Konfiguration und Beantragung eines eigenständigen Servers der C-Serie in Intersight nach dem Austausch des Motherboards

Inhalt

Einleitung Voraussetzungen Anforderungen Verwendete Komponenten Hintergrundinformationen Problem: Neuer RMA-Server wird in Intersight nicht beansprucht, und der ursprüngliche ausgefallene Server wird beansprucht Lösung Grundlegende Überprüfung bei Problemen mit Geräteansprüchen Allgemeine Anforderungen an die Netzwerkkonnektivität von Cisco Intersight Zugehörige Informationen

Einleitung

In diesem Dokument wird beschrieben, wie Sie in Cisco Intersight einen Standalone-Server der C-Serie konfigurieren und beanspruchen, nachdem die Hauptplatine ausgetauscht wurde.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Integrated Management Controller (CIMC)
- Cisco Interview
- Cisco Server der C-Serie

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Cisco C240-M5 4.1(3 d)
- Cisco Intersight Software-as-a-Service (SaaS)

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

Verwandte Produkte

Dieses Dokument kann auch mit folgenden Hardware- und Softwareversionen verwendet werden:

- C-Serie M4 3.0(4) und höher
- C-Serie M5 3.1 und höher
- C-Serie M6 4.2 und höher
- S-Serie M5 4.0(4e) und höher

Anmerkung: Eine umfassende Liste der unterstützten Hardware und Software finden Sie unter den folgenden Links: <u>Von Intersight unterstützte PIDs</u> und von <u>Intersight unterstützte</u> <u>Systeme.</u>

Hintergrundinformationen

- Der häufigste Anwendungsfall für dieses Dokument ist, wenn eine C-Serie bei Cisco Intersight angemeldet wurde und das Motherboard durch eine Retourengenehmigung (Return Material Authorization, RMA) ersetzt wird. Bei jeder RMA muss der ursprüngliche Server zurückgezogen werden, und der neue Server muss in Cisco Intersight angemeldet werden.
- In diesem Dokument wird davon ausgegangen, dass der ursprüngliche Server der C-Serie vor der RMA für das Motherboard erfolgreich angefordert wurde und dass es keine Konfigurations- oder Netzwerkprobleme gibt, die zu einem fehlgeschlagenen Anfrageprozess führen würden.
- Sie können Ziele direkt über das Cisco Intersight-Portal oder den Device Connector des Endpunkts selbst freigeben. Es wird empfohlen, Ziele über das Cisco Intersight-Portal freizugeben.
- Wenn ein Ziel direkt aus dem Device Connector und nicht aus dem Intersight-Portal entfernt wird, wird es in Cisco Intersight als nicht beansprucht angezeigt. Außerdem muss das Endgerät manuell aus Cisco Intersight entfernt werden.
- Der ursprüngliche Server der C-Serie zeigt in Cisco Intersight wahrscheinlich den Status Not Connected (Nicht verbunden) an. Dies kann je nach dem Grund, warum das Motherboard ausgetauscht werden muss, variieren.

Problem: Neuer RMA-Server wird in Intersight nicht beansprucht, und der ursprüngliche ausgefallene Server wird beansprucht

Wurde in Cisco Intersight ein Standalone-Server der C-Serie angefordert, wird die Seriennummer (SN) des Servers mit Cisco Intersight gepaart. Wenn der beanspruchte Server aufgrund eines Fehlers oder aus einem anderen Grund einen Austausch der Hauptplatine erfordert, muss der Anspruch für den ursprünglichen Server aufgehoben und der neue Server in Cisco Intersight eingefordert werden. Die SN der C-Serie ändert sich mit der RMA des Motherboards.

Lösung

Heben Sie die Rücknahme des Servers der C-Serie von Cisco Intersight auf, der ersetzt werden muss. Konfigurieren Sie die neuen Server CIMC und Device Connector, und fordern Sie den neuen Server bei Cisco Intersight an.

Schritt 1: Starten Sie Cisco Intersight, und klicken Sie auf Admin > Targets. Wählen Sie das Kästchen für die Zielgeräte aus, die ersetzt und nicht beansprucht werden sollen, und klicken Sie auf Trash Can Icon > Unclaim wie in diesem Bild dargestellt.

