在ISE中配置使用OCSP的EAP-TLS身份驗證

目錄

<u>必要條件</u>	
<u>需求</u>	
<u>採用元件</u>	
網路圖表	
<u>C1000中的配直</u>	
Windows PC中的配置	
<u>步驟1.配直使用者身份驗證</u> 止驟2.確認使用者樂運發	
<u>Windows Server中的配置</u>	
<u> 辺駅1.新増代用有</u> 生職2 確認OCSD服務	
<u>少球 1. 但加安直</u> 振聴 2. 新増Active Directory	
步驟3.增加證書身份驗證配置檔案	
<u>────────────────────────────────────</u>	
步驟 5.1SE中的確認證書	
步驟 6.增加允許的協定	
<u>步驟 7.增加策略集</u>	
<u>步驟 8.增加身份驗證策略</u>	
<u>步驟 9.增加授權策略</u>	
<u>步驟 1.確認身份驗證會話</u>	
步驟2.確認Radius即時日誌	
疑難排 <u>解</u>	
<u>1. 調試日誌</u>	
2. TCP轉儲	

簡介

本文檔介紹為即時客戶端證書撤銷檢查設定使用OCSP的EAP-TLS身份驗證所需的步驟。

必要條件

需求

思科建議您瞭解以下主題:

- 思科身份服務引擎的配置
- Cisco Catalyst的配置
- 線上憑證狀態通訊協定

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- 身分辨識服務引擎虛擬3.2修補程式6
- C1000-48FP-4G-L 15.2(7)E9
- Windows Server 2016
- Windows 10

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

網路圖表

下圖顯示本文檔示例中使用的拓撲。



網路圖表

背景資訊

在EAP-TLS中,使用者端將其數位憑證顯示給伺服器,作為驗證程式的一部分。 本文檔介紹ISE如

何透過根據AD伺服器檢查證書公用名(CN)並確認證書是否已使用OCSP(線上證書狀態協定)撤銷 來驗證客戶端證書,OCSP提供即時協定狀態。

在Windows Server 2016上配置的域名是ad.rem-xxx.com,本文檔中用作示例。

本文檔中引用的OCSP(線上證書狀態協定)和AD(Active Directory)伺服器用於證書驗證。

- · Active Directory FQDN : winserver.ad.rem-xxx.com
- CRL分發URL: <u>http://winserver.ad.rem-xxx.com/ocsp-ca.crl</u>
- 授權URL: <u>http://winserver.ad.rem-xxx.com/ocsp</u>

這是憑證鏈結,其中包含檔案中使用的每個憑證的一般名稱。

- CA : ocsp-ca-common-name
- 客戶端證書: clientcertCN
- 伺服器憑證: ise32-01.ad.rem-xxx.com
- OCSP簽名證書: ocspSignCommonName

組態

C1000中的配置

這是C1000 CLI中的最小配置。

aaa new-model

radius server ISE32 address ipv4 1.x.x.181 key cisco123

aaa group server radius AAASERVER server name ISE32

aaa authentication dot1x default group AAASERVER aaa authorization network default group AAASERVER aaa accounting dot1x default start-stop group AAASERVER dot1x system-auth-control

interface Vlan12 ip address 192.168.10.254 255.255.255.0

interface Vlan14
ip address 1.x.x.101 255.0.0.0

interface GigabitEthernet1/0/1
Switch port access vlan 14
Switch port mode access

interface GigabitEthernet1/0/3
switchport access vlan 12
switchport mode access
authentication host-mode multi-auth
authentication port-control auto

dot1x pae authenticator
spanning-tree portfast edge

Windows PC中的配置

步驟 1.配置使用者身份驗證

導覽至Authentication,checkEnable IEEE 802.1X authentication,然後選擇Microsoft:智慧卡或 其他憑證。

按一下「設定」按鈕,選中「使用此電腦上的證書」,然後選擇Windows PC的受信任CA。

pciPassthru0 Properties	× Smart Card or other Certificate Properties ×
Networking Authentication Select this option to provide authenticated network access for this Ethemet adapter. Enable IEEE 802.1X authentication Choose a network authentication method: Microsoft: Smart Card or other certificate Settings	When connecting:
 <u>Remember my credentials for this connection each time I'm logged on</u> <u>Fallback to unauthorized network access</u> <u>Additional Settings</u> 	Trusted <u>R</u> oot Certification Authorities:
	View Certificate Don't prompt user to authorize new servers or trusted certification authorities.
OK Cancel	Use a different user name for the connection

