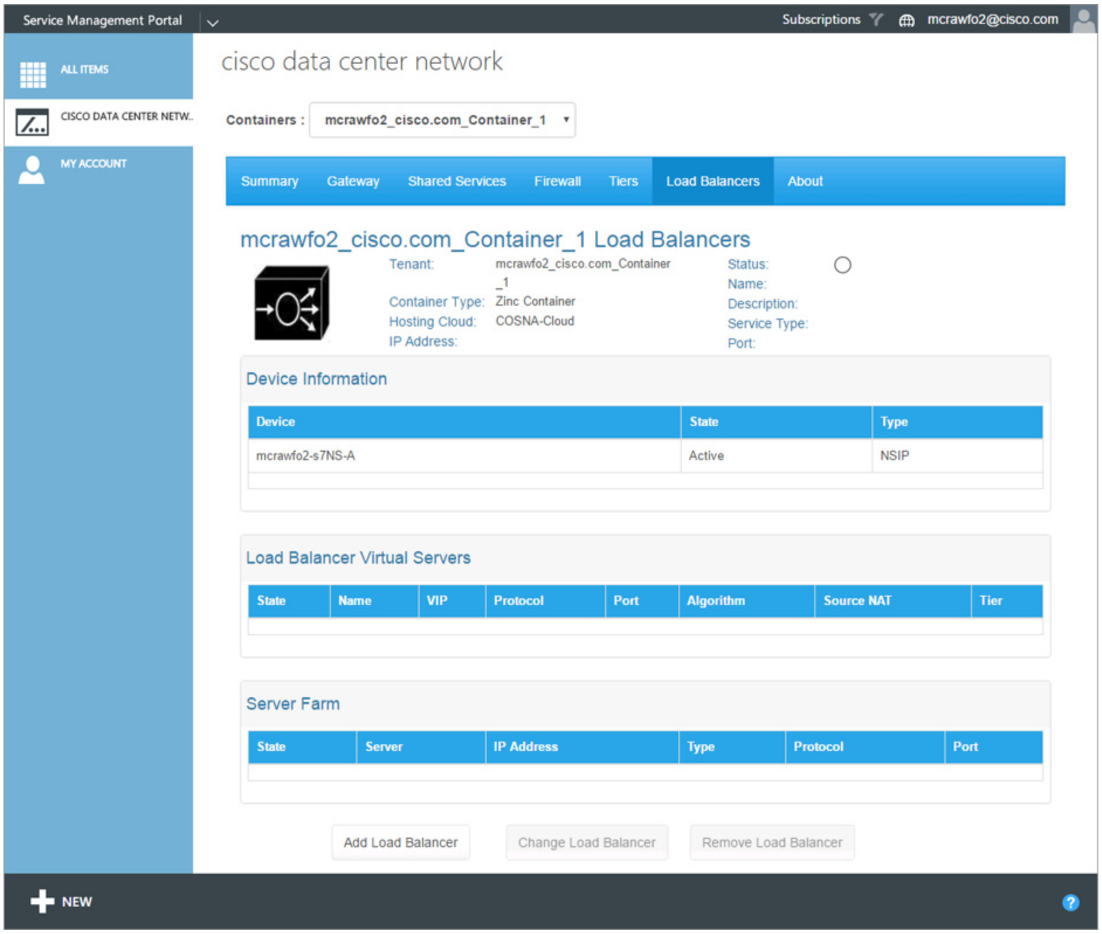
Viewing Load Balancer Information

Load balancing services are performed on a per-tenant container basis, so you can view information about a load balancer, such as the associated tenant, container type, hosting cloud, etc.

Step 1 If a load balancer has been created, to view information about it, click the **Load Balancers** tab.

You see the following screen.

Figure 2-55 Load Balancers Tab



Containers : mcrawfo2_cisco.com_Container_1

mcrawfo2_cisco.com_Container_1 Load Balancers

Tenant: mcrawfo2_cisco.com_Container _1
Container Type: Zinc Container
Hosting Cloud: COSNA-Cloud
IP Address:

Status: ○
Name:
Description:
Service Type:
Port:

Device Information

Device	State	Type
mcrawfo2-s7NS-A	Active	NSIP

Load Balancer Virtual Servers

State	Name	VIP	Protocol	Port	Algorithm	Source NAT	Tier

Server Farm

State	Server	IP Address	Type	Protocol	Port

If you click a specific Load Balancer Virtual Server, you see the corresponding Server Farm.

The screen displays the following information:

- Tenant:—Displays the tenant name.
- Container Type:—Displays the container type name.
- Hosting Cloud:—Displays the Hosting Cloud name.
- IP Address:—Displays the IP address of the load balancer.
- Status:—Displays the load balancer status. The icons indicate:
  - Green—Load balancer is Active.
  - Red— Load balancer is Inactive.
  - Yellow— Load balancer is Creating.
- Name:—Displays the name in the form lb*n*.
- Description:—Descriptive name.
- Service Type:—The type of service for which the load balancer is configured.
- Port:—The Port for which the load balancer is configured.
- Device Information:—Information about the load balancer device.

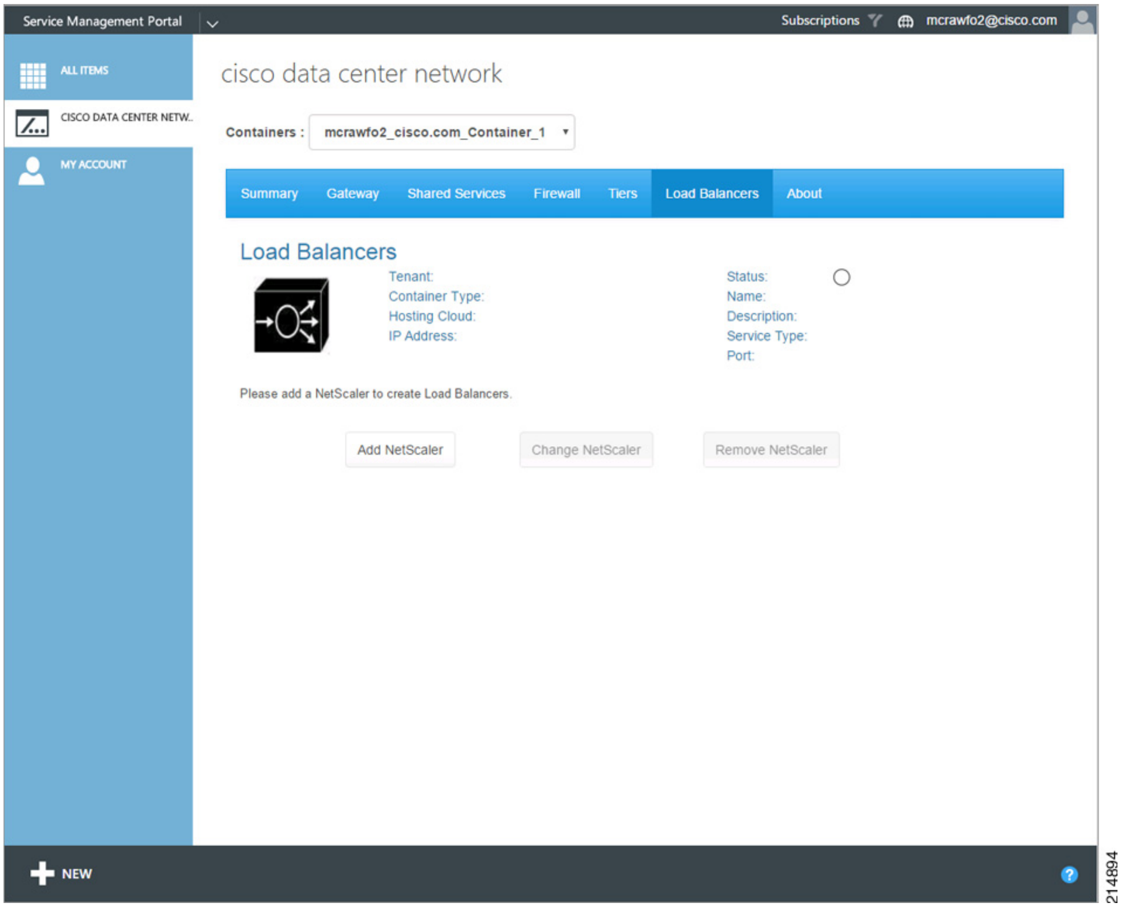
- Load Balancer Virtual Servers:—Lists all the VIPs configured on the VPX device.
- Server Farm:—The list of servers which are configured and attached to the load balancer virtual server.

Adding a Citrix NetScaler VPX

To add a load balancer for the first time, you must first add a Citrix NetScaler1000V:

Step 1 On the Load Balancers Tab screen, you see the message: “Please add a NetScaler to create Load Balancers”, as shown in the following screen.

