# Domain Controller virtualization solutions - Part 2

In Part 2 of this series, I will continue the discussion by showing you some options for domain controller virtualization.

**In the second part of this article series, I will continue the discussion by showing you some options for domain controller virtualization.**

At the end of Part 1, I talked about the ability to create a completely independent Active Directory forest to manage your virtual hosts. The advantage of this approach is that it allows you to virtualize all your production domain controllers while still using Active Directory dependency management tools.

Although there are some drawbacks to placing your virtual hosts in a dedicated forest. As we alluded to in the previous section, one of the major disadvantages is the requirement of infrastructure. In other words, a dedicated forest will require separate domain controllers, separate DNS servers, and it may also require other types of infrastructure servers such as patch management servers, antivirus management, or backup.

Another disadvantage in creating a dedicated forest for virtual hosts is the disconnection between the virtual forest and the production forest. Depending on your network configuration, this disconnection may prevent the sharing of Active Directory information between the two forests. This can be difficult to resolve if you are using a backup solution that relies on Active Directory and wants to backup servers from both forests.

Even if you don't care about Active Directory isolation caused by using multiple forests, the infrastructure requirement involved in creating a completely independent forest for virtualized hosts may be makes you wonder whether using this method is worth your effort. There is really no strategy for virtualization and organization of domain controllers is perfect. However, there are a few things you can do to make this method a little more appealing.

One method you can use here is to configure two physical servers to work as domain controllers for the production domain. You can then configure one of the two physical domain controllers to work as an Active Directory integrated DNS server.

When you complete this configuration, you can join your host servers into the production domain without having to worry about the 'previous or previous eggs' rebellion. You can safely perform virtualization of all your domain controllers, except for two domain controllers that have just been set up. Clearly in this way, we have acknowledged that the forest being addressed includes only one domain. In the later part of this series, we will cover multiple domain virtualization modes, but now we just want to simplify things by using a domain forest.

The underlying factor behind using this method is that it protects you from host host errors (at least a few levels). We assume that two physical domain controllers do not exist and that you have virtualized all your other domain controllers. Depending on how you configure these domain controllers, you may have a situation where the host server error will cause your virtualized domain controllers to become inaccessible, so it will prevent posting.

enter the network. Having two separate physical domain controllers will ensure that users can log on to the network even when the entire virtualization infrastructure fails.

Clearly simplifying the number of two physical domain controllers is not enough. As you can see, we mentioned that one of these two servers needs to be configured as a DNS server. Until now, we have not configured any machines on our network to use it like that. The advice here is to set up this server as the second DNS server. That way, hosts on your network will still be able to use the primary DNS server. In case your main DNS server or the host it resides on fails, the physical DNS server can still handle DNS queries in the network until the situation is fixed.

Another issue that you need to consider is whether or not to follow this approach in the Flexible Single Master Operation roles. Windows 2000 Server and recent versions use multi master replication mode, where updates to the Active Directory database can be overwritten into any available domain controller. However, some domain controllers are considered more important than some other domain controllers. Domain controllers assigned to the Flexible Single Master Operation roles will be responsible for maintaining the integrity of Active Directory. For example, the domain controller holding the Schema Master will be responsible for maintaining the Active Directory schema. All schema changes will be overwritten on this domain controller.

We will not turn this article into an in-depth discussion of the Flexible Single Master Operations role and their functions, only mentioning the replacement of the Flexible Single Master Operation role within the virtualized environment.

As you know, there are two types of Flexible Single Master Operation roles; domain level role and forest level role. When you create an Active Directory forest, the first domain controller that you set up is automatically assigned all roles at the forest level (forest level role) and all domain roles (domain level role) to the domain you have create. If you create additional domains within forest, the first domain controller in each domain will be assigned domain level roles for that domain.

With that in mind, let's go back to our virtualization mode with two physical domain controllers and all domain controllers have been virtualized. Let us continue to assume that this mode is applied to a forest consisting of only one single domain.

Since all existing domain controllers are virtualized, it also means that all flexible single master operation roles are being configured on the virtual domain controller. Since Active Directory cannot be done long without accessing the domain controller, where the roles are assigned, we need to be concerned about whether or not we virtualize this domain controller.

In our view, there is no disadvantage in virtualizing domain controllers that are keeping flexible single master operations roles. Although the host servers may fail, making the domain controller fail with it, physical servers may also fail.

The reason why we believe domain controller virtualization includes Flexible Single Master Operations roles is safe because the error with this domain controller will not be disastrous (assuming there are several other domain controllers on the network). As long as some domain controllers and a DNS server remain on your network, Active Directory will continue to function normally for a while.

If the error appears to indicate that recovery is not possible, you can remove the flexible single master operations role from the failed domain controller and assign roles to the working domain controller. This capability will be safer if you virtualize domain controllers even if they have flexible single master operations roles.

## Conclude

In this article, I have shown you some of the advantages of using a physical server to perform tasks such as domain controllers, which also cover the security of using domains. The controller has been assigned a flexible single master operations role. In the third part of this series, we will continue the discussion of the domain controller replacement mode and the replacement of the global catalog server.