Chapter No. 5
"Active Directory Failure On a Single Domain Controller"
In this package, you will find:

A Biography of the author of the book

A preview chapter from the book, Chapter NO.5 "Active Directory Failure On a Single Domain Controller"

A synopsis of the book’s content

Information on where to buy this book

---

About the Author

**Florian Rommel** was born and raised in his native Germany until the age of 15, when he moved with this family to Central America and then the US. He has worked in the IT industry for more than 15 years and has gained a wealth of experience in many different IT environments. He also has a long and personal interest in Information Security.

His certifications include CISSP, SANS GIAC:GCUX, MCSE, MCSA, MCDBA, and several others. Together with his extensive experience, he is a qualified and recognized expert in the area of Information Security. After writing several Disaster Recovery guides for Windows 2003 and Active Directory environments in large blue chip and manufacturing companies, he now brings you this unique publication, which he hopes will become a key title in the collection of many Windows Server Administrators.

Florian is currently working in the IT Management department at a large global manufacturing corporation in Finland where he has lived for the past ten years. His responsibility includes the Active Directory and the global security infrastructure.

This book is the result of long hours of research and not having time for the people around me. For that reason, I would like to thank and dedicate this book to my wife Kaisa and my daughter Sofia as well as my parents, and Neil. Without them and their support, as well as support from all of the other people involved in my career over the years, I would have never been able to start and complete this project. I would also like to give special thanks to the people at Microsoft Finland who helped me with questions and solutions, and Guido Grillenmeier who helped me by providing a lot of input and knowledge on the subject.

---

For More Information:

Active Directory Disaster Recovery

Murphy's Law states that anything that can go wrong will go wrong. In relation to Information Systems and Technology, this could mean an incident that completely destroys data, slows down productivity, or causes any other major interruption to your operations or your business. How bad can it get?—“Most large companies spend between 2% and 4% of their IT budget on disaster recovery planning; this is intended to avoid larger losses. Of companies that had a major loss of computerized data, 43% never reopen, 51% close within two years, and only 6% will survive long-term.” Hiroff, Jim.”

Back Up Business - Industry Trend or Event.

Active Directory (AD) is a great system but it is also very delicate. If you encounter a problem, you will need to know how to recover from it as quickly and completely as possible. You will need to know about Disaster Recovery and be prepared with a business continuity plan. If Active Directory is a part of the backbone of your network and infrastructure, the guide to bring it back online in case of an incident needs to be as clear and concise as possible. If it happens or if you want to avoid all of this happening, this is the book for you.

Recovering Active Directory from any kind of disaster is trickier than most people think. If you do not understand the processes associated with recovery, you can cause more damage than you fix.

This is why you need this book. This book has a unique approach - the first half of the book focuses on planning and shows you how to configure your AD to be resilient. The second half of the book is response-focused and is meant as a reference where we discuss different disaster scenarios and how to recover from them. We follow a Symptom-Cause-Recovery approach – so all you have to do is follow along and get back on track.

This book describes the most common disaster scenarios and how to properly recover your infrastructure from them. It contains commands and steps for each process, and also contains information on how to plan for disaster and how to leverage technologies in your favour in the event of a disaster.
You will encounter the following types of disaster or incident in this book, and learn how to recover from each of them.

- Recovery of deleted objects
- Single domain controller hardware failure
- Single domain controller AD corruption
- Site AD corruption
- Site hardware failure
- Corporate AD corruption
- Complete corporate hardware failure

**What This Book Covers**

*Chapter 1* provides an Overview of Active Directory Disaster Recovery.

*Chapter 2* discusses some of the key elements in Active Directory and then over to the actual design work. A few design models are dissected, which will give you a good starting point for your own design.

*Chapter 3* takes a look at all the steps and processes you should go through in order to have a DRP successfully implemented.

*Chapter 4* discusses directly (implementations) and indirectly (processes) related subjects that will help you make your AD environment stronger against events that can impact in a negative way.

*Chapter 5* looks at the different options and approaches for how to recover a DC that has a database corruption.

*Chapter 6* takes a look at the steps necessary to completely recover from a failed domain controller.

*Chapter 7* goes through the different methods of restoring deleted objects, and also looks at how to minimize the impact that such a deletion can have on your business.

*Chapter 8* provides a step-by-step guide to forest recovery.

*Chapter 9* discusses site AD infrastructure failure.

*Chapter 10* describes through a few tools and utilities that will help you monitor and diagnose your AD.

