Activer Secure Shell (SSH) sur un point d'accès (AP)

Table des matières

Introduction

Ce document décrit comment configurer un point d'accès (AP) afin d'activer l'accès basé sur Secure Shell (SSH).

Conditions préalables

Exigences

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

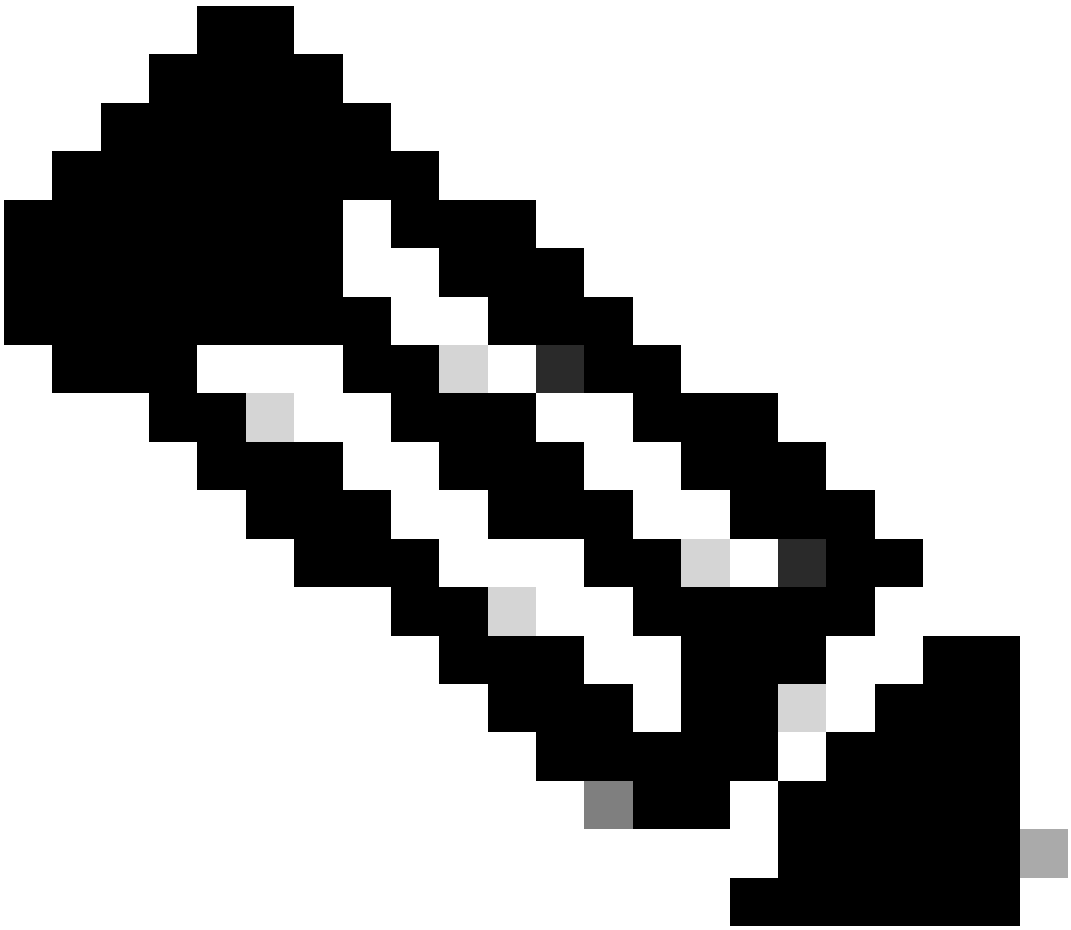
- Connaissance de la configuration des points d'accès Cisco Aironet
- Connaissances de base de SSH et des concepts de sécurité associés

Composants utilisés

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

- Point d'accès de la gamme Aironet 1200 qui exécute le logiciel Cisco IOS® Version 12.3(8)JEB

- PC ou ordinateur portable avec utilitaire client SSH



Remarque : ce document utilise l'utilitaire client SSH afin de vérifier la configuration. Vous pouvez utiliser n'importe quel utilitaire client tiers afin de vous connecter au point d'accès avec l'utilisation de SSH.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Conventions

