Microsoft Active Directory Best Practice Part II

Posted on July 29, 2012

I have written Active Directory Best Practice last year. I received huge feedback on this article. Recently I had to deal with an Active Directory disaster. I believe time is perfect to write part II on this same topics and educate others so that they learn Active Directory and prepare themselves for disaster recover. In this article I am also writing about Active Directory Design and the elements of the design. You may think you know Active Directory but have a look what you don't know!

Readers who may benefit from this article:

Technical Architect, Systems Engineer, Systems Administrator, Active Directory Designer

Active Directory FSMO Role Design Best Practice

Scope of AD Design

1. Provide Compliance, Governance and Oversee Network Authentication
2. Secure Servers, Users and Computers
3. Provide DNS Resolution
4. Create central repository of all IT objects and assets

What are the elements of Active Directory Design?

1. Forest Plan
2. Domain Plan
3. Organizational Unit Plan
4. Site and Services Plan

1. Key Consideration for Forest Plan

• Determine the number of forests for your network
• Create a forest change control policy
• Understand the impact of changes to the forest after deployment

Multi-Master Model:

A multi-master enabled database, such as the Active Directory, provides the flexibility of allowing changes to occur at any DC in the enterprise, but it also introduces the possibility of conflicts that can potentially lead to problems once the data is replicated to the rest of the enterprise. One way Windows deals with conflicting updates is by having a conflict resolution algorithm handle discrepancies in values by resolving to the DC to which changes were written last (that is, "the last writer wins"), while discarding the changes in all other DCs. Although this

resolution method may be acceptable in some cases, there are times when conflicts are just too difficult to resolve using the “last writer wins” approach. In such cases, it is best to prevent the conflict from occurring rather than to try to resolve it after the fact. For certain types of changes, Windows incorporates methods to prevent conflicting Active Directory updates from occurring.

Single-Master Model:

To prevent conflicting updates in Microsoft AD, the Active Directory performs updates to certain objects in a single-master fashion. In a single-master model, only one DC in the entire directory is allowed to process updates. This is similar to the role given to a primary domain controller (PDC) in earlier versions of Windows, in which the PDC is responsible for processing all updates in a given domain.
Microsoft Active Directory extends the single-master model found in earlier versions of Windows to include multiple roles, and the ability to transfer roles to any domain controller (DC) in the enterprise. Because an Active Directory role is not bound to a single DC, it is referred to as a Flexible Single Master Operation (FSMO) role. Currently in Windows there are five FSMO roles:

- Schema master
- Domain naming master
- RID master
- PDC emulator
- Infrastructure daemon

2. Domain Plan

The domain plan is perhaps the most complicated aspect of the Active Directory design process. The planning process described below is divided into three parts:
• Determining the number of domains
• DNS and Domain Names
• Post Deployment Change management

Who are the administrator and who are delegated in Active Directory?

• Current domain administrators who are responsible for user accounts, groups, and computers
• Teams that manage and monitor the physical networks
• Team that manage DNS
• Security teams

The steps to creating a domain plan for a forest are:
• Determine the number of domains in each forest
• Choose a forest root domain
• Assign a DNS name to each domain to create a domain hierarchy
• Plan DNS server deployment
• Optimize authentication with short cut trusts
• Understand the impact of changes to the domain plan after deployment

Active Directory domains are named with DNS names that are the locator services for the Active Directory. Clients

query DNS to locate services such as LDAP and Kerberos Key Distribution Centers. Also, a client uses DNS to determine what site it is in and what site its domain controller is in.

3. Organization Unit Plan

OU is the logical presentation of Company organogram, departmental organogram and Site/divisional organogram. OU design and planning is another very complex aspect of the design. However, changes to the design after deployment, are relatively easy to accomplish. A well-designed OU plan will ensure a return on investment for your AD effort. The decisions on OU design, GPO, security groups, and delegation are critical; however these aspects of AD are designed to handle the changes to your directory.

Here are some reasons why complexity should be handled at the OU level.
• Changing the OU Structure is fairly easy
• OUs are very flexible when used in conjunction with security groups and Group Policy Objects
• OUs offer a type of security boundary
• GPOs as a parent OU are inherited by a child OU (remember this does not happen at the domain level: a child domain does not inherit policy from its parent domain in the domain name space)
• OUs can be delegated administration rights, thus saving the cost of adding a domain just for administrative reasons
• The initial OU design requirements can be influenced by the down level domain migration requirements. The OU infrastructure can be redesigned after the migration

4. Site and Services Plan

An Active Directory site topology is a logical representation of a physical networks (WAN & LAN). Site topology is defined on a per-forest basis. Active Directory clients and servers use the site topology of a forest to route query and replication traffic efficiently. A site topology also helps you to decide where to place domain controllers on your network. Keep the following definition in mind when designing the site plan.

