|  |  |  |  |
| --- | --- | --- | --- |
| **Service** | **Type** | **Port#** | **Comments** |
| Default Instance | TCP | 1433 | Official IANA socket number for SQL Server which can be changed to anything above 1024. |
| Named Instance | TCP | XXXXX | As and what you assign. The new default start port is 49152 ending at 65535 (from win 6.0) which has changed a from the earlier Win port range of 1025 through 5000. |
| DAC Default Instance | TCP | 1434 | By default, remote connections through DAC are disabled. Ports other than 1434 are used for named instances. |
| SQL Browser / SQL Server Resolution Protocol | UDP | 1434 | SQL Server Named instances in default configuration.  Required by Browser Service when using named instances. Because in case of named instances TCP port is dynamic determined when the Database Engine starts.  SQL Server Browser service listens for incoming connections to a named instance and provides the client the TCP port number that corresponds to that named instance. Normally the SQL Server Browser service is started whenever named instances of the Database Engine are used. The SQL Server Browser service does not have to be started if the client is configured to connect to the specific port of the named instance. |
| DTS |  | 3882 | Required for SSIS, uses msdts1 protocol for service type msdts1. A malformed request to port 3882/tcp is known to cause denial of service attacks. |
| SSAS | TCP | 2393, 2394, 2725 | OLAP Services 7.0 used TCP ports 2393 & 2394. Though Ms has reserved UDP ports 2393 & 2394 those are not used by OLAP Services. Analysis Services uses TCP port 2725. For backward compatibility, Analysis Services uses TCP ports 2393 and 2394 when connected with an OLAP Services 7.0 client. |
| SSAS | TCP | 2383 | Standard port for the default instance of Analysis Services. |
| Browser SSAS | TCP | 2382 | TCP 2382 is needed for an Analysis Services named instance. Client connection requests for a named instance of Analysis Services that do not specify a port number are directed to port 2382, the port on which SQL Server Browser listens. SQL Server Browser then redirects the request to the port that the named instance uses. |
| RDP | TCP | 3389 | Providing the remote desktop to a client or VDI keep your eyes open because the default encryption certificate (RSA pk stored in mstlsapi.dll), is there with widows base install. A Man-in-the-Middle (MITM) attack can intercept the exchange of RDP encryption information. Check here for safety ribbons secure RDP using Transport Layer Security <http://technet.microsoft.com/en-us/library/cc782610%28WS.10%29.aspx>  For 6.0 Network Level Authentication offers much stronger protection <http://blogs.technet.com/askperf/archive/2008/02/16/ws2008-network-level-authentication-and-encryption.aspx> |
| Dynamic Port Range | To comply with Internet Assigned Numbers Authority recommendations, Ms has increased the dynamic client port range for outgoing connections from Win 6.0. New default port range is 49152 – 65535 which was earlier 1025 through 5000. | | |
| Service Broker | TCP | 4022 | As per the conventional configuration used in BOL otherwise there is no default port for Service Broker. |
| SQL Debugger |  | RPC | Transact-SQL debugger includes both server & client components which are installed with instance / client. Uses RPC in case the domain policy requires network communications to be done via IPsec, also add UDP port 4500 and UDP port 500 to the exception list. |
| SSL | TCP | 443 | With HTTP it establishes an encrypted communications channel to help prevent the interception of critical information. |
| HTTP endpoint |  |  | SQL Server instance running over an HTTP endpoint, used for an HTTP connection through a URL. Can be specified when an HTTP endpoint is created. The default is TCP port 80 for CLEAR\_PORT traffic and 443 for SSL\_PORT traffic. |
| HTTPS endpoint | TCP | 443 | Default instance running over an HTTPS endpoint. Used for an HTTPS connection through a URL. HTTPS is an HTTP connection that uses secure sockets layer (SSL). |
| iSCSI |  | 3260, 860 | Doesn’t support teamed NIC. |
| SQL Agent File Copy | 135 | | Agent to copy backup files to the shared folder on the standby server. |
| 137, 138, 139, 445 | | File copy on UNC shares. |
| Transact-SQL debugger | TCP | 135 | The IPsec exception might also be required.  If using Visual Studio, on the Visual Studio host computer, you must also add Devenv.exe to the Exceptions list and open TCP port 135.  If using Management Studio, on the Management Studio host computer, you must also add ssms.exe to the Exceptions list and open TCP port 135. For more information, see [Configuring the Transact-SQL Debugger](http://msdn.microsoft.com/en-us/library/cc646024.aspx) |
