ılıılı. cısco

Cisco Show and Share in a Multi-Forest Environment

This document discusses using Cisco Show and Share[®] in a Multi-Forest Environment.

Note: Active Directory Lightweight Directory Services (AD LDS) was known formerly as Active Directory Application Mode (ADAM); these terms are used interchangeably in this document.

Prerequisites

Ensure that you meet these requirements:

- You have knowledge of deploying and configuring Cisco Show and Share and Digital Media Manager (DMM).
- You are responsible for deploying, configuring, and maintaining Microsoft Active Directory Lightweight Directory Services 2008.

Note: The Lightweight Directory Access Protocol (LDAP) authentication user search base must match the ADAM domain as well. If the search base shows "LDAP user search base is formed using the User ID information", you cannot use the attribute that you have selected.

Components Used

The information in this document is based on these software versions:

- · Cisco Show and Share Release 5.2.3 or later
- Lightweight Directory Services 2008

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

You can use Microsoft Active Directory Lightweight Directory Services (AD LDS), formerly known as Active Directory Application Mode (ADAM), to provide directory services for directory-enabled applications. Instead of using your organization's Active Directory Domain Service (AD DS) database to store the directory-enabled application data, you can use AD LDS to store the data. You can use AD LDS in conjunction with AD DS, so that you have a central location for security accounts (AD DS) and another location to support the application configuration and directory data (AD LDS). Using AD LDS, you can reduce the overhead associated with AD replication. You do not have to extend the AD schema to support the application, and you can partition the directory structure so that the AD LDS service is deployed only to the servers that need to support the directory-enabled application.

Many differences exist between ADAM and Active Directory. ADAM can deliver only some of the AD functions, as shown in Figure 1.





ADAM can create a database of users and store the user details. Single Sign-On (SSO) functions are desired to avoid end users having to maintain different sets of credentials in different systems; therefore, ADAM bind redirection is used. ADAM bind redirection is a special function for applications that support LDAP bind as an authentication mechanism. In some cases, the special schema, or naming context, may force you to avoid AD, making ADAM a necessary choice.

A special user proxy object in ADAM maps to a regular AD user account. The user proxy does not have an actual password stored in the ADAM object itself. When performing its normal bind operation, the application checks the ID locally but checks the password against Active Directory in the background, as <u>Figure 2</u> illustrates. The application does not need to be aware of this AD interaction.

Figure 2. ADAM User Proxy Password Authentication



You should use ADAM bind redirection only in special cases where an application can perform a simple LDAP bind to ADAM. However, the application still needs to associate the user with a security principal in AD.

ADAM bind redirection occurs when a bind to ADAM is attempted using a special object called a proxy object, an object in ADAM that represents a security principal in AD. Each proxy object in ADAM contains the service identifier (SID) of a user in AD. When a user attempts to bind to a proxy object, ADAM takes the SID that is stored in the proxy object, together with the password that is supplied at bind time, and presents the SID and the password to AD for authentication. A proxy object in ADAM does not store a password, and users cannot change their AD passwords through ADAM proxy objects.

The password is presented in plaintext to ADAM because the initial bind request is a simple LDAP bind request. For this reason, a Secure Sockets Layer (SSL) connection is required by default between the directory client and ADAM. ADAM uses Windows Security application programming interfaces (APIs) to present the password to AD.

For more information about bind redirection, visit Understanding ADAM bind redirection on Microsoft.com.

Note: The requirement for SSL when using bind redirection should not be disabled in a production environment.

Active Directory Multiple Forest Support Scenario in Cisco Show and Share

For the purpose of explaining the configuration, we will use an example scenario where company MXABU (Forest 2) has acquired two companies: ICEPG (Forest 1) and CTG (Forest 3). In the migration phase, the AD structure of each company will be integrated, enabling the deployment of a single MXABU cluster (Figure 3).



Figure 3. Multi-Forest Scenario

In this example, company MXABU (Forest 2) is hosted on a server running Windows 2008 Server Service Pack 2 (SP2). Company ICEPG (Forest 1) has a single domain with a domain controller (DC) that is a Global Catalog hosted on a server running Windows 2008 R2 Server SP2. Company CTG (Forest 3) has a single domain with a DC that is also a Global Catalog hosted on a server running Windows 2008 Server SP2.

AD LDS is installed in the DC for domain MXABU; in fact, you can use any machine anywhere in one of the three forests. However, the Domain Name System (DNS) infrastructure must be in place so that domains in one forest can communicate with domains in other forests and can establish the appropriate trust relationships and validations between the forests.

This section describes the configuration that is required to support the example scenario.

1. Define the Domain Trust Relationship

For the authentication of the users to succeed, you need to have a trust between the domain where the ADAM instance is hosted and the other domain(s) that hosts the user accounts. This trust can be a one-way trust if required (outgoing trust from the domain that hosts the ADAM instance to the domain(s) that host the user accounts). Thus, the ADAM instance can forward the authentication requests to DCs in those account domains.

Furthermore, you need a user account from both account domains that have access to all attributes of all user accounts in the domain. ADAMSync uses this account to synchronize the account domain users to ADAM.

Finally, the machine that runs ADAM must be able to find all domains (DNS), find domain controllers in both domains (using DNS), and connect to these DCs.

Perform these steps to set up the inter-trust relationships:

1. Open Active Directory Domains and Trusts, choose the domain that hosts AD LDS, right-click on the domain, and choose Properties.

Active Directory Domains and Trus	ts				_ 🗆 ×	
File Action View Help						
🗢 🔿 🙎 🖬 🔯 🗟 🖬						
Active Directory Domains and Trusts [V	Name	Type		Actions		
mxabu.com	There ar	re no items to show in this	view.	mxabu.com	^	
	mxabu	.com Properties		? ×	•	
	Gener	ral Trusts Managed By	1			
	1	mxabu.com				
	44	P				
		ain name (pre-Windows 20				
	MX	ABU				
	Desc	cription:				
		Domain functional level: Windows Server 2008				
	Fore	st functional level:				
	Wind	dows Server 2008				
		ОК	Cancel App	y Help		
<u>↓</u>			Mpp	y 1100		
					h.	

Note: We tested the domain functional level and the forest functional level with Lightweight Directory Services 2008.

- 2. Go to the Trusts tab and click **New Trust**.
- Follow the wizard and provide the name of the domain with which you want to establish the trust (example: CTG) and click Next.
- 4. In the Trust Type window, choose Forest trust and click Next.
- 5. In the Direction of Trust window, choose **One-way: outgoing** (required) and click **Next**.
- 6. In the Sides of Trust window, allow the wizard to configure both domains. To do so, choose **Both this domain** and the specified domain and click **Next**.

