



Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Administrator Portal Guide, Release 2.1

October 12, 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 2.1

Part: CCAMCP-CNAP-Admin2-2.1

© 2016 Cisco Systems, Inc. All rights reserved.



CONTENTS

Preface v

- Document Objective and Scope** 2-v
- Useful Microsoft Windows Azure Pack References** 2-vi
- Useful Product Documentation** 2-vii

CHAPTER 1

Introduction 1-1

- Tasks You Can Perform in the Admin Portal** 1-1
 - Using Global Search on Admin Portal Tabs** 1-2
 - Understanding the Interrelationship of Tasks Performed in the Admin and Tenant Portals** 1-3
- Prerequisites for Using Cisco Cloud Network Automation Provisioner** 1-3
 - Build the Data Center Infrastructure** 1-4
- Prerequisites for Creating Network Container Plans and Containers** 1-5
- Accessing the Admin Portal** 1-6

CHAPTER 2

Configuring Global Settings and Regions 2-1

- Configuring Global Settings for the System and Fabric** 2-1
 - Creating the Cisco CSR 1000V Template Used by Cisco CNAP** 2-2
 - Configuring Global System Settings** 2-3
 - Configuring Global Fabric Settings** 2-5
- Starting the Cisco.Network.Provisioner Windows Service** 2-9
- Setting Up and Configuring Regions** 2-9
 - Understanding the Concept of Regions** 2-9
 - Adding a Region** 2-12
 - Viewing Information about a Region** 2-20
 - Modifying a Region** 2-24
 - Modifying the Description of a Region** 2-24
 - Modifying SCVMM Parameters for a Region** 2-25
 - Removing a Region** 2-26
- Restarting the Cisco.Network.Provisioner Windows Service** 2-28

CHAPTER 3

Building the Pool of Available Cloud Resources 3-1

- Configuring Data Center Devices** 3-1
 - Adding a Cisco Network Services Orchestrator Enabled by Tail-f** 3-2

Understanding the Difference Between Auto-provisioning and Manually Provisioning WAN Gateways 5-15

Setting Up a WAN Gateway 5-15

Setting up a MPLS WAN Gateway 5-15

Setting up an Auto-provisioned WAN Edge/PE 5-18

Setting up a Manually Provisioned WAN Edge/PE 5-19

Setting up a Site-to-Site VPN 5-21

Removing a Gateway 5-23

Configuring and Managing Firewalls 5-23

Understanding Firewall Creation 5-24

Viewing Summary Information about a Firewall 5-24

Viewing the Hierarchy of Information on the Firewall Tab 5-28

Configuring a Firewall 5-32

Changing a Policy Map for a Service Policy 5-38

Adding a New Class Map 5-39

Changing a Class Map 5-42

Creating a New Network Access Control List 5-43

Changing an Access List 5-46

Creating a New Object Group 5-47

Changing an Object Group 5-52

APPENDIX A

Cisco Application Policy Infrastructure Controller A-1

APPENDIX B

Sample Database as a Service Deployment B-1

Dedicated Service Deployment Mode—Failover Cluster Redundancy Option and SQL DBaaS Instance in Dedicated per-Tenant Virtual Machines B-1

Use the Administrator SQL Resource Provider User Interface to Create the DBaaS Plan and Resource Allocation B-2

Use the Tenant SQL Resource Provider User Interface to View Published Plan Options and Subscribe B-8

Shared Service Deployment Mode—Always-on Cluster Redundancy Option and DBaaS Instance per-Tenant on Multi-tenant SQL Server(s) B-13

Use the Administrator SQL Resource Provider User Interface to Create DBaaS Plan and Resource Allocation B-13

Use the Tenant SQL Resource Provider User Interface to Create DBaaS Plan and Resource Allocation B-25



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 2.1 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/2-0/CNAP2-RNs/CNAP2-Release-Notes.html	Describes caveats and other important information about Release 2.1.
Cisco Cloud Architecture for the Microsoft Cloud Platform: Infrastructure Foundation Guide, Release 2.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/2-0/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 2.0 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/2-0/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 2.1 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/2-0/CNAP2-Install/CNAP2-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 2.1 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/2-0/CNAP2-Admin/CNAP2-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 2.1 http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/2-0/CNAP2-Tenant/CNAP2-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-a-mp-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>

■ Useful Product Documentation

- 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>



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 region.
- 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 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 IP addresses and IP subnets, including add a new IP subnet, unallocate an IP subnet, remove an IP subnet, and allocate public IP addresses to a tenant.
- 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 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. Not supported in current release.

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.”](#)

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 2.1* (http://www.cisco.com/c/en/us/td/docs/solutions/Service_Provider/CCAMCP/2-0/CNAP2-Install/CNA-P2-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.

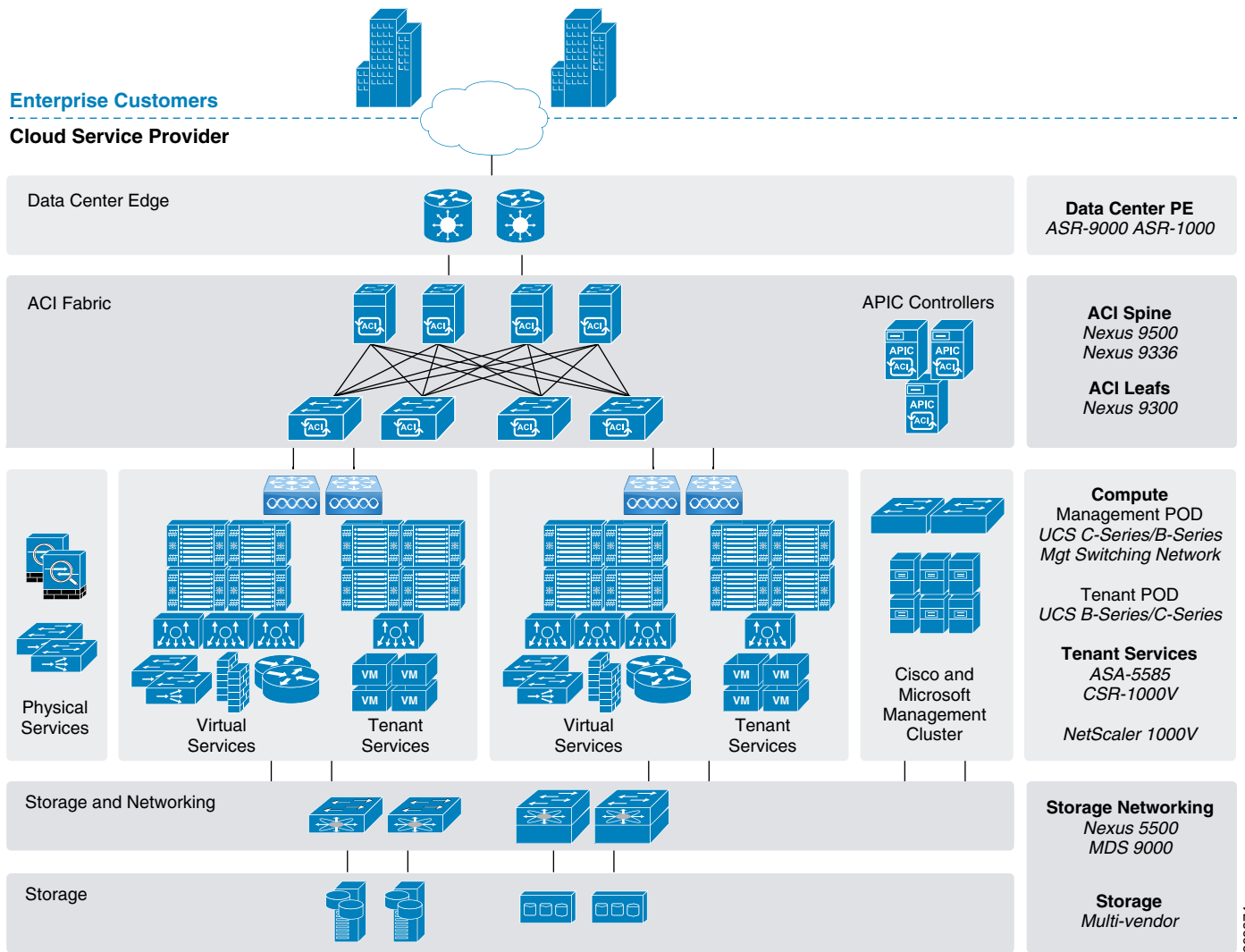
Refer to the *Cisco Cloud Architecture for the Microsoft Cloud Platform: Infrastructure Foundation Guide, Release 1.0* for detailed information on building data centers using physical components to implement compute, storage, and data center networking to create a pool of resources that are then used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

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**.

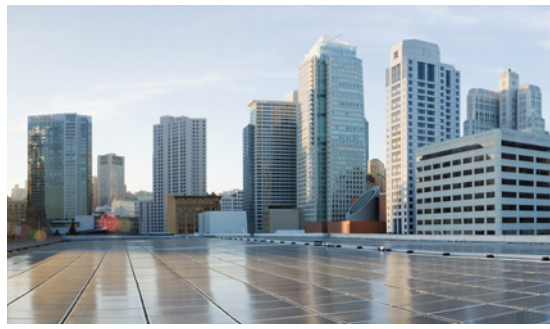
You see the main Cisco Datacenter Network screen, which is the Tenants tab, as shown in the following screen.

Figure 1-2 Tenants Tab Screen—Containers

The screenshot displays the Cisco Admin Portal interface for the 'cisco datacenter network'. The left-hand navigation menu includes categories such as ALL ITEMS, CISCO DATACENTER NET..., WEB SITE CLOUDS, VM CLOUDS, SERVICE BUS CLOUDS, SQL SERVERS, MYSQL SERVERS, AUTOMATION, TEAM ACCESS CONTROL, PLANS, USER ACCOUNTS, REQUEST MANAGEMENT, SNINE CLOUD SECURITY, and USER COSTS. The top navigation bar contains links for Tenants, Network Devices, Shared Services, Address Pool, Network Pool, Global Settings, Regions, and About. The main content area is titled 'Tenants' and has a sub-tab for 'Containers'. Below this, there is a 'Containers' section with a 'Container Details' table. The table has columns for Cont ID, Region, Admin Container Name, Tenant Container Name, Container State, Firewall, Network, SLB, Type, WAN, Tiers, and C. The table contains four rows of data:

Cont ID	Region	Admin Container Name	Tenant Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	C
6	T3R1	CMATPG1-01-03-006-cmatR1c1	cmatR1c1	Active	Inactive	3	Inactive	Zinc	Unknown	3	8%
7	T3R1	CMATPG1-01-04-007-cmatR1c2	cmatR1c2	Active	Inactive	3	Inactive	Zinc	Unknown	3	8%
8	T3R2	CMATPG1-02-03-008-cmatR2c1	cmatR2c1	Active	Inactive	3	Inactive	Zinc	Unknown	3	8%
9	T3R2	CMATPG1-02-04-009-cmatR2c2	cmatR2c2	Active	Inactive	3	Inactive	Zinc	Unknown	3	8%

At the bottom of the interface, there is a '+ NEW' button and a user ID '299718'.



CHAPTER 2

Configuring Global Settings and Regions



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 2.1*.

- In the Admin Portal, configure Global Settings for the System (**only required once**) and Fabric.
- Start the Cisco.Network.Provisioner Windows Service, which after a new installation creates the Cloud database.
- In the Admin Portal, set up and configure Regions.

In this release, Cisco CNAP uses the concept of Regions. You can think of a Region as a geographic area or a particular facility containing managed devices and containers. For more information, see [Understanding the Concept of Regions](#).

- 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 region settings, you must restart the Cisco.Network.Provisioner Windows Service for the updated settings to take effect.

Configuring Global Settings for the System and Fabric



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.



Caution

Pointing Cisco CNAP to an existing database during a **fresh** install (as opposed to an upgrade) stops the Cisco CNAP installation. You must drop the existing database from the target database server before continuing. This is a change from previous releases of Cisco CNAP in which fresh installations would also drop the existing database, potentially destroying unsaved data.


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 section as you will need this information to complete some fields:

- [Creating the Cisco CSR 1000V 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.
-

Configuring Global System Settings



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 2.1*.



Note

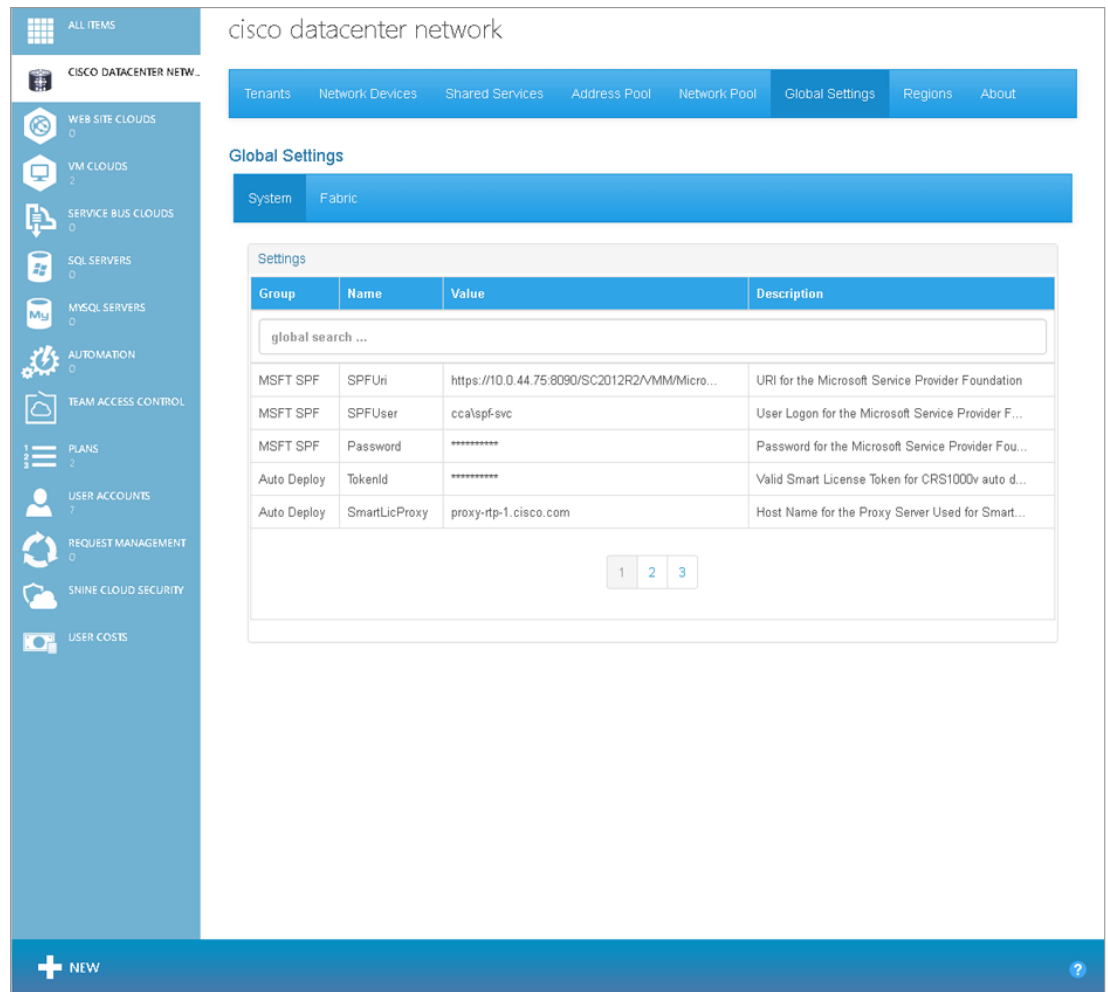
You only need to perform this step once.

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



Step 2

Move the cursor over the first row of the settings table to highlight the row. Click the highlighted row. You see a pop-up window, as shown in the following screen.

215823

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

The screenshot shows a 'System Settings' pop-up window. It has a title bar with a close button. Below the title is a 'Category' header. The main content area contains four fields: 'Setting' (MSFT SPF), 'Name' (SPFUri), 'Value' (https://10.0.44.75:8090/SC2012R2/MM/Microsoft.Management.Odata.sv), and 'Description' (URI for the Microsoft Service Provider Foundation). At the bottom, there are two buttons: 'Change' and 'Cancel'.

- Step 3** 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 4** 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 several 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	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	NameServer	10.0.43.10	Name Server Address for Virtual Network Devices
Auto Deploy	MgmtDomain	vmc-cosn.cisco.com	Domain name defined on the Management Network
Auto Deploy	SyslogServer	10.0.63.231	Syslog Server address for Virtual Network Devices.
Auto Deploy	HsrpAuthString	*****	Key for HSRP Authentication.
Auto Deploy	RouteDescriptorPrefix	PeAutoSystemNumber	Prefix source used for auto-generated Route Descriptors. Options are PEBundle or PEautoSystemNumber.

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

Configuring Global Fabric Settings

- Step 1** On the Tenants list screen, click the **Global Settings** tab, then click the **Fabric** tab. You see the Global Fabric Settings screen, as shown in the following screen.

Figure 2-3 Global Fabric Settings Screen

The screenshot displays the 'Global Fabric Settings' screen in the Cisco Cloud Network Automation Provisioner. The interface includes a navigation sidebar on the left with categories like 'ALL ITEMS', 'CISCO DATACENTER NET...', 'WEB SITE CLOUDS', 'VM CLOUDS', 'SERVICE BUS CLOUDS', 'SQL SERVERS', 'MYSQL SERVERS', 'AUTOMATION', 'TEAM ACCESS CONTROL', 'PLANS', 'USER ACCOUNTS', 'REQUEST MANAGEMENT', 'SINE CLOUD SECURITY', and 'USER COSTS'. The main content area shows the 'Global Settings' for the 'Fabric' tab, with a dropdown menu for 'Cloud' set to 'cca_cloud1_dc2'. Below this is a table of settings:

Cloud Id	Settings	Name	Value	Description
3	MPLS VPN	PEaciL2InterfacePrimary	1	MPLS Network, Primary PE ACI L2 Attachment
3	BGP	PEAutoSystemNumber	65002	Provider Edge Autonomous System Number
3	BGP	CEAutoSystemNumber	65002	Customer Edge Autonomous System Number
3	APIC	VmmDom	scvmm_t3_dc2	APIC Virtual Machine Manager (VMM) Domain
3	APIC	L2DomainPostfix	asr_phy	Name used for the Layer 2 Bridge Domain in A...

At the bottom of the table, there are pagination controls showing '1 2 3 4', with '2' highlighted. A 'global search ...' input field is located above the table. The bottom of the screen features a '+ NEW' button and a help icon.

- Step 2** Move the cursor over the first row of the settings table to highlight the row. Click the highlighted row.
- Step 3** 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 4** 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 Fabric Global Settings. [Table 2-2](#) describes the various fields and their possible values.

Table 2-2 Global Fabric Settings



Cloud ID	Settings	Name	Sample Values ¹	Description
1	MPLS VPN	PEaciL2InterfacePrimary	5	<p>Bundle-Ethernet or Port-channel interface on the PE connecting to the Cisco ACI Fabric.</p> <p>For the Cisco ASR 9000, the value is in the range <1-65535></p> <p>For the Cisco ASR 1000, the value is the range <1-64>.</p> <p> 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.</p>
1	BGP	PEAutoSystemNumber	200	Provider Edge Autonomous System Number.
1	BGP	CEAutoSystemNumber	65001	Customer Edge Autonomous System Number.
1	APIC	VmmDom	cca	<p>Cisco APIC Virtual Machine Manager (VMM) Domain.</p> <p>The VMM domain is located in the Cisco APIC GUI under VM Networking -> Inventory -> Microsoft.</p>
1	APIC	L2DomainPostfix	asr9k-l2domain ask9k-phy	<p>Name used for the Layer 2 Bridge Domain in the Cisco APIC if you are provisioning Zinc containers with a Single Cisco CSR 1000V or a Cisco CSR 1000V pair for each customer.</p> <p>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.</p> <p>For a multi-CSR Zinc container, the physical domain name is used instead.</p> <p>In the Cisco APIC GUI, navigate to Fabric -> Access Policies -> Physical and External Domains -> Physical Domains and select the domain that is assigned to the VLAN pool corresponding to the Network pool defined in Cisco CNAP for asr9k connectivity.</p>
1	APIC	L2extPathNode1	101	<p>Cisco ACI Leaf Node 1 ID which is part of the vPC to PE router.</p> <p>In the Cisco APIC GUI, navigate to Fabric -> Inventory -> Fabric Membership to view the node ID of all switches in the Cisco ACI fabric.</p>

Table 2-2 Global Fabric Settings

1	APIC	L2extPathNode2	102	<p>Cisco ACI Leaf Node 2 ID which is part of the vPC to PE router.</p> <p>In the Cisco APIC GUI, navigate to Fabric → Inventory → Fabric Membership to view the node ID of all switches in the Cisco ACI fabric.</p>
1	APIC	L2extIntPath1	vpc_n101_n102_asr9k_pe1	<p>Policy Group name for the vPC connecting the Cisco ACI leaf pair to PE1.</p> <p>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.</p>
1	APIC	L2extIntPath2	vpc_n101_n102_asr9k_pe2	<p>Policy Group name for the vPC connecting the Cisco ACI leaf pair to PE2.</p>
1	MPLS VPN	PEacilL2InterfaceSecondary		<p>Bundle-Ethernet or Port-channel interface on PE2 connecting to the Cisco ACI Fabric.</p> <p> Note This value is not used in the current Cisco CNAP release.</p>
1	APIC	VmmCntrl	cca-scvm	<p>Cisco APIC Virtual Machine Manager (VMM) Controller defined under the VmmDom (VMM Domain) described above.</p> <p>The VMM controller name is located in the Cisco APIC GUI under VM Networking → Inventory → Microsoft → <domain> → Controllers.</p>
1	Internet	InternetVMNetworkName	InternetVL0699VMNetwork	<p>Internet Network Name connecting to Internet for Internet provisioning.</p>
1	BGP	PEInternetRouterPrimaryAddresses	10.5.11.251	<p>Address of the Primary PE router on the Internet Subnet.</p>
1	BGP	PEInternetRouterSecondaryAddress	10.5.11.252	<p>Address of the Secondary PE router on the Internet Subnet.</p>
1	Internet	InternetHsrpGroupBase	1000	<p>Internal HSRP Group ID starting index for Internet provisioning.</p>

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 2.1*.

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).

To start the Cisco.Network.Provisioner Windows Service:

Step 1 Start Windows Task Manager.

**Note**

You can also use the Windows Start menu to search for Windows services.

Step 2 Click the **Services** tab.

Step 3 In the list of services, locate Cisco.Network.Provisioner, right-click it, and in the pop-up window that appears, click **Start**.

Setting Up and Configuring Regions

You can think of a region as a geographic area or a particular facility containing managed devices and containers. For example, one region might be used to indicate managed devices in Data Center 1 (DC1), used as the primary site for a particular tenant's hosted applications, and another region might be Data Center 2 (DC2), used as the secondary site in the event of an outage at DC1. Note that regions could be co-located in the same facility (e.g., in a particular room or cabinet row) or a region could indicate a set of remotely managed CPE devices (e.g., for a remote region).

On the Regions tab screen, you can:

- Add a region.
- Look at information about regions.
- Modify a region.
- Remove a region.

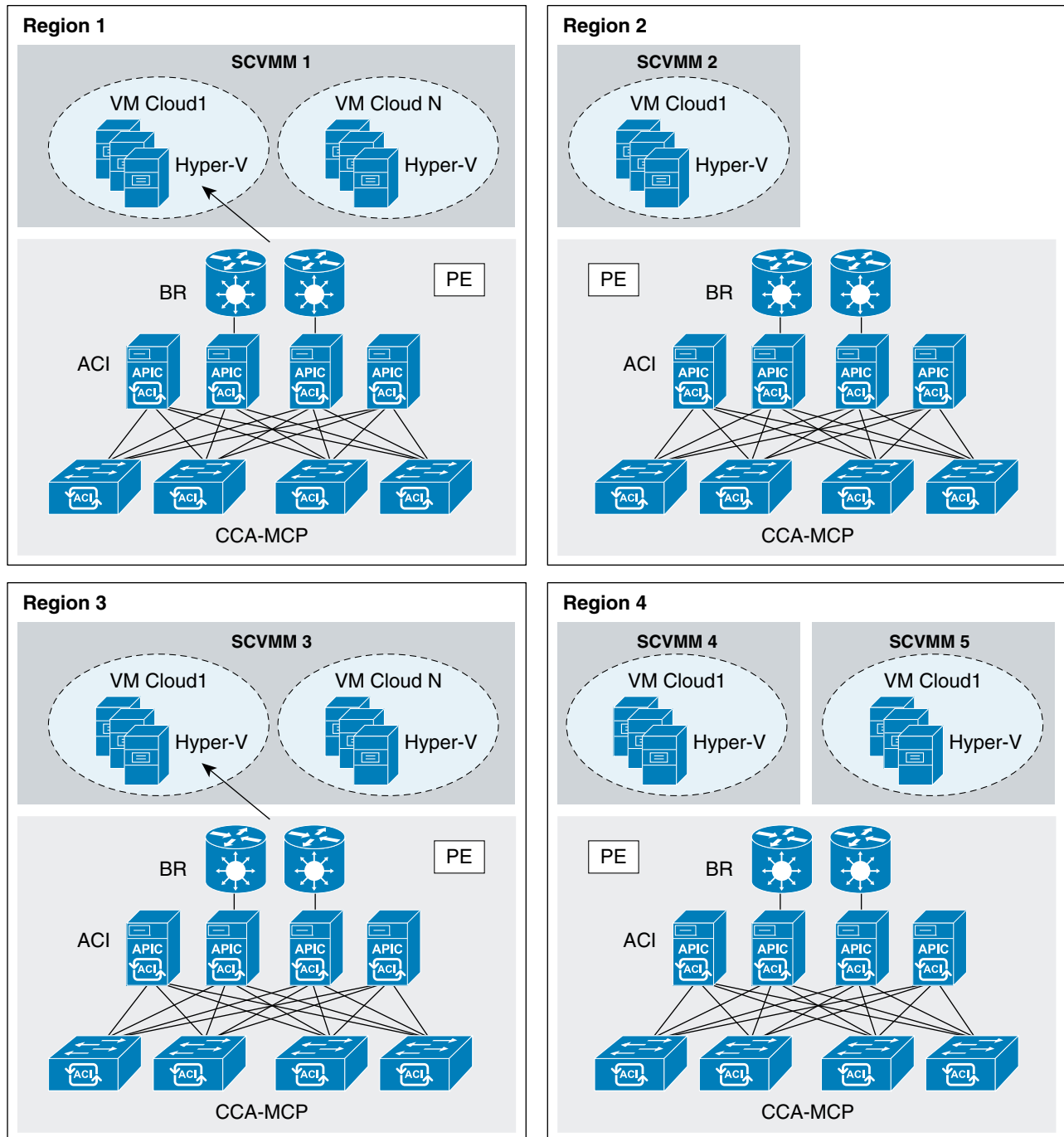
Understanding the Concept of Regions

As implemented by Cisco CNAP, Regions in effect comprise availability zones. However, in contrast to Openstack (where for example each AZ has a unique Openstack instance), in this case, the Regions are all under the control of a single WAP and Cisco CNAP instance. Thus WAP logical constraints apply, limiting the total number of supported SCVMM instances in the system to five and the total number of VM clouds per SCVMM to four. Additionally, the Cisco ACI APIC to SCVMM agent, which provides

for seamless integration of the Cisco Nexus 9000 DC switching fabrics with the VM Clouds within the overall system, constrains the relationship of ACI fabric to SCVMM instances to 1:N, where the maximum value for N is five (i.e., the maximum number of SCVMMs supported by WAP).

Figure 2-4 illustrates an example of a multi-Region, single WAP and Cisco CNAP administrative domain system. Note that the system shows the maximum number of possible SCVMM instances per WAP.

Figure 2-4 Multi-Region—Single WAP and Cisco CNAP System



215821

As previously discussed, while some of the regions above feature multiple SCVMM instances, they each have only one ACI fabric, preserving the 1:N relationship of ACI to SCVMM systems.



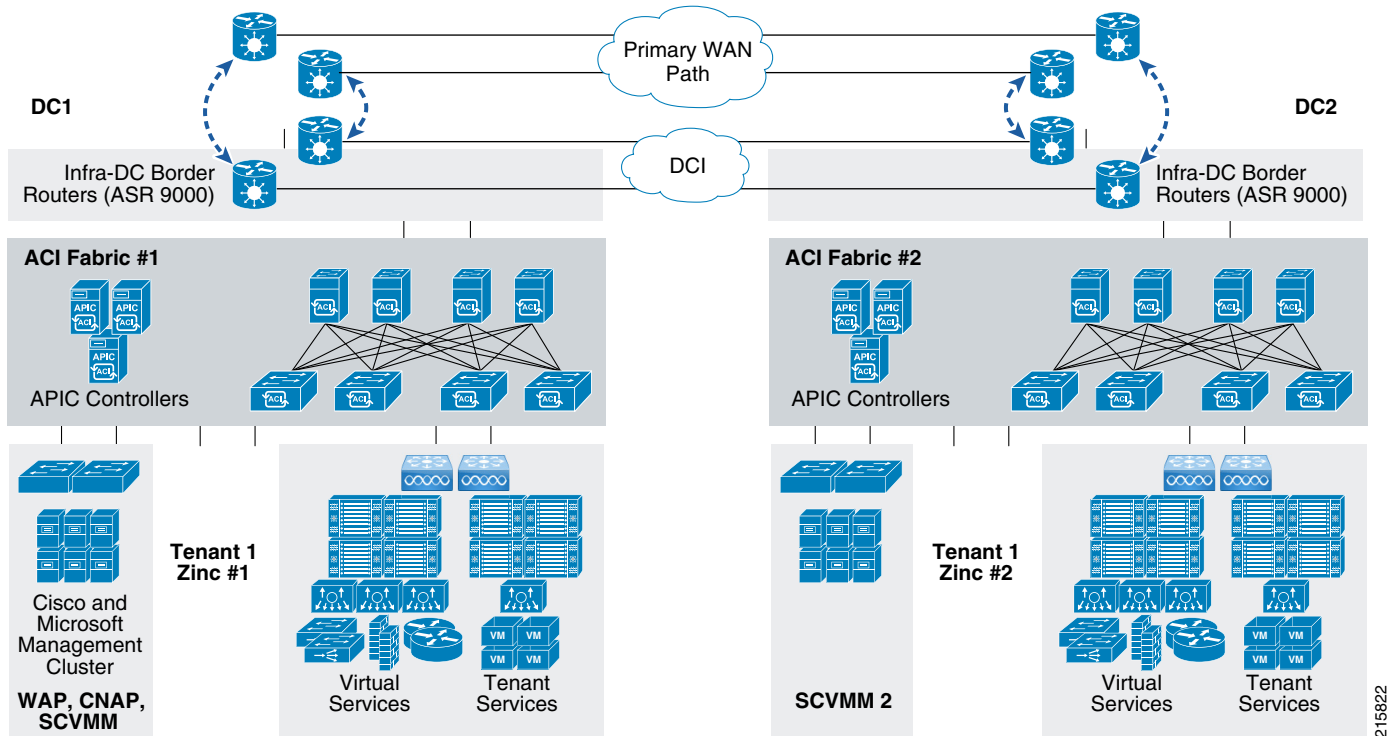
Note

In this release, Cisco CNAP only automates pushing of per-tenant routing information to the directly-attached Border Routers (BRs) in the system. Though technically possible, end-to-end routing between regions is not automated, as the assumption is that Provider-Edge (PE) to PE routed paths will be under the administrative control of a separate backbone transport operational team. Thus the BRs serve the role of an intra-DC or intra-Region administrative demarcation point.

Similarly, although the virtual machines or associated storage in a tenant container in one region may serve as backup resources for those in another container in another region, the tenant may only view network tiers and apply firewall policies for these workloads on a per-container basis because the container remains a logical routed boundary. The assumption is that in this case unique SCVMM instances will be utilized per Region.

Figure 2-5 illustrates a two-region system, with one management POD in Region “DC1” and a second SCVMM system associated with Region “DC2”. Figure 2-5 also more fully depicts the administrative demarcation of the PE routers, serving as the Layer 3 gateway to the provider backbone transport networks, versus the BRs, serving as Layer 3 gateways to DC staff-administered Data Center Interconnect networks.

Figure 2-5 Dual-DC with Single WAP and Cisco CNAP Management Fabric



When you configure data center devices, network pools, and address pools, you must indicate the Region with which these network resources will be associated. For more information, see Chapter 3, “Building the Pool of Available Cloud Resources.”

**Note**

You **must** have at least one region defined in CNAP. If you only have one region, you must set up and group all network devices, IP pools, VLAN ranges, etc. into that one region.

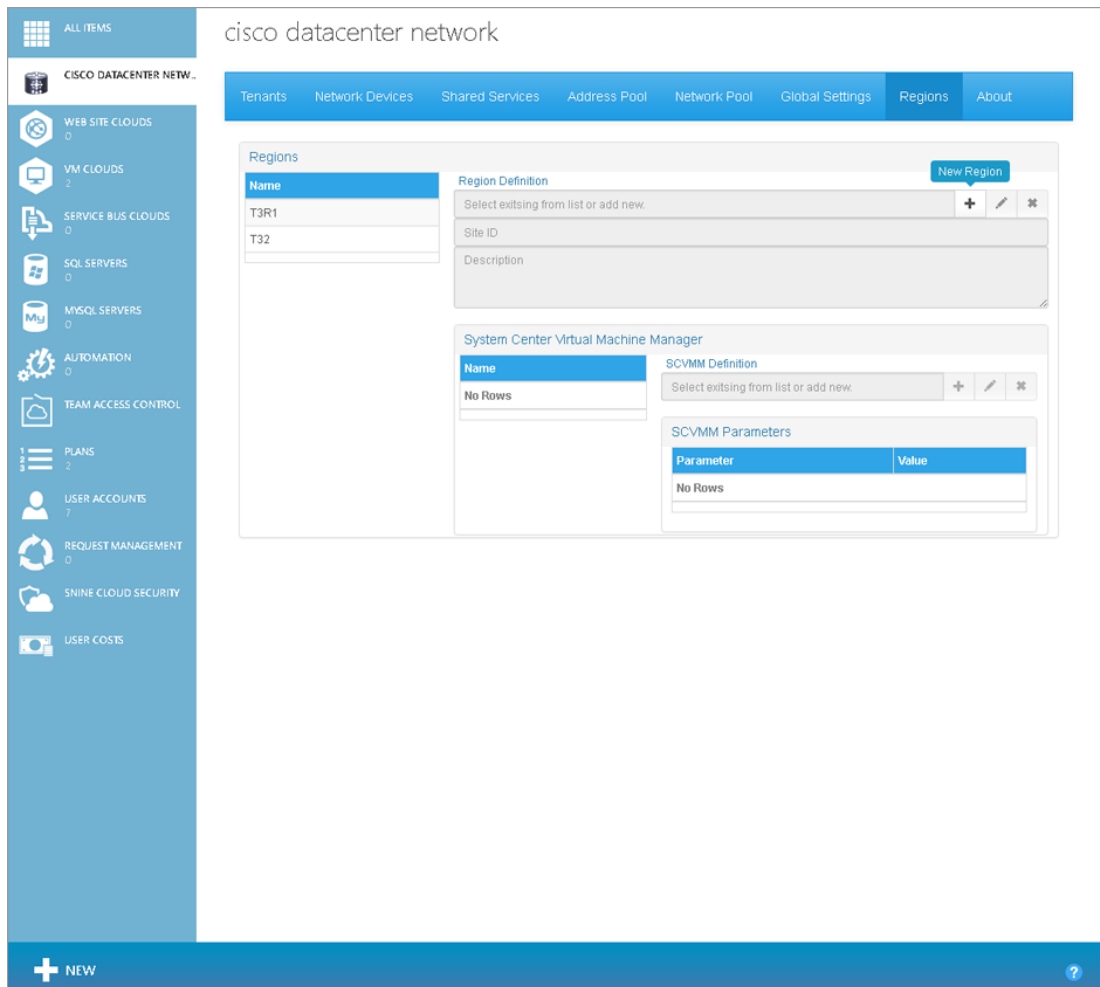
The resources within the scope of a particular region could include APIC clusters and nodes, MPLS and Internet gateway nodes (and related routing systems such as BGP or others), ASA5500 firewalls, and SCVMM controllers and their associated VM networks.

Adding a Region

To add a region:

- Step 1** On the Regions Tab screen, place the cursor over the plus sign (+), which displays the New Region tooltip, and click it, as shown in the following screen.

Figure 2-6 Regions Tab Screen—Add New Region Button



You see the following screen.

Figure 2-7 Regions Tab Screen—Add Region Popup

The screenshot shows a modal window titled "Add" with a close button in the top right corner. The main content area is titled "Region" and contains three input fields:

- *Name :** A text input field containing "Region3" with a green checkmark to its right.
- *Site ID :** A text input field containing "R3" with a green checkmark to its right.
- Description :** A text area containing "Description for region - max characters 256".

At the bottom of the modal, there are two buttons: "Cancel" on the left and "Next" with a right-pointing arrow on the right.

Step 2 Enter a Name, Site ID (must be at least two characters), and an optional Description.

A Site ID is a site identifier that is part of a container name. The Site ID appears in the container name in the format `xxxxxx-nn-xxxxx`, where *nn* is the Site ID.

When you are finished, click the **Next** arrow. You see the following screen

Figure 2-8 Regions Tab Screen—Associate SCVMM to Region Popup

The screenshot shows a web-based configuration popup titled "Add" for associating a System Center Virtual Machine Manager (SCVMM) to a region. The interface includes the following elements:

- Title Bar:** "Add" with a close button (X).
- Section Header:** "System Center Virtual Machine Manager" with a "+ New" button.
- Fields:**
 - *SCVMM Name: SCVMM1 (with a green checkmark)
 - Region Name: Region1
 - *SCVMM Host IP: 1.1.1.2 (with a green checkmark)
 - *SCVMM User: cnapuser (with a green checkmark)
 - *SCVMM Password: [Redacted] (with a green checkmark)
 - *CSRVM Template: CSR 1000v VM Template
 - *NSVM Template: Netscaler 1000v VM Template
 - *VM Mgmt Network: VMMcmNetwork (with a green checkmark)
 - *ISO Destination Folder: ISODestinationFolder (with a green checkmark)
 - *Clouds: A pull-down menu showing "Clouds" and a text box "One to many clouds associate with SCVMM".
- SCVMMs Table:** A table with columns for SCVMM Name, Host, User, CSRVM Template, NSVM Template, VM Mgmt Network, ISO Destination Folder, and Clouds. The table is currently empty, showing "No Rows".
- Buttons:** "+ Add", "Modify", and "- Remove" buttons are located above the table. At the bottom of the popup are "Back", "Save", and "Cancel" buttons.

215883

Step 3 Complete the following fields to associate an SCVMM to the Region you are adding:

- SCVMM Name—Name of the SCVMM.
- SCVMM Host IP—FQN/IP Address of System Center VMM Host.
- SCVMM User—User Logon for the Microsoft System Center VMM.
- SCVMM Password—Password for the Microsoft System Center VMM.
- CSRVM Template—Name of the Cisco CSR 1000V VM Template. For more information, see [Creating the Cisco CSR 1000V Template Used by Cisco CNAP](#).
- NSVM Template—Name of the Citrix NetScaler VPX VM Template. Not supported in the current release.
- VM Mgmt Network—VMNetwork used for management of the Cisco CSR 1000Vs. This is not the Logical Switch.
- ISO Destination Folder—Folder at the System Center VMM Host to hold post-deployment ISOs.

Step 4 Use the **Clouds** pull-down menu to associate clouds with the SCVMM, as shown in the following screen.

