

Backing Up & Restoring ADI DNS



Windows Server 2012 R2

Abstract:

This document is a quick explanation of how to backup and restore ADI DNS zones, and what the problems might be with the commonly discussed 'DNSCmd.exe /zoneExport' approach.

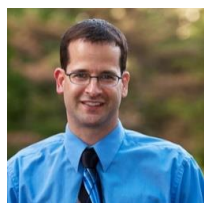
Document Revision and History:

version	date	description
1.0	7/12/2014	initial publication
1.1	7/13/2014	cleanup up references to record timestamps and record permissions

Freeware License and Disclaimer:

This document is freeware, done in the spirit of open-source. You may distribute unchanged copies of this document freely to anyone at any time. Care has been taken to cite contributing sources and individuals, please do the same. If you find errors in anything contained herein, please comment on them and/or contact me so that we may all help the community.

About the Author:



Daniel L. Benway

Systems & Network Administrator / Engineer
BS/CS, MCSE (NT4, 2000), MCTS (SCCM 2012), CCNA (2.0), Network+, CLP (AD R4)



<http://www.Linkedin.com/in/DaniellBenway>



<http://www.DaniellBenway.net>



@Daniel_L_Benway

Many websites say there are at least two ways to backup and restore ADI DNS zones (I disagree):

- **System State** backup and restore is probably the only MS supported way to backup and restore ADI DNS zones, and it's really not hard (it sounds so much worse than it really is).
- '**DNSCmd.exe /zoneExport**' to backup and eventually restore ADI DNS zones is kludgy, and probably non-supported, and might not even fully work especially considering permissions, timestamps, and multiple SOAs. Additionally, in a multi-master replication model a zone's SOA version number isn't quite so straight-forward as to who modifies it when, and what it means. In the event of a full zone restore using this method you will probably have to delete and re-create the zone on every DNS server that hosts the zone, and even then where are the permissions? Nonetheless, run the command anyway if you want to backup your ADI DNS zones because the created file might prove helpful and it is human readable.

System State Backup and Restore of ADI DNS Zone:

<http://blogs.technet.com/b/networking/archive/2007/05/10/oops-our-ad-integrated-dns-zone-s-are-missing-in-windows-2003.aspx>

NOTE: there is a missing step here: 'activate instance NTDS' needs to be run after 'NTDSUtil':

The most important thing to know is if the zone that was deleted was a Forest or Domain integrated partition. This is important because the data for each of these is stored in a different Active Directory partition. Since we want to do an authoritative restore for only the DNS information we want, and not all objects in the system state, we will need to specify which partition to mark as authoritative after we restore the system state. I recommend documenting all your DNS zone information so that you know how each zone is setup, and any know of any delegations assigned to the zone.

To restore your DNS partition:

Reboot the server in Directory Services Restore Mode by pressing F8 when booting and selecting that option from the menu. Then select Windows Server 2003.

While in Restore Mode, the machine will not replicate AD objects. This is important since we don't want the system state information we restore to get immediately overwritten by replication from another domain controller.

Logon to the server locally.

Open the backup program.

Restore the system state to its original location. This will be a non-authoritative restore, so any newer objects in Active Directory will overwrite the restored objects. We will specify what to restore authoritatively later on.

Once the restore is complete, open a command prompt.

From the command prompt type the following:

```
Ntldsutil
```

```
Authoritative restore
```

```
Restore subtree "dc=DeletedZone.com,cn=MicrosoftDNS,dc=forestDNSZones,dc=contoso,dc=com"
```

(This would restore a Forest Integrated zone named Deletedzone.com in the Contoso.com domain. For a Domain integrated zone you would replace forestDNSZones with domainDNSZones)

You should get a message that the Authoritative Restore completed successfully.

After that you reboot the server into normal mode and replicate AD. This will add the zone back to all your DNS servers.

