Guia de instalação do dispositivo Cisco Digital Network Architecture Center, versão 1.2.10 (chassi M4)

Primeira publicação: 2019-01-29

Última modificação: 2019-02-21

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

AS ESPECIFICAÇÕES E INFORMAÇÕES COM RELAÇÃO AOS PRODUTOS DESTE MANUAL ESTÃO SUJEITAS A ALTERAÇÕES SEM PRÉVIO AVISO. ACREDITA-SE QUE TODAS AS DECLARAÇÕES, INFORMAÇÕES E RECOMENDAÇÕES DESCRITAS NESTE MANUAL SEJAM VERDADEIRAS, MAS ELAS ESTÃO SENDO AQUI APRESENTADAS SEM GARANTIAS DE NENHUM TIPO, SEJAM EXPRESSAS OU IMPLÍCITAS. OS USUÁRIOS SÃO TOTALMENTE RESPONSÁVEIS PELA APLICAÇÃO DE QUALQUER UM DESTES PRODUTOS.

A LICENÇA DE SOFTWARE E A GARANTIA LIMITADA QUE ACOMPANHAM O PRODUTO ESTÃO DEFINIDAS NO PACOTE DE INFORMAÇÕES ENVIADO COM O PRODUTO, SENDO AQUI INCORPORADAS ATRAVÉS DESTA MENÇÃO. SE VOCÊ NÃO CONSEGUIR LOCALIZAR A LICENÇA DE SOFTWARE OU A GARANTIA LIMITADA, ENTRE EM CONTATO COM O REPRESENTANTE DA CISCO PARA SOLICITAR UMA CÓPIA.

A implementação da compactação de cabeçalho TCP pela Cisco é uma adaptação de um programa desenvolvido pela Universidade da Califórnia, Berkeley (UCB), como parte da versão de domínio público da UCB do sistema operacional UNIX. Todos os direitos reservados. Copyright © 1981, Membros da Universidade da Califórnia.

INDEPENDENTEMENTE DE QUALQUER OUTRA GARANTIA AQUI INCORPORADA, TODOS OS ARQUIVOS DE DOCUMENTOS E SOFTWARES DESSES FORNECEDORES SÃO FORNECIDOS "NO ESTADO EM QUE SE ENCONTRAM", COM TODAS AS FALHAS. A CISCO E OS FORNECEDORES ACIMA MENCIONADOS SE ISENTAM DE TODAS AS GARANTIAS, EXPRESSAS OU IMPLÍCITAS, INCLUINDO, SEM LIMITAÇÃO, AS GARANTIAS DE COMERCIABILIDADE, ADEQUAÇÃO A UM DETERMINADO OBJETIVO E NÃO VIOLAÇÃO OU ORIUNDAS DE UM CURSO DE NEGOCIAÇÃO, USO OU PRÁTICA COMERCIAL.

EM HIPÓTESE ALGUMA, A CISCO OU SEUS FORNECEDORES SE RESPONSABILIZARÃO POR DANOS INDIRETOS, ESPECIAIS OU INCIDENTAIS, INCLUINDO, SEM LIMITAÇÃO, LUCROS CESSANTES, PERDA OU DANOS AOS DADOS DECORRENTES DO USO OU DA INABILIDADE DE USO DESTE MANUAL, MESMO QUE A CISCO OU SEUS FORNECEDORES TENHAM SIDO AVISADOS SOBRE A POSSIBILIDADE DE TAIS DANOS.

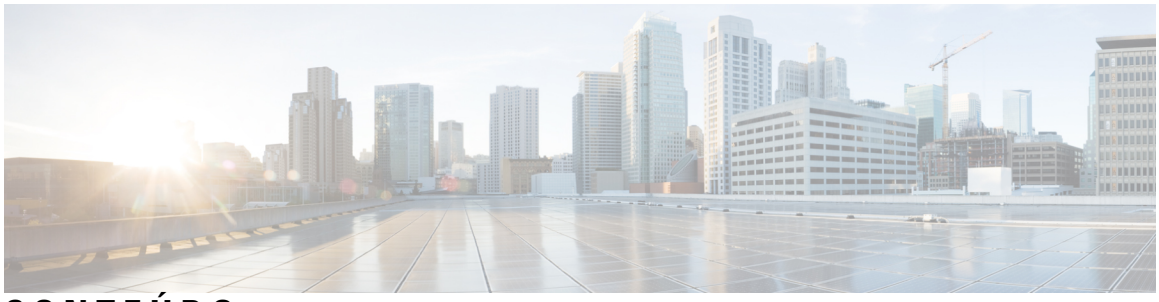
Os endereços IP (Internet Protocol) e números de telefone usados neste documento não pretendem ser endereços e números de telefone reais. Os exemplos, as saídas de exibição de comandos, os diagramas de topologias de rede e as figuras incluídas no documento são mostrados somente para fins ilustrativos. O uso de endereços IP ou números de telefone reais no conteúdo ilustrativo não é intencional e deve ser considerado uma coincidência.

Todas as cópias impressas e as duplicatas digitais deste documento são consideradas cópias sobre as quais não temos controle. Consulte a versão on-line atual para obter a versão mais recente.

A Cisco possui mais de 200 escritórios em todo o mundo. Os endereços, números de telefone e fax estão disponíveis no site www.cisco.com/go/offices.

Cisco e o logotipo da Cisco são marcas comerciais ou marcas comerciais registradas da Cisco e/ou suas afiliadas nos EUA e em outros países. Para exibir uma lista de marcas comerciais da Cisco, acesse este URL: www.cisco.com go trademarks. Todas as marcas de terceiros citadas pertencem a seus respectivos detentores. O uso do termo "parceiro" não implica uma relação de sociedade entre a Cisco e qualquer outra empresa. (1721R)

© 2019 Cisco Systems, Inc. Todos os direitos reservados.



CONTEÚDO

CAPÍTULO 1 **Revisar os recursos do dispositivo** 1

Resumo de recursos 1

Painéis frontal e traseiro 2

Especificações físicas 9

Especificações ambientais 9

Especificações de alimentação 10

CAPÍTULO 2 **Planejar a implantação** 13

Planejamento de fluxo de trabalho 13

Sobre Cisco DNA Center e Software-Defined Access 14

Conexões de cabo de interface 15

Sub-redes necessárias e endereços IP adicionais 17

Ordem de nomes de interface e configuração do assistente 20

URLs de Internet necessárias e nomes de domínio totalmente qualificados 21

Fornecer acesso seguro à Internet 22

Portas de rede obrigatórias 23

Portas e protocolos do SD-Access obrigatórios 25

Informações de configuração obrigatórias 33

Informações obrigatórias na primeira configuração 34

CAPÍTULO 3 **Instalar o dispositivo** 37

Fluxo de trabalho de instalação do dispositivo 37

Desempacotar e inspecionar o dispositivo 38

Revisar os avisos e as diretrizes de instalação 39

Analisar os requisitos do rack 40

Conectar e ligar o dispositivo 40

Verificar os LEDs 41

CAPÍTULO 4 **Configurar o dispositivo 45**

Fluxo de trabalho de configuração do dispositivo 45

Ativar acesso do navegador ao CIMC 46

Executar verificações preliminares 51

Verifique a imagem ISO de Cisco DNA Center 58

Criar uma unidade USB Bootable 59

Refazer a imagem do dispositivo 60

Instalar a imagem ISO do Cisco DNA Center 62

Configurar o nó mestre 62

Configurar os nós complementares 76

Cenários de implantação do cluster de alta disponibilidade 91

Nova implantação de HA 91

Implantação de HA atual do nó mestre com configurações de interface padrão 91

Implantação atual do nó mestre com configurações de interface fora do padrão 92

Considerações adicionais da implantação de HA 92

Telemetria 92

Controlador sem fio 93

Atualização para a versão Cisco DNA Center mais recente 93

CAPÍTULO 5 **Conclua a primeira configuração 95**

Fluxo de trabalho de primeira configuração 95

Navegadores compatíveis 96

Fazer login pela primeira vez 96

Integração do Cisco ISE com Cisco DNA Center 105

Configurar os servidores de autenticação e política 107

Configurar propriedades de SNMP 108

Redistribuir serviços 109

CAPÍTULO 6 **Soluções de problema da implantação 111**

Tarefas de identificação e solução de problemas 111

Logout 111

Reconfigurar o dispositivo usando o assistente de configuração 112

Reinicializar o dispositivo 113

CAPÍTULO 1

Revisar os recursos do dispositivo

- Resumo de recursos, na página 1
- Painéis frontal e traseiro, na página 2
- Especificações físicas, na página 9
- Especificações ambientais, na página 9
- Especificações de alimentação, na página 10

Resumo de recursos

A Cisco fornece Cisco DNA Center na forma de um dispositivo montável em rack (número de peça da Cisco DN1-HW-APL). O dispositivo consiste em um chassi Cisco UCS C220 M4, com a adição de uma placa de interface virtual (VIC) 1227 no slot mLOM. A imagem de software Cisco DNA Center é previamente instalada no dispositivo, mas deve ser configurada para uso.

A tabela a seguir resume os recursos do dispositivo.

Tabela 1: Cisco DNA Center Recursos de série de dispositivo

Recurso	Descrição
Chassis	Chassi de uma unidade de rack (1RU).
Processadores	Até duas CPUs da família de processadores Intel Xeon CPU E5-2699 2.20 GHz v4 Series.
Memória	24 slots para DIMMs registrados (RDIMMs) ou DIMMs de carga reduzida (LRDIMMs) (12 para cada CPU).
Armazenamento	Oito unidades de estado sólido (SSDs) de tamanho pequeno (SFF) de 2,5 polegadas.
Gerenciamento de Disco (RAID)	Três configurações RAID pré-configuradas: RAID 1 nos slots 1 e 2, RAID 1 nos slots 3 e 4 e RAID 10 nos slots 5, 6, 7 e 8. Essas configurações não são feitas pelo usuário.

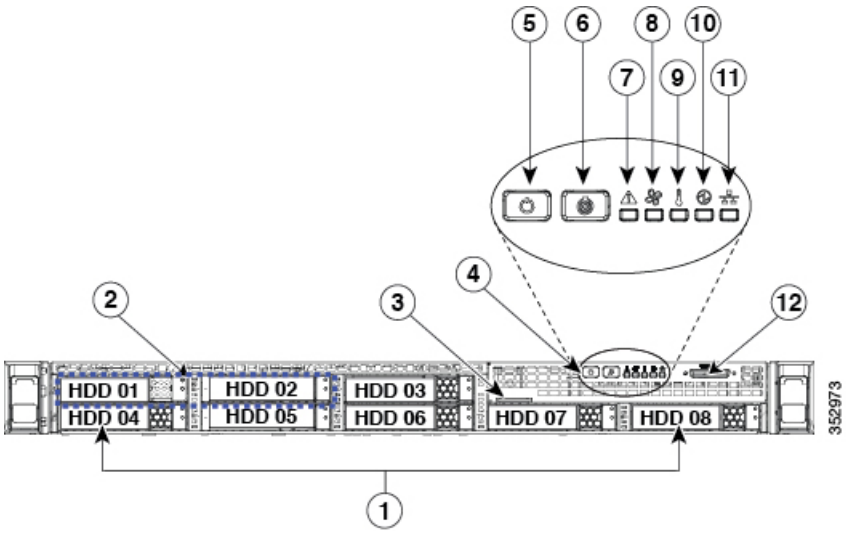
Recurso	Descrição
I/O de gerenciamento e de rede	Conectores compatíveis: • Duas portas Ethernet de 10 Gbps na placa de interface virtual Cisco UCS (VIC) 1227 • Uma porta de gerenciamento dedicada 1 Gbps • Duas portas de LAN 1 Gbps BASE-T Ethernet Os seguintes conectores estão disponíveis, mas não são usados com frequência na operação diária de Cisco DNA Center: • Uma porta serial RS-232 (conector RJ-45) • Um conector VGA2 de 15 pinos • Dois conectores USB 3.0 • Um conector KVM com painel frontal, usado com o cabo KVM, que forneça dois conectores USB 2.0, um VGA e um serial (DB-9).
Alimentação	Fontes de alimentação CA dual de 770 W cada. Não combine diferentes tipos de fonte de alimentação ou classificações de tensões no servidor. Redundantes, como a dupla (1+1).
Refrigeração	Seis módulos de ventilador com hot swap (troca a quente) para viabilizar a refrigeração frontal e traseira.
Vídeo	Resolução de vídeo VGA até 1920 x 1200, 16 bpp a 60 Hz e até 256 MB de memória de vídeo.

Painéis frontal e traseiro

As figuras e tabelas a seguir descrevem os painéis frontal e traseiro do dispositivo Cisco DNA Center com o chassi do Cisco UCS C220 M4.

Clique neste link para obter um vídeo breve que descreva os painéis frontal e traseiro do dispositivo e como as placas de rede são cabeadas.

Figura 1: Painel frontal do dispositivo



Componente	Descrição
1	Oito unidades SDD de 2,5 polegadas. Cada compartimento de unidade instalado tem um LED de falha e um LED de atividade. Quando o LED de falha da unidade está: • Desligado — a unidade está funcionando corretamente. • Âmbar — a unidade falhou. • Âmbar, piscando — a unidade está sendo recriada. Quando o LED de atividade da unidade está: • Desligado — não há unidade no SLED (sem acesso, sem falha). • Verde — a unidade está pronta. • Verde, piscando — a unidade está lendo ou gravando dados.
2	Os compartimentos de unidade 1 e 2 são compatíveis com as unidades de estado sólido (SSDs) SAS/SATA e NVMe PCIe. Os LEDs de falha e atividade e os estados são os mesmos que os das unidades de SDD de 2,5 polegadas instaladas.
3	Tag removível do recurso
4	LEDs e botões do subpainel de operações. Os estados dos LEDs para esses botões e as condições que eles indicam são descritos nas entradas a seguir.

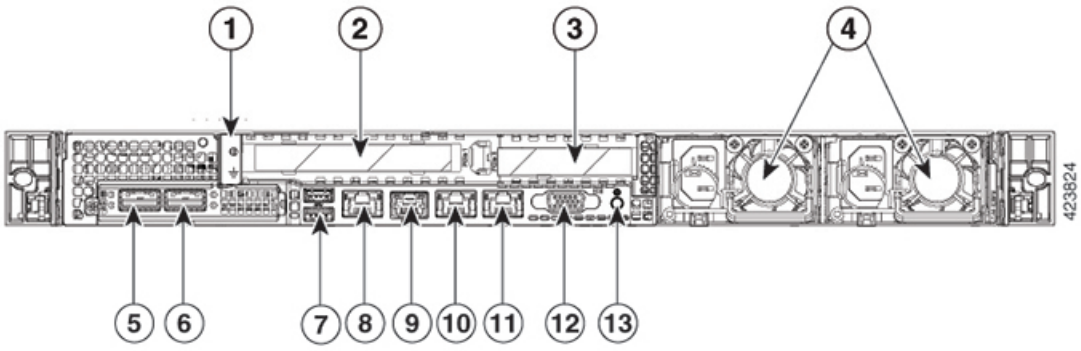
Componente	Descrição
5	Botão de energia/LED de status de energia. Quando o LED está: • Desligado — não há energia CA para o dispositivo. • Âmbar — o dispositivo está no modo de energia de standby. A energia é fornecida apenas para o CIMC e algumas funções da placa-mãe. • Verde — o dispositivo está no modo de energia principal. A energia é fornecida para todos os componentes do servidor.
6	Botão e LED de identificação da unidade. Quando o LED está: • Azul – a identificação da unidade está ativa. • Desligado — a identificação da unidade está inativa.

7	LED de status do sistema. Quando o LED está:
	• Verde — o dispositivo está sendo executado em uma condição de operação normal.
	• Verde, piscando — o dispositivo está executando verificações de memória e inicialização do sistema.
	• Âmbar, estável — o dispositivo está em um estado operacional degradado, o que pode ocorrer devido a uma ou mais das seguintes causas:
	  • A redundância da fonte de alimentação foi perdida.
	  • As CPUs não correspondem.
	  • Pelo menos uma CPU está com defeito.
	  • Pelo menos um DIMM está com defeito.
	  • Pelo menos uma unidade em uma configuração de RAID falhou.
	• Âmbar, piscando — o dispositivo está em um estado de falha grave, o que pode ocorrer devido a uma ou mais das seguintes causas:
	  • Falha na inicialização.
	  • Foi detectado um erro fatal de CPU e/ou barramento.
	  • O servidor está em uma condição de temperatura excessiva.

8	LED de status do ventilador. Quando o LED está: • Verde — todos os módulos de ventilação estão operando corretamente. • Âmbar, estável — um módulo de ventilação falhou. • Âmbar, piscando — falha grave, dois ou mais módulos de ventilação falharam.

Componente	Descrição
9	LED de status da temperatura. Quando o LED está: • Verde — o dispositivo está operando em temperatura normal. • Âmbar, estável — um ou mais sensores de temperatura excedeu um limite de aviso. • Âmbar, piscando — um ou mais sensores de temperatura excedeu um limite essencial
10	LED de status da fonte de alimentação. Quando o LED está: • Verde: todas as fontes de alimentação estão funcionando normalmente. • Âmbar, estável: uma ou mais fontes de alimentação estão em um estado operacional degradado. • Âmbar, piscando: uma ou mais fontes de alimentação estão em um estado de falha grave.
11	LED de atividade do link de rede. Quando o LED está: • Verde, piscando: uma ou mais portas Ethernet LOM são ativadas pelo link, com atividade. • Verde: uma ou mais portas Ethernet LOM são ativadas pelo link, mas não há atividade. • Desligado: o link Ethernet está ocioso.
12	Conector KVM. Usado com cabo KVM que forneça dois conectores USB 2.0, um VGA e um serial.

Figura 2: Painel traseiro do dispositivo



Componente	Descrição
1	Orifício para suporte de aterramento (para fontes de alimentação CC)
2	PCIe riser 1/slot 1
3	PCIe riser 2/slot 2

Componente	Descrição
4	Fontes de alimentação (até duas; redundantes, como 1+1). Cada fonte de alimentação tem um LED de falha da fonte de alimentação e um LED de energia CA. Quando o LED de falha está: • Desligado — a fonte de alimentação está funcionando normalmente. • Âmbar, piscando — um limite de aviso de evento foi atingido, mas a fonte de alimentação continua a operar. • Âmbar, estável — um limite de falha grave foi atingido, fazendo com que a fonte de alimentação seja desligada (por exemplo, uma falha de ventilação ou uma condição de aquecimento excessivo). Quando o LED de energia CA está: • Verde, estável — a energia CA está OK, a saída CC está OK. • Verde, piscando — a energia CA está OK, a saída CC não está ativada. • Desligado — não há energia CA para a fonte de alimentação. Para obter mais detalhes, consulte Especificações de alimentação.
5	**Porta de cluster de 10 Gbps (Porta 2, enp10s0, adaptador de rede 1)**: esta é a segunda porta de 10 Gbps na placa de interface virtual da Cisco (VIC) 1227 no slot mLOM do equipamento. O painel traseiro rotula a **Porta 2** e o Assistente de configuração do Maglev o identifica como **Enp10s0** e **Adaptador de rede 1**. Conecte essa porta a um switch com conexões a outros nós no cluster Cisco DNA Center. Essa porta tem um LED de status de link ("ACT") e um LED de velocidade de link ("LINK"). Quando o LED de status do link está: • Verde, piscando — o tráfego está presente no link ativo. • Verde — o link está ativo, mas não há tráfego presente. • Desligado — nenhum link está presente. Quando o LED de velocidade do link está: • Verde — a velocidade do link é de 10 Gbps. • Âmbar — a velocidade do link é de 1 Gbps. • Desligado — a velocidade do link é de 100 Mbps ou menos. **Observação** As portas corporativa e de cluster devem operar apenas em 10 Gbps.

Componente	Descrição
6	**Porta corporativa de 10 Gbps (Porta 1, enp9s0, adaptador de rede 4)**: esta é a primeira porta de 10 Gbps na placa de interface virtual da Cisco (VIC) 1227 no slot mLOM do equipamento. O painel traseiro rotula como **Porta 1** e o Assistente de configuração do Maglev o identifica como **enp9s0** e **Adaptador de rede 4**. Conecte esta porta a um switch com alcance IP para o equipamento de rede que Cisco DNA Center vai gerenciar. Essa porta tem um LED de status de link ("ACT") e um LED de velocidade de link ("LINK"). Quando o LED de status do link está: • Verde, piscando — o tráfego está presente no link ativo. • Verde — o link está ativo, mas não há tráfego presente. • Desligado — nenhum link está presente. Quando o LED de velocidade está: • Verde — a velocidade do link é de 10 Gbps. • Âmbar — a velocidade do link é de 1 Gbps. • Desligado — a velocidade do link é de 100 Mbps ou menos. **Observação** As portas corporativa e de cluster do dispositivo Cisco DNA Center devem operar apenas em 10 Gbps.
7	Portas USB 3.0 (duas)
8	**Porta CIMC de 1 Gbps (M)**: esta é a porta incorporada à direita das duas portas USB e à esquerda da porta serial RJ45. O painel traseiro rotula como **M** e você atribui um endereço IP a ele quando ativa o acesso do navegador à GUI CIMC do dispositivo (consulte Ativar acesso do navegador ao CIMC). Essa porta está reservada para o gerenciamento fora da banda (OOB) do chassi e do software do dispositivo Cisco DNA Center. Conecte-a a um switch que forneça acesso à rede de gerenciamento empresarial OOB dedicada. Essa porta tem um LED de status de link e um LED de velocidade de link. Quando o LED de status do link está: • Verde, piscando — o tráfego está presente no link ativo. • Verde — o link está ativo, mas não há tráfego presente. • Desligado — nenhum link está presente. Quando o LED de velocidade está: • Verde — a velocidade do link é de 1 Gbps. • Âmbar — a velocidade do link é de 100 Mbps. • Desativado — a velocidade do link é de 10 Mbps ou menos.
9	Porta serial (conector RJ-45)

Componente	Descrição
10	**1 Gbps Cisco DNA Center Porta de interface de usuário (1, enp1s0f0, Adaptador de rede 2)**: esta é a primeira porta de controlador Ethernet de 1 GB Intel i350. Ela é integrada à placa-mãe do dispositivo. O painel traseiro rotula como **1** e o Assistente de configuração do Maglev identifica como **enp1s0f0** e **Adaptador de rede 2**. Conecte-a a um switch que forneça acesso à rede de gerenciamento empresarial dedicada. Essa porta tem um LED de status de link e um LED de velocidade de link. Quando o LED de status está: • Verde, piscando — o tráfego está presente no link ativo. • Verde — o link está ativo, mas não há tráfego presente. • Desligado — nenhum link está presente. Quando o LED de velocidade está: • Verde — a velocidade do link é de 1 Gbps. • Âmbar — a velocidade do link é de 100 Mbps. • Desativado — a velocidade do link é de 10 Mbps ou menos.
11	**Porta de nuvem de 1 Gbps (2, enp1s0f1, Adaptador de rede 3)**: esta é a segunda porta de controlador Ethernet de 1 Gbps incorporada. O painel traseiro rotula como **2** e o Assistente de configuração do Maglev identifica como **enp1s0f1** e **Adaptador de rede 3**. Essa porta é opcional. Ela é usada para conectar-se à Internet quando não é possível fazer isso através da **porta de 10 Gbps corporativa** (porta 1, enp9s0, Adaptador de rede 4). Essa porta tem um LED de status de link e um LED de velocidade de link. Quando o LED de status do link está: • Verde, piscando — o tráfego está presente no link ativo. • Verde — o link está ativo, mas não há tráfego. • Desligado — nenhum link está presente. Quando o LED de velocidade está: • Verde — a velocidade do link é de 1 Gbps. • Âmbar — a velocidade do link é de 100 Mbps. • Desativado — a velocidade do link é de 10 Mbps ou menos.
12	Porta de vídeo VGA (DB-15). A área de painel em torno dessa porta é azul.
13	Botão localizador de LED azul

Especificações físicas

A tabela a seguir lista as especificações físicas para o dispositivo.

Tabela 2: Especificações físicas

Descrição	Especificação
Altura	4,32 cm (1,7 pol.)
Largura	43,0 cm (16,89 pol.) Incluindo alças: 48,2 cm (18,98 pol.)
Profundidade (comprimento)	75,6 cm (29,8 pol.) Incluindo alças: 78,7 cm (30,98 pol.)
Espaço frontal	76 mm (3 pol.)
Espaço livre lateral	25 mm (1 pol.)
Espaço livre traseiro	152 mm (6 pol.)
Peso máximo (chassi totalmente carregado)	17,2 kg (37,9 lb.)

Especificações ambientais

A tabela a seguir lista as especificações ambientais para o dispositivo.

Tabela 3: Especificações ambientais

Descrição	Especificação
Temperatura, operacional	5 a 35°C (41 a 95°F) Reduza a temperatura máxima em 1°C para cada 305 m (1.000 pés) de altitude acima do nível do mar.
Temperatura, não operacional (quando o dispositivo é armazenado ou transportado)	–40 a 149°F (–40 a 65°C)
Umidade (UR), operacional	10% a 90%, sem condensação a 28°C (82°F)
Umidade, não operacional	5% a 93% a 28°C (82°F)
Altitude, operacional	0 a 3.000 m (0 a 10.000 pés)

Descrição	Especificação
Altitude, não operacional (quando o dispositivo é armazenado ou transportado)	0 a 12.192 m (0 a 40.000 pés)
Nível de energia sonora, medida ponderada em A de acordo com ISO7779 LwAd (dBA), operação em 23°C (73°F)	5,4
Nível de pressão sonora, medida ponderada em A de acordo com ISO7779 LpAm (dBA), operação em 23°C (73°F)	37

Especificações de alimentação

As especificações da fonte de alimentação Dual 770 W CA (Número de peça da Cisco UCSC-PSU1-770W) fornecida com o dispositivo estão listadas na tabela abaixo.

⚠

Cuidado Não combine diferentes tipos de fonte de alimentação no dispositivo. Ambas as fontes de alimentação devem ser idênticas.

Tabela 4: Especificações da fonte de alimentação CA

Descrição	Especificação
Tensão de entrada CA	Intervalo nominal: 100–120 VCA, 200–240 VCA (Intervalo: 90 – 132 VCA, 180 – 264 VCA)
Frequência de entrada CA	Intervalo nominal: 50 a 60 Hz (Intervalo: 47 a 63 Hz)
Corrente CA máxima de entrada	9,5 A a 100 VCA 4,5 A a 208 VCA
Volt-ampères de entrada, no máximo	950 VA a 100 VCA
Potência máxima de saída por PSU	770 W
Corrente máxima de entrada	15 A (duração do subciclo)
Tempo máximo de retenção	12 MS a 770 W
Tensão de saída da fonte de alimentação	12 VCC
Tensão de standby da fonte de alimentação	12 VCC
Classificação de eficiência	Economizadores de clima de eficiência Platinum (80Plus Platinum certificado)

Descrição	Especificação
Tamanho	RSP2
Conector de entrada	IEC320 C14

Você pode obter informações de energia mais específicas para a configuração exata do dispositivo usando a Calculadora de Potência Cisco UCS: http://ucspowercalc.cisco.com

CAPÍTULO 2

Planejar a implantação

- Planejamento de fluxo de trabalho, na página 13
- Sobre Cisco DNA Center e Software-Defined Access, na página 14
- Conexões de cabo de interface, na página 15
- Sub-redes necessárias e endereços IP adicionais, na página 17
- URLs de Internet necessárias e nomes de domínio totalmente qualificados, na página 21
- Fornecer acesso seguro à Internet, na página 22
- Portas de rede obrigatórias, na página 23
- Portas e protocolos do SD-Access obrigatórios, na página 25
- Informações de configuração obrigatórias, na página 33
- Informações obrigatórias na primeira configuração, na página 34

Planejamento de fluxo de trabalho

A tabela a seguir detalha as tarefas de planejamento e a coleta de informações que você deve executar, antes de tentar instalar, configurar e montar os dispositivos. Ao concluir as tarefas desta tabela, você pode continuar instalando fisicamente os dispositivos no data center.

Clique neste link para obter uma série de vídeos que oferece uma visão geral do Cisco DNA Center em relação ao processo de instalação e configuração.

Para obter mais informações, Sobre Cisco DNA Center e Software-Defined Access.

Tabela 5: Tarefas de planejamento

Etapa	Descrição
1	Revise os requisitos de cabeamento e switching recomendados para instalações autônomas e de clusters: Conexões de cabo de interface.
2	Colete o endereçamento IP, a divisão em sub-redes e outras informações de tráfego IP que serão aplicadas durante a configuração do aplicativo: Sub-redes necessárias e endereços IP adicionais.
3	Prepare uma solução para o acesso necessário a recursos na Web: URLs de Internet necessárias e nomes de domínio totalmente qualificados e Fornecer acesso seguro à Internet.

Etapa	Descrição
4	Reconfigure os firewalls e as políticas de segurança para o tráfego de Cisco DNA Center: Portas de rede obrigatórias. Se estiver usando Cisco DNA Center para gerenciar uma rede de SDA, consulte também Portas e protocolos do SD-Access obrigatórios.
5	Colete informações adicionais usadas durante a configuração da aplicação e a configuração inicial: Informações de configuração obrigatórias e Informações obrigatórias na primeira configuração.

Sobre Cisco DNA Center e Software-Defined Access

Você pode usar Cisco DNA Center para gerenciar qualquer tipo de rede, incluindo redes que empregam a arquitetura de malha de acesso definida por software da Cisco (também conhecida como SD-Access ou SDA). A revolucionária abordagem de SDA transforma as redes convencionais em redes baseadas em intenção, nas quais a lógica de negócios se torna uma parte física da rede, o que facilita a automatização das tarefas diárias, como configuração, provisionamento e solução de problemas. A solução de SD-Access da Cisco reduz o tempo necessário para adaptar a rede às necessidades da empresa, aprimora as resoluções de problemas e reduz os impactos na violação de segurança.

Uma discussão completa da solução SDA está fora do escopo deste guia. Arquitetos e administradores de rede que planejam implementar uma arquitetura de malha de SDA para uso com Cisco DNA Center podem encontrar informações adicionais e orientações dos seguintes recursos:

- Para obter uma breve introdução ao SDA e ao Cisco Digital Network Architecture, consulte o white paper A visão do Cisco Digital Network Architecture – uma visão geral.
- Para obter mais informações sobe como o Cisco DNA Center utiliza o SD-Access para automatizar soluções que não são possíveis com abordagens e técnicas normais de rede, consulte Software-Defined Access: ativação de redes baseadas em intenção.
- Para designs validados que demonstram como implementar o SDA na rede, consulte a versão mais recente do Guia de design do Software-Defined Access da Cisco.
- Para obter orientação sobre como usar a segmentação de acesso SDA para melhorar a segurança de rede, consulte o Guia de design de segmentação do Software-Defined Access.
- Para obter orientações de design específicas sem fio, consulte o Guia de design e implantação sem fio de acesso SD.
- Para obter orientações sobre como implantar o SDA com o Cisco DNA Center, consulte o Guia de implantação do Software-Defined Access.
- Para obter mais informações sobre a Digital Network Architecture, que é a base de Cisco DNA Center e a solução SDA, e as funções de outros produtos e soluções da Cisco e de terceiros nessa arquitetura inovadora, consulte a Cisco DNA Design Zone.
- Para obter outros guias de design, guias de implantação e white papers, consulte a Zona de design da Cisco.

Conexões de cabo de interface

Conecte as portas no dispositivo aos switches que fornecem os seguintes tipos de acesso à rede. No mínimo, você deve configurar as interfaces corporativas e de porta de cluster, pois elas são necessárias para a funcionalidade de Cisco DNA Center.

- **(Obrigatório) Porta de cluster de 10 Gbps (Porta 2, enp10so, adaptador de rede 1)**: esta é a porta esquerda na placa VIC 1227 no slot mLOM do equipamento. A finalidade é habilitar as comunicações entre os nós mestre e complementares em um cluster de Cisco DNA Center. Conecte essa porta a um switch com conexões a outros nós no cluster e configure um endereço IP com máscara de sub-rede para a porta.

  Durante a configuração, o assistente de configuração do Maglev não permite prosseguir até que você atribua a opção de link de cluster a uma interface. Recomendamos que você atribua a porta enp10so como o link de cluster. No entanto, tenha em mente que a interface marcada como link de cluster não pode ser alterada após a conclusão da configuração. Se você precisar alterar posteriormente a interface marcada como o link de cluster, uma reinstalação será necessária. Com isso em mente, recomendamos a configuração da porta de cluster com um endereço IP, para permitir a expansão para um cluster de três nós no futuro. Além disso, certifique-se de que a interface de link de cluster esteja conectada a uma porta de switch no estado ativo.

- **(Opcional) Porta de interface de usuário de 1 Gbps de Cisco DNA Center (1, Enp1s0f0, adaptador de rede 2)**: esta porta fornece acesso à interface gráfica do usuário de Cisco DNA Center. A finalidade é permitir que os usuários usem o software no dispositivo. Conecte essa porta a um switch com conexões à rede de gerenciamento empresarial e configure um endereço IP com máscara de sub-rede para a porta.

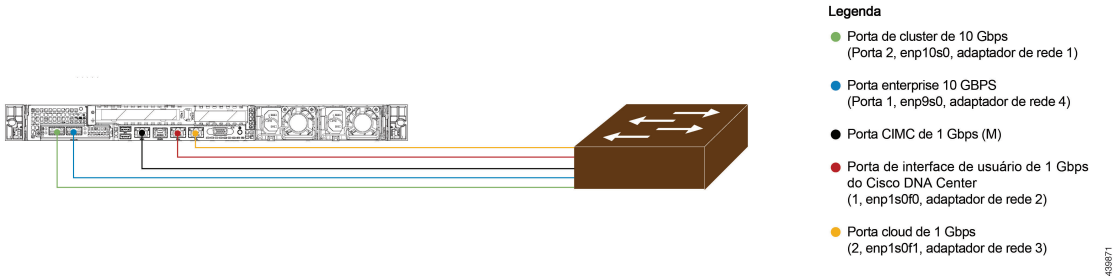
- **(Opcional) Porta de nuvem de 1 Gbps (2, enp1s0f1, adaptador de rede 3)**: essa porta é opcional. Use-a somente se não for possível conectar o dispositivo à Internet (incluindo o servidor proxy da Internet) com a porta empresarial de 10 Gbps (porta 1, enp9s0, adaptador de rede 4). Se você precisar usar a porta de nuvem, conecte essa porta a um switch com conexões ao servidor de proxy de Internet e configure um endereço IP com máscara de sub-rede para a porta.

- **(Obrigatório) Porta empresarial de 10 Gbps (porta 1, enp9s0, adaptador de rede 4)**: esta é a porta direita na placa VIC 1227 no slot mLOM do dispositivo. A finalidade é habilitar Cisco DNA Center para comunicação e gerenciamento da rede. Conecte essa porta a um switch com conexões à rede empresarial e configure um endereço IP com máscara de sub-rede para a porta.

- **(Opcional, mas altamente recomendável) Porta CIMC de 1 Gbps (M)**: essa porta fornece acesso ao navegador para a interface de gerenciamento de dispositivos fora de banda do CIMC e interface gráfica de usuário. A finalidade é permitir que você gerencie o dispositivo e o hardware. Conecte essa porta a um switch com conexões à rede de gerenciamento empresarial e configure um endereço IP com máscara de sub-rede para a porta.

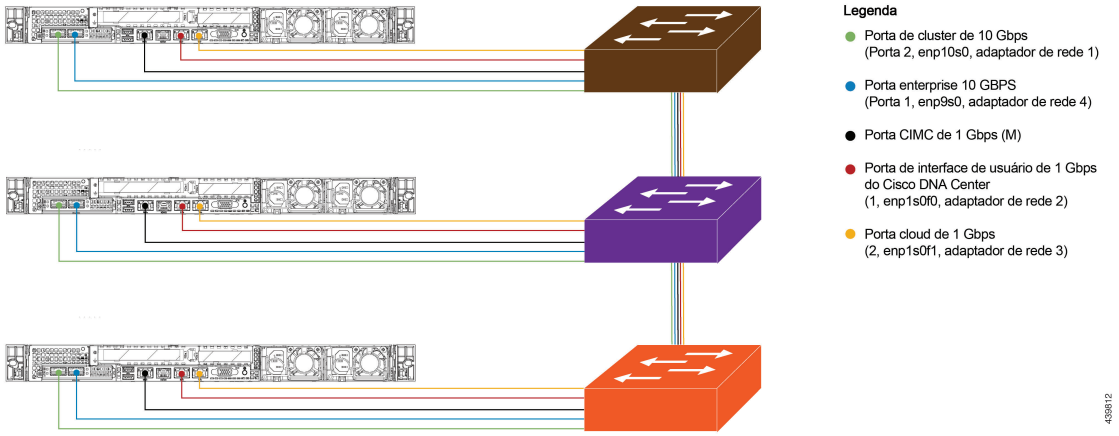
A figura a seguir mostra as conexões recomendadas para um cluster do Cisco DNA Center de nó único:

Figura 3: Cabeamento recomendado para cluster de nó único



A figura a seguir mostra as conexões recomendadas para um cluster do Cisco DNA Center de três nós: Todas as conexões, exceto uma, das conexões para cada nó no cluster de três nós são as mesmas do cluster de nó único e usam as mesmas portas. A exceção é a porta de cluster (porta 2, enp10so, adaptador de rede 1), necessária para que cada host no cluster de três nós possa se comunicar com os outros.

