

Configuration du flux d'autorisation pour les sessions d'ID passives dans ISE 3.2

Table des matières

[Introduction](#)

[Informations générales](#)

[Conditions préalables](#)

[Exigences](#)

[Composants utilisés](#)

[Configuration](#)

[Vérifier](#)

[Dépannage](#)

Introduction

Ce document décrit comment configurer les règles d'autorisation pour les événements d'ID passif afin d'attribuer des SGT aux sessions.

Informations générales

Les services d'identité passive (ID passive) n'authentifient pas les utilisateurs directement, mais collectent les identités des utilisateurs et les adresses IP à partir de serveurs d'authentification externes tels qu'Active Directory (AD), appelés fournisseurs, puis partagent ces informations avec les abonnés.

ISE 3.2 introduit une nouvelle fonctionnalité qui vous permet de configurer une stratégie d'autorisation pour attribuer une balise de groupe de sécurité (SGT) à un utilisateur en fonction de l'appartenance au groupe Active Directory.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Cisco ISE 3.X
- Intégration passive d'ID avec tout fournisseur
- Administration Active Directory (AD)
- Segmentation (Trustsec)
- PxGrid (Platform Exchange Grid)

Composants utilisés

- Logiciel Identity Service Engine (ISE) version 3.2

- Microsoft Active Directory
- SYSLOG

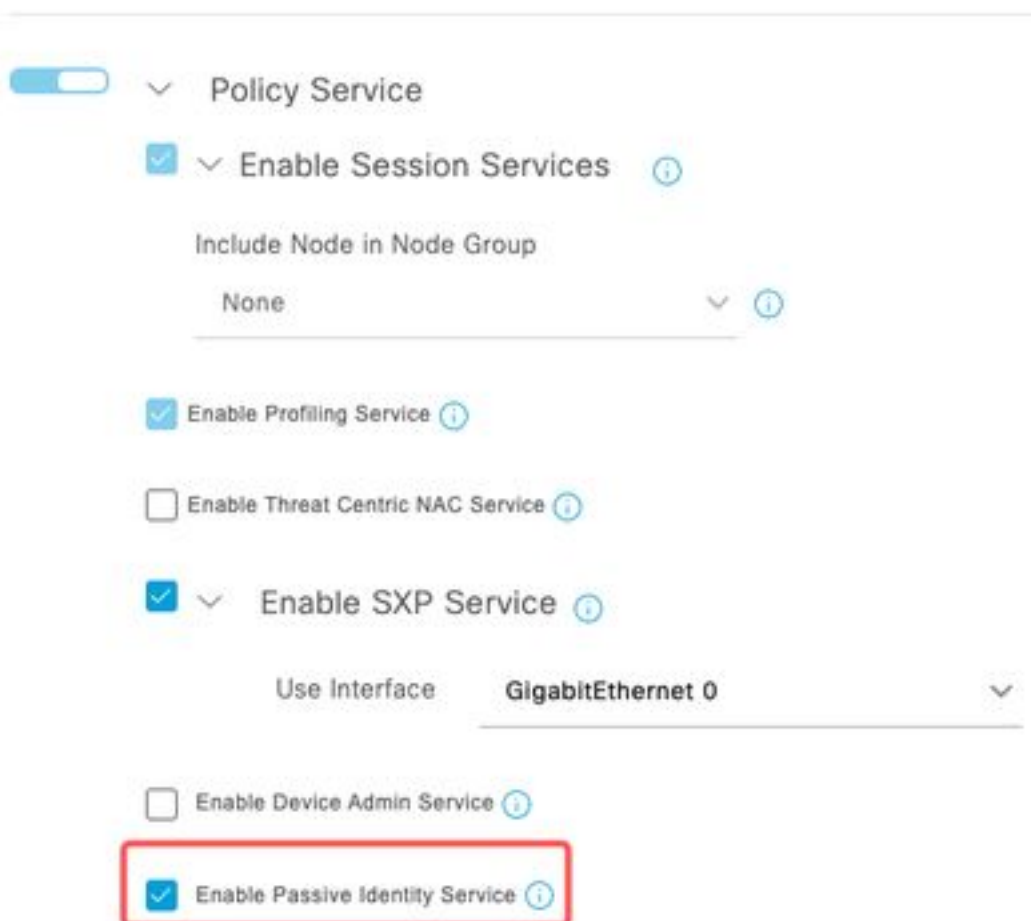
The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Configuration

Étape 1. Activez les services ISE.

