ISE 3.3パッチ4のSSH暗号化アルゴリズムについて

内容

はじめに

このドキュメントでは、ISEバージョン3.3パッチ4のSSH暗号化アルゴリズムについて説明します

前提条件

Cisco Identity Service Engine(ISE)の基本的な知識が必要です

SSHプロトコルに関する知識

ホストキーアルゴリズムの知識

必要なコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Services Engine 3.3パッチ4

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

目的

設定可能なSSHアルゴリズムをサポートするCLIコマンドを開発および実装し、要件に応じてセキュリティの脆弱性に対処する。

機能の利点

1. NISTガイドラインに準拠した拡張SSHセキュリティ
2. 特定のセキュリティポリシーに適合するSSHアルゴリズムの柔軟な設定オプション

実装された主な機能

1. CLIから設定可能なHostKeyおよびHostkeyアルゴリズム
2. ecdsa-sha2-nips256およびedホストキーのサポート
3. セキュアSSH接続でのhmac-sha2-256およびhmac-sha2-512のサポート

CLI コマンド

- Service ssh host-key-algorithm（SSHホストキーアルゴリズム）
- サービスsshdホストキー
- サービスsshdホストキーアルゴリズム
- サービスsshd macアルゴリズム

設定可能なSSHホストキーアルゴリズム

外部サーバ通信用のSSHホストキーアルゴリズムを設定するには

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

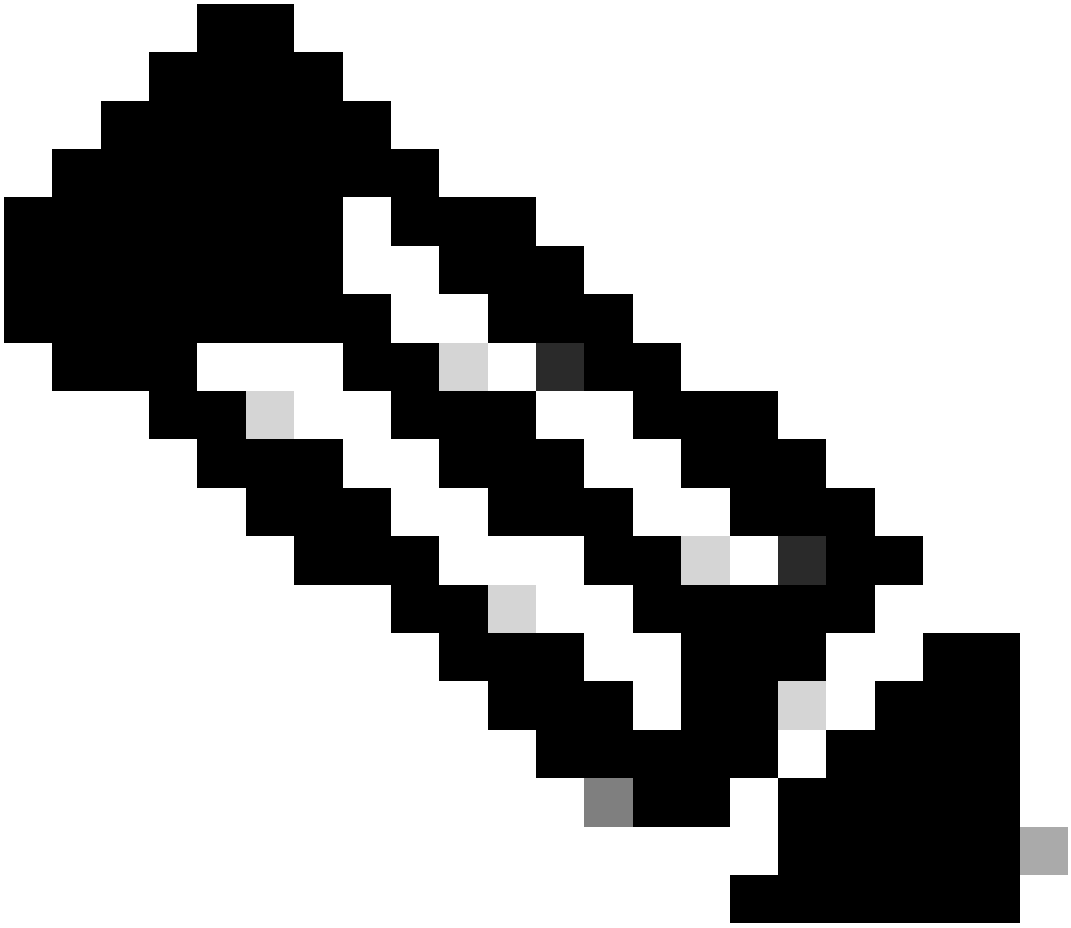
実行可能な完了：

ecdsa-sha2-nips256 ecdsa-sha2-nips256アルゴの設定

rsa-sha2-256 Rsa-sha2-256 algoの設定

rsa-sha2-512 Rsa-sha2-512 algoの設定

ssh-rsa ssh-rsa algoの設定



注：これはSSH用です。

設定可能なSSHDホストキーアルゴリズム

SSHサーバ認証用のSSHDホストキーを設定します。

コマンド:asc-ise33p4/admin(config)# service sshd host-key ?

実行可能な完了：

host-ecdsa-256 ssh host ecdsa 256キーの設定

host-ed25519 ssh host ed25519 keyを設定します。

host-rsa sshホストrsaキーの設定

SSHサーバ認証用にSSHDホストキーアルゴリズムを設定する。

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

実行可能な完了：

ecdsa-sha2-nips256 ecdsa-sha2-nips256アルゴの設定

rsa-sha2-256 Rsa-sha2-256 algoの設定

rsa-sha2-512 Rsa-sha2-512 algoの設定

ssh-ed25519ssh-ed25519 algoの設定

SSHサーバ認証用にSSHD MACアルゴリズムを設定する方法

コマンド: asc-ise33p4/admin(config)#service sshd mac-algorithm ?

