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

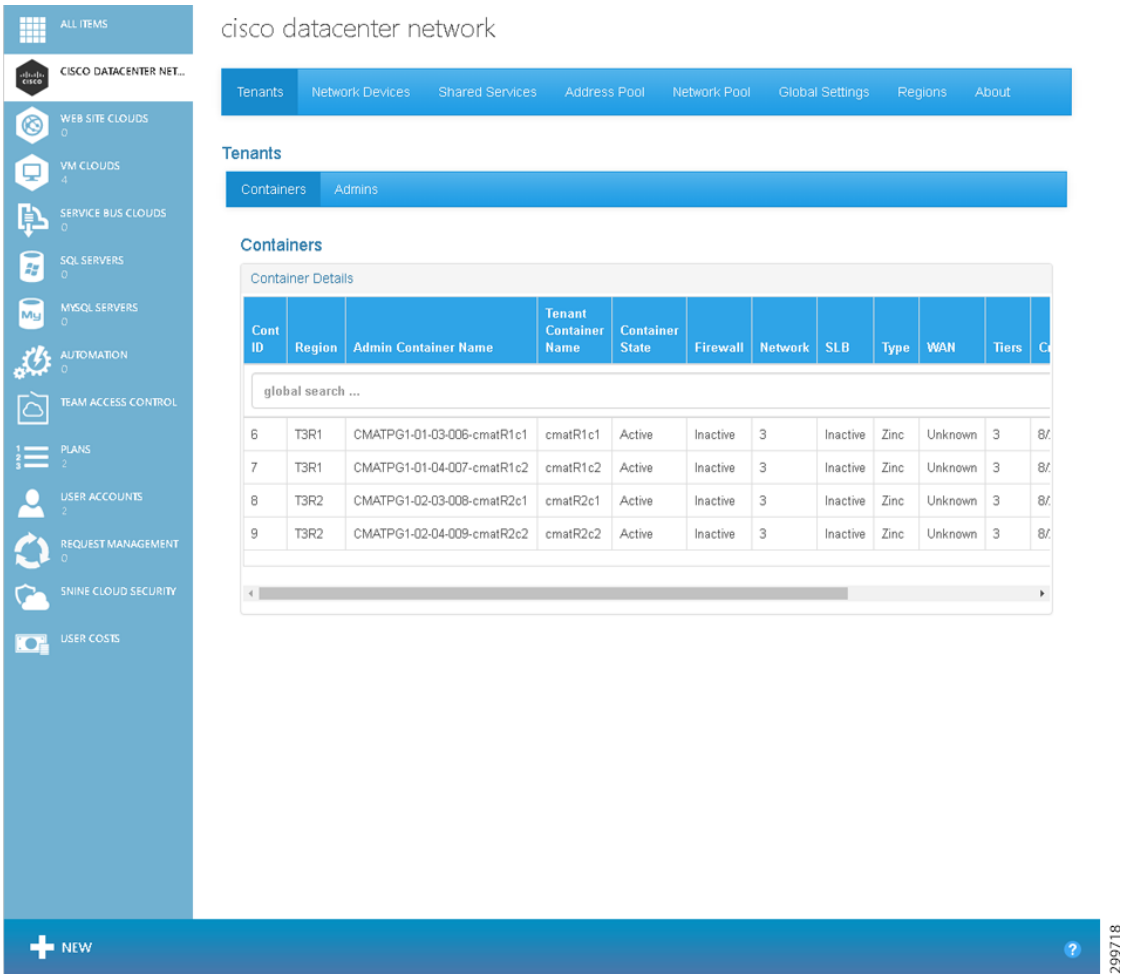
Once a container plan is created, customers can use the Tenant Portal to subscribe to any of the available public container plans. For more information, see *Cisco Cloud Network Automation Provisioner for the Microsoft Cloud Platform—Tenant Portal Guide, Release 2.1*.

Creating a Network and Virtual Machine Cloud Container Plan

To create a network and virtual machine cloud container plan:

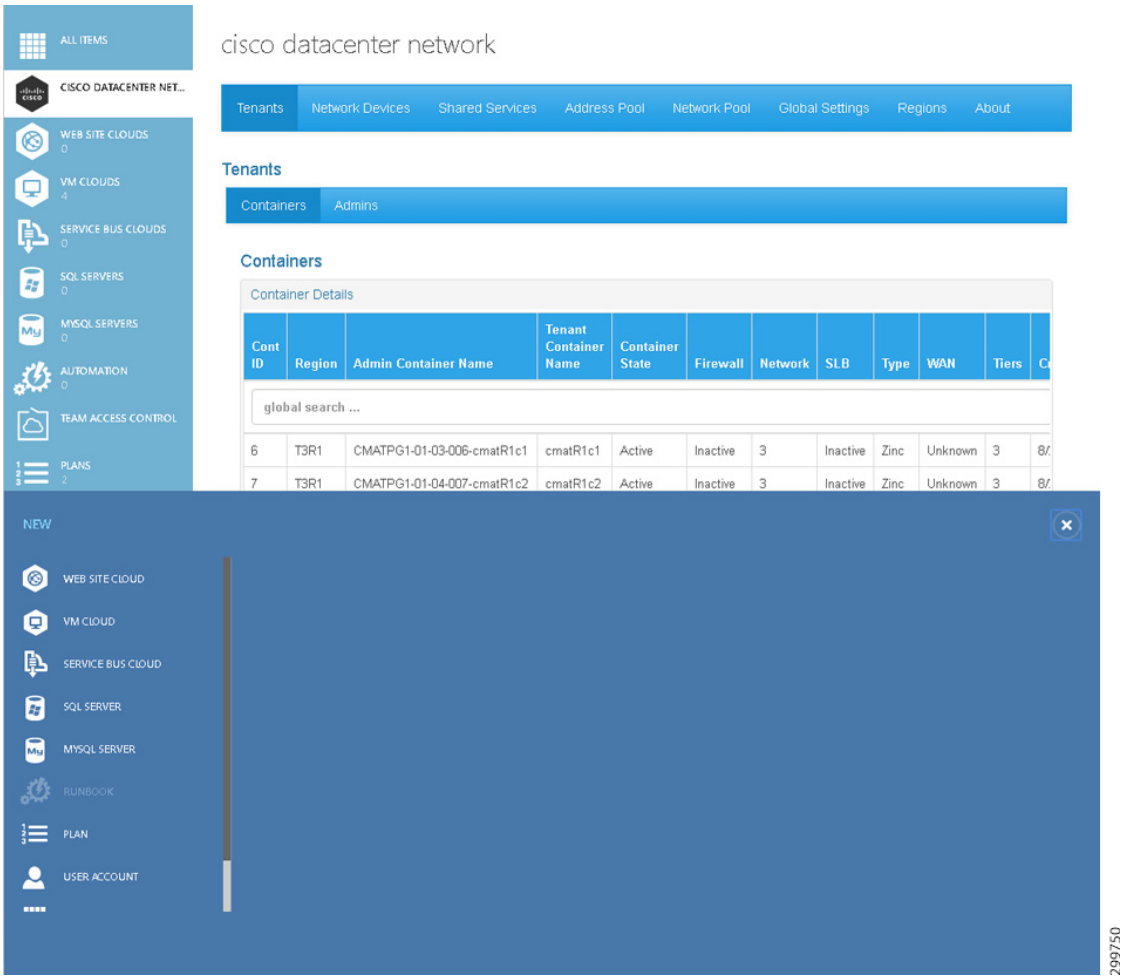
Step 1 On the Tenants Tab screen, click **+ New** in the lower left corner, as shown in the following screen. You can also click **PLANS** on the main WAP screen.

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.

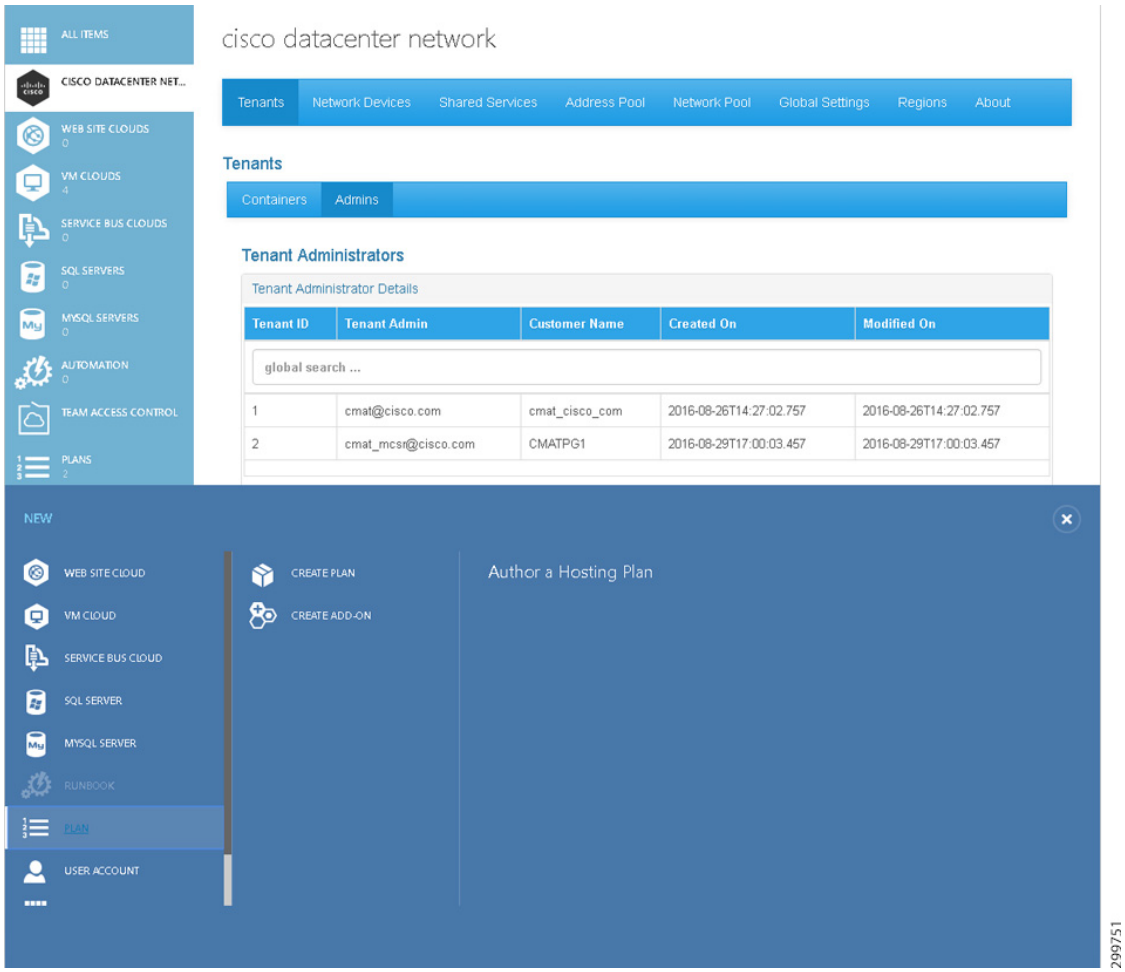
Figure 4-2 Creation Options Screen



Step 2 Click **Plan**.

