Provisioning del fabric di Software-Defined Access

Guida prescrittiva all'implementazione

Luglio, 2019

Sommario

Definizione e progettazione: Software-Defined Access

Cisco® Software-Defined Access (SD-Access) permette di trasformare le tradizionali progettazioni della LAN del campus in reti in grado di implementare direttamente l'intento di un'azienda. SD-Access viene fornito con pacchetto applicativo da usare insieme al software Cisco DNA Center per progettare, effettuare il provisioning, applicare le policy e facilitare la creazione di una rete per campus intelligente e sicura, cablata o wireless.

Questa guida viene usata per implementare l'infrastruttura di gestione, che comprende Cisco DNA Center, Cisco Identity Services Engine (ISE) e i Cisco Wireless LAN Controller (WLC), descritti nella guida alla progettazione della soluzione Software-Defined Access. L'implementazione descritta in questa guida precede l'implementazione di un fabric di Cisco Software-Defined Access, come descritto nella guida all'implementazione del fabric di Software-Defined Access.

Se questa guida non è stata scaricata da Cisco Community o Design Zone, controllare che sia la versione più recente.

Per la guida alla progettazione della soluzione Software-Defined Access, la guida prescrittiva all'implementazione dell'infrastruttura di gestione di Software-Defined Access, la guida prescrittiva all'implementazione di Software-Defined Access for Distributed Campus, le guide all'implementazione, le guide alla progettazione e i white paper correlati, fare riferimento alle seguenti pagine:

- https://www.cisco.com/go/designzone
- https://cs.co/en-cvds

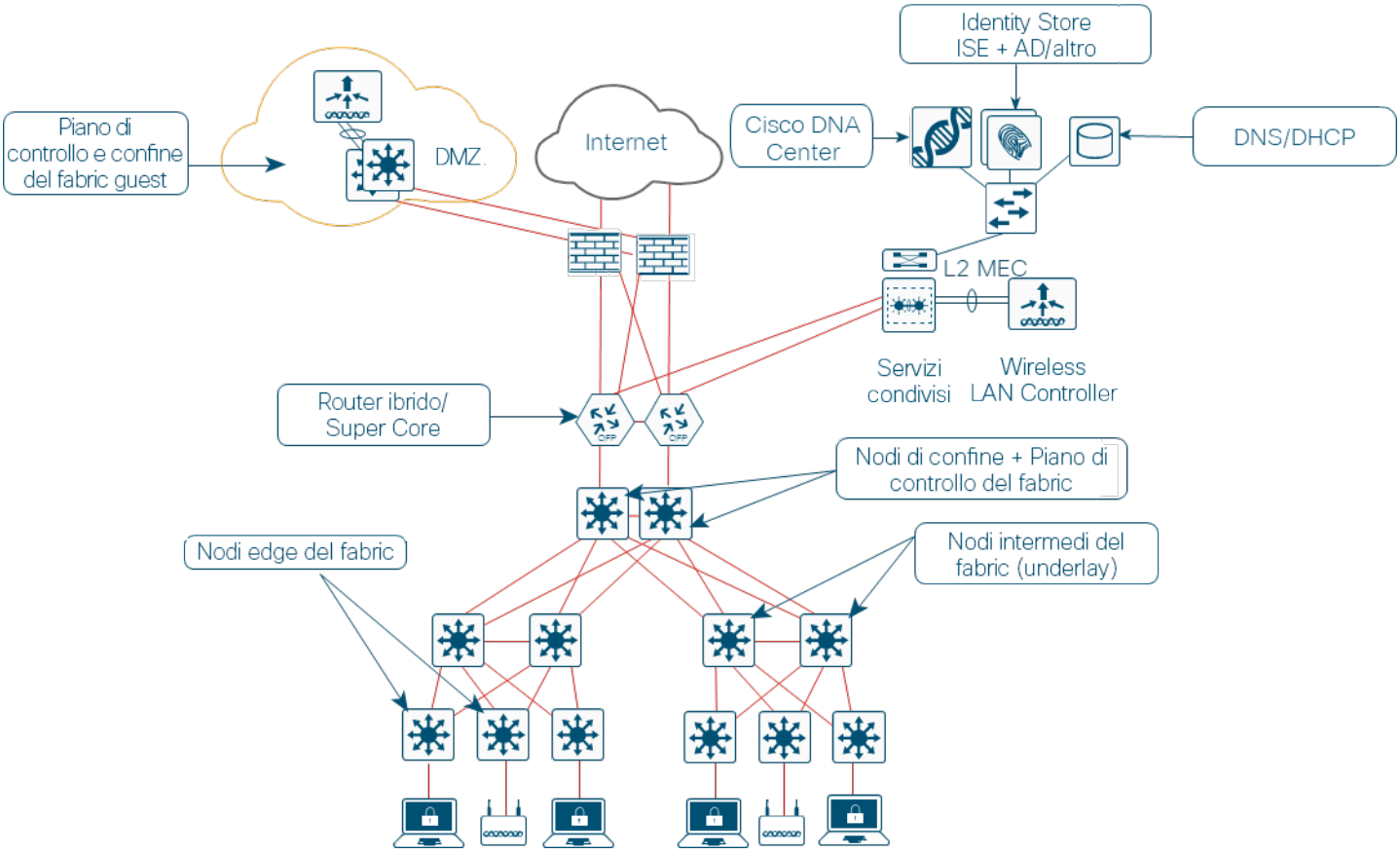
Implementazione: SD-Access Fabric

Come leggere i comandi di implementazione

Nella guida vengono utilizzate le seguenti convenzioni per i comandi da immettere sull'interfaccia della riga di comando (CLI).
Comandi da immettere al prompt della CLI:
`configure terminal`
Comandi che specificano un valore per una variabile (variabile in corsivo e in grassetto):
`ntp server` ***`10.4.0.1`***
Comandi con variabili che devono essere definite dall'utente (definizione in grassetto e in corsivo, racchiusa tra parentesi quadre):
`class-map` ***`[highest class name]`***
Comandi al prompt CLI o script (comandi da immettere in grassetto):
`Router#` **`enable`**
Comandi lunghi per cui è necessario andare a capo sulla pagina stampata (il testo sottolineato va immesso come un unico comando):
`police rate` ***`1000`*** `pps burst` ***`10000`***
`packets conform-action`

I componenti di gestione di SD-Access vengono implementati nella topologia descritta nella guida alla progettazione della soluzione Software-Defined Access, come mostrato nel relativo diagramma. In questa guida si presume che l'infrastruttura di gestione composta da Cisco DNA Center, Cisco Identity Services Engine (ISE) e Cisco Wireless LAN Controller (WLC) sia già stata installata e sia disponibile, come descritto nella guida all'implementazione dell'infrastruttura di gestione di Software-Defined Access.

Figura 1.
Topologia di convalida



La rete aziendale integrata nell'implementazione del fabric del campus descritto non è virtualizzata e usa il protocollo EIGRP (Enhanced Interior Gateway Routing Protocol) come protocollo di routing. I prefissi IP del campus, inclusi i servizi condivisi, devono essere disponibili sia sul fabric underlay sia sul fabric overlay; le varie reti overlay devono rimanere isolate. Per mantenere l'isolamento, VRF-Lite si estende dai nodi di confine del fabric a un gruppo di router ibridi. I router ibridi implementano il route leaking del VRF con una configurazione di importazione ed esportazione dei route target BGP ed eseguono una ridistribuzione reciproca con il protocollo EIGRP nella rete aziendale e con il protocollo BGP nel fabric del campus. Una configurazione route-map per assegnare i tag e applicare i filtri in modo dinamico alle route ridistribuite rappresenta un modo semplice e agile di impedire i loop di routing e allo stesso tempo di avere più punti di ridistribuzione in una progettazione ad alta disponibilità.

Procedura – Uso di Cisco DNA Center per la progettazione e il rilevamento iniziali della rete

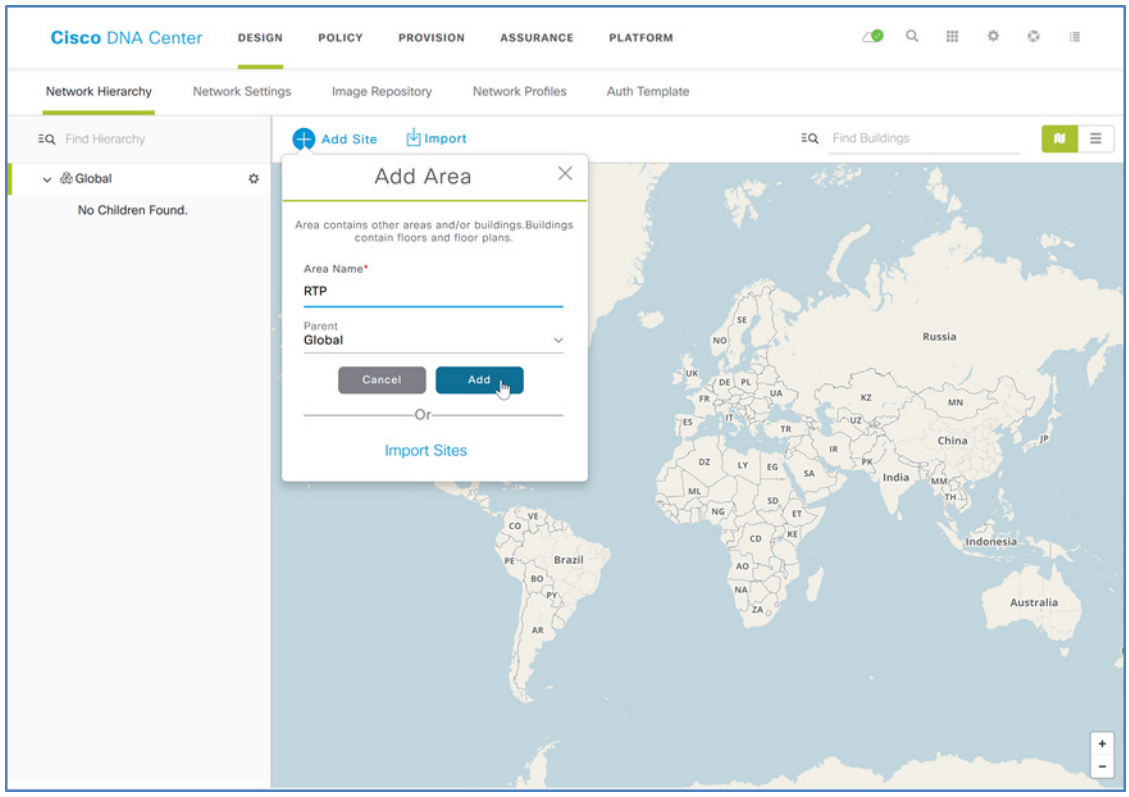
Cisco DNA Center offre un'applicazione di progettazione solida che permette a clienti di varie dimensioni e necessità di definire con facilità le sedi fisiche e le risorse comuni. Utilizzando un formato gerarchico intuitivo, l'applicazione di progettazione rende superflua la necessità di ridefinire le stesse risorse, come i server DHCP, DNS e AAA, in più posizioni durante il provisioning dei dispositivi. La gerarchia di rete creata nell'applicazione di progettazione deve simulare la gerarchia di rete fisica effettiva dell'implementazione.

Con Cisco DNA Center, è possibile creare una gerarchia di rete con aree che possono contenere altre aree o edifici e piani. I dispositivi sono associati agli edifici e ai piani per il provisioning dei servizi.

Procedura 1. Creazione delle sedi della rete

Passaggio 1. Accedere a Cisco DNA Center. Dalla dashboard principale di Cisco DNA Center, accedere a Design (Progettazione) > Network Hierarchy (Gerarchia di rete).

Passaggio 2. Fare clic su **Add Site** (Aggiungi sede), nel menu a discesa selezionare **Add Area** (Aggiungi area), fornire un nome appropriato in **Area Name** (Nome area), quindi fare clic su **Add** (Aggiungi).



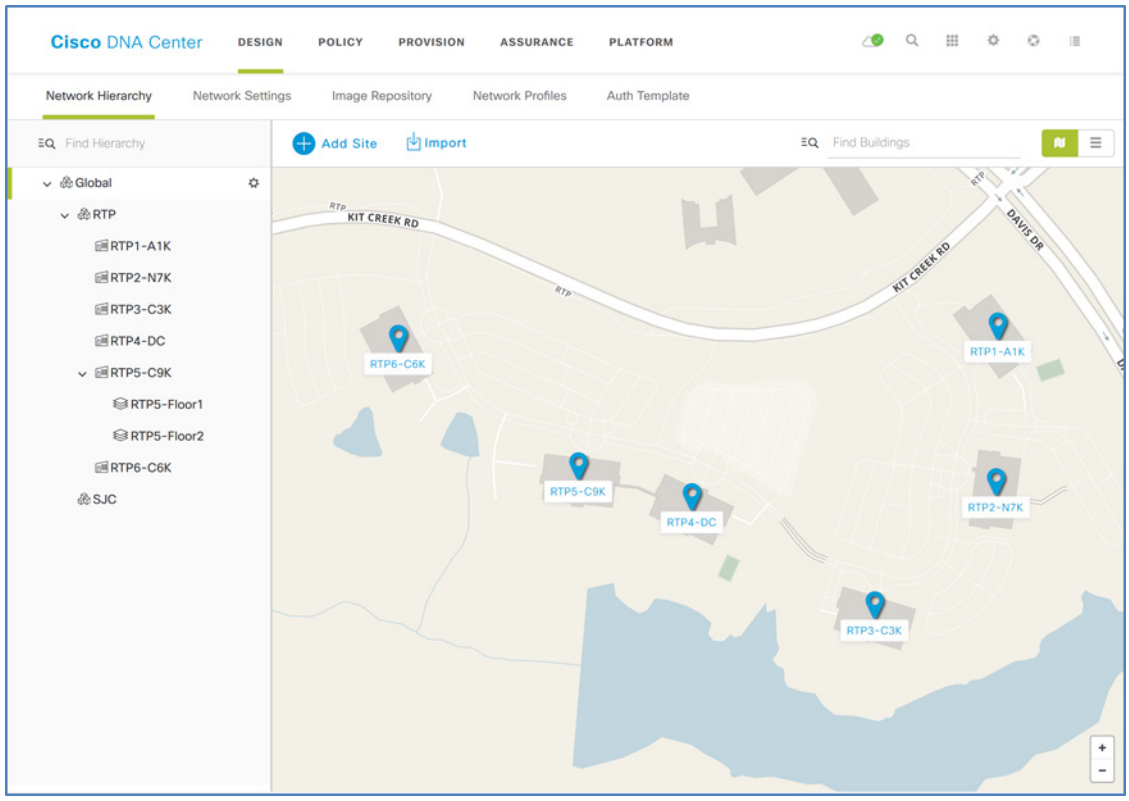
Passaggio 3. Fare clic su **Add Site** (Aggiungi sede), nel menu a discesa, premere il pulsante **Add Building** (Aggiungi edificio), fornire un nome appropriato in **Building Name** (Nome edificio), contrassegnare la sede creata al passaggio precedente come **Parent** (Principale), completare la procedura guidata per l'assegnazione di una posizione, quindi fare clic su **Add** (Aggiungi).

Per aggiungere un edificio, è possibile inserire un indirizzo nelle sue prossimità durante la procedura guidata oppure, se lo si desidera, specificare con maggiore precisione la posizione dell'edificio sulla mappa facendo clic direttamente sul punto desiderato.

Passaggio 4. Ripetere il passaggio precedente secondo necessità per aggiungere le sedi e gli edifici, creando una gerarchia che rifletta le esigenze dell'azienda.

Passaggio 5. Se si sta integrando un sistema wireless nell'edificio o le scelte di rete all'interno dell'edificio devono essere più granulari, selezionare l'edificio sulla mappa (oppure selezionare l'icona ingranaggio accanto all'edificio nella gerarchia), selezionare **Add Floor** (Aggiungi piano), quindi fornire i dettagli richiesti per completare la procedura guidata.

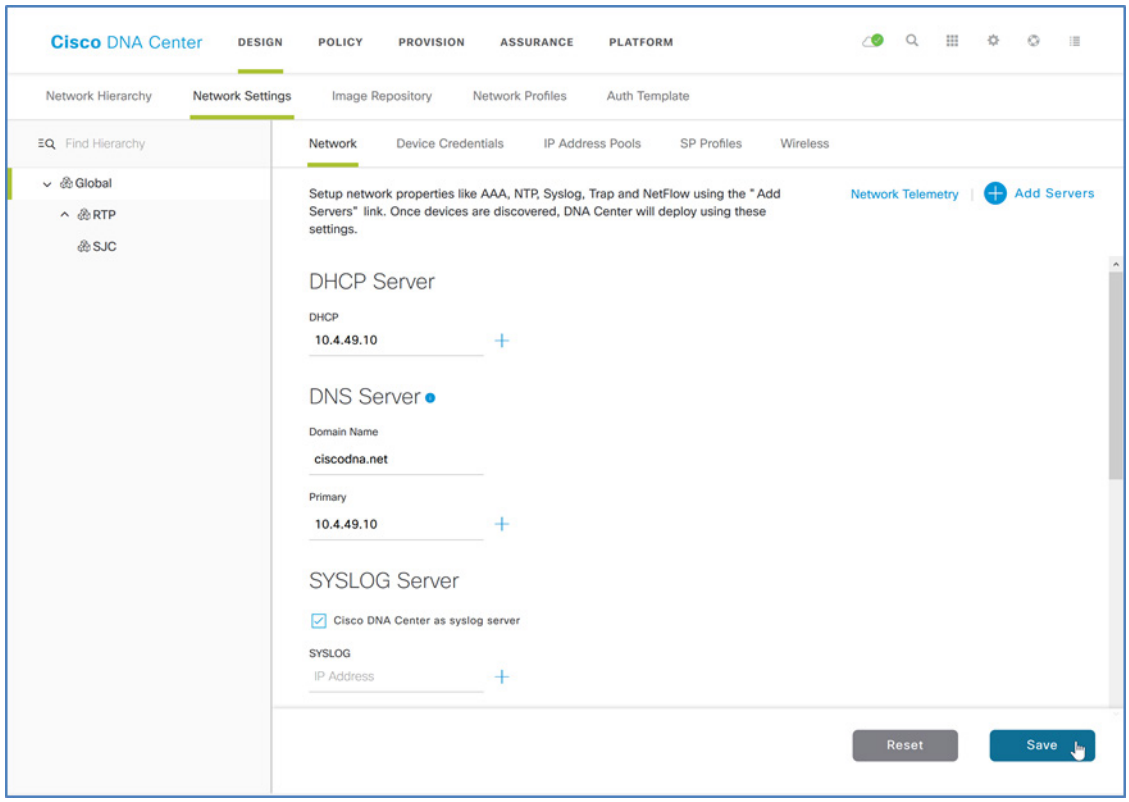
I riferimenti ai piani vengono assegnati durante il provisioning del sistema wireless. Se si dispone di diagrammi di planimetria nei formati DXF, DWG, JPG, GIF o PNG, aggiungerli ai piani definiti, in quanto rappresentano per le implementazioni wireless un utile strumento per visualizzare le posizioni e la copertura degli access point. È possibile aggiungere centinaia di sedi fino al limite massimo consentito come descritto nella guida alla progettazione della soluzione Software-Defined Access.



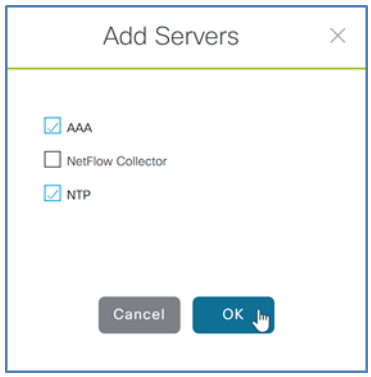
Procedura 2. Configurazione dei servizi di rete per le sedi

Configurare i servizi AAA, DHCP e DNS compatibili con la gerarchia di Cisco DNA Center. Se i servizi utilizzano gli stessi server nell'intera gerarchia, è possibile configurarli a livello globale: le proprietà di ereditarietà della gerarchia fanno sì che le impostazioni globali siano disponibili in tutte le sedi. Eventuali differenze possono poi essere applicate sulle singole sedi. In questa procedura viene descritta la configurazione a livello globale.

Passaggio 1. In Cisco DNA Center, accedere a **DESIGN** (Progettazione) **> Network Settings** (Impostazioni di rete) **> Network** (Rete). Nel riquadro a sinistra con la gerarchia delle sedi, selezionare il livello appropriato (ad esempio, Global (Globale)), specificare l'indirizzo IP nel campo **DHCP Server** (Server DHCP) (ad esempio, 10.4.49.10), in DNS Server (Server DNS) specificare il nome di dominio (ad esempio, ciscodna.net) e l'indirizzo IP **Primary** (Principale) del server (ad esempio, 10.4.49.10). Aggiungere eventuali server ridondanti o aggiuntivi (per usare Cisco DNA Center per i server SYSLOG e SNMP, lasciare invariate le impostazioni predefinite), quindi fare clic su **Save** (Salva).



Passaggio 2. Nella parte superiore della schermata, accanto a **Network Telemetry** (Telemetria di rete), fare clic sul pulsante **+ Add Servers** (+ Aggiungi server), selezionare le caselle di controllo **AAA** e **NTP**, quindi fare clic su **OK**.



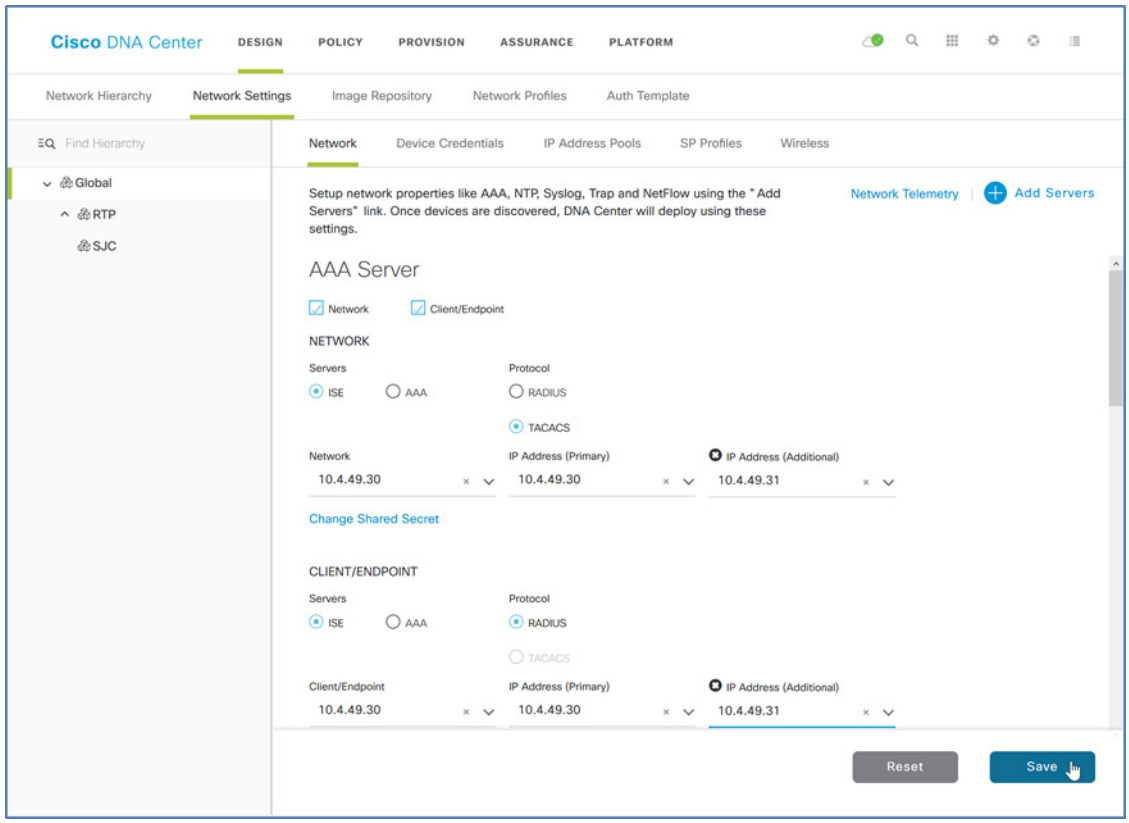
Il riquadro di configurazione viene aggiornato con le sezioni **AAA Server** (Server AAA) e **NTP Server** (Server NTP). I servizi AAA vengono configurati sia per l'amministrazione dei dispositivi dell'infrastruttura di rete sia per gli endpoint client che si connettono all'infrastruttura. In questo esempio, vengono utilizzati nodi ISE standalone ad alta disponibilità.

Suggerimento tecnico
Molte aziende utilizzano TACACS per il supporto amministrativo dei dispositivi dell'infrastruttura. Se si intende abilitare TACACS sullo stesso server ISE utilizzato per l'autenticazione dei client RADIUS, è possibile integrarlo in Cisco DNA Center durante questo passaggio utilizzando il menu a discesa **View Advanced Settings** (Visualizza impostazioni avanzate). Per informazioni sulla configurazione ISE per abilitare l'integrazione TACACS, in ISE accedere a **Work Centers** (Centri di lavoro) **> Device Administration** (Amministrazione dispositivi) **> Overview** (Panoramica).

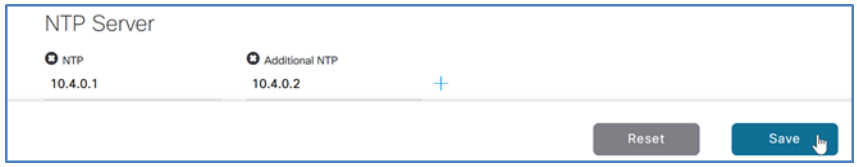
Passaggio 3. In **AAA Server** (Server AAA), selezionare le caselle di controllo **Network** (Rete) e **Client/Endpoint**, in **NETWORK** (Rete), selezionare il pulsante di scelta **ISE**, in **Network** (Rete) utilizzare il menu a discesa per selezionare il server ISE precompilato (ad esempio, 10.4.49.30). In **Protocol** (Protocollo), selezionare il pulsante di scelta **TACACS**, in **IP Address (Primary)** (Indirizzo IP – Principale) utilizzare il secondo menu a discesa e selezionare il server ISE principale (ad esempio, 10.4.49.30), fare clic sul pulsante con il segno più (**+**), quindi nel menu a discesa **IP Address (Additional)** (Indirizzo IP – Aggiuntivo), selezionare il nodo del server ISE ridondante (ad esempio, 10.4.49.31).

Per garantire che la ridondanza del server ISE sia stata abilitata correttamente, verificare che gli indirizzi IP principale e aggiuntivo vengano visualizzati insieme all'indirizzo di rete selezionato prima di continuare.

Passaggio 4. In **CLIENT/ENDPOINT** e **Servers** (Server), selezionare il pulsante di scelta **ISE**, in **Client/Endpoint**, dal menu a discesa selezionare il server ISE precompilato. In **Protocol** (Protocollo), selezionare il pulsante di scelta **RADIUS**, in **IP Address (Primary)** (Indirizzo IP – Principale), utilizzare il menu a discesa per selezionare il server ISE principale, fare clic sul pulsante con il segno più (**+**), quindi in **IP Address (Additional)** (Indirizzo IP – Aggiuntivo), dal menu a discesa selezionare il nodo del server ISE ridonante, quindi fare clic su **Save** (Salva).



Passaggio 5. Nella stessa schermata, scorrere verso il basso fino a **NTP Server** (Server NTP), aggiungere l'indirizzo IP del server NTP nel campo **IP address** (Indirizzo IP) (ad esempio, 10.4.0.1). In presenza di altri server NTP, selezionare il pulsante con il segno più (**+**), quindi in **Additional NTP** (NTP aggiuntivi), aggiungere l'indirizzo IP dei server NTP ridondanti (ad esempio, 10.4.0.2), quindi fare clic su **Save** (Salva).



I server ISE per AAA e i server per DHCP, DNS e NTP per il livello selezionato nella gerarchia delle sedi vengono tutti salvati per essere utilizzati durante il provisioning del fabric.

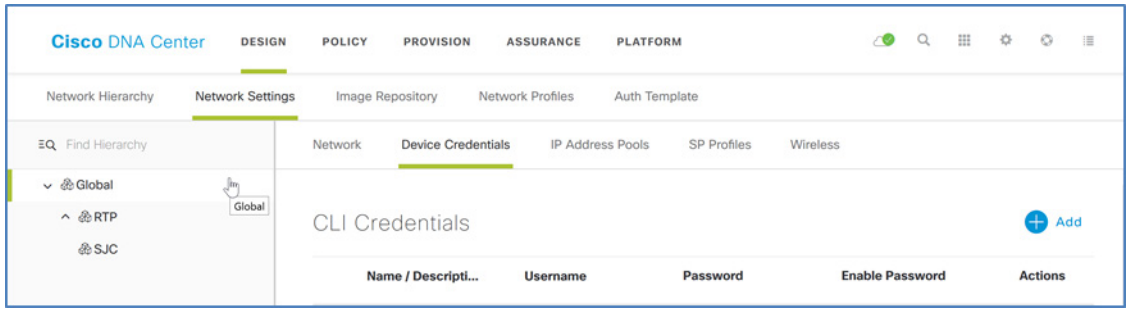
Procedura 3. Aggiunta delle credenziali dei dispositivi per consentirne il rilevamento e la gestione

Quando si implementa la rete underlay di SD-Access con i dispositivi già configurati e raggiungibili sulla rete da Cisco DNA Center, per rilevare e gestire i dispositivi è necessario fornire le credenziali CLI e SNMP (Simple Network Management Protocol).

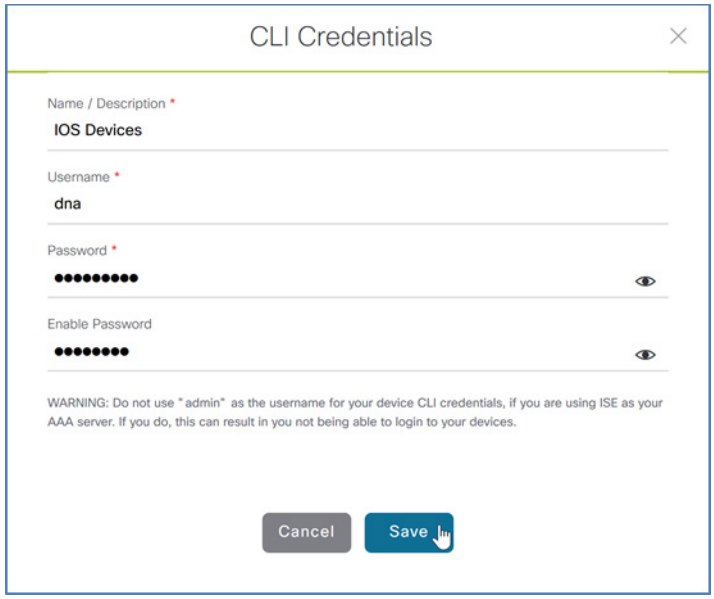
In alternativa, è possibile implementare gli switch LAN non ancora configurati nell'underlay utilizzando le funzionalità di automazione LAN di Cisco DNA Center. Cisco Network Plug and Play (PnP) è lo strumento che permette di connettere e configurare nella fase iniziale gli switch supportati. Per le implementazioni della funzionalità di automazione LAN, è necessario fornire le credenziali CLI e SNMP per accedere e preparare uno o più dispositivi seed PnP supportati, ad esempio i Cisco Catalyst serie 9500 Switch, in modalità distribuzione o core. L'automazione LAN rileva gli switch connessi direttamente alle interfacce dei dispositivi seed selezionati e gli switch nelle immediate vicinanze utilizzando Cisco Discovery Protocol; questi switch devono tutti utilizzare l'agente PnP e non avere configurazioni pregresse. Le credenziali fornite permettono a Cisco DNA Center e ai dispositivi seed di collaborare insieme per configurare i dispositivi rilevati e aggiungerli all'inventario gestito.