Here are some references on restore Active Directory objects:

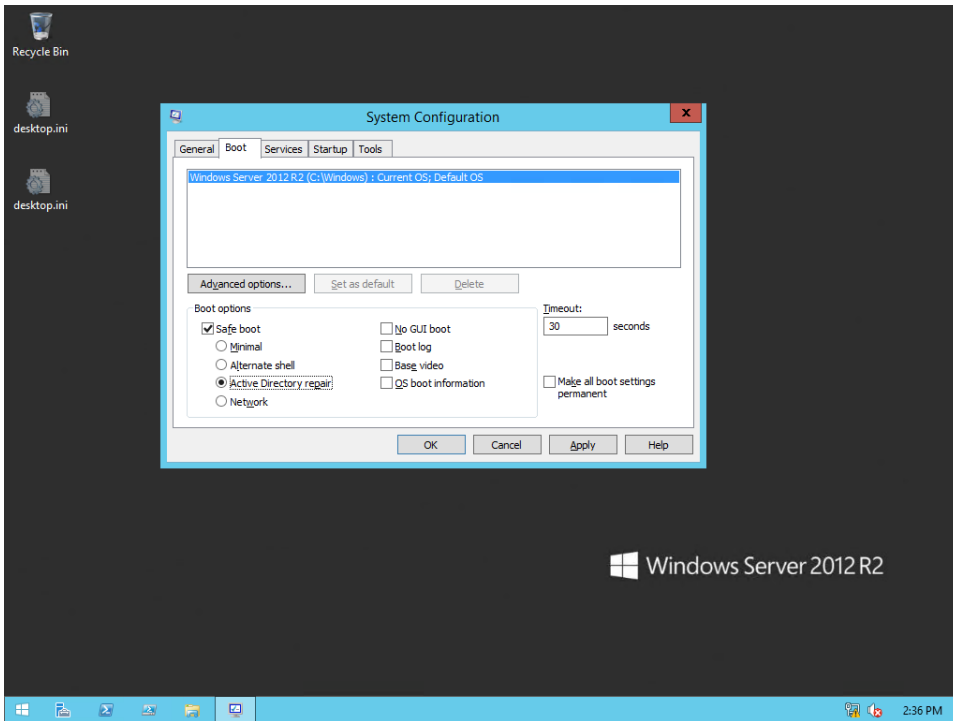
<http://technet2.microsoft.com/windowsserver/en/library/aec8cc76-c345-4cb6-83d9-b6009ba5d8801033.mspx?mfr=true> Performing a Nonauthoritative Restore of a Domain Controller

<http://technet2.microsoft.com/windowsserver/en/library/690730c7-83ce-4475-b9b4-46f76c9c7c901033.mspx?mfr=true> Mark the object or objects authoritative

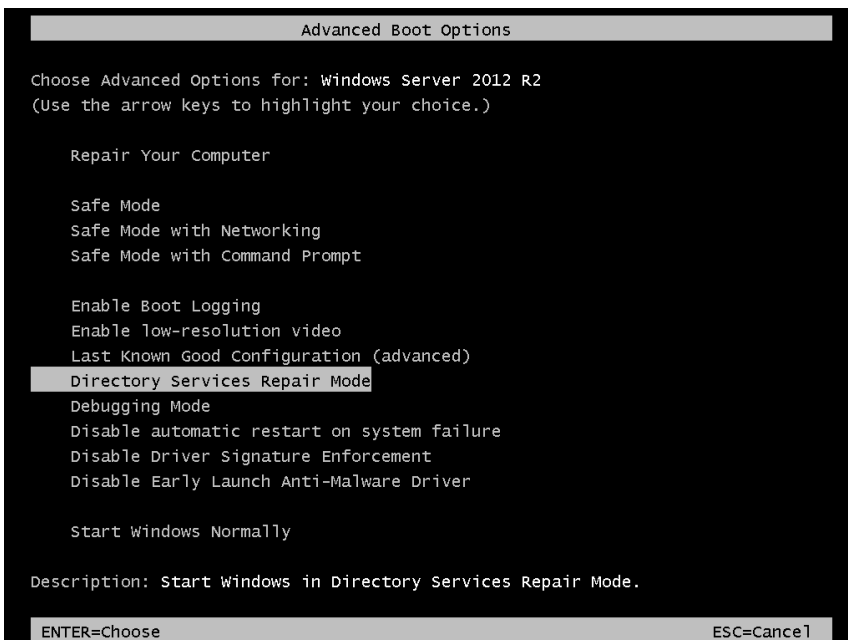
NOTE: there is a missing step here: 'activate instance NTDS' needs to be run after 'NTDSUtil':

The following screenshots correspond to the preceding steps:

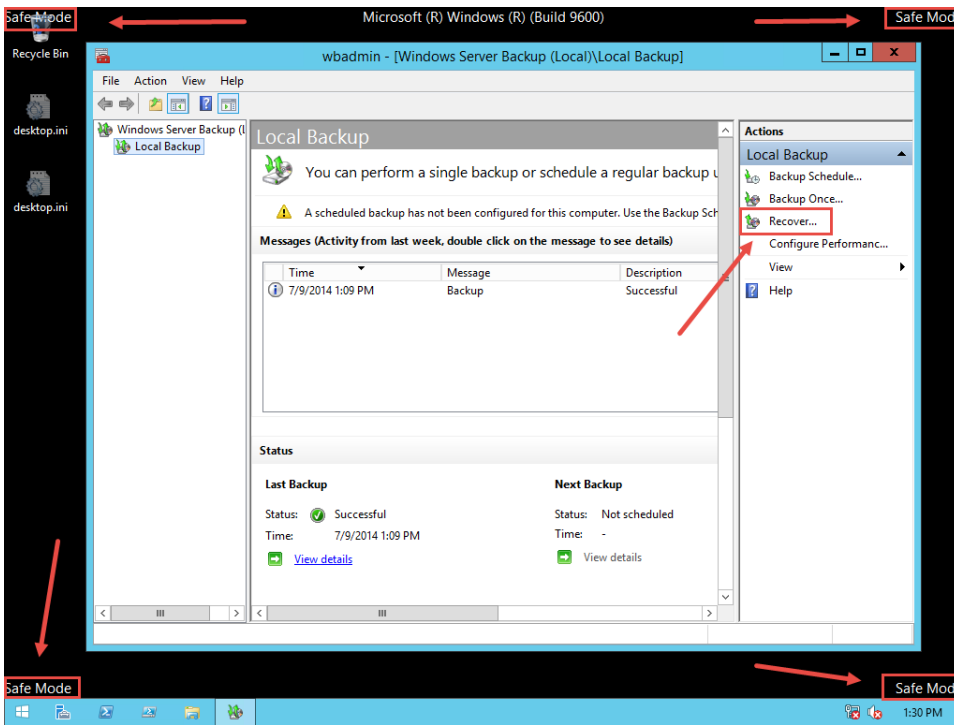
On the Domain Controller (DC) you will use for the System State restore, use MSConfig.exe to boot into Directory Services Repair Mode (DSRM), because MSConfig.exe is more reliable than trying to get the timing right for F8 on bootup. Now remember, you won't have access to the DC via RDP once the server reboots into DSRM, so use the console:



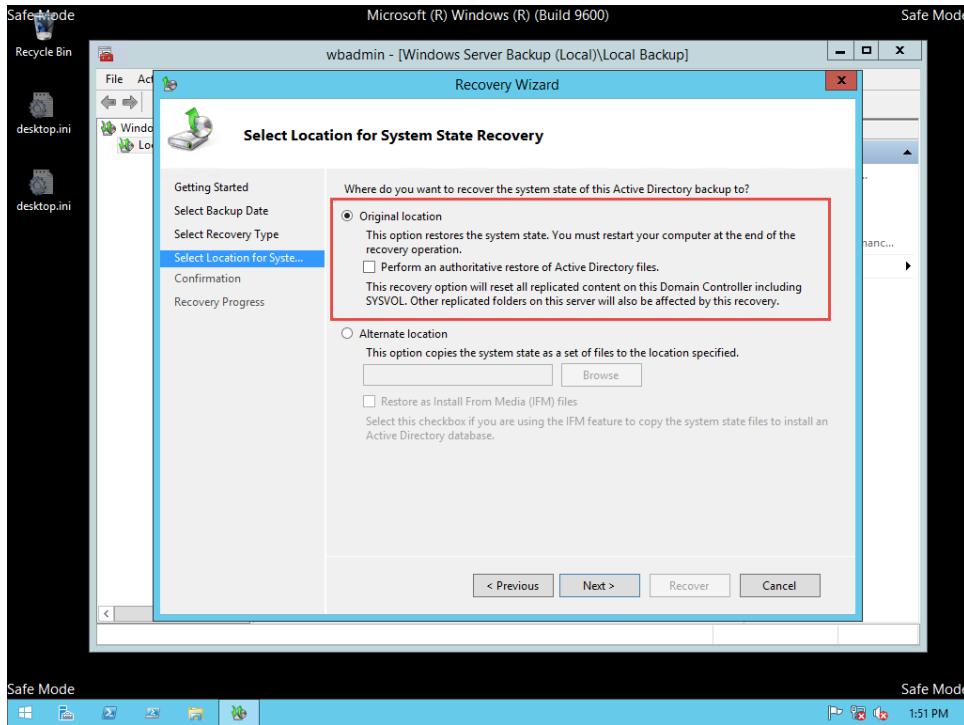
Just for reference, this is what F8 on bootup looks like:



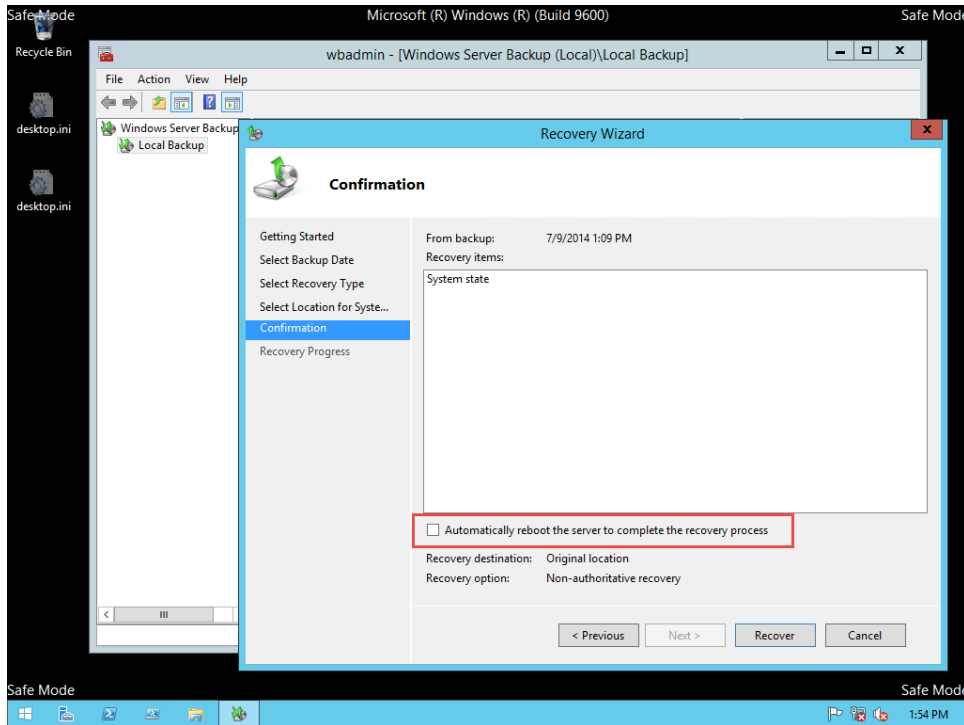
When the DC is done booting up, log in locally to DSRM (your desktop will indicate you're in 'Safe Mode'), open up the backup program (in this example I used the native Windows Server Backup), and restore the System State using the 'Recover' option:



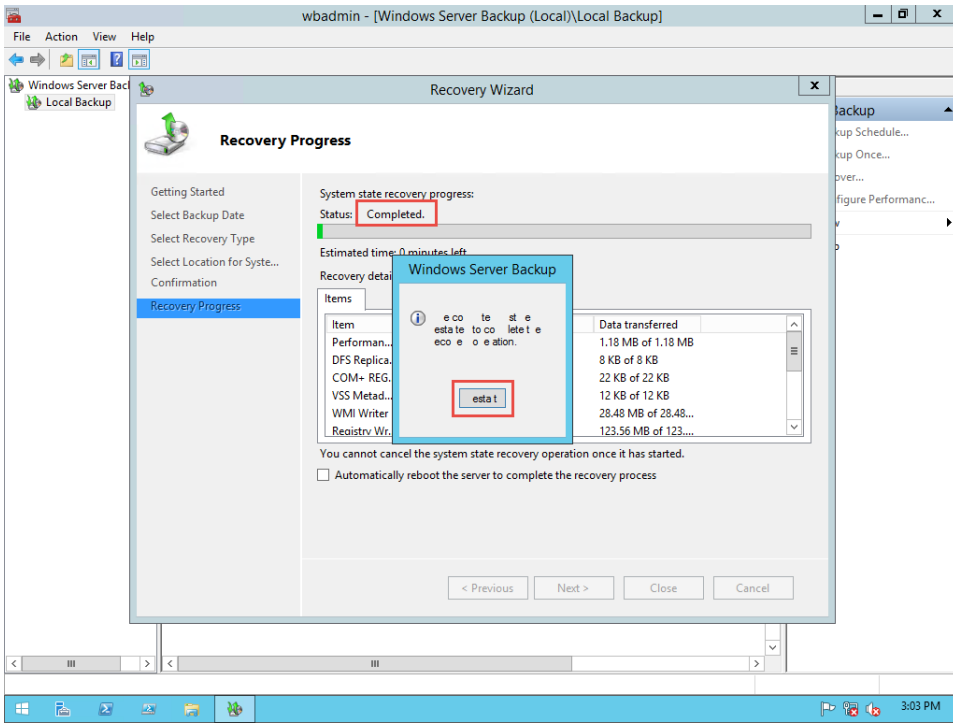
Keep the 'authoritative restore' checkbox CLEAR (because later we will manually specify what we want to authoritatively restore):



