Esempio di configurazione dei profili 802.1x EAP-TLS con confronto dei certificati binari da AD e NAM

Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Configurazione Topologia Dettagli topologia Flusso Configurazione degli switch Preparazione certificato Configurazione controller di dominio Configurazione supplicant **Configurazione ACS** Verifica Risoluzione dei problemi Impostazioni di ora non valide in ACS Nessun certificato configurato e associato al controller di dominio Active Directory Personalizzazione del profilo NAM Informazioni correlate

Introduzione

In questo documento viene descritta la configurazione 802.1x con EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) e ACS (Access Control System) in quanto questi eseguono un confronto binario tra un certificato client fornito dal richiedente e lo stesso certificato conservato in Microsoft Active Directory (AD). Il profilo AnyConnect Network Access Manager (NAM) viene usato per la personalizzazione. La configurazione per tutti i componenti è illustrata in questo documento, insieme a scenari per la risoluzione dei problemi relativi alla configurazione.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a <u>Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.</u>

Configurazione

Topologia

- Supplicant 802.1x Windows 7 con Cisco AnyConnect Secure Mobility Client release 3.1.01065 (modulo NAM)
- autenticatore 802.1x switch 2960
- Server di autenticazione 802.1x ACS release 5.4
- ACS integrato con Microsoft AD Controller di dominio Windows 2008 Server

Dettagli topologia

- ACS 192.168.10.152
- 2960 192.168.10.10 (e0/0 connessione supplicant)
- DC 192.168.10.101
- Windows 7 DHCP

Flusso

Sulla stazione di Windows 7 è installato AnyConnect NAM, che viene usato come supplicant per autenticarsi al server ACS con il metodo EAP-TLS. Lo switch con 802.1x funge da autenticatore. Il certificato utente viene verificato da ACS e l'autorizzazione criterio applica criteri basati sul nome comune (CN) del certificato. Inoltre, il servizio ACS recupera il certificato utente da AD ed esegue un confronto binario con il certificato fornito dal richiedente.

Configurazione degli switch

Lo switch ha una configurazione di base. Per impostazione predefinita, la porta è nella VLAN 666 in quarantena. Tale VLAN ha un accesso limitato. Dopo aver autorizzato l'utente, la porta VLAN viene riconfigurata.

aaa authentication login default group radius local aaa authentication dotlx default group radius aaa authorization network default group radius dotlx system-auth-control

interface Ethernet0/0
switchport access vlan 666
switchport mode access
ip device tracking maximum 10
duplex auto
authentication event fail action next-method
authentication order dot1x mab
authentication port-control auto
dot1x pae authenticator
end

radius-server host 192.168.10.152 auth-port 1645 acct-port 1646 key cisco

Preparazione certificato

Per EAP-TLS, è necessario un certificato sia per il richiedente che per il server di autenticazione. Questo esempio si basa sui certificati generati con OpenSSL. È possibile utilizzare Microsoft Certificate Authority (CA) per semplificare la distribuzione nelle reti aziendali.

1. Per generare la CA, immettere i seguenti comandi:

```
openssl genrsa -des3 -out ca.key 1024
openssl req -new -key ca.key -out ca.csr
cp ca.key ca.key.org
openssl rsa -in ca.key.org -out ca.key
openssl x509 -req -days 365 -in ca.csr -signkey ca.key -out ca.crt
Il certificato CA viene conservato nel file ca.crt e la chiave privata (e non protetta) nel file
```

ca.key.

2. Generare tre certificati utente e un certificato per ACS, tutti firmati da tale CA:

CN=prova1CN=prova2CN=prova3CN=acs54Lo script per generare un singolo certificato firmato dalla CA di Cisco è:

```
openssl genrsa -des3 -out server.key 1024
openssl req -new -key server.key -out server.csr
cp server.key server.key.org
openssl rsa -in server.key.org -out server.key
openssl x509 -req -in server.csr -CA ca.crt -CAkey ca.key -CAcreateserial
-out server.crt -days 365
```

openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt -certfile ca.crt La chiave privata si trova nel file server.key e il certificato nel file server.crt. La versione di

pkcs12 si trova nel file server.pfx.

