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

March 31, 2016

CCDE, CCENT, CCSI, Cisco Eos, Cisco Explorer, Cisco HealthPresence, Cisco IronPort, the Cisco logo, Cisco Nurse Connect, Cisco Pulse, Cisco SensorBase, Cisco StackPower, Cisco StadiumVision, Cisco TelePresence, Cisco TrustSec, Cisco Unified Computing System, Cisco WebEx, DCE, Flip Channels, Flip for Good, Flip Mino, Flipshare (Design), Flip Ultra, Flip Video, Flip Video (Design), Instant Broadband, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn, Cisco Capital, Cisco Capital (Design), Cisco:Financed (Stylized), Cisco Store, Flip Gift Card, and One Million Acts of Green are service marks; and Access Registrar, Aironet, AllTouch, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Lumin, Cisco Nexus, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, Continuum, EtherFast, EtherSwitch, Event Center, Explorer, Follow Me Browsing, GainMaker, iLYNX, IOS, iPhone, IronPort, the IronPort logo, Laser Link, LightStream, Linksys, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, PCNow, PIX, PowerKEY, PowerPanels, PowerTV, PowerTV (Design), PowerVu, Prisma, ProConnect, ROSA, SenderBase, SMARTnet, Spectrum Expert, StackWise, WebEx, and the WebEx logo are registered trademarks of Cisco and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1002R)

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.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

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—Administrator Portal Guide, Release 1.1

Part: CCAMCP-CNAP-Admin1-1.1

CONTENTS

Preface

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

Useful Microsoft Windows Azure Pack References

The following sources may provide useful information about Microsoft WAP:

- WAP Wiki—Source for general information on Microsoft WAP
  http://social.technet.microsoft.com/wiki/contents/articles/20689.the-azure-pack-wiki-wapack.aspx
- Building Clouds Blog—Maintained by the Windows Server & System Center Customer Advisory Team.
  - Overview of WAP on the blog
    http://blogs.technet.com/b/privatecloud/archive/2013/12/20/building-clouds-windows-azure-pack-blog-post-overview.aspx
  - Installing and Configuring Series
    http://blogs.technet.com/b/privatecloud/archive/2013/12/06/windows-azure-pack-installing-amp-configuring-series.aspx
  - Troubleshooting Installation and Configuration of WAP—Introduction
    http://blogs.technet.com/b/privatecloud/archive/2013/11/05/troubleshooting-configuration-of-windows-azure-pack.aspx
- PLA—Important as the IaaS Fabric and Fabric Management PLAs are the root source for SPRA and Fast Track.
  - Overview
    http://blogs.technet.com/b/privatecloud/archive/2014/04/28/iaas-product-line-architecture-available-for-download.aspx
  - Deployment Guide
    https://gallery.technet.microsoft.com/Infrastructure-as-a-ecf1cc0b
  - Cisco Fast Track—Provides extensive step-by-step instructions
    http://www.cisco.com/c/en/us/solutions/data-center-virtualization/microsoft-applications-on-cisco-ucs/index.html

Useful Product Documentation

- Cisco Adaptive Security Appliance 5585 (Cisco ASA 5585)
  http://www.cisco.com/c/en/us/products/security/asa-5500-series-next-generation-firewalls/index.html
- Cisco Aggregation Services Router—Cisco ASR 9000 and Cisco ASR 1000
  - Cisco ASR 9000
    http://www.cisco.com/c/en/us/products/routers/asr-9000-series-aggregation-services-routers/index.html
  - Cisco ASR 1000
    http://www.cisco.com/c/en/us/products/routers/asr-1000-series-aggregation-services-routers/index.html
- Cisco Application Centric Infrastructure (Cisco ACI)
  http://www.cisco.com/c/en/us/solutions/data-center-virtualization/application-centric-infrastructure/index.html
- Cisco Application Policy Infrastructure Controller (Cisco APIC)
  http://www.cisco.com/c/en/us/products/cloud-systems-management/application-policy-infrastructure-controller-apic/index.html

- Cisco Cloud Services Router 1000V (Cisco CSR 1000V)
  http://www.cisco.com/c/en/us/products/routers/cloud-services-router-1000v-series/index.html
- Cisco Network Services Orchestrator (Cisco NSO)
  http://www.cisco.com/c/en/us/products/cloud-systems-management/network-services-orchestrator/index.html
- Cisco Nexus 9000
  http://www.cisco.com/c/en/us/products/switches/nexus-9000-series-switches/index.html
- Citrix NetScaler VPX
  https://www.citrix.com/products/netscaler-application-delivery-controller/platforms.html

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 host and offer sophisticated tenant network containers over a Cisco cloud infrastructure, enabling tenants to deploy multi-tier applications in the cloud. The provisioning of such containers is enabled by the use of the Cisco Advance Data Center Network Resource Provider in the Microsoft Windows Azure Pack Portals. Cisco Cloud Network Automation Provisioner (CNAP) software includes the Cisco Advance Data Center Resource Provider component, which exposes the Cisco infrastructure resources to the:

- Service Provider Cloud Admin to publish plans that offer complex network containers
- Tenant to use the subscriptions to instantiate the network containers and, using the VMClouds Resource Provider, deploy tenant workloads and attach to tenant Virtual networks

A Microsoft WAP administrator can use the Cisco CNAP 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 Admin Portal

You can use the Admin Portal for:

- Global operations:

  - Configure global settings for each system and each cloud.
  - Manage network devices and end points, including view detailed information about a network device, add a network device, and delete a network device. You can also view information about the devices that are added as part of tenant container creation.
  - Manage IP addresses and IP subnets, including add a new IP subnet, unallocate an IP subnet, and remove an IP subnet.
  - Manage VLANs, including add a new VLAN range, make a VLAN range and specific VLAN pool available, unallocate a VLAN ID, and remove a VLAN range.
  - Manage access to Shared Services, such as Database as a Service (DBaaS), Disaster Recovery as a Service (DRaaS), etc., including add a Shared Service, modify a Shared Service, and remove a Shared Service.
  - Create container plans, configure them, and make them available so tenants can subscribe to them.
  - View tenant information.
- Tenant-specific operations:
  - Summary Tab—Review summary information about the container created, including WAN gateway, tier, and load balancer information. You can also delete a container.
  - Gateway Tab—Review the WAN gateway specific configuration applied to a tenant container. You can also add, modify, and remove a gateway from a tenant container.
  - Firewall Tab—Display and modify firewall information about a container.
  - Load Balancer Tab—Use this tab to acknowledge that a tenant has a licensed Citrix NetScaler VPX device.

Note In the current release, this is the only action that the admin can perform on the Admin Portal Load Balancer tab for SP-managed Citrix NetScaler VPX devices. The SP Admin will add license files to the tenant Citrix NetScaler VPX VMs either manually or by other methods and indicate to Cisco CNAP that licensing is completed.

Using Global Search on Admin Portal Tabs

All of the Admin Portal tabs have a **global search…** box that lets you search for specific items on the page you are currently on.

You can use global search to search for:

- An exact match—By default, when you type in a string, the system searches for an exact match.

  For example, if you want to search for:

  ```
  10.0.88.128
  ```

  Begin typing from the beginning of the string.
- A substring—If you want to search using only a part of a string, use an asterisk bracketed by periods (**.*.**) as a wild card search character.

  For example, if you want to search for:

  ```
  ASR1000
  ```

  You can type in the global search box:

```
ASR.*.0
```

Or if you want to search for:

```
SPFUri
```

You can type in the global search box:

```
s.*.i
```

Understanding the Interrelationship of Tasks Performed in the Admin and Tenant Portals

Certain tasks performed in the Admin and Tenant Portals are interdependent in that tasks must be completed in one portal before other tasks can be accomplished in the other portal. For example:

- Base container plans must be created in the Admin Portal before tenants can use the Tenant Portal to subscribe to them and create tenant containers.
- In the Tenant Portal, after a tenant subscribes to a plan and creates a container, then in the Admin Portal the admin can confirm that the newly-created tenant container is Active and configure the following for it:
  - WAN Gateway—When a tenant is creating a container for a plan to which they have subscribed, they see a screen indicating whether the plan includes entitlement for a WAN Gateway (e.g., MPLS VPN). If it does, they see a message to contact their cloud provider to activate the connection to the WAN Gateway. Once the tenant container is active, the admin can then configure the WAN Gateway in the Admin Portal. A firewall is created by default the moment you create a WAN Gateway. For more information, see Setting Up a WAN Gateway in Chapter 5, "Managing Container Plans."
  - Firewall—When a tenant is creating a container for a plan to which they have subscribed, they 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 in the Admin Portal. Each Tier and the Layer 3 VPN is considered a zone. 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. A firewall can be configured in either the Admin Portal or the Tenant Portal, however it can only be configured after the tenant has created a container and the admin has created a WAN Gateway. For more information, see Understanding Firewall Creation in Chapter 5, "Managing Container Plans."
  - Load Balancer—The only operation that can be performed in the Admin Portal related to setting up a server load balancer (SLB) is acknowledging that the Citrix NetScaler VPX is licensed. The remaining configuration is performed in the Tenant Portal. For more information, see Setting Up a Server Load Balancer in Chapter 5, "Managing Container Plans" and *Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Tenant Portal Guide, Release 1.1*.

Prerequisites for Using Cisco Cloud Network Automation Provisioner

Before you can use the Admin Portal to provision IaaS containers using Cisco CNAP, you **must**:

- Build the data center infrastructure (see the next section).
- Configure specific services that are supported by the Cisco Cloud Architecture for the Microsoft Cloud Platform architecture, such as Infrastructure as a Service (IaaS) with Zinc Container, Database as a Service (DBaaS), Disaster Recovery as a Service (DRaaS), etc. You must set up these services before you use Cisco CNAP to configure access to them. For more information, see Configuring Specific Services in Chapter 4, "Developing Container Plans."

Note For detailed information on the Cisco CNAP prerequisites, you should consult *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).

Build the Data Center Infrastructure

Container plans are built using a pool of resources. A Cloud Service Provider (CSP) builds this pool of resources—the data center infrastructure—which is then used to offer services to tenants.

The Cisco Cloud Architecture for Microsoft Cloud Platform (CCA MCP) base infrastructure is the foundation on which a variety of cloud services are offered. The base infrastructure consists of a set of physical components that implement compute, storage, and data center networking. These data center devices are set up, connected, and configured prior to adding tenant services.

Tenant services are offered using these physical resources and provisioned and managed using Cisco CNAP automation software to enable consumption of these services. When tenants are on boarded, cloud containers are created that provide a slice of resources from the pool that include compute, storage, and networking. This container is securely isolated from other tenants that are consuming similar services, thereby providing isolation for multi-tenant services.

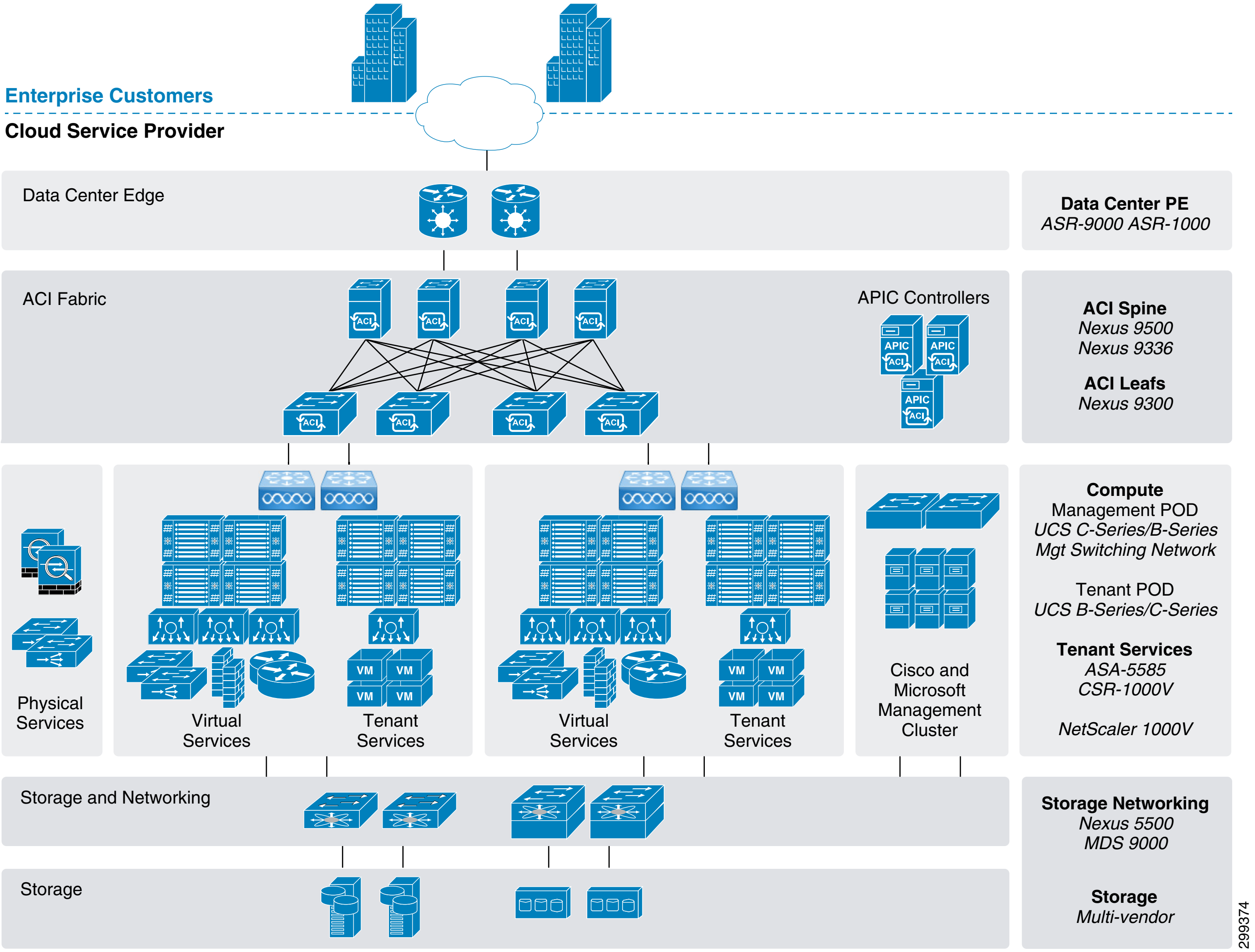
Refer to the *Cisco Cloud Architecture for the Microsoft Cloud Platform: Infrastructure Foundation Guide, Release 1.0* for detailed information on building data centers using physical components to implement compute, storage, and data center networking to create a pool of resources that are then used to offer services to tenants.

The CCA MCP architecture is built using a layered approach that enables a modular design, which lets you deploy a scalable solution with expansion capability that can be added in modular units. The *Cisco Cloud Architecture for the Microsoft Cloud Platform: Infrastructure Foundation Guide, Release 1.0* describes the following layers as well as specific implementation details:

- Data center network
- Compute for tenant workloads
- Storage and SAN
- Service tiers and differentiated services
- Cloud management

The following reference topology provides a view of the components and connections used.

Figure 1-1 CCA MCP Architecture Components



The *Cisco Cloud Architecture for the Microsoft Cloud Platform: Infrastructure Foundation Guide, Release 1.0* covers:

- Base infrastructure overview and considerations
- CCA MCP hardware and software components and component licensing
- Base infrastructure implementation details

Prerequisites for Creating Network Container Plans and Containers

Before you can use the Admin Portal for provisioning container plans, you **must**:

- Configure global settings for the system and for each cloud.
- Build the pool of available cloud resources.

These steps are summarized here and described in detail later in this document.

To build the pool of cloud resources, you:

- Configure data center devices, including adding, in the Cisco CNAP Admin Portal, a Cisco Network Services Orchestrator Enabled by Tail-f, a Cisco ASR 9000 or ASR 1000, and a Cisco APIC.

  If you are going to configure access to Shared Services, such as DBaaS, DRaaS, etc., you should add a Cisco Adaptive Security Appliance 5585 (Cisco ASA 5585) firewall to be used as the security access point to the Shared Services.
- Configure network pools and address pools, including:
  - VLANs, including adding a new VLAN range, making a VLAN range and specific VLAN pool available, unallocating a VLAN ID, and removing a VLAN range.

Note You **must** configure the VLAN pool which will be used for WAN gateway configuration. This VLAN range is needed when the PE router is managed from Cisco CNAP. If the WAN PE router is managed outside of Cisco CNAP, it is considered a VLAN hand-off use case and an onboarding a range is not mandatory.

  - IP addresses and IP subnets, including adding and configuring the IP subnets to be used for management connectivity, infrastructure, NAT, and tiers. You can also unallocate an IP subnet and remove an IP subnet.
- You can also configure access to Shared Services, such as Database as a Service (DBaaS), Disaster Recovery as a Service (DRaaS), etc., that you want to be available as options when you are creating and configuring network container plans. You can add a Shared Service, modify a Shared Service, and remove a Shared Service.

Accessing the Admin Portal

You access the Admin Portal from the WAP Admin site.

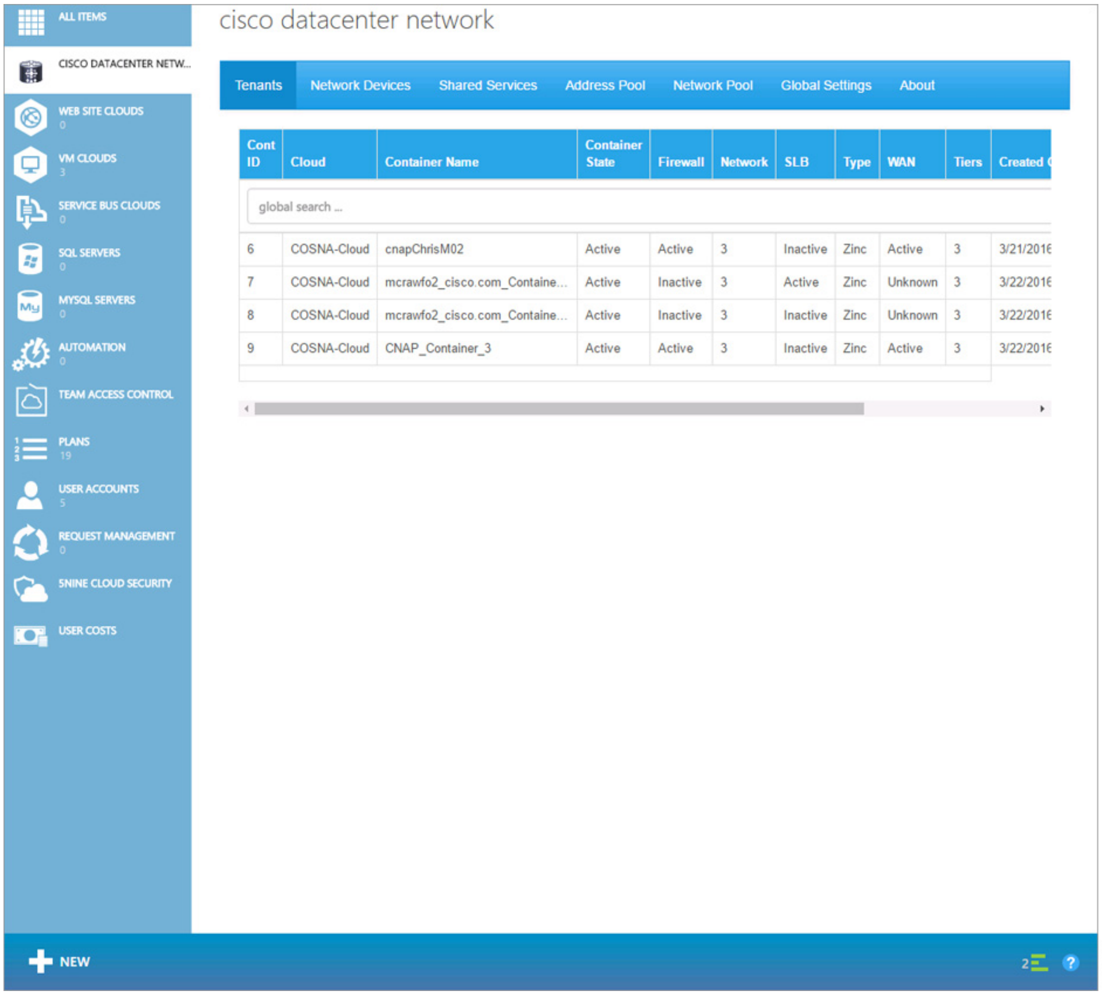
Step 1 Access the WAP Admin Site and log in as an administrator.

For information on accessing WAP, see the WAP documentation.

Step 2 In the WAP Admin Site, in the left column, click **Cisco Datacenter Network**.

You see the main Cisco Datacenter Network screen, which is the Tenants tab, as shown in the following screen.

Figure 1-2 Tenants Tab Screen



Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created (
6	COSNA-Cloud	cnapChrisM02	Active	Active	3	Inactive	Zinc	Active	3	3/21/2016
7	COSNA-Cloud	mcrawfo2_cisco.com_Containe...	Active	Inactive	3	Active	Zinc	Unknown	3	3/22/2016
8	COSNA-Cloud	mcrawfo2_cisco.com_Containe...	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/22/2016
9	COSNA-Cloud	CNAP_Container_3	Active	Active	3	Inactive	Zinc	Active	3	3/22/2016

CHAPTER 2

Configuring Global System and Cloud Settings

Note You typically perform the first two steps below as part of the post-installation set up procedures for Cisco CNAP. For more information, see the section Post-installation Set Up Procedures in *Installing Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 1.1*.

- In the Admin Portal, configure Global Settings for the System (**only required once**).
- Start the Cisco.Network.Provisioner Windows Service, which after a new installation creates the Cloud database.
- In the Admin Portal, configure Global Settings for each Cloud.
- Restart the Cisco.Network.Provisioner Windows Service, which loads the configuration changes to Cisco CNAP service.

Note Each time you make changes to global system or cloud settings, you must restart the Cisco.Network.Provisioner Windows Service for the updated settings to take effect.

Configuring Global Settings for the System

Note You typically perform this step as part of the post-installation set up procedures for Cisco CNAP. For more information, see the section Post-installation Set Up Procedures in *Installing Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 1.1*.

Caution Every time you install Cisco CNAP, the database is recreated. To preserve your data, you should always backup your database before reinstalling Cisco CNAP.

By setting these parameters, you enable Cisco CNAP to communicate with components in the data center, such as the Cisco NSO, SPF, VMM, etc.

Before you begin configuring global settings, complete the steps in the following sections as you will need this information to complete some fields:

- Creating the Cisco CSR 1000V Template Used by Cisco CNAP
- Creating the Citrix NetScaler VPX Template Used by Cisco CNAP

Creating the Cisco CSR 1000V Template Used by Cisco CNAP

To create the Cisco CSR 1000V template:

Step 1 Obtain a supported Cisco CSR 1000V ISO image.

Step 2 Copy the ISO image into the library ISO location of the targeted VMM and refresh the library.

Step 3 Create a virtual machine with a blank virtual hard disk using the following configuration parameters (if not specified, the default configuration will be used):

- General hardware configuration:
  - One (1) CPU

Note You can configure two (2) or four (4) CPUs. Cisco CNAP supports only one template and all Cisco CSR 1000Vs will be instantiated from the one template. See: http://www.cisco.com/c/en/us/products/collateral/routers/cloud-services-router-1000v-series/datasheet-c78-733443.html.

  - 4 GB memory
- Hardware bus configuration:
  - Virtual hard disk type is fixed and size is 8GB
  - Virtual DVD driver connecting to the Cisco CSR 1000V ISO you provided
- Hardware network adapters configuration:
  - Add seven (7) additional network adapters and change all eight (8) adapters' MAC addresses to static.
- Advanced hardware configuration:
  - Enable high availability and set priority to **High**.
  - Change CPU priority to **High**.
  - Change Memory weight to **High**.

Step 4 Boot the virtual machine and follow the prompt to create a default (blank) configuration for the Cisco CSR 1000V.

Step 5 Shut down the virtual machine and disconnect the ISO image from the virtual machine virtual DVD driver.

Step 6 In VMM, convert the virtual machine into a virtual machine template.

Creating the Citrix NetScaler VPX Template Used by Cisco CNAP

To create the Citrix NetScaler VPX template:

Step 1 Download the Citrix NetScaler Virtual Appliance setup files:

a. In a web browser, go to http://www.citrix.com and click **My Citrix**.

b. Type your username and password.

c. Click **Downloads**.

d. In search downloads by Product, select **NetScaler**.

e. Under Virtual Appliances, click **Netscaler VPX**.

f. Copy the compressed file to your server.

Step 2 Create the template:

a. Extract the contents of the compressed file.

b. There is a folder for Virtual Hard Disks that contains the VHD file, which by default is named “dynamic”. You can rename it.

c. Copy the VHD to the VMM library.

d. Refresh the VMM library and ensure you see the new VHD.

e. Right-click the VHD and select **Create VM Template**.

f. Set the number of processor to two (2).

g. Set the RAM to 2048.

h. Be default there is only one network adapter. Add one more. The first network adapter is used for management connectivity and the second one is used for the data path.

i. Change all adapters’ (two total) MAC addresses to static.

j. Set the VM to Highly Available.

k. Finish the creation process.

In summary, you create a virtual machine template with the VHD file using the following configuration parameters (if not specified, the default configuration will be used):

- General hardware configuration:
  - Two (2) CPUs
  - 2 GB memory
- Hardware network adapters configuration:
  - Add one (1) additional network adapter and change all two (2) adapters' MAC addresses to static.
- Advanced hardware configuration:
  - Enable high availability and set priority to **High**.
  - Change CPU priority to **High**.
  - Change Memory weight to **High**.

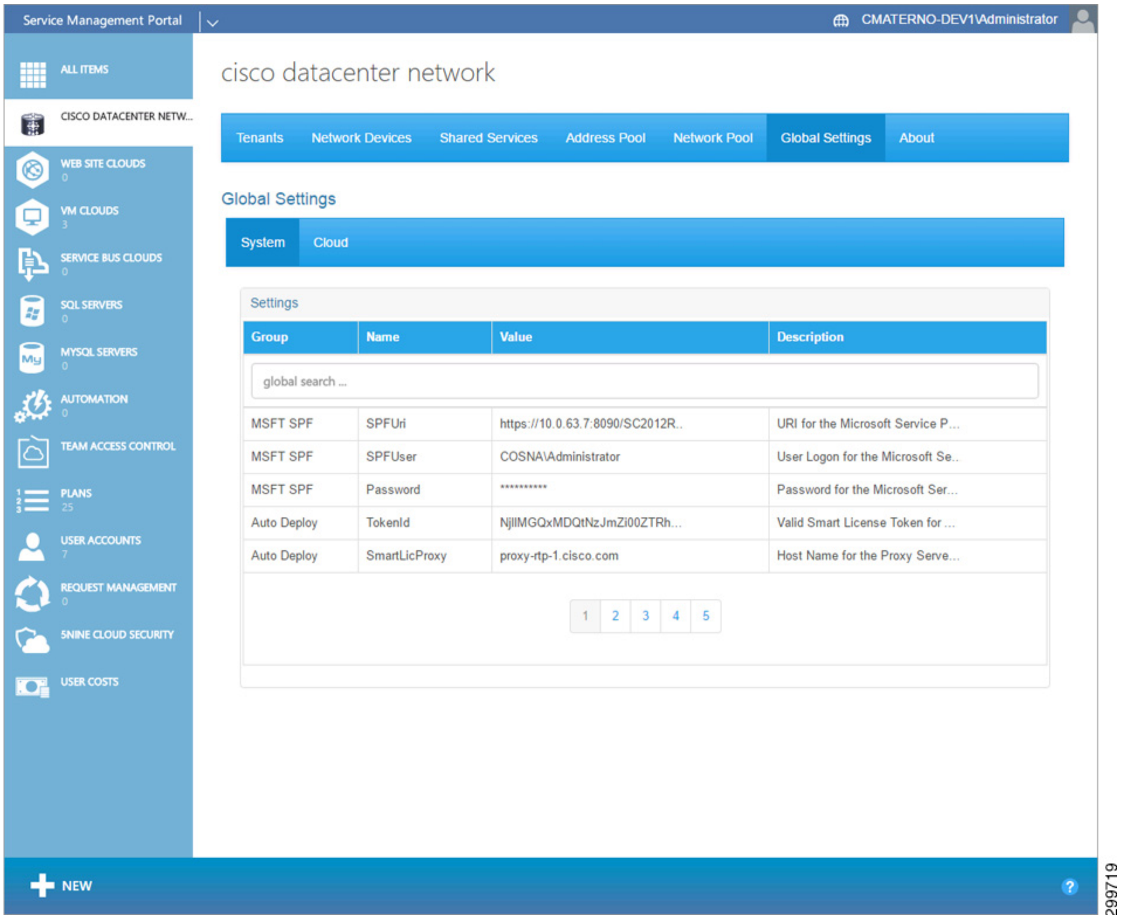
Configuring Global System Settings

Note You only need to perform this step once.

Step 1 On the Tenants list screen, click the **Global Settings** tab.

You see the Global System Settings screen, as shown in the following screen.

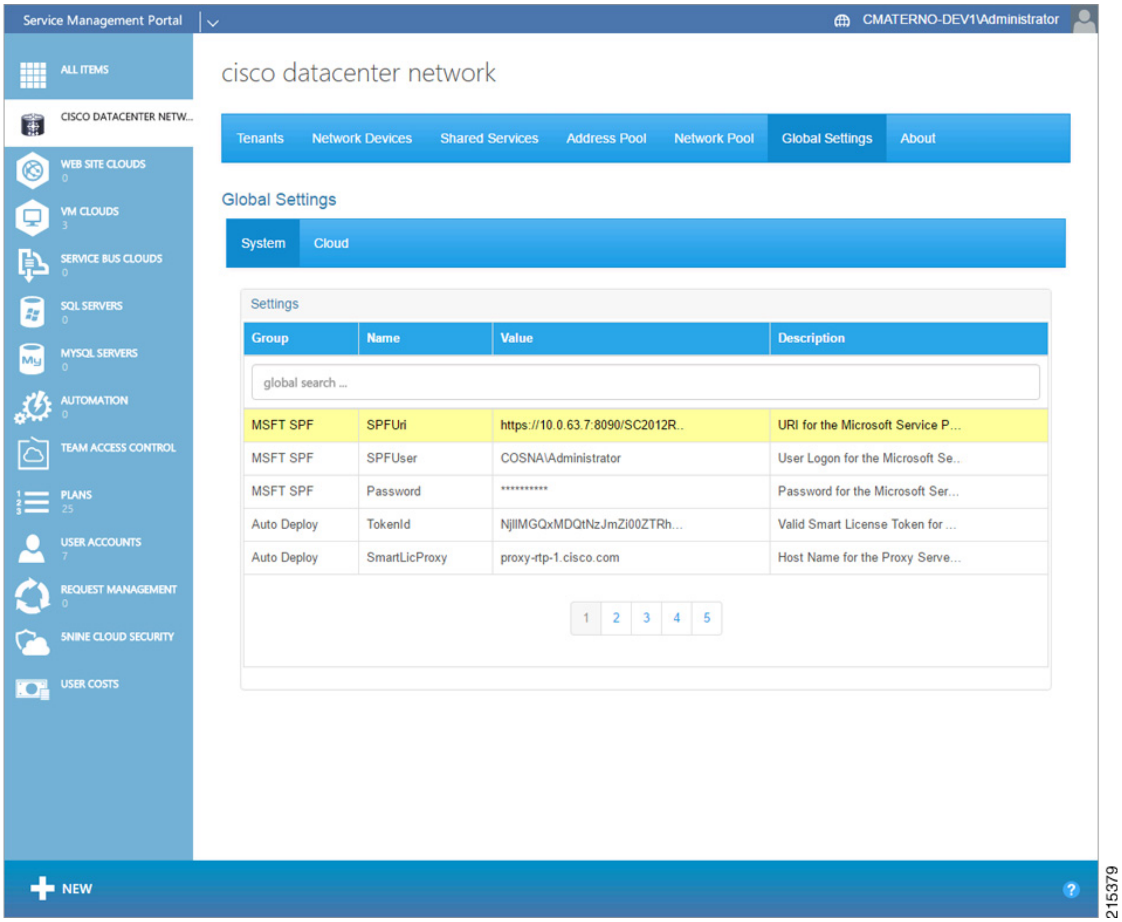
Figure 2-1 Global System Settings Screen



Group	Name	Value	Description
MSFT SPF	SPFUri	https://10.0.63.7:8090/SC2012R..	URI for the Microsoft Service P...
MSFT SPF	SPFUser	COSNA\Administrator	User Logon for the Microsoft Se..
MSFT SPF	Password	**********	Password for the Microsoft Ser...
Auto Deploy	TokenId	NjllMGQxMDQtNzJmZi00ZTRh...	Valid Smart License Token for ...
Auto Deploy	SmartLicProxy	proxy-rtp-1.cisco.com	Host Name for the Proxy Serve...

Step 2 Move the cursor over the first row of the settings table and the row is highlighted, as shown in the following screen.

Figure 2-2 Global System Settings Screen—Row Highlighted

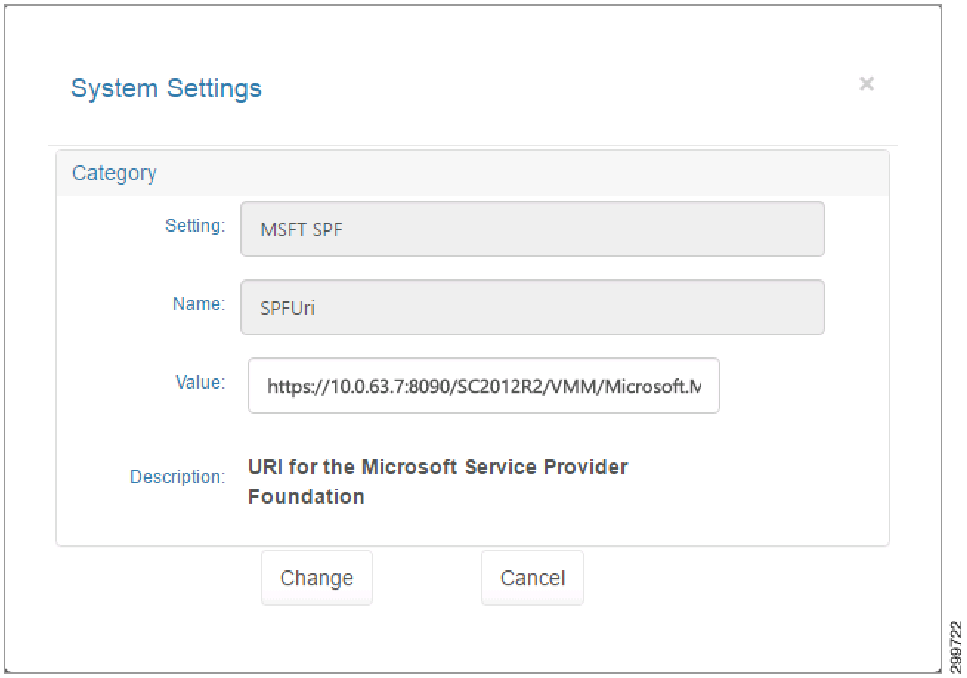


Group	Name	Value	Description
MSFT SPF	SPFUri	https://10.0.63.7:8090/SC2012R..	URI for the Microsoft Service P...
MSFT SPF	SPFUser	COSNA\Administrator	User Logon for the Microsoft Se..
MSFT SPF	Password	**********	Password for the Microsoft Ser...
Auto Deploy	TokenId	NjllMGQxMDQtNzJmZi00ZTRh...	Valid Smart License Token for ...
Auto Deploy	SmartLicProxy	proxy-rtp-1.cisco.com	Host Name for the Proxy Serve...

Step 3 Click the highlighted row.

You see a pop-up window, as shown in the following screen.

Figure 2-3 Global System Settings Screen—Parameter Pop-up Window



System Settings

Category

Setting: MSFT SPF

Name: SPFUri

Value: https://10.0.63.7:8090/SC2012R2/VMM/Microsoft.M

Description: URI for the Microsoft Service Provider Foundation

Step 4 You can specify or change the value for the parameter. When you are finished, click **Change**. Click **Cancel** to return to the previous screen without entering/changing any values.

Step 5 Highlight each row in turn and specify or change the value for each parameter in the pop-up windows. When you are finished with the parameters on the first screen, click **2** at the bottom of the screen to see the next set of values.

There are four screens where you can specify/change System Global Settings. Table 2-1 describes the various fields and their possible values.

Table 2-1 Global System Settings

Group	Name	Sample Values[1]	Description
MSFT SPF	SPFUri	https://{*spf-server-name*}:8090/SC2012/{provider-service}/{subscription-id}/Microsoft.Management.Odata.svc/	URI for the Microsoft Service Provider Foundation
MSFT SPF	SPFUser	*<domain>\<user name>*	User logon for the Microsoft Service Provider Foundation
MSFT SPF	Password	*********	Password for the Microsoft Service Provider Foundation
Auto Deploy	TokenID	<Token-string>	Valid Smart License Token for Cisco CRS1000V auto deployment
Auto Deploy	SmartLicProxy		Host Name for the Proxy Server Used for Smart Licensing Validation
Auto Deploy	SmartLicProxyPort		TCP Port for the Proxy Server Used for Smart Licensing Validation
Auto Deploy	PSHost	*n.n.n.n*	FQN/IP Address of System Center VMM Host
Auto Deploy	PSUser	*<domain>\<user name>*	User Logon for the Microsoft System Center VMM
Auto Deploy	PSPassword		Password for the Microsoft System Center VMM
Auto Deploy	CSRVmTemplateName	csr1000vfixeddisk	Name of the Cisco CSR 1000V VM Template. For more information, see Creating the Cisco CSR 1000V Template Used by Cisco CNAP.
Auto Deploy	NSVmTemplateName	netscaler1000vfixeddisk	Name of the Citrix NetScaler VPX VM Template. For more information, see Creating the Citrix NetScaler VPX Template Used by Cisco CNAP.
Auto Deploy	ISODestinationFolder	vmm Library on VMM management Server For example: VMMServ-er01\SEALibrary	Folder at the System Center VMM Host to hold Post deployment ISOs
Auto Deploy	CSRUser	admin	Administrator User Logon set at BOOTSTRAP of the Cisco CSR 1000V
Auto Deploy	CSRPassword	********	Administrator Password set at BOOTSTRAP of the Cisco CSR 1000V. You can change the password when initially defining global settings. Follow good security practices to set a secure password. However once you have onboarded devices, you **cannot** change the password since that will cause container creation to fail.
Auto Deploy	NSUser	nsroot	Administrator User Logon at BOOTSTRAP of the Citrix NetScaler VPX
Auto Deploy	NSRPassword	******	Administrator Password set at BOOTSTRAP of the Citrix NetScaler VPX

Table 2-1 Global System Settings

Auto Deploy	VMMgmtNetworkName	MgmtVL0046VMNetwork	VMNetwork used for management of the Cisco CSR 1000s and Citrix NetScaler VPXs. This is not the Logical Switch.
Auto Deploy	NameServer	10.0.43.10	Name Server Address for Virtual Network Devices
Auto Deploy	MgmtDomain	vmdc-cosn.cisco.com	Domain name defined on the Management Network
Auto Deploy	VMConfigFileFolder	C:\CNAPTemp\	This directory must be created before creating containers; if this directory is not present, container creation will fail. Directory on the Admin Portal server where the Cisco CSR 1000V and Citrix NetScaler VPX ISOs are created before they are copied to the Microsoft SCVMM. The default is "c:\temp\". If you change the default, ensure that you include a trailing "\" on the end of the path name.
Auto Deploy	SyslogServer	10.0.63.231	Syslog Server address for Virtual Network Devices.

[1] The values shown are examples. Use values appropriate for your cloud environment.

Starting the Cisco.Network.Provisioner Windows Service

Note You typically perform this step as part of the post-installation set up procedures for Cisco CNAP. For more information, see the section Post-installation Set Up Procedures in *Installing Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 1.1*.

The Cisco.Network.Provisioner Windows Service is installed as part of the Cisco CNAP installation process, however it is not started automatically since the Global System settings **must** first be set.

At this point, starting the Cisco.Network.Provisioner Windows Service loads all the global settings into the Cisco CNAP backend orchestrator and creates the Cloud record(s).

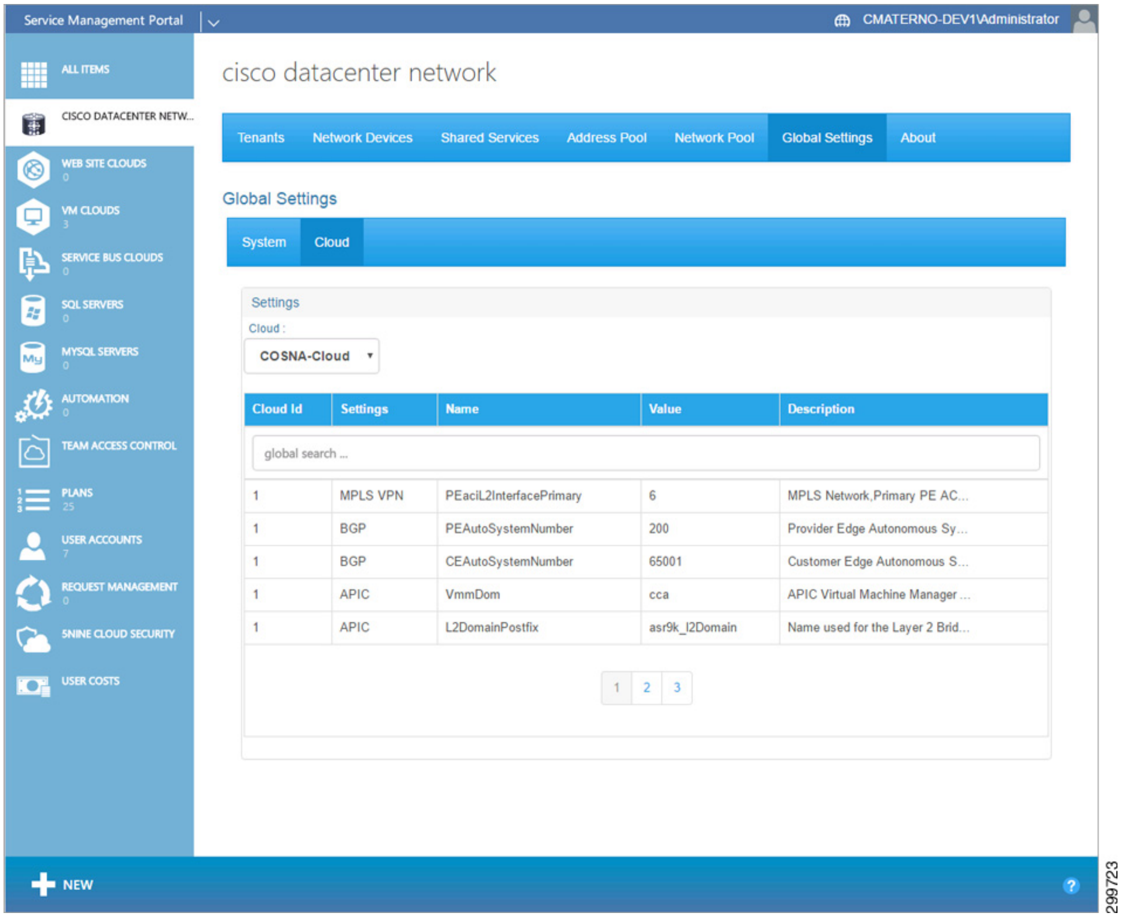
Locate and start the Cisco.Network.Provisioner Windows Service.

Configuring Global Settings for Each Cloud

Step 1 To configure the global settings for each cloud, on the Global Settings screen, click the **Cloud** tab.

You see the Global Cloud Settings screen, as shown in the following screen.

Figure 2-4 Global Cloud Settings Screen



Cloud : COSNA-Cloud

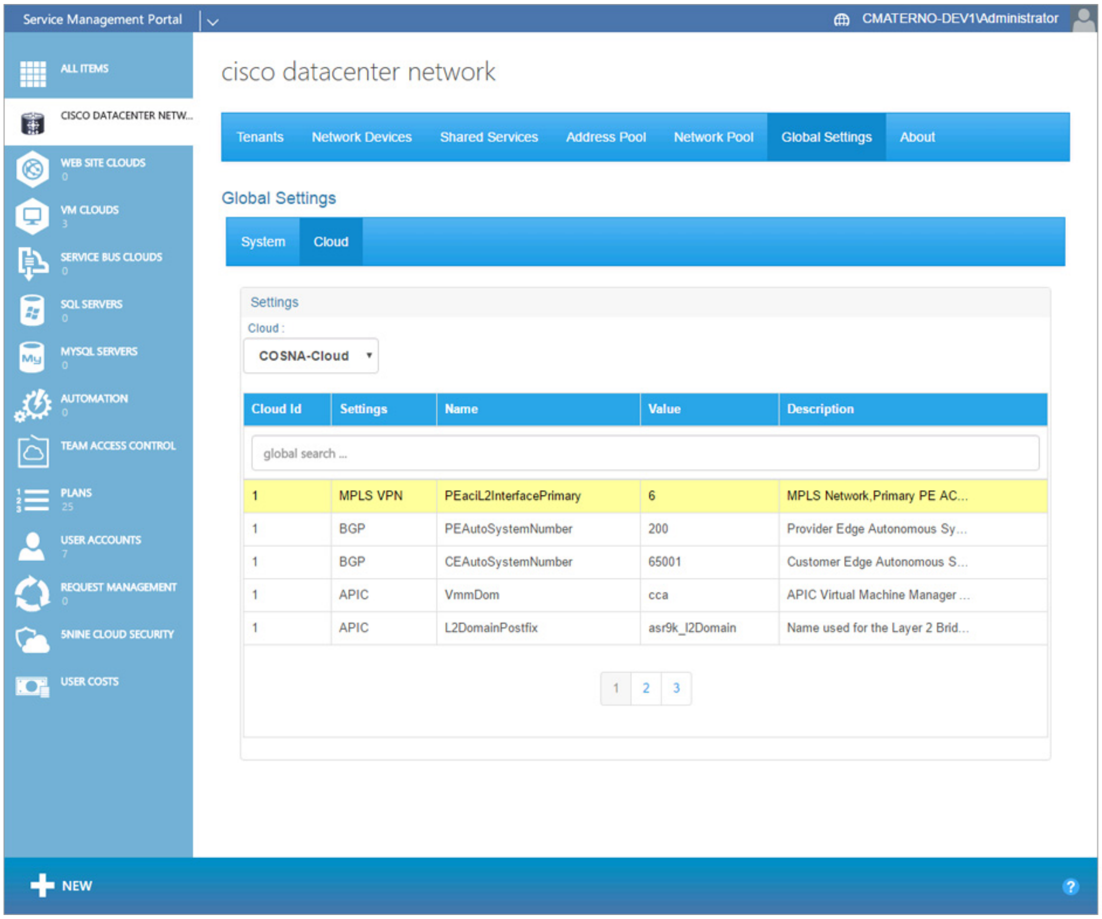
Cloud Id	Settings	Name	Value	Description
1	MPLS VPN	PEaciL2InterfacePrimary	6	MPLS Network,Primary PE AC...
1	BGP	PEAutoSystemNumber	200	Provider Edge Autonomous Sy...
1	BGP	CEAutoSystemNumber	65001	Customer Edge Autonomous S...
1	APIC	VmmDom	cca	APIC Virtual Machine Manager ...
1	APIC	L2DomainPostfix	asr9k_l2Domain	Name used for the Layer 2 Brid...

Step 2 Click the **Cloud:** pull-down menu to select the cloud for which you want to specify settings.

Note The list of displayed clouds is obtained from the Microsoft System Center Service Provider Foundation Server. The clouds from the SC VMMs appear in this list. The cloud selected will be used to deploy the network services VMs, such as the Cisco CSR 1000V and Citrix NetScaler VPX. Note that there are also network attributes that are modeled as Cloud Global Settings, such as the PEAutoSystemNumber, etc. to allow different data center networks to be used per cloud.

Step 3 Move the cursor over the first row of the settings table and the row is highlighted, as shown in the following screen.

Figure 2-5 Global Cloud Settings Screen—Row Highlighted

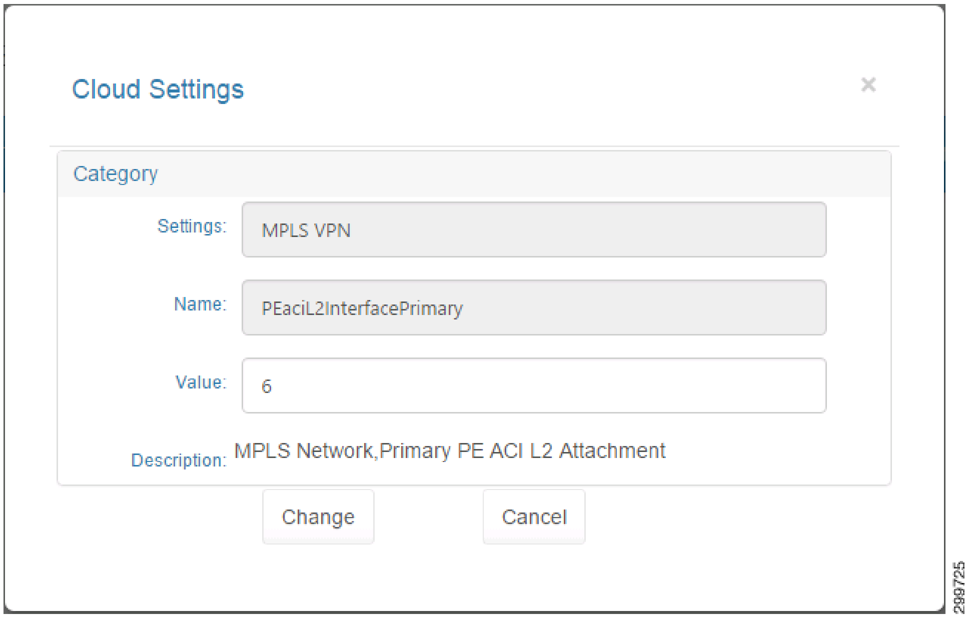


Cloud Id	Settings	Name	Value	Description
1	MPLS VPN	PEaciL2InterfacePrimary	6	MPLS Network,Primary PE AC...
1	BGP	PEAutoSystemNumber	200	Provider Edge Autonomous Sy...
1	BGP	CEAutoSystemNumber	65001	Customer Edge Autonomous S...
1	APIC	VmmDom	cca	APIC Virtual Machine Manager ...
1	APIC	L2DomainPostfix	asr9k_l2Domain	Name used for the Layer 2 Brid...

Step 4 Click the highlighted row.

You see a pop-up window, as shown in the following screen.

Figure 2-6 Global Cloud Settings Screen—Parameter Pop-up Window



Cloud Settings

Category

Settings: MPLS VPN

Name: PEaciL2InterfacePrimary

Value: 6

Description: MPLS Network,Primary PE ACI L2 Attachment

Step 5 You can specify or change the value for the parameter. When you are finished, click **Change**. Click **Cancel** to return to the previous screen without entering/changing any values.

Step 6 Highlight each row in turn and specify or change the value for each parameter in the pop-up windows. When you are finished with the parameters on the first screen, click **2** at the bottom of the screen to see the next set of values.

There are three screens where you can specify or change Cloud Global Settings. Table 2-2 describes the various fields and their possible values.

Table 2-2 Global Cloud Settings

Cloud ID	Settings	Name	Sample Values[1]	Description
1	MPLS VPN	PEaciL2InterfacePrimary	5	Bundle-Ethernet or Port-channel interface on the PE connecting to the Cisco ACI Fabric. For the Cisco ASR 9000, the value is in the range <1-65535> For the Cisco ASR 1000, the value is the range <1-64>. **Note** In the current Cisco CNAP release, this value is used on both PE devices. Make sure to use the same interface number when pre-provisioning the PE devices.
1	BGP	PEAutoSystemNumber	200	Provider Edge Autonomous System Number.
1	BGP	CEAutoSystemNumber	65001	Customer Edge Autonomous System Number.
1	APIC	VmmDom	cca	Cisco APIC Virtual Machine Manager (VMM) Domain. The VMM domain is located in the Cisco APIC GUI under **VM Networking** –> **Inventory** –> **Microsoft**.
1	APIC	L2DomainPostfix	asr9k-l2domain	Name used for the Layer 2 Bridge Domain in the Cisco APIC. In the Cisco APIC GUI, navigate to **Fabric** –> **Access Policies** –> **Physical and External Domains** –> **External Bridge Domains** and select the domain that is assigned to the VLAN pool corresponding to the Network pool defined in Cisco CNAP.
1	APIC	L2extPathNode1	101	Cisco ACI Leaf Node 1 ID which is part of the vPC to PE router. In the Cisco APIC GUI, navigate to **Fabric** –> **Inventory** –> **Fabric Membership** to view the node ID of all switches in the Cisco ACI fabric.
1	APIC	L2extPathNode2	102	Cisco ACI Leaf Node 2 ID which is part of the vPC to PE router. In the Cisco APIC GUI, navigate to **Fabric** –> **Inventory** –> **Fabric Membership** to view the node ID of all switches in the Cisco ACI fabric.

Table 2-2 Global Cloud Settings

1	APIC	L2extIntPath1	vpc_n101_n102_asr9k_pe1	Policy Group name for the vPC connecting the Cisco ACI leaf pair to PE1. In the Cisco APIC GUI, navigate to **Fabric** –> **Access Policies** –> **Interface Policies** –> **Profiles** and select the interface profile corresponding to the vPC. Use the Policy Group name associated with this interface profile.
1	APIC	L2extIntPath2	vpc_n101_n102_asr9k_pe2	Policy Group name for the vPC connecting the Cisco ACI leaf pair to PE2.
1	MPLS VPN	PEacilL2InterfaceSecondary		Bundle-Ethernet or Port-channel interface on PE2 connecting to the Cisco ACI Fabric. **Note** This value is not used in the current Cisco CNAP release.
1	APIC	VmmCntrl	cca-scvmm	Cisco APIC Virtual Machine Manager (VMM) Controller defined under the VmmDom (VMM Domain) described above. The VMM controller name is located in the Cisco APIC GUI under **VM Networking** –> **Inventory** –> **Microsoft** –> *<domain>* –> **Controllers**.
1	Shared Service	SharedServiceVmNetwork	SharedSvcVMNetwork	Specify the pre-configured VM network for Shared Services with a manually-provisioned PE.
1	Shared Service	SharedServiceASAContextName	Shared-SVC-FW	Specify the pre-configured Cisco ASA context Name for Shared Services with a manually-provisioned PE.

1. The values shown are examples. Use values appropriate for your cloud environment.

Restarting the Cisco.Network.Provisioner Windows Service

At this point, restarting the Cisco.Network.Provisioner Windows Service loads the configuration changes into the Cisco CNAP backend orchestrator.

Locate and restart the Cisco.Network.Provisioner Windows Service.

CHAPTER 3

Building the Pool of Available Cloud Resources

You have to add a variety of resources to Cisco CNAP to form the pool of devices and addresses that you can use in your clouds. This involves:

- Configuring Data Center Devices
- Configuring Network Pools and Configuring Address Pools

  You use Cisco CNAP to specify your IP addressing scheme details so that those IP addresses, VLAN pools, subnets, etc. are available during container creation.

  You must specify:

  – The VLAN ranges and their associated VLAN pools that you will be utilizing when creating network plans. When you add a VLAN range, Cisco CNAP populates the VLAN pool.

  – How IP subnets and their associated IP address pools will be utilized, such as for Infrastructure, Management, NAT, Shared Services, or Tier.

You can also configure access to Shared Services, such as Database as a Service (DBaaS), Disaster Recovery as a Service (DRaaS), etc., that you want to be available as options when you are creating and configuring network container plans. For more information, see Configuring Access to Shared Services.

Note Since Cisco CNAP is also pushing configurations for the automation of work flows on devices, certain precautions need to be followed when manually configuring devices to avoid disrupting Cisco CNAP-based automation. Changing configurations pushed from Cisco CNAP will cause the automated provisioning system to malfunction, which in some cases could cause all automated provisioning to stop until the error conditions are manually remediated. In general on the data center provider edge, all configurations under the tenant VRFs pushed by Cisco CNAP should not be edited or changed, including sub-interfaces and routing. Similarly on the Cisco APIC, the Cisco APIC tenants configured by Cisco CNAP should only be changed by Cisco CNAP. Any configurations pushed by Cisco CNAP should not be manually edited. For more information, see *Installing Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 1.1*.

Configuring Data Center Devices

You add network devices to form the pool of infrastructure resources available to a cloud. Network devices are associated with a specific cloud. In the current release, only one cloud is supported.

Note Enter device information carefully. In the current release, you cannot modify device information once you have added it. If you want to make changes after you have added a device, you must delete the device and add it again.

You must initially add the following three devices before you can perform network provisioning:

- Cisco Network Services Orchestrator Enabled by Tail-f
- Cisco Aggregation Services Router—Cisco ASR 9000 or Cisco ASR 1000 (WAN Gateway)

Note If you are manually provisioning WAN Edge/PE, you do not have to add a Cisco ASR 9000 or ASR 1000. For more information on manual provisioning, see Understanding the Difference Between Auto-provisioning and Manually Provisioning WAN Gateways in Chapter 5, "Managing Container Plans."

- Cisco Application Policy Infrastructure Controller (APIC)—SDN switching fabric

Note *Before* you add the Cisco APIC, you **must** create a directory to store the Cisco APIC configurations. As the admin user (or ensure the admin user has read and write access to the directory), create the directory:
/home/admin/cisco-apicdc

If you are going to configure access to Shared Services, such as DBaaS, DRaaS, etc., you should add a:

- Cisco Adaptive Security Appliance 5585 (Cisco ASA 5585) firewall to be used as the security access point to the Shared Services. The firewall context defined on the Cisco ASA 5585 **must** be preconfigured. For more information, see *Cisco Cloud Architecture for the Microsoft Cloud Platform: Infrastructure Foundation Guide, Release 1.0*.

You can also delete devices if necessary. Virtual network devices that are created by Cisco CNAP are displayed but cannot be deleted.

Adding a Cisco Network Services Orchestrator Enabled by Tail-f

You should have performed this step as part of the Cisco CNAP installation because the Cisco NSO should be the first network device you add.

For more information, see the section Connecting Cisco Cloud Network Automation Provisioner to the Cisco Network Services Orchestrator in *Installing Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 1.1*.

Adding a Cisco ASR, Cisco APIC, and Cisco ASA 5585

After you add the Cisco NSO, the next two devices you should add are:

- Cisco Aggregation Services Router—Cisco ASR 9000 or Cisco ASR 1000 (WAN Gateway)
- Cisco Application Policy Infrastructure Controller (APIC)—SDN switching fabric

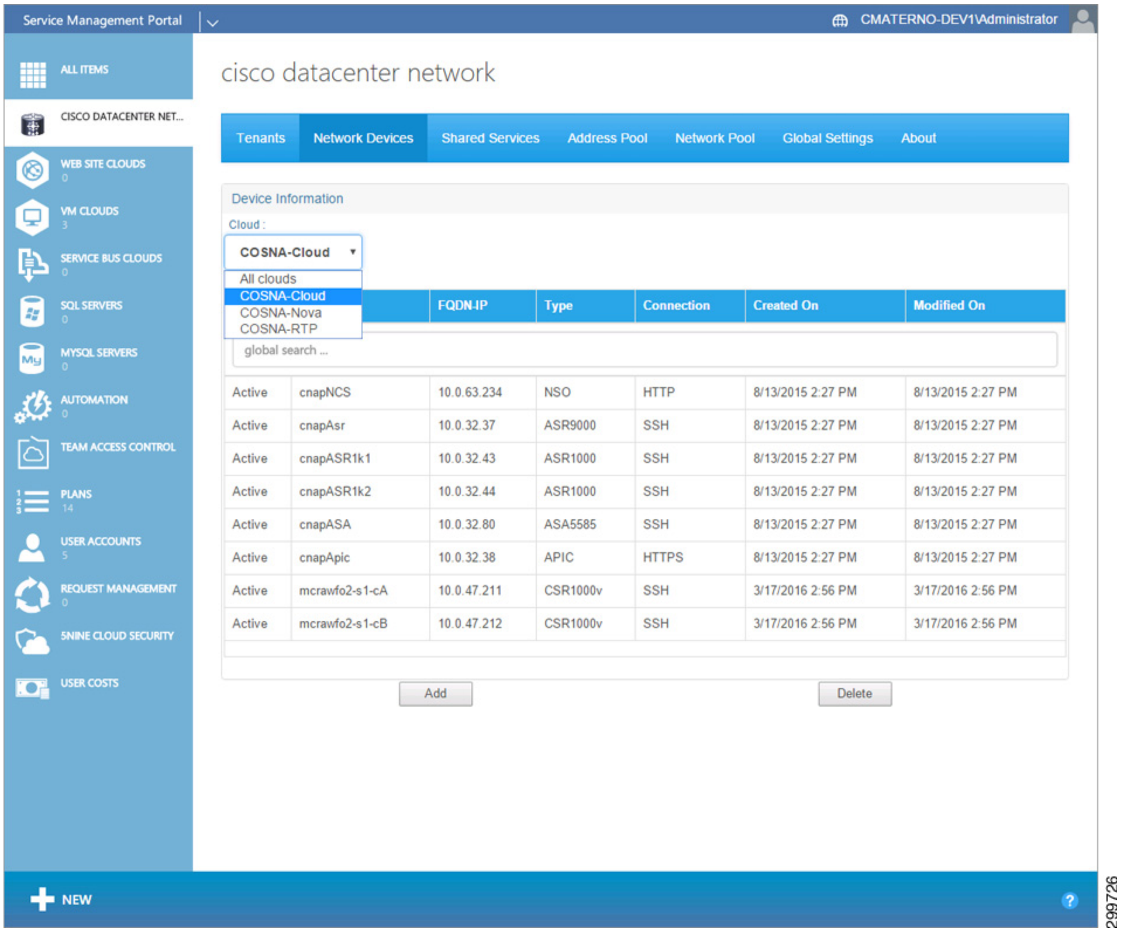
Note *Before* you add the Cisco APIC, you **must** create a directory to store the Cisco APIC configurations. As the admin user (or ensure the admin user has read and write access to the directory), create the directory: /home/admin/cisco-apicdc

Note When used with Cisco CNAP, the Cisco APIC cluster should be front-ended by a Server Load Balancer (SLB) and you should set up an HTTPS bridging session, which allows registration of one IP address on Cisco CNAP for the Cisco APIC cluster (basically the SLB VIP). Cisco CNAP expects a single IP address for the Cisco APIC cluster, which may have three or more nodes.

To add a Cisco ASR and Cisco APIC:

Step 1 On the Network Devices Tab screen, in the Cloud drop-down, click the cloud service to which you want to add a device, as shown in the following screen.

Figure 3-1 Network Devices Tab Screen



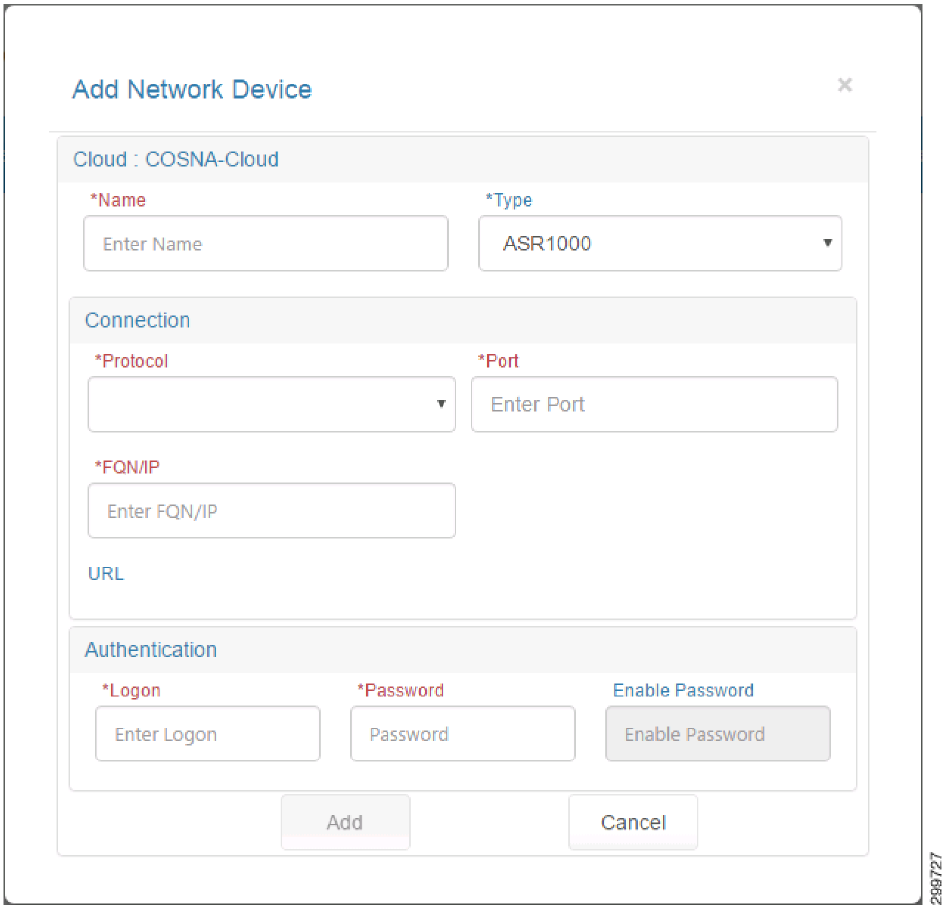
Cloud : COSNA-Cloud

		FQDN-IP	Type	Connection	Created On	Modified On
Active	cnapNCS	10.0.63.234	NSO	HTTP	8/13/2015 2:27 PM	8/13/2015 2:27 PM
Active	cnapAsr	10.0.32.37	ASR9000	SSH	8/13/2015 2:27 PM	8/13/2015 2:27 PM
Active	cnapASR1k1	10.0.32.43	ASR1000	SSH	8/13/2015 2:27 PM	8/13/2015 2:27 PM
Active	cnapASR1k2	10.0.32.44	ASR1000	SSH	8/13/2015 2:27 PM	8/13/2015 2:27 PM
Active	cnapASA	10.0.32.80	ASA5585	SSH	8/13/2015 2:27 PM	8/13/2015 2:27 PM
Active	cnapApic	10.0.32.38	APIC	HTTPS	8/13/2015 2:27 PM	8/13/2015 2:27 PM
Active	mcrawfo2-s1-cA	10.0.47.211	CSR1000v	SSH	3/17/2016 2:56 PM	3/17/2016 2:56 PM
Active	mcrawfo2-s1-cB	10.0.47.212	CSR1000v	SSH	3/17/2016 2:56 PM	3/17/2016 2:56 PM

Step 2 Click **Add**.

You see the Add Network Device screen.

Figure 3-2 Add Network Device Screen



Add Network Device

Cloud : COSNA-Cloud

*Name: Enter Name

*Type: ASR1000

Connection

*Protocol:

*Port: Enter Port

*FQN/IP: Enter FQN/IP

URL

Authentication

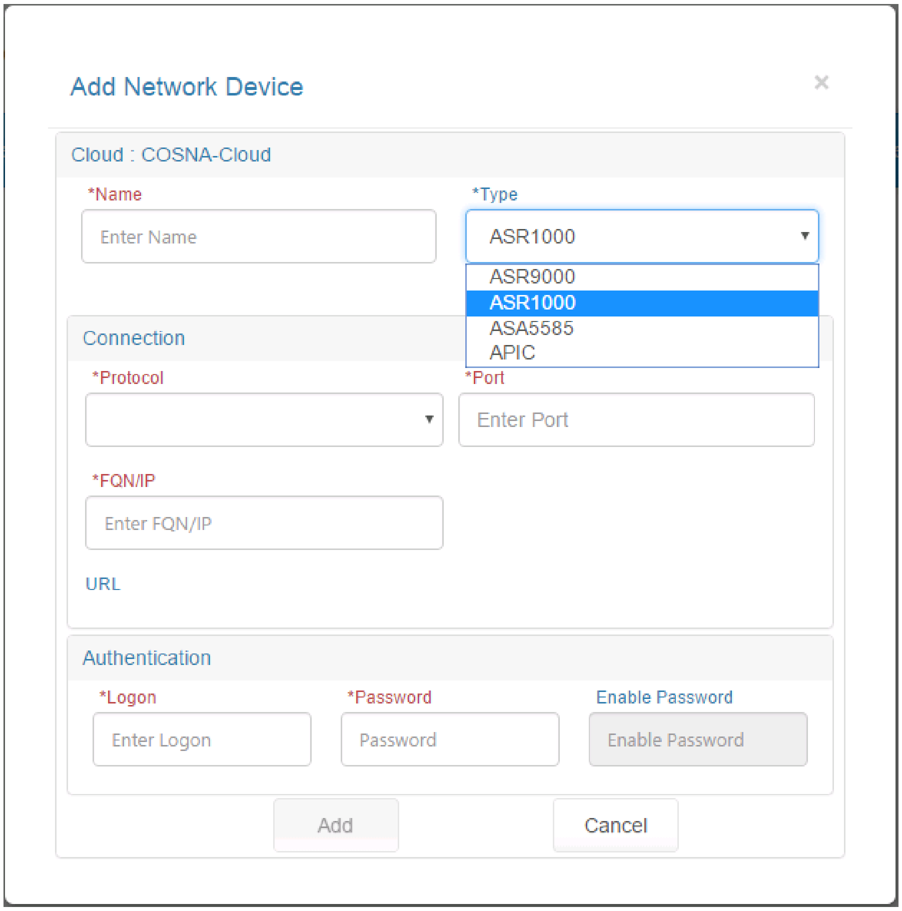
*Logon: Enter Logon

*Password: Password

Enable Password: Enable Password

The Type pull-down menu displays the devices you can add, as shown in the following screen.

Figure 3-3 *Add Network Device Screen—Type Pull-down Menu*



Add Network Device

Cloud : COSNA-Cloud

*Type: ASR1000

Step 3 Cloud: *Cloud Name* displays the Cloud Service to which the Network Device will be associated. Complete the following fields:

- Name—User-defined name given to the Network Device.
- Type—Device type: On the pull-down menu, select **ASR9000**, **ASR1000**, or **APIC**, depending on what device you are adding. The Cisco ASA 5585 (**ASA5585**) is also an option if you are going to configure access to Shared Services.
- Connection:
  - Protocol—Protocol used to connect to the device: SSH, HTTP, or HTTPS
  - Port—Port used to establish the connection to the device.
  - FQDN/IP—IP Address or FQN given to the Network Device at the Providers Network. Fully Qualified Name or Valid IP address in dotted format. Characters, numbers, and "-". (The period [.] is also used in DNS names, but only between DNS labels and at the end of an FQDN.) https://technet.microsoft.com/en-us/library/cc959336.aspx
- Authentication:
  - Login—Service Account Logon used to establish a connection with the Network Device.
  - Password—Service account password.
  - Enable Password—If the device you are adding has an enable password that is different than the device password, enter it here. Otherwise the device password will be used for enable mode.

Step 4 Click **Add** to add the network device or **Cancel** to cancel the addition.

Step 5 Repeat the procedure for the other device(s) you **must** add, such as a Cisco ASR 9000, Cisco ASR 1000, Cisco ASR 5585, or Cisco APIC.