- 7. In the User Name and Password window, provide the credentials for the other domain. Click Next.
- 8. In the Outgoing Trust Authentication Level Local Forest window, choose **Forest-wide authentication**. Click **Next**.
- 9. In the Confirm Outgoing Trust window, choose **Yes, confirm the outgoing trust** and click **Next**. Following is the completed configuration for the example ICEPG and CTG domains:

Active Directory Domains	and Trusts					_ 🗆 ×
	mxabu.com Propertie	5		? ×		
	General Trusts Man	aged By				
Active Directory Domains and mxabu.com	Domains trusted by this domain (outgoing trusts):				Actions	
El myabarcom	Domain Name	Trust Type	Transitive	Properties	mxabu.com	<u> </u>
	ctg.com	Forest	Yes		More Actions	•
	icepg.com	Forest	Yes	Remove		
	Domains that trust this	domain (incoming tru	sts):			
	Domain Name	Trust Type	Transitive	Properties		
				Remove		
	New Trust	1				
					 N	
	ОК	Cancel	Apply	Help	 R	
-	1					
•					 	

2. Install AD LDS

Perform these steps to install AD LDS:

1. Open Server Manager, click Roles, and choose add New.

erape (abliki-ti	Balas		
 I Baket <lii baket<="" li=""> <</lii>		on your sorver and add or remove relax and features.	
	Tales Summary		Ales Summy Hele
	Boles: 2 of 17 installed	Additions	
	A the Dectry Death Services		Be receivenes
	Active Directory Bomain Services		at an
	Stores drectory data and manages conversion	ton between users and domains, induding user legon processe	, authentication, and directory searche
	Role Status	6	Go to Active Directory Domain Dervices
	Hesages have		
	System Sanktaer Silvaning, 1 Steppe System 1: 45 varings, 83 efformational		
	Role Services: 1 Installed		Add Role Genices
	Kole Service	1919	Annove Role Services
	Althe Depictory Denar-Controller	Instand	
	Identity Nengement for UNIX Server for Network Information Serv	fup resteled	
	Pagevent Surchrengeton	Top restaled	
	Administration Toxic	Not netslee	
	Descriptions		

 In the Select Server Roles window, choose Active Directory Lightweight Directory Services and click Next. The Installation Progress window displays.

Add Roles Wizard	ales	X
Before You Begin Server Roles AD LDS Confirmation Progress Results	Select one of more roles to instal on this server. Roles: A care Directory Certificate Services A care Directory Pederation Services (Installed) A care Directory Redenation Services (Installed) A care Directory Redenation Services A calculation Server DHCP S	Des diption: Active Directors Lichinericht Cirrectory Services (ADL DS) prevides a store for application specific data, for directory require the infrastructure of Active Directory Domain Services AvVirble instances of AD LDS can exist on a single server, each of which can have its own schema.
	< Previous	Next> Install Cencel

3. Install the Instance for Multiple-Forest Support

AD LDS can run different instances of the services with different ports, enabling different user directory "applications" to run on the same machine. By default, AD LDS chooses ports 389/LDAP and 636/LDAPS. If the system already has any kind of LDAP services running, however, it uses ports 50000/LDAP and 50001/LDAPS. Each instance has a pair of ports that increment based on the previous numbers used.

Note: In some cases because of a Microsoft bug, the ports are already in use by the Microsoft DNS server and the instance wizard shows an error, which is not self-explanatory. To resolve this error, reserve the ports in the TCP/IP stack. If you find this problem, refer to <u>AD LDS service start fails with error "setup could not start the service..." + error code 8007041d</u> on Microsoft.com.

Perform these installation steps:

- 1. In the Server Manager, choose Roles>AD LDS.
- 2. Choose Click here to create an AD LDS instance.

Larver Hanager			
File Action Vievi Help			
💠 🗢 🐮 🖬 🖬			
Server Hanaper (422/3-1) D (D) Roter	Active Devictory Lightweight Deviciony Services		
R Active Directory Domain Se Active Directory Lightwegt H Directory Lightwegt H Directory Features	Wonder a stars for applicator open fit directory data.		
R Disgrestics R Configuration	@ Summary		
B B Storage	(i) No AD LDS instances have been created. Click have to prease an AD LDS instance.		
	Eventse Nora in Stalent 24 Inure	Go to Event Vesser	
	Paum	The Evens	
		Prigar Bas	
	54		
]	
	Advanced Tools		
	Create a new AD LDG instance	AD LDG Setup Waterd	
	Query, view, and edit objects and attributes in the directory	ADDIER	
	Perform LDAP operations against the directory such as connect, bind, search, modifie, add, and delete	CE LOLEVE	
	- E. Her J. West, Additional (London) and the price & Second Science Science Science Science Sciences and a so-solution.		
	C Resources and Support		
	Recommended configurations, tasks, best practices, and online resources	AD LDS Heb	
4 1	G Last Refeats 10(23)(309 6(47)-6(41 Configure refeats		

3. In the Setup Options window, choose A unique instance. Click Next.

Υ	ou can create a unique instance, or you can install a replica of an existing instance.
S	elect the type of instance you want to install.
6	A unique instance
1	This option automatically creates a new instance of AD LDS that uses the default configuration and schema partitions. The new instance will not be able to replicate with existing instances.
0	A replica of an existing instance
	This option creates a new instance of AD LDS that uses the configuration and schema partitions replicated from another instance of AD LDS. You can also select the application partitions to replicate.

4. In the Instance Name window, provide the name of the instance. In our example, it is MultiForest. Click Next.

Instance Name The instance name is used LDS instances on this cor	d to differentiate this instance of AD LDS from other AD puter.
Type a name forthis instar of AD LDS is intended.	nce. The name should reflect the use for which this instance
Instance name:	
MultiForest	
Example: Addressbook 1	
	e is created when the instance name is combined with the splayed in the list of Windows services.
AD LDS service display na AD LDS service name:	

5. In the Ports window, choose the ports or allow the system to choose them for you. Click **Next**.

Active Directory Lightweight Directory Services Setup Wizard	x
Ports Computers will connect to this instance of AD LDS using specific ports on all of the IP addresses associated with this computer.	
The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below. If you plan to install Active Directory Domain Services on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory Domain Services uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.	
LDAP port number:	
SSL port number: 50001	
< Back Next Cancel Help]

6. In the Application Directory Partition window, provide a partition name for the instance. Do not provide a "CN" such as the one provided in the example of the wizard because most of the time it will create an error in the Schemas. In the example configuration scenario, we chose the same partition as the AD DC that hosts AD LDS (dc=Mxabu,dc=com). Click Next.

Active Directory Lightwe	ight Directory	/ Services Set	up Wizard	
Application Directory Pa An application directory		pplication-specifi	c data.	20
Do you want to create an ap	plication director	v partition for this	instance of AD LD	e7
O No, do not create an app			Instance of AD LD	51
Select this option if the ap upon installation, or if you	plication that yo	u plan to install c	reates an applicatio	n directory
• Yes, create an applicatio	n directory partiti	on		
Select this option if the ap directory partition upon ins not already exist in this ins CN=Partition1,DC=Woodg	stallation. A valid stance. Example	partition name is	any distinguished r	
Partition name:				
dc=mxabu,dc=com				
	< Back	Next >	Cancel	Help
	< back	INEXT >	Cancel	нер

7. In the Service Account Selection window, provide an account to start the server. Click Next.

🛐 Active Directory Lightweight Directory Services Setup Wizard	×
Service Account Selection AD LDS performs operations using the permissions associated with the account you select.	8
Set up AD LDS to perform operations using the permissions associated with the following account.	
C Network service account	
AD LDS has the permissions of the default Windows service account.	
This account:	
AD LDS service has the permissions of the selected account.	
User name: 🕵 mxabu \Administrator 💌 Browse	
Password:	
i domoto.	
	1
< Back Next > Cancel	Help
5	

8. Provide the name of the user who has administrative permissions. Click Next.

Active Directory Lightweight Directory Services Setup Wizard	×
AD LDS Administrators You can specify the user or group that will have administrative privileges for this instance of AD LDS.	
Assign the following user or group of users administrative permissions for AD LDS.	
 Currently logged on user: MXABU\Administrator The user that is installing AD LDS will have administrative permissions for this instance of AD LDS. 	
 This account The selected user or group will have administrative permissions for this instance AD LDS. You can choose any user or group from this computer, this computer's domain, or any domain that is trusted by this computer's domain. Account name: Browse.	3
< Back Next > Cancel	Help

9. Import the highlighted default LDAP Data Interchange Format (LDIF) files to build the schema. Click Next.

a Active Directory Lightweight Dire	ectory Services Setup Wizard 🔀				
Importing LDIF Files You can import data from Lightweight Directory Interchange Format (LDIF) files into your AD LDS application directory partition.					
To configure the AD LDS service in a below.	specific way, import one or more of the LDIF files listed				
LDIF file name	Description				
MS-AdamSyncMetadata.LDF	ADAMSync metadata schema extension. Required for A				
MS-ADLDS-DisplaySpecifiers	AD LDS Display specifiers schema and display specifiers				
MS-AZMan.LDF	AD LDS schema extensions for AzMan.				
MS-InetOrgPerson.LDF	AD LDS inetOrgPerson, user and related classes.				
MS-User.LDF	AD LDS user class and related classes.				
MS-UserProxy.LDF	AD LDS simple userProxy class.				
MS-UserPraxyFull.LDF	AD LDS full userProxy class. Requires MS-User.LDF or N				
()				
< B:	ack Next > Cancel Help				

4. Copy the Schema from Each Domain to ADAM

Repeat this process for each domain that you need to synchronize. This example shows only the process against one of the domains in the scenario. If the domains have the same schema, then this process should be done only once.

