White Paper Public IIIIII CISCO The bridge to possible

Transition a Cisco UCS Configuration in FlexPod from Cisco UCS Manager to the Cisco Intersight Platform

Contents

FlexPod system overview	3
Cisco Intersight, IMM, and the IMM Transition Tool	4
Cisco IMM Transition Tool setup and configuration	5
Creating a Cisco IMM transition for a FlexPod Cisco UCS domain	7
Results of the IMM Transition Tool	11
Considerations and caveats for using the IMM Transition Tool	16
Conclusions	16
For more information	17

FlexPod system overview

FlexPod is a best-practices data center architecture that can include the following components (Figure 1):

- Cisco Unified Computing System[™] (Cisco UCS[®])
- Cisco Nexus[®] Family switches
- Cisco MDS Family switches
- NetApp FAS systems (including NetApp All Flash FAS [AFF])
- NetApp All SAN Array (ASA) systems



Figure 1.

FlexPod component families

These components, including NetApp AFF and NetApp ASA, are connected and configured according to the best practices of both Cisco and NetApp to provide an excellent platform for running a variety of enterprise workloads with confidence. FlexPod can scale up for greater performance and capacity (adding computing, network, and storage resources individually as needed), or it can scale out for environments that require multiple consistent deployments (such as rollout of additional FlexPod stacks).

Cisco Intersight, IMM, and the IMM Transition Tool

The Cisco Intersight[™] cloud operations platform consists of optional, modular advanced infrastructure, workload optimization, and Kubernetes services capabilities. This software-as-a-service (SaaS) management platform is augmented by other intelligent systems.

In addition to SaaS management, the Cisco Intersight platform offers on-premises capabilities. The Cisco Intersight Connected Virtual Appliance (CVA) provides a tethered connection back to Cisco for firewall upgrades, security advisories, and a connected Cisco[®] Technical Assistance Center (TAC) experience. Also available is the Cisco Intersight Private Virtual Appliance (PVA), which provides a completely air-gapped instance of Cisco Intersight, with no connection to the internet, for a highly secure environment.

Cisco Intersight Infrastructure Service includes the deployment, monitoring, management, and support of your physical and virtual infrastructure. You can connect to the Cisco Intersight platform from anywhere and manage infrastructure through a browser or mobile app. The Cisco Intersight secure device connector provides lifecycle management for Cisco UCS servers, Cisco HyperFlex[™] hyperconverged infrastructure (HCI), and third-party devices.

Cisco Intersight Managed Mode, referred to informally as IMM, is not a product, but instead is a capability that brings the features and functions of Cisco UCS Manager and the Cisco UCS Central Software policy model for service profiles to the Cisco Intersight platform. In effect, the policy model is built out, used, and consumed entirely from within Cisco Intersight. Cisco UCS Manager and Cisco UCS Central are replaced by Cisco Intersight, and Cisco UCS Manager and Cisco UCS Central service profiles become Cisco Intersight server profiles. To accommodate and communicate with the Cisco Intersight platform, the fabric interconnects must be set up initially, or rebuilt (erased and then rebuilt), in "Intersight" mode. Because of this, most customers likely will want to deploy their systems in Cisco Intersight from the start, rather than transition a fully operational production domain to Cisco Intersight.

With the creation of the Cisco Intersight platform, and particularly IMM, customers struggled with how best to create an environment in Cisco Intersight similar to an existing Cisco UCS managed domain or Cisco UCS Central managed domain. In the beginning, this was a difficult task, highly manual and time consuming, requiring the rebuilding of all the logical components of a Cisco UCS domain or Cisco UCS Central configuration. In particular, it required you to manually build organizations, pools, policies, VLANs, VSANs, templates, and server profiles in Cisco Intersight.

Introducing the IMM Transition Tool

Although the build-from-scratch approach certainly works, Cisco now offers a much better way to get most of the logical configuration of a Cisco UCS Manager or Cisco UCS Central environment into Cisco Intersight. The IMM Transition Tool allows you to transition, or import, an existing Cisco UCS environment to the Cisco Intersight platform in minutes and then simply edit or change approximately 10 percent of the configuration in Cisco Intersight, rather than spending hours or days building 100 percent of the configuration completely in Cisco Intersight.

The IMM Transition Tool accomplishes two primary goals, as shown in Figure 2. First, it interfaces with your existing Cisco UCS domain or Cisco UCS Central environment through the API in read-only mode to capture the hardware inventory (Cisco UCS Manager only) and policy configurations (Cisco UCS Manager and Cisco UCS Central). With this information, it generates a detailed and comprehensive IMM Readiness Report that can be viewed online or downloaded for review. This report gives you a complete assessment of all your hardware, firewall, and policy configurations to advise you as to the likely success of transitioning that environment to the Cisco Intersight platform. This report provides a wealth of information

that is readily available to you-a huge benefit of the tool in and of itself. In addition, you can run this report repeatedly to account for any changes to the domain resulting from the preceding run of the report.

