Cisco Physical Access Manager Deployment on UCS B and C-Series Platforms

Contents

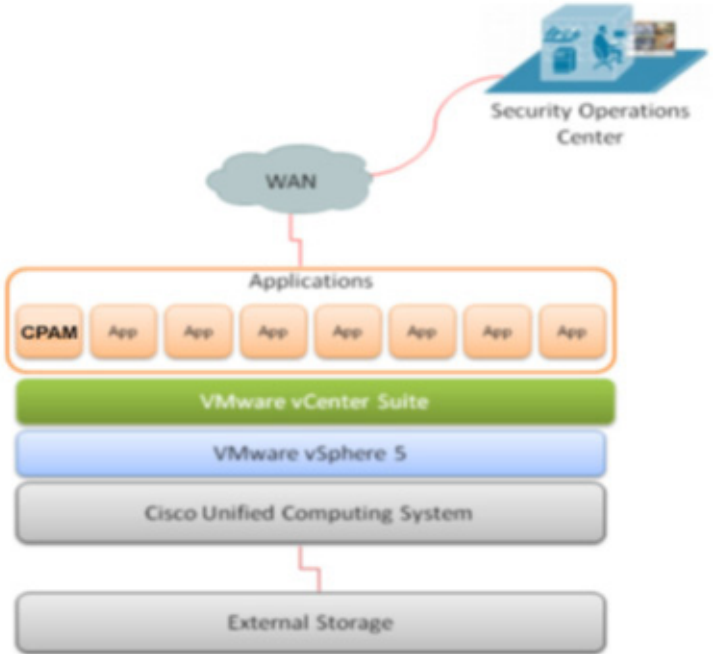
Implementing CPAM on the UCS B and C-Series Platforms

This section summarizes the high-level design recommendations and best practices for implementing CPAM on the UCS B and C-Series platforms. In some instances, existing network equipment and topologies have the necessary configuration and performance characteristics to support CPAM.

Figure 1 represents a virtualized CPAM application running on a UCS B-Series platform.

Cisco Systems, Inc.
www.cisco.com

Figure 1 Cisco Physical Access Manager on UCS.



Solution Components

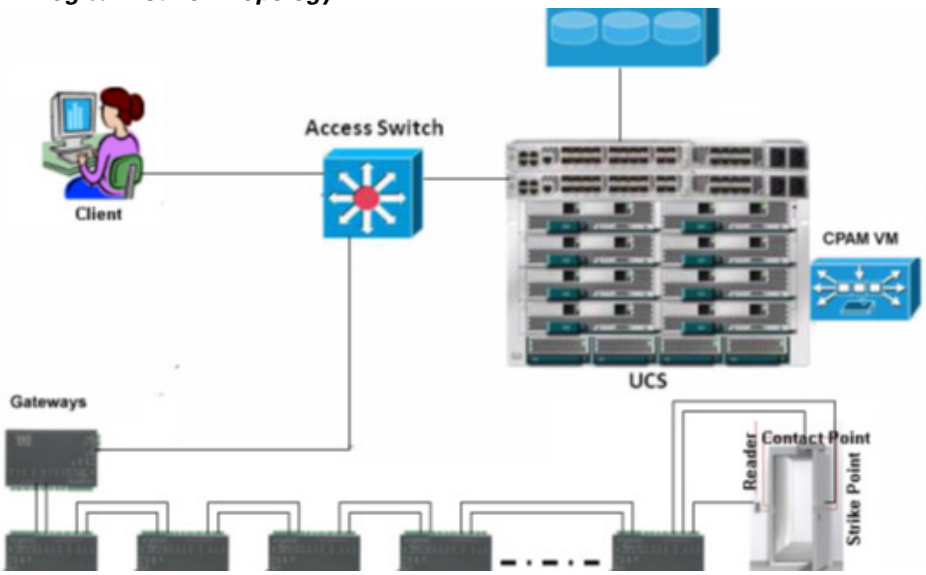
The components required for designing and deploying CPAM on UCS Band C–Series platforms include:

