

Configurare il flusso di autorizzazione per le sessioni ID passive in ISE 3.2

Sommario

[Introduzione](#)

[Premesse](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Verifica](#)

[Risoluzione dei problemi](#)

Introduzione

In questo documento viene descritto come configurare le regole di autorizzazione per gli eventi di ID passivo per assegnare i servizi SGT alle sessioni.

Premesse

I servizi di identità passiva (ID passivo) non autenticano direttamente gli utenti, ma raccolgono le identità e gli indirizzi IP degli utenti dai server di autenticazione esterni, ad esempio Active Directory (AD), noti come provider, e quindi condividono tali informazioni con i sottoscrittori.

ISE 3.2 introduce una nuova funzionalità che consente di configurare un criterio di autorizzazione per assegnare un tag del gruppo di sicurezza (SGT) a un utente in base all'appartenenza al gruppo Active Directory.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Cisco ISE 3.X
- Integrazione passiva di ID con qualsiasi provider
- Amministrazione di Active Directory (AD)
- Segmentazione (Trustsec)
- PxGrid (griglia di scambio piattaforma)

Componenti usati

- Software Identity Service Engine (ISE) versione 3.2
- Microsoft Active Directory

- Syslog

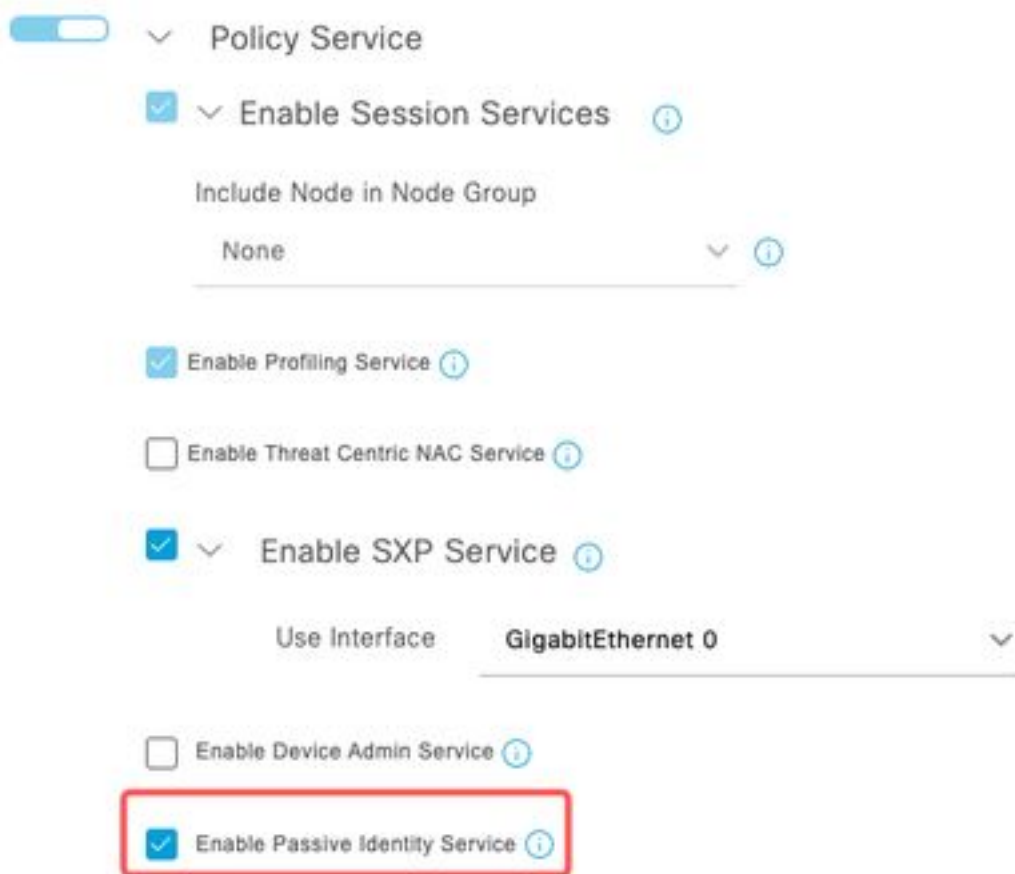
Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze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

Configurazione

Passaggio 1. Abilitare i servizi ISE.

1. Su ISE, selezionare Amministrazione > **Distribuzione**, scegliere il nodo ISE e fare clic su **Modifica**, abilita **Policy Service** e scegliere **Abilita Passive Identity Service**. Facoltativamente, è possibile abilitare SXP e PxGrid se le sessioni di ID passivo devono essere pubblicate tramite ognuna di esse. Fare clic su **Salva**.

Avviso: impossibile pubblicare in SXP i dettagli SGT degli utenti di accesso con ID passivo autenticati dal provider API. Tuttavia, i dettagli SGT di questi utenti possono essere pubblicati attraverso pxGrid e pxGrid Cloud.



Passaggio 2. Configurare Active Directory.

