O ISE com estática reorienta para o exemplo de configuração isolado das redes de convidado

Índice

Introdução

Este documento descreve como configurar o Cisco Identity Services Engine (ISE) com estática reorienta para redes de convidado isoladas a fim manter a Redundância. Igualmente descreve como configurar o nó da política de modo que os clientes não sejam alertados com um aviso não verificável do certificado.

Pré-requisitos

Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Autenticação da Web central de Cisco ISE (CWA) e todos os componentes relacionados
- Verificação do navegador da validade de certificado
- Versão 1.2.0.899 ou mais recente de Cisco ISE
- Versão 7.2.110.0 do controlador de LAN do Cisco Wireless (WLC) ou mais tarde (a versão é preferida 7.4.100.0 ou mais tarde)

  Nota: CWA é descrito na autenticação da Web central artigo de Cisco no exemplo de configuração WLC e ISE.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Versão 1.2.0.899 de Cisco ISE
- Versão 7.4.110.0 virtual de Cisco WLC (vWLC)
- Versão 8.2.5 adaptável da ferramenta de segurança de Cisco (ASA)

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Informações de Apoio

Em muitos ambientes de Bring Your Own Device (BYOD), a rede de convidado é isolada inteiramente da rede interna em um De-Militarized Zone (DMZ). Frequentemente, o DHCP no convidado DMZ oferece server do sistema do nome do public domain (DNS) aos usuários convidado porque o único serviço que é oferecido é acesso à internet.

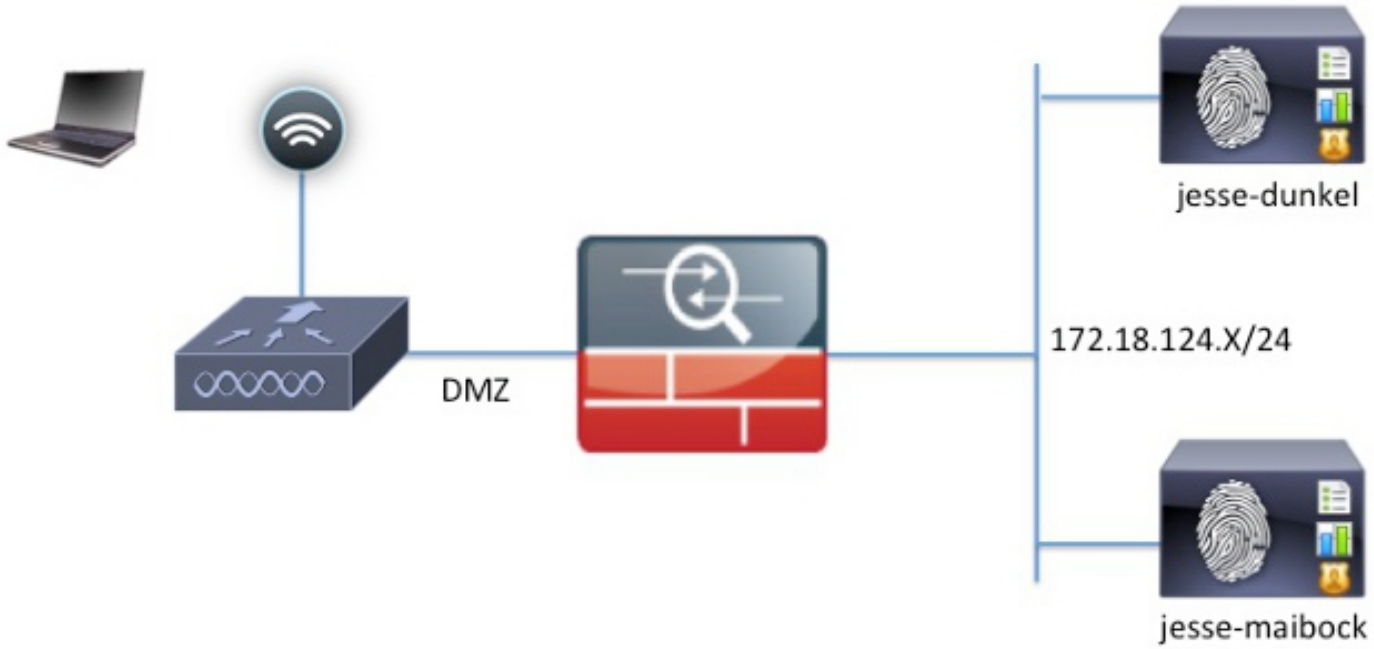
Isto faz a reorientação do convidado no ISE difícil antes da versão 1.2 porque o ISE reorienta clientes ao nome de domínio totalmente qualificado (FQDN) para a autenticação da Web. Contudo, com versões 1.2 e mais recente ISE, os administradores podem reorientar usuários convidado a um endereço IP estático ou a um hostname.

