

Configurazione di server RADIUS esterni su ISE

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione di ISE \(Frontend Server\)](#)

[Configurare il server RADIUS esterno](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Scenario 1. Evento - Richiesta RADIUS 5405 ignorata](#)

[Scenario 2. Evento - Autenticazione 5400 non riuscita](#)

Introduzione

In questo documento viene descritto come configurare un server RADIUS su ISE come proxy e server di autorizzazione. In questo caso, vengono utilizzati due server ISE, uno dei quali funge da server esterno. Tuttavia, è possibile utilizzare qualsiasi server RADIUS compatibile con RFC.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base del protocollo RADIUS
- Esperienza nella configurazione delle policy di Identity Services Engine (ISE)

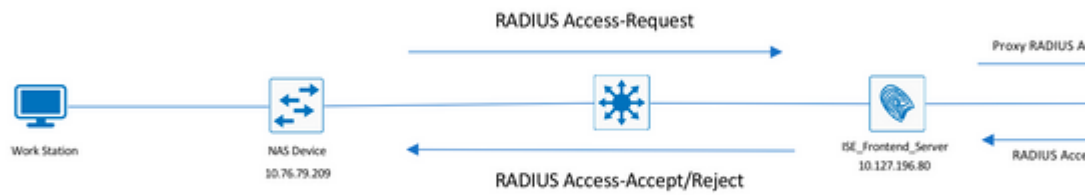
Componenti usati

Il riferimento delle informazioni contenute in questo documento è Cisco ISE versioni 2.2 e 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, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

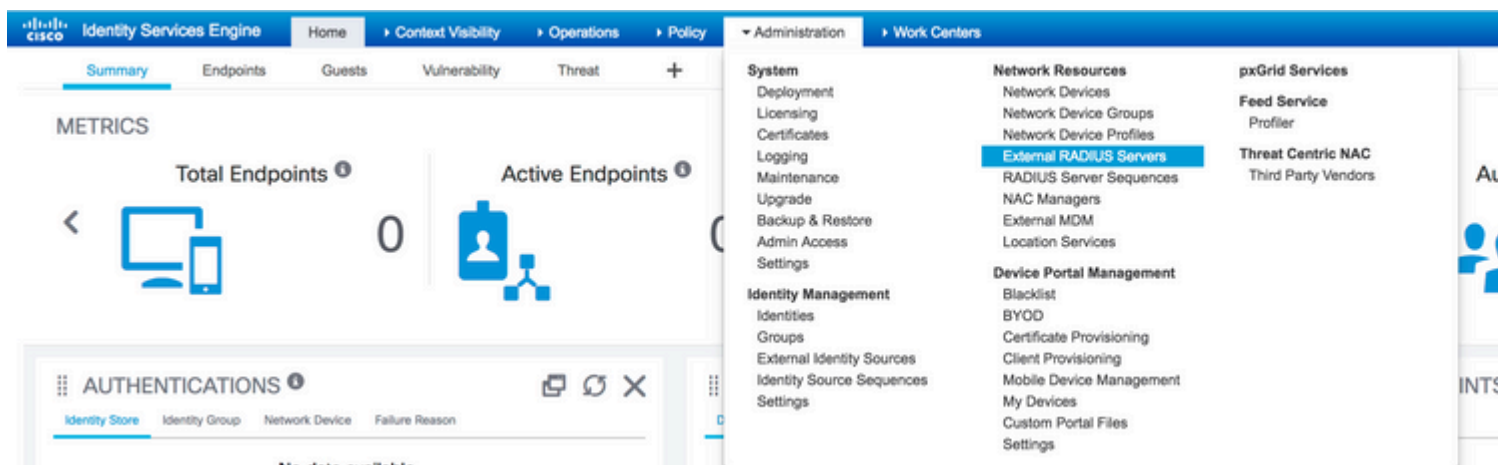
Configurazione

Esempio di rete



Configurazione di ISE (Frontend Server)

Passaggio 1. Per autenticare gli utenti sull'ISE, è possibile configurare e utilizzare più server RADIUS esterni. Per configurare i server RADIUS esterni, passare a Administration > Network Resources > External RADIUS Servers > Add, come mostrato nell'immagine:



External RADIUS Servers List > ISE_BackEnd_Server

External RADIUS Server

* Name

Description

* Host IP

* Shared Secret

Enable KeyWrap

* Key Encryption Key

* Message Authenticator Code Key

Key Input Format ASCII HEXADECIMAL

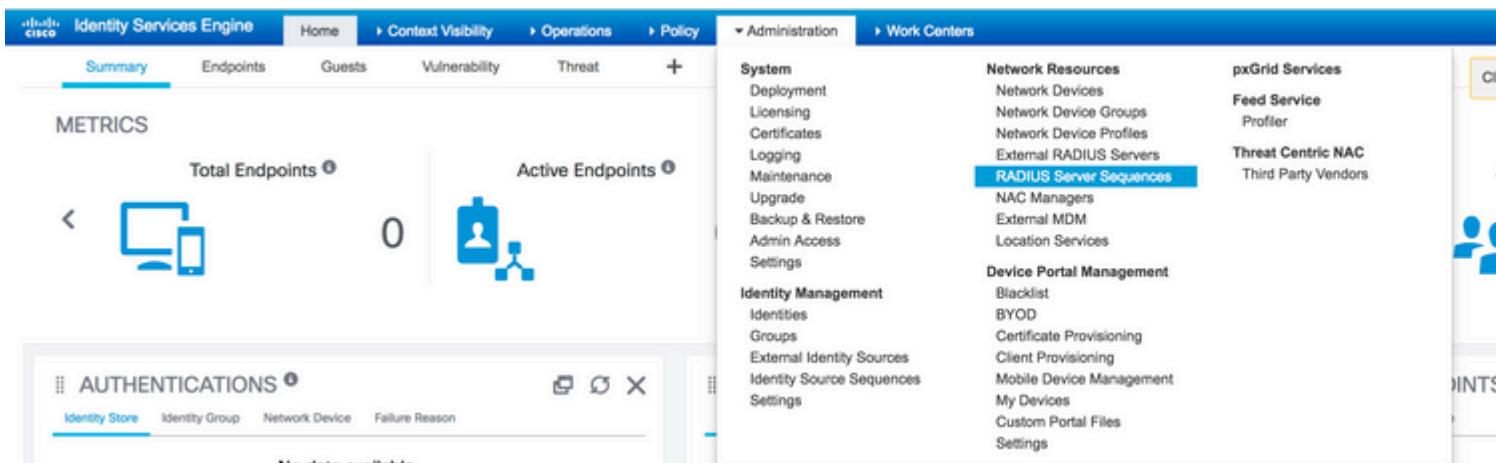
* Authentication Port (Valid Range 1 to 65535)

* Accounting Port (Valid Range 1 to 65535)

* Server Timeout Seconds (Valid Range 1 to 120)

* Connection Attempts (Valid Range 1 to 9)

Passaggio 2. Per utilizzare il server RADIUS esterno configurato, è necessario configurare una sequenza di server RADIUS simile alla sequenza di origine Identity. Per configurare lo stesso, passare a Administration > Network Resources > RADIUS Server Sequences > Add, come illustrato nell'immagine.





RADIUS Server Sequences List > **New RADIUS Server Sequence**

RADIUS Server Sequence

General

Advanced Attribute Settings

* Name

Description

Sequence in which the external servers should be used.

▼ User Selected Service Type

Select the set of external RADIUS servers to use to process requests. Servers are accessed in sequence until a

Available

* Selected

ISE_BackEnd_Server



Remote accounting

Local accounting

Submit

Cancel

Nota: una delle opzioni disponibili durante la creazione della sequenza del server consiste nel scegliere se l'accounting deve essere eseguito localmente sull'ISE o sul server RADIUS esterno. In base all'opzione scelta qui, ISE decide se inoltrare le richieste di accounting o archiviare i log a livello locale.

Passaggio 3. C'è una sezione aggiuntiva che offre maggiore flessibilità su come ISE deve comportarsi quando inoltra le richieste ai server RADIUS esterni. È disponibile in *Advance Attribute Settings*, come illustrato nell'immagine.

