Administration

Rack-Mount Server Daily Operations

At this point the application is installed and in operation. Daily operations for applications are similar to an installation on a physical server, including:

- Application configuration and integration with other applications
- RTMT performance monitoring
- SNMP monitoring and alarms
- DRS backup and restore
- CDR collection
- Device, trunk, gateway configuration and monitoring

Monitoring From Virtual Machine

Applications running in a VM have no ability to monitor the physical hardware. Any hardware monitoring must be done from the Cisco Integrated Management Controller, ESXi plugins, vCenter or by physical inspection (for flashing LEDs, and so on).

Monitoring of hardware is the customer's responsibility. It is assumed the customer is familiar with virtualized environments and knows how to manage hardware in these environments.

Monitoring From Cisco Integrated Management Controller

The Cisco Integrated Management Controller (Cisco IMC) provides the following hardware monitoring:

- An overview of CPU, memory, and power supply health
- An overview of hardware inventory, including CPUs, Memory, Power Supplies, and Storage
- Monitoring of sensors for Power Supplies, Fans, Temperature, Voltage, and Current
- A system event log that contains BIOS and Sensor entries
- LSI MegaRAID controller information, which includes physical and virtual drive layout and Battery Backup Unit information from the Inventory > Storage tab. This information was usually accessible for earlier UCS servers only by installing the MegaRAID plugin from ESXi.

For additional details, go to https://www.cisco.com/c/en/us/products/servers-unified-computing/index.html.

Monitoring From vSphere Client and vCenter

The vSphere Client provides the following monitoring:

- Hardware and system alarms defined under the Alarms tab in the vSphere Client when logged in to vCenter.
- VM resource usage under the Virtual Machines tab in the vSphere Client, as well as under the Performance tab for each VM.
- Host performance and resource usage under the Performance tab for the host.

For more information, go to http://www.VMware.com.

Server Health Monitoring From ESXi

You can monitor server health from ESXi by logging into the ESXi console and inspecting system /var/log/messages for telltale entries.

Disk Management for Cisco UCS Rack-Mount Servers

For details on the drive specifications for your Cisco UCS server, refer to RAID Configuration.

Disks are hot-swappable. This does not mean that you will be able to swap drives ad-hoc after a failure. A process exists to swap drives. When a drive fails, you need to follow these steps:

Note If you have an M4 server, refer to http://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/c/hw/C240M4/install/C240M4.pdf.

1. Reboot and enter the Preboot CLI.
2. Mark the defective drive for removal using **-PdPrpRmv -physdrv [<encl>:<slot>] -a0**.
3. Replace the drive.

The RAID array is rebuilt automatically when the replacement disk is inserted.

Note Although Preboot CLI is recommended, you can also perform this task through the LSI MegaRaid GUI, where you can swap drives out without having to power-cycle the server to get into the preboot CLI. However, this method requires you to procure a separate machine (Windows or Linux) on the same subnet as the ESXi host, installed with the LSI MegaRaid utility.

Automatic Update Statistics

Communications Manager uses Automatic Update Statistics, an intelligent statistics update feature that monitors the changes made in the database tables and updates only tables that need statistic updates. This feature saves considerable bandwidth, especially on VMware deployments of Communications Manager. Automatic Update Statistics is the default indexing method.

For more information about database services, see the *Cisco Unified Serviceability Administration Guide*.

New Identity

Cisco supports the New Identity process for use with Cisco Unified Communications Manager. The New Identity process is designed to start with a Communications Manager application that is fully installed and configured with common settings. Often, the initial VM is saved as a VMware template and cloned as new Communications Manager publisher nodes come online.

The New Identity process copies the VMware template and changes a set of primary settings, such as the IP address and hostname, to give a new VM a unique identity in the network.

Run New Identity Process

Procedure

Step 1 Create a new VM instance from the template of the deployed Unified CM application.

Step 2 Run the CLI command **utils import config**.

For more information about CLI commands, see the documentation at https://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.

New Identity Caveats

When you run the New Identity process, note the following:

- Although you can provide a new OS administrator user ID in the XML file, you cannot change the OS administrator user ID during the New Identity process.
- Each cloned VM has the same network configuration as the VMware template. The network must be functional during the New Identity process. If you run the cloned VMs on the same LAN there can be duplicate IP addresses. Ensure that you do not run the VMware template, or multiple VMs from the initial template, at the same time on the same LAN.
- The NTP server must be accessible before you can configure it on the Unified CM application. Ensure that the VM has access to the new NTP server.
- If DNS is used, DNS servers must be accessible when you run the New Identity process.
- For Cisco Unity Connection, you must set the SMTP domain address after you run the New Identity process.
- For Cisco Unified Presence, you must set the postinstallation steps that configure the Unified CM system with which Cisco Unified Presence communicates after you run the New Identity process.

Deploy Cluster Nodes Using Templates

Procedure

Step 1 Perform a skip install.

Step 2 When prompted for the floppy/USB drive in the **Pre-existing Configuration Information** window, power down the VM.

Step 3 Clone or convert the VM into a VM template.

Step 4 For a new node, deploy the template and mount a virtual floppy drive that contains the configuration file from the AFG tool.

Related Documentation

- **Cisco UCS documentation:** http://www.cisco.com/go/ucs
- **Cisco HyperFlex documentation:** www.cisco.com/go/hyperflex
- The official list of supported servers for Cisco Unified Communications Manager releases is available at the following URL: http://www.cisco.com/go/virtualized-collaboration
- Technical specifications of Cisco Unified Communications virtualized servers are available at the following URL: http://www.cisco.com/go/virtualized-collaboration
- TCP and UDP ports for vCenter Server, ESX hosts, and other management access for other network components are listed in article 1012382 at the following URL:

http://kb.vmware.com

- The Cisco Unified Communications Virtualization docwiki, which discusses deployment of other Cisco Unified Communications products on virtualized servers, is available at the following URL: http://www.cisco.com/go/virtualized-collaboration