Configurer les serveurs Radius externes sur ISE

Table des matières

Introduction

Ce document décrit la configuration d'un serveur RADIUS sur ISE en tant que serveur proxy et d'autorisation. Ici, deux serveurs ISE sont utilisés et l'un d'eux fait office de serveur externe. Cependant, n'importe quel serveur RADIUS compatible RFC peut être utilisé.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Connaissances de base du protocole RADIUS
- Expertise en configuration de politiques ISE (Identity Services Engine)

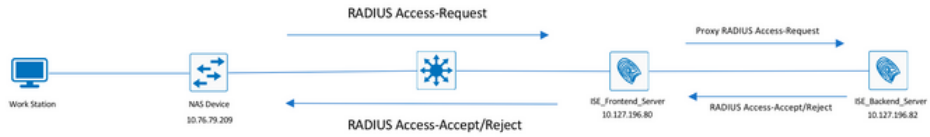
Composants utilisés

Les informations contenues dans ce document sont basées sur les versions 2.2 et 2.4 de Cisco ISE.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

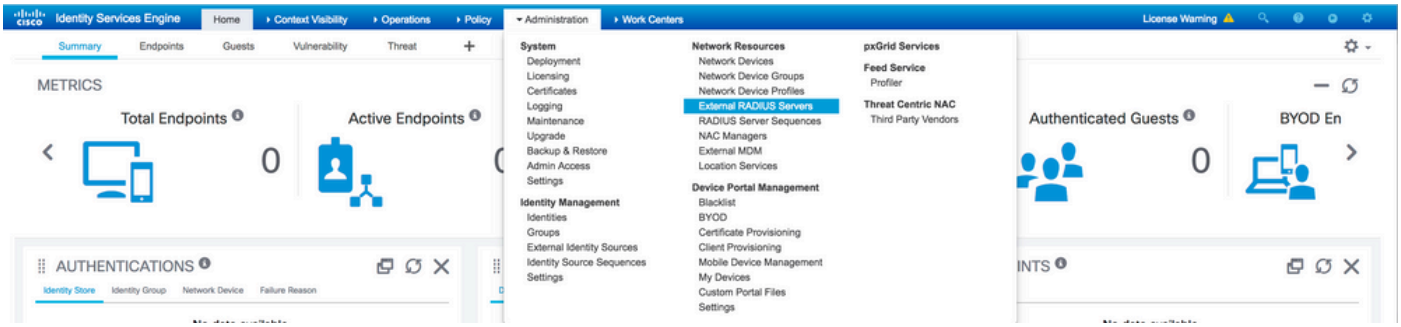
Configurer

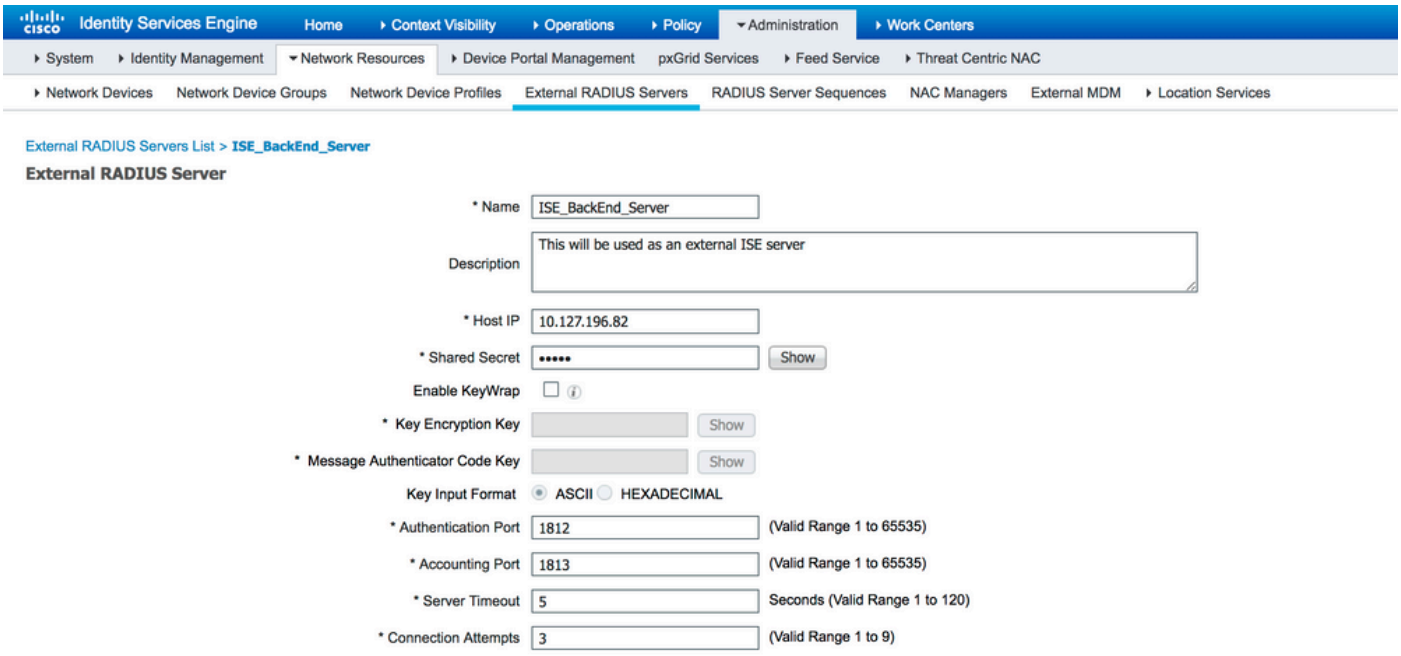
Diagramme du réseau



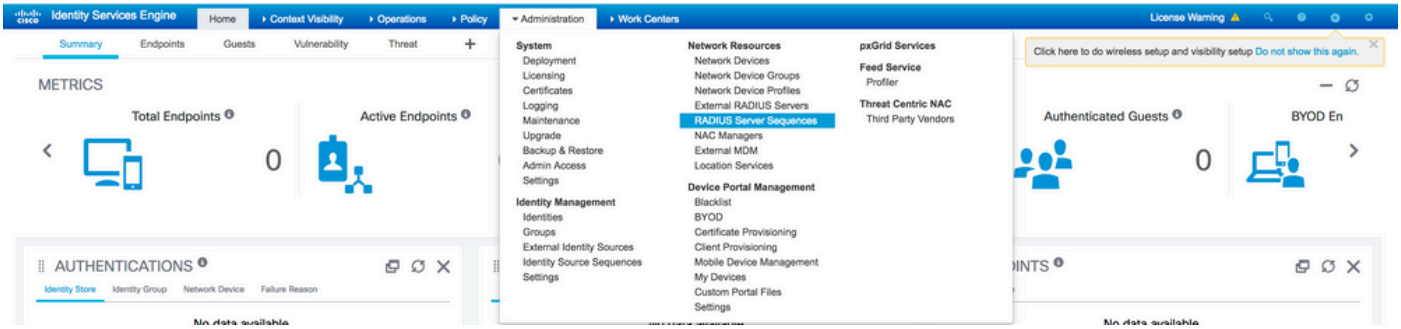
Configurer ISE (serveur frontal)