Figure 2-56 Create a Citrix NetScaler VPX



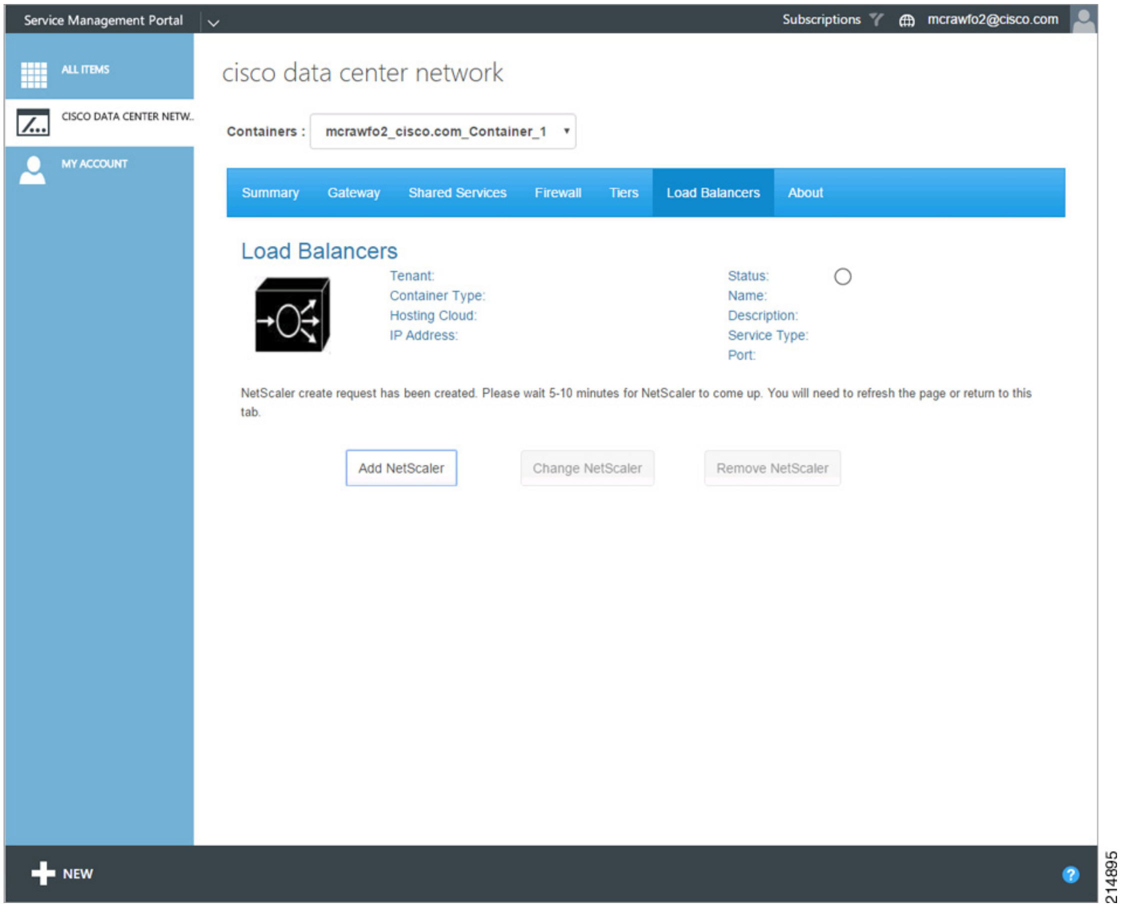
Containers : mcrawfo2_cisco.com_Container_1

Please add a NetScaler to create Load Balancers.

Step 2 Click **Add**.

You see the message “NetScaler create request has been created. Please wait 5-10 minutes for the NetScaler to come up. You will need to refresh the page or return to the tab.”, as shown in the following screen.

Figure 2-57 Citrix NetScaler VPX Being Created



Containers : mcrawfo2_cisco.com_Container_1

Load Balancers

Tenant:
Container Type:
Hosting Cloud:
IP Address:

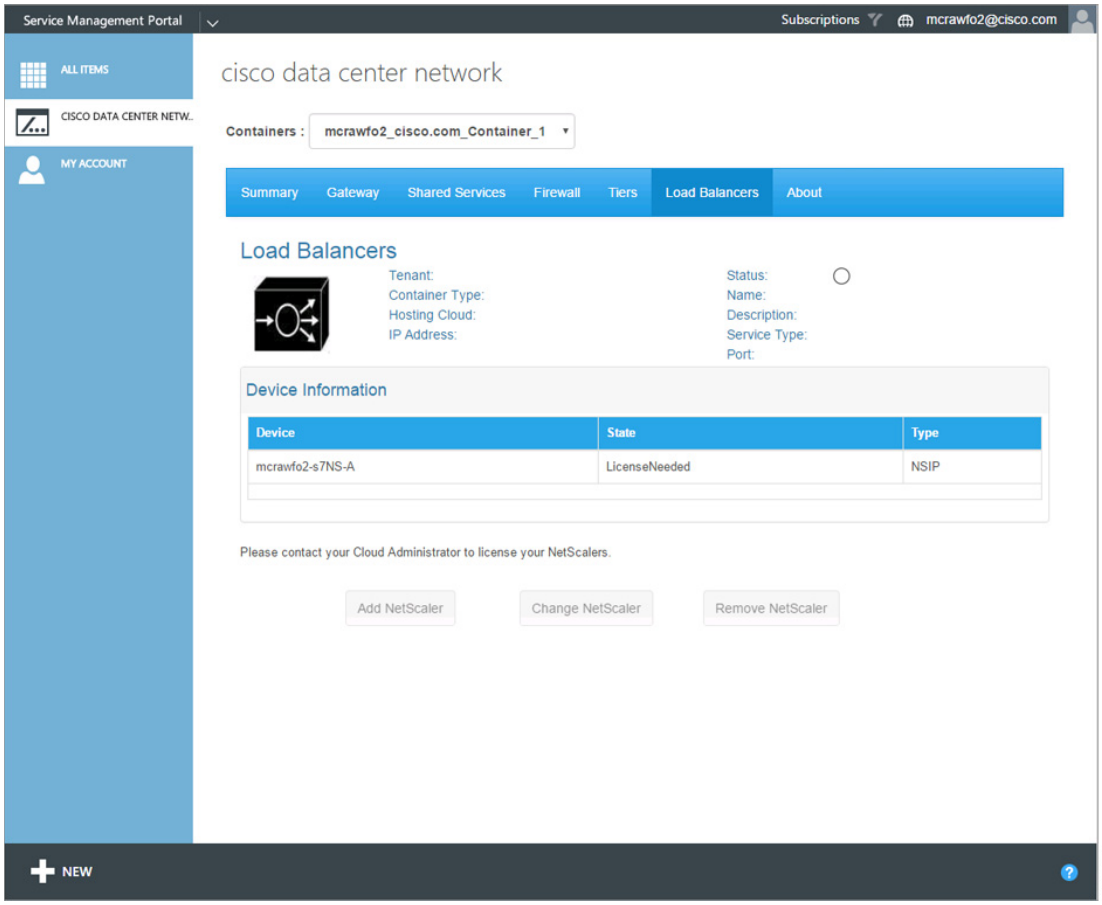
Status: ○
Name:
Description:
Service Type:
Port:

NetScaler create request has been created. Please wait 5-10 minutes for NetScaler to come up. You will need to refresh the page or return to this tab.

Cisco CNAP checks the configuration of your subscription to determine if it includes a SLB (Citrix NetScaler VPX). If it does, Cisco CNAP configures and onboards the Citrix NetScaler VPX.

Step 3 When the Citrix NetScaler VPX is configured, refresh the screen or click the Load Balancers tab again. You see the configured device with a State of LicenseNeeded and the message “Please contact your Cloud Administrator to license your NetScalers”, as shown in the following screen.

Figure 2-58 Citrix NetScaler VPX License Needed



Containers : mcrawfo2_cisco.com_Container_1

Load Balancers

Tenant:
Container Type:
Hosting Cloud:
IP Address:
Status: ○
Name:
Description:
Service Type:
Port:

Device Information

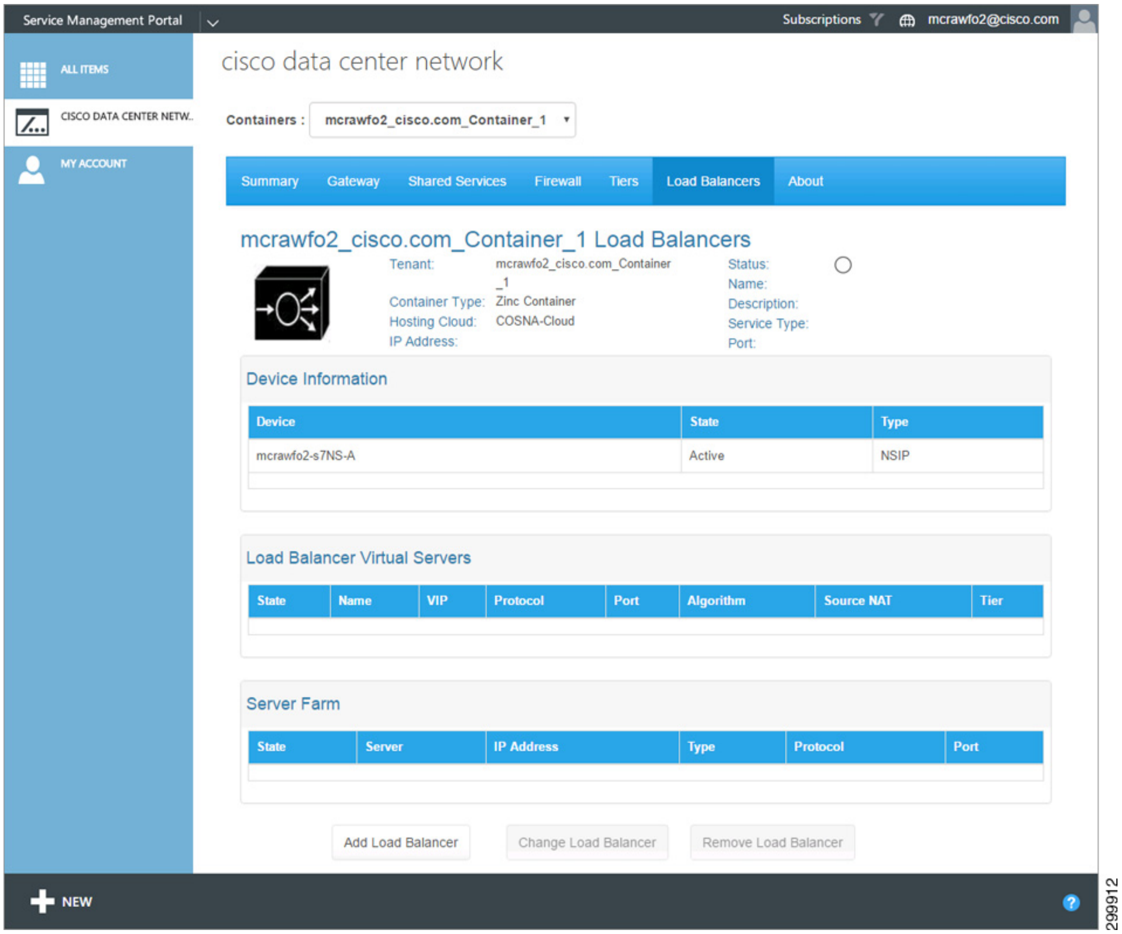
Device	State	Type
mcrawfo2-s7NS-A	LicenseNeeded	NSIP

Please contact your Cloud Administrator to license your NetScalers.

