This Cram Sheet contains the distilled, key facts about the Migrating from Microsoft Windows NT 4 to Microsoft Windows 2000 exam. Just before entering the test room, review this information; paying special attention to those areas where you feel you need the most review. You can transfer any of the facts from your memory onto a blank piece of paper before beginning the exam.

Developing the Migration Strategy

1. There are three migration paths:
   - Domain upgrade (in-place migration) - The system is upgraded, the network infrastructure does not change, and hardware does not change.
   - Domain restructuring - You can do interforest or intraforest restructuring:
   - Interforest restructuring (between forests) - Move and clone security principals into a pristine forest (using new equipment and a new infrastructure). Use tools such as ClonePrincipal and ADMT to clone objects.
   - Intraforest restructuring (within a forest) - Collapse a sprawling forest, and absorb resource and account domains into a single forest root. Use tools such as ADMT and MoveTree to move objects between domains.
   - Domain upgrade and restructuring - Perform a domain upgrade followed by a restructuring.
2. Order of migration for a domain upgrade:
   a. Upgrade account domains.
   b. Upgrade resource domains.
      1. Upgrade the domain PDC.
      2. Upgrade the domain BDCs and servers running DNS, WINS, and DHCP.
      3. Upgrade the application and member servers.
      4. Convert the domain to native mode after all domain controllers have been upgraded.
3. Order of migration for an interforest domain restructuring:
   a. Migrate account domains before resource domains to retain the sIDHistory.
      1. Create the Windows 2000 target domain (pristine forest).
      2. Use the ADMT Trust Migration Wizard or NETDOM to establish trusts between domains where the pristine forest is the trusting domain.
      3. Use the ADMT Group Migration Wizard or ClonePrincipal to migrate global groups.
      4. Use the ADMT User Migration Wizard to migrate user accounts.
      5. Decommission the source domain by demoting the domain controllers and moving the salvageable computers to the destination domain.
   b. Migrate resource domains.
      1. Use the ADMT Trust Migration Wizard to establish any needed trusts between domains.
      2. Use the ADMT Service Account Migration Wizard to identify service accounts.
      3. Use the ADMT Computer Migration Wizard to migrate workstations and member servers.
      4. Use the ADMT Security Translation Wizard to migrate local profiles.
      5. Use the ADMT Group Migration Wizard to migrate shared local groups.
      6. Use the ADMT User Migration Wizard to migrate service accounts. These accounts were identified in Step 2.
      7. Use the ADMT Security Translation Wizard to update service account user rights.
      8. Migrate a domain controller from the resource domain.
      9. Decommission source account domains by removing the last domain controller.
      10. Decommission source resource domains by removing the last domain controller.
4. Order of migration for an intraforest domain restructuring:
   a. Migrate resource domains before account domains.

1. Use the ADMT Service Account Migration Wizard to identify service accounts.
2. Use the ADMT User Migration Wizard to migrate service accounts. These accounts were identified in Step 1.
3. Use the ADMT Security Translation Wizard to update user rights and group memberships.
4. Use the ADMT Group Migration Wizard to migrate domain local groups.
5. Use the ADMT Computer Migration Wizard to migrate workstations and member servers.
6. Migrate a domain controller from the resource domain.
7. Decommission resource domains by removing the last domain controller.

b. Migrate account domains.
   1. Use the ADMT Group Migration Wizard to migrate global groups.
   2. Use the ADMT Service Account Migration Wizard to identify service accounts.
   3. Use the ADMT User Migration Wizard to migrate users, service accounts, and roaming profiles.
   4. Use the ADMT Security Translation Wizard to upgrade user rights, group memberships and migrate local profiles.
   5. Migrate a domain controller from the account domain.
   6. Decommission account domains by removing the last domain controller.

5. DNS server facts:
   - There are three types of DNS zones: primary, secondary, and Active Directory Integrated.
   - Primary and secondary zones are not Active Directory Integrated.
   - Active Directory Integrated zones provide fault tolerance, secure transfers and updates, and DNS replication that's integrated with Active Directory replication.
   - Active Directory requires DNS that supports SRV records and dynamic updates. BIND 8.1.2 or greater supports these records.
   - The same DNS namespace must be used for all domains within an Active Directory tree.
   - Multiple DNS namespaces can be used for an Active Directory forest, assuming that there is a common global catalog, configuration, and forest root.

6. Trust facts:
   - Transitive trusts are two-way, dynamic, and automatically generated.
   - Explicit trusts are one-way and are manually created.
   - All trusts between Windows 2000 parent and child domains and tree root domains are transitive.
   - External, one-way, nontransitive trusts must be manually created between Windows 2000 domains and Windows NT 4 domains or between Windows 2000 domains that are in different forests.
   - Shortcut trusts can be created between two domains in the same forest and are one-way. These trusts send the authentication request directly to the target domain without having to traverse the forest root.

Preparing the Environment for Migration

7. Prepare a disaster recovery plan:
   a. Synchronize and replicate the Windows NT BDCs with the PDC.
   b. Physically disconnect a BDC from the network.
   c. Back up the PDC.
   d. Perform a trial restoration of the PDC.

