

Guida alle best practice per il provisioning SDA (Software Defined Access)

Sommario

[Introduzione](#)

[1. Provisioning dei dispositivi:](#)

[2. Aggiunta/rimozione/modifica provisioning dispositivi fabric SDA](#)

[3. Rete virtuale - provisioning pool IP](#)

[4. Caricamento host - Assegnazione porta](#)

[5. Automazione LAN](#)

Introduzione

In questo articolo vengono elencati i vari controlli preliminari, dos e dont che l'utente può seguire per evitare le insidie durante il provisioning del fabric SDA (Software Defined Access) tramite Cisco DNA Center. Di seguito sono elencati i casi di utilizzo del provisioning e l'elenco di controllo.

1. Provisioning dei dispositivi:

1. Verificare che il dispositivo sia raggiungibile e in stato gestito nell'applicazione di inventario Cisco DNA Center.
2. Controllare la pagina di progettazione della rete e assicurarsi che le impostazioni a livello di sito corrispondenti (credenziali, server AAA) siano mantenute.
3. Verificare se sono in corso operazioni di provisioning a livello di infrastruttura nel sito di infrastruttura a cui è collegato il dispositivo.
4. Verificare che l'integrazione Cisco ISE (Identity Service Engine) sia attiva e che sia stato creato un dispositivo NAD (Network Access Device) per questo dispositivo in Identity Services Engine (ISE).
5. Verificare che lo stato di provisioning non sia "Configurazione in corso".
6. Se si desidera modificare l'indirizzo IP di gestione del dispositivo, modificarlo innanzitutto nella pagina Inventario di Cisco DNA Center. Quindi, modificarlo sul dispositivo. Per evitare conflitti di indirizzi IP, risincronizzare la pagina Inventario (**Inventario > Risincronizza dispositivo**).
7. Verificare che i dispositivi nell'infrastruttura non inviino trap, ad esempio LINK_UP o LINK_DOWN.
8. Prima di eseguire qualsiasi operazione di provisioning o fabric, esaminare i limiti di scala nel [foglio dati di Cisco DNA Center](#).

2. Aggiunta/rimozione/modifica provisioning dispositivi fabric SDA

1. Verificare che il dispositivo da aggiungere/rimuovere sia raggiungibile e in stato gestito

nell'app di inventario di Cisco DNA Center.

2. Prima di rimuovere il dispositivo dall'infrastruttura, verificare che faccia ancora parte della rete.
3. Verificare se sono in corso operazioni di provisioning a livello di infrastruttura nel sito di infrastruttura a cui è collegato il dispositivo.
4. In caso di rimozione e sostituzione di dispositivi border/control plane, assicurarsi che tutti i dispositivi edge siano raggiungibili e gestiti nell'applicazione di inventario di DNA Center.
5. Se in alcuni dispositivi si verificano errori di provisioning a livello di fabric precedenti, eseguire nuovamente il provisioning di tali dispositivi in modo che la configurazione più recente del fabric venga inviata a tutti i dispositivi.
6. Non provare a rimuovere il dispositivo dall'app di inventario di Cisco DNA Center finché il dispositivo non viene rimosso dall'infrastruttura. Non utilizzare l'API di inventario per rimuovere il dispositivo dall'inventario. Le API di inventario non eliminano i dati del fabric dallo switch né quelli del database (DataBase) di Cisco DNA Center.
7. Dalla versione 1.3.3.x, Cisco DNA Center non supporta RMA (Return Merchandise Authorization) per dispositivi fabric. Il modo migliore per eseguire RMA su un bordo o un nodo ai margini consiste nel rimuoverlo dalla struttura e utilizzare il flusso di lavoro RMA per sostituire il dispositivo e aggiungerlo nuovamente alla struttura.
8. Non includere dispositivi non raggiungibili come parte della struttura.
9. Prima di aggiungere un dispositivo all'infrastruttura, verificare che il dispositivo o l'interfaccia non disponga di una configurazione relativa all'infrastruttura, inclusa una configurazione della porta dello switch.
10. Cancellare la configurazione del dispositivo manualmente prima di aggiungerlo all'infrastruttura. Se si rimuove un dispositivo non raggiungibile dalla struttura, la configurazione viene mantenuta nel dispositivo.
11. Verificare che le configurazioni dei modelli definite dall'utente non interferiscano con la configurazione dell'infrastruttura.
12. La rimozione di un dispositivo dall'inventario non cancella alcuna configurazione di cui è stato eseguito il provisioning tramite un modello.
13. Per evitare la latenza o gli errori di provisioning, non utilizzare una configurazione di autorizzazione a livello di comando nei dispositivi fabric in un ambiente scalato.
14. Non eseguire di nuovo il provisioning di un dispositivo mentre è in corso un'operazione di provisioning a livello di struttura.
15. Non configurare alcuna configurazione manuale relativa all'infrastruttura su un dispositivo.