Contact your cloud provider to license the Citrix NetScaler VPX(s).

Step 4 Once the Cloud Administrator licenses the Citrix NetScaler VPX, on the Tenant Portal Load Balancers tab, the Citrix NetScaler VPX will now be in an Active state, as shown in the following screen.

Figure 2-59 Citrix NetScaler VPX Active after Licensing



Containers : mcrawfo2_cisco.com_Container_1

mcrawfo2_cisco.com_Container_1 Load Balancers

Tenant: mcrawfo2_cisco.com_Container_1
Container Type: Zinc Container
Hosting Cloud: COSNA-Cloud
IP Address:

Status: ○
Name:
Description:
Service Type:
Port:

Device Information

Device	State	Type
mcrawfo2-s7NS-A	Active	NSIP

Load Balancer Virtual Servers

State	Name	VIP	Protocol	Port	Algorithm	Source NAT	Tier

Server Farm

State	Server	IP Address	Type	Protocol	Port

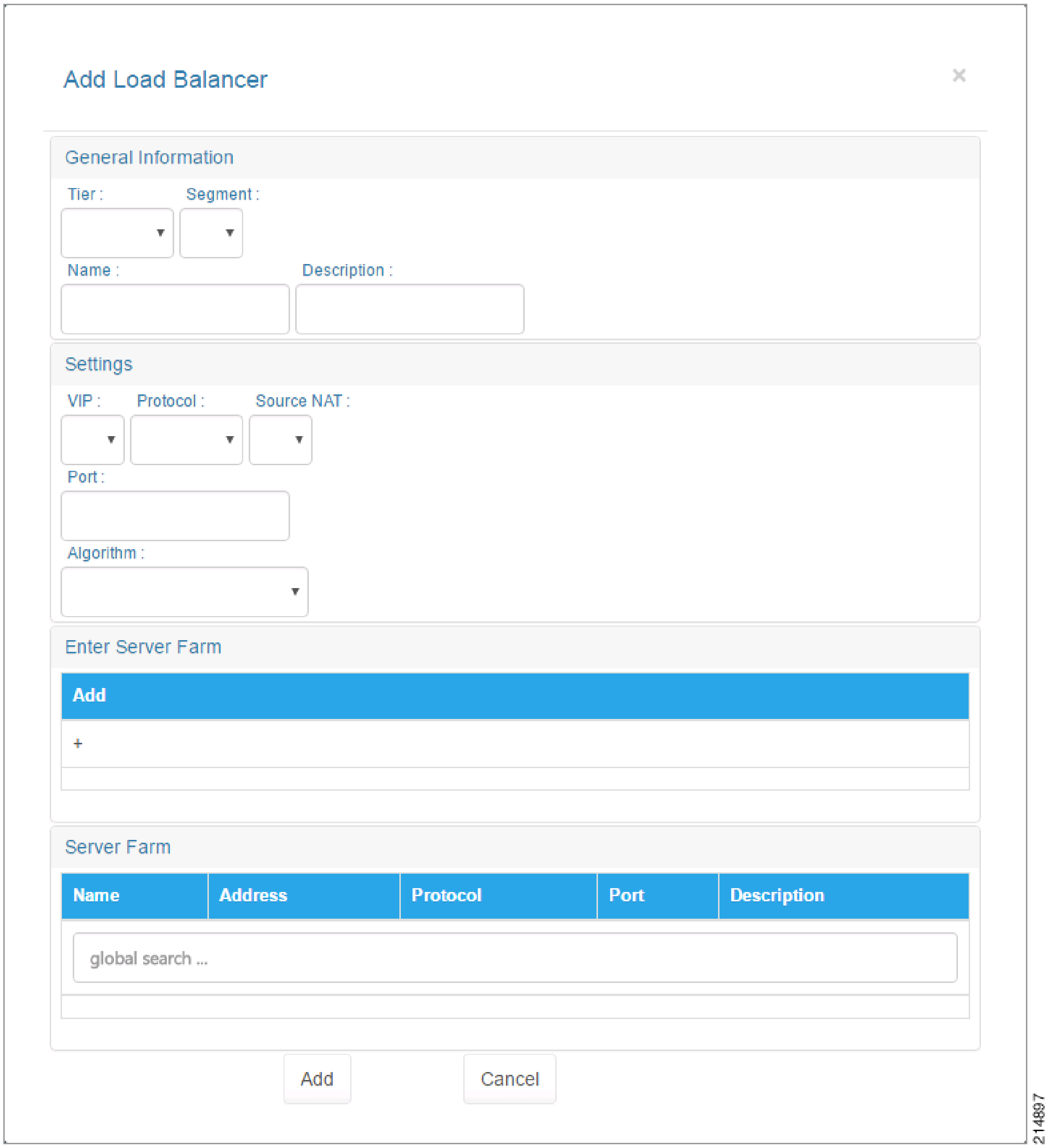
Adding a Load Balancer

After you have added a Citrix NetScaler VPX and confirmed that your cloud provider has licensed the Citrix NetScaler VPX (on the Load Balancers tab the Citrix NetScaler VPX is in an Active state), you can add a Virtual Server:

Step 1 On the Load Balancers Tab screen, click **Add Load Balancer**.

You see the following screen.

Figure 2-60 Add Load Balancer Screen



Enter the following information:

- General Information:
  - Tier:—Select the tier.
  - Segment:—Select the segment.
  - Name:—Enter a name.
  - Description:—Enter a description.
- Settings:
  - VIP:—Select a VIP.
  - Protocol:—Select a protocol: HTTP or SSL

- Port:—Enter the port number.
- Source NAT:—Select the source NAT.
- Algorithm:—Select the algorithm: LEASTCONNECTION or ROUNDROBIN.

You can add a server. For more information, see the next section.

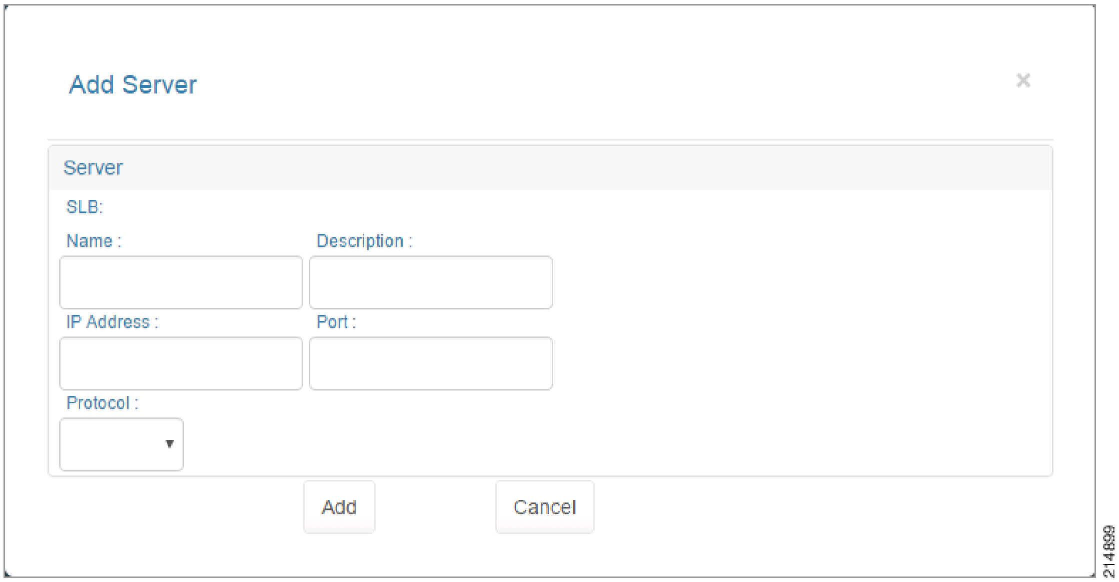
Step 2 When you are finished, click **Add**.

Adding a Load Balancer Server

Step 1 On the Add Load Balancer screen shown in the previous section, under Enter Server Farm, click +.

You see the following screen.

Figure 2-61 Add Server



Enter the following information:

- Name:—Enter a name for the server.
- Description:—Enter a description for the server.
- IP Address:—Enter the IP address of the server.
- Protocol:—Select the protocol: HTTP or SSL
- Port:—Enter the port number.

