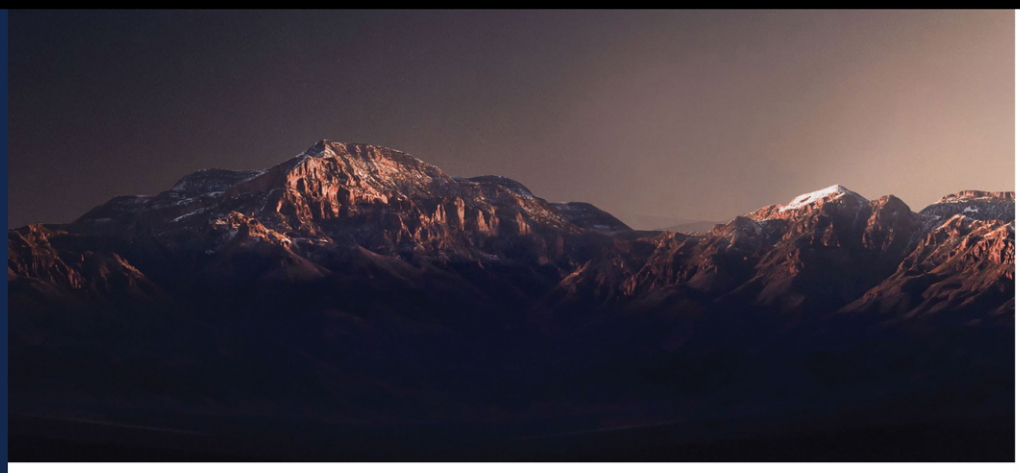

Cisco Intersight

A Handbook for Intelligent Cloud Operations

Matthew Baker | Brandon Beck
Doron Chosnek | Jason McGee | Sean McKeown
Bradley TerEick | Mohit Vaswani

ciscopress.com

Cisco Intersight: A Handbook for Intelligent Cloud Operations

Matthew Baker
Brandon Beck
Doron Chosnek
Jason McGee
Sean McKeown
Bradley TerEick
Mohit Vaswani

Cisco Press

Much as with policies, there are unique profile types for servers, chassis, UCS domains, and HyperFlex clusters. This chapter covers server profiles for both rack and blade servers. The other profile types are covered in other chapters.

Server Profile States

Because profiles do not have to be assigned to servers and because servers are not always guaranteed to match the configuration state of an assigned profile, profiles can be in one of several different states at a given point in time. Those states are detailed in Table 4-1.

Table 4-1 *Server Profile States*

Profile State	Description
Not Deployed	The profile has been assigned to a server but not deployed.
Not Assigned	The profile has not been assigned to a server.
OK	The profile has been successfully deployed to the server, and the server configuration matches the policies defined in the profile.
In Progress	The profile is in the process of being deployed to the server.
Not Deployed Changes	The current profile and its referenced policies are different from the last deployed policy configuration.
Failed	Server profile validation, configuration, or deployment has failed.
Out of Sync	The policy configuration at the server is not in sync with the last deployed policy configuration in the profile. If the server settings are altered manually after a profile is deployed, Intersight automatically detects configuration changes, and they are shown on the server profile as Out of Sync.

The most interesting of these server profile states have to do with the situation when a server profile is assigned to a server, and the server's configuration differs from the profile; this situation is known as *configuration drift*. Configuration drift is occurring when a policy state is marked as either of the following:

- **Out of Sync:** The configuration of the server has changed at the server, and it no longer matches the configuration that was assigned to the server by the Intersight server profile. The administrator can select the server profile in Intersight and select Deploy to overwrite configuration changes made locally at the server.
- **Not Deployed Changes:** The configuration of the server profile has changed in Intersight, and it no longer matches the configuration that is currently deployed to the server. This can occur when a profile or any of the policies mapped to that profile are changed by the administrator. The administrator can select the server profile in Intersight and select Deploy to push these configuration changes to the server.

Standalone Servers

Server profiles for UCS rack servers can either be created natively in Intersight or imported from the IMCs of existing UCS rack servers that have been configured locally.

When a profile is imported from an existing server into Intersight, a server profile and associated policies are created. This is a simple method for creating a golden configuration. Once the golden configuration has been imported, it can be cloned and applied to other UCS rack servers. In addition, those imported policies can be used for other profiles in the organization.

Most organizations create profiles natively in Intersight. As discussed earlier in this chapter, server profiles consist of policies. To create a new profile, administrators must create the necessary policies in advance or be prepared to create them inline while creating a new server profile.

Any server profile can be cloned, regardless of how it was initially created. Administrators can create server profiles and leave them unassigned. This allows administrators to perform all the configurations for new servers before physically installing them. The profiles can be deployed to the servers later.