Deleting a Network Device

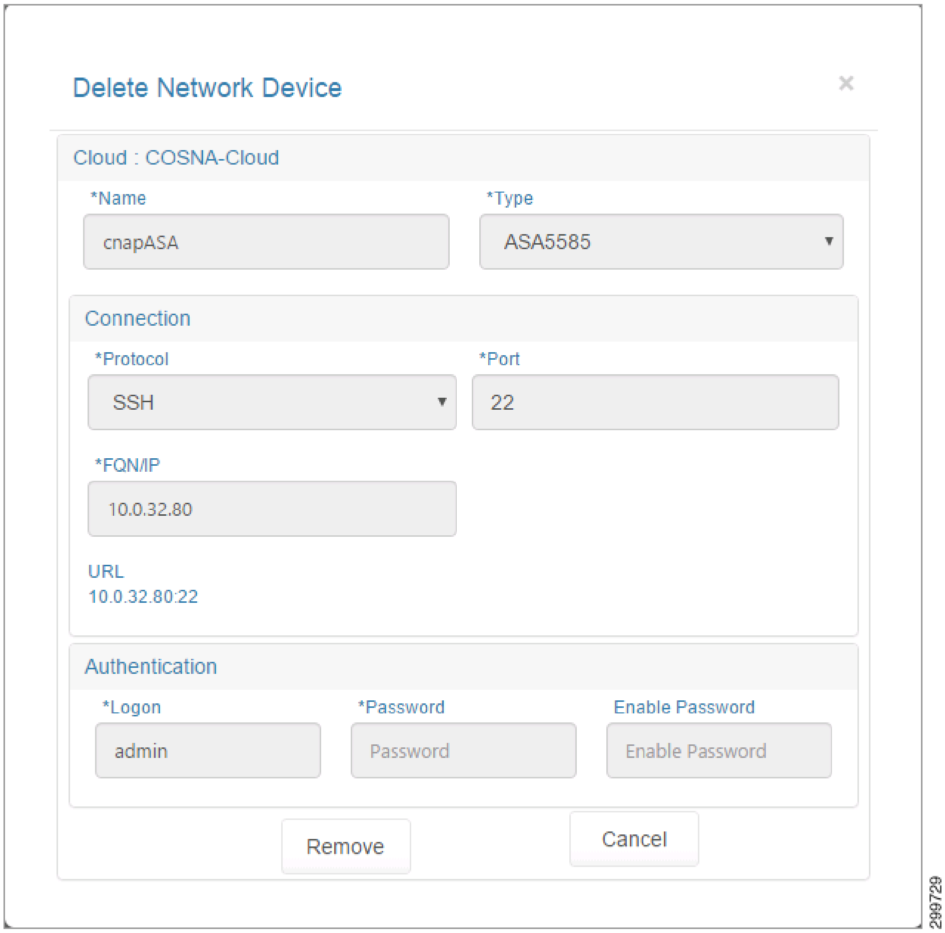
Step 1 On the Network Devices Tab Screen, in the Cloud tree on the left, click the cloud service containing the device you want to delete.

Note You can delete an existing Network Device only if the device is not being used by a network container, irrespective of whether the device is Active or Inactive.

Step 2 Click the specific device you want to delete, then click the **Delete** button.

You see the Delete Network Device screen.

Figure 3-4 Delete Network Device Screen



Delete Network Device

Cloud : COSNA-Cloud

*Name: cnapASA
*Type: ASA5585

Connection

*Protocol: SSH
*Port: 22
*FQN/IP: 10.0.32.80
URL
10.0.32.80:22

Authentication

*Logon: admin
*Password: Password
Enable Password: Enable Password

Step 3 Click **Remove** to remove the network device or **Cancel** to cancel the deletion.

Configuring Network Pools

You must specify the VLAN ranges and their associated VLAN pools that you will be utilizing when creating network plans. When you add a VLAN range, Cisco CNAP populates the VLAN pool.

For example, when you create a WAN Gateway, Cisco CNAP will acquire a VLAN ID from the VLAN pool and mark it as allocated.

On the Network Pool tab, you can:

- Add VLAN Ranges to the available Cloud resources.
- Once added, manage the VLAN ranges and VLAN IDs.

Important Considerations When Configuring Network Pools

You **must** take into consideration the following configuration requirements and recommendations:

- You **must** add a VLAN pool for the Cisco ASR 9000 or ASR 1000 with the same range as the VLAN pool defined on the Cisco APIC for use with the Cisco ASR 9000 or ASR 1000. On the Cisco APIC, the VLAN pool for the Cisco ASR 9000 or ASR 1000 should be assigned to a Physical Domain so it can be used to configure the trunk between the Cisco ASR 9000 or ASR 1000 and the Cisco APIC.
- It is recommended to use separate VLAN pools in Cisco CNAP for auto-provisioned and manually-provisioned WAN Edge/PEs. This lets you allocate and unallocate the VLANs for manually-provisioned WAN Edge/PEs separate from auto-provisioned WAN Edge/PEs, thereby eliminating overlapping VLAN issues. Cisco APIC, however, can use a single VLAN pool for auto-provisioned and manually-provisioned WAN Edge/PEs.

Managing Network Pools

You use the Network Pool tab to manage the VLANs that will be used during the orchestration of Network Containers. A group of VLANs make up each VLAN Range (on the Network Pool tab, the group of VLANs in a particular VLAN Range is also called the VLAN Pool). All of the VLAN Ranges collectively make up the Network Pool.

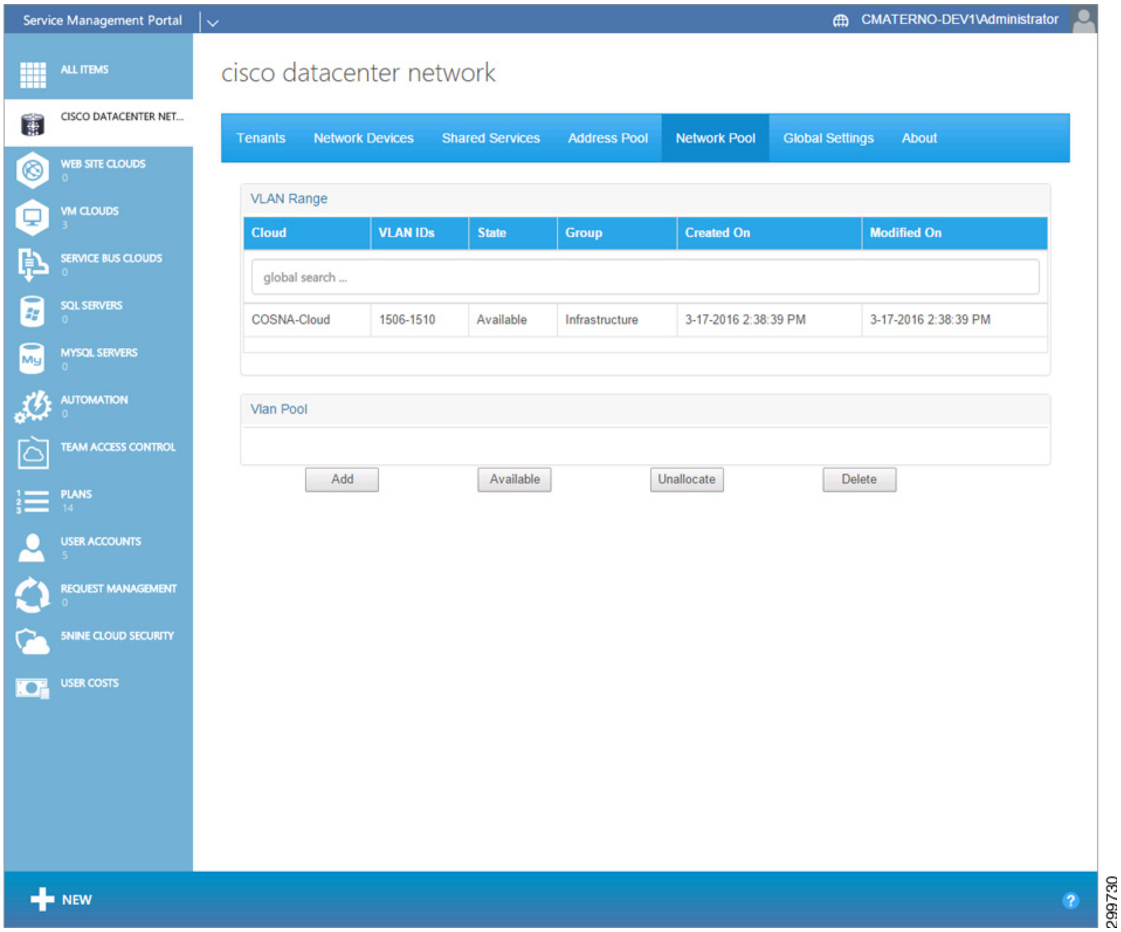
In the current release of Cisco CNAP, one VLAN Range must be created for WAN connectivity between data center PE routers and the Cisco ACI Fabric. Note that the VLAN Range entered into Cisco CNAP must be consistent with configurations on the Cisco ACI VLAN pools associated with the external interfaces to the data center PEs.

You can:

- Look at information about VLANs.
- Add a new VLAN Range.
- Mark a VLAN Range as available thereby automatically Unallocating all the VLANs in its VLAN Pool.
- Unallocate a VLAN ID.
- Remove a VLAN Range.

Viewing Information about VLANs

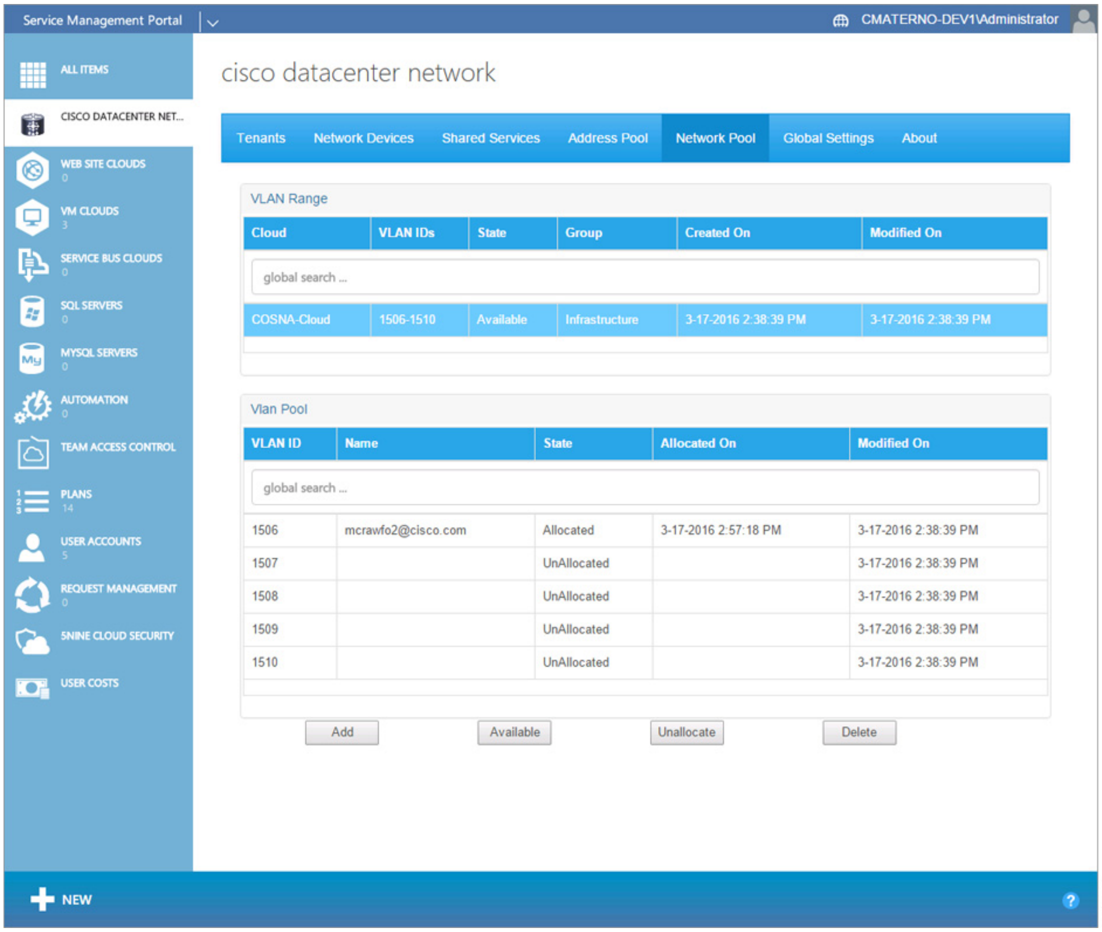
Figure 3-5 Network Pool Tab Screen



Cloud	VLAN IDs	State	Group	Created On	Modified On
COSNA-Cloud	1506-1510	Available	Infrastructure	3-17-2016 2:38:39 PM	3-17-2016 2:38:39 PM

If you click on a specific entry in the VLAN Range table, you see the associated VLAN Pool, as shown in the following screen.

Figure 3-6 VLAN Pool for Selected VLAN Range Screen



VLAN Range

Cloud	VLAN IDs	State	Group	Created On	Modified On
COSNA-Cloud	1506-1510	Available	Infrastructure	3-17-2016 2:38:39 PM	3-17-2016 2:38:39 PM

Vlan Pool

VLAN ID	Name	State	Allocated On	Modified On
1506	mcrawfo2@cisco.com	Allocated	3-17-2016 2:57:18 PM	3-17-2016 2:38:39 PM
1507		UnAllocated		3-17-2016 2:38:39 PM
1508		UnAllocated		3-17-2016 2:38:39 PM
1509		UnAllocated		3-17-2016 2:38:39 PM
1510		UnAllocated		3-17-2016 2:38:39 PM

The Network Pools tab contains the following:

- The VLAN Range table contains the following fields:
  - Cloud—Name of the cloud.
  - VLAN IDs—A range of VLAN IDs in the format: “Start Vlan ID - End Vlan ID”.
  - State—State of the VLAN Range, which is either Available or Unavailable. A VLAN Range is said to be Available when it still has VLANs that are not yet Allocated. The VLAN Range is marked Unavailable once all the constituent VLANs have been allocated.
  - Group—The VLAN Range group, which in the current release is Infrastructure for all VLANs. Infrastructure VLANs are used to “stitch” the provider edge (PE) to the customer edge (CE). In future releases, there may be container patterns that require these VLANs to be managed through Cisco CNAP by the user.
  - Created On—Date and time when the VLAN Range was created.
  - Modified On—Date and time when the VLAN Range was last modified.
- For the selected VLAN Range, the VLAN Pool table contains the following fields:
  - VLAN ID—Numeric value representing a VLAN.
  - Name—The Tenant Name.

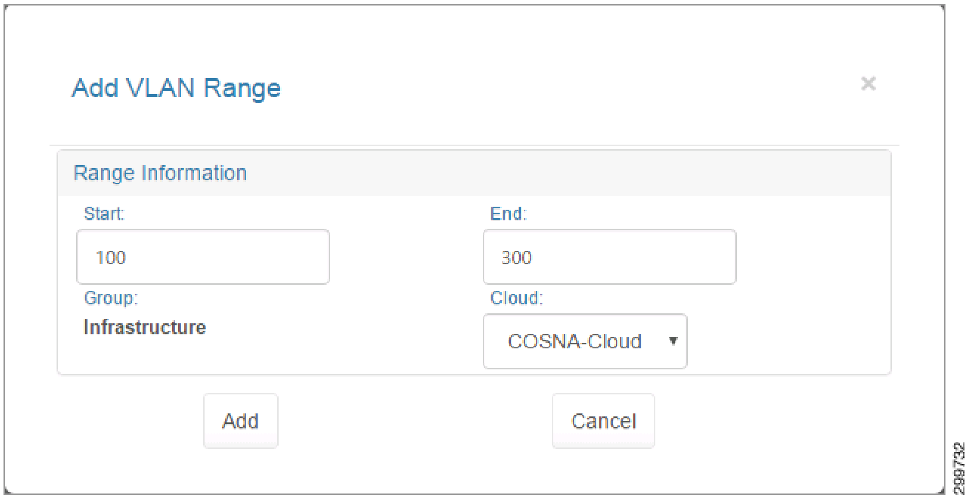
  - State—State of the VLAN, which is either Allocated or Unallocated. A VLAN will be marked "Unallocated" as long as it has not been used by any network component in the backend. Once it has been consumed by the network, the backend will mark it as "Allocated".
  - Allocated On—Date and time when the VLAN was allocated.
  - Modified On—Date and time when the VLAN was last modified.
- Add Button—Lets you add a new VLAN Range and its corresponding VLANs to the system.
- Available Button—**Should only be used for emergency clean up.** For example, if the system crashes and the configurations on the devices are corrupted or destroyed, but the database still reflects the VLAN Ranges as being unavailable. The Available button marks the selected VLAN Range as available and all the constituent VLANs as Unallocated. It does **not** decouple the constituent VLANs from the network components to which they may or may not be coupled (such as PE<—>CE stitching).
- Unallocate Button—**Should only be used for emergency clean up.** For example, if the system crashes and the configurations on the devices are corrupted or destroyed, but the database still reflects the VLANs as being Allocated. The Unallocate button marks the selected VLAN as Unallocated. It does **not** decouple the constituent VLANs from the network components to which they may or may not be coupled (such as PE<—>CE stitching).
- Delete Button—Lets you remove an existing VLAN Range from the system if it is not allocated to any tenant. and none of its VLANs are in the Allocated state.

Adding a New VLAN Range

Step 1 To add a new VLAN Range, select a Cloud in the VLAN Range table and click the **Add** button.

You see the Add VLAN Range screen.

Figure 3-7 Add VLAN Range Screen



Add VLAN Range

Range Information

Start: 100

End: 300

Group: Infrastructure

Cloud: COSNA-Cloud

Step 2 Enter information in the following fields:

- Range Info:
  - Start—The Starting VLAN ID on the Range. Enter a numeric value in the range [0,4096].
  - End—The Ending VLAN ID on the Range. Enter a numeric value in the range (Start, 4096].

  - Group—The VLAN Range group, which in the current release is Infrastructure for all VLANs. Infrastructure VLANs are used to "stitch" the provider edge (PE) to the customer edge (CE). In future releases, there may be container patterns that require these VLANs to be managed through Cisco CNAP by the user.
  - Cloud—Name of the Cloud Service given to it in SCVMM.
- VLAN Blocks:

Note If you use VLAN blocks, the range should be an exact multiple of the block size. For example, VLAN range 101-300, block size of 10.

  - Split Range in Blocks—Indicates whether or not the VLAN Range needs to be divided up into smaller VLAN Range blocks, which lets you add and delete in smaller blocks. If the value is true, then the VLAN Range defined by Start and End needs to be divided up into smaller VLAN Range blocks or else the VLAN Range will not be split.
  - Size—Total number of VLANs on each block. Enter a numeric value ≤ (End - Start).

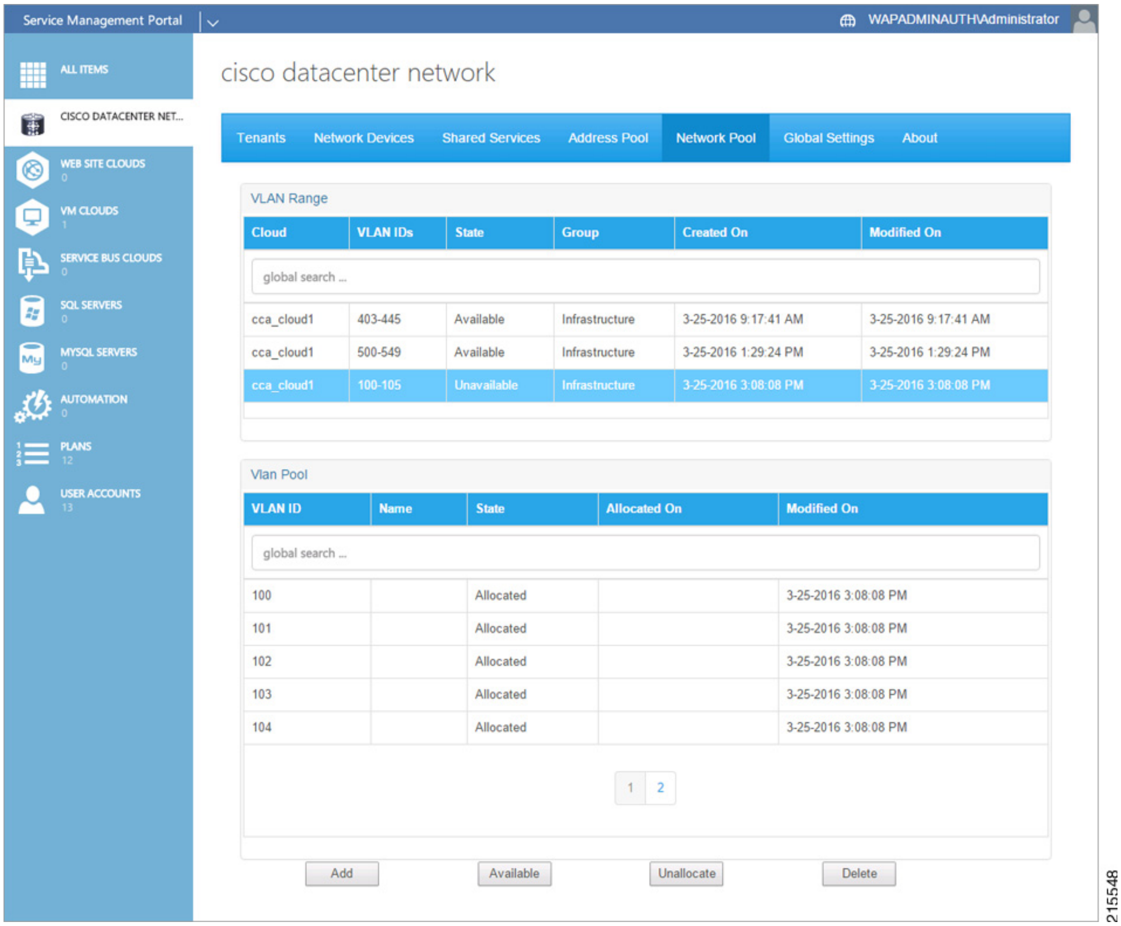
Step 3 Click **Add** to add the VLAN Range or **Cancel** to cancel the addition.

Making a VLAN Range and Specific VLAN Pool Available

Note New VLANs are Available by default. The **Available** button is active only if all the VLANs in a given range are allocated and the VLAN range itself is allocated.

Step 1 To make a VLAN Range and specific VLAN Pool available, on the Network Pool tab select a VLAN Range and a VLAN Pool, as shown in the following screen.

Figure 3-8 Select VLAN Range and Pool



VLAN Range

Cloud	VLAN IDs	State	Group	Created On	Modified On
cca_cloud1	403-445	Available	Infrastructure	3-25-2016 9:17:41 AM	3-25-2016 9:17:41 AM
cca_cloud1	500-549	Available	Infrastructure	3-25-2016 1:29:24 PM	3-25-2016 1:29:24 PM
cca_cloud1	100-105	Unavailable	Infrastructure	3-25-2016 3:08:08 PM	3-25-2016 3:08:08 PM

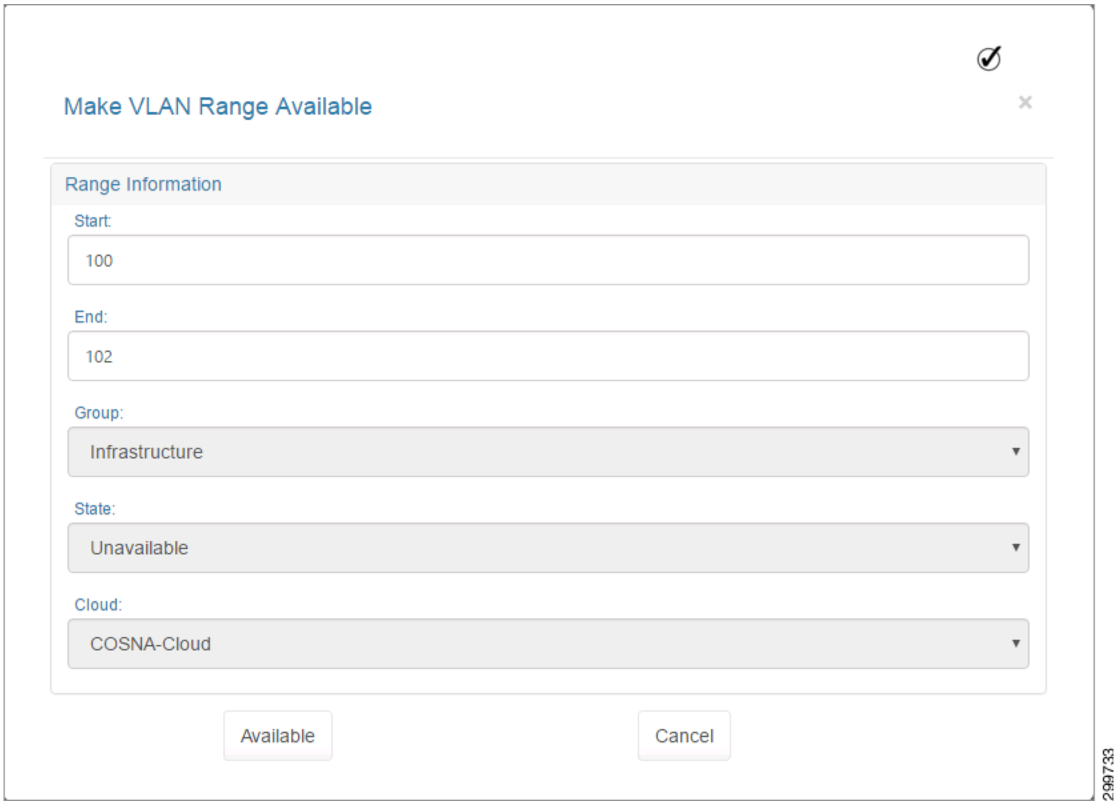
Vlan Pool

VLAN ID	Name	State	Allocated On	Modified On
100		Allocated		3-25-2016 3:08:08 PM
101		Allocated		3-25-2016 3:08:08 PM
102		Allocated		3-25-2016 3:08:08 PM
103		Allocated		3-25-2016 3:08:08 PM
104		Allocated		3-25-2016 3:08:08 PM

Step 2 Click **Available**.

You see the Make VLAN Range Available screen.

Figure 3-9 Make VLAN Range Available Screen



Make VLAN Range Available

Range Information

Start: 100

End: 102

Group: Infrastructure

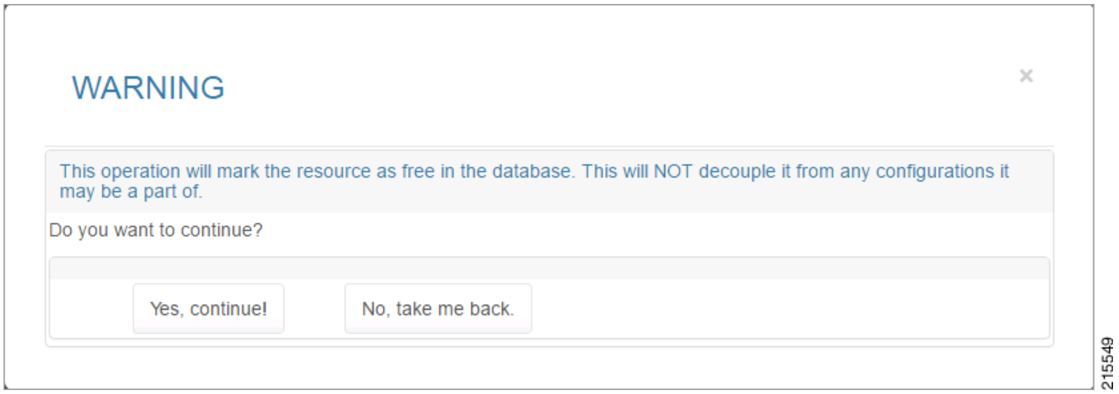
State: Unavailable

Cloud: COSNA-Cloud

Step 3 Click **Available** to make the VLAN Range available or **Cancel** to cancel the operation.

If you click **Available**, you see the following screen.

Figure 3-10 Make VLAN Range Available—Warning Screen



WARNING

This operation will mark the resource as free in the database. This will NOT decouple it from any configurations it may be a part of.

Do you want to continue?

Step 4 To make the VLAN Range available, click **Yes, continue!**

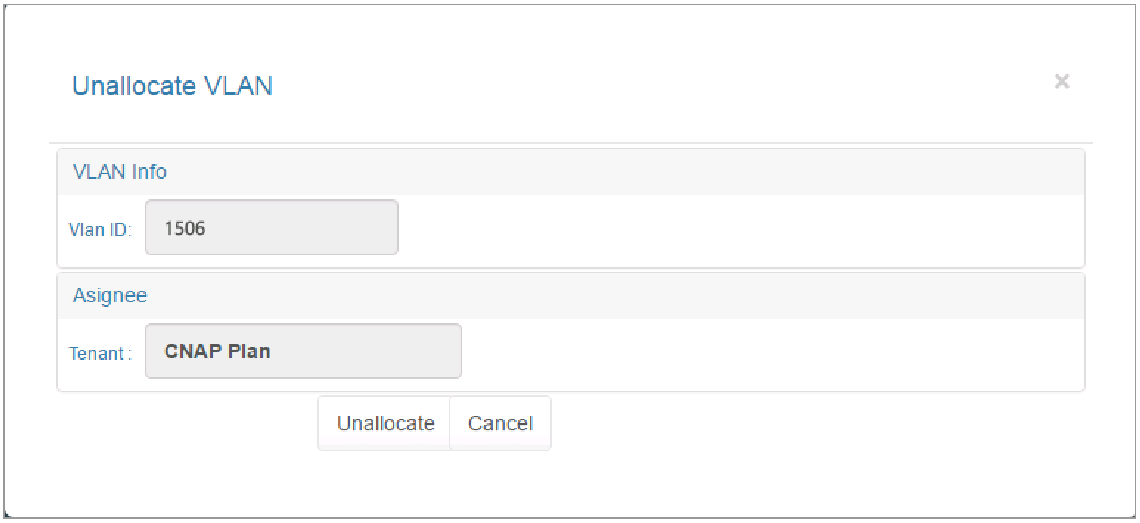
Unallocating a VLAN ID

Step 1 To unallocate a specific VLAN, on the Network Pool tab select a VLAN Pool, then click **Unallocate**.

Note On the Network Pools tab, you **cannot** de-couple a VLAN from the configurations in which it may be a part. Unallocating a VLAN merely resets a flag in the database and makes this VLAN available to Cisco CNAP. It does not actually remove it from any network configuration in which it may be a part.

You see the Unallocate VLAN screen.

Figure 3-11 Unallocate VLAN Screen



Unallocate VLAN

VLAN Info

Vlan ID: 1506

Asignee

Tenant : CNAP Plan

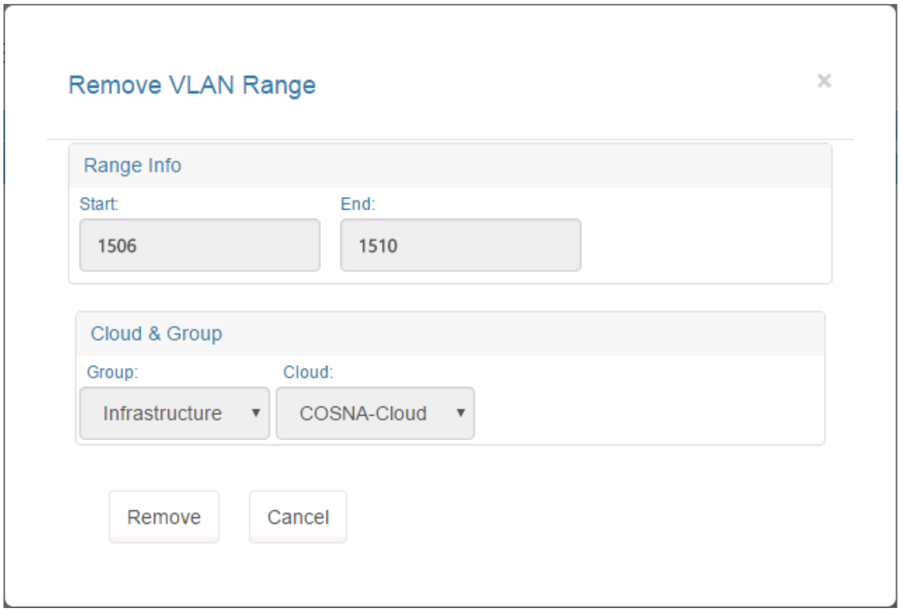
Step 2 Click **Unallocate** to unallocate the specified VLAN ID or **Cancel** to cancel the operation.

Removing a VLAN Range

Step 1 To remove a VLAN Range, on the Network Pool tab select a VLAN Range, then click **Delete**.

You see the Remove VLAN Range screen.

Figure 3-12 Remove VLAN Range Screen



Remove VLAN Range

Range Info

Start: 1506

End: 1510

Cloud & Group

Group: Infrastructure

Cloud: COSNA-Cloud

Step 2 Click **Remove** to remove the specified VLAN Range or **Cancel** to cancel the operation.

Configuring Address Pools

You must specify how IP subnets and their associated IP address pools will be utilized, such as for Infrastructure, Management, NAT, Shared Services, or Tier.

You use the Address Pool tab to manage the IP addresses and IP subnets that are used during the orchestration of network containers. IP addresses and IP subnets are associated with a specific cloud.

You can:

- Look at information about IP addresses and IP subnets
- Add a new IP subnet
- Remove an IP subnet

Important Considerations When Configuring Address Pools

You should carefully consider your IP addressing scheme and how you plan to use it when configuring address pools.

Table 3-1 shows the various IP subnet groups and how they are used by Cisco CNAP. Each subnet group is described in more detail in the following sections.

Table 3-1 IP Subnet Groups—Categories of IP Pools Consumed by Cisco CNAP

Subnet Group	Description
Infrastructure	Group of subnets used for stitching core network elements of the container (Public or Private). For example, the L3VPN interface on the Cisco CSR 1000V uses a Private IP subnet from this group. A Public IP subnet is used for the loopback address on the Cisco CSR 1000V.
Tier	Group of subnets used in the provisioning of network segments in a tier (Private). Tier1, Tier2, Tier3, and DMZ have unique IP subnets from this group.
Management	Group of subnets used for device management and other management functions. The Cisco CSR 1000V and Citrix NetScaler VPX management IP addresses use this pool.
Internet (not available in current release)	Subnet used for Internet interface on Cisco CSR 1000V. This is typically a large subnet, such as /22, as each Zinc container would require three IP addresses for stitching the Cisco CSR 1000V to the shared Internet subnet.
NAT	Group of subnets used for Dynamic and Static NATs. The NAT address pool uses public IP addresses. Each Cisco CSR 1000V is assigned a /32 address from this subnet pool.
VIP (not available in current release)	Group of subnets used for DMZ VIPs. This pool uses Public IP addresses.
SharedService	Group of subnets used for Shared Services firewall when manually provisioning WAN Edge/PE (i.e., subnets used for connecting Cisco CSR 1000V to a Shared Service firewall when the L3VPN path is not used for Shared Service access). This is a private IP subnet shared across multiple tenants. Each tenant requires three IP addresses from this pool.

You **must** take into consideration the following configuration requirements and recommendations:

- You **must** create a *separate* Management IP subnet pool for *each* cloud.
- The IP subnet you plan to use to manage the Cisco CSR 1000Vs and the Citrix NetScaler VPXs **must** be assigned to the Management Group and must be large enough to accommodate the required number of Cisco CSR 1000Vs and Citrix NetScaler VPXs.
- You **must** define a Public Infrastructure subnet that will be used for BGP routing between the Cisco CSR 1000Vs and the Cisco ASR 9000 or ASR 1000.
- If you are configuring access to Shared Services, you **must** add a Public NAT subnet.
- If you are manually provisioning WAN Edge/PE for Shared Services, you **must** add a SharedService firewall subnet, which will be Private and the owner is provider auto. Since every tenant requires three (3) unique IP addresses, a subnet mask of /22 can provide addresses for 300 tenants.
- You can define a Private Infrastructure subnet for Layer 3 VPN, however you do not have to. If you do not, Cisco CNAP will allocate IP addresses for Private Infrastructure with /29 if none are configured.
- You can define a Tier subnet, however you do not have to. If you do not, Cisco CNAP will allocate IP addresses for Tier if none are configured.

Infrastructure Subnet Group

The Infrastructure subnet group consists of Private and Public IP subnets.

A Private subnet with /29 network mask is used for stitching the Cisco CSR 1000V to the PE devices. This subnet is overlapping across tenants. Cisco CNAP uses the IP addressing scheme in Table 3-2 for L3VPN connectivity when a Zinc container is provisioned.

Table 3-2 Infrastructure Subnet Group

Subnet	IP address	Purpose
10.5.0.0/29		
	10.5.0.0	Subnet Address
	10.5.0.1	Cisco ASR 9000/ASR1000 Primary PE device
	10.5.0.2	Cisco ASR 9000/ASR1000 Secondary PE device
	10.5.0.3	L3VPN interface on Cisco CSR 1000V Primary
	10.5.0.4	L3VPN interface on Cisco CSR 1000V Secondary
	10.5.0.5	HSRP address on Cisco CSR 1000V
	10.5.0.6	Not used
	10.5.0.7	Broadcast Address

The Loopback IP address is derived from an IP address pool of type Public. Each Cisco CSR 1000V will inherit an IP address from this pool with a /32 network mask.

Tier Subnet Group

Each workload tier by default requires a Private IP subnet with a mask of /26 or lower. The first 20 IP addresses are reserved by Cisco CNAP for various purposes, as shown in Table 3-3. A /24 subnet is used in this example.

Table 3-3 Tier Subnet Group

Subnet	IP address	Purpose
192.168.1.0/24	192.168.1.0	Subnet Address
	192.168.1.1	Cisco CSR 1000V Primary
	192.168.1.2	Cisco CSR 1000V Secondary
	192.168.1.3	Cisco CSR 1000V HSRP
	192.168.1.4	Citrix NetScaler VPX Primary and Secondary
	192.168.1.5	Citrix NetScaler VPX Source NAT
	192.168.1.6-192.168.1.10	SLB VIP
	192.168.1.11-192.168.1.20	Not used
	192.168.1.21	First tenant VM in the subnet
	…	
	192.168.1.254	Last tenant VM in the subnet
	192.168.1.255	Broadcast Address

Management Subnet Group

The Management subnet group is used for assigning management IP address to virtual devices, such as the Cisco CSR1000V and the Citrix NetScaler VPX load balancer. This is typically a Private subnet configured to access the management network of the cloud service provider. You may choose the size of the subnet depending on the number of virtual devices that are managed by Cisco CNAP.

Internet Subnet Group

The Internet IP subnet is a Private subnet that is shared across each tenant Cisco CSR 1000V requiring Internet access. Tenants with active and standby Cisco CSR 1000Vs would require three unique IP addresses from this pool. Table 3-4 shows a sample scheme used for the Internet subnet.

Table 3-4 Internet Subnet Group

Subnet	IP address	Purpose
10.5.8.0/22	10.5.8.0	Subnet Address
	10.5.8.1	Tenant 1 Primary Cisco CSR 1000V
	10.5.8.2	Tenant 1 Secondary Cisco CSR 1000V
	10.5.8.3	Tenant 1 HSRP
	10.5.8.4	Tenant 2 Primary Cisco CSR 1000V
	10.5.8.5	Tenant 2 Secondary Cisco CSR 1000V
	10.5.8.6	Tenant 2 HSRP
	…..	
	10.5.11.251	Primary PE device (manually configured)
	10.5.11.252	Secondary PE device (manually configured)
	10.5.11.253	HSRP address on PE device (manually configured)
	10.5.11.255	Broadcast Address

NAT Subnet Group

The NAT subnet is used by the Cisco CSR 1000V for dynamic NAT when Internet or Shared Service access is required. Each tenant will get a unique NAT address from this pool for their Cisco CSR 1000Vs. With a /24 mask, Cisco CNAP can generate NAT addresses for 254 tenants. Choose the subnet size depending on the number of tenants that the cloud service provider is planning to support.

VIP Subnet Group

The VIP subnet is a Public subnet used within the DMZ tier.

SharedService Subnet Group

The SharedService subnet group uses the same scheme as the Internet subnet except that the next hop is on a shared firewall context and it requires only one IP address. The Gig6 interface on the Cisco CSR 1000V is assigned with an IP and HSRP address from this subnet pool.

Table 3-5 SharedService Subnet Group

Subnet	IP address	Purpose
10.5.16.0/22	10.5.16.0	Subnet Address
	10.5.16.1	Tenant 1 Primary Cisco CSR 1000V
	10.5.16.2	Tenant 1 Secondary Cisco CSR 1000V
	10.5.16.3	Tenant 1 HSRP
	10.5.16.4	Tenant 2 Primary Cisco CSR 1000V
	10.5.16.5	Tenant 2 Secondary Cisco CSR 1000V
	10.5.16.6	Tenant 2 HSRP
	…..	
	10.5.19.253	Shared Firewall context
	10.5.19.255	Broadcast Address

Managing Address Pools

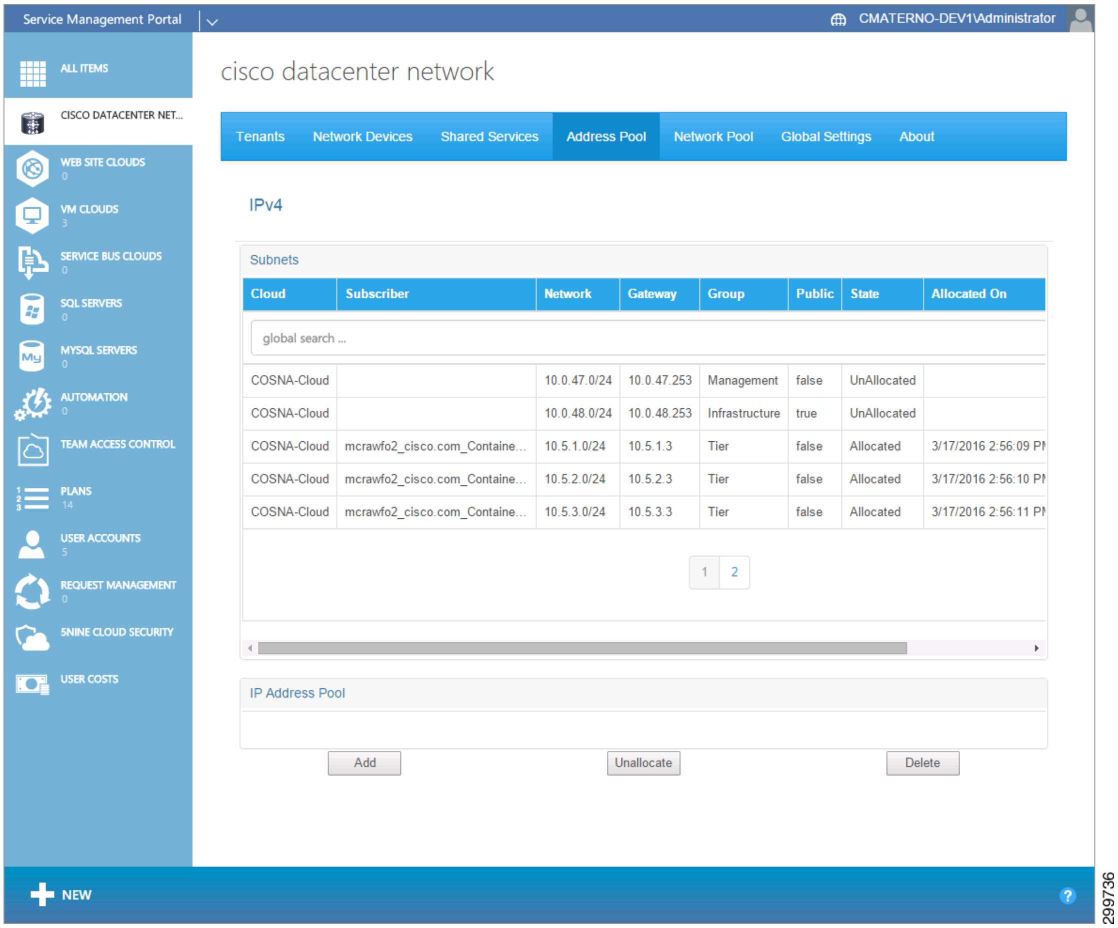
On the Address Pool tab, you manage IP addresses and IP subnets:

- Look at information about IP addresses and IP subnets
- Add an IP subnet to the pool of available IP subnets.
- Delete an IP subnet from the pool of available IP subnets.
- Assign the IP subnet to a Group (Infrastructure, Management, NAT, SharedService, or Tier), which defines how it is utilized.
- Allocate an IP subnet to a tenant.

Viewing Information about IP Subnets

You can view information about IP subnets on the Address Pool tab, as shown in the following screen.

Figure 3-13 Address Pool Tab Screen



Cloud	Subscriber	Network	Gateway	Group	Public	State	Allocated On
COSNA-Cloud		10.0.47.0/24	10.0.47.253	Management	false	UnAllocated	
COSNA-Cloud		10.0.48.0/24	10.0.48.253	Infrastructure	true	UnAllocated	
COSNA-Cloud	mcrawfo2_cisco.com_Containe...	10.5.1.0/24	10.5.1.3	Tier	false	Allocated	3/17/2016 2:56:09 PI
COSNA-Cloud	mcrawfo2_cisco.com_Containe...	10.5.2.0/24	10.5.2.3	Tier	false	Allocated	3/17/2016 2:56:10 PI
COSNA-Cloud	mcrawfo2_cisco.com_Containe...	10.5.3.0/24	10.5.3.3	Tier	false	Allocated	3/17/2016 2:56:11 PI

The Address Pool tab contains the following fields:

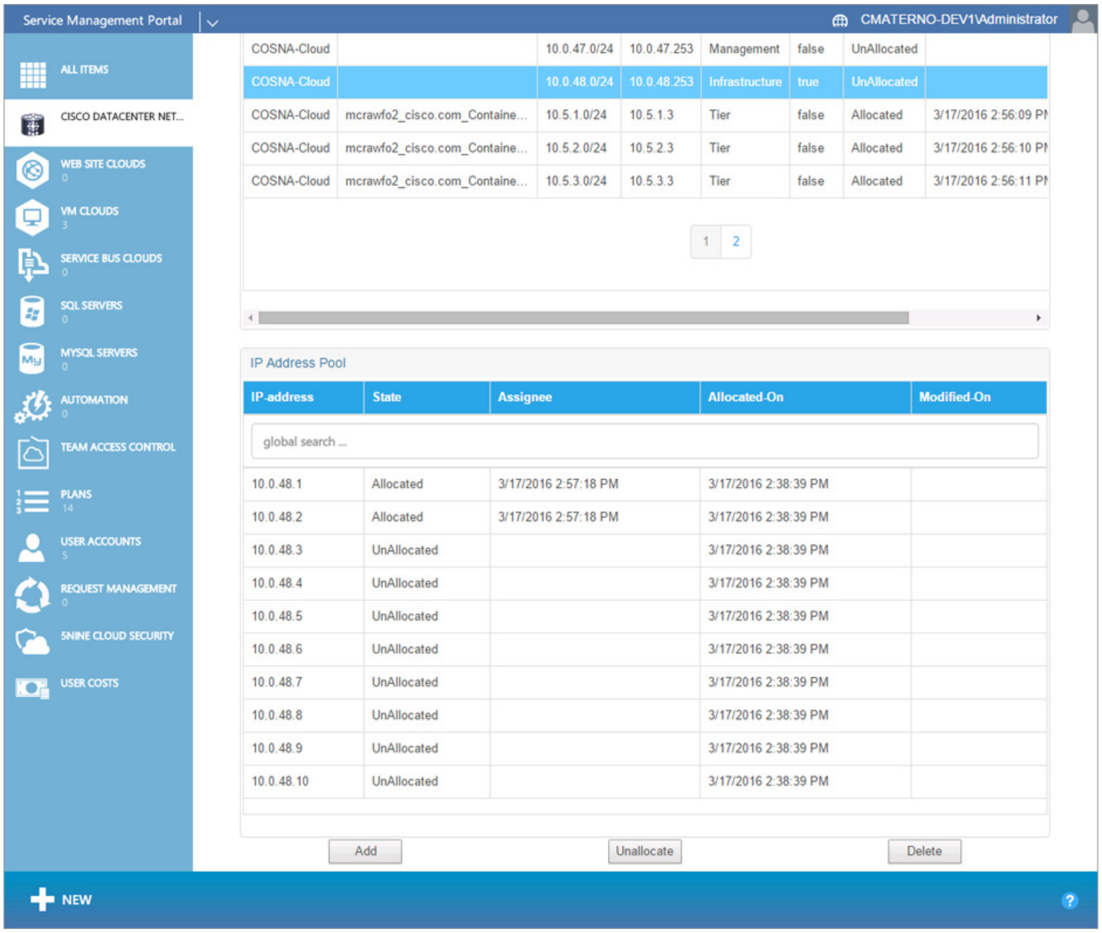
Subnets Table—Displays the IP subnets available for orchestration and automation of a Network Container or Network Service. The fields in the table are:

- Cloud—The associated cloud.
- Subscriber—The name of the tenant.
- Network—Subnet number in CDIR format.
- Gateway—The associated gateway for the subnet.
- Group—The subnet group:
  - Infrastructure—Group of subnets used for stitching core network elements of the container
  - Tier—Group of subnets used on the provisioning of network segments in a tier
  - Management—Group of subnets used for the data center management of each cloud
  - Internet—Group of subnets used for used for the Internet tier (not available in current release)
  - NAT—Group of subnets used for dynamic and static NAT
  - VIP—Group of subnets used for DMZ VIPs (not available in current release)
  - SharedService—Group of subnets used for Shared Services when manually provisioning WAN Edge/PE.

- Public—Whether the cloud is public or private.
- State—The subnet state (Allocated/Unallocated).
- Owner—The Owner (Provider, Provider Template, or Tenant).
- Allocated On—Date and time when the subnet was allocated.
- Modified On—Date and time when the subnet was last modified.

If you click a specific subnet, you see the corresponding IP Address Pool table, as shown in the following screen.

Figure 3-14 IP Address Pool Table Screen



COSNA-Cloud		10.0.47.0/24	10.0.47.253	Management	false	UnAllocated	
COSNA-Cloud		10.0.48.0/24	10.0.48.253	Infrastructure	true	UnAllocated	
COSNA-Cloud	mcrawfo2_cisco.com_Containe...	10.5.1.0/24	10.5.1.3	Tier	false	Allocated	3/17/2016 2:56:09 PI
COSNA-Cloud	mcrawfo2_cisco.com_Containe...	10.5.2.0/24	10.5.2.3	Tier	false	Allocated	3/17/2016 2:56:10 PI
COSNA-Cloud	mcrawfo2_cisco.com_Containe...	10.5.3.0/24	10.5.3.3	Tier	false	Allocated	3/17/2016 2:56:11 PI

IP Address Pool

IP-address	State	Assignee	Allocated-On	Modified-On
10.0.48.1	Allocated	3/17/2016 2:57:18 PM	3/17/2016 2:38:39 PM	
10.0.48.2	Allocated	3/17/2016 2:57:18 PM	3/17/2016 2:38:39 PM	
10.0.48.3	UnAllocated		3/17/2016 2:38:39 PM	
10.0.48.4	UnAllocated		3/17/2016 2:38:39 PM	
10.0.48.5	UnAllocated		3/17/2016 2:38:39 PM	
10.0.48.6	UnAllocated		3/17/2016 2:38:39 PM	
10.0.48.7	UnAllocated		3/17/2016 2:38:39 PM	
10.0.48.8	UnAllocated		3/17/2016 2:38:39 PM	
10.0.48.9	UnAllocated		3/17/2016 2:38:39 PM	
10.0.48.10	UnAllocated		3/17/2016 2:38:39 PM	

IP Address Pool Table—For the selected subnet, displays the IP Addresses available for orchestration and automation of a Network Container or Network Service. The fields in the table are:

- IP-address—String representation of the IP Address in dotted format.
- State—The subnet state (Allocated/Unallocated).
- Assignee—The container with which the IP address is associated.
- Allocated-On—Date and time when the IP Address was allocated.
- Modified-On—Date and time when the IP Address was last modified.

At the bottom of the screen are the following buttons:

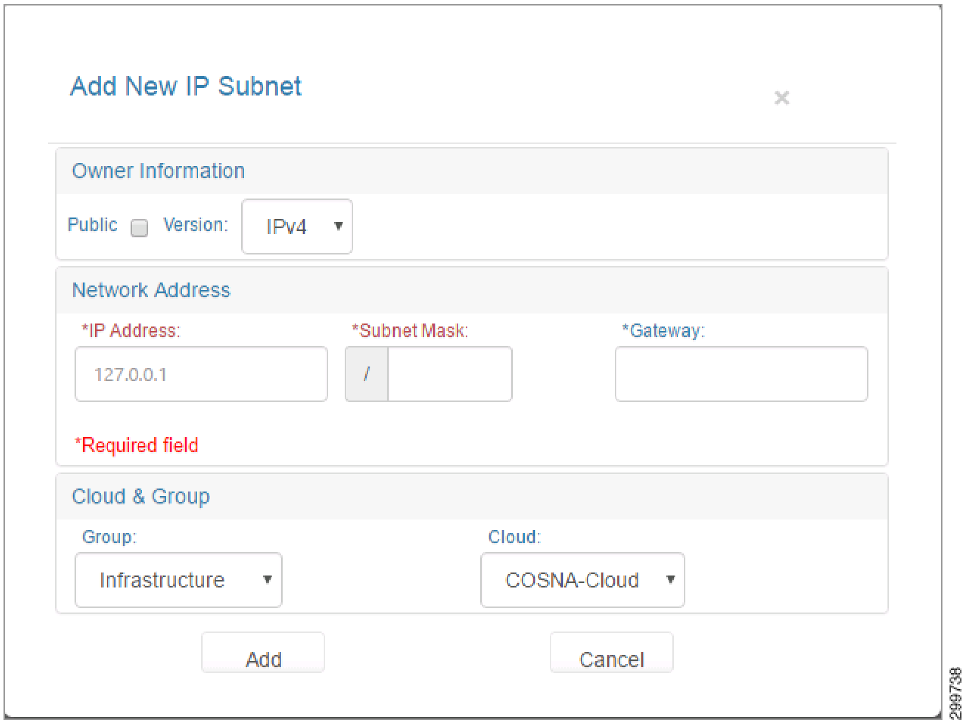
- Add Button—Lets you add a new IP subnet and its corresponding IP Address Pool.
- Delete Button—Lets you remove an existing IP subnet from the system.

Adding a New IP Subnet

Step 1 On the Address Pool tab, to add a new IP subnet, click the **Add** button.

You see the Add New IP Subnet screen.

Figure 3-15 Add New IP Subnet Screen



Add New IP Subnet

Owner Information

Public □ Version: IPv4

Network Address

*IP Address: 127.0.0.1

*Subnet Mask: /

*Gateway:

*Required field

Cloud & Group

Group: Infrastructure

Cloud: COSNA-Cloud

Step 2 To create a new IP subnet, complete the following fields:

- Public—Indicates whether or not the IP Address subnet is a collection of public addresses. The value is true if the subnet and its IP Address Pool are Public and false otherwise.
- Version—IP Addressing Version. In this release, only IPv4 addresses are allowed.
- Network Address—Network Address in dotted format.
- Subnet Mask—A “/” followed by a numeric value in the range [0,32]. (CIDR prefix value). For example a subnet of size /29 will have eight IP Addresses in the pool it defines.
- Gateway—Only available for management IP addresses.
- Group—A group defined classification for the IP subnet that describes how the subnet will be used. For example, if the subnet is used on a VLAN on which VMs will be deployed, the subnet will belong to the Host Network. The format is a string representation of the IP group (Infrastructure, Management, NAT, Tier, or SharedService) as described above.
- Cloud—The cloud to which the IP subnet is associated.

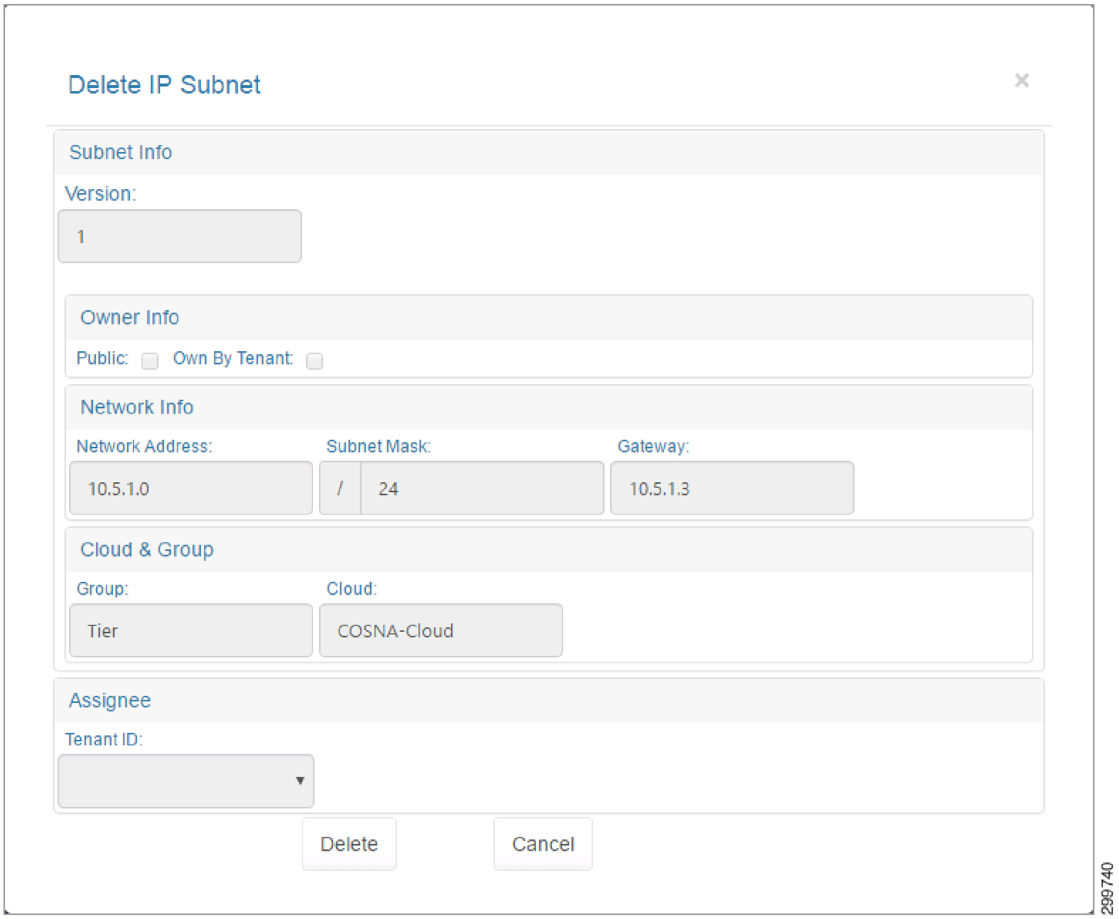
Step 3 Click **Add** to add the subnet or **Cancel** to cancel the addition.

Removing an IP Subnet

Step 1 On the Address Pool tab, to remove an IP subnet, click the subnet you want to remove and then click the **Delete** button.

You see the Delete IP Subnet screen.

Figure 3-16 Delete IP Subnet Screen



Delete IP Subnet

Subnet Info

Version: 1

Owner Info

Public: □ Own By Tenant: □

Network Info

Network Address: 10.5.1.0

Subnet Mask: / 24

Gateway: 10.5.1.3

Cloud & Group

Group: Tier

Cloud: COSNA-Cloud

Assignee

Tenant ID:

Step 2 Click **Delete** to delete the subnet or **Cancel** to cancel the deletion.

Configuring Access to Shared Services

You can also configure access to Shared Services, such as Database as a Service (DBaaS), Disaster Recovery as a Service (DRaaS), etc., that you want to be available as options when you are creating and configuring network container plans.

Note Before you configure access to Shared Services, you should add a Cisco ASA 5585 firewall to be used as the security access point to the Shared Services. The firewall context defined on the Cisco ASA 5585 **must** be preconfigured. For more information, see Configuring Data Center Devices.

Note You should also add a Public NAT IP subnet. For more information, see Important Considerations When Configuring Address Pools.

Note If you are manually provisioning WAN Edge/PE for Shared Services, you must add a SharedService firewall IP subnet. For more information, see Important Considerations When Configuring Address Pools

For more information on configuration requirements for deploying various services over the CCA MCP architecture, see Configuring Specific Services in Chapter 4, "Developing Container Plans." You can also refer to these documents; URLs are provided in the Preface:

- *Cisco Cloud Architecture for the Microsoft Cloud Platform: DBaaS Configuration Guide, Release 1.0*

  Note A sample Database as a Service deployment is described in Appendix B, "Sample Database as a Service Deployment.".

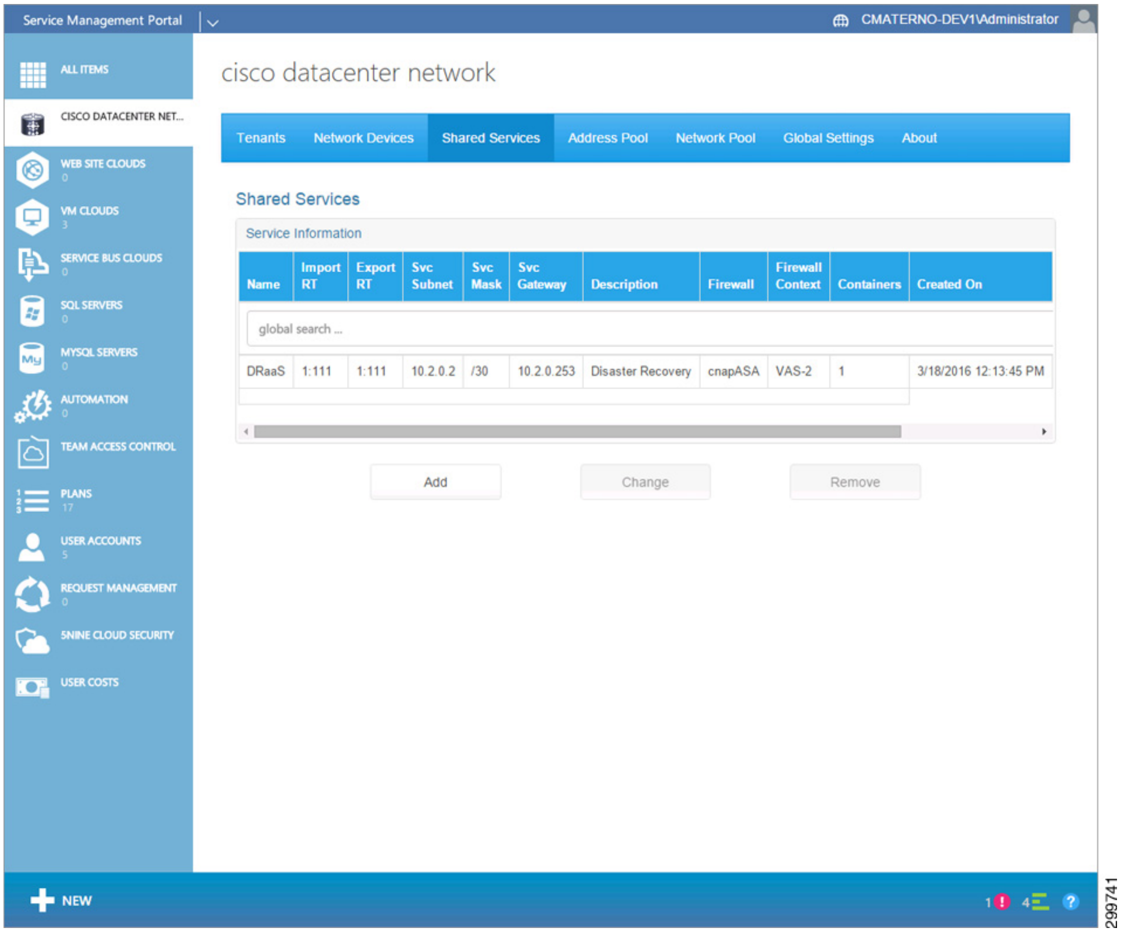
- *Cisco Cloud Architecture for the Microsoft Cloud Platform: DRaaS Application Note, Release 1.0*
- *Cisco Cloud Architecture for the Microsoft Cloud Platform: Backup as a Service Implementation Guide, Release 1.0*

On the Shared Services tab you can:

- Look at information about Shared Services
- Add a Shared Service
- Change a Shared Service
- Remove a Shared Service

Viewing Information about Shared Services

Figure 3-17 Shared Services Tab Screen



Shared Services

Service Information

global search ...

Name	Import RT	Export RT	Svc Subnet	Svc Mask	Svc Gateway	Description	Firewall	Firewall Context	Containers	Created On
DRaaS	1:111	1:111	10.2.0.2	/30	10.2.0.253	Disaster Recovery	cnapASA	VAS-2	1	3/18/2016 12:13:45 PM

Add Change Remove

The Shared Services tab contains the following fields:

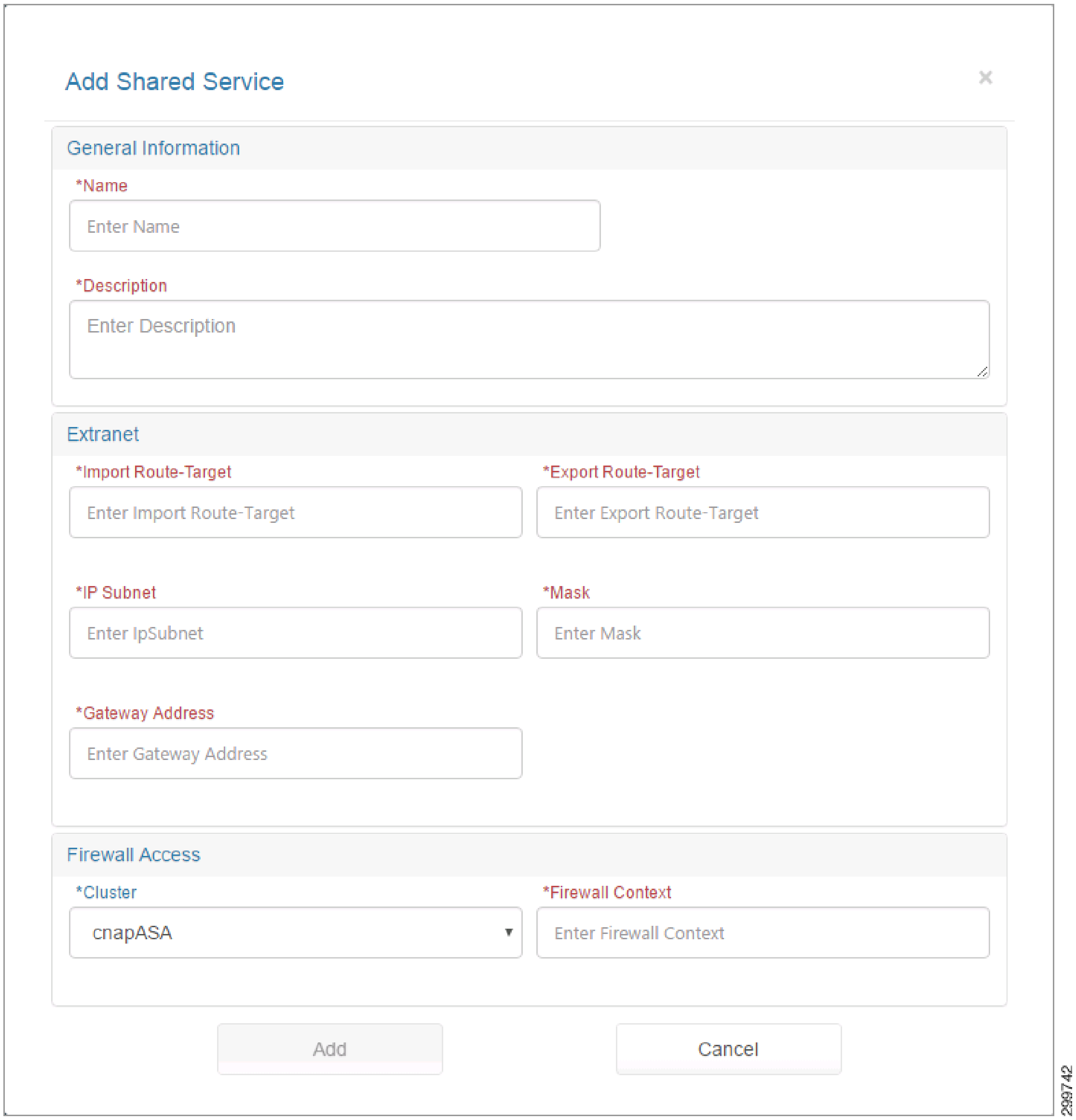
- Name—Name given to the Shared Service at the time the service was onboarded.
- Import RT—Import Route Target on the MPLS Network through which the Shared Service is accessible.
- Export RT—Export Route Target on the MPLS Network through which the Shared Service is accessible.
- Svc Subnet—IP subnet (Public) on which the Shared Service is available.
- Svc Mask—Subnet Mask associated with the Shared Service subnet.
- Description—Description of the Shared Service.
- Containers—Number of container instances that have activated access to the Shared Service.
- Created On—Date and time when the Shared Service configuration was created in Cisco CNAP.
- Modified On—Date and time when the Shared Service configuration was last modified in Cisco CNAP.

Adding a Shared Service

Step 1 On the Shared Services tab, to add a new Shared Service, click the **Add** button.

You see the Add Shared Service screen.

Figure 3-18 Add Shared Service Screen



Step 2 To add a new Shared Service, complete the following fields:

- General Information:
  - Name—Enter a name for the Shared Service, a text string with a maximum of 40 characters (alphanumeric, “-”, and “_”).
  - Description—Enter a description of the Shard Service, a text string with a maximum of 128 characters (alphanumeric).

- Extranet:
  - Import Route-Target—Text String in the format: <*number*>:<*number*>; e.g., 99:999. Import Route Target on the MPLS Network through which the Shared Service is accessible.
  - Export Route-Target—Text String in the format: <*number*>:<*number*>; e.g., 99:999. Export Route Target on the MPLS Network through which the Shared Service is accessible.
  - IP Subnet—IP subnet (Public) in dotted format: A.B.C.D.
  - Mask—Subnet Mask associated with the Shared Service subnet using the CIDR Notation: /<*number*>; e.g., /32.
- Gateway Address—Provider Edge (PE) gateway address in dotted format: A.B.C.D.

Note If you are using Shared Services with PE manual provisioning (VLAN hand-off mode), the gateway address is the inside interface of the shared service firewall context that connects to the outside interface of the Value Added Service (VAS) firewall context.

- Firewall Access:
  - Cluster—List of the names of all Cisco ASA Firewall devices (DeviceType= ASA5585) registered in Cisco CNAP using the Network Devices tab. If no Cisco ASA devices have been registered, you see a message to onboard a new Cisco ASA device.
  - Context—Text string with a maximum of 32 characters. The name of the firewall context defined in the Cisco ASA to handle the Shared Service.

Step 3 When you are finished, click **Add**.

The new Shared Service is shown on the Shared Services tab.

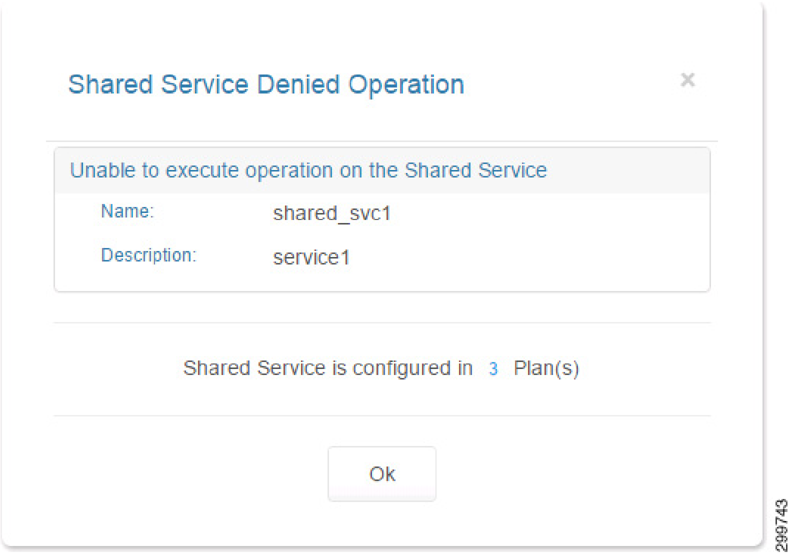
Changing a Shared Service

Note If the Shared Service has containers that have activated the service or the Shared Service is configured in a Cisco CNAP container plan, you cannot change it.

