El ISE con los parásitos atmosféricos reorienta para el ejemplo de configuración aislado de las redes del invitado

Contenido

Introducción

Este documento describe cómo configurar el Cisco Identity Services Engine (ISE) con los parásitos atmosféricos reorienta para las redes del invitado aisladas para mantener la Redundancia. También describe cómo configurar el nodo de la directiva para no indicar los clientes con una advertencia inverificable del certificado.

Prerequisites

Requisitos

Cisco recomienda que tenga conocimiento sobre estos temas:

- Autenticación Web central de Cisco ISE (CWA) y todos los componentes relacionados
- Verificación del navegador de la validez del certificado
- Versión 1.2.0.899 o posterior de Cisco ISE
- Versión 7.2.110.0 del controlador LAN de la tecnología inalámbrica de Cisco (WLC) o más adelante (la versión se prefiere 7.4.100.0 o más adelante)

Note: CWA se describe en la [autenticación Web central en](#) artículo de Cisco del [ejemplo de configuración del WLC y ISE](#).

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 1.2.0.899 de Cisco ISE
- Versión 7.4.110.0 virtual del WLC de Cisco (vWLC)
- Versión 8.2.5 adaptante del dispositivo de seguridad de Cisco (ASA)

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

En muchos entornos de Bring Your Own Device (BYOD), la red del invitado se aísla completamente de la red interna en un De-Militarized Zone (DMZ). A menudo, el DHCP en el invitado DMZ ofrece los servidores del sistema del nombre del public domain (DNS) a los Usuarios invitados porque el único servicio se ofrece que es acceso a internet.

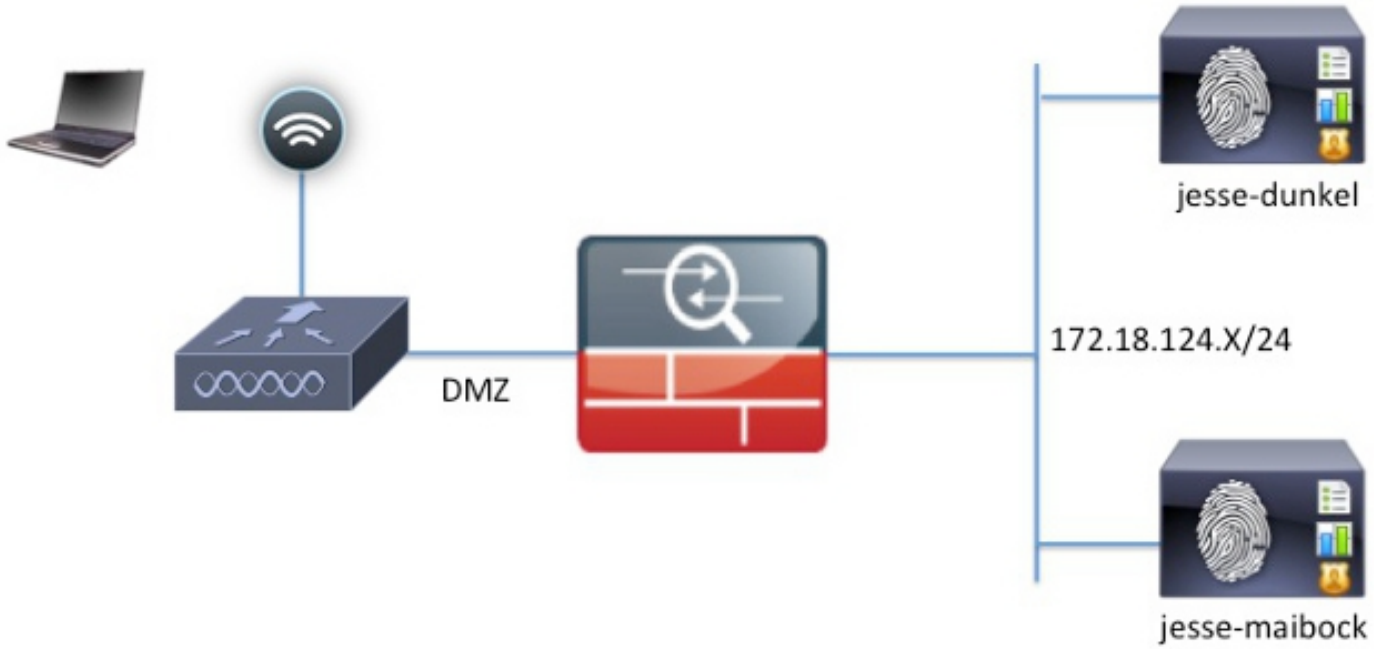
Esto hace el cambio de dirección del invitado en el ISE difícil antes de la versión 1.2 porque el ISE reorienta a los clientes al nombre de dominio completo (FQDN) para la autenticación Web. Sin embargo, con las versiones 1.2 ISE y posterior, los administradores pueden reorientar a los Usuarios invitados a un IP Address estático o a un nombre de host.

