Pre-Installation Requirements

Overview

Cisco Policy Suite (CPS) is a scalable software-based solution that requires installation of multiple virtual machines prior to the configuration phase.

The following steps outline the basic process for a new installation of CPS:

Chapter 1:

1. Review physical hardware and virtual machine requirements.
2. Install and Configure VMware®.
3. Plan and collect information prior to installation.

Chapter 2:

1. Download CPS software.
2. Deploy the Cluster Manager VM.
3. Populate the CPS Deployment Template file with information for your deployment.
4. Configure the Cluster Manager VM.
5. Configure and import the CPS Deployment Template information into the Cluster Manager VM.
6. Enable any custom features.
7. Install the CPS license.
8. Replace default SSL Certificates.

Chapter 3:

1. Deploy all other CPS VMs.

2. Update Default Credentials.
3. Initialize SVN synchronization.
4. Configure Session Manager for Database Replication.
5. Validate VM deployment.

Planning the CPS Deployment

CPS Dimensioning Evaluation

With assistance from Cisco Technical Representatives, a dimensioning evaluation must be performed for each CPS deployment. This dimensioning evaluation uses customer-specific information such as call model, product features to be used, and traffic profiles to determine the specific requirements for your deployment, including:

- hardware specifications (number and type of blades, memory, etc.)
- VM information (number, type and resource allocation).

The requirements established in the dimensioning evaluation must be met or exceeded.

The following sections, Hardware Requirements, on page 2 and Virtual Machine Requirements, on page 3, provide minimum guidelines for a typical CPS deployment.

Hardware Requirements

CPS is optimized for standard Commercial Off-The-Shelf (COTS) blade servers.

The following table provides a summary of the minimum requirements for a typical single-site High Availability (HA) CPS deployment.

Table 1: Hardware Requirements

Minimum Hardware Requirements (Blade Server)	
Memory	The total size of memory for a blade server should be sufficient to meet the memory needs for all the Virtual Machines (VMs) installed in the blade. Refer to the Virtual Machine Requirements, on page 3 section for the amount of memory needed for each VMs. Also consider the memory needed by the Hypervisor. For VMware 5.x it is recommended to reserve 8 GB memory.
Storage	Two (2) 400 GB Enterprise Performance SSD Drives Supporting hardware RAID 1 with write-back cache
Interconnect	Dual Gigabit Ethernet ports

Minimum Hardware Requirements (Blade Server)	
Virtualization	Must be listed in the VMware Compatibility Guide at: https://www.vmware.com/resources/compatibility/search.php
Minimum Hardware Requirements (Chassis)	
Device Bays	A minimum of 4 is required for HA deployments
Interconnect	Redundant interconnect support
Power	Redundant AC or DC power supplies (as required by the service provider)
Cooling	Redundant cooling support

Virtual Machine Requirements

High Availability Deployment

The following table provides the minimum CPU RAM and disk space requirements for each type of CPS virtual machine (VM) in a typical deployment (4 blade single-site high availability).

Important The requirements mentioned in the table is based on:

- Hyper-threading: Enabled (Default)
- CPU Pinning: Disabled
- CPU Reservation: Yes (if allowed by hypervisor)
- Memory Reservation: Yes
- Hard Disk (in GB): 100

Table 2: HA Virtual Machine Requirements - Chassis Architecture

Physical Cores / Blade	VM Type	Memory (in GB)	Hard Disk (in GB)	vCPU	Configuration
Blade with 16 CPUs	Policy Server VMs (QNS)	16	100	12	Threading = 200 Mongo per host = 10 Criss-cross Mongo for Session Cache = 2 on each VM
Blade with 16 CPUs	Session Manager VMs	128	100	6	
Blade with 16 CPUs	Control Center (OAM) VMs	16	100	6	
Blade with 16 CPUs	Policy Director VMs (LB)	32	100	12	
Blade with 16 CPUs	Cluster Manager	12	-	2	
Blade with 24 CPUs	Policy Server VMs (QNS)	16	100	10	Threading = 100 Mongo per host = 10 Criss-cross Mongo for Session Cache = 2 on each VM
Blade with 24 CPUs	Session Manager VMs	80	100	8	
Blade with 24 CPUs	Control Center (OAM) VMs	16	100	8	
Blade with 24 CPUs	Policy Director VMs (LB)	32	100	12	
Blade with 24 CPUs	Cluster Manager	12	-	2	

Table 3: HA Virtual Machine Requirements - Cloud Architecture

Physical Cores / Blade	VM Type	Memory (in GB)	Hard Disk (in GB)	vCPU	Configuration
Blade with 16 CPUs	Policy Server VMs	16	100	12+	Threading = 200 Mongo per host = 10 Criss-cross Mongo for Session Cache = 2 on each VM
Blade with 16 CPUs	Session Manager VMs	128	100	6+	
Blade with 16 CPUs	Control Center (OAM) VMs	16	100	6+	
Blade with 16 CPUs	Policy Director VMs	32	100	8+	
Blade with 16 CPUs	Cluster Manager	12	-	2+	