Step 1 To change a Shared Service, on the Shared Services tab, click the service you want to change to highlight it, then click **Change**.

If the Shared Service is configured in a plan or has active subscribers using the service, you see one of the following screens.

Figure 3-19 Shared Service Denied Operation Screen—Configured in Plan



Shared Service Denied Operation

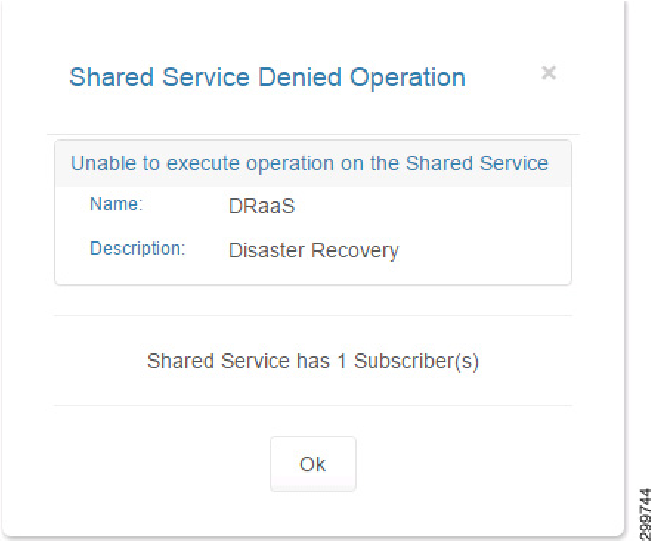
Unable to execute operation on the Shared Service

Name: shared_svc1

Description: service1

Shared Service is configured in 3 Plan(s)

Figure 3-20 Shared Service Denied Operation Screen—Service has Subscriber



Shared Service Denied Operation

Unable to execute operation on the Shared Service

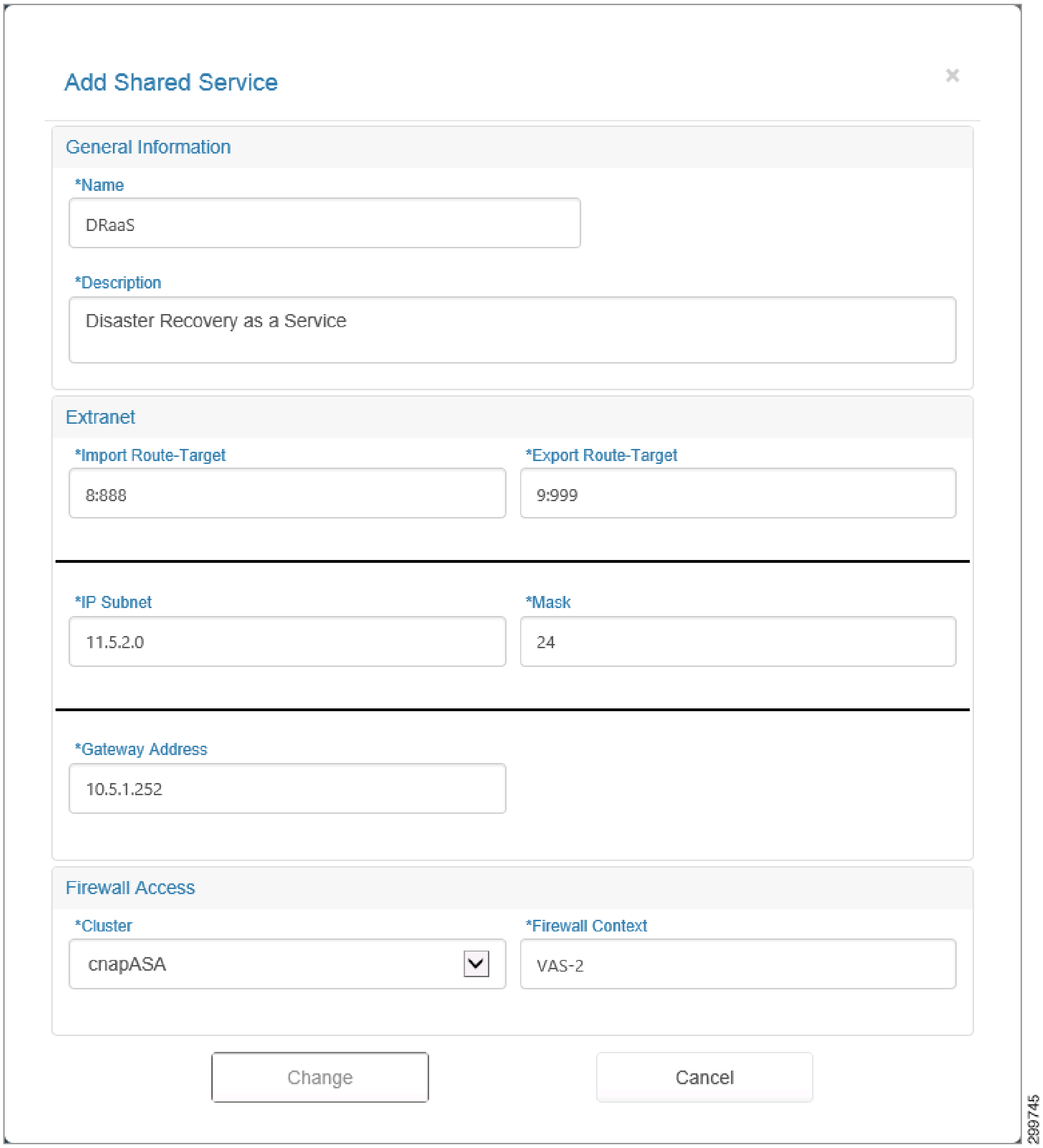
Name: DRaaS

Description: Disaster Recovery

Shared Service has 1 Subscriber(s)

If the service can be modified, you see the Add Shared Service screen with information about the existing Shared Service you selected.

Figure 3-21 Add Shared Service Screen—Modify Existing Information



Add Shared Service

General Information

*Name: DRaaS

*Description: Disaster Recovery as a Service

Extranet

*Import Route-Target: 8:888

*Export Route-Target: 9:999

*IP Subnet: 11.5.2.0

*Mask: 24

*Gateway Address: 10.5.1.252

Firewall Access

*Cluster: cnapASA

*Firewall Context: VAS-2

Step 2 To change the Shared Service, modify the fields you want to change:

- General Information:
  - Name—Enter a name for the Shared Service, a text string with a maximum of 40 characters.
  - Description—Enter a description of the Shard Service, a text string with a maximum of 128 characters.
- Extranet:

Note If VLAN handoff is being used for Shared Services, the Extranet Route Targets are ignored.

- Import Route-Target—Text String in the format: <*number*>:<*number*>; e.g., 99:999. Import Route Target on the MPLS Network through which the Shared Service is accessible.
- Export Route-Target—Text String in the format: <*number*>:<*number*>; e.g., 99:999. Export Route Target on the MPLS Network through which the Shared Service is accessible.
- IP Subnet—IP subnet (Public) in dotted format: A.B.C.D.
- Mask—Subnet Mask associated with the Shared Service subnet using the CDIR Notation: /<*number*>; e.g., /32.

- Firewall Access:
  - Cluster—List of the names of all Cisco ASA Firewall devices (DeviceType= ASA) registered in Cisco CNAP using the Cisco CNAP Network Devices tab. If no Cisco ASA devices have been registered, you see a message to onboard a new Cisco ASA device.
  - Context—Text string with a maximum of 32 characters. The name of the firewall context defined in the Cisco ASA to handle the Shared Service.

Step 3 When you are finished, click **Change**.

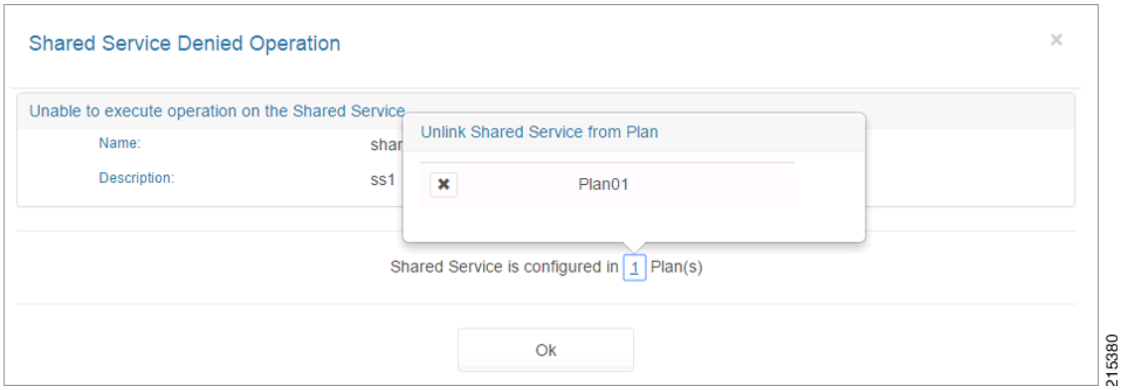
Removing a Shared Service

Note If the Shared Service has containers that have activated the service or the Shared Service is configured in a Cisco CNAP plan, you cannot remove it. You can unlink a Shared Service from a plan so you can remove it, as described below.

Step 1 To remove a Shared Service, on the Shared Services tab, click the service you want to remove to highlight it, then click **Remove**.

If the Shared Service has containers that have activated the service or the Shared Service is configured in a Cisco CNAP plan, you see one of the following screens.

Figure 3-22 Shared Service Denied Operation Screen—Configured in Plan



Shared Service Denied Operation

Unable to execute operation on the Shared Service

Name: shar

Description: ss1

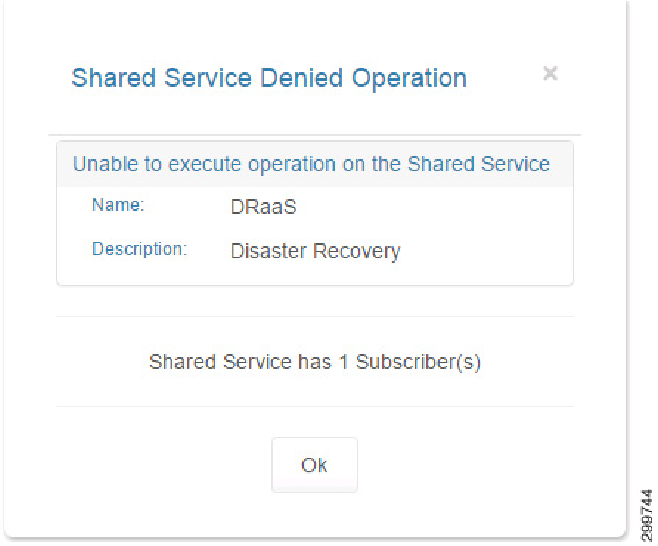
Unlink Shared Service from Plan

Plan01

Shared Service is configured in 1 Plan(s)

Step 2 To unlink a Shared Service from a plan so you can remove it, click the number before “Plan(s)’ as shown in the screen above, then click the plan you want to unlink.

Figure 3-23 ***Shared Service Denied Operation Screen—Service has Subscriber***



Shared Service Denied Operation

Unable to execute operation on the Shared Service

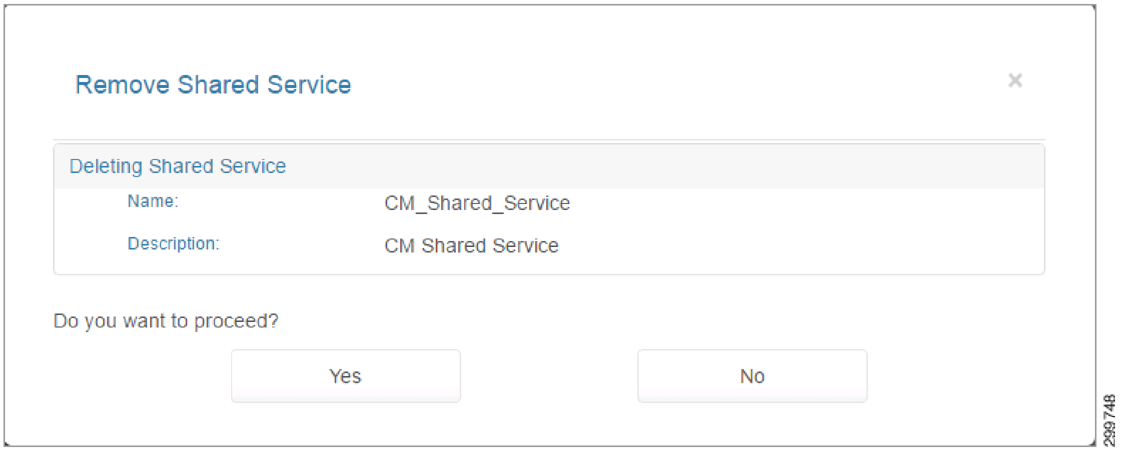
Name: DRaaS

Description: Disaster Recovery

Shared Service has 1 Subscriber(s)

If the Shared Service can be removed, you see the Remove Shared Service screen.

Figure 3-24 ***Remove Shared Service Screen***



Remove Shared Service

Deleting Shared Service

Name: CM_Shared_Service

Description: CM Shared Service

Do you want to proceed?

Step 3 To confirm the deletion, click **Yes**.

CHAPTER 4

Developing Container Plans

This section describes how a service provider administrator can create and configure container plans and make the available for tenants to use.

Types of Container Plans

The types of container plans you can create include:

- IaaS Plans: Containing Cisco Data Center Network(s) and VM Clouds in one plan
- DBaaS Plan: WAP/SQL-RP Plans

This document focuses on IaaS Plans. Note that IaaS Plans can also be used directly by tenants for their workloads as IaaS service. The SP Admin can also use IaaS Plan subscriptions to build hosted applications for tenants.

Configuring Specific Services

Each tenant service will need additional per-tenant configuration to onboard the tenant. The services that are supported by the CCA MCP architecture include Infrastructure as a Service (IaaS) with Zinc Container, Database as a Service (DBaaS), Disaster Recovery as a Service (DRaaS), and Backup as a Service (BaaS).

Each tenant gets a logical container of resources and the cloud container patterns provide a view of this logical network. Container models can be built in a variety of ways to support the use cases. A set of reference IaaS patterns have been built that are available “out of the box” for ready deployment. Orchestration of these containers is accomplished by using Cisco CNAP to provision the Cisco networking pieces for tenant services.

For specific configuration requirements for these services, see:

- *Cisco Cloud Architecture for the Microsoft Cloud Platform: Zinc Container Configuration Guide, Release 1.0*—Describes the Infrastructure as a Service (IaaS) model with per-tenant CSR 1000V-based router/firewall and provides implementation details of the CSR 1000V-based IaaS pattern for tenancy in CCA MCP.
- *Cisco Cloud Architecture for the Microsoft Cloud Platform: DBaaS Configuration Guide, Release 1.0*—Describes how Data Base as a Service can be deployed over the CCA MCP architecture.
- *Cisco Cloud Architecture for the Microsoft Cloud Platform: DRaaS Application Note, Release 1.0*—Describes how Disaster Recovery as a Service (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*—Describes how Backup as a Service (powered by Commvault Simpana) can be deployed over the CCA MCP architecture.

Note A sample Data Base as a Service deployment is described in Appendix B, "Sample Database as a Service Deployment.".

Creating Container Plans

This section describes:

- Using the container plan creation wizard to create a network and virtual machine cloud container plan, including details about:
  - WAN gateway
  - Tenant perimeter firewall
  - Server load balancer (SLB)

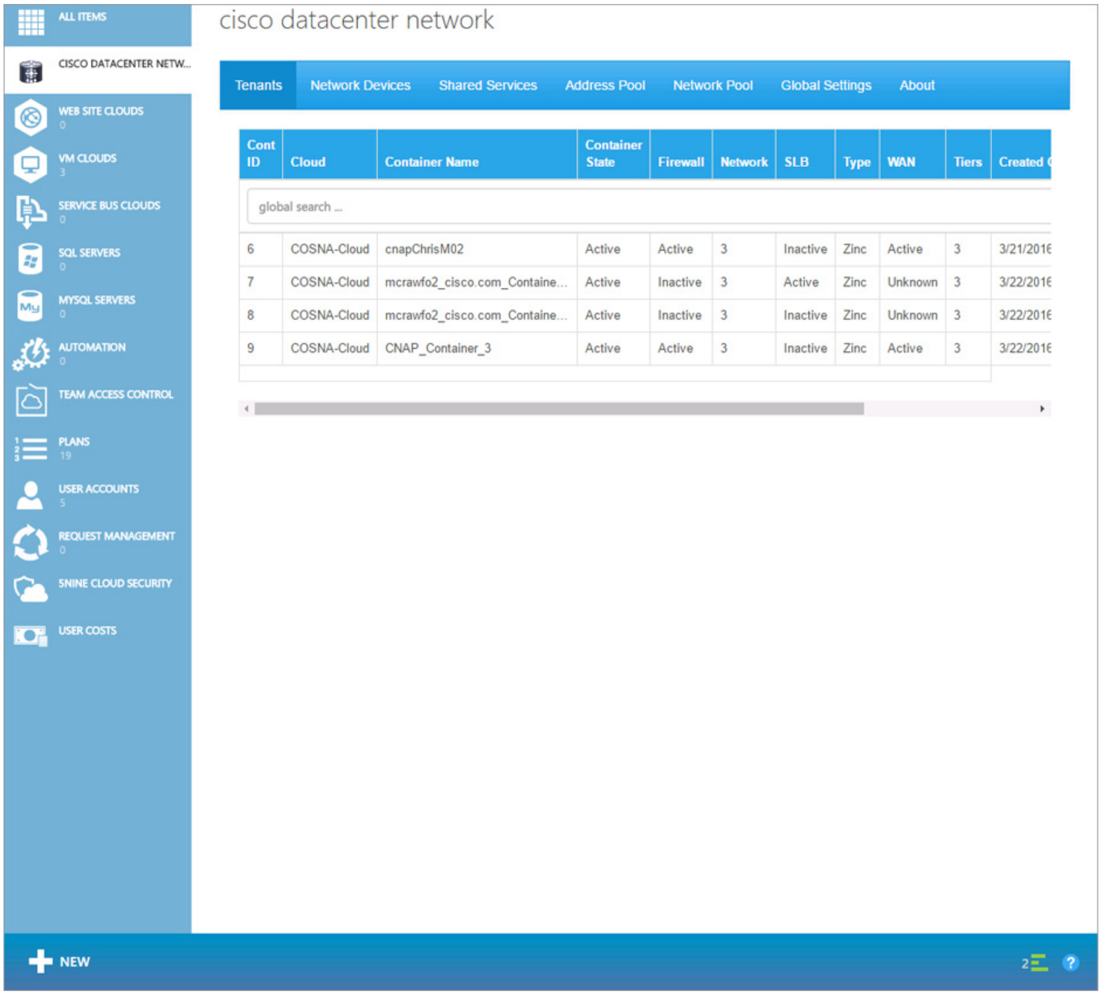
Once a container plan is created, customers can use the Tenant Portal to subscribe to any of the available public container plans. For more information, see *Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Tenant Portal Guide, Release 1.1*.

Creating a Network and Virtual Machine Cloud Container Plan

To create a network and virtual machine cloud container plan:

Step 1 On the Tenants Tab screen, click **+ New** in the lower left corner, as shown in the following screen. You can also click **PLANS** on the main WAP screen.

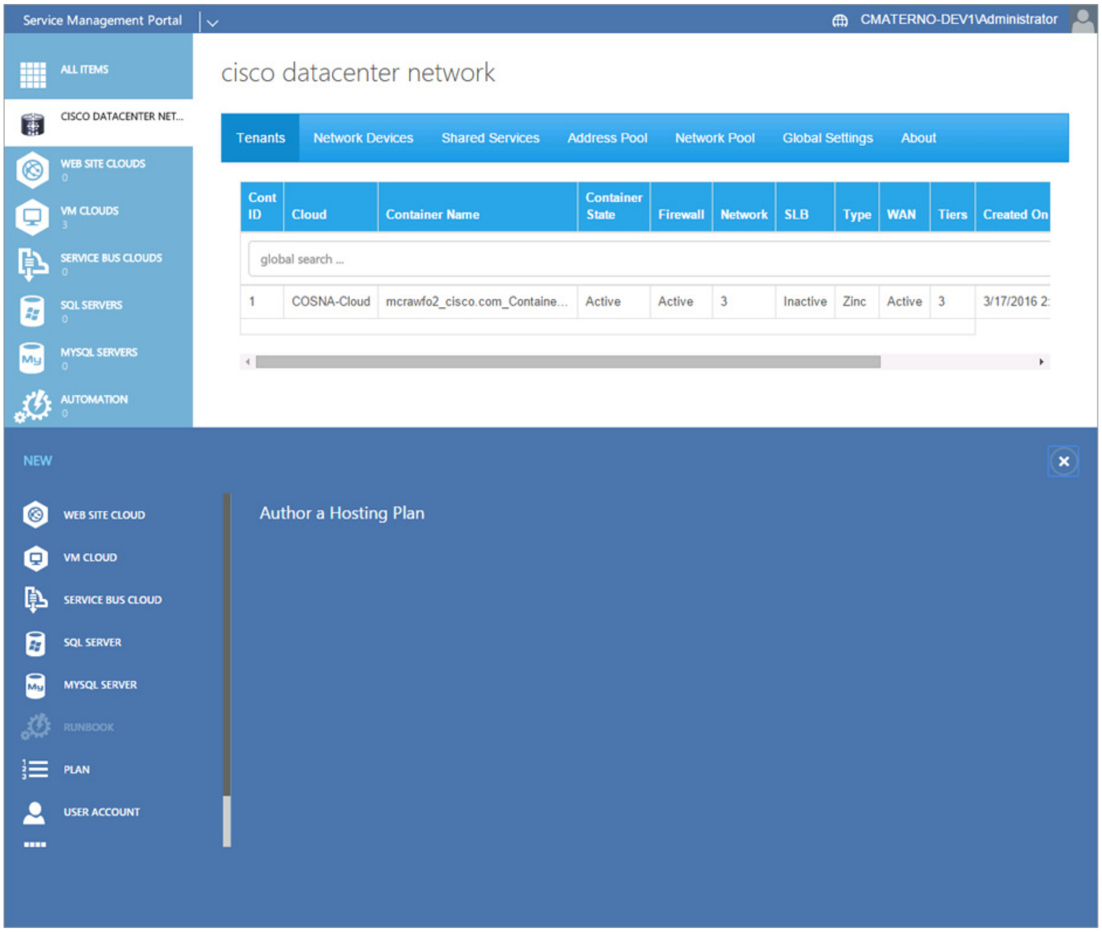
Figure 4-1 Tenants Tab Screen



Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created
6	COSNA-Cloud	cnapChrisM02	Active	Active	3	Inactive	Zinc	Active	3	3/21/2016
7	COSNA-Cloud	mcrawfo2_cisco.com_Containe...	Active	Inactive	3	Active	Zinc	Unknown	3	3/22/2016
8	COSNA-Cloud	mcrawfo2_cisco.com_Containe...	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/22/2016
9	COSNA-Cloud	CNAP_Container_3	Active	Active	3	Inactive	Zinc	Active	3	3/22/2016

You see a pop-up window with various options for what you can create, as shown in the following screen.

Figure 4-2 Creation Options Screen

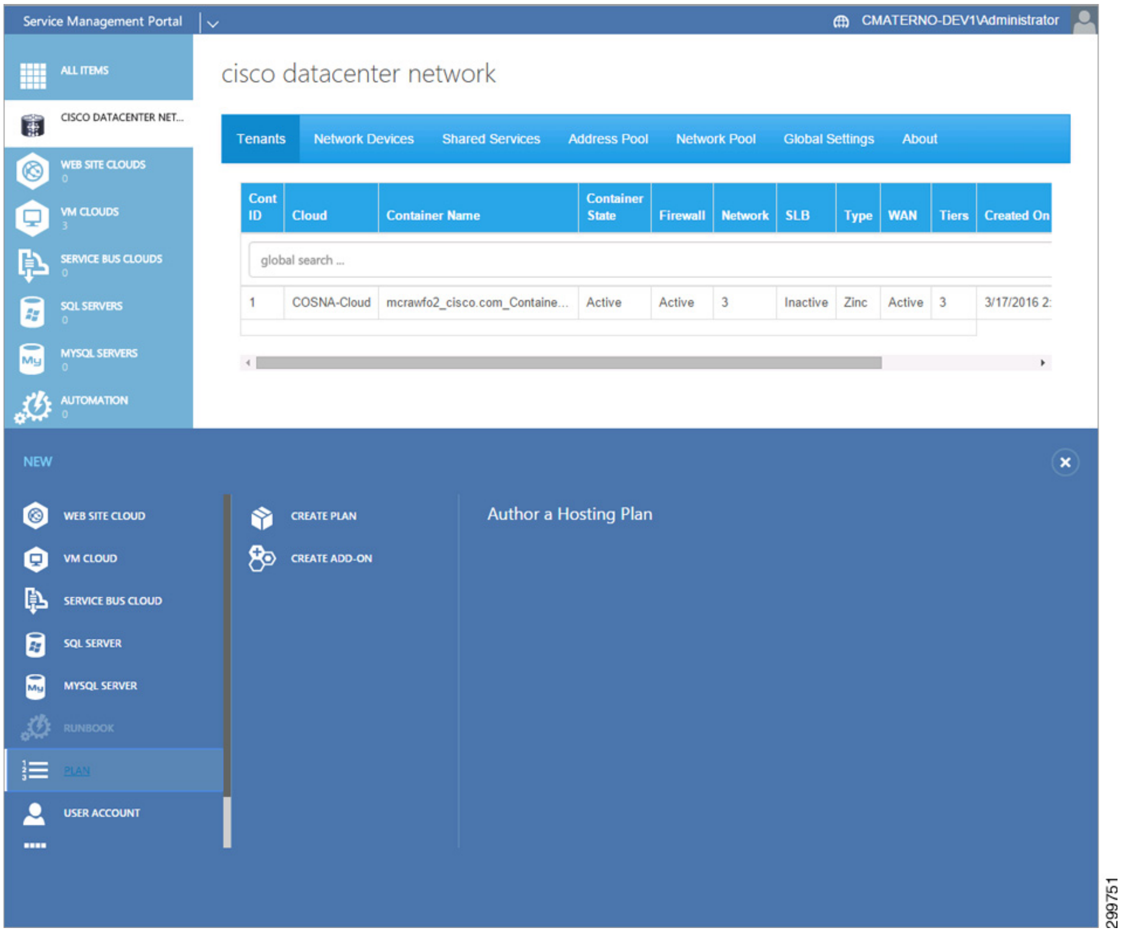


Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created On
1	COSNA-Cloud	mcrawfo2_cisco.com_Containe...	Active	Active	3	Inactive	Zinc	Active	3	3/17/2016 2:

Step 2 Click **Plan**.

You see options to Create Plan and Create Add-On, as shown in the following screen.

Figure 4-3 *Plan Creation Options Screen*

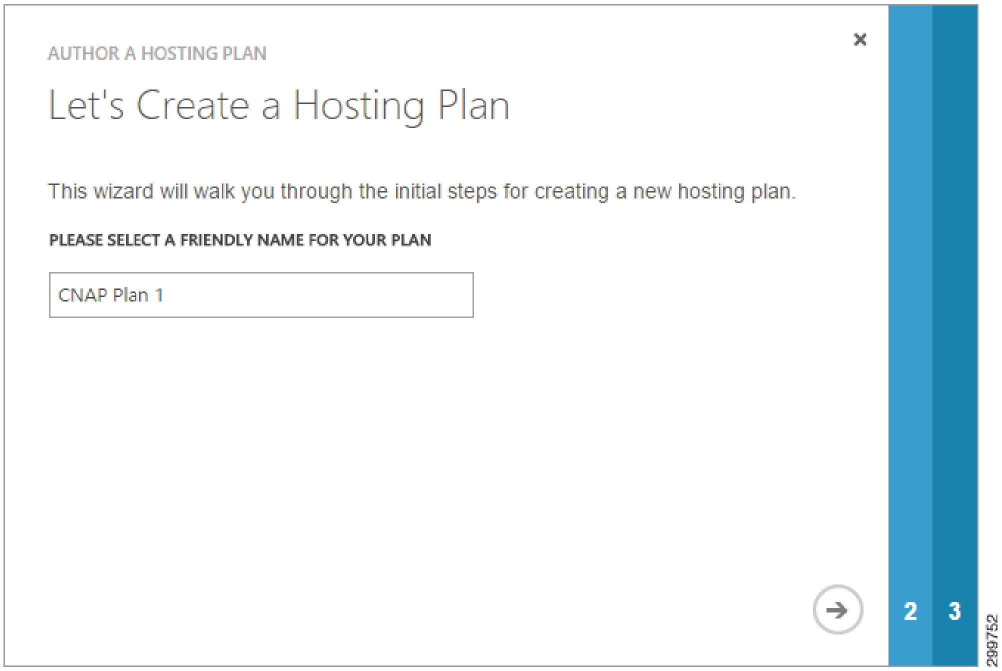


Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created On
1	COSNA-Cloud	mcrawfo2_cisco.com_Containe...	Active	Active	3	Inactive	Zinc	Active	3	3/17/2016 2:

Step 3 Click **Create Plan**.

You see a pop-up window, as shown in the following screen.

Figure 4-4 Create a Hosting Plan Screen



AUTHOR A HOSTING PLAN

Let's Create a Hosting Plan

This wizard will walk you through the initial steps for creating a new hosting plan.

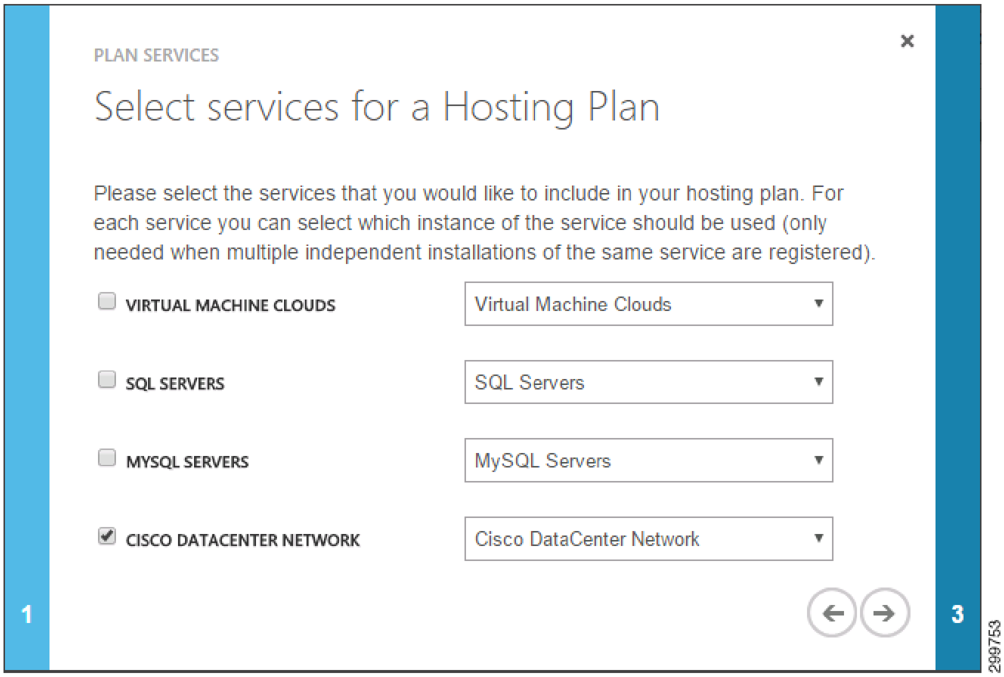
PLEASE SELECT A FRIENDLY NAME FOR YOUR PLAN

CNAP Plan 1

Step 4 Enter a name for the plan, then click the right arrow (–>).

You see a pop-up window, as shown in the following screen.

Figure 4-5 Select Services Screen



PLAN SERVICES

Select services for a Hosting Plan

Please select the services that you would like to include in your hosting plan. For each service you can select which instance of the service should be used (only needed when multiple independent installations of the same service are registered).

□ VIRTUAL MACHINE CLOUDS — Virtual Machine Clouds ▾

□ SQL SERVERS — SQL Servers ▾

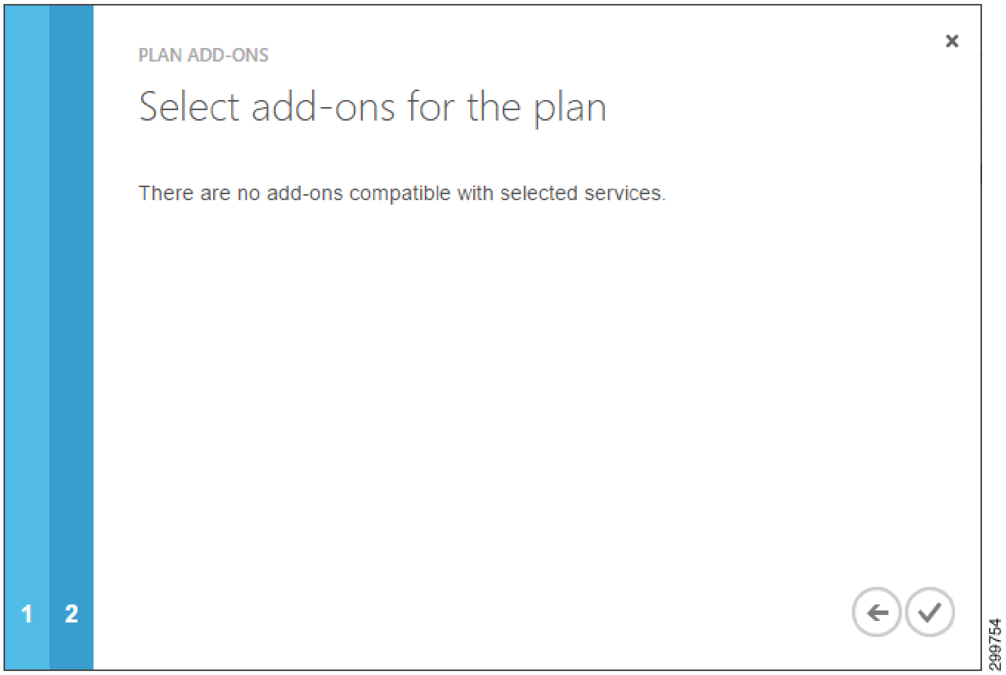
□ MYSQL SERVERS — MySQL Servers ▾

☑ CISCO DATACENTER NETWORK — Cisco DataCenter Network ▾

Step 5 Select **Cisco Datacenter Network**, then click the right arrow (–>).

You see a pop-up window, as shown in the following screen.

Figure 4-6 Select Add-Ons Screen



PLAN ADD-ONS

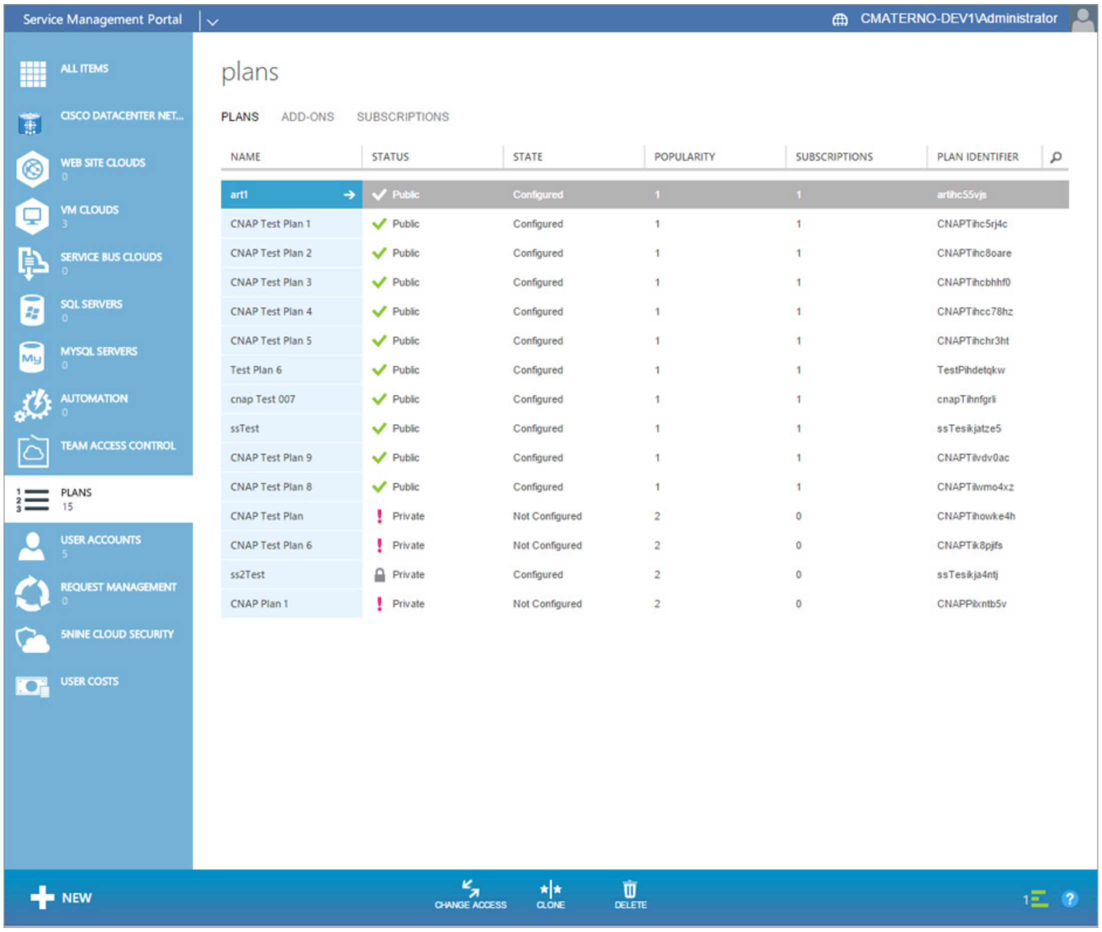
Select add-ons for the plan

There are no add-ons compatible with selected services.

Step 6 Click the check mark.

You see a window with the plan you created, which has a Status of Private and a State of Not Configured, as shown in the following screen.

Figure 4-7 ***Plans Screen***



plans

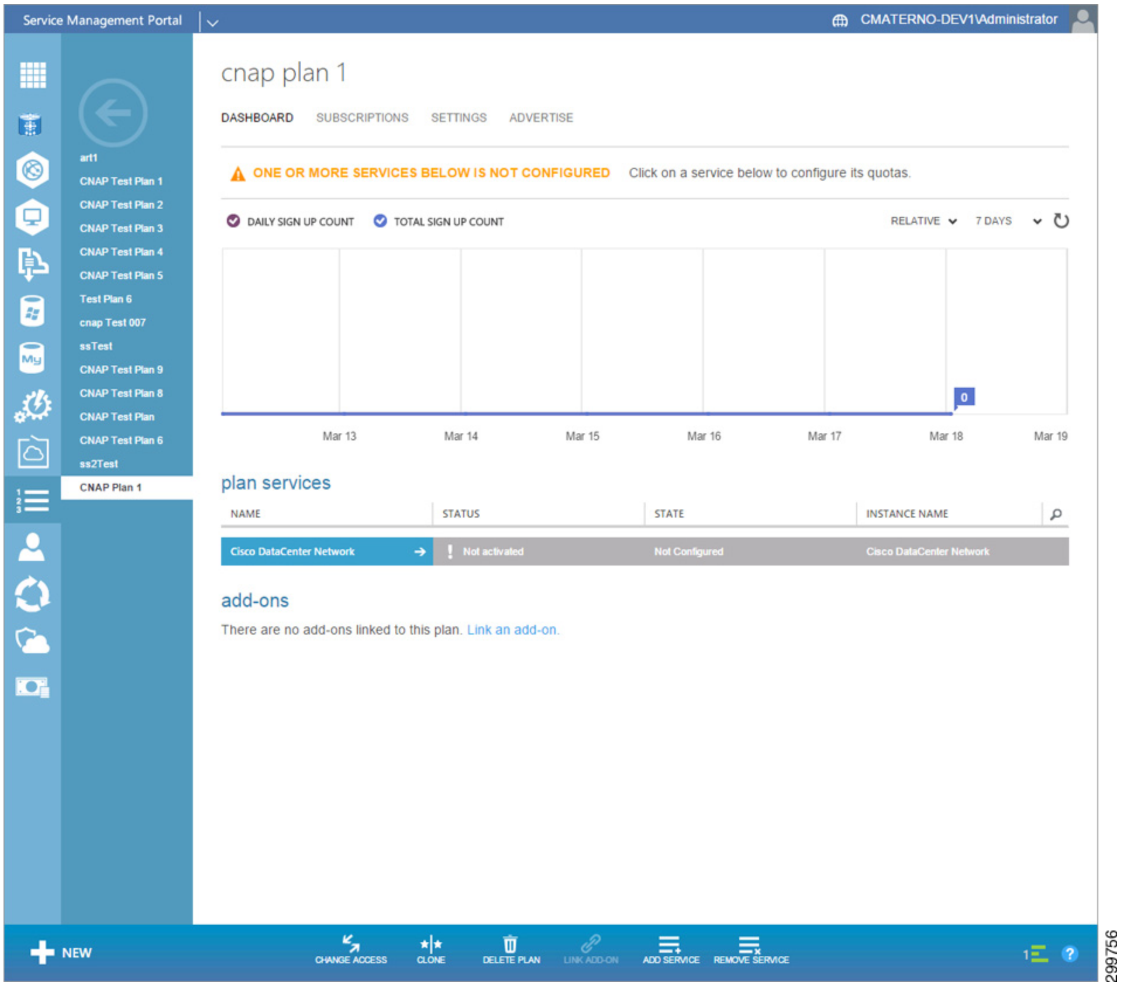
PLANS ADD-ONS SUBSCRIPTIONS

NAME	STATUS	STATE	POPULARITY	SUBSCRIPTIONS	PLAN IDENTIFIER
art1	✓ Public	Configured	1	1	artihc55vjs
CNAP Test Plan 1	✓ Public	Configured	1	1	CNAPTihc5rj4c
CNAP Test Plan 2	✓ Public	Configured	1	1	CNAPTihc8oare
CNAP Test Plan 3	✓ Public	Configured	1	1	CNAPTihcbhhf0
CNAP Test Plan 4	✓ Public	Configured	1	1	CNAPTihcc78hz
CNAP Test Plan 5	✓ Public	Configured	1	1	CNAPTihchr3ht
Test Plan 6	✓ Public	Configured	1	1	TestPihdetqkw
cnap Test 007	✓ Public	Configured	1	1	cnapTihnfgrli
ssTest	✓ Public	Configured	1	1	ssTesikjatze5
CNAP Test Plan 9	✓ Public	Configured	1	1	CNAPTilvdv0ac
CNAP Test Plan 8	✓ Public	Configured	1	1	CNAPTilwmo4xz
CNAP Test Plan	! Private	Not Configured	2	0	CNAPTihowke4h
CNAP Test Plan 6	! Private	Not Configured	2	0	CNAPTik8pjifs
ss2Test	🔒 Private	Configured	2	0	ssTesikja4ntj
CNAP Plan 1	! Private	Not Configured	2	0	CNAPPilxntb5v

Step 7 Click the name of the plan you just created.

You see the following screen, which displays assorted information about the plan.

Figure 4-8 Plan Detail Screen



cnap plan 1

ONE OR MORE SERVICES BELOW IS NOT CONFIGURED Click on a service below to configure its quotas.

plan services

NAME	STATUS	STATE	INSTANCE NAME
Cisco DataCenter Network	! Not activated	Not Configured	Cisco DataCenter Network

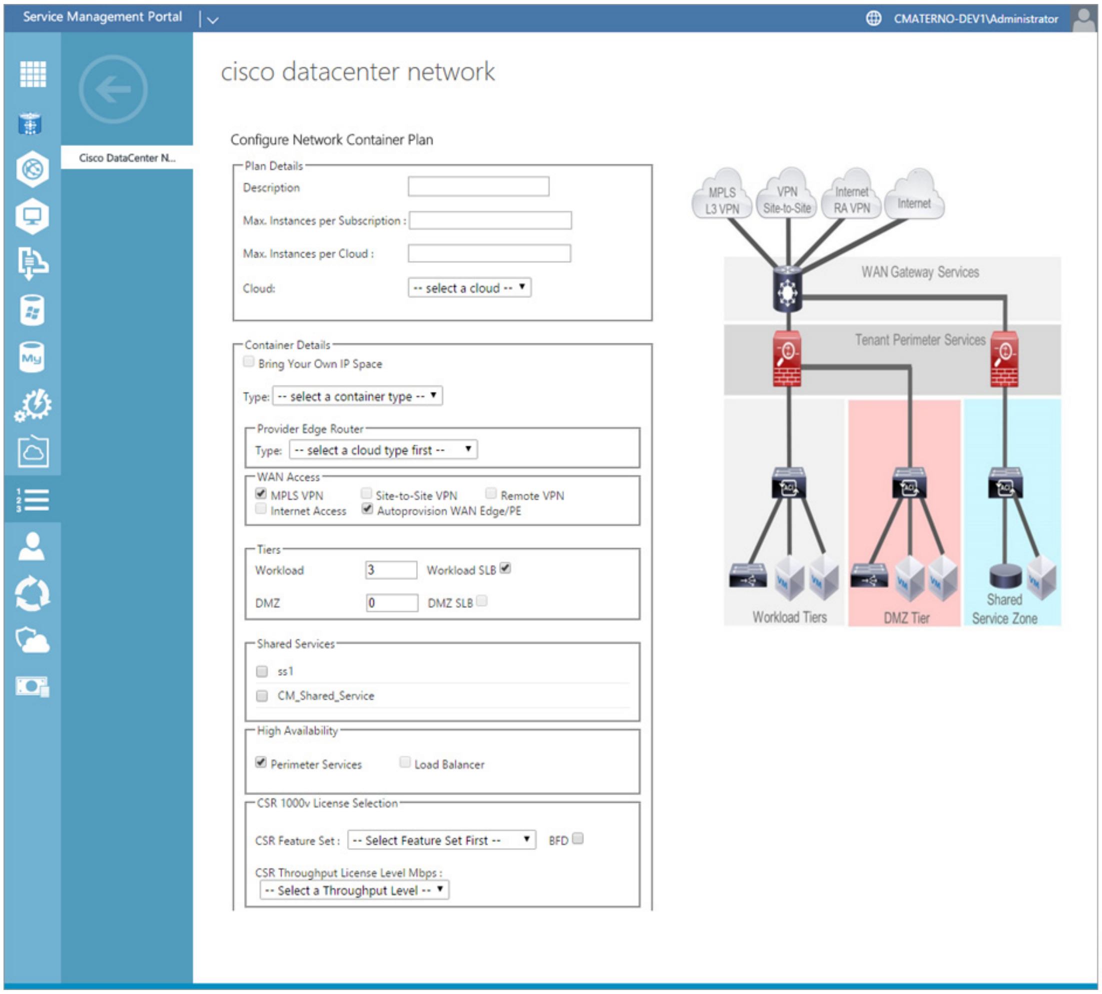
add-ons

There are no add-ons linked to this plan. Link an add-on.

Step 8 Under Plan services, click on the name of the plan you're going to configure. In this example, we click **Cisco DataCenter Network**.

You see the following screen.

Figure 4-9 Configure Network Container Plan Screen



cisco datacenter network

Configure Network Container Plan

Plan Details
Description
Max. Instances per Subscription :
Max. Instances per Cloud :
Cloud: -- select a cloud --

Container Details
□ Bring Your Own IP Space
Type: -- select a container type --

Provider Edge Router
Type: -- select a cloud type first --

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

Tiers
Workload 3 Workload SLB ☑
DMZ 0 DMZ SLB □

Shared Services
□ ss1
□ CM_Shared_Service

High Availability
☑ Perimeter Services □ Load Balancer

CSR 1000v License Selection
CSR Feature Set : -- Select Feature Set First -- BFD □
CSR Throughput License Level Mbps :
-- Select a Throughput Level --

Step 9 Complete the various fields to create a network container:

- Enter Plan Details about the container:
  - Description—Enter a descriptive name for the container.
  - Maximum Instances per Subscription—1-10
  - Maximum Instances per Cloud—1-2500
  - Cloud—Select the cloud service associated with the plan you are configuring.

Note The list of clouds in the drop-down menu is populated from the Cisco CNAP database. There is a service that updates this list every hour; hence if a new cloud is added to SCVMM, it can take up to one hour to show up in the Cisco CNAP plan creation wizard in the Admin Portal.

- Specify Container information:
  - Bring Your Own IP Space and Type—Not available in the current release. **Zinc Container** is preselected.
  - Perimeter Edge Router—Type: On the drop-down menu, select the PE router you are utilizing for the WAN Gateway, either the Cisco ASR9000 or Cisco ASR1000.

- WAN Access: Specify the type of WAN Access, MPLS VPN, Site-to-Site VPN, Remote VPN, or Internet Access. MPLS VPN is preselected as it is the only option available in the current release.

Note You can also specify whether you want Cisco CNAP to **Autoprovision WAN Edge/PE**, which provisions the Data Center Provider Edge Router with Tenant VRF and L3VPN configurations. For more information, see Understanding the Difference Between Auto-provisioning and Manually Provisioning WAN Gateways in Chapter 5, "Managing Container Plans."

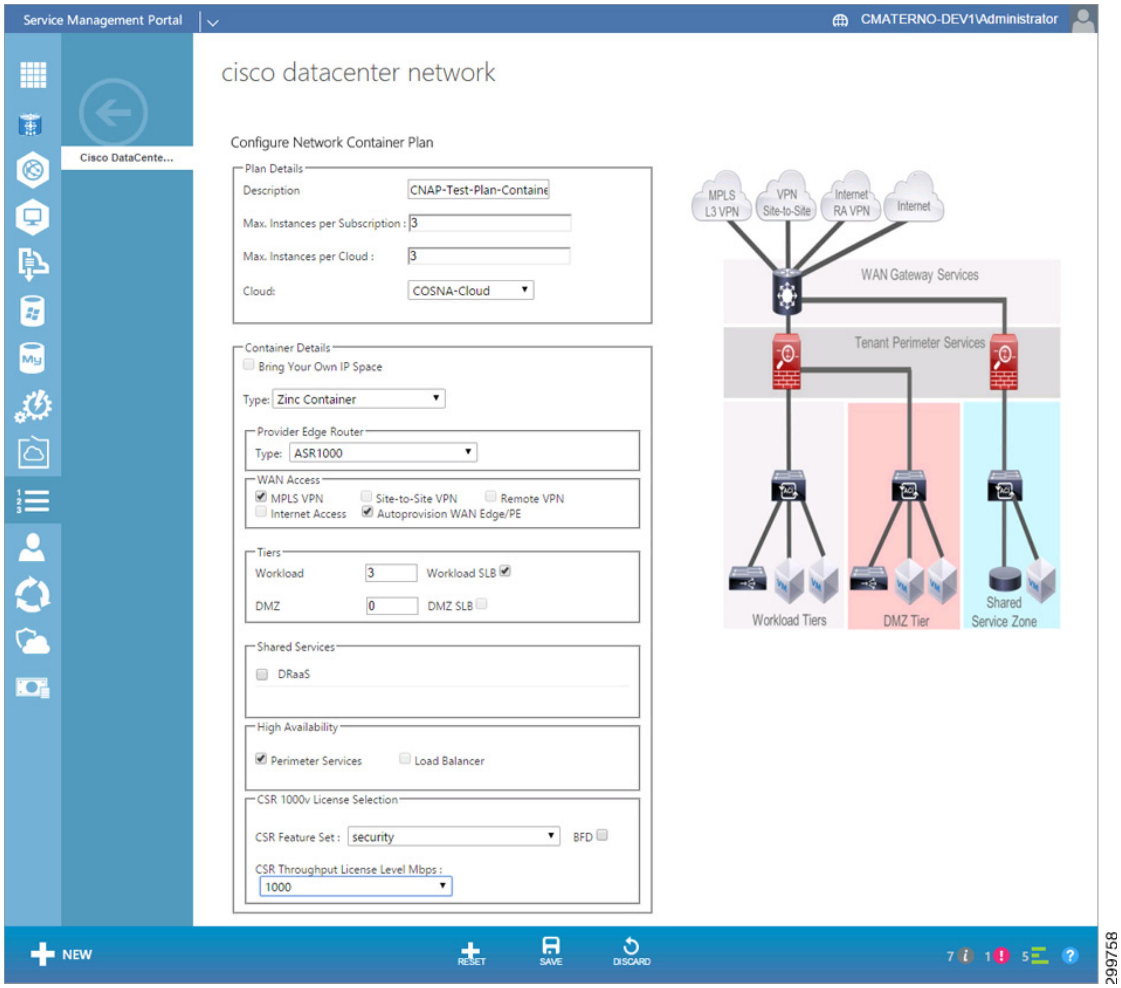
- Tiers: Workload, DMZ, Value Added—Only Workload is available in the current release.
- Shared Services—Select the Shared Services you want to be available in the container plan.Shared Services are displayed only if you have configured them.
- High Availability: Perimeter Services and Load Balancer—High Availability for Load Balancer is not available in the current release.
- High Availability:—When configuring service details in a plan, you can select High Availability for Perimeter Services (Cisco CSR 1000V) and Load Balancer (Citrix NetScaler VPX), although in the current release, HA is not supported for Load Balancer; HA is only available for Perimeter Services:
  - If High Availability is not checked (non-HA mode), only one network service virtual machine instance is created of the Cisco CSR1000V or Citrix NetScaler VPX. The service is still highly available, but an underlying host or OS failure will cause a reboot of the network service virtual machine, interrupting service for seven to 10 minutes.
  - If High Availability is checked, two virtual machine instances are created. In this mode, the two network service virtual machines are clustered and have application-level high availability protocols that will quickly restore service when one of the network service virtual machines has an outage due to software crashes or underlying node failures. The outage time to detection and failover is typically in seconds.

  IP Addresses are used by the Cisco NSO to communicate over the management interface to these virtual machine instances. Based on your HA selection for Perimeter Services, Cisco CNAP will allocate one or two IP addresses for Perimeter Services. For Load Balancer, Cisco CNAP will allocate only one IP address.
- CSR 1000V License Selection—First select the CSR Feature Set using the pull-down menu, then select the CSR Throughput Level using the pull-down menu. The options available on the CSR Throughput Level pull-down menu depend on what you selected for the CSR Feature Set.

  BFD—Bidirectional Forwarding Detection, a network protocol used to detect faults between two forwarding devices connected by a link, is used to ensure that the Cisco CSR 1000V has reachability to specific points in the network. If BFD loses a specific path, traffic can be rerouted to the backup path. If BFD is not configured, a network outage may go unnoticed or extend the time it takes for traffic to re-converge.

Step 10 When you are finished, as shown for example in the following screen, at the bottom of the screen click **Save**.

Figure 4-10 Configure Network Container Plan Screen—Completed Example



cisco datacenter network

Configure Network Container Plan

Plan Details

Description: CNAP-Test-Plan-Containe

Max. Instances per Subscription : 3

Max. Instances per Cloud : 3

Cloud: COSNA-Cloud

Container Details

☐ Bring Your Own IP Space

Type: Zinc Container

Provider Edge Router

Type: ASR1000

WAN Access

☑ MPLS VPN ☐ Site-to-Site VPN ☐ Remote VPN
☐ Internet Access ☑ Autoprovision WAN Edge/PE

Tiers

Workload 3 Workload SLB ☑

DMZ 0 DMZ SLB ☐

Shared Services

☐ DRaaS

High Availability

☑ Perimeter Services ☐ Load Balancer

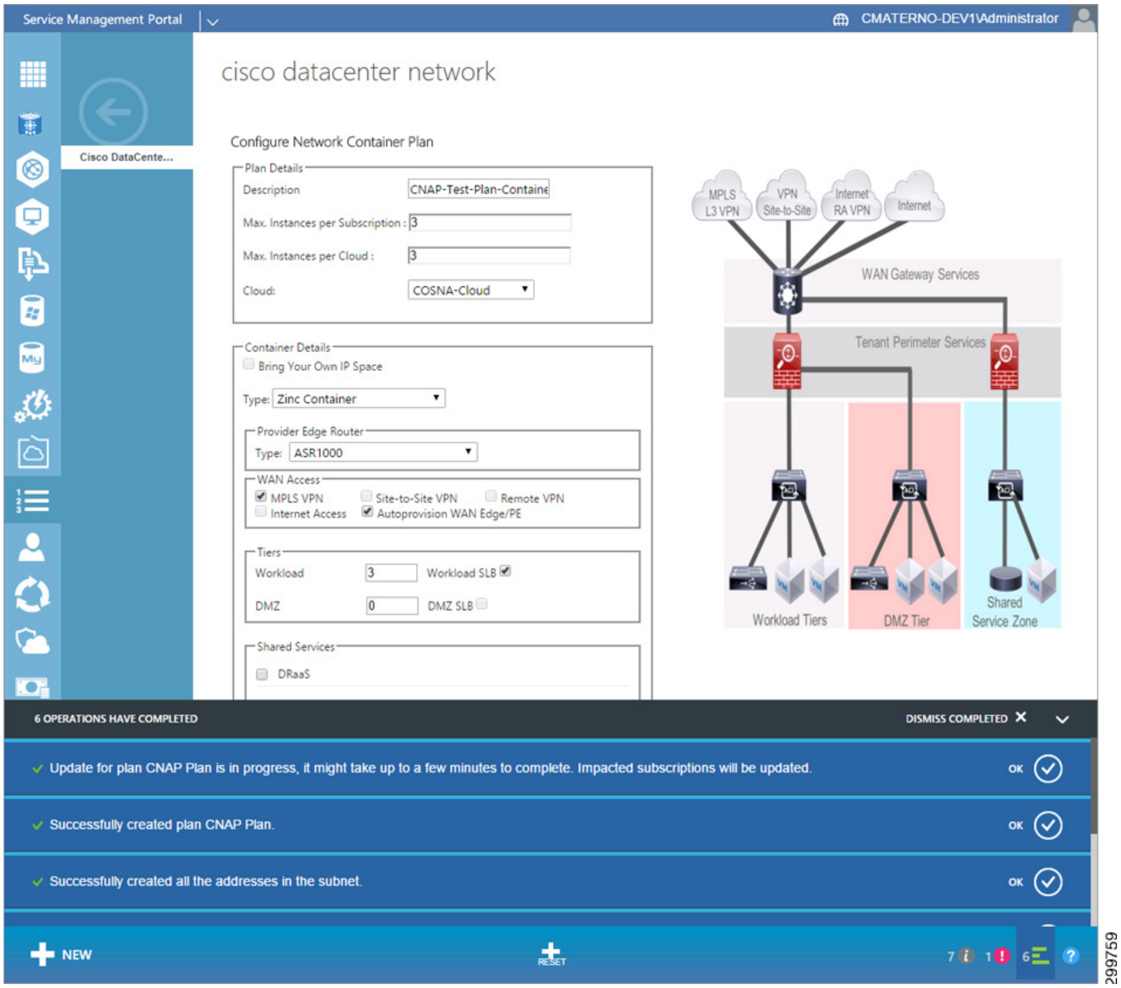
CSR 1000v License Selection

CSR Feature Set : security BFD ☐

CSR Throughput License Level Mbps : 1000

You see a message at the bottom of the screen while the configuration is being saved, as shown in the following screen.

Figure 4-11 Configure Network Container Plan Screen—Update in Progress



Service Management Portal

CMATERNO-DEV1\Administrator

cisco datacenter network

Cisco DataCente...

Configure Network Container Plan

Plan Details

Description: CNAP-Test-Plan-Containe

Max. Instances per Subscription : 3

Max. Instances per Cloud : 3

Cloud: COSNA-Cloud

Container Details

□ Bring Your Own IP Space

Type: Zinc Container

Provider Edge Router

Type: ASR1000

WAN Access

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

Tiers

Workload: 3 Workload SLB ☑

DMZ: 0 DMZ SLB □

Shared Services

□ DRaaS

6 OPERATIONS HAVE COMPLETED

DISMISS COMPLETED ✕

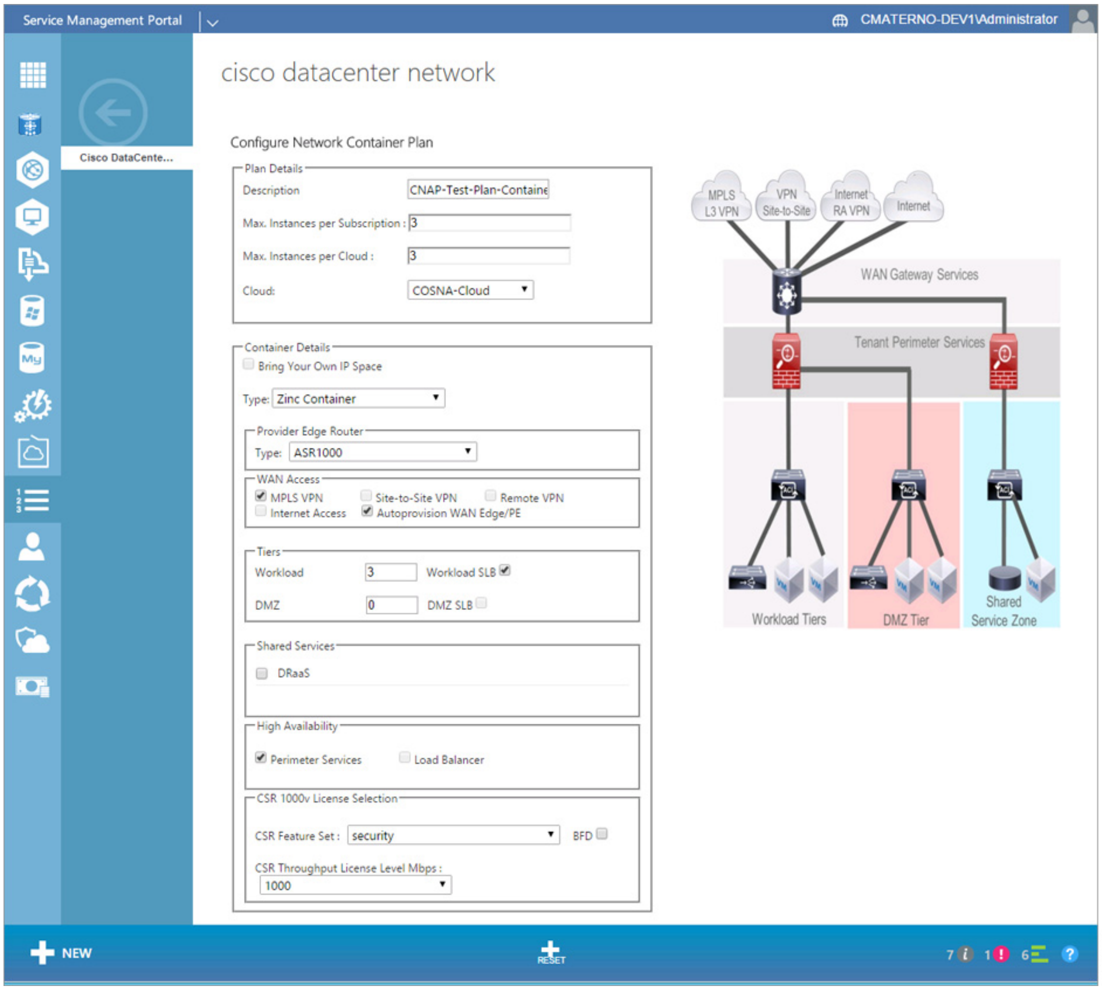
✓ Update for plan CNAP Plan is in progress, it might take up to a few minutes to complete. Impacted subscriptions will be updated. OK

✓ Successfully created plan CNAP Plan. OK

✓ Successfully created all the addresses in the subnet. OK

When the message disappears, you see the following screen.

Figure 4-12 Configure Network Container Plan Screen—Update Completed



cisco datacenter network

Configure Network Container Plan

Plan Details

Description: CNAP-Test-Plan-Containe

Max. Instances per Subscription : 3

Max. Instances per Cloud : 3

Cloud: COSNA-Cloud

Container Details

☐ Bring Your Own IP Space

Type: Zinc Container

Provider Edge Router

Type: ASR1000

WAN Access

☑ MPLS VPN ☐ Site-to-Site VPN ☐ Remote VPN
☐ Internet Access ☑ Autoprovision WAN Edge/PE

Tiers

Workload 3 Workload SLB ☑

DMZ 0 DMZ SLB ☐

Shared Services

☐ DRaaS

High Availability

☑ Perimeter Services ☐ Load Balancer

CSR 1000v License Selection

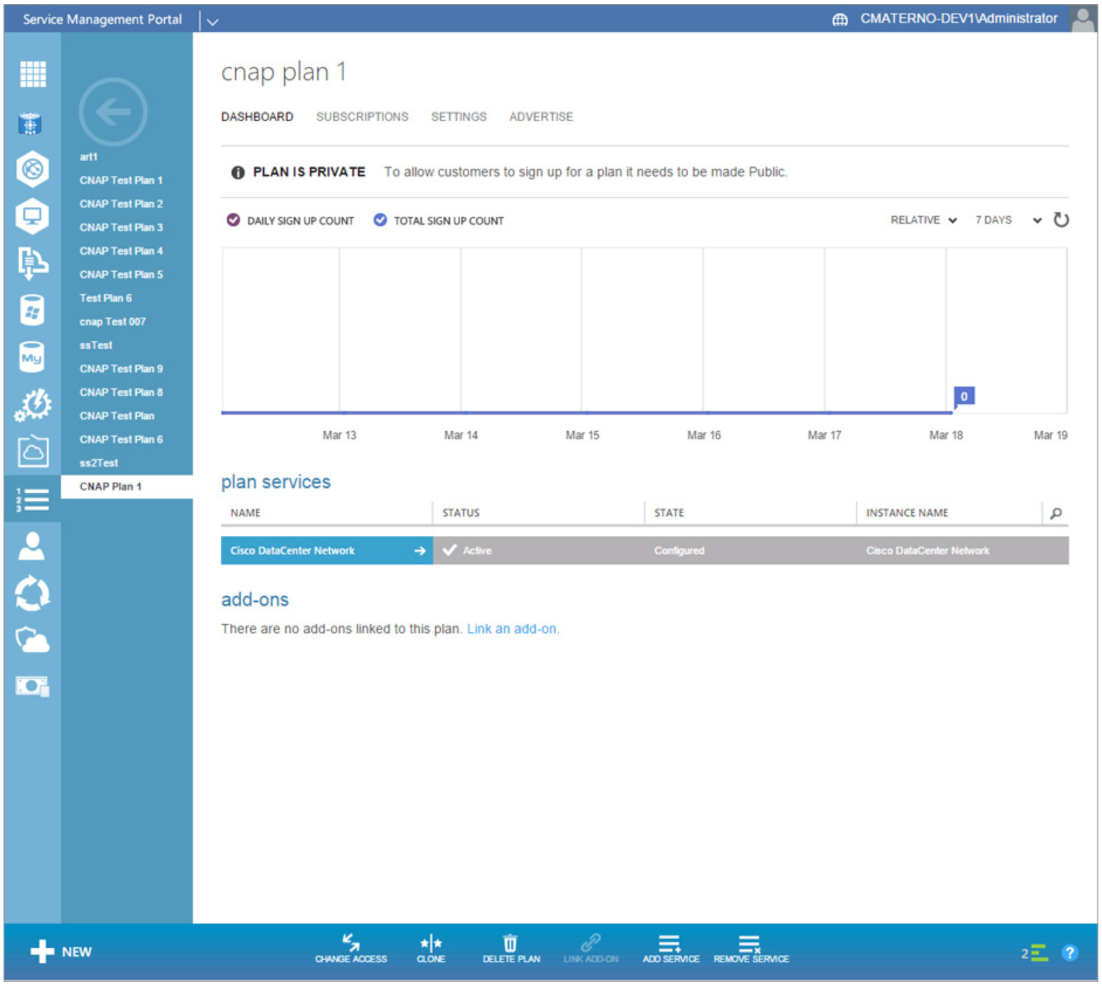
CSR Feature Set : security BFD ☐

CSR Throughput License Level Mbps : 1000

Step 11 Click the back arrow (<–) at the top left.

You see the following screen, which shows the plan is now Active and Configured.

Figure 4-13 Plan Detail Screen—Plan Active and Configured



PLAN IS PRIVATE To allow customers to sign up for a plan it needs to be made Public.

plan services

NAME	STATUS	STATE	INSTANCE NAME
Cisco DataCenter Network	✓ Active	Configured	Cisco DataCenter Network

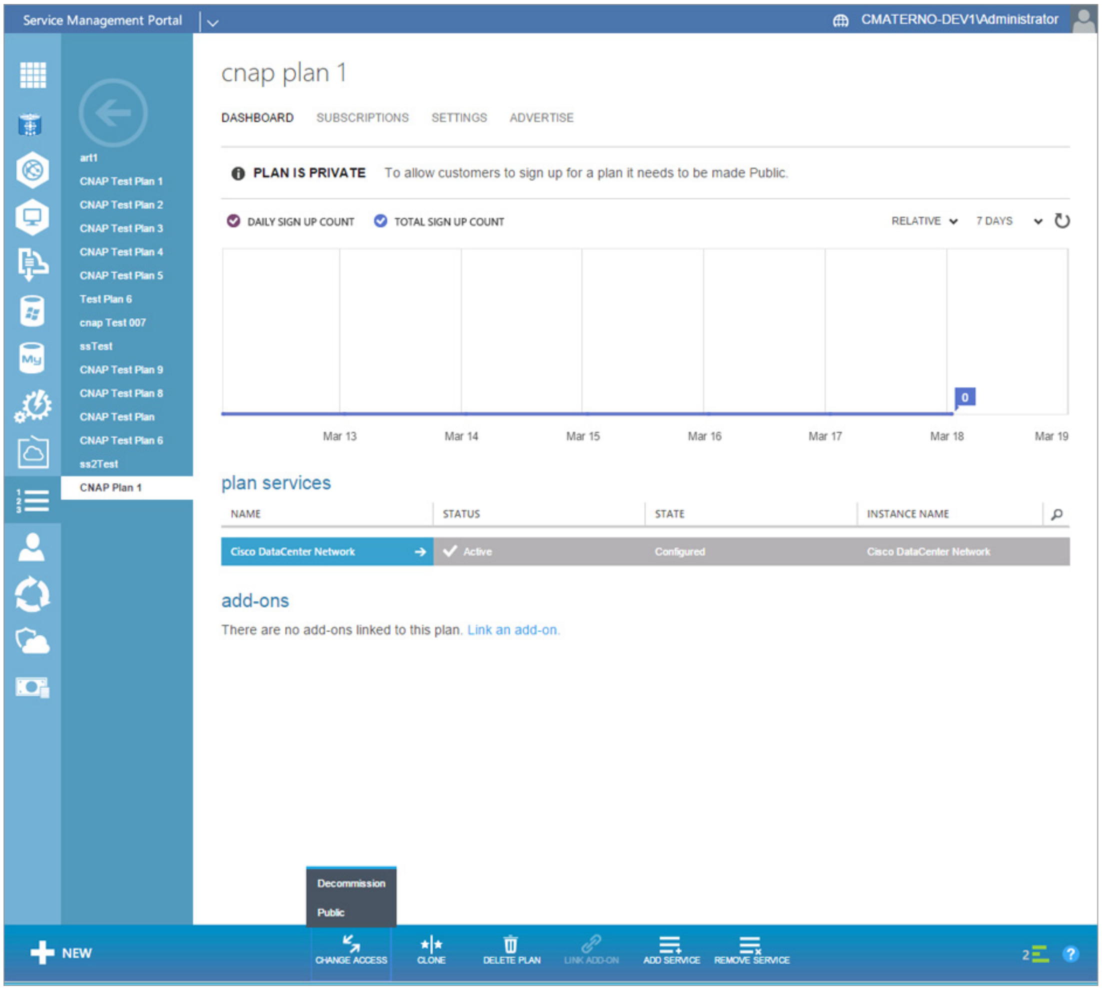
add-ons

There are no add-ons linked to this plan. Link an add-on.