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

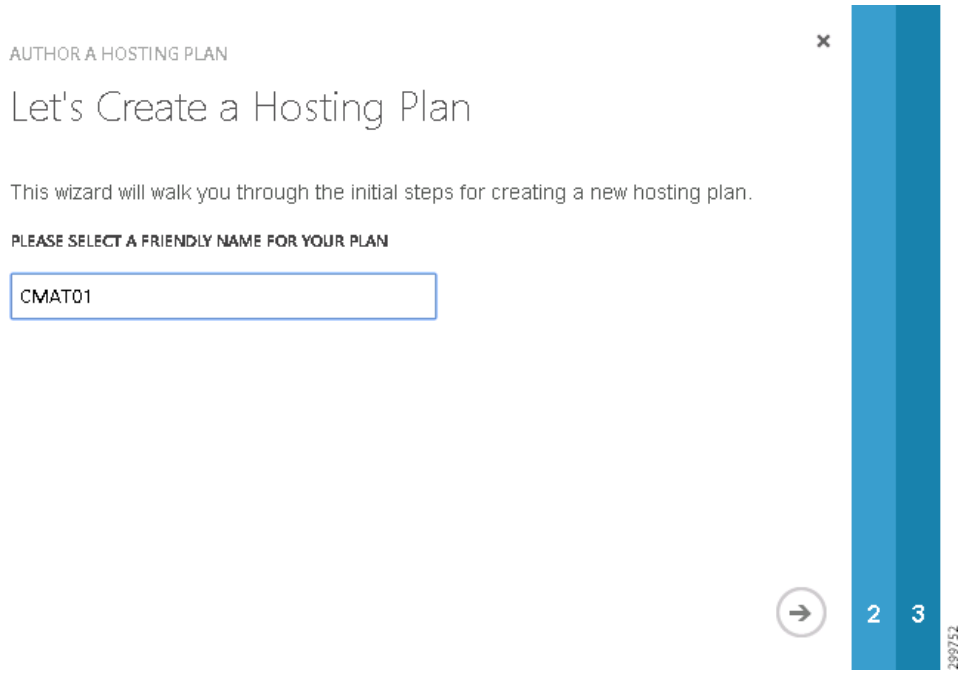
Figure 4-3 Plan Creation Options Screen



Step 3 Click **Create Plan**.

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

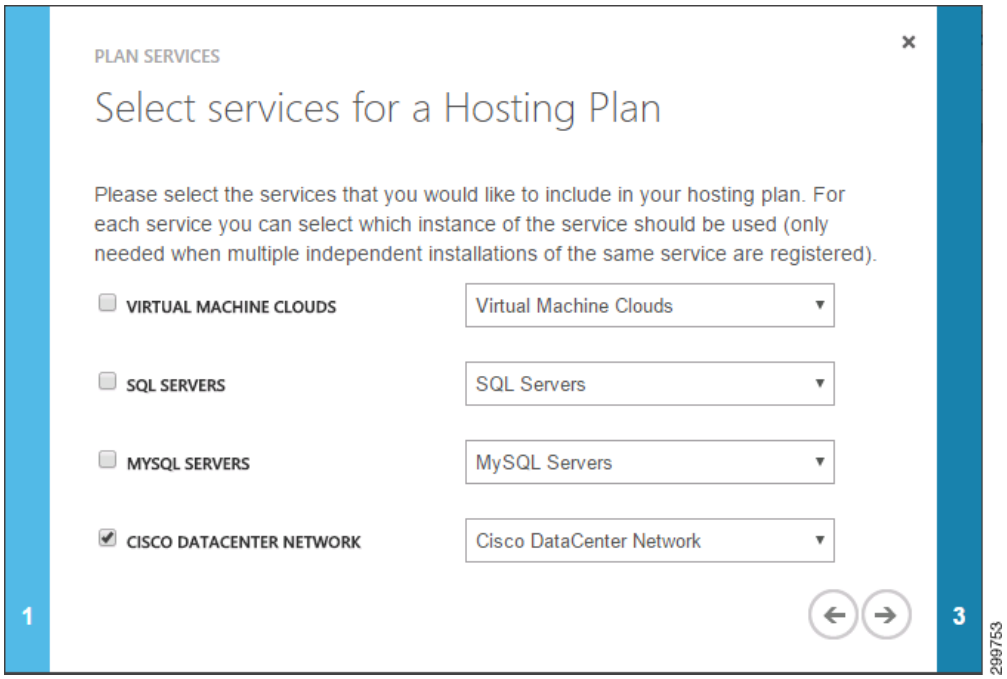
Figure 4-4 Create a Hosting Plan Screen



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.

