

# Configuring the Lightweight Directory Service service - Part 2

In this second part we will continue the introduction of AD LDS service by exploring some of the usable technologies and how to deploy AD LDS services.

**Network Administration** - In this second part we will continue the AD LDS service by exploring some of the technologies that can be used to plan the deployment process and how to deploy AD LDS services.

## Planning process

Planning to deploy AD LDS can indeed be said to be a trial and error process because Microsoft really doesn't provide much information. If you refer to the general knowledge introduced on TechNet about AD LDS here, you will see a section on hardware and software related issues with the section '*Use performance counters, testing in the lab, data. from existing hardware in a production environment, and pilot roll outs to determine the capacity needs of your server*' means '*Using performance testers, lab tests, data is taken from existing hardware in The production environment and what is available will help you determine the server's capacity needs*'.

So what is Microsoft really saying here? The above statement of Microsoft can be summarized as follows: To deploy AD LDS, you only need to have a server capable of running Windows Server 2008. However, it depends on how AD LDS is being used, which the server needs to support workflow. follow it. Our task is to perform calculations to ensure server hardware ensures sufficient capacity for the job to be done.

The most logical method for AD LDS planning is to know some of the resources that AD LDS consumes and, based on that, the capacity planning efforts for those resources that consume them.

Although Microsoft does not provide many guidelines for AD LDS capacity planning, the process is almost the same as the capacity planning process you use for domain controllers. As you can see, an AD LDS server is very similar to a domain controller. Both AD LDS servers and domain controllers configure directory services nearly equally. Active Directory capacity planning often takes into account the number of users, whereas for AD LDS, it is necessary to anticipate the number of LDAP requests that will be generated for the server. However, both of these planning processes often require you to create a topology and copy creation process.

## Differences between domain controller servers and AD LDS servers

Although domain controller and AD LDS servers have a lot of similarities at the architecture level, they still have some differences. Domain controllers are used to authenticate Windows logon and security policies, which also means that some aspects of domain controller planning will not be applicable to the scheduling process. planning for AD LDS.

One such difference is that AD LDS does not use forest concepts like Active Directory. In an Active Directory environment, a forest is a collection of domains. Although forests are completely independent of each other, they can still be joined together using the common trust.

AD LDS does not use the concept of forests and domains like domain controllers but instead the main structural component used by AD LDS is a service instance. An instance refers to a separate AD LDS partition. Each instance usually has a service name, directory data store, and a separate service description.

Another problem that you probably know is that a domain controller can only serve a specific domain. In contrast, a private server running AD LDS can host multiple instances. That means that an AD LDS server can have multiple directories.

This raises an interesting question. In an Active Directory environment, clients communicate with domain controllers using the Lightweight Directory Access Protocol (LDAP). Like most other protocols, LDAP is designed to use certain ports. For example, LDAP often uses port 389 for directory queries. If you need to encrypt LDAP communications, port 636 will be used instead. Domain controllers acting as global catalog servers will use ports 3268 and 3269 for related functions. And here you will wonder which port AD LDS will use.

Indeed AD LDS is not interested in implementing any global catalog functions so we can eliminate the use of port 3268 and 3269 from the beginning. However AD LDS uses ports 389 and 636 exactly as a domain controller uses.

So what happens if a server is hosting multiple AD LDS instances? Typically, the first instance created will be assigned using ports 389 and 636. When the second instance is created, Windows will see these ports being used and start scanning other unused ports starting from port 50,000. Assuming that port 50,000 is available then it will be used for standard LDAP communication with the second AD LDS instance. Port 50,001 will be used for LDAP communications with SSL encryption with the second AD LDS instance.

If you create a third AD LDS instance on the server, Windows will recognize that ports 389 and 636 are already in use, so it will look for other unused ports starting from 50,000. However, because ports 50,000 and 50,001 are already assigned, the LDAP partition will be assigned to ports 50,002 and 50,003.

## **DNS requests**

Another difference between Active Directory and AD LDS is that, Active Directory is entirely dependent on DNS servers. Without DNS, Active Directory will not work. Meanwhile AD LDS does not require DNS.

In some cases, Active Directory uses DNS as a mechanism to maintain the domain's hierarchical architecture. However, since there is no domain busy architecture associated with AD LDS, DNS for them is not necessary.

## **Install AD LDS service**

Installing AD LDS is really simple. To do this, simply open the *Server Manager* , and then click the *Add Roles* link. Windows will now launch the Add Roles Wizard. Click *Next* to bypass the Welcome screen and you will see a screen showing all available server roles.

Check the *Active Directory Lightweight Directory Service* menu items as shown in Figure A below.

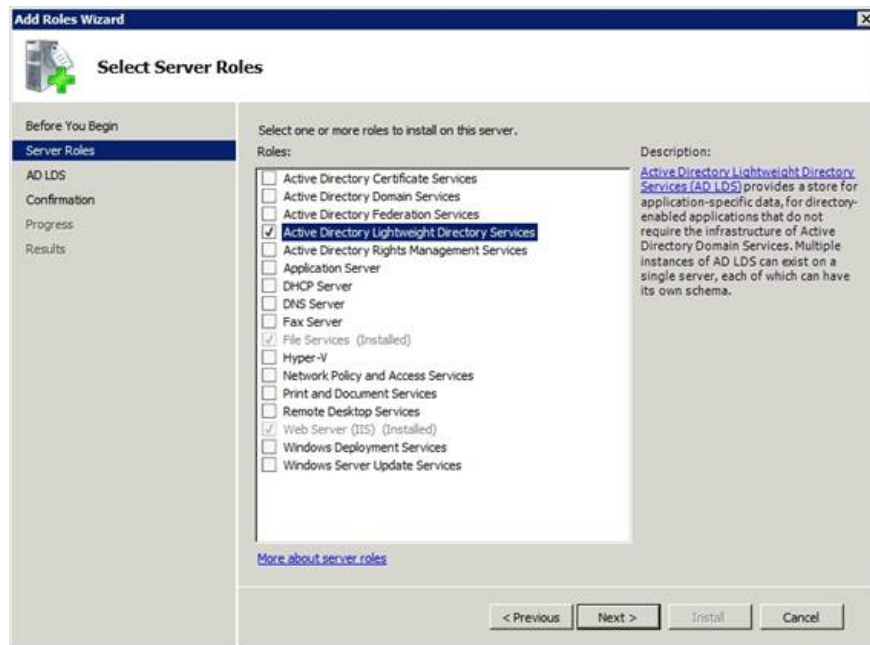


Figure A: AD LDS service

Click *Next* , and you will see a screen that appears to explain what AD LDS is and what it can do. Continue clicking *Next* , Windows will display a confirmation message indicating that the AD LDS server role will be installed. Click the *Install* button to begin this installation process.

The entire installation process only takes about 30 seconds. After finishing the installation process, click the *Close* button to finish. Unlike some Windows 2008 server roles, installing the AD LDS role does not require you to restart the server.

## Conclude

In this article, I have explained some differences between Active Directory and AD LDS. In the third part of this series, we will introduce some basic knowledge in the process of working with AD LDS.

You finished reading the article "**Configuring the Lightweight Directory Service service - Part 2**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.