Configurar

Diagrama de Rede

Este é um diagrama lógico.

> Nota: Fisicamente, há um controlador wireless na rede interna, os Access point (AP) estão na rede interna, e na identificação de conjunto de serviço (SSID) são ancorados ao controlador DMZ. Refira a documentação para Cisco WLC para mais informação.



Configuração

A configuração no WLC permanece inalterada de uma configuração normal CWA. O SSID é configurado a fim permitir o MAC que filtra com autenticação RADIUS, e os pontos explicando do RAIO para dois ou mais Nós da política ISE.

Este documento centra-se sobre a configuração ISE.

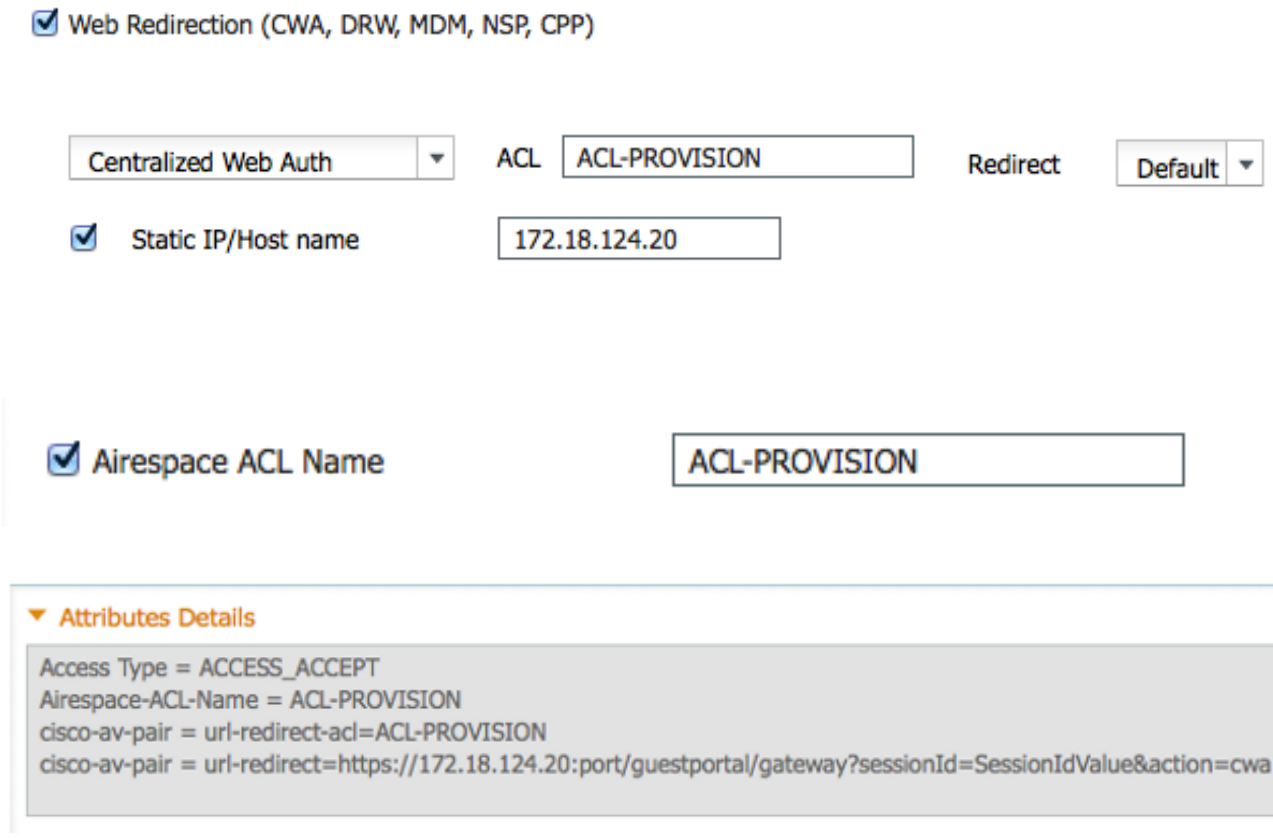
> Nota: Neste exemplo de configuração, os Nós da política são **jesse-dunkel** (172.18.124.20) e **jesse-maibock** (172.18.124.21).