Configurar

Diagrama de la red

Esto es un diagrama lógico.

> **Note**: Físicamente, hay regulador inalámbrico en la red interna, el (APS) de los Puntos de acceso está en la red interna, y la identificación de conjunto de servicio (SSID) se asegura al regulador DMZ. Refiera a la documentación para el WLCs de Cisco para más información.



Configuración

Sigue habiendo la configuración en el WLC sin cambiar de una configuración normal CWA. El SSID se configura para permitir el MAC que filtra con la autenticación de RADIUS, y las puntas que consideran RADIUS hacia dos o más Nodos de la directiva ISE.

Este documento se centra en la configuración ISE.

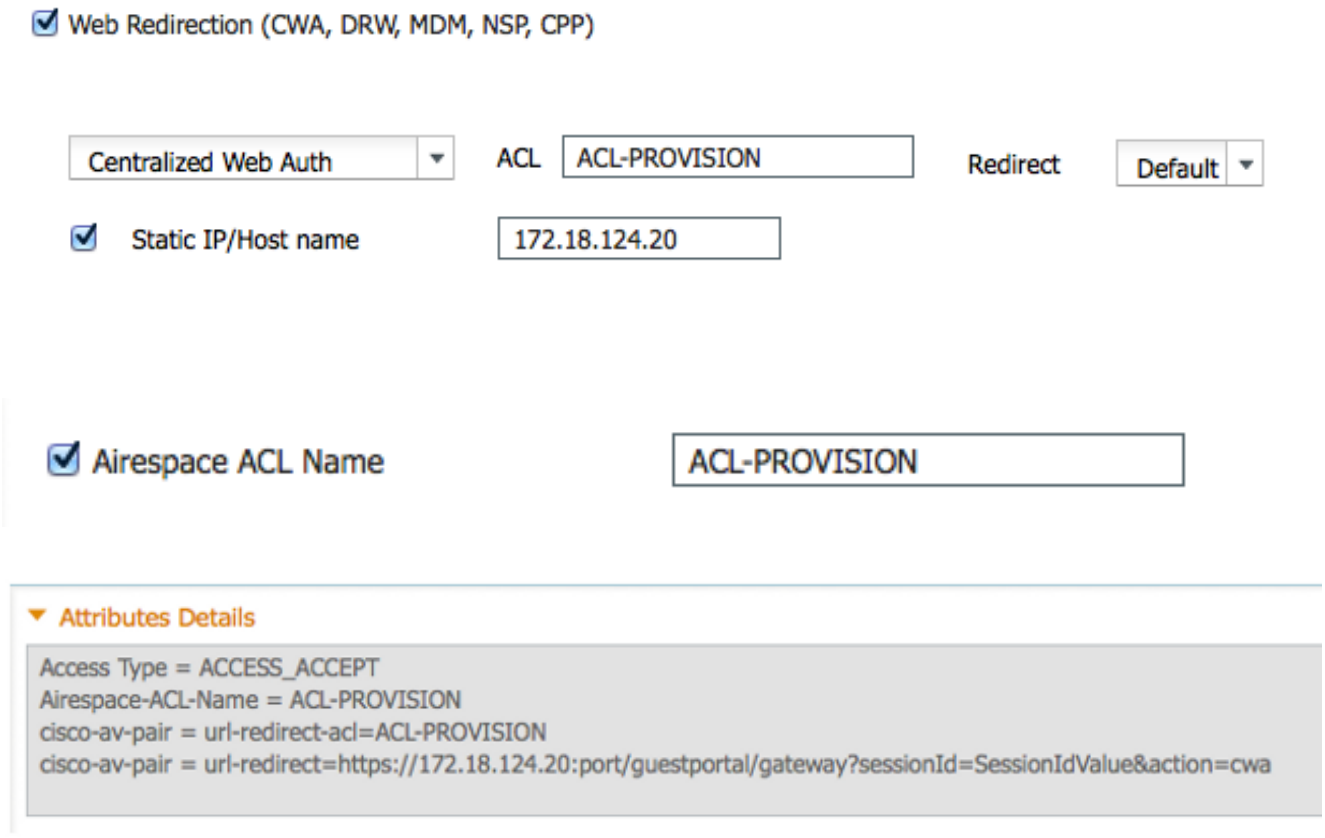
> **Note**: En este ejemplo de configuración, los Nodos de la directiva son **jesse-dunkel** (172.18.124.20) y el **jesse-maibock** (172.18.124.21).

