# ACS 5.x e versioni successive - Configurazione dell'integrazione con Microsoft AD

# Sommario

Introduzione Prerequisiti Requisiti Componenti usati Convenzioni Premesse Configurazione Configurazione di ACS 5.x Application Deployment Engine (ADE-OS) Aggiungi ACS 5.x ad AD Configura servizio di Access Verifica Informazioni correlate

# Introduzione

In questo documento viene fornita una configurazione di esempio per integrare Microsoft Active Directory con Cisco Secure Access Control System (ACS) 5.x e versioni successive. ACS utilizza Microsoft Active Directory (AD) come archivio identità esterno per archiviare risorse quali utenti, computer, gruppi e attributi. ACS autentica queste risorse in base ad AD.

# Prerequisiti

#### Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

- Il dominio di Windows Active Directory da utilizzare deve essere completamente configurato e operativo.
- Utilizzare Dominio di Microsoft Windows Server 2003, Dominio di Microsoft Windows Server 2008 o Dominio di Microsoft Windows Server 2008 R2, in quanto sono supportati da ACS 5.x.Nota: l'integrazione del dominio di Microsoft Windows Server 2008 R2 con ACS è supportata da ACS 5.2 e versioni successive.

#### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e

hardware:

- Cisco Secure ACS 5.3
- Dominio di Microsoft Windows Server 2003

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</u> <u>dei documenti.</u>

### **Premesse**

In Windows Active Directory sono disponibili molte funzionalità utilizzate nell'utilizzo quotidiano della rete. L'integrazione di ACS 5.x con AD consente l'utilizzo degli utenti di AD esistenti, dei computer e del relativo mapping di gruppo.

ACS 5.x integrato con AD offre le seguenti funzioni:

- 1. Autenticazione computer
- 2. Recupero attributi per autorizzazione
- 3. Recupero certificato per autenticazione EAP-TLS
- 4. Restrizioni account utente e computer
- 5. Restrizioni accesso computer
- 6. Controllo autorizzazioni chiamate in ingresso
- 7. Opzioni di richiamata per gli utenti che eseguono chiamate in ingresso
- 8. Attributi del supporto dial-in

# **Configurazione**

#### Configurazione di ACS 5.x Application Deployment Engine (ADE-OS)

Prima di integrare ACS 5.x in Active Directory, verificare che **TimeZone, Date & Time** su ACS corrisponda a quello sul controller di dominio primario di Active Directory. Inoltre, definire il server DNS su ACS per essere in grado di risolvere il nome di dominio da ACS 5.x. Completare questa procedura per configurare ACS 5.x Application Deployment Engine (ADE-OS):

- 1. SSH all'accessorio ACS e immettere le credenziali CLI.
- 2. Eseguire il comando **clock timezone** in modalità config come mostrato di seguito per configurare il **timezone** sull'ACS in modo che corrisponda a quello del controller di dominio.

clock timezone Asia/Kolkata

**Nota:** Asia/Calcutta è il fuso orario usato in questo documento. Per individuare il fuso orario specifico, usare il comando **show timezones in** modalità di esecuzione.

3. Se il controller di dominio Active Directory è sincronizzato con un server NTP che risiede nella rete, è consigliabile utilizzare lo stesso server NTP nell'ACS. Se non si dispone di un server NTP, andare al passaggio 4. Per configurare il server NTP, procedere come segue:Il server NTP può essere configurato con il comando <indirizzo ip server NTP> del server NTP in modalità di configurazione, come mostrato di seguito.

ntp server 192.168.26.55 The NTP server was modified.

If this action resulted in a clock modification, you must restart ACS.

Per ulteriori informazioni, fare riferimento al documento ACS 5.x: Esempio di

sincronizzazione Cisco ACS con il server NTP per ulteriori informazioni sulla configurazione NTP.

