Configuration de l'authentification EAP-TLS avec OCSP dans ISE

Table des matières

Introduction
Conditions préalables
Exigences
Composants utilisés
Diagramme du réseau
Informations générales
Configurations
Configuration dans C1000
Configuration dans le PC Windows
Étape 1. Configurer l'authentification utilisateur
Étape 2. Confirmer le certificat client
Configuration dans Windows Server
Étape 1. Ajouter des utilisateurs
Étape 2. Confirmer le service OCSP
Configuration dans ISE
Étape 1. Ajouter un périphérique
Étape 2. Ajouter Active Directory
Étape 3. Ajouter un profil d'authentification de certificat
Étape 4. Ajouter une séquence source d'identité
Étape 5. Confirmer le certificat dans ISE
Étape 6. Ajouter des protocoles autorisés
Étape 7. Ajouter un jeu de stratégies
Étape 8. Ajouter une stratégie d'authentification
Étape 9. Ajouter une stratégie d'autorisation
Vérifier
Étape 1. Confirmer la session d'authentification
Étape 2. Confirmer le journal Radius en direct
Dépannage
1. Journal de débogage
2. Dépôt TCP
Informations connexes

Introduction

Ce document décrit les étapes requises pour configurer l'authentification EAP-TLS avec OCSP pour les contrôles de révocation de certificat client en temps réel.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Cisco Identity Services Engine
- Configuration de Cisco Catalyst
- Protocole d'état de certificat en ligne

Composants utilisés

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Correctif 6 d'Identity Services Engine Virtual 3.2
- C1000-48FP-4G-L 15.2(7)E9
- Windows Server 2016
- Windows 10

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Diagramme du réseau

Cette image présente la topologie utilisée pour l'exemple de ce document.



Informations générales

Dans EAP-TLS, un client présente son certificat numérique au serveur dans le cadre du processus d'authentification. Ce document décrit comment l'ISE valide le certificat client en vérifiant le nom commun (CN) du certificat par rapport au serveur AD et en confirmant si le certificat a été révoqué à l'aide du protocole OCSP (Online Certificate Status Protocol), qui fournit l'état du protocole en temps réel.

Le nom de domaine configuré sur Windows Server 2016 est ad.rem-xxx.com, qui est utilisé comme exemple dans ce document.

Les serveurs OCSP (Online Certificate Status Protocol) et AD (Active Directory) référencés dans ce document sont utilisés pour la validation des certificats.

- · Nom de domaine complet Active Directory : winserver.ad.rem-xxx.com
- URL de distribution CRL : <u>http://winserver.ad.rem-xxx.com/ocsp-ca.crl</u>
- URL de l'autorité : <u>http://winserver.ad.rem-xxx.com/ocsp</u>

Il s'agit de la chaîne de certificats avec le nom commun de chaque certificat utilisé dans le document.

- CA : ocsp-ca-common-name
- Certificat client : clientcertCN
- Certificat du serveur : ise32-01.ad.rem-xxx.com
- Certificat de signature OCSP : ocspSignCommonName

Configurations

Configuration dans C1000

Il s'agit de la configuration minimale de l'interface de ligne de commande C1000.

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

Configuration dans le PC Windows

Étape 1. Configurer l'authentification utilisateur

Accédez àAuthentication, cochezEnable IEEE 802.1X authentication et sélectionnez Microsoft : Smart Card or other certificate.

Cliquez sur le bouton Paramètres, cochez la case Utiliser un certificat sur cet ordinateur, puis sélectionnez l'autorité de certification approuvée du PC Windows.