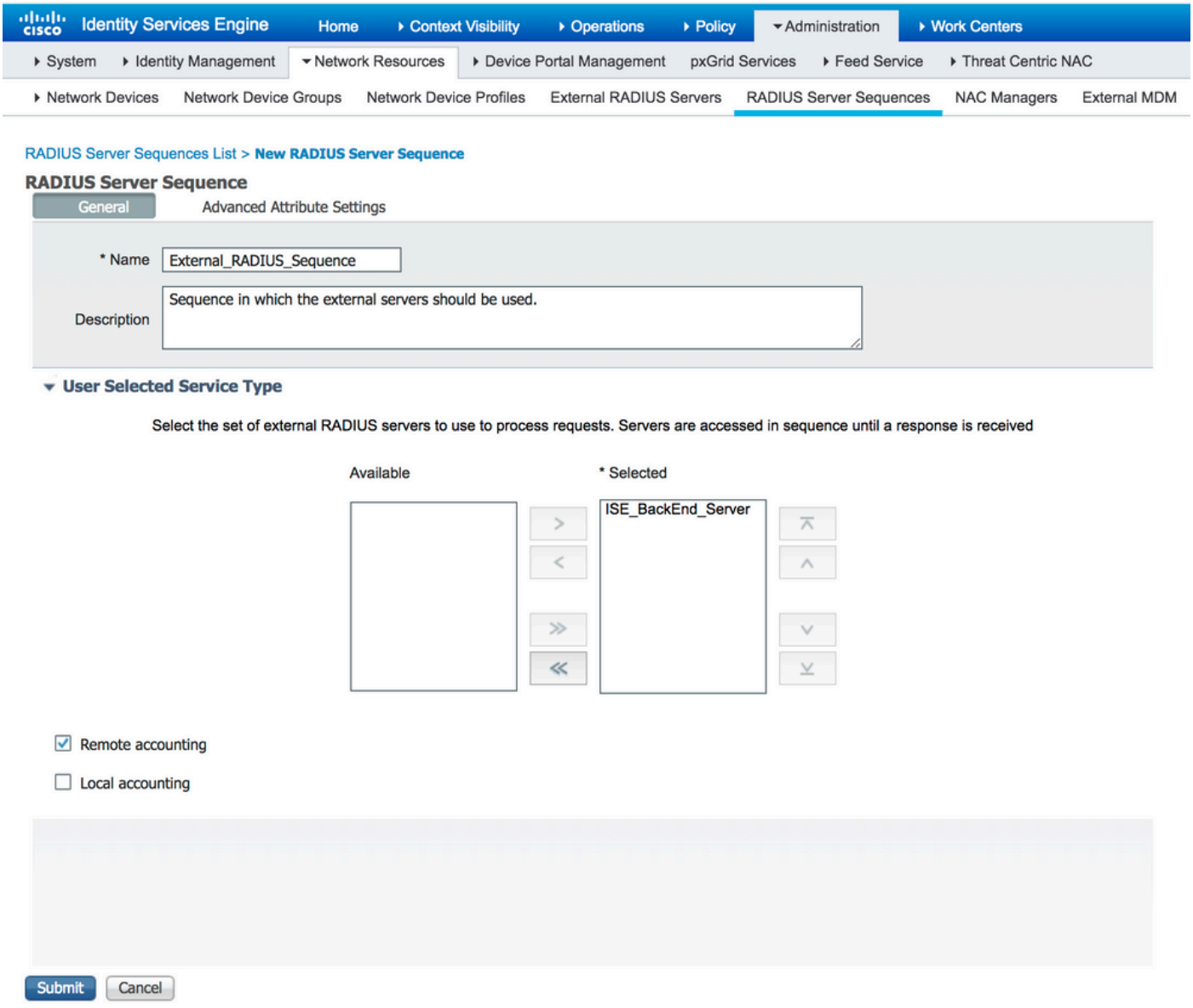
Étape 1. Plusieurs serveurs RADIUS externes peuvent être configurés et utilisés afin d'authentifier les utilisateurs sur ISE. Afin de configurer des serveurs RADIUS externes, accédez à Administration > Network Resources > External RADIUS Servers > Add, comme l'illustre l'image :





Étape 2. Pour utiliser le serveur RADIUS externe configuré, une séquence de serveur RADIUS doit être configurée de la même manière que la séquence source Identity. Pour configurer la même configuration, accédez à Administration > Network Resources > RADIUS Server Sequences > Add, comme l'illustre l'image.

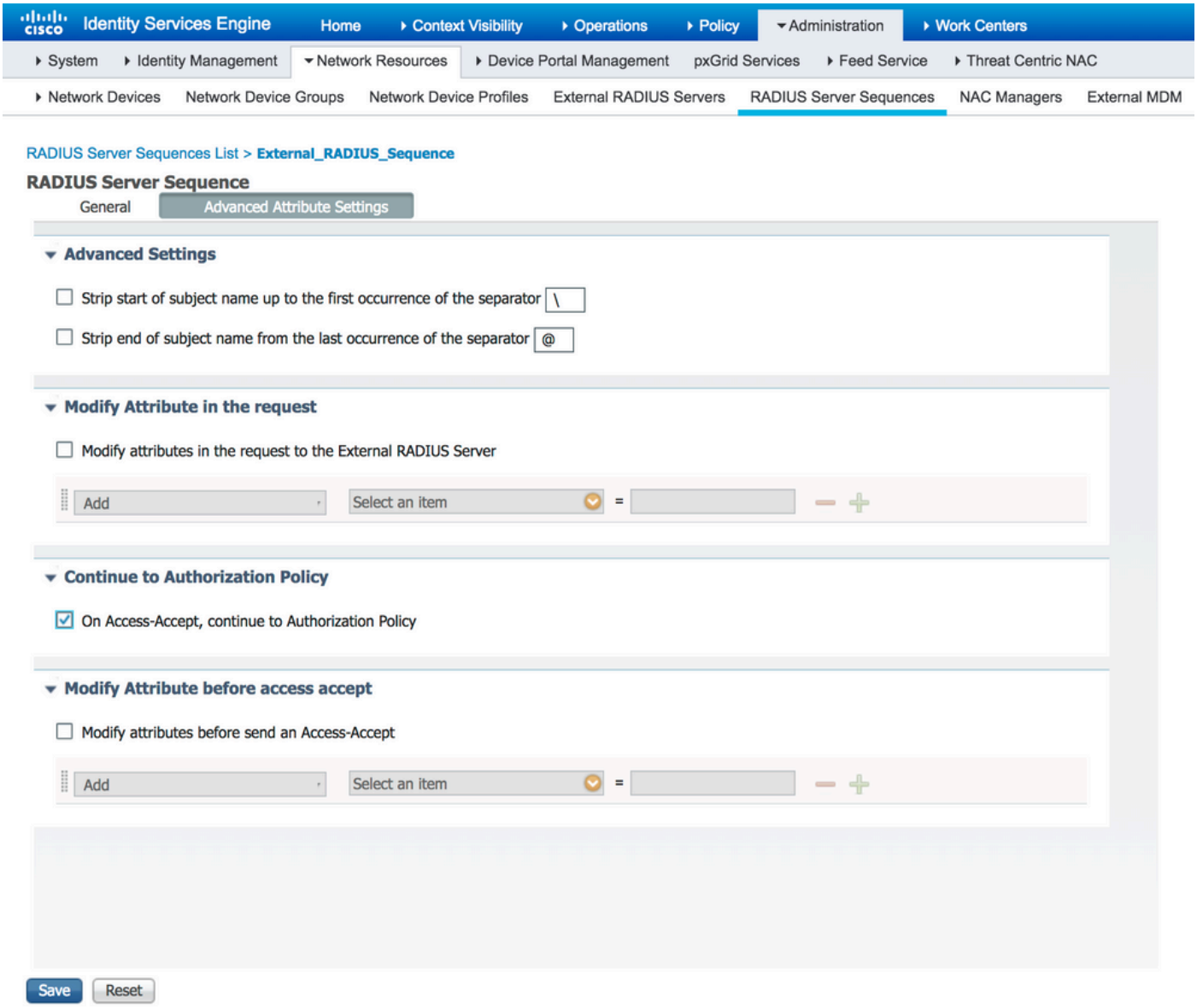




Remarque : l'une des options disponibles lors de la création de la séquence de serveur consiste à choisir si la gestion des comptes doit être effectuée localement sur l'ISE ou sur le serveur RADIUS externe. En fonction de l'option choisie ici, ISE décide si les requêtes de gestion des comptes doivent être transmises par proxy ou si ces journaux doivent être stockés localement.