Aggiungere le credenziali dei dispositivi per gestire gli ambiti della gerarchia delle sedi creati nella progettazione. Queste credenziali abilitano il rilevamento e la gestione della rete.

Passaggio 1. In Cisco DNA Center, accedere a **Design** (Progettazione) **> Network Settings** (Impostazioni di rete) **> Device Credentials** (Credenziali del dispositivo) e selezionare un livello appropriato per la gerarchia delle sedi sul riquadro sinistro (ad esempio, Global (Globale), per le credenziali comuni all'intera gerarchia).

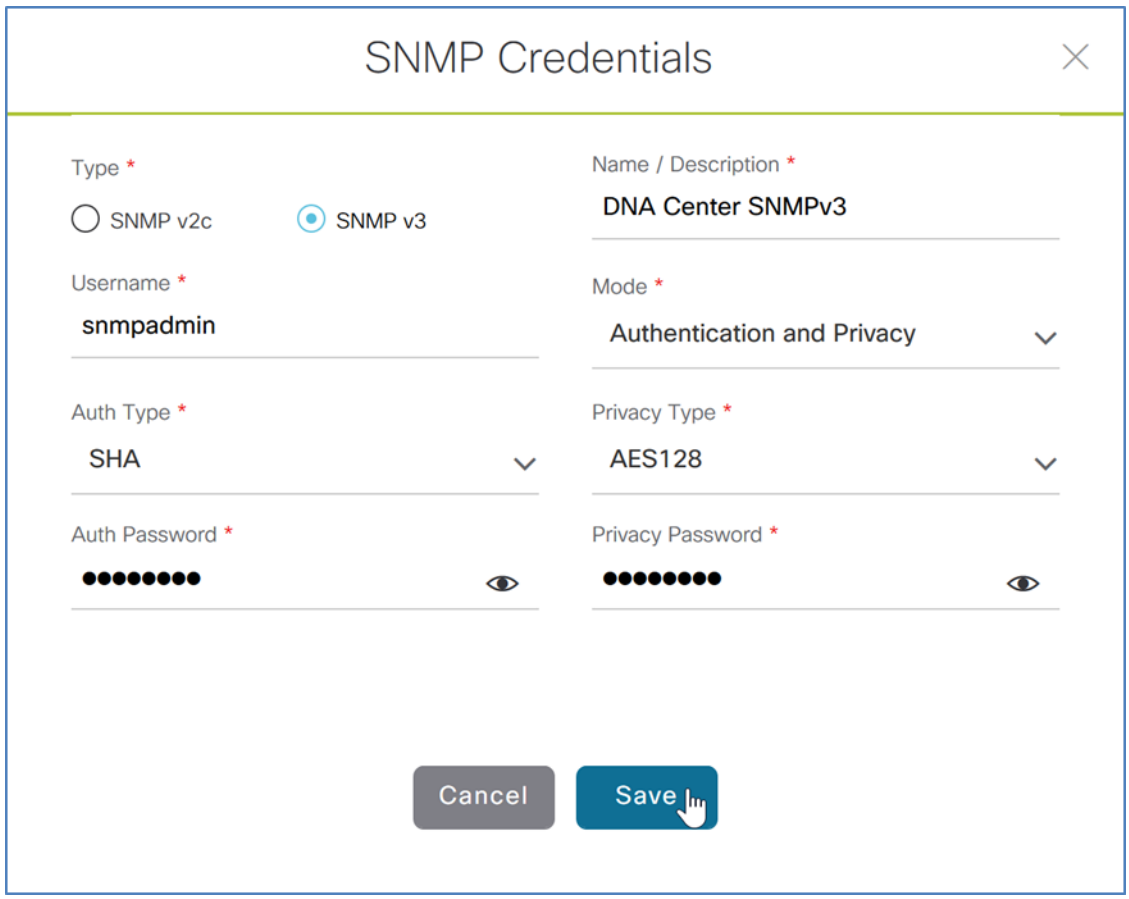


Passaggio 2. Nella parte superiore della sezione **CLI Credentials** (Credenziali CLI), fare clic su **Add** (Aggiungi), completare i campi **Name / Description** (Nome/descrizione) (ad esempio, dispositivi IOS), **Username** (Nome utente), **Password** e **Enable Password** (Password di abilitazione), quindi fare clic su **Save** (Salva).



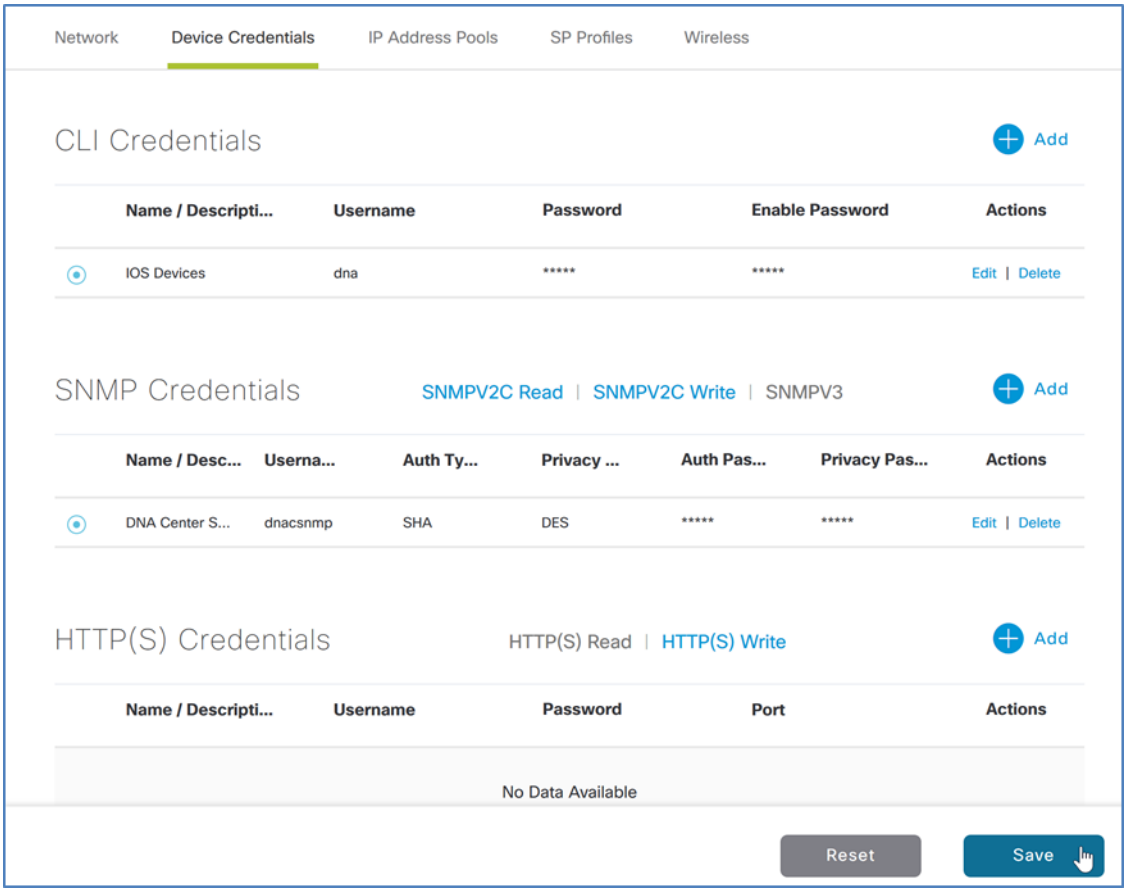
Attenzione
Se si utilizza ISE come server AAA, evitare di usare **admin** come nome utente per le credenziali CLI del dispositivo, perché ciò potrebbe entrare in conflitto con i dati di accesso dell'amministratore ISE e potrebbe bloccare l'accesso ai dispositivi.

Passaggio 3. Nella parte superiore della sezione **SNMP Credentials** (Credenziali SNMP), selezionare un tipo di credenziale SNMP da aggiornare (ad esempio, SNMPV3). Fare clic su **Add** (Aggiungi), selezionare il pulsante di scelta sulla riga accanto alla credenziale da aggiungere (una sola credenziale per riga alla volta), specificare i dettagli della credenziale (si consiglia l'uso di password di 12 caratteri compatibili con i Cisco WLC), quindi fare clic su **Save** (Salva).



Passaggio 4. Ripetere i passaggi 2 e 3 per tutte le credenziali aggiuntive richieste nella gerarchia. Le **credenziali CLI** e **SNMPV3** o entrambi **SNMPV2C Read** (SNMPV2C in lettura) e **SNMPV2C Write** (SNMPV2C in scrittura) sono i requisiti più comuni.

Passaggio 5. Per ciascuna delle credenziali CLI e SNMP assegnate, fare clic su tutti i pulsanti di scelta accanto a ciascuna assegnazione creata. Dopo ciascuna selezione, nella parte inferiore della schermata Device Credentials (Credenziali dispositivo), fare clic su **Save** (Salva). Se sono stati utilizzati più tipi di credenziali SNMP, ripetere questo passaggio selezionando ciascuna opzione delle credenziali SNMP, quindi fare clic sul pulsante di scelta accanto all'opzione e fare clic su **Save** (Salva).



Viene visualizzato un messaggio di conferma sulla corretta creazione delle impostazioni comuni. Le credenziali del dispositivo da usare per il rilevamento e la gestione della rete sono ora disponibili in Cisco DNA Center.

Procedura 4. Definizione dei pool di indirizzi IP globali

Definire gli indirizzi IP delle reti assegnandoli manualmente in Cisco DNA Center. Facoltativamente, è possibile inoltrare le assegnazioni degli indirizzi IP a un sistema di gestione specifico (IPAM) (ad esempio: Infoblox, BlueCat) integrando l'IPAM tramite le API. Per l'integrazione nell'IPAM, accedere a **System Settings** (Impostazioni di sistema) **> Settings** (Impostazioni) **> IP Address Manager** (Sistema di gestione indirizzi IP) e compilare il modulo con le specifiche del provider IPAM. In questo esempio, non utilizzando l'integrazione IPAM, gli indirizzi IP e gli ambiti DHCP devono essere configurati manualmente sui server IPAM in modo che corrispondano alle assegnazioni in Cisco DNA Center.

Gli ambiti DHCP configurati sul server DHCP devono supportare le allocazioni degli indirizzi ed eventuali opzioni DHCP aggiuntive necessarie per far funzionare un dispositivo. Ad esempio, alcuni fornitori di telefonia IP richiedono opzioni DHCP specifiche per assicurare il corretto funzionamento dei dispositivi (ad esempio, l'opzione DHCP 150 per la configurazione da parte del server TFTP). Controllare la documentazione del prodotto per adattare i requisiti all'implementazione.

In questa procedura viene descritto come definire manualmente i pool di indirizzi IP da usare durante il processo di prenotazione dei pool. Questi pool vengono assegnati alle sedi della rete e tale assegnazione deve essere fatta sia per le implementazioni manuali che per le implementazioni con IPAM integrato. È possibile creare un pool globale più grande e prenotare un sottoinsieme di un pool a livelli più bassi nella gerarchia delle sedi. I pool di indirizzi IP vengono creati solo a livello globale, mentre gli indirizzi prenotati dai pool vengono creati solo ai livelli diversi dal livello globale.

L'implementazione descritta in questa guida usa i pool di indirizzi globali elencati nella tabella. Per facilitare la comprensione, vengono usati spazi degli indirizzi più piccoli per il pool di indirizzi globale rispetto a quelli che verrebbero tipicamente usati da un'azienda, ad esempio uno spazio degli indirizzi /16 o superiore. I pool di indirizzi globali più grandi permettono di prenotare un numero maggiore di spazi degli indirizzi di dimensioni inferiori nella gerarchia delle sedi, come mostrato nell'esempio EMPLOYEE. Anche se è richiesta l'assegnazione dell'indirizzo di un gateway IP per ciascun pool, SD-Access usa il gateway solo quando si crea una rete overlay. Nella tabella sono inclusi anche i pool di esempio disponibili sia per la LAN underlay manuale che per una LAN underlay automatica separata e per il peering multicast.

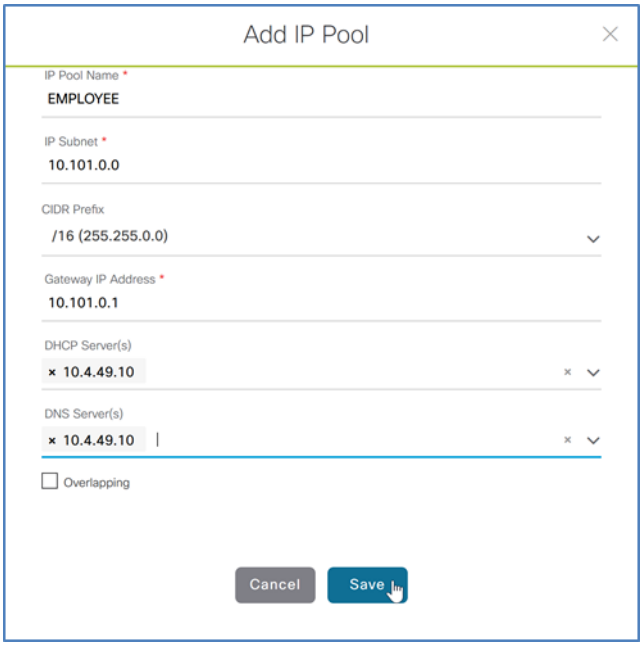
Tabella 1. Esempio di pool di indirizzi globali

Nome pool	Rete/maschera	IP gateway	Server DHCP	Server DNS
EMPLOYEE	10.101.0.0/16	10.101.0.1	10.4.49.10	10.4.49.10
BUILDING_CONTROL	10.102.114.0/24	10.102.114.1	10.4.49.10	10.4.49.10
GUEST	10.103.114.0/24	10.103.114.1	10.4.49.10	10.4.49.10
LAN_UNDERLAY	10.4.14.0/24	10.4.14.1	10.4.49.10	10.4.49.10
LAN_AUTOMATION	10.5.100.0/24	10.5.100.1	10.4.49.10	10.4.49.10
BORDER_HANDOFF	172.16.172.0/24	172.16.172.1	–	–
MULTICAST_PEER	172.16.173.0/24	172.16.174.1	–	–
ACCESS_POINT	172.16.174.0/24	172.16.173.1	10.4.49.10	10.4.49.10

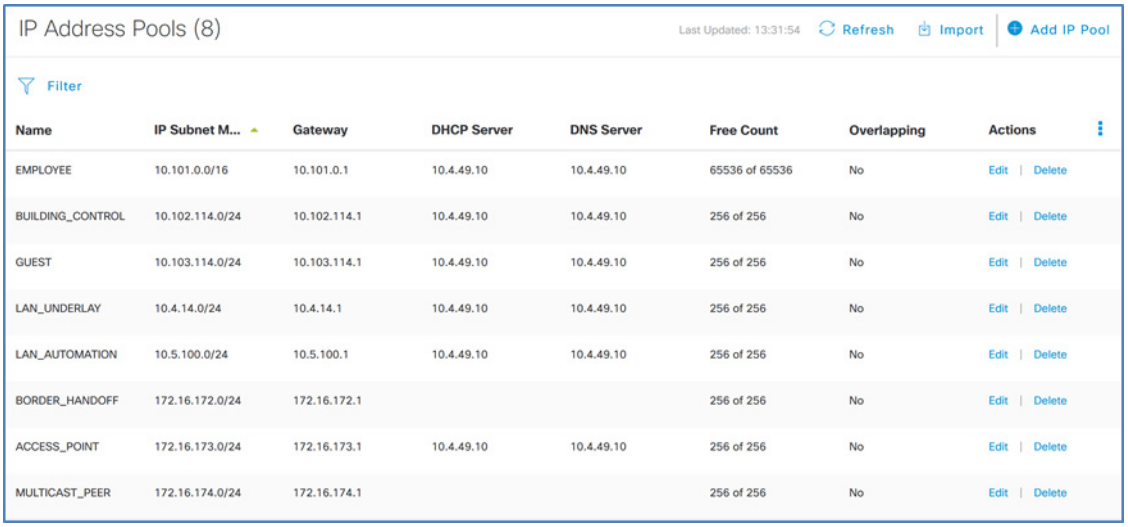
Tabella 2. Esempio di prenotazioni di pool di indirizzi dal pool globale EMPLOYEE

Nome pool	Rete/maschera	IP gateway	Server DHCP	Server DNS
DIPENDENTE-DATI-RTP5	10.101.114.0/24	10.101.114.1	10.4.49.10	10.4.49.10
DIPENDENTE-TELEFONO-RTP5	10.101.214.0/24	10.101.214.1	10.4.49.10	10.4.49.10

Passaggio 1. Aggiungere un pool globale in Cisco DNA Center dedicato al provisioning della connettività dei nodi di confine del fabric di SD-Access. In Cisco DNA Center, accedere a **DESIGN** (Progettazione) **> Network Settings** (Impostazioni di rete) **> IP Address Pools** (Pool di indirizzi IP). Nella gerarchia delle sedi a sinistra, selezionare **Global** (Globale), quindi fare clic su **+ Add IP Pool** (+ Aggiungi pool di IP). Inserire i valori per **IP Pool Name** (Nome pool di IP), **IP Subnet** (Subnet IP), **CIDR Prefix** (Prefisso CIDR) e **Gateway IP Address** (Indirizzo IP del gateway). Se il pool dispone di client endpoint, utilizzare i menu a discesa per assegnare il **server DHCP** e i **server DNS**. Non selezionare **Overlapping** (Sovrapposizione). Una volta terminate le modifiche, fare clic su **Save** (Salva).



Passaggio 2. Ripetere il passaggio precedente per tutti gli altri pool di IP globali che includono le subnet a livello di sede e di edificio. I pool vengono aggiunti all'elenco dei pool globali.

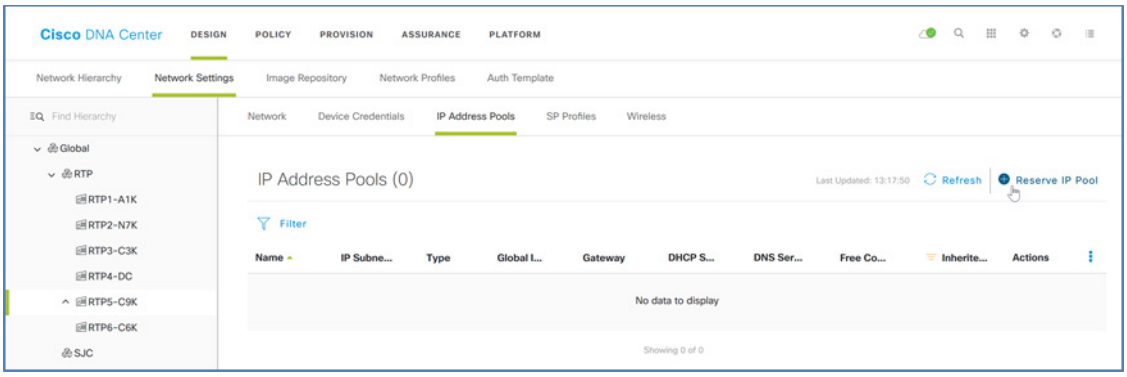


Name	IP Subnet M...	Gateway	DHCP Server	DNS Server	Free Count	Overlapping	Actions
EMPLOYEE	10.101.0.0/16	10.101.0.1	10.4.49.10	10.4.49.10	65536 of 65536	No	Edit | Delete
BUILDING_CONTROL	10.102.114.0/24	10.102.114.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit | Delete
GUEST	10.103.114.0/24	10.103.114.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit | Delete
LAN_UNDERLAY	10.4.14.0/24	10.4.14.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit | Delete
LAN_AUTOMATION	10.5.100.0/24	10.5.100.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit | Delete
BORDER_HANDOFF	172.16.172.0/24	172.16.172.1			256 of 256	No	Edit | Delete
ACCESS_POINT	172.16.173.0/24	172.16.173.1	10.4.49.10	10.4.49.10	256 of 256	No	Edit | Delete
MULTICAST_PEER	172.16.174.0/24	172.16.174.1			256 of 256	No	Edit | Delete

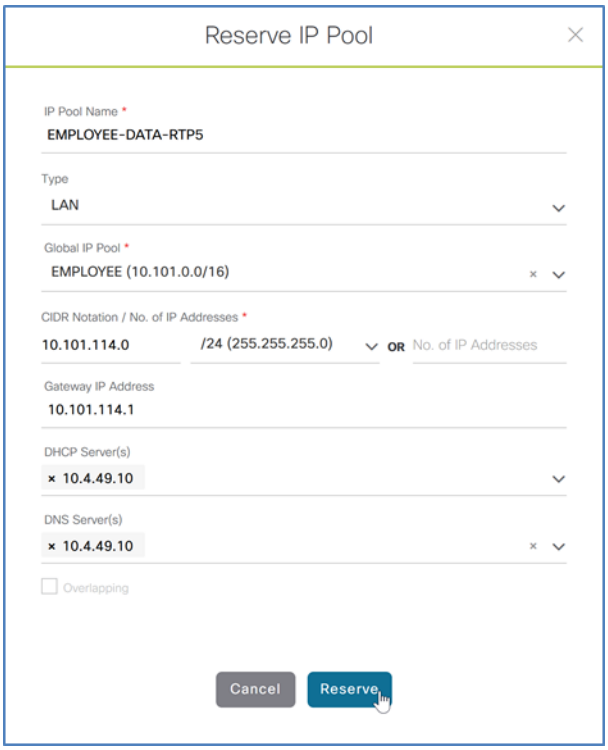
Procedura 5. Prenotazione dei pool di indirizzi IP

Utilizzare i pool di indirizzi IP globali definiti per prenotare gli indirizzi IP delle sedi utilizzando la gerarchia di rete. Nelle implementazioni con sede unica, è possibile prenotare l'intero gruppo di pool di indirizzi IP globali per quella sede. Quando si prenotano gli indirizzi dai pool di indirizzi IP globali definiti, è possibile usare i server DNS e DHCP oppure ignorarli.

Passaggio 1. In Cisco DNA Center, accedere a **DESIGN** (Progettazione) **> Network Settings** (Impostazioni di rete) **> IP Address Pools** (Pool di indirizzi IP), nella gerarchia delle sedi a sinistra, selezionare una sede o un livello inferiore per prenotare un pool di indirizzi IP (ad esempio, RTP5-C9K), quindi fare clic con il pulsante destro del mouse su **Reserve IP Pool** (Prenota pool di IP).



Passaggio 2. Fornire un valore per **IP Pool Name** (Nome pool di IP) (ad esempio, EMPLOYEE-DATA-RTP5), in **Type** (Tipo) selezionare **LAN**, selezionare l'origine di **Global IP Pool** (Pool di IP globale) per la prenotazione (ad esempio, EMPLOYEE). In **CIDR Notation / No. of IP Addresses** (Notazione CIDR / N. di indirizzi), selezionare la parte dello spazio degli indirizzi da usare (ad esempio, 10.101.114.0/24), assegnare un **Gateway IP Address** (Indirizzo IP gateway) (ad esempio, 10.101.114.1), utilizzare il menu a discesa per assegnare i **Server DHCP** e i **Server DNS**, quindi fare clic su **Reserve** (Prenota).



Passaggio 3. Ripetere il passaggio precedente per tutti i blocchi di indirizzi dei pool globali che devono essere prenotati nella gerarchia di ciascuna sede.

La gerarchia mostra i pool di indirizzi assegnati. Nell'esempio vengono mostrate le prenotazioni dei pool nella sede RTP, a livello di edificio RTP5-C9K.

Procedura – Creazione della segmentazione e della policy per la rete SD-Access

Tra le decisioni di progettazione da prendere per l'implementazione della rete SD-Access, rientrano anche le strategie di segmentazione della rete dell'azienda. La macro segmentazione usa reti overlay aggiuntive (VN) nel fabric, la micro segmentazione usa i tag dei gruppi scalabili per applicare la policy ai gruppi di utenti o di profili dei dispositivi.

Utilizzare le policy di gruppo per adattare con facilità i risultati desiderati dell'applicazione delle policy mediante segmentazione. In un ambiente universitario, ad esempio, le macchine degli studenti e della facoltà possono avere accesso alle risorse di stampa, ma le macchine degli studenti non devono comunicare direttamente con le macchine della facoltà e i dispositivi di stampa non devono comunicare tra loro.

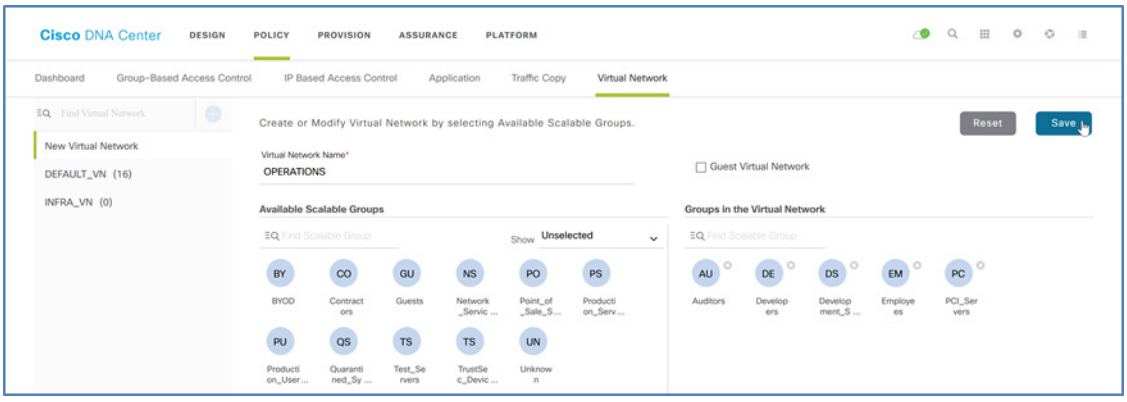
In altri casi, è necessario un maggiore isolamento. In un negozio al dettaglio, ad esempio, le macchine POS non devono mai comunicare con l'infrastruttura di rete di videosorveglianza, che a sua volta non deve mai comunicare con il sistema HVAC dell'edificio. Quando l'isolamento deve riguardare l'intera rete, dalla periferia al centro, per accedere ai servizi centralizzati, la macrosegmentazione con reti virtuali è la scelta migliore. Anche i requisiti di conformità di industrie ed enti governativi e le policy di rischio di un'azienda rendono la macrosegmentazione la scelta migliore.

Per un'analisi più approfondita delle fasi di progettazione della segmentazione per SD-Access, con scenari d'uso, vedere la guida alla progettazione della segmentazione di Software-Defined Access su cisco.com.

Utilizzare queste procedure come esempi per implementare le policy di micro e macrosegmentazione.

Procedura 1. Aggiunta di una rete virtuale overlay sulla rete SD-Access

Passaggio 1. Dalla dashboard principale di Cisco DNA Center, accedere a **POLICY > Virtual Network** (Rete virtuale), fare clic su **+** (segno più) per creare una nuova rete virtuale. Fornire un valore per **Virtual Network Name** (Nome rete virtuale) (ad esempio, OPERATIONS), trascinare i gruppi scalabili dal pool **Available Scalable Groups** (Gruppi scalabili disponibili) al pool **Groups in the Virtual Network** (Gruppi della rete virtuale) (ad esempio, Auditors, Developers, Development_Servers, Employees e PCI_Servers), quindi fare clic su **Save** (Salva).



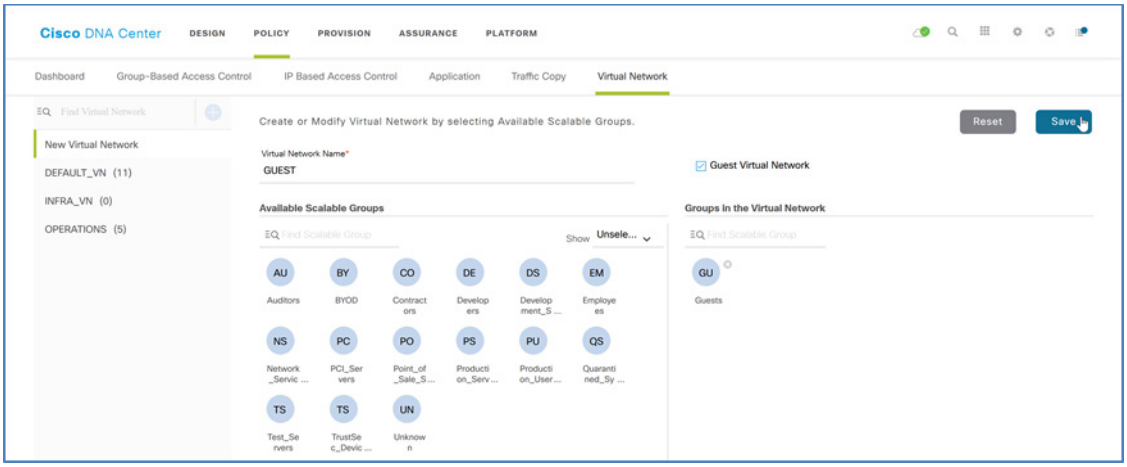
La rete virtuale con gruppi associati viene definita e visualizzata nell'elenco delle reti virtuali definite. Queste definizioni di reti virtuali sono disponibili per il provisioning dei fabric.

Suggerimento tecnico
Se non viene visualizzato alcun gruppo, probabilmente la connettività pxGrid tra Cisco DNA Center e ISE non è pienamente operativa. In questo caso, rivedere le procedure di integrazione di ISE in Cisco DNA Center e accertarsi di approvare la richiesta di connessione pxGrid in ISE da Cisco DNA Center.

Passaggio 2. In caso occorra utilizzare gruppi diversi da quelli predefiniti, creare gruppi personalizzati accedendo a **POLICY > Group-Based Access Control** (Controllo accessi basato su gruppo) **> Scalable Groups** (Gruppi scalabili), quindi fare clic su **Add Groups** (Aggiungi gruppi) per creare un nuovo gruppo e SGT.

Passaggio 3. Ripetere i primi due passaggi per ciascuna rete overlay. Inoltre, è possibile tornare a questi passaggi dopo il provisioning del fabric per creare altre reti overlay.

