Guide

Docker Enterprise Edition on Cisco UCS C220 M5 Servers for Container Management

July 2017

Contents

Introduction

Docker has become the leading software container platform for enterprises to build, ship, and run any applications anywhere. IT operations teams use Docker to run and manage applications side-by-side in isolated containers to get better compute density. Containerization provides the agility, control, and portability of application code to make it easy to build and deploy applications across any infrastructure. Enterprises use Docker to build agile software delivery pipelines to deliver new features quickly and more securely for both Linux and Windows Server applications on premises and in the cloud.

Using Docker, everything required to run a piece of software is packaged into isolated containers. Unlike VMs, containers do not bundle a full operating system; only libraries and settings required to make the software work are containerized thus making them efficient, lightweight, self-contained and portable regardless of where it is deployed. The containers then share the OS kernel on the underlying host, using less resources overall when compared to virtual machines.

Docker is at the heart of the modern application platform, bridging development and IT teams, Linux and Windows. Docker works as effectively in on-prem or cloud environments; and supports both traditional and microservices architectures. Docker is widely used for building, networking, securing and scheduling applications, and managing them right from development to production. Docker sets enterprises on the path to digital transformation by enabling all applications to be agile, cloud-ready and secure at optimal costs.

Docker Enterprise Edition (EE) is integrated, certified and supported to provide enterprises with the most secure container platform in the industry to modernize all applications. Docker EE, an application-centric platform, is designed to accelerate and secure the entire software supply chain, from development to production running on any infrastructure. Docker EE provides an integrated, tested and certified platform for applications running on enterprise Linux or Windows operating systems and Cloud providers. Docker EE is tightly integrated to the underlying infrastructure to provide a native, easy to install experience and an optimized Docker environment. Docker Certified Infrastructure, Containers and Plugins are exclusively available for Docker EE with cooperative support from Docker and the Certified Technology Partner.

Docker EE provides native container management tools, including Docker container engine, Docker Trusted Registry (DTR), and Docker Universal Control Plane (UCP). It can be deployed on-prem or in a cloud environment and is connected to the existing infrastructure and systems, such as storage, Microsoft Active Directory (AD), and Lightweight Directory Access Protocol (LDAP) services.

Cisco Unified Computing System™ (Cisco UCS®) servers adapt to meet rapidly changing business needs, including just-in-time deployment of new computing resources to meet requirements and improve business outcomes. The combination of Docker container technology and Cisco UCS server hardware supports highly scalable, resilient, elastic application deployment with the simplicity of the cloud and a full set of enterprise capabilities.

Docker and Cisco have developed a Cisco® Validated Design for Docker Datacenter on Cisco UCS. The validated design presents a defined process for provisioning and configuring the solution. The solution is tested in a lab setting to measure performance, scalability, availability, and failure using workloads that simulate actual production deployments. As a result, you can achieve faster, more reliable and predictable implementations.

This document demonstrates the benefits of using Cisco UCS C220 M5 servers with Docker EE to deploy, scale, and manage a production-ready application container environment. Cisco UCS is fully programmable, and it provides automated infrastructure lifecycle management. This document also describes how to deploy and run an application container using Docker EE components so that you can deploy containerized applications in your production environment with confidence. It also explains the unique and advanced capabilities of the solution to orchestrate the application container lifecycle using Docker EE on Cisco UCS infrastructure.

Reference Architecture

This section provides an overview of the Cisco UCS and Docker Enterprise Edition architectures.

Cisco UCS Programmable Infrastructure

Cisco UCS is an example of infrastructure as code (IaC). It was designed with four main technology innovations, so you can more easily define the desired state of the infrastructure and what you want to do with it. These four innovations provide the foundation for automated infrastructure management by making the infrastructure programmable:

- **Software object model:** Hardware is not configured manually in Cisco UCS. Instead, every identity and configuration setting for every device in the system is defined in software through policies and service profiles. This data model helps ensure that configurations are consistent and allows simple implementation of changes at scale.
- **API-centric approach:** The unified system control plane is accessible through a fully documented and open API.
- **Virtual interface card (VIC):** All network and SAN adapters are software defined, but they present themselves to the bare-metal OS or hypervisor as physical devices.
- **Service profiles and templates:** The infrastructure policies needed to deploy applications are encapsulated in service profiles templates, which are collections of policies needed for the specific applications. The service profile templates are then used to create one or more service profiles, which provide the complete definition of the server, storage, and fabric. Service profiles and service profile templates also help eliminate configuration drift and ensure a standardized environment for the applications.

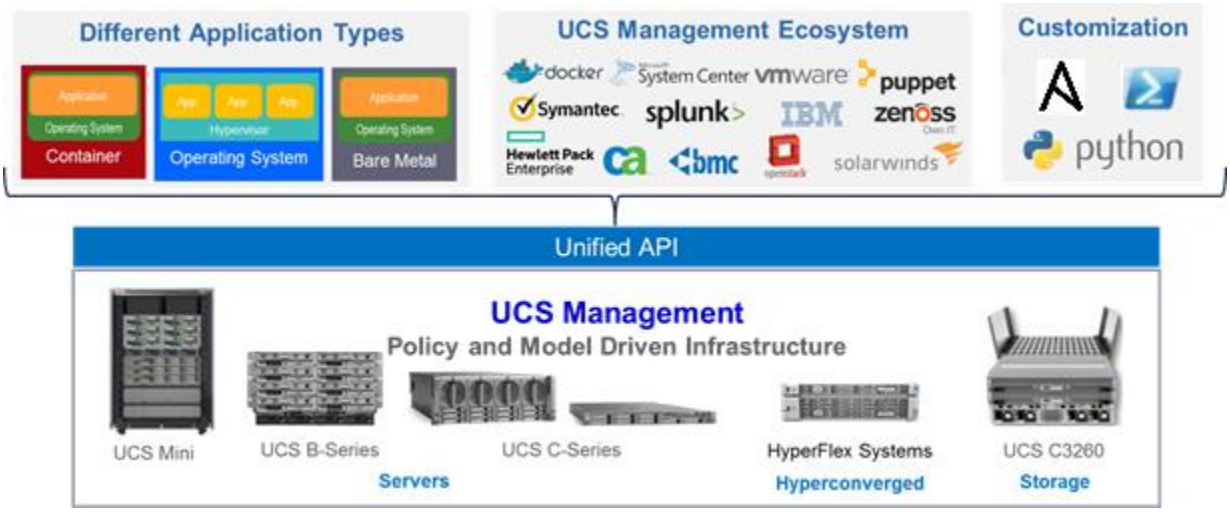
The software object model and unified API in the Cisco UCS management framework work in conjunction with the Cisco® fabric interconnects and the VICs to facilitate IaC. As a result of this programmatic capability, Cisco UCS simplifies and accelerates application and service deployment in bare-metal, virtualized, and containerized environments. Unified, model-based management, end-to-end provisioning, and migration support further ease deployment and enhance reliability and security.

