Configure External RADIUS Servers on ISE

Contents

Introduction
Prerequisites
Requirements
Components Used
Configure
Network Diagram
Configure ISE (Frontend Server)
Configure the External RADIUS Server
Verify
Troubleshoot
Scenario 1. Event - 5405 RADIUS Request Dropped
Scenario 2. Event - 5400 Authentication Failed

Introduction

This document describes how to configure two RFC-compliant RADIUS servers on ISE as proxy and authorization, respectively.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Basic knowledge of RADIUS protocol
- Expertise in Identity Services Engine (ISE) policy configuration

Components Used

The information in this document is based on Cisco ISE versions 2.2 and 2.4.

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. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram



Configure ISE (Frontend Server)

Step 1. Multiple external RADIUS servers can be configured and used in order to authenticate users on the ISE. In order to configure external RADIUS servers, navigate to Administration > Network Resources > External RADIUS Servers > Add, as shown in the image:

cisco Identity Services Engine Home Context Visibility Operations Policy	Administration Work Centers License Warning A Q @ Q Q
Summary Endpoints Guests Vulnerability Threat + S METRICS Total Endpoints Active Endpoints • Image: Comparison of the state of the state of the state fleason Image: Comparison o	System Network Resources pxGrid Services Deployment Network Device Groups Feed Service Certificates Network Device Broities Feed Service Logging Certificates Network Device Broities Maintenance RACIUIS Server Sequences Threat Centric NAC Maintenance RACIUS Server Sequences BYOD En Upgrade NAC Managers ByOD En Backup & Restore External KOM Biolisti Admin Access Location Services BYOD Settings Device Profiles Threat Centric NAC Markense External KOM Profile Settings Device Profiles Threat Centric NAC Markense External Statisti BYOD En Usentity Sources Cellert Provisioning Identity Sources Identity Sources Custom Profile Files Settings
Identity Services Engine Home → Context Visibility	Operations Policy Administration Work Centers
System Identity Management Network Resources Device Po	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
External RADIUS Servers List > ISE_BackEnd_Server External RADIUS Server * Name Description	This will be used as an external ISE server
* Host IP	0 10.127.196.82
* Shared Secret	t Show
Enable KeyWrap	
* Key Encountion Key	Chau
Rey Encryption Rey	Snow
* Message Authenticator Code Key	Show
 Message Authenticator Code Key Key Input Format 	Show ASCII HEXADECIMAL
* Message Authenticator Code Key Key Input Format * Authentication Port	Show Show Show HEXADECIMAL t 1812 (Valid Range 1 to 65535)
* Message Authenticator Code Key Key Input Format * Authentication Port * Accounting Port	Show Show Image: Show Image:
* Message Authenticator Code Key Key Input Format * Authentication Port * Accounting Port * Server Timeout	Show Show Image: The state of the

Step 2. In order to use the configured external RADIUS server, a RADIUS server sequence must be configured similar to the Identity source sequence. In order to configure the same, navigate to Administration > Network Resources > RADIUS Server Sequences > Add, as shown in the image:



cisco Ide	entity Services Engine	Home	Context	Visibility	 Operations 	Policy	- Administration	Work Centers	
 System 	Identity Management	✓ Network F	Resources	Device I	Portal Management	pxGrid S	ervices Feed Ser	vice	AC
Network	Devices Network Device	Groups No	etwork Devic	e Profiles	External RADIUS S	Servers	RADIUS Server Seque	nces NAC Managers	External MDM

RADIUS Server Sequences List > New RADIUS Server Sequence

RADIUS Server General	Sequence Advanced Attribute Settings
* Name	External_RADIUS_Sequence
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 response is received

	Available	* Selected	
	> <	ISE_BackEnd_Server	
 Remote accounting Local accounting 			
Submit Cancel			

Note: One of the options available while the server sequence is created is to choose whether accounting must be done locally on the ISE or on the external RADIUS server. Based on the option chosen here, ISE decides on whether to proxy the accounting requests or store those logs locally.

