

PUCE D'ESSAI 1

Introduction

Ce document décrit comment configurer un rôle Nexus personnalisé pour TACACS via CLI sur NK9.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- TACACS+
- ISE 3.2

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Cisco Nexus9000, fichier image NXOS : bootflash:///nxos.9.3.5.bin
- Identity Service Engine version 3.2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Informations générales

Conditions de licence

Cisco NX-OS - TACACS+ ne nécessite aucune licence.

Cisco Identity Service Engine

Pour les nouvelles installations ISE, vous disposez d'une licence d'évaluation de 90 jours qui a accès à toutes les fonctionnalités ISE. Si vous ne disposez pas d'une licence d'évaluation, vous devez disposer d'une licence d'administration de périphérique pour le noeud Policy Server qui effectue l'authentification afin d'utiliser la fonctionnalité ISE TACACS.

Une fois que les utilisateurs Admin/Help Desk se sont authentifiés sur le périphérique Nexus, ISE renvoie le rôle d'interpréteur de commandes Nexus souhaité.

L'utilisateur auquel ce rôle est attribué peut effectuer un dépannage de base et renvoyer certains ports.

La session TACACS qui obtient le rôle Nexus doit être en mesure d'utiliser et d'exécuter uniquement les commandes et actions suivantes :

- Accès pour configurer le terminal pour exécuter UNIQUEMENT les interfaces d'arrêt et aucune interface d'arrêt à partir du 1/1-1/21 et du 1/25-1/30
- ssh
- ssh6
- telnet
- Telnet6
- Traceroute
- Traceroute6
- Ping
- Ping6
- Activer

Configurer

Diagramme du réseau

Étape 1: Configuration du Nexus 9000

1. Configurez AAA.

Avertissement : Après avoir activé l'authentification TACACS, le périphérique Nexus cesse d'utiliser l'authentification locale et commence à utiliser l'authentification basée sur le serveur AAA.

```
Nexus9000(config)# feature tacacs+
Nexus9000(config)# tacacs-server host <Your ISE IP> key 0 Nexus3xample
Nexus9000(config)# tacacs-server key 0 "Nexus3xample"
Nexus9000(config)# aaa group server tacacs+ IsePsnServers
Nexus9000(config-tacacs+ )# server <Your ISE IP>
Nexus9000(config)# aaa authentication login default group IsePsnServers local
```

2. Configurez le rôle personnalisé avec les exigences spécifiées.

```
Nexus9000(config)# role name helpdesk
Nexus9000(config-role)# description Can perform basic Troubleshooting and bounce certain ports
Nexus9000(config-role)# rule 1 permit read
Nexus9000(config-role)# rule 2 permit command enable *
Nexus9000(config-role)# rule 3 permit command ssh *
Nexus9000(config-role)# rule 4 permit command ssh6 *
```

```
Nexus9000(config-role)# rule 5 permit command ping *
Nexus9000(config-role)# rule 6 permit command ping6 *
Nexus9000(config-role)# rule 7 permit command telnet *
Nexus9000(config-role)# rule 8 permit command traceroute *
Nexus9000(config-role)# rule 9 permit command traceroute6 *
Nexus9000(config-role)# rule 10 permit command telnet6 *
Nexus9000(config-role)# rule 11 permit command config t ; interface * ; shutdown
Nexus9000(config-role)# rule 12 permit command config t ; interface * ; no shutdown
```

```
vlan policy deny
interface policy deny
```

```
Nexus9000(config-role-interface)# permit interface Ethernet1/1
Nexus9000(config-role-interface)# permit interface Ethernet1/2
Nexus9000(config-role-interface)# permit interface Ethernet1/3
Nexus9000(config-role-interface)# permit interface Ethernet1/4
Nexus9000(config-role-interface)# permit interface Ethernet1/5
Nexus9000(config-role-interface)# permit interface Ethernet1/6
Nexus9000(config-role-interface)# permit interface Ethernet1/7
Nexus9000(config-role-interface)# permit interface Ethernet1/8
Nexus9000(config-role-interface)# permit interface Ethernet1/8
Nexus9000(config-role-interface)# permit interface Ethernet1/9
Nexus9000(config-role-interface)# permit interface Ethernet1/10
Nexus9000(config-role-interface)# permit interface Ethernet1/11
Nexus9000(config-role-interface)# permit interface Ethernet1/12
Nexus9000(config-role-interface)# permit interface Ethernet1/13
Nexus9000(config-role-interface)# permit interface Ethernet1/14
Nexus9000(config-role-interface)# permit interface Ethernet1/15
Nexus9000(config-role-interface)# permit interface Ethernet1/16
Nexus9000(config-role-interface)# permit interface Ethernet1/17
Nexus9000(config-role-interface)# permit interface Ethernet1/18
Nexus9000(config-role-interface)# permit interface Ethernet1/19
Nexus9000(config-role-interface)# permit interface Ethernet1/20
Nexus9000(config-role-interface)# permit interface Ethernet1/21
Nexus9000(config-role-interface)# permit interface Ethernet1/22
Nexus9000(config-role-interface)# permit interface Ethernet1/25
Nexus9000(config-role-interface)# permit interface Ethernet1/26
Nexus9000(config-role-interface)# permit interface Ethernet1/27
Nexus9000(config-role-interface)# permit interface Ethernet1/28
Nexus9000(config-role-interface)# permit interface Ethernet1/29
Nexus9000(config-role-interface)# permit interface Ethernet1/30
```

```
Nexus9000# copy running-config startup-config
[#####] 100%
Copy complete, now saving to disk (please wait)...
```