3. Rete virtuale - provisioning pool IP

r. Controllare la pagina Progettazione e assicurarsi che la prenotazione del pool IP venga visualizzata nell'interfaccia utente e che il valore percentuale utilizzato sia corretto.

b. Se l'operazione di provisioning dell'associazione del pool VirtualNetwork-IP non è riuscita per alcun dispositivo nell'infrastruttura, verificare il motivo e provare a eseguire di nuovo il provisioning di tali switch non riusciti prima di passare al provisioning successivo.

c. Se un pool IP non viene elencato quando si aggiunge un segmento, controllare la pagina di progettazione → Prenotazione pool IP e assicurarsi che non venga utilizzato al 100%.

d. Non aggiungere/rimuovere/modificare dispositivi di bordo/bordo dell'infrastruttura mentre è in

corso il provisioning del pool IP della rete virtuale nell'infrastruttura specifica.

e. Prima di rimuovere qualsiasi SGT (Scalable Group Tag) dalla pagina VN, verificare se viene utilizzato in una delle associazioni di pool VN-IP esistenti.

e. Prima di rimuovere un pool IP, verificare che non venga utilizzato in alcuna assegnazione di porta statica.

4. Caricamento host - Assegnazione porta

r. Verificare che tutte le porte di accesso del dispositivo siano visualizzate. In caso contrario, è necessario controllare lo switch o l'app di inventario Cisco DNA Center.

b. Se solo alcune delle interfacce non vengono visualizzate, controllare la matrice di compatibilità SDA e verificare che il dispositivo sia supportato ([matrice di compatibilità SDA](#)).

c. Se si riscontrano discrepanze nell'assegnazione della porta nella pagina relativa alla conformità della struttura, effettuare nuovamente il provisioning della porta (cancellare e configurare) da Cisco DNA Center durante un intervento di manutenzione e ricontrollare la conformità.

5. Automazione LAN

1. Prima di avviare l'automazione LAN, seguire i passaggi descritti nella [Cisco DNA Center SD-Access LAN Automation Deployment Guide](#).
2. Se un dispositivo automatizzato LAN viene eliminato da Cisco DNA Center, aggiungerlo nuovamente tramite l'automazione LAN. Non aggiungerlo di nuovo tramite le pagine Inventario o Rilevamento.
3. Non modificare manualmente la configurazione dell'interfaccia automatizzata LAN nel dispositivo, inclusi Loopback0 o Loopback6000.
4. Non spostare manualmente la configurazione dell'interfaccia LAN L3 automatizzata da un'interfaccia a un'altra o da un dispositivo a un altro dispositivo.
5. Non utilizzare un indirizzo IP del pool sottostante per altri scopi nella rete. Utilizza una piscina dedicata per la struttura
6. Confermare che il numero di serie dell'agente Plug and Play non esista già nelle pagine ISE e Plug and Play.