

Configurer l'authentification à deux facteurs de la machine pour l'accès demandeur

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. Ajouter un PC au domaine AD](#)

[Étape 2. Configurer l'authentification utilisateur](#)

[Configuration dans Windows Server](#)

[Étape 1. Confirmer les ordinateurs du domaine](#)

[Étape 2. Ajouter un utilisateur de domaine](#)

[Configuration dans ISE](#)

[Étape 1. Ajouter un périphérique](#)

[Étape 2. Ajouter Active Directory](#)

[Étape 3. Confirmer le paramètre d'authentification ordinateur](#)

[Étape 4. Ajouter des séquences source d'identité](#)

[Étape 5. Ajouter une DACL et un profil d'autorisation](#)

[Étape 6. Ajouter un jeu de stratégies](#)

[Étape 7. Ajouter une stratégie d'authentification](#)

[Étape 8. Ajouter une stratégie d'autorisation](#)

[Vérifier](#)

[Modèle 1. Authentification des ordinateurs et des utilisateurs](#)

[Étape 1. Se déconnecter d'un PC Windows](#)

[Étape 2. Confirmer la session d'authentification](#)

[Étape 3. Connexion au PC Windows](#)

[Étape 4. Confirmer la session d'authentification](#)

[Étape 5. Confirmer le journal Radius en direct](#)

[Modèle 2. Authentification utilisateur uniquement](#)

[Étape 1. Désactiver et activer la carte réseau du PC Windows](#)

[Étape 2. Confirmer la session d'authentification](#)

[Étape 3. Confirmer le journal Radius en direct](#)

[Dépannage](#)

[Informations connexes](#)

Introduction

Ce document décrit les étapes requises pour configurer l'authentification à deux facteurs avec l'authentification machine et dot1x.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration de Cisco Identity Services Engine
- Configuration de Cisco Catalyst
- IEEE802.1X

Composants utilisés

- Correctif 1 d'Identity Services Engine Virtual 3.3
- C1000-48FP-4G-L 15.2(7)E9
- Windows Server 2019

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.

Le nom de domaine configuré sur Windows Server 2019 est ad.rem-xxx.com, qui est utilisé comme exemple dans ce document.

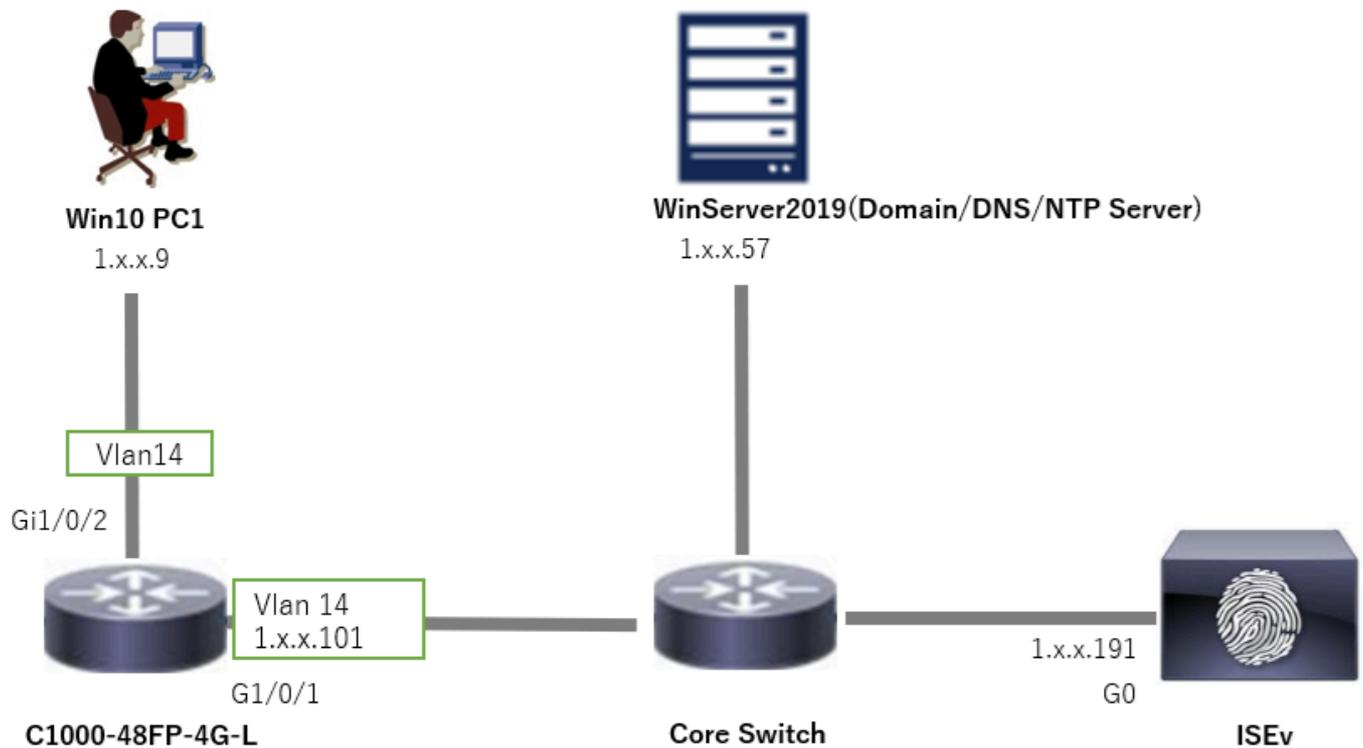


Diagramme du réseau

Informations générales

L'authentification de machine est un processus de sécurité qui vérifie l'identité d'un périphérique cherchant à accéder à un réseau ou à un système. Contrairement à l'authentification des utilisateurs, qui vérifie l'identité d'une personne en se basant sur des informations d'identification telles qu'un nom d'utilisateur et un mot de passe, l'authentification des ordinateurs se concentre sur la validation du périphérique lui-même. Cette opération est souvent effectuée à l'aide de certificats numériques ou de clés de sécurité uniques au périphérique.

En utilisant conjointement l'authentification des machines et des utilisateurs, une entreprise peut s'assurer que seuls les périphériques et les utilisateurs autorisés peuvent accéder à son réseau, offrant ainsi un environnement plus sécurisé. Cette méthode d'authentification à deux facteurs est particulièrement utile pour protéger les informations sensibles et respecter des normes réglementaires strictes.

Configurations

Configuration dans C1000

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

```
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
```

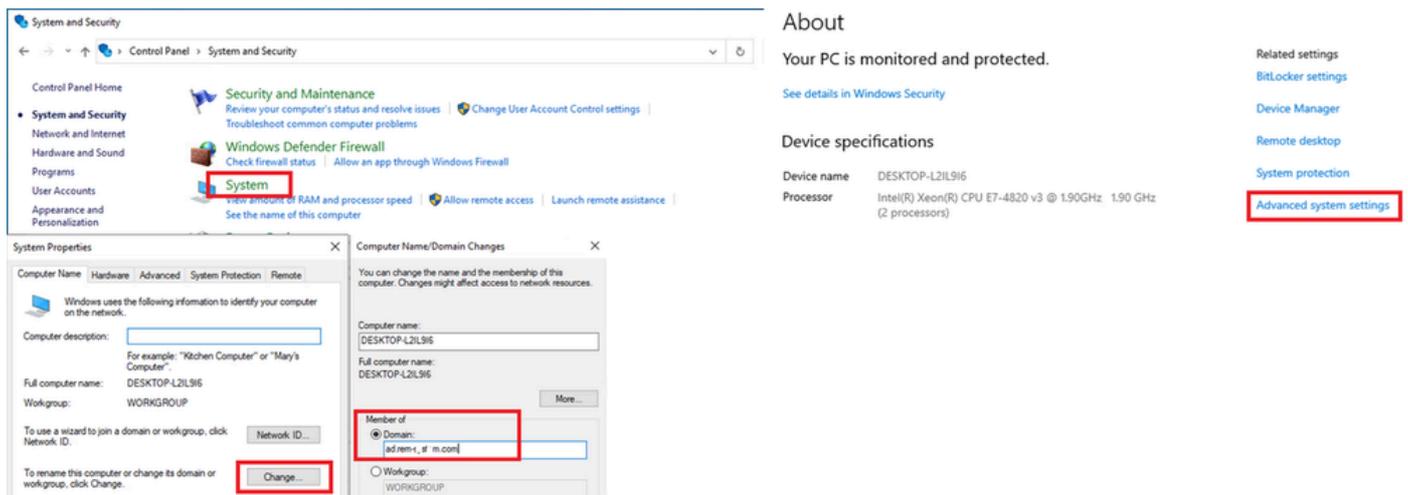
```
interface GigabitEthernet1/0/1  
switchport access vlan 14  
switchport mode access
```

```
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
```

