Comprendre les algorithmes de chiffrement SSH sur le correctif 4 d'ISE 3.3

Table des matières

Introduction

Ce document décrit à propos des algorithmes de chiffrement SSH sur ISE version 3.3 Patch 4

Conditions préalables

Vous devez posséder les connaissances de base de Cisco Identity Service Engine (ISE)

Connaissance du protocole SSH

Connaissance des algorithmes de clé hôte

Composants requis

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

- Correctif 4 de Cisco Identity Services Engine 3.3

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.

Objectifs

Développer et mettre en oeuvre des commandes CLI pour prendre en charge des algorithmes SSH configurables, en répondant aux vulnérabilités de sécurité selon vos besoins.

Avantages fonctionnels

1. Conformité de sécurité SSH améliorée avec les directives NIST.
2. Options de configuration flexibles pour les algorithmes SSH afin de répondre à des stratégies de sécurité spécifiques.

Fonctionnalités clés implémentées

1. Algorithme HostKey et Hostkey configurable à partir de l'interface CLI.
2. Prise en charge de ecdsa-sha2-nistp256 et de la clé d'hôte ed.
3. Prise en charge de hmac-sha2-256 et hmac-sha2-512 pour les connexions SSH sécurisées

Commandes CLI

- Service ssh host-key-algorithm
- Service sshd host-key
- Service sshd host-key-algorithm
- Service sshd mac-algorithm

Algorithme de clé hôte SSH configurable

Pour configurer l'algorithme SSH HostKey pour la communication avec un serveur externe

Commande : asc-ise33p4/admin(config)# service ssh host-key-algorithm ?

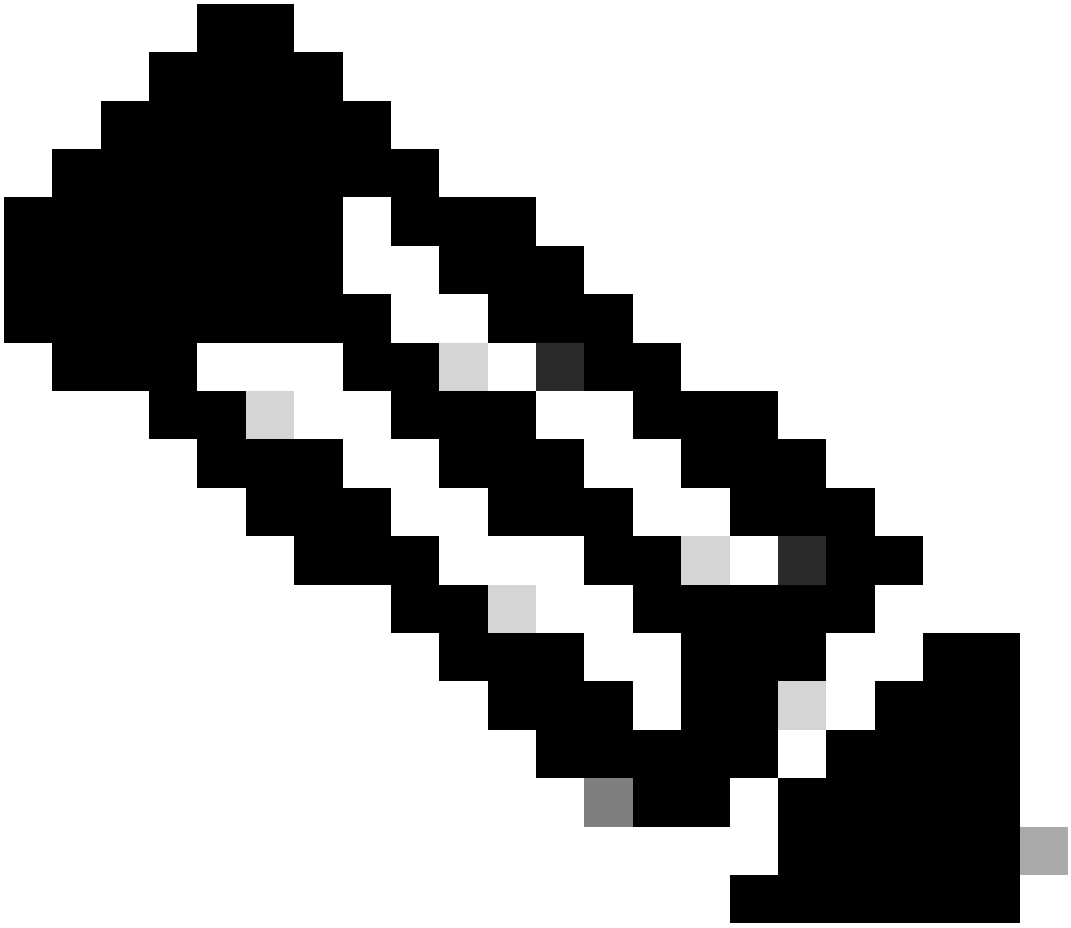
Achèvement possible :

