Konfigurieren der Zwei-Faktor-Authentifizierung für den Supplicant-Zugriff

Inhalt

Einleitung					
<u>Voraussetzungen</u>					
Anforderungen					
Verwendete Komponenten					
Netzwerkdiagramm					
Hintergrundinformationen					
Konfigurationen					
Konfiguration in C1000					
Konfiguration auf Windows-PCs					
Schritt 1: PC zur AD-Domäne hinzufügen					
Schritt 2: Benutzerauthentifizierung konfigurieren					
Konfiguration in Windows Server					
Schritt 1: Domänencomputer bestätigen					
Schritt 2: Domänenbenutzer hinzufügen					
Konfiguration in der ISE					
Schritt 1: Gerät hinzufügen					
Schritt 2: Active Directory hinzufügen					
Schritt 3: Einstellungen für die Computerauthentifizierung bestätigen					
Schritt 4: Identitätsquellensequenzen hinzufügen					
Schritt 5: DACL und Autorisierungsprofil hinzufügen					
Schritt 6: Policy Set hinzufügen					
Schritt 7. Authentifizierungsrichtlinie hinzufügen					
Schritt 8: Autorisierungsrichtlinie hinzufügen					
Überprüfung					
Muster 1. Systemauthentifizierung und Benutzerauthentifizierung					
Schritt 1: Abmelden von Windows-PC					
Schritt 2: Authentifizierungssitzung bestätigen					
Schritt 3: Windows-PC anmelden					
Schritt 4: Authentifizierungssitzung bestätigen					
Schritt 5: RADIUS-Live-Protokoll bestätigen					
Muster 2. Nur Benutzerauthentifizierung					
Schritt 1: Deaktivieren und Aktivieren der Netzwerkkarte von Windows PC					
Schritt 2: Authentifizierungssitzung bestätigen					
Schritt 3: RADIUS-Live-Protokoll bestätigen					
Fehlerbehebung					
Zugehörige Informationen					

Einleitung

In diesem Dokument werden die erforderlichen Schritte zur Konfiguration der Zwei-Faktor-Authentifizierung mit Computer- und Punkt1x-Authentifizierung beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Konfiguration der Cisco Identity Services Engine
- Konfiguration des Cisco Catalyst
- IEEE 802.1X

Verwendete Komponenten

- Identity Services Engine Virtual 3.3 Patch 1
- C1000-48FP-4G-L 15,2(7)E9
- Windows Server 2019

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Netzwerkdiagramm

Dieses Bild zeigt die Topologie, die für das Beispiel dieses Dokuments verwendet wird.

Der unter Windows Server 2019 konfigurierte Domänenname ist ad.rem-xxx.com. Dies wird in diesem Dokument als Beispiel verwendet.



Netzwerkdiagramm

Hintergrundinformationen

Die Systemauthentifizierung ist ein Sicherheitsprozess, der die Identität eines Geräts überprüft, das Zugriff auf ein Netzwerk oder System benötigt. Im Gegensatz zur Benutzerauthentifizierung, bei der die Identität einer Person anhand von Anmeldeinformationen wie Benutzername und Kennwort überprüft wird, konzentriert sich die Computerauthentifizierung auf die Validierung des Geräts selbst. Dies geschieht häufig mithilfe digitaler Zertifikate oder Sicherheitsschlüssel, die für das Gerät einzigartig sind.

Durch die kombinierte Verwendung von Computer- und Benutzerauthentifizierung kann ein Unternehmen sicherstellen, dass nur autorisierte Geräte und Benutzer auf sein Netzwerk zugreifen können, wodurch eine sicherere Umgebung geschaffen wird. Diese Zwei-Faktor-Authentifizierungsmethode ist besonders nützlich, um vertrauliche Informationen zu schützen und strenge gesetzliche Vorschriften einzuhalten.

Konfigurationen

Konfiguration in C1000

Dies ist die minimale Konfiguration in C1000 CLI.

aaa new-model

```
radius server ISE33
address ipv4 1.x.x.191
```

key cisco123

aaa group server radius AAASERVER server name ISE33

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 Vlan14
ip address 1.x.x.101 255.0.0.0

interface GigabitEthernet1/0/1
switchport access vlan 14
switchport mode access

interface GigabitEthernet1/0/2
switchport access vlan 14
switchport mode access
authentication host-mode multi-auth
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge

Konfiguration auf Windows-PCs

Schritt 1: PC zur AD-Domäne hinzufügen

Navigieren Sie zu Systemsteuerung > System und Sicherheit, klicken Sie auf System, und klicken Sie dann auf Erweiterte Systemeinstellungen. Klicken Sie im Fenster Systemeigenschaften auf Ändern, wählen Sie Domäne aus, und geben Sie den Domänennamen ein.