Los CWA fluyen comienzan cuando el WLC envía una petición de puente de la autenticación de MAC RADIUS (MAB) al ISE. El ISE contesta con una reorientación URL al regulador para reorientar el tráfico HTTP al ISE. Es importante que el RADIUS y el tráfico HTTP van al mismo nodo de los servicios de la directiva (PSN) porque la sesión se mantiene en un solo PSN. Esto se realiza normalmente con una sola regla, y el PSN inserta su propio nombre de host en el CWA URL. Sin embargo, con los parásitos atmosféricos reoriente, usted debe crear una regla para cada PSN para asegurarse de que el RADIUS y el tráfico HTTP están enviados al mismo PSN.

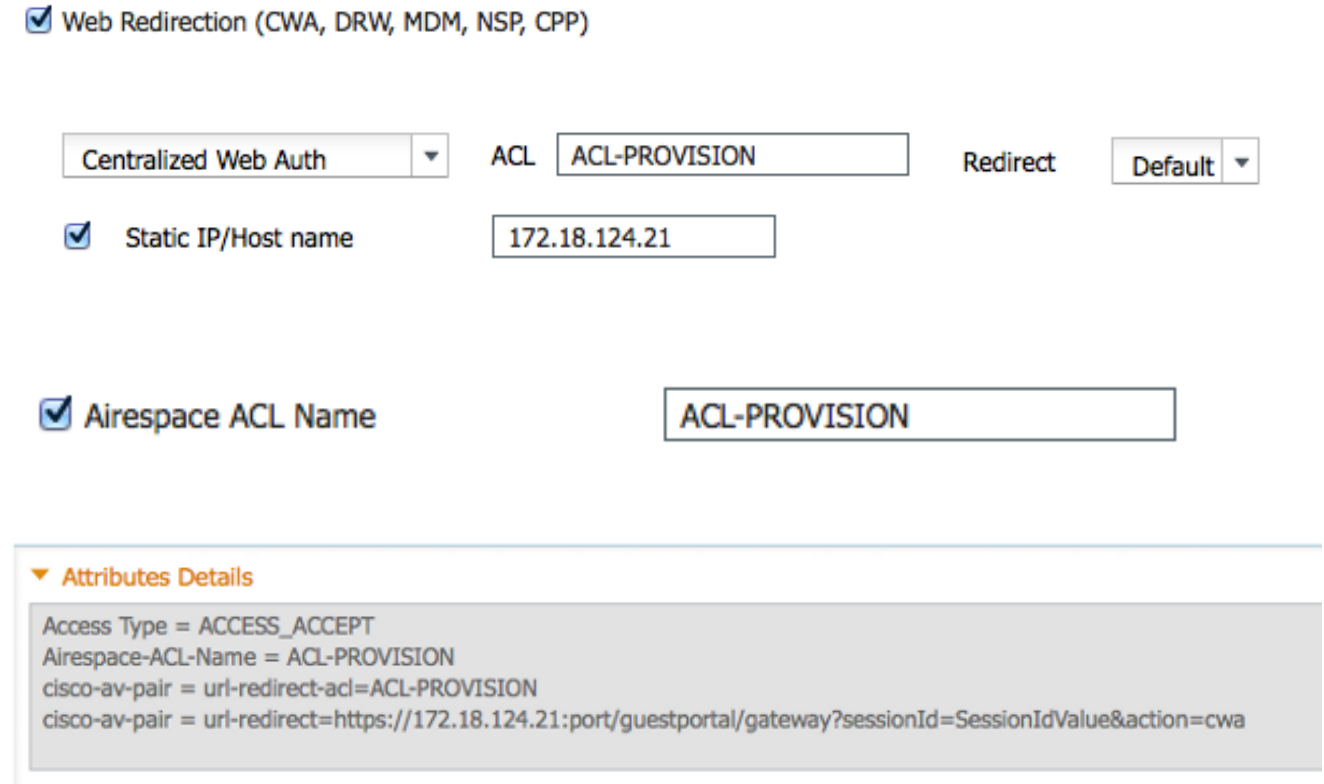
Complete estos pasos para configurar el ISE:

1. Configure dos reglas para reorientar al cliente a la dirección IP PSN. Navegue a la **directiva > a los elementos de la directiva > a los resultados > a la autorización > a los perfiles de la autorización**.

   Estas imágenes muestran la información para el nombre del perfil **DunkelGuestWireless**:



Estas imágenes muestran la información para el nombre del perfil **MaibockGuestWireless**:



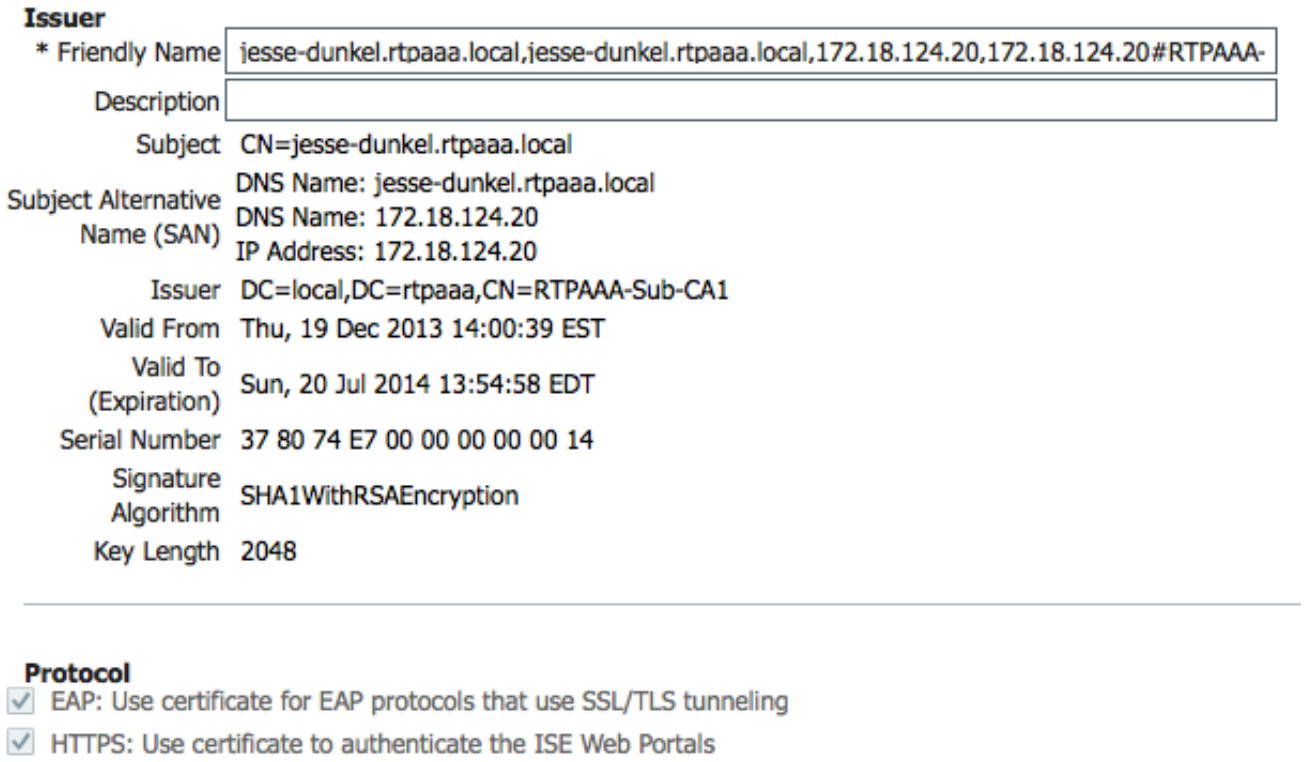
Note: **El ACL-PROVISION** es una lista de control de acceso (ACL) local que se configura en el WLC para permitir que el cliente comunique con el ISE sobre la autenticación. Refiera a la autenticación Web central en artículo de Cisco del ejemplo de configuración del WLC y ISE para más información.

