



Per iniziare

Converged Systems Advisor

NetApp
October 04, 2023

Sommario

- Per iniziare 1
 - Guida rapida per Converged Systems Advisor 1
 - Prepara il tuo ambiente 2
 - Creare account per i dispositivi FlexPod 2
 - Configurare e implementare l'agente 7
 - Aggiungere l'infrastruttura al portale 10
 - Condivisione di un'infrastruttura con altri utenti 11
 - Configurare le notifiche 12
 - Impostare un indirizzo IP statico sull'agente 12

Per iniziare

Guida rapida per Converged Systems Advisor

Per iniziare con l'agente Converged Systems Advisor e il portale per FlexPod sono necessari alcuni passaggi.

1 Prepara il tuo ambiente

Verificare il supporto per la configurazione. "[Prepara il tuo ambiente](#)".

2 Creare account sui dispositivi FlexPod

Configurare gli account in Cisco UCS Manager, sugli switch Cisco Nexus, sui sistemi ONTAP, su VMware e su APIC. Questi account vengono utilizzati dall'agente per raccogliere i dati di configurazione. "[Creare account sui dispositivi FlexPod](#)".

3 Concedere i privilegi dell'utente CSA utilizzando un server TACACS+

Per coloro che utilizzano un server TACACS+, è necessario concedere privilegi utente CSA per gli switch, creare un gruppo di privilegi utente e concedere al gruppo l'accesso ai comandi di configurazione specifici richiesti da CSA. "[Concedere i privilegi dell'utente CSA utilizzando un server TACACS+](#)"

4 Configurare e implementare l'agente

Implementare l'agente Converged Systems Advisor su un server VMware ESXi. L'agente raccoglie i dati di configurazione relativi a ciascun dispositivo dell'infrastruttura convergente FlexPod e li invia al portale Converged Systems Advisor. "[Implementare l'agente](#)".

5 Aggiungere/condividere l'infrastruttura nel portale

Aggiungere ciascun dispositivo FlexPod al portale Converged Systems Advisor per creare un'intera infrastruttura che è possibile monitorare. È inoltre possibile condividere un'infrastruttura convergente per consentire a un'altra persona di accedere al portale in modo che possa visualizzare e monitorare la configurazione. "[Aggiungere e condividere l'infrastruttura nel portale](#)".

6 Configurare le notifiche

Con una licenza Premium, è possibile impostare notifiche che avvisano l'utente in caso di modifiche all'infrastruttura FlexPod tramite notifiche e-mail. "[Configurare le notifiche](#)"



Impostare un indirizzo IP statico

Se l'ambiente non dispone di un server DHCP, è possibile impostare un indirizzo IP statico nell'agente Converged Systems Advisor. ["Impostare un indirizzo IP statico sull'agente"](#)

Prepara il tuo ambiente

Per iniziare a utilizzare Converged Systems Advisor, è necessario preparare il proprio ambiente. La preparazione dell'ambiente include la verifica del supporto per la configurazione e la registrazione per un account NetApp Support Site.

Potrebbe essere utile ["Scopri come funziona Converged Systems Advisor"](#) prima di iniziare.

Fasi

1. Verificare il supporto in ["Tool di matrice di interoperabilità NetApp"](#):
 - a. Verifica che Converged Systems Advisor supporti la tua infrastruttura convergente FlexPod.
 - b. Verificare di disporre di un server VMware ESXi supportato per l'agente Converged Systems Advisor.

Per ridurre al minimo l'utilizzo della larghezza di banda, NetApp consiglia di installare l'agente nello stesso data center dell'infrastruttura convergente FlexPod.

2. Assicurarsi che la rete in cui si installa l'agente consenta la connettività tra i componenti:
 - L'agente deve disporre di connettività a ciascun componente di FlexPod per poter raccogliere i dati di configurazione.
 - L'agente richiede inoltre una connessione Internet in uscita per comunicare con i seguenti endpoint:
 - csa.netapp.com
 - docker.com
 - docker.io

3. Accedere alla ["Sito di supporto NetApp"](#) e registratevi per un account, se non ne avete uno.

Per configurare l'agente e accedere al portale, è necessario disporre di un account NetApp Support Site.