ecdsa-sha2-nistp256 Configuration de l'algorithme ecdsa-sha2-nistp256

rsa-sha2-256 Configuration de l'algorithme rsa-sha2-256

rsa-sha2-512 Configuration de l'algorithme rsa-sha2-512

ssh-rsa Configuration de l'utilitaire ssh-rsa



Remarque : Ceci est pour SSH

Algorithme de clé hôte SSHD configurable

Pour configurer la clé hôte SSHD pour l'authentification du serveur SSH.

Commande : asc-ise33p4/admin(config)# service sshd host-key ?

Achèvement possible :

host-ecdsa-256 Configuration ssh host ecdsa 256 key

host-ed25519 Configurer ssh host ed25519 clé

host-rsa Configurer ssh host rsa key

Pour configurer l'algorithme de clé hôte SSHD pour l'authentification du serveur SSH.

Commande : asc-ise33p4/admin(config)#service sshd host-key-algorithm ?

Achèvement possible :

ecdsa-sha2-nistp256 Configuration de l'algorithme ecdsa-sha2-nistp256

rsa-sha2-256 Configuration de l'algorithme rsa-sha2-256

rsa-sha2-512 Configuration de l'algorithme rsa-sha2-512

ssh-ed25519 Configuration de l'algorithme ssh-ed25519

Pour configurer l'algorithme MAC SSHD pour l'authentification du serveur SSH.

Commande : asc-ise33p4/admin(config)#service sshd mac-algorithm ?

Achèvement possible :

hmac-sha1 Configuration de l'algorithme hmac-sha1

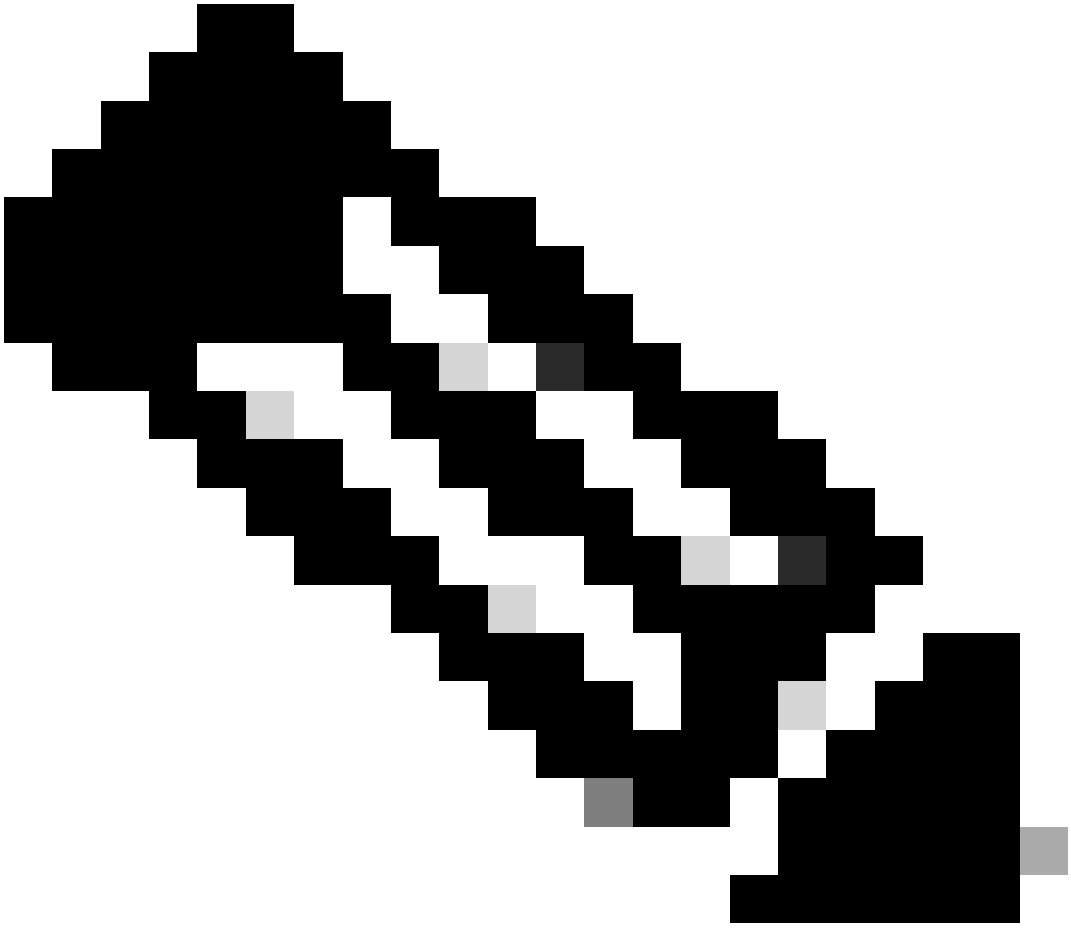
hmac-sha1-etm-openssh.com Configuration de l'algorithme hmac-sha1-etm-openssh.com

