Contenu

Introduction

Ce document décrit une procédure pas à pas d'ajouter le service d'authentification de Terminal Access Controller Access Control System (TACACS+) sur le Cisco MGX 8850/8950/8830 révision du logiciel du commutateur courante plus grande que 5.0, avec la version 4.2 et ultérieures du serveur de contrôle d'accès de Cisco (ACS).

Conditions préalables

Conditions requises

Cisco recommande que vous répondiez ce à des exigences avant que vous tentiez cette configuration :

? Le serveur d'AAA est accessible du MGX

Composants utilisés

Ce document est limité au Cisco MGX 8850/8950/8830 révision du logiciel du commutateur courante plus grande que 5.0 et avec la version ACS au-dessus de 4.2.

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.

Configurez

Remarque: Utilisez l'Outil de recherche de commande (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configuration sur MGX

Un exemple de la configuration exigée sur MGX est affiché ici

Étape 1. Vérifiez la version de logiciel de commutateur. Vous avez besoin de version 5.0 ou ultérieures pour configurer TACACS+

```
8950A.7.PXM.a > dspversion
 Type d'image version de type de carte de type de module établie en
fonction
 ----------   ----------   ----------    ------------   ------------
   Délai d'exécution MGX PXM45 5.1(20.200) 23 juin 2005, 21:36:08
     Démarrage MGX PXM45 4.0(0.11)P2 -
```

Étape 2. Vérifiez-vous ont l'adresse IP correcte :

```
8950A.7.PXM.a > dspifip
  Adr d'émission de subnet mask d'adresse IP d'indicateur d'interface
  --------------  ----  --------------  --------------  -------------
-
  Ethernet/lnPci0 LÈVENT 10.66.69.57 255.255.255.128 10.255.255.255
   SLIP/sl0 LÈVENT 127.0.0.2 255.0.0.0 (le NON APPLICABLE)
   ATM/atm0 VERS LE BAS 0.0.0.0 0.0.0.0 (NON APPLICABLE)
```

Étape 3. Vérifiez-vous peut cingler le serveur ACS : (Le serveur ACS est chez 10.106.60.182)

```
8950A.7.PXM.a > ping 10.106.60.182
PING 10.106.60.182 : 56 octets de données
64 octets de 10.106.60.182 : icmp_seq=0. time=250. ms
64 octets de 10.106.60.182 : icmp_seq=1. time=240. ms
64 octets de 10.106.60.182 : icmp_seq=2. time=240. ms
----10.106.60.182 Statistiques de PING----
3 paquets transmis, 3 paquets reçus, perte de paquets de 0%
min/moy/max aller-retour (de ms) = 240/243/250
```

Si doesn de ping ? t interviennent, nous doit vérifier l'accessibilité par IP. Vérifiez également le **dspifip** et le **bootchange** sont configurés avec l'adresse IP correcte.

```
8950A.7.PXM.a > bootchange

« . » = champ clair ;  « - » = allez au champ précédent ;  ^D = quitté

périphérique de démarrage : lnPci0
nombre de processeur : 0
nom d'hôte :
nom du fichier :
inet sur les Ethernets (e) : 172.16.157.88 >>
inet sur le fond de panier (b) :
```

```
inet d'hôte (h) :
inet (G) de passerelle : 172.16.157.1 >>
utilisateur (u) :
mot de passe de FTP (picowatt) (rsh de blanc = d'utilisation) :
indicateurs (f) : 0x0
nom cible (tn) :
script de démarrage (s) :
l'autre (o) :
```

Remarque: Vérifiez la configuration des paramètres de dspifip et avez changé l'adresse IP primaire de la Gestion de réseau pour relier l'adresse IP et atmosphère de RÉSEAU LOCAL comme secondaire (utilisant le **cnfndparm**). Également vous devez configurer les paramètres de bootchange mettant l'adresse IP et la passerelle correctes de RÉSEAU LOCAL. La sortie de commande de **routeshow** devrait indiquer la passerelle par défaut pour 0.0.0.0 comme adresse IP de RÉSEAU LOCAL.

