

Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Configurar](#)

[Troubleshooting](#)

[debug mab todo](#)

[dot1x todo del debug](#)

[debug radius](#)

[autenticación/autorización aaa del debug](#)

[Información Relacionada](#)

Introducción

Este documento describe el procedimiento para resolver problemas las autenticaciones en el Switches que utilizan los servicios de red basados en la identidad (IBNS)

Prerrequisitos

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Motor del servicio de la identidad (ISE)
- Conceptos del IEEE 802.1X (dot1x)
- Puente de la autenticación de MAC (MAB)

Componentes Utilizados

La información en este documento se basa en estas versiones de software y hardware pero no limited a:

- Switch Cisco - C3750X-48PF-S con IOS 15.2.1E3(ED)
- 2.1 del motor del servicio de la identidad

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.

Antecedentes

IBNS 2.0 es un nuevo motor de directivas que substituye al auténtico-administrador tradicional. Se

equipa de un conjunto de las capacidades mejoradas que ofrecen la configuración flexible con el lenguaje de la directiva de la clasificación típica de Cisco (C3PL). Ahora llamo al administrador de sesión del acceso, IBNS 2.0 da a administradores las opciones para configurar las directivas y las acciones basadas en las condiciones y los eventos específicos del punto final. En vez de las condiciones regulares, C3PL se utiliza para definir las condiciones de la autenticación, los parámetros y las acciones. Para más información sobre IBNS 2.0, siga el link dado en la sección de información relacionada.

Hay diversos tipos de correspondencias de políticas que se utilicen para los diversos propósitos. Este párrafo se centra en el tipo del suscriptor. Hay tres secciones en una correspondencia de políticas que se observará.

- Sección del evento
- Sección de la clase
- Sección de la acción

Siguen el **evento > la clase > la acción de la** jerarquía. Cuando una correspondencia de políticas se aplica a una interfaz, todos los eventos definidos en la correspondencia de políticas se evalúan. Basado sobre el evento actual, la acción apropiada definida en la correspondencia de políticas es aplicada en el nivel de la interfaz.

Una vez que el evento se corresponde con, hay una opción para evaluar las clases basadas en el evento/el método/el resultado de la autenticación/de la autorización. Los resultados de estas clases pueden ser **EJECUTAN** o llaman **SIEMPRE** en las correspondencias adicionales de la clase.

En la sección de la acción, las acciones importantes que pueden ser incluidas son:

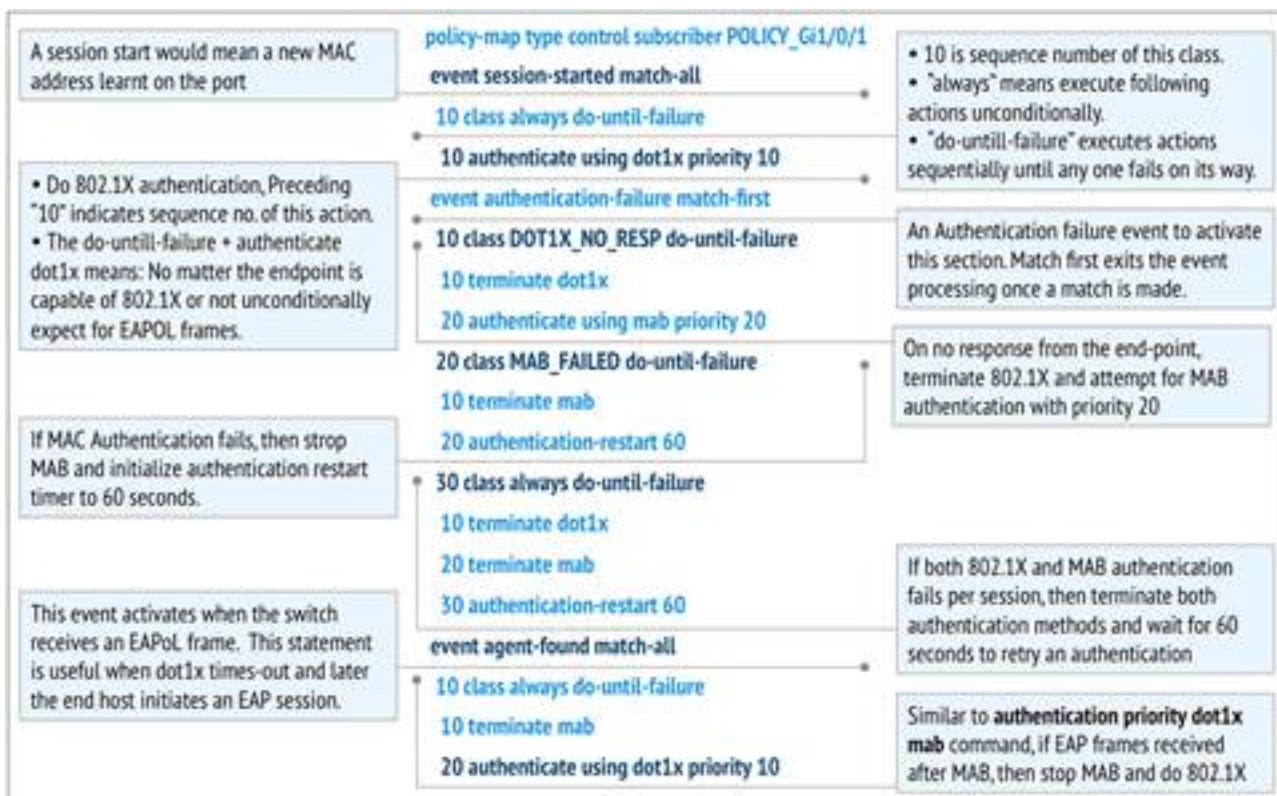
- Especifique un método de autenticación con una prioridad
- Especifique una lista del método de autenticación para un método de autenticación determinado
- Especifique una lista del método de autorización para un método de autenticación
- Especifique el número de recomprobaciones
- Substituya los datos existentes del authentication/de la autorización por los nuevos datos de la autenticación/de la autorización
- Fuerce la autorización
- Fuerce Unauthorization
- Active una plantilla del servicio