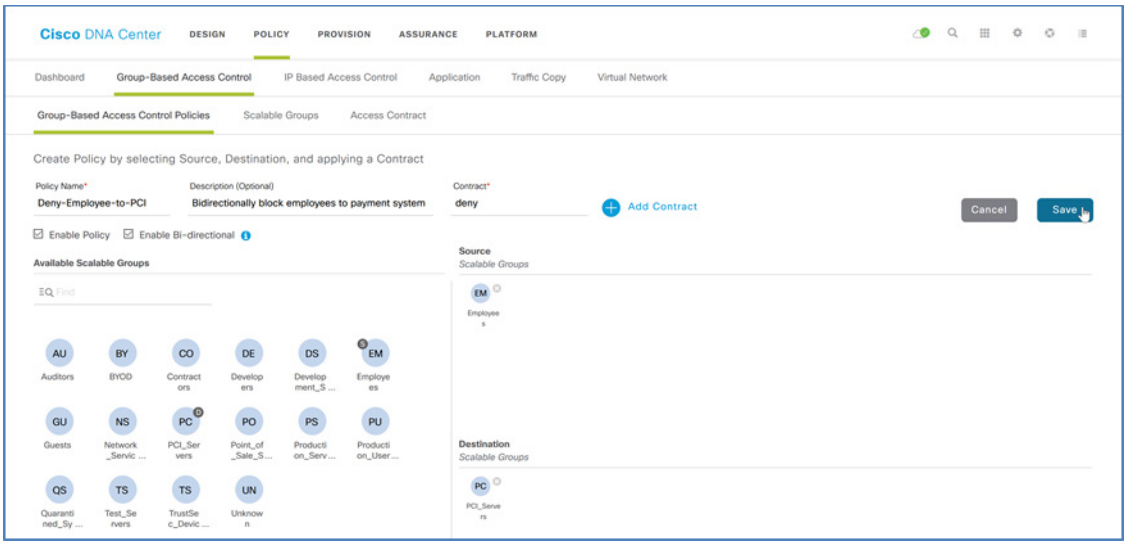
Passaggio 4. Molte reti richiedono un servizio guest per utenti wireless: creare una rete virtuale guest per supportare questa funzione. Dalla dashboard principale di Cisco DNA Center, accedere a **POLICY > Virtual Network** (Rete virtuale), fare clic su **+** (segno più) per creare una nuova rete virtuale. Fornire un valore per **Virtual Network Name** (Nome rete virtuale) (ad esempio, GUEST), selezionare la casella di controllo accanto a **Guest Virtual Network** (Rete virtuale guest), trascinare i gruppi scalabili **Guest** dal pool **Available Scalable Groups** (Gruppi scalabili disponibili) al pool **Groups in the Virtual Network** (Gruppi nella rete virtuale), quindi fare clic su **Save** (Salva).



Procedura 2. Creazione di una policy di microsegmentazione con SGT

Le policy di microsegmentazione sono personalizzate in base all'implementazione dell'azienda. Questo semplice esempio mostra una policy di base che può essere utilizzata per impedire agli utenti del gruppo Employee (Dipendenti) di comunicare con il gruppo PCI_Servers (Server PCI). Quando i profili di autenticazione assegnano correttamente un SGT a un endpoint o a un utente, ISE acquisisce l'intento di questa policy e la applica alla rete.

Passaggio 1. Dalla dashboard principale di Cisco DNA Center, accedere a **POLICY > Group-Based Access Control** (Controllo accessi basato su gruppo) **> Group-Based Access Control Policies** (Policy di controllo accessi basato su gruppo), fare clic su **+ Add Policy** (+ Aggiungi policy). Dal riquadro **Available Scalable Groups** (Gruppi scalabili disponibili), trascinare il gruppo **Employees** (Dipendenti) nel riquadro **Source** (Origine), trascinare il gruppo **PCI_Servers** (Server PCI) nel riquadro **Destination** (Destinazione), immettere un valore per **Policy Name** (Nome policy) (ad esempio, impedisci-ai-dipendenti-di-accedere-a-PCI), immettere una **descrizione**. Selezionare **Enable Policy** (Abilita policy), selezionare **Enable Bi-directional** (Abilita bidirezionale), fare clic su **+ Add Contract** (+ Aggiungi contratto), selezionare **deny** (rifiuta), fare clic su **OK**, quindi fare clic su **Save** (Salva).



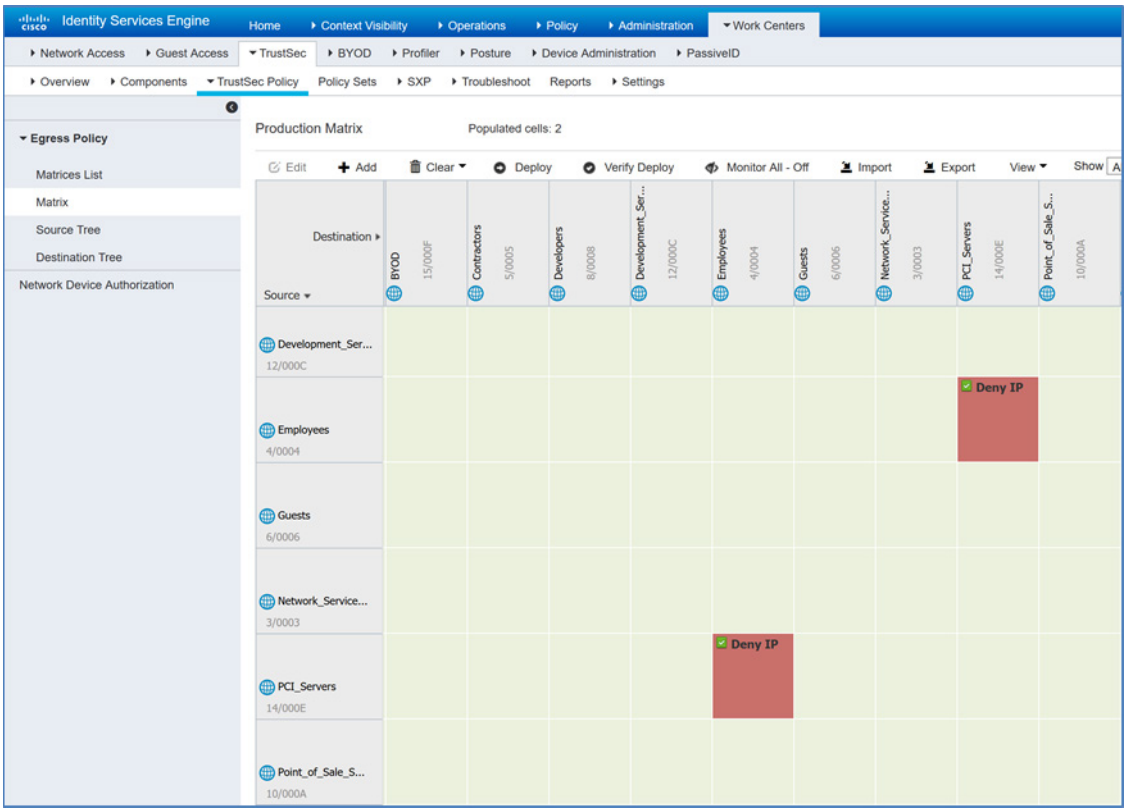
La policy viene creata ed elencata con lo stato **CREATED** (Creata). Avendo scelto l'opzione bidirezionale, viene creata anche la policy inversa.

Passaggio 2. Selezionare le policy create, quindi fare clic su **Deploy** (Implementa).

Lo stato cambia in **DEPLOYED** (Implementata) e le policy possono essere applicate ai fabric di SD-Access creati da Cisco DNA Center; inoltre, sono disponibili in ISE e visualizzabili con la matrice Cisco TrustSec.

Passaggio 3. In alto a destra, fare clic su **Advanced Options** (Opzioni avanzate). Il collegamento consente di accedere a ISE, andando a **Work Centers** (Centri di lavoro) **> TrustSec > TrustSec Policy** (Policy TrustSec), quindi selezionando sulla sinistra **Matrix** (Matrice). Si viene reindirizzati alla pagina di accesso a ISE, che a sua volta reindirizza il browser e visualizza la matrice di policy TrustSec.

Verificare che la policy sia stata aggiornata su ISE affinché venga applicata alla rete.



Procedura – Preparativi per l'automazione della gestione della rete

Prepararsi a implementare le progettazioni e le policy della rete creando un underlay operativo che includa la connettività di gestione dei dispositivi. Nell'ambito dell'integrazione di ISE in Cisco DNA Center descritta nella guida prescrittiva all'implementazione di Software-Defined Access for Distributed Campus, ISE viene configurato con il supporto TACACS per l'amministrazione dei dispositivi dell'infrastruttura. Nelle configurazioni TACACS, Cisco DNA Center modifica i dispositivi rilevati in modo che usino per impostazione predefinita i servizi di autenticazione e registrazione di ISE e i server failover locali. ISE deve essere preparato in modo da supportare le configurazioni di amministrazione applicate ai dispositivi durante il processo di rilevamento.

Procedura 1. Configurazione della gestione dei dispositivi della rete underlay dalla CLI di Cisco IOS-XE

Per la massima resilienza e larghezza di banda, usare un'interfaccia di loopback su ciascun dispositivo e abilitare la connettività di layer 3 per il rilevamento e la gestione in-band di Cisco DNA Center. I passaggi seguenti configurano la connettività Ethernet point-to-point tra i dispositivi utilizzando IS-IS come protocollo di routing e SSHv2 per la configurazione dei dispositivi con le relative interfacce di loopback. La configurazione SNMP viene applicata in una procedura successiva come parte del processo di rilevamento dei dispositivi.

Non aggiungere una configurazione ai dispositivi che si desidera rilevare e configurare in un secondo momento utilizzando l'automazione LAN. I dispositivi già configurati non potranno essere riconfigurati con l'automazione LAN. In questo esempio viene mostrata una configurazione che utilizza Cisco IOS XE su un Cisco Catalyst Switch.

Passaggio 1. Utilizzare la CLI del dispositivo per configurare il nome host in modo da poter identificare facilmente il dispositivo e disabilitare i servizi non utilizzati.

```
hostname [hostname]
no service config
```

Passaggio 2. Configurare i dati di accesso e la password locali.

```
username dna privilege 15 algorithm-type scrypt secret [password]
! older software versions may not support scrypt (type 9)
! username dna privilege 15 secret [password]
enable secret [enable password]
service password-encryption
```

Passaggio 3. Configurare Secure Shell (SSH) come metodo per l'accesso di gestione alla CLI.

```
ip domain-name ciscodna.net
! generate key with choice of modulus, required by some switches
crypto key generate rsa modulus 1024
ip ssh version 2
line vty 0 15
  login local
  transport input ssh
  transport preferred none
```

Passaggio 4. Configurare lo switch in modo che supporti i pacchetti jumbo frame di Ethernet. L'MTU scelta permette di usare ulteriori intestazioni del fabric e la compatibilità con il valore comune più alto condiviso dalla maggior parte degli switch; il numero tondo dovrebbe essere facile da ricordare durante la configurazione e la risoluzione dei problemi.

```
system mtu 9100
```

Suggerimento tecnico

La connettività dell'underlay che utilizza Cisco IOS XE sui router richiede l'uso di un comando **mtu** a livello di configurazione dell'interfaccia; i Cisco Catalyst e i Cisco Nexus® Switch che non utilizzano Cisco IOS XE usano un comando **system jumbo mtu** al livello di configurazione globale.

Passaggio 5. Configurare l'indirizzo di loopback dello switch e assegnarvi la gestione SSH.

interface Loopback***0***

ip address ***[indirizzo IP di loopback del dispositivo]*** 255.255.255.255

ip ssh source-interface Loopback***0***

Procedura 2. Configurazione dei collegamenti della rete per la connettività di accesso con routing

Se la rete underlay è già stata configurata con un modello di implementazione che prevede l'accesso con routing, ignorare questa procedura. In genere, sono le distribuzioni di layer 2 a richiedere questa procedura.

Non aggiungere una configurazione ai dispositivi che si desidera rilevare e configurare utilizzando la funzionalità di automazione LAN. I dispositivi con configurazioni esistenti non possono essere configurati usando l'onboarding dell'automazione LAN senza averne prima ripristinato le impostazioni di configurazione iniziali predefinite.

Passaggio 1. Configurare le connessioni dello switch all'interno dell'infrastruttura della rete underlay. Ripetere questo passaggio per ciascun collegamento a uno switch vicino all'interno del fabric underlay. Se il dispositivo underlay verrà trattato come nodo di confine del fabric durante il provisioning e la connessione deve essere utilizzata per il passaggio (handoff) dal fabric all'infrastruttura esterna, adottare la procedura successiva.

```
interface TenGigabitEthernet1/0/1
 no switchport
 ip address [Point-to-point IP address] [netmask]
```

Passaggio 2. Abilitare il routing IP e il protocollo di routing IS-IS sullo switch.

```
! ip routing is not enabled by default on some switches
ip routing
ip multicast-routing
ip pim register-source Loopback0
ip pim ssm default
router isis
 net 49.0000.0100.0400.0001.00
 domain-password [domain password]
 metric-style wide
 nsf ietf
 log-adjacency-changes
 bfd all-interfaces
```

Suggerimento tecnico

Una pratica comune del protocollo IS-IS è incorporare l'indirizzo IP di loopback nell'ID di sistema o NET univoco. Ad esempio, un indirizzo IP di loopback ***10.4.32.1*** (***010.004.032.001***) diventa ***0100.0403.2001*** con suffisso ***.00*** e prefisso corrispondente all'ID di un'area, ad esempio ***49.0000***, risultando infine come NET ***49.0000.0100.0403.2001.00***.

Passaggio 3. Abilitare il routing IS-IS su tutte le interfacce dell'infrastruttura configurate nell'underlay, ad eccezione delle interfacce handoff di confine, che verranno configurate nella procedura successiva. L'interfaccia di loopback è abilitata in modo che condivida l'indirizzo IP di gestione, le interfacce fisiche sono abilitate in modo da condividere le informazioni di routing con l'infrastruttura connessa.

```
interface Loopback0
! ip address assigned in earlier step
 ip router isis
 ip pim sparse-mode
interface range TenGigabitEthernet1/0/1-2,  TenGigabitEthernet2/0/1-2
! routed ports with ip addresses assigned via earlier steps
 ip router isis
 isis network point-to-point
 ip pim sparse-mode
 logging event link-status
 load-interval 30
 bfd interval 100 min_rx 100 multiplier 3
 no bfd echo
 dampening
```

Procedura 3. Abilitazione della connettività di routing al confine verso il router vicino esterno

Se la rete underlay è già configurata con modalità di accesso con routing e integrata nel resto della rete con il protocollo BGP e l'handoff 802.1Q, ignorare questa procedura. Questa procedura è richiesta nella maggior parte delle implementazioni.

Per connettere i dispositivi dei nodi di confine alla rete, stabilire la connettività tra le interfacce configurate con VRF-Lite: in questo modo le istanze VRF risulteranno separate dai tag VLAN 802.1Q. Connettere i servizi di rete comuni disponibili all'esterno dei nodi di confine, quali DNS, DHCP, WLC e la gestione di Cisco DNA Center quando non direttamente connessa ai nodi di rete SD-Access, estendendo la rete aziendale esistente all'underlay del confine. La connettività a Cisco DNA Center è necessaria per ulteriore provisioning.

Il routing di gestione dei dispositivi esterni tra più reti virtuali e un'istanza di routing globale agisce come router ibrido per queste reti. La separazione della connettività viene gestita usando istanze VRF connesse tramite le interfacce con tag 802.1Q al confine, note anche come VRF-Lite. Quando si stabilisce la connettività dell'underlay con il protocollo BGP, Cisco DNA Center può gestire le attività iniziali di rilevamento e configurazione utilizzando il collegamento e usare quindi lo stesso collegamento ampliato con tag e sessioni BGP aggiuntivi secondo le necessità di connettività della rete virtuale overlay.

Passaggio 1. Su ciascun nodo di confine, se si configura uno switch che supporta interfacce trunk VLAN come Cisco Catalyst serie 9000, 3800 o 6800 Switch, è necessario configurare un trunk sull'interfaccia connessa a una VLAN dedicata per stabilire la connettività dell'underlay per il peering al router ibrido.

```
vlan 100
interface vlan100
 ip address [IP address] [netmask]
 ip pim sparse-mode
 no shutdown
interface FortyGigabitEthernet1/0/24
```

```
 switchport
 switchport mode trunk
 switchport trunk allowed vlan add 100
 no shutdown
```

Passaggio 2. Su ciascun nodo di confine, se si configura un dispositivo come un router ASR o ISR che supporta i tag VLAN 802.1Q, usare una configurazione di sottointerfaccia alternativa anziché un'interfaccia trunk dello switch per stabilire la connettività dell'underlay al router ibrido.

```
interface TenGigabitEthernet0/1/0
 no shutdown
!
interface TenGigabitEthernet0/1/0.100
 encapsulation dot1Q 100
 ip address [IP address] [netmask]
 ip pim sparse-mode
 no shutdown
```

Passaggio 3. Connettere i nodi di confine ridondanti ad almeno un'interfaccia di routing per la comunicazione dell'underlay e il successivo peering del BGP. Viene visualizzata la configurazione per l'integrazione nel protocollo IS-IS. Ripetere questo passaggio per ciascuna interfaccia usata per connettersi ai nodi di confine.

```
interface FortyGigabitEthernet1/0/23
 no switchport
 ip address [Point-to-point IP address] [netmask]
 ip router isis
 isis network point-to-point
 ip pim sparse-mode
 logging event link-status
 load-interval 30
no shutdown
```

Passaggio 4. Abilitare il routing BGP al router ibrido per la connettività alle reti esterne al fabric e attivare il protocollo BGP sulle interfacce di connessione. Configurare il protocollo BGP in modo da permettere a Cisco DNA Center di accedere ai dispositivi di rete dell'underlay per la gestione, consentendo al contempo l'ulteriore provisioning delle reti virtuali sulle interfacce e riducendo al minimo le interruzioni della connettività di rete. Ripetere questo passaggio per ciascun nodo di confine.

```
router bgp [underlay AS number]
 bgp router-id [loopback 0 IP address]
 bgp log-neighbor-changes
! fusion router is an eBGP neighbor
 neighbor [fusion interface IP address] remote-as [external AS number]
! redundant border is an iBGP neighbor
 neighbor [redundant border Lo0 address] remote-as [underlay AS number]
 neighbor [redundant border Lo0 address] update-source Loopback0
 !
 address-family ipv4
  network [Lo0 IP address] mask 255.255.255.255
```

```
! advertise underlay IP network summary in global routing table
 aggregate-address [underlay IP network summary] [netmask] summary-only
 redistribute isis level-2
 neighbor [fusion interface IP address] activate
 neighbor [redundant border Lo0 address] activate
 maximum-paths 2
exit-address-family
```

Procedura 4. Ridistribuzione delle subnet dei servizi condivisi nell'IGP dell'underlay

Le API non possono utilizzare una route predefinita dell'underlay per contattare il WLC. Nella tabella di routing globale deve essere presente una route più specifica, ad esempio una route di subnet /24 o host /32, per l'indirizzo IP del WLC su ciascun nodo a cui si connettono le API per stabilire la connettività. Inserire le route più specifiche per i servizi condivisi WLC e DHCP richiesti dal protocollo BGP (ad esempio, 10.4.174.0/24 e 10.4.48.0/21) nella rete underlay. A tal fine, adottare questa procedura per ridistribuire la route dei servizi condivisi sul confine nel processo di routing IGP della rete underlay. In questa procedura, i prefissi utilizzati corrispondono ai prefissi inclusi nella tabella di routing del BGP.

Passaggio 1. Connettersi a ciascun nodo di confine e aggiungere un elenco di prefissi (prefix-list) e una mappa della route (route-map) per tutte le subnet utilizzate dai servizi condivisi.

```
ip prefix-list SHARED_SERVICES_NETS seq 5 permit 10.4.48.0/21
ip prefix-list SHARED_SERVICES_NETS seq 10 permit 10.4.174.0/24
route-map GLOBAL_SHARED_SERVICES_NETS permit 10
 match ip address prefix-list SHARED_SERVICES_NETS
```

Passaggio 2. In ogni nodo di confine, ridistribuire i prefissi nel protocollo di routing dell'underlay. In questo esempio si presume l'uso del protocollo IS-IS.

```
router isis
 redistribute bgp [underlay AS number] route-map GLOBAL_SHARED_SERVICES_NETS metric-type external
```

Procedura 5. Abilitazione della connettività al router ibrido esterno verso il vicino di confine

I router ibridi connessi ai router di confine del fabric richiedono che la configurazione della CLI per la connettività dell'underlay sia coerente con le procedure precedenti. Attenersi a questa procedura per ciascun router ibrido esterno connesso a un confine.

Il router ibrido di esempio è configurato con una connessione peering tra un'istanza VRF contenente le route globali a livello enterprise e la tabella di routing globale sul confine per la raggiungibilità dell'underlay del fabric, senza usare la tabella di routing globale del router ibrido.

In alternativa, effettuare il peering tra la tabella di routing globale a livello enterprise del router ibrido e la tabella di routing globale sul confine, senza utilizzare un'istanza VRF.

Passaggio 1. Su ciascun router ibrido esterno, creare l'istanza VRF, l'identificatore di route e i route target per la connettività di gestione iniziale al confine.

```
vrf definition VRF-GLOBAL_ROUTES
 rd 100:100
 !
 address-family ipv4
```

```
  route-target export 100:100
  route-target import 100:100
exit-address-family
```

Passaggio 2. Per ciascuna connessione del router ibrido esterno al confine del fabric di SD-Access, abilitare l'interfaccia, la sottointerfaccia con tag VLAN e gli indirizzi IP. In questo esempio vengono utilizzati i tag VLAN 802.1Q su un router con sottointerfacce. Per gli switch che richiedono configurazioni trunk delle porte, associare l'altro lato già configurato.

```
interface TenGigabitEthernet0/1/7
 description to Border
 mtu 9100
 no ip address
 no shutdown
interface TenGigabitEthernet0/1/7.100
 encapsulation dot1Q 100
 vrf forwarding VRF-GLOBAL_ROUTES
 ip address [IP network] [netmask]
```

La connettività IP alla VLAN è ora stabilita (ad esempio, 100) sulla connessione con tag 802.1Q tra il router ibrido e il nodo di confine.

Passaggio 3. Creare mappe di indirizzamento per contrassegnare le route ed evitare loop di routing quando si effettua la ridistribuzione tra il protocollo IGP utilizzato nel resto della rete e il protocollo BGP utilizzato per la connessione con collegamenti multipli. I protocolli IGP possono variare: nell'esempio mostrato viene usato il protocollo EIGRP che completa la connettività di routing tra IS-IS, BGP e EIGRP.

```
route-map RM-BGP-TO-EIGRP permit 10
 set tag 100
!
route-map RM-EIGRP-TO-BGP deny 10
 match tag 100
route-map RM-EIGRP-TO-BGP permit 20
```

Passaggio 4. Abilitare il peering BGP dai router ibridi ridondanti ai nodi di confine e ridistribuire l'IGP utilizzato per raggiungere le reti esterne ai router ibridi.

```
router bgp [external AS number]
 bgp router-id [loopback IP address]
 bgp log-neighbor-changes
 !
address-family ipv4 vrf VRF-GLOBAL_ROUTES
  redistribute eigrp 100 route-map RM-EIGRP-TO-BGP
  neighbor [redundant fusion IP] remote-as [external AS number]
  neighbor [redundant fusion IP] activate
  neighbor [border IP address] remote-as [underlay AS number]
  neighbor [border IP address] activate
  maximum-paths 2
  default-information originate
 exit-address-family
```

Passaggio 5. Ridistribuire il BGP nell'IGP per consentire la raggiungibilità. Gli IGP possono variare: nell'esempio mostrato viene usato il protocollo chiamato EIGRP.

```
router eigrp LAN
 !
 address-family ipv4 unicast vrf VRF-GLOBAL_ROUTES autonomous-system 100
  topology base
   redistribute bgp [external AS number] metric 1000000 1 255 1 9100 route-map RM-BGP-TO-EIGRP
  exit-af-topology
  network [external IP network address] [netmask]
  eigrp router-id [loopback IP address]
 exit-address-family
```

Procedura 6. Configurazione dell'MTU sui dispositivi intermedi non gestiti

Facoltativo

Cisco DNA Center offre molti vantaggi per la gestione di tutti i dispositivi nel dominio di un fabric. Cisco DNA Center gestisce già i nodi edge e di confine del fabric. Tuttavia, se sono presenti dispositivi intermedi nel fabric non gestiti da Cisco DNA Center (ad esempio, supporto hardware o software non disponibile in Cisco DNA Center), è comunque necessario garantire il passaggio del traffico SD-Access attraverso tali nodi intermedi. I requisiti principali che devono soddisfare i dispositivi a tale scopo sono:

- Dispositivi di layer 3 che partecipino attivamente nella topologia di routing negli altri dispositivi dell'underlay del fabric.
- Capacità di trasporto dei jumbo frame offerti dalle tecniche di incapsulamento del fabric.

Per i dispositivi dei nodi intermedi del fabric non gestiti, è necessario impostare una MTU appropriata (ad esempio, 9100) e configurare manualmente il routing con gli altri dispositivi dell'underlay. Le linee guida per la configurazione in questo caso dipendono dal dispositivo e non vengono discusse ulteriormente nella presente guida.

Non aggiungere una configurazione ai dispositivi che si desidera rilevare e configurare in un secondo momento utilizzando l'automazione LAN. I dispositivi già configurati non potranno essere riconfigurati con l'automazione LAN.

Procedura 7. Rilevamento e gestione dei dispositivi di rete

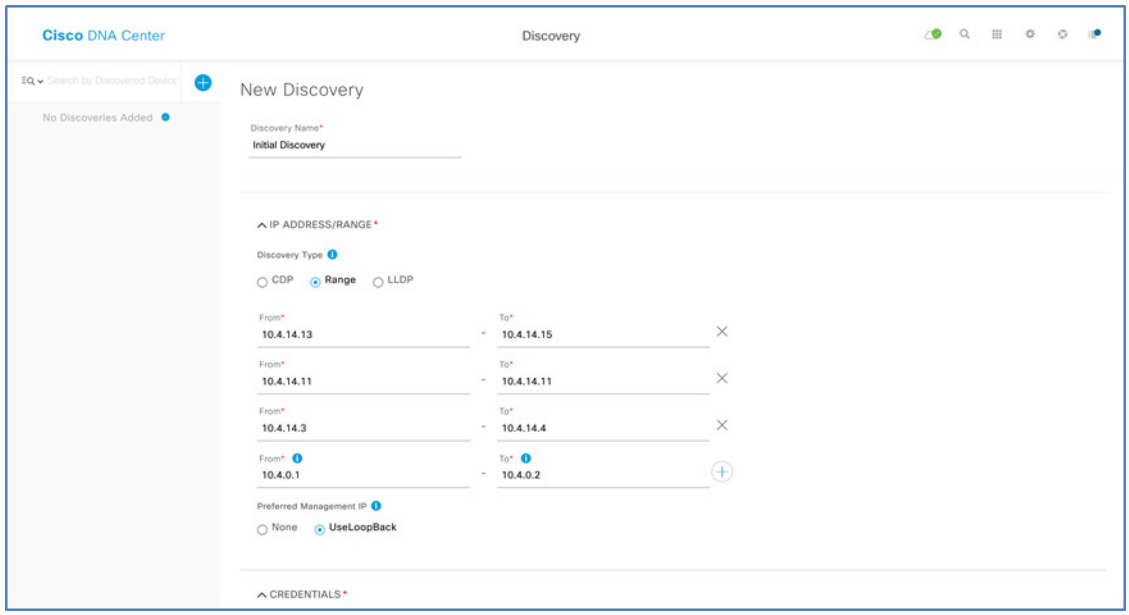
Affinché Cisco DNA Center possa essere usato per rilevare e gestire i dispositivi della rete underlay per SD-Access, è necessario abilitare la connettività IP ai dispositivi e fornire le credenziali di gestione per Cisco DNA Center. Adottare questa procedura per i dispositivi seed con automazione LAN e la procedura successiva per tutti gli altri dispositivi che non si desidera rilevare e gestire con l'automazione LAN.

Questi passaggi mostrano come avviare il rilevamento fornendo un intervallo di indirizzi IP o più intervalli per la scansione dei dispositivi di rete; in questo modo si restringe il campo della ricerca e teoricamente si possono ridurre i tempi. In alternativa, per i dispositivi che non utilizzano l'onboarding con automazione LAN, è possibile far rilevare a Cisco DNA Center un dispositivo iniziale e fare in modo che utilizzi Cisco Discovery Protocol per trovare i dispositivi vicini connessi. Quando si utilizza Cisco Discovery Protocol, ridurre il numero predefinito di hop a un valore ragionevole per velocizzare il processo di rilevamento.

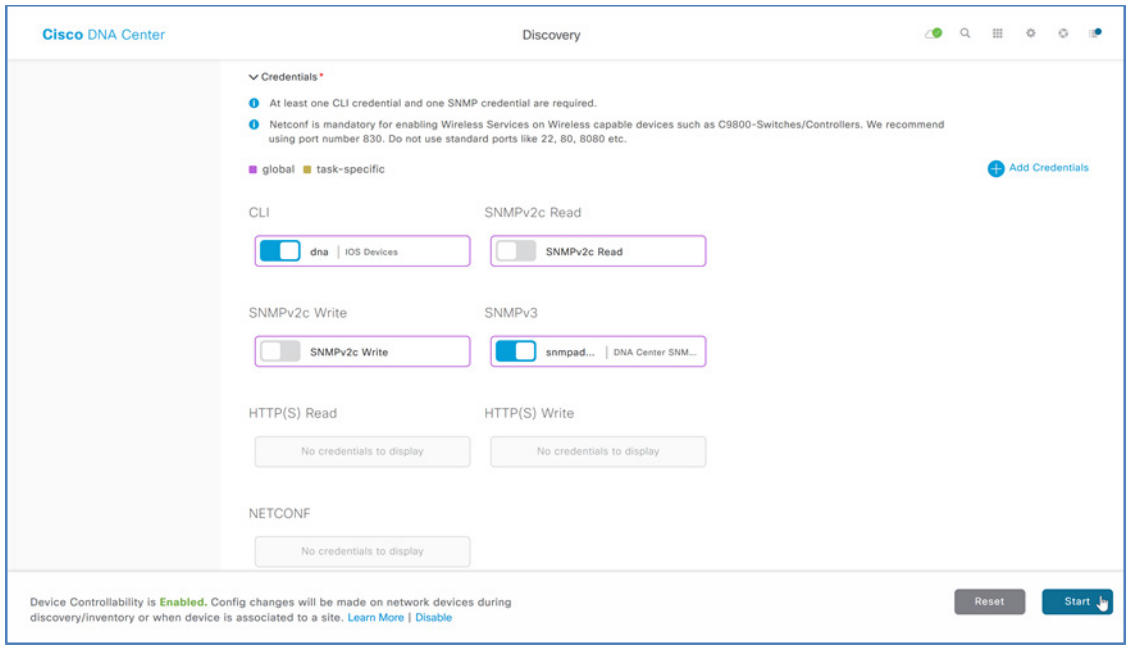
Passaggio 1. Accedere alla dashboard principale di Cisco DNA Center, scorrere fino alla sezione **Tools** (Strumenti), fare clic su **Discovery** (Rilevamento) e fornire un valore per **Discovery Name** (Nome rilevamento). Selezionare **Range** (Intervallo) e immettere un indirizzo IP di loopback di inizio e uno di fine in **IP Ranges** (Intervalli IP) (per coprire un singolo indirizzo, immettere lo stesso indirizzo all'inizio e alla fine dell'intervallo). In **Preferred Management IP** (IP di gestione preferito), se un dispositivo ha un'interfaccia di loopback dedicata alla gestione, selezionare **UseLoopBack** (Usa loopback).