Figure 2-9 Regions Tab Screen—Cloud Pull-down Menu

The screenshot shows the 'Add' configuration window for a System Center Virtual Machine Manager region. The title bar says 'Add' with a close button. The main content area is titled 'System Center Virtual Machine Manager' and includes a '+ New' button. The configuration fields are as follows:

- *SCVMM Name :** Region2 scvmm 1
- Region Name :** Region2
- *SCVMM Host IP :** 1.1.1.1
- *SCVMM User :** cnapuser
- *SCVMM Password :** [Redacted]
- *CSRVM Template :** csrvm
- *NSVM Template :** nsvm
- *VM Mgmt Network :** vmmgmtnetwork
- *ISO Destination Folder :** ISODestinationFolder
- *Clouds :** A dropdown menu is open, showing 'One to many clouds assoicate with SCVMM' and two options: cca_cloud1 and cca_cloud1_dc2. Below the dropdown are '+ Add', 'Modify', and '- Remove' buttons.

At the bottom, there is an 'SCVMMS' table with the following columns: SCVMM Name, SCVMM Host, SCVMM User, CSRVM Template, NSVM Template, VM Mgmt Network, ISO Destination Folder, and Clouds. The table currently contains the text 'No Rows'.

Navigation buttons at the bottom include 'Back', 'Save', and 'Cancel'.

You can associate more than one Cloud, as shown in the following screen.

215684

Figure 2-10 Regions Tab Screen—Two Clouds Selected

The screenshot shows the 'Add' dialog box for configuring a System Center Virtual Machine Manager (SCVMM). The dialog is titled 'Add' and has a close button (X) in the top right corner. The main heading is 'System Center Virtual Machine Manager' with a '+ New' button. The configuration fields are as follows:

- *SCVMM Name :** CNAPNS-SCVMM
- Region Name :** CNAP Region
- *SCVMM Host IP :** 127.0.0.1
- *SCVMM User :** admin
- *SCVMM Password :** [Redacted]
- *CSRVM Template :** CSRVM
- *NSVM Template :** NSVM
- *VM Mgmt Network :** VMMGMT
- *ISO Destination Folder :** 1.0.0.ISO
- *Clouds :** Clouds (dropdown menu) showing COSNA-Workload, COSNA-CNAP, COSNA-RP

Below the fields is a table titled 'SCVMMS' with columns: SCVMM Name, SCVMM Host, SCVMM User, CSRVM Template, NSVM Template, VM Mgmt Network, ISO Destination Folder, and Clouds. The table currently contains no rows. At the bottom of the dialog are 'Back', 'Save', and 'Cancel' buttons.

215685

Step 5 When you are finished, click + **Add**.

The SCVMM is added to the SCVMMS table, as shown in the following screen.

Figure 2-11 Regions Tab Screen—SCVMM Added to List

System Center Virtual Machine Manager + New

*SCVMM Name : Region Name : **CNAP Region**

Parameters

*SCVMM Host IP : *SCVMM User : *SCVMM Password :

*CSRVM Template : *NSVM Template : *VM Mgmt Network :

*ISO Destination Folder: *Clouds :

SCVMMs

SCVMM Name	SCVMM Host	SCVMM User	CSRVM Template	NSVM Template	VM Mgmt Network	ISO Destination Folder	Clouds
CNAPNS-SCVMM	127.0.0.1	admin	CSRVM	NSVM	VMMGMT	1.0.0.ISO	COSNA-Workload, COSNA-CNAP, COSNA-RP

Back Save Cancel

215686

Step 6 You can associate additional SCVMMs. In the upper right, click **+ New**, complete the fields, and when you click **+Add**, each is added to the SCVMMs table, as shown in the following screen.

Figure 2-12 Regions Tab Screen—Second SCVMM Added

The screenshot shows a configuration window titled 'add' for 'System Center Virtual Machine Manager'. It includes several input fields and a table of existing SCVMMs.

System Center Virtual Machine Manager + New

*SCVMM Name : Region Name : **north**

Parameters

*SCVMM Host IP : *SCVMM User : *SCVMM Password :

*CSRVM Template : *NSVM Template : *VM Mgmt Network :

*ISO Destination : *Clouds :

SCVMMs

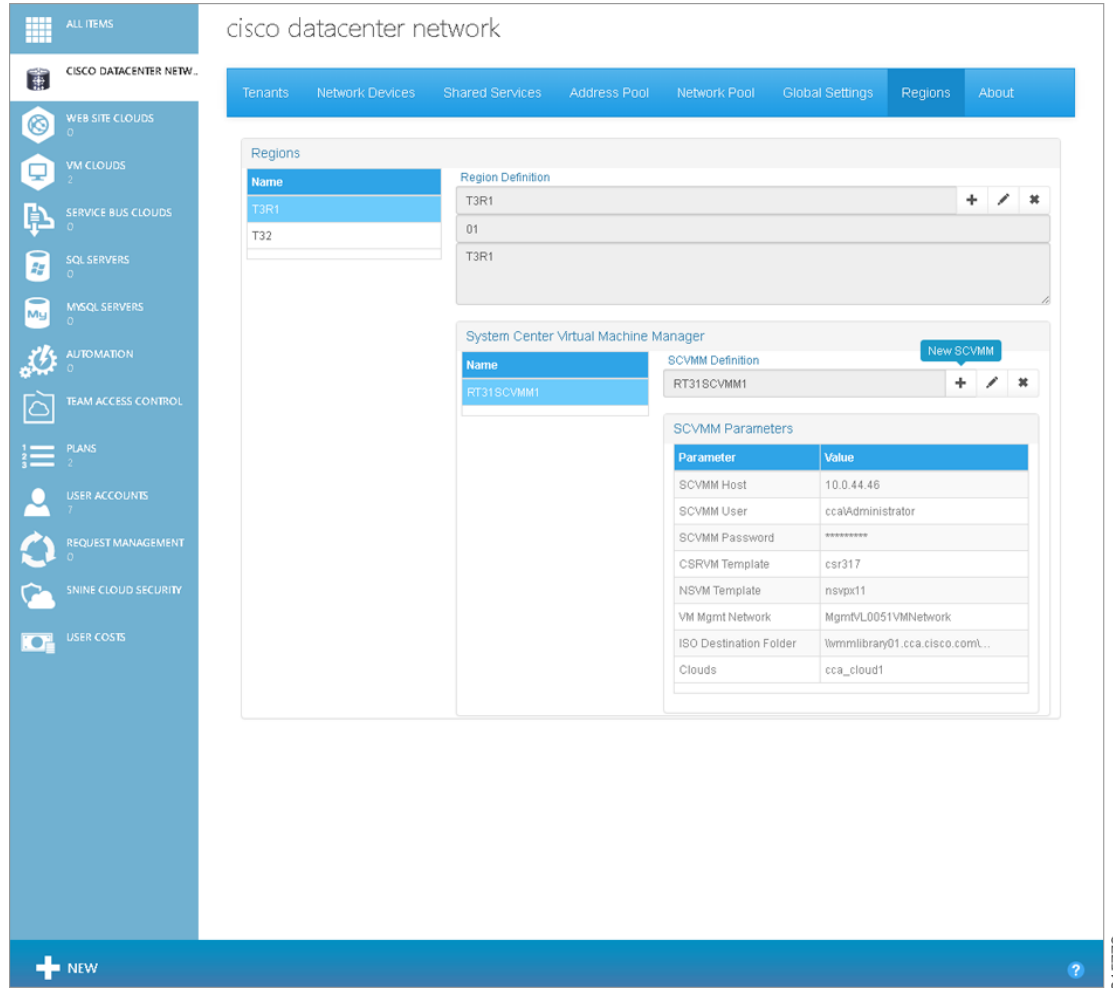
SCVMM Name	SCVMM Host	SCVMM User	C SRVM Template	NSVM Template	VM Mgmt Network	ISO Destination Folder	Clouds
north scvmm 1	1.1.1.1	joeuser	csrvm	nsvm	vmmgmtnetwork	\\1.1.1.1\isodesclon	COSNA-Nova,COSNA-RTP,
scvmm 2	2.2.2.2	joeuser	csrvm	nsvm	vmmgmtnetwork	\\10.1.2.2\iso	dc2-cloud1,

Buttons: Save, Cancel

215688

You can also add additional SCVMMs to a Region from the main Regions Tab screen. Next to the SCVMM Definition field, click the + (plus sign), as shown in the following screen.

Figure 2-13 Regions Tab Screen—Add New SCVMM



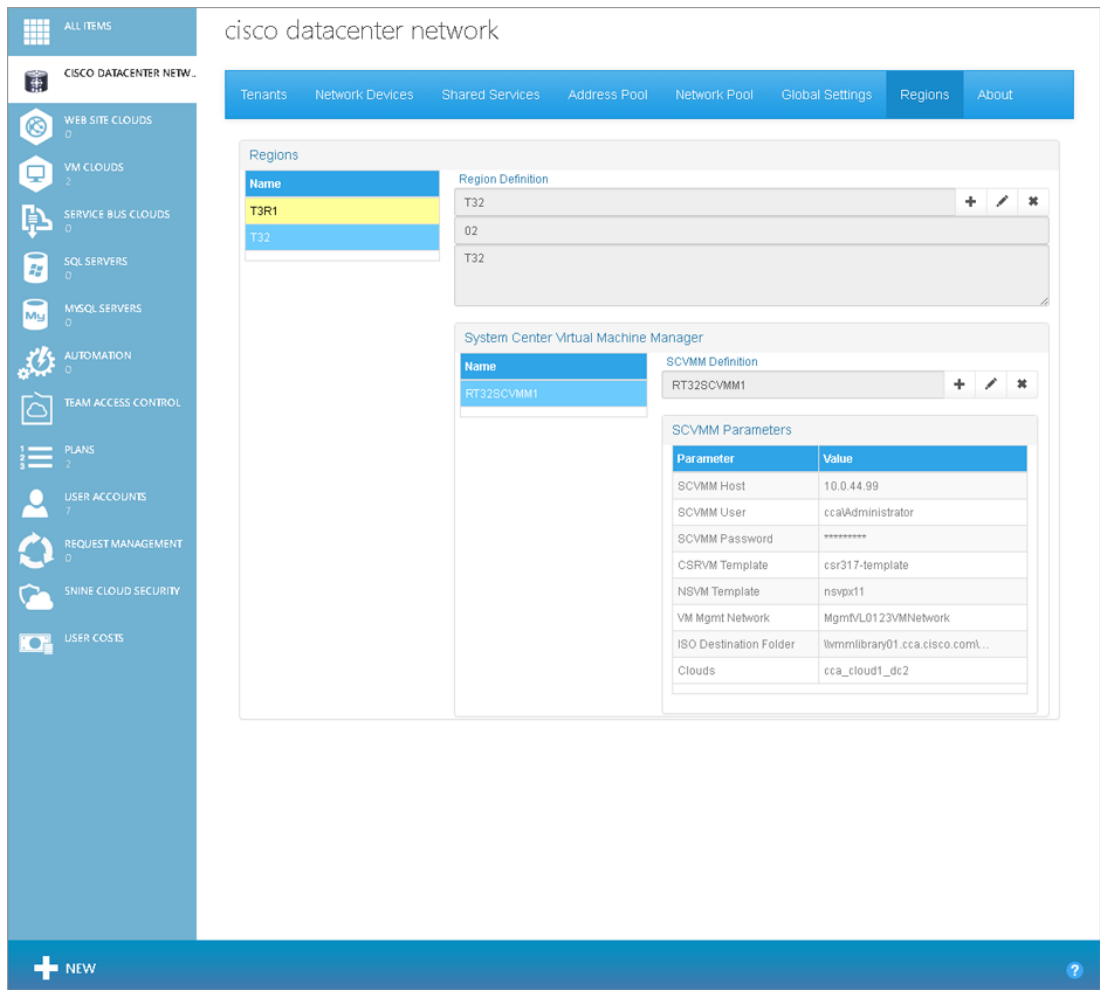
On the screen shown in Figure 2-8, in the upper right, click + **New**, complete the fields, and when you click +**Add**, the SCVMM is added to the SCVMMs table.

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

You see the following screen with the Region(s) you added displayed.

216778

Figure 2-14 Regions Tab Screen—Region Added



215687

Viewing Information about a Region

To view information about a region:

- Step 1** On the main Admin Portal screen, click the **Regions** tab. You see the following screen.

Figure 2-15 Regions Tab Screen

The screenshot shows the 'Regions' tab in the Cisco Datacenter Network Administration Portal. The left sidebar contains a navigation menu with various system components. The main area displays a table of regions and associated configuration options.

Name	Region Definition
T3R1	Select existing from list or add new. Actions for Regions + / ✖
T32	Site ID Description

Name	SCVMM Definition
No Rows	Select existing from list or add new. + / ✖

Parameter	Value
No Rows	

Step 2 On the left of the screen under Regions, click the name of a region. You see the following screen.

Figure 2-16 Regions Tab Screen—Region Selected

The screenshot displays the 'Regions' configuration page in the Cisco Datacenter Network portal. The page title is 'cisco datacenter network'. The navigation bar includes 'Tenants', 'Network Devices', 'Shared Services', 'Address Pool', 'Network Pool', 'Global Settings', 'Regions', and 'About'. The 'Regions' tab is active. On the left, a sidebar lists various categories like 'ALL ITEMS', 'CISCO DATACENTER NETWORK', 'WEB SITE CLOUDS', 'VM CLOUDS', 'SERVICE BUS CLOUDS', 'SQL SERVERS', 'MYSQL SERVERS', 'AUTOMATION', 'TEAM ACCESS CONTROL', 'PLANS', 'USER ACCOUNTS', 'REQUEST MANAGEMENT', 'SINE CLOUD SECURITY', and 'USER COSTS'. The main content area shows a 'Regions' table with columns 'Name' and 'Region Definition'. The table lists 'T3R1' and 'T32'. Below the table, there are sections for 'System Center Virtual Machine Manager' and 'SCVMM Parameters'. The 'SCVMM Parameters' section shows a table with columns 'Parameter' and 'Value', and the text 'No Rows'.

Step 3 Under System Center Virtual Machine Manager, click the name of a SCVMM. You see the following screen.

Figure 2-17 Regions Tab Screen—SCVMM Selected

The screenshot displays the 'Regions' configuration page for a 'cisco datacenter network'. The left sidebar contains various system categories like 'ALL ITEMS', 'CISCO DATACENTER NETW.', 'WEB SITE CLOUDS', 'VM CLOUDS', 'SERVICE BUS CLOUDS', 'SQL SERVERS', 'MYSQL SERVERS', 'AUTOMATION', 'TEAM ACCESS CONTROL', 'PLANS', 'USER ACCOUNTS', 'REQUEST MANAGEMENT', 'SHINE CLOUD SECURITY', and 'USER COSTS'. The top navigation bar includes tabs for 'Tenants', 'Network Devices', 'Shared Services', 'Address Pool', 'Network Pool', 'Global Settings', 'Regions', and 'About'. The main content area is divided into two primary sections:

- Region Definition:** A table with columns 'Name' and 'Region Definition'. It lists 'T3R1' and 'T32'. The 'Region Definition' for 'T3R1' is '01'.
- System Center Virtual Machine Manager:** A section containing a table with columns 'Name' and 'SCVMM Definition'. It lists 'RT318CVMM1'. Below this table is an 'SCVMM Parameters' table with the following data:

Parameter	Value
SCVMM Host	10.0.44.46
SCVMM User	ccaAdministrator
SCVMM Password	*****
CSRV Template	csr317
NSVM Template	nsvpx11
VM Mgmt Network	MgmtVL0051VMNetwork
ISO Destination Folder	\\vmmlibrary01.cca.cisco.com\...
Clouds	cca_cloud1

Under SCVMM Parameters, you see values for the following parameters for the selected SCVMM:

- SCVMM Host—FQN/IP Address of System Center VMM Host.
- SCVMM User—User Logon for the Microsoft System Center VMM.
- SCVMM Password—Password for the Microsoft System Center VMM.
- CSRV Template—Name of the Cisco CSR 1000V VM Template. For more information, see [Creating the Cisco CSR 1000V Template Used by Cisco CNAP](#).
- NSVM Template—Name of the Citrix NetScaler VPX VM Template. Not supported in the current release.
- VM Mgmt Network—VMNetwork used for management of the Cisco CSR 1000Vs. This is not the Logical Switch.
- ISO Destination Folder—Folder at the System Center VMM Host to hold post-deployment ISOs.
- Clouds—Clouds associated with the SCVMM.

Modifying a Region

You can modify:

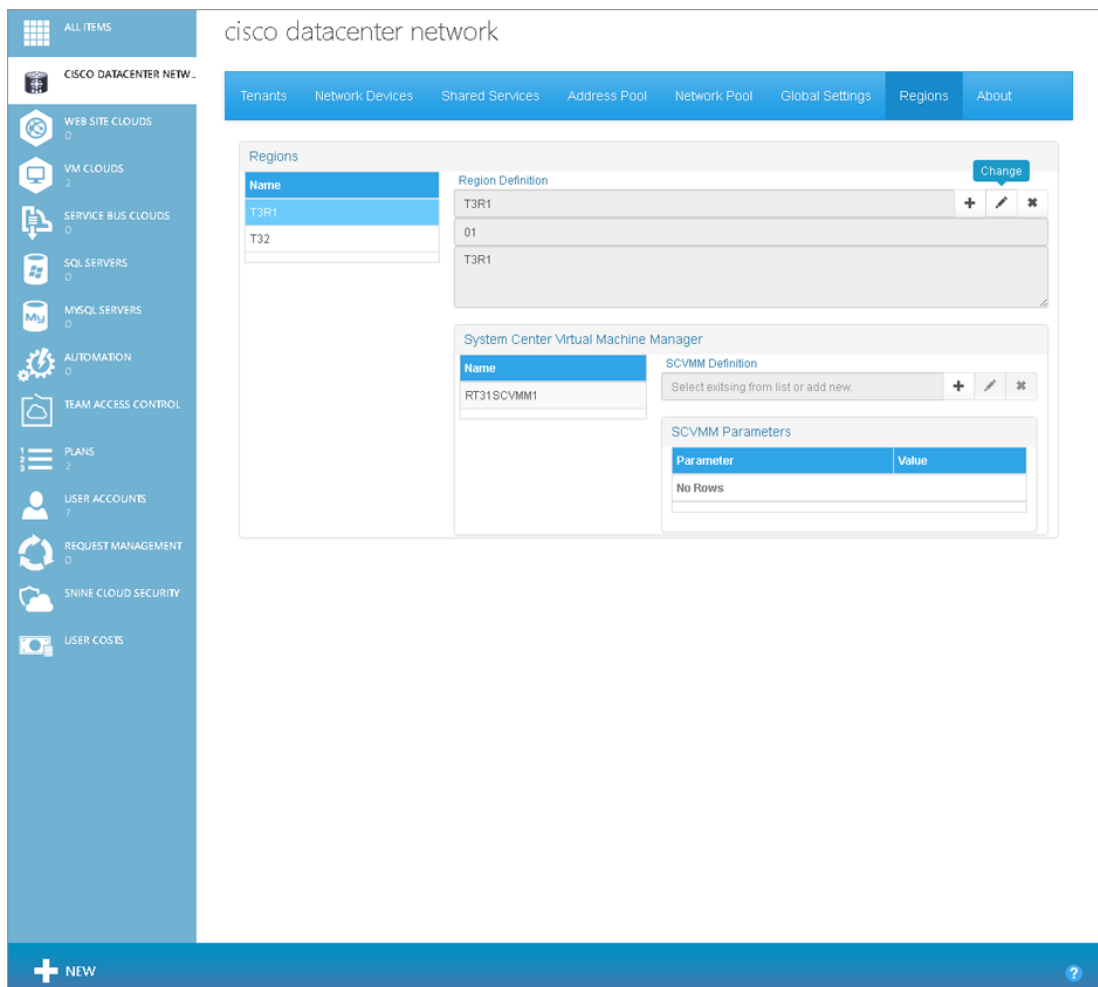
- The description of a region. You cannot modify the name or site ID of a region
- The parameters for SCVMMs associated with a region

Modifying the Description of a Region

To modify the description of a Region:

- Step 1** On the Regions Tab screen, in the list of Regions, click the Region you want to modify, then hover the cursor over the pencil icon to display the **Change** option, as shown in the following screen.

Figure 2-18 Change Region Icon



- Step 2** Click **Change**. You see the following screen.

Figure 2-19 Region Change Description

The screenshot shows a 'Change' dialog box with a close button in the top right corner. The dialog is titled 'Change' and contains a section labeled 'Region'. Inside this section, there are three input fields: '*Name :' with the value 'T3R1', '*Site ID :' with the value '01' and a green checkmark, and 'Description :' with the value 'T3R1'. At the bottom of the dialog, there are two buttons: 'Save' and 'Cancel'. The dialog is set against a light gray background.

Step 3 Under Description, change the description, then click **Save**.

Modifying SCVMM Parameters for a Region

Step 1 You can modify SCVMM parameters in two ways:

- On the Regions Tab screen, in the list of SCVMMs, click the SCVMM you want to modify, then under SCVMM Definition, click the pencil icon next to the name of the SCVMM.
- On the screen where you associate SCVMM(s) to a Region, click the SCVMM you want to modify.

The parameter values for the selected SCVMM are displayed, as shown in the following screen.

Figure 2-20 SCVMM Change screen

- Step 2** Change the values for any of the parameters. When you are finished, click **Save**. The updated values are reflected in the entry in the SCVMMMS table.

Removing a Region

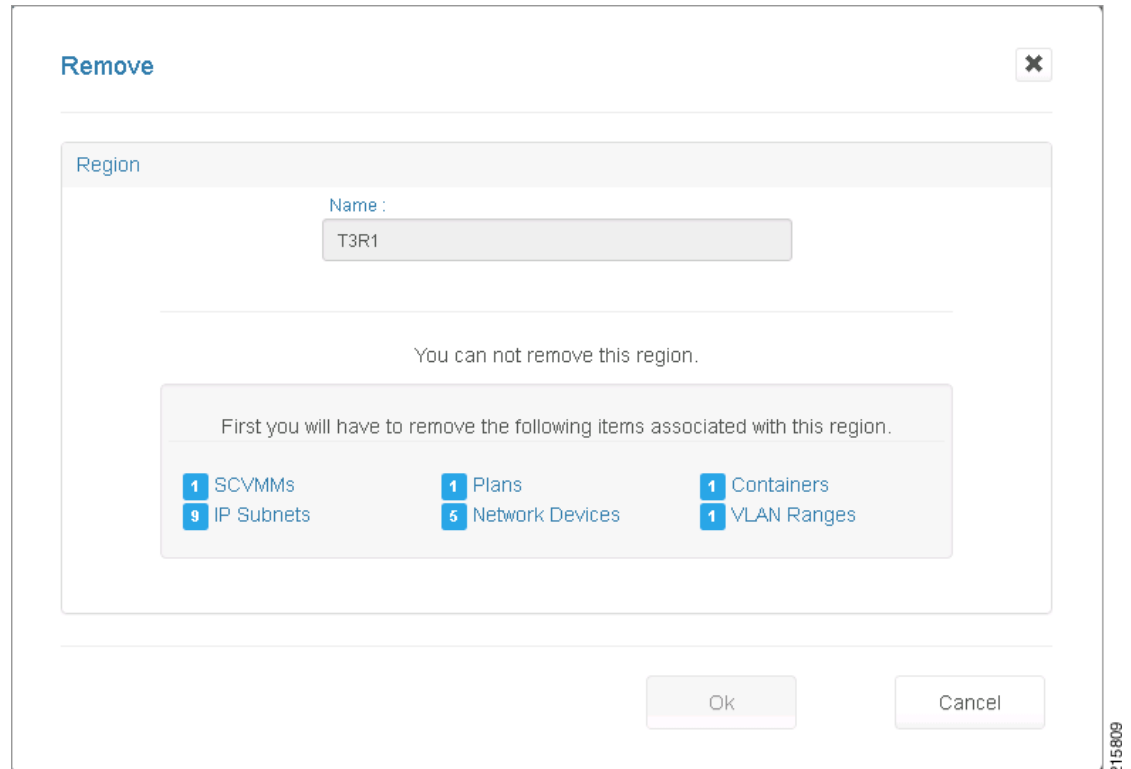
You can remove a region subject to the following restrictions:

- Before you can remove a region, you must remove the SCVMM(s) associated with the region.
- Before you can remove an SCVMM, you must remove any plans and containers associated with the SCVMM.

If you attempt to remove a region without completing these steps, you will see an error message.

To remove a region:

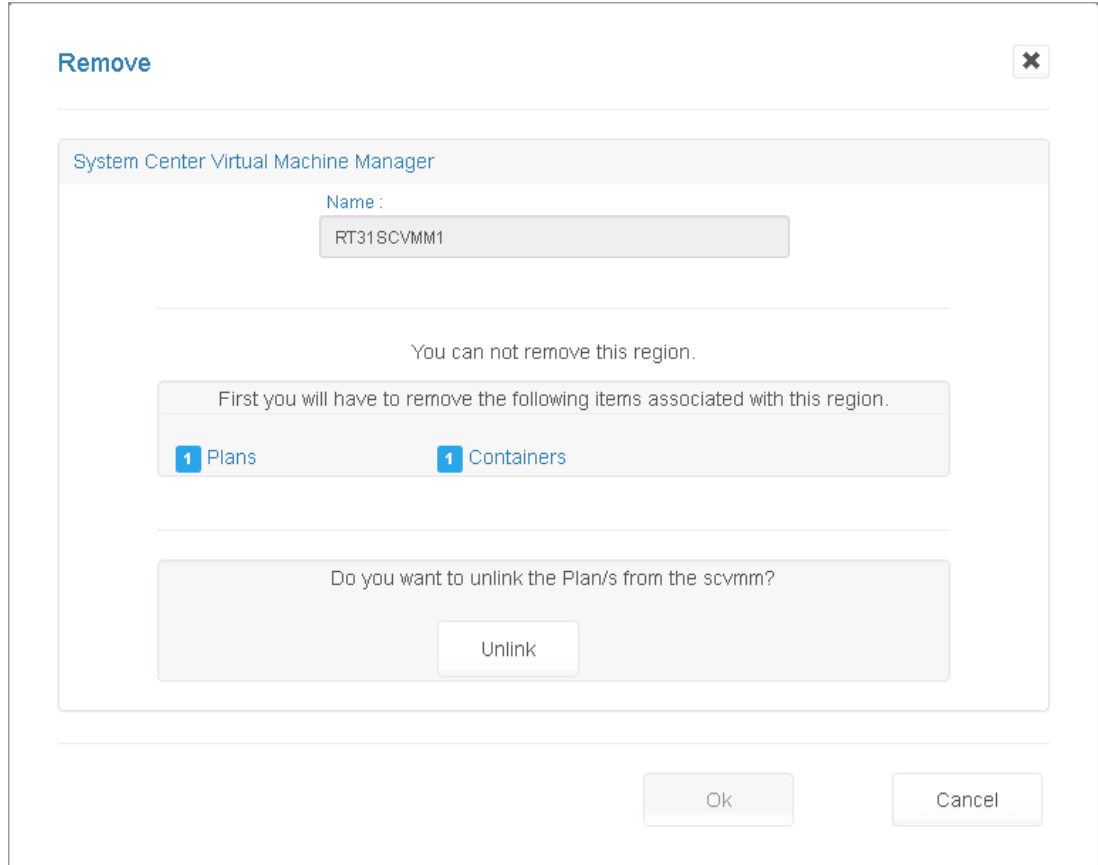
- Step 1** On the Region Tab screen, in the list of Regions, click the Region you want to remove, then click the **X** (Remove) button next to the name of the Region. You see the following screen.

Figure 2-21 Region Remove screen

You have to delete the indicated resources, such as SCVMMs, IP Subnets, Plans, Network Devices, Containers, and VLAN Ranges.

- Step 2** If there are SCVMMs associated with the Region, you must remove the SCVMM(s). On the screen where you associate SCVMM(s) to a Region, click the SCVMM you want to remove, then click **Remove**. You see the following screen.

Figure 2-22 Remove SCVMM



- Step 3** You have to remove any resources associated with the region before you can remove it. If there are additional SCVMMs associated with the region you are removing, remove those SCVMMs using the same procedure.
- Step 4** When you have finished removing SCVMMs, on the Regions Tab screen, remove the region.

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.

To restart the Cisco.Network.Provisioner Windows Service:

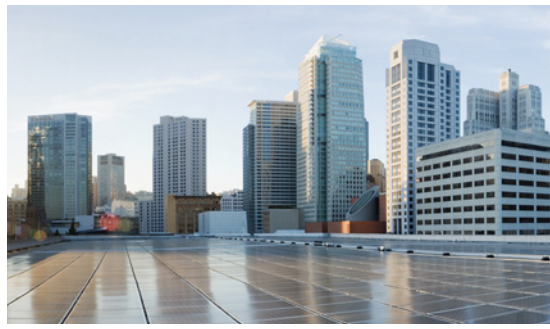
- Step 1** Start Windows Task Manager.



Note You can also use the Windows Start menu to search for Windows services.

- Step 2** Click the **Services** tab.

- Step 3** In the list of services, locate Cisco.Network.Provisioner, right-click it, and in the pop-up window that appears, click **Start**.
-



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, or Tier.



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 2.1*.

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 want to implement access control for the network, add a

- Cisco TACACS+ or RADIUS Server

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 2.1*.

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 Region drop-down, click the Region to which you want to add a device, as shown in the following screen.

Figure 3-1 Network Devices Tab Screen

The screenshot shows the 'Network Devices' tab in the Cisco Datacenter Network Management console. The main content area displays a table of network devices with the following data:

State	Name	FQDN/IP	Type	Connection	Created On	Modified On
Active	T31NSO	10.0.44.137	NSO	HTTP	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T31A1	10.0.44.24	APIC	HTTPS	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T31ASR1	10.0.44.120	ASR9000	SSH	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T31ASR2	10.0.44.121	ASR9000	SSH	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T31ASA	10.0.44.33	ASA5585	SSH	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T32NSO	10.0.44.137	NSO	HTTP	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T32A2	10.0.44.127	APIC	HTTPS	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T32ASR1	10.0.44.122	ASR9000	SSH	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T32ASR2	10.0.44.123	ASR9000	SSH	6/14/2016 3:39 PM	6/14/2016 3:39 PM

Below the table are 'Add' and 'Delete' buttons. The sidebar on the left contains various navigation options, and the top navigation bar includes 'Tenants', 'Network Devices', 'Shared Services', 'Address Pool', 'Network Pool', 'Global Settings', 'Regions', and 'About'.

- Step 2** Click **Add**.
You see the Add Network Device screen.

Figure 3-2 Add Network Device Screen

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

- Step 3** Region: *Region Name* displays the Region 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. For information on adding a Cisco TACACS+ or RADIUS server, see [Adding a Cisco TACACS+ or RADIUS Server](#).
 - 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:
 - Logon—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.
-

Adding a Cisco TACACS+ or RADIUS Server

During container creation, Cisco CNAP checks if a Cisco TACACS+ or RADIUS server has been onboarded. If it has, Cisco CNAP adds the configuration for it to the Cisco CSR 1000V. Cisco TACACS+ is used by default unless you have only onboarded a RADIUS server.

To add a Cisco TACACS+ or RADIUS server:

-
- Step 1** On the Network Devices Tab screen, in the Region drop-down, click the Region to which you want to add the server, as shown in the following screen.

Figure 3-4 Network Devices Tab Screen

The screenshot displays the 'Network Devices' tab in the Cisco Cloud Network Automation Provisioner. The interface includes a left-hand navigation menu with various categories like 'ALL ITEMS', 'CISCO DATACENTER NETWORKS', 'WEB SITE CLOUDS', 'VM CLOUDS', 'SERVICE BUS CLOUDS', 'SQL SERVERS', 'MYSQL SERVERS', 'AUTOMATION', 'TEAM ACCESS CONTROL', 'PLANS', 'USER ACCOUNTS', 'REQUEST MANAGEMENT', 'SINE CLOUD SECURITY', and 'USER COSTS'. The main content area is titled 'cisco datacenter network' and features a sub-header 'Network Devices'. Below this, there is a 'Device Information' section with a 'Region' dropdown set to 'All Regions'. A table lists the network devices with the following data:

State	Name	FQDN-IP	Type	Connection	Created On	Modified On
Active	T31NSO	10.0.44.137	NSO	HTTP	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T31A1	10.0.44.24	APIC	HTTPS	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T31ASR1	10.0.44.120	ASR9000	SSH	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T31ASR2	10.0.44.121	ASR9000	SSH	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T31ASA	10.0.44.33	ASA5585	SSH	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T32NSO	10.0.44.137	NSO	HTTP	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T32A2	10.0.44.127	APIC	HTTPS	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T32ASR1	10.0.44.122	ASR9000	SSH	6/14/2016 3:39 PM	6/14/2016 3:39 PM
Active	T32ASR2	10.0.44.123	ASR9000	SSH	6/14/2016 3:39 PM	6/14/2016 3:39 PM

At the bottom of the table, there are 'Add' and 'Delete' buttons. The 'Add' button is highlighted in the screenshot. A '+ NEW' button is located at the bottom left of the interface, and a help icon (?) is at the bottom right.

Step 2 Click **Add**.

You see the Add Network Device screen.

Figure 3-5 Add Network Device Screen

The screenshot shows a web-based form for adding a network device. The form is titled "Add Network Device" and has a close button in the top right corner. It is organized into several sections:

- Region :** T32
- Name:** A text input field with the placeholder "Enter Name".
- Type:** A pull-down menu.
- Connection:**
 - Protocol:** A pull-down menu.
 - Port:** A text input field with the placeholder "Enter Port".
 - FQNIIP:** A text input field with the placeholder "Enter FQNIIP".
 - URL:** A label for a URL field.
- Authentication:**
 - Logon:** A text input field with the placeholder "Enter Logon".
 - Password:** A text input field with the placeholder "Password".
 - Enable Password:** A button.

At the bottom of the form are two buttons: "Add" and "Cancel".

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

Figure 3-6 Add Network Device Screen—Type Pull-down Menu

The screenshot shows the 'Add Network Device' configuration interface. At the top, it indicates the 'Region : T3R1'. The form is divided into several sections:

- Name:** A text input field labeled '*Name' with the placeholder 'Enter Name'.
- Type:** A pull-down menu labeled '*Type' with a list of device types: ASR9000, ASR1000, ASA5585, APIC, TACACS+, and RADIUS. The 'TACACS+' option is currently selected.
- Connection:** A section containing a '*Protocol' pull-down menu and a '*FQNI/IP' text input field with the placeholder 'Enter FQNI/IP'.
- Authentication:** A section containing a '*Logon' text input field with the placeholder 'Enter Logon', a '*Password' text input field with the placeholder 'Password', and an 'Enable Password / Secret Key' button labeled 'Enable Password'.

At the bottom of the form are two buttons: 'Add' and 'Cancel'.

Step 3 Region: *Region Name* displays the Region to which the server will be associated. Complete the following fields:

- Name—User-defined name given to the server.
- Type—Device type: On the pull-down menu, select **TACACS+** or **RADIUS**, depending on what type of server you are adding.
- Connection:
 - Protocol—TCP is the default protocol used to connect to a Cisco TACACS+ server. UDP is the default protocol used to connect to a RADIUS server.
 - Port—443 is the default port used to establish the connection to a Cisco TACACS+ server. You can change this value. You must enter the port number for a RADIUS server.
 - 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 server.

- Password—Service account password.
- Enable Password—If the server you are adding has an enable password that is different than the server password, enter it here. Otherwise the server password will be used for enable mode.

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

Deleting a Network Device

Step 1 On the Network Devices Tab Screen, in the Region pull-down menu on the left, click the region 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 3-7 Delete Network Device Screen

The screenshot shows a 'Delete Network Device' dialog box. It is titled 'Delete Network Device' and has a close button (X) in the top right corner. The dialog is divided into several sections:

- Region:** T32
- *Name:** T32ASR1
- *Type:** ASR9000 (dropdown menu)
- Connection:**
 - *Protocol:** SSH (dropdown menu)
 - *Port:** 22
 - *FQDNIP:** 10.0.44.122
 - URL:** 10.0.44.122:22
- Authentication:**
 - *Logon:** admin
 - *Password:** Password
 - Enable Password:** Enable Password

At the bottom of the dialog are two buttons: 'Remove' and 'Cancel'.

299729

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 3-8 Network Pool Tab Screen

The screenshot displays the 'Network Pool' tab in the Cisco Cloud Network Automation Provisioner. The interface includes a left-hand navigation menu with various categories like 'WEB SITE CLOUDS', 'VM CLOUDS', and 'SQL SERVERS'. The main content area is titled 'cisco datacenter network' and features a breadcrumb trail: 'Tenants > Network Devices > Shared Services > Address Pool > Network Pool > Global Settings > Regions > About'. The 'Network Pool' section contains a 'VLAN Range' table with the following data:

Region	VLAN IDs	State	Group	Created On	Modified On
T3R1	521-530	Available	Infrastructure	6-14-2016 3:39:38 PM	6-14-2016 3:39:38 PM
T32	421-430	Available	Infrastructure	6-14-2016 3:39:39 PM	6-14-2016 3:39:39 PM

Below the table, there is a 'Vlan Pool' section with a search bar and four buttons: 'Add', 'Available', 'Unallocate', and 'Delete'. A '+ NEW' button is located at the bottom left of the interface, and a help icon (?) is at the bottom right. The user ID '299730' is visible in the bottom right corner.

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 3-9 VLAN Pool for Selected VLAN Range Screen

The screenshot displays the 'Network Pool' configuration screen for a selected VLAN range. The interface includes a sidebar with navigation options, a top navigation bar, and two main tables: 'VLAN Range' and 'Vlan Pool'.

VLAN Range Table:

Region	VLAN IDs	State	Group	Created On	Modified On
T3R1	521-530	Available	Infrastructure	6-14-2016 3:39:38 PM	6-14-2016 3:39:38 PM
T32	421-430	Available	Infrastructure	6-14-2016 3:39:39 PM	6-14-2016 3:39:39 PM

Vlan Pool Table:

VLAN ID	Name	State	Allocated On	Modified On
521		UnAllocated		6-14-2016 3:39:38 PM
522		UnAllocated		6-14-2016 3:39:38 PM
523		UnAllocated		6-14-2016 3:39:38 PM
524		UnAllocated		6-14-2016 3:39:38 PM
525		UnAllocated		6-14-2016 3:39:38 PM

At the bottom of the screen, there are buttons for 'Add', 'Available', 'Unallocate', and 'Delete'. A 'NEW' button is located in the bottom left corner, and a help icon (?) is in the bottom right corner.

The Network Pools tab contains the following:

- The VLAN Range table contains the following fields:
 - Region—Name of the Region.
 - 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 Region in the VLAN Range table and click the **Add** button. You see the Add VLAN Range screen.

Figure 3-10 Add VLAN Range Screen

- 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.
- Region—Name of the Region to which the VLAN Range will be associated.
- 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 \leq (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 3-11 Select VLAN Range and Pool

The screenshot displays the 'Network Pool' configuration page for 'cisco datacenter network'. The interface includes a left-hand navigation menu with various categories like 'ALL ITEMS', 'CISCO DATACENTER NETWORK', 'WEB SITE CLOUDS', 'VM CLOUDS', 'SERVICE BUS CLOUDS', 'SQL SERVERS', 'MYSQL SERVERS', 'AUTOMATION', 'TEAM ACCESS CONTROL', 'PLANS', 'USER ACCOUNTS', 'REQUEST MANAGEMENT', 'SINE CLOUD SECURITY', and 'USER COSTS'. The main content area is titled 'Network Pool' and contains two tables: 'VLAN Range' and 'Vlan Pool'. Below the tables are buttons for 'Add', 'Available', 'Unallocate', and 'Delete'. A 'NEW' button is visible at the bottom left of the interface.

