Planning Operations Master Role Placement

Updated: April 26, 2012

Applies To: Windows Server 2008, Windows Server 2008 R2, Windows Server 2012

Active Directory Domain Services (AD DS) supports multimaster replication of directory data, which means any domain controller can accept directory changes and replicate the changes to all other domain controllers. However, certain changes, such as schema modifications, are impractical to perform in a multimaster fashion. For this reason certain domain controllers, known as operations masters, hold roles responsible for accepting requests for certain specific changes.

Note
Operations master role holders must be able to write some information to the Active Directory database. Because of the read-only nature of the Active Directory database on a read-only domain controller (RODC), RODCs cannot act as operations master role holders.

Three operations master roles (also known as flexible single master operations or FSMO) exist in each domain:

- The primary domain controller (PDC) emulator operations master processes all password updates.
- The relative ID (RID) operations master maintains the global RID pool for the domain and allocates local RIDs pools to all domain controllers to ensure that all security principals created in the domain have a unique identifier.
- The infrastructure operations master for a given domain maintains a list of the security principals from other domains that are members of groups within its domain.

In addition to the three domain-level operations master roles, two operations master roles exist in each forest:

- The schema operations master governs changes to the schema.
- The domain naming operations master adds and removes domains and other directory partitions (for example, Domain Name System (DNS) application partitions) to and from the forest.

Place the domain controllers hosting these operations master roles in areas where network reliability is high, and ensure that the PDC emulator and the RID master are consistently available.

Operations master role holders are assigned automatically when the first domain controller in a given domain is created. The two forest-level roles (schema master and domain naming master) are assigned to the first domain controller created in a forest. In addition, the three domain-level roles (RID master, infrastructure master, and PDC emulator) are assigned to the first domain controller created in a domain.

Note
Automatic operations master role holder assignments are made only when a new domain is created and when a current role

holder is demoted. All other changes to role owners have to be initiated by an administrator.

These automatic operations master role assignments can cause very high CPU usage on the first domain controller created in the forest or the domain. To avoid this, assign (transfer) operations master roles to various domain controllers in your forest or domain. Place the domain controllers that host operations master roles in areas where the network is reliable and where the operations masters can be accessed by all other domain controllers in the forest.

You should also designate standby (alternate) operations masters for all operations master roles. The standby operations masters are domain controllers to which you could transfer the operations master roles in case the original role holders fail. Ensure that the standby operations masters are direct replication partners of the actual operations masters.

Planning the PDC emulator placement

The PDC emulator processes client password changes. Only one domain controller acts as the PDC emulator in each domain in the forest.

Even if all the domain controllers are upgraded to Windows 2000, Windows Server 2003, and Windows Server 2008, and the domain is operating at the Windows 2000 native functional level, the PDC emulator receives preferential replication of password changes performed by other domain controllers in the domain. If a password was recently changed, that change takes time to replicate to every domain controller in the domain. If logon authentication fails at another domain controller due to a bad password, that domain controller forwards the authentication request to the PDC emulator before deciding whether to accept or reject the logon attempt.

Place the PDC emulator in a location that contains a large number of users from that domain for password forwarding operations if needed. In addition, ensure that the location is well connected to other locations to minimize replication latency.

For a worksheet to assist you in documenting the information about where you plan to place PDC emulators and the number of users for each domain that is represented in each location, see Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink/?LinkID=102558), download Job_Aids_Designing_and_Deploying_Directory_and_Security_Services.zip, and open Domain Controller Placement (DSSTOPO_4.doc).

You need to refer to the information about locations in which you need to place PDC emulators when you deploy regional domains. For more information about deploying regional domains, see Deploying Windows Server 2008 Regional Domains.

Requirements for infrastructure master placement

The infrastructure master updates the names of security principals from other domains that are added to groups in its own domain. For example, if a user from one domain is a member of a group in a second domain and the user's name is changed in the first domain, the second domain is not notified that the user's name must be updated in the group's membership list. Because domain controllers in one domain do not replicate security principals to domain controllers in another domain, the second domain never becomes aware of the change in the absence of the infrastructure master.

The infrastructure master constantly monitors group memberships, looking for security principals from other domains. If it finds one, it checks with the security principal's domain to verify that the information is updated. If the information is out of date, the infrastructure master performs the update and then replicates the change to the other domain controllers in its domain.

Two exceptions apply to this rule. First, if all domain controllers are global catalog servers, the domain controller that hosts the infrastructure master role is insignificant because global catalogs replicate the updated information regardless of the domain to which they belong. Second, if the forest has only one domain, the domain controller that hosts the infrastructure master role is insignificant because security principals from other domains do not exist.

Do not place the infrastructure master on a domain controller that is also a global catalog server. If the infrastructure master and global catalog are on the same domain controller, the infrastructure master will not function. The infrastructure master will never find data that is out of date; therefore, it will never replicate any changes to the other domain controllers in the domain.

Operations master placement for networks with limited connectivity

Be aware that if your environment does have a central location or hub site in which you can place operations master role holders, certain domain controller operations that depend on the availability of those operations master role holders might be affected.

For example, suppose that an organization creates sites A, B, C, and D. Site links exist between A and B, between B and C, and between C and D. Network connectivity exactly mirrors the network connectivity of the sites links. In this example, all operations master roles are placed in site A and the option to **Bridge all site links** is not selected.

Although this configuration results in successful replication between all of the sites, the operations master role functions have the following limitations:

- Domain controllers in sites C and D cannot access the PDC emulator in site A to update a password or to check it for a password that has been recently updated.
- Domain controllers in sites C and D cannot access the RID master in site A to obtain an initial RID pool after the Active Directory installation and to refresh RID pools as they become depleted.
- Domain controllers in sites C and D cannot add or remove directory, DNS, or custom application partitions.
- Domain controllers in sites C and D cannot make schema changes.

For a worksheet to assist you in planning operations master role placement, see Job Aids for Windows Server 2003 Deployment Kit (http://go.microsoft.com/fwlink/?LinkID=102558), download Job_Aids_Designing_and_Deploying_Directory_and_Security_Services.zip, and open Domain Controller Placement (DSSTOPO_4.doc).

You will need to refer to this information when you create the forest root domain and regional domains. For more information about deploying the forest root domain, see Deploying a Deploying a Windows Server 2008 Forest Root Domain. For more information about deploying regional domains, see Deploying Windows Server 2008 Regional Domains.

Community Additions