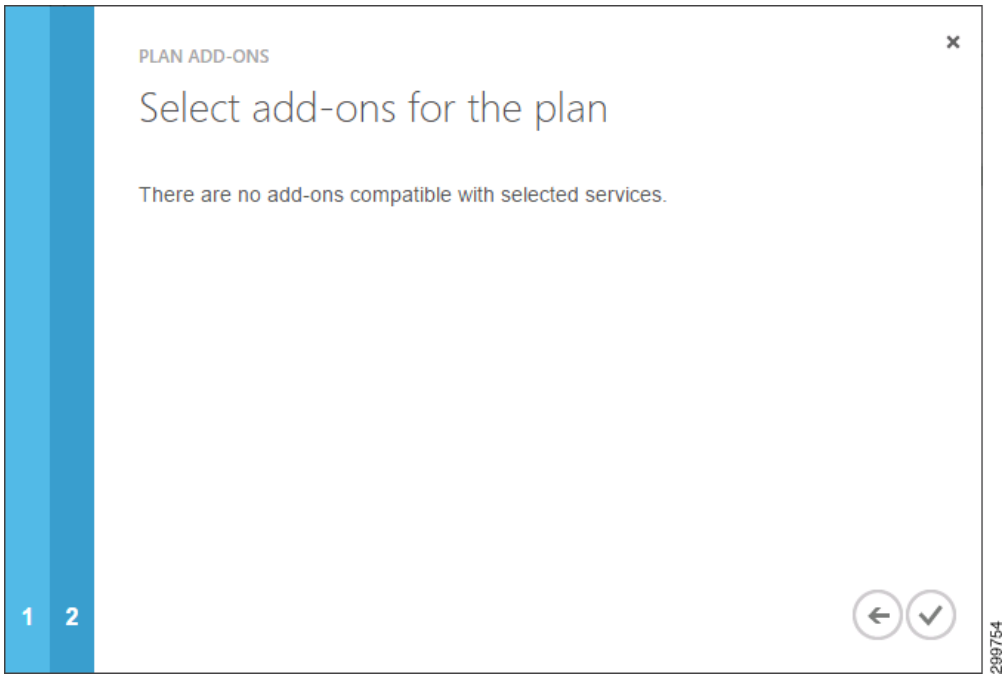
Figure 4-5 Select Services Screen



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

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

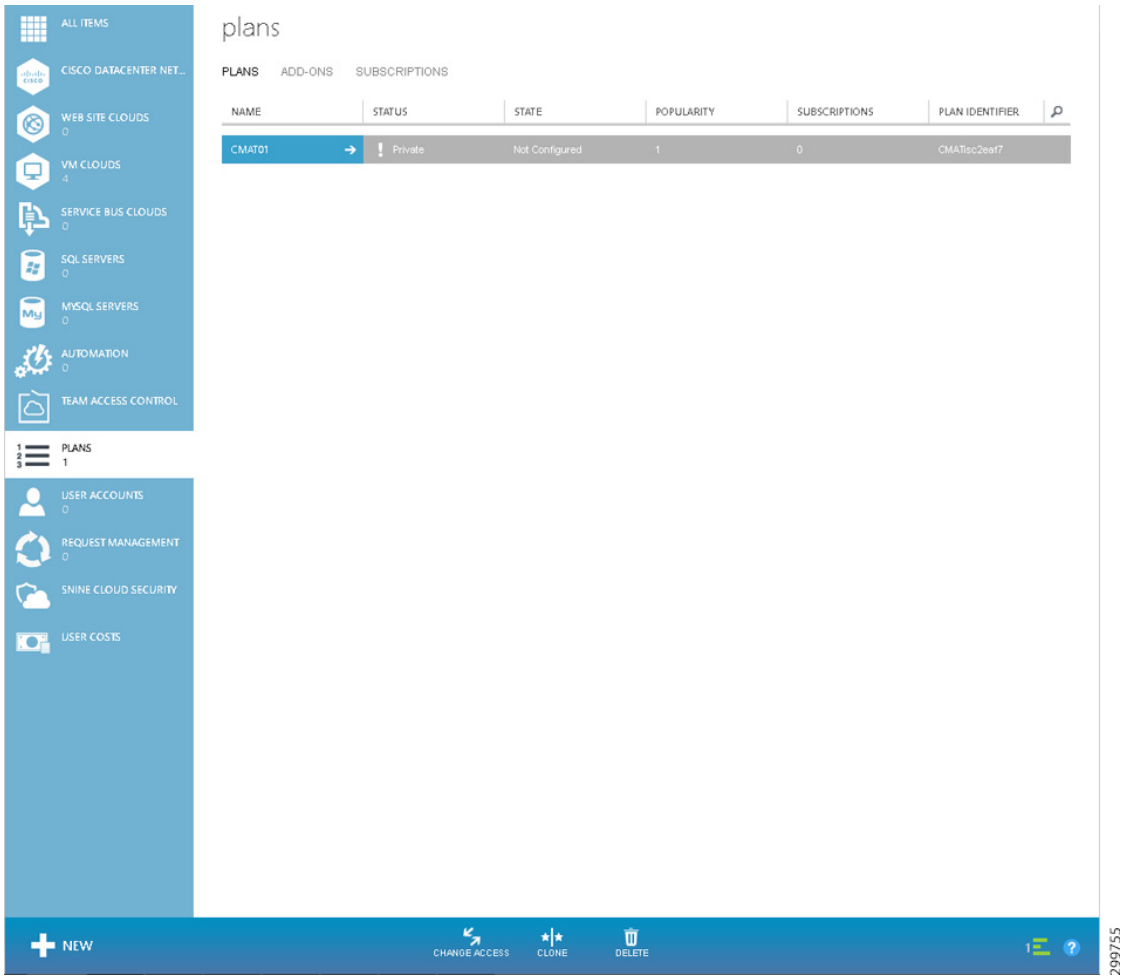
Figure 4-6 Select Add-Ons Screen



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.

