ACS 5.x: Konfigurationsbeispiel für LDAP-Server

Inhalt

Einführung Voraussetzungen Anforderungen Verwendete Komponenten Konventionen Hintergrundinformationen Verzeichnisdienst Authentifizierung über LDAP LDAP-Verbindungsmanagement Konfigurieren Konfigurieren von ACS 5.x für LDAP Konfigurieren des Identitätsspeichers Fehlerbehebung Zugehörige Informationen

Einführung

Lightweight Directory Access Protocol (LDAP) ist ein Netzwerkprotokoll zum Abfragen und Ändern von Verzeichnisdiensten, die auf TCP/IP und UDP ausgeführt werden. LDAP ist ein einfacher Mechanismus für den Zugriff auf einen x.500-basierten Verzeichnisserver. <u>RFC 2251</u> definiert LDAP.

Das Cisco Secure Access Control System (ACS) 5.x kann mithilfe des LDAP-Protokolls in eine externe LDAP-Datenbank (auch als Identitätsspeicher bezeichnet) integriert werden. Es gibt zwei Methoden, um eine Verbindung zum LDAP-Server herzustellen: Klartext (einfach) und SSL (verschlüsselt) Verbindung. ACS 5.x kann für die Verbindung mit dem LDAP-Server mit beiden dieser Methoden konfiguriert werden. Dieses Dokument enthält ein Konfigurationsbeispiel für die Verbindung von ACS 5.x mit einem LDAP-Server über eine einfache Verbindung.

Voraussetzungen

Anforderungen

In diesem Dokument wird davon ausgegangen, dass der ACS 5.x über eine IP-Verbindung zum LDAP-Server verfügt und der Port TCP 389 offen ist.

Standardmäßig ist der Microsoft Active Directory-LDAP-Server so konfiguriert, dass er LDAP-Verbindungen auf dem Port TCP 389 akzeptiert. Wenn Sie einen anderen LDAP-Server verwenden, stellen Sie sicher, dass dieser aktiv ist und Verbindungen auf Port TCP 389 akzeptiert.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Secure ACS 5.x
- Microsoft Active Directory LDAP-Server

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter <u>Cisco Technical Tips</u> <u>Conventions</u> (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

Verzeichnisdienst

Der Verzeichnisdienst ist eine Softwareanwendung oder eine Gruppe von Anwendungen, die zum Speichern und Organisieren von Informationen über die Benutzer und Netzwerkressourcen eines Computernetzwerks verwendet wird. Sie können den Verzeichnisdienst verwenden, um den Benutzerzugriff auf diese Ressourcen zu verwalten.

Der LDAP-Verzeichnisdienst basiert auf einem Client-Server-Modell. Ein Client stellt eine Verbindung zu einem LDAP-Server her, um eine LDAP-Sitzung zu starten, und sendet betriebliche Anforderungen an den Server. Der Server sendet dann seine Antworten. Ein oder mehrere LDAP-Server enthalten Daten aus der LDAP-Verzeichnisstruktur oder der LDAP-Backend-Datenbank.

Der Verzeichnisdienst verwaltet das Verzeichnis, d. h. die Datenbank, in der die Informationen gespeichert sind. Verzeichnisdienste verwenden ein verteiltes Modell, um Informationen zu speichern, und diese Informationen werden in der Regel zwischen Verzeichnisservern repliziert.

Ein LDAP-Verzeichnis ist in einer einfachen Baumhierarchie organisiert und kann auf viele Server verteilt werden. Jeder Server kann über eine replizierte Version des Gesamtverzeichnisses verfügen, die regelmäßig synchronisiert wird.

Ein Eintrag in der Struktur enthält eine Reihe von Attributen, bei denen jedes Attribut einen Namen (einen Attributtyp oder eine Attributbeschreibung) und einen oder mehrere Werte hat. Die Attribute werden in einem Schema definiert.

Jeder Eintrag verfügt über eine eindeutige ID, die als Distinguished Name (DN) bezeichnet wird. Dieser Name enthält den RDN (Relative Distinguished Name), der aus Attributen im Eintrag erstellt wurde, gefolgt von der DN des übergeordneten Eintrags. Sie können sich den DN als vollständigen Dateinamen und den RDN als relativen Dateinamen in einem Ordner vorstellen.