- **UCS B and C-Series servers**—The Cisco UCS Servers can be deployed as rack-mount servers (C-Series) or blade servers (B-Series) running the ESXi 5.0 virtualization software. The B-Series servers deliver a scalable and flexible architecture to meet your data center needs while helping to reduce the total cost of ownership. The C-Series servers address fluctuating workload challenges through a varying balance of processing, memory, I/O, and internal storage resources.
- **Cisco Physical Access Manger (CPAM) software**—This software runs on UCS B or C-Series server in a virtualized environment. The CPAM on UCS software is available for download with purchase of the CPAM on UCS software license R-CIAC-PAME-VM-K9=. This software is an Open Virtual Appliance (OVA) file on Cisco.com. The OVA package is a tar file with the Open Virtualization Format (OVF) directory inside.

Logical Network Topology

Figure 2 illustrates the overall logical topology of the networking and CPAM components, including a UCS B-Series containing the ESXi host CPAM, gateways, expansion modules, and the operator workstations running the CPAM client.

Figure 2 Logical Network Topology



Note This guide does not describe the configuration and operation of the Cisco Physical Access Manager (CPAM) products, For more information see, http://www.cisco.com/en/US/products/ps9688/prod_installation_guides_list.html

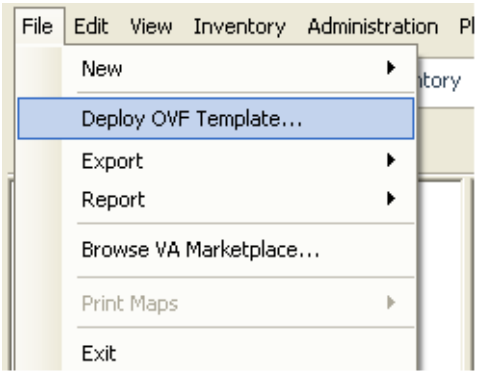
Deploying the OVF Template

Tip Before performing the following steps, ensure that the ESXi 5.0 Hypervisor is installed on the UCS B or C–Series platforms.

To deploy the OVF template, complete the following procedure:

Step 1 Login to vSphere Client.

Step 2 From the File menu, select **Deploy OVF Template**. The Deploy OVF Template page opens.



Step 3 Click **Browse** to select the path of the OVF file from the local directory or URL using the source window.

Step 4 Click **Next** and the OVF Template Details page appears displaying the CPAM version and disk properties.

Step 5 For a VMware vCenter Server, select the Host and Datastore. For a single ESXi Host, go to Step 8 and choose the disk format.

Step 6 Click **Next** and the Name and Location page opens.

Step 7 Enter the CPAM appliance name.

Step 8 Click **Next**, the Disk Format page opens.

Step 9 Select the desired provisioning policy for the virtual disk file.

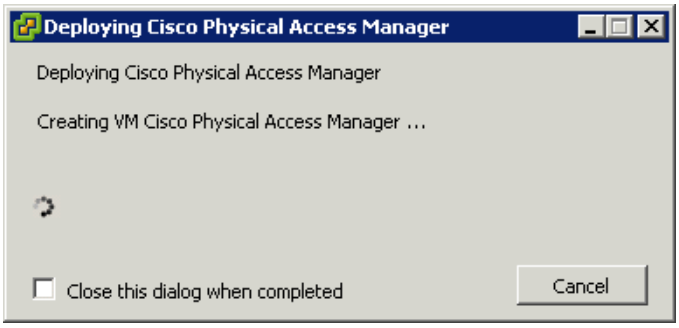
Note It is advisable to choose either Thick Provision Lazy Zeroed or Thin Provision. It takes a longer time to create a disk with Thick Provision Eager Zeroed format.

Step 10 Click **Next**, the Ready to Complete page opens.

