

Guida introduttiva a Cisco IQ Virtual Appliance

Introduzione

Cisco IQTM offre ai clienti miglioramenti e funzionalità progettate per migliorare la visibilità degli asset, offrire informazioni più dettagliate negli ambienti e semplificare la gestione dei casi. Inoltre, le funzioni di AI, come l'Assistente AI, ottimizzano i risultati operativi e l'esperienza utente di Cisco IQ fornendo una comprensione contestuale che consente agli utenti di prendere decisioni proattive e informate e di semplificare i processi per il coinvolgimento e il successo del cliente.

Cisco IQ On-Prem Air-Gapped è una delle modalità di implementazione di Cisco IQ, progettata per i clienti in settori altamente regolamentati con rigorosi requisiti di conformità, sovranità sui dati e sicurezza. In questa modalità, Cisco IQ viene fornito come macchina virtuale (VM) indipendente, nota come Cisco IQ Virtual Appliance (VA). Il VA viene eseguito interamente presso la sede del cliente e funziona in totale isolamento dalle reti esterne. Per mantenere questo isolamento, gli aggiornamenti software e i pacchetti di manutenzione vengono ottenuti da Cisco IQ SaaS e trasferiti all'appliance VA tramite un processo manuale approvato.

Cisco IQ On-Prem Air-Gapped estende le funzionalità chiave di Cisco IQ SaaS agli ambienti con air-gapped, consentendo ai team mission-critical di operare con velocità e intelligenza diagnostica paragonabili a quelle delle aziende connesse al cloud.

Questa guida fornisce istruzioni per la configurazione e l'implementazione di Cisco IQ VA per Air-Gapped, incluso il processo di configurazione dell'ambiente di rete richiesto.



Nota: Cisco IQ VA è attualmente limitato ai clienti iscritti al programma di rilascio controllato. L'accesso al download per VA e i suoi sistemi operativi (moduli, regole e diritti) è disponibile esclusivamente per i clienti selezionati. Per ulteriori informazioni, contattare il rappresentante commerciale.

Opzioni di implementazione

Cisco IQ VA offre un modello di implementazione flessibile progettato per offrire valore con opzioni adatte a diverse esigenze operative. La distribuzione di base fornisce funzionalità essenziali quali la gestione di asset e inventario, valutazioni e altre operazioni.

Per i clienti alla ricerca di informazioni dettagliate e automazione basate sull'intelligenza artificiale, VA offre anche un'opzione di installazione basata sull'intelligenza artificiale abilitata tramite l'hardware GPU (Graphics Processing Unit). È possibile sbloccare potenti funzionalità di

intelligenza artificiale, quali l'Assistente AI, le Informazioni chiave e l'approfondimento completo con l'aggiunta di intelligenza artificiale.

Questo approccio consente di scegliere la soluzione più adatta alle proprie esigenze operative e di sicurezza, rendendo la tecnologia VA una soluzione scalabile e pronta per il futuro.

Prerequisiti

Prima di configurare e installare Cisco IQ VA, verificare che siano soddisfatti i seguenti prerequisiti.

Requisiti di risorse hardware e VM

Cisco IQ VA è stato testato per la capacità su più scale e offre diverse dimensioni di installazione per supportare le esigenze di scalabilità dell'ambiente. Vedere la tabella seguente per selezionare la configurazione delle risorse appropriata in base al numero di rilevamenti di dispositivi pianificati.

Tabella 1: Requisiti di risorse hardware e VM

Risorsa	Fino a 5.000 dispositivi (non basati su GPU)	Fino a 20.000 dispositivi (non basati su GPU)	Fino a 20.000 dispositivi (basati su GPU)
vCPU	48	64	96
RAM	96 GB	128 GB	256 GB
Storage (SSD) (consigliato per prestazioni migliori)	1,3 TB	1,3 TB	1,3 TB
Pianificazione raccolta	24 ore o più	24 ore o più	24 ore o più
Hypervisor supportati	- VMware ESXi v8.0 o versioni successive con VMware vSphere Web Client v8.0 o versioni successive - Hyper-V su Microsoft Server 2022 e 2025		

	• Hypervisor KVM (Kernel-based Virtual Machine) su RHEL v9.7 o versioni successive
Server	• Unified Computing System M6 o modelli più recenti
Ulteriori suggerimenti	• Cisco consiglia di utilizzare il provisioning spesso. Anche se è possibile utilizzare il thin provisioning, l'over-provisioning può causare una mancanza di capacità di storage che può causare il degrado e la perdita di servizio. • Si consiglia di posizionare i dischi dell'accessorio su un volume supportato da unità a stato solido. • La velocità di scrittura del disco deve essere superiore a 70 megabyte al secondo.

Requisiti delle risorse per le funzioni AI

Cisco IQ VA è testato e supportato sulla GPU NVIDIA RTX Pro 6000 Blackwell Server Edition. Questa configurazione della GPU soddisfa i requisiti di prestazioni e latenza nella scalabilità dell'installazione pianificata.

Tabella 2: Requisiti delle risorse per le funzioni AI

Risorsa	Consigliato
GPU convalidata	NVIDIA RTX Pro 6000 Blackwell Server Edition
Opzioni GPU aggiuntive (non convalidate)	• NVIDIA H200 (141 GB)
Opzioni GPU aggiuntive (non convalidate, consigliate con un (1) utente simultaneo)	• NVIDIA H100 (80 GB) • NVIDIA H100 NVL (94 GB) • NVIDIA A100 (80 GB)



Nota: Le GPU diverse da NVIDIA RTX Pro 6000 Blackwell Server Edition non sono state convalidate nei laboratori Cisco sulla scala supportata. Le prestazioni e la latenza non sono garantite per le GPU non convalidate. Convalidare tutto l'hardware non supportato in base al carico di lavoro previsto in un ambiente di pre-produzione prima dell'installazione della

produzione.

Requisiti di rete

VA supporta un'unica interfaccia di rete.

Requisiti di indirizzo IP e nome host

È necessario soddisfare i seguenti requisiti di indirizzo IP e nome host:

- DNS (Domain Name System): Il DNS semplifica la gestione del sistema sostituendo gli indirizzi IP numerici con nomi host coerenti e leggibili. Questo approccio semplifica la manutenzione, l'integrazione dei servizi e la convalida affidabile dei certificati in ambienti sicuri. Verificare che l'indirizzo IPv4 sia configurato nel DNS con quanto segue:
- Record A: Associa il nome host all'indirizzo IPv4
- Record puntatore (PTR) associato: Necessario per supportare ricerche DNS inverse; se un indirizzo IP viene risolto in più nomi host, il primo nome host risolto viene utilizzato per accedere all'interfaccia utente

 Nota: DHCP non è attualmente supportato.

Requisiti delle porte

Nella tabella seguente vengono descritte le porte di rete necessarie per la comunicazione Cisco IQ VA.

Tabella 3. Requisiti delle porte

Porta/e	Protocollo	Descrizione
22	TCP	Utilizzato per le sessioni di debug di CLI Administrator e Cisco Support
443	TCP	Utilizzato per le comunicazioni tra i browser Web e On-Prem di Cisco IQ e le destinazioni degli endpoint
54, 123, 161	UDP	Utilizzato per inviare e ricevere traffico DNS, NTP e SNMP

Browser supportati

Per installare e avviare VA, è necessario utilizzare l'ultima versione stabile dei seguenti browser:

- Google Chrome
- Microsoft Edge
- Apple Safari
- Mozilla Firefox



Nota: Il supporto è limitato alle versioni correnti del browser e le versioni precedenti potrebbero non fornire funzionalità complete o non essere supportate a causa del rilascio di nuovi aggiornamenti.

