

Re: Best Way for restoring AD in a test lab

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2005-03/1291.html

From: Paul Bergson (*pbergson_nospam_at_allete.com*)

Date: 03/15/05

Date: Tue, 15 Mar 2005 08:01:12 -0600

Well do a backup and restore following most of the procedures outlined. Just do a backup on a production dc. In the lab promote a test server in it own environment and then do the restore on that dc and then follow the seizure, etc...

--

Paul Bergson MCT, MCSE, MCSA, CNE, CNA, CCA

This posting is provided "AS IS" with no warranties, and confers no rights.

"Rustom" <Rustom@discussions.microsoft.com> wrote in message

news:79B7526C-96D8-4BC4-9936-D5CACBE10CD1@microsoft.com...

> I need to conduct this process with a backup utility as I need to restore the

> DC to the test lab with the same Server Name and this is our DR process.

>

> Thanks

>

> "Paul Bergson" wrote:

>

> > I promo a machine in production, back it up and demote it. Move it to a

> > protected space and restore it and whah lah I have a system up and running.

> > I do have to go back and do some minor clean up mainly dns since we run

> > integrated dns.

> >

> > ++++++

> > +++++ See Below +++++

> > ++++++

> >

> >

> >

> > Creating A Test Domain

> >

> >

> >

> > This document was prepared for the building of a copy of the production

> > Active Directory. Following these steps will define how to rebuild the

> > entire Microsoft Active Directory for a test domain. *** Be careful ***

> >

> >

> >

> > The first set of steps is to get a good pc into the production domain.

Once

> > this pc is a member it needs to be promoted and be a healthy participant

in

> > the network. The new DC then needs to be removed from the network

microsoft.public.windows.server.active_directory: Re: Best Way for restoring AD in a test lab

```
before it
> > is restarted (From its restore) to prevent any replication activity from
> > damaging the production system. Reconnection to the production system
will
> > create major problems in the production system. x.x.201.101 is the only
IP
> > Address that has access to the production system via an allowed rule on
the
> > router. A windows 2000 workstation can be used to connect to the
internet
> > and the production system, not a test DC!
> >
> >
> > 1. Shutdown ALL pc's within the sub-net x.x.210.x
> >
> > 2. Remove the physical cable for the new pc and build
the
> > member server (This all should reside within the test domain)
> >
> > 3. Re-connect the cable and join the Domain_Name.com
domain
> >
> > . Select the IP Address x.x.210.101
> >
> > . Select the mask to 255.255.255.0
> >
> > . Select the Gateway x.x.210.250
> >
> > . Point the DNS services to a production AD DNS server
> >
> > 4. Promote the server to a Domain Controller (DC) via
> > dcpromo.exe
> >
> > 5. Promote the server to a Global Catalog Server
> >
> > 6. Let the system sit idle overnight for Replication to
> > sync up
> >
> > 7. Open up a command prompt
> >
> > . dcdiag /v /test:ridmanager
> >
> > . Make sure no errors with the rid manager
> >
> > . Create an object on the new DC
> >
> > . Physically disconnect the cable
> >
> > . Bring up "Active Directory Users and Computers"
> >
> > . By disconnecting you force the system to attach locally
> >
> > . Create a test user with the account disabled
> >
> > . Reconnect the physical cable
> >
> > 8. At a command prompt type in NTBACKUP and do a
system
> > state backup saving the file to the local server
> >
> > 9. Demote this server to a member server with in the
```

microsoft.public.windows.server.active_directory: Re: Best Way for restoring AD in a test lab

```
> > production domain (DCPROMO)
> >
> > 10.           Physically disconnect the server from the network by
> > unplugging the cable from the hub
> >
> > 11.           Change the server IP Address within the test domain
> >
> > .           x.x.201.101 has access to the production system via an allowed
rule
> > on the router.  If this DC was ever re-plugged into the hub (Without the
IP
> > address being changed) it would take over ownership of the production
> > system, (Domain_Name.com) it would have catastrophic results!
> >
> > 12.           Re-Promote once this system has been disconnected and
the
> > ip changed
> >
> > .           Dcpromo
> >
> > .           Domain Name = Domain_Name.com
> >
> > .           NetBios Name = GOB
> >
> > .           Allow the promotion to create the DNS domain
> >
> > .           Once this DC is brought online (The DNS services on the member
> > server can be shut down), define it with Integrated Active Directory DNS
and
> > all name space records will be restored.  Make sure to bring up DNS and
> > select reload to refresh all data
> >
> > .           Active Directory Integrated
> >
> > .           Only Secure Updates
> >
> >
> >
> > 13.           Reboot this server and After the POST Select F8
> >
> > .           Scroll down and select the option
> >
> > "Directory Services Restore Mode (Windows 2000 domain controllers only)"
> >
> > 14.           Log on as the administrator (This is within the old SAM
> > account)
> >
> > 15.           Restore the System State from the previous NTBACKUP
> >
> > 16.           Re-boot the Domain Controller (DC)
> >
> >
> >
> > Now that the DC is restored it needs to take control of all Flexible
Single
> > Master Operation roles (FSMO and the File Replication service).  Because
of
> > this utilities need to be loaded off of the Windows 2000 install CD.
> > NTDSUTIL will perform most of these steps.  Since this is the first DC
it
> > needs to be a Global Catalog server and validate that it is the primary
> > server in the domain.
```

