

# My Tech Blog

Hello all! Having worked for a while with various computer systems, primarily Active Directory and Exchange, I wanted to share some of my experiences with two objectives in mind: 1) obtain feedback to improve my mastery of those systems and 2) help others working on the same subject. Other posts are about CentOS, Citrix NetScaler, and VMware. NOTE: most of my posts are in English but some others in French, with a summary in English. However, some of the CentOS blog posts lack this summary.

Friday, January 10, 2014

## Windows Server 2012 - Active Directory - Backup and Restore, Part 1: System State

### Introduction

For my next serie of blog posts, I want to examine aspects of backing up and restoring Active Directory.

I've always thought that the native options for backing up Active Directory were not "efficient".

I do not mean to say that they "do not work" but rather that they require a certain "effort" to accomplish, one may argue, what should or could be a short and simple operation.

Essentially, we have to backup the "system state" which includes not only the Active Directory database, and the SYSVOL data (in substance, group policy and scripts), but also the registry, system files, and the COM+ database. If the domain controller holds other roles, the system state could include even more elements.

So if we needed to restore a single user, we would have to restore the entire system state (and then perform an "authoritative restore" - which will be presented later). All that for a single user? Well, we could simply recreate the user. However, since that user would be associated with a new SID they would not have access to the resources that they did before the deletion. So we would have to recreate their group memberships, for example. There could be a number of other relationships that would need to be re-established as well, such as Exchange mailboxes (their own and possibly access to shared mailboxes).

So, recreating the user object is not a solution as simple as it might seem. It is even less optimal when multiple users have been deleted or when an entire OU has been deleted. Manual recreation of all the deleted objects could take hours, days or weeks.

On the other hand, restoring what amounts to an entire domain controller, and an entire Active Directory database that could be hundreds of megabytes in size (or even gigabytes), could seem equally excessive. Yet until Windows 2008 R2, that was the only choice, unless administrators opted for third-party software.

In the lines (and posts) that follow, I want to examine three Active Directory restore methods.

1. System State restore. This implies a System State backup.
2. Active Directory Recycle Bin.
3. Third-party software.

## System State backup and restore

The first step, quite logically, is to perform a system state backup of the domain controller.

In fact, we have the option of performing a "Full Server Backup" which includes the System State as well.

The Full Server Backup has the advantage of allowing a bare metal restore of the domain controller. We would boot from the Windows Server 2012 media and essentially restore the image of the entire server from a .VHD file (since Windows 2008, the backup file exists in that format). A simple System State backup does not allow such a restore.

In any event, both types of backups can be performed in either the GUI or at the command line.

I'm going to choose the command line option:

```
PS C:\> wbadmin start backup -backuptarget:E: -allcritical -systemstate -vssfull -quiet
```

**wbadmin** is the Windows Server command line tool for backups since Windows 2008.

**wbadmin start backup** is the basic command to start a backup (self-explanatory).

We need to designate a target for the backup. This can be a local or external hard drive or a network share. I'll use an external hard drive for this post.

## **-backuptarget:E:**

The following command is the equivalent of the "Bare Metal" option in the Windows Server Backup graphical interface. In summary, it backs up all volumes necessary for the complete restoration of the server. This would be, at minimum, the C: drive and then any other drives housing elements such as the Active Directory database or logs files, if these were stored elsewhere.

## **-allcritical**

I have added the following parameter after having read that without it, we could not perform a simple system state restore from a Full Server Backup.

## **-systemstate**

### Bare Metal backup versus -allcritical

I have not tested the command without the -systemstate parameter to confirm that the assertion is exact but I can confirm that the command works just fine with the parameter, necessary or not.

As for the last two parameters...

## **-vssfull**

This configures the backup so that all files are marked as backed up and that logs of previous backups may be deleted. It should be added if Windows Backup is the only backup software in use.

## **-quiet**

This simply suppresses some of the prompts that would otherwise display.

The resulting output (edited here) should look something like this:

*Retrieving volume information...*

*This will back up System Reserved (350.00 MB),(C:) to E:.*

*The backup operation to E: is starting.*

*Creating a shadow copy of the volumes specified for backup...*

*Creating a backup of volume System Reserved (350.00 MB), copied (0%).*

*Creating a backup of volume System Reserved (350.00 MB), copied (62%).*

*The backup of volume System Reserved (350.00 MB) completed successfully.*

*Creating a backup of volume (C:), copied (0%).*

*Creating a backup of volume (C:), copied (2%).*

*Creating a backup of volume (C:), copied (4%).*

*Creating a backup of volume (C:), copied (7%).*

[snip]

Creating a backup of volume (C:), copied (94%).

Creating a backup of volume (C:), copied (96%).

Creating a backup of volume (C:), copied (99%).

The backup of volume (C:) completed successfully.

Summary of the backup operation:

-----

The backup operation successfully completed.