VLAN Range

Region	VLAN IDs	State	Group	Created On	Modified On
T3R1	521-530	Available	Infrastructure	6-14-2016 3:39:38 PM	6-14-2016 3:39:38 PM
T32	421-430	Available	Infrastructure	6-14-2016 3:39:39 PM	6-14-2016 3:39:39 PM

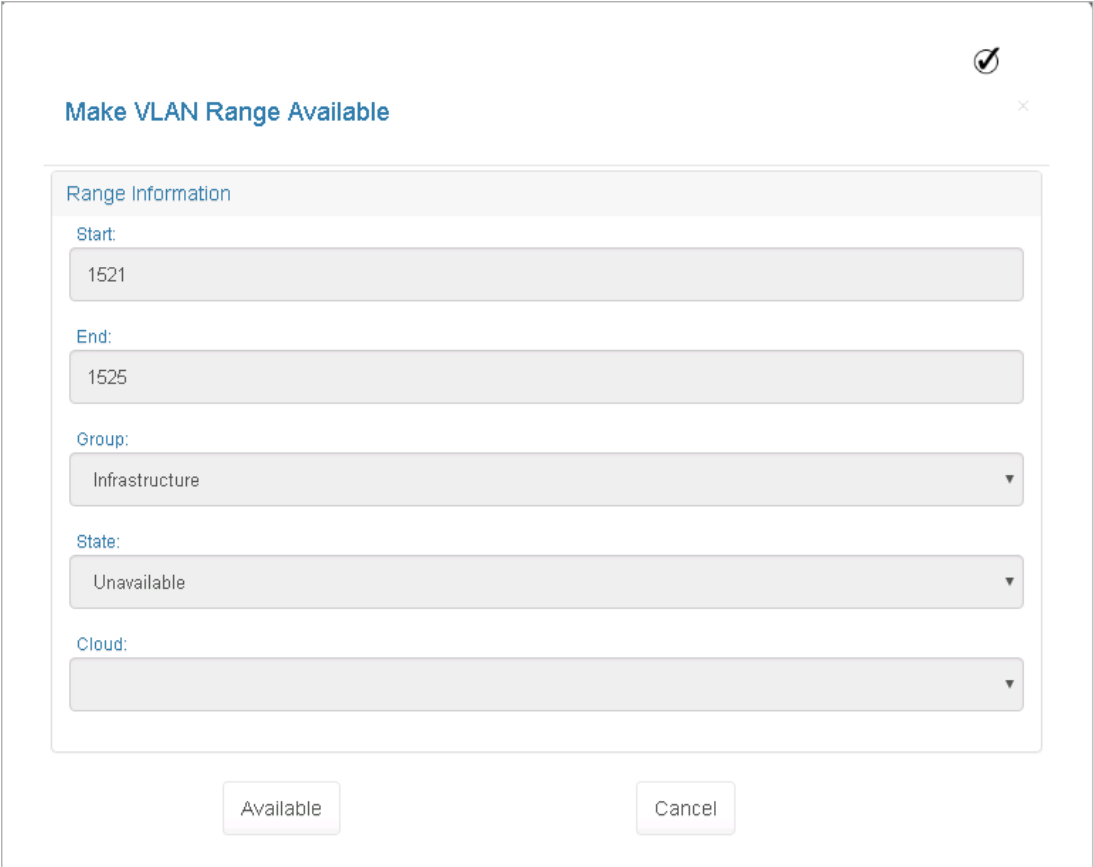
Vlan Pool

VLAN ID	Name	State	Allocated On	Modified On
521		UnAllocated		6-14-2016 3:39:38 PM
522		UnAllocated		6-14-2016 3:39:38 PM
523		UnAllocated		6-14-2016 3:39:38 PM
524		UnAllocated		6-14-2016 3:39:38 PM
525		UnAllocated		6-14-2016 3:39:38 PM

Buttons: Add, Available, Unallocate, Delete

Step 2 Click **Available**.

You see the Make VLAN Range Available screen.

Figure 3-12 Make VLAN Range Available Screen

Make VLAN Range Available

Range Information

Start:
1521

End:
1525

Group:
Infrastructure

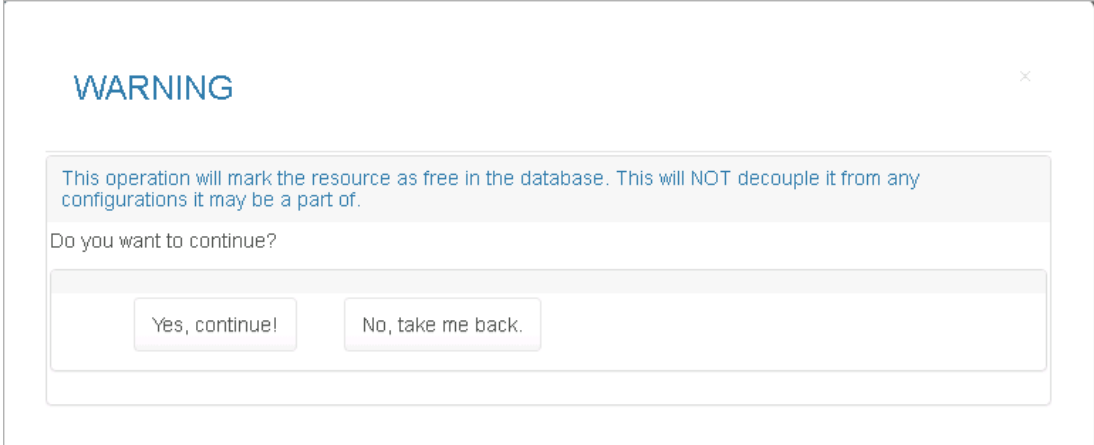
State:
Unavailable

Cloud:

Available Cancel

299733

- 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 3-13 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?

Yes, continue! No, take me back.

215549

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 3-14 Unallocate VLAN Screen

Unallocate VLAN ×

VLAN Info

Vlan ID:

Assignee

Tenant:

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 3-15 Remove VLAN Range Screen

The screenshot shows a dialog box titled "Remove VLAN Range". It has a close button in the top right corner. The dialog is divided into two main sections. The first section, "Range Information", contains two input fields: "Start" with the value "1521" and "End" with the value "1525". The second section, "Group & Region", contains two dropdown menus: "Group" set to "Infrastructure" and "Region" set to "Default Region 1". At the bottom of the dialog are two buttons: "Remove" and "Cancel". A mouse cursor is visible over the "Remove" button. On the right side of the dialog, there is a vertical text label "299735".

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, 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 management IP addresses use this pool.
Internet	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	Group of subnets used for DMZ VIPs. This pool uses Public IP addresses.

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 **must** be assigned to the Management Group and must be large enough to accommodate the required number of Cisco CSR 1000Vs.
- 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.
- 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

Table 3-2 Infrastructure Subnet Group

Subnet	IP address	Purpose
	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
	192.168.1.6-192.168.1.10	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. 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 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.

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 and unallocate public IP addresses 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 3-16 Address Pool Tab Screen

The screenshot displays the 'Address Pool' tab in the Cisco Datacenter Network interface. The main content area is titled 'cisco datacenter network' and features a navigation menu on the left. The 'Address Pool' tab is selected, showing a table of IPv4 subnets. The table has the following columns: Region, CustomerId, Subscriber, Network, Gateway, Group, Public, State, Allocated On, and Modified On. The table contains five rows of data, all with a 'Modified On' date of 6/14/2016 3:39:38 F. Below the table is a search bar and a pagination control showing '1 2 3'. At the bottom of the subnets section are 'Add' and 'Delete' buttons. Below that is an 'IP Address Pool' section with an empty input field and another 'Add' and 'Delete' buttons. A '+ NEW' button is at the bottom left, and a help icon is at the bottom right.

Region	CustomerId	Subscriber	Network	Gateway	Group	Public	State	Allocated On	Modified On
T3R1			10.0.51.0/24	10.0.51.253	Management	false	UnAllocated		6/14/2016 3:39:38 F
T3R1			10.5.16.0/22	10.5.19.253	SharedService	false	UnAllocated		6/14/2016 3:39:38 F
T3R1			12.1.1.0/24	12.1.1.253	Infrastructure	true	UnAllocated		6/14/2016 3:39:38 F
T3R1			11.1.1.0/24	11.1.1.253	NAT	true	UnAllocated		6/14/2016 3:39:38 F
T3R1			10.6.0.0/24	10.6.0.253	Infrastructure	false	UnAllocated		6/14/2016 3:39:38 F

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:

- **Region**—The associated Region.
- **Subscriber**—The name of the tenant.
- **Network**—Subnet number in CIDR 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)

- 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 3-17 IP Address Pool Table Screen

IP-address	State	Assignee	Allocated-On	Modified-On
12.1.1.0.71	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.72	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.73	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.74	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.75	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.76	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.77	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.78	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.79	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.80	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.81	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.82	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.83	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.84	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.85	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.86	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.87	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.88	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.89	UnAllocated			6/14/2016 3:39:38 PM
12.1.1.0.90	UnAllocated			6/14/2016 3:39:38 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 3-18 Add New IP Subnet Screen

- 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.

- Region—The Region 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 3-19 Delete IP Subnet Screen

The screenshot shows a 'Delete IP Subnet' dialog box with the following fields and values:

- Subnet Information:** Version: 1
- Owner Information:** Public: Own By Tenant:
- Network Information:** Network Address: 10.6.0.0, Subnet Mask: / 24, Gateway: 10.6.0.253
- Group & Region:** Group: Infrastructure, Region: T3R1
- Assignee:** Tenant ID: (empty dropdown)

Buttons: Delete, Cancel

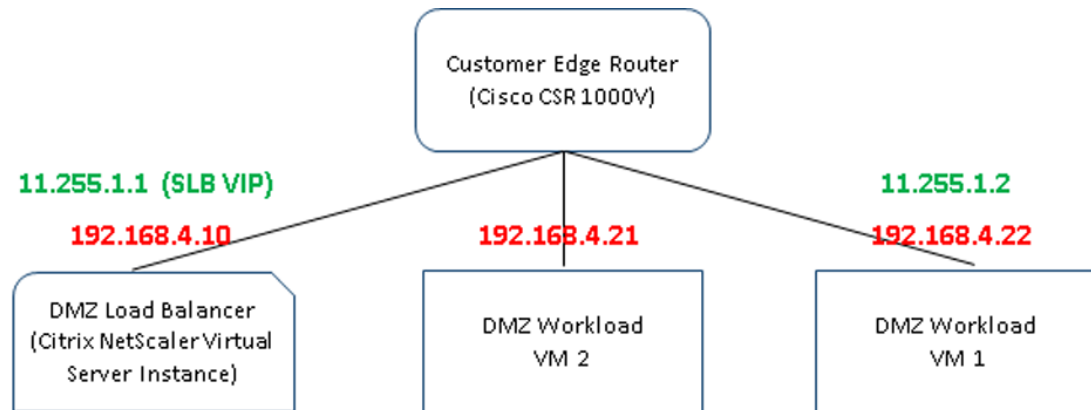
Step 2 Click **Delete** to delete the subnet or **Cancel** to cancel the deletion.

Understanding the Allocation of Public IP Addresses to Tenants

The DMZ tier is a perimeter network inside a tenant's container which is securely separated from the other interior networks of the container. The DMZ tier hosts applications and is accessible from the public Internet and other external networks having connectivity to the container edge.

To enable real-time inbound communication from the public Internet to the tenant's private cloud DMZ tier, you can allow tenant-administered servers to be addressable on the public Internet. You can create pools of unallocated (unassigned) public IP addresses. Then, as needed, you can allocate (assign) these public IP addresses to tenants. Tenants can map the allocated public IP addresses to private IP addresses within their DMZ tiers, including any DMZ Load Balancer VIP and any Workload VM addresses. Mapping directs inbound traffic from a public IP address to a private DMZ address. [Figure 3-20](#) illustrates this concept. Tenants can also unmap addresses.

Figure 3-20 Mapping Public IP Addresses to Private DMZ IP Addresses



Public IP Addresses – Mapped by the tenant

Private IP Addresses – Assigned by Cisco CNAP or SCVMM

415163

For example, a tenant might create a workload VM on the DMZ tier and want access to it from the Internet, in which case the tenant will request a public IP address, which you can provide from the VIP pool. The tenant can then map the workload VM address to the public IP address you allocated to the tenant.

For more information about the VIP Group of subnets used for DMZ VIPs, see [Important Considerations When Configuring Address Pools](#).

Allocating Public IP Addresses to a Tenant

To allocate public IP addresses to a tenant:

-
- Step 1** On the Address Pool tab, locate the VIP public IP subnet with the unallocated IP addresses you want to allocate and click it. You see the following screen showing the Unallocated IP Addresses in the selected subnet.

Figure 3-21 Unallocated IP Addresses

The screenshot displays the 'Address Pool' section of the Cisco Cloud Network Automation Provisioner. The interface is divided into a left-hand navigation menu and a main content area. The main content area is titled 'IPv4' and contains two tables: 'Subnets' and 'IP Address Pool'.

Subnets Table:

Region	CustomerId	Subscriber	Network	Gateway	Group	Public	State	Allocated On	Modified On
T3R1			11.6.1.0/24	11.6.1.253	VIP	true	UnAllocated		9/13/2016 11:16:01
T3R1			10.5.11.0/22	10.5.11.253	Internet	false	UnAllocated		9/13/2016 11:16:01
T3R2			10.0.123.0/24	10.0.123.253	Management	false	UnAllocated		9/13/2016 11:16:01
T3R2			12.6.1.0/24	12.6.1.253	Infrastructure	true	UnAllocated		9/13/2016 11:16:01
T3R2			10.6.250.0/24	10.6.250.253	Infrastructure	false	UnAllocated		9/13/2016 11:16:01

IP Address Pool Table:

IP-address	State	Assignee	Allocated-On	Modified-On
11.6.1.71	UnAllocated			9/14/2016 10:52:49 AM
11.6.1.72	UnAllocated			9/14/2016 10:53:05 AM
11.6.1.73	UnAllocated			9/14/2016 10:53:19 AM
11.6.1.74	UnAllocated			9/14/2016 10:53:33 AM
11.6.1.75	UnAllocated			9/14/2016 10:53:52 AM
11.6.1.76	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.77	UnAllocated			9/13/2016 11:16:01 AM

Step 2 At the bottom of the screen, click **Allocate**. You see the following screen.

Figure 3-22 Allocate IP Subnet

The screenshot shows a dialog box titled 'Allocate IP Subnet'. The dialog box contains a section for 'Public IP Address Allocation' with two input fields: 'Tenant' and '# of IP Addresses'. Below the input fields are two buttons: 'Allocate' and 'Cancel'.

- Step 3** Use the pull-down menu to select the tenant to which you want to assign IP addresses and enter the number of IP address you want to assign. Click **Allocate**. You see the following screen with the IP address allocated.

Figure 3-23 IP Addresses Allocated

The screenshot displays the Cisco Cloud Network Automation Provisioner interface. The left sidebar contains navigation options such as ALL ITEMS, CISCO DATACENTER NET..., WEB SITE CLOUDS, VM CLOUDS, SERVICE BUS CLOUDS, SQL SERVERS, MYSQL SERVERS, AUTOMATION, TEAM ACCESS CONTROL, PLANS, USER ACCOUNTS, REQUEST MANAGEMENT, SHINE CLOUD SECURITY, and USER COSTS. The main content area is titled 'IPv4' and shows two tables: 'Subnets' and 'IP Address Pool'.

Subnets Table:

Region	CustomerId	Subscriber	Network	Gateway	Group	Public	State	Allocated On	Modified On
T3R1			11.6.1.0/24	11.6.1.253	VIP	true	UnAllocated		9/13/2016 11:16:01
T3R1			10.5.11.0/22	10.5.11.253	Internet	false	UnAllocated		9/13/2016 11:16:01
T3R2			10.0.123.0/24	10.0.123.253	Management	false	UnAllocated		9/13/2016 11:16:01
T3R2			12.6.1.0/24	12.6.1.253	Infrastructure	true	UnAllocated		9/13/2016 11:16:01
T3R2			10.6.250.0/24	10.6.250.253	Infrastructure	false	UnAllocated		9/13/2016 11:16:01

IP Address Pool Table:

IP-address	State	Assignee	Allocated-On	Modified-On
11.6.1.71	Allocated	cmat_mcsr@cisco.com		9/13/2016 11:16:01 AM
11.6.1.72	Allocated	cmat_mcsr@cisco.com		9/13/2016 11:16:01 AM
11.6.1.73	Allocated	cmat_mcsr@cisco.com		9/13/2016 11:16:01 AM
11.6.1.74	Allocated	cmat_mcsr@cisco.com		9/13/2016 11:16:01 AM
11.6.1.75	Allocated	cmat_mcsr@cisco.com		9/13/2016 11:16:01 AM
11.6.1.76	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.77	UnAllocated			9/13/2016 11:16:01 AM

Unallocating Public IP Addresses from a Tenant

To unallocate a public IP address from a tenant:

- Step 1** Select the IP address you want to unallocate, then click **Unallocate** at the bottom of the screen, as shown in the following screen.

Figure 3-24 Unallocate IP Address

The screenshot shows the 'IP Address Pool' configuration page. On the left is a navigation menu with categories like 'ALL ITEMS', 'CISCO DATACENTER NET...', 'WEB SITE CLOUDS', 'VM CLOUDS', 'SERVICE BUS CLOUDS', 'SQL SERVERS', 'MYSQL SERVERS', 'AUTOMATION', 'TEAM ACCESS CONTROL', 'PLANS', 'USER ACCOUNTS', 'REQUEST MANAGEMENT', 'SNIPE CLOUD SECURITY', and 'USER COSTS'. The main content area shows a table of IP addresses. The IP address 11.6.1.71 is highlighted in blue. Below the table are buttons for 'Add', 'Delete', 'Allocate IP', and 'Unallocate IP'. The 'Unallocate IP' button is highlighted in blue.

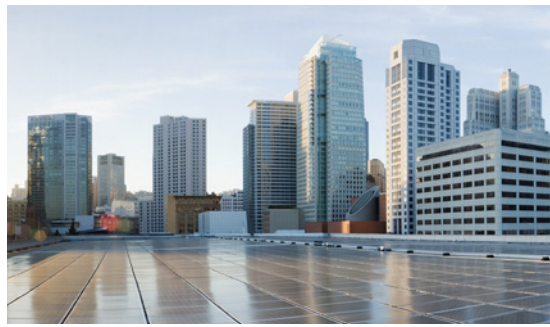
IP-address	State	Assignee	Allocated-On	Modified-On
11.6.1.71	Allocated	cmat_mcsr@cisco.com		9/13/2016 11:16:01 AM
11.6.1.72	Allocated	cmat_mcsr@cisco.com		9/13/2016 11:16:01 AM
11.6.1.73	Allocated	cmat_mcsr@cisco.com		9/13/2016 11:16:01 AM
11.6.1.74	Allocated	cmat_mcsr@cisco.com		9/13/2016 11:16:01 AM
11.6.1.75	Allocated	cmat_mcsr@cisco.com		9/13/2016 11:16:01 AM
11.6.1.76	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.77	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.78	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.79	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.80	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.81	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.82	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.83	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.84	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.85	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.86	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.87	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.88	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.89	UnAllocated			9/13/2016 11:16:01 AM
11.6.1.90	UnAllocated			9/13/2016 11:16:01 AM

You see the following screen asking you to confirm that you want to unallocate the IP address from the specified tenant.

Figure 3-25 Unallocate Confirmation

The screenshot shows a confirmation dialog box with the text: "Are you sure you want to unallocate the IP address 11.6.1.71 from this tenant 'cmat_mcsr@cisco.com'?". There are two buttons: "YES" with a checkmark icon and "NO" with an "X" icon. The "YES" button is highlighted in blue.

Step 2 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

- In this release, CNAP allows two types of Zinc containers: single Cisco CSR 1000V (non-redundant) or dual Cisco CSR 1000Vs (redundant).
- Cisco CNAP also supports a model wherein a single tenant, such as an agency in a government or a department in an enterprise, can instantiate a multi-Zinc container for the purpose of horizontal scale out. You can view this as a single, multi-redundant Cisco CSR 1000V container construct or as a case of “inter-container” routing.

This allows users within a single organization to:

- Scale out their network performance through the provisioning of additional Cisco CSR 1000V routers.
- Allocate Cisco CSR 1000Vs and the associated workload subnets to specific applications.
- Allocate Cisco CSR 1000Vs according to departments or work groups within an organization.

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

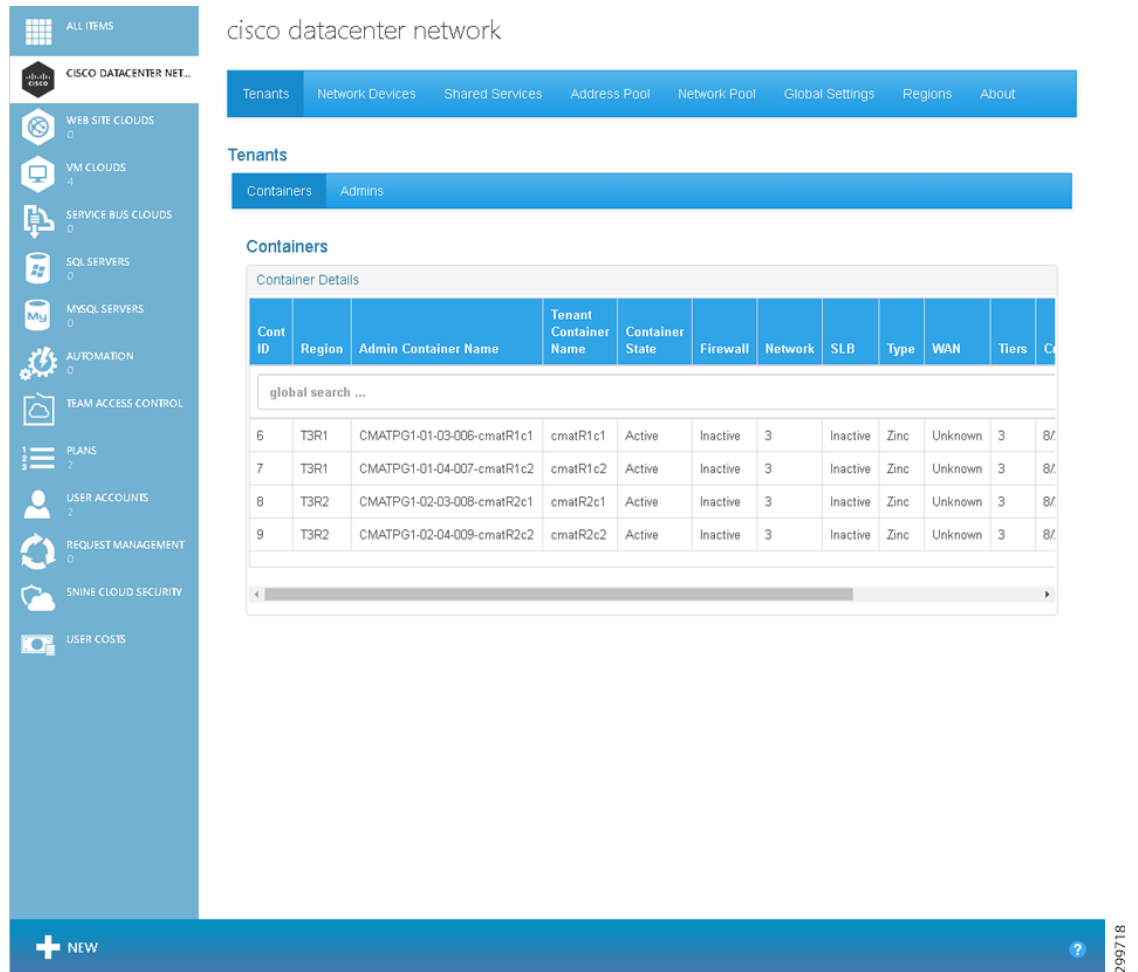
Once a container plan is created, customers can use the Tenant Portal to subscribe to any of the available public container plans. For more information, see *Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Tenant Portal Guide, Release 2.1*.

Creating a Network and Virtual Machine Cloud Container Plan

To create a network and virtual machine cloud container plan:

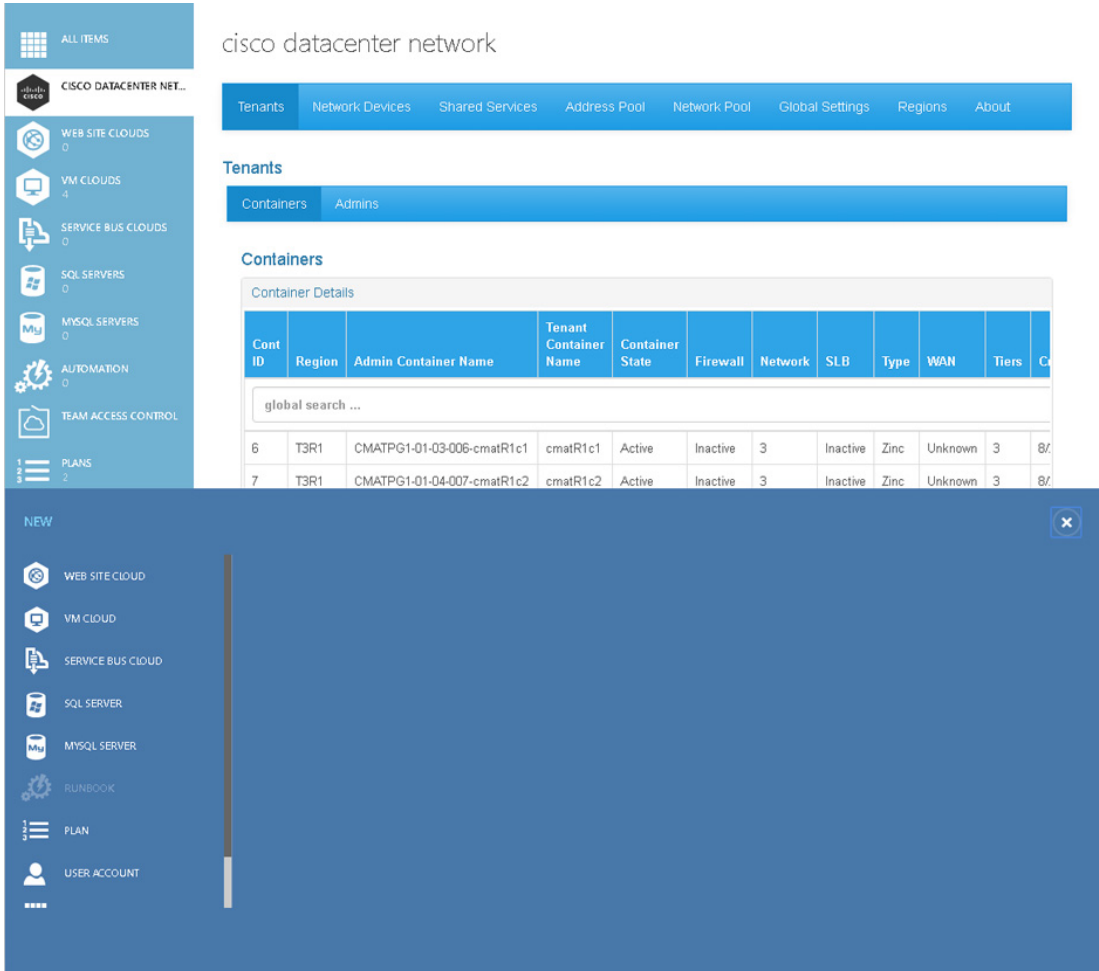
-
- Step 1** On the Tenants Tab screen, click + **New** in the lower left corner, as shown in the following screen. You can also click **PLANS** on the main WAP screen.

Figure 4-1 Tenants Tab Screen—Containers



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



Step 2 Click Plan.

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

299750

Figure 4-3 Plan Creation Options Screen

The screenshot displays the 'cisco datacenter network' interface. The top navigation bar includes tabs for Tenants, Network Devices, Shared Services, Address Pool, Network Pool, Global Settings, Regions, and About. The 'Tenants' tab is selected, showing a 'Tenant Administrators' table with columns for Tenant ID, Tenant Admin, Customer Name, Created On, and Modified On. A search bar is present above the table.

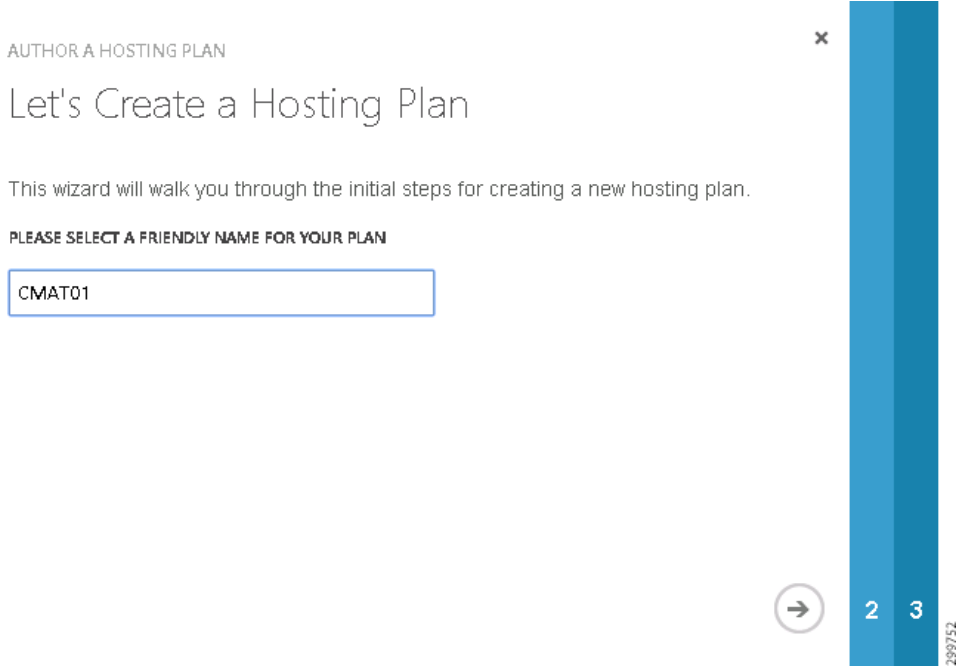
Tenant ID	Tenant Admin	Customer Name	Created On	Modified On
1	cmat@cisco.com	cmat_cisco_com	2016-08-26T14:27:02.757	2016-08-26T14:27:02.757
2	cmat_mcsr@cisco.com	CMATPG1	2016-08-29T17:00:03.457	2016-08-29T17:00:03.457

The 'NEW' pop-up window is titled 'Author a Hosting Plan' and contains two main options: 'CREATE PLAN' and 'CREATE ADD-ON'. The 'CREATE PLAN' option is highlighted.

Step 3 Click **Create Plan**.

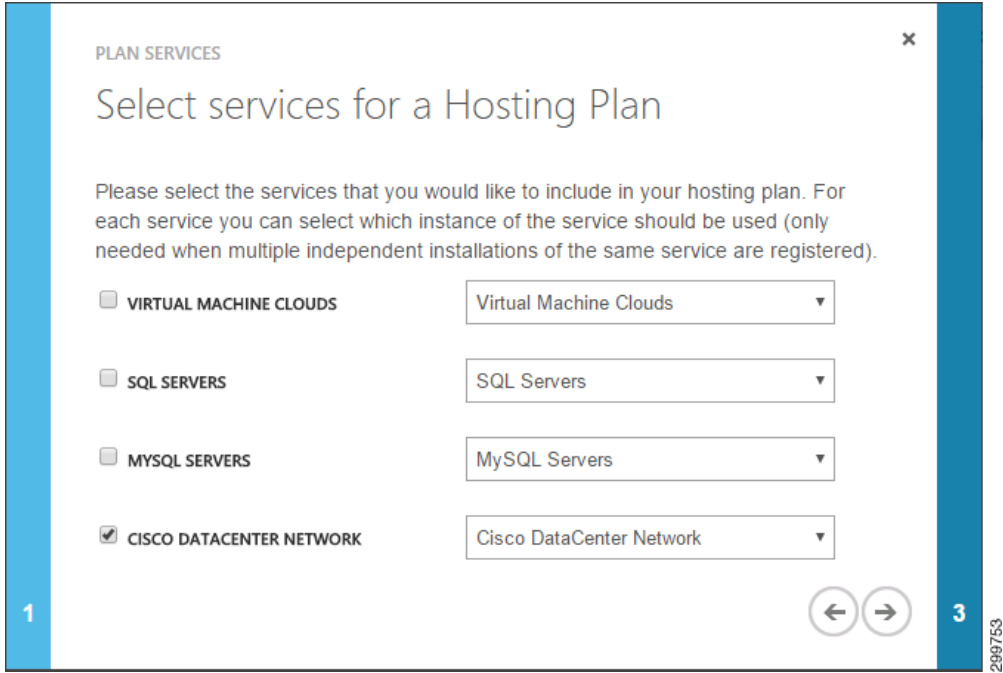
You see a pop-up window, as shown in the following screen.

Figure 4-4 Create a Hosting Plan Screen



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.

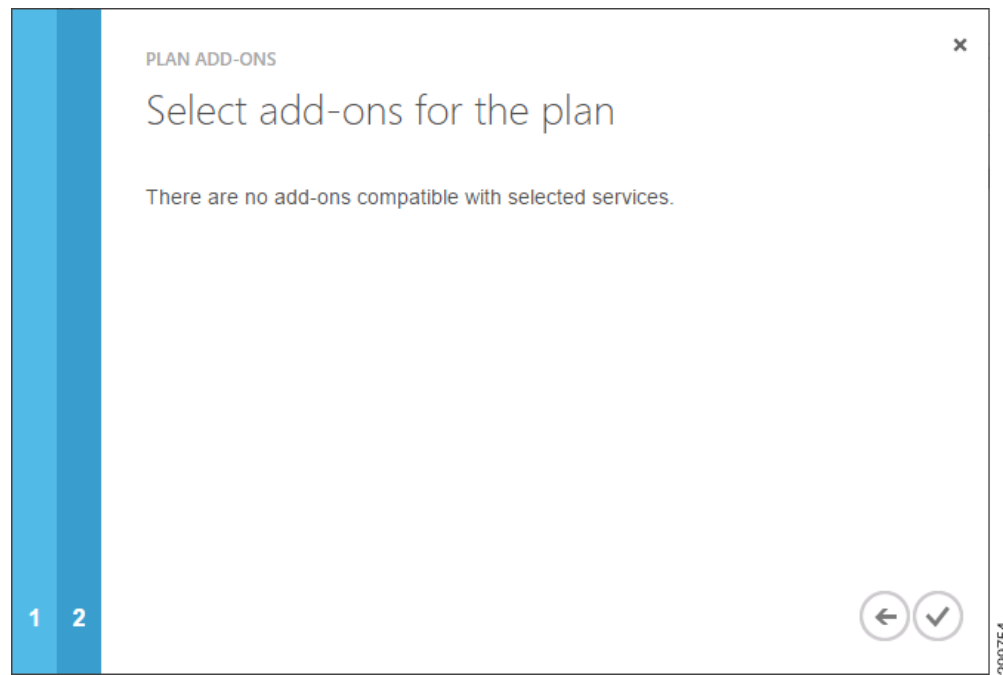
Figure 4-5 Select Services Screen



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

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

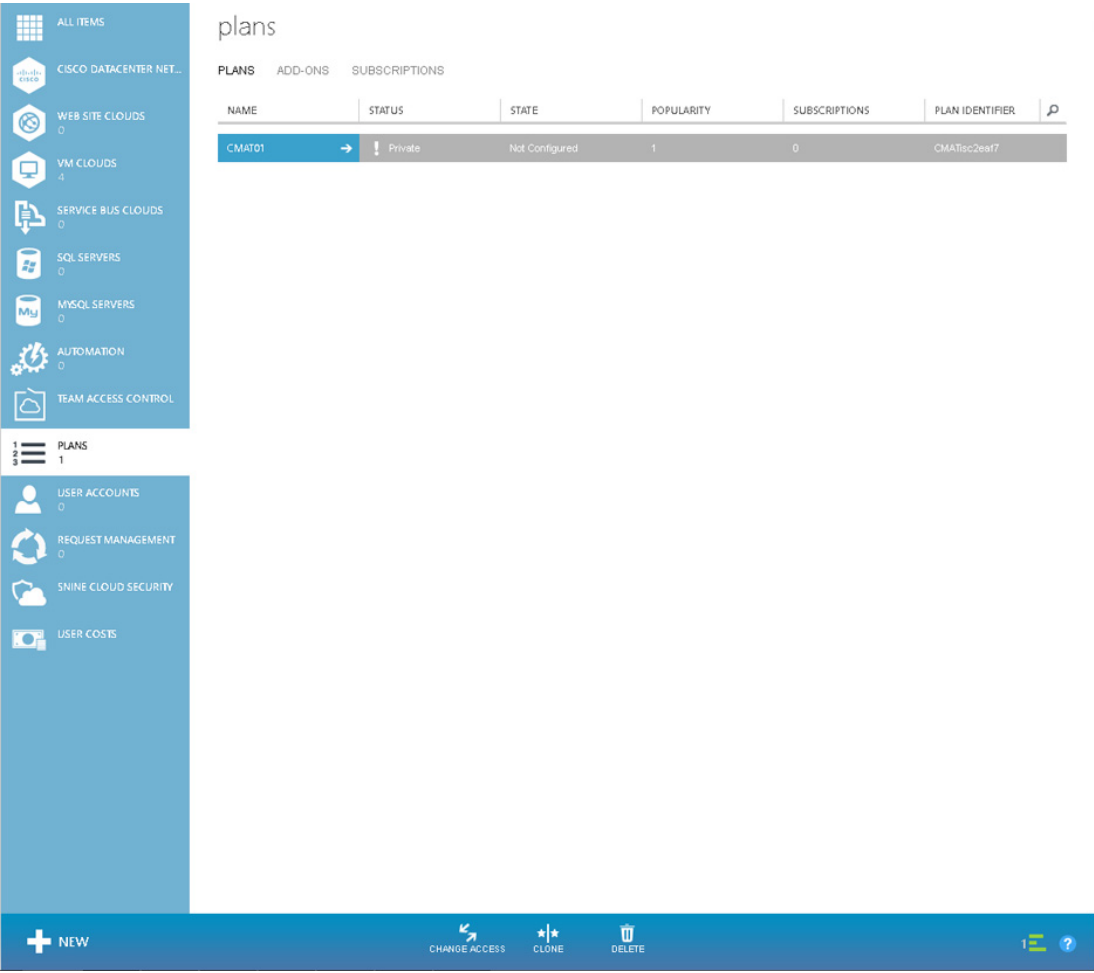
Figure 4-6 *Select Add-Ons Screen*



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



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

cmat01

DASHBOARD SUBSCRIPTIONS SETTINGS ADVERTISE

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

✓ DAILY SIGN UP COUNT ✓ TOTAL SIGN UP COUNT RELATIVE 7 DAYS ↻

Aug 20	Aug 21	Aug 22	Aug 23	Aug 24	Aug 25	Aug 26	Aug 27
						0	

plan services

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

add-ons

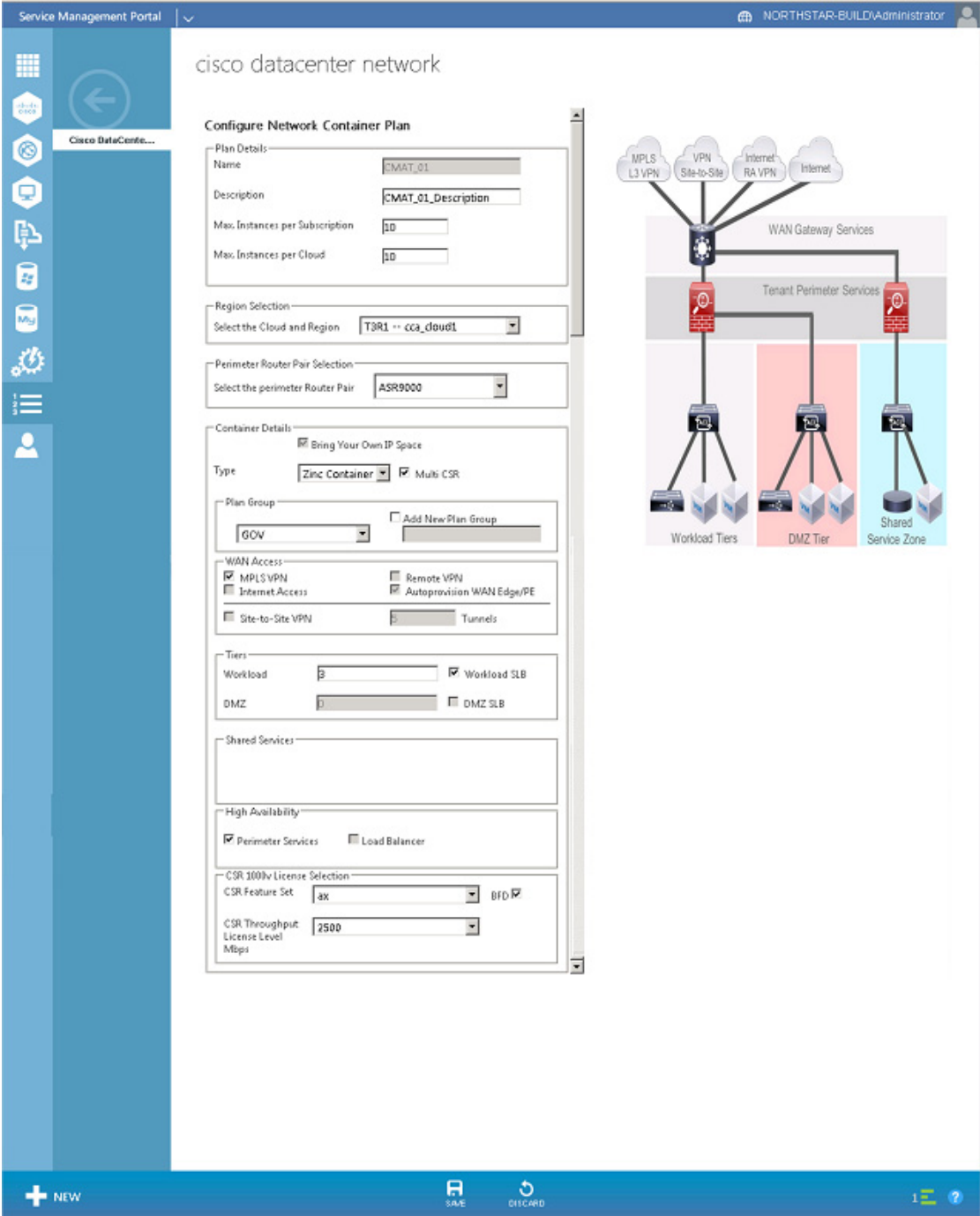
There are no add-ons linked to this plan. [Link an add-on.](#)

NEW CHANGE ACCESS CLONE DELETE PLAN LINK ADD-ON ADD SERVICE REMOVE SERVICE

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



- Step 9** Complete the various fields to create a network container:
- Enter Plan Details about the container:
 - Name—Enter a descriptive name for the container.
 - Customer Service ID—Used as part of the naming convention that is collected when creating a plan and can also be used to associate subnets with Customer Service IDs.
 - Description—Enter a description for the container.

