



# **Cloud Orchestration for VMDC VSA 1.0 with IAC 4.0 Design and Implementation Guide**

May 23, 2014

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, FIIP addressshare (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.

NetApp, the NetApp logo, Go further, faster, Data ONTAP, FlexPod, FlexVol, MetroCluster, OnCommand, RAID-DP, SnapMirror, Snapshot, and SyncMirror are trademarks or registered trademarks of NetApp, Inc. in the United States and/or other countries.

*Cloud Orchestration for VMDC VSA 1.0 with IAC 4.0 Design and Implementation Guide Design Guide*  
© 2014 Cisco Systems, Inc. All rights reserved.



## CHAPTER 1

### Solution Overview 1-1

Cloud Orchestration	1-2
VMDC Architecture	1-2
VMDC Modular Components	1-3
Pod	1-4
ICS Stack	1-4
VMDC VSA 1.0 Overview	1-5
VSA 1.0 Architecture	1-6
VSA 1.0 Virtual Service Platforms	1-8
IAC 4.0 Overview	1-9
IAC 4.0 Architecture	1-9
IAC 4.0 Components	1-10
Key New Features	1-13
High-Level Workflow	1-13
Validated Components	1-16
VSA 1.0 Components	1-16
IAC 4.0 Components	1-18

## CHAPTER 2

### Solution Design 2-1

VMDC VSA 1.0 Network Containers	2-1
VMDC VSA 1.0 Gold Network Container (Two Zones)	2-3
VMDC VSA 1.0 Silver Network Container	2-5
VMDC VSA 1.0 Bronze Network Container	2-6
VMDC VSA 1.0 Container Details Not Orchestrated by IAC 4.0	2-7
IAC 4.0 Orchestration Design	2-8
Physical Resources	2-8
Compute Pod	2-8
Network Pod	2-10
Discovery of Resources	2-11
Logical Resources	2-12
IP Addresses	2-12
VLANs	2-13
Networks	2-13

Network Provisioning	2-14
Layer 2 Provisioning	2-14
Layer 3 Provisioning	2-14
Tenant Design	2-17
Tenant Structure	2-17
IAC 4.0 Multi-Tenancy	2-18
IAC User Roles and RBAC	2-18
VDC Connection Type	2-19
Organization Design	2-20
Virtual Data Center (Network Container) Design	2-21
IAC 4.0 Network Containers	2-22
Gold Network Containers	2-23
Silver Network Containers	2-25
Bronze Network Containers	2-27

## CHAPTER 3

### Solution Implementation 3-1

Installation Overview	3-1
Planning Guide	3-1
Physical Component Layout	3-4
Logical Component Layout	3-5
IAC Component Installation Steps	3-6
IAC Scalability	3-7
Scale Factors	3-7
Tuning for Scale and Performance	3-8
IAC Redundancy	3-8
Redundant Components	3-8
IAC Licensing	3-9
Pod Discovery and Onboarding	3-9
Network Pod	3-9
Discovering Network Devices	3-9
Register/Create a Network Pod	3-12
Compute Pod	3-14
Discovering Compute Infrastructure	3-14
Register/Create a Compute Pod	3-15
Management Components	3-16
vCenter	3-16
PNSC	3-18
Network Types	3-20



Resource Pools	3-22
VLAN Pools	3-22
IP Subnet Pools	3-22
Private Pool	3-22
Public Pool	3-23
IPAM	3-24

## CHAPTER 4

<b>Workflows and Use Cases</b>	<b>4-1</b>
Onboard a Tenant	4-3
Create Tenant Administrative Users	4-7
Create an Organization	4-8
Create Organization Technical Administrators and Server Owners	4-10
Create a Virtual Data Center	4-11
Approve the Virtual Data Center	4-14
Provision a Virtual Machine	4-16
Provision a Virtual Machine from a Template	4-18
Provision a Virtual Machine and Install an Operating System	4-20
Provision a Physical Machine	4-20
Managing Network Virtual Services	4-24
Firewall Service Management	4-24
Firewall Security Zones	4-25
Firewall Service Group Usage by IAC	4-27
Security Policy Configured During Virtual Data Center Service Ordering	4-27
CSR 1000V Security Policies Configured During Virtual Data Center Ordering	4-29
VSG Security Policies Configured During Virtual Data Center Ordering	4-29
Firewall Management in IAC	4-30
Virtual Data Center Firewall Management	4-32
VM Firewall Rule Management in IAC	4-33
NAT/Floating IP Service Management	4-34
Load Balancing Service Management in IAC	4-36
Firewall Security Policies with Load Balancing Service	4-37
Create LB Server During Organization Creation	4-39
Create a LB Server from My VDC	4-40
Create a LB Service Group	4-40
Bind VM to the LB Server	4-41
Unbind VM from LB Server	4-41
Remove LB Server	4-41
Remove LB Service Group	4-41
Network Service Management	4-42

Add Network to VDC 4-42

Remove Network from VDC 4-43

**APPENDIX A** **Related Documents** A-1

**APPENDIX B** **Limitations, Restrictions, Caveats** B-1

**APPENDIX C** **Defects** C-1

**APPENDIX D** **Configurations** D-1

Two-Zone Gold Container with Internet Transit D-1

Org Creation for CSR 1000V, VPX, VSG D-1

CSR 1000V D-1

VSG D-4

Citrix NetScaler VPX D-6

VDC Creation for CSR 1000V and VSG D-9

CSR 1000V D-9

VSG D-10

Firewall Rule Creation for CSR 1000V and VSG D-10

Enterprise > Unprotected Private Network D-10

Enterprise > Protected Private Network D-11

Internet > Unprotected Public Network D-12

Protected Public > Protected Private Network D-13

SLB Policy Creation for CSR 1000V, VPX, VSG D-14

CSR 1000V D-14

VSG D-15

VPX D-16

NAT Creation for CSR 1000V D-17

Network Creation for CSR 1000V, VPX, VSG D-17

CSR 1000V - Adding Two New Networks D-17

VSG - Adding Two Networks D-18

**APPENDIX E** **Glossary** E-1



## Preface

---

The Cisco Virtualized Multiservice Data Center (VMDC) system provides design and implementation guidance for Enterprises deploying Private cloud services, and for Service Providers building Public and virtual Private services. With the goal of providing an end-to-end system architecture, VMDC integrates Cisco and third-party products in the cloud computing ecosystem.

This design and implementation guide documents the introduction of Cisco Intelligent Automation for Cloud (CIAC) 4.0 to the VMDC ecosystem. Designed for cloud orchestration, IAC 4.0 supports the network and compute orchestration of VMDC Virtual Services Architecture (VSA) 1.0.

## Audience

This guide is intended for, but not limited to, system architects, network design engineers, system engineers, field consultants, advanced services specialists, and customers who want to understand how to deploy a Public or Private cloud data center infrastructure using Cisco Intelligent Automation for Cloud (IAC). This guide assumes that the reader is familiar with the basic concepts of Cloud Orchestration, Infrastructure as a Service, Virtualized Multiservice Data Center (VMDC), IP protocols, Quality of Service (QoS), and High Availability (HA), and that readers are aware of general system requirements.

## Document Objective and Scope

This design and implementation guide provides a comprehensive description of Cisco's Cloud Orchestration for Virtualized Multiservice Data Center (VMDC) Virtual Services Architecture (VSA) 1.0 with the Intelligent Automation for Cloud (IAC) 4.0 solution. Until this release, both the VMDC and IAC systems have developed independently. This document represents the results of a joint development effort focused on the IAC based orchestration of VMDC VSA 1.0 network containers.

The document is divided into the following chapters:

- Chapter 1, Solution Overview, provides an overview of both the VMDC VSA 1.0 and the IAC 4.0 orchestration architectures.
- Chapter 2, Solution Design, describes the design for VSA network containers and the IAC Tenant, Organization, and VDC Structures used to orchestrate those network containers.

- Chapter 3, Solution Implementation, illustrates implementation topics to include IAC installation, component relationships, solution initial configuration, and resource discovery.
- Chapter 4, Workflows and Use Cases, shows operational usage of the IAC solution to present Tenant onboarding, Organization virtual services instantiation, VDC network container selection, End User workload creation, and network services management.
- Appendix A - Appendix E is a collection of reference information such as related documentation, solution limitations, known defects, and a solution-specific glossary.

**Note**

Both VMDC and IAC programs have developed a terminology to convey the concepts implemented by their respective technologies. From a VMDC viewpoint, a network container represents Tenant isolation based on a separation of physical, logical, and virtual network resources. A Tenant's compute workloads are attached to this network container. From the IAC 4.0 perspective, a network container is analogous to a Tenant's Virtual Data Center (VDC). The VDC is a construct within a Tenant and Organization hierarchy that collects virtual network and compute resources together. This document bridges the two concepts into one solution, while attempting to remain true to the natures of both VMDC and IAC in their use of terminologies.



# Solution Overview

---

The cloud orchestration of Cisco's Virtualized Multiservice Data Center (VMDC) Virtual Services Architecture (VSA) 1.0 solution with the Cisco Intelligent Automation for Cloud (IAC) 4.0 release provides design and implementation guidance for Enterprises to deploy Private cloud services and to Service Providers building virtual Private and Public cloud services. The VMDC infrastructure solution integrates various Cisco and third-party products into a validated system architecture that delivers a highly available, secure, flexible, and scalable Data Center (DC) infrastructure for implementing cloud deployments.

While IAC 4.0 can be customized to orchestrate other VMDC system versions, this guide provides details for using IAC 4.0 for orchestrating VMDC VSA 1.0-based cloud infrastructures. IAC 4.0 provides the foundation for scaling the cloud, and includes features such as multi-tenancy, Role-Based Access Control (RBAC), virtual and physical server provisioning, IP Address Management (IPAM), orchestrating virtual service appliances, and orchestrating the VSA 1.0-based network containers. This release provides virtual appliance orchestration by introducing orchestration capabilities for the Cisco Cloud Services Router (CSR) 1000V, Citrix NetScaler VPX, and Cisco Virtual Security Gateway (VSG). Some of these virtual service nodes are orchestrated through integration with the Cisco Prime Network Service Controller (PNSC), while others are orchestrated directly by IAC 4.0. In addition, a future update to IAC 4.0 will provide capability for orchestrating VMDC 2.3-based network containers.

This chapter provides an introduction to VMDC, which is the Cisco reference architecture for Infrastructure as a Service (IaaS) cloud deployments. This chapter also provides an overview of IAC 4.0, which is the cloud management software used to orchestrate the deployment of the VMDC reference architecture. IAC 4.0 provides rapid, on-demand, workload and virtual service appliance deployment in a multi-tenant environment, with portal-based resource provisioning and management capabilities.

The IAC 4.0 orchestration suite has been validated and comes pre-packaged (out-of-box) with VMDC VSA 1.0-based network containers, incorporating the CSR 1000V, VSG, and Citrix NetScaler VPX. While VMDC VSA 1.0 defines Gold, Silver, and Bronze network containers, IAC 4.0 extends these container models further to provide more flexibility and choices for deploying cloud containers. The VMDC VSA 1.0-based network containers that can be orchestrated out-of-box by IAC 4.0 are:

- Four-Zone Gold Container
- Two-Zone Gold Internet Container
- Two-Zone Gold Enterprise Container
- Two-Zone Silver Internet Container
- Two-Zone Silver Enterprise Container
- One-Zone Bronze Internet Container
- One-Zone Bronze Enterprise Container

# Cloud Orchestration

Cloud service orchestration is a multi-domain configuration Abstraction layer that sits on top of the cloud DC infrastructure. This Abstraction layer enables a portal-based configuration model in which the customer (application-hosting community) subscribing to the infrastructure can pick from a set of configurable, access-controlled services. Based upon these picks, configuration actions are executed across multiple domains and to the devices within these domains that together make up the service as represented within the customer-facing portal.

Orchestration (integration across the domain tools) is fundamental as there is no single tool within the DC that can configure the bundled services presented within the Service Catalog end-to-end. Orchestration coordinates the configuration requirements on top of the domain tools and ensures that all of the services defined within the Service Catalog/Portal are appropriately sequenced and correctly executed within each specific domain. Moreover, orchestration aggregates all of the individual service components within the Service Catalog as a total services pool and determines if sufficient resources exist across all of the components to provide the service.

The system infrastructure is based on the VMDC VSA 1.0 architecture. On top of the base infrastructure is a hypervisor-based compute virtualization based on VMware vSphere 5.1, along with network services virtualization based on the Nexus 1000V Distributed Virtual Switch (DVS) and virtual service appliances like the CSR 1000V, VSG, and Citrix NetScaler VPX. The focus of this solution is the automation of this infrastructure, specifically as implemented through the IAC 4.0 release. The IAC 4.0 solution provides End User Management, Tenant Admin Management, and Cloud Admin Management via RBAC to the portal and Service Catalog provided by the Cisco Prime Service Catalog (PSC), a provisioning automation engine provided by the Cisco Process Orchestrator (PO) and integration with domain specific automation and management systems. The individual components that make up the IAC 4.0 solution set are defined throughout this guide and are combined as a single “whole” system to provide IaaS capabilities and offerings.

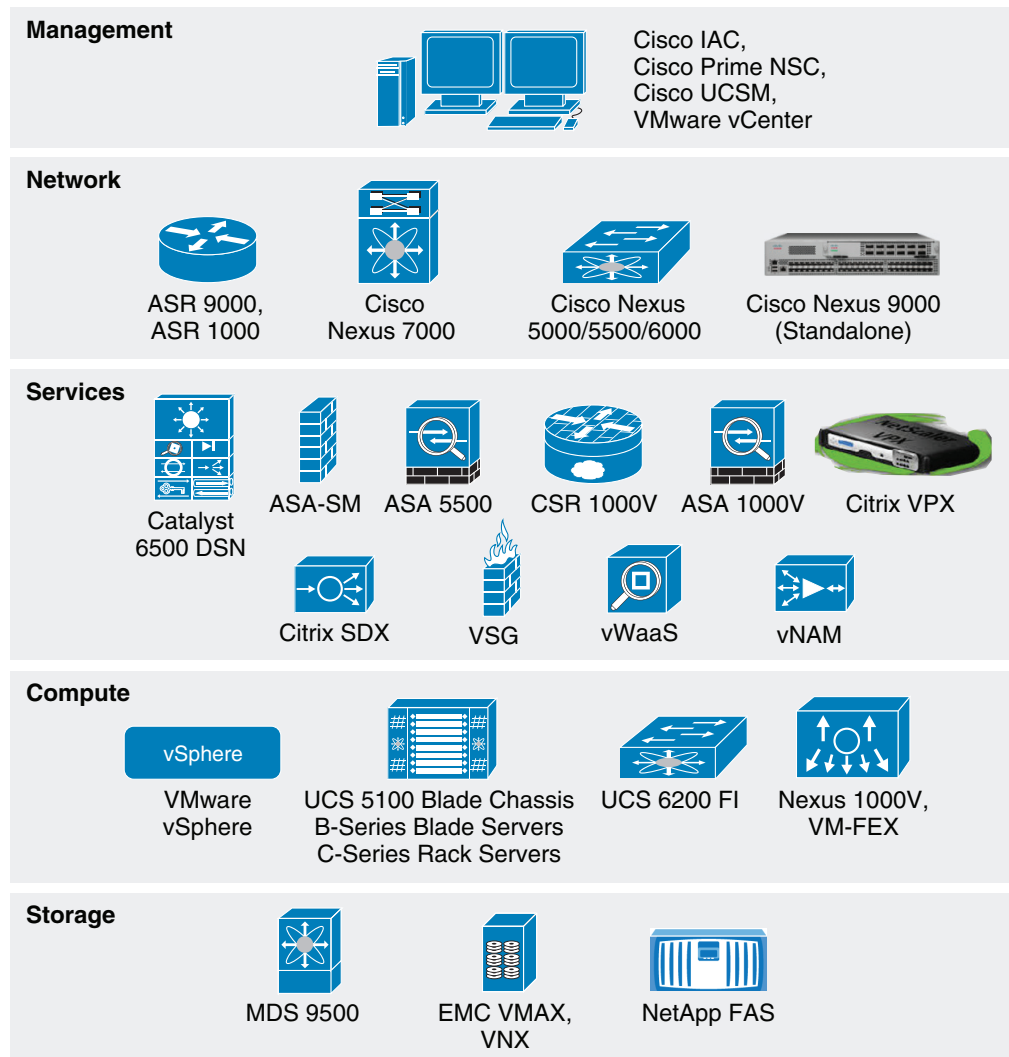
IAC 4.0 is made up of a number of components that, when combined, provide the foundation for an IaaS system. By leveraging the VMDC VSA 1.0 infrastructure, the IaaS offer becomes truly multi-tenant, secure, resilient, and scalable. These IAC components connect to and manage the VMDC VSA architecture, which is comprised of the Cisco Unified Computing System (UCS) compute platform, the Nexus family of DC switching systems, the CSR 1000V, VSG, and Citrix NetScaler VPX network services virtual appliances, and the Cisco Aggregation Services Router (ASR) core routing platforms deployed as specified in the VMDC VSA 1.0 infrastructure solution. In addition to the automation platform and physical infrastructure, the solution also leverages the VMware vSphere compute virtualization infrastructure, which provides for greater compute scalability than what the physical UCS infrastructure has on its own.

## VMDC Architecture

The VMDC system is the Cisco reference architecture for IaaS cloud deployments. This Cisco cloud architecture is designed around a set of modular DC components consisting of building blocks of resources called pods, or Points of Delivery. These pods comprise the Cisco UCS, SAN and NAS storage arrays, Access (switching) layers, Aggregation (switching and routing) layers connecting into the DSN-based Services layer or connecting directly to physical service appliances or virtual service appliances hosted on the UCS systems; and multiple 10 GE fabric using highly scalable Cisco network switches and routers. The VMDC system is built around the UCS, Nexus 1000V, Nexus 5000/6000 and Nexus 7000 switches, Multilayer Director Switch (MDS), ASR 1000, ASR 9000, ASA 5585-X or Adaptive Security Appliance Services Module (ASASM), Catalyst 6500 DSN, Citrix SDX, CSR 1000V,

ASA 1000V, Citrix NetScaler VPX, VSG, VMware vSphere, EMC VMAX, VNX, and NetApp FAS storage arrays. Cloud service orchestration is provided by the Cisco IAC solution. [Figure 1-1](#) provides a synopsis of the functional infrastructure components comprising the VMDC system.

**Figure 1-1 VMDC Functional Components**



## VMDC Modular Components

The VMDC system architecture provides a scalable solution that can address the needs of Enterprise and Service Provider cloud data centers. This architecture enables customers to select the design that best suits their immediate needs while providing a solution that can scale to meet future needs without retooling or redesigning the DC. This scalability is achieved using a hierarchical design with two different modular building blocks, Point of Delivery (Pod) and Integrated Compute and Storage (ICS) stack.

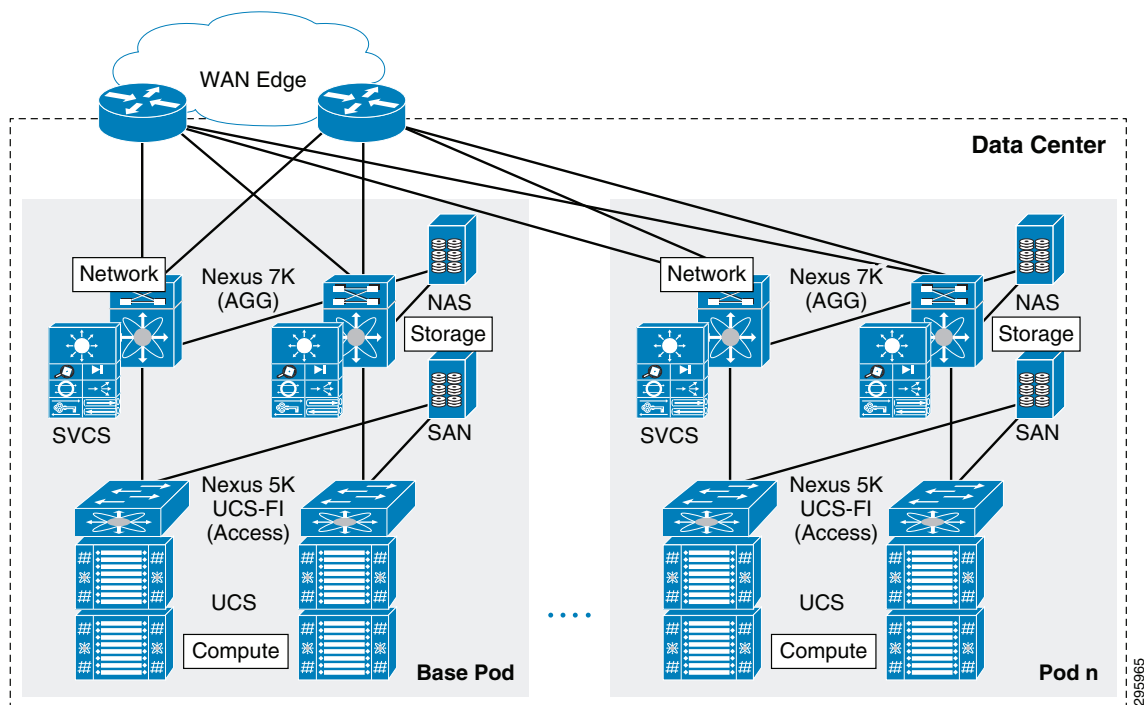


## Pod

The modular DC design starts with a basic infrastructure module called a pod. A pod is a repeatable, physical construct with predictable infrastructure characteristics and deterministic functions. A pod identifies a modular unit of DC components and enables customers to add network, compute, and storage resources incrementally. This modular architecture provides a predictable set of resource characteristics (network, compute, and storage resource pools, power and space consumption) per unit that are added repeatedly as needed.

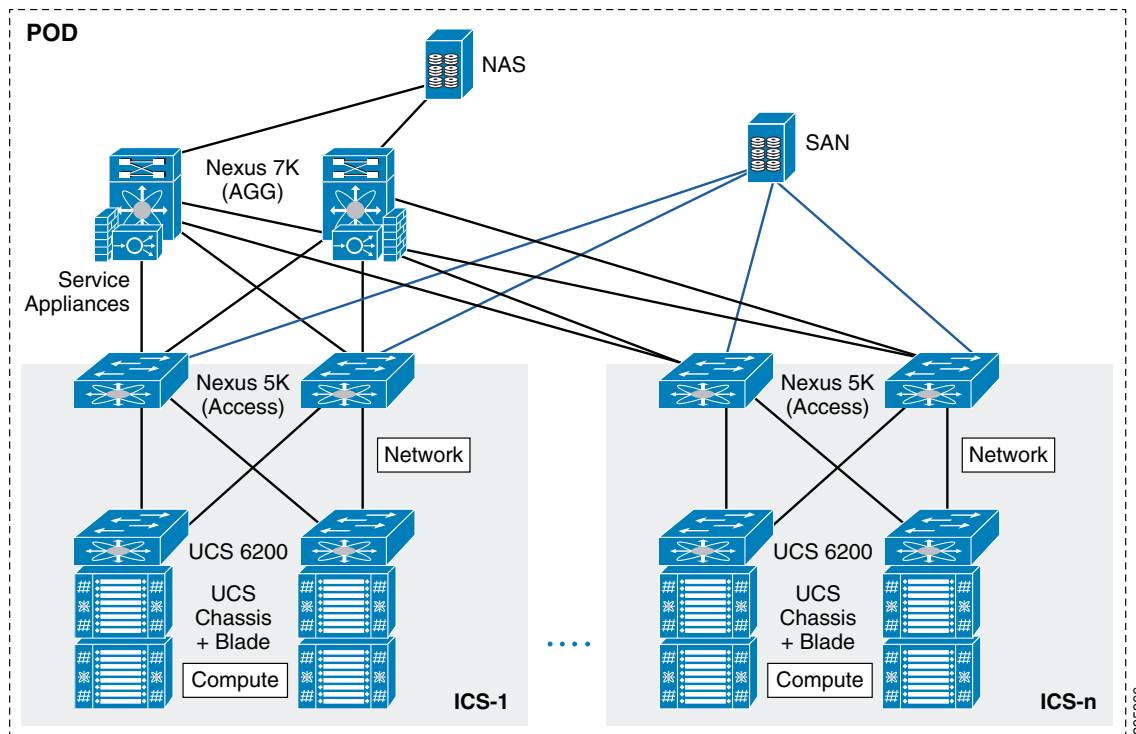
In this design, the Aggregation layer switch pair, Services layer nodes, and one or more ICS stacks are contained within a pod. The pod connects to the WAN-PE layer device in the DC, in the VMDC VSA 1.0 and VMDC 2.3 architectures. To scale a pod, providers can add additional integrated compute stacks and can continue to scale in this manner until the pod resources are exceeded. To scale the DC, additional pods can be deployed and connected to the Core layer devices. [Figure 1-2](#) illustrates how pods can be used to scale compute, network, and storage resources in predictable increments within the DC.

**Figure 1-2 Pods for Scaling the Data Center**



## ICS Stack

The second modular building block utilized is a generic ICS stack based on existing models, such as the VCE Vblock or Cisco/NetApp FlexPod infrastructure packages. The VMDC architecture is not limited to a specific ICS stack definition, but can be extended to include other compute and storage stacks. An ICS stack can include network, compute, and storage resources in a repeatable unit. In this release, the Access layer switch pair, storage, and compute resources are contained within an ICS stack. To scale a pod, customers can add additional ICS stacks and can continue to scale in this manner until the pod resources are exceeded. [Figure 1-3](#) illustrates how ICS stacks can be used to scale the pod.

**Figure 1-3 ICS Stacks for Scaling the Data Center**

## VMDC VSA 1.0 Overview

The VMDC VSA 1.0 system, while consistent with previous VMDC solutions in the L2 hierarchical design, pod and Integrated Compute and Storage (ICS) stack concepts, Tenant segregation, and service tiers, introduces several new design elements and technologies:

- Use of virtualized (x86) routing and services appliances
- Virtual Customer Edge (vCE) model to enable per-Tenant routing in the DC using the Cisco Cloud Services Router (CSR) 1000V
- Overlay L3 networking across DC fabric to allow direct Border Gateway Protocol (BGP) sessions between the Tenant CSR 1000V and WAN router (ASR 9000)
- Use of L2-only DC fabric - no VRF-Lite or L3 on the Nexus Aggregation Switches
- Overlay L2 networking using Virtual Extensible LAN (VXLAN) for Tenant Virtual Machine (VM) segments
- Service chaining of virtual services using Nexus 1000V vPath

The VMDC VSA 1.0 solution addresses the following key issues:

1. **Tenancy Scale.** The previous VMDC solution designs leveraged virtualization technologies like VLANs, VRF instances, virtual contexts, etc. for Tenant isolation. Each of these technologies has associated control-plane overhead and impacts logical scale. In a traditional hierarchical DC network model, the pressure point from a scalability and control-plane perspective is at the Aggregation layer of the infrastructure, with the number of routing peers, VRF instances, VLAN

instances, and MAC capacity supported by aggregation nodes. This solution presents an alternative, addressing tenancy scale with a centralized Provider Edge (PE) and distributed, per-Tenant vCE routing model, thereby mitigating the L3 control plane at the Aggregation layer. Tenancy scale is thus increased to the number of routing peers supported by the PE nodes. In addition, by using VXLANs for Tenant VM segments, this solution increases segment scale beyond the 4000 VLAN limit and mitigates the L2 and MAC scale pressure points on the Aggregation layer.

2. **Management Complexity.** The previous VMDC solution designs feature a relatively high degree of management complexity in provisioning back-to-back VRF-Lite across the DC routing platforms, provisioning the virtual contexts (firewall and load balancer) and stitching the services together through VLAN stitching and routing. This solution has a simplified service orchestration due to the logical topologies, instantiation of per-Tenant virtual appliances, service chaining through vPath, and elimination of cross-Tenant dependencies.
3. **Evolution to Virtual Services.** Many VMDC customers have envisioned a transition from physical to virtual services for their next-gen DC architectures to achieve increased flexibility and agility through greater software definability.

The VMDC VSA 1.0 solution provides the following key benefits to cloud deployments:

- Increased tenancy scale per-Tenant vCE model
- Increased segment scale through VXLAN for Tenant VM segments
- Virtual services providing Network as a Service
- Pay As You Grow to enable new business models
- Improved agility and elasticity
- Simplified service chaining through Nexus1000V vPath
- Evolution towards Network Function Virtualization (NFV) and Software Defined Networks (SDN)

The VMDC VSA 1.0 solution (as validated) is built around the Cisco UCS, Nexus 1000V and Nexus 7000/5000 switches, ASR 9000, CSR 1000V, Adaptive Security Appliance (ASA) 1000V, Virtual Security Gateway (VSG), Virtual WAAS (vWAAS), Virtual Network Application Monitoring (vNAM), Citrix NetScaler VPX, VMware vSphere 5.1, and NetApp FAS storage arrays. Cloud service orchestration for the VMDC VSA 1.0 solution is provided by the IAC 4.0 solution.

For detailed information on VMDC VSA 1.0 system architecture, refer to the [VMDC VSA 1.0 Design Guide](#) and [VMDC VSA 1.0 Implementation Guide](#).

In addition, the VMDC VSA 1.0 solution was also validated with the Nexus 9000 (standalone mode) platform as the L2 fabric. In this topology, the Nexus 9300 is used as the access switch instead of the Nexus 5000 FabricPath leaf, and the Nexus 9500 is used as the aggregation switch instead of the Nexus 7000 FabricPath spine node. The VMDC VSA 1.0.2 design uses vPC L2 connectivity in the Nexus 9000 standalone fabric, while the VMDC VSA 1.0 design utilizes the Nexus 5000 and 7000 platforms in FabricPath mode (alternately, they can also be used in vPC mode). This validated design is documented in the [VMDC VSA 1.0.2 Implementation Guide](#).

## VSA 1.0 Architecture

The VMDC VSA 1.0 solution utilizes a hierarchical DC network design for High Availability (HA) and scalability. The hierarchical or layered DC design uses redundant switches at each layer of the network topology for device-level failover that creates a highly available transport between end nodes using the network. While the Virtual Port Channel (vPC)-based Nexus DC fabric could also be utilized, the VMDC VSA 1.0 solution has been validated with a Leaf-Spine FabricPath design using Nexus platforms. DC networks often require additional services beyond basic packet forwarding such as Server Load Balancing (SLB), firewall, and Network Address Translation (NAT). These services are provided

by virtual service appliances hosted on the Cisco UCS in the VMDC VSA 1.0 solution. Each service approach also supports the deployment of redundant appliances to preserve HA standards set by the network topology. This layered and redundant approach is the basic foundation of the VMDC design to provide scalability, performance, flexibility, resiliency, and service assurance. VLANs and VXLANs are used to provide Tenant isolation within the DC architecture, and BGP or static routing is used to interconnect the different networking and service devices, in addition to utilizing the Nexus 1000V vPath for chaining some virtual services.

This multi-layered VMDC VSA DC architecture is comprised of WAN, Aggregation, Access and Compute layers, with Services residing in the Compute layer. This architecture allows for DC pods to be added as demand and load increases. It also provides the flexibility to create different logical topologies and insertion of new virtual service devices.

The layers of the VMDC VSA 1.0 architecture are briefly described below.

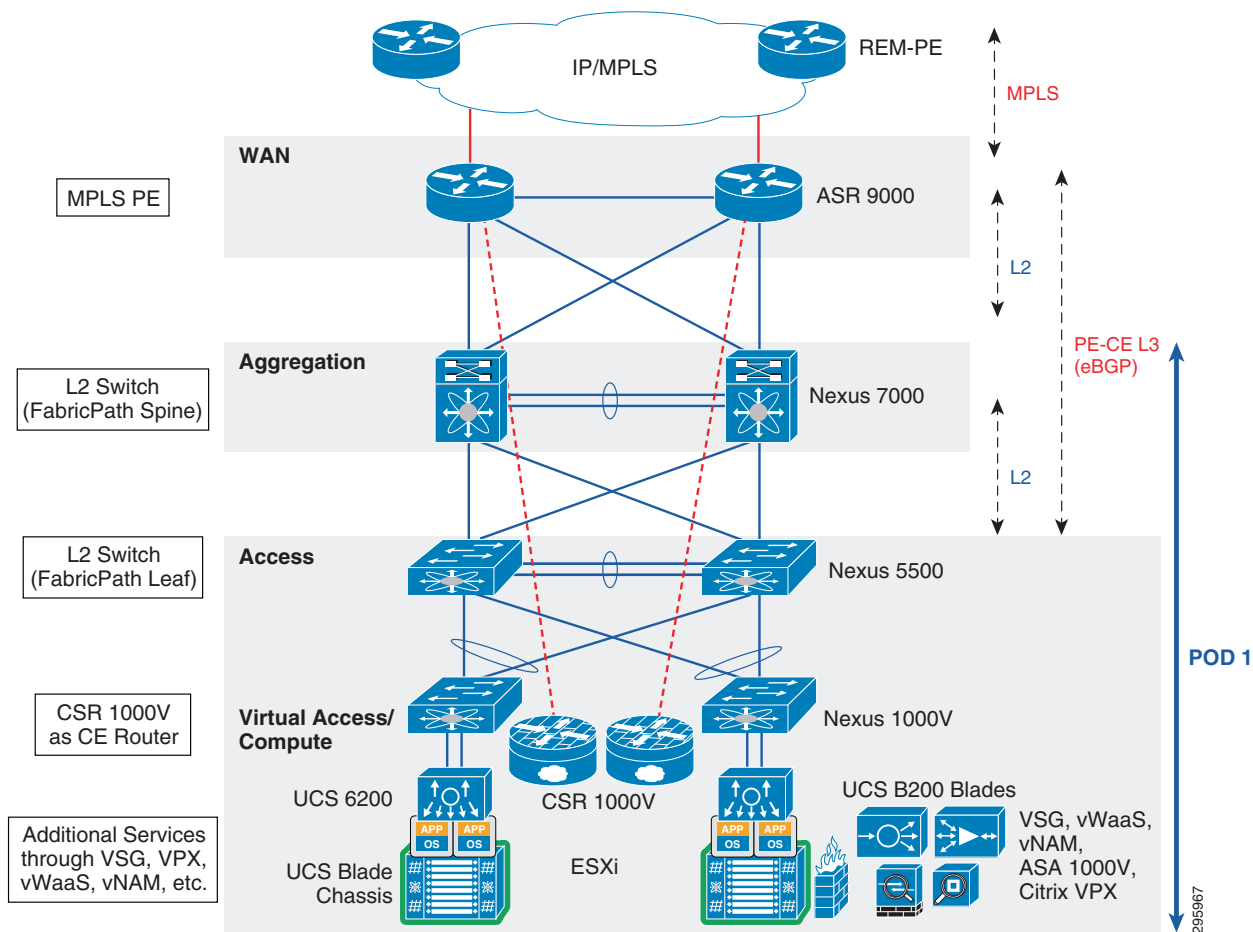
- **WAN/Edge.** The WAN or DC Edge layer connects the DC to the WAN. Typically, this provides IP or Multiprotocol Label Switching (MPLS)-based connectivity to the Internet or intranet. The ASR 9010 is used as an MPLS PE router in the VSA 1.0 design, providing L3VPN connectivity to the provider IP/MPLS network. It also provides aggregation of all DC pods as they connect directly to the ASR 9010 PE. The ASR 9010 is utilized in Network Virtualization (nV) mode, where two physical ASR 9000 devices have a single control plane and appear as a single logical device to adjacent nodes.
- **Aggregation.** The Aggregation layer of the DC provides a consolidation point where Access layer switches provide connectivity between servers for multi-tier applications and across the core of the network to clients residing within the WAN, Internet, or campus. This design utilizes Cisco FabricPath technology to provide provisioning simplicity, VLAN flexibility, MAC learning, and high bandwidth Equal-Cost Multipathing (ECMP) capabilities in the DC Fabric. The Nexus 7010 switches are utilized as the Aggregation layer or FabricPath Spine in this solution.
- **Access.** The Access layer of the network provides connectivity for server farm end nodes in the DC. The Nexus 5596 is utilized as the Access layer switch or FabricPath Leaf node in this design. The Nexus 5596 connects to multiple UCS fabrics (UCS 6200 Fabric Interconnects and UCS 5100 Blade Chassis with UCS B-series blade servers). Typically, the Nexus 5500, UCS Fabric-Interconnects, and UCS Blade-Chassis, along with storage resources, are bundled together in Integrated Compute and Storage (ICS) stacks such as the VCE Vblock and Cisco/NetApp FlexPod.
- **Services.** Network and security services, such as firewalls, server load balancers, intrusion prevention systems, application-based firewalls, and network analysis modules, are typically deployed at the DC Services layer. In the VMDC VSA 1.0 solution, these services are implemented by virtual appliances residing on the UCS blades. The firewall and VPN services are provided either by the CSR 1000V or ASA 1000V, while the SLB service is provided by the Citrix NetScaler VPX. In addition, the VSG working in conjunction with the Nexus 1000V Distributed Virtual Switch (DVS) provides Intra-VXLAN and Inter-VXLAN protection to the VMs.
- **Integrated Compute Stack.** This is the ICS stack such as FlexPod or Vblock. This typically consists of racks of compute based on UCS, storage and a pair of Nexus 5500 switches aggregating the connections out of the block. The Nexus 5500 Access switch within the ICS provides connectivity both for the LAN (via 10GE Ethernet links) and SAN (via dedicated FC links), and also connects to the storage for the ICS stack.
- **Virtual Access.** Access switch virtualization allows the function of the logical Layer 2 (L2) Access layer to span multiple physical devices. The Nexus 1000V DVS running on top of the VMware ESXi hypervisor is used in the solution.

The Compute and Storage layer in the VMDC VSA 1.0 solution has been validated with a FlexPod-aligned implementation using the following components:

- Compute. Cisco UCS 6296 Fabric Interconnect switches with UCS 5108 blade chassis populated with UCS B200 and B230 half-width blades. VMware vSphere 5.1 ESXi is the hypervisor for virtualizing the UCS blade servers.
- SAN. Cisco Nexus 5596 switches provide Fibre Channel (FC) connectivity between the UCS compute blades and the NetApp FAS 6040 storage array.

Figure 1-4 provides a logical representation of the VMDC VSA 1.0 solution architecture.

**Figure 1-4 VMDC VSA 1.0 System Architecture**



## VSA 1.0 Virtual Service Platforms

In this solution, the following virtual nodes provide the listed per-Tenant services to cloud users:

- Cisco CSR 1000V
  - Routing services
  - Site-site and remote access IPsec-VPN services
  - Perimeter and Zone-Based Policy Firewall (ZBF) services

- NAT services
  - Application visibility and control services
  - QoS and NetFlow services
- Citrix NetScaler VPX
  - L4-7 SLB services
  - SSL offload services
- Cisco VSG
  - Compute firewall services
  - Inter-VXLAN/VLAN and Intra-VXLAN/VLAN security policies
- Cisco ASA 1000V
  - Site-site IPsec VPN services
  - Perimeter firewall services
  - NAT services
- Cisco vWAAS
  - WAN Optimization services
- Cisco vNAM
  - Network analysis services
- Cisco Nexus 1000V
  - DVS services
  - VXLAN Termination and Endpoint (VTEP) services

**Note**

- While VMDC VSA 1.0 design uses the ASA 1000V, vWAAS and vNAM platforms, and utilizes VXLAN segments to place VM workloads into; the IAC 4.0 orchestration solution does not include these in the out-of-box containers being delivered in this release.
- While VMDC VSA 1.0 utilizes the CSR 1000V virtual appliance to provide IPsec-VPN services to cloud users, the VPN capability on CSR 1000V is currently not supported in IAC 4.0.

## IAC 4.0 Overview

The following sections present an overview of the IAC 4.0 orchestration system. The architecture of IAC is depicted along with its interaction with VMDC VSA 1.0 networking, compute, and storage infrastructure elements. The major IAC software components are described, giving a view of each components' purpose in the system. Key new IAC features are listed that distinguish IAC 4.0 from its 3.0 implementation. Finally, the basic operational usage of IAC 4.0 is illustrated from the perspective of various users and their workflows.

## IAC 4.0 Architecture

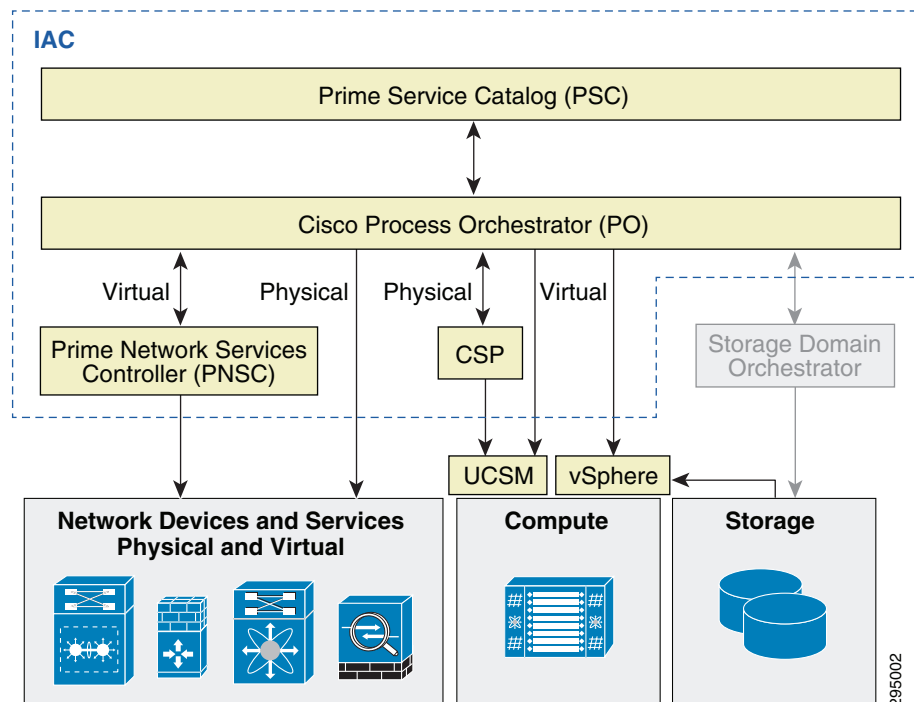
The IAC 4.0 solution utilizes a modular approach in enabling automation and orchestration of Infrastructure as a Service (IaaS) offerings for Tier 2 and 3 Service Providers, and Enterprise customers who want to provide cloud services to their users. This VMDC VSA orchestration solution is based on

the Cisco Intelligent Automation for Cloud (IAC) product suite, which consists of several individual product offerings including Cisco Prime Service Catalog (PSC), Cisco Process Orchestrator (PO) and Cisco Server Provisioner (SP).

Cisco Intelligent Automation for Cloud is a management and automation solution for Private, Public, and hybrid compute clouds. It provides a self-service experience for End Users through a web-based portal, taking service orders, and provisioning them through automation and integration with the infrastructure and supporting data center systems.

Figure 1-5 shows the IAC 4.0 system architecture.

**Figure 1-5 Cisco IAC 4.0 System Architecture**



## IAC 4.0 Components

The major functional components of the IAC 4.0 system, and their roles, are outlined below:

- The Prime Service Catalog (PSC) 10.0 provides the necessary functionality for the End User and Administrative portals and the End User-facing service catalog.
- The Process Orchestrator (PO) 3.0 provides the workflow engine and glue required to create complex service offerings from various domain managers. In this release, the PO provisions the physical networking devices - Nexus 5000/7000 and Nexus 1000V.
- Prime Network Services Controller (PNSC) 3.2 is the network domain orchestrator providing the capability to provision the virtual networking appliances like the CSR 1000V and VSG.
- IAC Management Appliance 4.0 is a Linux-based virtual appliance that provides several services for the IAC product suite including network discovery, message queuing, and software subcomponent delivery.
- Cisco SP 6.5 provides the functionality to provision bare-metal servers.