Step 2 When you are finished, click **Add**.

You return to the previous screen.

Step 3 Click **Add**.

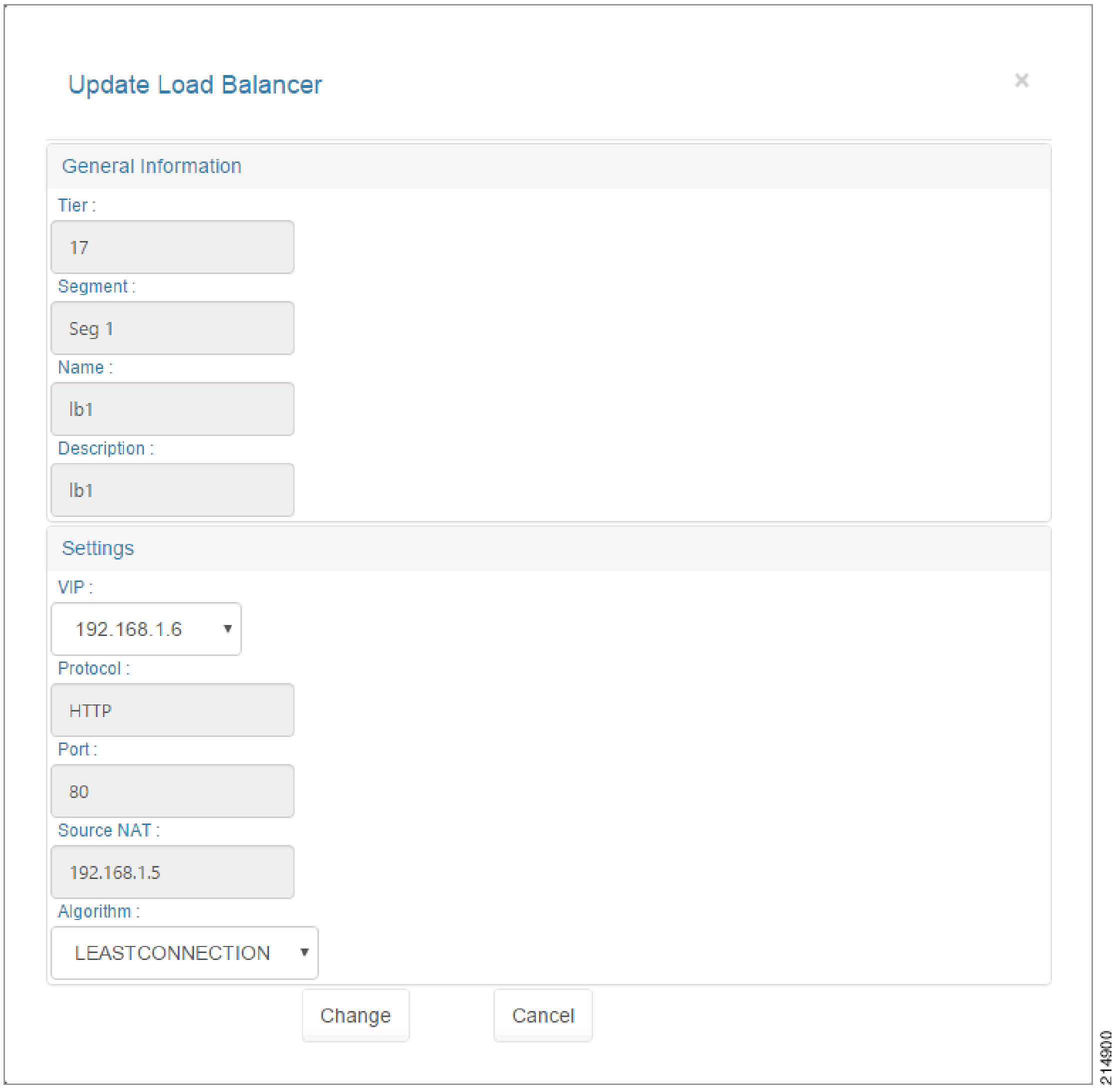
Changing a Load Balancer

To change a load balancer:

Step 1 On the Load Balancers Tab screen, under Load Balancer Virtual Servers, click the load balancer you want to change, then click **Change Load Balancer**.

You see the Update Load Balancer screen.

Figure 2-62 Update Load Balancer



Update Load Balancer

General Information

Tier : 17

Segment : Seg 1

Name : lb1

Description : lb1

Settings

VIP : 192.168.1.6

Protocol : HTTP

Port : 80

Source NAT : 192.168.1.5

Algorithm : LEASTCONNECTION

The screen displays the following fields, however you can only change the VIP and the Algorithm:

- General Information:
  - Tier:—The tier associated with the SLB.
  - Segment:—The segment associated with the SLB.
  - Name:—The name of the SLB.

  - Description:—A description of the SLB.
- Settings:
  - VIP:—You can change the VIP.
  - Protocol:—The protocol associated with the SLB: HTTP or SSL
  - Port:—The port number associated with the SLB.
  - Source NAT:—The source NAT associated with the SLB.
  - Algorithm:—You can change the algorithm: LEASTCONNECTION or ROUNDROBIN.

Step 2 When you are finished, click **Change**.

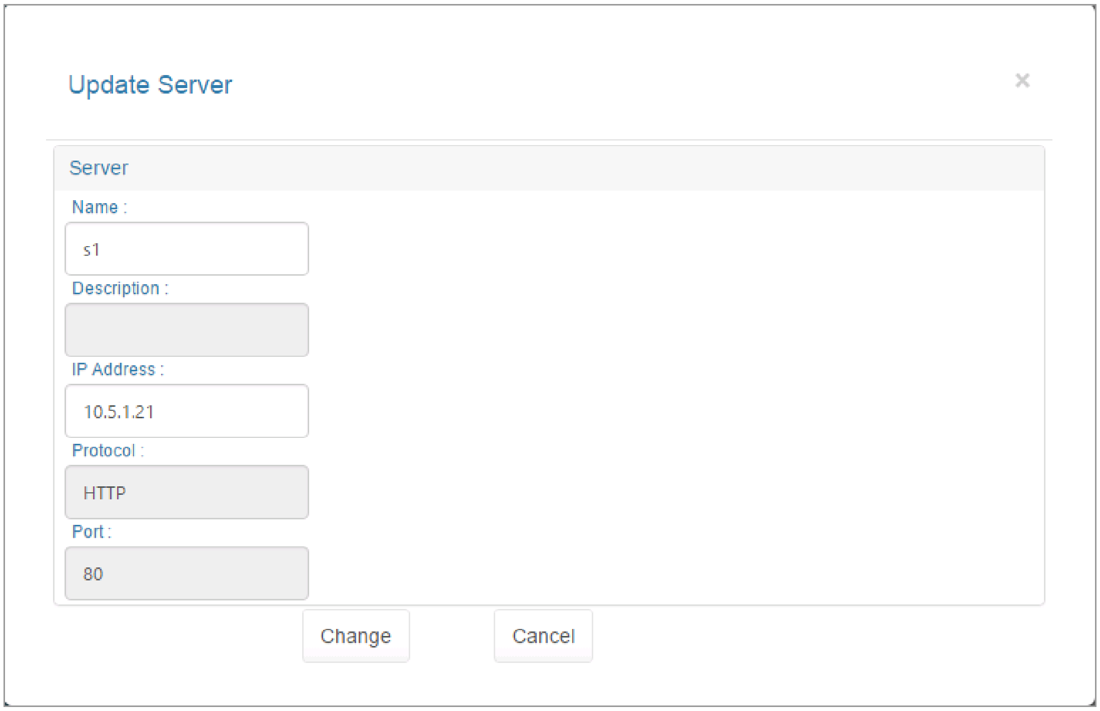
Changing a Server Farm Server

To change the IP address of a load balancer server:

Step 1 On the Load Balancers Tab screen, click the Load Balancer Virtual Server you want to change, then under Server Farm click the server you want to change, then click **Change Server**.

You see the Update Server screen.

Figure 2-63 Update Server Load Balancer Server



Update Server

Server

Name : s1

Description :

IP Address : 10.5.1.21

Protocol : HTTP

Port : 80

The screen displays the following:

- Name:—Name of the server.
- Description:—Displays a description.
- IP Address:—You can change this field.

- Protocol:—HTTP or SSL.
- Port:—The port number.

Step 2 When you are finished, click **Change**.

Removing a Load Balancer

To remove a load balancer, on the Load Balancers Tab screen, click the Load Balancer Virtual Server you want to remove, then click **Remove**.

Removing a Server Farm Server

To remove a server, on the Load Balancers Tab screen, click the Load Balancer Virtual Server you want with the server you want to remove, then under Server Farm click the server you want to remove, then click **Remove**.

Removing a Citrix NetScaler VPX

Step 1 To remove a Citrix NetScaler VPX, which also removes the current load balancers, on the Load Balancers Tab screen, click the Citrix NetScaler VPX you want to remove, then click **Remove**.

You see the NetScaler Removal screen.

Step 2 Click **Confirm**.

APPENDIX A

Onboarding an Application from a Subscription

Note Use only standalone VM creation.