Étape 3. Il existe une section supplémentaire qui offre plus de flexibilité sur la manière dont ISE doit se comporter lorsqu'il proxie des requêtes vers des serveurs RADIUS externes. Vous pouvez

le trouver sous Advance Attribute Settings, comme l'illustre l'image.



- Advanced Settings : fournit des options pour supprimer le début ou la fin du nom d'utilisateur dans les requêtes RADIUS avec un délimiteur.
- Modify Attribute in the request : permet de modifier n'importe quel attribut RADIUS dans les demandes RADIUS. La liste ci-dessous indique les attributs qui peuvent être ajoutés/supprimés/mis à jour :

```
User-Name--[1]
NAS-IP-Address--[4]
NAS-Port--[5]
Service-Type--[6]
Framed-Protocol--[7]
Framed-IP-Address--[8]
Framed-IP-Netmask--[9]
Filter-ID--[11]
Framed-Compression--[13]
Login-IP-Host--[14]
Callback-Number--[19]
```

```
State--[24]
VendorSpecific--[26]
Called-Station-ID--[30]
Calling-Station-ID--[31]
NAS-Identifier--[32]
Login-LAT-Service--[34]
Login-LAT-Node--[35]
Login-LAT-Group--[36]
Event-Timestamp--[55]
Egress-VLANID--[56]
Ingress-Filters--[57]
Egress-VLAN-Name--[58]
User-Priority-Table--[59]
NAS-Port-Type--[61]
Port-Limit--[62]
Login-LAT-Port--[63]
Password-Retry--[75]
Connect-Info--[77]
NAS-Port-Id--[87]
Framed-Pool--[88]
NAS-Filter-Rule--[92]
NAS-IPv6-Address--[95]
Framed-Interface-Id--[96]
Framed-IPv6-Prefix--[97]
Login-IPv6-Host--[98]
Error-Cause--[101]
Delegated-IPv6-Prefix--[123]
Framed-IPv6-Address--[168]
DNS-Server-IPv6-Address--[169]
Route-IPv6-Information--[170]
Delegated-IPv6-Prefix-Pool--[171]
Stateful-IPv6-Address-Pool--[172]
```

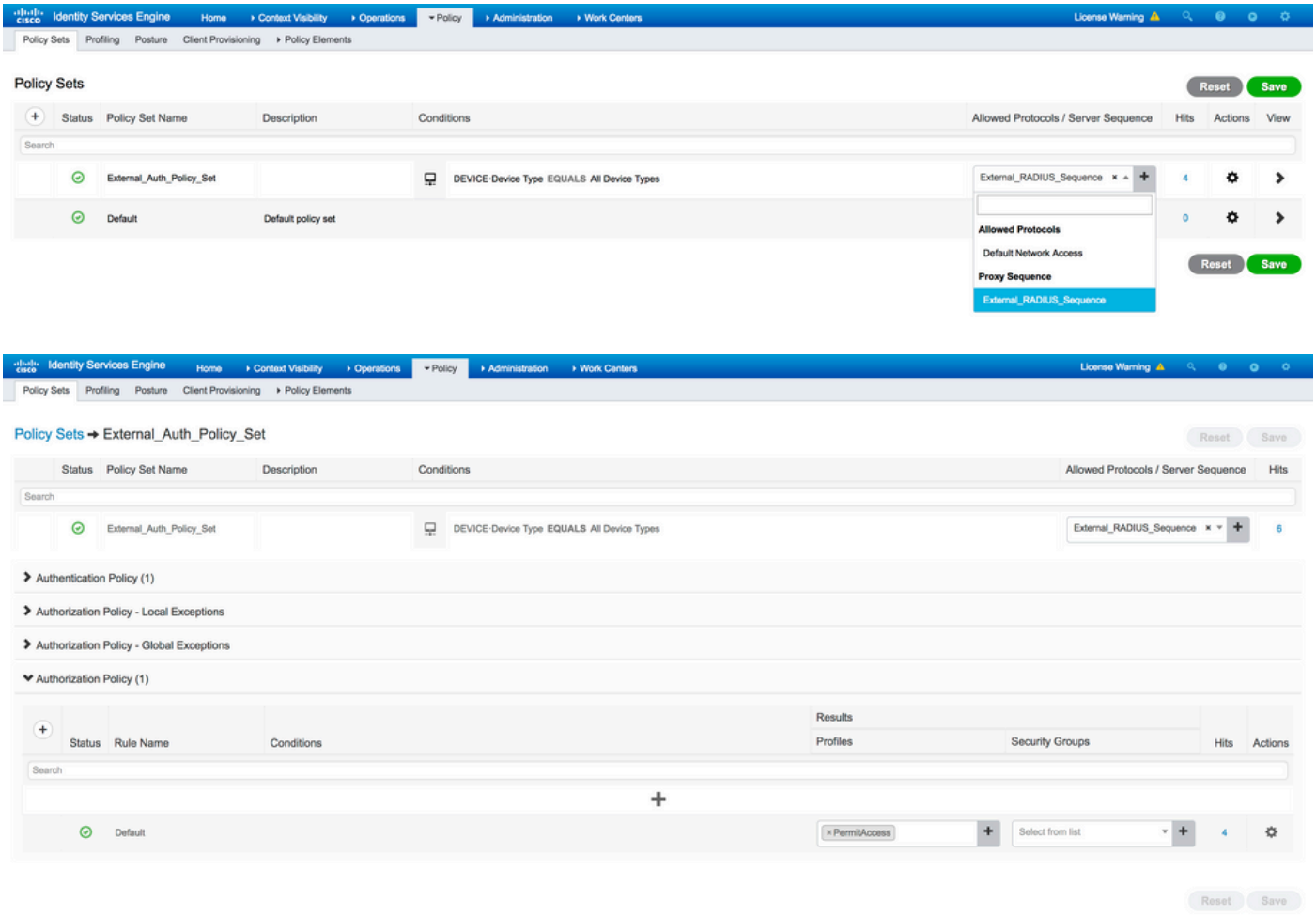
- Continue to Authorization Policy on Access-Accept : fournit une option permettant de choisir si ISE doit simplement envoyer l'autorisation d'accès telle quelle ou continuer à fournir un accès basé sur les politiques d'autorisation configurées sur l'ISE plutôt que sur l'autorisation fournie par le serveur RADIUS externe. Si cette option est sélectionnée, l'autorisation fournie par le serveur RADIUS externe est remplacée par l'autorisation fournie par ISE.

  Remarque : cette option ne fonctionne que si le serveur RADIUS externe envoie un Access-Accept en réponse à la requête d'accès RADIUS proxy.

- Modify Attribute before Access-Accept : similaire à la Modify Attribute in the request, les attributs mentionnés précédemment peuvent être ajoutés/supprimés/mis à jour présents dans l'acceptation d'accès envoyée par le serveur RADIUS externe avant d'être envoyés au périphérique réseau.