- Maximum Instances per Subscription—1-100
- Maximum Instances per Cloud—1-2500
- Region Selection—Select the region(s) with which the container will be associated.
- Perimeter Router Pair Selection—Select the perimeter router pair from the pull-down menu.
- Specify Container Details:
 - Bring Your Own IP Space (BYoIP)—BYoIP allows Tenant administrators to assign their own preferred address space (subnet) to each of the Workload Tiers within a Tenant container. They are isolated from other Container Groups and other Tenants, allowing the Tenant’s Enterprise Network to use the container and access each of the Tiers as per the firewall policy. Each Tier within a Container Group must have its own unique address space (subnet) to prevent conflicts within the container. To function properly the address space must not conflict with the Tenant’s Enterprise Network address space.

**Note**

When Multi-CSR is selected, BYoIP is **required** and does not have to be selected. When Multi-CSR is not selected, BYoIP is **not** supported. In this release, Multi-CSR is **preselected**.

- Type—**Zinc Container** is supported in the current release.
- Multi CSR—**Preselected** in this release. For more information, see [Types of Container Plans](#)
- WAN Access—Specify the type of WAN Access: MPLS VPN, Site-to-Site VPN, or Internet Access. Remote VPN is not available in the current release.

**Note**

Autoprovision WAN Edge/PE, which provisions the Data Center Provider Edge Router with Tenant VRF and L3VPN configurations, is **preselected** in this release. For more information, see [Understanding the Difference Between Auto-provisioning and Manually Provisioning WAN Gateways in Chapter 5, “Managing Container Plans.”](#)

- Tiers: Workload and DMZ—Three (3) Workload Tiers and one (1) DMZ Tier are available in the current release.
- 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. 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.

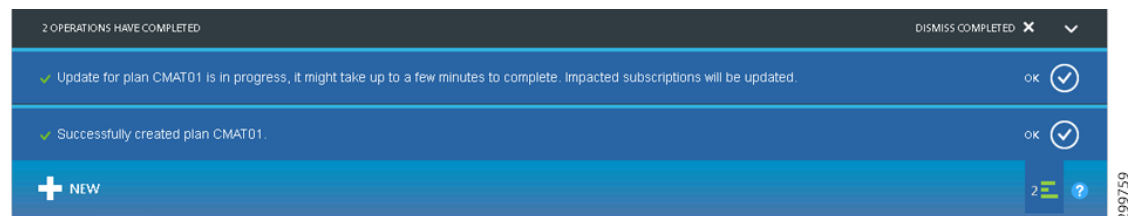
- CSR 1000V License Selection—First select the CSR Feature Set using the pull-down menu, then select the CSR Throughput Level using the pull-down menu. The options available on the CSR Throughput Level pull-down menu depend on what you selected for the CSR Feature Set.

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, at the bottom of the screen click **Save**.

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

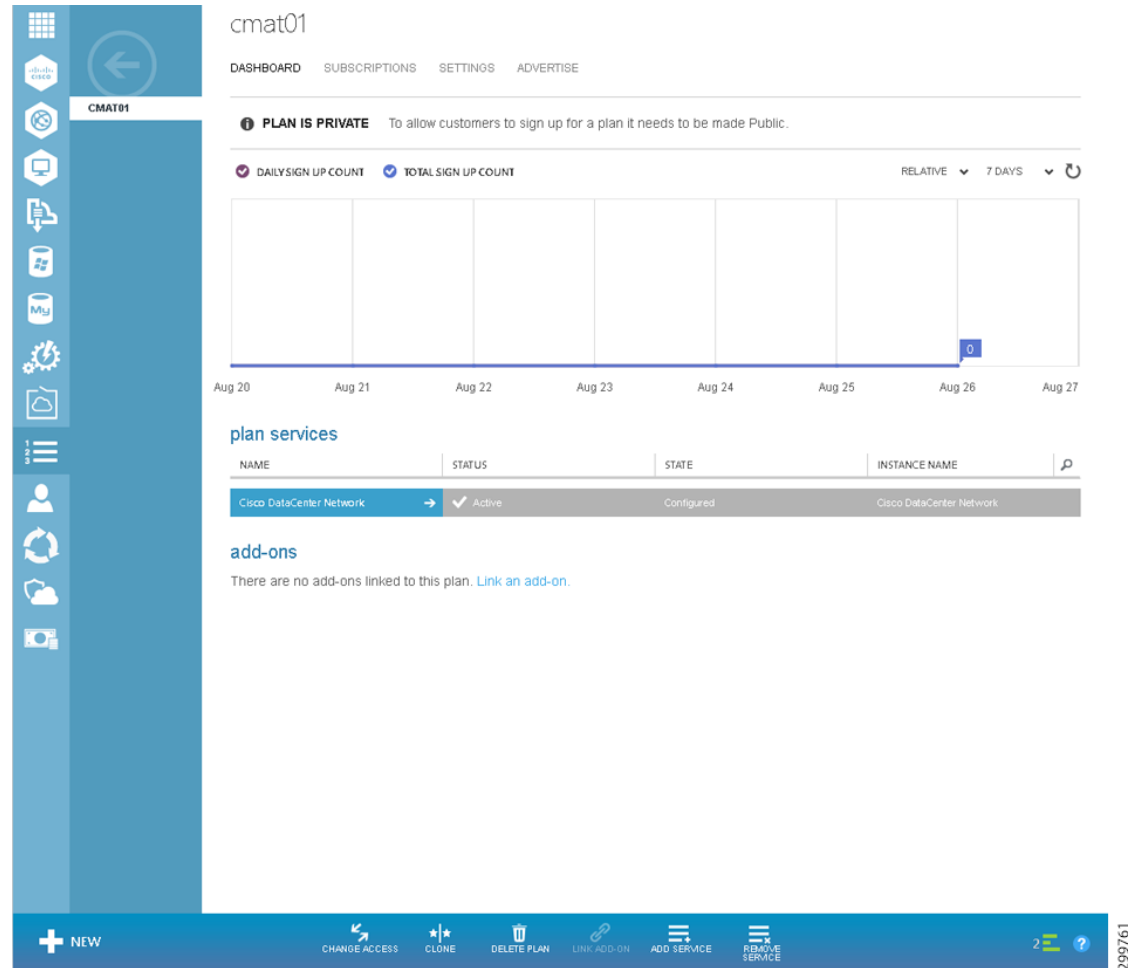
Figure 4-10 Configure Network Container Plan Screen—Update in Progress



Step 11 When the message disappears, click the back arrow (<–) at the top left.

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

Figure 4-11 Plan Detail Screen—Plan Active and Configured

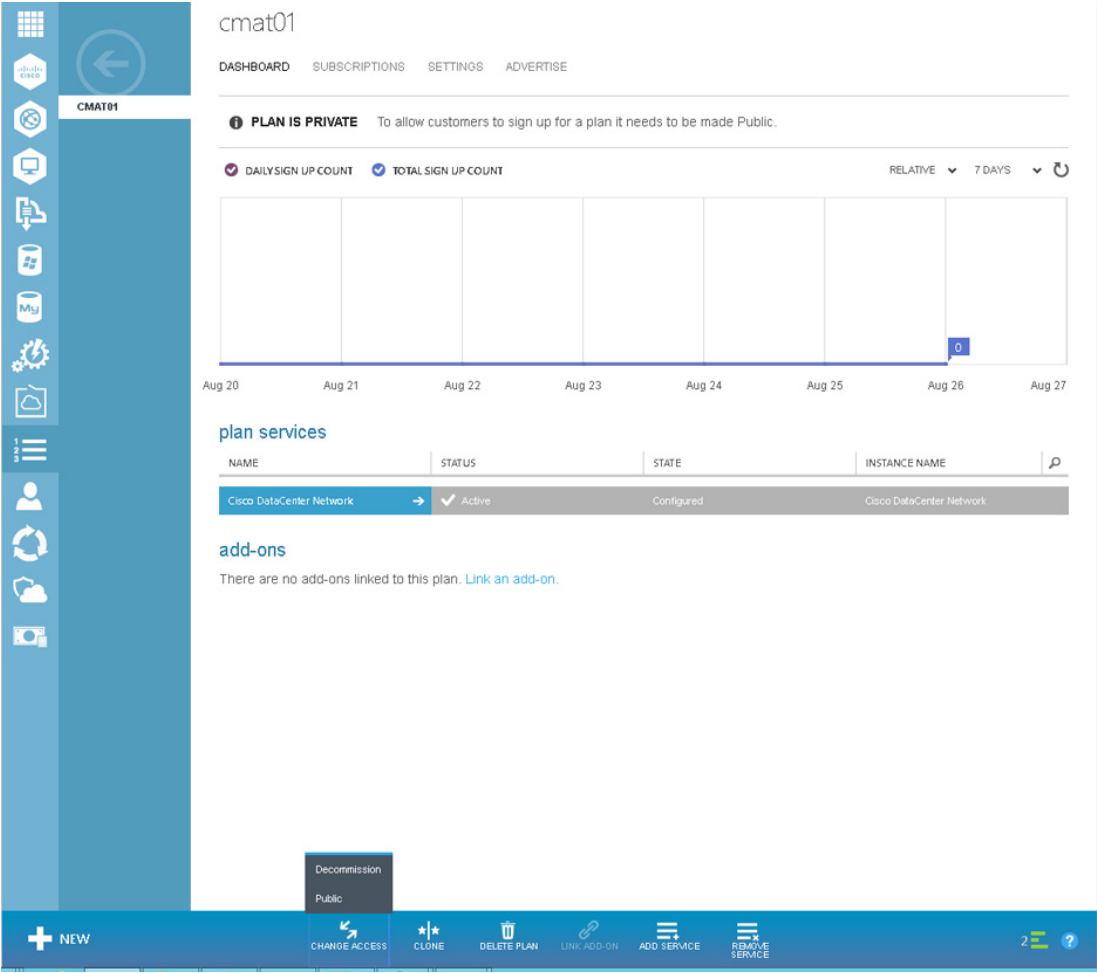


Step 12 As shown at the top, the **PLAN IS PRIVATE**. To make it public so tenants can subscribe to it, at the bottom of the screen click **Change Access** and then **Public**, as shown in the following screen.



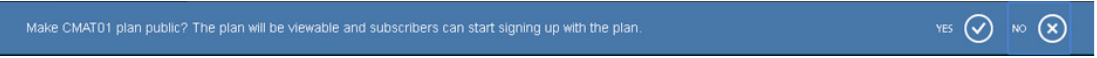
Note You can leave the plan Private and then manually assign tenants to the plan.

Figure 4-12 Change Access to Public Screen



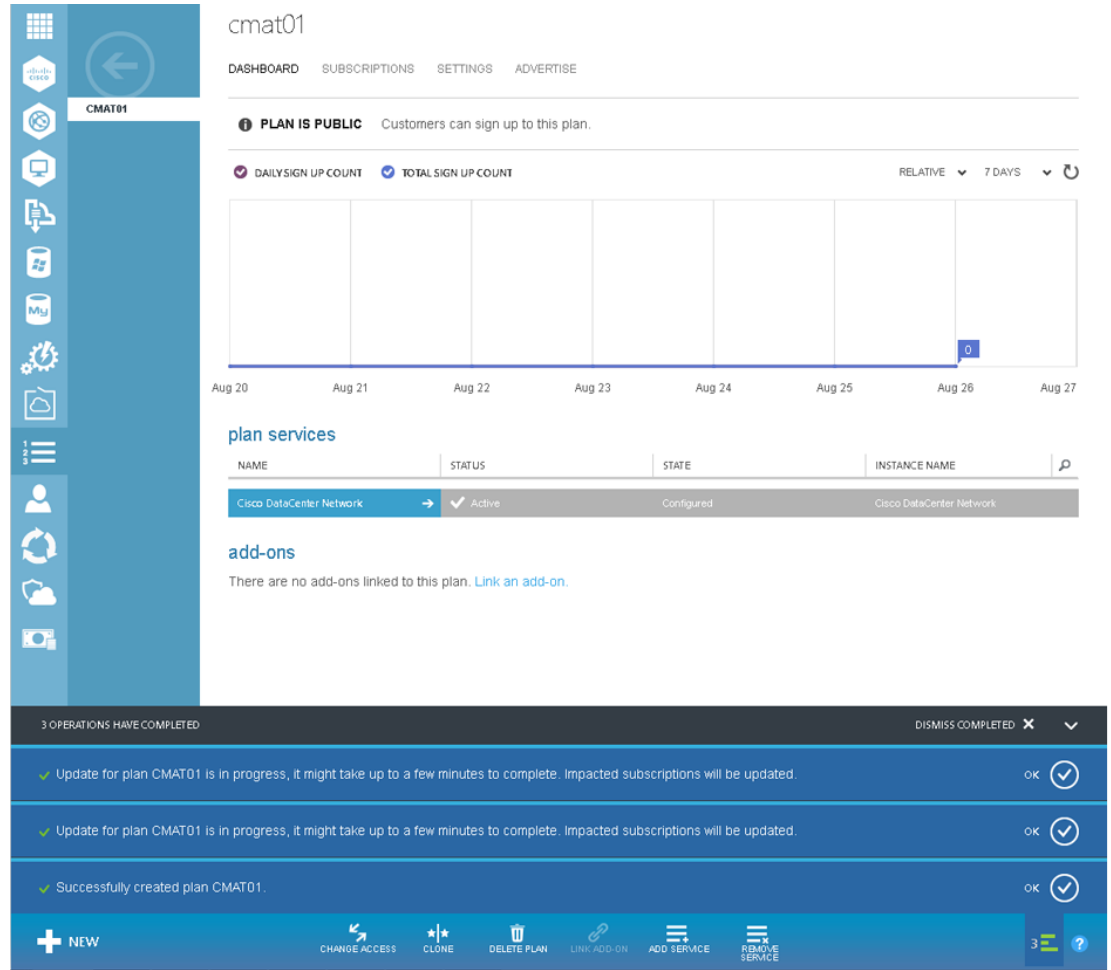
Step 13 You see a pop-up asking you to confirm you want the plan to be public, as shown in the following screen. Click Yes.

Figure 4-13 Confirm Public Access Screen



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

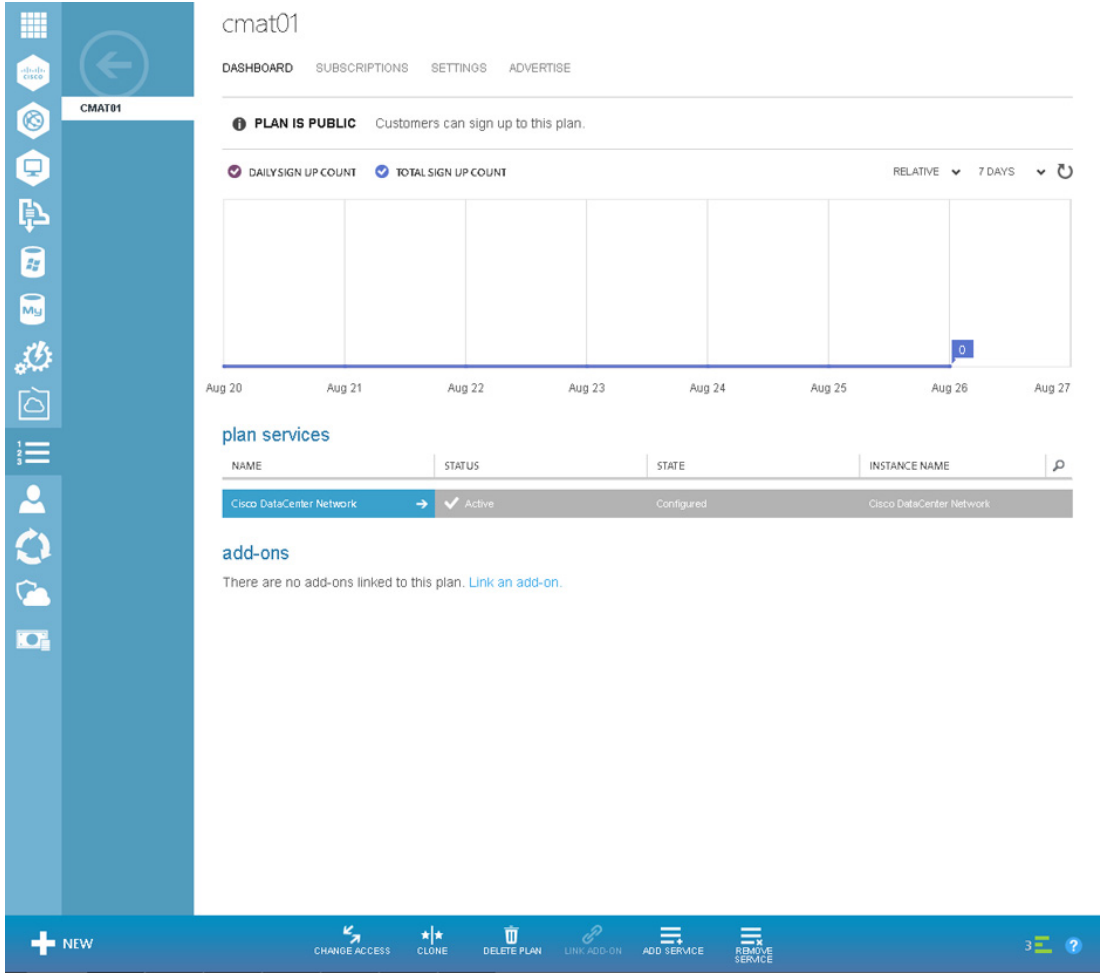
Figure 4-14 Change Access to Public Screen – Update in Progress



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

299764

Figure 4-15 Plan is Public Screen



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 containers and tenant administrators
- 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).
 - 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.



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 2.1*.

Viewing Summary Information about Containers and Tenant Administrators

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

Figure 5-1 Tenants Tab Screen—Containers

cisco datacenter network

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

Tenants

Containers Admins

Containers

Container Details

Cont ID	Region	Admin Container Name	Tenant Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	C
6	T3R1	CMATPG1-01-03-006-cmatR1c1	cmatR1c1	Active	Inactive	3	Inactive	Zinc	Unknown	3	8/
7	T3R1	CMATPG1-01-04-007-cmatR1c2	cmatR1c2	Active	Inactive	3	Inactive	Zinc	Unknown	3	8/
8	T3R2	CMATPG1-02-03-008-cmatR2c1	cmatR2c1	Active	Inactive	3	Inactive	Zinc	Unknown	3	8/
9	T3R2	CMATPG1-02-04-009-cmatR2c2	cmatR2c2	Active	Inactive	3	Inactive	Zinc	Unknown	3	8/

299718

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

- Cont ID—The ID of the container.
- Region—Name of the region to which the container is associated.
- Admin Container Name—Descriptive name of the container in the Admin Portal.
- Tenant Container Name—Descriptive name of the container in the Tenant Portal.
- 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.

The Admins tab under the Tenants tab displays a list of all the Tenant Administrators, as shown on the Tenants Tab—Admins screen.

Figure 5-2 *Figure Tenants Tab Screen—Admins*

The screenshot shows the Cisco Cloud Network Automation Provisioner interface. The left sidebar contains navigation options such as ALL ITEMS, CISCO DATACENTER NET., WEB SITE CLOUDS, VM CLOUDS, SERVICE BUS CLOUDS, SQL SERVERS, MYSQL SERVERS, AUTOMATION, TEAM ACCESS CONTROL, PLANS, USER ACCOUNTS, REQUEST MANAGEMENT, SNINE CLOUD SECURITY, and USER COSTS. The main content area is titled "cisco datacenter network" and includes a navigation bar with tabs for Tenants, Network Devices, Shared Services, Address Pool, Network Pool, Global Settings, Regions, and About. The "Tenants" tab is active, and the "Admins" sub-tab is selected. Below this, the "Tenant Administrators" section is displayed, featuring a search bar and a table with the following data:

Tenant ID	Tenant Admin	Customer Name	Created On	Modified On
1	cmat@cisco.com	cmat_cisco_com	2016-08-26T14:27:02.757	2016-08-26T14:27:02.757
2	cmat_mcsr@cisco.com	CMATPG1	2016-08-29T17:00:03.457	2016-08-29T17:00:03.457

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

- Tenant ID—The ID of the Tenant Administrator.
- Tenant Admin—The login credential of the Tenant Administrator.

- Customer Name—The name of the customer.
- Created On:—Displays the date and time when the Tenant Administrator was created.
- Modified On:—Displays the date and time when the Tenant Administrator was last modified.

Viewing Summary Information about a Specific 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 5-3 Tenants Tab—Container Selected

The screenshot shows the Cisco Cloud Network Automation Provisioner interface. The left sidebar contains a navigation menu with various categories like Web Site Clouds, VM Clouds, Service Bus Clouds, SQL Servers, MySQL Servers, Automation, Team Access Control, Plans, User Accounts, Request Management, SNINE Cloud Security, and User Costs. The main content area is titled "cisco datacenter network" and has a "Tenants" tab selected. Below the tabs, there is a "Containers" section with a table of container details. The table has columns for Cont ID, Region, Admin Container Name, Tenant Container Name, Container State, Firewall, Network, SLB, Type, WAN, Tiers, and C. The table contains four rows of data, with the first row highlighted in yellow.

Cont ID	Region	Admin Container Name	Tenant Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	C
6	T3R1	CMATPG1-01-03-006-cmatR1c1	cmatR1c1	Active	Inactive	3	Inactive	Zinc	Unknown	3	B/
7	T3R1	CMATPG1-01-04-007-cmatR1c2	cmatR1c2	Active	Inactive	3	Inactive	Zinc	Unknown	3	B/
8	T3R2	CMATPG1-02-03-008-cmatR2c1	cmatR2c1	Active	Inactive	3	Inactive	Zinc	Unknown	3	B/
9	T3R2	CMATPG1-02-04-009-cmatR2c2	cmatR2c2	Active	Inactive	3	Inactive	Zinc	Unknown	3	B/

You see the Tenants Summary screen.

Figure 5-4 Tenants Summary Screen

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.
- Region:—Displays the Region 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.
- 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 5-5 Summary Tab—WAN Gateway MPLS VPN Details

The screenshot shows the Summary Tab for a container named `CMATPG1-01-03-006-cmatR1c1`. The container is active and contains several resources:

Resource Name	Status	Count
WAN Gateways	Active	(1)
Firewalls	Active	(1)
Load Balancers	Inactive	(0)
Active Networks	Active	(3)

The WAN Gateway section shows details for the `MPLSVPN` gateway:

Property	Value
Container Name	cmatR1c1
Container Type	Zinc Container
Region	T3R1
Container Status	Active
Created On	Aug 29, 2016 5:05:53 PM
Modified On	Aug 30, 2016 8:35:01 AM

The WAN Gateway table includes the following information:

MPLSVPN	Status
CMATPG1-01-03-006-MplsVPN	Active

Additional details for the WAN Gateway:

Property	Value
Import RT	
Export RT	5-521
Route Descriptor	
VRF	CMATPG1-03
Primary IP	10.6.0.71
Secondary IP	10.6.0.72
Mask	255.255.255.0
Created On	Aug 30, 2016 8:33:28 AM
Modified On	Aug 30, 2016 8:35:01 AM

The Perimeter section shows details for the `Zone Based Firewall` and `Workload` resources:

Resource Name	Status
Zone Based Firewall: CMATPG1-01-03-006-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 5-6 Summary Tab—Perimeter Firewall Details

The screenshot displays the 'Summary Tab' for a container named 'cmatR1c1'. The interface includes a navigation sidebar on the left with categories like 'ALL ITEMS', 'WEB SITE CLOUDS', 'VM CLOUDS', 'SERVICE BUS CLOUDS', 'SQL SERVERS', 'MYSQL SERVERS', 'AUTOMATION', 'TEAM ACCESS CONTROL', 'PLANS', 'USER ACCOUNTS', 'REQUEST MANAGEMENT', 'SNINE CLOUD SECURITY', and 'USER COSTS'. The top navigation bar contains tabs for 'Tenants', 'Network Devices', 'Shared Services', 'Address Pool', 'Network Pool', 'Global Settings', 'Regions', and 'About'. The main content area shows the following details:

Container Details:

- Container Name: cmatR1c1
- Container Type: Zinc Container
- Region: T3R1
- Container Status: Active
- Created On: Aug 29, 2016 5:05:53 PM
- Modified On: Aug 30, 2016 8:35:01 AM

WAN Gateway Summary:

Category	Item	Status
MPLSVPN	CMATPG1-01-03-006-MplsVPN	Active
Site-to-Site VPN	Site-to-Site VPN	None

Perimeter Summary:

Category	Item	Status
Zone Based Firewall	CMATPG1-01-03-006-zbfb	Active
Primary IP	10.6.0.73	
Primary Mask	255.255.255.0	
Secondary IP	10.6.0.74	
Secondary Mask	255.255.255.0	
Created On	Aug 30, 2016 8:33:28 AM	
Modified On	Aug 30, 2016 8:33:28 AM	
Wokload	Tier 1	Online
Wokload	Tier 2	Online
Wokload	Tier 3	Online
Public	Public	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 5-7 Summary Tab—Perimeter Tier Details

The screenshot displays the Cisco Cloud Network Automation Provisioner interface. The left sidebar contains navigation options such as ALL ITEMS, CISCO DATACENTER NET., WEB SITE CLOUDS, VM CLOUDS, SERVICE BUS CLOUDS, SQL SERVERS, MYSQL SERVERS, AUTOMATION, TEAM ACCESS CONTROL, PLANS, USER ACCOUNTS, REQUEST MANAGEMENT, SNINE CLOUD SECURITY, and USER COSTS. The top navigation bar includes Tenants, Network Devices, Shared Services, Address Pool, Network Pool, Global Settings, Regions, and About. The main content area is titled 'Tenants' and shows 'Containers' and 'Admins' tabs. A dropdown menu for 'Containers' is set to 'CMATPG1-01-03-006-cmatR1c1'. Below this, there are tabs for 'Summary', 'Gateway', 'Firewall', and 'Load Balancer'. The 'Summary' tab is active, showing details for 'cmat_mcsr@cisco.com'. The details include: Container Name: cmatR1c1, Container Type: Zinc Container, Region: T3R1, Container Status: Active, Created On: Aug 29, 2016 5:05:53 PM, and Modified On: Aug 30, 2016 8:35:01 AM. To the right, there are statistics for WAN Gateways (1), Firewalls (1), Load Balancers (0), and Active Networks (3). Below the details, there are two main sections: 'WAN Gateway' and 'Perimeter'. The 'WAN Gateway' section shows 'MPLSVPN' with 'CMATPG1-01-03-006-MplsVPN' (Active) and 'Site-to-Site VPN' (None). The 'Perimeter' section shows 'Zone Based Firewall' with 'CMATPG1-01-03-006-zbfbw' (Active). Underneath, there are three workload tiers: Tier 1 (Online), Tier 2 (Online), and Tier 3 (Online). Each tier has a 'Workload Segment 1' with IP address, Created On, and Modified On dates. The 'Public' section is shown as '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



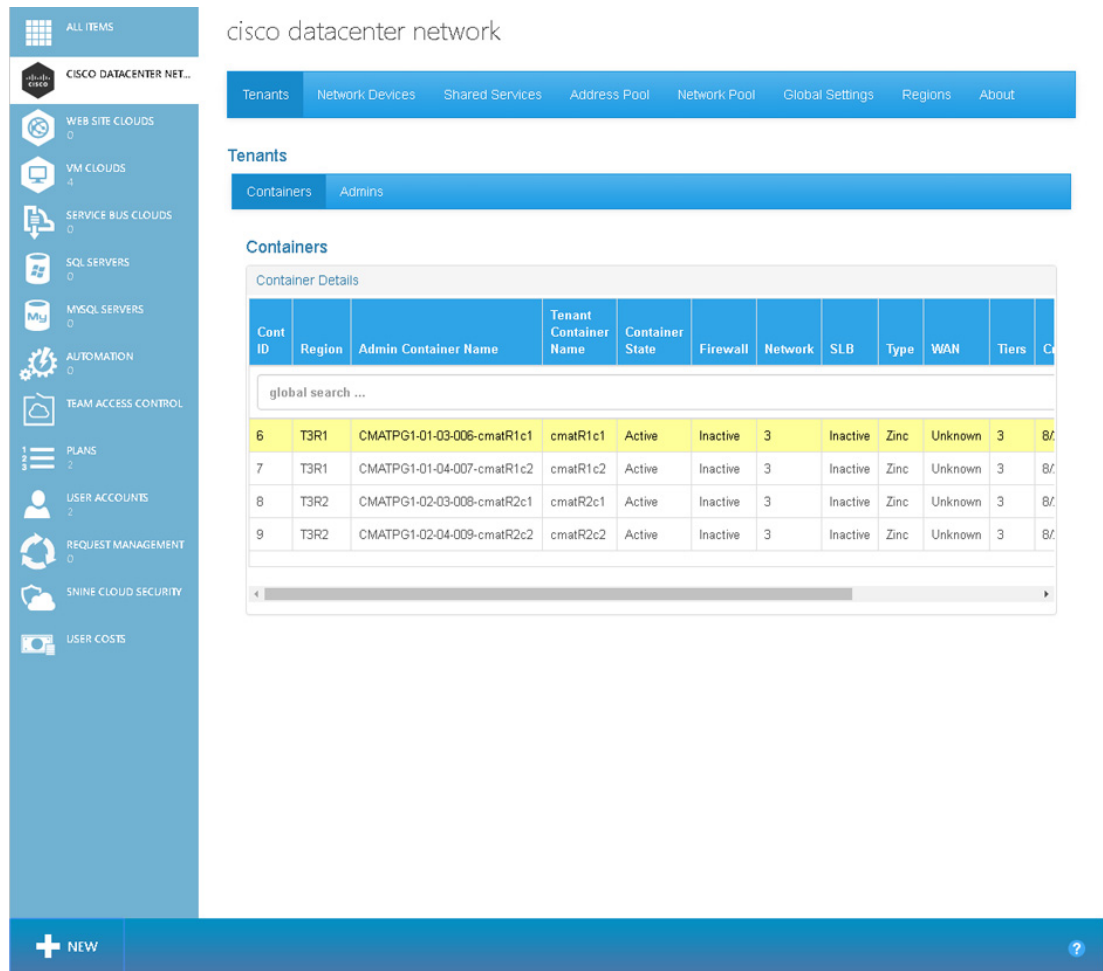
Note

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 5-8 Tenants Tab—Container Selected



You see the Tenants Summary screen.

299789

Figure 5-9 Tenants Summary Screen

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 5-10 Confirm Container Deletion

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 one option:

- Automated provisioning of MPLS L3VPN-based access for the tenant, including provisioning of the Data Center WAN Edge/PE.



Note

For single CSR containers, which are not supported in this release, there is an option for 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:

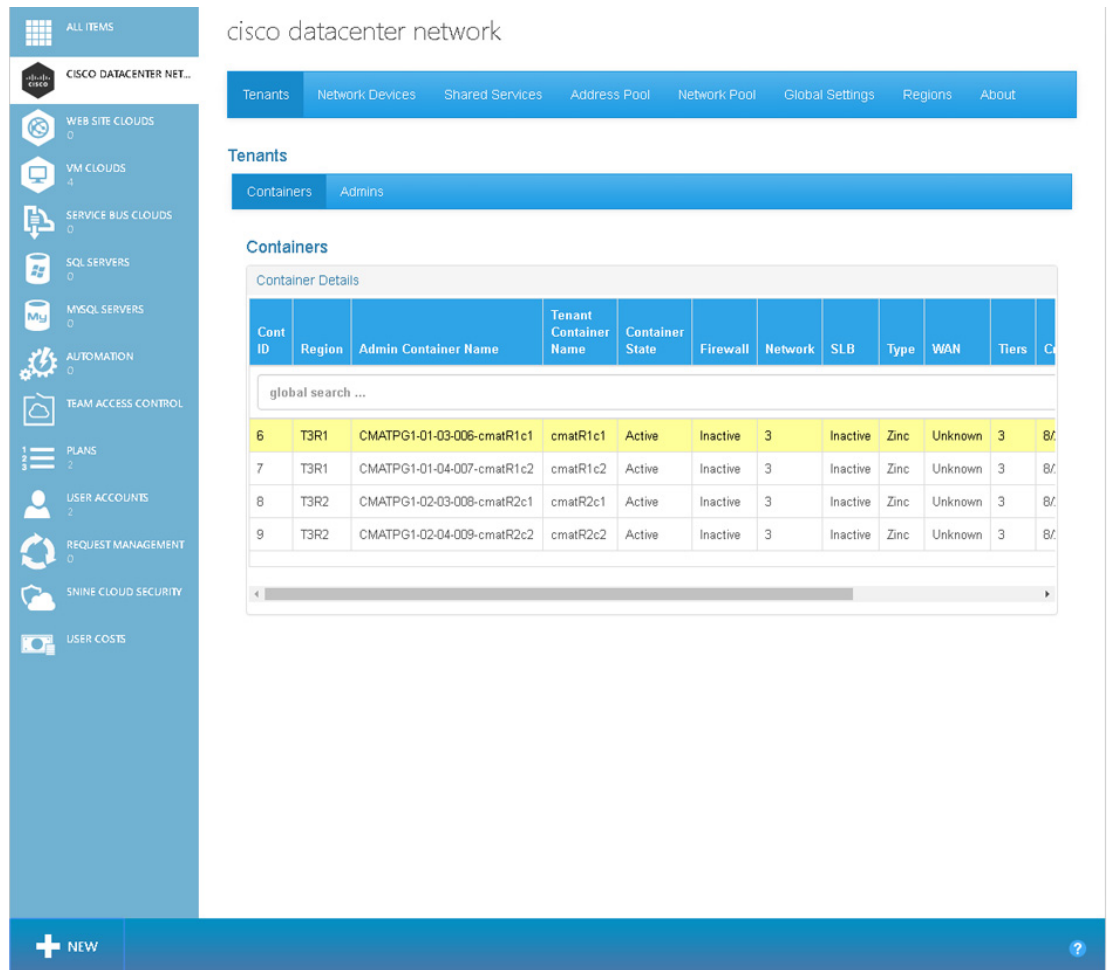
- Look at information about a gateway.
- Add a gateway.

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.

- 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 5-11 Tenants Tab—Container Selected Screen



You see the Tenants Summary screen.

Figure 5-12 Tenants Summary Screen

The screenshot displays the 'Tenants Summary Screen' for a tenant named 'cisco datacenter network'. The interface includes a left-hand navigation menu with categories like 'ALL ITEMS', 'WEB SITE CLOUDS', 'VM CLOUDS', 'SERVICE BUS CLOUDS', 'SQL SERVERS', 'MYSQL SERVERS', 'AUTOMATION', 'TEAM ACCESS CONTROL', 'PLANS', 'USER ACCOUNTS', 'REQUEST MANAGEMENT', 'SHINE CLOUD SECURITY', and 'USER COSTS'. The main content area shows the tenant's details and configuration options.

Tenants Summary:

- Container Name: cmatR1c1
- Container Type: Zinc Container
- Region: T3R1
- Container Status: Active
- Created On: Aug 29, 2016 5:05:53 PM
- Modified On: Aug 30, 2016 8:35:01 AM

WAN Gateway:

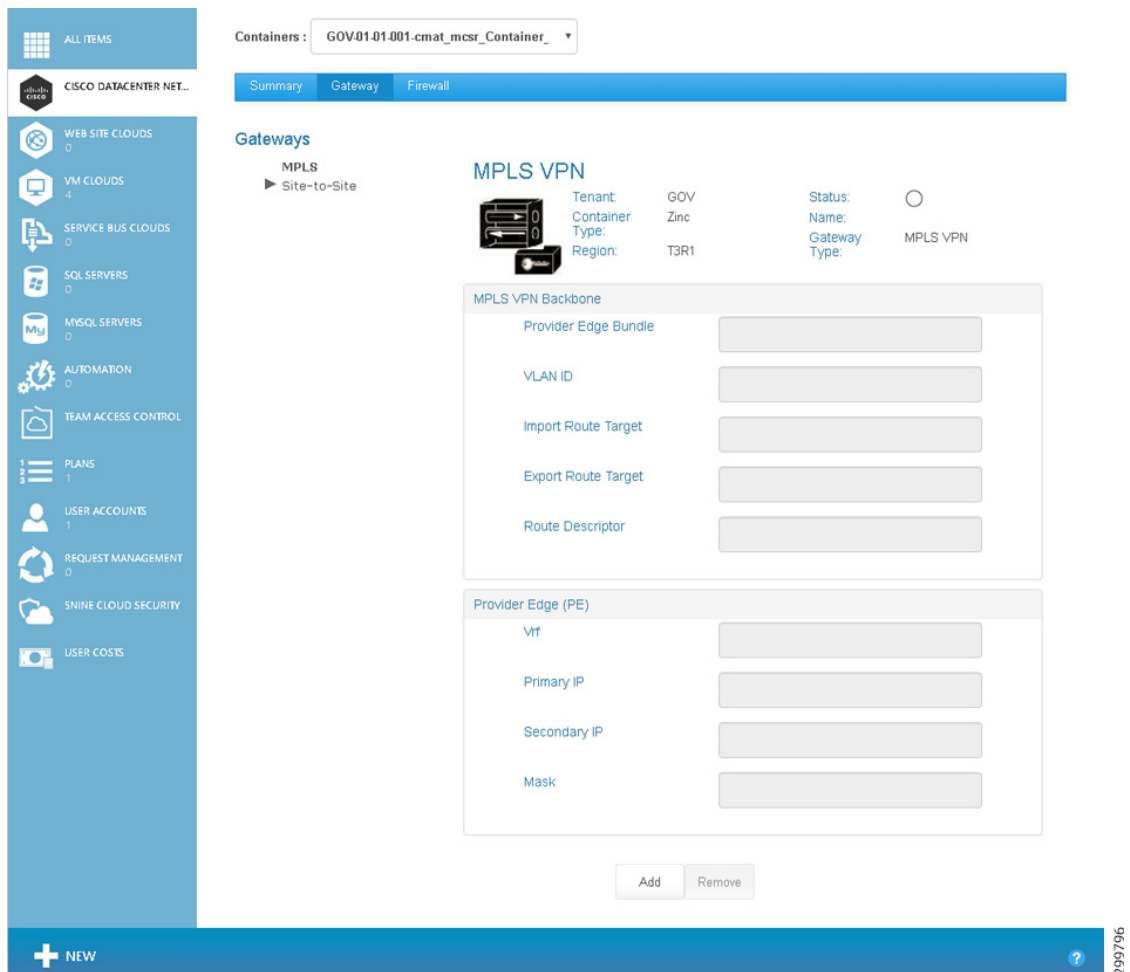
- MPLSVPN: CMATPG1-01-03-006-MplsVPN (Active)
- Site-to-Site VPN: None

Perimeter:

- Zone Based Firewall: CMATPG1-01-03-006-zbfbw (Active)
- Wkload Tier 1: Online
- Wkload Tier 2: Online
- Wkload Tier 3: Online
- Public: Inactive

- Step 2** Click the **Gateway** tab.
You see the Tenant Gateway screen.

