



Pour commencer

Converged Systems Advisor

NetApp
August 13, 2024

Sommaire

- Pour commencer 1
 - Démarrage rapide de Converged Systems Advisor 1
 - Préparez votre environnement 2
 - Créez des comptes pour les périphériques FlexPod 2
 - Configurer et déployer l'agent 7
 - Ajouter une infrastructure au portail 10
 - Partage d'une infrastructure avec d'autres utilisateurs 11
 - Configurez les notifications 12
 - Définissez une adresse IP statique sur l'agent 12

Pour commencer

Démarrage rapide de Converged Systems Advisor

La mise en route du portail et de l'agent Converged Systems Advisor pour FlexPod comprend quelques étapes.

1 Préparez votre environnement

Vérifiez la prise en charge de votre configuration. "[Préparez votre environnement](#)".

2 Créez des comptes sur les terminaux FlexPod

Configurez des comptes dans Cisco UCS Manager, sur vos commutateurs Cisco Nexus, pour vos systèmes ONTAP, pour VMware et pour le contrôleur APIC. Ces comptes sont utilisés par l'agent pour collecter les données de configuration. "[Créez des comptes sur les terminaux FlexPod](#)".

3 Accordez des privilèges utilisateur CSA à l'aide d'un serveur TACACS+

Pour ceux qui utilisent un serveur TACACS+, vous devez accorder des privilèges d'utilisateur CSA pour vos commutateurs, créer un groupe de privilèges d'utilisateur et accorder au groupe l'accès aux commandes de configuration spécifiques requises par CSA. "[Accordez des privilèges utilisateur CSA à l'aide d'un serveur TACACS+](#)".

4 Configurez et déployez l'agent

Déployez l'agent Converged Systems Advisor sur un serveur VMware ESXi. L'agent collecte des données de configuration sur chaque système de votre infrastructure convergée FlexPod et les envoie vers le portail Converged Systems Advisor. "[Déployez l'agent](#)".

5 Ajouter/partager une infrastructure dans le portail

Ajoutez chaque périphérique FlexPod au portail Converged Systems Advisor pour créer une infrastructure complète que vous pouvez surveiller. Vous pouvez également partager une infrastructure convergée pour permettre à une autre personne de se connecter au portail, afin qu'elle puisse afficher et contrôler la configuration. "[Ajouter et partager l'infrastructure dans le portail](#)".

6 Configurez les notifications

Avec une licence Premium, vous pouvez configurer des notifications qui vous signalent les modifications apportées à votre infrastructure FlexPod par le biais de notifications électroniques. "[Configurez les notifications](#)".



Définissez une adresse IP statique

Si votre environnement ne dispose pas d'un serveur DHCP, vous pouvez définir une adresse IP statique sur l'agent Converged Systems Advisor. ["Définissez une adresse IP statique sur l'agent"](#)

Préparez votre environnement

Pour commencer à utiliser Converged Systems Advisor, vous devez préparer votre environnement. La préparation de votre environnement comprend la vérification du support pour votre configuration et la création d'un compte sur le site de support NetApp.

Vous pouvez vouloir le faire ["Découvrez le fonctionnement de Converged Systems Advisor"](#) avant de commencer.

Étapes

1. Vérifier le support dans ["Matrice d'interopérabilité NetApp"](#):
 - a. Vérifiez que Converged Systems Advisor prend en charge l'infrastructure convergée FlexPod.
 - b. Vérifiez que vous disposez d'un serveur VMware ESXi pris en charge par l'agent Converged Systems Advisor.

Pour réduire l'utilisation de la bande passante, NetApp recommande d'installer l'agent dans le même data Center que l'infrastructure convergée FlexPod.

2. Assurez-vous que le réseau dans lequel vous installez l'agent autorise la connectivité entre les composants :
 - L'agent doit être connecté à chaque composant FlexPod afin qu'il puisse collecter des données de configuration.
 - L'agent nécessite également une connexion Internet sortante pour communiquer avec les noeuds finaux suivants :
 - csa.netapp.com
 - docker.com
 - docker.io

3. Accédez au ["Site de support NetApp"](#) et vous inscrire pour créer un compte, si vous n'en avez pas.

Un compte sur le site de support NetApp est nécessaire pour configurer l'agent et accéder au portail.