System and Security		About		
← → · ↑ 🌯 › Control Panel › System and Security	~ õ	Your PC is	monitored and protected.	Related settings
Control Panel Home Security and Mainter	ance	See details in V	Vindows Security	BitLocker settings
System and Security Review your computer's star Troubleshoot common con	tus and resolve issues 🔰 🌍 Change User Account Control settings 👘			Device Manager
Network and Internet Hardware and Sound Windows Defender F	irewall	Device spe	cifications	Remote desktop
Programs Check firewall status All	ow an app through Windows Firewall	Device name	DESKTOP-L2IL9I6	System protection
User Accounts System Appearance and See the name of this comp Personalization	rocessor speed 😻 Allow remote access Launch remote assistance .ter	Processor	Intel(R) Xeon(R) CPU E7-4820 v3 @ 1.90GHz 1.90 GHz (2 processors)	Advanced system settings
System Properties X	Computer Name/Domain Changes X			
Computer Name Hardware Advanced System Protection Remote Windows uses the following information to identify your computer	You can change the name and the membership of this computer. Changes might affect access to network resources.			
Computer description:	DESKTOP-L2IL9I5			
For example: "Kitchen Computer" or "Mary's Computer". Full computer name: DESKTOP-L2IL9/6	Ful computer name: DESKTOP-L2IL9I6			
Workgroup: WORKGROUP	More			
To use a wizard to join a domain or workgroup, click Network ID	Member of © Domain: ad rem r, st m.com			
To rename this computer or change its domain or Change	Workgroup: WORKGROUP			

PC zur AD-Domäne hinzufügen

Geben Sie im Fenster Windows-Sicherheit den Benutzernamen und das Kennwort des Domänenservers ein.

Windows Security	×	Computer Name/Domain Changes	×	Computer Name/Domain Changes
Computer Name/Domain	Changes	Welcome to the ad.zem-s 7 tm.com domain.		You must restart your computer to apply these changes
Enter the name and password of an	account with permission to			Before restarting, save any open files and close all
join the domain.		OK	1	programs.
administrator				ОК
•••••	•			
ОК	Cancel			

Benutzername und Kennwort eingeben

Schritt 2: Benutzerauthentifizierung konfigurieren

Navigieren Sie zu Authentication (Authentifizierung), und aktivieren Sie das Kontrollkästchen Enable IEEE 802.1X authentication. Klicken Sie im Fenster Protected EAP Properties auf Settings (Einstellungen), deaktivieren Sie Verify the server's identity by validating the certificate, und klicken Sie dann auf Configure. Aktivieren Sie im Fenster Eigenschaften von EAP MSCHAPv2 die Option Windows-Anmeldename und -Kennwort (und ggf. Domäne) automatisch verwenden, um den bei der Windows-Computeranmeldung eingegebenen Benutzernamen für die Benutzerauthentifizierung zu verwenden.



Benutzerauthentifizierung aktivieren

Navigieren Sie zu Authentifizierung, und aktivieren Sie Zusätzliche Einstellungen. Wählen Sie Benutzer- oder Computerauthentifizierung aus der Dropdown-Liste aus.

🖗 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
Choose a network authentication method: Microsoft: Protected EAP (PEAP) Remember my credentials for this connection each time I'm logged on Fallback to unauthorized network access Additional Settings	Delete credentials for all users 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

Authentifizierungsmodus angeben

Konfiguration in Windows Server

Schritt 1: Domänencomputer bestätigen

Navigieren Sie zu Active Directory-Benutzer und -Computer, und klicken Sie auf Computer. Vergewissern Sie sich, dass Win10 PC1 in der Domäne aufgeführt ist.



Domänencomputer bestätigen

Schritt 2: Domänenbenutzer hinzufügen

Navigieren Sie zu Active Directory-Benutzer und -Computer, und klicken Sie auf Benutzer. Fügen Sie testuser als Domänenbenutzer hinzu.



Domänenbenutzer hinzufügen

Fügen Sie den Domänenbenutzer einem Mitglied von Domänenadministratoren und Domänenbenutzern hinzu.

test user Properties			? ×	test user Properties				?	×
Member Of Remote control	Dial-in Remote (Environment	Sessions	Remote control	Remote	Desktop Se	rvices Profile	00	M+
General Address	Account	Profile Telephones	Organization	Member Of	Dial-in	Envi	ronment	Sessio	ns
User logon name:				Member of:					
testuser		@ad.rem-6,si.sm.com	~	Name	Active Direct	ory Domain	Services Folder		
User logon name (pre-	Windows 200	0):		Domain Admins	ad rem-sylling	m.com/Use	rs		
AD\		testuser		Domain Users	ad.rem-sy-1.r	m.com/Use	rs		
Account gotions:	ge password a ange password expires using reversibl	t next logon d le encryption	*	Add E Primary group: D	Gemove omain Users There is r	to need to a	change Primary (youp unit	
Never End of:	Thursday ,	June 6, 2024	.	Set Primary Group	you have applicatio	Macintosh ns.	clients or POSIJ	(-compilar	¢
0	ĸ	Cancel Apply	Help	0	K (Cancel	Apply	Н	вþ

Konfiguration in der ISE

Schritt 1: Gerät hinzufügen

Navigieren Sie zu Administration > Network Devices, und klicken Sie auf Add (Hinzufügen), um ein C1000-Gerät hinzuzufügen.