The Intelligent Automation for Cloud (IAC) 4.0 product provides the End User portal, End User-facing service catalog, Administrative portal, service orchestration, and billing and show-back and reporting functionality. In brief, End User requests for compute, network, and/or storage resources are received in the PSC and then passed to the PO. The PO then instructs the required domain orchestrators to execute the appropriate tasks to fulfill the End User request. In some cases, the PO itself executes individual tasks to accomplish a goal, specifically when there is not a domain manager to do so.

Multi-tenancy support in IAC 4.0 means that Tenant data is kept completely isolated from other Tenants' data, and features such as resource views, pricing policies, service options, and templates can be defined to be specific to each given Tenant. This is achieved through the use of different administrative and service portals, and different user roles within IAC, with Role-Based Access Control (RBAC). The following are the key technical roles within IAC 4.0:

- Cloud Provider Technical Administrator (CPTA)
  - Discover and inventory network devices
  - Create, update, and delete network and compute pod
  - Create and manage service offerings, catalog management
  - Onboard new Tenants
  - Manage Tenants and pod resources
  - Offboard Tenants
- Tenant Technical Administrator (TTA)
  - Resource and catalog management for the Tenant
  - Order and manage Tenant level resources
  - Create and manage Organizations
  - Define Tenant level firewall and LB policies and service groups
  - View and monitor networks and services ordered by Tenant users
- Organization Technical Administrator (OTA)
  - Order, manage and decommission Tenant VDCs
  - Modify VDC zones and networks
  - Create, update, and delete firewall and LB rules
  - Manage server and service groups
  - View and monitor available resources
- Cloud End Users, Virtual Server Owner (VSO), and Virtual and Physical Server Owner (VPSO)
  - Deploy and decommission virtual and physical servers
  - Create, update, and delete firewall and LB rules
  - Start, stop, and pause servers
  - View and monitor available resources

**Note**

There are other business oriented roles, not described in this document such as Cloud Provider Business Administrator (CPBA) and Tenant Business Administrator (TBA). Refer to [Cisco Intelligent Automation for Cloud Administrator Guide](#) for a description of these user roles.

IAC 4.0 enables onboarding and pooling of resources for compute, storage, and networking, and creation of policies to manage those pools. It provides functionality to provision network containers, physical servers, and virtual server instances. It also provides the ability for End Users, through a portal, to place service requests to create and manage server instances. IAC 4.0 is multi-tenant capable and can support simultaneous use of the cloud environment by multiple Tenants that can request, deploy, and operate services independently.

IAC 4.0 can out-of-box deploy and manage the VMDC VSA 1.0 and VSA 1.0.2 (with Nexus 9000 standalone) reference architectures, which include the deployment of the Gold, Silver, and Bronze, container models. IAC 4.0 can orchestrate the configuration of the following network devices in the VMDC VSA 1.0 architecture:

- Nexus 5500
- Nexus 7000
- Nexus 9000
- Nexus 1000V
- VSG
- CSR 1000V
- Citrix NetScaler VPX

**Note**

IAC orchestration focuses on the compute and virtual networking services of VMDC VSA 1.0, including the CSR 1000V, Citrix VPX, and the VSG. On the physical networking devices (Nexus 5000/7000/9000) IAC only orchestrates L2 (VLANs), and the CLI can assign the VLANs to uplink and downlink ports. IAC does not, however, orchestrate the FabricPath configuration on Nexus 5000/7000 switches or vPC configurations on Nexus 5000/7000/9000 platforms. These switches have to be provisioned as part of Day0 infrastructure setup.

IAC 4.0 orchestrates the complete data path in the pod and network container via service chaining and provisioning of VLANs, port profiles, vPath, routing protocols, firewall and LB virtual appliances, and ACL filters, security policies and LB policies on these devices. IAC 4.0 was validated at Cisco labs on VMDC VSA 1.0-based architectures. The validation covered the following resources out-of-box:

- Virtual Machine. VMs are hosted on UCS blades running VMware ESXi. VM lifecycle management is automated including memory, CPU, capacity management, and storage allocation.
- Network Virtualization for VMDC VSA 1.0 - Nexus 7000, Nexus 5500, Nexus 9000, CSR 1000V, VSG, Citrix VPX, and Nexus 1000V.

**Note**

Additional workflows in IAC 4.0 to provide support for orchestrating the VMDC 2.3 architecture have been built by Cisco Advanced Services. These workflows include network virtualization on the Nexus 7000 (VRF, VLAN, Switched Virtual Interface (SVI), HSRP, BGP routing, VLAN), Nexus 5500, (VLAN), ASA 5585-X, (creating virtual firewall contexts and provisioning security policies), Citrix SDX (creating NetScaler instances and provisioning LB policies), Nexus 1000V (creating port profiles), and VSG (creating compute firewall policies). These workflows have not been validated as part of the IAC 4.0 solution validation in the Cisco labs, but can be provided for customer deployments through Cisco AS engagements available as a cloud accelerator kit.

For more details on IAC 4.0 capabilities, refer to [Cisco Intelligent Automation for Cloud](#).

## Key New Features

IAC 4.0 includes the following new features:

- Multi-tenancy
- VMDC VSA 1.0 Gold, Silver, and Bronze containers
- Enhanced cloud object model
- Integration with PNSC
- CSR 1000V orchestration
- VSG orchestration
- Citrix NetScaler VPX orchestration

## High-Level Workflow

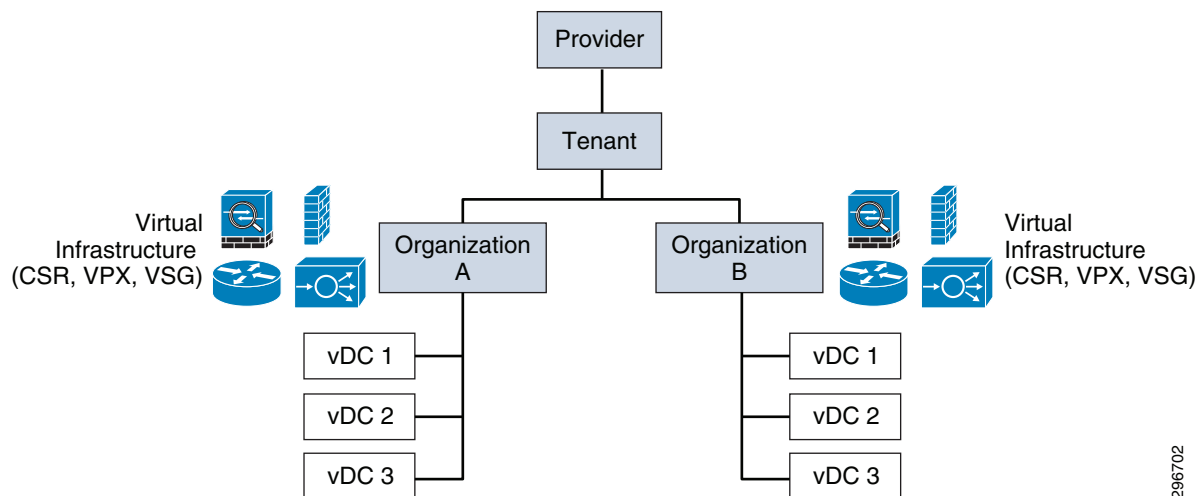
The IAC multi-tenancy structure consists of a hierarchical, three-tier model consisting of Tenant, Organizations and Virtual Data Centers (VDC). A Tenant can contain multiple Organizations, and each Organization can contain multiple VDCs. Each Organization under a Tenant shares a common set of network service devices, which includes the CSR 1000V, VPX, and VSG, as outlined in the VMDC VSA 1.0 architecture. IAC provisions a single CSR 1000V, VPX, and VSG per Organization.

The VDC is a logical network container created within an Organization (using the virtual network service devices created for that Organization) with a set of networks and a set of compute resources for VMs (vCPU, memory, etc.). IAC 4.0 provides a set of network containers, out-of-box, that are based on the VMDC VSA 1.0 network container models. Depending on the type of container chosen, the VDC can provide either Internet or Enterprise access, or both, to the VMs. Further, depending on the type of container model chosen, each VDC can have one or more of the following network zones:

- Unprotected Public
- Protected Public
- Unprotected Private
- Protected Private

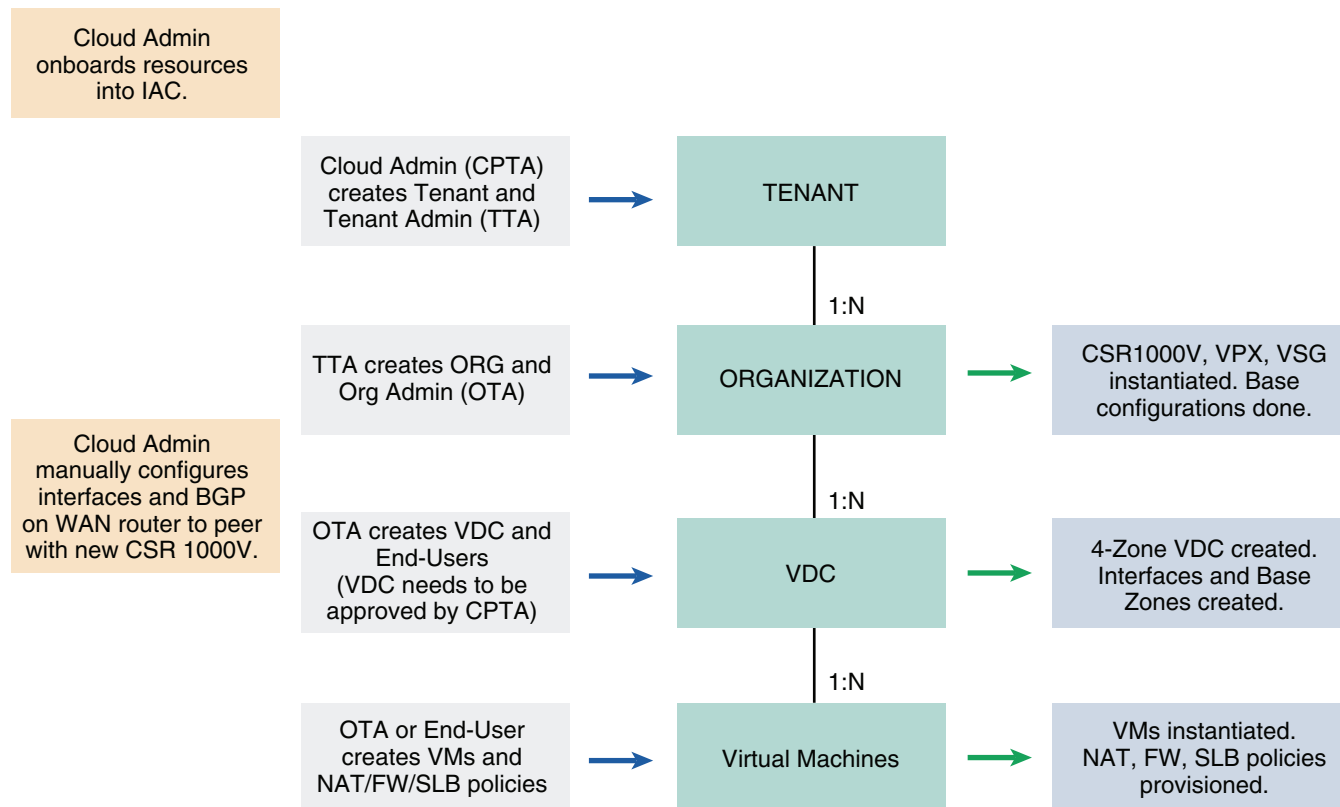
Each Organization can have multiple VDCs, and these VDCs do not need to be the same type.

[Figure 1-6](#) shows the IAC 4.0 tenancy hierarchy and how it relates to the virtual appliances and network containers. More details on the IAC Tenant, Organization, and VDC hierarchy are described in [Virtual Data Center \(Network Container\) Design](#).

**Figure 1-6 IAC 4.0 Tenant Hierarchy**

296702

Figure 1-7 shows the high-level workflow involved in creating a network container for a Tenant.

**Figure 1-7 IAC 4.0 High-Level Orchestration Workflow**

296701

The workflow involves the following key steps:

1. Network, Compute, and Storage infrastructure created as Day0 setup.
2. IAC installed and configured. Cloud Admin (CPTA) role created.
3. Cloud Admin (CPTA) onboards these resources into IAC.

4. CPTA onboards the Tenant and creates the Tenant Technical Administrator (TTA) role.
5. TTA creates the Organization and Organization Technical Administrator (OTA) role. When the Organization is created, IAC instantiates one instance each of CSR 1000V, VPX, and VSG for that Organization and does basic provisioning (interfaces, routing, etc.) on these appliances. This includes BGP provisioning (peering information obtained from the information provided in the Tenant onboarding screens) on the CSR 1000V to peer with the upstream ASR 9000 (or other) WAN router.
6. The CPTA or Network Admin has to manually provision the corresponding configurations on the upstream WAN router. This includes BGP peering on the WAN router.
7. The OTA creates a VDC by selecting one of the available network container types.
8. IAC provisions additional configurations on the CSR 1000V, VPX, and VSG (additional interfaces, basic firewall zones, etc.).
9. The OTA creates cloud End User roles.
10. The End User instantiates VMs into one or more zones in the VDC.
11. The End User selects to apply firewall, NAT, and SLB policies to one or more VMs. IAC provisions the appropriate NAT and ZBF policies on the CSR 1000V, LB policies on the VPX, or compute firewall policies on the VSG.

The following section provides a high-level description of the roles and responsibilities of the different user types involved in the above workflow.

1. Cloud Technical Administrator:

- Connections & Discovery
  - Connect to managers & devices
  - Discover and inventory virtual and physical network devices
  - Define, update, and remove Network & Compute pods
- Flexible Catalog Management
  - Offer basic or network services-enhanced VDCs
  - Manage network service offerings
- Tenant management
  - Onboard new Tenant and set up initial network services
  - Offboard existing Tenant and remove all network resources
- Ongoing Management
  - Display utilization of system network resources (networks, policies, etc.)

2. Tenant Technical Administrator:

- View
  - Available network services offered by the cloud provider
- Select
  - Network services to be offered to Tenant users
- Order
  - Tenant level resources (shared network zone, public IP pool, etc.)
- Manage

- Allow different Organizations access to the same VDC (share private VDCs)
  - Define Tenant network firewall and load balancer service groups
  - Define Tenant network security policy
  - View VDC, networks, and network services ordered by Tenant users
  - Monitor resource utilization of Tenant network resources
3. Organization Technical Administrator:
- View
    - Available Tenant VDCs and other resources
  - Order
    - A VDC, selecting size, zones and networks
  - Manage lifecycle
    - Modify VDC zones and networks
    - Add/modify/remove NAT, server firewall, SLB
    - Manage server and service groups
    - Decommission VDC
4. Cloud End User
- View
    - Available Organizational VDCs contained resources
  - Order
    - VMs, bare-metal machines
    - Add/modify/remove firewall, LB, and NAT rules
  - Manage lifecycle
    - Deploy VMs and physical machines
    - Start, stop, and pause servers
    - Undeploy (remove) virtual and physical machines

## Validated Components

This section provides the VSA 1.0 and IAC 4.0 components validated in this release.

### VSA 1.0 Components

Table 1-1 lists the hardware and software versions that were validated for VMDC VSA 1.0 and VMDC 1.0.2-based container creation using IAC 4.0.

**Table 1-1 VMDC VSA 1.0 Hardware and Software Versions Validated with IAC 4.0**

Component	Description	Hardware	Software
Cisco ASR 9000	WAN-PE Router	9010	4.3.4
Cisco Nexus 7000	DC Aggregation	7009  Line Cards: N7K-F248XP-25 N7K-M108X2-12L	NX-OS 6.1(6)
Cisco Nexus 5000	Access Switch	5548	NX-OS 7.0(0)N1(1)
Cisco Nexus 9500	DC Aggregation	9508  Line Cards: N9K-X9636PQ N9K-C9508-FM	NX-OS 6.1(2)I2(1)
Cisco Nexus 9300	Access Switch	93128  Line Cards: N9K-C93128TX N9K-M12PQ	NX-OS 6.1(2)I2(1)
Cisco UCS 6200	Fabric Interconnect	6248UP	2.1(3a)
Cisco UCS B-Series	Compute Platform	5108 with B200 M3 blades	2.1(3a)
VMware vSphere	Virtual Compute Platform	N/A	5.10
Cisco Nexus 1000V	Distributed Virtual Switch	N/A	2.2.1a
Cisco CSR 1000V	Cloud Services Router	N/A	9.03.11.00.S.15 - limited validation was also performed on CSR 3.12
Cisco VSG	Virtual Security Gateway	N/A	4.2(1)VSG(1.1)
Citrix NetScaler VPX	Load Balancer	N/A	10.1

**Note**

- The VMDC VSA 1.0 architecture and the IAC 4.0 orchestration for VSA 1.0 were validated with the Citrix NetScaler VPX virtual platform. Future versions of the VMDC VSA solution will validate with the Nexus 1000V vPath-based Citrix NetScaler 1000V platform (the Cisco OEM version of Citrix VPX). IAC 4.0 can also be extended to support orchestration for the Citrix NetScaler 1000V platform.
- The recently released Cisco Prime Network Services Controller (PNSC) 3.2 version can support the management and provisioning of the Cisco CSR 1000V, ASA 1000V, VSG, Citrix NetScaler VPX and Citrix NetScaler 1000V virtual appliances. However, due to timing and code availability reasons, IAC 4.0 utilizes PNSC for provisioning only the VSG and CSR 1000V platforms. IAC 4.0



provisions the Citrix NetScaler VPX platform directly (using Telnet/SSH methods to configure through CLI). Future versions of IAC can utilize the PNSC for provisioning Citrix NetScaler VPX and Citrix NetScaler 1000V platforms.

- The VMDC VSA 1.0 architecture was validated with the Citrix NetScaler VPX platform for providing SLB services. The NetScaler VPX was utilized along with the Nexus 1000V DVS, without vPath capability for service chaining. The Citrix NetScaler 1000V platform released by Cisco in Oct 2013 (release 10.1-120.17) utilizes the Nexus 1000V vPath service chaining capabilities. A new version of NetScaler 1000V (release 10.1-124.14) released by Cisco in March 2014, can be utilized with or without Nexus 1000V vPath service chaining. The Cisco Prime Network Services Controller (PNSC) 3.2 release (Jan 2014) supports Citrix NetScaler 1000V in vPath mode. A future version of PNSC (3.2.2 to be released June 2014) will add support for NetScaler 1000V in non-vPath mode. Future VMDC versions will cover the NetScaler 1000V operating in vPath mode for comprehensive virtual services chaining through the Nexus 1000V.

It is recommended that customers deploying the VMDC VSA architecture utilize the Citrix NetScaler 1000V platform. When used in the non-vPath mode, the NS1000V can replace the VPX in the VSA 1.0 design, with no changes in logical connectivity, service chaining or configurations. When used in the vPath mode, there are changes in the logical connectivity, service chaining, and configurations, as compared to the VMDC VSA 1.0 design.

The IAC 4.0 out-of-box orchestration for VSA 1.0 includes the Citrix NetScaler VPX platform. Using the Citrix NetScaler 1000V in non-vPath mode, instead of the Citrix VPX, should also work with IAC 4.0, however, this has not been validated by Cisco. Using the NetScaler 1000V in vPath mode requires changes in IAC 4.0 functionality for VSA 1.0. Please work with Cisco Advanced Services to make these changes.

## IAC 4.0 Components

Table 1-2 lists the IAC 4.0 solution components and the versions that were validated in Cisco labs.

**Table 1-2 Software Matrix for IAC 4.0 Components**

Component	Description	HW	SW
PSC	Service Catalog and Portal	N/A	10.0 R2
PO	IAC Orchestration Engine	N/A	3.0.0.1090
IAC Management Appliance	Device Discovery and Virtual Services	N/A	4.0
Server Provisioner	Physical Compute Provisioning	N/A	6.5
PNSC	Prime Network Services Controller	N/A	3.2.1d



### Note

IAC 4.0 supports multiple cloud technologies. i.e., VMware vCenter, VMware vCloud Director, OpenStack Cloud Manager, Cisco UCS Director, and Amazon EC2. For this validation, IAC 4.0 was deployed with VMware vCenter.



## Solution Design

---

This chapter provides design considerations for the Cisco Intelligent Automation for Cloud (IAC) 4.0 solution, and details on the IAC 4.0 components, interconnections, and the Cisco Virtualized Multiservice Data Center (VMDC) Virtual Service Architecture (VSA) 1.0 network containers that are orchestrated.

The IAC 4.0 orchestration suite has been validated and comes pre-packaged (out-of-box blueprints and templates) with the following sets of VMDC VSA 1.0-based network containers:

- VMDC VSA 1.0 Gold
- VMDC VSA 1.0 Silver
- VMDC VSA 1.0 Bronze

## VMDC VSA 1.0 Network Containers

The IAC 4.0 orchestration suite has been validated and comes pre-packaged (out-of-box blueprints and templates) for VMDC VSA 1.0 based Gold, Silver, and Bronze network containers. This section provides information on the VMDC VSA 1.0 network containers that can be orchestrated out-of-box with IAC 4.0.

Cloud providers whether Service Providers or Enterprises desire to deploy an IaaS offering with multiple feature tiers and pricing levels. To tailor workload or application requirements to specific customer needs, the cloud provider can differentiate services with a multi-tiered service infrastructure and Quality of Service (QoS) settings. The Cisco VMDC architecture allows customers to build differentiated service tiers and service level agreements that support their Tenant or application requirements. Such services can be used and purchased under a variable pricing model. Infrastructure and resource pools can be designed so that End Users can add or expand services by requesting additional compute, storage, or network capacity. This elasticity allows the provider to maximize the user experience by offering a custom, Private DC in virtual form.

The VMDC VSA 1.0 solution defines a reference multi-tier IaaS service model of Gold, Silver, Bronze and Zinc tiers. These service tiers (or network containers) define resource and service levels for compute, storage, and network performance. This is not meant to be a strict definition of appliance and resource allocation, but to demonstrate how differentiated service tiers could be built. These are differentiated based on the following features:

- Network Resources. Differentiation based on network resources and features.
  - Application Tiers. Service tiers can provide differentiated support for application hosting. In some instances, applications may require several application tiers of VMs (web, application, database). VMDC VSA 1.0 Gold and Silver services are defined with three application tiers on

three separate VXLANs (or VLANs) to host web, application, and database services on different VMs. The Bronze and Zinc service is defined with one VXLAN (or VLAN) only, so if there are multi-tiered applications, they must reside on the same VXLAN (or VLAN) or potentially on the same Virtual Machine (VM) (Linux, Apache, MySQL, PHP, Perl, and Python (LAMP)/Windows Apache, MySQL, PHP, Perl, and Python (WAMP) stack).

- Access Methods and Security. All four service tiers, Gold, Silver, Bronze, and Zinc, are defined with separate service appliances per-tenant to provide security and isolation. The Gold tier offers the most flexible access methods - through Internet, L3VPN, and secure VPN access over the Internet. Also, the Gold tier has multiple security zones for each Tenant. The Silver and Bronze tiers do not support any perimeter firewall service and provide access through L3VPN only. The Zinc tier supports access over Internet only, along with secure VPN access and perimeter firewall service.
- Stateful Services. Tenant workloads can also be differentiated by the services applied to each tier. The Gold tier is defined with a Zone-Based Policy Firewall (ZBF) and Network Address Translation (NAT) service on the CSR 1000V, Server Load Balancing (SLB) services on the Citrix NetScaler VPX, and secure remote access (IPsec-VPN) on the CSR 1000V. The Silver tier is defined with a Citrix NetScaler VPX SLB service. The Bronze tier is defined with no ZBF or SLB services. The Zinc tier provides NAT and perimeter firewall services with the ASA 1000V virtual appliance. For all four service tiers, security can be provided in the Compute layer by utilizing the VSG, in conjunction with the Nexus 1000V DVS. In addition, for the Gold tier, services such as Application Visibility and Control (AVC) on the CSR 1000V, WAN optimization on the vWAAS (through AppNav on the CSR 1000V), and Network Analysis through the vNAM can be provided to the Tenants.
- QoS. Bandwidth guarantee and traffic treatment can be a key differentiator. QoS policies can provide different traffic classes to different Tenant types and prioritize bandwidth by service tier. The Gold tier supports VoIP/real-time traffic, call signaling and data class, while the Silver, Bronze, and Zinc tiers have only data class. Additionally, Gold and Silver Tenants are given bandwidth guarantee, with Gold getting more bandwidth (2x) than Silver.
- VM Resources. Service tiers can vary based on the size of specific VM attributes such as CPU, memory, and storage capacity. The Gold service tier is defined with VM characteristics of 4 vCPU and 16 GB memory. The Silver tier is defined with VMs of 2 vCPU and 8 GB, while the Bronze tier VMs have 1 vCPU and 4 GB each.
- Storage Resources. To meet datastore protection, the recovery point, or the recovery time objectives, service tiers can vary based on provided storage features such as Redundant Array of Independent Disks (RAID) levels, disk types and speeds, and backup and snapshot capabilities. The Gold tier is defined with 15k FC disks, the Silver tier on 10k FC disks, and the Bronze tier on Serial AT Attachment (SATA) disks.

The network container is a logical (virtual) segment of the shared (common) physical network resources (end-to-end through the DC) that represents the DC network domain carrying Tenant traffic. The physical infrastructure is common to all Tenants, but each network device (routers, switches, firewalls, and so forth) is virtualized such that each Tenant's virtual network container is overlaid on the common physical network. In the case of virtual service appliances like CSR 1000V, VSG, Citrix VPX etc., each Tenant gets an individual instance of the virtual appliance. The virtual appliance instance is then a part of the specific Tenant network container.



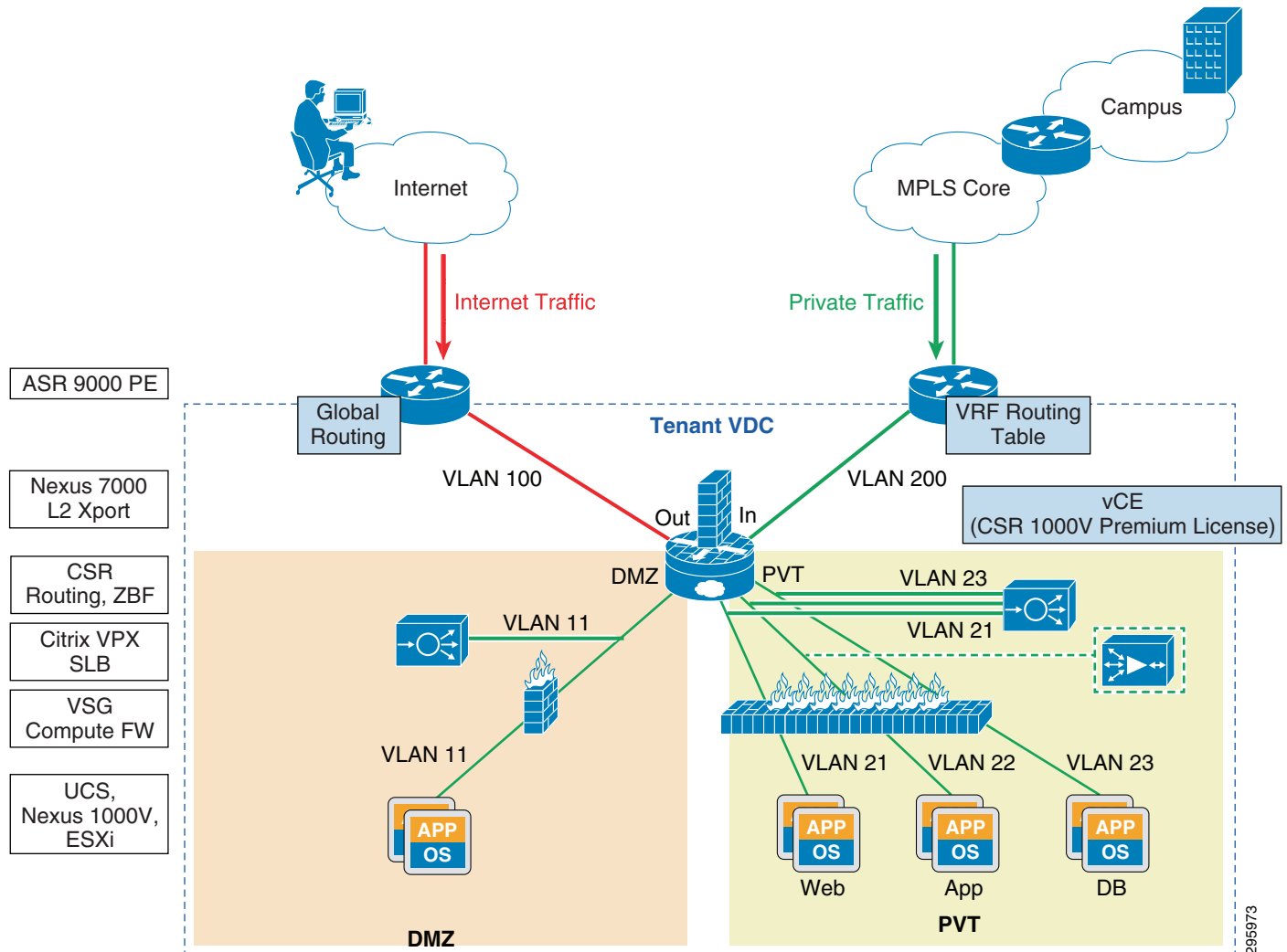
#### Note

- For detailed information on the VMDC VSA 1.0 network containers, refer to the [VMDC VSA 1.0 Implementation Guide](#).

## VMDC VSA 1.0 Gold Network Container (Two Zones)

Figure 2-1 shows a logical representation of a VMDC VSA 1.0 Gold service tier network container.

Figure 2-1 VMDC VSA 1.0 Gold Network Container



In the VMDC VSA architecture, each Tenant gets their own virtual service appliances as part of the network container. VLANs are utilized for connecting the Tenant routing instance (CSR 1000V) to the Tenant VRF instances on the ASR 9000 WAN router. In the IAC 4.0 orchestrated VMDC VSA 1.0 network containers, VLANs are utilized in the compute layer, to place workloads into, and to interconnect the virtual service appliances.

The Gold Tenant gets two network (and compute/storage) zones to place workloads into. Each Gold Tenant container has its own set of transport VLANs, compute segment VLANs and virtual routing instances (CSR 1000V). Each zone in a Gold container has its own compute segment VLANs and virtual appliances (VPX, VSG). This Gold service tier provides the highest level of sophistication by including the following services:

- Routing (BGP) on the CSR 1000V to connect the Tenant Virtual Data Center (VDC) to the Tenant VRF (or Internet) on the WAN router

- Access from Internet or MPLS-VPN to Tenant container (VDC)
- Two zones - Private (PVT) Zone and Demilitarized Zone (DMZ) - to place workloads. Each zone has its own VLAN segments.
- ZBF on the CSR 1000V to provide stateful perimeter and Inter-zone firewall services to protect the Tenant workloads
- Network Address Translation (NAT) on the CSR 1000V to provide static and dynamic NAT services to RFC1918 addressed VMs
- SLB on the Citrix VPX to provide L4-7 LB and SSL offload services to Tenant workloads. Note that the VMDC VSA 1.0 architecture was validated with the Citrix NetScaler VPX, and future versions of the VMDC VSA system will validate with the Nexus 1000V vPath-based Citrix NetScaler 1000V.
- Compute firewall on the VSG to provide Inter-VLAN and Intra-VLAN security service to the Tenant VMs
- Higher QoS SLA and two traffic classes - real-time (VoIP), and premium data.

The two zones can be used to host different types of applications to be accessed through different network paths. The two zones are discussed in detail below.

- **PVT Zone.** The PVT, or Private Zone, and its VMs can be used for cloud services to be accessed through the customer MPLS-VPN network. The customer sites connect to the provider MPLS-Core and the customer has their own MPLS-VPN (Cust-VRF). The VMDC DC Edge router (ASR 9000 PE) connects to the customer sites through the MPLS-VPN (via the Cust-VRF). This Cust-VRF is connected through the DC (Nexus 7000, UCS 6200 etc) to the customer's CSR 1000V fronting the customer VDC. For the VMDC VSA 1.0 Gold Tenant, the PVT zone is defined with three server VLANs. In addition, each Tenant is assigned a separate Nexus 1000V VSG instance in the PVT zone. The VSG is used to provide security policies to monitor and protect traffic between the VLANs and Zones.
- **DMZ.** The VMDC VSA 1.0 Gold container supports a DMZ for Tenants to place VMs into a DMZ area, for isolating and securing the DMZ workloads from the PVT workloads, and also to enable users on the Internet to access the DMZ-based cloud services. The ASR 9000 PE WAN router is also connected to the Internet, and a shared (common) VRF instance (usually global routing table) exists for all Gold Tenants to connect to. This traffic is sent to the customer's CSR 1000V on a second interface (the CSR 1000V has two interfaces, one connecting to the Internet, one connecting to the Cust-VRF). The CSR 1000V decrypts the traffic and forwards to the VMs in the DMZ. The DMZ can be used to host applications like proxy servers, Internet-facing web servers, email servers, etc. The DMZ consists of one server VLAN in this implementation. The VSG is used to provide security policies to monitor and protect traffic to the VMs.

In VMDC VSA 1.0, a Gold Tenant can choose to have only the PVT Zone, only the DMZ, or both the PVT Zone and DMZ. The CSR 1000V utilizes IOS ZBF to control and secure traffic flows from outside to the zones and between the zones. To facilitate traffic flows between the DMZ and PVT Zones (for example, proxy or web servers in the DMZ and application and database servers in the PVT Zone), appropriate security policies need to be configured on the CSR 1000V ZBF. The VSG is used to provide compute firewall services for VMs in the PVT Zone and DMZ. Load balanced traffic for all tiers of Gold Tenants is implemented using the Citrix NetScaler VPX, which has one interface in each of the tiers (VLAN segments). A separate VSG and VPX (pairs with redundancy) are used in the PVT Zone and DMZ.

The following cloud traffic services flows can be enabled in the VMDC VSA 1.0 Two-Zone Gold service tier, orchestrated by IAC 4.0:

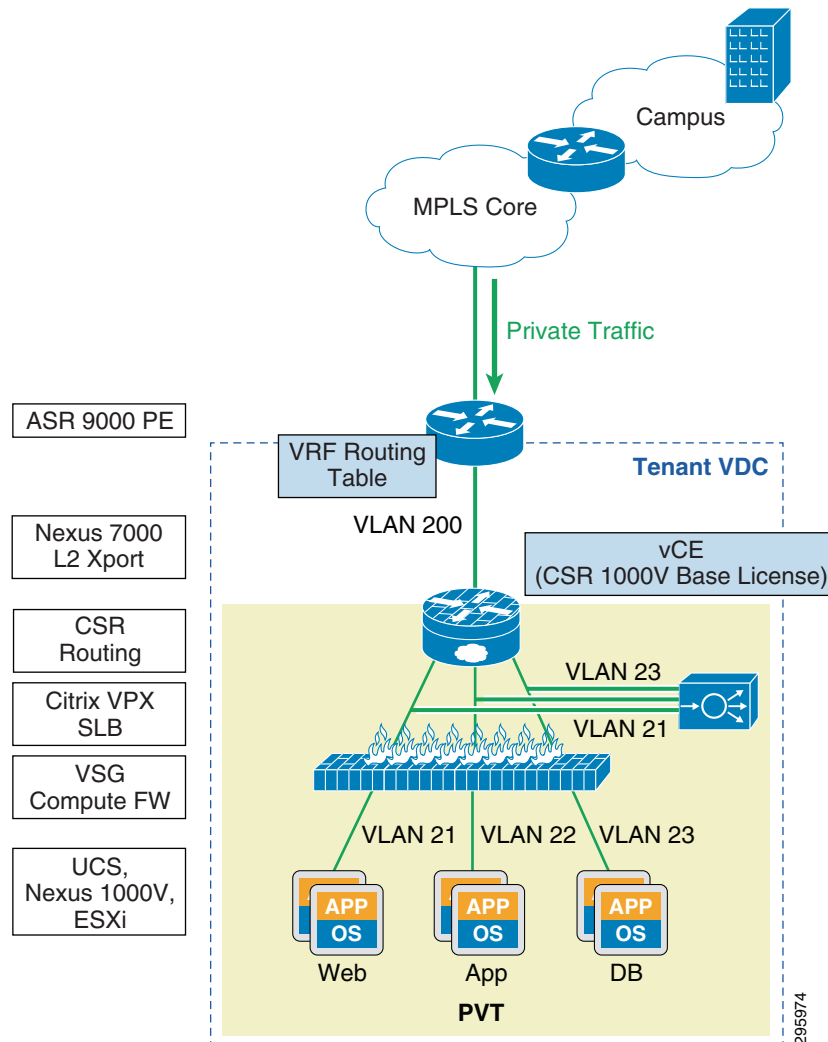
- MPLS-VPN to PVT Zone
- Internet to DMZ
- DMZ to PVT Zone

- MPLS-VPN to DMZ

## VMDC VSA 1.0 Silver Network Container

Figure 2-2 shows a logical representation of a VMDC VSA 1.0 Silver service tier network container.

**Figure 2-2 VMDC VSA 1.0 Silver Network Container**



The Silver Tenant gets one network (and compute/storage) zone (PVT) to place workloads into. Each Silver Tenant container has its own set of transport VLANs, compute segment VLANs, and virtual routing instances (CSR 1000V). This Silver service tier provides the following services:

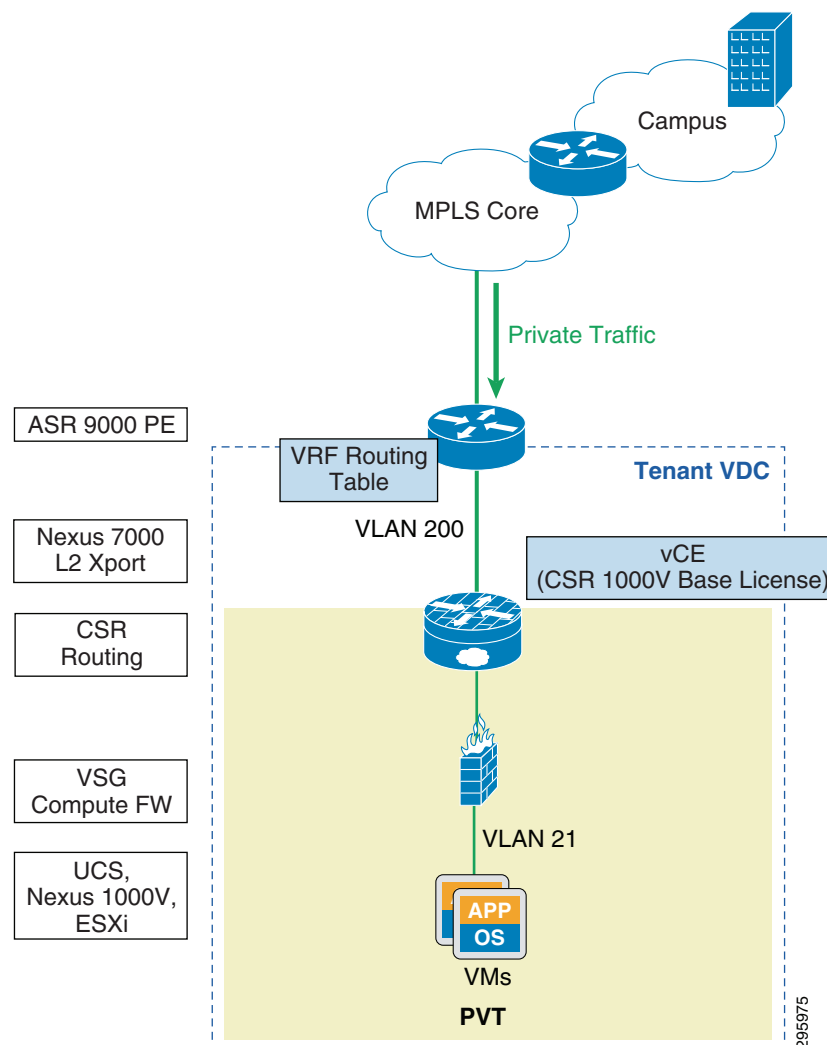
- Routing (BGP) on the CSR 1000V, to connect the Tenant VDC to the Tenant VRF instance on the WAN router
- Access from MPLS-VPN to Tenant container (VDC)
- One zone - PVT - to place workloads, with 3 VLAN segments in the zone

- SLB on the Citrix NetScaler VPX to provide L4-7 LB and SSL offload services to Tenant workloads. Note that the VMDC VSA 1.0 architecture was validated with the Citrix NetScaler VPX, and future versions of the VMDC VSA system will be validated with the Nexus 1000V vPath-based Citrix NetScaler 1000V.
- Compute firewall on the VSG to provide Inter-VLAN and Intra-VLAN security service to the Tenant VMs
- Medium QoS SLA with one traffic class - standard data
- Redundant virtual appliances for HA

## VMDC VSA 1.0 Bronze Network Container

Figure 2-3 shows a logical representation of a VMDC VSA 1.0 Bronze service tier network container.

**Figure 2-3 VMDC VSA 1.0 Bronze Network Container**





The Bronze Tenant gets one network (and compute/storage) zone (PVT) to place workloads into. Each Bronze Tenant container has its own set of transport VLAN, compute segment VLAN, and virtual routing instances (CSR 1000V). This Bronze service tier provides the following services:

- Routing (BGP) on the CSR 1000V, to connect the Tenant VDC to the Tenant VRF instance on the WAN router
- Access from MPLS-VPN to Tenant container (VDC)
- One zone - PVT - to place workloads, with 1 VLAN segment in the zone.
- Compute firewall on the VSG to provide Inter-VLAN and Intra-VLAN security service to the Tenant VMs
- Lower QoS SLA with one traffic class - premium data
- Redundant virtual appliances for HA

## VMDC VSA 1.0 Container Details Not Orchestrated by IAC 4.0

There are some differences between the VMDC VSA 1.0 network containers outlined above, and the VSA 1.0 based network containers available out-of-box in IAC 4.0. The details of the network containers orchestrated by IAC 4.0 are described later in this chapter. Some of these key differences between the network containers defined in the VSA 1.0 solution and the containers orchestrated by IAC 4.0 are highlighted below.

- IAC 4.0 can instantiate and orchestrate the CSR 1000V, VSG, Citrix VPX virtual platforms, port profiles on the Nexus 1000V, and can orchestrate VLANs on Nexus 5500, Nexus 7000 and Nexus 9000 switching platforms. IAC 4.0 cannot currently orchestrate other physical network devices, such as the ASR 9000, ASR 1000, ASA 5500 etc. out-of-box. Thus, the VSA 1.0 network containers that can be orchestrated out-of-box by IAC 4.0 do not include the ASR 9000 WAN-PE platform. Once IAC 4.0 instantiates the VSA container (CSR 1000V, VSG, VPX, Nexus 1000V and VLANs on the Nexus 5500/7000), the matching configuration (sub-interface, IP, Virtual Routing and Forwarding (VRF), Border Gateway Protocol (BGP) routing to CSR 1000V, and so on) needs to be manually configured on the ASR 9000 WAN-PE device, so that the Tenant network container becomes fully functional.
- IAC 4.0 does not currently support orchestrating the ASA 1000V platform, and hence, the VMDC VSA 1.0 Zinc Container defined in the VSA 1.0 solution is not supported in IAC 4.0.
- The IPsec-VPN capability defined on the CSR 1000V in the VSA 1.0 Gold Container is not orchestrated out-of-box by IAC 4.0.
- The AppNav and AVC features defined on the CSR 1000V in the VSA 1.0 Gold Container are not orchestrated by IAC 4.0.
- While the VSA 1.0 network containers utilize redundant CSR 1000, VSG, and VPX platforms, the IAC 4.0 orchestrated VSA containers can only be created with single CSR 1000V, VSG, and VPX instances. Customers can instead utilize the VMware vSphere High Availability (HA) features.
- The VSA 1.0 Gold container utilizes the vWAAS appliance to provide WAN optimization services, and the vNAM appliance to provide monitoring and visibility services. IAC 4.0 does not orchestrate the vWAAS or vNAM appliances, so these services are not available in the IAC 4.0 VSA 1.0 Gold Container.
- While VSA 1.0 Gold, Silver, and Bronze Containers utilize VXLAN segments to place VMs into, IAC 4.0 does not orchestrate VXLAN compute segments. Instead, IAC 4.0 utilizes VLANs to place VMs into the Gold, Silver, and Bronze Containers.

