Konfigurationsbeispiel für ISE mit statischer Umleitung für isolierte Gastnetzwerke

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die Cisco Identity Services Engine (ISE) mit statischer Umleitung für isolierte Gastnetzwerke konfiguriert wird, um Redundanz zu gewährleisten. Außerdem wird beschrieben, wie der Richtlinienknoten so konfiguriert wird, dass Clients keine nicht verifizierbare Zertifikatswarnung angezeigt wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Cisco ISE Central Web Authentication (CWA) und alle zugehörigen Komponenten
- Browser-Überprüfung der Gültigkeit von Zertifikaten
- Cisco ISE Version 1.2.0.899 oder höher
- Version des Cisco Wireless LAN Controller (WLC) 7.2.110.0 oder höher (bevorzugt wird Version 7.4.100.0 oder höher)

Hinweis: CWA wird im Artikel *Cisco* Konfigurationsbeispiel für WLC und ISE im Abschnitt Zentrale Webauthentifizierung beschrieben.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco ISE Version 1.2.0.899
- Cisco Virtual WLC (vWLC)-Version 7,4 110,0
- Cisco Adaptive Security Appliance (ASA)) Version 8.2.5

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

In vielen BYOD-Umgebungen (Bring Your Own Device) ist das Gastnetzwerk vollständig vom internen Netzwerk einer demilitarisierten Zone (DMZ) isoliert. Häufig bietet der DHCP-Server in der Gast-DMZ den Gastbenutzern öffentliche DNS-Server (Domain Name System), da der einzige angebotene Service der Internetzugang ist.

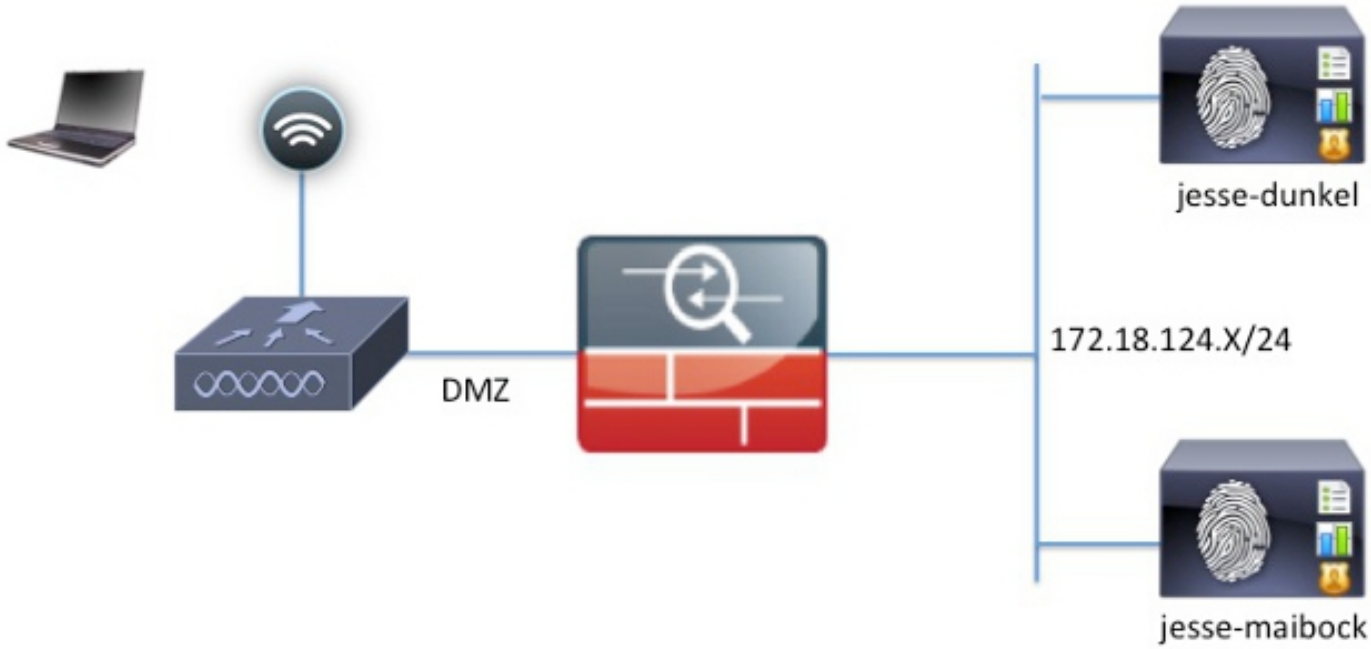
Dies erschwert die Umleitung von Gästen auf der ISE vor Version 1.2, da die ISE die Clients zur Webauthentifizierung an den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) umleitet. Mit ISE Version 1.2 und höher können Administratoren Gastbenutzer jedoch auf eine statische IP-Adresse oder einen statischen Hostnamen umleiten.