Créez des comptes pour les périphériques FlexPod

Pour commencer, configurez des comptes pour les appareils FlexPod :

- [Créez un compte en lecture seule pour Cisco UCS Manager](#)
- [Créez un compte en lecture seule pour les commutateurs Nexus](#)
- [Créez un compte admin pour ONTAP](#)
- [Créez un compte en lecture seule pour VMware](#)
- [Créez un compte en lecture seule sur le contrôleur APIC](#)

- [Accordez des privilèges utilisateur CSA à l'aide d'un serveur TACACS+](#)

L'agent utilise ces comptes pour recueillir des informations de configuration de chaque périphérique.

Créez un compte en lecture seule pour Cisco UCS Manager

Étapes

1. Connectez-vous à Cisco UCS Manager.
2. Créez un utilisateur authentifié localement nommé *csa-readonly*.



Par défaut, tous les nouveaux utilisateurs sont en lecture seule.

Créez un compte en lecture seule pour les commutateurs Nexus

Étapes

1. Connectez-vous à chaque commutateur Nexus à l'aide de SSH ou Telnet.
2. Passer en mode de configuration globale :

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

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

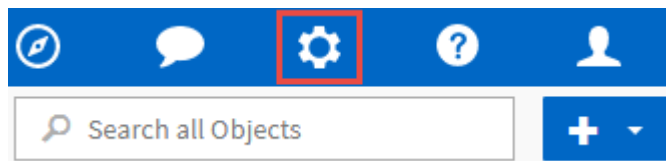
```
copy running configuration startup configuration
```

Si vous utilisez un serveur TACACS+ et que vous devez accorder des privilèges d'utilisateur CSA, rendez-vous sur "[Octroi de privilèges utilisateur CSA à l'aide d'un serveur TACACS+](#)".

Créez un compte admin pour ONTAP

Étapes

1. Connectez-vous à OnCommand System Manager et cliquez sur l'icône Paramètres :



2. Sur la page utilisateurs, cliquez sur **Ajouter**.
3. Entrez un nom d'utilisateur et un mot de passe et ajoutez **ssh**, **ontapi** et **console** comme méthodes de connexion utilisateur avec accès administrateur.

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

Créez un compte en lecture seule pour VMware

Étapes

1. Connectez-vous à vCenter.
2. Dans le menu vCenter, choisissez **Administration**.
3. Sous rôles, choisissez **lecture seule**.
4. Cliquez sur l'icône de l'action **Clone role** et remplacez le nom par **CSA**.
5. Sélectionnez le rôle **CSA** nouvellement créé.
6. Cliquez sur l'icône **Modifier le rôle**.
7. Sous **Modifier le rôle**, choisissez **Global**, puis cochez **licences**.
8. Dans la barre latérale, sélectionnez **Single Sign On** → **utilisateurs et groupes** → **Créer un nouvel utilisateur**.
9. Nommez le nouvel utilisateur **CSARO** sous DOMAINE **vsphere.local**.
10. Dans la barre latérale, sélectionnez **autorisations globales** sous **contrôle d'accès**.
11. Choisissez l'utilisateur **CSARO** et attribuez LE RÔLE **CSA**.
12. Connectez-vous au client Web.

Utilisez l'ID utilisateur : **CSARO@vsphere.locksbsbl** et le mot de passe précédemment créé.

