hQGMA4zJmb2qRccfAQv+PP0ICikBlEraqIREjf67wz1aG44Fcsi/0nZpzq53cn1b dy0OIcziXtKXI27PNK0hmYN8mBcjo5Pc2ZFgnacnVR/gVMk00GoWkHf9TCZ/ExmQ XK4CGR7ETkRY7NdBVTct+NsMQA9UJynCf0TlZFWvJcSwLKIDHn/qK6kF9YkH7Ebi tAJk63Xkkh76iqzx+ohAGAvxc8w/7N/cCdSclZ+xswpSB7EP0tSc37i1FbDtzGAm vcTHYbuMlbs9ieANOxv/zWP1+PmAYV/FKmR41j33Sor1oAXmTukb0H9hYw01bOPP



How to install an LDS for use with GnuPG VS-Desktop[®]

Guide for Administrators

Version 3.x Stand 2021-09-17 Revision 001

Content

1 Installing the LDS Service	4
1.1 Setting the LDS up as Keyserver	10
1.2 Assigning Permissions	12
2 Using GnuPG with an LDS Keyserver	15

Introduction

This is a guide on how to install a Windows LDS system for use as keyserver by GnuPG. LDS is the Lightweight Directory Service of Windows formerly known as ADAM. Instead of using the Active Directory (AD) directly for storing GnuPG keys it is often more appropriate to have a separate server running for this. The major benefit is that there is no need to touch the AD to extend its schema. However, for authentication purposes the AD can still be used with an LDS and replication of LDS instances is also possible.

Prerequisites

Assign a separate Windows instance for use with LDS or use an instances which does not run a domain controller but, for example, a machine which runs other internal services. In our example we use the domain w32demo.g10code.de and the LDS service runs on a machine named key-server. The screenshots have been acquired from an English version of Windows-10. The AD in this example has been configured for German; thus some accounts have localized names.

Manufacturer / Distributor

g10 Code GmbH Gutenbergweg 4 40699 Erkrath / Germany +49 2104 493 879 0 info@gnupg.com www.gnupg.com

1 Installing the LDS Service

- Create a user in your AD to maintain the LDS installation.
 In our example this is w32demo\ldsadmin.
- Login as Administrator to the LDS machine. The LDS service comes with all rent Windows version and can be easily enabled. Open the Windows Features dialog and enable LDS:



- Click [OK] and the feature will be installed. LDS might already be enabled and running an partition (i.e. an LDAP service). Note that several partitions can be used on one LDS instance; we will later get back to this.
- You also need some extra tools on that machine. Open the dialog to \emph{Add an Optional Feature} and scroll down to \emph{RSAT: Active Directory DomainSerives and Lightweight Directory Services Tool}and enable this:

~	Settings	Add	an o	ptional feature	
俞	Optional feature	Find	l an ava	ilable optional feature	Q
	Add a feature	Sort I	by: Nam	e ∨	
+	Adu a leature		<₿	RSAT: Active Directory Certificate Services Tools	6.74 MB
See o	pptional feature history	\checkmark	¢	RSAT: Active Directory Domain Services and Lightweight Directory Services Tools	37.5 MB
Inst	alled features			PSAT: Did asker Drive Exemption Administration Utilities	OCE VP
Fin	d an installed optional feature		- दु३	Non, orcocker once charpeon Administration dulities	003 KD
Sort	by: Name 🗸		{ }	RSAT: DHCP Server Tools	9.59 MB

- Click on [Install] to download and install this feature. You may then need to reboot.
- Open a command prompt in Admin mode and enter:

\Windows\adam\adaminstall

• A wizard dialog pops up:



Click [Next] and select "A unique instance":



 Click [Next]. On the next dialog enter the name used for the keyserver; it is best to use the name of the machine or an alias for it:

Active Directory Lightweight Directory Services Setup Wizard	×		
Instance Name The instance name is used to differentiate this instance of AD LDS from other AD LDS instances on this computer.			
Type a name for this instance. The name should reflect the use for which this instance of AD LDS is intended. Instance name:			
keyserver			
Example: Addressbook 1			
Description:			
AD LDS keyserver			
The AD LDS service name is created when the instance name is combined with the product name. It will be displayed in the list of Windows services, together with the description you enter. AD LDS service display name: keyserver AD LDS service name: ADAM keyserver			
< Back Next > Cancel Help			