啟用憑證驗證

導覽至Authentication, checkAdditional Settings。從下拉清單中選擇使用者或電腦身份驗證。

pciPassthru0 Properties ×	Advanced settings ×
Networking Authentication	802.1X settings
Select this option to provide authenticated network access for this Ethemet adapter.	Specify authentication mode User or computer authentication Save credentials Delete credentials for all users
Choose a network authentication <u>m</u> ethod: Microsoft: Smart Card or other certificate \checkmark <u>Settings</u>	Enable single sign on for this network Perform immediately before user logon Perform immediately after user logon
 <u>Remember my credentials for this connection each time I'm logged on</u> <u>Fallback to unauthorized network access</u> <u>Additional Settings</u> 	Maximum delay (seconds): Allow additional dialogs to be displayed during single sign on This network uses separate virtual LANs for machine and user authentication
OK Cancel	OK Cancel

指定驗證模式

步驟 2.確認使用者端憑證

導航到證書- Current User > Personal > Certificates,然後檢查用於身份驗證的客戶端證書。

🖀 Console1 - [Console Root\Certificates - Current User\S	Personal\Certificates]							-	
Tile Action View Favorites Window Help									- @ ×
🗢 🔿 🙍 📷 🔏 🗞 🗙 📾 🖬 📆									
Console Root	ssued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te	Actions	
Certificates - Current User	110.71.170.10	tutte	0/14/2024	Contraction of the second s	10.71.170.10			Certificates	
Certificates	clientcertCN	ocsp-ca-common-name	6/4/2025	Client Authentication	ocsp-client			More Actions	•
Trusted Root Certification Authorities								dischool Chi	
Certificates								clientcertory	-
> 🛄 Enterprise Trust								More Actions	•

確認使用者端憑證

按兩下客戶端證書,導航到Details,檢查Subject、CRL分發點、Authority Information Access的詳 細資訊。

- 主題:CN = clientcertCN
- CRL分發點: <u>http://winserver.ad.rem-xxx.com/ocsp-ca.crl</u>
- 授權資訊存取: <u>http://winserver.ad.rem-xxx.com/ocsp</u>



客戶端證書的詳細資訊

Windows Server中的配置

步驟 1.新增使用者

導覽至Active Directory Users and Computers,然後按一下Users。增加clientcertCN作為使用者登入名。

clientcert Civ Properti	es		? ×	clientcert CN Propertie	es		? ×
Member Of	Dial-In	Environment	Sessions	Remote control	Remote [Desktop Services Profile	COM+
Remote control	Remote D	esktop Services Profile	COM+	General Address	Account	Profile Telephones	Organization
General Address	Account	Profile Telephones	Organization	Member Of	Dial-in	Environment	Sessions
User logon name:				Member of:			
clientcertCN		@ad.rem-s_:: em.com	~	Name	Active Direct	ory Domain Services Folder	
User logon name (pre-	Windows 200	0):		Domain Admins	ad rem-s	n.com/Users	
AD)	<u></u>	dientcertCN		Domain Users	ad.rem-s (r	n.com/Users	
Unlock account Account gotions:	ge password a ange password	t next logon	^	44			
Store password Account expires	r expires using reversibl	e encryption	~	Primary group: Do	Semove omain Users There is n	o need to change Primary	group unless

使用者登入名稱

步驟 2.確認OCSP服務

導航到Windows,點選線上響應程式管理。確認OCSP伺服器的狀態。



OCSP伺服器的狀態

按一下winserver.ad.rem-xxx.com,檢查OCSP簽名證書的狀態。

Normal State (Online Responder: winserver.ad.rem-system.com\Array Configuration\winserver.ad.rem-system.com)

File Action View Help			
← ⇒ 21 🛛			
 Online Responder: winserver.ad.rem-s,::h.m.com Revocation Configuration Array Configuration winserver.ad.rem-t_:i.e.n.com 	Revocation Configuration Name ocsp-revocation Revocation Configuration Status Signing Cetificate: Ok Mew Staning Cetificate: Ok Mew Staning Cetificate: Ok Mew Staning Cetificate: Ok	Certificate Certification path Certification gath Certification gath Certificate gatus: This certificate is OK.	X Yew Certificate
	The revocation provider is successfully using	g the current configuration	

OCSP簽名證書的狀態

ISE中的配置

步驟 1.增加裝置

導航到管理>網路裝置,點選增加按鈕,增加C1000裝置。

Cisco ISE				Ac	Iministration • Netw	vork Resources		
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers	External MDM	pxGrid Direct Connectors	Location Services
Network Devices Default Device Device Security Settings	Network Devices List	t > C1000 CeS						
	Namo	C1000						
	Description							
	IP Address	 → (P) 1.10. \(101) 	/					
	Device Profile	# Cisco	~ <u>0</u>					
	Model Name		v					
	Software Versio	n	~					
	Network Device	e Group						
	Location	All Locations	✓ Set To	Default				
	IPSEC	No	✓ Set To	Default				
	Device Type	All Device Types	✓ Set To	Default				
	V RAI	DIUS Authentication Setti	ngs					
	RADIO	is our settings						
	Protoc	ol RADIUS						
	Shared	d Secret cisco123	Hid	•				
		se Second Shared Secret 🕡						