Installazione di Virtual Appliance

Questa sezione descrive le procedure di installazione per VA. L'ambito corrente include istruzioni per i seguenti hypervisor:

- VMWare ESXi
- Microsoft Hyper-V Server
- KVM Red Hat

Scarica Virtual Appliance

I file del programma di installazione VA sono disponibili per il download da Cisco IQ SaaS. Per scaricare VA:

1. Accedere a [Cisco IQ](#) (SaaS).
2. Passare a Impostazioni di sistema > Catalogo package.
3. Dalla scheda Cisco IQ VA, scegliere le opzioni di download. Viene visualizzata la finestra Installa package.
4. Selezionare una delle seguenti opzioni di hypervisor dall'elenco a discesa:
 - ESXi: per VMware ESXi
 - Hyper-V: per Microsoft Hyper-V
 - KVM: per la macchina virtuale basata su kernel Linux (KVM)
5. Selezionare una Versione dall'elenco a discesa.
6. Fare clic su Download per salvare il file localmente.



Nota: I file di installazione sono di grandi dimensioni (20-25 GB); assicurarsi di disporre di

spazio su disco sufficiente prima di eseguire il download.

Installazione di Virtual Appliance su VMware ESXi

Il file del programma di installazione VA scaricato è pronto per essere installato. Per installare VA su VMware ESXi:

 Nota: L'OAV deve essere implementato utilizzando VMware vCenter e non può essere implementato direttamente sui server ESXi.

1. Accedere a VMware vSphere Web Client con le credenziali dell'amministratore.
2. Fare clic con il pulsante destro del mouse sull'oggetto vCenter appropriato (centro dati, cluster o host ESXi) e scegliere Distribuisci modello OVF.
3. Nella procedura guidata Distribuisci modello OVF, scegliere la pagina del modello, specificare il percorso di origine e fare clic su Avanti. È possibile specificare un URL o selezionare una posizione accessibile.
4. Nella pagina Dettagli modello OVF verificare i dettagli del modello e fare clic su Avanti. Non è necessario alcun input.
5. Nella pagina Selezionare un nome e un percorso aggiungere o modificare Nome e Percorso per VA e fare clic su Avanti.
6. Nella pagina Selezionare una risorsa scegliere l'host (host ESXi), il cluster o il pool di risorse specifico in cui si desidera eseguire la distribuzione e fare clic su Avanti.

 Nota: Ogni VM deve essere assegnata a un host specifico su cluster configurati con vSphere High Availability (HA) o in modalità manuale vSphere Distributed Resource Scheduler (DRS).

7. Nella pagina Verifica dettagli verificare i dettagli del modello OVA e fare clic su Avanti.
8. Nella pagina Configurazione scegliere una configurazione di distribuzione e fare clic su Avanti.
9. Nella pagina Seleziona storage, scegliere il percorso di storage di destinazione per i file VM nell'host ESXi selezionato e fare clic su Avanti.
10. Scegliere il formato del disco per i dischi virtuali della VM.

 Nota: Si consiglia di utilizzare il provisioning thick. Sebbene sia possibile utilizzare il thin provisioning, un sovraccarico dello storage può causare la mancanza di capacità di storage, con conseguente degrado e perdita di servizio.

11. Nella pagina Seleziona reti, scegliere una rete di origine e mapparla a una rete di destinazione e fare clic su Avanti.
12. Nella pagina Pronto per il completamento, selezionare Accensione dopo la distribuzione e fare clic su Fine.
13. Verificare che le VM siano configurate con le seguenti impostazioni aggiuntive facendo clic con il pulsante destro del mouse sulla VM desiderata in VMware ESXi e scegliendo Modifica impostazioni.

- CPU: Selezionare Basso dal primo elenco a discesa Condivisioni
- Memoria: Selezionare la casella di controllo Riserva tutta la memoria guest (tutte bloccate)
- Impostare CPU e RAM in base alle dimensioni della scala; per ulteriori informazioni, vedere [Requisiti delle risorse hardware e VM](#)

14. In VMware ESXi, selezionare la VM desiderata.

15. Fare clic sulla scheda Riepilogo.

16. Fare clic sull'immagine visualizzata o sull'icona Avvia console per avviare la console.

17. Per i passaggi successivi, vedere [Configurazione di rete](#).

Installazione di Virtual Appliance in Microsoft Hyper-V Server

Per installare VA su Hyper-V:

1. Accedere alla console di gestione di Hyper-V Server con le credenziali di amministratore.
2. Estrarre il pacchetto VA nel percorso definito dall'amministratore di Hyper-V per archiviare tutti i dischi rigidi virtuali.
3. Verificare che tutti i dischi del file .tar.gz Cisco IQ originale si trovino nella cartella Virtual Hard Disks (Dischi rigidi virtuali).
4. Dal riquadro Azioni di Gestione Hyper-V, scegliere Nuovo > Macchina virtuale e fare clic su Avanti.
5. Immettere il Nome che si desidera assegnare alla VA e fare clic su Avanti.
6. Scegliere Generazione 2 e fare clic su Avanti.
7. Immettere il valore della memoria in base alle dimensioni consigliate in [Requisiti di risorse hardware e VM](#) e fare clic su Avanti.
8. Verificare che l'opzione Usa memoria dinamica non sia selezionata.
9. Scegliere la scheda di rete appropriata per la scheda VLAN e fare clic su Avanti.
10. Aggiungere il disco rigido virtuale VA fornito, accertandosi che il disco uno (1) sia il primo disco, quindi fare clic su Avanti.



Nota: Gli altri due (2) dischi rigidi virtuali vengono aggiunti in un passaggio successivo.

11. Verificare le selezioni nel Riepilogo e fare clic su Fine. Hyper-V visualizza la VM VA appena creata.
12. Fare clic con il pulsante destro del mouse sulla VM e scegliere Impostazioni.
13. In Protezione, deselezionare la casella di controllo Abilita avvio protetto.
14. Aggiungere gli altri due (2) dischi rigidi virtuali alla macchina virtuale ripetendo la stessa procedura utilizzata per aggiungere il primo disco rigido.
15. In Funzioni avanzate nella scheda di rete, verificare che l'opzione Abilita denominazione dispositivi sia selezionata.
16. Impostare il numero di processori sulle vCPU consigliate, come indicato in [Requisiti di risorse hardware e VM](#).
17. Nel riquadro Azioni selezionare Avvia per accendere la VM.

18. Nel riquadro Azioni selezionare Connetti per connettersi alla macchina virtuale. Viene visualizzata la console di connessione VM.
19. Per ulteriori informazioni, vedere [Configurazione della rete](#).

Installazione di un'appliance virtuale su KVM Red Hat

Prima di installare VA su KVM, verificare che siano soddisfatti i seguenti requisiti supportati.

- SO host RHEL
- Accesso amministrativo sul server Red Hat

Per installare VA su un hypervisor KVM, è necessario VM Manager.

