瞭解ISE 3.3補丁4上的SSH加密演算法

目錄

簡介

本文檔介紹ISE 3.3版補丁4上的SSH加密演算法

前提條件

您必須具備思科身份服務引擎(ISE)的基本知識

有關SSH協定的知識

主機金鑰演算法知識

所需元件

本文件中的資訊是以下列軟體和硬體版本為依據

- 思科身分識別服務引擎3.3補丁4

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

目標

開發並實施CLI命令以支援可配置的SSH演算法，根據您的要求解決安全漏洞。

功能優勢

1. 根據NIST准則增強了SSH安全合規性。
2. SSH演算法的靈活配置選項可滿足特定的安全策略。

實施的主要功能

1. 可在CLI上配置主機金鑰和主機金鑰演算法。
2. 支援ecdsa-sha2-nistp256和ed主機金鑰。
3. 支援安全SSH連線的hmac-sha2-256和hmac-sha2-512

CLI命令

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

可配置的SSH主機金鑰演算法

配置用於外部伺服器通訊的SSH主機金鑰演算法

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

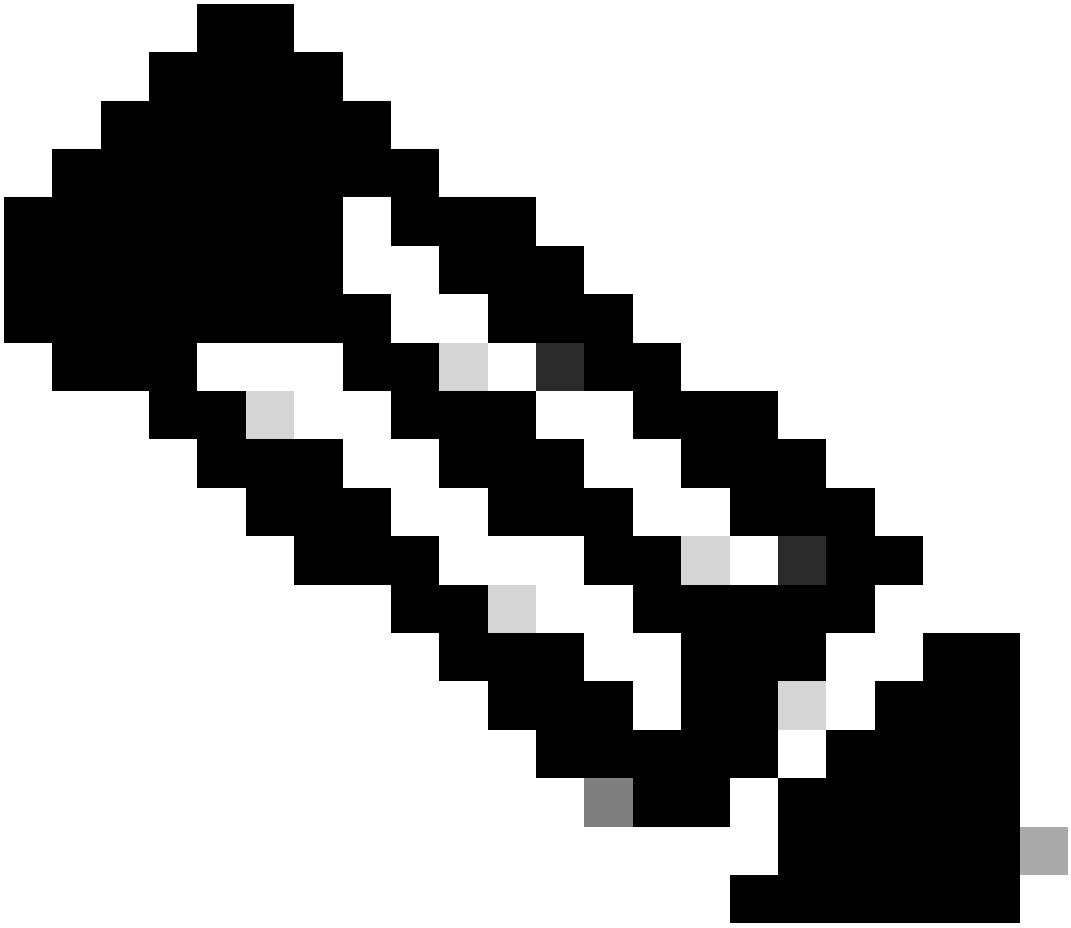
可能的完成：

ecdsa-sha2-nistp256配置ecdsa-sha2-nistp256 algo

rsa-sha2-256配置rsa-sha2-256 algo

rsa-sha2-512配置rsa-sha2-512 algo

ssh-rsa配置ssh-rsa algo



附註：此命令用於SSH

可設定SSHD主機金鑰演演算法

配置用於SSH伺服器身份驗證的SSHD主機金鑰。

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

可能的完成：

host-ecdsa-256配置ssh host ecdsa 256金鑰

host-ed25519配置ssh host ed25519 key

host-rsa配置ssh host rsa key

配置用於SSH伺服器身份驗證的SSHD主機金鑰演算法。

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

可能的完成：

ecdsa-sha2-nistp256配置ecdsa-sha2-nistp256 algo

rsa-sha2-256配置rsa-sha2-256 algo

rsa-sha2-512配置rsa-sha2-512 algo

ssh-ed25519配置ssh-ed25519 algo

配置用於SSH伺服器身份驗證的SSHD MAC演算法。

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

可能的完成：

hmac-sha1配置hmac-sha1 algo

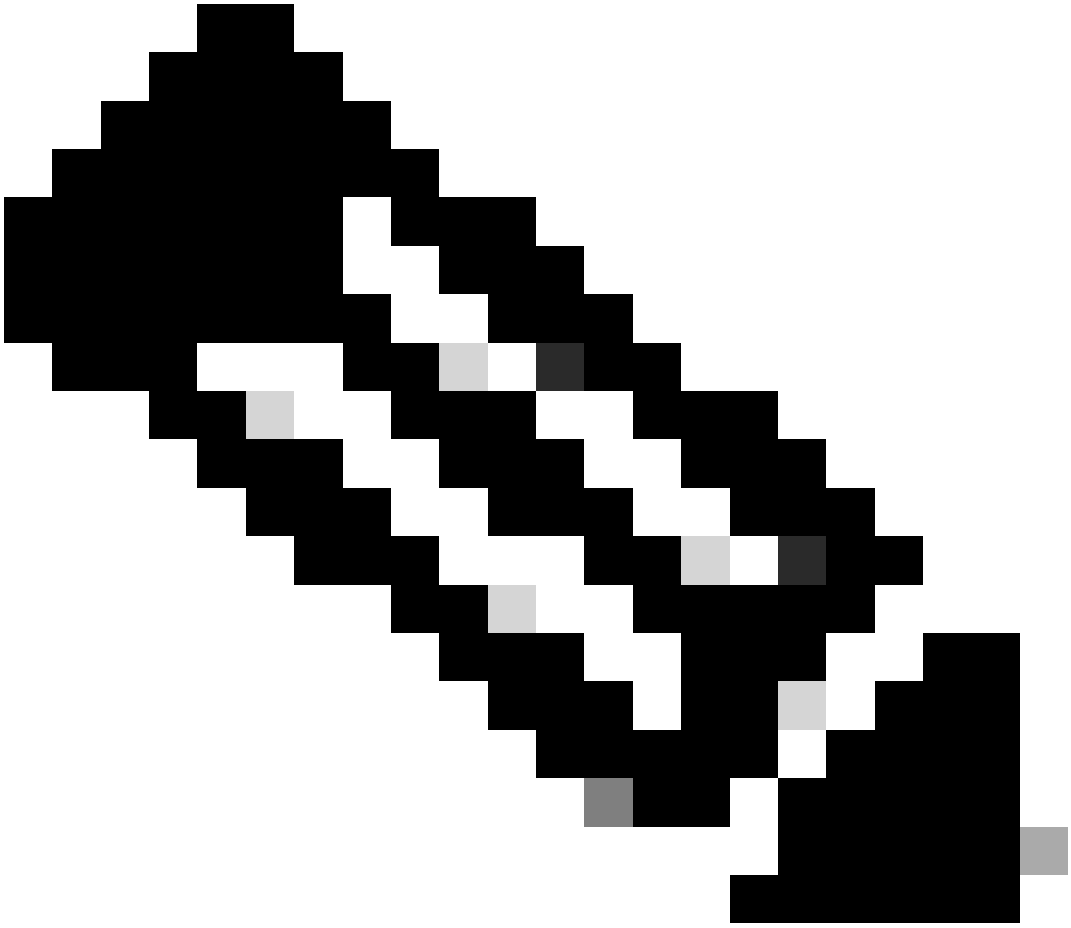
hmac-sha1-etm-openssh.com配置hmac-sha1-etm-openssh.com algo

hmac-sha2-256配置hmac-sha2-256 algo