3. Fare doppio clic su ogni certificato (file con estensione pfx) per importarlo nel controller di dominio. Nel controller di dominio tutti e tre i certificati devono essere attendibili.

| 📅 certmgr - [Certificates - Current | User\Personal\Certificate | | | | _ |
|---|---------------------------|--------------|--------------|--------------------------------------|----|
| File Action View Help | | | | | |
| 🧇 🔿 🖄 📆 🕹 🗙 🗒 | 🗟 🛛 🖬 | | (| ertificate X | ^ |
| Certificates - Current User | Issued To 🗠 | Issued By | | General Details Certification Path | - |
| E Personal | Administrator | Administrate | n | Certification path | |
| E Trusted Root Certification Author | E TAC | TAC | | TAC | |
| F Enterprise Trust | Saltest1 | TAC | | - 🕞 test3 | |
| 🗉 🚞 Intermediate Certification Autho | test3 | TAC | | | |
| 1 Active Directory User Object | | | | | |
| International Configuration | | | | | |
| Chrosted Certification At Third-Party Root Certification At | | | | | |
| 🗉 🚞 Trusted People | | | | | |
| 🗉 🛄 Certificate Enrolment Requests | | | | | |
| Smart Card Trusted Roots | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | Vew Certificate | |
| | | | | | |
| | | | | Certificate status: | |
| | • | | | This certificate is OK. | |
| | | | | | |
| - | | | | | |
| 🔒 Add roles | | Roles: | Active Direc | Learn more about certification paths | |
| | | | | | |
| Add features | | Features: | Group Polic | OK | CI |
| | | | | | |

Lo stesso processo può essere seguito in Windows 7 (supplicant) o utilizzare Active Directory per eseguire il push dei certificati utente.

Configurazione controller di dominio

Ènecessario mappare il certificato specifico all'utente specifico in AD.

- 1. Da Utenti e computer di Active Directory passare alla cartella Utenti.
- 2. Scegliere Caratteristiche avanzate dal menu Visualizza.

| Active Directory Users and Computers | |
|---|---|
| File Action View Help | |
| (nemove Columns | 7 🔁 🖗 |
| Active Direc Large Icons | Description |
| Saved (Small Icons | Wbudowane konto do ad |
| 🖂 🏭 cisco-te 🛛 List | . Wyznaczeni administrator |
| 🗄 🧮 Bull 🔹 Detail | . Wyznaczeni administrator |
| Con Con Contacte Groups and Computers as containers | . Wyznaczeni administrator |
| Don Osers, contacts, choops, and compaters as containers | . Grupa administratorów DNS |
| | . Klienci DNS, którzy są upo |
| | Wszyscy goście domeny |
| E Customize | Wbudowane konto do dos |
| Grupa bez re Security Group | Członkowie tej grupy nie |
| 🕫 🦰 NTDS Ouotas 🏻 🆓 Grupa z repli Security Group | Członkowie tej grupy mog |
| & Komputery d Security Group | Wszystkie stacje robocze i |
| & Kontrolery d Security Group | Wszystkie kontrolery dom |
| & Kontrolery d Security Group | Elementy członkowskie tej |
| & Kontrolery d Security Group | Elementy członkowskie tej |
| 🐍 krbtgt User | Konto usługi centrum dyst |
| Serwery RAS Security Group | Serwery w grupie mogą z |
| 🐍 test 1 User | |
| 🐍 test2 User | |
| 🔐 Twórcy-właś Security Group | Członkowie tej grupy mog |
| 🔐 Użytkownicy Security Group | Wszyscy użytkownicy do |
| & Wydawcy ce Security Group | Członkowie tej grupy maj |
| | |
| | |
| | |
| | |
| | |

- 3. Aggiungi questi utenti: test1test2test3Nota: La password non è importante.
- 4. Nella finestra Proprietà scegliere la scheda **Certificati pubblicati**. Scegliere il certificato specifico per il test. Ad esempio, per test1 l'utente CN è test1.**Nota:** Non utilizzare Mapping nomi (fare clic con il pulsante destro del mouse sul nome utente). Viene utilizzato per diversi servizi.