Figura 4: Cabeamento recomendado para o cluster de três nós



Para ver uma breve apresentação de vídeo sobre as portas do painel traseiro e como elas são usadas, consulte os primeiros cinco minutos de Desembalagem do dispositivo do Cisco DNA Center para Assurance e SD-Access (na seção "Comece agora mesmo").

Para obter mais detalhes sobre cada uma das portas, consulte o diagrama do painel traseiro e as descrições que acompanham o chassi do Cisco UCS C220 M4 nos Painéis frontal e traseiro.

Observação As implantações de cluster de vários nós exigem que todos os nós de membros estejam na mesma rede e no mesmo local. O dispositivo não oferece suporte à distribuição de nós em várias redes ou locais.

Ao cabear as portas corporativa e de cluster de 10 Gbps, observe que ambas as portas são compatíveis com os seguintes tipos de mídia:

- FP-10G-USR (Intervalo ultracurto, MMF)
- SFP-10G-SR (intervalo curto, MMF)
- SFP-10G-LR (intervalo longo, SMF)
- 10GBASE-CU SFP+, Cabo de 1 metro

- 10GBASE-CU SFP+ Cabo de 3 metros
- 10GBASE-CU SFP+, Cabo de 5 metros
- 10GBASE-CU SFP+, Cabo de 7 metros
- SFP-10GB-ACU, Cabo de 7 metros

Sub-redes necessárias e endereços IP adicionais

Antes de iniciar a instalação, você deve garantir que a rede tenha endereços IP suficientes disponíveis para atribuir a cada uma das portas de dispositivo que você planeja usar. Se você estiver instalando o dispositivo como um cluster de nó único ou como um nó de inclusão ou mestre em um cluster de três nós, precisará dos seguintes endereços de porta de dispositivo (NIC):

- **Endereço de porta empresarial (obrigatório)**: um endereço IP com máscara de sub-rede.
- **Endereço de porta de cluster (obrigatório)**: um endereço IP com máscara de sub-rede.
- **Endereço de porta de gerenciamento (opcional)**: um endereço IP com máscara de sub-rede.
- **Endereço de porta na nuvem (opcional)**: um endereço IP com máscara de sub-rede. Essa é uma porta opcional, usada somente quando você não consegue se conectar à nuvem usando a porta empresarial. Você não precisa de um endereço IP para a porta de nuvem, a menos que tenha que usá-lo para essa finalidade.
- **Endereço de porta de CIMC (opcional, mas altamente recomendável)**: um endereço IP com máscara de sub-rede.

Observação Todos os endereços IP chamados para esses requisitos devem ser endereços IPv4 físicos válidos com máscaras de rede IPv4 válidas. Certifique-se de que os endereços e as sub-redes correspondentes não se sobreponham. Poderá haver problemas de comunicação de serviço se isso acontecer.

Você também precisará dos seguintes endereços IP adicionais e de sub-redes IP dedicadas, que são solicitados e aplicados durante a configuração do dispositivo:

1. **Endereços IP virtuais do cluster**: um endereço IP virtual (VIP) por interface de rede configurada por cluster. Esse requisito se aplica a clusters de três nós e clusters de nó único que provavelmente serão convertidos em um cluster de três nós no futuro. Você deve fornecer um VIP para cada interface de rede configurada. Cada VIP deve ser da mesma sub-rede que o endereço IP da interface configurada correspondente. Há quatro interfaces em cada dispositivo: empresarial, cluster, gerenciamento e nuvem. No mínimo, você deve configurar as interfaces corporativas e de porta de cluster, pois elas são necessárias para a funcionalidade do Cisco DNA Center. Uma interface será considerada configurada se ela tiver um IP, juntamente com uma máscara de sub-rede e um ou mais gateways ou rotas estáticas associadas. Se você ignorar uma interface totalmente durante a configuração, ela será considerada não configurada.

   Observe o seguinte:

   - Se você tiver uma configuração de um único nó e não planeja convertê-la em um cluster de três nós no futuro, não será necessário especificar um endereço IP virtual. No entanto, se decidir fazer isso, especifique um endereço IP virtual para cada interface de rede configurada (da mesma forma que faria para um cluster de três nós).

- Se o link interno de um cluster de nó único ficar inativo, os endereços IP virtuais associados às interfaces de gerenciamento e corporativa também ficarão inativos. Quando isso acontece, Cisco DNA Center é inutilizável até que o link do cluster interno seja restaurado (pois a integração de SWIN e ISE não será operacional e os dados do Assurance não serão exibidos, já que as informações não poderão ser recolhidas de coletores NDP).

2. **Endereço IP do gateway padrão**: o endereço IP para o gateway padrão preferido da rede. Se nenhuma outra rota corresponder ao tráfego, o tráfego será roteado através desse endereço IP. Normalmente, você deve atribuir o gateway padrão à interface na configuração de rede que acessa a Internet. Para obter informações sobre considerações de segurança ao implantar o Cisco DNA Center, consulte o Guia de melhores práticas de segurança do Cisco Digital Network Architecture Center.
3. **Endereços IP do servidor DNS**: o endereço IP de um ou mais dos servidores DNS preferenciais da rede. Durante a configuração, você pode especificar vários endereços IP do servidor DNS e as máscaras de sub-rede, inserindo-os como uma lista separada por espaços.
4. **(Opcional) endereços de rotas estáticas**: os endereços IP, as máscaras de sub-rede e os gateways para uma ou mais rotas estáticas. Durante a configuração, você pode especificar vários endereços IP de rotas estáticas, máscaras de rede e gateways, inserindo-os como uma lista separada por espaços.

   Você pode definir uma ou mais rotas estáticas para qualquer interface no dispositivo. Você deve fornecer rotas estáticas quando quiser rotear o tráfego em uma direção específica diferente do gateway padrão. Cada uma das interfaces com rotas estáticas será definida como o *dispositivo* através do qual o tráfego será roteado na tabela de comando de roteamento de IP. Por esse motivo, é importante associar as direções da rota estática à interface através da qual o tráfego será enviado.

   As rotas estáticas não são recomendadas em tabelas de roteamento de dispositivos de rede, como aquelas usadas por switches e roteadores. Os protocolos de roteamento dinâmico são melhores para isso. No entanto, você deve adicioná-los onde necessário, para permitir que o dispositivo acesse partes específicas da rede que podem não ser mais convenientes.
5. **Endereços IP do servidor NTP**: o nome de host de DNS resolvível ou o endereço IP para pelo menos um servidor NTP (Network Time Protocol).

   Durante a configuração, você pode especificar vários IPs/máscaras de servidor NTP ou nomes de host, inserindo-os como uma lista separada por espaços. Para uma implantação de produção, recomendamos que você configure um mínimo de três servidores NTP.

   Você especificará esses servidores durante a sincronização de hardware antes da simulação e, novamente, durante a configuração do software em cada dispositivo no cluster. A sincronização de tempo é fundamental para a precisão dos dados e coordenação de processamento em um cluster de vários hosts. Antes de implantar o dispositivo na produção, certifique-se de que o horário no relógio do sistema do dispositivo seja atual e que os servidores NTP (Network Time Protocol) especificados estejam com o horário preciso. Se você estiver planejando integrar o dispositivo com Cisco Identity Services Engine (ISE), também deverá garantir que o ISE esteja sincronizando com os mesmos servidores NTP que o dispositivo.
6. **Sub-rede de serviços**: identifica uma sub-rede IP dedicada para o dispositivo usar no gerenciamento e na obtenção de IPS para comunicações entre os serviços de aplicações internas, como Assurance, coleta de inventário e assim por diante. A sub-rede de serviços IPv4 dedicados não deve entrar em conflito com ou se sobrepor a qualquer outra sub-rede usada pela rede interna do Cisco DNA Center ou qualquer rede externa. O tamanho mínimo da sub-rede é de 21 bits. A sub-rede de serviços IPv4 deve estar de acordo com as especificações IETF RFC 1918 e RFC 6598 para redes privadas, que são compatíveis com os seguintes intervalos de endereços:

   - 10.0.0.0/8

- 172.16.0.0/12
- 192.168.0.0/16
- 100.64.0.0/10

Para obter detalhes, consulte a RFC 1918, a Alocação de endereços para Internets privadas e a RFC 6598, Prefixo IPv4 de IANA-preservado para espaço de endereço compartilhado.

Importante

- Certifique-se de especificar uma sub-rede CIDR válida. Caso contrário, os bits incorretos estarão presentes nas sub-redes 172.17.1.0/20 e 172.17.61.0/20.
- Depois que a configuração do dispositivo Cisco DNA Center for concluída, você não poderá atribuir uma sub-rede diferente sem primeiro fazer a nova imagem do dispositivo (consulte o tópico "Nova imagem do dispositivo" no capítulo "Configurar o dispositivo" para obter mais informações).

7. **Sub-rede de serviços de cluster**: identifica uma sub-rede IP dedicada para o dispositivo usar no gerenciamento e na obtenção de IPS para comunicações entre os serviços de infraestrutura, como o acesso ao banco de dados, o barramento de mensagem e assim por diante. A sub-rede de serviços de cluster de IPv4 dedicados não deve entrar em conflito com ou se sobrepor a qualquer outra sub-rede usada pela rede interna do Cisco DNA Center ou qualquer rede externa. O tamanho mínimo da sub-rede é de 21 bits. A sub-rede de serviços de cluster IPv4 deve estar de acordo com as especificações IETF RFC 1918 e RFC 6598 para redes privadas, que são compatíveis com os seguintes intervalos de endereços:
   - 10.0.0.0/8
   - 172.16.0.0/12
   - 192.168.0.0/16
   - 100.64.0.0/10

   Para obter detalhes, consulte a RFC 1918, a Alocação de endereços para Internets privadas e a RFC 6598, Previxo IPv4 de IANA-preservado para espaço de endereço compartilhado.

   Se fosse necessário especificar 10.10.10.0/21 como a sub-rede de serviços, você também poderia especificar uma sub-rede de serviços de cluster de 10.0.8.0/21, pois essas duas sub-redes não se sobrepõem. Observe também que o assistente de configuração detecta sobreposições (se houver) entre essas sub-redes e solicita que você as corrija.

Importante

- Certifique-se de especificar uma sub-rede CIDR válida. Caso contrário, os bits incorretos estarão presentes nas sub-redes 172.17.1.0/20 e 172.17.61.0/20.
- Depois que a configuração do dispositivo Cisco DNA Center for concluída, você não poderá atribuir uma sub-rede diferente sem primeiro fazer a nova imagem do dispositivo (consulte o tópico "Nova imagem do dispositivo" no capítulo "Configurar o dispositivo" para obter mais informações).

O espaço de endereço IP total recomendado para os dois serviços e sub-redes de serviços de cluster contém 4.096 endereços, divididos em duas/21 sub-redes de 2.048 endereços cada. As duas/21 sub-redes não devem se sobrepor. Os serviços internos do Cisco DNA Center precisam de um conjunto dedicado de endereços IP

para operar (uma exigência da arquitetura de microsserviço do Cisco DNA Center). Para acomodar esse requisito, você deve alocar duas sub-redes dedicadas por sistema de Cisco DNA Center.

Um motivo pelo qual o dispositivo exige essa quantidade de espaço de endereço é manter o desempenho do sistema. Como ele usa as tecnologias internas de roteamento e tunelamento para as comunicações lado a lado (entre nós), a utilização de espaços de endereço sobrepostos forçaria o dispositivo a executar internamente os FIBs de roteamento e encaminhamento virtual. Isso levaria a vários encapsulamentos/desencapsulamentos para pacotes que passam de um serviço para outro, causando alta latência interna em um nível muito baixo, com impactos em cascata em camadas mais altas.

Outro motivo é a arquitetura de contêinerização de serviços baseada em kubernetes do Cisco DNA Center. Cada dispositivo usa os endereços IP nesse espaço por nó de kubernetes K8. Vários nós podem fazer um único serviço. No momento, Cisco DNA Center é compatível com mais de 100 serviços, cada um exigindo vários endereços IP, e novos recursos e serviços correspondentes são adicionados o tempo todo. O requisito de espaço de endereço é, por fim, mantido em grande parte no início para garantir que a Cisco possa adicionar novos serviços e recursos sem esgotar os IPs ou sem exigir que os clientes realoquem os espaços de endereço contíguos simplesmente para atualizar os sistemas.

Os serviços compatíveis nessas sub-redes também são ativados na camada 3. O espaço de serviços de cluster, em particular, transporta dados entre os serviços de aplicação e infraestrutura e é muito usado.

A exigência RFC 1918 e RFC 6598 é devido à necessidade de o Cisco DNA Center baixar pacotes e atualizações da nuvem. Se os intervalos de IP selecionados não estiverem em conformidade com a RFC 1918 e a RFC 6598, isso poderá causar problemas rapidamente com sobreposições de IP público.

Ordem de nomes de interface e configuração do assistente

Os nomes de interface e a ordem em que essas interfaces estão configuradas no assistente de configuração do Maglev são diferentes para os modelos de chassi M4 e M5 do dispositivo Cisco DNA Center, conforme ilustrado na tabela a seguir:

Tabela 6: Ordem de nomes de interface e configuração do assistente

Função	Cisco DNA Center Modelo do chassi da aplicação	Nome da interface	Ordem de configuração no assistente de configuração do Maglev
Cluster: vincula o dispositivo aos nós de cluster.	**M4**	**enp10s0**	**Adaptador de rede 1**
	M5	enp94s0f1	Adaptador de rede 4
Gerenciamento: permite que você acesse a interface do usuário de Cisco DNA Center da rede de gerenciamento.	**M4**	**enp1s0f0**	**Adaptador de rede 2**
	M5	eno1	Adaptador de rede 1
Nuvem: fornece acesso à Internet quando outra interface não está disponível para essa finalidade.	**M4**	**enp1s0f1**	**Adaptador de rede 3**
	M5	eno2	Adaptador de rede 2

Função	Cisco DNA Center Modelo do chassi da aplicação	Nome da interface	Ordem de configuração no assistente de configuração do Maglev
Empresarial: vincula o dispositivo à rede empresarial.	**M4**	**enp9s0**	**Adaptador de rede 4**
	M5	enp94s0f0	Adaptador de rede 3

URLs de Internet necessárias e nomes de domínio totalmente qualificados

O dispositivo requer acesso seguro à seguinte tabela de URLs e nomes de domínio totalmente qualificados (FQDNs).

A tabela descreve os recursos que usam cada URL e FQDN. Você deve configurar o firewall de rede ou um servidor proxy para que o tráfego IP possa sair e entrar do dispositivo e desses recursos. Se você não puder fornecer esse acesso em nenhuma URL e nenhum FQDN listado, os recursos associados ficarão prejudicados ou inoperáveis.

Para obter mais informações sobre os requisitos de acesso de proxy à Internet, consulte Fornecer acesso seguro à Internet.

Tabela 7: Acesso necessário às URLs e ao FQDN

Para...	... Cisco DNA Center deve acessar as URLs e os FQDNs a seguir
Baixe atualizações para o sistema e o software do pacote de aplicações, envie feedback do usuário para a equipe do produto.	Recomendado: *.ciscoconnectdna.com:443[1] Os clientes que desejam evitar curingas podem especificar estas URLs: • https://www.ciscoconnectdna.com • https://cdn.ciscoconnectdna.com • https://registry.ciscoconnectdna.com • https://registry-cdn.ciscoconnectdna.com
Cisco DNA Center atualizar pacote	https://*.ciscoconnectdna.com/* https://*.cloudfront.net/ https://maglev-catalog-1.s3.amazonaws.com https://maglev-catalogstaging.s3.amazonaws.com
Downloads de Software Smart Account e SWIM	https://apx.cisco.com https://cloudsso.cisco.com/as/token.oauth2 https://*.cisco.com/*
Feedback do usuário	https://dnacenter.uservoice.com

Para...	... Cisco DNA Center deve acessar as URLs e os FQDNs a seguir
Integre-se com Cisco Meraki.	Recomendado: *.meraki.com:443 Os clientes que desejam evitar curingas podem especificar essas URLs: • dashboard.meraki.com:443 • api.meraki.com:443 • n63.meraki.com:443
Integre com o Cisco.com e o Cisco Smart Licensing.	*.cisco.com:443 Os clientes que desejam evitar curingas podem especificar essas URLs: • software.cisco.com • cloudsso.cisco.com • cloudsso1.cisco.com • cloudsso2.cisco.com • apiconsole.cisco.com • api.cisco.com • apx.cisco.com • sso.cisco.com • apmx-prod1-vip.cisco.com • apmx-prod2-vip.cisco.com
Processe informações precisas no local e nos mapas de local.	• www.mapbox.com • *.tiles.mapbox.com/* :443. Para um proxy, o destino é *.tiles.mapbox.com/*

[1] A Cisco é proprietária e mantém ciscoconnectdna.com e os subdomínios. A infraestrutura do Cisco Connect DNA atende às diretrizes de segurança e confiança da Cisco e passa por testes contínuos de segurança. Essa infraestrutura é eficaz, com recursos integrados de balanceamento de carga e automação, e é monitorada e mantida por uma equipe de operações em nuvem para garantir a disponibilidade contínua.

Fornecer acesso seguro à Internet

Por padrão, o dispositivo é configurado para acessar o Cisco.com e outras URLs via Internet, para baixar atualizações de software, licenças e software de dispositivo, além de fornecer informações de mapa atualizadas, comentários do usuário e assim por diante.

Fornecer conexões com a Internet para esses fins é um requisito obrigatório.

Usar um servidor proxy HTTPS é uma maneira confiável de acessar URLs remotas com segurança. Recomendamos que você use um servidor proxy HTTPS para fornecer ao dispositivo o acesso necessário às URLs listadas em URLs de Internet necessárias e nomes de domínio totalmente qualificados. Durante a instalação, você será solicitado a inserir a URL e o número da porta do servidor proxy que deseja usar para essa finalidade, juntamente com as credenciais de login do proxy (se o proxy exigir).

A partir desta versão, o dispositivo é compatível com a comunicação com servidores proxy apenas por HTTP. Você pode localizar o servidor proxy HTTPS em qualquer lugar na rede. O servidor proxy pode se comunicar com a Internet usando HTTPS, enquanto o dispositivo se comunica com o servidor proxy via HTTP. Por esses motivos, você vai querer especificar a porta HTTP do proxy ao configurar o proxy durante a configuração.

Se, por qualquer motivo, você precisar alterar a configuração de proxy após a configuração, é possível fazer isso por meio da interface de usuário.

Portas de rede obrigatórias

As tabelas a seguir listam as portas de serviço de rede conhecidas que são usadas pelos dispositivos. Você deve garantir que essas portas estejam abertas para que o tráfego entre e saia dos dispositivos, independentemente de abri-las por meio de configurações de firewall ou de um gateway de proxy.

Portas, protocolos e tipos de tráfego adicionais devem ser acomodados se você estiver implantando o dispositivo em uma rede que utiliza infraestrutura SDA. Para obter detalhes, consulte Portas e protocolos do SD-Access obrigatórios.

Observação Para obter informações sobre considerações de segurança ao implantar o Cisco DNA Center, consulte o Guia de melhores práticas de segurança do Cisco Digital Network Architecture Center.

Tabela 8: Portas: tráfego de entrada

Número da Porta	Tráfego permitido	Protocolo (TCP ou UDP)
2.222	SSH	TCP
80	HTTP	TCP
123	NTP	UDP
162	SNMP	UDP
443	HTTPS	TCP

Tabela 9: Portas: tráfego de saída

Número da Porta	Tráfego permitido	Protocolo (TCP ou UDP)
22	SSH (para os dispositivos de rede)	TCP
23	Telnet (para os dispositivos de rede)	TCP

Número da Porta	Tráfego permitido	Protocolo (TCP ou UDP)
53	DNS	UDP
80	A porta 80 pode ser usada para uma configuração de proxy de saída. Além disso, outras portas comuns, como 8080, também podem ser usadas quando um proxy está sendo configurado pelo assistente de configuração (se um proxy já estiver em uso na rede). Para acessar os certificados e pools de confiança compatíveis com a Cisco, você pode configurar a rede para permitir o tráfego IP de saída do dispositivo para os endereços Cisco na seguinte URL: https://www.cisco.com/security/pki/	TCP
123	NTP	UDP
161	Agente SNMP	UDP
443	HTTPS	TCP
5222	ISE XMP para PxGrid	TCP
9060	Tráfego de API ISE ERS	TCP

A tabela a seguir lista as portas que permitem o tráfego IP de entrada para o dispositivo:

Tabela 10: Portas: tráfego de IP

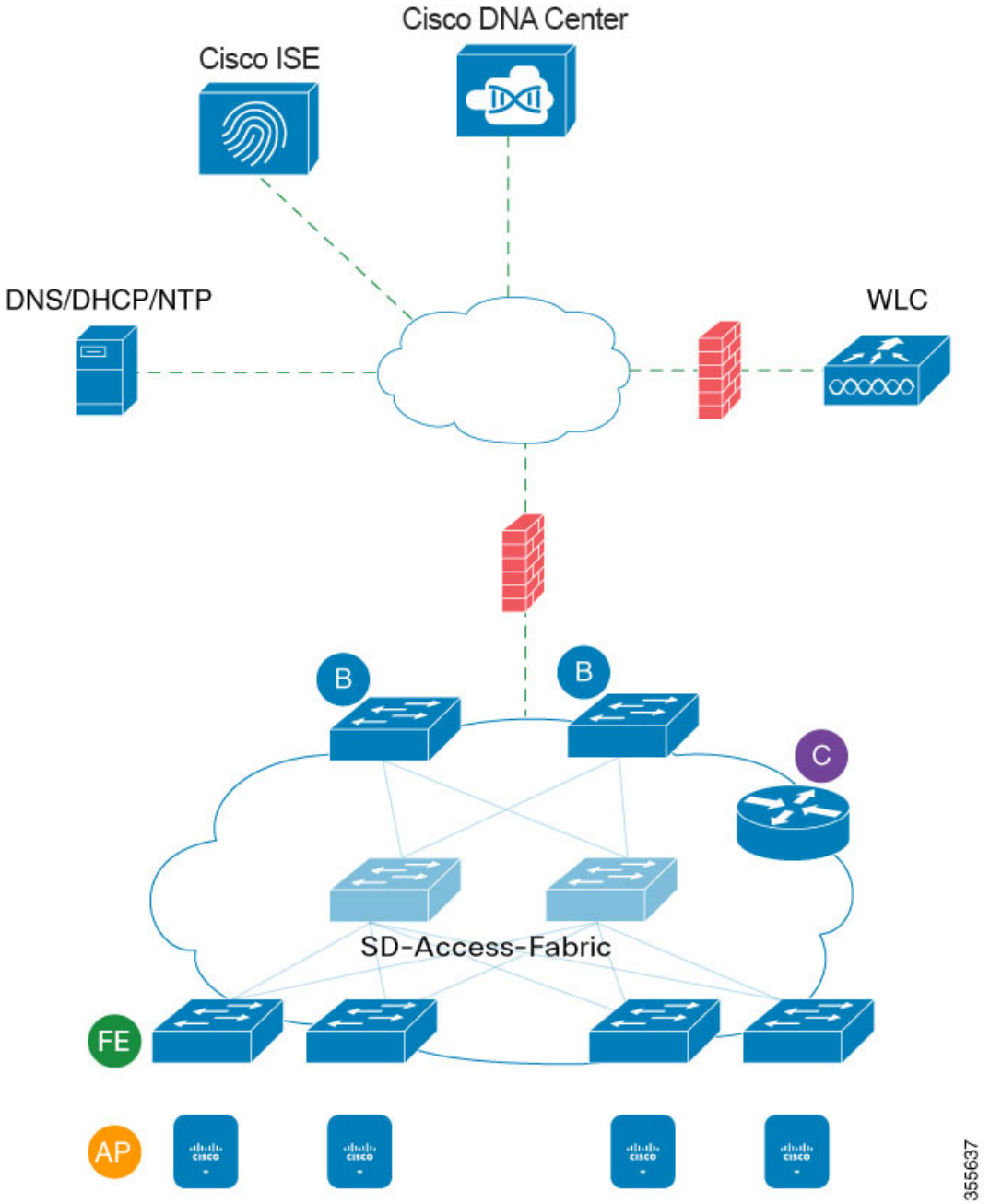
Protocolo (TCP ou UDP)	Número da Porta	Tipo de tráfego
TCP	22	SSH
TCP	2.222	SSH
TCP	80	HTTP
TCP	443	HTTPS
UDP	67	bootps
UDP	123	NTP
UDP	162	SNMP

Além disso, você pode configurar a rede para permitir o tráfego IP de saída do dispositivo para os endereços Cisco na seguinte URL: https://www.cisco.com/security/pki/. O dispositivo usa os endereços IP listados na URL acima para acessar os certificados compatíveis com a Cisco e os pools de confiança.

Portas e protocolos do SD-Access obrigatórios

Este tópico detalha as portas, os protocolos e os tipos de tráfego nativos em uma implantação de malha SDA típica, como mostra a figura abaixo.

Figura 5: Infraestrutura de malha SDA



Se você implementou o SDA na rede, use as informações nas tabelas a seguir para planejar as políticas de firewall e segurança que protegem corretamente a infraestrutura do SDA enquanto fornecem ao Cisco DNA Center o acesso necessário para automatizar o gerenciamento de rede.

Tabela 11: Cisco DNA Center Transito

Porta de origem[2]	Origem	Porta de destino	Destino	Descrição
Qualquer	Cisco DNA Center	UDP 53	Servidor DNS	De Cisco DNA Center para servidor DNS
Qualquer	Cisco DNA Center	TCP 22	Subjacência de malha	De Cisco DNA Center para os loopbacks dos switches de malha para SSH
Qualquer	Cisco DNA Center	TCP 23	Subjacência de malha	De Cisco DNA Center para os loopbacks de switches de malha para TELNET
Qualquer	Cisco DNA Center	UDP 161	Subjacência de malha	De Cisco DNA Center para os loopbacks de switches de malha para a descoberta de dispositivo SNMP
ICMP	Cisco DNA Center	ICMP	Subjacência de malha	De Cisco DNA Center para os loopbacks de switches de malha para a descoberta de dispositivo SNMP
Qualquer	Cisco DNA Center	TCP 443	Subjacência de malha	De Cisco DNA Center para switches de malha de atualizações de software (também para a Internet, se não houver proxy)
Qualquer	Cisco DNA Center	TCP 80	Subjacência de malha	De Cisco DNA Center para switches de malha de PnP (também para a Internet, se não houver proxy)
Qualquer	Cisco DNA Center	TCP 830	Subjacência de malha	De Cisco DNA Center para switches de malha de Netconf (SDA incorporado sem fio)
UDP 123	Cisco DNA Center	UDP 123	Subjacência de malha	De Cisco DNA Center para switches de malha de tempo inicial durante a automação de LAN
Qualquer	Cisco DNA Center	UDP 123	Servidor NTP	De Cisco DNA Center para o servidor NTP
Qualquer	Cisco DNA Center	TCP 22, UDP 161	WLC	De Cisco DNA Center para WLC
ICMP	Cisco DNA Center	ICMP	WLC	De Cisco DNA Center para WLC
Qualquer	Cisco DNA Center	TCP 80, TCP 443	AP	De Cisco DNA Center para AP como sensor e sensor ativo (Cisco Aironet 1800S)

Qualquer	Cisco DNA Center	TCP 32626	AP	De Cisco DNA Center para AP de gRPC

[2] O cluster, o PKI, o servidor SFTP e o tráfego de porta de proxy não estão incluídos nesta tabela.

Tabela 12: Tráfego de conectividade da Internet

Porta de origem	Origem	Porta de destino	Destino	Descrição
Qualquer	Cisco DNA Center	TCP 443	registry.ciscoconnectdna.com	Baixar atualizações de pacote do Cisco DNA Center
Qualquer	Cisco DNA Center	TCP 443	www.ciscoconnectdna.com	Baixar atualizações de pacote do Cisco DNA Center
Qualquer	Cisco DNA Center	TCP 443	registry-cdn.ciscoconnectdna.com	Baixar atualizações de pacote do Cisco DNA Center
Qualquer	Cisco DNA Center	TCP 443	cdn.ciscoconnectdna.com	Baixar atualizações de pacote do Cisco DNA Center
Qualquer	Cisco DNA Center	TCP 443	software.cisco.com	Baixar software do dispositivo
Qualquer	Cisco DNA Center	TCP 443	cloudsso.cisco.com	Validar credenciais de Cisco.com e Smart Account
Qualquer	Cisco DNA Center	TCP 443	cloudsso1.cisco.com	Validar credenciais de Cisco.com e Smart Account
Qualquer	Cisco DNA Center	TCP 443	cloudsso2.cisco.com	Validar credenciais de Cisco.com e Smart Account
Qualquer	Cisco DNA Center	TCP 443	apiconsole.cisco.com	API de Smart Licensing de CSSM
Qualquer	Cisco DNA Center	TCP 443	sso.cisco.com	CCO e Smart Licensing
Qualquer	Cisco DNA Center	TCP 443	api.cisco.com	CCO e Smart Licensing
Qualquer	Cisco DNA Center	TCP 443	apx.cisco.com	CCO e Smart Licensing
Qualquer	Cisco DNA Center	TCP 443	dashboard.meraki.com	Integração da Meraki
Qualquer	Cisco DNA Center	TCP 443	api.meraki.com	Integração da Meraki

Qualquer	Cisco DNA Center	TCP 443	n63.meraki.com	Integração da Meraki
Qualquer	Cisco DNA Center	TCP 443	dnacenter.uservoice.com	Envio de feedback do usuário
Qualquer	Cisco DNA Center Cliente admin	TCP 443	*.tiles.mapbox.com	Renderizar mapas no navegador (para acesso via proxy, o destino é *.tiles.mapbox.com/*)
Qualquer	Cisco DNA Center	TCP 443	www.mapbox.com	Identificação do código do país de mapas e WLC

Tabela 13: Tráfego subjacente de malha SDA

Porta de origem[3]	**Origem**	**Porta de destino**	**Destino**	**Descrição**
UDP 68	Subjacência de malha	UDP 67	servidor DHCP	De switches e roteadores de malha até o servidor DHCP para o pacote de relé de DHCP iniciado pelos nós da borda da malha.
Qualquer	Subjacência de malha	TCP 80	Cisco DNA Center	De switches de malha e roteadores IPs até Cisco DNA Center para PnP
Qualquer	Subjacência de malha	TCP 443	Cisco DNA Center	De switches de malha e roteadores IPs até Cisco DNA Center para atualização de imagem
Qualquer	Subjacência de malha	UDP 162	Cisco DNA Center	De switches de malha e roteadores IPs até Cisco DNA Center para interceptações de SNMP
Qualquer	Subjacência de malha	UDP 514	Cisco DNA Center	De switches e roteadores até Cisco DNA Center para Assurance
Qualquer	Subjacência de malha	UDP 6007	Cisco DNA Center	De roteadores de malha até Cisco DNA Center para NetFlow
Qualquer	Subjacência de malha	UDP 123	Cisco DNA Center	De switches de malha até Cisco DNA Center, para fazer automação de LAN
ICMP	Subjacência de malha	ICMP	Cisco DNA Center	De loopbacks de roteadores e switches de malha até Cisco DNA Center para SNMP: descoberta do dispositivo
UDP 161	Subjacência de malha	Qualquer	Cisco DNA Center	De switches de malha e loopbacks de roteadores até Cisco DNA Center para SNMP: descoberta de dispositivo

Qualquer	Subjacência de malha	UDP 53	Servidor DNS	De switches e roteadores de malha até o servidor DNS para resolução de nomes
TCP e UDP 4342	Subjacência de malha	TCP e UDP 4342	Roteadores e switches de malha	Mensagens de controle encapsuladas LISP
TCP e UDP 4342	Subjacência de malha	Qualquer	Roteadores e switches de malha	Comunicações de plano de controle LISP
Qualquer	Subjacência de malha	UDP 4789	Roteadores e switches de malha	Pacotes de dados encapsulados de malha (VXLAN-GPO)
Qualquer	Subjacência de malha	UDP 1645/1646/1812/1813	ISE	De switches de malha e roteadores de loopback IPs até ISE para RADIUS
ICMP	Subjacência de malha	ICMP	ISE	De switches de malha e roteadores até ISE para solução de problemas
UDP 1700/3799	Subjacência de malha	Qualquer	ISE	De switches de malha até ISE para COA
Qualquer	Subjacência de malha	UDP 123	Servidor NTP	De switches de malha e IPs de loopback de roteadores até o servidor NTP
Qualquer	control-plane	UDP e TCP 4342/4343	WLC	Do IP de loopback do plano de controle até WLC para conectividade sem fio habilitada para malha

[3] O protocolo de roteamento de fronteira, o span, a criação de perfil e o tráfego de telemetria não estão incluídos nesta tabela.

Tabela 14: Tráfego de Wireless LAN Controller (WLC)

Porta de origem	Origem	Porta de destino	Destino	Descrição
UDP 5246/5247/5248	WLC	Qualquer	Pool de IP do AP	De WLC até sub-rede de AP para CAPWAP
ICMP	WLC	ICMP	Pool de IP do AP	De WLC até APs, permitindo ping para solução de problemas
Qualquer	WLC	UDP 69/5246/5247 TCP 22	Pool de IP do AP	De WLC até sub-rede de AP para CAPWAP
Qualquer	WLC	UDP e TCP 4342/4343	Plano de controle	De WLC até IP de loopback do plano de controle

Qualquer	WLC	TCP 32222	Cisco DNA Center	De WLC até Cisco DNA Center para descoberta de dispositivos
UDP 161	WLC	Qualquer	Cisco DNA Center	Do WLC até Cisco DNA Center para SNMP
Qualquer	WLC	UDP 162	Cisco DNA Center	Do WLC até Cisco DNA Center para interceptações de SNMP
Qualquer	WLC	TCP 16113	MSE e Spectrum Expert	Do WLC até MSE e Spectrum Expert para NMSP
ICMP	WLC	ICMP	Cisco DNA Center	De WLC até permitir ping para solução de problemas
Qualquer	Servidor HA	TCP 1315	Cisco DNA Center	Servidor de banco de dados HA (QoS)
Qualquer	Servidor HA	TCP 1316 – 1320	Cisco DNA Center	Portas de banco de dados HA
Qualquer	Servidor Web HA	TCP 8082	Cisco DNA Center	Porta do monitoramento de integridade do servidor Web HA
Qualquer	WLC e vários servidores Syslog	UDP 514	WLC	Syslog (opcional)
Qualquer	WLC	UDP 53	Servidor DNS	Do WLC até o servidor DNS
Qualquer	WLC	TCP 443	ISE	Do WLC até ISE para autorização da Web de SSID de convidado
Qualquer	WLC	UDP 1645, 1812	ISE	Do WLC até ISE para autenticação RADIUS
Qualquer	WLC	UDP 1646, 1813	ISE	Do WLC até ISE para estatísticas do RADIUS
Qualquer	WLC	UDP 1700, 3799	ISE	Do WLC até ISE para CoA do RADIUS
ICMP	WLC	ICMP	ISE	Do WLC até ISE ICMP para solução de problemas
Qualquer	WLC	UDP 123	Servidor NTP	Do WLC até o servidor NTP

Tabela 15: Tráfego de pool de access point (AP) sem fio com malha ativada

Porta de origem	Origem	Porta de destino	Destino	Descrição
UDP 68	Pool de IP do AP	UDP 67	servidor DHCP	Do pool de IP do AP até o servidor DHCP
ICMP	Pool de IP do AP	ICMP	servidor DHCP	Do pool de IP do AP até o ICMP para solução de problemas

Qualquer	Pool de IP do AP	514	Vários	Syslog — o destino é configurável. O padrão é 255.255.255.255
Qualquer	Pool de IP do AP	UDP 69/5246/5247/5248	WLC	Do pool de IP do AP até WLC para CAPWAP
ICMP	Pool de IP do AP	ICMP	WLC	Do pool de IP do AP até WLC, permitindo o ping para solução de problemas

Tabela 16: Tráfego do Identity Services Engine (ISE)

Porta de origem[4]	**Origem**	**Porta de destino**	**Destino**	**Descrição**
Qualquer	ISE	TCP 64999	Borda	Do ISE até o nó de limite do SXP
Qualquer	ISE	UDP 514	Cisco DNA Center	Do ISE até servidor Syslog (Cisco DNA Center)
UDP 1645/1646/1812/1813	ISE	Qualquer	Subjacência de malha	Do ISE até os switches e roteadores de malha para RADIUS e autorização
Qualquer	ISE	UDP 1700/3799	Subjacência de malha	Do ISE até os switches de malha e os IPs de loopback de roteadores para care-of-address
ICMP	ISE	ICMP	Subjacência de malha	Do ISE até switches de malha para solução de problemas
Qualquer	ISE	UDP 123	Servidor NTP	Do ISE até o servidor NTP
UDP 1812/1645/1813/1646	ISE	Qualquer	WLC	Do ISE até WLC para RADIUS
ICMP	ISE	ICMP	WLC	Do ISE até WLC para solução de problemas

[4] Observação: o tráfego de alta disponibilidade e de criação de perfil não está incluído nesta tabela.