A site is defined as a set of IP sub networks connected by fast reliable connectivity. As a rule of thumb, networks with LAN speed or better are considered as fast networks.

To create a site topology for a forest, use the following process:

- Define sites and site links using your physical topology as a starting point. (Site links are connection objects, used to connect two sites, which are normally connected as a Wide Area Network)
- Place servers into sites
- Understand how changes to your site topology after deployment will impact end users

How many parties involve in Site Design

- Teams that manage and monitor the TCP/IP networks. (Network Team)
- Domain administrators for each domain in the forest (Wintel Team)

Writable DC or RODC?

Certain domain and enterprise-wide operations that are not well suited to multi-master updates must be performed on a single

domain controller in the domain or in the forest. The purpose of having a single-master owner is to define a well-known target for critical operations and to prevent the introduction of conflicts or latency that could be created by multi-master updates. Having a single-operation master means that the relevant FSMO role owner must be online, discoverable, and available on the network by computers needing to perform FSMO dependent operations.

As per above statement, you can adopt HUB-SPOKE model with writable DC in Head Office and RODC in Site office with small number of users. However if you have sites with many users accessing DFS data, Printing and NTFS files randomly than its better to have writable DCs in all sites as well. If you are using MPLS service such as Telstra IP-WAN enterprise managed network than you definitely on a mesh WAN topology in that case you can happily have writable DCs on sites with mesh topology configured AD Sites and Services. However you are in SMB market with only several sites and low bandwidth than I would recommend RODC as your site domain controller.

Relate the design with your organization or corporate scenario

- Design 1: Single Forest with a Single Domain
- Design 2: Single Forest with Multiple Domains
- Design 3: Multiple Forests

Ask yourself/client the following questions and find correct answer not reasonable answer

- How many Forests?
- How Many Domains?
- What is the best DNS Design for the Domain Name space?
- What are the Security verses Ease of Management Tradeoffs?

Understand FSMO Role Holder's tasks and functionality: The operations masters, their scope and functionality are shown in the following table.

FSMO Role	Scope	Function and availability requirements
Schema Master	Enterprise	▪ Used to introduce manual and programmatic schema updates, and this includes those updates that are added by Windows ADPREP /FORESTPREP, by Microsoft Exchange, and by other applications that use Active Directory Domain Services (AD DS). ▪ Must be online when schema updates are performed.
Domain Naming Master	Enterprise	▪ Used to add and to remove domains and application partitions to and from the forest. ▪ Must be online when domains and application partitions in a forest are added or removed.
Primary Domain Controller	Domain	▪ Receives password updates when passwords are changed for the computer and for user accounts that are on replica domain controllers. ▪ Consulted by replica domain controllers that service authentication requests that have mismatched passwords.

		▪ Default target domain controller for Group Policy updates. ▪ Target domain controller for legacy applications that perform writable operations and for some admin tools. ▪ Must be online and accessible 24 hours a day, seven days a week.
RID	Domain	▪ Allocates active and standby RID pools to replica domain controllers in the same domain. ▪ Must be online for newly promoted domain controllers to obtain a local RID pool that is required to advertise or when existing domain controllers have to update their current or standby RID pool allocation.
Infrastructure Master	Domain Application partition	▪ Updates cross-domain references and phantoms from the global catalog. For more information, click the following article number to view the article in the Microsoft Knowledge Base: 248047 Phantoms, tombstones and the infrastructure master ▪ A separate infrastructure master is created for each application partition including the default forest-wide and domain-wide application partitions created by Windows Server 2003 and later domain controllers. The Windows Server 2008 R2 ADPREP /RODCPREP command targets the infrastructure master role for default DNS application in the forest root domain. The DN path for this role holder is CN=Infrastructure,DC=DomainDnsZones,DC=<forest root domain>,DC=<top level domain> and CN=Infrastructure,DC=ForestDnsZones,DC=<forest root domain>,DC=<top level domain>.

Who owns what FSMO Roles & Where to place FSMO Roles

When the Active Directory Installation Wizard (Dcpromo.exe) creates the first domain in a new forest, the wizard adds five FSMO roles. A forest with one domain has five roles. The Active Directory Installation Wizard adds three domain-wide roles on the first domain controller in each additional domain in the forest. In addition, infrastructure master roles exist for each application partition. This includes the default domain and the forest-wide DNS application partitions that are created on Windows Server 2003 and on later domain controllers.

