Configurer TACACS+, RADIUS et Kerberos sur les commutateurs Catalyst

Contenu

Introduction

La gamme de commutateurs Cisco Catalyst (Catalyst 4000, Catalyst 5000 et Catalyst 6000, qui exécutent CatOS) prend en charge une forme d'authentification, qui commence par le code 2.2. Des améliorations ont été ajoutées avec des versions ultérieures. Le port 49 de TACACS+ TCP, non le port 49 de Protocole de datagramme utilisateur (UDP) XTACACS), RADIUS, ou la configuration utilisateur de serveur kerberos pour l'AAA (authentification, autorisation et traçabilité) (AAA) est le même que pour les utilisateurs du routeur. Ce document contient des exemples des commandes minimales nécessaires afin d'activer ces fonctions. Des options supplémentaires sont disponibles dans la documentation de commutateur pour la version en question.

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

Ce document n'est pas limité à des versions de matériel et de logiciel spécifiques.

Conventions

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

Informations générales

Puisque les versions ultérieures du code prennent en charge des options supplémentaires, vous devez émettre la commande **show version afin de déterminer la version du code sur le commutateur.** Une fois que vous avez déterminé la version du code qui est utilisé sur le commutateur, utilisez cette table afin de déterminer quelles options sont disponibles sur votre matériel, et quelles options vous souhaitez configurer.

Restez toujours dans le commutateur lorsque vous ajoutez l'authentification et l'autorisation. Testez la configuration dans une autre fenêtre afin d'éviter d'être accidentellement verrouillé.

Méthode (minimum)	**Version 2.2 à 5.1 de Cat**	**Version 5.1 à 5.4.1 de Cat**	**Version 5.4.1 à 7.5.1 de Cat**	**Versions 7.5.1 et ultérieures de Cat**
Authentification TACACS+ OU	Étape A	Étape A	Étape A	Étape A
Authentification RADIUS OU	S/O	Étape B	Étape B	Étape B
Authentification Kerberos OU	S/O	S/O	Étape K	Étape K
Authentification/ autorisation de nom d'utilisateur local	S/O	S/O	S/O	Étape C
Plus (options)				
Autorisation de commande avec TACACS+	S/O	S/O	Étape D	Étape D
Autorisation TACACS+ Exec	S/O	S/O	Étape E	Étape E
Autorisation RADIUS Exec	S/O	S/O	Étape F	Étape F
Gestion des comptes -	S/O	S/O	Étape G	Étape G

TACACS+ ou RADIUS				
Autorisation TACACS+ Enable	Étape H	Étape H	Étape H	Étape H
Autorisation RADIUS Enable	S/O	Étape I	Étape I	Étape I
Autorisation TACACS+ Enable	S/O	S/O	Étape J	Étape J

Configuration Steps

Étape A - Authentification TACACS+

Avec des versions antérieures de code, les commandes ne sont pas aussi complexes qu'avec quelques versions ultérieures. Des options supplémentaires dans des versions ultérieures sont disponibles sur votre commutateur.

1. Émettez la commande **set authentication login local enable afin de vous assurer qu'il y a une porte dérobée dans le commutateur si le serveur est en panne.**
2. Émettez la commande **set authentication login tacacs enable afin d'activer l'authentification TACACS+.**
3. Émettez la commande **set tacacs server #.#.#.# afin de définir le serveur.**
4. Émettez la commande **set tacacs key your_key afin de définir la clé du serveur, qui est facultative avec TACACS+, car elle entraîne le cryptage des données de commutateur à serveur.** En cas d'utilisation, elle doit s'entendre avec le serveur.**Remarque :** le logiciel Cisco Catalyst OS **n**'accepte pas que le point d'interrogation (**?**) fasse partie d'une clé ou d'un mot de passe. Le point d'interrogation est explicitement utilisé pour l'aide sur la syntaxe de commande.