Tabela 17: Tráfego de servidor DHCP

Porta de origem	**Origem**	**Porta de destino**	**Destino**	**Descrição**
UDP 67	servidor DHCP	UDP 68	Pool de IP do AP	Do servidor DHCP para os APs de malha
ICMP	servidor DHCP	ICMP	Pool de IP do AP	ICMP para solução de problemas: malha até DHCP
UDP 67	servidor DHCP	UDP 68	Subjacência de malha	Do DHCP até switches e roteadores de malha
ICMP	servidor DHCP	ICMP	Subjacência de malha	ICMP para solução de problemas: malha até DHCP

UDP 67	servidor DHCP	UDP 68	Pool de IP do usuário	Do servidor DHCP até switches e roteadores de malha
ICMP	servidor DHCP	ICMP	Pool de IP do usuário	ICMP para solução de problemas: usuário para DHCP

Tabela 18: Tráfego do servidor NTP

Porta de origem	Origem	Porta de destino	Destino	Descrição
UDP 123	Servidor NTP	Qualquer	ISE	Do servidor NTP até ISE
UDP 123	Servidor NTP	Qualquer	Cisco DNA Center	Do servidor NTP até Cisco DNA Center
UDP 123	Servidor NTP	Qualquer	Subjacência de malha	Do servidor NTP até switches de malha e loopback de roteadores
UDP 123	Servidor NTP	Qualquer	WLC	Do servidor NTP até WLC

Tabela 19: Tráfego do servidor DNS

Porta de origem	Origem	Porta de destino	Destino	Descrição
UDP 53	Servidor DNS	Qualquer	Subjacência de malha	Do servidor DNS até os switches de malha
UDP 53	Servidor DNS	Qualquer	WLC	Do servidor DNS até WLC

Informações de configuração obrigatórias

Durante a configuração da aplicação, você será solicitado a fornecer as seguintes informações, além dos Sub-redes necessárias e endereços IP adicionais:

1. **Nome do usuário Linux**: é **`maglev`**. Esse nome de usuário é o mesmo em todos os dispositivos em um cluster, incluindo o nó mestre e os nós complementares, e não pode ser alterado.
2. **Senha do Linux**: identifica a senha para o nome de usuário do Linux **`maglev`**. Essa senha garante o acesso seguro a cada dispositivo através da linha de comando Linux. Se decidir fazer isso, você pode atribuir uma senha de Linux diferente para cada nome de usuário Linux **`maglev`** de cada dispositivo em um cluster.

   Crie a senha do Linux, visto que não há uma senha padrão. A senha deve atender aos seguintes requisitos:

   - Tamanho mínimo de oito caracteres.
   - NÃO conter espaço de TAB ou quebra de linha.
   - Conter caracteres de pelo menos três das seguintes categorias:

- Letra em caixa alta
- Letra em caixa baixa
- Numeral
- Caracteres especiais (por exemplo, ! ou #)

A senha do Linux é criptografada e está em hash no banco de dados de Cisco DNA Center. Se você estiver implantando um cluster de vários nós, também será solicitado a inserir a senha do Linux do nó mestre em cada um dos nós complementares.

3. **Propagação de geração de senha (opcional)**: em vez de inventar a senha do Linux, você pode inserir uma frase de propagação e pressionar **Generate password** (Gerar senha). O assistente de configuração do Maglev vai gerar uma senha aleatória e segura usando essa frase de propagação. Você pode editar a senha gerada, usando o campo **Auto Generated Password** (Senha gerada automaticamente).
4. **Senha do administrador**: identifica a senha usada para acesso à Web do Cisco DNA Center em um cluster. Essa é a senha do **`administrador`** da conta de superusuário, que você usa para fazer login no Cisco DNA Center pela primeira vez (consulte Fazer login pela primeira vez). Você será solicitado a alterar essa senha quando fizer login pela primeira vez, para garantir que ela seja segura.

   É preciso criá-la, visto que não há uma senha padrão. A senha do administrador deve atender aos mesmos requisitos que a senha do Linux descrita acima.
5. **Senha do usuário do CIMC**: identifica a senha usada para acessar a interface de usuário gráfica do CIMC. O padrão de fábrica é *password*, mas você será solicitado a alterá-la quando configurar o CIMC para acesso através do navegador da Web (consulte Ativar acesso do navegador ao CIMC).

   A senha do usuário CIMC deve atender aos mesmos requisitos que a senha do Linux descrita acima. Ela pode ser alterada novamente para *password* apenas por uma redefinição para os padrões de fábrica.
6. **Endereço IP do nó mestre**: necessário somente quando você está instalando nós complementares em um cluster. Esse é o endereço IP da porta de cluster no nó mestre (consulte Conexões de cabo de interface).

Informações obrigatórias na primeira configuração

Depois de concluir a configuração das aplicações, você fará login no Cisco DNA Center pela primeira vez e concluirá as tarefas essenciais de configuração. Durante a primeira configuração, você precisará ter as seguintes informações:

1. **Nova senha de superusuário admin**: você será solicitado a inserir uma nova senha para o superusuário admin do Cisco DNA Center. A redefinição da senha de superusuário melhora a segurança operacional. Isso é especialmente importante se, por exemplo, os funcionários da empresa que instalaram e configuram o dispositivo do Cisco DNA Center não forem usuários ou administradores do Cisco DNA Center.
2. **Credenciais do Cisco.com**: a ID de usuário e a senha do Cisco.com que a empresa usa para registrar downloads de software e receber comunicações do sistema por e-mail.
3. **Credenciais da Smart Account da Cisco**: a ID de usuário da Smart Account do Cisco.com e a senha que a empresa usa para gerenciar as licenças de dispositivo e software.

4. **URL e credenciais do gerenciador de endereços IP**: o nome do host, a URL, o nome do usuário admin e a senha do administrador do servidor IPAM (IP address Manager) de terceiros que você planeja usar com o Cisco DNA Center. A versão atual é compatível com InfoBlox ou Bluecat.
5. **URL do proxy, porta e credenciais**: a URL (nome do host ou endereço IP), o número da porta, o nome de usuário e a senha do usuário do servidor proxy que você planeja usar com o Cisco DNA Center para obter atualizações para o software Cisco DNA Center, gerenciar licenças de dispositivo e recuperar outro conteúdo para download.
6. **Cisco DNA CenterUsuários**: nomes de usuário, senhas e configurações de privilégios para os novos usuários do Cisco DNA Center que você vai criar. A Cisco recomenda que você sempre use uma dessas novas contas de usuário para todas as operações normais do Cisco DNA Center. Evite usar a conta de superusuário admin para algo que não seja reconfigurar o Cisco DNA Center e outras operações nas quais os privilégios de superusuário são explicitamente necessários.

Para obter detalhes sobre como iniciar e responder ao assistente de configuração pela primeira vez quando ele solicitar essas informações, consulte Fazer login pela primeira vez.

Você também precisará das seguintes informações para concluir as tarefas de configuração restantes, que podem ser feitas após o primeiro login:

1. **IP e credenciais do servidor ISE**: você precisará do endereço IP do servidor Cisco Identify Services Engine (ISE), nome de usuário admin e senha. Eles são necessários para fazer login e configurar o servidor ISE da empresa para compartilhar dados com o Cisco DNA Center, conforme explicado em Integração do Cisco ISE com Cisco DNA Center.
2. **Informações do servidor de autorização e políticas:** se estiver usando o Cisco ISE como servidor de autenticação e políticas, você precisará das mesmas informações que as da integração com ISE acima, além de nome de usuário da CLI do ISE, senha da CLI, FQDN do servidor, nome do assinante (como `cdnac`), chave SSH do ISE (opcional), escolha de protocolo (RADIUS ou TACACS), porta de autenticação, porta designada e configurações de repetição/tempo limite.

   Se você estiver usando um servidor de autorização e políticas diferentes, serão necessários o endereço IP do servidor, a opção de protocolo (RADIUS ou TACACS), a porta de autenticação, a porta designada e as configurações de repetição/tempo limite.

   Você usará essas informações para integrar o Cisco DNA Center com o servidor de autenticação e política escolhido, conforme explicado em Configurar os servidores de autenticação e política.
3. **Os valores de tempo limite e de repetição SNMP**são necessários para configurar a sondagem e o monitoramento de dispositivos, conforme explicado em Configurar propriedades de SNMP.

CAPÍTULO 3

Instalar o dispositivo

- Fluxo de trabalho de instalação do dispositivo, na página 37
- Desempacotar e inspecionar o dispositivo, na página 38
- Revisar os avisos e as diretrizes de instalação, na página 39
- Analisar os requisitos do rack, na página 40
- Conectar e ligar o dispositivo, na página 40
- Verificar os LEDs, na página 41

Fluxo de trabalho de instalação do dispositivo

A tabela a seguir detalha as tarefas de instalação física e a ordem em que elas são realizadas. Siga estas etapas para cada dispositivo Cisco DNA Center que você instalar. Certifique-se de instalar todos os dispositivos antes de configurar o primeiro nó mestre.

Quando você tiver concluído todas as tarefas desta tabela com êxito, continue seguindo as etapas no Fluxo de trabalho de configuração do dispositivo.

Clique neste link para assistir ao vídeo que demonstra o processo de desempacotamento, instalação e configuração do dispositivo Cisco DNA Center.

Tabela 20: Cisco DNA Center Tarefas de instalação do dispositivo

Etapa	Descrição
1	Analise e atenda aos requisitos de planejamento de implantação, incluindo a coleta de informações que você precisará fornecer durante a configuração e a instalação: • Sobre Cisco DNA Center e Software-Defined Access • Conexões de cabo de interface • Sub-redes necessárias e endereços IP adicionais • URLs de Internet necessárias e nomes de domínio totalmente qualificados • Fornecer acesso seguro à Internet • Portas de rede obrigatórias • Informações de configuração obrigatórias • Informações obrigatórias na primeira configuração
2	Analise os recursos e as especificações do dispositivo: • Resumo de recursos • Painéis frontal e traseiro • Especificações físicas • Especificações ambientais • Especificações de alimentação
3	Desempacote o dispositivo: Desempacotar e inspecionar o dispositivo
4	Analise os avisos operacionais e as diretrizes sobre o dispositivo: Revisar os avisos e as diretrizes de instalação
5	Instale o dispositivo em um rack: Analisar os requisitos do rack
6	Conecte a energia ao dispositivo e ligue-o: Conectar e ligar o dispositivo
7	Verifique os LEDs dos painéis frontal e traseiro para garantir que o dispositivo esteja funcionando: Verificar os LEDs

Desempacotar e inspecionar o dispositivo

⚠

Cuidado Ao lidar com componentes de dispositivos internos, use uma pulseira de ESD e manipule módulos apenas pelas bordas do transportador.

Dica Mantenha o contêiner de envio caso o equipamento exija o envio no futuro.

Observação O chassi é inspecionado cuidadosamente antes do envio. Se algum dano ocorreu durante o transporte ou se algum item estiver ausente, entre em contato imediatamente com o representante de atendimento ao cliente.

Etapa 1 Remova o dispositivo do contêiner de papelão e guarde todos os materiais de embalagem.

Etapa 2 Compare a remessa com a lista de equipamentos fornecida pelo representante do atendimento ao cliente. Verifique se recebeu todos os itens.

Etapa 3 Verifique se há danos e informe quaisquer discrepâncias ou danos ao representante do atendimento ao cliente. Tenha as seguintes informações disponíveis:

- Número da fatura da transportadora (consulte a guia de remessa)
- Modelo e número de série da unidade danificada
- Descrição do dano
- Efeito do dano na instalação

Revisar os avisos e as diretrizes de instalação

Aviso **Para evitar o superaquecimento do sistema, não o opere em uma área que exceda a temperatura ambiente máxima recomendada de: 35°C (95°F).** Declaração 1047

Aviso **A tomada deve estar acessível a qualquer momento, uma vez que é o principal dispositivo de desconexão.** Declaração 1019

Aviso **Este produto depende da instalação elétrica do prédio para a proteção contra curtos-circuitos (sobrecarga). Certifique-se de que a capacidade do dispositivo protetor não seja superior a: 250 V, 15 A.**Declaração 1005

Aviso **A instalação do equipamento deve estar em conformidade com códigos locais e nacionais sobre uso de eletricidade.** Declaração 1074

Cuidado Para garantir o fluxo de ar apropriado, é necessário colocar os dispositivos em rack usando kits de trilhos. Colocar fisicamente as unidades umas sobre as outras ou "empilhar" sem o uso dos kits de trilhos bloqueia as saídas de ar sobre os dispositivos, o que pode resultar em superaquecimento, velocidades mais altas do ventilador e maior consumo de energia. Recomendamos que você monte os aparelhos em kits de trilhos quando estiver instalando-os no rack, pois esses trilhos fornecem o mínimo de espaço necessário entre os dispositivos. Nenhum espaçamento adicional entre os dispositivos é necessário ao montar as unidades usando kits de trilhos.

Cuidado Evite tipos de fontes de alimentação (UPS) que usam a tecnologia ferrorressonante. Esses tipos de UPS podem se tornar instáveis com sistemas como o Cisco UCS, e podem ter flutuações substanciais no projeto atual devido a padrões de tráfego de dados flutuantes.

Ao instalar um dispositivo, siga estas diretrizes:

- Planeje a configuração do local e prepare-o antes de instalar o dispositivo. Consulte o *Guia de preparação do local do UCS da Cisco* para obter ajuda com as tarefas recomendadas de preparação e planejamento do local.
- Certifique-se de que haja espaço adequado em torno do dispositivo para permitir a manutenção do dispositivo e o fluxo de ar adequado. O fluxo de ar neste dispositivo é de frente para trás.
- Verifique se o ar-condicionado do local atende aos requisitos térmicos listados nas Especificações ambientais.
- Certifique-se de que o gabinete ou rack atende aos requisitos listados em Analisar os requisitos do rack.
- Verifique se a energia do local atende aos requisitos listados em Especificações de alimentação. Se disponível, você pode usar a UPS para proteger contra falhas de energia.

Analisar os requisitos do rack

Para uma operação adequada, o rack em que você instala o dispositivo deve atender aos seguintes requisitos:

- Um rack EIA padrão de 48,3 cms (19 polegadas) de tela inteira, com colunas de montagem que estão em conformidade com o espaçamento universal de orifícios inglês, conforme a seção 1 de ANSI/EIA-310-D-1992.
- Os furos do rack podem ser quadrados de 9,6 mm (0,38 polegada), redondos de 7,1 mm (0,28 polegada), #12-24 UNC ou #10-32 UNC quando você usa os trilhos deslizantes fornecidos.
- O espaço de rack vertical mínimo por servidor deve ser um RU, igual a 44,45 mm (1,75 polegada).

Conectar e ligar o dispositivo

Esta seção descreve como ligar o dispositivo e verificar se ele está funcionando.

Etapa 1 Conecte o cabo de alimentação fornecido a cada fonte de alimentação no dispositivo e, em seguida, conecte os cabos de alimentação a uma tomada de energia CA com aterramento. Consulte as Especificações de alimentação para obter detalhes.

Aguarde aproximadamente dois minutos para permitir que o dispositivo inicialize no modo de energia de standby durante a primeira inicialização.

Você pode verificar o status de energia examinando o LED de status de energia:

- Desligado — não há energia CA presente no dispositivo.
- Âmbar — o dispositivo está no modo de energia de standby. A energia é fornecida apenas para o CIMC e algumas funções da placa-mãe.
- Verde — o dispositivo está no modo de energia principal. A energia é fornecida para todos os componentes do dispositivo.

Para obter mais informações sobre esses e outros LEDs do equipamento, consulte os Painéis frontal e traseiro.

Etapa 2 Conecte um monitor de teclado USB e VGA ao servidor, usando o cabo KVM fornecido ligado ao conector KVM no painel frontal. Como alternativa, você pode usar as portas VGA e USB no painel traseiro. Você só pode se conectar a uma interface VGA de cada vez.

O que Fazer Depois

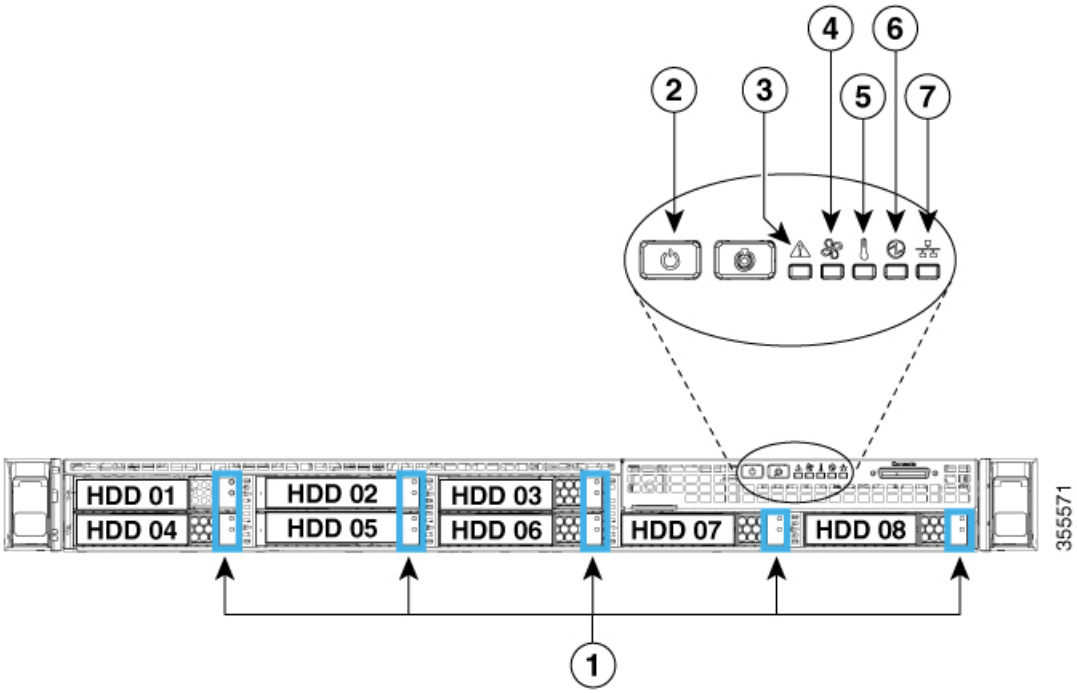
Continue seguindo o procedimento descrito em Verificar os LEDs.

Verificar os LEDs

Depois de ligar o dispositivo Cisco DNA Center, verifique o estado do painel frontal e os LEDs e botões traseiros do painel para garantir que eles estejam funcionando.

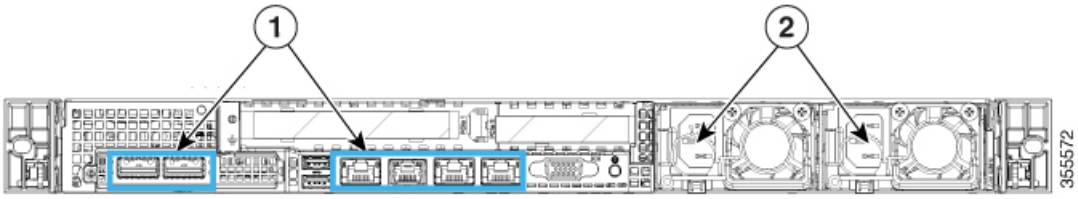
As seguintes ilustrações mostram os LEDs de um dispositivo funcional com um chassi Cisco UCS C220 M4, após a instalação física e a primeira inicialização e antes da configuração.

Figura 6: LEDs do painel frontal



LED	Indicador de status desejado
1	LEDs de falha da unidade: desligado. LEDs de atividade da unidade: verde
2	Status de energia: verde
3	Status do sistema: verde
4	Status do ventilador: verde
5	Status da temperatura: verde
6	Status da fonte de alimentação: verde
7	Atividade do link de rede: desligado

Figura 7: LEDs do painel traseiro



LED	Indicador de status desejado
1	Na primeira inicialização, todas as portas devem ter status de link e LEDs de velocidade de link aparecendo como desligados, e o LED de status de energia deve estar verde. Depois que as configurações de rede são configuradas e testadas usando o Assistente de configuração do Maglev (consulte Configurar o nó mestre e Configurar os nós complementares), o status do link, a velocidade do link e os LEDs de status de energia para todas as portas **cabeadas** devem ser verdes. Todos os LEDs de porta **não cabeada** devem estar inalterados.
2	LEDs de falha da fonte de alimentação: desligados. LEDs de energia CA: verde

Se os LEDs tiverem cores diferentes das mostradas acima, isso significa que há problema. Consulte os Painéis frontal e traseiro para obter detalhes sobre as causas prováveis do status. Certifique-se de corrigir qualquer condição de problema antes de prosseguir com a configuração do dispositivo.

CAPÍTULO 4

Configurar o dispositivo

- Fluxo de trabalho de configuração do dispositivo, na página 45
- Ativar acesso do navegador ao CIMC, na página 46
- Executar verificações preliminares, na página 51
- Verifique a imagem ISO de Cisco DNA Center, na página 58
- Criar uma unidade USB Bootable, na página 59
- Refazer a imagem do dispositivo, na página 60
- Instalar a imagem ISO do Cisco DNA Center, na página 62
- Configurar o nó mestre, na página 62
- Configurar os nós complementares, na página 76
- Cenários de implantação do cluster de alta disponibilidade, na página 91

Fluxo de trabalho de configuração do dispositivo

Você pode implantar o dispositivo na rede em um dos dois modos:

- Autônomo: como um único nó que oferece todas as funções. Essa opção geralmente é preferida para implantações iniciais ou de teste e em ambientes de rede menores.
- Cluster: um cluster de até três nós. Nesse modo, todos os serviços e dados são compartilhados entre os hosts. Essa é a opção preferida para grandes implantações.

Se você escolher o modo autônomo para a implantação inicial, poderá adicionar mais dispositivos posteriormente para formar um cluster. Certifique-se de configurar o host autônomo para defini-lo como o primeiro ou principal nó no cluster.

Se escolher o modo de cluster para a implantação inicial, conclua a configuração do nó mestre antes de começar a configurar os nós complementares.

A tabela a seguir detalha as tarefas de configuração e a ordem em que elas são realizadas. Quando você tiver concluído as tarefas desta tabela com êxito, continue concluindo a configuração inicial, conforme explicado no Fluxo de trabalho de primeira configuração.

Clique neste link para obter o vídeo que demonstra o processo de configuração do dispositivo.

Tabela 21: Tarefas de configuração do dispositivo

Etapa	Descrição
1	Ative o acesso do navegador à interface de usuário gráfica do Cisco Integrated Management Controller (CIMC) do dispositivo: Ativar acesso do navegador ao CIMC.
2	Garanta a configuração sem problemas verificando e ajustando o hardware e as configurações do switch: Executar verificações preliminares
3	Inicie o assistente de configuração do Maglev no CIMC e configure o nó mestre no cluster: Configurar o nó mestre
4	Se você instalou três dispositivos e deseja adicionar o segundo e terceiro nós ao cluster: Configurar os nós complementares

Ativar acesso do navegador ao CIMC

Após instalar o dispositivo conforme descrito no Fluxo de trabalho de instalação do dispositivo, use o Cisco IMC Configuration Utility para atribuir um endereço IP e um gateway à porta Cisco Integrated Management Controller (CIMC) do dispositivo. Isso dará ao navegador acesso à interface de usuário gráfico do CIMC, para que o dispositivo seja configurado para uso.

Depois de concluir essa configuração do CIMC, você precisará fazer login no CIMC e executar várias tarefas que ajudam a garantir a configuração correta (consulte Executar verificações preliminares).

Dica Para ajudar a garantir a segurança da implantação, o CIMC solicita que você altere a senha padrão do usuário do CIMC quando inicializa o dispositivo pela primeira vez. Se desejar alterar a senha do usuário do CIMC posteriormente, é mais fácil usar a interface do usuário do CIMC, da seguinte forma:

1. Selecione > **Admin** > **User Management** > **Local User Management** (Admin > Gerenciamento de usuário > Usuário local > Gerenciamento).
2. Selecione ID `1` e clique em **Modify User** (Modificar usuário).

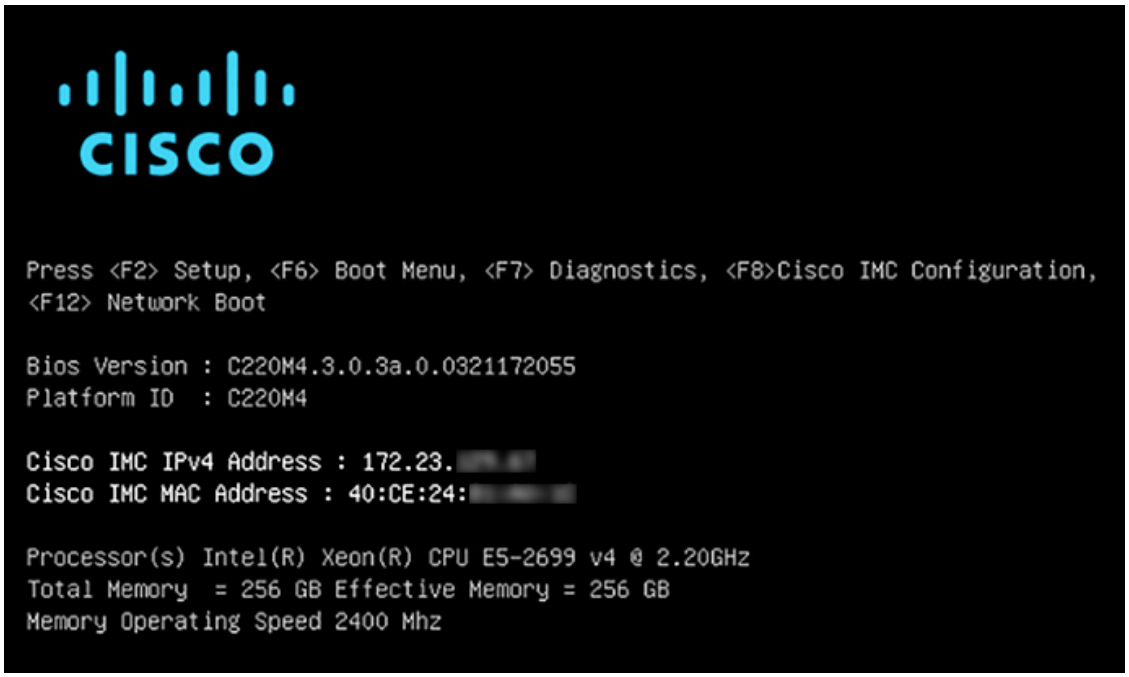
   Digite a nova senha no campo **Change Password** (Alterar senha) e clique em **Save** (Salvar).

Etapa 1 Acesse o console do dispositivo ao acoplar:

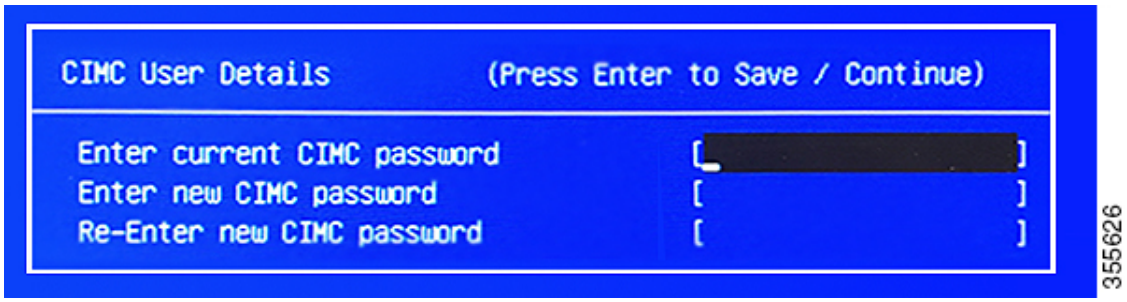
- Um cabo KVM ao conector KVM no painel frontal do dispositivo (componente 12 na ilustração do painel frontal nos Painéis frontal e traseiro) ou
- Um teclado e um monitor às portas USB e VGA no painel traseiro do dispositivo (componentes 7 e 12, respectivamente, na ilustração do painel traseiro nos Painéis frontal e traseiro).

Etapa 2 Verifique se o cabo de alimentação do dispositivo está conectado e se a energia está ligada.

Etapa 3 Pressione o botão **liga/desliga** no painel frontal para inicializar o dispositivo. Observe a tela de inicialização do Cisco IMC Configuration Utility que será exibida, como mostrado abaixo.

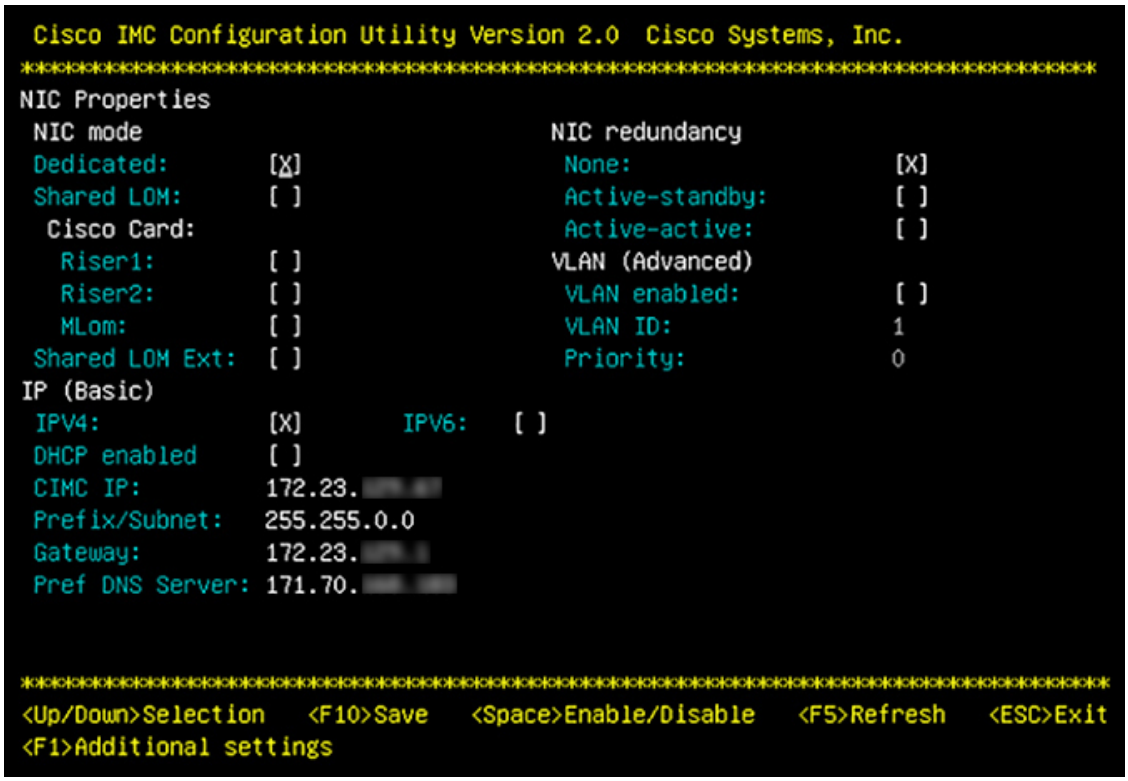


Etapa 4 Assim que a tela de inicialização for exibida, pressione **F8** para executar a **Configuração do IMC da Cisco**. O Cisco IMC Configuration Utility exibe a tela de detalhes do usuário do CIMC, como mostrado abaixo.



Etapa 5 Insira a senha de usuário padrão do CIMC (o padrão em um dispositivo novo é **password**) no campo **Enter current CIMC Password** (Inserir senha de CIMC atual). Em seguida, insira e confirme a nova senha do usuário do CIMC nos campos **Enter new CIMC password** (Inserir nova senha do CIMC) e **Re-Enter new CIMC password** (Reinserir nova senha do CIMC).

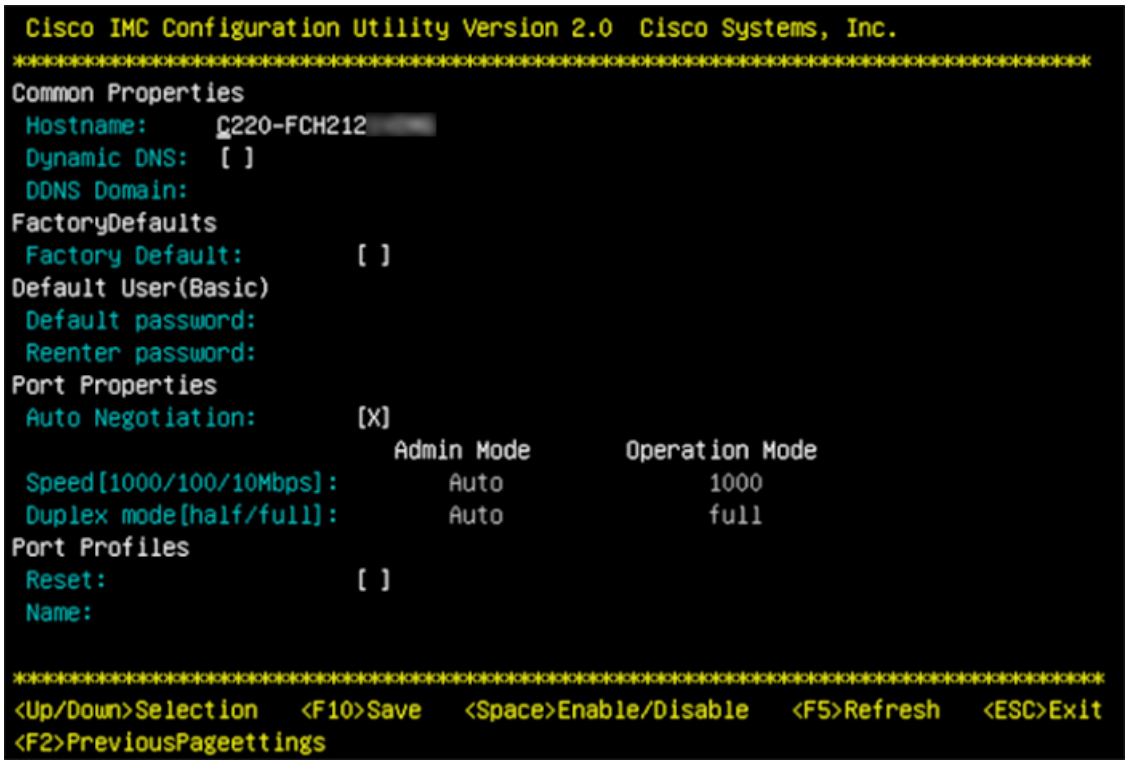
Etapa 6 Quando você pressiona **Enter** no campo **Re-Enter new CIMC password** (Reinserir nova senha de CIMC), o Cisco IMC Configuration Utility exibe a tela de **NIC Properties** (Propriedades da placa de interface de rede), como mostrado abaixo.



Etapa 7 Faça as seguintes alterações:

- **NIC mode** (Modo da placa de interface de rede) — Selecione **Dedicated** (Dedicado).
- **IP (Basic)** (IP [Básico]) — Selecione **IPV4**.
- **CIMC IP** (IP de CIMC) — Insira o endereço IP da porta de CIMC.
- **Prefix/Subnet** (Prefixo/sub-rede) — Insira a máscara de sub-rede para o endereço IP da porta CIMC.
- **Gateway** — Insira o endereço IP do gateway padrão preferencial.
- • **Pref DNS Server** (Servidor DNS preferencial) — especifique o endereço do servidor DNS preferencial.
- **NIC Redundancy** (Redundância de placa de interface de rede) — Selecione **None** (Nenhuma).

Etapa 8 Pressione **F1** para especificar **Additional settings** (Configurações adicionais). O Cisco IMC Configuration Utility exibe a tela de **Commom Properties** (Propriedades comuns), como mostrado abaixo.



Etapa 9 Faça as seguintes alterações:

- **Hostname** (Nome do host): insira um nome do host para CIMC neste dispositivo.
- **Dynamic DNS** (DNS Dinâmico): desmarque a caixa de seleção para desativar este recurso.
- **Fabric Defaults** (Padrões de fábrica): desmarque a caixa de seleção para desativar este recurso.
- **Default User (Basic)** (Usuário padrão [básico]): deixe esses campos em branco.
- **Port Properties** (Propriedades da porta): insira novas configurações ou aceite os padrões mostrados nesses campos.
- **Port Profiles** (Perfis da porta): desmarque a caixa de seleção para desativar este recurso.