Second, the IMM Transition Tool can help you convert the existing knowledge built in to your existing Cisco UCS or Cisco UCS Central environment from its XML format to a Cisco Intersight JavaScript Object Notation (JSON) format and then successfully push that JSON configuration to your Cisco Intersight account. The target for the push can be either Cisco Intersight SaaS or on-premises appliances: Cisco Intersight CVA or PVA.





The main use case for the IMM Transition Tool is to assist in new (greenfield) deployments of Cisco UCS domains in the Cisco Intersight platform. For instance, a greenfield installation of the new Cisco UCS X-Series requires IMM for computing resource management. The focus of this document is the deployment of Cisco UCS in a FlexPod environment, but almost any Cisco UCS solution can be supported with the principles discussed here. The IMM Transition Tool can even be used with older Cisco UCS environments (for example, with second-generation Cisco UCS fabric interconnects and Cisco UCS M3 and M4 servers) that are not compatible with IMM from a hardware standpoint. Nevertheless, you still can harness the configurations of those Cisco UCS domains and transition them to Cisco Intersight for a new greenfield buildout.

Cisco IMM Transition Tool setup and configuration

This document does not provide a step-by-step tutorial describing how to use the IMM Transition Tool. Although major steps and advice are provided here, watching the live YouTube demonstrations listed in the For more information section at the end of this document will provide more guidance. The videos demonstrate both a Cisco UCS Manager transition and a Cisco UCS Central transition.

The IMM Transition Tool is a simple Open Virtual Appliance (OVA) file download from the Cisco UCS Tools website. After downloading the file, deploy it in VMware vCenter. Use the following link to get the latest version, Release 2.0.1, of the IMM Transition Tool: <u>https://ucstools.cloudapps.cisco.com/</u>. Release notes and user guide, including a list of supported software versions, are also available at the website.

After installing and starting the tool, navigate to the IP or fully qualified domain name (FQDN) of the tool. You'll see the Login splash screen (Figure 3). Use the admin account and password you established during the installation process.





Now add your devices to the IMM Transition Tool (Figure 4). With the latest release of the tool, Release 2.0.1, the recommended approach is to prepopulate the device credentials for your Cisco UCS Manager domain, Cisco UCS Central Software, and Cisco Intersight account on the Device tab. This step will save you from having to add the information in the flow of the report generation and transition processes, and it allows you to use simple pull-down menus to select the appropriate target (Cisco UCS Manager or Cisco UCS Central) and destination (Cisco Intersight platform). For SaaS Cisco Intersight connectivity, simply add <u>www.intersight.com</u>. For on-premises Cisco Intersight connectivity, you must add the FQDN of the deployed appliance.



Figure 4. Add your devices to the tool

When you add the Cisco Intersight account, you'll need to provide the Cisco Intersight target, API key, and secret key. To generate the keys, log in to your Cisco Intersight account as Admin and go to Settings > API

Keys (Figure 5). From there you can generate the API key and secret key or your account. Be sure to choose the Version 3 (v3) API key.



Figure 5. Generate keys

Creating a Cisco IMM transition for a FlexPod Cisco UCS domain

Figure 6 shows an example of a FlexPod environment in Cisco UCS Manager.

Al v	Servers / Service Profile Templates		
m v Servers A	Service Profile Templates		
	+ - Ty Advanced Filter A Export I Print		0
v root	Name	Address	
Sub-Organizations	▼ root		^
E Service Profile Templates	▼ FlexPod-VMware		
✓ root	Service Template NX-IOM-Host-FCP		
Sub-Organizations ElevPort=VMware	- vHBAs		
Service Template NX-IOM-H	HBA EC-NUME-Envir-A	Derived	
Service Template NX-IOM-H	HIDA TO ATIME Fabric A	Defined	
Service Template NX-IOM-H		Denved	
Service Template NX-IOM-H	▶ vHBA FCP-Fabric-A	Derived	
 Service Template NX-IOM-H 	vHBA FCP-Fabric-B	Derived	
Service Template NX-IOM-H	▼ vNICs		
 Service Template NX-IOM-H 	▶ vNIC 00-vSwitch0-A	Derived	
Service Template NX-IOM-H	▶ vNIC 01-vSwitch0-B	Derived	
Service Template VM-Host-II Service Template VM-Host-II	▶ vNIC 02-vDS0-A	Derived	
Service Template VM-Host-II	vNIC 03-vDS0-B	Derived	
 Service Template VM-Host-Ir 	Consistent Translater MV (ON) Mark FOD ANA		
 Service Template VM-Host-Ir 	Service remplace NA-IOM-Host-PCP-MM		
 Service Template VM-Host-Ir 	Service Template NX-IOM-Host-FCP-MM-vM		
 Service Template VM-Host-Ir 	Service Template NX-IOM-Host-FCP-vM		
 Service Template VM-Host-li 	Service Template NX-IOM-Host-iSCSI		
Service Template VM-Host-Ii	Service Template NX-IOM-Host-iSCSI-MM		
Sub-Organizations	Service Template NX-IOM-Host-iSCSI-MM-vM		
 Policies root 	Service Template NX-IOM-Host-iSCSI-vM		u la
Adapter Policies		Add Defete Info	
 BIOS Defaults 			
 BIOS Policies 			
 Boot Policies 			
 Diagnostics Policies 			
< >>			