Step 12 As shown at the top, the **PLAN IS PRIVATE**. To make it public so tenants can subscribe to it, at the bottom of the screen click **Change Access** and then **Public**, as shown in the following screen.

Note You can leave the plan Private and then manually assign tenants to the plan.

Figure 4-14 Change Access to Public Screen



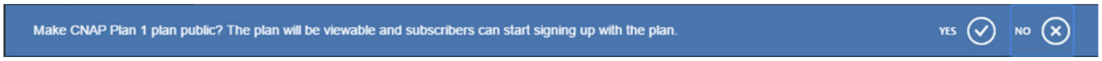
PLAN IS PRIVATE To allow customers to sign up for a plan it needs to be made Public.

NAME	STATUS	STATE	INSTANCE NAME
Cisco DataCenter Network	✓ Active	Configured	Cisco DataCenter Network

There are no add-ons linked to this plan. Link an add-on.

Step 13 You see a pop-up asking you to confirm you want the plan to be public, as shown in the following screen. Click **Yes**.

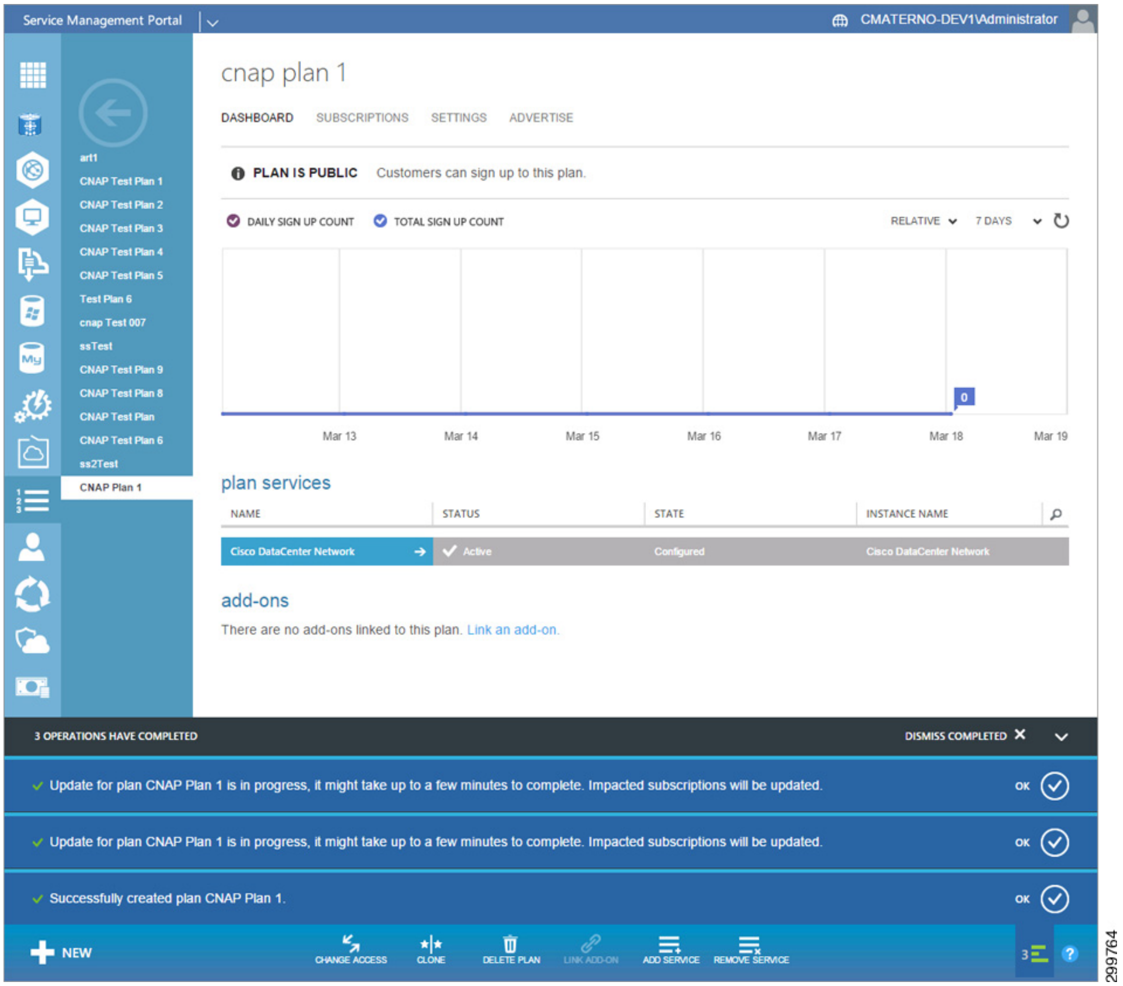
Figure 4-15 Confirm Public Access Screen



Make CNAP Plan 1 plan public? The plan will be viewable and subscribers can start signing up with the plan.

You see a message at the bottom of the screen while the configuration is being saved, as shown in the following screen.

Figure 4-16 Change Access to Public Screen —Update in Progress



cnap plan 1

PLAN IS PUBLIC Customers can sign up to this plan.

plan services

NAME	STATUS	STATE	INSTANCE NAME
Cisco DataCenter Network	Active	Configured	Cisco DataCenter Network

add-ons

There are no add-ons linked to this plan. Link an add-on.

3 OPERATIONS HAVE COMPLETED

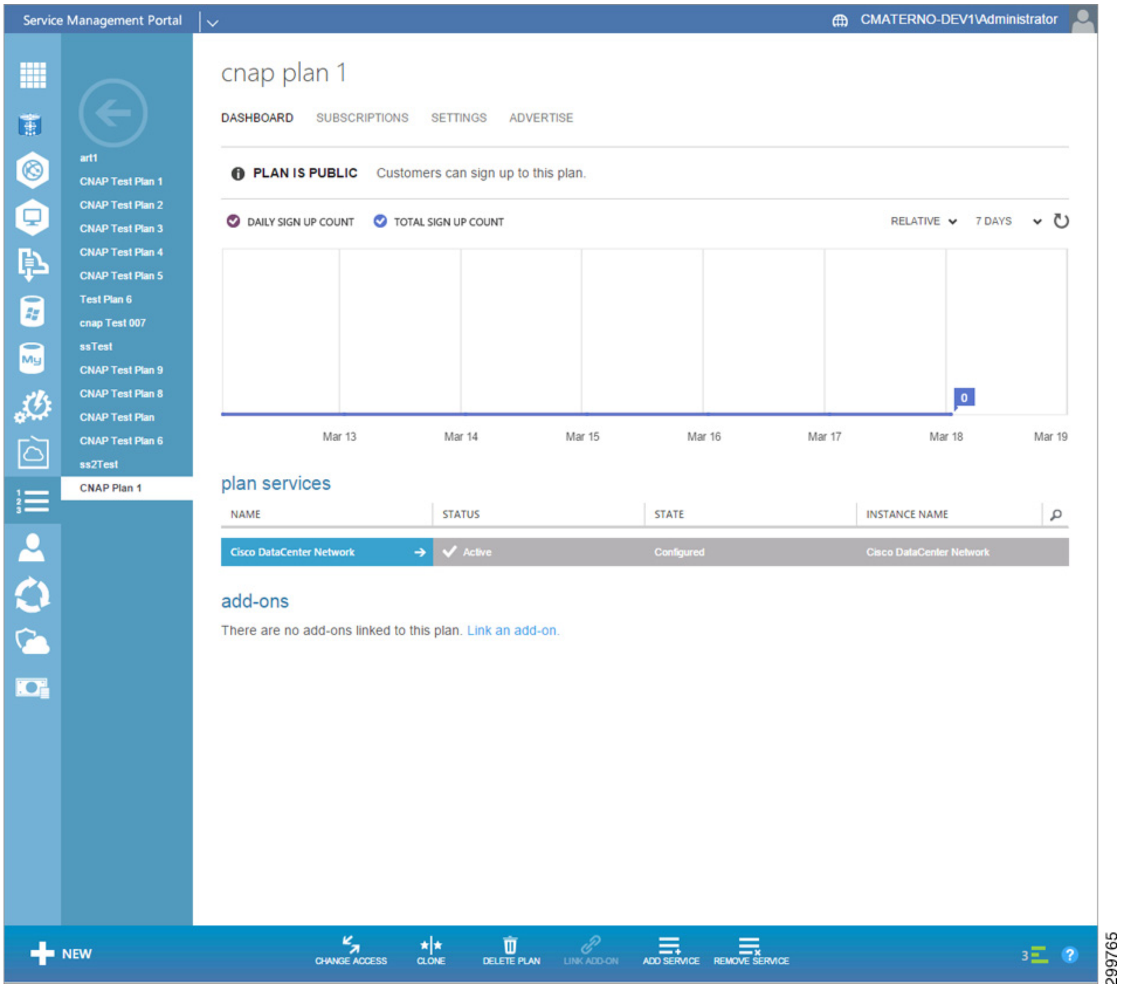
✓ Update for plan CNAP Plan 1 is in progress, it might take up to a few minutes to complete. Impacted subscriptions will be updated.

✓ Update for plan CNAP Plan 1 is in progress, it might take up to a few minutes to complete. Impacted subscriptions will be updated.

✓ Successfully created plan CNAP Plan 1.

When the message disappears, you see the following screen. As shown at the top, now the **PLAN IS PUBLIC**.

Figure 4-17 ***Plan is Public Screen***



PLAN IS PUBLIC Customers can sign up to this plan.

NAME	STATUS	STATE	INSTANCE NAME
Cisco DataCenter Network	✓ Active	Configured	Cisco DataCenter Network

There are no add-ons linked to this plan. Link an add-on.

Note that there are no subscriptions since the plan is new and tenants have not yet subscribed to it.

Note If you added a Virtual Machine Cloud plan to a Cisco Datacenter Network plan, then you **must** first have a container deployed.

CHAPTER 5

Managing Container Plans

The Service Provider administrator can use the Cisco CNAP Admin Portal to:

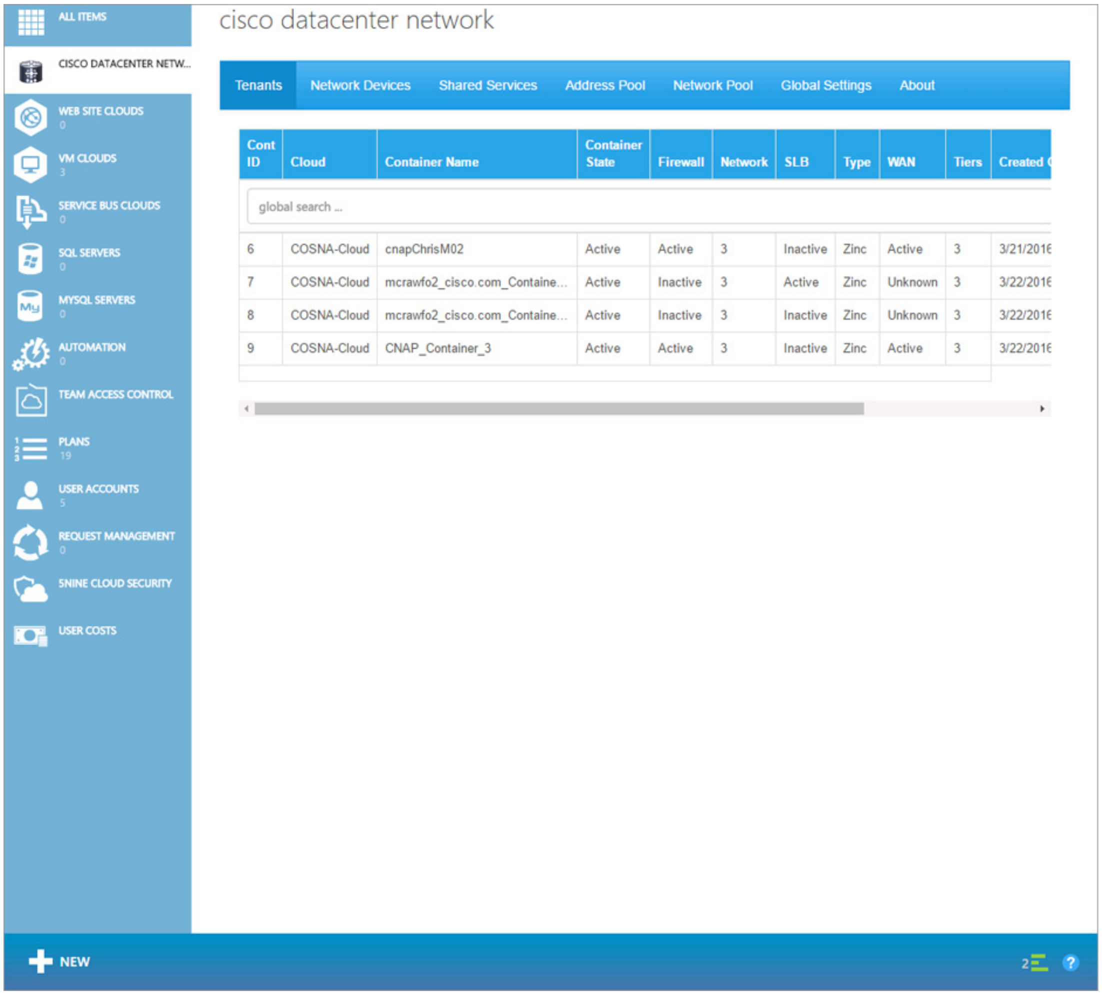
- Display summary information about a container
- Delete a container
- Display and modify gateway information about a container:
  - Look at information about a gateway.
  - Add a gateway (you cannot configure a WAN Gateway until a tenant has created a container and the container is active).
  - Modify a gateway.
  - Delete a gateway.
- Display and modify firewall information about a container:
  - View summary information about a firewall.
  - View the hierarchy of information on the Firewall tab.
  - Set up a tenant perimeter 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 List.
  - Create a new object group.
  - Change an object group.
- Display load balancer information about a container:
  - Confirm the licensing of a Citrix NetScaler VPX.
  - Look at load balancer information about a container.

Note Since Cisco CNAP is also pushing configurations for the automation of work flows on devices, certain precautions need to be followed when manually configuring devices to avoid disrupting Cisco CNAP-based automation. Changing configurations pushed from Cisco CNAP will cause the automated provisioning system to malfunction, which in some cases could cause all automated provisioning to stop until the error conditions are manually remediated. In general on the data center provider edge, all configurations under the tenant VRFs pushed by Cisco CNAP should not be edited or changed, including sub-interfaces and routing. Similarly on the Cisco APIC, the Cisco APIC tenants configured by Cisco CNAP should only be changed by Cisco CNAP. Any configurations pushed by Cisco CNAP should not be manually edited. For more information, see *Installing Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform, Release 1.1*.

Viewing Summary Information about Containers Managed by Cisco CNAP

The Tenants tab displays a list of all the tenant containers currently managed by Cisco CNAP, as shown on the Tenants Tab screen.

Figure 5-1 Tenants Tab Screen



Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created (
6	COSNA-Cloud	cnapChrisM02	Active	Active	3	Inactive	Zinc	Active	3	3/21/2016
7	COSNA-Cloud	mcrawfo2_cisco.com_Containe...	Active	Inactive	3	Active	Zinc	Unknown	3	3/22/2016
8	COSNA-Cloud	mcrawfo2_cisco.com_Containe...	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/22/2016
9	COSNA-Cloud	CNAP_Container_3	Active	Active	3	Inactive	Zinc	Active	3	3/22/2016

Each container row visible on the Tenants tab shows the following information:

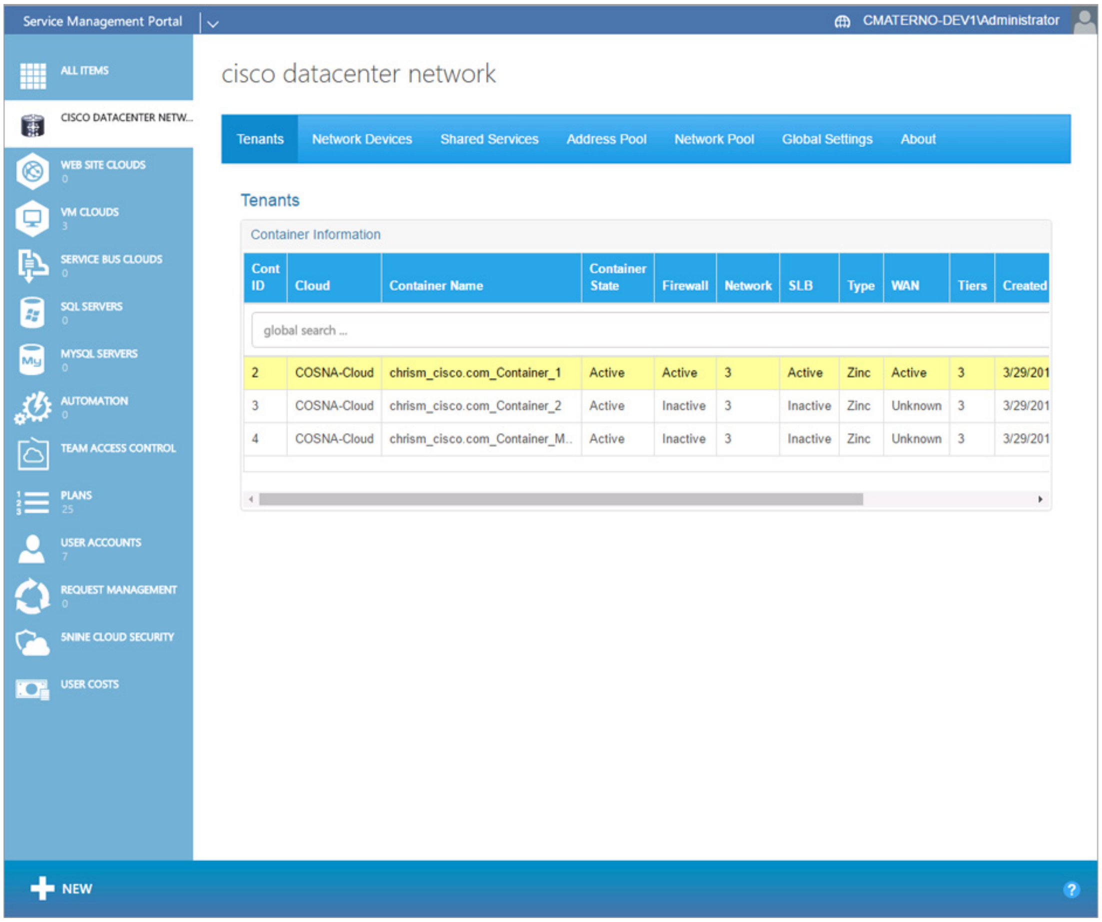
- Cont ID—The ID of the container.
- Cloud—Name of the Cloud Service in SCVMM to which the container is associated.
- Container Name—Descriptive name of the container.

- Container State—The current state of the container:
  - Active
  - Creating
  - Inactive
- Firewall—The status of all Firewall Services associated with a particular container.
- Network—Total number of networks in the container.
- SLB—The status of all Load Balancer Services associated with a particular container.
- Type—The type of container, which in the current release is only Zinc.
- WAN—The status of each of the WAN Gateway Services (MPLS VPN, Site-to-Site and Remote Access VPN, or Internet Access) associated with a particular container.
- Tiers—The number of tiers currently configured in the container.
- 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.

Viewing Summary Information about a Container

Step 1 To display summary information about a specific container, on the Tenants tab click on the row with the container you want to view, as shown in the following screen.

Figure 5-2 Tenants Tab—Container Selected



Tenants

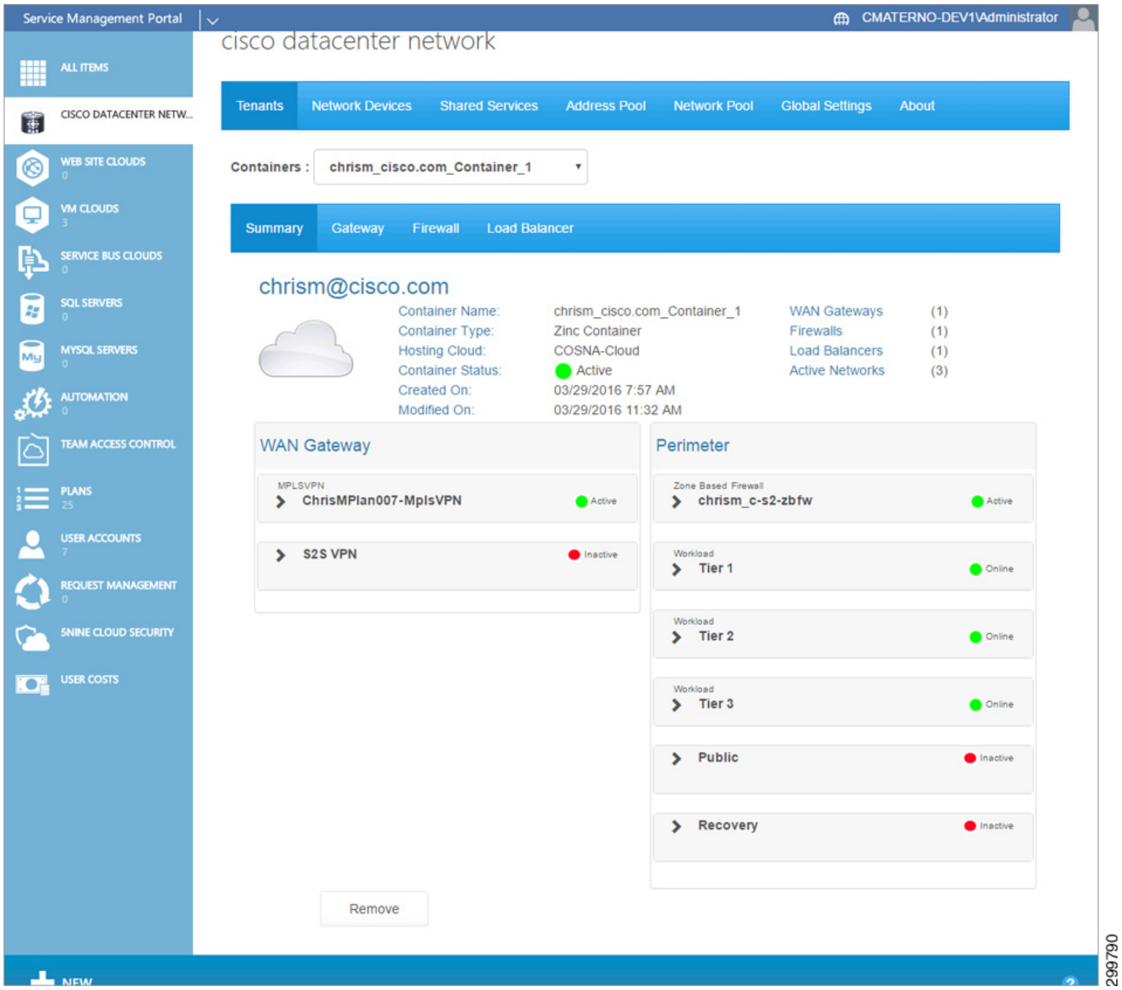
Container Information

global search ...

Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created
2	COSNA-Cloud	chrism_cisco.com_Container_1	Active	Active	3	Active	Zinc	Active	3	3/29/201
3	COSNA-Cloud	chrism_cisco.com_Container_2	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201
4	COSNA-Cloud	chrism_cisco.com_Container_M..	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201

You see the Tenants Summary screen.

Figure 5-3 Tenants Summary Screen



Containers : chrism_cisco.com_Container_1

chrism@cisco.com

Container Name:	chrism_cisco.com_Container_1	WAN Gateways	(1)
Container Type:	Zinc Container	Firewalls	(1)
Hosting Cloud:	COSNA-Cloud	Load Balancers	(1)
Container Status:	● Active	Active Networks	(3)
Created On:	03/29/2016 7:57 AM		
Modified On:	03/29/2016 11:32 AM		

WAN Gateway

- MPLSVPN ChrisMPlan007-MplsVPN ● Active
- S2S VPN ● Inactive

Perimeter

- Zone Based Firewall chrism_c-s2-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 the WAN Gateway services configured in the container (only MPLS VPN in current release) and a list of all the perimeter network services configured in the container (firewall, tiers, DMZ, etc.).

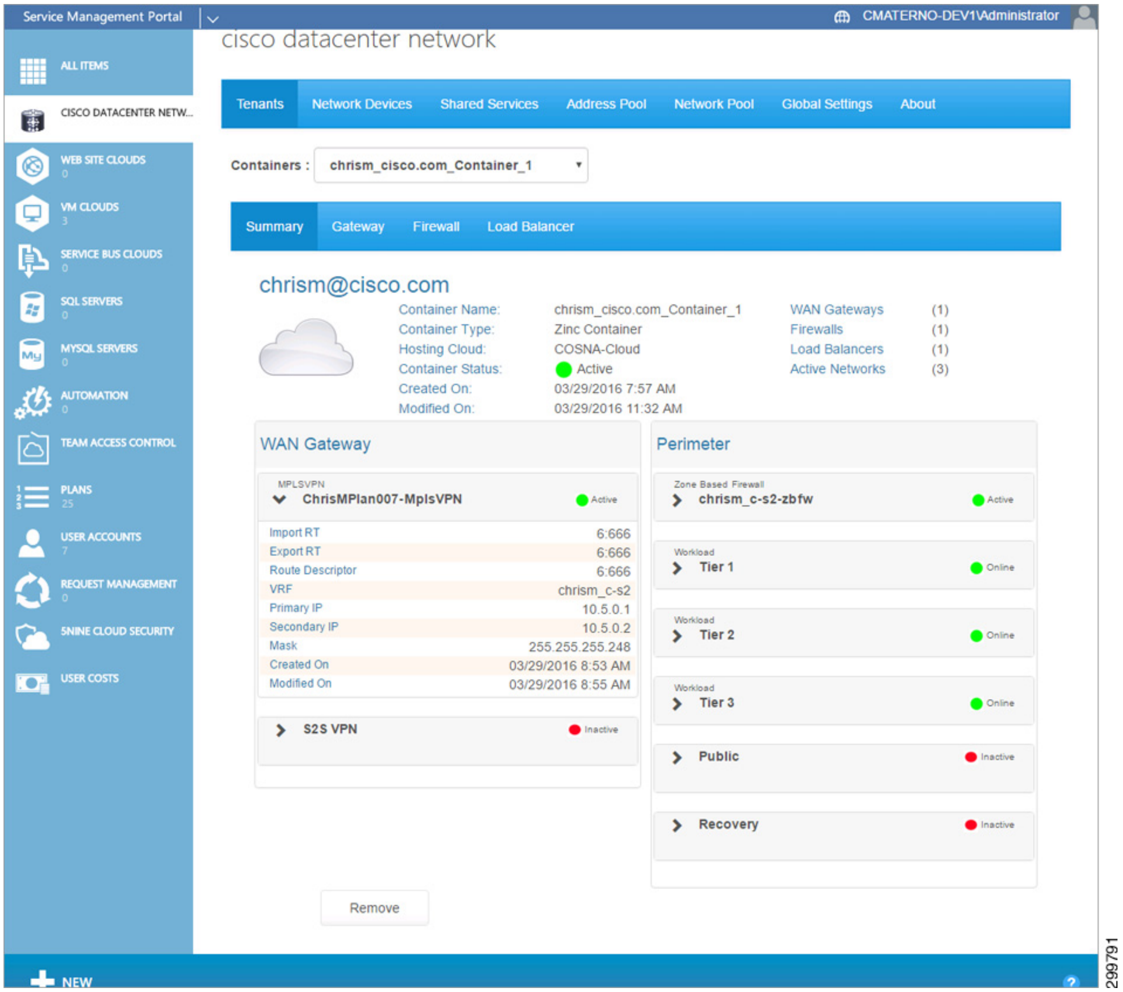
Specific information above the WAN Gateway and Perimeter tables includes:

- 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 Citrix NetScaler VPX resides in tier1 by design, but it can load balance any server in tier1, tier2, and tier3. 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 screens for the MPLS VPN WAN Gateway, Perimeter Firewall, and Perimeter Tier 1.

Figure 5-4 Summary Tab—WAN Gateway MPLS VPN Details



Containers : chrism_cisco.com_Container_1

chrism@cisco.com

Container Name:	chrism_cisco.com_Container_1	WAN Gateways	(1)
Container Type:	Zinc Container	Firewalls	(1)
Hosting Cloud:	COSNA-Cloud	Load Balancers	(1)
Container Status:	● Active	Active Networks	(3)
Created On:	03/29/2016 7:57 AM		
Modified On:	03/29/2016 11:32 AM		

WAN Gateway

MPLSVPN
ChrisMPlan007-MplsVPN ● Active

Import RT	6:666
Export RT	6:666
Route Descriptor	6:666
VRF	chrism_c-s2
Primary IP	10.5.0.1
Secondary IP	10.5.0.2
Mask	255.255.255.248
Created On	03/29/2016 8:53 AM
Modified On	03/29/2016 8:55 AM

S2S VPN ● Inactive

Perimeter

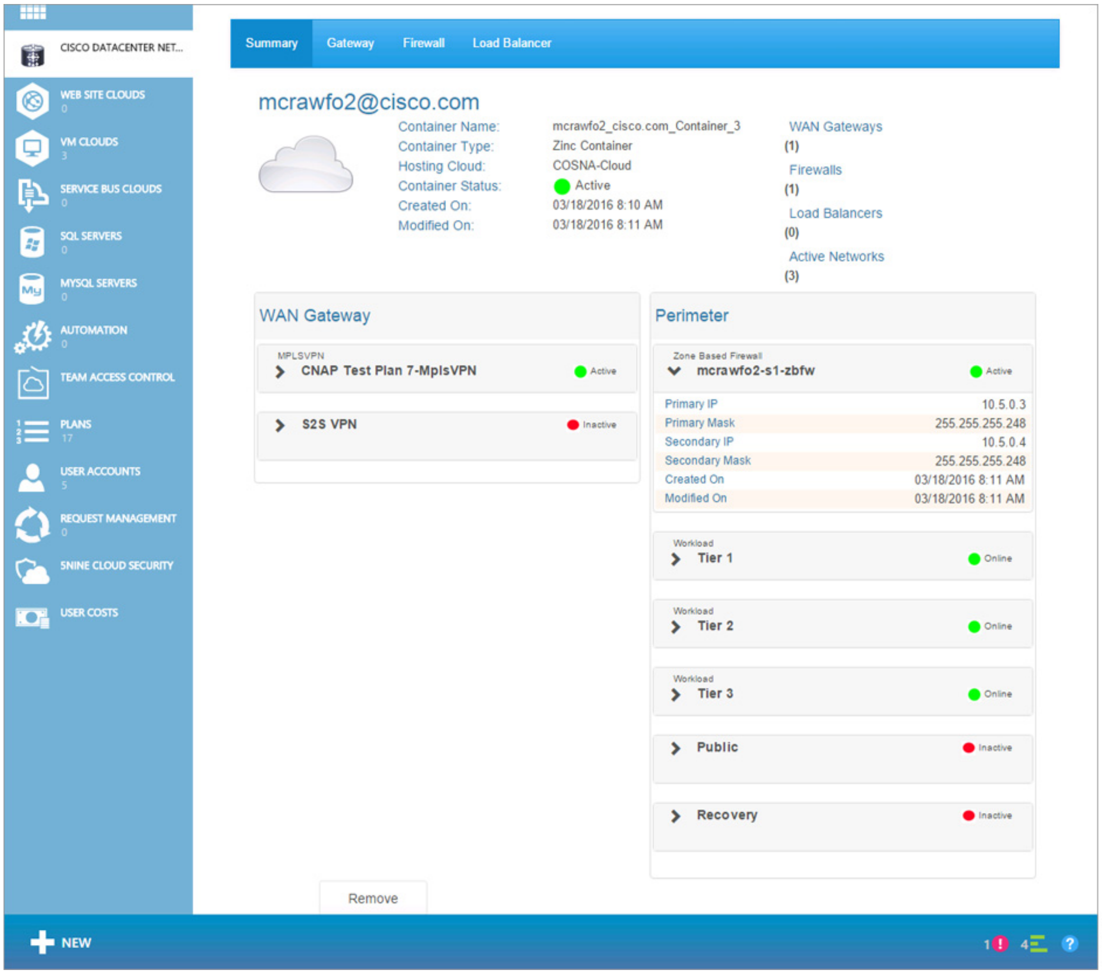
Zone Based Firewall	chrism_c-s2-zbfw	● Active
Workload	Tier 1	● Online
Workload	Tier 2	● Online
Workload	Tier 3	● Online
	Public	● Inactive
	Recovery	● Inactive

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—Displays the RT based on your network design.
- Export RT—Displays the RT based on your network design.
- Route Descriptor—Displays the descriptor based on your 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 5-5 Summary Tab—Perimeter Firewall Details



mcrawfo2@cisco.com

Container Name:	mcrawfo2_cisco.com_Container_3
Container Type:	Zinc Container
Hosting Cloud:	COSNA-Cloud
Container Status:	● Active
Created On:	03/18/2016 8:10 AM
Modified On:	03/18/2016 8:11 AM

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

WAN Gateway

- MPLSVPN — CNAP Test Plan 7-MplsVPN — ● Active
- S2S VPN — ● Inactive

Perimeter

Zone Based Firewall — mcrawfo2-s1-zbfw — ● Active

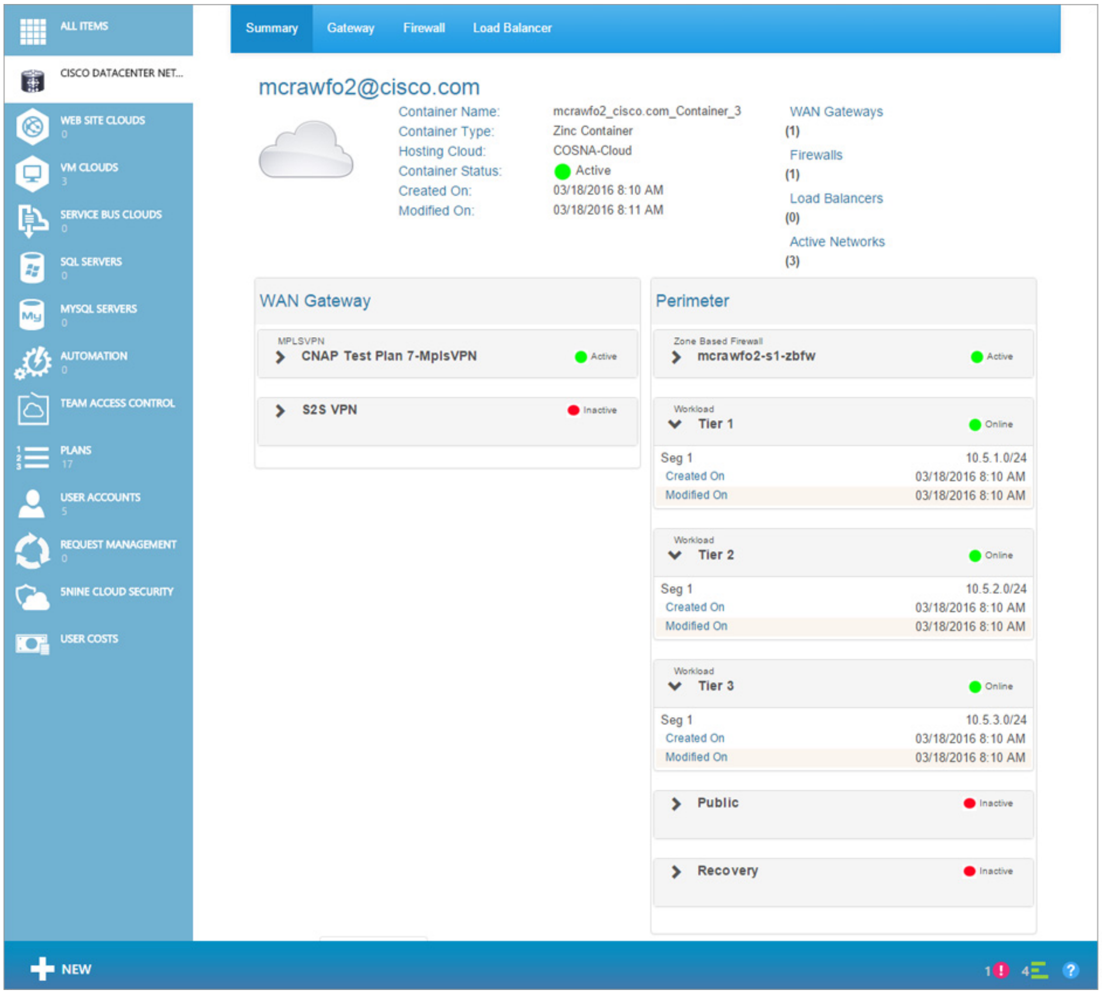
Primary IP	10.5.0.3
Primary Mask	255.255.255.248
Secondary IP	10.5.0.4
Secondary Mask	255.255.255.248
Created On	03/18/2016 8:11 AM
Modified On	03/18/2016 8:11 AM

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

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 in the form.
- Modified On:—Displays the date and time when the firewall was last modified.

Figure 5-6 Summary Tab—Perimeter Tier Details



mcrawfo2@cisco.com

Container Name:	mcrawfo2_cisco.com_Container_3
Container Type:	Zinc Container
Hosting Cloud:	COSNA-Cloud
Container Status:	● Active
Created On:	03/18/2016 8:10 AM
Modified On:	03/18/2016 8:11 AM

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

WAN Gateway

- MPLSVPN — CNAP Test Plan 7-MplsVPN — ● Active
- S2S VPN — ● Inactive

Perimeter

- Zone Based Firewall — mcrawfo2-s1-zbfw — ● Active
- Workload — Tier 1 — ● Online
  - Seg 1: 10.5.1.0/24
  - Created On: 03/18/2016 8:10 AM
  - Modified On: 03/18/2016 8:10 AM
- Workload — Tier 2 — ● Online
  - Seg 1: 10.5.2.0/24
  - Created On: 03/18/2016 8:10 AM
  - Modified On: 03/18/2016 8:10 AM
- Workload — Tier 3 — ● Online
  - Seg 1: 10.5.3.0/24
  - Created On: 03/18/2016 8:10 AM
  - Modified On: 03/18/2016 8:10 AM
- Public — ● Inactive
- Recovery — ● Inactive

Information in the Perimeter table for each Tier includes:

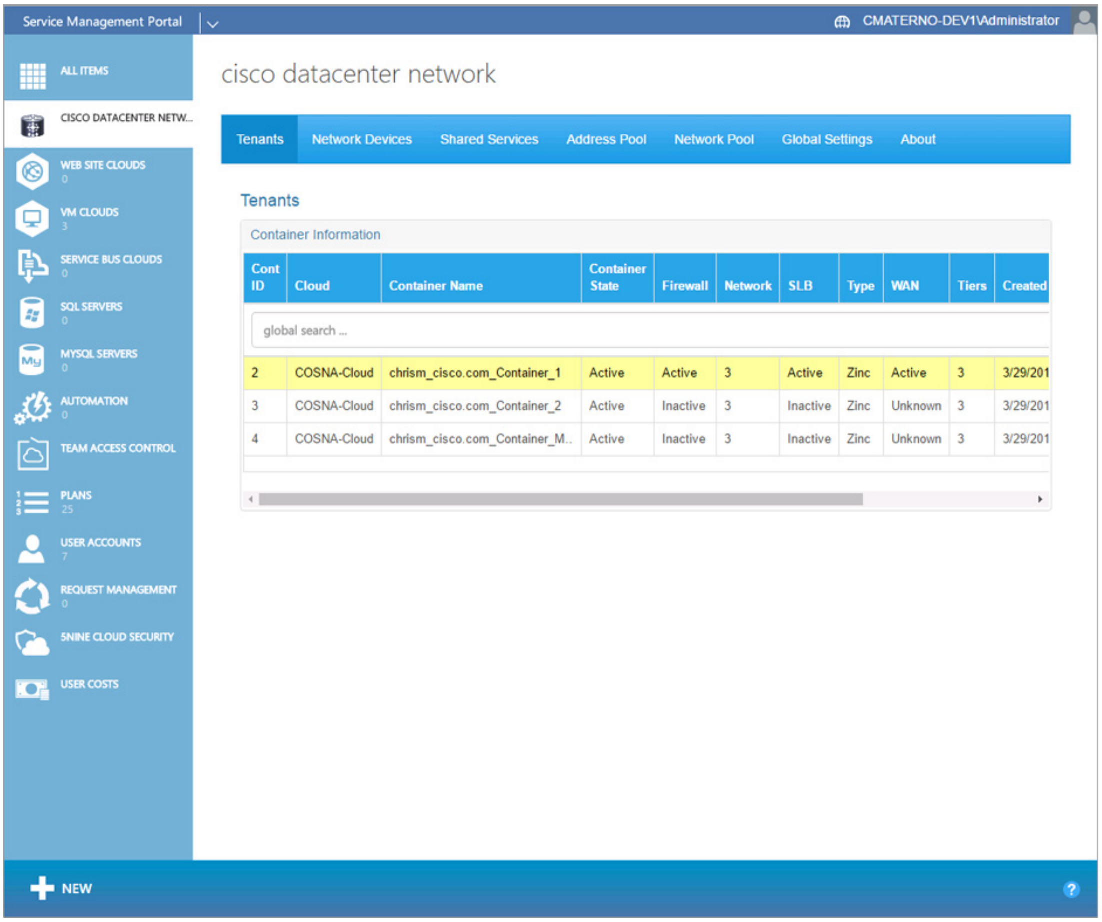
- Seg 1—IP Address of the tier segment.
- Created On:—Displays the date and time when the Tier 1 was created in the form mm-dd-yyyy hh:mm:ss.
- Modified On:—Displays the date and time when the tier was last modified in the form mm-dd-yyyy hh:mm:ss.

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 delete a container, on the Tenants tab click on the row with the container you want to delete, as shown in the following screen.

Figure 5-7 Tenants Tab—Container Selected



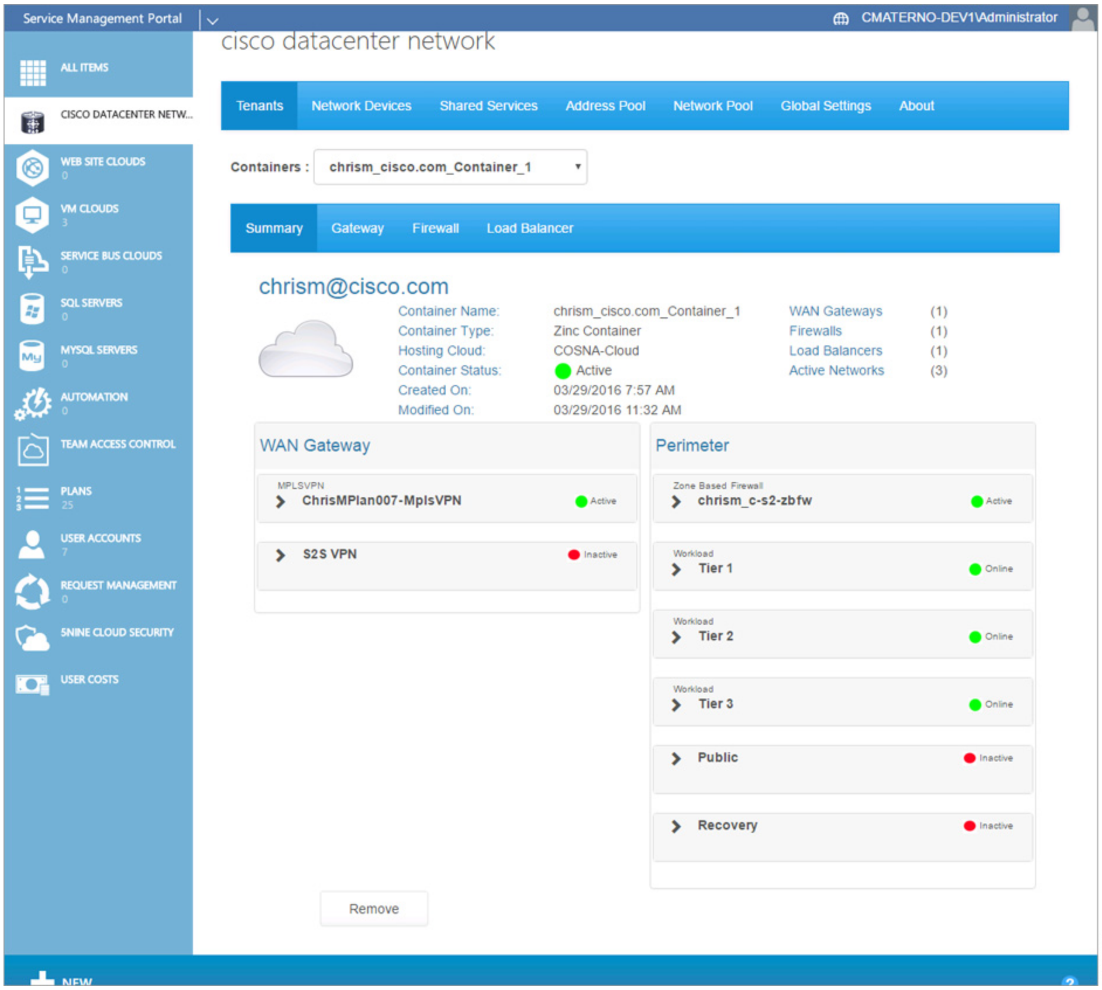
Tenants

Container Information

Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created
2	COSNA-Cloud	chrism_cisco.com_Container_1	Active	Active	3	Active	Zinc	Active	3	3/29/201
3	COSNA-Cloud	chrism_cisco.com_Container_2	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201
4	COSNA-Cloud	chrism_cisco.com_Container_M..	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201

You see the Tenants Summary screen.

Figure 5-8 Tenants Summary Screen



Containers : chrism_cisco.com_Container_1

chrism@cisco.com

Container Name: chrism_cisco.com_Container_1
Container Type: Zinc Container
Hosting Cloud: COSNA-Cloud
Container Status: ● Active
Created On: 03/29/2016 7:57 AM
Modified On: 03/29/2016 11:32 AM

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

WAN Gateway

- MPLSVPN ChrisMPlan007-MplsVPN ● Active
- S2S VPN ● Inactive

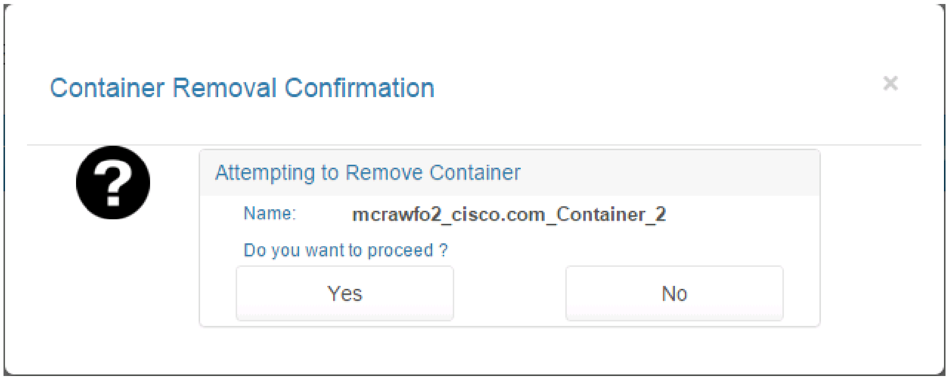
Perimeter

- Zone Based Firewall chrism_c-s2-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 5-9 Confirm Container Deletion



Container Removal Confirmation

Attempting to Remove Container

Name: mcrawfo2_cisco.com_Container_2

Do you want to proceed ?

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

Setting Up and Managing WAN Gateways

Tenants can access their cloud networks via a WAN. This section describes the provisioning of WAN Gateways for tenant containers, which in this release includes two options:

- Automated provisioning of MPLS L3VPN-based access for the tenant, including provisioning of the Data Center WAN Edge/PE.
- No automated provisioning of the Data Center PE. A VLAN-based hand-off from the Data Center PE to the Data Center Fabric/network is provisioned for each tenant.

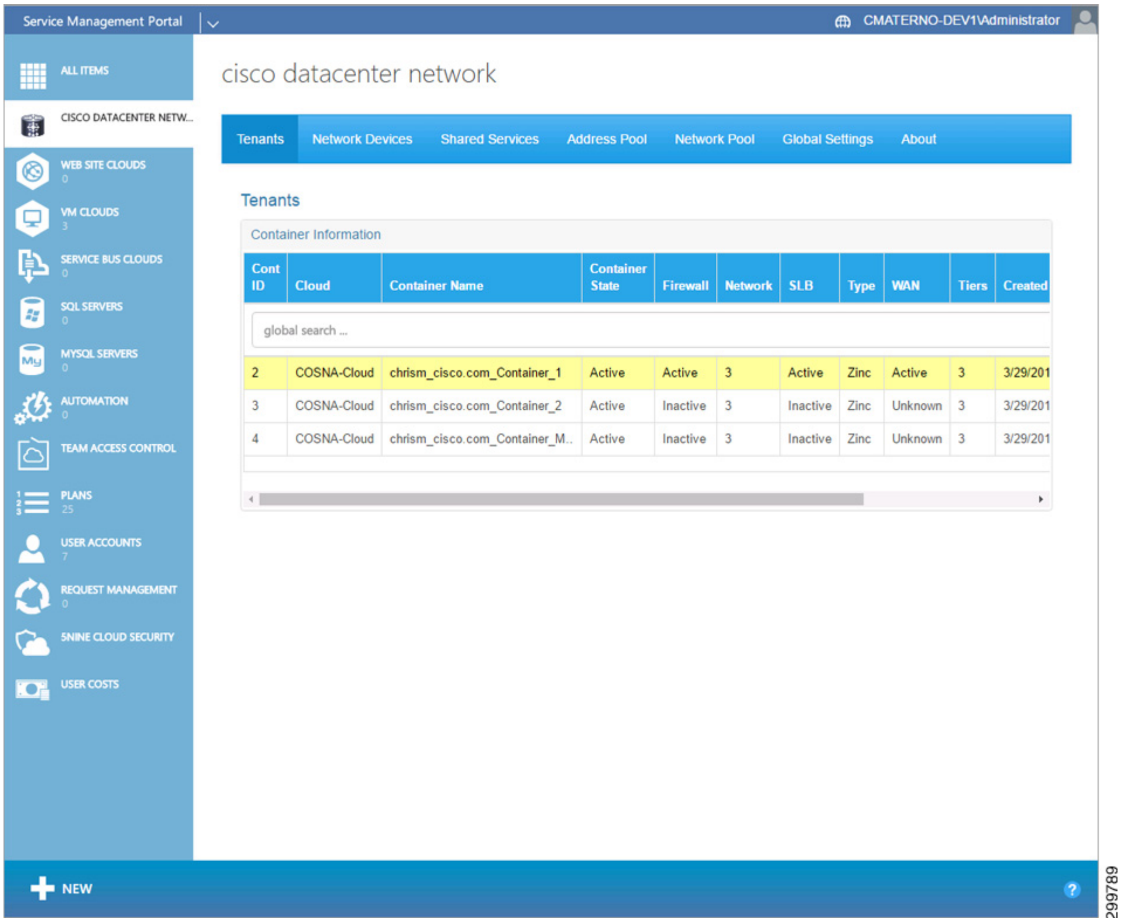
On the gateway tab screen, you can:

- Look at information about a gateway.
- Add a gateway.

  You should not configure a WAN Gateway until a tenant has created a container and the container is active. Check that the container is created and shown as active before provisioning the WAN Gateway.
- Modify a gateway.
- Remove a gateway.

Step 1 To display gateway information about a specific container, on the Tenants tab click on the row with the container you want to view, as shown in the following screen.

Figure 5-10 ***Tenants Tab—Container Selected Screen***



Tenants

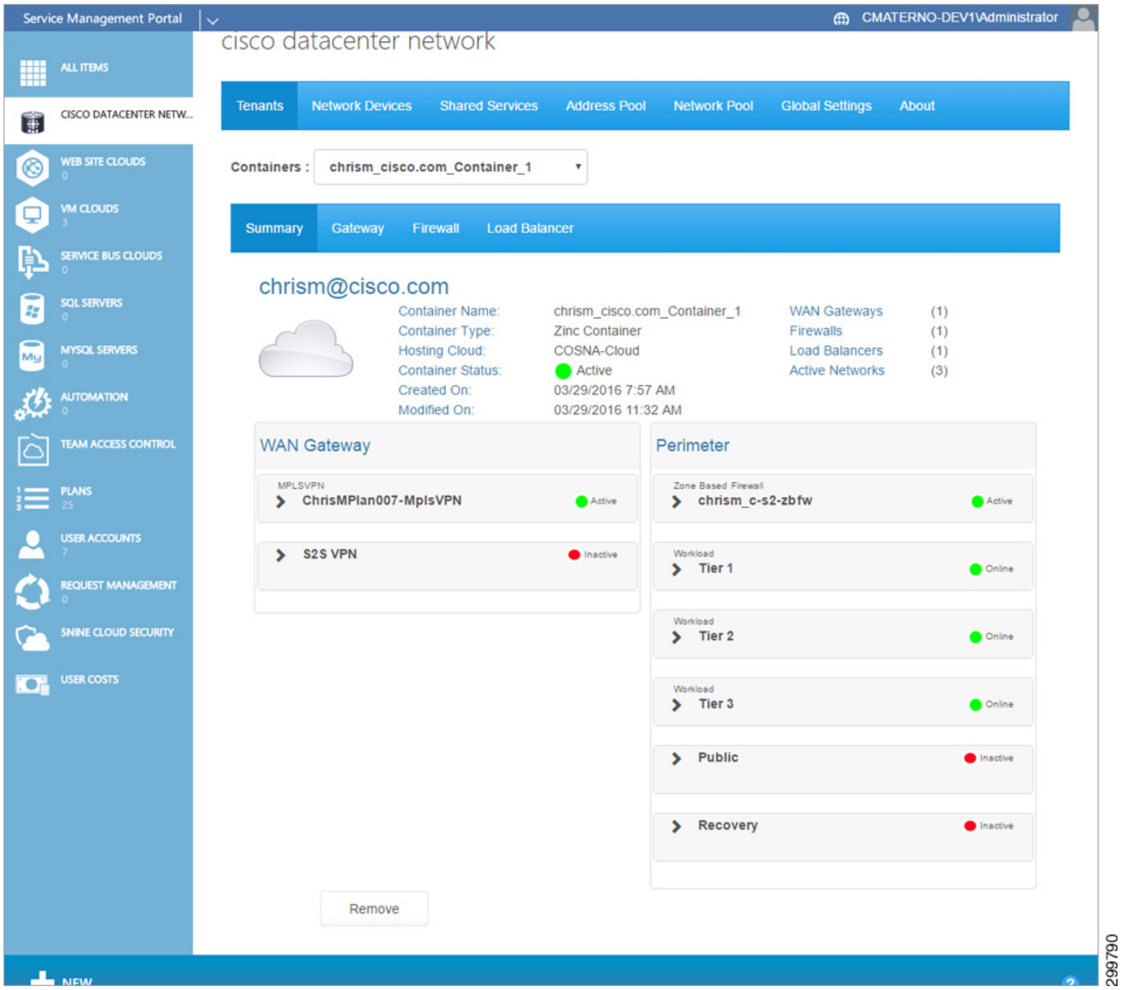
Container Information

global search ...

Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created
2	COSNA-Cloud	chrism_cisco.com_Container_1	Active	Active	3	Active	Zinc	Active	3	3/29/201
3	COSNA-Cloud	chrism_cisco.com_Container_2	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201
4	COSNA-Cloud	chrism_cisco.com_Container_M..	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201

You see the Tenants Summary screen.

Figure 5-11 Tenants Summary Screen



Containers : chrism_cisco.com_Container_1

chrism@cisco.com

Container Name:	chrism_cisco.com_Container_1	WAN Gateways	(1)
Container Type:	Zinc Container	Firewalls	(1)
Hosting Cloud:	COSNA-Cloud	Load Balancers	(1)
Container Status:	● Active	Active Networks	(3)
Created On:	03/29/2016 7:57 AM		
Modified On:	03/29/2016 11:32 AM		

WAN Gateway

- MPLSVPN ChrisMPlan007-MplsVPN ● Active
- S2S VPN ● Inactive

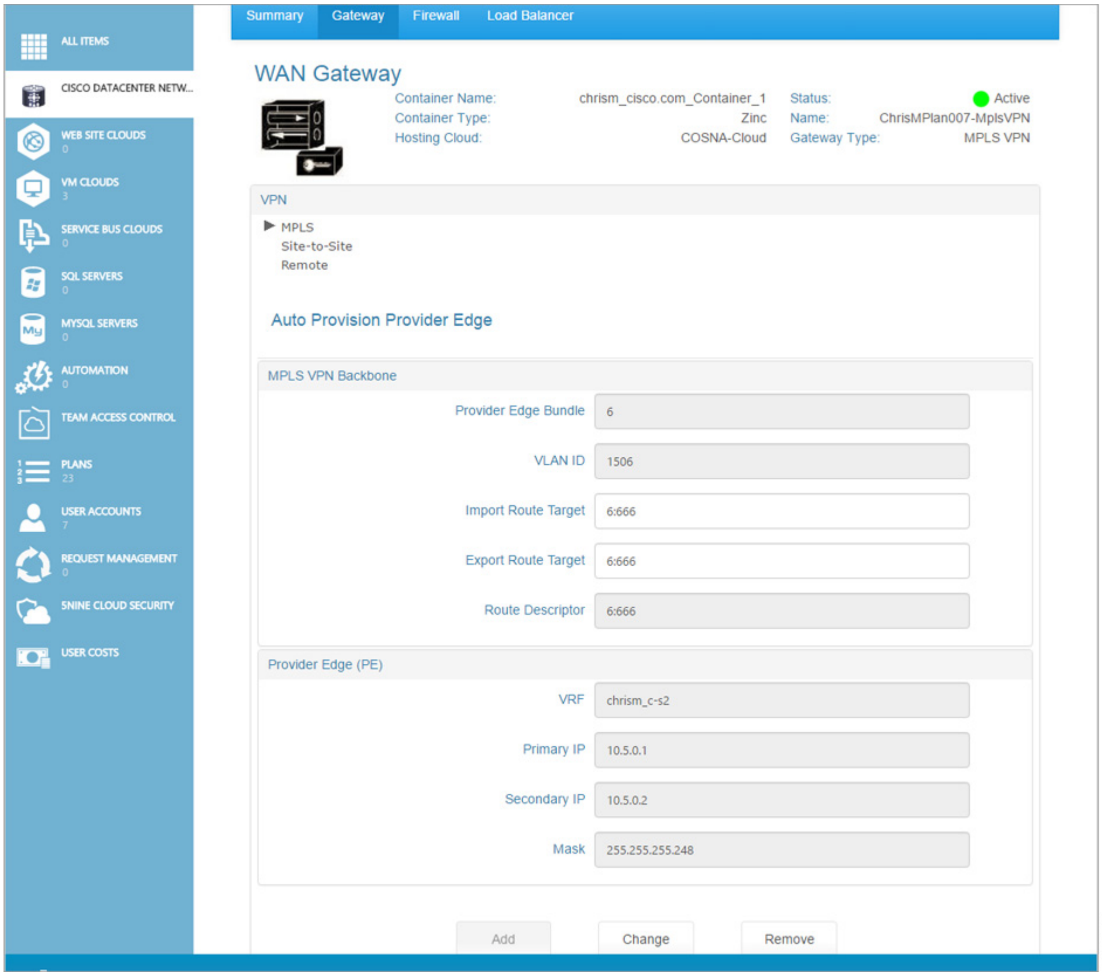
Perimeter

- Zone Based Firewall chrism_c-s2-zbfw ● Active
- Workload Tier 1 ● Online
- Workload Tier 2 ● Online
- Workload Tier 3 ● Online
- Public ● Inactive
- Recovery ● Inactive

Step 2 Click the **Gateway** tab.

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

Figure 5-12 Tenant Gateway Screen—MPLS



WAN Gateway

Container Name: chrism_cisco.com_Container_1
Container Type: Zinc
Hosting Cloud: COSNA-Cloud
Status: ● Active
Name: ChrisMPlan007-MplsVPN
Gateway Type: MPLS VPN

Auto Provision Provider Edge

MPLS VPN Backbone

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

Provider Edge (PE)

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

The screen displays the following information:

- Container Name:—Displays the container 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.

The MPLS VPN Backbone and PE fields are described in the next section on Setting Up a WAN Gateway.

Understanding the Difference Between Auto-provisioning and Manually Provisioning WAN Gateways

During container creation, you can specify whether you want to auto-provision WAN Edge/PE. If you select **Autoprovision WAN Edge/PE**, then during WAN setup you enter MPLS VPN information, such as route targets and route descriptor, and Cisco CNAP automatically selects a VLAN from the infrastructure pool and uses cloud settings that you defined for the Cisco APIC vPC information to set up the WAN Gateways in the plan.

If your network does not include PE equipment (e.g., Cisco ASRs), you can manually provision the WAN gateways in a plan. During container creation, do not select **Autoprovision WAN Edge/PE**. Then during set up of WAN Gateways, you can specify the VLAN that will be used on the vPC to connect to private network service, as well as the external PE A and PE B IP addresses.

Caution You can manually provision WAN gateways even if your network includes PE equipment. You can also use *both* auto-provisioning and manual provisioning, however you **must be extremely careful** not to introduce potential configuration conflicts.

All gateways set up in the plan will be provisioned in the same way, either automatically or manually.

Note If you are manually provisioning WAN Edge/PE for Shared Services, you must add a SharedService firewall subnet. For more information, see Configuring Network Pools in Chapter 3, “Building the Pool of Available Cloud Resources.”

Setting Up a WAN Gateway

Note You cannot configure a WAN Gateway until a tenant has created a container and the container is active.

To set up a WAN Gateway, you specify WAN Gateway settings as appropriate for the VPN access methods you select:

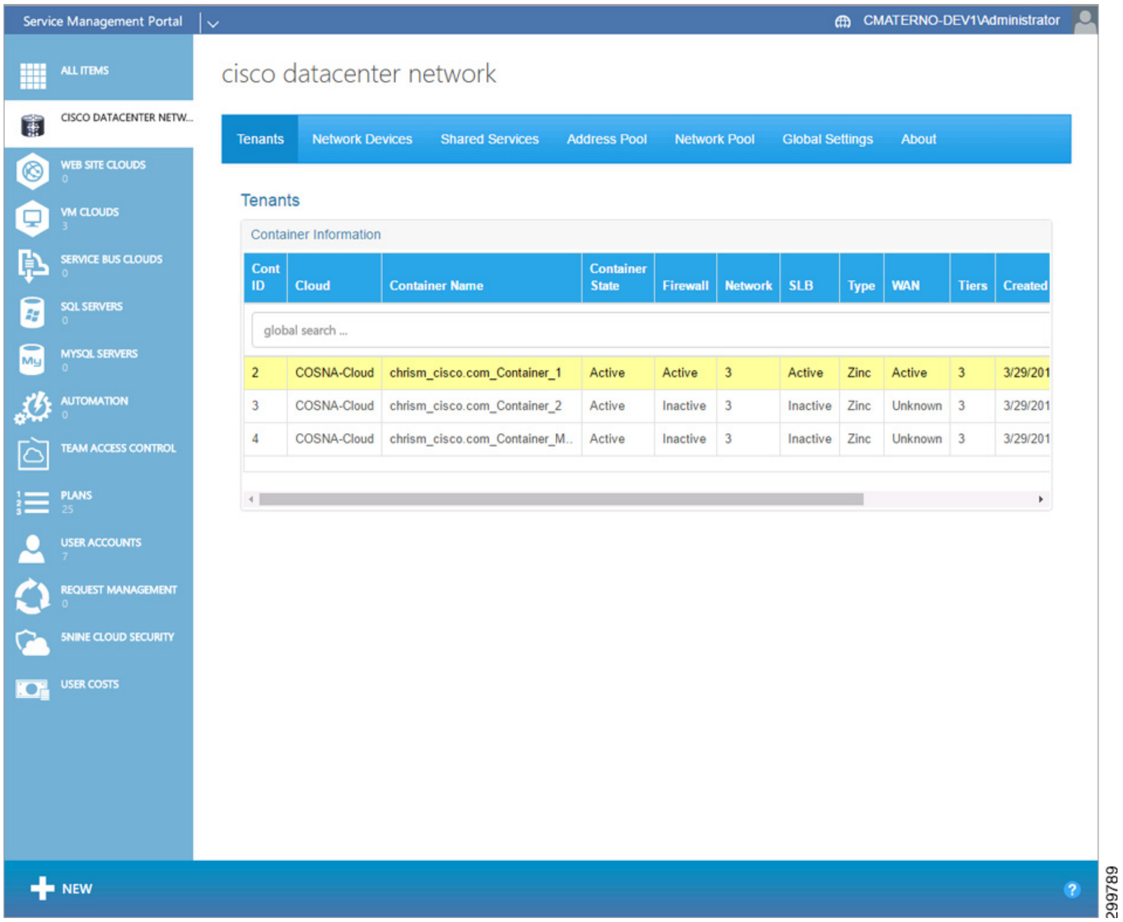
- MPLS VPN
- Site-to-Site VPN—Not available in the current release.
- Remote Access VPN—Not available in the current release.

The information you enter is different depending on whether during container creation you specified you wanted Cisco CNAP to **Autoprovision WAN Edge/PE**.

To set up a WAN Gateway for a container:

Step 1 On the Tenants tab click on the row with the container for which you want to set up a WAN Gateway, as shown in the following screen.

Figure 5-13 Tenants Tab—Container Selected Screen



cisco datacenter network

Tenants | Network Devices | Shared Services | Address Pool | Network Pool | Global Settings | About

Tenants

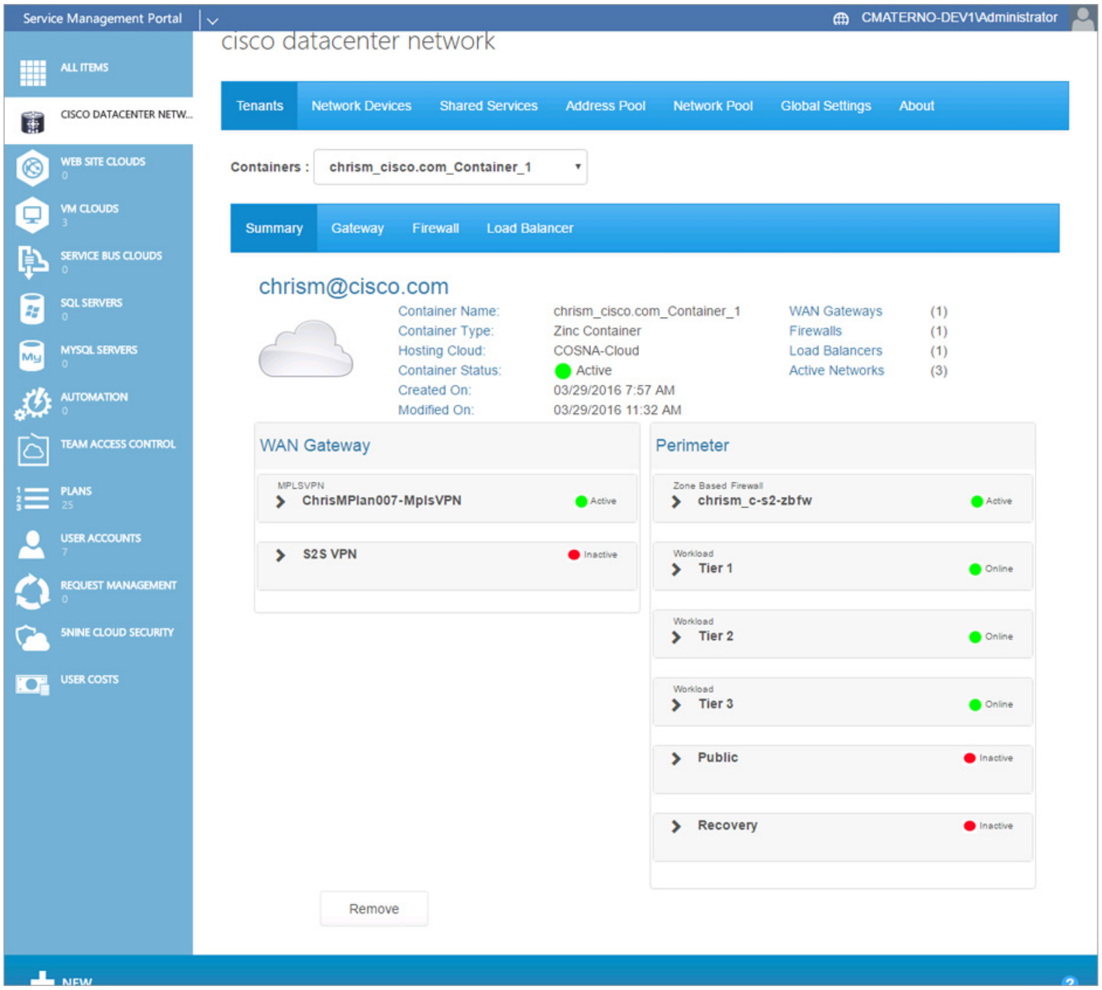
Container Information

global search ...

Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created
2	COSNA-Cloud	chrism_cisco.com_Container_1	Active	Active	3	Active	Zinc	Active	3	3/29/201
3	COSNA-Cloud	chrism_cisco.com_Container_2	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201
4	COSNA-Cloud	chrism_cisco.com_Container_M..	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201

You see the Tenants Summary screen.

Figure 5-14 Tenants Summary Screen



Containers : chrism_cisco.com_Container_1

chrism@cisco.com

Container Name:	chrism_cisco.com_Container_1	WAN Gateways	(1)
Container Type:	Zinc Container	Firewalls	(1)
Hosting Cloud:	COSNA-Cloud	Load Balancers	(1)
Container Status:	● Active	Active Networks	(3)
Created On:	03/29/2016 7:57 AM		
Modified On:	03/29/2016 11:32 AM		

WAN Gateway

- MPLSVPN — ChrisMPlan007-MplsVPN — ● Active
- S2S VPN — ● Inactive

Perimeter

- Zone Based Firewall — chrism_c-s2-zbfw — ● Active
- Workload — Tier 1 — ● Online
- Workload — Tier 2 — ● Online
- Workload — Tier 3 — ● Online
- Public — ● Inactive
- Recovery — ● Inactive

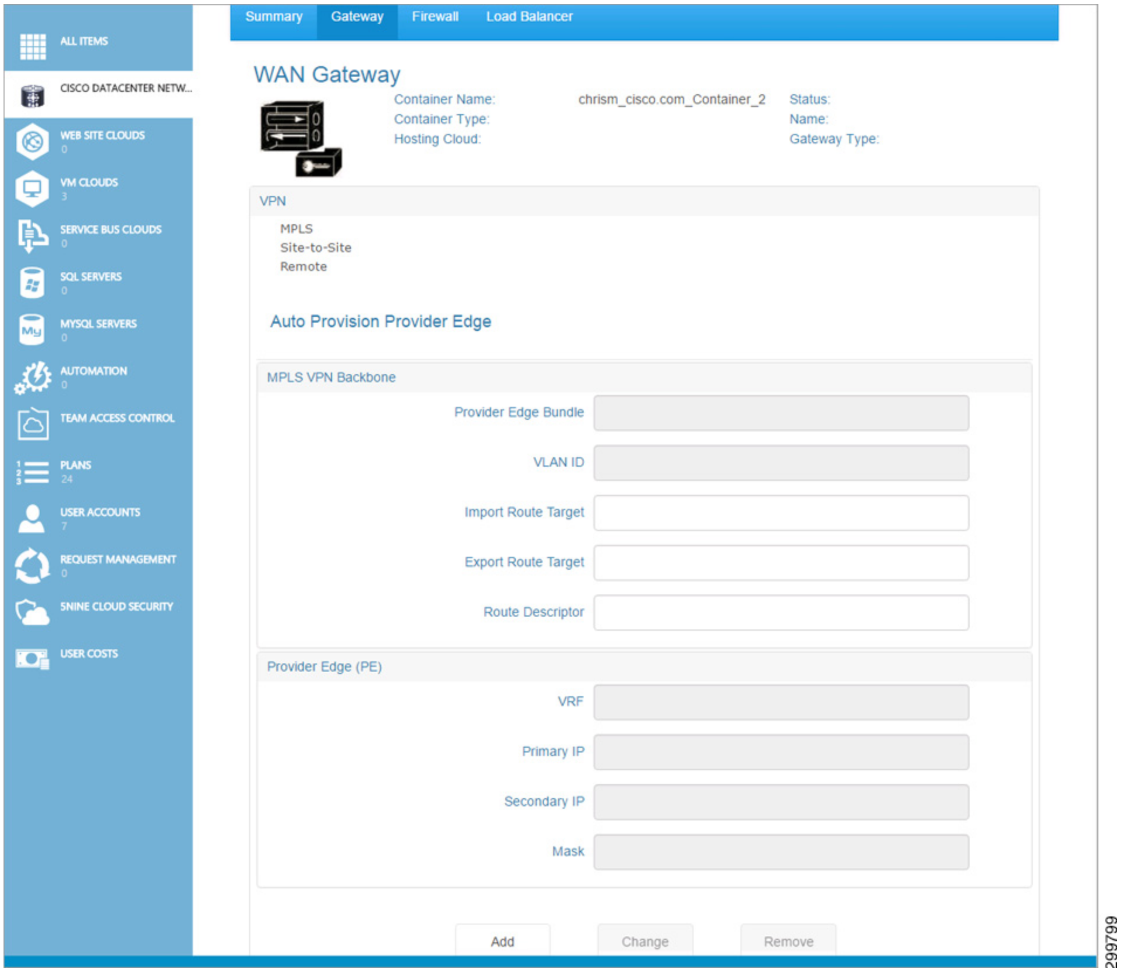
Step 2 Click the **Gateway** tab.