Créez un compte en lecture seule sur le contrôleur APIC

Étapes

1. Cliquez sur **Admin**.
2. Cliquez sur **Créer de nouveaux utilisateurs locaux**.
3. Sous **User Identity**, entrez les informations utilisateur.
4. Sous **sécurité**, sélectionnez toutes les options de domaine de sécurité.
5. Cliquez sur **+** pour ajouter des certificats utilisateur et des clés SSH si nécessaire.
6. Cliquez sur **Suivant**.
7. Cliquez sur **+** pour ajouter des rôles pour votre domaine.
8. Sélectionnez **Nom du rôle** dans le menu déroulant.
9. Sélectionnez **Lire** pour le **Type de privilège de rôle**.
10. Cliquez sur **Terminer**.

Accordez des privilèges utilisateur CSA à l'aide d'un serveur TACACS+

Si vous utilisez un serveur TACACS+ et que vous devez accorder des privilèges d'utilisateur CSA à vos commutateurs, vous devez créer un groupe de privilèges d'utilisateur et accorder au groupe l'accès aux commandes de configuration spécifiques requises par CSA.

Les commandes suivantes doivent être écrites dans le fichier de configuration de votre serveur TACACS+.

Étapes

1. Saisissez les éléments suivants pour créer un groupe de privilèges d'utilisateur avec accès en lecture seule :

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

1. Entrez ce qui suit pour autoriser l'accès aux commandes requises par 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. Entrez ce qui suit pour ajouter votre compte d'utilisateur CSA au nouveau groupe créé :


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

Configurer et déployer l'agent

Vous devez déployer l'agent Converged Systems Advisor sur un serveur VMware ESXi. L'agent collecte des données de configuration sur chaque système de votre infrastructure convergée FlexPod et les envoie vers le portail Converged Systems Advisor.

Étapes

1. [Téléchargez et installez l'agent](#)
2. [Configurer la mise en réseau de l'agent](#)
3. [Installez un certificat SSL sur l'agent](#)
4. [Configurez l'agent pour découvrir votre infrastructure FlexPod](#)

Téléchargez et installez l'agent

Vous devez déployer l'agent Converged Systems Advisor sur un serveur VMware ESXi.

Description de la tâche

Pour réduire l'utilisation de la bande passante, vous devez installer l'agent sur un serveur VMware ESXi situé dans le même centre de données que la configuration FlexPod. L'agent doit être connecté à chaque composant FlexPod et à Internet afin que les données de configuration puissent être envoyées au portail Converged Systems Advisor via le port HTTPS 443.

L'agent est déployé en tant que machine virtuelle VMware vSphere à partir d'un modèle OVF (Open Virtualization format). Le modèle est basé sur Debian avec 1 CPU virtuel et 2 Go de RAM (plus peut être nécessaire pour les systèmes FlexPod multiples ou plus grands).

Étapes

1. Téléchargez l'agent :
 - a. Connectez-vous au "[Portail Converged Systems Advisor](#)".
 - b. Cliquez sur **Download Agent**.
2. Installez l'agent en déployant le modèle OVF sur le serveur VMware ESXi.

Sur certaines versions de VMware, un avertissement peut s'afficher lors du déploiement du modèle OVF. La machine virtuelle a été développée à partir de la dernière version de vCenter avec une compatibilité matérielle pour les versions plus anciennes, ce qui peut entraîner un avertissement. Il est recommandé de passer en revue les options de configuration avant d'accuser réception de l'avertissement, puis de poursuivre l'installation.

Configurer la mise en réseau de l'agent

Vous devez vous assurer que la mise en réseau est correctement configurée sur la machine virtuelle de l'agent

pour permettre la communication entre l'agent et les périphériques FlexPod et entre l'agent et plusieurs points de terminaison Internet. Notez que la pile réseau est désactivée sur la machine virtuelle jusqu'à ce que le système s'initialise.

Étapes

1. Assurez-vous qu'une connexion Internet sortante permet d'accéder aux points de terminaison suivants :
 - `csa.netapp.com`
 - `docker.com`
 - `docker.io`
2. Connectez-vous à la console de la machine virtuelle de l'agent à l'aide du client VMware vSphere.

Le nom d'utilisateur par défaut est `csa` et le mot de passe par défaut est `netapp`.



Pour des raisons de sécurité, SSHD est désactivé par défaut.