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	When connecting: Use my gmart card Image: State on this computer Advanced Image: Use simple certificate selection (Recommended) Image: State Sta
Choose a network authentication method: Microsoft: Smart Card or other certificate	Connect to these servers (examples:srv1;srv2;:*\srv3\com):
Bemember my credentials for this connection each time I'm logged on Eallback to unauthorized network access Additional Settings	Trusted Boot Certification Authorities:
	View Certificate Don't grompt user to authorize new servers or trusted certification authorities.
OK Cancel	Use a different user name for the connection

Activer l'authentification du certificat

Accédez àAuthentification, cochezParamètres supplémentaires. Sélectionnez Authentification utilisateur ou ordinateur dans la liste déroulante.

pciPassthru0 Properties ×	Advanced settings ×
Networking Authentication Select this option to provide authenticated network access for this Ethemet adapter.	802. 1X settings Specify authentication mode User or computer authentication ∨ Save credentials Delete credentials for all users
Choose a network authentication method: Microsoft: Smart Card or other certificate Settings Bemember my credentials for this connection each time I'm logged on Eallback to unauthorized network access Adgitional Settings	 Enable single sign on for this network Perform immediately before user logon Perform immediately after user logon Maximum delay (seconds): 10 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

Spécifier le mode d'authentification

Étape 2. Confirmer le certificat client

Accédez à Certificates - Current User > Personal > Certificates, et vérifiez le certificat client utilisé pour l'authentification.

	🖀 Console1 - [Console Root\Certificates - Current L	Use	er\Personal\Certificates]							-		×
1	🖀 File Action View Favorites Window He	ielp	, ,								-	8 ×
Ī	Console Boot	•]	Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Name	Status	Certificate Te	Actions		
	Personal Certificates		ClientcertCN	ocsp-ca-common-name	6/4/2025	Client Authentication	ocsp-client			Certificates More Actions		•
	 Trusted Root Certification Authorities Certificates 									clientcertCN More Actions		-
I	> Enterprise Trust											

Confirmer le certificat client

Double-cliquez sur le certificat client, accédez à Details, vérifiez les détails de Subject, CRL Distribution Points, Authority Information Access.

- Objet : CN = clientcertCN
- Points de distribution CRL : <u>http://winserver.ad.rem-xxx.com/ocsp-ca.crl</u>
- Accès aux informations d'autorité : <u>http://winserver.ad.rem-xxx.com/ocsp</u>



Détail du certificat client

Configuration dans Windows Server

Étape 1. Ajouter des utilisateurs

Accédez à Utilisateurs et ordinateurs Active Directory, puis cliquez surUtilisateurs. Ajoutez clientcertCN en tant que nom de connexion utilisateur.

			?	×	clientcert CN Properti	es			?	>
Member Of	Dial-In	Environment	Sess	ions	Remote control	Remote I	Desktop Serv	vices Profile	CO	M+
Remote control	Remote D	esktop Services F	rofile C	OM+	General Address	Account	Profile	Telephones	Organiz	zation
General Address	Account	Profile Telep	hones Orga	nization	Member Of	Dial-in	Enviro	onment	Session	ns
User logon name:		-			Member of:					
clientcertCN		@ad.rem-s, : i sr	n.com	\sim	Name	Active Direct	ory Domain S	Services Folder		
User logon name (pre-	Windows 2000	D):		_	Domain Admins	ad rem-s	m.com/Users	3		
AD\		clientcertCN			Domain Users	ad.rem-s; (r	m.com/Users	s		
Cooperin Sheround.										
User must chan	ge password al ange password rexpires using reversibl	t next logon I e encryption		^	Add I Primary group: D	Gemove	us pased to ob	hange Dimose c		_
User must chan User cannot cha Password never Store password Account expires Never	ge password a ange password r expires using reversibl	t next logon I e encryption		~	Add	Bemove	no need to ch Macintosh c	hange Primary g	group unle	ess t
User must chan User cannot chi Password never Store password Account expires Never End of:	ge password a ange password rexpires using reversibl Friday .	t next logon e encryption July 5, 2024	4 Dig 1	•	Add I Primary group: D	emove	no need to ch Macintosh c ns.	hange Primary g dients or POSID	group unle (-complian	ess

Nom de connexion utilisateur

Étape 2. Confirmer le service OCSP

Accédez à Windows, cliquez sur Gestion des répondeurs en ligne. Confirmez l'état du serveur OCSP.



État du serveur OCSP

Cliquez sur winserver.ad.rem-xxx.com, vérifiez l'état du certificat de signature OCSP.