| File Action Were Help Image: Sever Queries Image: Type Description Image: Sever Queries Security Group Wyracceri at Image: Security Group Wyracceri at Image: Security Group Wyracceri at Image: Security Group Wyracceri at Image: Security Group Security Group Security Group Security Group Security Group Wyracceri at Image: Security Group Security | 🔁 Active Directory Users and Con | puters | | | test2 Properties |
|---|--|---|--|---|--|
| Image: Second | File Action View Help | | | | Security Environment Sessions Remote control |
| Active Directory Users and Comput Name Type Description Saved Queries Saved Queries Mainistrator User Woudowane Iv B Computers Administrator Security Group Wyznaczeni ac B Donain Controllers B Disadminis Security Group Wyznaczeni ac B Donain Controllers B Disadminis Security Group Wyznaczeni ac B Donain Controllers B Security Group Wyznaczeni ac Mainistrator Security Group Wyznaczeni ac B Donain Controllers B Security Group Grupa zefui. Security Group Grupa zefui. Security Group Wyznaczeni ac B Donain Controllers Bonaldminis Security Group Wiscowane Iv Security Group Wyznaczeni ac B DiscladetePr Security Group Security Group Wiscowane Iv Security Group Wiscowane Iv B DiscladetePr Security Group | 🇢 🔿 🔟 🚾 🖌 🗉 🗡 🖉 | 🗉 🚨 😹 🛯 🖬 | 1 2 2 3 7 | General Address Assessed Perfect Telephones Operation | |
| | Active Directory Users and Comput Saved Queries Cisco-test.com Cisco-test.com Computers Comput | Administrator Administrator Administrator Administrator Administrator Administrator DnsUpdatePr Cosć Cosć Cosć Cosć Cosć Cosć Cosć Cosć | Type User Security Group Security Group User Security Group Security Group Security Group Security Group Security Group Security Group Security Group Security Group | Członkowie tej | General Address Account Profile Telephones Organization Published Certificates Member OF Password Replication Dial-in Object List of X509 certificates published for the user account Issued To Issued By Intended Purposes Expiration Issued To Issued By Intended Purposes Expiration Image: Complex Profile TAC Server Authentication |
| UN Calloal Apply help | <u></u> | ļ | | | OK Cancel Apply Help |

In questa fase il certificato è associato a un utente specifico in Active Directory. È possibile verificare questa condizione tramite Idapsearch:

ldapsearch -h 192.168.10.101 -D "CN=Administrator,CN=Users,DC=cisco-test,DC=com" -w Adminpass -b "DC=cisco-test,DC=com"

Di seguito sono riportati alcuni risultati di esempio per test2.

test2, Users, cisco-test.com
dn: CN=test2,CN=Users,DC=cisco-test,DC=com

.....userCertificate:: MIICuDCCAiGgAwIBAgIJAP6cPWHhMc2yMA0GCSqGSIb3DQEBBQUAMFYxCzAJ BgNVBAYTA1BMMQwwCgYDVQQIDANNYXoxDzANBgNVBAcMBldhcnNhdzEMMAoGA1UECgwDVEFDMQwwC gYDVQQLDANSQUMxDDAKBgNVBAMMA1RBQzAeFw0xMzAzMDYxMjUzMjdaFw0xNDAzMDYxMjUzMjdaMF oxCzAJBgNVBAYTA1BMMQswCQYDVQQIDAJQTDEPMA0GA1UEBwwGS3Jha293MQ4wDAYDVQQKDAVDaXN jbzENMAsGA1UECwwEQ29yZTEOMAwGA1UEAwwFdGVzdDIwgZ8wDQYJKoZIhvcNAQEBBQADgY0AMIGJ AoGBAMFQZywrGTQKL+LeI19ovNavCFSG2zt2HGs8qGPrf/h3o4IIvU+nN6aZPdkTdsjiuCeav8HYD aRznaK1LURt1PeGtHlcTgcGZ1MwIGptimzG+h234GmPU59k4XSVQixARCDpMH8IBR9zOSWQLXe+kR iZpXC444eKOh6w0/+yWb4bAgMBAAGjgYkwgYYwCWYDVR0PBAQDAgTwMHcGA1UdJQRwMG4GCCsGAQU FBwMBBggrBgEFBQcDAgYKKwYBBAGCNwoDBAYLKwYBBAGCNwoDBAEGCCsGAQUFBwMBBggrBgEFBQgC FQYKKwYBBAGCNwoDAQYKKwYBBAGCNxQCAQYJKwYBBAGCNxUGBggrBgEFBQcDAjANBgkqhkiG9w0BA QUFAAOBgQCuXwAgcYqLNm6gEDTWm/OWmTFjPyA5KSDB76yVqZwr11ch7eZiNSmCtH7Pn+VILagf9o tiF15ttk9KX6tIvbeEC4X/mQVgAB3HuJH5sL1n/k2H10XCXKfMqMGrtsZrA64tMCcCeZRoxfAO94n PulwF4nkcnu1x0/B7x+LpcjxjhQ==