Suggerimento tecnico
Se si utilizza un Cisco Catalyst serie 6800 Switch con una configurazione grande, è possibile evitare i timeout di rilevamento aggiungendo il seguente comando in modalità configurazione: `snmp mib flash cache`

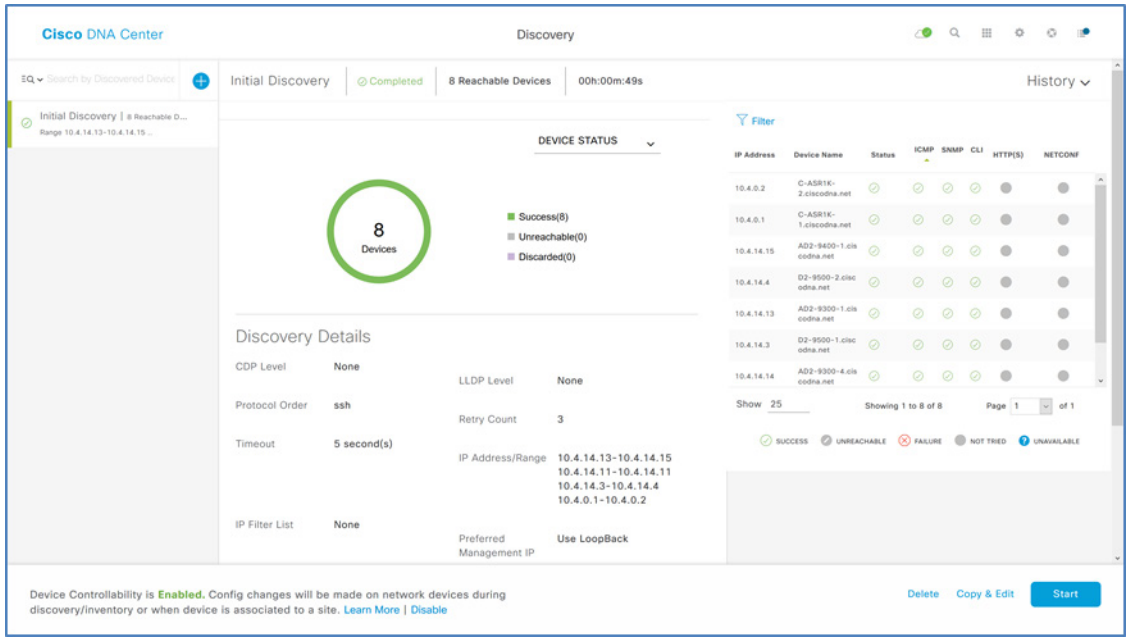
Passaggio 2. Se sono disponibili altri intervalli, accanto al primo intervallo fare clic su **+** (segno più), immettere l'intervallo aggiuntivo e ripetere l'operazione per gli intervalli rimanenti.



Passaggio 3. Scorrere verso il basso per verificare le credenziali CLI utilizzate per il rilevamento e le configurazioni delle credenziali SNMP applicate al dispositivo dalla funzione Device Controllability (Controllabilità dispositivi) di Cisco DNA Center, quindi fare clic in basso su **Start** (Avvia).



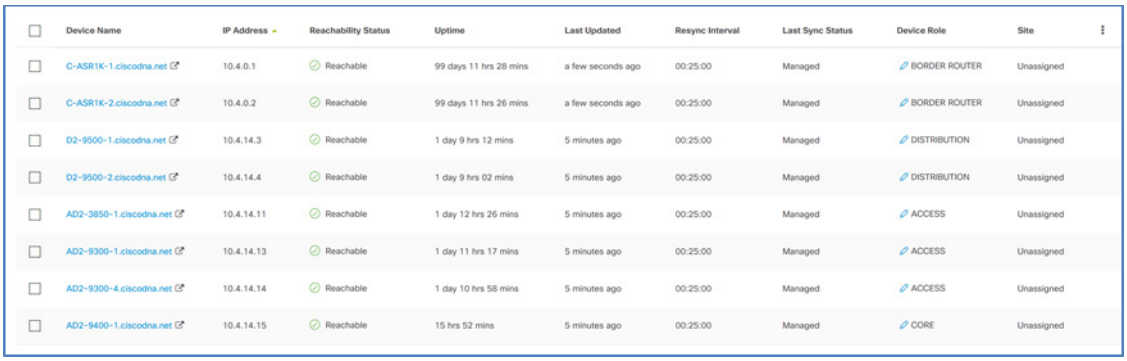
I dettagli di rilevamento vengono visualizzati durante l'esecuzione del processo.



Al termine del processo di rilevamento di un dispositivo con Device Controllability (Controllabilità dispositivi), le credenziali assegnate dalla CLI e memorizzate localmente sul dispositivo vengono utilizzate come backup. Le credenziali locali vengono utilizzate solo se si perde la connettività all'ISE, utilizzata per accedere alle credenziali centralizzate principali.

Passaggio 4. Se sono presenti errori di rilevamento, controllare l'elenco dei dispositivi, risolvere il problema e riavviare il processo di rilevamento per i dispositivi in errore e per eventuali altri dispositivi che si desidera aggiungere all'inventario.

Passaggio 5. Dopo aver completato correttamente tutte le attività di rilevamento, andare alla dashboard principale di Cisco DNA Center, quindi, nella sezione **Tools** (Strumenti), fare clic su **Inventory** (Inventario). Vengono visualizzati i dispositivi rilevati. Dopo aver completato la raccolta dell'inventario, su ciascun dispositivo viene visualizzato lo stato di sincronizzazione **Managed** (Gestito) per segnalare che Cisco DNA Center conserva un modello interno che rispecchia l'implementazione fisica del dispositivo.



Device Name	IP Address	Reachability Status	Uptime	Last Updated	Resync Interval	Last Sync Status	Device Role	Site
C-ASR1K-1.ciscodna.net	10.4.0.1	Reachable	99 days 11 hrs 28 mins	a few seconds ago	00:25:00	Managed	BORDER ROUTER	Unassigned
C-ASR1K-2.ciscodna.net	10.4.0.2	Reachable	99 days 11 hrs 26 mins	a few seconds ago	00:25:00	Managed	BORDER ROUTER	Unassigned
D2-9500-1.ciscodna.net	10.4.14.3	Reachable	1 day 9 hrs 12 mins	5 minutes ago	00:25:00	Managed	DISTRIBUTION	Unassigned
D2-9500-2.ciscodna.net	10.4.14.4	Reachable	1 day 9 hrs 02 mins	5 minutes ago	00:25:00	Managed	DISTRIBUTION	Unassigned
AD2-3850-1.ciscodna.net	10.4.14.11	Reachable	1 day 12 hrs 26 mins	5 minutes ago	00:25:00	Managed	ACCESS	Unassigned
AD2-9300-1.ciscodna.net	10.4.14.13	Reachable	1 day 11 hrs 17 mins	5 minutes ago	00:25:00	Managed	ACCESS	Unassigned
AD2-9300-4.ciscodna.net	10.4.14.14	Reachable	1 day 10 hrs 58 mins	5 minutes ago	00:25:00	Managed	ACCESS	Unassigned
AD2-9400-1.ciscodna.net	10.4.14.15	Reachable	15 hrs 52 mins	5 minutes ago	00:25:00	Managed	CORE	Unassigned

Cisco DNA Center può ora accedere ai dispositivi, sincronizzare l'inventario della configurazione e apportare modifiche alla configurazione dei dispositivi.

Suggerimento tecnico

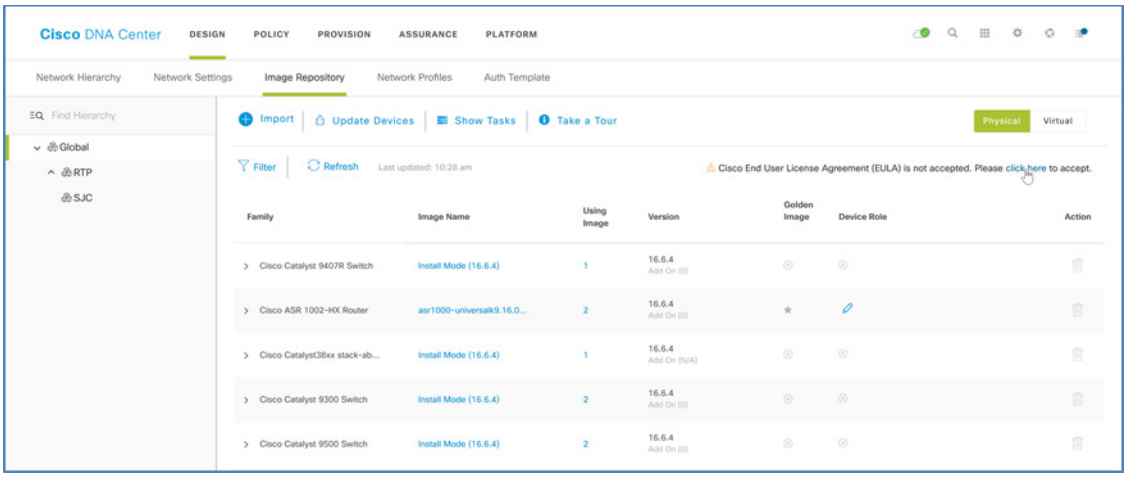
Sulla riga del titolo della tabella dell'inventario, sul lato destro, è possibile scegliere quali colonne visualizzare. Utilizzare la colonna **Device Role** (Ruolo dispositivo) per visualizzare il ruolo assegnato dal processo di rilevamento in base al tipo di dispositivo e per modificarlo in modo che rappresenti il più fedelmente l'implementazione effettiva, scegliendo tra router di accesso, di distribuzione, core o di confine. In questa visualizzazione, il router di confine è un ruolo generico che non appartiene al fabric. La modifica del ruolo in questa fase, senza attendere le procedure successive, può migliorare l'aspetto delle mappe della topologia iniziale.

Procedura 8. Gestione delle immagini software dei dispositivi nell'inventario

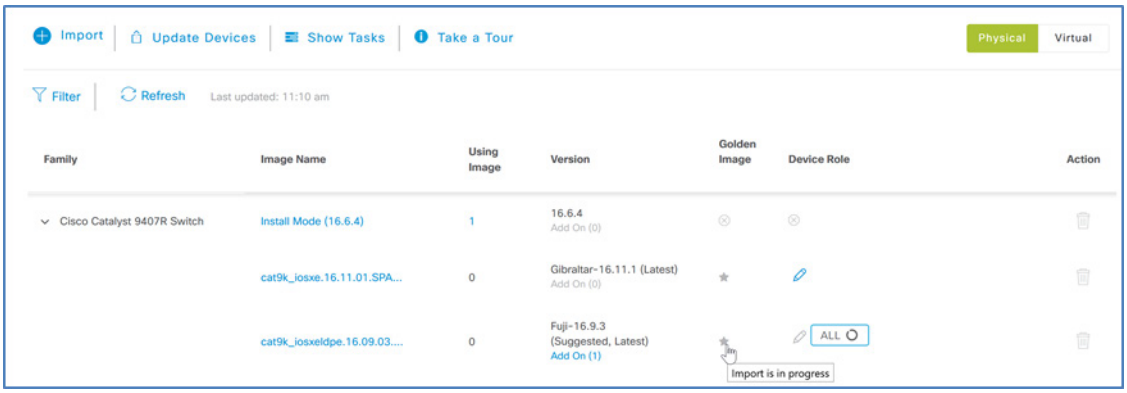
Per usufruire di tutte le funzionalità del pacchetto SD-Access in Cisco DNA Center, è necessario rispettare i requisiti minimi per la versione software dei dispositivi su cui verrà effettuato il provisioning. La funzionalità di gestione delle immagini software integrata in Cisco DNA Center viene utilizzata per aggiornare i dispositivi la cui immagine non ha la versione consigliata. Le immagini consigliate per SD-Access con matrice di compatibilità hardware e software di SD-Access si trovano sul sito cisco.com. Le immagini utilizzate per la convalida sono elencate nell'Appendice A – Elenco dei prodotti.

Effettuare i passaggi seguenti per applicare ai dispositivi gli aggiornamenti delle immagini e gli aggiornamenti di manutenzione del software (SMU), importando le immagini richieste, contrassegnandole come preferite e applicandole ai dispositivi.

Passaggio 1. Accedere alla dashboard principale di Cisco DNA Center, fare clic su **Design** (Progettazione) e su **Image Repository** (Archivio immagini). Se questa è la prima volta che si utilizza il software, in alto a destra sulla notifica **Cisco End User License Agreement** (Contratto di licenza con l'utente finale Cisco), selezionare **click here** (fare clic qui), quindi fare clic su **Accept License Agreement** (Accetta contratto di licenza).



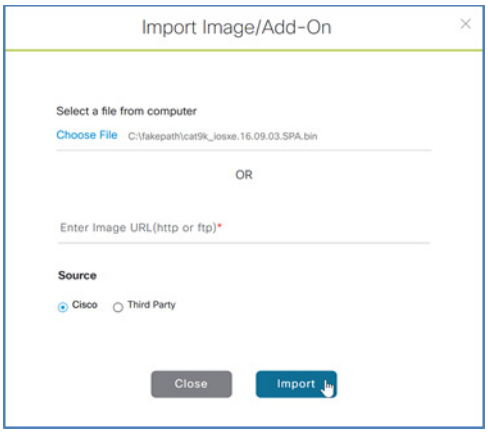
Passaggio 2. Se si desidera che Cisco DNA Center scarichi una nuova immagine da applicare a un dispositivo, nella colonna **Image Name** (Nome immagine), fare clic sulla freccia Giù accanto all'immagine elencata per una famiglia di dispositivi, quindi fare clic sulla stella **Golden Image** (Immagine preferita) per contrassegnare l'immagine come preferita per la piattaforma.



Le immagini non ancora importate vengono importate automaticamente, utilizzando le credenziali di cisco.com. È possibile aggiornare le credenziali cisco.com utilizzando **Settings** (Impostazioni) (icona ingranaggio) **> System Settings** (Impostazioni di sistema) **> Settings** (Impostazioni) **> Cisco Credentials** (Credenziali Cisco).

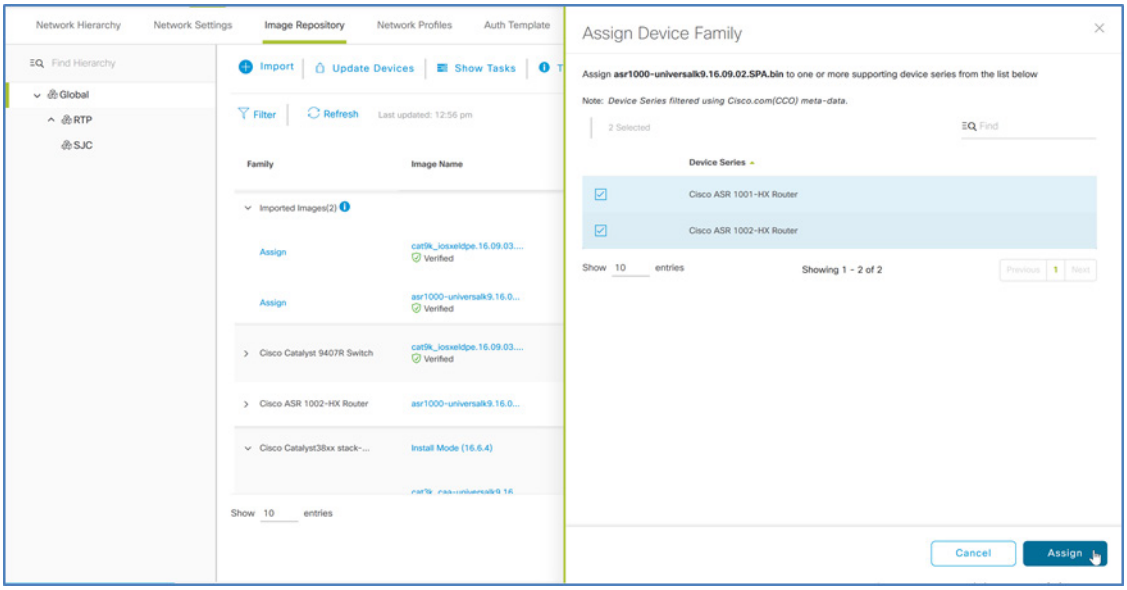
Passaggio 3. Ripetere l'importazione e contrassegnare le immagini come preferite finché tutti i dispositivi non sono contrassegnati con un'immagine adatta.

Passaggio 4. Se si sceglie di importare un'immagine dalla macchina locale, fare clic su **+ Import** (+ Importa), nella finestra di dialogo Import Image/Add-On (Importa immagine/Aggiungi), selezionare la posizione di un file, quindi fare clic su **Import** (Importa).



Viene avviata l'importazione dell'immagine in Cisco DNA Center.

Passaggio 5. Dopo aver completato l'importazione, assegnare l'immagine importata ai dispositivi. Accanto all'immagine importata, fare clic su **Assign** (Assegna), selezionare i dispositivi che utilizzeranno l'immagine, quindi nella finestra popup fare clic su **Assign** (Assegna).



L'immagine è ora nell'archivio e può essere contrassegnata come preferita per questi dispositivi.

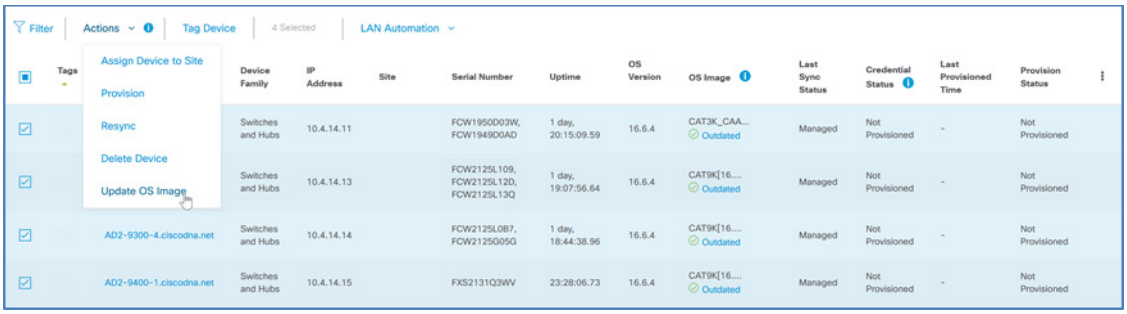
Passaggio 6. Per ciascun dispositivo con nuova assegnazione di un'immagine, fare clic sulla stella **Golden Image** (Immagine preferita) per contrassegnare l'immagine desiderata come immagine preferita della piattaforma.

Passaggio 7. Ripetere questi passaggi per tutte le immagini che si desidera implementare con Cisco DNA Center. Tutti i tipi di dispositivi con un'immagine preferita assegnata sono pronti per la distribuzione dell'immagine software.

Procedura 9. Uso della gestione delle immagini software per aggiornare il software del dispositivo

Cisco DNA Center esegue un controllo di conformità dei dispositivi presenti nell'inventario confrontando le immagini contrassegnate come preferite. I dispositivi non conformi all'immagine preferita vengono contrassegnati come **Outdated** (Obsoleti) nell'inventario. Aggiornare le immagini alla versione contrassegnata come preferita. Prima di continuare, la raccolta dell'inventario deve essere stata completata correttamente e i dispositivi devono essere nello stato **Managed** (Gestito). Distribuire prima le immagini software, quindi pianificare o attivare manualmente i dispositivi con le immagini distribuite.

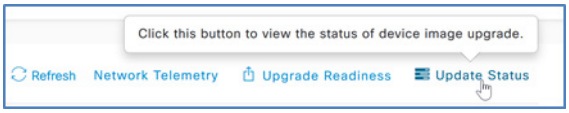
Passaggio 1. Accedere a **PROVISION** (Provisioning) **> Devices** (Dispositivi) **> Inventory** (Inventario), selezionare tutti i dispositivi contrassegnati come **Outdated** (Obsoleti), quindi dal menu **Actions** (Azioni), fare clic su **Update OS Image** (Aggiorna immagine del sistema operativo). Per un maggior controllo, avviare gli aggiornamenti del sistema operativo sui dispositivi che possono essere riavviati senza influire sulla connettività agli altri dispositivi in corso di aggiornamento.



Passaggio 2. Nel riquadro a comparsa visualizzato, in **Distribute** (Distribuisci) **> When** (Quando) selezionare **Now** (Ora), fare clic su **Next** (Avanti), in **Activate** (Attiva) selezionare **Schedule Activation after Distribution is completed** (Pianifica attivazione al completamento della distribuzione), fare clic su **Next** (Avanti), quindi in **Confirm** (Conferma), fare clic sul pulsante **Confirm** (Conferma).

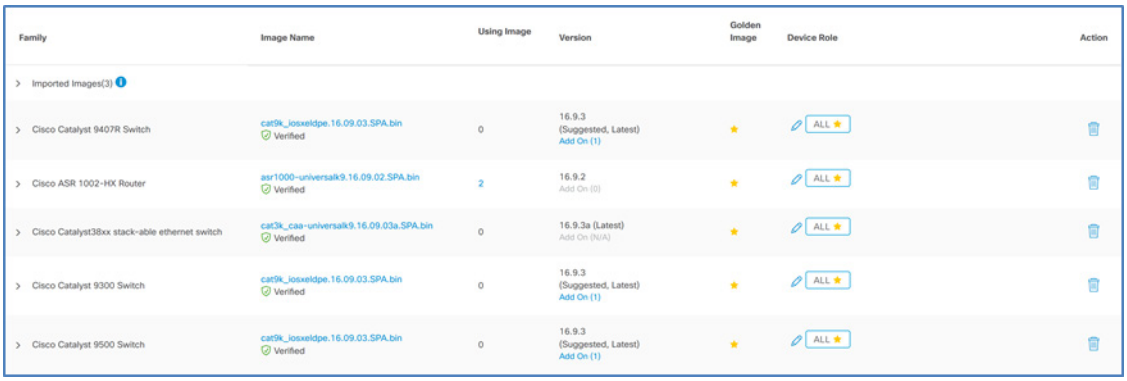
Le immagini vengono distribuite ai dispositivi selezionati.

Passaggio 3. In alto a destra, fare clic su **Update Status** (Aggiorna stato).



Sulla schermata di stato vengono forniti ulteriori dettagli rispetto alla schermata principale, compresa la spiegazione di eventuali errori. Utilizzare il pulsante **Refresh** (Aggiorna) finché lo stato **In Progress** (In corso) non cambia in **Successful** (Completato).

Passaggio 4. Ripetere questa procedura secondo necessità per aggiornare il software del dispositivo alle versioni richieste per l'implementazione della rete. Al termine, tutti i dispositivi per l'implementazione risultano associati a un'immagine preferita e l'immagine è installata.



Procedura – Provisioning della rete underlay per SD-Access

Dopo che Cisco DNA Center ha rilevato i dispositivi su cui è in esecuzione la versione software corretta di SD-Access, e ne ha assunto la gestione, è possibile utilizzarlo per effettuare il provisioning dei dispositivi nella rete underlay.

Procedura 1. Provisioning degli switch dell'underlay con la funzione LAN Automation (Automazione LAN)

Facoltativo

Utilizzare questa procedura se si stanno implementando switch LAN nuovi e non configurati nell'underlay con la funzione LAN Automation (Automazione LAN) di Cisco DNA Center. Adottare le procedure precedenti per configurare uno o più dispositivi seed (i dispositivi gestiti a cui si connette la nuova rete non gestita), le credenziali CLI e SNMP del dispositivo che PnP dovrà applicare e il pool di indirizzi IP raggiungibile dalla rete e utilizzato per la connettività. Anche se non si tratta di un requisito obbligatorio, ciascun dispositivo seed è in genere uno switch assegnato in una fase successiva come dispositivo di confine, con una modalità VTP e una configurazione MTU appropriate (ad esempio, modalità VTP trasparente, MTU di sistema 9100). Le porte sul dispositivo seed connesse ai dispositivi da rilevare devono essere in modalità layer 2 (porta di accesso anziché porta con routing) e le porte dei dispositivi seed non possono essere porte di gestione out-of-band (OOB) dedicate.

Suggerimento tecnico

La funzione di automazione LAN permette il rilevamento degli switch supportati da parte di dispositivi seed supportati (gli switch utilizzati per questa convalida sono elencati nell'appendice). Gli switch rilevati vengono connessi direttamente alle interfacce dei dispositivi seed selezionati (le porte di gestione OOB non possono essere connesse durante l'onboarding dei dispositivi con automazione LAN perché bloccherebbero l'automazione della LAN sulle porte non OOB) e agli switch connessi con al massimo un hop aggiuntivo, per un totale di due hop dal dispositivo seed. Le credenziali fornite permettono a Cisco DNA Center e ai dispositivi seed di collaborare insieme per configurare i dispositivi rilevati e aggiungerli all'inventario gestito. Poiché i dispositivi rilevati devono eseguire l'agente PnP senza configurazioni pregresse, gli switch eventualmente già configurati devono essere ripristinati a uno stato in cui l'agente PNP è in esecuzione, utilizzando i seguenti comandi della modalità di configurazione e della modalità di esecuzione:

```
(config)#config-register 0x2102
(config)#crypto key zeroize
(config)#no crypto pki certificate pool
delete /force vlan.dat
delete /force nvram:*.cer
delete /force nvram:pnp*
delete /force flash:pnp*
delete /force stby-nvram:*.cer
delete /force stby-nvram:*.pnp*
! previous two lines only for HA systems
write erase
reload
```

Non salvare le configurazioni per il processo di ricarica. Per preparare gli stack di switch per l'automazione LAN, utilizzare gli stessi comandi di ripristino per ciascun switch dello stack.

I requisiti per lo stacking degli switch non cambiano per l'automazione LAN: tutti gli switch dello stack devono avere la stessa licenza e versione software in grado di supportare le funzionalità di routing IP e devono essere in modalità di installazione (non in modalità bundle). Per avere il massimo controllo sulla numerazione delle porte e il comportamento dello stack, prima di avviare il processo di automazione LAN, è possibile modificare la numerazione degli switch nello stack e assegnare a uno di loro il ruolo ACTIVE (Attivo) aumentandone quindi la priorità. A tal fine usare i seguenti comandi in modalità di esecuzione:

```
switch [switch stack number] renumber [new stack number]
switch [switch stack number] priority 15
```

Identificare uno o due dispositivi presenti nell'inventario e gestiti da Cisco DNA Center per assegnare il ruolo di dispositivo seed a una sede. È possibile utilizzare gli stessi dispositivi seed per più esecuzioni della funzionalità di automazione LAN, in modo che i dispositivi rilevati vengano assegnati a diversi edifici o piani in ciascuna esecuzione.

Passaggio 1. Dalla dashboard principale di Cisco DNA Center, accedere a **PROVISION** (Provisioning) **> Devices** (Dispositivi) **> Inventory** (Inventario). Selezionare un massimo di due dispositivi seed, dal menu a discesa **Actions** (Azioni), fare clic su **Assign Device to Site** (Assegna dispositivo alla sede). Sulla schermata **Assign Device to Site** (Assegna dispositivo alla sede), selezionare le assegnazioni, quindi fare clic su **Apply** (Applica).

Passaggio 2. Se il dispositivo seed è un Catalyst serie 6800, utilizzare i comandi della modalità di configurazione dell'interfaccia per modificare le porte dei dispositivi rilevati in porte di layer 2.

```
switchport
```

Dopo aver salvato le modifiche alla configurazione, sincronizzare nuovamente il dispositivo dalla dashboard principale di Cisco DNA Center: in **Tools** (Strumenti), selezionare **Inventory** (Inventario), selezionare il Catalyst 6800 Switch modificato, quindi in alto sulla schermata, dal menu a discesa **Actions** (Azioni), selezionare **Resync** (Risincronizza).

Suggerimento tecnico

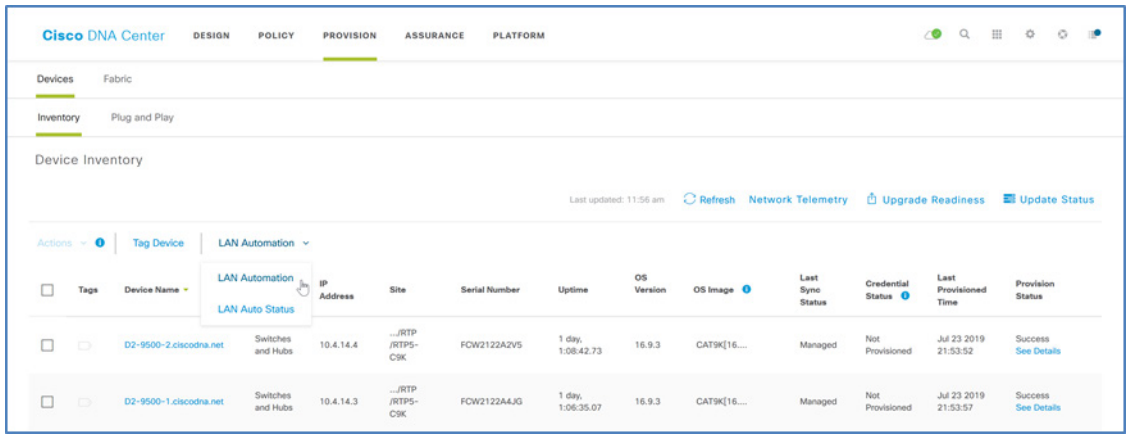
Il pool di IP utilizzato per l'automazione LAN deve essere notevolmente più grande del numero di dispositivi da rilevare. Il pool è diviso in due, una metà viene utilizzata per i servizi DHCP VLAN 1 forniti dai dispositivi seed. L'altra metà del pool viene nuovamente divisa a metà, assegnando un quarto dello spazio degli indirizzi totale alla gestione degli indirizzi di collegamento point-to-point e l'altro quarto alla gestione degli indirizzi di loopback. Gli endpoint non devono essere collegati agli switch, in quanto possono esaurire il pool di IP che DHCP usa per il provisioning PnP.

Gli indirizzi del pool di automazione LAN devono essere raggiungibili da Cisco DNA Center in modo da completare correttamente il provisioning e non devono essere utilizzati altrove nella rete. Se Cisco DNA Center usa la rete di gestione dedicata facoltativa per la porta di accesso al Web anziché una singola porta con route predefinita, accertarsi che la route al pool di IP con automazione LAN sia disponibile tramite la porta dell'infrastruttura di rete aziendale. Se il pool IP non è incluso nelle route configurate su Cisco DNA Center, connettersi a Cisco DNA Center utilizzando la porta SSH 2222, quindi effettuare l'accesso come maglev ed eseguire il comando:

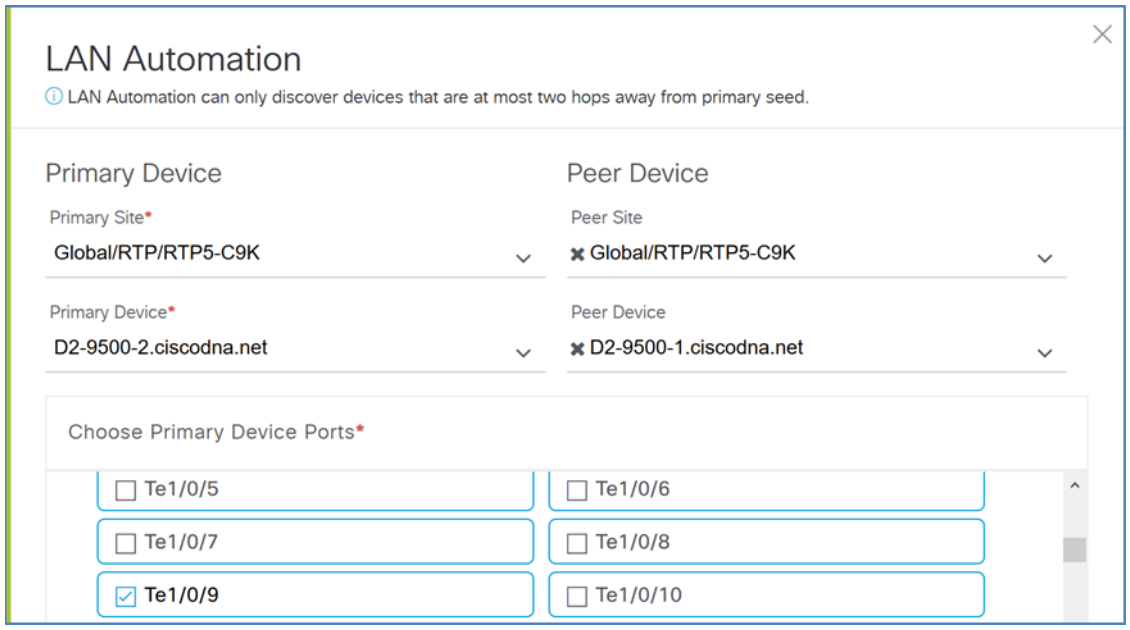
```
sudo Maglev-config Update
```

Utilizzare la procedura di configurazione guidata per configurare le route statiche e includere il pool di IP nella scheda di rete corretta prima di avviare l'automazione della LAN.