The backup of volume System Reserved (350.00 MB) completed successfully.

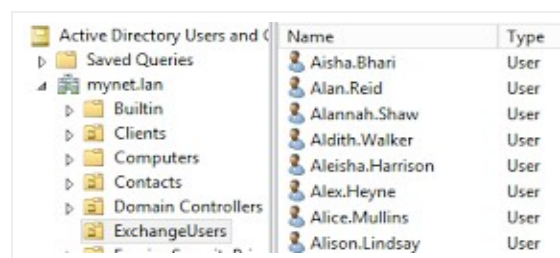
The backup of volume (C:) completed successfully.

Log of files successfully backed up:

C:\Windows\Logs\WindowsServerBackup\Backup-01-01-2014\_02-36-34.log

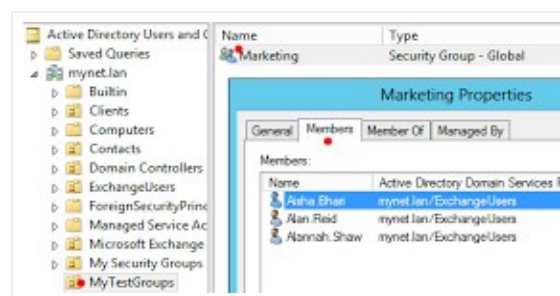
Now we have a backup.

Next, I'm going to delete three users: Aisha Bhari, Alannah Shaw and Alan Reid:



Name	Type
Aisha.Bhari	User
Alan.Reid	User
Alannah.Shaw	User
Aldith.Walker	User
Aleisha.Harrison	User
Alex.Heyne	User
Alice.Mullins	User
Alison.Lindsay	User

Note that they are also members of the "Marketing" group. After the restore, we will want to verify that group membership was re-established:



Name	Type
Marketing	Security Group - Global

Marketing Properties	
Members	
Aisha.Bhari	mynt.lan/ExchangeUsers
Alan.Reid	mynt.lan/ExchangeUsers
Alannah.Shaw	mynt.lan/ExchangeUsers

I won't waste space by posting another screenshot, but once the users are deleted they not only disappear (as expected) on DC5 but no longer appear in ADUC on DC2 less than a minute later. So replication acts immediately.

Now we learn that those users were not supposed to be deleted! Now we are in a predicament!

What can we do?

## 1. Boot into "Directory Service Restore Mode"

First we have to boot into what is called "Directory Service Restore Mode" (DSRM) on the server on which we performed the backup.

Tapping the F8 key should display a boot menu but it does not - not with a Windows Server 2012 guest in VMware. There might be a trick to this and I might succeed if I tried some more but there is another option.

At the command line, we enter the following (and then restart the computer):

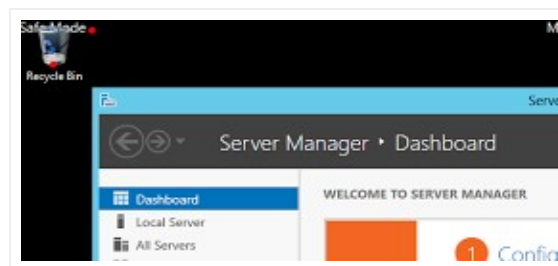
**bcdedit /set safeboot dsrepair**

**restart-computer**

*Note: to return to a normal boot, once the restore operation is complete, we enter this command:*

***bcdedit /deletevalue safeboot***

Once the server restarts and we login, the screen should look like this:



Note the words "Safe Mode" in the corners of the desktop. I only show the upper left-hand corner above, but the indication is present in all four corners. That informs us that the boot into DSRM was successful.

## 2. Restore the System State

The next step is to restore the system state.

I would like to point out that in this practice scenario, there can be no confusion about the backup to restore since we only have one and created it only minutes ago. Likewise, we only backed up one server. In reality, the backup media could contain not only several backups but backups of several servers. Therefore, we have to identify the backup we want with the following command:

**wbadmin get versions -backuptarget:E: -machine:DC5**

Among other information, this command produces an entry for:

Version Identifier: 01/01/2014-2:36

This output is important because we must indicate the backup version (even if there is only one) in the command that restores the system state:

**wbadmin start systemstaterecovery -version:01/01/2014-2:36 -backuptarget:E: -machine:DC5**

At this point we are all set... or so it seems. Our three user accounts have been restored - as well as the rest of Active Directory and all the other elements of the "System State".

But there is a problem. The three user accounts have been marked as deleted. These deleted accounts, though "invisible" to the administrator, still have a certain form of existence in Active Directory (for a while) and are replicated as deleted accounts to the other domain controller(s). The replication of what is called a "tomb-stoned" object is necessary so the other domain controllers are aware of the deletion and can update their copy of the Active Directory database accordingly. Now, these deleted user accounts, even though they are deleted, have a higher version number than the user accounts that were backed up earlier. The correct term for this "version number" is "USN" or "update sequence number" and it helps govern replication:

Newer versions of an object, updated on a given domain controller, replace older versions of an object that exist on other domain controllers.

