附录 A　AD DS 与防火墙

如果两台域控制器之间，或域控制器与成员计算机之间，被防火墙隔开的话，则如何让AD DS数据库复制、用户身份验证、网络资源访问等行为穿越防火墙的阻隔，便成为系统管理员必须了解的重要课题。

- AD DS相关的端口
- 限制动态RPC端口的使用范围
- IPSec与VPN端口

A.1 AD DS相关的端口

不同的网络服务会使用到不同的TCP或UDP端口（port），如果防火墙没有开放相关端口的话，将造成这些服务无法正常运行。我们先在表 A-1-1中列出AD DS （Active Directory域服务）一些相关的服务与其所占用的TCP/UDP端口号码，然后再说明这些服务的使用场合。

表A-1-1

服务	TCP端口	UDP端口
RPC Endpoint Mapper	135	
Kerberos	88	88
LDAP	389	389
LDAPS （LDAP over SSL）	636	636
LDAP GC （LDAP Global Catalog）	3268	
LDAPS GC （LDAP Global Catalog over SSL）	3269	
SMB（Microsoft CIFS）	445	
DNS	53	53
Network Time Protocol （NTP）		123
AD DS数据库复制、文件复制服务（FRS）、分布式文件系统（DFS）等服务	使用动态端口：需要限制端口范围或更改为静态端口	
NetBIOS Name Service		137
NetBIOS Datagram Service		138
NetBIOS Session Service	139	

附注

如果为了降低开放端口的复杂性、确保所有与AD DS有关的工作都能够正常运行的话，可以将以下所提到的端口全部开放。

A.1.1 将客户端计算机加入域、用户登录时会用到的端口

将客户端计算机加入域、用户登录时会用到以下的服务，因此如果客户端计算机与域控制器之间被防火墙隔开的话，请在防火墙开放以下的端口：

- Microsoft CIFS：445/TCP
- Kerberos：88/TCP、88/UDP
- DNS：53/TCP、53/UDP
- LDAP：389/TCP、389/UDP

- Netlogon服务：NetBIOS Name Service（137/UDP）/NetBIOS Datagram Service（138/UDP）/NetBIOS Session Service（139/TCP）与SMB（445/ TCP）。

A.1.2 计算机登录时会用到的端口

计算机登录到域控制器时会用到以下的服务，因此如果域成员计算机与域控制器之间是被防火墙隔开的话，请在防火墙开放以下的端口：

- Microsoft CIFS：445/TCP
- Kerberos：88/TCP、88/UDP
- LDAP：389/UDP
- DNS：53/TCP、53/UDP

A.1.3 建立域信任时会用到的端口

位于不同林的域之间在建立快捷方式信任、外部信任等**显性的信任**（explicit trust）关系时，会用到以下的服务，因此如果这两个域的域控制器之间是被防火墙隔开的话，请在防火墙开放以下的端口：

- Microsoft CIFS：445/TCP
- Kerberos：88/TCP、88/UDP
- LDAP：389/TCP、389/UDP
- LDAPS：636/TCP（如果使用SSL的话）
- DNS：53/TCP、53/UDP

A.1.4 验证域信任时会用到的端口

不同域的域控制器之间在验证信任关系时会用到以下的服务，因此如果这些域控制器之间是被防火墙隔开的话，请在防火墙开放以下的端口：

- Microsoft CIFS：445/TCP
- Kerberos：88/TCP、88/UDP
- LDAP：389/TCP、389/UDP
- LDAPS：636/TCP（如果使用SSL的话）
- DNS：53/TCP、53/UDP
- Netlogon服务：NetBIOS Name Service（137/UDP）/NetBIOS Datagram Service（138/UDP）/NetBIOS Session Service（139/TCP）与SMB（445/ TCP）。

A.1.5 访问文件资源时会用到的端口

访问文件资源时所使用的服务为SMB（445/TCP）或NetBIOS Name Service（137/UDP）/NetBIOS Datagram Service（138/UDP）/NetBIOS Session Service（139/TCP），因此如果用户的计算机与资源所在的计算机是被防火墙隔开的话，请在防火墙开放这些服务的端口。

