



## FOREST

Decisions	References
<p><b>Forest Plan</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Determine number of forests (single or multiple) based on:                             <ul style="list-style-type: none"> <li>Technical factors and Organizational factors</li> </ul> </li> <li><input type="checkbox"/> Determine the Forest Model</li> <li><input type="checkbox"/> Identify all Directory Services currently in use</li> <li><input type="checkbox"/> Determine number of trees within each forest</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Business Requirements</li> <li><input type="checkbox"/> Management Model</li> <li><input type="checkbox"/> Technological Standards</li> <li><input type="checkbox"/> Projected Growth Strategies</li> </ul>
<p><b>Forest Examples</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Production Forest</li> <li><input type="checkbox"/> Staging Forest same structure as Production Forest</li> <li><input type="checkbox"/> Development Forest</li> <li><input type="checkbox"/> Utilitarian Forest single combined root and Production domain</li> <li><input type="checkbox"/> Application Forest</li> <li><input type="checkbox"/> Perimeter Forest made of a single domain</li> </ul>	<p><b>Forest Models</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Unique Global Forest</li> <li><input type="checkbox"/> Multiple Forests to represent Business Units</li> <li><input type="checkbox"/> Functional Forests</li> </ul>

### Best Practices

1. Identify and justify each forest
2. Create a Design plan for each forest
3. Identify and justify each tree

Forest Criteria	Tree Criteria
<p><b>Single Forest</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Extremely rare, everyone upgrading to WS03 should have at least a Staging Forest</li> </ul> <p><b>Multiple forests</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Acquisitions or mergers</li> <li><input type="checkbox"/> Disagreements over scope of administrative control</li> <li><input type="checkbox"/> Disagreements over the forest change control policy</li> <li><input type="checkbox"/> Requirements for multiple schemas</li> <li><input type="checkbox"/> Forest for development and testing</li> <li><input type="checkbox"/> Legal or regulatory constraints</li> <li><input type="checkbox"/> Impossible to guarantee security of DCs</li> </ul> <p><b>Multiple forest disadvantages</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Increased fixed costs</li> <li><input type="checkbox"/> Separate management of forest-wide components</li> <li><input type="checkbox"/> Additional configuration for resource access between forests</li> <li><input type="checkbox"/> Default User Principal Name (UPN) required to log on from a different forest</li> <li><input type="checkbox"/> Moving security principals between forest can impact user logon</li> <li><input type="checkbox"/> Moving domains between forests is not possible</li> </ul> <p><b>Benefits of a single production forest design</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Minimizes administration costs</li> <li><input type="checkbox"/> Provides users with a single location to search for objects in the organization</li> <li><input type="checkbox"/> Makes logon easy for users</li> <li><input type="checkbox"/> Eliminates the need for explicit trusts between forests</li> <li><input type="checkbox"/> Forest owners manage forest-wide services</li> </ul>	<p><b>Rules for Tree attribution</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Inter-service reliability</li> <li><input type="checkbox"/> Close collaboration between organizations</li> <li><input type="checkbox"/> Mergers</li> <li><input type="checkbox"/> IT management resource sharing</li> </ul> <p><b>Single Tree versus multiple Trees</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Use the fewest number of trees possible to reduce administrative overhead</li> <li><input type="checkbox"/> Multiple namespaces require multiple trees</li> <li><input type="checkbox"/> The name of each namespace is the name of the root for that tree</li> </ul> <p><b>Multiple Trees</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Organizations operate with multiple public names</li> <li><input type="checkbox"/> Organizations that rely on others for service completion</li> <li><input type="checkbox"/> Partnerships and collaborators</li> <li><input type="checkbox"/> Enterprises that merge with each other</li> <li><input type="checkbox"/> Organizations who share IT management resources</li> <li><input type="checkbox"/> Organization is one single enterprise, but each of its business units is known under a different public name domain in each tree</li> </ul>