The Active Directory Installation Wizard performs the initial placement of roles on domain controllers. This placement is frequently correct for directories that have just a few domain controllers. In a directory that has

many domain controllers, the default placement may not be the best match for your network.

Consider the following in your selection criteria:

- It is easier to keep track of FSMO roles if you host them on fewer computers.
- Place roles on domain controllers that are can be accessed by the computers that need access to a given role, especially on networks that are not fully routed. For example, to obtain a current or standby RID pool, or perform pass-through authentication, all DCs need network access to the RID and PDC role holders in their respective domains.
- If a role has to be moved to a different domain controller, and the current role holder is online and available, you should transfer (not seize) the role to the new domain controller. FSMO roles should only be sized if the current role holder is not available.
- FSMO roles that are assigned to domain controllers that are offline or in an error state only have to be transferred or seized if role-dependent operations are being performed. If the role holder can be made operational before the role is needed, you may delay seizing the role. If role availability is critical, transfer or seize the role as required. The PDC role in each domain should online 24×7.
- Select a direct intra-site replication partner for existing role holders to act as a standby role holder. If the primary owner goes offline or fails, transfer or seize the role to the designated standby FSMO domain controller as required.

General recommendations for FSMO placement

- Place the schema master on the PDC of the forest root domain.
- Place the domain naming master on the forest root PDC.
  The addition or removal of domains should be a tightly controlled operation. Place this role on the forest root PDC. Certain operations that use the domain naming master, such as creating or removing domains and application partitions, fail if the domain naming master is not available. On a domain controller that runs Microsoft Windows 2000, the domain naming master must also be hosted on a global catalog server. On domain controllers that run Windows Server 2003 or later versions, the domain naming master does not have to be a global catalog server.
- Place the PDC on your best hardware in a reliable hub site that contains replica domain controllers in the same Active Directory site and domain.
- In large or busy environments, the PDC frequently has the highest CPU utilization because it handles pass-thru authentication and password updates. If high CPU utilization becomes a problem, identify the source, and this includes applications or computers that may be performing too many operations (transitively) targeting the PDC.
- All domain controllers in a given domain, and computers that run applications and admin tools that target the PDC, must have network connectivity to the domain PDC.
- Place the RID master on the domain PDC in the same domain.
  RID master overhead is light, especially in mature domains that have already created the bulk of their users, computers, and groups. The domain PDC typically receives the most attention from administrators, therefore, co-locating this role on the PDC helps insure good availability. Make sure that existing domain controllers and newly promoted domain controllers, especially those promoted in remote or staging sites, have network connectivity to obtain active and standby RID pools from the RID master.
- Legacy guidance suggests placing the the infrastructure master on a non-global catalog server. There are two

rules to consider:

- Single domain forest:
  In a forest that contains a single Active Directory domain, there are no phantoms. Therefore, the infrastructure master has no work to do. The infrastructure master may be placed on any domain controller in the domain, regardless of whether that domain controller hosts the global catalog or not.
- Multi-domain forest:
  If every domain controller in a domain that is part of a multi-domain forest also hosts the global catalog, there are no phantoms or work for the infrastructure master to do. The infrastructure master may be put on any domain controller in that domain. In practical terms, most administrators host the global catalog on every domain controller in the forest.
- If every domain controller in a given domain that is located in a multi-domain forest does not host the global catalog, the infrastructure master must be placed on a domain controller that does not host the global catalog.

Techniques to reduce CPU include the following:

- adding more or faster CPUs
- Adding additional replicas
- Adding additional memory to cache Active Directory objects
- Removing the global catalog to avoid global catalog lookups
- Reducing the number of incoming and outgoing replication partners
- Increasing the replication schedule
- Reducing authentication visibility by using LDAPSRVWEIGHT and LDAPPRIORITY that is described in KB296716 and the Randomize1CList described in KB231305

In short human readable English language I would recommend follow the following FSMO roles structure.

Domain Controller 1: Place the two forest roles on this server.

- Schema Master
- Domain Master

Domain Controller 2 Place the three domain roles on this server.

