

Configurare ASR9K TACACS con Cisco Identity Services Engine 2.4

Sommario

[Introduzione](#)

[Premesse](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Componenti predefiniti di IOS® XR](#)

[Gruppi di utenti predefiniti](#)

[Gruppi di task predefiniti](#)

[Gruppi di task definiti dall'utente](#)

[Configurazione AAA sul router](#)

[Configurazione server ISE](#)

[Verifica](#)

[Operatore](#)

[Operatore con AAA](#)

[Sysadmin](#)

[Root-System](#)

[Risoluzione dei problemi](#)

Introduzione

Questo documento descrive la configurazione di ASR serie 9000 Aggregation Services Router (ASR) per l'autenticazione e l'autorizzazione tramite TACACS+ con il server Cisco Identity Services Engine 2.4.

Premesse

Illustra l'implementazione del modello amministrativo di autorizzazione basata su attività utilizzato per controllare l'accesso degli utenti al sistema software Cisco IOS® XR. Le attività principali necessarie per implementare l'autorizzazione basata su attività riguardano la configurazione dei gruppi di utenti e dei gruppi di attività. I gruppi di utenti e i gruppi di attività vengono configurati tramite il set di comandi del software Cisco IOS® XR utilizzato per i servizi di autenticazione, autorizzazione e accounting (AAA). I comandi di autenticazione vengono utilizzati per verificare l'identità di un utente o di un'entità. I comandi di autorizzazione vengono utilizzati per verificare che a un utente autenticato (o entità) venga concessa l'autorizzazione per eseguire un'attività specifica. I comandi di accounting vengono utilizzati per registrare le sessioni e per creare un riepilogo di controllo registrando determinate azioni generate dall'utente o dal sistema.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Installazione di ASR 9000 e configurazione base
- Protocollo TACACS+
- Installazione e configurazione di ISE 2.4

Componenti usati

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

- ASR 9000 con software Cisco IOS® XR, versione 5.3.4
- Cisco ISE 2.4

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, verificare che l'impatto potenziale di qualsiasi modifica alla configurazione sia completamente compreso.

Configurazione

Componenti predefiniti di IOS® XR

In IOS® XR sono disponibili gruppi di utenti e di attività predefiniti. L'amministratore può utilizzare questi gruppi predefiniti o definire gruppi personalizzati in base alle esigenze.

Gruppi di utenti predefiniti

Questi gruppi di utenti sono predefiniti in IOS® XR:

Gruppo utenti	Privilegi
supporto cisco	Funzioni di debug e risoluzione dei problemi (in genere, utilizzate dal personale del supporto tecnico Cisco).
netadmin	Configurare i protocolli di rete, ad esempio Open Shortest Path First (OSPF), generalmente utilizzati dagli amministratori di rete.
operatore root-lr	Eseguire attività di monitoraggio quotidiane e disporre di diritti di configurazione limitati. Visualizzare ed eseguire tutti i comandi all'interno di un singolo RP.
sistema radice	Visualizzare ed eseguire tutti i comandi per tutti i RP nel sistema.
sysadmin	Eseguire attività di amministrazione del sistema per il router, ad esempio mantenere la posizione in cui sono archiviati i dump di base o configurare l'orologio NTP (Network Time Protocol).
serviceadmin	Eseguire attività di amministrazione del servizio, ad esempio SBC (Session Border Control).

A ogni gruppo di utenti predefinito sono associati determinati gruppi di attività e non possono essere modificati. Per controllare i gruppi di utenti predefiniti, usare questi comandi:

```
RP/0/RSP0/CPU0:ASR9k#sh aaa usergroup ?
```

```
|          Output Modifiers
root-lr    Name of the usergroup
netadmin   Name of the usergroup
operator   Name of the usergroup
sysadmin   Name of the usergroup
retrieval  Name of the usergroup
maintenance Name of the usergroup
root-system Name of the usergroup
provisioning Name of the usergroup
read-only-tg Name of the usergroup
serviceadmin Name of the usergroup
cisco-support Name of the usergroup
WORD       Name of the usergroup
<cr>
```

Gruppi di task predefiniti

Gli amministratori possono utilizzare questi gruppi di task predefiniti, in genere per la configurazione iniziale:

- supporto cisco: Attività del personale di supporto Cisco
- netadmin: Attività dell'amministratore di rete
- operatore: Attività quotidiane dell'operatore (a scopo dimostrativo)
- root-lr: Attività di amministrazione del router di dominio sicuro
- sistema radice: Attività di amministratore a livello di sistema
- sysadmin: Attività dell'amministratore di sistema
- serviceadmin: Attività di amministrazione del servizio

Utilizzare questi comandi per verificare i gruppi di operazioni predefiniti:

```
RP/0/RSP1/CPU0:ASR9k#show aaa taskgroup ?
```

```
|          Output Modifiers
root-lr    Name of the taskgroup
netadmin   Name of the taskgroup
operator   Name of the taskgroup
sysadmin   Name of the taskgroup
root-system Name of the taskgroup
serviceadmin Name of the taskgroup
cisco-support Name of the taskgroup
WORD       Name of the taskgroup
<cr>
```

Utilizzare questo comando per verificare le attività supportate:

```
RP/0/RSP1/CPU0:ASR9k#show aaa task supported
```

Di seguito sono elencate le attività supportate:

Aaa	Acl	Admin	Ancp	Atm	servizi di base	Bcdl	Bfd	bgp
Avvio	Pacchetto	call-home	Cdp	Cef	Cgn	supporto cisco	config-mgmt	servizi di configurazione
Crittografia	Diag	Non consentito	Driver	Dwdm	Eem	EIGRP	servizi ethernet	accesso esterno
Fabric	fault-mgr	File system	Firewall	Fr	Hdlc	servizi host	Hsrp	interfaccia

Inventario	servizi ip	IPv4	Ipv6	Isis	L2vpn	Li	Lisp	registrazione
Lpt	Monitor (Monitora)	mpls-ldp	mpls-static	mpls-te	Multicast	NetFlow	Rete	nps
OSPF	Ouni	Pbr	pkg-mgmt	pos-dpt	Ppp	Qos	Rcmd	costola
RIP	root-Ir	sistema radice	route-map	route-policy	Sbc	Snmp	sonet-sdh	statico
Sysmgr	Sistema	Trasporto	tty-access	Tunnel	Universale	VLAN	Vpdn	vrp

Ognuna di queste attività può essere assegnata con una o tutte le quattro autorizzazioni seguenti:

Letture	Specifica una designazione che consente solo un'operazione di lettura.
Scrittura	Specifica una designazione che consente un'operazione di modifica e un'operazione di lettura.
Immettere il comando	Specifica una designazione che consente un'operazione di accesso; ad esempio, ping e telnet.
Debug	Specifica una designazione che consente un'operazione di debug.

Gruppi di task definiti dall'utente

Gli amministratori possono configurare gruppi di attività personalizzati per soddisfare esigenze particolari. Di seguito è riportato un esempio di configurazione:

```
RP/0/RSP1/CPU0:ASR9k(config)#taskgroup TAC-Defined-TASK
```

```
RP/0/RSP1/CPU0:ASR9k(config-tg)#task ?
```

```
debug    Specify a debug-type task ID
execute  Specify a execute-type task ID
read     Specify a read-type task ID
write    Specify a read-write-type task ID
```

```
RP/0/RSP1/CPU0:ASR9k(config-tg)#task read aaa
```

```
RP/0/RSP1/CPU0:ASR9k(config-tg)#task write aaa
```

```
RP/0/RSP1/CPU0:ASR9k(config-tg)#task execute aaa
```

```
RP/0/RSP1/CPU0:ASR9k(config-tg)#task debug aaa
```

```
RP/0/RSP1/CPU0:ASR9k(config-tg)#task read acl
```

```
RP/0/RSP1/CPU0:ASR9k(config-tg)#task write acl
```

```
RP/0/RSP1/CPU0:ASR9k(config-tg)#task execute acl
```

```
RP/0/RSP1/CPU0:ASR9k(config-tg)#commit
```

```
RP/0/RSP1/CPU0:ASR9k#show aaa taskgroup TAC-Defined-TASK
```

```
Task group 'TAC-Defined-TASK'
```

```
Task IDs included directly by this group:
```

```
Task:          aaa : READ    WRITE    EXECUTE    DEBUG
```

```
Task:          acl  : READ    WRITE    EXECUTE
```

```
Task group 'TAC-Defined-TASK' has the following combined set
```

```
of task IDs (including all inherited groups):
```

```
Task:          aaa : READ    WRITE    EXECUTE    DEBUG
```

```
Task:          acl  : READ    WRITE    EXECUTE
```

Il comando **Descrivi** può essere utilizzato per individuare il gruppo di attività e le autorizzazioni necessarie per un determinato comando.

