The MCSE™ Exchange 2000 Administration Cram Sheet

This Cram Sheet contains the distilled, key facts about the Microsoft Exchange Administration 2000 exam. Review this information last thing before entering the test room, paying special attention to those areas where you feel you need the most review. You can transfer any of the facts onto a blank piece of paper before beginning the exam.

INSTALLING EXCHANGE 2000

1. Microsoft Exchange 2000 cannot be installed in a Windows NT 4 network, and you cannot install Microsoft Exchange 2000 on a Windows 2000 member server operating in a Windows NT 4 domain.
2. To install Microsoft Exchange 2000, you must be using both Windows 2000 and Active Directory.
3. Windows 2000 Server must be using Service Pack 1 or later, and Internet Information Server must be installed with NNTP. If this protocol is not available when you install Exchange 2000, setup will complete but your installation will not be fully functional.
4. To use advanced encryption techniques, you must install Microsoft Key Management Service.
5. You must run setup with the **/ForestPrep** switch *once* for each forest that will have Microsoft Exchange 2000 installed. Only members of the Schema Admins group have the ability to make changes to the Active Directory Schema.
6. You must run setup with the **/DomainPrep** switch in *each domain* into which Microsoft Exchange 2000 will be installed.
7. **/DomainPrep** performs the following actions:
   - Creates Exchange Domain Servers, a Global group
   - Creates Exchange Enterprise Server, a domain local group
   - Creates EUSER_EXSTOREEVENT, a user account
8. If you decided not to use the **/ForestPrep** and **/DomainPrep** options before running the setup program, they are run for you during the first installation of Microsoft Exchange 2000.
9. An organization is the largest unit of administration.
10. You can have more than one Microsoft Exchange 2000 server within a Windows 2000 forest, but you can have only one organization.
11. You can run setup with the **/createunattend** switch to create an initialization file for the unattended installation on remote servers.

EXCHANGE 2000 AND 5.5 INTEGRATION

12. The Active Directory Connector (ADC) is a utility that allows data to be replicated between the Exchange 5.5 directory and Active Directory.
13. Microsoft offers two versions of the ADC. Use the Exchange 2000 version when planning to have Exchange 5.5 and 2000 coexist.
14. For replication to work, the Exchange 5.5 server must be running Service Pack 3 or higher.
15. You can configure replication either as one-way or two-way. Two-way replication works in both directions, from Exchange 5.5 to Windows 2000 and from Windows 2000 to Exchange. If you choose a one-way connection agreement, you can specify which direction you want replication to take place.
16. If Exchange 5.5 is installed on a Windows 2000 domain controller, Exchange and Windows 2000 will contend for the default LDAP port, 389. For the ADC to successfully communicate through LDAP with the Exchange 5.5 directory, you must specify a different port number.
17. A primary connection agreement is capable of creating new objects in its respective directory.
18. The Site Replication Service (SRS) is an Exchange 2000 service installed during setup which emulates an Exchange 5.5 directory and makes communication between Exchange 2000 and 5.5 possible.
19. Exchange 2000 uses the Simple Mail Transport Protocol (SMTP) for its intrasite communications, while Exchange 5.5 uses remote procedure calls (RPC).
20. The preferred tool for moving mailboxes between servers is Active Directory Users And Computers.
21. When Exchange 2000 is coexisting with 5.5, it is running in what is known as *Mixed mode*. After all Exchange servers have been upgraded to 2000 and you're certain you no longer need 5.5 servers, you can switch to Native mode.

RECIPIENT OBJECTS

22. Exchange Server 2000 provides for the following types of recipient types: User, Contact, Group, and Public folder.
23. A mail-enabled user is one that can receive but cannot send email.
24. By default, Instant Messaging (IM) is disabled for user accounts.
25. A storage group is a container that can hold two different types of information stores, Mailbox stores and Public folder stores.
26. You can configure up to four storage groups per Exchange 2000 server.
27. You can have up to six information store databases per storage group.
28. By default, full-text indexing is off and must be enabled.
29. Exchange 2000 makes use of two different types of groups: *security* and *distribution*.
30. Distribution groups exist to group email recipients and can't have permissions applied to them.
31. The Recipient Update Service is an Exchange 2000 service that updates recipient objects with information such as address list membership and email addresses.

MANAGING ADMINISTRATIVE GROUPS

32. Routing groups are used to define the physical network. This means that the connectivity between your various Microsoft Exchange 2000 servers dictates your routing groups.
33. The three administrative models are Centralized, Decentralized, and Mixed.
34. The two security groups within your Windows 2000 environment that inherit a broad range of permissions are Enterprise Admins and Domain Admins.
35. You use Exchange System Manager to create administrative groups.
36. Exchange 2000 policies are sets of configuration options that can be defined and then applied to one or more objects in your environment.
37. Exchange 2000 offers two types of policies, System and Recipient.
38. In order for a policy to be applied, you must add a server to the policy.

ROUTING GROUPS

39. Exchange 2000 can run in either Mixed mode or Native mode; this has nothing to do with Windows 2000 Active Directory Mixed mode and Native mode.