So what will happen once the domain controller reboots and begins to replicate with the other domain controller? The "invisible" deleted user account, since it has a higher "version number", or USN, will replace the newly restored (but technically older) user account.

We need to mark the restored object(s) as "authoritative" which essentially increases

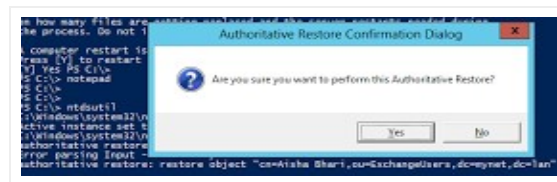
their USN number so it is (much) higher than that of the deleted user account (the tombstoned object) that continues to represent it in Active Directory.

### 3. Mark the restored objects as authoritative (authoritative restore)

We manage the authoritative restore at the command line using the ntdsutil tool. We'll start by restoring the user Alan Reid, entering the commands as follows:

```
C:\Users\admin>ntdsutil
ntdsutil: activate instance ntds
Active Instance set to "NTDS".
ntdsutil: authoritative restore
authoritative restore: restore object "cn=Alan Reid,ou=ExchangeUsers,dc=mynet,dc=lan"
```

When prompted for confirmation, I select "Yes":



I repeat the process for the other users.

The restore is successful. Once again, the users appear as they do in the screenshots above. What's more, the group membership is re-established as well. This was always a complex element in the restore process since membership in a group is not a property of the user, but rather of the group, and something known as the "back link" had to be restored, possibly in a second authoritative restore. Since group membership is restored here, at least in this rather simple scenario - single domain, single site, I'm led to believe that a Windows 2012 authoritative restore is able to process this element successfully.

The restore can be even more complex. If we had deleted the entire ExchangeUsers OU we could attempt to restore it with the "restore subtree" command in ntdsutil (instead of a single "object"):

```
authoritative restore: restore subtree "ou=ExchangeUsers,dc=mynet,dc=lan"
```

\*\*\*

So the restore is successful but some might perceive it as cumbersome. In my next blog post, I'll examine the "Active Directory Recycle Bin" option, first introduced with Windows

2008 R2 and improved in Windows 2012 Server, notably by the addition of a graphical user interface.

## Reference:

### [Recovering Active Directory Domain Services](#)

This article is about Windows 2008 R2 but the underlying principles still apply to Windows Server 2012. The article explains how group membership is re-established automatically since Windows 2003, at least in certain circumstances.

David M at 6:51 PM

Share



---

## 8 comments:



**Paul Allen** January 20, 2015 at 9:40 PM

thank you so much a nice tutorial for backup and restore window server 2012.  
[download free full version software for pc](#)

[Reply](#)



**Bruce Wolf** January 27, 2015 at 10:47 PM

this post is very useful and nice method for Windows Server 2012 backup or restore.  
[Full Software Download](#)

[Reply](#)



**Thomas Anderson** February 5, 2015 at 8:28 PM

Thanks for sharing info about backup or restore, it's a very useful and nice method for Windows Server.  
[Portable Software](#)

[Reply](#)



**Scarlet Emma** June 9, 2015 at 2:21 AM

Amazing discussion on software technology. Go ahead and update us through these type of posts.  
Wow amazing blog.I always love to read these kind of blogs.



[Free Download Software Full Version](#)

[Reply](#)



**Alice Riley** August 3, 2015 at 3:10 AM

thank you so much!! its wonderful information.  
[cracked software download](#) | [all cracked software](#)

[Reply](#)



**Chasityzwy85 Wellsqqw352** January 11, 2016 at 9:38 PM

Personally recommend you that site: [www.cdekey.com](http://www.cdekey.com), it is reliable and offers the cheaper price, good choice for you.

[Reply](#)



**Martha Whitmore** February 25, 2016 at 2:24 AM

thanks..  
[Serial Microsoft Office 2010 Professional Plus](#) | [Ashampoo Slideshow Studio Hd 3 Serial Key](#)

[Reply](#)



**贾璐瑶** June 19, 2016 at 11:27 PM

activation key for window 7 ultimate 32 bit , windows 10 product key surface 3 , [windows 10 key sale](#) , [office 2013 key sale](#) , wholesale norton antivirus , windows 10 serial key crack , windows 10 home serial key , windows 10 product key trouble , l8dbiy

[buy office 2016 product key](#)

[windows server 2012 r2 free](#)

[rosetta stone french key sale](#)

[Reply](#)

Enter your comment...

Comment as:

Hervé Franco - ▾

[Sign out](#)



Home



[View web version](#)

**About Me**

**David M**

[View my complete profile](#)

Powered by [Blogger](#).