Configuration dans le PC Windows

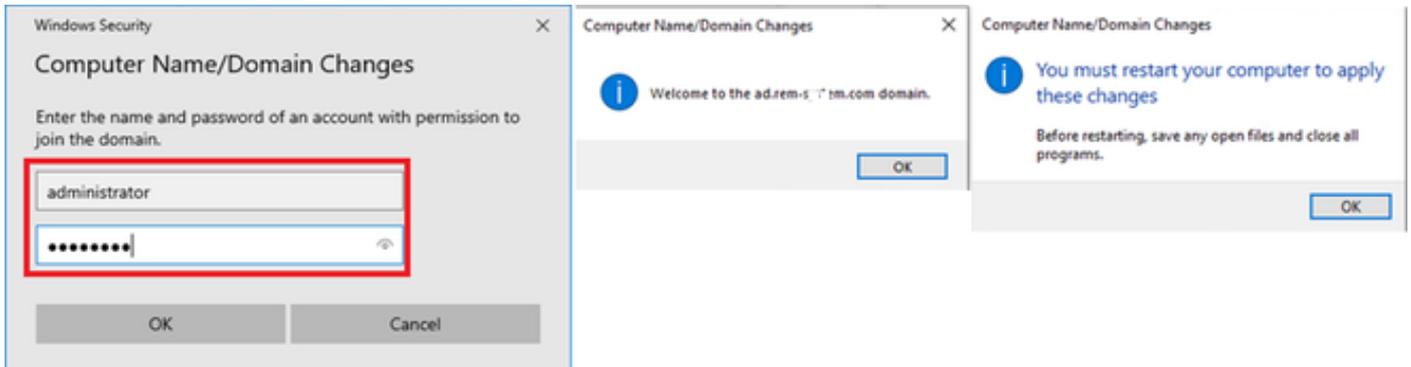
Étape 1. Ajouter un PC au domaine AD

Accédez à Panneau de configuration > Système et sécurité, cliquez sur Système, puis cliquez sur Paramètres système avancés. Dans la fenêtre Propriétés système, cliquez sur Modifier, sélectionnez Domaine et entrez le nom de domaine.



Ajouter un PC au domaine AD

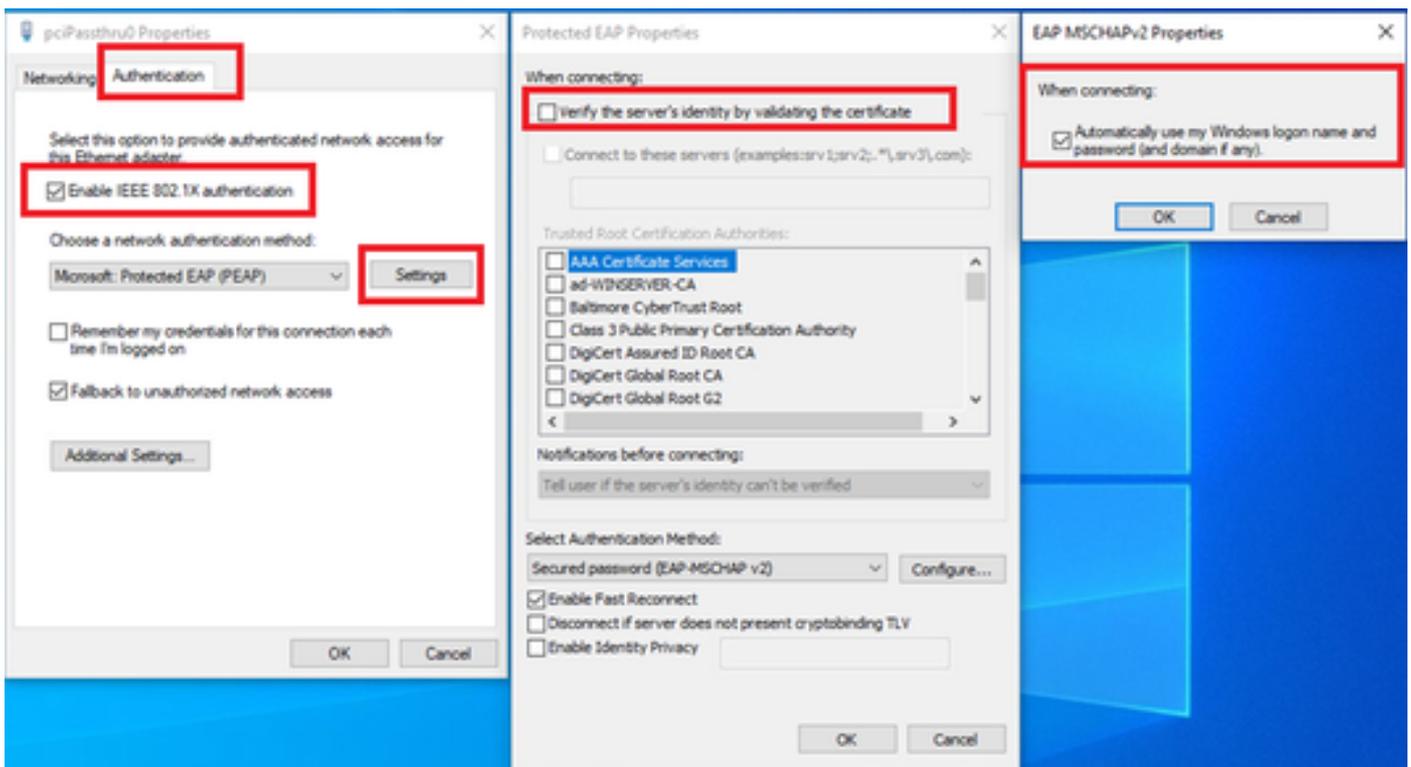
Dans la fenêtre Sécurité Windows, entrez le nom d'utilisateur et le mot de passe du serveur de domaine.



Nom d'utilisateur et mot de passe

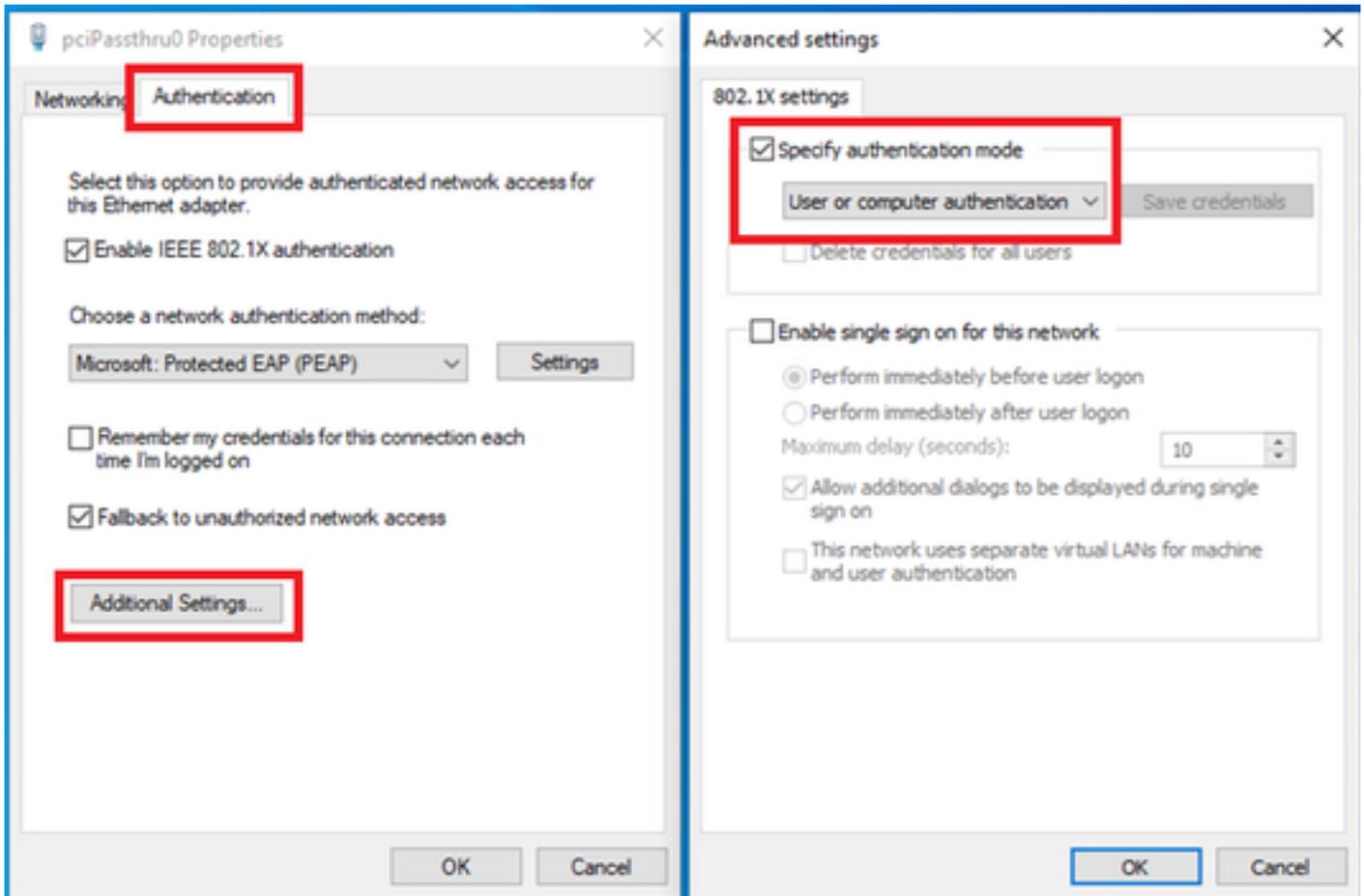
Étape 2. Configurer l'authentification utilisateur