1. Accedere al server del sistema operativo host Red Hat con le credenziali dell'amministratore.
2. Scaricare ed estrarre il pacchetto VA sull'host.
3. Avviare il client Virtual Machine Manager (VMM).
4. Scegliere File > Nuova macchina virtuale dal menu per installare una nuova VA.
5. Scegliere Importa immagine disco esistente e fare clic su Inoltra.
6. In Specificare il percorso di archiviazione esistente fare clic su Sfoglia.
7. Creare un nuovo pool di archiviazione utilizzando il percorso in cui è stato estratto il pacchetto VA.
8. Scegliere il primo disco del VA dal pool di storage creato nel passaggio precedente e fare clic su Scegli volume.
9. In Choose an operating system type and version, selezionare AlmaLinux 9, quindi fare clic su Forward.
10. In Scegli le impostazioni della memoria e della CPU, immettere i dettagli in base alle dimensioni della scala e fare clic su Avanti. Per ulteriori informazioni, vedere [Requisiti delle risorse hardware e VM](#).
11. Nella finestra di dialogo, completate la seguente configurazione:
 1. In Pronto per iniziare l'installazione, immettere un Nome per l'istanza di VA.
 2. Fare clic sull'opzione Personalizza configurazione prima dell'installazione.
 3. In Selezione rete verificare di aver selezionato la rete virtuale appropriata.
12. Fare clic su Finish (Fine) per completare l'aggiunta del primo disco.
13. Aggiungere i due (2) dischi rimanenti:
 1. Nella console VMM fare clic su Add Hardware (Aggiungi hardware).
 2. In Archiviazione verificare che la casella di controllo Seleziona o crea archivio personalizzato sia selezionata e fare clic su Gestisci.
 3. Selezionare il secondo disco del file VA estratto nel sistema.
 4. Fare clic su Scegli volume.
14. Ripetere gli stessi passaggi (Installazione hardware) per aggiungere il terzo disco VA.
15. Verificare che tutti i tipi di bus del disco siano SCSI.
16. Fare clic su Finish (Fine).
17. Nella sezione Panoramica, scegliere UEFI per il firmware.

18. Fare clic su Inizia installazione.
19. Per i passaggi successivi, vedere [Configurazione di rete](#).

Configurazione della rete

1. Avviare VA dalla console VM.

```
***** WARNING!!! *****  
***** READ THIS BEFORE ATTEMPTING TO LOGON *****  
#  
#   This System is for the use of authorized users only. Individuals  
#   using this computer without authority, or in excess of their  
#   authority, are subject to having all of their activities on this  
#   system monitored and recorded by system personnel. In the course  
#   of monitoring individuals improperly using this system, or in the  
#   course of system maintenance, the activities of authorized users  
#   may also be monitored. Anyone using this system expressly  
#   consents to such monitoring and is advised that if such  
#   monitoring reveals possible criminal activity, system personnel  
#   may provide the evidence of such monitoring to law enforcement  
#   officials. You cannot copy, disclose, display or otherwise  
#   communicate the contents of this server except to other Cisco  
#   employees who have been authorized to access this server.  
#  
***** Confidential Information *****  
cmae-infra login: admin  
Password:
```

Accedi

2. Accedere alla console utilizzando le credenziali di rete predefinite immettendo "admin" sia per il nome di accesso che per la password. Viene visualizzato il menu principale.



Nota: Le credenziali predefinite vengono fornite per la configurazione iniziale solo perché in questa fase dell'installazione non sono presenti dati da proteggere.



Navigation **Main Menu** > **Configure Network Settings**

CONFIGURATION SETTINGS

Configured network settings:

Please provide the following network settings:

Enter IP Address/Mask

(e.g., 192.168.1.100/24):

Valid IP/Mask format ✓

Enter Gateway IP

(e.g., 192.168.1.1):

Valid Gateway IP ✓

Enter DNS IP List (comma-separated)

(e.g., 8.8.8.8,8.8.4.4):

Valid DNS list (1 servers) ✓

Enter Search Domain

(default: local.domain) - press Enter to use default:

Menu principale

3. Immettere "1" e premere Invio per configurare le impostazioni di rete.
4. Specificare le impostazioni di rete seguenti:

 **Nota:** Gli utenti possono premere Invio per utilizzare i valori rilevati, se disponibili.

- Indirizzo IP
- IP gateway
- Elenco IP DNS
- Cerca nel dominio
- Elenco server NTP

 **Nota:** È supportato l'immissione di più server NTP utilizzando un formato separato da virgole.

5. Configurare l'autenticazione NTP premendo N per procedere senza un metodo di

autenticazione

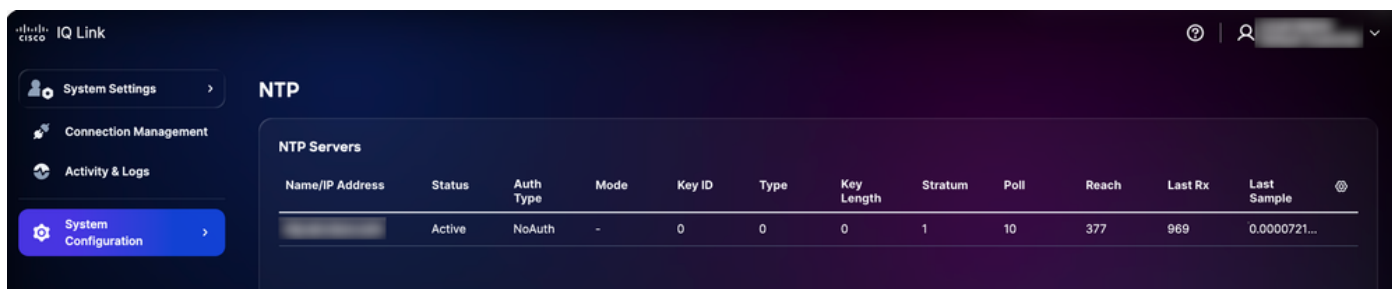
O

Premere Y e inserire il numero corrispondente di un'opzione elencata di seguito:

- Autenticazione tradizionale basata su chiavi: Utilizza le credenziali fornite per la sincronizzazione sicura dell'ora; dopo aver selezionato questa opzione, immettere un algoritmo valido e una chiave esadecimale
- NTS (Network Time Security): Utilizza il protocollo NTS per garantire una comunicazione NTP sicura



Nota: Le informazioni NTP possono essere convalidate nell'interfaccia utente dopo l'installazione passando a Impostazioni di sistema.



Name/IP Address	Status	Auth Type	Mode	Key ID	Type	Key Length	Stratum	Poll	Reach	Last Rx	Last Sample	
[REDACTED]	Active	NoAuth	-	0	0	0	1	10	377	969	0.0000721...	

Convalida NTP nell'interfaccia utente

6. Immettere e confermare una password dopo aver esaminato i requisiti della password su schermo.
7. Rivedere il riepilogo e premere Y per continuare. L'installazione può richiedere alcuni minuti.
8. Una volta ricevuto il messaggio di operazione riuscita, premere Invio per tornare al menu principale.



Menu Cisco IQ

Le impostazioni di rete sono ora configurate, ma VA non è ancora stato installato. Si consiglia di tornare all'hypervisor e creare un'istanza della nuova VM per riferimento futuro. A questo punto, è inoltre possibile avviare una connessione Secure Shell utilizzando l'indirizzo IP e le credenziali appena configurati.

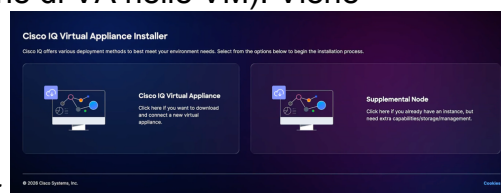
La configurazione manuale di VA è stata completata.