Physical Cores / Blade	VM Type	Memory (in GB)	Hard Disk (in GB)	vCPU	Configuration
Blade with 24 CPUs	Policy Server VMs	16	100	10+	Threading = 100 Mongo per host = 10 Criss-cross Mongo for Session Cache = 2 on each VM
Blade with 24 CPUs	Session Manager VMs	80	100	8+	
Blade with 24 CPUs	Control Center (OAM) VMs	16	100	8+	
Blade with 24 CPUs	Policy Director VMs	32	100	12+	
Blade with 24 CPUs	Cluster Manager	12	-	2+	

Important On VMware, virtual NUMA topology is enabled by default when the number of virtual CPUs is greater than 8. You can ignore the following warning message displayed on mongo console which is generated when you configure more than 8 vCPUs on VM:

```
2016-06-03T21:40:03.130-0400 [initandlisten]
** WARNING: You are running on a NUMA machine.
2016-06-03T21:40:03.130-0400 [initandlisten]
** We suggest launching mongod like this to avoid performance problems:
2016-06-03T21:40:03.130-0400 [initandlisten] **
```

Note For large scale deployments having Policy Server (qns) VMs more than 35, Session Manager (sessionmgr) VMs more than 20, Policy Director (lb) VMs more than 2, recommended RAM for OAM (pcrfclient) VMs is 64GB.

Note If CPS is deployed in a cloud environment where over-allocation is possible, it is recommended to enable hyper-threading and double the number of vCPUs.

Note The hard disk size of all VMs are fixed at 100 GB (thin provisioned). Contact your Cisco Technical Representative if you need to reduce this setting.

The `/var/data/sessions.1` directory size of all sessionmgr VMs are 60% of actual allocated RAM size of that VM and this directory is mounted on tmpfs file system and used for session replica set. If you want to change `/var/data/sessions.1` directory size you must update (increase/decrease) the RAM size of that VM and re-deploy it.

For example, if 24 GB RAM is allocated to the Session Manager VM, 16 GB is allocated to `/var/data/sessions.1` directory on tmpfs.

If you need to update `sessions.1` directory settings consult your Cisco Technical Representative.

Considerations

- Each blade should have at least 2 CPU's reserved for the Hypervisor.
- When supported by the Hypervisor, deployments must enable CPU and memory reservation.
- For VMware environments, hardware must be ESX/ESXi compatible.
- The total number of VM CPU cores allocated should be 2 less than the total number of CPU cores per blade.
- CPU must be a high performance Intel x86 64-bit chipset.

Note BIOS settings should be set to high-performance values, rather than energy saving, hibernating, or speed stepping (contact hardware vendor for specific values).

- CPU benchmark of at least 13,000 rating per chip and 1,365 rating per thread.
- Monitor the CPU STEAL statistic. This statistic should not cross 2% for more than 1 minute^1.

Note ^1 A high CPU STEAL value indicates the application is waiting for CPU, and is usually the result of CPU over allocation or no CPU pinning. CPS performance cannot be guaranteed in an environment with high CPU STEAL.

- Scaling and higher performance can be achieved by adding more VM's, not by adding more system resources to VM's.
- For deployments which cannot scale by adding more VM's, Cisco will support the allocation of additional CPU's above the recommendation, but does not guarantee a linear performance by increasing more number of the VMs.
- Cisco will not support performance SLA's for CPS implementations with less than the recommended CPU allocation.
- Cisco will not support performance SLA's for CPS implementations with CPU over-allocation (assigning more vCPU than are available on the blade, or sharing CPU's).
- RAM latency should be lower than 15 ns.
- RAM should be error-correcting ECC memory.
- Disk storage performance needs to support less than 2ms average latency.
- Disk storage performance needs to support greater than 5000 input/output operations per second (IOPS) per CPS VM.
- Disk storage must provide redundancy and speed, such as RAID 0+1.
- Hardware must support 1 Gbps ports/links for each VM network interface.
- Hardware and hardware design must be configured for better than 99.999% availability.

- For HA deployments, Cisco requires the customer designs comply with the Cisco CPS HA design guidelines, such as:
  - At least two of each CPS VM type (PD, PS, SM, CC) for each platform.
  - Each CPS VM type (PD, PS, SM, CC) must not share common HW zone with the same CPS VM type.
- VMWare memory (RAM) Reservation must be enabled at the maximum for each CPS VM (no over-subscription of RAM).

All-in-One Deployment

The following table provides the minimum CPU RAM and disk space requirements for an All-in-One (AIO) deployment for use only in a lab for non-HA functional test purposes.