40. Switching from Mixed mode to Native mode is a *one-way* change.
41. Microsoft Exchange 5.5 treats all servers within the administrative group as though they are in the same routing group.
42. Routing groups can span administrative groups.
43. Microsoft Exchange 2000 uses a *link state table* when routing messages. This table contains information regarding the routing groups and connectors that are contained within the entire organization.
44. The link state table is constructed and replicated by the routing group master. Each routing group has its own routing group master.
45. Routing between routing groups is determined by two critical factors: the *connector type* and *bridgehead servers*.
46. Connectors support different protocols (such as SMTP and RPC). Messages within a routing group are always transferred using SMTP.
47. You can use three different types of connectors: Routing group, SMTP, and X.400.
48. You cannot configure security on the routing group connector; it cannot encrypt messages.
49. The SMTP connector supports message encryption using Secure Sockets Layer (SSL).
50. The X.400 connector is primarily designed for networks that have limited bandwidth. It supports two protocols: TCP and X.25.
51. Link state data is passed over port 25 for updates between routing groups and over TCP port 691 within a routing group.
52. To send mail to foreign mail systems, install a foreign connector: These include cc:Mail, Lotus Notes, Novell GroupWise, and MS Mail connectors.

INSTANT MESSAGING

53. Instant Messaging communication uses Rendezvous Protocol (RVP), a subset of the WebDAV protocol.
54. A virtual server runs and appears to client computers as if it were a physical server. Exchange 2000 runs virtual servers for many Internet protocols, such as SMTP, POP3, IMAP4, and HTTP.
55. A Web site cannot be used by more than one Instant Messaging virtual server.
56. To configure IM settings for a firewall or proxy, use the Exchange System Manager utility.
57. Granting users permissions to use Instant Messaging is done through the Active Directory Users And Computers administrative utility.
58. Privacy settings must be configured on a per-user basis and can't be configured for groups or multiple users simultaneously.
59. By default, Instant Messaging uses integrated Windows authentication to validate IM users. If communicating through a proxy or non-Windows clients, you might need *standard Digest* authentication.
60. To enable Digest authentication, open the Internet Services Manager administrative utility.

CHAT SERVICE

61. Chat Service uses a protocol known as Internet Relay Chat (IRC) protocol.
62. Chat Service uses port 6667.
63. The two types of channels are a *registered channel* and a *dynamic channel*.
64. The sysop has privileges including the ability to close a channel, whether predefined or dynamic.
65. Some nicknames are reserved. Reserved names include "sysop", "Chanserv", and "NickServ."
66. In previous versions of Microsoft Exchange, it was possible to have a chat community that was spread among multiple servers. This is no longer supported in the new version of Chat Service.

SUPPORTING EXCHANGE 2000 CLIENTS AND VIRTUAL SERVERS

67. The four common methods of accessing Exchange Server from a client computer include Microsoft Exchange Server Service, POP3, IMAP4, and HTTP (Outlook Web Access).
68. When sending email using Outlook 2000, messages are sent to the server over port 25.
69. POP3 gives access only to a user's inbox.
70. POP3 communication occurs over TCP port 110. If you are using Secure Sockets Layer (SSL) security, POP3 will also utilize port 995.
71. IMAP4 users can access public folders as well as the Inbox.
72. IMAP4 communicates over TCP port 143. If using SSL security, IMAP4 will also utilize port 993.
73. Outlook Web Access communicates over TCP port 80, which is the standard for HTTP traffic. If Secure Sockets Layer (SSL) is used, port 443 will be used as well.
74. For client computers to access mailboxes using Outlook Web Access, their user accounts must be validated by IIS.
75. If a firewall exists between your Outlook Web Access server and a domain controller, the following ports must be open:
    - LDAP ports 389 and 3268
    - NetBIOS port 139
    - DNS port 53
    - RPC port 111, 135, and 1024
    - NetLogon port 445

PUBLIC FOLDER DEPLOYMENT

76. You can create public folders using the Exchange System Manager or Microsoft Outlook.
77. Exchange System Manager has several important advantages over Microsoft Outlook 2000: It allows you to view an entire public folder tree; it allows you to mail-enable a public folder; and it can specify retention and replication rules.
78. In previous versions of Microsoft Exchange 5.5, it was only possible to have one public folder tree. Microsoft Exchange 2000 supports multiple public folder trees.
79. New top-level public folder hierarchies are not available from a MAPI client unless viewed as a Web page.
80. New top-level public folder hierarchies are not by default mail-enabled.
81. The default top-level public folder is replicated automatically. This cannot be changed.
82. A replica is an instance of a public folder store.

ADVANCED SECURITY

83. Before installing the Exchange 2000 Key Management Service (KMS), install three templates: Enrollment Agent (Computer), Exchange User, and Exchange Signature Only.
84. To install KMS, rerun Exchange 2000 Server setup from the installation CD.
85. KMS cannot be set to automatically start when the computer boots up and other services start.

BACKUP AND RESTORE

86. The four backup types include Full, Copy, Incremental, and Differential.
87. A copy backup is similar to a full backup, except that it does not manipulate the archive bit.
88. An incremental backup backs up only files that have been changed since the last backup.
89. A differential backup backs up only data that has the archive bit set; unlike differential backups, a differential backup will not clear the archive bit.
90. An offline backup requires that all necessary services be stopped in order to back up the databases.
91. Exchange 2000 extends the standard Windows 2000 Backup program to allow for online backups.

CORIOLIS™ Certification Insider Press
© 2001 The Coriolis Group. All rights reserved.