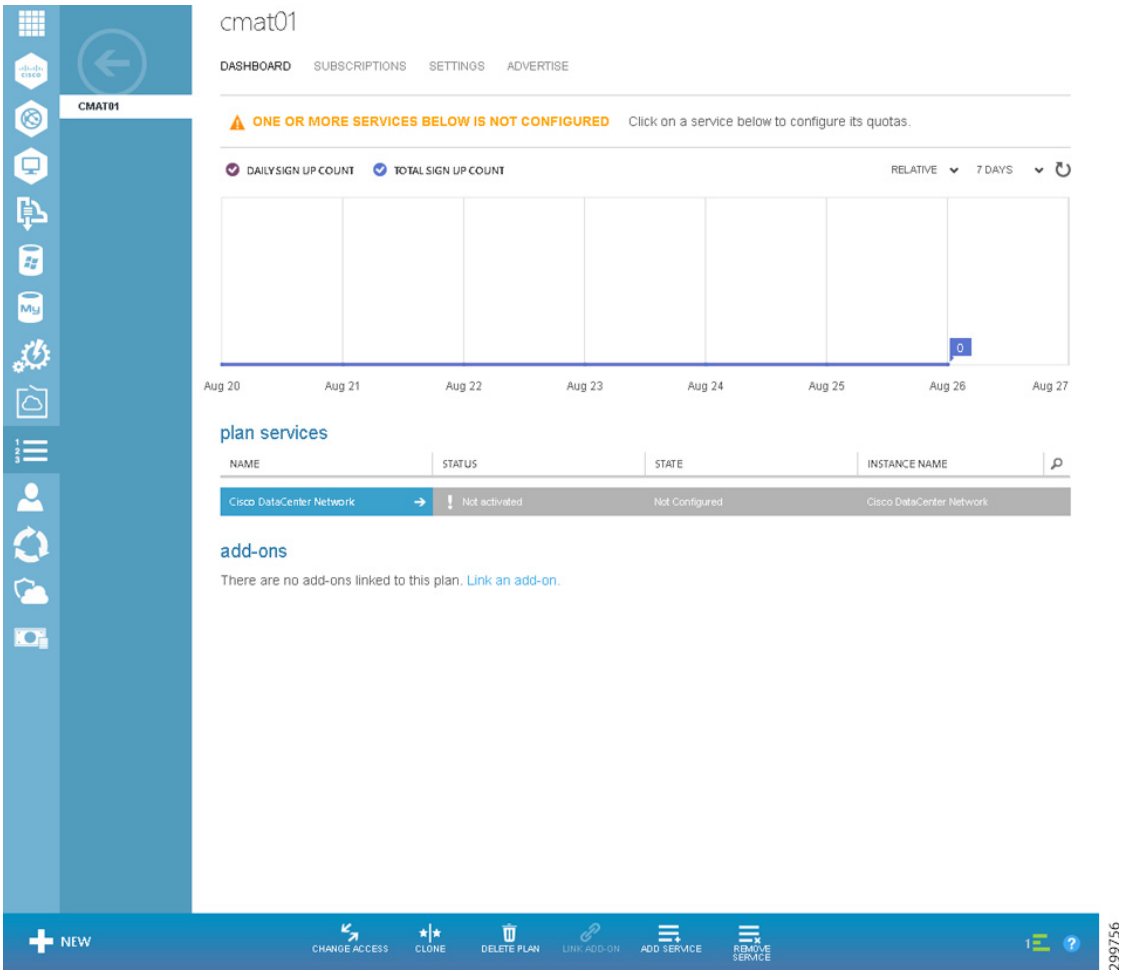
Figure 4-7 Plans Screen



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

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

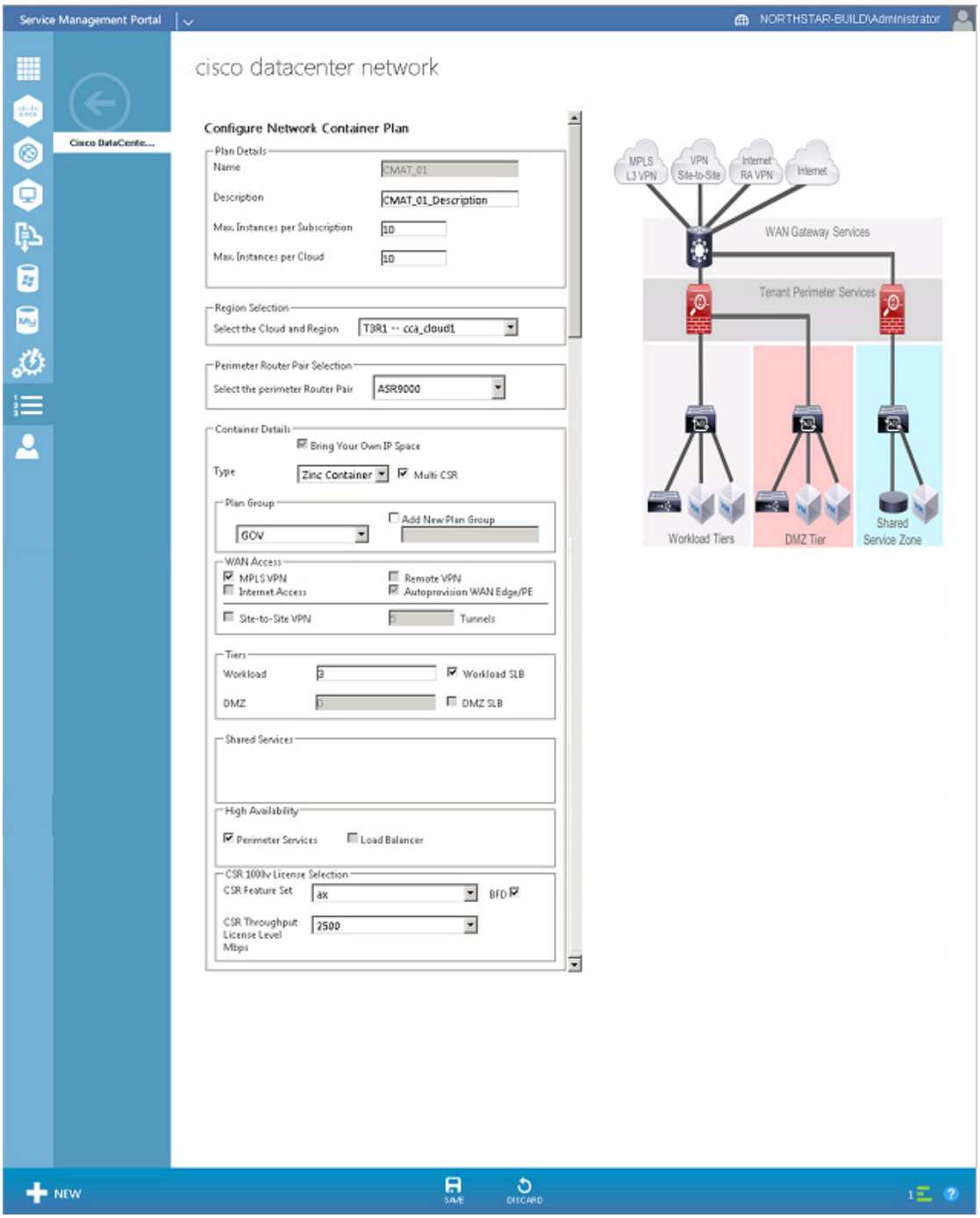
Figure 4-8 Plan Detail Screen



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.

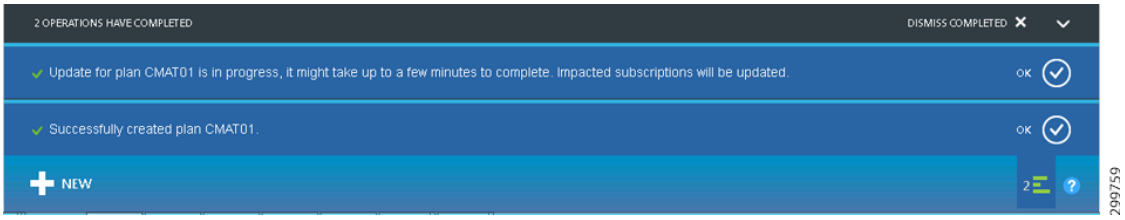
– CSR 1000V License Selection—First select the CSR Feature Set using the