Cisco UCS Manager automates the provisioning, configuration, and monitoring of the infrastructure. It includes a unified API that serves as a unified control plane for integration with Puppet and a wide range of independent software vendor (ISV) configuration, orchestration, and monitoring tools. You can use Cisco UCS PowerTool for Microsoft Windows PowerShell and a Python software development kit (SDK) for customization and further integration. You can also use Ansible, an excellent framework for organizing the data used in infrastructure configuration management. Ansible performs automation and orchestration of IT environments via Playbooks. The Playbooks are written in YAML (Yet Another Markup Language), defines a series of 'plays' that automates the

tasks across a set of hosts, known as the 'inventory'. Each 'play' consists of multiple 'tasks,' that can target one, many, or all of the hosts in the inventory. Each task is a call to an Ansible module. Cisco and Red Hat have worked together to develop an Ansible module for UCS Manager. This module works with the UCS API.

Figure 1 provides an overview of the Cisco UCS ecosystem.

Figure 1. Cisco UCS Ecosystem: High-Level View



For more information about Cisco UCS, see Cisco Unified Computing System.

Docker Enterprise Edition (EE)

Docker Datacenter is now a part of Docker EE - providing integrated container management and security from development to production. Enterprise ready capabilities like multi-tenancy, security and full support for the Docker API give IT teams the ability to scale operations efficiently without breaking the developer experience. Open interfaces allow for easy integration into existing systems and the flexibility to support any range of business processes. Docker EE provides a unified software supply chain for all apps - commercial off the shelf, homegrown monoliths to modern microservices written for Windows or Linux environments on any server, VM or cloud.

Some of the usecases for Docker Enterprise Edition include:

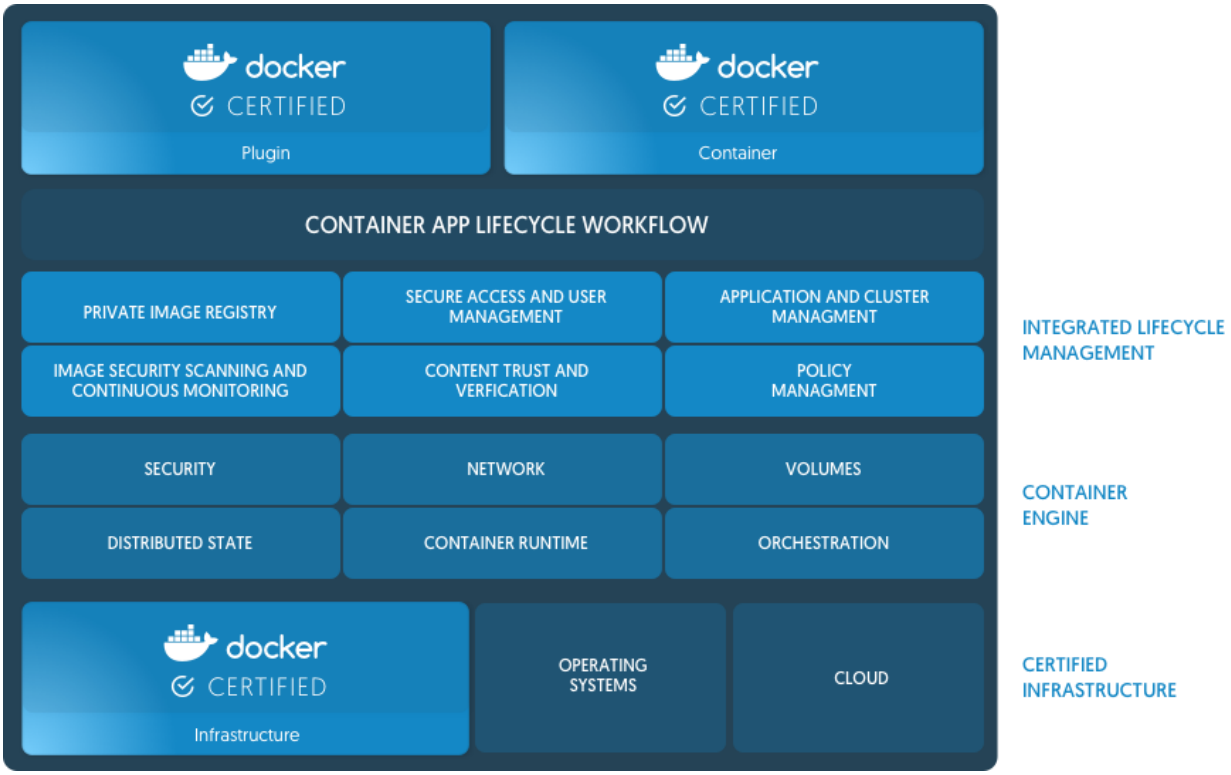
- Modernize Traditional Applications (MTA) – Improves security, costs, and cloud portability by packaging the existing applications into containers without changing the application code.
- DevOps (CI/CD) – Eliminates application conflicts and increases productivity in the development environments.
- Microservices – Streamlines application development designs with Microservices architecture.
- Hybrid Cloud – Provides application code portability from private data centers to public cloud infrastructure to another without any rework.
- Infrastructure Optimization – Improves the workload density by containerizing the applications and running them side-by-side on the same servers. This proves to be cost effective by consolidating infrastructure, improving utilization, and accelerating cloud migration.

Docker Enterprise Edition (EE) includes commercial software comprised of leading open source container technology and integration with validated and supported configurations. Docker EE comprises:

- Docker Universal Control Plane, (UCP), provides an embedded Swarm scheduler for integrated management and orchestration of the Docker environment.
- Docker Trusted Registry, (DTR), supports Docker image management, security, and collaboration.
- Docker Content Trust Security provides a multilayered approach to security, with the capability to sign images with digital keys and then verify the signature of those images.
- Docker container engine provides for a robust container runtime environment.

