# ACS 5.x en hoger - Integratie met Microsoft AD configureren

#### Inhoud

Inleiding Voorwaarden Vereisten Gebruikte componenten Conventies Achtergrondinformatie Configuratie ACS 5.x Application Deployment Engine (ADE-OS) configureren Samenvoegen ACS 5.x tot AD Toegangsservice configureren Verifiëren Gerelateerde informatie

# **Inleiding**

Dit document biedt een voorbeeldconfiguratie voor het integreren van Microsoft Active Directory met Cisco Secure Access Control System (ACS) 5.x en hoger. ACS gebruikt Microsoft Active Directory (AD) als een externe identiteitsopslag om resources zoals gebruikers, machines, groepen en eigenschappen op te slaan. ACS bevestigt deze middelen tegen AD.

# Voorwaarden

#### **Vereisten**

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

- Windows Active Directory Domain om te worden gebruikt, moet volledig worden geconfigureerd en gebruiksklaar zijn.
- Gebruik Microsoft Windows Server 2003 Domain, Microsoft Windows Server 2008 Domain of Microsoft Windows Server 2008 R2 Domain aangezien deze door ACS 5.x worden ondersteund.Opmerking: Integratie van Microsoft Windows Server 2008 R2-domein met ACS wordt ondersteund door ACS 5.2 en later.

#### Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco beveiligde ACS 5.3
- Microsoft Windows Server 2003-domein

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

#### **Conventies**

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

# **Achtergrondinformatie**

Windows Active Directory biedt veel functies die in het dagelijkse netwerkgebruik worden gebruikt. De integratie van ACS 5.x met AD maakt het gebruik van bestaande AD-gebruikers, machines en hun groepstoewijzing mogelijk.

ACS 5.x geïntegreerd met AD biedt deze functies:

- 1. Machine-verificatie
- 2. Teruggave van kenmerken voor autorisatie
- 3. certificaatvernieuwing voor EAP-TLS-verificatie
- 4. Beperking aantal gebruikers- en machineaccount
- 5. Beperkingen van toegang machine
- 6. Controleer inbeltoegangsrechten
- 7. Terugbellen voor inbelgebruikers
- 8. Ondersteuning van inbellen

# **Configuratie**

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

Zorg ervoor dat de **TimeZone, datum en tijd** op de ACS-overeenkomsten overeenkomen met die op de AD-primaire domeincontroller voordat u ACS 5.x in de AD integreert. Bepaal ook de DNS server op ACS om de domeinnaam van ACS 5.x op te lossen. Voltooi deze stappen om ACS 5.x Application Engine (ADE-OS) te configureren:

- 1. SSH aan het ACS-apparaat en voer de CLI-referenties in.
- 2. Geef de opdracht **kloktijd uit** in de configuratie-modus zoals getoond om de **TIMEZONE** op de ACS te configureren om deze op de domeincontroller af te stemmen.

clock timezone Asia/Kolkata

**Opmerking:** Asia/Kolkata is de tijdzone die in dit document wordt gebruikt. U kunt uw specifieke tijdzone vinden door exec mode **de** opdracht **van de tijdzones te tonen**.

3. Indien uw AD-domeincontroller gesynchroniseerd is met een NTP-server die in uw netwerk verblijft, wordt het sterk aanbevolen om dezelfde NTP-server op de ACS te gebruiken. Als u geen NTP-server hebt, sla dan over naar **stap 4**. Dit zijn de stappen om NTP-server te

configureren:NTP-server kan met het **ntp server <ip-adres van de NTP server>**-opdracht worden ingesteld in configuratie-modus zoals getoond.

ntp server 192.168.26.55

The NTP server was modified.

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

Raadpleeg <u>ACS 5.x: Cisco ACS-synchronisatie met NTP Server Configuration Voorbeeld</u> voor meer informatie over NTP-configuratie.

4. Om datum en tijd handmatig te configureren gebruikt u de **klokinstelling** opdracht in **execmodus**. Hier wordt een voorbeeld getoond:

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. Controleer nu de **Time-zone, datum** en **tijd** bij de opdracht **Show kloktijd**. De uitvoer van de opdracht Kloktijd wordt hier weergegeven:

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

6. Configureer DNS op ACS met het **<ip-naam-server <ip-adres van de DNS>**-opdracht in **configuratiemodus** zoals hier wordt getoond:

ip name-server 192.168.26.55

Opmerking: Het DNS IP-adres is door de beheerder van uw Windows-domein beschikbaar.