## DOMAINS

Decisions	References
<p><b>Domain Strategy</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Determine number of domains                             <ul style="list-style-type: none"> <li><input type="checkbox"/> Number of users in the forest</li> <li><input type="checkbox"/> Bandwidth availability in the Network to support DC replication</li> <li><input type="checkbox"/> Scope of each Domain</li> <li><input type="checkbox"/> Decide on the Domain model (global or regional)</li> <li><input type="checkbox"/> Name of each Domain</li> <li><input type="checkbox"/> Use of a Dedicated Root Domain?</li> <li><input type="checkbox"/> Decide if additional Domains are required</li> </ul> </li> <li><input type="checkbox"/> Determine when to create a domain                             <ul style="list-style-type: none"> <li><input type="checkbox"/> To support a decentralized administration</li> <li><input type="checkbox"/> To isolate Domain replication traffic</li> <li><input type="checkbox"/> To balance Domain replication traffic</li> <li><input type="checkbox"/> To support different policies for multiple domains</li> <li><input type="checkbox"/> To conform to internal political situations</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Business Structure</li> <li><input type="checkbox"/> Network Architecture</li> <li><input type="checkbox"/> Technical Standards</li> <li><input type="checkbox"/> Hardware/Software Lists</li> <li><input type="checkbox"/> Windows NT Domain Architecture</li> <li><input type="checkbox"/> Forest Model</li> <li><input type="checkbox"/> Projected Growth and Strategy</li> </ul>
<p><b>Domain Design Examples</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Protected Forest Root Domain</li> <li><input type="checkbox"/> Global Single Child Domain</li> <li><input type="checkbox"/> Production Domain</li> <li><input type="checkbox"/> Staging Domain</li> <li><input type="checkbox"/> Development Domain</li> <li><input type="checkbox"/> Training Domain</li> <li><input type="checkbox"/> Utilitarian Domain</li> <li><input type="checkbox"/> Other Domain (if required) in Production Forest</li> </ul>	<p><b>Domain Models</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Unique Domain</li> <li><input type="checkbox"/> Multiple Domain</li> <li><input type="checkbox"/> Dedicated Root Domain</li> <li><input type="checkbox"/> Global Single Child Domain</li> </ul>
<p><b>Best Practices</b></p> <ol style="list-style-type: none"> <li>1. Wherever possible, create a protected forest root domain</li> <li>2. If required, create a Filter Tree or Site root domain</li> <li>3. Identify the number of additional domains required within each tree</li> <li>4. Identify the scope and contents of each domain</li> <li>5. Justify each domain</li> <li>6. Choose the generic name for each domain</li> <li>7. Once the domain structure for the production forest is complete, design the domain structure for the other forests</li> </ol>	
Domain Criteria	Domain Criteria
<p><b>Domains are used to:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Regroup objects into smaller portions</li> <li><input type="checkbox"/> Administrative Requirements</li> <li><input type="checkbox"/> Security Policy Requirements</li> <li><input type="checkbox"/> Replication Requirements</li> <li><input type="checkbox"/> Retain Windows NT domain structure</li> <li><input type="checkbox"/> Native WS03 domain</li> </ul> <p><b>Potential costs for additional domains</b></p> <p>More Domain administrators:</p> <ul style="list-style-type: none"> <li>• The Domain Admins group for each domain requires close monitoring</li> <li>• Domain administrators for each domain perform redundant administration tasks</li> <li>• Can be reduced to a single set of Forest administrators</li> </ul> <p>More Domain Controller hardware:</p> <ul style="list-style-type: none"> <li>• Each Domain requires at least two Domain Controllers</li> <li>• Domain Controllers must be physically guarded</li> </ul> <p>More communication between Domain Controllers in different Domains:</p> <ul style="list-style-type: none"> <li>• Domain Controllers in different Domains must communicate to authenticate users</li> <li>• More trust relationships</li> </ul> <p>The need to move security principals between domains:</p> <ul style="list-style-type: none"> <li>• More Domains increases the probability of moving</li> </ul>	<p><b>Protected Forest Root Domain:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Smaller than Production Domain</li> <li><input type="checkbox"/> Contains Forest Management groups and users</li> <li><input type="checkbox"/> Minimum amount of data which reduces replication</li> <li><input type="checkbox"/> Easier to rebuild in case of disasters</li> <li><input type="checkbox"/> Small group of forest-wide administrators</li> <li><input type="checkbox"/> Never retired since does not contain Production data</li> <li><input type="checkbox"/> Organizational restructuring is easier to accomplish</li> <li><input type="checkbox"/> Easier to secure</li> </ul> <p><b>Global Single Child Domain:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Regroup all users</li> <li><input type="checkbox"/> Users are identifiable</li> <li><input type="checkbox"/> Their actions are traceable</li> </ul> <p><b>Single Domain Structure</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Less than 500 users</li> <li><input type="checkbox"/> Rare in a large organization</li> <li><input type="checkbox"/> Ease of management and delegation</li> <li><input type="checkbox"/> Lower costs</li> <li><input type="checkbox"/> Simplified Global Catalog implementation</li> </ul> <p><b>Multiple Domain Structure</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Operations span several different countries</li> <li><input type="checkbox"/> Legal requirements that differ country to country</li> <li><input type="checkbox"/> To filter forest inheritance</li> <li><input type="checkbox"/> Test and stage global modifications</li> </ul>