*Appendix A* provides an example of Business Continuity plan. *Bibliography*
Active Directory Failure On a Single Domain Controller

Active Directory (AD) failure, which includes corruption, is something that is dreaded by any administrator. Simply put, it means that the directory service can no longer read the Active Directory database that it has locally. This will prevent logon and authentication as well as any directory-dependent services. Essentially, it renders the domain controller useless. What's worse, though, is that several times, the replication keeps going so that the corrupted database spreads out to the other DCs.

In this chapter we will look at the different options and approaches available to recover a DC that has a database corruption. In addition, this chapter outlines, symptoms, causes, and solutions for this scenario.

Problems and Symptoms
Let's take a look at the symptoms and then the causes.

Symptoms
The database gets corrupted and the DC is no longer able to process and authenticate or perform directory lookups. This becomes apparent when replication fails for some reason, or a large amount of specific event log errors appear. Another symptom could be that the AD services don't start on the DC.
Active Directory Failure On a Single Domain Controller

Causes
This scenario can be caused by:

- A software glitch, which can due to upgrading the schema, but having customized schema entries
- An unclean AD write
- A replication that has been interrupted
- An accidental or malicious change in the AD schema with low level tools such as ADSledit or something similar.

Solution Process
The recovery process is as follows:

- You will have to verify that it is, in fact, a failure or corruption within the AD database, and not a network-related problem or other problem.
- You will then have to perform a specific directory restore mode recovery, where you have to decide between an authoritative and a non-authoritative mode.
- Once the recovery is complete, you will need to verify whether the DC is replicating and functioning properly.

Solution Details
What follows is a complete outline of what to do during each part of the solution process.

Verification of Corruption
If the AD on a domain controller becomes corrupted, or stops replicating to other DC’s, or both, find out the root cause for this. A good starting point is to check again that the DNS is in order, and revert any manual changes that may have been made recently. Also, ensure that it is not a network-related problem — this means that no routers and routes have been changed, or firewalls re-configured, and the connection is not down. These are more often than not the main causes, and not an actual corruption.

If you can safely rule out those causes, you can use utilities such as ReplMon and DCDiag, which are included in the Windows 2003 support tools, available free from Microsoft’s website or on your install CD. Although ReplMon is a graphical utility,
it is pretty small, and one of the best tool for checking whether or not there are replication errors within an entire domain. It shows which DCs are not replicating and why. The other utility, DCDiag, scans every DC, and determines if and why they have replication and other errors.

When you have checked that all other DCs replicate just fine, you should check the Event log for specific event IDs (467 and 1018), that only occur when you have a real database corruption, and the AD jet database, which AD uses, is unreadable.

Tools for Verification
The Windows 2003 support tools (found on your installation CD under the SUPPORT folder) and the Windows 2003 resource kit tools (found at http://www.microsoft.com/downloads/details.aspx?FamilyID=9d467a69-57ff-4ae7-9ee-b18c4790cffd&displaylang=en) provide a variety of tools to verify if the DC is still operational, if there is actually a problem, and where the problem lies. Although the usage of these programs can also be described as part of an AD health check, in this case, we will focus on a single DC. The output from some of these tools is fairly long, and for brevity's sake, we will focus on only the relevant parts.

ReplMon
ReplMon, short for Replication Monitor, is essential in your arsenal of tools for detecting replication errors within a domain. It can also provide you with a good view of replication partners for each DC, and allows you to run a check against an entire domain for replication errors. The following screenshot shows the default ReplMon window, while the next screenshot shows the right-click action menu for a monitored DC. To run ReplMon, simply type replmon from the command line.
An example of where ReplMon becomes very useful is to detect errors while trying to replicate to other DCs. There are different errors for different scenarios. But, for example, a server that cannot be reached, or is offline, would show the following error in the domain-wide search for errors:

**DCDiag**

DCDiag is a command line utility that performs a full check of the DC as regards AD. These tests include forest DNS tests, to check that the DNS is okay at the forest level, domain DNS tests, to do the same on a domain level, configuration test, schema test, and the FSMO test to check that all FSMO servers are available. Running it is as simple as typing `dcdiag` at the command line, and watching the output. You might want to add an output file such as `dcdiag > c:\dcdiag_output.txt` at the end, to save everything to a text file that you can read easily.
A successful DCDiag test would have the following results:

NetDiag and DNSDiag
Both of these utilities check the network connectivity of the DC on which they are installed. DNSDiag is more geared towards Exchange, and checks that all of the essential DNS records are valid and are working, by pretending to follow the MX records. It also gives us a lot of output with regard to the domain DNS structure, and identifies if there are any problems. NetDiag checks the local networking stack. It tests all the installed protocols and services, including WINS, NetBT, and TCP/IP.
**Sonar**

The Sonar.exe utility provides a GUI, which shows exactly where a replication failed, and what the state of the File Replication Service (FRS) is on each of the DCs. This is particularly useful for large environments. It also has different views that allow you to troubleshoot your FRS on a DC.