No. 10 Configuration winserver.ad.rem-system.com/Array Configuration/winserver.ad.rem-system.com

File Action View Help			
💠 🔿 🖄 🛛			
 Online Responder: winserver.ad.rem-s,::1um.com Revocation Configuration Array Configuration winserver.ad.rem-i_i.e.m.com 	Revocation Configuration Name	Certificate Certification Path Certification gath Certification gath Certificate gatus: This certificate is OK.	X Vew Certificate
	Revocation Configuration Status		OK
	Type: Microsoft CRL-based revocation statu The revocation provider is successfully using	is provider g the current configuration	

État du certificat de signature OCSP

Configuration dans ISE

Étape 1. Ajouter un périphérique

Accédez à Administration > Network Devices, cliquez sur Addbutton pour ajouter un périphérique

C1000.

					Adr	ministration · Netw	ork Resources		
Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Se	rvers RADIUS Server S	equences	NAC Managers	External MDM	pxGrid Direct Connectors	Location Services
Network Devices Default Device Device Security Settings	Network Devices List	> c1000 es							
	Namo	C1000							
	Description								
	IP Address	 **P: 1.10. \.101 	/ 32 🔍						
	Device Profile	# Cisco	× 0						
	Model Name		~						
	Software Version		~						
	Network Device	Group							
	Location	All Locations	~	Set To Default					
	IPSEC	No	~ :	Set To Default					
	Device Type	All Device Types	~	Set To Default					
	🔽 🗸 RAD	IUS Authentication Setti	ngs						
	RADIU	S UDP Settings							
	Protoco Shared	RADIUS Secret cisco123 e Second Shared Secret 0		Hide					

Étape 2. Ajouter Active Directory

Accédez à Administration > Sources d'identité externes > Active Directory, cliquez sur l'onglet Connexion, ajoutez Active Directory à ISE.

- Nom du point de jointure : AD_Join_Point
- Domaine Active Directory : ad.rem-xxx.com

■ Cisco ISE	Administration - Identity Management
Identities Groups External Ide	entity Sources Identity Source Sequences Settings
External Identity Sources	Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
< E	Join Point Name AD_Join_Point
Active Directory AD_Join_Point	* Active Directory ad.rem-s_tin.com
LDAP	+ Join + Leave A Test User 🎗 Diagnostic Tool 📿 Refresh Table
RADIUS Token	ISE Node ^ ISE Node R Status Domain Controller Site
C RSA SecurID	ise32-01.ad.rem-sy wm.c STANDALONE 🛛 Operational winserver.ad.rem-s, ste Default-First-Site-Na
SAML Id Providers	
Social Login	

Ajouter Active Directory

Ajouter un périphérique

Accédez à l'onglet Groups, sélectionnez Select Groups From Directory dans la liste déroulante.

≡ Cisco ISE		Administration - Identity Management					
Identities Groups	External Identity Sources	Identity Source Sequences	Settings				
External identity Sources < Image: Control of Co	s Connection	Allowed Domains PassiveID	Groups Attributes ID Values SID	Advanced Settings			

Sélectionner des groupes dans le répertoire

Cliquez sur la liste déroulante Récupérer des groupes. Checkad.rem-xxx.com/Users/Cert Publishers et cliquez sur OK.