7. Geef de opdracht **nslookup <domeinnaam>** uit om de bereikbaarheid van de domeinnaam zoals aangegeven te controleren

zoals aangegeven te o				
acs51/admin# <b>nslookup MC</b>	S55.com			
Trying "MCS55.com"				
;; ->>HEADER<<- opcode:	QUERY,	status:	NOERROR,	id: 60485
;; flags: qr aa rd ra;	QUERY: 1	, ANSWER	: 3, AUT	HORITY: 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.	3600	IN	SOA	admin-zq2ttn9ux.MCS55.com.
hostmaster.MCS55.com	n. 635 90	0 600 86	400 3600	
;; ADDITIONAL SECTION:				
admin-zq2ttn9ux.MCS55.c	om. 3600	IN	A	192.168.26.55

Received 136 bytes from 192.168.26.55#53 in 0 ms

**Opmerking:** Als het **gedeelte ANTWOORD** leeg is, neem dan contact op met de beheerder van het Windows-domein om te weten te komen welke DNS-server het juiste is.

8. Geef de opdracht **ip-domeinnaam <domeinnaam>** uit om **DOMAIN-NAME** op de ACS te configureren zoals hier wordt getoond:

ip domain-name MCS55.com

9. Geef de **hostname <hostname>** opdracht uit om **HOSTNAME** op de ACS te configureren zoals hier wordt getoond:

hostname acs51

**N.B.:** Vanwege de beperkingen van het NETzien, moeten ACS-hostnamen minimaal 15 tekens bevatten.

10. Geef de opdracht Schrijfgeheugen op om de configuratie op ACS op te slaan.

#### Samenvoegen ACS 5.x tot AD

Voltooi deze stappen om zich aan te sluiten bij ACS5.x tot AD:

1. Kies gebruikers en identiteitsopslag > Externe identiteitsopslag > Actieve map en geef de domeinnaam, AD-account (gebruikersnaam) en het wachtwoord op en klik op Test Connection Opmerking: AD-account vereist voor domeintoegang in ACS moet een van de volgende kenmerken hebben: Voeg werkstations toe aan het juiste domein van de gebruiker in het betreffende domein. Maak Computer Objects of verwijder Computer Objects toestemming op corresponderende computercontainer waar de ACS-machineaccount is gemaakt voordat u de ACS-machine naar het domein sluit Opmerking: Cisco raadt u aan het uitsluitingsbeleid voor de ACS-account uit te schakelen en de AD-infrastructuur te configureren om signaleringen naar de beheerder te verzenden als er een fout wachtwoord voor die account wordt gebruikt. Dit komt doordat als u een fout wachtwoord invoert, ACS het rekenschap van de machine niet aanmaakt of wijzigt wanneer het nodig is en daarom mogelijk alle authenticaties ontkent. Opmerking: De Windows AD-account, dat ACSbestanden naar het AD-domein voegt, kan in de eigen organisatie-eenheid (OU) worden geplaatst. Deze account is aangemaakt of heeft een beperking waardoor de naam van het apparaat moet overeenkomen met de naam van de ADaccount