microsoft.public.windows.server.active_directory: Re: Best Way for restoring AD in a test lab

```
> >
> >
> >
> > 17.          After the POST Select F8
> >
> > .          Scroll down and select the option
> >
> > "Directory Services Restore Mode (Windows 2000 domain controllers only)"
> >
> > 18.          Log on as the administrator (This is within the old SAM
> > account)
> >
> > 19.          Install the Windows 2000 Active Directory
Administration
> > Tools from the server cd
> >
> > .          D:\i386\ Adminpak.msi
> >
> > 20.          Install the Windows 2000 Server Resource Kit from the
> > server cd
> >
> > .          D:\support\tools\2000rkst.msi
> >
> > 21.          Re-boot the Domain Controller (DC)
> >
> > 22.          Log on as the administrator (This is with the AD
account)
> >
> > 23.          Reset the ip address to the test domain, the restore
resets
> > the ip address.  Make sure to also point the dns server to itself as
well
> >
> > 24.          Set this server as a Global Catalog (Ignore this step
in a
> > multi-domain environment and this DC holds the Infrastructure Master
Role)
> >
> > .          Click Start, click Run, type mmc, and then click OK
> >
> > .          On the Console menu, click Add/Remove Snap-in, click Add,
> > double-click Active Directory Sites and Services, click Close, and then
> > click OK
> >
> > .          Double Click Active Directory Sites and Services
> >
> > .          Double Click Sites
> >
> > .          Double Click MP-Default-Site
> >
> > .          Double Click Servers
> >
> > .          Double Click the DC
> >
> > .          Right Click on NTDS Settings and Select Properties
> >
> > .          If the "Global Catalog" check box is not checked, check it
> >
> > 25.          All Flexible Single Master Operations (FSMO) roles need
to
> > reside on this DC
> >
```

microsoft.public.windows.server.active_directory: Re: Best Way for restoring AD in a test lab

```
> > .      Seize the PDC
> >
> > .      Click Start and then click Run
> >
> > .      In the Open text box, type ntdsutil
> >
> > .      Type roles
> >
> > .      Type connections
> >
> > .      Type connect to server <DC name>
> >
> > .      Type q
> >
> > .      Type seize pdc
> >
> > .      Click "Yes"
> >
> > .      Seize the Infrastructure master role
> >
> > .      Type seize infrastructure master
> >
> > .      Click "Yes"
> >
> > .      Seize the Domain Naming master role
> >
> > .      Type seize domain naming master
> >
> > .      Click "Yes"
> >
> > .      Seize the schema master role
> >
> > .      Type seize schema master
> >
> > .      Click "Yes"
> >
> > .      Seize the RID Master Role
> >
> > .      Type seize rid master
> >
> > .      Click "Yes"
> >
> > .      Type q
> >
> > .      Type q
> >
> > 26.      Remove all other DC server objects (Repeat this step
for
> > each DC) Q216498
> >
> > .      Click Start and then click Run
> >
> > .      In the Open text box, type ntdsutil
> >
> > .      Type metadata cleanup
> >
> > .      Type connections
> >
> > .      Type connect to server <DC>
> >
> > .      Type q (The metadata cleanup prompt should now show)
> >
```

microsoft.public.windows.server.active_directory: Re: Best Way for restoring AD in a test lab

```
> > .      Type select operation target
> >
> > .      Type list domains (A list of domains should be displayed)
> >
> > .      Type select domain <#> (This is the domain of the server to be
> > pruned)
> >
> > .      Type list sites (A list of sites should be displayed)
> >
> > .      Type select site <#> (This is the site of the server to be
pruned)
> >
> > .      Type list servers in site (A list of servers should be
displayed)
> >
> > .      Type select server <#> (This is the server to be pruned)
> >
> > .      Type q
> >
> > .      Type remove selected server (You should get confirmation of the
> > removal)
> >
> > .      Type q
> >
> > .      Type q
> >
> > 27.          Remove all other DC orphaned records in Active
Directory
> > (Repeat this step for each DC) Q216498
> >
> > .      Click Start - Programs - Windows 2000 Support Tools - Tools -
ADSI
> > Edit
> >
> > .      Delete the computer account in OU=Domain Controllers,
> > DC=Domain_Name,DC=com
> >
> > .      Delete the FRS member object in CN=Domain System Volume (SYSVOL
> > share),CN=File Replication Service,CN=System,DC=Domain_Name,DC=com
> >
> > 28.          Remove all other DC orphaned records in DNS
> >
> > .      Click Start - Programs - Administrative Tools - DNS
> >
> > .      Click <DC>.Domain_Name.com - Forward Lookup Zones -
Domain_Name.com
> >
> > .      Delete the cname (alias) of all other DC's
> >
> > .      Delete the a record of all other DC's
> >
> > 29.          This DC needs to be the File Replication Service Master
> > (Q316790)
> >
> > .      Stop the File Replication service on the DC
> >
> > .      Make sure the following folders exist, if not create them
> >
> > .      C:\WINNT\SYSVOL\staging
> >
> > .      C:\WINNT\SYSVOL\sysvol (Share as SYSVOL)
> >
```