- RID Master
- Infrastructure Master
- PDC Emulator

Global Catalog Rules:

Rule#1: The Infrastructure Master (IM) role should be held by a domain controller that is not a Global Catalog server(GC). If the Infrastructure Master runs on a Global Catalog server it will stop updating object information because it does not contain any references to objects that it does not hold. This is because a Global Catalog server holds a partial replica of every object in the forest. As a result, cross-domain object references in that domain will not be updated and a warning to that effect will be logged on that DC's event log.

Rule#2: If all the domain controllers in a domain also host the global catalog, all the domain controllers have the current data, and it is not important which domain controller holds the infrastructure master role. In simple plain English yes you configure IM FSMO role holder a GC if all DCs are GC.

Group Policy Hierarchy Best Practice:

Group Policy(s) will flow down a hierarchy in the following order:
• Site
• Domain
• OU

The following are key element of Active Directory Users and Computer Policy:

• Password Policies, such as password length, password expiry interval and so forth
• Account Lockout Policies
• Kerberos policies
• Encrypted file system recovery policies
• IP security policies
• Public Key encryption policies
• Certificate authorities

Default Domain Policy determination

- Encrypted File System Recovery Policies
- IP Security Policies
- Public Key Infrastructure Policies
- Certificate Authorities
- Password Policy
- Account Lockout Policy
- Kerberos Policies

How long can a PDC and DC be offline? In theory, you can take PDC master offline for tombstone lifetime period and get away with warnings, but without breaking anything.
By default the DCs will look for PDCE as authoritative time source and you will have issues related to editing GPOs, but as long as you do not have legacy clients, you can take the PDCE down for up to 60 days pre-W2K3 SP1 environment (DCs) and for 180 days if all the DCs are W2K3 SP1.

Another issue would have to do with password chaining – if PDCE is down, you might get temporary authentication failures after changing user passwords. see the KB for details on how password chaining works.

However in practice you shouldn't shutdown a DC for longer than necessary that may create lot of issues such as replication issue and authentication issues for site users. You can patch and update a domain controller using SCCM/WSUS and reboot the DC without any issues.

Transferring the Flexible Single Master Operation Role

The transfer of an FSMO role is the suggested form of moving a FSMO role between domain controllers and can be initiated by the administrator or by demoting a domain controller, but is not initiated automatically by the operating system. This includes a server in a shut-down state. FSMO roles are not automatically relocated during the shutdown process–this must be considered when shutting down a domain controller that has an FSMO role for maintenance, for example.

In a graceful transfer of an FSMO role between two domain controllers, a synchronization of the data that is maintained by the FSMO role owner to the server receiving the FSMO role is performed prior to transferring the role to ensure that any changes have been recorded before the role change.

Operational attributes are attributes that translate into an action on the server. This type of attribute is not defined in the schema, but is instead maintained by the server and intercepted when a client attempts to read or write to it. When the attribute is read, generally the result is a calculated result from the server. When the attribute is written, a pre-defined action occurs on the domain controller.

The following operational attributes are used to transfer FSMO roles and are located on the RootDSE (or Root DSA Specific Entry–the root of the Active Directory tree for a given domain controller where specific information about the domain controller is kept). In the operation of writing to the appropriate operational attribute on the domain controller to receive the FSMO role, the old domain controller is demoted and and the new domain controller is promoted automatically. No manual intervention is required. The operational attributes that represent the FSMO roles are:

becomeRidMaster
becomeSchemaMaster
becomeDomainMaster
becomePDC
becomeInfrastructureMaster

If the administrator specifies the server to receive the FSMO role using a tool such as Ntdsutil, the exchange of the FSMO role is defined between the current owner and the domain controller specified by the administrator. When a domain controller is demoted, the operational attribute “GiveAwayAllFsmoRoles” is written, which triggers the domain controller to locate other domain controllers to offload any roles it currently owns. Windows 2000 determines which roles the domain controller being demoted currently owns and locates a suitable domain controller by following these rules:

1. Locate a server in the same site.
2. Locate a server to which there is RPC connectivity.
3. Use a server over an asynchronous transport (such as SMTP).

In all transfers, if the role is a domain-specific role, the role can be moved only to another domain controller in the same domain. Otherwise, any domain controller in the enterprise is a candidate.

Seizing the Flexible Single Master Operation Role

Administrators should use extreme caution in seizing FSMO roles. This operation, in most cases, should be

performed only if the original FSMO role owner will not be brought back into the environment.
When the administrator seizes an FSMO role from an existing computer, the “fsmoRoleOwner” attribute is modified on the object that represents the root of the data directly bypassing synchronization of the data and graceful transfer of the role. The “fsmoRoleOwner” attribute of each of the following objects is written with the Distinguished Name (DN) of the NTDS Settings object (the data in the Active Directory that defines a computer as a domain controller) of the domain controller that is taking ownership of that role. As replication of this change starts to spread, other domain controllers learn of the FSMO role change.