E Cisco ISE		Administration - Identity Management	
Identities Groups External Ide	entity Sources Identity Sc	Select Directory Crowne	×
		Select Directory Groups	
External Identity Sources	Connection Allowed Dom	This dialog is used to select groups from the Directory.	
		Domain adzen-oj t k.com	
) 🗇 Certificate Authentication I	7.0. 7.0. 7.0	Name, SID, Type ALL	
Active Directory	Name	Fiber Fiber	
1 AD_Join_Point	ad.rem-system.com	Review Groups	
C LOAP		Name Group SID Group Type	
C000C		ad rem-ts; / m.com/Users/Alowed RODO Pass. 5-1-5-21-4193743415-4133520026-20442399. DOMAIN LOCAL	^
C RADIUS Token		ad new with moon/Users/Cert Publishers 5-1-5-21-2192742415-2132520226-20442309 DOMAN LOCAL	
C RSA Securio		ad rem-errs in conf/berry/Donestie Donesin C. 5-1-5-21-4193743415-4133530026-30482399. 0L084L	
C SAME to Providers			
Social Login			
		adver-sy inconvolutionalities 5-1-0-21-4182202110-412202000-20462299. DOMAN LOCAL	
		ad.rem:s i pm.com/Uners/Dev/JodeteProxy 5-1-5-21-4193742415-4133520026-20462299 GL08AL	
	<	ad rem-e,m.com/Users/Domain Admins 5-1-5-21-6193393815-6133520026-30462209. 0L08AL	1 - I
		ad rem-sr 11 m.com/Uwen/Domain Computers 5-1-5-21-4193742415-4133520026-20462299 GL084L	
		ad.rem-syr x .com/Users/Domain Controllers 5-1-5-21-4193743415-4133520026-30442299 GL084L	
		ad.vem-ey,.n. n.com/Users/Domain Guests 5-1-5-21-4193743415-4133520026-30482399. GLOBAL	
		ad.rem-e- 1 m.com/Uners/Domain Users 5-1-5-21-4193342415-4133520026-20442209. 0L084L	
		()	÷
		Cancel	ĸ

Vérifier les éditeurs de certificats

Étape 3. Ajouter un profil d'authentification de certificat

Accédez à Administration > External Identity Sources > Certificate Authentication Profile, cliquez sur le bouton Add pour ajouter un nouveau profil d'authentification de certificat.

- Nom : cert_authen_profile_test
- Magasin d'identités : AD_Join_Point
- Utiliser L'Identité De L'Attribut De Certificat : Objet Nom Commun.
- Faire correspondre le certificat client avec le certificat dans le magasin d'identités :

uniquement pour résoudre l'ambiguïté d'identité.

≡ Cisco ISE		Administration - Identity Management
Identities Groups External Id	entity Sources Identity S	Source Sequences Settings
External Identity Sources	Certificate Authentication Profile Certificate Authenticat	s List > cert_authen_profile_test
2 cert_authen_profile_test	* Name	cert_authen_profile_test
2 Preloaded_Certificate_Prof	Description	
Active Directory		
AD_Join_Point		http://www.analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/analysis.com/ana
t LDAP		
DDBC	Identity Store	AD_Join_Point V
RADIUS Token		
E RSA SecurID	Use Identity From	 Certificate Attribute Subject - Common Name O
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	Newer Only to resolve identity ambiguity Always perform binary comparison

Ajouter un profil d'authentification de certificat

Étape 4. Ajouter une séquence source d'identité

Accédez à Administration > Identity Source Sequences, ajoutez une Identity Source Sequence.

- Nom : Identity_AD
- Sélectionnez Certificate Authentication Profile: cert_authen_profile_test
- Liste de recherche d'authentification : AD_Join_Point

Cisco ISE

Identities	Groups	External Identity Sou	rces Identity Sour	ce Sequences	Settings
Identity Source	e Sequences List ource Seque	> Identity_AD			
✓ Identity * Name Description	y Source Se Identit	quence			
					li.
∨ Certifi v Se	icate Based	Authentication	cert_authen_profil~]	
✓ Auther A s	ntication Se et of identity s	arch List purces that will be access	sed in sequence until firs	t authentication st	succeeds
	Available		Selected		
	Internal Endpo	nts	AD_Join_Point	^	
	Guest Users				
	All_AD_Join_F	oints			2
				Ē	
		>> (∑ ¥

Ajouter des séquences source d'identité

Étape 5. Confirmer le certificat dans ISE

Accédez à Administration > Certificates > System Certificates, confirmez que le certificat du serveur est signé par l'autorité de certification approuvée.