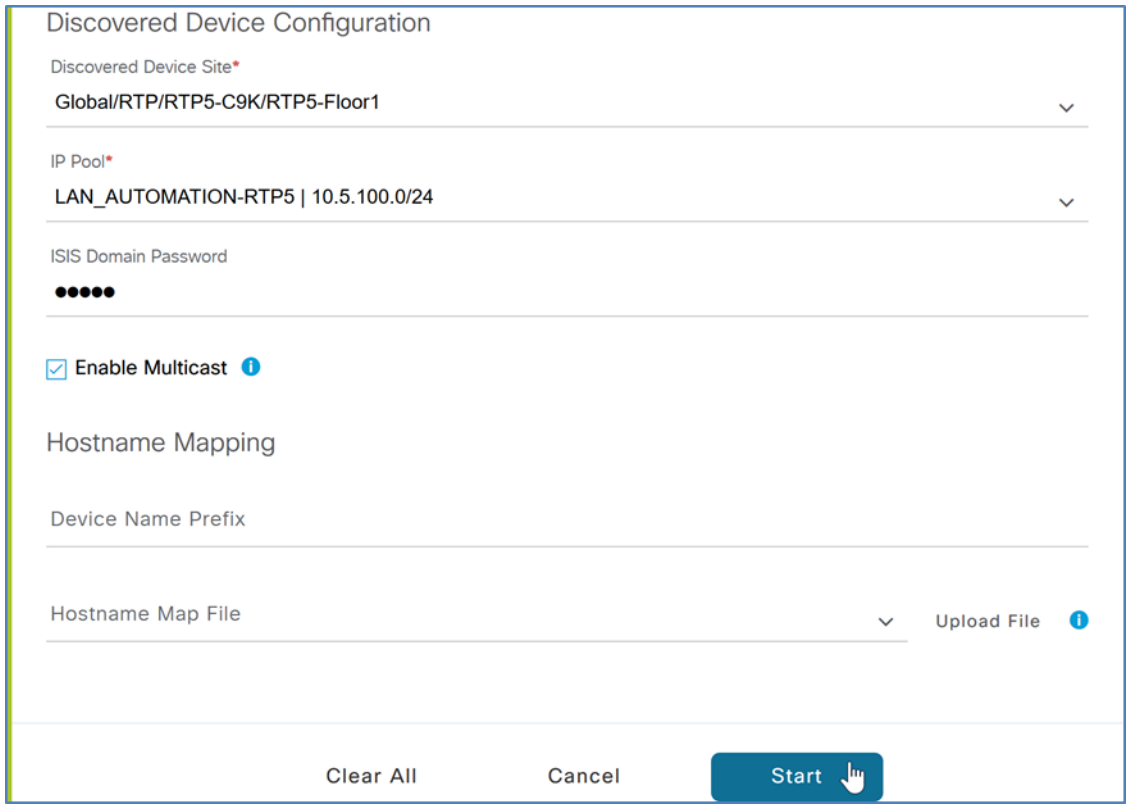
Passaggio 3. Accedere a **PROVISION (Provisioning) > Devices (Dispositivi) > Inventory (Inventario)**. Nella parte superiore, fare clic sul menu a discesa **LAN Automation** (Automazione LAN), quindi fare clic su **LAN Automation** (Automazione LAN).



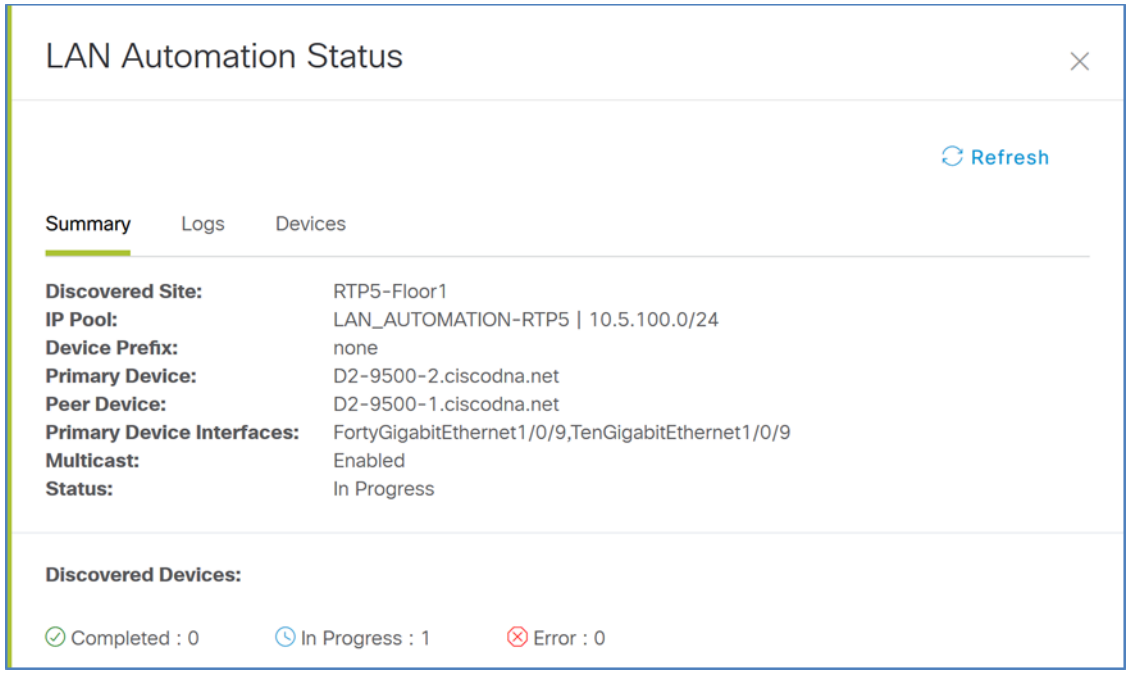
Passaggio 4. A destra nel riquadro a comparsa LAN Automation (Automazione LAN), completare i parametri di rilevamento. In **Primary Device** (Dispositivo principale), fornire un valore per **Primary Site*** (Sede principale), **Primary Device*** (Dispositivo principale), **Choose Primary Device Ports*** (Seleziona porte dispositivo principale). In **Peer Device** (Dispositivo peer), fornire un valore per **Peer Site** (Sede peer) e **Peer Device** (Dispositivo peer).



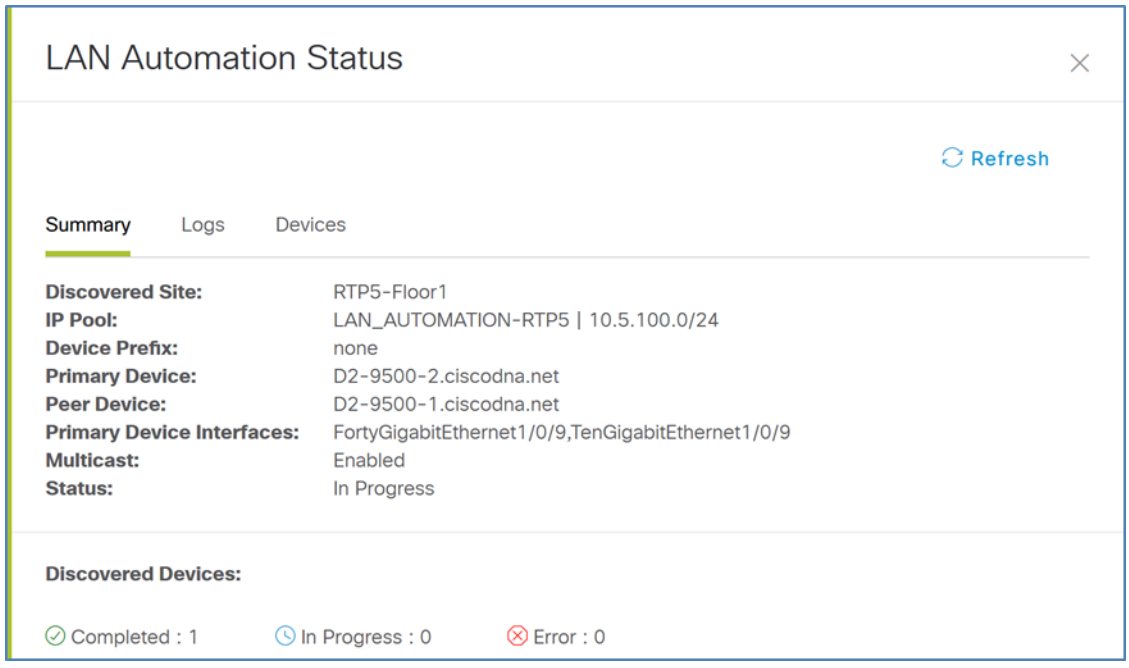
Passaggio 5. A destra nel riquadro a comparsa di LAN Automation (Automazione LAN), completare i parametri di rilevamento. In **Discovered Device Configuration** (Configurazione dispositivi rilevati), fornire un valore per **Discovered Device Site*** (Sede dispositivo rilevato), **IP Pool*** (Pool di IP), se utilizzato, **ISIS Domain Password** (Password dominio IS-IS), selezionare **Enable Multicast** (Abilita multicast), quindi fare clic su **Start** (Avvia).



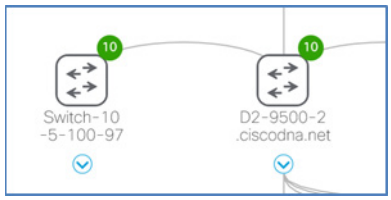
Passaggio 6. Nella parte superiore, fare clic sul menu a discesa **LAN Automation** (Automazione LAN), quindi fare clic su **LAN Auto Status** (Stato automatico LAN) per visualizzare lo stato di avanzamento.



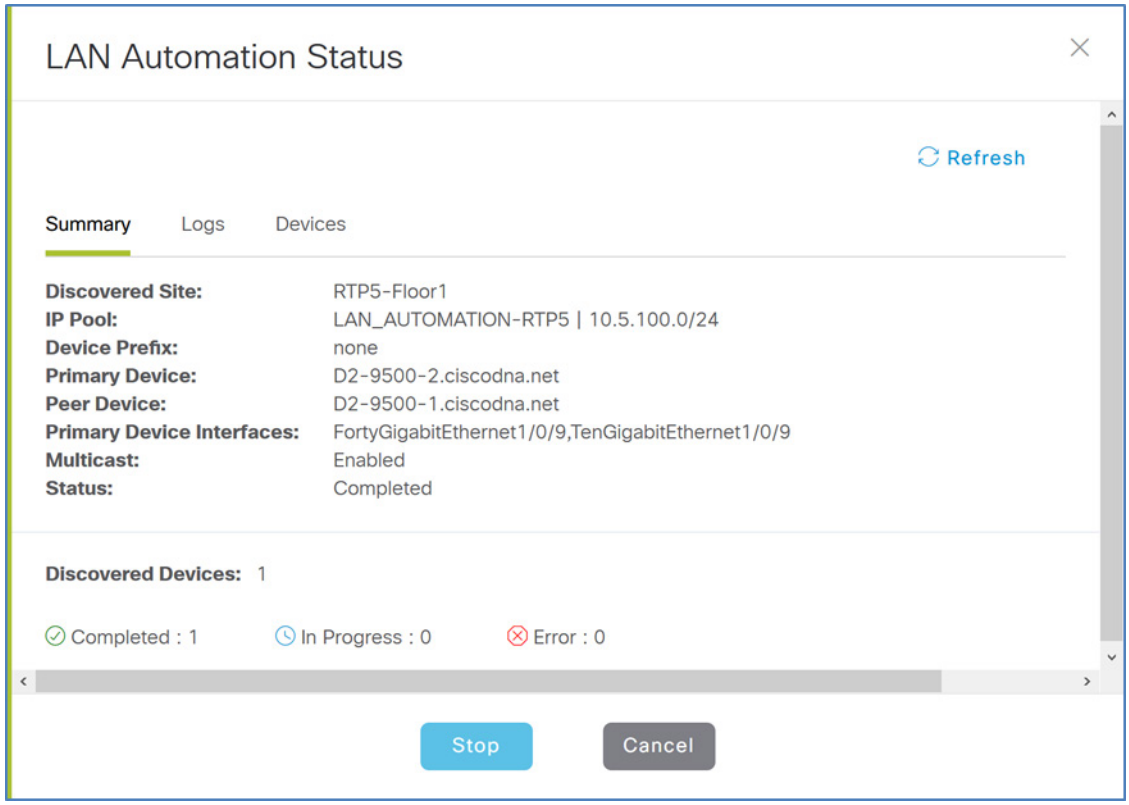
Non fare clic su **Stop** (Arresta) in questa fase. Attendere che tutti i dispositivi visualizzino lo stato **Completed** (Completato), quindi passare alla fase di verifica successiva. L'arresto anticipato del processo PnP rende necessario un intervento di ripristino manuale del processo di rilevamento. Se i dispositivi da rilevare distano dal seed di un hop, i tempi di completamento possono aumentare notevolmente.



Passaggio 7. Accedere alla dashboard principale di Cisco DNA Center, in **Tools** (Strumenti), selezionare **Topology** (Topologia). Tutti i collegamenti devono essere rilevati. Se nella topologia mancano alcuni collegamenti, verificare la connettività fisica.



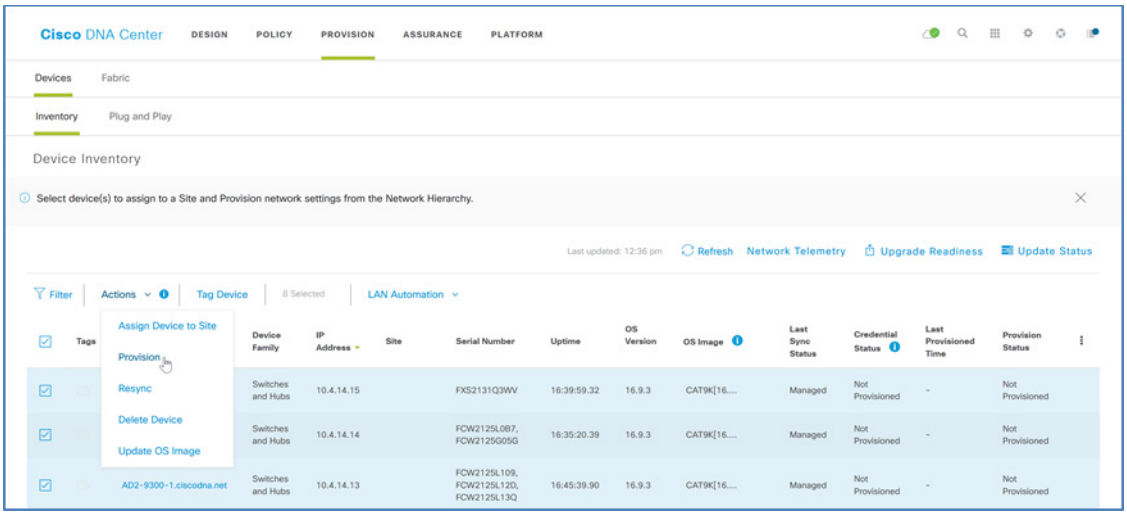
Passaggio 8. Accedere a **PROVISION (Provisioning) > Devices (Dispositivi) > Inventory (Inventario)**. Nella parte superiore, fare clic sul menu a discesa **LAN Automation** (Automazione LAN), quindi fare clic su **LAN Auto Status** (Stato automatico LAN). Una volta che tutti i dispositivi rilevati hanno lo stato **Completed** (Completato), fare clic su **Stop** (Arresta). L'automazione LAN interrompe tutta la connettività di layer 2 sulla VLAN 1, viene usato il processo di routing IS-IS dell'underlay per la raggiungibilità della rete con routing e i dispositivi vengono gestiti nell'inventario.



Procedura 2. Provisioning dei dispositivi e assegnazione alle sedi per la preparazione di SD-Access

Eseguire il provisioning dei dispositivi di rete, quindi assegnare i dispositivi a una sede per integrarli nella rete SD-Access.

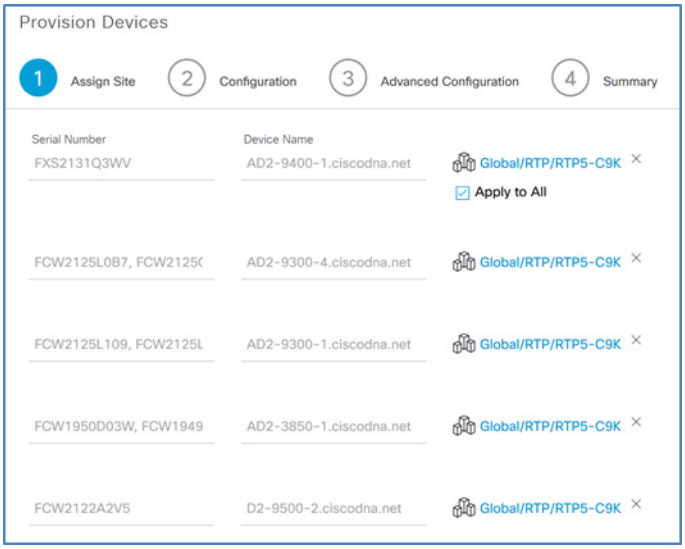
Passaggio 1. In Cisco DNA Center, accedere a **PROVISION (Provisioning) > Devices (Dispositivi) > Inventory (Inventario)**, selezionare i dispositivi dello stesso tipo (ad esempio, tutti switch) su cui effettuare il provisioning nella rete, quindi fare clic su **Actions** (Azioni) e su **Provision** (Effettua il provisioning).



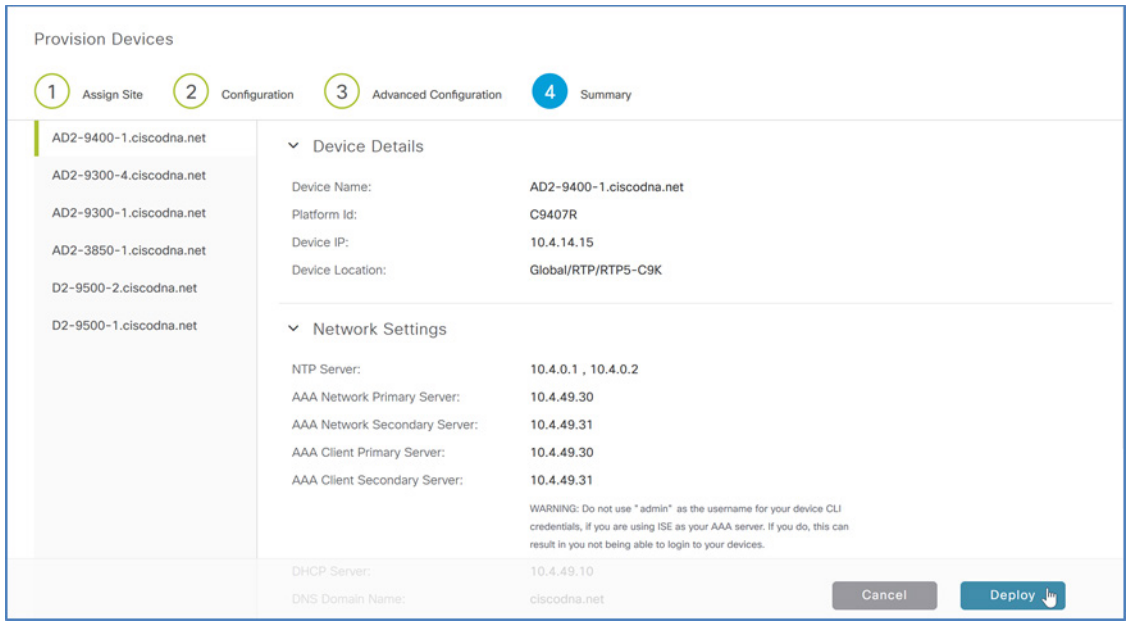
Viene visualizzata la procedura guidata **Provision Devices** (Provisioning dei dispositivi).

Suggerimento tecnico
I dispositivi devono essere dello stesso tipo (ad esempio, tutti router) per effettuarne il provisioning contemporaneamente. È possibile raggruppare le operazioni di provisioning in più batch piccoli e assegnarli alle sedi comuni, se necessario.

Passaggio 2. Nella prima schermata della procedura guidata, selezionare le assegnazioni delle sedi dei dispositivi, quindi nella parte inferiore della schermata fare clic su **Next** (Avanti).



Passaggio 3. Fare clic su **Next** (Avanti) due volte per ignorare le schermate **Configuration** (Configurazione) e **Advanced Configuration** (Configurazione avanzata), nella schermata **Summary** (Riepilogo) riesaminare i dettagli di ciascun dispositivo, quindi fare clic su **Deploy** (Implementa).

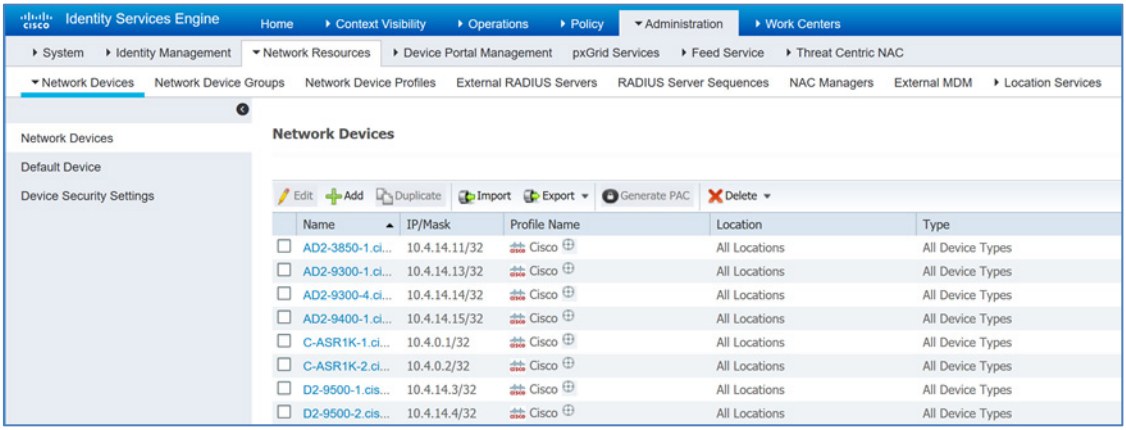


Passaggio 4. Nella schermata popup, confermare l'impostazione predefinita **Now** (Ora), quindi fare clic su **Apply** (Applica).

Viene avviata la configurazione di ciascun dispositivo; al completamento del provisioning viene visualizzato un messaggio di stato. Sulla schermata Device Inventory (Inventario dei dispositivi), i valori di **Provision Status** (Stato provisioning) e **Sync Status** (Stato sincronizzazione) vengono aggiornati. Utilizzare il pulsante **Refresh** (Aggiorna) per aggiornare lo stato finale.

Passaggio 5. Ripetere i passaggi di provisioning di Cisco DNA Center per ciascun gruppo di dispositivi aggiunti. L'integrazione pxGrid di Cisco DNA Center aggiorna i dispositivi in ISE.

Passaggio 6. Verificare la funzione di integrazione ISE accedendo a ISE e selezionando **Administration (Amministrazione) > Network Resources (Risorse di rete) > Network Devices (Dispositivi di rete)**. Vengono visualizzati i dispositivi di cui è stato effettuato il provisioning.



Procedura – Provisioning della rete overlay di SD-Access

In Cisco DNA Center viene creata una rete overlay del fabric utilizzando i dispositivi rilevati, aggiunti all'inventario e assegnati a una sede. Cisco DNA Center automatizza la configurazione supplementare dei dispositivi supportando le reti overlay di SD-Access.

La soluzione SD-Access supporta il provisioning dei seguenti componenti del fabric:

- Sede del fabric: un fabric indipendente, che include un nodo del piano di controllo e un nodo edge, che usa un nodo di confine per l'uscita dalla sede e che in genere include un PSN ISE e un WLC in modalità fabric
- Sede di transito: nota anche come rete di transito, connette una sede del fabric a una rete esterna (transito basato su IP) o a uno o più sedi del fabric che conservano in modo nativo la segmentazione (transito SD-Access)
- Dominio del fabric: comprende una o più sedi del fabric e le eventuali sedi di transito corrispondenti

Le reti di transito basate su IP collegano il fabric alle reti esterne, in genere utilizzando VRF-Lite per la connettività IP. I transiti SD-Access trasportano informazioni SGT e VN, trasportando implicitamente la policy e la segmentazione tra le sedi del fabric e creando un campus distribuito.

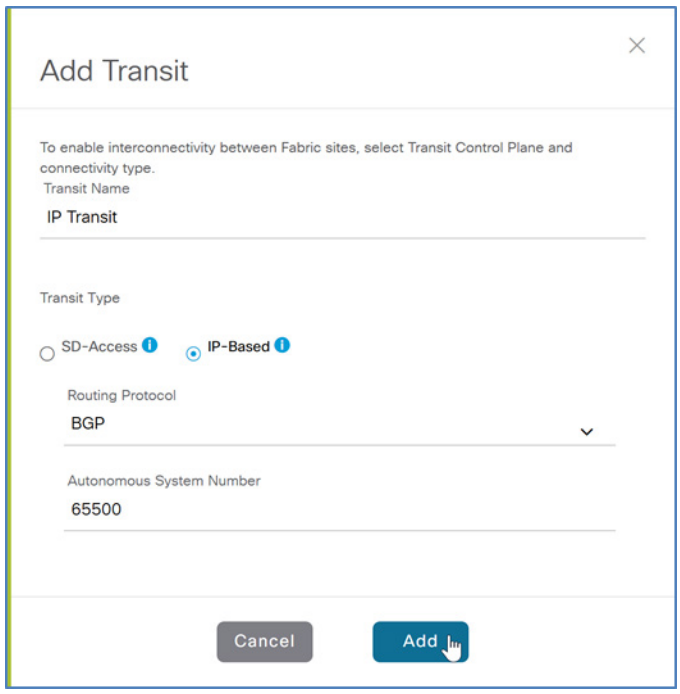
Suggerimento tecnico
Il software Cisco DNA Center e il software Cisco IOS elencati nell'appendice non includono la convalida del transito SD-Access, descritto nella guida prescrittiva all'implementazione di Software-Defined Access for Distributed Campus. È possibile trovare versioni software alternative che possono supportare ulteriori opzioni consultando la matrice di compatibilità hardware e software di SD-Access sul sito cisco.com.

Il software Cisco DNA Center e il software Cisco IOS elencati nell'appendice non includono la convalida del transito SD-Access, descritto nella guida prescrittiva all'implementazione di Software-Defined Access for Distributed Campus. È possibile trovare versioni software alternative che possono supportare ulteriori opzioni consultando la matrice di compatibilità hardware e software di SD-Access sul sito cisco.com.

Procedura 1. Creazione di una sede di transito basata su IP, un dominio del fabric e delle sedi del fabric

La sede di transito basata su IP rappresenta il sistema autonomo (AS) remoto BGP. Il sistema autonomo BGP locale viene configurato come parte del provisioning del confine del fabric in una procedura successiva.

Passaggio 1. In Cisco DNA Center, accedere a **PROVISION (Provisioning) > Fabric**, in alto a destra sulla schermata fare clic su **+ Add Fabric or Transit** (+ Aggiungi fabric o transito), quindi fare clic su **Add Transit** (Aggiungi transito). Nel riquadro a comparsa fornire un valore per **Transit Name** (Nome transito) (ad esempio, IP_Transit), selezionare **IP-Based** (Basato su IP) per **Routing Protocol** (Protocollo di routing), selezionare **BGP**, fornire un valore per **Autonomous System Number** (Numero sistema autonomo) per il sistema autonomo remoto BGP (ad esempio, 65500), quindi fare clic su **Add** (Aggiungi).

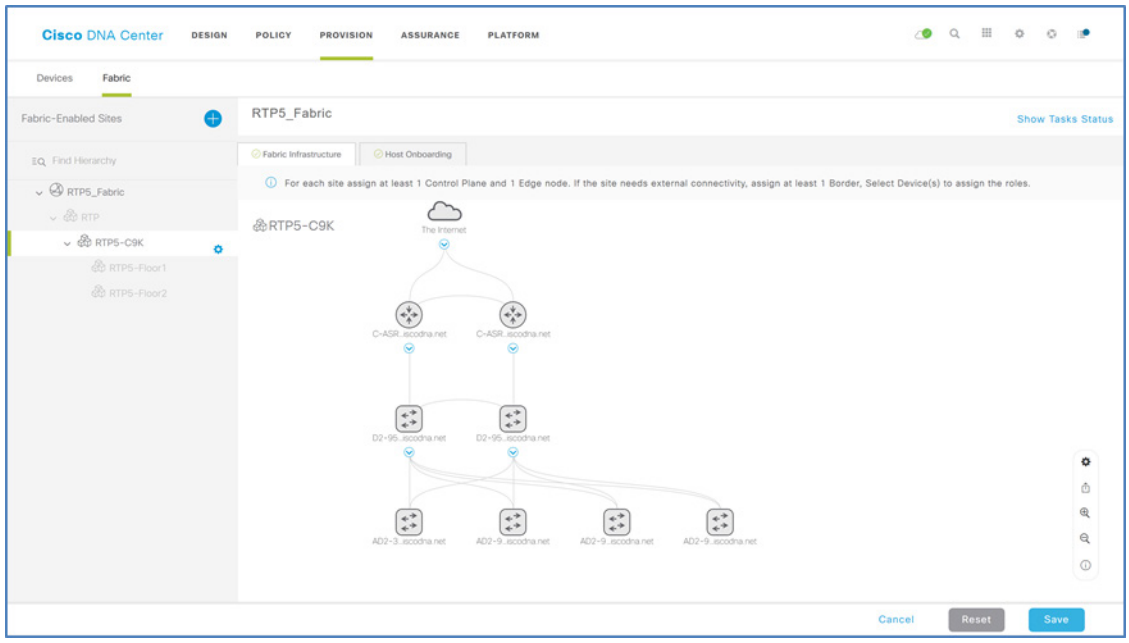


Viene visualizzato un messaggio di stato e la sede di transito viene creata.

Passaggio 2. Accedere a **PROVISION (Provisioning) > Fabric**, in alto a destra sulla schermata fare clic su **+ Add Fabric or Transit** (+ Aggiungi fabric o transito), fare clic su **Add Fabric** (Aggiungi fabric). Nel riquadro a comparsa fornire un valore per **Fabric Name** (Nome fabric) (ad esempio, RTP5_Fabric), utilizzare la gerarchia delle sedi per selezionare una posizione che contenga le sedi per abilitare il fabric (ad esempio, RTP5-C9K), quindi fare clic su **Add** (Aggiungi).