Accédez à Authentication, cochez Enable IEEE 802.1X authentication. Cliquez sur Settings dans la fenêtre Protected EAP Properties, décochez Verify the server's identity by validating the certificate, puis cliquez sur Configure. Dans la fenêtre Propriétés de EAP MSCHAPv2, cochez Utiliser automatiquement mon nom d'ouverture de session Windows et mon mot de passe (et le domaine s'il y a lieu) pour utiliser le nom d'utilisateur saisi lors de la connexion de l'ordinateur Windows pour l'authentification de l'utilisateur.



Activer l'authentification utilisateur

Accédez à Authentication, cochez Additional Settings. Sélectionnez Authentification utilisateur ou ordinateur dans la liste déroulante.

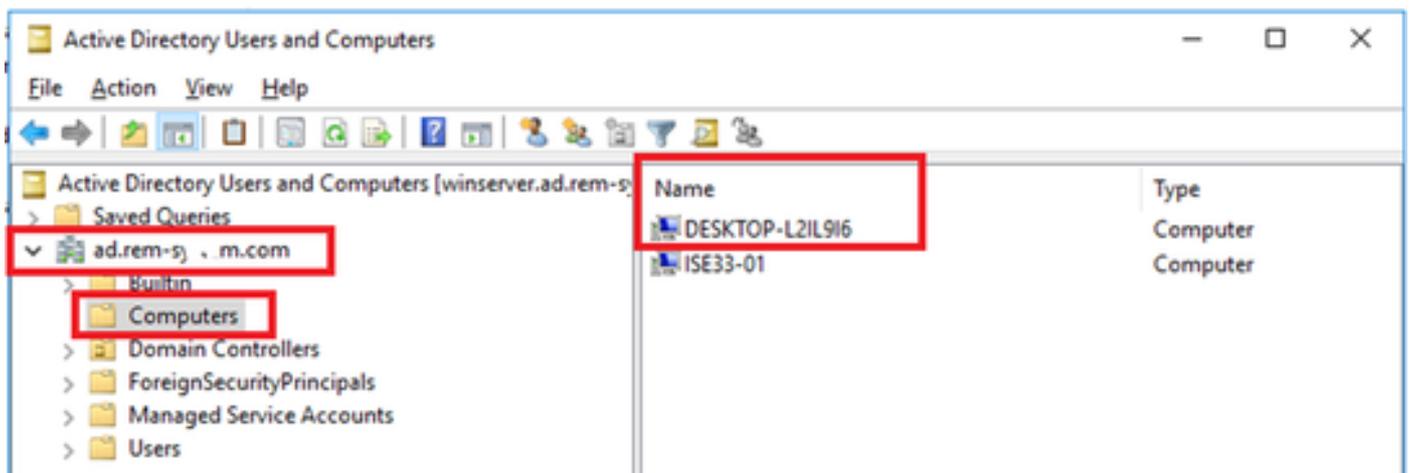


Spécifier le mode d'authentification

Configuration dans Windows Server

Étape 1. Confirmer les ordinateurs du domaine

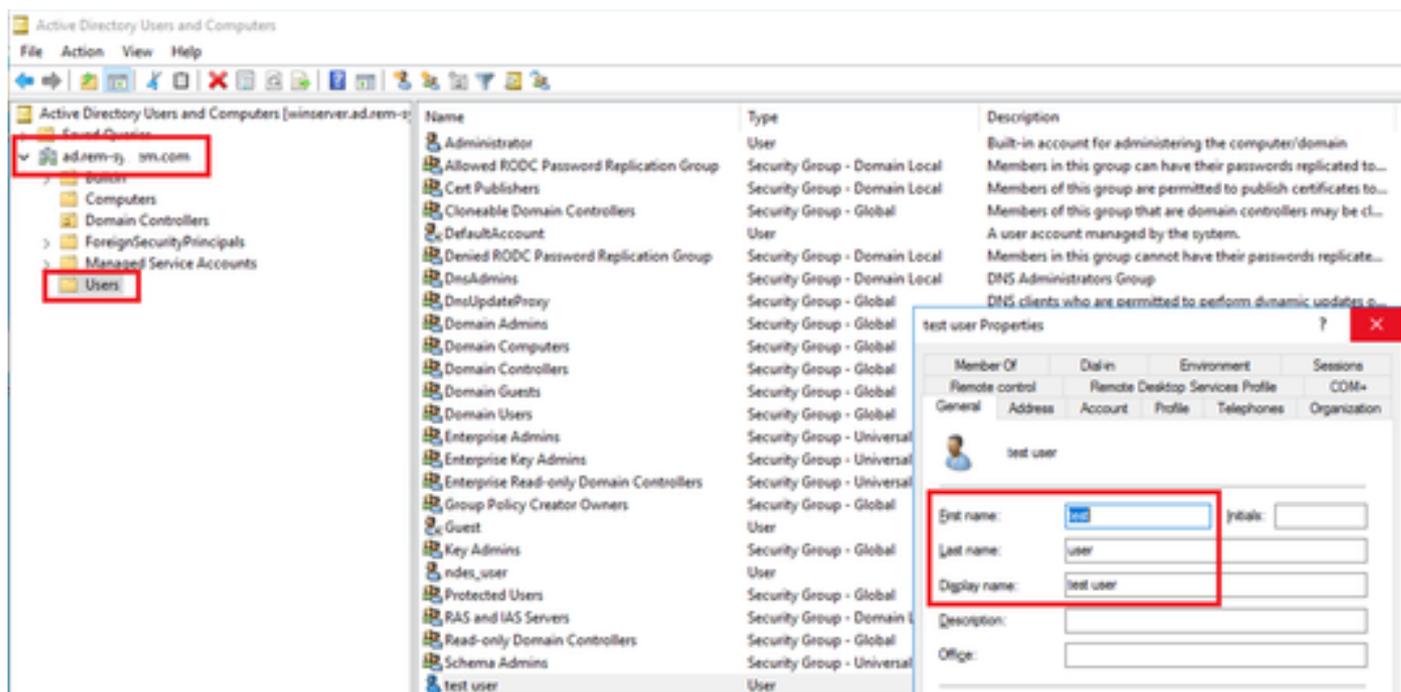
Accédez à Utilisateurs et ordinateurs Active Directory, cliquez sur Ordinateurs. Vérifiez que Win10 PC1 est répertorié dans le domaine.



