

ISE の FIPS モード

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[ISE の FIP モードを設定して下さい](#)

[FIP モードをイネーブル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 をイネーブル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しては個別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。

本書の情報は、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、初期 (デフォルト) 設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

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。

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service PassiveID

Deployment Licensing Certificates Logging Maintenance Upgrade Backup & Restore Admin Access Settings

Client Provisioning

FIPS Mode

FIPS Mode Enabled

Alarm Settings

Posture

Profiling

Protocols

Save Reset

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: 証明書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 モードをイネーブル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」。編集されるまでイネーブルになります



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無効に 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 ノードがある場合イネーブルになります。

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イネーブルになってい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**に無効にするため。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