2. Configure la autorización limpia de modo que hagan juego en el **acceso a la red:** El atributo

de **nombre del host ISE** y proporciona el perfil apropiado de la autorización:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	GuestAccess	if Network Access:UseCase EQUALS Guest Flow	then GuestPermit
✓	DunkelGuestWireless	if Network Access:ISE Host Name EQUALS jesse-dunkel	then DunkelGuestWireless
✓	MaibockGuestWireless	if Network Access:ISE Host Name EQUALS jesse-maibock	then MaibockGuestWireless
✓	Default	if no matches, then DenyAccess	

Ahora que reorientan al cliente a una dirección IP, los usuarios reciben las advertencias del certificado porque el URL no hace juego la información en el certificado. Por ejemplo, el FQDN en el certificado es **jesse-dunkel.rtpaaa.local, pero el URL es 172.18.124.20**. Hereis un certificado del **ejemplo** que permite que el navegador valide el certificado con la dirección IP:



Con el uso de las entradas alternativas sujetas del nombre (SAN), el navegador puede validar el URL que incluye a la dirección IP 172.18.124.20. Tres entradas SAN se deben crear para dirigir las diversas incompatibilidades del cliente.

3. Cree una entrada SAN para el nombre DNS y asegúrese de que hace juego la entrada **CN= del** campo Subject.

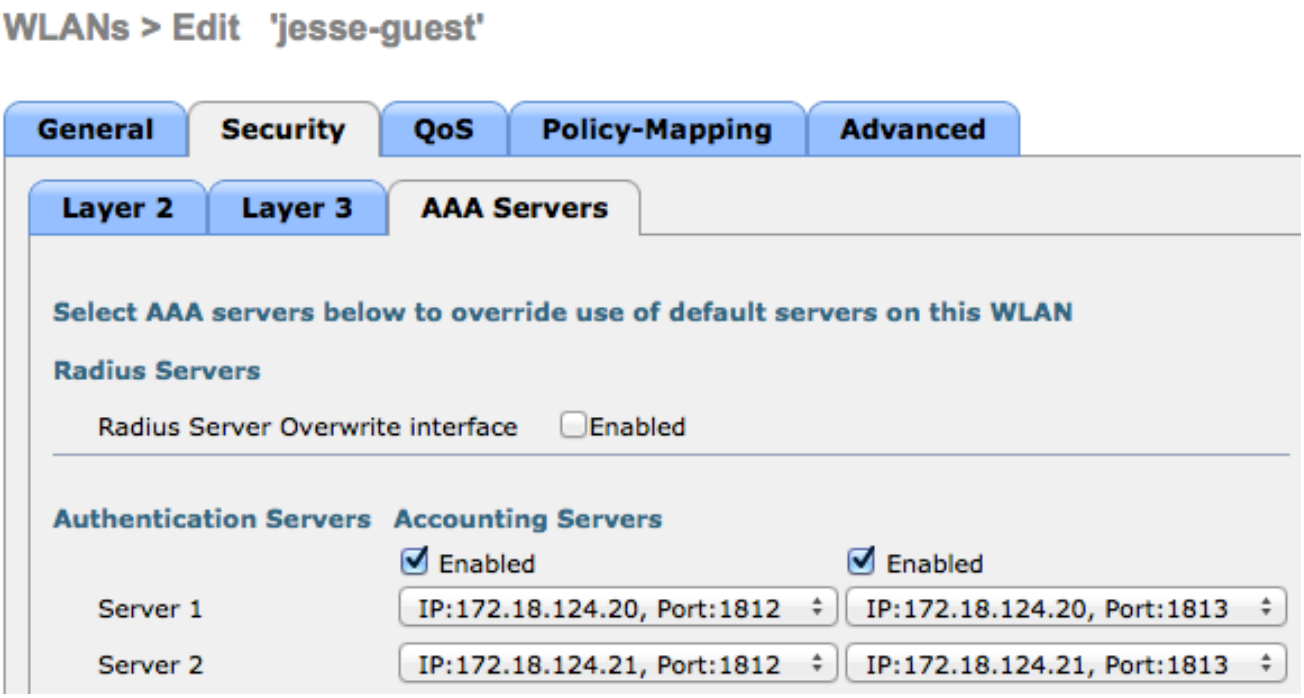
4. Cree dos entradas para permitir que los clientes validen la dirección IP; éstos están para el nombre DNS de la dirección IP así como la dirección IP que aparece en el atributo de la dirección IP. Algunos clientes refieren solamente al nombre DNS. Otros no validan una dirección IP en el atributo de nombre DNS sino que por el contrario se refieren al atributo de la dirección IP.

