Active Directory Lightweight Directory Services

Installation, configuration et gestion

Date	Version	Auteur	Actions
21/11/2022	1.00	Thierry Adrian	Création
	1		



Sommaire

Somm	naire	2
1.	Préambule	
2.	Déploiement du rôle AD LDS	
2.1. 2.2. 3.	Via PowerShell	3 3 4
4.	Analyse des Schémas	10
5.	Exemple d'export LDIF	11
6.	Exemple d'import LDIF	12
7.	Synchronisation AD LDS	13
8.	Gestion du service AD LDS	13
9.	Suppression de l'instance AD LDS	14



1. Préambule

La mise en application de cette procédure nécessite la lecture et la bonne compréhension de l'article associé publié à l'aide de l'adresse : <u>https://neoconsultin.io/</u>

2. Déploiement du rôle AD LDS

2.1. Via PowerShell

'S C:\> Add-Wir	ndowsFeature ADLDS, R	SAT-ADLDS
uccess Restart	t Needed Exit Code	Feature Result
rue No ARNING: To cre ightweight Di	Success sate a new AD LDS ins rectory Services Setu	Active Directory Lightweight Directory Se tance on server, log on to the destination server and then run th p Wizard. For more information, see http://go.microsoft.com/fwlir
s c:\>		

2.2. Par interface graphique

ad Koles and Features Wizard		- U X
elect server roles		DESTINATION SERVER adids01.nci.lab
Before You Begin	Select one or more roles to install on the selected server.	
Installation Type	Roles	Description
Server Selection	Activo Directory Cortificate Services	Windows Server Update Services
Server Roles	Active Directory Domain Services	allows network administrators to
Features	Active Directory Federation Services	specify the Microsoft updates that should be installed, create separate
	Active Directory Lightweight Directory Services Active Directory Rights Management Services	groups of computers for different
	Device Health Attestation	sets of updates, and get reports on
	DHCP Server	the compliance levels of the
	DNS Server	must be installed
	Fax Server	indet be instance.
	Host Guardian Service	
	Hyper-V	
	Network Policy and Access Services	
	Print and Document Services	
	Remote Access	



3. Configuration de l'instance AD LDS

Active Directory	Lightweight Dir Module for Win Sites and Services
Component Sen	vices of the second sec
Active Directory Ligh	itweight Directory Services Setup Wizard X
	Welcome to the Active Directory Lightweight Directory Services Setup Wizard
	AD LDS is a powerful directory service that is easy to install and deploy. It provides a dedicated data store for applications, and can be configured and managed independently.
	To continue, dick Next.
	< Back Next > Cancel Help
L Active Directory Link	tweight Directory Services Setup Wizard
I neave brieddy Light	
Setup Options An AD LDS instance	a is created each time AD LDS is installed.
Setup Options An AD LDS instance You can create a un	e is created each time AD LDS is installed.
Setup Options An AD LDS instance You can create a un Select the type of ins () A unique instance This option autor configuration and with existing insta	a is created each time AD LDS is installed.
Setup Options An AD LDS instance You can create a un Select the type of ins Aunique instance This option autor configuration and with existing insta A replica of an ex This option create schema partitions the application part	a is created each time AD LDS is installed.

Installation, configuration et gestion d'AD LDS Thierry Adrian



The instance name is used to differentiate this instance of LDS instances on this computer.	f AD LDS from other AD
Type a name for this instance. The name should reflect th of AD LDS is intended.	ne use for which this instan
Instance name:	
instance1	
Example: Addressbook 1	
Description:	
AD LDS instance	
The AD LDS service name is created when the instance product name. It will be displayed in the list of Windows se description you enter. AD LDS service name: ADAM instance1	name is combined with the ervices, together with the

Ports Cor IP a	mputers will connect to this instance of AD LDS using specific ports on all of the addresses associated with this computer.
The	e ports displayed below are the first available for this computer. To change these is, type the new port numbers in the text boxes below.
If yo for t use 102	ou plan to install Active Directory Domain Services on this computer, do not use 389 the LDAP port or 636 for the SSL port because Active Directory Domain Services s these port numbers. Instead, use available port numbers from the following range: 25-65535.
<u>L</u> D/	AP port number:
<u>L</u> D/ 38	AP port number: 9
LD/ 38 SSI	AP port number: 9 L port number:
LD/ 38 <u>S</u> SI	AP port number: 9 L port number: 6
LD/ 38 <u>S</u> SI 63	AP port number: 9 L port number: 6