Figure 6.

FlexPod environment in Cisco UCS Manager

To transition a FlexPod configuration from a Cisco UCS domain to Cisco Intersight, in the IMM Transition Tool create a new transition (Figure 7).



Figure 7. Create a new transition

Choose either Cisco UCS Manager or Cisco UCS Central. The example here uses Cisco UCS Manager. If you prepopulated your infrastructure on the Device tab at the beginning of the process, as recommended, then simply access the infrastructure in the pull-down menus. The data collection process can take 15 minutes or longer for a Cisco UCS domain, and much longer for a large Cisco UCS Central environment. If you've previously performed a collection with the IMM Transition Tool on a given Cisco UCS Domain, you'll see the Refresh button enabled for the next iteration, as shown in Figure 8. If you simply click Next, the same cached data used in the previous, original data collection will be used to build the IMM Readiness Report and perform data conversion. In that case, report generation will be completed quickly. If instead you want to collect new, fresh data from the Cisco UCS domain (perhaps because domain changes have been made), click Refresh to cause another data collection process to take place.



Figure 8.

Choose cached or fresh data for the data collection process

The latest release –Release 2.0.1–of the tool provides some excellent and flexible settings to make your transition experience even better (Figure 9). Familiarize yourself with the settings, and don't forget to use the tooltips to learn more about what each setting does.

Note: By default, conversion of service profiles is disabled. Cisco highly recommends that you leave this setting disabled until we develop the capability to preserve and retain service profile IDs during transitioning. This capability is coming in the next IMM Transition Tool release.



Figure 9. Transition settings

Another great feature in IMM Transition Tool Release 2.0.1 is the capability to filter the templates (and consequently the underlying consumed policies that support those templates) to allow some flexibility and support an incremental progressive process in transitioning configurations to the Cisco Intersight platform. For the example here, all templates in the FlexPod-VMware organization are selected in Figure 10 and will be converted (along with their underlying and supporting policies). For more information about this incremental progressive process, see the section <u>Considerations and caveats for using the IMM Transition Tool</u> later in this document.



Figure 10.

Select the templates for conversion

After the IMM Readiness Report has been generated, you can either view it online or download it (Figure 11).



Figure 11. View or download the IMM Readiness Report

Results of the IMM Transition Tool

The IMM Transition Tool accomplishes two goals: it generates the IMM Readiness Report, and it transitions your Cisco UCS configuration to the Cisco Intersight platform.

IMM Transition Tool: IMM Readiness Report

As described previously, an especially useful benefit of the IMM Transition Tool is the capability to collect inventory and configuration information from a Cisco UCS Manager domain and automatically generate an IMM Readiness Report. The report provides extremely detailed information about hardware inventory, firewall versions, and policy configurations. Figure 12 provides just a sample. The entire report contains 117 pages (the report can be viewed online or downloaded in PDF format). This report is useful in everyday operations of any Cisco UCS domain and can be run against any generation of hardware (even hardware not supported for transitioning to IMM, such as second-generation fabric interconnects). Basically, all Cisco UCS domains are supported.

Note that faults within the IMM Readiness Report are raised in the context of "Is this hardware, or is this policy (or setting), compatible with Cisco IMM?" You may have no intention of migrating existing hardware to IMM; however, the policy configuration itself is valuable, it includes intellectual capital, and it can always be transitioned regardless of the age of the underlying hardware.

Figure 12 provides an example the IMM Readiness Report showing the hardware inventory for the FlexPod and Cisco UCS domain.