Étape 4. Vérifiez la configuration d'AAA utilisant le **dspaaa.** Par défaut aucun AAA n'est configuré

```
8950A.7.PXM.a > dspaaa
CONFIGURATION D'AAA :
 Méthodes d'authentification :  gens du pays Cisco
 Authorizations method :  gens du pays Cisco
 Type d'autorisation :  groupe
 Niveau de privilège par défaut :  NOUSER_GP
 Affichage prompt :  acs
 Type de message SSH/FTP :  Procédure de connexion d'arrivée ASCII
 Liste d'exclusion IOS :

SERVEURS TACACS+ :    primaire est affiché d'abord

          Temps complètement simple
 Le port d'adresse IP chronomètrent la clé de chiffrement partagée par
conn.
---------------  ----  ------  ----  ------ --------------------------
-----------
```

Étape 5. Configurez l'adresse IP du serveur et la clé d'AAA :

```
8950A.7.PXM.a > cnfaaa-serveur tacacs+ - IP 10.66.79.246
Voulez-vous changer la clé de chiffrement (oui/non) ? oui
Introduisez la clé de chiffrement : Cisco
Ressaisissez la clé de chiffrement : Cisco

SERVEURS TACACS+ :    primaire est affiché d'abord

          Temps complètement simple
 Le port d'adresse IP chronomètrent la clé de chiffrement partagée par
conn.
---------------  ----  ------  ----  ------ --------------------------
-----------
10.66.79.246 49 5 0 Cisco vrais
```

Étape 6. Configurez l'authentification :

```
8950A.7.PXM.a > cnfaaa-authen
Syntaxe : cnfaaa-authen le <method> [le <method>…]

   méthode -- {gens du pays | par défaut | tacacs+ | Cisco}
     gens du pays : Utilisez la base de données locale pour
l'authentification.
    par défaut : Mêmes que des gens du pays.
    tacacs+ : Utilisez le protocole TACACS+ pour l'authentification.
    Cisco : Seulement on permet à l'l'utilisateur de base de « Cisco »
pour ouvrir une session.
```

Ici nous faisons les gens du pays et puis le Cisco TACACS+ puis. (Il est recommandé pour avoir Cisco en dernier recours dedans là ?)

```
8950A.7.PXM.a > cnfaaa-authen des gens du pays Cisco tacacs+
CONFIGURATION D'AAA :
 Méthodes d'authentification :  gens du pays Cisco tacacs+
 Authorizations method :  gens du pays Cisco
 Type d'autorisation :  groupe
 Niveau de privilège par défaut :  NOUSER_GP
 Affichage prompt :  acs
 Type de message SSH/FTP :  Procédure de connexion d'arrivée ASCII
 Liste d'exclusion IOS :
```

AVERTISSEMENT : L'authentification/authorizations method nouvellement configurées s'applique aux nouvelles sessions. Cette configuration n'a aucune incidence sur des sessions existantes.

Étape 7. Configurez le niveau de privilège par défaut si vous voulez. Nous ne le configurons pas dans cet exemple, c.-à-d. nous le laissons en tant que par défaut :

```
8950A.7.PXM.a > cnfaaa-priv
Syntaxe : cnfaaa-priv <CISCO_GP | SERVICE_GP | SUPER_GP | GROUP1 |
ANYUSER |
         NOUSER_GP | default>
         (NOTE : le « par défaut » correspond NOUSER_GP.)

8950A.7.PXM.a > par défaut de cnfaaa-priv
CONFIGURATION D'AAA :
 Méthodes d'authentification :  gens du pays Cisco tacacs+
 Authorizations method :  gens du pays Cisco tacacs+
 Type d'autorisation :  groupe
 Niveau de privilège par défaut :  NOUSER_GP
 Affichage prompt :  acs
 Type de message SSH/FTP :  Procédure de connexion d'arrivée ASCII
 Liste d'exclusion IOS :
```

Étape 8. Vérifiez la configuration :

```
8950A.7.PXM.a > dspaaa
CONFIGURATION D'AAA :
 Méthodes d'authentification :  gens du pays Cisco tacacs+
```