Copy complete.

Étape 2 : configuration du moteur Identity Service Engine 3.2

1. Configurez l'identité utilisée pendant la session Nexus TACACS.

L'authentification locale ISE est utilisée.

Accédez à l'onglet Administration > Identity Management > Groups et créez le groupe dont l'utilisateur a besoin pour faire partie, le groupe d'identité créé pour cette démonstration est iseUsers.

Cliquez sur le bouton Envoyer.

Accédez ensuite à Administration > Gestion des identités > onglet Identity.

Cliquez sur le bouton Ajouter.

Dans le cadre des champs obligatoires, commencez par le nom de l'utilisateur, le nom d'utilisateur iseiscool est utilisé dans cet exemple.

L'étape suivante consiste à attribuer un mot de passe au nom d'utilisateur créé. VainillaISE97 est le mot de passe utilisé dans cette démonstration.

Enfin, affectez l'utilisateur au groupe précédemment créé, qui est dans ce cas iseUsers.

2. Configurez et ajoutez le périphérique réseau.

Ajout du périphérique NEXUS 9000 à l'administration ISE > Ressources réseau > Périphériques réseau

Cliquez sur le bouton Add afin de démarrer.

Entrez les valeurs dans le formulaire, attribuez un nom au NAD que vous créez et une adresse IP à partir de laquelle le NAD contacte ISE pour la conversation TACACS.

Les options de la liste déroulante peuvent être laissées vides et peuvent être omises. Ces options sont destinées à classer vos NAD par emplacement, type de périphérique, version, puis à modifier le flux d'authentification en fonction de ces filtres.

Dans Administration > Network Resources > Network Devices > Your NAD > TACACS Authentication Settings, ajoutez le secret partagé que vous avez utilisé dans votre configuration NAD. Nexus3example est utilisé dans cette démonstration.

Enregistrez les modifications en cliquant sur le bouton Envoyer.

3. Configurez TACACS sur ISE.

Vérifiez à nouveau que l'option Device Admin est activée sur le PSN que vous avez configuré dans le Nexus 9k.

Remarque : L'activation du service d'administration de périphériques n'entraîne PAS de redémarrage sur ISE.

Vous pouvez le vérifier dans le menu ISE Administration > System > Deployment > Your PSN > Policy Server section > Enable Device Admin Services.

- Créez un profil TACACS, qui renvoie le centre d'assistance aux rôles au périphérique Nexus si l'authentification réussit.

Dans le menu ISE, accédez à Workcenters > Device Administration > Policy Elements > Results >

TACACS Profiles et cliquez sur le bouton Add.

Attribuez un nom et éventuellement une description.

Ignorez la section Vue des attributs de tâche et accédez à la section Vue brute.

Et entrez la valeur shell : roles="helpdesk".

Configurez l'ensemble de stratégies qui inclut la stratégie d'authentification et la stratégie d'autorisation.

Dans le menu ISE, accédez à Work Centers > Device Administration > Device Admin Policy Sets.

À des fins de démonstration, le jeu de stratégies par défaut est utilisé. Cependant, un autre jeu de stratégies peut être créé, avec des conditions pour correspondre à des scénarios spécifiques.

Cliquez sur la flèche à la fin de la ligne.

Une fois dans la configuration du jeu de stratégies, faites défiler vers le bas et développez la section Authentication Policy.

Cliquez sur l'icône Ajouter.