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

Accédez à l'interface de ligne de commande (CLI) sur le point

d'accès Aironet

Vous pouvez utiliser l'une de ces méthodes afin d'accéder à l'interface de ligne de commande (CLI) sur l'AP Aironet :

- Le port de console
- Telnet
- SSH

Si l'AP a un port de console et que vous avez un accès physique à l'AP, vous pouvez utiliser le port de console afin de vous connecter à l'AP et modifier la configuration si nécessaire. Pour plus d'informations sur la façon d'utiliser le port de console afin de se connecter au point d'accès, référez-vous à la section Connexion aux points d'accès de la gamme 1200 localement du documentConfigurer le point d'accès pour la première fois.

Si vous ne pouvez accéder au point d'accès que par le biais d'Ethernet, utilisez le protocole Telnet ou le protocole SSH afin de vous connecter au point d'accès.

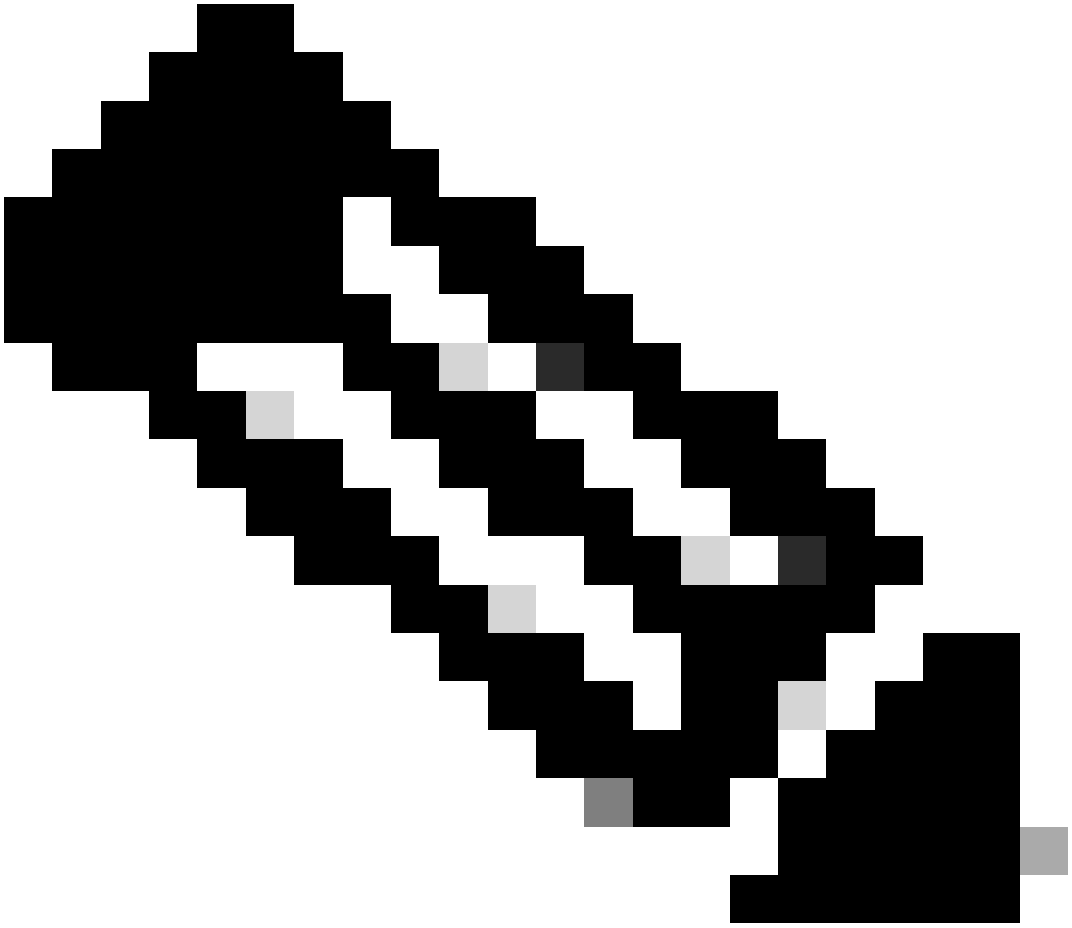
Le protocole Telnet utilise le port 23 pour la communication. Telnet transmet et reçoit des données en texte clair. Comme la communication de données s'effectue en texte clair, un pirate peut facilement compromettre les mots de passe et accéder au point d'accès. La RFC 854 définit Telnet et étend Telnet avec des options de nombreuses autres RFC.