Table 4: AIO Virtual Machine Requirements

Role	Hard Disk (in GB)	Memory	vCPU
AIO (all CPS roles/functions are combined in a single VM)	100	12288 MB	8

Note AIO deployments need eth0 device. This is specifically used in `/etc/puppet/modules/qps/manifests/roles/aio.pp` file.

Deployment Examples

All-in-One (AIO) Deployment Example

All functions combined into one VM (non-HA lab/test environments only).

High Availability (HA) Deployment Example

Note The session replica-set for mongo port 27717 must always be built by using sessionmgr01 and sessionmgr02.

If you build session replica-set for mongo port 27717 with other session managers other than SM01 and SM02, the Policy Server (qns) process does not come up.

Table 5: 2 Blade Setup with 16 CPU

Blade	VM Type	Replica-sets
1	CC 6, LB 8, QNS 8, SM 6, CM 2	SM: ADMIN, Balance, Session, SPR, Reporting
2	CC 6, LB 8, QNS 8, SM 6	SM: ADMIN, Balance, Session, SPR, Reporting

Table 6: 2 Blade Setup with 24 CPU

Blade	VM Type	Replica-sets
1	CC 6, LB 12, 2 x QNS 8, SM 8, CM 4	SM: ADMIN, Balance, Session, SPR, Reporting
2	CC 6, LB 12, 2 x QNS 8, SM 8	SM: ADMIN, Balance, Session, SPR, Reporting

Table 7: 4 Blade Setup with 16 CPU

Blade	VM Type	Replica-sets
1	CM 4, CC 8, LB 8, QNS 8	-
2	CC 8, LB 8, QNS 8	-
3	2 x QNS 8, SM 8	SM: ADMIN, Session RS1,2, Balance RS1, SPR RS1, Reporting RS1
4	2 x QNS 8, SM 8	SM: ADMIN, Session RS1,2, Balance RS1, SPR RS1, Reporting RS1

Table 8: 4 Blade Setup with 24 CPU

Blade	VM Type	Replica-sets
1	CM 4, CC 8, LB 8, QNS 10, SM 8, HSF 8	SM: ADMIN, Session (Backup), Balance (Backup), SPR
2	CC 8, LB 8, QNS 10, SM 8, HSF 8	SM: ADMIN, Session (Backup), Balance (Backup), SPR
3	3 x QNS 10, 2 x SM 8	SM: Session RS1,2, Balance RS1
4	3 x QNS 10, 2 x SM 8	SM: Session RS1,2, Balance RS1

Table 9: 8 Blade Setup with 16 CPU

Blade	VM Type	Replica-sets
1	CM 4, CC 6, LB 12, HSF 6	SM: ADMIN, Session (Backup), Balance (Backup)
2	CC 6, LB 12, HSF 6	SM: ADMIN, Session (Backup), Balance (Backup)
3	2 x QNS 12, SM 6	SM: Session RS1,2, Balance RS1
4	2 x QNS 12, SM 6	SM: Session RS2,1, Balance RS2

Blade	VM Type	Replica-sets
5	2 x QNS 12, SM 6	SM: Session RS3,4, SPR RS1
6	2 x QNS 12, SM 6	SM: Session RS4,3, SPR RS2
7	2 x QNS 12, SM 6	SM: Session RS5,6, Reporting RS1
8	2 x QNS 12, SM 6	SM: Session RS6,5, Reporting RS2

Table 10: 8 Blade Setup with 24 CPU

Blade	VM Type	Replica-sets
1	CM 4, CC 8, 2 x LB 12, HSF 8	SM: ADMIN, Session (Backup), Balance (Backup)
2	CC 8, 2 x LB 12, HSF 8	SM: ADMIN, Session (Backup), Balance (Backup)
3	3 x QNS 10, 2 x SM 8	SM: Session RS1,2,7,8, Balance RS1
4	3 x QNS 10, 2 x SM 8	SM: Session RS2,1,8,7, Balance RS2
5	3 x QNS 10, 2 x SM 8	SM: Session RS3,4,9,10, SPR RS1
6	3 x QNS 10, 2 x SM 8	SM: Session RS4,3,10,9, SPR RS2
7	3 x QNS 10, 2 x SM 8	SM: Session RS5,6,11,12, Reporting RS1
8	3 x QNS 10, 2 x SM 8	SM: Session RS6,5,12,11, Reporting RS2

Install and Configure VMware

Prior to installing CPS make sure you have the ESXi hosts details like, blade IP address, user name, password, datastore name, and network name.

Install VMware vSphere Hypervisor (ESXi)

VMware ESXi™ 6.0 or 6.5 must be installed on all the blades that are used to host CPS. For more details see https://www.vmware.com/support/vsphere-hypervisor.html.

You can install upgrade or migrate ESXi from a CD/DVD drive using a script that specifies the installation or upgrade options.