Konfigurieren

Netzwerkdiagramm

Dies ist ein logisches Diagramm.

> **Hinweis**: Im physischen Netzwerk befindet sich ein Wireless-Controller, die Access Points (APs) befinden sich im internen Netzwerk, und die Service Set Identification (SSID) ist mit dem DMZ-Controller verbunden. Weitere Informationen finden Sie in der Dokumentation zu Cisco WLCs.



Konfiguration

Die Konfiguration auf dem WLC bleibt unverändert von der normalen CWA-Konfiguration. Die SSID wird so konfiguriert, dass eine MAC-Filterung mit RADIUS-Authentifizierung und die RADIUS-Accounting-Punkte zu zwei oder mehr ISE-Richtlinienknoten zugelassen werden.

Der Schwerpunkt dieses Dokuments liegt auf der ISE-Konfiguration.

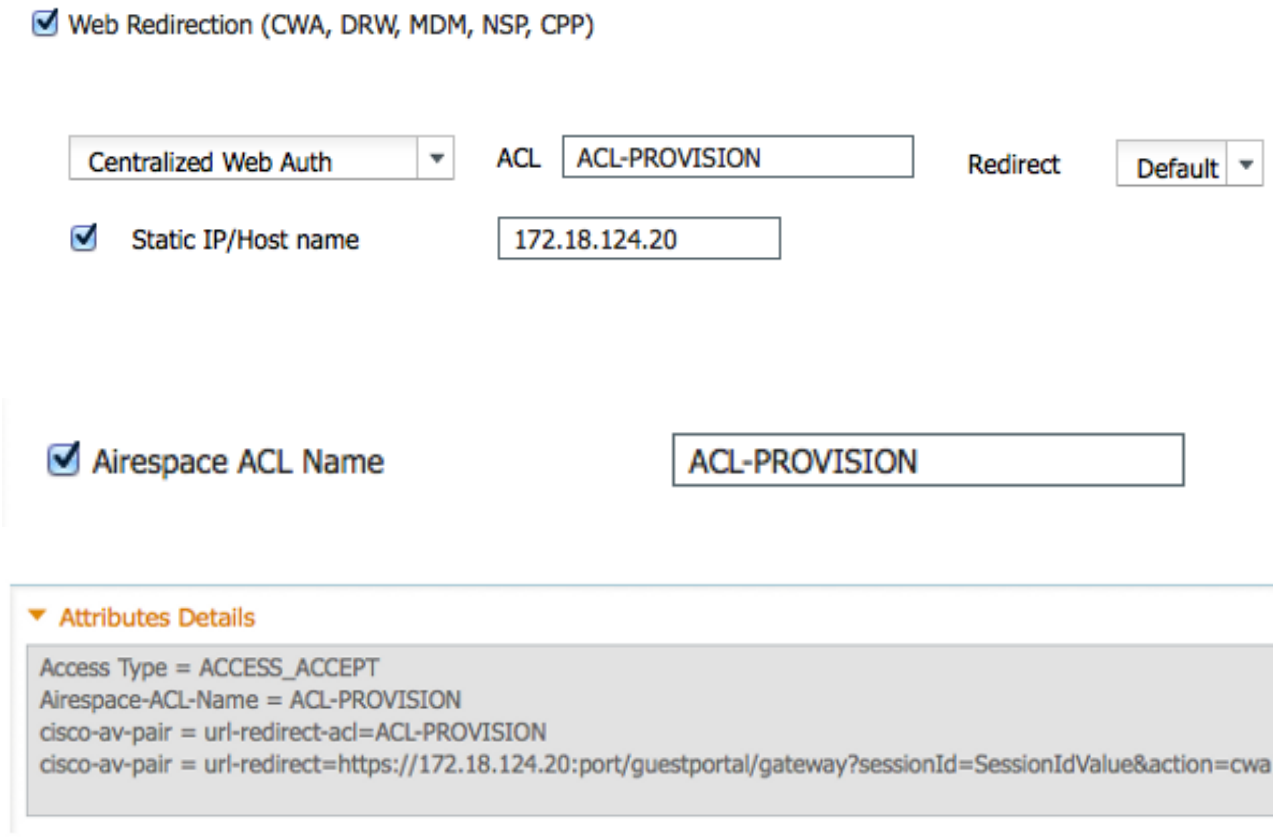
> **Hinweis**: In diesem Konfigurationsbeispiel sind die Richtlinienknoten **jesse-Dunkel** (172.18.124.20) und **jesse-maibock** (172.18.124.21).