Confirmer l'ordinateur du domaine

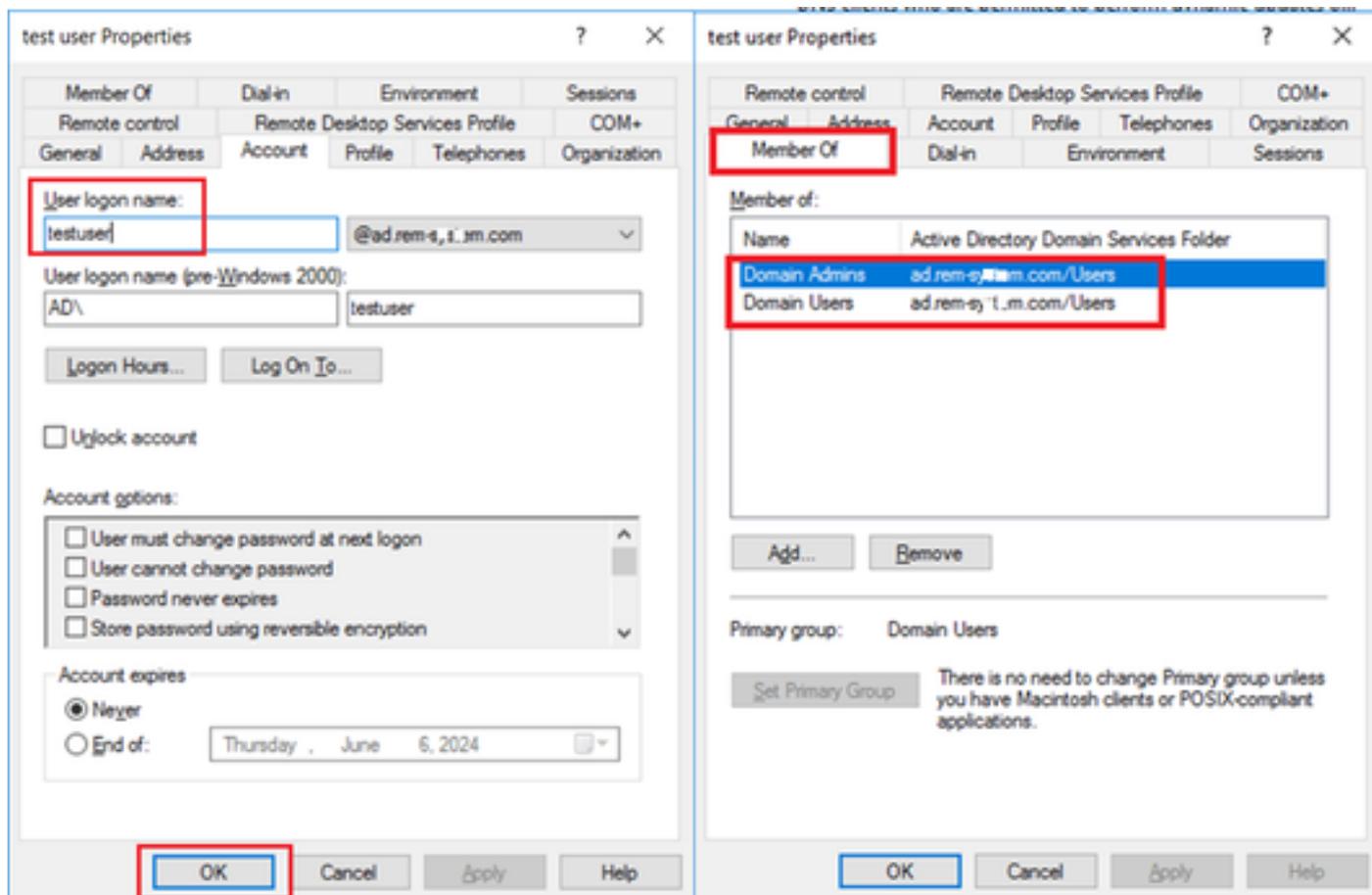
Étape 2. Ajouter un utilisateur de domaine

Accédez à Utilisateurs et ordinateurs Active Directory, cliquez sur Utilisateurs. Ajoutez testuser en tant qu'utilisateur de domaine.



Ajouter un utilisateur de domaine

Ajoutez l'utilisateur du domaine aux membres Admins du domaine et Utilisateurs du domaine.

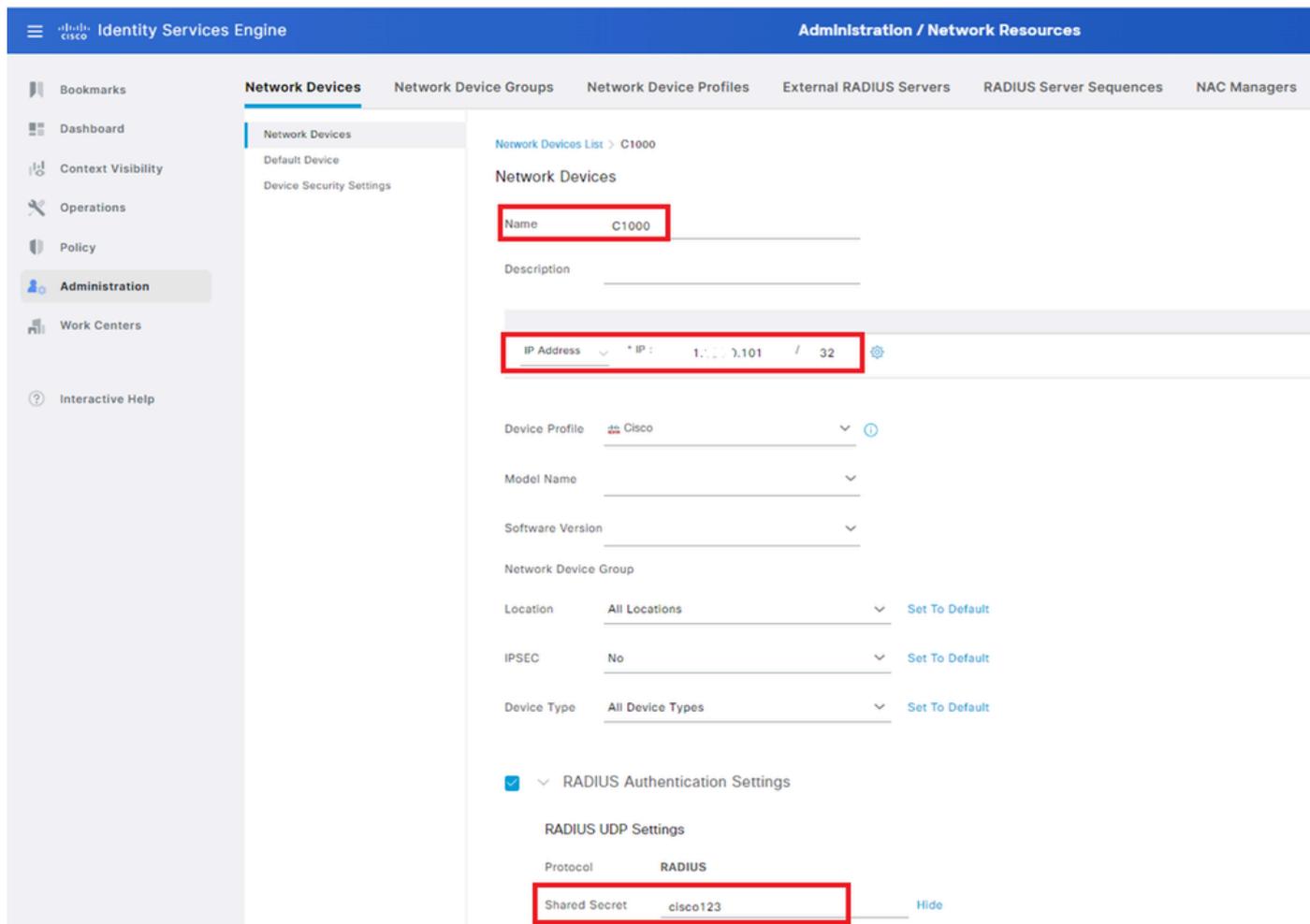


Administrateurs de domaine et utilisateurs de domaine

Configuration dans ISE

Étape 1. Ajouter un périphérique

Accédez à Administration > Network Devices, cliquez sur Add button to add C1000 device.