実行可能な完了：

hmac-sha1設定hmac-sha1 algo

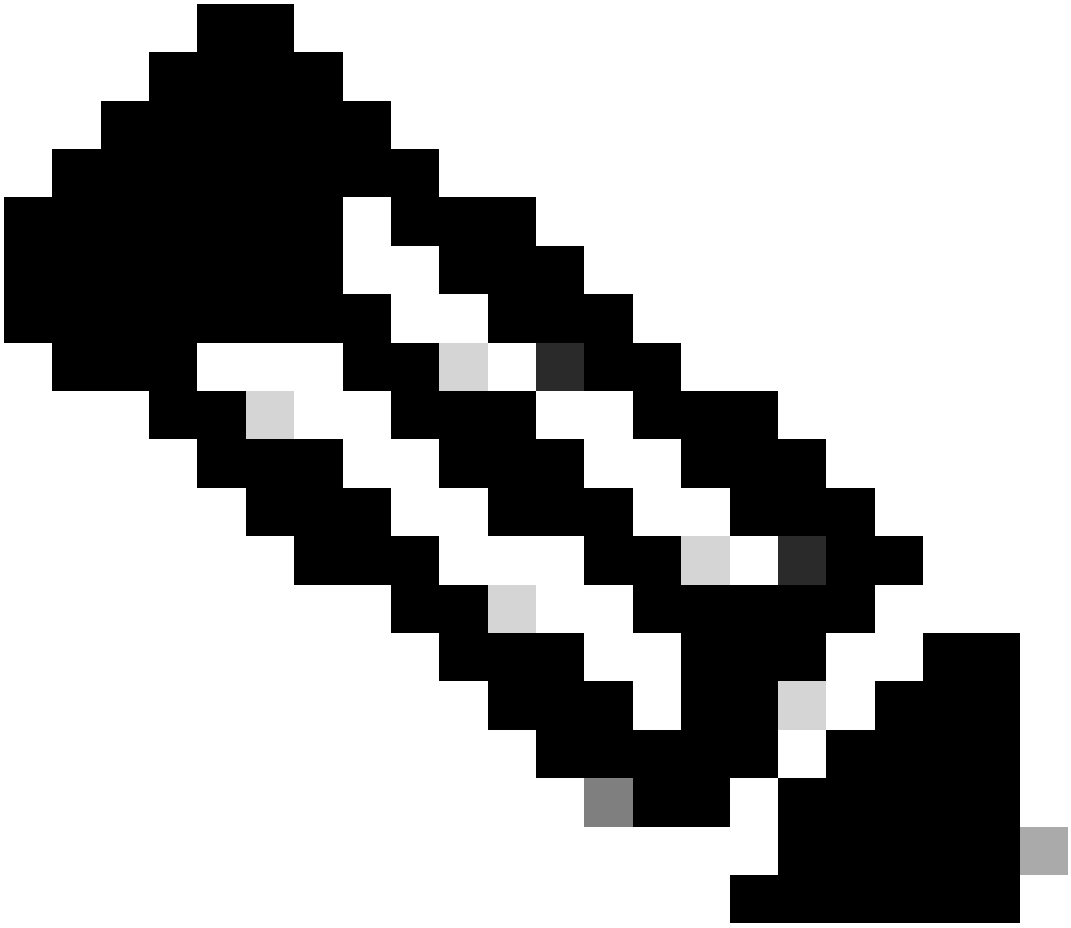
hmac-sha1-etm-openssh.com hmac-sha1-etm-openssh.com algoの設定

hmac-sha2-256 hmac-sha2-256 algoの設定

hmac-sha2-256-etm-openssh.com hmac-sha2-256-etm@openssh.com algoの設定

hmac-sha2-512 hmac-sha2-512 algoの設定

hmac-sha2-512-etm-openssh.com hmac-sha2-512-etm@openssh.com algoの設定



注：これはSSHD用です

トラブルシューティング

確認

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（ゲートキーパー制御）

SSHD:

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

isepri33/admin#show running-config service sshd
service sshd enable (サービスSSHDの有効化)
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コマンド

ログの一部：

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 Updated SSH Host Keys Algorithms successfully
2025-03-18 08:35:39,056 [INFO] service_conf.py update_host_key_algorithms line:567 Host key Algorithms:ecdsa-sha2-nips256
2025-03-18 08:35:39,260 [INFO] service_conf.py restart_sshd line:259 Restarted sshd successfully

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 Restarted sshd successfully
2025-03-18 08:48:20,400 [INFO] service_conf.py update_host_key_algorithms line:575 Updated SSH Host Keys Algorithms successfully
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 Restarted sshd successfully
2025-03-18 08:49:00,674 [INFO] service_conf.py update_host_key_algorithms line:575 Updated SSH Host Keys Algorithms successfully

FAQ

質問：ISEで有効になっているデフォルトのSSHホストキーアルゴリズムは何ですか。

正解：次のとおりです。

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

質問：デフォルトのSSHD MACキーアルゴリズムは何ですか。

正解：次のとおりです。

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

質問：デフォルトのSSHDホストキーは何ですか。

正解：host-rsa

質問：デフォルトのSSHホストキーは何ですか。

正解：次のとおりです。

- rsa-sha2-256
- rsa-sha2-512
- ssh-rsa（セキュアシェル）

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。