The screenshot shows the Cisco Identity Services Engine (ISE) configuration interface. The breadcrumb trail is: Home > Context Visibility > Operations > Policy > Administration > System > Identity Management > Network Resources > Device Portal Management > pxGrid Services > Feed S > Network Devices > Network Device Groups > Network Device Profiles > External RADIUS Servers > RADIUS Server Sequ. The main heading is 'RADIUS Server Sequence' with sub-headings 'General' and 'Advanced Attribute Settings'. Under 'Advanced Settings', there are two checkboxes: 'Strip start of subject name up to the first occurrence of the separator' with a text box containing '\', and 'Strip end of subject name from the last occurrence of the separator' with a text box containing '@'. Below this is the 'Modify Attribute in the request' section with a checkbox 'Modify attributes in the request to the External RADIUS Server' and a configuration row: 'Add' | 'Select an item' | '=' | an empty text box | '-' | '+'. The 'Continue to Authorization Policy' section has a checked checkbox 'On Access-Accept, continue to Authorization Policy'. The 'Modify Attribute before access accept' section has a checkbox 'Modify attributes before send an Access-Accept' and a configuration row: 'Add' | 'Select an item' | '=' | an empty text box | '-' | '+'. At the bottom are 'Save' and 'Reset' buttons.

- Impostazioni avanzate: fornisce opzioni per rimuovere l'inizio o la fine del nome utente nelle richieste RADIUS con un delimitatore.

- **Modify Attribute in the request:** fornisce l'opzione per modificare qualsiasi attributo RADIUS nelle richieste RADIUS. L'elenco mostra gli attributi che possono essere aggiunti/rimossi/aggiornati:

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:** fornisce un'opzione per scegliere se ISE deve semplicemente inviare l'Access-Accept così com'è o procedere per fornire l'accesso in base ai criteri di autorizzazione configurati sull'ISE piuttosto che all'autorizzazione fornita dal server RADIUS esterno. Se questa opzione è selezionata, l'autorizzazione fornita dal server RADIUS esterno viene sovrascritta dall'autorizzazione fornita da ISE.

Nota: questa opzione funziona solo se il server RADIUS esterno invia un Access-Accept in

risposta alla richiesta di accesso RADIUS proxy.

- Modifica attributo prima di Access-Accept: simile alla Modify Attribute in the request, gli attributi menzionati in precedenza possono essere aggiunti/rimossi/aggiornati presenti nell'Access-Accept inviato dal server RADIUS esterno prima dell'invio al dispositivo di rete.

Passaggio 4. La parte successiva consiste nel configurare i set di criteri in modo da utilizzare la sequenza di server RADIUS anziché i protocolli consentiti in modo che le richieste vengano inviate al server RADIUS esterno. Può essere configurato in Policy > Policy Sets. I criteri di autorizzazione possono essere configurati in Policy Set ma entrano in vigore solo se il Continue to Authorization Policy on Access-Accept è selezionata. In caso contrario, ISE agirà semplicemente come proxy per le richieste RADIUS in modo da soddisfare le condizioni configurate per questo set di criteri.

Status	Policy Set Name	Description	Conditions
On	External_Auth_Policy_Set		DEVICE:Device Type EQUALS All Device Types
On	Default	Default policy set	

Status	Policy Set Name	Description	Conditions
On	External_Auth_Policy_Set		DEVICE:Device Type EQUALS All Device Types

Authentication Policy (1)

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (1)

Status	Rule Name	Conditions
On	Default	

PermitAccess

Configurare il server RADIUS esterno

Passaggio 1. Nell'esempio, viene usato un altro server ISE (versione 2.2) come server RADIUS esterno denominato ISE_Backend_Server. L'interfaccia ISEISE_Frontend_Server) deve essere configurato come dispositivo di rete o denominato in modo tradizionale NAS nel server RADIUS esterno (ISE_Backend_Server in questo esempio), poiché NAS-IP-Address nella richiesta di accesso inoltrata al server RADIUS esterno viene sostituito con l'indirizzo IP del ISE_Frontend_Server. Il segreto condiviso da configurare è uguale a quello configurato per il server RADIUS esterno sul server ISE_Frontend_Server.