Step 3. There is an additional section that gives more flexibility on how ISE must behave when it proxies requests to external RADIUS servers. It can be found under Advance Attribute Settings, as shown in the image:

uluilu cisco	Identity S	ervices Engine	Home	► Contex	t Visibility	 Operations 	s ► Policy	- → Adr	ninistration	→ W	ork Centers	
System	tem 🕨 Ide	ntity Management	- Networ	k Resources	Device I	Portal Managem	nent pxGrid	Services	Feed Se	rvice	 Threat Centric N 	AC
Net	work Device	Network Device	Groups	Network Devic	ce Profiles	External RAD	IUS Servers	RADIUS	Server Sequ	ences	NAC Managers	External MDM
RADIU RADI	S Server Se US Serve General	quences List > Exter Sequence Advanced Att	mal_RADIU	JS_Sequence								
+ /	dvanced s	ettings										
	Strip start	of subject name up t	o the first o	occurrence of th	ne separator	· \						
	Strip end o	f subject name from	the last oc	currence of the	separator	@						
÷ 1	lodify Attı	ibute in the requ	est									
	Modify attr	butes in the request	to the Exte	ernal RADIUS S	erver							
	Add		, Se	elect an item		=			- +			
+ (Continue to	Authorization P	olicy									
~	On Access-	Accept, continue to A	Authorizatio	on Policy								
* 1	1odify Attı	ibute before acc	ess accep	t								
	Modify attr	butes before send a	n Access-Ac	ccept								
	Add		, Se	elect an item		- 2			- +			
Save	Reset											