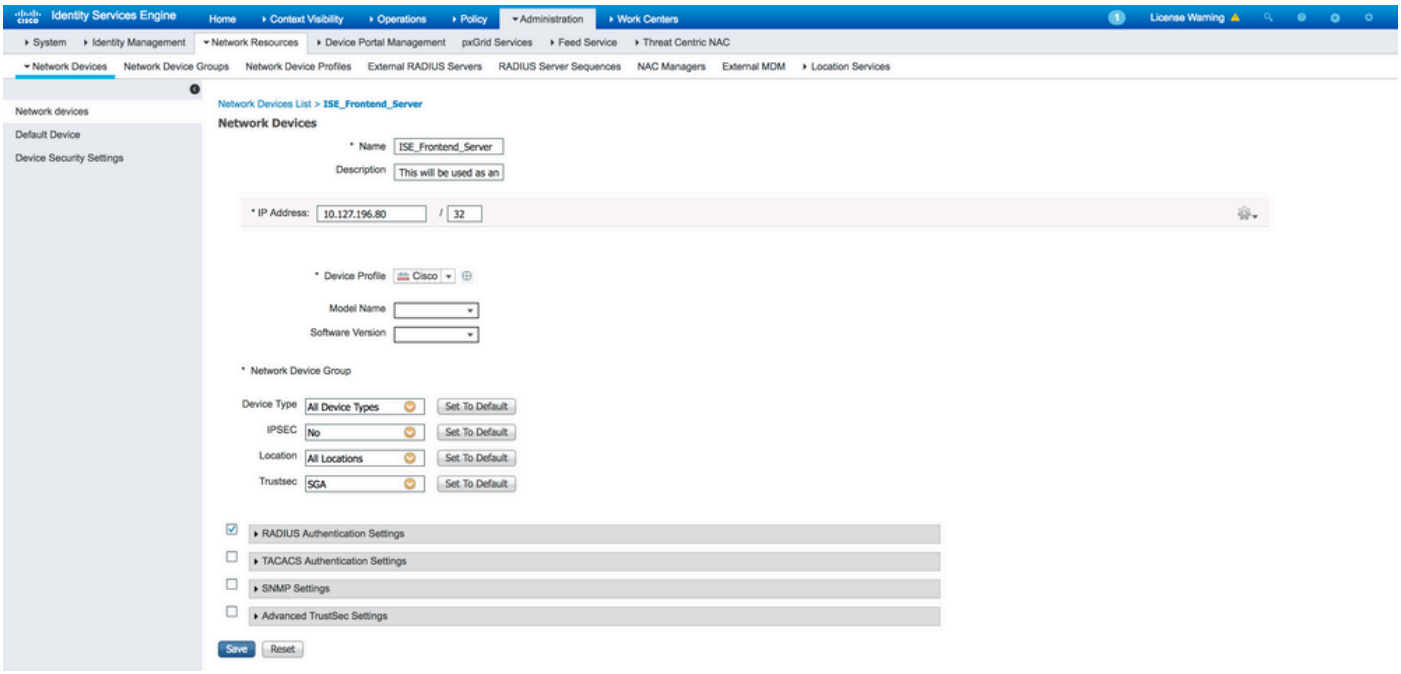
Étape 4. La partie suivante consiste à configurer les ensembles de stratégies afin d'utiliser la séquence de serveur RADIUS au lieu des protocoles autorisés afin que les demandes soient envoyées au serveur RADIUS externe. Il peut être configuré sous Policy > Policy Sets. Les stratégies d'autorisation peuvent être configurées sous Policy Set mais n'entrent en vigueur que si Continue to Authorization Policy on Access-

Accept est sélectionnée. Dans le cas contraire, ISE agit simplement en tant que proxy pour les requêtes RADIUS afin de correspondre aux conditions configurées pour cet ensemble de stratégies.

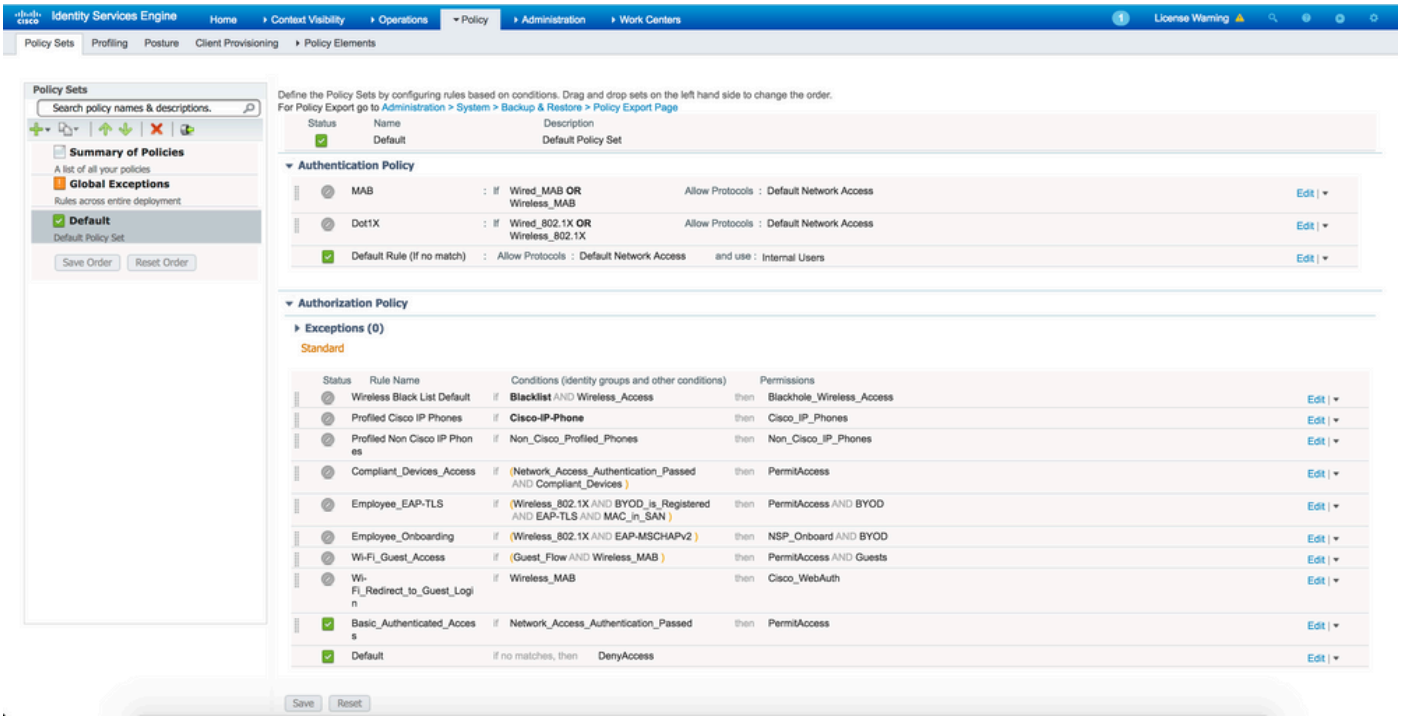


Configuration du serveur RADIUS externe

Étape 1. Dans cet exemple, un autre serveur ISE (version 2.2) est utilisé en tant que serveur RADIUS externe nommé ISE_Backend_Server. L'ISE (ISE_Frontend_Server) doit être configuré en tant que périphérique réseau ou traditionnellement appelé NAS dans le serveur RADIUS externe (ISE_Backend_Server dans cet exemple), puisque la NAS-IP-Address dans la requête d'accès qui est transmise au serveur RADIUS externe est remplacé par l'adresse IP duISE_Frontend_Server. Le secret partagé à configurer est le même que celui configuré pour le serveur RADIUS externe sur le ISE_Frontend_Server.



