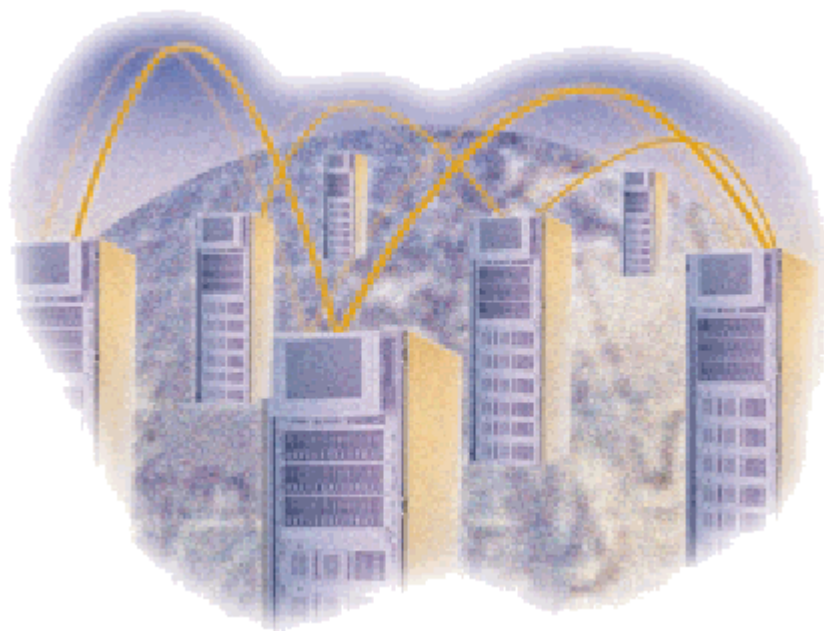




Domain Controller Failover When Using Active Directory



Domain Controller Failover When Using Active Directory published January 2002

NSI and Double-Take are registered trademarks of Network Specialists, Inc. All other products are trademarks of their respective companies. © 1996–2002 NSI Software

Double-Take Support for Application Failover

Double-Take's file system replication process is application independent and replicates any file system changes (including permissions and attributes) written to NTFS, FAT or FAT32 file systems by any application or process, subject to specific exceptions called out in the *User's Guide* or *readme.txt* file. Maintaining point-in-time consistent file system replicas and providing server monitoring and automatic or manual failover of the server name and IP address are the primary functions of the Double-Take software and we offer support to qualified customers should these functions fail to operate in accordance with our published documentation, regardless of what application or process is manipulating the data.

NSI Software may provide application notes and other documents that provide implementation guidelines on how to use Double-Take functions and replicas to manually or automatically failover or recover many popular third party applications and a general process to accomplish failover or recovery of many other third party applications. While these steps are believed to be accurate for the specific configuration, Double-Take version, and application versions originally tested, due to the number of possible configurations and variables, NSI Software can only test selected combinations and may provide only limited support for the operation and configuration of third party applications or the behavior of those applications before, during, or after failover, in its discretion. In cases where NSI Software has no direct access to or experience with a particular application or configuration, NSI Software support may also be limited to only the actual replication of the file system data and failover (name and IP address) of the server.

For assistance in validating, implementing or troubleshooting these or other possible configurations with third party applications, NSI Software and its partners may offer professional services on a fee basis to apply best practices for assisting with third party applications to recover automatically or manually using replicated data.

This, and any other, application note is provided solely for the convenience of our customers and is not intended to bind NSI Software to any obligation.

Table of Contents

Introduction	1
Configuring Failover	2
Configuring the User Account Running the Double-Take Service	6

Introduction

Active Directory catalogs information about all the objects on a network, including people, computers, and printers, and distributes that information throughout your network. Security is integrated with Active Directory through logon authentication and access control. Active Directory gives network users access to permitted resources anywhere on the network using a single logon process. It provides network administrators with an intuitive hierarchical view of the network and a single point of administration for all network objects.

To achieve this level of access for services, Active Directory clients use the Service Principal Names (SPN) directory property to locate a target principal name for a service. It is not usually necessary to modify SPNs. They are set up by a computer when it joins a domain and when services are installed on the computer. In some cases, however, this information can become obsolete. For example, if the computer name is changed, the SPNs for installed services would need to be changed to match the new computer name.