≡	diada Identity Services	Engine			Administration / Net	work Resources	
Щ	Bookmarks	Network Devices	Network Device Groups	Network Device Profiles	External RADIUS Servers	RADIUS Server Sequences	NAC Managers
	Dashboard	Network Devices	Network Device	List > C1000			
18	Context Visibility	Device Security Settings	Network De	vices			
*	Operations		Name	C1000			
0	Policy		Description				
20	Administration						
nii:	Work Centers			* 10 -	1		
			B' Addres	1.1.1.0.101	7 32 🐵		
?	Interactive Help						
			Device Profi	e de Cisco	<u> </u>		
			Model Name		~		
			Software Ve	sion	~		
			Network Dev	ice Group			
			Location	All Locations	Set To D	efault	
			IPSEC	No	✓ Set To D	efault	
			Device Type	All Device Types	Set To D	efault	
			22.00 1990				
			🗹 🗸 R/	ADIUS Authentication Settin	ngs		
			RADI	US UDP Settings			
			Proto	col RADIUS			
			Share	d Secret cisco123	Hide		

Gerät hinzufügen

Schritt 2: Active Directory hinzufügen

Navigieren Sie zu Administration > External Identity Sources > Active Directory, klicken Sie auf die Registerkarte Connection, und fügen Sie Active Directory zur ISE hinzu.

- Verknüpfungspunkt-Name: AD_Join_Point
- Active Directory-Domäne: ad.rem-xxx.com

=	diala Identity Services I	gine Administration / Identity Management
н	Bookmarks	entities Groups External Identity Sources Identity Source Sequences Settings
	Dashboard	
1H	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	Certificate Authenticat Join Point Name AD_Join_Point
-0	Policy	Active Directory * Active Directory ad.rem-st L.m.com
2.	Administration	AD_Join_Point

Active Directory hinzufügen

Navigieren Sie zur Registerkarte Gruppen, und wählen Sie Gruppen aus Verzeichnis aus der Dropdown-Liste aus.

	alialia cisco Identity Services E	Engine	Administration / Identity Management
Щ	Bookmarks	Identities Groups External Ident	ty Sources Identity Source Sequences Settings
-	Dashboard		
망	Context Visibility	External Identity Sources	Connection Allowed Domains PassiveID Groups Attributes Advanced Settings
*	Operations	Certificate Authenticat	C Edit + Add - Delete Group Update SID Values
0	Policy	Active Directory	Select Groups From Directory
å 0	Administration	AD_Join_Point	Add Group Control Assist ad.rem-sy im.com/S-1-5-32-579

Gruppen aus Verzeichnis auswählen

Klicken Sie auf Gruppen aus Dropdown-Liste abrufen. Aktivieren Sie ad.rem-

xxx.com/Users/Domain Computers and ad.rem-xxx.com/Users/Domain Users, und klicken Sie auf OK.

≡	the intervices	Engine		×	4
н	Bookmarks	Identities Groups E	Select Directory Groups		
-	Dashboard	C Centricale At C Active Directo	This dialog is used to select groups from the Directory. Domain at rem-s 1 m com		
18	Context Visibility	1 AD_Join_Poin	Name, SD, Type ALL		
*	Operations	CI LOAP	Retrieve Groups	_	
0	Policy	C RADUS Triter			
3.	Administration	CI RSA SecuriD	Name Group SID Group SID		
ų.	Work Centers	CI SAM, Id Provide	ad remove the same Charles Decision and the same set of the State	<u>~</u>	
		C Social Login	ad rem-a), "em.com/Users/Domain Admins 5-1-5-21-4113/N2415-4133130028-20482398. GLOBAL		
	Interactive Help		ad nem-sp. 1. m. com/Users/Domain Computers 5-1-5-21-41192742415-4130320026-20442299 04/0844		
			al removes stum complement Connectors 5+1-5-21-61182742415-4132828028-20482398 GLOBAL		
			ad rem-s, ir im com/Uwen/Domain Guess 5-1-5-21-4110742415-413052028-20482299 GLOBAL		
			ad rem-ray - J.m. Lem/Weens/Domain Viens 5+1+5+21+4190742415+4100920028+20482099 6L0844		
			ad rem-e; / m.com/Users/Cherginal Admins 5-1-5-21-6133192415-4133120028-20482398. UNIVDRSAL		
			ad rem-ej ir m.com/Uners/Emergelies Kay Adminis 5-1-5-21-41103142415-4130120124-20482308. UNIVDRSAL		
			advenue, straces/Nees/Deeplee Readvery. 5-1-5-21-0193N24/5-413312028-20482998. UNVDRAL	- 1 H	
			ad rem-ay, am com/comm/Croup Petry Craster 5-1-5-21-4183/12415-4133(2020-2042299 6L084L		
			4		
			Cancel		



Schritt 3: Einstellungen für die Computerauthentifizierung bestätigen

Navigieren Sie zur Registerkarte Erweiterte Einstellungen, und bestätigen Sie die Einstellung der Computerauthentifizierung.

- Computerauthentifizierung aktivieren: So aktivieren Sie die Computerauthentifizierung
- Aktivieren der Einschränkung des Computerzugriffs: So kombinieren Sie Benutzer- und Computerauthentifizierung vor der Autorisierung



Hinweis: Der gültige Bereich für die Alterungszeit liegt zwischen 1 und 8760.

≡	diale Identity Services E	Engine Administration / Identity Management	A Evaluation Mode
щ	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings	
53	Dashboard		
망	Context Visibility	External Identity Sources Connection Allowed Domains PassiveID Groups Attributes Advanced Settings	
×	Operations	Cartificate Authenticat	
.0	Policy	Cachine Directory Fachine Description	
80	Administration	AD_Join_Point Schable Machine Authentication	
ก็เ	Work Centers	LDAP Enable Machine Access Restrictions ODBC Aging Time 5 hours ()	
?	Interactive Help	C RADIUS Token Machine Access Restrictions Cache will be replicated between PSN instances in each node group. C RSA SecurID To configure MAR Cache distribution groups: Administration > System > Deployment	
		SAML Id Providers Enable dial-in check Social Login Enable callback check for dial-in clients Use Kerberos for Plain Text Authentications	

Einstellungen für die Computerauthentifizierung

Schritt 4: Identitätsquellensequenzen hinzufügen

Navigieren Sie zu Administration > Identity Source Sequences, und fügen Sie eine Identity Source Sequence hinzu.