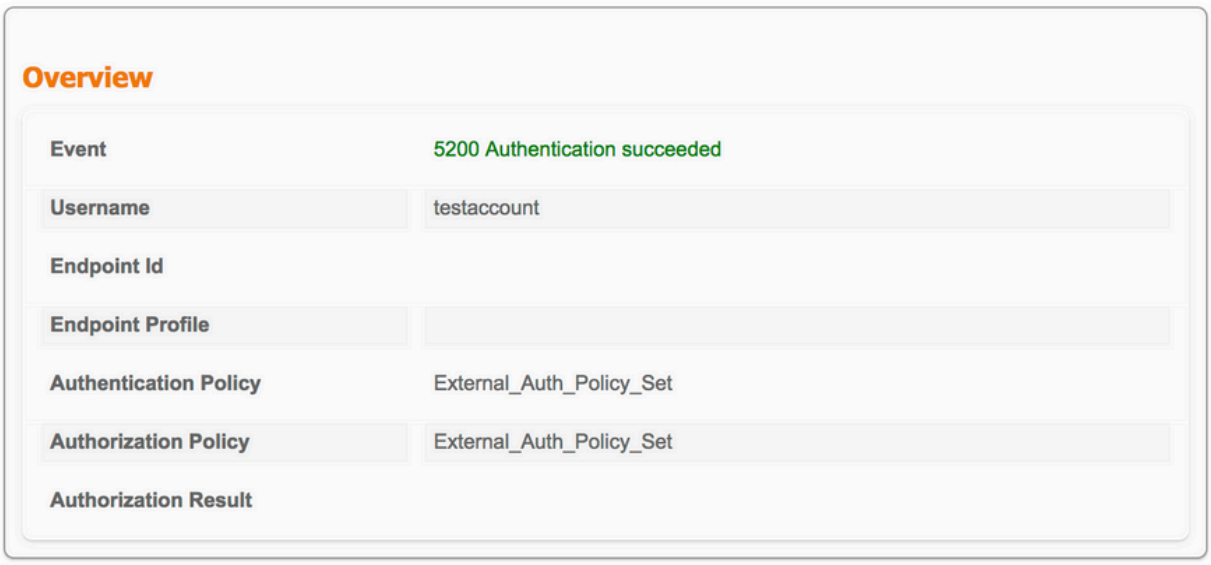
Étape 2. Le serveur RADIUS externe peut être configuré avec ses propres stratégies d'authentification et d'autorisation afin de servir les requêtes proxy par l'ISE. Dans cet exemple, une stratégie simple est configurée afin de vérifier l'utilisateur dans les utilisateurs internes, puis d'autoriser l'accès si authentifié.



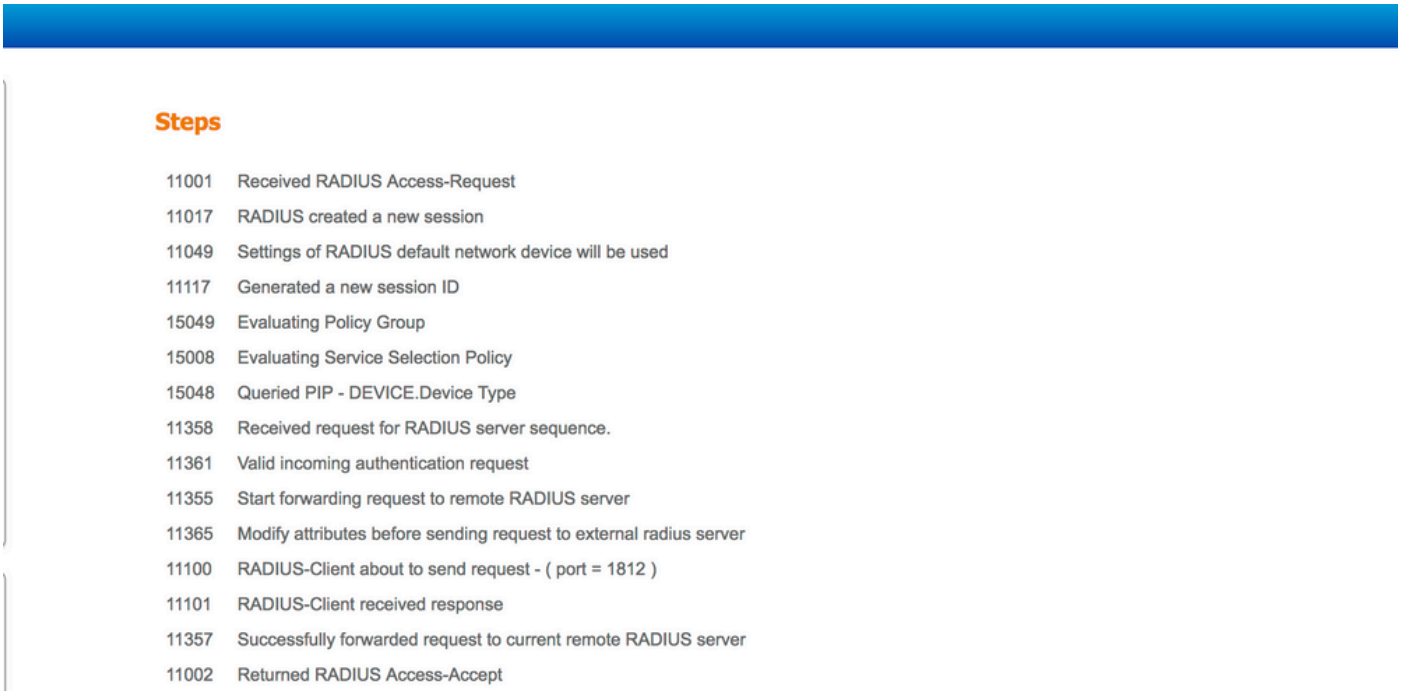
Vérifier

Étape 1. Vérifiez les journaux en direct ISE si la demande est reçue, comme indiqué dans l'image.