=	cisco Intersight	ADMIN > Targets	٩	2	₽ °	0) Jan	nes Delli Paoli 🗕
<u>e0o</u>	MONITOR						Clair	n a New Target
	OPERATE ^							
3	Servers	All largets 0 +			1 items found	10 ∽ perp	age 🗹 🔇 👘	1 of 1 [2] [3]
	Chassis	Connection X Top Targets by Types X Vend	dor					-
	Fabric Interconnects	Connected 1						
	HyperFlex Clusters							
×	CONFIGURE ^	🔽 Name Status L	Unclaim Target From Intersight		Claimed	By :	Product ID	
	Profiles	C-Series-Claim-Original-MB IN Not Connected T	arget Calence Intersignt. Unclaiming the	this target	jdellipa@	icisco.com	UCSC-C240-M	5SN
	Posis	Selected 1 of 1 Show Selected Unselect All	va device conseponding data inom your intensight account. The endpoint was onligured settings.	w retain its			K.	of 1 🕞 🗵
0	ADMIN ^		ee you sure you want to unclaim?					
-	Targets		Cancel	in .				

Schritt 2: Schließen Sie einen Keyboard Video Monitor (KVM) an den neu ausgetauschten Server an (überspringen Sie diesen Schritt, wenn CIMC bereits konfiguriert wurde). Wählen Sie im Cisco Begrüßungsbildschirm beim Start F8 um CIMC zu konfigurieren. Konfigurieren Sie die entsprechenden Network Interface Card (NIC) Properties für Ihre Umgebung und drücken Sie F10 zu Save. Verlegen Sie physische Kabel zum Server und zum angeschlossenen Gerät auf Basis des NIC Properties zur Verwaltung verwendet.

Anmerkung: Schritt 2. zeigt und beschreibt eine lokale Einrichtung des CIMC mit einem angeschlossenen KVM direkt an einen C240-M5. Die erste CIMC-Einrichtung kann auch remote über DHCP durchgeführt werden. Bitte beachten Sie die Installationsanleitung für Ihr Servermodell, und wählen Sie die für Sie optimale CIMC-Ersteinrichtung aus.



Schritt 3: Starten Sie die grafische Benutzeroberfläche (GUI) von CIMC, und navigieren Sie zur Admin > Device Connector. Wenn Device Connector ist deaktiviert. Wählen Sie Turn On. Nach der Aktivierung wählen Sie Settings.

Tipp: Navigieren Sie in der CIMC-GUI zu Chassis > Summary und vergleichen Sie Firmware Version um zu bestätigen, dass die Firmware-Mindestanforderungen erfüllt sind und von Cisco Intersight angefordert werden. Verwenden Sie diesen Link, um die Mindestanforderungen für Ihr spezifisches Servermodell zu überprüfen: <u>Intersight Supported</u> <u>Systems (Intersight-unterstützte Systeme)</u>. Wenn die Firmware nicht die erforderlichen Mindestanforderungen erfüllt, führen Sie ein Host Upgrade Utility (HUU) auf dem Server aus. Weitere Informationen finden Sie hier: <u>Cisco Host Upgrade Utility-Prozess</u>.

	Se disco Integrated Management Controller	🐥 🔽 admin(
	Admin / Device Connector *	Refresh Host Power Launch vKVM Pir
Chassis •	The Device Connector is an embedded management controller that enables the capabilities of Cisco In	tersight, a cloud-based management platform. For detailed information about configuring the device connec
Compute		
Networking	Cisco Intersight [™] provides intelligent cloud-based infrastructure management with embedded analytics for the Cisco United Computing System [™] (Cisco UCS®) and Cisco HyperFlex® platforms.	
Storage	This platform offers an intelligent level of management that enables IT organizations to analyze, simplify, and automate their enviroments in more advanced ways than the prior generation of tools.	
Admin .	Turn on the Device Connector to enable Intersight Management.	
User Management	Turn On	
Networking		
Communication Services		Device Connector Internet
Security Management		
Event Management		
Firmware Management		
Utilities		
Device Connector		