A.1.6 执行DNS查询时会用到的端口

如果要通过防火墙来向DNS服务器提出查询请求的话，例如查询域控制器的IP地址，就需要开放DNS服务的端口：53/TCP与53/UDP。

A.1.7 执行AD DS数据库复制时会用到的端口

两台域控制器之间在进行AD DS数据库复制时会用到以下服务，因此如果这两台域控制器之间被防火墙隔开的话，请在防火墙开放以下端口：

- AD DS数据库复制
  它不是使用静态RPC（Remote Procedure Call）端口，而是使用动态RPC端口（其范围为 49152 ~ 65535之间），此时我们要如何来开放端口呢？还好动态RPC端口可以被限制在一段较小的范围内（参见**限制所有服务的动态RPC端口范围**的说明），因此我们只要在防火墙开放这一小段范围的TCP端口即可。
  也可以自行指定一个静态的端口，参见**限制AD DS数据库复制使用指定的静态端口**的说明。
- RPC Endpoint Mapper：135/TCP
  使用动态RPC端口时，需要搭配RPC Endpoint Mapper服务，因此请在防火墙开放此服务的端口。
- Kerberos：88/TCP、88/UDP
- LDAP：389/TCP、389/UDP
- LDAPS：636/TCP（如果使用SSL的话）
- DNS：53/TCP、53/UDP
- Microsoft CIFS：445/TCP

A.1.8 文件复制服务（FRS）会用到的端口

如果域功能级别是Windows Server 2008以下的话，则同一个域的域控制器之间在复制SYSVOL文件夹时，会使用FRS（File Replication Service）。FRS也是采用动态RPC端口，因此如果将动态RPC端口限制在一段较小范围内的话（参见**限制所有服务的动态RPC端口范围**

的说明），则我们只要在防火墙开放这段范围的TCP端口即可。但是使用动态RPC端口时，需要搭配RPC Endpoint Mapper服务，因此请在防火墙开放RPC Endpoint Mapper：135/TCP。

也可以自行指定一个静态的端口，参见**限制FRS使用指定的静态端口**的说明。

A.1.9 分布式文件系统（DFS）会用到的端口

如果域功能级别为Windows Server 2008（含）以上的话，则Windows Server 2008（含）以上的域控制器之间在复制SYSVOL文件夹时需利用**DFS复制服务**（DFS Replication Service），如果这些域控制器之间是被防火墙隔开的话，请在防火墙开放以下的端口：

- LDAP：389/TCP、389/UDP
- Microsoft CIFS：445/TCP
- NetBIOS Datagram Service：138/UDP
- NetBIOS Session Service：139/TCP
- Distributed File System（DFS）
  DFS也是采用动态RPC端口，如果将动态RPC端口限制在一段较小范围内的话（参见**限制所有服务的动态RPC端口范围**的说明），则只要在防火墙开放这段范围的TCP端口即可。
  也可以自行指定一个静态的端口，参见**限制DFS使用指定的静态端口**的说明。
- RPC Endpoint Mapper：135/TCP
  使用动态RPC端口时，需要搭配RPC Endpoint Mapper服务，因此请在防火墙开放此服务的端口。

A.1.10 其他可能需要开放的端口

- LDAP GC、LDAPSGC：3268/TCP、3269/TCP（如果使用SSL的话）
  假设用户登录时，负责验证用户身份的域控制器需要通过防火墙来向**全局编录服务器**查询用户所隶属的通用组数据时，就需要在防火墙开放端口3268或3269。
  又例如Microsoft Exchange Server需要访问位于防火墙另外一端的**全局编录服务器**的话，您也需要开放端口3268或3269。
- Network Time Protocol（NTP）:123/UDP
  它负责时间的同步，参见第10章关于**PDC模拟器操作主机**的说明。
- NetBIOS的相关服务：137/UDP、138/UDP、139/TCP
  开放这些端口，以便通过防火墙来使用NetBIOS服务，例如支持旧客户端来登录、浏览网上邻居等。

