Esempio di configurazione di ISE con reindirizzamento statico per reti guest isolate

Sommario

Introduzione

In questo documento viene descritto come configurare Cisco Identity Services Engine (ISE) con reindirizzamento statico per reti guest isolate per mantenere la ridondanza. Viene inoltre descritto come configurare il nodo dei criteri in modo che ai client non venga visualizzato un avviso di certificato non verificabile.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ISE Central Web Authentication (CWA) e tutti i componenti correlati
- Verifica tramite browser della validità del certificato
- Cisco ISE Versione 1.2.0.899 o successiva
- Versione Cisco Wireless LAN Controller (WLC) 7.2.110.0 o successiva (si consiglia la versione 7.4.100.0 o successiva)

Nota: CWA è descritto nell'articolo Central Web Authentication on the WLC and ISE Configuration Example in Cisco.

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco ISE Versione 1.2.0.899
- Cisco Virtual WLC (vWLC) versione 7.4.110.0
- Cisco Adaptive Security Appliance (ASA)a) Versione 8.2.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Premesse

In molti ambienti BYOD (Bring Your Own Device), la rete guest è completamente isolata dalla rete interna in una zona demilitarizzata. Spesso, il DHCP nella DMZ guest offre server DNS (Domain Name System) pubblici agli utenti guest perché l'unico servizio offerto è l'accesso a Internet.

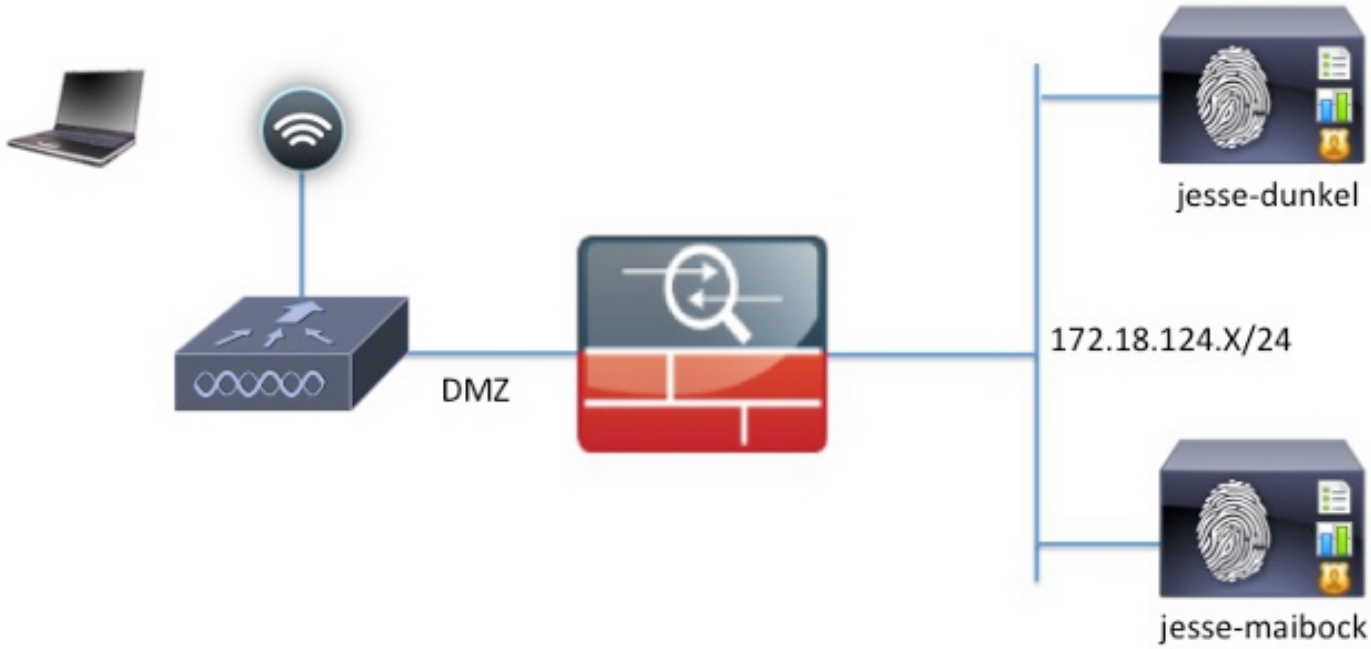
Ciò rende difficile il reindirizzamento guest sull'ISE prima della versione 1.2, in quanto ISE reindirizza i client al nome di dominio completo (FQDN) per l'autenticazione Web. Tuttavia, con ISE versione 1.2 e successive, gli amministratori possono reindirizzare gli utenti guest a un indirizzo IP statico o a un nome host.