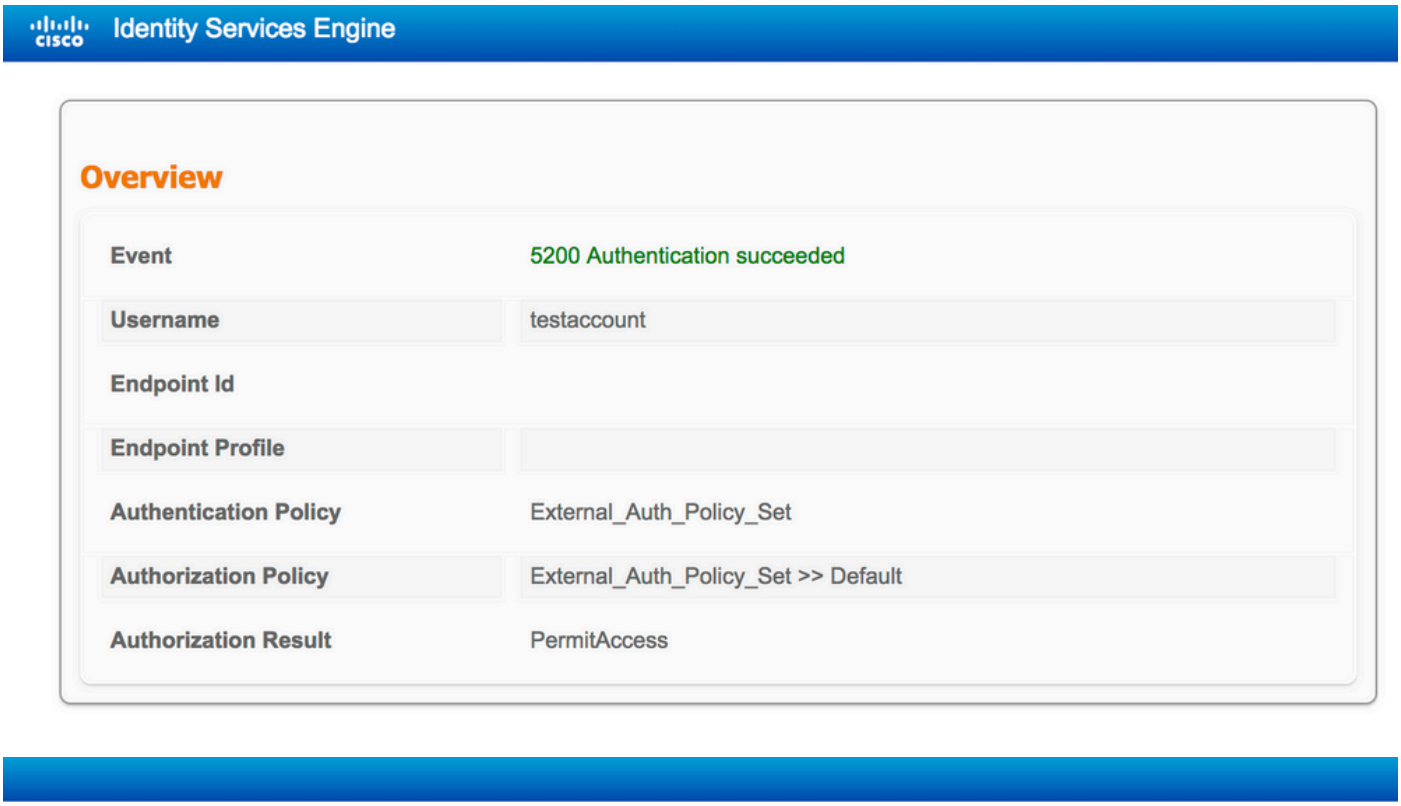
Étape 2. Vérifiez si le jeu de stratégies correct est sélectionné, comme illustré dans l'image.

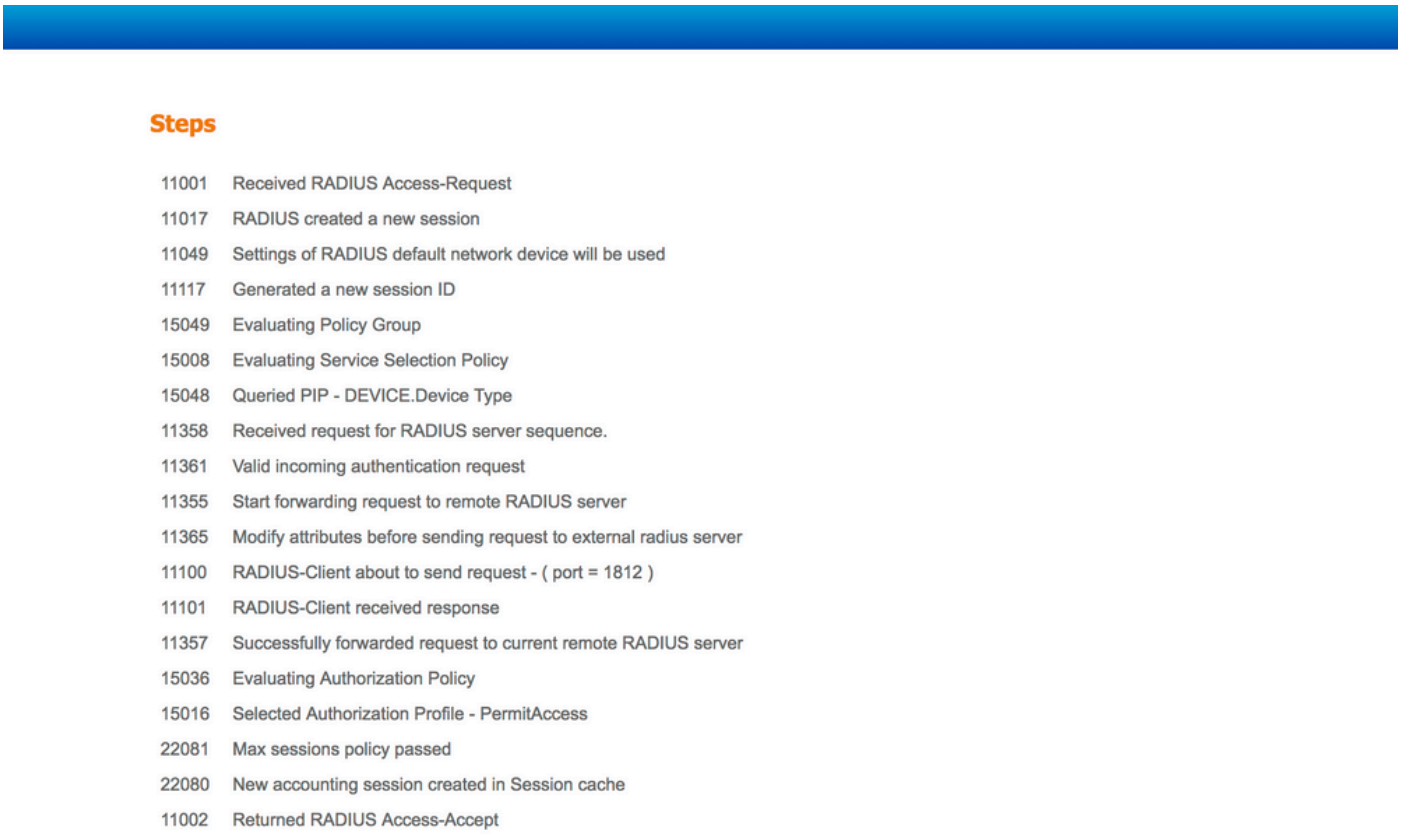


Étape 3. Vérifiez si la demande est transmise au serveur RADIUS externe.



4. Si la Continue to Authorization Policy on Access-Accept est sélectionnée, vérifiez si la stratégie d'autorisation est évaluée.