Étape B - Authentification RADIUS

Avec des versions antérieures de code, les commandes ne sont pas aussi complexes qu'avec quelques versions ultérieures. Des options supplémentaires dans des versions ultérieures sont disponibles sur votre commutateur.

1. Émettez la commande **set authentication login local enable afin de vous assurer qu'il y a une porte dérobée dans le commutateur si le serveur est en panne.**
2. Émettez la commande **set authentication login radius enable afin d'activer l'authentification RADIUS.**
3. Définissez le serveur. Sur tout autre équipement Cisco, les ports RADIUS par défaut sont 1645/1646 (authentification/gestion des comptes).Sur le Catalyst, le port par défaut est 1812/1813. Si vous utilisez Cisco Secure ou un serveur qui communique avec un autre équipement Cisco, utilisez le port 1645/1646. Émettez la **commande principale set radius server #.#.#.# auth-port 1645 acct-port 1646 afin de définir le serveur et la commande équivalente dans le Cisco IOS comme radius-server source-ports 1645-1646**.
4. Définissez la clé du serveur.C'est obligatoire, car elle entraîne le chiffrement du mot de

passe de commutateur à serveur comme dans l'Authentication RADIUS/Autorisation RFC 2865 et la Gestion des comptes RADIUS RFC 2866 . En cas d'utilisation, elle doit s'entendre avec le serveur. Émettez la commande **set radius key *your_key*** .

Étape C - Authentification/autorisation de nom d'utilisateur local

Débutant dans la version 7.5.1 de CatOS, l'authentification des utilisateurs locaux est possible. Par exemple, vous pouvez réaliser l'authentification/autorisation en utilisant un nom d'utilisateur et mot de passe enregistré sur le Catalyst, au lieu d'une authentification avec un mot de passe local.

Il y a seulement deux niveaux de privilège pour l'authentification des utilisateurs locaux, 0 ou 15. Le niveau 0 est le niveau exec non privilégié. Le niveau 15 est le niveau enable privilégié.

Si vous ajoutez ces commandes dans cet exemple, l'utilisateur `poweruser arrive dans le mode enable sur un telnet ou la console dans le commutateur et l'utilisateur nonenable arrive dans le mode exec sur un telnet ou une console dans le commutateur.`

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

Remarque : Si l'utilisateur `non-enable` connaît le mot de passe **set enable**, cet utilisateur peut continuer à activer le mode.

Après la configuration, les mots de passe sont enregistrés chiffrés.

L'authentification de nom d'utilisateur local peut être utilisée en même temps que TACACS+ exec à distance, la gestion des comptes de commande, ou la gestion des comptes RADIUS exec à distance. Elle peut également être utilisée en même temps que TACACS+ exec à distance ou l'autorisation de commande, mais cela n'a aucun sens de l'utiliser de cette façon parce que le nom d'utilisateur doit être enregistrée sur le serveur TACACS+ ainsi que localement sur le commutateur.

Étape D - Autorisation de commande TACACS+

Dans cet exemple, le commutateur doit demander l'autorisation seulement pour les commandes de configuration avec TACACS+. Au cas où le serveur TACACS+ serait en panne, l'authentification est none. Ceci s'applique au port de console et à la session Telnet. Émettez la commande suivante :

set authorization commands enable config tacacs none both

Dans cet exemple, vous pouvez configurer le serveur TACACS+ pour autoriser quand vous défini ces paramètres :

```
command=set
arguments (permit)=port 2/12
```

La commande **set port enable 2/12 est envoyé au serveur TACACS+ pour vérification.**

Remarque : avec l'autorisation de commande activée, contrairement au routeur où enable n'est pas considéré comme une commande, le commutateur envoie la commande **enable** au serveur

lorsqu'une tentative d'activation est effectuée. Assurez-vous que le serveur est également configuré pour permettre la commande **enable.**

Étape E - Autorisation TACACS+ Exec

Dans cet exemple, le commutateur doit requérir l'autorisation pour une session exec avec TACACS+. Au cas où le serveur TACACS+ serait en panne, l'autorisation est none. Ceci s'applique au port de console et à la session Telnet. Émettez la commande **set authorization exec enable tacacs+ none both .**

En plus de la demande d'authentification, ceci envoie une demande d'autorisation distincte au serveur TACACS+ depuis le commutateur. Si le profil d'utilisateur est configuré pour shell/exec sur le serveur TACACS+, cet utilisateur peut accéder au commutateur.