Esempio 1.

```
RP/0/RSP1/CPU0:ASR9k#describe show aaa usergroup
Package:
.....
User needs ALL of the following taskids:

aaa (READ)
RP/0/RSP1/CPU0:ASR9k#
```

Per consentire a un utente di eseguire il comando **show aaa usergroup**, assegnare al gruppo di utenti il comando **task read aaa**.

Esempio 2.

```
RP/0/RSP1/CPU0:ASR9k(config)#describe aaa authentication login default group tacacs+
Package:
.....
User needs ALL of the following taskids:

aaa (READ WRITE)
RP/0/RSP1/CPU0:ASR9k(config)#
```

Per consentire a un utente di eseguire il **gruppo predefinito tacacs+** di accesso con autenticazione CommandAccess dalla modalità di configurazione, è necessario assegnare al gruppo di utenti il gruppo di attività: **task read write aaa**.

Gli amministratori possono definire il gruppo di utenti che può ereditare diversi gruppi di operazioni. Di seguito è riportato l'esempio di configurazione:

```
RP/0/RSP1/CPU0:ASR9k#show aaa usergroup TAC-Defined
Tue Feb 16 00:50:56.799 UTC
User group 'TAC-Defined'
  Inherits from task group 'operator'

User group 'TAC-Defined' has the following combined set
of task IDs (including all inherited groups):
Task:      basic-services  : READ      WRITE      EXECUTE    DEBUG
Task:      cdp             : READ
Task:      diag            : READ
Task:      ext-access      : READ              EXECUTE
Task:      logging         : READ

RP/0/RSP1/CPU0:ASR9k#conf t
RP/0/RSP1/CPU0:ASR9k(config)#usergroup TAC-Defined
RP/0/RSP1/CPU0:ASR9k(config-ug)#taskgroup TAC-Defined-TASK
RP/0/RSP1/CPU0:ASR9k(config-ug)#commit

RP/0/RSP1/CPU0:ASR9k#show aaa usergroup TAC-Defined
Tue Feb 16 00:51:31.494 UTC
User group 'TAC-Defined'
  Inherits from task group 'operator'
  Inherits from task group 'TAC-Defined-TASK'

User group 'TAC-Defined' has the following combined set
of task IDs (including all inherited groups):
Task:      aaa             : READ      WRITE      EXECUTE    DEBUG
Task:      acl             : READ      WRITE      EXECUTE
```

```
Task:          basic-services  : READ      WRITE      EXECUTE    DEBUG
Task:          cdp             : READ
Task:          diag           : READ
Task:          ext-access     : READ          EXECUTE
Task:          logging        : READ
```

Configurazione AAA sul router

Configurare il server TACACS sul router ASR con l'indirizzo IP e il segreto condiviso da utilizzare.

```
RP/0/RSP1/CPU0:ASR9k(config)#tacacs-server host 10.106.73.233 port 49
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#key 0 cisco
RP/0/RSP1/CPU0:ASR9k(config-tacacs-host)#commit
```

```
!
tacacs-server host 10.127.196.160 port 49
key 7 14141B180F0B
!
```

Configurare l'autenticazione e l'autorizzazione per utilizzare il server TACACS configurato.

```
#aaa authentication login default group tacacs+ local
#aaa authorization exec default group tacacs+ local
```

Configurare l'autorizzazione del comando per l'utilizzo del server TACACS configurato (facoltativo):

Nota: Verificare che l'autenticazione e l'autorizzazione funzionino come previsto e che i set di comandi siano configurati correttamente prima di abilitare l'autorizzazione del comando. Se la configurazione non è corretta, gli utenti potrebbero non essere in grado di immettere comandi nel dispositivo.

```
#aaa authorization commands default group tacacs+
```

Configurare l'accounting dei comandi per utilizzare il server TACACS configurato (facoltativo).

```
#aaa accounting commands default start-stop group tacacs+
#aaa accounting update newinfo
```

Configurazione server ISE

Passaggio 1. Per definire l'indirizzo IP del router nell'elenco dei client AAA sul server ISE, selezionare **Administration > NR** risorse di rete > **Dispositivi di rete** come mostrato nell'immagine. Il segreto condiviso deve essere uguale a quello configurato sul router ASR, come mostrato nell'immagine.