Os CWA fluem começam quando o WLC envia um pedido do desvio da autenticação de MAC do RAIO (MAB) ao ISE. O ISE responde com uma reorientação URL ao controlador a fim reorientar o tráfego de HTTP ao ISE. É importante que o RAIO e o tráfego de HTTP vão ao mesmo nó dos serviços da política (PSN) porque a sessão é mantida em um único PSN. Isto é executado normalmente com uma única regra, e o PSN introduz seu próprio hostname no CWA URL. Contudo, com uma estática reoriente, você deve criar uma regra para cada PSN a fim assegurar-se de que o RAIO e o tráfego de HTTP estejam enviados ao mesmo PSN.

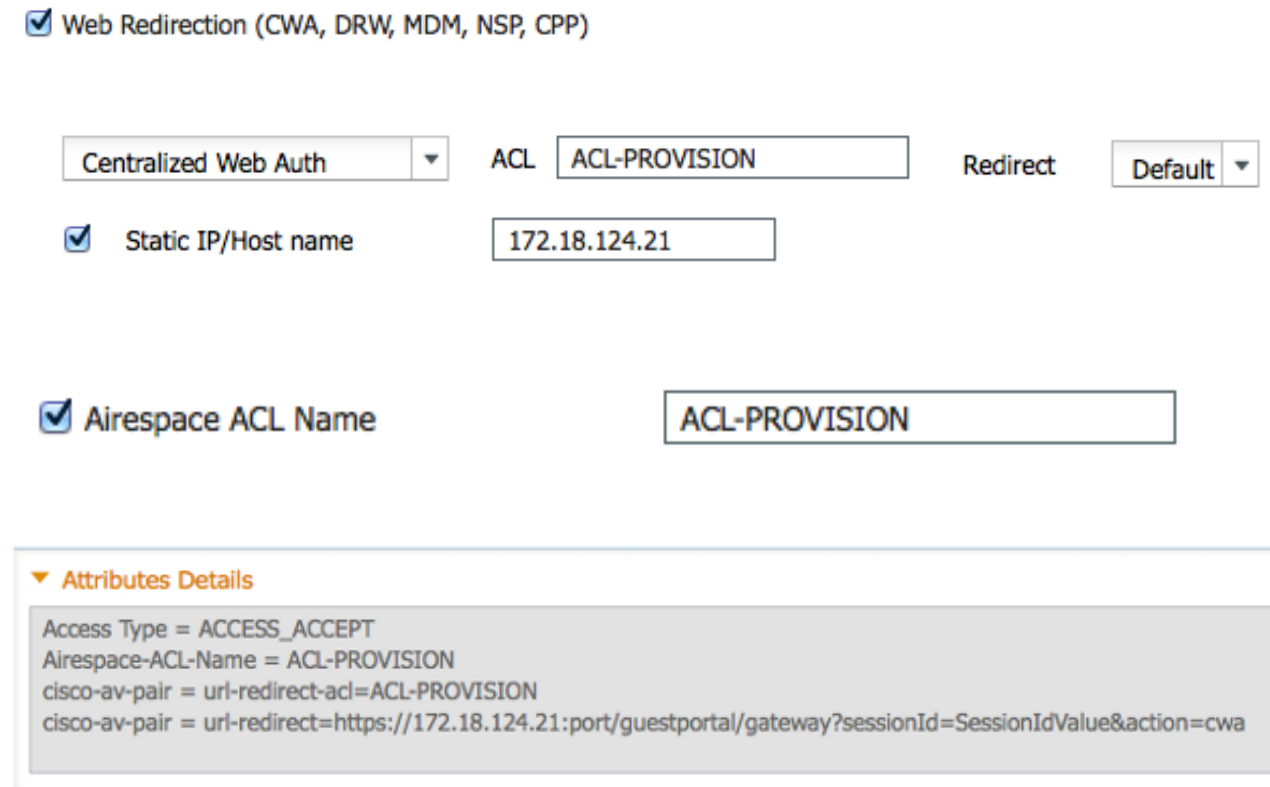
Termine estas etapas a fim configurar o ISE:

1. Estabelecer duas regras a fim reorientar o cliente ao endereço IP de Um ou Mais Servidores Cisco ICM NT PSN. Navegue à **política > aos elementos da política > aos resultados > à autorização > aos perfis da autorização**.