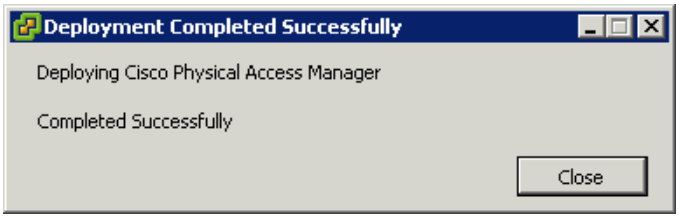
Step 11 Check the **Power on** after deployment checkbox.

Step 12 Click **Finish** to start the OVF deployment process.

Step 13 While processing, the following dialog box appears.



Step 14 When deployment is complete, the following dialog box appears.



Configuring Ethernet 0 IP Address

To configure Ethernet 0(eth0) IP address, complete the following procedure:

Step 1 Launch console connection for the installed Cisco Physical Access Manager from vSphere Client.

Step 2 Login with the default user name and password (cpamadmin/cpamadmin).

Step 3 Change the permission to super user (sudo su-).

Step 4 Copy ifcfg-eth0 file in **/**home/cpamadmin to /etc/sysconfig/network-scripts/ using the following command:

```
cp /home/cpamadmin/ifcfg-eth0/etc/sysconfig/network-scripts/
```

Step 5 Edit the file using vi and change the default IP, subnet mask, and the default Gateway for the **ifcfg-eth0** file in - **/ etc/sysconfig/network-scripts/**.

Sample configuration of ifcfg-eth0:

```
DEVICE=eth0
BOOTPROTO=static
USERCTL=no
PEERDNS=yes
IPADDR=192.168.1.2
NETMASK=255.255.255.0
ONBOOT=yes
TYPE=Ethernet
GATEWAY=192.168.1.1,
```

Note The above network parameters IPADDR, NETMASK, and GATEWAY must be configured based on the network.

Step 6 Restart the network services using - **/sbin/service network restart**

Step 7 Check the eth0 configuration using - **/sbin/ifconfig**

Step 8 Restart the cpamadmin service using- **/sbin/service immortal restart**

Now the CPAM appliance is ready for the Initial setup.

Note The CPAM VM, gateways, expansion modules, and CPAM client workstations are reachable in the network.

Upgrading/Downgrading Memory Configuration

CPAM 1.5.1 OVA supports change in VM memory configuration to 16, 32, or 64GB.

Note This procedure is applicable only when CPAM 1.5.1 is running on UCS servers.

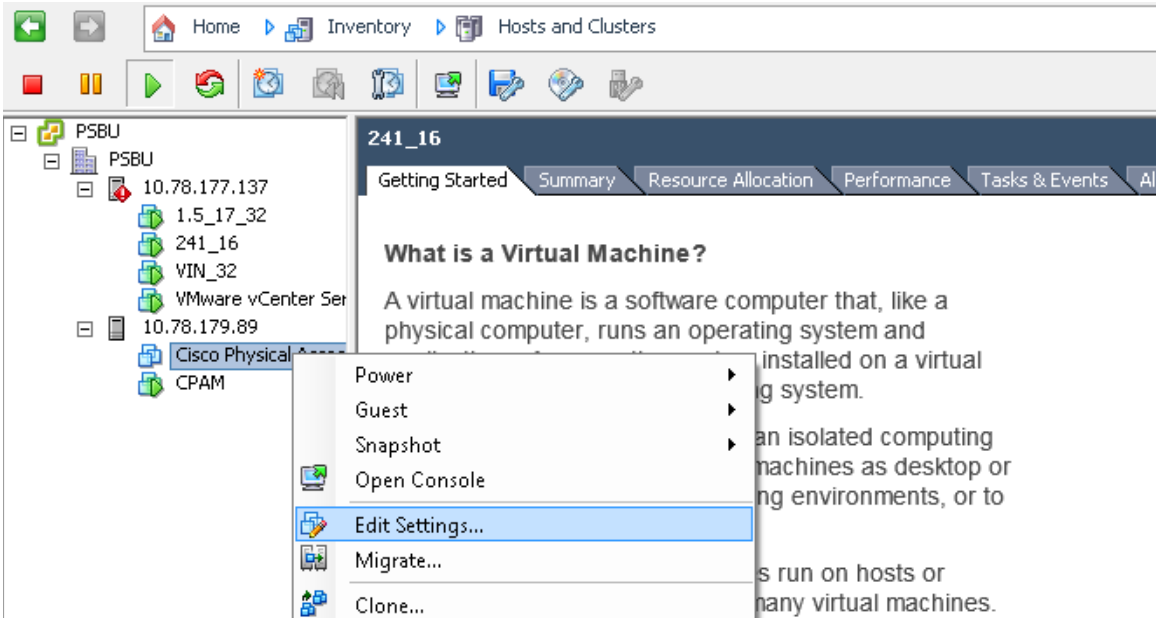
Note In case of a HA enabled setup, follow steps 1 to 5 in the Standby server before performing the steps in the Active server.