MM Transition v2.0.1						0				
ack FXTrans-2	Readiness Report									
	Intersight Manad	ed Mode Hardware Compatibility				î				
Overall Summary	This section details the Ha	muare Compatibility status of your current UCS Mana	ner domain hantwore for intervient blananed Mode (MMI) surgert							
Hardware Compatibility	,									
Canfig Canversian 🛛 🛓 🧰	Fabric Hardware C	ompatibility								
Transition Settings	Fabric Internet									
Fabric Config Conversion	> Pashe Interconnects	Rectal March 10	Farmer	Armystella (194	demonstration (2018)					
Poels Conversion	>	Security Handler	- Purchase	Companion HW7	Compatible PW7					
UCS Server Profiles Conversion	3 8 6454	FD024490JQK	4.2/1m)A	Yes	Yes					
	~									
Organizations	Chassis Hardware	Compatibility								
1100 Polices	>									
Broot Policies	Chassis Overview									
Erhamat Advoter Bellerian	10 SKU		Name	Serial Number	Compatible HW7					
Control House Concession	1 UCS	3-5106-AC2	5108 AC2	F0X204303ZL	Yes					
Ethernet fortwork Control Policies										
Ethemet Network Group Policies	2 Chasses 1									
Ethemet GoS Policies	2 IO Modules									
Fibre Channel Adapter Policies	> ID Name	Serial Number	Fermine	Compatible HW?	Compatible FW?					
Fibre Channel Network Policies	> 1 2408	FCH234278KC	4.2(1m)A	Yes	Yes					
Fibre Channel QoS Policies	5 2 2408	FCH2342780L	4.2(1m)A	Yes	Yes					
IME Access Polices										
IPMI over LAN Policies	Blade Servers									
IICE Adams Palmes	Blade Server 1/1 details									
2001 Bank Balance	Blade ID	Adaptor ID Name	Serial Number	Firmware	Compatible HW?	Compatible FW7				
NOLON DAVE FORDES	1/1	8200 M	6 FCH245270TW	4.2(1m)8	Yes	Yes				
iSCSI Static Target Policies	>	1 VIC 144	0 FCH25037105	4.2(1m)8	Yes	Yes				
LBN Consectuity Policies 🗼 🔘		2 Port Ex	pander FLM25040110		Yes	N/A				
SAN Connectivity Palicies										
SD Card Policies	Blade Server 1/2 details									

Figure 12.

IMM Readiness Report showing hardware inventory for the FlexPod and Cisco UCS domain

Figure 13 provides another example from the IMM Readiness Report. This example shows a particular BIOS token (quiet boot token) that does not transition between Cisco UCS Manager and IMM. It appears in yellow.

= :	India IMM Transition v2.0.1		0	۰ ک
6	(Back FXTrans-2	Readiness Report		
Ø	PETrans2 ~	A BIOS Policy Intel-M6-Virt		
	Hurdware Compatibility 3	Could not find mapping to consent UCB BIOD Takes of BIOD Ruley to Henright		
	Condig Conversion 🛓 🔵 🗸 🗸	'gent.boor'		
	Fabric Config Conversion	Description Value		
	Pools Conversion >	Name IntelAd5-Vit		
	UCS Server Profiles Conversion	Organization FilesPublishame		
		cdr_mable enabled		
	Gravitzations	spLpef_enhancement Auto		
	Internet A D	nimdime, perform, config Balanced Profile		
	Boat Policies >			
	Ethernet Adapter Policies. 3			
	Ethernet Network Control Policies >			
	Ethernet Network Group Policies >			
	Ethernet QoS Policies >			
	Fibre Channel Adapter Policies			
	Fibre Channel Network Policies >			
	Fibre Channel QoS Policies >			
	ILIC Access Polisies 🛓 🔕			
	IPMI over LAN Policies >			
	ICS) Adapter Policies 🛓 🔕 5			
	ISCSI Boot Policies >			
	ISCSI Static Target Policies			
8	LAN Convestivity Pulsers			

Figure 13.

Token that does not transition to IMM

IMM Transition Tool: Transitioned configurations

The IMM Transition Tool transitions all policies and settings to the best of its capabilities. These capabilities are impressive, but there's no guarantee that you won't have to make some final edits after configurations are transitioned to Cisco Intersight. However, as stated previously in this document, it is better to spend a small amount of time editing perhaps 5 to 10 percent of the entire configuration in the Cisco Intersight platform after the transition than having to build out the entire the configuration, which could take hours or days.

As an example, examine a customer Ethernet adapter policy (customized for FlexPod) in Cisco UCS Manager.

Note some of the customized settings implemented based on the Cisco Validated Design guide (Figure 14).