Application Direct An application di	ory Partition rectory partition sto	ores appli	cation-specifi	ic data.		
			-			
Do you want to creat	e an application dir	ectory pa	artition for this	s instance o	f AD LDS	?
O No. do not create	an application dire	ctory par	tition			
Select this option upon installation, o	f the application th r if you plan to cre	at you pl ate one l	an to install c ater.	reates an a	pplication	directory
• Yes, create an ap	plication directory p	partition				
Select this option i directory partition not already exist in CN=Partition1,DC	f the application th upon installation. A this instance. Exa Woodgrove,DC=0	at you pl valid par mple dist COM	an to install d rtition name is tinguished na	loes not cre any disting me:	ate an app juished na	olication me that does
Datžice came:						
CN-MyFirstApp	C-nci DC-lab					
Gri-ingrillatripp,c	0-10,00-100					

Vous avez la possibilité de créer ou non la partition dès à présent

Installation, configuration et gestion d'AD LDS Thierry Adrian



<u>о</u> А	ctive Directory Lightweight Directory Services Setup Wizard X
Fil	e Locations You can specify a location for each type of file associated with this instance of AD LDS.
	Specify the locations to store files associated with AD LDS.
	Data files:
	C:\Program Files\Microsoft ADAM\instance1\data Browse
	D <u>a</u> ta recovery files:
	C:\Program Files\Microsoft ADAM\instance1\data Browse
	(Bally Marks Council Hale
	< <u>B</u> ack <u>N</u> ext > Cancel Help

AD LDS perfor you select.	ns operations using the permissions associated with the account
Set up AD LDS to p account.	berform operations using the permissions associated with the following
ONetwork service	account
AD LDS has the	permissions of the default Windows service account.
AD LDS service	has the permissions of the selected account.
Password:	••••••
	< Back Next > Cancel Help

Installation, configuration et gestion d'AD LDS Thierry Adrian



)irectory Lightwe					
	ficetory Eightwo	eight Directory	bernees setup			
D LDS	Administrators					
You	an specify the use	er or group that v	will have administra	tive privilege:	s for this	
instar	ice of AD LDS.					
Assig	n the following use	er or group of use	ers administrative p	ermissions for	AD LDS.	
Οū	irrently logged on i	user:				
T	e user that is insta	alling AD LDS wi	ll have administrati	ve permission	s for this	
IT IS	Lance of AD LD3.					
OT	is account					
<u>е</u> л	a calacted upor or	r aroun will bowa	administrativa pag	minational for th	ie instance	n of
A) LDS. You can ch	hoose any user of	or group from this o	computer, this	computer	s
do	main, or any doma	ain that is trusted	by this computer's	domain.		
A	count name:					
N	CI\GS_ADLDS-AI	DM			Browse	
	-					
		< <u>B</u> ack	<u>N</u> ext >	Cance		Help
		< <u>B</u> ack	<u>N</u> ext >	Cance		Help
		< <u>B</u> ack	<u>N</u> ext >	Cancel		Help
-	_	< <u>B</u> ack	<u>N</u> ext >	Cance		Help
-	-	< <u>B</u> ack	<u>N</u> ext >	Cancel		Help
	-	< <u>B</u> ack	<u>N</u> ext >	Cance		Help
•	-	< <u>B</u> ack	<u>N</u> ext >	Cance		Help
	-	< <u>B</u> ack	<u>N</u> ext >	Cancel		Help
Active	Directory Lightw	< Back	Next >	Cancel		Help
Active I	Directory Lightw	< Back	Next >	Cancel		Help
Active I	Directory Lightw	< Back	Next >	Cancel		Help
Active I ervice AD L	Directory Lightw Account Select	eight Director tion ations using the	y Services Setup	Cancel Wizard iated with the	e account	Help
Active I ervice AD L you s	Directory Lightw Account Select DS performs opera	< Back	y Services Setup	Cancel Wizard iated with the	e account	Help
Active I Gervice AD L you s	Directory Lightw Account Selec DS performs opera elect.	< Back	y Services Setup	Cancel Wizard iated with the	account	Help
Active I ervice AD L you s et up AI	Directory Lightw Account Selec DS performs opera elect.	< Back	y Services Setup permissions assoc	Cancel Wizard iated with the	e account	Help >
Active I ervice AD L you s et up AI ccount.	Directory Lightw Account Selec DS performs opera elect.) LDS to perform of dependent account	< Back	y Services Setup permissions assoc the permissions as	Cancel Wizard iated with the	e account	Help >
Active I AD L you s et up AI ccount.	Directory Lightw Account Selec DS performs opera elect. DLDS to perform o the service accourt	< Back	y Services Setup permissions assoc the permissions as	Cancel Wizard iated with the	e account	Help >
Active I AD L you s et up AI ccount.	Directory Lightw Account Selec DS performs oper elect. DDS to perform o dk service account S has the permiss	eight Director tion ations using the operations using ti iions of the defa	y Services Setup permissions assoc the permissions ar	Cancel Wizard iated with the ssociated with	e account	Help >
Active I AD L you s et up AI ccount.	Directory Lightw Account Select DS performs oper elect. I LDS to perform o rk service accour S has the permiss	< Back reight Director ations using the operations using it ions of the defa	y Services Setup permissions assoc the permissions ar	Cancel Wizard iated with the ssociated with ce account.	e account	Help >
Active I ervice AD L you s et up AI ccount. Netwo AD LD	Directory Lightw Account Selec DS performs oper- elect.) LDS to perform of dk service accourt S has the permiss account:	< Back	y Services Setup permissions assoc the permissions at ult Windows servic	Cancel Wizard iated with the ssociated with ce account.	e account	Help >
Active I AD L you s et up AI ccount. AD LD	Directory Lightw Account Selec DS performs opera- elect. DLDS to perform of the service account S has the permiss account: S service has the	< Back	y Services Setup permissions assoc the permissions as ult Windows servic	Cancel Wizard iated with the ssociated with	e account	Help >
Active I ervice AD L you s et up AI ccount. AD LC	Directory Lightw Account Selec DS performs oper elect. D LDS to perform o rk service accour S has the permiss ccount: S service has the	eight Director tion ations using the apperations using ti ions of the defa	y Services Setup permissions assoc the permissions as ult Windows servio he selected accou	Cancel Wizard iated with the ssociated with se account.	e account	Help >
Active I arvice AD L you s et up AI AD LC	Directory Lightw Account Selec DS performs oper elect. DLDS to perform of the service account S has the permiss account: S service has the	eight Director tion ations using the operations using tions of the defa	y Services Setup permissions assoc the permissions are ult Windows servic he selected accou	Cancel Wizard iated with the sesociated with se account.	account	Help >
Active I and L and L you s et up AI ccount. AD LC	Directory Lightw Account Selec DS performs oper- elect. DDS to perform o fk service accour S has the permiss account: S service has the	< Back reight Director ations using the operations using til ions of the defa	y Services Setup permissions assoc the permissions are ult Windows servic he selected account	Cancel Wizard iated with the ssociated with ce account. unt.	account the follow	Help >
Active I AD L you s et up AI AD LC D This a AD LC	Directory Lightw Account Selec DS performs opera- elect. D LDS to perform of rk service account S has the permiss account: S service has the ame:	< Back reight Director ations using the operations using til permissions of the defa	y Services Setup permissions assoc the permissions ar ult Windows servio he selected account	Cancel Wizard iated with the ssociated with se account. int.	e account In the follow	Help