Pour cet exemple de configuration, la valeur Name est Internal Authentication et la condition choisie est l'adresse IP du périphérique réseau (Nexus) (remplacer l'adresse A.B.C.D.). Cette stratégie d'authentification utilise le magasin d'identités des utilisateurs internes.

Voici comment la condition a été configurée.

Sélectionnez Network Access > Device IP address Dictionary Attribute.

Remplacez le commentaire <Nexus IP address> par l'adresse IP correcte.

Cliquez sur le bouton Utiliser.

Cette condition n'est remplie que par le périphérique Nexus que vous avez configuré. Cependant, si l'objectif est d'activer cette condition pour un grand nombre de périphériques, considérez une condition différente.

Accédez ensuite à la section Politique d'autorisation et développez-la.

Cliquez sur l'icône + (plus).

Dans cet exemple, NEXUS HELP DESK comme nom de la politique d'autorisation a été utilisé.

La même condition que celle configurée dans la stratégie d'authentification est utilisée pour la stratégie d'autorisation.

Dans la colonne Profils Shell, le profil configuré avant la sélection de Nexus Helpdesk.

Enfin, cliquez sur le bouton Enregistrer.

Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Dans l'interface utilisateur graphique d'ISE, accédez à Operations > TACACS > Live Logs. Identifiez l'enregistrement qui correspond au nom d'utilisateur utilisé, puis cliquez sur Live Log Detail de l'événement Authorization.

Dans le cadre des détails inclus dans ce rapport, vous pouvez trouver une section Réponse, où vous pouvez voir comment ISE a retourné la valeur shell : roles="helpdesk"

Sur le périphérique Nexus :

```
Nexus9000 login: iseiscool
Password: VainillaISE97
```

```
Nexus9000# conf t
Enter configuration commands, one per line. End with CNTL/Z.
Nexus9000(config)# interface ethernet 1/23
% Interface permission denied
```

```
Nexus9000(config)# ?
  interface  Configure interfaces
  show       Show running system information
  end        Go to exec mode
  exit       Exit from command interpreter
```

```
Nexus9000(config)# role name test
% Permission denied for the role
```

```
Nexus9000(config)#
```

```
Nexus9000(config)# interface loopback 0
% Interface permission denied
```

```
Nexus9000(config)#
Nexus9000# conf t
```

```
Nexus9000(config)# interface ethernet 1/5
Notice that only the commands allowed are listed.
Nexus9000(config-if)# ?
```

```
no          Negate a command or set its defaults
show        Show running system information
shutdown    Enable/disable an interface
end         Go to exec mode
exit        Exit from command interpreter
```

```
Nexus9000(config-if)# cdp
Nexus9000(config-if)# cdp enable
% Permission denied for the role
Nexus9000(config-if)#
```

Dépannage

- Vérifiez qu'ISE est accessible à partir du périphérique Nexus :

```
Nexus9000# ping <Votre adresse IP ISE>
PING <Votre adresse IP ISE> (<Votre adresse IP ISE>) 56 octets de données
64 octets de <Votre adresse IP ISE> : icmp_seq=0 ttl=59 time=1,22 ms
64 octets de <Votre adresse IP ISE> : icmp_seq=1 ttl=59 time=0,739 ms
64 octets de <Votre adresse IP ISE> : icmp_seq=2 ttl=59 time=0,686 ms
64 octets de <Votre adresse IP ISE> : icmp_seq=3 ttl=59 time=0,71 ms
64 octets de <Votre adresse IP ISE> : icmp_seq=4 ttl=59 time=0,72 ms
```

- Vérifiez que le port 49 est ouvert entre ISE et le périphérique Nexus :

```
Nexus9000# telnet <Votre IP ISE> 49
Essai de <votre adresse IP ISE>...
Connecté à <votre adresse IP ISE>.
Le caractère d'échappement est '^]'.
```