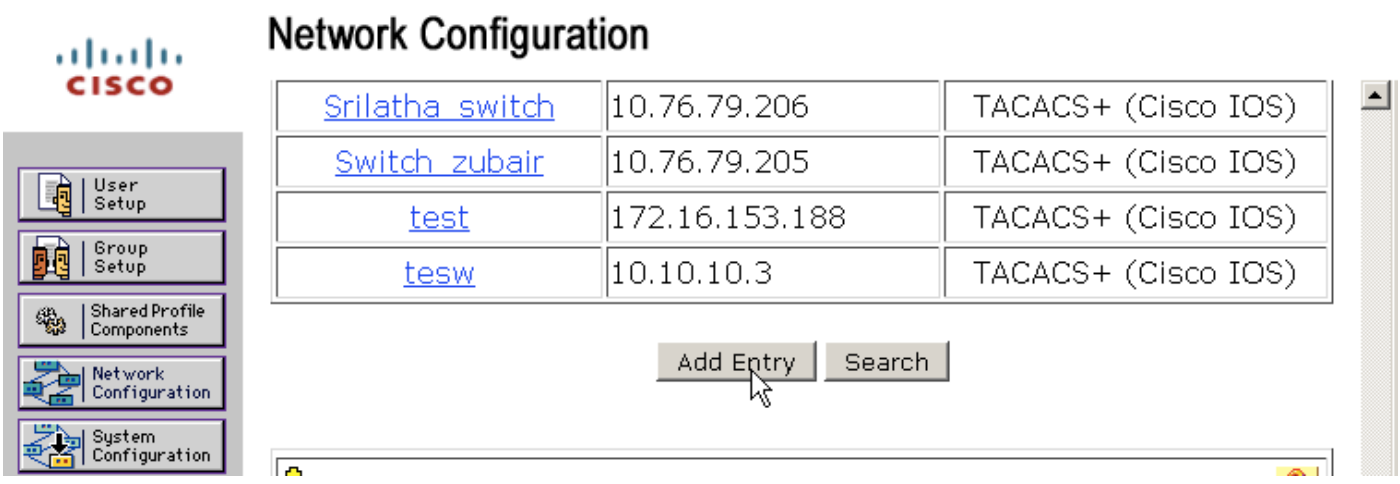
```
 Authorizations method :  gens du pays Cisco tacacs+
 Type d'autorisation :  groupe
 Niveau de privilège par défaut :  NOUSER_GP
 Affichage prompt :  acs
 Type de message SSH/FTP :  Procédure de connexion d'arrivée ASCII
 Liste d'exclusion IOS :

SERVEURS TACACS+ :    primaire est affiché d'abord

          Temps complètement simple
 Le port d'adresse IP chronomètrent la clé de chiffrement partagée par
conn.
---------------  ----  ------  ----  ------ --------------------------
-----------
10.66.79.246 49 5 0 Cisco vrais

8950A.7.PXM.a > dspaaa-serveurs
SERVEURS TACACS+ :    primaire est affiché d'abord

          Temps complètement simple
 Le port d'adresse IP chronomètrent la clé de chiffrement partagée par
conn.
---------------  ----  ------  ----  ------ --------------------------
-----------
10.66.79.246 49 5 0 Cisco vrais
```

Configuration sur ACS

Un exemple de la configuration exigée sur ACS est affiché ici :