Configurazione supplicant

- 1. Installare questo editor di profili, anyconnect-profileeditor-win-3.1.00495-k9.exe.
- 2. Aprire l'Editor profili di Network Access Manager e configurare il profilo specifico.
- 3. Creare una rete cablata specifica.

| File Help | | | | | | |
|------------------|---------|----------------------------|------------------|----------------|--------|---|
| Network Access N | fanager | Networks Profile: C:\1\ | prof1.xml | | | |
| Networks | 05 | Network | | | | - |
| | - | Name | Media Type | Group* | | |
| | | my configured 802 | 1x profile Wired | Local networks | Add | |
| | | | | | Delete | |

In questa fase è molto importante offrire all'utente la possibilità di utilizzare il certificato per ogni autenticazione. Non memorizzare nella cache tale scelta. Utilizzare inoltre 'username' come ID non protetto. È importante ricordare che non si tratta dello stesso ID utilizzato da ACS per eseguire una query su AD per il certificato. L'ID verrà configurato in ACS.

| Network Access Manager | Networks Profile: C:\1\prof1.xml | [username] | Media Type Security Leve Connection Ty User Auth |
|------------------------|--|--|---|
| | User Credentials Use Single Sign On Credentials Prompt for Credentials Remember Forever Remember while User is Never Remember | (Requires Smart Card) Logged On | Crebentias |
| | Certificate Sources Smart Card or OS certificates Smart Card certificates only | Remember Smart Card Pin Remember Forever Remember while User is Logged On Never Remember | |

- 4. Salvare il file con estensione xml come c:\Users\All Users\Cisco\Cisco AnyConnect Secure Mobility Client\Network Access Manager\system\configuration.xml.
- 5. Riavviare il servizio Cisco AnyConnect NAM.

Nell'esempio è illustrata una distribuzione manuale del profilo. AD potrebbe essere utilizzato per distribuire il file per tutti gli utenti. Inoltre, se integrata con le VPN, l'ASA può essere utilizzata per effettuare il provisioning del profilo.

Configurazione ACS

1. Aggiungere il computer al dominio Active

| Directory. | | | | | | | | | | | |
|--|--|---|-------------------------|----------------|--------------------------------|--|--|--|--|--|--|
| * 😚 My Workspace | pace Users antidently Stores > External identity Stores > Active Directory | | | | | | | | | | |
| * * Network Resources * Deers and Identity Stores Identity Groups | General Directory Group Connection Details | s Directory Atributes Man | Nne Access Restrictions | | | | | | | | |
| Internal Identity Stores | Node | Node Naide Rate Status Domain Name Domain Control of Name | | | | | | | | | |
| Hosts | ace54 | Primary | Joined and Connected | cisco-test.com | win-grag7twttmt.cisco-test.com | | | | | | |
| External Identity Stores LDAP | Join/Test Connection | Leave | • | | | | | | | | |
| RSA Security Networks RSA Security Televisies RADIUS Identify Servers Centricate Authentication Profile Menthy Store Sequences Policy Elements Construction Security Security Construction Security Securit | Click on Save Changes' to save AD configuration. Once you have successfully connected to the Domain, you can select Directory Oncups and Directory Attributes to be available for uses in policy rules. Pressing on 'Clear Configuration' will remove the AD configuration and remove ADS machine from the Domain. End User Authentication Settings End User Authentication Settings End User Authentication Settings End User Authentication End User Authentication | | | | | | | | | | |
| Moniforing and Reports | e = Required fields | | | | | | | | | | |
| a M Bankarn Administration | | | | | | | | | | | |