## NAMESPACE STRATEGY

Decisions	References
<p><b>Naming Strategy</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Identify Root Domain Name                             <ul style="list-style-type: none"> <li><input type="checkbox"/> Internal vs External name</li> </ul> </li> <li><input type="checkbox"/> Identify names for forest objects                             <ul style="list-style-type: none"> <li><input type="checkbox"/> Differentiate between Domain and server objects (see table 3.3 — Domain objects)</li> </ul> </li> <li><input type="checkbox"/> Directory Scope</li> <li><input type="checkbox"/> Name resolution</li> <li><input type="checkbox"/> DNS structure</li> </ul>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Domain Hierarchy diagram</li> <li><input type="checkbox"/> DNS environment</li> <li><input type="checkbox"/> Projected growth and strategies</li> </ul>
Best Practices	
<ol style="list-style-type: none"> <li>1. Make sure it is different from external name</li> <li>2. Before proceeding, buy the name</li> <li>3. Use a reserved domain name for internal forest</li> <li>4. Use standard Internet characters</li> <li>5. Use 15 characters or less for each name</li> <li>6. For the root name, use a simple, short name that is representative of the identity of the organization</li> <li>7. Follow all DNS standards</li> </ol>	
Criteria	Rules
<p><b>DNS Name</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Existing DNS</li> <li><input type="checkbox"/> Delegated</li> <li><input type="checkbox"/> Different namespace</li> <li><input type="checkbox"/> Internal Name</li> <li><input type="checkbox"/> External Name</li> <li><input type="checkbox"/> Names for AD domains</li> </ul> <p><b>Namespace hierarchy</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Represents the entire organization</li> <li><input type="checkbox"/> Security</li> <li><input type="checkbox"/> Political considerations</li> <li><input type="checkbox"/> Cost</li> <li><input type="checkbox"/> Registered for the Internet</li> </ul> <p><b>Type and version of DNS software</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Support AD — WINS — DNS (Bind 8.1.2)</li> <li><input type="checkbox"/> Does not support AD</li> </ul> <p><b>Technical Requirements</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Support for SRV records</li> <li><input type="checkbox"/> Support for Dynamic Update Protocol</li> <li><input type="checkbox"/> Support for incremental zone transfers</li> </ul> <p><b>AD Namespace:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Defines the scope of the AD</li> <li><input type="checkbox"/> Based on hierarchical nature of DNS</li> <li><input type="checkbox"/> Define the naming boundaries of the AD database</li> <li><input type="checkbox"/> Defines the structure of the database and the relationships between its objects</li> </ul>	<p><b>DNS names:</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Use only registered DNS names</li> <li><input type="checkbox"/> Ensure that you have complete ownership over it</li> <li><input type="checkbox"/> If you use an unregistered name, verify that it does not exist on the Internet</li> <li><input type="checkbox"/> Segregate internal namespace from the external namespace</li> <li><input type="checkbox"/> Never use the same forest name twice</li> <li><input type="checkbox"/> NetBIOS names must be unique within a domain</li> <li><input type="checkbox"/> The first part of the DNS name must be the same as the NetBIOS name</li> <li><input type="checkbox"/> Use short, distinct, and meaningful names</li> <li><input type="checkbox"/> Distinguish between domain and machine names</li> <li><input type="checkbox"/> Forest, tree and domain names should be considered static</li> <li><input type="checkbox"/> Don't use organizational structure to name domains</li> <li><input type="checkbox"/> Domains should not be renamed (event if you can!)</li> <li><input type="checkbox"/> Geographic names are recommended</li> <li><input type="checkbox"/> Use Standards Internet characters A-Z, a-z, 0-9, (-), no numeric names</li> <li><input type="checkbox"/> Use 15 characters or less NetBIOS has a maximum of 15 usable characters</li> </ul>
Use Existing DNS Namespace	
<ul style="list-style-type: none"> <li>• Users can access a single domain name when accessing resources both internally and externally</li> <li>• Additional names need not be registered with a DNS name registration authority</li> <li>• Additional administration is required to ensure appropriate records are on the internal and external DNS servers</li> <li>• Possible security risk</li> </ul>	
Use Delegated Namespace	
<ul style="list-style-type: none"> <li>• A contiguous namespace which is understood by administrative staff and clients</li> <li>• All AD data in a domain or domain tree is isolated</li> <li>• A separate DNS server is required for the delegated AD Root Domain</li> <li>• AD namespace is long</li> </ul>	