4. Per configurare manualmente data e ora, utilizzare il comando **clock set** in **modalità di esecuzione**. Di seguito è riportato un esempio:

```
clock set Jun 8 10:36:00 2012
Clock was modified. You must restart ACS.
Do you want to restart ACS now? (yes/no) yes
Stopping ACS.
Stopping Management and View.....
Stopping Runtime.....
Stopping Database...
Cleanup....
Starting ACS ....
```

To verify that ACS processes are running, use the 'show application status acs' command.

5. Verificare ora il **fuso orario, la data** e l'**ora** con il comando **show clock**. Di seguito è riportato l'output del comando show clock:

acs51/admin# **show clock** Fri Jun 8 10:36:05 IST 2012

6. Configurare DNS su ACS con il comando <ip name-server <ip address of the DNS> in modalità di configurazione, come mostrato di seguito: ip name-server 192.168.26.55

Nota: l'indirizzo IP DNS viene fornito dall'amministratore del dominio Windows.

7. Utilizzare il comando **nslookup <nome dominio>** per verificare che il nome di dominio sia raggiungibile, come mostrato.

```
acs51/admin#nslookup MCS55.com

Trying "MCS55.com"

;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 60485

;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:

;MCS55.com. IN ANY

;; ANSWER SECTION:

MCS55.com. 600 IN A 192.168.26.55

MCS55.com. 3600 IN NS admin-zq2ttn9ux.MCS55.com.

MCS55.com. 635 900 600 86400 3600

;; ADDITIONAL SECTION:

admin-zq2ttn9ux.MCS55.com. 3600 IN A 192.168.26.55
```

Received 136 bytes from 192.168.26.55#53 in 0 ms

**Nota:** se la **SEZIONE RISPOSTA** è vuota, contattare l'amministratore di dominio di Windows per individuare il server DNS corretto per il dominio.

8. Usare il comando **ip domain-name <nome dominio>** per configurare **DOMAIN-NAME** sull'ACS, come mostrato di seguito:

ip domain-name MCS55.com

 Utilizzare il comando hostname <hostname> per configurare HOSTNAME sull'ACS, come mostrato di seguito:

hostname acs51

**Nota:** a causa dei limiti di NETBIOS, i nomi host ACS devono contenere un numero di caratteri inferiore o uguale a 15.

10. Usare il comando Write memory per salvare la configurazione su ACS.

#### Aggiungi ACS 5.x ad AD

Completare questa procedura per aggiungere ACS5.x ad AD:

1. Scegliere Utenti e archivi identità > Archivi identità esterni > Active Directory e specificare il nome di dominio, l'account AD (nome utente) e la relativa password, quindi fare clic su Test connessione.Nota: l'account AD richiesto per l'accesso al dominio in ACS deve avere una delle caratteristiche seguenti:Aggiungere workstation al diritto utente del dominio nel dominio corrispondente.Autorizzazione Crea oggetti computer o Elimina oggetti computer nel contenitore computer corrispondente in cui viene creato l'account del computer ACS prima di aggiungere il computer ACS al dominio.Nota: Cisco consiglia di disabilitare il criterio di blocco per l'account ACS e configurare l'infrastruttura AD in modo che invii avvisi all'amministratore se per l'account viene utilizzata una password errata. Infatti, se si immette una password errata, ACS non crea né modifica il proprio account computer quando necessario e quindi probabilmente nega tutte le autenticazioni.Nota: l'account Windows AD, che aggiunge ACS al dominio AD, può essere inserito nella propria unità organizzativa. Si trova nella propria unità organizzativa al momento della creazione dell'account o in un secondo momento con una restrizione che prevede che il nome dell'accessorio corrisponda al nome dell'account

