Modo FIP en el ISE

Contenido

Introducción

Este documento describe los protocolos obedientes de los Estándares de procesamiento de la información federales (FIP) en el motor de Servce de la identidad (ISE) y los problemas comunes encontraron mientras que habilitaban los FIP. Los FIP son los estándares que son desarrollados por el gobierno federal de Estados Unidos para el uso en los sistemas informáticos por las agencias gubernamentales y los contactores no militares del gobierno.

Prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

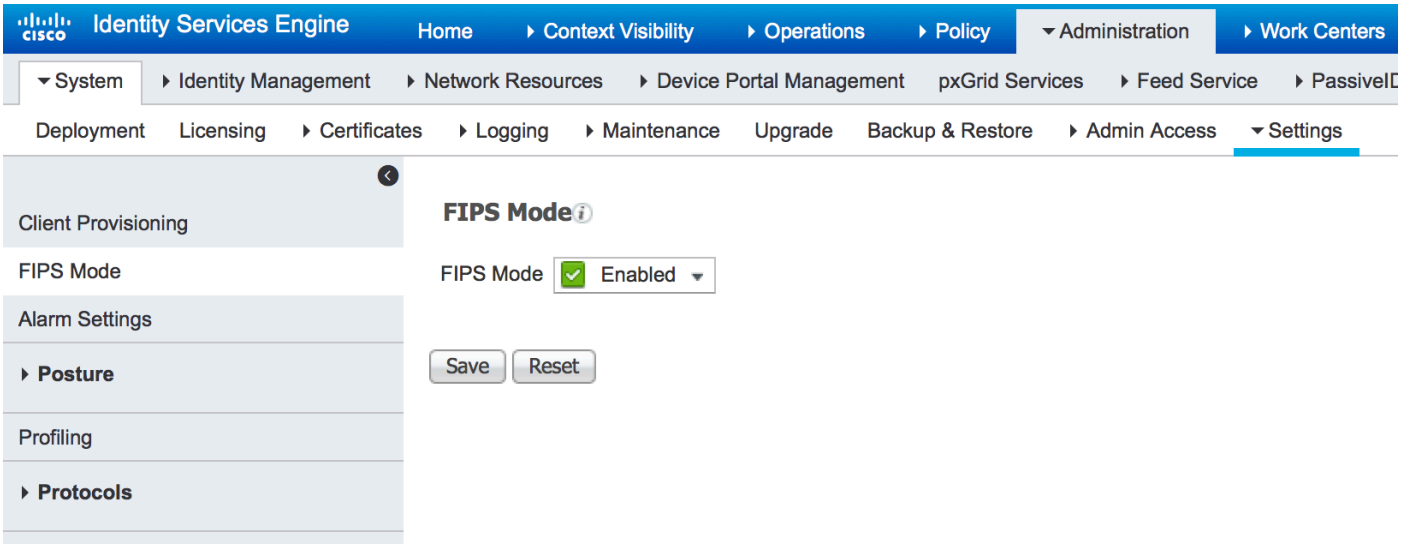
Componentes Utilizados

La información en este documento se basa en la versión del 2.1 ISE.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Configure el modo FIP en el ISE

Para asegurar el despliegue ISE es FIP obedientes, hay una opción en el ISE para girar el modo FIP, navega a la **administración > al sistema > a las configuraciones > a los FIP.**



En este modo, solamente los pocos protocolos seleccionados enumerados aquí se permiten ser utilizados para las autenticaciones.

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

Nota: El protocolo del L-bit del EAP-TLS no es FIP obedientes y no se permite en el modo FIP.

Nota: La opción anónima del aprovisionamiento PAC en el EAP-FAST no se permite en el modo FIP.

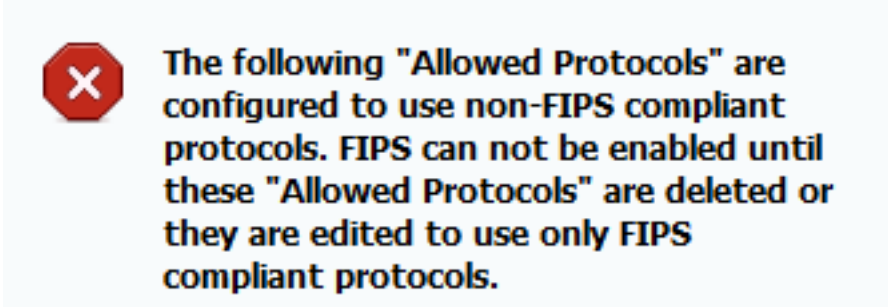
Nota: Los Certificados y las claves privadas deben utilizar solamente el hash obediente y los algoritmos de encripción FIP. Las claves privadas deben ser más grandes de 1024 bytes de largo.

Problemas comunes mientras que habilita el modo FIP

Problema

Protocolos permitidos usando los protocolos obedientes NON-FIP.

Mensaje de error: ““Los protocolos permitidos siguientes” se configuran para utilizar los protocolos obedientes NON-FIP. Los FIP no pueden ser habilitados hasta que se borren éstos los “protocolos permitidos” o se editan para utilizar solamente los protocolos obedientes FIP.”