Primary Domain Controller (PDC) FSMO:

LDAP://DC=MICROSOFT,DC=COM

RID Master FSMO:

LDAP://CN=Rid Manager$,CN=System,DC=MICROSOFT,DC=COM

Schema Master FSMO:

LDAP://CN=Schema,CN=Configuration,DC=Microsoft,DC=Com

Infrastructure Master FSMO:

LDAP://CN=Infrastructure,DC=Microsoft,DC=Com

Domain Naming Master FSMO:

LDAP://CN=Partitions,CN=Configuration,DC=Microsoft,DC=Com

For example, if Server1 is the PDC in the MicrosoftGuru.com.au domain and is retired and the administrator is unable to demote the computer properly, Server2 needs to be assigned the FSMO role of the PDC. After the seizure of the role takes place, the value

CN=NTDS Settings,CN=SERVER2,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=Microsoft,DC=Com

is present on the following object: LDAP://DC=MICROSOFTGURU,DC=COM,DC=AU

How to Fix ForestDnsZones and DomainDnsZones after failed demotion attempt

cscript fixfsmo.vbs DC=DomainDnsZones,DC=contoso,DC=com

cscript fixfsmo.vbs DC=ForestDnsZones,DC=contoso,DC=com

Can I change Active Directory Schema using ADSIEDIT? yes you can change Active Directory Schema using ADSIedit tools.

Microsoft recommend that you transfer FSMO roles in the following scenarios:

- The current role holder is operational and can be accessed on the network by the new FSMO owner.
- You are gracefully demoting a domain controller that currently owns FSMO roles that you want to assign to a specific domain controller in your Active Directory forest.
- The domain controller that currently owns FSMO roles is being taken offline for scheduled maintenance and you need specific FSMO roles to be assigned to a “live” domain controller. This may be required to perform operations that connect to the FSMO owner. This would be especially true for the PDC Emulator role but less true for the RID master role, the Domain naming master role and the Schema master roles.

Microsoft recommend that you seize FSMO roles in the following scenarios:

- The current role holder is experiencing an operational error that prevents an FSMO-dependent operation from completing successfully and that role cannot be transferred.
- A domain controller that owns an FSMO role is force-demoted by using the **dcpromo /forceremoval** command.
- The operating system on the computer that originally owned a specific role no longer exists or has been reinstalled.

The partition for each FSMO role is in the following list:

FSMO role	Partition
Schema	CN=Schema,CN=configuration,DC=microsoftguru,dc=com,dc=au
Domain Naming Master	CN=configuration,DC=microsoftguru,dc=com,dc=au
PDC	DC=microsoftguru,dc=com,dc=au
RID	DC=microsoftguru,dc=com,dc=au
Infrastructure	DC=microsoftguru,dc=com,dc=au

How to View/create/remove a new global catalog on the destination global catalog server

1. On the domain controller where you want the new global catalog, start the Active Directory Sites and Services snap-in. To start the snap-in, click Start, point to Programs, point to Administrative Tools, and then click Active Directory Sites and Services.
2. In the console tree, double-click Sites, and then double-click *sitename*.
3. Double-click Servers, click your domain controller, right-click NTDS Settings, and then click Properties.
4. On the General tab, click to select the Global catalog check box to assign the role of global catalog to this server. Deselect the Global Catalog check box to remove GC from the DC.
5. Restart the domain controller.

How to view and transfer FSMO roles in Windows Active Directory

1. Click Start, and then click Run.
2. Type regsvr32 schmmgmt.dll in the Open box, and then click OK.
3. Click OK when you receive the message that the operation succeeded.

Transfer the Schema Master Role

1. Click Start, click Run, type mmc in the Open box, and then click OK.
2. On the File, menu click Add/Remove Snap-in.
3. Click Add.
4. Click Active Directory Schema, click Add, click Close, and then click OK.
5. In the console tree, right-click Active Directory Schema, and then click Change Domain Controller.
6. Click Specify Name, type the name of the domain controller that will be the new role holder, and then click OK.
7. In the console tree, right-click Active Directory Schema, and then click Operations Master.
8. Click Change.
9. Click OK to confirm that you want to transfer the role, and then click Close.