Installazione di VA per la modalità Air-Gapped

Per installare VA:

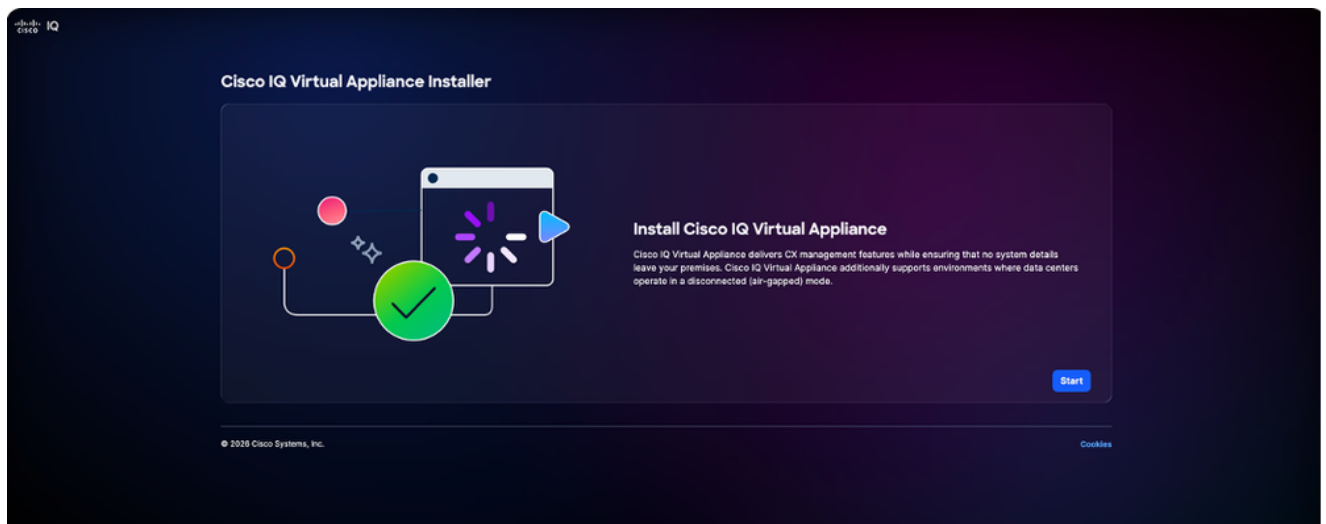
1. Passare all'interfaccia Web del programma di installazione di VA (<https://<CIQ-HOST>/installer/welcome>) (ricevuta dopo la configurazione di VA nelle VM). Viene

visualizzata la pagina Cisco IQ Virtual Appliance Installer.