- In the VMDC VSA 1.0 Gold and Silver containers, the Citrix VPX is utilized in one-arm mode sitting in the server segment (VXLAN or VLAN). In the IAC 4.0 orchestrated VSA 1.0-based containers, however, the VPX is connected in one-arm mode to the CSR 1000V on a separate interface from the server VLANs. This consumes an extra interface on the CSR 1000V, but requires only one interface (instead of one per server VLAN) on the VPX.

The VMDC VSA 1.0 architecture, and the IAC 4.0 orchestration for VSA 1.0, were validated with the Citrix NetScaler VPX virtual platform. Future versions of the VMDC VSA solution will validate with the Nexus 1000V vPath-based Citrix NetScaler 1000V platform (the Cisco OEM version of Citrix VPX). IAC 4.0 can also be extended to support orchestration for the Citrix NetScaler 1000V platform.

## IAC 4.0 Orchestration Design

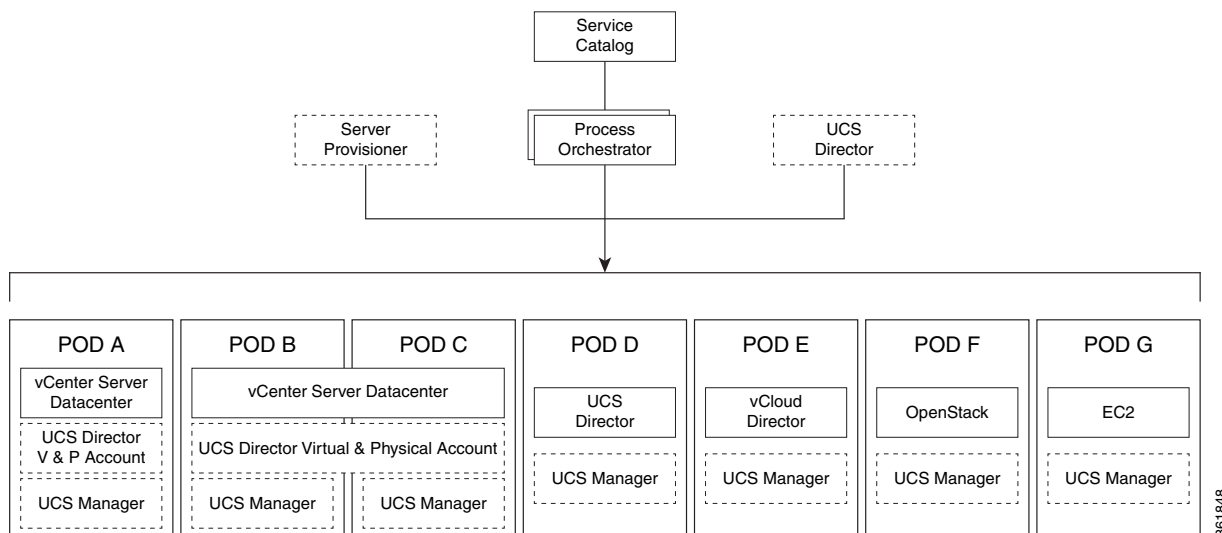
### Physical Resources

The resources in IAC are divided into Compute and Network pods.

### Compute Pod

The Compute pod is a grouping of compute and storage resources. VMware vCenter was the only type of Compute pod used in this release. Multiple Compute pods consisting of VMware vCenter and the Unified Computing System Manager (UCSM) were tested in this release. There were multiple data centers and resource pods configured on the vCenter. Multiple UCS Managers were also used. [Figure 2-4](#) shows the supported Compute pod implementations.

**Figure 2-4** Compute Pod

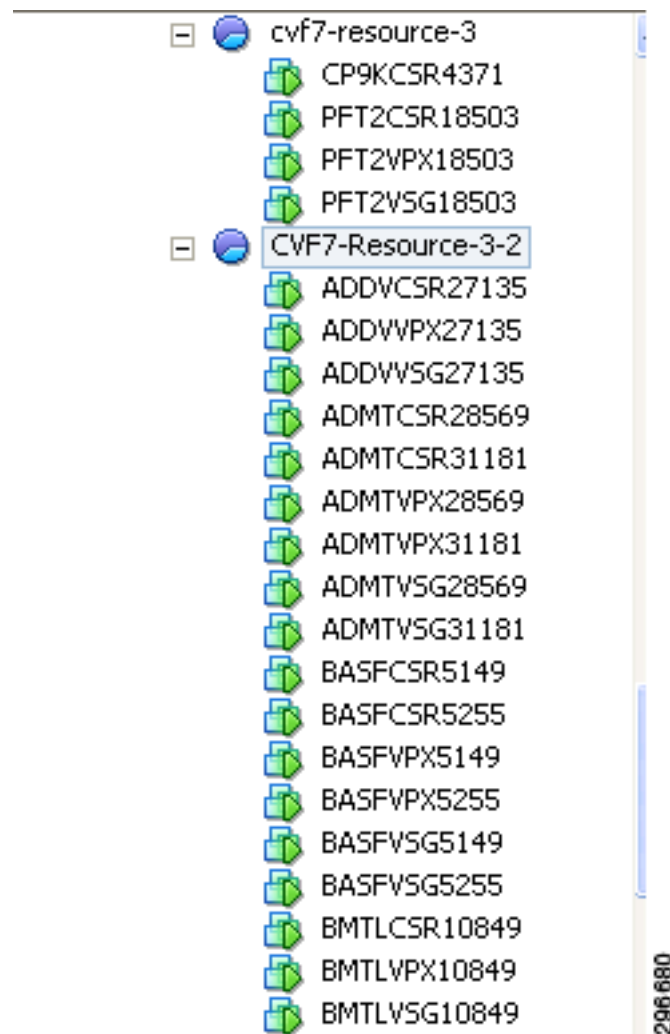


IAC needs to be able to deploy the service nodes and user VMs on some type of compute structure. There are no requirements. Our IAC deployment consisted of 2 UCS chassis, 16 blade servers and a storage array all managed by VMware vCenter. This could have been performed on a single server with locally attached storage, similar to the IAC 4.0 Proof of Concept (PoC) validation.

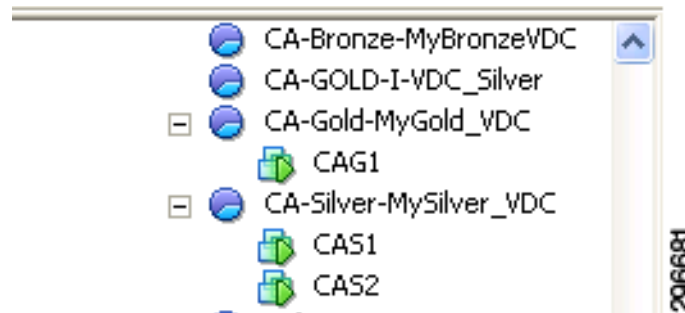
IAC requires that the vCenter has been pre-configured with data center(s), resource pool(s), and storage and networking resources, including Cisco's virtual distributed switch, Nexus 1000V. If using the UCS chassis, then vNIC templates need to be configured to allow IAC to provision the VM interfaces. If provisioning bare-metal servers on the UCS chassis, then service profiles also need to be configured.

IAC deploys the service nodes in a resource pool on vCenter. The resource pool needs to be created prior to creating the Organization. When creating the Organization, you can use the drop-down menus to request a resource pool. The resource pool is a way to Organize IAC created service nodes, or all service nodes can be installed in a single resource pool (see [Figure 2-5](#)).

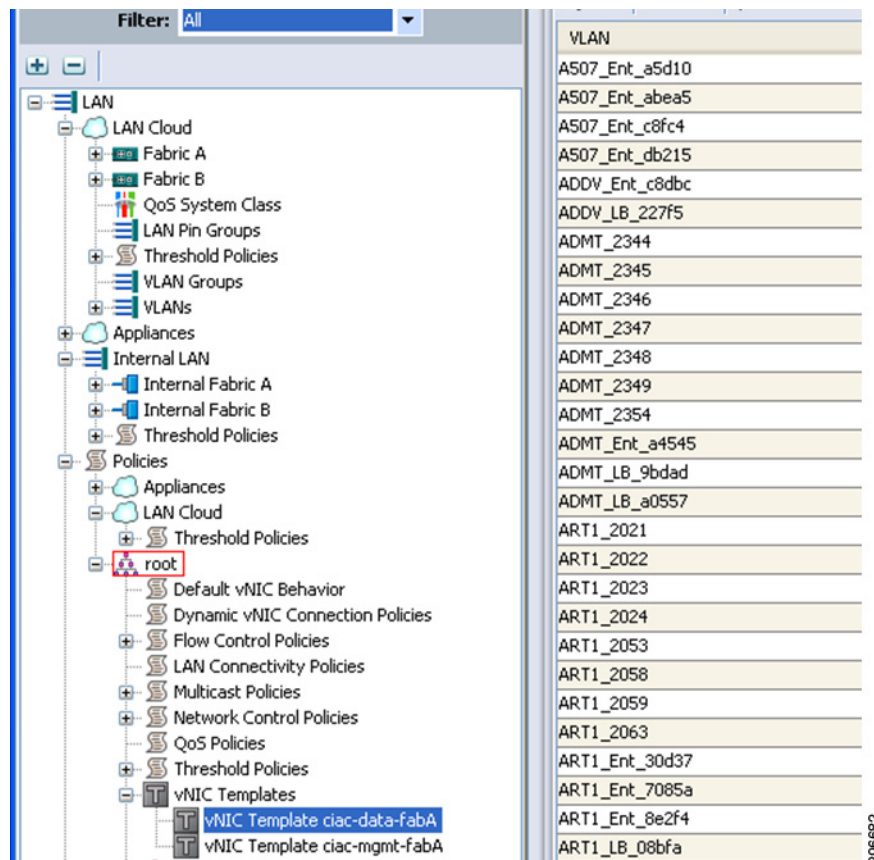
**Figure 2-5** Resource Pools Containing Org Service Nodes



IAC creates a resource pool on the vCenter for each VDC to store user VMs (see [Figure 2-6](#)).

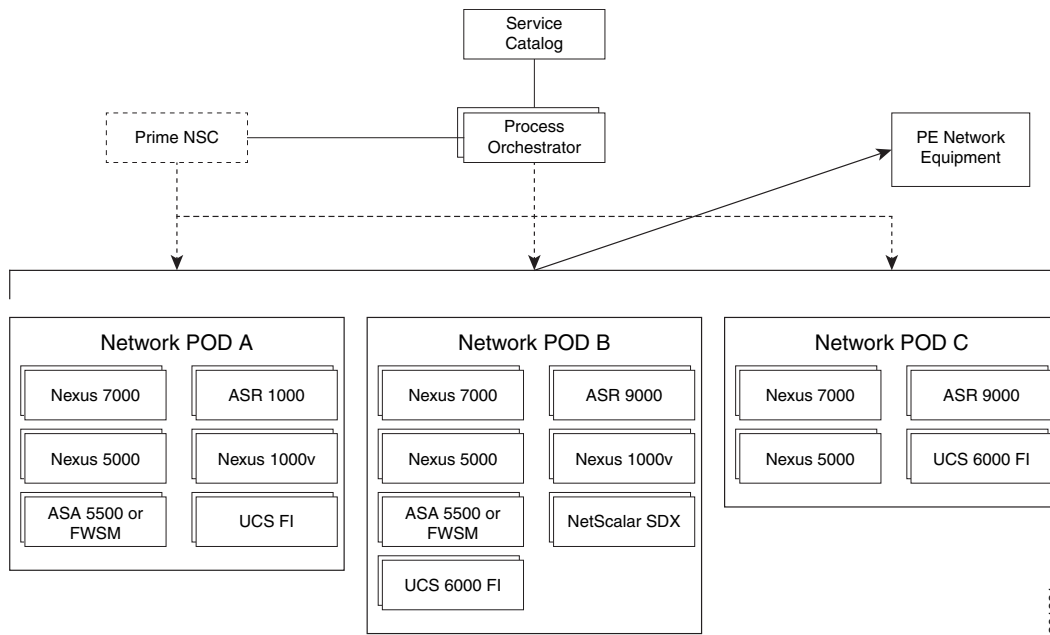
**Figure 2-6 Resource Pools for VDC VMs**

IAC provisions the data uplinks on the UCS to allow IAC created service nodes and user VMs to communicate. If the vNIC templates are not used, then VLANs need to be manually added to the data uplinks (see [Figure 2-7](#)).

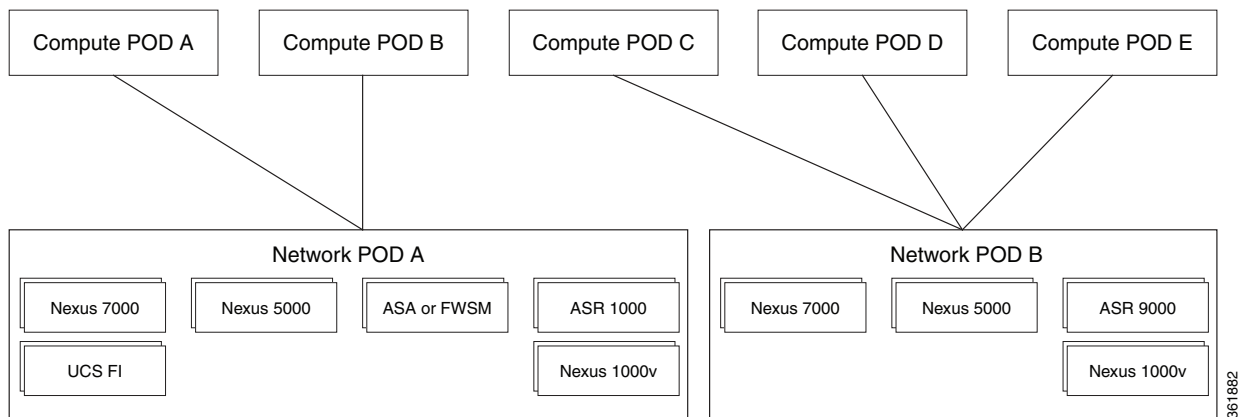
**Figure 2-7 UCS vNIC Template with VLANs**

## Network Pod

The Network pod (see [Figure 2-8](#)) is a group of physically connected network devices. There were two Network pods used in this release: the first Network pod contained the Nexus 7000, 5000, 1000V and UCS Fabric Interconnect (FI), and the second Network pod contained Nexus 9000 switches and the UCS FI.

**Figure 2-8 Network Pod**

Within IAC, there is also the relationship between the Network and Compute pods. There can be multiple Compute pods per Network pod. This release includes one Network pod to one Compute pod. [Figure 2-9](#) shows a typical Compute pod to Network pod setup.

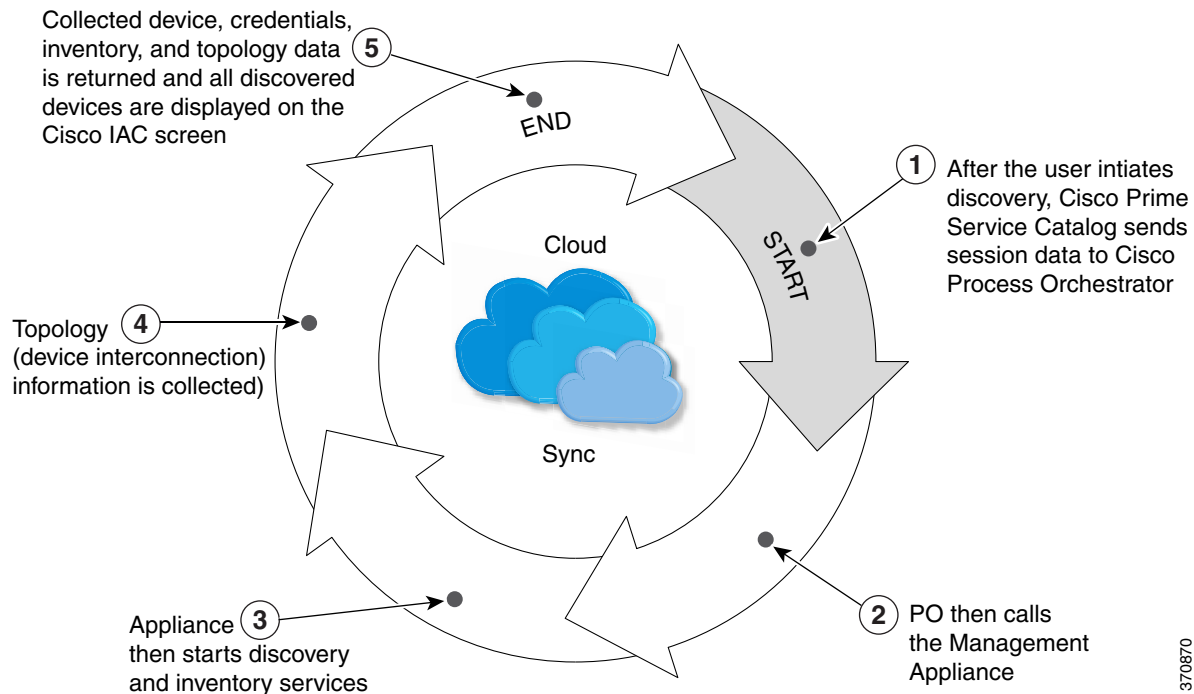
**Figure 2-9 Compute Pod to Network Pod Setup**

## Discovery of Resources

IAC uses Cisco's eXtensible Management Platform (XMP) running on a dedicated VM for discovering network components. IAC supports a VMware-based virtual appliance that provides two functions, depending on how it is deployed. The IAC virtual appliance comes with IAC 4.0 XMP pre-installed. When deploying the virtual appliance, there is an option to deploy the appliance as a management appliance or Prime Service Catalog (PSC). If you want to deploy both options, then you need to deploy two virtual appliances.

The discovery process on IAC is called CloudSync (see [Figure 2-9](#)). IAC uses Simple Network Management Protocol (SNMP) to discover devices and then uses Cisco Discovery Protocol (CDP) to further identify and create a topology.

**Figure 2-10 Network Discovery Flow**



## Logical Resources

### IP Addresses

IAC has its own internal IP Address Management (IPAM) system. There are four different pools of addresses:

- Public IP addresses used for servers in the DMZ, Public accessible Virtual IP (VIP) addresses and Network Address Translation (NAT)
- Internet Transit IP addresses
- Enterprise Transit IP addresses
- Private IP addresses (RFC1918) for all non-DMZ types

These pools are assigned when the IAC is first installed and Network pods are created. Additional pools can be created as needed. IAC takes care of tracking assigned and unassigned status when IP addresses are in use. IP ranges are used in a round-robin fashion.

The pool of Public (Unprotected) IP addresses is the Service Provider's Internet routable IP address. These are the IP addresses that are advertised to the Internet. IAC creates smaller subsets to be used for DMZ-based servers based on the requested number of hosts. VIP addresses and NAT (floating IP) use a /32 subnet. End Users cannot request a specific IP address. An example of what IAC might allocate for Public IP addresses is shown below.

```
64.171.5.163/32 for NAT
64.171.4.101/32 for VIP
64.171.5.177/28 for DMZ
```

The pool of Private IP addresses is used everywhere else. IP addresses from the Private pool are used for the Citrix NetScaler VPX gateway, SNIP addresses, and any Private VIP addresses. These IP addresses are also used for all Protected Public, Unprotected Private, and Protected Private zones. An example of what IAC might allocate based on an expected 12 hosts per network is shown below.

```
172.16.0.0/24 LB Network
172.16.0.4 SNIP
172.16.1.17/28 Protected Public
172.16.1.33/28 Unprotected Private
172.16.1.49.28 Protected Private
```

## VLANs

VLANs are used for Layer 2 (L2) separation. IAC does not use Virtual Routing and Forwarding (VRF) instances.

Unlike in other VMDC releases, which typically display Gold, Silver, and Bronze networks using a pool of pre-defined VLANs for each container type, IAC does not allow for this distinction. VLANs are allocated as needed, regardless of container type.

When setting up IAC, the Service Provider allocates a range of VLANs per Network pod. Additional pools are created for each Network pod. When an Organization is created, IAC assigns a VLAN from this pool for all of the requested networks, with up to two VLANs used per Organization for an Organization with a connection type of Enterprise and requesting LB services.

VLANs are chosen based on availability. On a fresh install when first deploying Organizations, the VLANs are typically in sequential order. This changes if the VLAN pool has been consumed and VLANs are recycled. When creating VDCs, IAC again allocates VLANs from this pool. IAC assigns up to four VLANs, depending on the network container type.

IAC starts configuring the management interface using the management VLAN. The Internet Transit interface uses the Transit network VLAN. If requested, then the Enterprise Transit interface uses the first available VLAN in the pool of VLANs. If requested, then the LB network uses the next available VLAN in the pool of VLANs.

As VDCs are deployed, IAC assigns a VLAN from the pool of VLANs. End Users are not able to choose a VLAN and are typically unaware of which VLANs are being used.

## Networks

IAC needs Infrastructure, Service, and Internet Transit networks available before installing. IAC allocates IP addresses from these networks when creating service nodes. These should all be dedicated networks with IAC maintaining the pool of IP addresses.

The Infrastructure network could be considered a separate virtual services management network. Every network service node uses this network for management. The CSR 1000V consumes two of these IP addresses. Every Org that has a CSR 1000V, VSG, and VPX requires four IP addresses, so 30 Orgs could use 120 IP addresses. There is a Nexus 1000V port profile associated with this network, so ensure that the max-ports statement is set to the value of expected IP addresses. This network needs to be routable to the network that the PO and PNSC servers reside on. This is the network that the PO and PNSC servers access to configure.

The Service network is the data network used on the VSG. Since the VSG is operating in Layer 3 (L3) mode, this network's gateway needs to allow proxy-arp and needs to be routable to the management network. This is the network that the Nexus 1000V uses to communicate with the VSG. Only one IP address is used per Organization.

The Internet Transit network is used for the Internet connection on a network container with Public access. This network is used when configuring the CSR 1000V for BGP routing. This can be on the same network as the gateway to the Internet. If in a different network, then the eBGP multi-hop option is used, and a static route to the eBGP peer address is created on the CSR 1000V with the next hop being the Tenant gateway.

## Network Provisioning

### Layer 2 Provisioning

IAC requires that the network be configured using Virtual Port Channels (vPC) and port channels in order for IAC to provision the network. IAC also requires that all network devices be discovered during the discovery process. IAC provisions the network by adding VLANs to the VLAN database and VLANs to all port-channel switched ports.

```
cvf7-n9508-1# sho vlan id 2260
VLAN Name                               Status    Ports
-----
2260 ART9_2260                          active    Po31, Po35, Eth1/1/1, Eth1/1/2
                                                Eth2/35, Eth2/36

VLAN Type  Vlan-mode
-----
2260 enet  CE
Remote SPAN VLAN
-----
Disabled
Primary  Secondary  Type          Ports
-----
cvf7-n9508-1# sho run int Po31
!Command: show running-config interface port-channel31
!Time: Wed May 14 20:47:14 2014
version 6.1(2)I2(1)
interface port-channel31
  switchport
  switchport mode trunk
  switchport trunk allowed vlan 100-101,2000-2001,2015,2030,2042
  switchport trunk allowed vlan add 2044,2055,2060-2061,2065,2071,2076-2077
  switchport trunk allowed vlan add 2104-2105,2132-2134,2137,2140,2146-2165
  switchport trunk allowed vlan add 2167-2218,2220,2224-2230,2232-2268
  switchport trunk allowed vlan add 2270-2325,2327-2354
  vpc 1

cvf7-n9508-1#
```

### Layer 3 Provisioning

IAC uses BGP routing for Tenant containers to access the Internet or the Enterprise. Depending on the container type, IAC places the following configuration on the CSR 1000V:

```
router bgp 65500
  bgp log-neighbor-changes
  redistribute connected
```



```

redistribute static
neighbor 10.2.2.1 remote-as 109
neighbor 10.2.2.1 description Enterprise neighbor
neighbor 10.2.2.1 prefix-list Private-net-list out
neighbor 20.1.2.1 remote-as 109
neighbor 20.1.2.1 description Internet neighbor
neighbor 20.1.2.1 prefix-list Public-net-list out

```

If the Internet gateway router is not the next hop, then IAC adds an additional statement:

```
neighbor 20.1.2.1 ebgp-multihop 2
```

IAC currently only configures a single IP address for either the Internet or Enterprise neighbor. IAC uses the VIP address with a /32 subnet to create a static route to redistribute the route to the VIP address:

```
ip route 64.171.5.160 255.255.255.255 GigabitEthernet4 172.16.4.4
```

For NAT, IAC creates a loopback interface to be used as a connected interface to redistribute the route to the NAT.

IAC starts configuring the management interface using the management VLAN. The Internet Transit interface uses the Transit network VLAN. If requested, then the Enterprise Transit network interface uses the first available VLAN in the pool of VLANs. If requested, then the LB network uses the next available VLAN in the pool of VLANs.

As VDCs are deployed, IAC assigns a VLAN from the pool of VLANs. End Users are not able to choose a VLAN and are typically unaware of which VLANs are used.

```

interface Loopback1
description cf54169a-62c1-4342-8f57-49187fffa8f5
ip address 64.171.5.163 255.255.255.255

```

IAC uses a prefix list to prevent Private IP addresses from being routed to the Internet and Public IP addresses from being routed to the Enterprise.

```

ip prefix-list Private-net-list seq 10 permit 10.0.0.0/8 le 32
ip prefix-list Private-net-list seq 11 permit 172.16.0.0/12 le 32
ip prefix-list Private-net-list seq 12 permit 192.168.0.0/16 le 32
ip prefix-list Private-net-list seq 13 deny 0.0.0.0/0 le 32
!
ip prefix-list Public-net-list seq 10 deny 10.0.0.0/8 le 32
ip prefix-list Public-net-list seq 11 deny 172.16.0.0/12 le 32
ip prefix-list Public-net-list seq 12 deny 192.168.0.0/16 le 32
ip prefix-list Public-net-list seq 13 permit 0.0.0.0/0 le 32

```

### CSR 1000V Internet Interface Configuration

IAC does not configure the Internet or Enterprise gateways. These two devices need to be configured manually. For the external gateways to communicate with the Tenant's VDC, the gateway's BGP needs to include the IP addresses from the CSR 1000V configured for that VDC.

For the Internet gateway, the IP address from interface GigabitEthernet2 needs to be added to the BGP configuration on the Internet gateway. This is assuming the gateway device is configured with an IP address on the Internet Transit network. The CSR 1000V should already contain the proper BGP configuration.

```

NTCCSR28868#sho run int gi 2
Building configuration...
Current configuration : 246 bytes
!
interface GigabitEthernet2
description configured by PolicyAgent
ip address 20.1.2.60 255.255.255.0
ip nat outside
ip access-group default-ingress in
ip access-group default-egress out

```

```

zone-member security Internet
negotiation auto
end

```

### Internet Gateway

```

RP/0/RSP0/CPU0:cvf7-wan-9k1#sho run | b router bgp 109
Wed May 14 09:59:26.926 EDT
Building configuration...
router bgp 109
  address-family ipv4 unicast
  !
  address-family vpv4 unicast
  !
  af-group IAC-TENANTS address-family ipv4 unicast
    route-policy allow-all in
    route-policy allow-all out
  !
  neighbor-group IAC-TENANTS
    remote-as 65500
    address-family ipv4 unicast
    use af-group IAC-TENANTS
  !
  !
  neighbor 20.1.2.60
    use neighbor-group IAC-TENANTS
  !

```

A sub-interface needs to be created with the VLAN of the Enterprise network in the network for the Enterprise gateway. Unlike the Internet Transit network, which has a shared VLAN and shared IP subnet, the Enterprise VLAN is allocated when the Organization is created with the VLAN obtained from the pool of VLANs. An IP subnet is used from the pool of available subnets associated with the Tenant Private supernet when configuring a Private network interface of a Tenant resource, e.g., CSR 1000V, VPX, or VM.

The configuration applied on the ASR 9000 should match the configuration applied on the Enterprise interface of the CSR 1000V and the VLAN associated with this interface. A sample configuration is shown below.

### CSR 1000V Enterprise Interface Configuration

```

interface GigabitEthernet3
description configured by PolicyAgent
ip address 10.2.2.2 255.255.255.240
ip access-group default-ingress in
ip access-group default-egress out
zone-member security Enterprise
negotiation auto
end

```

### Nexus 1000V Configuration

```

cvf7-n1kv-3# sho vlan | b NTC_Ent
2351 NTC_Ent_c060f          active      Po6, Po7, Po8, Po9, Po10, Po11
                           Po13, Po15, Veth423

```

### ASR 9000 Configuration

```

interface Bundle-Ether13.2351
vrf IAC-TENANT4
ipv4 address 10.2.2.1 255.255.255.240 << matching Tenant Enterprise Subnet
encapsulation dot1q 2351 << match Tenant Enterprise VLAN

```

```

Under BGP router config add the IP of the CSR
vrf IAC-TENANT4
  rd 100:4
  address-family ipv4 unicast
  !
  neighbor 10.2.2.2
    use neighbor-group IAC-TENANTS
    address-family ipv4 unicast

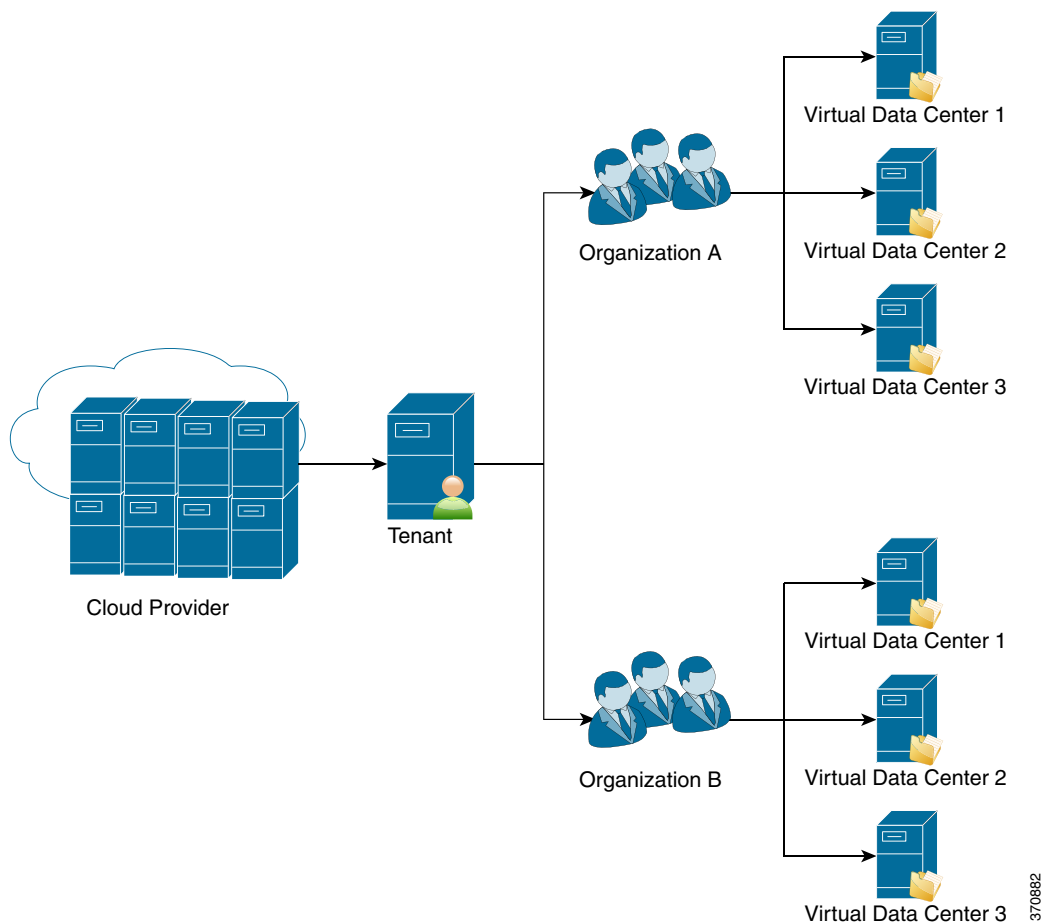
```

## Tenant Design

### Tenant Structure

The IAC Tenant structure (see [Figure 2-11](#)) consists of a hierarchical, three-tier model with a top-level Tenant and multiple Organizations and VDCs. A Tenant can contain multiple Organizations, and each Organization can contain multiple VDCs.

**Figure 2-11** IAC Tenant Structure



## IAC 4.0 Multi-Tenancy

IAC is multi-tenancy and multi-organizational with the capability of creating multiple VDCs. Users of one Tenant should not be able to see objects in another Tenant. Within the same Tenant, users of one Organization should not be able to see objects in another Organization. Within Organizations, users of one VDC should not be able to see objects in another VDC. The CPTA user has access to all Tenants, Organizations, and VDCs. Operations that one Tenant performs should have no impact on any other Tenants.

The following is a multi-tenancy feature summary:

- Onboard/modify/offboard Tenants
- Complete data isolation between Tenants
- Tenant Admin user roles
- Tenant-specific views and summaries
- Tenant-specific pricing policies
- Provider and Tenant control of service offering elections
- Tenant-specific template catalog
- Tenant control of VDC access
- Order on behalf for VDC and load balancers

There are some limitations to multi-tenancy when it comes to naming. The same user names cannot be used across multiple Tenants, and the same VDC name cannot be used across multiple Tenants. If UserA exists in TenantA, then UserA cannot be used in TenantB. A message warning that the user name is not available appears. The same occurs if there is a VDC named VDC1 in TenantA. If TenantB tried to create a VDC with the name VDC1, then a message appears that this name has been used.

## IAC User Roles and RBAC

The IAC Administration Guide lists typical user roles and their responsibilities, but these are guidelines. The majority of testing for this release followed those guidelines.

The ISAC user roles are defined below.

- The Cloud Provider Technical Administrator (CPTA) creates the Tenant and Tenant Technical Administrator (TTA) user. The CPTA account is the first user account created and is created during the initial configuration of IAC.
- The Tenant Technical Administrator (TTA) creates the Organization and the Organization Technical Administrator (OTA) user and Virtual Server Owner (VSO) or Virtual and Physical Server Owner (VPSO) users.
- The Organization Technical Administrator (OTA) creates the VDC and any of the VSO or VPSO users. The OTA, VSO, or VPSO is responsible for the majority of the VM tasks, such as configuring firewall rules or managing load balancers.

Not all roles need to be created. All of the roles are hierarchical, with the CPTA user capable of performing all tasks. The TTA user is capable of performing all tasks of the OTA, VSO, or VPSO users.

The following are default user roles for managing and reporting that were not tested in this release:

- Cloud Provider Business Administrator (CPBA)
- Tenant Business Administrator (TBA)

For a complete list of user roles and capabilities, refer to the [Cisco Intelligent Automation for Cloud Administrator Guide](#).

### Onboarding a Tenant Considerations

Consider the following options when onboarding a Tenant:

1. **Run Rate.** The run rate cannot currently be increased, so plan accordingly. If the rate limit is reached, then no other services can be ordered.
2. **Private Subnet.** The drop-down menu option allows for three predefined RCF1918 address ranges, plus the option to select “Other” to create a personal IP address range. This is the pool of IP addresses used when creating service nodes and End User servers. These addresses are expected to be internal IP addresses and not routed to the Internet. Public IP addresses from the Service Provider are used for any Internet-facing requirements, such as Public accessible VIP addresses and servers placed in a DMZ (Unprotected Public) and for NAT to servers on the Protected Public network. The pool of Public IP addresses are created when the Service Provider first installs and configures the IAC software.
3. **Service Options.** These system-wide options list all available options that the Service Provider is offering. The options selected when onboarding a Tenant are passed down to the available options used when creating the Organization.
4. **Advance Network Services.** If this options is selected, then an Organization is allowed to order and instantiate a CSR 1000V. This is a required option. Without this option IAC, is not able to configure any of the other service nodes, and there is no routing for the Organization or any underlying VDCs.
5. **Multiple Security Zones.** This option defaults to “Yes” and cannot be changed. This option allows IAC to create ZBF rules on the CSR 1000V.
6. **Enhanced VM Security.** If this option is selected, then an Organization is allowed to order and instantiate a VSG.
7. **Load Balancing Services.** If this option is selected, then an Organization is allowed to order and instantiate a VPX. This allows the VDCs created under the Organization the option to use LB services.

## VDC Connection Type

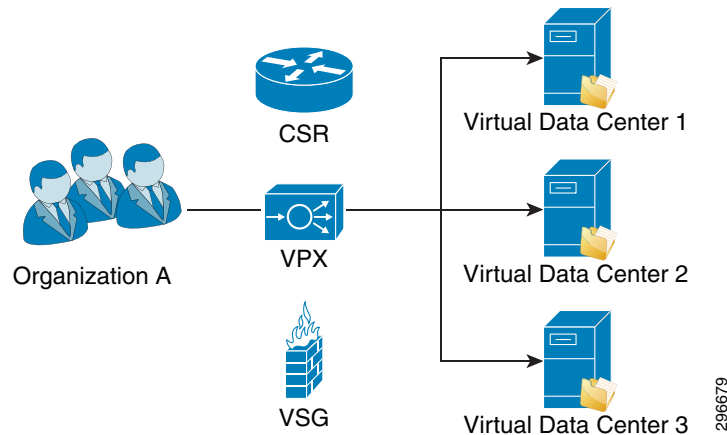
There are three VDC connection type: Both, Enterprise-Connected, and Internet-Connected. This connection determines how the CSR 1000V for the Organization is configured. This option cannot be changed after the Tenant has been onboarded.

The Enterprise Transit network allows the VDC to communicate with the Enterprise Network. The options are pre-populated when the Service Provider installs and configures IAC. These options can be changed. These values are used when configuring the CSR1 1000V’s BGP routing profile. Note that there are no options to change the Internet Transit network. This is typically one Internet connection or possible redundant Internet connections, and they are maintained by the Service Provider. Those values are configured when the Service Provider installs and configures IAC. An Enterprise could possibly have their own endpoint and could possible need to modify these values. Care must be used when selecting the network size. IAC configures the max-ports statement on the Nexus 1000V based on the size of the network selected. It is possible to exhaust the available ports in the virtual distributed switch.

## Organization Design

Each Organization under a Tenant shares a common set of network services devices, which includes the CSR 1000V, VPX, and VSG. IAC provisions a single CSR 1000V, VPX, and VSG per Organization (see [Figure 2-12](#)). There is a capacity limit on the CSR 1000V and VMware that restricts the number of available interfaces to ten. Depending on the number and type of VDCs that are planned, additional Organizations may be required to accommodate the required number of VDCs and networks.

**Figure 2-12** *Single CSR 1000V, NetScaler VPX, VSG Per Organization*



### Creating an Organization Considerations

The options available here are based on the options selected when onboarding a Tenant.

- **VDC Type.** The options here depend on what is available to the Tenant. A Tenant might have both an Internet connection and an Enterprise connection, but TTA may select only one of these options when creating the Organization. If the Tenant has only an Internet-Connection type or Enterprise-Connection type, then this option defaults to one of them.
- **Organization-wide Service.** The TTA is allowed to select a smaller subset of options provided by the Tenant. These follow the same guidelines as the Tenant.
- **Advance Network Services.** If this options is selected, then an Organization is allowed to order and instantiate a CSR 1000V. This is a required option. Without this option, IAC is not able to configure any of the other service nodes, and there is no routing for the Organization or any underlying VDCs.
- **Multiple Security Zones.** This option defaults to “Yes” and cannot be changed. This option is to allow IAC to create ZBF rules on the CSR 1000V.
- **Enhanced VM Security.** If this options is selected, then an Organization is allowed to order and instantiate a VSG.
- **Load Balancing Services.** If this option is selected, then an Organization is allowed to order and instantiate a VPX. This allows the VDCs created under the Organization the option to use LB services.
- **Resource Type.** These are the available options for the Tenant. These correspond to a Service Resource container that was created by the Service Provider. A Service Resource Container defines the network and compute resources set aside for a Tenant, from which a VDC is constructed. Selecting this option determines where the service nodes are instantiated and what networks are used by these service nodes.

- Add Load Balancer for HTTP and HTTPS. If the LB service is selected, then these fields are required. There is one thing to note here for the available service group. If no other service groups have been defined, then these drop-down menus default to HTTP or HTTPS. This is what is typically seen on a new deployment. If these are not the options that are used, then additional service groups can be created for this Tenant before creating the Organization. Otherwise, after the Organization has been created, the LB options need to be modified or new LB options need to be created.

## Virtual Data Center (Network Container) Design

IAC 4.0 provides a set of network containers, out-of-box, that approximate the VMDC VSA 1.0 network container reference model. This set of pre-defined network containers are not implemented as a one-to-one mapping to the previously described VMDC container types. IAC uses the concept of four different network zone types:

- Unprotected Public
- Protected Public
- Unprotected Private
- Protected Private

In VMDC VSA 1.0 equivalent terminology, the Unprotected Public network is the DMZ. The other zones are PVT Zones.

Each Organization can have multiple VDCs, and these VDCs do not need to be the same type. There are restrictions on the number of VDCs based on the number of available networks. Since IAC provisions a single CSR 1000V, VPX, and VSG per Organization, multiple Organizations may be required to accommodate the required number of VDCs.

Creating an Organization uses the first four network interfaces on the CSR 1000V:

- Gigabit 1 is used for management.
- Gigabit 2 is used for the Internet Transit network.
- Gigabit 3 is used for the Enterprise Transit network.
- Gigabit 4 is used for the LB network.

IAC is not flexible in this area.

Creating an Organization consumes the first four network interfaces, regardless of the options selected when onboarding a Tenant or when ordering an Organization. If the connection type is Internet-connected with no LB services, then IAC still consumes Gigabit 3 and 4, and these interfaces are not available to the VDC. These interfaces remain shutdown with no configuration.

When creating VDCs, IAC assigns networks as requested. The End User does not have the ability to choose which interface is used. An example of this is when selecting a Four-Zone Gold container as the first container type, Gigabit 5 is always the Unprotected Public network, and Gigabit 6 is always the Protected Public network. Gigabit 7 is always the Unprotected Private network, and Gigabit 8 is always be Protected Private network.

With the remaining six interfaces, multiple combinations of network containers can be created. There could be three Two-Zone networks that could include a Two-Zone Gold Internet container, or a Two-Zone Gold Enterprise container and a Two-Zone Silver Enterprise container. There could also be six One-Zone Bronze containers, or a single Four-Zone Gold container with two additional Public or Private network zones.