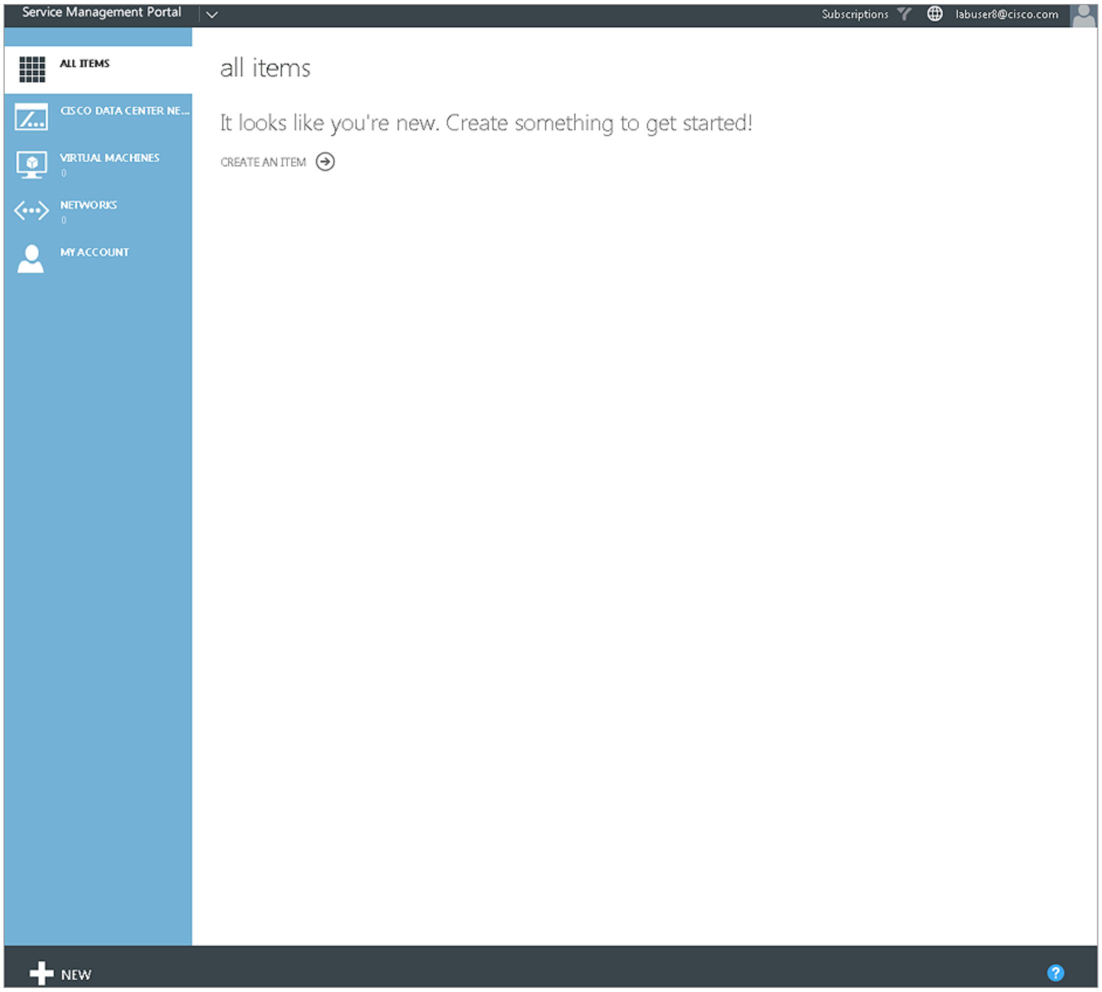
To onboard an application from a subscription:

Step 1 Subscribe to a plan with a network and Virtual Machine Cloud.

For information on subscribing to a plan, see Subscribing to a Plan in Chapter 1, "Introduction." For information on the plans to which you can subscribe, contact your cloud provider.

On the main Tenant Portal screen you should see Virtual Machines in the left column, as shown in the following screen.

Figure A-1 Main Tenant Portal Screen

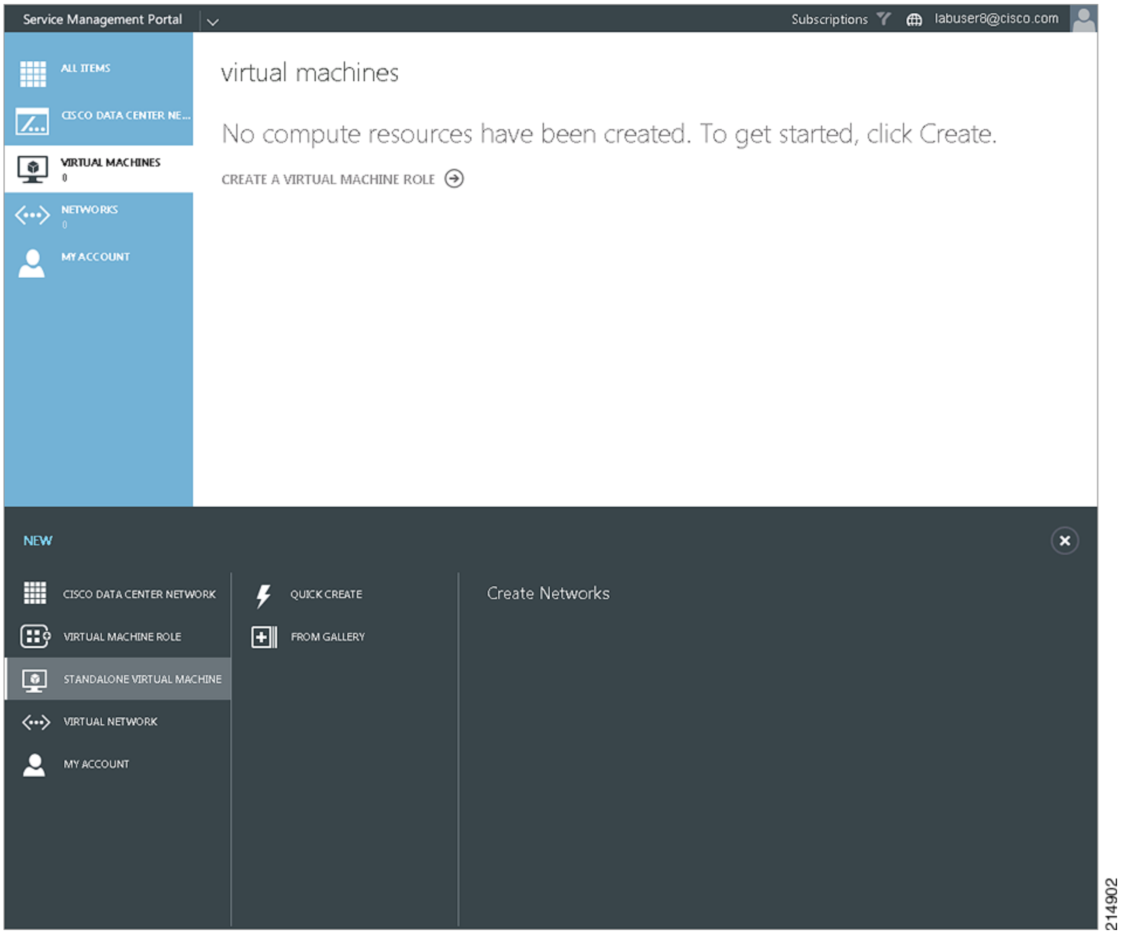


all items

It looks like you're new. Create something to get started!

Step 2 Click + **New**, **Standalone Virtual Machine**, then **From Gallery**, as shown in the following screen.

Figure A-2 Create Virtual Machine Screen



Service Management Portal

Subscriptions labuser8@cisco.com

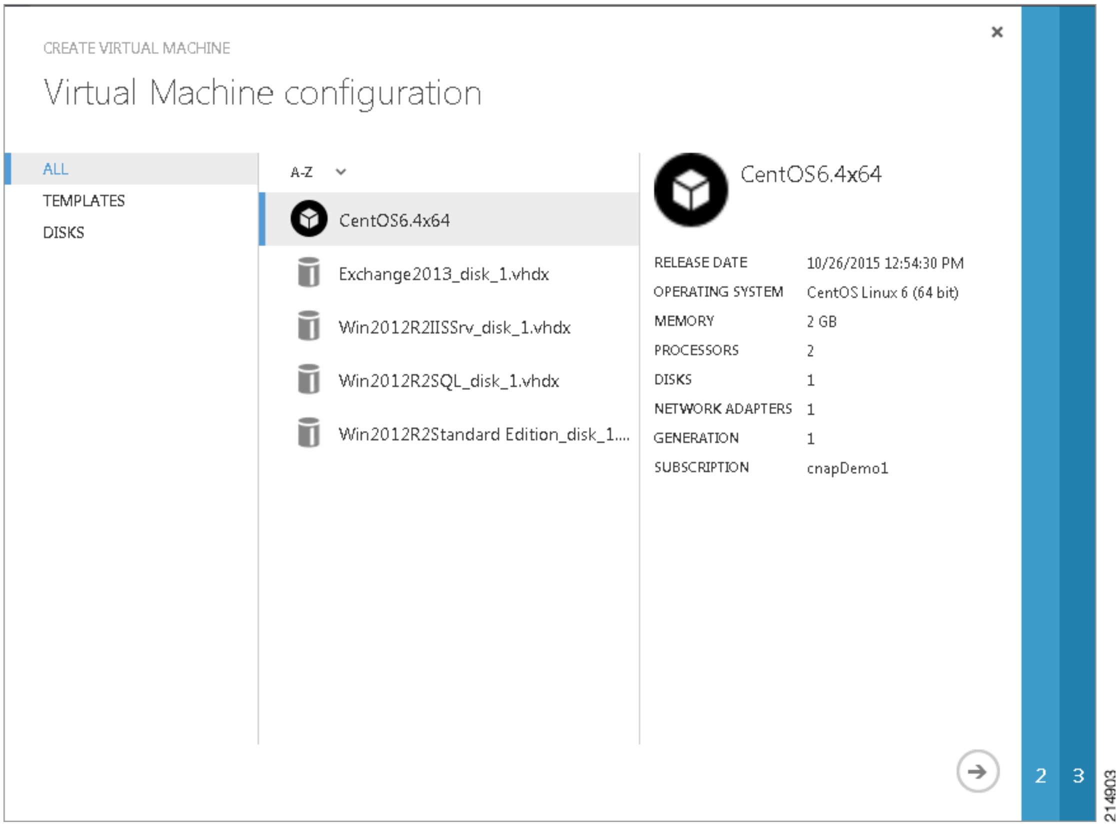
virtual machines

No compute resources have been created. To get started, click Create.