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices List > New Network Device

Network Devices

* Name: LAB_ASR
Description: LAB_ASR device

IP Address: 10.106.37.160 / 32

* Device Profile: Cisco
Model Name: []
Software Version: []

* Network Device Group

Location: LAB [Set To Default]
IPSEC: Is IPSEC Device [Set To Default]
Device Type: ASR [Set To Default]

RADIUS Authentication Settings
 TACACS Authentication Settings

Shared Secret: [] [Show]
Enable Single Connect Mode:
 Legacy Cisco Device
 TACACS Draft Compliance Single Connect Support

SNMP Settings
 Advanced TrustSec Settings

[Submit] [Cancel]

Configurazione dispositivo di rete

Identity Services Engine Administration Work Centers

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC

Network Devices Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM Location Services

Network Devices

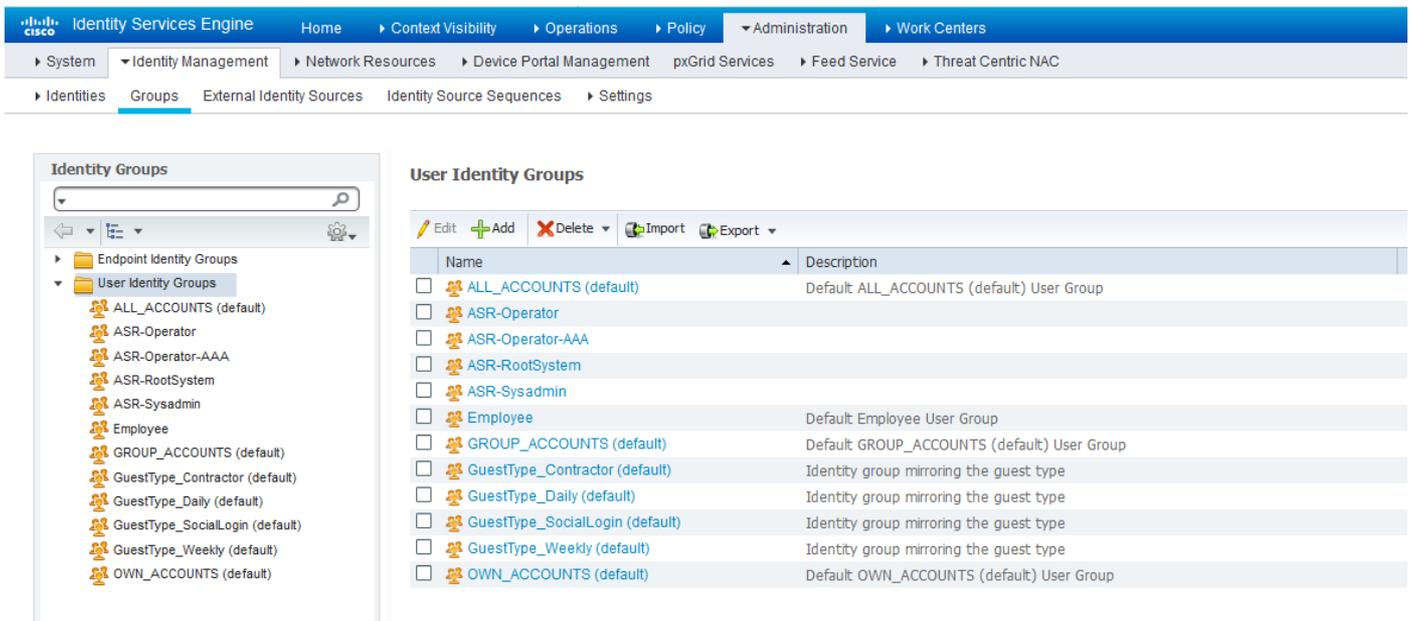
Edit Add Duplicate Import Export Generate PAC Delete

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> LAB_ASR	10.106.37.16...	Cisco	LAB	ASR	LAB_ASR device