1. Sur ISE, accédez à Administration > **Deployment**, choisissez le noeud ISE et cliquez sur **Edit**, activez **Policy Service** et sélectionnez **Enable Passive Identity Service**. Facultatif, vous pouvez activer SXP et PxGrid si les sessions d'ID passives doivent être publiées via chacune d'elles. Cliquez sur Save.

Avertissement : les détails SGT des utilisateurs de connexion PassiveID authentifiés par le fournisseur d'API ne peuvent pas être publiés dans SXP. Cependant, les détails SGT de ces utilisateurs peuvent être publiés via pxGrid et pxGrid Cloud.





Services activés


Étape 2. Configurez Active Directory.


1. Accédez à Administration > **Identity Management** > **External Identity Sources** et choisissez **Active directory** puis cliquez sur le bouton **Add**.
2. Saisissez le **nom du point de jonction** et le **domaine Active Directory**. Cliquez sur **Submit**.

Identities Groups **External Identity Sources** Identity Source Sequences

External Identity Sources

<  

>  Certificate Authentication F

 Active Directory

Connection

* Join Point Name **aaamexrub**

* Active Directory Domain **aaamexrub.com**

Ajouter Active Directory

3. Une fenêtre contextuelle apparaît pour joindre ISE à AD. Cliquez sur Yes. Saisissez le nom d'utilisateur et mot de passe. Click OK.



Information

Would you like to Join all ISE Nodes to this Active Directory Domain?

No **Yes**

Continuer à rejoindre

Join Domain

Please specify the credentials required to Join ISE node(s) to the Active Directory Domain.

* AD User Name  **user**

* Password *****

Specify Organizational Unit 

Store Credentials 

Cancel **OK**

ISE
Directory

Rejoindre Active

4. Récupérez les groupes AD. Accédez à **Groups**, cliquez sur **Add**, puis cliquez sur **Retrieve Groups** et choisissez tous les groupes intéressés et cliquez sur **OK**.

Select Directory Groups

This dialog is used to select groups from the Directory.

Domain: aaamexrub.com

Name Filter: _____ SID Filter: _____ Type Filter: All

[Retrieve Groups...](#) 53 Groups Retrieved.

<input type="checkbox"/>	aaamexrub.com/Users/Cloneable Domain Contro...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Denied RODC Password ...	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
<input type="checkbox"/>	aaamexrub.com/Users/DnsAdmins	S-1-5-21-144182218-1144227253-205214604...	DOMAIN LOCAL
<input type="checkbox"/>	aaamexrub.com/Users/DnsUpdateProxy	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input checked="" type="checkbox"/>	aaamexrub.com/Users/Domain Admins	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Computers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Controllers	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Domain Guests	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input checked="" type="checkbox"/>	aaamexrub.com/Users/Domain Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Enterprise Admins	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
<input type="checkbox"/>	aaamexrub.com/Users/Enterprise Read-only De...	S-1-5-21-144182218-1144227253-205214604...	UNIVERSAL
<input type="checkbox"/>	aaamexrub.com/Users/Group Policy Creator Ow...	S-1-5-21-144182218-1144227253-205214604...	GLOBAL
<input type="checkbox"/>	aaamexrub.com/Users/Protected Users	S-1-5-21-144182218-1144227253-205214604...	GLOBAL

[Cancel](#) [OK](#)

Récupérer les groupes AD

Connection Allowed Domains PassiveID **Groups**

[Edit](#) [+ Add](#) [Delete Group](#) [Update SID Values](#)

<input type="checkbox"/>	Name	S
<input type="checkbox"/>	aaamexrub.com/Users/Domain Admins	S
<input type="checkbox"/>	aaamexrub.com/Users/Domain Users	S
<input type="checkbox"/>	aaamexrub.com/Users/sponsors	S

Groupes récupérés

5. Activez le flux d'autorisation. Accédez à **Advanced Settings** et dans la section **PassiveID Settings**, cochez la case **Authorization Flow**. Cliquez sur Save.