ACS confronta i nomi utente AD con l'utilizzo del campo CN del certificato ricevuto dal richiedente (in questo caso test1, test2 o test3). È inoltre abilitato il confronto binario. In questo modo ACS ottiene il certificato utente da AD e lo confronta con lo stesso certificato ricevuto dal richiedente. Se non corrisponde, l'autenticazione non riesce.

| 🕨 🥳 My Workspace | Users and Identity Stores > Certificate Authentication Profile > Edit "cert profile 2" |
|--|---|
| Network Resources Users and Identity Stores Identity Groups Internal Identity Stores Users Hosts External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authorities | General ○ Name: cert profile 2 Description: Certificate Definition Principal Username X509 Attribute: Common Name ✓ Perform Binary Certificate Comparison with Certificate retrieved from LDAP or Active Directory Name: AD1 Select ○ = Required fields |
| Identity Store Sequences Identity Store Sequences Policy Elements Access Policies Monitoring and Reports System Administration | |

2. Configurare le sequenze dell'archivio identità, che utilizza AD per l'autenticazione basata su certificati insieme al profilo del certificato.

| Network Resources Centeral Users and identity Stores Identity Groups Internal Identity Stores Users Hosts Extarnal Identity Stores LDAP Active Directory RADIUS Identity Servers Certificate Authonities Access Policies Monitoring and Reports System Administration | My Workspace | Users and identity Stores > identity Store Sequences > Edit: "seq" |
|---|--|---|
| ✓ Users and identity Stores Identity Groups ✓ Internal Identity Stores Users ✓ External Identity Stores LDAP Active Directory RSA SecurID Token Servers RADIUS Identity Servers Certificate Authentication Profile ✓ Password Based Additional Attribute Retrieval Search List An optional set of additional identity stores from which attributes will be retrieved Available ✓ Policy Elements ✓ Access Policies ✓ Monitoring and Reports ✓ System Administration ✓ Advanced Options | Network Resources | General |
| | Solution System Administration System Administration | Image: Seq Description: Authentication Method List Image: Certificate Based Certificate Based Image: Password Based Additional Attribute Retrieval Search List An optional set of additional identity stores from which attributes will be retrieved Available Selected Internal Hosts Internal Users NAC Profiler Win2k3 Advanced Options Image: Particular fields |

Utilizzato come origine identità nei criteri di identità RADIUS.

| 🕨 😚 My Workspace | Access Policies > Access Services > Default Network Access > Identity |
|--|---|
| Network Resources | Single result selection O Rule based result selection |
| Users and Identity Stores | Identity Source: seq Select |
| Policy Elements | Advanced Options |
| 👻 🌉 Access Policies | |
| Access Services Service Selection Rules O Default Device Admin Identity Authorization O Default Network Access Identity Authorization | |
| Max User Session Policy Max Session User Settings Max Session Group Settings | |
| Monitoring and Reports | |
| System Administration | |

3. Configurare due criteri di autorizzazione. Il primo criterio viene utilizzato per test1 e nega l'accesso all'utente. Il secondo criterio viene utilizzato per il test 2 e consente l'accesso con il profilo

| VLAN2. | | | | | | | | | | |
|--|---------|--------------------------------|-----------|----------------------------|------------------|---------------|---|-----------------------------------|-----------|--|
| 🔸 🞲 Ny Workspace | Arcents | Philip into | » Access | Services > Default Network | Access > Autoria | ation | | | | |
| Network Resources | Standa | and Pol | icy Excer | tion Policy | | | | | | |
| 🔹 👪 Users and Identity Stores | Netw | ander Feiner Aufherinden Beker | | | | | | | | |
| Policy Elements | T Her | | | Harts B. C. | unte de l'Es | abian india | Class Tiles Or - | | | |
| 🔹 🛼 Access Policies | 100 | 514 | us | * Nachit Et | trais 🔺 En | enico + | Grear Priter Go | | | |
| Access Services Service Selection Rules | | | Status | Name | NDB:Location | Time And Date | Conditions Compound Condition | Results Authorization Profiles | Hit Count | |
| 👻 😑 Default Device Admin | 5 | | | <u>ONtesti</u> | ANY | -ANY | Certificate Dictionary:Common Name equals test1 | DenyAccess | 6 | |
| Identity Automization | 8 | | | Chites:2 | -ANY- | -ANH | Certificate Dictionary:Common Name equals test2 | vtan2 | 7 | |
| | | | | | | | | | | |