### Ordering a VDC Considerations

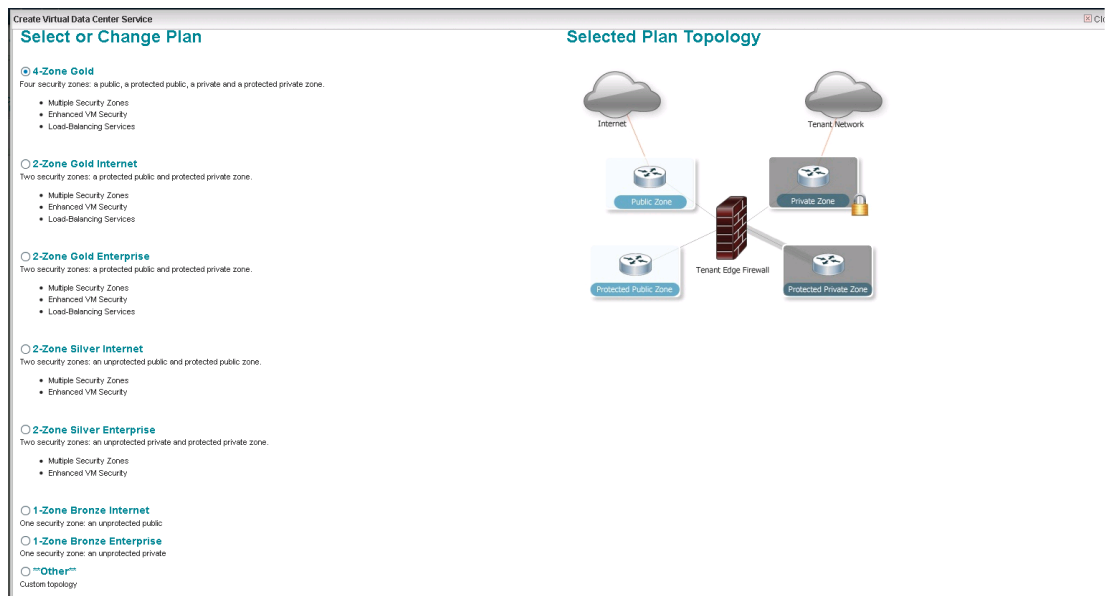
Consider the following options after selecting the type of network container:

- **VDC Size.** There is a drop-down menu with available sizes. These options limit the number of VMs, vCPUs, CPU limit, VM storage, VM memory, and physical servers that can be consumed by the VDC. By default, there are three sizes, but the Admin of the site can create additional sizes. These options can be increased by modifying the VDC.
- **Network Details.** It is suggested that a good naming convention be used for reference when creating VMs. The type of zone can be seen under the VDC details, but when creating VMs, the only option on where to deploy the VM is a name.
- The max-number of hosts expected is applied to the max-ports statement on the Nexus 1000V. Selecting this option correlates to the network subnet used on the interface. If 12 hosts are selected, then a 255.255.255.240 subnet is used. This option cannot be modified.

## IAC 4.0 Network Containers

When onboarding a Tenant and creating the Organization, the connection type (Both, Internet, or Enterprise) dictates what type of network container can be built. Network containers are selected when creating VDCs. [Figure 2-13](#) shows the options that are available when creating a VDC.

**Figure 2-13** Select or Change Plan



These predefined network containers can be modified by adding additional networks to the VDC after the VDC has been created. A Two-Zone Gold Container with one Unprotected Public and one Protected Public network can become a Two-Zone Gold Container with one Unprotected network and three Protected networks.

Based on the way IAC orchestrates networks, there really are no Unprotected networks. IAC creates a VSG per Organization, so by default, Unprotected networks have an allow all policy, but deny policies can also be created for VMs on an Unprotected network.

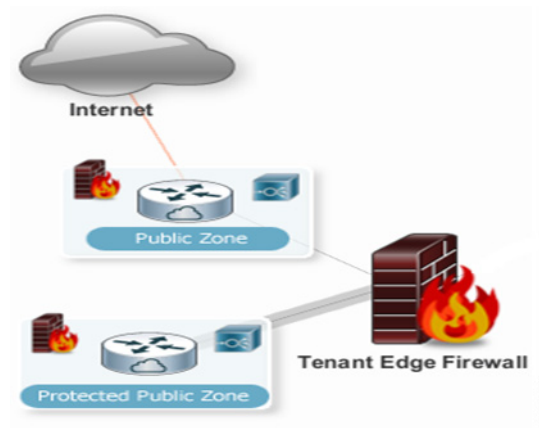


## Gold Network Containers

### Two-Zone Gold Public (Internet Container)

This container includes two security zones (Unprotected Public and Protected Public), enhanced VM security, and LB services. This container is suitable for Tenant clients located only in the Internet.

**Figure 2-14 Two-Zone Gold Container**

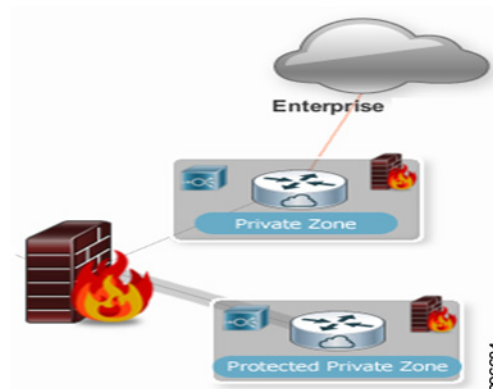


#### Two-Zone Gold Internet Attributes

- Routing (BGP) on the CSR 1000V to connect the Tenant VDC to the Service Provider WAN router
- Access from Internet to the Tenant container (VDC)
- Two zones - Protected Public and Unprotected Public - to place workloads. Each zone has its own VLAN segments.
- ZBF on the CSR 1000V to provide Inter-zone firewall services to protect the Tenant workloads
- NAT on the CSR 1000V to provide static and dynamic NAT services to RFC1918 addressed VMs
- SLB on the Citrix VPX, to provide L4-7 LB and SSL-Bridging services to Tenant workloads.
- Compute firewall on the VSG to provide Inter-VLAN and Intra-VLAN security service to the Tenant VMs

### Two-Zone Gold Private (Enterprise) Container

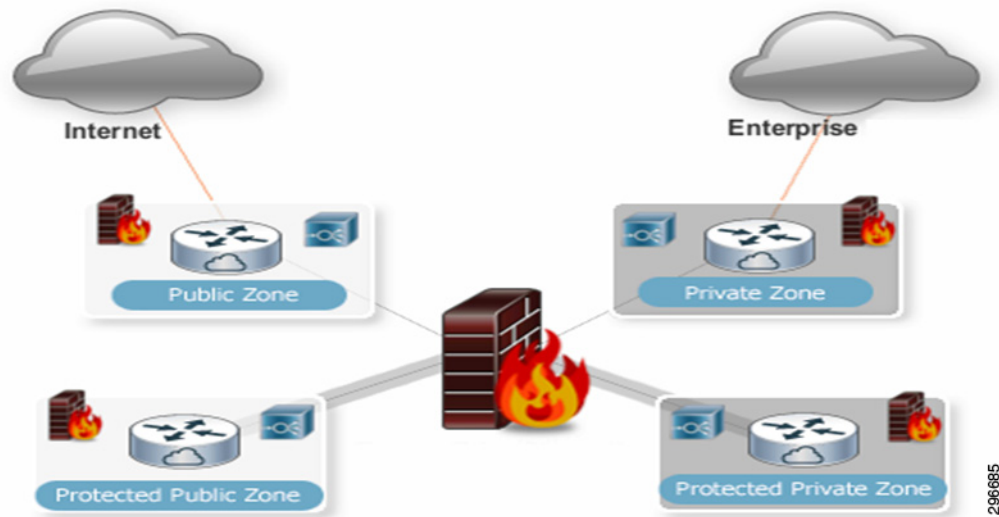
This container includes two Private security zones (Unprotected Private and Protected Private), enhanced VM security, and LB services. This container is suitable for Tenant clients located only in the Enterprise network.

**Figure 2-15 Two-Zone Gold Private (Enterprise) Container****Two-Zone Gold Private (Enterprise) Container**

- Routing (BGP) on the CSR 1000V to connect the Tenant VDC to the Enterprise connected router
- Access from Enterprise to the Tenant container (VDC)
- Two zones - Protected Private and Unprotected Private - to place workloads. Each zone has its own VLAN segments.
- ZBF on the CSR 1000V to provide Inter-zone firewall services to protect the Tenant workloads
- SLB on the Citrix VPX, to provide L4-7 LB and SSL-Bridging services to Tenant workloads.
- Compute firewall on the VSG to provide Inter-VLAN and Intra-VLAN security service to the Tenant VMs

**Four-Zone Gold Container**

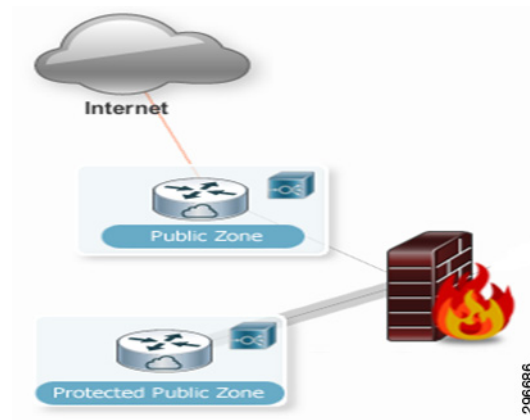
A Four-Zone Gold Container requires that the connection type be both when onboarding a Tenant. This container includes four security zones (Unprotected Public, Protected Public, Unprotected Private, and Protected Private), enhanced VM security, and LB services. This container is suitable for clients located both in the Enterprise and Internet.

**Figure 2-16 Four-Zone Gold Container****Four-Zone Gold Attributes**

- Routing (BGP) on the CSR 1000V to connect the Tenant VDC to the Service Provider WAN router and to the Enterprise connected router
- Access from Internet and from the Enterprise to the Tenant container (VDC)
- Four zones - Protected Public, Unprotected Public, Protected Private and Unprotected Private - to place workloads. Each zone has its own VLAN segments.
- ZBF on the CSR 1000V to provide Inter-zone firewall services to protect the Tenant workloads
- NAT on the CSR 1000V to provide static and dynamic NAT services to RFC1918 addressed VMs on the Protected Public Zone
- SLB on the Citrix VPX, to provide L4-7 LB and SSL-Bridging services to Tenant workloads
- Compute firewall on the VSG to provide Inter-VLAN and Intra-VLAN security service to the Tenant VMs

**Silver Network Containers****Two-Zone Silver Internet**

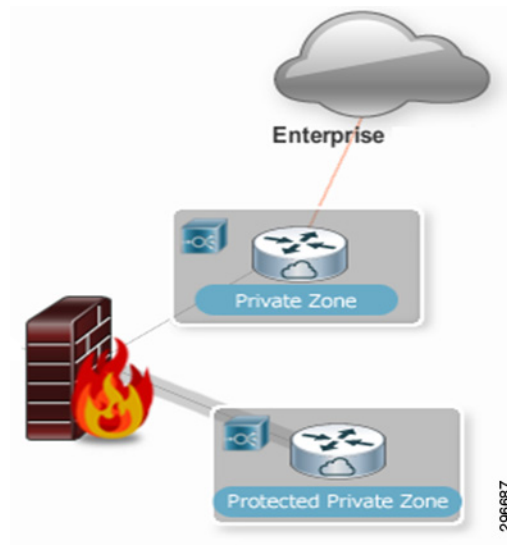
This container includes two security zones (Unprotected Public and Protected Public), enhanced VM security, and optional LB services. This container is suitable for Tenant clients located only in the Internet.

**Figure 2-17 Two-Zone Silver Internet Container****Two-Zone Silver Internet Attributes**

- Routing (BGP) on the CSR 1000V to connect the Tenant VDC to the Service Provider WAN router
- Access from Internet to the Tenant container (VDC)
- Two zones - Protected Public and Unprotected Public - to place workloads. Each zone has its own VLAN segments.
- ZBF on the CSR 1000V to provide Inter-zone firewall services to protect the Tenant workloads
- NAT on the CSR 1000V to provide static and dynamic NAT services to RFC1918 addressed VMs
- Compute firewall on the VSG to provide Inter-VLAN and Intra-VLAN security service to the Tenant VMs
- Optional: SLB on the Citrix VPX to provide L4-7 LB and SSL-Bridging services to Tenant workloads

**Two-Zone Silver Enterprise**

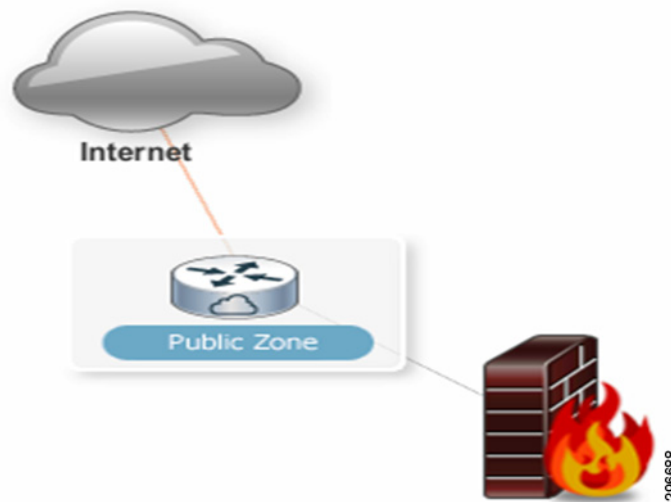
This container includes two security zones (Unprotected Private and Protected Private), enhanced VM security, and optional LB services.

**Figure 2-18 Two-Zone Silver Enterprise Container****Two-Zone Silver Enterprise Attributes**

- Routing (BGP) on the CSR 1000V to connect the Tenant VDC to the Enterprise connected router
- Access from Enterprise to the Tenant container (VDC)
- Two zones - Protected Private and Unprotected Private - to place workloads. Each zone has its own VLAN segments.
- ZBF on the CSR 1000V to provide Inter-zone firewall services to protect the Tenant workloads
- Compute firewall on the VSG to provide Inter-VLAN and Intra-VLAN security service to the
- Tenant VMs
- Optional: SLB on the Citrix VPX to provide L4-7 LB and SSL-Bridging services to Tenant workloads

**Bronze Network Containers****One-Zone Bronze Internet**

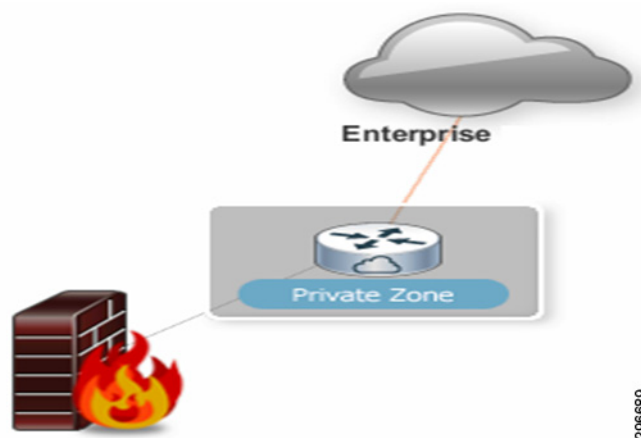
This container includes one security zone, which is an Unprotected Public zone. This container is suitable for Tenant clients located only in the Internet network.

**Figure 2-19 One-Zone Bronze Internet Container****One-Zone Bronze Internet Attributes**

- Routing (BGP) on the CSR 1000V to connect the Tenant VDC to the Service Provider WAN router
- Access from Internet to the Tenant container (VDC)
- A single zone - Unprotected Public - to place workloads

**One-Zone Bronze Enterprise**

This container includes one security zone, which is an Unprotected Private zone. This container is suitable for Tenant clients located only in the Enterprise network.

**Figure 2-20 One-Zone Bronze Enterprise Container****One-Zone Bronze Enterprise Attributes**

- Routing (BGP) on the CSR 1000V to connect the Tenant VDC to the Enterprise connected router
- Access from Enterprise to the Tenant container (VDC)

- A single zone - Unprotected Private - to place workloads

### Other Container

For added flexibility, there is an “Other” option when creating a VDC. The number of networks and the zone types are options that are provided in the drop-down menus. There is a maximum of four networks. The zone types are based on options selected when creating the Tenant and Org. If a Tenant and Org are created with the connection type of Both, then all four possible zones are provided as an option in the drop-down menu. When using this option, a VDC can be created with four networks all in the same zone, or with four networks all in different zones, similar to a Four-Zone Gold container.







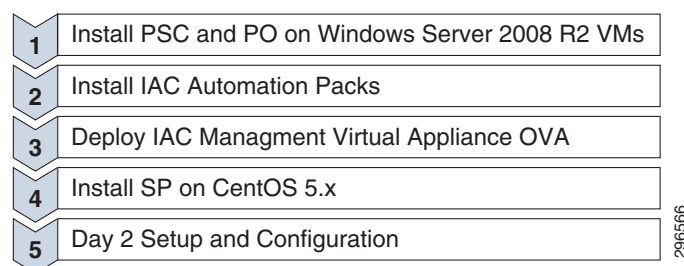
# Solution Implementation

## Installation Overview

This chapter provides a high-level overview of the Cisco Intelligent Automation for Cloud (IAC) 4.0 installation procedure, including the management components' logical and physical layout. [Table 3-1](#) provides a planning guide that indicates the key parameters to be considered before beginning installation. The planning guide also has the values for those parameters chosen for the testing deployment. This chapter does not cover the step-by-step installation of the solution. For that level of installation guidance, refer to the IAC documentation listed in Appendix A, [Related Documents](#).

The main components of the IAC stack are the Cisco Prime Service Catalog (PSC), Cisco Process Orchestrator (PO), IAC Automation Packs, IAC Management Appliance, and the Cisco Server Provisioner (SP). After the prerequisites (VMware infrastructure, Cisco Prime Network Services Controller (PNSC), Nexus 1000V, Active Directory (AD)) are set up, the IAC components can be installed.

**Figure 3-1** High-Level View of Installation



296566

## Planning Guide

Use [Table 3-1](#) to plan your set up. The table is based on the sample values used in preparation of this document. It has a few details about the network prerequisites, IP subnets, and VLANs used. It also has IP addresses and login information of IAC components, vCenter, PNSC, MS SQL, AD, Nexus 1000V, and the edge ASR router. You might see these values referenced across the document and in various screen shots. The table provides an overview of the management components and sets a context for the physical and logical component diagrams.

Table 3-1 Planning Guide

Parameter	Value Used in this Document	Purpose	Your Values
Mgmt VLAN	7	Mgmt Network	
Mgmt Subnet	192.168.7.0/24	Mgmt Network	
Mgmt Default GW	192.168.7.97/24	Mgmt Network	
CIMC VLAN	7	C-series initial configuration	
CIMC IP Address	192.168.7.114/24	C-series initial configuration	
CIMC Default GW	192.168.7.97	C-series initial configuration	
Data VLAN for Uplink	100	Service Network	
Mgmt Server ESXi Mgmt IP Address	192.168.7.113/24	vSphere infrastructure	
Mgmt Server ESXi Login	root/Cisco12345	vSphere infrastructure	
vCenter Virtual Appliance	192.168.7.241/24	vSphere infrastructure	
vCenter Virtual Appliance Account/Password	root/vmware	vSphere infrastructure	
Cisco Service Catalog	192.168.7.181/24	IAC portal	
Cisco Service Catalog Login	admin/Cisco12345	IAC portal	
Cisco Process Orchestrator	192.168.7.182/24	IAC automation engine	
Cisco Process Orchestrator Login	administrator/Cisco12345	IAC automation engine	
SQL Server	192.168.7.183	IAC database server	
SQL Server Login	administrator/cisco	IAC database server	
Active Directory Server	192.168.7.242	IAC install requirement	
Active Directory Server Login	administrator/Cisco12345	IAC install requirement	
PNSC	192.168.7.246	Network domain manager	

Parameter	Value Used in this Document	Purpose	Your Values
PNSC Login	admin/Cisco12345	Network domain manager	
IAC Mgmt Appliance	192.168.7.247	Network discovery, software package repository	
IAC Mgmt Appliance Login	root/ Cisco12345	Network discovery, software package repository	
Pool of VLANs	600 - 750	Tenant VLAN resource pool. See the <a href="#">VLAN Pools</a> section for details.	
Pool of Private IP Addresses	192.168.0.0/16 172.16.0.0/12 10.0.0.0/8	Any of the three RFC 1918 ranges or a custom range - for Private IP and Private VIP addresses	
Pool of Public Addresses	64.100.0.0/16	Used for Public IP addresses, NAT, and Public VIP addresses	
Nexus 1000V-VSM Mgmt	192.168.7.100/24	Virtual Network Mgmt	
Nexus 1000V-VSM control0	Not configured	Virtual Network Mgmt	
Nexus 1000V-VSM L3 Control Port Profile	VLAN 74	Virtual Network Mgmt	
Nexus 1000V-VSM-VE M and VEM-VSG VLAN	VLAN 75	Virtual Network Mgmt	
Nexus 1000V-VSM Mgmt Account	admin/Cisco12345	Virtual Network Mgmt	
ASR 9010 Router Mgmt Account	admin/ Cisco12345	CSE PE Peer Mgmt	
ASR 9010 Router Gi1	192.168.7.72/24	CSE PE Peer Mgmt	

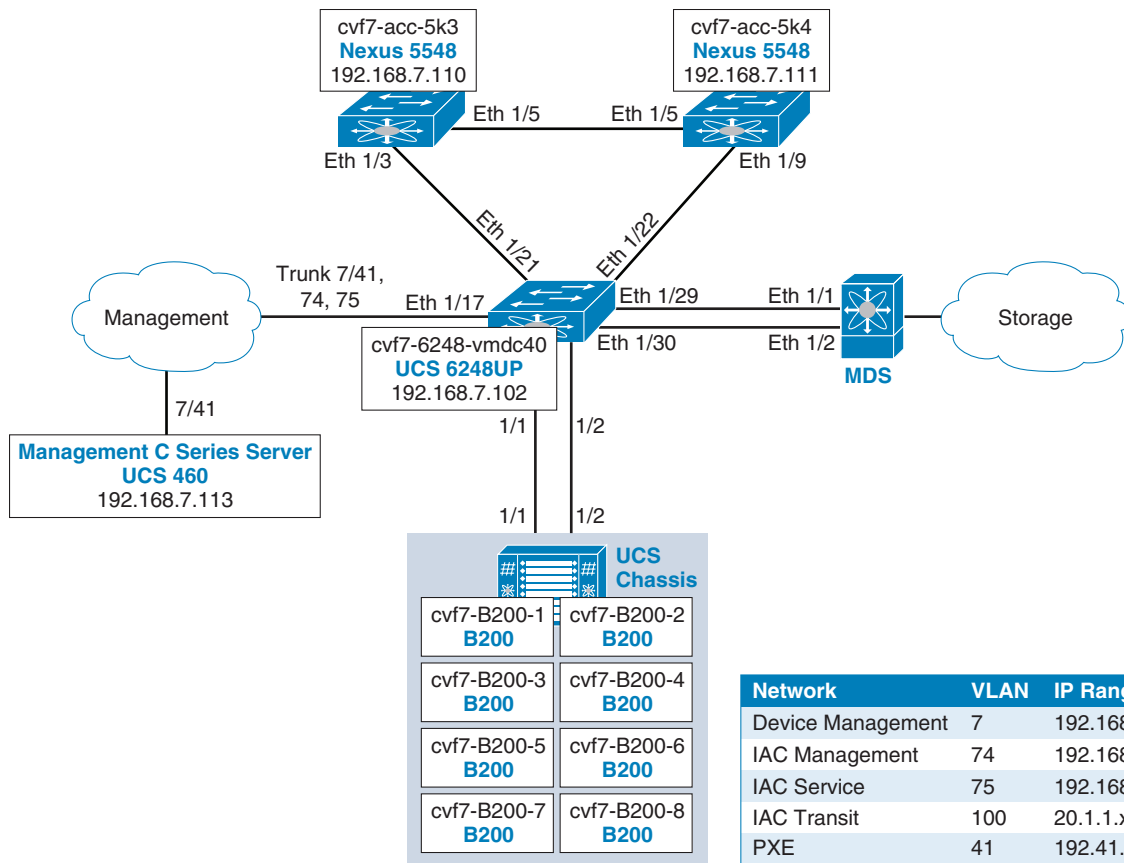
Parameter	Value Used in this Document	Purpose	Your Values
ASR 9010 Router Gi2	20.1.1.1/24	Link to Tenant1-CSR1000V	
ASR 9010 Router Gi2 VLAN	100	VLAN for CSR 1000V PE peering	
ASR 9010 Router Gi3	30.2.1.1/24	Internet clients	

## Physical Component Layout

This IAC deployment uses a Cisco Unified Computing System (UCS) C460 rack server to host all of the management components (vCenter/IAC Components/Nexus 1000V, etc.). The compute resource blades use a Cisco UCS 5108 chassis with four blade servers. This is connected to the UCS 6248 Fabric Interconnect (FI) for chassis management and both LAN and SAN connectivity. The 6248 FI and the C460 server connect to a Catalyst 4948 switch for management connectivity. The FI is connected to a pair of Nexus 5000 switches for Internet and Tenant Enterprise connectivity.

The CSR 1000V serves as a Tenant-specific router, using External Border Gateway Protocol (eBGP) to peer with the ASR 9000 data center Edge Routers. An L2 network exists between the CSR1000V and the ASR 9000 that consists of Nexus 5548 and Nexus 7009 switches.

[Figure 3-2](#) shows the way management/compute resource blades and the FI are tied into the topology.

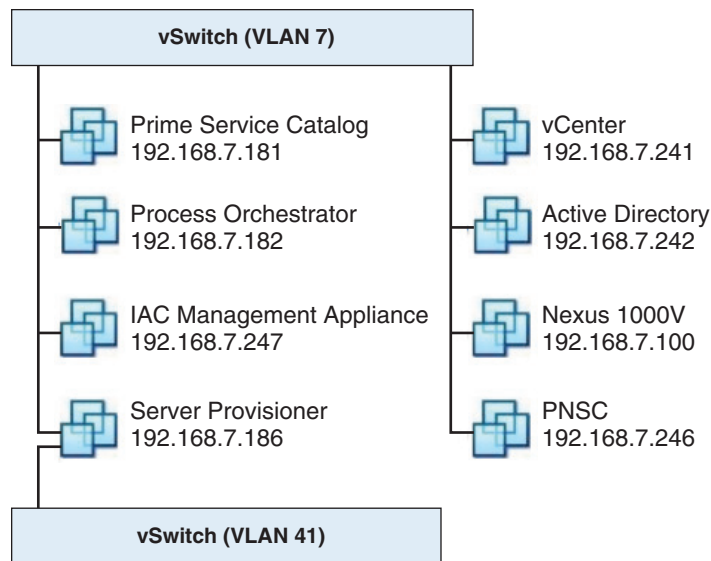
**Figure 3-2 Physical Component Layout**

296567

## Logical Component Layout

All IAC components are VMs on the management UCS C460 rack server. These components have IP addresses in the device management subnet (192.168.7.x). The SP has two NICs, with one on the management VLAN and the other on the PXE network that is dedicated for physical server provisioning.

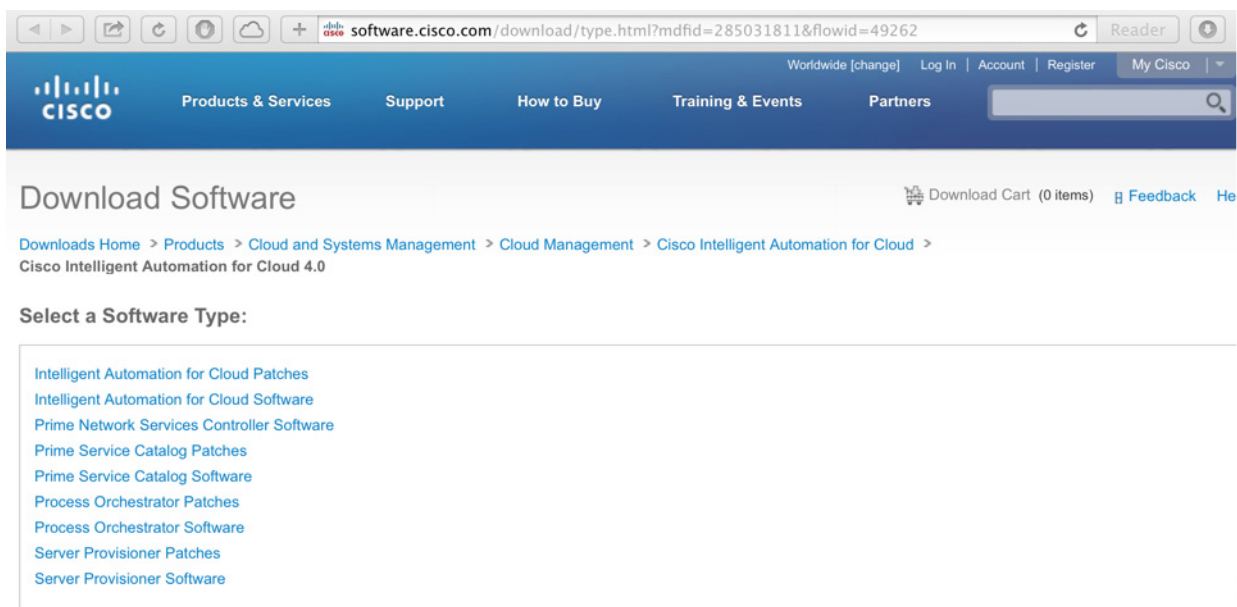
The testing setup uses the same vCenter for both management and production data centers. It is recommended to use separate instances in a customer deployment. They could be set up in a linked mode for operational convenience. Figure 3-3 shows the management components layout.

**Figure 3-3 Management Components Layout**

## IAC Component Installation Steps

The sequence of steps below provides an overview of the installation of IAC 4.0 in a VMware vSphere environment. You can download the four IAC components (PSC/PO/IAC/SP) from the following URL:

<http://software.cisco.com/download/type.html?mdfid=285031811&flowid=49262>

**Figure 3-4 Download Software Page**

- 
- Step 1** Prepare the compute infrastructure:.
- Install ESXi hypervisor on servers.
  - Install VMware vCenter.
  - Create a Windows OS Virtual Machine (VM) for each of the following components:
    - Active Directory
    - MS SQL
    - PO
    - PSC
- Step 2** Install prerequisite software:.
- Active Directory on Windows VM
  - MS SQL on Windows VM
  - NTP server
  - Nexus 1000V
- Step 3** Install Core IAC Orchestration Components (Day 0) (refer to the [IAC Installation Guide](#) for details).
- PSC on a Windows VM (make sure that the VM is on the AD domain before installing)
  - PO on a Windows VM (make sure the VM is on the AD domain for installation to succeed)
  - IAC Management Appliance from OVA file
  - PNSC from OVA file
  - SP (optional – for physical windows/Linux server provisioning)
  - Include any required patches for PSC or PO
- Step 4** Configure IAC (Day 1).
- PO Tidal Automation Packs (TAP)
  - Service Catalog components (refer to the [IAC Installation Guide](#) for details)
    - Install REX Adapter.
    - Extract RequestCenter war files.
    - Import IAC portal pages and catalogs.
  - IAC Configuration Wizard
- Step 5** Connect all cloud infrastructure components and create resource pods.

## IAC Scalability

### Scale Factors

Each individual component of IAC has a hardware sizing guide in the installation section. PSC suggests to have a minimum of three servers in a typical non-clustered environment. PO suggests a separate server for database, a separate high speed disk operating system, program files and swap files, and enough memory to avoid paging.

## Tuning for Scale and Performance

### PSC Server with JBoss Application Server

PSC uses two JBoss instances, RequestCenter and ServiceLink. When installing PSC and selecting the JBoss Application server, there are two options, a typical installation or advance installation. A typical installation places both JBoss instances on the same server, but these are not required to be on the same server. The JBoss instances can be placed on two separate servers, but the PSC interface needs to be on the server holding the RequestCenter.

If running PSC with WebLogic or WebSphere instead of JBoss both WebLogic or WebSphere can run in a cluster environment.

The web server does not need to reside on the same server as the application server. Using another server for the web server or using multiple web servers in front of a server load balancer helps with scale and performance, as well as offering some HA.

### PO Server

Multiple PO servers can be used to distribute the load. The PO is multi-threaded and uses as many CPUs/vCPUs cores as provided. Adding additional cores should be the first step when evaluating scale or performance issues on the PO server.

### Database Servers

There are multiple databases instances and they can be placed on different database servers. Database servers can be clustered for both performance and availability. Placing servers on individual servers rather than running them on VMs and ensuring not running multiple applications on the same servers. High speed disks and dedicated high speed management network should be used to increase scale and performance.

## IAC Redundancy

IAC has limited support for redundancy. The only IAC component that supports High Availability (HA) is the PO. The suggested method for redundancy is using VMware's HA capabilities.

## Redundant Components

The PO is the only component that directly supports High Availability (HA).



### Note

HA was not configured for any components during this test phase. For additional information on managing HA and resiliency for the PO, refer to Chapter 5 of the [Cisco Process Orchestrator User Guide](#).

The PSC can offer some additional HA protection by using multiple web servers combined with an SLB. The PSC can be used with WebLogic or WebSphere in a clustered environment.

The IAC Management Appliance is deployed as a single instance. Any outage only impacts initial networking infrastructure standup during creation and onboarding of new Organizations. In its other role, network discovery, an appliance outage is not time critical and does not block orders. IAC can continue to function using data from prior network discovery until the appliance is recovered.



# IAC Licensing

Licensing for IAC is applied to the PO server. CPO is installed with a 30 day trial license which enables full use of the product. Customers receive a Claim Certificate containing PAK keys and need to go through the standard Cisco licensing process from Global Licensing Operations (GLO). The license is node locked to the PO server.

Licenses need to be purchased and applied to each PO server in the case of multiple PO servers used for redundancy or scaling.

Refer to <https://tools.cisco.com/SWIFT/LicensingUI/Quickstart> or email [licensing@cisco.com](mailto:licensing@cisco.com) for more information.

## Licensing for Service Nodes

The CSR 1000V is installed with a temporary advanced license, which is active for 90 days. You need to obtain a permanent license after this period. The NetScaler VPX is installed without a license. This does allow for the VPX to be configured, but not all of the features function until a license is installed. The VSG does not require a separate license. The VSG license is installed as part of the Nexus 1000V license. The PNSC is licensed for managing the VSG, ASA for Nexus 1000V, CSR 1000V, and Citrix NetScaler VPX or 1000V when purchasing an IAC license.

# Pod Discovery and Onboarding

Pods are groups of network, compute, and storage components that work together to deliver services. The pod is a repeatable pattern, and its components increase the modularity, scalability, and manageability of data centers. You must be logged in as a Cloud Provider Technical Administrator to create pods. The two types of pods available on IAC are the Network pod and the Compute pod.

This section explains the prerequisites and the procedure to create these pods. Below is a high level overview of the process. They are explained in more detail in the following sections:

1. Deploy and register the Linux XMP appliance for network discovery.
2. Discover the network devices.
3. Register the Nexus 1000V.
4. Register a network pod.
5. Connect vCenter and UCSM as cloud infrastructure components.
6. Register a Compute pod.

## Network Pod

### Discovering Network Devices

IAC performs network discovery, inventory, and topology (device interconnection) as a function of the IAC Management Appliance. It uses the eXtensible Metadata Platform (XMP), which is the standard used by IAC to gather data about network resources. This VM is deployed from the provided IAC virtual appliance OVA file. This appliance is initially added as an infrastructure component on IAC in step 3 of the Day 1 configuration wizard. This step needs to be completed by the CPTA.

Figure 3-5 shows step 3 of the configuration wizard.

**Figure 3-5 Step 3 of the Configuration Wizard**

29/05/09

After the IAC Management Appliance is connected, the network devices are discovered in step 4 in the configuration wizard. Change the Discovery Type to “Neighbor Discovery.” Provide the host name/IP address of a device in the topology as the “seed device.” All of the seed’s neighboring devices, including the Nexus 1000, should be discovered. IAC uses SNMP and SSH details in the discovery procedure. You should have them pre-configured. Add the details in the form and submit the order, as shown in [Figure 3-6](#).

**Figure 3-6 Discover Network Devices**

Discover Network Devices

Discovers devices on the network.

Discover Network Devices

Discovery Type: Neighbor Discovery Please select a value to perform the discovery of the infrastructure.

\* Seed Device: 192.168.7.100 Enter a seed device for Nexus 1000v.

Note : Select at least one SNMP v3 or SNMP v2 Credentials.

SNMP V3 Credentials					
SNMPV3User	Security Level	Authentication Protocol	Authentication Password	Privacy Protocol	Privacy Password
admin	authPriv	MD5	*****	DES	*****

SNMP V2 Credentials	
R0 Community	RW Community

SSH Credentials		
* SSH User	* SSH Password	* Enable SSH Password
admin	*****	*****

Continue to the second part of step 4 in the configuration wizard and register the Nexus 1000V discovered from the earlier step, as shown in [Figure 3-6](#) and [Figure 3-7](#). Note that in “Network Device” drop-down menu on the form, you need to select the Nexus 1000V’s IAC generated unique name. If you do not find the Nexus 1000V listed, then try repeating the previous discovery process. Change the “Device Role” to “Virtual Access Switch.”

**Note**

In the form, make sure to select the appropriate vNICs as updating vNIC templates. When Tenant networks are created, those VLANs are added to the vNICs selected here. The list of vNICs that are displayed is fetched from the available vNIC templates on UCSM. This validation uses the data vNIC template that was created manually on the UCSM earlier (see [Figure 3-7](#) and [Figure 3-8](#)).

**Figure 3-7 Register the Nexus 1000V as the Virtual Access Switch – Part 1**

**Connect Cloud Infrastructure**

Register and connect the various platform elements to be used for the cloud. This setup must be completed before any further setup or usage of the cloud environment can take place.

**Network Devices**

Network Device: 192.168.7.100\*192.168.7.100\*1.3.6.1.4.1.9.12.3.1.3.840 Select the Network Device Unique Name from the drop-down list.

IP Address: 192.168.7.100

Hostname: 192.168.7.100

System Object ID: 1.3.6.1.4.1.9.12.3.1.3.840

System Name: cvf-n1k-vsm

System Description: Cisco NX-OS(bn) nexus Software (nexus-1000v) Version 4.2(1)SV2(2.1a)  
RELEASE SOFTWARE Copyright (c) 2002-2009 by Cisco Systems Inc. Device  
Manager Version nms.sro not found Compiled 9/28/2013 17:00:00

Device Role: ☐ Edge Router  
☐ Layer 2 Aggregation Switch  
☐ Layer 2 Aggregation/Fire Channel Switch  
☐ Layer 3 Aggregation Switch  
☐ Layer 3 Services  
☐ UCS Manager  
☒ Virtual Access Switch

Note: A device can have only one role. If multiple roles are specified, the automated network provisioning processes will not configure this device.

Friendly Name: cvf-n1k

Credentials: false SSH Account to connect to the Device.

Administrator Username: admin

Cisco Prime Network Services Controller: 192.168.7.246 Select Cisco Prime Network Services Controller.

UCS Manager: 192.168.7.102 Select the UCS Manager instance that this VSM will be located under.

296692

**Figure 3-8 Register the Nexus 1000V as the Virtual Access Switch - Part 2**

Updating vNIC templates: ... Select the updating vNIC templates that will be updated when new networks are added.

org-rootlan-conn-templ-data  
org-rootlan-conn-templ-management

**Administrator Password**

Password: ..... Enter the password to use when connecting to the platform element.

Re-Enter Password: ..... Enter the password again.

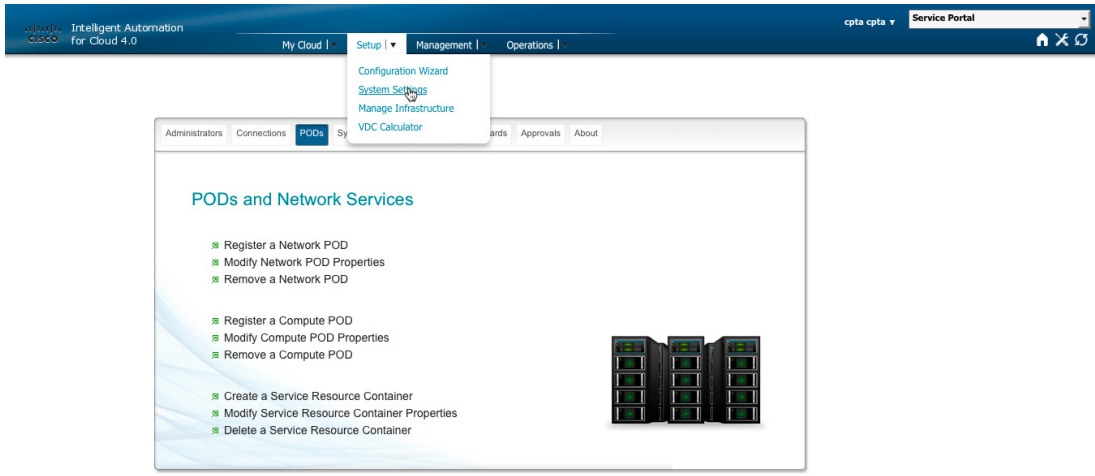
Network Interconnections		
Local Interface	Peer Device	Peer Interface

296693

This completes the network discovery process. Verify that all devices in the topology are discovered at this point by checking the list of discovered devices under Setup > Manage Infrastructure > Network Elements > Network Devices. If any devices are missing, then try discovering them again, maybe with a different seed. The next section discusses creating / onboarding a new Network pod once all of the devices are discovered.

## Register/Create a Network Pod

Creating a Network pod can initially be done in step 5 of the configuration wizard. Any additional network pods can be created from Setup > System Settings > Pods > Register a Network Pod (see [Figure 3-9](#)). You must be logged in as a CPTA to create a network pod.

**Figure 3-9 Register a Network Pod Form**

In the creation form, select the devices in the various categories (Access, Aggregate, Edge, etc.) that you want to be grouped into a Network pod and submit the order, as shown in [Figure 3-10](#). For more details on VLAN pools and recommended pool size, see the [VLAN Pools](#) section.

**Figure 3-10 Create Network Pod Form**

The screenshot shows the 'Create Network POD' form. The form includes the following fields and options:

- Network POD Name:** cvf7-NetworkPod-3
- Description:** (Empty text area)
- VLANPool:** 2000- 2311, 2313- 3000
- Edge Router:** 192.168.7.76
- Layer 3 Aggregate Switch:** (Empty dropdown)
- Layer 3 Service Node:** (Empty dropdown)
- Layer 2 Aggregate Switch:** 192.168.7.98, 192.168.7.99, 192.168.7.110, 192.168.7.86
- UCS Fabric Interconnects:** (Empty dropdown)
- Virtual Access Switch:** 192.168.7.100, 192.168.7.29

At the bottom right, there are 'Submit Order' and 'Reset' buttons.

# Compute Pod

## Discovering Compute Infrastructure

IAC discovers the available compute blade resources when a UCSM is connected as an infrastructure element from Setup > System Settings > Connections > Connect Cloud Infrastructure. [Figure 3-11](#) shows the form for registering the UCSM. Provide the IP address and the access credentials for the UCSM. Make sure to select the correct port and connection type. If you chose to use a secure connection, but the UCSM has an invalid/self-signed SSL security certificate., then set the “Ignore certificate error” option to “True.”

**Figure 3-11 Register the UCSM Form**

**Connect Cloud Infrastructure**

Register and connect the various platform elements to be used for the cloud. This setup must be completed before any further setup or usage of the cloud environment can take place.

**Select Platform Element Type**

Platform Element Type:  Choose the type of platform element that you would like to connect to.

**Connect Cisco UCS Manager**

\* Host Name:  Enter the host name or IP address of the Cisco UCS Manager.

\* Port:  Enter the TCP/IP port used to connect to the Cisco UCS Manager.

Description:  Enter a description for this Cisco UCS Manager.

\* Time Zone:  Enter the time zone of the Cisco UCS Manager.

Secure connection: ☒ True ☐ False Determines if communication is secured.

Ignore Certificate Error: ☒ True ☐ False Determine whether SSL certificate errors should be ignored.

Managed by Cisco UCS Director: ☐ True ☒ False

\* User Name:  Enter the account name to use when connecting for the platform element.

**Administrator Password**

\* Password:  Enter the password to use when connecting to the platform element.

\* Re-Enter Password:  Enter the password again.

After the requisition completes, the discovered blades can be viewed from Setup > Manage Infrastructure > Cisco UCS Manager. If any of those blades have a service profile associated to them then they are marked as “in-use” by IAC. [Figure 3-12](#) shows the discovered UCS blades.