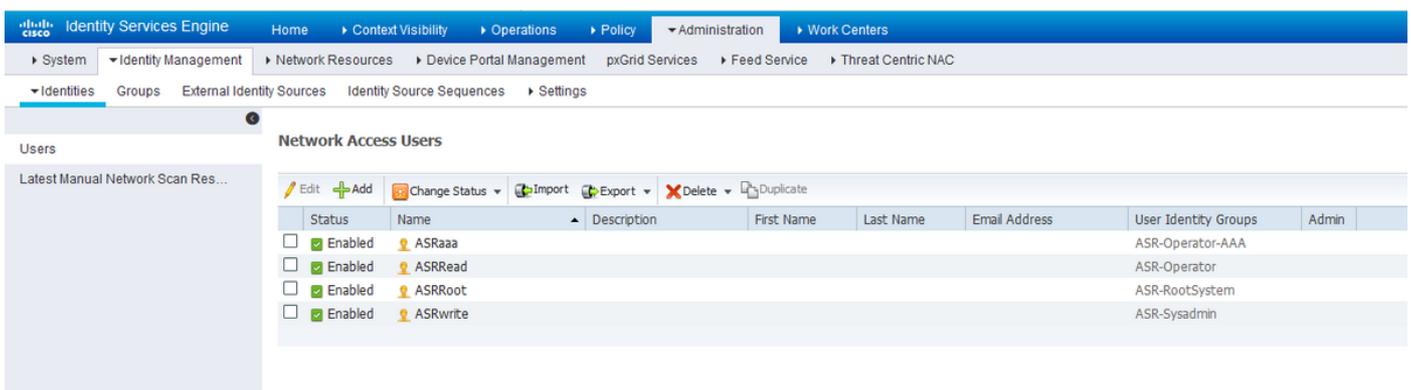
Configurazione dispositivo di rete

Passaggio 2. Definire i gruppi di utenti in base alle proprie esigenze. Nell'esempio, come mostrato in questa immagine, si utilizzano quattro gruppi. È possibile definire i gruppi in **Amministrazione > Gestione delle identità > Gruppi > Gruppi identità utente**. I gruppi creati in questo esempio sono:

1. Operatore ASR
2. ASR-Operator-AAA
3. ASR-RootSystem
4. ASR-Sysadmin



Gruppi di identità Passaggio 3. Come mostrato nell'immagine, creare gli utenti e mapparli al rispettivo gruppo di utenti creato in precedenza.



Identità/Utenti

Nota: Nell'esempio, gli utenti interni di ISE vengono usati per l'autenticazione e l'autorizzazione. Le autenticazioni e le autorizzazioni con origine identità esterna non rientrano nell'ambito del presente documento.

Passaggio 4. Definire il profilo di shell da sottoporre a push per i rispettivi utenti. A tale scopo, selezionare **Centri di lavoro > Amministrazione dispositivi > Elementi della policy > Risultati > Profili TACACS**. È possibile configurare un nuovo profilo della shell come mostrato nelle immagini e nelle versioni precedenti di ISE. I profili di shell definiti in questo esempio sono:

1. Operatore_ASR
2. ASR_RootSystem
3. ASR_Sysadmin
4. Operator_with_AAA

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles

0 Selected

Refresh Add Duplicate Trash Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	ASR_Operator	Shell	
<input type="checkbox"/>	ASR_RootSystem	Shell	
<input type="checkbox"/>	ASR_Sysadmin	Shell	
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	Operator_with_AAA	Shell	
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR

Profili shell per TACACS

È possibile fare clic sul pulsante **Add** (Aggiungi) per immettere i campi **Type** (Tipo), **Name** (Nome) e **Value** (Valore), come mostrato nelle immagini della sezione **Custom Attributes** (Attributi personalizzati).

Per il ruolo Operatore:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassiveID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles > ASR_Operator

TACACS Profile

Name: ASR_Operator

Description:

Task Attribute View Raw View

Common Tasks

Common Task Type: Shell

- Default Privilege: (Select 0 to 15)
- Maximum Privilege: (Select 0 to 15)
- Access Control List:
- Auto Command:
- No Escape: (Select true or false)
- Timeout: Minutes (0-9999)
- Idle Time: Minutes (0-9999)

Custom Attributes

+ Add Trash Edit

<input type="checkbox"/>	Type	Name	Value
<input type="checkbox"/>	MANDATORY	task	nwc,#operator

Cancel Save

Profilo shell operatore ASRPer il ruolo del sistema radice:

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface for a TACACS Profile named ASR_RootSystem. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Device Administration > PassiveID > Policy Elements > TACACS Profiles > ASR_RootSystem.