	S Manager								
D	All v	Servers /	olicies /	root / Ad	dapter Policies / Eth Adap	ter Policy VMware-HighTrf			
	FlexPod-VMware	General] Event	65					
rvice	Profile Templates	1							
toot		Actions					Properties		
Su	b-Organizations	Dalaas					Name	· VManna High	54
licies		Cheve					The second second		
root		SHOW PO	cy chaigh				Descriptio	·	
• Ad	Japter Policies						Owner	Local	
	Eth Adapter Policy default								
	Eth Adapter Policy Linux								
- 8	Eth Adapter Policy Linux-NVMe-RoCE	⊖ Rest	urces						
	Eth Adapter Policy MQ	Pooled		Dist	bled C Frabled				
	Eth Adapter Policy MQ-SMBd			0.000					
	Eth Adapter Policy SMBCkent	Transmit (ueues	1	[1-1000]				
	Ein Avlanter Policy SM856rV6r	Ring Size		4095	[64-4096]				
	Eth Adanter Policy SDICV	-			0 - 02 - 02 - 02 - 02 - 02 - 02 - 02 - 0		_	_	ElexPod Ethernet adapter policy: Notice the size buffers
	Eth Adapter Policy usNIC	Receive C	ANUES	: 8	[1-1000]				increased completion queries and intermeter edited at
	Eth Adapter Policy usNiCOracleRAC	Ring Size		: 4095	[64-4096]				increased, completion queues and interrupts adjusted,
	Eth Adapter Policy VMWare	-			e.				and RSS scaling enabled as recommended by FlexPod
1.3	Eth Adapter Policy VMware-16RXQs	Completic	1 Queues	: 9	[1-2000]			1	Cieco Validatod Dosign guidanco
	Eth Adapter Policy VMware-HighTrf	Interrupts		: 11	[1-1024]				cisco validated Design guidance.
	Eth Adapter Policy VMWarePassThru							/	
1	Eth Adapter Policy WIN-AzureStack	(a) Onti	ins.					/	
1.1	Eth Adapter Policy Win-HPN	Copp						/	
	Eth Adapter Policy Win-HPN-SMBd	Transmit 0	hecksum	Offload		: Disabled Enabled	/		
	Eth Adapter Policy Windows	Receive C	hecksum (Difficial		Disabled Enabled			
	FC Adapter Policy default	TCP Seat	entation (beoffic		Disabled Finabled	/		
1.3	FC Adapter Policy FCNVMelnitiator								
1.1	FC Adapter Policy FCNVMeTarget	TCP Large	Receive	Jffioad		: Disabled . Enabled			
	FC Adapter Policy Initiator	Receive S	de Scaling	(RSS)		: Olisabled Enabled			
	FC Adapter Policy Linux	Accelerat	d Receive	Flow Stot	ring	Oisabled O Enabled			
	FC Advoter Dolicy Target	Network V	itualizatio	in using Gr	neric Routing Encapsulation	: Disabled Enabled			
	EC Adapter Policy VMWare	Virtual Ext	A I eldered	N		Disabled C Enabled			
	FC Adapter Policy Windows	orium -		52		Do Bushing O Bushing			
	FC Adapter Policy WindowsBoot	GENEVE				. Contraction Character			
	ISCSI Adapter Policy default	AzureStoc	e-Host Qo	ŝ		Disabled Enabled			
· BK	OS Defaults	Failback T	meout (Se	econds)		: 5			[0-600]
• BK	OS Policies	Interrupt I	lode			MSLX OMSLO N TX			
	AMD-C125-Virt	in the second seco		Trees		(ONE ONE]			
1	Intel-M5-Virt	Interrupt (salescing	1Xbe		• wen Crae			
	Intel-M6-Virt	Interrupt 1	mer (us)			125			[0-65535]
8	SRIOV	RoCE				Disabled Enabled			
- 9	usNIC	Advance I	iter			Disabled C Enabled			
• Bo	ot Policies	later of the				O Deabled O Fashing			
	Inservative Dollarian	incorrupt 3	caring			Enabled			



Cisco UCS Manager policy

Keeping in mind these settings in the FlexPod Cisco UCS Manager for the VMware-HighTrf policy, look at the same setting transitioned properly to the Cisco Intersight platform (Figure 15).