3. Lorsque vous y êtes invité, modifiez le mot de passe par défaut et notez le mot de passe, car il ne peut pas être récupéré.

Après avoir modifié le mot de passe, le système redémarre et démarre le logiciel de l'agent.

4. Si DHCP n'est pas disponible dans le sous-réseau, configurez une adresse IP statique et des paramètres DNS à l'aide des outils Debian standard, puis redémarrez l'agent.

["Cliquez ici pour obtenir des instructions détaillées"](#).

Par défaut, la configuration réseau de la machine virtuelle Debian est DHCP. NetworkManager est installé et fournit une interface utilisateur texte que vous pouvez démarrer à partir de la commande `nmtui` (voir ["page de manuel"](#) pour en savoir plus).

Pour obtenir de l'aide supplémentaire sur la mise en réseau, voir ["La page de configuration réseau sur le wiki Debian"](#).

5. Si vos stratégies de sécurité exigent que l'agent se trouve sur un réseau pour communiquer avec les périphériques FlexPod et un autre réseau pour communiquer avec Internet, ajoutez une deuxième interface réseau dans vCenter et configurez les VLAN et les adresses IP corrects.
6. Si un serveur proxy est requis pour l'accès à Internet, exécutez la commande suivante :

```
sudo csa_set_proxy
```

La commande génère deux invites et affiche le format requis pour l'entrée de proxy. La première invite vous permet de spécifier un proxy HTTP, tandis que la seconde vous permet de spécifier un proxy HTTPS.

Entrez le proxy HTTP ci-dessous au format suivant :

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

Laissez ce champ vide si aucun proxy HTTP n'est requis pour l'accès à Internet.

7. Une fois le réseau en marche, attendez environ 5 minutes pour que le système se mette à jour et démarre.

Un message de diffusion apparaît sur la console lorsque l'agent est opérationnel.

8. Vérifiez la connectivité en exécutant la commande CLI suivante à partir de l'agent :

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

Si la commande échoue, vérifiez les paramètres DNS. La machine virtuelle de l'agent doit être dotée d'une configuration DNS valide et pouvoir atteindre csa.netapp.com.

Installez un certificat SSL sur l'agent

Facultatif : si nécessaire, installez un certificat SSL sur l'agent.

L'agent crée un certificat auto-signé lors du premier démarrage de la machine virtuelle. Si nécessaire, vous pouvez supprimer ce certificat et utiliser votre propre certificat SSL.

Description de la tâche

Converged Systems Advisor prend en charge : * tout chiffrement compatible avec OpenSSL version 1.0.1 ou ultérieure * TLS 1.1 et TLS 1.2

Étapes

1. Connectez-vous à la console de la machine virtuelle de l'agent.
2. Accédez à `/opt/csa/certs`
3. Supprimez le certificat auto-signé que l'agent a créé.
4. Collez votre certificat SSL.
5. Redémarrez la machine virtuelle.

Configurez l'agent pour découvrir votre infrastructure FlexPod

Vous devez configurer l'agent pour qu'il collecte les données de configuration de chaque périphérique de votre infrastructure convergée FlexPod. L'agent nécessite des informations d'identification pour collecter les données de configuration. Vous devez fournir les informations d'identification lors de la configuration de l'agent.

Étapes

1. Ouvrez un navigateur Web et saisissez l'adresse IP de la machine virtuelle de l'agent.
2. Connectez-vous à l'agent avec le nom d'utilisateur et le mot de passe du compte sur le site de support NetApp du client.



Pour tout partenaire qui déploie une version sous licence de CSA pour le compte de son client, il est important que le compte du client soit utilisé à cette étape (pour le support NetApp et la gestion des enregistrements).

3. Ajoutez les périphériques FlexPod que l'agent doit détecter.

Vous avez deux options :

- a. Cliquez sur **Ajouter un périphérique** pour entrer des détails sur vos périphériques FlexPod, un par un.
- b. Cliquez sur **Importer les périphériques** pour remplir et télécharger un modèle CSV qui contient des détails sur tous les périphériques.