When a Double-Take failover occurs, the NetBIOS name of the original source machine will be represented by the target machine. If you are failing over domain servers without Active Directory or member servers, the source's NetBIOS name appears on the network as it did before failover. But, if you are using a domain controller with Active Directory, the SPN that associates the source's NetBIOS host name with the source's computer account in Active Directory must be changed so that the source machine name is associated with the target server's computer account in Active Directory. This can be easily accomplished using the NSISPN utility, developed by NSI Software. This utility allows you to view the current SPNs, reset the host SPNs, and add or delete supplemental SPNs.

Each machine typically has two HOST SPNs, one with the base NetBIOS name and one with the fully qualified domain name. During failover, and failback, both of these SPNs must be moved. This document walks you through configuring failover for domain controllers using Active Directory. It contains instructions for modifying your failover and failback scripts to automate the SPN functions as well as steps for changing the user account used to run the Double-Take service so that the scripts will run with sufficient security access.

NOTE: Double-Take does not failover any operations master roles that may be assigned to the source server, so this must be taken into account in your Active Directory failover design. If your source server is assigned one of the operations master roles (Schema, Domain Naming, Relative ID, PDC Emulator, Infrastructure) at the time when failover occurs, these roles will not be available within Active Directory until the source is brought back online. It is recommended that these roles be assigned to domain controllers that are not in use as Double-Take failover sources. See Microsoft Active Directory documentation for further information on these roles and recommended active directory layout.

Configuring Failover

The following steps walk you through your failover configuration and the creation of the failover and failback script files. The sample scripts used can be downloaded from www.nsisoftware.com/main/spnscrp.exe and the nsispn utility can be downloaded from <http://www.nsisoftware.com/updates/nsispn.html>.

1. If a failure occurs, you will want to have the addition and removal of SPNs automated. To do this, create a batch file called `prefailover.bat` using the sample batch file below. Save the batch file to the same directory where your Double-Take files are installed.

PreFailover.bat

```
rem This sample batch file contains the four lines necessary to change the location of the
rem source's SPNs in Active Directory to the target during failover
rem Make the following substitutions in the commands below
rem      Substitution                Description
rem -----
rem <drive:\directory>              full path to nsispn.exe
rem source                          name of your source server
rem full_domain_source_name         fully qualified name of your source server
rem target                          name of your target server
<drive:\directory>\nsispn -D HOST/source source
<drive:\directory>\nsispn -D HOST/full_domain_source_name source
<drive:\directory>\nsispn -A HOST/source target
<drive:\directory>\nsispn -A HOST/full_domain_source_name target
rem For example, your commands may look like this
rem c:\Program Files\DoubleTake\utilities\nsispn -D HOST/saturn saturn
rem c:\Program Files\DoubleTake\utilities\nsispn -D HOST/saturn.nsisw.com saturn
rem c:\Program Files\DoubleTake\utilities\nsispn -A HOST/saturn mars
rem c:\Program Files\DoubleTake\utilities\nsispn -A HOST/saturn.nsisw.com mars
```

NOTE: When the target server is a domain controller, any SPNs added to the target server object will be removed automatically from Active Directory approximately every 10 minutes due to a standard refresh process used by each domain controller. Once the source SPN is removed from the target machine object, the NetBIOS name will still be reachable, but Kerberos authentication using the source server name will fail. If standard NTLM authentication is allowed, it will automatically be tried and will succeed. If Kerberos authentication using the source name is required, a domain controller should not be used as the failover target.

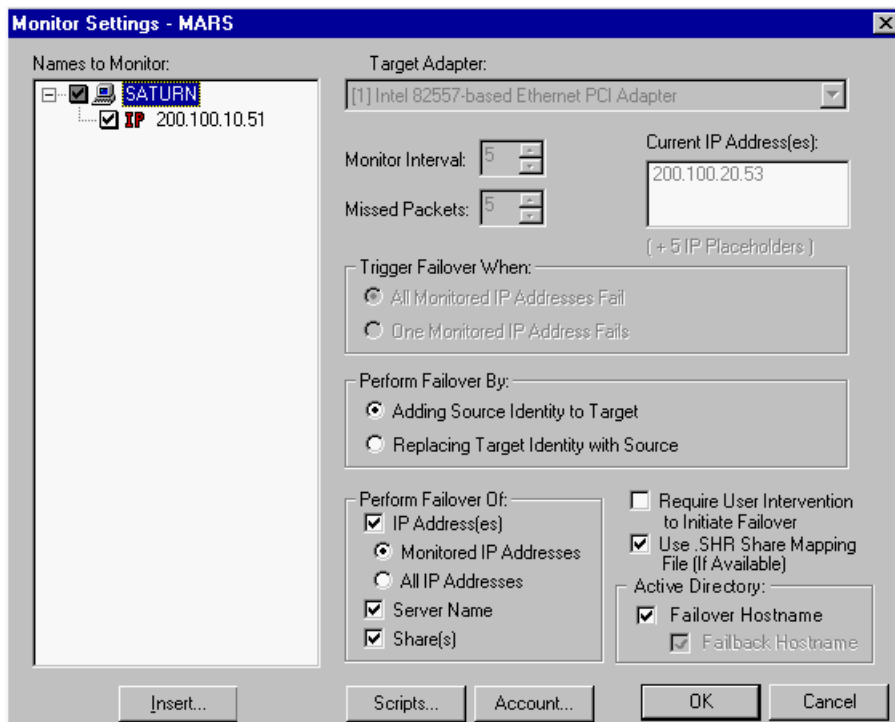
-
- After a failure is resolved, you will also want to have the addition and removal of SPNs automated. To do this, create a batch file called `prefailback.bat` using the sample batch file below. Save the batch file to the same directory where your Double-Take files are installed.