- Name: Identity_AD
- Authentifizierungs-Suchliste: AD_Join_Point

≡	dentity Services	ngine Administration / Identity Management
Щ	Bookmarks	Identities Groups External Identity Sources Identity Source Sequences Settings
-	Dashboard	Identity Source Sequences List > Identity_AD
1d	Context Visibility	Identity Source Sequence
~%	Operations	
0	Policy	V Identity Source Sequence
80	Administration	Identity_AD
đ.	Work Centers	Description
?	Interactive Help	✓ Certificate Based Authentication
		Select Certificate Authentication 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

Schritt 5: DACL und Autorisierungsprofil hinzufügen

Navigieren Sie zu Richtlinie > Ergebnisse > Autorisierung > Herunterladbare ACLs, und fügen Sie eine DACL hinzu.

- Name: MAR_Passed
- DACL Content: permit ip any host 1.x.x.101 and permit ip any host 1.x.x.105

$\equiv \frac{1}{1000}$ Identity S	Services Engine	Policy / Policy Elements
Bookmarks	Dictionaries Conditions	Results
Dashboard	Authentication	> Downloadable ACL List > MAR_Passed
III Context Visibility	Authorization	Downloadable ACL
X Operations	Authorization Profiles	E Mano MAR Parend
Policy	Downloadable ACLs	Description
▲ Administration	Profiling	> ID varaine
Work Centers	Posture	Approximation and the second sec
	Client Provisioning	891011 permit ip any host 1.13 - 0.151 2131415 3131415

DACL hinzufügen

Navigieren Sie zu Richtlinie > Ergebnisse > Autorisierung > Autorisierungsprofile, und fügen Sie ein Autorisierungsprofil hinzu.

- Name: MAR_Passed
- DACL-Name: MAR_Passed

≡	diala Identity Services	Engine			Policy / Policy Elements
Щ	Bookmarks	Dictionaries Conditions	Re	sults	
51	Dashboard			Authorization Profiles > MAR	Passed
망	Context Visibility	Authentication	-	Authorization Profile	
×	Operations	Authorization Authorization Profiles	~	* Name	
Ū.	Policy	Downloadable ACLs		Hally	MAR_Passed
20	Administration	Profilies		Description	
di.	Work Centers	Profiling		* Access Type	
		Posture	-		NOC23_NOCE1 -
?	Interactive Help	Client Provisioning	>	Network Device Profile	
				Service Template	
				Agentiess Posture	
				Passive Identity Tracking	
				✓ Common Tasks	
				DACL Name	MAR_Passed ~

Autorisierungsprofil hinzufügen

Schritt 6: Policy Set hinzufügen

Navigieren Sie zu Policy > Policy Sets, und klicken Sie auf +, um einen Policy Set hinzuzufügen.

- Richtliniensatzname: MAR_Test
- Bedingungen: Wired_802.1X
- Zulässige Protokolle/Serversequenz: Standard-Netzwerkzugriff

≡	dealer Identity Services Er	ngine		Policy / Policy Sets		A Evaluation M	rde 89 Days	۹	۵	0	0	۹
н	Bookmarks	Policy Sets				Click here to	do visibilit	ty setup	Do not	show th	ils again	×
51	Dashboard	 Status Policy Set Name 	Description	Conditions	Allowe	d Protocols / Se	rver Seque	ince	Hits /	Actions	View	
15	Context Visibility	Q Search										
*	Operations	MAR_Test		Www.d_s002.1X	Defaul	t Network Acces	- 2	+	15	¢	>	
£.	Administration	Default	Default policy set		Defaul	t Network Acces	1	+	0	¢	•	
ń	Work Centers								leset		Save	

Policy Set hinzufügen

Schritt 7. Authentifizierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf MAR_Test, um eine Authentifizierungsrichtlinie hinzuzufügen.

- Regelname: MAR_dot1x
- Bedingungen: Wired_802.1X
- Verwenden: Identity_AD

C	√Authenticat	ion Policy(2)				
	💿 Statu	is Rule Name	Conditions	Use	Hits	Actions
	Q Sear	ch				
	۰	MAR_dot1x	T Wired_B02.1X	Identity_AD //	11	¢
	•	Default		All_User_ID_Stores /	0	٥

Authentifizierungsrichtlinie hinzufügen

Schritt 8: Autorisierungsrichtlinie hinzufügen

Navigieren Sie zu Policy Sets, und klicken Sie auf MAR_Test, um eine Autorisierungsrichtlinie hinzuzufügen.