Etapa 10 Pressione **F10** para **salvar** as configurações.

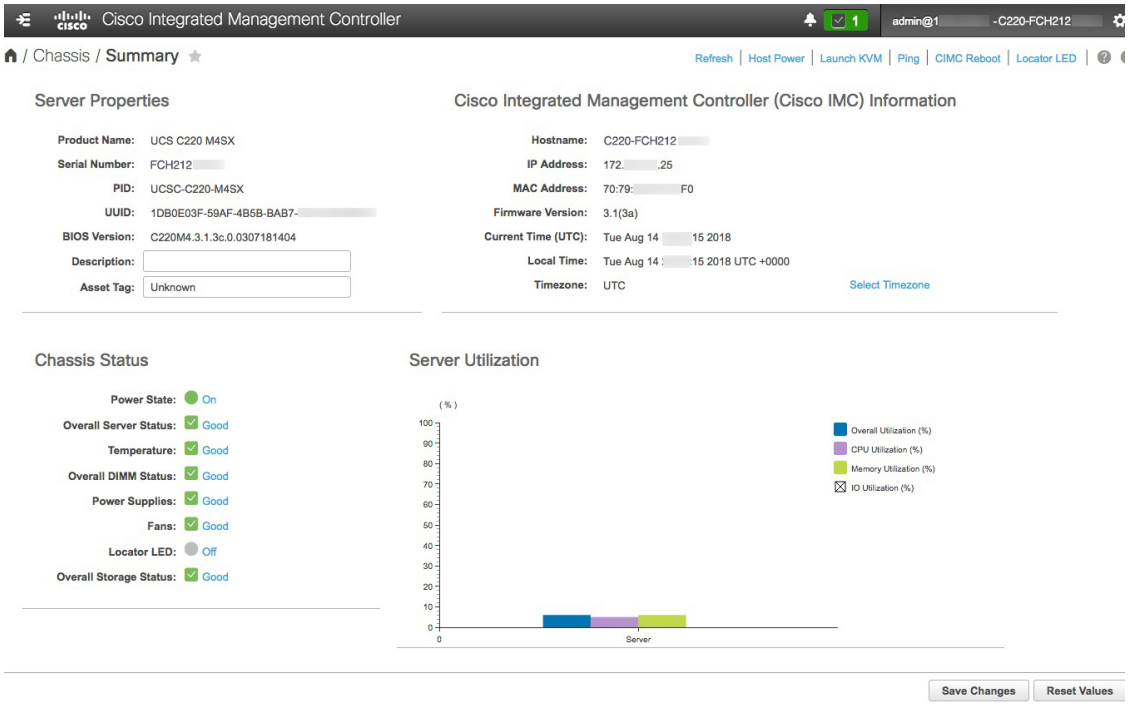
Etapa 11 Pressione **Escape** para **sair** e reiniciar o dispositivo.

Etapa 12 Depois que as configurações forem salvas e o dispositivo concluir a reinicialização, abra um navegador compatível em uma máquina cliente com acesso à sub-rede em que o dispositivo está instalado e digite a seguinte URL:

`https://`*`CIMC_ip_address`* em que ***`CIMC_ip_address`*** é o endereço IP da porta CIMC inserida na etapa 5.

O navegador exibe uma janela principal da interface de usuário do Cisco Integrated Management Controller, como a mostrada abaixo.

Etapa 13 Faça login usando a ID de usuário CIMC e a senha que você definiu na etapa 5. Se o login for bem-sucedido, o navegador exibirá uma janela de **Cisco Integrated Management Controller Chassis Summary** (Resumo do chassi do Cisco Integrated Management Controller), como a mostrada abaixo.



O que Fazer Depois

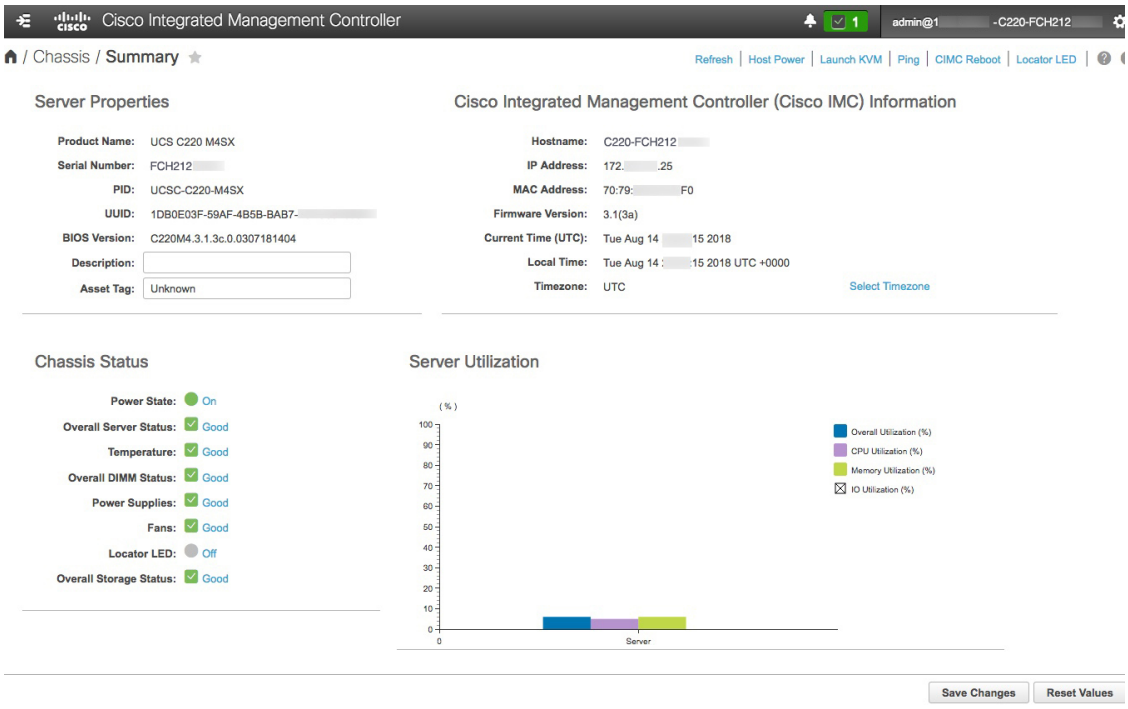
Execute tarefas que ajudam a garantir uma configuração sem problemas: Executar verificações preliminares.

Executar verificações preliminares

Após instalar o dispositivo conforme descrito no Fluxo de trabalho de instalação do dispositivo e configurar o acesso à interface do usuário do CIMC conforme descrito em Ativar acesso do navegador ao CIMC, use o CIMC para executar as seguintes tarefas de pré-configuração, que ajudam a garantir a configuração e a implantação corretas:

1. Sincronize o hardware do dispositivo com os servidores Network Time Protocol (NTP) que você usa para gerenciar a rede. Eles devem ser os mesmos servidores NTP cujos nomes de host ou IPs você coletou para serem usados ao planejar a implementação, conforme explicado em Sub-redes necessárias e endereços IP adicionais. Essa é uma tarefa importante que garante que os dados do Cisco DNA Center sejam sincronizados corretamente na rede.
2. Verifique se as portas de 10 Gbps do dispositivo estejam ativadas e corretamente configuradas para alta produtividade.
3. Reconfigure os switches conectados às portas de dispositivo de 10 Gbps para respaldar as configurações de taxa de processamento mais alta.
4. Reconfigure os switches conectados às portas de dispositivo de 10 Gbps para respaldar os quadros de 802.1p de tamanho excessivo.

Etapa 1 Faça login no CIMC do dispositivo usando o endereço IP do CIMC, a ID de usuário e a senha que você definiu em Ativar acesso do navegador ao CIMC. Se o login for bem-sucedido, o navegador exibirá a janela **Cisco Integrated Management Controller Chassis Summary** (Resumo do chassi do Cisco Integrated Management Controller), como mostrada abaixo.

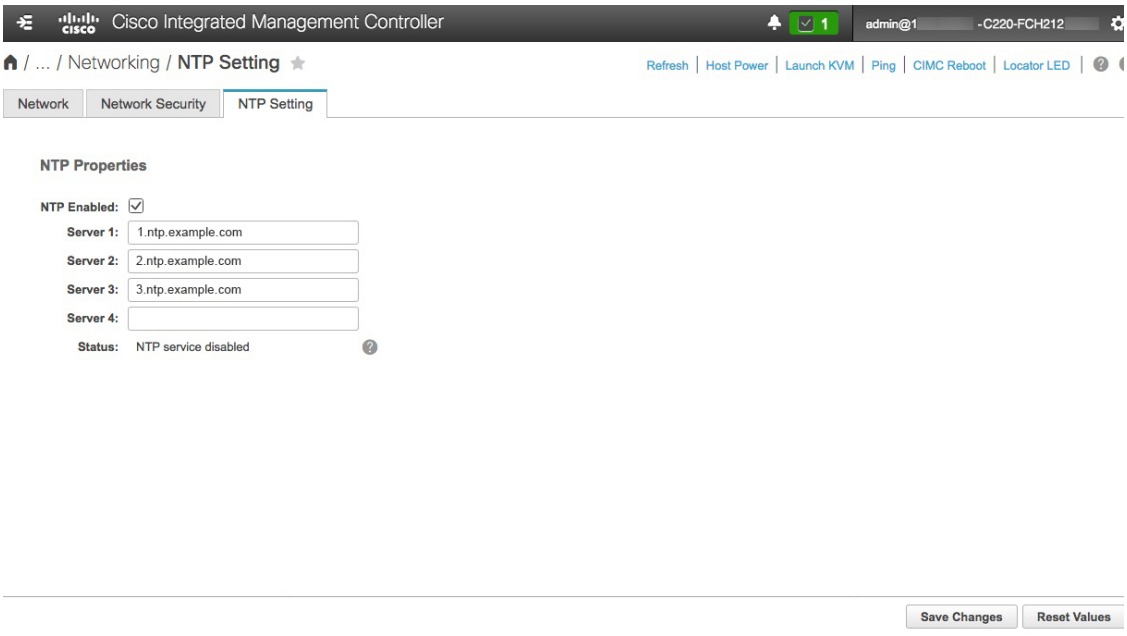


Etapa 2 Sincronize o hardware do dispositivo com os servidores Network Time Protocol (NTP) que você usa para gerenciar a rede, da seguinte maneira:

a) Com a janela Chassis Summary (Resumo do chassi) exibida, clique no ícone para exibir o menu CIMC.

b) No menu CIMC, selecione **Admin** > **Networking** > **NTP Setting** (Admin > Rede > Configuração de NTP). O CIMC exibe a guia **NTP Setting** (Configuração de NTP).

c) Certifique-se de que a caixa **NTP Enabled** (NTP ativado) esteja marcada e, em seguida, insira até quatro nomes ou endereços de host de servidor NTP nos quatro campos **Server** (Servidor) numerados, como no exemplo mostrado abaixo.

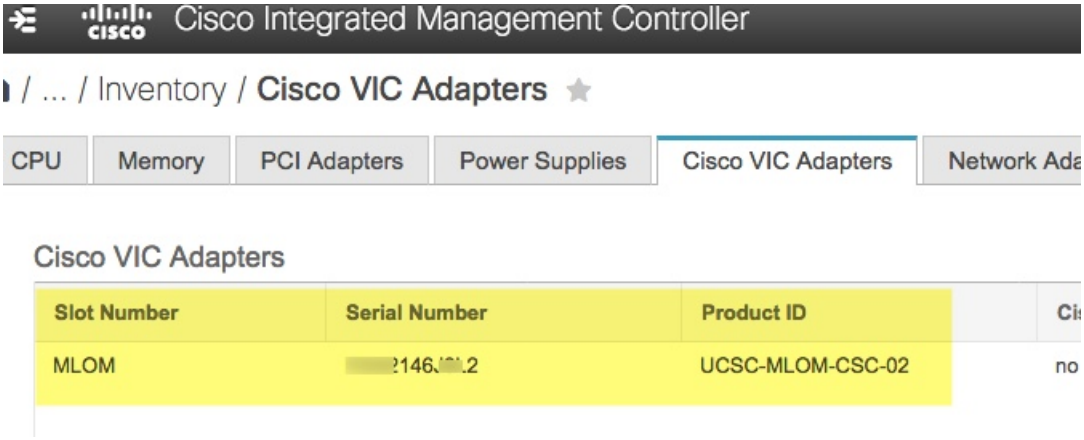


d) Ao concluir, clique em **Save Changes** (Salvar alterações). O CIMC validará as entradas e, em seguida, começará a sincronizar a hora no hardware do dispositivo com o tempo nos servidores NTP.

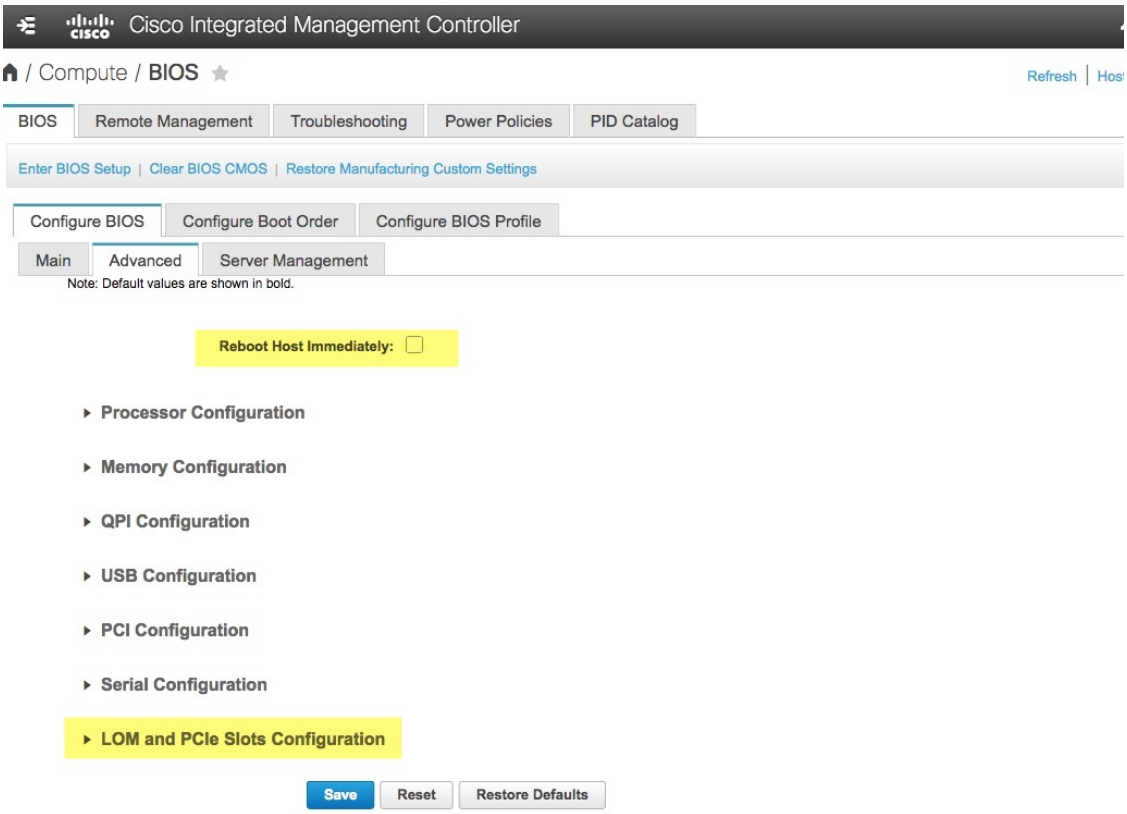
Etapa 3 Em seguida, verifique se as placas de interface de rede do dispositivo estão configuradas para respaldar a alta produtividade, da seguinte forma:

a) Se necessário, clique no ícone para exibir o menu CIMC.

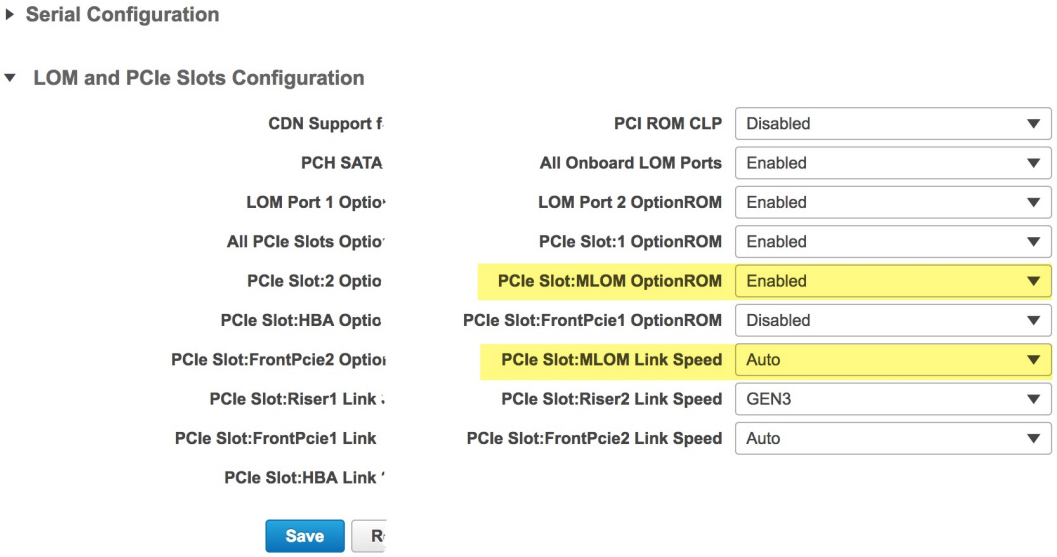
b) No menu CIMC, selecione **Chassis** > **Inventory** > **Cisco VIC Adapters** (Chassi > Inventário > Adaptadores VIC da Cisco). Verifique se a ID do produto "UCSC-MLOM-CSC-02" está listada para o slot MLOM, como mostrado abaixo:



c) Selecione > **Compute** > **BIOS** > **Configure BIOS** > **Advanced** (Computar > BIOS > Configurar BIOS > Avançado). Verifique se a caixa de seleção **Reboot Host Immediately** (Reinicializar host imediatamente) está desmarcada e anote o local do menu suspenso **LOM and PCIe Slots Configuration** (Configuração dos slots Lom e PCIe).

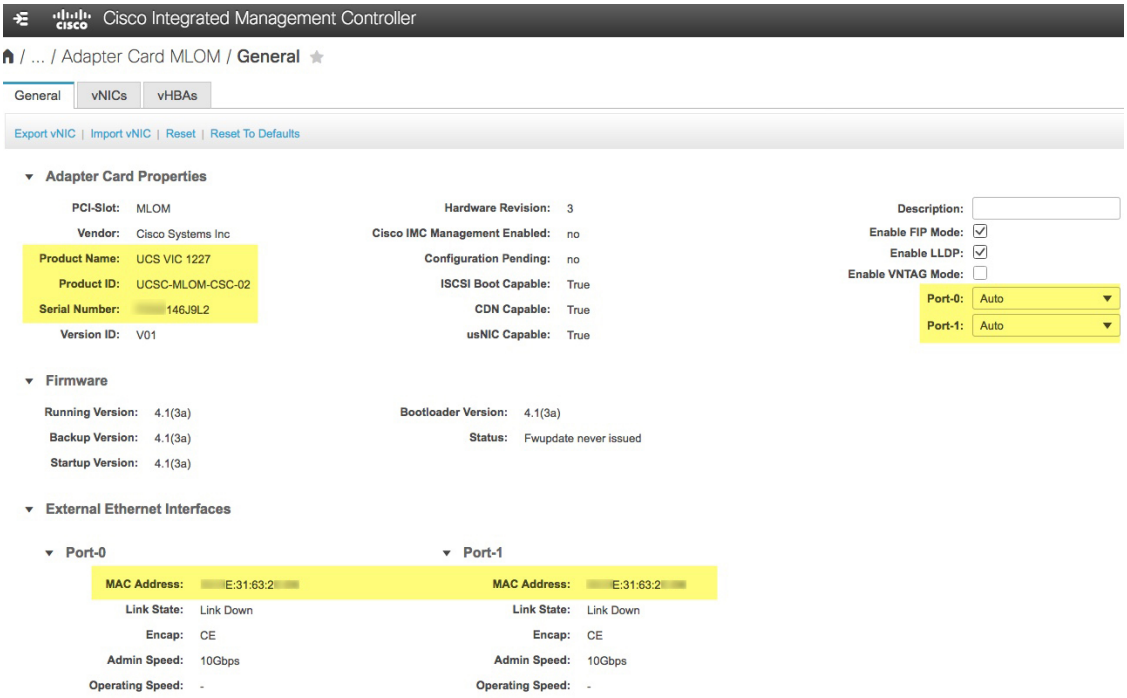


d) Selecione **LOM and PCIe Slots Configuration** (Configuração dos slots Lom e PCIe). Em seguida, usando os seletores suspensos, defina **PCIe Slot: MLOM OptionROM** como **Enabled** (Ativado) e **PCIe Slot: MLOM Link Speed** como **Auto** (Automático).



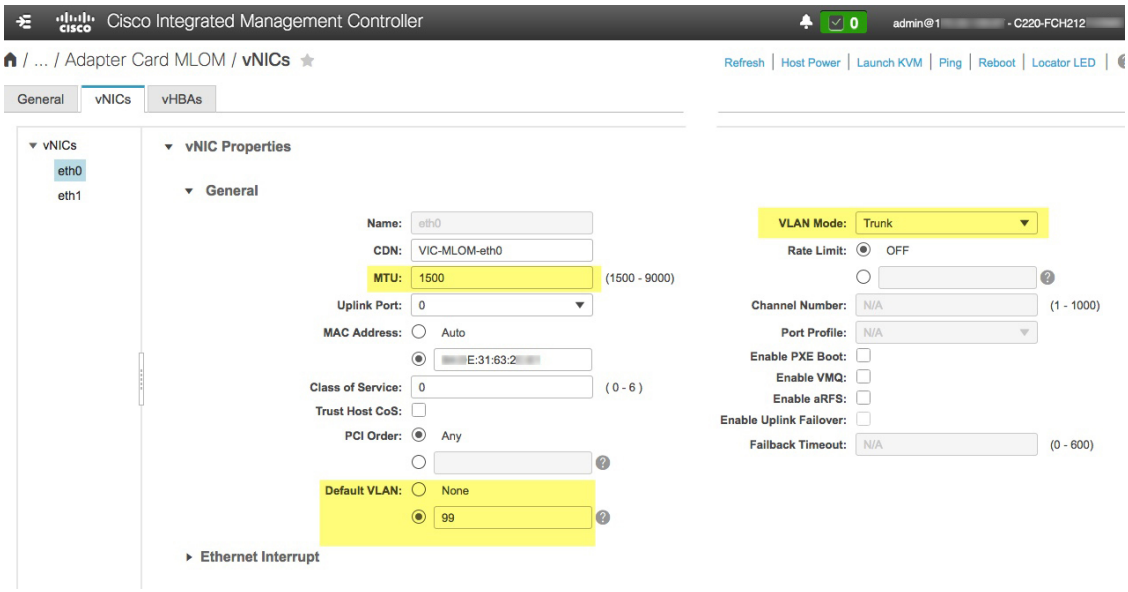
e) Clique em **Salvar**. Você será solicitado a reinicializar o host. Clique em **Cancel** (Cancelar) para continuar em vez de reiniciar.

f) Selecione ☰ > **Networking** > **Adapter Card MLOM** > **General** (Rede > MLOM da placa adaptadora > Geral). Anote os endereços MAC para a **porta-0** e a **porta-1** (conforme aparece na seção **External Ethernet Interfaces** [Interfaces Ethernet externas] na parte inferior da página). Na seção **Adapter Card Properties** (Propriedades da placa de adaptador), use os seletores suspensos ao lado da **porta-0** e **porta-1** para definir a velocidade dessas duas portas como **Auto** (Automático), como mostrado abaixo. Em seguida, clique em **Save Changes** (Salvar alterações).



g) Clique na guia **vNICs** e selecione **eth0** na lista suspensa **vNICs** . Use os seletores e os campos para definir esses valores como **eth0**:

- **Modo VLAN: tronco**
- **MTU: 1500**
- **VLAN padrão: 99** (Observe que "99" é apenas um exemplo. Você deve inserir a VLAN padrão que deseja que os dispositivos e switches usem.)



Dica 1500 é o tamanho mínimo da MTU. Você pode melhorar a produtividade nas portas 10 Gbps inserindo qualquer valor mais alto, até o máximo de 9000.

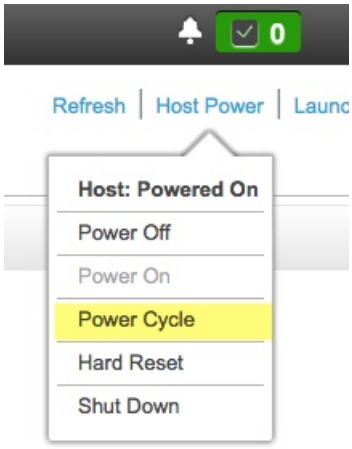
h) Clique em **Salvar alterações**. Você será solicitado a reinicializar o host novamente. Clique em **Cancel** (Cancelar) para continuar em vez de reiniciar.

i) Selecione **eth1** no menu suspenso **vNICs** . Use os seletores suspensos para definir os mesmos valores de **eth1** que você definiu para o **eth0** acima.

j) Ao concluir, clique em **Save Changes** (Salvar alterações). Você será solicitado a reinicializar o host. Desta vez, clique em **OK** para reinicializar o dispositivo.

k) Quando o dispositivo terminar a reinicialização, faça login na interface gráfica do CIMC novamente. Selecione > **Networking** > **Adapter Card MLOM** > **General** > **vNICs** (Rede > MLOM da placa adaptadora > Geral > vNICs). Verifique a precisão dos endereços MAC do vNIC e os parâmetros de MTU, VLAN e modo de VLAN que você definiu anteriormente.

l) Quando terminar: clique no menu **Host Power** (Alimentação do host) no canto superior direito e selecione **Power Cycle** (Ciclo de energia). Em seguida, clique em **OK**.



Etapa 4 Depois, reconfigure os switches para corresponder às configurações de alta produtividade no dispositivo, da seguinte forma:

a) Usando um cliente SSH (Secure Shell), faça login no switch a ser configurado e digite o modo EXEC no prompt do switch.

b) Insira a seguinte série de comandos para configurar a porta do switch:

```
MySwitch#Config terminal
MySwitch(config)#interface tengigabitethernet 1/1/3
MySwitch(config-if)#switchport mode trunk
MySwitch(config-if)#switchport trunk allowed vlan 99
MySwitch(config-if)#speed auto
MySwitch(config-if)#duplex full
MySwitch(config-if)#mtu 1500
MySwitch(config-if)#no shut
MySwitch(config-if)#end
MySwitch(config)#copy running-config startup-config
```

Observe que esses comandos são apenas exemplos. Use os mesmos valores de ID de VLAN e MTU que você inseriu ao configurar as placas de interface de rede de dispositivo acima. Os valores de comando para velocidade de link, duplex e MTU são os padrões do switch de exemplo, portanto, você precisará inseri-los somente se tiver alterado os padrões. Você também pode, como ocorre com as placas de interface de rede do dispositivo, definir o MTU como o máximo de 9000, para melhorar a produtividade.

c) Execute o comando `show interface tengigabitethernet` *portID* e verifique se a porta está conectada e em execução e se tem as configurações corretas de MTU, duplex e tipo de link na saída do comando. Por exemplo:

```
MySwitch#show interface tengigabitethernet 1/1/3
TenGigabitEthernet1/1/3 is up, line protocol is up (connected)
  Hardware is Ten Gigabit Ethernet, address is XXXe.310.8000 (bia XXX.310.8000)
  MTU 1500 bytes, BW 10000000 Kbit/sec, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive not set
  Full-duplex, 10GB/s, link type is auto, media type is SFP-10Gbase-SR
```

d) Execute o comando `show execute interface tengigabitethernet` *portid* para configurar as portas do switch em que os cabos das portas Vic 1227 estão conectados. Por exemplo:

```
MySwitch#show run interface tengigabitethernet 1/1/3
Building configuration...
Current configuration : 129 bytes
! interface TenGigabitEthernet1/1/3
 switchport trunk allowed vlan 99
 switchport mode trunk
 ip device tracking maximum 10
end

MySwitch#
```

e) Execute o comando `show mac address-table interface tengigabitethernet` *portid* e verifique o endereço MAC da saída do comando. Por exemplo:

```
MySwitch#show mac address-table interface tengigabitethernet 1/1/3
          Mac Address Table
-------------------------------------------
Vlan     Mac Address       Type      Ports
----     -----------       ----      -----
99       XXXe.3161.1000    DYNAMIC   Te1/1/3
Total Mac Addresses for this criterion: 1

MySwitch#
```

Etapa 5 Por fim, configure os switches conectados às portas de dispositivo 10 Gbps para respaldar os quadros de 802.1p de tamanho excessivo.

a) Se você ainda não tiver feito isso, use um cliente do Secure Shell (SSH) para fazer login no switch a ser configurado e entre no prompt do switch.

b) Digite a seguinte série de comandos para configurar a porta do switch e respaldar quadros 802.1P:

```
MySwitch#Config terminal
MySwitch(config)#interface tengigabitethernet 1/1/3
MySwitch(config-if)#switchport voice vlan dot1p
MySwitch(config-if)#no shut
MySwitch(config-if)#end
MySwitch(config)#copy running-config startup-config
```

c) Execute o comando `show execute interface tengigabitethernet` *`portid`* e verifique na saída do comando se a porta tem a configuração correta de `voice vlan dot1p`. Por exemplo:

```
MySwitch#show run interface tengigabitEthernet 1/1/3
Building configuration...

Current configuration : 62 bytes
!
interface tengigabitethernet1/1/3
switchport mode trunk
switchport voice vlan dot1p
MySwitch#end
```

O que Fazer Depois

Continue configurando o primeiro dispositivo instalado como o nó mestre do cluster. Consulte Configurar o nó mestre.

Verifique a imagem ISO de Cisco DNA Center

Antes de implantar o Cisco DNA Center, aconselhamos enfaticamente que você verifique se a imagem ISO baixada é uma imagem autêntica da Cisco.

Antes de Iniciar

Obtenha o local da imagem ISO de Cisco DNA Center (seja por e-mail ou entre em contato com a equipe de suporte da Cisco).

Etapa 1 Baixe a imagem ISO de Cisco DNA Center (.iso) do local especificado pela Cisco.

Etapa 2 Baixe a chave pública da Cisco (cisco_image_verification_key. pub) para verificar a assinatura do local especificado pela Cisco.

Etapa 3 Baixe o arquivo de soma de verificação do algoritmo de hash seguro (SHA512) para a imagem ISO do local especificado pela Cisco.

Etapa 4 Obtenha o arquivo de assinatura da imagem ISO (.sig) do suporte da Cisco por e-mail ou baixe-o no site seguro da Cisco (se disponível).

Etapa 5 (Opcional) Execute uma verificação de SHA para determinar se a imagem ISO foi corrompida devido a um download parcial.

Execute um dos seguintes comandos (dependendo do sistema operacional):

- Em um sistema Linux: **sha512sum** *ISO-image-filename*
- Em um sistema Mac: **shasum -a 512** *ISO-image-filename*

O Microsoft Windows não inclui um utilitário de soma de verificação interno, mas você pode instalar um utilitário da Microsoft neste link: http://www.microsoft.com/en-us/download/details.aspx?id=11533. Compare a saída do comando acima (ou do Microsoft Windows Utility) com o arquivo de soma de verificação do SHA512 baixado anteriormente na etapa 3. Se a saída do comando não corresponder, baixe a imagem ISO novamente e execute o comando apropriado pela segunda vez. Se a saída ainda não corresponder, entre em contato com o suporte da Cisco.

Etapa 6 Verifique se a imagem ISO é autêntica e proveniente da Cisco pela assinatura:

openssl dgst -sha512 -verify cisco_image_verification_key.pub -signature*signature-filename ISO-image-filename*

Observação Esse comando funcionará em ambientes MAC e Linux. No Windows, você precisa baixar e instalar o OpenSSL (disponível aqui) se ainda não tiver feito isso.

Se a imagem ISO for autêntica, a execução desse comando deverá resultar em uma mensagem **Verified OK** (Verificada como OK). Se essa mensagem não aparecer, não instale a imagem ISO e entre em contato com o suporte da Cisco.

Etapa 7 Depois de confirmar que você baixou uma imagem ISO da Cisco, crie uma unidade USB Bootable que contenha a imagem ISO do Cisco DNA Center. Consulte Criar uma unidade USB Bootable.

Criar uma unidade USB Bootable

Conclua o procedimento a seguir para criar uma unidade USB Bootable da qual você pode instalar a imagem ISO do Cisco DNA Center.

Antes de Iniciar

- Baixe e verifique a cópia da imagem ISO do Cisco DNA Center. Consulte Verifique a imagem ISO de Cisco DNA Center.
- Confirme se a unidade flash USB que você está usando tem uma capacidade de pelo menos 32 GB.

Etapa 1 Baixe e instale o Etcher (versão 1.3.1 ou posterior), um utilitário freeware de código aberto que permite criar uma unidade USB Bootable no notebook ou desktop.

As versões do Etcher para Linux, macOS e Windows estão disponíveis no momento. Você pode baixar uma cópia em https://www.balena.io/etcher/.

Observação Use apenas a versão do Etcher do Windows em máquinas que executam o Windows 10, pois há problemas de compatibilidade conhecidos com versões mais antigas do Windows.

Etapa 2 Na máquina em que você instalou o gravador, conecte uma unidade USB e inicie o Etcher.

Etapa 3 Clique no ícone de engrenagem no canto superior direito da janela e verifique se as seguintes configurações do Etcher estão definidas:

- Desmontagem automática no êxito

- Validar a gravação no êxito

Etapa 4 Clique em **Back** (Voltar) para retornar à janela principal.

Etapa 5 Clique em **Select Image** (Selecionar imagem).

Etapa 6 Navegue até a imagem ISO do Cisco DNA Center baixada anteriormente, selecione-a e clique em **Open** (Abrir).

O nome da unidade USB conectada deve estar listado no ícone da unidade. Se não estiver:

1. Clique em **Select drive** (Selecionar unidade).
2. Clique no botão de opção da unidade USB correta e, em seguida, clique em **Continue** (Continuar).

Etapa 7 Clique em **Flash!** para copiar a imagem ISO para a unidade USB.

O entalhe configura a unidade USB como uma unidade bootable com a imagem ISO do Cisco DNA Center instalada.

Refazer a imagem do dispositivo

Pode haver situações que exigem que você refaça a imagem do dispositivo Cisco DNA Center, como a recuperação de um backup ou a alteração da configuração do link de cluster. Para fazer isso, conclua o procedimento a seguir.

Etapa 1 Baixe a imagem ISO do Cisco DNA Center e verifique se é uma imagem autêntica da Cisco.

Consulte "Verificar a imagem ISO do Cisco DNA Center".

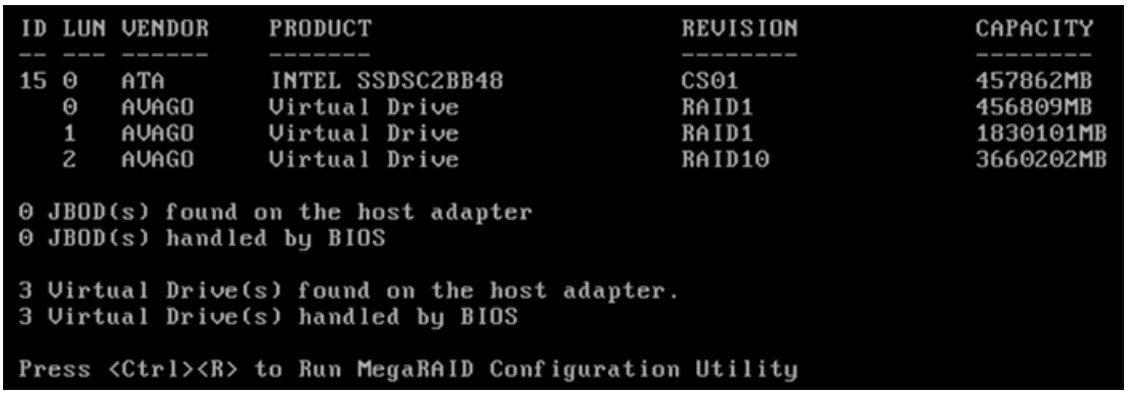
Etapa 2 Crie uma unidade USB Bootable que contenha a imagem ISO do Cisco DNA Center.

Consulte "Criar uma unidade USB Bootable".