Ceci empêche les utilisateurs qui ne disposent pas du service shell/exec sur le serveur, tels que les utilisateurs PPP, de se connecter au commutateur. Vous recevez le message `Exec mode authorization failed`. En plus d'autoriser/refuser le mode exec pour les utilisateurs, vous pouvez être contraint d'accéder au mode enable quand vous entrez avec le niveau de privilège 15 attribué sur le serveur. Il doit exécuter le code dans lequel le bogue Cisco dont l'ID est CSCdr51314 (clients enregistrés uniquement) est réparé.

Étape F - Autorisation RADIUS exec

Il n'existe aucune commande pour activer l'autorisation RADIUS exec. L'alternative consiste à définir le Type de service (attribut RADIUS 6) sur Administrative (une valeur de 6) dans le serveur RADIUS pour démarrer l'utilisateur dans le mode enable dans le serveur RADIUS. Si le service-type est défini pour tout sauf 6-administrative, par exemple, 1-login, 7-shell ou 2-framed, l'utilisateur arrive à l'invite exec de commutateur, mais pas à l'invite d'enable.

Ajoutez ces commandes dans le commutateur pour l'authentification et l'autorisation :

```
aaa authorization exec TEST group radius
 line vty 0 4
 authorization exec TEST
 login authentication TEST
```

Étape G - Gestion des comptes - TACACS+ ou RADIUS

Pour activer la gestion des comptes TACACS+ dans les cas suivants :

1. Si vous obtenez l'invite de commutateur, émettez la commande **set accounting exec enable start-stop tacacs+.**
2. Les utilisateurs de Telnet hors du commutateur doivent émettre la commande **set accounting connect enable start-stop tacacs+.**
3. Si vous redémarrez le commutateur, émettez la commande **set accounting system enable start-stop tacacs+.**
4. Les utilisateurs qui exécutent des commandes doivent émettre la commande **set accounting commands enable all start-stop tacacs+.**
5. Les rappels au serveur, par exemple, pour mettre à jour les enregistrements toutes les minutes afin de montrer que l'utilisateur est toujours connecté, émettez la commande **set accounting update periodic 1.**

Pour activer la gestion des comptes RADIUS dans les cas suivants :

1. Les utilisateurs qui obtiennent l'invite de commutateur doivent émettre la commande **set accounting exec enable start-stop radius.**
2. Les utilisateurs de Telnet hors du commutateur doivent émettre la commande **set accounting connect enable start-stop radius**.
3. Si vous redémarrez le commutateur, émettez la commande **set accounting system enable start-stop radius .**
4. Les rappels au serveur, par exemple, pour mettre à jour les enregistrements toutes les minutes afin de montrer que l'utilisateur est toujours connecté, émettez la commande **set accounting update periodic 1**.

Enregistrements de logiciel gratuit TACACS+

Ce résultat est un exemple de la façon dont les enregistrements peuvent apparaître sur le serveur :

```
Fri Mar 24 13:22:41 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=5 start_time=953936729 timezone=UTC
service=shell disc-cause=2 elapsed_time=236
Fri Mar 24 13:22:50 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=15 start_time=953936975 timezone=UTC
service=shell priv-lvl=0 cmd=enable
Fri Mar 24 13:22:54 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=16 start_time=953936979 timezone=UTC
service=shell priv-lvl=15 cmd=write terminal
Fri Mar 24 13:22:59 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=17 start_time=953936984 timezone=UTC
service=shell priv-lvl=15 cmd=show version
Fri Mar 24 13:23:19 2000 10.31.1.151 pinecone telnet85
171.68.118.100 update task_id=14 start_time=953936974 timezone=UTC
service=shell
```