Figure 2 provides an overview of the Docker architecture.

Figure 2. Docker Enterprise Edition: High-Level View



Solution Components

This section introduces the Cisco and Docker components used in the solution.

Cisco UCS C220 M5 Servers

Cisco is introducing Cisco UCS C220 M5 servers which follow the Cisco C220 M4 servers. This product-line is proven to be the most versatile, high-density, general purpose enterprise infrastructure and application server. It delivers world-record performance for a wide range of enterprise workloads, including Virtualization, Collaboration, Containerization and Bare-metal applications.

The enterprise-class UCS C220 M5 server extends the capabilities of the Cisco Unified Computing System (UCS) portfolio in a one rack-unit (RU) form-factor. It provides:

- Support for 1 RU - 2 socket server using Intel® Xeon® scalable processors product family code named – Skylake-EP/ Purley
- Support for 2666MHz DDR4 DIMMs and 128GB DIMMs
- Increased storage density 10 front pluggable, 2.5" SFF drive bays, or 4 front pluggable, 3.5" LFF drive bays
- NVMe PCIe SSD support (for up to 2 drives on the standard chassis SKU or up to 10 drives on the NVMe optimized SKU)
- Cisco 12G SAS RAID Modular Controller
- 2 x Flexible Flash SD Card slots or 2 x Modular M.2 SATA slots
- 10G Embedded Intel x550 10GBase-T LOM
- 1 MLOM slot
- 2 PCIe Gen 3 Slots
- Up to 2 hot-pluggable, redundant power supplies

The new Intel® Xeon® Scalable processors provide increased core counts and faster memory. This brings in performance improvements which is ideal for scaling-up container workloads. Faster CPUs and larger memory increase workload capacity, which translates to cost effectiveness and provides quicker time to value for customers as they refresh their environment.

Cisco UCS Fabric Interconnect 6332-16UP

The 6332-16UP Fabric Interconnect is the management and communication backbone for Cisco UCS B-Series Blade Servers, C-Series Rack Servers, and 5100 Series Blade Server Chassis. All servers attached to a 6332-16UP Fabric Interconnect become part of one highly available management domain.

Because it supports unified fabric, the Cisco UCS 6300 Series Fabric Interconnect provides both LAN and SAN connectivity for all servers within its domain.

The 6332-16UP offers 40 ports in one rack unit (RU), including:

- 24 40-Gigabit Ethernet and Fibre Channel over Ethernet (FCoE)
- 16 1- and 10-Gbps and FCoE or 4-,8-, and 16-Gbps Fibre Channel unified ports
- Enhanced features and capabilities include:
- Increased bandwidth up to 2.43 Tbps
- Centralized unified management with Cisco UCS Manager
- Efficient cooling and serviceability such as front-to-back cooling, redundant front-plug fans and power supplies, and rear cabling

Cisco UCS Manager

Cisco UCS Manager provides unified, embedded management for all software and hardware components in Cisco UCS servers. It manages, controls, and administers multiple chassis for thousands of virtual machines as a single logical entity through an intuitive GUI, a command-line interface (CLI), or an XML API. Cisco UCS Manager resides

on a pair of Cisco UCS fabric interconnects using a clustered, active-standby configuration for high availability. It provides an embedded management interface that integrates server, network, and storage resources. The manager performs auto-discovery to detect, manage, and provision system components that are added or changed. The API exposes 9000 points of integration and facilitates integration with third-party operations management tools and custom development for automation, orchestration, and monitoring.

Service profiles benefit both virtualized and nonvirtualized environments and increase the mobility of nonvirtualized servers: for instance, when moving workloads from server to server or taking a server offline for maintenance or upgrade. Profiles can also be used in conjunction with virtualization clusters to bring new resources online easily, complementing existing virtual machine mobility.

For more information about Cisco UCS Manager, see http://www.cisco.com/c/en/us/products/servers-unified-computing/ucs-manager/index.html

Docker Universal Control Plane

Universal Control Plane is a containerized application that runs on Docker Enterprise Edition and extends its functionality to make it easier to deploy, configure, and monitor your applications at scale. It also secures Docker with role-based access control so that only authorized users can make changes and deploy applications to your Docker cluster.

Once Universal Control Plane (UCP) is deployed, developers and IT operators no longer interact with Docker Engine directly, interact with UCP instead. Since UCP exposes the standard Docker API this is all done transparently, so that you can use the tools such as the Docker CLI client and Docker Compose.

Docker UCP leverages the clustering and orchestration functionality provided by Docker. The cluster management and orchestration features embedded in the Docker Engine are built using **SwarmKit**. Docker engines participating in a cluster are running in **swarm mode**. You enable swarm mode for an engine by either initializing a swarm or joining an existing swarm.

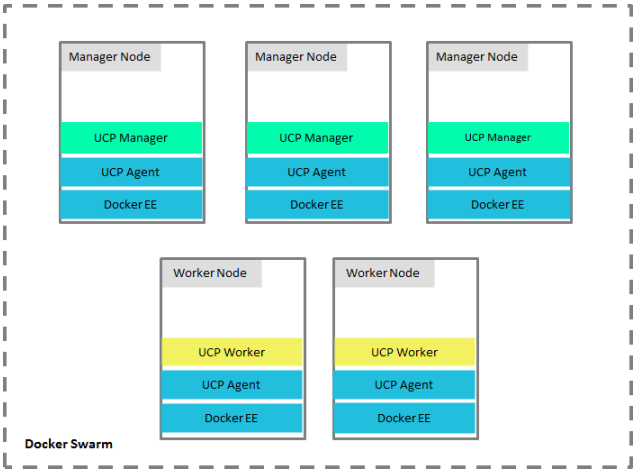
A **swarm** is a cluster of Docker engines, or UCP nodes, where you deploy services. The Docker Engine CLI and API include commands to manage swarm nodes (e.g., add or remove nodes), and deploy and orchestrate services across the swarm.

If the UCP node is a:

- **Manager**: the `ucp-agent` service automatically starts serving all UCP components including the UCP web UI and data stores used by UCP. The `ucp-agent` accomplishes this by deploying several containers on the node. By promoting a node to manager, UCP automatically becomes highly available and fault tolerant.
- **Worker**: on worker nodes the `ucp-agent` service starts serving a proxy service that ensures only authorized users and other UCP services can run Docker commands in that node. The `ucp-agent` only deploys a subset of containers on worker nodes.