PassiveID Settings

The PassiveID settings that are configured in this section are applied to all the join points in Cisco ISE.

History interval*	10
Domain Controller event inactivity time* (monitored by Agent)	0
Latency interval of events from agent*	0
User session aging time*	24

Authorization Flow ⓘ

Activer le flux d'autorisation

Étape 3. Configurer le fournisseur Syslog

1. Accédez à Work Centers > **PassiveID** > **Providers**, choisissez **Syslog Providers**, cliquez sur **Add** et complétez les informations. Cliquez sur Save (enregistrer)

Attention : dans ce cas, ISE reçoit le message syslog d'une connexion VPN réussie dans un ASA, mais ce document ne décrit pas cette configuration.

Syslog Providers

Name*
ASA

Description


Status*
Enabled

Host FQDN*
asa-rudelave.aaamexrub.com

Connection Type*
UDP - Port 40514

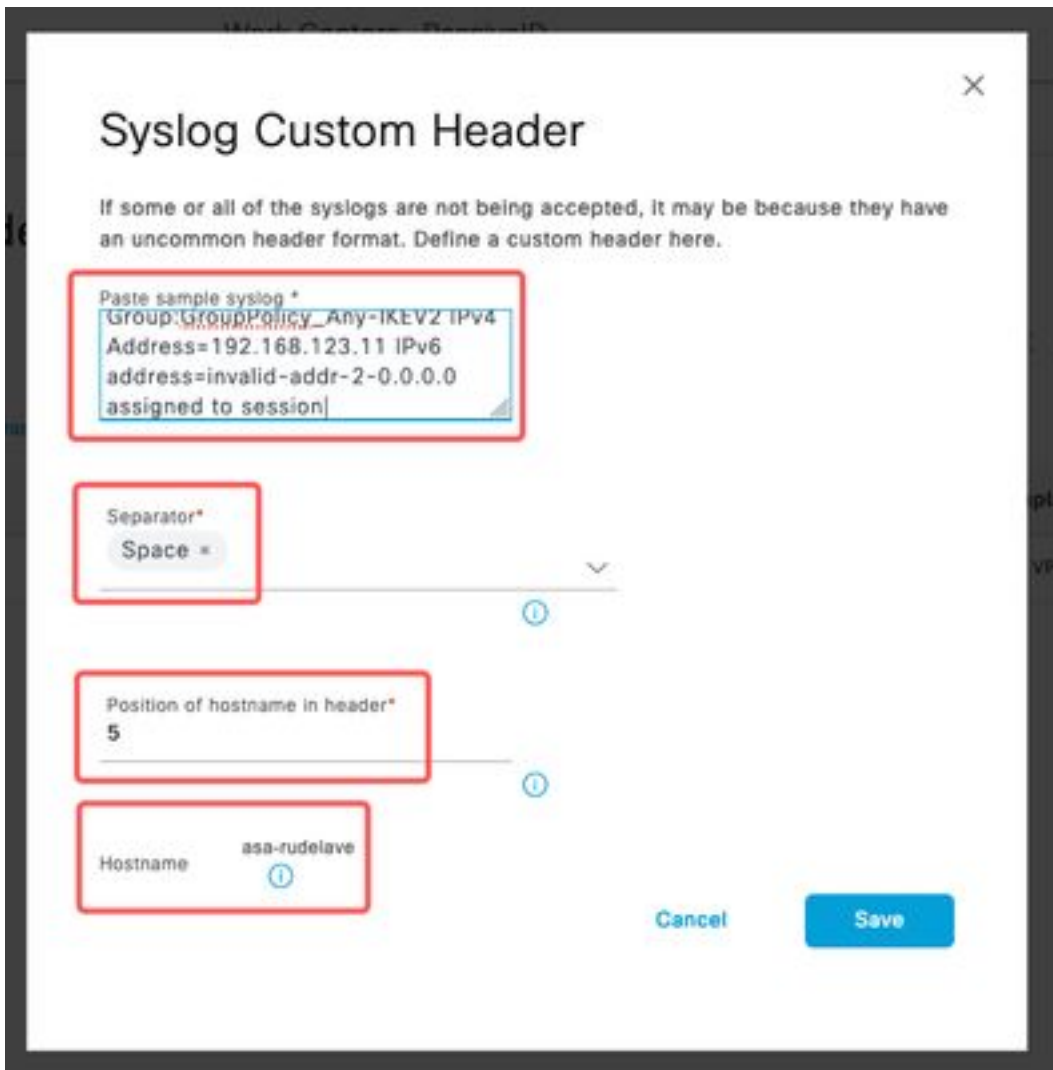
Template* ASA VPN [View](#) [New](#)