RADIUS sur le résultat d'enregistrement UNIX

Ce résultat est un exemple de la façon dont les enregistrements peuvent apparaître sur le serveur :

```
Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Start
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
```

```
Login-Host = 171.68.118.100
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Stop
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Session-Time = 9
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Received unknown attribute 49
Acct-Session-Time = 30
Acct-Delay-Time = 0
```

Étape H - Authentification TACACS+ Enable

Procédez comme suit :

1. Émettez la commande **set authentication enable local enable** pour vous assurer qu'il y a une porte dérobée à l'intérieur si le serveur est en panne.
2. Émettez la commande **set authentication enable tacacs enable afin de dire au commutateur d'envoyer des requêtes d'activation au serveur.**

Étape I - Authentification RADIUS Enable

Ajoutez ces commandes pour que le commutateur envoie le nom d'utilisateur `$enab15$ au serveur RADIUS`. Tous les serveurs RADIUS ne prennent pas en charge ce type de nom d'utilisateur. Voir l'Étape E pour une autre alternative, par exemple, si vous défini un type de service [attribut RADIUS 6 - sur Administrative], qui démarre des utilisateurs individuels dans le mode enable.

1. Émettez la commande **set authentication enable local enable pour vous assurer qu'il y a une porte dérobée à l'intérieur si le serveur est en panne.**
2. Émettez la commande **set authentication enable radius enable afin de dire au commutateur d'envoyer des demandes d'activation au serveur si votre serveur RADIUS prend en charge le nom d'utilisateur $enab15$.**

Étape J - Autorisation TACACS+ Enable

L'ajout de cette commande conduit le commutateur à envoyer la commande enable au serveur quand l'utilisateur essaie d'activer. La commande **enable doit être autorisée sur le serveur.** Dans cet exemple, il y a un basculement sur none en cas de panne du serveur :

set author enable enable tacacs+ none both

Étape K - Authentification Kerberos

Consultez Contrôler et surveiller l'accès au commutateur à l'aide de l'authentification, l'autorisation et de la gestion des comptes pour plus d'informations sur la façon d'installer le Kerberos sur le commutateur.

Récupération de mot de passe

Consultez les Procédures de récupération de mot de passe pour plus d'informations sur les procédures de récupération de mot de passe.

Cette page est un index des procédures de récupération de mot de passe pour les produits Cisco.

Commandes ip permit pour une sécurité supplémentaire

Pour une sécurité supplémentaire, le Catalyst peut être configuré pour contrôler l'accès Telnet via les commandes **ip permit :**

set ip permit enable telnet

set ip permit ***range mask*** **|*****host***

Ceci autorise seulement la plage ou les hôtes spécifiés au Telnet dans le commutateur.

Débogage sur le Catalyst

Avant d'activer le débogage sur le Catalyst, recherchez les raisons de la panne dans les journaux du serveur. C'est plus facile et cela perturbe moins le commutateur. Sur des versions de commutateur plus récentes, le **débogage s'effectuait dans le mode engineering.** Il n'est pas nécessaire d'accéder au mode engineering afin d'exécuter des commandes de **débogage dans les versions ultérieures du code :**

set trace tacacs|radius|kerberos 4

Note : La commande **set trace tacacs|radius|kerberos 0** retourne Catalyst au mode no-trace.

Consultez la Page d'assistance des commutateurs pour plus d'informations sur les commutateurs LAN multicouche.

Informations connexes

- Comparaison entre TACACS+ et RADIUS
- RADIUS, TACACS+ et Kerberos dans la documentation Cisco IOS
- Page d'assistance RADIUS
- Page de support TACACS/TACACS+
- Page d'assistance de Kerberos
- Demandes de commentaires (RFC)
- Support et documentation techniques - Cisco Systems