It is recommended to run UCP Manager nodes in high-availability mode. For high-availability, a minimum of three manager nodes are required. The figure below shows UCP Managers running high-availability mode with rest of the nodes configured as UCP Worker.

Figure 3. Containerized Docker UCP in a Docker Swarm Cluster



A swarm is a collection of nodes that are in the same Docker swarm. Nodes in a Docker swarm operate in one of two modes: Manager or Worker. If nodes are not already running in a swarm when installing UCP, nodes will be configured to run in swarm mode.

For more information on Docker UCP, see: https://docs.docker.com/datacenter/ucp/2.1/guides/architecture/#how-you-interact-with-ucp

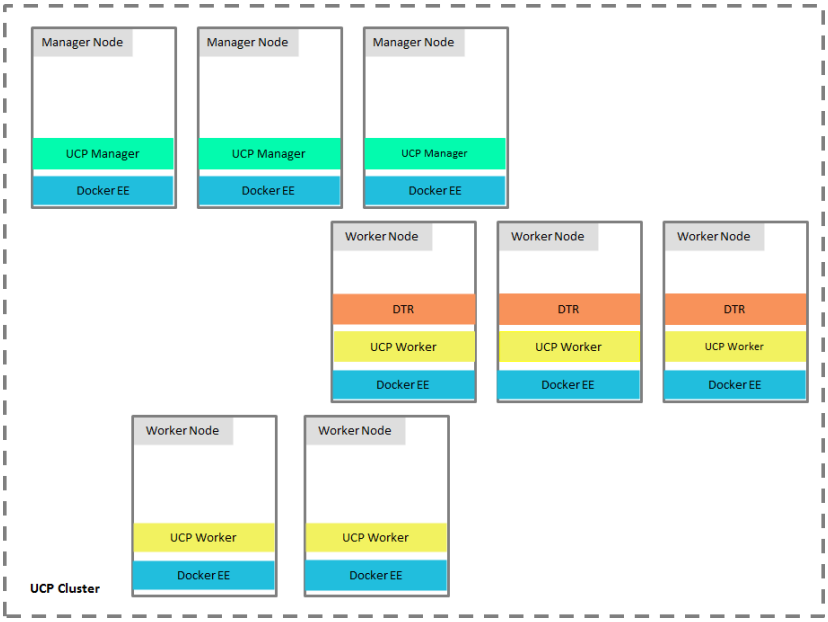
Docker Trusted Registry

Docker Trusted Registry (DTR) is a containerized application that runs on a Docker Universal Control Plane cluster. Docker DTR gives Enterprise a trusted image repository for their application container images used locally.

For high-availability you can deploy multiple DTR replicas - minimum number of replicas being three, one on each UCP Worker node. All DTR replicas run the same set of services and changes to their configuration are automatically propagated to other replicas.

The figure below shows DTR running in HA mode with three DTR replicas on three different UCP Worker nodes.

Figure 4. Containerized DTR Application in UCP Cluster



For more information on DTR, see: https://docs.docker.com/datacenter/dtr/2.2/guides/architecture/ - dtr-internal-components

Solution Components

Table 1 lists the infrastructure hardware components used in this solution.

Table 1. Solution Components

Component	Model	Quantity
Docker UCP Manager + DTR and Docker UCP Worker	Cisco UCS C220 M5 Server	4
Fabric interconnect	Cisco UCS 6332-16UP Fabric Interconnect	2
Switch	Cisco Nexus® 9396PX Switch	2

Physical Topology

Figure 5 shows the topology with Cisco Nexus 9396PX top-of-rack (ToR) switches, Cisco UCS 6332-16UP fabric interconnects, and Cisco UCS C220 M5 servers forming the Cisco UCS infrastructure for Docker Enterprise Edition.

A Docker UCP cluster consists of two types of nodes:

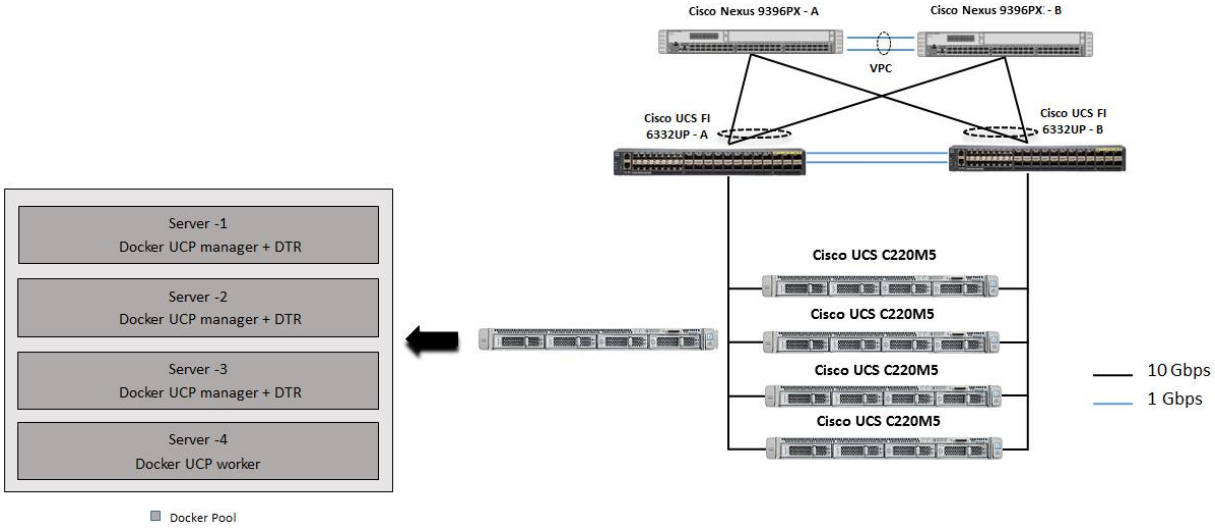
- UCP Worker node is primarily for running containers.
- UCP Manager nodes are for running containerized UCP services. The UCP Manager node acts as the primary node for the UCP cluster and UCP Manager replicas are in HA mode with the UCP Manager.

The UCP Manager nodes persistently manage the cluster and cluster configurations. All UCP services nodes can handle application container workloads and can be configured to run only UCP services such as scheduler and

orchestration tasks. UCP Worker nodes act as computing nodes and handle application container workloads. DTR services are co-hosted and run as an application container stack on the UCP Manager nodes.