SSH est une application et un protocole qui permet de remplacer les outils Berkley en toute sécurité. SSH est un protocole qui fournit une connexion à distance sécurisée à un périphérique de couche 2 ou 3. Il existe deux versions de SSH : SSH version 1 et SSH version 2. Cette version du logiciel prend en charge les deux versions SSH. Si vous ne spécifiez pas le numéro de version, le point d'accès utilise par défaut la version 2.

SSH offre plus de sécurité pour les connexions distantes que Telnet, car il fournit un chiffrement fort lorsqu'un périphérique est authentifié. Ce chiffrement est un avantage par rapport à une session Telnet, dans laquelle la communication s'effectue en texte clair. Pour plus d'informations sur SSH, référez-vous à la FAQ sur Secure Shell (SSH). La fonctionnalité SSH dispose d'un serveur SSH et d'un client SSH intégré.

Le client prend en charge les méthodes d'authentification suivantes :

- RADIUS
- Authentification et autorisation locales.



Remarque : la fonctionnalité SSH de cette version logicielle ne prend pas en charge la sécurité IP (IPSec).

Vous pouvez configurer des AP pour SSH à l'aide de l'interface de ligne de commande ou de l'interface graphique utilisateur. Ce document explique les deux méthodes de configuration.

Configurer

Configuration CLI

Cette section fournit des informations sur la configuration des fonctionnalités à l'aide de l'interface de ligne de commande.

Instructions pas à pas

Afin d'activer l'accès basé sur SSH sur l'AP, vous devez d'abord configurer l'AP en tant que

serveur SSH. Suivez ces étapes afin de configurer un serveur SSH sur l'AP à partir de l'interface de ligne de commande :

1. Configurez un nom d'hôte et un nom de domaine pour le point d'accès.

```
<#root>

AP#

configure terminal

!--- Enter global configuration mode on the AP.

AP<config>#

hostname Test

!--- This example uses "Test" as the AP host name.

Test<config>#

ip domain name domain

!--- This command configures the AP with the domain name "domain name".
```

