

ISE の FIPS モード

目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ISE の設定 FIP モード](#)

[FIP モードを有効にしている間よくある問題](#)

[問題](#)

[解決策](#)

[問題](#)

[解決策](#)

概要

この資料は識別 Service エンジン (ISE) の連邦情報処理標準 (FIP) 対応プロトコルを記述したもので、FIP を有効にしている間よくある問題は出会いました。FIP は非軍事政府関係機関および政府接触器による計算機 システムの使用のための米国連邦 政府によって開発される規格です。

前提条件

要件

このドキュメントに関する固有の要件はありません。

使用するコンポーネント

この文書に記載されている情報は ISE 2.1 バージョンに基づいています。

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たものです。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。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

ISE の FIP モードを設定して下さい

ISE 配備を確認することは対応 FIP です Administration > システム > 設定 > FIP に FIP モードをつける ISE にオプションがナビゲート しますあります。

The screenshot shows the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar includes 'Home', 'Context Visibility', 'Operations', 'Policy', 'Administration', and 'Work Centers'. The left sidebar shows a navigation menu with 'Client Provisioning' selected, and sub-items for 'FIPS Mode', 'Alarm Settings', 'Posture', 'Profiling', and 'Protocols'. The main content area is titled 'FIPS Mode' and shows a dropdown menu for 'FIPS Mode' set to 'Enabled'. There are 'Save' and 'Reset' buttons below the dropdown.

このモードでは、『Protocols』を選択される少数ただここにリストされていて認証に使用することができます。

- EAP-TLS
- PEAP
- EAP-FAST
- EAP-TTLS

注: EAP-TLS L ビット プロトコルは対応 FIP でし、FIP モードで許されません。

注: EAP-FAST の匿名 PAC プロビジョニング オプションは FIP モードで許可されません。

注: 認証およびプライベートキーは FIP 対応ハッシュおよび暗号化アルゴリズムだけ使用する必要があります。プライベートキーは長さが 1024 バイトより大きいはずです。

FIP モードを有効にしている間よくある問題

問題

非 FIPS 対応プロトコルを使用する許可されたプロトコル。

エラー メッセージ：非 FIPS 対応プロトコルを使用するために「次の「許可されたプロトコル」は設定されます。FIP はこれらが「許可されたプロトコル」削除されるか、または FIP 対応プロトコルだけ使用するために」。編集されるまで有効にすることができません



The following "Allowed Protocols" are configured to use non-FIPS compliant protocols. FIPS can not be enabled until these "Allowed Protocols" are deleted or they are edited to use only FIPS compliant protocols.

解決策

edit プロトコルが不適合なプロトコルをディセーブルにするようにしました。

ポリシー > ポリシー要素へのナビゲートは >> 認証 > 許可されたプロトコル生じます。

これらのサービスは FIP 不適合なプロトコルを使用しないために削除されるか、または編集することができます。

このイメージのプロトコルの選択不可能にされたチェックボックスは対応 FIP ではないです。選択不可能にならない物だけ FIP モードで使用することができます。

Process Host Lookup ⓘ

Authentication Protocols

Allow PAP/ASCII

Allow CHAP

Allow MS-CHAPv1

Allow MS-CHAPv2

Allow EAP-MD5

Allow EAP-TLS

Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy ⓘ

Allow LEAP

Allow PEAP

Allow EAP-FAST

Allow EAP-TTLS

Preferred EAP Protocol

EAP-TLS L-bit ⓘ

Allow weak ciphers for EAP ⓘ

問題

FIP は配備に pxGrid ノードがある場合有効に することができません。

エラー メッセージ :



FIPS cannot be enabled if there are pxGrid nodes in deployment. Following node has pxGrid enabled: ise02

OK

解決策

すべてのノードのディセーブル PxGrid ペルソナ

PxGrid サービスは FIP 規格に適合ではありません。それ故に、pxGrid は配備のノードの何れかで有効にすることができません。

pxGrid サービスを、ナビゲート **Administration > システム > 配備** にディセーブルにするため。エラーで述べられるノードを選択し、そのノードのための pxGrid ペルソナをチェックを外し、イメージに示すように設定を保存して下さい。

Hostname **ise02**
FQDN **ise02.raghav.com**
IP Address **10.106.73.104**
Node Type **Identity Services Engine (ISE)**

Personas

Administration Role **STANDALONE**

Monitoring Role **PRIMARY** Other Monitoring Node

Policy Service

Enable Session Services

Enable Profiling Service

Enable SXP Service Use Interface **GigabitEthernet 0**

Enable Device Admin Service

Enable Identity Mapping

pxGrid