   Estas imagens mostram a informação para o nome de perfil **DunkelGuestWireless**:



Estas imagens mostram a informação para o nome de perfil **MaibockGuestWireless**:



Nota: **O ACL-PROVISION** é um Access Control List local (ACL) que é configurado no WLC a fim permitir que o cliente se comunique com o ISE em cima da autenticação. Refira a autenticação da Web central artigo de Cisco no exemplo de configuração WLC e ISE para mais informação.

2. Configurar a autorização policia de modo que combinem no **acesso de rede:** O atributo de

nome de host ISE e fornece o perfil apropriado da autorização:

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	

Agora que o cliente é reorientado a um endereço IP de Um ou Mais Servidores Cisco ICM NT, os usuários recebem avisos do certificado porque a URL não combina a informação no certificado. Por exemplo, o FQDN no certificado é **jesse-dunkel.rtpaaa.local, mas a URL é 172.18.124.20**. Hereis um certificado do **exemplo** que permita que o navegador valide o certificado com o endereço IP de Um ou Mais Servidores Cisco ICM NT:

Issuer

* Friendly Name	jesse-dunkel.rtpaaa.local,jesse-dunkel.rtpaaa.local,172.18.124.20,172.18.124.20#RTPAAA-
Description	
Subject	CN=jesse-dunkel.rtpaaa.local
Subject Alternative Name (SAN)	DNS Name: jesse-dunkel.rtpaaa.local DNS Name: 172.18.124.20 IP Address: 172.18.124.20
Issuer	DC=local,DC=rtpaaa,CN=RTPAAA-Sub-CA1
Valid From	Thu, 19 Dec 2013 14:00:39 EST
Valid To (Expiration)	Sun, 20 Jul 2014 13:54:58 EDT
Serial Number	37 80 74 E7 00 00 00 00 00 14
Signature Algorithm	SHA1WithRSAEncryption
Key Length	2048

Protocol

- ✓ EAP: Use certificate for EAP protocols that use SSL/TLS tunneling
- ✓ HTTPS: Use certificate to authenticate the ISE Web Portals

Com o uso de entradas alternativas sujeitas do nome (SAN), o navegador pode validar a URL que inclui o endereço IP 172.18.124.20. Três entradas SAN devem ser criadas a fim endereçar as várias incompatibilidades do cliente.

3. Crie uma entrada SAN para o nome de DNS e assegure-se de que combine a entrada **CN= do** campo de assunto.

4. Crie duas entradas a fim permitir que os clientes validem o endereço IP de Um ou Mais Servidores Cisco ICM NT; estes são para o nome de DNS do endereço IP de Um ou Mais Servidores Cisco ICM NT assim como o endereço IP de Um ou Mais Servidores Cisco ICM NT que aparece no atributo do endereço IP de Um ou Mais Servidores Cisco ICM NT. Alguns clientes referem somente o nome de DNS. Outro não aceitam um endereço IP de