Fabric Interconnect (FI)–Attached Servers

FI-attached servers deployed within an Intersight-managed compute domain are referred to as *Intersight managed* (discussed at length in the next section) and are not deployable as standalone systems; therefore, the profile and policy import capabilities described previously are not applicable.

The creation of an FI-attached server profile has all the same prerequisites as the creation of a standalone server profile. Similarly, these profiles also can be cloned and templated, and they can reference reusable policy for configuration.

Server Profile Templates

Server profile templates are used to ensure the consistent configuration of groups of servers by modeling the configuration of a server as a reusable object in Intersight. Server profile templates may be created from scratch or created from an existing server profile. These templates can then be used to create multiple server profiles containing the same configuration as the template. If a configuration change is made to the server profile template, all attached server profiles will be synced to the new configuration settings in the template. In this scenario, any server profile assigned to a server and derived from the modified server profile template will change to the Not Deployed Changes state.

A server profile may be attached to a server profile template as long as the server profile is not attached to any other server profile template. When a server profile is attached to a server profile template, the server profile template configuration overrides the existing server profile configuration. Once a server profile is attached to a template, the server

profile cannot be directly modified; instead, the server profile template must be modified. To modify an attached server profile, the server profile must be detached from the server profile template.

Server profile templates may also be cloned to create additional server profile templates.

Domain Management

The UCS architecture for blade servers (and FI-attached rack-mount servers) uses a pair of Fabric Interconnect switches as the network infrastructure for the servers. The combination of a pair of these Fabric Interconnect switches and the servers attached to them is referred to as a *UCS domain*. Each of these domains contains its own configuration and policy manager, known as UCS Manager, and is limited to 20 chassis, or approximately 160 servers. With Intersight, an updated architecture both consolidates the configuration and policy management and allows for an unlimited number of domains. This section discusses the management and operation of both types of UCS architectures with Intersight.

Traditional UCS Domains

Intersight can be used to perform day-to-day operations on traditional UCS Manager (UCSM) domain infrastructure, such as powering on, powering off, accessing the vKVM, and updating firmware. This provides a consistent operational model for standalone rack servers, traditional UCS domains, and the newer architecture that is discussed below.

Intersight coordinates server operations with UCSM by using the embedded Device Connector (discussed in Chapters 1 and 2). Beginning with the 3.2 software release, Device Connector was integrated into UCS Manager. As with other Cisco targets, administrators simply claim a traditional UCS domain in Intersight by using the device ID and claim code obtained from UCSM Device Connector.

Upon successfully claiming a traditional UCS domain, Intersight conducts an inventory collection of the entire domain infrastructure. All components (servers, chassis, FIs, and so on) within the claimed domain are added to Intersight's inventory of managed devices. Intersight can perform operational tasks within the domain by working in harmony with UCSM.

Examples of Intersight's operational capabilities within a traditional domain include:

- Device inventory
- Graphical server views
- Health and monitoring
- Search and tagging
- vKVM or tunneled vKVM

- Firmware upgrades
- Advisories
- Hardware compatibility list (HCL) compliance
- TAC case creation
- Proactive RMA
- License operations
- UCS Manager launch

When the need arises to change or update traditional UCS servers' configurations, Intersight provides a seamless and intuitive approach to access necessary configuration tools. Intersight is unable to directly configure or change policies on traditional UCSM domain infrastructure because UCSM acts as its own configuration manager. Intersight provides an option to directly interface with UCSM for blade and FI-attached servers or the IMC for standalone UCS servers.

Pass-through authentication is used with authorization via the operator's current Intersight credentials and role-based access controls when these control planes are accessed from Intersight. While the Launch UCS Manager or Launch IMC action may load a web page closely resembling the actual UCSM or IMC interface, the resulting web pages are not actually presented by these interfaces. Instead, the resulting web pages are Intersight-constructed pages that use API calls to interact with the actual UCSM or IMC interfaces. To ensure that a security loophole is not introduced, the ability to configure Device Connector is disabled. Anyone enabling Intersight connectivity or changing Device Connector settings must have direct local access to the interface of the device being managed. (This concept of using Launch UCS Manager or Launch IMC is often referred to as using the "UCS Manager provider" or "IMC provider" to clarify the nomenclature and more accurately describe the connectivity to these interfaces.)

Intersight Managed Mode

Intersight Managed Mode (IMM) is an FI runtime mode that enables Cisco's computing platform architecture, often referred to as Cisco's "modernized compute architecture." This modernized architecture has many similarities to traditional UCS domains, including FIs, server chassis, and servers. The two architectures are physically cabled the same way; a pair of FIs form the top-of-rack (ToR) switching fabric for the chassis and servers, ultimately coming together to form a UCS domain. While the terminology and physical attributes of the two architectures are identical, this is where the similarities end. The underlying software architectures and the governing control planes are fundamentally different.