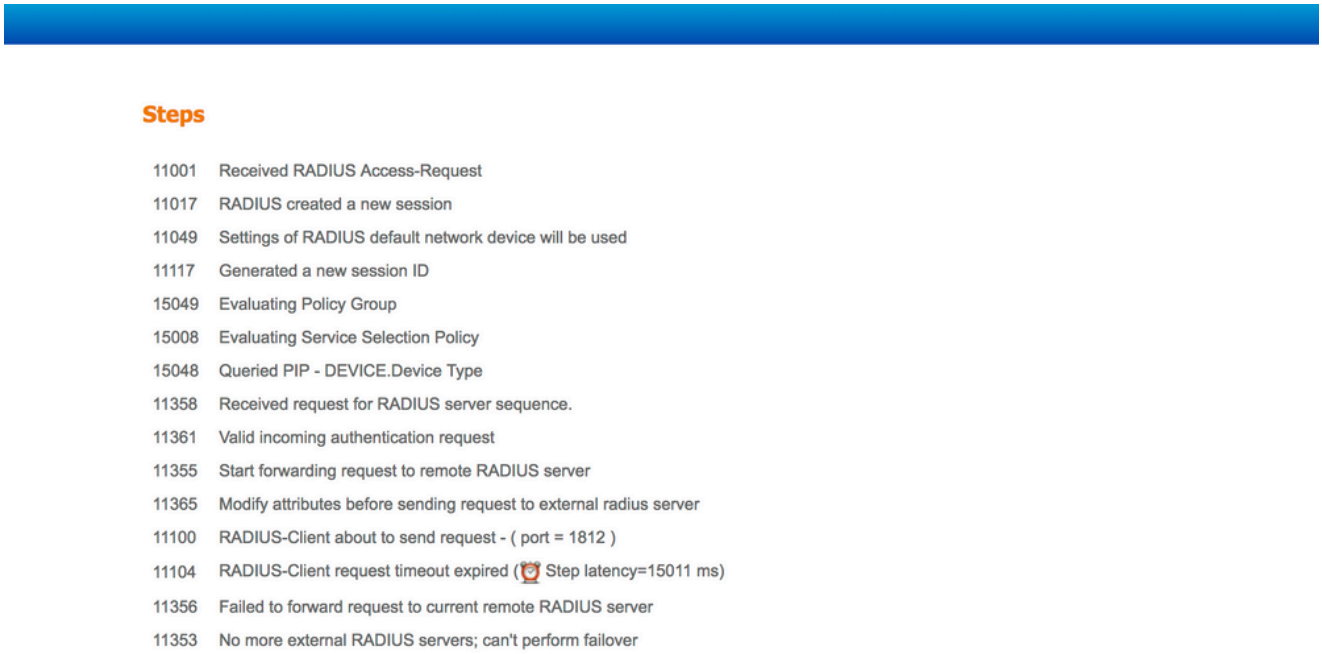
Dépannage

Scénario 1. Événement - Demande RADIUS 5405 abandonnée

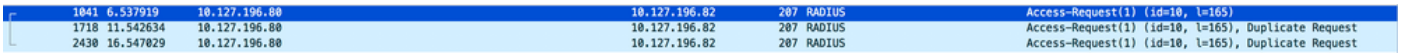
- La chose la plus importante qui doit être vérifiée est les étapes dans le rapport d'authentification détaillé. Si les étapes indiquent la RADIUS-Client request timeout expired, cela signifie que l'ISE n'a reçu aucune réponse du serveur RADIUS externe configuré. Cela peut se

produire lorsque :

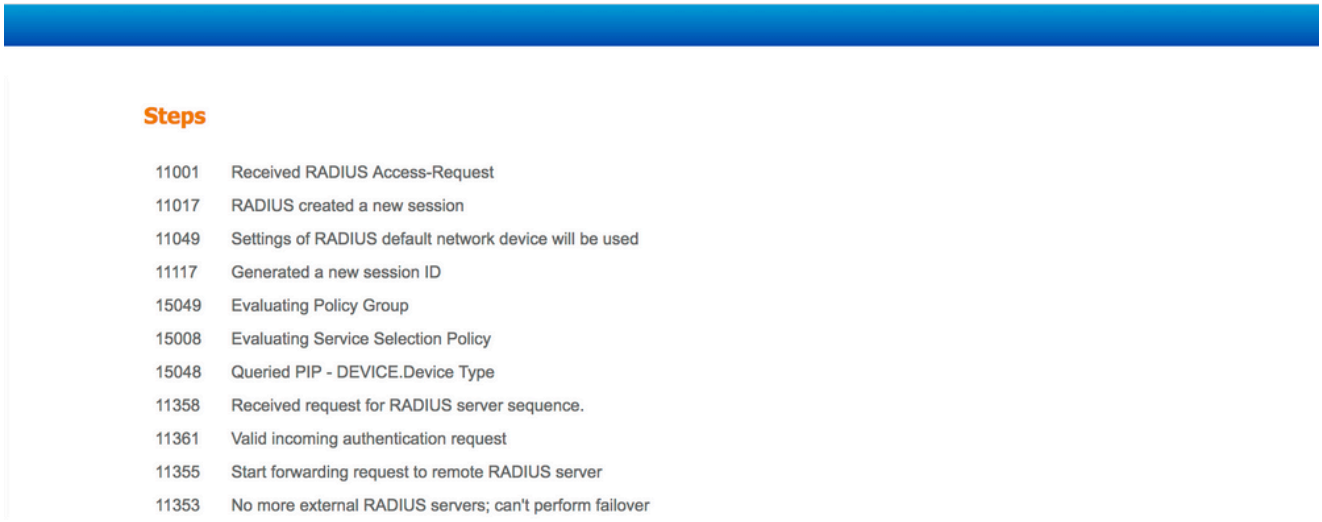
1. Il y a un problème de connectivité avec le serveur RADIUS externe. ISE ne parvient pas à atteindre le serveur RADIUS externe sur les ports configurés pour lui.
2. ISE n'est pas configuré en tant que périphérique réseau ou NAS sur le serveur RADIUS externe.
3. Les paquets sont abandonnés par le serveur RADIUS externe, soit par configuration, soit en raison d'un problème sur le serveur RADIUS externe.



Vérifiez également les captures de paquets afin de voir s'il ne s'agit pas d'un faux message, c'est-à-dire qu'ISE reçoit le paquet en retour du serveur mais signale quand même que la requête a expiré.



- Si les étapes indiquent Start forwarding request to remote RADIUS server et l'étape immédiate est No more external RADIUS servers; can't perform failover, cela signifie alors que tous les serveurs RADIUS externes configurés sont actuellement marqués comme morts et que les requêtes ne sont servies qu'après l'expiration du minuteur d'arrêt.