Perform these steps:

- 1. Open the AD DS/LDS schema analyzer (ADSchemaAnalyzer.exe) in the directory C:\windows\adam.
- 2. Choose File>Load target schema.

AD DS/LDS Schema Analyzer e Schema Tools	
Lord target schema Ctf +T	
LiaXusesciena Ch+5	
Greate LDIF-He. CH4	
Dit	

3. Provide the credentials of the source AD DC from which you want to import.

Load target so	chema	- 🗆 ×
Server[:port]	win2008ad	
<u>U</u> sername	Administrator	
Password		
<u>D</u> omain	mxabu	
Bind type	← Secure ← Simple	
Server type		
C AD DS/LD)S	
C Generic (subschemaSubentry)	
Load LDIF	Ok	Cancel

4. Choose File>Load base schema.

AD DS/LDS Schema Analyzer			
File Scheme Tools			
Load target schema Ctri+T			
Lord base schema Ctrl+8			
Create LDCP fie Ctrl+L			
Ext			
			_
			_
			_
			_
National and an and an and a second		 	
Validating schema Schema is ck.			<u>^</u>
Processing dependencies . Loaded schema: 1205 attributes, 230 classes, 1			
Loaded schema: 1285 attributes, 230 classes, 19	5 property sets.		
			×

5. Specify the AD LDS that you want to connect to and extend the schema.

Load base sch	ema <mark>_ 🗆 ×</mark>
Server[:port]	localhost:50000
Username	
Password	
Domain	
Bind type	● Secure C Simple
Server type	
Auto	
C AD DS/LD	s
C Generic (subschemaSubentry)
1	
Load LDIF	Ok Cancel

6. Choose Schema>Mark all non-present elements as included.

🗖 AD DS/LDS Schema Analyzer	×
File Scherra Toos	
🕑 🧧 Hide present dementa	
E Show present elements	
Mark aligen present elements as included	
(A: CODDLC SWRFWFDTLDCRSDRCWDWD::SY)(A: LCRFLORC::AU), base D S:	
staeContainer defaultSecurtyDexceptor monatch target D (A: CODCLCSWRPWP0TLOCRSDRCwDW0; ;DA)	
(ACCOLLCS/VHFWFUTLDURSDRUWOWOUST(ACCOLLFPCORLERA), DBBE DIS. subnat: dataut SecurityDeenreter miamatch: taroet DIA-CCDCLCSWRPWFDTLOCRSDRCWDWO ::DA)	
A-CCDCLCSWRPWPDTLDCRSDRCWDW0.SY(A-LCRPLORC.AU). bee D.S.	
subnetContainer: defaultSecure/Descenter mematch: target Dr.(A; CCDCLCSWRPWPLOCRRCWDWO_DA)	
too: default Society Description (and the second of a CCDCLCSWEPWPD TLDCBSDECWDWD - DA)	
Inselfcraner statußseut/biosepter norsetin tage 10 /b.COCCLS/NPRVF01DCHSBR/W0000;304 A.CODCLS/NPRVF01DCRSBRCMV00: STYL LEFR-00C.AU, base 0 Nation: dirat-liseut/fileeration nerstart: tage 10 /b.COCLSNPRVF01DCRSBRCW000;304 A.CODCLS/NPRVF01DCRSBRCMV00: STALLEFR-00C.AU, base 0 National Status and Sta	
[A:CCDCLCSWRPWPDTLDCRSDRCWDWD::SY(A:CCDCLCSWRPWPDTL0CRSDRCWDWD::A0(A:LCRPL0RC:::P5) IOA:CRiab 721a53:1e2F11d0 5819 (0aa0040529b :PSW0A:CRiab 721a54 1e2F11d0 9819 00aa0040529b :PSW0A:CRiab 721a56 1e2	
-11d0-8613-0C0a00405236 P St004; RPWP:775564845-9444-11d1-ebid-00008036751 P St004; RPWP:e4575512-9455-11d1-aetid-	1
0000/00367c1; PS)(DA; RPWP 645795b3 9455 1141 aebd 0000/00367c1; PS)(DA; RP;0370088 0ee1 11426422 00e0; 969939 (RS)	
IOA, RP 4c154200-20c0-11c0-e786-00ee005e0525; R5)IOA, RP bollec240-75e5-11c0-9020-00c04fc2(4cf, R5)(A, RC, AU IOA, RP 53ba 242, 75a2-11d0-9020-00e04e243cf :AUNOA; RP 77b5b385,544a, 11d1-aebd 0000380367e1; AUNOA; RP e45785b3-9455	
11d1++bit (CO080367-1 AUROA FP +4M0154-bit8 11d1-8702-C0-04b 5605) AUROA CB +t 721+53-11+2-11+0-8015-	100
00aa0010529b; WD (0A; FP; 5/202010-75a5-11c0-8020-00c0/fe2exef; R5)(0A; RPWP or 567a7/ 0ce5-11c0-a285-00aa003015e2; CA)	
OX: RP 45a9s11s Gize 4C5s 57e54565645562; S-1-5-32-560(OA: RPWP 5d559s1s-9422-11s1-eso5000290367s1; S-1-5-32-551 OA: RPWP 5805s528cs34428a5e2455a04c135e; S-1-5-32-551; taxes 0: IOA: CR ab721a53-1a27-11s35815-00aa0040529x; PS1	
(DR, REVP, Southors/Addots-4423-add/Addate(1556, 3-1-5-32-061), base U (DR, CR, adv2 ta 53-1627-1105-5515-3044006250, PS) user: eviter Roce memoion forcet 16, base 0	1
Done concering schemes.	_
	٠

7. Choose File>Create LDIF file. In this example, the file created is diff-schema.ldf. To simplify the process, create the file in C:\windows\adam.

Tip: You can create a separate directory to keep the files that are generated separate from the main C:\windows\adam directory.