pull-down menu, then select the CSR Throughput Level using the pull-down menu. The options available on the CSR Throughput Level pull-down menu depend on what you selected for the CSR Feature Set.

  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.

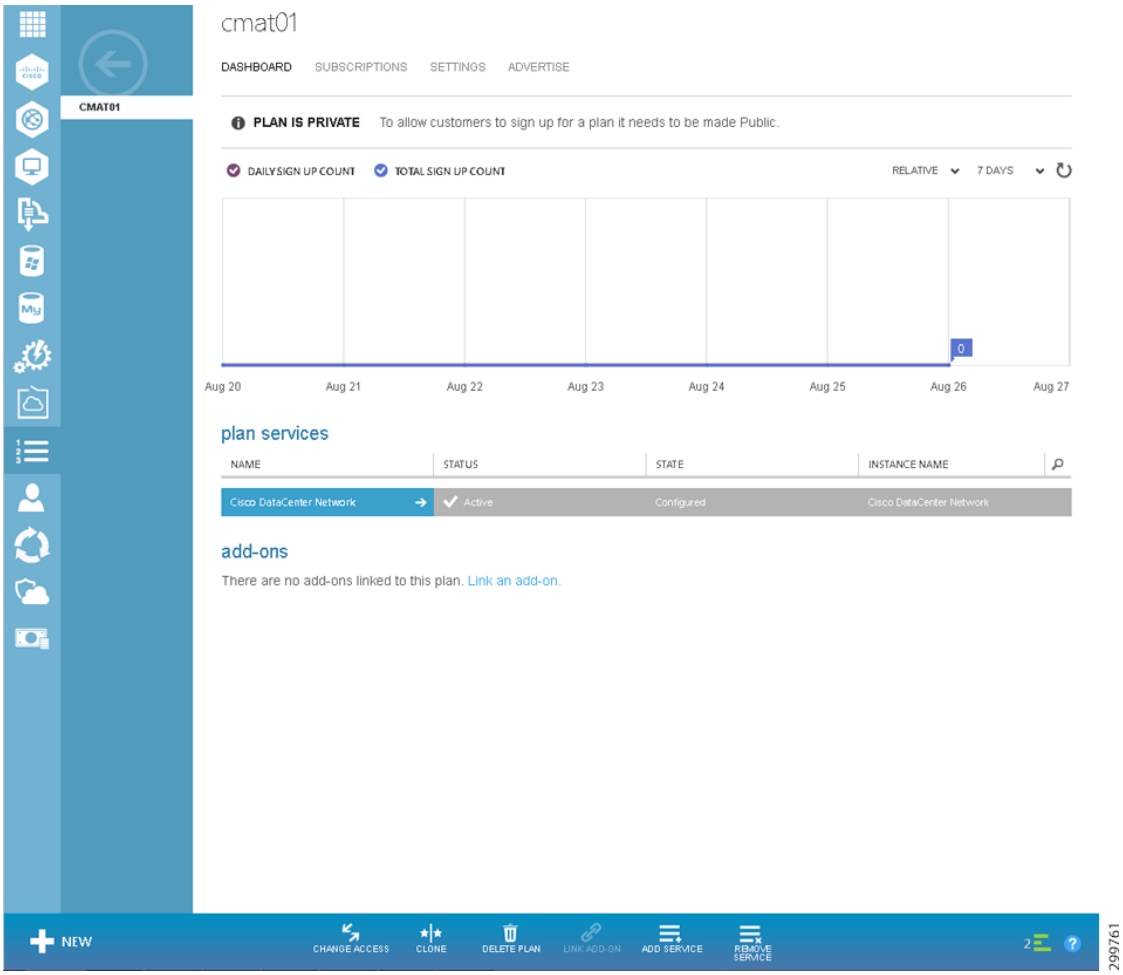
Figure 4-10 Configure Network Container Plan Screen—Update in Progress



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.

