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/CNAP2-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.

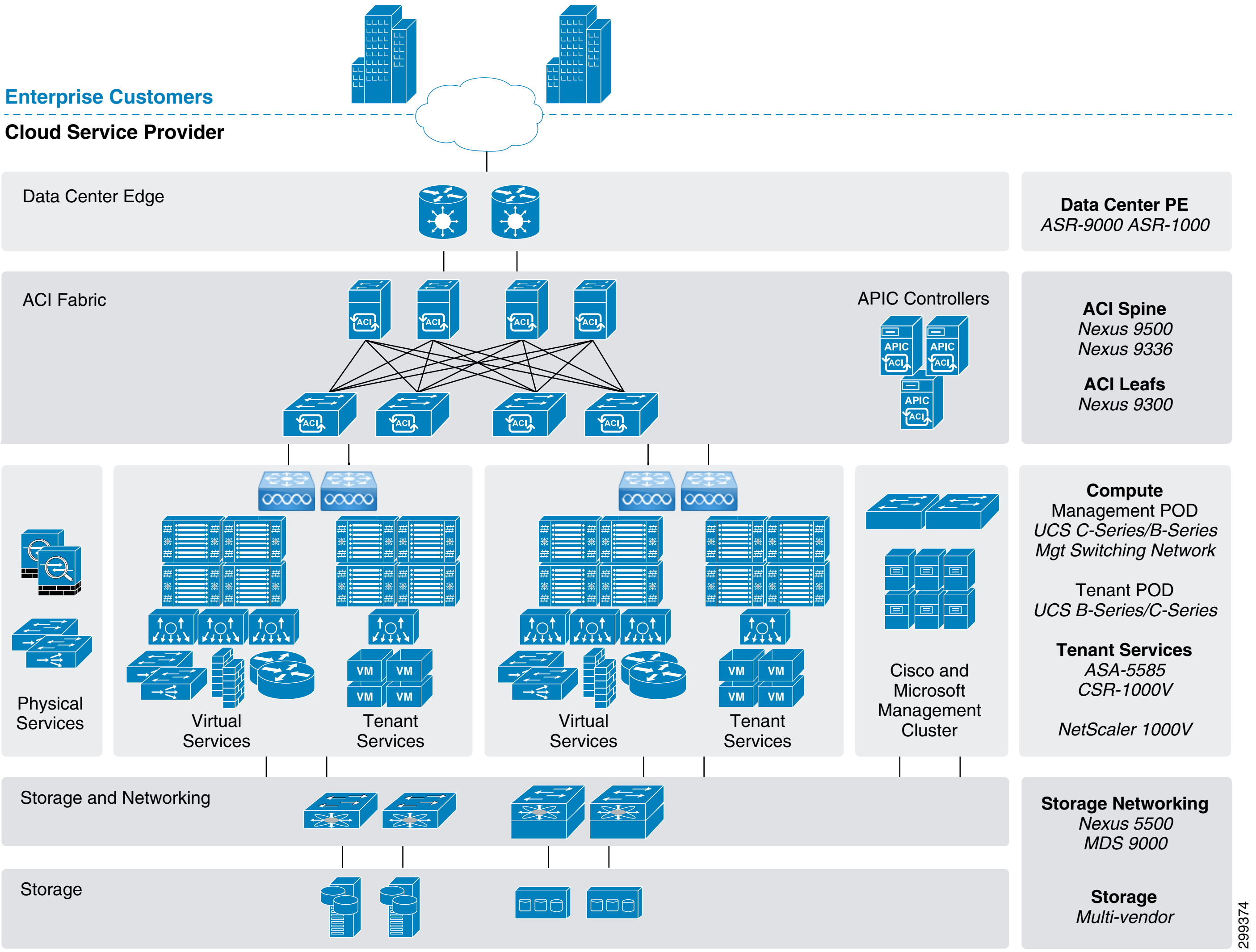
Refer to the *Cisco Cloud Architecture for the Microsoft Cloud Platform: Infrastructure Foundation Guide, Release 1.0* for detailed information on building data centers using physical components to implement compute, storage, and data center networking to create a pool of resources that are then used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