Authentifizierung über LDAP

ACS 5.x kann einen Principal für einen LDAP-Identitätsspeicher authentifizieren, indem er eine Bindungsoperation auf dem Verzeichnisserver durchführt, um den Principal zu finden und zu authentifizieren. Wenn die Authentifizierung erfolgreich ist, kann der ACS Gruppen und Attribute abrufen, die dem Principal angehören. Die abzurufenden Attribute können in der ACS-Webschnittstelle (LDAP-Seiten) konfiguriert werden. Diese Gruppen und Attribute können von ACS verwendet werden, um den Principal zu autorisieren.

Um einen Benutzer zu authentifizieren oder den LDAP-Identitätsspeicher abzufragen, stellt der ACS eine Verbindung zum LDAP-Server her und verwaltet einen Verbindungspool. Siehe LDAP-Verbindungsverwaltung.

LDAP-Verbindungsmanagement

ACS 5.x unterstützt mehrere gleichzeitige LDAP-Verbindungen. Verbindungen werden bei Bedarf zum Zeitpunkt der ersten LDAP-Authentifizierung geöffnet. Die maximale Anzahl von Verbindungen wird für jeden LDAP-Server konfiguriert. Das Öffnen von Verbindungen im Voraus verkürzt die Authentifizierungszeit.

Sie können die maximale Anzahl von Verbindungen festlegen, die für gleichzeitige Bindungsverbindungen verwendet werden sollen. Die Anzahl der geöffneten Verbindungen kann für jeden LDAP-Server (primär oder sekundär) unterschiedlich sein und wird anhand der maximalen Anzahl der für jeden Server konfigurierten Administrationsverbindungen bestimmt.

ACS behält eine Liste offener LDAP-Verbindungen (einschließlich der binden Informationen) für jeden LDAP-Server bei, der in ACS konfiguriert ist. Während des Authentifizierungsprozesses versucht der Verbindungs-Manager, eine offene Verbindung aus dem Pool zu finden.

Wenn keine offene Verbindung vorhanden ist, wird eine neue geöffnet. Wenn der LDAP-Server die Verbindung geschlossen hat, meldet der Verbindungs-Manager beim ersten Aufruf zum Durchsuchen des Verzeichnisses einen Fehler und versucht, die Verbindung zu erneuern.

Wenn der Authentifizierungsprozess abgeschlossen ist, gibt der Connection Manager die Verbindung zum Connection Manager frei. Weitere Informationen finden Sie im <u>ACS 5.X-Benutzerhandbuch</u>.

Konfigurieren

In diesem Abschnitt erhalten Sie Informationen zum Konfigurieren der in diesem Dokument beschriebenen Funktionen.

Konfigurieren von ACS 5.x für LDAP

Gehen Sie wie folgt vor, um ACS 5.x für LDAP zu konfigurieren:

 Wählen Sie Benutzer und Identitätsdatenbanken > Externe Identitätsdatenbanken > LDAP, und klicken Sie auf Erstellen, um eine neue LDAP-Verbindung zu erstellen.

denuty Stores	Showing 0-0 of 0 50 - per page Go
Filter: • Match if: • Go	7
Name - Type Description	
No data to display	

2. Geben Sie auf der Registerkarte Allgemein den **Namen** und die **Beschreibung** (optional) für das neue LDAP an, und klicken Sie auf

Step 1 - Ge	eneral	7		
Name:	myLDAP			
Description:	Sample LDAP server			
Database Type	EDAP			
= Required fiel	lds			

3. Geben Sie auf der Registerkarte "Serververbindung" im Abschnitt "Primärer Server" den Hostnamen, den Port, die Admin-DN und das Kennwort ein. Klicken Sie auf Testbindung an Server.Hinweis: Die IANA-zugewiesene Portnummer für LDAP ist TCP 389. Bestätigen Sie jedoch die Portnummer, die Ihr LDAP-Server verwendet, vom LDAP-Administrator. Die Admin-DN und das Passwort sollten Ihnen vom LDAP-Administrator bereitgestellt werden. Ihre Admin-DN muss über alle Berechtigungen für alle OUs auf dem LDAP-Server verfügen.