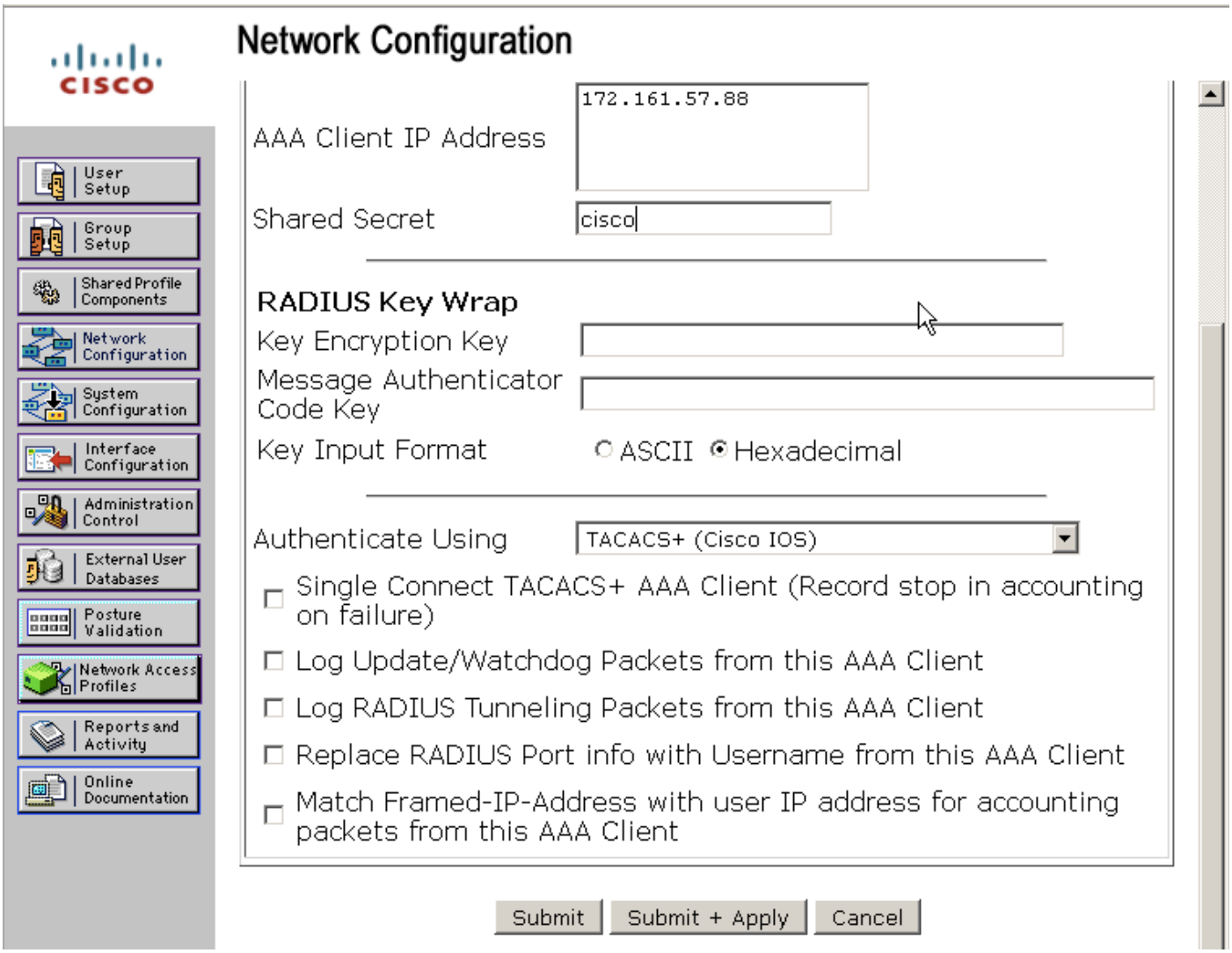
Étape 1. Ajoutez le MGX comme client sur l'ACS : (le nom utilisé ici est PXM_MGX, peut être quelque chose)

Cliquez sur en fonction la **configuration réseau**
(le nom utilisé ici est PXM_MGX, peut être quelque chose)



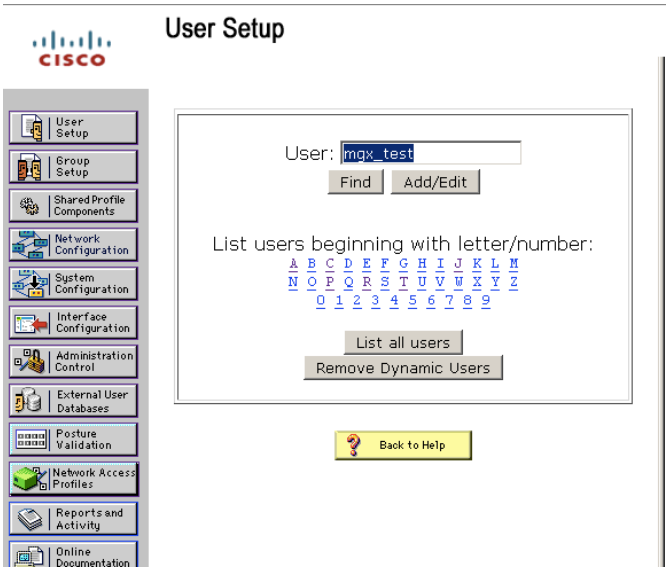
Étape 2. Cliquez sur Add l'**entrée** et configurez l'adresse Internet de client

Étape 3. Configurez l'adresse IP du client d'AAA (**MGX** dans ce cas) et ? **clé** ? que doit s'assortir avec le config MGX (la clé utilisée ici est-elle ? **Cisco** ?).