AD DS/LDS Schema Analyzer	_ [] >
Te Schema Toolo	
Load target schema, Ctrl+T	
Load base schema Ctrl+8	
Create LDF Re Cel H.	
CCDCLCSWRPWPDTLCCRSDRCWDW0 _SY(A_LCRPLORC_AUI_base D.S.	
CCDCLCSWRPWPDTLOCRSDRCWDW0 SY(A:LCRPLORC AU) base D.S.	
CCDCLCSWRPWPDTL0CRSDRCWDW0::SY(A:LCRPL0RC::AU): base D:S: bnetCentainer: defaultSecurityDescriptor manatich: target D (A:CCDCLCSWRPWPL0CRRCWDW0;)	
(CCDLCSWRPWPDTuCRSDRCWDWO)_SYX;LCRPU0RC=XU) base D-5: bretContainer default SecurityDescriptor manatoly: target D (A; CCDCLCSWRPWP LOCRRCWDWO; .CCDCLCSWRPWPDTuCRSDRCWDWO_SY(A; LCRPu0RC_XU) base D-5:	
-CDDLCSWRPWPD10CFS9RCVPW0_SVV-LCPR/GRC-AU) base D-5- benformaner edualSecutySecution manufactor target D(x,CDCLCSWRPWPL0CFRCWDW0; .CDDLCSWRPWPD10CFS9RCVPW0_SVVA.CDPL0RC-AU) base D-5; .edualSecutySecutor mission target D(x,ACCDLCSWRPWPD1L0CFRSPRCWDW0;;DA)	
-CCDLCSWRPWPDTLOCRSDRCVDWO-SYVALCRPLORC-AU base D-S benctmatter: edualseuxty-beapter manterio target D (ACCELCSURPW/LOCRRCVDWO; -CCDLCSWRPWPDTLOCRSDRCVDWO - SYVALCRPLORC-AU base D-S - delat Security-Security manador. target D (A CCDCLSWRPWPTLOCRSDRCVDWD; -CCDLCSWRPWPDTLOCRSDRCVDWO - SYVALCRPLORC-AU base D-S -CCDLCSWRPWPDTLOCRSDRCVDWO - SYVALCRPLORC-AU base D-S -CCDLCSWRPWPDTLOCRSDRCVDWO - SYVALCRPLORC-AU base D-S	
.ccbb.csviR9W907L0CR5B0CVDV0_SYV_LCRPL0R_UNL_base 0.5 .opencharaer offan beautybesport manaton target 0.4, ccbb.csviR9V910CR3CVDV00_ .ccbb.csviR9V97L0CR5D0CVDV0_SYV_LCRPL0R_UNL_base 0.5 .ode1stSeutybeston trimaton target 0.4 ccbb.csVR9VPV0T0CR5RPVVDV0_D4) .ccbb.csviR9V97L0CR5B0CVDV0_SYV_LCRPL0R_UNL_base 0.5 .ccbb.csviR9V97L0CR5B0CVDV0_SYV_LCRPL0R_UNL_base 0.5 .ccbb.csviR9V97L0CR5B0CVDV0_SVV_LCRPL0R_UNL_base 0.5 .ccbb.csviR9V97L0CF5B0CVDV0_SVV_LCRPL0R_UNL_base 0.5 .ccbb.csviR9V97L0CF5B0CVDV0_SVV_LCRPL0	(DA)
CEDECSWIPP/EDTLOGSBORVEWORDSHIPP/EDFLOGSB	:04) (ALLCRF.LORC: /5) 28:-P510A: CR 40721456-142
CCDC.SWIRPVPDTLCCFSBPCVVVV0-SVV/LCF8/CRC-XVI, texe D-5 condicitateer deal issuity benome material texp 0.5 (CCCLSWIRPV7DLCCRCWVV0v0, CCDCSSWIRPV7DLCFSBPCVVVV0-SVVLCPFVCRC-XVI aee D-5 codd.Security explore instance texp 0.4 CCDCLSWIRPV7BLDCRCBVVDV0-DA CCDCSSWIRPV7EVCOSBPCVVV0-SVVLCPFCRC-XVI aee D-5 codd.Security explore instance texp CCDCLSWIRPV7EVCOSBPCVVV0-SVVLCPCRC-XVI aee D-5 codd.Security explore instance texp CCDCLSWIRPV7EVCOSBPCVV0-SVVLCPCRC-XVI aee D-5 CCDCLSWIRPV7EVCOSBPCVV0-SVVLCPCRC-XVI aee D-5 CCDCLSWIRPVFEVCOSBPCVV0-SVVLCPCRC-XVI aee D-5 A CCBC 2FVFEVCOSBPCVV0-SVVLCPCRC-XVI aee D-5 SVFEVCOSBPCVV0-SVC ACCBC 2FVFEVCOSBPCVV0-SVVLCPCRC-XVI aee D-5 SVFEVCOSBPCVV0-SVC ACCBC 2FVFEVCOSBPCVV0-SVVLCPCRC-XVI aee D-5 SVFEVCOSBPCVV0-SVC ACCBC 2FVFEVCOSBPCVV0-SVVLCPCRC-XVVC-SVC ACCBC 2FVFEVCOSBPCVV0-SVC ACCBC 2FVFEVCOSBPC ACCBC 2FVFEVCOSBPCVV0-SVC ACCBC 2FVFEVCOSBPC ACCBC 2FVFEVCOSBPC ACCBCC 2FVFEVCOSBPC ACCBC 2FVFE	(A;LCRF(L0RC::-P5) 28:-P5I(0A:CR ab721a55-1a2 24:57582-2455-11d1-ubb
CCCC.SWRPVE7LOFSBRVVFW0 ⁻ -SVV-LGRURC-XU, see D-S conditioner read-based because and set to D-SCCC.SWRPVE7LOFBBRVDW0- CCCCL.SWRPVFV1COCHSBRVVFW0 ⁻ -D-SCCCL.SWRPVE7LOFBBRVDW0- CCCL.SWRPVFV1COCHSBRVVFW0 ⁻ -D-SCCCL.SWRPVE7LOFBBRVDW0- D-SCCL.SWRPVFV1COCHSBRVVFW0 ⁻ -D-SVV-LFR-RCVCL.SWRPVE7LOFBBRVDW0- coldbased based based and based based based based based based in detailsbased based based based based based based based based based based of Class D-SWRPVFV1COCHSBRVVFV1CO-SWRPVE7LOFBBRVDW0- CCLL.SWRPVFV1COCHSBRVVFV1CO-SWRPVE7LOFBBRVDW0- ACCLLSWRPVFV1COCHSBRVVFV1CO-SWRPVE7LOFBBRVDW0- ACCLLSWRPVFV1COCHSBRVVFV1CO-SWRPVE7LOFBBRVDW0- ACCLLSWRPVFV1COCHSBRVVFV1CO-SWRPVF0CO-SWRPVE7LOFBBRVVF0- ACCLLSWRPVFV1COCHSBRVVFV1CO-SWRPVF0CO-SWRPVE7LOFBBRVVF0- ACCLLSWRPVFV1COCHSBRVVFV1CO-SWRPVF0CO-SWRPVE7LOFBBRVVF0- ACCLLSWRPVFV1COCHSBRVVFV1CO-SWRPVF0CO-SWRPVE7LOFBBRVVF0- ACCLLSWRPVFV1COCHSBRVVFV1CO-SWRPVF0CO-SWRPVF0- ACCLLSWRPVFV1COCHSBRVVFV1CO-SWRPVF0-SWRPVF0- ACCLLSWRPVF1COCHSBRVVFV1CO-SWRPVF0-SWRPVF0- ACCLLSWRPVF1COCHSBRVVFV1CO-SWRPVF0-SWRPVF0- ACCLLSWRPVF1COCHSBRVVFV1CO-SWRPVF0-SWRPVF0- ACCLLSWRPVF1COCHSBRVVFV1CO-SWRPVF0-SWRPVF0- ACCLLSWRPVF0-SWRPVF0-SWRPVF0-SWRPVF0-SWRPVF0- ACCLLSWRPVF0-SWRPVF0-SWRPVF0-SWRPVF0-SWRPVF0- ACCLLSWRPVF0-SWRPVF0-SWRPVF0-SWRPVF0-SWRPVF0-SWRPVF0- ACCLLSWRPVF0-SWRPVF0	0.6) (ALLCRFLORC::-F5) 28:_F5)(0.4:_CR-ab.721a56-1a2 (a45.78)(2.3405-11d1-aub 11d2-6422.480-56135-135) -R5)