		LOF TREFESH Host Power Launch vKVM Ping CIMC Reboot			
Chassis hent controller that enables the capabilities of Cisco Intersight, a cloud based management platform. For detailed information about configuring the device connector, please visit i					
Compute				Settings	C Refresh
Networking	+	ACCESS MODE ALLOW CONTROL	Device ID		
Storage	+		1071-740		Ē
Admin	•				
User Management		Internet Intersight			
Networking					
Communication Services					
Security Management					
Event Management		s successful, but device is still not claimed. To claim the device open Cisco Intersight, create a new account and follow the guidance or Open Device for existing account. Intersight			
Firmware Management					
Utilities					
Device Connector					

Schritt 3.1. Navigieren Sie zu Admin > Device Connector > Settings > DNS Configuration und die entsprechenden DNS Server und Save wie in diesem Bild dargestellt.

iguration	Configure DNS settings for IMC Software		
iguration figuration	Domain Name	٥	
e Manager	DNS Server		
	144.117/2286.109	• +	

Schritt 3.2. Navigieren Sie zu Admin > Device Connector > Settings > NTP Configuration. Konfigurieren Sie NTP Server für die jeweilige Umgebung zu adressieren und Save wie in diesem Bild dargestellt.

Admin / Device	Connector \pm		Refresh	Host Power Launch vKVM Ping CIMC Reboot Locator LED @
he Device Connector is an embe	edded management controller that enables the capabilities of	Cisco Intersight, a cloud-based managem	ent platform. For detailed information	on about configuring the device connector, please visit Help Center
Settings				×
General				
DNS Configuration	Configure NTP settings for IMC Software			
NTP Configuration	NTP Server			
Proxy Configuration	2222	0	+	
Certificate Manager				
Connection				Cancel Save
1.0.11-2209				

Schritt 3.3. Konfigurieren Sie bei Bedarf optional einen Proxy, um Cisco Intersight zu erreichen. Navigieren Sie zu Admin > Device Connector > Settings > Proxy Configuration > Enable Proxy. Konfigurieren Sie Proxy Hostname/IP Und Proxy Port Und Save.

Admin / Device Connector *

Refresh | Host Power | Launch vKVM | Ping | CIMC Reboot | Locator LED | @

The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud-based management platform. For detailed information about configuring the device connector, please visit Help Center

Settings			\$
General			
DNS Configuration	Configure proxy settings		
NTP Configuration	Enable Proxy		
Proxy Configuration	Proxy Hostname/IP *	0	Proxy Port *
Certificate Manager			1+65535
Connection	Authentication		
			Cancel

Schritt 4: Wählen Admin > Device Connector und kopieren Sie Device ID und Claim Code. Kopieren Sie beide in einen Notizblock oder eine Textdatei zur späteren Verwendung.

	Services Cisco Integrated Management Contr	🐥 🔽 - C-Series-Reclaim-New-RMA-MB 🌣
Chassis	Admin / Device Connector *	Refresh Host Power Launch vKVM Ping CIMC Reboot Locator LED 🖉 🕚
Compute	The Device Connector is an embedded management controller that enables the capabilities of Cisco Intersight, a cloud bas Help Center	sed management platform. For detailed information about configuring the device connector, please visit
Networking	Device Connector	③ Settings 〇 Refresh
Storage .	ACCESS MODE - ALLOW CONTROL	Device ID
Admin •		Claim Code
Networking Communication Services	Device Connector Internet	Intersight
Security Management	Not Claimed	
Event Management Firmware Management	The connection to the Cisco Intersight Portal is successful, but device is still not claimed. To claim the device open Cisco account and follow the guidance or go to the Targets page and click Claim a New Device for existing account.	o Intersight, create a new Open Intersight
Utilities	10.11-2299	
Device Connector		

Schritt 5: Starten Sie Cisco Intersight, und navigieren Sie zu Admin > Targets > Claim a New Target > Cisco UCS Server (Standalone) > Start. Geben Sie Device ID und Claim Code der aus der CIMC-GUI kopiert wurde, und wählen Sie Claim.