A.2 限制动态RPC端口的使用范围

动态RPC端口是如何工作的呢？以Microsoft Office Outlook（MAPI客户端）与Microsoft Exchange Server之间的通信为例来说：客户端Outlook先连接Exchange Server的RPC Endpoint Mapper（RPC Locator Services，TCP 端口135）、RPC Endpoint Mapper再将Exchange Server所使用的端口（动态范围在49152~65535之间）通知客户端、客户端Outlook再通过此端口来连接Exchange Server。

AD DS数据库的复制、Outlook与Exchange Server之间的通信、文件复制服务（File Replication Service，FRS）、分布式文件系统（Distributed File System，DFS）等默认都是使用动态RPC端口，也就是没有固定的端口，这将造成在防火墙配置上的问题，还好动态RPC端口可以被限制在一段较小的范围内，因此只要在防火墙开放这段范围的端口即可。

A.2.1 限制所有服务的动态RPC端口范围

以下说明如何将计算机所使用的动态RPC端口限制在指定的范围内。假设不论是使用IPv4或IPv6，都要将其限制在从8000起开始，总共1000个端口号（端口号码最大为65535）。

打开Windows PowerShell窗口（或**命令提示符**）、执行以下命令（参见图A-2-1）：

```
netsh int ipv4 set dynamicport tcp start = 8000 num = 1000
netsh int ipv4 set dynamicport udp start = 8000 num = 1000
netsh int ipv6 set dynamicport tcp start = 8000 num = 1000
netsh int ipv6 set dynamicport udp start = 8000 num = 1000
```

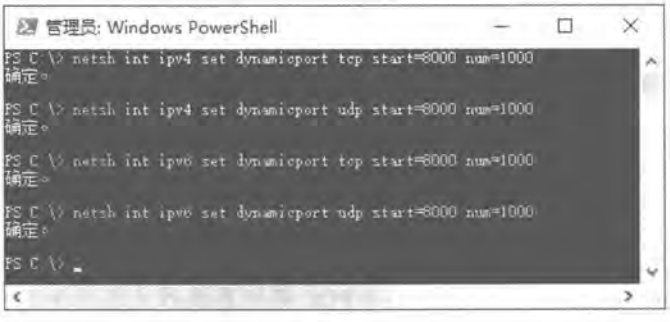

图 A-2-1

如果要检查当前动态RPC端口范围的话，请执行以下命令：

```
netsh int ipv4 show dynamicport tcp
netsh int ipv4 show dynamicport udp
netsh int ipv6 show dynamicport tcp
```

```
netsh int ipv6 show dynamicport udp
```

如图A-2-2所示为显示ipv4、tcp通信协议的动态RPC端口范围。

图 A-2-2

如果是修改域控制器的上述键值的话，请随便找一台域成员计算机来与这台域控制器通信，然后在这台域控制器上打开Windows PowerShell窗口、执行**netstat–n**命令来查看此域控制器当前所使用的端口，此时应该可以看到某些服务所使用的端口是在我们所设置的从8000开始，如图A-2-3所示（包含IPv4与IPv6）。