Viene creato il nuovo fabric del campus.

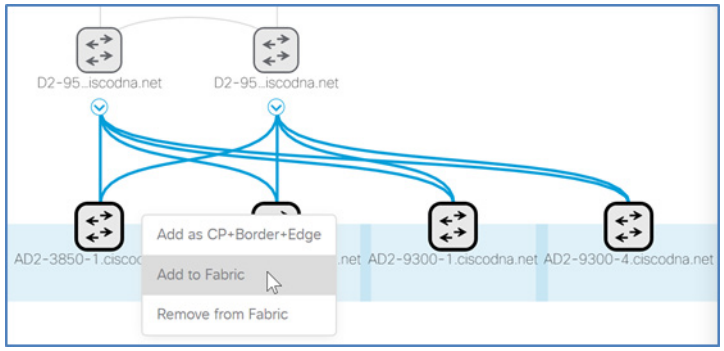
Passaggio 3. Fare clic sul nome di dominio del fabric appena creato (ad esempio, RTP5_Fabric), nella gerarchia a sinistra **Fabric-Enabled Sites** (Sedi basate sul fabric), selezionare la sede aggiunta al passaggio precedente (ad esempio, RTP5-C9K). Viene visualizzata una vista del fabric e delle sedi correlate.



Se il diagramma della topologia del fabric visualizzato non simula la topologia implementata a due livelli (distribuzione/accesso) o a tre livelli (core/distribuzione/accesso), correggere la topologia selezionando **Tools (Strumenti) > Inventory (Inventario)**. In alto a destra sulla riga del titolo della tabella dell'inventario, scegliere quali colonne visualizzare per includere **Device Role** (Ruolo dispositivo), quindi modificare il ruolo in modo che rifletta il più fedelmente possibile l'implementazione effettiva del dispositivo. Tornare alla vista della topologia del dominio del fabric dopo aver modificato i ruoli dei dispositivi per una vista aggiornata.

Procedura 2. Creazione di un fabric overlay

Passaggio 1. Nella vista della topologia del dominio del fabric, tenere premuto il tasto Maiusc, fare clic su tutti i nodi edge del fabric, quindi nella finestra popup, fare clic su **Add to Fabric** (Aggiungi a fabric).



I bordi delle icone vengono visualizzati in blu e compaiono i simboli dei ruoli del fabric per segnalare il comportamento previsto dei dispositivi.

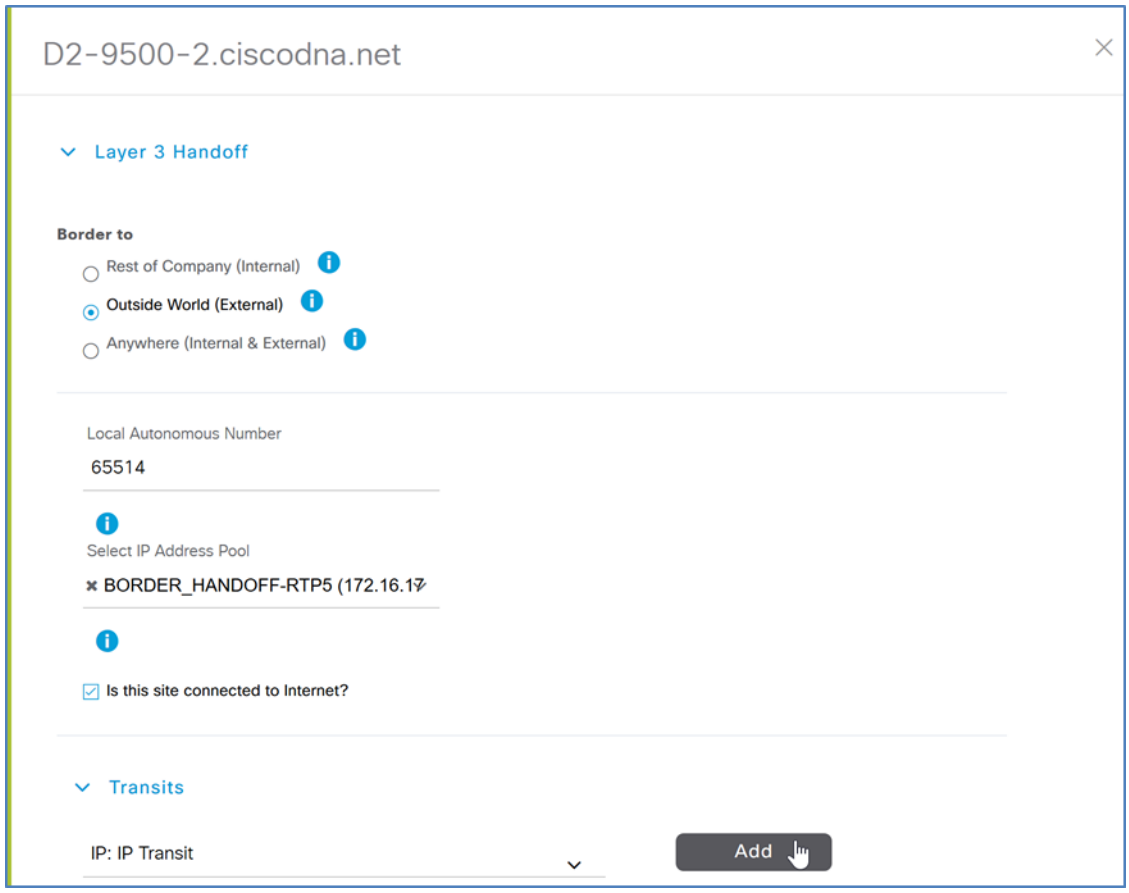
Passaggio 2. Se un nodo del fabric è stato dedicato al ruolo di piano di controllo senza funzionalità di confine, fare clic su di esso, quindi nella finestra popup, fare clic su **Add as CP** (Aggiungi come piano di controllo).

Ripetere questo passaggio per un nodo del piano di controllo dedicato ridondante senza funzionalità di confine.

Suggerimento tecnico

Se i nodi di confine sono Cisco Nexus serie 7700 Switch, utilizzare il software elencato nell'Appendice A – Elenco dei prodotti, utilizzare nodi dei piani di controllo dedicati e connetterli direttamente agli switch serie 7700, configurati come nodi di confine esterni. Se la versione di NX-OS lo richiede, abilitare la licenza MPLS. Configurare l'LDP MPLS sui collegamenti fisici ai nodi dei piani di controllo per supportarne la connettività.

Passaggio 3. Fare clic su un dispositivo per eseguire il ruolo di confine del fabric, nella finestra popup fare clic su **Add as Border** (Aggiungi come confine) o su **Add as CP+Border** (Aggiungi come piano di controllo+confine) (se il passaggio precedente è stato ignorato), quindi completare i dati sul riquadro a comparsa. In **Layer 3 Handoff** (Handoff layer 3), selezionare **Border** (Confine) (ad esempio, Outside World (External) (Mondo esterno)), fornire un valore per **BGP Local Autonomous Number** (Numero autonomo locale BGP) (ad esempio, 65514). In **Select IP Address Pool** (Seleziona pool di indirizzi IP), selezionare il pool globale configurato in precedenza per la connettività di confine (ad esempio, BORDER_HANDOFF-RTP5), per i confini esterni selezionare **Is this site connected to the Internet?** (Questa sede è collegata a Internet?), nel menu **Transit** (Transito), selezionare il transito (ad esempio, IP: IP Transit (IP: Transito IP)), quindi accanto al transito fare clic sul pulsante grigio **Add** (Aggiungi).

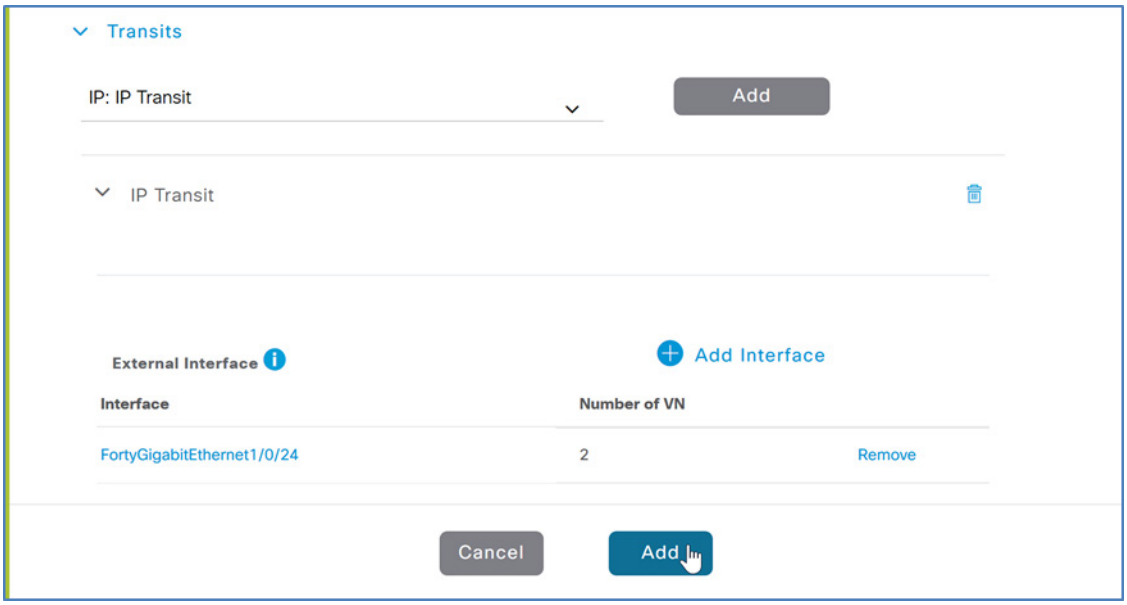


Viene visualizzata una sezione **IP Transit** (Transito IP).

Suggerimento tecnico

Se il confine è l'unico percorso per uscire dal fabric e raggiungere il resto della rete, scegliere un confine esterno. Quando si usa una funzionalità combinata di piano di controllo e nodo di confine e il nodo utilizza la funzione di confine interna, potrebbe essere necessario un ulteriore filtraggio del piano di controllo quando si usano le versioni convalidate contenute nell'Appendice A – Elenco dei prodotti.

Passaggio 4. Fare clic sul testo **IP Transit** (Transito IP), fare clic su **+ Add Interface** (+ Aggiungi interfaccia), nel riquadro a comparsa selezionare l'interfaccia della connessione al router ibrido esterno al fabric. In **Remote AS Number** (Numero AS remoto) del protocollo BGP del dispositivo esterno al fabric visualizzato, espandere il pannello di selezione **Virtual Network** (Rete virtuale). Selezionare ciascuna VN utilizzata nel fabric per includere l'handoff di layer 3 esterno al fabric (ad esempio, INVRA_VN, OPERATIONS), fare clic su **Save** (Salva), quindi fare clic su **Add** (Aggiungi).

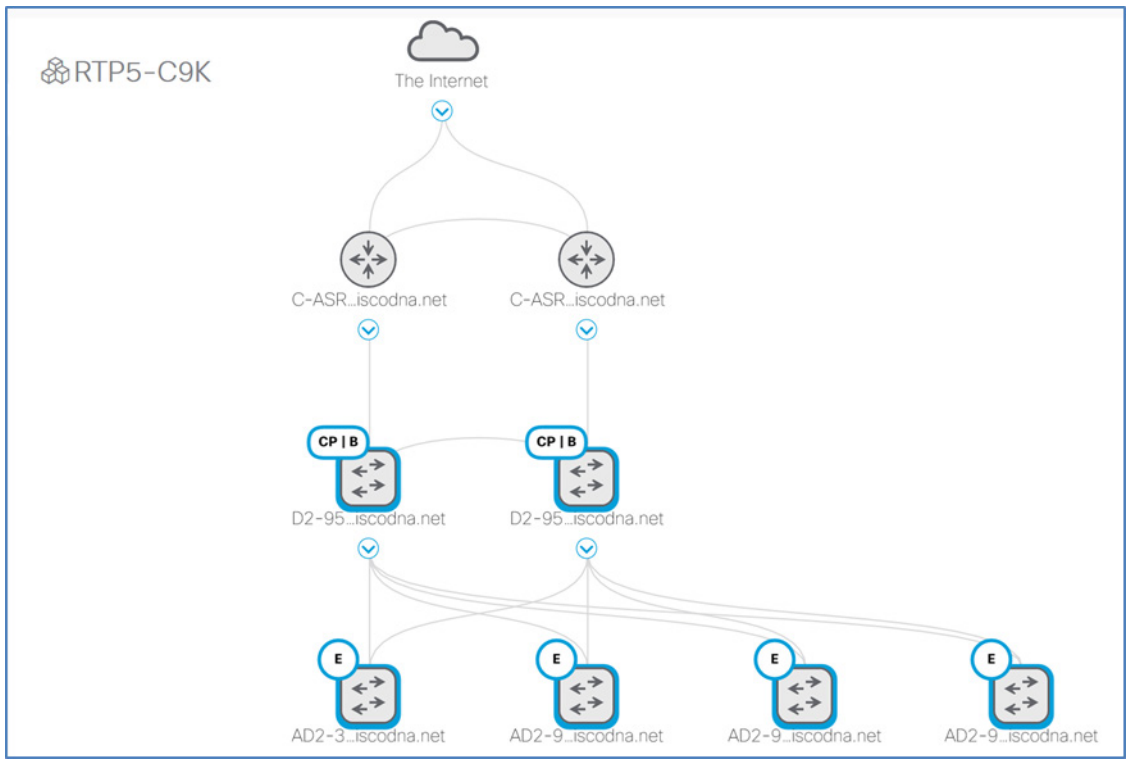


Confermare eventuali schermate popup informative.

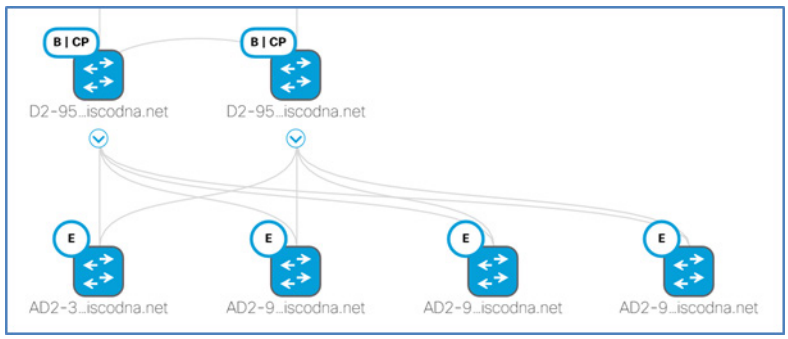
Passaggio 5. Se si dispone di un altro nodo di confine del fabric, ripetere i due passaggi precedenti.

Suggerimento tecnico
Per configurare un'interfaccia handoff VRF-Lite dal confine al resto della rete, è necessario usare un'interfaccia con tag 802.1Q. Se si gestisce il confine con la connettività in-band sui collegamenti ridondanti da convertire, stabilire prima la connessione su un'interfaccia con tag, come descritto nelle procedure di gestione della configurazione su un dispositivo di confine per il rilevamento della rete. Quando si utilizza la versione dell'SD-Access convalidata in questa guida, il provisioning non avrà esito positivo se l'interfaccia include già una configurazione senza tag.

Passaggio 6. Dopo aver assegnato i ruoli richiesti ai nodi del fabric, in basso sulla schermata fare clic su **Save** (Salva), utilizzare l'impostazione predefinita **Now** (Ora), quindi fare clic su **Apply** (Applica). Viene creato il dominio del fabric del campus.



Le icone del fabric diventano blu per segnalare l'intento dell'utente di creare il fabric. Il provisioning effettivo dei dispositivi può richiedere più tempo.



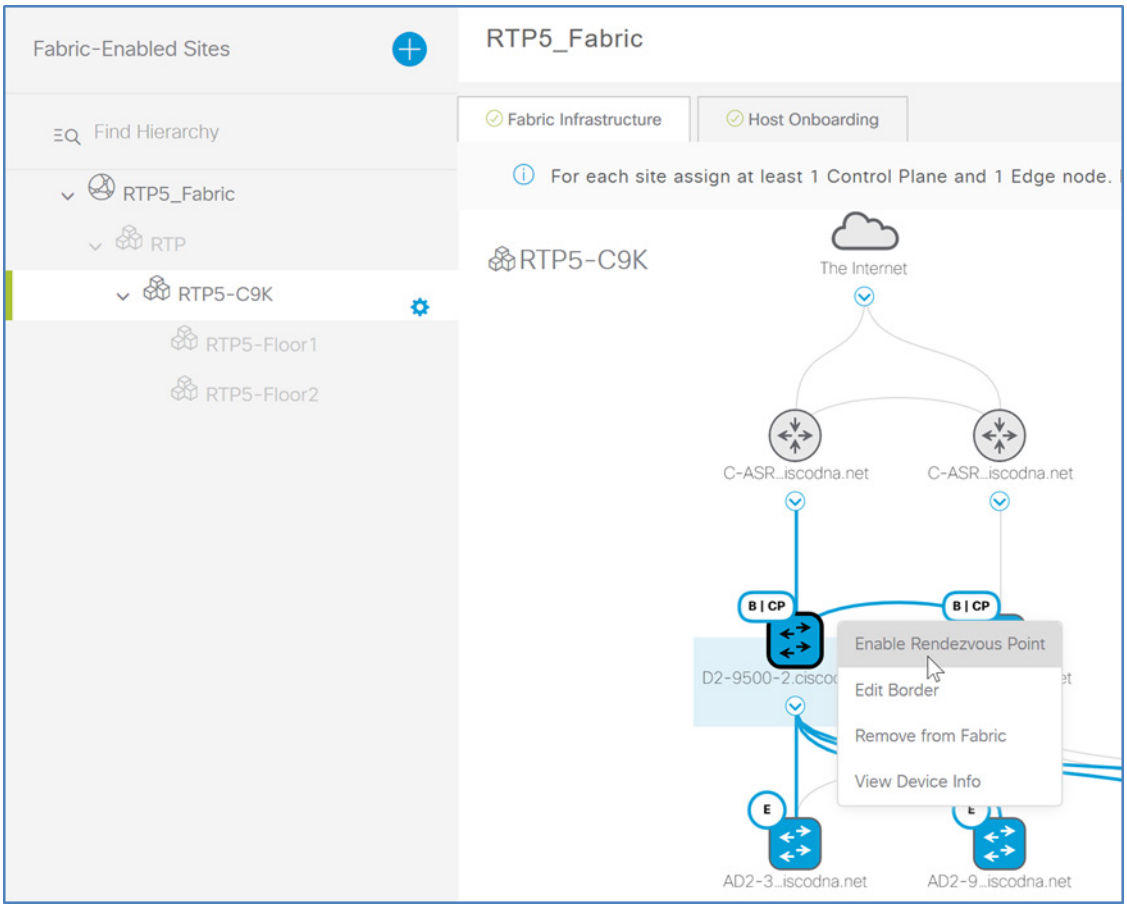
Procedura 3. Abilitazione del multicast per il fabric

Utilizzare questa procedura per configurare il supporto multicast nel fabric overlay.

I fabric SD-Access possono supportare i multicast ASM (Any Source Multicast) e SSM (Source Specific Multicast). Le origini possono essere all'interno o all'esterno del fabric, la configurazione RP (Rendezvous Point) è disponibile solo sui nodi di confine del fabric. I messaggi PIM sono trasmessi in unicast tra i nodi di confine e gli edge del fabric, i pacchetti multicast vengono replicati nei dispositivi di confine del fabric iniziali diretti ai nodi dell'edge del fabric.

Passaggio 1. In Cisco DNA Center viene usato un pool globale dedicato per le interfacce IP unicast per configurare il multicast su ciascuna rete virtuale in cui questa modalità è abilitata. Se questo pool non esiste, riesaminare la procedura " Definizione dei pool di indirizzi IP globali" per crearne uno.

Passaggio 2. Dalla dashboard di Cisco DNA Center, accedere a **PROVISION (Provisioning) > Fabric**, in **Fabrics** fare clic sulla sede del fabric creata (ad esempio, RTP5_Fabric). Nel riquadro di navigazione sinistro, fare clic sulla sede del fabric (ad esempio, RTP5-C9K), in alto sulla schermata fare clic sulla scheda **Fabric Infrastructure** (Infrastruttura del fabric), fare clic su un nodo di confine del fabric, quindi selezionare **Enable Rendezvous Point** (Abilita Rendezvous Point).



Passaggio 3. Nella finestra popup **Associate Multicast Pools to VNs** (Associa pool multicast alle reti virtuali), in Associate Virtual Networks (Associa reti virtuali), selezionare la rete virtuale (ad esempio, OPERATIONS). In **Select IP Pools** (Seleziona pool di IP), selezionare il pool creato per il multicast (ad esempio, MULTICAST_PEER-RTP5), fare clic su **Next** (Avanti), selezionare una rete virtuale (ad esempio, OPERATIONS), quindi fare clic su **Enable** (Abilita).

Passaggio 4. Ripetere il passaggio precedente per gli altri nodi di confine del fabric. Nella parte inferiore della schermata, fare clic su **Save** (Salva), quindi fare clic su **Apply** (Applica).

Cisco DNA Center applica le configurazioni multicast ai nodi del fabric e crea i loopback e il peering del Multicast Source Discovery Protocol (MSDP) per la comunicazione RP (Rendezvous Point) tra i nodi di confine.

Passaggio 5. Se è richiesta la comunicazione multicast esterna al confine e indirizzata al router ibrido, abilitare i seguenti comandi su ciascun dispositivo.

Global:

```
ip multicast-routing
ip pim rp address [RP Address]
ip pim register-source Loopback0
ip pim ssm default
```

Interface or subinterface (for each virtual network):

```
ip pim sparse-mode
```

Passaggio 6. Nel riquadro di navigazione sinistro sulla sede configurata con il fabric, accanto al nome della sede, fare clic sull'icona ingranaggio, quindi fare clic su **Enable Native Multicast for IPv4** (Abilita multicast nativo per IPv4). In basso sulla schermata, fare clic su **Save** (Salva), nel riquadro a comparsa, confermare l'impostazione predefinita **Now** (Ora), quindi fare clic su **Apply** (Applica).

La configurazione multicast dell'overlay viene implementata in modo da usare il multicast dell'underlay per una comunicazione efficiente nell'infrastruttura.

Procedura 4. Abilitazione della connettività eBGP per VN sul router di confine vicino (ibrido)

L'applicazione SD-Access in Cisco DNA Center configura l'handoff BGP del nodo di confine del fabric sulle reti esterne. Nella versione SD-Access descritta, configurare manualmente i peer di rete esterna dei dispositivi di confine con le informazioni di peering compatibili con VRF-Lite e BGP.

Passaggio 1. Utilizzare la CLI per accedere ai dispositivi di confine ed esaminare le configurazioni automatizzate per la connettività IP esterna al confine creato dall'applicazione SD-Access di Cisco DNA Center. Alcuni dei seguenti comandi possono tornare utili.

```
show running-config brief
show running-config | section vrf definition
show running-config | section interface Vlan
show running-config | section router bgp
```

Suggerimento tecnico

Per evitare errori di connettività tra i nodi di confine e i router ibridi, implementare una coppia resiliente di nodi di confine collegati direttamente tra loro. Per abilitare il reindirizzamento automatico del traffico, creare una relazione iBGP tra i nodi di confine per ciascuna rete virtuale configurata. Supportare le connessioni logiche multiple utilizzando i tag 802.1Q mediante la configurazione delle porte trunk sugli switch e le sottointerfacce sui router.

Passaggio 2. Accedere a ciascun dispositivo ibrido esterno al fabric e collegato al confine utilizzando la configurazione del confine come guida, configurare le istanze VRF come richiesto dalle reti virtuali create sul confine. Le istanze VRF separano la comunicazione tra i gruppi di interfacce e i contesti delle reti virtuali all'interno del fabric.

```
vrf definition [VRF name]
 rd [Route Distinguisher]
 address-family ipv4
  route-target export [Route Target]
  route-target import [Route Target]
 exit-address-family
```

Ad esempio, se viene effettuato il provisioning della seguente configurazione sul confine:

```
vrf definition OPERATIONS
 rd 1:4099
 !
 address-family ipv4
  route-target export 1:4099
  route-target import 1:4099
 exit-address-family
```

Configurare le stesse impostazioni per il router ibrido.

Ripetere questo passaggio per ciascun contesto di rete virtuale (inclusa GUEST VRF, se presente), coerentemente con la configurazione del nodo di confine.

Suggerimento tecnico

Il nome dell'istanza VRF, l'identificatore delle route e i route target configurati sul router ibrido devono corrispondere a quanto configurato sul nodo di confine.

Passaggio 3. Configurare ciascuna interfaccia del dispositivo vicino. Alcuni dispositivi supportano la configurazione della sottointerfaccia VLAN direttamente sui trunk mentre altri dispositivi richiedono che le interfacce VLAN vengano create e associate a un trunk. Ripetere la configurazione dell'interfaccia adiacente per ciascun vicino su ciascun peer al confine.

```
interface [Peer physical interface]
 switchport mode trunk
interface [VLAN interface]
 vrf forwarding [VN/VRF name]
 ip address [Peer point-to-point IP address]
```

Ad esempio, se viene effettuato il provisioning della seguente configurazione sul confine:

```
vlan 3003
vlan 3004
interface FortyGigabitEthernet1/0/24
 switchport mode trunk
interface Vlan3003
 description vrf interface to External router
 vrf forwarding OPERATIONS
 ip address 172.16.172.9 255.255.255.252
interface Vlan3004
 description vrf interface to External router
 ip address 172.16.172.13 255.255.255.252
```

Configurare la connettività e gli indirizzi compatibili per il router ibrido. Nella tabella di routing globale, viene usata un'interfaccia VLAN senza istruzione di inoltro VRF associata per la comunicazione INFRA_VN.

```
vlan 3003
vlan 3004
interface FortyGigabitEthernet1/0/7
 switchport mode trunk
interface Vlan3003
 description vrf interface to External router
 vrf forwarding OPERATIONS
 ip address 172.16.172.10 255.255.255.252
interface Vlan3004
 description vrf interface to External router
 ip address 172.16.172.14 255.255.255.252
```

Passaggio 4. Configurare il routing unicast IPv4 del BGP verso il confine per supportare la connettività di ciascuna VRF associata a ciascuna rete virtuale del fabric.

```
router bgp [Local BGP AS]
 bgp router-id interface Loopback0
```

```
 bgp log-neighbor-changes
 neighbor [Border VLAN IP Address] remote-as [Fabric BGP AS]
 neighbor [Border VLAN IP Address] update-source [VLAN interface]
 ! repeat for any additional neighbors
address-family ipv4
  network [Loopback IP Address] mask 255.255.255.255
  neighbor [Border VLAN IP Address] activate
! repeat for any additional neighbors
  maximum-paths 2
 exit-address-family
 address-family ipv4 vrf [VN/VRF name]
  neighbor [Border VLAN IP Address] remote-as [Fabric BGP AS]
  neighbor [Border VLAN IP Address] update-source [VLAN interface]
  neighbor [Border VLAN IP Address] activate
! repeat for any additional neighbors
 exit-address-family
```

Ad esempio, se viene effettuato il provisioning della seguente configurazione sul confine:

```
router bgp 65514
 bgp router-id interface Loopback0
 neighbor 172.16.172.14 remote-as 65500
 neighbor 172.16.172.14 update-source Vlan3004
 !
 address-family ipv4
  network 172.16.173.1 mask 255.255.255.255
  aggregate-address 172.16.173.0 255.255.255.0 summary-only
  neighbor 172.16.172.14 activate
exit-address-family
 !
 address-family ipv4 vrf OPERATIONS
  neighbor 172.16.172.10 remote-as 65500
  neighbor 172.16.172.10 update-source Vlan3003
  neighbor 172.16.172.10 activate
exit-address-family
```

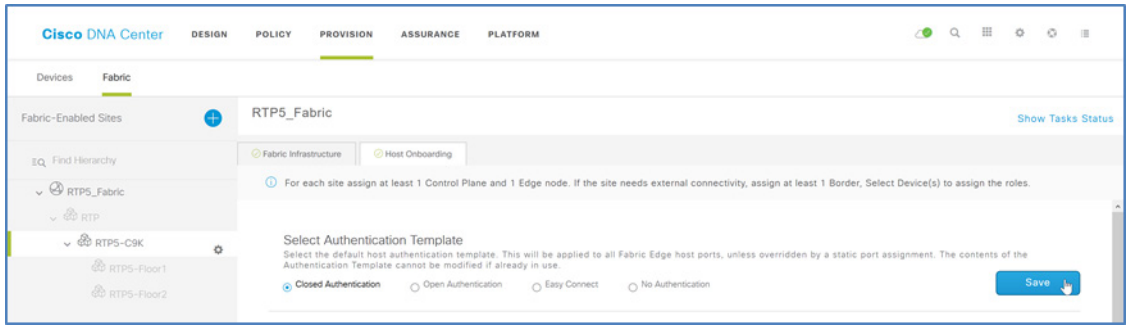
Configurare quanto segue sul router ibrido:

```
router bgp 65500
 bgp router-id interface Loopback0
 bgp log-neighbor-changes
 neighbor 172.16.172.13 remote-as 65514
 neighbor 172.16.172.13 update-source Vlan3004
 !
 address-family ipv4
```

```
  neighbor 172.16.172.13 activate
 exit-address-family
 !
 address-family ipv4 vrf OPERATIONS
  neighbor 172.16.172.9 remote-as 65500
  neighbor 172.16.172.9 update-source Vlan3003
  neighbor 172.16.172.9 activate
exit-address-family
```

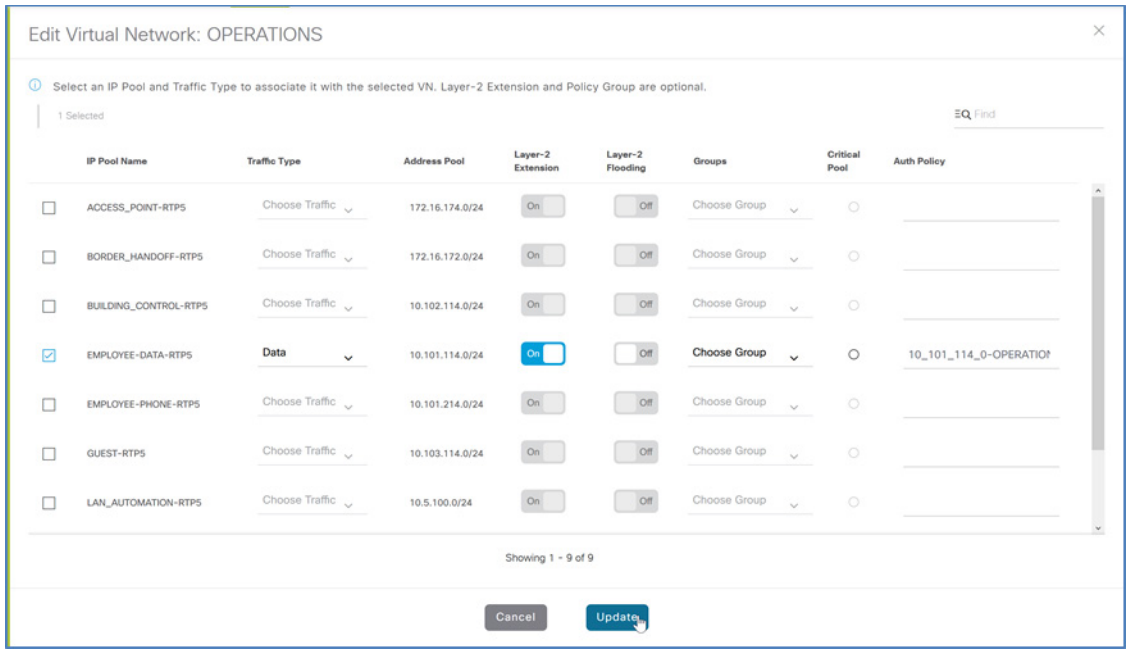
Procedura 5. Assegnazione di client cablati alla rete virtuale e abilitazione della connettività

Passaggio 1. Dalla dashboard di Cisco DNA Center, accedere a **PROVISION (Provisioning) > Fabric**, in **Fabrics** (Fabric), fare clic sulla sede del fabric creata (ad esempio, RTP5_Fabric). Nel riquadro di navigazione sinistro, fare clic sulla sede del fabric (ad esempio, RTP5-C9K), in alto sulla schermata fare clic sulla scheda **Host Onboarding** (Onboarding host), in **Select Authentication template** (Seleziona modello di autenticazione), selezionare **Closed Authentication** (Autenticazione chiusa), in alto sulla sezione, fare clic su **Save** (Salva), quindi fare clic su **Apply** (Applica).