## Use a different Namespace

- Resources are easy to manage and secure
- Internal naming hierarchy is not exposed on the Internet
- AD resources are inaccessible from the Internet when using the external DNS namespace
- External server content need not be replicated to internal servers
- Existing DNS zones and DNS topology can remain unchanged
- Recommended approach

## General Comments:

---

---

---

---

---

---

---

---

---

---

## ORGANIZATIONAL UNIT

### Decisions

#### Organizational Unit Strategy

- Identify OU strategies
- Identify accounts OUs
  - Assign owners
- Identify resource OUs
  - Assign owners
- Identify every manageable object in the network (see table 3.4 — Manageable objects within AD)
- User a questioning process for each OU
- Categorize PCs
- Organize the services in the network
- Delegate application servers
- Replicate the OU structure to other domains (see table 3.5 — OU structure in other domains)
- Categorize people

#### Reasons to create OUs:

- Required to regroup AD object types
- Required to administer AD objects
- Required to delegate the administration of AD objects
- Required to hide objects

### References

- Domain Hierarchy diagram
- DNS environment
- Projected growth and strategies

### Best Practices

1. Think in terms of equipment and objects in the directory
2. Determine how you will implement the administrative delegation process
3. Identify standards for all administrative categories within the organization structure
4. Name OUs by administrative service or function, not by organization
5. Limit the structure to five levels
6. Remember the four reasons for the creation of OUs
7. Each OU created must add value to the system
8. Never create an OU that does not contain any objects or a specific purpose
9. If an OU reaches an empty state, consider removing it
10. Identify an OU Owner for each one
11. Justify all OUs
12. If two OUs have the same purpose, merge them
13. Use default OUs to administer the whole domain
14. Use the Production domain OU strategy to define the OU strategy for other domains and forests Don't forget to define and put in place standards for the recurring creation and deletion of OUs

## Characteristics

### OU Structure

- Use OUs to:
    - Group objects or resources
    - Simplify management of commonly grouped resources
    - Allow delegation of administrative tasks
    - Manage users/computers with Group Policy
  - OUs:
    - Can be nested
    - Can be used to delegate administrative control
    - Enable Group Policy to be applied to them
    - Are not security principals
    - Are not navigated by users
- OU advantages:**
- Ability to delegate management
  - Designed to help support the data/service concept of AD
  - Contain AD objects and their properties, and contain data
  - Must be contained in a domain
  - Identify network administration structure
  - Can contain other OUs

## Characteristics

- Account and Group Definition
- Group Policy Object Management Strategy
- PC Management Strategy
- Delegation Plan
  - Object types
  - Geographic-based
  - Organization-based
  - Business Function-based
  - Hybrid
- Administration Plan
  - Centralize
  - Centralize/decentralize
  - Decentralize
  - Hybrid
    - Geographic then organization
    - Organization then geographic
- Hide Objects and Limit Access
- Group Policy application
  - Local
  - Sites
  - Domains
  - Organizational Units

## Upper-Level OU

- Base upper-level OU on a static aspect of the administrative model (object types)
- Make upper-level OU standard in all domains (if possible)
- Use names that are meaningful to the administrative staff

## Lower-Level OU

- Lower level OUs mirror the structure of the administrative model (based on functions or Business Units)
- Use lower-level OUs to:
  - Delegate administration
  - Apply Group Policy
- Design considerations:
  - OUs can be administrated independently
  - Nest organizational units to mirror administrative model
  - Group Policy is applied to objects in OUs