1. Passare a Amministrazione > **Gestione identità** > **Origini identità esterne** e scegliere **Active Directory**, quindi fare clic sul **pulsante Aggiungi**.
2. Immettere il **nome del punto di join** e il **dominio di Active Directory**. Fare clic su **Invia**.

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**

Aggiungi Active Directory

3. Viene visualizzata una schermata di popup per unire ISE ad AD. Fare clic su **Sì**. Immettere il **nome utente** e la **password**. Fare clic su **OK**.

Information

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

No **Yes**

Partecipate anche voi ad

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 *Aggiungi ad Active*

4. Recuperare i gruppi AD. Passare a **Gruppi**, fare clic su **Aggiungi**, quindi su **Recupera gruppi** e scegliere tutti i gruppi interessati, quindi fare clic su **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](#)

Recupera gruppi 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

Gruppi recuperati

5. Abilitare il flusso di autorizzazione. Passare a **Impostazioni avanzate** e nella sezione **Impostazioni ID passivo** selezionare la casella di controllo **Flusso di autorizzazione**. Fare clic su **Salva**.

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 ⓘ

Abilita flusso di autorizzazione

Passaggio 3. Configurare il provider Syslog.

1. Passare a Centri di lavoro > **ID passivo** > **Provider**, scegliere **Provider di syslog**, fare clic su **Aggiungi** e completare le informazioni. Fare clic su **Salva**.

Attenzione: in questo caso, ISE riceve il messaggio syslog da una connessione VPN riuscita in un'appliance ASA, ma questo documento non descrive la configurazione.

Syslog Providers

Name*
ASA

Description


Status*
Enabled

Host FQDN*
asa-rudelave.aaamexrub.com

Connection Type*
UDP - Port 40514

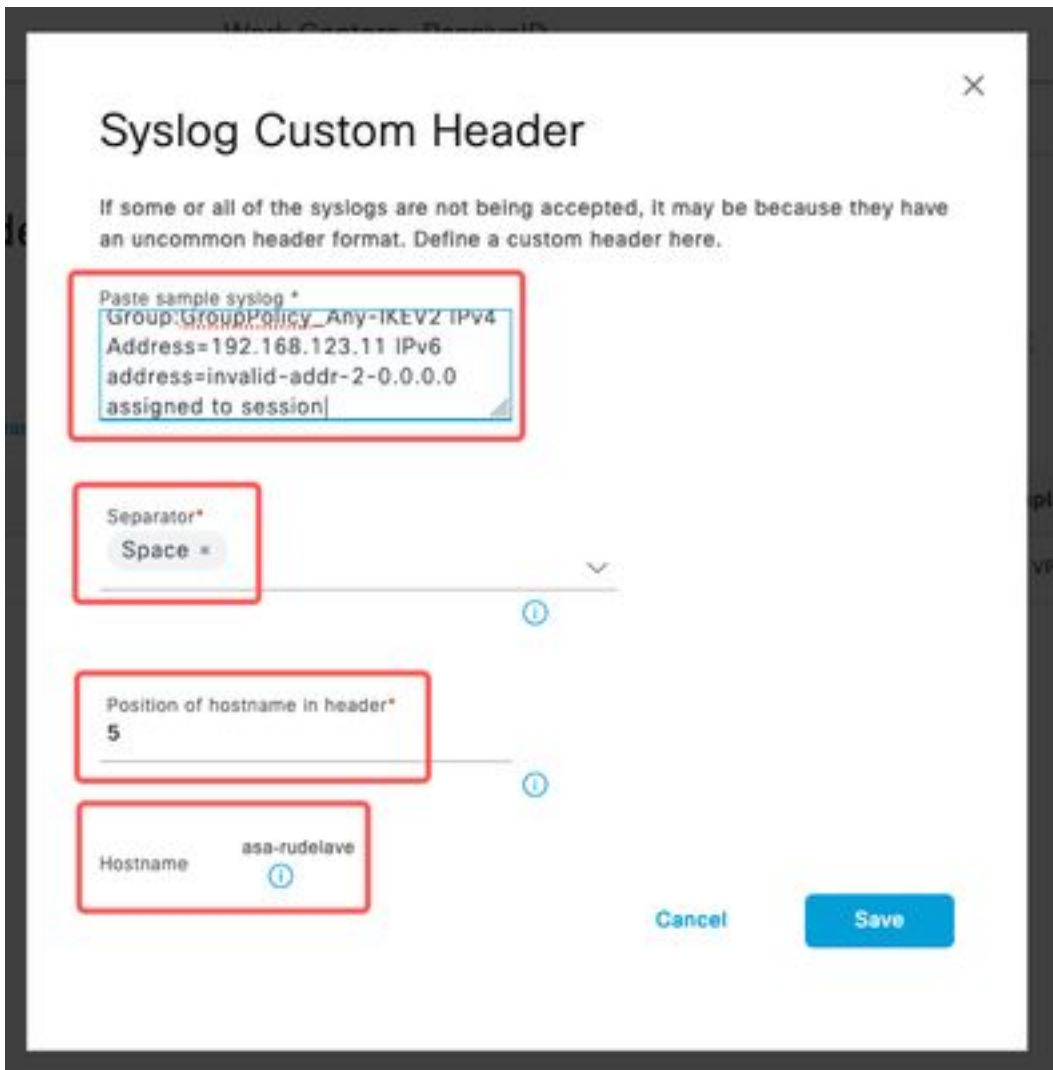
Template* ASA VPN [View](#) [New](#)