The specific Tenant Gateway screen you see and the fields you complete depend on whether or not during container creation you specified **Autoprovision WAN Edge/PE**.

The screens below show examples for MPLS.

Setting up an Auto-provisioned WAN Edge/PE

Figure 5-15 Tenant Gateway Screen—Auto-provision Provider Edge



WAN Gateway

Container Name: chrism_cisco.com_Container_2
Container Type:
Hosting Cloud:
Status:
Name:
Gateway Type:

VPN

MPLS
Site-to-Site
Remote

Auto Provision Provider Edge

MPLS VPN Backbone

Provider Edge Bundle
VLAN ID
Import Route Target
Export Route Target
Route Descriptor

Provider Edge (PE)

VRF
Primary IP
Secondary IP
Mask

a. Complete the modifiable fields to set up the gateway.

Note Modifiable fields when auto-provisioning WAN Edge/PE are **Import Route Target**, **Export Route Target**, and **Route Descriptor**, which are noted in **bold** below.

- VPN:
  - Provider Edge Bundle—The bundled interface on the ASR, the same as in the Global settings for clouds, MPLS Network, Primary PE ACI L2 Attachment.
  - VLAN ID—The VLAN ID that Cisco CNAP allocates.

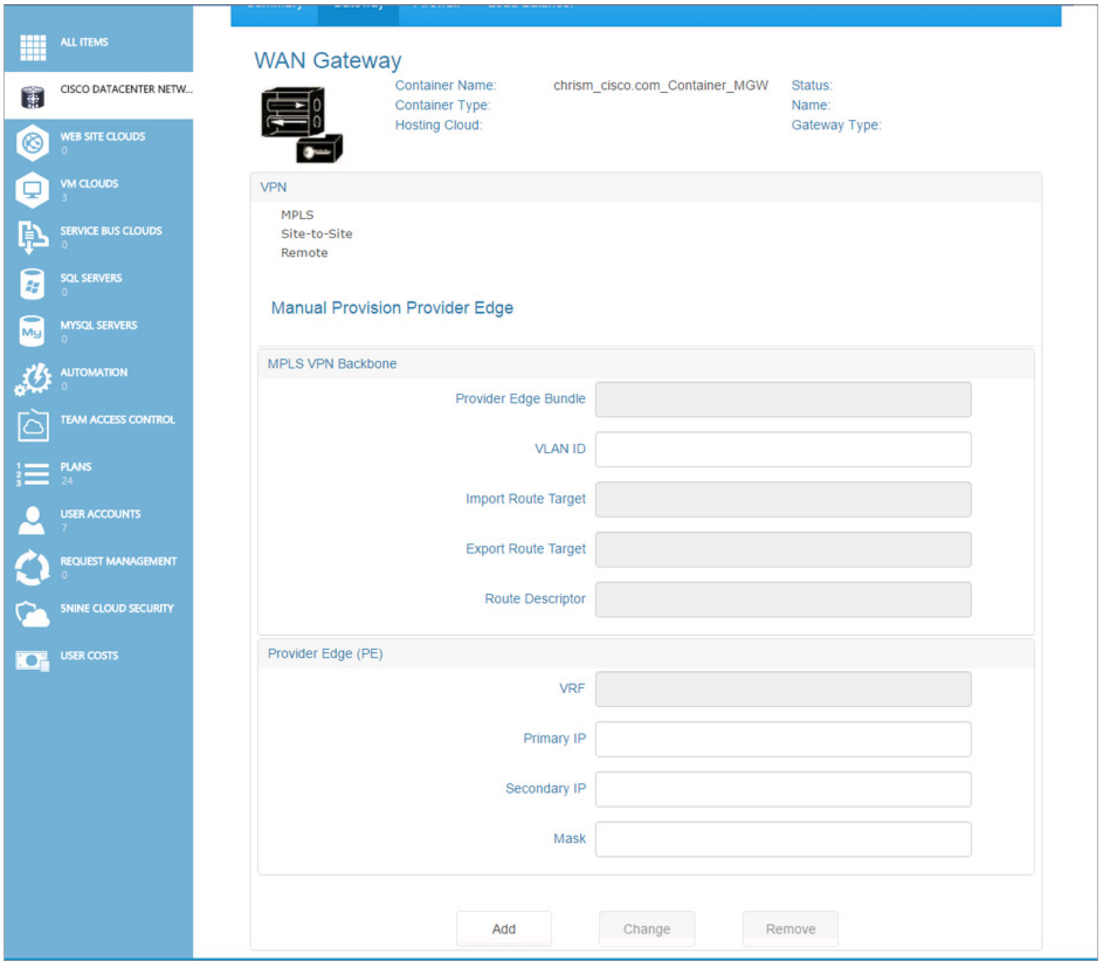
Note The values for Route Targets and Route Descriptor must be verified and accurately entered to prevent any security violation of a tenant network. You must ensure that tenant cloud networks (containers) are only mapped to their specific VPN by using the correct values for the Route Targets and Route Descriptor of that specific tenant L3VPN.

  - **Import Route Target**—Enter the proper RT based on the network design.
  - **Export Route Target**—Enter the proper RT based on the network design.
  - **Route Descriptor**—Enter the proper descriptor based on the 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

b. When you are finished, click the **Add** button.

Setting up a Manually Provisioned WAN Edge/PE

Figure 5-16 Tenant Gateway Screen—Manual Provision Provider Edge



WAN Gateway

Container Name: chrism_cisco.com_Container_MGW

Container Type:

Hosting Cloud:

Status:

Name:

Gateway Type:

VPN

MPLS
Site-to-Site
Remote

Manual Provision Provider Edge

MPLS VPN Backbone

Provider Edge Bundle

VLAN ID

Import Route Target

Export Route Target

Route Descriptor

Provider Edge (PE)

VRF

Primary IP

Secondary IP

Mask

a. Complete the modifiable fields to add the gateway:

Note Modifiable fields when manually-provisioning WAN Edge/PE are **VLAN ID**, **Primary IP**, **Secondary IP**, and **Mask**, which are noted in **bold** below.

- VPN:
  - Provider Edge Bundle—The bundled interface on the ASR, the same as in the Global settings for clouds, MPLS Network, Primary PE ACI L2 Attachment.
  - **VLAN ID**—Enter the VLAN ID.

Note The following fields are not displayed when manually provisioning WAN Edge/PE. The SP administrator should consult with the Microsoft WAP PE administrator to provision the tenant network into the correct L3VPN or other private network for the tenant and agree on the VLAN used for the hand-off of tenant traffic to the cloud data center.

  - Import Route Target—RT based on the network design.
  - Export Route Target—RT based on the network design.
  - Route Descriptor—Descriptor based on the network design.
- PE:
  - VRF—Generated by Cisco CNAP based on the abbreviation of the container ID.
  - **Primary IP**—Enter the external PE IP Address in dotted format.
  - **Secondary IP**—Enter the external PE IP Address in dotted format.
  - **Mask**—Enter the external PE Mask in dotted format.

Note Based on the PE IP address and subnet mask you specify, Cisco CNAP automatically provisions the Cisco CSR 1000V interface IP and HSRP address.

b. When you are finished, click the **Add** button.

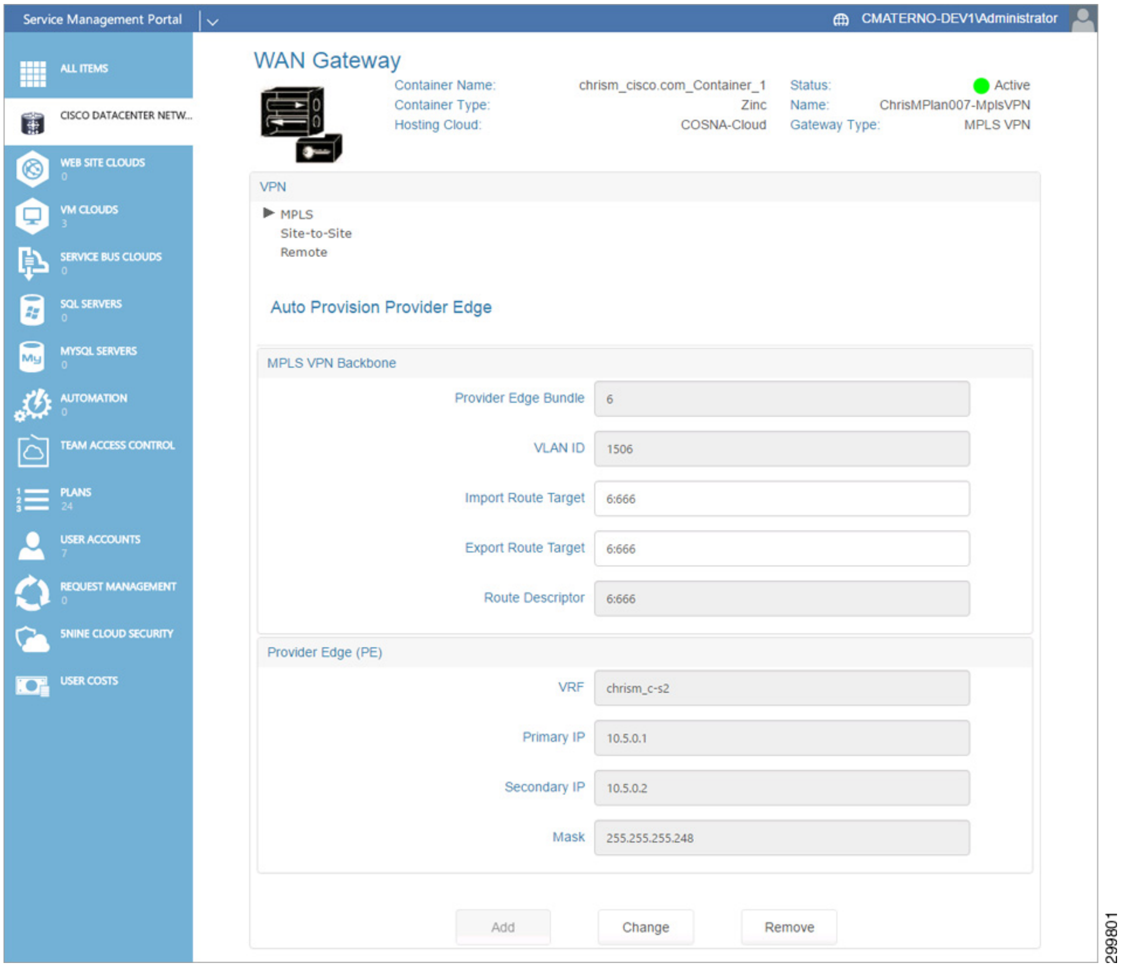
Changing a WAN Gateway

Step 1 On the Tenants tab, click on the row with the container whose WAN Gateway you want to change, then on the Gateway tab, click **Change**.

Once a container is created, the only WAN Gateway fields you can change are the Import Route Target and Export Route Target, as shown in the following screen.

Note If you manually provisioned the WAN gateways, you cannot change any of the fields.

Figure 5-17 Tenant Gateway Screen—Change WAN Gateway Settings



WAN Gateway

Container Name: chrism_cisco.com_Container_1
Container Type: Zinc
Hosting Cloud: COSNA-Cloud
Status: ● Active
Name: ChrisMPlan007-MplsVPN
Gateway Type: MPLS VPN

VPN

▶ MPLS
Site-to-Site
Remote

Auto Provision Provider Edge

MPLS VPN Backbone

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

Provider Edge (PE)

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

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

Removing a Gateway

On the Tenants tab, click on the row with the container whose WAN Gateway you want to remove, then on the Gateway tab, click **Remove**.

Configuring and Managing Firewalls

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 Access Control List (ACL)
- Change an Access List
- Create a new object group
- Change an object group

Understanding Firewall Creation

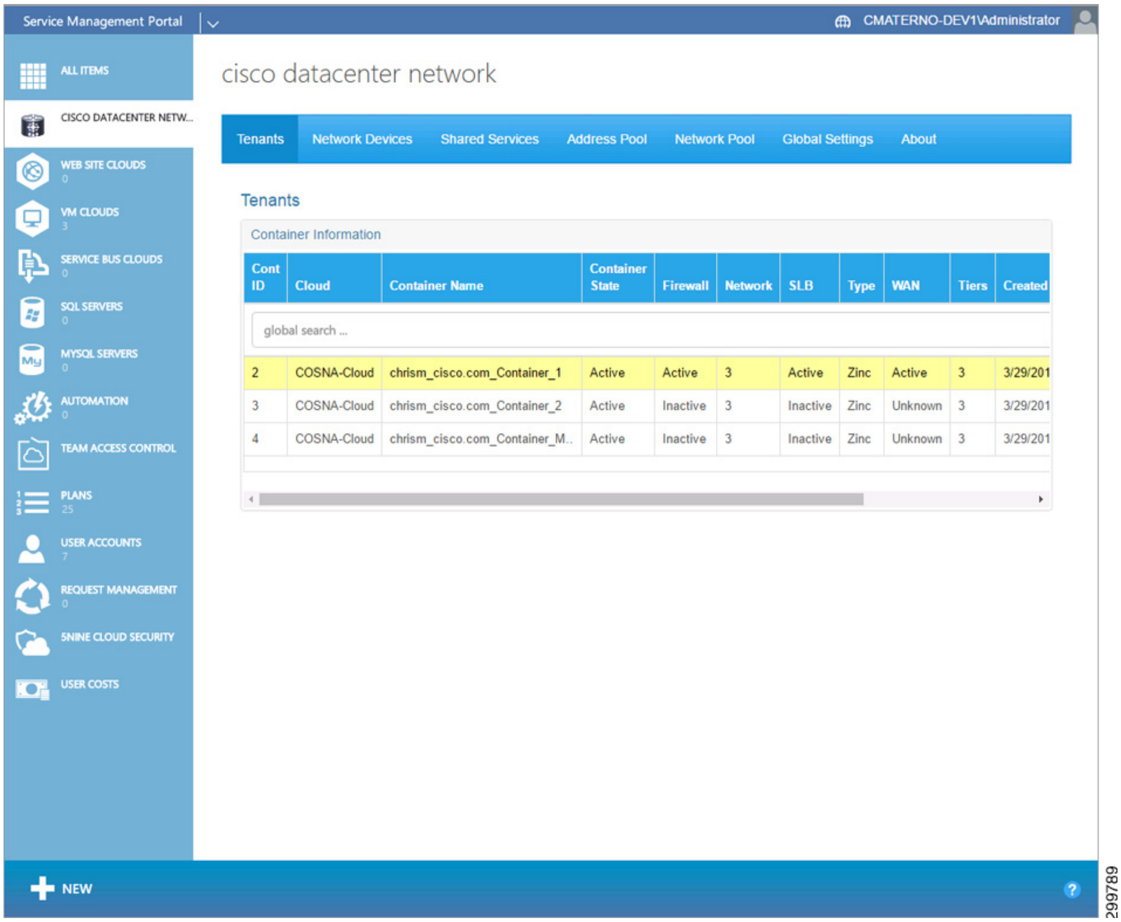
A firewall is created by default the moment you create a WAN Gateway in the Zinc container and a default policy is applied that allows inside to outside traffic, but restricts outside to inside traffic. The SP administrator can view and manage tenant firewalls, depending on the agreement with the tenant (e.g., you might do it as a managed service or while troubleshooting a customer reported problem). 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 the tenant 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 display firewall information about a specific container, on the Tenants tab click on the row with the container you want to view, as shown in the following screen.

Figure 5-18 Tenants Tab Screen—Container Selected



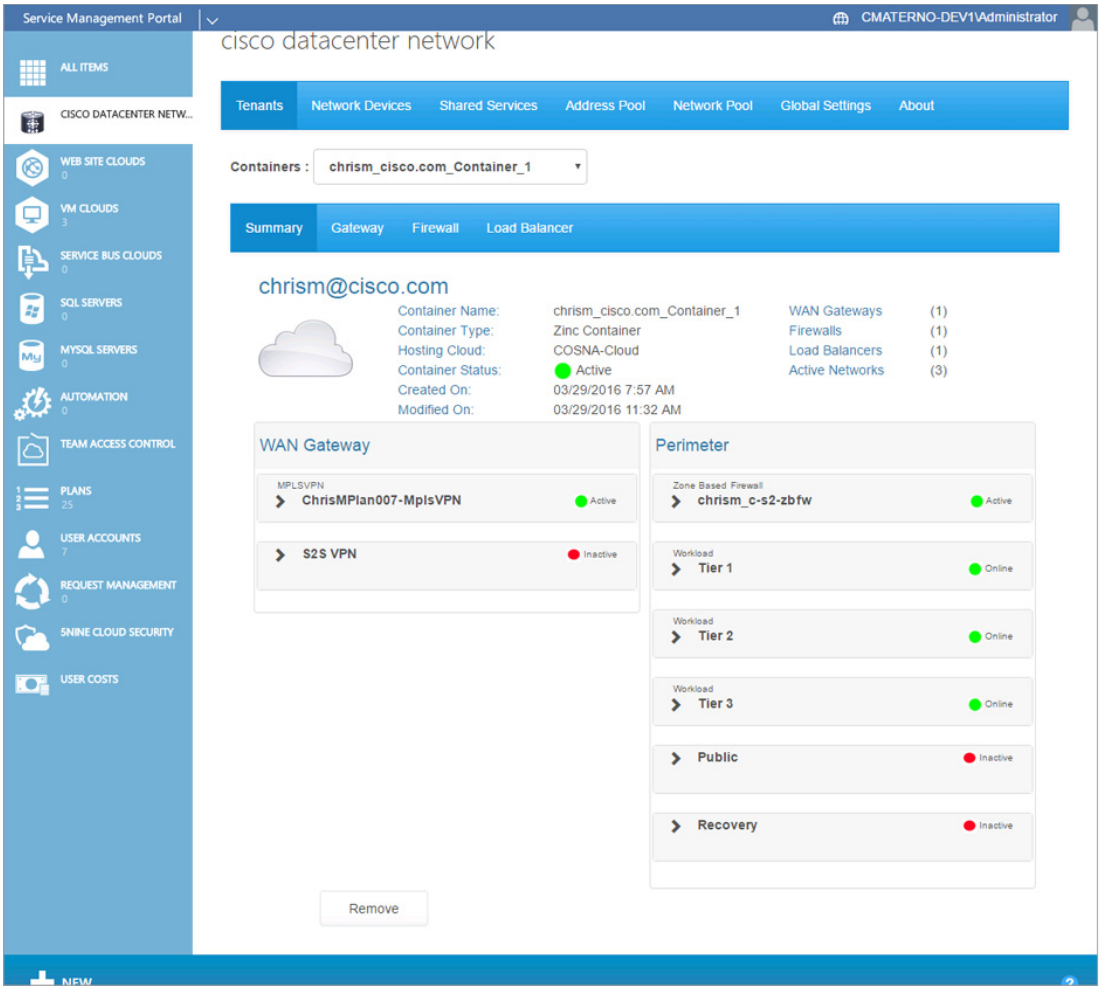
Tenants

Container Information

Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created
2	COSNA-Cloud	chrism_cisco.com_Container_1	Active	Active	3	Active	Zinc	Active	3	3/29/201
3	COSNA-Cloud	chrism_cisco.com_Container_2	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201
4	COSNA-Cloud	chrism_cisco.com_Container_M..	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201

You see the Tenants Summary screen.

Figure 5-19 Tenants Summary Screen



Containers : chrism_cisco.com_Container_1

chrism@cisco.com

Container Name:	chrism_cisco.com_Container_1	WAN Gateways	(1)
Container Type:	Zinc Container	Firewalls	(1)
Hosting Cloud:	COSNA-Cloud	Load Balancers	(1)
Container Status:	● Active	Active Networks	(3)
Created On:	03/29/2016 7:57 AM		
Modified On:	03/29/2016 11:32 AM		

WAN Gateway

- MPLSVPN ChrisMPlan007-MplsVPN ● Active
- S2S VPN ● Inactive

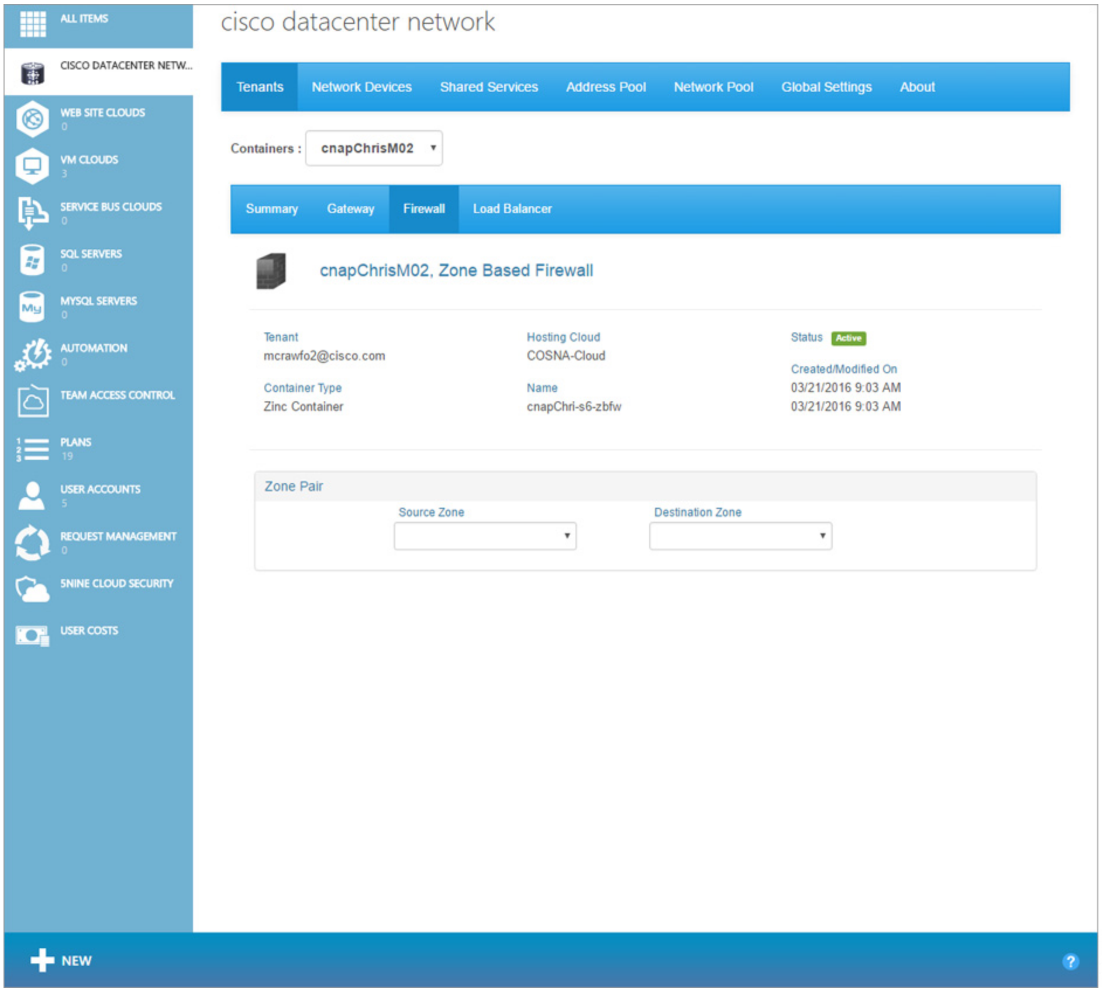
Perimeter

- Zone Based Firewall chrism_c-s2-zbfw ● Active
- Workload Tier 1 ● Online
- Workload Tier 2 ● Online
- Workload Tier 3 ● Online
- Public ● Inactive
- Recovery ● Inactive

Step 2 Click the **Firewall** tab.

You see the Tenant Firewall screen.

Figure 5-20 Tenant Firewall Screen



Containers : cnapChrisM02

cnapChrisM02, Zone Based Firewall

Tenant
mcrawfo2@cisco.com

Container Type
Zinc Container

Hosting Cloud
COSNA-Cloud

Name
cnapChri-s6-zbfw

Status Active

Created/Modified On
03/21/2016 9:03 AM
03/21/2016 9:03 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 in the form mm-dd-yyyy hh:mm:ss.
- 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 in the form mm-dd-yyyy hh:mm:ss.

- Zone Pair—Source Zone and Destination Zone are the zones between which the firewall is configured.

Note In rare instances, the retrieval of Zone Pairs may take longer than approximately 20 seconds, in which case you will see an error message. Dismiss the error message and refresh the screen.

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.

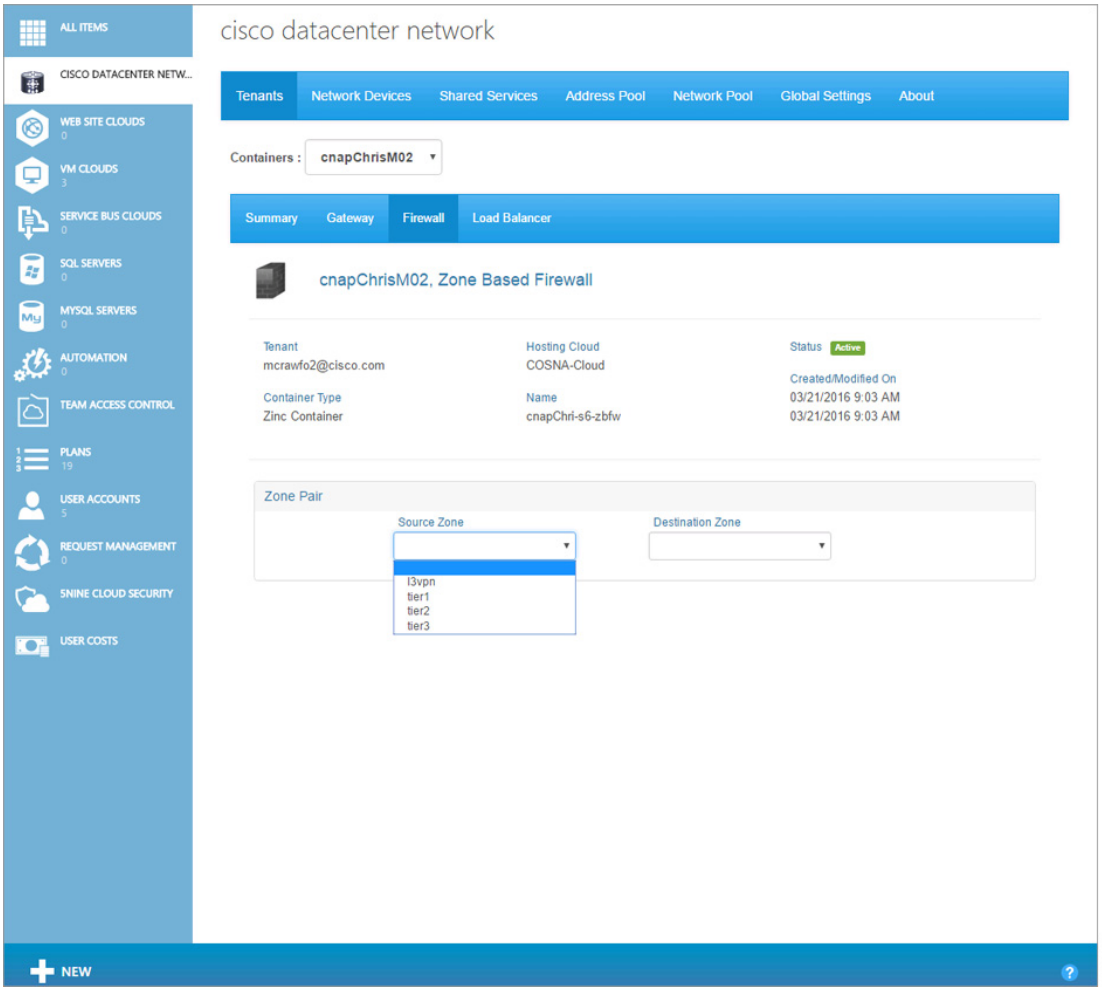
- Class Maps in a Policy Map
- Access Lists within a Class Map
- Rules in an Access List
- Object Groups of a Rule

Note You can view the list of all Object Groups, but you cannot view or edit the details of any specific Object Group.

To display the various layers of information about a firewall:

Step 1 On the Firewall tab screen, use the Source Zone: and Destination Zone: pull-down menus to select the relevant zones, as shown in the following screens.

Figure 5-21 Firewall Source Zone Pull-down Menu Screen



Containers : cnapChrisM02

Tenant: mcrawfo2@cisco.com

Hosting Cloud: COSNA-Cloud

Status: Active

Container Type: Zinc Container

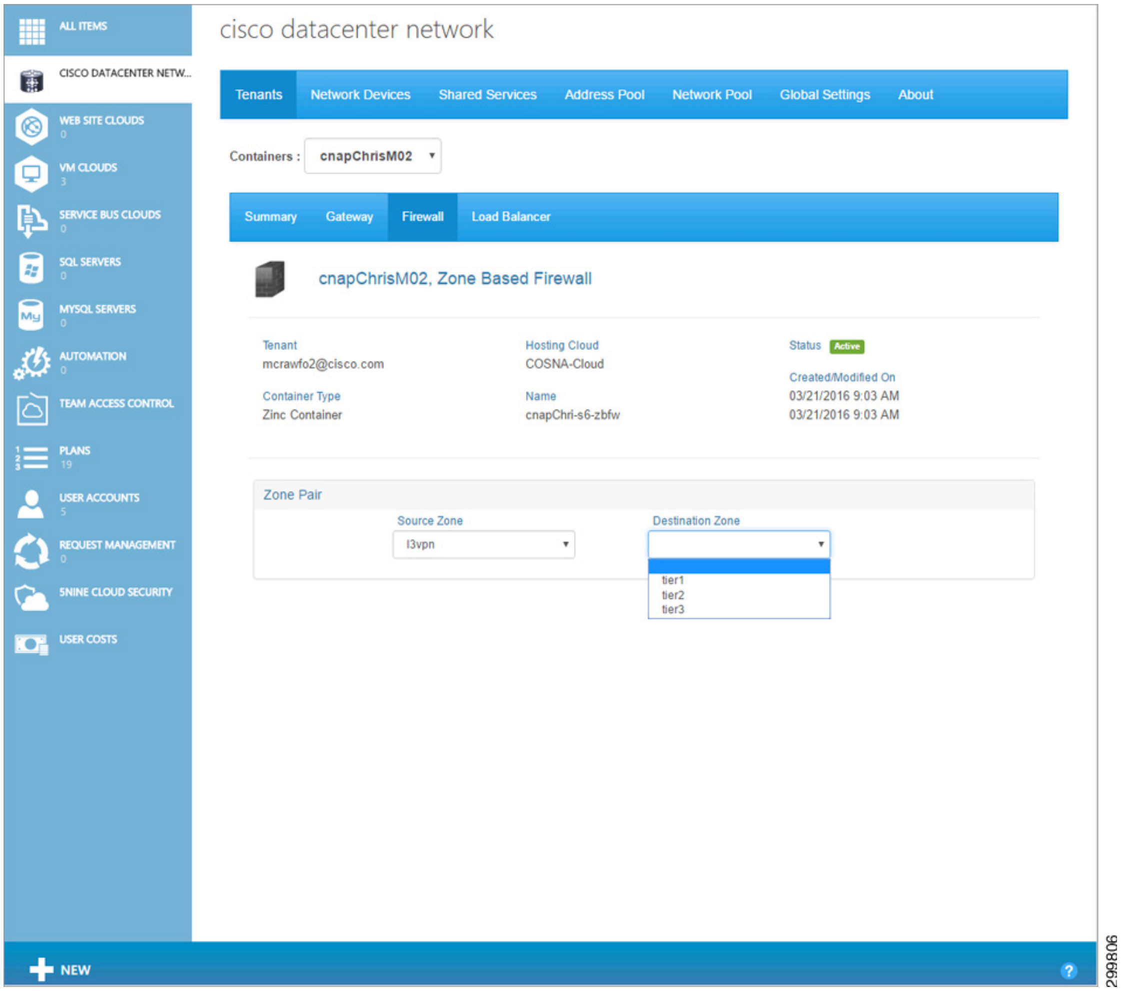
Name: cnapChri-s6-zbfw

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

Source Zone:

Destination Zone:

Figure 5-22 Firewall Destination Zone Pull-down Menu Screen



Containers : cnapChrisM02

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

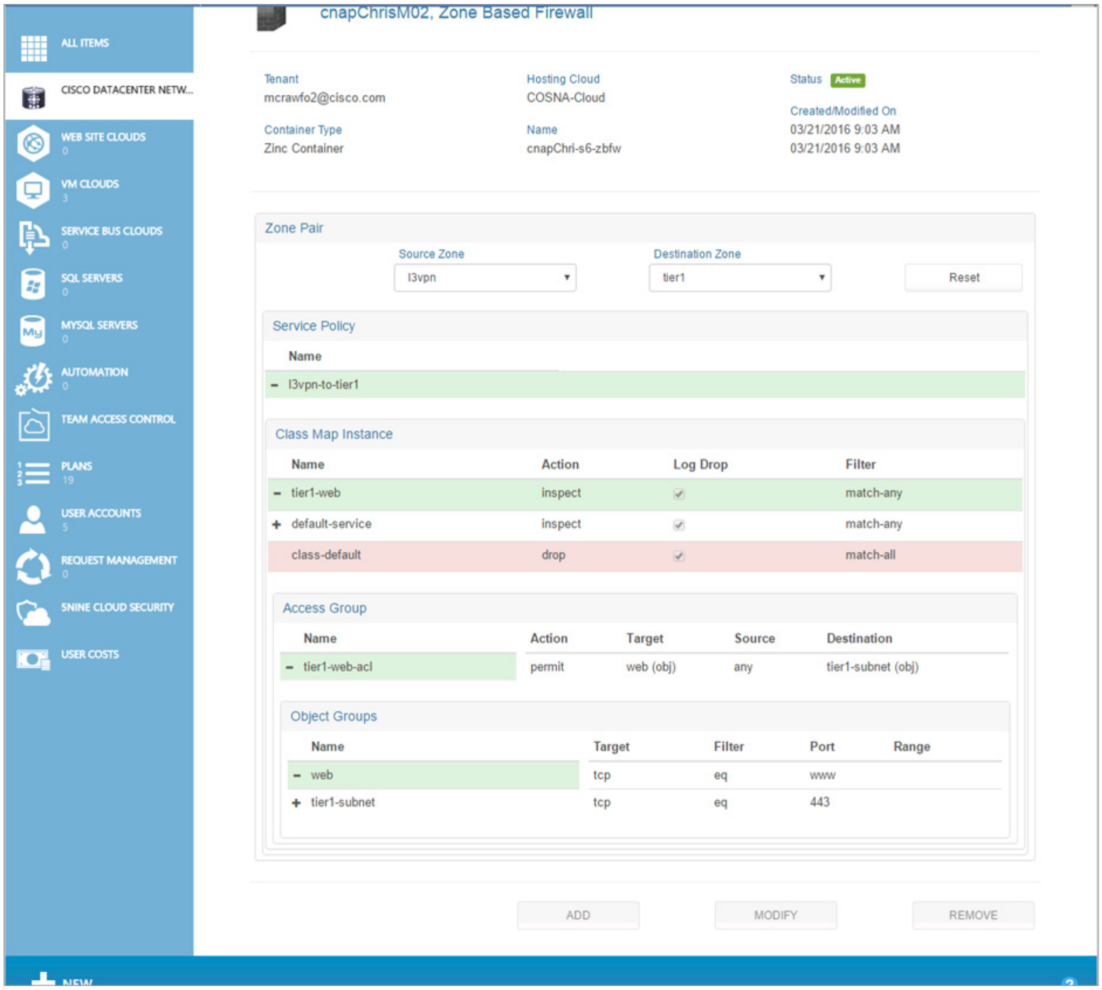
Zone Pair

Source Zone
l3vpn

Destination Zone
tier1
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 5-23 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
03/21/2016 9:03 AM
03/21/2016 9:03 AM

Container Type
Zinc Container

Name
cnapChri-s6-zbfw

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	

215545

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

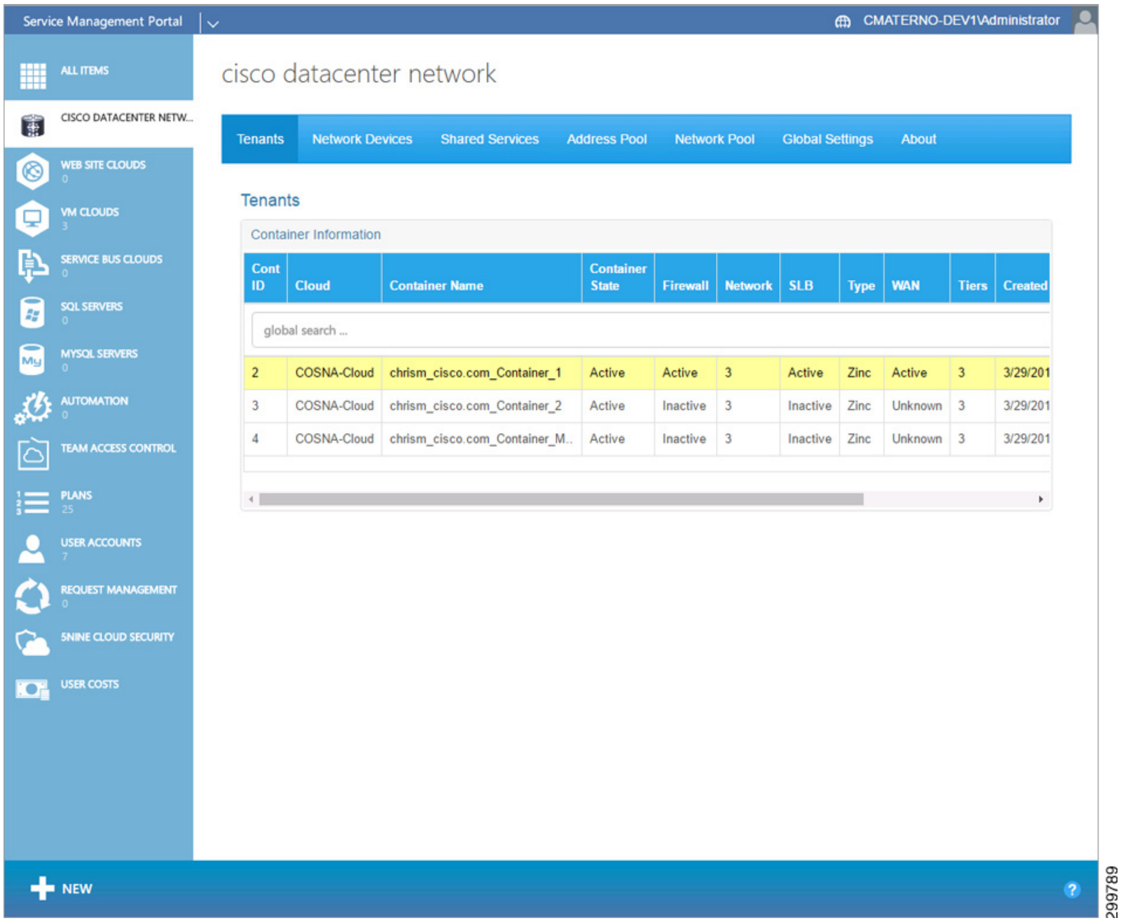
Note You can only configure a firewall after a tenant has created a container and the Admin has created a WAN Gateway. The firewall is automatically created with a base configuration during container creation. When the WAN gateway is created, another firewall zone is created for the WAN edge. For more information, see 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 On the Tenants tab, click the row with the container for which you want to configure a firewall, as shown in the following screen.

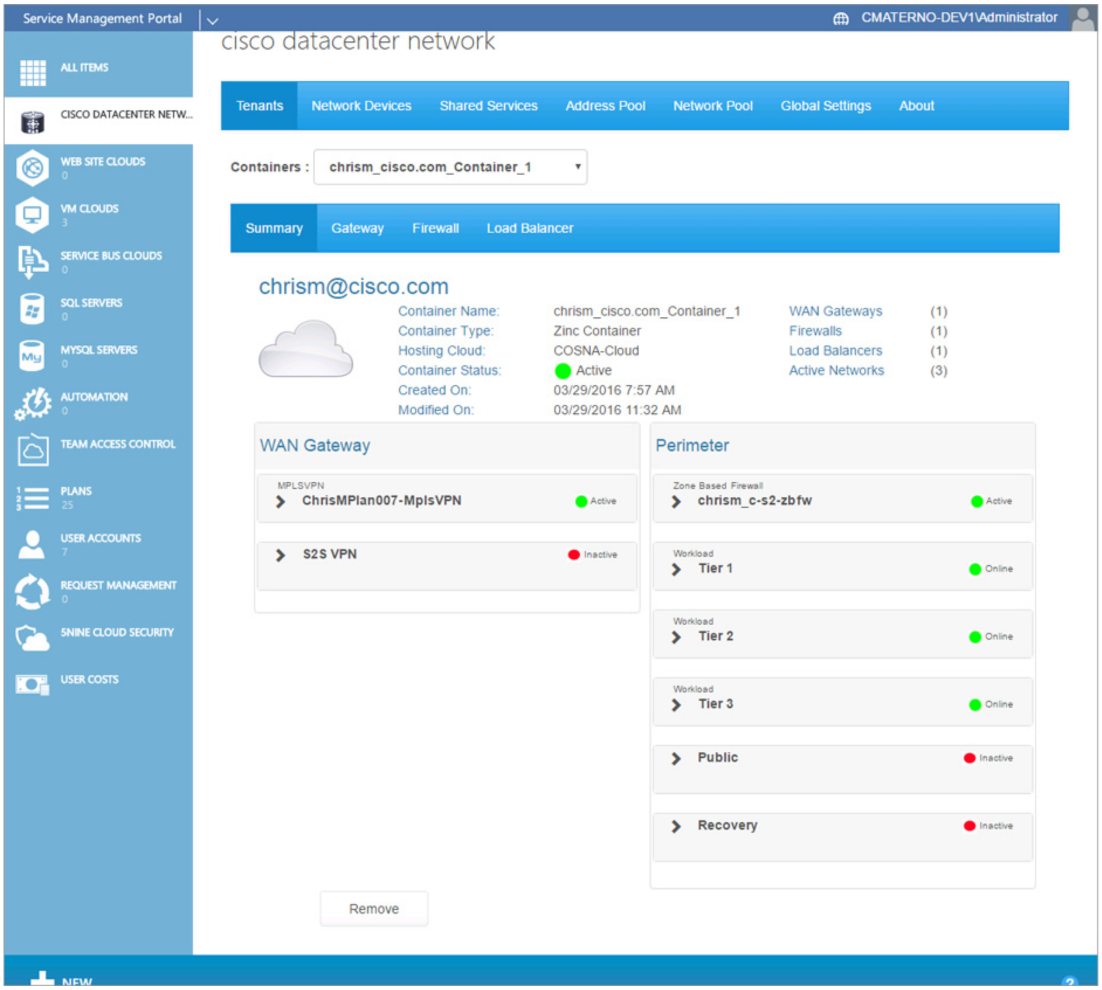
Figure 5-24 Tenants Tab Screen—Container Selected



Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created
2	COSNA-Cloud	chrism_cisco.com_Container_1	Active	Active	3	Active	Zinc	Active	3	3/29/201
3	COSNA-Cloud	chrism_cisco.com_Container_2	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201
4	COSNA-Cloud	chrism_cisco.com_Container_M..	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201

You see the Tenants Summary screen.

Figure 5-25 *Tenants Summary Screen*



Containers : chrism_cisco.com_Container_1

chrism@cisco.com

Container Name:	chrism_cisco.com_Container_1	WAN Gateways	(1)
Container Type:	Zinc Container	Firewalls	(1)
Hosting Cloud:	COSNA-Cloud	Load Balancers	(1)
Container Status:	● Active	Active Networks	(3)
Created On:	03/29/2016 7:57 AM		
Modified On:	03/29/2016 11:32 AM		

WAN Gateway

- MPLSVPN — ChrisMPlan007-MplsVPN — ● Active
- S2S VPN — ● Inactive

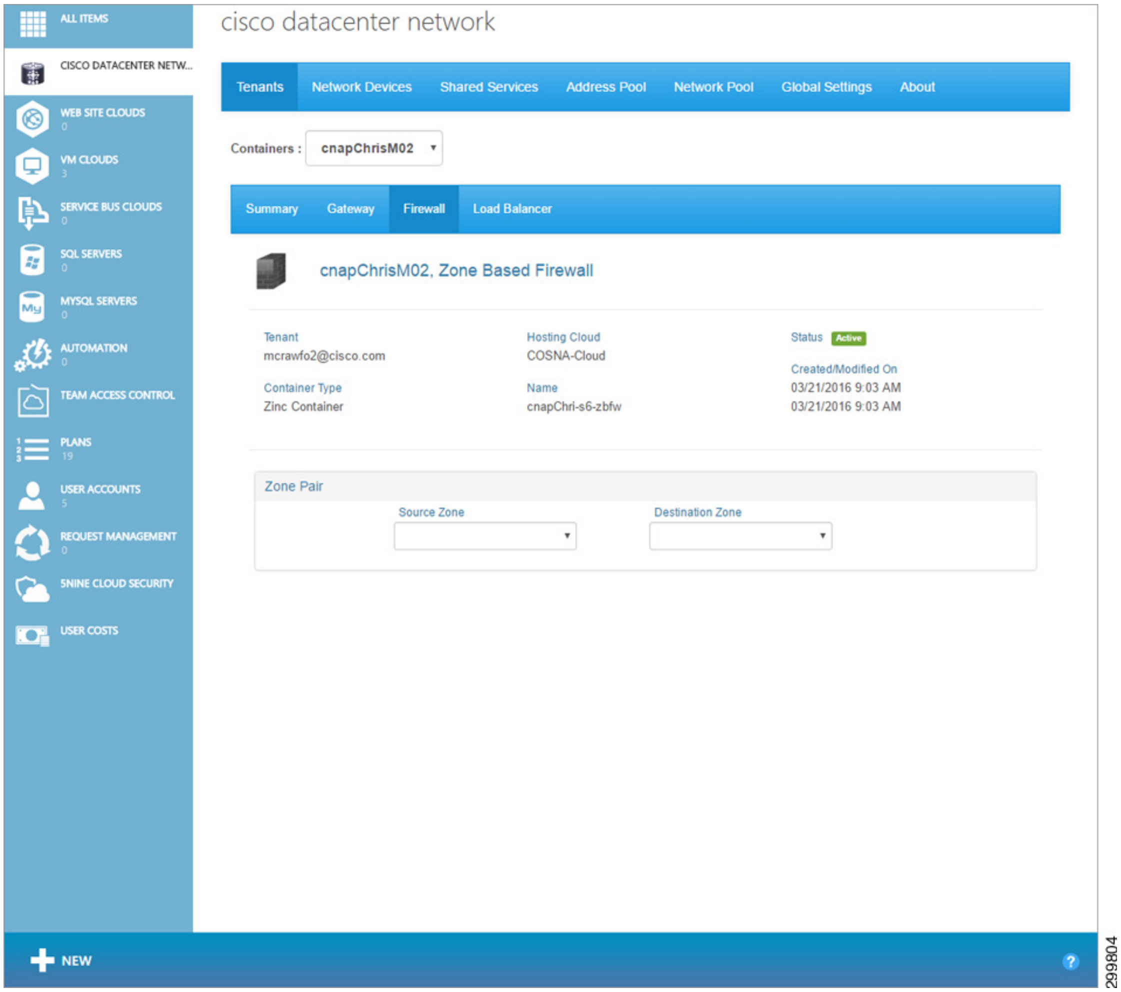
Perimeter

- Zone Based Firewall — chrism_c-s2-zbfw — ● Active
- Workload — Tier 1 — ● Online
- Workload — Tier 2 — ● Online
- Workload — Tier 3 — ● Online
- Public — ● Inactive
- Recovery — ● Inactive

Step 2 Click the **Firewall** tab.

You see the Tenant Firewall screen.

Figure 5-26 Tenant Firewall Screen



Containers : cnapChrisM02

cnapChrisM02, Zone Based Firewall

Tenant
mcrawfo2@cisco.com

Hosting Cloud
COSNA-Cloud

Status Active

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

Container Type
Zinc Container

Name
cnapChri-s6-zbfw

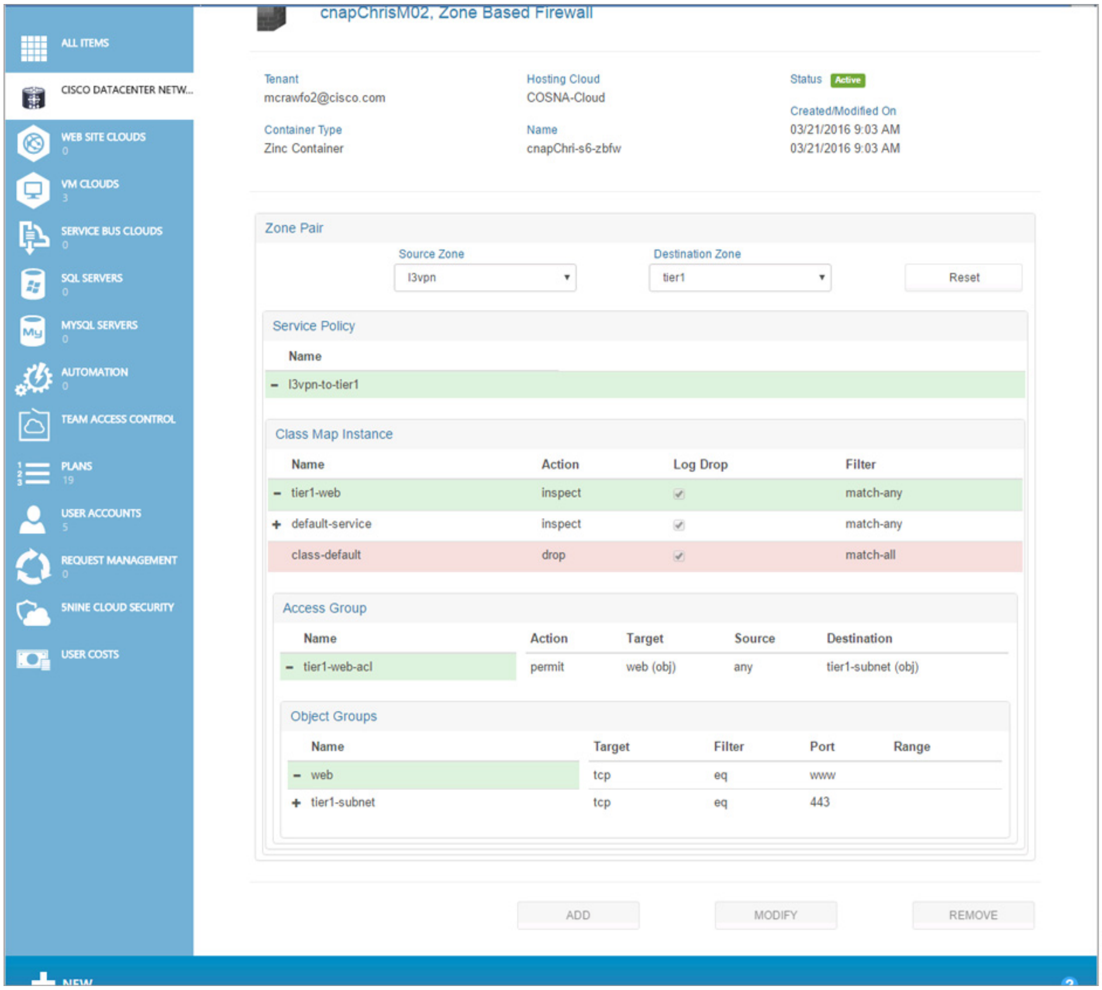
Zone Pair

Source Zone

Destination Zone

Step 3 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 5-27 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

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

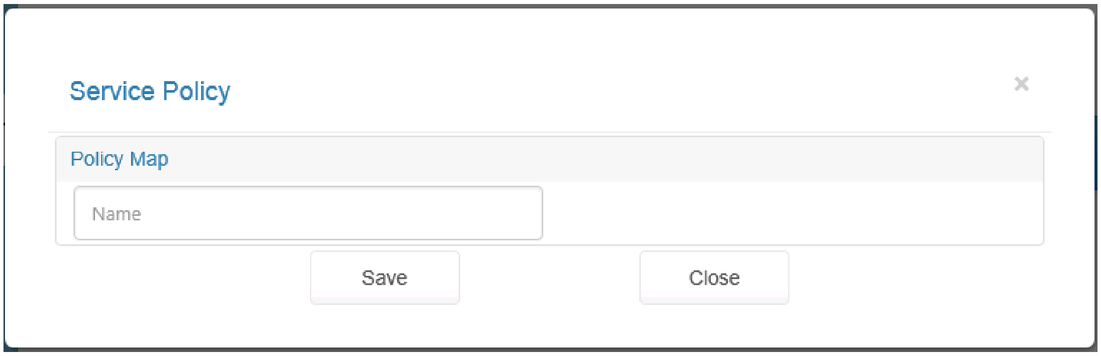
Name	Action	Target	Source	Destination
– tier1-web-acl	permit	web (obj)	any	tier1-subnet (obj)

Object Groups

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

Step 4 To add a Policy Map, click the Policy Map under Service Policy, then click the **Add** button. You see the following screen.

Figure 5-28 Add Policy Map for Service Policy Screen



Service Policy

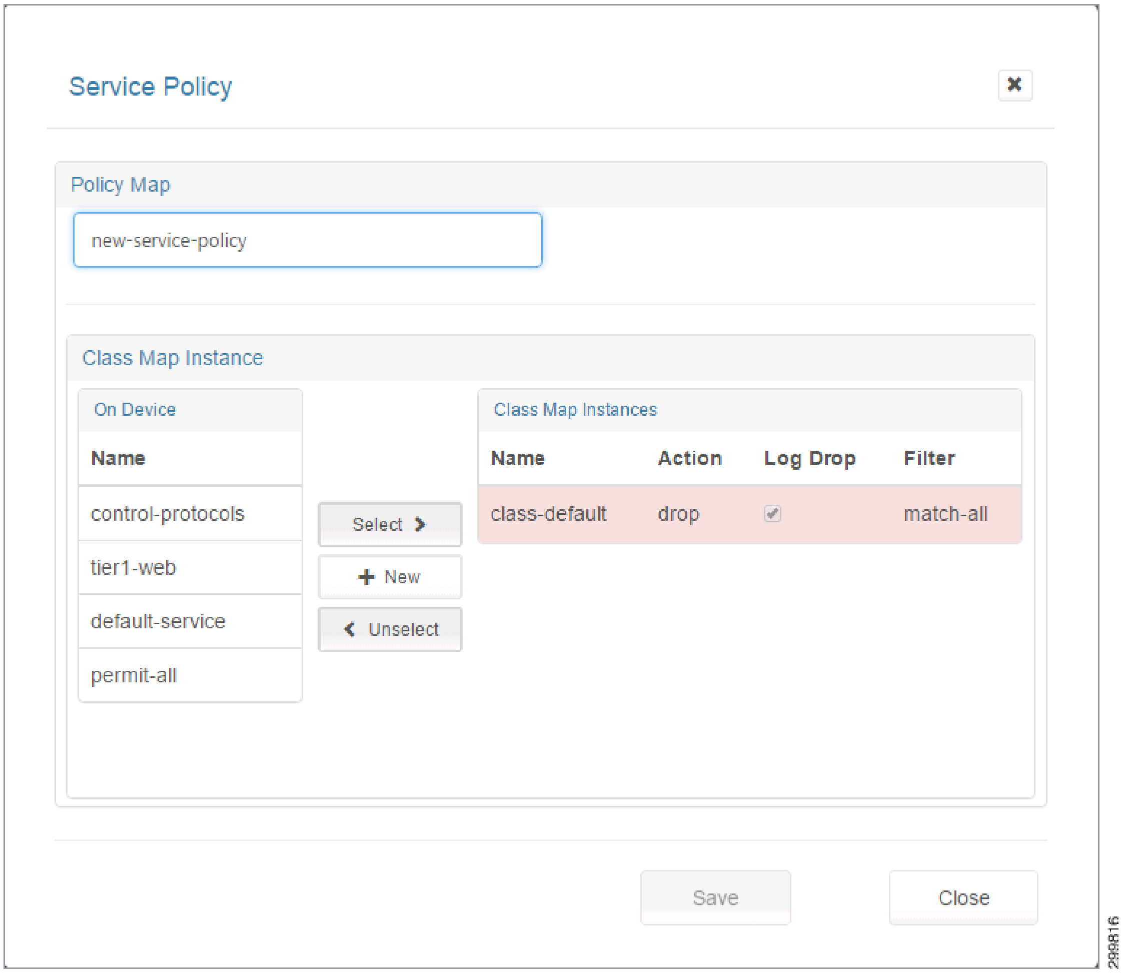
Policy Map

Name

Step 5 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 5-29 New Policy Map—Class Maps Screen



Policy Map

new-service-policy

Class Map Instance

On Device

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

Class Map Instances

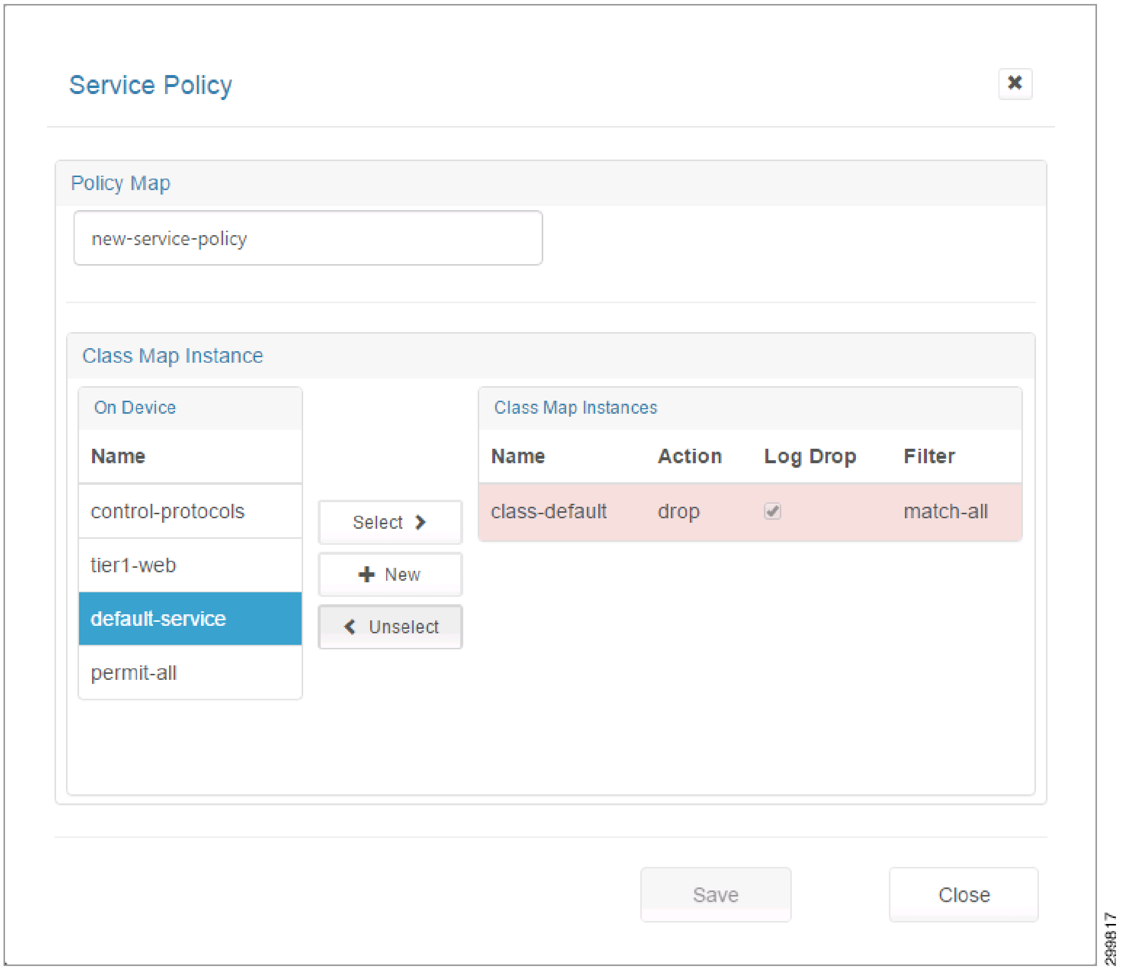
Name	Action	Log Drop	Filter
class-default	drop	☑	match-all

Step 6 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 5-30 Class Map Instance class-default Screen



Service Policy

Policy Map: new-service-policy

Class Map Instance

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

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

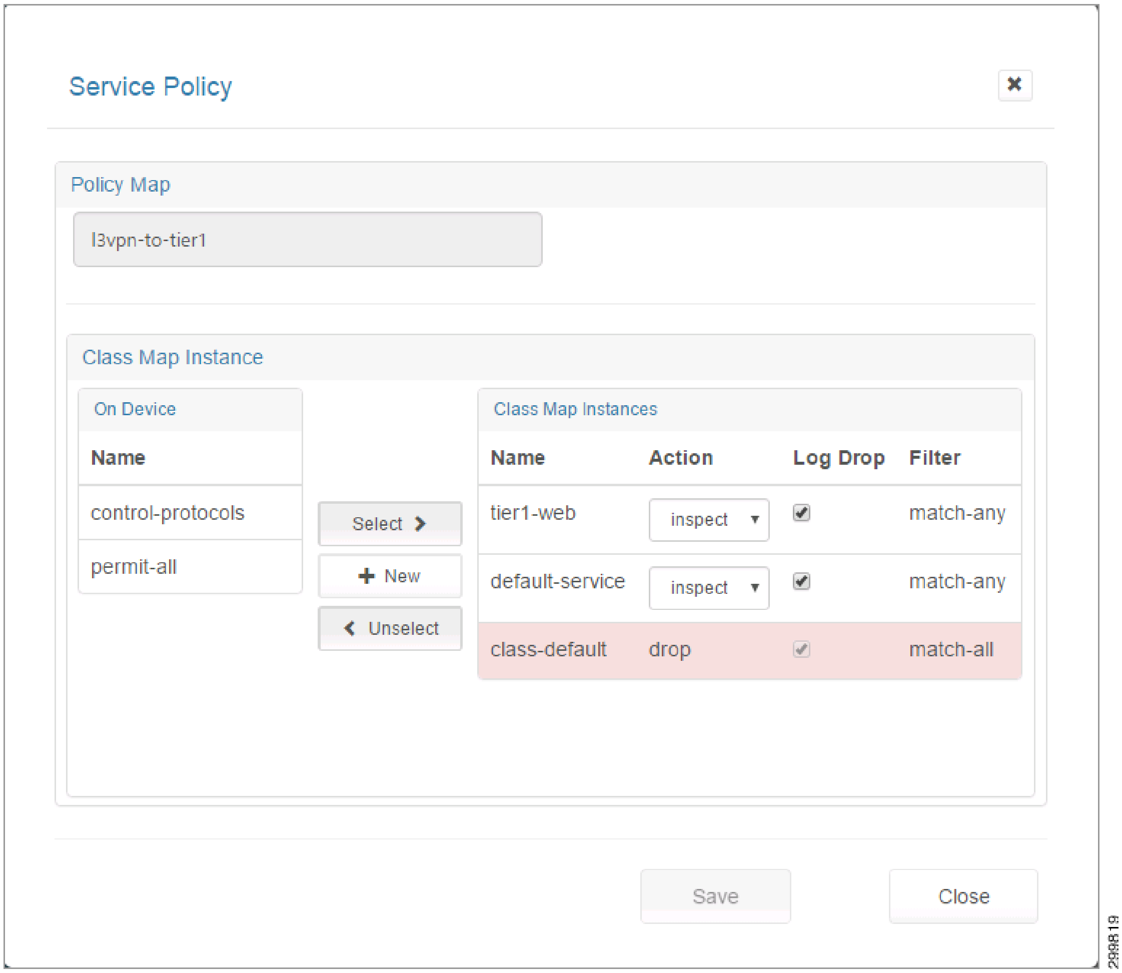
Step 7 When you are finished, click **Save**.

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 5-31 Policy Map Pop-up Screen



Service Policy

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

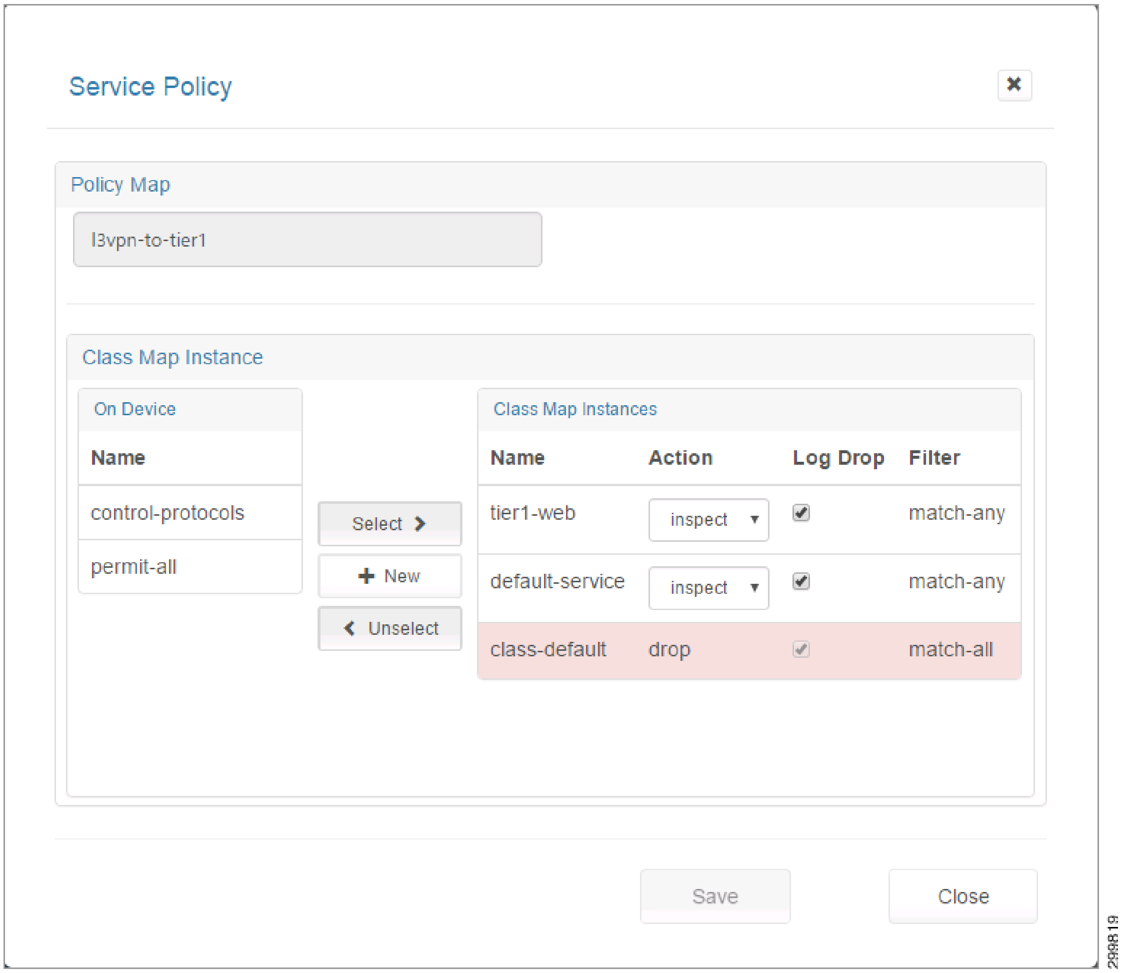
This is the same as the Create Service Policy page, but with the name field deactivated. You can click:

- **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 5-32 Class Map Instance Screen—Click +New



Policy Map

l3vpn-to-tier1

Class Map Instance

On Device

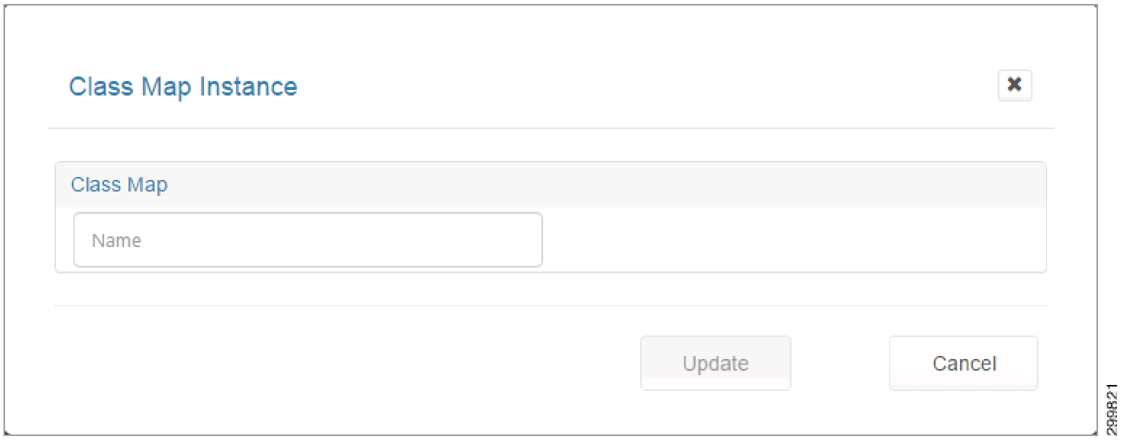
Name
control-protocols
permit-all

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 5-33 New Class Map Instance Screen



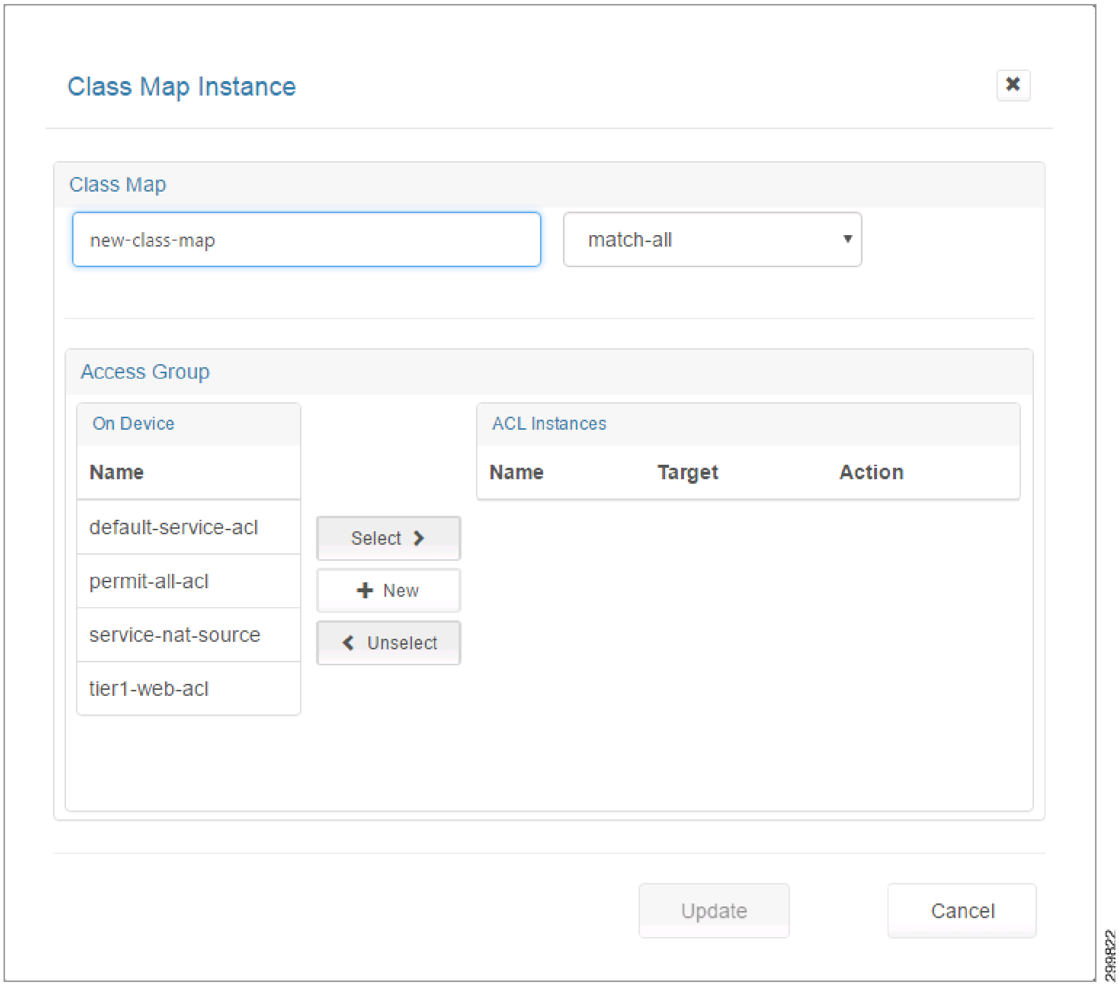
Class Map

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 5-34 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.