hmac-sha2-256 Configuration de l'algorithme hmac-sha2-256

hmac-sha2-256-etm-openssh.com Configuration de l'utilitaire hmac-sha2-256-etm@openssh.com

hmac-sha2-512 Configuration de l'algorithme hmac-sha2-512

hmac-sha2-512-etm-openssh.com Configuration de l'utilitaire hmac-sha2-512-etm@openssh.com



Remarque : Ceci est pour SSHD

Dépannage

Vérifier

SSH :
isepri33/admin(config)#service ssh host-key-algorithm ecdsa-sha2-nistp256

isepri33/admin#show running-config service ssh
service ssh host-key-algorithm ecdsa-sha2-nistp256

SSHD :

isepri33/admin(config)#service sshd host-key-algorithm ecdsa-sha2-nistp256

isepri33/admin#show running-config service sshd
service sshd enable
service sshd encryption-algorithm aes128-ctr aes128-gcm-openssh.com aes256-ctr aes256-gcm-openssh.com chacha20-poly1305-openssh.com
service sshd host-key-algorithm ecdsa-sha2-nistp256
service sshd mac-algorithm hmac-sha1 hmac-sha2-256 hmac-sha2-512
service sshd host-key host-rsa

Extrait de journal :

isepri33/admin#show logging system confd/confd.log
2025-03-18 08:35:25,241 [INFO] service_conf.py update_host_key_algorithms line:575 Mise à jour des algorithmes de clés d'hôte SSH avec succès
2025-03-18 08:35:39,056 [INFO] service_conf.py update_host_key_algorithms line:567 Host key Algorithms : ecdsa-sha2-nistp256
2025-03-18 08:35:39,260 [INFO] service_conf.py restart_sshd line:259 Sshd redémarré avec succès

2025-03-18 08:48:20,194 [INFO] service_conf.py update_host_key_algorithms line:567 Host key Algorithms : ecdsa-sha2-nistp256
2025-03-18 08:48:20,396 [INFO] service_conf.py restart_sshd line:259 Sshd redémarré avec succès
2025-03-18 08:48:20,400 [INFO] service_conf.py update_host_key_algorithms line:575 Mise à jour des algorithmes de clés d'hôte SSH avec succès
2025-03-18 08:49:00,442 [INFO] service_conf.py update_host_key_algorithms line:567 Host key Algorithms : ecdsa-sha2-nistp256
2025-03-18 08:49:00,672 [INFO] service_conf.py restart_sshd line:259 Sshd redémarré avec succès
2025-03-18 08:49:00,674 [INFO] service_conf.py update_host_key_algorithms line:575 Mise à jour des algorithmes de clés d'hôte SSH avec succès

Forum aux questions

Question : Quel est l'algorithme de clé d'hôte SSH par défaut activé sur ISE ?

Réponse : Elles sont :

- rsa-sha2-256
- rsa-sha2-512

Question : Quel est l’algorithme de clé MAC SSHD par défaut ?

Réponse : Elles sont :

- hmac-sha1
- hmac-sha2-256
- hmac-sha2-512

Question : Quelle est la clé hôte SSHD par défaut ?

Réponse : host-rsa

Question : Où se trouve la clé d'hôte SSH par défaut ?

Réponse : Elles sont :

- rsa-sha2-256
- rsa-sha2-512
- ssh-rsa

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.