Figure 3-12 UCS Blades

UCS Blades

UCS Manager	Server Name	Model	Number of...	Number of...	Total Memory...	Status	Pool Type
192.168.7.102	sys/chassis-1/blade-8	UCSB-B200-M3	16	2	98304	Discovered	Physical
192.168.7.102	sys/chassis-1/blade-2	UCSB-B200-M3	16	2	98304	Discovered	None
192.168.7.102	sys/chassis-1/blade-1	UCSB-B200-M3	16	2	98304	Discovered	None
192.168.7.102	sys/chassis-1/blade-3	UCSB-B200-M3	16	2	98304	Discovered	None
192.168.7.102	sys/chassis-1/blade-4	UCSB-B200-M3	16	2	98304	Registered	Physical
192.168.7.102	sys/chassis-1/blade-5	UCSB-B200-M3	16	2	98304	Registered	Physical
192.168.7.102	sys/chassis-1/blade-6	UCSB-B200-M3	16	2	98304	Registered	Physical
192.168.7.102	sys/chassis-1/blade-7	UCSB-B200-M3	16	2	98304	Registered	Physical

296575

## Register/Create a Compute Pod

The CPTA can onboard new Compute pods from Setup > System Settings > Pods > Register a Compute Pod, as shown in [Figure 3-13](#).

**Figure 3-13 Create Compute Pod**

**Create Compute POD**

Use this service to register an installed compute POD (Point Of Delivery) and select the cloud infrastructure platform elements that manage its resources.

**POD Details**

<p>★ Compute POD Name: <input type="text" value="&lt;name&gt;"/></p> <p>Description: <input type="text"/></p> <p>★ Cloud Infrastructure Type: <input type="text" value="VMware vCenter Server"/></p> <p>Network POD Name: <input type="text" value="CVF7-NetworkPod-3"/></p> <p>★ VMware vCenter Instance: <input type="text" value="192.168.7.241"/></p> <p>★ VMware Datacenter: <input type="text" value="vmdc40-cluster-3"/></p> <p>Cisco UCS Manager Instance: <input type="text" value="192.168.7.102"/></p> <p>Cisco Server Provisioner: <input type="text" value="192.168.7.186"/></p> <p>★ Provisioning UCS VLAN: <input type="text" value="vian41-pxe"/></p> <p>★ Provisioning Hypervisor VLAN: <input type="text" value="vian41"/></p>	<p>Enter a new short name for the Compute POD.</p> <p>Enter a full description of the Compute POD.</p> <p>Select Cloud Infrastructure Type.</p> <p>Select the Network POD instance that serves in this POD.</p> <p>Select the vCenter instance that controls hypervisor hosts in this POD.</p> <p>Select the vCenter datacenter that contains the hypervisor hosts in this POD.</p> <p>Select the UCS Manager instance that controls the servers in this POD.</p> <p>Select the Cisco Server Provisioner instance that serves in this POD.</p> <p>Select the UCS VLAN that will serve as a physical server bare-metal provisioning network for Cisco Server Provisioner in this POD.</p> <p>Select the hypervisor VLAN that will serve as a VM bare-metal provisioning network for Cisco Server Provisioner in this POD.</p>
--	--

296577

Multiple compute pods can use the same attributes seen in [Figure 3-13](#), including the Network pod.

Data centers need to be created on the vCenter before creating a Compute pod. The drop-down menu in this form is populated by entities discovered when the vCenter is connected as a Cloud Infrastructure component. If the required data center is not found in the list, run Setup > Manage Infrastructure > VMware vCenter Server > Data Centers > Discover Data Centers.

If an SP instance is chosen, then specify a UCS VLAN and a Hypervisor VLAN for the PXE network. These attributes are used to identify the network to use for Windows/Linux physical server provisioning or ordering VMs and installing Windows/ Linux from ISOs instead of the available VM templates.

## Management Components

### vCenter

The vCenter is an integral entity in this IAC deployment. It is used to deploy the virtual infrastructure entities including the IAC components, Tenant VMs, and Tenant virtual services like the CSR 1000V/VSG/VPX. VMware vCenter v5.1 is used in this release.

vCenter is connected to the IAC stack in Step 3 of the configuration wizard, as shown in [Figure 3-14](#).



**Figure 3-14**      **Connect vCenter to the IAC Stack**

**Connect Cloud Infrastructure**

Register and connect the various platform elements to be used for the cloud. This setup must be completed before any further setup or usage of the cloud environment can take place.

---

**Select Platform Element Type**

Platform Element Type: VMware vCenter Server Choose the type of platform element that you would like to connect to.

---

**Connect VMware vCenter Server**

\* Host Name:  Enter the host name or IP address of the VMware vCenter Server.

\* Port: 443 Enter the TCP/IP port used to connect to the VMware vCenter Server.

Description:  Enter a description for this VMware vCenter Server.

\* Secure Connection: ☒ True ☐ False Determines if communication is secured.

Ignore Certificate Error: ☒ True ☐ False Determine whether SSL certificate errors should be ignored.

Managed by Cisco UCS Director: ☐ True ☒ False

\* User Name:  Enter the account name to use when connecting for the platform element.

---

**Administrator Password**

\* Password:  Enter the password to use when connecting to the platform element.

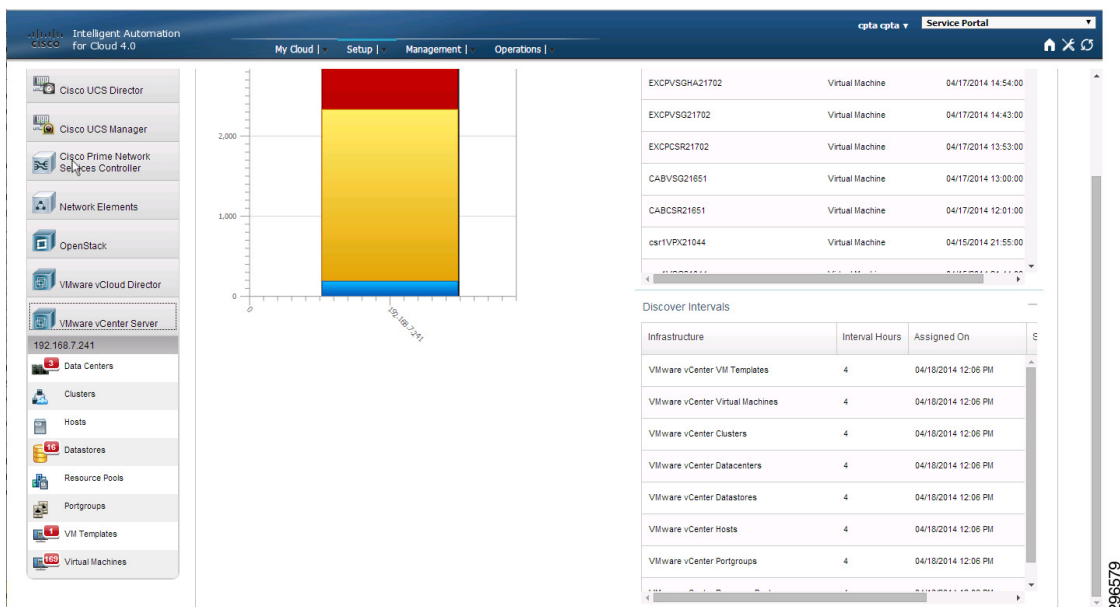
\* Re-Enter Password:  Enter the password again.

Submit Order Reset

296578

Make sure to select the correct port and connection type. If you chose to use a secure connection, but the vCenter has an invalid/ self-signed SSL security certificate, then set the “Ignore certificate error” option to “True.” This validation uses a standalone vCenter that is not managed by a UCS Director, so the “Managed by Cisco UCS Director” option is set to “False.”

This process discovers all existing data centers/clusters/VM templates/datastores, etc. These discovered entities can be seen from Setup > Manage Infrastructure > VMware vCenter Server (see [Figure 3-15](#)).

**Figure 3-15** *Discovered Entities*

## PNSC

Cisco's Prime Network Services Controller (PNSC) provides centralized multi-device and policy management for network virtual services. IAC uses PNSC to automate network configuration processes of the CSR 1000V and VSG. In this release, the PNSC does not automate configuration of the Nexus 1000V or VPX. Both are configured directly by IAC via CLI/API.

PNSC v3.2 (1d) was used in this release. Connecting the PNSC to the IAC stack is similar to the vCenter connection. It is registered in Step 3 of the configuration wizard (see [Figure 3-16](#)).

**Figure 3-16** *Connect PNSC to the IAC Stack*

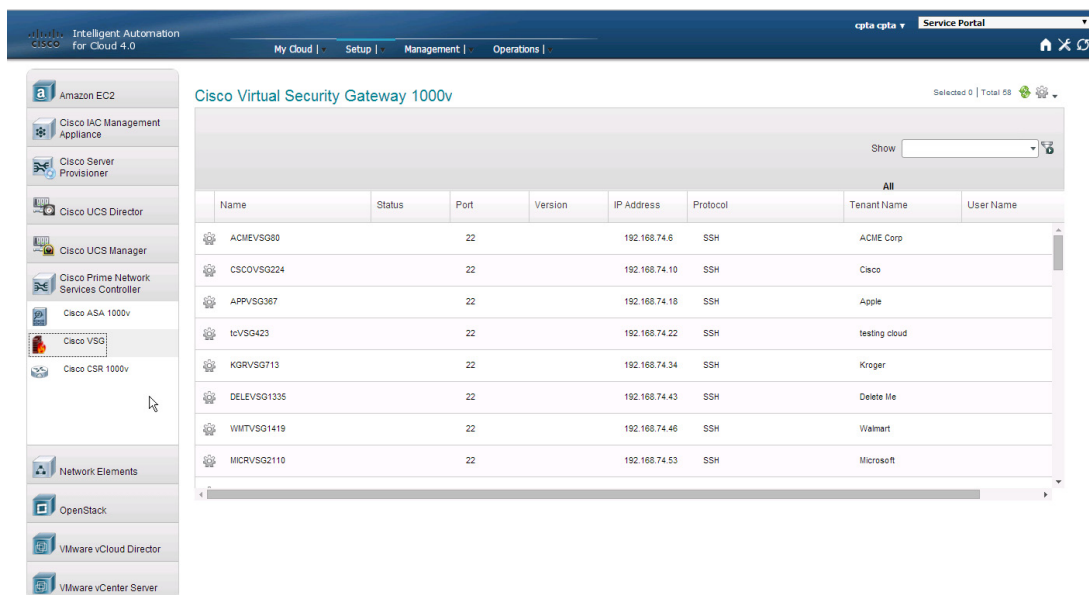
Make sure to select the correct port and connection type. If you chose to use a secure connection, but the PNSC has an invalid/ self-signed SSL security certificate, then set the “Ignore certificate error” option to “True.”

PNSC supports multi-tenancy management of virtual service, and each Tenant Organization’s CSR 1000V and VSG instances are put in their own specific Org Structures in PNSC, as shown in [Figure 3-17](#).

**Figure 3-17** *PNSC Multi-Tenancy*

Name	Type	Instantiation	Management IP	Primary/ Standalone Status	Secondary Status	Placement	Description
NXCSR10413	Edge Router	No	192.168.76.170	running	n/a	Enterprise	
NXVSG10413	Compute Firewall	No	192.168.76.171	running	n/a	Enterprise	

Discovered PNSC elements can also be seen from Setup > Manage Infrastructure > Cisco Prime Network Services Controller, as shown in [Figure 3-18](#).

**Figure 3-18** PNSC Elements

296582

## Network Types

The system has three important types of networks that need to be added during the Day 1 configuration. These networks are considered as “Infrastructure” networks. Table 3-2 shows the network types.

**Table 3-2** Network Types

Network	Role
Mgmt Network	This network contains the Management IP address of CSR 1000V, VSG and VPX virtual devices instantiated by IAC. The management network should be reachable from an IAC server to a UCS Blade server vNIC.
Service Network	This network contains the data interfaces of all VSGs created by IAC. This network should be reachable from the VSG data interface to the VSM management IP address.
Internet-Facing Network	This network represents the Transit VLAN used for Internet connectivity from the CSR 1000V. This VLAN is shared with all other Tenants created by IAC and the ASR 9000.

Port profiles on the Nexus 1000V and VLANs on the 6248 FI need to be created for these networks before they can be added in IAC. To add networks, select Setup > System Settings > Networks > Add a Network. [Figure 3-19](#) shows a sample form. You must complete the form once for each network and then submit three orders.



### Note

- Change the Cloud Infrastructure Type to be VMware vCenter Server.
- Change Community Network = No and Public Network = Yes.
- Change Network Type = Infrastructure and Network Source = Internal

For more details on network source, see the [IPAM](#) section.

**Figure 3-19      Add Network Form**

## Add Network

Define a VLAN and subnet to select in the cloud system, user servers, server management, or the cloud infrastructure services.

POD Information

Cloud Infrastructure Type:

VMware vCenter Server

Select the Cloud Infrastructure Type.

Network Information

Network Name:

Enter a short name for the network that will be shown to users in drop-down selection lists.

Subnet Address Specification:

Enter the network for this subnet in CIDR notation. For example, 192.168.20.0/24. Enter only an IPv4 type of IP address. Note: Only networks from /23 through /29 are supported.

Community Network:

No

Choose the network access scope for user networks. A community network is available to users in shared zones. Non-community networks require explicit VDC level access to be set before users can deploy servers to it, which can be useful for traffic isolation and better security.

Public Network:

Yes

Specify the duplication policy for this network. Public networks are globally unique, while private networks must only be unique within associated network device contexts.

Network Type:

---

Choose a network type to determine how this network can be used. User networks are used for deploying virtual machines or physical servers. Management networks are used for management access to cloud servers. Infrastructure networks are used for management interfaces of hypervisor hosts and other infrastructure devices.

Network Source:

---

Select how IP addresses management is done in this network: Internally by Cisco IAC, or via an external IP management tool.

vCenter Portgroups:

vCenter Portgroups			
Portgroup Name	Host Name	Network Path	VMware vCenter Server
<input type="checkbox"/> dummy	192.168.7.171	IAC-clients/dummy	192.168.7.241
<input type="checkbox"/> enterprise-facing-103	192.168.7.172	IAC-clients/enterprise-facing-103	192.168.7.241
<input type="checkbox"/> IAC-CLIENT1	192.168.7.171	IAC-clients/IAC-CLIENT1	192.168.7.241
<input type="checkbox"/> IAC-CLIENT2	192.168.7.171	IAC-clients/IAC-CLIENT2	192.168.7.241
<input type="checkbox"/> IAC-CLIENT3	192.168.7.171	IAC-clients/IAC-CLIENT3	192.168.7.241
<input type="checkbox"/> IAC-CLIENT4	192.168.7.171	IAC-clients/IAC-CLIENT4	192.168.7.241
<input type="checkbox"/> INTERNET	192.168.7.171	IAC-clients/INTERNET	192.168.7.241
<input type="checkbox"/> internet-facing-101	192.168.7.172	IAC-clients/internet-facing-101	192.168.7.241
<input type="checkbox"/> Management Network	192.168.7.172	IAC-clients/Management Network	192.168.7.241
<input type="checkbox"/> Management Network	192.168.7.171	IAC-clients/Management Network	192.168.7.241

UCS VLAN:

UCS VLAN			
VLAN Name	UCS Distinguished Name	Cisco UCS Manager	
<input type="checkbox"/> A507_Ent_a5d10	fabric/lan/net-A507_Ent_a5d10	192.168.7.106	
<input type="checkbox"/> A507_Ent_abea5	fabric/lan/net-A507_Ent_abea5	192.168.7.106	
<input type="checkbox"/> A507_Ent_c8b4	fabric/lan/net-A507_Ent_c8b4	192.168.7.106	
<input type="checkbox"/> A507_Ent_db215	fabric/lan/net-A507_Ent_db215	192.168.7.106	
<input type="checkbox"/> APP_616	fabric/lan/net-APP_616	192.168.7.102	
<input type="checkbox"/> APP_618	fabric/lan/net-APP_618	192.168.7.102	
<input type="checkbox"/> APP_619	fabric/lan/net-APP_619	192.168.7.102	
<input type="checkbox"/> APP_653	fabric/lan/net-APP_653	192.168.7.102	
<input type="checkbox"/> APP_654	fabric/lan/net-APP_654	192.168.7.102	
<input type="checkbox"/> APP_705	fabric/lan/net-APP_705	192.168.7.102	

Subnet Mask:

Enter the subnet mask resulting from the network prefix entered above.

Gateway Address:

Enter the default gateway for this network or keep the suggested value. This address will be excluded from allocation to any server deployed by this system. This address will be assigned as the default gateway for servers deployed on this network.

FHRP1 Address:

Enter the FHRP (First Hop Redundancy Protocol) gateway 1 network address or keep the default value. This IP address will not be assigned to any server deployed by the system.

FHRP2 Address:

Enter the FHRP gateway 2 network address or keep the default value. This IP address will not be assigned to any server deployed by the system.

Broadcast Address:

Enter the broadcast network address or keep the default value. This IP address will not be assigned to any server deployed by the system.

Primary DNS:

Enter the primary DNS address for servers on this network. This IP address will not be assigned to any server deployed by the system.

Secondary DNS:

Enter the secondary DNS address for servers on this network. This IP address will not be assigned to any server deployed by the system.

Submit Order

# Resource Pools

## VLAN Pools

VLAN pools are created during Network pod registration and is associated to that particular pod. The VLAN IDs from this pool are used for all networks created in any Tenants/Org VDC that is bound to the Network pod. The created pool is global and a per-tenant pool creation is not needed. Every Org under a Tenant can use up to eight of these VLAN IDs.

**Note**

A good VLAN pool size estimate is eight times the number of Orgs expected to be created using that Network pod.

Figure 3-20 shows the Create Network pod form.

**Figure 3-20** Create VLAN Pools

### Create Network POD



Use this service to register a Network POD (Point Of Delivery) and select the Device Roles for that POD.

#### Network POD

★

Network POD Name:

Enter a new short name for the Network POD.

Description:

Enter a full description of the Network POD.

★

VLAN Pool

VLAN numbers may be comma-separated (,), hyphenated-range (-) or combination of both.

296584

## IP Subnet Pools

There are two types of IP address pools available for Tenants – Public and Private.

### Private Pool

This pool is assigned at Tenant onboarding. The CPTA decides which of the three available RFC 1918 addresses is assigned to the Tenant depending on the Tenant's IP address requirements/expected scale. The CPTA could also choose to input a custom IP address range for a Tenant by choosing "Other" from the drop-down menu (see Figure 3-21).

**Figure 3-21 Available Private IP Subnet Pools for a Tenant**

**Onboard Tenant**

Define a new tenant of cloud users.

★ **Company Name:**  Enter the full name of the company.

★ **Company Abbreviation:**  Enter the company abbreviation. (Maximum 4 characters)

**Description:**  Enter the description.

★ **Run rate limit:**  Select the Quotas, this is used to determine the quotas for the tenant.

**Private Subnet:**    
 192.168.0.0/16  
 172.16.0.0/12  
 10.0.0.0/8  
 \*\*Other\*\*

296695

## Public Pool

A Public IP subnet is assigned to a Network pod by the CPTA to provide a collection of available, Public IP addresses to be used for assignment to singular servers as either floating or VIP addresses. These IP addresses are also assigned to the Public interface and Public VIP address of the CSR 1000V and VPX respectively. These addresses are available to all Tenants whose Compute pods are linked to that Network pod. [Figure 3-22](#) shows how to add a Public IP subnet to a Network pod.

**Figure 3-22 Add Public Subnet to Network Pod**

**Add Public Subnet to Network POD**

Select this service to add a new public subnet to the provider subnet pool.

★ **Subnet Address:**  64.100.0.0 The network address of the subnet

★ **Subnet Bitmask:**  16 The bitmask (numeric) of the subnet you are adding. Do not include the slash.

★ **Network POD Name:**  CVF7-Network-Pod1

**Assigned Subnets:** The public subnets that have already been assigned.

**Unassigned Subnets:** The free public subnets remaining in the pool.

296696

When an OTA is creating a new VDC under a Tenant's Organization, if the selected VDC plan has an Unprotected Public network, IAC carves out a CIDR subnet (see [Figure 3-23](#)) from the global Public IP subnet of the Network pod. The OTA creating the VDC selects the number of IP addresses to reserve, but the CPTA, who has to approve the VDC creation, might choose to change that number depending on the available address space remaining.

**Figure 3-23 Adding a Public IP Subnet to a VDC in a Tenant's Org**

**Configure Network for VDC**

Select a Network Service: 1-Zone Bronze Internet

Number Of Networks: 1

---

**Network Details**

★ Network Name: testnamechange Enter a name for network associated with virtual data center.

Zone Type: Unprotected Public

IP Address Type: Public

Max Hosts: 12 Select the number of host expected in each network. This will determine the size of the networks to be provisioned.

Management Network: 12

4

28

60

124

252

508

296697

## IPAM

IAC offers four IPAM options - Cisco IP Address Management (IPAM), Dynamic Host Configuration Protocol (DHCP), internal, and external management of IP addresses. One of these four options needs to be selected as the network source when creating a new network. The internal IPAM tool was used in this deployment (see [Figure 3-24](#)).



### Note

Cisco IPAM is provided by Cisco Prime Network Registrar (CPNR). Internal IPAM is provided by IAC. External IPAM allows integration with third-party services such as InfoBlox.

**Figure 3-24 IPAM Options in IAC**

**Add Network**

Define a VLAN and subnet to select in the cloud system, user servers, server management, or the cloud infrastructure services.

---

**POD Information**

★ Cloud Infrastructure Type: VMware vCenter Server Select the Cloud Infrastructure Type.

---

**Network Information**

★ Network Name: Enter a short name for the network that will be shown to users in drop-down selection lists.

★ Subnet Address Specification: Enter the network for this subnet in CIDR notation. For example, 192.168.20.0/24. Enter only an IPv4 type of IP address. Note: Only networks from /23 through /29 are supported.

Community Network: No Choose the network access scope for user networks. A community network is available to users in shared zones. Non-community networks require explicit VDC level access to be set before users can deploy servers to it, which can be useful for traffic isolation and better security.

Public Network: Yes Specify the duplication policy for this network. Public networks are globally unique, while private networks must only be unique within associated network device contexts.

★ Network Type: Infrastructure Choose a network type to determine how this network can be used. User networks are used for deploying virtual machines or physical servers. Management networks are used for management access to cloud servers. Infrastructure networks are used for management interfaces of hypervisor hosts and other infrastructure devices.

★ Network Source: Internal Select how IP addresses management is done in this network: Internally by Cisco IAC, or via an external IP management tool.

vCenter Portgroups:

Portgroup Name	Host Name	Network Path	VMware vCenter Server
Internal			

296695

IP address usage of each Tenant network can be monitored from Operations > Network Management. When selecting a particular network, the status of each IP address in that range is shown to be either assigned/unassigned or excluded (see [Figure 3-25](#)).



Figure 3-25 IAC Internal IPAM

Intelligent Automation for Cloud 4.0

My Cloud | Setup | Management | Operations

cpa cpa Service Portal

### Networks

	Network Name	Network Source	Available IP's	Assigned IP's	Total IP's	% Utilized	VDC	Organization	Tenant
<input type="radio"/>	...	...	251	0	251	0%			Bronze_Films
<input checked="" type="radio"/>	A507EntTrans13597	Internal	4	1	7	43%		ArP3B507-Eng	ArP3B507
<input type="radio"/>	A507EntTrans14130	Internal	4	1	7	43%		ArP3B507-Fin	ArP3B507
<input type="radio"/>	A507EntTrans14273	Internal	5	0	7	29%		ArP3B507-MRKT	ArP3B507
<input type="radio"/>	A507EntTrans15203	Internal	4	1	7	43%		ArP3B507-Dev	ArP3B507
<input type="radio"/>	A507SNIP13597	Internal	249	2	251	1%		ArP3B507-Eng	ArP3B507
<input type="radio"/>	A507SNIP14130	Internal	248	3	251	1%		ArP3B507-Fin	ArP3B507
<input type="radio"/>	A507SNIP14273	Internal	251	0	251	0%		ArP3B507-MRKT	ArP3B507
<input type="radio"/>	A507SNIP15203	Internal	249	2	251	1%		ArP3B507-Dev	ArP3B507
<input type="radio"/>	ACMEEntTrans2156	Internal	252	1	255	1%			ACME Corp

### IP Address Assignments: A507EntTrans13597

	IP Addresses	Server	Assigned Date	Status	Action
<input type="checkbox"/>	10.2.2.1	Enterprise_A507CSR13597	03/27/2014 8:58 AM	Excluded	
<input type="checkbox"/>	10.2.2.2		03/27/2014 9:58 AM	Assigned	
<input type="checkbox"/>	10.2.2.3		03/27/2014 8:58 AM	Unassigned	
<input type="checkbox"/>	10.2.2.4		03/27/2014 8:58 AM	Unassigned	
<input type="checkbox"/>	10.2.2.5		03/27/2014 8:58 AM	Unassigned	
<input type="checkbox"/>	10.2.2.6		03/27/2014 8:58 AM	Unassigned	
<input type="checkbox"/>	10.2.2.7		03/27/2014 8:58 AM	Excluded	

296586



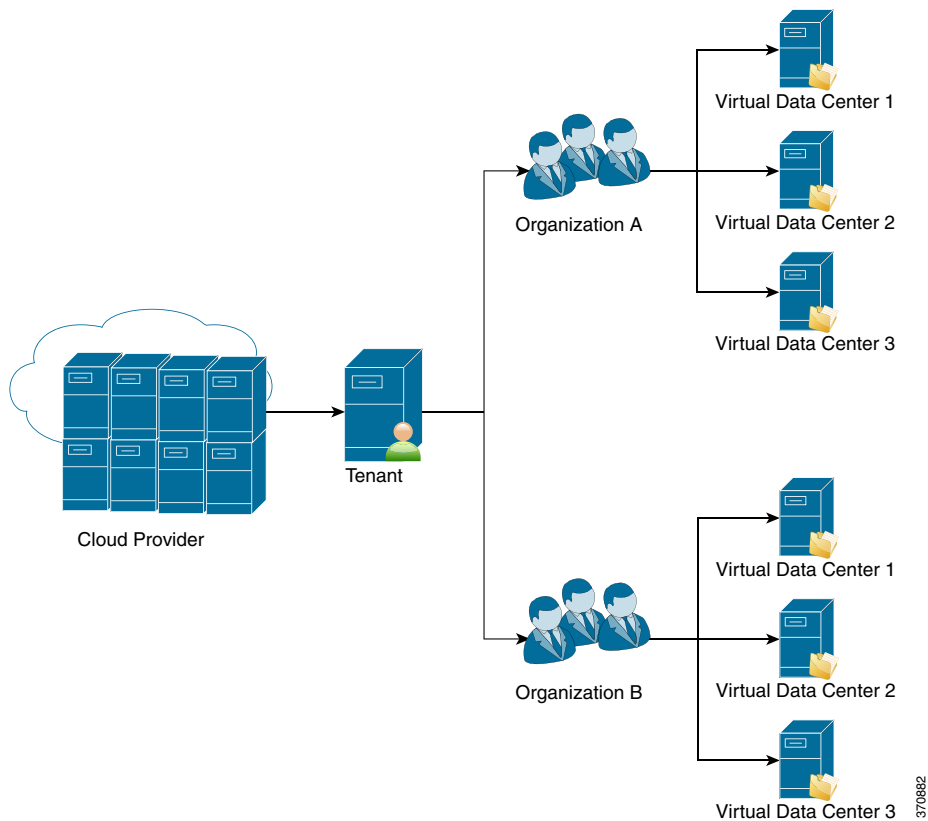


## Workflows and Use Cases

---

This chapter shows the general workflow of onboarding a Tenant and providing access to cloud resources through the Cisco Intelligent Automation for Cloud (IAC) 4.0 solution. This chapter also discusses in detail various use cases for Virtual Data Center (VDC) configuration, in particular: service groups, firewall rules, Network Address Translation (NAT), load balancing, and adding or removing networks on a VDC.

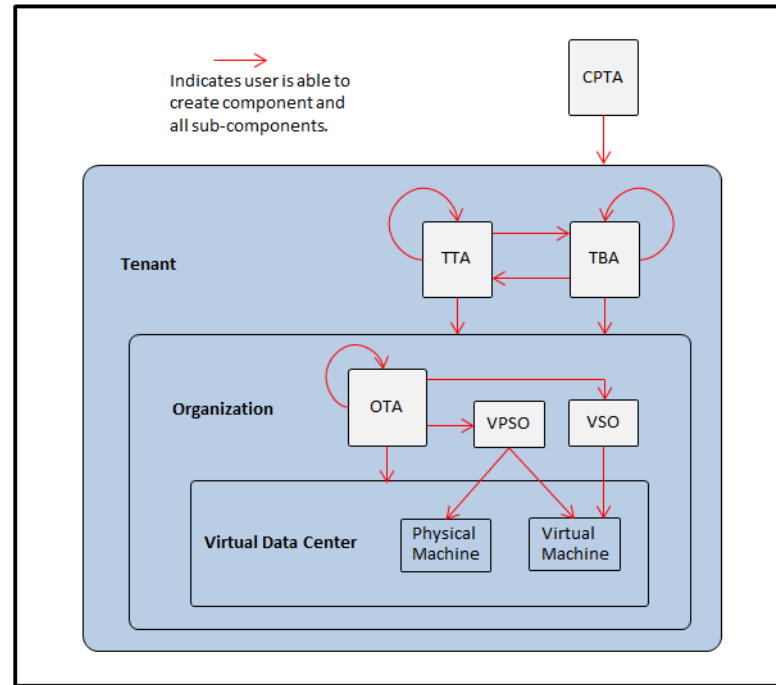
In general, a Tenant is first created, then an Organization, and finally a VDC. Once a VDC is created, Virtual Machines (VMs) can be provisioned, however, an administrator may wish to customize the VDC before doing so. The general hierarchy of an IAC cloud Tenant is illustrated in [Figure 4-1](#). The first part of this chapter demonstrates the use case of a single Tenant, Organization, and VDC (Two- Zone Gold Internet) creation.

**Figure 4-1 IAC 4.0 Components**

During initial configuration, the Cloud Provider Administrative Organization as well as the Cloud Provider Technical Administrator (CPTA) is created. Refer to the [IAC Installation Guide](#) for more information.

Once the solution is completely configured, the CPTA then typically creates Tenant accounts as well as Tenant Technical Administrators (TTAs) for each account. The TTAs then create Organizations and Organization Technical Administrators (OTAs) for each Organization. OTAs then order VDCs for their Organization. OTAs also create Virtual and Physical Server Owners (VSOs/VPSOs) for their Organization. Finally, VSOs/VPSOs order VMs within any VDC in their Organization.

As mentioned in [IAC User Roles and RBAC](#), all of the roles are hierarchical, with the CPTA user capable of performing all tasks, the TTA user capable of performing all tasks of the OTA, VSO, or VPSO, and the OTA capable of performing all VSO or VPSO tasks. An overview of these permissions is shown in [Figure 4-2](#).

**Figure 4-2 IAC Permissions Overview**

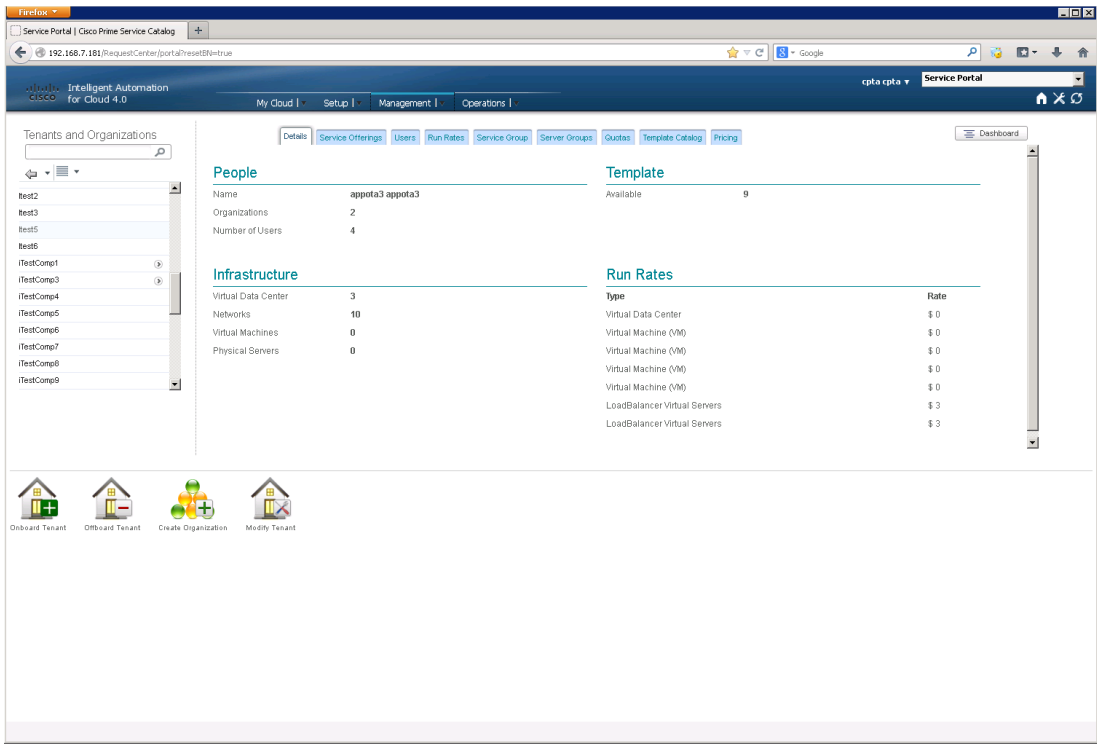
The following sections provide a typical workflow for creating a Tenant, Organization, VDC, and VM. The last section discusses options for managing virtual network services.

## Onboard a Tenant

Onboarding a Tenant is the first step in providing a customer access to cloud resources. In this step, a Tenant account is created and preliminary settings such as run rates and Tenant-wide services are configured. The Tenant is always onboarded by a Cloud Provider Technical Administrator (CPTA).

- 
- Step 1** Log into the Cisco Service Catalog as CPTA.
  - Step 2** Select Service Portal under the module drop-down list.
  - Step 3** Under the IAC menu bar, select Management > Tenant Management. A list of existing Tenants opens, as shown in [Figure 4-3](#).

Figure 4-3 Tenant Management Page



**Step 4** Click the Onboard Tenant icon at the bottom of the page. The Onboard Tenant form opens.

**Step 5** Complete the form by adding the Tenant’s information. Required values have a red star next to them (see Figure 4-4).

Figure 4-4 Onboard Tenant Form

## Onboard Tenant

Define a new tenant of cloud users.

<p>★ Company Name: <input type="text" value="Example Company"/></p> <p>★ Company Abbreviation: <input type="text" value="EXCP"/></p> <p>Description: <input type="text" value="Full Service Media Production and Storage Company."/></p> <p>★ Run rate limit: <input type="text" value="Large"/></p> <p>Currency Limit: 10000</p> <p>Private Subnet: <input type="text" value="192.168.0.0/16"/></p>	<p>Enter the full name of the company.</p> <p>Enter the company abbreviation. (Maximum 4 characters)</p> <p>Enter the description.</p> <p>Select the Quotas, this is used to determine the quotas for the tenant.</p> <p>Quota for the maximum currency limit for the tenant.</p>
--	---

Primary Contact

<p>★ Action: <input type="text" value="Create New User"/></p> <p>★ First Name: <input type="text" value="Jonathan"/></p> <p>★ Last Name: <input type="text" value="Houser"/></p> <p>★ Login: <input type="text" value="JHouser"/></p> <p>★ Password: <input type="password" value="••••••••"/></p> <p>★ Confirm Password: <input type="password" value="••••••••"/></p> <p>★ Primary Contact Email: <input type="text" value="JHouser@example.com"/></p> <p>Primary Contact Title: <input type="text" value="Manager"/></p> <p>Primary Contact Number: <input type="text" value="555-555-5555"/></p> <p>Street#1: <input type="text" value="699 12th Ave"/></p> <p>Street#2: <input type="text" value="Suite 9178"/></p> <p>City: <input type="text" value="New York"/></p> <p>State: <input type="text" value="New York"/></p> <p>Country: <input type="text" value="United States"/></p> <p>Postal Code: <input type="text" value="10001"/></p>	<p>Chose an appropriate action to set the User as a Tenant Technical Administrator.</p> <p>Enter the first name of the new user.</p> <p>Enter the last name of the new user.</p> <p>Login ID <b>JHouser</b> is currently available.</p> <p>Enter the contact email address.</p> <p>Enter the contact title.</p> <p>Enter the contact number.</p>
---	--

Set Tenant-wide Service Options

<p>Virtual Machine From Template Ordering: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> <p>Virtual Machine and Install OS Ordering: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> <p>Physical Server Ordering: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> <p>Virtual Data Center Ordering: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> <p>Community VDC Ordering: <input type="radio"/> Yes <input checked="" type="radio"/> No</p> <p>Advanced Network Services: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> <p>Multiple Security Zones: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> <p>Enhanced VM Security: <input checked="" type="radio"/> Yes <input type="radio"/> No</p> <p>High Availability: <input type="checkbox"/> Yes</p> <p>Load balancing Services: <input checked="" type="radio"/> Yes <input type="radio"/> No</p>	<p>Amazon EC2 / OpenStack / Cisco UCS Director / VMware vCenter Element Available</p> <p>Cisco SP Element Available</p> <p>UCS Manager Element Available</p> <p>Cisco SP Element Available</p> <p>Amazon EC2 / OpenStack / Cisco UCS Director / VMware vCenter Element Available</p> <p>Amazon EC2 / OpenStack / Cisco UCS Director / VMware vCenter Element Not Required</p> <p>IAC Management Appliance and Cisco Nexus 1000v are Required</p> <p>VDCs may have multiple tiers of network security zones between groups of networks. Supports deployments of Physical Servers.</p> <p>VDCs may have multiple tiers of network security zones (e.g. web tier, application tier, database tier) within a single or between networks.</p> <p>Allow deployment of HA pair of security services for resiliency.</p> <p>VDCs may distribute network traffic between group of servers.</p>
---	---

VDC Connection Type

<p>★ VDC Connection Type: <input type="text" value="Both"/></p>	<p>Select a connection type for Virtual Data Centers for this tenant.</p>
---	---

Enterprise Transit Network Details

<p>★ Enterprise Transit Network: <input type="text" value="10.2.2.0/24"/></p> <p>★ Enterprise Gateway: <input type="text" value="10.2.2.1"/></p> <p>★ Enterprise Remote BGP Peer IP: <input type="text" value="10.2.2.1"/></p>	<p>Enter IP Address Space to be used as transit network for Enterprise Connectivity.</p> <p>The IP address of the gateway router interface that will be used as the next hop for traffic leaving the VDCs destined for the Enterprise.</p> <p>The IP address used for BGP peering by the gateway router for advertising routes to the Enterprise.</p>
--	---

296698

A description of each field is provided below. For considerations to take when creating a Tenant, see [Onboarding a Tenant Considerations](#).

- a. **Company Name.** The full name of the company.
- b. **Abbreviation.** A four character abbreviation for the company (must begin with a letter and may not contain any special characters).
- c. **Description.** A description for the company.
- d. **Run rate limit.** A limit for the set of recurring cloud service charges that Tenant or Tenant users can purchase. This is essentially a Tenant quota.
- e. **Private Subnet.** The IP address subnet to be associated on Private/Enterprise interfaces created under the Tenant.
- f. **Primary Contact.** This is the user who is the TTA of the account. The TTA oversees the entire company account, and has a primary function of creating and maintaining Organizations. If there is an existing user that you wish to make the TTA of this account, then choose the “Select Existing User” option under Action. Otherwise, select “Create New User” and complete the contact information.
- g. **Set Tenant-wide Service options.** Tenant-wide Service options enable or disable a service for all Organizations and VDCs within the Tenant. If a service is disabled at the Tenant level, then it cannot be used in any Organization or VDC. If a service is enabled at the Tenant level, however, it can still be disabled at the Organization level. For this reason, it is better to leave these options as enabled if the Tenant is not sure if they will be used. These settings can be modified after creation, but any service provisioned while the option was enabled is not automatically rolled back if the option is later disabled.
- h. **Virtual Machine from Template Ordering.** Enables the Tenant to order VMs from registered templates on Amazon EC2, OpenStack, Cisco UCS Director, or VMware vCenter. Note that for VM provisioning, only VMware vCenter was validated in this release.
- i. **Virtual Machine and Install OS Ordering.** Enables the Tenant to order VMs and clean install an OS from the Cisco Server Provisioner (SP).
- j. **Physical Server Ordering.** Enables the Tenant to order physical servers and clean install an OS from the SP.
- k. **VDC Ordering.** Enables Tenant Organizations to order VDCs. VDCs are a container of virtualized routing and service components in the Compute layer.
- l. **Community VDC Ordering.** Allows the creation of a VDC, which is shared across all Tenants.
- m. **Advanced Network Services.** When enabled, provides automated network provisioning, security zones on network boundary, and optionally, intra-network security zones and LB services.
- n. **Multiple Security Zones.** Allows VDCs to have multiple tiers of network security zones between groups of networks. Supports deployments of Physical Servers.
- o. **Enhanced VM Security.** VDCs may have multiple tiers of network security zones (e.g., web tier, application tier, database tier) within a single network or between networks.
- p. **High Availability.** Allows deployment of HA pairs of security services for resiliency. Note that when onboarding a Tenant, do not select “High Availability.” HA for virtual network services is unsupported in this release and not validated in this deployment.
- q. **Load Balancing Services.** Allows VDCs to distribute network traffic between groups of servers. Enabling this option instantiates a VPX for the Organization and allows you to multiplex traffic between servers providing the same service.



- r. VDC Connection Type. Decides whether the Tenant uses Internet, Enterprise, or Both type VDC connections. An Internet type connection shares a Transit connection to the cloud edge with other Tenants. An Enterprise type connection has a Private Transit connection to the cloud edge. A Both type connection indicates that the Tenant uses both Internet and Enterprise connections. If Enterprise or Both is selected, then you are prompted to enter the Enterprise Transit Network details.
- s. Enterprise Transit Network. Address space to be associated with the Enterprise Transit network.
- t. Enterprise Gateway. Address of the gateway router interface that is used as the next hop for Enterprise traffic leaving the VDC.
- u. Enterprise Remote BGP Peer IP. Address used for BGP peering by the gateway router for advertising routes to the Enterprise. This can be the same as the Enterprise Gateway IP address, or it can be a loopback interface on the gateway router.

**Step 6** Click Submit. The order typically takes up to 10 minutes to complete. When the order is complete, you should now be able to select the Tenant on the Tenant Management page. The Tenant user you created is now able to log in.

## Create Tenant Administrative Users

Once the Tenant is created, you can create Tenant administrative users at the Tenant level. There should already be a TTA account under the Tenant, which was created during onboarding. As mentioned in the previous section, TTAs oversee the entire company account.

A Tenant Business Administrator (TBA) is the second type of administrative user that can be created at the Tenant level. A TBA is similar to a TTA, but deals primarily with price-related functions for the entire account.

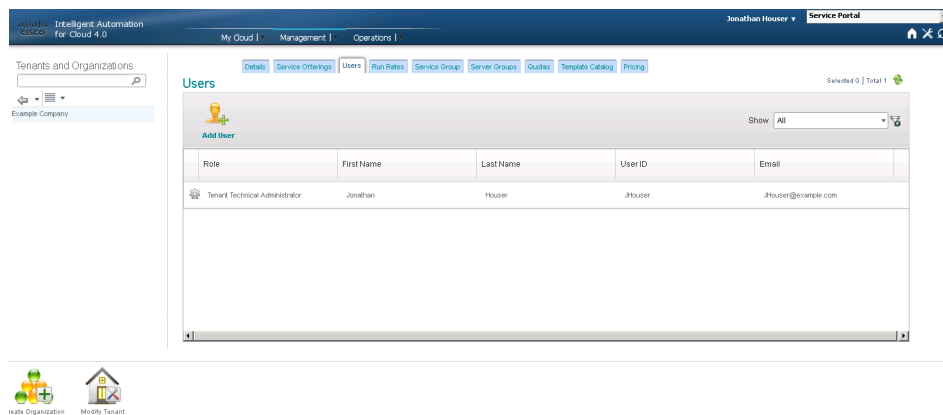


### Note

Note that although a TBA is created in this example, full capabilities and limitations were not tested for in this release. Refer to the [IAC Administration Guide](#) for more information on IAC user roles.

