FSMO placement and optimization on Active Directory domain controllers

http://support.microsoft.com/kb/223346

Summary

This article describes the placement of Active Directory Flexible Single-Master (FSMO) roles in the domain and forest for operations that are best performed on a single domain controller.

More information

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 that have to perform FSMO-dependent operations.

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. Additionally, 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-later domain controllers. The operations masters and their scope 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>.

FSMO availability and placement

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's 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 seized if the current role holder is not available. For more information, go to the following Microsoft website:

  http://technet.microsoft.com/en-us/library/cc816945(WS.10).aspx

- 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 at all times.
- Select a direct intrasite 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. 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, and by using the Randomize1CList feature that's described in 231305.

  All domain controllers in a particular 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 ensure reliable 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 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.
  - Multidomain forest:

    If every domain controller in a domain that is part of a multidomain 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 multidomain forest does not host the global catalog, the infrastructure master must be placed on a domain controller that does not host the global catalog.