2. Générez une clé Rivest, Shamir et Adelman (RSA) pour votre point d'accès.

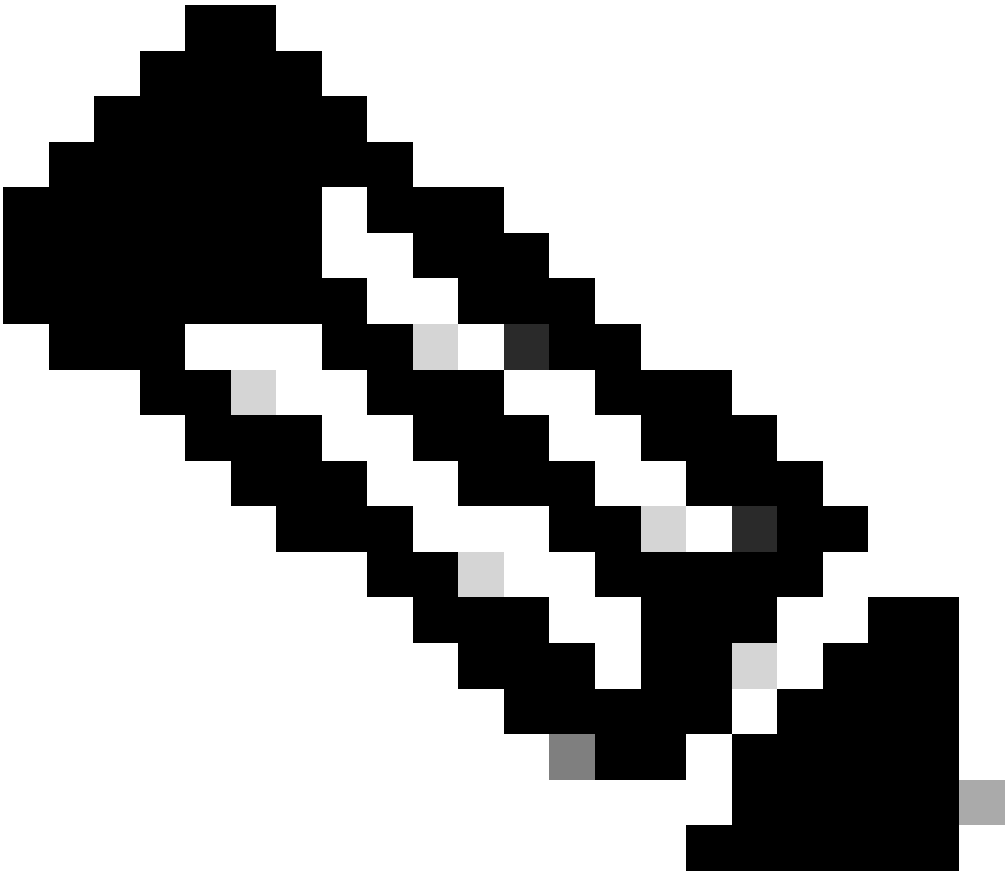
   La génération d'une clé RSA active SSH sur l'AP. Exécutez cette commande en mode de configuration globale :

```
<#root>

Test<config>#

crypto key generate rsa rsa_key_size

!--- This generates an RSA key and enables the SSH server.
```



Remarque : la taille de clé RSA minimale recommandée est 1024.

3. Configurez l'authentification des utilisateurs sur le point d'accès.

   Sur le point d'accès, vous pouvez configurer l'authentification des utilisateurs pour qu'elle utilise la liste locale ou un serveur AAA (Authentication, Authorization, and Accounting) externe. Cet exemple utilise une liste générée localement afin d'authentifier les utilisateurs :

   <#root>

   ```
   Test<config>#
   aaa new-model

   !--- Enable AAA authentication.

   Test<config>#
   aaa authentication login default local none
   ```

```
!--- Use the local database in order to authenticate users.

Test<config>#

username Test password Test123

!--- Configure a user with the name "Test".

Test<config>#

username ABC password xyz123

!--- Configure a second user with the name "Domain".
```

Cette configuration configure le point d'accès pour effectuer l'authentification basée sur l'utilisateur avec l'utilisation d'une base de données locale qui est configurée sur le point d'accès. L'exemple configure deux utilisateurs dans la base de données locale, "Test" et "ABC".