A complete list of Tenant users can be viewed on the Users tab on the Tenant Management page (see [Figure 4-5](#)).

**Figure 4-5** Tenant Management User Tab



**Step 1** Log into the Service Catalog as CPTA or the user you created during Tenant onboarding.

- Figure 4-6**      **Created Users**

Example Company

Users

Add User

Selected 0 | Total 2

Show

All

⌵

Role	First Name	Last Name	User ID	Email	
Tenant Technical Administrator	Jonathan	Houser	JHouser	JHouser@example.com	
Tenant Business Administrator	Lisa	Roland	LRoland	LRoland@example.com	

An Organization is used to contain users who are grouped according to a certain function or business. Organizations are usually either business units, i.e., Marketing or Sales, or Service Teams, which provide support for the IAC Solution. If Advance Network Services was enabled, then an Organization is provided with a Cloud Services Router (CSR) to act as the Organization's edge router. In addition, an Organization is provided a Virtual Security Gateway (VSG), and a NetScaler VPX if enhanced VM security and LB services were enabled, respectively.

<b>Step 1</b>	Log in as the CPTA or TTA.
<b>Step 2</b>	Select Service Portal from the module drop-down list.
<b>Step 3</b>	Select Management > Tenant Management from the IAC menu bar.
<b>Step 4</b>	Select the company name.
<b>Step 5</b>	Click the Create Organization icon. The Create Organization form opens (see <a href="#">Figure 4-7</a> ).

**Figure 4-7 Create Organization Form**

**Step 6** Complete the form by adding the Organization's information. Required values have a red star next to them. The values for creating an Organization are explained below. For considerations to take when creating an Organization, see [Creating an Organization Considerations](#).

- a. Organization Name. Name of the Organization. Must be one word.
- b. Organization Description. Description for the Organization.
- c. VDC Connection Type. Decides whether the Organization uses Internet, Enterprise, or Both type VDC connections. This option is available only if a Both VDC connection type is enabled for the Tenant. See the previous section for more details.
- d. Set Organization-wide Service Options. Organization-wide service options enable or disable a service for all VDCs within the Organization. These options are the same as those set during Tenant creation. See the previous section for more details.
- e. Resource Name. Decides which resource container is used for the Organization's virtual service devices, such as the CSR 1000, VSG, and VPX. These devices are placed in the resource pool defined in the resource container.
- f. Add Load Balancer for HTTP and HTTPS. As mentioned before, load balancers allow VDCs to distribute network traffic between groups of servers. If LB services are enabled, then you must define a LB for HTTP and HTTPS services.
- g. Load Balancing Server. Friendly name for the LB server.
- h. Description. Description for the LB server.
- i. IP Address Type. Public or Private. A Public type assigns the LB an IP address from the Resource Container's Public subnet. The CPTA must add a Public subnet to the Network pod to use a Public address (see [Public Pool](#) for more information). A Private type assigns the LB an IP address from whatever Private subnet was chosen when the Tenant was onboarded.
- j. Method. Determines what method the LB uses to load balance traffic.

- k. **Service Group.** The service group that the LB balances traffic on. A Tenant is initially provided two service groups, HTTP and HTTPS. One of each must be configured during Organization creation. Additional service groups can be defined once the Organization is created.

**Step 7** Click submit. The order typically takes around an hour to complete, but can vary greatly depending on the IAC infrastructure setup.

**Step 8** Refresh the portlet. You should now see an arrow next to the company name.

**Step 9** Click the arrow to see a list of all Organizations created under the Tenant.

**Note**

Once the Organization is complete, a CSR 1000V, VSG, and VPX are provisioned if the respective advance services were enabled. Appendix D, [Configurations](#), shows some examples of initial configurations on the Organization's virtual devices. Some configurations may vary depending on which Organization services were enabled.

## Create Organization Technical Administrators and Server Owners

Once the Organization is created, you can create Virtual Server Owners (VSO), Virtual and Physical Server Owners (VPSO), and Organization Technical Administrators (OTA) at the Organization level.

Organization Technical Administrators manage resources within the entire Organization such as VDCs, firewall rules, LB services, VDC zones, and networks. OTAs can also create and manage server owners (VSO/VPSO). The VPSO is an End User who can order and manage virtual and physical machines. The VSO can order and manage only VMs. OTAs and server owners are created at the Organization level.

Complete the following steps to create OTA and server owners:

**Step 1** Log in as the TTA.

**Step 2** Select Service Portal from the module drop-down list.

**Step 3** Select Management from the IAC menu bar.

**Step 4** Select Tenant Management.

**Step 5** Select the Company.

**Step 6** Select the Organization.

**Step 7** Click the Users tab.

**Step 8** Click the Add User icon. The Add User to an Organization form opens (see [Figure 4-8](#)).

**Figure 4-8 Add User to an Organization Form**

**Add User**

**Add User to an Organization**

Select a user to be added to an Organization.

**User Organization**

Organization Name: Example Company-Production

Action:  Chose an appropriate action.

**Create New User As OTA**

\* First Name:  Enter the first name of the new user.

\* Last Name:  Enter the last name of the new user.

\* Login:  Login ID JSmith is currently available.

\* Email:  Email address is valid.

\* Roles: ☐ Virtual Server Owner  
☐ Virtual and Physical Server Owner  
☒ Organization Technical Administrator Select a Role to assign to the User.

Time Zone:  Select the time zone associated with the user's primary address.

Organization name: Example Company-Production

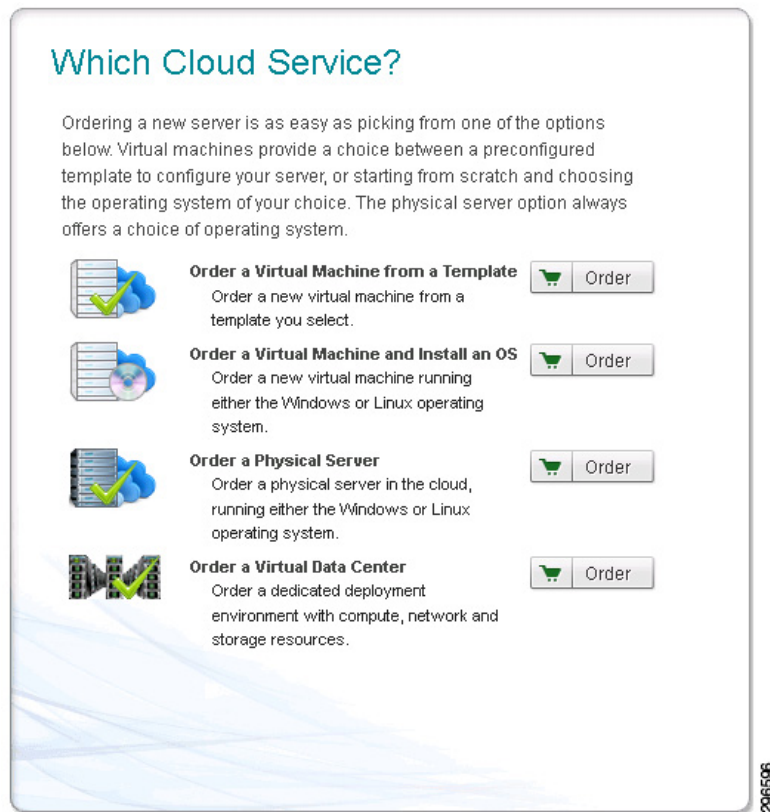
\* Password:  Enter the password of the user.

\* Confirm Password:  Enter the password again for the confirmation.

**Step 9** Complete the form by adding the user's information. Required values have a red star next to them. The order typically takes up to 5 minutes to complete. When the order is complete, the user is visible under the Users tab and can now login. Be sure to create at least one OTA for each Organization.

## Create a Virtual Data Center

Once the Organization is created, you should be able to create VDCs. VDCs are a major component within the IAC solution and allow the creation of network zones, firewall rules, physical machines, and VMs.

**Figure 4-9** *Order Services Menu*

Complete the following steps to create a VDC:

- 
- Step 1** Login as the OTA.
  - Step 2** Select Service Portal from the module drop-down list.
  - Step 3** Select My Cloud from the IAC menu bar.
  - Step 4** Select Order Services.
  - Step 5** Click Order a Virtual Data Center. The Select or Change Plan form opens (see [Figure 4-10](#)). As discussed in [Virtual Data Center \(Network Container\) Design](#), IAC provides multiple choices for VDC network containers. This example uses a Two-Zone Gold Internet container.

**Figure 4-10 Create Virtual Data Center Form - Part 1**

**Create Virtual Data Center Service**

### Select or Change Plan

☐ **4-Zone Gold**  
Four security zones: a public, a protected public, a private and a protected private zone.

- Multiple Security Zones
- Enhanced VM Security
- Load-Balancing Services

☒ **2-Zone Gold Internet**  
Two security zones: a protected public and protected private zone.

- Multiple Security Zones
- Enhanced VM Security
- Load-Balancing Services

☐ **2-Zone Gold Enterprise**  
Two security zones: a protected public and protected private zone.

- Multiple Security Zones
- Enhanced VM Security
- Load-Balancing Services

☐ **2-Zone Silver Internet**  
Two security zones: an unprotected public and protected public zone.

- Multiple Security Zones
- Enhanced VM Security

☐ **2-Zone Silver Enterprise**  
Two security zones: an unprotected private and protected private zone.

- Multiple Security Zones
- Enhanced VM Security

☐ **1-Zone Bronze Internet**  
One security zone: an unprotected public

☐ **1-Zone Bronze Enterprise**  
One security zone: an unprotected private

☐ **Other**  
Custom topology

### Selected Plan Topology

Public Zone

Protected Public Zone

Tenant Edge Firewall

296597

**Step 6** Click Next. The Create Virtual Data Center form opens (see [Figure 4-11](#)). The VDC attribute field descriptions are described below.

- VDC Name. Name for the VDC.
- Description. Description for the VDC.
- Size. Size of the VDC. Determines the limit for VMs, CPUs, storage, memory, and physical servers within the VDC.
- Network Details. Each VDC contains at least one network. For this container, there are two zones, Unprotected Public and Protected Public. It is important to understand that the CSR 1000V has a limit of ten virtual interfaces. For every network provisioned, a CSR 1000V interface is consumed. For this reason, Organizations and VDCs should be designed such that the ten interface limit is not exceeded. See [Virtual Data Center \(Network Container\) Design](#) for more details.
- Network Name. Name for the network or zone.
- Max Hosts. Maximum number of hosts expected on this network. IAC uses this value to create the appropriate subnet size for that network.

**Figure 4-11** Create Virtual Data Center Form - Part 2

**Create Virtual Data Center Service**

**Create Virtual Data Center**

Order a dedicated deployment environment with compute, network and storage resources.

No change to the pricing information.

**Organization Details**

Tenant: Example Company

Organization: Example Company-Production

**Virtual Data Center**

VDC Name: BroadcastProductions

Description: Compute Center for Broadcast Media.

Size: Medium

Virtual Machines Limit: 100

VM CPUs Limit: 145

CPU Limit (MHz): 43500

VM Storage Limit (GB): 14750

VM Memory Limit (GB): 590

Physical Servers Limit: 2

**Configure Network for VDC**

Select a Network Service: 2-Zone Gold Internet

Number Of Networks: 2

**Network Details**

Network Name: Subscriber Network

Zone Type: Unprotected Public

IP Address Type: Public

Max Hosts: 124

Second Network Name: Production Network

Zone Type: Protected Public

- Step 7** Click submit. Before the process can start, it must be approved by the CPTA (explained in the next section). The time it takes to provision a VDC can vary greatly depending on the topology selected and the IAC infrastructure setup.
- Step 8** Select My Cloud in the IAC menu bar.
- Step 9** Select My VDCs. You should now see the VDC you created in the list.

## Approve the Virtual Data Center

VDCs must be approved by the CPTA before they are provisioned. Complete the following steps to approve a VDC request:

- Step 1** Log in as the CPTA.
- Step 2** Select Service Portal from the module drop-down list.
- Step 3** Select Operations from the IAC menu bar.
- Step 4** Select Approvals.
- Step 5** Select “My Assigned and Unassigned” and “Ongoing” as the first and second sort options. The order number for the requested VDC should appear in the list. (see [Figure 4-12](#)).



**Figure 4-12** Order Number Details

Order #	Customer	Service Name	Cost	Priority
22054	Justin Smith: Example Company-Production	Create Virtual Data Center	0	Normal

**Step 6** Click the order number to open the request. The Create Virtual Data Center form opens (see Figure 4-13).

**Figure 4-13** Create Virtual Data Center Form

**Create Virtual Data Center**

Description:  Enter an informative description and any guidelines for using this virtual data center.

Community VDC: No

Size:  Select the virtual data center resource capacity from the available standard options.

Snapshots per VM Limit: 5

Virtual Machines Limit: 100

VM CPUs Limit: 145

CPU Limit (MHz): 43500

VM Storage Limit (GB): 14750

VM Memory Limit (GB): 580

Physical Servers Limit: 2

Compute POD:  Select the POD in which to place the virtual data center.

Cluster:  Select the virtual cluster for the virtual data center.

Datastore:  Select a datastore for the virtual data center VM storage.

Description:

Datastore Cluster: Yes

Capacity (GB): 1998.75000

Free space (GB): 1655.52000 Available Free Space information is captured from last time when collect metrics process executed.

**Resource Pool**

Resource Pool Name: Example Company-BroadcastProductions

CPU Shares: Normal

CPU Limit (MHz): 43500

Memory Limit (GB): 580

CPU Reservation (MHz):  Enter the amount of CPU reservation in MHz to exclusively set aside for this shared zone resource pool.

Memory Reservation (GB):  Enter the amount of memory to exclusively set aside for this shared zone resource pool.

**Step 7** All of the details of the VDC request are listed on the form and can be modified, although this is usually not done. As the CPTA, however, you must select which Compute pod, Data Center Cluster, and Datastore you want to use for the VDC. After selecting these values, click Update. Navigate to the top of the form and select Task Details.

**Step 8** Select Approve. Once this is done, the VDC provisioning process begins.

**Figure 4-14** Task Details

**Task Details**

Cisco Intelligent Automation for Cloud 4.0

Approve Reject Check out

**Task Details**

Task Data

Comments and History

Attachments

Ad-Hoc Tasks

Name: Need Approval for Create Virtual Data Center Due On: 04/18/2014 12:17 PM

**Note**

Note that the CPTA can also create VDCs for any Organization. As an alternative to the approval process, an OTA or TTA can request for the CPTA to create VDCs directly.

**Note**

Once the VDC is provisioned, some configurations changes are made on the CSR 1000V and VSG. Appendix D, [Configurations](#), shows what lines were added to virtual devices' configurations. Note that there are no changes made to the VPX during VDC creation. The VPX is configured when provisioning LB services.

## Provision a Virtual Machine

Once the VDC is created, you can provision VMs. VMs are typically ordered by Virtual Server Owners (VSO) or Virtual and Physical Server Owners (VPSO). OTAs, TTAs, and CPTAs can also order VMs and re-assign ownership.

There are two options for provisioning a VM, provisioning from a template and installing an OS. Provisioning a VM from a template creates a VM by cloning it from a template registered in the IAC infrastructure database. Installing an OS provisions a VM from scratch and installs an OS using the SP.

### Register a Virtual Machine Template

Before you can provision a VM from a template, you must register the template under the management infrastructure menu by completing the following steps:

- 
- Step 1** Log in as CPTA.
  - Step 2** Select Service Portal from the module drop-down list.
  - Step 3** Select Setup from the IAC menu bar.
  - Step 4** Select Manage Infrastructure. You should see a list of platform elements. Note that VMware vCenter was used in this setup and is the only platform validated for provisioning VMs.
  - Step 5** Select VM Templates under the Platform Elements list (see [Figure 4-15](#)). Any VM template configured in your setup should appear in the list. The Platform Elements can have one of the following statuses:
    - a. A status of “Discovered” indicates that IAC has found the VM template, but it cannot be used until registered.
    - b. A status of “Registered” indicates that it can be used in the IAC solution.
    - c. A status of “Not Found” indicates that the template was previously discovered and or registered, but IAC can no longer find it. A template can migrate to the “Not Found” state if it is renamed or moved. For this reason, it is important to avoid making changes to templates once they are discovered.

**Figure 4-15** VM Templates

The screenshot shows the VMware vCenter console interface. On the left, a sidebar lists various infrastructure components: Amazon EC2, Cisco IAC Management Appliance, Cisco Server Provisioner, Cisco UCS Director, Cisco UCS Manager, Cisco Prime Network Services Controller, Network Elements, OpenStack, VMware vCloud Director, VMware vCenter Server, and a list of resources including Data Centers (3), Clusters, Hosts, Datastores (16), Resource Pools, Portgroups, VM Templates (1), and Virtual Machines (163). The 'VM Templates' option is selected in the sidebar.

The main panel is titled 'VM Templates' and contains two buttons: 'Discover VM Templates' and 'Discover VMware vCenter Cloud Resources'. Below these buttons is a table listing VM templates:

VM Template Name	Status
template-websrv	NotFound
template-min-websrv	NotFound
template-min-WinSrv	NotFound
template-min-WinServer	NotFound
template-websrv-https	Registered
template-min-websrv2	Registered
mailsrv-bkup	Discovered
lamp-template	NotFound
template-lamp	NotFound

- Step 6** VM templates that were recently created may not appear in the list at all. To have IAC rediscover VM templates, click the Discover VM Templates icon near the top of the page. A confirmation with a requisition number should open. Once the order is complete, any new templates should appear in the list with a “Discovered” status.
- Step 7** Click the gear icon next to the template you wish to register.
- Step 8** Select Register VM Template. The Register VM Template form opens, as shown in [Figure 4-16](#).

**Figure 4-16 Register VM Template Form**

**Register VM Template**

Register this virtual machine template to be available for selection when deploying virtual machines. The template will then be uniformly available to all users.

**VM Template Information**

Template Name: mailsrv-blup

Template FullPath: mgmt/mailsrv-blup

Operating System Family: Linux

Operating System: CentOS 5/6 64-bit

Display Name: Mail Server

Description: Linux Template for SMTP Servers.

App Code:

Access Tenants: ☒ All Tenants ☐ Specific Tenants

Price: 15

The vSphere UI inventory path of the Virtual Machine Template

Select an operating system family category for the template.

Select the operating system of this template.

Enter a short friendly name that will identify this template in selection lists.

Enter a friendly description for the VM template. Include enough details here to help users make good decisions about which template to choose for their VM.

Enter up to 6 digits to use when automatically creating hostnames. These characters must adhere to NetBIOS and hypervisor restrictions and do not have to be unique.

Choose who has access to this template.

Please enter the price of the template.

Submit Order Reset

## Provision a Virtual Machine from a Template

Complete the following steps to provision a VM from a template:

- Step 1** Log in as a VSO or any user with access to a VDC.
- Step 2** Select Service Portal from the module drop-down list.
- Step 3** Select My Cloud from the IAC menu bar.
- Step 4** Select Order Services.
- Step 5** Click Order a Virtual Machine. The Order a Virtual Machine from Template form opens (see [Figure 4-17](#)).

**Figure 4-17** Order a Virtual Machine from Template Form

- Step 6** Complete the form by adding the VM's information. Required values have a red star next to them.
- VDC Name. Select the VDC on which to deploy the server.
  - Friendly Name. Friendly name that you wish to use to identify the VM.
  - Operating System Family. Operating system family of the template (Windows, Linux).
  - Operating System. Operating system for the selected family (Windows 2008, CentOS 5/6).
  - vCenter Template. Registered VM template you wish to use for deploying the VM.
  - Virtual Machine Size. Determines the hardware configuration sizes (CPU, memory, storage) for the virtual machine.
  - Deploy to Network. Determines the VDC network on which to deploy the server. The server is automatically assigned and set up with a static IP address on this network.
  - Quantity. Determines the number of servers to provision. All servers in the order inherit the friendly name with a number appended to the end.
  - Lease Term. Determines the duration of the lease term. The server is decommissioned automatically at the end of the selected lease term unless you extend the lease.
- Step 7** Click Submit Order. The order typically takes up to 25 minutes to complete.
- Step 8** Select My Cloud from the IAC menu bar.
- Step 9** Select My Servers. The VM should now be visible in the list.

## Provision a Virtual Machine and Install an Operating System

To provision a VM and install a guest OS, you must have the SP installed and connected to IAC. You must also register at least one OS template for the SP. Registering an OS template is done the same way VM templates are done, except with the SP as the platform element (see [Figure 4-17](#)). Note that this step assumes that the ISOs have already been added to the SP. For more information, refer to the [Cisco Server Provisioner Guide](#).

Complete the following steps to provision a VM:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Log in as a Virtual Server Owner or any user with access to a VDC.   |
| <b>Step 2</b> | Select Service Portal from the module drop-down list.  |
| <b>Step 3</b> | Select My Cloud from the IAC menu bar.   |
| <b>Step 4</b> | Select Order Services.   |
| <b>Step 5</b> | Click Order a Virtual Machine and Install OS. The Order Virtual Machine from Template form opens. Select the SP template to install from rather than the platform template. You are also asked to provide an administrator password for initial login. See the previous section for the field descriptions. If the OS fields are not selectable or empty, then it usually means that there are no OS templates registered with the SP, or the VDC was configured with a Compute pod that does not include an SP. In the latter case, the CPTA must either modify the Compute pod to include a SP or a new VDC must be created. |
| <b>Step 6</b> | Complete the form by adding the VM's information. Required values have a red star next to them.  |
| <b>Step 7</b> | Click Submit Order. The order typically takes up to 25 minutes to complete, but may vary depending on the OS template.   |
| <b>Step 8</b> | Select My Cloud from the IAC menu bar.   |
| <b>Step 9</b> | Select My Servers. The VM should now be visible in the list.   |

## Provision a Physical Machine

Physical machines are typically ordered by VPSOs, however, OTAs, TTAs, and CPTAs can also order physical machines and re-assign ownership. To provision a physical machine, you must have the following prerequisites completed:

- SP installed and connected to IAC
- At least one OS template registered for the SP
- UCS service profile template registered for the UCS Manager
- Use a VDC configured with a Compute pod that has the SP
- Use a VDC large enough to handle physical servers
- Register all servers intended for provisioning under the Manage Infrastructure menu.
- Ensure that the blades are in the available state and in the physical pool.

To provision a physical machine, you must have the SP installed and connected to IAC. You must also register at least one OS template for the SP. Registering an OS template is done the same way VM templates are done, except with the SP as the platform element. A UCS Service Profile template is also registered in the same manner under UCS Manager. The Service Profile template must be setup in a specific manner to work with the SP. Refer to the “Understanding Cisco UCS Manager” chapter of the [IAC Installation Guide](#) for more information.

The VDC must use a size that allows physical servers. This example uses a size of “Medium,” which allows for two physical servers to be provisioned. Ensure that whatever VDC you use is defined to allow at least one physical server. In addition, the CPTA must be sure to assign the VDC to a Compute pod that has the SP included.

When cloud resources are initially discovered (usually during initial configuration), UCS blades with a Service Profile template associated are set to an “In Use” server state. IAC only provisions registered blades with an “Available” server state, therefore any “In Use” servers that you wish to provision must be manually changed using the CloudSync Edit Infrastructure option on the blade in question. This can be done after the blade is registered. See the following section for information on how to register a UCS blade server.

It is highly recommended that you dissociate any service profile template from a blade before making it available in IAC. IAC does not check to see if the blade is in use within the solution, therefore it is important to ensure there are no VMs in use on the blade and disassociate it from a template before making it available for server provisioning. If a blade server contains Tenant VMs and is made available, then they are erased upon provisioning and may be unrecoverable.

### Register a UCS Blade Server

Complete the following steps to register a UCS Manager Blade Server:

- 
- Step 1** Log in as CPTA.
  - Step 2** Select Service Portal from the module drop-down list.
  - Step 3** Select Setup from the IAC menu bar.
  - Step 4** Select Manage Infrastructure. You should see a list of platform elements.
  - Step 5** Select UCS Manager.
  - Step 6** Select UCS Blades. Any UCS blade server in your setup should appear in the list (see [Figure 4-18](#)). The UCS blade server can have one of the following statuses:
    - a. A status of “Discovered” indicates that IAC has found the UCS blade, but it cannot be used until registered.
    - b. A status of “Registered” indicates that it can be deployed in the IAC solution if made available.
    - c. A status of “Not Found” indicates that the blade was previously discovered and or registered, but IAC can no longer find it.
    - d. A status of “In Use” indicates that the blade is not available to be deployed as a physical server.
    - e. A status of “Available” means that the blade is ready for physical server deployment.
    - f. A status of “Pending” indicates that the blade is currently being deployed as a physical server.

Figure 4-18 UCS Blades Menu

IP	Model	Number of...	Number of...	Total Memory(...)	Status	Pool Type	Server State	First [
UCSB-B200-M3	16	2	98304	Discovered	None	In Use	01/2	
UCSB-B200-M3	16	2	98304	Discovered	None	In Use	01/2	
UCSB-B200-M3	16	2	98304	Discovered	None	In Use	01/2	
UCSB-B200-M3	16	2	98304	Discovered	None	In Use	01/2	
UCSB-B200-M3	16	2	98304	Registered	Physical	In Use		
192.168.7.102 sys/chassis-1/blade-5	UCSB-B200-M3	16	2	98304	Registered	Physical	In Use	
192.168.7.102 sys/chassis-1/blade-6	UCSB-B200-M3	16	2	98304	Registered	Physical	In Use	
192.168.7.102 sys/chassis-1/blade-7	UCSB-B200-M3	16	2	98304	Registered	Physical	Available	

- Step 7** Blade servers that were recently added may not appear in the list at all. To have IAC rediscover blade servers, click the Discover UCS blades icon near the top of the page. A confirmation with a requisition number should appear. Once the order is complete, any new templates should appear in the list with a “Discovered” status.
- Step 8** Click the gear icon next to the blade you wish to register.
- Step 9** Select Register Cisco UCS Server. A form should appear.
- Step 10** Ensure that “Physical” is selected as the pool type.
- Step 11** Click Submit Order. The process typically takes less than 5 minutes to complete.
- Step 12** After registration, if the blade is in the “In Use” server state, you may want to make it available by using the CloudSync Edit Infrastructure option under the same gear icon. It is very important that you take precaution before doing this to ensure that Tenant VMs are not wiped out (see the previous section). Once the UCS blade is registered and made available, it can be deployed within the IAC solution.

### Provision a UCS Blade Server


Complete the following steps to provision a UCS blade server:

- Step 1** Log in as a VPSO or any user with access to a VDC (excluding VSOs).
- Step 2** Select Service Portal from the module drop-down list.
- Step 3** Select My Cloud from the IAC menu bar.
- Step 4** Select Order Services.
- Step 5** Click Order a Physical Machine. The Order Physical Server form opens (see [Figure 4-19](#)).



**Figure 4-19** Order Physical Server Form

Order a Physical Server



Order a physical server in the cloud, running either the Windows or Linux operating system.

### Virtual Data Center Selection

VDC Name:  Select the virtual data center on which to deploy the server.

Physical Servers Available: 2 Number of Servers available for order.

### Physical Server

\* Friendly Name:

\* Operating System Family:  Select the operating system family (Ex: Windows, Linux) of the desired operating system template from the list.

\* Operating System:  Select the operating system of the desired operating system template from the list.

\* Operating System Template:  Select the operating system template you wish to use for deploying the physical server from the list.

\* Cisco UCS Service Profile Template:  Select the Cisco UCS service profile template you wish to use for the physical server from the list.

\* Service Profile Template Description:  Select the time zone of the physical server.

Storage (GB):  
Memory(GB): 98304  
Number of CPUs: 2  
Number of Cores: 16

### Network Selection

\* Deploy to Network:  Select the network on which to deploy the server. The server will be assigned and set up with a static IP address on this network.

Remaining Addresses: 11 The number of addresses remaining on the network at the time of ordering.

### Lease Term

Lease Term:  Select the duration of the lease term. The server will be decommissioned automatically at the end of the selected lease term unless you extend the lease.

### Order Quantity

\* Quantity:  Select the number of servers to Order.

### Administrator Password

\* Password:  Enter the password to use when connecting to the platform element.

\* Re-Enter Password:  Enter the password again.

- Step 6** Complete the form by adding the server's information. Required values have a red star next to them.
- VDC Name. Select the VDC on which to deploy the server. Ensure that the VDC is configured to use a Compute pod that includes an SP. If there are servers available in the pool, then the remaining fields are populated. If not, then an error message appears. See the previous section for information on making servers available.
  - Friendly Name. Friendly name that you wish to use to identify the physical machine.
  - Operating System Family. OS family of the template (Windows, Linux).
  - Operating System. OS for the selected family (Windows 2008, CentOS 5/6).
  - Operating System Template. Registered SP template that you wish to install on the physical machine.
  - Cisco UCS Profile Template. Service Profile template to be associated with the server.
  - Time Zone. Determines the time zone the physical server uses.
  - Deploy to Network. Determines the VDC network on which to deploy the server. The server is automatically assigned and set up with a static IP address on this network.

- i. Lease Term. Determines the duration of the lease term. The server is decommissioned automatically at the end of the selected lease term unless you extend the lease.
  - j. Quantity. Determines the number of servers to Order. All servers in the order inherit the friendly name with a number appended to the end.
  - k. Password. Administrator password that is initially configured on the physical server.
- Step 7** Click Submit Order. The order typically takes up to 60 minutes to complete, but can vary depending on the server and OS template being used.
- Step 8** Select My Cloud from the IAC menu bar.
- Step 9** Select My Servers. The physical server should now be visible in the list.

## Managing Network Virtual Services

The following sections describe how to manage network virtual services.

### Firewall Service Management

In IAC, firewall management can be done from the following tabs in the Request Center portal:

- My Cloud Tab. This tab provides access to the My VDC and My Server resource where firewall policies can be created.
- User Management Tab. This tab provides access to the Service Group tab where IAC firewall service groups can be configured.

IAC allows users to create the following firewall policies:

- Firewall Service Group. This is a collection of ports that can be used to create firewall rules. This can be created at either a Tenant or Organization level.
- Firewall Server Group. This is a collection of VMs belonging to a network segment assumed to have the similar function, e.g., group of VMs belonging to the same network segment that provides a web/application/database service. IAC provides this object for use for easier configuration of VDC/Server firewall policies.
- VDC Firewall Rule. This creates security policies that define what is permitted to the VDC. Security policies are configured on the CSR 1000V and VSG as part of this task.
- VM Firewall Rule. This creates a security policies that defines what is permitted to a specific server. This task requires configuration on both the CSR 1000V and VSG.
- Firewall service group management

IAC allows the user to perform the following tasks with firewall service group:

- Create firewall service group
- View firewall service group
- Add member to firewall service group
- Manage Firewall service group membership
- Delete firewall service group

## Firewall Security Zones

Depending on the virtual appliance platform, firewall zones are used to group set of network objects having similar functions. In the CSR 1000V, these network objects are network interfaces, and in the case of the VSG, the network objects could be network addresses and VMs represented using VM attributes. On these devices, security policies are applied against firewall zones to determine what is permitted through these zones. The security configuration approach defers based on the platform. On the CSR 1000V, zone pairs are configured to represent the relationship between two firewall zones with one zone being the Source Zone and other the Destination Zone. Security policy maps are applied on these zone pairs and the action can be inspect, pass, drop, or reset depending on if this is an application security policy map. Also, security class maps are configured and used to match traffic that needs to be allowed through the security zones. These security class maps are applied to the security policy map that is used in the zone pairs.

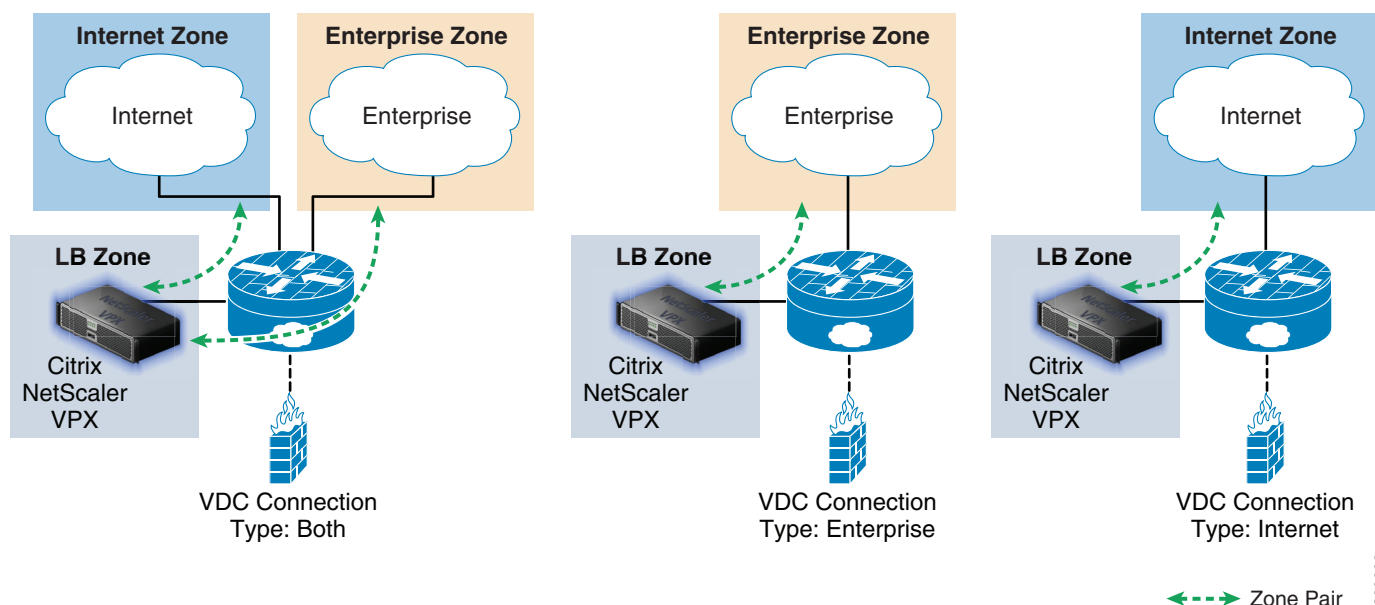
The VSG is used to protect VMs and it uses ACLs to determine what is permitted to and from the VMs. With the Cisco VSG, these zones regarded as vZones can be used in either source or destination condition in the creation of security ACL. Only network addresses are configured as members of a vZones by IAC.

The PNSCs are used to manage the VSG and CSR 1000V. These devices must be registered to the PNSC to be managed. Once registered, these devices can be assigned to a Tenant (an object in PNSC representing an owner of compute and network resources). IAC uses the PNSC to configure the security policies on these virtual appliances in use by a Tenant. IAC does this by leveraging the northbound XML Restful API provided by the PNSC appliance and uses these API to configure all security policies required on the virtual appliance.

An IAC Tenant must create an Organization to have access to cloud resources. During creation of an Organization, all virtual appliance are instantiated and registered to the PNSC with exception of Citrix NetScaler VPX. PNSC 3.2 and later supports the management of the Citrix NetScaler 1000V and IAC support will be available in a future release. After the virtual appliances are registered, IAC configures default security zone policies on the CSR 1000V. These security policies are dependent on the following options:

- VDC connection type. Connection methods used to access the VDC resources. This could either be Enterprise, Internet, or Both (Internet & Enterprise). This option can be selected during onboarding of the Tenant or creation of an Organization. The available option during Organization creation depends on option selected during Tenant onboarding.
- Load Balancing Services. Adding an appliance that load balances requests to VMs in the VDC. This option can be selected during Tenant onboarding or creation of an Organization
- VDC Service Type. Type of VDC added to the Tenant Org. IAC provides the following options:
  - Four-Zone Gold
  - Two-Zone Enterprise Gold
  - Two-Zone Internet Gold
  - Two-Zone Enterprise Silver
  - Two-Zone Internet Silver
  - One-Zone Enterprise Bronze
  - One-Zone Internet Bronze
- Other. Available VDC service types are dependent on the VDC connection type selected during Tenant onboarding and Organization creation.

The goal of security policies configured by IAC is to ensure that allowed communication between network segments are permitted. [Figure 4-20](#) shows the default security zones on the CSR 1000V after creation of an IAC Organization. VSG security policies are configured during creation of a VDC in IAC.

**Figure 4-20** Default Security Zones on the CSR 1000V

296603

## Security Policies Configured During Organization Creation

All security policies at this stage are configured on the CSR 1000V. There is no security policy configured on the VSG.

## CSR 1000V Security Class Maps Created with Organization Ordering

Security class maps are used to match IP address traffic that is inspected. During Organization ordering, these class maps are configured on the CSR 1000V to match traffic destined to the vServer IP address and return traffic from the Citrix NetScaler VPX back to the clients. Security ACLs are used to define traffic destined to the vServer IP address and return traffic from the vServer IP address back to the clients. As a result, four class maps are configured on the CSR 1000V if the VDC connection type is Both, and two class maps are configured if the VDC connection type is either Enterprise or Internet.

## CSR 1000V Security Policy Maps Created with Organization Ordering

Security policy maps are configured to determine what action to take against traffic that is matched when moving between two security zones. During Organization ordering, IAC configures security policy maps that pass traffic destined to or coming from the Citrix NetScaler VPX vServer IP address. As a result, four security policy maps are configured on the CSR 1000V if the VDC connection type is Both, and two policy maps are configured if the VDC connection type is either Enterprise or Internet.

## CSR 1000V Security Zones Created with Organization Ordering

The following are the security zones configured on the CSR 1000V upon creation of an IAC Organization:

- **Enterprise Zone.** Security zone that is assigned to the Enterprise facing interface on the CSR 1000V. This zone is configured if either VDC connection type Both or Enterprise is selected during Organization ordering.
- **Internet Zone.** Security zone that is assigned to the Internet facing interface on the CSR 1000V. This is configured if either VDC connection type Both or Internet is selected.

- LB\_<TenantAbbreviation>CSR<RuntimeID>. Security zone assigned to the NetScaler VPX facing interface on the CSR 1000V. Tenant abbreviation is the four character description given during ordering of a Tenant, while RuntimeID is the requisition number associated with the ordered Organization.

### CSR 1000V Security Zone Pair Configuration Created with Organization Ordering

The following zone pairs are configured on the CSR 1000V when an IAC Organization is ordered:

- A zone pair for communication between the Internet Zone and the zone assigned to the NetScaler VPX interface on the CSR 1000V. This zone pair is created if either the VDC connection option is Both or Internet. For this zone pair, the security policy is to pass matched traffic. A reverse security zone pair is also required since a pass policy is used.
- A zone pair for communication between the Enterprise Zone and the zone assigned to the NetScaler VPX interface on the CSR 1000V. This zone pair is selected if either the VDC connection type is Both or Enterprise. For this zone, the security policy is to pass matched traffic. A reverse security zone pair is also required for return traffic from the NetScaler VPX interface of the CSR 1000V to the Enterprise.

### Firewall Service Group Usage by IAC

Firewall service groups in IAC are group of TCP or UDP ports that can be used to create firewall rules in IAC. These ports can be used as part of source or destination condition in the creation of these rules. These service groups are configured as a port object group in the PNSC.

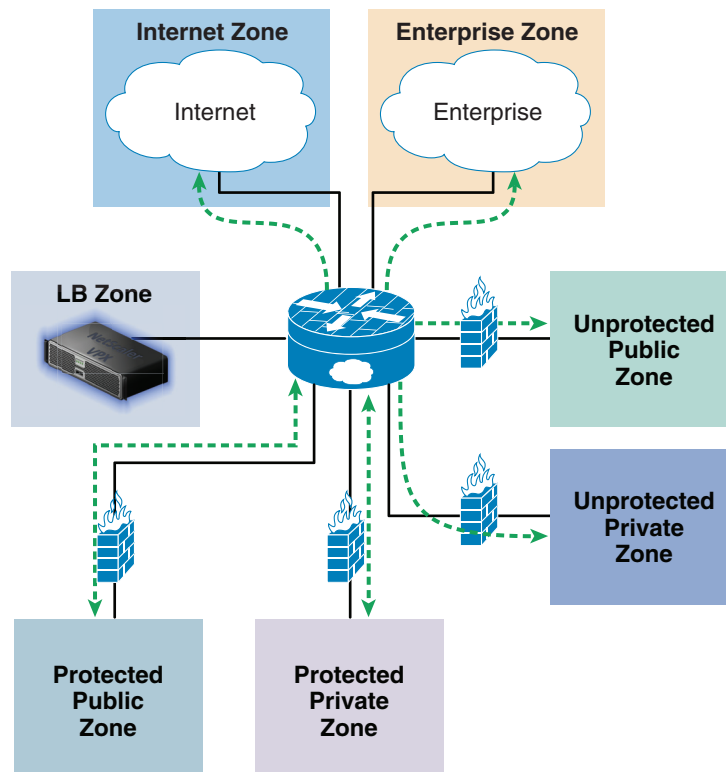
provides information on the ports included in default firewall service group created by IAC during Organization ordering.

**Table 4-1** Firewall Service Group Created During Organization Ordering

Firewall Service Group Name	TCP Ports	UDP Ports
Web	80, 443	N/A
Database (Oracle)	1521	N/A
Database (MySQL)	3306	N/A
Database (Microsoft)	1433	N/A
Database (PostGRES)	5432	N/A
Remote Access	22, 3389, 5900	N/A
FTP	20, 21	N/A

### Security Policy Configured During Virtual Data Center Service Ordering

Figure 4-21 shows the network types available during VDC service ordering.

**Figure 4-21** Network Types Available During VDC Service Ordering

VDC Connection Type: Both  
VDC Service Type: 4-Zone Gold

296604

The following network types are available:

- Unprotected Public. Allows for unrestricted Internet access to resources contained in the network.
- Unprotected Private. Allows for unrestricted Enterprise access to resources contained in the network.
- Protected Public. Allows for restricted Internet access to resources contained in the network.
- Protected Private. Allows for restricted Enterprise access to resources contained in the network.

Table 4-2 shows the network types provided with each VDC Type.

**Table 4-2** Network Types Provided with Each Virtual Data Center Type

Service Type	Unprotected Public	Unprotected Private	Protected Public	Protected Private
Four-Zone Gold	Y	Y	Y	Y
Two-Zone Enterprise Gold	N	Y	N	Y
Two-Zone Internet Gold	Y	N	Y	N
Two-Zone Enterprise Silver	N	Y	N	Y
Two-Zone Internet Silver	Y	N	Y	N
One-Zone Enterprise Bronze	N	Y	N	N
One-Zone Internet Bronze	Y	N	N	N
Other	Y	Y	Y	Y

## CSR 1000V Security Policies Configured During Virtual Data Center Ordering

A zone is configured for each network type / interface added to the CSR 1000V during VDC ordering. By default, communication to and from the Unprotected network segments are permitted after VDC service creation. By default, IAC configures CSR 1000V security policies that allow communication through the following security zones:

- Enterprise to Unprotected Private
- Unprotected Private to Enterprise
- Internet to Unprotected Public
- Unprotected Public to Internet

Table 4-3 indicates the CSR 1000V zone security policies that are created with creation of a VDC service.