hmac-sha2-256-etm-openssh.com配置hmac-sha2-256-etm@openssh.com algo

hmac-sha2-512配置hmac-sha2-512 algo

hmac-sha2-512-etm-openssh.com配置hmac-sha2-512-etm@openssh.com algo



附註：這是為SSHD設計的

疑難排解

驗證

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

isepri33/admin#show running-config service ssh
服務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
```

日誌片段：

```
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已成功更新SSH主機金鑰演算法
2025-03-18 08:35:39,056 [INFO] service_conf.py update_host_key_algorithms行：567主機金鑰演算法：ecdsa-sha2-nistp256
2025-03-18 08:35:39,260 [INFO] service_conf.py restart_sshd行：259成功重新啟動sshd

2025-03-18 08:48:20,194 [INFO] service_conf.py update_host_key_algorithms行：567主機金鑰演算法：ecdsa-sha2-nistp256
2025-03-18 08:48:20,396 [INFO] service_conf.py restart_sshd line:259成功重新啟動sshd
2025-03-18 08:48:20,400 [INFO] service_conf.py update_host_key_algorithms line:575已成功更新SSH主機金鑰演算法
2025-03-18 08:49:00,442 [INFO] service_conf.py update_host_key_algorithms行：567主機金鑰演算法：ecdsa-sha2-nistp256
2025-03-18 08:49:00,672 [INFO] service_conf.py restart_sshd行：259成功重新啟動sshd
2025-03-18 08:49:00,674 [INFO] service_conf.py update_host_key_algorithms line:575已成功更新SSH主機金鑰演算法
```

常見問題

問題：在ISE上啟用的預設SSH主機金鑰演算法是什麼？

答案：它們是：

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

問題：預設的SSHD MAC金鑰演算法是什麼？

答案：它們是：

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

問題：預設的SSHD主機金鑰是什麼？

答案：host-rsa

問題：預設SSH主機金鑰在哪裡？

答案：它們是：

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

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。