Figure 5-13 Tenant Gateway Screen



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.
- Region:—Displays the Region 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

**Note**

This distinction only applies to single CSR containers, which are not supported in this release.

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.

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
- Internet Access—Set up by a tenant in the Tenant Portal.
- Remote Access VPN—Not available in the current release.

Setting up a MPLS WAN Gateway

The information you enter is different depending on whether during container creation you specified you wanted Cisco CNAP to **Autoprovision WAN Edge/PE**. (This distinction only applies to single CSR containers, which are not supported in this release.)

To set up a MPLS 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 MPLS WAN Gateway, as shown in the following screen.

Figure 5-14 Tenants Tab—Container Selected Screen

The screenshot displays the 'cisco datacenter network' interface. The top navigation bar includes 'Tenants', 'Network Devices', 'Shared Services', 'Address Pool', 'Network Pool', 'Global Settings', 'Regions', and 'About'. Below this, the 'Tenants' section is active, showing a sub-tab for 'Containers'. The main content area is titled 'Containers' and features a 'Container Details' table. The table has columns for Cont ID, Region, Admin Container Name, Tenant Container Name, Container State, Firewall, Network, SLB, Type, WAN, Tiers, and C. The table contains four rows of data, with the first row highlighted in yellow. A search bar is located above the table.

Cont ID	Region	Admin Container Name	Tenant Container Name	Container State	Firewall	Network	SLB	Type	WAN	Tiers	C
6	T3R1	CMATPG1-01-03-006-cmatR1c1	cmatR1c1	Active	Inactive	3	Inactive	Zinc	Unknown	3	B/
7	T3R1	CMATPG1-01-04-007-cmatR1c2	cmatR1c2	Active	Inactive	3	Inactive	Zinc	Unknown	3	B/
8	T3R2	CMATPG1-02-03-008-cmatR2c1	cmatR2c1	Active	Inactive	3	Inactive	Zinc	Unknown	3	B/
9	T3R2	CMATPG1-02-04-009-cmatR2c2	cmatR2c2	Active	Inactive	3	Inactive	Zinc	Unknown	3	B/

You see the Tenants Summary screen.

Figure 5-15 Tenants Summary Screen

Step 2 Click the **Gateway** tab.



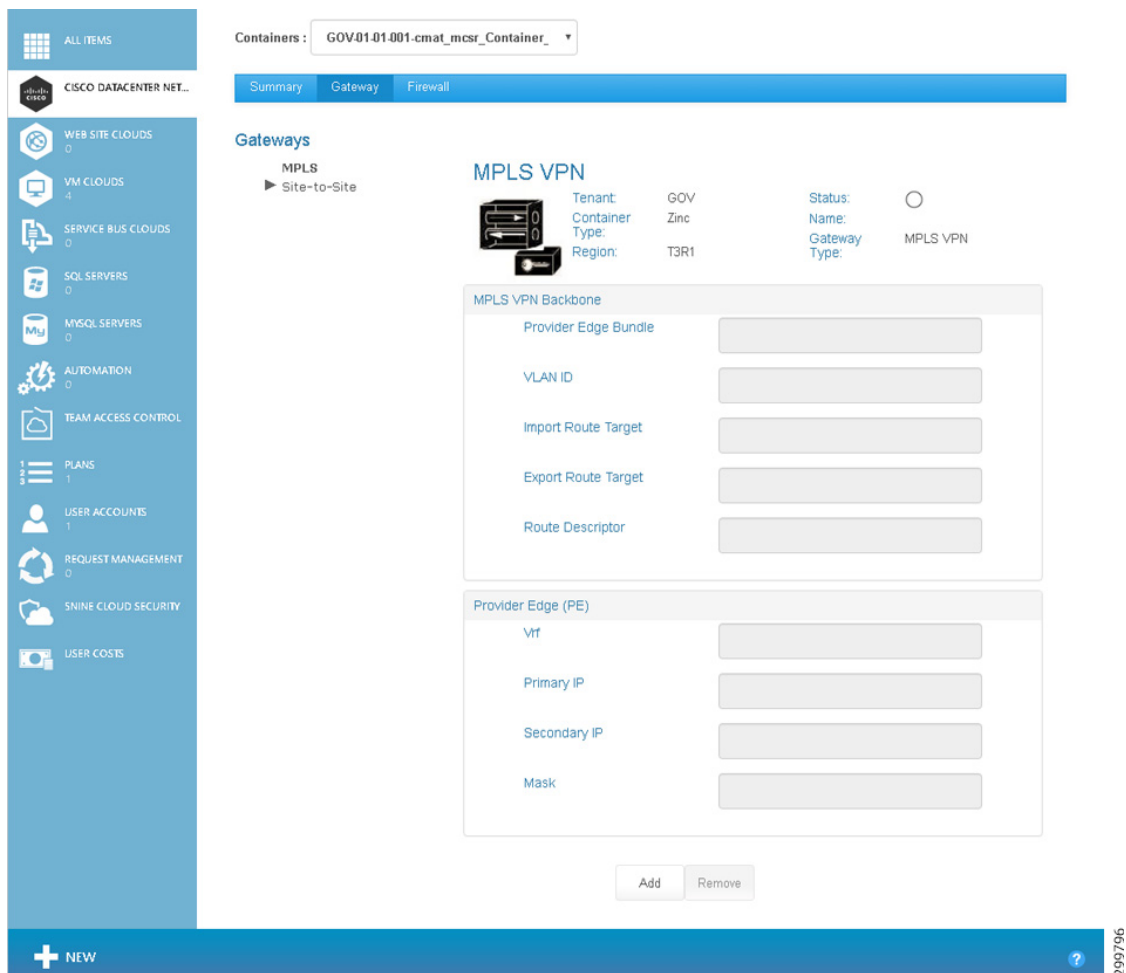
Note

The specific Tenant Gateway screen you see depends on whether or not during container creation you specified **Autoprovision WAN Edge/PE**. (Note: This distinction only applies to single CSR containers, which are not supported in this release.)

The screens below show examples for MPLS.

Setting up an Auto-provisioned WAN Edge/PE

Figure 5-16 Tenant Gateway Screen—Auto-provision Provider Edge



Step 3 Click the **Add** button.

The route descriptor is auto-generated depending on the value of the RouteDescriptorPrefix global system setting, as well as the VLAN used. The RouteDescriptorPrefix setting accepts either:

- PeBundle—Uses the PE Bundle for this region.
- PeAutoSystemNumber—Uses the BGP Provider Edge AS number for this cloud.

The following screen shows a gateway being created with auto-populated values.

Figure 5-17 Gateway Creation

Setting up a Manually Provisioned WAN Edge/PE



Note

This distinction only applies to single CSR containers, which are not supported in this release.

Figure 5-18 Tenant Gateway Screen—Manual Provision Provider Edge

The screenshot displays the 'Manual Provision Provider Edge' configuration screen for a 'cmat03scsr WAN Gateway'. The interface includes a sidebar with navigation options like 'WEB SITE CLOUDS', 'VM CLOUDS', 'SERVICE BUS CLOUDS', 'SQL SERVERS', 'MSSQL SERVERS', 'AUTOMATION', 'TEAM ACCESS CONTROL', 'PLANS', 'USER ACCOUNTS', 'REQUEST MANAGEMENT', 'SNINE CLOUD SECURITY', and 'USER COSTS'. The main content area shows the gateway configuration details, including tenant information (cmat01scsr@cisco.com), container type (Zinc Container), and region (T3R1). The configuration fields are organized into two sections: 'MPLS VPN Backbone' and 'Provider Edge (PE)'. The 'MPLS VPN Backbone' section includes fields for Provider Edge Bundle, VLAN ID, Import Route Target, Export Route Target, and Route Descriptor. The 'Provider Edge (PE)' section includes fields for VRF, Primary IP, Secondary IP, and Mask. At the bottom, there are 'Add' and 'Remove' buttons.

- 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.
-

Setting up a Site-to-Site VPN

To set up Site-to-Site VPN:

-
- Step 1** Click the **Gateway** tab, then under Gateways, click **Site-to-Site**. You see the following screen.

Figure 5-19 Site-to-Site VPN Screen

The screenshot displays the 'Site To Site VPN' configuration page in the Cisco Cloud Network Automation Provisioner. The page is organized into several sections:

- Tenants:** A navigation bar at the top with tabs for 'Containers' and 'Admins'. Below it, a dropdown menu shows 'Containers: cma01Scs001'.
- Gateways:** A section with a 'Site-to-Site' link. To the right, a 'Site To Site VPN' card displays:
 - Container Name: cma01Sc1
 - Container Type: Zinc
 - Hosting Cloud: zinc_cloud
 - Status: Name:
- IKE Policy:** A form with three columns:
 - Encryption:** AES (dropdown)
 - Hash:** SHA (dropdown)
 - Keep Alive:** 10 (input field)
 - Retry:** 2 (input field)
 - Group:** Group 14 (dropdown)
- Authentication:** A form with:
 - Method:** Pre-Shared Key (dropdown)
 - Shared Key:** (input field)
- Transformation Set:** A form with:
 - ESP Encryption:** (dropdown, selected)
 - ESP Authentication:** (dropdown, selected)
 - AH:** (dropdown, unselected)

An 'Enable' button is located at the bottom right of the configuration area. The bottom of the page features a blue bar with a '+ NEW' button and a help icon.

Step 2 Complete the following fields:

- IKE Policy:
 - Encryption—Encryption used for the IKE proposal; used to ensure the secrecy of data during traffic flow: AES, DES, or Triple DES.
 - Hash—Specifies the hash algorithm within an IKE policy; used to authenticate data during traffic flow: MD5, SHA, or SHA256.
 - Keep Alive—Number of seconds during which traffic is not received from the peer before keep-alive messages are sent if there is data traffic to send.
 - Retry—Number of seconds between keep-alive packet retries if the keep-alive message fails.
 - Group—Specify which Diffie-Hellman Modulus Group to use.
- Authentication:
 - Method—Pre-Shared Key: Allow for a secret key to be shared between two peers for mutual authentication prior to tunnel activation.
 - Shared Key—The shared secret for authentication. The shared key must be configured and equal at each peer or the IKE SA cannot be established.
- Transformation Set: ESP Encryption Transform

- esp-des—ESP with the 56-bit Data Encryption Standard (DES) encryption algorithm (no longer recommended).
- esp-3des—ESP with the 168-bit DES encryption algorithm (3DES or Triple DES) (no longer recommended).
- esp-null—Null encryption algorithm.
- esp-aes—SP with the 128-bit Advanced Encryption Standard (AES) encryption algorithm.
- esp-aes-192—SP with the 192-bit Advanced Encryption Standard (AES) encryption algorithm.
- esp-aes-256—SP with the 256-bit Advanced Encryption Standard (AES) encryption algorithm.
- Transformation Set: ESP Authentication Transform
 - esp-md5-hmac—ESP with the MD5 (HMAC variant) authentication algorithm (no longer recommended).
 - esp-sha-hmac—ESP with the SHA (HMAC variant) authentication algorithm.
- Transformation Set: Ah Transform
 - ah-md5-hmac—AH with the MD5 (Message Digest 5) (an HMAC variant) authentication algorithm (no longer recommended).
 - ah-sha-hmac—AH with the SHA (Secure Hash Algorithm) (an HMAC variant) authentication algorithm.

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

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”.

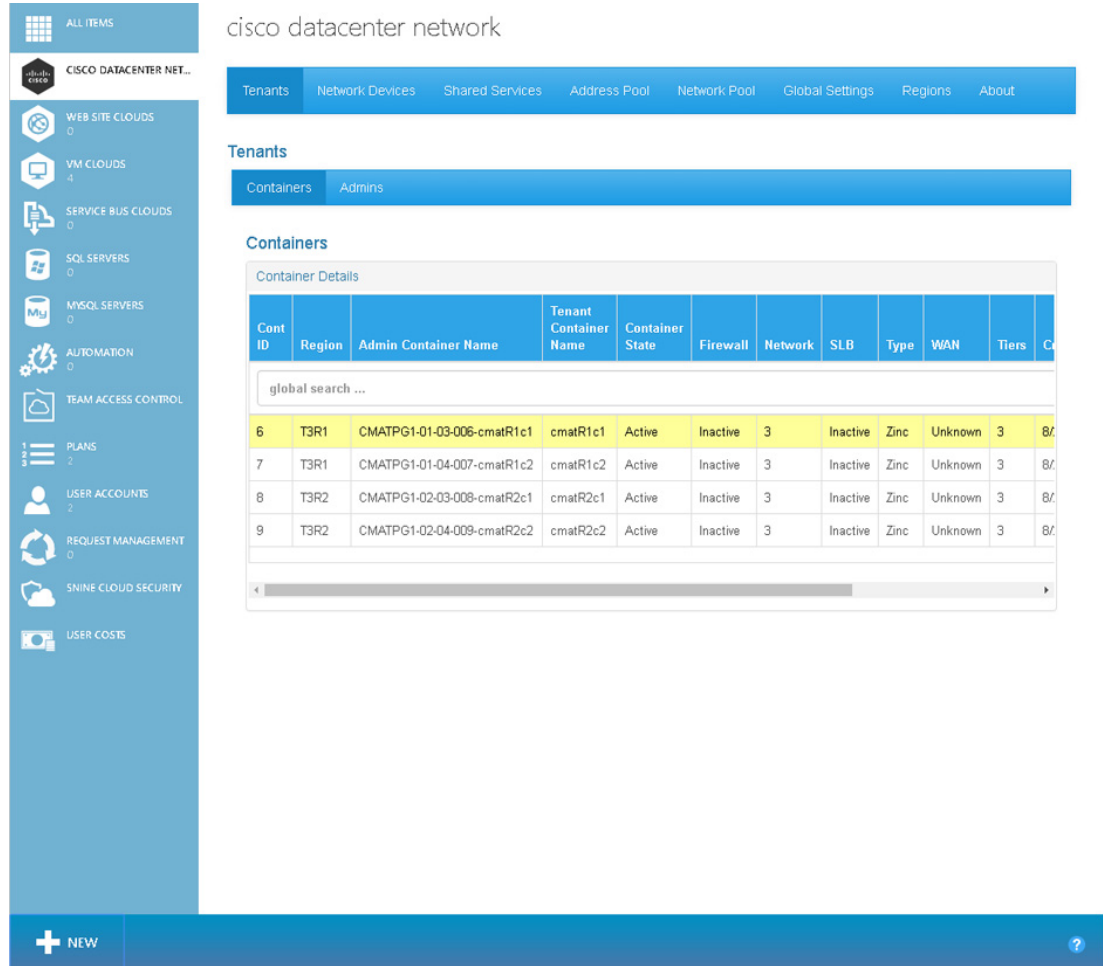
For detailed information on the base firewall configuration, see: *Cisco Cloud Architecture for the Microsoft Cloud Platform: Zinc Container Configuration Guide, Release 1.0*

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.

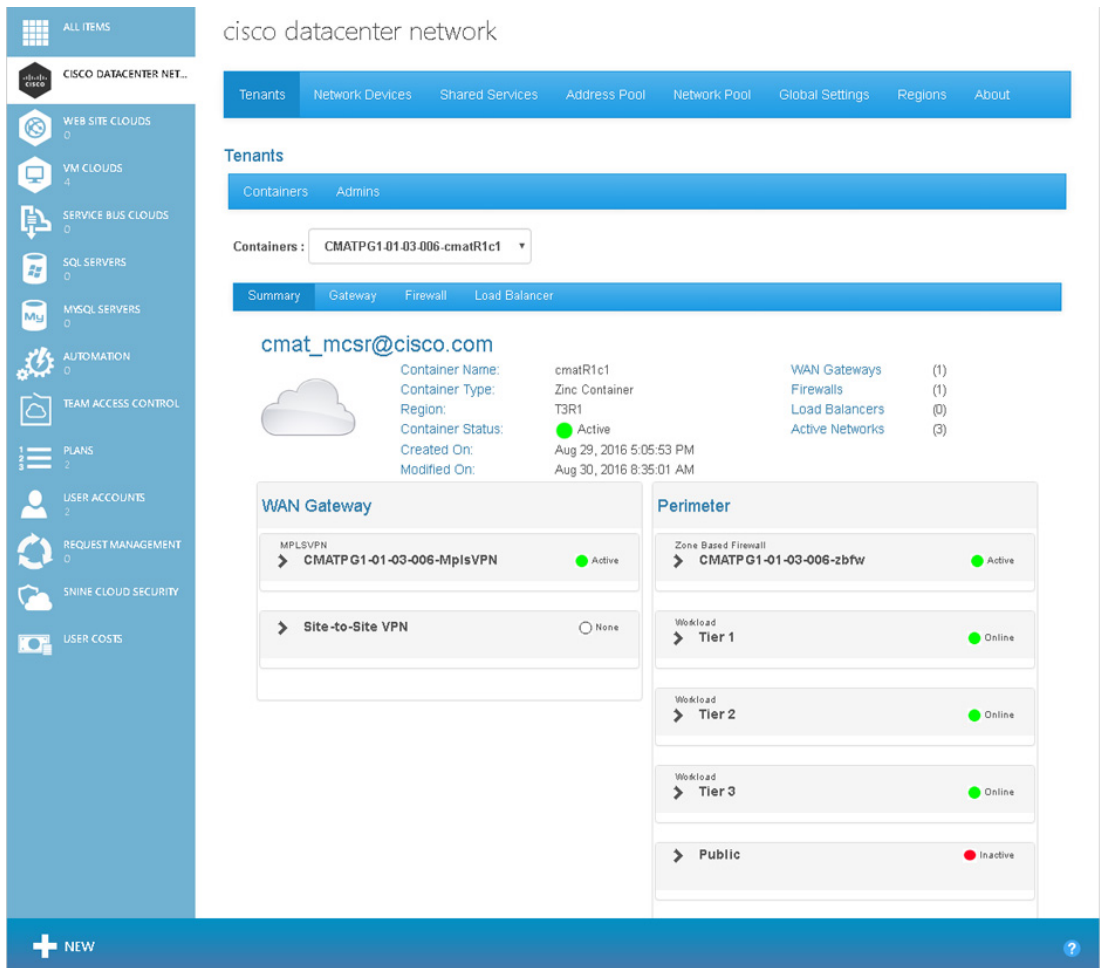
Figure 5-20 Tenants Tab Screen—Container Selected



You see the Tenants Summary screen.

299789

Figure 5-21 Tenants Summary Screen



Step 2 Click the **Firewall** tab.
 You see the Tenant Firewall screen.

Figure 5-22 Tenant Firewall Screen

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

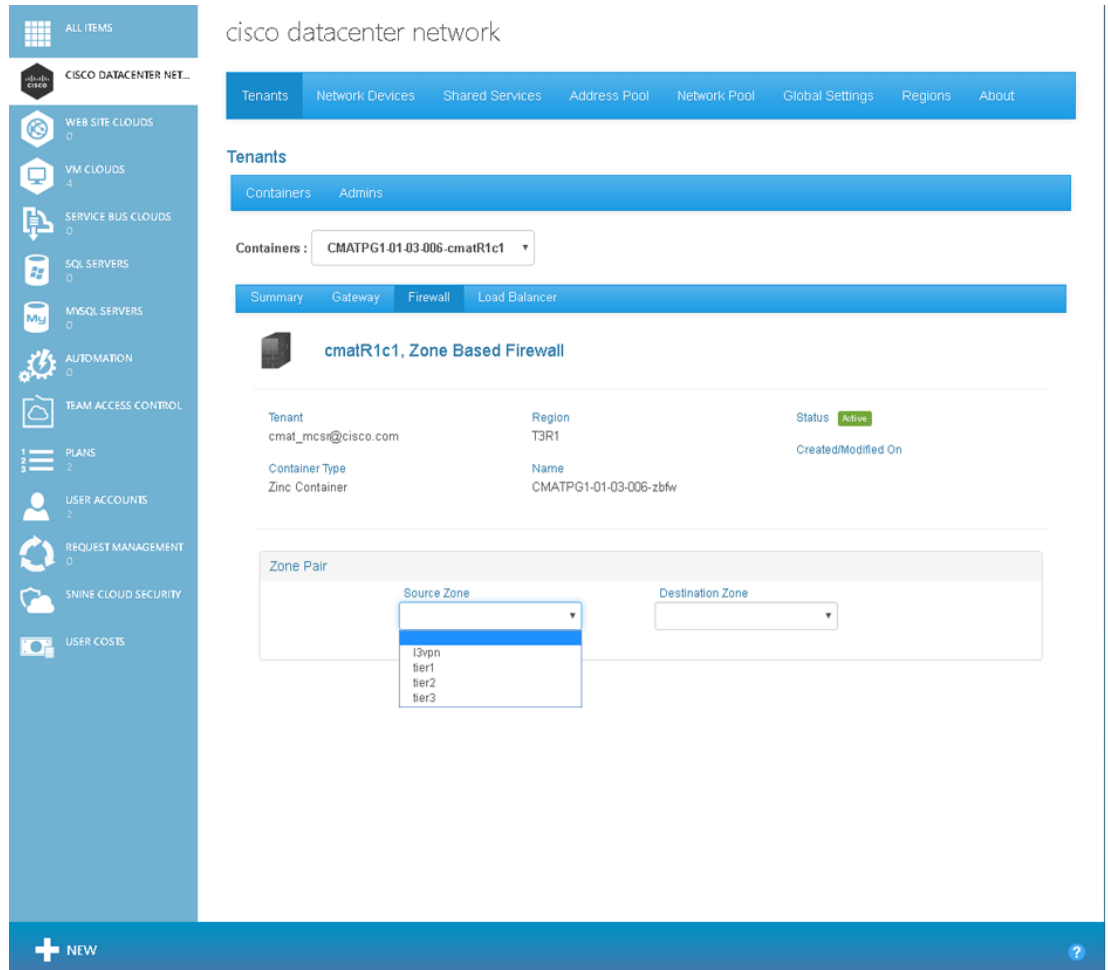


Note You can view the list of all Object Groups, but you cannot view or edit the details of any specific Object Group.

To display the various layers of information about a firewall:

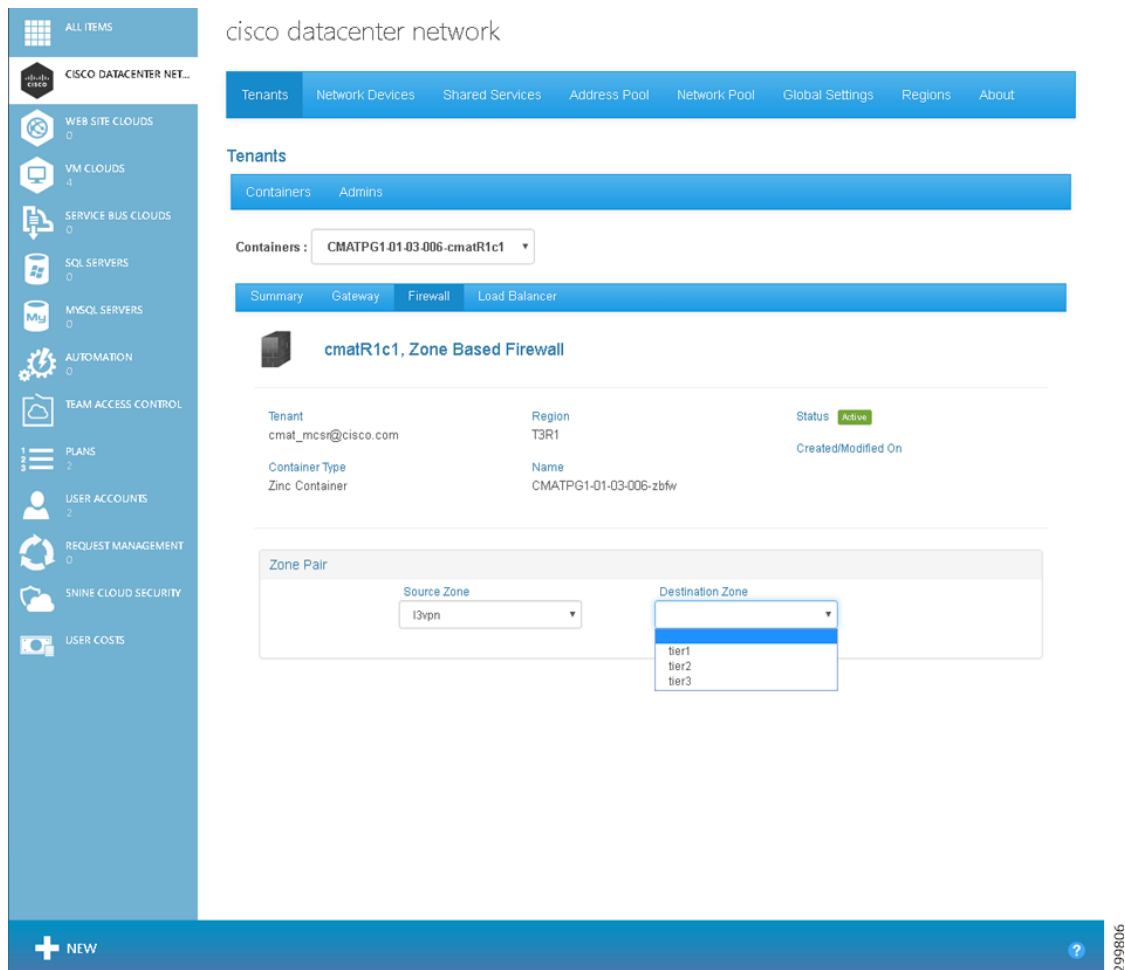
-
- Step 1** On the Firewall tab screen, use the Source Zone: and Destination Zone: pull-down menus to select the relevant zones, as shown in the following screens.

Figure 5-23 Firewall Source Zone Pull-down Menu Screen



299805

Figure 5-24 Firewall Destination Zone Pull-down Menu Screen



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

Figure 5-25 Firewall Zones Selected Screen—Detailed Firewall Information Displayed

The screenshot displays the 'Zone Pair' configuration screen in Cisco Datacenter Network Assistant. The 'Source Zone' is 'I3vpn' and the 'Destination Zone' is 'tier1'. The 'Service Policy' is 'I3vpn-to-tier1'. The 'Class Map Instance' table shows:

Name	Action	Log Drop	Filter
- tier1-web	inspect	<input checked="" type="checkbox"/>	match-any
+ default-service	inspect	<input checked="" type="checkbox"/>	match-any
class-default	drop	<input checked="" type="checkbox"/>	match-all

The 'Access Group' table shows:

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

The 'Object Groups' table shows:

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

Buttons for 'ADD', 'MODIFY', and 'REMOVE' are located at the bottom of the main content area.

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 I3vpn-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**

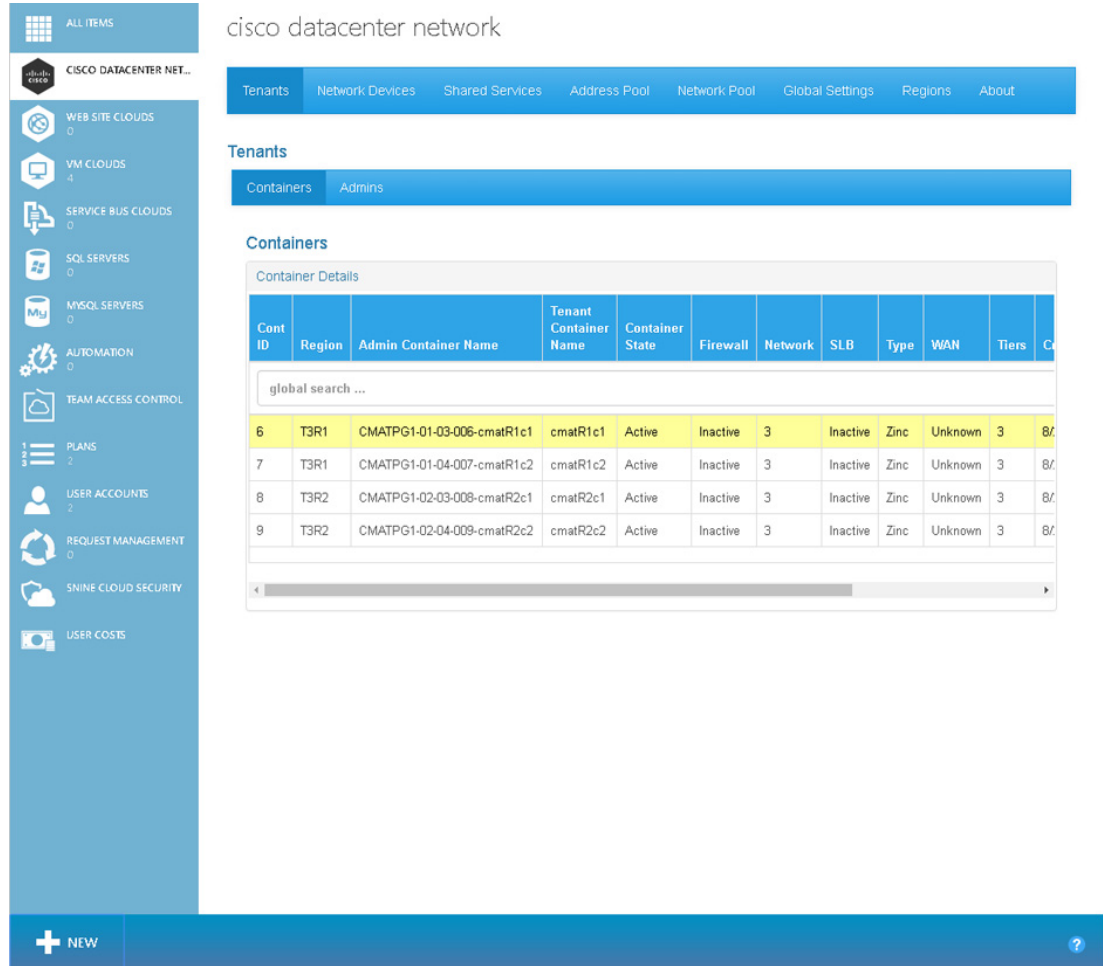
You can only configure a firewall after a tenant has created a container and the Admin has created a WAN Gateway. The firewall is automatically created with a base configuration during container creation. When the WAN gateway is created, another firewall zone is created for the WAN edge. For more information, 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 5-26 Tenants Tab Screen—Container Selected



You see the Tenants Summary screen.

299789

Figure 5-27 Tenants Summary Screen

The screenshot displays the 'Tenants Summary Screen' for a Cisco Datacenter Network. The interface is organized into a left-hand navigation pane and a main content area. The navigation pane includes categories such as 'ALL ITEMS', 'CISCO DATACENTER NET...', 'WEB SITE CLOUDS', 'VM CLOUDS', 'SERVICE BUS CLOUDS', 'SQL SERVERS', 'MYSQL SERVERS', 'AUTOMATION', 'TEAM ACCESS CONTROL', 'PLANS', 'USER ACCOUNTS', 'REQUEST MANAGEMENT', 'SINE CLOUD SECURITY', and 'USER COSTS'. The main content area is titled 'cisco datacenter network' and features a top navigation bar with tabs for 'Tenants', 'Network Devices', 'Shared Services', 'Address Pool', 'Network Pool', 'Global Settings', 'Regions', and 'About'. The 'Tenants' tab is selected, showing a 'Containers' dropdown menu with 'CMATPG1-01-03-006-cmatR1c1' chosen. Below this, there are sub-tabs for 'Summary', 'Gateway', 'Firewall', and 'Load Balancer'. The 'Summary' tab is active, displaying the email 'cmat_mcsr@cisco.com' and a cloud icon. To the right, a summary of resources is shown: WAN Gateways (1), Firewalls (1), Load Balancers (0), and Active Networks (3). Below this, two panels are visible: 'WAN Gateway' and 'Perimeter'. The 'WAN Gateway' panel shows 'MPLSVPN' (Active) and 'Site-to-Site VPN' (None). The 'Perimeter' panel shows 'Zone Based Firewall' (Active) and three 'Workload' tiers (Tier 1, Tier 2, Tier 3) all Online, plus a 'Public' tier that is Inactive.

- Step 2** Click the **Firewall** tab.
You see the Tenant Firewall screen.

Figure 5-28 Tenant Firewall Screen

The screenshot displays the 'Tenant Firewall Screen' in the Cisco Cloud Network Automation Provisioner. The interface is divided into several sections:

- Left Sidebar:** A vertical navigation menu with icons and labels for various system components: ALL ITEMS, CISCO DATACENTER NET., WEB SITE CLOUDS (0), VM CLOUDS (4), SERVICE BUS CLOUDS (0), SQL SERVERS (0), MYSQL SERVERS (0), AUTOMATION (0), TEAM ACCESS CONTROL, PLANS (2), USER ACCOUNTS (2), REQUEST MANAGEMENT (0), SHINE CLOUD SECURITY, and USER COSTS.
- Top Navigation:** A horizontal bar with tabs for Tenants, Network Devices, Shared Services, Address Pool, Network Pool, Global Settings, Regions, and About.
- Main Content Area:**
 - Header:** 'cisco datacenter network' and 'Tenants'.
 - Containers:** A dropdown menu showing 'CMATPG1-01-03-006-cmatR1c1'.
 - Configuration Tabs:** Summary, Gateway, Firewall (selected), and Load Balancer.
 - Firewall Details:**
 - Title:** cmatR1c1, Zone Based Firewall
 - Tenant:** cmat_mcsr@cisco.com
 - Region:** T3R1
 - Status:** Active
 - Container Type:** Zinc Container
 - Name:** CMATPG1-01-03-006-zbfw
 - Created/Modified On:** (blank)
 - Zone Pair Configuration:** A section with two dropdown menus labeled 'Source Zone' and 'Destination Zone'.
- Bottom Bar:** A blue bar with a '+ NEW' button on the left and a help icon (?) on the right.

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 5-29 Firewall Zones Selected Screen—Detailed Firewall Information Displayed

The screenshot shows the Cisco Cloud Network Automation Provisioner interface. The sidebar on the left contains navigation options: ALL ITEMS, CISCO DATACENTER NEW, WEB SITE CLOUDS (0), VM CLOUDS (2), SERVICE BUS CLOUDS (0), SQL SERVERS (0), MYSQL SERVERS (0), AUTOMATION (0), PLANS (12), and USER ACCOUNTS (3). The main content area is titled "Zone Pair" and shows the following configuration:

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	<input checked="" type="checkbox"/>	match-any
+ default-service	inspect	<input checked="" type="checkbox"/>	match-any
class-default	drop	<input checked="" type="checkbox"/>	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	

Buttons: ADD, MODIFY, REMOVE

Footer: + NEW, 215645

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

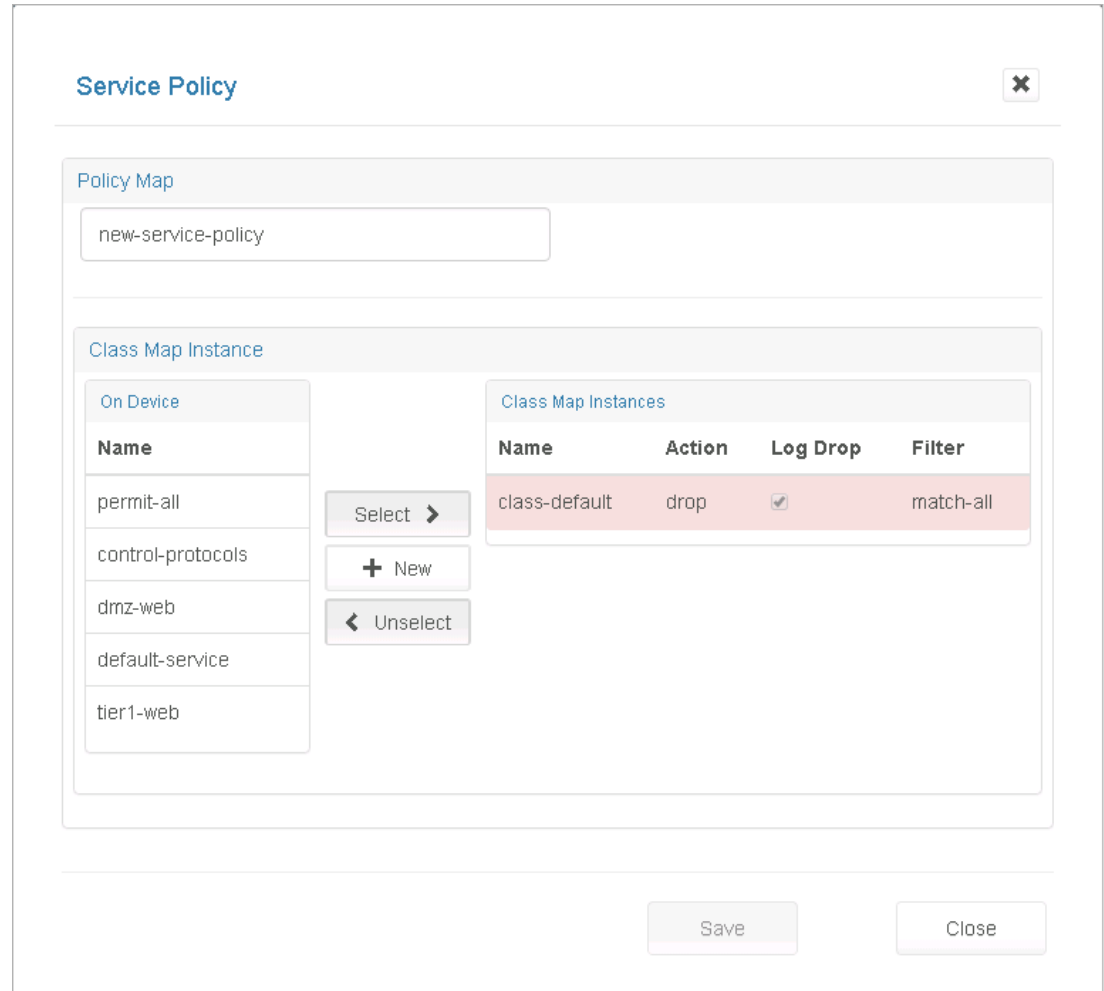
Figure 5-30 Add Policy Map for Service Policy Screen

The screenshot shows the "Service Policy" dialog box. It has a title bar with "Service Policy" and a close button (X). Below the title bar is a "Policy Map" section with a "Name" input field. At the bottom of the dialog are "Save" and "Close" buttons. The number 299815 is visible in the bottom right corner.