Etapa 3 Reinicialize as três unidades virtuais que são gerenciadas pelo controlador RAID do dispositivo:

a) Faça login no Cisco IMC e inicie uma sessão KVM.
b) Ligue ou ligue e desligue o dispositivo escolhendo uma das seguintes opções de menu:
   - **Power** > **Power On System** (Ligar > Ligar o sistema)
   - **Power** > **Power Cycle System (cold boot)** (Ligar > Desligar e ligar o sistema [inicialização a frio])

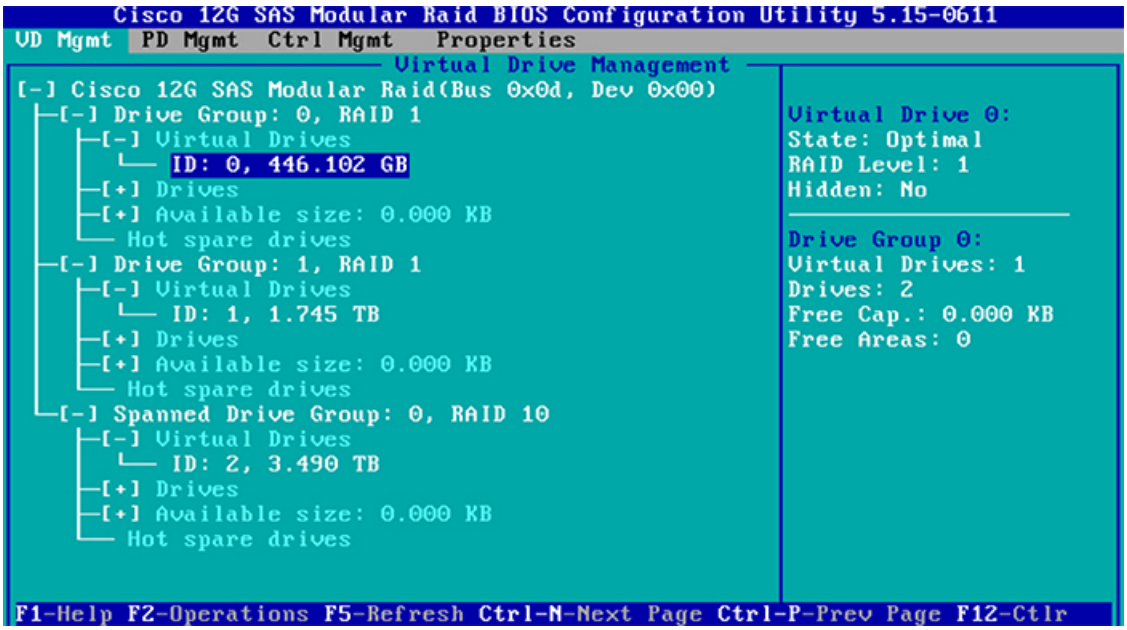
À medida que o dispositivo é reinicializado, uma tela que lista cada unidade no dispositivo (física e virtual) será exibida.



c) Assim que você vir esta tela, pressione **Ctrl + R** para executar o utilitário de configuração do MegaRAID.

Se você esperar muito tempo, esta tela desaparecerá. Para voltar a esta tela, escolha **Power** > **Reset System (warm boot)** (Ligar > Reiniciar o sistema [inicialização a quente]) no menu KVM para reinicializar o dispositivo.

d) Selecione uma entrada da unidade (`ID: 0, 446.102 GB`, por exemplo) e, em seguida, pressione **F2**.



Isso abre a tela da unidade **Advanced Properties** (Propriedades avançadas).

e) No menu resultante, escolha **Initialization > Fast Initialization** (Inicialização > Inicialização rápida).

f) Repita as etapas de 3B a 3E para as outras unidades virtuais no dispositivo.

Etapa 4 Reinstale Cisco DNA Center no dispositivo.

Consulte "Instalar a imagem ISO do Cisco DNA Center".

Instalar a imagem ISO do Cisco DNA Center

Conclua o procedimento a seguir para instalar a imagem ISO do Cisco DNA Center no dispositivo.

Antes de Iniciar

- Crie a unidade USB Bootable da qual você vai instalar a imagem ISO do Cisco DNA Center. Consulte "Criar uma unidade USB Bootable".
- Se outra versão do Cisco DNA Center já estiver instalada no dispositivo, conclua o procedimento descrito em "Refazer a imagem do dispositivo".

Etapa 1 Conecte a unidade USB Bootable com a imagem ISO do Cisco DNA Center ao dispositivo.

Etapa 2 Faça login no CIMC e inicie uma sessão KVM.

Etapa 3 Ligue apenas ou ligue e desligue o dispositivo:

- Selecione **Power** > **Power On System** (Ligar > Ligar o sistema) se o dispositivo não estiver em execução no momento.
- Escolha **Power** > **Power Cycle System (cold boot)** (Ligar > Desligar e ligar o sistema [inicialização a frio]) se o dispositivo já estiver em execução.

Etapa 4 Na janela pop-up resultante, clique em **Yes** (Sim) para confirmar que você está prestes a executar uma ação de controle de servidor.

Etapa 5 Quando o logotipo da Cisco aparecer, pressione a tecla **F6** ou escolha **Macros** > **User Defined Macros** > **F6** (Macros > Macros definidas pelo usuário) no menu KVM.

O menu de seleção de dispositivos de inicialização é exibido.

Etapa 6 Selecione a unidade USB e pressione **Enter**.

Etapa 7 Na janela **GNU GRUB** do carregador de DP, escolha **Manufacture Cisco DNA Appliance** (Manufatura do dispositivo Cisco DNA) e pressione **Enter**.

Observação Caso você não faça uma seleção em 30 segundos, o bootloader inicializará automaticamente o instalador do Maglev. Certifique-se de fazer a seleção antes desse período.

Quando a instalação da imagem ISO do Cisco DNA Center é concluída, o instalador é reinicializado e abre o assistente de configuração do Maglev.

Configurar o nó mestre

Execute as seguintes etapas para configurar o primeiro dispositivo instalado como o nó mestre. Configure sempre em primeiro lugar o dispositivo como o nó mestre, independentemente se ele for operado como autônomo ou parte de um cluster.

Se você estiver configurando o dispositivo instalado como um nó complementar para um cluster atual que já tenha um nó mestre, siga as etapas em " Configurar os nós complementares".

Importante Para cada dispositivo no cluster, configure os servidores DNS em apenas uma das interfaces. Pode ocorrer problemas se você configurar servidores DNS em várias interfaces.

Antes de Iniciar

Certifique-se de que você:

- Coletou todas as informações necessárias em Sub-redes necessárias e endereços IP adicionais (Endereços IP e sub-redes necessárias) e Informações de configuração obrigatórias (Informações de configuração obrigatórias).
- Instalou o primeiro dispositivo conforme descrito no Fluxo de trabalho de instalação do dispositivo.
- Configurou o acesso do navegador CIMC no nó mestre, conforme descrito em Ativar acesso do navegador ao CIMC.
- Verificou se as portas do dispositivo do nó mestre e os switches que ele usa estão configurados corretamente, conforme descrito em Executar verificações preliminares.
- Esteja usando um navegador compatível com CIMC e Cisco DNA Center. Para obter uma lista de navegadores compatíveis, consulte as notas da versão do Cisco DNA Center que você está instalando.
- Ativou o ICMP no firewall entre o Cisco DNA Center e o servidor DNS que será especificado na etapa 8 do procedimento a seguir. O assistente de configuração do Maglev usa ping para verificar o servidor DNS especificado. Esse ping pode ser bloqueado se houver um firewall entre Cisco DNA Center e o servidor DNS, e o ICMP não estiver ativado nesse firewall. Quando isso acontecer, você não poderá concluir o assistente.

Etapa 1 Aponte o navegador para o endereço IP CIMC definido durante a configuração da interface de usuário do CIMC que você executou e faça login na interface de usuário do CIMC como o usuário CIMC (consulte Ativar acesso do navegador ao CIMC).

Após o login bem-sucedido, o dispositivo exibe a janela **Cisco Integrated Management Controller Chassis Summary** (Resumo do chassi do Cisco Integrated Management Controller), com um menu de link azul no canto superior direito, como mostrado abaixo.

Etapa 2 No menu de link azul, escolha **Launch KVM** (Iniciar KVM) e, em seguida, selecione o **KVM baseado em Java** ou o **KVM baseado em HTML**. Se você selecionar o KVM baseado em Java, precisará iniciar o arquivo de inicialização do Java no navegador ou no Gerenciador de arquivos para visualizar o console KVM em sua própria janela. Se você

selecionar o KVM baseado em HMTL, ele iniciará automaticamente o console KVM em uma janela do navegador ou em uma guia separada.

Independentemente do tipo de KVM escolhido, use o console KVM para monitorar o progresso da configuração e responder aos prompts do assistente de configuração do Maglev.

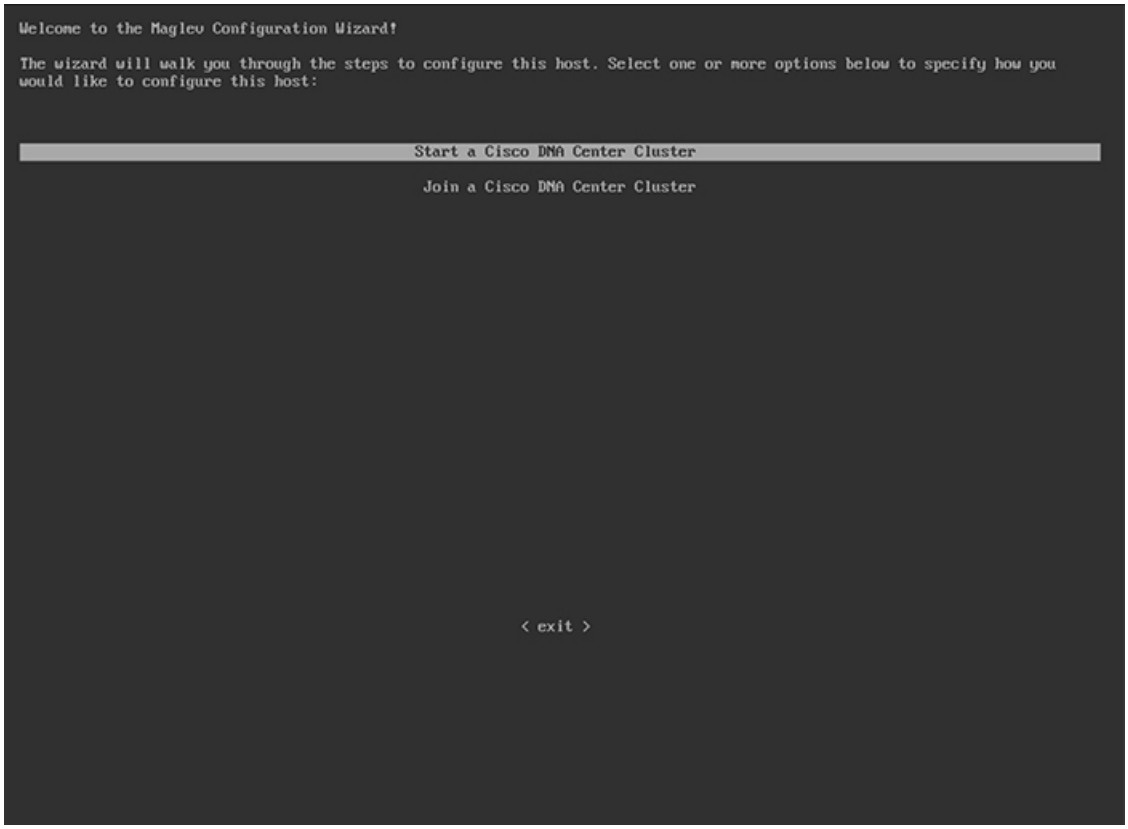
Etapa 3 Com o KVM exibido, reinicialize o dispositivo fazendo uma das seguintes seleções:

a) Na janela principal do navegador da interface do usuário CIMC: escolha **Host Power** > **Power Cycle** (Alimentação do host > Desligar e ligar). Em seguida, alterne para o console do KVM para continuar.

b) No console do KVM, selecione **Power** > **Power Cycle System (cold boot)** (Desligar e ligar o sistema [inicialização a frio].

Se for solicitado que você confirme a escolha para reiniciar o dispositivo, clique em **OK**.

Após exibir as mensagens de reinicialização, o console KVM exibe a tela de boas-vindas do assistente de configuração do Maglev, mostrada abaixo.



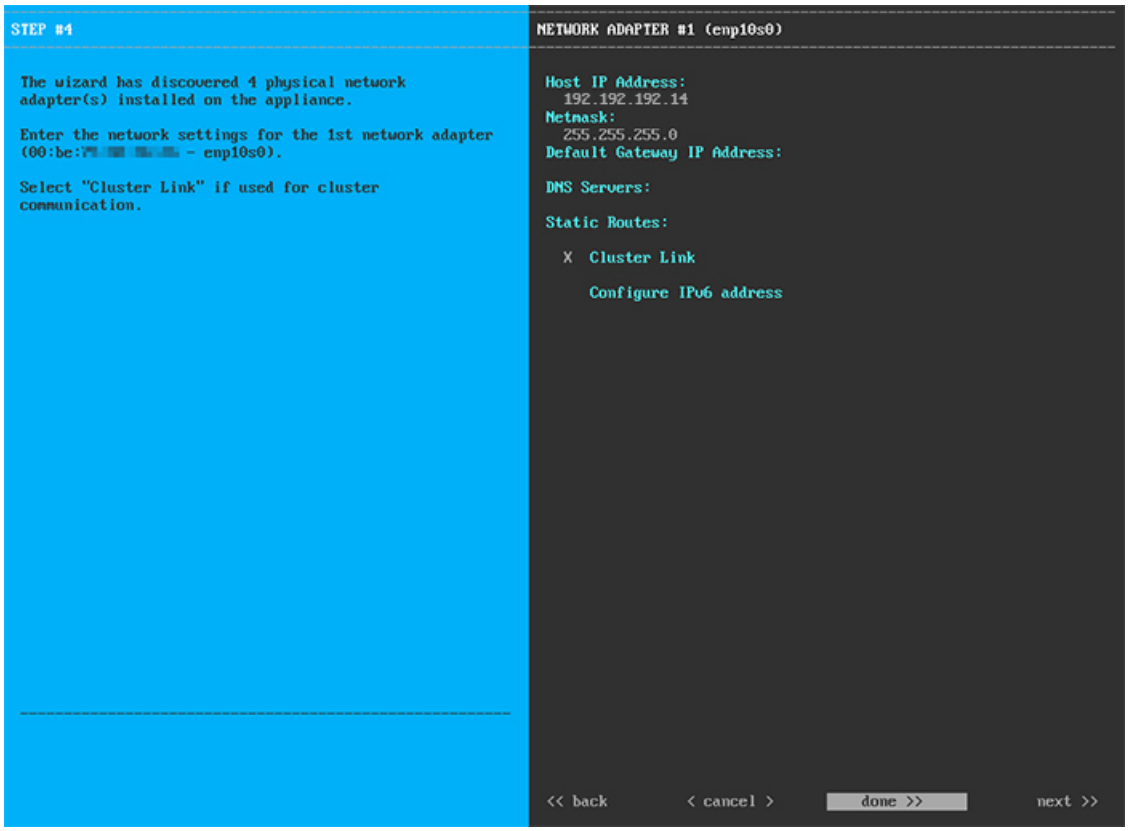
Etapa 4 Escolha **Start a DNA-C cluster** (Iniciar um cluster DNA-C) para começar a configurar o nó mestre.

O assistente descobre todas as portas no dispositivo e as apresenta uma por uma, em telas separadas, na seguinte ordem:

1. Porta de cluster 10 Gbps (porta 2, enp10s0, adaptador de rede 1)
2. Porta de interface de usuário do Cisco DNA Center de 1 Gbps (1, Enp1s0f0, adaptador de rede 2)
3. Porta de nuvem de 1 Gbps (2, Enp1s0f0, adaptador de rede 3)
4. Porta empresarial de 10 Gbps (porta 1, enp9s0, adaptador de rede 4)

Observação Caso o assistente não mostre uma ou ambas as portas de 10 Gbps durante a configuração, essas portas não estão funcionando ou estão desativadas. Essas portas de 10 Gbps são necessárias para a funcionalidade do Cisco DNA Center. Se você descobrir que não estão funcionando, escolha **Cancel** (Cancelar) para sair da configuração imediatamente. Verifique se você concluiu todas as etapas fornecidas em Executar verificações preliminares, antes de retomar à configuração ou entrar em contato com o Cisco Technical Assistance Center (TAC).

Etapa 5 O assistente descobre a porta de cluster 10 Gbps (porta 2, enp10s0) primeiro e a apresenta como **ADAPTADOR DE REDE 1**. Como explicado em Conexões de cabo de interface, essa porta é usada para vincular o dispositivo ao cluster, portanto, aplique o endereço IP do host, a máscara de rede e outros valores apropriados para essa finalidade (consulte Sub-redes necessárias e endereços IP adicionais e Informações de configuração obrigatórias para obter os valores a serem inseridos.



Insira os valores de configuração do **ADAPTADOR DE REDE 1** como mostrado na tabela abaixo.

Tabela 22: Entradas do nó mestre para o adaptador de rede 1: porta de cluster de 10 Gbps (enp10s0)

Endereço IP do host	Digite o endereço IP da porta de cluster. Isso é obrigatório. Observe que você não pode alterar posteriormente o endereço da porta de cluster.
Máscara de rede	Insira a máscara de rede para o endereço IP da porta. Isso é obrigatório.

Endereço IP do gateway padrão	Insira um endereço IP de gateway padrão para usar na porta. Isso geralmente é obrigatório apenas na porta corporativa.
Servidores DNS	Digite o endereço IP do servidor DNS preferencial. Se inserir vários servidores DNS, separe os endereços IP na lista com espaços.
Rotas estáticas	Insira uma ou mais rotas estáticas no formato a seguir, separadas por espaços: <rede>/<máscara de rede>/<gateway>. Isso geralmente é obrigatório apenas na porta da interface de usuário.
Link de cluster	Marque a caixa de seleção para indicar que essa porta será o link para um cluster. Isso é obrigatório somente na porta de cluster.
Configurar endereço IPv6	Reservado para uso futuro. Deixe este campo em branco.

Quando terminar de inserir os valores de configuração, insira **next >>** para continuar. Após inserir **next>>**, o assistente valida os valores que você inseriu e emite uma mensagem de erro, se houver algum incorreto. Se você receber uma mensagem de erro, verifique se o valor inserido está correto e insira-o novamente. Se necessário, selecione **<<back** para inseri-lo novamente.

Etapa 6 Após a validação bem-sucedida dos valores de porta de cluster que você digitou, o Assistente apresenta a porta de interface de usuário do Cisco DNA Center de 1 Gbps (1, enp1s0f0) como **ADAPTADOR DE REDE 2**. Como explicado nas Conexões de cabo de interface, essa porta é usada para acessar a interface de usuário do Cisco DNA Center na rede de gerenciamento. Aplique o endereço IP do host, a máscara de rede e outros valores apropriados para essa finalidade (consulte Sub-redes necessárias e endereços IP adicionais e Informações de configuração obrigatórias para obter os valores a serem inseridos).

Insira os valores de configuração do **ADAPTADOR DE REDE 2** como mostrado na tabela abaixo.

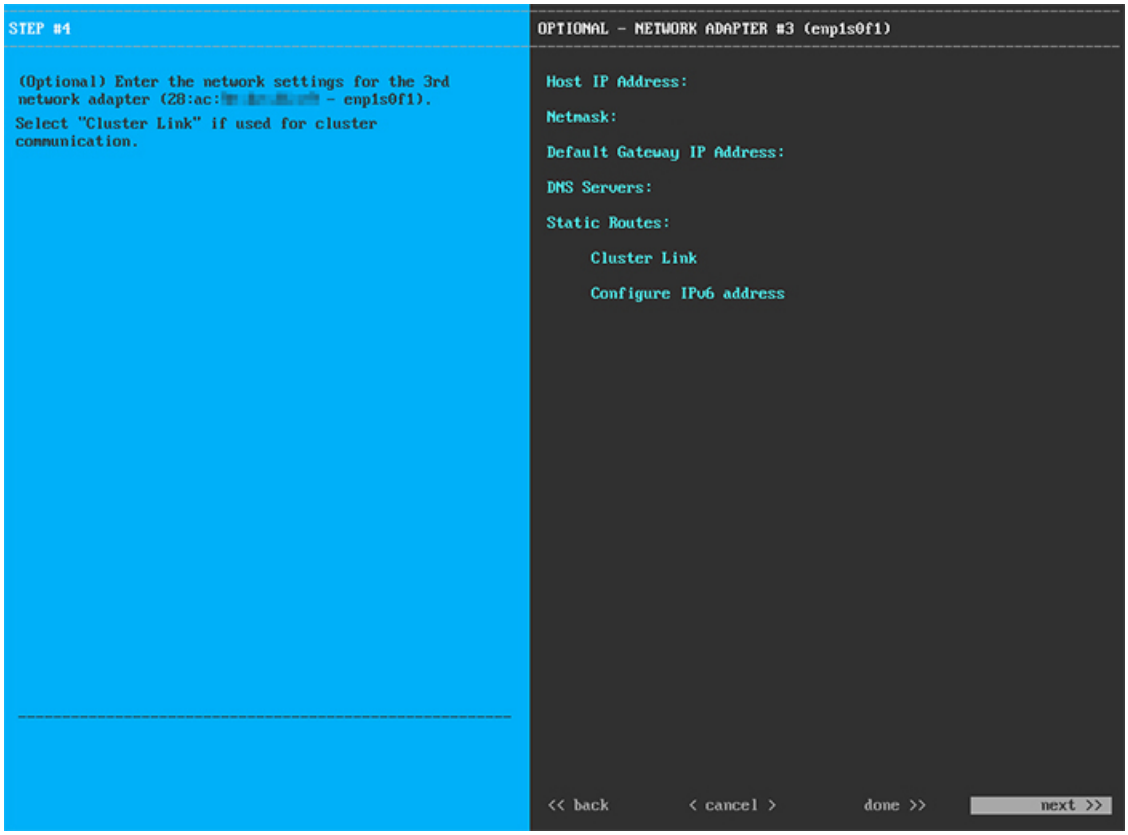
Tabela 23: Entradas do nó mestre para o adaptador de rede 2: porta de interface de usuário de 1 Gbps (enp1s0f0)

Endereço IP do host	Insira o endereço IP para a porta de interface de usuário de 1 Gpbs. Isso é obrigatório.
Máscara de rede	Insira a máscara de rede para o endereço IP da porta. Isso é obrigatório.
Endereço IP do gateway padrão	Insira um endereço IP de gateway padrão para usar na porta. Isso geralmente é obrigatório apenas na porta corporativa.
Servidores DNS	Digite o endereço IP do servidor DNS preferencial. Se inserir vários servidores DNS, separe os endereços IP na lista com espaços. **Observação** Para NTP, verifique se a porta 121 (UDP) está aberta entre Cisco DNA Center e o servidor NTP.
Rotas estáticas	Insira uma ou mais rotas estáticas no formato a seguir, separadas por espaços: <rede>/<máscara de rede>/<gateway>.

Link de cluster	Deixe este campo em branco. É obrigatório somente na porta de cluster.
Configurar endereço IPv6	Reservado para uso futuro. Deixe este campo em branco.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores.

Etapa 7 Após a validação bem-sucedida dos valores de porta de interface de usuário de Cisco DNA Center inseridos, o assistente apresenta a porta de nuvem de 1 Gbps (2, enp1s0f1) como **ADAPTADOR DE REDE 3**. Como explicado em Conexões de cabo de interface, essa é uma porta opcional usada para vincular o dispositivo à Internet quando não for possível fazer isso através da porta de 10 Gbps empresarial (porta 1, enp9s0). Aplique o endereço IP do host, a máscara de rede e outros valores apropriados para essa finalidade (consulte Sub-redes necessárias e endereços IP adicionais e Informações de configuração obrigatórias para obter os valores a serem inseridos).



Insira os valores de configuração do **ADAPTADOR DE REDE 3** como mostrado na tabela abaixo.

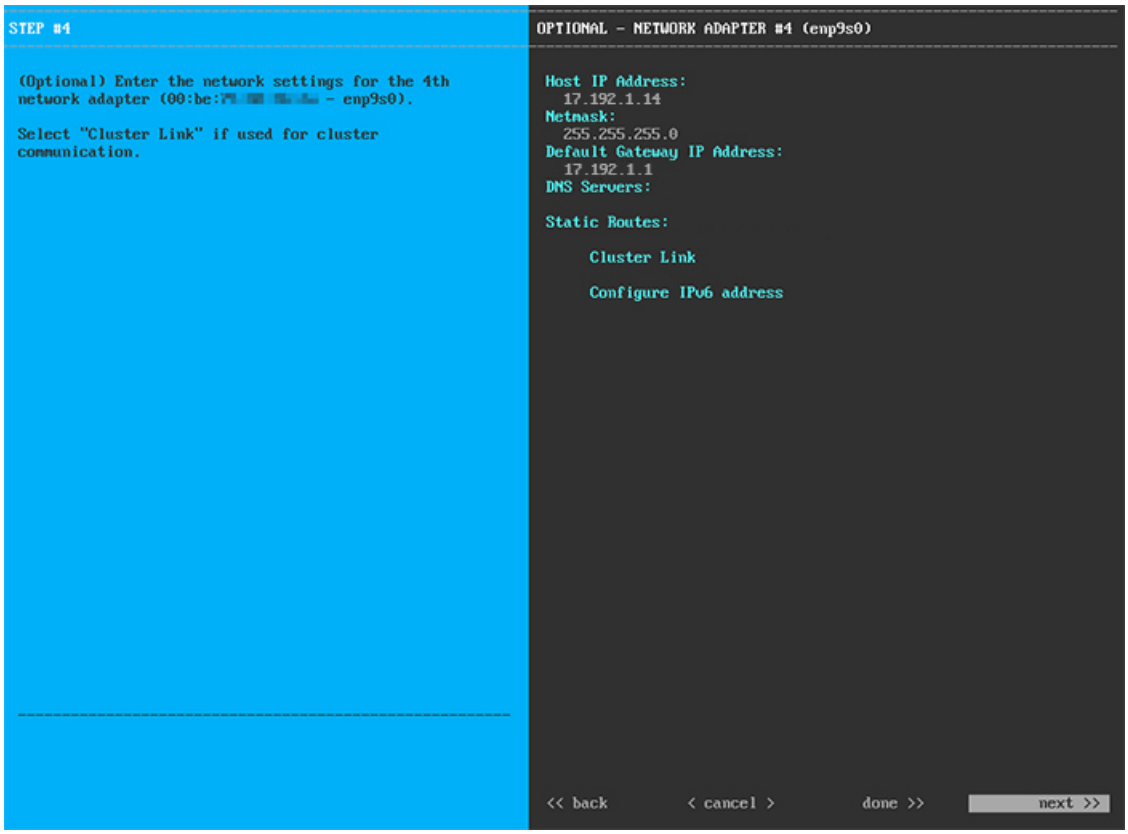
Tabela 24: Entradas do nó mestre para o adaptador de rede 3: porta de nuvem de 1 Gbps (enp1s0f1)

Endereço IP do host	Digite o endereço IP da porta de nuvem. Isso é obrigatório somente se você estiver usando a porta de nuvem para conexão com a Internet; caso contrário, pode deixá-lo em branco.
Máscara de rede	Insira a máscara de rede para o endereço IP da porta. Isso será obrigatório se você inserir um endereço IP.

Endereço IP do gateway padrão	Insira um endereço IP de gateway padrão para usar a porta de nuvem. Isso geralmente é obrigatório apenas na porta corporativa.
Servidores DNS	Digite o endereço IP do servidor DNS preferencial. Se inserir vários servidores DNS, separe os endereços IP na lista com espaços.
Rotas estáticas	Insira uma ou mais rotas estáticas no formato a seguir, separadas por espaços: <rede>/<máscara de rede>/<gateway>. Isso geralmente é obrigatório apenas na porta da interface de usuário do Cisco DNA Center.
Link de cluster	Deixe este campo em branco. É obrigatório somente na porta de cluster.
Configurar endereço IPv6	Reservado para uso futuro. Deixe este campo em branco.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores.

Etapa 8 Após a validação bem-sucedida dos valores de porta na nuvem que você inseriu, o assistente apresenta a porta de 10 Gbps empresarial (porta 1, enp9s0) como **ADAPTADOR DE REDE 4**. Como explicado em Conexões de cabo de interface, essa é uma porta obrigatória usada para vincular o dispositivo à rede corporativa. Aplique o endereço IP do host, a máscara de rede e outros valores apropriados para essa finalidade (consulte Sub-redes necessárias e endereços IP adicionais e Informações de configuração obrigatórias para obter os valores a serem inseridos).



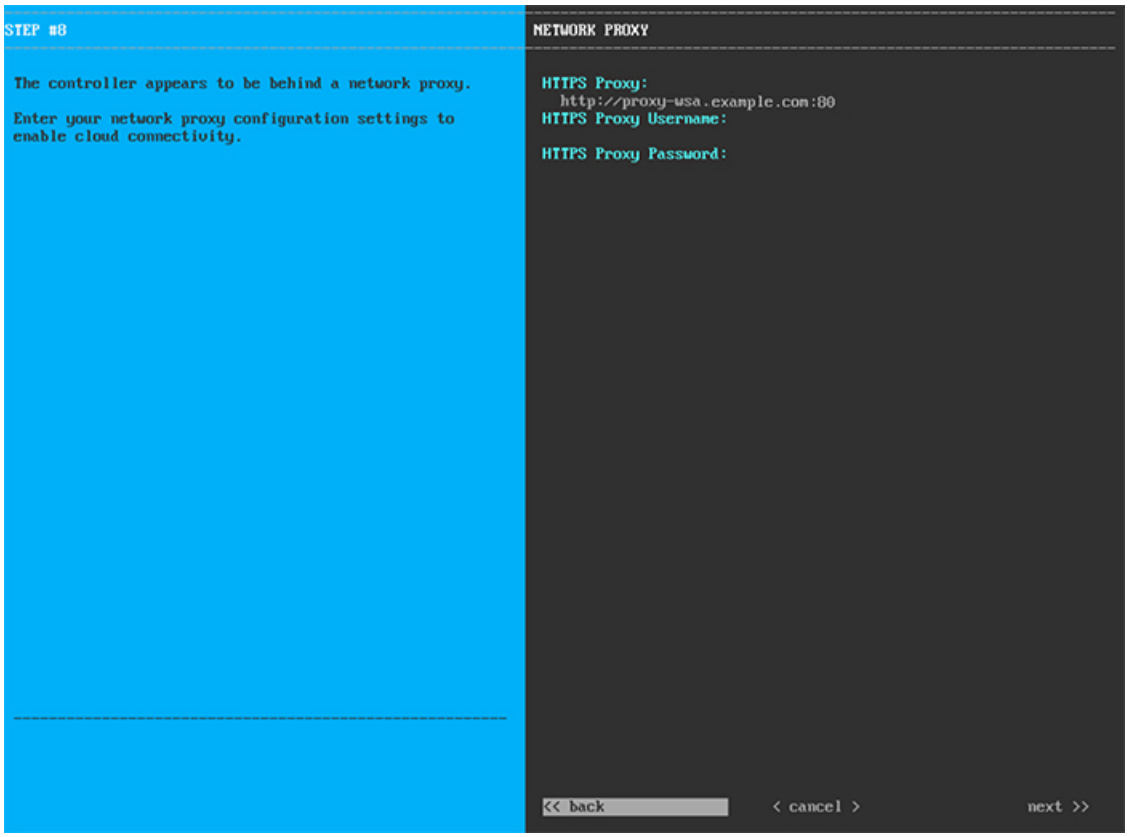
Insira os valores de configuração do **ADAPTADOR DE REDE 4** como mostrado na tabela abaixo.

Tabela 25: Entradas do nó mestre para o adaptador de rede 4: porta empresarial de 10 Gbps (enp9s0)

Endereço IP do host	Digite o endereço IP para a porta empresarial de 10 Gpbs. Isso é obrigatório.
Máscara de rede	Insira a máscara de rede para o endereço IP da porta. Isso é obrigatório.
Endereço IP do gateway padrão	Insira um endereço IP de gateway padrão para usar na porta. Isso é obrigatório.
Servidores DNS	Digite o endereço IP do servidor DNS preferencial. Se inserir vários servidores DNS, separe os endereços IP na lista com espaços.
Rotas estáticas	Insira uma ou mais rotas estáticas no formato a seguir, separadas por espaços: <rede>/<máscara de rede>/<gateway>. Isso geralmente é obrigatório apenas na porta da interface de usuário do Cisco DNA Center.
Link de cluster	Deixe este campo em branco. É obrigatório somente na porta de cluster.
Configurar endereço IPv6	Reservado para uso futuro. Deixe este campo em branco.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores. O assistente validará e aplicará as configurações do adaptador de rede.

Etapa 9 Quando a configuração do adaptador de rede estiver concluída, o assistente solicitará que você insira os valores de configuração para o **NETWORK PROXY** (PROXY DE REDE) que está usando, como mostrado abaixo.



Insira valores de configuração para o **NETWORK PROXY** (PROXY DE REDE), conforme mostrado na tabela abaixo.

Tabela 26: Entradas do nó mestre para o proxy de rede

Proxy HTTPS	Digite a URL ou o nome do host de um proxy de rede HTTPS usado para acessar a Internet. **Observação** A conexão do Cisco DNA Center ao proxy HTTPS é compatível apenas via http nesta versão.
Nome de usuário do proxy HTTPS	Insira o nome de usuário usado para acessar o proxy de rede. Se nenhum login de proxy for necessário, deixe este campo em branco.
Senha do proxy HTTPS	Insira a senha usada para acessar o proxy de rede. Se nenhum login de proxy for necessário, deixe este campo em branco.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores.

Etapa 10 Quando a configuração do proxy de rede for concluída, o assistente solicitará que você insira endereços IP virtuais para o nó mestre, em **MAGLEV CLUSTER DETAILS** (DETALHES DO CLUSTER MAGLEV), como mostrado abaixo.

Insira uma lista separada por espaços dos endereços IP virtuais usados para o tráfego entre o cluster e a rede. Isso é obrigatório para clusters de três nós e clusters de nó único que serão convertidos em um cluster de três nós no futuro. Se você tiver uma configuração de cluster de nó único e planeja continuar com ela, pule esta etapa e prossiga para a etapa 11.

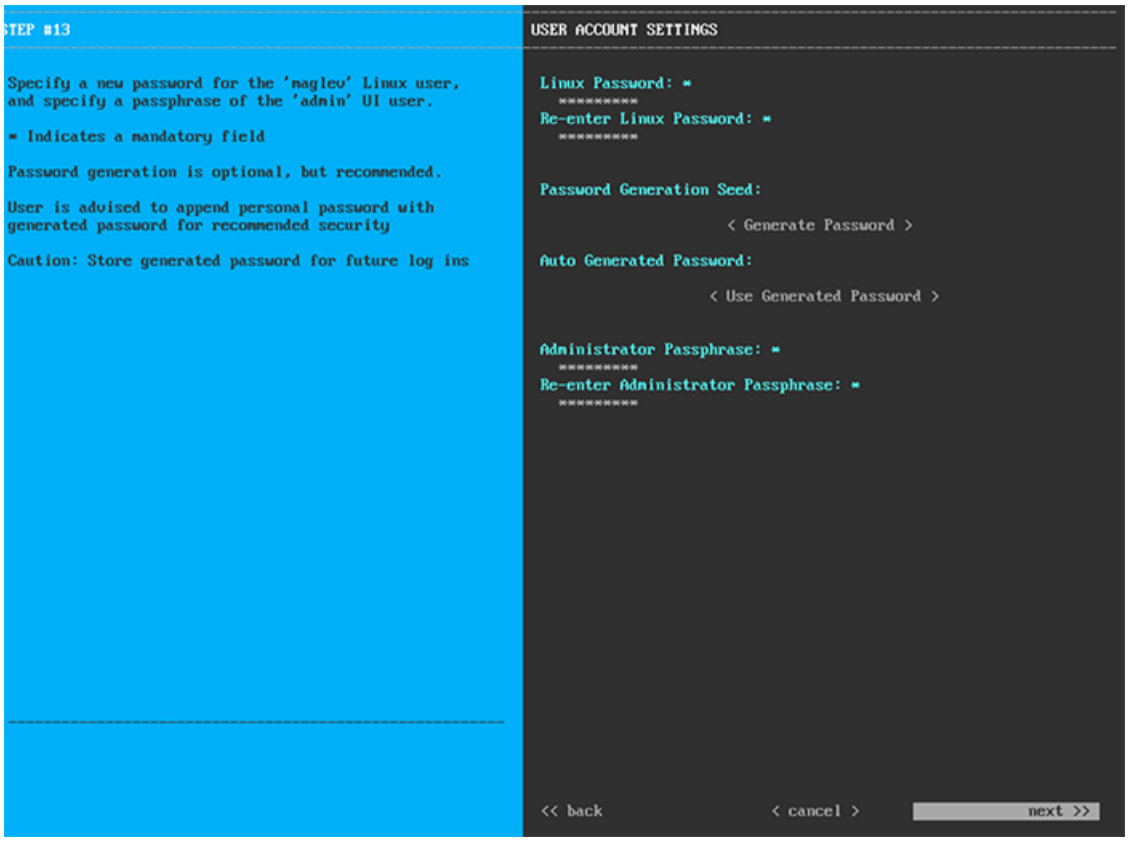
Importante Você deve inserir um endereço IP virtual para cada interface de rede configurada. Só será possível concluir o assistente, se você fizer isso. Esses endereços estão vinculados ao status do link do cluster, que deve estar no estado **UP** (ATIVO).