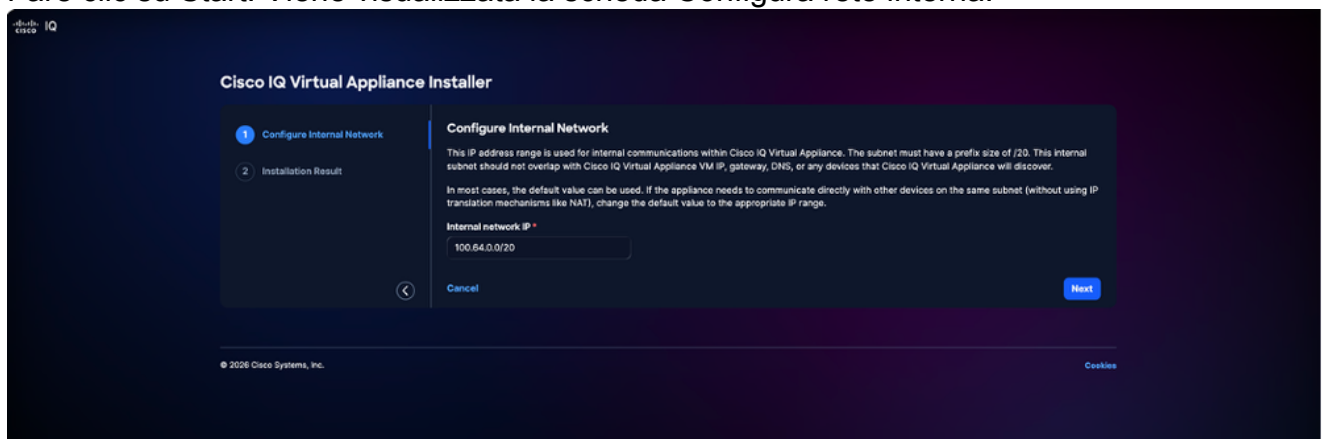
Pagina Virtual Appliance Installer

2. Fare clic su Cisco IQ Virtual Appliance. Viene visualizzata la pagina Installa Cisco IQ Virtual Appliance.



Installa Virtual Appliance

3. Fare clic su Start. Viene visualizzata la scheda Configura rete interna.

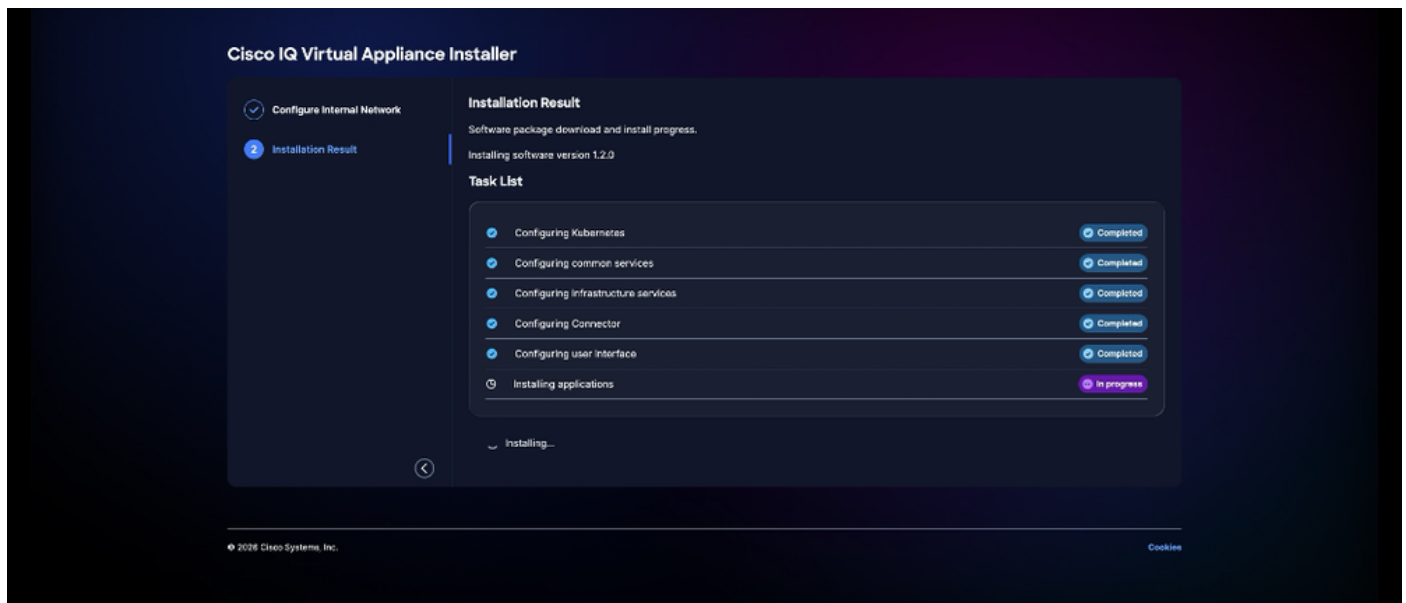


Configurazione della rete interna

4. Immettere l'intervallo IP interno.

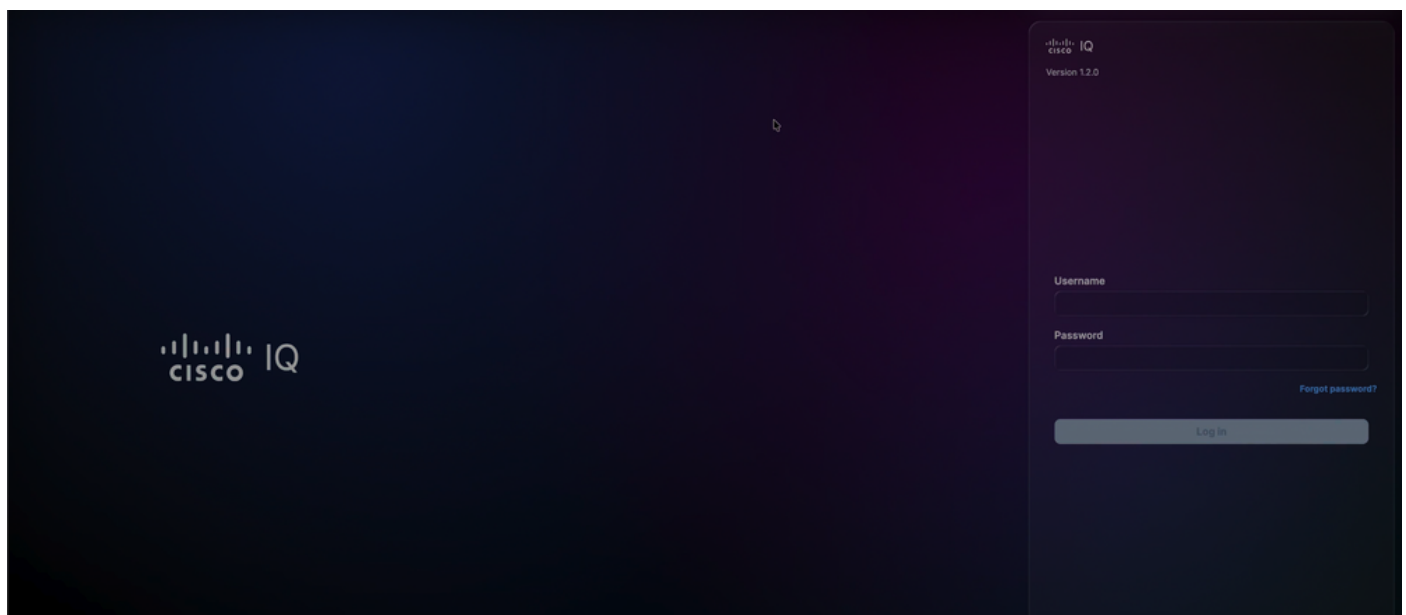
 **Nota:** Verificare che la subnet interna non si sovrapponga agli intervalli IP, gateway, DNS o di rete raggiungibili della macchina virtuale.

5. Fare clic su Avanti. Viene visualizzata la pagina Risultato installatore.



Risultato installazione

6. Attendere il completamento di tutti i task visualizzati. Al termine, il browser passa automaticamente alla pagina di accesso di Cisco IQ VA. L'installazione può richiedere fino a due (2) ore.



Accesso

Una volta completato l'accesso, il sistema è pronto per rilevare i dispositivi e supporta l'applicazione Assets senza supporto AI.

Installazione di moduli e regole

Per espandere le funzionalità del sistema, è possibile scaricare moduli e regole aggiuntivi direttamente dal portale SaaS Cisco IQ e completare l'installazione in VA. Per ulteriori informazioni, vedere Installazione dei pacchetti nella [Guida operativa](#).



Nota: Il modulo Assets è preinstallato nel programma di installazione VA e disponibile per l'uso immediato. È possibile aggiornare il modulo asset o la versione della regola asset come qualsiasi altro modulo e regola in base alle esigenze.

Caratteristiche con tecnologia AI

Cisco IQ offre un modello di implementazione flessibile che include una funzionalità aggiuntiva basata su AI per migliorare le conoscenze dei clienti e le funzionalità di automazione. Cisco IQ VA può essere installato con o senza supporto GPU.

Installazione di appliance virtuali senza supporto GPU (funzionalità non AI)

1. Accedere a [Cisco IQ](#).
2. Selezionare System Settings > Package Catalog per scaricare Cisco IQ VA Installer e il programma di installazione dei moduli Cisco IQ desiderato. Per ulteriori informazioni, vedere Installazione dei pacchetti nella [Guida operativa](#).
3. Allocazione delle risorse IP e VM e installazione della VM. Per il carico di lavoro della CPU è richiesto almeno un (1) computer virtuale.
4. Installare il programma di installazione di Cisco IQ VA per preparare il sistema. Per ulteriori informazioni, vedere [Installazione del programma di installazione](#) di [Virtual Appliance](#).
5. Una volta installato, accedere all'interfaccia utente di Cisco IQ VA.
6. Installare i moduli scaricati passando a Impostazioni di sistema > Gestione pacchetti in VA. Per ulteriori informazioni, vedere Installazione dei pacchetti nella [Guida operativa](#).

Il sistema è ora pronto per l'uso senza supporto AI.

Installazione di un'appliance virtuale con supporto GPU (funzionalità AI)

Per abilitare le funzionalità basate su AI, il sistema deve essere configurato come "AI Ready".

Prerequisiti

- Verificare che il nodo primario sia completamente configurato e operativo.
- Esaminare i requisiti hardware della GPU e selezionare un nodo supplementare con funzionalità GPU. Per ulteriori informazioni, vedere [Requisiti delle risorse per le funzioni AI](#).

- Seguire la procedura di distribuzione a più nodi, designando il nodo supplementare come nodo GPU. Per ulteriori informazioni, vedere [Aggiunta del supporto di nodi supplementari e nodi multipli](#).

Installazione con supporto GPU (funzionalità AI)

1. Accedere a [Cisco IQ](#).
2. Selezionare System Settings > Package Catalog per scaricare Cisco IQ VA Installer, i moduli Cisco IQ desiderati e Cisco IQ AI Inference Infrastructure. Per ulteriori informazioni, vedere Installing Packages and AI-Powered features in [Operations Guide](#) (Guida operativa).
3. Allocazione di risorse IP e VM e installazione delle VM. Sono necessarie almeno due (2) VM: uno (1) per il carico di lavoro della CPU e uno (1) per il carico di lavoro della GPU.
4. Installare il programma di installazione di Cisco IQ VA per preparare il sistema. Per ulteriori informazioni, vedere [Installazione del programma di installazione](#) di [Virtual Appliance](#).
5. Una volta installato, accedere all'interfaccia utente di Cisco IQ VA.
6. Installare l'infrastruttura di inferenza AI selezionando Impostazioni di sistema > Gestione pacchetti. Per ulteriori informazioni, vedere Funzionalità basate su AI nella [Guida operativa](#).
7. Installare i moduli aggiuntivi scaricati passando a Impostazioni di sistema > Gestione pacchetti. Per ulteriori informazioni, vedere Aggiunta di moduli nella [Guida operativa](#).

Il sistema è ora pronto per l'uso con funzioni basate su AI.

Per ulteriori informazioni sull'attivazione delle funzioni basate su AI, consultare la [Guida operativa](#).

Supporto di più nodi

L'architettura a più nodi consente di espandere un VA standalone in un cluster, fornendo una maggiore capacità delle risorse per l'elaborazione e l'installazione delle applicazioni. Questa configurazione consente di aggiungere nodi supplementari a un nodo di gestione principale, consentendo al sistema di scalare in base ai requisiti specifici del carico di lavoro.