Configurazione

Esempio di rete

Questo è un diagramma logico.

> **Nota:** Fisicamente, nella rete interna è presente un controller wireless, i punti di accesso (AP) si trovano nella rete interna e il SSID (Service Set Identification) è ancorato al controller DMZ. Per ulteriori informazioni, consultare la documentazione dei Cisco WLC.



Configurazione

La configurazione sul WLC rimane invariata rispetto a una configurazione CWA normale. Il SSID è configurato in modo da consentire il filtro MAC con autenticazione RADIUS e l'accounting RADIUS punta verso due o più nodi dei criteri ISE.

Nel documento si fa riferimento alla configurazione ISE.

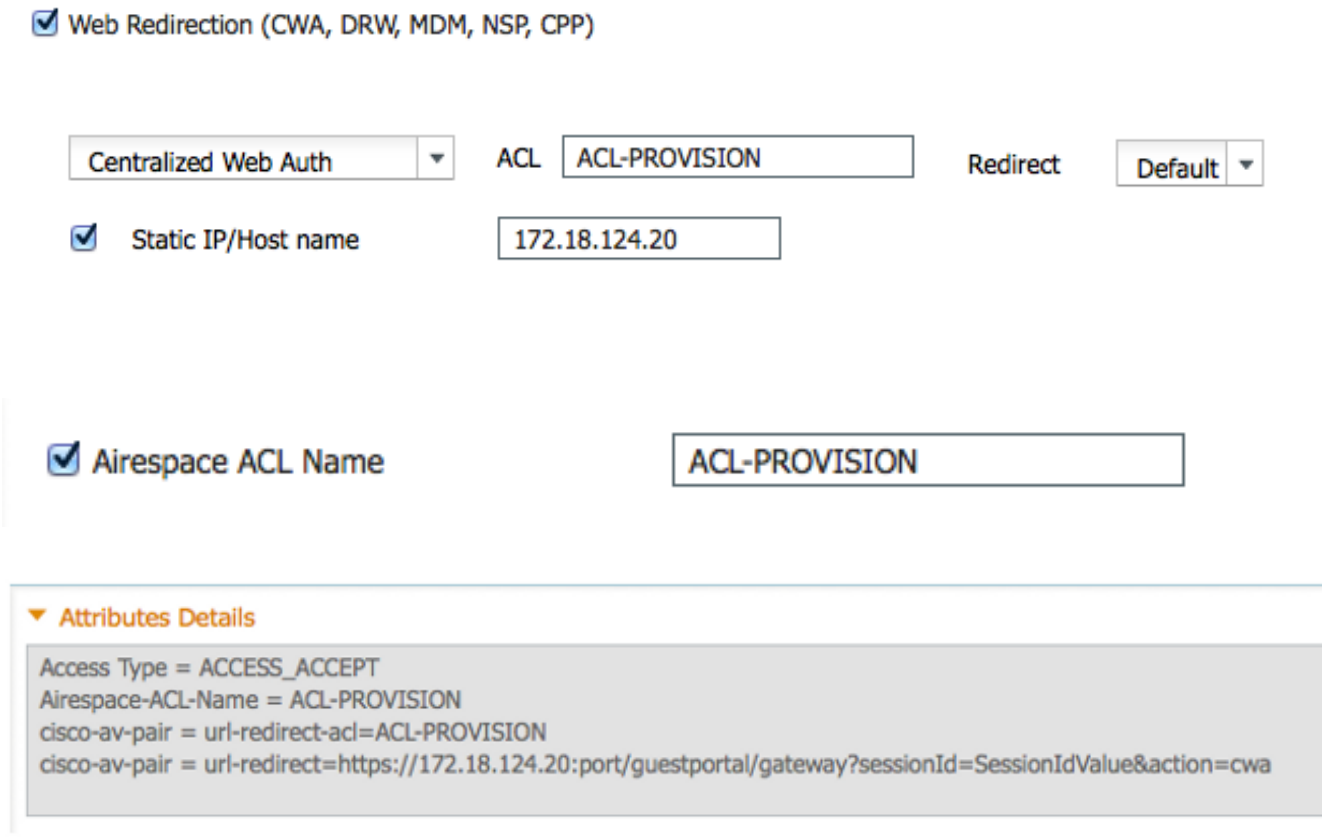
> **Nota:** In questa configurazione di esempio, i nodi dei criteri sono **jesse-dunkel** (172.18.124.20) e **jesse-maibock** (172.18.124.21).