You can start the installation or upgrade script by entering a boot option when you start the host. You can also create an installer ISO image that includes the installation script. With an installer ISO image you can perform a scripted unattended installation when you boot the resulting installer ISO image.

Important User must use simple passwords (not containing special characters) during ESXi Installation. The CPS script uses this EXSi password to deploy the CPS VMs. Once the installation is complete, user can change the password to a more complex one.

In vSphere 6.0 and later, the vSphere Web Client is installed as part of the vCenter Server on Windows or the vCenter Server Appliance deployment.

Prerequisites

- You must have the ESXi installer ISO in one of the following locations:
  - On CD or DVD. If you do not have the installation CD/DVD you can create one. Download and burn the ESXi Installer ISO Image to a CD or DVD.
  - On a USB flash drive.
- Verify that the server hardware clock is set to UTC. This setting is in the system BIOS.
- Consider disconnecting your network storage. This action decreases the time it takes the installer to search for available disk drives. Note that when you disconnect network storage any files on the disconnected disks are unavailable at installation.
- Do not disconnect a LUN that contains an existing ESX or ESXi installation. Do not disconnect a VMFS datastore that contains the Service Console of an existing ESX installation. These actions can affect the outcome of the installation.
- Gather the information required by the ESXi installation wizard.
- Verify that ESXi Embedded is not present on the host machine. ESXi Installable and ESXi Embedded cannot exist on the same host.

Installation

For more information related to ESXi installation, refer to http://www.vmware.com/support/vsphere-hypervisor.html.

Step 1 Download the ESXi installable ISO file.

Step 2 Mount the ISO file to a CD and feed the CD to the server where you want to install ESXi to.

Step 3 After you boot from the CD, the installer loads. Press Enter to begin and then F11 to accept the licensing agreement. Next, choose a disk to install to (All data will be erased). After ejecting the install CD, press **F11** to start the installation.

Step 4 After the installation is completed, press **Enter** to reboot, and ESXi starts.

What to do next

Open a Web browser and enter the URL for the vSphere Web Client: https://*vcenter_server_ip_address*.

If a warning message about an untrusted SSL certificate appears, select the appropriate action based on your security policy.

Note After you complete installation, IPv6 must be enabled on each blade. For more information on enabling IPv6, refer to IPv6 Support - VMware.

Enable SSH

CPS software installation requires SSH to be enabled for each blade server host.

After you complete installation and configuration of CPS, you can disable SSH for security purposes.

To enable SSH, perform the following steps:

Step 1 Log in to the vSphere Web Client.

Step 2 Select the host by IP address or name in the left panel.

Step 3 Click **Configure** tab from the top menu from the right panel.

Step 4 Under **System**, click **Security Profile** from the options available.

Step 5 Click **Edit...** in the upper right corner of the **Firewall** panel.

The **Edit Security Profile** window opens.

Step 6 Check **SSH Server** and configure the required port and protocol. Click **OK**.

Note By default, daemons will start automatically when any of their ports are opened, and stopped when all of their ports are closed.

Configure VMware ESXi Timekeeping

Both VMware ESXi and Load Balancers time must be configured correctly. Other VMs in CPS use Load Balancers as the NTP source.

To configure VMware ESXi Timekeeping, you must coordinate with customers or gain access to their NTP servers.

Log in as an administrator to every VMWare ESXi host to be used for the deployment using the VMware vSphere client.

For each host perform the following:

Step 1 Click the host (IP address or name) in the left column.

Step 2 Click **Configure** tab from the top menu from the right panel.

Step 3 Under **System**, click **Time Configuration** from the options available.

Step 4 Click **Edit...** in the upper right corner of the **Time Configuration** panel.

The **Edit Time Configuration** window opens.

Step 5 Check Use Network Time Protocol (Enable NTP Client). The following parameter can be set:

a) NTP Service Status: Options are Start, Stop and Restart. The NTP Service settings are updated when you click Start, Restart or Stop.
b) NTP Server Startup Policy: Options are Start and stop with host, Start and stop with port usage, Start and stop manually.
c) STP Servers: Add NTP Server given by or coordinated with the customer.

Step 6 After configuring the parameters according to your requirement click **OK**.
Date and Time should now show correctly in the Time Configuration window in vSphere Client. Date and Time displayed in red color indicates NTP skew that should be resolved.

Collect Virtualization Parameters for CPS Installation

Before starting the CPS deployment prepare and make sure the following items are ready:

- The traffic analysis for the capacity needed for this deployment.
- Number of VMs (the type of VMs such as Policy Director (LB), OAM (PCRFCLIENT), sessionmgr, Policy Server (QNS), node).
- The size of VMs, for each type of VMs, the size of disk memory CPU etc.
- The number of blades.
- The number of networks that the deployment will be deployed to.