PreFailback.bat

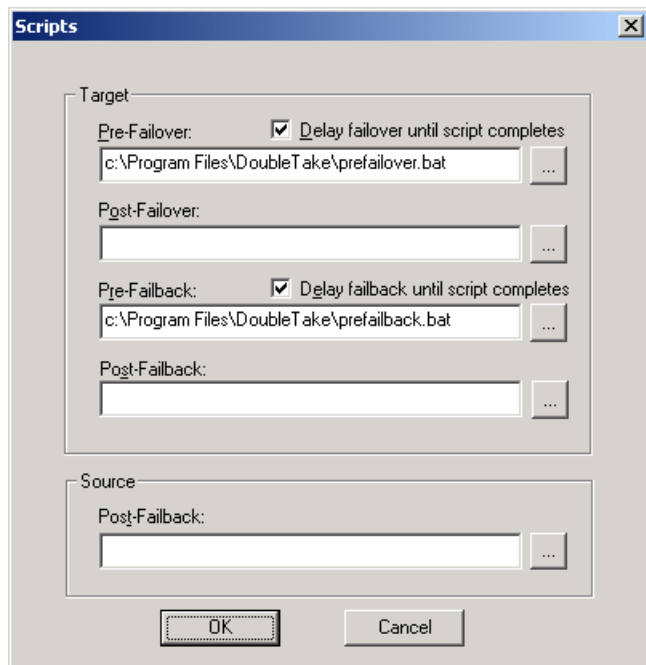
```
rem This sample batch file contains the four lines necessary to change the location of the
rem source's SPNs in Active Directory back to the source during failback
rem Make the following substitutions in the commands below
rem      Substitution                Description
rem -----
rem <drive:\directory>              full path to nsispn.exe
rem source                          name of your source server
rem full_domain_source_name        fully qualified name of your source server
rem target                          name of your target server
<drive:\directory>\nsispn -D HOST/source target
<drive:\directory>\nsispn -D HOST/full_domain_source_name target
<drive:\directory>\nsispn -A HOST/source source
<drive:\directory>\nsispn -A HOST/full_domain_source_name source
rem For example, your commands may look like this
rem c:\Program Files\DoubleTake\utilities\nsispn -D HOST/saturn mars
rem c:\Program Files\DoubleTake\utilities\nsispn -D HOST/saturn.nsisw.com mars
rem c:\Program Files\DoubleTake\utilities\nsispn -A HOST/saturn saturn
rem c:\Program Files\DoubleTake\utilities\nsispn -A HOST/saturn.nsisw.com saturn
```

- Select **Start, Programs, Double-Take, Failover Control Center**.
- Select the target machine from the list of available machines. If the target you need is not displayed, click **Add Target**, enter the machine name, and click **OK**.
- To add a monitor for the selected target, click **Add Monitor**. Type the name of the source machine and click **OK**. The Monitor Settings window will open.

6. In the Monitor Settings window, mark the IP address that is going to failover and verify that **Adding Source Identity to Target** is selected.



-
7. Click **Scripts** and specify the location and file names of the scripts that were created in steps 1 and 2.