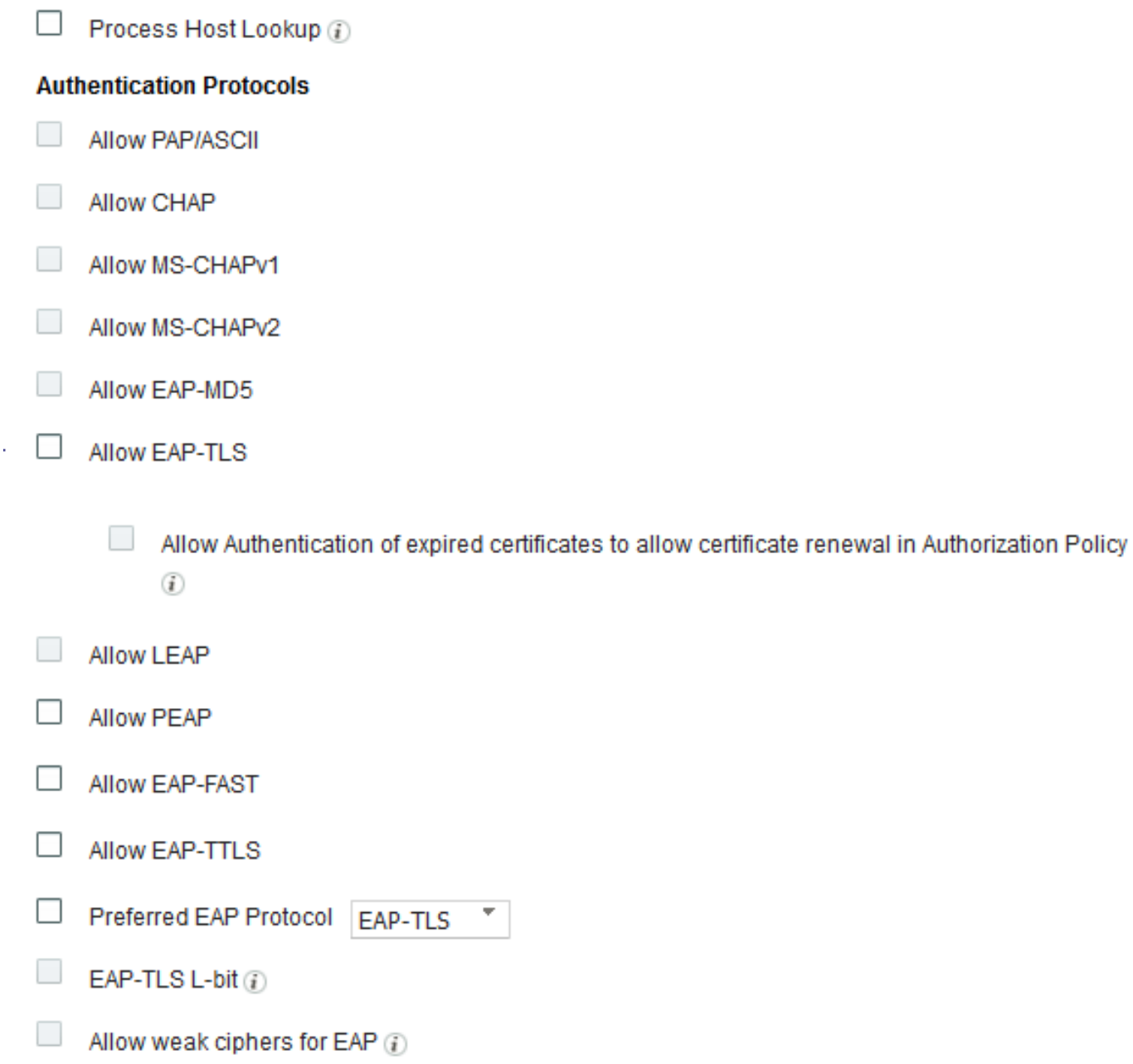
Solución

Edit permitió que los protocolos inhabilitaran los protocolos no obedientes.

Navegue a la **directiva > a los elementos > a los resultados > a la autenticación de la directiva > los protocolos permitidos.**

Estos servicios pueden ser borrados o ser editados para no utilizar los protocolos no obedientes FIP.

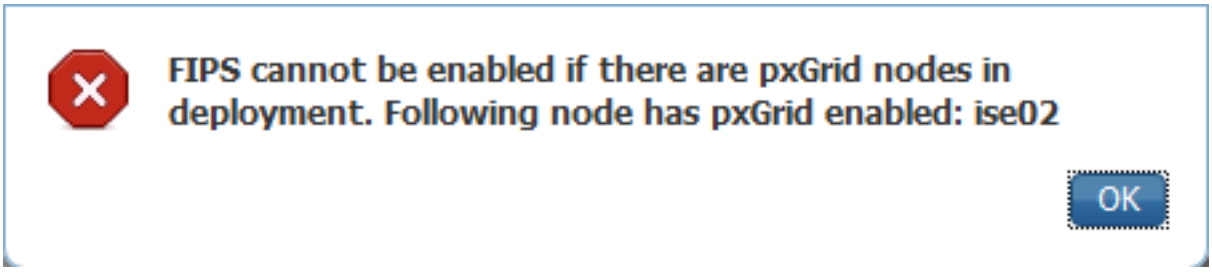
Del greyed las casillas de verificación hacia fuera de los protocolos en esta imagen no son FIP obedientes. Solamente los que no son greyed hacia fuera se pueden utilizar en el modo FIP.



Problema

Los FIP no pueden ser habilitados si hay Nodos del pxGrid en el despliegue.

Mensaje de error:



Solución

Personaje de PxGrid de la neutralización en todos los Nodos

El servicio de PxGrid no es obediente con los estándares FIP. Por lo tanto, el pxGrid no se puede habilitar en los Nodos uces de los en el despliegue.

Para inhabilitar el servicio del pxGrid, navegue a la **administración > al sistema > al despliegue.** Seleccione los Nodos mencionados en el error y desmarque el personaje del pxGrid para ese nodo y salve la configuración tal y como se muestra en de la imagen.