Remarque : * le nom d'utilisateur et le mot de passe doivent correspondre au compte que vous avez

créé précédemment pour le terminal. * Si la gestion des utilisateurs LDAP est configurée dans votre environnement UCS, vous devez ajouter le domaine de l'utilisateur avant le nom d'utilisateur. Par exemple : local\csa-readonly

Résultat

Chaque périphérique de l'infrastructure FlexPod doit être coché dans le tableau.

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	✓

Ajouter une infrastructure au portail

Une fois l'agent configuré, il envoie des informations relatives à chaque périphérique FlexPod au portail Converged Systems Advisor. Vous devez maintenant sélectionner chacun de ces composants sur le portail pour créer une infrastructure complète que vous pouvez surveiller.

Étapes

1. Dans le "Portail Converged Systems Advisor", Cliquez sur **Ajouter une infrastructure**.
2. Suivez les étapes pour ajouter l'infrastructure :
 - a. Saisissez les informations de base sur l'infrastructure.

Si vous ajoutez une infrastructure Cisco ACI, entrez **yes** lorsque le système FlexPod utilise Cisco UCS Manager et entrez **commutateur Nexus en mode ACI** lorsqu'on vous demande le type de configuration réseau contenu par votre FlexPod.

- b. Sélectionnez chaque périphérique faisant partie de la configuration FlexPod.



Lorsque vous sélectionnez un périphérique, la colonne éligibilité affiche **éligible** ou **non éligible**. Un périphérique n'est pas éligible s'il a été découvert par un autre agent.

3. Après avoir sélectionné tous les composants requis, une coche verte s'affiche en regard de chaque type de périphérique.

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	<ul style="list-style-type: none"> ✓ 1 Cisco UCS Manager ✓ 1 Cisco ACI APIC ✓ 1 NetApp ONTAP Cluster ✓ 0 or 1 VMware vCenter
<input checked="" type="checkbox"/> stack4-fas	10.61.183.249	Ontap	701510000664-701510000665	Pikes_ACI	✓ Eligible	Online	
<input checked="" type="checkbox"/> stack4	10.61.186.244	UCS	FOX2010G275-FOX2013G9ZS	Pikes_ACI	✓ Eligible	Online	

- a. Ajoutez votre "Numéro de série de Converged Systems Advisor" pour déverrouiller la fonctionnalité des touches.
- b. Passez en revue le résumé, acceptez les termes du contrat de licence et cliquez sur **Ajouter une infrastructure**.



Si vous êtes un partenaire ou un revendeur, vous pouvez ignorer les étapes d'ajout d'une licence ou d'un numéro de série et simplement cliquer sur **Ajouter une infrastructure**.

Résultat

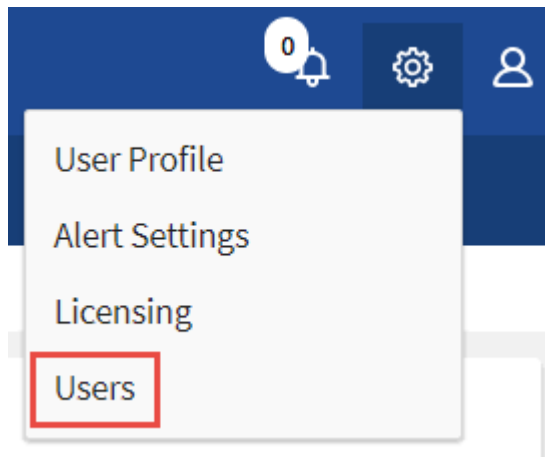
Converged Systems Advisor ajoute l'infrastructure au portail et commence à collecter les données de configuration sur chaque périphérique. Attendez quelques minutes pour que l'agent collecte des informations sur les périphériques.