Il flusso CWA inizia quando il WLC invia una richiesta RADIUS MAC Authentication Bypass (MAB) all'ISE. L'ISE risponde con un URL di reindirizzamento al controller per reindirizzare il traffico HTTP all'ISE. È importante che il traffico RADIUS e HTTP venga indirizzato allo stesso PSN (Policy Services Node) perché la sessione viene gestita su un singolo PSN. Questa operazione viene in genere eseguita con una singola regola e il PSN inserisce il proprio nome host nell'URL di CWA. Tuttavia, con un reindirizzamento statico, è necessario creare una regola per ogni PSN per garantire che il traffico RADIUS e HTTP venga inviato allo stesso PSN.

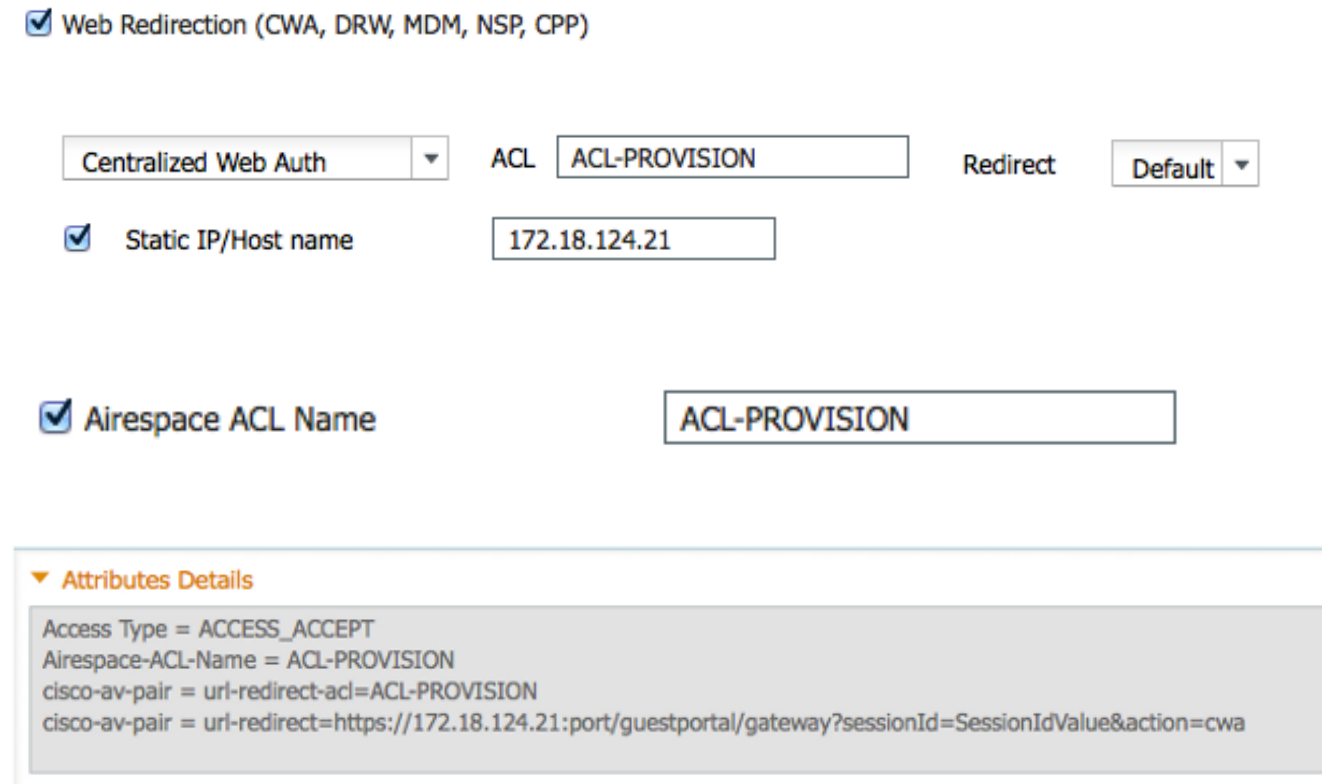
Per configurare l'ISE, completare la procedura seguente:

1. Impostare due regole per reindirizzare il client all'indirizzo IP PSN. Passare a **Criterio > Elementi criteri > Risultati > Autorizzazione > Profili di autorizzazione**.

   Le immagini seguenti mostrano le informazioni relative al nome del profilo **DunkelGuestWireless**:



Le immagini seguenti mostrano le informazioni relative al nome del profilo **MaibockGuestWireless**:

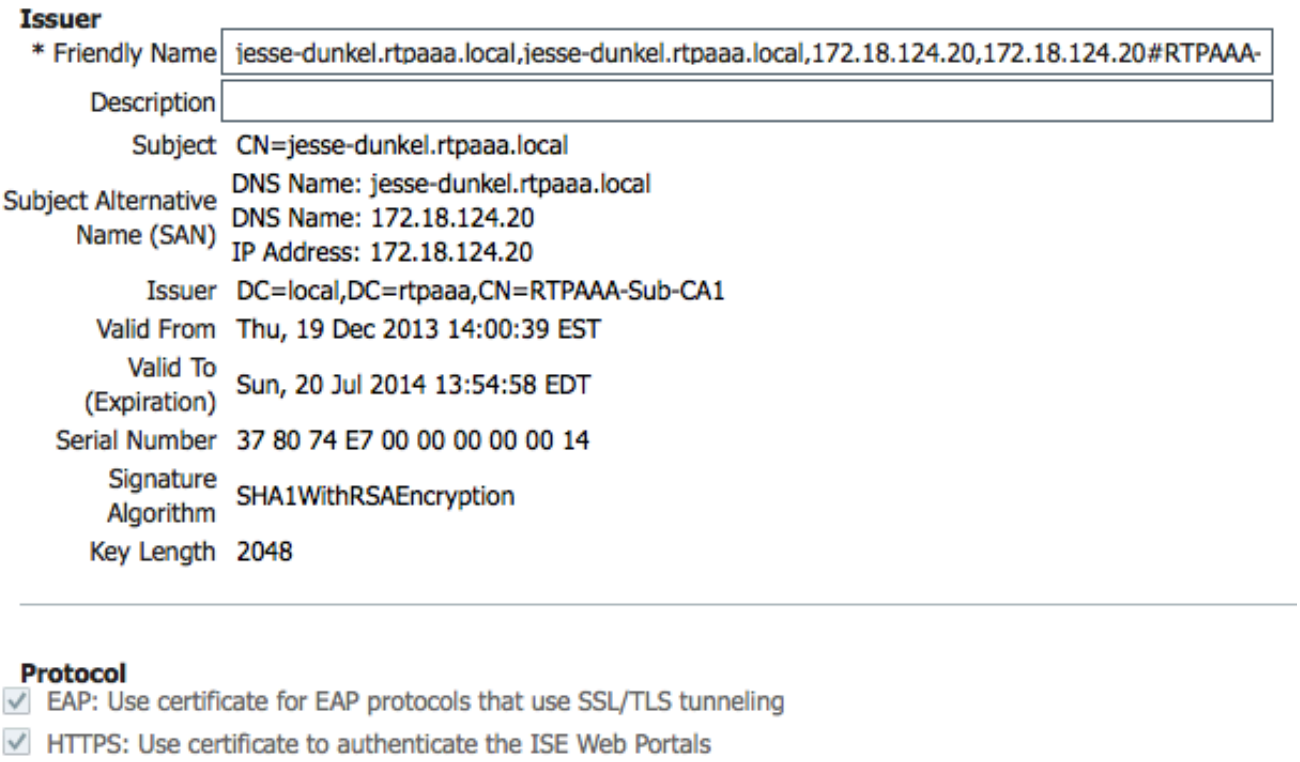


Nota: ACL-PROVISION è un elenco di controllo di accesso (ACL) locale configurato sul WLC per consentire al client di comunicare con ISE dopo l'autenticazione. Per ulteriori informazioni, fare riferimento all'articolo sull'autenticazione Web centrale sul WLC e sull'esempio di configurazione di Cisco ISE.

2. Configurare i criteri di autorizzazione in modo che corrispondano nell'attributo **Network Access:ISE Host Name** (Accesso di rete:nome host ISE) e fornire il profilo di autorizzazione appropriato:

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	