## By object type

- Three OUs required
  - People, PCs, Services

## Geographic-based Structure

- Is resistant to company reorganizations
- Accommodates mergers and expansions
- Takes advantage of network strengths
- May compromise security (local security admins)

## Organization-based Structure

- Reflects business model
- Is vulnerable to reorganizations
- Maintains departmental and departmental autonomy
- Accommodates mergers and expansions
- May affect replication

## Business Function-based Structure

- Is immune to reorganizations
- May require additional layers
- May affect replication





## SERVICE POSITIONING AND SITE TOPOLOGY

### Decisions

#### Service positioning

- Operations Master Positioning
  - For the Forest
  - For the Domain(s)
- Domain Controller (DC) Positioning
- Global Catalog Positioning
- DNS Server Positioning

#### DC positioning and roles in each forest and domain

- Evaluate network performance
- At least two DCs in every Domain in every forest
- DC in a site with large numbers of users
- DC if the site contains server resources
- No DC if no adequate security or proper computer maintenance

#### Global Catalog positioning

- If network spans several regions, place at least one GC server per region
- Useful for WAN and for applications using port 3268 for authentication requests

#### DNS Server Configuration

- Marry DNS service with the Domain Controller service
- Zone positioning and type identification
- The recursive Name Resolution method

### Decisions

#### Topology Design

- Site boundaries for each geographic location
  - Site replication links
  - Backup replication for each link
  - Costing scheme for each link
  - Site link should follow the Enterprise TCP/IP Network design
  - Site links to connect sites
  - Replication transports
  - Site link schedules and costs
  - Number and location of sites
  - WAN topology and link speed for each location
  - Number of DCs in each site
  - Split Production Domain if they replicate over links speed of 56Kb per second or lower
  - Large Production Domains require high speed WAN links
- #### Sites (Service Illustration 3-9)
- Should follow the Enterprise TCP/IP Network design
  - Document the criteria for site creation
  - For site configuration, consider GC requirements
  - The minimum recommended WAN circuit is 128Kbps

### Best Practices for Service Positioning

1. Place the RID Master and the PDC Emulator role on the same DC
2. Create a dedicated PDC Emulator role in domains that have more than 50,000 users
3. Separate Global Catalogs and Infrastructure Masters if you can
4. If a small domain spans two sites, use at least two DCs, one for each site
5. Place a GC server in each geographic site that contains at least one DC
6. Enable Universal Group Membership Caching in each geographic site
7. Place at least two DCs wherever there are more than ten users
8. Add a regional DC whenever there are more than 50 users per DC
9. Install DNS on every DC

### Best Practices for Site Topology

1. Use the default configuration for Inter-site replication
2. Do not disable the Knowledge Consistency Checker
3. Do not disable Transitive trusts
4. Do not specify Bridgehead Servers
5. Calculate Replication Latency between sites
6. Create sites according to Network topology; site links and WAN links should correspond
7. Ensure that no single site is connected to more than 20 other sites
8. Each site must house at least one DC
9. Do not use SMTP for Domain-centric replication
10. Do not use SMTP replication if at all possible
11. Use 128Kbps as the minimum WAN circuit for a site link
12. Associate every site with at least one subnet and one site link, otherwise it will be unusable
13. Create backup site links for each site
14. If your available network bandwidth, can afford it, ignore replication schedules in all sites
15. Enable Universal Group Membership Caching for all DCs in the region
16. Use Preferred Bridgehead Servers if replication must cross a firewall

## Service Positioning characteristics

- Relates to the position and role for DCs within each forest and each domain

### Domain Controllers:

- Core service provider for AD
- Provide multimaster replication for the entire forest
- Some have special roles:
  - Operations Master
    - Schema Master
    - Domain Naming Master
    - Relative ID Master
    - PDC Emulator
    - Infrastructure Master
- Global Catalog

## Replication — Sites characteristics

- Intra-site Replication
- Inter-site Replication
- Site links are IP subnets
- Site link bridges allow the replication to use the bridging site to create a direct connection to the destination site
- Bridgehead servers manage all inter-site replication within a site.