TACACS Profile

Name: ASR_RootSystem

Description: [Empty field]

Task Attribute View | Raw View

Common Tasks

Common Task Type: Shell

- Default Privilege: [Dropdown] (Select 0 to 15)
- Maximum Privilege: [Dropdown] (Select 0 to 15)
- Access Control List: [Dropdown]
- Auto Command: [Dropdown]
- No Escape: [Dropdown] (Select true or false)
- Timeout: [Dropdown] Minutes (0-9999)
- Idle Time: [Dropdown] Minutes (0-9999)

Custom Attributes

+ Add | Trash | Edit

Type	Name	Value
<input type="checkbox"/> MANDATORY	task	nxc,#root-system

Cancel Save

Profilo shell sistema radice ASRPer il ruolo sysadmin:

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Network Access Guest Access TrustSec BYOD Profiler Posture Device Administration PassivID

Overview Identities User Identity Groups Ext Id Sources Network Resources Policy Elements Device Admin Policy Sets Reports Settings

TACACS Profiles > ASR_Sysadmin

TACACS Profile

Name ASR_Sysadmin

Description

Task Attribute View Raw View

Common Tasks

Common Task Type Shell

Default Privilege (Select 0 to 15)
 Maximum Privilege (Select 0 to 15)
 Access Control List
 Auto Command
 No Escape (Select true or false)
 Timeout Minutes (0-9999)
 Idle Time Minutes (0-9999)

Custom Attributes

+ Add Trash Edit

Type	Name	Value
<input type="checkbox"/> MANDATORY	task	rw: #sysadmin

Cancel Save

Profilo shell Sysadmin ASRPer operatore e ruolo AAA:

Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassiveID

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

TACACS Profiles > Operator_with_AAA

TACACS Profile

Name: Operator_with_AAA

Description:

Task Attribute View | Raw View

Common Tasks

Common Task Type: Shell

- Default Privilege (Select 0 to 15)
- Maximum Privilege (Select 0 to 15)
- Access Control List
- Auto Command
- No Escape (Select true or false)
- Timeout (Minutes (0-9999))
- Idle Time (Minutes (0-9999))

Custom Attributes

+ Add | Trash | Edit

Type	Name	Value
<input type="checkbox"/> MANDATORY	task	nwc:aaa,#operator

Cancel Save

Operatore con profilo shell AAPasso 5: configurare la sequenza di origine delle identità in modo che utilizzi gli utenti interni in **Amministrazione > Gestione delle identità > Sequenze di origine delle identità**. È possibile aggiungere una nuova sequenza di origine delle identità o modificare quelle disponibili.

The screenshot shows the configuration page for the 'All_User_ID_Stores' Identity Source Sequence in Cisco ISE. The page is divided into several sections:

- Identity Source Sequence:** The name is 'All_User_ID_Stores' and the description is 'A built-in Identity Sequence to include all User Identity Stores'.
- Certificate Based Authentication:** A checkbox for 'Select Certificate Authentication Profile' is unchecked, and the dropdown menu shows 'Preloaded_Certificate_1'.
- Authentication Search List:** A set of identity sources that will be accessed in sequence until first authentication succeeds. It shows two columns: 'Available' and 'Selected'.
 - Available:** Internal Endpoints
 - Selected:** Internal Users, All_AD_Join_Points, Guest Users
- Advanced Search List Settings:** Two radio buttons are present:
 - Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"
 - Treat as if the user was not found and proceed to the next store in the sequence

At the bottom, there are 'Save' and 'Reset' buttons.

Passaggio 6. Configurare il criterio di autenticazione in **Centri di lavoro > Amministrazione dispositivi > Set di criteri di amministrazione dispositivi > [Scegli set di criteri]** per utilizzare la sequenza di archivio identità che contiene gli utenti interni. Configurare l'autorizzazione in base al requisito utilizzando i gruppi di identità utente creati in precedenza e mappare i rispettivi profili di shell, come mostrato nell'immagine.

The screenshot shows the configuration page for the 'ASR TACACS policy' in Cisco ISE. The page displays the following details:

- Policy Set Name:** ASR TACACS policy
- Conditions:**
 - AND
 - DEVICE Device Type EQUALS All Device Types#ASR
 - DEVICE Location EQUALS All Locations#LAB
- Authentication Policy (1):**
 - Default
 - Associated Identity Source: All_User_ID_Stores

At the bottom right, there are 'Options' and a gear icon.

Criteri di autenticazione

I criteri di autorizzazione possono essere configurati in molti modi in base ai requisiti. Le regole mostrate nell'immagine si basano sulla posizione del dispositivo, sul tipo e sul gruppo di identità utente interno specifico. I profili di shell selezionati verranno sottoposti a push al momento

dell'autorizzazione insieme ai set di comandi.

