RTN – EC2LT

Authentification Radius - Cisco

I. Configuration de freeradius -ldap

I.1 Ajouter le schema de radius dans l'annuaire LDAP

- Pour la version 2.2 et inférieur

Ajouter la ligne :

include /etc/ldap/schema/radius.schema

dans le fichier /etc/ldap/slapd.conf

NB : vérifier que le fichier /etc/ldap/schema/radius.schema existe.

- Pour la version 2.3 et supérieur (avec une configuration utilisant le cn=config)

cd /etc/ldap/schema
touch schema-convert

Ajouter la ligne :

include /etc/ldap/schema/radius.schema

dans le fichier schema-convert

mkdir convert-output
slaptest -f schema-convert -F ./convert-output/

vim convert-output/cn\=config/cn\=schema/cn\=\{0\}radius.ldif

cd convert-output/cn\=config/cn\=schema/
ldapadd -Y EXTERNAL -H ldapi:/// -f ./cn\=\{0\}radius.ldif

I.2 Dans le fichier default activer le paramètre ldap dans les sections suivantes :

- authorize
- authenticate
- post-auth

I.3 Dans le fichier modules/ldap activer les paramètres ci-dessus:

server = "localhost" //l'adresse IP du serveur
identity = "cn=admin,dc=ec2lt,dc=sn" //le compte de l'admin
password = passer //mdp de l'admin
basedn = "dc=ec2lt,dc=sn" //le suffix
filter = "(uid=%{%{Stripped-User-Name}:-%{User-Name}})" //le filtre
password_attribute = userPassword //l'attribut qui correspond au mdp

I.4 Dans le fichier sites-enabled/inner-tunnel :

Activer le paramètre ldap de la section authorize

I.5 Utilisateur Radius

I.5.1 Utilisateur LDAP:

dn: uid=vitou,dc=ec2lt,dc=sn
objectClass: radiusprofile
objectClass: radiusObjectProfile
uid: vitou
userPassword: passer
radiusTunnelMediumType: IEEE-802
radiusTunnelType: VLAN
radiusTunnelPrivateGroupId: 10
cn: vitou

NB : L'attribut radiusTunnelPrivateGroupId définit le numéro de VLAN.

I.5.2 Utilisateur dans le fichier users :

babadi Login-Time := "any0700-1646", Cleartext-Password := "passer"
Tunnel-type = VLAN,
Tunnel-Medium-Type = IEEE-802,
Tunnel-Private-Group-ID = 20

II. Création de compte pour le client radius (le commutateur)

Le compte se crée dans le fichier clients.conf avec la syntaxe ci-dessus :

```
client ADRESSE_IP_CLIENT {
        secret = CLÉ_PARTAGÉE
}
```

Exemple :

```
client 192.168.1.1 {
        secret = passer123
}
```

III. Configuration du commutateur Cisco

III.1 Pour activer 802.1X pour l'ensemble du commutateur et déclarer le serveur Radius:

```
Switch#config terminal
Switch(config)#aaa new-model
Switch(config)#aaa authentication dot1x default group radius
```

III.2 Authentification réseau avec Radius

```
Switch(config)#dot1x system-auth-control
Switch(config)#aaa authorization network default group radius
Switch(config)#radius-server host ADRESSE_IP_SERVEUR_RADIUS auth-port 1812 key
CLÉ_PARTAGÉE
```

III.3 Configuration des ports sous contôle

Pour chaque port qui doit être sous contrôle 802.1X, les commandes suivantes doi- vent être passées:

```
Switch(config)#interface fastEthernet x/y    ;"x" le numéro de slot et "y"  le numéro de port
Switch(config-if)#switchport mode access
Switch(config-if)#dot1x port-control auto
```

IV. Test

test aaa group radius [user] [password]