CEDICLOSVIER/VEDTLOESBORVEWONG-SYVELEBRICINE-AU, and Co. Compositioner and a strand became and an operation of the CEDICLOSVIER/OF and a strandown of details and became and an operation of the CEDICLOSVIER/OF AUXIENT OF details and the CEDICLOSVIER/VEDTLOESBORVEWONG INCOME. CEDICLOSVIER/VEDICLOSVIER/VEDTLOESDORVEWONG INCOME AND A ceDICLOSVIER/VEDICLOSVIER/VEDTLOESDORVEWONG INCOME AND A ceDICLOSVIER/VEDICLOSVIER/VEDTLOESDORVEWONG INCOME AND A ceDICLOSVIER/VEDICLOSVIER/VEDTLOESDORVEWONG INCOME AND A ceDICLOSVIER/VEDICLOSVIER/VEDTLOESDORVEWONG INCOME AND a ceDICLOSVIER/VEDICLOSVIER/VEDTLOESDORVEWONG INCOME and a ceDICLOSVIER/VEDICLOSVIER/VEDTLOESDORVEWONG INCOME and a ceDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/ VEDICLOSVIER/ VEDICLOSVIER/VEDICLOSVIER/ V	0A) (A-LCRFLORC: 95) 28: F30(A-CR ab/721656-1e2) ad5/3952.9455-1141-auto 1142-642-050-68959-83) 144: F50(A-C, AU)
CCCC.SWIRPVEDTLOESSORVEWOD': SVVLCERPLOE_AULess Dis CCCC.SWIRPVEDTLOESSORVEWOD': SVVLCERPLOE_AULESE Dis CCCC.SWIRPVEDTLOESSORVEWOD': SVVLCERPLOE_AULESE Dis CCCC.SWIRPVEDTLOESSORVEWOD': SVVLCERPLOE_AULESE Dis CCCC.SWIRPVEDTLOESSORVEWOD': SVVLCERPLOE CCCC.SWIRPVEDTLOESSORVEWOD': SVVLCERPLOE CCCC.SWIRPVEDTLOESSORVEWOD': SVVLCERPLOE CCCC.SWIRPVEDTLOESSORVEWOD': SVVLCERPLOE CCCC.SWIRPVEDTLOESSORVEWOD': SVVLCERPLOE CVCC.SWIRPVEDTLOESSORVEWOD': SVVLCERPLOE SVVVLCERPLOE SVVLCERPLOE SVVLCERPLOE SVV	0A) (ALLCRPLORC: P5) 2b: P5)(A-CR ab 721656-162 w657852-2465-1141 auto 1142-1422 (ALGC6889399-R3) 1441 R3(A-RC: AU) 1441 R3(A-RC: AU)
CCCC.SWIRPVPDTLCCES.BROVTWOT-SYVELEBRIDR_ALIser_Color_Aliser_Color_	(04) (ALCS9 (0RC - 95) (28, PSI(0A)CR ab 7216561e2 (26)S122405(0689535 RS) (44)S1242205(0689535 RS) (44)S12475(24)5(068953 RS) (44)S12476(24)S125(24) (5)S12471102515)
CCDC.SWIRPVPDTLCCFSBPCVVVV0-SVVVCTBPLCRPLCRC-XVV area D-S conditionant michailanus (honorana market hand 1000 conditional hand 1000 conditional conditionant michailanus (honorana market hand 1000 conditional hand 1000 conditional conditional hand 1000 conditional hand 1000 conditional hand 1000 conditional conditional hand 1000 conditional hand 1000 conditional hand 1000 conditional conditional hand 1000 conditional hand 1000 conditional hand 1000 conditional conditional hand 1000 conditional hand 1000 conditional hand 1000 conditional conditional hand 1000 condi	(CA) (ALLOST LORC 5.) (24FS)(CACR ab 72.456 he2 (45.522.2465 h11 fato) (14.522.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.533.465
CCCC.SWIRPVPDTLCCES.BOCVTW07-CVVLCEBFLORC-AU, see Col- complex.memory.com/science/s	(CA) (ALLOST LORC 5.) (24FS)(CACR ab 72.456 he2 (45.522.2465 h11 fato) (14.522.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.523.465 h12 (14.533.465
ccdbbcsWiRPWPDTL0CBSRPCVTWWC=VYVLCBPL0RC=XVILsee DS- exectmenter of two-factures/bency/	(CA) (ALLOST LORC 5.) (24: - PSI(-) - (21: ab 72: ab 5-1 ac 2 - ad 5: 302, 2 = 40, 5-1 ab 72: ab 5-1 ac 2 - ad 5: 302, 2 = 40, 5-1 ab 72: ab 7
CCDDLSWIRPVFDTLOCESDPCVFW0 ⁻² -SYV-LLSBLORC-XU, texp D-5 conditionare real-standy hostopart comparison tage 10, CCDLSWIRPVFDLOCESDWIRPVFD to destinate real-standy hostopart comparison tage 10, CCDLSWIRPVFDLOCESDWIRPVFD conditionare real-standy and tage 20, CCDLSWIRPVFDLOCESDWIRPVFDURPVFDLOCESDWIRPVFDURPVFDURPVFDLOCESDWIRPVFDURPVFDURPVFDURPVFDURPVFDURPVFDURPVFDURPVFDURPVFDURPVF	(CA) (ALLOST LORC 5.) (24: - PSI(-) - (21: ab 72: ab 5-1 ac 2 - ad 5: 302, 2 = 40, 5-1 ab 72: ab 5-1 ac 2 - ad 5: 302, 2 = 40, 5-1 ab 72: ab 7
er stelle Beurg Desopor manter langet D. (ACCDL/SWRPWPCT_OCREDRCWRWO_AA) CCDL_SWRPWPCTOLCREDRCWRWO_X01A, CCDL_SWRPWPCTLOCREDRCWRWO_AA ACRes 72165-162-1162-8315-06650005260 (5306-074), CR 6472165-162-130581 5-06651005 100 887 0 (6680-01250), FSQL, RPW7-7546085 5-944, 1114 avod 000038571 FSIGA, RPWR	(CA) (ALLOST LORC 5.) (24: - PSI(-) - (21: ab 72: ab 5-1 ac 2 - ad 5: 302, 2 = 40, 5-1 ab 72: ab 5-1 ac 2 - ad 5: 302, 2 = 40, 5-1 ab 72: ab 7