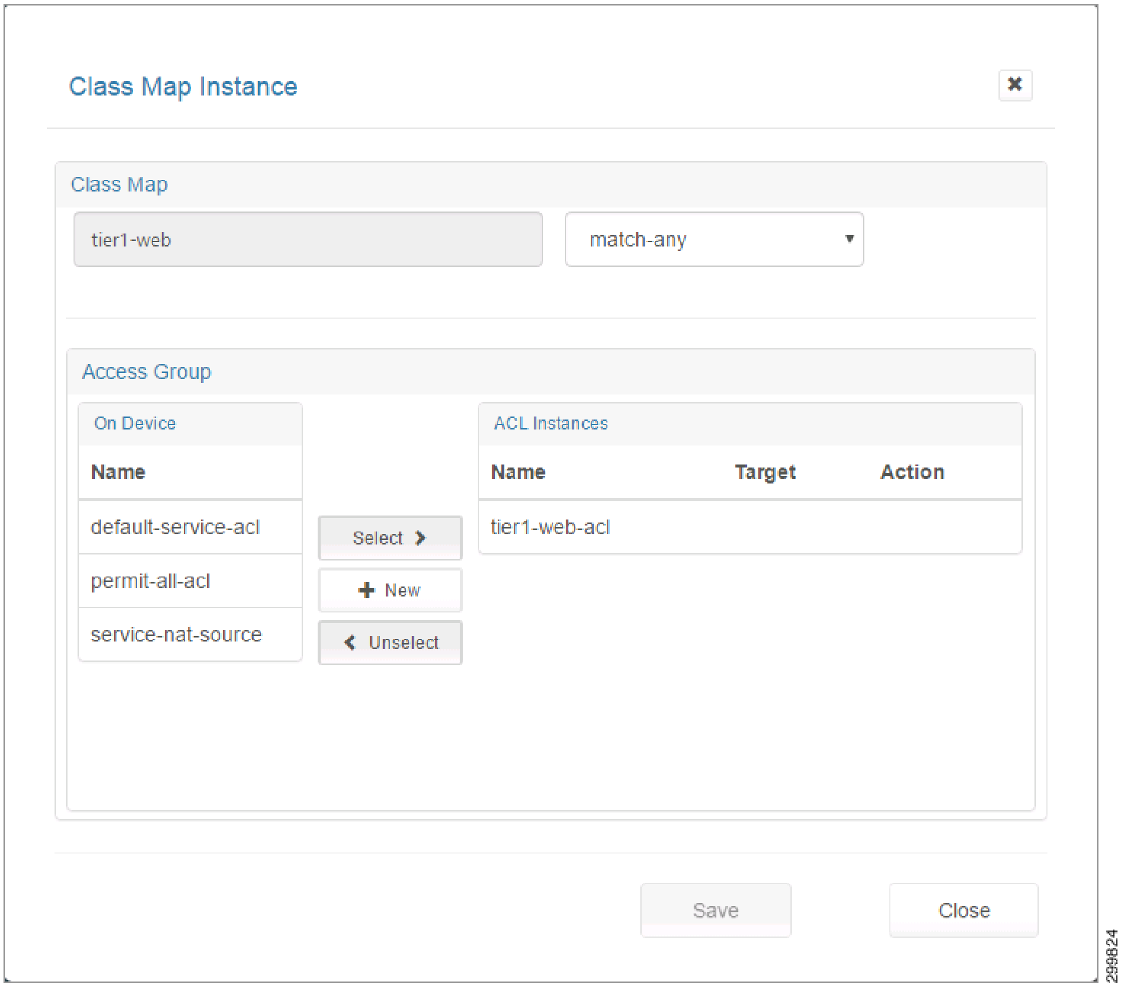
Changing a Class Map

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

Step 2 Click **Modify**.

You see the following screen.

Figure 5-35 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.

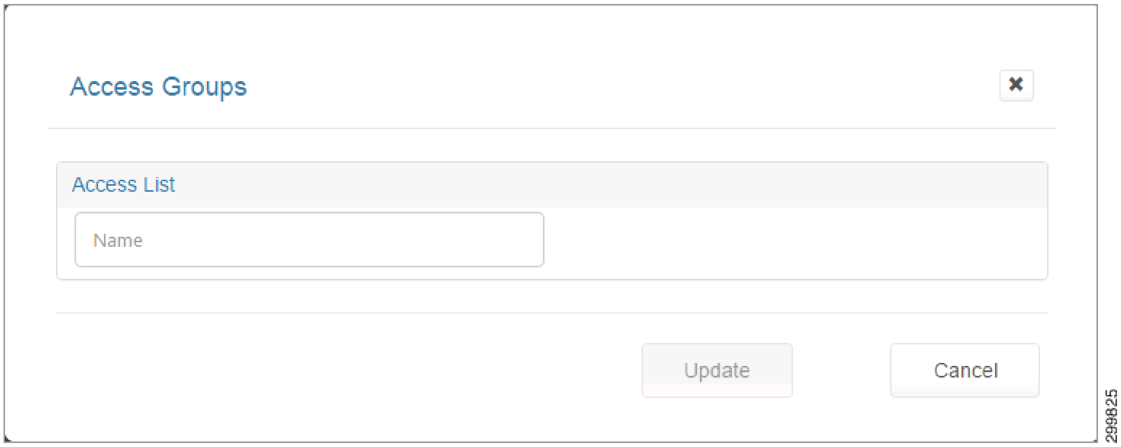
Step 3 You can:

- **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 5-36 Access Groups Screen



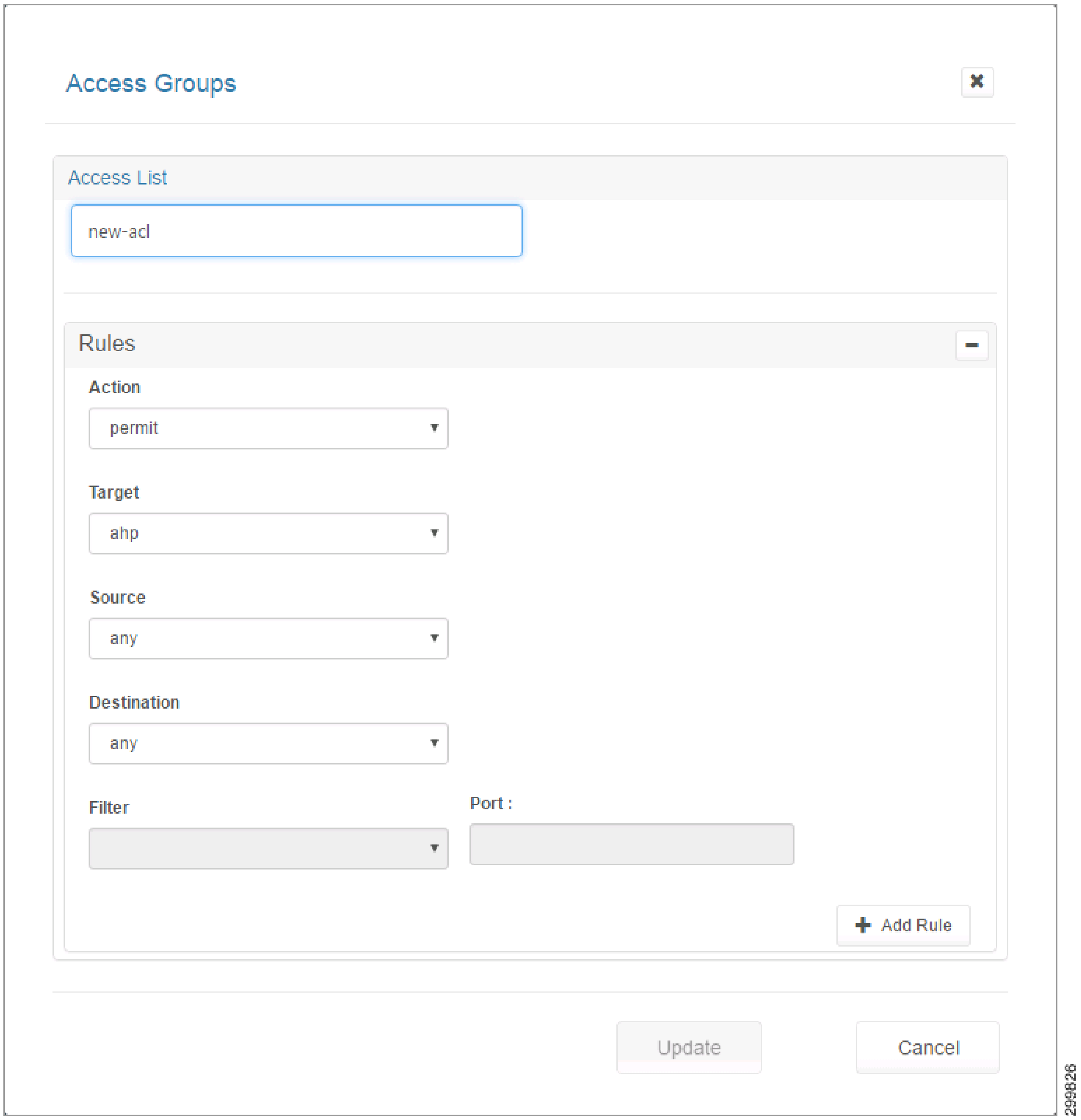
Access Groups

Access List

Name

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 5-37 Access Groups Details Screen



Access Groups

Access List

new-acl

Rules

Action: permit

Target: ahp

Source: any

Destination: any

Filter:

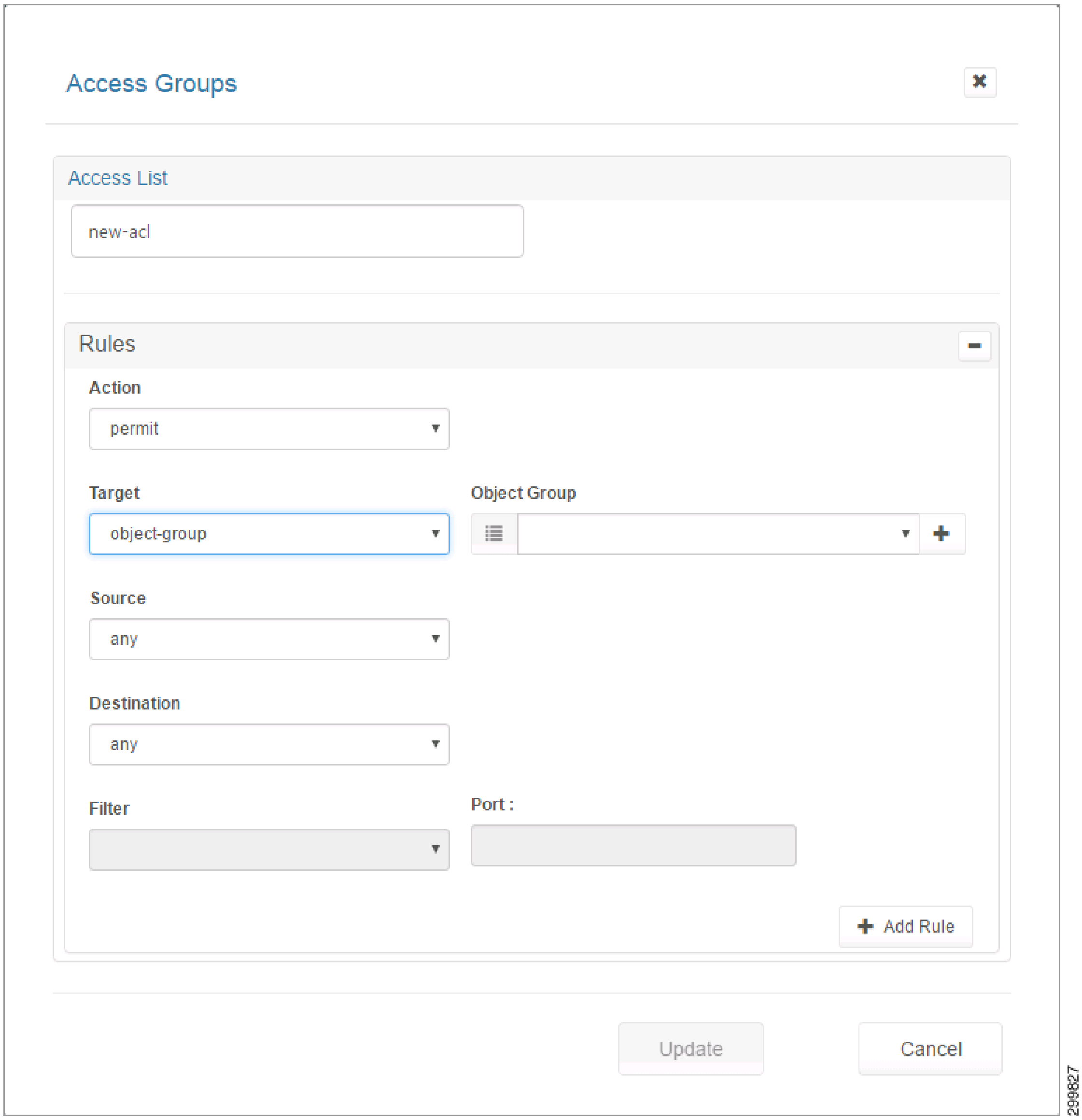
Port :

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 5-38 Access Groups Screen—Object Group Selected



Access Groups

Access List: new-acl

Rules

Action: permit

Target: object-group

Object Group:

Source: any

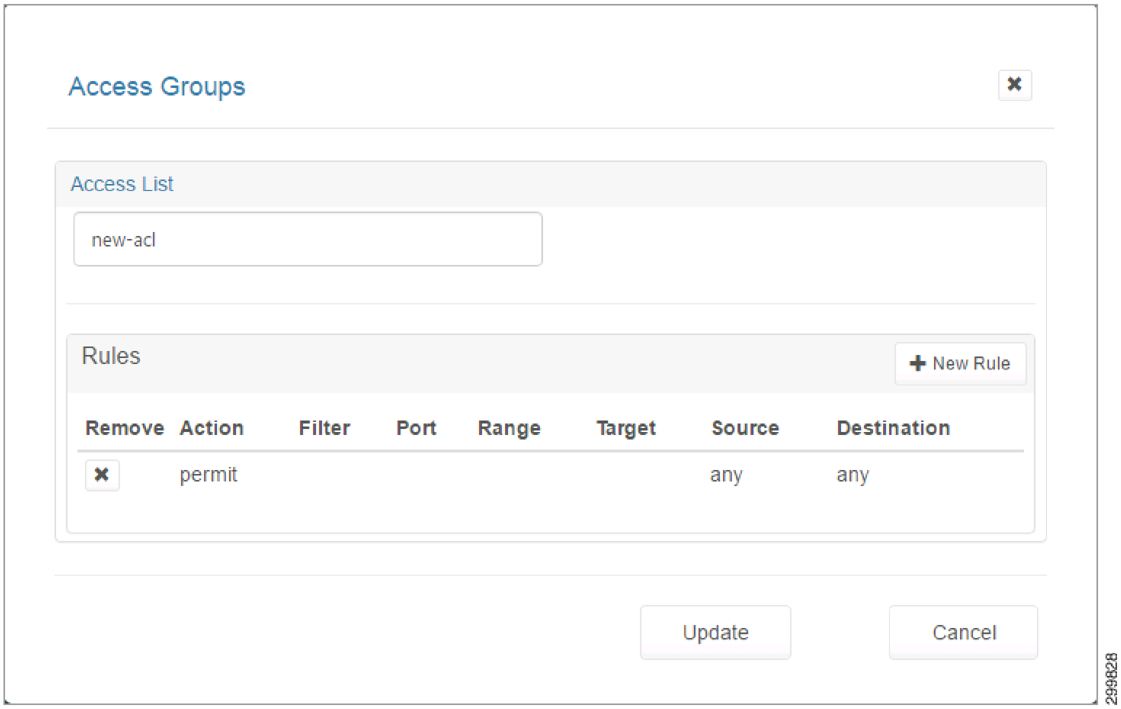
Destination: any

Filter:

Port :

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

Figure 5-39 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.

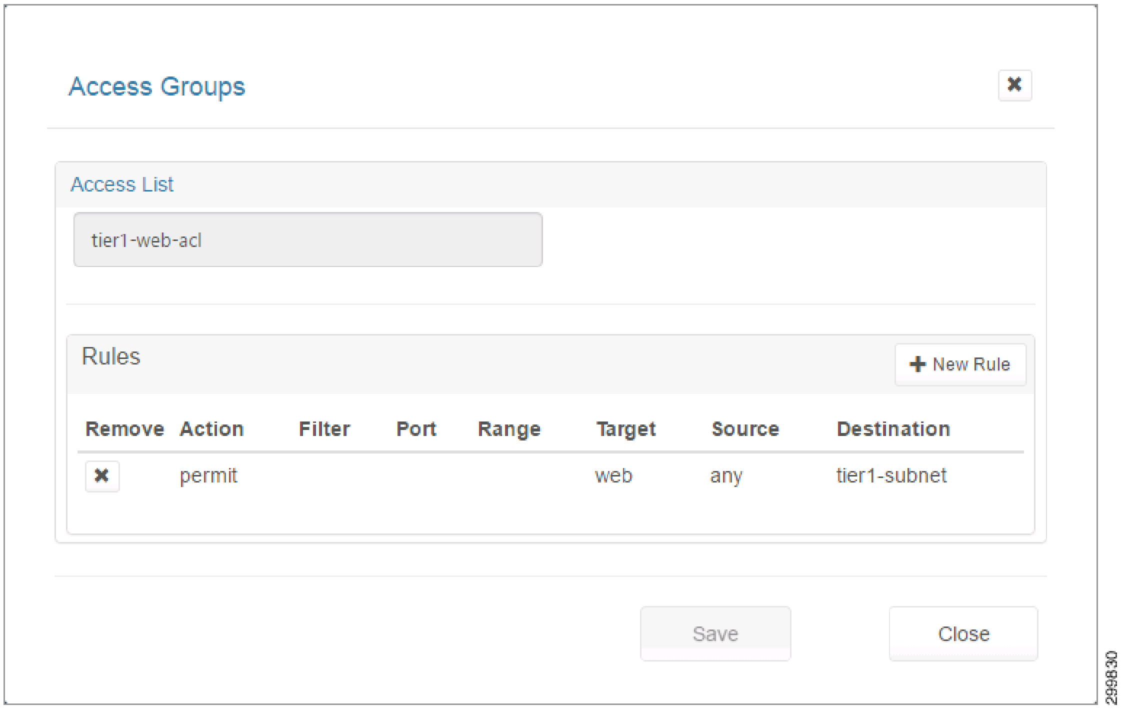
Step 7 Click the **Update** button to exit the Add Rule mode and show the list of all rules in the ACL.

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 5-40 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.

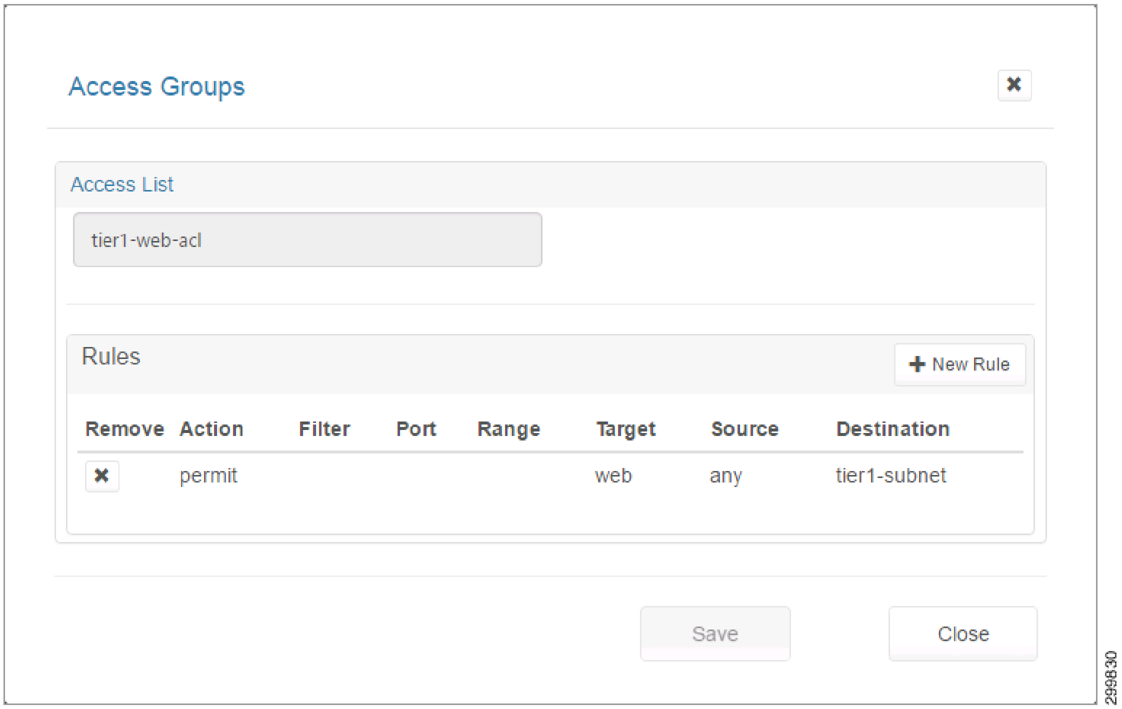
Step 4 If you make any changes to the list of Rules, the **Save** button is activated and you can click it to save the changes.

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 5-41 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

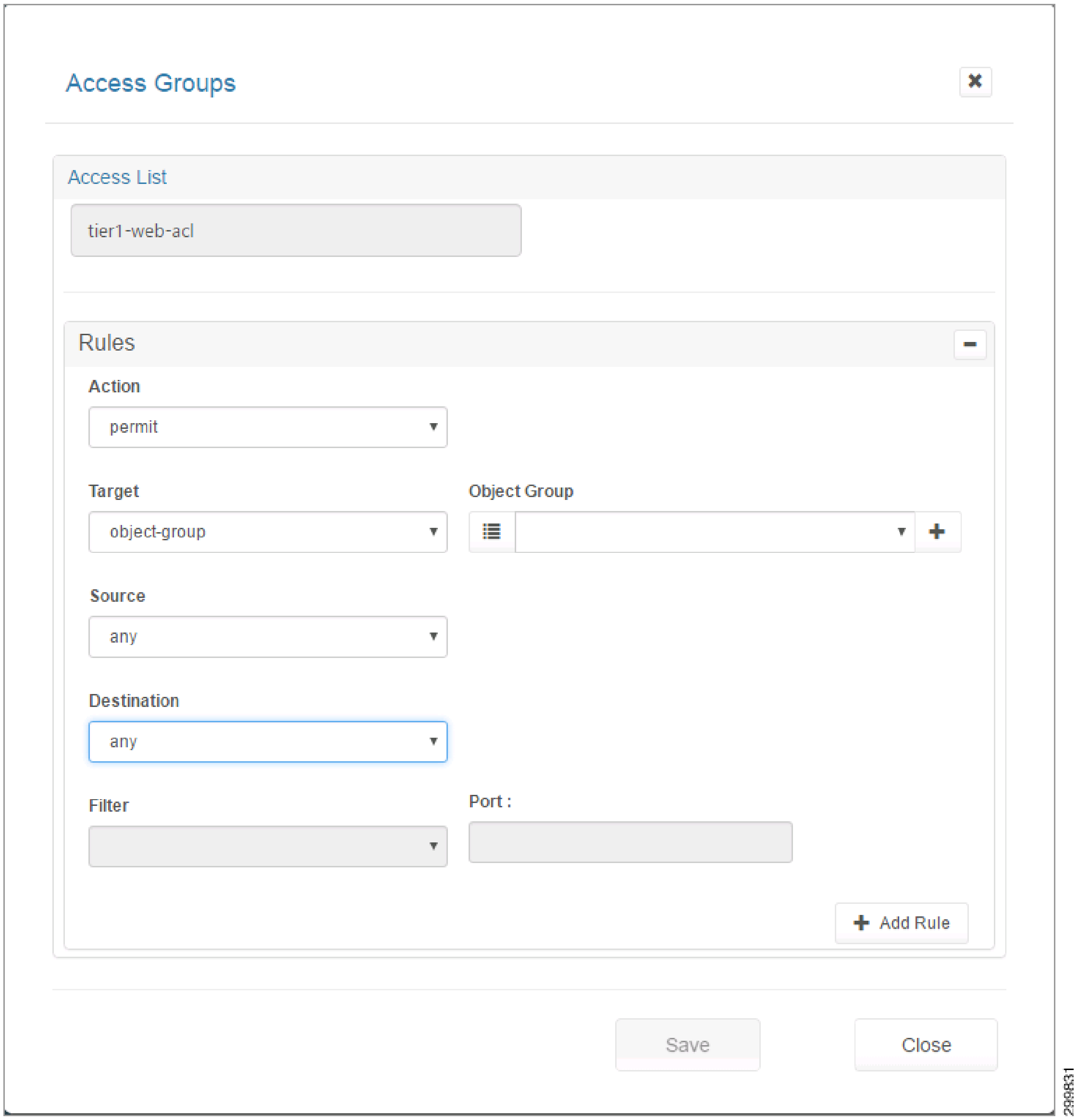
Step 3 Click the **+New Rule** button.

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 5-42 Access Groups Screen—Object Group Selected



Access Groups

Access List: tier1-web-acl

Rules

Action: permit

Target: object-group

Object Group:

Source: any

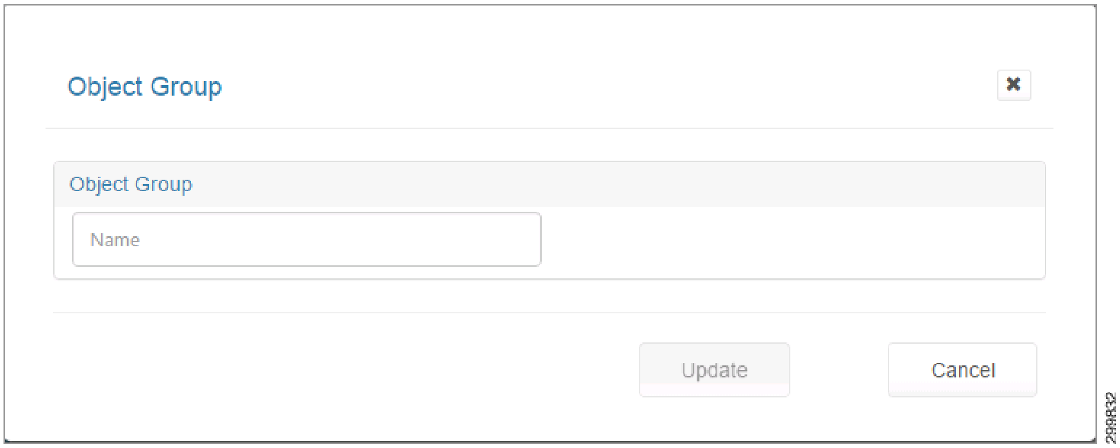
Destination: any

Filter:

Port :

You see the following screen.

Figure 5-43 Object Group Screen



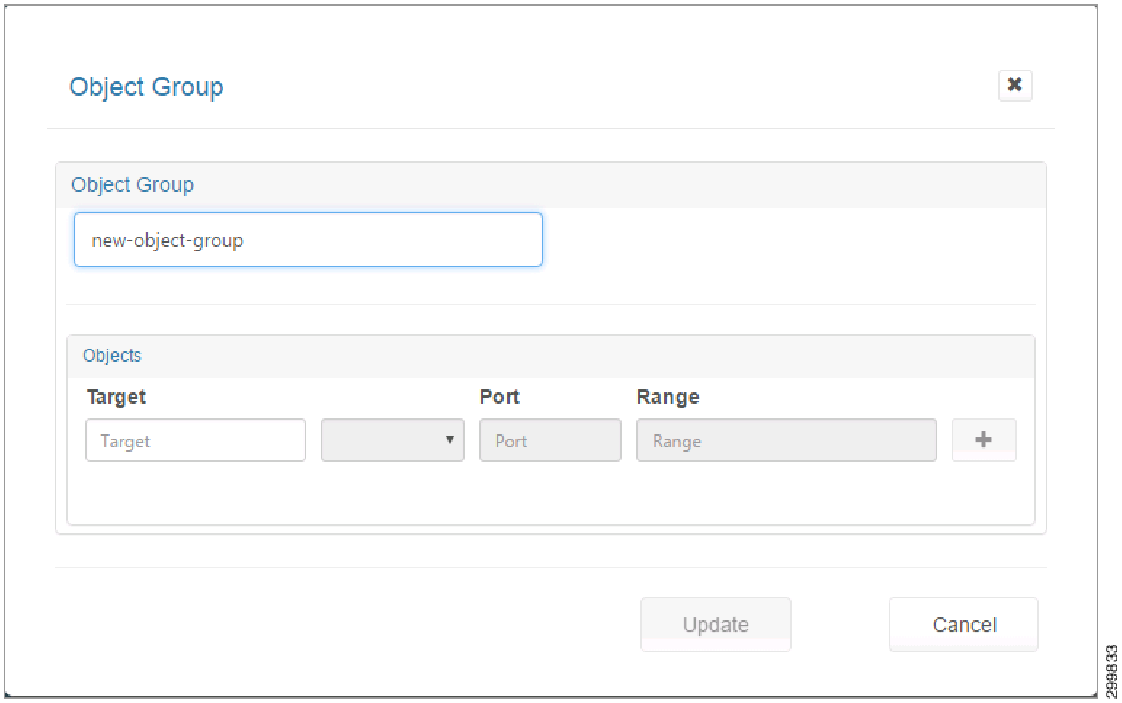
Object Group

Object Group

Name

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

Figure 5-44 Add Object Screen



Object Group

Object Group

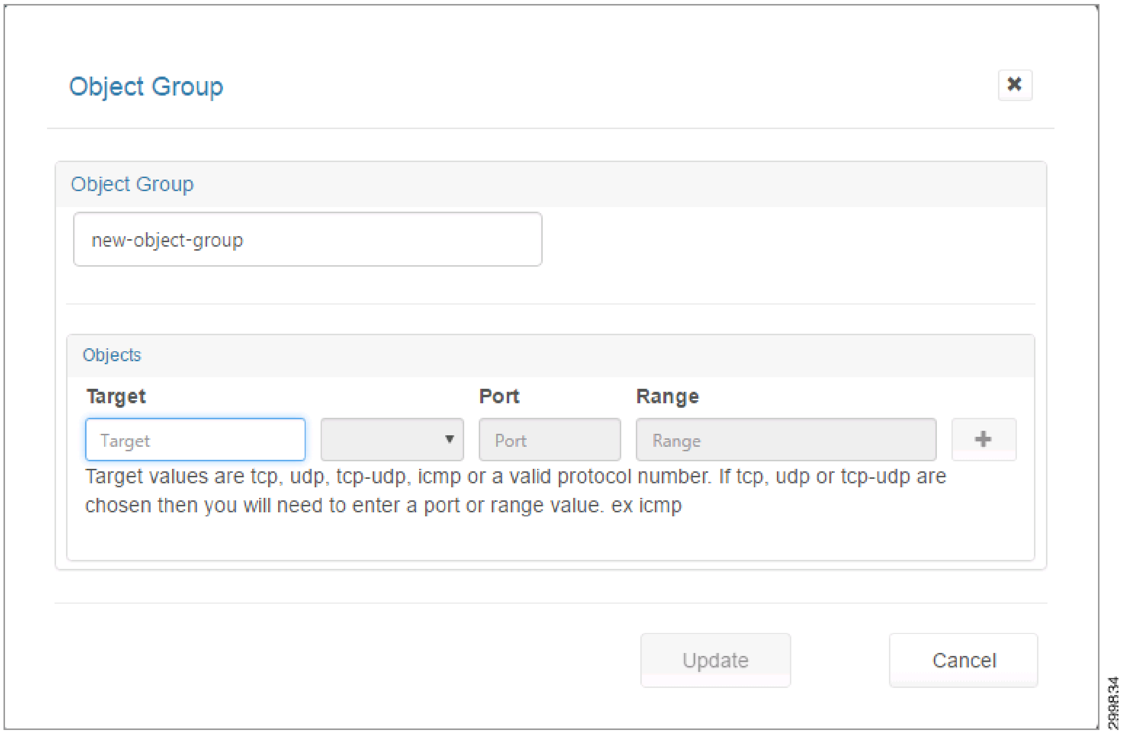
new-object-group

Objects

Target		Port	Range	
Target	▾	Port	Range	+

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

Figure 5-45 Add Object Screen—Possible Field Values Displayed



Object Group

Object Group

new-object-group

Objects

Target		Port	Range
Target	▾	Port	Range

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.

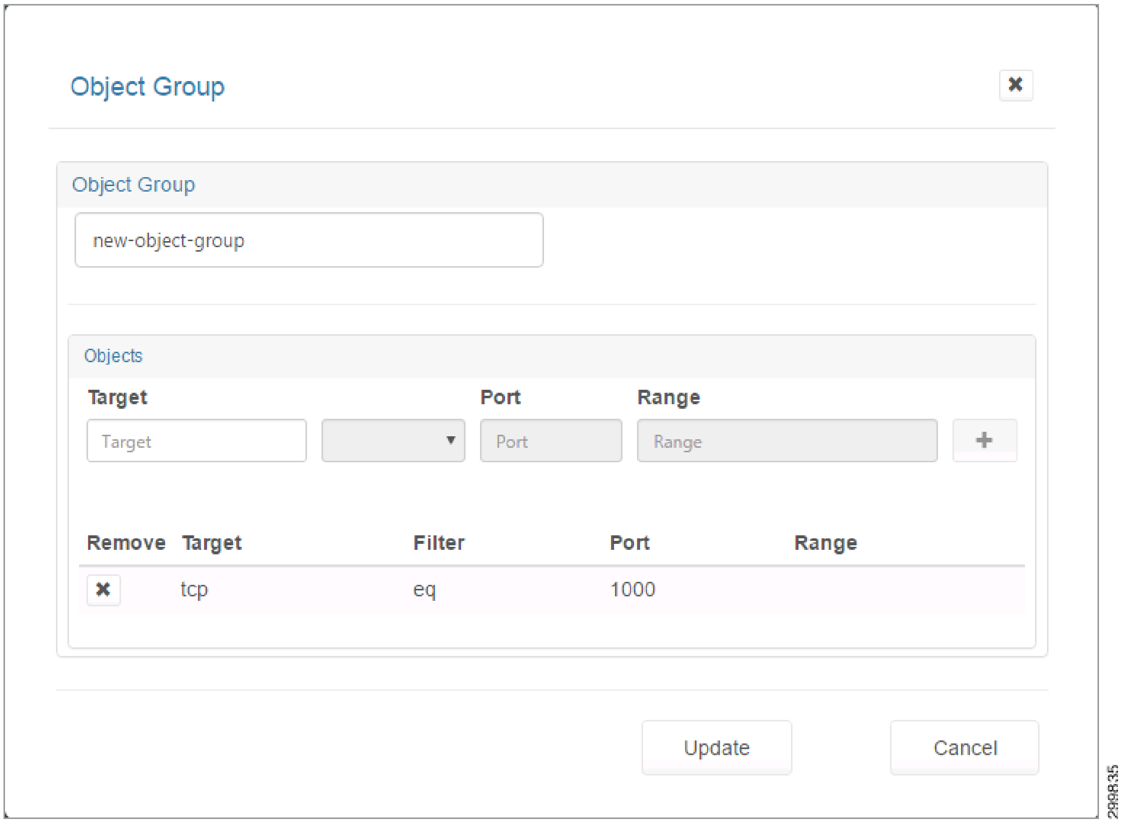
Note If “range” is present, the “filter” and “port” properties are ignored.

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 5-46 Object Added to Group Screen

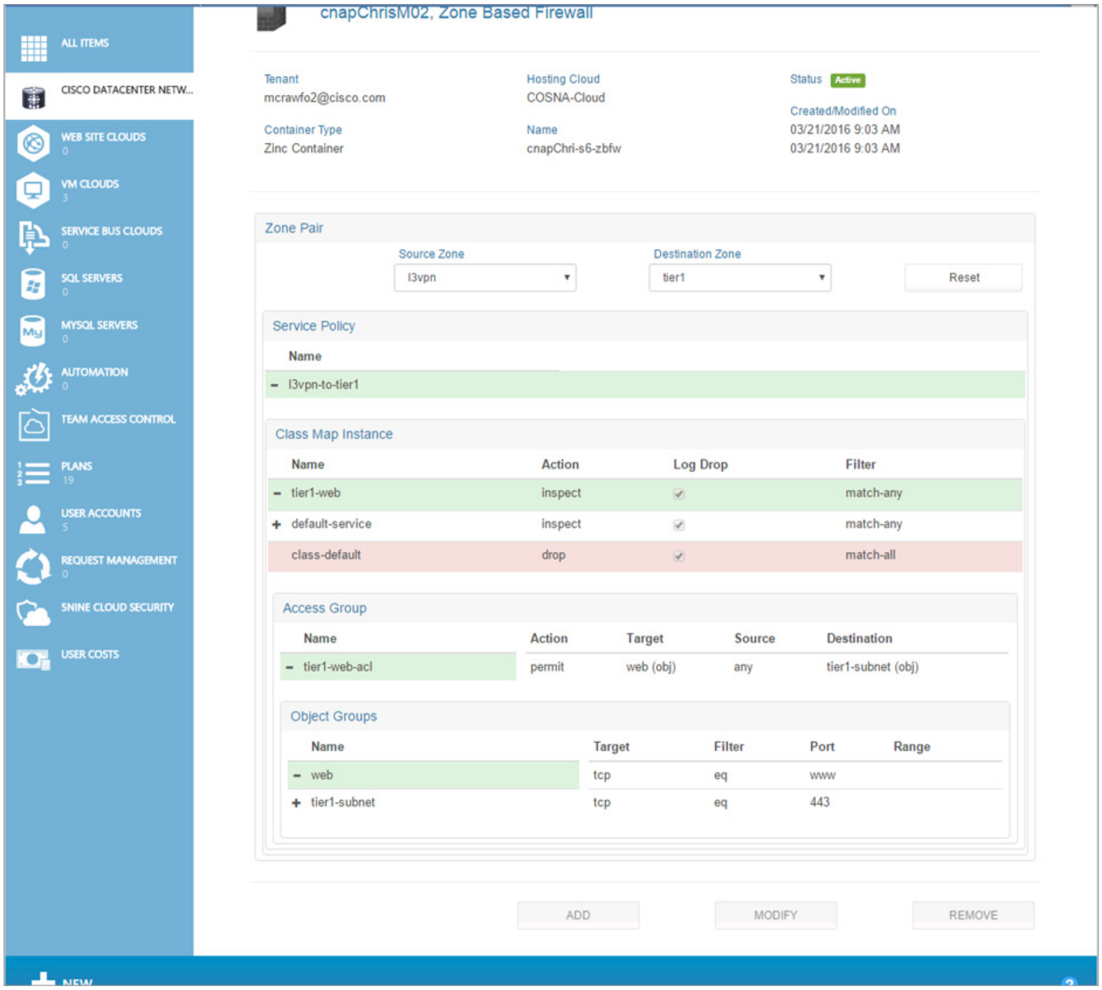


Step 10 Click the **X** under **Remove** to remove an object from the group.

Changing an Object Group

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

Figure 5-47 Firewall Zones Selected Screen—Select Object Group



cnapChrisM02, Zone Based Firewall

Tenant
mcrawfo2@cisco.com

Hosting Cloud
COSNA-Cloud

Status Active

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

Container Type
Zinc Container

Name
cnapChri-s6-zbfw

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)

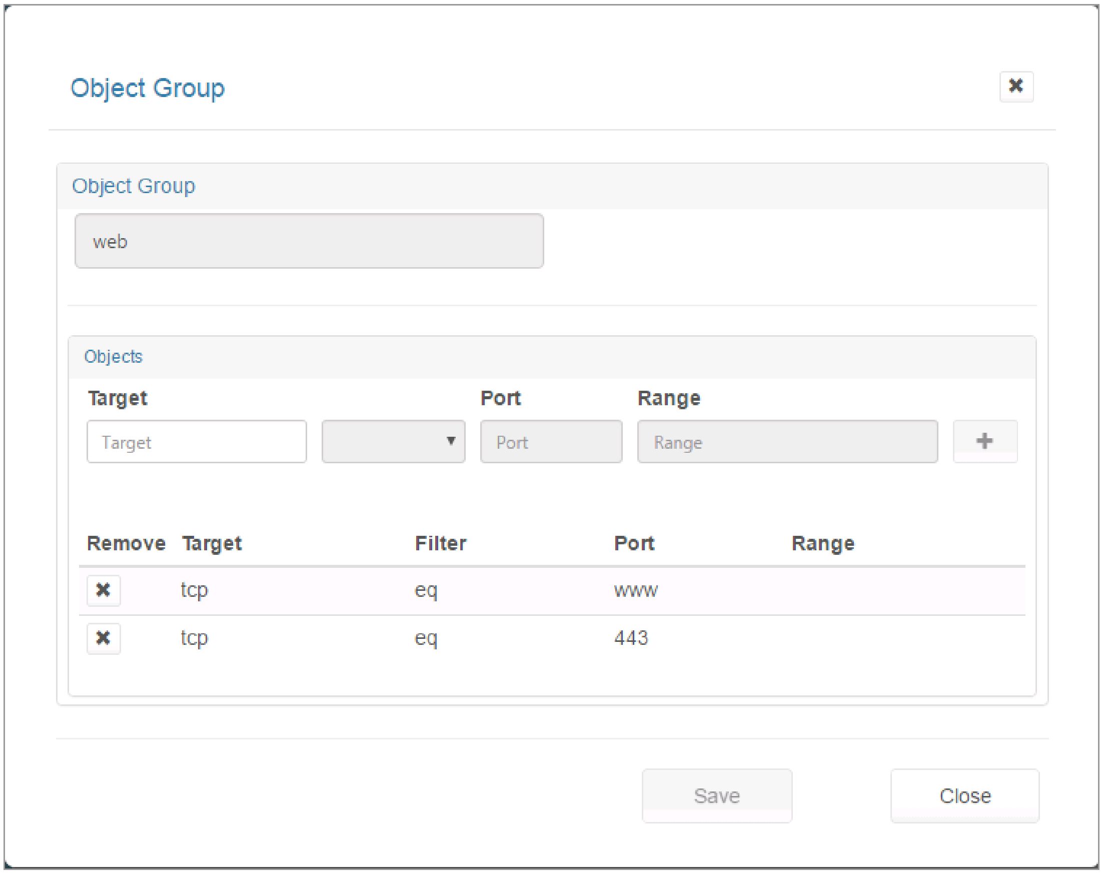
Object Groups

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

ADD MODIFY REMOVE

You see the following screen.

Figure 5-48 Modify Object Group Screen



Object Group

Object Group: web

Objects

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.

Managing Load Balancers

On the load balancer tab screen, you can:

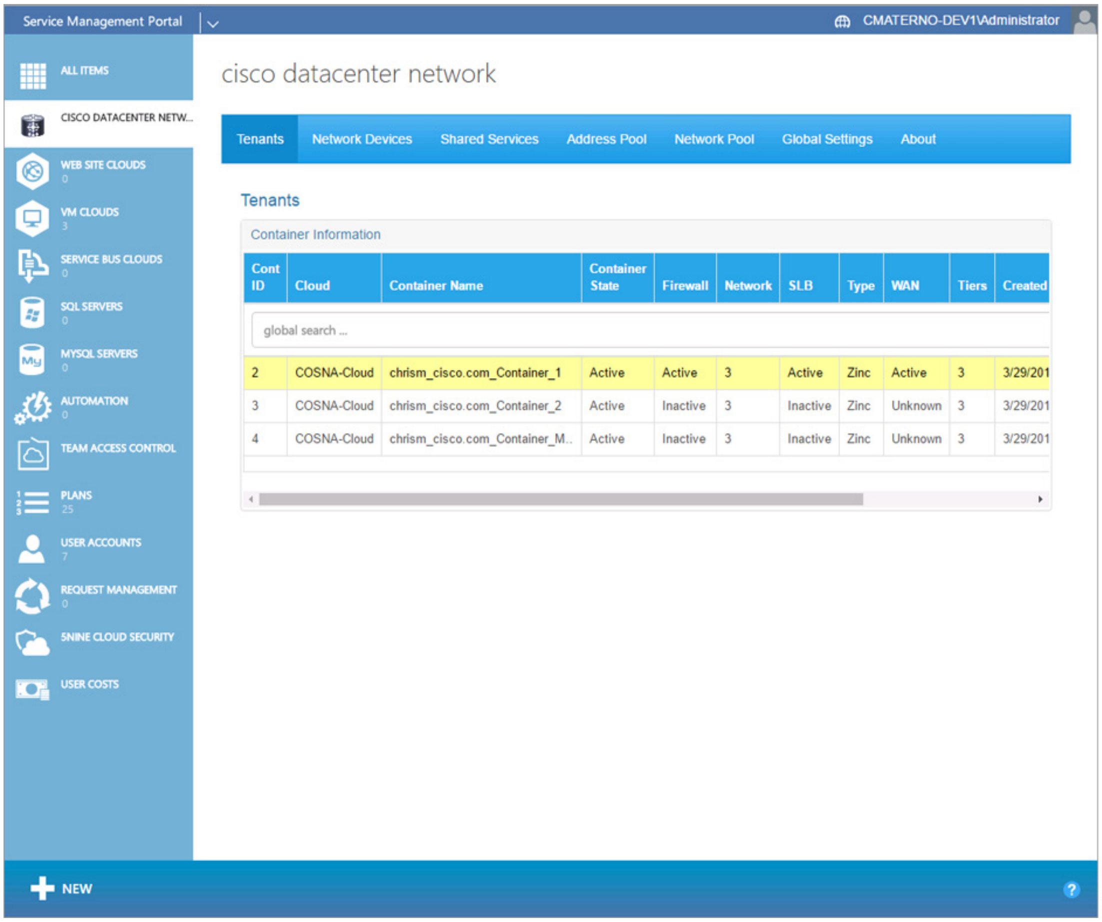
- Look at information about a load balancer.
- Enable set up of a load balancer by confirming the licensing of a Citrix NetScaler VPX.

Viewing Load Balancer Information about a Container

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

Step 1 To display load balancer information about a specific container, on the Tenants tab click on the row with the container you want to view, as shown in the following screen.

Figure 5-49 Tenants Tab Screen—Container Selected



Tenants

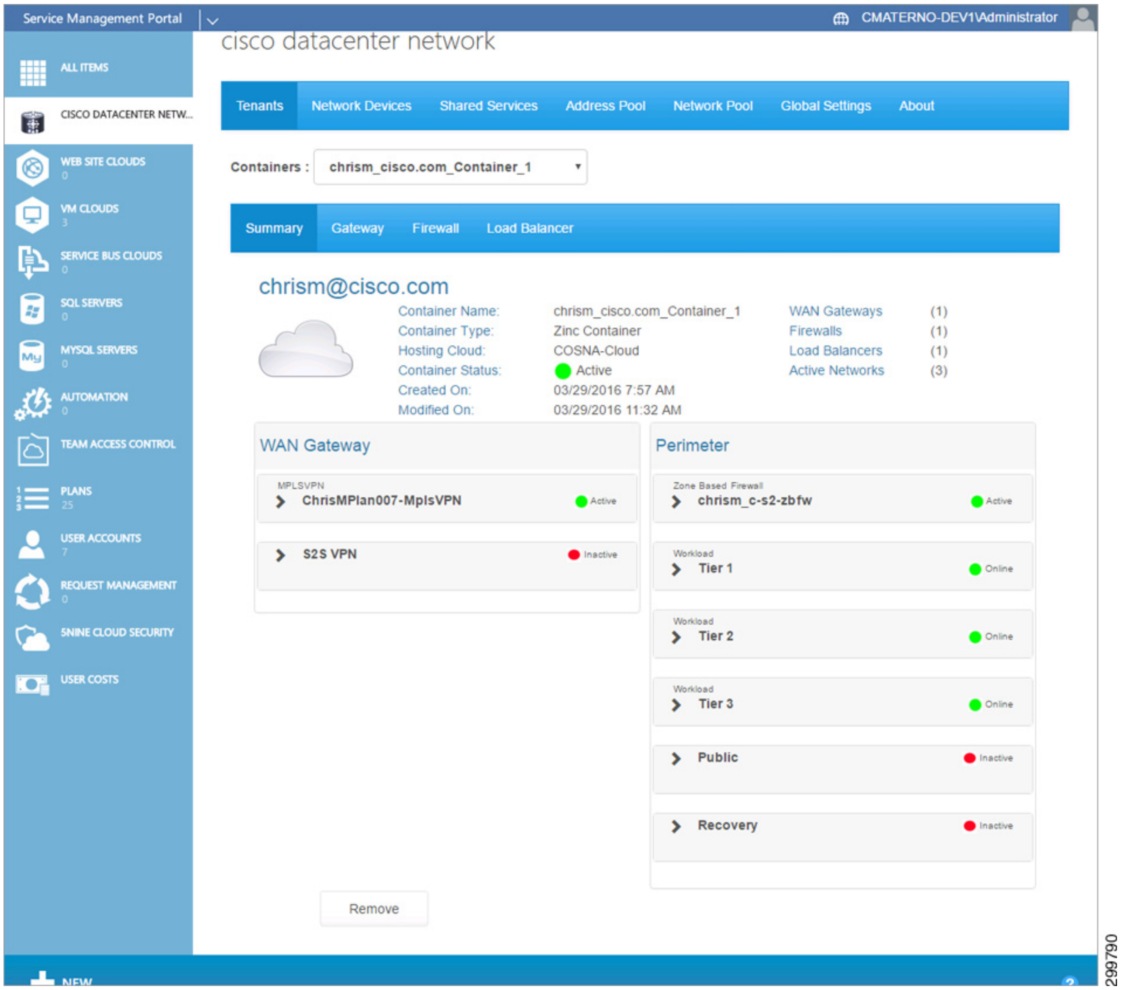
Container Information

global search ...

Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created
2	COSNA-Cloud	chrism_cisco.com_Container_1	Active	Active	3	Active	Zinc	Active	3	3/29/201
3	COSNA-Cloud	chrism_cisco.com_Container_2	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201
4	COSNA-Cloud	chrism_cisco.com_Container_M..	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201

You see the Tenants Summary screen.

Figure 5-50 Tenants Summary Screen



Containers : chrism_cisco.com_Container_1

chrism@cisco.com

Container Name:	chrism_cisco.com_Container_1	WAN Gateways	(1)
Container Type:	Zinc Container	Firewalls	(1)
Hosting Cloud:	COSNA-Cloud	Load Balancers	(1)
Container Status:	● Active	Active Networks	(3)
Created On:	03/29/2016 7:57 AM		
Modified On:	03/29/2016 11:32 AM		

WAN Gateway

- MPLSVPN ChrisMPlan007-MplsVPN ● Active
- S2S VPN ● Inactive

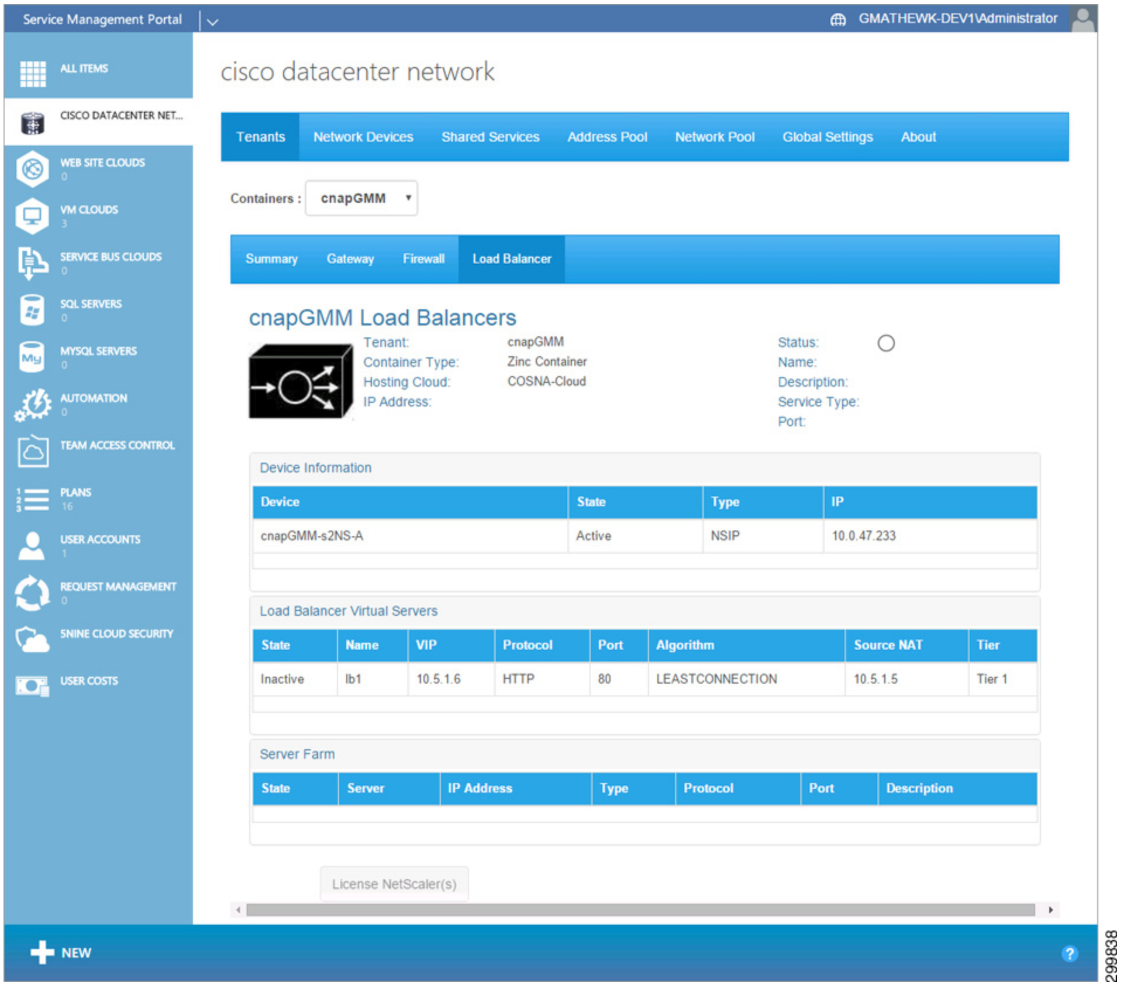
Perimeter

- Zone Based Firewall chrism_c-s2-zbfw ● Active
- Workload Tier 1 ● Online
- Workload Tier 2 ● Online
- Workload Tier 3 ● Online
- Public ● Inactive
- Recovery ● Inactive

Step 2 Click the **Load Balancer** tab.

You see the Tenant Load Balancer screen.

Figure 5-51 Tenant Load Balancer Screen



cnapGMM Load Balancers

Tenant: cnapGMM
Container Type: Zinc Container
Hosting Cloud: COSNA-Cloud
IP Address:

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

Device Information

Device	State	Type	IP
cnapGMM-s2NS-A	Active	NSIP	10.0.47.233

Load Balancer Virtual Servers

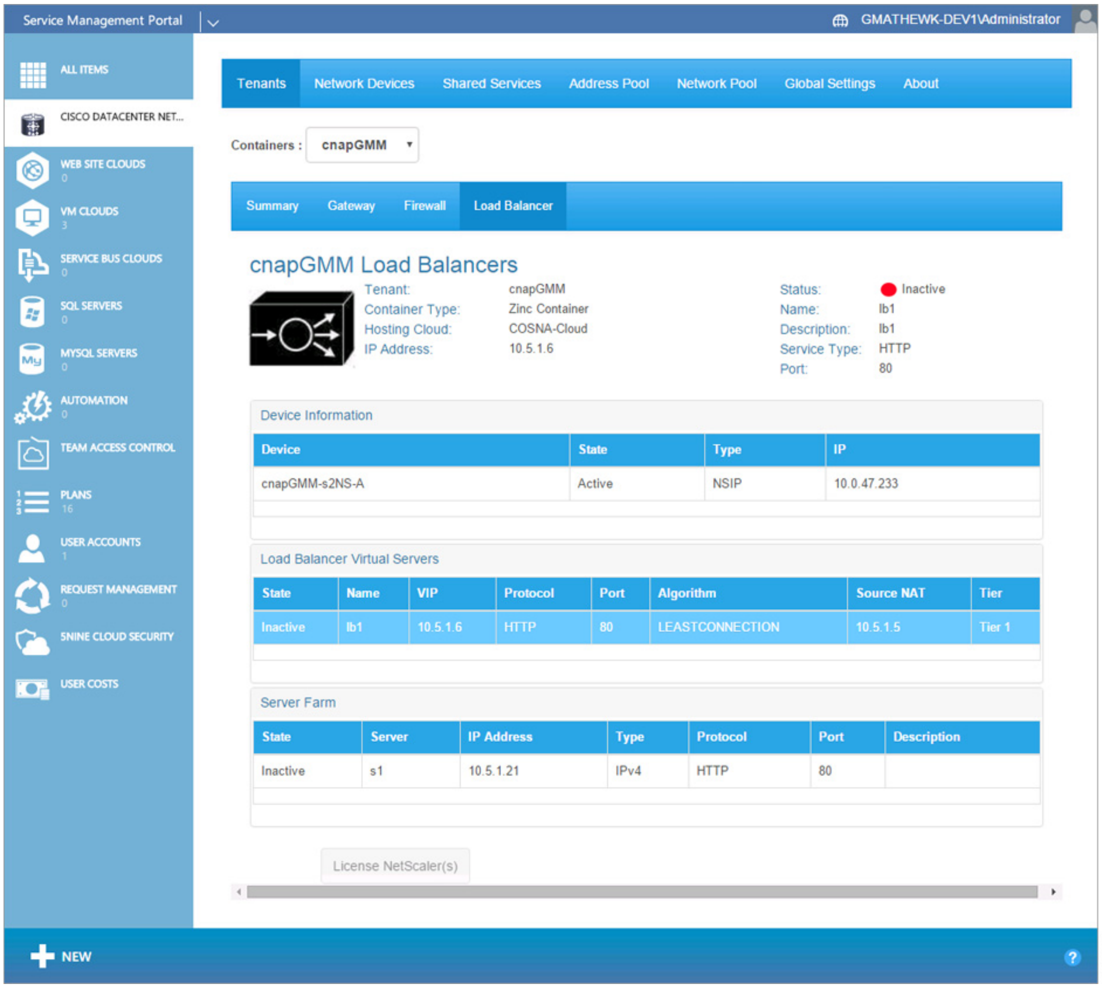
State	Name	VIP	Protocol	Port	Algorithm	Source NAT	Tier
Inactive	lb1	10.5.1.6	HTTP	80	LEASTCONNECTION	10.5.1.5	Tier 1

Server Farm

State	Server	IP Address	Type	Protocol	Port	Description

Step 3 If you click a specific Load Balancer Virtual Server, you see the corresponding Server Farm, as shown in the following screen.

Figure 5-52 *Tenant Load Balancer Screen—Server Farm*



Containers : cnapGMM

cnapGMM Load Balancers

Tenant: cnapGMM
Container Type: Zinc Container
Hosting Cloud: COSNA-Cloud
IP Address: 10.5.1.6

Status: ● Inactive
Name: lb1
Description: lb1
Service Type: HTTP
Port: 80

Device Information

Device	State	Type	IP
cnapGMM-s2NS-A	Active	NSIP	10.0.47.233

Load Balancer Virtual Servers

State	Name	VIP	Protocol	Port	Algorithm	Source NAT	Tier
Inactive	lb1	10.5.1.6	HTTP	80	LEASTCONNECTION	10.5.1.5	Tier 1

Server Farm

State	Server	IP Address	Type	Protocol	Port	Description
Inactive	s1	10.5.1.21	IPv4	HTTP	80	

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 (icons are only meaningful on initial configuration as status is not routinely monitored):
  - Green—Load balancer is Active.
  - Red— Load balancer is Inactive.
  - Yellow— Load balancer state 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 (HTTP, HTTPS, FTP).
- 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.

Setting Up a Server Load Balancer

Note In the current release, the only operation that can be performed in the Admin Portal related to setting up a server load balancer (SLB) is confirming that the Citrix NetScaler VPX is licensed. The remaining configuration is performed in the Tenant Portal. For more information on the Tenant Portal steps, see *Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Tenant Portal Guide, Release 1.1*.

The steps required in the Tenant Portal and Admin Portal to set up a server load balancer are:

Step 1 On the Tenant Portal Load Balancers tab, the tenant should add a Citrix NetScaler VPX device.

The Citrix NetScaler VPX that was added will be in a “LicenseNeeded” state. The tenant will see the message: “Please contact your Cloud Administrator to license your NetScalers”.

Note The administrator **must** license the Citrix NetScaler VPX, which is not performed within the Cisco CNAP portals nor within the Microsoft WAP interface. You must license and reboot the Citrix NetScaler VPX **before** you confirm the licensing in Cisco CNAP or the Citrix NetScaler VPX will be deleted.

Step 2 On the Admin Portal, under the Tenants tab screen, Load Balancer tab, the administrator **must** confirm that the Citrix NetScaler VPX is licensed (this sets the base configuration on the Citrix NetScaler VPX and changes the database information for the device). Information on confirming the licensing of the Citrix NetScaler VPX is shown in the next section.

On the Tenant Portal Load Balancers tab, the Citrix NetScaler VPX will now be in an Active state.

On the Tenant Portal Load Balancers tab, the tenant can now:

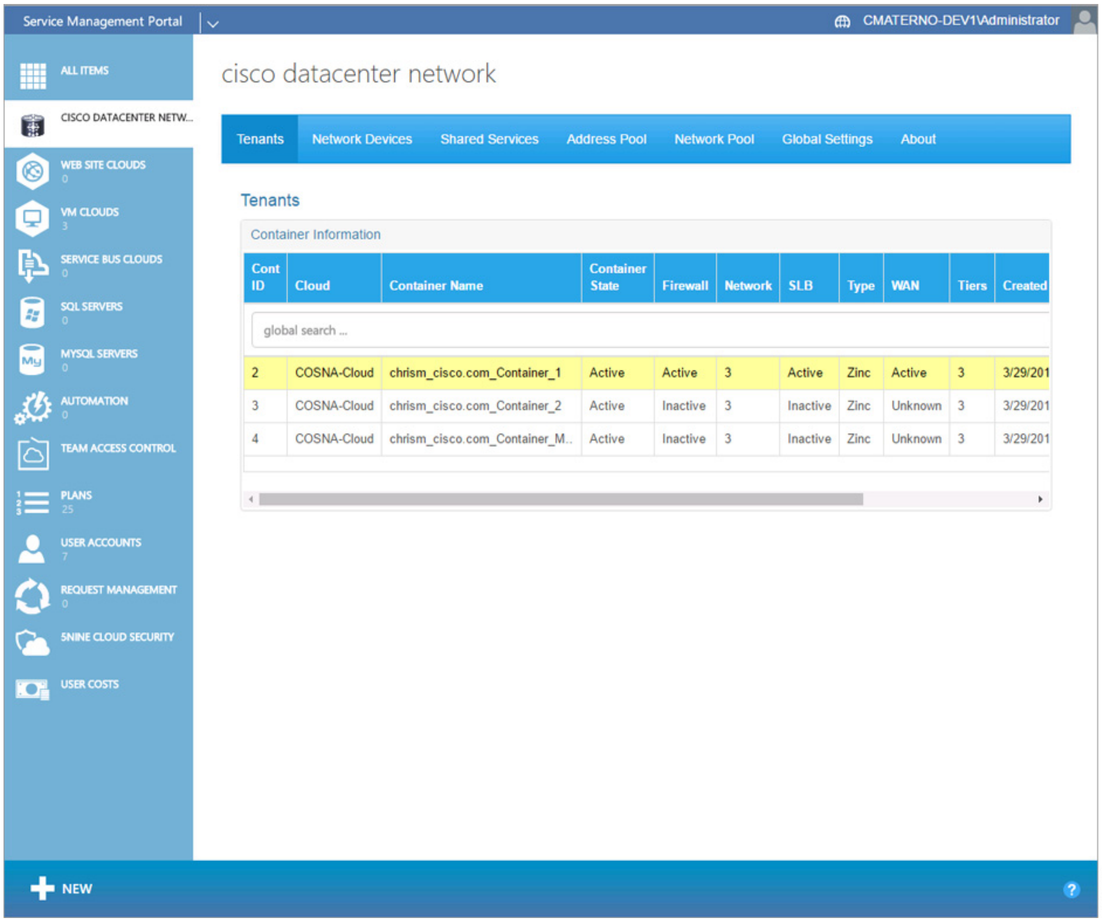
- Add a server
- Change a load balancer
- Change a server
- Remove a load balancer
- Remove a server
- Remove a Citrix NetScaler VPX

For more information, see *Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Tenant Portal Guide, Release 1.1*.

Confirming that a Citrix NetScaler VPX is Licensed

Step 1 On the Tenants tab, click on the row with the container for which you want to confirm the Citrix NetScaler VPX license, as shown in the following screen.

Figure 5-53 Tenants Tab Screen—Container Selected



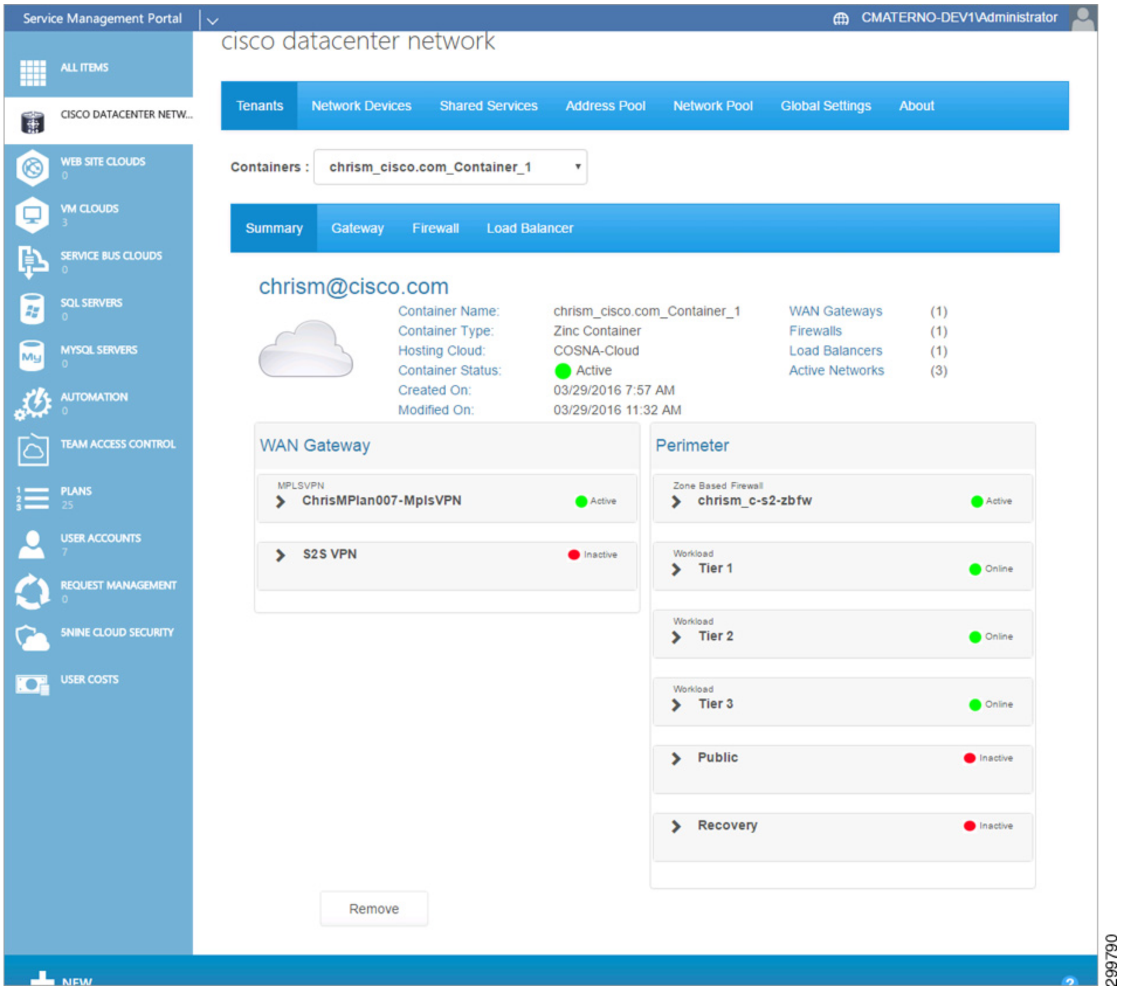
Tenants

Container Information

Cont ID	Cloud	Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	Created
2	COSNA-Cloud	chrism_cisco.com_Container_1	Active	Active	3	Active	Zinc	Active	3	3/29/201
3	COSNA-Cloud	chrism_cisco.com_Container_2	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201
4	COSNA-Cloud	chrism_cisco.com_Container_M..	Active	Inactive	3	Inactive	Zinc	Unknown	3	3/29/201

You see the Tenants Summary screen.