Creare account per i dispositivi FlexPod

Per iniziare, configurare gli account per i dispositivi FlexPod:

- [Creare un account di sola lettura per Cisco UCS Manager](#)
- [Creare un account di sola lettura per gli switch Nexus](#)
- [Creare un account admin per ONTAP](#)
- [Creare un account di sola lettura per VMware](#)
- [Creare un account di sola lettura sull'APIC](#)
- [Concedere i privilegi dell'utente CSA utilizzando un server TACACS+](#)

L'agente utilizza questi account per raccogliere le informazioni di configurazione da ciascun dispositivo.

Creare un account di sola lettura per Cisco UCS Manager

Fasi

1. Accedere a Cisco UCS Manager.
2. Creare un utente autenticato localmente denominato *csa-readonly*.



Tutti i nuovi utenti sono di sola lettura per impostazione predefinita.

Creare un account di sola lettura per gli switch Nexus

Fasi

1. Accedere a ogni switch Nexus utilizzando SSH o Telnet.
2. Accedere alla modalità di configurazione globale:

```
configure terminal
.. Create a new user:
```

```
username [name] password [password] role network-operator
.. Save the configuration:
```

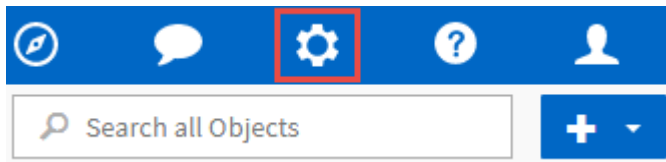
```
copy running configuration startup configuration
```

Se si utilizza un server TACACS+ e si devono concedere privilegi utente CSA, visitare il sito "[Concessione di privilegi utente CSA mediante un server TACACS+](#)".

Creare un account admin per ONTAP

Fasi

1. Accedere a Gestore di sistema di OnCommand e fare clic sull'icona delle impostazioni:



2. Nella pagina utenti, fare clic su **Aggiungi**.
3. Inserire un nome utente e una password e aggiungere **ssh**, **ontapi** e **console** come metodi di accesso utente con accesso admin.

Add User

Username: CSA

Password:

Confirm Password:

User Login Methods

Application	Authentication	Role
console	Password	admin
ssh	Password	admin
ontapi	Password	admin

[Tell me more about roles](#)

Add Cancel

Creare un account di sola lettura per VMware

Fasi

1. Accedere a vCenter.
2. Nel menu vCenter, scegliere **Amministrazione**.
3. In ruoli, scegliere **sola lettura**.
4. Fare clic sull'icona **Clone role action** (Copia azione ruolo) e modificare il nome in **CSA**.
5. Selezionare il ruolo **CSA** appena creato.
6. Fare clic sull'icona **Edit role** (Modifica ruolo).
7. In **Edit role** (Modifica ruolo), scegliere **Global** (Globale), quindi selezionare **Licenses** (licenze).
8. Nella barra laterale, selezionare **Single Sign on**→**Users and groups**→**Create a new user**.
9. Assegnare un nome al nuovo utente **CSARO** nel DOMINIO vpsphere.local.
10. Nella barra laterale, selezionare **permessi globali** in **controllo accessi**.
11. Scegliere l'utente **CSARO** e assegnare IL RUOLO **CSA**.
12. Accedere al client Web.

USA ID utente: **CSARO@vpsphere.local** e password creata in precedenza.

Creare un account di sola lettura sull'APIC

Fasi

1. Fare clic su **Admin**.
2. Fare clic su **Crea nuovi utenti locali**.
3. In **User Identity** (identità utente), immettere le informazioni sull'utente.
4. In **Security** (sicurezza), selezionare tutte le opzioni del dominio di protezione.
5. Fare clic su **+** per aggiungere certificati utente e chiavi SSH, se necessario.
6. Fare clic su **Avanti**.
7. Fare clic su **+** per aggiungere ruoli per il dominio.
8. Selezionare **Nome ruolo** dal menu a discesa.
9. Selezionare **Read** (lettura) per il tipo di privilegio del ruolo **Role Privilege Type** (tipo di privilegio del
10. Fare clic su **fine**.

Concedere i privilegi dell'utente CSA utilizzando un server TACACS+

Se si utilizza un server TACACS+ e si devono concedere privilegi utente CSA per gli switch, creare un gruppo di privilegi utente e concedere al gruppo l'accesso ai comandi di configurazione specifici richiesti da CSA.

I seguenti comandi devono essere scritti nel file di configurazione del server TACACS+.