Você também tem a opção de especificar o nome de domínio totalmente qualificado (FQDN) para o cluster. O Cisco DNA Center faz o seguinte com este nome de host:

- Ele usa esse nome de host para acessar a interface da Web do cluster e as APIs REST (Representational State Transfer) usadas por dispositivos na rede empresarial que Cisco DNA Center gerencia.
- No campo Subject Alternative Name (SAN) (Nome alternativo de entidade) de certificados do Cisco DNA Center, ele usa o FQDN para definir o servidor Plug and Play para o provisionamento de dispositivos.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores.

Etapa 11 Quando os endereços IP virtuais forem inseridos, o assistente solicitará que você insira os valores de **USER ACCOUNT SETTINGS** (CONFIGURAÇÕES DE CONTA DO USUÁRIO), como mostrado abaixo.



Insira os valores de **USER ACCOUNT SETTINGS** (CONFIGURAÇÕES DE CONTA DE USUÁRIO), conforme mostrado na tabela abaixo.

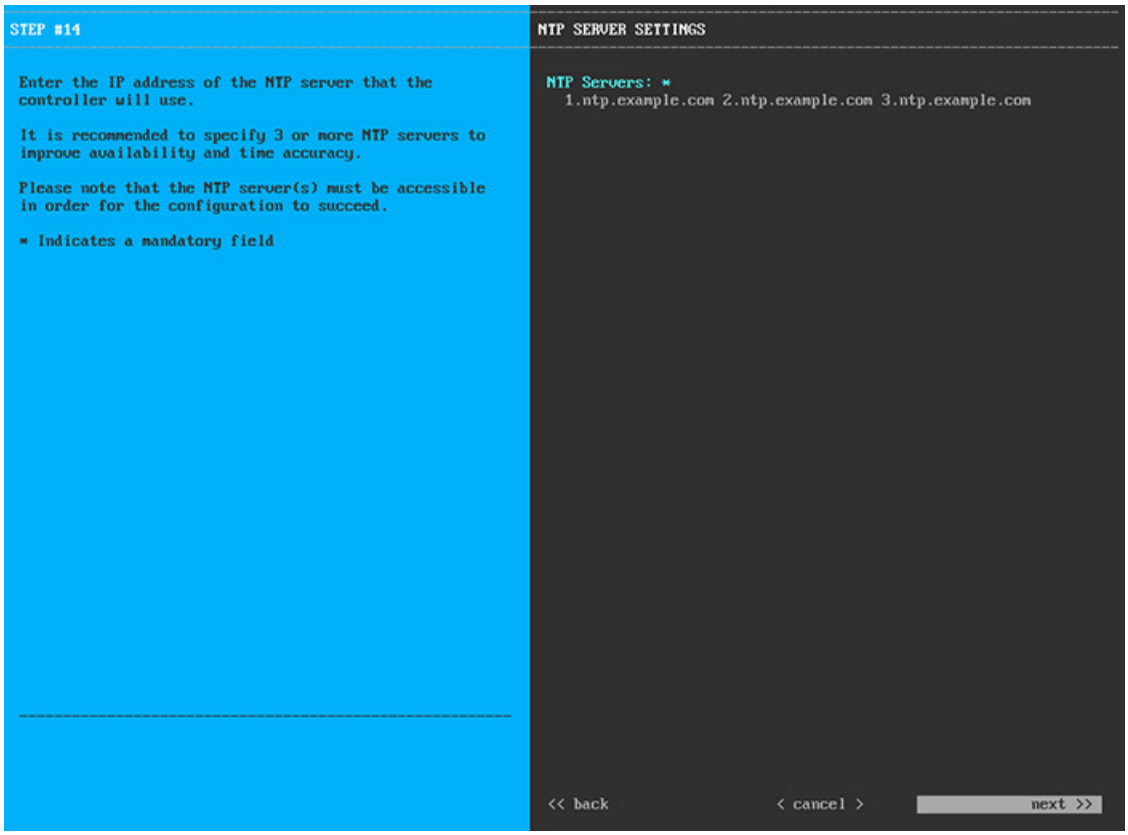
Tabela 27: Entradas de nó mestre para configurações de conta de usuário

Senha do Linux	Insira uma senha de Linux para o usuário Maglev.
Insira novamente a senha do Linux	Confirme a senha do Linux inserindo-a uma segunda vez.
Propagação de geração de senha	Se você não quiser criar a senha do Linux, insira uma frase de propagação neste campo e pressione <**Generate Password**> (Gerar senha) para gerar a senha.
Senha gerada automaticamente	(Opcional) A frase de propagação aparece como parte de uma senha aleatória e segura. Se desejar, você pode usar essa senha "como está" ou pode editar a senha gerada automaticamente. Pressione <**Use Generated Password**> (Usar a senha gerada) para salvar a senha.
Senha do administrador	Insira uma senha para o superusuário do administrador padrão, usada para fazer login no Cisco DNA Center pela primeira vez.

Insira novamente a senha do administrador	Confirme a senha do administrador inserindo-a uma segunda vez.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores.

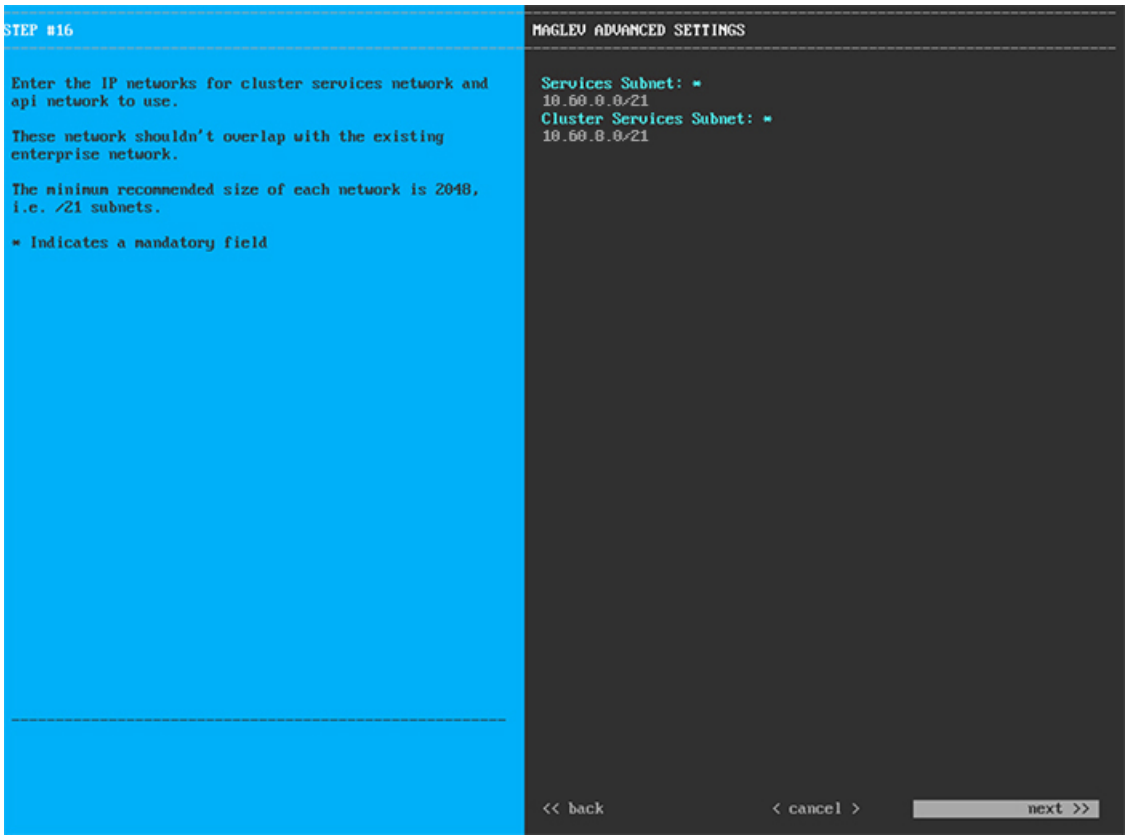
Etapa 12 Quando os detalhes da conta de usuário forem inseridos, o assistente solicitará que você insira os valores de **NTP SERVER SETTINGS** (CONFIGURAÇÕES DO SERVIDOR NTP), como mostrado abaixo.



Insira um ou mais endereços de servidor NTP ou nomes de host, separados por espaços. Pelo menos um endereço ou nome de host NTP é obrigatório. Para uma implantação de produção, a Cisco recomenda que você configure um mínimo de três servidores NTP.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores. O assistente validará e aplicará a configuração do servidor NTP.

Etapa 13 Depois de especificar os servidores NTP, o assistente solicitará que você insira valores para **MAGLEV ADVANCED SETTINGS** (CONFIGURAÇÕES AVANÇADAS DO MAGLEV), como mostrado abaixo.



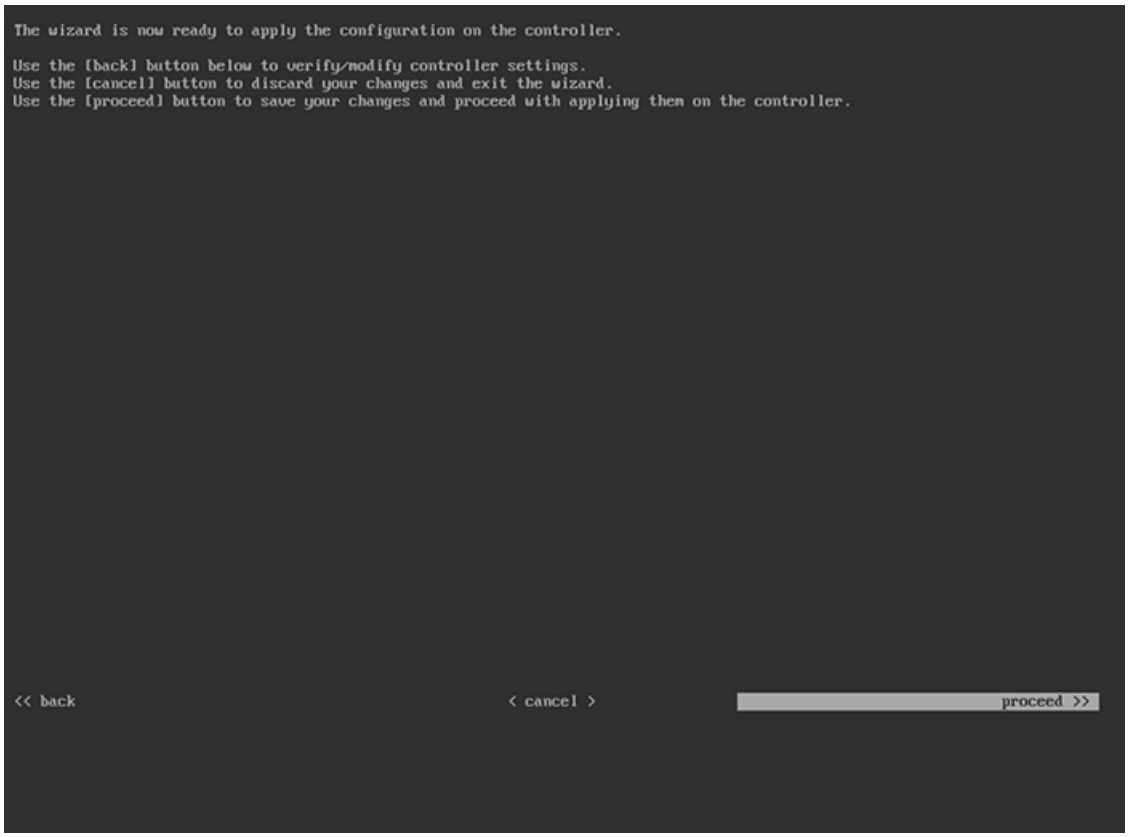
Insira os valores de configuração para **MAGLEV ADVANCED SETTINGS** (CONFIGURAÇÕES AVANÇADAS DO MAGLEV), conforme mostrado na tabela abaixo.

Tabela 28: Entradas do nó mestre para configurações avançadas do Maglev

Sub-rede de serviços	Insira uma sub-rede IP dedicada ao Cisco DNA Center, para usar no gerenciamento de seus próprios serviços.
Sub-rede de serviços de cluster	Insira uma sub-rede IP dedicada ao Cisco DNA Center, para usar no gerenciamento dos serviços de clustering.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores.

Etapa 14 Quando você terminar de inserir as configurações avançadas do Maglev, uma mensagem final será exibida informando que o assistente está pronto para continuar com a aplicação da configuração, como mostrado abaixo.



Insira **proceed>>** para concluir a configuração.

O host será reinicializado automaticamente e exibirá mensagens no console do KVM, enquanto aplica as configurações e mostra os serviços. Esse processo pode levar várias horas. Você pode monitorar o progresso pelo console do KVM.

No final do processo de configuração, o dispositivo desliga e liga novamente, em seguida, é exibida uma mensagem **CONFIGURATION SUCCEEDED!** (CONFIGURAÇÃO BEM-SUCEDIDA!).

O que Fazer Depois

Quando esta tarefa estiver concluída:

- Se você estiver implantando este dispositivo somente no modo autônomo, continue executando a configuração inicial: Fluxo de trabalho de primeira configuração.
- Se você estiver implantando esse dispositivo Cisco DNA Center como o nó mestre em um cluster, configure o segundo e terceiro dispositivos instalados no cluster: Configurar os nós complementares.

Configurar os nós complementares

Siga as etapas deste procedimento para configurar o segundo e terceiro dispositivos no cluster.

Importante Para cada dispositivo no cluster, configure os servidores DNS em apenas uma das interfaces. Pode ocorrer problemas se você configurar servidores DNS em várias interfaces.

Ao ingressar em cada novo nó complementar no cluster, você deve especificar o primeiro host no cluster como o nó mestre. Observe o seguinte ao unir os nós complementares a um cluster:

- Não se esqueça de entrar em um único nó no cluster de cada vez. Não tente adicionar vários nós ao mesmo tempo, pois isso resultará em um comportamento imprevisível.
- Antes de adicionar um novo nó ao cluster, certifique-se de que todos os pacotes instalados sejam implantados no nó mestre. Você pode verificar isso usando o Secure Shell para fazer login na interface de usuário do Cisco DNA Center do nó mestre como usuário Linux (maglev) e, em seguida, executar o comando `maglev package status`. Todos os pacotes instalados devem aparecer na saída do comando como `DEPLOYED` (IMPLANTADOS). No exemplo a seguir, os pacotes application-policy, sd-access, sensor-assurance e sensor-automation não foram instalados, portanto, são os únicos pacotes cujo status é `NOT_DEPLOYED` (NÃO IMPLANTADOS). O status do pacote deve ser semelhante a isso antes de configurar um nó complementar.

```
$ ssh maglev@172.29.131.14 -p 2222
The authenticity of host '[172.29.131.14]:2222 ([172.29.131.14]:2222)' can't be
established.
ECDSA key fingerprint is SHA256:scye+2ll6NFHAkOZDs0cNLHBR75j1KV3ZXIKuUaiadk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[172.29.131.14]:2222' (ECDSA) to the list of known hosts.
Welcome to the Maglev Appliance
maglev@172.29.131.14's password:

Welcome to the Maglev Appliance

System information as of Thu Dec 20 03:07:13 UTC 2018

System load: 4.08                   IP address for enp9s0: 17.192.1.14
Usage of /: 59.8% of 28.03GB        IP address for enp10s0: 192.192.192.14
Memory usage: 21%                   IP address for enp1s0f0: 172.29.131.14
Swap usage: 0%                      IP address for docker0: 169.254.0.1
Processes: 831                      IP address for tun10: 10.60.3.0
Users logged in: 0

To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.

[Thu Dec 20 03:07:13 UTC] maglev@192.192.192.14 (maglev-master-1) ~
$ maglev package status
[administration] password for 'admin':

maglev-1 [main - https://kong-frontend.maglev-system.svc.cluster.local:443]

NAME                            DEPLOYED        AVAILABLE       STATUS
-------------------------------------------------------------------------------------
application-policy              -               2.1.10.170000   NOT_DEPLOYED
assurance                       1.0.5.686       1.1.8.1440      DEPLOYED
automation-core                 2.1.8.60044     2.1.12.60011    DEPLOYED
base-provision-core             2.1.8.60044     2.1.12.60016    DEPLOYED
command-runner                  2.1.8.60044     2.1.9.60029     DEPLOYED
device-onboarding               2.1.8.60044     2.1.12.60016    DEPLOYED
image-management                2.1.8.60044     2.1.12.60011    DEPLOYED
ncp-system                      2.1.8.60044     2.1.9.60029     DEPLOYED
ndp-base-analytics              1.0.7.878       1.0.7.908       DEPLOYED
ndp-platform                    1.0.7.829       1.0.7.866       DEPLOYED
```

```
ndp-ui                          1.0.7.956       1.0.7.975       DEPLOYED
network-visibility              2.1.8.60044     2.1.12.60016    DEPLOYED
path-trace                      2.1.8.60044     2.1.12.60016    DEPLOYED
sd-access                       -               2.1.12.60016    NOT_DEPLOYED
sensor-assurance                -               1.1.5.40        NOT_DEPLOYED
sensor-automation               -               2.1.9.60029     NOT_DEPLOYED
system                          1.0.4.807       1.0.4.855       DEPLOYED
```

- Espere algum tempo de inatividade do serviço durante o processo de anexação de cluster para cada nó complementar. Os serviços precisarão ser redistribuídos nos nós e o cluster ficará inativo por alguns períodos durante o processo.

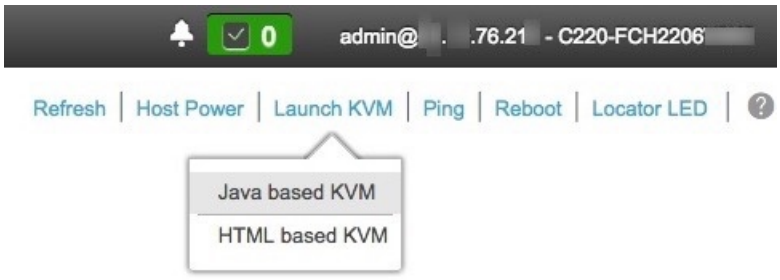
Antes de Iniciar

Certifique-se de que você:

- Configurou o primeiro dispositivo no cluster, seguindo as etapas em Configurar o nó mestre.
- Coletou todas as informações necessárias em Sub-redes necessárias e endereços IP adicionais e Informações de configuração obrigatórias.
- Instalou o segundo e terceiro dispositivos, conforme descrito no Fluxo de trabalho de instalação do dispositivo.
- Configurou o acesso do navegador CIMC em ambos os dispositivos complementares, conforme descrito em Ativar acesso do navegador ao CIMC.
- Verificou se as portas dos dispositivos do nó complementar e os switches que eles usam estão configurados corretamente, conforme descrito em Executar verificações preliminares.
- Esteja usando um navegador compatível com CIMC e Cisco DNA Center. Para obter uma lista de navegadores compatíveis, consulte as notas da versão do Cisco DNA Center que você está instalando.
- Ative o ICMP no firewall do Cisco DNA Center entre e o servidor DNS que será especificado na etapa 8 do procedimento a seguir. O assistente de configuração do Maglev usa ping para verificar o servidor DNS especificado. Esse ping pode ser bloqueado se houver um firewall entre Cisco DNA Center e o servidor DNS, e o ICMP não estiver ativado nesse firewall. Quando isso acontecer, você não poderá concluir o assistente.

Etapa 1 Aponte o navegador para o endereço IP CIMC definido durante a configuração da interface de usuário do CIMC que você executou e faça login na interface de usuário do CIMC como o usuário CIMC (consulte Ativar acesso do navegador ao CIMC).

Após o login bem-sucedido, o dispositivo exibe a janela de **Resumo do chassi do Cisco Integrated Management Controller**, com um menu de link azul no canto superior direito, como mostrado abaixo.



Etapa 2 No menu de link azul, escolha **Launch KVM** (Iniciar KVM) e, em seguida, selecione o **KVM baseado em Java** ou **KVM baseado em HTML**. Se você selecionar o KVM baseado em Java, precisará iniciar o arquivo de inicialização do Java no navegador ou Gerenciador de arquivos para visualizar o console KVM em sua própria janela. Se você selecionar o KVM baseado em HMTL, ele iniciará automaticamente o console KVM em uma janela do navegador ou guia separada.

Independentemente do tipo de KVM escolhido, use o console KVM para monitorar o progresso da configuração e responder aos prompts do assistente de configuração do Maglev.

Etapa 3 Com o KVM exibido, reinicialize o dispositivo fazendo uma das seguintes seleções:

a) Na janela principal do navegador da interface do usuário CIMC: escolha **Host Power** > **Power Cycle** (Alimentação do Host > Desligar e ligar). Em seguida, alterne para o console do KVM para continuar.

b) No console do KVM, selecione **Power** > **Power Cycle System (cold boot)** (Desligar e ligar o sistema [inicialização a frio].

Se for solicitado que você confirme sua escolha para reiniciar o dispositivo, clique em **OK**.

Após exibir as mensagens de reinicialização, o console KVM exibe a tela de boas-vindas do assistente de configuração do Maglev, mostrada abaixo.

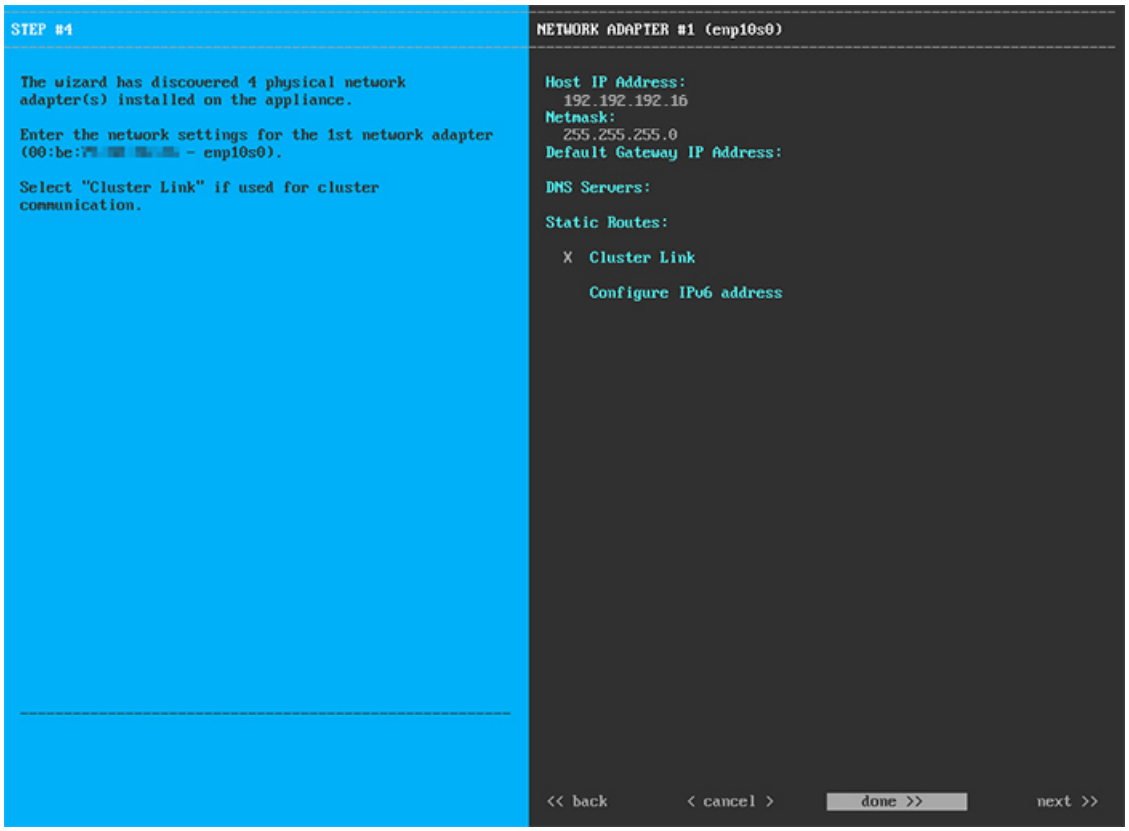
Etapa 4 Escolha **Join a DNA-C cluster** (Entrar para um cluster DNA-C) para começar a configurar o nó complementar.

O assistente descobre todas as portas no dispositivo e as apresenta uma por uma, em telas separadas, na seguinte ordem:

1. Porta de cluster 10 Gbps (porta 2, enp10s0, adaptador de rede 1)
2. Porta de interface de usuário do Cisco DNA Center de 1 Gbps (1, Enp1s0f0, adaptador de rede 2)
3. Porta de nuvem de 1 Gbps (2, Enp1s0f0, adaptador de rede 3)
4. Porta empresarial de 10 Gbps (porta 1, enp9s0, adaptador de rede 4)

Observação Se o assistente não exibir uma ou ambas as portas de 10 Gbps durante a configuração, essas portas podem não estar funcionando ou estarem desativadas. Essas portas 10 Gbps são necessárias para a funcionalidade do Cisco DNA Center. Se você descobrir que eles não estão funcionando, escolha **Cancel** (Cancelar) para sair da configuração imediatamente. Verifique se você concluiu todas as etapas fornecidas em Executar verificações preliminares, antes de retomar à configuração ou entrar em contato com o Cisco Technical Assistance Center (TAC).

Etapa 5 O assistente descobre a porta de cluster 10 Gbps (porta 2, enp10s0) primeiro e a apresenta como **ADAPTADOR DE REDE 1**. Como explicado em Conexões de cabo de interface, essa porta é usada para vincular o dispositivo ao cluster, portanto, aplique o endereço IP do host, a máscara de rede e outros valores apropriados para essa finalidade (consulte Sub-redes necessárias e endereços IP adicionais e Informações de configuração obrigatórias para obter os valores a serem inseridos.



Insira os valores de configuração do **ADAPTADOR DE REDE 1** como mostrado na tabela abaixo.

Tabela 29: Entradas do nó complementar para o Adaptador de rede 1: porta de cluster de 10 Gbps (enp10s0)

Endereço IP do host	Digite o endereço IP da porta de cluster. Isso é obrigatório. Observe que você não pode alterar posteriormente o endereço da porta de cluster.
Máscara de rede	Insira a máscara de rede para o endereço IP da porta. Isso é obrigatório.
Endereço IP do gateway padrão	Insira um endereço IP de gateway padrão para usar na porta. Isso geralmente é obrigatório apenas na porta corporativa.
Servidores DNS	Digite o endereço IP do servidor DNS preferencial. Se inserir vários servidores DNS, separe os endereços IP na lista com espaços.
Rotas estáticas	Insira uma ou mais rotas estáticas no formato a seguir, separadas por espaços: <rede>/<máscara de rede>/<gateway>. Isso geralmente é obrigatório apenas na porta da interface de usuário do Cisco DNA Center.

Link de cluster	Marque a caixa de seleção para indicar que essa porta será o link para um cluster. Isso é obrigatório somente na porta de cluster.
Configurar endereço IPv6	Reservado para uso futuro. Deixe este campo em branco.

Quando terminar de inserir os valores de configuração, insira **next >>** para continuar. Após inserir **next>>**, o assistente valida os valores que você inseriu e emite uma mensagem de erro, se houver algum incorreto. Se você receber uma mensagem de erro, verifique se o valor inserido está correto e insira-o novamente. Se necessário, selecione **<<back** para inseri-lo novamente.

Etapa 6 Após a validação bem-sucedida dos valores de porta de cluster que você digitou, o Assistente apresenta a porta de interface de usuário do Cisco DNA Center de 1 Gbps (1, enp1s0f0) como **ADAPTADOR DE REDE 2**. Como explicado nas Conexões de cabo de interface, essa porta é usada para acessar a interface de usuário do Cisco DNA Center da rede de gerenciamento. Aplique o endereço IP do host, a máscara de rede e outros valores apropriados para essa finalidade (consulte Sub-redes necessárias e endereços IP adicionais e Informações de configuração obrigatórias para obter os valores a serem inseridos).

Insira os valores de configuração do **ADAPTADOR DE REDE 2** como mostrado na tabela abaixo.

Tabela 30: Entradas do nó complementar para o Adaptador de rede 2: porta de interface de usuário de 1 Gbps (enp1s0f0)

Endereço IP do host	Insira o endereço IP para a porta de interface de usuário de 1 Gpbs do Cisco DNA Center. Isso é obrigatório.

Máscara de rede	Insira a máscara de rede para o endereço IP da porta. Isso é obrigatório.
Endereço IP do gateway padrão	Insira um endereço IP de gateway padrão para usar na porta. Isso geralmente é obrigatório apenas na porta corporativa.
Servidores DNS	Digite o endereço IP do servidor DNS preferencial. Se inserir vários servidores DNS, separe os endereços IP na lista com espaços. **Observação** Para NTP, verifique se a porta 121 (UDP) está aberta entre Cisco DNA Center e o servidor NTP.
Rotas estáticas	Insira uma ou mais rotas estáticas no formato a seguir, separadas por espaços: <rede>/<máscara de rede>/<gateway>.
Link de cluster	Deixe este campo em branco. É obrigatório somente na porta de cluster.
Configurar endereço IPv6	Reservado para uso futuro. Deixe este campo em branco.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores.

Etapa 7 Após a validação bem-sucedida dos valores de porta de interface de usuário de Cisco DNA Centerinseridos, o assistente apresenta a porta de nuvem de 1 Gbps (2, enp1s0f1) como **ADAPTADOR DE REDE 3**. Como explicado em Conexões de cabo de interface, essa é uma porta opcional usada para vincular o dispositivo à Internet quando não for possível fazer isso através da porta de 10 Gbps empresarial (porta 1, enp9s0). Aplique o endereço IP do host, a máscara de rede e outros valores apropriados para essa finalidade (consulte Sub-redes necessárias e endereços IP adicionais e Informações de configuração obrigatórias para obter os valores a serem inseridos).

Insira os valores de configuração do **ADAPTADOR DE REDE 3** como mostrado na tabela abaixo.

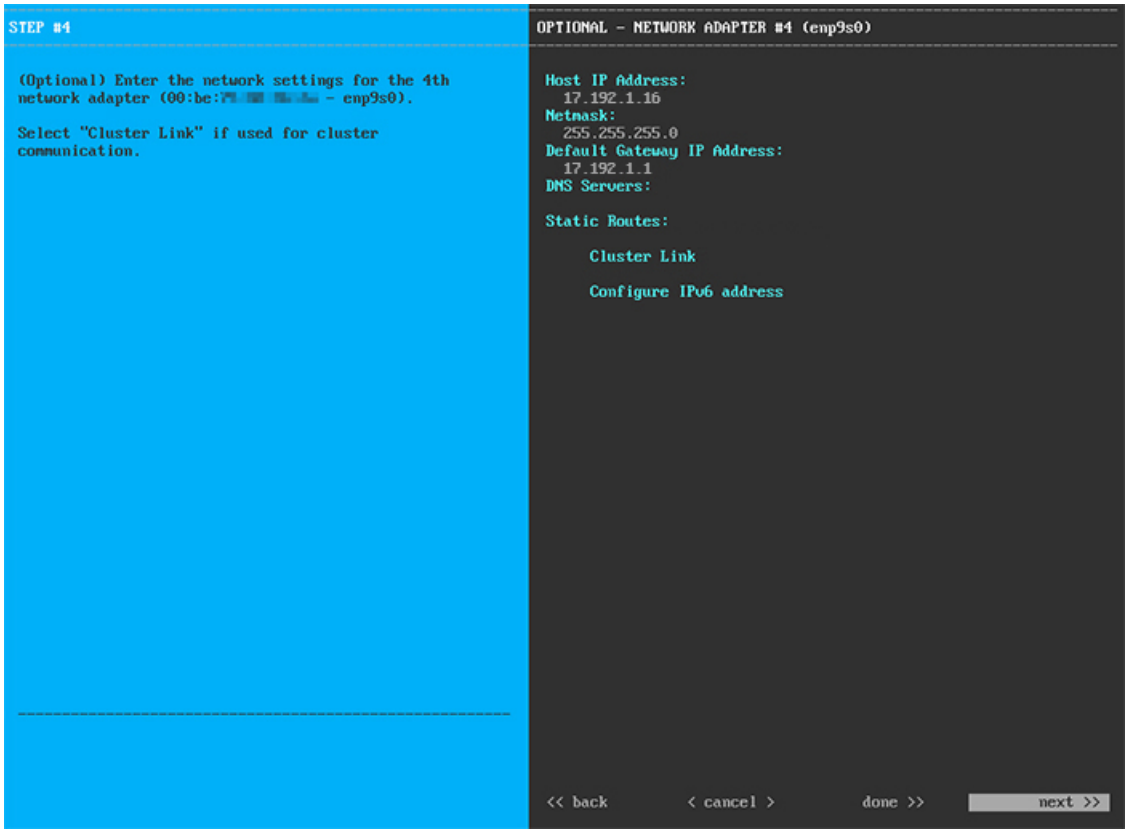
Tabela 31: Entradas do nó complementar para o adaptador de rede 3: porta de nuvem de 1 Gbps (enp1s0f1)

Endereço IP do host	Digite o endereço IP da porta de nuvem. Isso é obrigatório somente se você estiver usando a porta de nuvem para conexão com a Internet; caso contrário, pode deixá-lo em branco.
Máscara de rede	Insira a máscara de rede para o endereço IP da porta. Isso será obrigatório se você inserir um endereço IP.
Endereço IP do gateway padrão	Insira um endereço IP de gateway padrão para usar a porta de nuvem. Isso geralmente é obrigatório apenas na porta corporativa.
Servidores DNS	Digite o endereço IP do servidor DNS preferencial. Se inserir vários servidores DNS, separe os endereços IP na lista com espaços.
Rotas estáticas	Insira uma ou mais rotas estáticas no formato a seguir, separadas por espaços: <rede>/<máscara de rede>/<gateway>. Isso geralmente é obrigatório apenas na porta da interface de usuário.

Link de cluster	Deixe este campo em branco. É obrigatório somente na porta de cluster.
Configurar endereço IPv6	Reservado para uso futuro. Deixe este campo em branco.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores.

Etapa 8 Após a validação bem-sucedida dos valores de porta na nuvem que você inseriu, o assistente apresenta a porta de 10 Gbps empresarial (porta 1, enp9s0) como **ADAPTADOR DE REDE 4**. Como explicado em Conexões de cabo de interface, essa é uma porta obrigatória usada para vincular o dispositivo à rede corporativa. Aplique o endereço IP do host, a máscara de rede e outros valores apropriados para essa finalidade (consulte Sub-redes necessárias e endereços IP adicionais e Informações de configuração obrigatórias para obter os valores a serem inseridos).



Insira os valores de configuração do **ADAPTADOR DE REDE 4** como mostrado na tabela abaixo.