- Advanced Settings: Provides options to strip the start or the end of the username in RADIUS requests with a delimiter.
- Modify Attribute in the request: Provides the option to modify any RADIUS attribute in the RADIUS requests. The list here shows the attributes that can be added/removed/updated:

```
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: Provides an option to choose if ISE must just send the Access-Accept as it is or proceed to provide access based on the Authorization Policies configured on the ISE rather than the authorization provided by the external RADIUS server. If this option is selected, the authorization provided by the external RADIUS server is overwritten with the authorization provided by ISE.

Note: This option works only if the external RADIUS server sends an Access-Accept in response to the proxied RADIUS Access-Request.

• Modify Attribute before Access-Accept: Similar to the Modify Attribute in the request, the attributes mentioned earlier can be added/removed/updated present in the Access-Accept sent by the external RADIUS server before it is sent to the network device.

Step 4. The next part is to configure the Policy Sets in order to use the RADIUS Server Sequence instead of Allowed Protocols so that the requests are sent to the external RADIUS server. It can be configured under Policy > Policy Sets. Authorization policies can be configured under the Policy Set but only come into effect if the Continue to Authorization Policy on Access-Accept option is chosen. If not, ISE simply acts as a proxy for the RADIUS requests in order to match the conditions configured for this Policy Set.

Hicy Sets	Allowed Protocols / Server Sequence Hits Action External_RADIUS_Sequence * * * * * * * * * * * * * * * * * * *
Status Policy Set Name Description Conditions earch	Allowed Protocols / Server Sequence Hits Action
ierch Image: Statemal_Auth_Policy_Set Image: Default Default Default Default Default Default Default Default Image: Statemal_Auth_Policy_Set Image: Statemal_	External_RADIUS_Sequence X + + 4 + + + 4 + + + 4 +
Image: Statumal_Auth_Policy_Set Default Image: Statumal_Auth_Policy_Set Default Image: Statumal_Auth_Policy_Set Image: Statumal_Auth_Policy_Set Image: Statumal_Auth_Policy_Set Default Image: Statumal_Auth_Policy_Set Image: Statumal_Auth_Policy_Set	Edemal_RADIUS_Sequence * • • • 4 • • 4 • • 4 • • 4 • • 4 • • • 4 • • • • 4 •
O befault Contract Valability Policy Policy P	Allowed Protocols Default Network Access Proxy Sequence External_RADIUS_Sequence Locense Warning C Reset Allowed Protocols / Server Sequence
Videntify Services Engine Home Context Visibility Operations Policy Administration Work Centers Status Policy Sets External_Auth_Policy_Set External_Auth_Policy_Set External_Auth_Policy_Set External_Auth_Policy_Set External_Auth_Policy_Set Authentication Policy (1) Policy Administration Work Centers Work Centers	Default Network Access Proxy Sequence External_RADRUS_Sequence License Warning A Q @ Reset Allowed Protocols / Server Sequence
Identity Services Engine Home Contact Visibility Operations Policy Administration Work Centers Work Centers Identity Services Engine Policy Elements Identity Services Client Provisioning Policy Elements Conditions Batus Policy Set Name Description Conditions External_Auth_Policy_Set External_Auth_Policy_Set Device Type EQUALS All Device Types Authentication Policy (1) 	Loonse Warning A C C Reset Allowed Protocols / Server Sequence
y Identity Services Engine Home > Context Visibility > Operations > Policy > Administration > Work Centers icry Sets > External_Auth_Policy_Set	License Warning A Q @ Reset Allowed Protocols / Server Sequence
Identity Services Engine Home Contact Visibility Operations Policy Administration Work Centers Work Centers Work Centers Work Centers Contact Visibility Operations Policy Administration Work Centers Work Center	License Warning A Reset Allowed Protocols / Server Sequence
Construction Posture Posture Construction Icy Sets Profiling Posture Client Provisioning > Policy Elements Icy Sets > External_Auth_Policy_Set Conditions Status Policy Set Name Description Conditions arch Image: Client Provision Policy_Set Image: Device Type EQUALS All Device Types Authentication Policy (1) Image: Device Type EQUALS All Device Types	Allowed Protocols / Server Sequence
cy Sets → External_Auth_Policy_Set Status Policy Set Name Description Conditions ch	Reset Allowed Protocols / Server Sequence
cy Sets → External_Auth_Policy_Set Status Policy Set Name Description Conditions Inch In	Allowed Protocols / Server Sequence
Status Policy Set Name Description Conditions arch Image: Condition Set	Allowed Protocols / Server Sequence
arch Image: Constraint of the second seco	Extend DADUS Secure
External_Auth_Policy_Set DEVICE-Device Type EQUALS All Device Types Authentication Policy (1)	Esternal DADILIC Commences and
Authentication Policy (1)	External_KADIUS_Sequence × • •
wareneoador r forcy (1)	
Authonization Policy - Local Exceptions	
Authorization Policy - Global Exceptions	
Authorization Policy (1)	
Resulta	
Status Rule Name Conditions Profiles	Security Groups Hits
Search	
+	
O Default (*Per	Access + Select from list + 4

Configure the External RADIUS Server

Step 1. In this example, another ISE server (version 2.2) is used as an external RADIUS server named ISE_Backend_Server. The ISE (ISE_Frontend_Server) must be configured as a network device or traditionally called NAS in the external RADIUS server (ISE_Backend_Server in this example), since the NAS-IP-Address attribute in the Access-Request that is forwarded to the external RADIUS server is replaced with the IP address of theISE_Frontend_Server. The shared secret to be configured is the same as the one configured for the external RADIUS server on the ISE_Frontend_Server.

