Configure e reivindique um servidor independente C-Series na Intersight após a substituição da placa-mãe

Contents

Introduction Prerequisites Requirements Componentes Utilizados Informações de Apoio Problema: O novo servidor de RMA não é reivindicado na Intersight e o servidor com falha original é reivindicado Solução Verificação básica para problemas de declaração do dispositivo Requisitos gerais de conectividade de rede da Cisco Intersight Informações Relacionadas

Introduction

Este documento descreve como configurar e reivindicar um servidor C-Series independente no Cisco Intersight após a substituição da placa-mãe.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Controlador de gerenciamento integrado da Cisco (CIMC)
- Entrevista da Cisco
- Servidores Cisco C-Series

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco C240-M5 4.1(3d)
- Software como serviço (SaaS) Cisco Intersight

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Produtos Relacionados

Este documento também pode ser usado com as seguintes versões de hardware e software:

- C-Series M4 3.0(4) e posterior
- C-Series M5 3.1 e posterior
- C-Series M6 4.2 e posterior
- S-Series M5 4.0(4e) e posterior

Note: Para obter uma lista abrangente de hardware e software compatíveis, consulte estes links: <u>PIDs com suporte da Intersight</u> e <u>sistemas com suporte da Intersight</u>.

Informações de Apoio

- O caso de uso mais comum para este documento é quando uma C-Series foi solicitada à Cisco Intersight e a placa-mãe é substituída pela RMA (Return Material Authorization, Autorização para material de devolução). Sempre que ocorre uma RMA, o servidor original precisa ser cancelado e o novo servidor precisa ser cancelado no Cisco Intersight.
- Este documento supõe que o servidor C-Series original foi reivindicado com êxito antes da RMA da placa-mãe e que não há problemas de configuração ou de rede que contribuam para um processo de reivindicação com falha.
- Você pode cancelar a reivindicação de alvos diretamente do Cisco Intersight Portal ou do Device Connector do próprio endpoint. Recomenda-se cancelar a reivindicação de alvos do Cisco Intersight Portal.
- Se um destino não for reivindicado diretamente do conector do dispositivo e não do portal Intersight, ele mostrará o destino dentro do Cisco Intersight como não reivindicado. O endpoint também precisa ser manualmente cancelado da Cisco Intersight.
- O servidor C-Series original provavelmente exibe o status como Não conectado no Cisco Intersight. Isso pode variar dependendo do motivo pelo qual a placa-mãe precisa ser substituída.

Problema: O novo servidor de RMA não é reivindicado na Intersight e o servidor com falha original é reivindicado

Se um servidor C-Series autônomo foi reivindicado no Cisco Intersight, o número de série do servidor (SN) torna-se emparelhado com o Cisco Intersight. Se o servidor solicitado precisar de uma substituição de placa-mãe devido a uma falha ou por qualquer outro motivo, o servidor original precisa ser cancelado e o novo servidor precisa ser solicitado no Cisco Intersight. O SN C-Series muda com a RMA da placa-mãe.

Solução

Não solicite a substituição do servidor C-Series da Cisco Intersight. Configure os novos servidores CIMC e Device Connector e solicite o novo servidor para a Cisco Intersight.

Etapa 1. Inicie o Cisco Intersight e clique em Admin > Targets. Selecione a caixa para o(s) destino(s) que deve(m) ser substituído(s) e não reivindicado(s) e clique no botão Trash Can Icon > Unclaim como mostrado nesta imagem.

≡	cisco intersight	ADMIN > Targets	۵ 🗖	🕞 9, 🧔 🕥 James Delli Paoli 🧕
<u>00o</u>	MONITOR			Claim a New Target
	OPERATE ^			
3	Servers	All Targets +	G Expo	t 1 items found 10 v per page 또 또 1 of 1 관 계
B	Chassis	Connection % Top Targets by Types %	Vendor	
	Fabric Interconnects	Connected 1	\bigcirc	
	HyperFlex Clusters	* Standakone Mo Server 1	e Calco system, inc. 1	
×	CONFIGURE ^	Vame Status	Unclaim Target From Intersight	Claimed By Product ID 🖇
	Profiles	C-Series-Claim-Original-MB III Not Connected	Target will be unclaimed from intersight. Unclaiming this targ	t jdellipa@cisco.com UCSC-C240-M5SN ····
	Policies	Belected 1 of 1 Show Selected Unselect All	will delete corresponding data from your intersight account. The endpoint will retain configured settings.	•
	Pools		Are you sure you want to unclaim?	
١	ADMIN ^		Cancel	1
	Targets			2 .

