Active Directory Port and Protocol Information

Port Information

http://msdn.microsoft.com/en-us/library/hh872062.aspx

Protocol name	Description	Short name
Active Directory extensions for Lightweight Directory Access Protocol (LDAP), versions 2 and 3	Active Directory is a server for LDAP. [MS-ADTS] section 3.1.1.3 specifies the extensions and variations of LDAP that are supported by Active Directory. **Note** In a reference to LDAP without a version number, LDAP refers to both versions 2 and 3.	[MS-ADTS] section3.1.1.3.1
Directory Replication Service Remote Protocol (drsuapi) - Replication	The Directory Replication Service (DRS) Remote Protocol. This protocol includes the drsuapi and dsaop RPC interfaces. Methods on these interfaces provide replication of directory information among the domain controllers of an AD DS domain. Methods on these interfaces also provide a variety of functionality to clients, such as converting names between formats and retrieving information about AD DS domain controllers. This protocol also supports DC cloning operations.<3>	[MS-DRSR]
SMTP Replication Protocol Extensions	The Directory Replication Service (DRS) Protocol Extensions for SMTP. This protocol provides Simple Mail Transfer Protocol (SMTP) transport of replication information as an alternative to RPC.	[MS-SRPL]
Directory Services Setup Remote Protocol	The Directory Services Setup Remote Protocol, as defined in [MS-DSSP]. This protocol can be used to retrieve information about the state of a computer in a domain or a non-domain workgroup.	[MS-DSSP]

The protocols in the following table enable account maintenance when the Active Directory system is operating in AD DS mode. This includes the creation, modification, retrieval, and deletion of users and groups.

Protocol name	Description	Short name
Security Account Manager (SAM) Remote Protocol (Client-to-Server)	The Security Account Manager (SAM) Remote Protocol. Clients can use this protocol to perform account maintenance, for example, to create and delete accounts. The capabilities of this protocol are a subset of the capabilities of LDAP.	[MS-SAMR]
Security Account Manager (SAM) Remote Protocol (Server-to-Server)	The Security Account Manager (SAM) Remote Protocol. Domain controllers (DCs) use this protocol to forward time-critical database changes to the primary domain controller (PDC), and to forward time-critical database changes from a read-only domain controller (RODC) to a writable NC replica within the same domain outside the normal replication protocol. This protocol is used only between Active Directory servers in the same domain.	[MS-SAMS]

The protocols in the following table allow clients to retrieve security policy information and translate security identifiers (SIDs) that identity security principals, such as users, to human-readable names.

Protocol name	Description	Short name
Local Security Authority (Domain Policy) Remote Protocol	The Local Security Authority (Domain Policy) Remote Protocol. Clients can use this protocol to retrieve security policy information.	[MS-LSAD]
Local Security Authority (Translation Methods) Remote Protocol	The Local Security Authority (Translation Methods) Remote Protocol. Clients can use this protocol to translate security identifiers (SIDs) of security principals to human-readable names, and vice versa.	[MS-LSAT]

The protocols in the following table enable Web services for the Active Directory system that allow access to the directory tree and the management of Active Directory account information and topologies.

Protocol name	Description	Short name
Active Directory Web Services Custom Action Protocol	The Active Directory Web Services Custom Action Protocol. It is a SOAP-based Web Services protocol for managing account and topology information.	[MS-ADCAP]

WS-Transfer: Identity Management Operations for Directory Access Extensions	WS-Transfer: Identity Management Operations for Directory Access Extensions. This is a set of protocol extensions to WS-Transfer that allows directory objects to be manipulated at a finer level of granularity than unextended WS-Transfer.	[MS-WSTIM]
WS-Enumeration	The WS-Enumeration protocol. This protocol allows directory objects to be queried by using a SOAP-based Web Services protocol.	[WSENUM]
WS-Transfer	The WS-Transfer protocol. This protocol allows directory objects to be created, removed, modified, and read by using a SOAP-based Web Services protocol.	[WXFR]
WS-Enumeration: Directory Services Protocol Extensions	The WS-Enumeration Directory Services Protocol Extensions. This is a set of protocol extensions to WS-Enumeration that, among other things, allows a client to request that query results be sorted. It also specifies a query language that is used by clients to specify which directory objects are to be returned from the query.	[MS-WSDS]
WS-Transfer and WS-Enumeration Protocol Extension for Lightweight Directory Access Protocol v3 Controls	WS-Transfer and WS-Enumeration Protocol Extension for Lightweight Directory Access Protocol v3 Controls. This is a protocol extension to WS-Transfer and WS-Enumeration. It permits LDAP extended controls to be attached to operations in the protocols that it extends.	[MS-WSPELD]
Active Directory Web Services: Data Model and Common Elements	The Active Directory Web Services: Data Model and Common Elements. Although not a protocol itself, this defines an XML data model that is shared by the other Web Service protocols and protocol extensions, as well as common protocol elements referenced by the other documents.	[MS-ADDM]

Active Directory Port information

(http://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