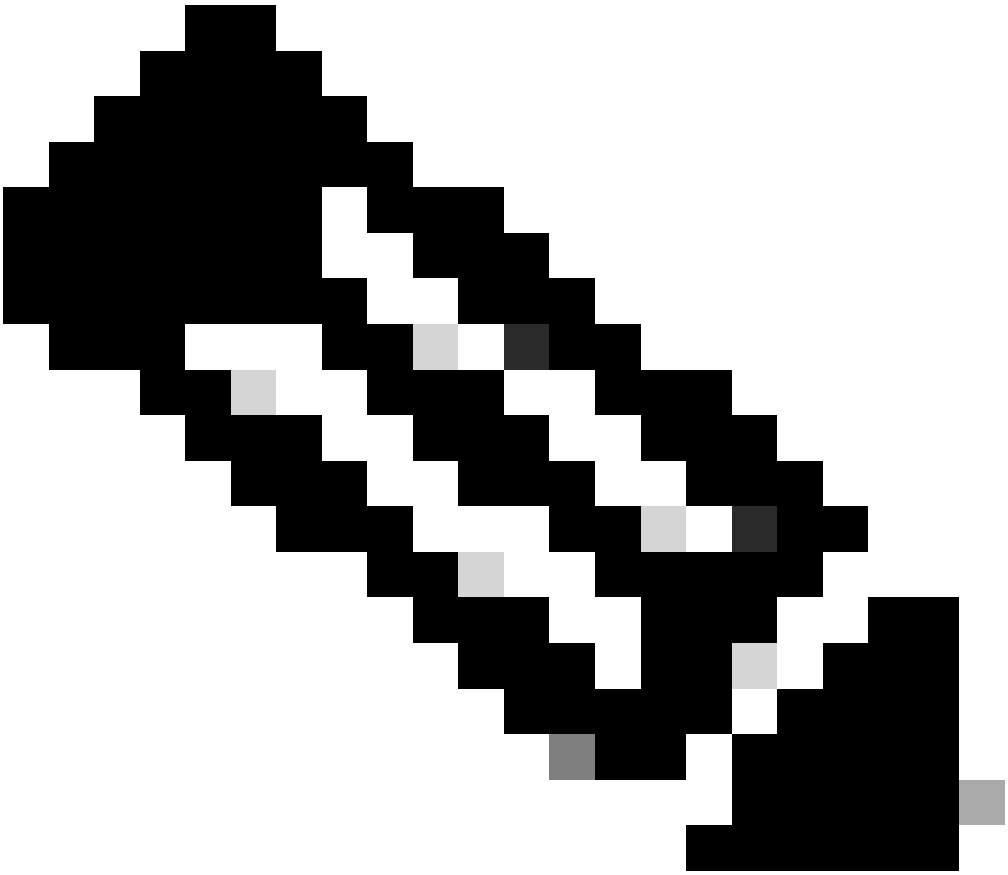
4. Configurez les paramètres SSH.

<#root>

```
Test<config>#

ip ssh {[timeout seconds] | [authentication-retries integer]}

!--- Configure the SSH control variables on the AP.
```



Remarque : vous pouvez spécifier le délai d'attente en secondes, mais il ne doit pas dépasser 120 secondes. Il est défini par défaut à 120. Il s'agit de la spécification qui s'applique à la phase de négociation SSH. Vous pouvez également spécifier le nombre de tentatives d'authentification, mais ne pas dépasser cinq. La valeur par défaut est trois.

Configuration de la GUI

Vous pouvez également utiliser la GUI afin d'activer l'accès basé sur SSH sur le point d'accès.

Instructions pas à pas

Procédez comme suit :

1. Connectez-vous au point d'accès via le navigateur.

   La fenêtre Summary Status s'affiche.

2. Cliquez sur Services dans le menu de gauche.

La fenêtre Récapitulatif des services s'affiche.

3. Cliquez sur Telnet/SSH afin d'activer et de configurer les paramètres Telnet/SSH.

   La fenêtre Services : Telnet/SSH s'affiche. Faites défiler jusqu'à la zone Secure Shell Configuration. Cliquez sur Enable à côté de Secure Shell, et entrez les paramètres SSH comme le montre cet exemple :

   Cet exemple utilise les paramètres suivants :