CREATE A VIRTUAL MACHINE ROLE

You see the following screen.

Figure A-3 Virtual Machine Configuration



CREATE VIRTUAL MACHINE

Virtual Machine configuration

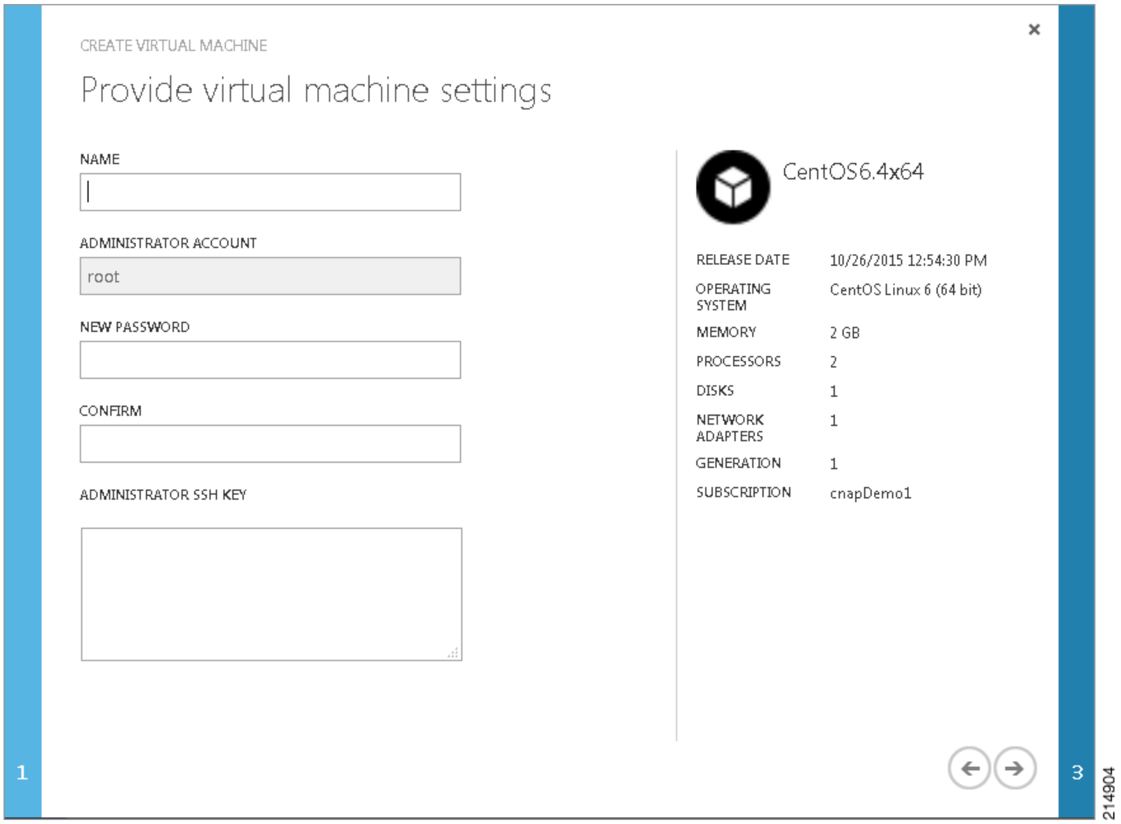
CentOS6.4x64

RELEASE DATE	10/26/2015 12:54:30 PM
OPERATING SYSTEM	CentOS Linux 6 (64 bit)
MEMORY	2 GB
PROCESSORS	2
DISKS	1
NETWORK ADAPTERS	1
GENERATION	1
SUBSCRIPTION	cnapDemo1

Step 3 In this example we selected **CentOS6.4x64**. Click the right arrow (–>).

You see the following screen.

Figure A-4 Virtual Machine Settings



CREATE VIRTUAL MACHINE

Provide virtual machine settings

NAME

ADMINISTRATOR ACCOUNT: root

NEW PASSWORD

CONFIRM

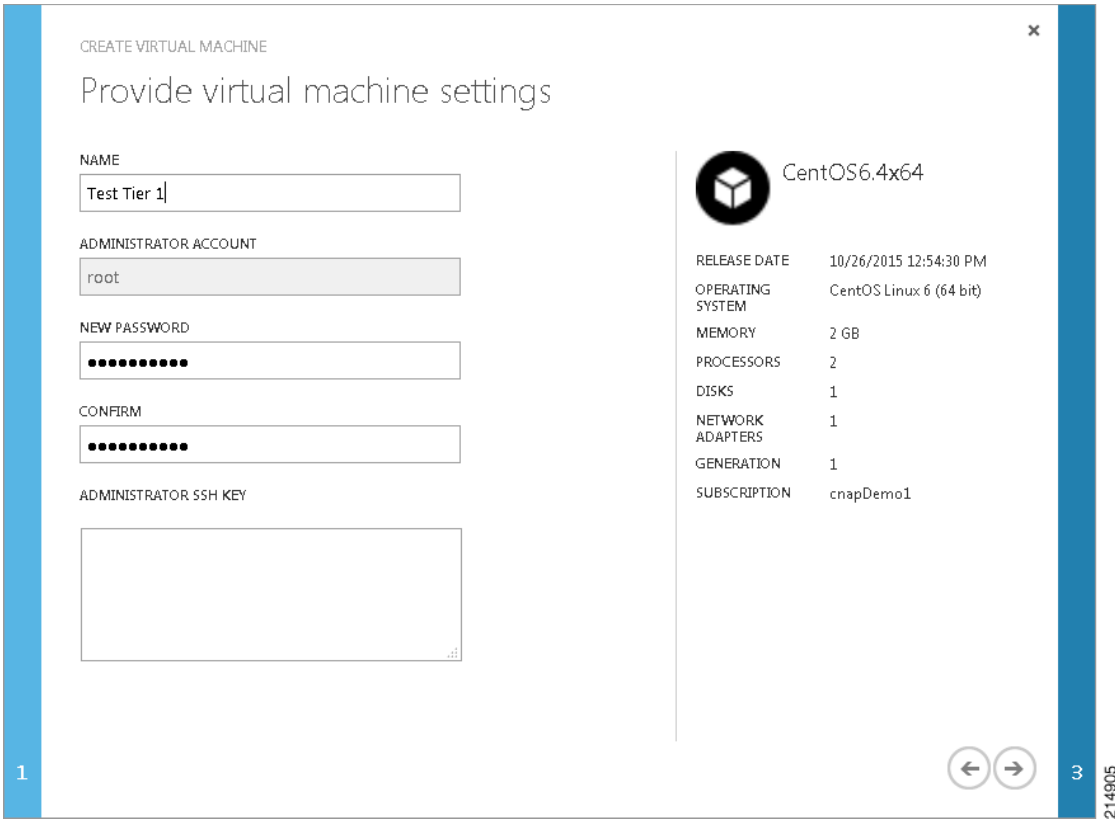
ADMINISTRATOR SSH KEY

CentOS6.4x64

RELEASE DATE	10/26/2015 12:54:30 PM
OPERATING SYSTEM	CentOS Linux 6 (64 bit)
MEMORY	2 GB
PROCESSORS	2
DISKS	1
NETWORK ADAPTERS	1
GENERATION	1
SUBSCRIPTION	cnapDemo1

Step 4 Enter a Name for the virtual machine, create a New Password, and Confirm it, as shown in the following screen.