isers and identity Stores > External identity	y Stores > LDAP > Create	
General Server Connection	Directory Organization	
Step 2 - Server Connect	tion	
Server Connection	Always Access Primary Server First	
	Failback To Primary Server After:	S Minutes
Primary Server		Secondary Server
O Hostname:	192.168.26.55	Hostname:
· Port	389	Port 389
C Anonymous Access		Anonymous Access
Authenticated Access		C Authenticated Access
Admin DN:	CN=training,CN=users,DC=	Admin DN.
Password	•••••	Password.
Use Secure Authentication		Use Secure Authentication
Root CA:		Root CA:
Server Timeout	10 Seconds	Server Timeout 10 Seconds
Max. Admin Connections:	20	Max. Admin Connections: 20
	Test Bind To Server	Test Bind To Server
e = Required fields		
		Back Next Finish Cancel

4. Dieses Bild zeigt, dass das **Verbindungstestbind zum Server** erfolgreich war.

Step 1 - General Name: myLDAP Description: Sample LDAP server Database Type LDAP Connection test biad Succeeded. Image: Connection test biad Succeeded. Image: Connection test biad Succeeded. Image: Connection test biad Succeeded. Image: Connection test biad Succeeded. Image: Connection test biad Succeeded. Image: Connection test biad Succeeded.	Step 1 - General Name: myLDAP Description: Sample LDAP server Database Type LDAP = Required fields Back Next Finish C	sers and identity Si General S	tores > External identity Stores > L erver Connection Directory	DAP > Create	
Image: myLDAP Mame: myLDAP Description: Sample LDAP server Connection test bind Succeeded. Database Type LDAP Connection test bind Succeeded. Image: myLDAP Image: myLDAP server Image: myLDAP server Image: myL	Name: myLDAP Description: Sample LDAP server Database Type LDAP = Required fields Back Next Finish C	Step 1 - Ge	eneral		
Description: Sample LDAP server Connection test bind Succeeded. Database Type LDAP = Required fields	Description: Sample LDAP server Database Type LDAP Connection test biad Succeeded. = Required fields Image: Connection test biad Succeeded. Back Next Finish Connection test biad Succeeded.	A Name:	myLDAP		
Ø = Required fields	= Required fields Back Next Finish C	Description: Database Type	Sample LDAP server e LDAP	Connection test bind Succeeded.	
	Back Next Finish C	a = Required fie	lds	OK	

Hinweis: Wenn die Testbindung nicht erfolgreich ist, überprüfen Sie den Hostnamen, die Portnummer, die Admin-DN und das Passwort Ihres LDAP-Administrators.

5. Klicken Sie auf **Weiter**.

ers and identity Stores > External identit	ty Stores > LDAP > Create			
General Server Connection	Directory Organization			
Step 2 - Server Connec	tion			
Server Connection				
📃 Enable Secondary Server	Always Access Primary Server Fir	st		
	Failback To Primary Server After.	0	Minutes	
Primary Server			Secondary Server	
Hostname:	192.168.26.55		Hostname:	
· Port	389		Port:	0
C Anonymous Access			Anonymous Access	
Authenticated Access			Authenticated Access	
Admin DN:	CN=training,CN=users,DC=		Admin DN:	
Password:			Password:	
Use Secure Authentication	1		Use Secure Authenticatio	n
Root CA:			Root CA:	
Server Timeout	10 Seconds		Server Timeout	0 Beconds
o Max Admin Connections:	20		Max Admin Connections:	10
	Tast Rind To Conner			Test Find To Senor
e = Required fields	Test Bind to Server		-	1601 Dalia 10-361461
				Back Ned Finish Cancel

6. Geben Sie auf der Registerkarte Verzeichnisorganisation im Abschnitt Schema die erforderlichen Details ein. Geben Sie entsprechend die erforderlichen Informationen im Bereich Verzeichnisstruktur an, wie vom LDAP-Administrator bereitgestellt. Klicken Sie auf **Testkonfiguration**.