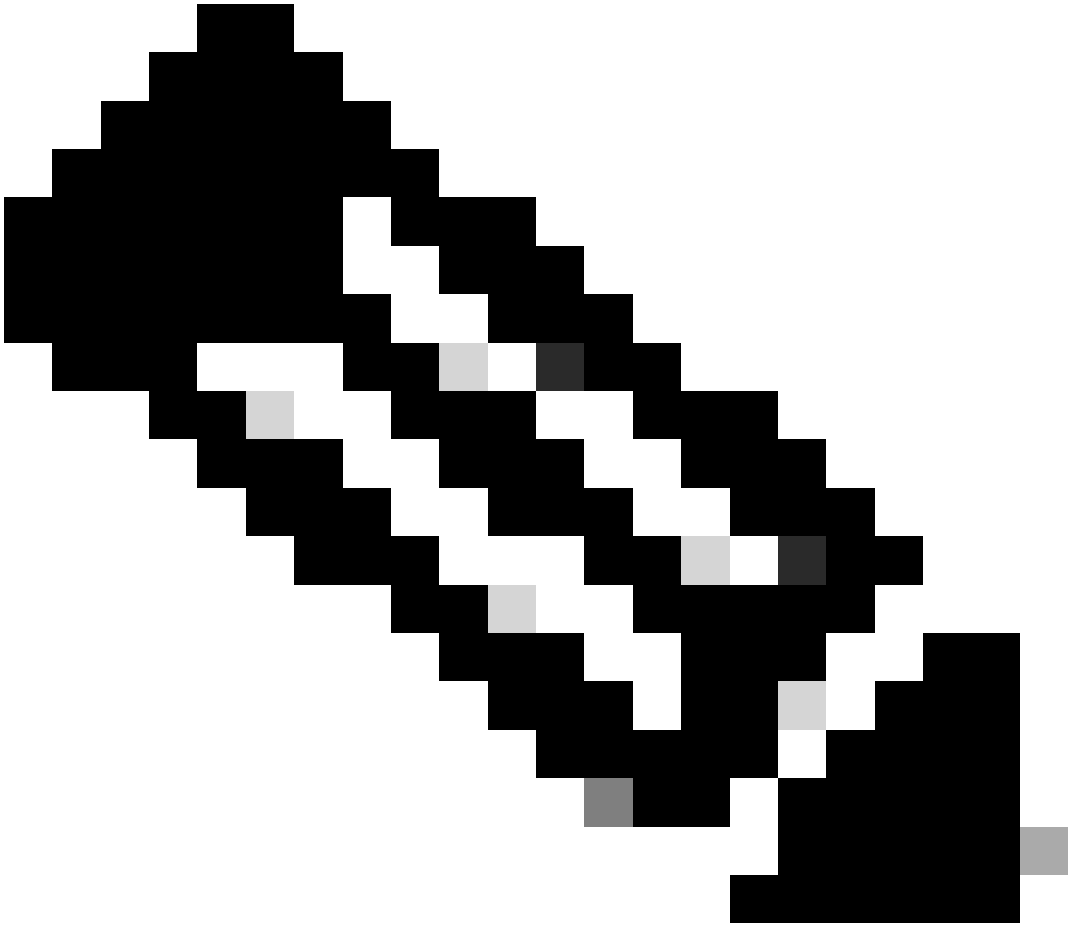
   - Nom du système : Test
   - Nom de domaine : DOMAINE
   - Taille de la clé RSA : 1024
   - Délai d'authentification : 120
   - Tentatives d'authentification : 3

4. Cliquez sur Apply afin de sauvegarder les modifications.

Vérifier

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

L'outil Output Interpreter Tool (OIT) prend en charge certaines commandes show. Utilisez l'OIT pour afficher une analyse de la sortie de la commande show .



Remarque : seuls les utilisateurs Cisco enregistrés peuvent accéder aux informations et aux outils Cisco internes.

- show ip ssh : vérifie si SSH est activé sur l'AP et vous permet de vérifier la version de SSH qui s'exécute sur l'AP. Ce résultat fournit un exemple :
- show ssh : permet d'afficher l'état de vos connexions au serveur SSH. Ce résultat fournit un exemple :

À présent, initiez une connexion via un PC qui exécute un logiciel SSH tiers, puis essayez de vous connecter au point d'accès. Cette vérification utilise l'adresse IP AP, 10.0.0.2. Étant donné que vous avez configuré le nom d'utilisateur Test, utilisez ce nom afin d'accéder à l'AP via SSH :

Dépannage

Utilisez cette section pour dépanner votre configuration.

Si vos commandes de configuration SSH sont rejetées comme des commandes illégales, vous n'avez pas correctement généré une paire de clés RSA pour votre AP.

Désactiver SSH

Afin de désactiver SSH sur un AP, vous devez supprimer la paire RSA qui est générée sur l'AP. Afin de supprimer la paire RSA, émettez la commande crypto key zeroize rsa en mode de configuration globale. Lorsque vous supprimez la paire de clés RSA, vous désactivez automatiquement le serveur SSH. Ce résultat fournit un exemple :

Informations connexes

- Page d'assistance SSH (Secure Shell)
- Assistance technique de Cisco et téléchargements

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.