< Back Next > Cancel

Help



Importing LDIF Files You can import data from Lightwei your AD LDS application directory	ght Directory Interchange Format (LDIF) files into partition.	8
To configure the AD LDS service in a s below.	specific way, import one or more of the LDIF files liste	d
LDIF file name	Description	^
MS-AdamSyncMetadata.LDF	ADAMSync metadata schema extension. Required	fc
MS-ADLDS-DisplaySpecifiers.L	AD LDS Display specifiers schema and display spe	ci
MS-AZMan.LDF	AD LDS schema extensions for AzMan.	
MS-InetOrgPerson.LDF	AD LDS memberhain transitive	
MS-ParentDistname.LDF	AD LDS parent dist name.	
MS-ReplValMetadataExt.LDF	AD LDS ReplValueMetaDataExt.	~
<		>
< <u>B</u>	ack <u>N</u> ext > Cancel He	٩þ

Ne pas tout choisir comme illustré. N'importez que ce qui est nécessaire. Vous avez la possibilité d'importer ultérieurement un fichier au formation LDF personnalisé

you want AD LDS Se	nt does not have permission to run as a service. Do etup to add this permission to the account?	
<u> </u>		
	<u>Y</u> es <u>N</u> o	
Active Directory Lightw	eight Directory Services Setup Wizard	×
Ready to Install The AD LDS Setup Wi	zard is ready to install AD LDS with the following	
configuration.		
Before continuing, revie	w and confirm your selections.	
6 L .::		
Install a unique instance	e of AD LDS.	^
Instance name: instanc	ne1	
Computers will connect	t to this instance of AD LDS using the following ports:	
DAP port: 200		
LDAP port: 389 SSL port: 636		
LDAP port: 389 SSL port: 636 AD LDS replication will	use Negotiate authentication.	
LDAP port: 389 SSL port: 636 AD LDS replication will Store AD LDS data file	use Negotiate authentication. s in the following location:	~
LDAP port: 389 SSL port: 636 AD LDS replication will Store AD LDS data file To change your selectii	use Negotiate authentication. s in the following location: ons. click Back. To install AD LDS. click Next	*
LDAP port: 389 SSL port: 636 AD LDS replication will Store AD LDS data file To change your selection	use Negotiate authentication. s in the following location: ons, click Back. To install AD LDS, click Next.	~
LDAP port: 389 SSL port: 636 AD LDS replication will Store AD LDS data file To change your selection	use Negotiate authentication. s in the following location: ons, click Back. To install AD LDS, click Next.	~



nstalling AD LDS The AD LDS Setup Wizard is installing AD I	Active Directory Lightweight Directo ? X
Installing AD LDS	R
Please wait while the wizard completes the f ✓ Copied files Starting the AD LDS service	To import LDIF files, you must be an administrator of this AD LDS instance. Enter the credentials of an account with administrative permissions for AD LDS. The user name must be qualified by a domain or computer name. User name:
	OK Cancel