Fasi

1. Immettere quanto segue per creare un gruppo di privilegi utente con accesso di sola lettura:

```
group=group_name {
  default service=deny
  service=exec{
    priv-lvl=0
  }
}
```

1. Immettere quanto segue per consentire l'accesso ai comandi richiesti da CSA:

```
cmd=show {
  permit "environment"
  permit "version"
  permit "feature"
  permit "feature-set"
  permit hardware.*
  permit "interface"
  permit "interface"
  permit "interface transceiver"
  permit "inventory"
  permit "license"
  permit "module"
  permit "port-channel database"
  permit "ntp peers"
  permit "license usage"
  permit "port-channel summary"
  permit "running-config"
  permit "startup-config"
  permit "running-config diff"
  permit "switchname"
  permit "int mgmt0"
  permit "cdp neighbors detail"
  permit "vlan"
  permit "vpc"
  permit "vpc peer-keepalive"
  permit "mac address-table"
  permit "lACP port-channel"
  permit "policy-map"
  permit "policy-map system type qos"
  permit "policy-map system type queuing"
  permit "policy-map system type network-qos"
  permit "zoneset active"
  permit "san-port-channel summary"
  permit "flogi database"
  permit "fcns database detail"
  permit "fcns database detail"
  permit "zoneset active"
  permit "vsan"
  permit "vsan usage"
  permit "vsan membership"
}
```

1. Immettere quanto segue per aggiungere l'account utente CSA al gruppo appena creato:


```
user=user_account{
  member=group_name
  login=file/etc/passwd
}
```

Configurare e implementare l'agente

È necessario implementare l'agente Converged Systems Advisor su un server VMware ESXi. L'agente raccoglie i dati di configurazione relativi a ciascun dispositivo dell'infrastruttura convergente FlexPod e li invia al portale Converged Systems Advisor.

Fasi

1. [Scaricare e installare l'agente](#)
2. [Impostare la rete per l'agente](#)
3. [Installare un certificato SSL sull'agente](#)
4. [Configurare l'agente per rilevare l'infrastruttura FlexPod](#)

Scaricare e installare l'agente

È necessario implementare l'agente Converged Systems Advisor su un server VMware ESXi.

A proposito di questa attività

Per ridurre al minimo l'utilizzo della larghezza di banda, è necessario installare l'agente su un server VMware ESXi che si trova nello stesso data center della configurazione FlexPod. L'agente deve essere connesso a ciascun componente FlexPod e a Internet in modo da poter inviare i dati di configurazione al portale Converged Systems Advisor utilizzando la porta HTTPS 443.

L'agente viene implementato come macchina virtuale VMware vSphere da un modello OVF (Open Virtualization Format). Il modello è basato su Debian con 1 vCPU e 2 GB di RAM (potrebbe essere necessario un numero maggiore di sistemi FlexPod multipli o maggiori).

Fasi

1. Scarica l'agente:
 - a. Accedere a ["Portale Converged Systems Advisor"](#).
 - b. Fare clic su **Download Agent**.
2. Installare l'agente implementando il modello OVF sul server VMware ESXi.

Su alcune versioni di VMware, potrebbe essere visualizzato un avviso durante l'implementazione del modello OVF. La macchina virtuale è stata sviluppata sulla versione più recente di vCenter con compatibilità hardware per le versioni precedenti, il che potrebbe causare l'avviso. Esaminare le opzioni di configurazione prima di confermare l'avviso e procedere con l'installazione.

Impostare la rete per l'agente

Per consentire la comunicazione tra l'agente e i dispositivi FlexPod e tra l'agente e diversi endpoint Internet, è necessario assicurarsi che la rete sia configurata correttamente sulla macchina virtuale dell'agente. Si noti che

lo stack di rete viene disattivato sulla macchina virtuale fino all'inizializzazione del sistema.

Fasi

1. Assicurarsi che una connessione Internet in uscita consenta l'accesso ai seguenti endpoint:

- csa.netapp.com
- docker.com
- docker.io

2. Accedere alla console della macchina virtuale dell'agente utilizzando il client VMware vSphere.

Il nome utente predefinito è `csa` e la password predefinita è `netapp`.



Per motivi di sicurezza, SSHD è disattivato per impostazione predefinita.

3. Quando richiesto, modificare la password predefinita e prendere nota della password, perché non può essere recuperata.