**Table 4-3** *CSR 1000V Zone Security Policies Created with Virtual Data Center Service*

Service Type	Internet > Unprotected Public & Unprotected Public > Internet	Enterprise > Unprotected Public & Unprotected Public > Enterprise
Four-Zone Gold	Y	Y
Two-Zone Enterprise Gold	N	Y
Two-Zone Internet Gold	Y	N
Two-Zone Enterprise Silver	N	Y
Two-Zone Internet Silver	Y	N
One-Zone Enterprise Bronze	N	Y
One-Zone Internet Bronze	Y	N
Other	Y	Y

## VSG Security Policies Configured During Virtual Data Center Ordering

A vZone is created containing the network address for each network segment created during VDC ordering. These vZone are used in creation of the some of the VSG ACL policies used to protect the VM. IAC configures VSG ACL policies during VDC ordering to permit the following communication

- Communication between VM belonging to the same network segment (Intra-vZone ACL)
- Communication from the CSR 1000V interface to the VM network (CSR 1000V interface ACL)
- Explicit permit all (explicit permit ACL)
- Explicit deny of all communication to the network segment (explicit deny ACL)

Table 4-4 indicates the VSG ACL that are created during VDC service creation for each network segment.

**Table 4-4** *VSG ACL Created During Virtual Data Center Service Creation*

Network Type	Intra-Zone ACL	CSR 1000V Interface ACL	Explicit Permit	Explicit Deny
Unprotected Public	N	N	Y	N
Unprotected Private	N	N	Y	N

Network Type	Intra-Zone ACL	CSR 1000V Interface ACL	Explicit Permit	Explicit Deny
Protected Public	Y	Y	N	Y
Protected Private	Y	Y	N	Y

## Firewall Management in IAC

The following restrictions are applicable with IAC firewall management:

- IAC does not provide an option to individually manage security policies on the VSG and CSR 1000V.
- Firewall management tasks are only configurable by a user with the proper privileges.
- Log into the security device or PNSC to view actual security configuration.
- Only TCP and UDP protocols are supported during firewall rule creation
- Range operator “-” is not currently supported for firewall rule creation.
- The following network destination types are supported: server, server group, network, and zones.

The following configuration examples provide information on how to manage firewall service groups.

### View or Create Firewall Service Group

Complete the following steps to view or create a firewall service group:

- 
- Step 1** Log into the IAC Request Center as either CPTA/TTA/OTA.
  - Step 2** Select Organization Management.
  - Step 3** Select the Firewall tab. The available service groups are shown.
  - Step 4** Select Create Service Group.
  - Step 5** Complete the required form and submit the request.

### Firewall Service Group Management

Complete the following steps to manage the firewall service group:

- 
- Step 1** Log into the IAC Request Center as either CPTA/TTA/OTA.
  - Step 2** Select Organization Management.
  - Step 3** Select the Firewall tab.
  - Step 4** Select the firewall service group to manage.
  - Step 5** Select any of the following tasks:
    - a. Add member to Service Group to add additional ports to the service group.
    - b. Manage Service Group Membership to remove or add a port or ports in a service group.
    - c. Delete Service Group to delete a firewall service group.
  - Step 6** Make the required modification and click Submit.

IAC allows the user to perform the following tasks with server groups:

- Create firewall server group
- Add servers to firewall server group



- Delete firewall server group

Server groups can be created at the Organization level in the following locations in the Request Center portal:

- Tenant Management / Organization Management page
- My VDC resource on the My Cloud page

### Create Firewall Server Group

Complete the following steps to create a firewall server group:

- 
- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
- Step 2** If logged in as non-OTA, then do the following:
- a. Select Tenant Management, which bring up the web page associated with this resource.
  - b. On the left side of the Request Center portal under Tenants and Organization, click the > sign to view the Organizations under the current Tenant.
  - c. Select the Organization.
  - d. Click Server Group.
  - e. Select Create Server Group.
  - f. Add the required server groups details.
  - g. Create a firewall rule to permit required communication to server group.
- Step 3** If logged in as OTA, then do the following:
- a. Select Organization Management. This step can also be done by the CPTA/TTA.
  - b. Select Server Group.
  - c. Click Create Server Group.
  - d. Add the required server group details.
  - e. Create a firewall rule to permit required communication to the server group.

### Remove a Server Group

Complete the following steps to remove a server group:

- 
- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
- Step 2** Select My VDC on the My Cloud tab.
- Step 3** Select the details tab for the VDC that contains the server group.
- Step 4** Select Delete Server Group.
- Step 5** Select the server group to delete from the drop-down list.
- Step 6** Submit the request.

### Add a Server to the Firewall Server Group

Complete the following steps to add a server to the firewall server group:

- 
- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
- Step 2** Select My Servers on the My Cloud tab.

- Step 3** Select the Details tab for the server to be added.
- Step 4** Select Add to Server Group.
- Step 5** Submit the request.

#### Remove a Server from a Firewall Server Group

---

- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
- Step 2** Select My Servers on the My Cloud tab.
- Step 3** Select the Details tab for the server to be removed,
- Step 4** Select Remove from Server Group.
- Step 5** Submit the request.

## Virtual Data Center Firewall Management

VDC firewall rules are used to configure what is allowed to access VDC resources and from where this access should be granted. These VDC resources could be applications running on VM and request for these resources could come from the Enterprise, Internet or could come from resources located within the Organization, e.g., resource request from the Citrix NetScaler VPX or VMs located in a different network segment. In most cases, to permit access to resources not initially allowed during VDC ordering, a VDC firewall rule must be created. VDC firewall policies are located under the My VDC tab in the IAC Request Center portal. The following are conditions used in creation of a VDC firewall rule:

- Enterprise. A specific network or any network reachable through the Enterprise interface of the Organization CSR 1000V.
- Internet. A specific network or any network reachable through the Internet interface of the Organization CSR 1000V.
- Single Server. A single server located in a VDC network
- Server Group. A group of servers located in a VDC network.
- Network. A network address assigned to a VDC network.
- Zone. Any of the four zones that can be created by IAC during VDC creation.
- Service Type. Port allowed in this firewall rule. Options available include Any, Single Port, and Service Group. A new firewall service group can be created as part of VDC firewall rule creation.

IAC currently supports all of these options as source conditions while only Single Server, Server Group, Network and Zone are supported as destination conditions during creation of a VDC rule.

The following tasks can be done in IAC as part of management of VDC firewall rules:

- Create a VDC firewall rule
- Delete a VDC firewall rule

#### Add a VDC Firewall Rule

Complete the following steps to add a VDC firewall rule:

- 
- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
  - Step 2** Select My VDC on the My Cloud tab.

- Step 3** Select the Details tab for the VDC.
- Step 4** Select Create VDC Firewall Rule. As shown in [Figure 4-22](#), the current configured firewall rules are shown under applied firewall rules.
- Step 5** Add the required entries, taking into consideration that the right source and destination condition should be chosen for an effective firewall security policy for the VDC.
- Step 6** Submit the request.

**Figure 4-22** Current Configured Firewall Rules

**Create VDC Firewall Rule**

This service creates a new firewall policy from the MyVDC Popout.

**Firewall Rule Details**

Rule Name:

Action: **permit**

VDC Name: **VDC\_2**

Source Type: **---**

Destination Type: **---**

Service Type: **Any**

**Service Group**

FriendlyName	SourceType	Source	DestinationType	Destination	ServiceType	Service
app_80	Network	protected_app_network	Server Group	Any	Any	Any
app_internet_80	Server Group	app_80	Single Server	Any	Service Group	Cust_2_Internet_Web_Ports
test_int_80	Network	Second Network	Any External (Internet)	Any	Any	Any
p_web_app_80	Network	Fourth Network	Network	protected_app_network	Service Group	Cust_2_Ent_Ports
ent_app_80	External Subnet (Ente...	protected_app_network	Network	protected_app_network	Service Group	Cust_2_Ent_Ports
db_80	Network	protected_db_network	Server Group	Any	Any	Any

Submit Order | Reset

296605

### Remove a VDC Firewall Rule

Complete the following steps to remove a VDC firewall rule:

- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
- Step 2** Select My VDC on the My Cloud tab.
- Step 3** Select the Details tab for the VDC.
- Step 4** Select Delete VDC Firewall Rule.
- Step 5** Select the appropriate VDC firewall rule from the rule name drop-down list.
- Step 6** Submit the request.

## VM Firewall Rule Management in IAC

IAC allows you to create the following firewall rules with the VM:

- Create a VM firewall rule
- Delete a VM firewall rule

### Create a VM Firewall Rule

Complete the following steps to create a VM firewall rule:

- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
- Step 2** Select My Servers on the My Cloud tab.

- Step 3** Select the Details tab for the VM to be associated with the server
- Step 4** Select Create VM Firewall Rule. As shown in [Figure 4-23](#), the current applied VM firewall rules are shown under the applied firewall rule.
- Step 5** Add the required entries.
- Step 6** Submit the request.

**Figure 4-23** Current Applied VM Firewall Rules

Create VM Firewall Rule

This service creates a new firewall policy.

**Virtual Machine**

Server Name: test-vm1111

**Firewall Rule Details**

Rule Name:

Action:

Source Type:

Service Type:

**Service Group**

Rule Name	Source Type	Source	Destination Type	Destination	Service Type	Service
test-rule	Any External (Internet)	Protected Public	Single Server	test-vm1111	Service Group	Web

Submit Order Reset

296606

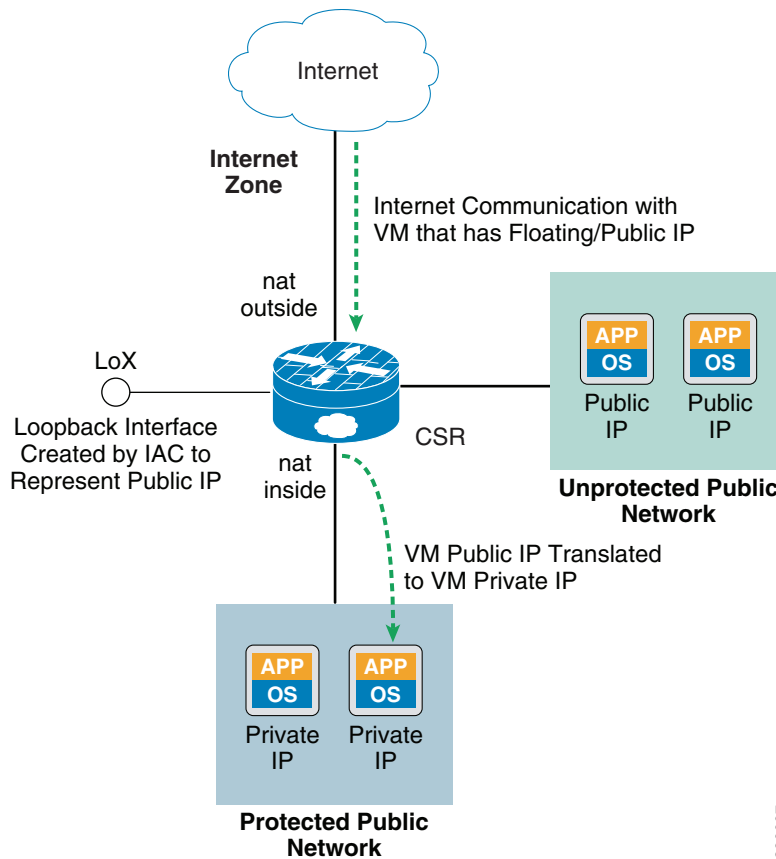
### Remove a VM Firewall Rule

Complete the following steps to remove a VM firewall rule:

- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
- Step 2** Select My Servers on the My Cloud tab.
- Step 3** Select the Details tab for the VM to be associated with the server.
- Step 4** Select Delete VM Firewall Rule.
- Step 5** Select the rule from the drop-down list.
- Step 6** Submit the request.

## NAT/Floating IP Service Management

Network Address Translation (NAT) is used to translate IP address of a host as it's traffic crosses a network boundary. In NAT, the network boundary is represented by the Inside Network and Outside Network, and the device providing this service should have an interface in each network. The host address can be translated to a static or dynamic address and conditions using an ACL to specify the condition that must be met in order for NAT to occur. [Figure 4-24](#) shows the NAT configuration.

**Figure 4-24 NAT Configuration**

For IAC implementation, the NAT service can be used to enable hosts configured with Private (RFC1918) addresses to communicate with the Internet. In this case this service makes sense for IAC Tenants that have an Internet VDC connection and configured with a Two-Zone Internet Gold VDC service, since it is expected that VMs in the Protected Private networks can have Private IP addresses. For automation, IAC assumes that the Outside Network boundary and Inside Network Boundary for NAT are Internet and Protected Public Networks of the Tenant respectively. Also this NAT service is provided on a per-VM basis, and as a result, only static NAT of the VM IP address is provided in IAC.

NAT service is provided by the Tenant CSR 1000V. IAC uses PNSC for NAT configuration on the CSR 1000V. Note that dynamic NAT and static NAT are currently supported on the PNSC, while NAT overload translating hosts IP to a single IP is not supported. The Public IP address used for translation is advertised by the CSR 1000V to the Internet.

To enable NAT for a VM resource using IAC, use the Allocate Floating IP Address Service on the My Servers page. This service is only available for VMs that are located in a Protected Public network of a Gold VDC.

The following NAT automation tasks can be done:

- Allocate floating IP address
- Release floating IP address

The following restrictions are applicable with IAC NAT management:

- Dynamic NAT service is not currently supported.
- NAT management tasks are only configurable by a user with the proper privileges.

- Log into the CSR 1000V or PNSC to view the actual NAT configuration.
- The NAT option is only provided for a VM located in the Protected Public network.

#### Allocate a Floating IP Address

Complete the following steps to allocate a floating IP address:

- 
- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
  - Step 2** Select My Servers on the My Cloud tab.
  - Step 3** Select the Details tab for the VM to be associated with the server.
  - Step 4** Select Allocate Floating IP Address.
  - Step 5** Submit the request.

#### Remove a Floating IP Address

Complete the following steps to remove a floating IP address:

- 
- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
  - Step 2** Select My Servers on the My Cloud tab.
  - Step 3** Select the Details tab for the VM with the floating IP address.
  - Step 4** Select Release Floating IP Address.
  - Step 5** Submit the request.

## Load Balancing Service Management in IAC

Most cloud / data center providers use application load balancers to efficiently distribute and offload client application requests to and from server resources in their data center. These appliances typically run faster application algorithms, faster application hardware and cache engines thereby enabling the data center provider to optimize the application response times. Clients accessing this resource have a better experience.

IAC uses the Citrix NetScaler VPX to provide LB services to onboarded Tenants. The Citrix NetScaler VPX is inserted in the Tenant network in one-arm mode. In this mode, IAC configures the Citrix NetScaler VPX to have a single network interface that is used to communicate with all server resources. The Tenant CSR 1000V is used to route between the Citrix NetScaler VPX and the server networks. To ensure that all load balanced client requests replied by the servers are received at the LB before being forwarded to the clients, these client IP addresses are translated to NetScaler IP addresses called Subnet IP (SNIP) addresses when they are forwarded to the servers. To ensure that load balanced client requests are received on the NetScaler VPX, the client requests must be destined to the vServer IP address. A vServer is used to represent a set of servers that provide the same application resource that client are trying to access.

As part of the load balancing configuration on the NetScaler VPX, a service or service group must be configured. A service is an object that associates a server to an application resource e.g HTTP, HTTPS, SSL\_BRIDGE, FTP etc. A service group is an object that can be used to associate one or more servers to an application resource. This object is then associated / bound to a vServer configuration on the NetScaler VPX. IAC supports all service groups supported on the NetScaler VPX with the default being HTTP and HTTPS during Organization creation.

The Citrix NetScaler VPX uses Health Monitors to determine the status of a service/service group or vServer. If the object being monitored is active, then client requests are successfully load balanced. If the object being monitored is down, then client requests are dropped on the LB appliance. The health monitors continues to check the status of the service group and the response of these monitors determines if the LB maintains the current status or moves it to from a UP/DOWN state to DOWN/UP state. Several default health monitors are supported on NetScaler VPX and also custom defined monitors can be configured. IAC supports the following default health monitors

- PING. With this monitor, the NetScaler VPX sends ICMP echo requests and expects ICMP echo replies,
- HTTP. With this monitor, the NetScaler VPX sends HTTP Header Requests to the service/service group.
- HTTPS. With this monitor, the NetScaler VPX sends HTTPS Header Requests to the service/service group.

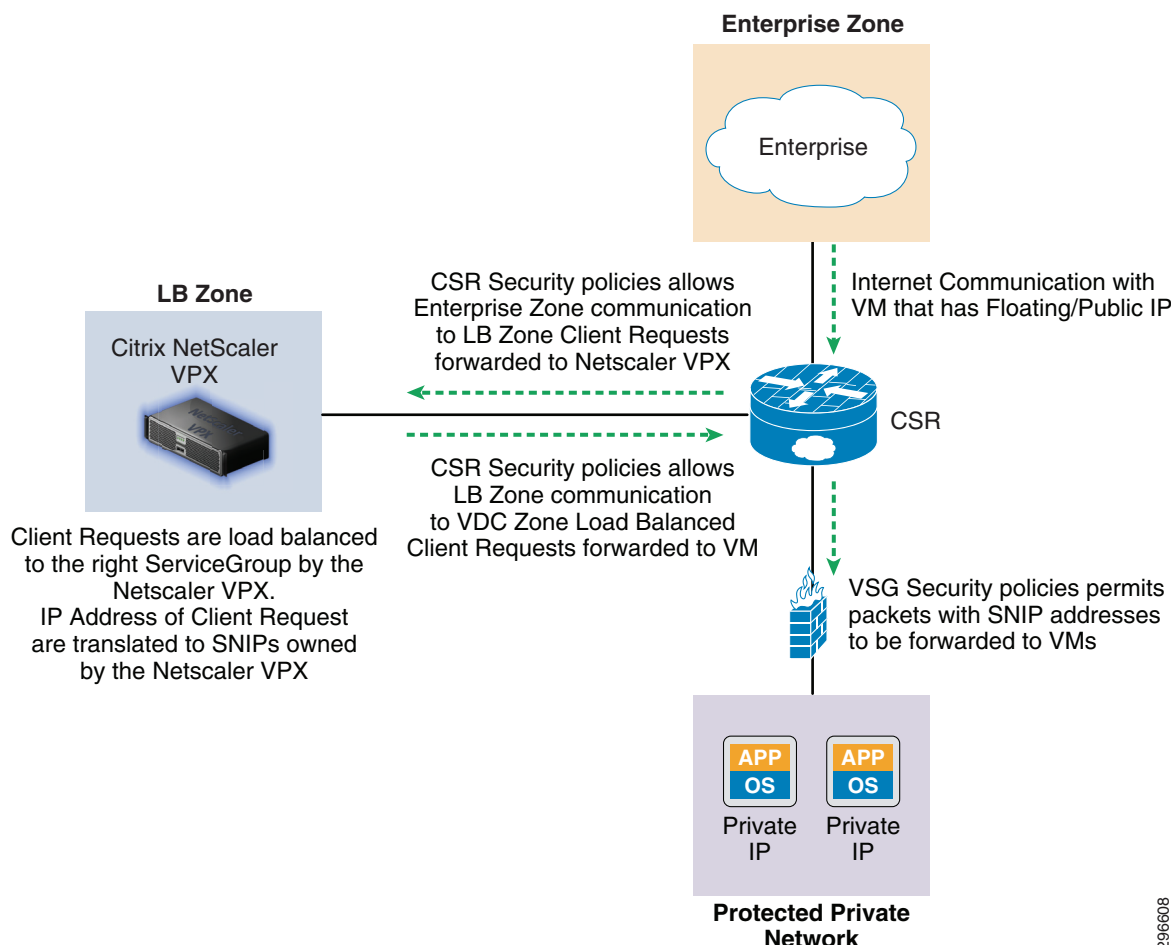
## Firewall Security Policies with Load Balancing Service

To ensure that load balanced requests successfully sent to the servers, appropriate security policies are configured on the CSR 1000V and VSG to permit these clients. The following security policies are configured

- CSR 1000V security zone policies to permit client requests to the NetScaler VPX from Internet and Enterprise Interfaces of the CSR 1000V
- CSR 1000V security zone policies to permit client requests sent from the NetScaler VPX to the servers. The source address of these client request are SNIP addresses configured on the NetScaler VPX.
- VSG security policies to permit client requests to the servers

These security policies are configured when IAC creates a vServer IP address and binds a VM to a vServer.

Figure 4-25 shows the path taken and security policies required for effective load balancing of Enterprise client requests to a LB VIP address on the NetScaler VPX.

**Figure 4-25 Enterprise Client Request to a LB VIP Address on the NetScaler VPX**

## NetScaler VPX Routing and Address Types in IAC

As stated earlier, the Tenant NetScaler VPX is deployed and configured in one-arm network mode. Static routing is used for reachability to and from the NetScaler VPX. The NetScaler VPX has a default route with the gateway being the Tenant CSR 1000V interface. This route is configured during the initial setup of the NetScaler VPX.

IAC also configures a specific static route to the Process Orchestrator (PO), since this is the IAC component that configures the NetScaler VPX. Every time a new NetScaler VPX vServer IP address is added, IAC configures static routes to this address as well as static routes to the SNIP associated with this vServer.

When using IAC, the NetScaler VPX IP can either be Public (non RFC 1918 address) or Private (RFC 1918 address). When binding a VM to a vServer, the address type of the vServer determines the VDC connection where client requests are received, and hence, it makes sense to bind VM in the Protected and Unprotected Public networks to a Public vServer and VM in the Protected and Unprotected Private networks to a Private vServer.

## Load Balancing Management in IAC

The following LB management tasks can be performed in IAC:



- Create LB server
- Create LB service group
- Bind VM to LB server
- Delete LB server
- Delete LB service group
- Unbind VM from LB server

These tasks assume that the Tenant is created with the Advanced Network Service option and that the LB service is enabled.

The following restrictions are applicable with IAC NAT management

- NetScaler VPX license management is not supported, and hence, the required NetScaler VPX feature, e.g., LB, is disabled .
- SSL offload service is currently not supported.
- SSL-BRIDGE service group type is used to provide support for HTTPS load balancing. Actual use of HTTPS service group type is not supported due to lack of NetScaler VPX certificate management support by IAC.

The following service groups types have been tested and validated:

- HTTP
- SSL-BRIDGE

Only HTTP, HTTPS, and PING health monitors are supported. LB service group management is not supported.

## Create LB Server During Organization Creation

Complete the following steps to create an LB server during Organization creation:

- 
- |               |  |
|---------------|--|
| <b>Step 1</b> | Log into the Request Center portal as either CPTA/TTA/OTA.   |
| <b>Step 2</b> | Select Tenant Management.  |
| <b>Step 3</b> | If logged in as CPTA, then select the Tenant.  |
| <b>Step 4</b> | Select Create Organization.  |
| <b>Step 5</b> | Add the required entries for General Organization information, VDC Connection Type, and Set Organization-wide Service options. Note that the Advanced Network Service option and LB service should be enabled. Also, select the Virtual Network Service Resource to use.   |
| <b>Step 6</b> | Complete the required entries for Add Load Balancer for HTTP and HTTPS. Note the following: <ul style="list-style-type: none"> <li>a. Load Balancing Server. Friendly name used to represent the vServer.</li> <li>b. IP Address Type. IP address type assigned to the vServer. Note that the Public and Private options are available if the Organization's VDC has both an Enterprise and Internet connection. Only Private or Public IP address types are available with either an Enterprise or Internet VDC connection respectively.</li> <li>c. Method. Load balancing distribution method in use.</li> <li>d. Least Response Time. Allows the NetScaler VPX to distribute load based on response time values of the health monitors. A new client request is sent to a server with least response time to health monitors.</li> </ul> |

- e. Least Request. Allows the NetScaler VPX to distribute load based on active requests on the server. A new client request is sent to a servers with few client request.
- f. Round Robin. Allows the NetScaler VPX to distribute load equally on all servers. A new client request is sent to the next server
- g. Least Connection. Allows the NetScaler VPX to distribute load based on active connections on the server. A new client request is sent to a servers with few active connections.
- h. Service Group. Service group to be associated with the server. Only HTTP and HTTPS are provided during Organization creation. The same service group can be used for the two LB servers.

**Step 7** Submit the request.

## Create a LB Server from My VDC

Complete the following steps to create a LB server from My VDC:

- 
- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
  - Step 2** Select the My Clouds tab.
  - Step 3** Select My VDC.
  - Step 4** Select Manage Load Balancers.
  - Step 5** Select Create. The following tasks can be performed:
    - Create virtual IP address
    - Use existing virtual IP address
  - Step 6** If creating a new VIP address, then add the required entries and submit the request. If using an existing VIP address, then select the appropriate friendly name from the LB Server drop- down list and submit the request.

## Create a LB Service Group

Complete the following steps to create a LB service group:

- 
- Step 1** Log into the Request Center as either CPTA/TTA/OTA.
  - Step 2** Select Tenant Management.
  - Step 3** If logged in as CPTA or TTA, then navigate to the Tenant and Organization.
  - Step 4** Select Service Group on the Tenant Management page.
  - Step 5** Select Load Balancer.
  - Step 6** Select Create Service Group.
  - Step 7** Add the required entries and submit the request. The following should be noted:
    - Protocol refers to the application type used to represent the resource provided by the servers, e.g., HTTP, HTTPS, etc.
    - Port refers to the port on which the application listens.
    - Monitor refers to the health monitor. IAC only supports HTTP, HTTPS, and PING.

## Bind VM to the LB Server

Complete the following steps to bind the VM to the LB server:

- 
- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
  - Step 2** Select My Cloud.
  - Step 3** Select My Servers.
  - Step 4** Select the details tab for the VM.
  - Step 5** Select Manage Load Balancer.
  - Step 6** Select the appropriate name requesting the LB server.
  - Step 7** Submit the request.

## Unbind VM from LB Server

Complete the following steps to unbind the VM from the LB server:

- 
- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
  - Step 2** Select My Cloud.
  - Step 3** Select My Servers.
  - Step 4** Select the details tab for the VM.
  - Step 5** Select Manage Load Balancer.
  - Step 6** Select the appropriate name from the drop-down list for the LB server to remove.
  - Step 7** Submit the request.

## Remove LB Server

Complete the following steps to remove the LB server:

- 
- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
  - Step 2** Select My Cloud.
  - Step 3** Select My VDC.
  - Step 4** Select Manage Load Balancers.
  - Step 5** Select Remove.
  - Step 6** Select the appropriate name from the drop-down list for the LB server.
  - Step 7** Submit the request.

## Remove LB Service Group

Complete the following steps to remove the LB service group:

- 
- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.

- Step 2** Select Tenant Management.
- Step 3** If logged in as CPTA or TTA, then go to Tenant > Organization.
- Step 4** Select Service Group from the Tenant Management page.
- Step 5** Select Load Balancer.
- Step 6** Select the details tab for the VM.
- Step 7** Select Delete Load Balancer Service Group.
- Step 8** Select Delete.

## Network Service Management

The VDCs created in IAC are made of networks, and Tenant virtual servers are located in these networks. VDC access is provided by the CSR 1000V. As a result, the maximum number of interfaces possible on the CSR 1000V bounds how many networks a VDC can have. When deploying a CSR 1000V, four interfaces are pre-assigned for the Management, Internet, Enterprise, and NetScaler VPX connections, irrespective of whether these connections are required at the Organization level. A VDC in can have up to six networks. In a Four-Zone, Two-Zone, and One-Zone VDC, there can be up to two, four, and five additional networks added. This is due to virtual hardware limitations of the VMware Hypervisor.

An IAC customer may want to add networks to a VDC if there is a need to increase the number of network segments. For example, to provide a three-tier service located in different Private network segments, a user can two additional networks to a VDC. Each VDC network must belong to an IAC firewall zone. The firewall zones available when adding a network to a VDC include the following:

- Unprotected Public. Allows for unrestricted Internet access to resources contained in this network.
- Unprotected Private. Allows for unrestricted Enterprise access to resources contained in the network
- Protected Public. Allows for restricted Internet access to resources contained in the network
- Protected Private. Allows for restricted Enterprise access to resources contained in the network

As with VDC ordering, when a network is added to a VDC, the applicable security policies are configured on the CSR 1000V and VSG to ensure either unrestricted or restricted access to the network resources.

The following network management tasks can be performed:

- Add network to VDC
- Remove network from VDC

The following restrictions apply with VDC network management in IAC:

- A VDC can only have six networks.
- CSR 1000V interfaces are not removed when networks are remove from a VDC. These interfaces are placed in a VMware quarantine port group.

## Add Network to VDC

Complete the following steps to add a network to the VDC:

- 
- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
  - Step 2** Select My Cloud.

- Step 3** Select My VDC.
- Step 4** Select the details for the VDC.
- Step 5** Select Add Network to VDC.
- Step 6** Add the required entries.
- Step 7** Submit the request.

## Remove Network from VDC

Complete the following steps to remove a network from the VDC:

- 
- Step 1** Log into the Request Center portal as either CPTA/TTA/OTA.
  - Step 2** Select My Cloud,
  - Step 3** Select My VDC.
  - Step 4** Select the details for the VDC.
  - Step 5** Select Remove Network from VDC.
  - Step 6** Select the network to be removed from the drop-down list.
  - Step 7** Submit the request.





## Related Documents

---

The VMDC design recommends that general Cisco data center design best practices be followed as the foundation for Infrastructure as a Service (IaaS) deployments. The companion documents listed in this appendix provide guidance on such a foundation.

### **Cisco Intelligent Automation for Cloud 4.0**

- [Cisco Intelligent Automation for Cloud Documentation Set](#)
- [Cisco Intelligent Automation for Cloud 4.0 Documentation Overview](#)
- [Cisco Intelligent Automation for Cloud Compatibility Matrix](#)
- [Cisco Intelligent Automation for Cloud 4.0 Quick Start Guide](#)
- [Cisco Intelligent Automation for Cloud 4.0 Installation Guide](#)
- [Cisco Intelligent Automation for Cloud Administrator Guide](#)
- [Cisco Intelligent Automation for Cloud User Guide 4.0](#)

### **VMDC VSA 1.0**

- [VMDC VSA 1.0 Design Guide](#)
- [VMDC VSA 1.0 Implementation Guide](#)
- [VMDC VSA 1.0 Proof of Concept Orchestration Guide](#)
- [VMDC VSA 1.0.2 Implementation Guide](#)







## Limitations, Restrictions, Caveats

---

The following limitations, restrictions, and caveats should be noted when orchestrating the Virtualized Multiservice Data Center (VMDC) Virtual Services Architecture (VSA) 1.0 with the Cisco Intelligent Automation for Cloud (IAC) 4.0 solution.

- **Licensing.** The Cloud Services Router (CSR) 1000V is installed with a 90-day license and the VPX is installed with a demo license. Both of these licenses need to be upgraded manually. The Nexus 1000V should have the proper license to support the Virtual Security Gateway (VSG).
- **Port Group Discovery Inefficiency.** One of the items noticed during validation that has impacted performance is the port group discovery process on the Process Orchestrator (PO). There have been a few port group discovery issues discovered and resolved. Before a lot of tasks, for example creating or adding a Virtual Data center (VDC), can be completed, IAC runs a port group discovery process against the known port groups in the database. There is the potential of thousands of port groups that need to be looked up every time.
- **CSR 1000V Interface Limitation.** Interfaces on the CSR 1000V are limited to ten. This is a result of the VMware vCenter limitation of ten vNICs per Virtual Machine (VM).
- **VDC Limitation.** The limitation of the number of interfaces on the CSR 1000V directly impacts the number of VDCs that can be created in an Organization. After an Organization is created, there are only six interfaces available for VDC creation.
- **Redundant Virtual Services.** When onboarding a Tenant, do not select “High Availability” under “Set Tenant-wide Service options.” HA for virtual network services is unsupported in this release and not validated in this deployment.
- **Multi-Tenancy Naming.** There are some limitations to multi-tenancy when it comes to naming. The same user names cannot be used across multiple Tenants, and the same VDC name cannot be used across multiple Tenants. If UserA exists in TenantA, then UserA cannot be used in TenantB. A message warning that the user name is not available appears. The same happens if there is a VDC named VDC1 in TenantA. If TenantB tried to create a VDC with the name VDC1, then a message appears stating that this name has been used.
- **Cisco Discovery Protocol (CDP) Discovery Issue.** During network discovery, IAC may not discover all of the interconnects. If after running network discovery there are some missing interconnects, then there are a couple of options. Log into all of the network devices and issue the clear cdp table command and re-run the network discovery process. Another option is to reboot the IAC Management Appliance and re-run the network discovery process.
- **Nexus 1000V/VSG.** The Nexus 1000V needs to be configured to accommodate installing the VSG in Layer 3 (L3) mode. This includes the proper license, proxy-arp capable gateway router, increased MTU size (1594), and port profile with L3 control and L3-vService capabilities.

- Network Devices. There are a few things that IAC expects to be configured on the network devices to allow network provisioning:
  - Simple Network Management Protocol (SNMP) enabled, v2c or v3
  - SSH enabled
  - CDP enabled
  - Port channels with a switchport trunk allowed vlan statement
- A TTA/OTA is not able to re-activate user login accounts that they deactivated. To do so, they have to contact the CPTA, who can do it from the User Management page in the Organization Designer portal.
- IAC does not automatically enable Remote Desktop Protocol (RDP) on deployed Windows servers. Do one of the following tasks to gain remote access to the servers:
  - For a VM cloned from a template, make sure that the base template has RDP enabled.
  - For a VM deployed with the Service Provisioner (SP), open the VM console from vCenter and enable RDP.
  - For a physical server, open the KVM console from the Unified Computing System Manager (UCSM) and enable RDP.



## Defects

---

The following defects are planned to be fixed in the Cisco Intelligent Automation for Cloud (IAC) 4.1 release:

- CSCuo11557 IAC is stuck in Create Org Automation Tasks. A status update between the PO and PSC may timeout, causing the order to be stuck indefinitely.
- CSCuo13988. Tenant VDC quota not enforced. Able to exceed Tenant agreement on the number of VDCs allowed per Tenant.
- CSCuo46255. Virtual Machine Provisioning time too long. When provisioning a Virtual Machine (VM) from a template, the sleep timers may be longer than necessary.
- CSCuo46430. Organization / VDC Creation time is too long. Provisioning time for a new Organization and an attached VDC should take under an hour.
- CSCuo52120. IAC should restrict adding networks when VDC max is reached. IAC doesn't indicate that a user has tried to add a network to a VDC beyond a 6 network interface limit.
- CSCuo57301. Decommission VM while member of Server Group does not delete CSR config. When decommissioning a VM while it is a member of a server group, IAC does not delete any of the related configurations on the CSR 1000V.
- CSCuo60078. Entries in PNSC not getting removed when off boarding a Tenant. Tenant should also be removed from PNSC when deleting a Tenant.
- CSCun54029. Prevent the on-boarding of a previously existing Tenant. There should be a check to ensure CPTA cannot use a name that has previously existed.
- CSCun63287. FW rule created on one VM applied to same Org VMs with same name. Use the unique host name assigned to each VM for firewall rule creation instead of using friendly names.
- CSCuo65369. VDC Error Remediation creates additional duplicate interfaces. Error Remediation creates additional duplicate interfaces when either trying to retry a failed VDC creation as IAC will continue to try and add an Interface and assign it an IP address that IAC has already assigned.
- CSCun69052. TTA/OTA not able to re-activate user accounts that they deactivated. Provide TTA/OTA the ability to re-activate the users in their particular Tenant/Org from the User Management page.
- CSCun71781. MYSQL/MSSQL LB Service Group should have options for DB User & Password. IAC currently supports the configuration of MYSQL and MSSQL LB service group, however to get this working with the NetScaler VPX, you need to configure a DB user and password.
- CSCun73838. System Resource Capacity dashboard page often loads incorrectly. The page may load incorrectly with missing graphs and details.

- CSCun81970. Disable Manage Disk option in Order VM page. IAC user can add as many disks as possible in the Order VM page.
- CSCuo00068. Incorrect Network and Broadcast address configured on physical server. After provisioning a CentOS physical server, the config in the `/etc/sysconfig/network-scripts/ifcfg-eth0` has an incorrect broadcast and network address. It is assuming a /24 mask when you are actually using a /28.



## Configurations

---

This appendix presents the configurations used in the Virtualized Multiservice Data Center (VMDC) Virtual Services Architecture (VSA) 1.0 solution with the Cisco Intelligent Automation for Cloud (IAC) 4.0 release.

### Two-Zone Gold Container with Internet Transit

#### Org Creation for CSR 1000V, VPX, VSG

##### CSR 1000V

```
version 15.4
service timestamps debug datetime msec
service timestamps log datetime
no platform punt-keepalive disable-kernel-core
platform console virtual
!
hostname EXCPCSR23824
!
boot-start-marker
boot-end-marker
!
!
logging buffered critical
no logging console
no logging monitor
enable secret 5 $1$d mw9$tozXYZ/bxtIsRrcpUr/sd0
!
no aaa new-model
!
subscriber templating
!
multilink bundle-name authenticated
!
crypto pki trustpoint TP-self-signed-2413853978
  enrollment selfsigned
  subject-name cn=IOS-Self-Signed-Certificate-2413853978
  revocation-check none
  rsakeypair TP-self-signed-2413853978
!
crypto pki certificate chain TP-self-signed-2413853978
```

```

certificate self-signed 01
3082022B 30820194 A0030201 02020101 300D0609 2A864886 F70D0101 05050030
31312F30 2D060355 04031326 494F532D 53656C66 2D536967 6E65642D 43657274

69666963 6174652D 32343133 38353339 3738301E 170D3134 30343234 30333537
30375A17 0D323030 31303130 30303030 305A3031 312F302D 06035504 03132649
4F532D53 656C662D 5369676E 65642D43 65727469 66696361 74652D32 34313338
35333937 3830819F 300D0609 2A864886 F70D0101 01050003 818D0030 81890281
8100A036 5877E1F6 DAFA4CBC 2F687EA0 70FCA37A 1F843A2D 9F961814 2B8B1168
1213689E DAFED58A 3022A626 BA43DE21 D06D1465 9FD8AD7A BE049082 04C4E9B3
5FCE9B39 B3085217 E6908ABD 5435F5DC B7194CF6 0332C2DB EBC5440E 581304C0
A2D58F02 11AE327A EA67C82C 2BDC3A57 A0EF2A7A B30029B6 09783BDF BE694E7A
BCF10203 010001A3 53305130 0F060355 1D130101 FF040530 030101FF 301F0603

551D2304 18301680 1480C1E6 64701D2E 16D74B23 6FA88F5E 8C0AEE78 A6301D06
03551D0E 04160414 80C1E664 701D2E16 D74B236F A88F5E8C 0AEE78A6 300D0609
2A864886 F70D0101 05050003 8181003E 907E5131 7F05FD9C 1D0E318C D19F002A
4B20604D B0886D15 AF8C8796 C4555073 BBAA7501 8A45869C 2A2B2D41 3B85D053
683476DC 53F8376A D75EE4C6 15E6909D F57629BA 63C64109 F6665A27 A4B1E9A7
B5C09196 20F6DA3F CE833A41 FDCB8AD3 CEDFAAE8 AF9023A4 206C0AA7 B21946AA
D65DCCF6 E585F2B5 5CFA94F9 D3DC33
quit
remote-management
  pncsc host 192.168.7.246 local-port 8443 shared-secret
  fd[QHUPLCqIRMOB\[aaUdDfKBSCSXCSbAAAB
  license udi pid CSR1000V sn 9UWW0BJ0XM4
  license boot level advanced
!
username admin privilege 15 secret 5 $1$00/X$thgTQNNv1BfCXft4/t134/
!
redundancy
  mode none
!
ip ssh rsa keypair-name ssh-key
ip ssh version 2
!
class-map type inspect match-all LB_IN_Allow_d6f6792Int_CMAP
  match access-group name LB_IN_Allow_d6f6792Int_ACL
class-map type inspect match-all LB_OUT_Allow_646b1a2_CMAP
  match access-group name LB_OUT_Allow_646b1a2_ACL
class-map type inspect match-all LB_OUT_Allow_6d77354Int_CMAP
  match access-group name LB_OUT_Allow_6d77354Int_ACL
class-map type inspect match-all LB_OUT_Allow_d6f6792Int_CMAP
  match access-group name LB_OUT_Allow_d6f6792Int_ACL
class-map type inspect match-all LB_IN_Allow_646b1a2_CMAP
  match access-group name LB_IN_Allow_646b1a2_ACL
class-map type inspect match-all LB_IN_Allow_6d77354Int_CMAP
  match access-group name LB_IN_Allow_6d77354Int_ACL
!
policy-map type inspect VIP_LB_Internet
  class type inspect LB_IN_Allow_646b1a2_CMAP
    pass
  class type inspect LB_OUT_Allow_646b1a2_CMAP
    pass
  class type inspect LB_IN_Allow_6d77354Int_CMAP
    pass
  class type inspect LB_OUT_Allow_6d77354Int_CMAP
    pass
  class type inspect LB_IN_Allow_d6f6792Int_CMAP
    pass
  class type inspect LB_OUT_Allow_d6f6792Int_CMAP
    pass
  class class-default
!