Ш	cisco Intersigh	t	ADMIN > Targets > Claim a New Target	٥	⊠	o 0	James Delli Paoli	ತಿ
<u>⊪</u> ⊛	MONITOR OPERATE Servers Chassis			Claim Cisco UCS Server (Standalone) Target To claim your target, provide the Devic Code and select the appropriate Resou	e ID, Claim Irce Groups.			
	Fabric Interconnects HyperFlex Clusters		General Device ID * Claim Code *	1				
×	CONFIGURE						0	
	Profiles		Resource Groups					
	Policies							
	Pools		 Select the Resource Groups if required. However, this selection is the selection of all Organizations with the Resource Group type 	: All'.	Resource Group typ	e is All. The claimed	target will	
ğ	ADMIN			D items found	10 v per page	ाटी दी 0 of 0 जि	8	
	Targets		□ Name	Usace	Desc	ription		
						0 2 2	of 0 [>] [>]	
						-		
			K Back Cancel				Claim	

Schritt 6: Navigieren Sie zu Admin > Targets. Ein erfolgreicher Anspruch zeigt die Status > Connected, wie in diesem Bild dargestellt.

	cisco Intersight	ADMIN > Targets	🗘 🗖 1 🛛 🖓 💮 💮 James Deli Pacil 🖉
<u>alo</u>	MONIFOR		Claim a New Target
ø	OPERATE A	× 1970-100 0 1	
	Servers		☐ Export 1 Rems found 10 ∨ per page (C < 1 of 1 ≥ 20
	Chassie	Connection X Top Targets by Types X Vendur	
	Fabric Interconnects	Convected 1	
	HyperFlex Clusters		
×	CONFIGURE ^	Name Status Type Target D Claimed Time	Claimed By Product 10
	Profiles	Connected Standalone MS Server WERESENTERVY S minutes ago	jółilpagcisco.com anteriorationette
	Porces	/ 1	
ത	1010		
ιψ.	ALMIN P		
	Tapka		

Grundlegende Überprüfung bei Problemen mit Geräteansprüchen

Anmerkung: Eine umfassende Liste der Fehlerbedingungen und Problembehebungen finden Sie unter: <u>Device Connector Error Conditions and Remediation Steps.</u>

Statusbeschreibungen der Geräteanschlussverbindungen

Gefordert

Statuserklärungen für Geräteanschluss-Verbindungen Die Verbindung zur Cisco Intersight-Plattform wurde erfolgreich

Mögliche Problembehebung

	hergestellt, und Sie haben die Verbindung angefordert.	
Nicht beansprucht	Die Verbindung zur Cisco Intersight- Plattform ist erfolgreich, der Anspruch auf das Endgerät steht jedoch noch aus.	Sie können über Cisco Intersig eine noch nicht beanspruchte Verbindung anfordern.
Administrator deaktiviert	Zeigt an, dass der Intersight- Management-/Geräteanschluss auf dem Endpunkt deaktiviert wurde.	Aktivieren Sie den Geräteansc am Endpunkt.
DNS falsch konfiguriert	DNS wurde im CIMC falsch oder überhaupt nicht konfiguriert.	Zeigt an, dass keiner der auf d System konfigurierten DNS- Namenserver erreichbar ist. Überprüfen Sie, ob Sie gültige Adressen für die DNS-Namens eingegeben haben. Über diesen Link können Sie feststellen, ob Intersight derzei
Intersight-DNS-Auflösungsfehler	DNS ist konfiguriert, kann jedoch den DNS-Namen von Intersight nicht auflösen.	gewartet wird: <u>Status des</u> <u>Interviews</u> . Wenn Intersight betriebsbereit ist, weist dies wahrscheinlich darauf hin, das DNS-Name des Intersight-Dier nicht aufgelöst wurde. Prüfen und bestätigen: MTU is End-to-End korrekt. Port 443 u
UCS Connect-Netzwerkfehler	Zeigt die ungültigen Netzwerkkonfigurationen an.	sind zulässig, die Firewall lässi physischen und virtuellen IPs z DNS und NTP werden auf dem
Fehler bei der Zertifikatsüberprüfung	Das Endgerät weigert sich, eine Verbindung zur Cisco Intersight- Plattform herzustellen, da das von der Cisco Intersight-Plattform vorgelegte Zertifikat ungültig ist.	Abgelaufenes oder noch ungül Zertifikat: Überprüfen der ordnungsgemäßen Konfigurati des NTP und der Synchronisie der Gerätezeit mit der koordinie Weltzeit Überprüfen der ordnungsgemäßen Konfigurati des DNS Wenn ein transparen Webproxy verwendet wird, stel Sie sicher, dass das Zertifikat n abgelaufen ist. Der vom Webserver angegebe Zertifikatname stimmt nicht mit DNS-Namen des Intersight-Die überein: Überprüfen der ordnungsgemäßen Konfigurati des DNS Wenden Sie sich an Webproxy-Administrator, um z überprüfen, ob der transparent Webproxy richtig konfiguriert is Insbesondere muss der Name vom Webproxy bereitgestellter Zertifikats mit dem DNS-Name Intersight-Dienstes