microsoft.public.windows.server.active_directory: Re: Best Way for restoring AD in a test lab

```
> > .           C:\WINNT\SYSVOL\sysvol\Domain_Name.com
> >
> > .           copy the contents of C:\WINNT\SYSVOL\domain
to
> > this folder
> >
> > .           Start Registry Editor (Regedt32.exe)
> >
> > .           Locate and then click the BurFlags value under the following
key in
> > the registry:
> >
> > .
> >
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NtFrs\Parameters\Backup
> > /Restore\Process at Startup
> >
> > .           On the Edit menu, click DWORD, click Hex, type D2, and then
click
> > OK
> >
> > .           Quit Registry Editor
> >
> > .           Restart the File Replication Service
> >
> > .           Check the FRS event viewer to see if the system states that the
> > sysvol is now being shared and defines all the paths
> >
> > 30.           Ensure that the DC has registered the proper computer
role
> >
> > .           Enter net accounts at a dos prompt
> >
> > .           The computer role should say "primary"
> >
> >
> >
> > Finally any information related to the old DC's need to be purged from
AD.
> >
> >
> >
> > 31.           Re-boot the Authoritatively restored DC
> >
> > 32.           Within the production system delete the test user and
> > computer account
> >
> > 33.           Within the production system delete the server object
> > within the site that it was placed into for replication
> >
> >
> >
> > Note: The File Replication Service can prevent the computer from
becoming a
> > Domain Controller (See below).  If when doing a dcdiag a message states
that
> > the rid pool is corrupt, what is probably happening is there are
problems
> > with replication.  Check the "File Replication Service" Event Log.  Also
> > make sure that all sub-folders are available within c:\winnt\sysvol.
> >
> > To re-test just the rid pool:           dcdiag /v
```

microsoft.public.windows.server.active_directory: Re: Best Way for restoring AD in a test lab

```
> > test:ridmanager
> >
> >
> >
> >
> >
> >
> > Never again connect this server to the production system!!!
> >
> >
> >
> >
> >
> > When you restore a domain controller from backup (or when you restore
the
> > System State), the FRS database is not restored because the most
up-to-date
> > state exists on a current replica instead of in the restored database.
When
> > FRS starts, it enters a "seeding" state and then tries to locate a
replica
> > with which it can synchronize. Until FRS completes replication, it
cannot
> > share Sysvol and Netlogon.
> >
> > If you restore all of the domain controllers in the domain backup, all
the
> > domain controllers enter the seeding state for FRS and try to
synchronize
> > with an online replica. This replication does not occur because all of
the
> > domain controllers are in the same seeding state. Setting the primary
domain
> > controller FSMO role holder to be authoritative forces the domain
controller
> > to rebuild its database based on the current contents of the system
volume.
> > When that task is completed, the Sysvol and Netlogon shares are shared.
All
> > the other domain controllers can then start synchronizing from the
online
> > replica
> >
> > (See - Q316790)
> >
> >
> >
> >
> >
> > --
> >
> > Paul Bergson MCT, MCSE, MCSA, CNE, CNA, CCA
> >
> > This posting is provided "AS IS" with no warranties, and confers no
rights.
> > Be careful and understand all steps!!!!!!!!!!!!!!!!!!!!!!
> > This works in my environment that doesn't mean it will work in
> > yours!!!!!!!!!!!!!!!!!!!!!!
```

microsoft.public.windows.server.active_directory: Re: Best Way for restoring AD in a test lab

```
> > If you screw up you could be reloading your Production
AD!!!!!!!!!!!!!!!!!!!!!!
> >
> >
> > "Rustom" <Rustom@discussions.microsoft.com> wrote in message
> > news:4C6FE9C2-B03E-4838-938F-4F40D43D5807@microsoft.com...
> > > What is the best practice with regards to restoring Active Directory
to a
> > > test lab from production. I have two domains (Seperate Domain Trees)
> > within
> > > a forest.
> > >
> > > I am assuming I should backup and restore the production system states
on
> > > identical machines in the lab? Should the servers in lab be built
with
> > the
> > > same name and in a workgroup? Or should I DCPROMO them then conduct
the
> > > restore.
> > >
> > > I will also use the NTSUTIL and conduct an authoritative restore.
> > >
> > > Thanks for clarifying...
> >
> >
> >
```