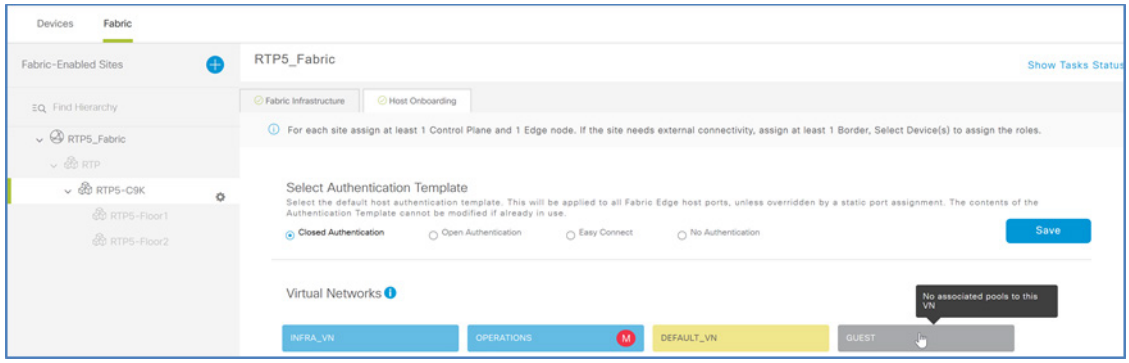
L'autenticazione chiusa è impostata come predefinita per le porte host e richiede l'autenticazione 802.1x per la connessione degli endpoint al fabric. Questa impostazione può essere sovrascritta dalla porta per altri scopi, ad esempio per le porte degli access point.

Passaggio 2. In **Virtual Networks** (Reti virtuali), selezionare una VN da utilizzare per i client cablati (ad esempio, OPERATIONS), nel riquadro a comparsa **Edit Virtual Network: *OPERATIONS*** (Modifica rete virtuale: OPERATIONS), selezionare i nomi di **IP Pools** (Pool di IP) da aggiungere alla VN (ad esempio, EMPLOYEE-DATA-RTP5), per **Traffic Type** (Tipo di traffico), selezionare **Data** (Dati), verificare che **Layer 2 Extension** (Estensione layer 2) sia **On** (Attivata). Se desiderato, modificare il nome per **Auth Policy** (Policy di autenticazione) adattandolo alla sede, fare clic su **Update** (Aggiorna), quindi fare clic su **Apply** (Applica).

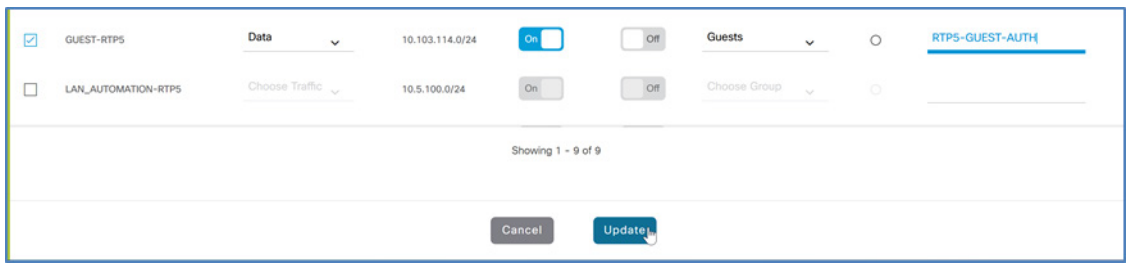


Viene visualizzato un messaggio di stato, quindi viene visualizzata la schermata **Host Onboarding** (Onboarding host).

Passaggio 3. Se è stata creata una rete virtuale guest, associare un pool di IP ai servizi guest. In **Virtual Networks** (Reti virtuali), selezionare una rete virtuale da utilizzare per i client wireless guest (ad esempio, GUEST).



Passaggio 4. Nel riquadro a comparsa **Edit Virtual Network: *GUEST*** (Modifica rete virtuale: GUEST), selezionare i nomi per **IP Pools** (Pool di IP) che si desidera aggiungere alla VN (ad esempio, EMPLOYEE-DATA-RTP5), per **Traffic Type** (Tipo di traffico), selezionare **Data** (Dati), verificare che **Layer 2 Extension** (Estensione layer 2) sia **On** (Attivata). Se desiderato, modificare il nome per **Auth Policy** (Policy di autenticazione) adattandolo alla sede, fare clic su **Update** (Aggiorna), quindi fare clic su **Apply** (Applica).



Viene visualizzato un messaggio di stato, quindi viene visualizzata la schermata **Host Onboarding** (Onboarding host).

Procedura 6. Abilitazione delle porte edge del fabric per l'onboarding dei client

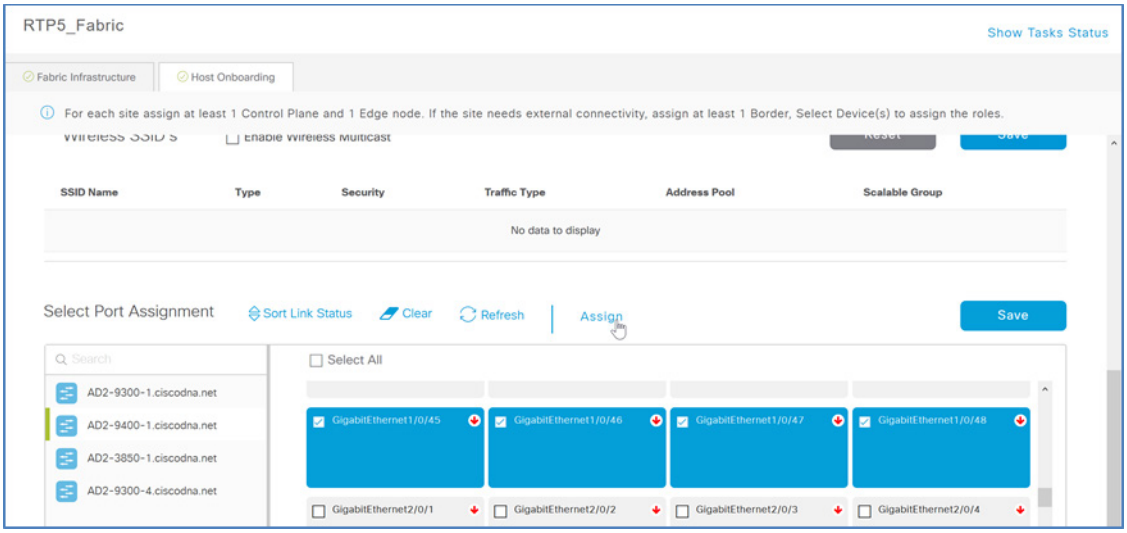
Facoltativo

Sovrascrivere il modello di autenticazione predefinito (autenticazione chiusa) assegnato nella procedura precedente quando i dispositivi connessi non supportano 802.1x o quando si utilizzano altri metodi di autenticazione, come l'autenticazione MAB per i dispositivi IOT, o quando si assegna manualmente un pool di indirizzi a una porta.

Ripetere questa procedura per ciascun edge switch del fabric con client che si connette alle porte edge del fabric e che richiede di sovrascrivere il modello di autenticazione predefinito.

Passaggio 1. Accedere a **PROVISION (Provisioning) > Fabric**, in **Fabrics** (Fabric), fare clic sulla sede del fabric creata (ad esempio, RTP5_Fabric). Nel riquadro di navigazione sinistro, fare clic sulla sede del fabric (ad esempio, RTP5-C9K), in alto sulla schermata fare clic sulla scheda **Host Onboarding** (Onboarding host) e nella sezione **Select Port Assignment** (Seleziona assegnazione porte), nella colonna di sinistra, selezionare uno switch.

Passaggio 2. Nell'elenco delle porte dello switch, selezionare un set di porte edge del fabric cablato da usare in una VN del fabric, quindi fare clic su **Assign** (Assegna).



Passaggio 3. Nel riquadro a comparsa, selezionare il valore appropriato per **Connected Device Type** (Tipo di dispositivo connesso) (ad esempio, User Devices (Dispositivi utente) (ip-phone, computer, laptop)), selezionare un valore per **Address Pool** (Pool di indirizzi) (ad esempio, 10_101_114_0(EMPLOYEE-DATA-RTP5)), **Group** (Gruppo) (ad esempio, Employees (Dipendenti)), **Voice Pool** (Pool voce) se necessario, selezionare un valore per **Auth Template** (Modello di autenticazione) (ad esempio, No Authentication (Nessuna autenticazione)), quindi fare clic su **Update** (Aggiorna).

Passaggio 4. A destra della sezione **Select Port Assignment** (Seleziona assegnazione porte), selezionare **Save** (Salva), confermare l'impostazione predefinita **Now** (Ora), quindi fare clic su **Apply** (Applica).

Passaggio 5. Ripetere i passaggi precedenti per gli altri switch aggiunti.

I dispositivi possono ora connettersi alle porte edge del fabric utilizzando l'overlay della rete cablata e il metodo di autenticazione creato.

Suggerimento tecnico
Se la porta edge del fabric non riceve l'assegnazione di un gruppo in modo dinamico con il server di autenticazione, è possibile effettuare l'assegnazione in modo statico. Questa procedura può essere utile per alcuni tipi di dispositivi usati in azienda. Se il metodo di autenticazione è " No Authentication" (Nessuna autenticazione), Cisco DNA Center applica il modello di autenticazione predefinito globale, selezionato nella sezione " Select Authentication template" (Seleziona modello di autenticazione) in alto sulla schermata. Cisco DNA Center applica una configurazione delle porte quando si seleziona " Closed Authentication" (Autenticazione chiusa) e " Open Authentication" (Autenticazione aperta).

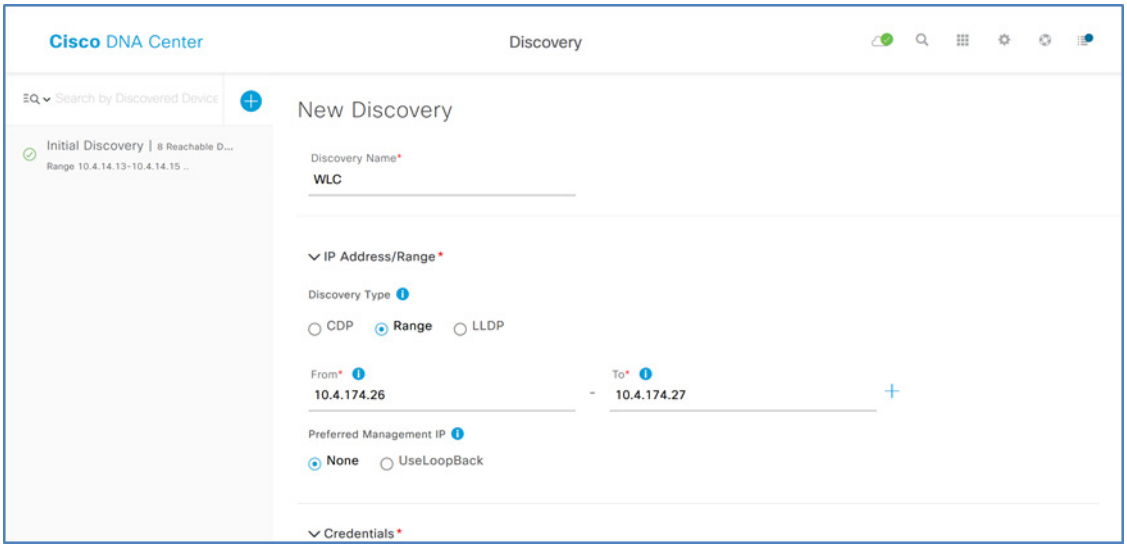
Procedura – Integrazione di SD-Access Wireless nel fabric

La procedura di installazione dei controller LAN wireless per SD-Access è descritta nella guida prescrittiva all'implementazione di Software-Defined Access for Distributed Campus. Questa procedura di integrazione wireless presume che i controller possano essere integrati nel fabric utilizzando Cisco DNA Center.

Procedura 1. Aggiungere i controller wireless all'inventario e creare una coppia SSO ad alta disponibilità

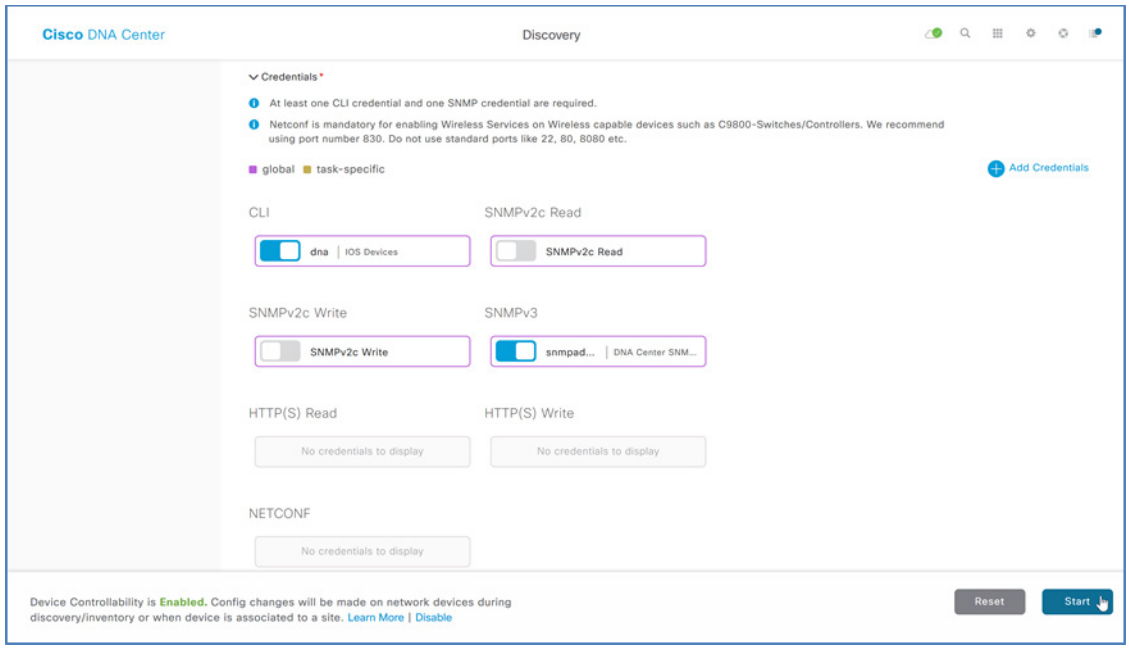
Se i controller LAN wireless non sono presenti nell'inventario di Cisco DNA Center, è necessario aggiungerli prima dell'integrazione wireless. Per la resilienza, è necessario utilizzare anche due WLC dello stesso tipo affinché la coppia SSO creata sia ad alta disponibilità.

Passaggio 1. Accedere alla dashboard principale di Cisco DNA Center, scorrere fino alla sezione **Tools** (Strumenti), fare clic su **Discovery** (Rilevamento) e fornire un valore per **Discovery Name** (Nome rilevamento). Selezionare **Range** (Intervallo) e immettere un indirizzo IP di loopback di inizio e uno di fine in **IP Ranges** (Intervalli IP) (per coprire un singolo indirizzo, immettere lo stesso indirizzo all'inizio e alla fine dell'intervallo). Per **Preferred Management IP** (IP di gestione preferito), selezionare **None** (Nessuno).

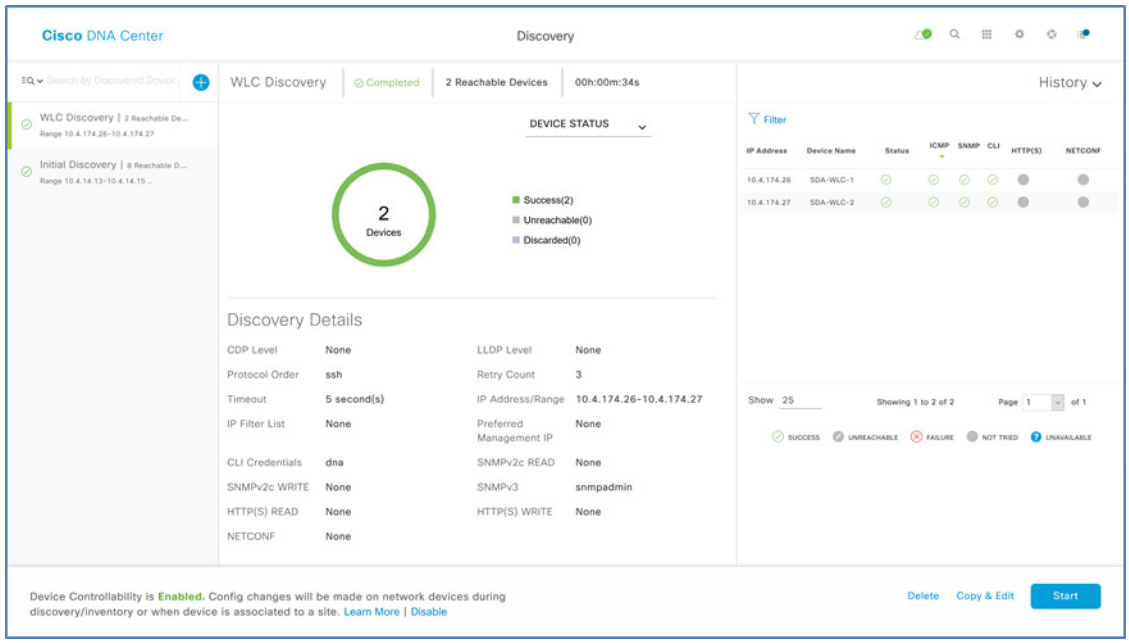


Passaggio 2. Se sono disponibili altri intervalli, accanto al primo intervallo fare clic su **+** (segno più), immettere l'intervallo aggiuntivo e ripetere l'operazione per gli intervalli rimanenti.

Passaggio 3. Scorrere verso il basso per verificare le credenziali CLI utilizzate per il rilevamento e le configurazioni delle credenziali SNMP applicate al dispositivo dalla funzione Device Controllability (Controllabilità dispositivi) di Cisco DNA Center. Se si dispone di credenziali univoche, specifiche per il rilevamento, fare clic su **+ Add Credentials** (+ Aggiungi credenziali), aggiungere ciascuna nuova credenziale, salvarle, quindi fare clic su **Start** (Avvia) in basso sulla schermata.



I dettagli di rilevamento vengono visualizzati durante l'esecuzione del processo.



Passaggio 4. Se sono presenti errori di rilevamento, controllare l'elenco dei dispositivi, risolvere il problema e riavviare il processo di rilevamento per i dispositivi in errore e per eventuali altri dispositivi che si desidera aggiungere all'inventario.

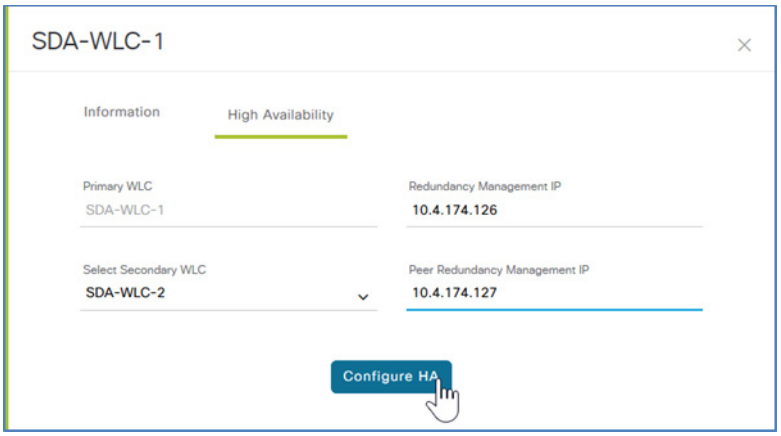
Passaggio 5. Dopo aver completato correttamente tutte le attività di rilevamento, andare alla dashboard principale di Cisco DNA Center, quindi, nella sezione **Tools** (Strumenti), fare clic su **Inventory** (Inventario). Vengono visualizzati i dispositivi rilevati. Dopo aver completato la raccolta dell'inventario, su ciascun dispositivo viene visualizzato lo stato di sincronizzazione **Managed** (Gestito) per segnalare che Cisco DNA Center conserva un modello interno che rispecchia l'implementazione fisica del dispositivo.

Cisco DNA Center può ora accedere ai dispositivi, sincronizzare l'inventario della configurazione e apportare modifiche alla configurazione dei dispositivi.

Suggerimento tecnico
Sulla riga del titolo della tabella dell'inventario, sul lato destro, è possibile scegliere quali colonne visualizzare. Utilizzare la colonna **Device Role** (Ruolo dispositivo) per visualizzare il ruolo assegnato dal processo di rilevamento in base al tipo di dispositivo e per modificarlo in modo che rappresenti il più fedelmente l'implementazione effettiva, scegliendo tra router di accesso, di distribuzione, core o di confine. In questa visualizzazione, il router di confine è un ruolo generico che non appartiene al fabric. La modifica del ruolo in questa fase, senza attendere le procedure successive, può migliorare l'aspetto delle mappe della topologia iniziale. Quando si assegna il ruolo core ai WLC, i controller si avvicinano di più alla loro posizione tipica.

Prima di continuare, utilizzare il pulsante **Refresh** (Aggiorna) finché il valore di **Last Inventory Collection Status** (Stato ultima raccolta inventario) non cambia in **Managed** (Gestito).

Passaggio 6. Se si crea una coppia SSO ad alta disponibilità con un gruppo di controller al momento non associati, accedere alla dashboard principale di Cisco DNA Center e selezionare **PROVISION (Provisioning) > Devices (Dispositivi) > Inventory (Inventario)**. Fare clic sul testo di **Device Name** (Nome dispositivo) del WLC principale (ad esempio, SDA-WLC1). In alto a destra sulla finestra popup, selezionare **High Availability** (Alta disponibilità), in **Select Secondary WLC** (Seleziona WLC secondario), selezionare il secondo WLC della coppia SSO ad alta disponibilità (ad esempio, SDA-WLC-2), fornire i valori per **Redundancy Management IP** (IP di gestione ridondanza) e **Peer Redundancy Management IP** (IP di gestione ridondanza peer) (ad esempio, 10.4.174.126, 10.4.174.127), fare clic su **Configure HA** (Configura alta disponibilità), quindi nella schermata di richiesta di riavvio, fare clic su **OK**.



Sul browser vengono visualizzati dei messaggi di avviso.

```
Configuring HA for Primary. Please do not Refresh the page..
Configuring HA for Secondary...
```

I processi di riconfigurazione e riavvio possono impiegare diversi minuti.

Passaggio 7. Per aggiornare la schermata fino a visualizzare i WLC in modalità HA come un unico dispositivo, utilizzare il pulsante Refresh (Aggiorna). Controllare lo stato HA facendo clic sul testo di **Device Name** (Nome dispositivo) del WLC principale (nell'esempio, SDA-WLC1), sul lato destro della finestra popup selezionare **High Availability** (Alta disponibilità), quindi verificare che **Redundancy State** (Stato ridondanza) sia **SSO** e che **Sync Status** (Stato sincronizzazione) sia **Complete** (Completato).

Procedere al passaggio successivo dopo aver completato la configurazione HA.

Passaggio 8. Andare alla dashboard principale di Cisco DNA Center, quindi accedere a **DESIGN (Progettazione) > Image Repository (Archivio immagini)**. Individuare la famiglia di dispositivi e verificare la versione del software. Se l'immagine WLC è della versione corretta, continuare. Se l'immagine è presente nell'elenco ma deve essere aggiornata, fare clic sulla stella accanto all'immagine per contrassegnarla come preferita, quindi aggiornare il software. Per usare un'immagine non inclusa nell'elenco, fare clic su Import Image/SMU (Importa immagine/SMU), seguire le istruzioni per effettuare l'importazione, aggiornare la schermata, quindi utilizzare l'elenco a discesa del dispositivo per contrassegnare l'immagine come preferita.

Passaggio 9. Se si sta aggiornando il dispositivo, accedere a **PROVISION (Provisioning) > Devices (Dispositivi) > Inventory (Inventario)**, selezionare il WLC contrassegnato come **Outdated** (Obsoleto), quindi dal menu **Actions** (Azioni), fare clic su **Update OS Image** (Aggiorna immagine del sistema operativo). Confermare la scelta del dispositivo da aggiornare, per **When** (Quando), utilizzare l'impostazione predefinita **Now** (Ora), fare clic su **Apply** (Applica), quindi sulla schermata di avviso del riavvio, fare clic su **OK**.

Le immagini vengono distribuite al dispositivo selezionato, quindi al termine del processo di distribuzione, il dispositivo viene riavviato per attivare immediatamente la nuova immagine. Utilizzare il pulsante **Refresh** (Aggiorna) finché lo stato di **In Progress** (In corso) non scompare.

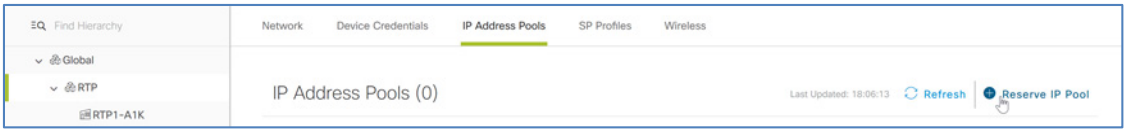
Procedura 2. Creazione di pool di indirizzi IP per gli access point

Verificare che Cisco DNA Center abbia un pool globale per l'assegnazione degli indirizzi in modo che la rete possa gestire gli access point.

Passaggio 1. Accedere a **DESIGN (Progettazione) > Network Settings (Impostazioni di rete) > IP Address Pools (Pool di indirizzi IP)**. Nella gerarchia delle sedi a sinistra, selezionare **Global** (Globale), quindi nell'elenco dei pool di indirizzi IP individuare un pool dedicato all'infrastruttura di access point (ad esempio, ACCESS_POINT).

Passaggio 2. Se non è presente alcun pool dedicato per gli access point, fare clic su **+ Add IP Pool** (+ Aggiungi pool di IP), fornire i valori per **IP Pool Name** (Nome pool IP), **IP Subnet** (Subnet IP), **CIDR Prefix** (Prefisso CIDR) e **Gateway IP address** (Indirizzo IP gateway) (ad esempio, ACCESS_POINT, 172.16.173.0, /24, 172.16.173.1), selezionare **DHCP Server** (Server DHCP) e **DNS Server** (Server DNS), quindi fare clic su **Save** (Salva).

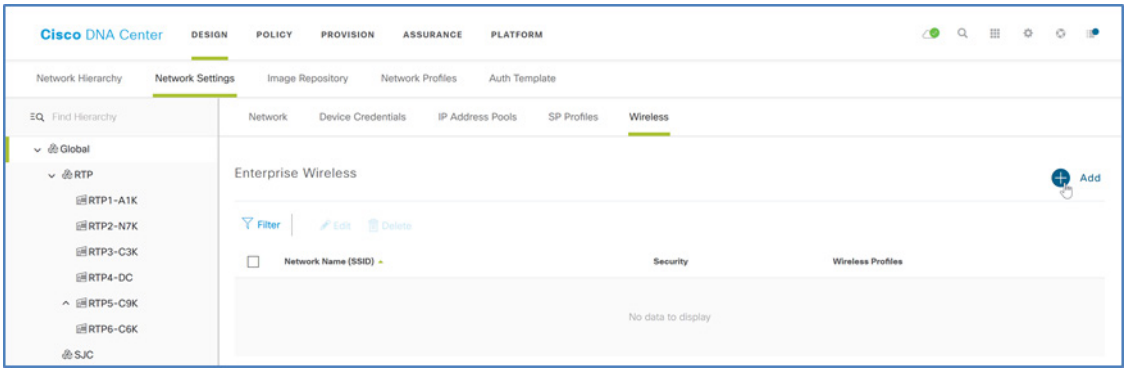
Passaggio 3. Accedere a **DESIGN (Progettazione) > Network Settings (Impostazioni di rete) > IP Address Pools (Pool di indirizzi IP)**, sulla gerarchia delle sedi, a sinistra, selezionare una sede o un livello inferiore per prenotare un pool di indirizzi IP (ad esempio, RTP5-C9K). Se il pool non è ancora stato prenotato, fare clic in alto a destra su Reserve IP Pool (Prenota pool di IP).



Passaggio 4. Se si sta prenotando un pool, fornire un valore per **IP Pool Name** (Nome pool di IP) (ad esempio, ACCESS_POINT-RTP5), in **Type** (Tipo) selezionare **LAN**, selezionare l'origine **Global IP Pool** (Pool di IP globale) per la prenotazione. In **CIDR Notation / No. of IP Addresses** (Notazione CIDR / N. di indirizzi IP), selezionare la parte dello spazio degli indirizzi da utilizzare, assegnare un **Gateway IP Address** (Indirizzo IP gateway), **DHCP Server(s)** (Server DHCP) e **DNS Servers(s)** (Server DNS), quindi fare clic su **Reserve** (Prenota).

Procedura 3. Progettazione degli SSID wireless aziendali del fabric

Passaggio 1. Dalla dashboard principale di Cisco DNA Center, accedere a **DESIGN (Progettazione) > Network Settings (Impostazioni di rete) > Wireless**, nel riquadro della gerarchia a sinistra, selezionare il livello **Global** (Globale), quindi nella sezione **Enterprise Wireless** (Wireless aziendale), fare clic su **+ Add** (+ Aggiungi).



Viene visualizzata la procedura guidata **Create an Enterprise Wireless Network** (Creazione di una rete aziendale wireless).