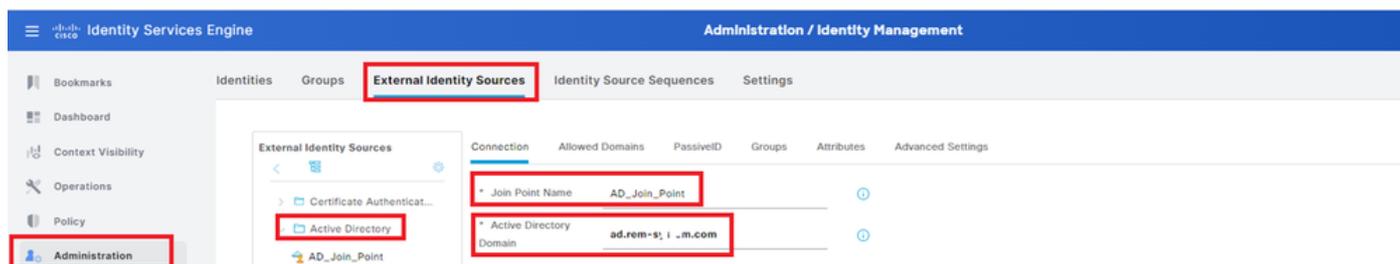


Ajouter un périphérique

Étape 2. Ajouter Active Directory

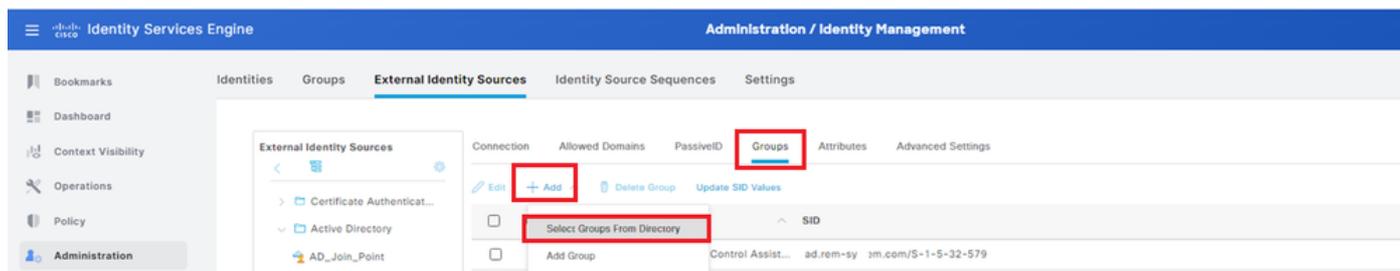
Accédez à Administration > External Identity Sources > Active Directory, cliquez sur l'onglet Connection, ajoutez Active Directory à ISE.

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



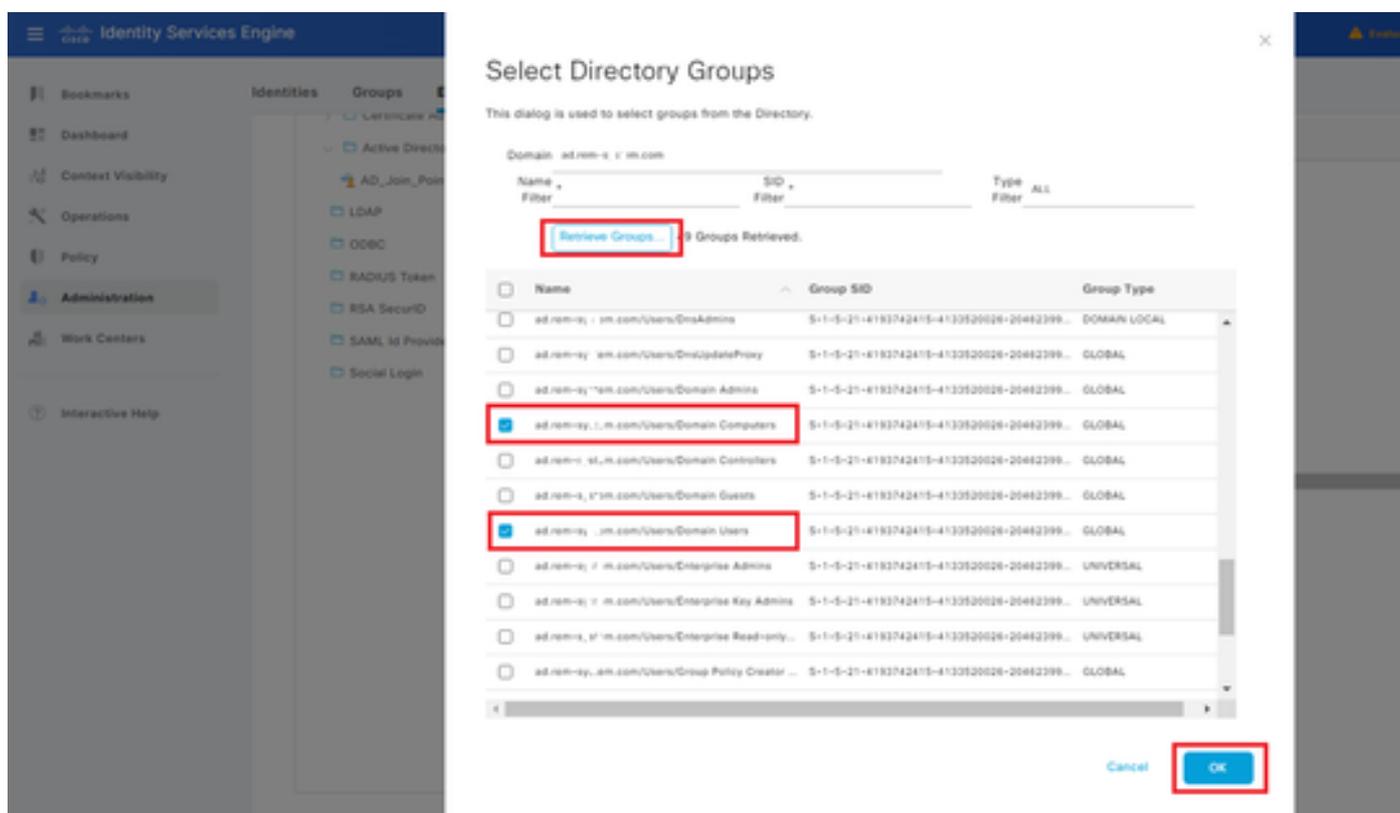
Ajouter Active Directory

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



Sélectionner des groupes dans le répertoire

Cliquez sur Récupérer des groupes dans la liste déroulante. Cochez ad.rem-xxx.com/Users/Domain Computers et ad.rem-xxx.com/Users/Domain Users et cliquez sur OK.



Ajouter des ordinateurs et des utilisateurs de domaine

Étape 3. Confirmer le paramètre d'authentification ordinateur

Accédez à l'onglet Advanced Settings, confirmez le paramètre de l'authentification de l'ordinateur.

- Enable Machine Authentication : pour activer l'authentification de l'ordinateur
- Enable Machine Access Restriction : pour combiner l'authentification des utilisateurs et des ordinateurs avant l'autorisation

Remarque : la plage de temps de vieillissement valide est comprise entre 1 et 8 760.

The screenshot displays the Cisco Identity Services Engine (ISE) Administration console. The top navigation bar shows 'Identity Services Engine' and 'Administration / Identity Management'. The main content area is divided into several tabs: 'Identities', 'Groups', 'External Identity Sources', 'Identity Source Sequences', and 'Settings'. The 'External Identity Sources' tab is active, and the 'Advanced Settings' sub-tab is selected and highlighted with a red box. The 'Advanced Authentication Settings' section is expanded, showing the following options:

- Enable Password Change
- Enable Machine Authentication
- Enable Machine Access Restrictions
- Aging Time: 5 hours