| Database Mirroring |  |  | Though BOL examples use TCP port 7022 there is no default port for Database mirroring. It is very important to avoid interrupting an in-use mirroring endpoint, especially in high-safety mode with automatic failover. Firewall configuration must avoid breaking quorum. For details, see [Specifying a Server Network Address (Database Mirroring)](http://msdn.microsoft.com/en-us/library/ms189921.aspx). SELECT name, port FROM sys.tcp\_endpoints. |
| Replication | TCP | 1433 | Replication connections to SQL Server using regular Database Engine ports  Web synchronization and FTP/UNC access for replication snapshot require additional ports to be opened on the firewall. To transfer initial data and schema from one location to another, replication can use FTP (TCP port 21), or sync over HTTP (TCP port 80) or File and Print Sharing (TCP port 137,138, or 139).  For sync over HTTP, replication uses the IIS endpoint (ports for which are configurable but is port 80 by default), but the IIS process connects to the backend SQL Server through the standard ports (1433 for the default instance.  During Web synchronization using FTP, the FTP transfer is between IIS and the SQL Server publisher, not between subscriber and IIS.  For details, see [Configuring Microsoft Internet Security and Acceleration Server for Microsoft SQL Server 2000 Replication over the Internet](http://go.microsoft.com/fwlink/?LinkId=118370). |
| Cluster Service | UDP | 3343 | Cluster services control and manage the cluster database. Like the Heartbeat process - Cluster network driver (Clusnet.sys) performs intra-node communication between each node of the cluster by periodically exchanging sequenced, unicast/multicast UDP datagrams in the cluster. This determines whether all nodes are running correctly & network links are healthy. Generally this does not happens over the public network.  There are cases when the range of random available IP ports that the cluster service uses to initiate communication through RPCs is less than 100 ports and connection to the Cluster Admin fails (refer to [154596](http://support.microsoft.com/kb/154596)(http://support.microsoft.com/kb/154596/ ) ).  135 (RPC) / 3343 (Cluster Network Driver) / 445 SMB / 139 NetBIOS / 5000-5099 (RPC) / 8011-8031 (RPC)   * 135 (RPC endpoint mapper/DCOM), (RPC endpoint mapper over UDP). * 3343 (used by the Cluster Network Driver). * 445 (SMB). * 139 (NetBIOS session service). * For cluster nodes running many services, ports 5000-5099 (or more) might need to be open for remote RPC connectivity to Cluster Administrator. When these ports are closed, event log error 1721 might occur when you connect to a cluster through Cluster Administrator (unless you just type a period in Cluster Administrator). This problem can occur because the Cluster service requires at least 100 ports for communication through remote procedure calls (RPC). The number of ports available to the Cluster service can become too small when other services are using some of the necessary ports. Such services include Windows DNS service, Windows Internet Name Service (WINS), the Microsoft SQL Server service, and others. * If the nodes are separated by a firewall, ports 8011-8031 must be open for internode RPC connectivity. Otherwise, errors in the cluster log will indicate that a "Sponsor" is not available. These errors occur because there are not enough ports available for RPC communication between a node that is trying to join the cluster and a node that can "sponsor" that node. |
| Cluster Admin | UDP | 137 |
| Random Ports | UDP | Check dynamic port range |
| RPC | TCP | 135 |
| Filestream |  |  | 139 y 445. |
| SSIS | TCP | 135 | (DCOM) |
| WMI | TCP | 135 | WMI runs as part of a shared service host with ports assigned through DCOM. WMI might be using TCP port 135. |
| IPsec traffic | UDP | 500 & 4500 | Should be set to allow ISAKMP traffic to be forwarded for both inbound and outbound filters. |
| MsDTC |  | RPC | Since [NT 4,](http://en.wikipedia.org/wiki/Windows_NT_4.0) MSDTC has been performing as the transaction coordinator for components with [COM](http://en.wikipedia.org/wiki/Component_Object_Model) & [.NET](http://en.wikipedia.org/wiki/.NET_Framework) architectures. Connected resources can be databases, message queues or file systems which may be distributed. Messages are sent on TCP 135 while the responses are on a dynamically assigned |