dentity Services Engine	Home Context Vability Operations Policy Administration Work Centers	1	License Warning 🔺	٩,	9 Q	0
System Identity Management	Network Resources Device Portal Management pxGrid Services Feed Service Threat Centric NAC					
Network Devices Network Device 0	roups Network Device Profiles External RADIUS Servers RADIUS Server Sequences NAC Managers External MDM + Location Services					
0	Mahurah Daviana List v TEE Established Gamma					
Network devices	Network Devices					
Default Device	* Name ISE_Frontend_Server					
Device Security Settings	Description This will be used as an					
	* IP Address: 10.127.196.80 / 32		÷.			
	* Device Profile 🔝 Cisco 💌 🕀					
	Model Name v					
	Software Version					
	* Network Device Group					
	Device Type All Device Types 📀 Set To Default					
	IPSEC No O Set To Default					
	Location All Locations 🙄 Set To Default					
	Trustsec SGA O Set To Default					
	RADIUS Authentication Settings					
	TACACS Authentication Settings					
	SNMP Settings					
	Advanced TrustSec Settings					
	Save Reset					

Step 2. The external RADIUS server can be configured with its own authentication and authorization policies in order to serve the requests proxied by the ISE. In this example, a simple policy is configured in order to check the user in the internal users and then permit access if authenticated.

cy Sets	Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.	
Par ↑ ♦ X œ	Status Name Description	
Summary of Policies	Default Default Policy Set	
A list of all your policies	Authentication Policy	
Global Exceptions Rules across entire deployment	MAB : If Wired_MAB OR Allow Protocols : Default Network Access Wireless_MAB	Edit *
Default Default Policy Set	Dot1X : If Wired_802.1X OR Allow Protocols : Default Network Access Wireless_802.1X	Edit *
Save Order Reset Order	Default Rule (If no match) : Allow Protocols : Default Network Access and use : Internal Users	Edt *
	✓ Authorization Policy	
	Authorization Policy Exceptions (0)	
	Authorization Policy Exceptions (0) Standard	
	Authorization Policy Exceptions (0) Standard Status Rule Name Conditions (identity groups and other conditions) Permissions	
	Authorization Policy Exceptions (0) Standard Status Rule Name Conditions (identity groups and other conditions) Permissions @ Wretess Black List Default II Blacklist AND Wretess_Access Den Blackhole_Wretess_Access	Edt
	Authorization Policy Exceptions (0) Standard Status Rule Name Conditions (dentity groups and other conditions) Permissions @ Wretess Black Las Default I Blacklist AND Wretess_Access Pen Blackhole_Viretess_Access @@ Profiled Claco IP Phones II Claco-IP-Phone Pen Claco IP_Phones	Edt Edt
	Authorization Policy Exceptions (0) Standard Status Rule Name Conditions (dentify groups and other conditions) Permissions @ Wreitess Black List Default II Blacklist AND Wreitess_Access then Blackhole_Wireless_Access @ Profiled Claco IP Phones II Claco-IP-Phone then Claco_IP-Phones @ Profiled Non Claco IP Phone II Non_Claco_Profiled_Phones then Non_Claco_IP_Phones @ Profiled Non Claco IP Phone II Non_Claco_Profiled_Phones then Non_Claco_IP_Phones @ Profiled Non Claco IP Phone II Non_Claco_Profiled_Phones then Non_Claco_IP_Phones @ Profiled Non Claco IP Phone II Non_Claco_Profiled_Phones then Non_Claco IP_Phones	Edit Edit Edit
	Authorization Policy Exceptions (0) Standard Stands Rule Name Conditions (identity groups and other conditions) Permissions @ Wretess Black List Default Blacklist AND Wretess Access then Blackhole_Wretess_Access @ Profiled Cisco IP Phones @ Profiled Non Cisco IP Phone @ Profiled Non Cisco IP Phones @ Compliant_Derives_Access If (Network_Access_Authentication_Passed then PermitAccess for PermitAcces fo	Edit Edit Edit Edit
	Authorization Policy Exceptions (0) Standard Status Ruke Name Conditions (dentify groups and other conditions) Permissions @ Wreless Black List Default if Blacklist AND Wireless Access @ Profiled Cool IP Phones @ Profiled Cool IP Phones @ Profiled Non Cisco IP Phone @ Profiled Non Cisco IP Phones @ Compliant_Devices Access # (Network_Access_Authentication_Passed AND Compliant_Devices) @ Employee_EAP-TLS # (Wreless, B02, TX AND BYDD, is, Registered then PermiAccess AND BYDD AND EAP-TLS If (Wreless, AND MAC_In, SN)	Edit Edit Edit Edit Edit
	Authorization Policy Exceptions (0) Standard Status Rule Name Conditions (identity groups and other conditions) Permissions Wretess Black List Default BlackList AND Writess, Access then Blackhole_Writeless_Access Profiled Cisco IP Phones Cisco_IP-Phones Profiled Non Cisco IP Phone res Compliant_Devices_Access If (Network_Access_Authentication_Passed AND Compliant_Devices Compliant_Devices_Access If (Network_Access_Authentication_Passed AND Compliant_Devices Compliant_Devices_Access If (Network_Access_Authentication_Passed AND Compliant_Devices Compliant_Devices Compliant_Devices If (Writeless_B22,1X AND BYNOD ls_Registered AND Compliant_Devices (Writeless_B22,1X AND BYNOD AND Compliant_Devices (Writeless_B22,1X AND BYNOD (Writeless_B22,1X AND	Edit Edit Edit Edit Edit Edit
	Authorization Policy Exceptions (0) Standard Status Rule Name Conditions (dentify groups and other conditions) Permissions @ Wreless Black List Default II Blacklist AND Wreless_Access then Blackhole_Wireless_Access @ Profiled Claco IP Phones II Claco-IP-Phone then Claco IP_Phones @ Profiled Non Claco IP Phone II Non_Claco_Profiled_Phones then Non_Claco_IP_Phones @ Compliant_Devices Access II (Network_Access Authentication_Passed AND Compliant_Devices II (Network_Access II (Network_Access II (Network II AND EAP-TLS AND MACC_III SAN) @ Employee_Onboarding II (Wreless_B02LX AND EAP-MSCHAPv2) then NSP_Onboard AND BYDD @ Wrel_Guast_Access II (Clacet_Flow AND Wreless_MAB) then PermiAccess AND Guasts	Edit Edit Edit Edit Edit Edit