Note: Docker UCP Manager nodes can also take up application container workload based on the administrator's choice.

Figure 5. Docker Enterprise Edition on Cisco C220 M5 Servers



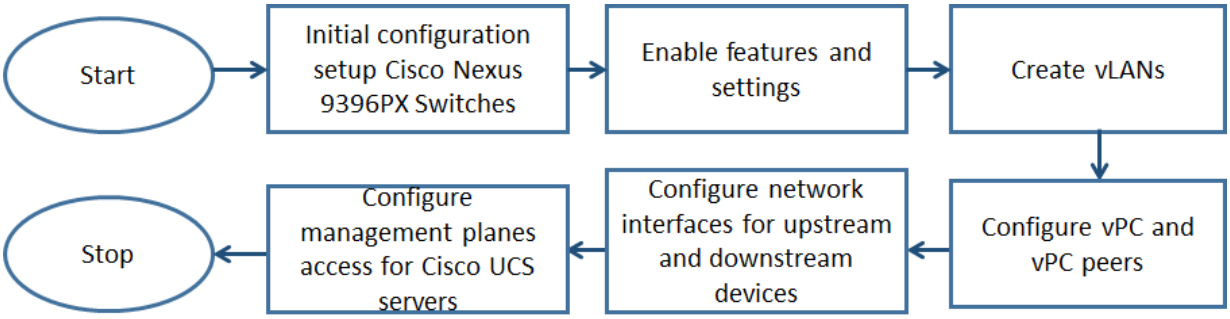
Installation Workflow

The solution as a whole consists of Cisco UCS C220 M5 servers, Cisco UCS 6332-16UP fabric interconnects, and Cisco Nexus 9396PX ToR switches as hardware components. The Docker Enterprise Edition and Cisco UCS Manager are part of the software components of the solution. The Docker software stack runs on the Red Hat Enterprise Linux 7.3 bare metal OS. Managed Cisco UCS C220 M5 servers provide a converged and highly available hardware platform centrally managed by Cisco UCS Manager software residing on third generation Cisco UCS fabric interconnects. An important component of the Docker Enterprise Edition product, Docker UCP provides the redundancy, orchestration services and high availability of the Docker Enterprise Engine and management interface. This solution holistically offers a container-as-a-service model that supports deployment of diverse application environments in DevOps and production use cases.

Cisco Nexus 9396PX Switch Configuration

Figure 6 shows the configuration process for the Cisco Nexus 9396PX Switches.

Figure 6. Cisco Nexus 9396PX Configuration Process

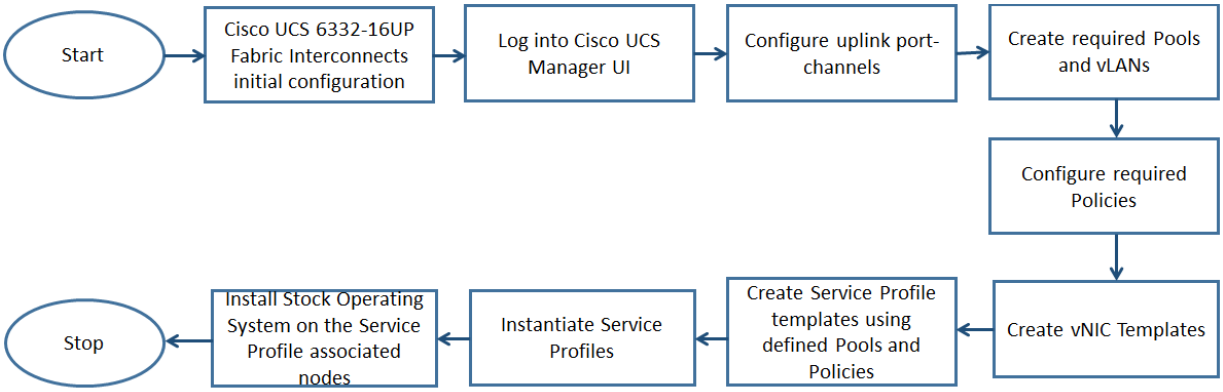


Cisco Nexus 9396PX Switches include ToR or middle-of-row (MoR) fiber-based server connectivity suitable for deployment in small business, enterprise, and service provider environments. Enhanced Cisco NX-OS Software is designed to provide a robust feature set, including performance, resiliency, scalability, manageability, and programmability features. In this solution, a pair of Cisco Nexus 9396PX upstream switches is deployed to provide northbound network connectivity for the application containers. Furthermore, these switches provide redundancy for the application container data path, using a Cisco virtual port-channel (vPC) configuration between the Cisco Nexus 9396PX Switches and Cisco UCS 6332UP fabric interconnects.

Cisco UCS Manager Configuration

Figure 7 shows the configuration process for Cisco UCS Manager.

Figure 7. Cisco UCS Manager Configuration Process



Cisco UCS management software delivers policy-based automation and role-based access capabilities to help you effectively administer and manage data center infrastructure at scale. This tightly integrated management solution uses a DevOps-friendly architecture that treats infrastructure as lines of code, with every component programmable. It provides a model-based foundation to simplify the day-to-day processes of provisioning, monitoring, and managing computing and local storage resources and storage and network connections. These novel features coupled with an open XML API facilitates integration with third-party infrastructure automation tools such as Ansible, Puppet, and Chef for day-zero provisioning, management, and monitoring tasks.

The Cisco UCS converged infrastructure model emphasizes the use logical servers rather than traditional physical servers (blade or rack). Service profiles, which are software definitions of servers, shift Cisco UCS from conventional servers to logical servers. The service profile contains all the server hardware identifier, firmware, state, configuration, connectivity, and behavior information, but is totally abstracted from the physical server.