General		
Connection Details		
Active Directory Domain Name:	MCS55.com	
Please specify the credentials used to,	oin this machine to the Active Directory Domain:	
🜣 Usemame:	training	
Password:		
Vou may use the Text Connection Duty	n in annung madaritate and evened and federa Directors P	resin is reachable.
rou may use the rest Connection Build	into ensure credentials are correct and Active Directory D	main is reachable.
	To all Operational Sectors	
	Test Connection	
	Test Connection	
Click on 'Save Changes' to connect to t	Test Connection	ice you have successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to t Directory Groups and Directory Attribute	Test Connection the Active Directory Domain and save this configuration. O is to be available for use in policy rules.	ice you have successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to t Directory Groups and Directory Athibute	Test Connection the Active Directory Domain and save this configuration. O is to be available for use in policy rules.	ice you have successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to t Directory Groups and Directory Athibute End User Authentication Settings	Test Connection the Active Directory Domain and save this configuration. O is to be available for use in policy rules.	ice you have successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to t Directory Groups and Directory Attribute End User Authentication Settings I Enable password change	Test Connection the Active Directory Domain and save this configuration. O is to be available for use in policy rules.	ice you have successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to 1 Directory Groups and Directory Attribute End User Authentication Settings Denable password change Denable machine authentication	Test Connection the Active Directory Domain and save this configuration. O is to be available for use in policy rules.	ice you have successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to 1 Directory Groups and Directory Attribute End User Authentication Settings Directory Enable password change Enable machine authentication Enable Machine Access Restrict	Test Connection te Active Directory Domain and save this configuration. O is to be available for use in policy rules.	ice you have successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to t Directory Groups and Directory Attribute End User Authentication Settings Directory Enable password change Enable machine authentication Enable Machine Access Restrict Acting time (hours):	Test Connection the Active Directory Domain and save this configuration. O is to be available for use in policy rules.	ice you have successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to t Directory Groups and Directory Athibute End User Authentication Settings Enable password change Enable Machine Access Restrict Aging time (hours): Enable dial-in check	Test Connection the Active Directory Domain and save this configuration. O is to be available for use in policy rules.	ice you have successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to 1 Directory Groups and Directory Athibute Ind User Authentication Settings I Enable password change Enable Machine Access Restrict Aging time (hours): Enable dial-in check Enable caliback check for dial-in	Test Connection the Active Directory Domain and save this configuration. O is to be available for use in policy rules. ions	ice you have successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to 1 Directory Groups and Directory Attribute End User Authentication Settings C Enable password change E Enable machine authentication E Enable Machine Access Restrict Aging time (hours): E Enable dial-in check E Enable caliback check for dial-in Connectivity Status	Test Connection the Active Directory Domain and save this configuration. O is to be available for use in policy rules. tions	ice you have successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to 1 Directory Groups and Directory Athibute End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrict Aging time (hours): Enable disi-in chack Enable caliback check for diai-in Connectivity Status Joined to Domain. Connectivity Sta	Test Connection the Active Directory Domain and save this configuration. O is to be available for use in policy rules. tions clients duest:	ice you have successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to 1 Directory Groups and Directory Athibute End User Authentication Settings Enable password change Enable Machine Access Restrict Aging time (hours): Enable dial-In check Enable caliback check for dial-in Connectivity Status Janed to Domain. Connectivity Sta = Required fields	Test Connection the Active Directory Domain and save this configuration. O is to be available for use in policy rules. tions output: dients shus:	ice you have successfully connected to the Domain, you can select the

2. In questa schermata viene mostrato come il test della connessione ad Active Directory sia

# riuscito. Quindi fare clic su OK.

ieneral 🗋										
onnection Details										
Active Directory Domain Name.	MCS55.com									
lease specify the credentials used to join		2								
Usemame:										
	Connection test to 'MCS55.com' succeeded.	1								
Password:										
na colomá a talica omá a t <mark>alic</mark> .		12.12								
ou may use the Test Connection Butten to	OK	ctory Do	main is	read	hable	÷., ;				
s el se consider el se consider plus		10.53								

**Nota: la** configurazione centrificata viene influenzata e talvolta viene disconnessa quando la risposta del server è lenta durante il test della connessione ACS con il dominio AD. Tuttavia, funziona correttamente con le altre applicazioni.