VLAN2 è il profilo di autorizzazione che restituisce gli attributi RADIUS che associano l'utente alla VLAN2 sullo switch.

| My Workspace | Policy Elements > Authorization and Permissions > Network Access > Authorization Profiles > Edit "\ |
|---|--|
| In the sources | |
| B Users and Identity Stores | General Common Tasks RADIUS Attributes |
| 🔹 🎭 Policy Elements | Downloadable ACL Name: Not in Use 💌 |
| Session Conditions Date and Time Custom Network Conditions End Station Filters Device Filters Device Port Filters Authorization and Permissions Network Access Authorization Profiles Device Administration Shell Profiles Command Sets | Filter-ID ACL: Not in Use Proxy ACL: Not in Use Voice VLAN Permission to Join: Not in Use VLAN VLAN VLAN ID/Name: Static Walue 2 Reauthentication Reauthentication Timer: Not in Use Maintain Connectivity during Reauthentication: QOS |
| Named Permission Objects Downloadable ACLs | Input Policy Map: Not in Use Output Policy Map: Not in Use R02 1Y PEV |
| Access Policies Monitoring and Reports System Administration | LinkSec Security Policy: Not in Use URL Redirect When a URL is defined for Redirect an ACL must also be defined URL for Redirect: Not in Use URL Redirect ACL: Not in Use C = Required fields |

4. Installare il certificato CA su

| ACS. | | | | | | | | | | |
|--|-----------|---|---------|------------------|-----------|-----------|-------------|--|--|--|
| 🕨 😚 My Workspace | Users and | Jsers and identity Stores > Certificate Authorities | | | | | | | | |
| Network Resources | Certifi | Certificate Authorities | | | | | | | | |
| 🔹 🎒 Users and Identity Stores | Filter | | [▼ Ma | tch if: | [▼ Go ▼ | | | | | |
| Identity Groups | | | | | | | | | | |
| | | Friendly Name | - | Expiration | Issued To | Issued By | Description | | | |
| Users | | TAC | | 08:11 16.11.2013 | TAC | TAC | | | | |
| Hosts | _ | | | | | | | | | |
| External Identity Stores | | | | | | | | | | |
| LDAP | | | | | | | | | | |
| Active Directory | | | | | | | | | | |
| RSA SecurID Token Servers | | | | | | | | | | |
| RADIUS Identity Servers | | | | | | | | | | |
| Certificate Authorities | | | | | | | | | | |
| Certificate Authentication Profile | | | | | | | | | | |
| Identity Store Sequences | | | | | | | | | | |

5. Generare e installare il certificato (per l'utilizzo del protocollo Extensible Authentication Protocol) firmato dalla CA di Cisco per ACS.

| ➤ I MyWorkspace | System | Administration > Conf | guratio | n > Local Server Cen | ificates > Local (| Sertific | cates | | |
|---|--------|-----------------------|---------|----------------------|--------------------|----------|------------------|-----------------------|---------------------------|
| By Network Resources | Loca | I Certificates | | | | | | | |
| Busers and Identity Stores | Fifte | r. | | Match if: | [*] | Gr | | | |
| Policy Elements | | | | | | _ | | | |
| Access Policies | | Friendly Name | * | Issued to | Issued By | | Valid From | valid to (expiration) | Protocol |
| Monitoring and Reports | 븝 | <u>acs54</u> | | acso4 | DAG | | 09:23 22:02:2013 | 09:23 22:02:2014 | EAP, Management Interface |
| System Administration Aumorearion Users Authentication Settings Max User Session Slobal Settings Purge User Session Operations Distributed System Management Software Repositories Scheduled Backups Local Operations Configuration Clobal System Options TACACS+ Settings EAP-FLS Settings EAP-FLS Settings EAP-FAST Satings Generate PAD RSA SecuritD Prompts Dictionaries Protocols Identity Local Server Certificates Local Server Certificates Dustanding Signing Requests | | <u>acs54</u> | | acs54 | ac554 | | 17:21 18.02.2013 | 17:21 18.05.2013 | ΝA |