![Sonar GUI](image)

**Options to Recover and Stop the Spread of Corruption**

If, in effect, you have a corrupted or failed AD database, and it hasn't spread yet, meaning it is only on one DC, you should remove that DC from the replication chain as quickly as possible. A good way is, of course, to disconnect the network connection, though this will have an impact if you are working remotely on the machine. The other option is to isolate the DC with firewall rules. This is also the safest way that still gives you access to the machine remotely. If neither option is available to you, you can use the Repadmin utility to stop outbound and inbound replication. The two options are `repadmin /options DCNAME +DISABLE_INBOUND_REPL` and `repadmin /options DCNAME +DISABLE_OUTBOUND_REPL`, where **DCNAME** is the name of the DC that should be disabled. If you want to enable the replication, simply retype the command with a `-` instead of a `+` so as `repadmin /options DCNAME -DISABLE_INBOUND_REPL`. 
The following screenshot shows the command line for disabling outbound replication with Repadmin.

Please note that when you disable outbound replication, errors with Event ID 1115 will appear in the event log, just as errors with event ID 1113 will show when inbound replication is disabled. When either one is re-enabled, informative Event IDs 1116 (outbound) and 1114 (inbound) will appear in the event log.

The fastest way to recover from a corrupted AD database is to forcefully demote the DC to become a member server, and to promote it again to replicate off of another DC, if there is one in the same network. You should take this step only if you are sure, and have verified that the AD is actually working on the other DC. You can use DCDiag to easily verify whether everything is correctly order. You should not replicate from another DC within the same site if you cannot verify whether the DC is actually operational. Make sure that the event log does not contain any Jet database, or FRS errors such as 1173, which would indicate an internal error in the Jet Database.

You will have to perform a metadata cleanup if you force-demote the DC because a clean demotion is not an option. If you use Dcpromo normally, it will replicate its "change" out to another DC. In other words, you are spreading the corrupted or non-functioning database this way. You can easily force-demote it by running dcpromo/forceremoval, and then follow the steps outlined in Chapter 4 for a metadata cleanup.
Non-Authoritative and Authoritative Restore

To speed up the data replication of the AD, for example, for sites that have a slow or saturated network connection, or to make the whole restore process much quicker, you should perform a non-authoritative restore of the AD database. Non-authoritative restore means that you are restoring a database, but that database will not assert authority in the AD. This means that it will take all changes that the replication partners send it, where an authoritative restore is set to be the master replication in your domain. It will restore itself, and give itself such high update sequence numbers to objects that every other DC in the domain replicates from it because it is assumed it has the newest copy.

Effectively, you are restoring a backup of the AD database to its original location, overwriting the current database. This can only be done when you are in Directory Restore mode. After the database is restored, reboot your DC normally. If you have changed the boot order, reverse the order again.

Please make sure your backups are run regularly, whether it is on tape or on disk, according to your organization's backup policy.

After the restore is complete, and you reboot the DC, the next replication will be much faster because only changed objects will be replicated to the server. This is because it has most of the AD database already, depending on how much the AD has changed, and how recent the backup was.

In a non-authoritative restore, data that is restored includes AD objects with original update sequence numbers. This requires a lot of caution, as any data that is restored with a non-authoritative restore will appear to be outdated to the AD replication system. Hence, the data will not get replicated to other domain controllers. You therefore run the risk of having the data overwritten from DCs that have not yet been restored to, and contain somewhat newer data, including other corruptions.

Since this chapter is meant for a corruption or AD failure on a single DC only, with a replication partner relatively close by, we will skip the authoritative restore. This will be addressed in the following chapters. The following figure illustrates how authoritative and non-authoritative restores work.
Option One: Restoring AD from a Backup

In order to restore an AD database on a Domain Controller, you have to go into the "Directory Services Restore" mode.