s and identity Stores > External identity Stores	Active Directory	and the second
General		
Connection Details		
Active Directory Domain Name:	MCS55.com	
Please specify the credentials used to jo	in this machine to the Active Directory Domain:	
🗢 Usemame:	training	
C Password:		
	k i se	
Very may use the Text Connection Dates	to ensure credentials are correct and Active Directory Domain is r	achable.
TOU IT AT USE THE TEST OUT ECOUT EQUID		
rou may use the resconnection button	Test Connection	
for may use the fest connection building	Test Connection	
for may use the rest connection ballon	Test Connection	
Click on 'Save Changes' to connect to the	Test Connection	ve successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes	Active Directory Domain and save this configuration. Once you ha	ve successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes	Active Directory Domain and save this configuration. Once you have to be available for use in policy rules.	ve successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Athibutes End User Authentication Settings	Active Directory Domain and save this configuration. Once you have to be available for use in policy rules.	ve successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Athibutes End User Authentication Settings	Test Connection Active Directory Domain and save this configuration. Once you have to be available for use in policy rules.	ve successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings Enable password change Enable machine authentication	Test Connection Active Directory Domain and save this configuration. Once you have to be available for use in policy rules.	ve successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings Enable password change Enable machine authentication	Test Connection	ve successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictio Acling time (hours):	Active Directory Domain and save this configuration. Once you have to be available for use in policy rules.	ve successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings Set Enable password change Enable machine authentication Enable Machine Access Restriction Aging time (hours):	Test Connection Active Directory Domain and save this configuration. Once you have to be available for use in policy rules.	ve successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Athibutes End User Authentication Settings I Enable password change Enable Machine Access Restrictio Aging time (hours): Enable dial-in check	Test Connection Active Directory Domain and save this configuration. Once you have to be available for use in policy rules.	ve successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Athibutes End User Authentication Settings Set Enable password change Enable machine Access Restrictio Aging time (hours): Enable dial-in check Enable caliback check for dial-in c	Active Directory Domain and save this configuration. Once you have to be available for use in policy rules.	ve successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Athibutes End User Authentication Settings Solution Enable password change Enable Machine Access Restriction Aging time (hours): Enable dial-in check Enable callback check for dial-in cl Connectivity Status	Active Directory Domain and save this configuration. Once you have the available for use in policy rules.	ve successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Athibutes End User Authentication Settings Enable password change Enable Machine Access Restrictio Aging time (hours): Enable dial-in check Enable caliback check for dial-in cl Connectivity Status Joined to Domain: Connectivity Status	Test Connection Active Directory Domain and save this configuration. Once you have to be available for use in policy rules.	ve successfully connected to the Domain, you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Athibutes End User Authentication Settings   Enable password change  Enable machine authentication  Enable Machine Access Restrictio Aging time (hours):  Enable dial-in check Enable caliback check for dial-in cl Connectivity Status Joined to Domain: Connectivity Status	Test Connection Active Directory Domain and save this configuration. Once you have to be available for use in policy rules. IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII	ve successfully connected to the Domain, you can select the

2. Dit screenshot laat zien dat de testverbinding met de AD succesvol is. Klik vervolgens op **OK**.

Users and Identity Stores > External Identity Stores > A	ctive Directory				
General					
Connection Details     Active Directory Domain Name.	MCS55.com	<u> </u>			
Please specify the credentials used to join O Username: O Password:	Connection test to MCS55.com succeeded.				
You may use the Test Connection Butten to	OK	ctory Domain is reachab	le.		
Click on 'Save Changes' to connect to the Act Directory Groups and Directory Altributes to b	ive Directory Domain and save this configu e available for use in policy rules.	ration. Or ce you have suc	cessfully conne	cted to the Dom	iain, you can select the

**Opmerking:** Centrify configuratie wordt beïnvloed en wordt soms losgekoppeld als er een trage reactie van de server is terwijl u de ACS verbinding met het AD-domein test. Maar het werkt prima voor de andere toepassingen.

3. Klik op Wijzigingen opslaan voor ACS om mee te doen met

seneral		
Connection Details		
Active Directory Domain Name:	MC855.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	correct and Active Directory Domain is reachable.
	Test Opposition	7
Click on 'Save Changes' to connect to the	e Active Directory Domain a	und save this configuration. Once you have successfully connected to the Domain you can select the
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes	e Active Directory Domain a	und save this configuration. Once you have successfully connected to the Domain, you can select the policy 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	and save this configuration. Once you have successfully connected to the Domain, you can select the policy 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	and save this configuration. Once you have successfully connected to the Domain, you can select the policy rules.
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings I Enable password change	e Active Directory Domain a	and save this configuration. Once you have successfully connected to the Domain, you can select the policy 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	e Active Directory Domain a	and save this configuration. Once you have successfully connected to the Domain, you can select the policy 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 Restriction	e Active Directory Domain a to be available for use in p	and save this configuration. Once you have successfully connected to the Domain, you can select the policy nules.
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictic Aging time (hours):	e Active Directory Domain a to be available for use in p	and save this configuration. Once you have successfully connected to the Domain, you can select the policy nules.
Click on 'Save Changes' to connect to the Directory Groups and Directory Altributes End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictic Aging time (hours): Enable dial-in check	e Active Directory Domain a to be available for use in p	and save this configuration. Once you have successfully connected to the Domain, you can select the policy rules.
Click on 'Save Changes' to connect to the Directory Groups and Directory Altributes End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictic Aging time (hours): Enable dial-in check Enable callback check for dial-in c	e Active Directory Domain a to be available for use in p ons	and save this configuration. Once you have successfully connected to the Domain, you can select the policy rules.
Click on 'Save Changes' to connect to the Directory Groups and Directory Attributes End User Authentication Settings Enable password change Enable machine authentication Enable Machine Access Restrictic Aging time (hours): Enable dial-in check Enable callback check for dial-in c Connectivity Status Joined to Domain: Connectivity Stat	e Active Directory Domain a to be available for use in p ons	and save this configuration. Once you have successfully connected to the Domain, you can select the policy nulas.

