

Configuring the Lightweight Directory Service service - Part 1

In this article series, I will show you how and how to use the Lightweight Directory Service services.



Network Administration –In this series, we will cover how and how to use the Lightweight Directory Service services.

The Lightweight Directory Service is useful for situations where applications need to access a directory service, but you don't want to risk compromising your Active Directory database. Because of this usefulness, I want to show you a series of articles about Lightweight Directory Service services, specifically about how and how to use it.

When Microsoft introduced Active Directory in Windows 2000, users soon realized that the Active Directory was not just a centralized database, but could be used for many other purposes before. is intended to arrive.

Soon, almost all software vendors designed their software to integrate Active Directory. Many such applications have stored configuration information in Active Directory, some even consider Active Directory as an alternative database for SQL databases and save all real application data into the database. Active Directory database.

Today, most third-party software publishers use a less dependent method of communicating with Active Directory. Many applications still read Active Directory data, but not nearly all save data to Active Directory like a few years ago.

Although software publishers may not use Active Directory for the scope they have done, Active Directory authentication is still very useful in supporting a number of other applications. To explain this, we can see immediately that Microsoft still designs many of their server applications with very high levels of Active Directory integration. Exchange Server 2007 and Exchange Server 2010 are examples, designed in such a way that all server configuration information is stored in Active Directory instead of being stored locally on a server. The advantage of this method is that it is possible to reconstruct a faulty server immediately.

For example, you have a serious hard drive error on the Exchange 2010 server that is hosting the Hub Transport Server Role. Since Exchange stores its configuration information in Active Directory, you do not need to restore a backup to fix the problem, but instead do the repair by resetting the computer account for the server with internal errors. Active Directory. Then install Windows and application service packs into the new server. Next, assign that server a name similar to the server name that was used previously and join this new server to Active Directory. Since the Active Directory computer account has been reset, the new server can fully use it.

From here, fixing the problem becomes as simple as running the Exchange Server Setup program and using a special command switch. The Setup program will need the necessary binary binaries and then configure the server according to the configuration information available in Active Directory. The new server can be put into service less than an hour later without having to restore a backup.

Our view is that Active Directory is very useful for application support, but many software publishers are not willing to use it for the scope that Microsoft can manage because of a drawback in scalability. Active Directory schema.

Another reason why you don't see many software publishers storing data in Active Directory is replication. In general, any data stored in Active Directory will be replicated to all domain controllers in the domain (maybe even all domain controllers in the forest). So if an application stores a large amount of data in Active Directory, this data can affect the speed of the replication process - especially if there is a frequent change.

Despite these difficulties, we still have a way to take advantage of Active Directory integration without affecting our Active Directory database. Windows Server 2008 and Windows Server 2008 R2 both have a service called Active Directory Lightweight Directory Service or AD LDS for short. There is also a similar service that exists inside Windows Server 2003 but is known as Active Directory Application Mode (ADAM).

AD LDS provides you with a similar environment but completely separate from Active Directory. AD LDS is a standalone service that does not depend on the Active Directory Directory Service. In fact, people often deploy AD LDS in environments where there are no Active Directory domains.

A perfect example for this is Microsoft Exchange Server. Previously we knew that Exchange Server 2007 and 2010 were both designed to store all their configuration information in the Active Directory database. There is an exception, though, in this case.

Exchange Server defines a series of roles (roles) to manage Exchange Server servers and the tasks that servers perform. However, there is a server role designed to store server configuration in Active Directory.

The server role does not use the Active Directory known as the Edge Transport Server Role. Edge Transport Server is designed to reside in the network ring and keep other Exchange Server servers from being exposed directly to the Internet.

Because the Edge Transport Server is exposed to Internet dangers, it is a security risk to become a member of the Active Directory domain. If someone can compromise the Edge Transport Server, they can also use it to exploit information about Active Directory.

To avoid that, the Edge Transport Server does not need to be a domain member, nor does it hold any other Exchange Server roles. However, because the Edge Transport Server requires access to a small amount of Active Directory information to perform its work. Rather than providing the server with direct access to the Active Directory, Microsoft has designed the Edge Transport Server role to use AD LDS.

One of the backend Exchange Server will read this required information from Active Directory and send information to the AD LDS partition on the Edge Transport Server. That way, the Edge Transport Server will have the information it needs without having to access the Active Directory. However, the Edge Transport Server can also store its own configuration information in the AD LDS partition as if the Exchange Server roles still store configuration information in Active Directory.

Conclude

So far we have shown you what AD LDS is and what it is used for, however, because I want to focus on using this service in each separate organization, part 2 of the series. This article will continue to provide more information about hardware and software requirements for using AD LDS.

You finished reading the article "**Configuring the Lightweight Directory Service service - Part 1**" 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.