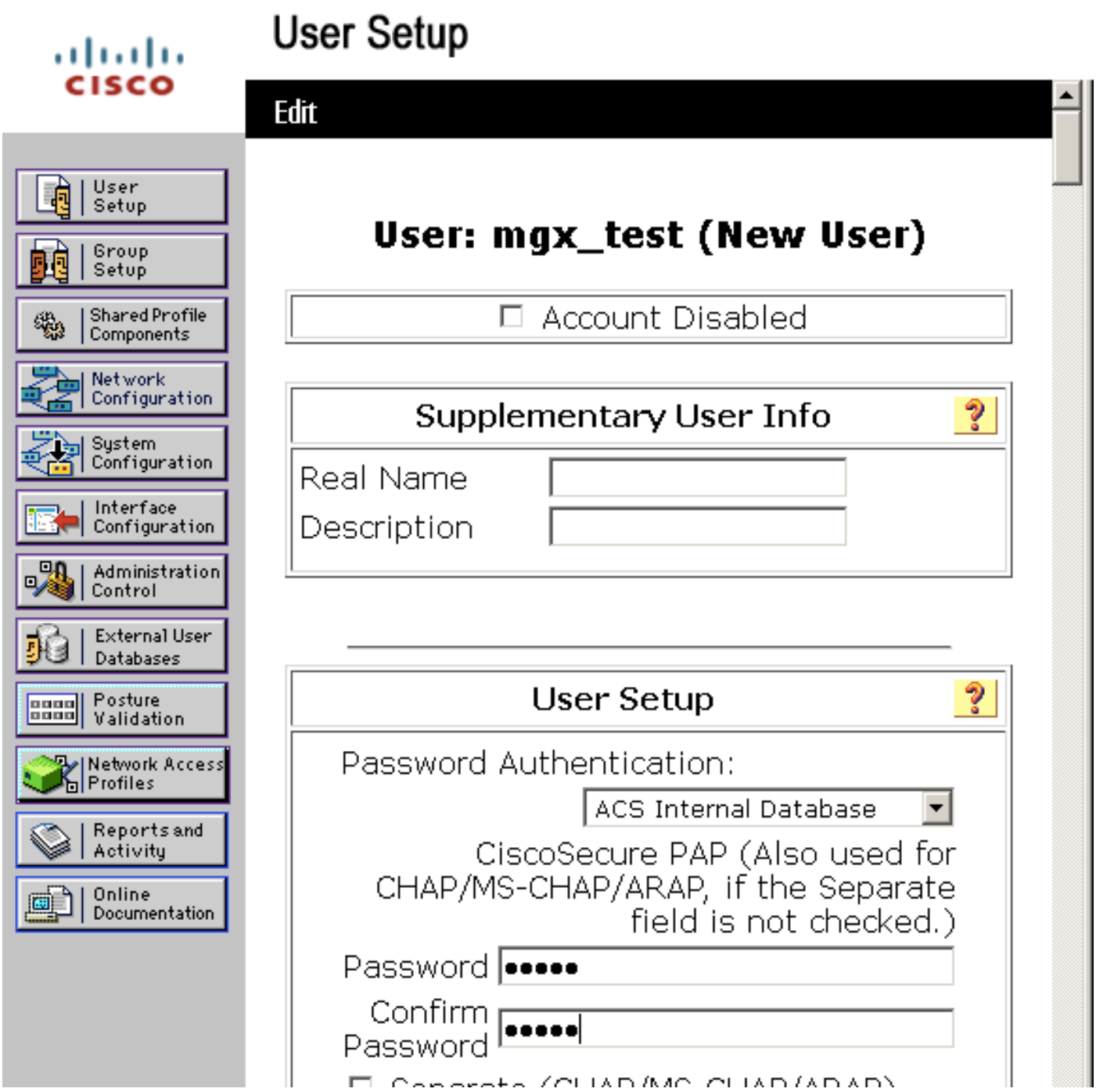


Clic **Submit+Apply**

Étape 4. Configurez un UTILISATEUR. Cliquez sur en fonction l'**installation utilisateur.** L'utilisateur ici s'appelle ? mgx_test ? . Cliquez sur Add**/éditez**, après avoir tapé dans un nouveau nom d'utilisateur

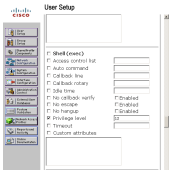


Étape 5. Configurez un mot de passe pour l'utilisateur. Nous configurons un mot de passe « **Cisco** » dans cet exemple



Étape 6. Installez le niveau de privilège de l'utilisateur sous le **shell (exécutif)**. Ici l'utilisateur est donné le niveau de privilège 12 ou le Service_GP.