Default Domain
aaamexrub.com



Configurer le fournisseur Syslog

2. Cliquez sur **En-tête personnalisé**. Collez l'exemple de syslog et utilisez un séparateur ou une tabulation pour trouver le nom d'hôte du périphérique. S'il est correct, le nom d'hôte apparaît. Cliquez sur Save (enregistrer)

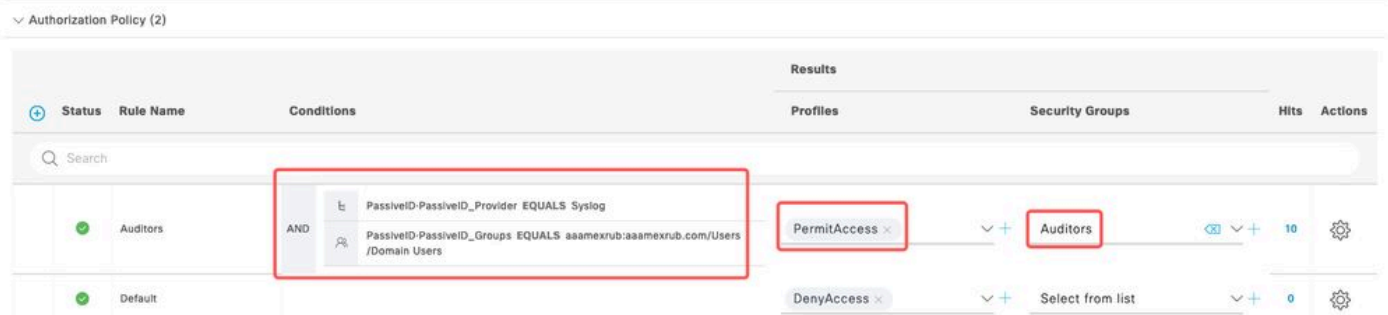


Configurer un en-tête

personnalisé

Étape 4. Configurer les règles d'autorisation

1. Rendez-vous à Policy > Policy Sets (Politique > Ensembles de politiques). Dans ce cas, il utilise la stratégie par défaut. Cliquez sur la stratégie **par défaut**. Dans la **Stratégie d'autorisation**, ajoutez une nouvelle règle. Dans les politiques PassiveID, ISE a tous les fournisseurs. Vous pouvez combiner celui-ci avec un groupe PassiveID. Choisissez **Permit Access** as Profile, et dans **Security Groups** choisissez le SGT dont vous avez besoin.



Configurer les règles d'autorisation

Vérifier

Une fois qu'ISE reçoit le Syslog, vous pouvez vérifier les journaux Radius Live pour voir le flux d'autorisation. Accédez à **Operations > Radius > Live logs**.