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 5-31 New Policy Map—Class Maps Screen



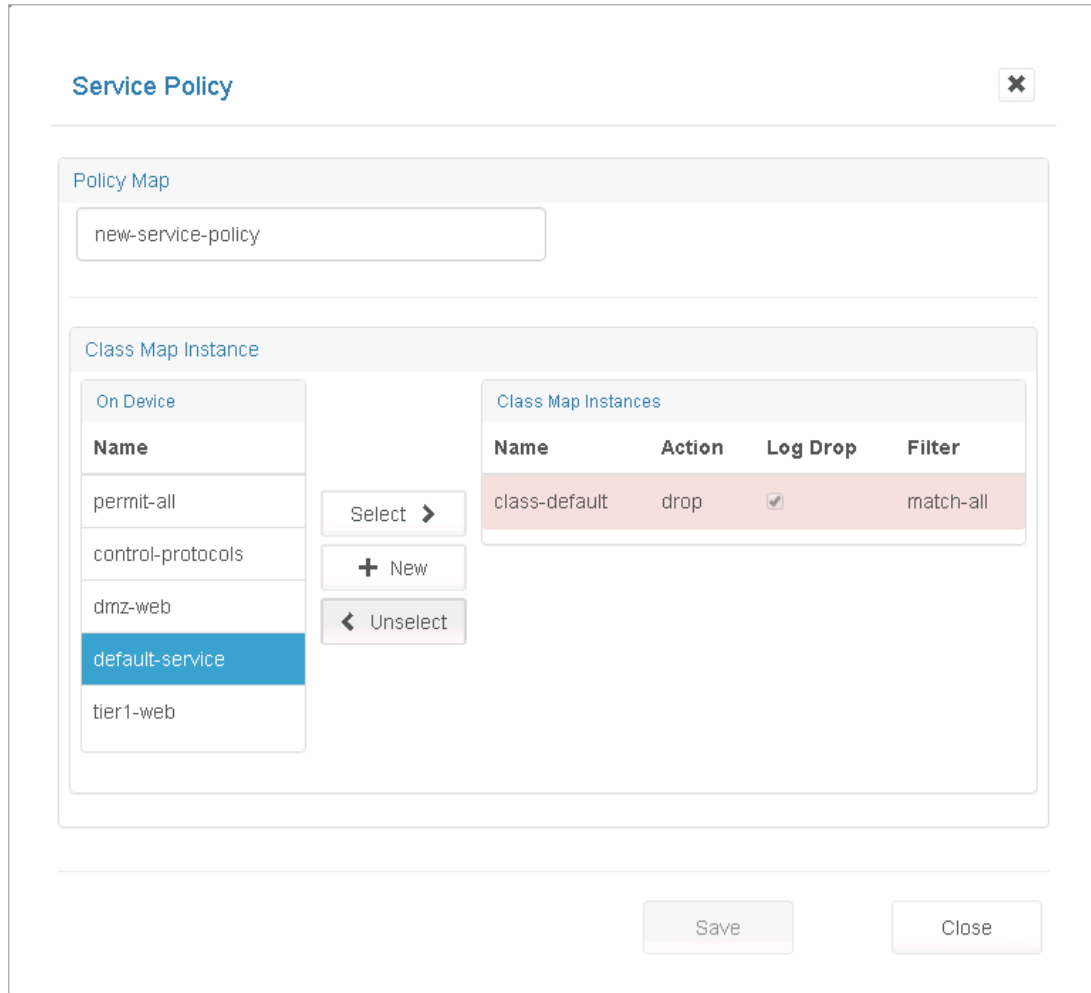
Step 6 Associate class maps with the new Policy Map:

- **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 5-32 Class Map Instance class-default Screen



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 5-33 Policy Map Pop-up Screen

Service Policy [X]

Policy Map

l3vpn-to-tier1

Class Map Instance

On Device

Name
permit-all
control-protocols
dmz-web

Select > + New < Unselect

Class Map Instances

Name	Action	Log Drop	Filter
tier1-web	inspect	<input checked="" type="checkbox"/>	match-any
default-service	inspect	<input checked="" type="checkbox"/>	match-any
class-default	drop	<input checked="" type="checkbox"/>	match-all

Save Close

296819

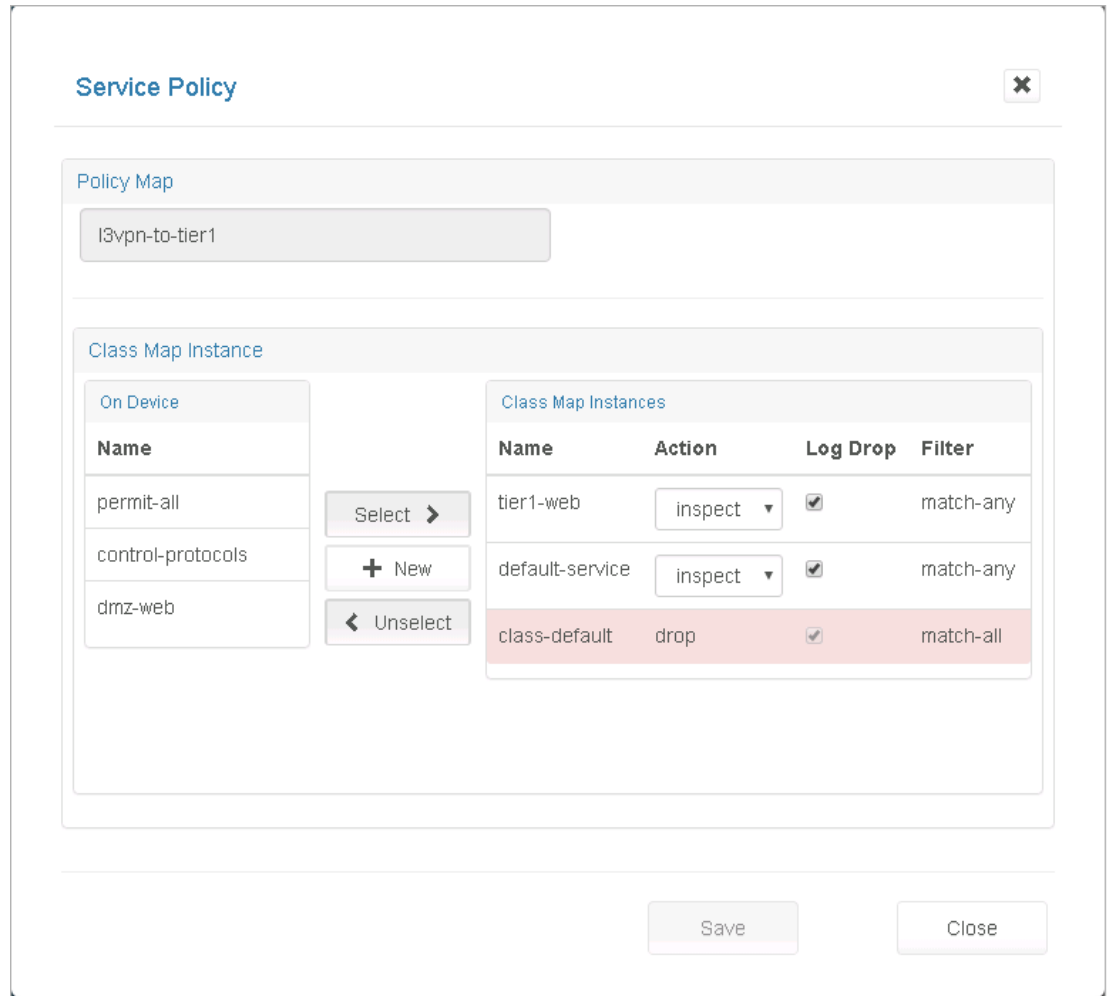
This is the same as the Create Service Policy page, but with the name field deactivated. You can click:

- **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

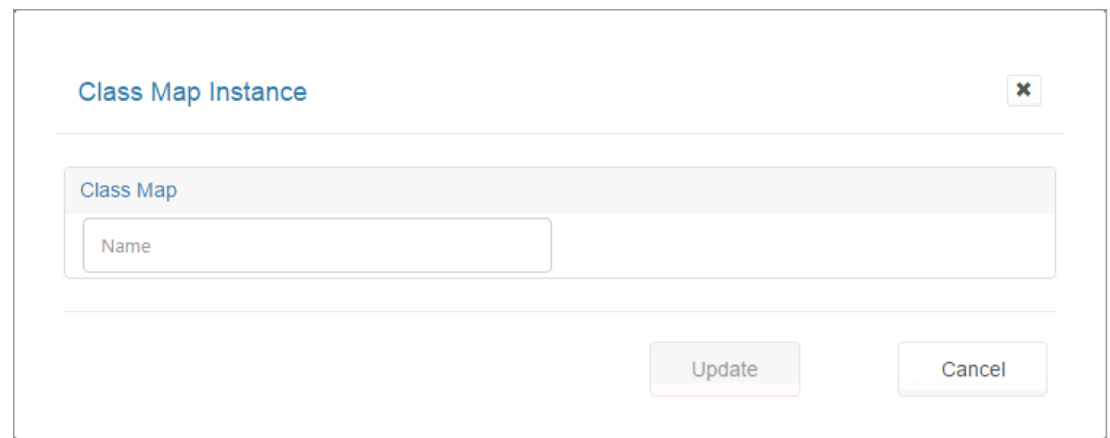
Step 1 Click **+New** in the Class Map Instance section on the Policy Map screen shown below.

Figure 5-34 Class Map Instance Screen—Click +New



You see the following screen.

Figure 5-35 New Class Map Instance Screen



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 5-36 New Class Map Instance Details Screen

The screenshot shows the 'Class Map Instance' configuration interface. At the top, the title 'Class Map Instance' is displayed with a close button. Below this, the 'Class Map' section features a text input field containing 'new-class-map' and a dropdown menu set to 'match-all'. The 'Access Group' section is split into two panes. The left pane, 'On Device', lists four ACLs: 'default-service-acl', 'dmz-web-acl', 'permit-all-acl', and 'tier1-web-acl'. Between the panes are three buttons: 'Select >', '+ New', and '< Unselect'. The right pane, 'ACL Instances', contains a table with columns 'Name', 'Target', and 'Action'. At the bottom of the screen are two buttons: 'Update' and 'Cancel'.

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.

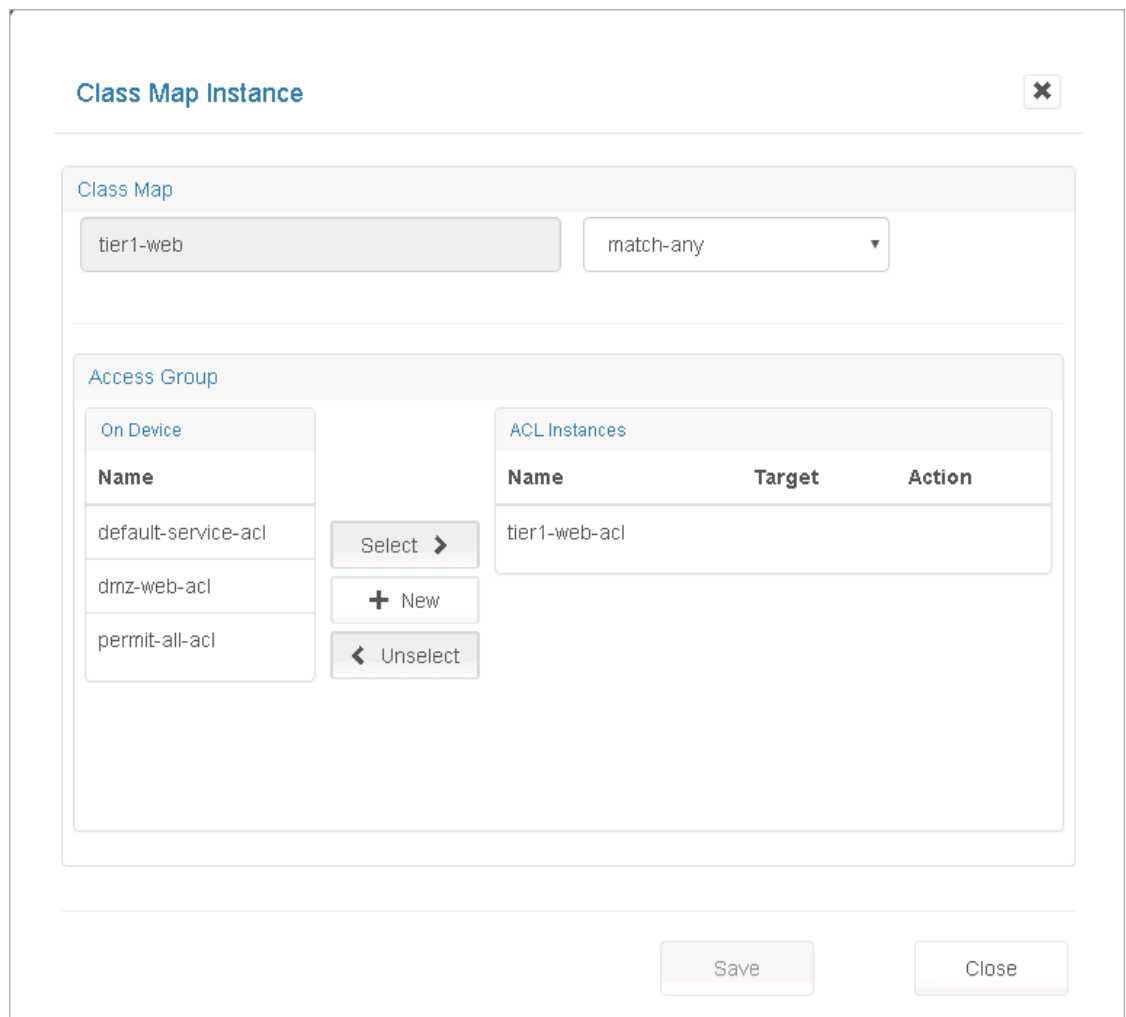
Changing a Class Map

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

Step 2 Click **Modify**.

You see the following screen.

Figure 5-37 Class Map Instance Screen



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.

9824

Creating a New Network Access Control List

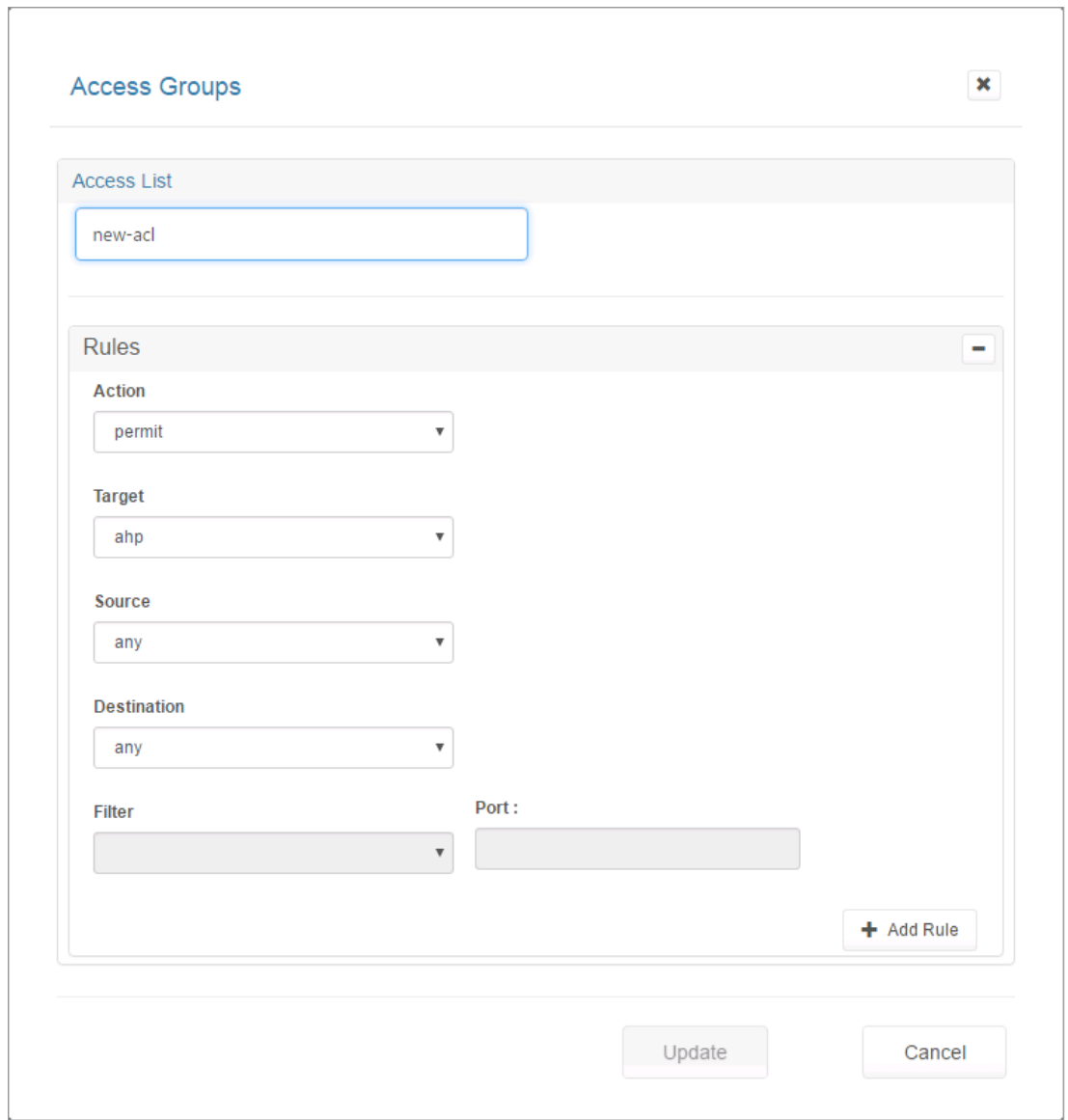
- Step 1** Click **New** on the Class Map Instance screen shown above, which displays the Access Group screen shown below.

Figure 5-38 Access Groups Screen

The screenshot shows a web interface for managing Access Groups. The main heading is "Access Groups" with a close button (X) in the top right corner. Below this heading is a section titled "Access List" which contains a text input field labeled "Name". At the bottom of the interface are two buttons: "Update" and "Cancel". A vertical ID number "299625" is visible on the right side of the screenshot.

- 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 5-39 Access Groups Details Screen



Step 3 The fields you can complete include:

- Action—Indicates whether 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 5-40 Access Groups Screen—Object Group Selected

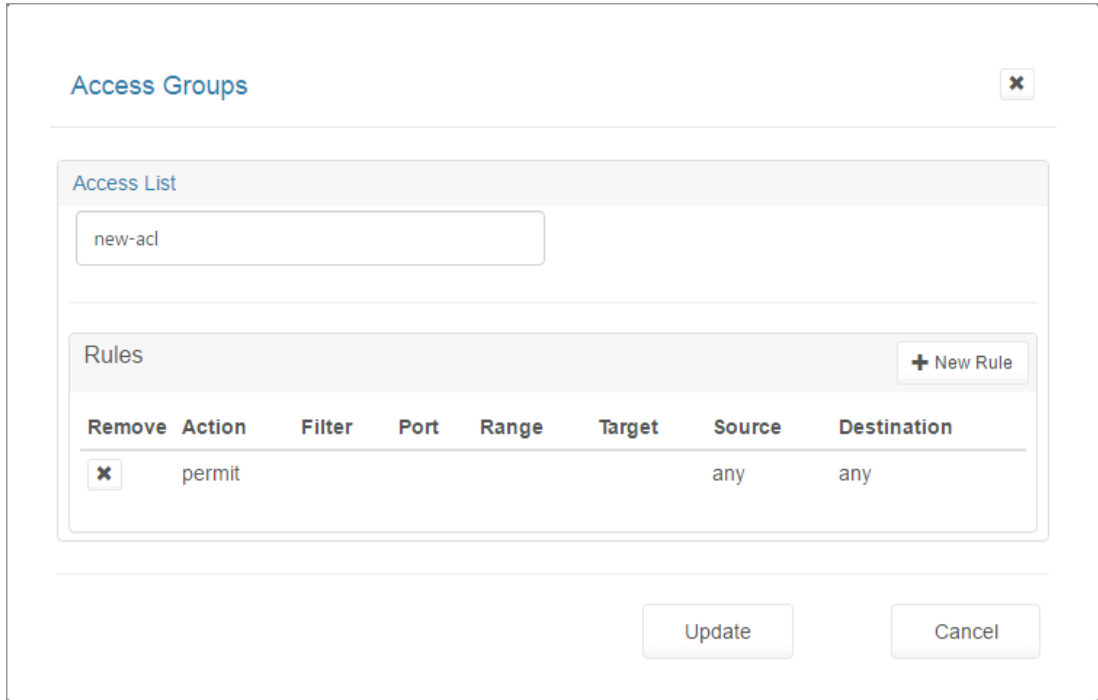
The screenshot displays the 'Access Groups' configuration interface. At the top, the title 'Access Groups' is shown with a close button (X). Below this, the 'Access List' section contains a text input field with the value 'new-acl'. The main 'Rules' section is expanded, showing the following configuration options:

- Action:** A dropdown menu set to 'permit'.
- Target:** A dropdown menu set to 'object-group'.
- Object Group:** A field with a list icon, a dropdown menu, and a plus sign (+).
- Source:** A dropdown menu set to 'any'.
- Destination:** A dropdown menu set to 'any'.
- Filter:** A dropdown menu.
- Port:** A text input field.

At the bottom right of the 'Rules' section is a '+ Add Rule' button. At the bottom of the entire screen are 'Update' and 'Cancel' buttons. A vertical ID number '299827' is located on the right edge of the screenshot.

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

Figure 5-41 Rule Added to ACL Screen

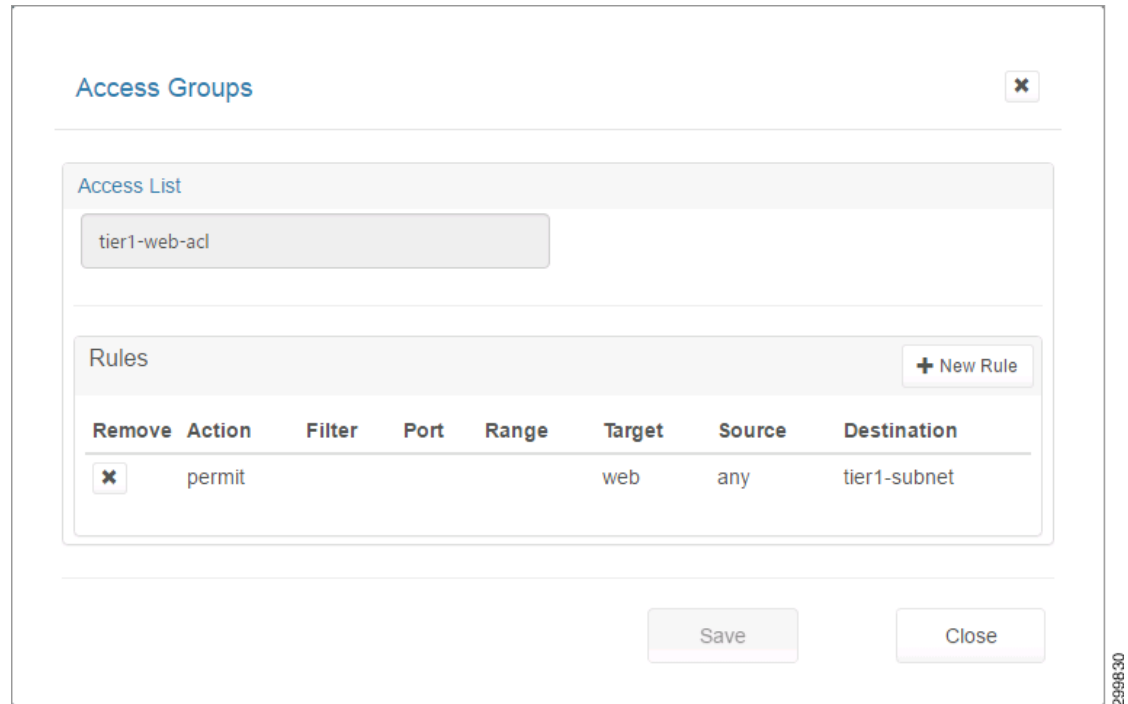


- Step 6** Click **+New Rule** to add more rules.
- Step 7** Click the **Update** button to exit the Add Rule mode and show the list of all rules in the ACL.

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 5-42 Access List Pop-up Screen

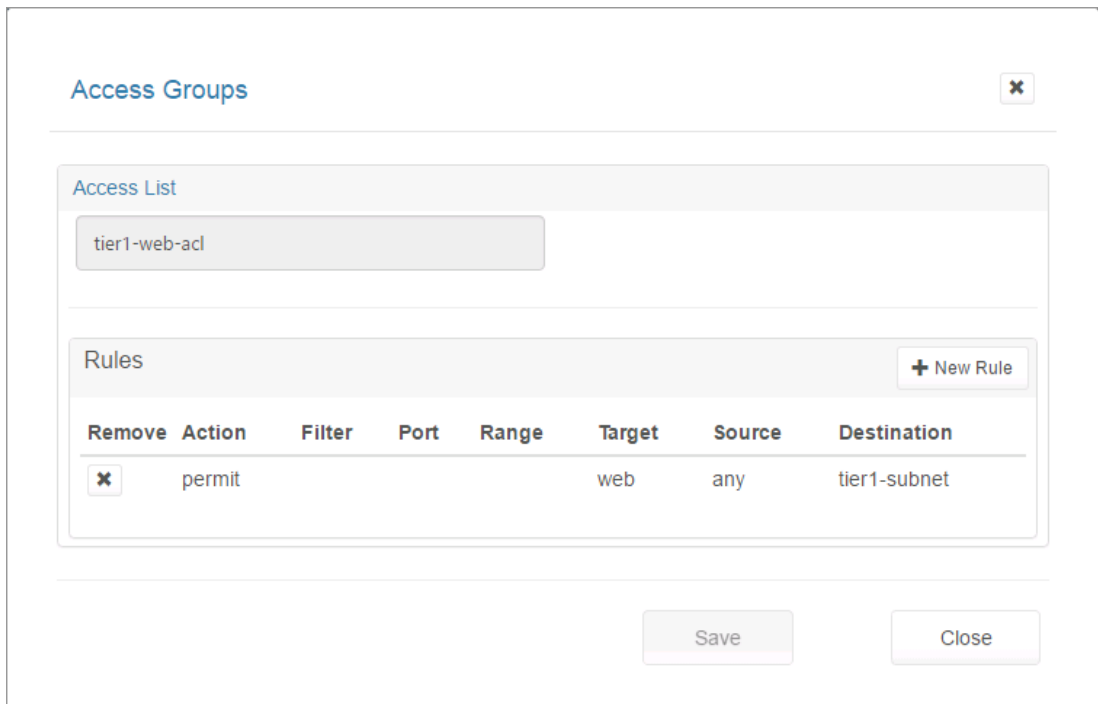


- Step 3** You can add and remove rules as explained in [Creating a New Network Access Control List](#).
- Step 4** If you make any changes to the list of Rules, the **Save** button is activated and you can click it to save the changes.

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 5-43 Access List Pop-up Screen



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 5-44 Access Groups Screen—Object Group Selected

The screenshot displays the "Access Groups" configuration interface. At the top, the title "Access Groups" is shown with a close button (X). Below this, the "Access List" section contains a text input field with the value "tier1-web-acl". The main "Rules" section is expanded, showing the following configuration:

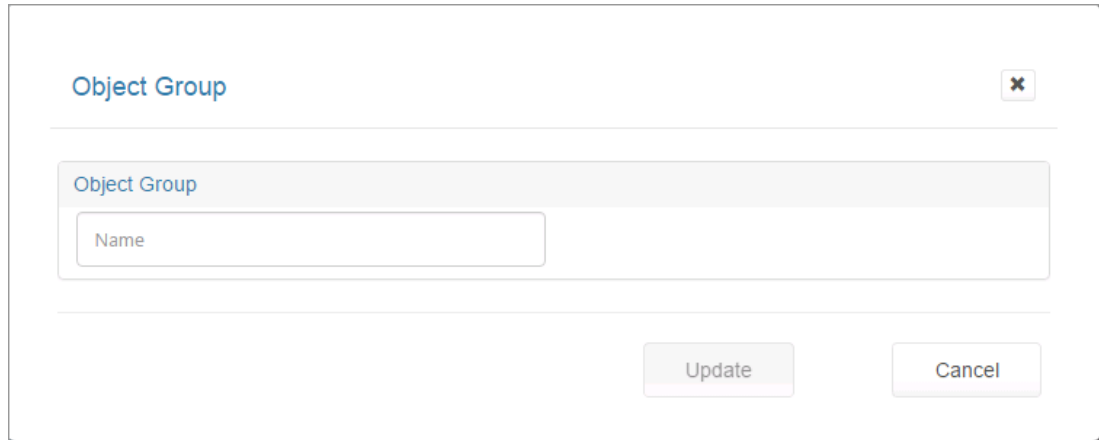
- Action:** A dropdown menu set to "permit".
- Target:** A dropdown menu set to "object-group".
- Object Group:** A dropdown menu with a list icon and a plus sign, currently empty.
- Source:** A dropdown menu set to "any".
- Destination:** A dropdown menu set to "any", which is highlighted with a blue border.
- Filter:** A dropdown menu, currently empty.
- Port:** A text input field, currently empty.

At the bottom right of the Rules section is a "+ Add Rule" button. At the bottom of the entire screen are "Save" and "Close" buttons.

You see the following screen.

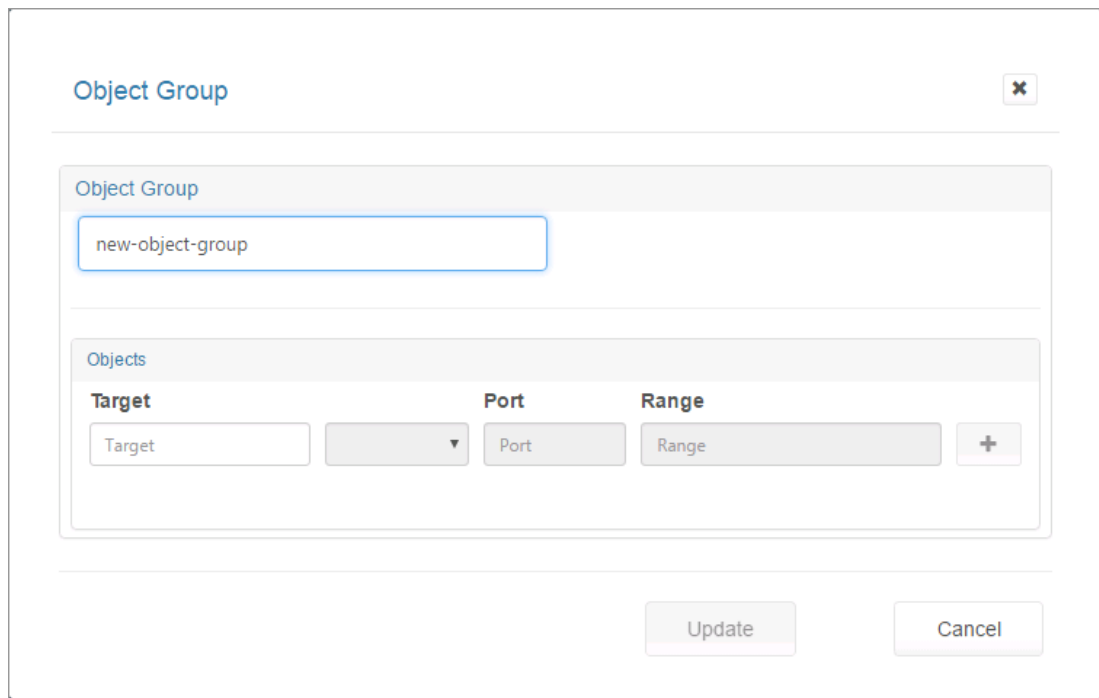
298831

Figure 5-45 Object Group Screen



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

Figure 5-46 Add Object Screen



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

Figure 5-47 Add Object Screen—Possible Field Values Displayed

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.



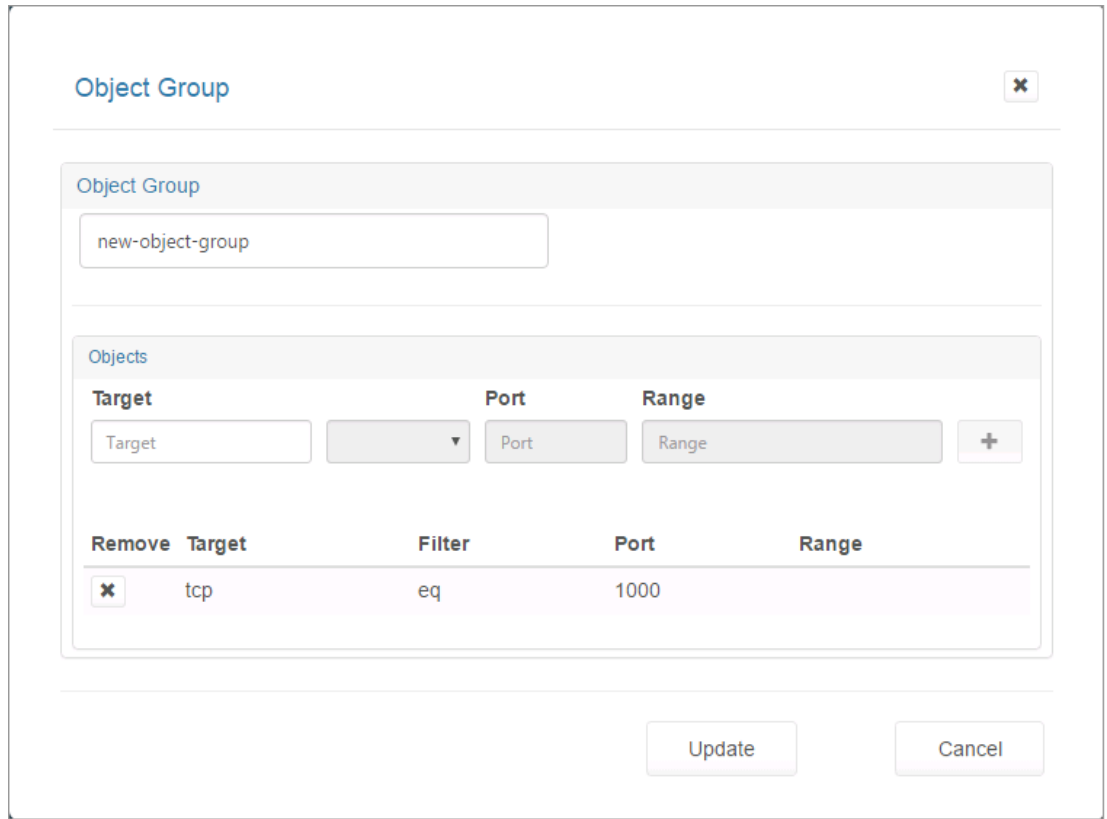
Note If “range” is present, the “filter” and “port” properties are ignored.

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 5-48 Object Added to Group Screen

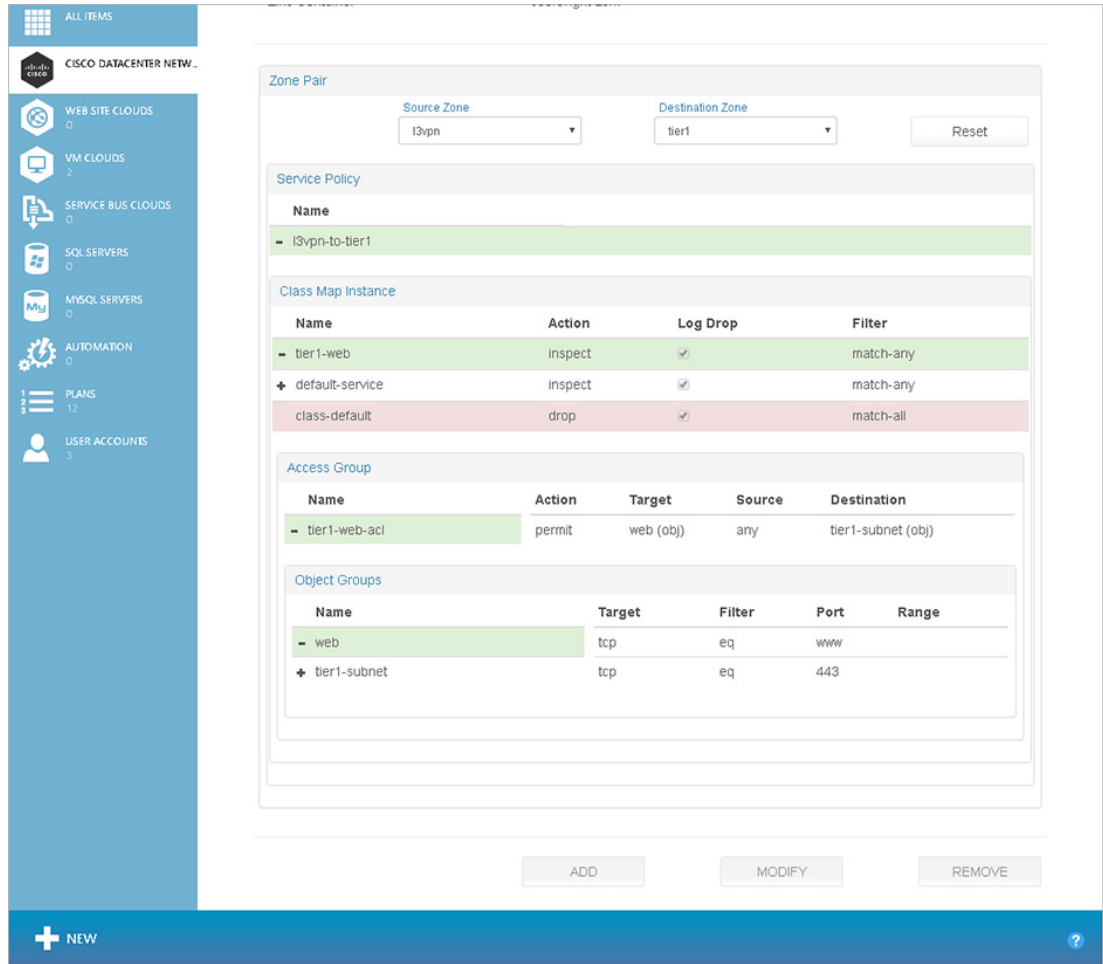


Step 10 Click the X under **Remove** to remove an object from the group.