4. Zodra ACS met succes tot het AD Domein is toegetreden, toont het in de connectiviteitsstatus.



**Opmerking:** 

Wanneer u een AD-identiteitswinkel configureren maakt ACS ook:Een nieuw woordenboek voor die winkel met twee eigenschappen: Externe groepen en een ander kenmerk voor elke eigenschap die uit de map wordt opgeroepen.Een nieuw kenmerk, IdentityAccessBeperkt. U kunt handmatig een aangepaste voorwaarde voor deze eigenschap maken.Een aangepaste voorwaarde voor groepstoewijzing van de eigenschap ExternGroup; de naam van de douaneconditie is AD1:Extern Groepen en een andere maatvoorwaarde voor elke

eigenschap geselecteerd in de pagina van de Eigenschappen van de Map, bijvoorbeeld, AD1:cn.

#### Toegangsservice configureren

Voltooi deze stappen om de configuratie van de toegangsservice te voltooien zodat ACS de nieuw geconfigureerd AD-integratie kan gebruiken.

1. Kies de service vanuit welke u wilt dat de gebruikers worden geauthentiseerd vanuit AD en klik op **Identity**. Klik nu op **Selecteren** naast het veld Identity Source.

Access Policies > A	ccess Services > Default Device Admin > Identity
Identity Source: [	DenyAccess Select
•	Advanced Options
Save Changes	Discard Changes

2. Kies AD1 en klik op OK.

Ident	ity Store		Showing 1-9 of 9 50 👻 per page	Go
Filter	r: •	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≪ → Page 1 of 1 ►	) <b>H</b>
ОК	Cancel			

3. Klik op Wijzigingen

. . . . . .

C	psiaan.
	Access Policies > Access Services > Default Device Admin > Identity
	Single result selection
	Identity Source: AD1 Select
	Advanced Options
	Save Changes Discard Changes

# **Verifiëren**

Om AD-verificatie te verifiëren, stuurde zij een verificatieaanvraag van een NAS met ADreferenties. Zorg ervoor dat de NAS op de ACS is geconfigureerd en dat het verzoek wordt verwerkt door de toegangsservice die in de vorige sectie is ingesteld.

1. Na succesvolle verificatie van NAS-loggen in de ACS-GUI en kies **monitoring en rapporten >** AAA-protocol > TACACS+verificatie. Identificeer de passerende authenticatie uit de lijst en

# klik op het **vergrootglas** symbool zoals getoond.



2. U kunt verifiëren uit de stappen die ACS verificatieaanvraag naar AD heeft

#### verzonden. acsadmin acs51 Log Out - About - Holp cisco Cisco Secure ACS View Moniform and Reports 그 🐴 📦 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 Authentication Type Matchedester ASCI Envortes Schooled Assess Service - Defailt 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) Matchiel DeLink Zale Session Directory Access Policy Schooled Marriely Steen - ADI h, User Access Service: Default Device Admin Anthon Seating our against Active Directory E Inubeshoching Identity Store AD1 Use autominution spinet Active Directory Connectivity Tests Permit Access Selected Shell Profile ACS Support Bundle Anthropication Research MC855.com Active Directory Domain Evaluation Group Managing Policy Expert Troubleshooter Identity Group Evaluation Exception Arthonization Policy Access Service Selection Matched Rule : + 🚯 Maritaing 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 TACACS1 Authentication Raply Selected Query Identity Stores Group Mapping Policy Matched Bule

# Gerelateerde informatie

- <u>Cisco Secure Access Control-systeem</u>
- <u>Technische ondersteuning en documentatie Cisco Systems</u>