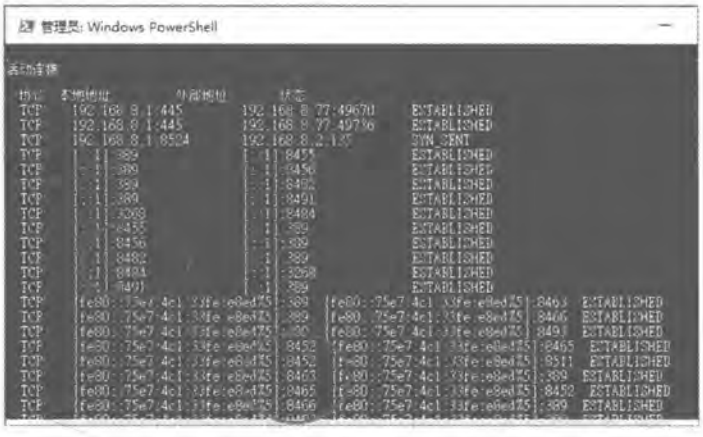

图 A-2-3

A.2.2 限制AD DS数据库复制使用指定的静态端口

域控制器执行AD DS数据库复制工作时，默认是使用动态RPC端口，但是我们也可以自行指定一个静态的端口。请到域控制器上执行注册表编辑器REGEDIT.EXE，然后通过以下路径来设置：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters
```

在上述路径之下新建一个如表A-2-1所示的数值，图A-2-4为完成后的界面，图中我们将端口号码设置为56789（十进制），注意此端口不能与其他服务所使用的端口相同。

表A-2-1

数值名称	数据类型	数值
TCP/IP Port	REG_DWORD （DWORD（32-位）值）	自定义，例如56789

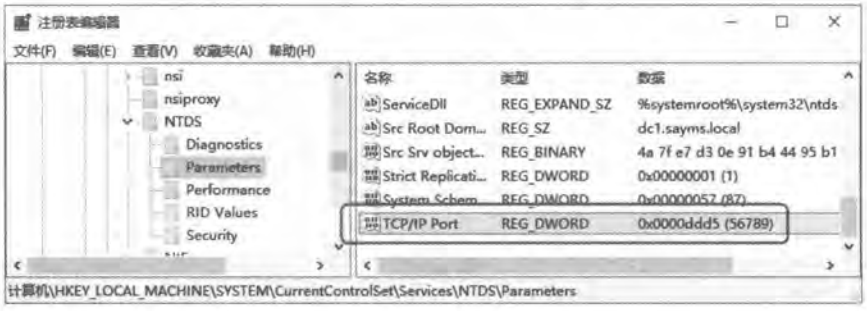

图 A-2-4

完成后重新启动，以后这台域控制器在执行AD DS数据库复制时所使用到的端口将会是56789（包含IPv4与IPv6）。可以先利用**Active Directory站点和服务**来手动与其他域控制器之间执行AD DS数据库复制的工作，然后在这台域控制器上打开Windows PowerShell窗口、执行**netstat–n**命令来查看其所使用的端口。如图A-2-5所示可看到它使用到我们所指定的端口56789（图中为IPv4，往下翻还可看到IPv6）。

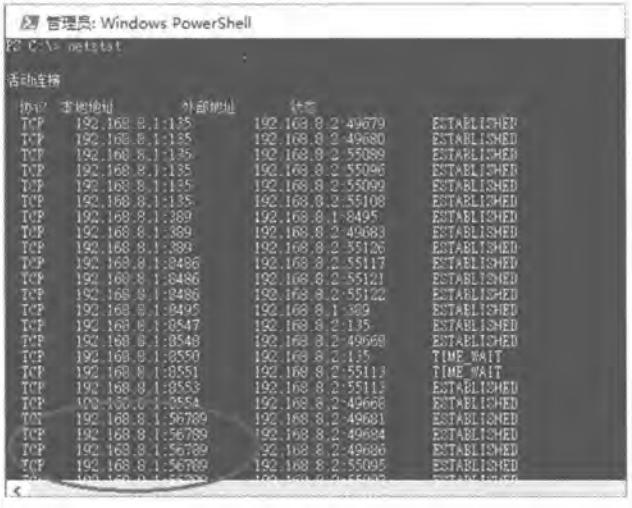

图 A-2-5

A.2.3 限制FRS使用指定的静态端口

如果域功能级别是Windows Server 2008以下的话，则同一个域的域控制器之间在复制SYSVOL文件夹时，会使用FRS（File Replication Service）。FRS默认也是采用动态RPC端口，但是我们也可以自行指定一个静态的端口。请到域控制器上执行注册表编辑器

REGEDIT.EXE，然后通过以下路径来设置：

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTFRS\Parameters
```

请在上述路径之下新建一个如表A-2-2所示的数值，表中我们将端口号码设置为45678（十进制），注意此端口不能与其他服务所使用的端口相同。完成后重新启动。以后这台域控制器的FRS服务所使用的端口将会是45678。

表A-2-2

数值名称	数据类型	数值
RPC TCP/IP Port Assignment	REG_DWORD	自定义，例如45678

A.2.4 限制DFS使用指定的静态端口

如果域功能级别为Windows Server 2008（含）以上的话，则Windows Server 2008 （含）以上的域控制器之间在复制SYSVOL文件夹时需要利用**DFS复制服务**，而它也是采用动态RPC端口，但是我们可以将其固定到一个静态的端口。请到域控制器上打开Windows PowerShell窗口，然后执行以下命令（如图A-2-6所示，图中假设将端口固定到34567）：

```
DFSRDIAGStaticRPC  /Port:34567
```