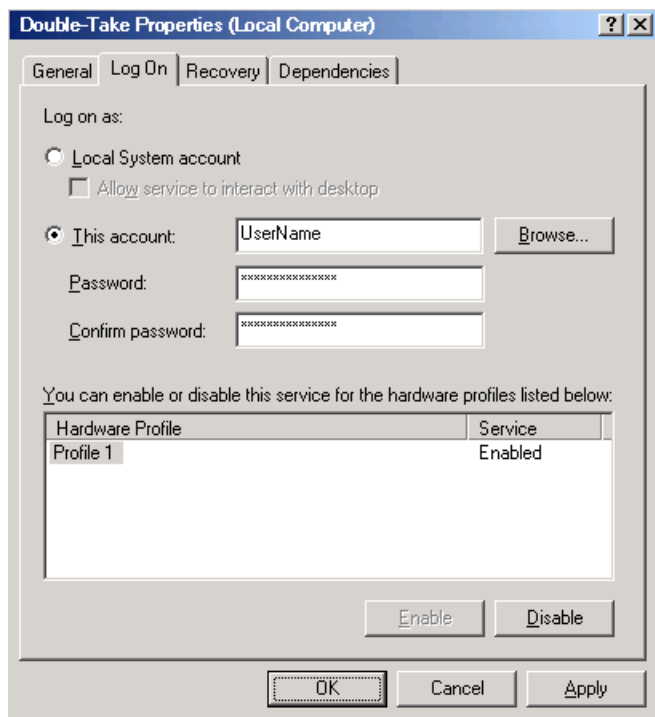
8. Click **OK** to go back to the Monitor Settings dialog box.
9. Click **OK** to begin monitoring the source machine.

Your failover configuration is complete. Because of the security associated with Active Directory, you must also configure the Double-Take service so that the failover and failback scripts can be run with the proper access. Continue with the next section [Configuring the User Account Running the Double-Take Service](#).

Configuring the User Account Running the Double-Take Service

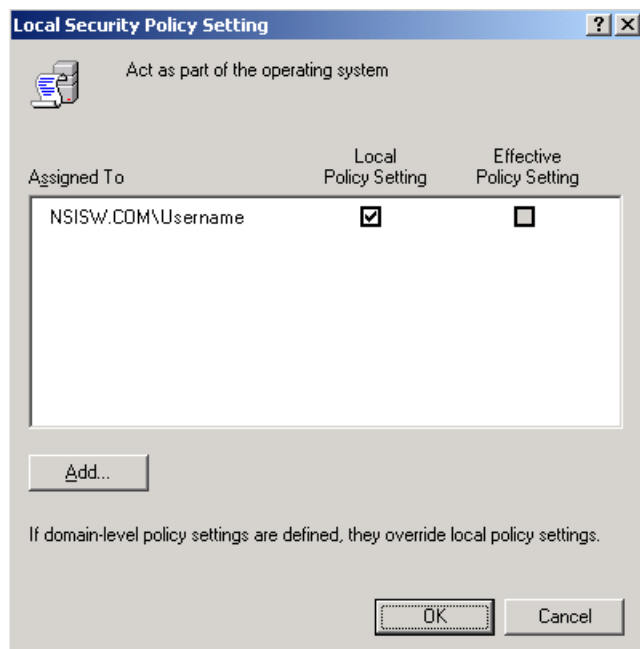
By default, the Double-Take service is configured to log on as the local system account. This account does not have sufficient access in Active Directory to make the SPN attribute changes. Therefore, the Double-Take service on the target must be modified to use a user account that has full update privileges within Active Directory. This account must also be granted access for Double-Take processing as well. The following instructions step you through changing the account and verifying the correct Double-Take access for the account.

1. Open the Double-Take service settings by selecting **Start, Programs, Administrative Tools, Services** and double-click the Double-Take service.
2. On the **Log On** tab, select **This Account** and enter a valid account that has full update privileges within Active Directory.
3. Enter the password for this account.



4. Click **OK** to save these settings.
5. Close the Services dialog box.

-
6. Select **Start, Programs, Administrative Tools, Local Security Policy**.
 7. Expand the **Local Policies** folder and then the **User Rights Assignment** folder.
 8. Double-click the option **Act as part of operating system** on the right pane of the screen.



9. Add the user that you selected to run the Double-Take service and click **OK**.
10. Double-click the option **Log on as a service** on the right pane of the screen.
11. Add the user that you selected to run the Double-Take service and click **OK**.
12. Exit the Local Security Settings dialog box. This user is now configured to run the Double-Take service.

NOTE: If domain-level policy settings are defined (through **Domain Security Policy, Security Settings, Local Policies, User Rights Assignment**), they will override local policy settings.