	Authorization Policy Exceptions (0) Standard Status Rule Name Conditions (dentity groups and other conditions) Permissions @ Status Rule Name Conditions (dentity groups and other conditions) Permissions @ Perfield Closo IP Phones @ Profiled Non Closo IP Phones @ Compliant_Devices_Access # (Network_Access_Authentication_Passed AND Compliant_Devices_Access # (Wreless_B021X AND BYOD Is_Registered AND Compliant_Devices_Access # (Wreless_B021X AND EAP-MISCHAPV2) then PermitAccess AND BYOD @ Compliant_Access # (Guest_Flow AND Wreless_MAB) then PermitAccess AND Guests # @ Wreless_MAB PermitAccess AND Closo # (Guest_Flow AND Wreless_MAB PermitAccess AND Closo # Wreless_MAB PermitAccess # Wreless_MAB PermitAccess AND Closo Wreless_MAB PermitAccess AND Closo Wreless_MAB PermitAccess AND Closo Wreless_MAB PermitAccess AND Closo Wreless AND Second Wreless_MAB PermitAccess AND Closo Wreless AND Closo Wreless AND Closo Wreless AND Wreless AND Wreless MAB PermitAccess AND Closo Wreless AND Wreless AND Wreless AND Wreless AND Wreless MAB Wreless Wreless Wreless AND Wreless AND Wreless Wreless Wreless Wreles Wreless MAB Wreless Wreles Wrel	Edit Edit Edit Edit Edit Edit Edit Edit
	Authorization Policy Exceptions (0) Standard Status Rule Name Conditions (identify groups and other conditions) Permissions @ Wreless Black List Default Blacklist AND Wreless_Access then Blackhole_Wireless_Access @ Profiled Cisco IP Phones @ Profiled Cisco IP Phones @ Profiled Non Cisco IP Phone f Compliant_Devices Access if (Network_Access_Authentication_Passed Men PermitAccess AND Compliant_Devices (identify Broups (id	Edit Edit Edit Edit Edit Edit Edit Edit

External_Auth_Policy_Set

External_Auth_Policy_Set

Verify

Apr 19, 2018 07:01:54.570 PM

¥

ò

Step 1. Check ISE live logs if the request is received, as shown in the image.

Step 2. Check if the correct policy set is selected, as shown in the image.

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

Step 3. Check if the request is forwarded to the external RADIUS server.

	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
1	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. If the Continue to Authorization Policy on Access-Accept option is chosen, check if the authorization policy is evaluated.

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

Troubleshoot

Scenario 1. Event - 5405 RADIUS Request Dropped

• The most important thing that must be verified is the steps in the detailed authentication report. If the steps say the "**RADIUS-Client request timeout expired''**, it means that the ISE did not receive any response from the configured external RADIUS server. This can happen when:

- 1. There is a connectivity issue with the external RADIUS server. ISE is unable to reach the external RADIUS server on the ports configured for it.
- 2. ISE is not configured as a Network Device or NAS on the external RADIUS Server.
- 3. Packets are dropped by the external RADIUS Server either by configuration or because of some problem on the external RADIUS server.

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 (11 Step latency=15011 ms)
11356	Failed to forward request to current remote RADIUS server
11353	No more external RADIUS servers; can't perform failover

Check packet captures as well in order to see if it is not a false message; that is, ISE receives the packet back from the server but still reports that the request timed out.

r.	1841 6.537919	10.127.196.80	10.127.196.82	207 RADIUS	Access-Request(1) (id=10, l=165)
	1718 11.542634	10.127.196.80	10.127.196.82	207 RADIUS	Access-Request(1) (id=10, l=165), Duplicate Request
L	2430 16.547029	10.127.196.80	10.127.196.82	207 RADIUS	Access-Request(1) (id=10, l=165), Duplicate Request

• If the steps say "Start forwarding request to remote RADIUS server" and the immediate step is "No more external RADIUS servers; cannot perform failover", it means that all the configured external RADIUS servers are currently marked dead and the requests are only served after the dead timer expires.

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

Note: The default **dead time** for external RADIUS Servers in ISE is **5 minutes**. This value is hardcoded and cannot be modified as of this version.

• If the steps say "**RADIUS-Client encountered error during processing flow**" and are followed by "**Failed to forward request to current remote RADIUS server; an invalid response was received**", it means that ISE has encountered a problem while the request to the external RADIUS server was forwarded. This is usually seen when the RADIUS request sent from the Network Device/NAS to the ISE does not have the **NAS-IP-Address** as one of the attributes. If there is no **NAS-IP-Address** attribute and if external RADIUS servers are not in use, ISE populates the **NAS-IP-Address** field with the source IP of the packet. However, this does not apply when an external RADIUS server is in use.

Scenario 2. Event - 5400 Authentication Failed

• In this event, if the steps say "11368 Please review logs on the External RADIUS Server to determine the precise failure reason", it means that the authentication has failed on the external RADIUS server itself and it has sent an Access-Reject.

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

• If the steps say "**15039 Rejected per authorization profile**", it means that ISE received an Access-Accept from the external RADIUS server but ISE rejects the authorization based on the authorization policies configured.

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

• If the **Failure Reason** on the ISE is anything else apart from the ones mentioned here in case of an authentication failure, then it can mean a potential issue with the configuration or with the ISE itself. A TAC case is recommended to be opened at this point.