增加裝置

步驟 2.新增Active Directory

導航到管理>外部身份源> Active Directory,點選連線頁籤,將Active Directory增加到ISE。

- 連線點名稱: AD_Join_Point
- Active Directory域: ad.rem-xxx.com

≡ Cisco ISE	Administration - Identity Management
Identities Groups External Ide	Intity Sources Identity Source Sequences Settings
External Identity Sources	Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
	* Join Point Name AD_Join_Point () * Active Directory ad.rem-s_** (n.com ()
	+ Join + Leave 🔉 Test User 🎗 Diagnostic Tool 💋 Refresh Table
CODBC RADIUS Token	ISE Node ^ ISE Node R Status Domain Controller Site
RSA SecurID	ise32-01.ad.rem-sy um.c STANDALONE 🗹 Operational winserver.ad.rem-s, ste Default-First-Site-Na
SAML Id Providers	
🛅 Social Login	

新增Active Directory

導航到組頁籤,從下拉選單中選擇從目錄選擇組。



從目錄選取群組

按一下「擷取群組」下拉式清單。Checkad.rem-xxx.com/Users/Cert Publishers 並按一下確定。

E Cisco ISE		Administra	tion - Identity Management		
Identities Groups External Ide	entity Sources Identity Sc	Select Directory Gro	oups		×
External Identity Sources	Connection Allowed Dom Allowed Dom Allowed Dom Allowed Dom Allowed Dom and an annual and a second and a	This dialog is used to select groups from Domain atzen-s; 1 x.com Name , Fiber Retrieve Groups	SID . Filter ps Retrieved.	Type ALL Filter	
 CORC RADIUS Token RSA SecuriO SAM: Id Providers Social Login 	*	Name Aram-o, / m.com/Users/Aloved I Advem-o; / m.com/Users/Context Advem-o; it m.com/Users/Cont	Crowp SBD COCO Press. 5-1-5-21-4193742415-41 Infers 5-1-5-21-4193742415-41	Group Type 23520024-2046239900MAN LOCAL 23520024-2046239900MAN LOCAL 23520024-2046239900MAN LOCAL 23520024-2046239900MAN LOCAL 23520024-204623990L0MAL 23520024-204623990L0MAL 23520024-204623990L0MAL 23520024-204623990L0MAL 23520024-204623990L0MAL 23520024-204623990L0MAL 23520024-204623990L0MAL	* *

檢查憑證發行者

步驟 3.增加證書身份驗證配置檔案

導航到Administration > External Identity Sources > Certificate Authentication Profile,按一下Add 按鈕以增加新的證書身份驗證配置檔案。

- 名稱:cert_authen_profile_test
- 身份庫: AD_Join_Point
- 使用Identity From Certificate屬性:使用者-一般名稱。
- 將使用者端憑證與辨識存放區中的憑證比對:僅用於解決辨識模糊問題。

Cisco ISE	Administration - Identity Management
Identities Groups External Id	entity Sources Identity Source Sequences Settings
External Identity Sources	Certificate Authentication Profiles List > cert_authen_profile_test Certificate Authentication Profile
<pre>ect_authen_profile_test</pre>	* Name cert_authen_profile_test
Preloaded_Certificate_Prof ∼ ⊂ Active Directory	Description
AD_Join_Point	
🗁 LDAP	
C ODBC	Identity Store AD_Join_Point V
RADIUS Token	
C RSA SecuriD	Use Identity From O Certificate Attribute Subject - Common Name V 🛈
SAML Id Providers	Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)
Social Login	
	Match Client Certificate Against Certificate In Identity Store Only to resolve identity ambiguity Always perform binary comparison

增加證書身份驗證配置檔案

步驟 4.增加身份源隔離

導航到管理>身份源序列,增加身份源序列。

- 名稱 : Identity_AD
- 選取「憑證驗證」 Profile: cert_authen_profile_test
- 身份驗證搜尋清單: AD_Join_Point

Cisco ISE

Identities	Groups	External Identity Sources	Identity Source Sequences	Settings
Identity Source	e Sequences Lis Durce Sequ	t > Identity_AD ence		
∨ Identity *Name	y Source S Ident	equence ity_AD		
Description				
✓ Certifi	icate Based	d Authentication	ithen profile	

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available		Selected	
Internal Endpoints	^	AD_Join_Point	^
Internal Users			
Guest Users			
All_AD_Join_Points			
		3	
	>>		
		Ō	