To do this, reboot the DC, and at the boot prompt, which is where the boot process waits for a second before the splash screen of Windows 2003 comes up, press the F8 key, after which you will be presented with a menu similar to the following:

Windows 2003 Advanced Options Menu
Please select an option:

Safe Mode
Safe Mode with Networking
Safe Mode with Command Prompt

Enable Boot Logging
Enable VGA Mode
Last Known Good Configuration
Directory Services Restore Mode (Windows NT domain controllers only)
Debugging Mode

Use | and | to move the highlight to your choice.
Press Enter to choose.

At the menu, select the Directory Services Restore Mode, by moving up and down with the arrow keys on your keyboard, and then press ENTER. You will then be in the same menu again. Press ENTER again, after which, your display will show Directory Restore Mode at the bottom of the screen. Your DC will now boot, but no AD-related services will be started. Once booted, restore the AD/system state from a trusted and recent backup, and reboot the machine. After the machine is rebooted, you should have working AD services with a slightly outdated AD database. Wait for the replication to take effect, and your AD will be updated.
No Physical Access to the Machine

If you do not have physical access to the machine in question, you can achieve the same effect by editing the boot.ini file, which is located in c:\. This file, by default, is hidden and may be write-protected. To see the hidden files and system files, you will need to change your Windows Explorer settings, as shown in the following screenshot.

When you can see the file, check its properties, that is, whether it is read-only or not, by right-clicking on it and selecting Properties. However, instead of changing file permissions of system files, you can edit this quite easily with the Graphical User Interface. Some people are not comfortable editing protected files, and then you can also run into problems if you forget to un-mark or re-mark the read-only flag.

To get to the GUI editor, right-click on My Computer in your Start menu, or click the icon with the server name in the right hand upper-right, and then select Properties. Once you have done this, the following screen will appear:
On the properties window, go to the **Advanced** tab, as shown in the following screenshot:
Active Directory Failure On a Single Domain Controller

And then Click on **Settings** in the **Startup and Recovery** section of the **Advanced** tab, as shown in the screenshot below:

![System Properties](image)

For More Information:
www.packtpub.com/active-directory-disaster-recovery/book
In the resulting window, which contains quite a few options and sections, you can click on the **Edit** button and the `boot.ini` file will be opened in Notepad. Once editing is completed, and the file has been saved and closed, all permissions will be reset to their original settings.

The editing of this file is pretty straightforward, yet not easily understandable for someone who has never done this. In the following screenshot, you can see the actual file displayed:

![Boot.ini - Notepad](image)

To edit the file in order to reboot in Directory Restore Mode, it is recommended to just copy and paste the last line again, and perform two changes:

1. Change the display name by adding something like `Recovery`.
2. Add the `/safeboot:dsrepair` at the end of the line, as shown in the following screenshot:

![Boot.ini - Notepad](image)

When editing is done, save and close the file as you would with any other text file, and click **OK** in the **Startup and Recovery** window so that it closes.
Active Directory Failure On a Single Domain Controller

To select the option on which you want to boot, click **SETTINGS** in the **Startup and recovery** section again. And as you can see in the following screenshot, you can now select the boot default from the drop-down menu in the opening window:

![Startup and Recovery](image)

Select the Recovery line and click **OK**. Then click **OK** again to reboot the server. It will now boot automatically into the Directory Restore Mode.

**Restoring from a Backup**

Once you are in Directory Restore Mode (DRM), you can use your company's backup software to recover the AD database. If you use Windows backup, you can safely backup and restore the system state of the server, as you can see in the following screenshot. This will allow you to fully revert to a completely working system.

![Backup or Restore Wizard](image)
However, if you do not need to, or do not want to, recover the whole system state, you can easily choose to restore only AD from the list, as shown in the following screenshot. We assume that we have a complete backup of the server, and that we need to restore the AD database.

You can restore the AD or system state to a different location, or overwrite the original files, depending on whether you want to perform an authoritative or a non-authoritative restore, or even an install from media.

Option Two: Replication
In case you have no valid recent backup media from which to restore the AD, or you need to act very fast, you can restore the AD by first force-demoting the DC in question with `dcpromo /forceremoval`.

This way, demoting will prevent replication to any replication partners, but will successfully demote the DC from the domain. If you have any important Flexible Server Master Operations (FSMO) roles running on the DC that you are removing by force, you will be presented with the following warning:
Refer to Chapter 3 for more information on the importance of FSMO, and how to seize FSMO roles. Make sure that you seize the FSMO roles after you have demoted the DC, or after you disconnect its network cable. Do not forget this though, as the FSMO roles are quite important.