■ Cisco ISE	Administration - System	🛕 Evaluation Mode I (Days Q 🛛 💭
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Access Settings	
Certificate Management ~ System Certificates	Default self-signed sami server cer SAML_ iss22-01.ad.rem-syum.co SAML_iss22-01.ad.rem-sy. m.co Thu, 2 May 2024 trifeate - CN+SAML_iss22-01.ad.re m m-sym.com	Tue, 1 May 2029
Trusted Certificates OCSP Client Profile Certificate Signing Requests	CN-Ise32-01.ad.rem-ty: tm.com, ISE Messaging Service ise32-01.ad.rem-ty: tm.com Certificate Services Endpoint Sub C: Wed, 1 May 2024 OU-ISE Messaging ServiceMCertific add Services Endpoint Sub C: A - ise 32-01m00001	Wed, 2 May 2029 2 Active
Certificate Periodic Check Se Certificate Authority >	CN-Ise32-01.ad.rem-5j. t.m.com, Not In use ise32-01.ad.rem-5j. em.com Cartificate Services Endpoint Sub C. Wed, 1 May 2024 OU-Certificate Services Stytem Ce 118/Certificate Services Endpoint Sub C. Wed, 1 May 2024 A - Ise32-01 Int Sub CA - Ise32-01800002	Wed, 2 May 2029 Zactive
	CN-Ise32-01.ad.rem-1, i sm.comit Portal Default Portal Certificate Group 🕠 Ise32-01.ad.rem-1; i m.com rootCACommonName Tue, 4 Jun 2024	Wed, 4 Jun 2025
	Ise-server-cert-friendly-name Admin, EAP () Ise32-01.ad.rem-s.it.m.com ocsp-ca-common-name Tue, 4 Jun 2024 Authentication, RADiuts DTLS, packrid, Portall	Wed, 4 Jun 2025

certificat du serveur

Accédez à Administration > Certificates > OCSP Client Profile, cliquez sur Add button to add a

new OCSP client profile.

- Nom : ocsp_test_profile
- Configurer l'URL du répondeur OCSP : <u>http://winserver.ad.rem-xxx.com/ocsp</u>

≡ Cisco ISE	Administration - System	
Deployment Licensing	Certificates Logging Maintenance Upgrade Health Checks Backup & Restore Admin Acces	ss Settings
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 () 	
	VIRL http:// r.ad.rem-t_;s'sm.com/ocspl Lable Nonce Extension Support Validate Response Signature Use OCSP URLs specified in Authority Information Access (AIA)	✓ Secondary Server URL http:// ☑ Enable Nonce Extension Support ☑ Validate Response Signature
	Enable Nonce Extension Support Validate Response Signature	

Profil du client OCSP

Accédez à Administration > Certificates > Trusted Certificates, confirmez que l'autorité de certification approuvée est importée vers ISE.

Cisco ISE				Administra	tion - System				Evaluation Mode	Days Q	0	<u>, a</u>
Deployment Licensing	Certificates Logging	Maintenance U	Jpgrade Health	Checks Bac	kup & Restore Admin A	ccess Settings						
	Cisco Manufac	turing 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			1
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	Enabled			
Trusted Certificates OCSP Cilent 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			1
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_co	ommon_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			L
	CN=rootCACor	nmonName#rootCACom	Infrastructure Cisco Services Endpoints AdminAuth	21 31 D3 DE	rootCACommonName	rootCACommonName	Tue, 4 Jun 2024	Sun, 4 Jun 20	Enabled			L
	Default self-sig	aned 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 38 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 C	A	Endpoints Infrastructure	02 AC 5C 26	DigiCert High Assurance EV	DigiCert High Assurance EV	Fri, 10 Nov 2006	Mon, 10 Nov	Enabled			1
	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 Com	mercial Root CA 1	Cisco Services	0A 01 42 80 0	IdenTrust Commercial Root	IdenTrust Commercial Root	Fri, 17 Jan 2014	Tue, 17 Jan 2	Enabled			
	ocsp-ca-friend	lly-name	Cisco Services Endpoints	1A 12 1D 58	ocsp-ca-common-name	ocsp-ca-common-name	Tue, 4 Jun 2024	Sun, 4 Jun 20	Enabled			

Autorité de certification approuvée

Vérifiez l'autorité de certification et cliquez sur le bouton Edit, entrez les détails de la configuration OCSP pour la validation de l'état du certificat.