Der CWA-Fluss beginnt, wenn der WLC eine RADIUS MAC Authentication Bypass (MAB)-Anfrage an die ISE sendet. Die ISE antwortet mit einer Umleitungs-URL zum Controller, um HTTP-Datenverkehr an die ISE umzuleiten. Es ist wichtig, dass der RADIUS- und HTTP-Datenverkehr zum gleichen Policy Services Node (PSN) geleitet wird, da die Sitzung auf einem einzelnen PSN verwaltet wird. Dies wird normalerweise mit einer einzigen Regel durchgeführt, und das PSN fügt einen eigenen Hostnamen in die CWA-URL ein. Bei einer statischen Umleitung müssen Sie jedoch eine Regel für jedes PSN erstellen, um sicherzustellen, dass der RADIUS- und der HTTP-Datenverkehr an dasselbe PSN gesendet werden.

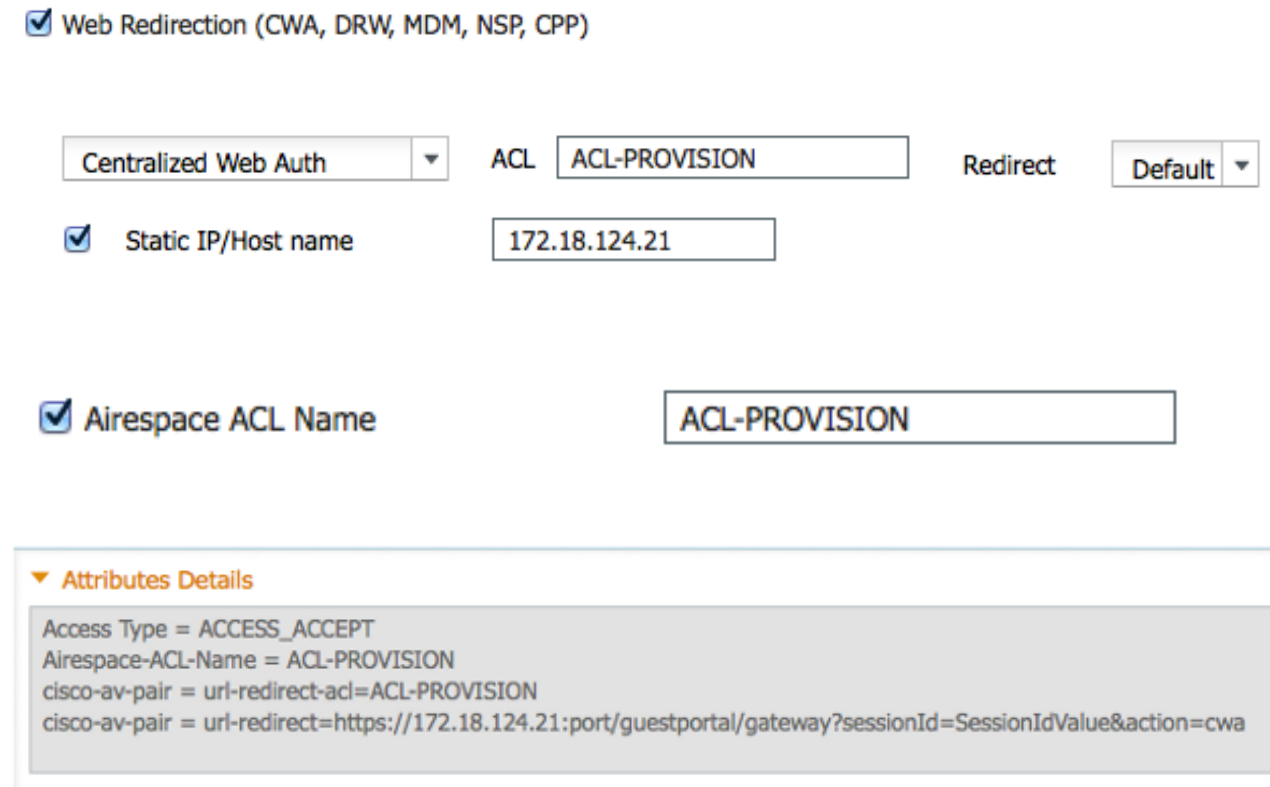
Gehen Sie wie folgt vor, um die ISE zu konfigurieren:

1. Legen Sie zwei Regeln fest, um den Client an die PSN-IP-Adresse umzuleiten. Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile**.

   Diese Bilder zeigen die Informationen für den Profilnamen **DunkelGuestWireless**:



Diese Bilder zeigen die Informationen für den Profilnamen **MaibockGuestWireless**:



Hinweis: Die **ACL-BEREITSTELLUNG** ist eine lokale Zugriffskontrollliste (ACL), die auf dem WLC konfiguriert ist, damit der Client bei der Authentifizierung mit der ISE kommunizieren kann. Weitere Informationen finden Sie im Artikel Cisco Central Web Authentication on the WLC and ISE Configuration Example (Zentrale Webauthentifizierung im WLC und ISE-Konfigurationsbeispiel).

2. Konfigurieren Sie die Autorisierungsrichtlinien so, dass sie mit dem **Network Access:ISE Host Name-**Attribut übereinstimmen, und stellen Sie das entsprechende Autorisierungsprofil bereit:

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	

Nachdem der Client an eine IP-Adresse umgeleitet wurde, erhalten Benutzer Zertifikatswarnungen, da der URL nicht mit den Informationen im Zertifikat übereinstimmt. Der FQDN im Zertifikat ist z. B. **jesse-Dunkel.rtpaa.local**, aber die URL ist **172.18.124.20**. Das folgende Beispiel-Zertifikat ermöglicht es dem Browser, das Zertifikat mit der IP-Adresse zu validieren:

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

Mithilfe von SAN-Einträgen (Subject Alternative Name) kann der Browser die URL validieren, die die IP-Adresse **172.18.124.20** enthält. Es müssen drei SAN-Einträge erstellt werden, um die verschiedenen Client-Inkompatibilitäten zu beheben.

