Appendix

- Recommendations and Best Practices, on page 1
- Configuration Examples, on page 4
- Glossary, on page 4

Recommendations and Best Practices

Pools

Pools are the base building blocks for uniquely identifying hardware resources. As the basis for the UCS management model, they allow Service Profiles to be associated with any blade, while still providing the exact same ID and presentation to the upstream LAN or SAN. There are three sets of pools used as part of best practices:

- WWNN and WWPN pools: Provide unique IDs for Fibre Channel resources on a server (Fibre Channel nodes and ports).
- MAC address pools: Provide unique IDs for network interface ports.
- UUID pools: Provide IDs similar to a serial number or service tag.

In the Cisco UCS Manager GUI, these pools are all functionally organized, with UUID pools maintained from the Server tab, WWNN and WWPN pools maintained from the SAN tab, and MAC address pools maintained from the LAN tab.

Define and use Pools as a standard practice. Ensure the following:

- UUID pools are referenced when you create Service Profiles.
- MAC address pools are referenced when you create vNICs.
- WWNN pools are referenced when you create Service Profiles.
- WWPN pools are referenced when you create vHBAs.

Similarly, Pools should also be referenced when you create any corresponding template objects (vNICs, vHBAs, and Service Profiles). Trade-offs exist when considering pool management. There are two simple ways to manage pools: populate and use the default pools, or create domain-wide pools. This approach reduces the number of objects that need to be configured and managed. Alternatively, operators are free to configure

different pools on a per-tenant or per-application basis. This approach can provide more specific identity management and more granular traffic monitoring of tenants, applications.

Policies

Policies are a primary mechanism for enforcing rules, which helps ensure consistency and repeatability. Defining and using a comprehensive set of policies enables greater consistency, control, predictability and automation. The following sections contain various policy-related best practices.

Boot Policies

Boot Policy determines how a server boots, specifying the boot devices, the method, and the boot order.

The traditional use of SAN boot requires manual configuration for each server performing SAN boot. Typically, having 100 servers SAN-boot would require configuring 100 servers manually and individually. Cisco UCS inverts this unwieldy model, and instead requires configuring only in proportion to the number of storage arrays serving SAN-boot images, regardless of the number of servers doing SAN-boot. A single boot policy, with the WWPNs of a single storage array can be referenced and reused by any number of servers, without additional manual configuration.

Much of the Cisco UCS core value around availability is predicated on SAN boot. Therefore, the use of SAN boot within a Boot policy is a most highly recommended best practice to improve service availability.

Refer to the following best practices for boot policies:

- Have a CD-ROM as the first in the boot order, for emergencies and for booting in recovery mode.
- For SAN boot, define separate boot policies for each storage array that would be serving boot LUNs.
- For network boot, define the vNIC device as last in the boot order, following either SAN or local boot. This allows you to perform a network boot and installation, only if the OS was not previously been installed.

Host Firmware Policies

Use Host Firmware Policy to associate qualified or well-known versions of the BIOS, adapter ROM, or local disk controller with logical Service Profiles, as described earlier. A best practice is to create one policy, based on the latest packages that correspond with the Cisco UCS Manager infrastructure and server software release, and to reference that Host Firmware Package for all Service Profiles and templates created. This best practice will help ensure version consistency of a server's lowest-level firmware, regardless of physical server failures that may cause re-association of Service Profiles on other blades.

Maintenance Policies

Use the Maintenance Policy to specify how Cisco UCS Manager should proceed for configuration changes that will have a service impact or require a server reboot. Values for the Maintenance Policy can be "immediate," "userack," or "timer automatic". The best practice is to not use the "default" policy, and instead to create and use Maintenance Policies for either "user-ack" or "timer automatic", and to always have these as elements of the Service Profile or Service Profile Template definition.

Local Disk Policies

Local disk policy specifies how to configure any local disks on the blade. A best practice is to specify no local storage for SAN boot environments, thereby precluding any problems at Service Profile association time,

when local disks may present themselves to the host OS during installation. You can also remove or unseat local disks from blades completely, especially blades used for OS installation.

Scrub Policies

Scrub policy determines what happens to local disks and BIOS upon Service Profile disassociation. The default policy is no scrubbing. A best practice is to set the policy to scrub the local disk, especially for service providers, multi-tenant customers, and environments in which network installation to a local disk is used.

BIOS Policies

BIOS policy enables very specific control of CPU settings that are normally accessible only through the console during startup. For VMware and virtual environments that depend on CPU support for Intel Virtualization Technology, a corresponding policy can be created, removing any requirement for manual intervention during server provisioning. Similarly, applications that are sensitive to Intel Turbo Boost or Hyper-Threading can have dedicated BIOS policies referenced. Also, setting "Quiet Boot" to "disabled" allows diagnostic message visibility, which may be helpful in troubleshooting situations.

Templates

Refer to the following best practices for templates:

- In the Cisco UCS Manager GUI, use expert mode when creating Service Profile templates to achieve the optimal level of control and definition.
- When creating templates, reference the subordinate Pools and Policies that have been previously defined.

vNIC and vHBA Templates

Create reusable vNIC and vHBA templates in which termination is either reflected in the name (e.g., "fc0-A") or through well-accepted conventions (e.g., an even interface to A side, and an odd interface to B side). vNIC templates should be thought of as application-specific network profiles that include important security definitions, such as VLAN mappings.