A UCS domain can either be configured by an embedded UCSM instance for traditional UCS domains or by Intersight for modernized UCS domains. Traditional domains, running UCSM, are 100% dependent on UCSM to derive their configuration. Conversely, modern domains, configured by Intersight, have no embedded UCSM running in the Fabric Interconnects and are dependent on Intersight to derive their configuration. These modern domains are said to be running in Intersight mode. The domain mode is determined during the initial setup of a pair of Fabric Interconnects and cannot be changed or converted without reconfiguration of the domain.

Since Intersight mode is not dependent on an FI-embedded configuration control plane, it enables broader configuration scope. Intersight can configure the domain-based server infrastructure, and it can also use policy- and profile-based configuration methods to configure the domain switching fabric or Fabric Interconnects. All UCS infrastructure is defined by a policy managed by Intersight directly.

The following sections provide more details on this modern operational mode as well as how organizations can benefit from Intersight's operational capabilities for both traditional UCSM and Intersight managed domains.

Benefits of Domains Running Intersight Mode

While Intersight can perform day-to-day operations for traditional UCS domains, the policy (or configuration) management is still handled at the individual domain level. In contrast, the policy for devices connected to a domain running in Intersight mode is managed and maintained by Intersight. This allows limitless scale for pools, policies, and profiles across an organization's infrastructure, all within a single operational view.

For organizations with multiple Intersight managed compute domains, policies and pools become easier to consume and can be shared globally. The risk of identifiers, such as MAC addresses or Fibre Channel WWNs, overlapping across domains is removed, and existing policies can be reused in new domains located anywhere in the world.

An NTP policy, for example, can be shared among thousands of standalone rack servers, and that same policy can also be used by UCS domains in Intersight mode. Figure 4-7 shows an NTP policy used by both UCS server and UCS domain profile types.

Intersight's ability to manage both standalone and domain-attached servers with a single policy model provides true administrative flexibility and configuration consistency, and it simplifies the operational burden whether the computer infrastructure is a handful of servers or a large, diverse, distributed server infrastructure.

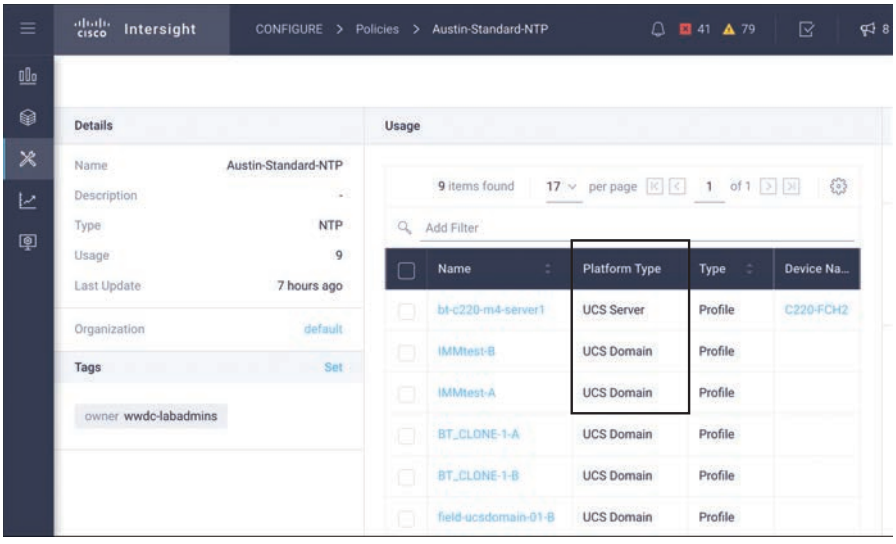

Figure 4-7 *Using policies across different device types in Intersight mode*

Getting Started with Intersight Mode

There are minimum hardware and software requirements for running an FI with Intersight mode. The latest details for supported systems are available at https://intersight.com/help/supported_systems#supported_hardware_systems_and_software_versions.

The first step to getting started with IMM-compatible systems is to place the Fabric Interconnects in Intersight Managed Mode. A new FI presents the administrator with three questions (when connected to the FI serial port). An FI that was previously configured to run with UCS Manager must have its configuration erased before proceeding. Beginning with the primary FI, the questions and appropriate answers to enable Intersight Managed Mode are shown in Figure 4-8.

```
Type 'X' to cancel GUI configuration and go back to console or
press any other key to see the installation progress from GUI
(reboot/X) ? X

Enter the configuration method. (console/gui) ? console

Enter the management mode. (ucsm/intersight) ? intersight
```

Figure 4-8 *Initial configuration of the primary Fabric Interconnect*

The FI then guides the administrator through a basic networking setup for the primary FI. Configuring the subordinate FI is even easier, as it can retrieve most of its settings from the primary FI. When connected to the subordinate FI serial port, the administrator answers the questions shown in Figure 4-9 and provides an IP address for the subordinate FI.