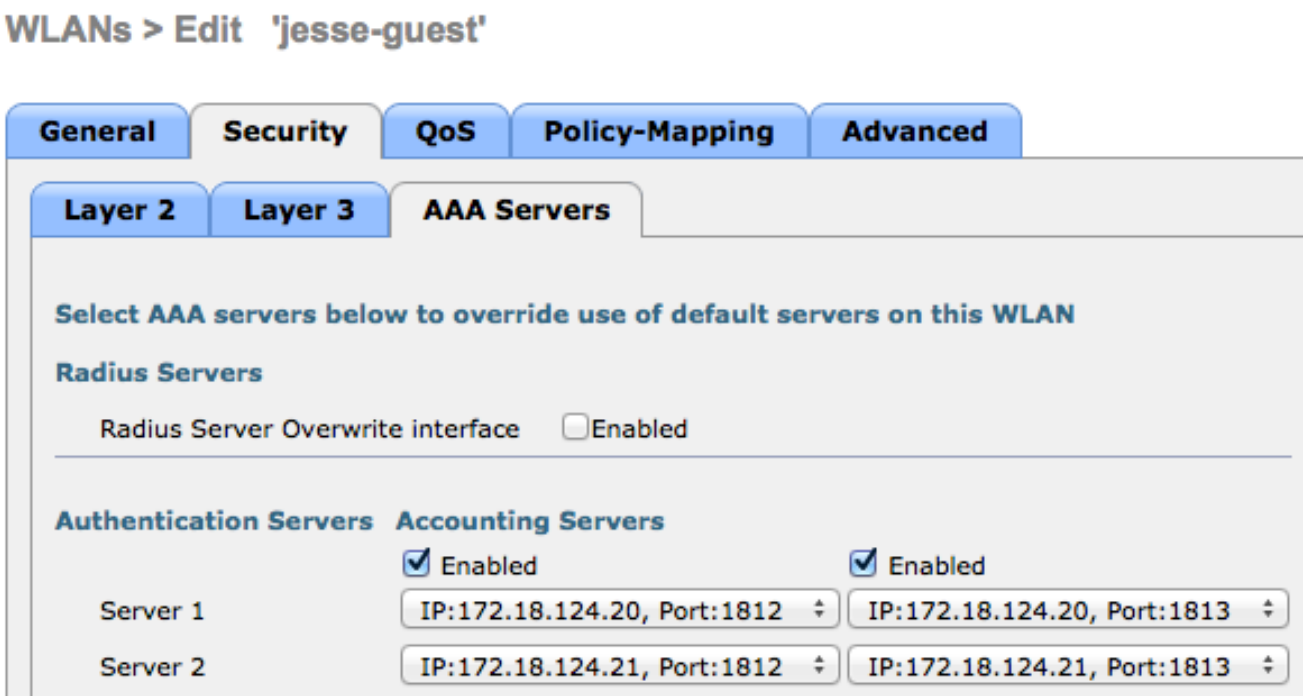
Um ou Mais Servidores Cisco ICM NT no atributo de nome de DNS mas proveem pelo contrário o atributo do endereço IP de Um ou Mais Servidores Cisco ICM NT.

Nota: Para obter mais informações sobre da geração do certificado, refira o **guia de instalação de hardware do Cisco Identity Services Engine, a liberação 1.2**.

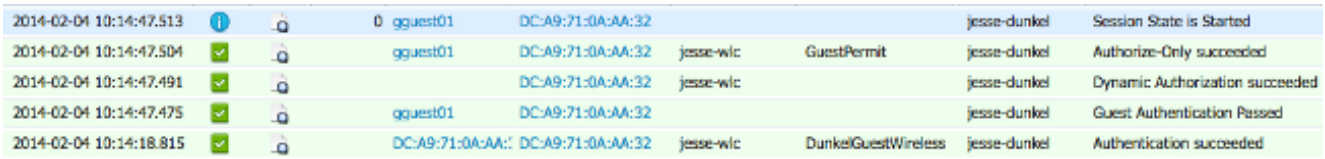
Verificar

Termine estas etapas a fim confirmar que sua configuração trabalha corretamente:

1. A fim verificar que ambas as regras são funcionais, ajuste manualmente a ordem do ISE PSN que é configurado no WLAN:



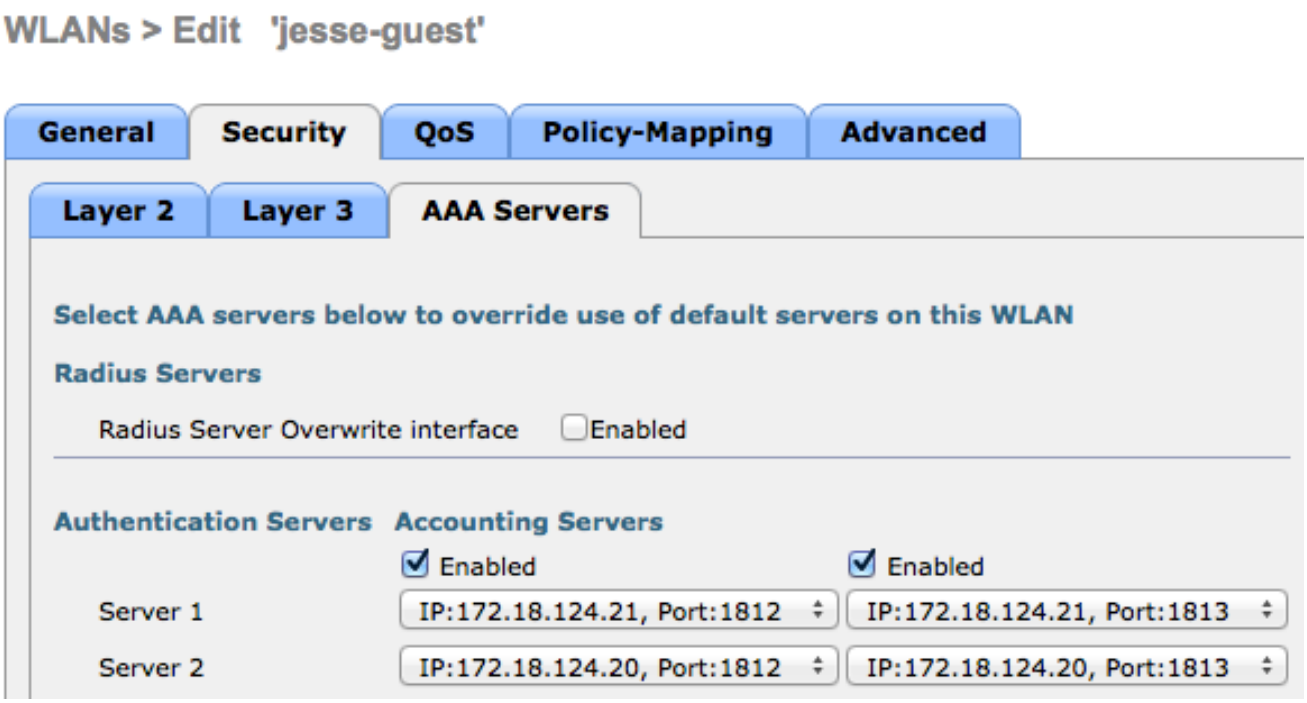
2. O log no convidado SSID, navega à **operação > às autenticações no** ISE, e verifica que as regras corretas da autorização estão batidas:



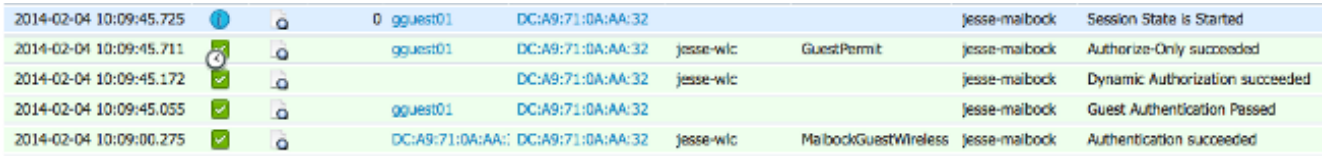
A autenticação inicial MAB é dada ao perfil da autorização de **DunkelGuestWireless**. Esta é a regra que reorienta especificamente ao **jesse-dunkel**, que é o primeiro nó ISE. Depois que o usuário **gguest01** entra, a permissão final correta de **GuestPermit** está dada.

3. A fim cancelar as sessões da autenticação do WLC, desligue o dispositivo do cliente da rede Wireless, navegue **para monitorar > clientes no** WLC, e suprima da sessão da saída. O WLC guarda a sessão ociosa por cinco minutos à revelia, assim que a fim executar um teste válido, você deve começar de novo.

4. Inverta a ordem do ISE PSN sob a configuração do convidado WLAN:



5. O log no convidado SSID, navega à **operação > às autenticações no** ISE, e verifica que as regras corretas da autorização estão batidas:



Para a segunda tentativa, o perfil da autorização de **MaibockGuestWireless** é batido corretamente para a autenticação inicial MAB. Similar à primeira tentativa ao **jesse-dunkel** (etapa 2), a autenticação ao **jesse-maibock** bate corretamente o **GuestPermit** para a autorização final. Porque não há nenhuma informação PSN-específica no perfil da autorização de **GuestPermit**, uma única regra pode ser usada para a autenticação a todo o PSN.

Troubleshooting

O indicador dos detalhes da autenticação é uma vista poderosa que indique cada etapa da autenticação/processo da autorização. A fim alcançá-lo, navegue às **operações > às autenticações** e clique o ícone da lupa sob a coluna dos detalhes. Use este indicador a fim verificar que as condições da regra da autenticação/autorização estão configuradas corretamente.

Neste caso, o campo do servidor da política é a área preliminar do foco. Este campo contém o hostname do ISE PSN por que a autenticação é prestada serviços de manutenção:

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 a entrada do servidor da política à condição da regra e assegure-se de que o fósforo dois (este valor é diferenciando maiúsculas e minúsculas):

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

Nota: É importante recordar que você deve desligar do SSID e cancelar a entrada de cliente do WLC entre testes.