(svc.intersight.com) übereinstimmen. Das Zertifikat wurde von einer vertrauenswürdigen Zertifizierungsstelle ausgestell Überprüfen der ordnungsgemä Konfiguration des DNS Wende sich an Ihren Webadministrato an infosec, um zu überprüfen, der transparente Webproxy ric konfiguriert ist. Insbesondere r der Name des vom Webproxy bereitgestellten Zertifikats mit o DNS-Namen des Intersight-Die übereinstimmen.

Allgemeine Anforderungen an die Netzwerkkonnektivität von Cisco Intersight

- Eine Netzwerkverbindung zur Intersight-Plattform wird über den Device Connector im Endpunkt hergestellt.
- Überprüfen Sie, ob zwischen dem verwalteten Ziel und Intersight eine Firewall implementiert ist oder ob sich die Regeln für eine aktuelle Firewall geändert haben. Dies kann zu End-to-End-Verbindungsproblemen zwischen dem Endgerät und Cisco Intersight führen. Wenn die Regeln geändert werden, stellen Sie sicher, dass die geänderten Regeln den Datenverkehr durch die Firewall zulassen.
- Wenn Sie einen HTTP-Proxy verwenden, um den Datenverkehr von Ihrem Standort aus weiterzuleiten, und wenn Sie Änderungen an der Konfiguration des HTTP-Proxyservers vorgenommen haben, stellen Sie sicher, dass Sie die Konfiguration des Gerätekonnektors entsprechend den Änderungen ändern. Dies ist erforderlich, da Intersight HTTP-Proxyserver nicht automatisch erkennt.
- Konfigurieren Sie DNS, und lösen Sie den DNS-Namen auf. Der Geräte-Connector muss DNS-Anfragen an einen DNS-Server senden und DNS-Einträge auflösen können. Der Geräteanschluss muss in der Lage sein, svc.intersight.com in eine IP-Adresse aufzulösen.
- Konfigurieren Sie das NTP, und überprüfen Sie, ob die Gerätezeit ordnungsgemäß mit einem Zeitserver synchronisiert wurde.

Anmerkung: Eine umfassende Liste der Verbindungsanforderungen für Intersight finden Sie in <u>Intersight Network Connectivity Requirements.</u>

Zugehörige Informationen

- <u>Cisco Intersight: Erste Schritte Forderungsziele</u>
- SaaS-unterstützte Systeme von Cisco Intersight
- Von Cisco Intersight SaaS unterstützte PIDs
- <u>Cisco Intersight-Netzwerkanbindungsanforderungen</u>
- <u>Cisco Interview-Schulungsvideos</u>
- Cisco Bug-ID <u>CSCvw76806</u> Ein eigenständiger Server der C-Serie kann in Cisco Intersight nicht erfolgreich behaupten, wenn die Geräteanschlussversion kleiner als 1.0.9 ist.
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.