## Rules for AD Replication and Sites

- Ensures that all information in AD is available to all domain controllers and client computers across the entire network
- Uses site topology information to update AD changes from one Domain Controller to another Domain Controller
- Occurs between Domain Controllers located on the same site, called intra-site replication
- Occurs between Domain Controllers located in different sites, called inter-site replication

## Potential Sites

- Is a set of contiguous physical networks that are connected by fast, inexpensive, and reliable network links
- Can be determined by grouping IP subnets that are connected by a LAN
- Is connected to other potential sites by slow, expensive, or unreliable network links

## Placing DCs in Potential Sites

- Place DCs in a potential site if there is a large number of users in the site
- Place DCs in a potential site if the site contains server resources that you want users to access when the WAN link is unavailable for authentication
- Do not place DCs in a potential site if there is no adequate physical security or proper computer maintenance at the site

## Determining Sites

- Every user location, physical network connection, and domain controller should be associated with exactly one site
- Every site should contain a domain controller
- Every site should represent a set of fast, reliable, and inexpensive physical network connections

## Using Site Links to connect Sites

- A site link is a low-bandwidth or unreliable network that connects two or more sites
- A site link has four parameters:
  - Replication schedule
  - Replication interval
  - Cost
  - Transport

## Site Link Bridges

- Model the routing behavior of a network
- Are not necessary in fully routed IP networks
- For the same transport, work together to model multi-hop routing

## Existing DNS Service Configuration

- Server positioning — all DCs must also have DNS service
- Recursive name resolution method — determine the recursive name resolution method to use
- Zone positioning —

Forest Root contains zone for:

- Root Domain
- Forest (`_msdcs.<forest-root>`) in forest-wide application partition

Each Regional or Child Domain contains zone for:

- Their own Child Domain
- Forest (`_msdcs.<forest-root>`) in forest-wide application partition

## SCHEMA

Decisions	Decisions
<p><b>Schema modifications strategy</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Identify the elements of the Schema modification policy</li> <li><input type="checkbox"/> Identify the members and the charter for the Schema Change Management Committee (SCMC)</li> <li><input type="checkbox"/> Identify the process for the Schema Change Management                             <ul style="list-style-type: none"> <li><input type="checkbox"/> Type of the changes that can be made</li> <li><input type="checkbox"/> Approval process for change requests</li> <li><input type="checkbox"/> Define the policy for making changes for the schema and the configuration partition</li> <li><input type="checkbox"/> Type of the changes</li> </ul> </li> <li><input type="checkbox"/> Guidelines and Processes for :                             <ul style="list-style-type: none"> <li><input type="checkbox"/> Who can modify the schema</li> <li><input type="checkbox"/> Initiating schema modifications</li> <li><input type="checkbox"/> Planning, testing, and implementing</li> <li><input type="checkbox"/> Who can modify the forest configuration</li> <li><input type="checkbox"/> Creating new domains in the forest</li> <li><input type="checkbox"/> Modify the forest site topology</li> </ul> </li> <li><input type="checkbox"/> Identify the new roles for the organization</li> </ul>	<p><b>Members of the SCMC</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> IT Planning &amp; Enterprise Architecture</li> <li><input type="checkbox"/> IT Group</li> <li><input type="checkbox"/> Help &amp; Support</li> <li><input type="checkbox"/> Training</li> <li><input type="checkbox"/> IS Group</li> </ul> <p><b>Rules for the SCMC</b></p> <ul style="list-style-type: none"> <li><input type="checkbox"/> Each member has a single vote</li> <li><input type="checkbox"/> Every modification must be voted on</li> <li><input type="checkbox"/> The Production Schema Owner, the CIO, has veto power over the committee</li> <li><input type="checkbox"/> Committee meets on a biannual basis</li> <li><input type="checkbox"/> Change request strategy must be in place to support the schema modification requests</li> <li><input type="checkbox"/> Collect change requests form the agenda of each committee meeting</li> <li><input type="checkbox"/> Every committee member must have appropriate AD training</li> </ul>
<p><b>Best Practices for Schema policies</b></p>	
<ol style="list-style-type: none"> <li>1. Identify who controls Schema Administrators Universal Group</li> <li>2. Identify the Enterprise Administrators</li> <li>3. Create a Committee to approve modifications</li> <li>4. Document the steps required for a modification:                             <ol style="list-style-type: none"> <li>a. Modification description</li> <li>b. Modification justification</li> <li>c. Impact evaluation on the modification</li> </ol> </li> <li>5. If a new object is added                             <ol style="list-style-type: none"> <li>a. Object identifier for the new class</li> <li>b. Class type</li> <li>c. Class localization in the hierarchy</li> <li>d. Verify system stability and security</li> </ol> </li> <li>6. Document the steps required to test a modification                             <ol style="list-style-type: none"> <li>a. Test the modification</li> <li>b. Determine if the modification meets the requirements</li> <li>c. Test and plan for a recovery method</li> <li>d. Obtain committee approval for the implementation</li> </ol> </li> <li>7. Document the steps required to implement a modification                             <ol style="list-style-type: none"> <li>a. Restrict the number of administrators for the Schema</li> <li>b. Enable a write copy on the Operation Master</li> <li>c. Verify that all DCs receive the change</li> <li>d. Reset the Operations Master to Read only</li> </ol> </li> </ol>	
<p><b>Services and roles</b></p>	
<p>Forest owners manage forest-wide services</p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Forest-wide Operations Master Administrators</li> <li><input type="checkbox"/> Root Domain Administrators</li> <li><input type="checkbox"/> Root Domain Data Owner</li> <li><input type="checkbox"/> Forest-wide Security Group Owner</li> <li><input type="checkbox"/> Root Domain Security Group Owner</li> </ul>
<p>New roles</p>	<ul style="list-style-type: none"> <li><input type="checkbox"/> Forest Owner</li> <li><input type="checkbox"/> Forest Administrator</li> <li><input type="checkbox"/> Domain Owner</li> <li><input type="checkbox"/> Domain Administrator</li> <li><input type="checkbox"/> Domain Operator</li> <li><input type="checkbox"/> DNS Administrator</li> <li><input type="checkbox"/> Site Topology Administrator</li> <li><input type="checkbox"/> Root Domain Owner</li> <li><input type="checkbox"/> OU Owners</li> <li><input type="checkbox"/> OU Administrators</li> </ul>