- Utilisez ces débogages :

```
debug tacacs+ all
```

```
Nexus9000#
```

```
Nexus9000# 2024 19 avril 22:50:44.199329 tacacs : event_loop() : appel de process_rd_fd_set
2024 Avr 19 22:50:44.199355 tacacs : process_rd_fd_set : rappel d'appel pour fd 6
2024 Avr 19 22:50:44.199392 tacacs : fsrv n'a pas consommé l'opcode 8421
2024 Avr 19 22:50:44.199406 tacacs : process_implicit_cfs_session_start : saisie en cours...
2024 Avr 19 22:50:44.199414 tacacs : process_implicit_cfs_session_start : sortie ; l'état de
distribution est désactivé
2024 Avr 19 22:50:44.199424 tacacs : process_aaa_tplus_request : saisie pour l'id de session aaa
0
2024 Avr 19 22:50:44.199438 tacacs : process_aaa_tplus_request:vérification de l'état du port
mgmt0 avec servergroup lsePsnServers
2024 Avr 19 22:50:44.199451 tacacs : tacacs_global_config(4220) : saisie en cours...
2024 Avr 19 22:50:44.199466 tacacs : tacacs_global_config(4577) : GET_REQ...
2024 Avr 19 22:50:44.208027 tacacs : tacacs_global_config(4701) : Récupération de la valeur de
retour de l'opération de configuration globale du protocole :SUCCESS
2024 Avr 19 22:50:44.208045 tacacs : tacacs_global_config(4716) : REQ:num. serveur 0
2024 Avr 19 22:50:44.208054 tacacs : tacacs_global_config : REQ : groupe de numéros 1
2024 Avr 19 22:50:44.208062 tacacs : tacacs_global_config : REQ:num timeout 5
2024 Avr 19 22:50:44.208070 tacacs : tacacs_global_config : REQ : num deadtime 0
2024 Avr 19 22:50:44.208078 tacacs : tacacs_global_config : REQ : num encryption_type 7
2024 Avr 19 22:50:44.208086 tacacs : tacacs_global_config : renvoi de retval 0
2024 Avr 19 22:50:44.208098 tacacs : process_aaa_tplus_request : group_info est renseigné dans
aaa_req, donc Utilisation de servergroup lsePsnServers
2024 Avr 19 22:50:44.208108 tacacs : tacacs_servergroup_config : entrée pour le groupe de
serveurs, index 0
2024 Avr 19 22:50:44.208117 tacacs : tacacs_servergroup_config : GETNEXT_REQ pour l'index
```

de groupe de serveurs de protocole :0 nom :

2024 Avr 19 22:50:44.208148 tacacs : tacacs_pss2_move2key : rcode = 40480003 syserr2str = aucune clé pss de ce type

2024 Avr 19 22:50:44.208160 tacacs : tacacs_pss2_move2key : appel de pss2_getkey

2024 Avr 19 22:50:44.208171 tacacs : tacacs_servergroup_config : GETNEXT_REQ a obtenu l'index de groupe de serveurs de protocole :2 nom:IsePsnServers

2024 Avr 19 22:50:44.208184 tacacs : tacacs_servergroup_config : Récupération de la valeur de retour du fonctionnement du groupe de protocoles :SUCCESS

2024 Avr 19 22:50:44.208194 tacacs : tacacs_servergroup_config : renvoi de retval 0 pour le groupe de serveurs de protocole:IsePsnServers

2024 Avr 19 22:50:44.208210 tacacs : process_aaa_tplus_request : Groupe IsePsnServers trouvé. vrf correspondant est default, source-intf est 0

2024 Avr 19 22:50:44.208224 tacacs : process_aaa_tplus_request : vérification de mgmt0 vrf:management par rapport à vrf:default du groupe demandé

2024 Avr 19 22:50:44.208256 tacacs : process_aaa_tplus_request:mgmt_if 83886080

2024 Avr 19 22:50:44.208272 tacacs : process_aaa_tplus_request : global_src_intf : 0, src_intf local est 0 et vrf_name est la valeur par défaut

2024 Avr 19 22:50:44.208286 tacacs : create_tplus_req_state_machine(902) : saisie pour l'id de session aaa 0

2024 Avr 19 22:50:44.208295 tacacs : nombre de machines d'état 0

2024 Avr 19 22:50:44.208307 tacacs : init_tplus_req_state_machine : saisie pour l'id de session aaa 0

2024 Avr 19 22:50:44.208317 tacacs : init_tplus_req_state_machine(1298):tplus_ctx a la valeur NULL si author et test

2024 Avr 19 22:50:44.208327 tacacs : tacacs_servergroup_config : saisie pour le serveur groupIsePsnServers, index 0

2024 Avr 19 22:50:44.208339 tacacs : tacacs_servergroup_config : GET_REQ pour index de groupe de serveurs de protocole:0 nom:IsePsnServers

2024 Avr 19 22:50:44.208357 tacacs : find_tacacs_servergroup : saisie pour le groupe de serveurs IsePsnServers

2024 Avr 19 22:50:44.208372 tacacs : tacacs_pss2_move2key : rcode = 0 syserr2str = SUCCESS

2024 Avr 19 22:50:44.208382 tacacs : find_tacacs_servergroup : sortie pour le groupe de serveurs L'index IsePsnServers est 2