Changing an Object Group

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

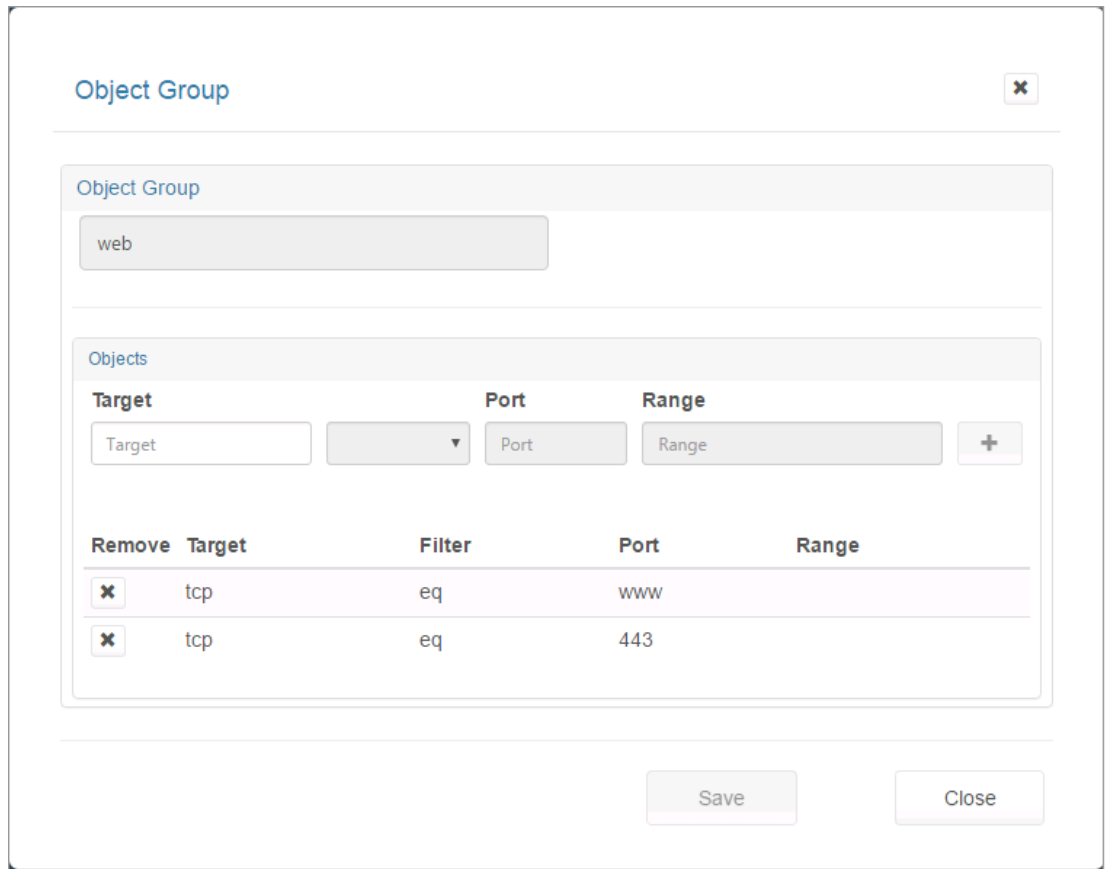
Figure 5-49 Firewall Zones Selected Screen—Select Object Group



215545

You see the following screen.

Figure 5-50 Modify Object Group Screen



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.

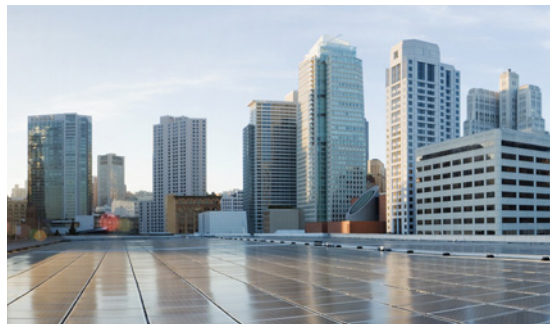


Note If “range” is present, the “filter” and “port” properties are ignored.

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.



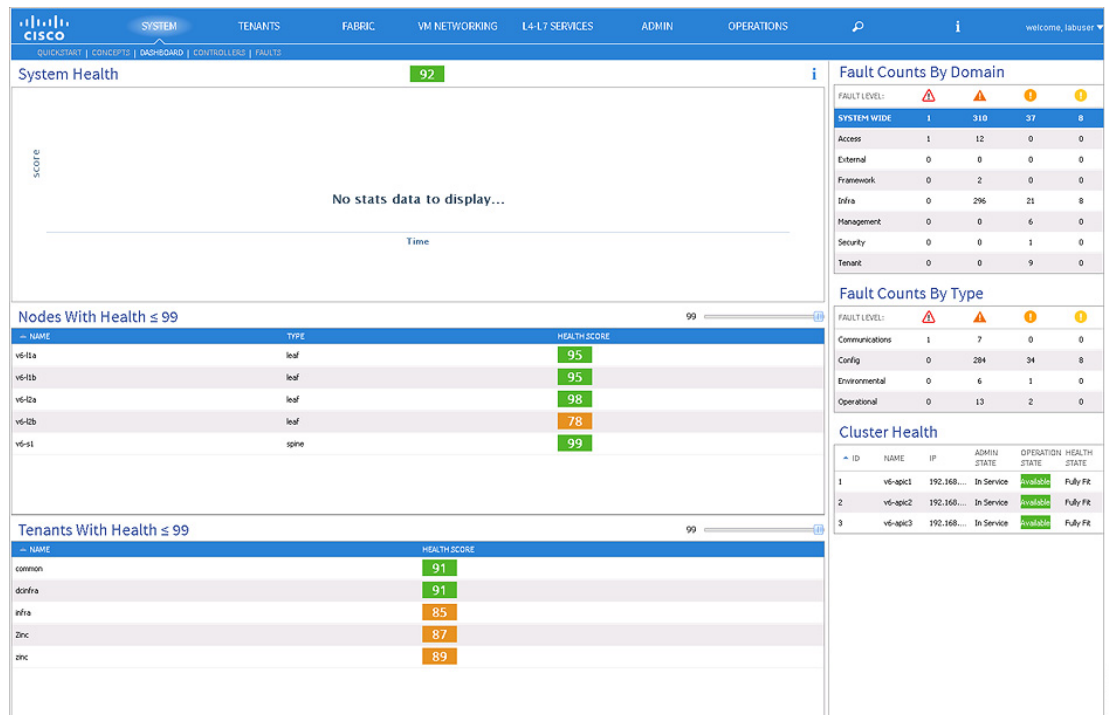
APPENDIX **A**

Cisco Application Policy Infrastructure Controller

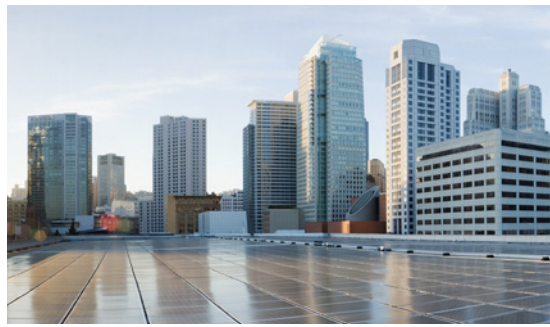
The Cisco Application Policy Infrastructure Controller (APIC) user interface provides useful information about your Cisco CNAP provisioned containers and network. For more information, consult the Cisco APIC documentation:

<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



299848



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.

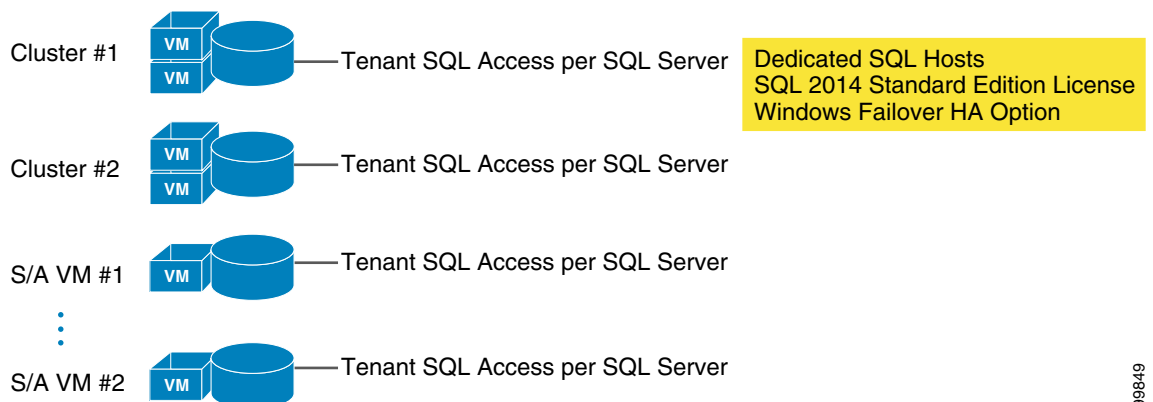
For detailed information on deploying DBaaS, see *Cisco Cloud Architecture for the Microsoft Cloud Platform: DBaaS Configuration Guide, Release 1.0* and the Microsoft Azure Pack documentation.

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



299849

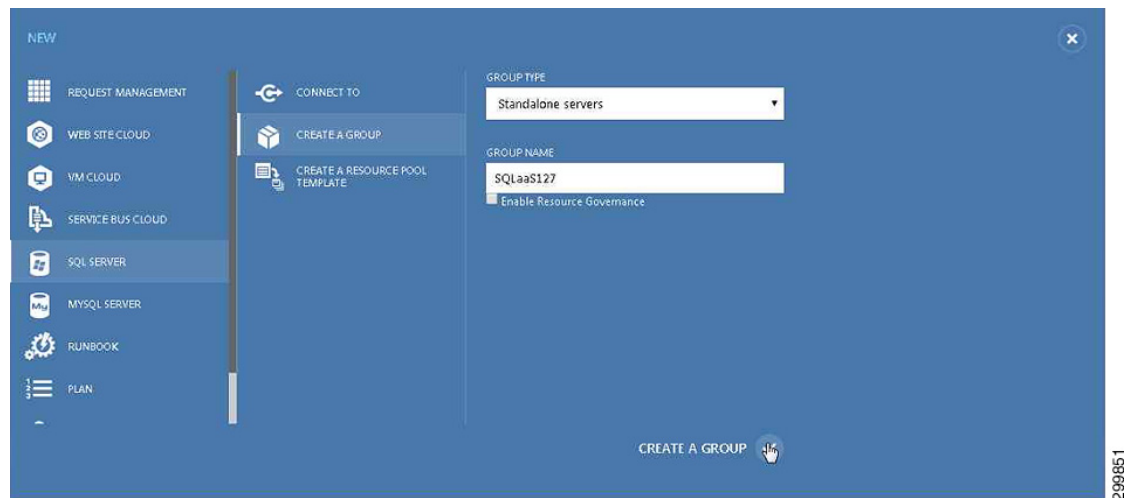
Use the Administrator SQL Resource Provider User Interface to Create the DBaaS Plan and Resource Allocation

- 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.

The screenshot displays the Administrator SQL Resource Provider User Interface. The left sidebar contains navigation options: CISCO DATACENTER NET., REQUEST MANAGEMENT (0), WEB SITE CLOUDS (0), VM CLOUDS (2), SERVICE BUS CLOUDS (0), SQL SERVERS (7), MYSQL SERVERS (0), AUTOMATION (29), PLANS (31), USER ACCOUNTS (31), and USER COSTS. The main content area shows a table of SQL Server Groups under the 'GROUPS' tab. The table has columns for NAME, STATUS, SERVERS, RESOURCE GO..., ALWAYS ..., and NETWORK FILE SHARE. The 'DBaaS18-RG' group is highlighted in blue and is in an 'Active' state. Below the table, there are buttons for '+ NEW', '+ ADD GROUP', and 'DELETE GROUP'.

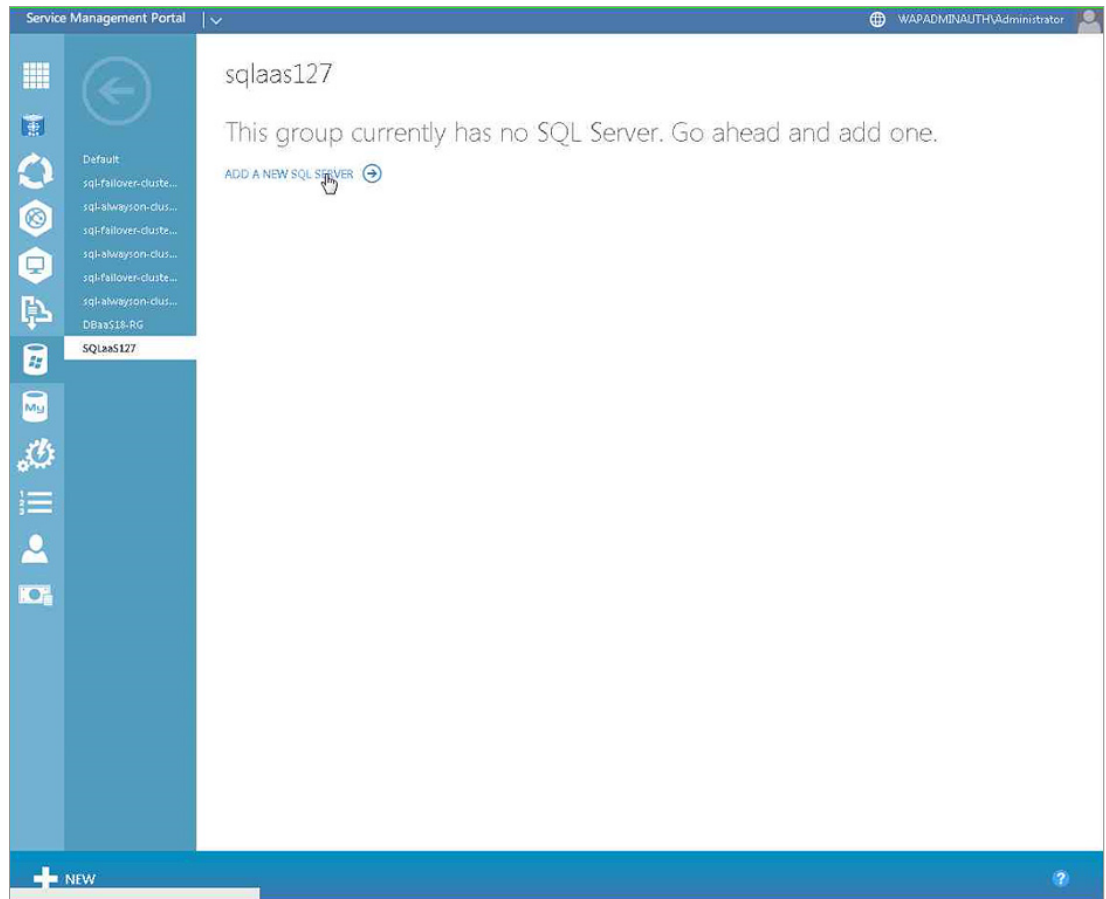
NAME	STATUS	SERVERS	RESOURCE GO...	ALWAYS ...	NETWORK FILE SHARE
DBaaS18-RG	Active	1	Enabled	Yes	\\dbaaS-fs1\AlwaysOnShare
Default	Ready	0	Disabled	No	Not applicable
sql-alwayson-cluster-01	Active	1	Enabled	Yes	\\ics3-c3b3\share
sql-alwayson-cluster-02	Active	1	Enabled	Yes	\\DBaaS-FS1\AlwaysOnShare
sql-alwayson-cluster-03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

299850



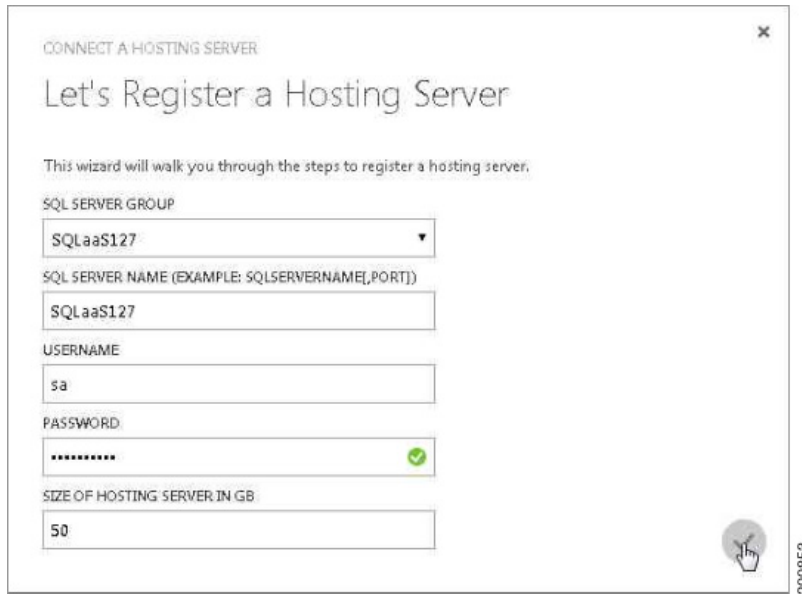
299851

Step 5 Add a server to the new group.

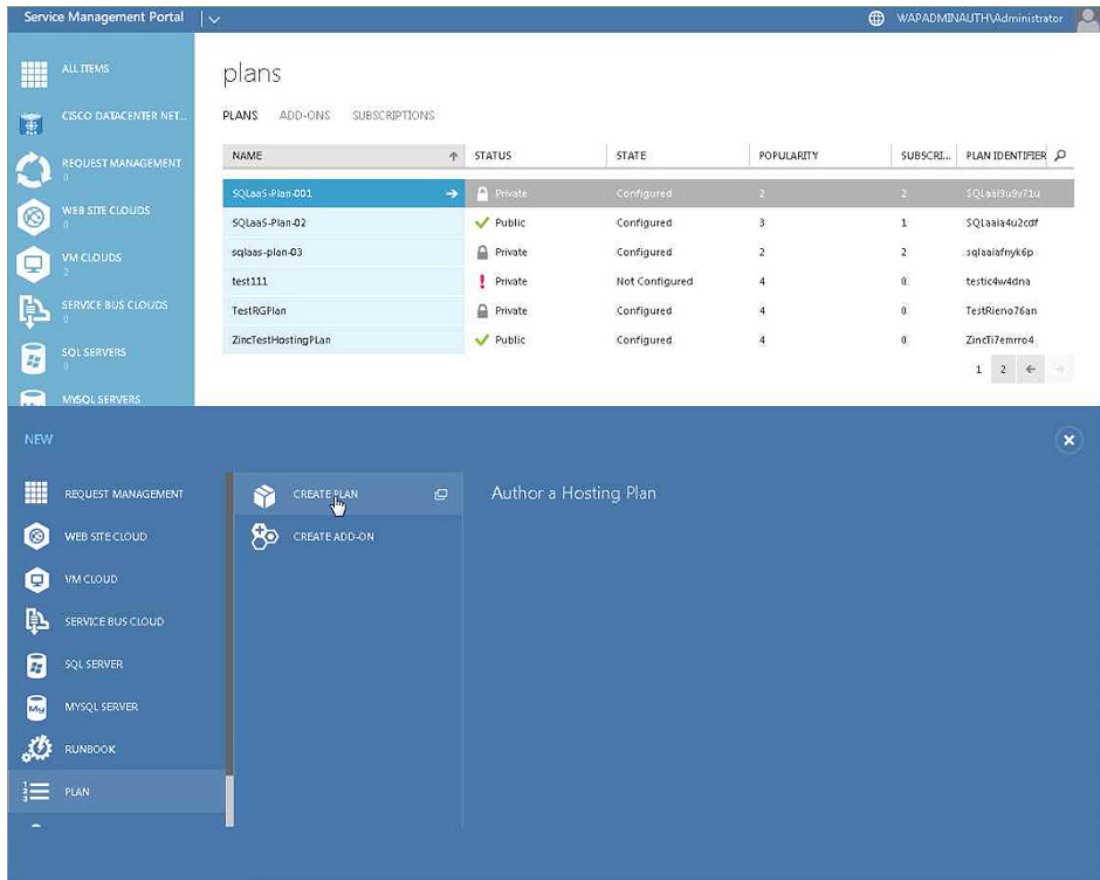


299852

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



Step 7 Create a plan.



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

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

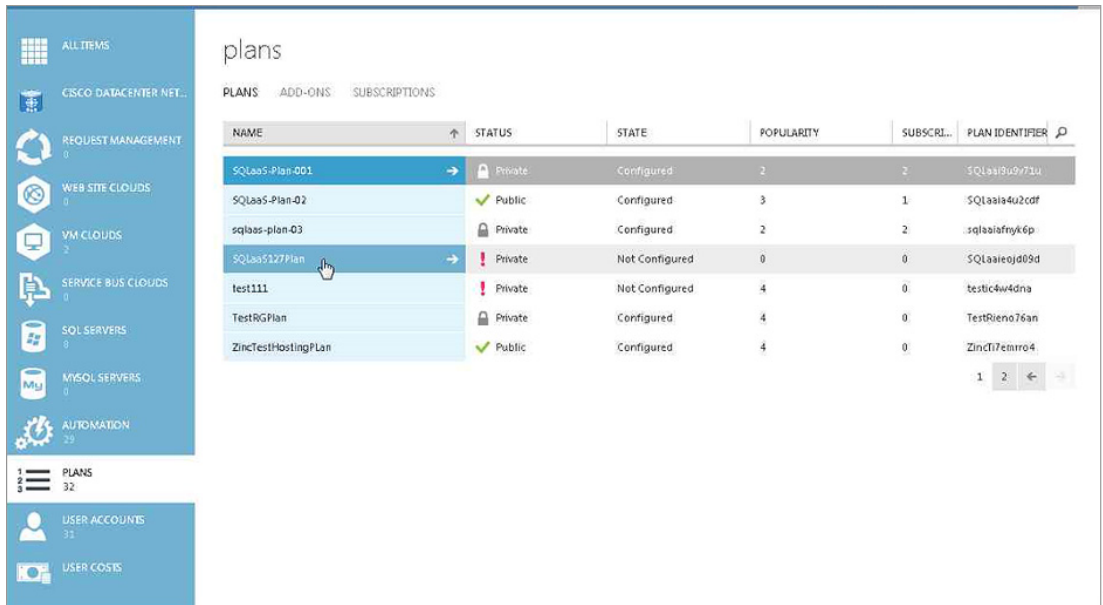
SQL SERVERS

SQL Servers

CISCO DATACENTER NETWORK

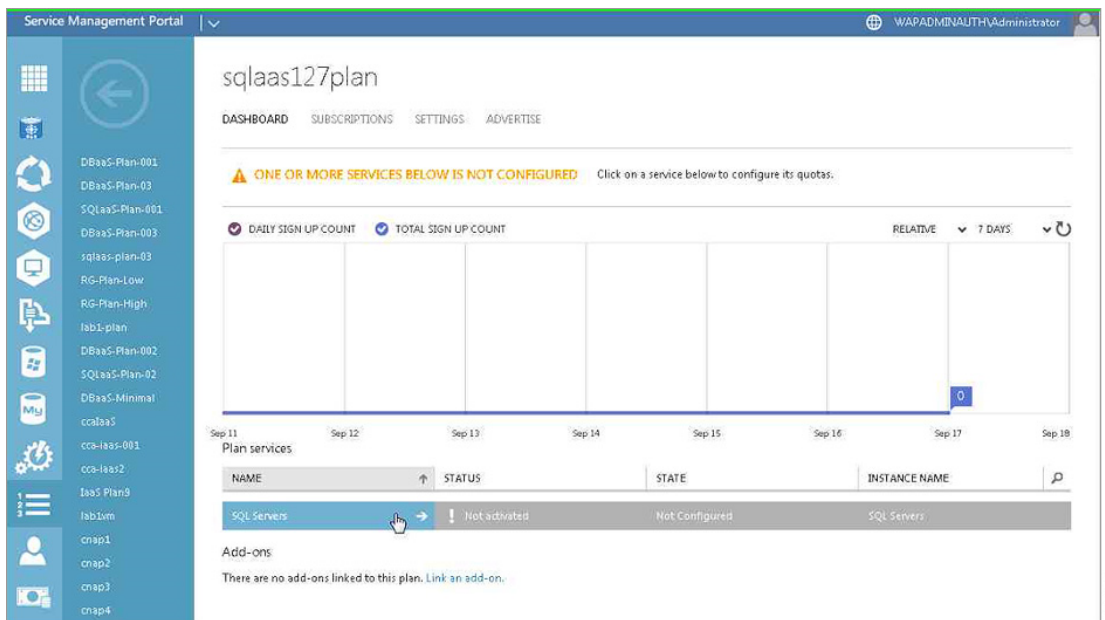
Cisco DataCenter Network

Step 10 Verify plan creation from the Plan Windows SQL.

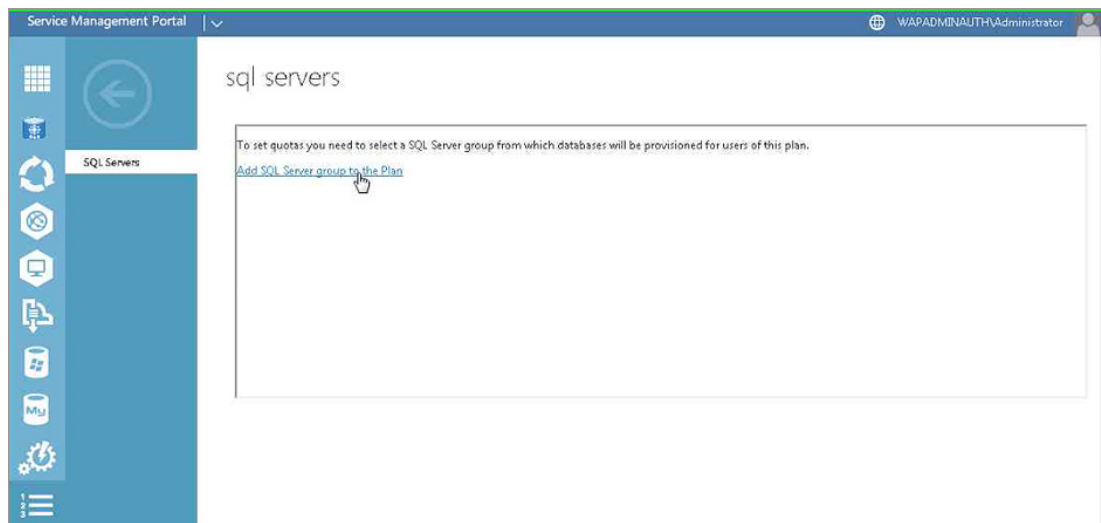


299857

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



299858



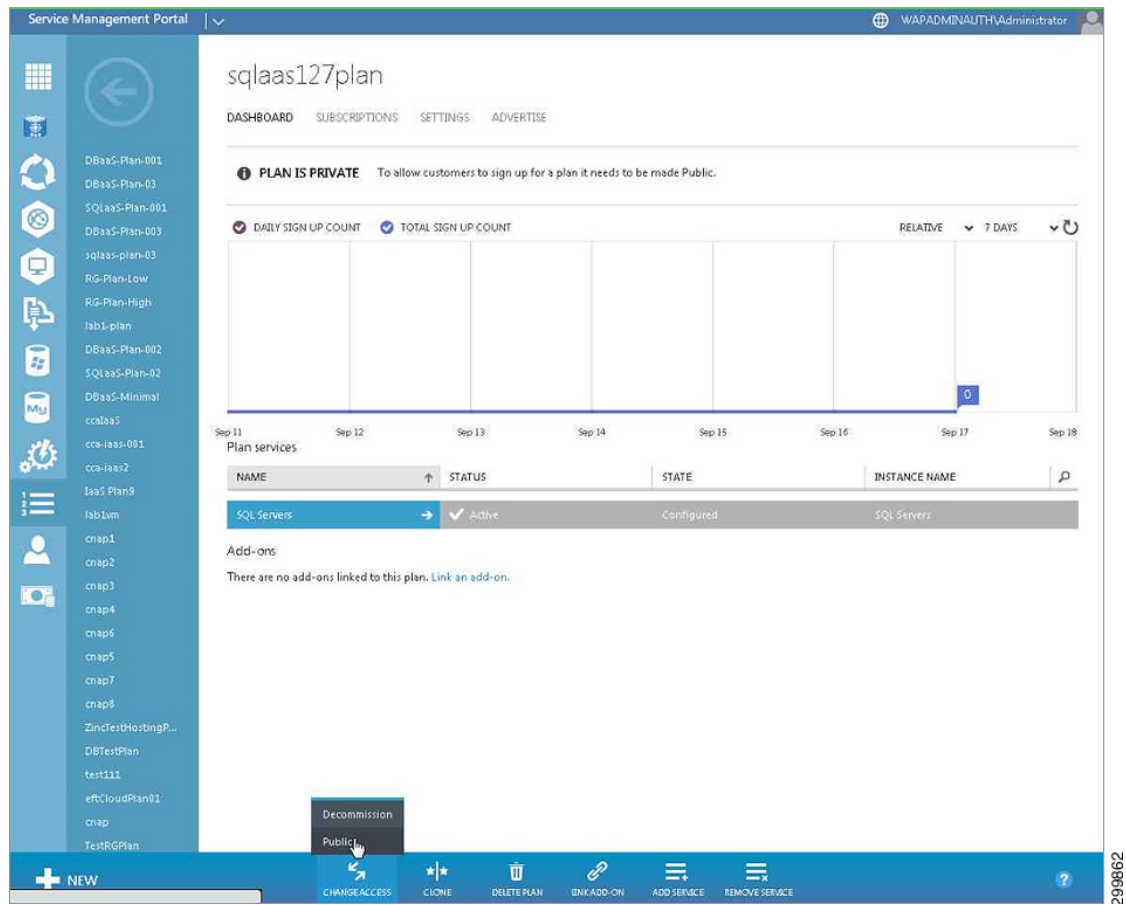
- Step 12** Add SQL Server Group to the Plan. Specify resource allocation per instance; i.e., allowed databases and size of database per subscription.

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



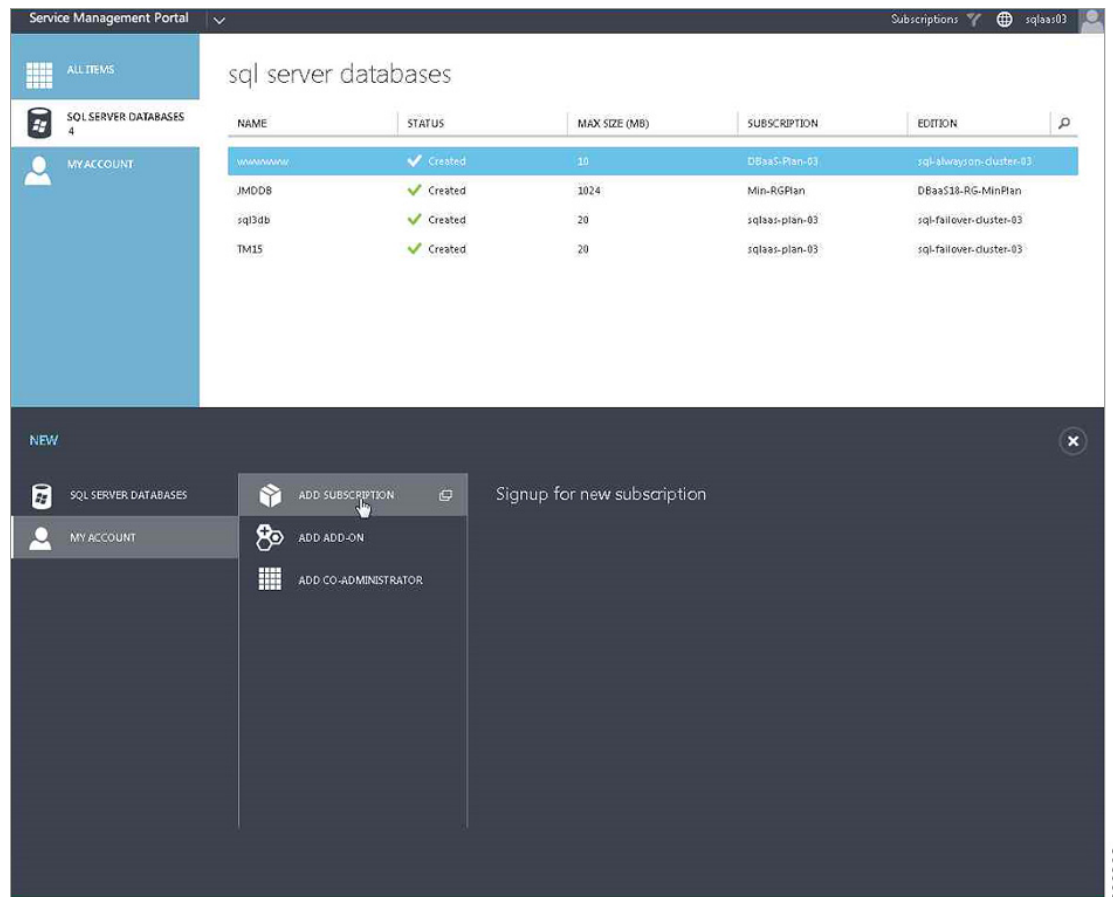
Note

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.

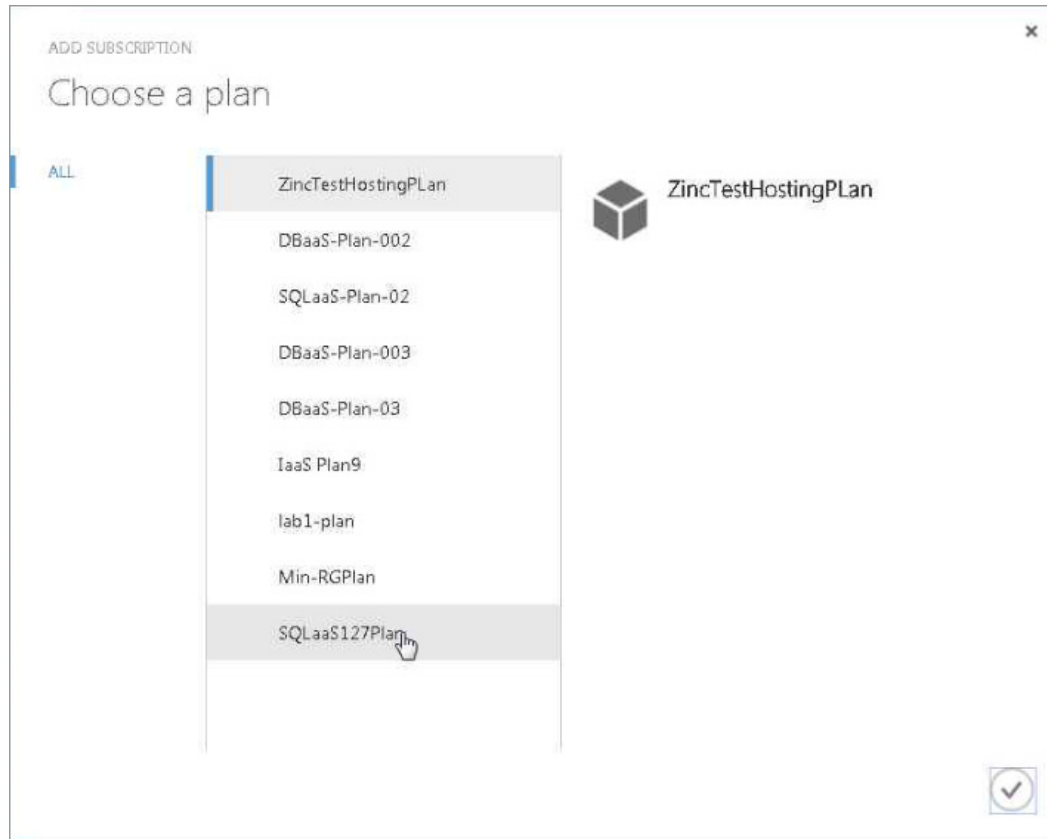


Use the Tenant SQL Resource Provider User Interface to View Published Plan Options and Subscribe

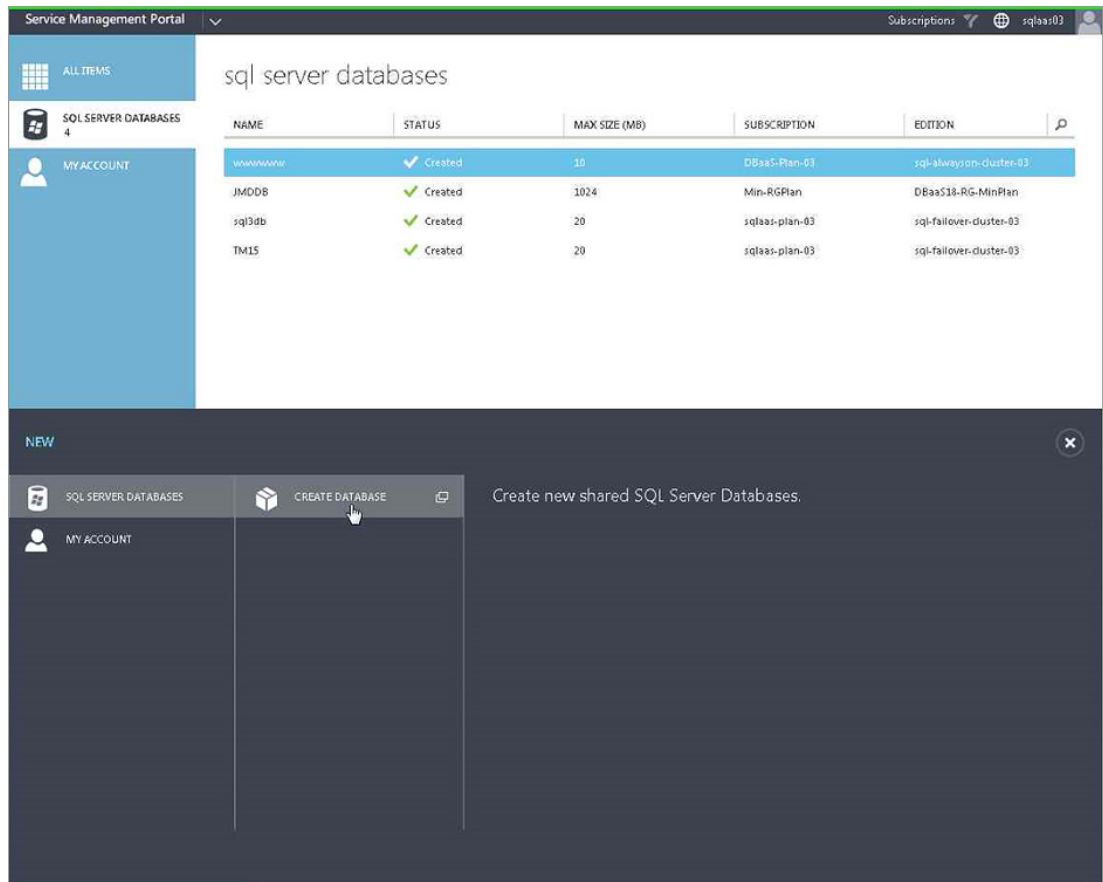
- Step 1** Login to the WAP Tenant Administrator portal. Enter your username and password.
- Step 2** Go to My Account and select **Add Subscription**. From the available plan(s) previously created and published through the SP Admin UI, select a plan.



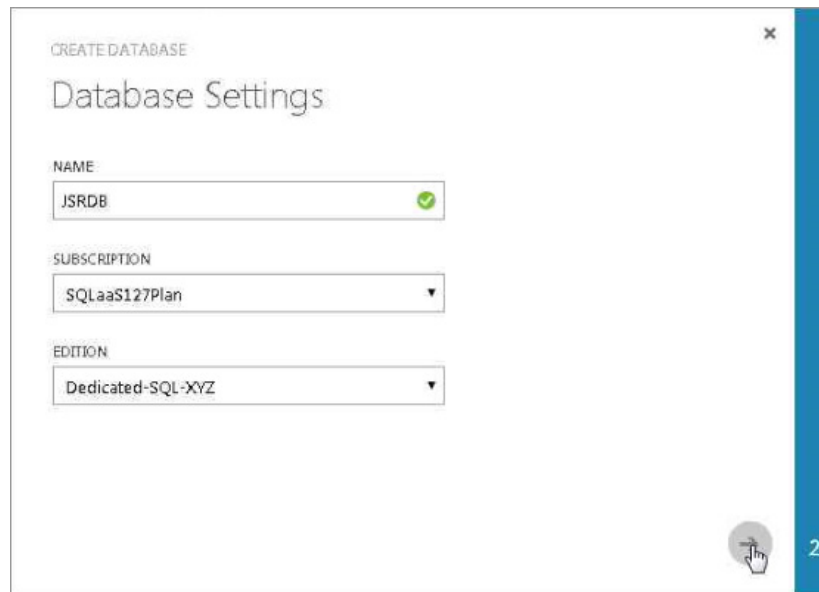
299863



- 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.



