Chapitre 4 - Sécurité

Sécurisation des accès

Configurer le mot de passe privilégié

`enable secret <MOT_DE_PASSE>`

Protège l'accès au mode privilégié.

Il est préférable d'utiliser `enable secret` plutôt que `enable password`.

Créer un compte administrateur local

`username admin privilege 15 secret <MOT_DE_PASSE>`

Crée l'utilisateur `admin` avec les droits administrateur.

Sécuriser la console

`line console 0`

Entre dans la configuration de la console.

`login local`

Utilise la base d'utilisateurs locale.

`exec-timeout 10 0`

Déconnecte la session après 10 minutes d'inactivité.

`logging synchronous`

Évite que les messages système perturbent la saisie.

Sécuriser les lignes VTY

`line vty 0 15`

Entre dans la configuration des accès distants.

Selon le modèle, la plage peut être `0 4` ou `0 15`.

`login local`

Utilise les comptes locaux.

`exec-timeout 10 0`

Déconnecte les sessions inactives après 10 minutes.

`transport input ssh`

Autorise uniquement SSH.

Chiffrer les mots de passe simples

`service password-encryption`

Masque les mots de passe configurés en clair dans la configuration.

Cette protection est faible et ne remplace pas l’utilisation de `secret`.

Vérifier les utilisateurs

`show running-config | include username`

Affiche les comptes locaux configurés.

Vérifier les lignes de connexion

`show running-config | section line`

Affiche la configuration des lignes console et VTY.

Configuration_SSH

Configurer le nom de l’équipement

```
hostname SW-ACC-01
```

Définit le nom du switch.

Configurer le nom de domaine

```
ip domain-name lab.local
```

Définit le domaine nécessaire à la génération des clés RSA.

Créer un utilisateur local

```
username admin privilege 15 secret <MOT_DE_PASSE>
```

Crée le compte administrateur.

Générer les clés RSA

```
crypto key generate rsa modulus 2048
```

Génère une clé RSA de 2048 bits.

Selon la version de Cisco IOS, la commande peut demander la taille de la clé après validation.

Activer SSH version 2

```
ip ssh version 2
```

Force l’utilisation de SSH version 2.

Configurer les lignes VTY

`line vty 0 15`

Sélectionne les lignes d’accès distant.

`login local`

Utilise les comptes locaux.

`transport input ssh`

Autorise uniquement SSH.

`exec-timeout 10 0`

Déconnecte les sessions inactives après 10 minutes.

Configurer l’adresse de management

`interface vlan 99`

Sélectionne l’interface VLAN de management.

`ip address 192.168.99.2 255.255.255.0`

Configure l’adresse IP.

`no shutdown`

Active l’interface VLAN.

`ip default-gateway 192.168.99.1`

Configure la passerelle du switch de niveau 2.

Vérifier SSH

`show ip ssh`

Affiche l’état du serveur SSH.

`show ssh`

Affiche les connexions SSH actives.

Se connecter depuis un ordinateur

`ssh admin@192.168.99.2`

Ouvre une connexion SSH vers le switch.

Supprimer les clés RSA

`crypto key zeroize rsa`

Supprime les clés RSA existantes.

Cette commande désactive temporairement SSH jusqu’à la génération de nouvelles clés.

Port Security

Port Security limite les adresses MAC autorisées sur un port Access.

Configurer Port Security

`interface GigabitEthernet0/1`

Sélectionne le port.

`switchport mode access`

Configure le port en mode Access.

`switchport access vlan 10`

Affecte le port au VLAN 10.

`switchport port-security`

Active Port Security.

`switchport port-security maximum 1`

Autorise une seule adresse MAC.

`switchport port-security mac-address sticky`

Apprend automatiquement l’adresse MAC connectée.

`switchport port-security violation restrict`

Bloque les trames non autorisées et incrémente le compteur de violations.

Modes de violation

`switchport port-security violation protect`

Ignore les trames des adresses MAC non autorisées sans désactiver le port.

`switchport port-security violation restrict`

Ignore les trames non autorisées et enregistre les violations.

`switchport port-security violation shutdown`

Place le port en état `err-disabled` lors d'une violation.

Le mode `shutdown` est souvent le mode par défaut.

Vérifier Port Security

`show port-security`

Affiche un résumé global.

`show port-security interface GigabitEthernet0/1`

Affiche les informations détaillées du port.

`show mac address-table secure`

Affiche les adresses MAC sécurisées.

Réactiver un port désactivé

`interface GigabitEthernet0/1`

Sélectionne le port.

`shutdown`

Désactive administrativement le port.

`no shutdown`

Réactive le port.

Il faut d'abord supprimer la cause de la violation.

Sécurisation des ports inutilisés

Créer un VLAN parking

`vlan 999`

Crée le VLAN 999.

`name PARKING`

Nomme le VLAN `PARKING`.

Sélectionner les ports inutilisés

`interface range GigabitEthernet0/10 - 22`

Sélectionne les ports inutilisés.

Affecter les ports au VLAN parking

`switchport mode access`

Configure les ports en mode Access.

`switchport access vlan 999`

Affecte les ports au VLAN parking.

Désactiver les ports

`shutdown`

Désactive administrativement les ports.

Ajouter une description

`description PORT_INUTILISE`

Ajoute une description claire.

Vérifier les ports désactivés

`show interfaces status`

Affiche l’état des ports.

Les ports désactivés administrativement apparaissent généralement en état `disabled`.

Réactiver un port

`interface GigabitEthernet0/12`

Sélectionne le port.

`no shutdown`

Réactive le port.

Pense à modifier le VLAN et la description avant de remettre le port en service.