- Validation par rapport au service OCSP : ocsp_test_profile
- Rejeter la demande si OCSP renvoie l'état UNKNOWN : vérifier
- Rejeter la demande si le répondeur OCSP est inaccessible : vérifier

Cisco ISE				Admi	inistration - System			
Deployment Licensing	Certificates	Logging Ma	aintenance Upgrade	Health Checks	Backup & Restore	Admin Access	Settings	
	Issuer							
Certificate Management V								
System Certificates		* Friendly Name	ocsp-ca-friendly-name					
Trusted Certificates			-					
OCSP Client Profile		Status	Enabled V					
Certificate Signing Requests		Description						
Certificate Periodic Check Se		6.No.						
		Subject	CN=ocsp-ca-common-name					
Certificate Authority >		Issue	CN=ocsp-ca-common-name					
		Valid From	Tue, 4 Jun 2024 13:52:00 JST					
		Valid To (Expiration)	Sun, 4 Jun 2034 13:52:00 JST	r:				
		Serial Number	1A 12 1D 58 59 6C 75 1B					
		Signature Algorithm	SHA256withRSA					
		Key Length	2048					
	Usage							
			Trusted For:					
			Trust for authentication within	ISE				
			Trust for client authentica	tion and Syslog				
			Trust for certificate	based admin authentic	cation			
			Trust for authentication of Cisc	to Services				
	Certificate	Status Validation	1					
			To verify certificates, enable the	he methods below. I	f both are enabled, OCSP	will always be tried fir	st.	
			OCSP Configuration					
			Validate against OCSP Servic	 ocsp_test_profi 	le ~			
			Reject the request if OC	SP returns UNKNOWN	status			
			Reject the request if OC	SP Responder is unrea	chable			
			Certificate Revocation List C	onfiguration				
			Download CRL					
			CRL Distribution URL					
			Retrieve CRL	 Automatical 	N 5	Minutes	~	before expiration.
				O Every	1	Hours	~	
							had an anti-	
			If download failed, w	ant 10	Minut	105	oerore retry.	

Validation du statut du certificat

Étape 6. Ajouter des protocoles autorisés

Accédez à Policy > Results > Authentication > Allowed Protocols, modifiez la liste de services Default Network Access et cochez la case Allow EAP-TLS.