Figure A-5 Name and Password Screen



CREATE VIRTUAL MACHINE

Provide virtual machine settings

NAME: Test Tier 1

ADMINISTRATOR ACCOUNT: root

NEW PASSWORD: ●●●●●●●●●●●

CONFIRM: ●●●●●●●●●●●

ADMINISTRATOR SSH KEY

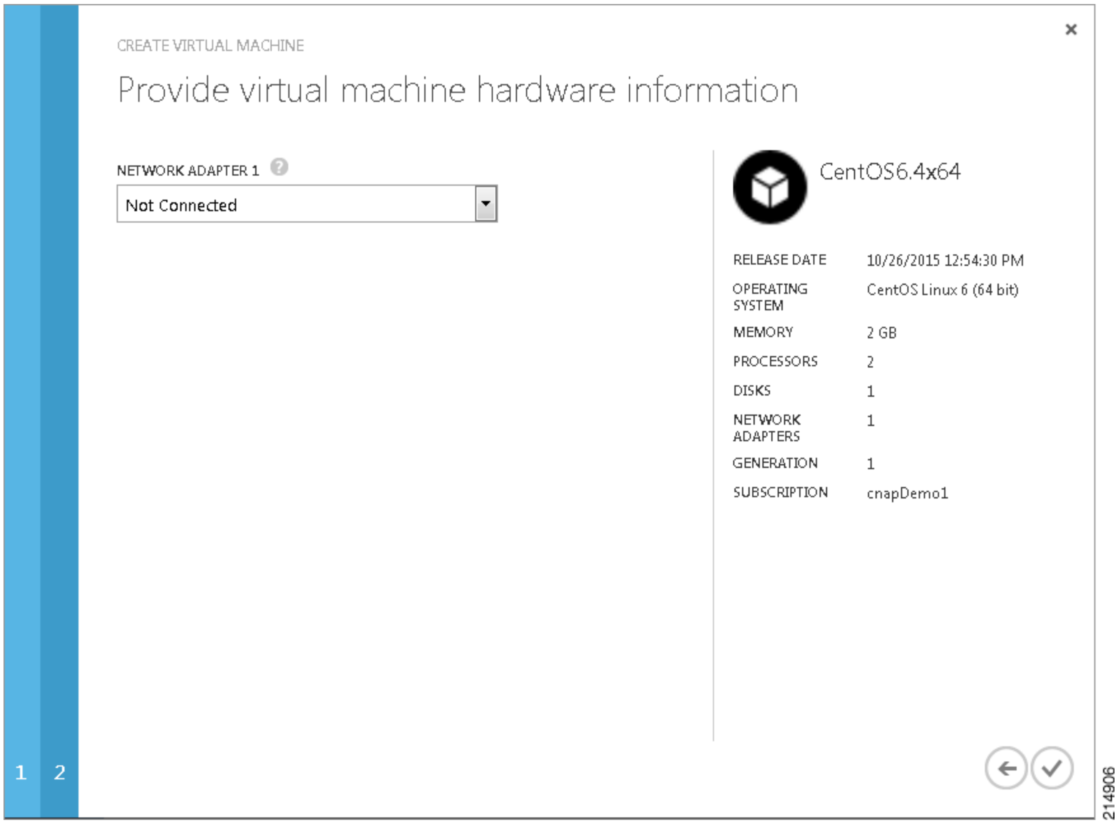
CentOS6.4x64

RELEASE DATE	10/26/2015 12:54:30 PM
OPERATING SYSTEM	CentOS Linux 6 (64 bit)
MEMORY	2 GB
PROCESSORS	2
DISKS	1
NETWORK ADAPTERS	1
GENERATION	1
SUBSCRIPTION	cnapDemo1

Step 5 Click the right arrow (–>).

You see the following screen.

Figure A-6 Network Adapter Screen



CREATE VIRTUAL MACHINE

Provide virtual machine hardware information

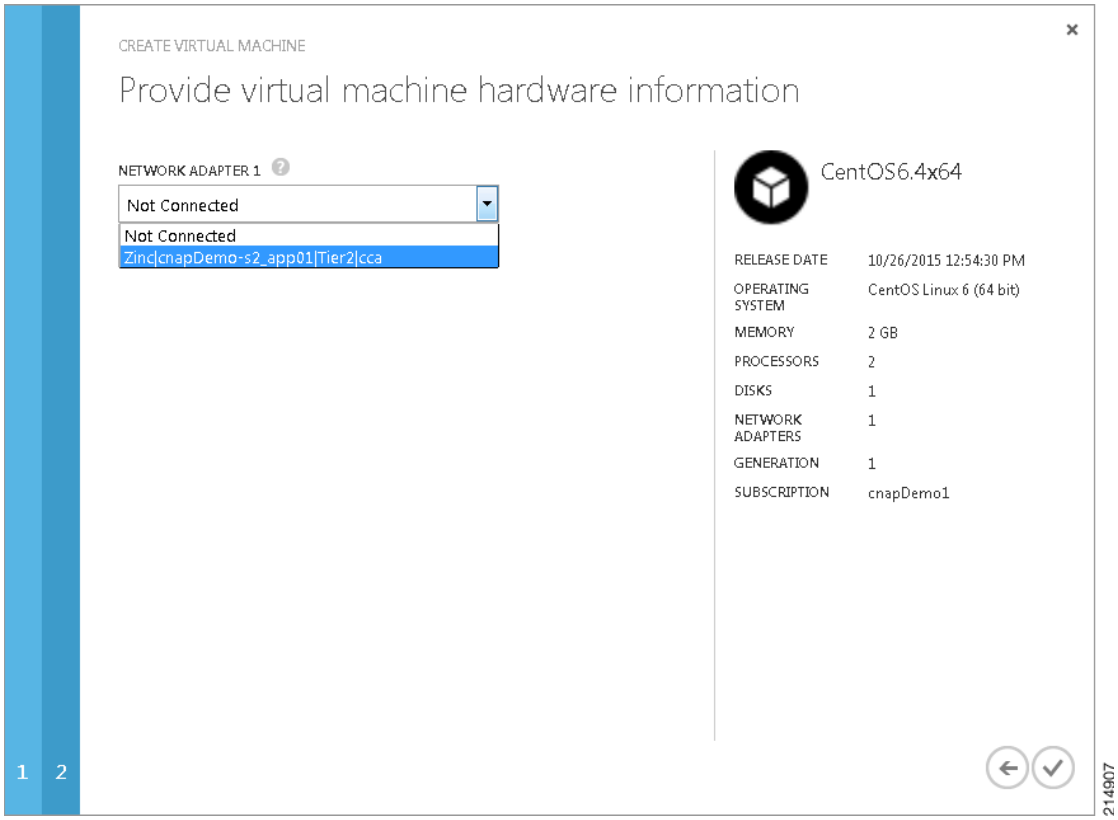
NETWORK ADAPTER 1: Not Connected

CentOS6.4x64

RELEASE DATE	10/26/2015 12:54:30 PM
OPERATING SYSTEM	CentOS Linux 6 (64 bit)
MEMORY	2 GB
PROCESSORS	2
DISKS	1
NETWORK ADAPTERS	1
GENERATION	1
SUBSCRIPTION	cnapDemo1

Step 6 Select an adapter from the drop-down menu, as shown in the following screen.

Figure A-7 Network Adapter Selection



CREATE VIRTUAL MACHINE

Provide virtual machine hardware information

NETWORK ADAPTER 1: Not Connected

Not Connected
Zinc|cnapDemo-s2_app01|Tier2|cca

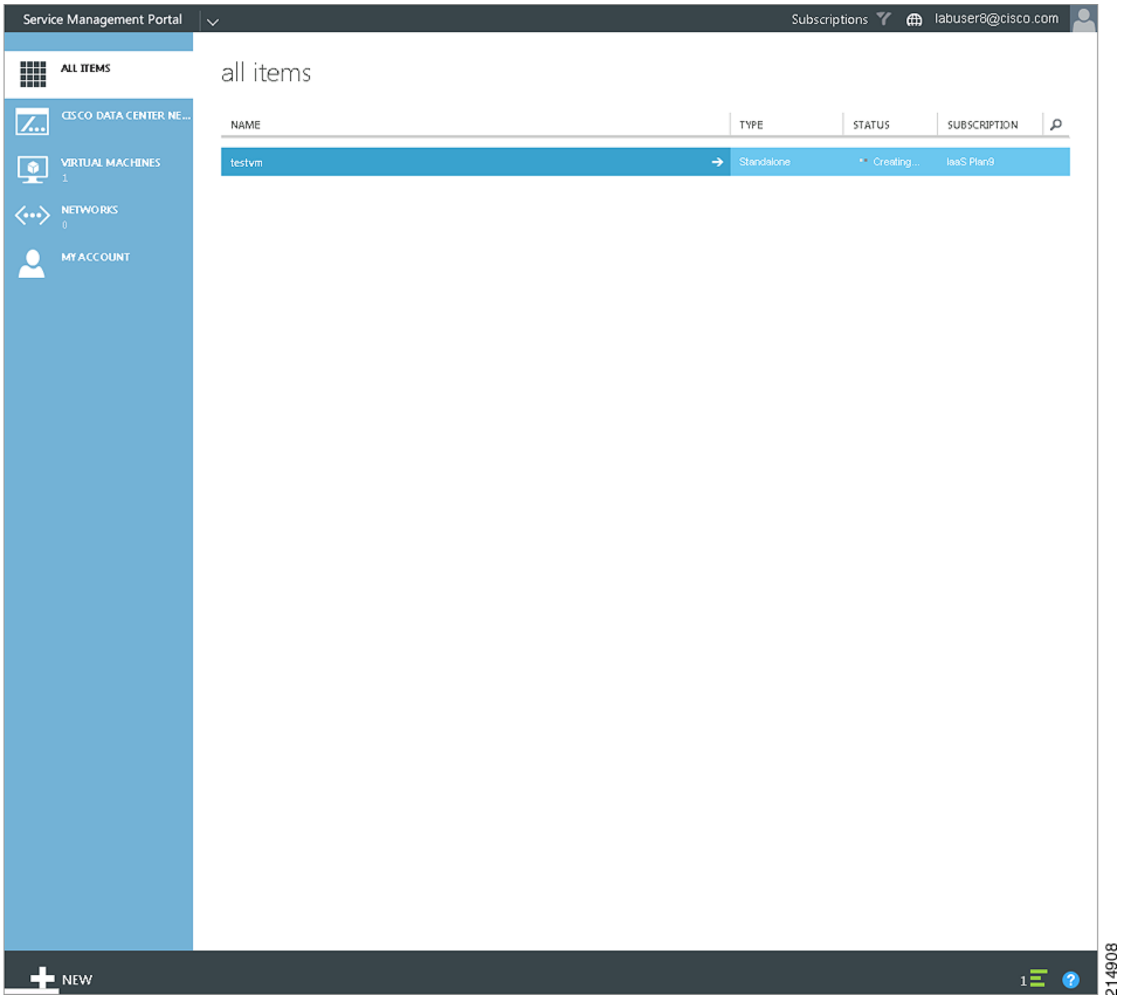
CentOS6.4x64

RELEASE DATE	10/26/2015 12:54:30 PM
OPERATING SYSTEM	CentOS Linux 6 (64 bit)
MEMORY	2 GB
PROCESSORS	2
DISKS	1
NETWORK ADAPTERS	1
GENERATION	1
SUBSCRIPTION	cnapDemo1

Step 7 Click the check mark.