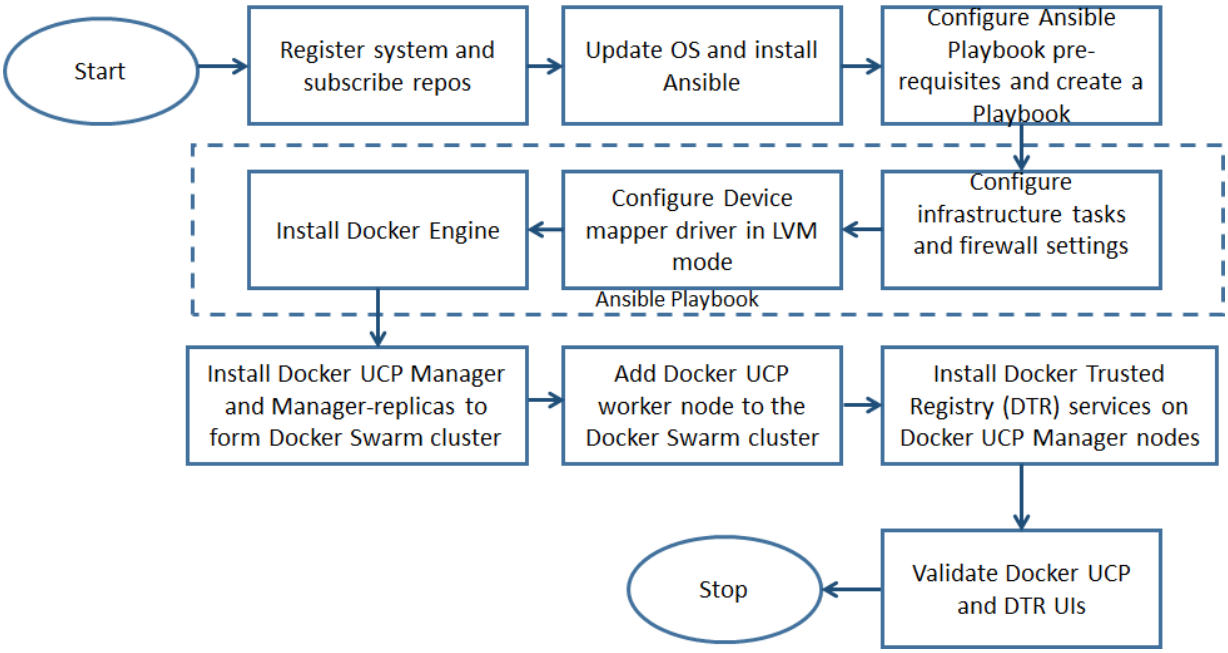
Service profiles form the foundation for the stateless, utility computing model in Cisco UCS. Virtualization of MAC addresses and World Wide Port Name (WWPN) identifiers has been evolving in the industry for years, but Cisco UCS extends the logical service profile definition to include the hardware, BIOS, CPU, I/O adapter, local storage configurations through policies, pools, isolation, and templates.

One of the main benefits of application containers is software portability. Cisco UCS infrastructure extends the concept of portability to include the operating system and underlying hardware in addition to the deployed applications. Stateless computing, a distinguishing feature of Cisco UCS servers, provides the capability to move workloads from one sever to another in the event of hardware failure with little downtime.

Docker Enterprise Edition Deployment

Figure 8 shows the Docker Enterprise Edition deployment process.

Figure 8. Docker Enterprise Edition Deployment Process



Host setup day-zero automation tasks are run on all the participating server nodes in the cluster using the Ansible automation tool. This tool does not use a client-server model and does not need an additional build server. Any node can be initiated to run some limited host setup tasks even before the Docker Enterprise Edition is deployed on the nodes.

Validation

After the stack is up and running, you can validate the stack by installing a sample WordPress two-tier application on the stack.

The WordPress application is an open-source blogging tool and content-management system based on PHP and MySQL. The application runs on a web hosting service. It has two components: a front-end web interface and a back-end MySQL or MariaDB database. Both components run as application containers on Docker UCP nodes as scheduled by the UCP services nodes. This scheduling is performed through either the Docker UCP dashboard user interface or the UCP CLI.

Figures 9 through 14 show the various stages of containerized application deployment using Docker EE on Cisco UCS C-Series servers.

- **Cluster status**: Docker UCP shows all the Manager nodes with their status. The dashboard in Figure 9 shows the number of containers spawned and the number of nodes used in this solution.