ers and identity Stores > Extern	al Identity Stores > LDAP > Cr	ente			
🗸 General 🖌 Server Conn	Directory Organ	ization			
Step 3 - Directory	Organization				
olep o - Directory	Organization				
Schema					
Subject Objectclass:	user	Group Objectclass:	group		
 Subject Name Athibute: 	sAMAccountName	Group Map Attribute:	member		
Certificate Attribute:	usercertificate				
Subject Objects Cor	ntain Reference To Groups				
Group Objects Conf	tain Reference To Subjects				
1	Subjects In Groups Are Stor	ed in Member Attribute As:	distinguished name +		
Directory Structure					
Subject Search Base: (CNausers DCamos55 DCa	000			
Group Search Base: (CN=users,DC=mcs55,DC=	com			
	Test Configuration				
Username Prefix Suffix St	rapping				
E Strip start of subject	t name up to the last occur	ence of the separator:	(e.g. if separator set to *	", subject name 'acmelsmith'	becomes 'smith')
Strip end of subject	I name from the first occum	ance of the separator:	(e.g. if separator set to '	@', subject name 'smith@acn	me.com'becomes 'smith')
MAC Address Enrmat					
MAC AGRESS FOR MAR					
Search for MAC Address	In Format Incidence-rocide-roci	•			
Required fields					
					Batk Next Finish C;

7. Dieses Bild zeigt, dass der **Konfigurationstest** erfolgreich durchgeführt wurde.



Hinweis: Wenn der Konfigurationstest nicht erfolgreich ist, überprüfen Sie die Parameter im Schema und in der Verzeichnisstruktur erneut von Ihrem LDAP-Administrator.

8. Klicken Sie auf **Fertig**

Step 3 - Directory	Organization		
Schema	-		
Subject Objectclass:	USEF	Group Objectclass:	group
Subject Name Attribute:	sAMAccountName	Group Map Attribute:	member
Certificate Attribute:	usercertificate		
🗇 Subject Objects Co	ntain Reference To Group	\$	
Group Objects Con	tain Reference To Subject	8	
	Subjects in Groups Are Str	ored in Member Attribute As:	disänguished name 👻
irectory Structure			
Subject Search Base: 0	ON=users,DC=mcs55,DC	=com	
Group Search Base: 0	N=users,DC=mcs55,DC	=com	
	Test Configuration		
Isername Prefix'Suffix St	ripping		
📋 Strip start of subject	t name up to the last occu	rrence of the separator.	(e.g. if separator set to 1', subject name 'acmeismith' becomes 'smith)
📋 Strip end of subject	name from the first occur	rence of the separator:	(e.g. if separator set to '@', subject name 'smith@acme.com' becomes 'smith')
MAC Address Format			
Search for MAC Address	in Format: 30-30-30-30-30-30-3	0. •	

9. Der LDAP-Server wurde erfolgreich erstellt.

dentity	y Stores				Showing 1-1 of 1	50	🝷 per page	Go
Filter:		Match if	•	Go 🔻				
	Name 🔺	Туре	Description					
	myLDAP	LDAP	Sample LDAP server					

Konfigurieren des Identitätsspeichers

Gehen Sie wie folgt vor, um den Identity Store zu konfigurieren:

1. Wählen Sie Zugriffsrichtlinien > Zugriffsdienste > Service Selection Rules

(Dienstauswahlregeln) aus, und überprüfen Sie, welcher Dienst den LDAP-Server für die Authentifizierung verwendet. In diesem Beispiel verwendet die LDAP-Serverauthentifizierung den Standard-

ervio	e Sele	ction Pol	icy	and the life second life	And the second	and the second		
Filter:	Statu	s •	Match if	Equals 🔹	Enabled 👻 Clear Filter	Go 🔻		
		Status	Name	Protocol	Conditions	Results Service	Hit Count	
1	23	0	Rule-1	match Radius		Default Network Access	0	
2		•	Rule-2	match Tacacs		Default Device Admin	2	
		Default		if no rules defin	ed or no enabled rule matches.	DenyAccess	0	
reate	-	Duplical	te	Edit Delete	∧ Move to ∨			Customize Hit Coun

 Sobald Sie den Service in Schritt 1 überprüft haben, gehen Sie zum jeweiligen Dienst, und klicken Sie auf Zulässige Protokolle. Vergewissern Sie sich, dass PAP/ASCII zulassen aktiviert ist, und klicken Sie auf Senden. Hinweis: Sie können andere Authentifizierungsprotokolle zusammen mit PAP/ASCII zulassen auswählen.