2024 Avr 19 22:50:44.208401 tacacs : tacacs_servergroup_config : GET_REQ : find_tacacs_servergroup error 0 pour le groupe de serveurs de protocole IsePsnServers

2024 Avr 19 22:50:44.208420 tacacs : tacacs_pss2_move2key : rcode = 0 syserr2str = SUCCESS

2024 Avr 19 22:50:44.208433 tacacs : tacacs_servergroup_config : GET_REQ a obtenu l'index de groupe de serveurs de protocoles :2 nom:IsePsnServers

2024 A2024 19 avril 22:52024 19 avril 22:52024 19 avril 22:5

Nexus9000#

- Effectuez une capture de paquets. (Pour afficher les détails du paquet, vous devez modifier les préférences TACACS+ de Wireshark, et mettre à jour la clé partagée utilisée par Nexus et ISE.)
- Vérifiez que la clé partagée est identique côté ISE et côté Nexus. Cette option peut

également être cochée dans Wireshark.

Introduction

Ce document décrit comment installer un produit A.

Essai A

1. Le premier ul a un problème.
2. Assurez-vous que les machines virtuelles sont configurées avec les paramètres supplémentaires suivants en cliquant avec le bouton droit sur la machine virtuelle souhaitée dans VMware ESXi et en cliquant sur Modifier les paramètres.
 - Balise ul2test, pas de balise Span CPU : Sélectionnez Bas dans la liste déroulante firstShares
 - Balise ul2, Pas de balise Span CPU : Sélectionnez Bas dans la liste déroulante firstShares
 - Balise ul2, No span tag Mémoire : Cochez la case Reserve all guest memory (All locked).
 - balise ul2. No span tag Définissez le processeur et la mémoire vive en fonction de votre taille d'échelle. Voir [pour plus de détails](#)
 - ul3 copié à partir de ul présentant un problème. Balise span supprimée, balise p ajoutée.CPU : Sélectionnez Bas dans la liste déroulante firstShares
 - ul3 copié à partir de ul présentant un problème. Balise span supprimée, balise p ajoutée.Mémoire : Cochez la case Reserve all guest memory (All locked).
 - ul3 copié à partir de ul présentant un problème. Balise span supprimée, balise p ajoutée. Définissez le processeur et la mémoire vive en fonction de votre taille d'échelle. Voir [Tester Self Link](#) pour plus de détails
 - ul4. vient d'être copié à partir de ul1.CPU : Sélectionnez Bas dans la liste déroulante firstShares
 - ul4. vient d'être copié à partir de ul1.Memory : Cochez la case Reserve all guest memory (All locked).
 - ul4. vient d'être copié à partir de ul1. Définissez le processeur et la mémoire vive en fonction de votre taille d'échelle. Voir [Composants utilisés](#) pour plus de détails
 - ul5. copié à partir de l'original, sans balise p, avec span tagCPU : Sélectionnez Faible dans la première liste déroulante Partages
 - ul5. copié à partir de l'original, sans balise p, avec span tagMemory : Cochez la case

Reserve all guest memory (All locked)

- ul5. copié à partir de l'original, sans balise p, avec balise spanDéfinissez le processeur et la mémoire vive en fonction de votre taille d'échelle. Voir [Besoins en ressources matérielles et VM](#) pour plus de détails
- ul1 avec un problème. Balise span supprimée, balise p ajoutée.CPU : Sélectionnez Bas dans la liste déroulante firstShares
- ul1 avec un problème. Balise span supprimée, balise p ajoutée.Mémoire : Cochez la case Reserve all guest memory (All locked).
- ul1 avec un problème. Balise span supprimée, balise p ajoutée. Définissez le processeur et la mémoire vive en fonction de votre taille d'échelle. Voir [Besoins en ressources matérielles et VM](#) pour plus de détails

1. La version est correcte. Connectez-vous au serveur système d'exploitation hôte Red Hat avec les informations d'identification administrateur.
2. Dans la boîte de dialogue, procédez comme suit :
 - Sous Ready (Prêt) pour commencer l'installation, entrez Name (Nom) pour l'instance Cisco IQ Link.
 - Cliquez sur l'option Personnaliser la configuration avant l'installation.
 - Sous Sélection du réseau, assurez-vous de sélectionner le réseau virtuel approprié.
3. Cliquez sur Terminer pour terminer l'ajout du premier disque.
4. Sur la console VMM, personnalisez la configuration du mot de passe et les propriétés IP.

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.