3. Erstellen Sie einen SAN-Eintrag für den DNS-Namen, und stellen Sie sicher, dass dieser dem **CN=**-Eintrag im Feld "Betreff" entspricht.

4. Erstellen Sie zwei Einträge, damit Clients die IP-Adresse validieren können. Diese beziehen sich sowohl auf den DNS-Namen der IP-Adresse als auch auf die IP-Adresse, die im IP Address-Attribut angezeigt wird. Einige Clients verweisen nur auf den DNS-Namen. Andere

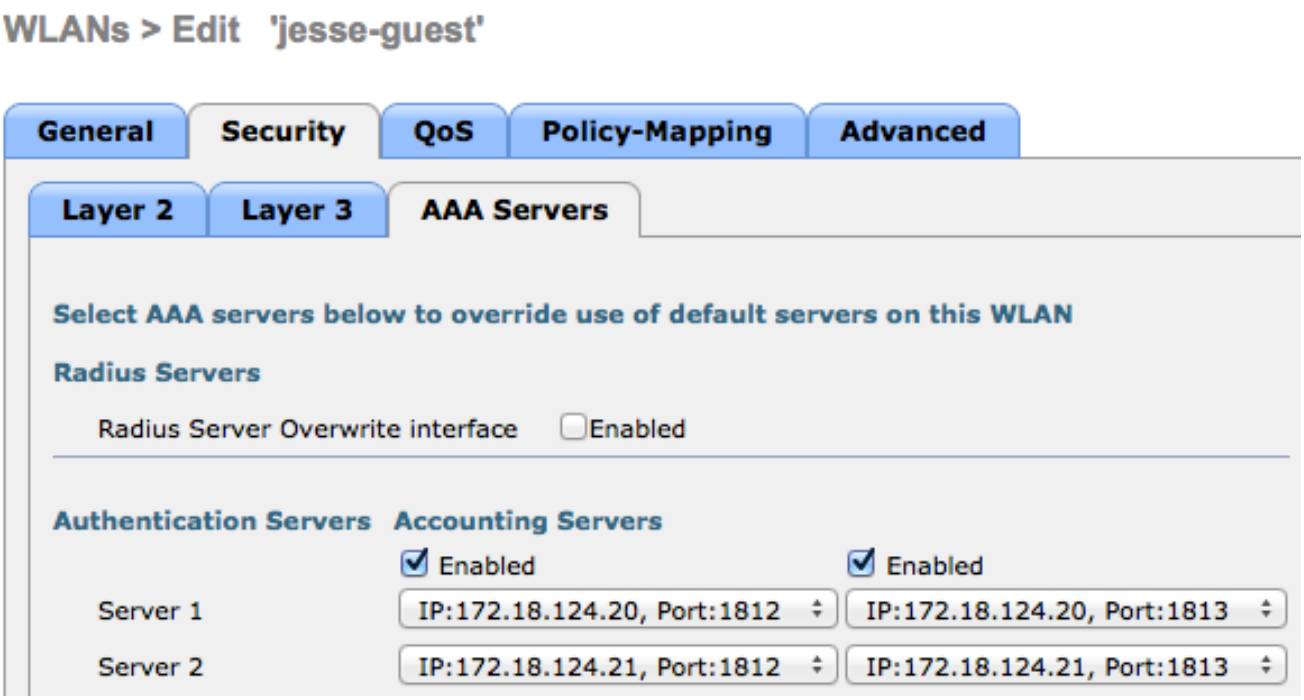
akzeptieren keine IP-Adresse im DNS-Name-Attribut, verweisen aber stattdessen auf das IP-Adresse-Attribut.

Hinweis: Weitere Informationen zur Zertifikatsgenerierung finden Sie im **Cisco Identity Services Engine Hardware Installation Guide, Release 1.2**.

