Active Directory and Active Directory Domain Services Port Requirements

https://technet.microsoft.com/en-us/library/dd772723%28v=WS.10%29.aspx

Applies To: Windows Server 2000, Windows Server 2003, Windows Server 2003 R2, Windows Server 2003 with SP1, Windows Server 2003 with SP2, Windows Server 2008, Windows Server 2008 Foundation, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Vista

This guide contains port requirements for various Active Directory® and Active Directory Domain Services (AD DS) components. Both writable domain controllers and read-only domain controllers (RODCs) have the same port requirements. For more information about RODCs, see Designing RODCs in the Perimeter Network.

Default dynamic port range

In a domain that consists of Windows Server® 2003–based domain controllers, the default dynamic port range is 1025 through 5000. Windows Server 2008 R2 and Windows Server 2008, in compliance with Internet Assigned Numbers Authority (IANA) recommendations, increased the dynamic port range for connections. The new default start port is 49152, and the new default end port is 65535. Therefore, you must increase the remote procedure call (RPC) port range in your firewalls. If you have a mixed domain environment that includes a Windows Server 2008 R2 and Windows Server 2008 server and Windows Server 2003, allow traffic through ports 1025 through 5000 and 49152 through 65535.

When you see “TCP Dynamic” in the **Protocol and Port** column in the following table, it refers to ports 1025 through 5000, the default port range for Windows Server 2003, and ports 49152 through 65535, the default port range beginning with Windows Server 2008.

Note

For more information about the change in the dynamic port range beginning in Windows Server 2008, see article 929851 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkId=153117).
You can find additional information about this change on the Ask the Directory Services Team blog. See the blog entry Dynamic Client Ports in Windows Server 2008 and Windows Vista (http://go.microsoft.com/fwlink/?LinkId=153113).

Restricting RPC to a specific port

RPC traffic is used over a dynamic port range as described in the previous section, “Default dynamic port range.” To restrict RPC traffic to a specific port, see article 224196 in the Microsoft Knowledge Base (http://go.microsoft.com/fwlink/?LinkID=133489).

Communication to Domain Controllers

The following table lists the port requirements for establishing DC to DC communication in all versions of Windows Sever beginning with Windows Server 2003.

Additional ports are required for communication between a read-only domain controller (RODC) and a writeable DC.

Protocol and Port	AD and AD DS Usage	Type of traffic
TCP and UDP 389	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP
TCP 636	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP SSL
TCP 3268	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP GC

TCP 3269	Directory, Replication, User and Computer Authentication, Group Policy, Trusts	LDAP GC SSL
TCP and UDP 88	User and Computer Authentication, Forest Level Trusts	Kerberos
TCP and UDP 53	User and Computer Authentication, Name Resolution, Trusts	DNS
TCP and UDP 445	Replication, User and Computer Authentication, Group Policy, Trusts	SMB,CIFS,SMB2, DFSN, LSARPC, NbtSS, NetLogonR, SamR, SrvSvc
TCP 25	Replication	SMTP
TCP 135	Replication	RPC, EPM
TCP Dynamic	Replication, User and Computer Authentication, Group Policy, Trusts	RPC, DCOM, EPM, DRSUAPI, NetLogonR, SamR, FRS
TCP 5722	File Replication	RPC, DFSR (SYSVOL)
UDP 123	Windows Time, Trusts	Windows Time
TCP and UDP 464	Replication, User and Computer Authentication, Trusts	Kerberos change/set password
UDP Dynamic	Group Policy	DCOM, RPC, EPM
UDP 138	DFS, Group Policy	DFSN, NetLogon, NetBIOS Datagram Service
TCP 9389	AD DS Web Services	SOAP
UDP 67 and UDP 2535	DHCP **Note** DHCP is not a core AD DS service but it is often present in many AD DS deployments.	DHCP, MADCAP
UDP 137	User and Computer Authentication,	NetLogon, NetBIOS Name Resolution
TCP 139	User and Computer Authentication, Replication	DFSN, NetBIOS Session Service, NetLogon