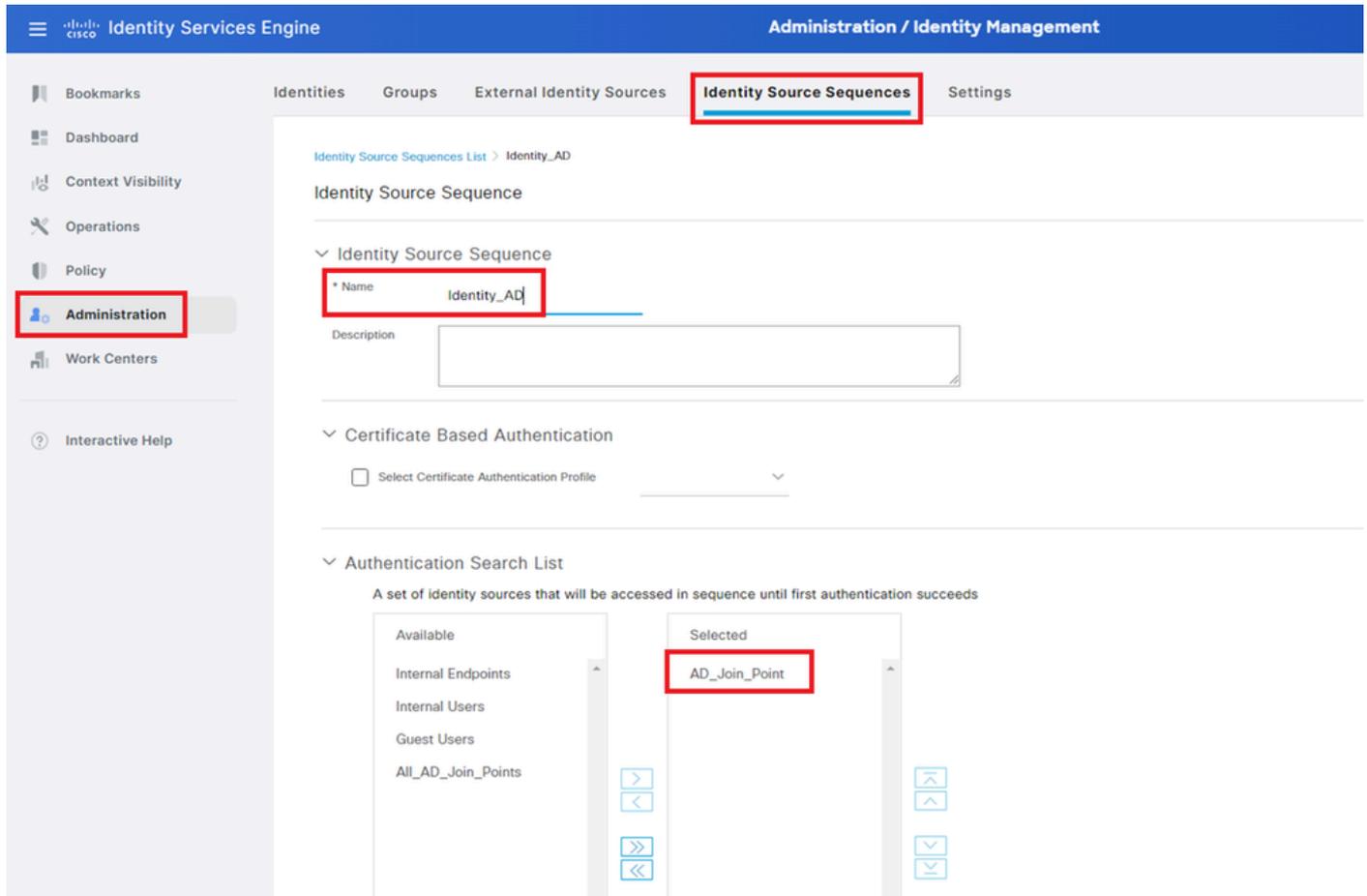
Below these settings, there is a note: 'Machine Access Restrictions Cache will be replicated between PSN instances in each node group. To configure MAR Cache distribution groups: [Administration > System > Deployment](#)'. Other options include:

- Enable dial-in check
- Enable callback check for dial-in clients
- Use Kerberos for Plain Text Authentications

Étape 4. Ajouter des séquences source d'identité

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

- Nom : Identity_AD
- Liste de recherche d'authentification : AD_Join_Point



Ajouter des séquences source d'identité

Étape 5. Ajouter une DACL et un profil d'autorisation

Accédez à Policy > Results > Authorization > Downloadable ACLs, ajoutez une DACL.

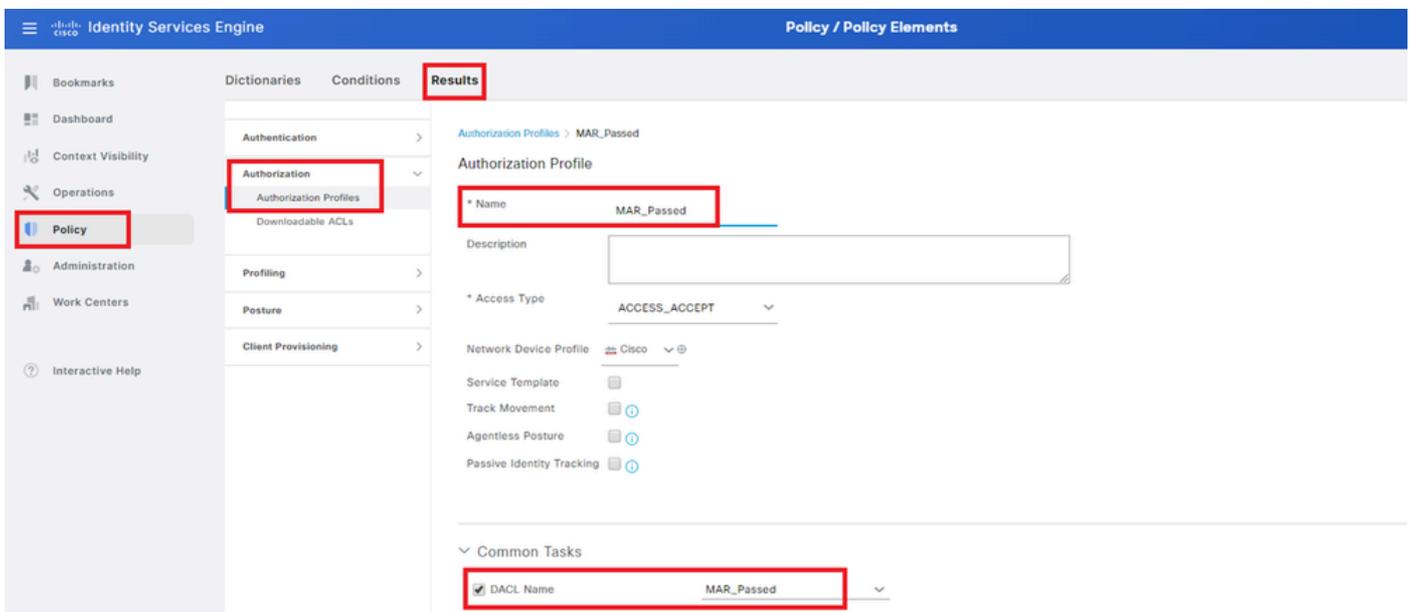
- Nom : MAR_Passed
- Contenu DACL : permit ip any host 1.x.x.101 et permit ip any host 1.x.x.105



Ajouter une DACL

Accédez à Policy > Results > Authorization > Authorization Profiles, ajoutez un profil d'autorisation.

- Nom : MAR_Passed
- Nom DACL : MAR_Passed

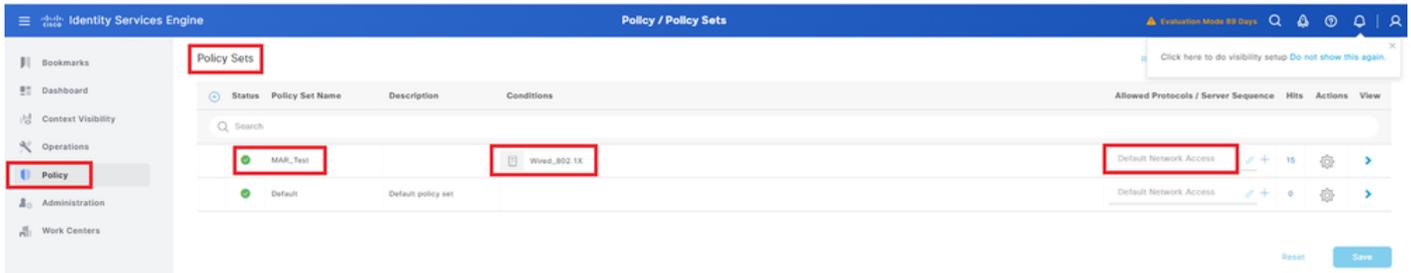


Ajouter un profil d'autorisation

Étape 6. Ajouter un jeu de stratégies

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

- Nom du jeu de stratégies : MAR_Test
- Conditions : Wired_802.1X
- Protocoles autorisés / Séquence de serveurs : Accès réseau par défaut

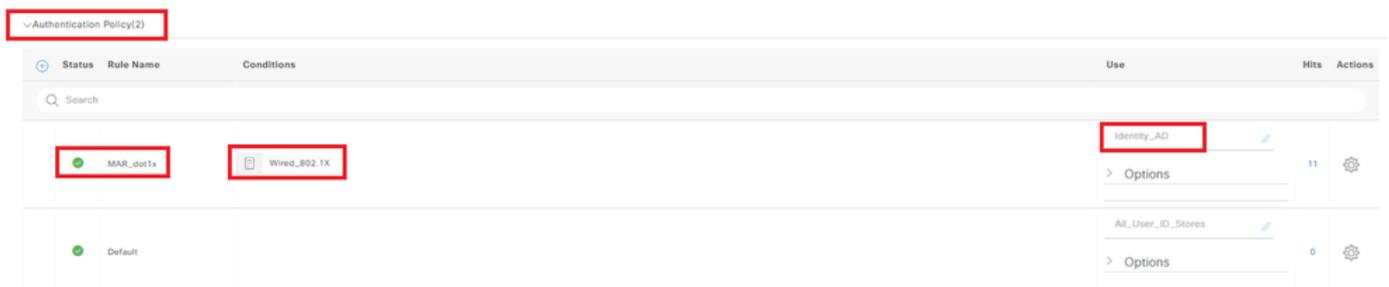


Ajouter un jeu de stratégies

Étape 7. Ajouter une stratégie d'authentification

Accédez à Jeux de stratégies, cliquez sur MAR_Test pour ajouter une stratégie d'authentification.