- Regelname: MAR_Passed
- Bedingungen: AD_Join_Point
 ExternalGroups GLEICHT ad.rem-xxx.com/Users/Domain Computers AND Network_Access_Authentication_Passed
- Ergebnisse: MAR_Passed
- Regelname: User_MAR_Passed
- Bedingungen: Netzwerkzugriff
 WasMachineAuthenticated ENTSPRICHT True UND AD_Join_Point
 ExternalGroups ENTSPRICHT ad.rem-xxx.com/Users/Domain
- Ergebnisse: PermitAccess

		Results			
Status Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
Q Search					
MAR_Passed	AND AD_Join_PointExternalGroups EQUALS ad rem-sy "Im.com/Users/Domain Computers AND Image: The two int_Access_Authentication_Passed	MAR_Passed	+ Select from list / +	i.	ŵ
User_MAR_Passed	AND	PermitAccess	Select from list	- 1	命
Oefault		DenyAccess	/ + Select from list / +	9	٨

Autorisierungsrichtlinie hinzufügen

Überprüfung

Muster 1. Systemauthentifizierung und Benutzerauthentifizierung

Schritt 1: Abmelden von Windows-PC

Klicken Sie auf Abmelden in Win10 PC1, um die Computerauthentifizierung auszulösen.



Interface: GigabitEthernet1/0/2 MAC Address: b496.9115.84cb IPv6 Address: Unknown IPv4 Address: 1.x.x.9 User-Name:

host/DESKTOP-L2IL9I6.ad.rem-xxx.com

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: 5s Common Session ID: 01C200650000049AA780D80 Acct Session ID: 0x000003C Handle: 0x66000016 Current Policy: POLICY_Gi1/0/2 Local Policies: Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)

Server Policies: ACS ACL: xACSACLx-IP-MAR_Passed-6639ba20

Method status list: Method State

dot1x Authc Success

Schritt 3: Windows-PC anmelden

Melden Sie sich bei Win10 PC1 an, geben Sie Benutzername und Kennwort ein, um die Benutzerauthentifizierung auszulösen.



Windows-PC anmelden

Schritt 4: Authentifizierungssitzung bestätigen

show authentication sessions interface GigabitEthernet1/0/2 details Führen Sie den Befehl aus, um die Benutzerauthentifizierungssitzung in C1000 zu bestätigen.

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/2 details

Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9
User-Name:

AD\testuser

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: 85s
Common Session ID: 01C200650000049AA780D80
Acct Session ID: 0x000003D
Handle: 0x66000016
Current Policy: POLICY_Gi1/0/2
Local Policies:
Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150)
Server Policies:
Method status list:
Method status list:
Method State
dot1x Authc Success
```

Schritt 5: RADIUS-Live-Protokoll bestätigen

Navigieren Sie zu **Operations > RADIUS > Live Logs (Vorgänge > RADIUS > Live-Protokolle**) in der ISE-GUI, und bestätigen Sie das Live-Protokoll für die Computer- und Benutzerauthentifizierung.

	abada Identity Services	Engine					Operations /	RADIUS				A Evaluation Mode	. D 🗝		1 2
Щ	Bookmarks	Live Log	s Live Sessions												
51	Dashboard														
명	Context Visibility	Mise	configured Supplicants 📀			Mis	configured Network Devices 🔘		RADIUS Drops	0	Client Stopped Respondi	9 O		Repeat Cour	nter
*	Operations		0				0		0		0			0	
U	Policy										Refres	Show	20 records	Within	
20	Administration										Neve	v cates	zu records 🗸	Last 3 nours	-
nii.	Work Centers	9	S Reset Repeat Counts											Filter 🗸	0
			Time	Status	Detalls	Repea	Identity	Endpoint ID	Endpoint	Authentication Policy	Authorization Policy	Authorization P	IP Address	Network D	De
(?)	Interactive Help	×		v			Identity	Endpoint ID	Endpoint Pr	Authentication Policy	Authorization Policy	Authorization Profi	IP Address	V Network Dr	levic
			May 07, 2024 04:36:14	•	ò	0	AD(testuser	84:96:91:15:84:	Intel-Devi	$MAR_Test \Rightarrow MAR_dot1x$	$MAR_Test \mapsto User_MAR_Passed$	PermitAccess	1.1 2.9		
			May 07, 2024 04:36:13	8	ō.		ADitestuser	B4:96:91:15:84:	Intel-Devi	MAR_Test >> MAR_dot1s	$MAR_Test \Rightarrow User_MAR_Passed$	PermitAccess	1.1 2.9	C1000	
			May 07, 2024 04:35:12	8	à		#ACSACL#-IP-MAR_Passed-6639ba20							C1000	
			May 07, 2024 04:35:12	8	ø		host/DESKTOP-L2IL9I6.ad.rem-s_rhm	B4:96:91:15:84:	Intel-Devi	MAR_Test >> MAR_dot1x	$MAR_Test \Rightarrow MAR_Passed$	MAR_Passed	169.254.90.1	C1000	

Radius-Live-Protokoll

Bestätigen Sie das detaillierte Live-Protokoll der Computerauthentifizierung.

Cisco ISE

Overview	
Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-s_s_bm.com
Endpoint Id	B4:96:91:15:84:CB ⊕
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> MAR_Passed
Authorization Result	MAR_Passed

Authentication Details	
Source Timestamp	2024-05-07 16:35:12.222
Received Timestamp	2024-05-07 16:35:12.222
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL9I6.ad.rem-sy rem.com
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	169.254.90.172
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C2006500000049AA780D80
Authentication Method	dot1x

Steps		
Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-sy .em.com	0
15049	Evaluating Policy Group - AD_Join_Point	1
15008	Evaluating Service Selection Policy	0
15048	Queried PIP - Normalised Radius.RadiusFlowType	3
11507	Extracted EAP-Response/Identity	2
12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	1
11001	Received RADIUS Access-Request	6
11018	RADIUS is re-using an existing session	0
12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
12300	Prepared EAP-Request proposing PEAP with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	5
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated	1
61025	Open secure connection with TLS peer	1
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	25
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	1
11001	Received RADIUS Access-Request	14
11018	RADIUS is re-using an existing session	0

Details zur Computerauthentifizierung

Authentication Protocol

Bestätigen Sie das detaillierte Live-Protokoll der Benutzerauthentifizierung.

PEAP (EAP-MSCHAPv2)

Cisco ISE

Overview			Steps		
Event	5200 Authentication succeeded		Step ID	Description	Latency (ms)
			11001	Received RADIUS Access-Request - AD_Join_Point	
Username	AD\testuser		11017	RADIUS created a new session - ad.rem-sy .em.com	0
Endpoint Id	B4:96:91:15:84:CB ⊕		15049	Evaluating Policy Group - AD_Join_Point	0
Endpoint Profile	Intel-Device		15008	Evaluating Service Selection Policy	1
		1	11507	Extracted EAP-Response/Identity	7
Authentication Policy	MAR_Test >> MAR_dot1x		12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
Authorization Policy	MAR_Test >> User_MAR_Passed		12625	Valid EAP-Key-Name attribute received	0
Authorization Result	PermitAccess		11006	Returned RADIUS Access-Challenge	0
			11001	Received RADIUS Access-Request	8
			11018	RADIUS is re-using an existing session	0
Authentication Details			12301	Extracted EAP-Response/NAK requesting to use PEAP instead	0
Source Timestamp	2024-05-07 16:36:13.748		12300	Prepared EAP-Request proposing PEAP with challenge	1
			12625	Valid EAP-Key-Name attribute received	0
Received Timestamp	2024-05-07 16:36:13.748		11006	Returned RADIUS Access-Challenge	0
Policy Server	ise33-01		11001	Received RADIUS Access-Request	11
Event	5200 Authentication succeeded		11018	RADIUS is re-using an existing session	0
Username	AD\testuser		12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated	0
Endpoint Id	B4:96:91:15:84:CB		61025	Open secure connection with TLS peer	0
			12318	Successfully negotiated PEAP version 0	1
Calling Station Id	B4-96-91-15-84-CB		12800	Extracted first TLS record; TLS handshake started	0
Endpoint Profile	Intel-Device		12805	Extracted TLS ClientHello message	0
IPv4 Address	1.111 0.9		12806	Prepared TLS ServerHello message	0
			12807	Prepared TLS Certificate message	0
Store	AD_Join_Point		12808	Prepared TLS ServerKeyExchange message	28
Idealty Course	DecElect		12810	Prepared TLS ServerDone message	0
Identity Group	Profiled		12305	Prepared EAP-Request with another PEAP challenge	1
Audit Session Id	01C2006500000049AA780D80		11006	Returned RADIUS Access-Challenge	0
Authentication Method	dot1x		11001	Received RADIUS Access-Request	30
Authentication Droto and	DEAD (EAD MCCHAD-2)		11018	RADIUS is re-using an existing session	0
Authentication Protocol	PEAP (EAP-MSCHAPVZ)		12304	Extracted EAP-Response containing PEAP challenge-	0

Details zur Benutzerauthentifizierung

Muster 2. Nur Benutzerauthentifizierung

Schritt 1: Deaktivieren und Aktivieren der Netzwerkkarte von Windows PC