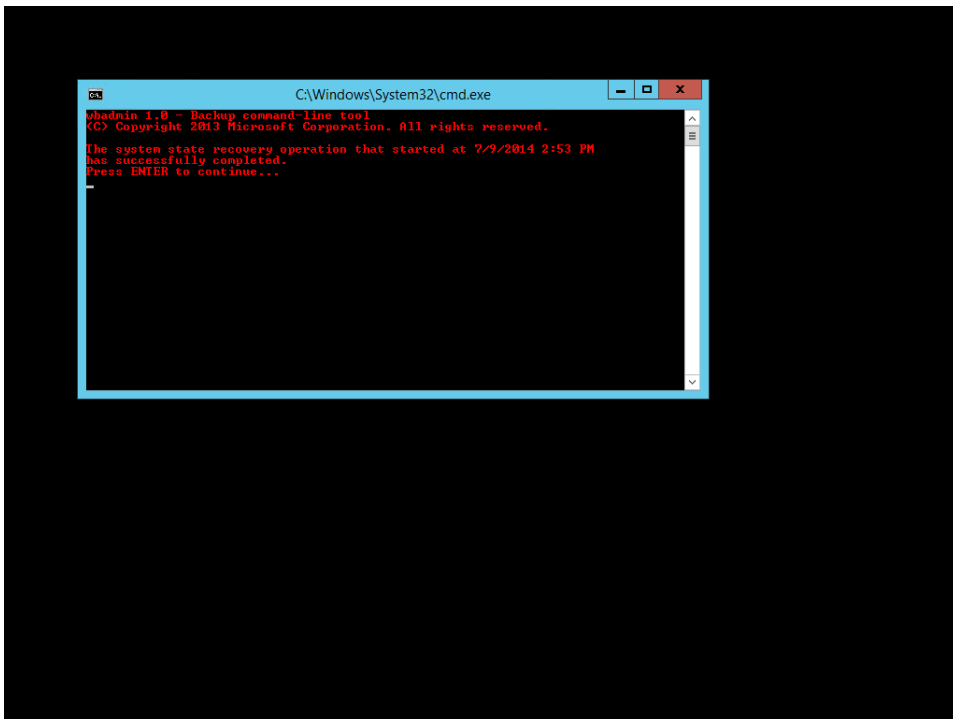
Do NOT automatically reboot:



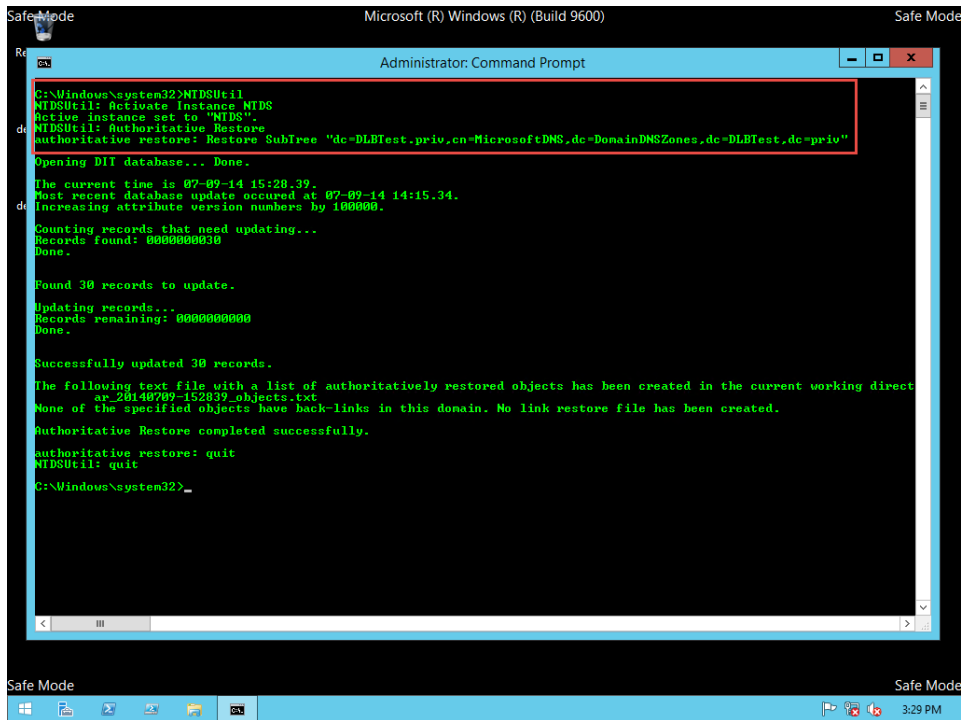
In my tests, once Windows Server Backup is done I'm pretty much forced to reboot (which might be good because the GUI sometimes gets flakey, as seen in this screenshot), and the MSCConfig.exe settings should still make the DC bootup into DSRM (but if the GUI is stable enough, then check MSCConfig.exe to be sure):



On boot, you will be told that the System State was recovered, and you'll need to press 'enter':



Next, run NTDSUtil.exe and perform the authoritative restore on the ADI DNS zone:



```
Safe Mode Microsoft (R) Windows (R) (Build 9600) Safe Mode
Administrator: Command Prompt
C:\Windows\system32>NTDSUtil
NTDSUtil: Activate Instance NTDS
Active instance set to "NTDS".
NTDSUtil: Authoritative Restore
Authoritative restore: Restore SubTree "dc=DLBTest.priv, cn=MicrosoftDNS, dc=DomainDNSZones, dc=DLBTest, dc=priv"
Opening DIT database... Done.
The current time is 07-09-14 15:28:39.
Most recent database update occurred at 07-09-14 14:15:34.
Increasing attribute version numbers by 100000.
Counting records that need updating...
Records found: 000000030
Done.
Found 30 records to update.
Updating records...
Records remaining: 000000000
Done.
Successfully updated 30 records.
The following text file with a list of authoritatively restored objects has been created in the current working direct
at_20140709-152839.objects.txt
None of the specified objects have back-links in this domain. No link restore file has been created.
Authoritative Restore completed successfully.
authoritative restore: quit
NTDSUtil: quit
C:\Windows\system32>
```

Last, change MSConfig.exe back to normal, and reboot.

DNSCmd.exe Backup and Restore of ADI DNS Zone:

I don't believe this method is supported or even complete, especially considering permissions, timestamps, and multiple SOAs, but here's what I've found online:

Backup:

DNSCmd.exe [ServerName] /zoneExport ZoneName ZoneExportFile

example: DNSCmd.exe DLB-ADDS1.DLBTest.priv. /zoneExport DLBTest.priv. DLBTest.priv.bak

Restore:

<http://sysbadmin.wordpress.com/2012/10/02/how-to-backuprestore-an-active-directory-integrated-dns-zone/>

- Hop onto the DNS Management Console and delete the zone
- Rename your zone backup to have a .dns extension, in the example above this would go from `example.com.bak` to `example.com.dns`
- Create a new zone with the FQDN of the zone you deleted, if using the New Zone Wizard be sure to uncheck the Store in Active Directory option.
- When prompted to create a new zone file or use an existing file, choose an existing file, the wizard should automatically fill in the zone FQDN with the .dns extension, this should look the same as your renamed zone file (`example.com.dns`)
- Complete the wizard
- Check the zone information is as per the zone before the changes
- If all is well, simply change the zone type to Active Directory Integrated.