Default Domain
aaamexrub.com



Configura provider Syslog

2. Fare clic su **Intestazione personalizzata**. Incollare il syslog di esempio e utilizzare un separatore o una tabulazione per trovare il nome host del dispositivo. Se è corretto, viene visualizzato il nome host. Fare clic su Salva.

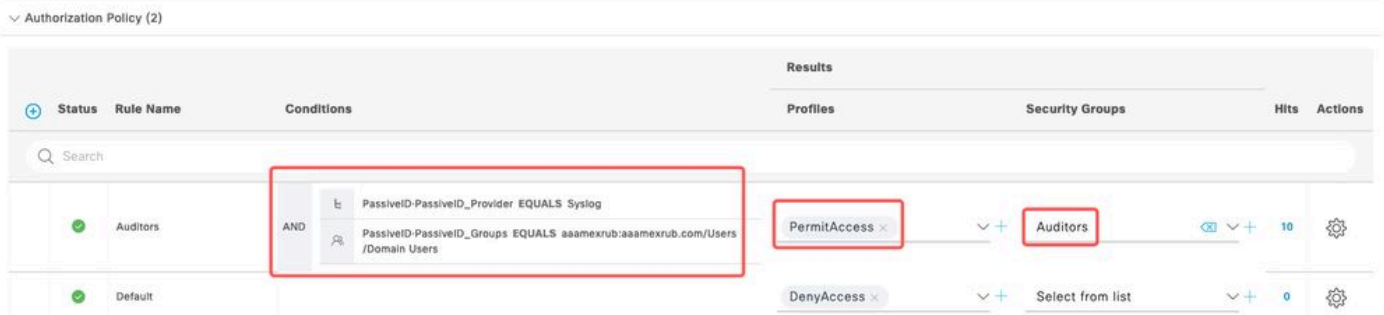


Configura intestazione

personalizzata

Passaggio 4. Configurazione delle regole di autorizzazione

1. Passare a **Criterio > Set di criteri**. In questo caso, viene utilizzato il criterio Predefinito. Fare clic sul criterio **Predefinito**. Nel **criterio di autorizzazione** aggiungere una nuova regola. Nelle policy PassiveID, ISE ha tutti i provider. È possibile combinare questo gruppo con un gruppo PassiveID. Scegliere **Permit Access as Profile** (Consenti accesso come profilo) e in **Security Groups (Gruppi di sicurezza)** scegliere il tipo di servizio desiderato.



Configurazione delle regole di autorizzazione

Verifica

Una volta che ISE ha ricevuto il syslog, è possibile controllare i log di Radius Live per verificare il flusso di autorizzazione. Passare a **Operazioni > Raggio > Log attivi**.

Nei registri è possibile visualizzare l'evento Authorization. Questo contiene il nome utente, il criterio di autorizzazione e il tag del gruppo di sicurezza associati.

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

Registro Radius Live

Per controllare ulteriori dettagli, fare clic sul **report dettagliato**. Qui è possibile vedere il flusso di sola autorizzazione che valuta i criteri per assegnare il 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

Report registro Radius Live

Risoluzione dei problemi

In questo caso, vengono utilizzati due flussi, ovvero le sessioni passiveID e il flusso di autorizzazione. Per abilitare i debug, selezionare **Operations > Troubleshoot > Debug Wizard > Debug Log Configuration**, quindi scegliere il nodo ISE.

Per l'ID passivo, abilitare i componenti successivi al livello **DEBUG**:

- ID passivo

Per controllare i registri, in base al provider di ID passivo, il file da controllare per questo scenario, è necessario rivedere il file **passiveid-syslog.log** per gli altri provider:

- passiveid-agent.log

- passiveid-api.log
- passiveid-endpoint.log
- passiveid-span.log
- passiveid-wmilog

Per il flusso di autorizzazione, abilitare i componenti successivi al livello **DEBUG**:

- motore delle regole
- prrt-JNI

Esempio:

The screenshot shows the 'Debug Wizard' interface for a node named 'asc-ise32-726.aamexrub.com'. The 'Debug Level Configuration' section is active, showing a table of components and their log levels. The log level is set to 'debug'. Three components are listed: 'PassiveID', 'policy-engine', and 'prrt-JNI', all with a log level of 'DEBUG'. The log file names for these components are 'passiveid-wmi.log', 'ise-psc.log', and 'prrt-management.log' respectively. The log file names are highlighted with red boxes in the original image.

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

Debug abilitati

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).