8. Open a command prompt and create a log directory in the C:\windows\adam directory:

cd \windows\adam mkdir logs

9. Import the LDIF schema that was created using the ADSchemaAnalyzer to AD LDS:

ldifde -i -s localhost:50000 -c CN=Configuration,DC=X #ConfigurationNamingContext -f diff-schema.ldf -j c:\windows\adam\logs

For more information about ldifde options and command formats, go to <u>Using LDIFDE to import and export</u> <u>directory objects to Active Directory</u> on Microsoft.com.

Administrator: C/Windows/system32/cmd.csc	. 🗆 ×
:\Windows\ADAH>ldifde -i -s localhost:50000 -c CN-Configuration,DC-X #Config ionNamingContext -f diff-cohema.ldf -j c:\vindovs\adam\logs onnecting to "localhost:50000"	ura 🔺
ogging in as current user using SEPI monthing directory from file "diff-schema.ldf" cading entries	-
oacing energes	
163 entries modified successfully.	
to command has completed successfully	
=\Windows\ADAH)	-

5. Extend the AD LDS Schema with the User-Proxy Objects

The object for the proxy authentication needs to be created, but do not use the object class **user**. Instead, the object class **userProxy** is created to allow the bind redirection, and the object class detail is created in a new LDIF file. The example file below, **MS-UserProxy-Mxabu.Idf**, was generated from the original MS-UserProxy.Idf and then edited by using a text editor so that it has the following content:

```
#_____
# @@UI-Description: AD LDS simple userProxy class.
# This file contains user extensions for default ADAM schema.
# It should be imported with the following command:
# ldifde -i -f MS-UserProxy-Mxabu.ldf -s localhost:50000 -j
c:\windows\adam\logs -c "CN=Schema,CN=Configuration,DC=X"
#schemaNamingContext
dn: CN=User-Proxy, CN=Schema, CN=Configuration, DC=X
changetype: ntdsSchemaAdd
objectClass: top
objectClass: classSchema
cn: User-Proxy
subClassOf: top
governsID: 1.2.840.113556.1.5.246
schemaIDGUID:: bxjWYLbzmEiwrWU1r8B2IA==
rDNAttID: cn
showInAdvancedViewOnly: TRUE
adminDisplayName: User-Proxy
adminDescription: Sample class for bind proxy implementation.
objectClassCategory: 1
lDAPDisplayName: userProxy
systemOnly: FALSE
possSuperiors: domainDNS
possSuperiors: organizationalUnit
possSuperiors: container
possSuperiors: organization
defaultSecurityDescriptor:
D:(OA;;CR;ab721a53-1e2f-11d0-9819-00aa0040529b;;PS)S:
defaultHidingValue: TRUE
defaultObjectCategory: CN=User-Proxy, CN=Schema, CN=Configuration, DC=X
systemAuxiliaryClass: msDS-BindProxy
systemMayContain: userPrincipalName
systemMayContain: givenName
systemMayContain: middleName
systemMayContain: sn
systemMayContain: manager
systemMayContain: department
```

```
systemMayContain: telephoneNumber
systemMayContain: mail
systemMayContain: title
systemMayContain: homephone
systemMayContain: mobile
systemMayContain: pager
systemMayContain: msDS-UserAccountDisabled
systemMayContain: samAccountName
systemMayContain: employeeNumber
dn:
```

```
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
```

Perform these steps:

- 1. Save the MS-UserProxy-Mxabu.Idf file in the C:\windows\adam directory.
- 2. Import the new object class to AD LDS:

ldifde -i -s localhost:50000 -c CN=Configuration,DC=X #ConfigurationNamingContext -f MS-UserProxy-Mxabu.ldf -j c:\windows\adam\logs



6. Import Users from AD DC to AD LDS

The user from each domain now needs to be imported to AD LDS.

Note:

- You must add a service account from each of the domains to the Administrators group in the LDS server.
- Repeat this step for each domain that needs to be synchronized. This example shows the process against only two of the domains.

Perform these steps:

First Domain: MXABU.COM

1. Starting with the original MS-AdamSyncConf.xml file, create an XML file for each domain that needs to be synchronized and modify the file with the details specific to each domain so that it has the following content:

```
<?xml version="1.0"?>
<doc>
<configuration>
<description>mxabu.com</description>
```

```
<security-mode>object</security-mode>
<source-ad-name>mxabu.com</source-ad-name>
<source-ad-partition>dc=mxabu,dc=com</source-ad-partition>
<source-ad-account></source-ad-account>
<account-domain></account-domain>
```

```
<target-dn>dc=mxabu,dc=com</target-dn>
<query>
<base-dn>dc=mxabu,dc=com</base-dn>
<object-filter>
(|(&(objectClass=user)(objectCategory=person))
(&(objectClass=user)(isDeleted=TRUE)))
</object-filter>
```

```
<attributes>
<include>objectSID</include>
<include>mail</include>
<include>userPrincipalName</include>
<include>middleName</include>
```

```
<include>manager</include>
<include>givenName</include>
<include>sn</include>
<include>department</include>
<include>telephoneNumber</include>
```

```
<include>title</include>
<include>homephone</include>
<include>mobile</include>
<include>pager</include>
<include>msDS-UserAccountDisabled</include>
```

```
<include>samAccountName</include>
<include>employeeNumber</include>
<exclude></exclude>
</attributes>
</query>
<user-proxy>
```

```
<source-object-class>user</source-object-class>
<target-object-class>userProxy</target-object-class>
</user-proxy>
<schedule>
<aging>
<frequency>0</frequency>
<num-objects>0</num-objects>
</aging>
<schtasks-cmd></schtasks-cmd>
</schedule>
</configuration>
<synchronizer-state>
<dirsync-cookie></dirsync-cookie>
<status></status>
<authoritative-adam-instance></authoritative-adam-instance>
<configuration-file-guid></configuration-file-guid>
<last-sync-attempt-time></last-sync-attempt-time>
<last-sync-success-time></last-sync-success-time>
<last-sync-error-time></last-sync-error-time>
<last-sync-error-string></last-sync-error-string>
<consecutive-sync-failures></consecutive-sync-failures>
<user-credentials></user-credentials>
<runs-since-last-object-update></runs-since-last-object-update>
<runs-since-last-full-sync></runs-since-last-full-sync>
</synchronizer-state>
```

</doc>

- 2. In this file, place the following tags to match the domain:
 - <source-ad-name>: Use the DNS name of the domain, for example, mxabu.com.
 - <source-ad-partition>: Use the root partition from the source AD DC that you want to import from; for example, dc=Mxabu, dc=com.
 - <base-dn>: Choose the container to import from. If all users of the domain are required, this container would be the same as <source-ad-partition>, but if users are from a specific organizational unit, for example, Finance OU, it would be similar to OU=Finance,DC=Mxabu,DC=com.
- 3. Save the newly created XML file in the C:\windows\adam directory.
- 4. Open a command window.

cd \windows\adam

5. Run the following command:

ADAMSync/install localhost:50000 AdamSyncConfMxabu.xml/log logs\install.log

Note: The file AdamSyncConfMxabu.xml is the newly created XML file.

6. Synchronize the users with the following command:

ADAMSync/sync localhost:50000 "dc=mxabu,dc=com"/log logs\sync.log

The log result should be similar to the following:

Adding target object CN=Administrator,CN=Users,dc=mxabu,dc=com. Adding attributes: sourceobjectguid, instanceType, objectSid, SAMAccountName, lastagedchange, ob Conflicting object detected. Requesting rename. Renaming conflicting target object CN=Administrator,CN=Users,dc=mxabu,dc=com to CN=445216f1-9a21 Previous entry took 0 seconds (0, 0) to process Processing Entry: Page 1, Frame 1, Entry 3, Count 2, USN 0 Processing in-scope entry 475e9fd29c173747af29ed3e62c67228> Processing in-scope entry 475e9fd29c173747af29ed3e62c67228. Adding target object CN=Administrator,CN=Users,dc=mxabu,dc=com. Adding target object CN=Administrator,CN=Users,dc=mxabu,dc=com. Adding target object GN=Administrator,CN=Users,dc=mxabu,dc=com. Adding target object GN=Administrator,CN=Users,dc=mxabu,dc=com. Adding the configuration file DirSync cookie with a new value. Beginning processing of deferred dn references. Finished processing of deferred dn references. Finished forcessful) synchronization run. Number of entries processed via dirSync: 6 Number of entries processed via lap: 0 Processing took 0 seconds (0, 0). Number of object additions: 1 Number of object additions: 1 Number of object renames: 1 Number of object renames: 1 Number of references processed / dropped: 0, 0 Maximum number of attributes seen on a single object: 6 Maximum number of values retrieved via range syntax: 0 Beginning aging run. Aging requested every 0 runs. We last aged 1 runs ago. Saving Configuration File.