Partage d'une infrastructure avec d'autres utilisateurs

Le partage d'une infrastructure convergée permet à une autre personne de se connecter au portail Converged Systems Advisor pour qu'elle puisse afficher et contrôler la configuration. La personne avec laquelle vous partagez l'infrastructure doit avoir un "Site de support NetApp" compte.

Étapes

1. Dans le portail Converged Systems Advisor, cliquez sur l'icône **Paramètres**, puis sur **utilisateurs**.



2. Sélectionnez la configuration dans le tableau utilisateur.
3. Cliquez sur le bouton  icône.
4. Saisissez une ou plusieurs adresses e-mail en regard du rôle d'utilisateur que vous souhaitez fournir.

["Afficher les différences entre chaque rôle"](#).



Vous pouvez entrer plusieurs adresses e-mail dans un seul champ en appuyant sur **entrée** après la première adresse e-mail.

5. Cliquez sur **Envoyer**.

Résultat

L'utilisateur doit recevoir un e-mail contenant les instructions pour accéder à Converged Systems Advisor.

Configurez les notifications

Si vous disposez d'une licence Premium, Converged Systems Advisor vous informe des modifications apportées à votre infrastructure FlexPod par l'intermédiaire de notifications par e-mail.

Étapes

1. Dans le portail Converged Systems Advisor, cliquez sur l'icône **Paramètres**, puis sur **Paramètres d'alerte**.
2. Cochez la notification que vous souhaitez recevoir pour chaque infrastructure convergée avec une licence Premium.

Chaque notification comprend les informations suivantes :

Échecs de collecte

Vous avertit lorsque Converged Systems Advisor ne peut pas collecter de données dans une infrastructure convergée.

Agent hors ligne

Vous alerte lorsqu'un agent Converged Systems Advisor n'est pas en ligne.

Résumé quotidien des alertes

Vous signale les échecs de règles qui se sont produits le jour précédent.

3. Cliquez sur **Enregistrer**.

Résultat

Converged Systems Advisor enverra désormais des notifications par e-mail aux utilisateurs associés à l'infrastructure convergée.

Définissez une adresse IP statique sur l'agent

Si votre environnement ne dispose pas d'un serveur DHCP, vous pouvez définir une adresse IP statique sur l'agent Converged Systems Advisor.

Étapes

1. Connectez-vous à la console de la machine virtuelle de l'agent à l'aide du client VMware vSphere.

Le nom d'utilisateur par défaut est **csa** et le mot de passe par défaut est **netapp**. Modifiez le mot de passe, si vous y êtes invité.

2. Entrez `sudo su -` à l'invite `csa` pour devenir `root`.
3. Entrez `# systemctl stop csa.service` Pour arrêter le service CSA.
4. Entrez ce qui suit pour déterminer le nom correct du fichier d'interface.

Dans cet exemple, le nom du fichier d'interface est `eth0`.

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

5. Entrez `# /sbin/ifdown eth0` pour arrêter l'interface active.

6. Modifiez le fichier `/etc/network/interfaces.d/eth0` avec l'éditeur de votre choix.

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

Le fichier contient les éléments suivants :

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

7. Déposer `iface eth0 inet dhcp` et ajoutez les éléments suivants. REMARQUE : vous devez remplacer les valeurs correctes par celles de toutes les entrées qui suivent les noms de champs dans l'exemple ci-dessous. Par exemple : `192.168.11.1` est la valeur de la passerelle dans l'exemple. Cependant, au lieu de `192.168.11.1`, vous devez saisir l'adresse correcte pour votre passerelle.

```
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. Enregistrez le fichier.

Dans nano, vous entrez **ctrl + o**, suivi de **ctrl + x** pour enregistrer.

9. Entrez `vi/etc/resolv.conf` pour ouvrir le fichier de configuration.

10. Autres `nameserver <ip_address>` en haut du fichier.

11. Entrez `# ifup eth0` pour démarrer l'interface réseau.

12. Entrez `systemctl start csa.service` Pour redémarrer Converged Systems Advisor.

Informations sur le copyright

Copyright © 2024 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTEUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site <http://www.netapp.com/TM> sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.