Figure 5-54 Tenants Summary Screen



Containers : chrism_cisco.com_Container_1

chrism@cisco.com

Container Name:	chrism_cisco.com_Container_1	WAN Gateways	(1)
Container Type:	Zinc Container	Firewalls	(1)
Hosting Cloud:	COSNA-Cloud	Load Balancers	(1)
Container Status:	● Active	Active Networks	(3)
Created On:	03/29/2016 7:57 AM		
Modified On:	03/29/2016 11:32 AM		

WAN Gateway

- MPLSVPN ChrisMPlan007-MplsVPN ● Active
- S2S VPN ● Inactive

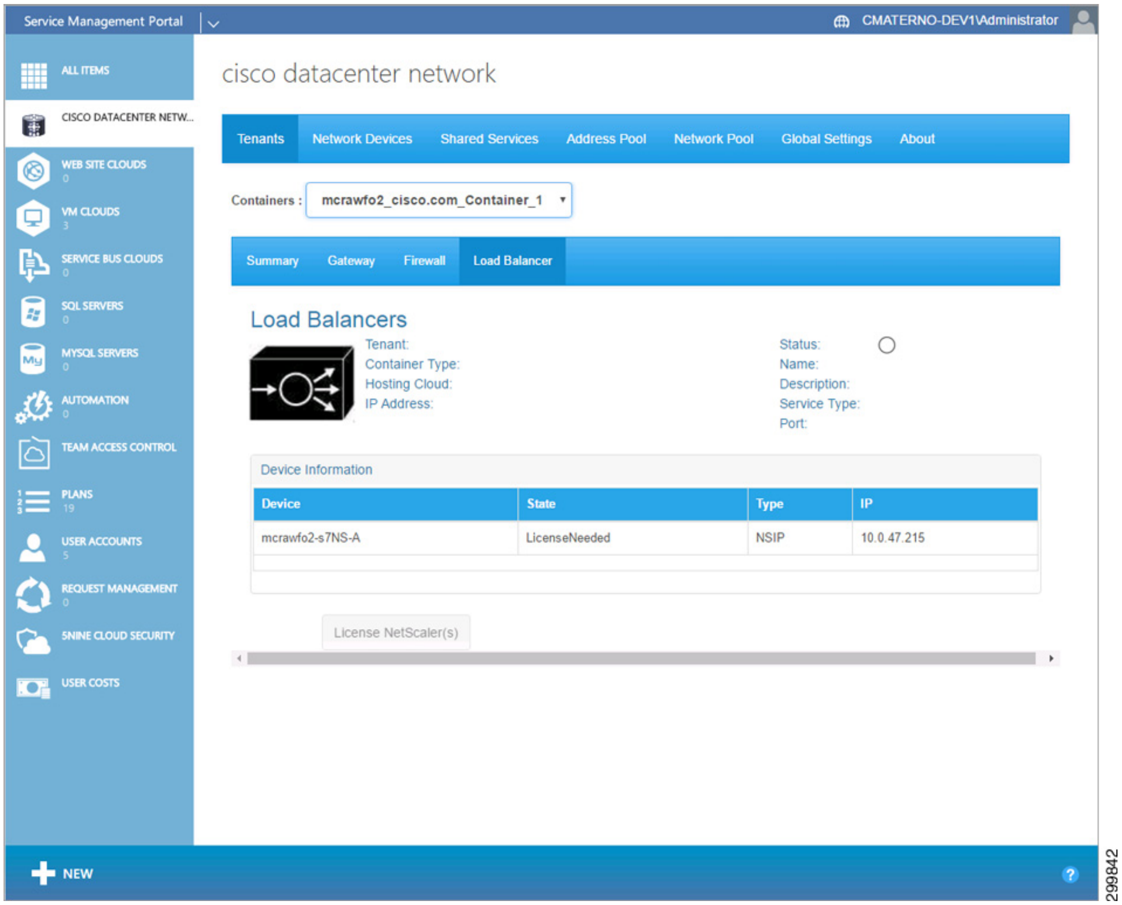
Perimeter

- Zone Based Firewall chrism_c-s2-zbfw ● Active
- Workload Tier 1 ● Online
- Workload Tier 2 ● Online
- Workload Tier 3 ● Online
- Public ● Inactive
- Recovery ● Inactive

Step 2 Click the **Load Balancer** tab.

You see the Tenant Load Balancer screen.

Figure 5-55 Tenant Load Balancer Screen



Containers : mcrawfo2_cisco.com_Container_1

Tenant:
Container Type:
Hosting Cloud:
IP Address:

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

Device Information

Device	State	Type	IP
mcrawfo2-s7NS-A	LicenseNeeded	NSIP	10.0.47.215

Note You **must** license and reboot the Citrix NetScaler VPX **before** you confirm the licensing in Cisco CNAP or the Citrix NetScaler VPX will be deleted.

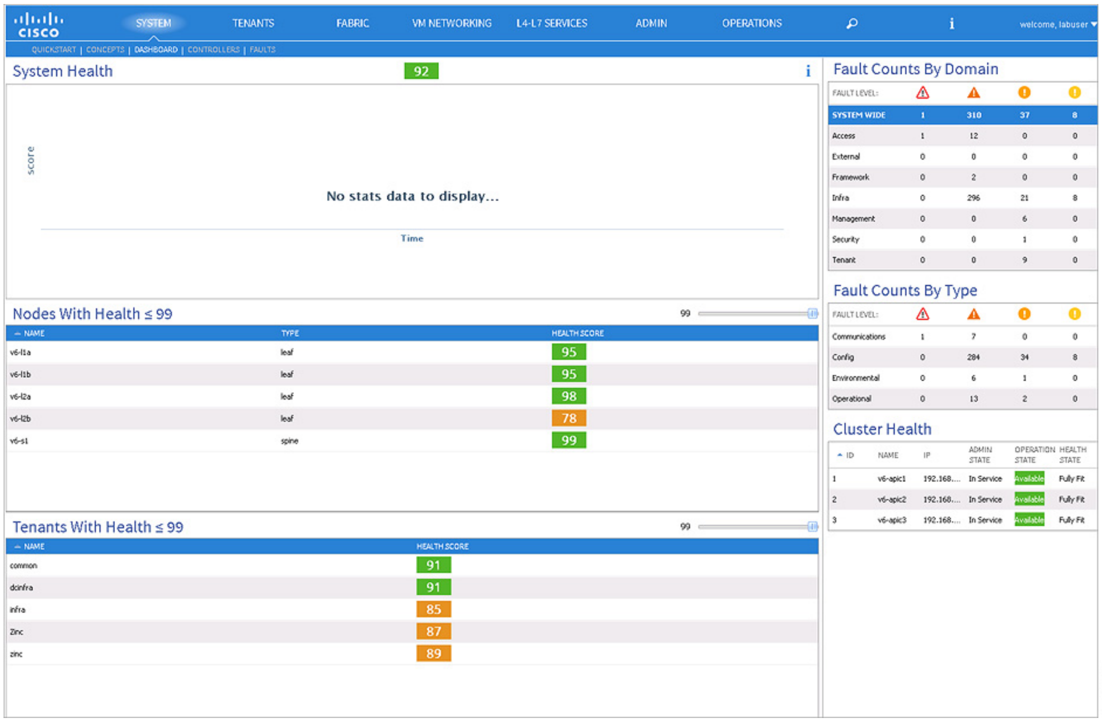
Step 3 The Citrix NetScaler VPX that requires license confirmation will be in a "LicenseNeeded" state. Click the device, then click **License NetScaler(s)**.

APPENDIX A

Cisco Application Policy Infrastructure Controller

The Cisco Application Policy Infrastructure Controller (APIC) user interface provides useful information about your Cisco CNAP provisioned containers and network. For more information, consult the Cisco APIC documentation: http://www.cisco.com/c/en/us/support/cloud-systems-management/application-policy-infrastructure-controller-apic/tsd-products-support-series-home.html

Figure A-1 Cisco Application Policy Infrastructure Controller Screen



Nodes With Health ≤ 99

NAME	TYPE	HEALTH SCORE
v6-l1a	leaf	95
v6-l1b	leaf	95
v6-l2a	leaf	98
v6-l2b	leaf	78
v6-s1	spine	99

Tenants With Health ≤ 99

NAME	HEALTH SCORE
common	91
dcinfra	91
infra	85
Zinc	87
zinc	89

Fault Counts By Domain

FAULT LEVEL:	⚠	⚠	❗	❗
SYSTEM WIDE	1	310	37	8
Access	1	12	0	0
External	0	0	0	0
Framework	0	2	0	0
Infra	0	296	21	8
Management	0	0	6	0
Security	0	0	1	0
Tenant	0	0	9	0

Fault Counts By Type

FAULT LEVEL:	⚠	⚠	❗	❗
Communications	1	7	0	0
Config	0	284	34	8
Environmental	0	6	1	0
Operational	0	13	2	0

Cluster Health

ID	NAME	IP	ADMIN STATE	OPERATION STATE	HEALTH STATE
1	v6-apic1	192.168....	In Service	Available	Fully Fit
2	v6-apic2	192.168....	In Service	Available	Fully Fit
3	v6-apic3	192.168....	In Service	Available	Fully Fit

APPENDIX B

Sample Database as a Service Deployment

This appendix provides an overview of how you can deploy Database as a Service (DBaaS) over the CCA MCP solution. The deployment procedures guide you through the required steps.

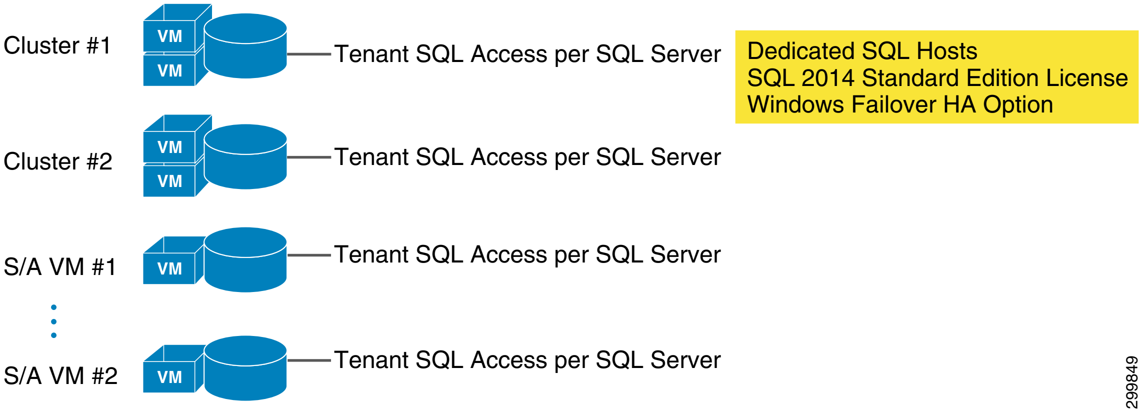
For detailed information on deploying DBaaS, see *Cisco Cloud Architecture for the Microsoft Cloud Platform: DBaaS Configuration Guide, Release 1.0* and the Microsoft Azure Pack documentation.

This appendix describes two deployment modes:

- Dedicated Service Deployment Mode—Failover Cluster Redundancy Option and SQL DBaaS Instance in Dedicated per-Tenant Virtual Machines
- Shared Service Deployment Mode—Always On Cluster Redundancy Option and DBaaS Instance per-Tenant on Multi-tenant SQL Server(s)

Dedicated Service Deployment Mode—Failover Cluster Redundancy Option and SQL DBaaS Instance in Dedicated per-Tenant Virtual Machines

Figure B-1 Failover Cluster Redundancy Option


Cluster #1
VM
VM
Tenant SQL Access per SQL Server
Dedicated SQL Hosts
SQL 2014 Standard Edition License
Windows Failover HA Option
Cluster #2
VM
VM
Tenant SQL Access per SQL Server
S/A VM #1
VM
Tenant SQL Access per SQL Server
S/A VM #2
VM
Tenant SQL Access per SQL Server
299849

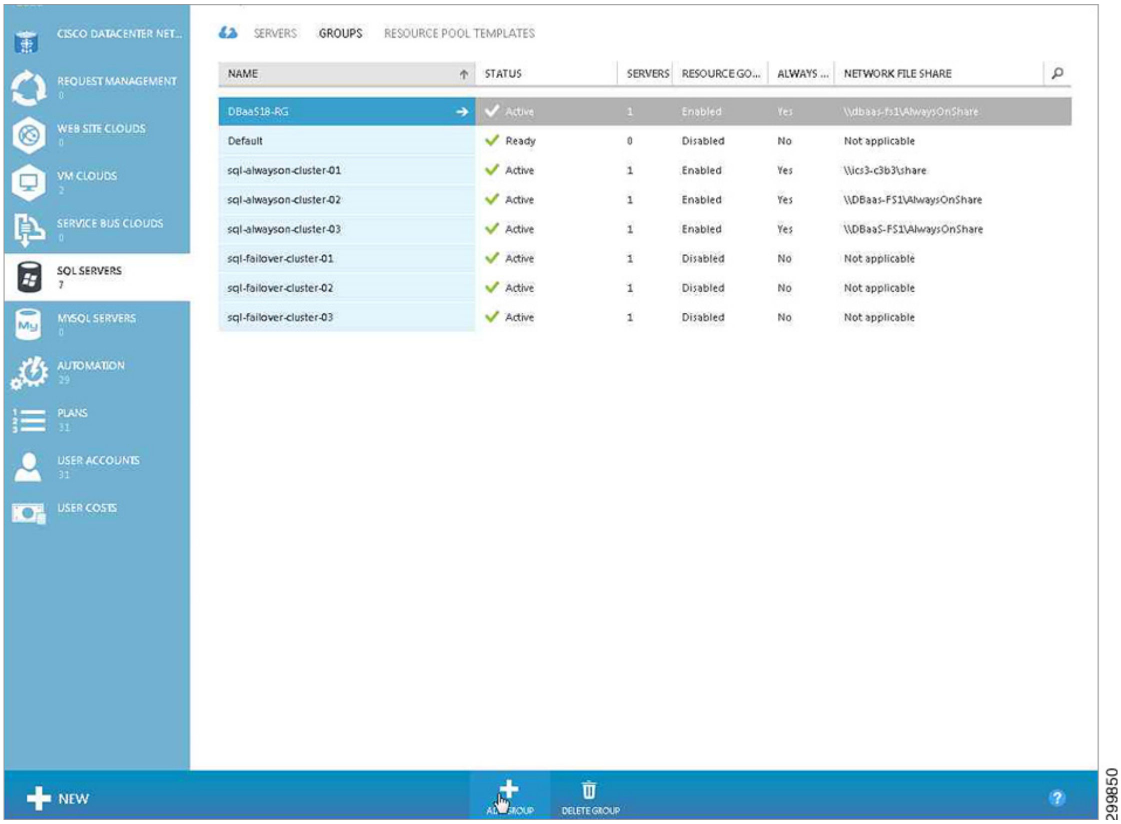
Use the Administrator SQL Resource Provider User Interface to Create the DBaaS Plan and Resource Allocation

Step 1 On the WAP Admin Portal, log in with your Active Directory user ID and password.

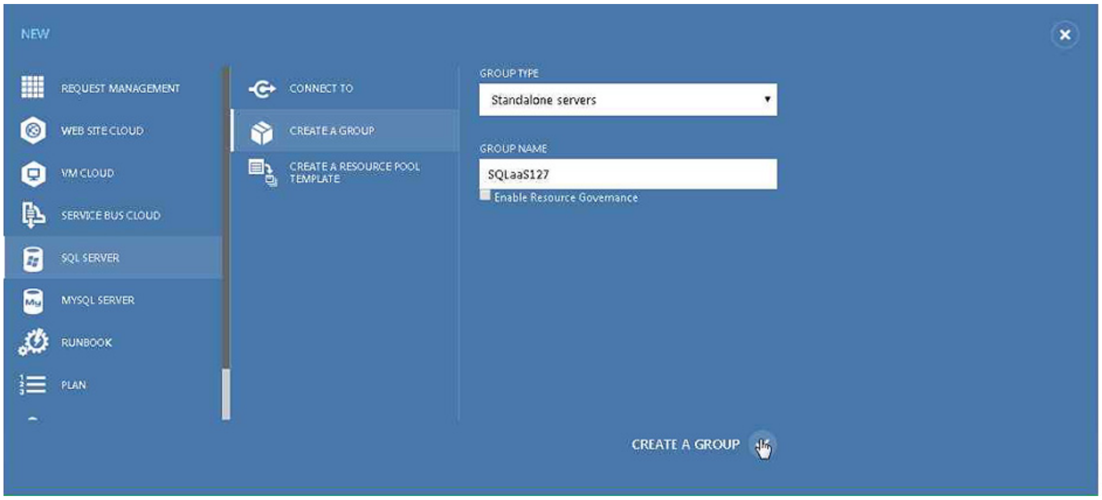
Step 2 Open the SQL Server RP tab. At the bottom of screen, click **+ New** to add a group.

Step 3 Enter the Group Name and specify whether it is standalone or HA.

Step 4 Check the SQL Server Group View to verify that the Group is created when you are done.



NAME	STATUS	SERVERS	RESOURCE GO...	ALWAYS ...	NETWORK FILE SHARE
DBaaS18-RG	✓ Active	1	Enabled	Yes	\\dbaas-fs1\AlwaysOnShare
Default	✓ Ready	0	Disabled	No	Not applicable
sql-alwayson-cluster-01	✓ Active	1	Enabled	Yes	\\ics3-c3b3\share
sql-alwayson-cluster-02	✓ Active	1	Enabled	Yes	\\DBaas-FS1\AlwaysOnShare
sql-alwayson-cluster-03	✓ Active	1	Enabled	Yes	\\DBaaS-FS1\AlwaysOnShare
sql-failover-cluster-01	✓ Active	1	Disabled	No	Not applicable
sql-failover-cluster-02	✓ Active	1	Disabled	No	Not applicable
sql-failover-cluster-03	✓ Active	1	Disabled	No	Not applicable

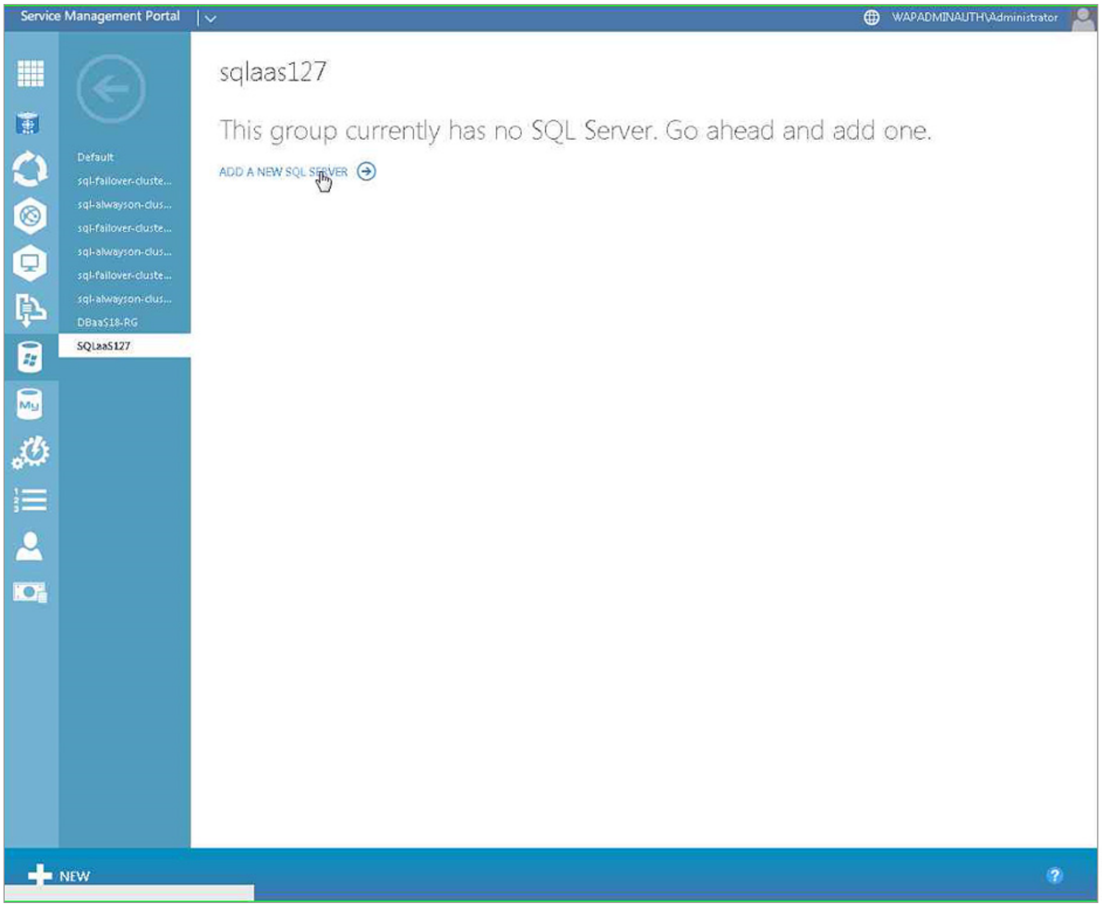


GROUP TYPE: Standalone servers

GROUP NAME: SQLaaS127

□ Enable Resource Governance

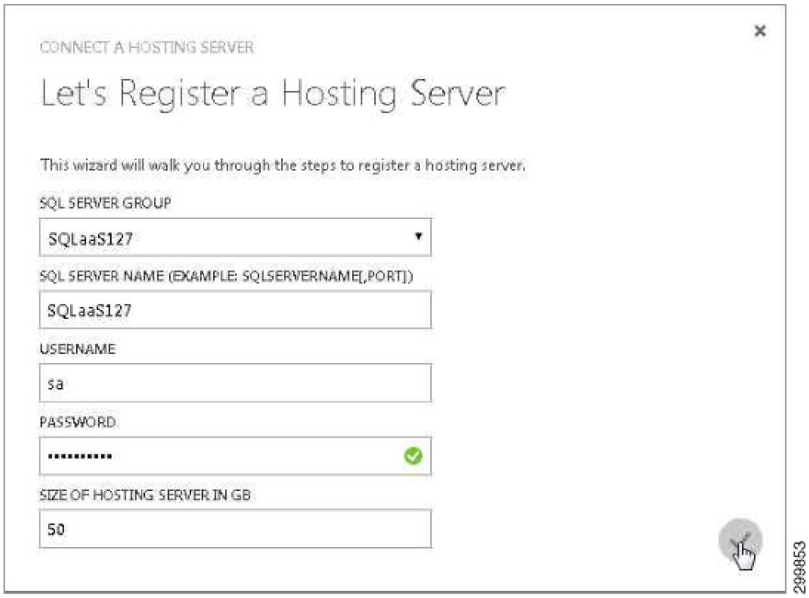
Step 5 Add a server to the new group.



sqlaas127

This group currently has no SQL Server. Go ahead and add one.

Step 6 Specify the Server Name, User Name/Password, and Instance Disk Size Allocation.



CONNECT A HOSTING SERVER

Let's Register a Hosting Server

This wizard will walk you through the steps to register a hosting server.

SQL SERVER GROUP: SQLaaS127

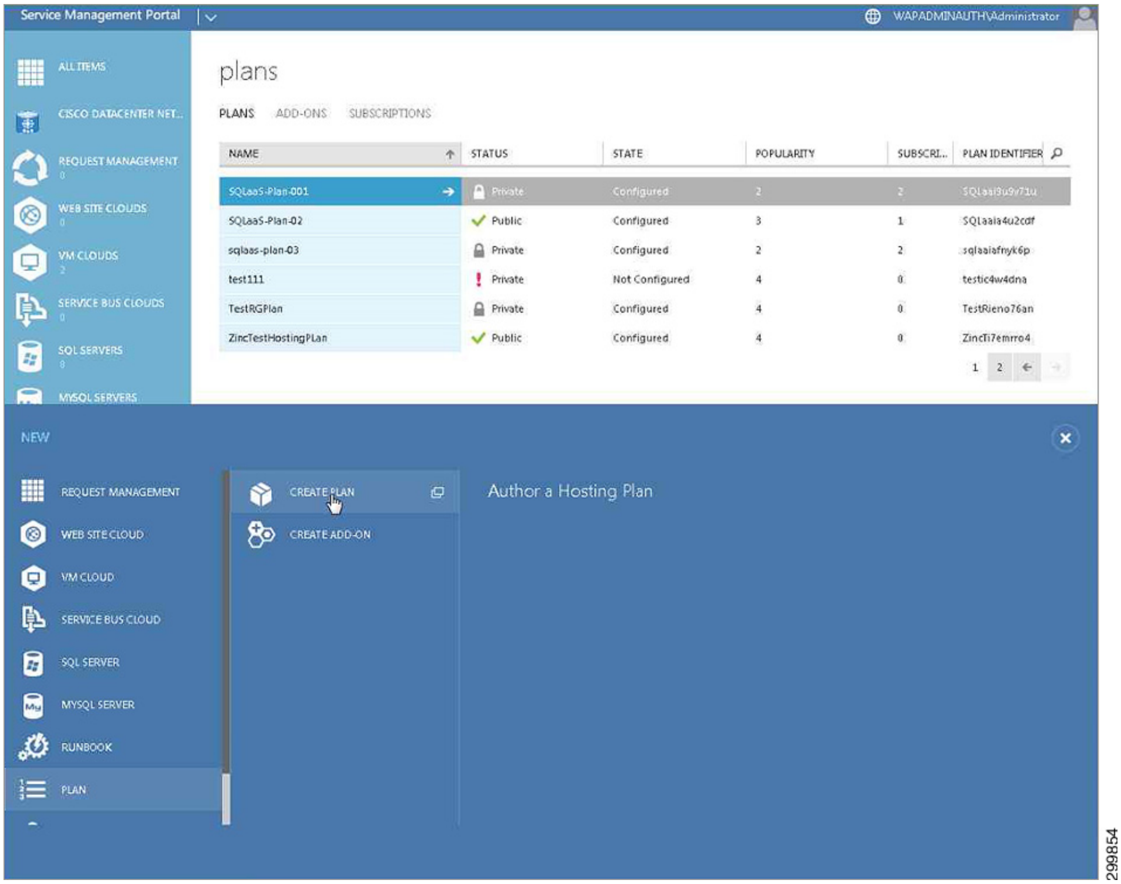
SQL SERVER NAME (EXAMPLE: SQLSERVERNAME[,PORT]): SQLaaS127

USERNAME: sa

PASSWORD: ••••••••••

SIZE OF HOSTING SERVER IN GB: 50

Step 7 Create a plan.



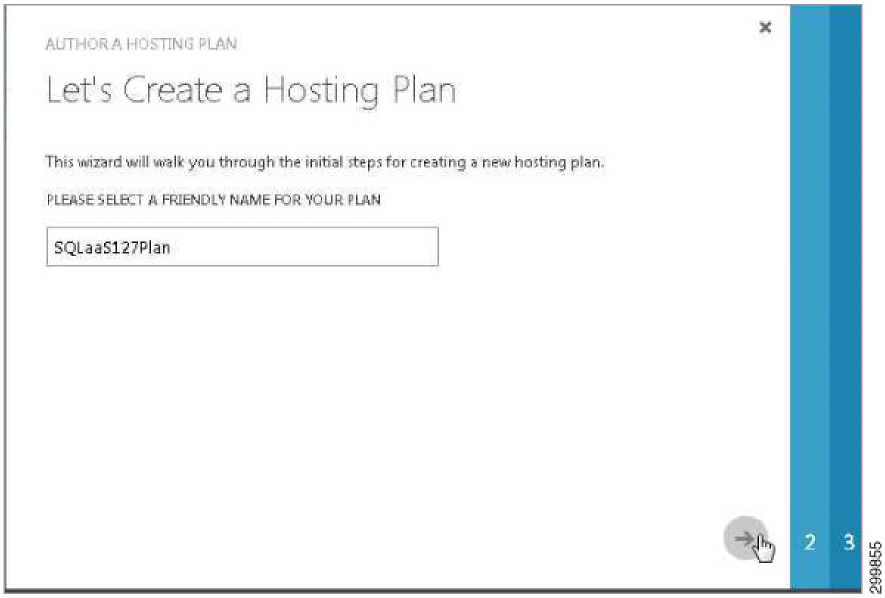
plans

PLANS ADD-ONS SUBSCRIPTIONS

NAME	STATUS	STATE	POPULARITY	SUBSCRI...	PLAN IDENTIFIER
SQLaaS-Plan-001	Private	Configured	2	2	SQLaai9u9v71u
SQLaaS-Plan-02	✓ Public	Configured	3	1	SQLaaia4u2cdf
sqlaas-plan-03	Private	Configured	2	2	sqlaaiafnyk6p
test111	! Private	Not Configured	4	0	testic4w4dna
TestRGPlan	Private	Configured	4	0	TestRieno76an
ZincTestHostingPLan	✓ Public	Configured	4	0	ZincTi7emrro4

1 2

Step 8 Specify the plan name and services (SQL Server Name Selection)



AUTHOR A HOSTING PLAN

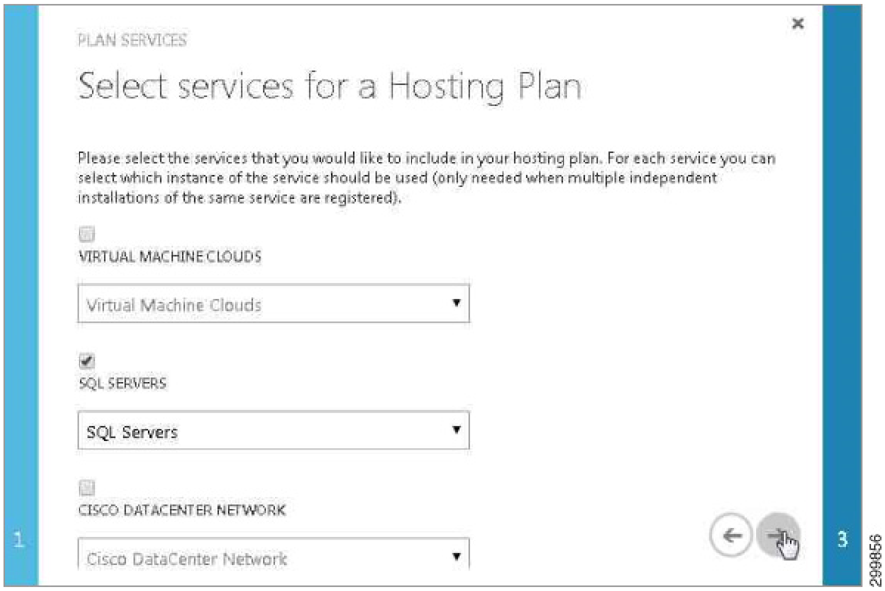
Let's Create a Hosting Plan

This wizard will walk you through the initial steps for creating a new hosting plan.

PLEASE SELECT A FRIENDLY NAME FOR YOUR PLAN

SQLaaS127Plan

Step 9 Select services for the plan (SQL Servers)



PLAN SERVICES

Select services for a Hosting Plan

Please select the services that you would like to include in your hosting plan. For each service you can select which instance of the service should be used (only needed when multiple independent installations of the same service are registered).

□ VIRTUAL MACHINE CLOUDS

Virtual Machine Clouds

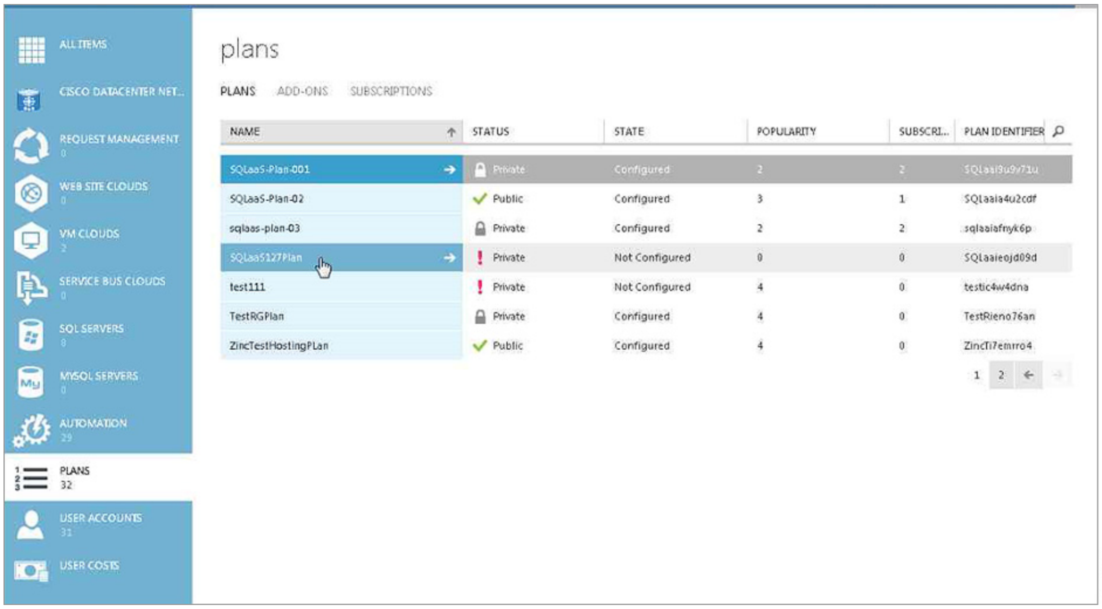
☑ SQL SERVERS

SQL Servers

□ CISCO DATACENTER NETWORK

Cisco DataCenter Network

Step 10 Verify plan creation from the Plan Windows SQL.

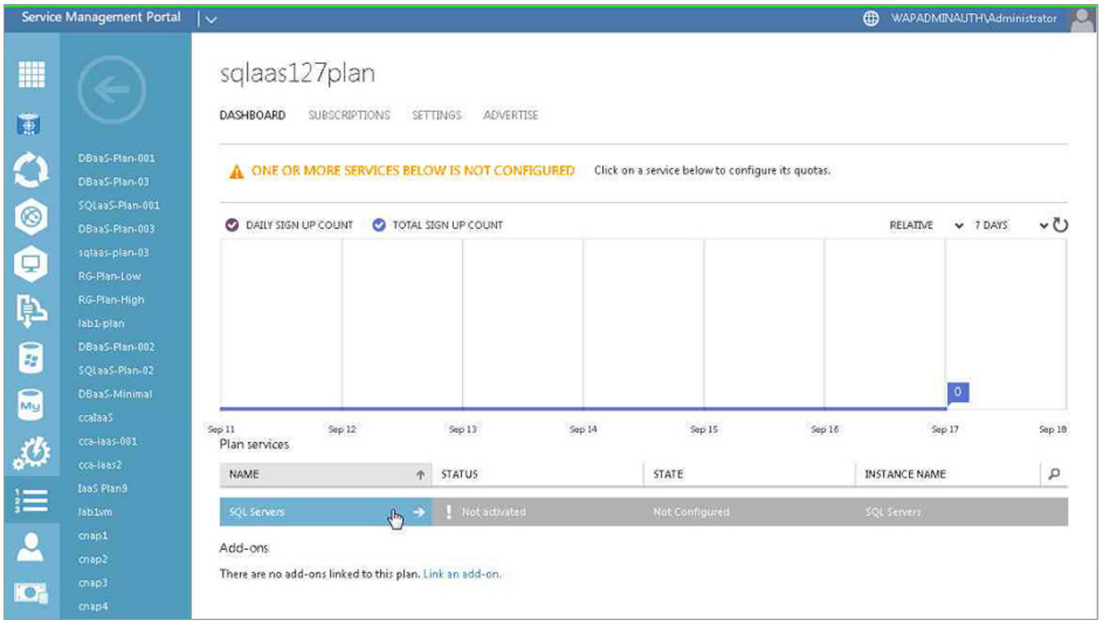


plans

NAME	STATUS	STATE	POPULARITY	SUBSCRI...	PLAN IDENTIFIER
SQLaaS-Plan-001	Private	Configured	2	2	SQLaai9u9v71u
SQLaaS-Plan-02	✓ Public	Configured	3	1	SQLaaia4u2cdf
sqlaas-plan-03	Private	Configured	2	2	sqlaaiafnyk6p
SQLaaS127Plan	! Private	Not Configured	0	0	SQLaaieojd09d
test111	! Private	Not Configured	4	0	testic4w4dna
TestRGPlan	Private	Configured	4	0	TestRieno76an
ZincTestHostingPLan	✓ Public	Configured	4	0	ZincTi7emrro4

299857

Step 11 Open the created plan and select SQL server group to add to the plan.



sqlaas127plan

ONE OR MORE SERVICES BELOW IS NOT CONFIGURED Click on a service below to configure its quotas.

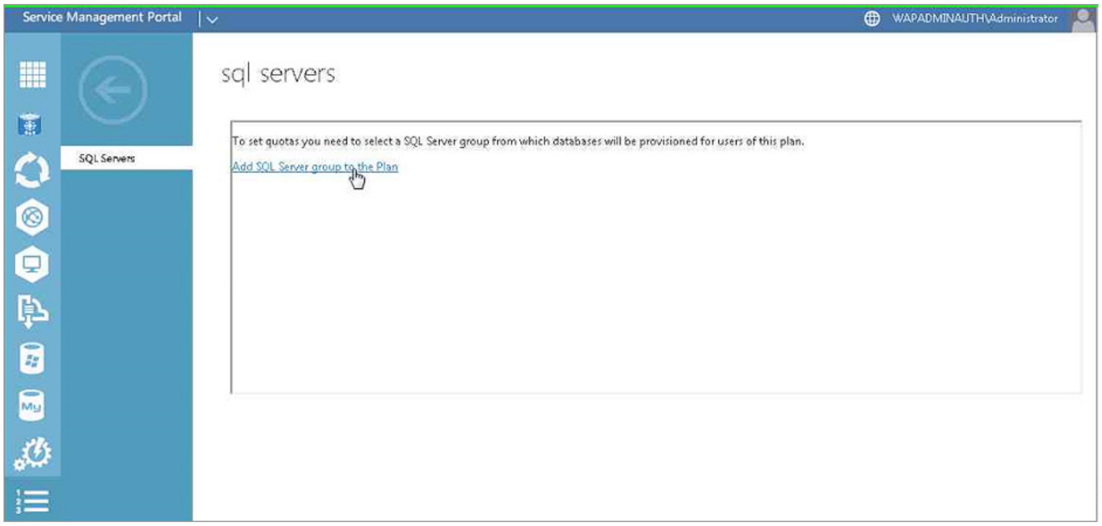
Plan services

NAME	STATUS	STATE	INSTANCE NAME
SQL Servers	! Not activated	Not Configured	SQL Servers

Add-ons

There are no add-ons linked to this plan. Link an add-on.

299858



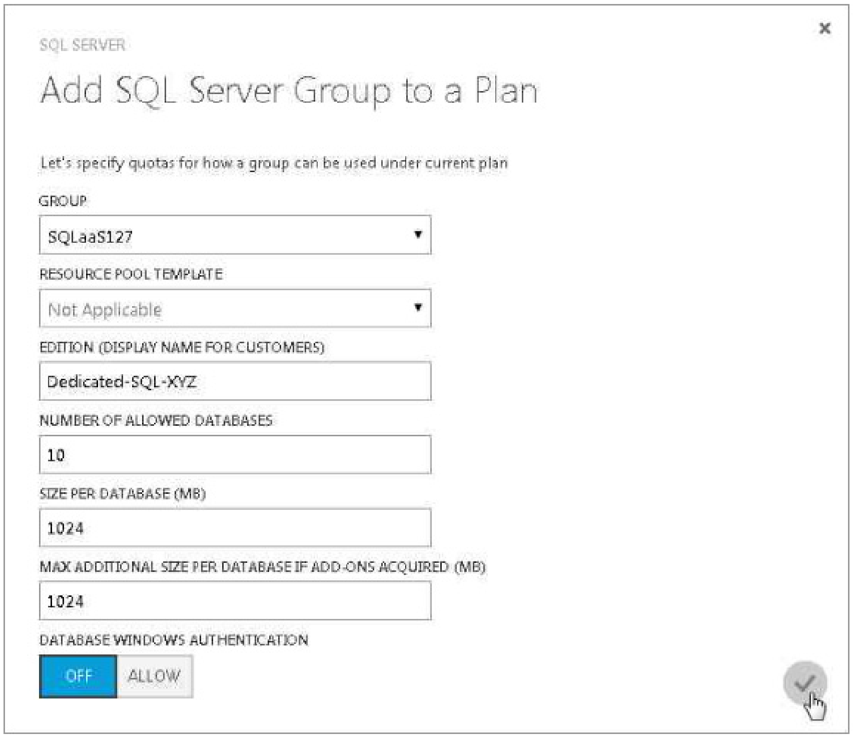
sql servers

To set quotas you need to select a SQL Server group from which databases will be provisioned for users of this plan.

Add SQL Server group to the Plan

299859

Step 12 Add SQL Server Group to the Plan. Specify resource allocation per instance; i.e., allowed databases and size of database per subscription.



SQL SERVER

Add SQL Server Group to a Plan

Let's specify quotas for how a group can be used under current plan

GROUP: SQLaaS127

RESOURCE POOL TEMPLATE: Not Applicable

EDITION (DISPLAY NAME FOR CUSTOMERS): Dedicated-SQL-XYZ

NUMBER OF ALLOWED DATABASES: 10

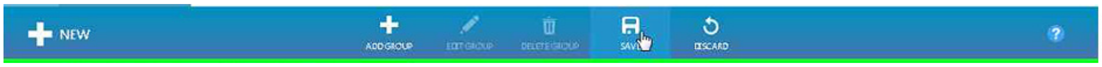
SIZE PER DATABASE (MB): 1024

MAX ADDITIONAL SIZE PER DATABASE IF ADD-ONS ACQUIRED (MB): 1024

DATABASE WINDOWS AUTHENTICATION: [✓ OFF] ALLOW

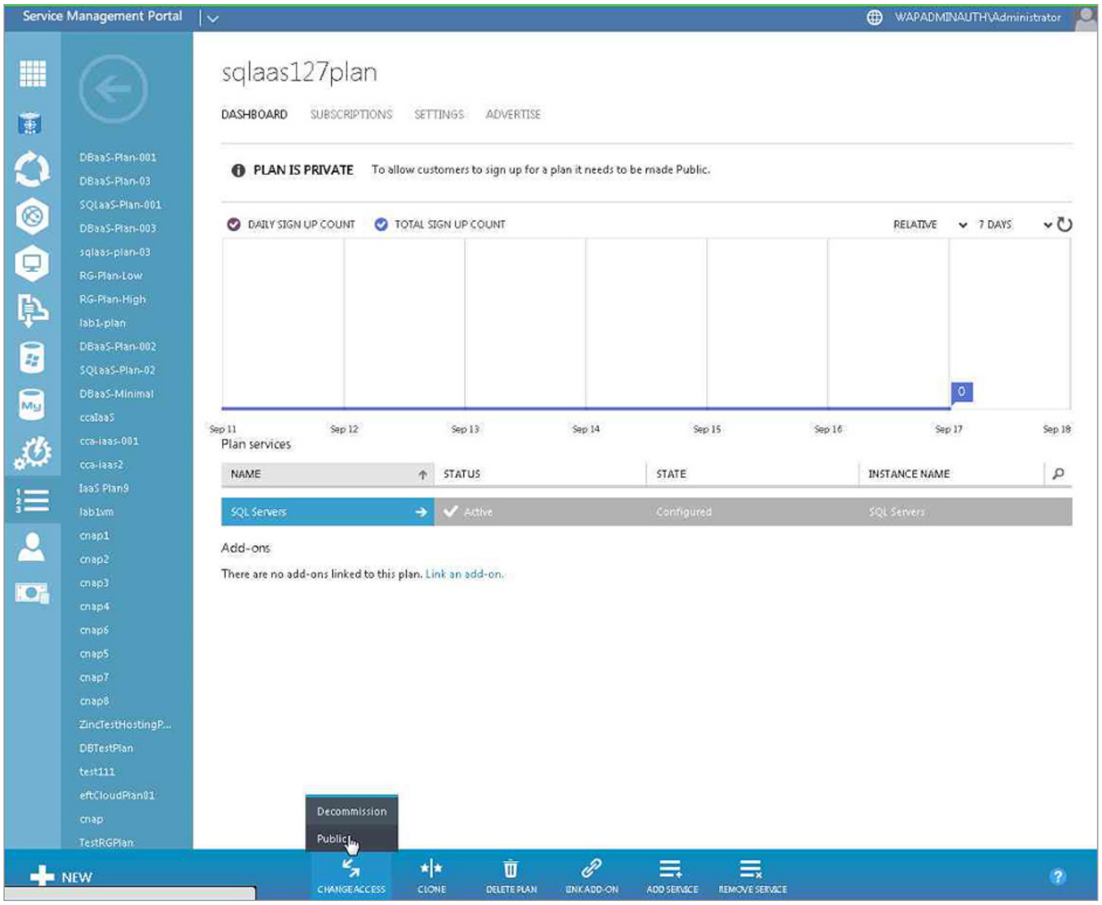
299860

Step 13 Save and verify the addition. By default, plans are created as Private.



299861

Note The plan can be updated to public status from the screen below. For purposes of this appendix, change it to a public plan so it can be viewed and selected from the Tenant Portal.



PLAN IS PRIVATE To allow customers to sign up for a plan it needs to be made Public.

Plan services

NAME	STATUS	STATE	INSTANCE NAME
SQL Servers	✓ Active	Configured	SQL Servers

Add-ons

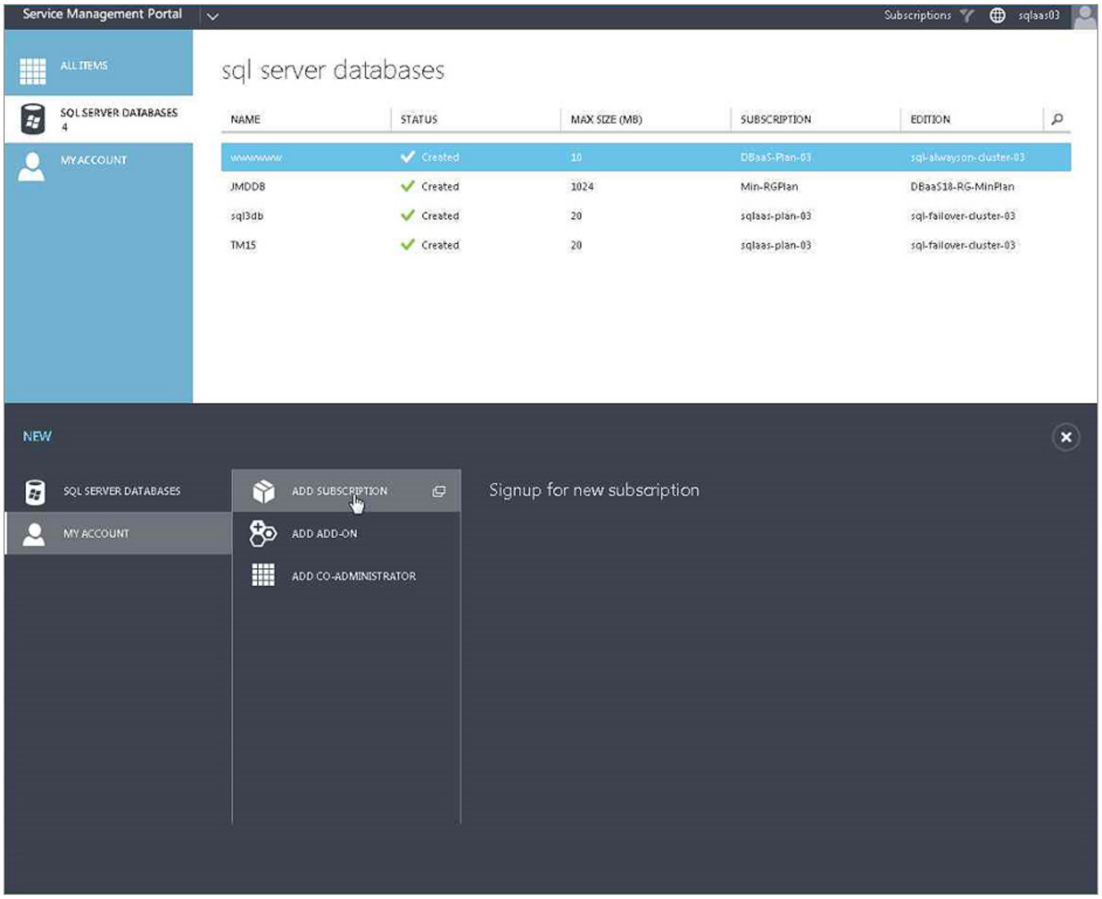
There are no add-ons linked to this plan. Link an add-on.

299862

Use the Tenant SQL Resource Provider User Interface to View Published Plan Options and Subscribe

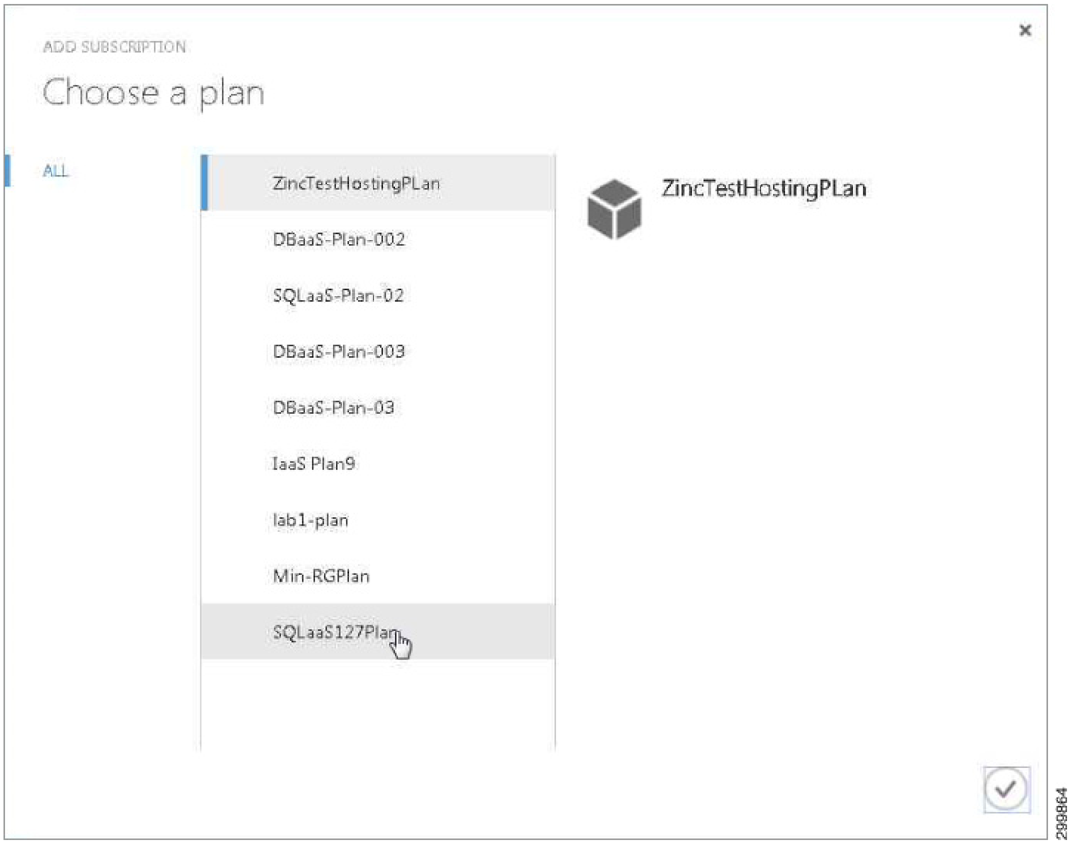
Step 1 Login to the WAP Tenant Administrator portal. Enter your username and password.

Step 2 Go to My Account and select **Add Subscription**. From the available plan(s) previously created and published through the SP Admin UI, select a plan.

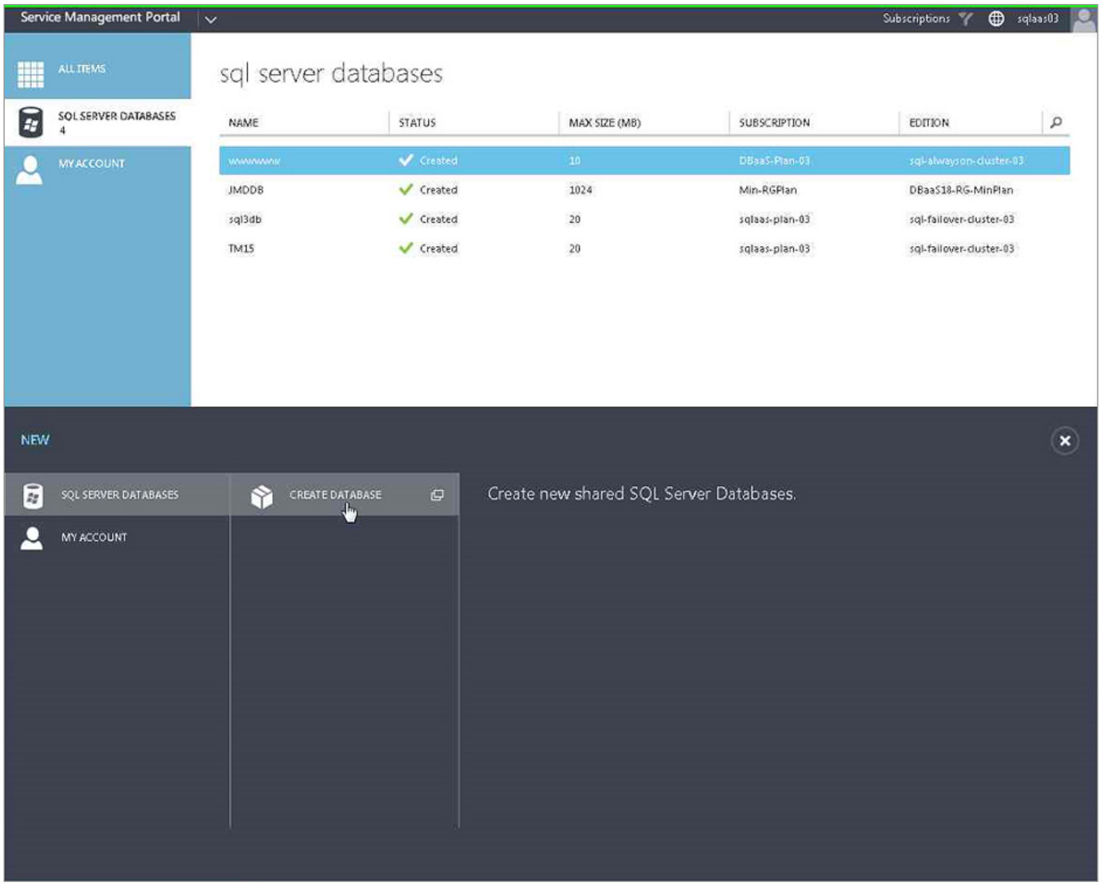


sql server databases

NAME	STATUS	MAX SIZE (MB)	SUBSCRIPTION	EDITION
wwwwwww	✓ Created	10	DBaaS-Plan-03	sql-alwayson-cluster-03
JMDDB	✓ Created	1024	Min-RGPlan	DBaaS18-RG-MinPlan
sql3db	✓ Created	20	sqlaas-plan-03	sql-failover-cluster-03
TM15	✓ Created	20	sqlaas-plan-03	sql-failover-cluster-03



Step 3 Create databases under the subscribed plan. At the bottom of screen, click **+ New** to add a database and enter the database name. If there is more than one service subscription, select from the drop-down menu to associate the new database with the proper service option.

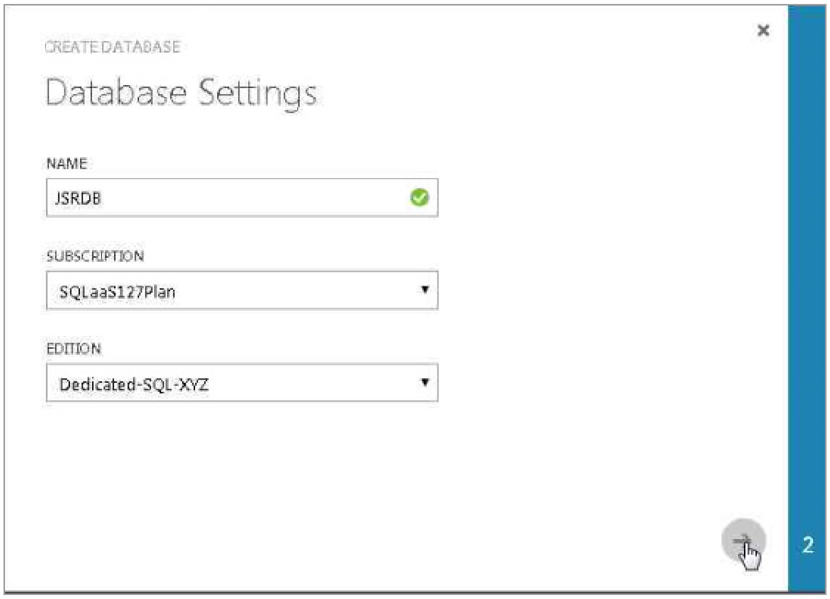


sql server databases

NAME	STATUS	MAX SIZE (MB)	SUBSCRIPTION	EDITION
wwwwww	✓ Created	10	DBaaS-Plan-03	sql-alwayson-cluster-03
JMDDB	✓ Created	1024	Min-RGPlan	DBaaS18-RG-MinPlan
sql3db	✓ Created	20	sqlaas-plan-03	sql-failover-cluster-03
TM15	✓ Created	20	sqlaas-plan-03	sql-failover-cluster-03

Create new shared SQL Server Databases.

299865



Database Settings

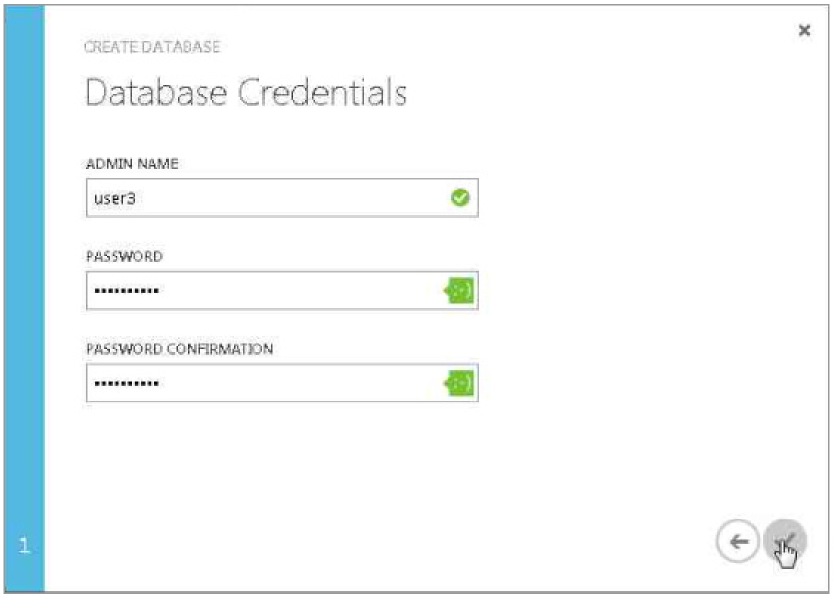
NAME: JSRDB

SUBSCRIPTION: SQLaaS127Plan

EDITION: Dedicated-SQL-XYZ

299866

Step 4 Specify the username/password credentials for database user access.



Database Credentials

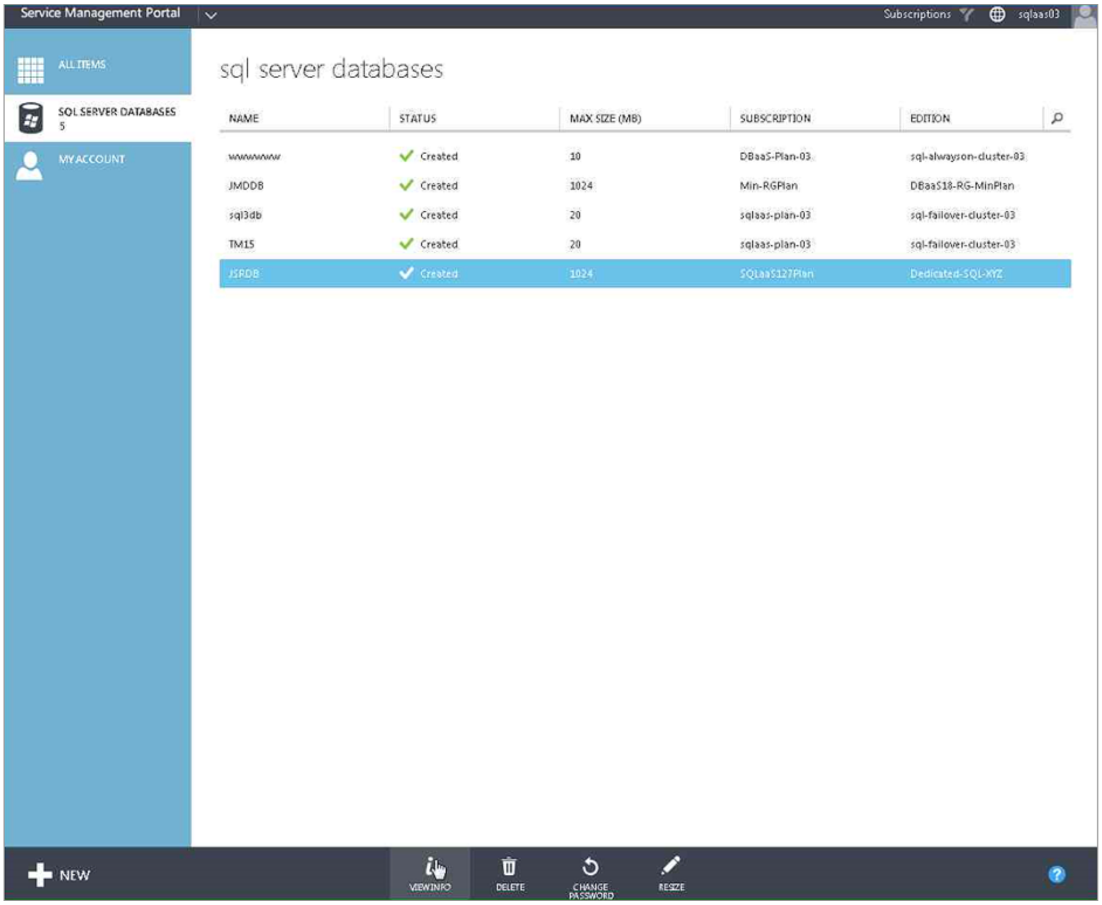
ADMIN NAME: user3

PASSWORD: ••••••••••

PASSWORD CONFIRMATION: ••••••••••

299867

Step 5 Once created, the tenant is able to view their existing databases, including the one just created in the step above.

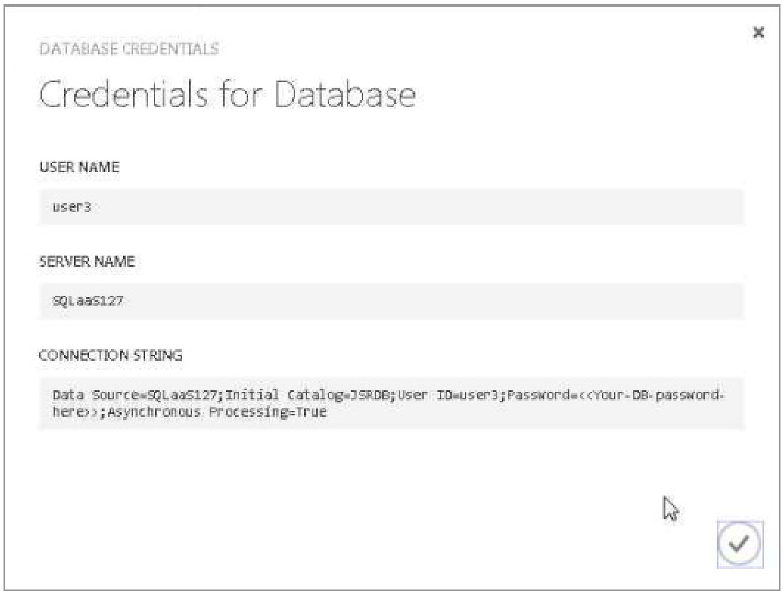


sql server databases

NAME	STATUS	MAX SIZE (MB)	SUBSCRIPTION	EDITION
wwwwww	✓ Created	10	DBaaS-Plan-03	sql-alwayson-cluster-03
JMDDB	✓ Created	1024	Min-RGPlan	DBaaS18-RG-MinPlan
sql3db	✓ Created	20	sqlaas-plan-03	sql-failover-cluster-03
TM15	✓ Created	20	sqlaas-plan-03	sql-failover-cluster-03
JSRDB	✓ Created	1024	SQLaaS127Plan	Dedicated-SQL-XYZ

299868

Step 6 By selecting **View Info** (bottom of screen above), the tenant is able to view the defined SQL Server database credentials. These credentials may be required as part of front-end operations for database connections.



DATABASE CREDENTIALS

Credentials for Database

USER NAME

user3

SERVER NAME

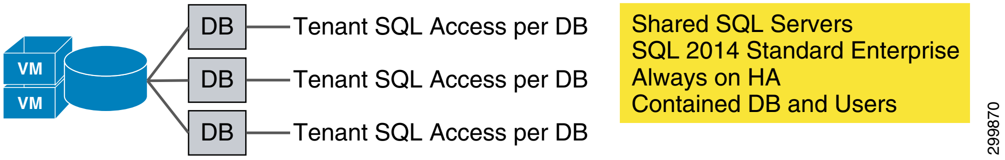
SQLaaS127

CONNECTION STRING

```
Data Source=SQLaaS127;Initial Catalog=JSRDB;User ID=user3;Password=<<Your-DB-password-
here>>;Asynchronous Processing=True
```

Shared Service Deployment Mode—Always-on Cluster Redundancy Option and DBaaS Instance per-Tenant on Multi-tenant SQL Server(s)

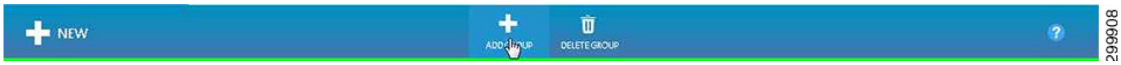
Figure B-2 Always-on Cluster Redundancy Option



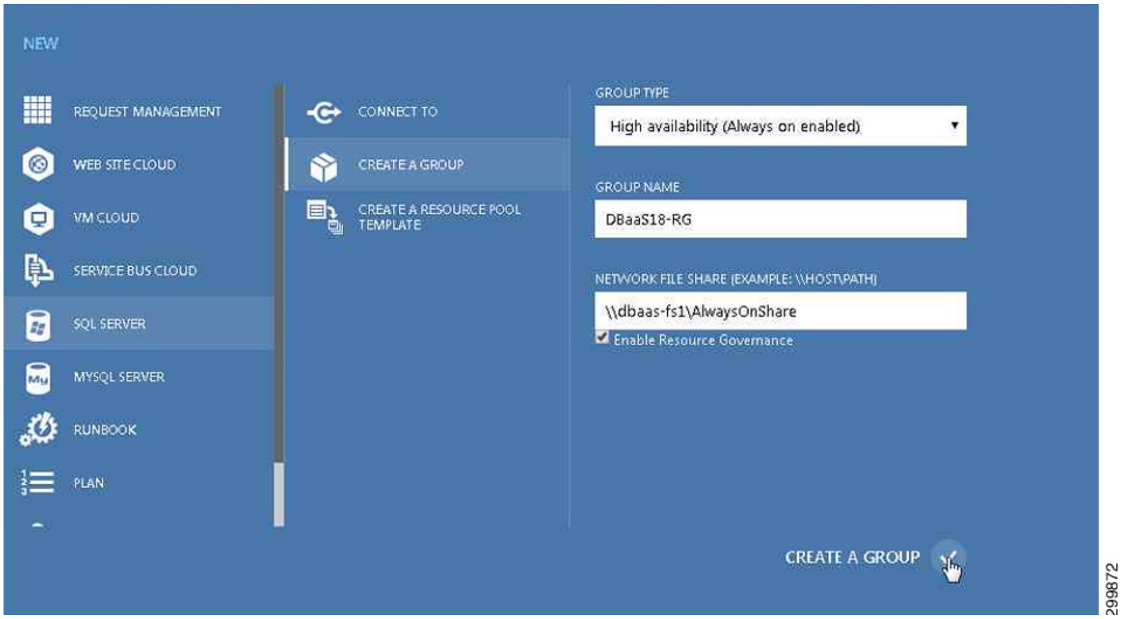
Use the Administrator SQL Resource Provider User Interface to Create DBaaS Plan and Resource Allocation

Step 1 On the WAP Admin Portal, log in with your Active Directory user ID and password.

Step 2 Open the SQL Server RP tab. At the bottom of screen, click **+ New** to add a group.



Step 3 Enter the Group Name and specify whether it is standalone or HA. In this example, HA selection is Always on (enabled).

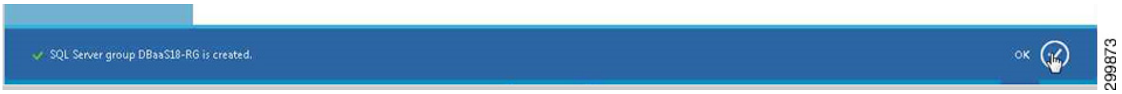


GROUP TYPE: High availability (Always on enabled)

GROUP NAME: DBaaS18-RG

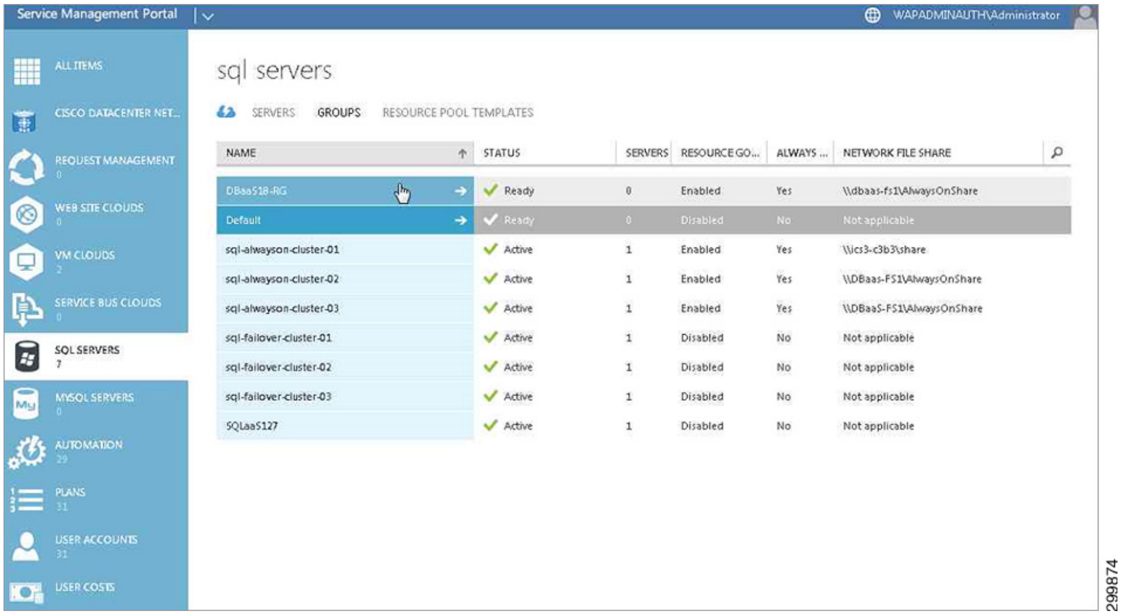
NETWORK FILE SHARE (EXAMPLE: \\HOST\PATH): \\dbaas-fs1\AlwaysOnShare

☑ Enable Resource Governance



✓ SQL Server group DBaaS18-RG is created.