Um die Benutzerauthentifizierung auszulösen, deaktivieren und aktivieren Sie die Netzwerkkarte von Win10 PC1.

Schritt 2: Authentifizierungssitzung bestätigen

show authentication sessions interface GigabitEthernet1/0/2 details Führen Sie den Befehl aus, um die Benutzerauthentifizierungssitzung in C1000 zu bestätigen.

<#root>

Switch#

show authentication sessions interface GigabitEthernet1/0/2 details

Interface: GigabitEthernet1/0/2
MAC Address: b496.9115.84cb
IPv6 Address: Unknown
IPv4 Address: 1.x.x.9

User-Name: AD\testuser 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: 419s Common Session ID: 01C2006500000049AA780D80 Acct Session ID: 0x000003D Handle: 0x66000016 Current Policy: POLICY_Gi1/0/2 Local Policies: Service Template: DEFAULT_LINKSEC_POLICY_SHOULD_SECURE (priority 150) Server Policies: Method status list: Method State dot1x Authc Success

Schritt 3: RADIUS-Live-Protokoll bestätigen

Navigieren Sie zu **Operations > RADIUS > Live Logs (Vorgänge > RADIUS > Live-Protokolle** in der ISE-GUI), und bestätigen Sie das Live-Protokoll für die Benutzerauthentifizierung.



Hinweis: Da der MAR-Cache in der ISE gespeichert ist, ist nur eine Benutzerauthentifizierung erforderlich.

$\equiv \frac{1}{1000}$ identity Services	Engine		Operations / F	RADIUS		A	Evaluation Mode =Days Q 🖌) • • + ×
JI Bookmarks	Live Logs Live Sessions							
E Dashboard								
Id Context Visibility	Misconfigured Supplicants 🔾	Miscon	figured Network Devices	RADIUS Drop	0	Client Stopped Responding		Repeat Counter 🕕
😤 Operations	0		0	0		0		0
Policy						Refresh Never	Show Latest 20 records	Within Last 3 hours
Administration	🖉 🖆 Reset Repeat Counts 🛛	± Export To ∨						Filter V 0
	Time	Status Details Repea Id	entity	Endpoint ID Endpoint	Authentication Policy	Authorization Policy	Authorization P IP Address	Network De
(?) Interactive Help	×	<u>k</u>	entity	Endpoint ID Endpoint Pr	Authentication Policy	Authorization Policy	Authorization Profi IP Address	Network Devic
	May 07, 2024 04:42:05	 à A 	Kestuser	84:96:91:15:84: Intel-Devi	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess 1.1.1.1.9	
	May 07, 2024 04:42:04		Vitestuser	84:96:91:15:84: Intel-Devi	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess 1	C1000
	May 07, 2024 04:36:13	2 6 4	Voestuser	84:96:91:15:84: Intel-Devi	MAR_Test >> MAR_dot1x	MAR_Test >> User_MAR_Passed	PermitAccess 1.1 , 0.9	C1000
	May 07, 2024 04:35:12	a a	CSACL#-IP-MAR_Passed-6639ba20					C1000
	May 07, 2024 04:35:12	🖬 🐻 🗠	st/DESKTOP-L2IL9I6.ad.rem-s 1.am	84:96:91:15:84: Intel-Devi	MAR_Test >> MAR_dot1x	MAR_Test >> MAR_Passed	MAR_Passed 169.254.90.1	C1000

Radius-Live-Protokoll

Bestätigen Sie das detaillierte Live-Protokoll der Benutzerauthentifizierung.

Steps Step ID 11001 11017 15049 15008 11507 12500 12625 11006 11001 12300 12625 11006 11001	Description Received RADIUS Access-Request - AD_Join_Point RADIUS created a new session - ad.rem-s_s.em.com Evaluating Policy Group - AD_Join_Point Evaluating Service Selection Policy Extracted EAP-Response/Identity Prepared EAP-Request proposing EAP-TLS with challenge Valid EAP-Key-Name attribute received Returned RADIUS Access-Challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response/NAK requesting to use PEAP Instead Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received	Latency (ms) 0 1 0 16 2 0 5 0 5 0
Step ID 11001 11017 15049 15008 11507 12500 12625 11006 11001 12300 12625 11006 11001	Description Received RADIUS Access-Request - AD_Join_Point RADIUS created a new session - ad.rem-s_t.em.com Evaluating Policy Group - AD_Join_Point Evaluating Service Selection Policy Extracted EAP-Response/Identity Prepared EAP-Request proposing EAP-TLS with challenge Valid EAP-Key-Name attribute received Returned RADIUS Access-Challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response/NAK requesting to use PEAP instead Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received	Latency (ms) 0 1 0 16 2 0 0 5 0 5 0
Step ID 11001 11017 15049 15008 11507 12500 12625 11006 11018 12300 12625 11006 11006 11001	Description Roceived RADIUS Access-Request - AD_Join_Point RADIUS created a new session - ad.rem-s_t_em.com Evaluating Policy Group - AD_Join_Point Evaluating Service Selection Policy Extracted EAP-Response/Identity Prepared EAP-Request proposing EAP-TLS with challenge Valid EAP-Key-Name attribute received Roteived RADIUS Access-Challenge Roceived RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response/NAK requesting to use PEAP Instead Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received	Latency (ms) 0 1 0 16 2 0 0 5 0 0 0
11001 11017 15049 15008 11507 12500 12625 11006 11001 12300 12625 11006 11001	Received RADIUS Access-Request - AD_Join_Point RADIUS created a new session - ad.rem-s.t.em.com Evaluating Policy Group - AD_Join_Point Evaluating Service Selection Policy Extracted EAP-Response/Identity Prepared EAP-Request proposing EAP-TLS with challenge Valid EAP-Key-Name attribute received Returned RADIUS Access-Challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response/NAK requesting to use PEAP Instead Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received	0 1 0 16 2 0 0 5 0 5 0
11017 15049 15008 11507 12625 11006 11001 11018 12300 12625 11006 11001	RADIUS created a new session – ad.rem-s_t_em.com Evaluating Policy Group – AD_Join_Point Evaluating Service Selection Policy Extracted EAP-Response/Identity Prepared EAP-Request proposing EAP-TLS with challenge Valid EAP-Key-Name attribute received Returned RADIUS Access-Challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response/NAK requesting to use PEAP Instead Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received	0 1 0 16 2 0 0 5 0 0
15049 15008 11507 12625 11006 11001 11018 12300 12625 11006 11001	Evaluating Policy Group - AD_Join_Point Evaluating Service Selection Policy Extracted EAP-Response/Identity Prepared EAP-Request proposing EAP-TLS with challenge Valid EAP-Key-Name attribute received Returned RADIUS Access-Challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response/NAK requesting to use PEAP Instead Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received Detword DADIUS Gaston Chilenge	1 0 16 2 0 5 0 0