Dopo aver modificato la password, il sistema si riavvia e avvia il software dell'agente.

4. Se DHCP non è disponibile nella subnet, configurare un indirizzo IP statico e le impostazioni DNS utilizzando gli strumenti standard di Debian, quindi riavviare l'agente.

["Fare clic qui per istruzioni dettagliate"](#).

La configurazione di rete per la macchina virtuale Debian è DHCP per impostazione predefinita. NetworkManager è installato e fornisce un'interfaccia utente di testo che è possibile avviare dal comando `nmtui` (vedere la ["pagina man"](#) per ulteriori dettagli).

Per ulteriori informazioni sulla rete, vedere ["La pagina di configurazione di rete nel wiki Debian"](#).

5. Se le policy di sicurezza stabiliscono che l'agente deve trovarsi su una rete per comunicare con i dispositivi FlexPod e un'altra rete per comunicare con Internet, aggiungere una seconda interfaccia di rete in vCenter e configurare le VLAN e gli indirizzi IP corretti.

6. Se per l'accesso a Internet è necessario un server proxy, eseguire il seguente comando:

```
sudo csa_set_proxy
```

Il comando genera due prompt e mostra il formato richiesto per la voce del proxy. Il primo prompt consente di specificare un proxy HTTP, mentre il secondo consente di specificare un proxy HTTPS.

Immettere il proxy HTTP seguente utilizzando il formato:

```
http://user:password@proxy-server:proxy-port
```

Lasciare vuoto se non è richiesto alcun proxy HTTP per l'accesso a Internet.

7. Una volta attivata la rete, attendere circa 5 minuti per l'aggiornamento e l'avvio del sistema.

Quando l'agente è operativo, sulla console viene visualizzato un messaggio broadcast.

8. Verificare la connettività eseguendo il seguente comando CLI dall'agente:

```
curl -k https://www.netapp.com/us/index.aspx
```

Se il comando non riesce, verificare le impostazioni DNS. La macchina virtuale dell'agente deve avere una configurazione DNS valida e la capacità di raggiungere `csa.netapp.com`.

Installare un certificato SSL sull'agente

Facoltativo: Se necessario, installare un certificato SSL sull'agente.

L'agente crea un certificato autofirmato al primo avvio della macchina virtuale. Se necessario, è possibile eliminare il certificato e utilizzare il proprio certificato SSL.

A proposito di questa attività

Converged Systems Advisor supporta quanto segue: * Qualsiasi crittografia compatibile con OpenSSL versione 1.0.1 o superiore * TLS 1.1 e TLS 1.2

Fasi

1. Accedere alla console della macchina virtuale dell'agente.
2. Selezionare `/opt/csa/certs`
3. Eliminare il certificato autofirmato creato dall'agente.
4. Incollare il certificato SSL.
5. Riavviare la macchina virtuale.

Configurare l'agente per rilevare l'infrastruttura FlexPod

È necessario configurare l'agente in modo che raccolga i dati di configurazione da ciascun dispositivo nell'infrastruttura convergente FlexPod. L'agente richiede credenziali per raccogliere i dati di configurazione. Quando si configura l'agente, è necessario fornire le credenziali.

Fasi

1. Aprire un browser Web e inserire l'indirizzo IP della macchina virtuale dell'agente.
2. Accedere all'agente con il nome utente e la password dell'account NetApp Support Site del cliente.



Per tutti i partner che implementano una versione concessa in licenza di CSA per conto del cliente, è importante che l'account del cliente venga utilizzato in questa fase (per il supporto NetApp e la gestione dei record).

3. Aggiungere i dispositivi FlexPod che l'agente deve rilevare.

Sono disponibili due opzioni:

- a. Fare clic su **Aggiungi un dispositivo** per immettere i dettagli relativi ai dispositivi FlexPod, uno alla volta.
- b. Fare clic su **Import Devices** (Importa dispositivi) per compilare e caricare un modello CSV che include i dettagli su tutti i dispositivi.

Nota: * Il nome utente e la password devono corrispondere all'account creato in precedenza per la periferica. * Se nell'ambiente UCS è configurata la gestione utente LDAP, è necessario aggiungere il

dominio dell'utente prima del nome utente. Ad esempio: Locale/csa-readonly

Risultato

Ogni dispositivo nell'infrastruttura FlexPod deve essere visualizzato nella tabella con un segno di spunta.