Note: Para más información sobre la generación del certificado, refiera al **guía de instalación del hardware del Cisco Identity Services Engine, la versión 1.2**.

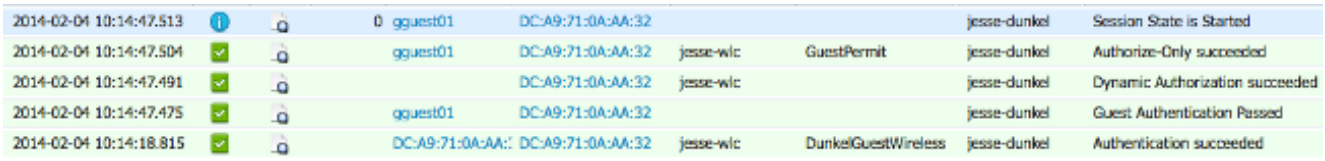
Verificación

Complete estos pasos para confirmar que su configuración trabaja correctamente:

1. Para verificar que ambas reglas sean funcionales, fije manualmente la orden del ISE PSN que se configura en la red inalámbrica (WLAN):



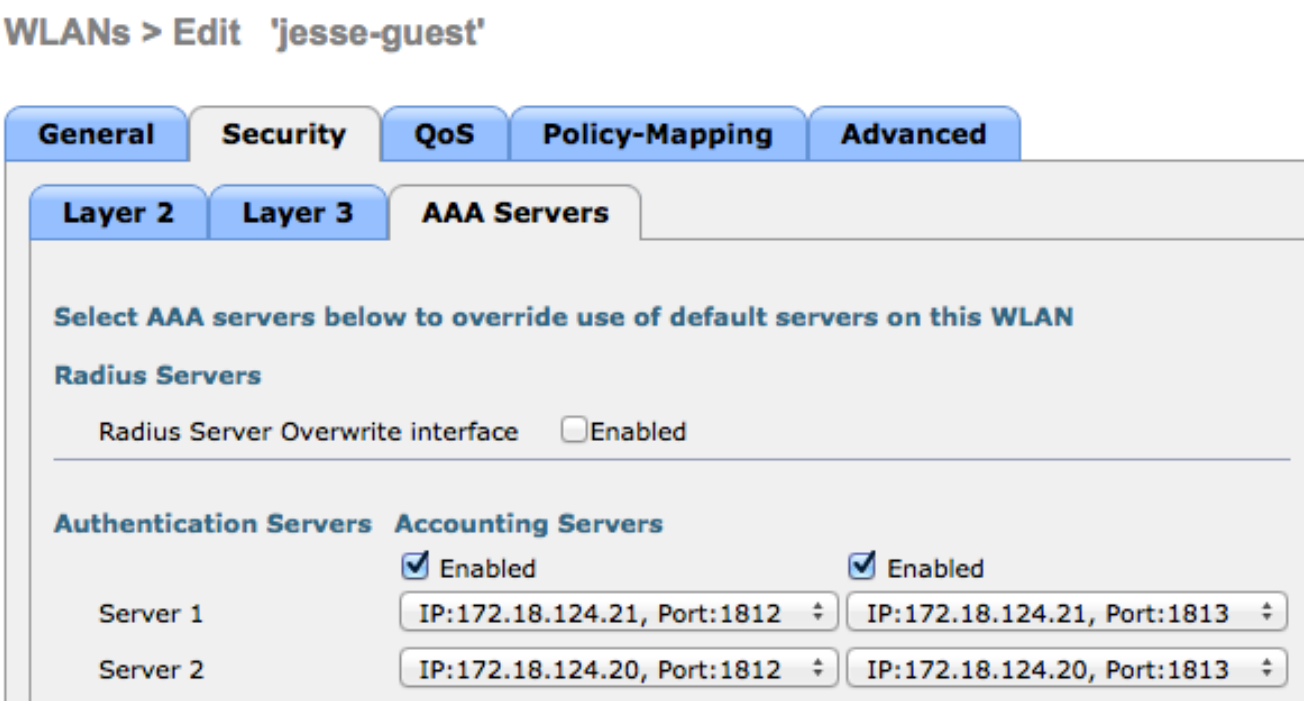
2. El registro en el invitado SSID, navega a la **operación > a las autenticaciones** en el ISE, y verifica que las reglas correctas de la autorización están golpeadas:



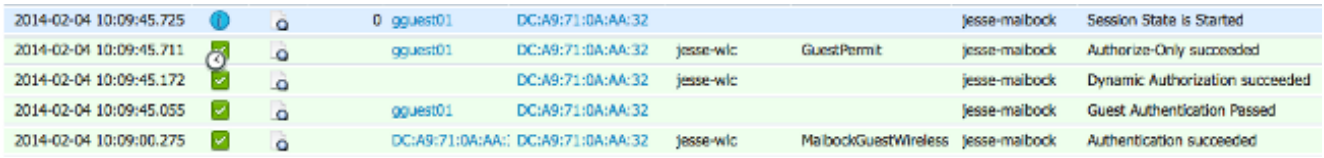
La autenticación inicial MAB se da al perfil de la autorización de **DunkelGuestWireless**. Ésta es la regla que reorienta específicamente al **jesse-dunkel**, que es el primer nodo ISE. Después de que el usuario **gguest01** abra una sesión, el permiso final correcto de **GuestPermit** se da.

3. Para borrar las sesiones de la autenticación del WLC, desconecte el dispositivo del cliente de la red inalámbrica, navegue **para monitorear > los clientes** en el WLC, y borre la sesión de la salida. El WLC lleva a cabo a la sesión inactiva por cinco minutos por abandono, así que para realizar una prueba válida, usted debe comenzar de nuevo.

4. Invierta la orden del ISE PSN bajo configuración de la red inalámbrica (WLAN) del invitado:



5. El registro en el invitado SSID, navega a la **operación > a las autenticaciones** en el ISE, y verifica que las reglas correctas de la autorización están golpeadas:



Para la segunda tentativa, el perfil de la autorización de **MaibockGuestWireless** se golpea correctamente para la autenticación inicial MAB. Similar a la primera tentativa al **jesse-dunkel** (el paso 2), la autenticación al **jesse-maibock** golpea correctamente el **GuestPermit** para la autorización final. Porque no hay información PSN-específica en el perfil de la autorización de **GuestPermit**, una sola regla se puede utilizar para la autenticación a cualquier PSN.

Troubleshooting

La ventana de los detalles de la autenticación es una visión potente que visualiza cada paso de la autenticación/del proceso de la autorización. Para accederla, navegue a las **operaciones > a las autenticaciones** y haga clic el icono de la lupa bajo la columna de los detalles. Utilice esta ventana para verificar que las condiciones de la regla de la autenticación/de la autorización están configuradas correctamente.

En este caso, el campo del servidor de políticas es el área primaria del foco. Este campo contiene el nombre de host del ISE PSN por el cual la autenticación es mantenida:

Overview

Event	5200 Authentication succeeded
Username	DC:A9:71:0A:AA:32
Endpoint Id	DC:A9:71:0A:AA:32
Endpoint Profile	
Authorization Profile	DunkelGuestWireless
AuthorizationPolicyMatchedRule	DunkelGuestWireless
ISEPolicySetName	GuestWireless
IdentitySelectionMatchedRule	Default

Authentication Details

Source Timestamp	2014-02-04 10:14:18.79
Received Timestamp	2014-02-04 10:14:18.815
Policy Server	jesse-dunkel
Event	5200 Authentication succeeded

Compare la entrada del servidor de políticas a la condición de la regla y asegúrese de que la coincidencia dos (este valor es con diferenciación entre mayúsculas y minúsculas):

DunkelGuestWireless	if	Network Access:ISE Host Name EQUALS jesse-dunkel

Note: Es importante recordar que usted debe desconectar del SSID y borrar la entrada del cliente del WLC entre las pruebas.