注意此端口不能与其他服务所使用的端口相同。如果无法执行此程序的话，请先安装**DFS管理工具**（通过**服务器管理器**➲添加角色和功能➲在**选择功能**界面展开**远程服务器管理工具**➲**角色管理工具**➲**文件服务工具**➲……）。完成后，重新启动这台域控制器，以后其**DFS复制服务**所使用的端口将会是34567。

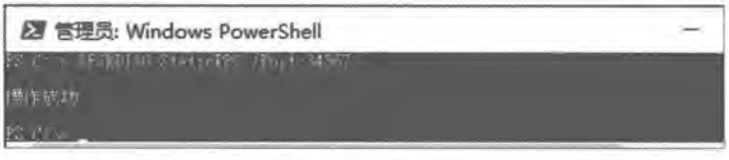

图 A-2-6

可以先利用**Active Directory站点和服务**来手动与其他域控制器之间执行AD DS复制工作（它也会复制SYSVOL文件夹），然后在这台域控制器上打开Windows PowerShell窗口、执行**netstat–n**命令来查看其所使用的端口。如图A-2-7所示可看到它使用到我们所指定的连接34567。

图 A-2-7

也可以在**WindowsPowerSehell**窗口下，执行以下命令来达到相同目的（如图A-2-8所示，图中假设将端口固定到34567）：

```
Set-DfsrServiceConfiguration  -RPCPort  34567
```

完成后重新启动此域控制器，以后其**DFS复制服务**所使用的端口将会是34567。

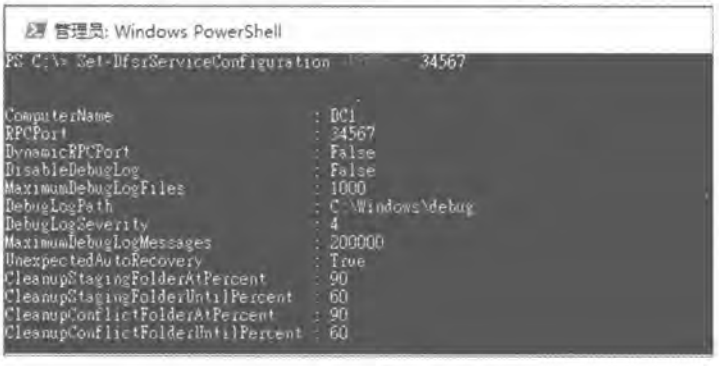

图 A-2-8

A.3 IPSec与VPN端口

如果域控制器之间，或域控制器与成员计算机之间，不但被防火墙隔开，而且所传输的数据还经过IPSec的处理，或经过PPTP、L2TP等VPN安全传输通道来传送的话，则还有一些通信协议或端口需要在防火墙开放。

A.3.1 IPSec所使用的通信协议与端口

IPSec除了用到UDP通信协议外，还会用到ESP与AH通信协议，因此我们需要在防火墙

开放相关的UDP端口与ESP、AH通信协议：

- Encapsulation Security Payload（ESP）：通信协议号为50
- Authentication Header（AH）：通信协议号为51
- Internet Key Exchange（IKE）：所使用的是UDP端口号500

A.3.2 PPTP VPN所使用的通信协议与端口

除了TCP通信协议外，PPTP VPN还会使用到GRE通信协议：

- General Routing Encapsulation（GRE）：通信协议号为47
- PPTP：所使用的是TCP端口号1723

A.3.3 L2TP/IPSec所使用的通信协议与端口

除了UDP通信协议外，L2TP/IPSec还会用到ESP通信协议：

- Encapsulation Security Payload（ESP）：通信协议号为50
- Internet Key Exchange（IKE）：所使用的是UDP端口号500
- NAT-T：所使用的是UDP端口号码4500，它让IPSec可以穿越NAT

附注

虽然L2TP/IPSec还会使用到UDP端口1701，但它是被封装在IPSec数据包内，因此不需要在防火墙开放此端口。