Ora che il client viene reindirizzato a un indirizzo IP, gli utenti ricevono avvisi relativi ai certificati perché l'URL non corrisponde alle informazioni contenute nel certificato. Ad esempio, l'FQDN nel certificato è **jesse-dunkel.rtpaaa.local**, ma l'URL è **172.18.124.20**. Di seguito è riportato un esempio di certificato che consente al browser di convalidare il certificato con l'indirizzo IP:



Tramite l'utilizzo di voci SAN (Subject Alternative Name), il browser può convalidare l'URL che include l'indirizzo IP **172.18.124.20**. Per risolvere le varie incompatibilità dei client, è necessario creare tre voci SAN.

3. Creare una voce SAN per il nome DNS e verificare che corrisponda alla voce **CN=** del campo Oggetto.

4. Creare due voci per consentire ai client di convalidare l'indirizzo IP; queste informazioni sono valide sia per il Nome DNS dell'indirizzo IP sia per l'indirizzo IP visualizzato nell'attributo Indirizzo IP. Alcuni client fanno riferimento solo al nome DNS. Altri non accettano un indirizzo

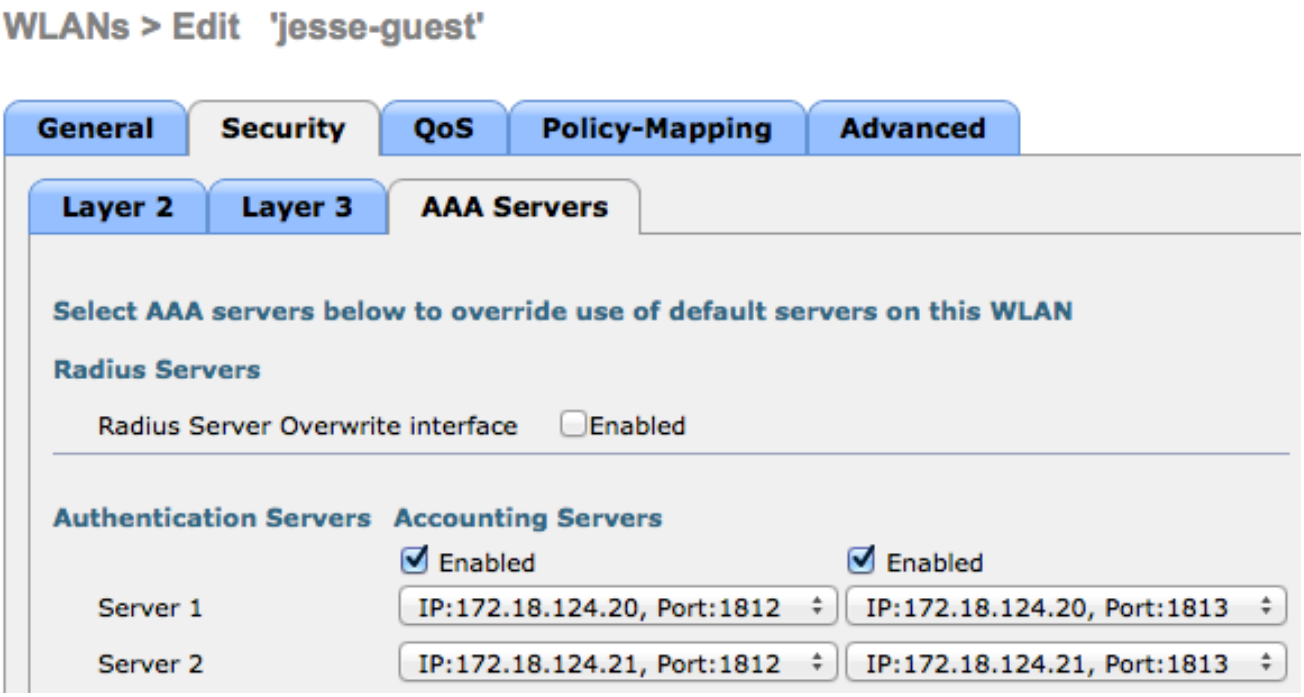
IP nell'attributo Nome DNS ma fanno riferimento all'attributo Indirizzo IP.