Service Profile Templates

Use a Service Profile template as a definition for a class or type or version of an application, service, or operating system.

Monitoring

Cisco UCS provides the standard set of health and monitoring methods, such as syslog and Simple Network Management Protocol (SNMP) with its associated MIBs8 (get and fault traps only; no set). The best practice for Cisco UCS monitoring is to use existing methods and frameworks that are already familiar and well understood, such as SCOM, OpenView, or BPPM.

Network Availability

For network availability, either use hardware failover or use NIC teaming (or bonding), but do not use both concurrently. After a vNIC and vHBA template is defined, it can be referenced through expert-mode service-profile creation by selecting Use LAN (or SAN) Connectivity Template.

Best Practices for Installing ESXi 5.5 U2 Custom ISO to FlexFlash

Before installing the ESXi 5.5 U2 custom ISO to FlexFLash, scrub the FlexFlash drives to avoid any ISO installation issues.

Configuration Backup

The Cisco UCS configuration can be backed up easily and should be backed up regularly through the GUI or automated scripts. There are four types of backups:

Type	Description
Full State	Used for full system restore as part of disaster recovery.
System Configuration	Roles, Call Home, communication services and distributed virtual switch.
Logical Configuration	Service profiles, VLANs, VSANs, pools, policies and templates
All Configurations	Both Logical and System configurations

For the Logical Configuration and All Configurations backups, select the Cisco UCS Manager Preserve Identities feature to preserve the actual MAC address, WWN, and UUID values; otherwise, the backup references only the logical pool names, but not the actual identities. The following are configuration backup related best practices:

- Use the Preserve Identities feature when backing up individual domains for prescribed restoration (same site or domain or exact recovery site or domain).
- Do not use Preserve Identities when creating "gold UCSM domain configuration" templates.

Configuration Examples

Refer to Configuration Examples and TechNotes for Cisco UCS Manager configuration examples.

Glossary

AD

Active Directory. A distributed directory service.

adapter port channel

A channel that groups all the physical links from a Cisco UCS Virtual Interface Card (VIC) to an IOM into one logical link.

BIOS

Basic Input Output System. In a computer system, it performs the power up self-test procedure, searches, and loads to the Master Boot Record in the system booting process.

DNS

Domain Name System. An application layer protocol used throughout the Internet for translating hostnames into their associated IP addresses.

Dyname FCoE

The ability to overlay FCoE traffic across Spine-Leaf data center switching architecture. In its first instantiation, Dynamic FCoE allows running FCoE on top of Cisco FabricPath network in a converged fashion.

Ethernet Port

A generic term for the opening on the side of any Ethernet node, typically in an Ethernet NIC or LAN switch, into which an Ethernet cable can be connected.

Fabric port channel

Fibre Channel uplinks defined in a Cisco UCS Fabric Interconnect, bundled together and configured as a port channel, allowing increased bandwidth and redundancy.

FCoE

Fibre Channel over Ethernet. A computer network technology that encapsulates Fibre Channel frames over Ethernet networks. This allows Fibre Channel to use 10 Gigabit Ethernet networks (or higher speeds) while preserving the Fibre Channel protocol characteristics. The specification is part of the International Committee for Information Technology Standards T11 FC-BB-5 standard published in 2009. FCoE maps Fibre Channel directly over Ethernet while being independent of the Ethernet forwarding scheme.

Hypervisor

A software allowing multiple operating systems, known as guest operating systems, to share a single physical server. Guest operating systems run inside virtual machines and have fair scheduled access to underlying server physical resources.

IP address (IP version 4)

IP version 4 (IPv4), a 32-bit address assigned to hosts using TCP/IP. Each address consists of a network number, an optional subnetwork number, and a host number. The network and subnetwork numbers together are used for routing, and the host number is used to address an individual host within the network or subnetwork.

IP address (IP version 6)

In IP version 6 (IPv6), a 128-bit address assigned to hosts using TCP/IP. Addresses use different formats, commonly using a routing prefix, subnet, and interface ID, corresponding to the IPv4 network, subnet, and host parts of an address.

KVM

Keyboard, video, and mouse

LAN

Logical Area Network. A computer network that interconnects computers within a limited area, such as a home, school, computer laboratory, or office building, using network media. The defining characteristics

of LANs, in contrast to Wide-Area Networks (WANs), include their smaller geographic area and non-inclusion of leased telecommunication lines.

Logical unit number

Logical unit number. In computer storage, a number used to identify a logical unit, which is a device addressed by the SCSI protocol or protocols that encapsulate SCSI, such as Fibre Channel or iSCSI. A LUN may be used with any device that supports read/write operations, such as a tape drive, but is most often used to refer to a logical disk as created on a SAN.

MAC address

A standardized data link layer address that is required for every device that connects to a LAN. Ethernet MAC addresses are 6 bytes long and are controlled by the IEEE.

out-of-band

A storage virtualization method that provides separate paths for data and control, presenting an image of virtual storage to the host by one link and allowing the host to directly retrieve data blocks from physical storage on another.