Status	Rule Name	Conditions	Command Sets	Shell Profiles	Hits	Actions
ASR_Root-System_Rule	AND	InternalUser IdentityGroup EQUALS User Identity Groups ASR-RootSystem DEVICE Location EQUALS All Locations#LAB DEVICE Device Type EQUALS All Device Types#ASR	PermiAllCommands	ASR_RootSystem	0	
ASR_Sysadmin-Rule	AND	InternalUser IdentityGroup EQUALS User Identity Groups ASR-Sysadmin DEVICE Location EQUALS All Locations#LAB DEVICE Device Type EQUALS All Device Types#ASR	PermiAllCommands	ASR_Sysadmin	0	
ASR_Operator_AAA_Rule	AND	InternalUser IdentityGroup EQUALS User Identity Groups ASR-Operator-AAA DEVICE Location EQUALS All Locations#LAB DEVICE Device Type EQUALS All Device Types#ASR	PermiAllCommands	Operator_with_AAA	0	
ASR_Operator_Rule	AND	InternalUser IdentityGroup EQUALS User Identity Groups ASR-Operator DEVICE Location EQUALS All Locations#LAB DEVICE Device Type EQUALS All Device Types#ASR	PermiAllCommands	ASR_Operator	0	
Default			DenyAllCommands	Deny All Shell Profile	0	

Criteri di autorizzazione

Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Operatore

Verificare il gruppo di utenti e i gruppi di operazioni assegnati **quando un utente letto** accede al router.

```
username: ASRread  
password:
```

```
RP/0/RSP1/CPU0:ASR9k#show user  
ASRread
```

```
RP/0/RSP1/CPU0:ASR9k#show user group  
operator
```

```
RP/0/RSP1/CPU0:ASR9k#show user tasks  
Task:          basic-services  : READ      WRITE      EXECUTE    DEBUG  
Task:          cdp             : READ  
Task:          diag            : READ  
Task:          ext-access      : READ      EXECUTE  
Task:          logging         : READ
```

Operatore con AAA

Verificare il gruppo di utenti e i gruppi di operazioni assegnati quando **asraaa** l'utente accede al router.

Nota: asraa è l'operazione dell'operatore inviata dal server TACACS insieme alle autorizzazioni di lettura, scrittura ed esecuzione dell'operazione AAA.

```
username: asraaa
password:
```

```
RP/0/RSP1/CPU0:ASR9k#sh user
asraaa
```

```
RP/0/RSP1/CPU0:ASR9k#sh user group
operator
```

```
RP/0/RSP1/CPU0:ASR9k#sh user tasks
Task:          aaa      : READ      WRITE      EXECUTE
Task:    basic-services : READ      WRITE      EXECUTE      DEBUG
Task:          cdp      : READ
Task:          diag     : READ
Task:    ext-access    : READ          EXECUTE
Task:    logging      : READ
```

Sysadmin

Verificare il gruppo di utenti e i gruppi di operazioni assegnati quando **ascrittura** l'utente accede al router.

```
username: asrwrite
password:
```

```
RP/0/RSP1/CPU0:ASR9k#sh user
asrwrite
```

```
RP/0/RSP1/CPU0:ASR9k#sh user group
sysadmin
```

```
RP/0/RSP1/CPU0:ASR9k#sh user tasks
Task:          aaa      : READ
Task:          acl      : READ      WRITE      EXECUTE      DEBUG
Task:          admin    : READ
Task:          ancp     : READ
Task:          atm      : READ
Task:    basic-services : READ      WRITE      EXECUTE      DEBUG
Task:          bcdl     : READ
Task:          bfd      : READ
Task:          bgp      : READ
Task:          boot     : READ      WRITE      EXECUTE      DEBUG
Task:          bundle   : READ
Task:    call-home     : READ
Task:          cdp      : READ      WRITE      EXECUTE      DEBUG
Task:          cef      : READ
Task:          cgn      : READ
Task:    config-mgmt   : READ      WRITE      EXECUTE      DEBUG
Task:    config-services : READ      WRITE      EXECUTE      DEBUG
Task:          crypto   : READ      WRITE      EXECUTE      DEBUG
Task:          diag     : READ      WRITE      EXECUTE      DEBUG
Task:          drivers  : READ
Task:          dwdm     : READ
Task:          eem      : READ      WRITE      EXECUTE      DEBUG
Task:          eigrp    : READ
Task:    ethernet-services : READ
--More--
(output omitted )
```