Step 1 Launch the CPAM web admin and enter **Stop** command.

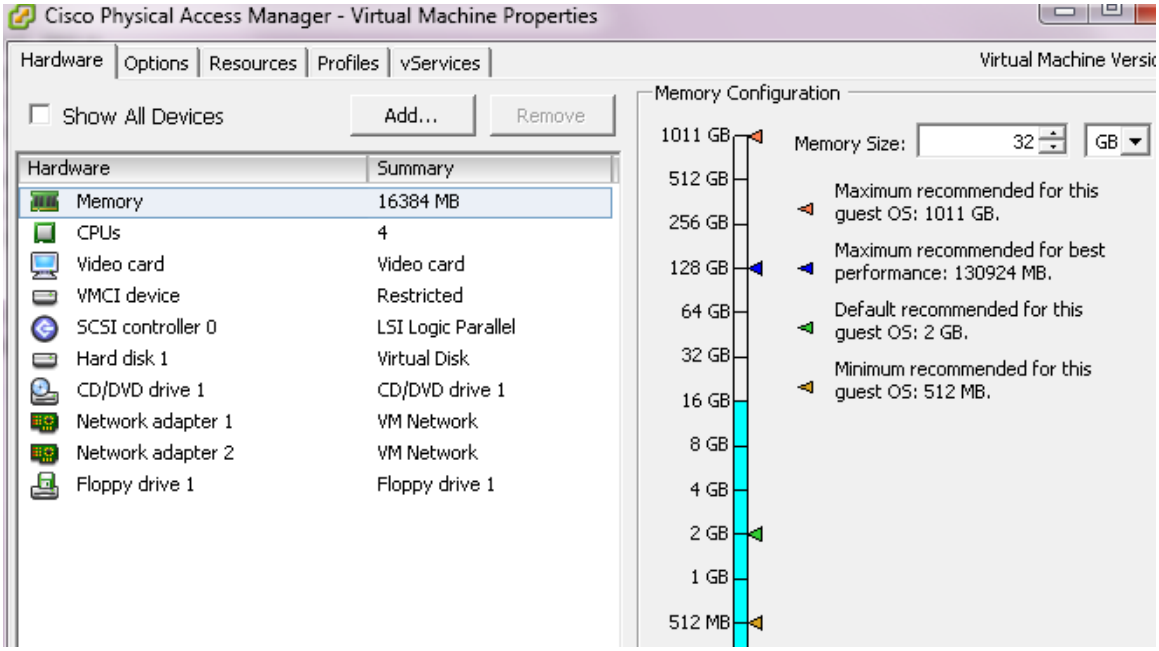
Step 2 Verify that the server status is down and then choose **Commands > Shutdown**. This will power off the VM.

Step 3 Log in to vSphere Client.