3. Fare clic su Salva modifiche per consentire ad ACS di partecipare ad

seneral		
Connection Details		
Active Directory Domain Name:	MC355.com	
Please specify the credentials used to jo	in this machine to the Activ	e Directory Domain:
O Usemame:	training	
Password:		
You may use the Test Connection Button	to ensure credentials are o	correct and Active Directory Domain is reachable.
	Test Connection	
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes	e Active Directory Domain a to be available for use in p	U ind save this configuration. Once you have successfully connected to the Domain, you can select the folicy rules.
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes	e Active Directory Domain a to be available for use in p	U ind save this configuration. Once you have successfully connected to the Domain, you can select the folloy rules.
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings	e Active Directory Domain a to be available for use in p	U ind save this configuration. Once you have successfully connected to the Domain, you can select the folloy rules.
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings I Enable password change Enable machine authentication	e Active Directory Domain a to be available for use in p	U ind save this configuration. Once you have successfully connected to the Domain, you can select the folloy rules.
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings I Enable password change Enable machine authentication	e Active Directory Domain a to be available for use in p	U ind save this configuration. Once you have successfully connected to the Domain, you can select the volicy rules.
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings I Enable password change Enable machine authentication Enable Machine Access Restrictio Aging time (hours):	e Active Directory Domain a to be available for use in p tris	U ind save this configuration. Once you have successfully connected to the Domain, you can select the folloy rules.
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings Directory Enable password change Enable machine authentication Enable Machine Access Restrictio Aging time (hours): Enable dial-in check	e Active Directory Domain a to be available for use in p yns	U nd save this configuration. Once you have successfully connected to the Domain, you can select the folloy niles.
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings Directory Groups and Directory Attributes Enable password change Enable Machine Access Restriction Aging time (hours): Enable dial-in check Enable caliback check for dial-in c	e Active Directory Domain a to be available for use in p one	U nd save this configuration. Once you have successfully connected to the Domain, you can select the folloy rules.
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings Enable password change Enable Machine Access Restriction Aging time (hours): Enable dial-in check Enable caliback check for dial-in of Connectivity Status	e Active Directory Domain a to be available for use in p ma	U nd save this configuration. Once you have successfully connected to the Domain, you can select the folloy rules.
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings C Enable password change C Enable machine authentication Enable Machine Access Restriction Aging time (hours): Enable dial-in check Enable callback check for dial-in of Connectivity Status Joined to Domain: Connectivity Stati	e Active Directory Domain a to be available for use in p ms glients us:	U nd save this configuration. Once you have successfully connected to the Domain, you can select the folloy rules.

4. Una volta che l'ACS è stato aggiunto correttamente al dominio AD, viene visualizzato lo stato della



connettività.

**Nota:** quando si configura un archivio identità di Active Directory, ACS crea anche:Nuovo dizionario per l'archivio con due attributi: ExternalGroups e un altro attributo per qualsiasi attributo recuperato dalla pagina Attributi directory.Un nuovo attributo,

IdentityAccessRestricted. È possibile creare manualmente una condizione personalizzata per

questo attributo.Condizione personalizzata per il mapping di gruppi dall'attributo ExternalGroup. il nome della condizione personalizzata è AD1:ExternalGroups e un'altra condizione personalizzata per ogni attributo selezionato nella pagina Attributi directory, ad esempio AD1:cn.

#### Configura servizio di Access

Completare questi passaggi per completare la configurazione del servizio Access in modo che ACS possa utilizzare l'integrazione AD appena configurata.

 Scegliere il servizio da cui si desidera autenticare gli utenti da AD e fare clic su Identità. Fare clic su Seleziona accanto al campo Origine identità.