Your devices list

Minimum required FlexPod configuration - 1 NetApp ONTAP, 2 Cisco Nexus and 1 Cisco UCS.

Device Type	Host Name	IP Address	Last Updated	Status
VMWare vCenter	10.61.184.230	10.61.184.230	7/12/18, 1:39 PM	✓
UCS	10.61.186.134	10.61.186.134	7/12/18, 1:36 PM	✓
NetApp ONTAP	10.61.186.82	10.61.186.82	7/12/18, 1:35 PM	✓
Cisco Nexus	10.61.186.81	10.61.186.81	7/12/18, 1:35 PM	✓
Cisco Nexus	10.61.186.80	10.61.186.80	7/12/18, 1:34 PM	✓

Aggiungere l'infrastruttura al portale

Dopo aver configurato l'agente, invia le informazioni relative a ciascun dispositivo FlexPod al portale Converged Systems Advisor. È ora necessario selezionare ciascuno di questi componenti nel portale per creare un'intera infrastruttura che è possibile monitorare.

Fasi

1. In ["Portale Converged Systems Advisor"](#), Fare clic su **Aggiungi infrastruttura**.
2. Completare la procedura per aggiungere l'infrastruttura:
 - a. Inserire i dettagli di base sull'infrastruttura.

Se si sta aggiungendo un'infrastruttura Cisco ACI, inserire **yes** quando viene richiesto se il FlexPod utilizza Cisco UCS Manager e inserire **Nexus switch in modalità ACI** quando viene richiesto il tipo di configurazione di rete in cui si trova il FlexPod.

- b. Selezionare ciascun dispositivo che fa parte della configurazione FlexPod.



Quando si seleziona un dispositivo, la colonna idoneità visualizza **idoneo** o **non idoneo**. Un dispositivo non è idoneo se rilevato da un altro agente.

3. Dopo aver selezionato tutti i componenti richiesti, viene visualizzato un segno di spunta verde accanto a ciascun tipo di dispositivo.

Device Name	Device IP	Device Type	Serial No.	CI Name	Eligibility	Agent Status	FlexPod Validation Criteria
<input checked="" type="checkbox"/> ACI Fabric1	10.61.186.190	ACI APIC	WZP23140FFB	Pikes_ACI	✓ Eligible	Online	✓ 1 Cisco UCS Manager
<input checked="" type="checkbox"/> stack4-fas	10.61.183.249	Ontap	701510000664-701510000665	Pikes_ACI	✓ Eligible	Online	✓ 1 Cisco ACI APIC
<input checked="" type="checkbox"/> stack4	10.61.186.244	UCS	FOX2010G275-FOX2013G9ZS	Pikes_ACI	✓ Eligible	Online	✓ 1 NetApp ONTAP Cluster ✓ 0 or 1 VMware vCenter

- a. Aggiungere il ["Numero di serie di Converged Systems Advisor"](#) per sbloccare la funzionalità delle

chiavi.

- b. Leggere il riepilogo, accettare i termini del contratto di licenza e fare clic su **Add Infrastructure** (Aggiungi infrastruttura).



Se sei un partner o un rivenditore, puoi saltare la procedura relativa all'aggiunta di una licenza o di un numero di serie e fare clic su **Add Infrastructure** (Aggiungi infrastruttura).

Risultato

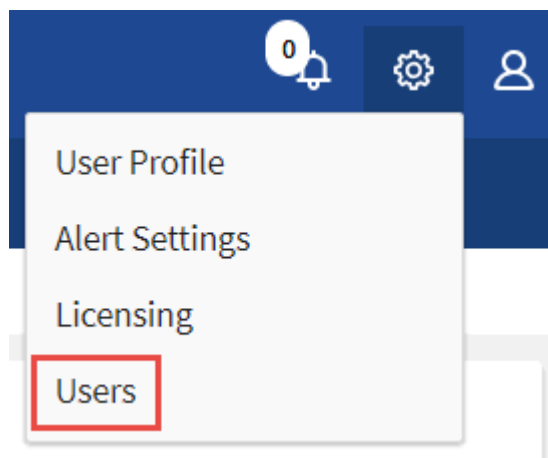
Converged Systems Advisor aggiunge l'infrastruttura al portale e inizia a raccogliere i dati di configurazione relativi a ciascun dispositivo. Attendere alcuni minuti per consentire all'agente di raccogliere informazioni dai dispositivi.