The screenshot displays the configuration page for a Network Device in the Cisco Identity Services Engine (ISE) interface. The page is titled "Network Devices List > ISE_Frontend_Server" and "Network Devices". The configuration fields are as follows:

- Name: ISE_Frontend_Server
- Description: This will be used as an
- IP Address: 10.127.196.80 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group: (empty)
- Device Type: All Device Types (Set To Default)
- IPSEC: No (Set To Default)
- Location: All Locations (Set To Default)
- Trustsec: SGA (Set To Default)
- Authentication Settings:
 - RADIUS Authentication Settings
 - TACACS Authentication Settings
 - SNMP Settings
 - Advanced TrustSec Settings

Buttons for "Save" and "Reset" are located at the bottom of the configuration area.

Passaggio 2. Il server RADIUS esterno può essere configurato con propri criteri di autenticazione e autorizzazione in modo da soddisfare le richieste inoltrate dall'ISE. In questo esempio, viene configurato un criterio semplice per controllare l'utente negli utenti interni e quindi consentire l'accesso se autenticato.

Identity Services Engine Home Context Visibility Operations Policy Administration Work Centers

Policy Sets Profiling Posture Client Provisioning Policy Elements

Policy Sets

Search policy names & descriptions.

Summary of Policies
A list of all your policies

Global Exceptions
Rules across entire deployment

Default
Default Policy Set

Save Order Reset Order

Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
<input checked="" type="checkbox"/>	Default	Default Policy Set

Authentication Policy

Status	Name	Conditions (Identity groups and other conditions)	Allow Protocols	and use
<input checked="" type="checkbox"/>	MAB	if Wired_MAB OR Wireless_MAB	Default Network Access	
<input checked="" type="checkbox"/>	Dot1X	if Wired_802.1X OR Wireless_802.1X	Default Network Access	
<input checked="" type="checkbox"/>	Default Rule (If no match)		Default Network Access	Internal Users

Authorization Policy

Exceptions (0)

Standard

Status	Rule Name	Conditions (Identity groups and other conditions)	Permissions
<input checked="" type="checkbox"/>	Wireless Black List Default	if Blacklist AND Wireless_Access	then Blackhole_Wireless_Access
<input checked="" type="checkbox"/>	Profiled Cisco IP Phones	if Cisco-IP-Phone	then Cisco_IP_Phones
<input checked="" type="checkbox"/>	Profiled Non Cisco IP Phones	if Non_Cisco_Profiled_Phones	then Non_Cisco_IP_Phones
<input checked="" type="checkbox"/>	Compliant_Devices_Access	if (Network_Access_Authentication_Passed AND Compliant_Devices)	then PermitAccess
<input checked="" type="checkbox"/>	Employee_EAP-TLS	if (Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then PermitAccess AND BYOD
<input checked="" type="checkbox"/>	Employee_Onboarding	if (Wireless_802.1X AND EAP-MSCHAPV2)	then NSP_Onboard AND BYOD
<input checked="" type="checkbox"/>	Wi-Fi_Guest_Access	if (Guest_Flow AND Wireless_MAB)	then PermitAccess AND Guests
<input checked="" type="checkbox"/>	Wi-Fi_Redirect_to_Guest_Login	if Wireless_MAB	then Cisco_WebAuth
<input checked="" type="checkbox"/>	Basic_Authenticated_Access	if Network_Access_Authentication_Passed	then PermitAccess
<input checked="" type="checkbox"/>	Default	if no matches, then	DenyAccess

Save Reset

Verifica

Passaggio 1. Controllare se la richiesta è stata ricevuta dai log live ISE, come mostrato nell'immagine.

Apr 19, 2018 07:01:54.570 PM testaccount External_Auth_Policy_Set External_Auth_Policy_Set

Passaggio 2. Verificare che sia selezionato il set di criteri corretto, come mostrato nell'immagine.

Overview

Event 5200 Authentication succeeded

Username testaccount

Endpoint Id

Endpoint Profile

Authentication Policy External_Auth_Policy_Set

Authorization Policy External_Auth_Policy_Set

Authorization Result

Passaggio 3. Verificare se la richiesta viene inoltrata al server RADIUS esterno.