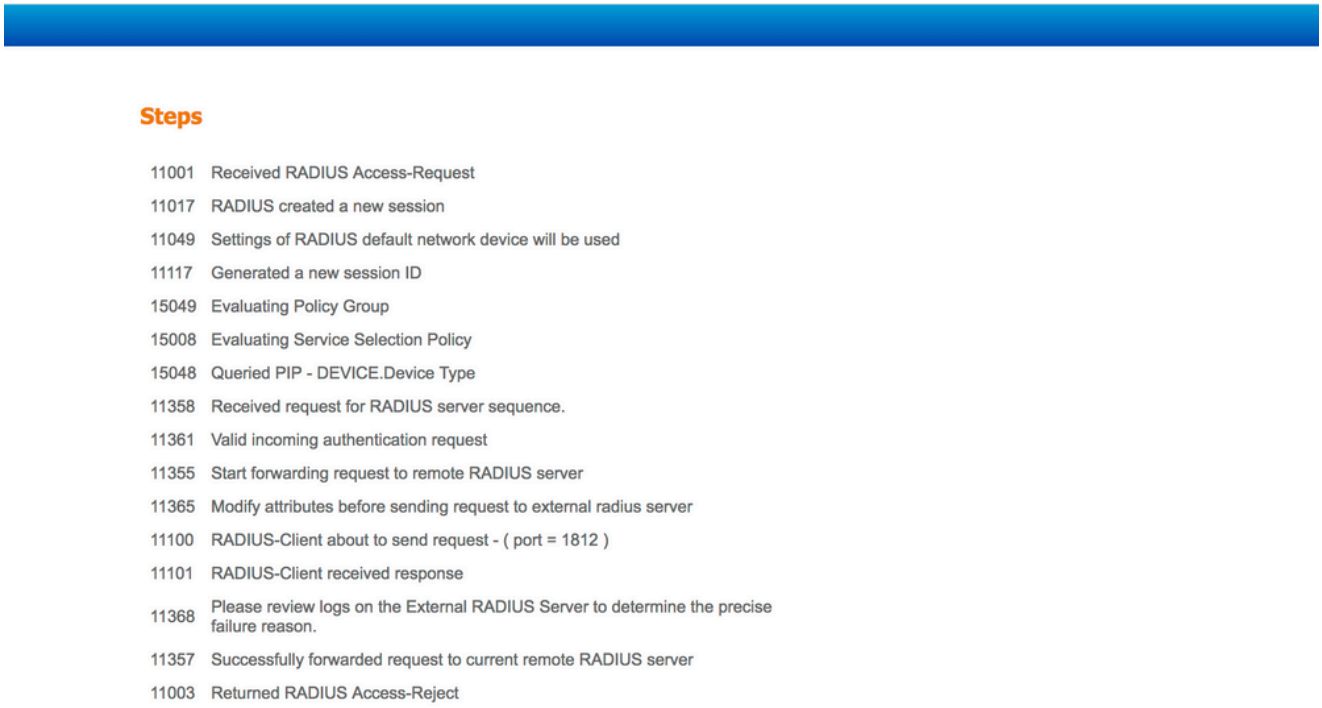


Remarque : le temps mort par défaut des serveurs RADIUS externes dans ISE est de 5 minutes. Cette valeur est codée en dur et ne peut pas être modifiée à partir de cette version.

- Si les étapes indiquent RADIUS-Client encountered error during processing flow et sont suivis de Failed to forward request to current remote RADIUS server; an invalid response was received,cela signifie alors qu'ISE a rencontré un problème lors du transfert de la requête au serveur RADIUS externe. Cela se produit généralement lorsque la requête RADIUS envoyée par le périphérique réseau/NAS à l'ISE ne dispose pas de NAS-IP-Address comme l'un des attributs. S'il n'y a NAS-IP-Address et si les serveurs RADIUS externes ne sont pas utilisés, ISE renseigne le NAS-IP-Address avec l'adresse IP source du paquet. Toutefois, cela ne s'applique pas lorsqu'un serveur RADIUS externe est en cours d'utilisation.

Scénario 2. Événement - Échec de l'authentification 5400

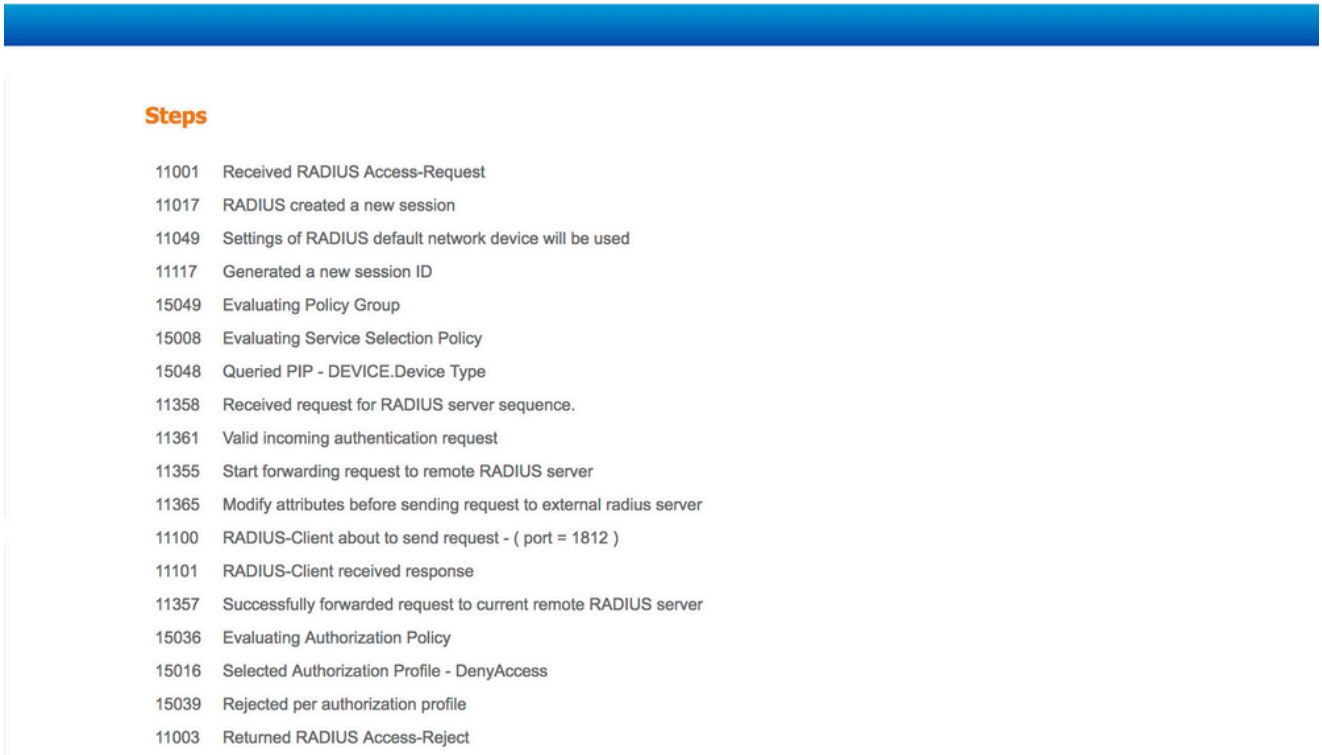
- Dans ce cas, si les étapes indiquent 11368 Please review logs on the External RADIUS Server to determine the precise failure reason, cela signifie que l'authentification a échoué sur le serveur RADIUS externe lui-même et qu'il a envoyé un refus d'accès.



Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11049	Settings of RADIUS default network device will be used
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - DEVICE.Device Type
11358	Received request for RADIUS server sequence.
11361	Valid incoming authentication request
11355	Start forwarding request to remote RADIUS server
11365	Modify attributes before sending request to external radius server
11100	RADIUS-Client about to send request - (port = 1812)
11101	RADIUS-Client received response
11368	Please review logs on the External RADIUS Server to determine the precise failure reason.
11357	Successfully forwarded request to current remote RADIUS server
11003	Returned RADIUS Access-Reject

- Si les étapes indiquent 15039 Rejected per authorization profile, cela signifie qu'ISE a reçu un Access-Accept du serveur RADIUS externe, mais qu'ISE rejette l'autorisation en fonction des stratégies d'autorisation configurées.



Steps

11001	Received RADIUS Access-Request
11017	RADIUS created a new session
11049	Settings of RADIUS default network device will be used
11117	Generated a new session ID
15049	Evaluating Policy Group
15008	Evaluating Service Selection Policy
15048	Queried PIP - DEVICE.Device Type
11358	Received request for RADIUS server sequence.
11361	Valid incoming authentication request
11355	Start forwarding request to remote RADIUS server
11365	Modify attributes before sending request to external radius server
11100	RADIUS-Client about to send request - (port = 1812)
11101	RADIUS-Client received response
11357	Successfully forwarded request to current remote RADIUS server
15036	Evaluating Authorization Policy
15016	Selected Authorization Profile - DenyAccess
15039	Rejected per authorization profile
11003	Returned RADIUS Access-Reject

- Si la Failure Reason sur l'ISE est autre chose que ceux mentionnés ici en cas d'échec d'authentification, alors il peut signifier un problème potentiel avec la configuration ou avec l'ISE elle-même. Il est recommandé d'ouvrir un dossier TAC à ce stade.

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.