 Click [Next]. The next dialog requests the port numbers to connect to the service. If this is the first instance, use the suggested standard ports. However, if other partitions are already running on that LDS instance you need to choose other ports which will later be part of the GnuPG configuration. Here is the standard case:

T Active Directory Lightweight Directory Services Setup Wizard	×
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:	
636	
< Back Next > Cancel Help	

• Click [Next]. In the next dialog you need to create a partition. Enter the DN of the service:

🛐 Active Directory Lightweight Directory Services Setup Wizard	×
Application Directory Partition An application directory partition stores application-specific data.	
Do you want to create an application directory partition for this instance of AD LDS?	
 No, do not create an application directory partition Select this option if the application that you plan to install creates an application direct upon installation, or if you plan to create one later. Yes, create an application directory partition Select this option if the application that you plan to install does not create an application directory partition upon installation. A valid partition name is any distinguished name that not already exist in this instance. Example distinguished name: CN=Partition 1,DC=Woodgrove,DC=COM 	nn at does
CN=keyserver,DC=w32demo,DC=g10code,DC=de	
< Back Next > Cancel	lelp
	ioip

 Click [Next]. The next dialog allows to change the location of the LDS files; in general you will use the defaults:

The Active Directory Lightweight Directory Services Setup Wizard X
File 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\keyserver\data Browse
Data recovery files:
C:\Program Files\Microsoft ADAM\keyserver\data Browse
< Back Next > Cancel Help

• Click [Next]. In the next dialog select the account under which the the service will run. Use the [Browse]-button to select the *"ldsadmin"* account:

Active Directory Light	tweight Directory Services Setup Wizard X		
Service Account Sele AD LDS performs op you select.	ection erations using the permissions associated with the account		
Set up AD LDS to perform operations using the permissions associated with the following account.			
 Network service acco 	unt		
AD LDS has the permi	ssions of the default Windows service account.		
This account: AD LDS service has the permissions of the selected account.			
Usemame:	😰 w32demoVdsadmin 🗸 Browse		
Password:	•••••		
	< Back Next > Cancel Help		

Click [Next]. You now need to specify an account to administer the LDS instance; obviously we
use the "Idsadmin" account:

TActive Directory Lightweight Directory Services Setup Wizard X
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: WIN-WICHMANN1\g10code
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 of 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:
ldsadmin@w32demo.g10code.de Browse
< Back Next > Cancel Help

• Click [Next]. Check all boxes to import the usual schemes:

Active Directory Lightweight Direc	tory Services Setup Wizard	×
Importing LDIF Files You can import data from Lightweig your AD LDS application directory	ght Directory Interchange Format (LDIF) files into partition.	
To configure the AD LDS service in a s below.	pecific way, import one or more of the LDIF files listed	
LDIF file name	Description ^]
MS-AdamSyncMetadata.LDF MS-ADLDS-DisplaySpecifiers.L MS-AZMan.LDF MS-InetOroPerson.LDF	ADAMSync metadata schema extension. Required fc AD LDS Display specifiers schema and display specif AD LDS schema extensions for AzMan. AD LDS inetOrgPerson, user and related classes	
MS-Membership Transitive.LDF	AD LDS memberhsip transitive.	
MS-Parent Distname.LDF	AD LDS parent dist name. AD LDS ReplValueMetaDataExt.	
<	>	
< Ba	ick Next > Cancel Help	

• Click [Next] to view a summary of the configuration options:

Active Directory Lightweight Directory Services Setup Wizard	×
Ready to Install The AD LDS Setup Wizard is ready to install AD LDS with the following configuration.	
Before continuing, review and confirm your selections.	
Selections:	
Install a unique instance of AD LDS.	^
Instance name: keyserver Computers will connect to this instance of AD LDS using the following ports: LDAP port: 389 SSL port: 636	
AD LDS replication will use Negotiate authentication.	
Store AD LDS data files in the following location:	~
To change your selections, click Back. To install AD LDS, click Next.	
< Back Next > Cancel	Help

• Click [Next] to start the installation. You will be asked to enter the credentials for the administrative account for this LDS. For us this is the *"Idsadmin"*:

Active Directory Lightweight Directory Se	ervices Setup Wizard X
Installing AD LDS The AD LDS Setup Wizard is installing AD	LDS.
Installing AD LDS	
	Active Directory Lightweight Direct ? X
Please wait while the wizard completes the ✓ 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.
	Username: 🙍 w32demo\dsadmin 🗸
< Back	Password:
	OK Cancel

 That's it. You now have a running LDS instance which we extend in the next step to host keys for GnuPG.