You should be able to see your virtual machine being created from your dashboard, as shown in the following screen, where the virtual machine has a Status of Creating.

Figure A-8 Virtual Machine Creation in Process

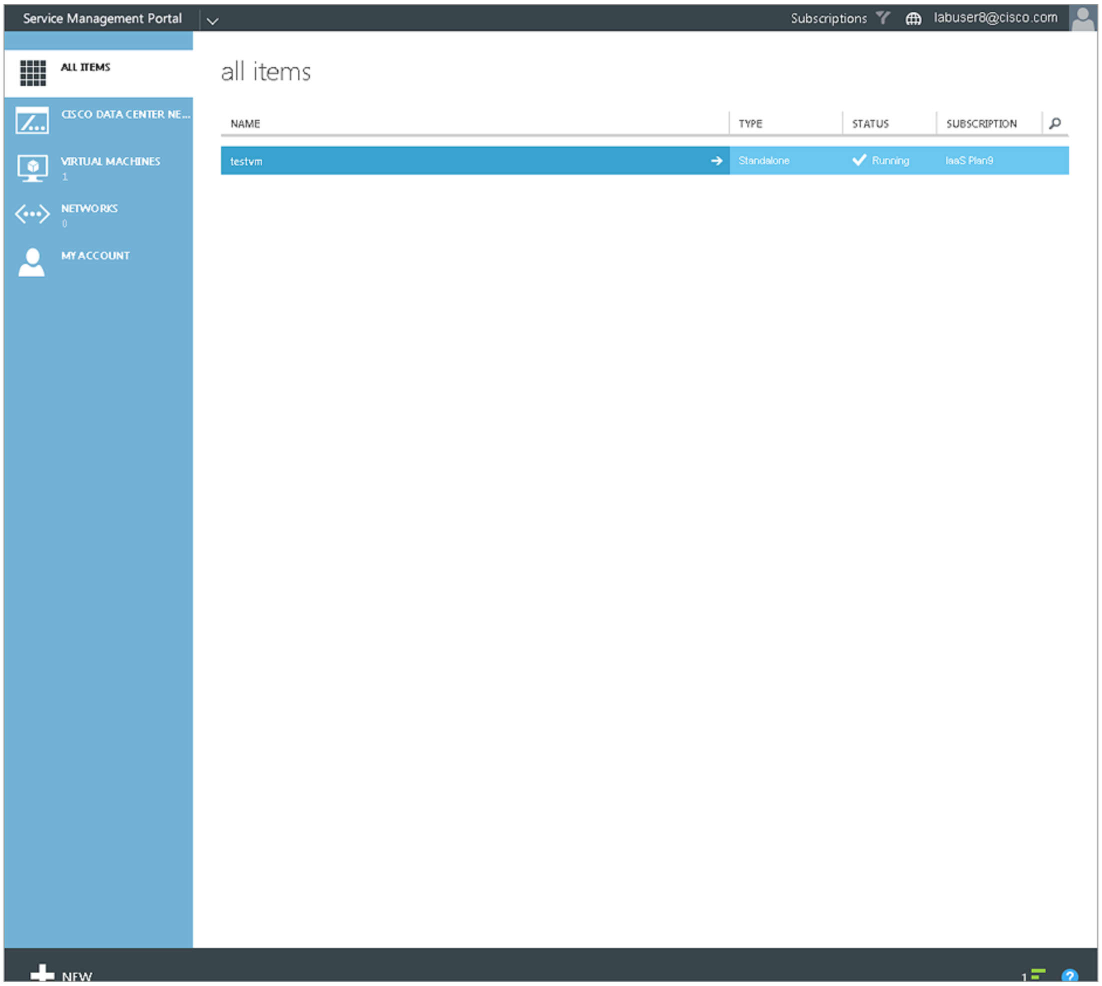


all items

NAME	TYPE	STATUS	SUBSCRIPTION
testvm	Standalone	Creating...	IaaS Plan9

Virtual machine creation takes a few minutes as the virtual machine is created, boots, and is configured. When the virtual machine has been created, you see a screen like the following.

Figure A-9 Virtual Machine Created



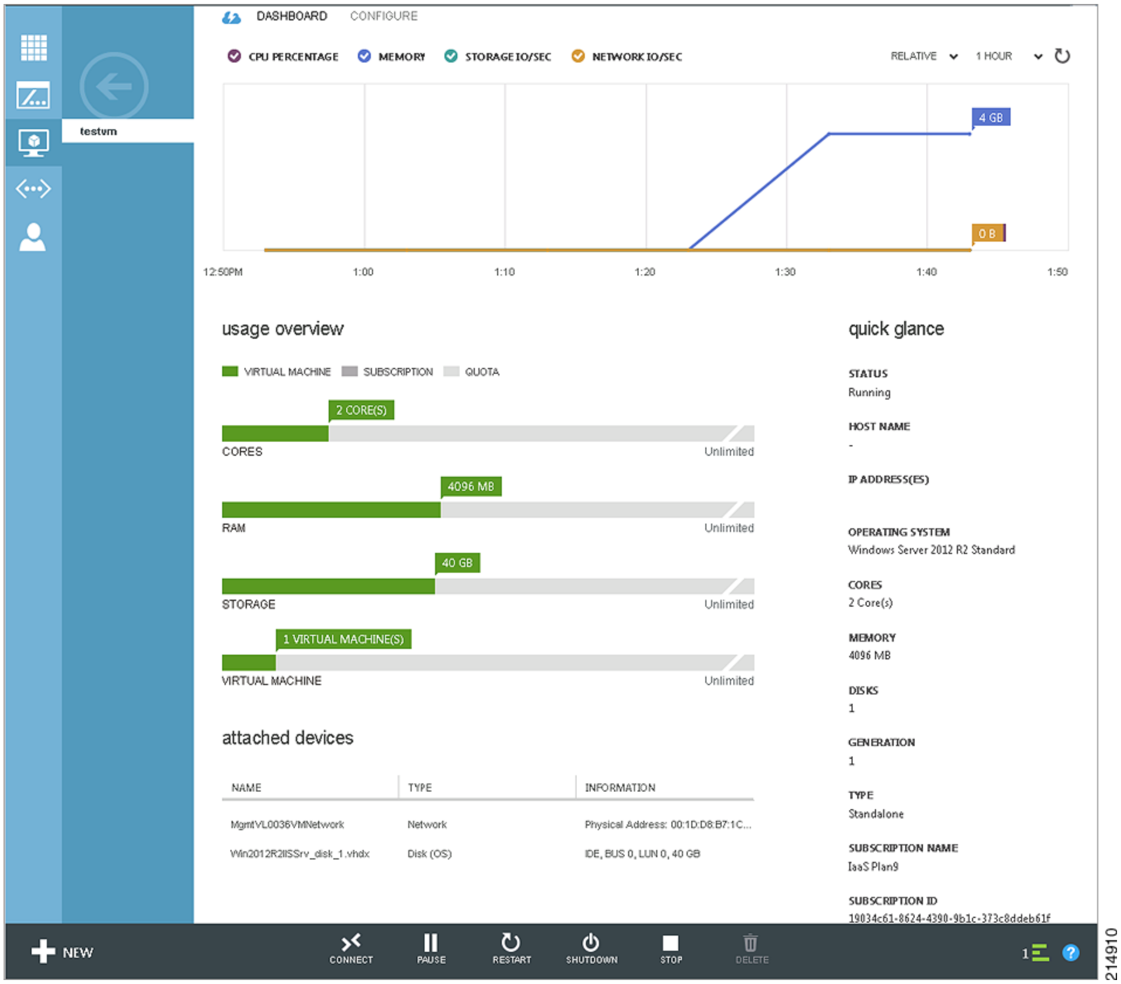
all items

NAME	TYPE	STATUS	SUBSCRIPTION
testvm	Standalone	✓ Running	IaaS Plan9

Step 8 When creation is complete, the Status will change to Running. Click on the plan name, then click **Dashboard**.

You see the following screen, which shows you information about your virtual machine.

Figure A-10 Virtual Machine Information



usage overview

🟩 VIRTUAL MACHINE ▨ SUBSCRIPTION □ QUOTA

CORES	2 CORE(S)	Unlimited
RAM	4096 MB	Unlimited
STORAGE	40 GB	Unlimited
VIRTUAL MACHINE	1 VIRTUAL MACHINE(S)	Unlimited

attached devices

NAME	TYPE	INFORMATION
MgmtVL0036VMNetwork	Network	Physical Address: 00:1D:D8:B7:1C...
Win2012R2IISSrv_disk_1.vhdx	Disk (OS)	IDE, BUS 0, LUN 0, 40 GB

quick glance

STATUS
Running

HOST NAME
-

IP ADDRESS(ES)

OPERATING SYSTEM
Windows Server 2012 R2 Standard

CORES
2 Core(s)

MEMORY
4096 MB

DISKS
1

GENERATION
1

TYPE
Standalone

SUBSCRIPTION NAME
IaaS Plan9

SUBSCRIPTION ID
19034c61-8624-4390-9b1c-373c8ddeb61f