As you can see in the following screenshot, the Active Directory wizard will now proceed to remove AD without updating the forest. This means that it will not replicate out its own data or changes.

Once demoted, reboot the server, and follow the steps to remove its leftover information from AD as a DC, as described in Chapter 4. Then, verify whether the network connection is fully functional, and promote the DC again with the same name.

You should encounter no problems in completing the promotion. The AD will replicate to it during the next scheduled replication.
Chapter 5

If your AD is very large and contains many records or files, such as pictures in the user information, the replication to a "blank" DC will take a long time and stress your network quite heavily.

The replication option in a larger environment with a large dataset can take a long time if the other DC is either busy, or the replication link is not a very high-speed connection. The size of the AD databases can start from 1 GB and may run up to several gigabytes. If your DC has to replicate from a DC over a leased line, or an average consumer Internet class connection (2 to 8mbit), you may have to consider the other option of restoring from a backup, or performing a non-authoritative restore.

Option Three: Rebuild DC with Install from Media
Starting from Windows 2000 SP3, there is a dcpromo option available called "IFM" (install from media). This option adds a step to the DC promotion that will pre-populate the AD database on the promoted DC from a recent system state backup of a working DC, which is restored to a disk, CD or DVD.

IFM is the fastest option if you have to install, recover, or re-install a DC that is connected by only a slow link to its closest replication partner. As you are pre-populating the local AD, the replication changes it will get from its partner are much smaller, and therefore will replicate much faster.

To use IFM, restore the backup to the server BEFORE you make it a DC, and before you run dcpromo. A good way to do this, if you want to, or need to, restore several DCs with IFM, is to restore it to a network drive. To prepare a backup and restore for IFM, please see Microsoft's Knowledge base article http://support.microsoft.com/kb/311078.

IFM can only be used for additional DCs within a domain, not for the first DC. You can also only pre-populate, or restore a DC with a backup of the domain that you are building in.

A good option for this is to force-demote the DC, reboot it, and start it as a normal member server. You then need to clean up all of the records from the AD regarding the DC, and then perform an install from Media.

Restore the most recent backup to a separate directory, for example, c:\restore. This restore should be a restore of the System State of a DC, and the directory will contain sub-directories such as AD, Boot Files, Registry and so on.

For More Information:
www.packtpub.com/active-directory-disaster-recovery/book
Once the restore has succeeded, click on Start, Run, and enter `dcpromo /adv` as shown:

![Run](image)

The `/adv` flag in the Dcpromo command gives you advanced options within Dcpromo, such as the install from media options.

Follow the dialog as you would normally do for a `dcpromo`. However, when you see the screen regarding Copying Domain Information, select the option: **From these restored backup files**, and navigate to and select the directory to which you restored the system state.

![Active Directory Installation Wizard](image)

As you can see in this screenshot, you also have the option to pre-populate immediately from an existing DC. This is, of course, an option, but if your link is slow, or if your replication partner is busy serving other partners, it will be much slower than from media.
Not just for disaster recovery!

If you have to install several DCs for any reason, the \texttt{/adv} switch can save you the time spent waiting for the first replication, if you have a fast link, or a backup, that you can use to pre-populate.

When following the wizard, you will be asked if you want to make this DC a Global Catalog, and then you may be required to use an account with Administrator privileges in order to proceed with the \texttt{dcpromo}.

Once the \texttt{Dcpromo} wizard completes its task, and the AD records are copied from a previous backup, at the next replication only the changes since the last backup will be replicated. This saves a lot of bandwidth and time. This is especially useful for sites with a slow or saturated network connection, where replication would take far too long, so if you need to recover or install fast, this is probably your best bet.

Summary

In this chapter, we looked at the recovery procedure in the event of a corruption or failure of the AD database on a single domain controller. This is a scenario that happens more frequently than one might expect. So, instead of “just re-installing”, these options and procedures will help you get a healthy DC back in no time while limiting the amount of errors in the event log.

We also looked at some tools that will help you not only diagnose AD problems, but also allow you to perform, when used regularly, AD health tests to make sure your AD is always in perfect working order. This way, you might prevent failures because you might find the symptoms earlier.
Where to buy this book


Free shipping to the US, UK, Europe and selected Asian countries. For more information, please read our shipping policy.

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.