8. If a disaster occurs during upgrade:
   a. Physically remove the failed domain controller from the network.
   b. Promote the BDC to a PDC.
   c. Physically reconnect the promoted BDC to the network.
   d. Synchronize and replicate the promoted BDC to other network BDCs.
   e. Restore the PDC.

Planning and Deploying a Domain Upgrade

9. Group policy placement and order of inheritance:
    a. NT system policy - Primarily oriented for Windows NT clients.
    b. Local policy - Is manually configured on the local machine.
    c. Site policy - Is based on the site where the client is assigned.
    d. Domain policy - Applies specifically to the domain. Password, account lockout, and Kerberos policies can be set only at the domain level.
    e. Organizational unit - Can be nested within a parent OU. Inheritance flows within an organizational unit from parent to child, with the lowest OU having the greatest precedence.
    f. Computer configuration - Sets system-specific policies.
    g. User configuration - Takes precedence over all policies listed previously.
    h. Inheritance can be modified via the following:
        - Loopback - Reapplies the computer configuration after the user configuration has been applied.
        - Block Inheritance - Prevents policies from being applied to a specific object.
        - No Override - Prevents inheritance blocking.
10. Post-migration functionality of network services:
    - The DHCP server must be authorized within Active Directory in order to start after the upgrade.
    - DNS can be configured to allow DHCP to dynamically update down-level client entries in the DNS database.
    - LAN Manager Replication (LMRepl) has been replaced by the File Replication Service (FRS).
    - The Distributed File System (DFS) relies on the File Replication Service (FRS) to synchronize DFS links.
    - Mixed-mode domains must establish a file replication bridge in order to maintain replication between Windows 2000 and Windows NT. You can use the lbridge.cmd script to copy files from an NT replication server to a Windows 2000 domain controller.
11. The Directory Service Client software allows clients in a native-mode domain to change passwords on any domain controller in the domain. The client can also search Active Directory and access site-aware services such as DFS.
12. Active Directory permissions will need to be loosened for remaining NT servers whose applications, such as RAS, will need to maintain anonymous Read access to the Active Directory database.

Planning and Deploying intraforest and interforest domain restructuring

13. Active Directory logical components:
    - Forest - A collection of domains that share a common forest root, global catalog, schema, and configuration.
    - Tree - A group of domains arranged in parent-child relationships in a single forest that share a contiguous namespace.
    - Domain - A security and replication boundary. Domains can exist as part of a tree or as part of a separate forest.
    - Organizational units - The smallest segment of the Active Directory logical structure. OUs provide the ability to segment Active Directory into manageable pieces; OUs can be based on location, role, department, or any other criteria that define administrative boundaries.
14. Active Directory physical components:
    - The physical setup should be designed to reduce latency, improve resource access, and control replication.
    - Sites are a group of well-connected TCP/IP subnets that send users to servers based upon IP address and site membership.
15. To move a domain controller to a new domain:

- Upgrade Windows NT to Windows 2000. Rename, move, and promote the member server to domain controller with Dcpromo.exe.
- Demote the Windows 2000 domain controller to a member server with Dcpromo.exe. Rename the server, move it to a new domain, and promote it to domain controller with Dcpromo.exe.

16. The sIDHistory attribute is available only in a native-mode domain. The sIDHistory attribute contains the security identifier of a cloned user account and can be used to maintain access to the same resources that the source domain account had access to before the migration.

17. Migration tools and features:

Tool Feature	ADMT	ClonePrincipal	Netdom	MoveTree
Interforest	Yes	Yes	Yes	No
Intraforest	Yes	No	Yes	Yes
Migrate users and groups	Yes	Yes	No	Yes
Migrate computers	Yes	No	Yes	No
Migrate service accounts	Yes	No	No	No

18. ADMT and ClonePrincipal configuration requirements must be met for the migration to be successful:
    - The PDC in the source domain must have the TcpipClientSupport Registry value added to the Registry key HKLM\System\CurrentControlSet\Control\Lsa with the value's data set to 1.
    - The user performing the restructuring must be an administrator in both source and target domains.
    - Auditing of account management must be enabled in both source and target domains.
    - A local group named sourcedomainname$$$ - where sourcedomainname is the NetBIOS name of the source domain - must be created on the source domain's PDC.
    - You must create a trust between source and target domains with the target domain configured as the trusted domain.
    - Source and target domains must be in different forests.

19. MoveTree has the following requirements:
    - The source and target domains must be in the same forest.
    - The RID master in the source domain must be able to be contacted by the MoveTree application.
    - Both the source and target domains must be Windows 2000 domains.

20. ClonePrincipal is a group of Visual Basic scripts that are designed to clone a security principal to a new forest.
    - Cloning works only between forests.
    - Clone global groups before cloning users to maintain group membership.
    - Clonegg.vbs clones global groups.
    - Cloneggu.vbs clones users and global groups.
    - Clonelg.vbs clones local groups.
    - Clonepr.vbs clones a single security principal.

Troubleshooting

21. Active Directory must access DNS. If clients are unable to log on, and the network isn't an issue, ensure that the DNS entry under TCP/IP properties is correct.

22. DHCP client configuration for DNS and default gateway servers can cause name resolution and Internet connectivity problems.

23. Use Nltest.exe to determine and test the domain status of servers and domain controllers.