Figure 9. Cluster Status – Docker UCP UI

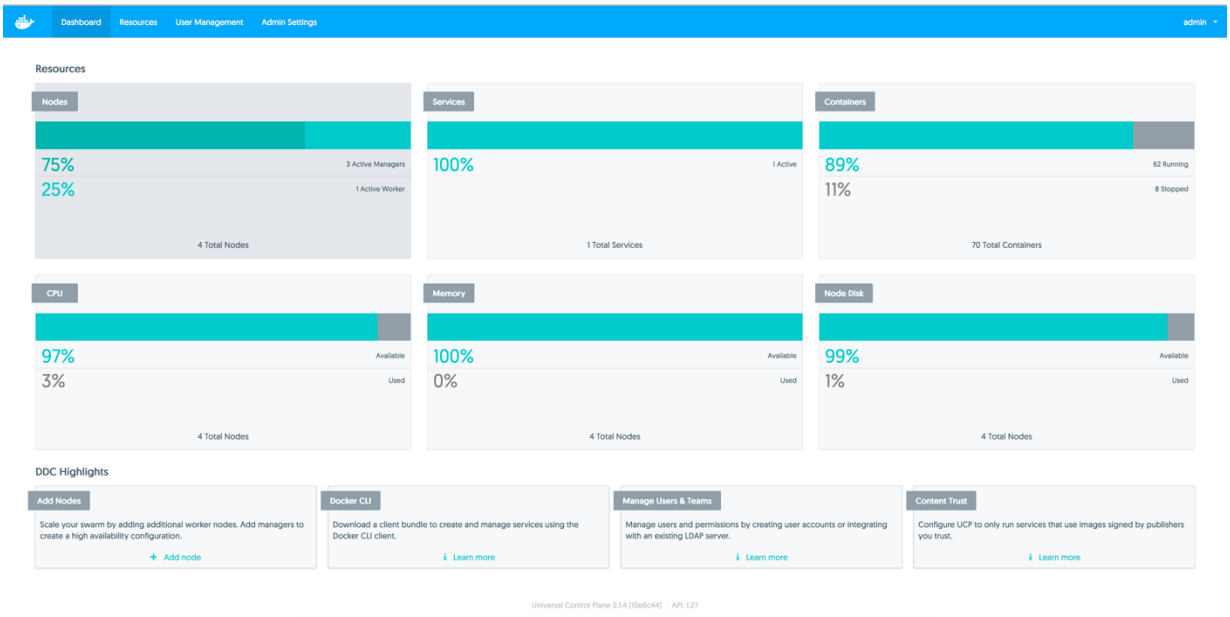
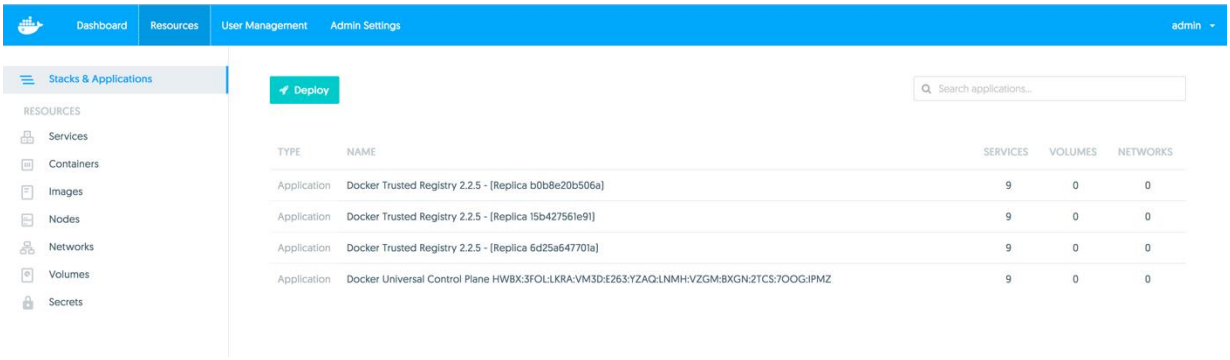
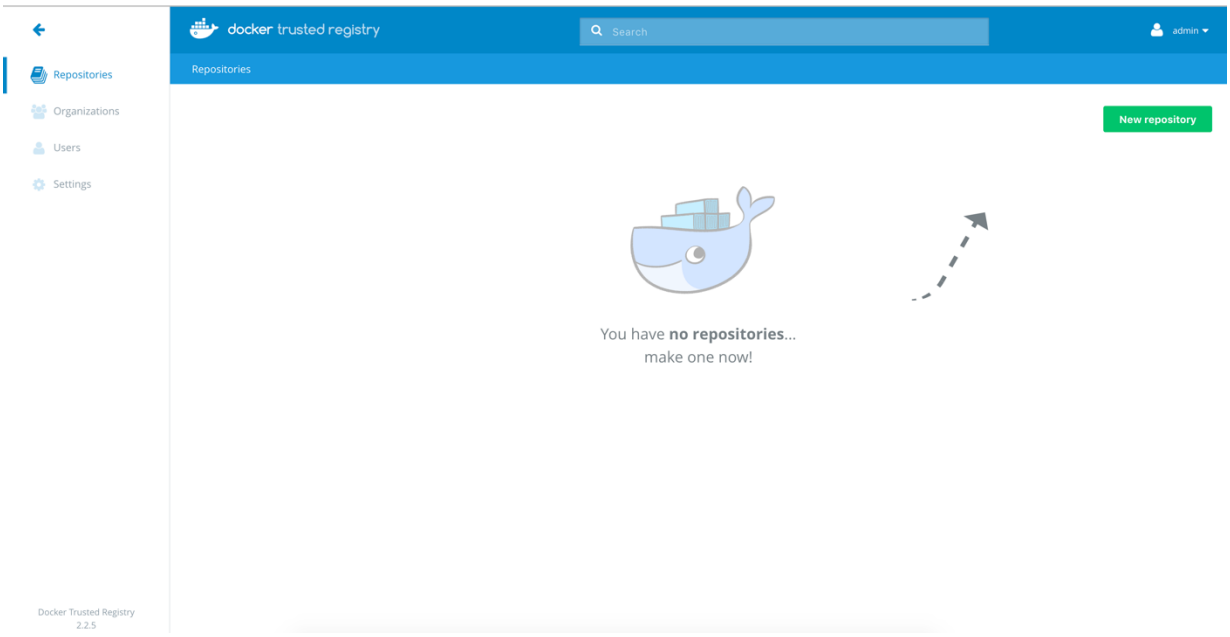


Figure 10. DTR Application Co-hosted on Docker UCP Manager and Replica Nodes



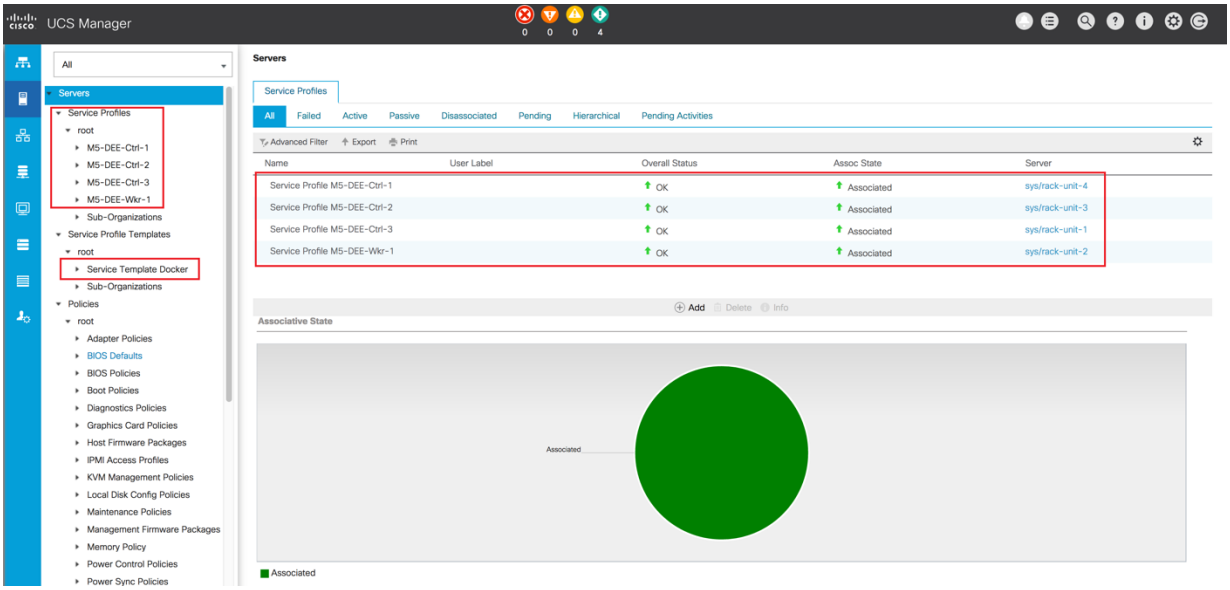
- **DTR status**: The dashboard in Figure 11 shows the configured DTR and the number of instances running. DTR is responsible for Docker image management, security, and collaboration.