Verifica

Èbuona norma disabilitare il servizio 802.1x nativo sul supplicant Windows 7 poiché viene utilizzato AnyConnect NAM. Con il profilo configurato, il client può selezionare un certificato specifico.

| + | | | |
|---|---|---|-------------------|
| | Cisco AnyConnect | | |
| | Choose certificate for the connection my configured | Cisco AnyConnect Secure Mobility Client | |
| | test3@ test3@ test2@ | VPN: Verify your network connection. | Connect |
| / | test1@ Issued By: TAC | No Network Connectivity | |
| | Expiration Date: 2014-03-06 12:54:24 UTC Serial Number: FE9C3D61E131CDB3 | Network: Authenticating | |
| | OK Cancel | my configured 802.1x profile | « • := |
| | | ‡ () | -ditalit cisco |

Quando si utilizza il certificato test2, lo switch riceve una risposta di esito positivo insieme agli attributi RADIUS.

| 00:02:51: %DOT1X-5-SUCCESS: Authentication successful for client | |
|--|------|
| (0800.277f.5f64) on Interface Et0/0 | |
| 00:02:51: %AUTHMGR-7-RESULT: Authentication result 'success' from 'dot | :1x' |
| for client (0800.277f.5f64) on Interface Et0/0 | |

```
switch#
00:02:51: %EPM-6-POLICY_REQ: IP=0.0.0.0| MAC=0800.277f.5f64|
AUDITSESID=C0A80A0A0000001000215F0| AUTHTYPE=DOT1X|
EVENT=APPLY
```

```
switch#show authentication sessions interface e0/0
```

```
Interface: Ethernet0/0
         MAC Address: 0800.277f.5f64
          IP Address: Unknown
          User-Name: test2
          Status: Authz Success
          Domain: DATA
      Oper host mode: single-host
    Oper control dir: both
       Authorized By: Authentication Server
        Vlan Policy: 2
     Session timeout: N/A
       Idle timeout: N/A
  Common Session ID: COA80A0A00000001000215F0
     Acct Session ID: 0x0000005
          Handle: 0xE8000002
Runnable methods list:
```

Method State dotlx Autho Succes

Notare che la VLAN 2 è stata assegnata. È possibile aggiungere altri attributi RADIUS a tale profilo di autorizzazione in ACS (ad esempio, Advanced Access Control List o timer di riautorizzazione).

I log su ACS sono i seguenti:

| | 12813 | Extracted TLS CertificateVerify message. |
|---|----------------|--|
| | 12804 | Extracted TLS Finished message. |
| | 12801 | Prepared TLS ChangeCipherSpec message. |
| | 12802 | Prepared TLS Finished message. |
| | 12816 | TLS handshake succeeded. |
| | 12509 | EAP-TLS full handshake finished successfully |
| | 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 challenge-response |
| | <u>Evaluat</u> | ting Identity Policy |
| | 15006 | Matched Default Rule |
| | 24432 | Looking up user in Active Directory - test2 |
| | 24416 | User's Groups retrieval from Active Directory succeeded |
| | 24469 | The user certificate was retrieved from Active Directory successfully. |
| | 22054 | Binary comparison of certificates succeeded. |
| | 22037 | Authentication Passed |
| | 22023 | Proceed to attribute retrieval |
| | 22038 | Skipping the next IDStore for attribute retrieval because it is the one we authenticated against |
| | 22016 | Identity sequence completed iterating the IDStores |
| | <u>Evaluat</u> | ing Group Mapping Policy |
| | 12506 | EAP-TLS authentication succeeded |
| | 11503 | Prepared EAP-Success |
| | <u>Evaluat</u> | ing Exception Authorization Policy |
| | 15042 | No rule was matched |
| | <u>Evaluat</u> | ting Authorization Policy |
| | 15004 | Matched rule |
| | 15016 | Selected Authorization Profile - vlan2 |
| | 22065 | Max sessions policy passed |
| | 22064 | New accounting session created in Session cache |
| l | 11002 | Returned RADIUS Access-Accept |