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
- 11002 Returned RADIUS Access-Accept

4. Se il Continue to Authorization Policy on Access-Accept è stata scelta, verificare se il criterio di autorizzazione è stato valutato.



Overview

Event	5200 Authentication succeeded
Username	testaccount
Endpoint Id	
Endpoint Profile	
Authentication Policy	External_Auth_Policy_Set
Authorization Policy	External_Auth_Policy_Set >> Default
Authorization Result	PermitAccess

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 - PermitAccess
22081 Max sessions policy passed
22080 New accounting session created in Session cache
11002 Returned RADIUS Access-Accept

Risoluzione dei problemi

Scenario 1. Evento - Richiesta RADIUS 5405 ignorata

- La cosa più importante da verificare sono i passaggi del report dettagliato sull'autenticazione. Se i passaggi indicano RADIUS-Client request timeout expired, significa che l'ISE non ha ricevuto alcuna risposta dal server RADIUS esterno configurato. Questo problema può verificarsi quando:
 1. Problema di connettività con il server RADIUS esterno. ISE non è in grado di raggiungere il server RADIUS esterno sulle porte configurate per tale server.
 2. ISE non è configurato come dispositivo di rete o NAS sul server RADIUS esterno.
 3. I pacchetti vengono scartati dal server RADIUS esterno in base alla configurazione o a causa di un problema nel server RADIUS esterno.

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)
11104 RADIUS-Client request timeout expired (🕒 Step latency=15011 ms)
11356 Failed to forward request to current remote RADIUS server
11353 No more external RADIUS servers; can't perform failover

Controllare anche le acquisizioni dei pacchetti per verificare se non è un messaggio falso, ossia se ISE riceve il pacchetto dal server, ma segnala comunque il timeout della richiesta.

1041	6.537919	10.127.196.80	10.127.196.82	207	RADIUS	Acc
1718	11.542634	10.127.196.80	10.127.196.82	207	RADIUS	Acc
2430	16.547029	10.127.196.80	10.127.196.82	207	RADIUS	Acc

- Se i passaggi dicono Start forwarding request to remote RADIUS server e il passo più immediato è No more external RADIUS servers; can't perform failover, quindi indica che tutti i server RADIUS esterni configurati sono attualmente contrassegnati come **inattivi** e che le richieste vengono servite solo dopo la scadenza del timer inattivo.

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
11353	No more external RADIUS servers; can't perform failover

Nota: in ISE, il **tempo di inattività** predefinito per i server RADIUS esterni è di **5 minuti**. Questo valore è hardcoded e non può essere modificato con questa versione.

- Se i passaggi dicono RADIUS-Client encountered error during processing flow e sono seguiti da Failed to forward request to current remote RADIUS server; an invalid response was received, indica quindi che si è verificato un problema con ISE durante l'inoltro della richiesta al server RADIUS esterno. Questa condizione si verifica in genere quando la richiesta RADIUS inviata dal dispositivo di rete/NAS all'ISE non presenta NAS-IP-Address come uno degli attributi. Se non è presente NAS-IP-Address e, se i server RADIUS esterni non sono in uso, ISE popola il NAS-IP-Address con l'IP di origine del pacchetto. Tuttavia, ciò non è valido quando è in uso un server RADIUS esterno.

Scenario 2. Evento - Autenticazione 5400 non riuscita

- In questo caso, se i passaggi indicano 11368 Please review logs on the External RADIUS Server to determine the precise failure reason, significa che l'autenticazione non è riuscita sul server RADIUS esterno e che è stato inviato un messaggio di rifiuto di accesso.

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

- Se i passaggi dicono 15039 Rejected per authorization profile, significa che ISE ha ricevuto un'autorizzazione di accesso dal server RADIUS esterno, ma che rifiuta l'autorizzazione in base ai criteri di autorizzazione configurati.

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

- Se il Failure Reason se l'ISE è un'applicazione diversa da quelle citate in questo documento in caso di errore di autenticazione, potrebbe significare un potenziale problema con la configurazione o con l'ISE stessa. Si consiglia di aprire una richiesta TAC a questo punto.

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).