=	cisco Intersight	CONFIGURE > Policies > VMware-HighTrf		🕫 9. 🕲 🗇 Matthew Faiello 🔔
×				Edit Policy
		Details	Usage	Configuration
6	Profiles Templates Policies Pools	Name VMwareHighTrf Description Type Ethernet Adapter Ursope 0 Last Update 20 hours apo	Q. Add Filter 0 items found 10 v per page 0 of 0 0 Name : Blatform Type Type Device Name Last Update :	Enable RDMA over Converged Off Ethernet Interrupt Scittings Interrupt Mode MSIx Interrupt Trate; us 125
	Taroets	Organization HexPod-VMware		Interrupt Coalescing Type Min
	Targets	imm_transition_v., 2.0.1	\$	Receive Receive Queue Count 8
5			Transitioned settings of the VMware-HighTrf Ethernet adapter policy	Heckelve king 528 4076 Transmit Transmit 04eee Count 1 Transmit Ring Size 4096
				Completion Completion Quive Court 9 Completion Ring Size 1 Uplink Fallback Timeout (seconds) (seconds) TCP Office Falleb Tr Indextum (Riflood Dr
				Enable Tri Checksum Offload On Enable Tri Checksum Offload On Enable Large Send Offload On Enable Large Pricerve Offload On Receive Side Scaling On
				Enable IPv4 Hash On

Figure 15. Settings transitioned to the Cisco Intersight platform

ucs Manager		8 9 9 9			• • • • • • • • •				
T. AI +	Servers / Policies / root / BIOS Policies / Intel-MS-Virt								
	Man Manurat Norofolion Sever Memorian Sever								
Caco HX240c MSSX HyperTex Syster	The second second second second second								
Cisco HXAF220: M4S HyperFlex Syste	Actions								
Cisco HXAF220c MSSX HyperFlex Sys	Dokts								
Ciaco HXAF220c M55X HyperFiles Sys	Show Polcy Usige								
Cisco HXAF240c M45X HyperFlex Sys									
Cleco HXAF240c MSSD HyperFlex Sys	And the second se								
Calco PXAP 2400 MOSX Pypernex Sys									
Cisco UCS 8200 M4	Name : Intel-MS-Virt	CDN enabled							
Cieco UCS 5200-WS	Description								
Calco OCS 6200-440	Owner : Local								
Conce UCS D4D0-MS	Reboot on BIOS Settings Change :								
Circo UCS C3K-M45R8									
Ceco UCS C3x80-M4598									
Ceco UCS C3X60-SV9NB	5 Adversed Filter III Export III Print				0				
Cisco UCS S3200-MSSRB	BOSSetting		Value						
Cisco UCSB EX-M4 1	PCie Slots CDN Control		Platform Delaut		*				
Oteco UCSB EX-M4 2	CDN Control		Enabled						
Cisco UCS8 EX-M4 3	Front panel locksut		Platian Delait						
UCSO-C125	DOIT anno an at								
 BIOS Policies 	Post env pase		Parter Centre						
AMD-C125-Virt	Quet Boot		Deabled		•				
PEM-MS-VM	Resume on AC power loss	Servers / Publics / cost / BCS Publics / boat MI-Ver	Muslima Pade A		*				
intel-MS-Virt		the I shared I doubters. They been	and faith						
SROV		The second second second second	who is an in characteristic house	and the design of the second se					
USNIC	O THE REAL PROPERTY AND A REAL PROPERTY AND A	Antonio Alexa Alexa							
 Boot Policies 	C-states disabled on the	and famous	Salawether - E Just - @ No.						
Diagnostics volces	Advanced > Processor tab								
Graphics Card Policies	Autonocu - Frocessor tas	NC restance		Patter Intel					
Post remeat Packages		Test sectors		Protect Local					
KVM Masanement Dräniss		Sat Webb Chatterry		Partien Delaut					
Local Disk Confin Polinies		Local 3D Apre		Pattern Dalaut					
Maintenance Policies		Max Variable Of THE Service		Platent Delaut					
Management Firmware Packages		# (Table Conviction		Photose (John #					
Memory Policy		Parrage C Stars Love		Parture Debuilt					
Persistent Memory Policy		Admention Cere C-state		Patters Sela-8					
Power Control Policies		Passani Chan		Distance					
Power Sync Policies		Promer Cit							
 SPDM Certificate Policies 		Princesson C3 Report		Dealer					
Scrub Policies		Processor CC Report		The second se					
 Serial over LAN Policies 		Processor GHO		Platen Delas					
 Server Post Policies 		Page Indentity		Later					
Server Pool Policy Qualifications		Europ Nationana		Pattern Delauk					
 Threshold Policies 		Processor UP Crains		Platian Delast					
ISCSI Authentication Profiles		PromodalPolts		Pattern Delad					
()									

Next, examine a BIOS policy, Intel-M5-Virt, a custom Cisco UCS Manager BIOS policy (Figure 16).

Figure 16.

Custom Cisco UCS Manager BIOS policy

Now examine the Intel-M5-Virt BIOS policy, specifically the content delivery network (CDN) and C-state tokens, after the transition to the Cisco Intersight platform using the IMM Transition Tool (Figure 17).