Per aggiungere un nodo GPU è essenziale abilitare la funzionalità a più nodi. Questa integrazione consente all'ambiente locale di sfruttare le risorse GPU per la deduzione dell'IA. In questa sezione vengono fornite indicazioni dettagliate sulla connessione della GPU come nodo supplementare per l'On-Prem, necessaria per consentire agli utenti di utilizzare le funzionalità della GPU in modo efficace.

Requisiti di rete

VA supporta un'unica interfaccia di rete. Per ulteriori informazioni, vedere [Requisiti di rete](#).

Requisiti delle porte

Nella tabella seguente vengono descritte le porte di rete necessarie per la comunicazione Cisco IQ VA in un ambiente a più nodi.

Tabella 4. Requisiti delle porte a più nodi

Porta/e	Protocollo	Descrizione	Tipo di nodo
22	TCP	Utilizzato per le sessioni di debug di CLI Administrator e Cisco Support	Nodi di gestione e supplementari
443	TCP	Utilizzato per le comunicazioni tra i browser Web e On-Prem di Cisco IQ e le destinazioni degli endpoint	Nodi di gestione e supplementari
54, 123, 161	UDP	Utilizzato per inviare e ricevere traffico DNS, NTP e SNMP	Nodi di gestione e supplementari
10250, 10256	TCP	Utilizzato per la comunicazione Kubernetes tra il nodo	Nodi di gestione e supplementari
179	TCP	Utilizzato per il control plane VXLAN (BGP) tra nodi	Nodi di gestione e supplementari
4789	UDP	Utilizzato per il traffico VXLAN tra i nodi	Nodi di gestione e supplementari
500, 4500	UDP	Utilizzato per il traffico IKE IPsec tra nodi	Nodi di gestione e supplementari
Tutto	ESP (50)	Utilizzato per il traffico IPsec ESP tra nodi	Nodi di gestione e supplementari
6443	TCP	Utilizzato per il server API Kubernetes	Solo nodo di gestione



Nota: Il clustering a più nodi è supportato solo per le distribuzioni VA standard.

 Nota: Un nodo supplementare deve avere la stessa versione del nodo di gestione principale durante il processo di join iniziale.

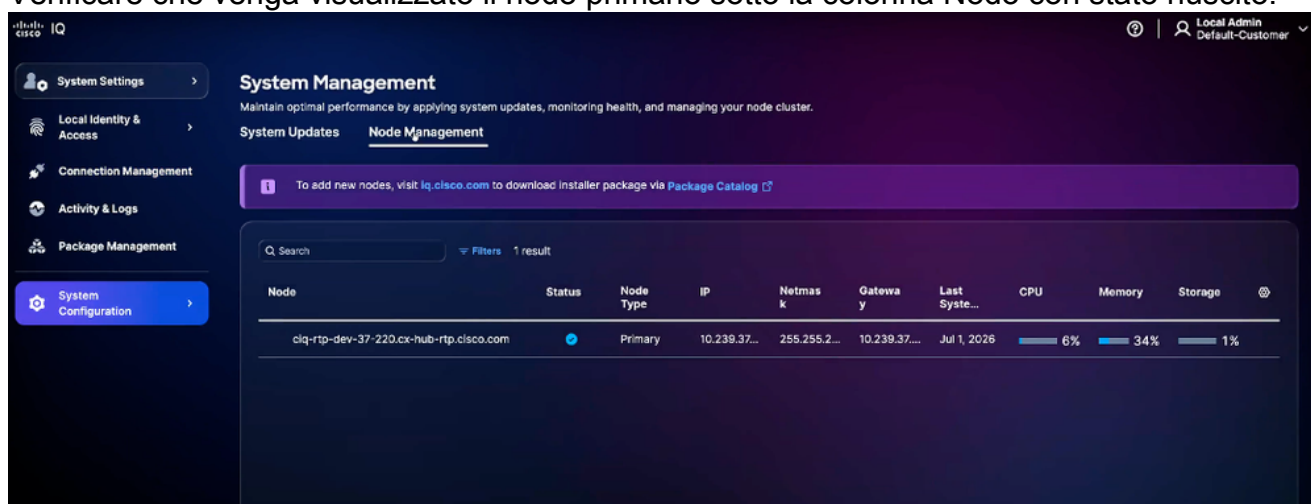
 Nota: L'implementazione corrente su più nodi non fornisce l'alta disponibilità (HA, High Availability) per il piano di gestione. Se il nodo di gestione principale non è più disponibile, le operazioni del cluster saranno interessate.

Aggiunta di un nodo supplementare

L'aggiunta di un nodo supplementare richiede lo stesso processo dell'installazione di VA. Dopo aver scaricato il programma di installazione VA dal catalogo pacchetti in Cisco IQ (SaaS), installarlo sull'hypervisor scelto. Per ulteriori informazioni, vedere [Installazione del programma di installazione di Virtual Appliance](#).

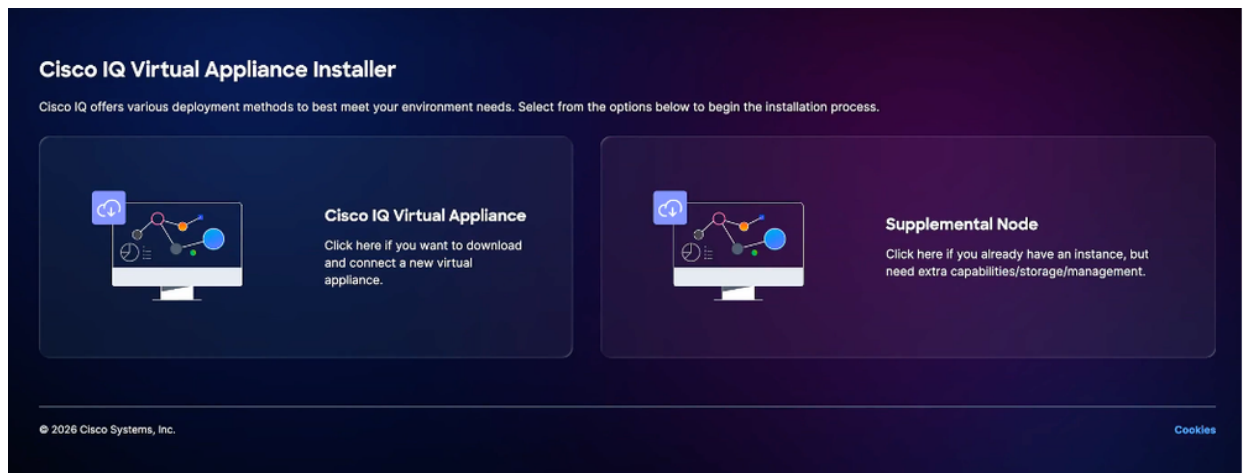
Prima di aggiungere un nodo supplementare, verificare che il primo nodo sia completamente configurato come VA standard. Per aggiungere un nodo supplementare:

1. Passare a Configurazione di sistema > Gestione nodi.
2. Verificare che venga visualizzato il nodo primario sotto la colonna Nodo con stato riuscito.



Gestione dei nodi

3. Passare a Virtual Appliance Installer. Vengono visualizzate le seguenti opzioni:
 - Cisco IQ Virtual Appliance
 - Nodo supplementare



Nodo supplementare

4. Fare clic sull'opzione Nodo supplementare. Viene visualizzata la pagina Supplemental Node Installer.

Supplemental Node Installer

Connect to node

Select an action and provide your credentials to establish connection to your cluster.