Authentication Protocols			
Allow PAPIASCI			
Allow CHAP			
Allow MS-CHAPv1			
Allow MS-CHAPv2			
Allow EAP-MD5			
Allow EAP-TLS			
Allow LEAP			
Allow PEAP			
Allow EAP-FAST			
Preferred EAP protocol LEAP	*		

3. Klicken Sie auf den in Schritt 1 identifizierten Service und anschließend auf **Identität**. Klicken Sie rechts neben dem Feld Identitätsquelle auf

Single result	selection 🔘 Rule based re	sult selection	
dentity Source:	nternal Users	Select	
•	Advanced Options	<u> </u>	

 Wählen Sie den neu erstellten LDAP-Server (in diesem Beispiel myLDAP) aus, und klicken Sie auf OK.

dentity	/ Store			Showing 1-6 of 6 50	👻 per page 🛛 Go
Filter:	•	Match if:	👻 😡 🔻		
	Name 🔺	Description			
0	A				
0	CN Username	Predefined Certificat	e Authentication Profile		
0	DenyAccess				
0	Internal Hosts				
0	Internal Users				
0	myLDAP	Sample LDAP server			
				i 💽 Page	1 of 1 🕨 🕨
ok	Cancel				

5. Klicken Sie auf Änderungen

speichern.

Identity Source: myl DAP
injust i
Advanced Options

6. Gehen Sie zum Abschnitt Autorisierung des in Schritt 1 identifizierten Dienstes, und stellen Sie sicher, dass mindestens eine Regel für die **Authentifizierung** vorhanden

letwo	rk Ac	cess Aut	thorizatio	n Policy			
Filter.	State	15		• Match if: Equals • Enabled •	Clear Filter Go	*	
	0	Status	Name	Conditions NDG1.ocation Time And Date	Results Authorization Profiles	Hit Count	
		No data	to displa	y .			
	123	Default		If no rules defined or no enabled rule matches.	Permit Access	3	
reat	1-	Dunlic	ate 1+	Edit Delete A Move to V			Customize Hit Cour

Fehlerbehebung

ACS sendet eine Verbindungsanforderung, um den Benutzer gegen einen LDAP-Server zu authentifizieren. Die Bindungsanforderung enthält die DN und das Benutzerkennwort des

Benutzers in Klartext. Ein Benutzer wird authentifiziert, wenn die DN und das Kennwort des Benutzers mit dem Benutzernamen und Kennwort im LDAP-Verzeichnis übereinstimmen.

- Authentifizierungsfehler ACS protokolliert Authentifizierungsfehler in den ACS-Protokolldateien.
- Initialisierungsfehler Verwenden Sie die Zeitüberschreitungseinstellungen des LDAP-Servers, um die Anzahl der Sekunden zu konfigurieren, die der ACS auf eine Antwort von einem LDAP-Server wartet, bevor festgestellt wird, dass die Verbindung oder Authentifizierung auf diesem Server fehlgeschlagen ist. Mögliche Gründe, warum ein LDAP-Server einen Initialisierungsfehler zurückgibt, sind:LDAP wird nicht unterstütztDer Server ist ausgefallen.Der Server ist nicht ausgelastet.Der Benutzer hat keine Berechtigungen.Falsche Administratoranmeldeinformationen werden konfiguriert.
- **Bind-Fehler** Möglicherweise gibt ein LDAP-Server Bind-Fehler (Authentifizierung) zurück:FilterfehlerEine Suche mithilfe von Filterkriterien schlägt fehlParameterfehlerUngültige Parameter wurden eingegeben.Das Benutzerkonto ist eingeschränkt (deaktiviert, gesperrt, abgelaufen, Kennwort abgelaufen usw.)

Diese Fehler werden als externe Ressourcenfehler protokolliert, was auf ein mögliches Problem mit dem LDAP-Server hinweist:

- Es ist ein Verbindungsfehler aufgetreten
- Das Timeout ist abgelaufen
- Der Server ist ausgefallen.
- Der Server ist nicht ausgelastet.

Der Fehler Ein Benutzer ist nicht in der Datenbank vorhanden wird als Fehler Unbekannter Benutzer protokolliert.

Der Fehler Ein ungültiges Kennwort wurde eingegeben wird als Fehler mit ungültigem Kennwort protokolliert, wenn der Benutzer vorhanden ist, das gesendete Kennwort jedoch ungültig ist.

Zugehörige Informationen

- <u>Cisco Secure Access Control System</u>
- Anforderungen für Kommentare (RFCs)
- <u>Technischer Support und Dokumentation Cisco Systems</u>