Access Policies > Access Services > Default Device Admin > Identity  Single result selection  Rule based result selection						
Identity Source: DenyAccess	Select					
Advanced Options						
Save Changes Discard Changes						

2. Scegliere AD1 e fare clic su OK.

Identi	ity Store		Showing 1-9 of 9 50 👻 per page Go
Filter		Match if: 🗾 👻 😡	
	Name 🔺	Description	
۲	AD1		
0	CN Username	Predefined Certificate Authentication Profile	
0	DenyAccess		
0	Internal Hosts		
0	Internal Users		
0	LDAP	Domain Controller LDAP	
0	NAC Profiler	Default Entry for NAC Profiler	
0	safeword	THIS IS NOT USED - nic 2011.11.22	
0	safeword-ias		
			I I I Page 1 of 1 ► ►
OK	Cancel		

3. Fare clic su **Salva** 

modifiche.						
Access Policies > Access Services > Default Device Admin > Identity						
Single result selection	selection					
Identity Source: AD1	Select					
<ul> <li>Advanced Options</li> </ul>	and the second					
Save Changes Discard Changes						

# **Verifica**

Per verificare l'autenticazione AD, inviare una richiesta di autenticazione da un server NAS con credenziali AD. Verificare che il server NAS sia configurato sul server ACS e che la richiesta venga elaborata dal servizio di accesso configurato nella sezione precedente.

1. Dopo aver eseguito l'autenticazione da NAS, accedere alla GUI di ACS e scegliere Monitoraggio e report > Protocollo AAA > Autenticazione TACACS+. Identificare l'autenticazione passata dall'elenco e fare clic sul simbolo della **lente di ingrandimento** come mostrato.



2. Èpossibile verificare dai passaggi che ACS ha inviato ad AD una richiesta di

#### autenticazione. acsadmin acs51 Log Out About Holp cisco Cisco Secure ACS View Moniforing and Reports. 말 🙀 📦 Launch Interactive Viewer . P Dashboard Showing Page 1 of 1 Goto Page: Go E Alarma Jun 8, 2012 5:37 AM inbax. Logged At: Steps Jun 8, 2012 5:37 AM ACS Time: Thresholds Secalized TACADS1 Authoritization START Sequent Schedules aca51 PAP\_ASCI ACS Instance Reducing Service Martine Publics Authentication Method: Reports Matchedester Authentication Type ASCI Envortes Schooled Assess Service - Default Device Admin Stared Privilege Level 1 Reducing Martin Paling 🗄 Catalog User Material Default Zale Usemame dvishwak Selected Mentity Store - ADU Access Service Remote Address: 0.0.0.0 TACACSI will use the password prompt from global TACACSI configuration ACS Instance Velwork Device Saturned TACACS1 Authoritation Reply Endpoint Network Device Sectived TACACS1 Authoritation CONTINUE Segue: 192 168 26 13 Failure Reason Network Device IP Address Using previously selected Access Service Network Device Device Type:All Device Types, Location:All Locations Network Device Croups Sectorizer Martin Pelice Security Group Access (SGA) Matelial Defails Zale Session Directory Access Policy School Marriely Steer - ADI k User Access Service: Default Device Admin Anthon Seating our against Active Directory E Inubeshoching Identity Store AD1 The adhesishes against Artice Directory of Connectivity Tests Permit Access Selected Shell Profile ACS Support Bundle Anthropication Research MCS55.com Active Directory Domain Evaluation Group Managing Policy Expert Troubleshooter Identity Group Evaluation Exception Arthonization Policy Access Service Selection Matched Rule : 🔒 🗓 Manitoring Configuration Rule-1 No relevant matched Identity Policy Matched Role Defaul Evaluation Actionization Policy Selected identity Stores: AD1, AD1 Matched Detroit Sole Query Identity Stores Saturned TACACO1 Authoritication Reply Selected Query Identity Stores Group Mapping Policy Matched Bule

# Informazioni correlate

- <u>Cisco Secure Access Control System</u>
- Documentazione e supporto tecnico Cisco Systems