Primary node FQDN

Local admin username

Password

[Show](#)

Node type

GPU

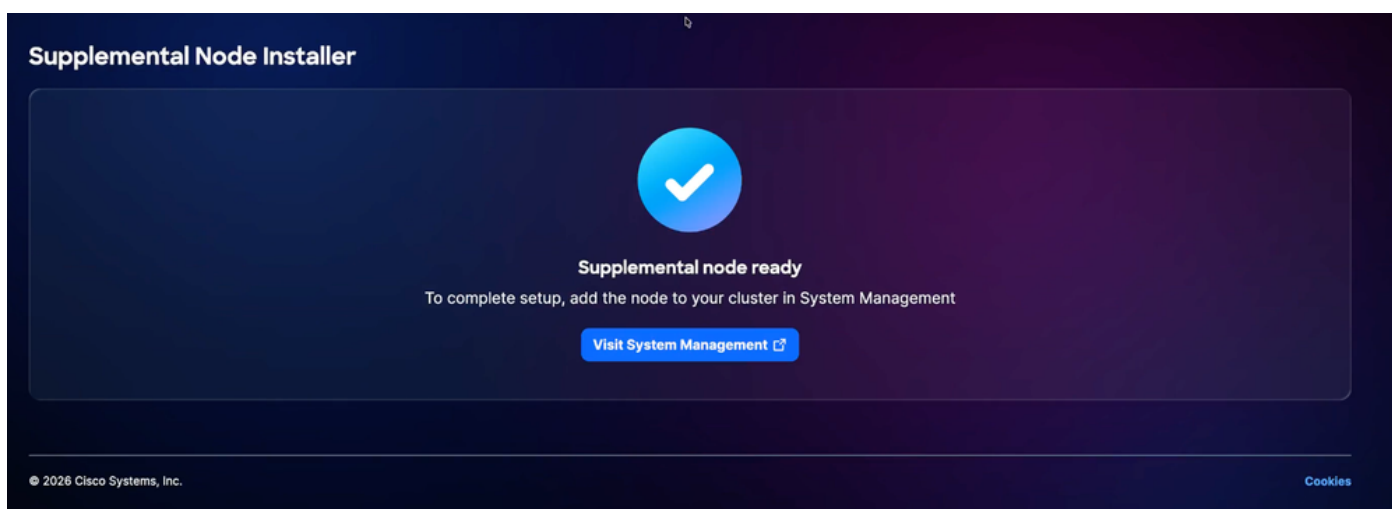
[Add node](#) [Cancel](#)

Pagina Nodo supplementare

5. Immettere il nome di dominio completo (FQDN) del nodo primario.
6. Immettere il nome utente dell'amministratore locale.
7. Immettere la password.
8. Selezionare Tipo nodo dall'elenco a discesa.

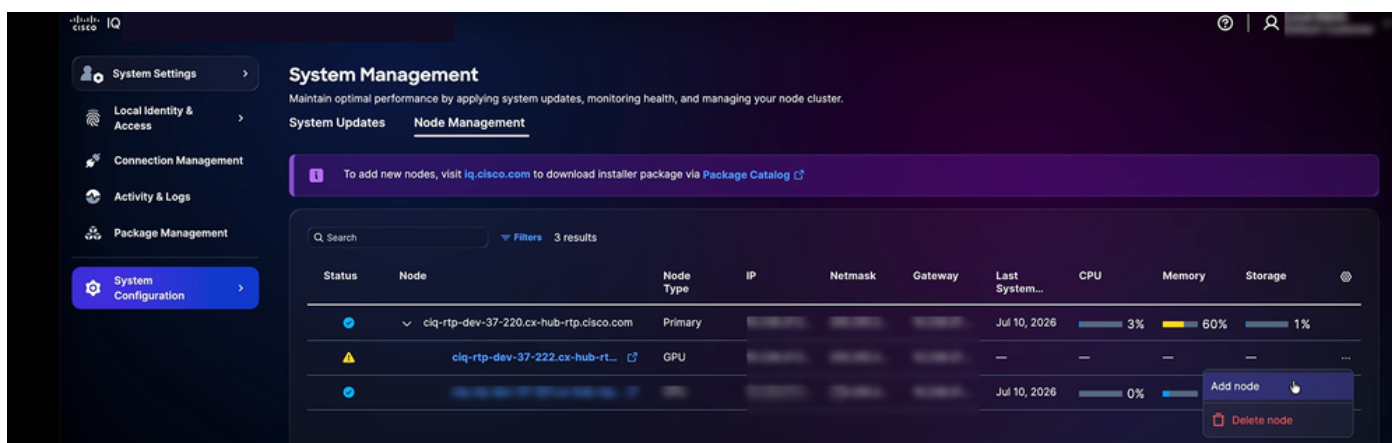
 **Nota:** È possibile scegliere il nodo di lavoro GPU. Quando si scelgono i nodi di lavoro GPU, assicurarsi che l'ambiente dell'hypervisor (ad esempio, VMware o Hyper-V) sia configurato con l'hardware necessario per supportare i dispositivi GPU, in quanto sono necessari per l'accessibilità dei nodi GPU. Per ulteriori informazioni, vedere [Opzioni](#) di [distribuzione](#).

9. Fare clic su Aggiungi nodo. Il messaggio "Supplemental node ready" (Pronto nodo supplementare) viene visualizzato dopo l'aggiunta del nodo.



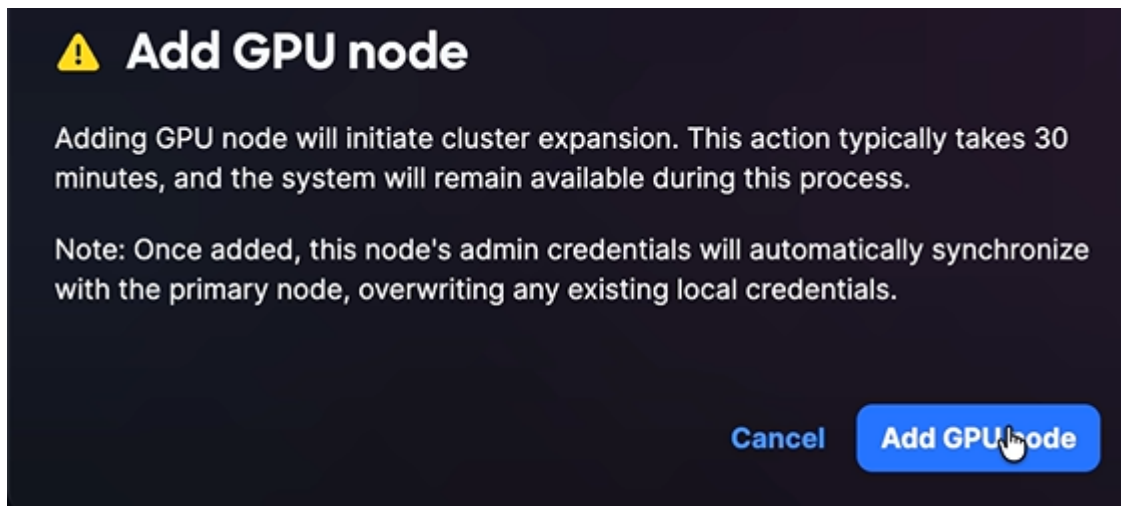
Pronto per il nodo supplementare

10. Quando viene visualizzato "Supplemental node ready" (Pronto nodo supplementare), fare clic sul collegamento Visita gestione sistema o passare a Gestione sistema > Gestione nodo per attivare l'azione di aggiunta nodo per completare l'integrazione.