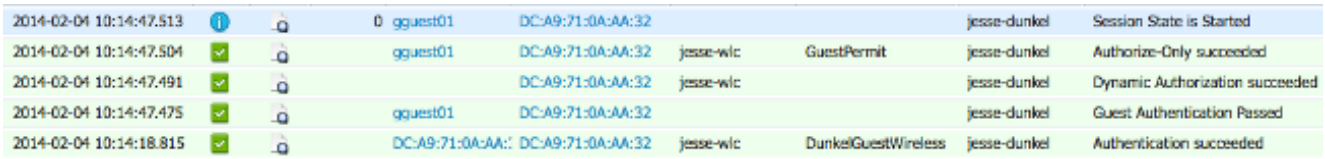
Überprüfen

Gehen Sie wie folgt vor, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert:

1. Um zu überprüfen, ob beide Regeln funktionsfähig sind, legen Sie die Reihenfolge der ISE-PSNs, die im WLAN konfiguriert sind, manuell fest:



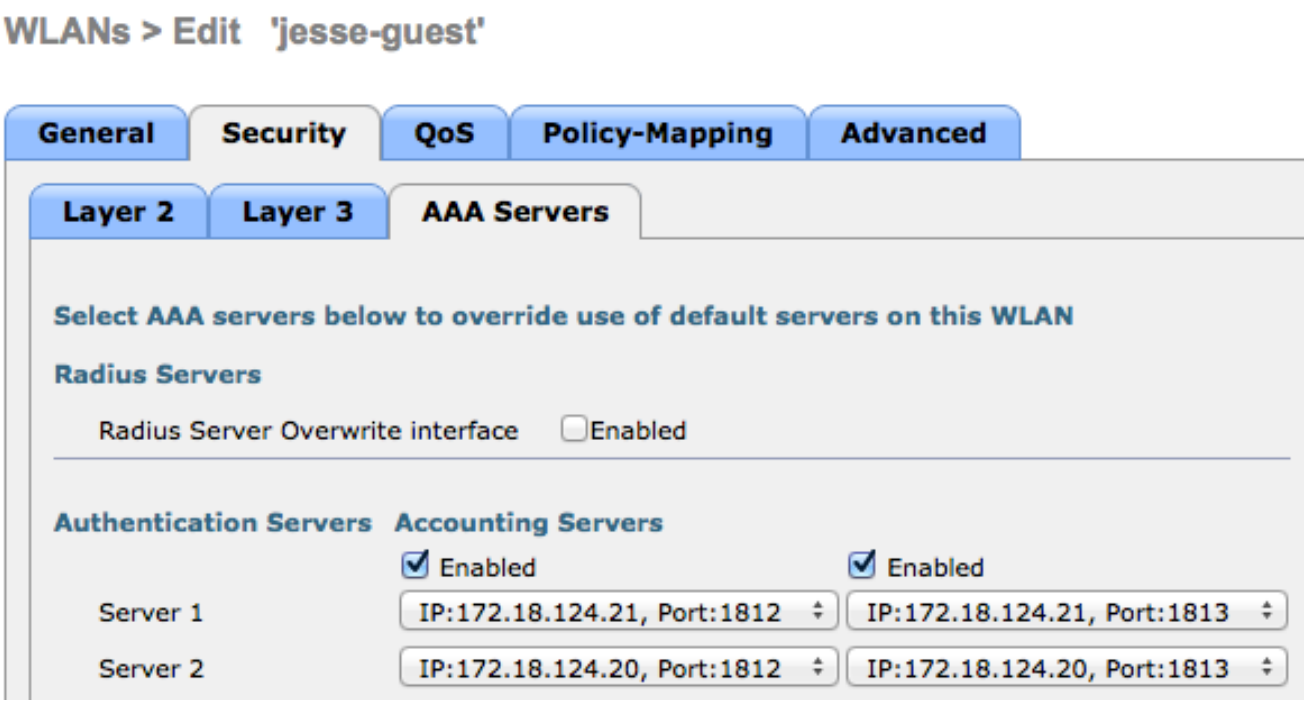
2. Melden Sie sich bei der Gast-SSID an, navigieren Sie zu **Operation > Authentications** in der ISE, und überprüfen Sie, ob die richtigen Autorisierungsregeln eingehalten werden:



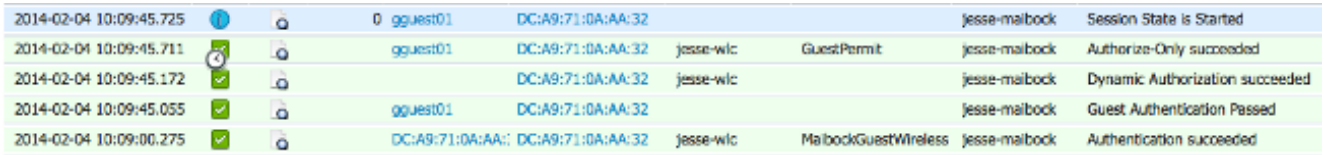
Die erste MAB-Authentifizierung wird dem **DunkelGuestWireless-**Autorisierungsprofil gegeben. Dies ist die Regel, die speziell zu **Jesse-Dunkel** umleitet, dem ersten ISE-Knoten. Nachdem sich der Benutzer **gguest01** angemeldet hat, wird die richtige endgültige Berechtigung für **GuestPermit** erteilt.

3. Um die Authentifizierungssitzungen aus dem WLC zu löschen, trennen Sie das Client-Gerät vom Wireless-Netzwerk, navigieren Sie zu **Monitor > Clients** im WLC, und löschen Sie die Sitzung aus der Ausgabe. Der WLC hält die Leerlaufsitzung standardmäßig für fünf Minuten an. Um einen gültigen Test durchführen zu können, müssen Sie also einen neuen beginnen.

4. Umkehren der Reihenfolge der ISE-PSNs unter der Gast-WLAN-Konfiguration:



5. Melden Sie sich bei der Gast-SSID an, navigieren Sie zu **Operation > Authentications** in der ISE, und überprüfen Sie, ob die richtigen Autorisierungsregeln eingehalten werden:



Beim zweiten Versuch wird das **MaibockGuestWireless-**Autorisierungsprofil für die erste MAB-Authentifizierung korrekt aufgerufen. Ähnlich wie beim ersten Versuch, **jesse-Dunkel** zu (Schritt 2), trifft die Authentifizierung zu **jesse-maibock** die **GuestPermit** für die endgültige Autorisierung korrekt. Da das **GuestPermit-**Autorisierungsprofil keine PSN-spezifischen Informationen enthält, kann eine einzelne Regel für die Authentifizierung mit einem beliebigen PSN verwendet werden.

Fehlerbehebung

Das Fenster Authentifizierungsdetails ist eine leistungsstarke Ansicht, die jeden Schritt des Authentifizierungs-/Autorisierungsprozesses anzeigt. Navigieren Sie zu **Operations > Authentications (Vorgänge > Authentifizierungen),** und klicken Sie in der Spalte Details auf das Lupensymbol. Verwenden Sie dieses Fenster, um zu überprüfen, ob die Authentifizierungs-/Autorisierungsregelbedingungen korrekt konfiguriert sind.

In diesem Fall ist das Feld "Policy Server" der primäre Fokusbereich. Dieses Feld enthält den Hostnamen des ISE-PSN, über den die Authentifizierung abgewickelt wird:

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

Vergleichen Sie den Richtlinienserver-Eintrag mit der Regelbedingung, und stellen Sie sicher, dass beide übereinstimmen (bei diesem Wert ist die Groß- und Kleinschreibung zu beachten):

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

Hinweis: Beachten Sie, dass Sie zwischen den Tests die Verbindung zum SSID trennen und den Clienteintrag aus dem WLC löschen müssen.