增加身份源序列

步驟 5.ISE中的確認證書

導航到管理>證書>系統證書,確認伺服器證書由受信任CA簽署。

Cisco ISE	Administration - System	🛕 Evaluation Mode J Days Q 🕥 🖉 🐡
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings	
Certificate Management System Certificates	Default belf-signed saml server cer SAML, SAML_be32-01.ad.rem-sy. um.co SAML_be32-01.ad.rem-sy m.co Thu, ttficate - CN+SAML_be32-01.ad.rem-sy m.co Thu, m m m m m m m m m m m m m m m m m m m	2 May 2024 Tue, 1 May 2029 Z
Trusted Certificates OCSP Client Profile Certificate Signing Requests	CN+1se32-01.ad.rem-#; em.com, ISE Messaging Service Ise32-01.ad.rem-#; i m.com Certificate Services Endpoint Sub C Wed, OU-SEE Messaging ServiceetCentific ads Services Endpoint Sub CA = Ise 32-01800001	, 1 May 2024 Wed, 2 May 2029 Z
Certificate Periodic Check Se	CN+lse32-01.ad.rem-ty_t m.com, Not in use Ise32-01.ad.rem-ty_em.com Certificate Services Endpoint Sub C Wed, OU-Certificate Services System Ce A - Ise32-01	1 May 2024 Wed, 2 May 2029
Certificate Authority	> Int Sub CA - Ise32-01#00002	Active
	CN+lse32-01.ad.rem-#, I Im.comit Purtal Default Portal Certificate Group 🕦 Ise32-01.ad.rem-#) - Im.com rootCACommonName Tue, rootCACommonName#00004	4. Jun 2024 Wed, 4. Jun 2025 C
	Ise-server-cert-friendly-name Admin, CAP () Ise32-01.ad.rem-s xt m.com ocsp-ca-common-name Tue, Authentication, RADIUS OTLS, peOrid, Portal	4 Jun 2024 Wed, 4 Jun 2025 🖬 Active

伺服器憑證

導航到管理>證書> OCSP客戶端配置檔案,按一下「增加」按鈕增加新的OCSP客戶端配置檔案。

- 名稱: ocsp_test_profile
- 配置OCSP響應程式URL: <u>http://winserver.ad.rem-xxx.com/ocsp</u>

■ Cisco ISE	Administration - System	
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access S	ettings
Certificate Management System Certificates Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Se	Edit OCSP Profile * Name ocsp_test_profile Description	
Certificate Authority >	 Server Connection Enable Secondary Server Always Access Primary Server First Failback to Primary Server After Interval 5 Minutes () 	
	V Primary Server Validate Response Signature Validate Response Signature	Condary Server http:// Enable Nonce Extension Support Validate Response Signature
	Use OCSP URLs specified in Authority Information Access (AIA) Enable Nonce Extension Support Validate Response Signature	
	✓ Response Cache * Cache Entry Time To Live 1440 Minutes ⊙ Clear Cache	
OCSP客戶端配置檔案		

導航到管理>證書>受信任證書,確認受信任CA已導入到ISE。

Cisco ISE				Administra	tion - System				Evaluation Mode 11 Days Q	05	,7
Deployment Licensing	Certificate	s Logging Maintenance	Upgrade Health	Checks Bac	kup & Restore Admin A	ccess Settings					
		Cisco Manufacturing CA SHA2	Infrastructure	02	Cisco Manufacturing CA SH	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2	Enabled		10
Certificate Management \sim		Cisco Root CA 2048	Endpoints Infrastructure	5F F8 7B 28 2	Cisco Root CA 2048	Cisco Root CA 2048	Sat, 15 May 2004	Tue, 15 May 2 (Disabled		
System Certificates		Cisco Root CA 2099	Cisco Services	01 9A 33 58 7	Cisco Root CA 2099	Cisco Root CA 2099	Wed, 10 Aug 2016	Mon, 10 Aug 8	Enabled		
Trusted Certificates OCSP Client Profile		Cisco Root CA M1	Cisco Services	2E D2 0E 73 4	Cisco Root CA M1	Cisco Root CA M1	Wed, 19 Nov 2008	Sat, 19 Nov 2	Enabled		
Certificate Signing Requests		Cisco Root CA M2	Infrastructure Endpoints	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2	Enabled		
Certificate Periodic Check Se		Cisco RXC-R2	Cisco Services	01	Cisco RXC-R2	Cisco RXC-R2	Thu, 10 Jul 2014	Mon, 10 Jul 2	Enabled		
Certificate Authority		CN=root_ca_common_name, OU=cisc	Infrastructure Cisco Services Endpoints AdminAuth	20 BF 12 86 F	root_ca_common_name	root_ca_common_name	Thu, 16 May 2024	Tue, 16 May 2	Enabled		
	0	CN=rootCACommonName#rootCACom	Infrastructure Cisco Services Endpoints AdminAuth	21 31 D3 DE	rootCACommonName	rootCACommonName	Tue, 4 Jun 2024	Sun, 4 Jun 20	Enabled		
		Default self-signed server certificate	Endpoints Infrastructure	37 66 FC 29	ise32-01.ad.rem-system.com	ise32-01.ad.rem-system.com	Thu, 2 May 2024	Sat, 2 May 20	Enabled		
		DigiCert Global Root CA	Cisco Services	08 3B E0 56 9	DigiCert Global Root CA	DigiCert Global Root CA	Fri, 10 Nov 2006	Mon, 10 Nov	Enabled		
		DigiCert Global Root G2 CA	Cisco Services	03 3A F1 E6	DigiCert Global Root G2	DigiCert Global Root G2	Thu, 1 Aug 2013	Fri, 15 Jan 20	Enabled		
		DigiCert root CA	Endpoints Infrastructure	02 AC 5C 26	DigiCert High Assurance EV	DigiCert High Assurance EV	Fri, 10 Nov 2006	Mon, 10 Nov	Enabled		
		DigiCert SHA2 High Assurance Server	Endpoints Infrastructure	04 E1 E7 A4	DigiCert SHA2 High Assuran	DigiCert High Assurance EV	Tue, 22 Oct 2013	Sun, 22 Oct 2	Enabled		
		IdenTrust Commercial Root CA 1	Cisco Services	0A 01 42 80 0	IdenTrust Commercial Root	IdenTrust Commercial Root	Fri, 17 Jan 2014	Tue, 17 Jan 2	2 Enabled		
		ocsp-ca-friendly-name	Cisco Services Endpoints	1A 12 1D 58	ocsp-ca-common-name	ocsp-ca-common-name	Tue, 4 Jun 2024	Sun, 4 Jun 20 🚦	2 Enabled		