=	cisco Intersight		CONFIGURE > Policies > Intel MS-Virt Q 2									Matthew Falello
×												Edit Policy
	Orchestration	Details	s Usage						Configuration OPI 2	_		
	Templates Policies		Intel-M5-Virt BIOS 2					items found 10 🗸	per page 🔍 🔇 _1 Device Name			platform-default platform-default
			21 hours ago					Template		21 hours ago	Serial Port 1	-
Đ								Template		21 hours ago		platform-default
		Tags					Server Management 19	6				
l.												platform-default
		imm transition n. FX-Trans-3						platform-default				
									platform-default			
											Consistent Device Naming	enabled
												platform-default
												platform-default
			Elsewhe	ere in	the long l	BIOS toke	n list on th	e right side	9		OptionROM Launch Optimization	platform-default
			of the pa	ane,	you can se	ee that C-	states are	disabled.				platform-default
							-					platform-default
												platform-default
												platform-default
		-										platform-default
			Processor CTE deatled								OS Boot Watchdog Timer Policy	platform-default
		Processor CIE deabled Processor CI Singert deabled Processor CI Singert deabled								disabled	OS Boot Watchdog Timer Timeout	platform-default
								Processor C6 Report		disabled		platform-default
										Concerto -		platform-default
		L. L	_									platform-default
												platform-default

Figure 17.

The BIOS policy after the transition to the Cisco Intersight platform

As you can see, the token settings transitioned properly to IMM.

The example in Figure 18 shows a FlexPod SAN boot policy, Boot-FCP, from Cisco UCS Manager. All four paths are configured according to best practices.

-1 1.1 1. CISCO	UCS Manager			8 8 9 9						0) () ()
ж	м .	Servers / Policies / root / Sub-Organizations / RexPod-V	Mware / Boot Policies / Boot Policy Boot-FCP									
•	Cisco UCSB EX-M4 2 Cisco UCSB EX-M4 3	General Events	Providerilies									
also a	UC9C-C125	Dente	Name	Boot-FCP								
	AMD-C125-Vitt	Show Policy Usage	Description									
	intel-MS-Virt		Owner	Local								
=	Intel-M5-Virt		Reboot on Boot Order Change	0								
	SROV		Enforce vNC/vH8A/iSCSI Name									
•	usNIC		Boot Made	Legacy (e) Ueft								
	Boot Polices		Boot Security									
40	Boot Policy default-LIFF	Warning										
	Boot Policy deg											
	Boot Policy utility	The type (primary/secondary) does not indicate a boot order pr The effective order of boot devices within the same device class	resence. ss (LAN/Storage/(SCSI) is determined by PCIe bus scan order.									
	Diagnostics Policies	If Enforce vNIC/VHBA/ISCSI Name is selected and the vNIC/V If it is not selected, the vAICsAbiliAs sea selected if they avait	HBA/ISCSI does not exist, a config error will be reported.									
	Graphics Card Policies											
	 Host Finnware Packages 											
	IPM/Redfish Access Profiles	Local Devices	Boot Order									
	 KVM Management Policies 		+ - Ty Advanced Filter + Export	e Pres								0
	Local Dek Centrg Policies	CIMC Mounted vMedia	Name Order	 www.ebassce.wwc 	Type	LUN Name	WWW	Slot Number	Boot Name	Boot Path	Description	
	Management Foreses Management Foreses	(a) while	Pernote CD/DVD 1									<u>^</u>
	Memory Drive	(i) energy	+ Sen 2									
	Persistent Memory Policy	(+) vHBAs	- SAN Diman	DDD-Dates-A	Domasia							
	Power Control Policies		PAN Tasan Ibi		Distant	0	200120-20164-17	13.60				
	Power Sync Policies	ISCSI vNICs	SAM Karget PR.		enerary	0	2010 (100:2010)(1)	12:00				
	SPDM Certificate Policies		SAN target 5		becondary	.0	20.03.00.39364.17	12.98				
	Scrub Policies	(EFI Shell	= SAN Secondary	FCP-Fabre-R	Secondary							
	 Serial over LAN Policies 											
	Server Pool Policies											
	Server Pool Policy Qualifications											
	Internal Policies Internation Dentine		FlexPod	SAN boot pa	ramete	rs with fo	our naths					
	vMedia Policies		TICKI OG	or it boot pu	Tunicie	,	a putito					
	sNC/vHBA Placement Policies		configu	red: primary a	and sec	ondary p	aths for					
	 Sub-Organizations 		heath fal	and a substant share		denter a	A DIA -					
	 FlexPod-VMware 		both fac	pric virtual no	st bus a	idapters (VHBAS)					
	Adapter Policies											
	BIOS Policies											
	 Boot Policies 											
	Boot Policy Boot-PCP											
	Boot Policy Boot-SCS											
	Book Holey NATION -BOOK-FCP											
	 Gauching Card Projects 											
	and the second second and the second s											
	Host Firmware Packages											

Figure 18.