Second Domain: ICEPG.COM

 Starting with the original MS-AdamSyncConf.xml file, create an XML file for each domain that needs to be synchronized and modify the file with the details specific to each domain so that it has the following content:

```
<?xml version="1.0"?>
<doc>
<configuration>
<description>icepg.com</description>
<security-mode>object</security-mode>
<source-ad-name>icepg.com</source-ad-name>
<source-ad-partition>dc=icepg,dc=com</source-ad-partition>
<source-ad-account></source-ad-account>
<account-domain></account-domain>
<target-dn>dc=mxabu,dc=com</target-dn>
<query>
<base-dn>dc=icepg, dc=com</base-dn>
<object-filter>
(|(&(objectClass=user)(objectCategory=person))
(& (objectClass=user) (isDeleted=TRUE)))
</object-filter>
<attributes>
<include>objectSID</include>
<include>mail</include>
<include>userPrincipalName</include>
<include>middleName</include>
```

```
<include>manager</include>
<include>givenName</include>
```

```
<include>sn</include>
<include>department</include>
<include>telephoneNumber</include>
```

```
<include>title</include>
<include>homephone</include>
<include>mobile</include>
<include>pager</include>
<include>msDS-UserAccountDisabled</include>
```

```
<include>samAccountName</include>
<include>employeeNumber</include>
<exclude></exclude>
</attributes>
</query>
<user-proxy>
```

```
<source-object-class>user</source-object-class>
<target-object-class>userProxy</target-object-class>
</user-proxy>
<schedule>
<aging>
<frequency>0</frequency>
<num-objects>0</num-objects>
</aging>
<schtasks-cmd></schtasks-cmd>
</schedule>
</configuration>
<synchronizer-state>
<dirsync-cookie></dirsync-cookie>
```

```
<status></status>
<authoritative-adam-instance></authoritative-adam-instance>
<configuration-file-guid></configuration-file-guid>
<last-sync-attempt-time></last-sync-attempt-time>
<last-sync-success-time></last-sync-success-time>
<last-sync-error-time></last-sync-error-time>
```

```
<last-sync-error-string></last-sync-error-string>
<consecutive-sync-failures></consecutive-sync-failures>
<user-credentials></user-credentials>
<runs-since-last-object-update></runs-since-last-object-update>
<runs-since-last-full-sync></runs-since-last-full-sync>
</synchronizer-state>
</doc>
```

- 2. In this file, the following tags should be replaced to match the domain:
 - <source-ad-name>: Use the DNS name of the domain; for example, icepg.com.
 - <source-ad-partition>: Use the root partition from the source AD DC that you want to import from; for example, dc=lcepg, dc=com.
 - <base-dn>: Choose the container to import from. If all users of the domain are required, this container would be the same as <source-ad-partition>, but if users are from a specific organizational unit, for example, Finance OU, it would be similar to OU=Finance,DC=icepg,DC=com.
- 3. Save the newly created XML file in the C:\windows\adam directory.

4. Open a command window.

cd \windows\adam

5. Run the following command:

ADAMSync/install localhost:50000 AdamSyncConfIcepg.xml/log logs\install.log

Note: The file AdamSyncConflcepg.xml is the newly created XML file.

6. Synchronize the users with the following command:

ADAMSync/sync localhost:50000 "dc=mxabu,dc=com"/log logs\sync.log

The log result should be similar to the following:

```
updating the configuration file DirSync cookie with a new value.
Beginning processing of deferred dn references.
Finished processing of deferred dn references.
Finished (successful) synchronization run.
Number of entries processed via dirSync: 9
Number of entries processed via ldap: 2
Processing took 0 seconds (0, 0).
Number of object additions: 8
Number of object deletions: 0
Number of object deletions: 0
Number of object renames: 2
Number of references processed / dropped: 0, 0
Maximum number of attributes seen on a single object: 6
Maximum number of values retrieved via range syntax: 0
Beginning aging run.
Aging requested every 0 runs. We last aged 1 runs ago.
Saving Configuration File on DC=mxabu,DC=com
Saved configuration file.
```

- 7. To perform a periodic sync from AD to ADAM, use the Task Scheduler in Windows.
- 8. Create a .cmd or .bat file with the following content:

```
cd \Windows\ADAM
ADAMSync /install localhost:50000 AdamSyncConfMxabu.xml /log logs\install.log
ADAMSync /sync localhost:50000 "dc=mxabu,dc=com" /log logs\sync.log
ADAMSync /install localhost:50000 AdamSyncConfIcepg.xml /log logs\install.log
ADAMSync /sync localhost:50000 "dc=mxabu,dc=com" /log logs\sync.log
```

- 9. Schedule the task to run the .cmd or .bat file as required. This process helps ensure that additions, modifications, and deletions in AD are reflected in ADAM.
- 10. You can create another .cmd or .bat file and schedule it to perform a periodic sync from the other forest.

7. Create the User in AD LDS for DMM Synchronization and Cisco Show and Share Authentication

Perform these steps:

- 1. From the Administrator tools in the Start menu, open ADSI Edit.
- 2. On the Action menu, choose **Connect to**.
- Connect to base DN of the AD LDS tree (DC=Mxabu,DC=com) and specify the host and port where it is hosted (localhost:50000). Click OK.

Connec	tion Settings	×
Name:	Default naming context	
Path:	LDAP://localhost:50000/dc=mxabu,dc=com	
	ection Point ielect or type a Distinguished Name or Naming Context:	
	dc=mxabu,dc=com	
C s	elect a well known Naming Context:	
	Default naming context	
Comp	uter elect or type a domain or server: (Server Domain [:port])	7
	Iocalhost:50000	
00	Default (Domain or server that you logged in to)	
Г	Jse SSL-based Encryption	
Advar	OK Cancel	

4. Right-click on the base DN, and then choose New>Object.

Create Ob	Jeek .	
Sele	ct a dass:	
	oncRpc organization organization physical.ocation printQueue remoteMailRedpient rFC5223.ocaPart rpcContainer samServer user	-
	userProxy volume	
		- k

- 5. Select a class of user and click **Next**. In this example, "LDAPuser" was chosen, but you can choose any name here.
- 6. Provide a password for the new user, right-click on the user, and then choose **Reset Password**.

7. Enable the new user; it is disabled by default. Right-click on the user and choose **Properties**.

ADSI Edit Default naming	context [localhost:50000]		
DC=mxabu CN=1	,dc=com		
	N=LDAPuser Properties		?
CN=	Attribute Editor		
CN=	1		
OU= ON=	Attributes:		
CN=	Attribute	Value	
CN=	msDS-PhoneticComp	<not set=""></not>	
	msDS-PhoneticDepar	<not set=""></not>	
	msDS-PhoneticDispla	<not set=""></not>	
	msDS-PhoneticFirstN	<not set=""></not>	
	msDS-PhoneticLastN	<not set=""></not>	
	msDS-SecondaryKrb	<not set=""></not>	_
	msDS-Site-Affinity	<not set=""></not>	
	msDS-SourceObjectDN	<not set=""></not>	
	msDS-SupportedEncr	<not set=""></not>	
	msDS-UserAccountDi	TRUE	
	msDS-UserDontExpir	<not set=""></not>	
	ms-DS-UserEncrypte		
	ms-DS-UserPassword	(not set>	
	msExchAssistantName	<not set=""></not>	-
			<u>ت</u>
			-
	Edt		Filter
	Eat		riter

8. Browse to the msDS-UserAccountDisabled attribute.

Attribute	Value
mail	<not set=""></not>
manager	<not set=""></not>
middleName	<not set=""></not>
mobile	<not set=""></not>
mS-DS-ConsistencyC	<not set=""></not>
mS-DS-ConsistencyG	
msDS-UserAccountDi	. TRUE
msDS-UserDontExpir	<not set=""></not>
ms-DS-UserEncrypte	<not set=""></not>
me-DS-UserPassword	<not est=""></not>
name	root
ntPwdHistory	<not set=""></not>
0	<not set=""></not>
objectCategory	CN=Person,CN=Schema,CN=Configuration,C
4	

9. Choose **Edit** and change the value to **False**.

Attribute mail manager middle Boolean Att	Value <not set=""> <not set=""> <not set=""> </not></not></not>	
mobile mS-DS Attribute: mS-DS Value: mS-DS C Trub mS-DS Falce ms-DS SNot set name rtPwd	ribute Editor X msDS-UserAccountDisabled OK Cancel	
objectCategory	CN=Person,CN=Schema,CN=Configur	ation,C

- 10. The new user needs to be added to one group that has read permission to the AD LDS. In this example, Administrators was chosen.
- 11. Browse to the CN=Roles container, right-click the CN=Administrators group, and choose Properties.