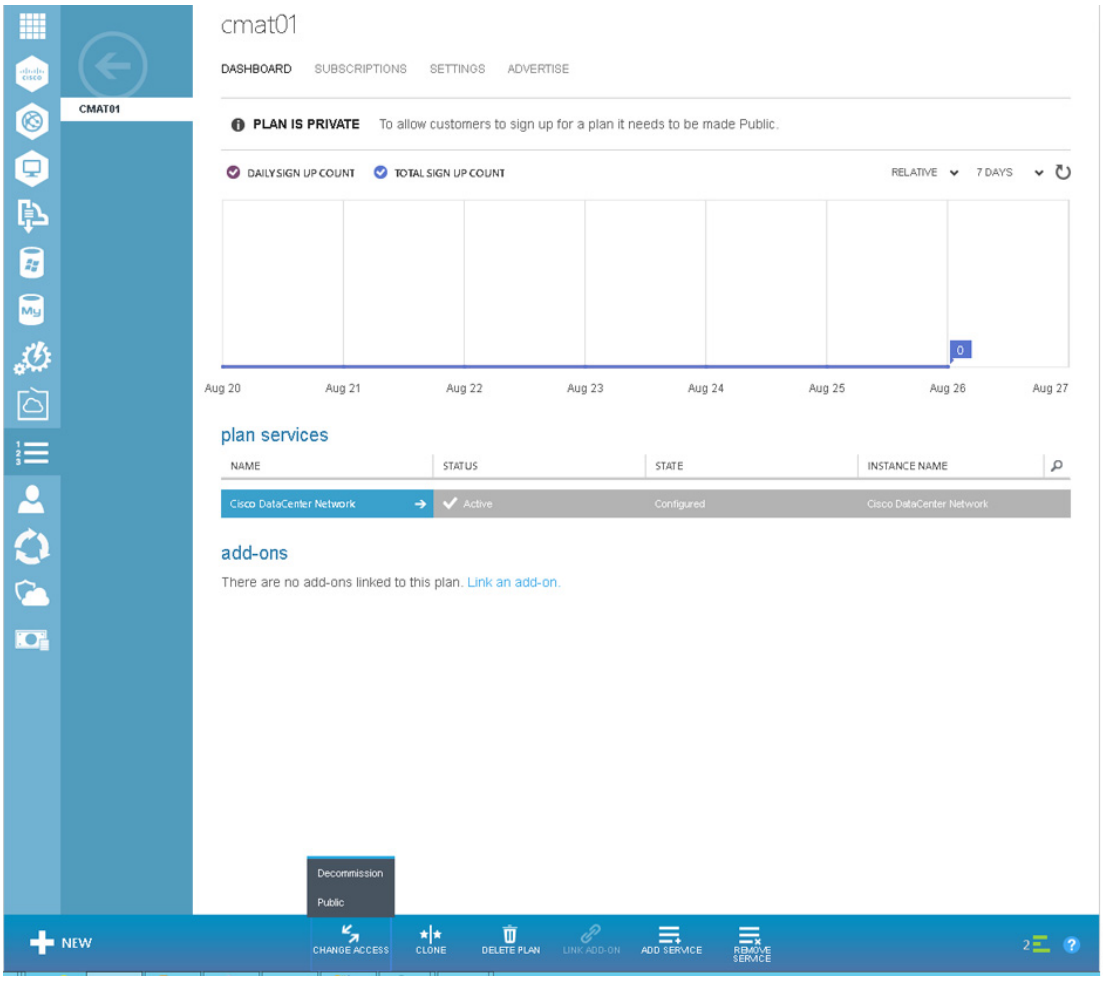
Figure 4-11 Plan Detail Screen—Plan Active and Configured



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.

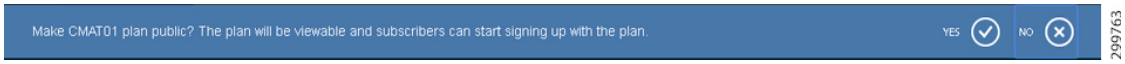
Note You can leave the plan Private and then manually assign tenants to the plan.