Cisco ISE

Policy · Policy Elements

Automication Automication Automication Proting Petiting Petiting Citient Provisioning		
Nuthorization Protiling Posture Citient Provisioning Citient Provisioning <th>Authentication V A Allowed Protocols</th> <th>Allowed Protocols Services List > Default Network Access Allowed Protocols</th>	Authentication V A Allowed Protocols	Allowed Protocols Services List > Default Network Access Allowed Protocols
Protiling Posture Cilient Provisioning Allowed Protocols Authentication Bypass Process House Lookup Authentication Protocols Allow AMPA/ASCII Allow K3-CHAPv1 Allow K3-CHAPv2 Allow K3-CHAPv1 Allow K3-CHAPv2 Allow K3-CHAPv3 Allow K3-CHAPv3<!--</th--><th>Authorization ></th><th>Name Default Network Access</th>	Authorization >	Name Default Network Access
Postare Citeret Provisioning	Profiling >	Description Default Allowed Protocol Service
Citent Provisioning Allowed Protocols Authentication Bypass Process Host Lookup () Authentication Protocols Allow AP/ASCII Allow CHAP Allow MS-CHAPv1 Allow AS-CHAPv2 Allow EAP-MDS I allow Authentication of expired certificates to allow certificate renewal in Authorization Policy () Enable Stateless Session Resume Session ticket time to live Proactive session ticket update will occur after 90 % of Time To Live has expired Allow LEAP Allow PEAP Allow PEAP Allow PEAP Allow PEAP-GTC Allow PAP-GTC Allow EAP-GTC Allow EAP-GTC Allow EAP Allow Password Change Retries 1 (Valid Range 0 to 3) Allow EAP-GTC Allow EAP-GTC Allow EAP Allow EAP-GTC Allow EAP Allow EAP Allow EAP Allow EAP Allow EAP-GTC Allow EAP Allow Password Change Retries 1 (Valid Range 0 to 3) <li< th=""><th>Posture ></th><th></th></li<>	Posture >	
Allow Password Change Retries 1 (Valid Range 0 to 3)	Client Provisioning	Allowed Protocols Authentication Bypass Process Host Lookup () Authentication Protocols Allow AP/ASCII Allow MS-CHAPV1 Allow MS-CHAPv1 Allow MS-CHAPv2 Allow MS-CHAPv1 Allow MS-CHAPv2 Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy () Enable Stateless Session Resume Session ticket time to live 2 Hours Proactive session ticket update will occur after 90 % of Time To Live has expired Allow FAP Allow EAP Session ticket update will occur after 90 % of Time To Live has expired Allow EAP Allow FAP-MS-CHAPv2 Allow Allow FAP Allow EAP V Allow EAP-MS-CHAPv2 Image: Allow FAP-MS-CHAPv2 Image: Allow FAP-GTC Image: Allow FAP-TIS Image: Allow FAP-TIS Image: Allow FAP-TIS Image: Allow FAP-TIS Image: Allow FAP-GTC Image: Allow FAP-TIS Image: Allow FAP-TIS Image: Allow FAP-GTC
Allow PEAPv0 only for legacy clients		Allow PEAPv0 only for legacy clients

Autoriser EAP-TLS

Étape 7. Ajouter un jeu de stratégies

Accédez à Policy > Policy Sets, cliquez sur + pour ajouter un jeu de stratégies.

- · Nom du jeu de stratégies : EAP-TLS-Test
- Conditions : Le protocole d'accès au réseau ÉGALE RADIUS
- · Protocoles autorisés / Séquence de serveurs : Accès réseau par défaut

≡ Cisco ISE	Policy - Policy Sets	▲ Evaluation Mode :) Days Q ③ 53 ◎			
Policy Sets Reset Policyset Hitcounts					
Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View			
Q Search					
Satuliainu	2 Network Access Protocol EQUALS RADIUS	Default Network Access 🥒 + 75 🔅 🕻			

Ajouter un jeu de stratégies

Étape 8. Ajouter une stratégie d'authentification

Accédez à Jeux de stratégies, cliquez sur EAP-TLS-Test pour ajouter une stratégie d'authentification.

- Nom de la règle : EAP-TLS-Authentication
- Conditions : Accès réseau EAPauthentication ÉGALE EAP-TLS ET Wired_802.1 X
- Utiliser : Identity_AD

Status Rule Name Conditions Use Hits Action Q Search Identity_AD Identit	I	V Authentication Policy (2)				
Q Search		(Status Rule Name	Conditions	Use	Hits	Actions
Identity_AD		Q Search				
A FAD TO A MANAGEMENT AND			D Network Access EstAuthentication EDUALS EAP-TLS	Identity_AD		
B Wred_602.1X > Options		EAP-TLS-Authentication	AND B Wired_602.1X	> Options	26	傪

Ajouter une stratégie d'authentification

Étape 9. Ajouter une stratégie d'autorisation

Accédez à Jeux de stratégies, cliquez sur EAP-TLS-Test pour ajouter une stratégie d'autorisation.

- · Nom de la règle : EAP-TLS-Authorization
- · Conditions : CERTIFICAT Objet Nom commun EQUALS clientcertCN
- Résultats : PermitAccess

\sim Authorization Polic	y (2)					
			Results			
💽 Status Ru	e Name Conditions		Profiles	Security Groups	Hits	Actions
Q Search						
EA	CERTIFICATE-Subject - Common Name	EQUALS clientcertCN	PermitAccess	A + Select from list	<i>⊘</i> + 17	٩

Ajouter une stratégie d'autorisation

Vérifier

Étape 1. Confirmer la session d'authentification

Exécutezshow authentication sessions interface GigabitEthernet1/0/3 details la commande pour confirmer la session d'authentification dans C1000.