## AD IMPLEMENTATION

Focus	References
<p><b>AD Implementation Plan</b></p> <ul style="list-style-type: none"><li><input type="checkbox"/> Forest, Tree, Domain installation</li><li><input type="checkbox"/> OU and Group design</li><li><input type="checkbox"/> Service Positioning</li><li><input type="checkbox"/> Site topology implementation</li></ul> <p><b>AD Implementation Blueprint</b></p> <ul style="list-style-type: none"><li><input type="checkbox"/> Uses a parallel network (see Chapter 2)</li><li><input type="checkbox"/> Implementation of a new Active Directory (see Chapter 4)</li><li><input type="checkbox"/> Implementation of the IP Network infrastructure (see Chapter 4)</li></ul> <p><b>Mode:</b></p> <ul style="list-style-type: none"><li><input type="checkbox"/> Mixed:<ul style="list-style-type: none"><li><input type="checkbox"/> Coexistence is possible</li><li><input type="checkbox"/> NT 4 limits AD possibilities</li><li><input type="checkbox"/> Windows 2000 limits Windows Server 2003</li></ul></li><li><input type="checkbox"/> Native Windows 2000:<ul style="list-style-type: none"><li><input type="checkbox"/> All DCs run on Windows 2000 or WS03</li></ul></li><li><input type="checkbox"/> Native Windows Server 2003:<ul style="list-style-type: none"><li><input type="checkbox"/> All DCs run WS03 native mode</li><li><input type="checkbox"/> Forest runs WS03 native mode</li></ul></li></ul>	<p><b>Tools:</b></p> <ul style="list-style-type: none"><li><input type="checkbox"/> AD Design Blueprint — Figure 3-2</li><li><input type="checkbox"/> Visio for the Active Directory Design process</li><li><input type="checkbox"/> Step by step to import and export AD to Visio on Microsoft site</li></ul> <p><b>Reasons to stay in a mixed mode</b></p> <ul style="list-style-type: none"><li><input type="checkbox"/> Maintain regional BDCs in the Domain</li><li><input type="checkbox"/> No physical security for BDCs</li><li><input type="checkbox"/> Allows rollback to Windows NT</li></ul>

General Comments:

---

---

---

---

---

---

---

---

Date: \_\_\_\_\_

By: \_\_\_\_\_