Aggiungi nodo

11. Fare clic su Icona Altro > Aggiungi nodo. Viene visualizzata la finestra Aggiungi nodo GPU.



Aggiungi nodo GPU

12. Fare clic su Aggiungi nodo GPU. Una volta aggiunto correttamente, il nodo viene visualizzato in cluster.

Sincronizzazione e gestione cluster

Quando si aggiunge un nodo di lavoro, le credenziali amministrative del nodo di gestione primario vengono sincronizzate automaticamente con il nodo di lavoro. L'accesso al nodo di lavoro deve essere eseguito utilizzando queste credenziali sincronizzate.

 **Nota:** Il cluster gestisce in modo dinamico la distribuzione delle applicazioni. Quando un'applicazione richiede capacità di elaborazione avanzate, il sistema verifica la disponibilità dei nodi abilitati per GPU. Se è presente una scheda GPU e il pacchetto di applicazioni appropriato è installato, il sistema attiva queste funzionalità avanzate. Se il cluster non dispone delle risorse hardware necessarie, il sistema funzionerà in modalità non accelerata per mantenere la stabilità.

Supporto

È possibile creare richieste di supporto per VA e moduli specifici da Cisco IQ SaaS. Il modulo di supporto è disponibile in Cisco IQ SaaS e offre una visualizzazione consolidata delle richieste di supporto. Consente di filtrare, ordinare e personalizzare la visualizzazione dell'elenco di richieste, fornendo visibilità sia sulle richieste aperte che su quelle chiuse a cui si è autorizzati ad accedere. Per informazioni più dettagliate sul modulo di supporto in Cisco IQ SaaS, vedere la [guida introduttiva a Cisco IQ SaaS](#).



Nota: I clienti Cisco IQ VA possono accedere alla maggior parte delle funzionalità del modulo di supporto SaaS per Cisco IQ, tra cui l'apertura di richieste TAC (Technical Assistance Center) relative a Cisco IQ VA e ai relativi moduli, nonché la creazione e la gestione di richieste di prodotti.

Creazione di una richiesta di assistenza

È possibile creare richieste VA e specifiche per il modulo in Cisco IQ SaaS. Per creare una richiesta:

1. Accedere a [Cisco IQ \(SaaS\)](#).
2. Fare clic sull'icona Guida > Segnala un problema. Viene visualizzata la finestra Segnala un problema.

Report an Issue

Experiencing an issue with Cisco IQ? Let us know what's going on and we'll open a support case for you.

Issue type

☐ Portal login issues ☐ Error message ☐ Data discrepancy ☐ Other

Issue description

Describe what happened.

The more detail you give, the faster we can help.

Preferred contact method

☐ Telephone ☐ Email ☐ Virtual space via Webex

Include recipients (optional)

Select or add email addresses

Select or enter email addresses to include.

Cancel Submit

Segnala un problema

3. Fornire i dettagli richiesti.
4. Fare clic su Invia.

Appendice A

BOM di riferimento per appliance virtuale locale con GPU

Di seguito è riportata la distinta base di riferimento per VA locale che supporta fino a 10.000 dispositivi:

Tabella 5. Distinta base di riferimento

Codice prodotto	Descrizione	Quantità
UCS-M8-MLB	UCS M8 RACK MLB	1
UCS-C240-M8SX	Rack UCS C240 M8 senza CPU, memoria, unità, backplane 2U con SFF	1
CON-L1NCO-UCSCCX4S	CX LEVEL 1 8X7XNCDOS UCS C240 M8 Rack a due CPU, mem, unità, 2	1
RHEL-2S2V-D3A	Red Hat Enterprise Linux (1-2 CPU, 1-2 VN); Richiesta di supporto per 3 anni	1
CON-ISV1-RHEL62S2	ISV 24 ore su 24, 7 giorni su 7 Red Hat Enterprise Linux 1-2 CPU, 1-2 VPN	1
COMPUTE-AI	Caso di utilizzo di Compute Artificial Intelligence	1
GESTITO DA ISM	Modalità di distribuzione per i server serie C in modalità standalone	1
UCS-GPUAD-240M8	CONDOTTO DELL'ARIA GPU	1

	PER C240M8	
UCS-M-V5Q50GV2-D	Cisco VIC 15427 4x 10/25/50G mLOM serie C con avvio protetto	1
UCS-TPM-002D-D	TPM 2.0 TCG FIPS140-2 CC+ Cert M7 conforme a Intel MSW2022	1
UCS-RAIL-D	Kit binario per cuscinetto a sfere per server rack C220 e C240 M7/M8	1
CIMC-LATEST-D	Ultima release del software IMC (consigliata) per server serie C	1
UCS-HSLP-C220M8	Dissipatore di calore per C220M8, C240M8L e C240M8 con GPU	2
UCS-DDR5-BLK	DIMM DDR5 UCS vuota	24
UCS-BBLKD-M7	UCS serie C M7 SFF drive blanking panel	20
CBL-RAID 16-240M8	Cavo Y C240M8 da MB a RAID16/HBA	1
CBL-NVME-240M8-P4	Cavo NVMe C240M8SFF per unità 1-4 (P4)	1
CBL-NVME-240M8-P2	Cavo NVMe C240M8SFF per unità 21-24 (P2)	1
UCS-SDBKT-24XM7	UCS serie C M7 2U SD RAID Controller Staffa	1

CBL-G5GPU-C240M7	Cavo di alimentazione 12 VHPWR conforme a PCIe CEM C240M7 (fino a 450 W)	1
UCS-MRX64G2RE5	RDIMM DDR5-6400 da 64 GB 2Rx4 (16 Gb)	4
UCS-RIS1A-240M8	Riser UCS C240 M8 1A PCIe Gen5 (x8, x16, x8)	1
UCS-RIS2A-240M8	Riser UCS C240 M8 2A PCIe Gen5 (x8, x16, x8) (CPU2)	1
UCS-RIS3C-240M8	UCS C240 M8 Riser 3C PCIe Gen5 (x16)(CPU2)	1
UCS-RAID-MP1L32	Controller RAID MP1 tripla modalità 24G con FBWC da 4 GB, 32 drv con Brkt 2U	1
UCS-GPU-RTXP600	NVIDIA RTX Pro 6000: GPU FHFL a 2 slot da 600 W, 96 GB	1
NV-GRID-OPT-OUT	OPT-OUT SOFTWARE NVIDIA GRID	1
UCS-M2-HWRAID2	Controller RAID M.2 ottimizzato per l'avvio Cisco per unità SATA	1
UCS-M2-480G-D	SSD SATA M.2 DA 480 GB	2
UCS-M2I-240M8	UCS C240 M8 Internal M.2 Module	1
UCS-SDB1T9SA1VD	SATA 1,9 TB 2,5" 6 G 1X SSD Samsung G1PM893A	4

UCS-CPU-I650P	Intel I6520P 2,4 GHz/210W DDR5 da 24 C/144 MB 6400 MT/s	2
UCS-PSU1-2300W-D	Cisco UCS 2300W AC Power Supply per server rack Titanium	2
CAB-C19-CBN	Cavo di alimentazione a ponticello, 250 V CA, 16A, connettori C20-C19	2
UCS-RISAB-24XM7	UCS serie C M7 2U Air Blocker GPU solo	2
DC-MGT-SAAS	Cisco Intersight SaaS	1
DC-MGT-ISSAAS-ES	Servizi per l'infrastruttura SaaS/CVA - Essentials	1
SVS-DCM-SUPT-BAS	Cisco Support Basic per DCM	1
DC-MGT-UCSC1S	UCS Central per Server - Licenza per 1 server	1
DC-MGT-ADOBE-BAS	Intersight - Sessione di adozione virtuale http://cs.co/requestCSS	1

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).