```

```

zone security LB_EXCPCSR23824
zone security Enterprise
zone security Internet

zone-pair security EXCPCSR23824_LB_Internet source LB_EXCPCSR23824 destination Internet
service-policy type inspect VIP_LB_Internet

zone-pair security Internet_LB_EXCPCSR23824 source Internet destination LB_EXCPCSR23824
service-policy type inspect VIP_LB_Internet
!
interface VirtualPortGroup0
ip unnumbered GigabitEthernet1
!
interface GigabitEthernet1
ip address 192.168.74.242 255.255.255.0
negotiation auto
!
interface GigabitEthernet2
description configured by PolicyAgent
ip address 20.1.1.43 255.255.255.0
ip nat outside
ip access-group default-ingress in
ip access-group default-egress out
zone-member security Internet
negotiation auto
!
interface GigabitEthernet3
description configured by PolicyAgent
ip address 10.2.2.2 255.255.255.0
ip access-group default-ingress in
ip access-group default-egress out
zone-member security Enterprise
negotiation auto
!
interface GigabitEthernet4
description configured by PolicyAgent

ip address 192.168.4.1 255.255.255.0

ip access-group default-ingress in
ip access-group default-egress out
zone-member security LB_EXCPCSR23824
negotiation auto
!
router bgp 65500
bgp log-neighbor-changes
redistribute connected
redistribute static
neighbor 10.2.2.1 remote-as 109
neighbor 10.2.2.1 description Enterprise neighbor
neighbor 10.2.2.1 prefix-list Private-net-list out
neighbor 20.1.2.1 remote-as 109
neighbor 20.1.2.1 description Internet neighbor
neighbor 20.1.2.1 prefix-list Public-net-list out
!
virtual-service csr_mgmt
vnic gateway VirtualPortGroup0
guest ip address 192.168.74.243
activate
!
ip forward-protocol nd
!
no ip http server
ip http secure-server

```

```

ip route 0.0.0.0 0.0.0.0 GigabitEthernet1 192.168.74.1
ip route 192.168.7.0 255.255.255.0 GigabitEthernet1 192.168.74.1
ip route 192.168.74.243 255.255.255.255 VirtualPortGroup0
!
ip access-list extended LB_IN-Allow_646b1a2_ACL
 permit ip any host 64.100.1.247
ip access-list extended LB_IN-Allow_6d77354Int_ACL
 permit ip any host 64.100.4.192
ip access-list extended LB_IN-Allow_d6f6792Int_ACL
 permit ip any host 64.100.4.193
ip access-list extended LB_OUT-Allow_646b1a2_ACL
 permit ip host 64.100.1.247 any
ip access-list extended LB_OUT-Allow_6d77354Int_ACL
 permit ip host 64.100.4.192 any
ip access-list extended LB_OUT-Allow_d6f6792Int_ACL
 permit ip host 64.100.4.193 any
ip access-list extended default-egress
ip access-list extended default-ingress
!
ip prefix-list Private-net-list seq 10 permit 10.0.0.0/8 le 32
ip prefix-list Private-net-list seq 11 permit 172.16.0.0/12 le 32
ip prefix-list Private-net-list seq 12 permit 192.168.0.0/16 le 32
ip prefix-list Private-net-list seq 13 deny 0.0.0.0/0 le 32
!
ip prefix-list Public-net-list seq 10 deny 10.0.0.0/8 le 32
ip prefix-list Public-net-list seq 11 deny 172.16.0.0/12 le 32
ip prefix-list Public-net-list seq 12 deny 192.168.0.0/16 le 32
ip prefix-list Public-net-list seq 13 permit 0.0.0.0/0 le 32
!
control-plane
!
banner exec WARNING: This device is managed by Prime Network Services Controller. RESTful
API is read only. Changing configuration using CLI is not recommended.
banner login WARNING: This device is managed by Prime Network Services Controller. RESTful
API is read only. Changing configuration using CLI is not recommended.
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 login local
!
end

```

## VSG

```

version 4.2(1)VSG2(1.1)
no feature telnet

username admin password 5 $1$be6ZcA6Z$Y1PI9X.BZgqu07qEvid5G/ role network-admin

banner motd #Nexus Virtual Security Gateway#

ssh key rsa 2048
no ip domain-lookup
ip host EXCPVSG23824 192.168.74.244
hostname EXCPVSG23824
errdisable recovery cause failed-port-state
no snmp-server protocol enable
snmp-server user admin network-admin auth md5 0xc36fb6c0f30b9b94e08df2d8c8911119 priv
0xc36fb6c0f30b9b94e08df2d8c8911119 localizedkey

```



```

vrf context management
  ip route 0.0.0.0/0 192.168.74.1
vlan 1

port-profile default max-ports 32

system storage-loss log time 30
vdc EXCPVSG23824 id 1
  limit-resource vlan minimum 16 maximum 2049
  limit-resource monitor-session minimum 0 maximum 2
  limit-resource vrf minimum 16 maximum 8192
  limit-resource port-channel minimum 0 maximum 768
  limit-resource u4route-mem minimum 1 maximum 1
  limit-resource u6route-mem minimum 1 maximum 1
  limit-resource m4route-mem minimum 58 maximum 58
  limit-resource m6route-mem minimum 8 maximum 8

interface mgmt0
  ip address 192.168.74.244/24

interface data0
  ip address 192.168.75.60/24
line vty
  exec-timeout 5
line console
  exec-timeout 5
boot kickstart bootflash:/nexus-1000v-kickstart.VSG2.1.1.bin sup-1
boot system bootflash:/nexus-1000v.VSG2.1.1.bin sup-1
boot kickstart bootflash:/nexus-1000v-kickstart.VSG2.1.1.bin sup-2
boot system bootflash:/nexus-1000v.VSG2.1.1.bin sup-2
  ha-pair id 62

security-profile EXCP_732@root/EXCP
  policy EXCP_732@root/EXCP
  custom-attribute vnspOrg "root/excp"

security-profile EXCP_733@root/EXCP
  policy EXCP_733@root/EXCP
  custom-attribute vnspOrg "root/excp"

security-profile EXCP_734@root/EXCP
  policy EXCP_734@root/EXCP
  custom-attribute vnspOrg "root/excp"

security-profile EXCP_736@root/EXCP
  policy EXCP_736@root/EXCP
  custom-attribute vnspOrg "root/excp"

security-profile EXCP_737@root/EXCP
  policy EXCP_737@root/EXCP
  custom-attribute vnspOrg "root/excp"

security-profile default@root
  policy default@root
  custom-attribute vnspOrg "root"
zone PPublic_2c4f0a@root/EXCP cond-match-criteria: match-any
  condition 10 net.ip-address prefix 192.168.1.32 255.255.255.240
zone PPublic_a6e7c9@root/EXCP cond-match-criteria: match-any
  condition 10 net.ip-address prefix 192.168.1.0 255.255.255.248
rule EXCP_732_pmt_all/PermitAll@root/EXCP cond-match-criteria: match-all
  src-attributes
    condition 10 src.net.ip-address prefix 0.0.0.0 0.0.0.0
  action permit

```

```

rule EXCP_733_dny_all/EXCP_733@root/EXCP cond-match-criteria: match-all
  dst-attributes
    condition 10 dst.zone.name eq PPublic_a6e7c9@root/EXCP
  src-attributes
    condition 11 src.net.ip-address prefix 0.0.0.0 0.0.0.0
  action drop
rule EXCP_736_pmt_all/PermitAll@root/EXCP cond-match-criteria: match-all
  src-attributes
    condition 10 src.net.ip-address prefix 0.0.0.0 0.0.0.0
  action permit
rule EXCP_737_dny_all/EXCP_737@root/EXCP cond-match-criteria: match-all
  dst-attributes
    condition 10 dst.zone.name eq PPublic_2c4f0a@root/EXCP
  src-attributes
    condition 11 src.net.ip-address prefix 0.0.0.0 0.0.0.0
  action drop
rule PPublic_e5969d_pmt_int_CSR/PPublic_a6e7c9@root/EXCP cond-match-criteria: match-all
  dst-attributes
    condition 10 dst.net.ip-address prefix 192.168.1.0 255.255.255.248
  src-attributes
    condition 11 src.net.ip-address eq 192.168.1.1
  action permit
rule PPublic_f1365a_pmt_int_CSR/PPublic_2c4f0a@root/EXCP cond-match-criteria: match-all
  dst-attributes
    condition 10 dst.net.ip-address prefix 192.168.1.32 255.255.255.240
  src-attributes
    condition 11 src.net.ip-address eq 192.168.1.33
  action permit
rule default/default-rule@root cond-match-criteria: match-all
  action drop
rule default/default-rule@root/EXCP cond-match-criteria: match-all
  action drop
Policy EXCP_732@root/EXCP
  rule EXCP_732_pmt_all/PermitAll@root/EXCP order 101
Policy EXCP_733@root/EXCP
  rule PPublic_e5969d_pmt_int_CSR/PPublic_a6e7c9@root/EXCP order 2
  rule EXCP_733_dny_all/EXCP_733@root/EXCP order 1001
Policy EXCP_734@root/EXCP
  rule default/default-rule@root/EXCP order 2
Policy EXCP_736@root/EXCP
  rule EXCP_736_pmt_all/PermitAll@root/EXCP order 101
Policy EXCP_737@root/EXCP
  rule PPublic_f1365a_pmt_int_CSR/PPublic_2c4f0a@root/EXCP order 2
  rule EXCP_737_dny_all/EXCP_737@root/EXCP order 1001
Policy default@root
  rule default/default-rule@root order 2
vnm-policy-agent
  registration-ip 192.168.7.246
  shared-secret *****
  policy-agent-image bootflash:/vnmc-vsgpa.2.1.1b.bin
  log-level
logging logfile messages 2 size 4194303

```

## Citrix NetScaler VPX

```

#NS10.1 Build 119.7
# Last modified by `save config`, Fri Apr 25 14:46:02 2014
set ns config -IPAddress 192.168.74.245 -netmask 255.255.255.0
enable ns mode FR L3 Edge USNIP PMTUD
set system parameter -natPcbForceFlushLimit 4294967295
set system user nsroot 1050a3c86e20223596a6a5a847c0d81b3c4255deb3ccb34c6 -encrypted
set rsskeytype -rsstype ASYMMETRIC

```

```

set lACP -sysPriority 32768 -mac 00:50:56:9e:05:66
set interface 0/1 -throughput 0 -bandwidthHigh 0 -bandwidthNormal 0 -intftype "XEN
Interface" -ifnum 0/1
set interface 1/1 -throughput 0 -bandwidthHigh 0 -bandwidthNormal 0 -intftype "XEN
Interface" -ifnum 1/1
set interface LO/1 -haMonitor OFF -throughput 0 -bandwidthHigh 0 -bandwidthNormal 0
-intftype Loopback -ifnum LO/1
add vlan 741
add ns ip6 fe80::250:56ff:fe9e:566/64 -scope link-local -type NSIP -vlan 1 -vServer
DISABLED -mgmtAccess ENABLED -dynamicRouting ENABLED
add ns ip 192.168.4.4 255.255.255.0 -vServer DISABLED
add ns ip 192.168.4.5 255.255.255.0 -vServer DISABLED
set IP addressesec parameter -lifetime 28800
add IP addressesec profile ns_IP addressesec_default_profile -ikeRetryInterval 60
bind vlan 741 -ifnum 1/1
bind vlan 741 -IPAddress 192.168.4.4 255.255.255.0
set nd6RAvariables -vlan 1
bind nd6RAvariables -vlan 1 -ipv6Prefix ::
set ipv6 -natprefix ::
add IP addresseset EXCPubNAT23824
bind IP addresseset EXCPubNAT23824 192.168.4.5
add netProfile EXCPubNAT23824 -srcIP EXCPubNAT23824
set netProfile EXCPubNAT23824 -srcIP EXCPubNAT23824
set snmp alarm SYNFLOOD -timeout 1
set snmp alarm HA-VERSION-MISMATCH -time 86400 -timeout 86400
set snmp alarm HA-SYNC-FAILURE -time 86400 -timeout 86400
set snmp alarm HA-NO-HEARTBEATS -time 86400 -timeout 86400
set snmp alarm HA-BAD-SECONDARY-STATE -time 86400 -timeout 86400
set snmp alarm HA-PROP-FAILURE -timeout 86400
set snmp alarm IP-CONFLICT -timeout 86400
set snmp alarm APPFW-START-URL -timeout 1
set snmp alarm APPFW-DENY-URL -timeout 1
set snmp alarm APPFW-REFERER-HEADER -timeout 1
set snmp alarm APPFW-CSRF-TAG -timeout 1
set snmp alarm APPFW-COOKIE -timeout 1
set snmp alarm APPFW-FIELD-CONSISTENCY -timeout 1
set snmp alarm APPFW-BUFFER-OVERFLOW -timeout 1
set snmp alarm APPFW-FIELD-FORMAT -timeout 1
set snmp alarm APPFW-SAFE-COMMERCE -timeout 1
set snmp alarm APPFW-SAFE-OBJECT -timeout 1
set snmp alarm APPFW-POLICY-HIT -timeout 1
set snmp alarm APPFW-VIOLATIONS-TYPE -timeout 1
set snmp alarm APPFW-XSS -timeout 1
set snmp alarm APPFW-XML-XSS -timeout 1
set snmp alarm APPFW-SQL -timeout 1
set snmp alarm APPFW-XML-SQL -timeout 1
set snmp alarm APPFW-XML-ATTACHMENT -timeout 1
set snmp alarm APPFW-XML-DOS -timeout 1
set snmp alarm APPFW-XML-VALIDATION -timeout 1
set snmp alarm APPFW-XML-WSI -timeout 1
set snmp alarm APPFW-XML-SCHEMA-COMPILE -timeout 1
set snmp alarm APPFW-XML-SOAP-FAULT -timeout 1
set snmp alarm DNSKEY-EXPIRY -timeout 1
set snmp alarm HA-LICENSE-MISMATCH -timeout 86400
set snmp alarm CLUSTER-NODE-HEALTH -time 86400 -timeout 86400
set snmp alarm CLUSTER-NODE-QUORUM -time 86400 -timeout 86400
set snmp alarm CLUSTER-VERSION-MISMATCH -time 86400 -timeout 86400
set ns tcpProfile nstcp_default_tcp_lfp -mss 0
set ns tcpProfile nstcp_default_tcp_lnp -mss 0
set ns tcpProfile nstcp_default_tcp_lan -mss 0
set ns tcpProfile nstcp_default_tcp_lfp_thin_stream -mss 0
set ns tcpProfile nstcp_default_tcp_lnp_thin_stream -mss 0
set ns tcpProfile nstcp_default_tcp_lan_thin_stream -mss 0
set ns tcpProfile nstcp_default_tcp_interactive_stream -mss 0

```

```

set ns tcpProfile nstcp_internal_apps -mss 0
set ns tcpProfile nstcp_default_XA_XD_profile -mss 0
set ns tcpProfile nstcp_default_Mobile_profile -mss 0
add serviceGroup EXCPHTTP23824 HTTP -maxClient 0 -maxReq 0 -cip DISABLED -usip NO
-useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
add serviceGroup EXCPSSL_BRIDGE23824 SSL_BRIDGE -maxClient 0 -maxReq 0 -cip DISABLED -usip
NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
add ssl certKey ns-server-certificate -cert ns-server.cert -key ns-server.key
bind cmp global ns_adv_nocmp_xml_ie -priority 8700 -gotoPriorityExpression END -type
RES_DEFAULT
bind cmp global ns_adv_nocmp_mozilla_47 -priority 8800 -gotoPriorityExpression END -type
RES_DEFAULT
bind cmp global ns_adv_cmp_mscss -priority 8900 -gotoPriorityExpression END -type
RES_DEFAULT
bind cmp global ns_adv_cmp_msapp -priority 9000 -gotoPriorityExpression END -type
RES_DEFAULT
bind cmp global ns_adv_cmp_content_type -priority 10000 -gotoPriorityExpression END -type
RES_DEFAULT
set lb parameter -sessionsThreshold 150000
add lb vserver EXCPHTTP23824 HTTP 64.100.4.193 80 -persistenceType NONE -lbMethod
ROUNDROBIN -cltTimeout 180 -netProfile EXCPPubNAT23824
add lb vserver EXCPSSL_BRIDGE23824 SSL_BRIDGE 64.100.4.193 443 -persistenceType SSLSESSION
-lbMethod ROUNDROBIN -cltTimeout 180 -netProfile EXCPPubNAT23824
set cache parameter -via "NS-CACHE-10.0: 245"
set aaa parameter -maxAAAUUsers 5
set ns rpcNode 192.168.74.245 -password
8a7b474124957776a0cd31b862cbe4d72b5cbd59868a136d4bdeb56cf03b28 -encrypted -srcIP *
set responder param -undefAction NOOP
bind lb vserver EXCPHTTP23824 EXCPHTTP23824
bind lb vserver EXCPSSL_BRIDGE23824 EXCPSSL_BRIDGE23824
set ns diameter -identity netscaler.com -realm com
add nd6 ::/0 00:00:00:00:00:00 0/84/80
add dns nsRec . a.root-servers.net -TTL 3600000
add dns nsRec . b.root-servers.net -TTL 3600000
add dns nsRec . c.root-servers.net -TTL 3600000
add dns nsRec . d.root-servers.net -TTL 3600000
add dns nsRec . e.root-servers.net -TTL 3600000
add dns nsRec . f.root-servers.net -TTL 3600000
add dns nsRec . g.root-servers.net -TTL 3600000
add dns nsRec . h.root-servers.net -TTL 3600000
add dns nsRec . i.root-servers.net -TTL 3600000
add dns nsRec . j.root-servers.net -TTL 3600000
add dns nsRec . k.root-servers.net -TTL 3600000
add dns nsRec . l.root-servers.net -TTL 3600000
add dns nsRec . m.root-servers.net -TTL 3600000
add dns addRec l.root-servers.net 199.7.83.42 -TTL 3600000
add dns addRec b.root-servers.net 192.228.79.201 -TTL 3600000
add dns addRec d.root-servers.net 128.8.10.90 -TTL 3600000
add dns addRec j.root-servers.net 192.58.128.30 -TTL 3600000
add dns addRec h.root-servers.net 128.63.2.53 -TTL 3600000
add dns addRec f.root-servers.net 192.5.5.241 -TTL 3600000
add dns addRec k.root-servers.net 193.0.14.129 -TTL 3600000
add dns addRec a.root-servers.net 198.41.0.4 -TTL 3600000
add dns addRec c.root-servers.net 192.33.4.12 -TTL 3600000
add dns addRec m.root-servers.net 202.12.27.33 -TTL 3600000
add dns addRec i.root-servers.net 192.36.148.17 -TTL 3600000
add dns addRec g.root-servers.net 192.112.36.4 -TTL 3600000
add dns addRec e.root-servers.net 192.203.230.10 -TTL 3600000
set lb monitor ldns-dns LDNS-DNS -query . -queryType Address
bind serviceGroup EXCPHTTP23824 -monitorName ping
bind serviceGroup EXCPSSL_BRIDGE23824 -monitorName ping
add route 0.0.0.0 0.0.0.0 192.168.4.1
add route 192.168.7.0 255.255.255.0 192.168.74.1
add route6 ::/0 ::/0 -cost 0

```

```

set ssl service nshttps-::11-443 -eRSA ENABLED -sessReuse DISABLED -tls11 DISABLED -tls12
DISABLED
set ssl service nsrpcs-::11-3008 -eRSA ENABLED -sessReuse DISABLED -tls11 DISABLED -tls12
DISABLED
set ssl service nskrpcs-127.0.0.1-3009 -eRSA ENABLED -sessReuse DISABLED -tls11 DISABLED
-tls12 DISABLED
set ssl service nshttps-127.0.0.1-443 -eRSA ENABLED -sessReuse DISABLED -tls11 DISABLED
-tls12 DISABLED
set ssl service nsrpcs-127.0.0.1-3008 -eRSA ENABLED -sessReuse DISABLED -tls11 DISABLED
-tls12 DISABLED
set vpn parameter -forceCleanup none -clientOptions all -clientConfiguration all
apply ns acls6
apply ns pbr6
bind ssl service nshttps-::11-443 -certkeyName ns-server-certificate
bind ssl service nsrpcs-::11-3008 -certkeyName ns-server-certificate
bind ssl service nskrpcs-127.0.0.1-3009 -certkeyName ns-server-certificate
bind ssl service nshttps-127.0.0.1-443 -certkeyName ns-server-certificate
bind ssl service nsrpcs-127.0.0.1-3008 -certkeyName ns-server-certificate
set ns encryptionParams -method AES256 -keyValue
ffe316156e6152dc7994de922b29a80397c8b5acbff6e3d59c1c823e20b5c009b8a8d6134d73b1b8f1de857ef
2b3ef75fe712b8 -encrypted
set inatparam -nat46v6Prefix ::/96
set ip6TunnelParam -srcIP ::
set ptp -state ENABLE

```

## VDC Creation for CSR 1000V and VSG

### CSR 1000V

```

...
security-profile EXCP_738@root/EXCP
  policy EXCP_738@root/EXCP
  custom-attribute vnspOrg "root/excp"

security-profile EXCP_740@root/EXCP
  policy EXCP_740@root/EXCP
  custom-attribute vnspOrg "root/excp"
...
zone PPublic_23debb@root/EXCP cond-match-criteria: match-any
  condition 10 net.ip-address prefix 192.168.1.64 255.255.255.240
...
rule EXCP_738_pmt_all/PermitAll@root/EXCP cond-match-criteria: match-all
  src-attributes
    condition 10 src.net.ip-address prefix 0.0.0.0 0.0.0.0
  action permit
rule EXCP_740_dny_all/EXCP_740@root/EXCP cond-match-criteria: match-all
  dst-attributes
    condition 10 dst.zone.name eq PPublic_23debb@root/EXCP
  src-attributes
    condition 11 src.net.ip-address prefix 0.0.0.0 0.0.0.0
  action drop
rule PPublic_18b3a6_pmt_int_CSR/PPublic_23debb@root/EXCP cond-match-criteria: match-all
  dst-attributes
    condition 10 dst.net.ip-address prefix 192.168.1.64 255.255.255.240
  src-attributes
    condition 11 src.net.ip-address eq 192.168.1.65
  action permit
...
Policy EXCP_738@root/EXCP
  rule EXCP_738_pmt_all/PermitAll@root/EXCP order 101

```

```
Policy EXCP_740@root/EXCP
  rule PPublic_18b3a6_pmt_int_CSR/PPublic_23debb@root/EXCP order 2
  rule EXCP_740_dny_all/EXCP_740@root/EXCP order 1001
```

## VSG

```
...
class-map type inspect match-all UnpPublic_23debb_pmt_int
  match access-group name EXCP_738_pmt_all
...
policy-map type inspect EXCP_738
  class type inspect UnpPublic_23debb_pmt_int
    pass
  class class-default
...
zone security EXCP_738
zone-pair security EXCP_738_Internet source EXCP_738 destination Internet
  service-policy type inspect EXCP_738
zone-pair security Internet_EXCP_738 source Internet destination EXCP_738
  service-policy type inspect EXCP_738
```

## Firewall Rule Creation for CSR 1000V and VSG

The following configurations provide information on firewall rules created on the CSR 1000V and VSG during IAC Organization creation and when an IAC user creates a firewall rule.

### Enterprise > Unprotected Private Network

These are the IAC firewall policies created during Organization creation.

#### CSR 1000V

```
policy-map type inspect HI5_2074
  class type inspect UnpPrivate_e50577_pmt_int
    pass
  class class-default

  class-map type inspect match-all UnpPrivate_e50577_pmt_int
    match access-group name HI5_2074_pmt_all

  ip access-list extended HI5_2074_pmt_all
    permit ip any any

  zone-pair security Enterprise_HI5_2074 source Enterprise destination HI5_2074
    service-policy type inspect HI5_2074

  zone-pair security HI5_2074_Enterprise source HI5_2074 destination Enterprise
    service-policy type inspect HI5_2074
```

## VSG

```
security-profile HI5_2074@root/HI5
  policy HI5_2074@root/HI5
  custom-attribute vnsporg "root/hi5"

rule HI5_2074_pmt_all/PermitAll@root/HI5 cond-match-criteria: match-all
  src-attributes
```

```
condition 10 src.net.ip-address prefix 0.0.0.0 0.0.0.0
action permit
```

```
Policy HI5_2074@root/HI5
rule HI5_2074_pmt_all/PermitAll@root/HI5 order 101
```

## Enterprise > Protected Private Network

These are the IAC user created policies using the VDC firewall rule resource.

### CSR 1000V

```
policy-map type inspect Enterprise_HI5_2075
class type inspect RULE_f5b2b928
inspect
class class-default

class-map type inspect match-all RULE_f5b2b928
match access-group name RULE_f5b2b928_noog
ip access-list extended RULE_f5b2b928_noog
permit tcp 31.0.0.0 0.255.255.255 10.249.1.128 0.0.0.31 eq 3306
permit tcp 31.0.0.0 0.255.255.255 10.249.1.128 0.0.0.31 eq 443
permit tcp 31.0.0.0 0.255.255.255 10.249.1.128 0.0.0.31 eq www
permit tcp 31.0.0.0 0.255.255.255 10.249.1.128 0.0.0.31 eq 22
permit tcp 31.0.0.0 0.255.255.255 10.249.1.128 0.0.0.31 eq ftp
permit tcp 31.0.0.0 0.255.255.255 10.249.1.128 0.0.0.31 eq ftp-data

zone-pair security Enterprise_HI5_2075 source Enterprise destination HI5_2075
service-policy type inspect Enterprise_HI5_2075
```

### VSG

```
security-profile HI5_2075@root/HI5
policy HI5_2075@root/HI5
custom-attribute vnsporg "root/hi5"

rule RULE_de8699e5/DefaultRule@root/HI5 cond-match-criteria: match-all
src-attributes
condition 11 src.net.ip-address prefix 10.249.1.128 255.255.255.224
service/protocol-attribute
condition 10 net.service member-of SG_9a686ee@root/HI5
action permit
rule RULE_332fbb18/DefaultRule@root/HI5 cond-match-criteria: match-all
dst-attributes
condition 11 dst.net.ip-address prefix 10.249.1.160 255.255.255.240
src-attributes
condition 12 src.net.ip-address prefix 10.249.1.128 255.255.255.224
service/protocol-attribute
condition 10 net.service member-of SG_9a686ee@root/HI5
action permit
rule RULE_f5b2b928/DefaultRule@root/HI5 cond-match-criteria: match-all
dst-attributes
condition 11 dst.net.ip-address prefix 10.249.1.128 255.255.255.224
src-attributes
condition 12 src.net.ip-address prefix 31.0.0.0 255.0.0.0
service/protocol-attribute
condition 10 net.service member-of SG_9a686ee@root/HI5
action permit
rule RULE_524f0d48/DefaultRule@root/HI5 cond-match-criteria: match-all
```

```

dst-attributes
  condition 10 dst.net.ip-address member-of SG_2075_82b640e@root/HI5
src-attributes
  condition 11 src.net.ip-address prefix 10.249.1.128 255.255.255.224
action permit
rule RULE_c4deeda5/DefaultRule@root/HI5 cond-match-criteria: match-all
dst-attributes
  condition 11 dst.net.ip-address member-of SG_2075_82b640e@root/HI5
src-attributes
  condition 12 src.net.ip-address member-of SG_2073_3637bde@root/HI5
service/protocol-attribute
  condition 10 net.service member-of SG_9a686ee@root/HI5
action permit
rule RULE_4a85027e/DefaultRule@root/HI5 cond-match-criteria: match-all
dst-attributes
  condition 11 dst.net.ip-address member-of SG_2073_3637bde@root/HI5
src-attributes
  condition 12 src.net.ip-address member-of SG_2075_82b640e@root/HI5
service/protocol-attribute
  condition 10 net.service member-of SG_2f1e052@root/HI5
action permit
rule PPrivate_5726ab_pmt_int/PPrivate_e50577@root/HI5 cond-match-criteria: match-all
dst-attributes
  condition 10 dst.zone.name eq PPrivate_e50577@root/HI5
src-attributes
  condition 11 src.zone.name eq PPrivate_e50577@root/HI5
action permit
rule PPrivate_5726ab_pmt_int_CSR/PPrivate_e50577@root/HI5 cond-match-criteria: match-all
dst-attributes
  condition 10 dst.net.ip-address prefix 10.249.1.128 255.255.255.224
src-attributes
  condition 11 src.net.ip-address eq 10.249.1.129
action permit

rule HI5_2075_dny_all/HI5_2075@root/HI5 cond-match-criteria: match-all
dst-attributes
  condition 10 dst.zone.name eq PPrivate_e50577@root/HI5
src-attributes
  condition 11 src.net.ip-address prefix 0.0.0.0 0.0.0.0
action drop

Policy HI5_2075@root/HI5
rule RULE_de8699e5/DefaultRule@root/HI5 order 2
rule RULE_332fbb18/DefaultRule@root/HI5 order 4
rule RULE_f5b2b928/DefaultRule@root/HI5 order 6
rule RULE_524f0d48/DefaultRule@root/HI5 order 8
rule RULE_c4deeda5/DefaultRule@root/HI5 order 10
rule RULE_4a85027e/DefaultRule@root/HI5 order 12
rule PPrivate_5726ab_pmt_int/PPrivate_e50577@root/HI5 order 14
rule PPrivate_5726ab_pmt_int_CSR/PPrivate_e50577@root/HI5 order 16
rule HI5_2075_dny_all/HI5_2075@root/HI5 order 1015

```

## Internet > Unprotected Public Network

These are the IAC firewall policies created during Organization creation.

### CSR 1000V

```

policy-map type inspect HI5_2072
  class type inspect UnpPublic_e50577_pmt_int

```



```

pass
class class-default

class-map type inspect match-all UnpPublic_e50577_pmt_int
match access-group name HI5_2072_pmt_all

ip access-list extended HI5_2072_pmt_all
permit ip any any

zone-pair security Internet_HI5_2072 source Internet destination HI5_2072
service-policy type inspect HI5_2072

zone-pair security HI5_2072_Internet source HI5_2072 destination Internet
service-policy type inspect HI5_2072

```

**VSG**

```

security-profile HI5_2072@root/HI5
policy HI5_2072@root/HI5
custom-attribute vnsporg "root/hi5"

rule HI5_2072_pmt_all/PermitAll@root/HI5 cond-match-criteria: match-all
src-attributes
condition 10 src.net.ip-address prefix 0.0.0.0 0.0.0.0
action permit

Policy HI5_2072@root/HI5
rule HI5_2072_pmt_all/PermitAll@root/HI5 order 115

```

**Protected Public > Protected Private Network**

These are the IAC user created policies using the VDC firewall rule resource.

**CSR 1000V**

```

policy-map type inspect HI5_2073_HI5_2075
class type inspect RULE_c4deeda5
inspect
class class-default

class-map type inspect match-all RULE_c4deeda5
match access-group name RULE_c4deeda5_noog
ip access-list extended RULE_c4deeda5_noog
permit tcp host 10.249.1.68 host 10.249.1.132 eq 3306
permit tcp host 10.249.1.68 host 10.249.1.132 eq 443
permit tcp host 10.249.1.68 host 10.249.1.132 eq www
permit tcp host 10.249.1.68 host 10.249.1.132 eq 22
permit tcp host 10.249.1.68 host 10.249.1.132 eq ftp
permit tcp host 10.249.1.68 host 10.249.1.132 eq ftp-data

zone-pair security HI5_2073_HI5_2075 source HI5_2073 destination HI5_2075
service-policy type inspect HI5_2073_HI5_2075

```

**VSG**

```

security-profile HI5_2073@root/HI5
policy HI5_2073@root/HI5
custom-attribute vnsporg "root/hi5"

```

```

rule RULE_76cbf42a/DefaultRule@root/HI5 cond-match-criteria: match-all
  dst-attributes
    condition 11 dst.net.ip-address eq 10.249.1.68
rule RULE_4a85027e/DefaultRule@root/HI5 cond-match-criteria: match-all
  dst-attributes
    condition 11 dst.net.ip-address member-of SG_2073_3637bde@root/HI5
  src-attributes
    condition 12 src.net.ip-address member-of SG_2075_82b640e@root/HI5
  service/protocol-attribute
    condition 10 net.service member-of SG_2f1e052@root/HI5
  action permit
rule RULE_948a9829/DefaultRule@root/HI5 cond-match-criteria: match-all
  dst-attributes
    condition 10 dst.net.ip-address prefix 0.0.0.0 0.0.0.0
  src-attributes
    condition 11 src.net.ip-address member-of SG_2073_3637bde@root/HI5
  action permit
rule RULE_02caebe0/DefaultRule@root/HI5 cond-match-criteria: match-all
  dst-attributes
    condition 10 dst.net.ip-address prefix 0.0.0.0 0.0.0.0
  src-attributes
    condition 11 src.net.ip-address prefix 10.249.1.64 255.255.255.224
  action permit
rule PPublic_5726ab_pmt_int/PPublic_e50577@root/HI5 cond-match-criteria: match-all
  dst-attributes
    condition 10 dst.zone.name eq PPublic_e50577@root/HI5
  src-attributes
    condition 11 src.zone.name eq PPublic_e50577@root/HI5
  action permit
rule PPublic_5726ab_pmt_int_CSR/PPublic_e50577@root/HI5 cond-match-criteria: match-all
  dst-attributes
    condition 10 dst.net.ip-address prefix 10.249.1.64 255.255.255.224
  src-attributes
    condition 11 src.net.ip-address eq 10.249.1.65
  action permit
rule HI5_2073_dny_all/HI5_2073@root/HI5 cond-match-criteria: match-all
  dst-attributes
    condition 10 dst.zone.name eq PPublic_e50577@root/HI5
  src-attributes
    condition 11 src.net.ip-address prefix 0.0.0.0 0.0.0.0
  action drop
Policy HI5_2073@root/HI5
  rule RULE_02ccb088/DefaultRule@root/HI5 order 2
  rule RULE_c4deeda5/DefaultRule@root/HI5 order 4
  rule RULE_4d1ee2eb/DefaultRule@root/HI5 order 6
  rule RULE_76cbf42a/DefaultRule@root/HI5 order 8
  rule RULE_4a85027e/DefaultRule@root/HI5 order 10
  rule RULE_948a9829/DefaultRule@root/HI5 order 12
  rule RULE_02caebe0/DefaultRule@root/HI5 order 14
  rule PPublic_5726ab_pmt_int/PPublic_e50577@root/HI5 order 16
  rule PPublic_5726ab_pmt_int_CSR/PPublic_e50577@root/HI5 order 18
  rule HI5_2073_dny_all/HI5_2073@root/HI5 order 1017

```

## SLB Policy Creation for CSR 1000V, VPX, VSG

### CSR 1000V

```

class-map type inspect match-all LB_OUT_Allow_5e94d95_CMAP
  match access-group name LB_OUT_Allow_5e94d95_ACL

```

```

class-map type inspect match-all NTC_2290_SNIP_LB_CMAP
  match access-group name NTC_2290_SNIP_LB_ACL
class-map type inspect match-all SNIP_LB_NTC_2290_CMAP
  match access-group name SNIP_LB_NTC_2290_ACL
class-map type inspect match-all LB_IN_Allow_5e94d95_CMAP
  match access-group name LB_IN_Allow_5e94d95_ACL

policy-map type inspect VIP_LB_Internet
  class type inspect LB_IN_Allow_5e94d95_CMAP
    pass
  class type inspect LB_OUT_Allow_5e94d95_CMAP
    pass
  class class-default

policy-map type inspect SNIP_LB_NTC_2290
  class type inspect SNIP_LB_NTC_2290_CMAP
    pass
  class type inspect NTC_2290_SNIP_LB_CMAP
    pass
  class class-default

zone security LB_NTCCSR20392
zone security Internet
zone security NTC_2290

zone-pair security Internet_LB_NTCCSR20392 source Internet destination LB_NTCCSR20392
  service-policy type inspect VIP_LB_Internet
zone-pair security NTCCSR20392_LB_Internet source LB_NTCCSR20392 destination Internet
  service-policy type inspect VIP_LB_Internet
zone-pair security NTCCSR20392_LB_NTC_2290 source LB_NTCCSR20392 destination NTC_2290
  service-policy type inspect SNIP_LB_NTC_2290
zone-pair security NTC_2290_LB_NTCCSR20392 source NTC_2290 destination LB_NTCCSR20392
  service-policy type inspect SNIP_LB_NTC_2290

ip route 64.171.4.101 255.255.255.255 GigabitEthernet4 172.16.3.4

ip access-list extended LB_IN_Allow_5e94d95_ACL
  permit ip any host 64.171.4.101
ip access-list extended LB_OUT_Allow_5e94d95_ACL
  permit ip host 64.171.4.101 any
ip access-list extended NTC_2290_SNIP_LB_ACL
  permit ip host 172.16.2.68 172.16.3.0 0.0.0.255
  permit icmp host 172.16.2.68 172.16.3.0 0.0.0.255
ip access-list extended SNIP_LB_NTC_2290_ACL
  permit tcp 172.16.3.0 0.0.0.255 host 172.16.2.68 eq www
  permit icmp 172.16.3.0 0.0.0.255 host 172.16.2.68

```

## VSG

```

rule NTC_2290_SNIP_LB_ACL/NTC720725_80@root/NTC cond-match-criteria: match-all
  dst-attributes
    condition 10 dst.net.ip-address prefix 172.16.3.0 255.255.255.0
  src-attributes
    condition 11 src.net.ip-address eq 172.16.2.68
  action permit
rule NTC_2290_SNIP_LB_ACL/NTC720725_ICMP@root/NTC cond-match-criteria: match-all
  dst-attributes
    condition 11 dst.net.ip-address prefix 172.16.3.0 255.255.255.0
  src-attributes
    condition 12 src.net.ip-address eq 172.16.2.68
  service/protocol-attribute
    condition 10 net.service eq protocol 1

```

```

    action permit

rule SNIP_LB_NTC_2290_ACL/NTC720725_80@root/NTC cond-match-criteria: match-all
    dst-attributes
        condition 11 dst.net.ip-address eq 172.16.2.68
    src-attributes
        condition 12 src.net.ip-address prefix 172.16.3.0 255.255.255.0
    service/protocol-attribute
        condition 10 net.service eq protocol 6 port 80
    action permit
rule SNIP_LB_NTC_2290_ACL/NTC720725_ICMP@root/NTC cond-match-criteria: match-all
    dst-attributes
        condition 11 dst.net.ip-address eq 172.16.2.68
    src-attributes
        condition 12 src.net.ip-address prefix 172.16.3.0 255.255.255.0
    service/protocol-attribute
        condition 10 net.service eq protocol 1
    action permit

Policy NTC_2290@root/NTC
    rule SNIP_LB_NTC_2290_ACL/NTC720725_80@root/NTC order 2
    rule SNIP_LB_NTC_2290_ACL/NTC720725_ICMP@root/NTC order 3
    rule NTC_2290_SNIP_LB_ACL/NTC720725_80@root/NTC order 5
    rule NTC_2290_SNIP_LB_ACL/NTC720725_ICMP@root/NTC order 6
    rule PPublic_6e22dd_pmt_int/PPublic_593cac@root/NTC order 8
    rule PPublic_6e22dd_pmt_int_CSR/PPublic_593cac@root/NTC order 10
    rule NTC_2290_dny_all/NTC_2290@root/NTC order 1009

```

## VPX

```

add server 172.16.2.68 172.16.2.68
add service 172.16.2.68 172.16.2.68 HTTP 80 -gslb NONE -maxClient 0 -maxReq 0 -cip
DISABLED -usip NO -useproxyport YES -sp OFF -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB
NO -CMP NO

add serviceGroup NTCHTTP20392 HTTP -maxClient 0 -maxReq 0 -cip DISABLED -usip NO
-useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO
add serviceGroup NTCSSL_BRIDGE20392 SSL_BRIDGE -maxClient 0 -maxReq 0 -cip DISABLED -usip
NO -useproxyport YES -cltTimeout 180 -svrTimeout 360 -CKA NO -TCPB NO -CMP NO

add lb vserver NTCHTTP20392 HTTP 64.171.4.101 80 -persistenceType NONE -lbMethod
ROUNDROBIN -cltTimeout 180 -netProfile NTCPubNAT20392
add lb vserver NTCSSL_BRIDGE20392 SSL_BRIDGE 64.171.4.101 443 -persistenceType SSLSESSION
-lbMethod ROUNDROBIN -cltTimeout 180 -netProfile NTCPubNAT20392

bind lb vserver NTCHTTP20392 NTCHTTP20392
bind lb vserver NTCSSL_BRIDGE20392 NTCSSL_BRIDGE20392

set lb monitor ldns-dns LDNS-DNS -query . -queryType Address

bind serviceGroup NTCHTTP20392 172.16.2.68 80
bind serviceGroup NTCHTTP20392 -monitorName ping
bind serviceGroup NTCSSL_BRIDGE20392 -monitorName ping

```

## NAT Creation for CSR 1000V

When creating NAT, a loopback interface is created on the CSR 1000V. This address is redistributed into the local BGP process for advertisement to the Internet gateway. The CSR 1000V interface for the Protected Public network is the only interface with an “ip nat inside” statement. Only VMs on the Protected Public network can be NATed.

```
!
interface Loopback1
  description 97029be7-b827-4e51-bd5e-1dfd1ecb58d3
  ip address 64.171.4.107 255.255.255.255
!

interface GigabitEthernet6
  description configured by PolicyAgent
  ip address 172.16.1.49 255.255.255.240
  ip nat inside
  ip access-group default-ingress in
  ip access-group default-egress out
  zone-member security csr1_2316
  negotiation auto

ip nat inside source static 172.16.1.52 64.171.4.107
```

## Network Creation for CSR 1000V, VPX, VSG



### Note

Adding new networks has no impact on the VPX.

When adding networks to an existing VDC, IAC adds interfaces on the CSR 1000V and sets up default ACLs, class maps, policy maps and zone pairs, depending on type of network. IAC also adds these policy maps to the VSG. IAC also adds VLANs to all networks in the pod.

In this example, two networks were added, one Unprotected Public and one Protected Public. The Unprotected Network has a permit all statement, so this zone pairing is configured. Zone pairs are not configured until needed, so there are not any zone pairs for the Protected Public network until something is configured that requires one.

## CSR 1000V - Adding Two New Networks

```
class-map type inspect match-all UnpPublic_4e9440_pmt_int
  match access-group name csr1_2315_pmt_all

policy-map type inspect csr1_2315
  class type inspect UnpPublic_4e9440_pmt_int
    pass
  class class-default

zone-pair security Internet_csr1_2315 source Internet destination csr1_2315
  service-policy type inspect csr1_2315
zone-pair security csr1_2315_Internet source csr1_2315 destination Internet
  service-policy type inspect csr1_2315

zone security csr1_2315
zone security csr1_2316

interface GigabitEthernet9
```

```

description configured by PolicyAgent
ip address 64.171.5.33 255.255.255.240
ip access-group default-ingress in
ip access-group default-egress out
zone-member security csr1_2315
negotiation auto
!
interface GigabitEthernet10
description configured by PolicyAgent
ip address 172.16.1.49 255.255.255.240
ip nat inside
ip access-group default-ingress in
ip access-group default-egress out
zone-member security csr1_2316
negotiation auto

ip access-list extended csr1_2315_pmt_all
permit ip any any

```

## VSG - Adding Two Networks

```

security-profile csr1_2315@root/csr1
policy csr1_2315@root/csr1
custom-attribute vnspOrg "root/csr1"

security-profile csr1_2316@root/csr1
policy csr1_2316@root/csr1
custom-attribute vnspOrg "root/csr1"

rule csr1_2315_pmt_all/PermitAll@root/csr1 cond-match-criteria: match-all
src-attributes
condition 10 src.net.ip-address prefix 0.0.0.0 0.0.0.0
action permit

rule csr1_2316_dny_all/csr1_2316@root/csr1 cond-match-criteria: match-all
dst-attributes
condition 10 dst.zone.name eq PPublic_4e9440@root/csr1
src-attributes
condition 11 src.net.ip-address prefix 0.0.0.0 0.0.0.0
action drop

Policy csr1_2315@root/csr1
rule csr1_2315_pmt_all/PermitAll@root/csr1 order 101
Policy csr1_2316@root/csr1
rule csr1_2316_dny_all/csr1_2316@root/csr1 order 1004

```



# Glossary

---

**ACL**

Access Control List

**API**

Application Programming Interface

**ARP**

Address Resolution Protocol

**ASA**

Adaptive Security Appliance

**ASR**

Aggregation Services Router

**BGP**

Border Gateway Protocol

**CDP**

Cisco Discovery Protocol

**CIAC**

Cisco Intelligent Automation for Cloud

**CIMC**

C-Series Integrated Management Controller

**CPTA**

Cloud Provider Technical Administrator (Super User)

**CSR**

Cloud Services Router (Cisco)

**DC**

Data Center

**DHCP**

Dynamic Host Configuration Protocol

**DNS**

Domain Name System (RFC 1034, RFC 1035)

**FEX**

Fabric Extender (Nexus)

**FI**

Fabric Interconnect

**HA**

High Availability

**IaaS**

Infrastructure as a Service

**IAC**

Intelligent Automation for Cloud (Cisco)

**ICS**

Integrated Compute and Storage

**JRE**

Java Runtime Environment

**LB**

Load Balancer

**MPLS**

Multiprotocol Label Switching

**NAS**

Network Attached Storage

**NAT**

Network Address Translation

**NFS**

Network File System

**NSIP**

NetScaler IP (Citrix)

**NTP**

Network Time Protocol (RFC 1305)



**OTA**

Organization Technical Administrator

**OVA**

Open Virtualization Archive

**OVF**

Open Virtualization Format

**PE**

Provider Edge

**PO**

Process Orchestrator (Cisco)

**Pod**

Point of Delivery. A basic infrastructure module that is a physical, repeatable construct with predictable infrastructure characteristics and deterministic functions. A pod identifies a modular unit of data center components and enables customers to add network, compute, and storage resources incrementally.

**PNSC**

Prime Network Services Controller (Cisco)

**PSC**

Prime Service Catalog (Cisco)

**RDP**

Remote Desktop Protocol

**SAN**

Storage Area Network

**SLA**

Service Level Agreement

**SLB**

Server Load Balancing

**SNIP**

Subnet IP

**SNMP**

Simple Network Management Protocol

**SP**

Server Provisioner (Cisco, VM and bare metal operating system)

**TTA**

Tenant Technical Administrator

**UCS**

Unified Computing System (Cisco)

**UCSM**

Unified Computing System Manager (Cisco)

**vApp**

Virtual Application

**VDC**

Virtual Data Center

**VEM**

Virtual Ethernet Module

**VIP**

Virtual IP

**VM**

Virtual Machine

**VMDC**

Virtual Multiservice Data Center

**vPC**

Virtual Port Channel

**VRF**

Virtual Routing and Forwarding

**VSA**

Virtual Services Architecture (Cisco)

**VSG**

Virtual Security Gateway (Cisco)

**VSM**

Virtual Supervisor Module

**VXLAN**

Virtual Extensible LAN

**ZBF**

Zone-Based Policy Firewall