1.1 Setting the LDS up as Keyserver

- Logout as Administrator of the local machine and login as "Idsadmin".
- Download these files:

https://gnupg.org/misc/gnupg-ldap-ad-schema-v1.ldif

https://gnupg.org/misc/gnupg-ldap-ad-init-v1.ldif

• Open a command prompt and enter as one line:

```
ldifde -i -s localhost -f gnupg-ldap-ad-schema-v1.ldif
-c "DC=EXAMPLEDC" "#configurationNamingContext"
```

Then enter as one line:

```
ldifde -i -s localhost -f gnupg-ldap-ad-init-v1.ldif
-c "DC=EXAMPLEDC" "CN=keyserver,DC=w32demo,DC=g10code,DC=de"
```

 Here you need to replace the last part with the keyserver DN you specified during installation. If you do not use the default port (ie. 389) for your LDS installation, but, say 11371, you need to use localhost:11371 for the -s option. If everything works you should see this on your command window:



 That's all. If you want to test this and GnuPG is also installed on this machine you may run this (as always on a single line):

```
gpg --keyserver ldap://localhost/???gpgNtds=1 --batch
--locate-key info@gnupg.com
```

which imports a public key. Take the fingerprint of that key and run:

gpg --keyserver ldap://localhost/???gpgNtds=1 --batch
--send CBAEDE4E5746B3A3A27C4C696004F15E7DE1AC76

to send this key to your new keyserver.

To test whether you can retrieve this key use:

gpg --keyserver ldap://localhost/???gpgNtds=1 --batch
--search-keys info@gnupg.com

Command Prompt	—		×
<pre>C:\Users\ldsadmin>gpgkeyserver ldap://localhost/???gpgntds=1batchlocate-keys info@gnupg.com pub rsa2048 2018-12-10 [SC] [expires: 2024-06-27] CBAEDE4E5746B3A3A27C4C696004F15E7DE1AC76 uid [unknown] info@gnupg.com sub rsa2048 2018-12-10 [E] sub ed25519 2018-12-10 [S] sub brainpoolP256r1 2021-06-28 [E] sub brainpoolP256r1 2021-06-28 [S]</pre>			^
C:\Users\ldsadmin>gpgkeyserver ldap://localhost/????gpgntds=1batchsend-key CBAEDE4E5746B3A3A27C4C AC76 gpg: sending key 6004F15E7DE1AC76 to ldap://localhost/????gpgntds=1	696004	4F15E7(DE1
<pre>C:\Users\ldsadmin>gpgkeyserver ldap://localhost/????gpgntds=1batchsearch-keys info@gnupg.com (1) info@gnupg.com 256 bit RSA key 6004F15E7DE1AC76, created: 2018-12-10, expires: 2024-06-27 Keys 1-1 of 1 for "info@gnupg.com". gpg: Sorry, we are in batchmode - can't get input</pre>			
C:\Users\ldsadmin>			

 If you see information about the key everything is fine (the warning about "batchmode" can be ignored). The final step will assigning of permissions to the LDS so that other users in the domain can access retrieve and send keys. See the next section.

1.2 Assigning Permissions

- We want to allow all domain users to retrieve keys and users from an assigned group to send keys. Surely, this depends on your exact needs but here we describe our standard method.
- Login as "Idsadmin", start ldp, and connect to the localhost:

C:\Users\ldsadmin>ldp									
🔝 Ldp									
Connection	Browse	View	Options	Utilities	Help				
						Connect Server: Port: 389 OK	alhost 9	Connectionless	×

 After you have connected establish a binding using your current user. Use [Connection] > [Bind] from the menu or hit [Ctrl] + [B]:

Bind	×					
User: Password: Domain: Bind type Bind type Bind as currently logged on user Bind with credentials Simple bind Advanced (DIGEST)						
Encrypt traffic after bind						
Advanced Cancel OK						

 To browse the DIT use [View] > [Tree] or hit [Ctrl] + [T]. Just hit hinter on the dialog asking for the Base-DN. Then select the DN for your service and use the context menu to open the dialog for the "Security Descriptor":