4. Analyse des Schémas

A l'aide de l'utilitaire ADAMSchemaAnalyzer vous pouvez créer un import LDIF personnalisé. L'idée est la suivante :

- Analyser le schéma côté Active Directory
- Analyser le schéma au niveau AD LDS
- Identifier le delta
- Générer le fichier LDF correspondant à ce delta
- Injecter le fichier LDF

\ADAM>ADSchemaAnalyzer.ex	2		
\ADAM>			
🞇 AD DS/LDS Schema Analy	zer	-	
File Schema Tools			
Load target schema	Ctrl+T		
Load base schema	Ctrl+B		
Create LDIF file	Ctrl+L		
Exit			

Server[:port]	adlds01.nci.lab		
Username	svc.adlds		
Password	•••••		
Domain	nci.lab		
Bind type	• Secure O	Simple	alyzer -
Server type -			
C AD DS/LDS	1		
C Generic (st	ubschemaSuber	itry)	



📊 AD DS/LDS Schema Analyzer			_	\times	
File Schema Tools					
Classes Options Dependencies graph LDIF generation Miscellaneous Present elements On't update present elements On't update with references to new elements only Update with references to new and present elements Allowed to write systemPossSuperiors and systemAu possSuperiors and auxClasses, if schema circular de	- D	×			



R AD DS/LDS Schema Analyzer	_	×
File Schema Tools		
Classes Attributes Property sets		
Adding classes (pass 13)		^
Updating new classes Updating present elements		
LDIF file created: 354 attributes, 62 classes, 0 property sets, 0 updated present elements.		~

5. Exemple d'export LDIF



🔤 Administrator: Command Prompt - powershell

Exporting directory to file nci-export-from-ad.ldf Searching for entries Writing out entries 3 entries exported	
The command has completed successfully	

6. Exemple d'import LDIF

Administrator: Command Prompt	-		×
\Windows\ADAM>ldifde -i -f My-LDIF-4-Sync.ldf -s localhost:389 -b administrator nci * -jc " onfigurationNamingContext pe the password for localhost:389: nnecting to "localhost:389" gging in as "administrator" in domain "nci" using SSPI porting directory from file "My-LDIF-4-Sync.ldf" ading entries	cn=Configura	ation,do	:=X"
05 entries modified successfully.			
e command has completed successfully			
Awingows (ADAMS)			



7. Synchronisation AD LDS

Cette configuration s'installe ou s'initialise si vous voulez via la une ligne de commande comme suit :

ADAMSync /install %servername% :%port% %XMLconfigurationfilename%

Vous devez donc préalablement éditer le fichier XML de configuration.

Il y a par la suite deux types de synchronisation, i.e. partiel ou complet (exemple disponible sur le site Web)

8. Gestion du service AD LDS

En faisant référence à notre exemple, voici deux commandes simples :

- Arrêt : net stop Instance1
- Démarrage : net start Instance1

Ces mêmes actions sont faisables via l'interface graphique au niveau du Server Manager (illustration ci-dessous)

	All services 1 total	
Local Server	Filter P 🗐 🕶 🖲 🕶	
All Servers	Server Name Display Name Service Name Start Type	Status
File and Storage Services	ADLDS01 instance1 ADAM_instance1 Automatic	Runnin



9. Suppression de l'instance AD LDS

→ ✓ ↑ 🗿 > Control F	anel > Programs > Programs and Features		
Control Panel Home	Uninstall or change a program		
View installed updates	To uninstall a program, select it from the l	ist and then	click Uninstall, Change, or Repair.
Turn Windows features on or	, , ,		
off	Organize 🝷 Uninstall		
Install a program from the	Name		Publisher
network	AD LDS Instance		Microsoft Corporation
	Microsoft Visual	le (x64)	Microsoft Corporation
	Microsoft Visual C++ 2015-2019 Redistribut	able (x86)	Microsoft Corporation
	Motepad++ (64-bit x64)		Notepad++ Team
	VMware Tools		VMware, Inc.

10. Suppression d'AD LDS

Inutile à documenter.