Nota: Per ulteriori informazioni sulla generazione dei certificati, consultare la **guida all'installazione dell'hardware di Cisco Identity Services Engine, versione 1.2**.

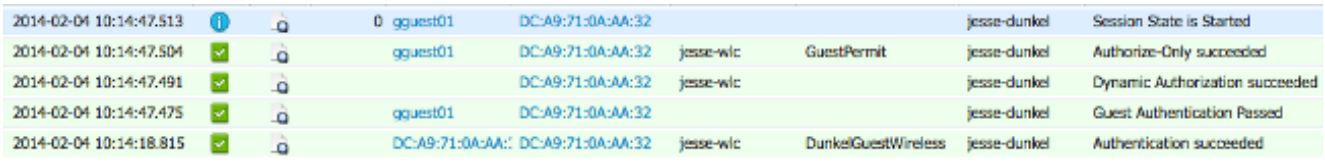
Verifica

Per verificare che la configurazione funzioni correttamente, completare la procedura seguente:

1. Per verificare che entrambe le regole siano funzionali, impostare manualmente l'ordine dei PSN ISE configurati sulla WLAN:



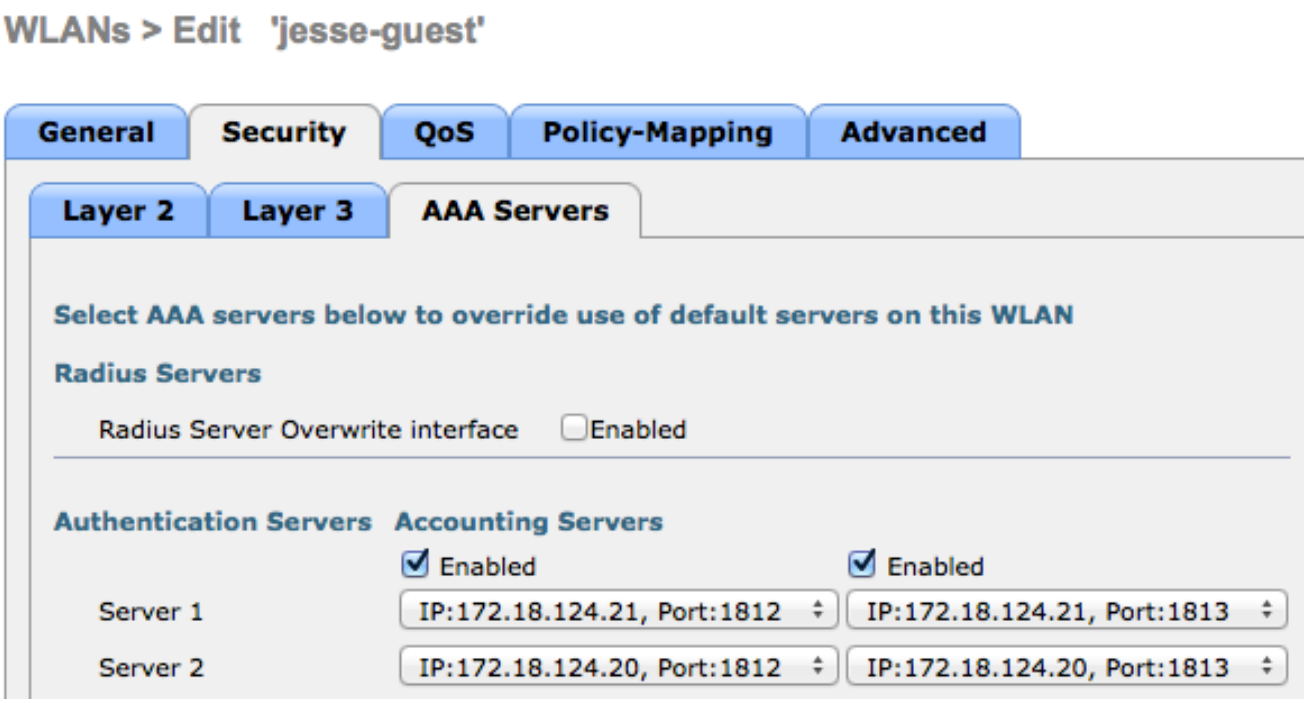
2. Accedere all'SSID guest, selezionare **Operation > Authentications** in ISE e verificare che siano state trovate le regole di autorizzazione corrette:



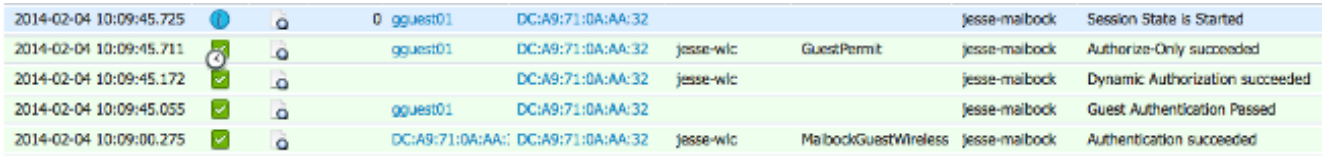
L'autenticazione MAB iniziale viene assegnata al profilo di autorizzazione **DunkelGuestWireless**. Questa è la regola che reindirizza specificamente a **jesse-dunkel**, che è il primo nodo ISE. Dopo che l'utente **guest01** ha eseguito l'accesso, viene fornita l'autorizzazione finale corretta di **GuestPermit**.

3. Per cancellare le sessioni di autenticazione dal WLC, disconnettere il dispositivo client dalla rete wireless, selezionare **Monitor > Client** sul WLC ed eliminare la sessione dall'output. Per impostazione predefinita, il WLC mantiene la sessione inattiva per cinque minuti, quindi per eseguire un test valido è necessario ricominciare.

4. Invertire l'ordine dei PSN ISE nella configurazione WLAN guest:



5. Accedere all'SSID guest, selezionare **Operation > Authentications** in ISE e verificare che siano state trovate le regole di autorizzazione corrette:



Per il secondo tentativo, il profilo di autorizzazione **MaibockGuestWireless** viene attivato correttamente per l'autenticazione MAB iniziale. Come nel primo tentativo di **jesse-dunkel** (punto 2), l'autenticazione a **jesse-maibock** incontra correttamente **GuestPermit** per l'autorizzazione finale. Poiché nel profilo di autorizzazione **GuestPermit** non sono presenti informazioni specifiche di PSN, è possibile utilizzare una sola regola per l'autenticazione in qualsiasi PSN.

Risoluzione dei problemi

La finestra Dettagli autenticazione è una visualizzazione avanzata che mostra tutte le fasi del processo di autenticazione/autorizzazione. Per accedervi, selezionare **Operazioni > Autenticazioni** e fare clic sull'icona della lente di ingrandimento nella colonna Dettagli. Utilizzare questa finestra per verificare che le condizioni della regola di autenticazione/autorizzazione siano configurate correttamente.

In questo caso, il campo Server dei criteri è l'area di interesse principale. Questo campo contiene il nome host del numero di serie del servizio (PSN) ISE tramite il quale viene servita l'autenticazione:

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

Confrontare la voce Server dei criteri con la condizione della regola e verificare che i due valori corrispondano (questo valore fa distinzione tra maiuscole e minuscole):

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

Nota: È importante ricordare che è necessario disconnettersi dall'SSID e cancellare la voce del client dal WLC tra un test e l'altro.