Figure 4-12 Change Access to Public Screen



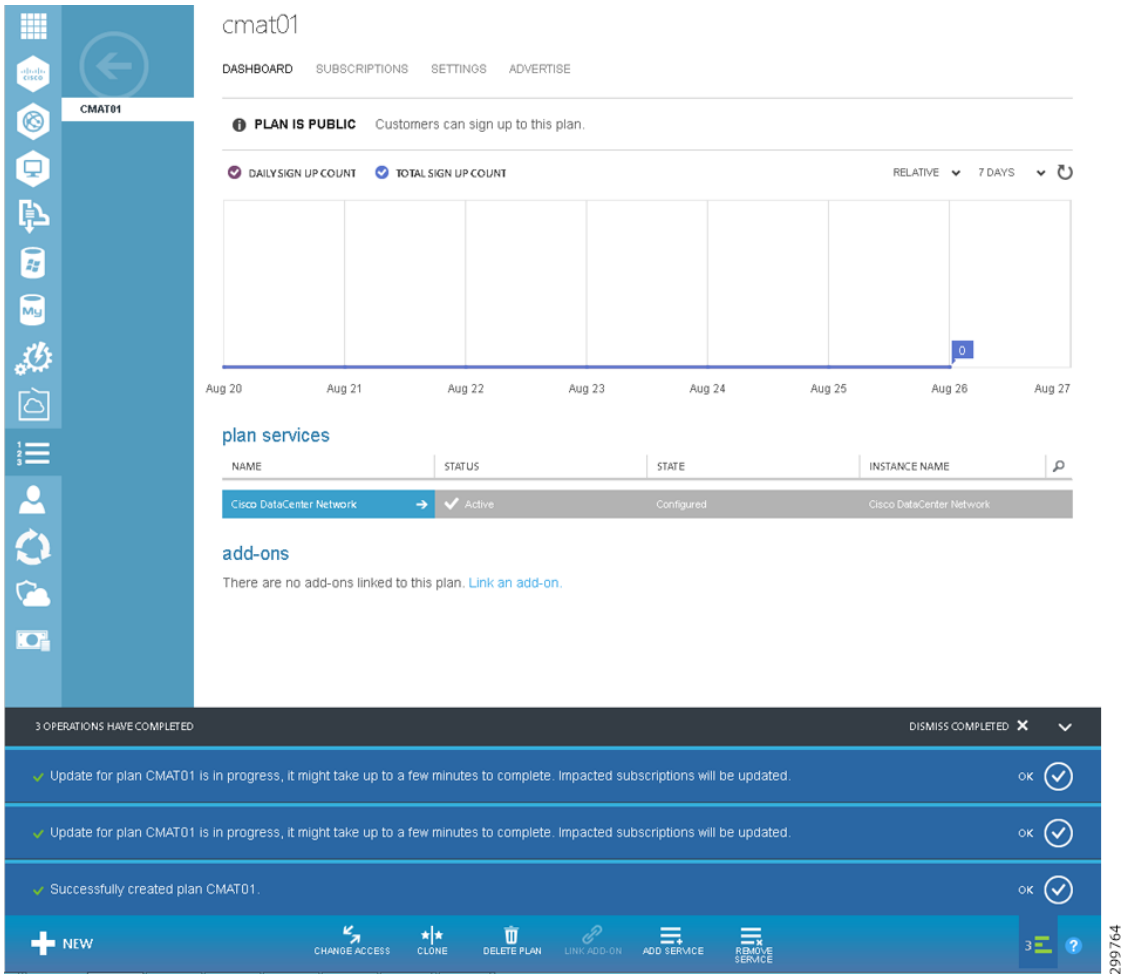
Step 13 You see a pop-up asking you to confirm you want the plan to be public, as shown in the following screen. Click **Yes**.

Figure 4-13 Confirm Public Access Screen



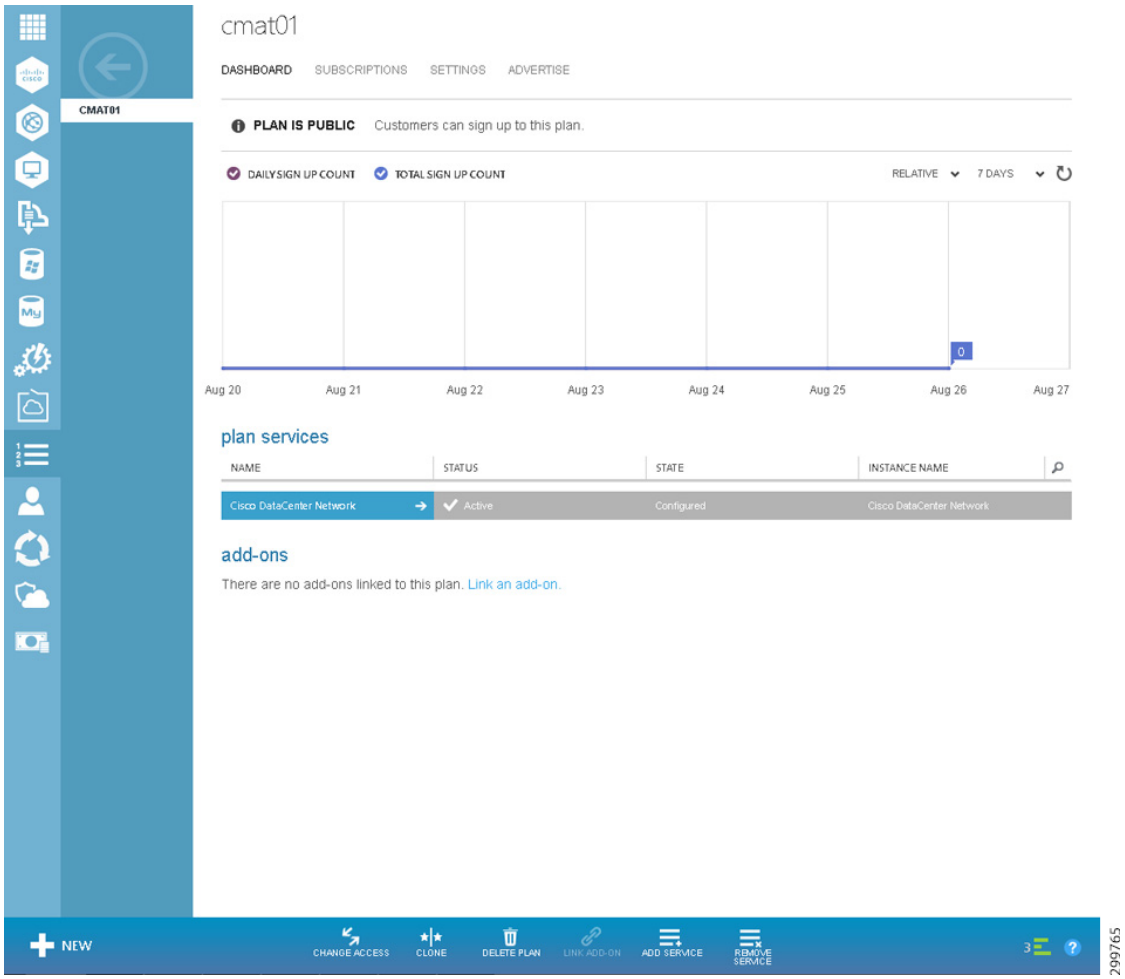
You see a message at the bottom of the screen while the configuration is being saved, as shown in the following screen.

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**.

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.