受信任的CA

選中CA並按一下Edit按鈕,輸入OCSP配置的詳細資訊以進行證書狀態驗證。

- 根據OCSP服務進行驗證:ocsp_test_profile
- 如果OCSP返回UNKNOWN狀態,則拒絕請求:檢查
- 如果OCSP響應程式無法訪問,則拒絕請求:檢查

Cisco ISE	Administration - System								
Deployment Licensing	Certificates Logging Maintena	ance Upgrade Health Checks	Backup & Restore	Admin Access	Settings				
Certificate Management System Certificates Trusted Certificates OCSP Client Profile Certificate Signing Requests Certificate Periodic Check Se	* Friendly Name ocs Status I Description	p-ca-friendly-name							
Certificate Authority >	Valid From Tue, Valid From Tue, Valid To (Expiration) Sun, Serial Number 1A 1 Signature Algorithm SHA2 Key Length 2048	csp-ca-common-name 4 Jun 2024 13:52:00 JST 4 Jun 2034 13:52:00 JST 2 1D 58 59 6C 75 18 256withRSA							
	Truse Truse T Certificate Status Validation	d For: () hust for authentication within ISE Trust for client authentication and Syslog Trust for certificate based admin auther hust for authentication of Clisco Services	ntication						
	To vi OCS	arify certificates, enable the methods below P Configuration Validate against OCSP Service ocsp_test_pre Reject the request if OCSP returns UNKNOW Reject the request if OCSP Responder is un ficate Revocation List Configuration Download CRL	v. If both are enabled, OCSP o ofile N status eachable	will always be tried first.					
		CRL Distribution URL Retrieve CRL Every	ally 5	Minutes Hours	before expiration.				
憑證狀態驗證		If download failed, wait 10	Minute	s v	before retry.				

步驟 6.增加允許的協定

導航到策略>結果>身份驗證>允許的協定,編輯預設網路訪問服務清單,然後選中允許EAP-TLS。

Cisco ISE

Policy · Policy Elements

Dictionaries C	onditions	Results
Authentication Allowed Protocols	×	Allowed Protocols Services List > Default Network Access Allowed Protocols
Authorization	>	Name Default Network Access
Profiling	>	Description Default Allowed Protocol Service
Posture	>	
Client Provisioning	>	V Allowed Protocols
		Authentication Bypass Process Host Lookup Authentication Protocols Authentication Protocols Allow CHAP Allow S-CHAPv1 Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy Allow EAP-TLS Proactive session ticket update will occur after 90 Allow LAP PEAP Inner Methods Allow EAP-MS-CHAPv2 Allow EAP-MS-CHAPv2 Allow PEAPv2 Allow PEAPv2 Allow EAP-GTC Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy Allow EAP-TLS PEAP Inner Methods Allow EAP-GTC Allow PEAPv2 Allow PEAPv0 only for legacy clients



步驟 7.增加策略集

導航到策略>策略集,點選+增加策略集。

- 策略集名稱: EAP-TLS-Test
- 條件:網路訪問協定等於RADIUS
- 允許的協定/伺服器序列:預設網路訪問

≡ Cisco ISE	Policy - Policy Sets	🛕 Evaluation Mode :) Days Q 💿 🖼 🚳
Policy Sets	Reset Reset Policyset Hitcounts Save	
Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q. Search		
Edillizion	2 Network Access Protocol EQUALS RADIUS	Default Network Access 🥒 + 🤧 🚳 🕨