<#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: 01C2006500000933E4E87D9 Acct Session ID: 0x00000078 Handle: 0x86000043 Current Policy: POLICY_Gi1/0/3 Local Policies: Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150) Server Policies: Method status list: Method status list: Method State dot1x Authc Success

Étape 2. Confirmer le journal Radius en direct

Accédez à **Operations > RADIUS > Live Login** ISE GUI, confirmez le journal en direct pour l'authentification.

■ Cisco ISE		Operations · RADIUS	A Evaluation Mode TJ Days	Q () 🕫 🕸
Live Logs Live Sessions				
Misconfigured Supplicants 🕕	Misconfigured Network Devices 🕕	RADIUS Drops 🕢	Client Stopped Responding 🕕	Repeat Counter 🕕
0	0	0	0	0
경 - 는 Reset Repeat Counts - 쇼 Export To \vee			Refresh Show Never V Latest 50 reco_V	v Within Last 24 hours v Filter ∨ ⊗
Time Status	Details Repea Identity	Endpoint ID Endpoint Authentication Policy	Authorization Policy Authorizatio	IP Address
×	V Identity	Endpoint ID Endpoint Pr Authentication Policy	Authorization Policy Authorization Pr	IP Address 🗸 🗸
Jun 05, 2024 09:43:36.3	O 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	clientcentCN	84:96:91:14:3 Intel-Device EAP-TLS-Test >> EAP-TLS-Authentication	EAP+TLS-Test >> EAP+TLS+Authorization PermitAccess	

Journal Radius Live

Confirmez le journal en direct détaillé de l'authentification.

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

Steps 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 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 ClientKevExchange 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.rems' em.com 24319 Single matching account found in forest - ad.rem-sr. tom.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 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

Détail de l'authentification

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. Dépôt TCP

Dans le dump TCP dans ISE, vous vous attendez à trouver des informations sur la réponse OCSP et la session Radius.

Requête et réponse OCSP :

No.	Time	Identification	Source	S.Port Destination	D.Port Time to L	ve Protocol	Length T(CP.Se Next se 1	TCP.Ac Info
+	140 2024-06-05 00:43:33.093523	0x0295 (661)	1.1181	25844 1.: H	80	64 OCSP	262	1 197	1 Request
+	141 2024-06-05 00:43:33.104108	0x0117 (279)	1.1 7 9.57	80 1.1	25844	128 OC5P	1671	1 1607	197 Response

Capture de paquets de requête et réponse OCSP

> > .	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)						
2	Internet Protocol Version 4, Src: 1.: . 0.57, Dst: 1.13181						
>	ransmission Control Protocol, Src Port: 80, Dst Port: 25844, Seq: 1, Ack: 197, Len: 1605						
> Hypertext Transfer Protocol							
\sim	nline 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 09:43:33,00000000						
	V neconnest 1 (tem						
	V SingleBernonse						
	* Singlenesponse						
	<pre>> certStatus: good (0) thisopdate: Jun 4, 2024 16:05:00.000000000 nextUpdate: Jul 4, 2024 16:05:00.000000000</pre>						
	<pre> v responseExtensions: 1 item </pre>						

Capturer les détails de la réponse OCSP

Session Radius :

146 2024-06-05 00:43:33.118175	0x9bc6 (39878)	1.100.101	67181 1.17	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)	1.1.1.1.1.101	1646 1	1646	255 RADIUS	328	Accounting-Request id=10
188 2024-06-05 00:43:33.350936	0x037a (890)	1.17181	1646 1.:)101	1646	64 RADIUS	62	Accounting-Response id=10
267 2024-06-05 00:43:36.359621	0x9bc8 (39880)	1.004.4.101	1646 1.1J4.J.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

Capture de paquets de session Radius

Informations connexes

Configuration de l'authentification EAP-TLS avec ISE

Configuration des certificats TLS/SSL dans ISE

À propos de cette traduction

Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.