En el Switches tradicional IOS, no había opción para aplicar un específico de la lista de métodos a una sesión autenticada. IBNS 2.0 proporciona esta capacidad usando las servicio-plantillas. La plantilla del servicio se configura localmente en el Switch y la autorización aplicada de la sesión exitosa del poste. Hay también una opción para avanzar la plantilla del servicio solicitado de un servidor de AAA.

El atributo de RADIUS que se utiliza para hacer lo mismo es *suscriptor: servicio-nombre = <name del template> del servicio*. En el motor del servicio de la identidad (ISE), usted puede nombrar el perfil de la autorización exactamente lo mismo a partir de la servicio-plantilla local configurada en el Switch y marcar la casilla de verificación de la *plantilla del servicio*. Este perfil de la autorización junto con cualquier otro perfil de la autorización se puede avanzar como resultado de la autorización.

En el informe del resultado de la autorización, hay un Cisco-av-pair nombrado *suscriptor: servicio-nombre = <name del template> del servicio*. Este indicates que el swich se ha notificado para aplicar esa plantilla del servicio para esa sesión.

Aquí está una imagen que muestra el significado exacto de cada entidad de una correspondencia de políticas de la muestra.



Configurar

Configuración AAA

Configuración de servidor de RADIUS

Configuración de correspondencia de políticas

La clase asocia la configuración

Configuración de la interfaz

Troubleshooting

La mejor manera de resolver problemas es comparar los registros de trabajo y los registros

festivos. Se sabe esta manera, el paso exacto en el cual el proceso salió mal. Hay algunos debugs que son necesarios ser habilitados para resolver problemas los problemas mab/dot1x. Aquí están los comandos de habilitar esos debugs.

- debug aaa authentication
- **debug aaa authorization**
- debug mab todo
- dot1x todo del debug
- debug radius

Aquí están los registros de trabajo con el dot1x y el mab habilitados al mismo tiempo.

debug mab todo

dot1x todo del debug

Puesto que el dot1x tiene muchos intercambios del mensaje debido a las negociaciones del protocolo, los intercambios del certificado y así sucesivamente, no todas las los registros del debug se han mencionado aquí. El flujo de eventos en la orden en la cual se suponen para ocurrir y sus registros correspondientes del debug se han documentado aquí.

debug radius

Puesto que hay porción de mensajes EAP, los paquetes RADIUS enviaron al servidor y recibido también sea más. No cada autenticación del dot1x acaba apagado con en el pedido de acceso. Por lo tanto los registros mostrados aquí son los que son importantes y pues va el flujo.

autenticación/autorización aaa del debug

haga el debug de la autenticación aaa y la información útil de las demostraciones del debug aaa authorization durante la diversos autenticación/métodos de autorización. En este caso, es solamente una sola línea que especifica la lista de métodos que es utilizada.

Esto muestra si los métodos de autenticación uces de los son inasequibles/no habilitados.

El procedimiento para resolver problemas CWA/Posture/DACLs etc., es lo mismo que el del Switches tradicional IOS. La verificación de la configuración es el primer paso en el troubleshooting. Asegúrese que la configuración cumpla los requisitos. Si la configuración de la correspondencia de políticas, correspondencia de la clase está hasta la marca, después los problemas del debug si ningunos, pueden ser muy fáciles. Para otros detalles en la configuración usando IBNS 2.0, refiera la sección de información relacionada.

Información Relacionada

- [Guía de despliegue IBNS 2.0](#)