Dans les journaux, vous pouvez voir l'événement Authorization. Celui-ci contient le nom d'utilisateur, la stratégie d'autorisation et la balise de groupe de sécurité qui lui sont associés.

Reset Repeat Counts Export To

Time	Status	Details	Repea...	Identity	Endpoint ID	Authenticatio...	Authorization Policy	Authorization ...	Security ...	IP Address
Jan 31, ...			0	test	192.168.123.10	PassiveID provider	PassiveID provider >> Auditors	PermitAccess	Auditors	192.168.123.10
Jan 31, ...				test	192.168.123.10	PassiveID provider	PassiveID provider >> Auditors	PermitAccess		192.168.123.10

Journal Radius Live

Pour vérifier plus de détails, cliquez sur le **rapport détaillé**. Ici, vous pouvez voir le flux Authorize-Only qui évalue les stratégies pour attribuer le SGT.

Overview

Event: **5236 Authorize-Only succeeded**

Username: test

Endpoint Id: 192.168.123.10

Endpoint Profile:

Authentication Policy: PassiveID provider

Authorization Policy: PassiveID provider >> Auditors

Authorization Result: PermitAccess

Steps

15041 Evaluating Identity Policy

15013 Selected Identity Source - All_AD_Join_Points

24432 Looking up user in Active Directory - All_AD_Join_Points

24325 Resolving identity - test@aaamexrub.com

24313 Search for matching accounts at join point - aaamexrub.com

24319 Single matching account found in forest - aaamexrub.com

24323 Identity resolution detected single matching account

24355 LDAP fetch succeeded - aaamexrub.com

24416 User's Groups retrieval from Active Directory succeeded - All_AD_Join_Points

22037 Authentication Passed

90506 Running Authorize Only Flow for Passive ID - Provider Syslog

15049 Evaluating Policy Group

15008 Evaluating Service Selection Policy

15036 Evaluating Authorization Policy

90500 New Identity Mapping

5236 Authorize-Only succeeded

Authentication Details

Source Timestamp: 2023-01-31 16:15:04.507

Received Timestamp: 2023-01-31 16:15:04.507

Policy Server: asc-ise32-726

Event: **5236 Authorize-Only succeeded**

Username: test

Endpoint Id: 192.168.123.10

Calling Station Id: 192.168.123.10

IPv4 Address: 192.168.123.10

Authorization Profile: PermitAccess

Rapport du journal Radius Live

Dépannage

Dans ce cas, il utilise deux flux : les sessions passiveID et le flux Authorization. Pour activer les débogages, accédez à **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration**, puis choisissez le noeud ISE.

Pour l'ID passif, activez les composants suivants au niveau **DEBUG** :

- ID passif

Pour vérifier les journaux, en fonction du fournisseur d'ID passif, le fichier à vérifier pour ce scénario, vous devez examiner le **fichier** passiveid-syslog.log, pour les autres fournisseurs :

- passiveid-agent.log

- passiveid-api.log
- passiveid-endpoint.log
- passiveid-span.log
- phlébotome passif

Pour le flux d'autorisation, activez les composants suivants au niveau **DEBUG** :

- moteur politique
- port-JNI

Exemple :

The screenshot shows the 'Debug Wizard' interface with the 'Debug Level Configuration' section active. The configuration is for the node 'asc-ise32-726.aamexrub.com'. A search filter 'debug' is applied. Three components are listed with their log levels set to 'DEBUG' and their corresponding log file names:

Component Name	Log Level	Description	Log file Name
<input type="radio"/> PassiveID	DEBUG	PassiveID events and messages	passiveid-wmi.log
<input type="radio"/> policy-engine	DEBUG	Policy Engine 2.0 related messages	ise-psc.log
<input type="radio"/> prrt-JNI	DEBUG	prrt policy decision request processing layer related ...	prrt-management.log

Débogages activés

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.