SAN boot policy configured in Cisco UCS Manager

Figure 19 shows Boot-FCP in IMM. You can see that the policy values have properly transitioned.



Figure 19.

Properly transitioned policy values in Cisco Intersight platform

Considerations and caveats for using the IMM Transition Tool

Note the following considerations and warnings when using the IMM Transition Tool:

- Because a Cisco UCS Central transition likely encompasses many individual Cisco UCS domains, when running the IMM Transition Tool for a Cisco UCS Central instance, you will not see the hardware Inventory in the IMM Readiness Report. Also, you will not see domain policies or a domain profile in the Cisco UCS Central configuration transition to the Cisco Intersight platform. Therefore, if you are transitioning from Cisco UCS Central, follow the Cisco UCS Central transition with individual fabric-only transitions for the desired target Cisco UCS Manager domains to get the hardware readiness information for that domain and, more important, to transition the domain policies and resulting domain profile for that domain to the Cisco Intersight platform. A Cisco UCS Manager domain transition gives you the option and flexibility of transitioning the fabric only (fabric interconnect configurations), the server only (server pools, policies, and templates), or both.
- Currently, the transitioning of service profiles is not recommended (the capability to do so exists, but IDs are not retained). Server profile templates are transitioned to the Cisco Intersight platform, and after they are in Cisco Intersight the administrator can derive IMM server profiles from the migrated templates. Pay close attention to the migrated ID pools. If those IDs will remain in use in Cisco UCS Manager or Cisco UCS Central, then you'll need to edit and change the Cisco Intersight pools to make sure that there are no possible conflicts. Also, if you want to have the same identities in the IMM server profile (universally unique ID [UUID], MAC address, World Wide Node Name [WWNN], etc.), then you'll need to manually assign the desired, applicable IDs in the server profile.

Note: Service profile transitioning (with IDs maintained) will be supported in the next release of the IMM Transition Tool. Contact your Cisco account team for more information about the next release of the tool.

- If you are performing multiple data collections or transitions for the same Cisco UCS domain or Cisco UCS Central instance, remember to use the Refresh button in the Transition user interface to generate a new inventory and configuration transition, instead of simply clicking Next and using the cached data from the prior collection or transition.
- The IMM Transition Tool allows progressive, iterative transitioning of your Cisco UCS or Cisco UCS Central configurations to the Cisco Intersight platform. Consider migrating a just a portion of the service profile templates at a time (using the filtering option), or if you have a multiple-organization architecture, consider transitioning one organization at a time. Although the name of only the transition needs to be unique, using a descriptive name including the domain name and perhaps the organization name is useful to help you keep track of multiple transitions.

Conclusions

Note the following main points about the IMM Transition Tool:

- The IMM Transition Tool is a valuable asset to have in your Cisco UCS environment. The IMM Readiness Report alone is extremely useful for quickly generating all the required details about a Cisco UCS domain or Cisco UCS Central environment.
- The IMM Transition Tool is free of cost and poses no threat to running workloads in Cisco UCS domains. Querying is completely read-only through the API.
- The IMM Transition Tool can be used with essentially any Cisco UCS environment and allows configurations to transition to both SaaS-based and on-premises Cisco Intersight platforms.

- If you are transitioning a Cisco UCS or Cisco UCS Central configuration to Cisco Intersight, and you
 decide that you want to delete that transition within the Cisco Intersight, platform you must follow
 this sequence of steps:
 - 1. Delete domain profiles.
 - 2. Delete service profile templates.
 - 3. Delete all policies.
 - 4. Delete organization from the Settings tab.

Note: The Cisco Intersight platform does not permit the deletion of objects that are in use.

For more information

Consult the resources listed here for additional information.

YouTube videos

If you are new to the IMM Transition Tool, watch both of the following YouTube videos:

- Advantage IMM 2–IMM Transition Tool (Cisco UCS Manager transition example): <u>https://www.youtube.com/watch?v=Oqmf2CAPxtE&t=2s</u>
- New Release–IMM Transition Tool Version 2.0.1 (Cisco UCS Central transition example): <u>https://youtu.be/duczkcICYrk</u>

Software and guides

- IMM transition software, release notes, and user guide: <u>https://ucstools.cloudapps.cisco.com/#/downloadApp</u>
- FlexPod design guides: https://www.cisco.com/c/en/us/solutions/design-zone/data-centerdesign-guides/FlexPod-design-guides.html

Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at https://www.cisco.com/go/offices.

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: https://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)

Printed in USA