Risoluzione dei problemi

Impostazioni di ora non valide in ACS

Errore possibile - errore interno in ACS Active Directory

12504 Extracted EAP-Response containing EAP-TLS challenge-response 12571 ACS will continue to CRL verification if it is configured for specific CA 12571 ACS will continue to CRL verification if it is configured for specific CA 12811 Extracted TLS Certificate message containing client certificate. 12812 Extracted TLS ClientKeyExchange message. 12813 Extracted TLS CertificateVerify message. 12804 Extracted TLS Finished message. 12801 Prepared TLS ChangeCipherSpec message. 12802 Prepared TLS Finished message. 12816 TLS handshake succeeded. 12509 EAP-TLS full handshake finished successfully 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 challenge-response Evaluating Identity Policy 15006 Matched Default Rule 24432 Looking up user in Active Directory - test1 24416 User's Groups retrieval from Active Directory succeeded 24463 Internal error in the ACS Active Directory 22059 The advanced option that is configured for process failure is used. 22062 The 'Drop' advanced option is configured in case of a failed authentication request.

Nessun certificato configurato e associato al controller di dominio Active Directory

Errore possibile - impossibile recuperare il certificato utente da Active Directory

| 12571 / | ACS will continue to CRL verification if it is configured for specific CA |
|----------|--|
| 12811 | Extracted TLS Certificate message containing client certificate. |
| 12812 | Extracted TLS ClientKeyExchange message. |
| 12813 | Extracted TLS CertificateVerify message. |
| 12804 | Extracted TLS Finished message. |
| 12801 | Prepared TLS ChangeCipherSpec message. |
| 12802 | Prepared TLS Finished message. |
| 12816 | TLS handshake succeeded. |
| 12509 | EAP-TLS full handshake finished successfully |
| 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 challenge-response |
| Evaluati | ing Identity Policy |
| 15006 | Matched Default Rule |
| 24432 | Looking up user in Active Directory - test2 |
| 24416 | User's Groups retrieval from Active Directory succeeded |
| 24100 | Some of the expected attributes are not found on the subject record. The default values, if configured, will be used for these attributes. |
| 24468 | Failed to retrieve the user certificate from Active Directory. |
| 22049 | Binary comparison of certificates failed |
| 22057 | The advanced option that is configured for a failed authentication request is used. |
| 22061 | The 'Reject' advanced option is configured in case of a failed authentication request. |
| 12507 | EAP-TLS authentication failed |
| 11504 | Prepared EAP-Failure |
| 11003 | Returned RADIUS Access-Reject |

Personalizzazione del profilo NAM

Nelle reti aziendali, si consiglia di eseguire l'autenticazione con l'utilizzo di certificati sia del computer che dell'utente. In questo scenario, si consiglia di utilizzare la modalità 802.1x aperta sullo switch con VLAN limitata. Al riavvio del computer per 802.1x, la prima sessione di autenticazione viene avviata e autenticata con il certificato del computer AD. Quindi, dopo che l'utente ha fornito le credenziali e ha effettuato l'accesso al dominio, viene avviata la seconda sessione di autenticazione con il certificato utente. L'utente utilizza la VLAN corretta (attendibile) con accesso completo alla rete. Si integra perfettamente con Identity Services Engine (ISE).



Èquindi possibile configurare autenticazioni separate dalle schede Autenticazione computer e

Autenticazione utente.

Se la modalità 802.1x aperta non è accettabile sullo switch, è possibile utilizzare la modalità 802.1x prima che la funzionalità di accesso sia configurata nella policy del client.

Informazioni correlate

- Guida per l'utente di Cisco Secure Access Control System 5.3
- Guida dell'amministratore di Cisco AnyConnect Secure Mobility Client, versione 3.0
- AnyConnect Secure Mobility Client 3.0: Network Access Manager ed Editor di profili su Windows
- Documentazione e supporto tecnico Cisco Systems