增加策略集

步驟 8.增加身份驗證策略

導航到策略集,點選EAP-TLS-Testto增加身份驗證策略。

- 規則名稱: EAP-TLS-Authentication
- 條件:網路訪問EapAuthentication 等於EAP-TLS 和Wired_802.1 X
- 使用:Identity_AD

Status Rule Name Conditions Use Hits Action Q. Search	✓ Authentication Policy (2)				
Q Search Identity_AD	Status Rule Name	Conditions	Use	Hits	Actions
Identity_AD /	Q Search				
Network Access-EapAuthentication EQUALS EAP-TLS		2 Network Access Esplantmentication EQUALS EAP-TLS	Identity_AD		
EAP-TLS-Authentication AND Wred_602.1X Options 26	EAP-TLS-Authentication	AND B Wired_602.1X	> Options	26	¢

增加身份驗證策略

步驟 9.增加授權策略

導航到策略集,點選EAP-TLS-Test增加授權策略。

- 規則名稱: EAP-TLS-Authorization
- 條件:證書使用者-公用名等於clientcertCN
- 結果:PermitAccess

\sim Authoriza	tion Policy (2)					
			Results			
 Stat 	tus Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Se	arch					
٩	EAP-TLS-Authorization	L CERTIFICATE Subject - Common Name EQUALS clientcentCN	PermitAccess	+ Select from list	+ 17	\$

增加授權策略

驗證

步驟 1.確認身份驗證會話

運行show authentication sessions interface GigabitEthernet1/0/3 details命令,確認C1000中的身份驗證會話。

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/3 details

Interface: GigabitEthernet1/0/3 MAC Address: b496.9114.398c IPv6 Address: Unknown IPv4 Address: 192.168.10.10 User-Name: clientcertCN Status: Authorized Domain: DATA Oper host mode: multi-auth Oper control dir: both Session timeout: N/A Restart timeout: N/A Periodic Acct timeout: N/A Session Uptime: 111s Common Session ID: 01C20065000000933E4E87D9 Acct Session ID: 0x00000078 Handle: 0xB6000043 Current Policy: POLICY_Gi1/0/3 Local Policies:

Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies:

Method status list: Method State

dot1x Authc Success

步驟 2.確認Radius即時日誌

在ISE GUI中導航到操作> RADIUS >即時日誌,確認身份驗證的即時日誌。

■ Cisco ISE		Operations · RADIUS	A Evaluation Mode 70 Da	ya Q 🖉 🖗
Live Logs Live Sessions				
Misconfigured Supplicants 📀	Misconfigured Network Devices 🕕	RADIUS Drops 🕡	Client Stopped Responding 🕠	Repeat Counter ①
0	0	0	0	0
\mathcal{O} . Seaset Repeat Counts . In Export To \vee			Refresh Show Never V Latest 50 reco	
Time Status	Details Repea Identity	Endpoint ID Endpoint Authentication Policy	Authorization Policy Authorization	IP Address
×	V Identity	Endpoint ID Endpoint Pr Authentication Policy	Authorization Policy Authorization	Pi IP Address 🗸
Jun 05, 2024 09:43:36.3 🔵	a 0 clientcertCN	84:96:91:14:3 Intel-Device EAP-TLS-Test >> EAP-TLS-Authentication	EAP-TLS-Test >> EAP-TLS-Authorization PermitAccess	192.168.10.10
Jun 05, 2024 09:43:33.2	Q clientcertCN	84:96:91:14:3 Intel-Device EAP-TLS-Test >> EAP-TLS-Authentication	EAP-TLS-Test >> EAP-TLS-Authorization PermitAccess	

Radius即時日誌

確認身份驗證的詳細即時日誌。

Cisco ISE

Overview				
Event	5200 Authentication succeeded			
Username	clientcertCN			
Endpoint Id	B4:96:91:14:39:8C ①			
Endpoint Profile	Intel-Device			
Authentication Policy	EAP-TLS-Test >> EAP-TLS-Authentication			
Authorization Policy	EAP-TLS-Test >> EAP-TLS-Authorization			
Authorization Result	PermitAccess			

Authentication Details

Source Timestamp	2024-06-05 09:43:33.268
Received Timestamp	2024-06-05 09:43:33.268
Policy Server	ise32-01
Event	5200 Authentication succeeded
Username	clientcertCN
Endpoint Id	B4:96:91:14:39:8C
Calling Station Id	B4-96-91-14-39-8C
Endpoint Profile	Intel-Device
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C20065000000933E4E87D9
Other Attributes	
ConfigVersionId	167
DestinationPort	1645
Protocol	Radius
NAS-Port	50103
Framed-MTU	1500
State	37CPMSessionID=01C2006500000933E4E87D9;31SessionI D=ise32-01/506864164/73;
AD-User-Resolved-Identities	clientcertCN@ad.rem-s;=:em.com
AD-User-Candidate- Identities	clientcertCN@ad.rem-sy:.tem.com
TotalAuthenLatency	324
ClientLatency	80
AD-User-Resolved-DNs	CN=clientcert CN,CN=Users,DC=ad,DC=rem- strictem,DC=com
AD-User-DNS-Domain	ad.rem-sy:tem.com
AD-User-NetBios-Name	AD
IsMachineldentity	false
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy:::+m.com
AD-User-SamAccount-Name	clientcertCN
AD-User-Qualified-Name	clientcertCN@ad.rem-sy*t:.m.com
TLSCipher	ECDHE-RSA-AES256-GCM-SHA384
TLSVersion	TLSv1.2
DTLSSupport	Unknown
Subject	CN=clientcertCN