Transfer the Domain Naming Master Role

1. Click Start, point to Administrative Tools, and then click Active Directory Domains and Trusts.
2. Right-click Active Directory Domains and Trusts, and then click Connect to Domain Controller.
   NOTE: You must perform this step if you are not on the domain controller to which you want to transfer the role. You do not have to perform this step if you are already connected to the domain controller whose role you want to transfer.
3. Do one of the following:
   - In the Enter the name of another domain controller box, type the name of the domain controller that will be the new role holder, and then click OK.
     -or-
   - In the Or, select an available domain controller list, click the domain controller that will be the new role holder, and then click OK.
4. In the console tree, right-click Active Directory Domains and Trusts, and then click Operations Master.
5. Click Change.
6. Click OK to confirm that you want to transfer the role, and then click Close.

Transfer the RID Master, PDC Emulator, and Infrastructure Master Roles

1. Click Start, point to Administrative Tools, and then click Active Directory Users and Computers.
2. Right-click Active Directory Users and Computers, and then click Connect to Domain Controller.
   NOTE: You must perform this step if you are not on the domain controller to which you want to transfer the role. You do not have to perform this step if you are already connected to the domain controller whose role you want to transfer.
3. Do one of the following:
   - In the Enter the name of another domain controller box, type the name of the domain controller that will be the new role holder, and then click OK.
     -or-
   - In the Or, select an available domain controller list, click the domain controller that will be the new role holder, and then click OK.
4. In the console tree, right-click Active Directory Users and Computers, point to All Tasks, and then click Operations Master.
5. Click the appropriate tab for the role that you want to transfer (RID, PDC, or Infrastructure), and then click Change.

6. Click OK to confirm that you want to transfer the role, and then click Close.

Transfer FSMO roles using ntdsutil

- Click Start, click Run, type ntdsutil in the Open box, and then click OK.
- Type roles, and then press ENTER
- Type connections, and then press ENTER
- Type Connect to Server ServerName and Press Enter
- At the server connections prompt, type q, and then press ENTER
- Type transfer *role*, where *role* is the role that you want to transfer. For a list of roles that you can transfer, type ? at the fsmo maintenance prompt, and then press ENTER,
- At the fsmo maintenance prompt, type q, and then press ENTER to gain access to the ntdsutil prompt. Type q, and then press ENTER to quit the Ntdsutil utility

To seize the FSMO roles by using the Ntdsutil utility, follow these steps:

- Click Start, click Run, type ntdsutil in the Open box, and then click OK.
- Type roles, and then press ENTER.
- Type connections, and then press ENTER.
- Type connect to server *servername*, and then press ENTER, where *servername* is the name of the domain controller that you want to assign the FSMO role to.
- At the server connections prompt, type q, and then press ENTER.
- Type seize *role*, where *role* is the role that you want to seize. For a list of roles that you can seize, type ? at the fsmo maintenance prompt, and then press ENTER,
- At the fsmo maintenance prompt, type q, and then press ENTER to gain access to the ntdsutil prompt. Type q, and then press ENTER to quit the Ntdsutil utility.
  Notes

Important KBs and Readings

Repadmin Examples and Dcdiag Examples

Best Practices Analyzer for Active Directory Domain Services

Microsoft Premier Field Engineering Platform Reporting Tool (MPS_REPORTS)

Microsoft Product Support Reports Viewer 2.0

Best Practice Active Directory Design for Managing Windows Networks

Windows 2000 Active Directory FSMO roles

FSMO placement and optimization on Active Directory domain controllers

Flexible Single Master Operation Transfer and Seizure Process

Phantoms, tombstones and the infrastructure master

How to view and transfer FSMO roles in Windows Server 2003

Managing Operations Master Roles

How to remove data in active directory after an unsuccessful domain controller demotion

FSMO placement and optimization on Windows 2000 domain controllers

Using Ntdsutil.exe to transfer or seize FSMO roles to a domain controller

About Raihan Al-Beruni

My Name is Raihan Al-Beruni. I am working as an Infrastructure Architect in Data Center Technologies in Perth, Western Australia. I have been working on Microsoft technologies for more than 15 years. Other than Microsoft technologies I also work on Citrix validated solution and VMware data center virtualization technologies. I have a Masters degree in E-Commerce. I am certified in Microsoft, VMware, ITIL and EMC. My core focus is on cloud technologies. In my blog I share my knowledge and experience to enrich information technology community as a whole. I hope my contribution through this blog will help someone who wants more information on data center technologies.

View all posts by Raihan Al-Beruni →