CN=Administrate	Move	
CN=Users	New Connection from Here	
	New	۲
	View	•
	Delete	
	Rename	
	Refresh	
	Export List	
	Properties	
	Help	

12. Browse to the member attribute and click Edit.

	1
Value	
<not set=""></not>	
<not set=""></not>	
inde	
	Distinguished Name / SID CN=LDAPuser.DC=mxabu.DC=com
1	
nt	Remov

- 13. Add the new Distinguished Name (DN) that was previously created (for example, cn=LDAPuser,dc=mxabu,dc=com) to this group.
- 14. Update the schema.



15. Restart AD LDS.

Am im Harlager (Mildrid-1) D Rubes	Added Desidory Lightenight Devidery Services		
Active Devices a Domain Sec.	Provide a state for againstic specific checking state		
Charlottia	C Samery		-
En Provingt	S () texater information trainet in trainet	THE GA IN EVENT SERVER	
	7 then	Eis zeisertinente	
	Lot with an and the second the second seco	C Pole Alfreda	
	⊗ System Services: Alluring Budechers Education Dense Parts Tracks Tax (Merice)	C. for to Carnese	
	Chaldford Multiplation Assess	All they	
	Peargetary	D neggt	
	C Advanced State		
	Greate a nex AD IDIS instance	AD LOS Server Mount	
	Query, envy, and additulgestic and attributes in the sheatery	ADDERen	
	Faction (that specifiers against the deather such as instruct, bod, east it, routh, add, and chiefs	Call Lotto want	

8. Configure Bind Redirection

By default, binding to ADAM with bind redirection requires an SSL connection. SSL requires the installation and use of certificates on the server that is running ADAM and on the server that connects to ADAM as a client. If certificates are not installed in your ADAM test environment, you can disable the requirement for SSL as an alternative.

Note: Disabling the requirement for SSL for bind redirection causes the password of a Windows security principal to pass to the computer that is running ADAM without encryption. Thus, you should disable the SSL requirement only in a test environment.

By default, SSL is enabled. Perform these steps:

- Generate the certificate for ADAM/AD LDS. Consult Microsoft documentation for information about ADAM/AD LDS certification generation.
- 2. Upload the ADAM/AD LDS certificate to the Cisco DMM for Show and Share[®]. Refer to the <u>User Guide for</u> <u>Cisco Digital Media Manager</u> on Cisco.com for more information.
- 3. Choose the checkbox to use SSL in the LDAP Directory page and the LDAP Authentication page.
- 4. Enter 50001 (in our example) for the LDAP port, which is the SSL port number given while installing the ADAM/AD LDS instance.

To disable the SSL requirement for bind redirection, perform these steps:

- 1. Click Start, point to Administrative Tools, and click ADSI Edit.
- 2. On the Action menu, choose **Connect to**.
- 3. Under computer, type localhost:50000, the host and port for ADAM.

onnection Settings	
Name: Configuration	
Path: LDAP://localhost:50000/Configuration	
Connection Point	
C Select or type a Distinguished Name or Naming	Context:
	-
Select a well known Naming Context:	
Configuration	
Computer	
 Select or type a domain or server: (Server D 	omain (:port])
localhost:50000 K	
C Default (Domain or server that you logged in t	•)
	•)
C Default (Domain or server that you logged in t	o)

- 4. Under Connection point, choose Select a well-known Naming Context>Configuration and then click OK.
- 5. In the console tree, browse to this container object in the configuration partition: CN=Windows NT,CN=Services.

Configuration [localhost: 50000] CN=Configuration,CN=(48E9D889 CN=DisplaySpecifiers CN=DisplaySpecifiers CN=Extended-Rights CN=Extended-Rights CN=LostAndPoundConfig CN=NTDS Quotas CN=Partitions CN=Partitions CN=Services CN=Services CN=Vindows NT CM=Configure CN=Vindows NT	9-DFS	
CN=Sites	Move New Connection from Here	
	New	•
	View	•
Opens the properties dialog box for the curr	Delete Rename Refresh Export List	
System	Properties	
1 item selected	Help	5/5

6. Right-click **CN=Directory Service** and then choose **Properties**.

- 7. In Attributes, click msDS-Other-Settings and then click Edit.
- 8. In Values, click RequireSecureProxyBind=1 and then click Remove.
- 9. In Value to add, type RequireSecureProxyBind=0, click Add, and then click OK.
- 10. Restart AD LDS for the changes to take effect.

For more information, refer to Managing Authentication in ADAM on Microsoft.com.

9. Configure DMM for Cisco Show and Share

Perform these steps:

- 1. Log in to DMM as superuser.
- 2. Choose Administration>Security>Select Mode.
- 3. Perform these steps to add the LDAP to the DMM:
 - a. For Authentication Mode, choose LDAP.
 - b. Add the Host: [IP address of the LDS Server] and Port: 50000.
 - c. For Administrator DN, add: cn=ldapuser,dc=mxabu,dc=com.
 - d. Add the LDAPuser Password created in LDS.

Dashboard	Fallover	Settings	Security	Users	Alerts	Services	Licensing
Authentication	Session						
* Select the a * Enter the ro	to do any of the f authentication mo utable IP address	following: [Select Mode, ide for user accounts. s or DNS-resolvable hos tication credentials for a	tname for the authentic	ation system, the		sumber that the authen	tication system uses.
Select Mode	Define Filter	Synchronize Users	Manage Attributes				
Authenticatio	on Mode:	O Embedded	● LDAP ○ Fed	eration			
LDAP Config	guration	Anonymous					
Host		10.35.174.35	Port: 50000				
Administrato	or DN:	cn=ldapuser,dc	=mxabu,dc=com				
Password:		•••••					
Use SSL End	cryption:	0					

4. Choose Define Filter.

- a. Add a description to the filter.
- b. For User Base DN, add: ou=active,ou=mxabuusers,dc=mxabu,dc=com.
- c. For User Filter, add: objectClass=userProxy.
- d. Click Validate and then click Add.

For the icepg.com user, the filter would be similar to the following:

- a. Add a description to the filter.
- b. For User Base DN, add:ou=activeusers,ou=icepgusers,dc=mxabu,dc=com.
- c. For User Filter, add: objectClass=userProxy.
- d. Click Validate and then click Add.

D: 9 Description: M	XABU Users Us	ser Group Name:	MXABU-Users		
iser Base DN: ou=active,o ilter: objectClass=userPro		mxabu,dc≕com			
ynchronization:	O Initial	 Update 	Overwrite	O Delete	Submit Cancel
D: 10 Description: I	CEPG Users U	ser Group Name:	ICEPG-Users		
ser Base DN: ou=activeur ilter: objectClass=userPro		rs,dc=mxabu,dc=com			
ynchronization:	O Initial	 Update 	Overwrite	O Delete	Submit Cancel
D: 12 Description: (CTG Users User	r Group Name: C	TG-Users		
		abu,dc=com			
		abu deseom			

The DMM has imported all users, and you can manage them now in Show and Share. For authentication, users will need to enter the same user ID and password that is in the original AD. Refer to the <u>Administrator Guide for Cisco</u> <u>Show and Share</u> on Cisco.com for more information.



Americas Headquarters Cisco Systems, Inc. San Jose, CA Asia Pacific Headquarters Cisco Systems (USA) Pte. Ltd. Singapore Europe Headquarters Cisco Systems International BV Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Printed in USA