CN+ocsp-ca-common-name

11001 Received RADIUS Access-Request 11017 RADIUS created a new session 15049 Evaluating Policy Group 15008 Evaluating Service Selection Policy 11507 Extracted EAP-Response/Identity 12500 Prepared EAP-Request proposing EAP-TLS with challenge 12625 Valid EAP-Key-Name attribute received 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request 11018 RADIUS is re-using an existing session 12502 Extracted EAP-Response containing EAP-TLS challengeresponse and accepting EAP-TLS as negotiated 12800 Extracted first TLS record; TLS handshake started 12545 Client requested EAP-TLS session ticket The EAP-TLS session ticket received from supplicant 12542 while the stateless session resume is disabled. Performing full authentication 12805 Extracted TLS ClientHello message 12806 Prepared TLS ServerHello message 12807 Prepared TLS Certificate message 12808 Prepared TLS ServerKeyExchange message 12809 Prepared TLS CertificateRequest message 12810 Prepared TLS ServerDone message 12505 Prepared EAP-Request with another EAP-TLS challenge 11006 Returned RADIUS Access-Challenge 11001 Received RADIUS Access-Request

Steps

- 11018 RADIUS is re-using an existing session
- 12504 Extracted EAP-Response containing EAP-TLS challengeresponse
- 12988 Take OCSP servers list from OCSP service configuration certificate for clientcertCN
- 12550 Sent an OCSP request to the primary OCSP server for the CA - External OCSP Server
- 12553 Received OCSP response certificate for clientcertCN 12554 OCSP status of user certificate is good - certificate for clientcertCN
- 12811 Extracted TLS Certificate message containing client certificate
- 12812 Extracted TLS ClientKeyExchange message
- 12813 Extracted TLS CertificateVerify message
- 12803 Extracted TLS ChangeCipherSpec message

24432 Looking up user in Active Directory - AD_Join_Point 24325 Resolving identity - clientcertCN

- 24313
 Search for matching accounts at join point ad.remsr. imm.com

 24319
 Single matching account found in forest - ad.remsr. :-m.com

 24323
 Identity resolution detected single matching account
- 24700
 Identity resolution by certificate succeeded -AD_Join_Point

 22037
 Authentication Passed

 12506
 EAP-TLS authentication succeeded

 24715
 ISE has not confirmed locally previous successful machine authentication for user in Active Directory

 15036
 Evaluating Authorization Policy

 24209
 Looking up Endpoint in Internal Endpoints IDStore tionarce
- 24209 clientcertCN 15036 Evaluating Authorization Policy 24209 Looking up Endpoint in Internal Endpoints IDStore clientcertCN 24211 Found Endpoint in Internal Endpoints IDStore
- 15016 Selected Authorization Profile PermitAccess
- 22081 Max sessions policy passed
- 22080 New accounting session created in Session cache
- 11503 Prepared EAP-Success
- 11002 Returned RADIUS Access-Accept

Issuer

Crypto,2024-06-05 09:43:33,064,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, CryptoLib.CSSL.OCSP Callback -

starting OCSP request to primary

,SSL.cpp:1444 Crypto,2024-06-05 09:43:33,064,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Start processing OCSP request

,

URL=<u>http://winserver.ad.rem-xxx.com/ocsp</u>

, use nonce=1,0cspClient.cpp:144

Crypto, 2024-06-05 09:43:33, 104, DEBUG, 0x7f9822961700, NIL-CONTEXT, Crypto::Result=0, Crypto.0cspClient::pe

Received OCSP server response

,0cspClient.cpp:411 Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.0cspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, Crypto.OcspClient::pe

User certificate status: Good

,OcspClient.cpp:598
Crypto,2024-06-05 09:43:33,104,DEBUG,0x7f9822961700,NIL-CONTEXT,Crypto::Result=0, CryptoLib.CSSL.OCSP C

perform OCSP request succeeded

, status: Good,SSL.cpp:1684

// Radius session
Radius,2024-06-05 09:43:33,120,DEBUG,0x7f982d7b9700,cntx=0000017387,sesn=ise32-01/506864164/73,CPMSessi

Code=1(AccessRequest)