Condivisione di un'infrastruttura con altri utenti

La condivisione di un'infrastruttura convergente consente a un'altra persona di accedere al portale Converged Systems Advisor per visualizzare e monitorare la configurazione. La persona con cui condividi l'infrastruttura deve disporre di un "Sito di supporto NetApp" account.

Fasi

1. Nel portale Converged Systems Advisor, fare clic sull'icona **Impostazioni**, quindi su **utenti**.



2. Selezionare la configurazione dalla tabella User (utente).
3. Fare clic su  icona.
4. Inserire uno o più indirizzi e-mail accanto al ruolo utente che si desidera fornire.

"Visualizzare le differenze tra ciascun ruolo".



È possibile inserire più indirizzi e-mail in un singolo campo premendo **Invia** dopo il primo indirizzo e-mail.

5. Fare clic su **Invia**.

Risultato

L'utente deve ricevere un'e-mail contenente le istruzioni per l'accesso a Converged Systems Advisor.

Configurare le notifiche

Se disponi di una licenza Premium, Converged Systems Advisor ti avvisa in caso di modifiche all'infrastruttura FlexPod tramite notifiche via email.

Fasi

1. Nel portale Converged Systems Advisor, fare clic sull'icona **Impostazioni**, quindi su **Impostazioni avvisi**.
2. Controllare la notifica che si desidera ricevere per ogni infrastruttura convergente che dispone di una licenza Premium.

Ciascuna notifica include le seguenti informazioni:

Errori di raccolta

Avvisa l'utente quando Converged Systems Advisor non è in grado di raccogliere dati da un'infrastruttura convergente.

Agente offline

Avvisa l'utente quando un agente di Converged Systems Advisor non è online.

Daily Alert Digest

Avvisa l'utente in merito alle regole non riuscite che si sono verificate il giorno precedente.

3. Fare clic su **Save** (Salva).

Risultato

Converged Systems Advisor invierà ora notifiche e-mail agli utenti associati all'infrastruttura convergente.

Impostare un indirizzo IP statico sull'agente

Se l'ambiente non dispone di un server DHCP, è possibile impostare un indirizzo IP statico nell'agente Converged Systems Advisor.

Fasi

1. Accedere alla console della macchina virtuale dell'agente utilizzando il client VMware vSphere.

Il nome utente predefinito è **csa** e la password predefinita è **netapp**. Modificare la password, se richiesto.

2. Invio `sudo su -` al prompt `csa` di diventare root.
3. Invio `# systemctl stop csa.service` Per interrompere il servizio CSA.
4. Immettere quanto segue per determinare il nome corretto del file di interfaccia.

In questo esempio, il nome del file di interfaccia è `eth0`.

```
# ls /etc/network/interfaces.d/
```

5. Invio `# /sbin/ifdown eth0` per interrompere l'interfaccia attiva.
6. Modificare il file `/etc/network/interfaces.d/eth0` con l'editor desiderato.

```
# nano /etc/network/interfaces.d/eth0`oppure
```

```
`# vi /etc/network/interfaces.d/eth0
```

Il file contiene quanto segue:

```
allow-hotplug eth0  
iface eth0 inet dhcp
```

7. Rimuovere `iface eth0 inet dhcp` e aggiungere quanto segue. NOTA: È necessario sostituire i valori corretti per tutte le voci che seguono i nomi dei campi nell'esempio seguente. Ad esempio, `192.168.11.1` è il valore del gateway nell'esempio. Tuttavia, invece di `192.168.11.1`, inserire l'indirizzo corretto per il gateway.

```
iface eth0 inet static  
address 192.168.11.100  
netmask 255.255.255.0  
gateway 192.168.11.1  
dns-domain example.com  
dns-nameservers 192.168.11.1
```

8. Salvare il file.

In nano, inserisci **ctrl + o** seguito da **ctrl + x** per salvare.

9. Invio `vi/etc/resolv.conf` per aprire il file di configurazione.
10. Aggiungi `nameserver <ip_address>` nella parte superiore del file.
11. Invio `# ifup eth0` per avviare l'interfaccia di rete.
12. Invio `systemctl start csa.service` Per riavviare Converged Systems Advisor.

Informazioni sul copyright

Copyright © 2023 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIALIZZABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEGUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina <http://www.netapp.com/TM> sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.