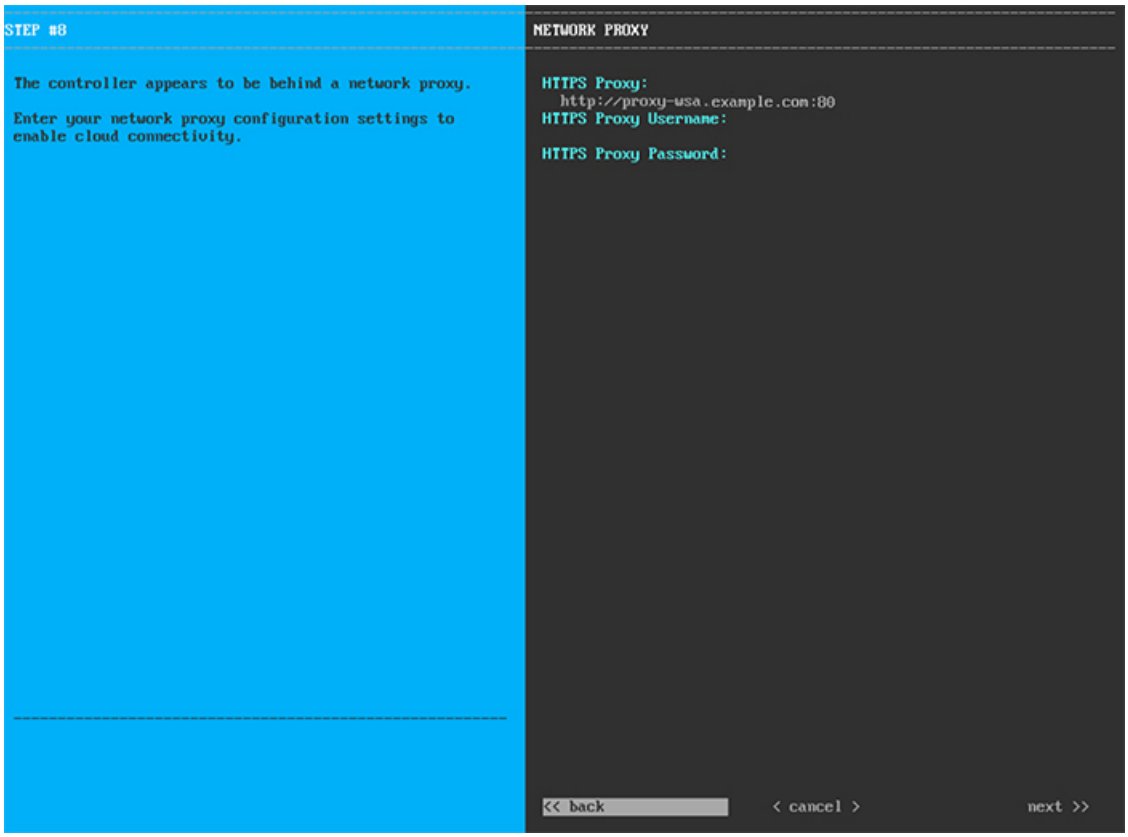
Tabela 32: Entradas do nó complementar para o adaptador de rede 4: porta empresarial de 10 Gbps (enp9s0)

Endereço IP do host	Digite o endereço IP para a porta empresarial de 10Gpbs. Isso é obrigatório.
Máscara de rede	Insira a máscara de rede para o endereço IP da porta. Isso é obrigatório.
Endereço IP do gateway padrão	Insira um endereço IP de gateway padrão para usar na porta. Isso é obrigatório.

Servidores DNS	Digite o endereço IP do servidor DNS preferencial. Se inserir vários servidores DNS, separe os endereços IP na lista com espaços.
Rotas estáticas	Insira uma ou mais rotas estáticas no formato a seguir, separadas por espaços: <rede>/<máscara de rede>/<gateway>. Isso geralmente é obrigatório apenas na porta da interface de usuário.
Link de cluster	Deixe este campo em branco. É obrigatório somente na porta de cluster.
Configurar endereço IPv6	Reservado para uso futuro. Deixe este campo em branco.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores.

Etapa 9 Quando a configuração do adaptador de rede estiver concluída, o assistente solicitará que você insira os valores de configuração para o **NETWORK PROXY** (PROXY DE REDE) que está usando, como mostrado abaixo.



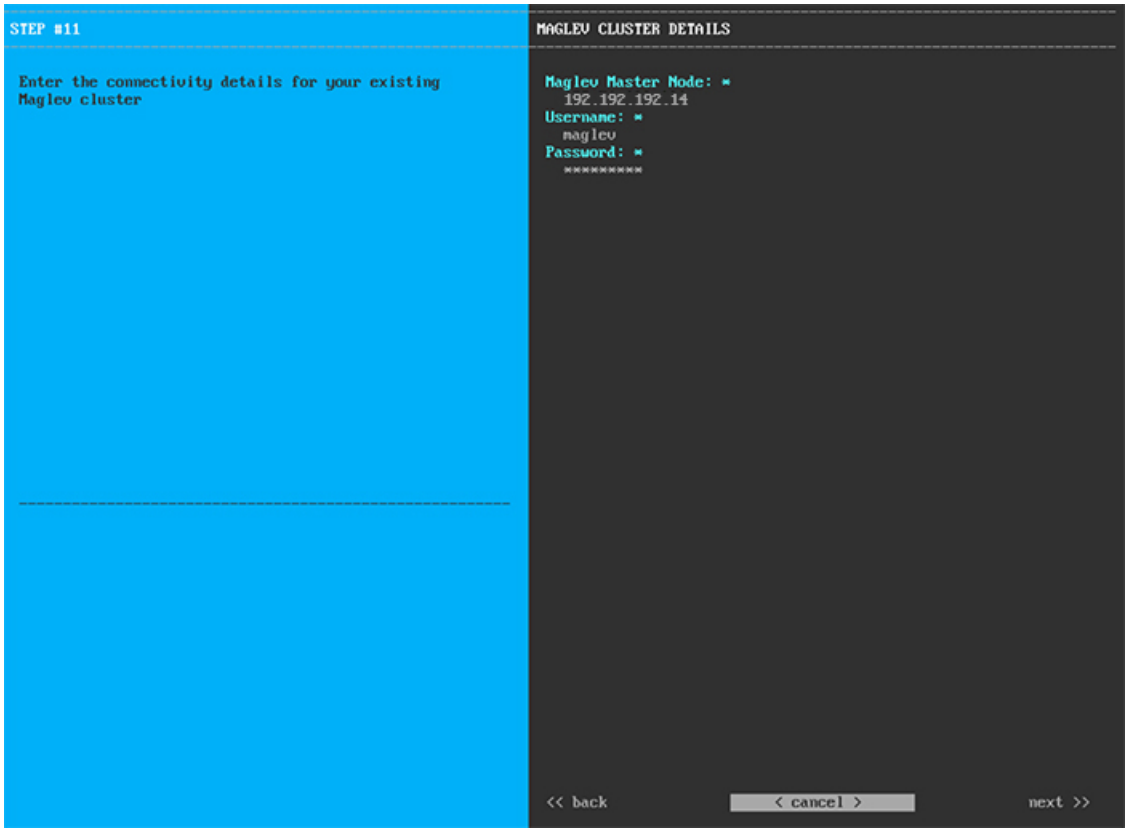
Insira valores de configuração para o **NETWORK PROXY** (PROXY DE REDE), conforme mostrado na tabela abaixo.

Tabela 33: Entradas do nó complementar para o proxy de rede

Proxy HTTPS	Digite a URL ou o nome do host de um proxy de rede HTTPS usado para acessar a Internet. **Observação** A conexão do Cisco DNA Center ao proxy HTTPS é compatível apenas via http nesta versão.
Nome de usuário do proxy HTTPS	Insira o nome de usuário usado para acessar o proxy de rede. Se nenhum login de proxy for necessário, deixe este campo em branco.
Senha do proxy HTTPS	Insira a senha usada para acessar o proxy de rede. Se nenhum login de proxy for necessário, deixe este campo em branco.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores.

Etapa 10 Quando a configuração do proxy de rede for concluída, o assistente solicitará que você identifique a porta do cluster no nó mestre e nos detalhes de login do nó mestre em **MAGLEV CLUSTER DETAILS** (DETALHES DO CLUSTER MAGLEV), como mostrado abaixo.



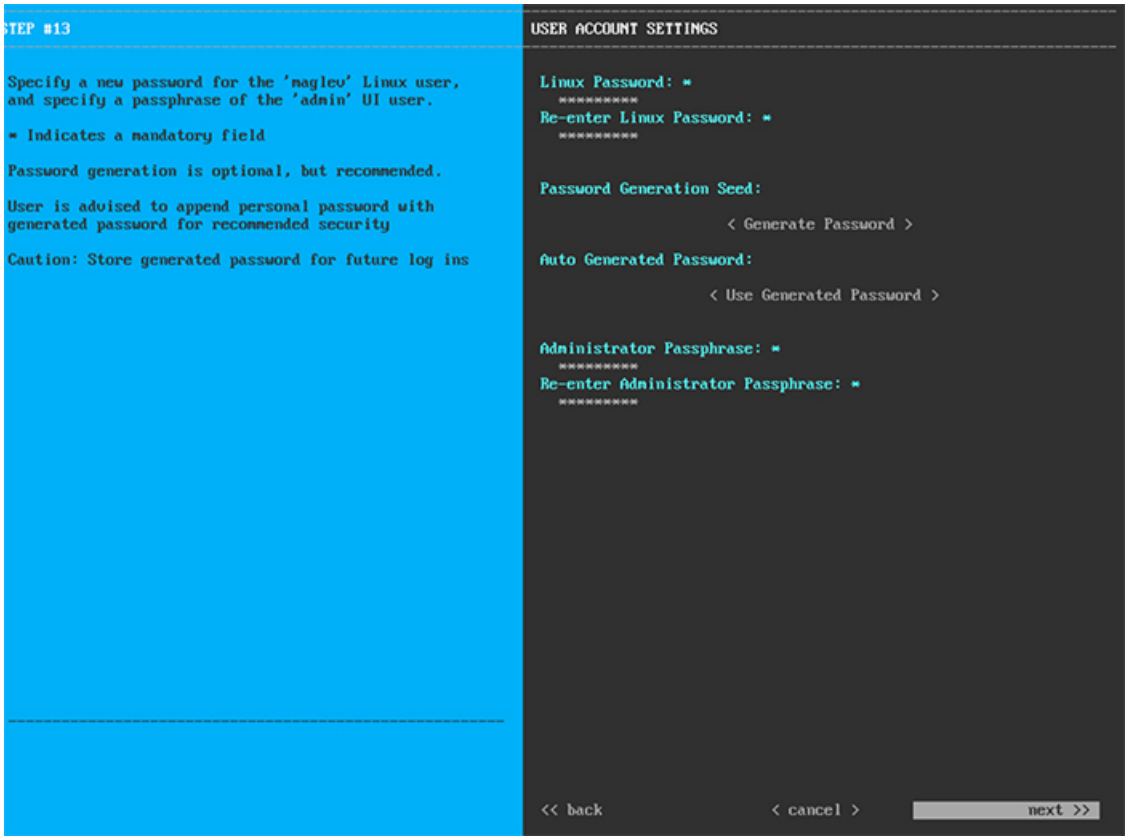
Insira valores para os **MAGLEV CLUSTER DETAILS** (DETALHES DO CLUSTER MAGLEV), conforme mostrado na tabela abaixo.

Tabela 34: Entradas de nó complementar para detalhes do cluster Maglev

Nó mestre Maglev	Insira o endereço IP da porta de cluster no nó mestre no cluster. Se você seguiu as recomendações para atribuição de porta, este será o endereço IP da porta 2, enp10s0, adaptador de rede 1 no nó mestre.
Nome de usuário	Digite **`Maglev`**.
Senha	Insira a senha de Linux configurada no nó mestre.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores.

Etapa 11 Quando os detalhes do cluster Maglev forem inseridos, o assistente solicitará que você insira os valores de **USER ACCOUNT SETTINGS** (CONFIGURAÇÕES DE CONTA DE USUÁRIO) desse nó complementar, como mostrado abaixo.



Insira os valores de **USER ACCOUNT SETTINGS** (CONFIGURAÇÕES DE CONTA DE USUÁRIO), conforme mostrado na tabela abaixo.

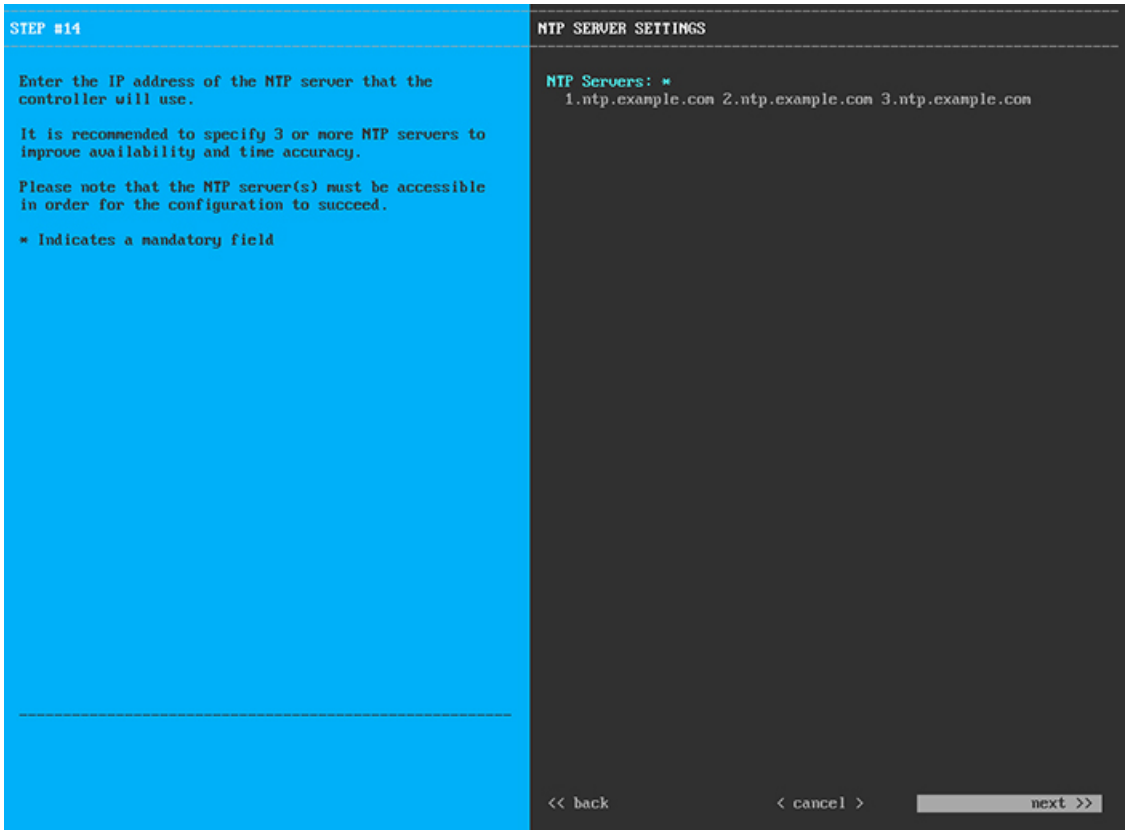
Tabela 35: Entradas de nó complementar para as configurações de conta de usuário

Senha do Linux	Insira uma senha de Linux para o usuário Maglev.
Insira novamente a senha do Linux	Confirme a senha do Linux inserindo-a uma segunda vez.

Propagação de geração de senha	Se você não quiser criar a senha do Linux, insira uma frase de propagação neste campo e pressione <**Generate Password**> (Gerar senha) para gerar a senha.
Senha gerada automaticamente	(Opcional) A frase de propagação aparece como parte de uma senha aleatória e segura. Se desejar, você pode usar essa senha "como está" ou pode editar a senha gerada automaticamente. Pressione <**Use Generated Password**> (Usar a senha gerada) para salvar a senha.
Senha do administrador	Insira uma senha para o superusuário do administrador padrão, usado para fazer login ao Cisco DNA Center pela primeira vez.
Insira novamente a senha do administrador	Confirme a senha do administrador inserindo-a uma segunda vez.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores.

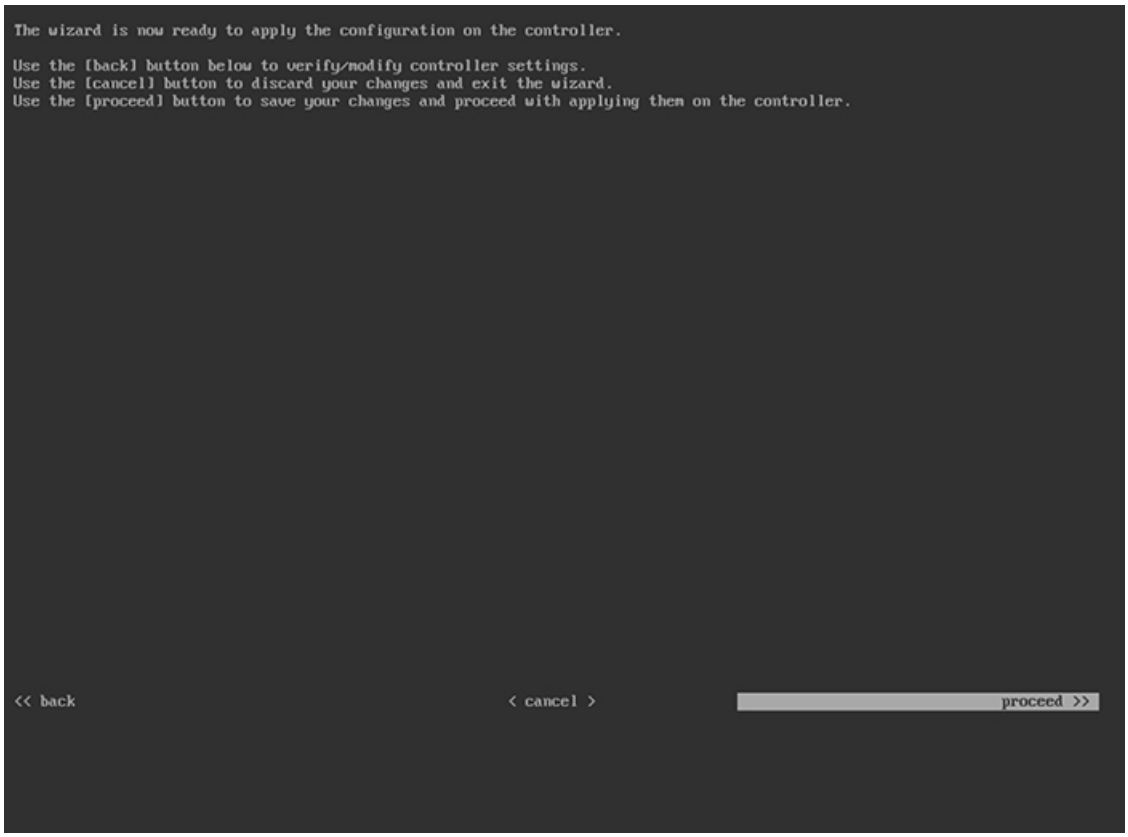
Etapa 12 Quando os detalhes da conta de usuário forem inseridos, o assistente solicitará que você insira os valores de **NTP SERVER SETTINGS** (CONFIGURAÇÕES DO SERVIDOR NTP), como mostrado abaixo.



Insira um ou mais endereços de servidor NTP ou nomes de host, separados por espaços. Pelo menos um endereço ou nome de host NTP é obrigatório. Eles devem ser os mesmos servidores NTP que você especificou para o nó mestre.

Quando terminar, digite **next>>** para continuar. Corrija todos os erros de validação como nas telas anteriores.

Etapa 13 Quando você terminar de inserir as configurações do servidor NTP, uma mensagem final será exibida informando que o assistente está pronto para continuar com a aplicação da configuração, como mostrado abaixo.



Insira **proceed>>** para concluir a configuração.

O host será reinicializado automaticamente e exibirá mensagens no console do KVM, enquanto aplica as configurações e mostra os serviços. Esse processo pode levar várias horas. Você pode monitorar o progresso pelo console do KVM.

No final do processo de configuração, o dispositivo desliga e liga novamente, em seguida, é exibida uma mensagem **CONFIGURATION SUCCEEDED!** (CONFIGURAÇÃO BEM-SUCEDIDA!).

O que Fazer Depois

Quando esta tarefa estiver concluída:

- Se você tiver um equipamento Cisco DNA Center adicional para implantar como terceiro e último nó no cluster, repita este procedimento.
- Se você tiver terminado de adicionar hosts ao cluster, continue executando a configuração inicial: Fluxo de trabalho de primeira configuração.

Cenários de implantação do cluster de alta disponibilidade

Você pode implantar o dispositivo na rede como um de um cluster de até três nós. Nesse modo, todos os serviços e dados são compartilhados entre os hosts.

Ao implantar em um cluster, escolha o cenário de implantação apropriado para a rede:

- Nova implantação de HA
- Implantação de HA atual do nó mestre com configurações de interface padrão
- Implantação atual do nó mestre com configurações de interface fora do padrão

Cada cenário é descrito nas seções a seguir.

Nova implantação de HA

Para instalar um cluster de alta disponibilidade de marca, siga estas etapas:

Etapa 1 Configure o primeiro dispositivo instalado como o nó mestre.

Consulte Configurar o nó mestre.

Etapa 2 Configure o segundo e terceiro dispositivos no cluster.

Consulte Configurar os nós complementares.

Implantação de HA atual do nó mestre com configurações de interface padrão

Para implantar um cluster de HA atual em que o nó mestre usa as configurações de cabo de interface necessárias, siga as etapas a seguir.

Etapa 1 Atualize o nó mestre para Cisco DNA Center 1.2.10.

Para obter informações sobre como atualizar a versão atual do Cisco DNA Center, consulte as Notas de versão para Cisco Digital Network Architecture Center.

Etapa 2 Confirme se você está usando as configurações de cabo de interface necessárias no nó mestre.

Consulte Conexões de cabo de interface.

Etapa 3 Atualize o endereço IP virtual (se o VIP ainda não estiver adicionado).

Consulte Reconfigurar o dispositivo usando o assistente de configuração.

Etapa 4 Configure o segundo e terceiro dispositivos no cluster.

Consulte Configurar os nós complementares.

Etapa 5 Digite o seguinte comando para verificar o tamanho do glusterfs:

sudo du -h /data/maglev/srv/maglev-system/glusterfs/mnt/bricks/default_brick/ | tail -1 | awk '{print $1}'

Se o tamanho do sistema de arquivos glusterfs for maior que 150 GB, conclua as etapas em Implantação atual do nó mestre com configurações de interface fora do padrão.

Implantação atual do nó mestre com configurações de interface fora do padrão

Para implantar um cluster de HA atual em que o nó mestre usa configurações de interface fora do padrão, conclua as etapas a seguir.

Etapa 1 Atualize o nó mestre para Cisco DNA Center 1.2.10.

Para obter informações sobre como atualizar a versão atual do Cisco DNA Center, consulte as Notas de versão para Cisco Digital Network Architecture Center.

Etapa 2 Crie um backup do repositório remoto.

Consulte o capítulo "Backup e restauração" no Guia do administrador do Cisco Digital Network Architecture Center.

Etapa 3 Refaça a imagem do nó mestre com a configuração necessária de cabo de interface.

Consulte Conexões de cabo de interface e Instalar a imagem ISO do Cisco DNA Center. Certifique-se de que o VIP foi configurado corretamente no nó mestre.

Etapa 4 No nó mestre, instale o mesmo conjunto de pacotes que você selecionou durante o backup.

Etapa 5 Restaure o arquivo de backup que você criou na etapa 2.

Etapa 6 Configure o segundo e terceiro dispositivos no cluster.

Consulte Configurar os nós complementares.

Considerações adicionais da implantação de HA

Para uma implantação de HA atual, as seguintes configurações adicionais devem ser feitas.

Observação Para obter informações sobre erros e soluções de alta disponibilidade conhecidas, consulte "Open bugs — HA" (Bugs abertos — HA) nas Notas de versão para Cisco Digital Network Architecture Center.

Telemetria

Se você ativou a telemetria para um dispositivo (sem ativar o VIP), siga estas etapas:

Etapa 1 Use o comando **maglev-config update** para atualizar o VIP do cluster.

Etapa 2 Desative a telemetria no dispositivo:

1. Na página inicial do Cisco DNA Center, escolha **Telemetry** (Telemetria) na área **Tools** (Ferramentas).

A janela **Telemetry** (Telemetria) será exibida.

2. Clique na guia **Site View** (Exibição do local).
3. Marque a caixa de seleção do dispositivo em que deseja desativar a telemetria; em seguida, escolha **Actions** > **Disable_Telemetry** (Ações < Desativar telemetria).

Etapa 3 Reative a telemetria com a associação de perfil de telemetria anterior aos dispositivos.

Controlador sem fio

Você deve atualizar os controladores sem fio na rede com o novo VIP de Cisco DNA Center.

Atualização para a versão Cisco DNA Center mais recente

Para obter informações sobre como atualizar a versão atual do Cisco DNA Center, consulte o Guia de atualização para Cisco Digital Network Architecture Center.

CAPÍTULO 5

Conclua a primeira configuração

- Fluxo de trabalho de primeira configuração, na página 95
- Navegadores compatíveis, na página 96
- Fazer login pela primeira vez, na página 96
- Integração do Cisco ISE com Cisco DNA Center, na página 105
- Configurar os servidores de autenticação e política, na página 107
- Configurar propriedades de SNMP, na página 108
- Redistribuir serviços, na página 109

Fluxo de trabalho de primeira configuração

Depois de concluir a configuração de todos os dispositivos do Cisco DNA Center instalados, você precisará executar as tarefas listadas na tabela a seguir para preparar o Cisco DNA Center para o uso em produção.

Para obter as informações de parâmetro necessárias para concluir esse trabalho, consulte Informações obrigatórias na primeira configuração.

Tabela 36: Cisco DNA Center Tarefas de primeira configuração do dispositivo

Etapa	Descrição
1	Certifique-se de que você esteja acessando o Cisco DNA Center usando um navegador compatível. Para obter uma lista de navegadores compatíveis, consulte as notas da versão do Cisco DNA Center que você está instalando.

Etapa	Descrição
2	Faça login na interface de usuário do Cisco DNA Center, como administrador, pela primeira vez. Durante esse primeiro login administrativo, você será solicitado a: **1.** Fornecer uma nova senha para o superusuário admin. **2.** Inserir o nome de usuário e a senha do cisco.com que a empresa usa para baixar imagens de software e receber comunicações por e-mail da Cisco. **3.** Inserir o nome de usuário e a senha do cisco.com que a empresa usa para gerenciar as licenças de Smart Account. **4.** Configurar o servidor IPAM (Gerenciador de endereços IP) que você planeja usar com Cisco DNA Center. Para obter detalhes sobre essas tarefas, consulte Fazer login pela primeira vez.
3	Se você planeja usar o Cisco DNA Center com Cisco Identity Services Engine (ISE), certifique-se de que os dois estejam devidamente integrados: Integração do Cisco ISE com Cisco DNA Center.
4	Conecte o Cisco DNA Center com a política e o servidor AAA (incluindo ISE): Configurar os servidores de autenticação e política.
5	Configure os parâmetros básicos de repetição e sondagem SNMP: Configurar propriedades de SNMP.
6	Redistribua serviços entre os nós de cluster para otimizar a operação de HA: Redistribuir serviços
7	Quando você tiver concluído a configuração inicial: Logout.

Navegadores compatíveis

A interface da Web do Cisco DNA Center é compatível com os seguintes navegadores habilitados para https:

- Google Chrome — versão 62.0 ou posterior.
- Mozilla Firefox — versão 54.0 ou posterior.

A Cisco recomenda que os sistemas clientes que você usa para fazer login no Cisco DNA Center sejam equipados com sistemas operacionais e navegadores de 64 bits.

Fazer login pela primeira vez

Depois de instalar e configurar o dispositivo Cisco DNA Center, você pode fazer login na interface de usuário baseada na Web. Você deve usar um navegador compatível com HTTPS ativado ao acessar o Cisco DNA Center.

Ao fazer login pela primeira vez como o superusuário do administrador (o nome de usuário é "admin" e tem a função SUPER-ADMIN-ROLE atribuída), você será solicitado a concluir um assistente de configuração de

primeira vez que ajuda a melhorar a segurança do sistema e a concluir as tarefas de configuração essenciais. Embora você possa ignorar cada uma das etapas do assistente, a Cisco recomenda que você conclua todas elas como indicado, para que o sistema esteja pronto para ser usado o mais rápido possível.

Você também precisará criar novos usuários do Cisco DNA Center. A Cisco recomenda que você crie pelo menos uma conta de usuário adicional para ser usada para operações diárias e que essa conta de usuário tenha a função NETWORK-ADMIN-ROLE.

Antes de Iniciar

Para fazer login no Cisco DNA Center e concluir o assistente de configuração pela primeira vez, você precisará de:

- Nome de usuário e senha do "admin" que você especificou ao seguir as etapas em Configurar o nó mestre.
- Informações solicitadas nas Informações obrigatórias na primeira configuração.

Etapa 1 Após a conclusão da reinicialização do Cisco DNA Center, inicie o navegador.

Etapa 2 Insira o endereço IP do host para acessar a interface de usuário do Cisco DNA Center.

Use o HTTPS e o endereço IP da interface de usuário do Cisco DNA Center exibida no final do processo de configuração.

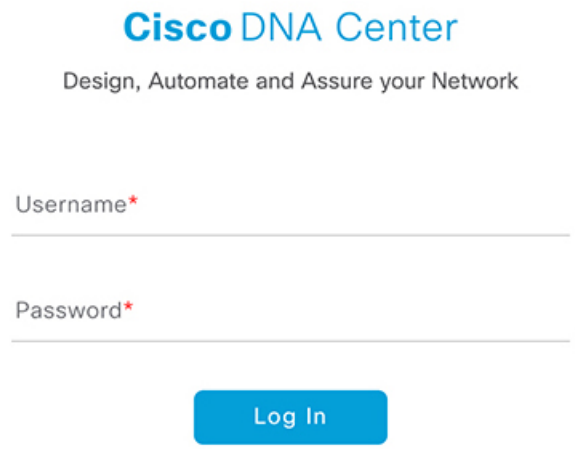
Etapa 3 Após inserir o endereço IP no navegador, é exibida uma mensagem indicando que "A conexão não é privada".

Desconsidere a mensagem e clique em **Avançado**.

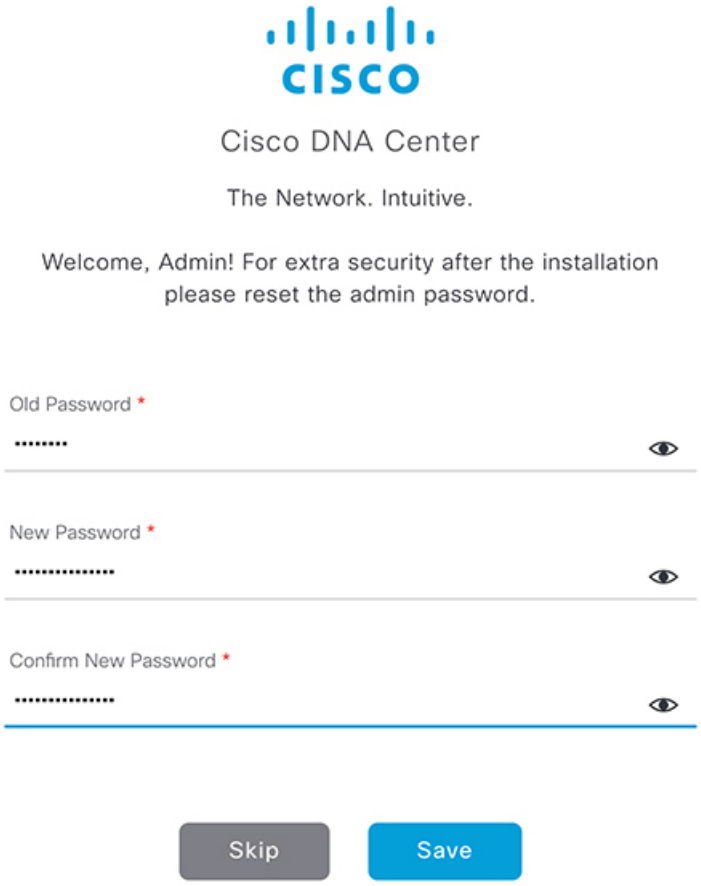
Etapa 4 É exibida uma mensagem indicando que o certificado de segurança do site não é confiável.

Essa mensagem aparece porque o controlador utiliza um certificado com assinatura automática. Posteriormente, você terá a opção de carregar um certificado confiável usando a interface de usuário do Cisco DNA Center.

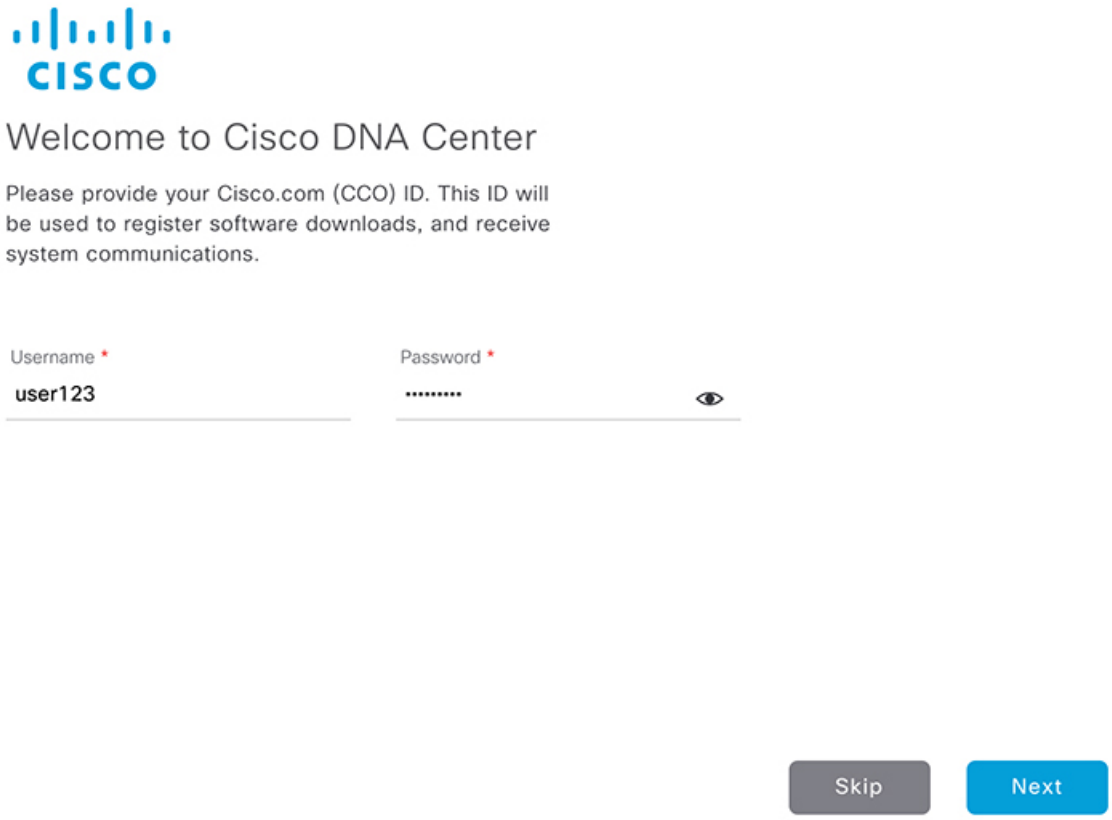
Desconsidere a mensagem e clique no link na parte inferior da página. A janela Cisco DNA Center **Login** é exibida.



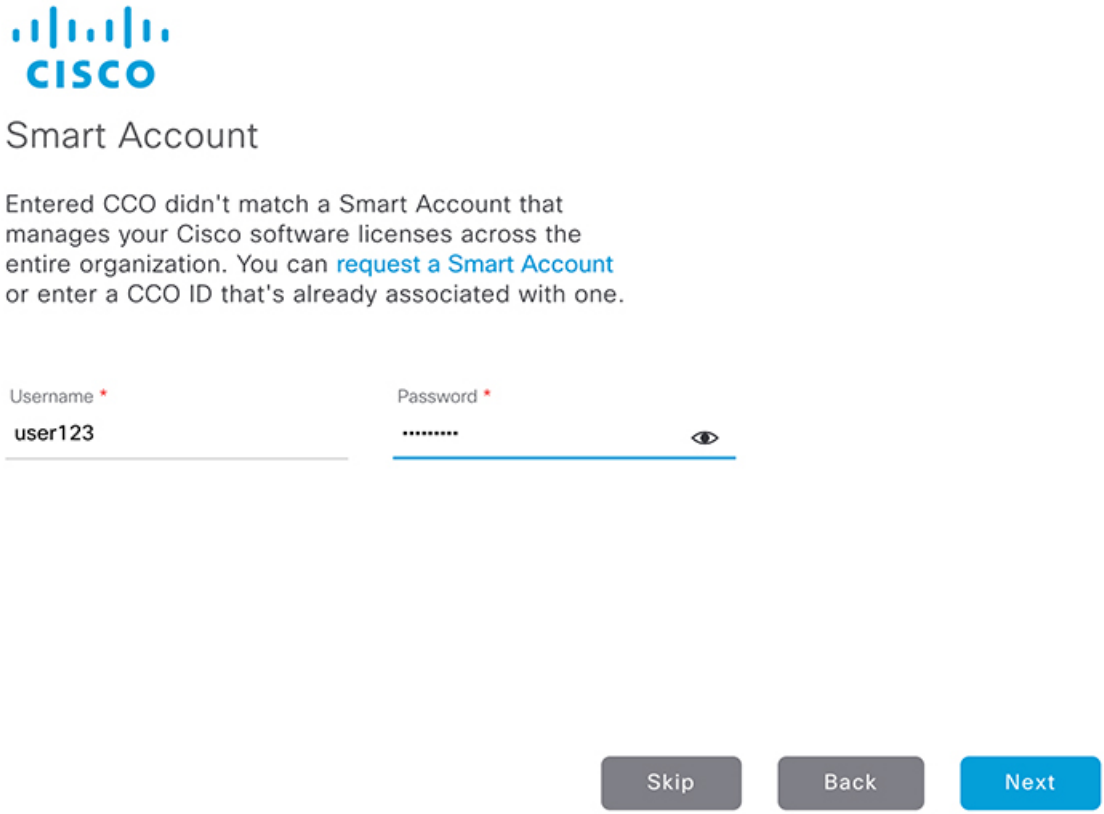
Etapa 5 Na janela de **Login**, digite o nome de usuário (admin) e a senha do administrador configurados no Cisco DNA Center. Em seguida, clique em **Login**. A janela **Reset Login** (Redefinir login) é exibida.