Identifier=238 Length=324
[1] User-Name - value: [

clientcertCN

] [4] NAS-IP-Address - value: [1.x.x.101] [5] NAS-Port - value: [50103] [24] State - value: [37CPMSessionID=01C20065000000933E4E87D9;31SessionID=ise32-01/506864164/73;] [87] NAS-Port-Id - value: [GigabitEthernet1/0/3]

Radius, 2024-06-05 09:43:33, 270, DEBUG, 0x7f982d9ba700, cntx=0000017387, sesn=ise32-01/506864164/73, CPMSessi

Code=2(AccessAccept)

Identifier=238 Length=294
[1] User-Name - value: [clientcertCN]

Radius, 2024-06-05 09:43:33, 342, DEBUG, 0x7f982d1b6700, cntx=0000017401, sesn=ise32-01/506864164/74, CPMSessie

Code=4(AccountingRequest)

```
Identifier=10 Length=286
[1] User-Name - value: [clientcertCN]
[4] NAS-IP-Address - value: [1.x.x.101]
[5] NAS-Port - value: [50103]
[40] Acct-Status-Type - value: [Interim-Update]
[87] NAS-Port-Id - value: [GigabitEthernet1/0/3]
[26] cisco-av-pair - value: [audit-session-id=01C2006500000933E4E87D9]
[26] cisco-av-pair - value: [method=dot1x] ,RADIUSHandler.cpp:2455
```

Radius, 2024-06-05 09:43:33, 350, DEBUG, 0x7f982e1be700, cntx=0000017401, sesn=ise32-01/506864164/74, CPMSessi

Code=5(AccountingResponse)

Identifier=10 Length=20,RADIUSHandler.cpp:2455

2. TCP轉儲

在ISE中的TCP轉儲中,您會發現有關OCSP響應和Radius會話的資訊。

OCSP請求和響應:

No.	Time	Identification	Source	S.Port Destination	D.Port Time to	Live Protocol	Length T	CP.Se Next se 1	CP.Ac Info
+	140 2024-06-05 00:43:33.093523	0x0295 (661)	1.1181	25844 1.1 1	80	64 OCSP	262	1 197	1 Request
•	141 2024-06-05 00:43:33.104108	0x0117 (279)	1.1 2 0.57	80 1.1 181	25844	128 OCSP	1671	1 1607	197 Response

OCSP請求和響應的資料包捕獲

>	Frame 141: 1671 bytes on wire (13368 bits), 1671 bytes captured (13368 bits)							
>	Ethernet II, Src: VMware_98:c9:91 (00:50:56:98:c9:91), Dst: VMware_98:57:1c (00:50:56:98:57:1c)							
>	Internet Protocol Version 4, Src: 1.1 . 1.57, Dst: 1.131.1.181							
>	Transmission Control Protocol, Src Port: 80, Dst Port: 25844, Seq: 1, Ack: 197, Len: 1605							
>	Hypertext Transfer Protocol							
v	Online Certificate Status Protocol							
	responseStatus: successful (0)							
	✓ responseBytes							
	ResponseType Id: 1.3.6.1.5.5.7.48.1.1 (id-pkix-ocsp-basic)							
	> BasicOCSPResponse							
	✓ tbsResponseData							
> responderID: byKey (2)								
	producedAt: Jun 5, 2024 09:43:33.000000000							
	✓ responses: 1 item							
	✓ SingleResponse							
	> certStatus: good (0)							
	chisopoace: Jun 4, 2024 16:05:00.000000000							
	nextUpdate: Jul 4, 2024 16:05:00.000000000							
	✓ responseExtensions: 1 item							

擷取OCSP回應的詳細資訊

Radius會話:

146 2024-06-05 00:43:33.118175	0x9bc6 (39878)	1.100.101	67181 1.1 7 J. 181	1645	255 RADIUS	366	Access-Request id=238
185 2024-06-05 00:43:33.270244	0x033d (829)	1.1	67181 1	1645	64 RADIUS	336	Access-Accept id=238
187 2024-06-05 00:43:33.341233	0x9bc7 (39879)	1.1	1646 1	1646	255 RADIUS	328	Accounting-Request id=10
188 2024-06-05 00:43:33.350936	0x037a (890)	1.10181	1646 1.:)101	1646	64 RADIUS	62	Accounting-Response id=10
267 2024-06-05 00:43:36.359621	0x9bc8 (39880)	1.704.4.101	1646 1.134.3.181	1646	255 RADIUS	334	Accounting-Request id=11
268 2024-06-05 00:43:36.369035	0x0489 (1161)	1.1 1.1.181	1646 1.174 1.101	1646	64 RADIUS	62	Accounting-Response id=11

Radius會話的資料包捕獲

相關資訊

配置使用ISE的EAP-TLS身份驗證

在ISE中配置TLS/SSL證書

關於此翻譯

思科已使用電腦和人工技術翻譯本文件,讓全世界的使用者能夠以自己的語言理解支援內容。請注 意,即使是最佳機器翻譯,也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準 確度概不負責,並建議一律查看原始英文文件(提供連結)。