Step 4 Right click the VM and choose **Edit Settings.**

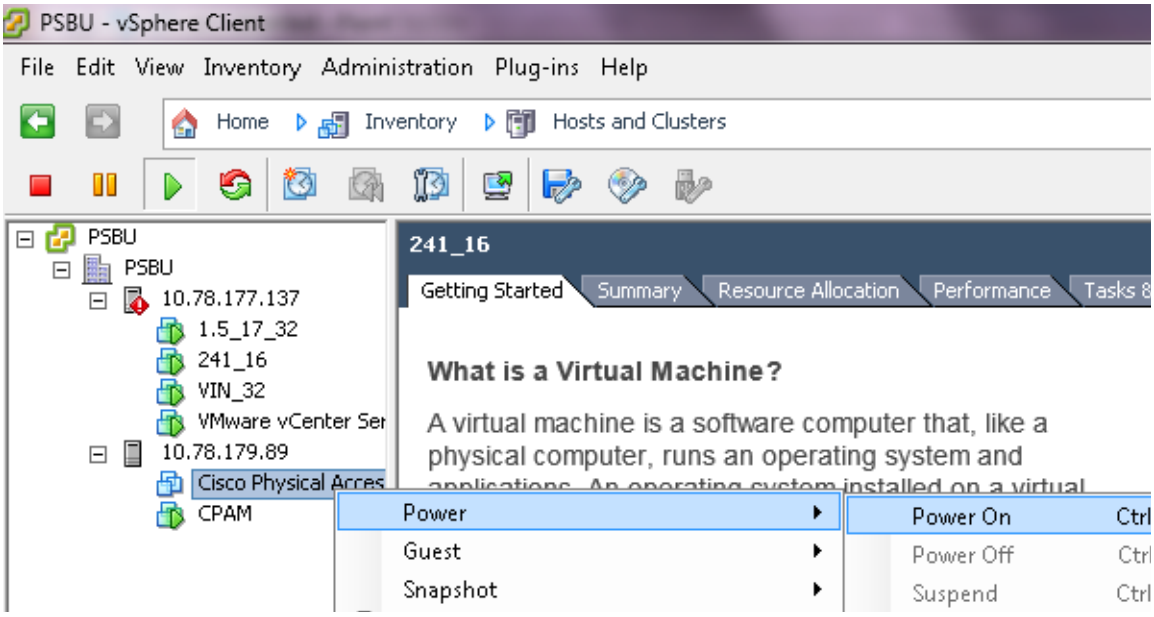


Step 5 Choose **Memory** in the **Hardware** tab, and edit the memory configuration as required.



Note In case of a HA enabled setup, follow Step 6 and Step 7 in Active server before performing the steps in the Standby server.

Step 6 Start the VM.



Step 7 Launch the web admin and start the CPAM server.

Related Documentation

For more information on Cisco-related products, see the following resources:

Cisco Physical Security product information:

http://www.cisco.com/go/physec/

Cisco UCS Manager Configuration Guide:

http://www.cisco.com/en/US/products/ps10281/products_installation_and_configuration_guides_list.html

Cisco UCS B Series Blade Servers Data Sheet and Literature:

http://www.cisco.com/en/US/products/ps10280/prod_literature.html

Cisco Physical Access Manager User guide:

http://www.cisco.com/en/US/products/ps9688/products_user_guide_list.html

Release Notes for Cisco Physical Access Manager

http://www.cisco.com/en/US/products/ps9688/prod_release_notes_list.html

Cisco Physical Access Manager API Reference Guide

http://www.cisco.com/en/US/products/ps9688/products_programming_reference_guides_list.html

Cisco Physical Access Manager Migration Guide

http://www.cisco.co“Related Documentation”m/en/US/products/ps9688/prod_installation_guides_list.html

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned 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. (1110R)

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

© 2012 - 2013 Cisco Systems, Inc. All rights reserved.