Ad design scenario

Design

Two domain controllers are recommended for environments of up to 200 users. It is important to not have the Domain Naming Master on the same server as the RID Master or the PDP Master, because if it stopped working it would be difficult to create a new DC to replace the failed DC as the Domain Naming Master must be live to use promote/ create a new DC. The PDP (Primary Domain Controller) Master and RID (Relative Identifier) Master are the roles that have the biggest initial impact on the environment if lost to both users and Systems Administrators. 2.

What servers/server re global catalog servers? All domain controllers can be a global catalog. When every domain controllers is a global catalog it does increase the replication work load, but this has minimal impact and speeds up the performance of AD. The global catalog provides the ability to locate objects from any domain without having to know the domain name. A global catalog server is a domain controller that, in addition to its full, writable domain directory partition replica, and it stores a partial, read-only replica of all other domain directory partitions in the forest.

The additional domain rectory partitions are partial because only a limited set of attributes is included for each object. By including only the attributes that are most used for searching, every object in every domain in even the largest forest can be represented in the database of a single global catalog server. 3. Do you have a single or multiple domain forest? In a single domain forest I would recommend that we leave all the FSML roles on the first controller in the forest and I would make all of the domain controllers global catalog servers.

In a multiple domain forest I would use the following guidelines: In he forest root domain: If all domain controllers are also global catalog servers, I would leave all of the FSML roles on the first DC in the forest. If the domain controllers are not global catalog servers, I would move all of the FSML roles to a domain controller that is not a global catalog server. In each child domain, I will leave the PDP emulator, RID master, and Infrastructure master roles on the first DC in the domain, and ensure that this DC is never designated as a global catalog server unless the child domain only contains one DC. . Do you have any sites in remote regions? Sites with slow connections will hinder the effectiveness of replication. 5. Where are you going to place the domain controllers that have these roles installed on them? I need to know this because we are going to have to put the domain controllers hosting these operations master roles in areas where network reliability is high, and ensure that the PDP 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 main naming master, are assigned to the first domain controller created in a forest and the three domain-level roles, RID master, infrastructure master, and PDP emulator are assigned to the first domain controller created in a domain. Forest-wide Operations Master Roles Every forest must have the following roles: Schema master and Domain naming master.

The schema is the Active Directory component that defines all the objects and attributes that the directory service uses to store data. These roles must be unique in the forest which means that in the entire forest there can be only one chem. master and one domain naming master. The schema master domain controller controls all updates and modifications to the schema. To update the schema of a forest, you must have access to the schema master. The domain controller holding the domain naming master role controls the addition or removal of domains in the forest.

Domain-wide operations master roles Every domain in the forest must have the following roles, relative ID (RID) master, primary domain controller (PDP) emulator master, and Infrastructure master These roles must be unique in each domain which means that each domain in the forest an have only one RID master, PDP emulator master, and infrastructure master. The RID master allocates sequences of relative IDs (RIDS) to each of the various domain controllers in its domain. At any time, there can be only one domain controller acting as the RID master in each domain in the forest.

Whenever a domain controller creates a user, group, or computer object, it assigns the object a unique security ID (SIDED). The SIDED consists of a domain SIDED, which is the same for all KIDS created in the domain, and a RID, which is unique for each SIDED created in the domain. To move an object between domains (using Movers. Ex), you must initiate the move on the domain controller acting as the RID master of the domain that currently contains the object. The PDP emulator master processes password changes from client computers and replicates these updates to all domain controllers throughout the domain.

At any time, there can be only one domain controller acting as the PDP emulator master in each domain in the forest. The PDP emulator role is used in the following ways: To provide consistent password experience for users across sites, the PDP emulator is used as a reference DC to double-check incorrect swords and it receives new password changes. When the PDP is reachable, users can use a new password immediately and consistently across the environment and as a point of contact for applications hard-coded to the PDP.

It can also be used as a default time server for all other Docs in the domain - The time server configuration of a PDP requires manual consideration and should be reviewed when you change the owner of the PDP role. At any time, there can be only one domain controller acting as the infrastructure master in each domain. The infrastructure master is responsible for updating preferences from objects in its domain to objects in other domains. The infrastructure master compares its data with that of a global catalog.

Global catalogs receive regular updates for objects in all domains through replication, so the global catalog data will always be up to date. If the infrastructure master finds data that is out of date, it requests the updated data from a global catalog. The infrastructure master then replicates that updated data to the other domain controllers in the domain. The infrastructure master is also responsible for updating the group-to-user references whenever the members of groups are renamed or changed.

When you rename or move a member of a group (and that member resides in a different domain from the group), the group may temporarily appear not to contain that member. The infrastructure master of the group's domain is responsible for updating the group so it knows the new name or location of the member. This prevents the loss of group memberships associated with a user account when the user account is renamed or moved. The infrastructure master distributes the update via MultiMate replication. There is no compromise to security during the time between the member rename and the group update.