Etapa 2. Conectar um KVM (Keyboard Video Monitor, Monitor de vídeo do teclado) ao servidor recém-substituído (ignore esta etapa se o CIMC já tiver sido configurado). Na tela inicial da Cisco na inicialização, selecione F8 para configurar o CIMC. Configure o Network Interface Card (NIC) Properties para o seu ambiente e pressione F10 para Save. Insira cabos físicos ao servidor e ao dispositivo conectado com base no NIC Properties usado para gerenciamento.

Note: Etapa 2. ilustra e descreve uma configuração local do CIMC com um KVM conectado diretamente a um C240-M5. A configuração inicial do CIMC também pode ser feita remotamente com DHCP. Consulte o Guia de instalação adequado ao seu modelo de servidor e escolha qual configuração inicial do CIMC é melhor para você.

File View Macros Tools Power Boot Device Virtual Media Help	S
Cisco IMC Configuration Utility Version 2.0 Cisco Systems, Inc. MIC Properties NIC mode Dedicated: [X] Shared LOM: [] Cisco Card: Riser1: [] NLOm: [] Shared LOM: [] HLOM: [] Shared LOM: [] Shared LOM: [] Shared LOM: [] Shared LOM: [] Shared LOM: [] Shared LOM: [] DMCP enabled [] CICC TP: Pref (MS Server: Smart Access USB Enabled []	

Etapa 3. Inicie a interface gráfica do usuário (GUI) do CIMC e navegue até Admin > Device Connector.

Tip: Na GUI do CIMC, navegue até **Chassis > Summary** e comparar o **Firmware Version** para confirmar se os requisitos mínimos de firmware foram atendidos e serão solicitados pela Cisco Intersight. Utilize esse link para verificar os requisitos mínimos para seu modelo de servidor específico: <u>Sistemas suportados pela Intersight</u>. Se o firmware não atender aos requisitos mínimos a serem solicitados, execute um Host Upgrade Utility (HUU) no servidor, consulte aqui: <u>Processo do utilitário de atualização de host da Cisco</u>.

	Cisco Integrated Management Controller	🜲 🔽 admin
	A / Admin / Device Connector *	Refresh Host Power Launch vKVM Pir
Chassis •	The Device Connector is an embedded management controller that enables the capabilities of Cisco Int	ersight, a cloud-based management platform. For detailed information about configuring the device connect
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
Security Management		
Event Management		
Firmware Management		
Utilities		
Device Connector		
		Refearb Meet Dennes Loursch of OAL Diss CIMC Debrast Locates LED #
Chassis +	nent 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
Compute		🛞 Settings 📿 Refrest
Networking +	ACCESS MODE ALLOW CONTROL	Device ID
Storage +		li de la companya de
Admin 🗸	••••••	•••••• 🔿
User Management	Internet	Intersight
Networking		
Communication Services		
Security Management		
Event Management	a successful, but device is still not claimed. To claim the device open Cisco Intersight, create a new ac pevice for existing account.	count and follow the guidance or Open Intersight
Firmware Management		
Utilities		
Device Connector		

Etapa 3.1. Navegue até Admin > Device Connector > Settings > DNS Configuration e configurar o DNS Server e selecione Save como mostrado nesta imagem.

Admin / Device Connector *

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 DNS settings for IMC Software		
NTP Configuration			
Proxy Configuration	Domain Name	©	
Certificate Manager	DNS Server		
Connection		• +	
			Cancel

Etapa 3.2. Navegue até Admin > Device Connector > Settings > NTP Configuration. Configurar o NTP Server por ambiente e selecione Save como mostrado nesta imagem.

n / Admin / Device	e Connector *		Refresh Host Power Launch vKVM Ping CIMC Reboot Locator LED					
he Device Connector is an emb	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 NTP settings for IMC Software							
NTP Configuration	NTP Server							
Proxy Configuration		0	+					
Certificate Manager								
Connection				Cancel Save				

Etapa 3.3. Configure opcionalmente um proxy, se necessário, para acessar a Cisco Intersight. Navegue até Admin > Device Connector > Settings > Proxy Configuration > Enable Proxy. Configurar o Proxy Hostname/IP e o Proxy Port e selecione Save.

ings			
neral			
S Configuration	Configure proxy settings		
Configuration	C Enable Proxy		
cy Configuration	Proxy Hostname/IP *	Proxy Port *	<u></u>
lificate Manager			1 - 6553
nection	Authentication		

Etapa 4. Selecione Admin > Device Connector e copiar o Device ID e Claim Code. Copie ambos em um bloco de notas ou arquivo de texto para uso posterior.