Root-System

Verificare il gruppo di utenti e i gruppi di operazioni assegnati quando **radice** l'utente accede al router.

```
username: asrroot
password:
```

```
RP/0/RSP1/CPU0:ASR9k#show user
asrroot
```

```
RP/0/RSP1/CPU0:ASR9k#show user group
root-system
```

```
RP/0/RSP1/CPU0:ios#show user tasks
```

Task:	aaa	: READ	WRITE	EXECUTE	DEBUG
Task:	acl	: READ	WRITE	EXECUTE	DEBUG
Task:	admin	: READ	WRITE	EXECUTE	DEBUG
Task:	anclp	: READ	WRITE	EXECUTE	DEBUG
Task:	atm	: READ	WRITE	EXECUTE	DEBUG
Task:	basic-services	: READ	WRITE	EXECUTE	DEBUG
Task:	bcdl	: READ	WRITE	EXECUTE	DEBUG
Task:	bfd	: READ	WRITE	EXECUTE	DEBUG
Task:	bgp	: READ	WRITE	EXECUTE	DEBUG
Task:	boot	: READ	WRITE	EXECUTE	DEBUG
Task:	bundle	: READ	WRITE	EXECUTE	DEBUG
Task:	call-home	: READ	WRITE	EXECUTE	DEBUG
Task:	cdp	: READ	WRITE	EXECUTE	DEBUG
Task:	cef	: READ	WRITE	EXECUTE	DEBUG
Task:	cgn	: READ	WRITE	EXECUTE	DEBUG
Task:	config-mgmt	: READ	WRITE	EXECUTE	DEBUG
Task:	config-services	: READ	WRITE	EXECUTE	DEBUG
Task:	crypto	: READ	WRITE	EXECUTE	DEBUG
Task:	diag	: READ	WRITE	EXECUTE	DEBUG
Task:	drivers	: READ	WRITE	EXECUTE	DEBUG
Task:	dwdm	: READ	WRITE	EXECUTE	DEBUG
Task:	eem	: READ	WRITE	EXECUTE	DEBUG
Task:	eigrp	: READ	WRITE	EXECUTE	DEBUG

```
--More--
```

```
(output omitted )
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Verificare il report ISE da **Operations > TACACS > Live Log**. Per visualizzare il report dettagliato, fare clic sul simbolo della lente di ingrandimento.

Refresh	Export To	Logged Time	Status	Details	Username	Type	Network Device IP	Remote Address	Authorization Policy	Authentication Policy	Ise Node
x					Username		Network Device IP	Remote Address	Authorization Policy	Authentication Policy	Ise Node
		May 14, 2018 03:35:25.792 PM	✓		ASRwrite	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Sysadmin Rulef		mumanika22
		May 14, 2018 03:35:25.695 PM	✓		ASRwrite	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Sysadmin Rulef		mumanika22
		May 14, 2018 03:35:25.597 PM	✓		ASRwrite	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22
		May 14, 2018 03:35:12.959 PM	✓		ASRRoot	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Rootsystem rule		mumanika22
		May 14, 2018 03:35:12.859 PM	✓		ASRRoot	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Rootsystem rule		mumanika22
		May 14, 2018 03:35:12.771 PM	✓		ASRRoot	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22
		May 14, 2018 03:34:53.788 PM	✓		ASRRead	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator Rule		mumanika22
		May 14, 2018 03:34:53.685 PM	✓		ASRRead	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator Rule		mumanika22
		May 14, 2018 03:34:53.581 PM	✓		ASRRead	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22
		May 14, 2018 03:29:46.359 PM	✓		ASRaaa	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator AAA Rule		mumanika22
		May 14, 2018 03:29:46.257 PM	✓		ASRaaa	Authorization	10.106.37.175	173.39.69.10	ASR_LAB_Policy >> ASR Operator AAA Rule		mumanika22
		May 14, 2018 03:29:46.150 PM	✓		ASRaaa	Authentication	10.106.37.175	173.39.69.10		ASR_LAB_Policy >> Default >> Default	mumanika22

Di seguito sono riportati alcuni comandi utili per risolvere i problemi relativi a ASR:

- mostra utente
- mostra gruppo utenti
- mostra attività utente
- mostra tutti gli utenti