- Nom de la règle : MAR_dot1x
- Conditions : Wired_802.1X
- Utiliser : Identity_AD

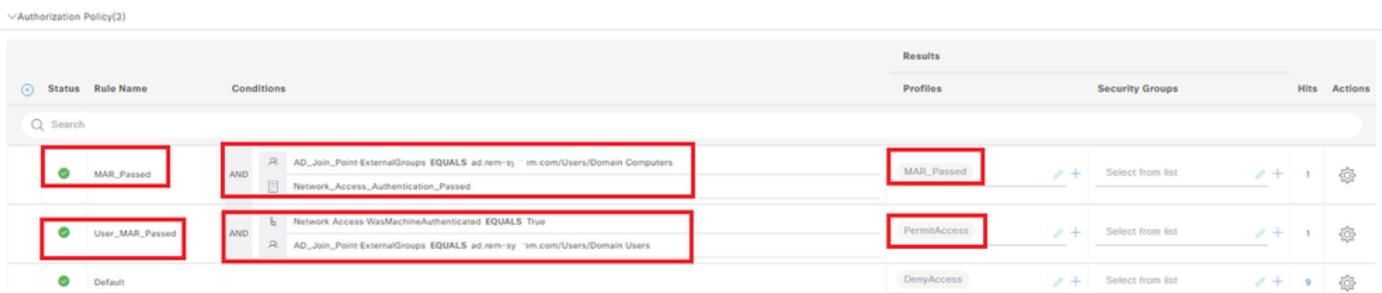


Ajouter une stratégie d'authentification

Étape 8. Ajouter une stratégie d'autorisation

Accédez à Jeux de stratégies, cliquez sur MAR_Test pour ajouter une stratégie d'autorisation.

- Nom de la règle : MAR_Passed
- Conditions : AD_Join_Point·ExternalGroups ÉGALE ad.rem-xxx.com/Users/Domain Ordinateurs ET Network_Access_Authentication_Passed
- Résultats : MAR_Passed
- Nom de la règle : User_MAR_Passed
- Conditions : Accès réseau·WasMachineAuthenticated EQUALS True ET AD_Join_Point·ExternalGroups EQUALS ad.rem-xxx.com/Users/Domain Utilisateurs
- Résultats : PermitAccess



Ajouter une stratégie d'autorisation

Vérifier

Modèle 1. Authentification des ordinateurs et des utilisateurs

Étape 1. Se déconnecter d'un PC Windows

Cliquez sur le bouton Déconnexion de Win10 PC1 pour déclencher l'authentification de l'ordinateur.

 Change account settings

 Lock

 Sign out

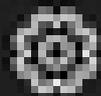
 Switch user

  FileZilla FTP Client

  Firefox

  G

  Get Help

  Google Chrome

  M

  Mail

show authentication sessions interface GigabitEthernet1/0/2 details la commande pour confirmer la session d'authentification de la machine dans C1000.

<#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:

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: 01C2006500000049AA780D80

Acct Session ID: 0x0000003C

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

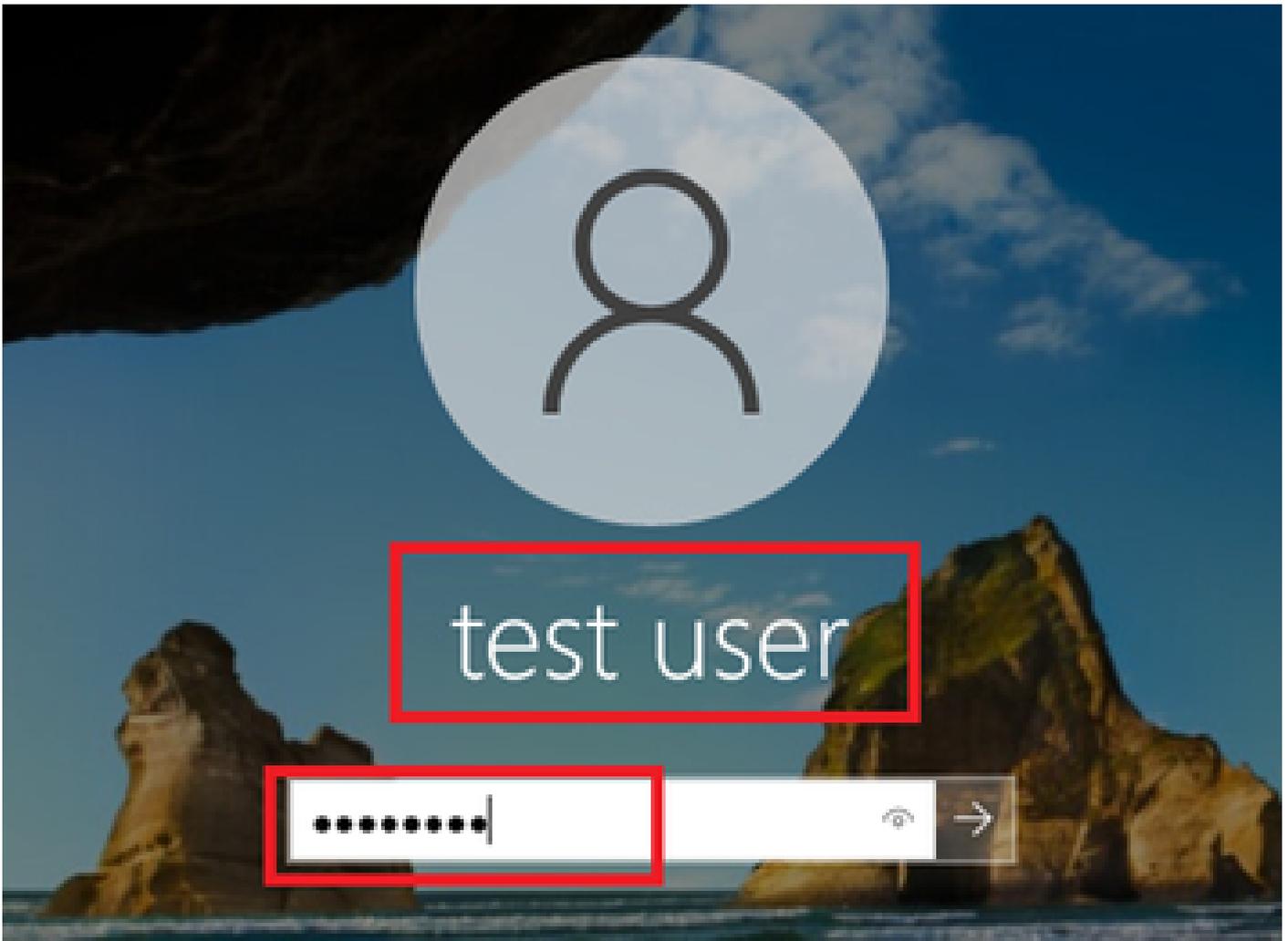
Method status list:

Method State

dot1x Authc Success

Étape 3. Connexion au PC Windows

Connectez-vous à Win10 PC1, entrez le nom d'utilisateur et le mot de passe pour déclencher l'authentification utilisateur.