Remarque: C'est la principale différence avec l'authentification IOS. Avec PXM que nous le privilège n'assignons pas enable, plutôt nous assignent le privilège de shell (exécutif) à l'utilisateur.



Cliquez sur Submit pour commettre les modifications.

Vérifiez

Le telnet à MGX et s'assurent que l'utilisateur obtiennent le niveau de privilège que nous avons configuré sur le serveur ACS (c.-à-d. SERVICE_GP ou niveau de privilège 12) :

```
telnet 172.16.157.88 d'aptcwm02%
Essayant 172.16.157.88…
Connecté à 172.16.157.88.
Le caractère d'échappement est « ^] ».
Nom d'utilisateur : mgx_test
Mot de passe : Cisco


8950A.7.PXM.a > qui

ID utilisateur Access d'inactif d'emplacement de port de commencé à
-------------------------------------------------------------------
-------
consolez 7 le port de console de 0:00:14 Cisco CISCO_GP 20:55:29 JUL28
telnet.01 * 7 le <<< mgx_test de 0:00:00 SERVICE_GP 10.66.69.126
21:04:11 JUL28
```

Vérifiez les stats d'AAA pour voir l'événement d'authentification TACACS+ :

```
8950A.7.PXM.a > dspaaa-stats

Dernier effacé en fonction : 07/28/2005 17:55:42 (PST)


La dernière bonne procédure de connexion authen : le
telnet.01 mgx_test 10.66.69.126
           tacacs+ 10.66.79.246/49
          07/28/2005 21:27:34 (PST)
Dernier bon priv de grp :     le telnet.01 mgx_test 10.66.69.126
           tacacs+ 10.66.79.246/49
          07/28/2005 21:27:34 (PST)
Dernier cmd défectueux :        AUCUN

Tapez <CR> pour continuer, Q<CR> à arrêter :

NIVEAU COUNTS__ ____SWITCH
Méthode :                gens du pays TACACS de Cisco
# authen les pannes :      0 18 0
# pannes d'auteur de grp :  0 0 0
# pannes d'auteur de cmd :  0                -----             0
# authen les chutes de nouveau à : 0 32 0
# l'auteur tombe de nouveau à : 0 1 0
# authen inaccessible :   -----             -----             0
# auteur inaccessible :   -----             -----             0
```

```
# défis RX :        -----              -----              0
# commandes de puissance de socket :     -----              -----
            0
# messages TX :          -----              -----              9
# messages RX :          -----              -----              9
# messages vidés :     -----              -----              0
# messages d'arrêt envoyés :  -----              -----              0
# AVPs pris en charge RX :    -----              -----              2
# AVPs non vérifié RX :  -----              -----              0
# AVPs inconnu RX :      -----              -----              0

Tapez <CR> pour continuer, Q<CR> à arrêter :

NIVEAU DU SERVEUR COUNTS__ ____TACACS+
Adresse IP du serveur :      10.66.79.246 0.0.0.0 0.0.0.0
Port de serveur :            49 0 0
# authen les pannes :      0 0 0
# pannes d'auteur de cmd :  0 0 0
# authen les chutes de nouveau à : 0 0 0
# l'auteur tombe de nouveau à : 0 0 0
# authen inaccessible :   0 0 0
# auteur inaccessible :   0 0 0
# défis RX :        0 0 0
# messages TX :          9 0 0
# messages RX :          9 0 0
# messages vidés :     0 0 0
# messages d'arrêt envoyés :  0 0 0
# AVPs pris en charge RX :    2 0 0
# AVPs non vérifié RX :  0 0 0
# AVPs inconnu RX :      0 0 0
Moyenne retard de réponse :     9 0 0
Retard maximum de réponse :     15 0 0
```

Les commandes suivantes sont liées à TACACS sur MGX :

```
M7.8.PXM.a > ? AAA

  Commandes disponibles
  ------------------
  cnfaaa-authen
  cnfaaa-auteur
  cnfaaa-ftpssh
  cnfaaa-ignorer-IOS
  cnfaaa-priv
  cnfaaa-demande
  cnfaaa-serveur
  delaaa-serveur
  dspaaa
  dspaaa-serveurs
  dspaaa-stats
  dspaaa-TAC-suivi
  setaaa-TAC-suivi
```

Informations connexes

- Gamme 8800/8900 guide de configuration du logiciel de Cisco MGX, version 5.4
- **Support et documentation techniques - Cisco Systems**