Connection Bro	wse View	Options	Utilities	Help				
CN=Configuration, CN={4329FB05-AFB9-4489-BCA5-E675BEF38302} CN=Schema, CN=Configuration, CN={4329FB05-AFB9-4489-BCA5-E675						=g10code,DC=de; Quotas,CN=keyse B:32:AB8153B776		
⊞- CN= Keyserver,	UC-W3	Search Virtual Li	st View	Ctrl+S		demo,DC=g10code Objects,CN=keyse whenChanged: 9/2/202		
		Delete Modify		Ctrl+D Ctrl+M		Expanding base 'CN=keyse		
		Add chile Compare	DN d ≘	Ctrl+R Ctrl+A		Getting 1 entries: Dn: CN=keyserver,DC=w cn: keyserver; distinguishedName: CN		
		Advance	d	> Repl		ication Metadata		
		Copy DN Copy Select all Clear out	l	Ctrl+C Ctrl+N	Secu	rity Descriptor msDs-masteredBy: CN Skeyserver, CN=Se Name, CN=Sites, CN name: keyserver; objectCotecoper CN=CC		

The Access Control Entry opens and add as "Trustee" the value "Authenticated Users" prefixed with your domain name (you may also use the entire DN of that group). Note that in the screenshot below you see "Domänen-Benutzer", which is what you need to use on an German installation of the Active Directory instead of "Authenticated Users". This group has all users (and otehr objects) which are allowed to login to the domain with the exception of the "Guest" and "Anonymous accounts". Give the DN full read access and make it inheritable:

ACE - Access Control Entry X							
Trustee: W32DEMO\Domänen-Benutzer							
ACE type: Allow	O Deny O Audit O Alarm						
Access mask Read property List List object Read permissions	Write property Write DACL Write owner Write SACL	Create child Delete child Delete Delete	Control access				
ACE flags ☑ Inherit ☑ No propagate	Inherited	Success Failure					
Object type:	(none)		~				
Inherited object type:	(none)		~				
		OK	Cancel				

 Next is to expand the DN and open the security descriptor dialog for the DN starting with "CN=GnuPG Keys":

Connection Browse Vi	ew Options Utilities	Help			
CN=Configuration,CN: CN=Schema,CN=Conf CN=keyserver,DC=w32 CN=keyserver,DC=w32 CN=GnuPG Keys,C CN=LostAndFour CN=NTDS Quota: CN=PGPServerInf CN=Roles,CN=ke	={4329FB05-AFB9-4489 iguration, CN={4329FB0 ldemo, DC=g10code, DC N= kovcover DC=w22d Search Virtual List View Delete Modify Modify DN Add child Compare	BCA5-E675BI I5-AFB9-4489- = de Ctrl+S Ctrl+D Ctrl+M Ctrl+R Ctrl+A	EF38302} BCA5-E675 code,DC= de code,DC= ode,DC= code,DC= = de	cn: keyserver; distinguishedName: Cl dSASignature: { V1: F c86df0a0-4342-4 dSCorePropagationDa instanceType: 0x5 = (msDs-masteredBy: Cl Skeyserver,CN=S Name,CN=Sites,C name: keyserver; objectCategory: CN=C BCA5-E675BEF33 objectClass (2): top; c objectClass (2): top; c	
	Advanced	>	Replic	ation Metadata	
	Copy DN		Security Descriptor		
	Copy Select all	Ctrl+C		=g10code,DC=de, Quotas,CN=keyse B:32:AB8153B770 demo,DC=g10cod	
	Clear output	Ctrl+N		Objects, CN=keys	

 Give the same permissions as above and add "Write property" and "Create Child". Now all authenticated users may read from the keuyserver and also update or insert keys. If you want to restrict update and insert capabilities to a dedicated group of users, you can use the permission system to do this.

2 Using GnuPG with an LDS Keyserver

• Since GnuPG version 2.2.26 you can put:

keyserver ldap://mykeyserver.example.org/???gpgNtds=1

into dirmngr.conf and gpg.conf and Windows takes care of authentication.

 GnuPG can also be advised to consult this configured LDS similar to a Web Key Directory. For this put:

```
auto-key-locate local,ntds,wkd
```

into gpg.conf so that a missing key is first looked up on the LDS keyserver before a WKD query is done.