

Intégration de Nexus avec l'exemple de configuration ACS 5.2

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez](#)

[Périphérique de Nexus pour l'authentification et autorisation avec la configuration ACS 5.2](#)

[Configuration ACS 5.x](#)

[Vérifiez](#)

[Informations connexes](#)

[Introduction](#)

Ce document fournit un exemple de configuration d'authentification TACACS+ sur un commutateur de Nexus. Par défaut, si vous configurez le commutateur de Nexus afin d'authentifier par le serveur de contrôle d'accès (ACS), vous êtes automatiquement placé dans le rôle d'opérateur réseau/volts continu-opérateur, qui fournit l'accès en lecture seule. Afin d'être placé dans le rôle de réseau-admin/volts continu-admin, vous devez créer un shell sur l'ACS 5.2. Ce document décrit ce processus.

[Conditions préalables](#)

[Conditions requises](#)

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

- Définissez votre commutateur de Nexus en tant que client dans ACS.
- Définissez l'adresse IP et une clé secrète partagée identique sur l'ACS et le Nexus.

Note: Créez un point de reprise ou une sauvegarde sur le Nexus avant que vous apportiez toutes les modifications.

[Composants utilisés](#)

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

- ACS 5.2

- Nexus 5000, 5.2(1)N1(1)

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à [Conventions relatives aux conseils techniques Cisco](#).

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Note: Utilisez l'outil [Command Lookup Tool](#) (clients [enregistrés](#) seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Périphérique de Nexus pour l'authentification et autorisation avec la configuration ACS 5.2

Procédez comme suit :

1. Créez un utilisateur local sur le commutateur de Nexus avec de pleins privilèges pour le retour :

```
username admin privilege 15 password 0 cisco123!
```

2. Activez TACACS+, puis fournissez l'adresse IP du serveur TACACS+ (ACS) :

```
feature tacacs+
```

```
tacacs-server host IP-ADDRESS key KEY
```

```
tacacs-server key KEY
```

```
tacacs-server directed-request
```

```
aaa group server tacacs+ ACS
```

```
server IP-ADDRESS
```

```
use-vrf management
```

```
source-interface mgmt0
```

Note: La clé doit apparier le secret partagé configuré sur l'ACS pour ce périphérique de Nexus.

3. Testez la Disponibilité de serveur TACACS :

```
test aaa group group-name username password
```

Le test d'authentification devrait échouer avec un message d'anomalie du serveur, puisque le serveur n'a pas été configuré. Ce message d'anomalie confirme que le serveur TACACS+ est accessible.

4. Configurez les authentifications de connexion :

```
aaa authentication login default group ACS
```

```
aaa authentication login console group ACS
```

```
aaa accounting default group ACS
```

```
aaa authentication login error-enable
```

```
aaa authorization commands default local
```

```
aaa authorization config-commands default local
```

Note: Le Nexus utilise l'authentification locale si le serveur d'authentification est inaccessible.

[Configuration ACS 5.x](#)

Procédez comme suit :

1. Naviguez des **profils** vers des **éléments de stratégie > l'authentification et des autorisations > de périphérique gestion > shell** afin de créer un profil de shell.
2. Écrivez un nom pour le profil.
3. Sous les attributs personnalisés tablez, écrivez ces valeurs :Attribut : Cisco-poids du

commerce-pairesCondition requise : ObligatoireValeur : shell : roles* " volts continu-admin de réseau-admin »

4. Soumettez les modifications afin de créer un rôle basé sur attribut pour le commutateur de Nexus.
5. Créez une nouvelle règle d'autorisation, ou éditez une règle existante, dans la stratégie correcte d'accès. Par défaut, des demandes TACACS+ sont traitées par la stratégie par défaut d'accès d'admin de périphérique.
6. Dans la région de conditions, choisissez les conditions appropriées. Dans la région de résultats, choisissez le profil de shell de SYSTÈME D'EXPLOITATION de Nexus.
7. Cliquez sur **OK**.

Vérifiez

Référez-vous à cette section pour vous assurer du bon fonctionnement de votre configuration.

L'[Outil Interpréteur de sortie](#) (clients [enregistrés](#) uniquement) (OIT) prend en charge certaines commandes **show**. Utilisez l'OIT pour afficher une analyse de la sortie de la commande **show** .

- [show tacacs+](#) — Affiche les statistiques TACACS+.
- [show running-config tacacs+](#) — Affiche la configuration TACACS+ en configuration en cours.
- [show startup-config tacacs+](#) — Affiche la configuration TACACS+ dans la configuration de démarrage.
- [show tacacs-server](#) — Affiche tous les paramètres configurés de serveur TACACS+.

Informations connexes

- [Support et documentation techniques - Cisco Systems](#)