	Services Cisco Integrated Management Contr	+ V2
Chassis	A / Admin / Device Refres Connector ★	n 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 based manage Help Center	ment platform. For detailed information about configuring the device connector, please visit
Networking +	Device Connector	③ Settings 〇 Refresh
Storage	ACCESS MORE ALLOW CONTROL	Device ID
Admin •	□	
Networking Communication Services	Device Connector Internet	Intersight
Security Management	Not Claimed	
Event Management	The connection to the Cisco Intersight Portal is successful, but device is still not claimed. To claim the device open Cisco Intersight, account and follow the guidance or go to the Targets page and click Claim a New Device for existing account.	create a new Open Intersight
Utilities	10.11-2299	
Device Connector		

Etapa 5. Inicie o Cisco Intersight e navegue até Admin > Targets > Claim a New Target > Cisco UCS Server (Standalone) > Start. Digite o Device ID e Claim Code que foi copiado da GUI do CIMC e selecione Claim.

Ξ	cisco Intersight	ADMIN > Targets	ධ 🖸 🤤 🧿 James Delli Paoli 🧕
<u>00o</u>	MONITOR		Claim a New Target
ø	OPERATE ^		
	Servers	+ All Targets 0 +	
	Chassis		U v per page ™ ⊆ V or U ≥ 20
ţ,	Fabric Interconnects	Connection X Top Targe X Vendor	
	HyperFlex Clusters	NO DATA AVAILABLE NO TYPES NO DATA AVAILABLE	
×	CONFIGURE ^		
	Profiles	Name Status	Type Target ID Claimed Time Claimed By Product ID
	Policies		
	Pools		
Q	ADMIN ^		K C 0 to 0 D
	Targets		
≡	cisco Intersight	ADMIN > Targets > Claim a New Target	📮 🔽 🔍 🕝 James Delli Paoli 🖉
<u>08o</u>	MONITOR		
Ø	OPERATE ^		Select Target Type
	Servers	Filters	Q. Search
	Chassis		
	Fabric Interconnects	Available for Claiming	Compute / Fabric
	HyperFlex Clusters	Categories	Clico LICS Server Clico All Comain Clico All Comain (LICS)
×	CONFIGURE ^	All	(Intersight Managed) Managed
	Profiles	Cloud	¢ ¢
	Policies	Hyperconverged	Cisco UCS C890
	Pools	Network	Hedtish Server
ģ	ADMIN ^	Orchestrator	Platform Services
	Targets	Platform Services	
			Cisco Intersight Appliance Cisco Intersight Assist Intersight Workload Engine
			Cloud
			Siart

	cisco Intersigh	t	ADMIN > Targets > C	laim a New Target		٩	ß ď	o o	James Delli Pa	ioli <u>&</u>
<u>⊪</u> ⊛	MONITOR OPERATE			Ę	Claim (Stand To claim y	Cisco UCS Server alone) Target our target, provide the De	vice ID, Claim			
	Chassis				Code and	select the appropriate Re	source Groups.			
	Fabric Interconnects		General							
	HyperFlex Clusters		Device ID *	Claim Co	ide *				0	
×	CONFIGURE		1079							
	Profiles		Resource Groups							
	Policies		O Select the	Resource Groups if required. How	wever, this selection is no	It mandatory as one or mo	are Resource Group t	pe is 'All'. The claimed t	irget will	
	Pools		be part of a	Il Organizations with the Resour	rce Group type 'All'.					
Q	ADMIN	^				0 items found	10 v per pag	e K K 0 of 0 5 [
	Targets		Name			Usage	Det	cription		
								K () (f0 [5] [5]	•
_			C Bank	Cased					Claim	_

Etapa 6. Navegue até Admin > Targets. Uma reivindicação bem-sucedida mostra o Status > Connected, como mostrado nesta imagem.

	cisco Intersight	ADMIN > Targets Q 🖬 1 🛛 🖓	🗿 🕥 James Dell Paol 🖉
<u>allo</u>	MONIFOR		Claim a New Target
Ø	OPERATE ^	★ All Tangets ⊙ +	
	Servers	C Equal 1 Americana	19 ✓ perpage (K < <u>1</u> of 1 ⊃ Э
	Fabric Interconnects	Connection 2 Top Targets by Types 2 Vendor	Ø
	HyperFlex Clusters	1 * Backlane MB have 1 1 * Data Systems Inc. 1	
×	CONFIGURE ^	Name Status Type Target D Clubmed Time Clubmed By	Product ID
	Policies	Connected Standatore MS Server Connected Standatore MS Server	
	Pools		
ছ	ADMIN ^		
	Targeta		

Verificação básica para problemas de declaração do dispositivo

Note: Para obter uma lista abrangente de Condições de erro e correções, consulte este link: <u>Condições de erro do conector do dispositivo e Etapas de correção.</u>