299865



299866

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

CREATE DATABASE

Database Credentials

ADMIN NAME

PASSWORD

PASSWORD CONFIRMATION

1

299867

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

Service Management Portal

Subscriptions sqlaaS03

ALL ITEMS

SOL SERVER DATABASES 5

MY ACCOUNT

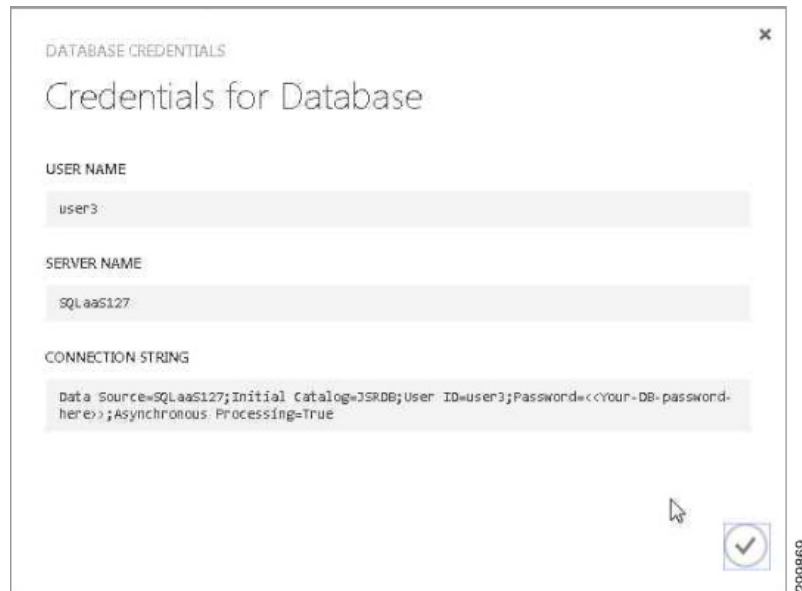
sql server databases

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

+ NEW VIEW INFO DELETE CHANGE PASSWORD RESIZE ?

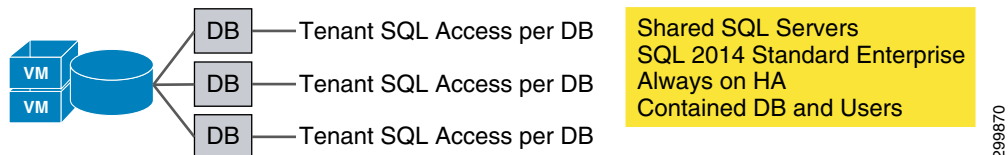
299868

- 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.



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

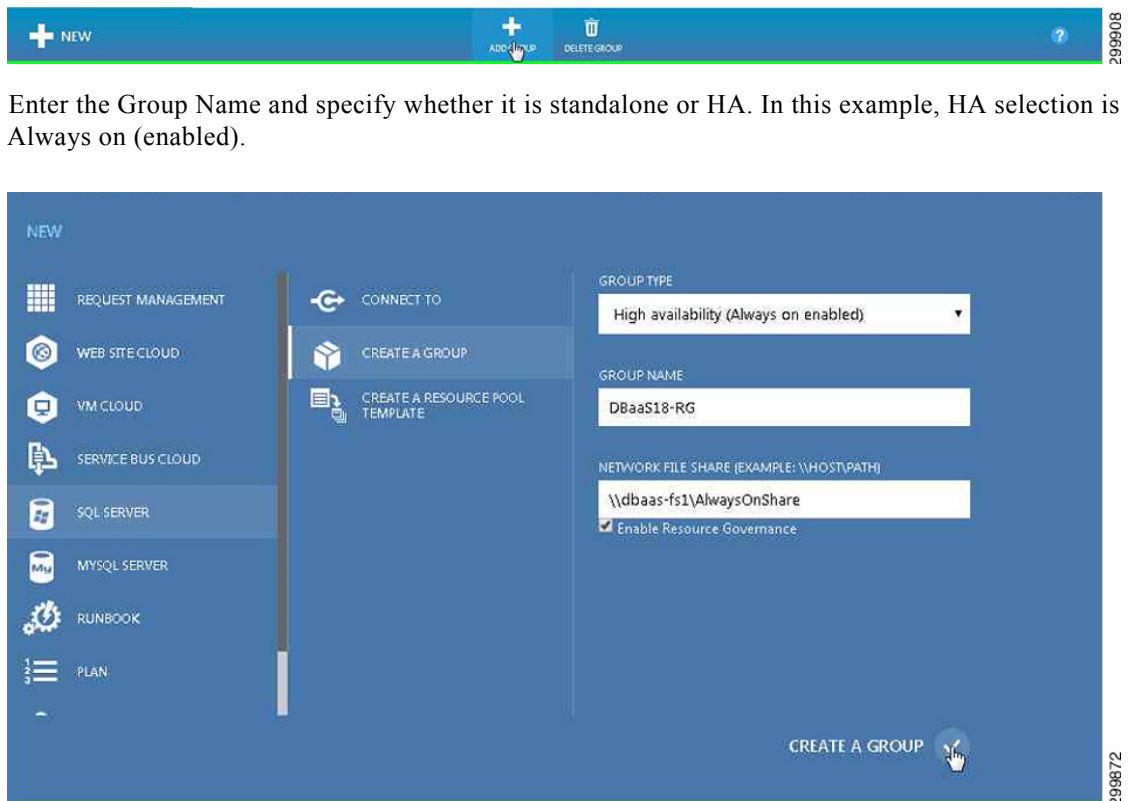
Figure B-2 Always-on Cluster Redundancy Option



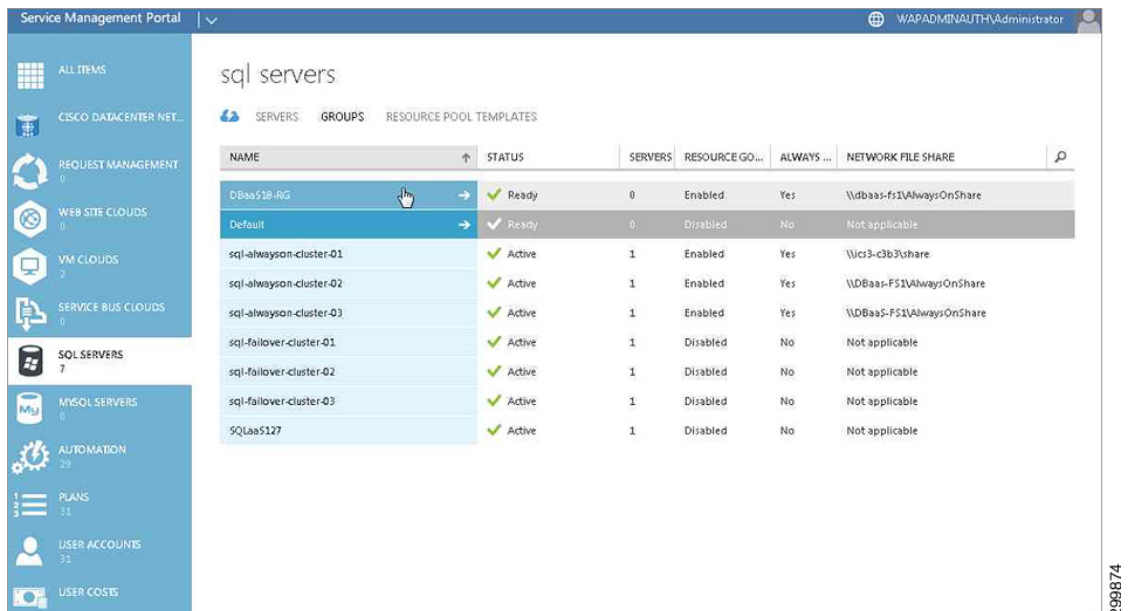
Use the Administrator SQL Resource Provider User Interface to Create DBaaS Plan and Resource Allocation

- 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.

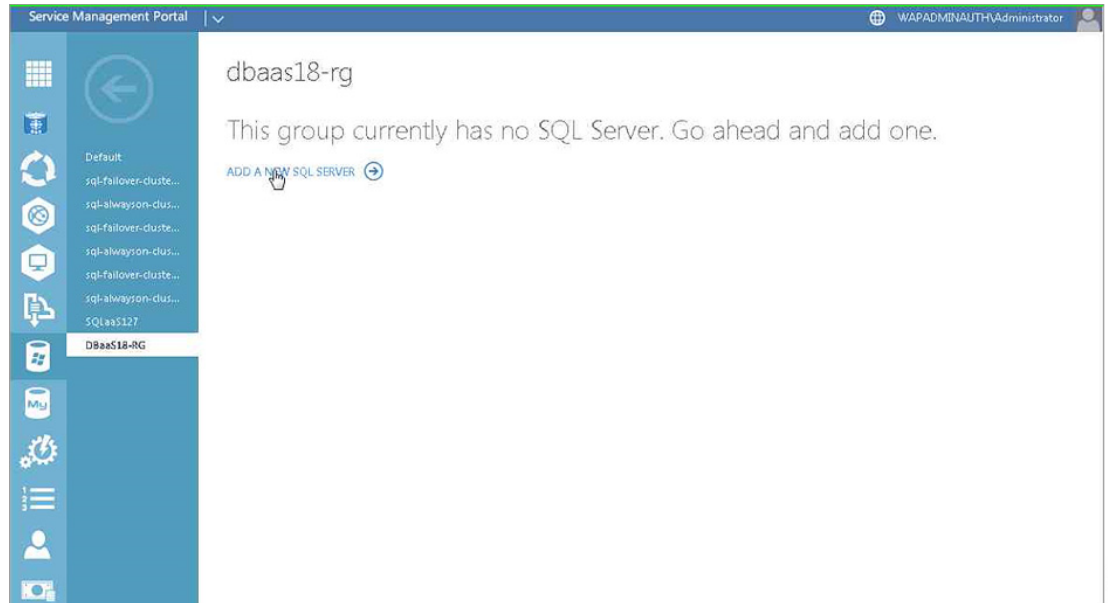
Step 3 Enter the Group Name and specify whether it is standalone or HA. In this example, HA selection is Always on (enabled).



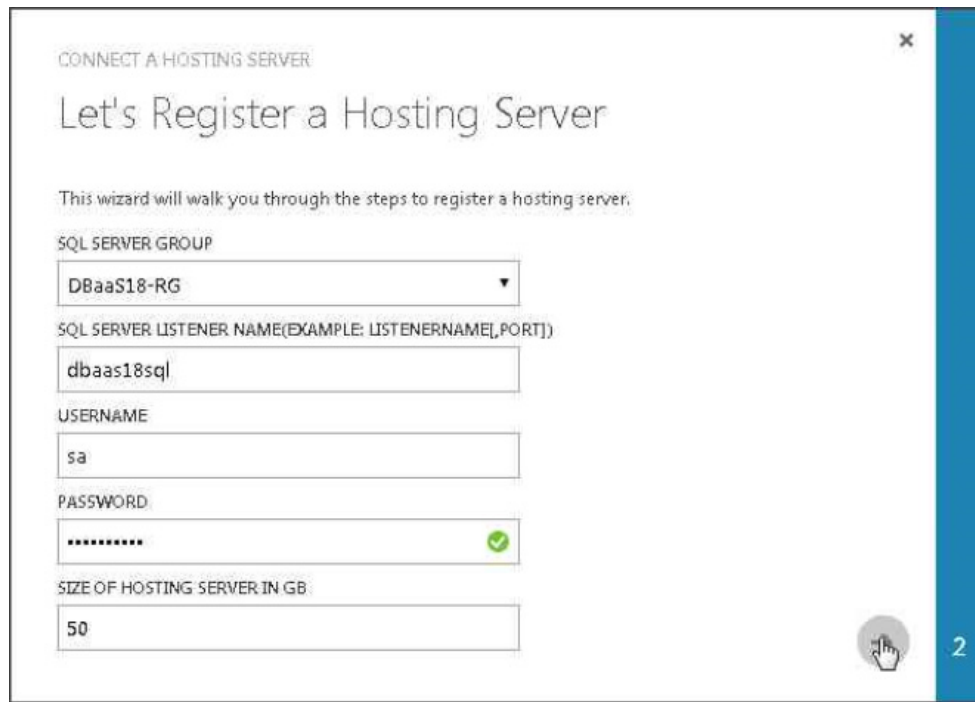
Step 4 Check the SQL Server Group View to verify that the Group is created when done.



Step 5 Add an SQL Server to the new group.



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



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

1

299877

299907

✓ SQL Server dbaaS181q1 has been added. OK

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

The screenshot displays the 'RESOURCE POOL TEMPLATES' section of the Cisco Cloud Network Automation Provisioner. The interface includes a left-hand navigation menu with categories like 'REQUEST MANAGEMENT', 'WEB SITE CLOUDS', 'VM CLOUDS', 'SERVICE BUS CLOUDS', 'SQL SERVERS', 'MYSQL SERVERS', 'AUTOMATION', 'PLANS', 'USER ACCOUNTS', and 'USER COSTS'. The main area shows a table of resource pool templates with columns for Name, Status, Instances, Max Subscriptions, CPU Cores, and Memory MB. The 'template-alwayson-cluster-01' is highlighted, and the 'ADD TEMPLATE' button is being clicked.

NAME	STATUS	INSTANCES	MAX SUBSCRIPTIONS	CPU CORES [MIN, MAX]	MEMORY MB [MIN, MAX]	...
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]
RS_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.

299878

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

MINIMUM SUBSCRIPTIONS PER VOLUME ?

10

2

299879

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)

MAXIMUM CPU TIME IN SECONDS PER REQUEST

Unlimited
MEMORY GRANT TIMEOUT IN SECONDS PER QUERY

Use Default
MAXIMUM SIMULTANEOUS REQUESTS Unlimited

MAXIMUM DEGREE OF PARALLELISM (DOP) Use

Default

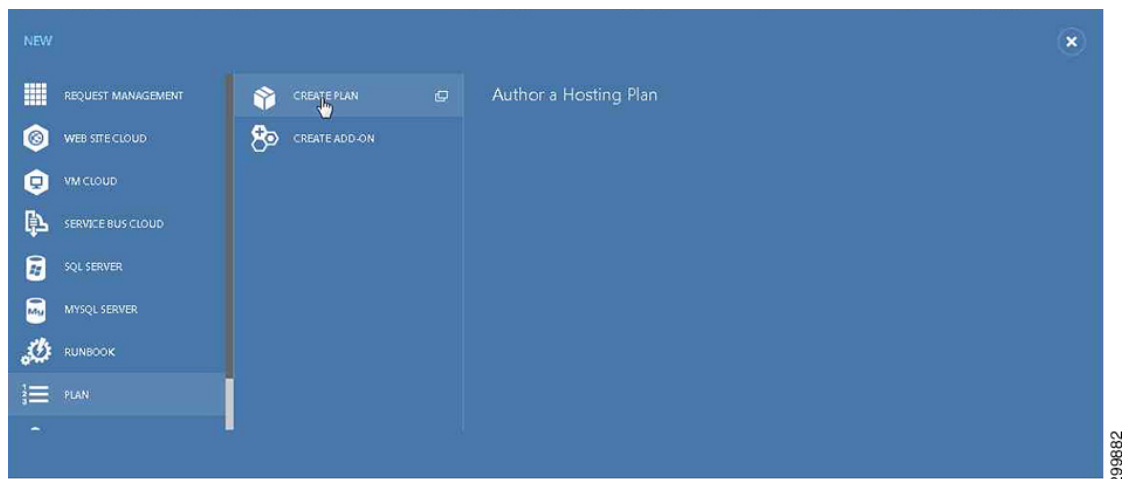
1

299880

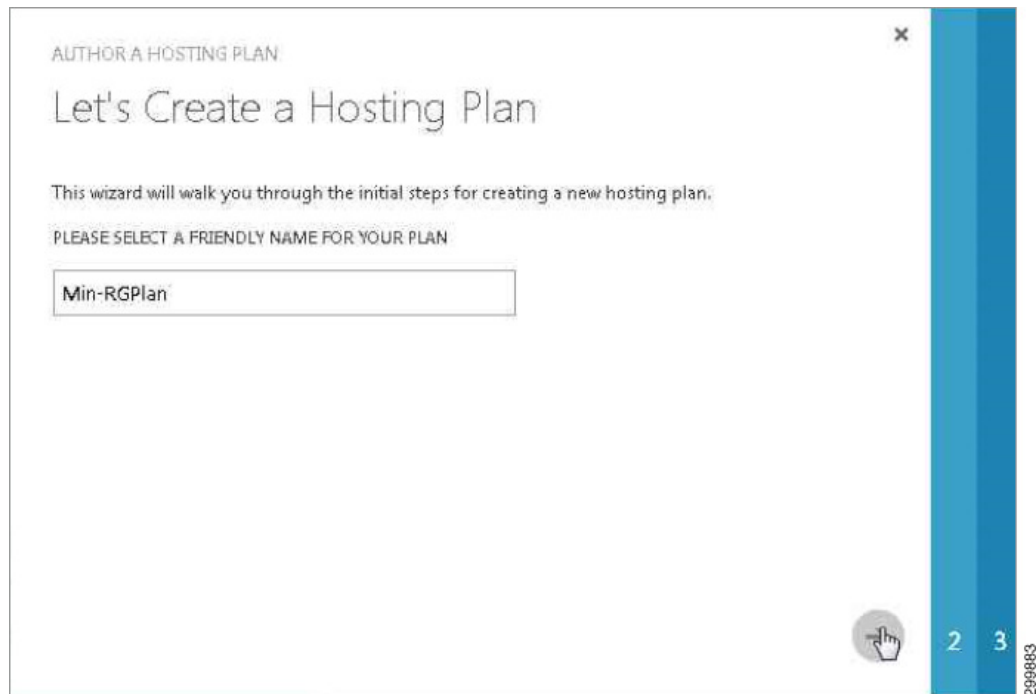
✓ Resource pool template Min-RG has been created. OK

299881

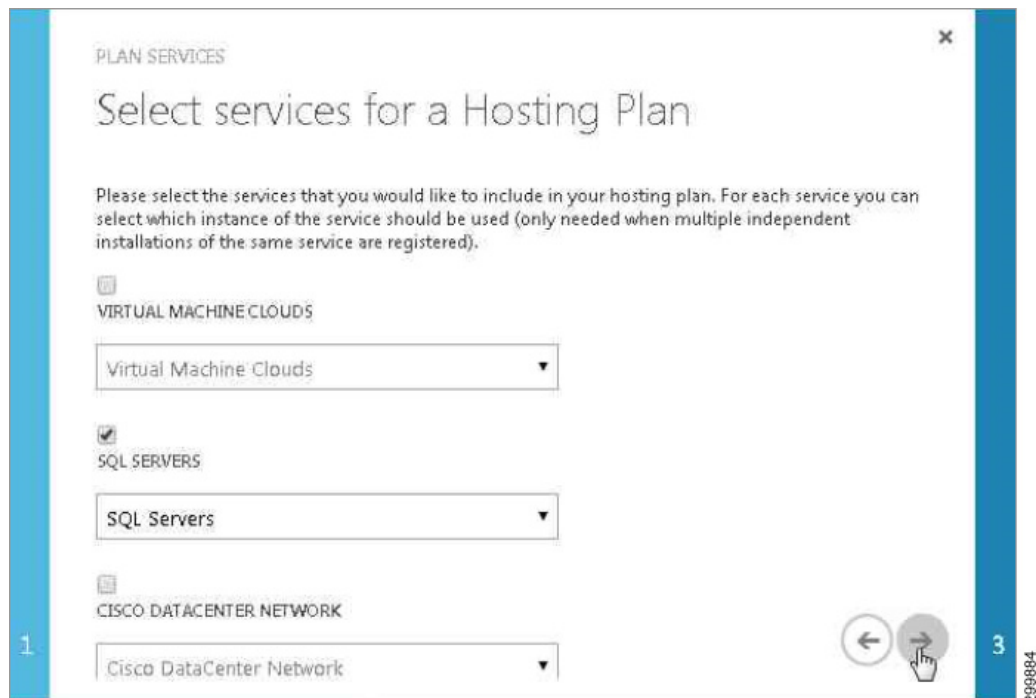
Step 10 Create a new plan.



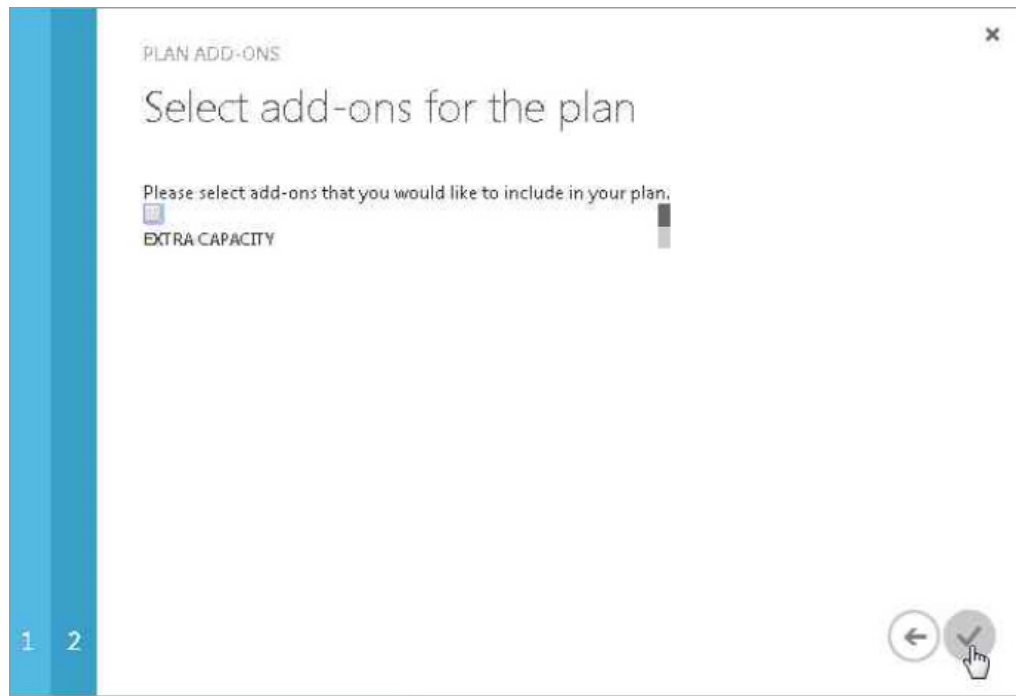
Step 11 In the plan creation view, specify the plan name.



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



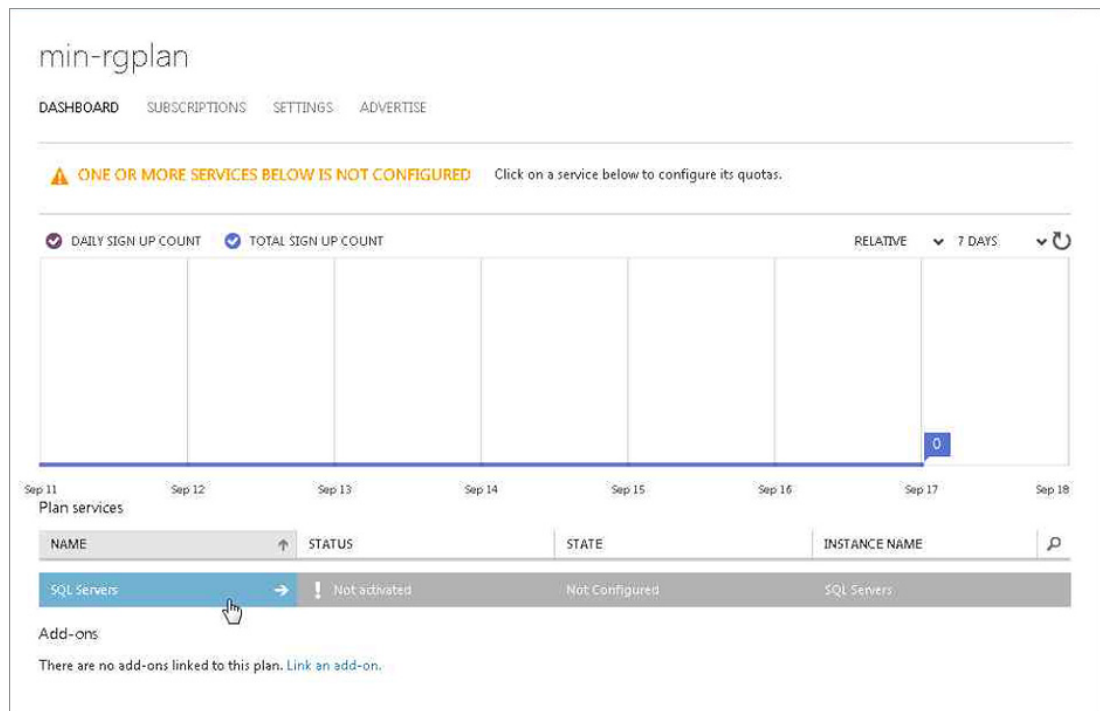
If add-on service options are defined (extra capacity in this example), they may be offered for inclusion in this new plan.



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

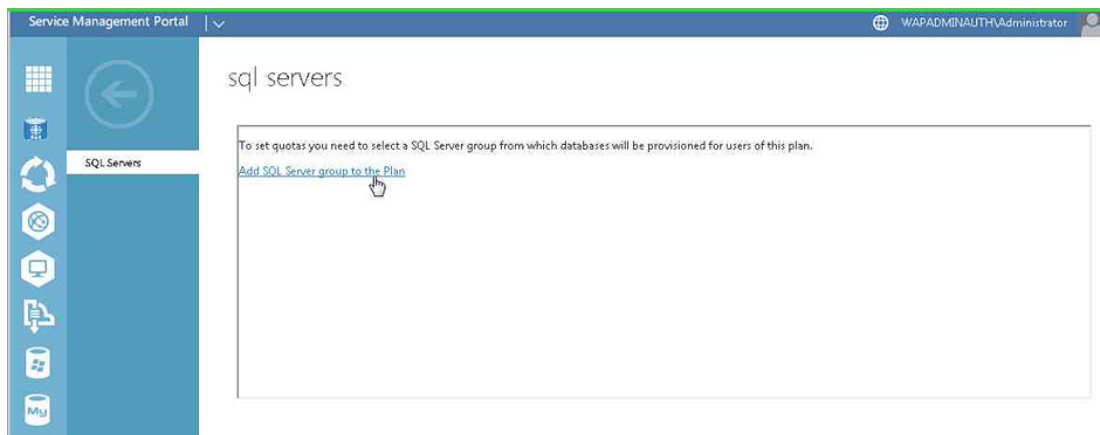
Plan Name	Visibility	Status	Count 1	Count 2	Identifier
DBaaS-Plan-001	Private	Configured	1	3	DBaaS19u9wor3
DBaaS-Plan-002	Public	Configured	3	1	DBaaS19ub0b4x
DBaaS-Plan-003	Public	Configured	2	2	DBaaS19a5h06rs
DBaaS-Plan-03	Public	Configured	1	3	DBaaS19ar0awb
DBTestPlan	Private	Not Configured	4	0	DBTest16q0lu
effCloudPlan01	Private	Configured	4	0	effC1iek8ygt1
IaaS-Plan9	Public	Configured	3	1	IaaS19ieffvo
lab1-plan	Public	Configured	2	2	lab11emz3h4j
lab1vm	Private	Configured	3	1	lab1vm1en3ogpk
Min-RGPlan	Private	Not Configured	4	0	MinRG1eoink2g
RG-Plan-High	Private	Configured	2	2	RGPla1azmuhi7
RG-Plan-Low	Private	Configured	2	2	RGPla1azmu73l

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.



299888

- 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.



299889

- 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

208809

- 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.

The screenshot displays the 'sql servers' management interface. On the left is a navigation sidebar with various icons. The main area shows a table with the following data:

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

At the bottom of the interface, a blue notification bar contains the following text: "Update for plan Min-RGPlan is in progress, it might take up to a few minutes to complete. Impacted subscriptions will be updated." with an 'OK' button and a refresh icon.

- 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.

The screenshot displays the 'min-rgplan' dashboard in the Tenant SQL Resource Provider User Interface. The interface includes a left-hand navigation menu with various plan and service options. The main content area shows a 'PLAN IS PRIVATE' warning, a chart for sign-up counts, and a table of plan services. A 'Decommission' button is visible in the bottom right corner of the main content area. Below the screenshot are two notification banners: one indicating an update for the plan is in progress, and another asking to make the plan public.

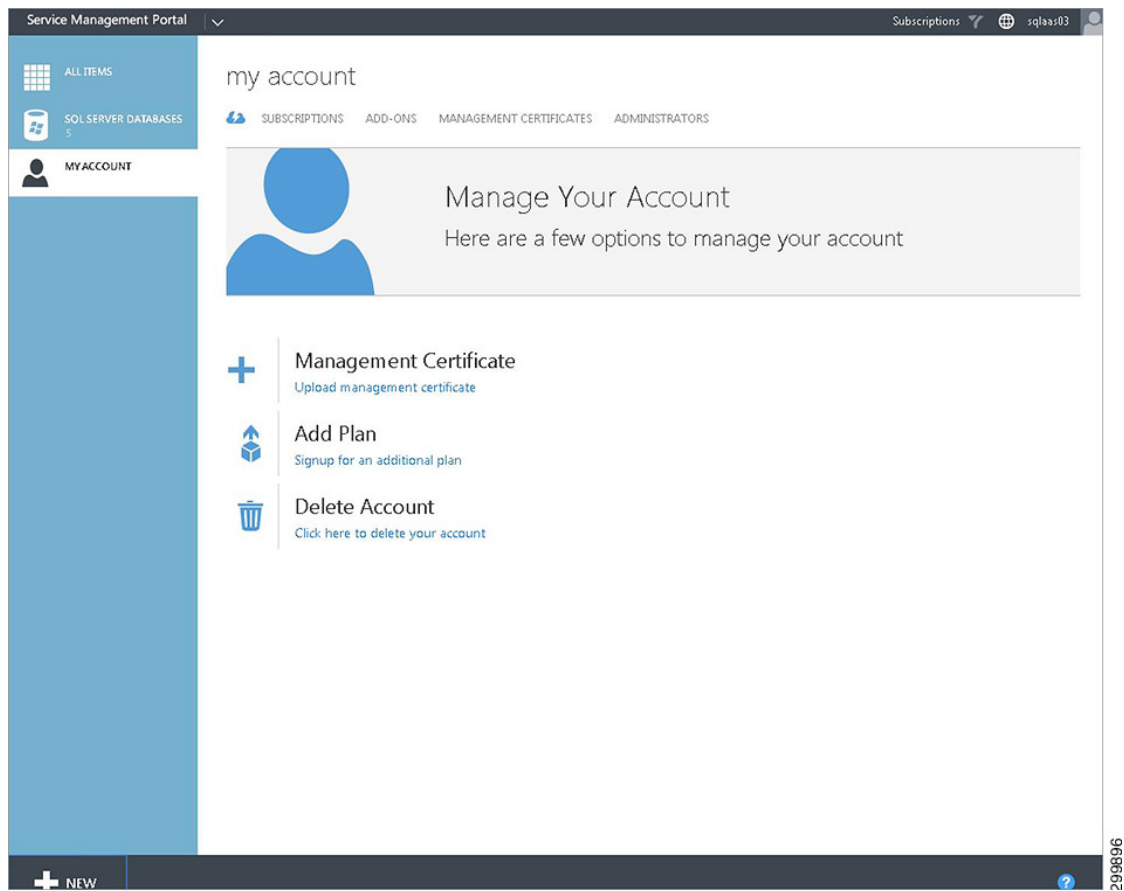
299893

299894

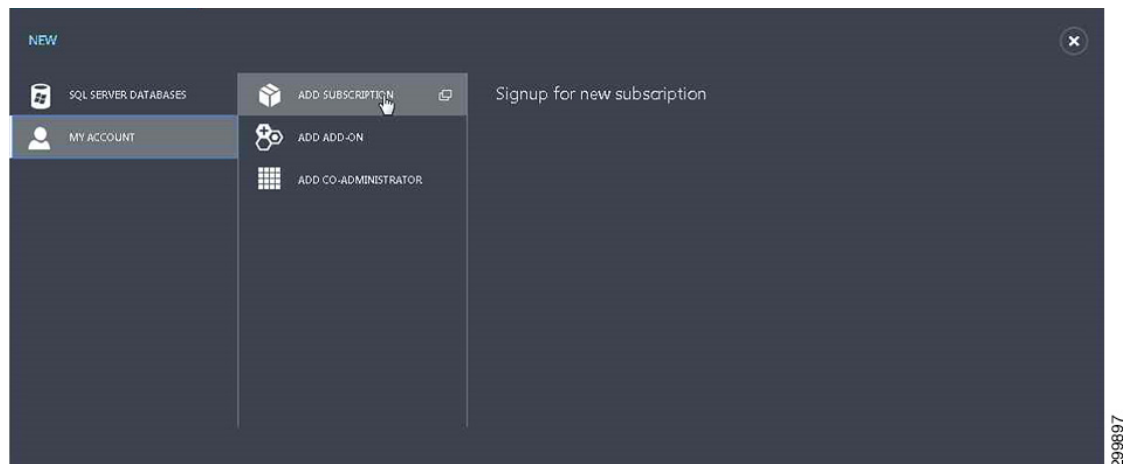
299895

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

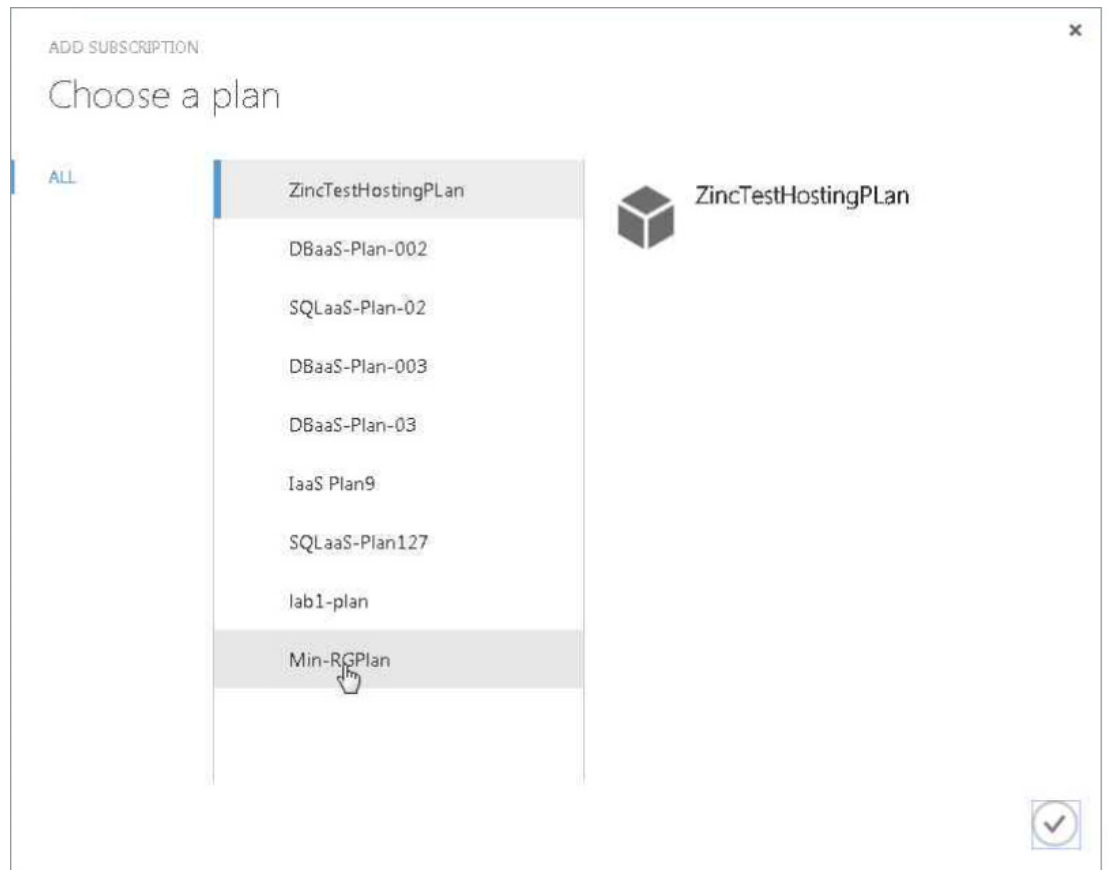
- Step 1** Login to the WAP Tenant Administrator portal. Enter your username/password.
- Step 2** Subscribe to a plan. Go to My Account and select **Add Plan**.



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

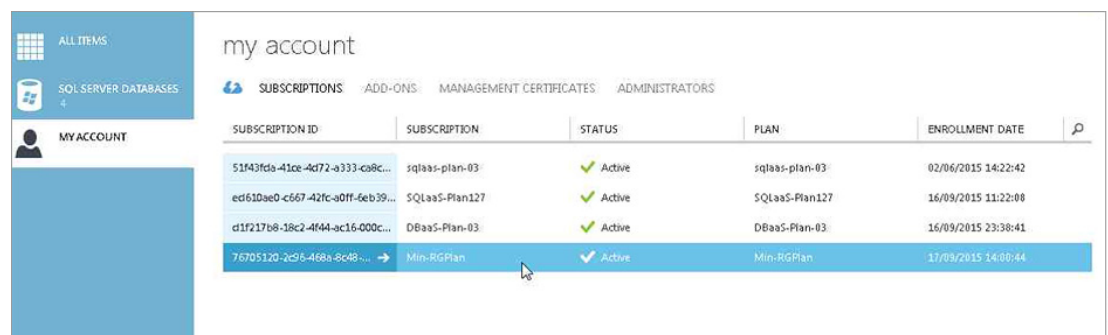


- Step 3** From the resulting list of available plan(s) previously created and published through the SP Admin UI, select a shared DBaaS plan.



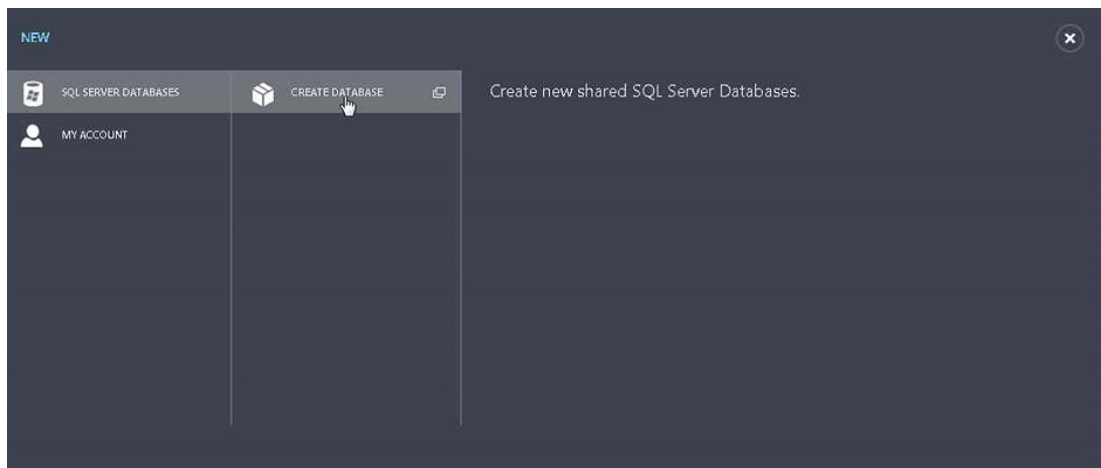
299898

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



299899

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.

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

CREATE DATABASE

Database Credentials

ADMIN NAME
User2 ✓

PASSWORD
***** ✓

PASSWORD CONFIRMATION
***** ✓

1

← →

2999002

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

Service Management Portal

Subscriptions sqlbaa:03

ALL ITEMS

SQL SERVER DATABASES 5

MYACCOUNT

sql server databases

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

2999003

✓ Successfully created database JMDDb. OK

2999004

+ NEW

VIEW INFO DELETE CHANGE PASSWORD RESIZE

2999005

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=MDDB;User ID=User2;Password=<<Your-DB-password-here>>;Asynchronous Processing=True



2989006