Connexion au PC Windows

Étape 4. Confirmer la session d'authentification

Exécutez `show authentication sessions interface GigabitEthernet1/0/2 details` la commande pour confirmer la session d'authentification utilisateur dans C1000.

```
<#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: 0x0000003D
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

Étape 5. Confirmer le journal Radius en direct

Accédez à **Operations** > **RADIUS** > **Live Logs** dans l'interface utilisateur graphique ISE, confirmez le journal en direct pour l'authentification de la machine et l'authentification de l'utilisateur.

The screenshot displays the 'Live Logs' section of the ISE Operations / RADIUS interface. The table below shows the log entries:

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint P	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...
May 07, 2024 04:36:14...	●		0	AD\testuser	84-96-91-15-84...	Intel-Dev...	MAR_Test => MAR_dot1x	MAR_Test => User_MAR_Passed	PermiAccess	1.1.1.39	
May 07, 2024 04:36:13...	●			AD\testuser	84-96-91-15-84...	Intel-Dev...	MAR_Test => MAR_dot1x	MAR_Test => User_MAR_Passed	PermiAccess	1.1.1.39	C1000
May 07, 2024 04:35:12...	●			hso\DESKTOP-L2696-40-rem-1-r1m	84-96-91-15-84...	Intel-Dev...	MAR_Test => MAR_dot1x	MAR_Test => MAR_Passed	MAR_Passed	169.254.90.1...	C1000

Journal Radius Live

Confirmez le journal en direct détaillé de l'authentification de la machine.

Overview

Event	5200 Authentication succeeded
Username	host/DESKTOP-L2IL916.ad.rem-sy .em.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-L2IL916.ad.rem-sy .em.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
Authentication Protocol	PEAP (EAP-MSCHAPv2)

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

Détail de l'authentification machine

Confirmez le journal en direct détaillé de l'authentification utilisateur.

Overview

Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Endpoint Profile	Intel-Device
Authentication Policy	MAR_Test >> MAR_dot1x
Authorization Policy	MAR_Test >> User_MAR_Passed
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2024-05-07 16:36:13.748
Received Timestamp	2024-05-07 16:36:13.748
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	1.x.x.9
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C200650000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)

Steps

Step ID	Description	Latency (ms)
11001	Received RADIUS Access-Request - AD_Join_Point	
11017	RADIUS created a new session - ad.rem-sy .am.com	0
15049	Evaluating Policy Group - AD_Join_Point	0
15008	Evaluating Service Selection Policy	1
11507	Extracted EAP-Response/Identity	7
12500	Prepared EAP-Request proposing EAP-TLS with challenge	0
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	8
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	1
12625	Valid EAP-Key-Name attribute received	0
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	11
11018	RADIUS is re-using an existing session	0
12302	Extracted EAP-Response containing PEAP challenge-response and accepting PEAP as negotiated	0
61025	Open secure connection with TLS peer	0
12318	Successfully negotiated PEAP version 0	1
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	28
12810	Prepared TLS ServerDone message	0
12305	Prepared EAP-Request with another PEAP challenge	1
11006	Returned RADIUS Access-Challenge	0
11001	Received RADIUS Access-Request	30
11018	RADIUS is re-using an existing session	0
12304	Extracted EAP-Response containing PEAP challenge-	0

Détail de l'authentification utilisateur

Modèle 2. Authentification utilisateur uniquement

Étape 1. Désactiver et activer la carte réseau du PC Windows

Afin de déclencher l'authentification de l'utilisateur, désactivez et activez la carte réseau de Win10 PC1.

Étape 2. Confirmer la session d'authentification

Exécutez `show authentication sessions interface GigabitEthernet1/0/2 details` la commande pour confirmer la session d'authentification utilisateur dans C1000.

```
<#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: 0x0000003D
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

Étape 3. Confirmer le journal Radius en direct

Accédez à **Operations > RADIUS > Live Logs** dans l'interface utilisateur graphique ISE, confirmez le journal en direct pour l'authentification de l'utilisateur.

Remarque : le cache MAR étant stocké dans ISE, seule l'authentification des utilisateurs est nécessaire.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Identity Services Engine' and 'Operations / RADIUS'. The left sidebar contains various menu items, with 'Operations' selected. The main area displays a 'Live Logs' section with several summary cards: 'Misconfigured Supplicants', 'Misconfigured Network Devices', 'RADIUS Drops', 'Client Stopped Responding', and 'Repeat Counter', all showing a count of 0. Below these cards is a table of RADIUS logs. The table has columns for Time, Status, Details, Repeats, Identity, Endpoint ID, Endpoint IP, Authentication Policy, Authorization Policy, Authorization Profile, IP Address, and Network Device. A red box highlights a log entry for 'AD\testuser' with a status of 'Success' and a 'Repeat' count of 0. The entry shows a successful authentication for user 'AD\testuser' from endpoint '84-96-91-15-84...' on network device 'C1000'.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication Policy	Authorization Policy	Authorization P...	IP Address	Network De...
May 07, 2024 04:42:05...	Success		0	AD\testuser	84-96-91-15-84...	Intel-Devi...	MAR_Test == MAR_dot1x	MAR_Test == User_MAR_Passed	PermiAccess	1.1.1.1	C1000
May 07, 2024 04:42:04...	Success		0	AD\testuser	84-96-91-15-84...	Intel-Devi...	MAR_Test == MAR_dot1x	MAR_Test == User_MAR_Passed	PermiAccess	1.1.1.1	C1000
May 07, 2024 04:36:13...	Success		0	AD\testuser	84-96-91-15-84...	Intel-Devi...	MAR_Test == MAR_dot1x	MAR_Test == User_MAR_Passed	PermiAccess	1.1.1.1	C1000
May 07, 2024 04:35:12...	Success		0	WACSACLIP-MAR_Passed-6639ba20							C1000
May 07, 2024 04:35:12...	Success		0	hos\DESKTOP-L2L96-ad.rem-s..._sm...	84-96-91-15-84...	Intel-Devi...	MAR_Test == MAR_dot1x	MAR_Test == MAR_Passed	MAR_Passed	169.254.90.1...	C1000

Confirmez le journal en direct détaillé de l'authentification utilisateur.

Cisco ISE

Overview		Steps		
Event	5200 Authentication succeeded	Step ID	Description	Latency (ms)
Username	AD\testuser	11001	Received RADIUS Access-Request - AD_Join_Point	
Endpoint Id	B4:96:91:15:84:CB	11017	RADIUS created a new session - ad.rem-s...em.com	0
Endpoint Profile	Intel-Device	15049	Evaluating Policy Group - AD_Join_Point	1
Authentication Policy	MAR_Test >> MAR_dot1x	15008	Evaluating Service Selection Policy	0
Authorization Policy	MAR_Test >> User_MAR_Passed	11507	Extracted EAP-Response/Identity	16
Authorization Result	PermitAccess	12500	Prepared EAP-Request proposing EAP-TLS with challenge	2
		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
		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	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
		24432	Looking up user in Active Directory - AD\testuser	
		24355	LDAP fetch succeeded	
		24416	User's Groups retrieval from Active Directory succeeded	
		15048	Queried PIP - AD_Join_Point.ExternalGroups	11
		15016	Selected Authorization Profile - PermitAccess	5
		22081	Max sessions policy passed	0
		22080	New accounting session created in Session cache	0
		12306	PEAP authentication succeeded	0
		61026	Shutdown secure connection with TLS peer	0
		11503	Prepared EAP-Success	1
		11002	Returned RADIUS Access-Accept	2

Authentication Details	
Source Timestamp	2024-05-07 16:42:04.467
Received Timestamp	2024-05-07 16:42:04.467
Policy Server	ise33-01
Event	5200 Authentication succeeded
Username	AD\testuser
Endpoint Id	B4:96:91:15:84:CB
Calling Station Id	B4-96-91-15-84-CB
Endpoint Profile	Intel-Device
IPv4 Address	1.1.1.9
Authentication Identity Store	AD_Join_Point
Identity Group	Profiled
Audit Session Id	01C2006500000049AA780D80
Authentication Method	dot1x
Authentication Protocol	PEAP (EAP-MSCHAPv2)
Service Type	Framed
Network Device	C1000
CiscoAVPair	service-type=Framed, audit-session-id=01C2006500000049AA780D80, method=dot1x, AuthenticationIdentityStore=AD_Join_Point, FQSubjectName=2ce19620-0842-11ef-a5ec-362cec4b4f3d@testuser@ad.rem-sy...em.com, UniqueSubjectID=9273f674e52338d8f4807c495e1ff4c2ef9217f9
AD-Groups-Names	ad.rem-sy...em.com/Builtin/Users
AD-Groups-Names	ad.rem-sy...em.com/Builtin/Administrators
AD-Groups-Names	ad.rem-sy...em.com/Users/Denied RODC Password Replication Group
AD-Groups-Names	ad.rem-sy...em.com/Users/Domain Admins
AD-Groups-Names	ad.rem-sy...em.com/Users/Domain Users

Result

Détail de l'authentification utilisateur

Dépannage

Ces journaux de débogage (prtt-server.log) vous aident à confirmer le comportement détaillé de l'authentification dans ISE.

- runtime-config

- journalisation de l'exécution
- runtime-AAA

Ceci est un exemple du journal de débogage pour le **modèle 1. Authentification de l'ordinateur et authentification de l'utilisateur** dans ce document.

<#root>

// machine authentication

MAR,2024-05-08 16:54:50,582,DEBUG,0x7fb2fd3db700,cntx=0000034313,sesn=ise33-01/504417979/41,CPMSessionID=01C2006500000049AA780D8

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,CPMSessionID

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 and

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

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

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

// user authentication

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

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,CPMSessionID

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

Informations connexes

[Restrictions d'accès aux machines Avantages et inconvénients](#)

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.