Descrições de Status de Conexão do Conector de Dispositivo	Explicações de Status de Conexão do Conector de Dispositivo	Possíveis correções
Reivindicado	A conexão com a plataforma Cisco Intersight foi bem-sucedida e você solicitou a conexão.	N/A

Não reivindicado Administrativamente desabilitado	A conexão com a plataforma Cisco Intersight foi bem-sucedida, mas o endpoint ainda não foi reivindicado. Indica que o Gerenciamento de Intersight/Conector do Dispositivo foi desabilitado no ponto de	Você pode solicitar uma conex não solicitada pela Cisco Inters Ative o conector do dispositivo endpoint.
DNS configurado incorretamente	O DNS foi configurado incorretamente no CIMC ou não foi configurado.	Indica que nenhum dos servido de nome DNS configurados no sistema está acessível. Verifiq você inseriu endereços IP válio para os servidores de nome D Verifique este link para ver se
Erro de Resolução DNS de Intersight	O DNS está configurado, mas não é possível resolver o nome DNS da Intersight.	Intersight esta passando por manutenção: <u>Status de Intersig</u> Se a Intersight estiver operació isso provavelmente indica que nome DNS do serviço de Intersi não foi resolvido. Verifique e confirme: O MTU e
Erro de rede do UCS Connect	Indica as configurações de rede inválidas.	correto de ponta a ponta, as po 443 e 80 são permitidas, o Fire permite que todos os IPs físico virtuais, DNS e NTP sejam configurados no endpoint. Certificado expirado ou ainda r válido: Verifique se o NTP está configurado corretamente e se hora do dispositivo está sincronizada com o Tempo Universal Coordenado. Verifiqu o DNS está configurado corretamente. Se um proxy da transparente estiver em uso, verifique se o certificado não expirou. O nome do certificado apresen
Erro de validação de certificado	O endpoint se recusa a estabelecer uma conexão com a plataforma Cisco Intersight porque o certificado apresentado pela plataforma Cisco Intersight é inválido.	pelo servidor Web não corresp ao nome DNS do serviço de Intersight: Verifique se o DNS configurado corretamente. Ent contato com o administrador de proxy da Web para verificar se proxy da Web transparente est configurado corretamente. Especificamente, o nome do certificado apresentado pelo pel da Web deve corresponder ao nome DNS do serviço Intersigh (svc.intersight.com). O certificado foi emitido por un Autoridade de Certificação (CA confiável: Verifique se o DNS e

configurado corretamente. Ent contato com o administrador d Web ou o infosec para verifica proxy da Web transparente es configurado corretamente. Especificamente, o nome do certificado apresentado pelo p da Web deve corresponder ao nome DNS do serviço de Inter

Requisitos gerais de conectividade de rede da Cisco Intersight

- Uma conexão de rede com a plataforma Intersight é estabelecida a partir do conector do dispositivo no endpoint
- Verifique se um firewall foi introduzido entre o destino gerenciado e a Intersight ou se as regras de um firewall atual foram alteradas. Isso pode causar problemas de conexão fim-a-fim entre o endpoint e a Cisco Intersight. Se as regras forem alteradas, verifique se as regras alteradas permitem o tráfego pelo firewall.
- Se você usar um proxy HTTP para rotear o tráfego para fora das suas instalações e tiver feito alterações na configuração do servidor proxy HTTP, certifique-se de alterar a configuração do conector de dispositivo para refletir as alterações. Isso é necessário porque o Intersight não detecta automaticamente servidores proxy HTTP.
- Configure DNS e resolva o nome DNS. O Conector do Dispositivo deve ser capaz de enviar solicitações DNS a um servidor DNS e resolver registros DNS. O Conector do Dispositivo deve ser capaz de resolver svc.intersight.com para um endereço IP.
- Configure o NTP e valide se a hora do dispositivo está sincronizada corretamente com um servidor de hora.

Note: Para obter uma lista abrangente de Requisitos de Conectividade da Intersight, consulte <u>Requisitos de Conectividade de Rede da Intersight.</u>

Informações Relacionadas

- Metas da reivindicação do Cisco Intersight Getting Started
- <u>Sistemas Cisco Intersight SaaS suportados</u>
- PIDs compatíveis com Cisco Intersight SaaS
- Requisitos de conectividade da Cisco Intersight Network
- <u>Vídeos de treinamento do Cisco Intersight</u>
- ID de bug da Cisco <u>CSCvw76806</u> Um servidor autônomo C-Series pode falhar ao solicitar com êxito no Cisco Intersight se a versão do seu conector de dispositivo for inferior a 1.0.9.
- <u>Suporte Técnico e Documentação Cisco Systems</u>

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.