Passaggio 2. Per la procedura guidata **Create an Enterprise Wireless Network** (Creazione di una rete aziendale wireless) è necessario fornire le seguenti informazioni:

- Immettere un valore per **Wireless Network Name(SSID)** (Nome della rete wireless (SSID)) (ad esempio, Employee)
- In **TYPE OF ENTERPRISE NETWORK** (Tipo di rete aziendale), selezionare Voice and Data (Voce e dati) e Fast Lane
- Selezionare o confermare **WIRELESS OPTION** (Opzione wireless)
- Per **LEVEL OF SECURITY** (Livello di sicurezza), selezionare un'opzione (ad esempio, WPA2 Enterprise)
- In **ADVANCED SECURITY OPTIONS** (Opzioni di sicurezza avanzate), selezionare Adaptive (Adattabile)

Passaggio 3. Fare clic su **Next** (Avanti) per proseguire la procedura guidata e fornire le seguenti informazioni:

- Immettere un valore per **Wireless Profile Name** (Nome del profilo wireless) (ad esempio, RTP5-Wireless)
- In **Fabric**, selezionare **Yes** (Sì)
- In **Choose a site** (Seleziona una sede), selezionare la posizione in cui verranno trasmessi gli SSID (ad esempio, Global (Globale)/RTP/RTP5-C9K), quindi specificare i piani da includere nella copertura SSID (ad esempio, Global (Globale)/RTP/RTP5-C9K/Floor 1 (Piano 1))

Passaggio 4. Fare clic su **Finish** (Fine) per continuare. Viene visualizzata la schermata **DESIGN (Progettazione) > Network Settings (Impostazioni di rete) > Wireless**.

Passaggio 5. Ripetere questa procedura per gli altri SSID utilizzando lo stesso profilo di rete e tutti i nuovi profili di posizione da associare a un SSID.

Procedura 4. Progettazione di un SSID per il wireless guest del fabric

Passaggio 1. Accedere a **DESIGN (Progettazione) > Network Settings (Impostazioni di rete) > Wireless**, nella sezione **Guest Wireless** (Wireless guest) fare clic su **+ Add** (+ Aggiungi), quindi nella procedura guidata **Create a Guest Wireless Network** (Creazione di una rete wireless guest) fornire le seguenti informazioni:

- Immettere un valore per **Wireless Network Name(SSID)** (Nome della rete wireless (SSID)) (ad esempio, Guest)
- In **LEVEL OF SECURITY** (Livello di sicurezza), selezionare Web Auth (Autenticazione Web)
- In **AUTHENTICATION SERVER** (Server di autenticazione), selezionare ISE Authentication (Autenticazione ISE)

Confermare le altre impostazioni predefinite e fare clic su **Next** (Avanti) per proseguire la procedura guidata.

Passaggio 2. In **Wireless Profiles** (Profili wireless), selezionare per **Profile Name** il nome del profilo corrispondente alla posizione di implementazione (ad esempio, RTP5-Wireless). Nel riquadro a comparsa, per **Fabric** confermare l'impostazione predefinita **Yes** (Sì), confermare le altre impostazioni predefinite, in basso sulla schermata fare clic su **Save** (Salva), quindi fare clic su **Next** (Avanti).

Passaggio 3. Nella fase **Portal Customization** (Personalizzazione del portale), fare clic su **+ Add** (+ Aggiungi). Viene visualizzata la schermata **Portal Builder**.

Passaggio 4. Fornire un nome per **Guest Portal** (Portale guest) (ad esempio, Guest-RTP5), apportare le modifiche personalizzate desiderate, quindi in basso sulla schermata fare clic su **Save** (Salva). Viene generato un portale di autenticazione Web guest per la sede, quindi viene nuovamente visualizzata la schermata precedente.

Passaggio 5. Fare clic su **Finish** (Fine).

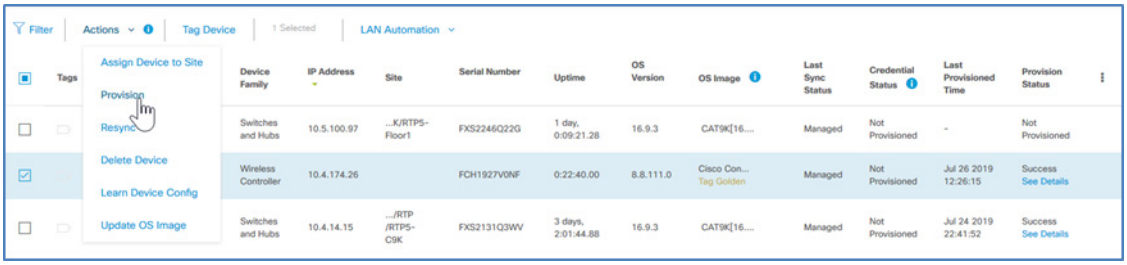
La progettazione della LAN wireless viene creata ed è pronta per essere implementata.

Procedura 5. Provisioning dei WLC per l'integrazione del fabric di SD-Access Wireless

Dopo aver completato la progettazione di SD-Access Wireless, forzare la configurazione dall'applicazione di progettazione al WLC.

Passaggio 1. Accedere a PROVISION (Provisioning) > Devices (Dispositivi) > Inventory (Inventario), trovare il WLC e selezionare la casella di controllo accanto, quindi in alto sulla schermata, dal menu a discesa Actions (Azioni), selezionare Provision (Effettua il provisioning). Viene visualizzata la procedura guidata per il provisioning dei dispositivi.

Suggerimento tecnico
Quando si configura una coppia di WLC in modalità SSO ad alta disponibilità, nell'inventario di Cisco DNA Center viene visualizzato un unico WLC. Per verificare che sia stata configurata una coppia SSO ad alta disponibilità, fare clic sul nome del dispositivo, quindi fare clic sulla scheda **High Availability** (Alta disponibilità).



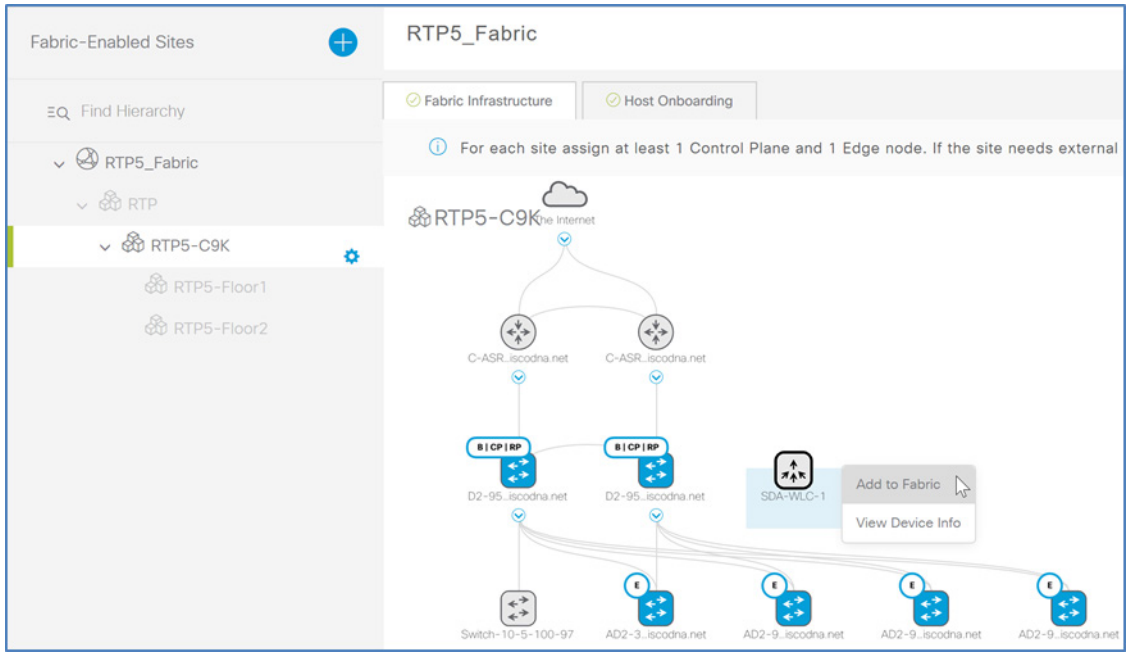
Passaggio 2. Assegnare la sede (ad esempio, Global (Globale)/RTP/RTP5-C9K), fare clic su **Next** (Avanti), nella fase **Configuration** (Configurazione) in **Managed AP Location** (Posizione AP gestito), selezionare le assegnazioni degli altri piani per gli access point gestiti dal WLC (ad esempio, Global (Globale)/RTP/RTP5-C9K/Floor 1 (Piano 1)), fare clic su **Next** (Avanti), quindi nella fase **Advanced Configuration** (Configurazione avanzata), fare clic su **Next** (Avanti).

Passaggio 3. In **Summary** (Riepilogo), riesaminare le configurazioni, fare clic su **Deploy** (Implementa), sul riquadro a comparsa, confermare l'impostazione predefinita **Now** (Ora), quindi fare clic su **Apply** (Applica).

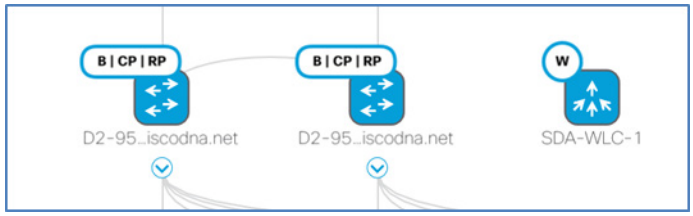
Il WLC viene assegnato alla sede e il processo di provisioning ha inizio. Utilizzare il pulsante **Refresh** (Aggiorna) finché per **Provision Status** (Stato provisioning) non viene mostrato **Success** (Completato) prima di procedere.

Procedura 6. Provisioning di SD-Access Wireless nel fabric

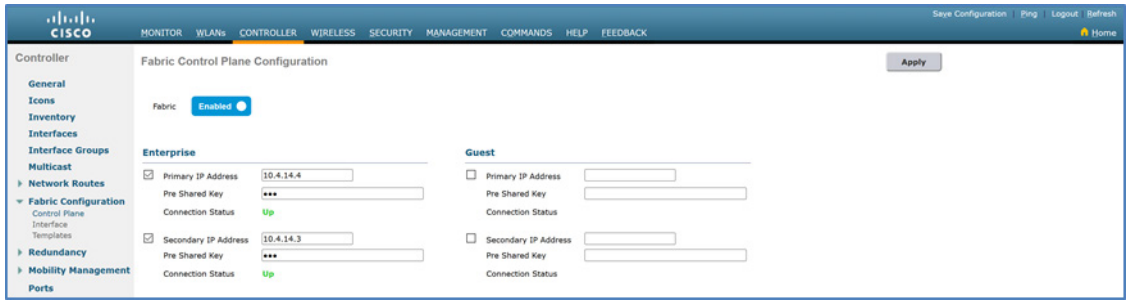
Passaggio 1. Dalla dashboard di Cisco DNA Center, accedere a **PROVISION (Provisioning) > Fabric**, in **Fabric** fare clic sulla sede del fabric creata (ad esempio, RTP5_Fabric). Nel riquadro di navigazione a sinistra, **Fabric-Enabled Sites** (Sedi basate sul fabric), fare clic sulla sede associata (ad esempio, Global (Globale)/RTP/RTP5-C9K), fare clic sul WLC, quindi nella finestra popup fare clic su **Add to Fabric** (Aggiungi al fabric).



Passaggio 2. Nella parte inferiore della schermata, fare clic su **Save** (Salva), nel menu a comparsa confermare l'impostazione predefinita **Now** (Ora) e fare clic su **Apply** (Applica). Vengono create le configurazioni WLC per stabilire una connessione sicura con il piano di controllo del fabric.



Per verificare che la coppia di controller WLC sia integrata nel fabric, dalla console di gestione del WLC accedere a **CONTROLLER > Fabric Configuration (Configurazione del fabric) > Control Plane (Piano di controllo)**. Qui è possibile verificare se l'integrazione del fabric è abilitata e lo stato di connessione è attivo.



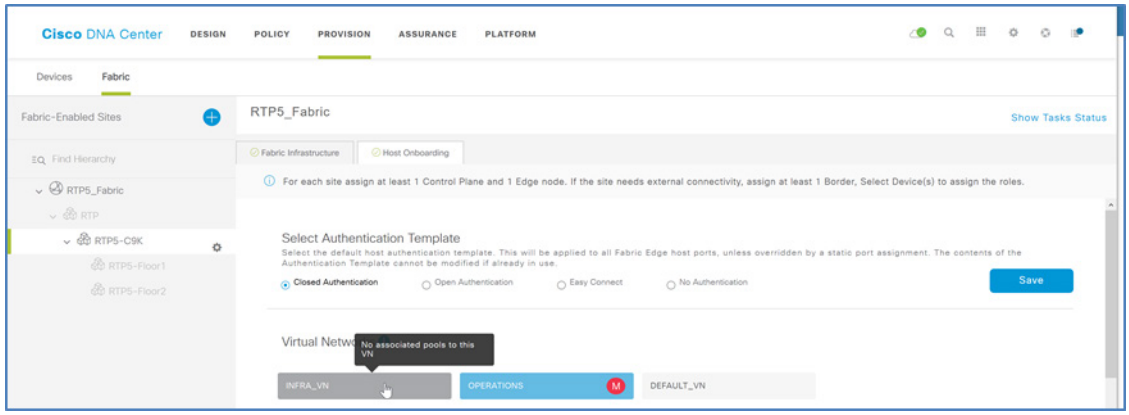
Procedura 7. Abilitazione dell'onboarding degli access point nel fabric wireless

Gli access point sono host che partecipano al fabric e sono assegnati a una rete virtuale chiamata INFRA_VN. Questa rete virtuale speciale per dispositivi dell'infrastruttura quali gli access point permette la comunicazione di gestione tra gli access point sui nodi edge del fabric utilizzando il piano di controllo del fabric e il WLC che si trovano all'esterno del fabric come parte di una connettività di routing globale.

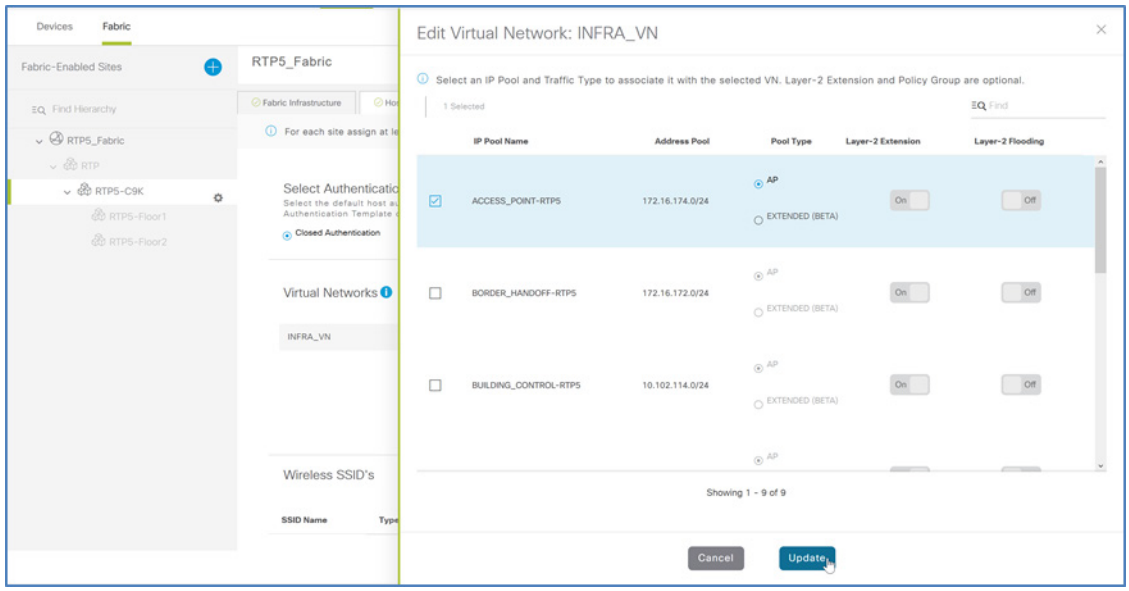
Passaggio 1. Collegare gli access point da utilizzare per il fabric direttamente al nodo edge all'interno del fabric.

Passaggio 2. Dalla dashboard Cisco DNA Center, accedere a **PROVISION (Provisioning) > Fabric**, in **Fabric Domains** (Domini del fabric), fare clic sulla sede del fabric creata (ad esempio, RTP5_Fabric), sul riquadro di navigazione in **Fabric-Enabled Sites** (Sedi basate sul fabric), fare clic sulla sede associata (ad esempio, Global (Globale)/RTP/RTP5-C9K), quindi fare clic su **Host Onboarding** (Onboarding host).

Passaggio 3. In **Virtual Networks** (Reti virtuali), selezionare **INFRA_VN**.

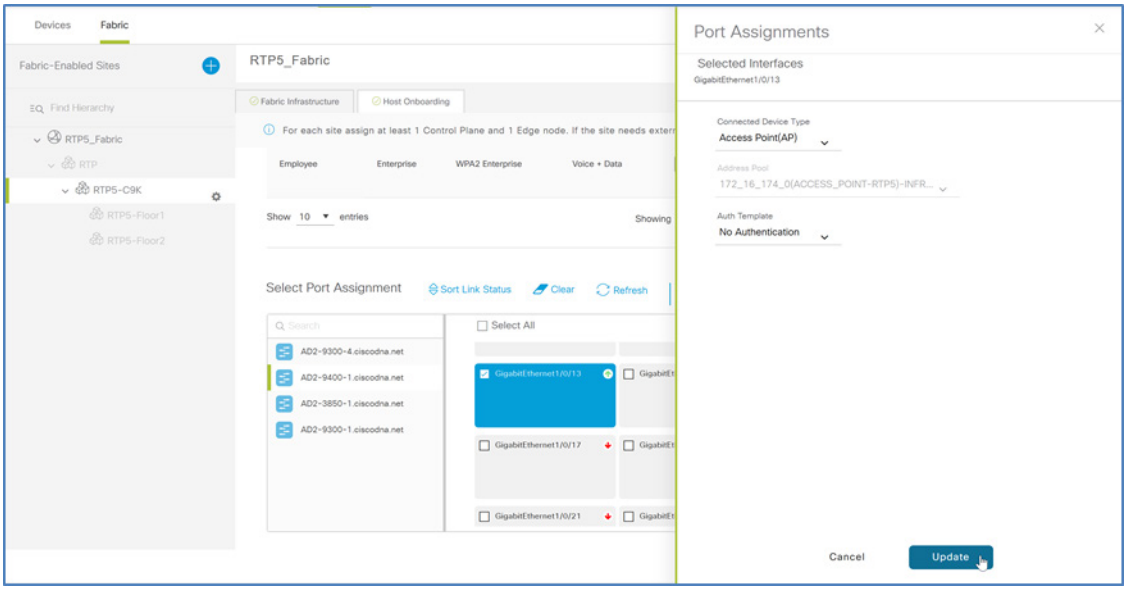


Passaggio 4. Selezionare la casella di controllo accanto al nome del pool di IP degli access point (ad esempio, ACCESS_POINT-RTP5), in **Pool Type** (Tipo di pool), selezionare **AP**, quindi fare clic su **Update** (Aggiorna).



Passaggio 5. Nel riquadro a comparsa Modify Virtual Network (Modifica rete virtuale), confermare l'impostazione predefinita **Now** (Ora), quindi fare clic su **Apply** (Applica).

Passaggio 6. In **Select Port Assignment** (Seleziona assegnazione porte), selezionare le porte degli switch da dedicare agli access point, selezionare **Assign** (Assegna). Nel riquadro a comparsa **Port Assignments** (Assegnazioni porte), in **Connected Device Type** (Tipo di dispositivo connesso), selezionare **Access Point (AP)**, confermare l'impostazione predefinita **Address Pool** (Pool di indirizzi). In **Auth Template** (Modello di autenticazione), selezionare **No Authentication** (Nessuna autenticazione), quindi fare clic su **Update** (Aggiorna).



Suggerimento tecnico

Cisco DNA Center consente l'onboarding automatico degli access point mediante il provisioning di una macro CDP negli edge switch del fabric quando il modello di autenticazione è impostato su **No Authentication** (Nessuna autenticazione). In alternativa, utilizzare le configurazioni delle porte dello switch in Cisco DNA Center per assegnare una porta al pool di indirizzi IP per gli access point.

Passaggio 7. Ripetere il passaggio precedente per eventuali switch aggiuntivi con porte dedicate agli access point.

Passaggio 8. Dopo aver selezionato tutte le porte che supportano gli access point, in alto sulla sezione **Select Port Assignment** (Seleziona assegnazione porte), fare clic su **Save** (Salva), confermare l'impostazione predefinita **Now** (Ora), quindi fare clic su **Apply** (Applica).

Al termine dell'aggiornamento, le porte dello switch del nodo edge connesse agli access point vengono abilitate con una configurazione di monitoraggio dei dispositivi che riconosce gli access point e consente loro di connettersi alla rete.

Suggerimento tecnico

Le API non possono utilizzare una route predefinita dell'underlay per contattare il WLC. Nella tabella di routing globale deve essere presente una route più specifica, ad esempio una route di subnet /24 o host /32, agli indirizzi IP dei WLC su ciascun nodo raggiunto dalle API per stabilire la connettività. Ridistribuire la route del WLC sul confine nel processo di routing IGP dell'underlay per una maggiore efficienza. In alternativa, è possibile creare voci statiche su ciascun nodo edge che supporti gli access point.

Passaggio 9. Accedere alla dashboard principale di Cisco DNA Center, in **PROVISION (Provisioning) > Devices (Dispositivi) > Inventory (Inventario)**, quindi in alto sulla schermata, dal menu a discesa **Actions** (Azioni), selezionare **Resync** (Risincronizza). Gli access point associati al WLC vengono aggiunti all'inventario senza attenderne l'aggiornamento.

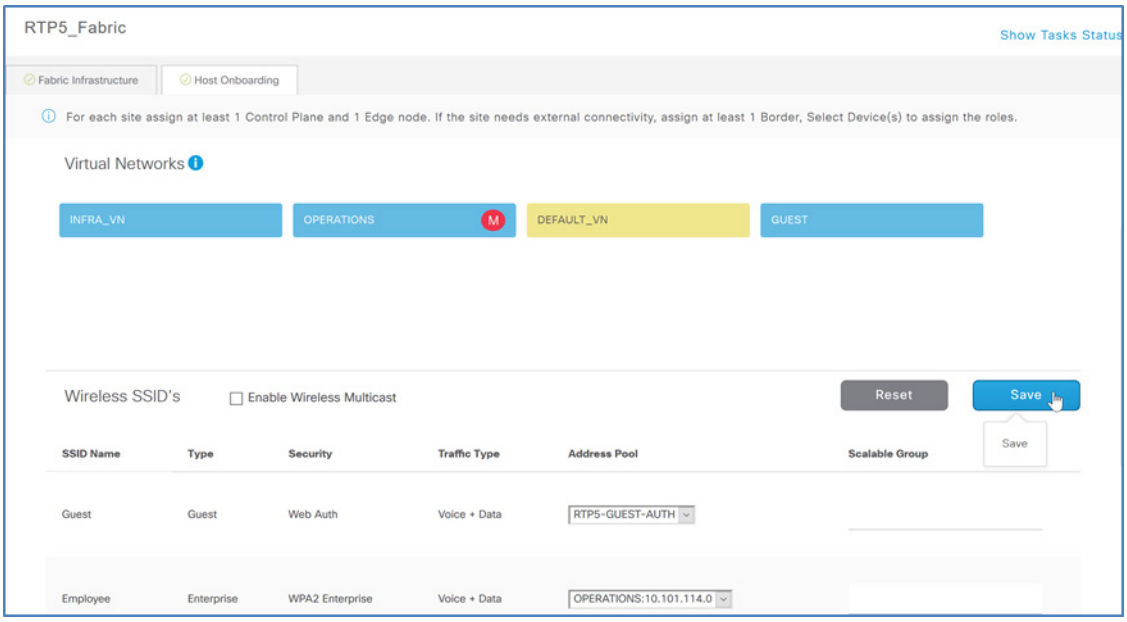
Passaggio 10. Accedere alla dashboard principale di Cisco DNA Center, in **PROVISION (Provisioning) > Devices (Dispositivi) > Inventory (Inventario)** selezionare gli access point da aggiungere, quindi in alto sulla schermata, dal menu a discesa **Actions** (Azioni), selezionare **Provision** (Effettua il provisioning).

Passaggio 11. Sulla schermata **Provision Devices** (Effettua il provisioning dei dispositivi), assegnare gli access point a un piano (ad esempio, Global (Globale)/RTP/RTP5-C9K/ Floor 1 (Piano 1)), fare clic su **Next** (Avanti). In **RF Profile** (Profilo RF), se non ne è stato creato uno personalizzato, selezionare **TYPICAL**, fare clic su **Next** (Avanti), sulla pagina **Summary** (Riepilogo), fare clic su **Deploy** (Implementa) e nel riquadro a comparsa, confermare l'impostazione predefinita **Now** (Ora), quindi fare clic su **Apply** (Applica). Confermare eventuali avvisi di riavvio.

Procedura 8. Assegnazione di client wireless alla rete virtuale e abilitazione della connettività

Passaggio 1. Dalla dashboard di Cisco DNA Center, accedere a **PROVISION (Provisioning) > Fabric**, in **Fabric Domains** (Domini del fabric) fare clic sulla sede del fabric creata (ad esempio, RTP5_Fabric). Nel riquadro di navigazione a sinistra **Fabric-Enabled Sites** (Sedi basate sul fabric), fare clic sulla sede associata (ad esempio, Global (Globale)/RTP/RTP5-C9K), quindi fare clic sulla scheda **Host Onboarding** (Onboarding host).

Passaggio 2. Nella sezione **Wireless SSID's** (SSID wireless), per ciascun **SSID Name** (Nome SSID), selezionare un **pool di indirizzi** associato, selezionare eventuali gruppi scalabili associati in **Scalable Group** (Gruppo scalabile), fare clic su **Save** (Salva), confermare l'impostazione predefinita **Now** (Ora), quindi fare clic su **Apply** (Applica).



I dispositivi possono ora connettersi tramite le reti wireless.

Appendice A – Elenco dei prodotti

I seguenti prodotti e versioni software sono stati inclusi come parte del processo di convalida di questa guida, ma non devono essere considerati esaustivi. Le opzioni hardware aggiuntive sono elencate nella guida alla progettazione della soluzione Software-Defined Access, nella matrice di compatibilità dei prodotti SD-Access; nelle schede tecniche di Cisco DNA Center potrebbero esserci linee guida che non sono state collaudate per la redazione di questa guida. I file di pacchetti Cisco DNA Center aggiornati vengono rilasciati regolarmente e sono disponibili negli elenchi dei pacchetti e degli aggiornamenti.

Tabella 3. Cisco DNA Center

Prodotto	Codice prodotto	Versione del software
Appliance di Cisco DNA Center	DN2-HW-APL-L (Chassis basato su M5)	1.2.10.4 (Sistema 1.1.0.754)

Tabella 4. Pacchetti di Cisco DNA Center

Sono elencati tutti i pacchetti in esecuzione su Cisco DNA Center durante la convalida; non tutti i pacchetti sono inclusi nei test di convalida di SD-Access.

Pacchetto	Versione
Application Policy	2.1.28.170011
Assurance - Base	1.2.11.304
Assurance – Sensor	1. 2.10.254
Automation – Base	2.1.28.600244.9
Automation – Intelligent Capture	2.1.28.60244
Automation – Sensor	2.1.28.60244
Cisco DNA Center UI	1.2.11.19
Command Runner	2.1. 28.60244
Device Onboarding	2.1.18.60024
DNAC Platform	1.0.8.8
Image Management	2.1.28.60244
NCP – Base	2.1.28.60244
NCP – Services	2.1.28.60244.9
Network Controller Platform	2.1.28.60244.9
Network Data Platform – Base Analytics	1.1.11.8
Network Data Platform – Core	1.1.11.77
Network Data Platform – Manager	1.1.11.8

Pacchetto	Versione
Path Trace	2.1.28.60244
SD-Access	2.1.28.60244.9

Tabella 5. Gestione delle identità

Area funzionale	Prodotto	Versione del software
Server Cisco ISE	Cisco Identity Services Engine	2.4 Patch 6

Tabella 6. Confine e piano di controllo del fabric di SD-Access

Area funzionale	Prodotto	Versione del software
Confine e piano di controllo	Switch Cisco Catalyst serie 9500	16.9.3
Confine e piano di controllo	Switch Cisco Catalyst serie 9400	16.9.3
Confine e piano di controllo: sede piccola	Cisco Catalyst 3850 XS Switch (fibra ottica da 10 Gbps)	16.9.3
Confine e piano di controllo	Cisco serie 4000 Integrated Services Router	16.9.2
Confine e piano di controllo: larga scala	Cisco ASR serie 1000-X e 1000-HX Aggregation Services Router	16.9.2
Border	Chassis di Cisco Catalyst 6807 a 7 slot con Supervisor Engine 6T o Supervisor Engine 2T e 6800 a 32 porte da 10 GE con doppia DFC4 integrata	15.5 (1) SY2
Confine	Cisco Catalyst serie 6880-X e 6840-X Switch	15.5(1)SY2
Confine esterno	Chassis di Cisco Nexus 7700 Switch a 2 slot con modulo Supervisor 2 Enhanced e Cisco Nexus 7700 serie M3 a 48 porte da 1/10 Gigabit Ethernet	8.3(2)
Piano di controllo	Cisco Cloud Services Router serie 1000V	16.9.2

Tabella 7. Edge del fabric di SD-Access

Area funzionale	Prodotto	Versione del software
Edge del fabric	Cisco Catalyst serie 9300 – impilabile	16.9.3
Edge del fabric	Cisco Catalyst serie 9400 con Supervisor Engine-1 - chassis modulare	16.9.3

Area funzionale	Prodotto	Versione del software
Edge del fabric	Cisco Catalyst serie 3850 – impilabile	16.9.3
Edge del fabric	Cisco Catalyst serie 3650 – standalone con opzione impilabile	16.9.3
Edge del fabric	Cisco Catalyst serie 4500E con Supervisor 8-E – chassis modulare	3.10.2E

Tabella 8. SD-Access Wireless

Area funzionale	Prodotto	Versione del software
Wireless LAN Controller	Cisco serie 8540, 5520 e 3504 Wireless Controller	8.8.111.0 (8.8 MR1)
Access point in modalità fabric	Cisco Aironet® serie 1800, 2800 e 3800 (Wave 2)	8.8.111.0 (8.8 MR1)

Tabella 9. Switch di automazione LAN testati per questa guida (non include tutte le possibilità)

Area funzionale	Prodotto
Cisco Catalyst serie 9500 (prestazioni standard)	Dispositivo seed
Cisco Catalyst switch 3850 XS (10 Gbps in fibra)	Dispositivo seed
Cisco Catalyst serie 9300 – impilabile	Dispositivo seed / Dispositivo rilevato
Cisco Catalyst serie 9400 con Supervisor Engine-1 – chassis modulare	Dispositivo seed / Dispositivo rilevato (Interfaccia da 10 Gbps)
Cisco Catalyst serie 3850 – impilabile	Dispositivo rilevato
Cisco Catalyst serie 3650 – standalone con opzione impilabile	Dispositivo rilevato
Cisco Catalyst serie 4500E con Supervisor 8-E – chassis modulare	Dispositivo rilevato

Feedback

Per commenti e suggerimenti su questa guida e le guide correlate, partecipa ai dibattiti della Cisco Community all'indirizzo https://cs.co/en-cvds.

Sede centrale Americhe
Cisco Systems Inc.
San Jose. CA (USA)

Sede centrale Asia e Pacifico
Cisco Systems (USA) Pte. Ltd.
Singapore

Sede centrale Europa
Cisco Systems International BV Amsterdam,
Paesi Bassi

Le sedi Cisco nel mondo sono oltre 200. Gli indirizzi, i numeri di telefono e di fax sono disponibili sul sito web Cisco all'indirizzo **www.cisco.com/go/offices**.