15008 11507 12500 12625 11006 11001 11018 12300 12625 11006 11001	Evaluating Service Selection Policy Extracted EAP-Response/Identity Prepared EAP-Request proposing EAP-TLS with challenge Valid EAP-Key-Name attribute received Returned RADIUS Access-Challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response/NAK requesting to use PEAP Instead Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received Detword DADIUS Gaston Chilenge	16 2 0 5 0
11307 12500 12625 11006 11001 11018 12301 12300 12625 11006 11001	Extracted EAP-Response/releasing Prepared EAP-Request proposing EAP-TLS with challenge Valid EAP-Key-Name attribute received Returned RADIUS Access-Challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response/NAK requesting to use PEAP instead Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received Detword DADIUS GASS-Challenge	2 0 5 0
12625 11006 11001 11018 12301 12300 12625 11006 11001	Valid EAP-Key-Name attribute received Returned RADIUS Access-Challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response/NAK requesting to use PEAP instead Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received Detword BADIUS GADESS-Challenge	0 0 5 0
11006 11001 11018 12301 12300 12625 11006 11001	Returned RADIUS Access-Challenge Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response/NAK requesting to use PEAP Instead Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received Returned RADIUS Access Challenge	0 5 0
11001 11018 12301 12300 12625 11006 11001	Received RADIUS Access-Request RADIUS is re-using an existing session Extracted EAP-Response/NAK requesting to use PEAP Instead Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received Resurced RADIUS GADESS Challenge	5 0 0
11018 12301 12300 12625 11006 11001	RADIUS is re-using an existing session Extracted EAP-Response/NAK requesting to use PEAP Instead Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received Destroed BADIUS General Challenge	0
12301 12300 12625 11006 11001	Extracted EAP-Response/NAK requesting to use PEAP instead Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received	0
12300 12625 11006 11001	Prepared EAP-Request proposing PEAP with challenge Valid EAP-Key-Name attribute received	
12625 11006 11001	Valid EAP-Key-Name attribute received	0
11006 11001	Poturoad PADIUS Access Challenge	0
11001	Returned RADIOS Access-Challenge	0
	Received RADIUS Access-Request	25
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge- response and accepting PEAP as negotiated	1
61025	Open secure connection with TLS peer	0
12318	Successfully negotiated PEAP version 0	0
12800	Extracted first TLS record; TLS handshake started	0
12805	Extracted TLS ClientHello message	0
12806	Prepared TLS ServerHello message	0
12807	Prepared TLS Certificate message	0
12808	Prepared TLS ServerKeyExchange message	26
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	14
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge- response	1
12305	Prepared EAP-Request with another PEAP challenge	0
24422	ISE has confirmed previous successful machine authentication for user in Active Directory	0
15036	Evaluating Authorization Policy	0
24209	Looking up Endpoint in Internal Endpoints IDStore - AD\testuser	1
24211	Found Endpoint in Internal Endpoints IDStore	3
	Looking up user in Active Directory - AD\testuser	
24432	LDAP fetch succeeded	
24432	User's Groups retrieval from Active Directory succeeded	
24432 24355 24416	Queried PIP - AD_Join_Point.ExternalGroups	11
24432 24355 24416 15048	Selected Authorization Profile - PermitAccess	5
24432 24355 24416 15048 15016		0
24432 24355 24416 15048 15016 22081	Max sessions policy passed	0
24432 24355 24416 15048 15016 22081 22080	Max sessions policy passed New accounting session created in Session cache	0
24432 24355 24416 15048 15016 22081 22080 12306 61126	Max sessions policy passed New accounting session created in Session cache PEAP authentication succeeded Shutdhaun secura connection with TLS pass	
24432 24355 24416 15048 15016 22081 22080 12306 61026	Max sessions policy passed New accounting session created in Session cache PEAP authentication succeeded Shutdown secure connection with TLS peer Propaged EAP-Success	1
	15048 15016	15048 Queried PIP - AD_Join_Point.ExternalGroups 15016 Selected Authorization Profile - PermitAccess 22081 Max sessions policy passed 22080 New accounting session created in Session cache 12306 PEAP authentication succeeded Closs External course consection with TLS peer

Details zur Benutzerauthentifizierung

Fehlerbehebung

Diese Debug-Protokolle (prrt-server.log) helfen Ihnen, das detaillierte Verhalten der Authentifizierung in der ISE zu bestätigen.

• Laufzeitkonfiguration

- Laufzeitprotokollierung
- Laufzeit-AAA

Dies ist ein Beispiel für das Debug-Protokoll für Muster 1. Systemauthentifizierung und Benutzerauthentifizierung in diesem Dokument.

<#root>

// machine authentication

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::checkInsertConditions:

subject=machine

, calling-station-id=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6\$@ad.rem-xxx.com,MARCache.cpp:105

// insert MAR cache
MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,

Inserting new entry to cache

CallingStationId=B4-96-91-15-84-CB, HostName=DESKTOP-L2IL9I6\$@ad.rem-xxx.com, IDStore=AD_Join_Point an MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionI

user=host/DESKTOP-L2IL9I6.ad.rem-xxx.com

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onInsertRequest: event not locall

// user authentication
MAR,2024-05-08 16:55:11,120,DEBUG,0x7fb2fdde0700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionI

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onQueryRequest:

machine authentication confirmed locally

,MARCache.cpp:222 MAR,2024-05-08 16:55:11,130,DEBUG,0x7fb2fe5e4700,cntx=0000034409,sesn=ise33-01/504417979/45,CPMSessionI

user=AD\testuser

,CallingStationID=B4-96-91-15-84-CB,FramedIPAddress=1.x.x.9,MARCache::onMachineQueryResponse:

machine DESKTOP-L2IL9I6\$@ad.rem-xxx.com valid in AD

,MARCache.cpp:316

Zugehörige Informationen

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.