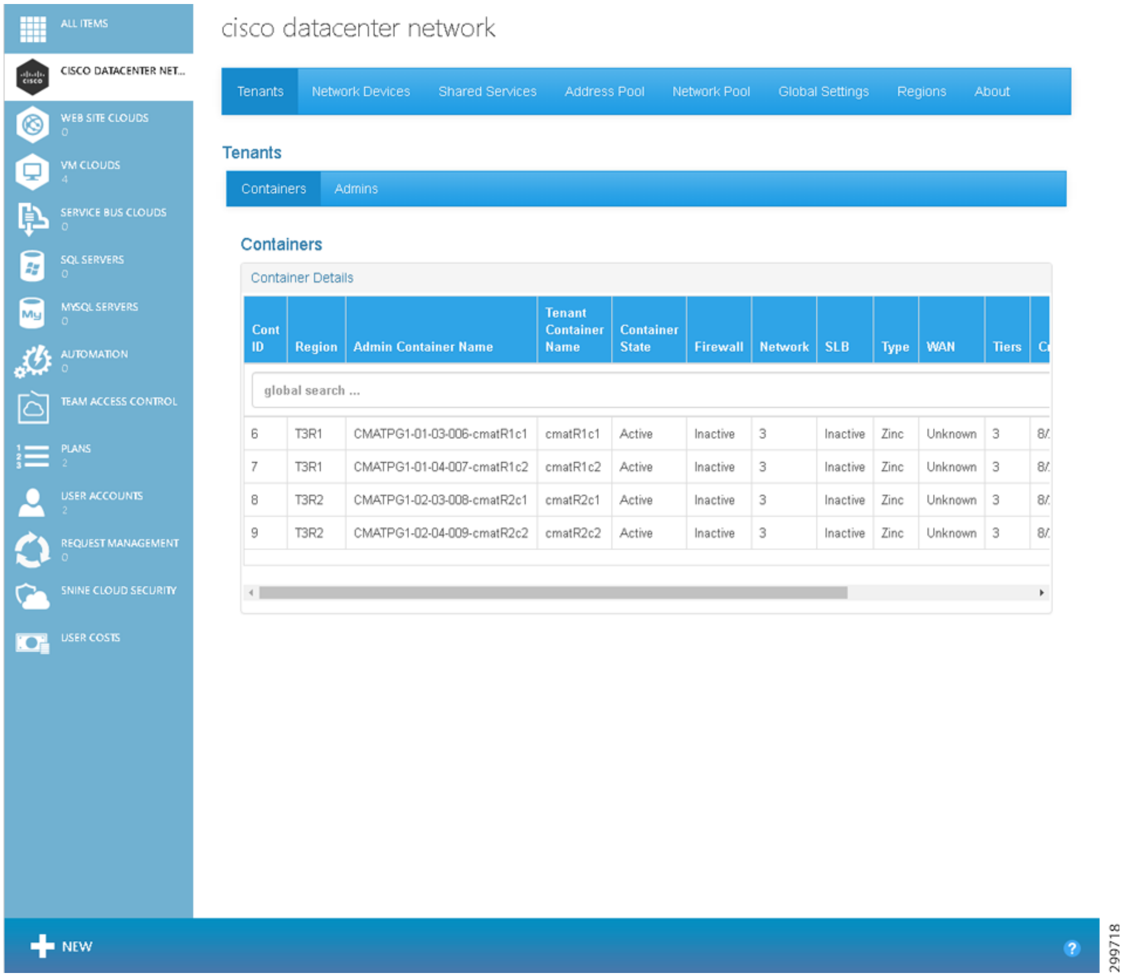
Step 1 Access the WAP Admin Site and log in as an administrator.

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



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/