Figure 11. Docker Trusted Registry Status



- **Cisco UCS Manager**: The Cisco UCS Manager GUI shows four service profiles configured for Cisco UCS C220 M5 servers. The status details in Figure 12 screenshot show the assignment and association status of the C220 M5 servers with respective service profiles.

Figure 12. Cisco UCS Manager Details

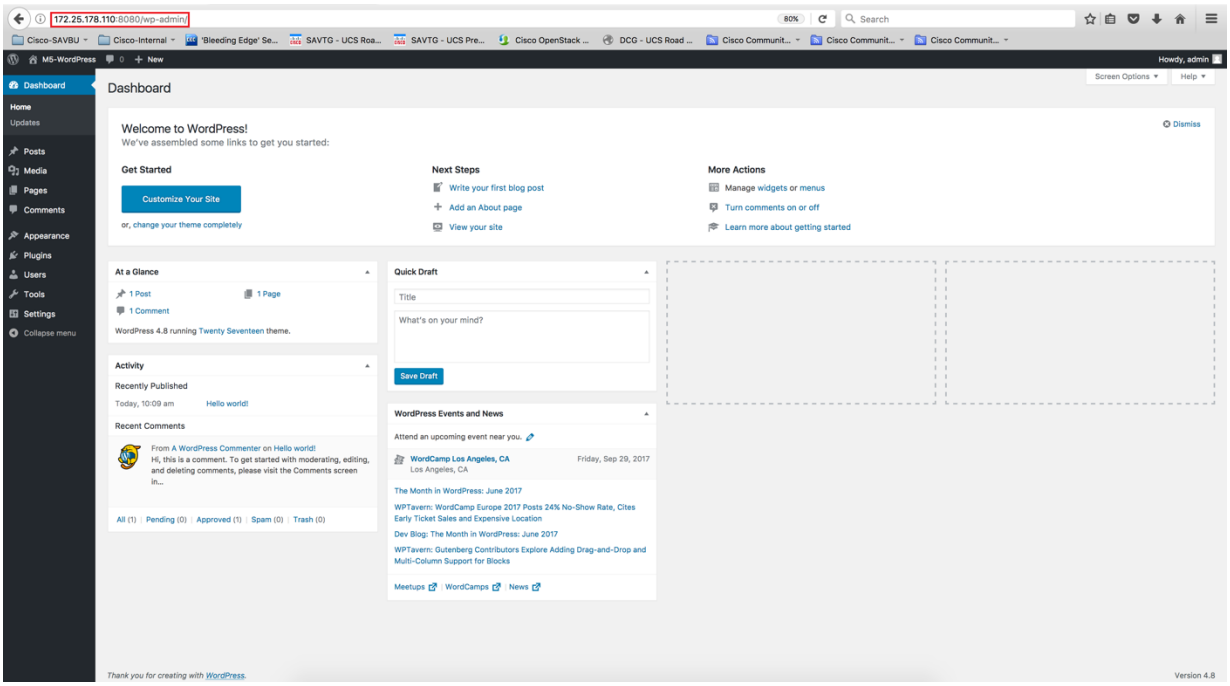


- **Application container**: In this solution, the WordPress application is deployed on the Cisco UCS C220 M5 servers. Figure 13 shows the successful deployment of the WordPress application using Docker Enterprise Edition on a Cisco UCS C220 M5 server. You can see the status of the containerized application on the Docker Enterprise Edition platform by entering the **docker ps** command on all the configured server nodes. Figure 14 shows the WordPress application webpage accessed with the UCP Worker node IP address with the specified port number appended to it.

Figure 13. WordPress Application Container Shown on Docker UCP Worker Node

```
[root@M5-DEE-Wkr-1 ~]# docker ps
CONTAINER ID        IMAGE                                                                                                COMMAND                  CREATED
      STATUS              PORTS                    NAMES
cc904e4773aa        wordpress                                                                                            "docker-entrypoint..."   5 minutes ago
      Up 5 minutes        0.0.0.0:8080->80/tcp     wordpress_wordpress_1
66b24e89fd08        mariadb                                                                                              "docker-entrypoint..."   5 minutes ago
      Up 5 minutes        3306/tcp                 wordpress_db_1
b4642b7b5651        docker/ucp-agent@sha256:d072694d639fbbe1a0e3e6a0e2ac9fdf4770daa186a5d7f39a4a0e0aadfe4be6   "/bin/ucp-agent agent"   58 minutes ago
      Up 58 minutes       2376/tcp                 ucp-agent.at1ccp56e01sunha3tzn5iiwu.0m159ipka43vfxr20jz322va3
fa618cb15ca8        docker/ucp-agent:2.1.4                                                                               "/bin/ucp-agent pr..."   About an hour
ago   Up About an hour    0.0.0.0:12376->2376/tcp  ucp-proxy
[root@M5-DEE-Wkr-1 ~]#
```

Figure 14. Accessing Application Container Deployed on UCS Worker Node



Conclusion

The integration of Docker Enterprise Edition with Cisco UCS M5 C-Series Servers is intuitive and gives improved processing performance and faster memory which is best suited for Container application at scale. This platform also provides high density compute nodes for scaling container application environment at will. This integration enables enterprises to deploy and manage highly scalable and fast-evolving application containers to the data center environment. This document provides insight into deploying the Docker Enterprise Edition on Cisco UCS. It explains the deployment, management, and scalability aspects of Docker containers. Large numbers of nodes can easily be deployed, and they can be easily added into the existing cluster by using infrastructure automation tools such as Ansible. Docker UCP provides a single control plane for operations from runtime container processing through container lifecycle management, and Cisco UCS provides the converged computing, network, and storage platform needed to run the entire stack.

References

- Design and Deployment Guide for Cisco UCS Infrastructure with Docker Datacenter for Container: Management: http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/ucs_docker.html
- Cisco UCS Infrastructure with Docker Datacenter for Container Management: http://www.cisco.com/c/en/us/solutions/collateral/data-center-virtualization/unified-computing/whitepaper-c11-737985.html

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

Printed in USA

C11-739330-00 07/17