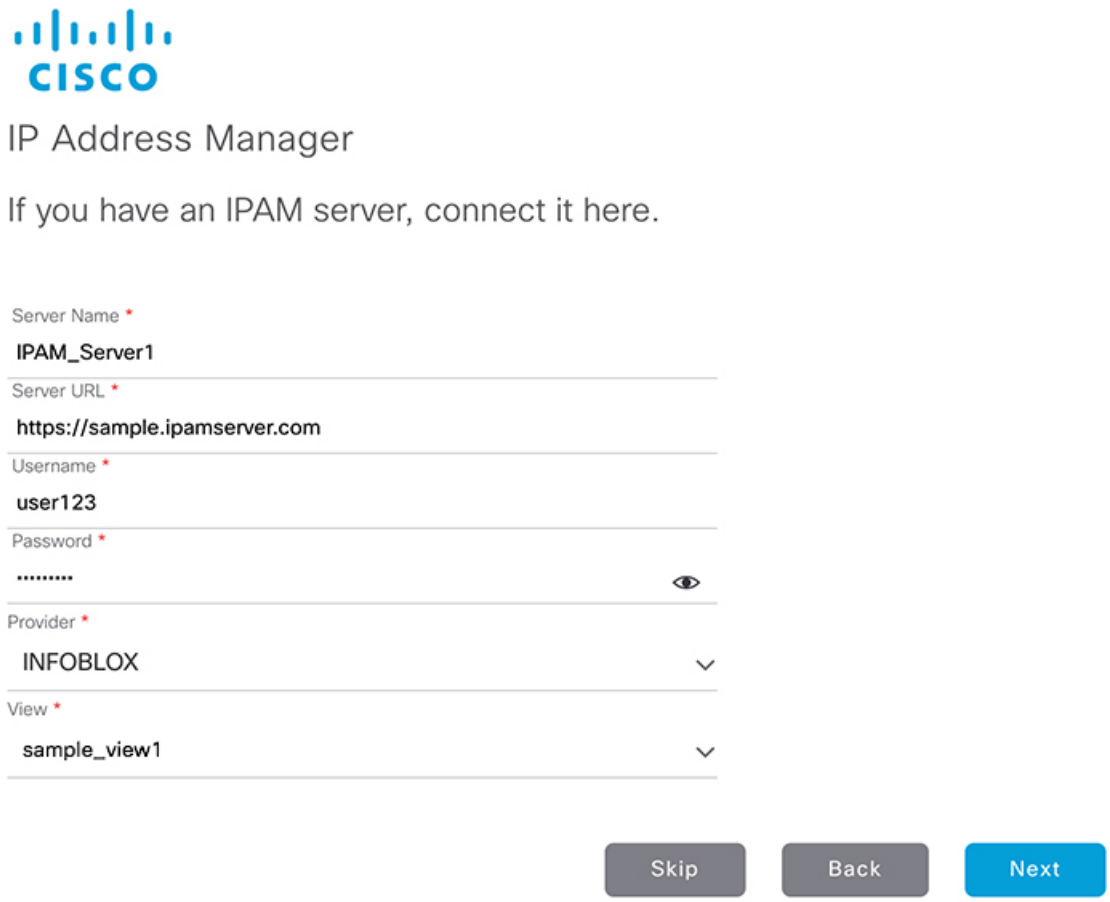
Etapa 6 Digite a senha antiga e, em seguida, insira e confirme uma nova senha para o superusuário admin. Em seguida, clique em **Save** (Salvar). A janela **Enter Cisco.com ID** (Inserir ID do Cisco.com) é exibida.



Etapa 7 Digite o nome de usuário e a senha do usuário do cisco.com e, em seguida, clique em **Next** (Avançar). Se o login de usuário do Cisco.com não corresponder a nenhum login de usuário da conta inteligente conhecido da Cisco, a janela **Smart Account** será exibida.



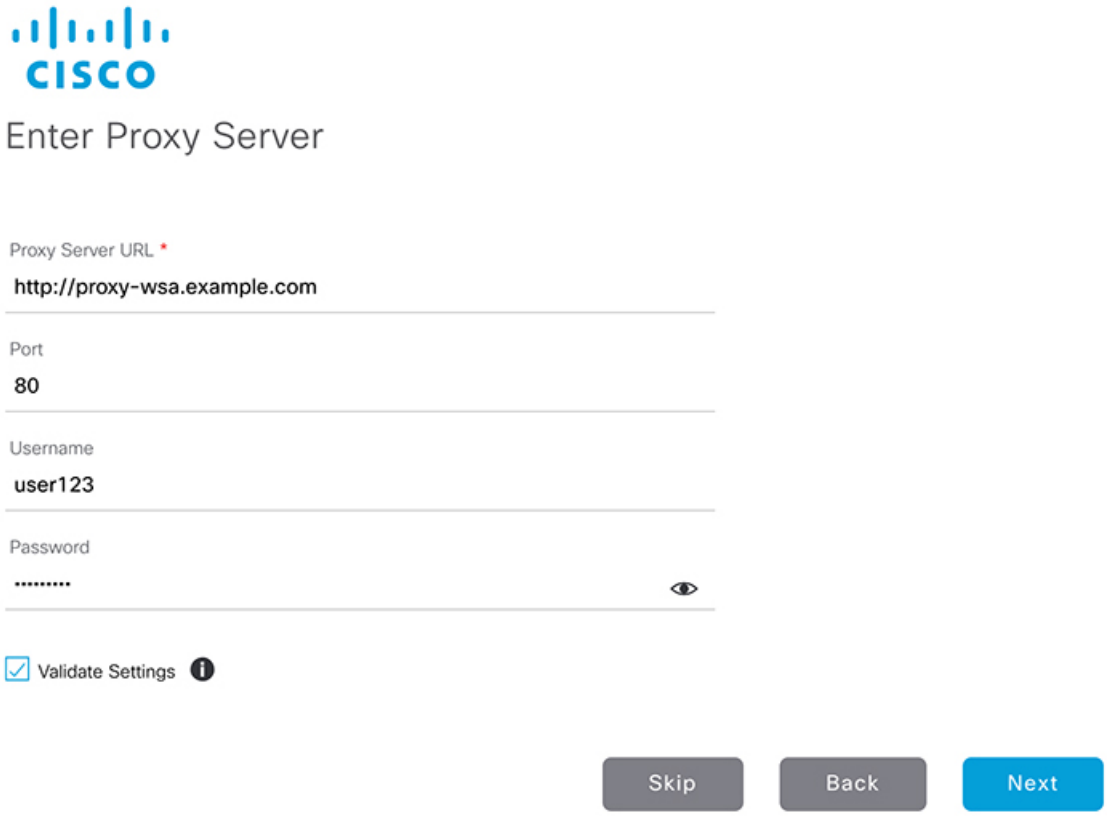
Etapa 8 Se a janela **Smart Account** aparecer, insira o nome de usuário e a senha da Smart Account da empresa ou clique no link para abrir uma nova Smart Account. Quando terminar, clique em **Next** (Avançar). A janela **IP Address Manager** (Gerenciador de endereço de IP é exibida).



Etapa 9 Se a empresa usa um gerenciador de endereço IP externo (IPAM), faça o seguinte e clique em **Next** (Avançar):

- Insira o nome e a URL do servidor IPAM.
- Insira o nome de usuário e a senha necessários para acesso ao servidor.
- Escolha o provedor de IPAM (como Infoblox).
- Escolha a exibição de endereços IP disponíveis no banco de dados do servidor IPAM que você quer que Cisco DNA Center use.

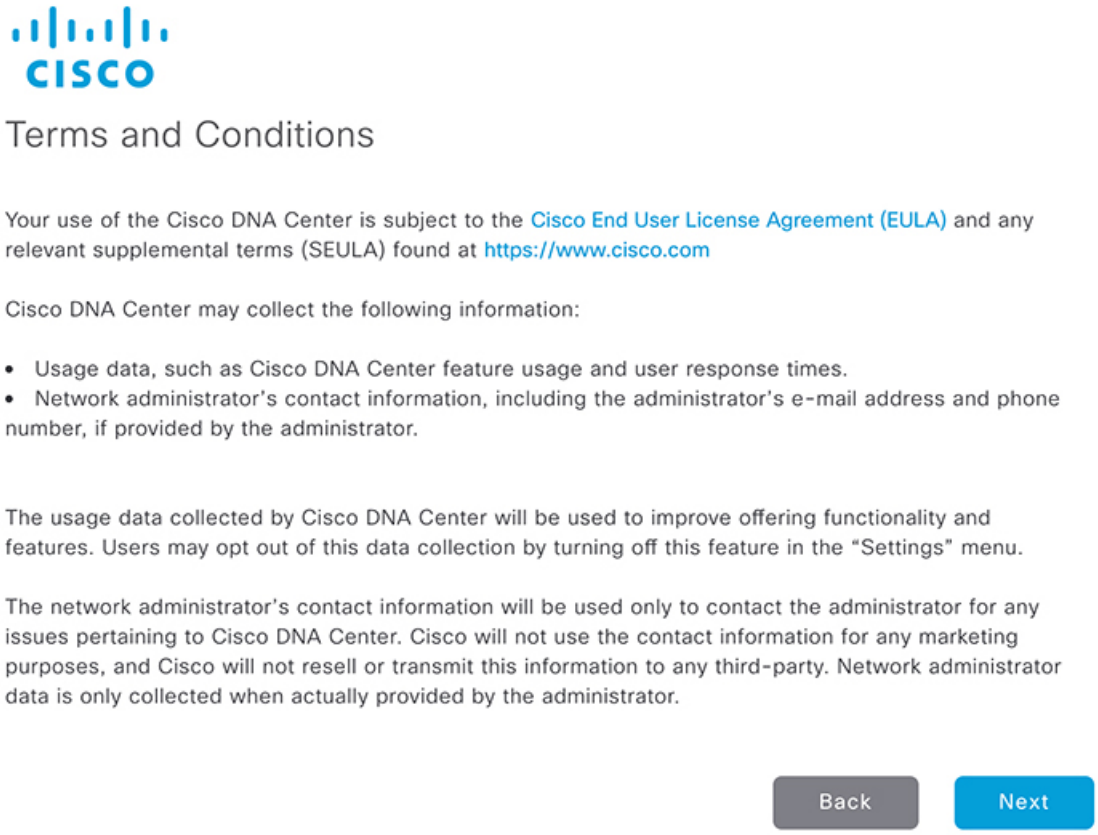
A janela **Enter Proxy Server** (Inserir servidor proxy) é exibida.



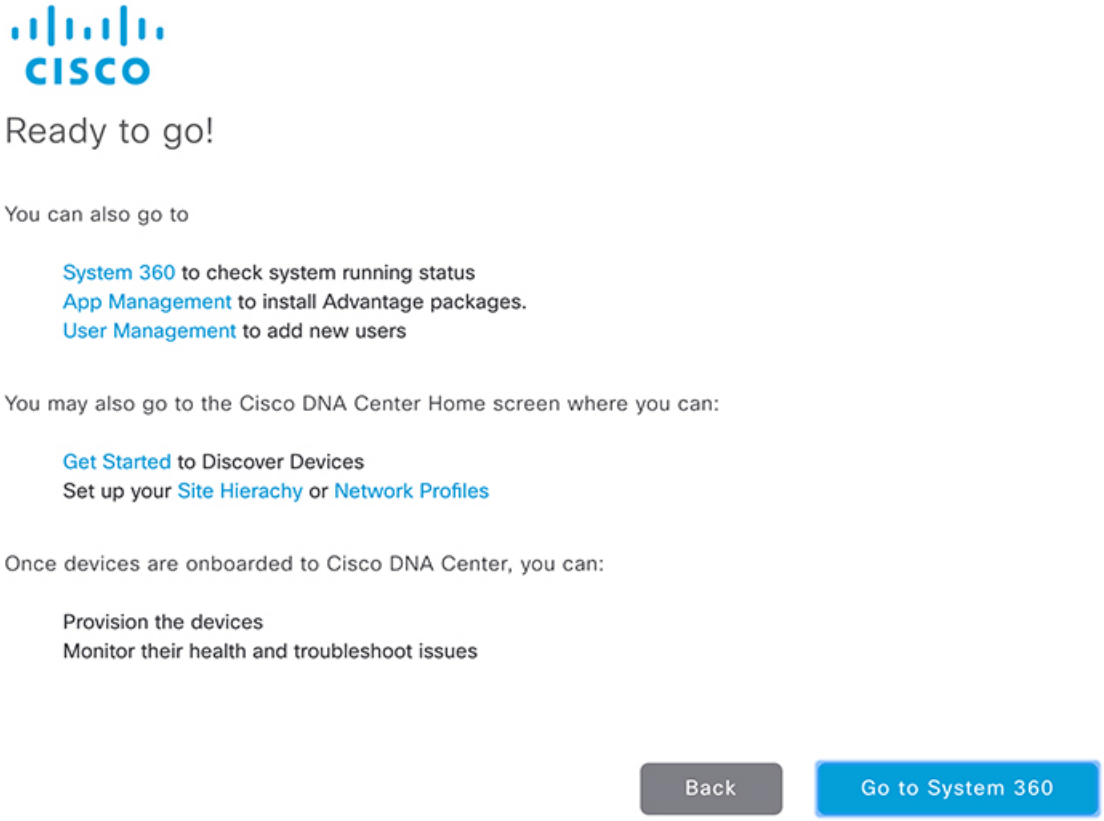
Etapa 10 Insira as informações do servidor proxy que a empresa vai usar. Inclua o nome de usuário e a senha do servidor, se o servidor proxy exigir um login.

Se desejar validar essas informações antes de continuar (recomendado), certifique-se de que a caixa de seleção **Validate Settings** (Validar configurações) esteja marcada.

Quando terminar, clique em **Next** (Avançar). A janela de software **EULA** é exibida.



Etapa 11 Clique em **Next** (Avançar) para aceitar o Contrato de licença de usuário final do software e continue. A janela **Ready to go!** (Pronto!) é exibida.



Etapa 12 Você pode clicar em qualquer um dos links nesta janela ou clicar em **Go to System 360** (Ir para o sistema 360) para exibir o painel do sistema 360 e começar a usar o Cisco DNA Center.

A Cisco recomenda que você clique no link de **User Management** (Gerenciamento de usuário) para exibir a janela **User Management**. Em seguida, clique em **Add** (Adicionar) para começar a adicionar novos usuários do Cisco DNA Center. Depois de inserir o nome e a senha do novo usuário e selecionar a função do usuário, clique em **Save** (Salvar) para criar o novo usuário. Repita isso conforme necessário, até que você tenha adicionado todos os novos usuários para a implantação inicial. Certifique-se de criar pelo menos um usuário com a função NETWORK-ADMIN-ROLE.

O que Fazer Depois

Conclua outras tarefas administrativas de configuração, em qualquer ordem:

- Integração do Cisco ISE com Cisco DNA Center
- Configurar os servidores de autenticação e política
- Configurar propriedades de SNMP

Integração do Cisco ISE com Cisco DNA Center

Essa versão do Cisco DNA Center fornece um mecanismo para criar um link de comunicação confiável com o Cisco Identity Services Engine (ISE) e permite que o Cisco DNA Center compartilhe dados com o ISE de forma segura. Quando o ISE é registrado com Cisco DNA Center, qualquer descoberta de dispositivo Cisco DNA Center, juntamente com a configuração relevante e outros dados, é enviada para o ISE. Os usuários podem usar o Cisco DNA Center para descobrir dispositivos e, em seguida, aplicar as funções de Cisco DNA Center e ISE a eles, pois esses dispositivos serão expostos em ambos os aplicativos. Os dispositivos ISE e Cisco DNA Center são identificados exclusivamente pelos nomes de dispositivos.

Os dispositivos Cisco DNA Center, assim que são provisionados e pertencerem a um determinado local na hierarquia de locais de Cisco DNA Center, são enviados para o ISE. Todas as atualizações em um dispositivo Cisco DNA Center (como alterações de endereço IP, credenciais de CLI ou SNMP, segredo compartilhado do ISE e assim por diante) fluirão automaticamente para a instância do dispositivo correspondente no ISE. Quando um dispositivo Cisco DNA Center é excluído, ele também é removido do ISE. Observe que os dispositivos Cisco DNA Center são enviados para o ISE somente quando eles estão associados a um local específico onde o ISE está configurado como servidor AAA.

Antes de Iniciar

Antes de tentar integrar o ISE com Cisco DNA Center, certifique-se de ter atendido aos seguintes pré-requisitos:

- Você implantou um ou mais hosts ISE versão 2.3 (e posterior) na rede. Para obter informações sobre como instalar o ISE, consulte os Guias de instalação e atualização do Cisco Identity Services Engine para a versão 2.3 e posterior.
- Se você tiver uma implantação autônoma do ISE, integre e ative o serviço de pxGrid e o ERS no nó ISE.
- Se você tiver uma implantação do ISE distribuída:
    - Integre Cisco DNA Center com o nó de administração do ISE (PAN primário) e ative o ERS no PAN.
    - Como nas implantações de um único nó, você deve ativar o serviço de pxGrid em um dos nós ISE na implantação distribuída. Embora você possa optar por fazer isso, não é necessário ativar pxGrid no PAN. Você pode ativar o pxGrid em qualquer um dos outros nós ISE na implantação distribuída.
- O host ISE no qual o pxGrid está ativado deve ser acessado do Cisco DNA Center no endereço IP da interface eth0 do ISE.
- O nó ISE pode acessar a rede subjacente de malha por meio da placa de interface de rede do dispositivo.
- O SSH está ativado para o nó ISE.
- As contas de usuário de CLI e GUI do ISE devem usar o mesmo nome de usuário e senha.
- O certificado do nó de administração do ISE deve conter o endereço IP ou o nome de domínio totalmente qualificado (FQDN) do ISE no nome do assunto do certificado ou no SAN.
- O certificado do sistema do Cisco DNA Center deve listar o endereço IP do dispositivo Cisco DNA Center e o FQDN no campo Subject Alternative Name (SAN) (Nome alternativo do assunto).

Etapa 1 Ative o serviço pxGrid ISE e o ERS da seguinte maneira:

a) Faça login no nó de administração principal do ISE (PAN).
b) Escolha **Administration** > **Deployment** (Administração > Implantação).
c) Escolha o nome de host do nó de ISE no qual deseja ativar os serviços de pxGrid. Em uma implantação distribuída, pode ser qualquer nó ISE na implantação.
d) Na guia **General Settings** (Configurações gerais), certifique-se de que a caixa de seleção **pxGrid** esteja marcada.
e) Clique em **Salvar**.
f) Selecione **Administration** > **System** > **Settings** > **ERS Settings** (Administração > Sistema > Configurações > Configurações de ERS) e clique em **Enable ERS for Read/Write** (Ativar ERS para leitura/gravação). Clique em **OK** no prompt de notificação.

Etapa 2 Adicione o nó ISE a Cisco DNA Center como um servidor AAA, da seguinte forma:

a) Faça login na interface de usuário do Cisco DNA Center baseada na Web.
b) Clique em ⚙ e selecione **System Settings** (Configurações do sistema).
c) No painel Cisco ISE, escolha o link **Configure Settings** (Configurar configurações).
d) Na página **Settings - Authentication and Policy Servers** (Configurações - autenticação e servidores de política), clique no ícone de adição (+) grande para exibir as configurações de AAA.
e) Clique no controle deslizante do **Cisco ISE** para garantir que todos os campos relacionados ao ISE sejam exibidos.
f) Digite o endereço IP de gerenciamento de ISE no campo **IP address** (Endereço IP).
g) Insira o **Segredo compartilhado** usado para proteger as comunicações entre os dispositivos de rede e ISE.
h) Insira as credenciais de administrador do ISE correspondentes nos campos **Username** (Nome de usuário) e **Password** (Senha).
i) Insira o **FQDN** para o nó ISE.
j) Insira o **Subscriber Name** (Nome do assinante); por exemplo, **`cdnacenter`**.
k) A **SSH Key** (chave SSH) é opcional e pode ser deixada em branco.

Etapa 3 Quando terminar de preencher esses campos, clique em **Update** (Atualizar) e aguarde o status do servidor ser exibido como **`Active`** (Ativo).

Etapa 4 Verifique se o ISE está conectado ao Cisco DNA Center e se a conexão tem assinaturas, da seguinte maneira:

a) Faça login no nó ISE com o qual você integrou o Cisco DNA Center.
b) Escolha **Administration** > **pxGrid Services** (Administração > Serviços pxGrid). Você verá que um assinante com o nome inserido (por exemplo, **`cdnacenter`**) tem o status atual **`on-line`**.
c) Se o status do assinante estiver **`Pending`** (Pendente), escolha **Total Pending Approval** > **Approve all Clients** (Aprovação total pendente < Aprovar todos os clientes) para aprovar este assinante. O status do assinante deve mudar para **`on-line`**.

Etapa 5 Verifique se Cisco DNA Center está conectado ao ISE e se os grupos e dispositivos ISE SGT estão sendo enviados para Cisco DNA Center, da seguinte maneira:

a) Faça login na interface de usuário do Cisco DNA Center baseada na Web.
b) Clique em ⚙ e selecione **System Settings** (Configurações do sistema).
c) No painel Cisco ISE, escolha o link **Configure Settings** (Configurar configurações).
d) Na página **Settings - Authentication and Policy Servers** (Configurações - autenticação e servidores de política), clique no ícone de adição (+) grande para exibir as configurações de AAA.
e) Verifique se o status do servidor AAC do Cisco ISE ainda está **`Active`** (Ativo).

f) Selecione **Policy** > **Registry** > **Scalable Groups** (Política < Registro < Grupos escalonáveis). Você deve ver os grupos ISE SGT na lista de grupos escalonáveis.

Configurar os servidores de autenticação e política

O Cisco DNA Center usa servidores AAA para autenticação de usuário do Cisco ISE e para autenticação de usuário e controle de acesso. Use este procedimento para configurar servidores AAA, incluindo Cisco ISE.

Antes de Iniciar

- Se estiver usando o Cisco ISE para realizar as funções política e AAA, verifique se Cisco DNA Center e Cisco ISE estão integrados conforme descrito em Integração do Cisco ISE com Cisco DNA Center (Integrar).
- Se você estiver usando outro produto (que não seja o Cisco ISE) para executar funções AAA, certifique-se de fazer o seguinte:
  - Registre Cisco DNA Center no servidor AAA, incluindo a definição do segredo compartilhado no servidor AAA e Cisco DNA Center.
  - Defina um nome de atributo do Cisco DNA Center no servidor AAA.
  - Para uma configuração de cluster de vários hosts do Cisco DNA Center, defina todos os endereços IP de host individuais e o endereço IP virtual para o cluster de vários hosts no servidor AAA.

Etapa 1 Na página inicial do Cisco DNA Center, escolha > **System Settings** > **Settings** > **Authentication and Policy Servers** (Configurações do sistema < Configurações < Servidores de autenticação e política).

Etapa 2 Clique em Add.

Etapa 3 Configure o servidor AAA primário fornecendo as seguintes informações:

- **Server IP Address** (Endereço IP do servidor) — endereço IP do servidor AAA.
- **Shared Secret** (Segredo compartilhado) — chave para autenticações de dispositivo. O segredo compartilhado pode ter até 128 caracteres de comprimento.

Etapa 4 Para configurar um servidor AAA (não Cisco ISE), deixe o botão do **Cisco ISE Server** (Servidor do Cisco ISE) na posição **Off** (Desligada) e vá para a próxima etapa.

Para configurar um servidor do Cisco ISE, clique no botão **Cisco ISE Server** (Servidor do Cisco ISE) para a posição **On** (Ligada) e insira as informações nos seguintes campos:

- **Cisco ISE** — configuração que indica se o servidor é de Cisco ISE. Clique na configuração do **Cisco ISE** para ativar o Cisco ISE.
- **Username** (Nome de usuário) — nome usado para fazer login na interface de linha de comando (CLI) de Cisco ISE.

  Observação Este usuário deve ser um superadministrador.

- **Password** (Senha) — senha para o nome de usuário de CLI do Cisco ISE.
- **FQDN** — nome de domínio totalmente qualificado (FQDN) do servidor do Cisco ISE.

  Observação
  - Recomendamos que você copie o FQDN definido no Cisco ISE (**Administration** > **Deployment** > **Deployment Nodes** > **List** [Administração > Implantação > Nós de implantação > Lista]) e cole-o diretamente neste campo.
  - O FQDN inserido deve corresponder ao FQDN, ao nome comum (CN) ou ao nome alternativo de entidade (SAN) definido no certificado de Cisco ISE.

  O FQDN consiste em duas partes, um nome de host e o domínio, no seguinte formato:

  hostname.domainname.com.

  Por exemplo, o FQDN de um servidor do Cisco ISE pode ser ise.cisco.com.
- **Subscriber Name** (Nome do assinante) — sequência de caracteres de texto exclusiva que identifica um registro de cliente pxGrid para serviços de pxGrid do Cisco ISE; por exemplo, `acme`. O nome do assinante é usado durante a integração entre Cisco DNA Center e Cisco ISE.
- SSH Key (Chave SSH) — chave SSH Diffie-Hellman-Group14-SHA1 usada para conectar e autenticar o Cisco ISE.
- **Virtual IP Address(es)** (Endereços IP virtual) — endereço IP virtual do balanceador de carga em que os nós de serviço de política do Cisco ISE (PSNs) estão localizados. Se você tiver vários farms de PSN por trás de balanceadores de carga diferentes, poderá inserir um máximo de seis endereços IP virtuais.

Etapa 5 Clique em **View Advanced Settings** (Exibir configurações avançadas) e defina as configurações:

- **Protocol** (Protocolo) — **TACACS** ou **RADIUS**.

  Observação A opção esmaecida é a opção escolhida (RADIUS, por padrão). Para selecionar a opção TACACS, você precisa selecioná-la e, em seguida, desmarcar manualmente a opção RADIUS.
- **Authentication Port** (Porta de autenticação) — porta usada para retransmitir mensagens de autenticação para o servidor AAA. O padrão é UDP porta 1812.
- **Accounting Port** (Porta designada) — porta usada para retransmitir eventos importantes para o servidor AAA. As informações nesses eventos são usadas para fins de segurança e cobrança. A porta UDP padrão é 1813.
- **Retries** (Novas tentativas) — número de vezes que Cisco DNA Center tenta se conectar ao servidor AAA antes de abandonar a tentativa de conexão. O número de tentativas padrão é 1.
- **Timeout** (Tempo limite) — período que o dispositivo aguarda para o servidor AAA responder antes de abandonar a tentativa de conexão.

Etapa 6 Clique em **Adicionar**.

Etapa 7 Para adicionar um servidor secundário, repita as etapas 2 a 6.

Configurar propriedades de SNMP

Você pode configurar valores de novas tentativas e de tempo limite para SNMP.

Antes de Iniciar

Somente um usuário com permissões SUPER-ADMIN-ROLE pode executar esse procedimento. Para obter mais informações, consulte *Guia do administrador de Cisco Digital Network Architecture Center*.

Etapa 1 Na página inicial do Cisco DNA Center, clique no ícone de engrenagem (⚙) e, em seguida, escolha **System Settings** > **Settings** > **SNMP Properties** (Configurações do sistema > Configurações > Propriedades de SNMP).

Etapa 2 Configure os seguintes campos:

Tabela 37: Propriedades de SNMP

Campo	Descrição
Novas tentativas	Número de tentativas permitidas para se conectar ao dispositivo. Os valores válidos são de 1 a 3. O padrão é 3.
Tempo limite (em segundos)	Número de segundos que o Cisco DNA Center aguarda ao tentar estabelecer uma conexão com um dispositivo antes do tempo limite. Os valores válidos são de 1 a 300 segundos em intervalos de 5 segundos. O padrão é 5 segundos.

Etapa 3 Clique em **Aplicar**.

Observação Para retornar às configurações padrão, clique em **Revert to Defaults** (Reverter aos padrões).

Redistribuir serviços

A implementação de Cisco DNA Center de alta disponibilidade (HA) está descrita no *Guia do administrador do Cisco Digital Network Architecture Center*. Recomendamos que você primeiro analise essas informações e determine se deseja implantar a HA no ambiente de produção. Se decidir fazer isso, otimize a operação de alta disponibilidade redistribuindo serviços entre os nós de cluster:

1. Clique em ⚙ e selecione **System Settings** (Configurações do sistema).

   A guia **System 360** (Sistema 360) é exibida por padrão.

2. Na área **Hosts**, clique em **Enable Service Distribution** (Ativar distribuição de serviço).

Depois de clicar em **Enable Service Distribution** (Ativar distribuição de serviço), Cisco DNA Center entra no modo de manutenção. No modo de manutenção, Cisco DNA Center fica indisponível até que o processo seja concluído. Você deve levar isso em consideração ao agendar uma implantação de alta disponibilidade.

Observação Cisco DNA Center entra no modo de manutenção sempre que você restaurar o banco de dados, executar uma atualização do sistema (não uma atualização de pacote) e habilitar uma redistribuição de serviço para HA (conforme descrito acima).

CAPÍTULO 6

Soluções de problema da implantação

- Tarefas de identificação e solução de problemas, na página 111
- Logout, na página 111
- Reconfigurar o dispositivo usando o assistente de configuração, na página 112
- Reinicializar o dispositivo, na página 113

Tarefas de identificação e solução de problemas

Ao solucionar problemas com a configuração do dispositivo, você normalmente executará as seguintes tarefas:

Tabela 38: Tarefas de solução de problemas básica

Etapa	Descrição
1	Se você estiver usando a interface de usuário do Cisco DNA Center: Logout.
2	Se você precisar reconfigurar o hardware do dispositivo, faça login e use a interface de usuário do CIMC, conforme explicado nas etapas 12 e 13 de Ativar acesso do navegador ao CIMC.
3	Se você precisar alterar a configuração do dispositivo, inicie e use o assistente de configuração do Maglev conforme explicado em Reconfigurar o dispositivo usando o assistente de configuração.
4	Desligue e ligue o dispositivo, de modo que as alterações estejam ativas: Reinicializar o dispositivo.

Para obter mais informações sobre os adaptadores de rede do dispositivo, consulte a seção Gerenciamento de adaptadores do *Guia de configuração de CLI do Servers Integrated Management Controller Cisco UCS C-Series, versão 3.1*. Como mencionado em outro lugar, nunca tente gerenciar o hardware do dispositivo por meio da CLI do Linux. Use somente a interface do usuário de CIMC ou o assistente de configuração do Maglev para alterar as configurações do dispositivo.

Logout

Siga as etapas abaixo para fazer logoff da interface de usuário do Cisco DNA Center baseada na Web.

Por motivos de segurança, recomendamos que você faça logoff sempre que concluir uma sessão de trabalho. Se você não fizer logoff, será desconectado automaticamente após 30 minutos de inatividade.

Etapa 1 Clique em ⚙.

Etapa 2 Clique em **Sign out** (Sair). Isso encerra a sessão e o desconecta.

Reconfigurar o dispositivo usando o assistente de configuração

Se precisar reconfigurar um dispositivo, use o assistente de configuração para atualizar as configurações do dispositivo. Você não pode usar a CLI do Linux para fazer isso. Os procedimentos de administração de Linux normais que você pode usar para atualizar as definições de configuração em um servidor de Linux padrão não funcionarão e não deverão ser tentados.

Quando o dispositivo estiver configurado, você não poderá usar o assistente de configuração para alterar todas as configurações do dispositivo. As alterações são restritas apenas às seguintes configurações:

- Endereço IP do host do dispositivo
- Endereços IP do servidor DNS
- Endereço IP do gateway padrão
- Endereços IP do servidor NTP
- Endereço IP virtual do cluster
- Rotas estáticas
- Endereço IP do servidor proxy
- Senha de usuário do Maglev
- Senha de usuário admin

Antes de Iniciar

Você vai precisar do seguinte:

- Software cliente Secure Shell (SSH).
- O endereço IP que você configurou para a porta empresarial no dispositivo que precisa de reconfiguração. Para identificar essa porta, consulte a figura do painel traseiro nos Painéis frontal e traseiro. Você fará login no dispositivo neste endereço, na porta 2222.
- O nome de usuário Linux (**`Maglev`**) e a senha configurados no dispositivo de destino.

Etapa 1 Usando um cliente SSH (Secure Shell), faça login no endereço IP da porta empresarial do dispositivo que precisa ser reconfigurado, na porta 2222. Por exemplo:

ssh maglev@*Enterprise-port's-IP-address* **-p 2222**

Etapa 2 Quando solicitado, insira a senha do Linux.

Etapa 3 Digite o comando a seguir para acessar o assistente de configuração.

```
$ sudo maglev-config update
```

Se for solicitada a senha de Linux, insira-a novamente.

Etapa 4 O assistente de configuração apresentará uma versão abreviada da mesma série de telas mostrada em, por exemplo, Configurar os nós complementares. Faça todas as alterações necessárias nas configurações apresentadas. Quando terminar de fazer as alterações em cada tela, escolha **[Next]** [Avançar] conforme necessário para prosseguir pelo assistente de configuração.

Etapa 5 No final do processo de configuração, uma mensagem será exibida informando que o assistente de configuração está pronto para aplicar as alterações. As seguintes opções estão disponíveis:

- **[back]** [voltar] — revise e verifique as alterações.
- **[cancel]** [cancelar] - descarte as alterações e saia do assistente de configuração.
- **[proceed]** [continuar] — salve as alterações e comece a aplicá-las.

Escolha **proceed>>** (prosseguir) para concluir a instalação. O assistente de configuração aplica as alterações que você fez.

No final do processo de configuração, uma mensagem de **CONFIGURATION SUCCEEDED!** (CONFIGURAÇÃO BEM-SUCEDIDA!) é exibida.

O que Fazer Depois

Certifique-se de que as alterações sejam aplicadas e estejam ativas ao desligar e ligar o dispositivo, conforme explicado no tópico Reinicializar o dispositivo.

Observação Se você atualizou os endereços IP do servidor DNS, recomendamos que faça uma inicialização a frio ao desligar o dispositivo. Isso garantirá que as alterações de DNS sejam aplicadas.

Reinicializar o dispositivo

Conclua o procedimento a seguir no dispositivo Cisco DNA Center para interrompê-lo ou executar uma reinicialização a quente. Você pode interromper o dispositivo antes de fazer reparos de hardware ou pode iniciar uma reinicialização a quente após ter corrigido os problemas de software. Todas as alterações de hardware feitas usando o Cisco IMC serão aplicadas depois que o dispositivo for reinicializado.

Observe que também é possível reinicializar um dispositivo da interface de usuário do Cisco IMC e do console do KVM que pode ser acessado pela interface gráfica do Cisco IMC. Para obter detalhes, consulte as etapas de 1 a 3 em Configurar o nó mestre ou Configurar os nós complementares.

Cuidado Desligar e ligar o equipamento da interface de usuário do Cisco IMC pode resultar em danos ou perda de dados. Faça isso apenas se o dispositivo não responder completamente ao SSH, ao console Cisco IMC ou ao console físico.

Antes de Iniciar

Você vai precisar do seguinte:

- Software cliente Secure Shell (SSH).
- O endereço IP que você configurou para a porta empresarial de 10 Gbps no dispositivo que precisa de reconfiguração. Para identificar essa porta, consulte a figura do painel traseiro nos Painéis frontal e traseiro. Você fará login no dispositivo neste endereço, na porta 2222.
- O nome de usuário Linux (*Maglev*) e a senha atualmente configurada no dispositivo de destino.

Etapa 1 Usando um cliente SSH (Secure Shell), faça login no endereço IP da porta empresarial do dispositivo que precisa ser reconfigurado, na porta 2222.

ssh maglev@*Enterprise-port's-IP-address* **-p 2222**

Etapa 2 Quando solicitado, insira a senha do Linux.

Etapa 3 Digite o comando apropriado para a tarefa que você deseja executar:

- Para interromper o dispositivo, digite: **sudo shutdown -h now**
- Para iniciar uma reinicialização a quente, insira: **sudo shutdown -r now**

  Se for solicitada a senha de Linux, insira-a novamente.

Etapa 4 Revise a saída do comando exibida quando o host é desligado.

Etapa 5 Se você interrompeu o equipamento, desligue o processo raiz do Maglev ligando o dispositivo novamente, com o botão liga/desliga do painel frontal.