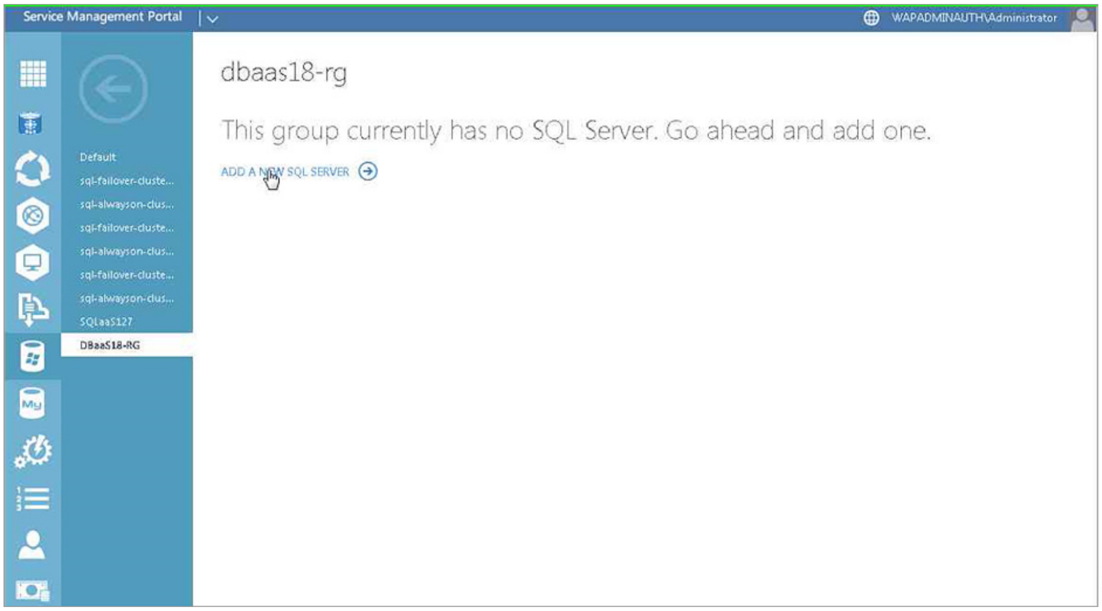
Step 4 Check the SQL Server Group View to verify that the Group is created when done.



sql servers

NAME	STATUS	SERVERS	RESOURCE GO...	ALWAYS ...	NETWORK FILE SHARE
DBaaS18-RG	✓ Ready	0	Enabled	Yes	\\dbaas-fs1\AlwaysOnShare
Default	✓ Ready	0	Disabled	No	Not applicable
sql-alwayson-cluster-01	✓ Active	1	Enabled	Yes	\\ics3-c3b3\share
sql-alwayson-cluster-02	✓ Active	1	Enabled	Yes	\\DBaas-FS1\AlwaysOnShare
sql-alwayson-cluster-03	✓ Active	1	Enabled	Yes	\\DBaaS-FS1\AlwaysOnShare
sql-failover-cluster-01	✓ Active	1	Disabled	No	Not applicable
sql-failover-cluster-02	✓ Active	1	Disabled	No	Not applicable
sql-failover-cluster-03	✓ Active	1	Disabled	No	Not applicable
SQLaaS127	✓ Active	1	Disabled	No	Not applicable

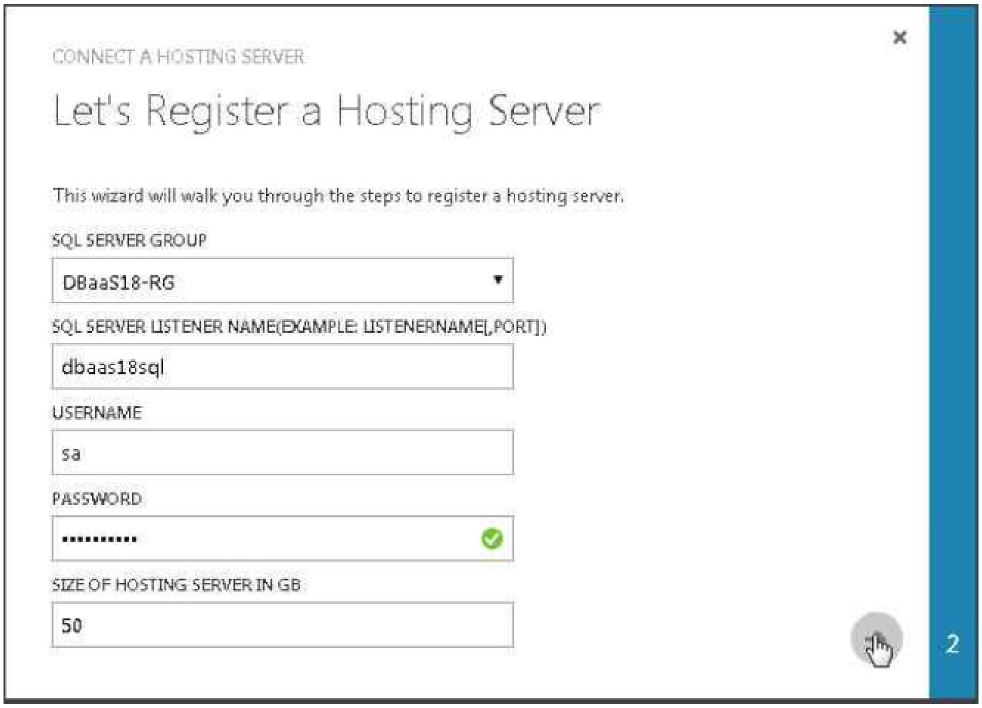
Step 5 Add an SQL Server to the new group.



dbaas18-rg

This group currently has no SQL Server. Go ahead and add one.

Step 6 Specify the Server Name, User Name/Password, and Instance Disk Size Allocation.



CONNECT A HOSTING SERVER

Let's Register a Hosting Server

This wizard will walk you through the steps to register a hosting server.

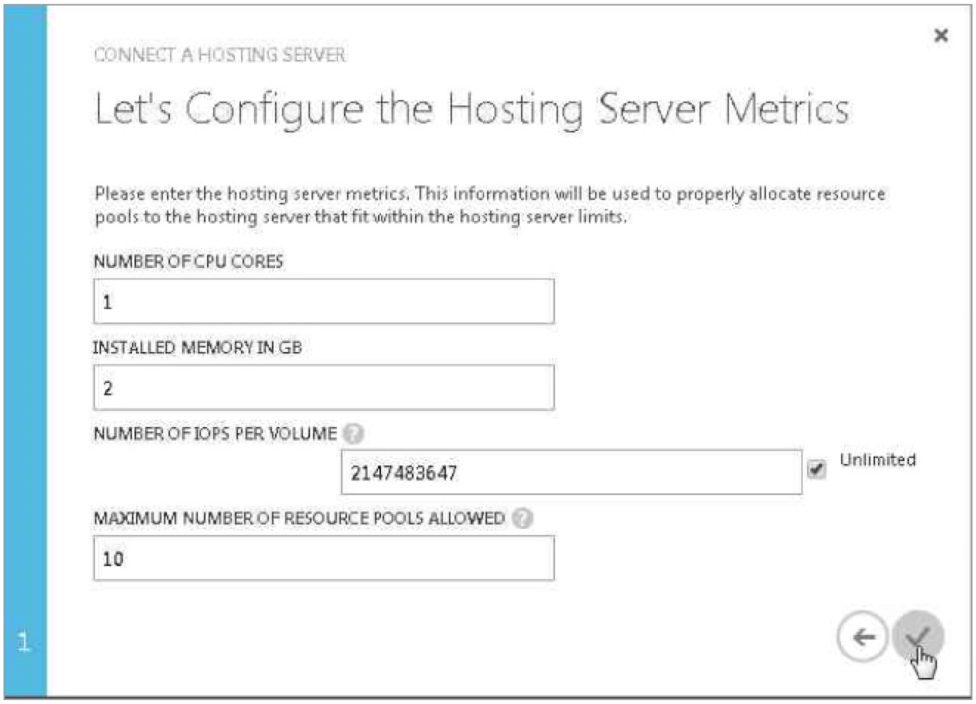
SQL SERVER GROUP: DBaaS18-RG

SQL SERVER LISTENER NAME(EXAMPLE: LISTENERNAME[,PORT]): dbaas18sql

USERNAME: sa

PASSWORD: ••••••••••

SIZE OF HOSTING SERVER IN GB: 50



CONNECT A HOSTING SERVER

Let's Configure the Hosting Server Metrics

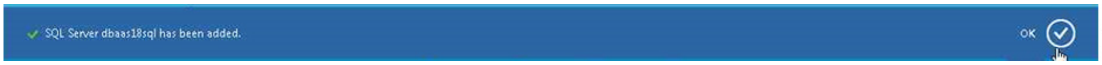
Please enter the hosting server metrics. This information will be used to properly allocate resource pools to the hosting server that fit within the hosting server limits.

NUMBER OF CPU CORES: 1

INSTALLED MEMORY IN GB: 2

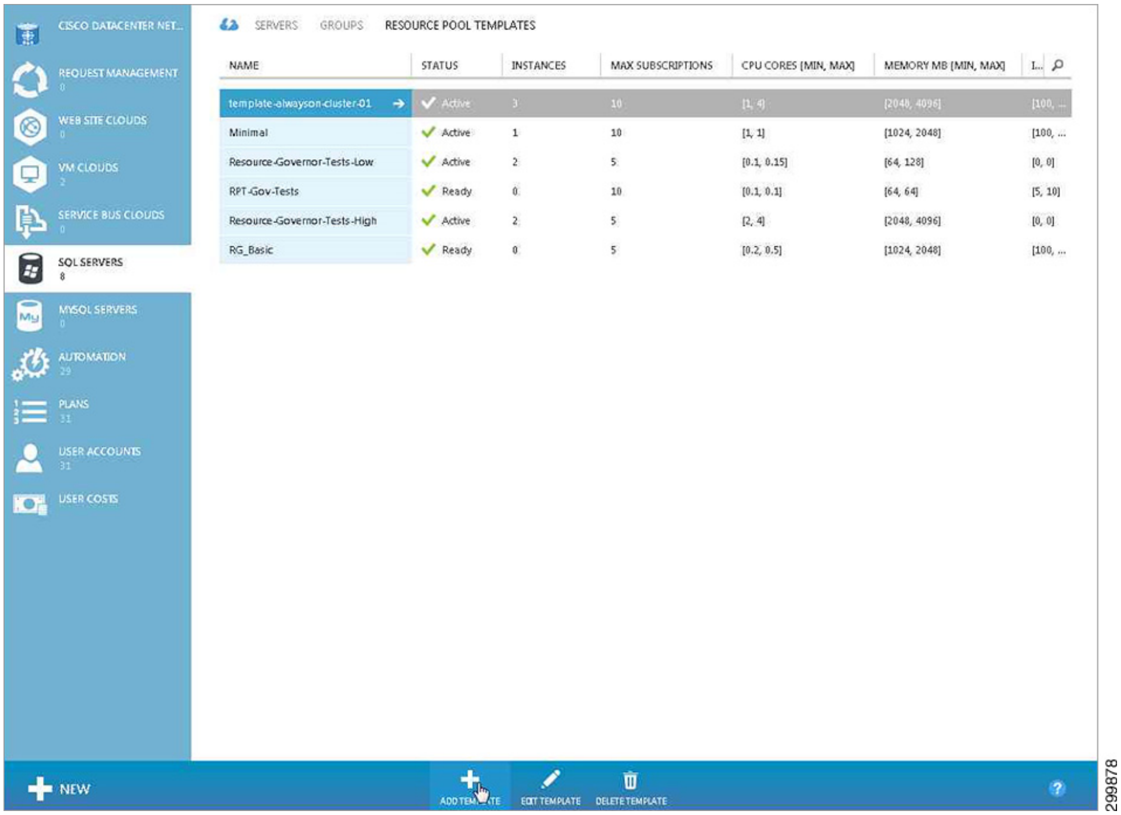
NUMBER OF IOPS PER VOLUME: 2147483647 ☑ Unlimited

MAXIMUM NUMBER OF RESOURCE POOLS ALLOWED: 10



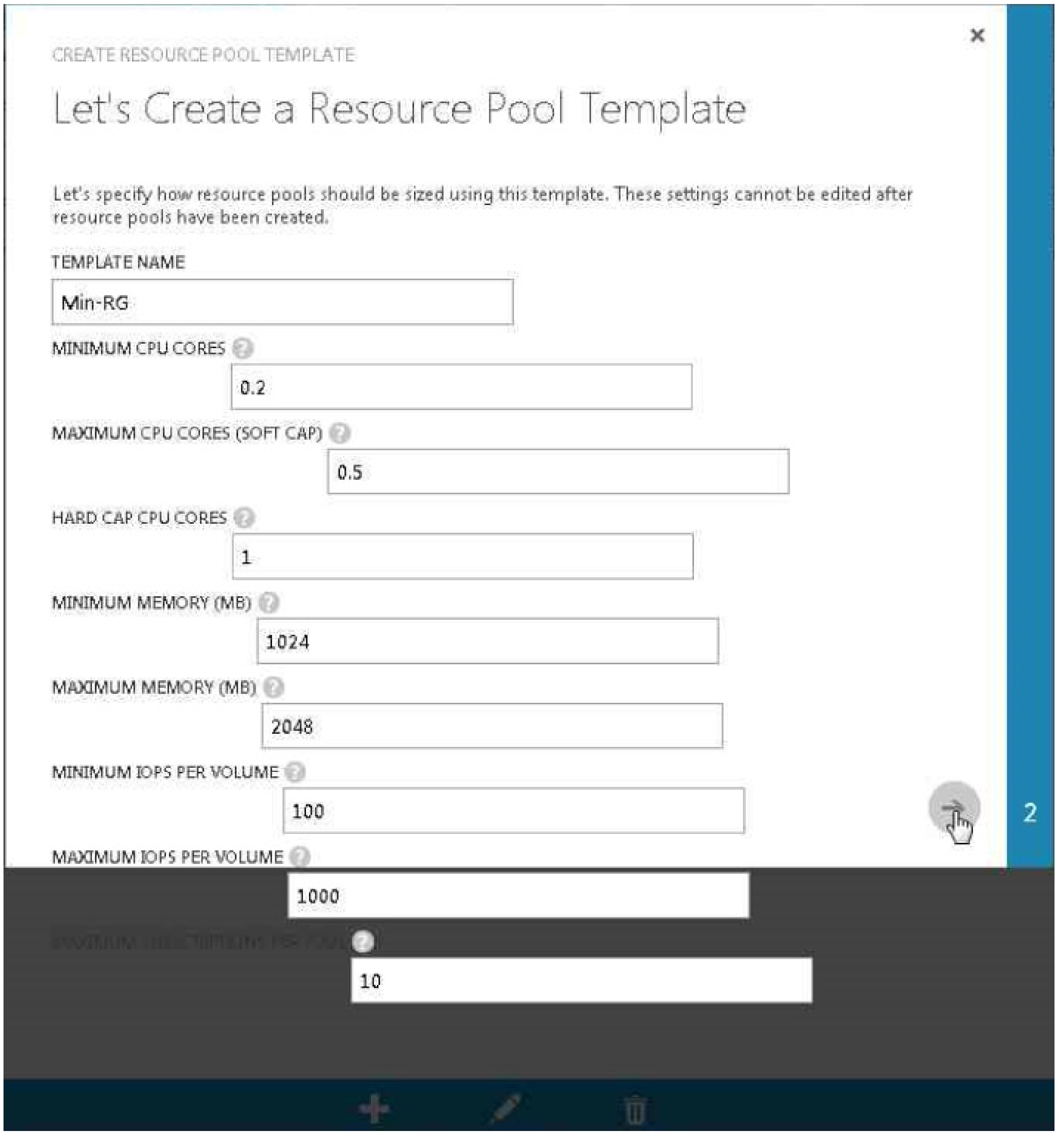
✓ SQL Server dbaas18sql has been added.

Step 7 Create a New Resource Pool Template by clicking **+ New (Add Template)**.



NAME	STATUS	INSTANCES	MAX SUBSCRIPTIONS	CPU CORES [MIN, MAX]	MEMORY MB [MIN, MAX]	I...
template-alwayson-cluster-01	✓ Active	3	10	[1, 4]	[2048, 4096]	[100, ...
Minimal	✓ Active	1	10	[1, 1]	[1024, 2048]	[100, ...
Resource-Governor-Tests-Low	✓ Active	2	5	[0.1, 0.15]	[64, 128]	[0, 0]
RPT-Gov-Tests	✓ Ready	0	10	[0.1, 0.1]	[64, 64]	[5, 10]
Resource-Governor-Tests-High	✓ Active	2	5	[2, 4]	[2048, 4096]	[0, 0]
RG_Basic	✓ Ready	0	5	[0.2, 0.5]	[1024, 2048]	[100, ...

Step 8 In the resulting form, specify the template name and define the resource allocation.



CREATE RESOURCE POOL TEMPLATE

Let's Create a Resource Pool Template

Let's specify how resource pools should be sized using this template. These settings cannot be edited after resource pools have been created.

TEMPLATE NAME: Min-RG

MINIMUM CPU CORES: 0.2

MAXIMUM CPU CORES (SOFT CAP): 0.5

HARD CAP CPU CORES: 1

MINIMUM MEMORY (MB): 1024

MAXIMUM MEMORY (MB): 2048

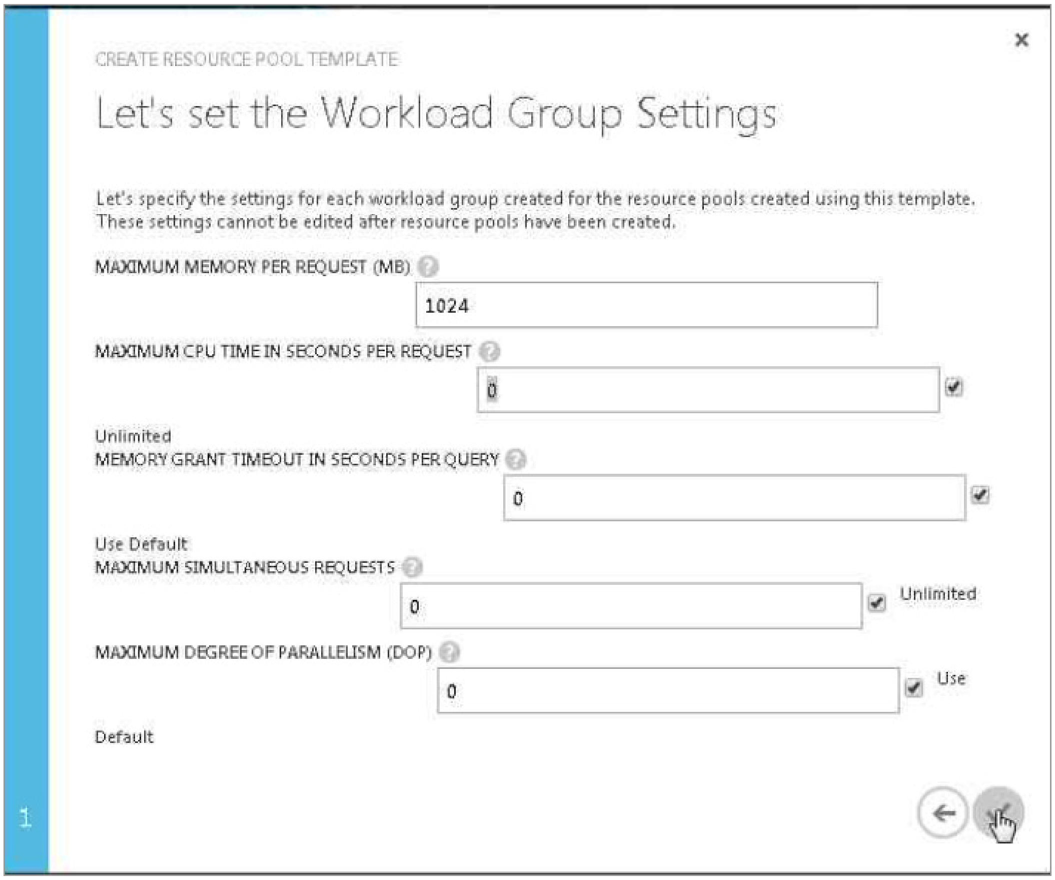
MINIMUM IOPS PER VOLUME: 100

MAXIMUM IOPS PER VOLUME: 1000

MAXIMUM SUBSCRIPTIONS PER POOL: 10

Step 9 Set the Workload Group settings for the new template

Note The maximum memory **must** be the same as the minimum assigned memory previously defined in the resource allocation parameters.



CREATE RESOURCE POOL TEMPLATE

Let's set the Workload Group Settings

Let's specify the settings for each workload group created for the resource pools created using this template. These settings cannot be edited after resource pools have been created.

MAXIMUM MEMORY PER REQUEST (MB): 1024

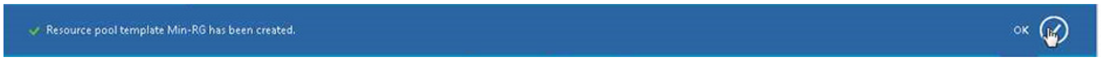
MAXIMUM CPU TIME IN SECONDS PER REQUEST: 0 ☑ Unlimited

MEMORY GRANT TIMEOUT IN SECONDS PER QUERY: 0 ☑ Use Default

MAXIMUM SIMULTANEOUS REQUESTS: 0 ☑ Unlimited

MAXIMUM DEGREE OF PARALLELISM (DOP): 0 ☑ Use Default

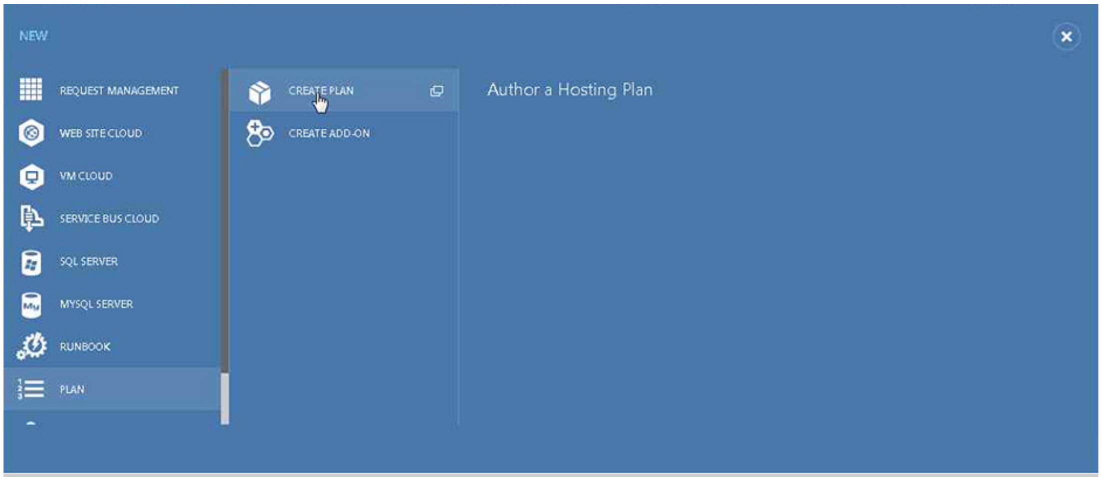
299880



✓ Resource pool template Min-RG has been created.

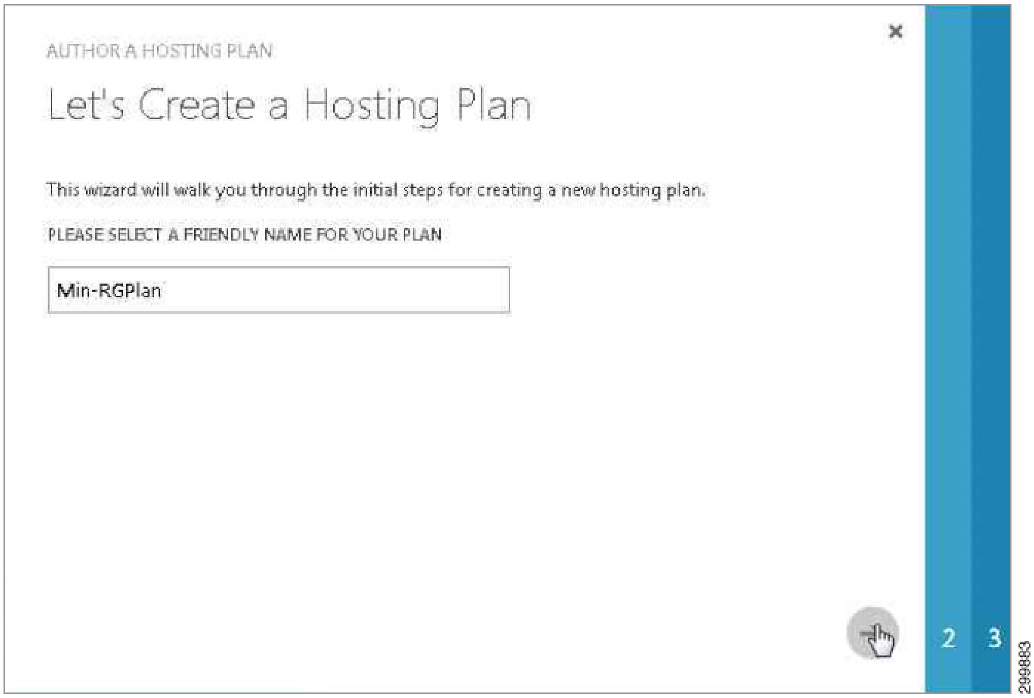
299881

Step 10 Create a new plan.



299882

Step 11 In the plan creation view, specify the plan name.



AUTHOR A HOSTING PLAN

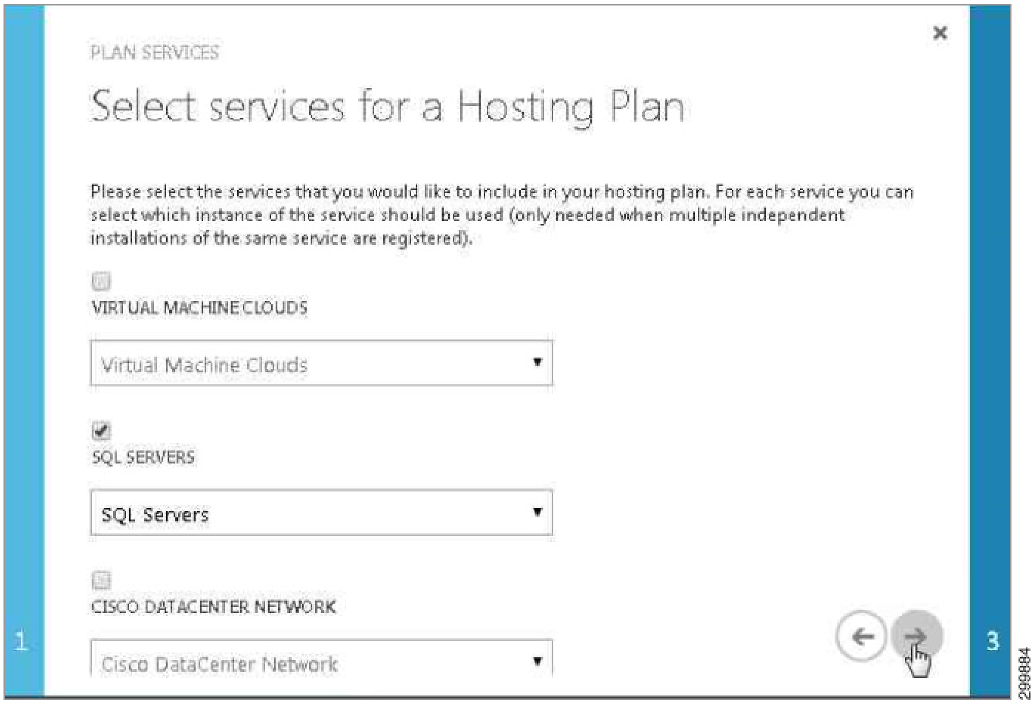
Let's Create a Hosting Plan

This wizard will walk you through the initial steps for creating a new hosting plan.

PLEASE SELECT A FRIENDLY NAME FOR YOUR PLAN

Min-RGPlan

Step 12 Select the applicable services (a function of the resource providers previously registered to WAP for the cloud).



PLAN SERVICES

Select services for a Hosting Plan

Please select the services that you would like to include in your hosting plan. For each service you can select which instance of the service should be used (only needed when multiple independent installations of the same service are registered).

□ VIRTUAL MACHINE CLOUDS

Virtual Machine Clouds ▾

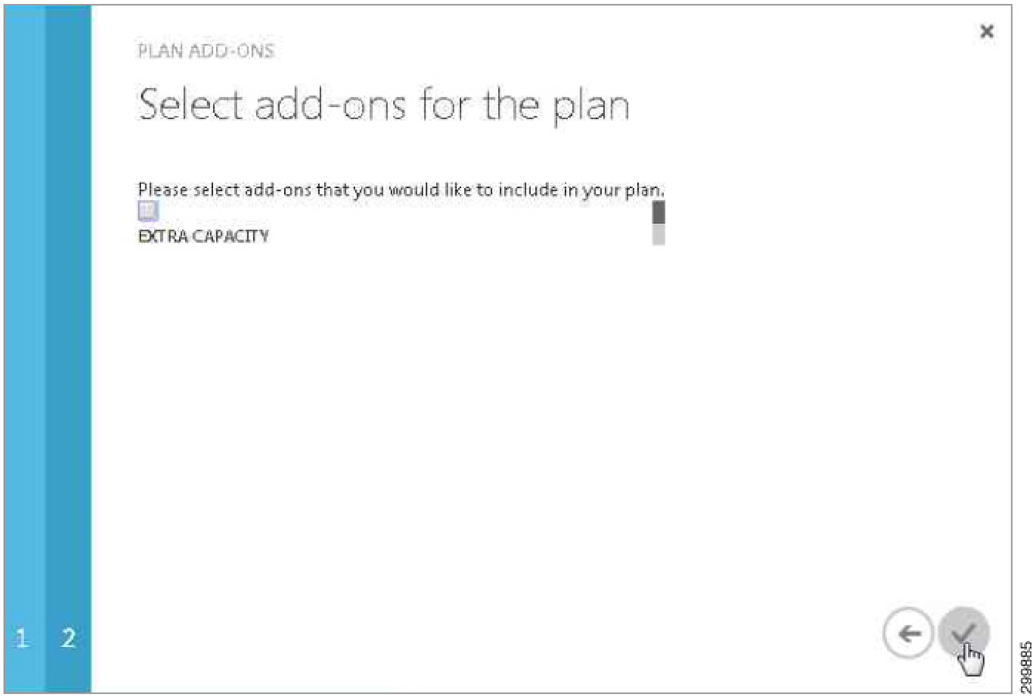
☑ SQL SERVERS

SQL Servers ▾

□ CISCO DATACENTER NETWORK

Cisco DataCenter Network ▾

If add-on service options are defined (extra capacity in this example), they may be offered for inclusion in this new plan.

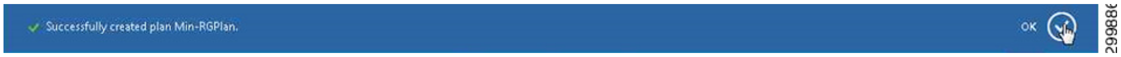


PLAN ADD-ONS

Select add-ons for the plan

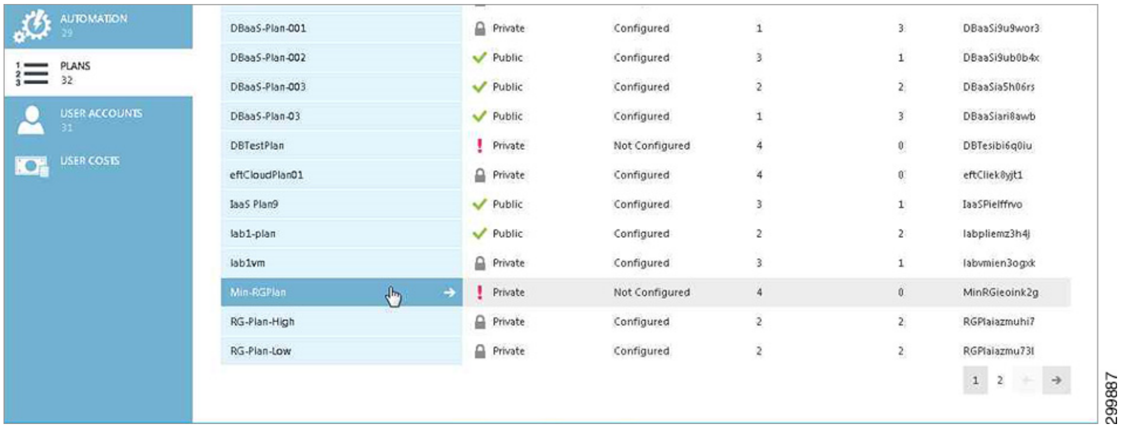
Please select add-ons that you would like to include in your plan.

□ EXTRA CAPACITY



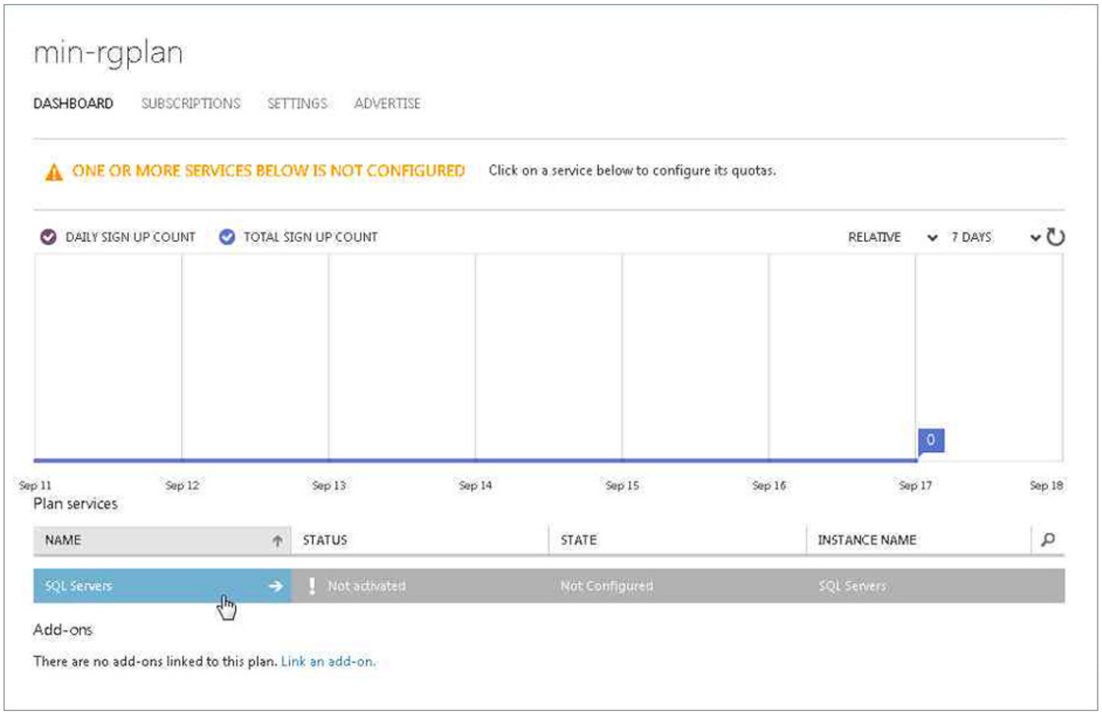
✓ Successfully created plan Min-RGPlan.

Step 13 View the list of defined plans to verify that the new plan is included.



DBaaS-Plan-001	🔒 Private	Configured	1	3	DBaaSi9u9wor3
DBaaS-Plan-002	✓ Public	Configured	3	1	DBaaSi9ub0b4x
DBaaS-Plan-003	✓ Public	Configured	2	2	DBaaSia5h06rs
DBaaS-Plan-03	✓ Public	Configured	1	3	DBaaSiari8awb
DBTestPlan	! Private	Not Configured	4	0	DBTesibi6q0iu
eftCloudPlan01	🔒 Private	Configured	4	0	eftCliek8yjt1
IaaS Plan9	✓ Public	Configured	3	1	IaaSPielffrvo
lab1-plan	✓ Public	Configured	2	2	labpliemz3h4j
lab1vm	🔒 Private	Configured	3	1	labvmien3ogxk
Min-RGPlan	! Private	Not Configured	4	0	MinRGieoink2g
RG-Plan-High	🔒 Private	Configured	2	2	RGPlaiazmuhi7
RG-Plan-Low	🔒 Private	Configured	2	2	RGPlaiazmu73l

Step 14 Configure service quotas. Click the new plan (**Min-RGPlan**) from the list in the view above to view its dashboard listing the available services.



ONE OR MORE SERVICES BELOW IS NOT CONFIGURED Click on a service below to configure its quotas.

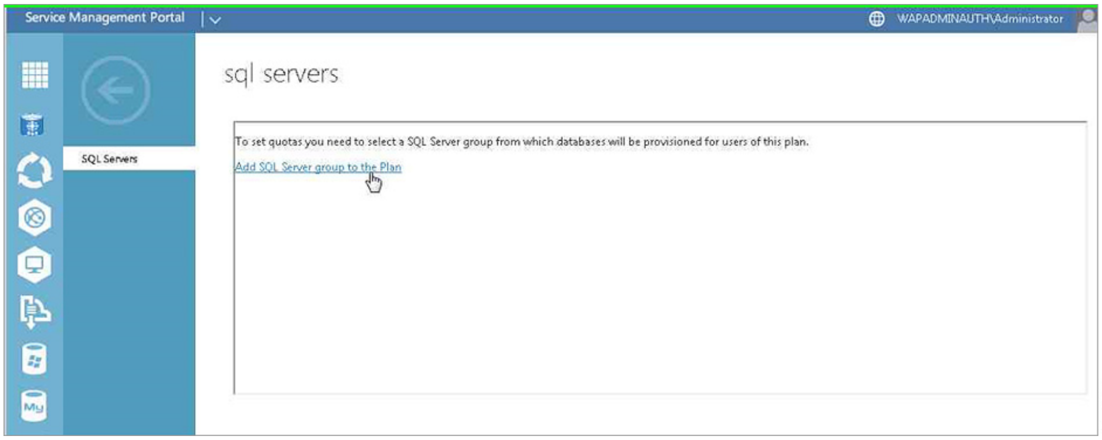
Plan services

NAME	STATUS	STATE	INSTANCE NAME
SQL Servers	! Not activated	Not Configured	SQL Servers

Add-ons

There are no add-ons linked to this plan. Link an add-on.

Step 15 Click the **SQL Servers** service to begin configuring quotas for the servers associated with this DBaaS plan on which the databases will be created per tenant request.

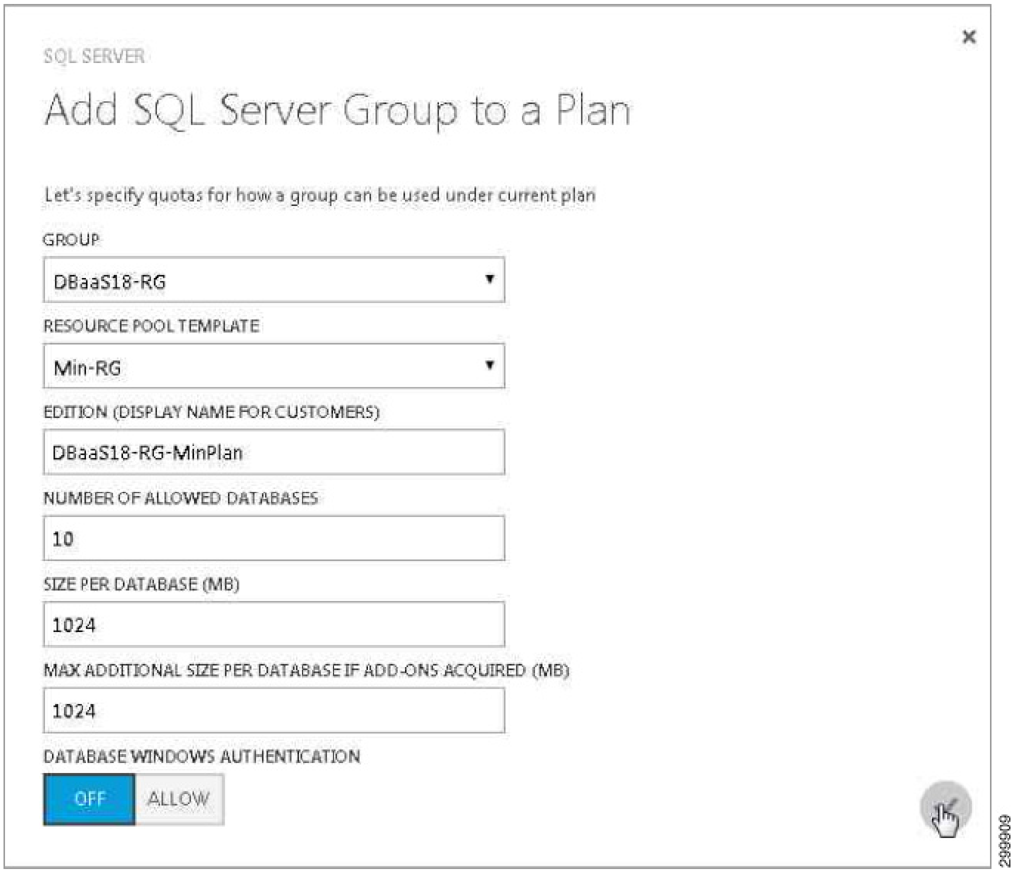


sql servers

To set quotas you need to select a SQL Server group from which databases will be provisioned for users of this plan.

Add SQL Server group to the Plan

Step 16 Add the SQL Server Group to the plan with the desired quotas. These include the number of allowed databases and size per database, per tenant subscription.



SQL SERVER

Add SQL Server Group to a Plan

Let's specify quotas for how a group can be used under current plan

GROUP: DBaaS18-RG

RESOURCE POOL TEMPLATE: Min-RG

EDITION (DISPLAY NAME FOR CUSTOMERS): DBaaS18-RG-MinPlan

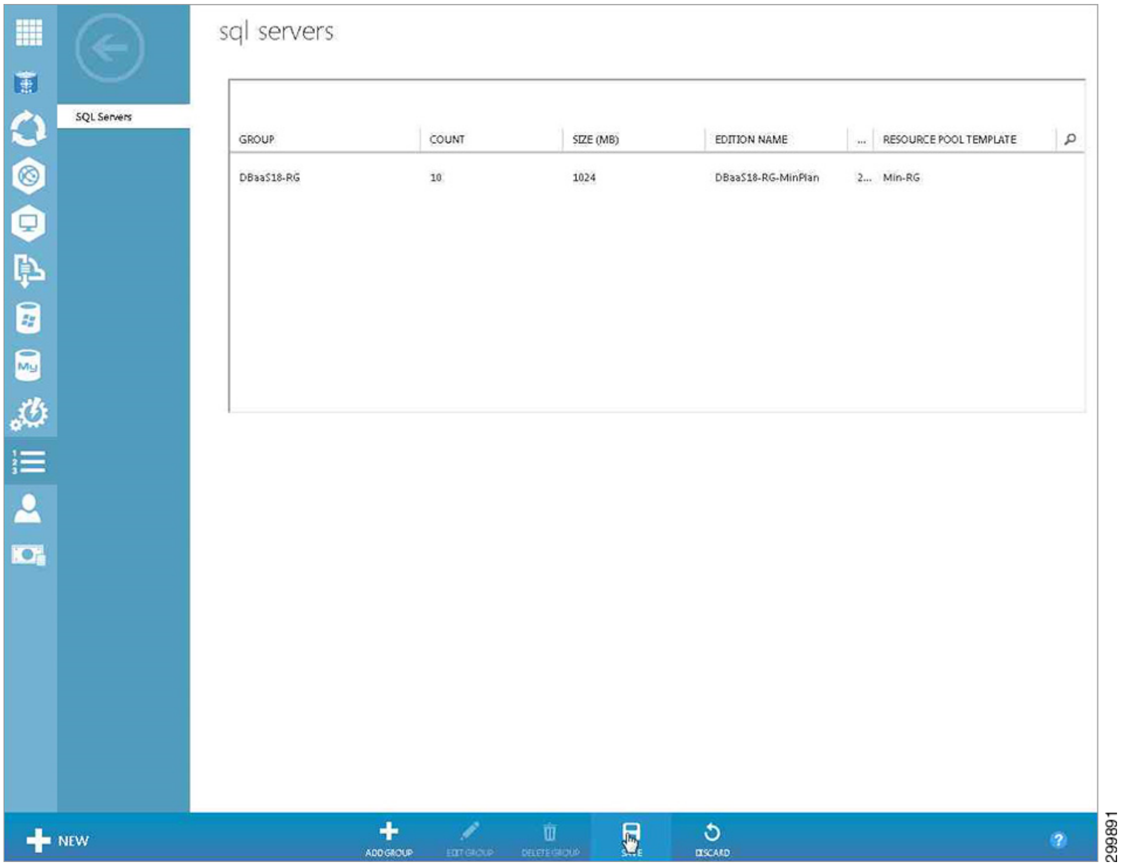
NUMBER OF ALLOWED DATABASES: 10

SIZE PER DATABASE (MB): 1024

MAX ADDITIONAL SIZE PER DATABASE IF ADD-ONS ACQUIRED (MB): 1024

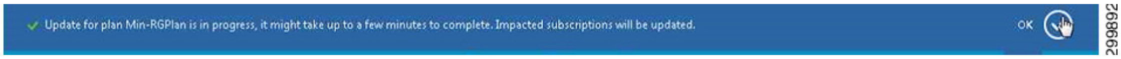
DATABASE WINDOWS AUTHENTICATION: [✓ OFF] ALLOW

Step 17 From the SQL Server view within the plan, see the list of defined groups to verify that the newly defined group is listed.



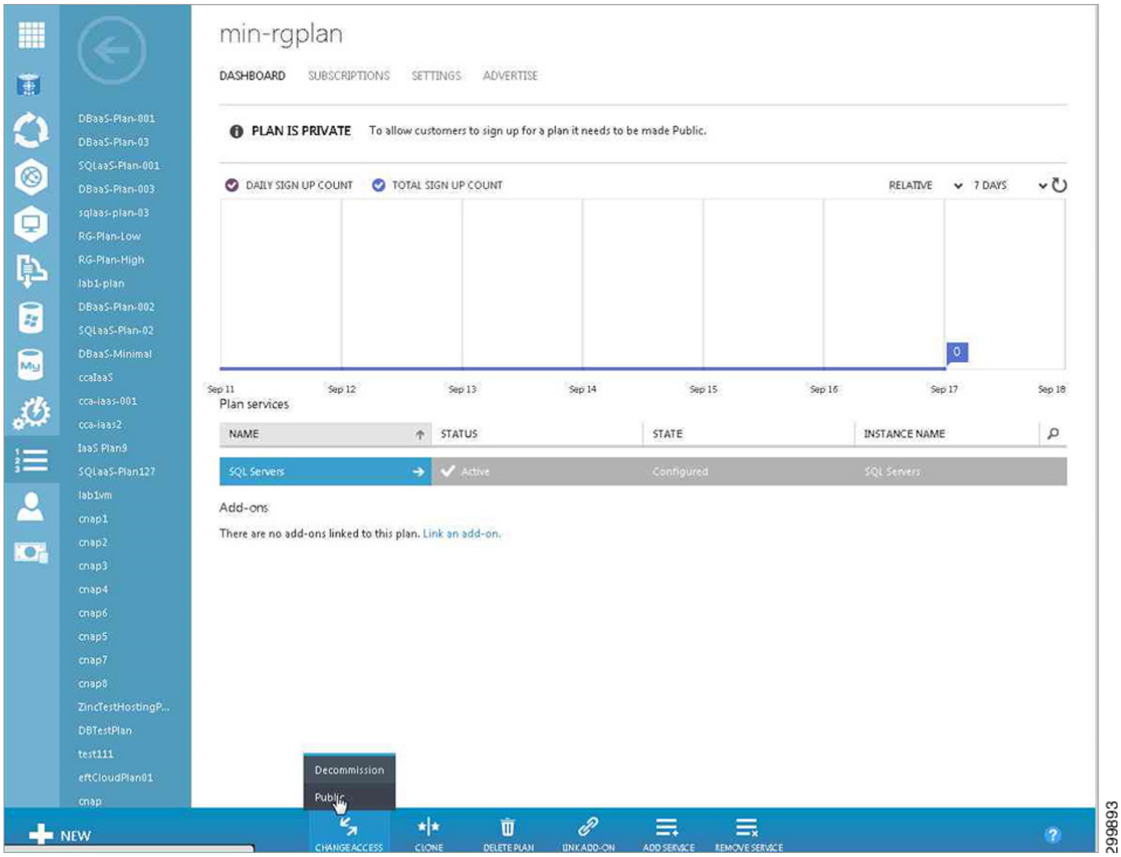
sql servers

GROUP	COUNT	SIZE (MB)	EDITION NAME	...	RESOURCE POOL TEMPLATE
DBaaS18-RG	10	1024	DBaaS18-RG-MinPlan	2...	Min-RG



Update for plan Min-RGPlan is in progress, it might take up to a few minutes to complete. Impacted subscriptions will be updated.

Step 18 Select the newly created plan from the plan list to change the plan from the default “private” to “public” so that it is selectable from the tenant service management portal.



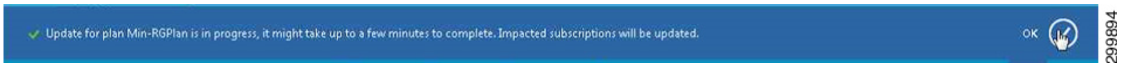
PLAN IS PRIVATE To allow customers to sign up for a plan it needs to be made Public.

Plan services

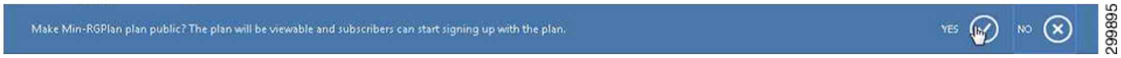
NAME	STATUS	STATE	INSTANCE NAME
SQL Servers	✓ Active	Configured	SQL Servers

Add-ons

There are no add-ons linked to this plan. Link an add-on.



✓ Update for plan Min-RGPlan is in progress, it might take up to a few minutes to complete. Impacted subscriptions will be updated.

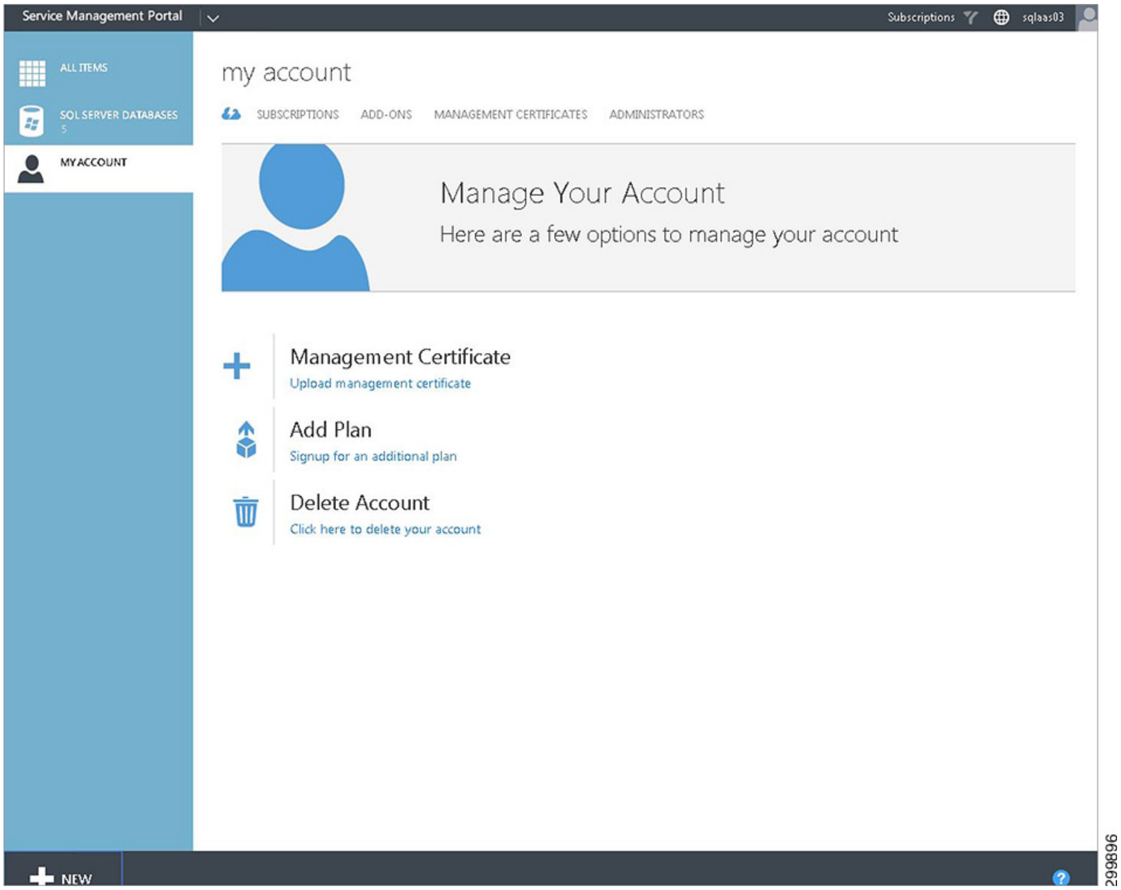


Make Min-RGPlan plan public? The plan will be viewable and subscribers can start signing up with the plan.

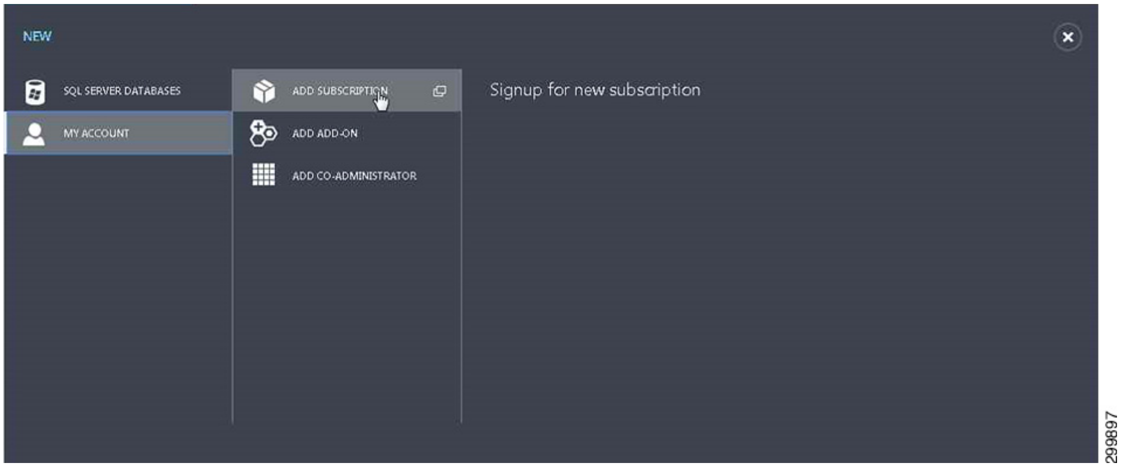
Use the Tenant SQL Resource Provider User Interface to Create DBaaS Plan and Resource Allocation

Step 1 Login to the WAP Tenant Administrator portal. Enter your username/password.

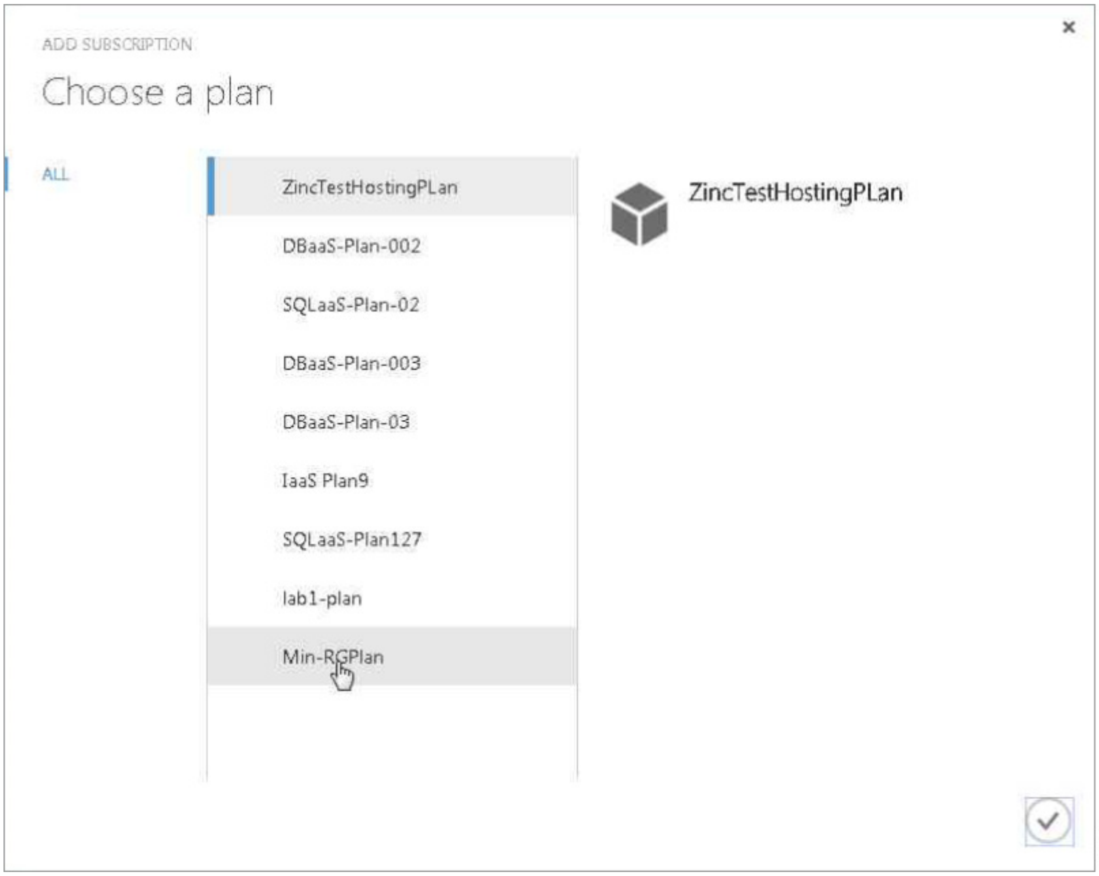
Step 2 Subscribe to a plan. Go to My Account and select **Add Plan**.



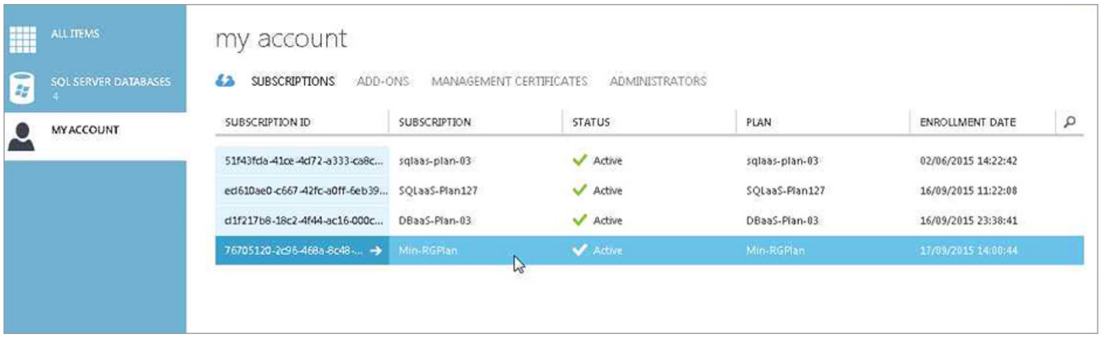
Alternatively, **+New** may be used to add a subscription.



Step 3 From the resulting list of available plan(s) previously created and published through the SP Admin UI, select a shared DBaaS plan.

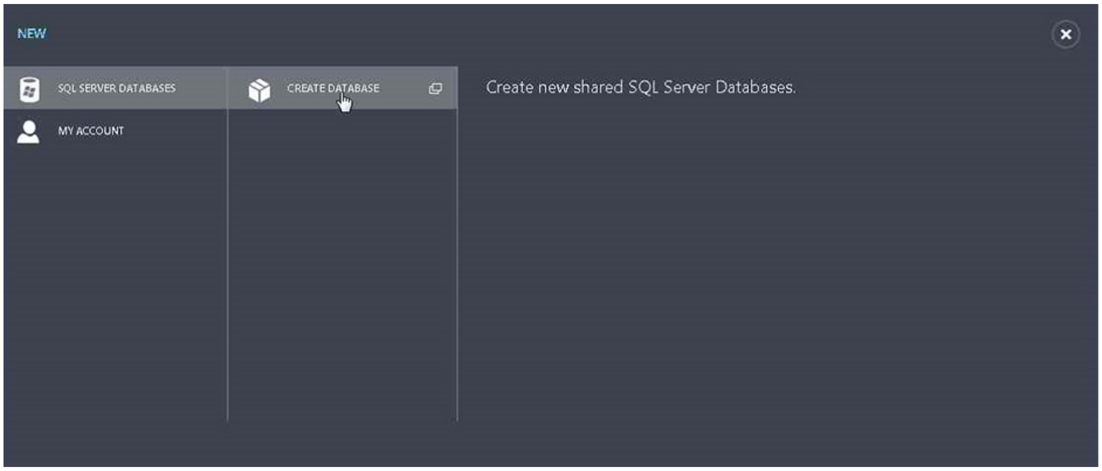


Step 4 Check My Account subscriptions to verify that the new service subscription is listed.

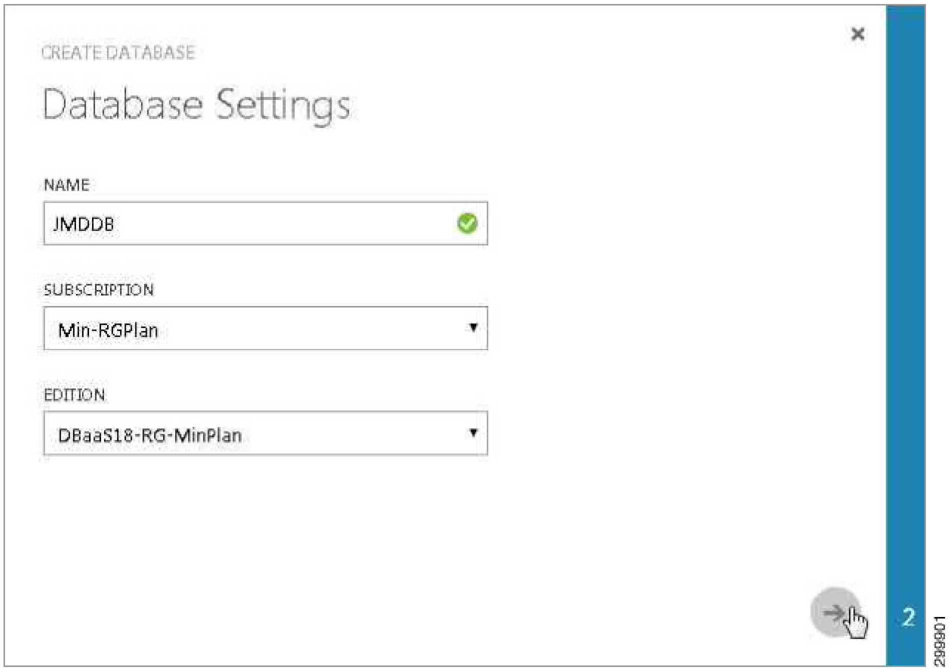


SUBSCRIPTION ID	SUBSCRIPTION	STATUS	PLAN	ENROLLMENT DATE
51f43fda-41ce-4d72-a333-ca8c...	sqlaas-plan-03	✓ Active	sqlaas-plan-03	02/06/2015 14:22:42
ed610ae0-c667-42fc-a0ff-6eb39...	SQLaaS-Plan127	✓ Active	SQLaaS-Plan127	16/09/2015 11:22:08
d1f217b8-18c2-4f44-ac16-000c...	DBaaS-Plan-03	✓ Active	DBaaS-Plan-03	16/09/2015 23:38:41
76705120-2c96-468a-8c48-... →	Min-RGPlan	✓ Active	Min-RGPlan	17/09/2015 14:00:44

Step 5 Create new database. Click **+ New** to bring up the SQL Server Database/Create Database option.



Step 6 In resulting view, select the database name and associated plan from the pull-down list of plans to which the tenant has subscribed.


CREATE DATABASE

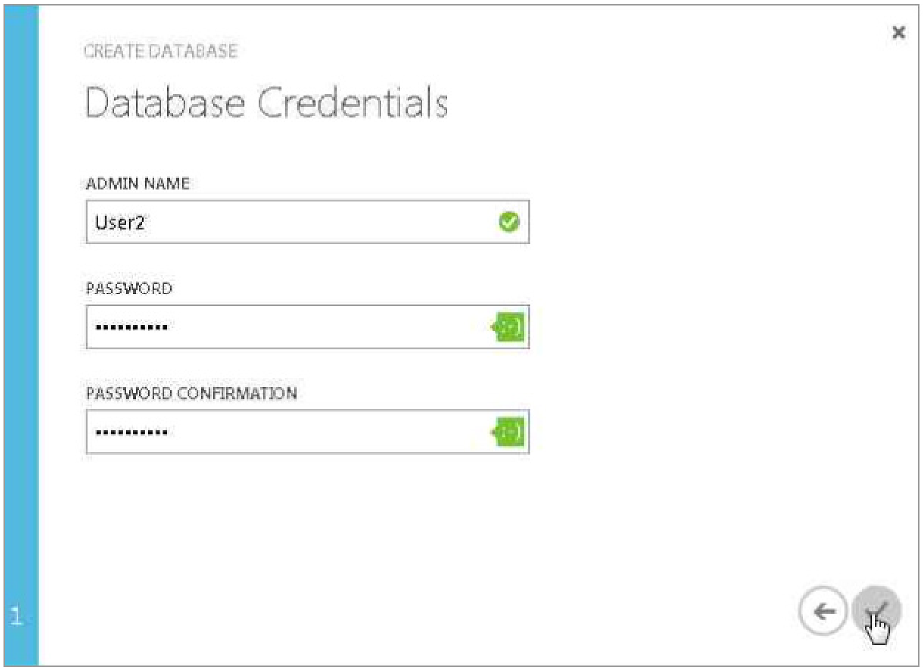
Database Settings

NAME: JMDDB

SUBSCRIPTION: Min-RGPlan

EDITION: DBaaS18-RG-MinPlan

Step 7 Enter credentials for database access in the resulting view.



CREATE DATABASE

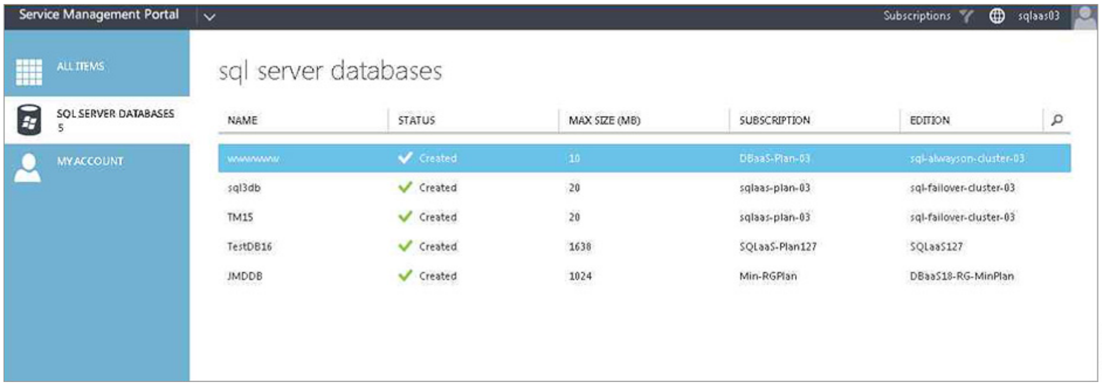
Database Credentials

ADMIN NAME: User2

PASSWORD: ••••••••••

PASSWORD CONFIRMATION: ••••••••••

Step 8 View the list of defined SQL databases to verify that the newly created one is included.



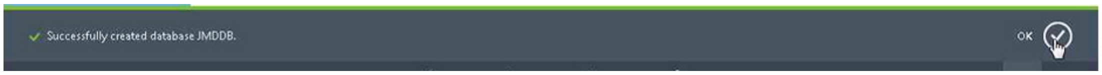
Service Management Portal

Subscriptions sqlaas03

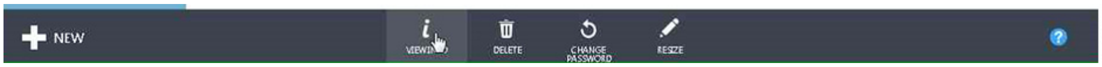
ALL ITEMS
SQL SERVER DATABASES 5
MY ACCOUNT

sql server databases

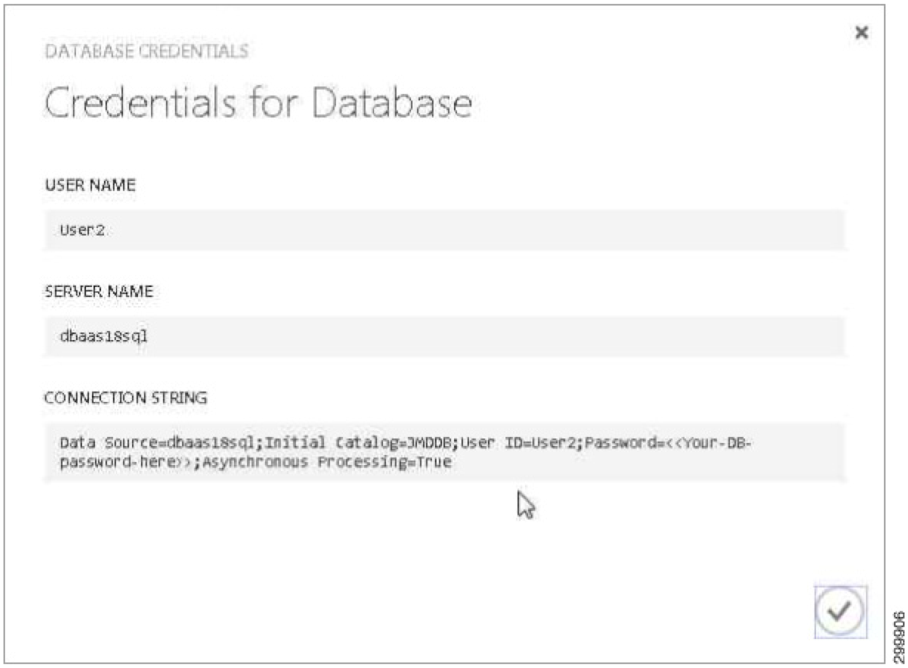
NAME	STATUS	MAX SIZE (MB)	SUBSCRIPTION	EDITION
wwwwww	✓ Created	10	DBaaS-Plan-03	sql-alwayson-cluster-03
sql3db	✓ Created	20	sqlaas-plan-03	sql-failover-cluster-03
TM15	✓ Created	20	sqlaas-plan-03	sql-failover-cluster-03
TestDB16	✓ Created	1638	SQLaaS-Plan127	SQLaaS127
JMDDB	✓ Created	1024	Min-RGPlan	DBaaS18-RG-MinPlan



✓ Successfully created database JMDDB.



Step 9 View the Database Credentials. Select the newly created database from the list. From the bottom of the Tenant Service Management Portal, select **View Info** to see the SQL database access credentials for that database.



DATABASE CREDENTIALS

Credentials for Database

USER NAME

User2

SERVER NAME

dbaas18sql

CONNECTION STRING

```
Data Source=dbaas18sql;Initial Catalog=JMDDB;User ID=User2;Password=<<Your-DB-
password-here>>;Asynchronous Processing=True
```