Resources: Virtualizing Microsoft Active Directory

The purpose of this document is to collect together resources into one useful document on the topicof Virtualizing Microsoft Active Directory.

There are many guides, discussions, white papers and blog articles on virtualizing AD - because lots of VMware customers ARE virtualizing their product AD systems, in fact some chose AD as the very first application to virtualize (why the first? Because the people running the virtualizaiton project are also the people who own the AD servers).

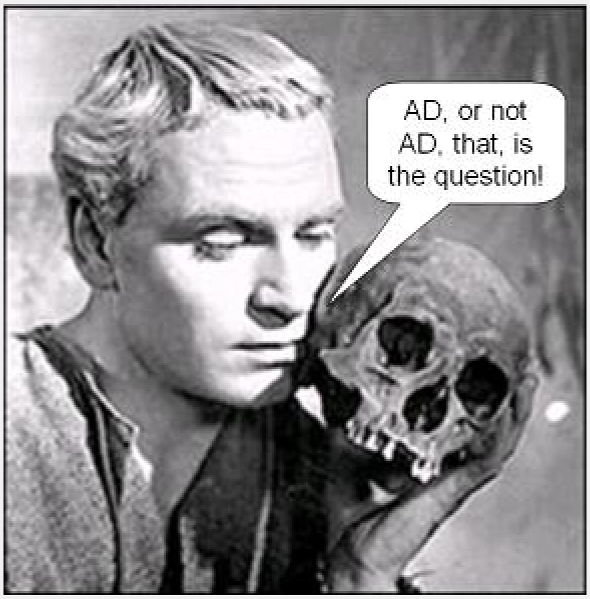
This is not a proven practice document because it doesn't say who or how someone has done this - instead, it brings together a substantial selection of resources together into a format that should guide you through this challenge and leaves the actual steps up to you. A proven practice would be an excellent companion to this document to show the specific decisions and steps taken for a specific situation.

So what is this document? It's a mixture of guidance and supporting resources. I've tried to order this document as you would work through the challenge, from "thinking about it" through to "operations" and the "disaster recovery" stage. The end result is a document that hopefully flows in a reasonable way, and provides enough information within itself without being just an index of links. For each link, I try to provide a summary and outline of the resource and not just the URL.

I hope you find this Resource useful - if you DO - please RATE this document at the bottom (also do that if you hate it!) - please leave comments, and please feedback - even better, JOIN IN!

Credits

Although this document brings together many links, it owes a lot to Chris Skinner's VMworld presentation TAC9710- Chris consistently gives a top class performance to over-booked rooms at VMworld, year after year, and I hope to see him again at VMworld Europe 2009.

Thinking about virtualizing Active Directory?	

Why, or Why Not?

I don't know of any reason NOT to virtualize AD... but I have heard some excuses (all can be overcome).

For **Why Not?** I've heard:

- **Time drift** - this is now largely solved on all platforms, even when the underlying CPU timer likes to run fast... You just need to make sure you are using VMtools timesync? Time sync is important with AD, with a five minute drift tolerance the norm. VMware Tools now have a feature called Deschedule Time Accounting
- **It's against my IT morals/beliefs** - get over yourself there are real business, operational and technology reasons to virtualize.
- **Our IT policy says AD should run on physical** - does it? I bet that policy was written without virtualization in mind... time to revist it.
- **It's not supported** - If you have premier support, yes it is: http://support.microsoft.com/kb/897615/

You will also find unsubstantiated (ie. statements that are not backed up by fact/data) "do not virtualize" comments, especially from Microsoft and folks like in this article Considerations when hosting Active Directory domain controller in virtual hosting environments - with lines like this: "We recommend that you locate critical server roles on domain controllers that are installed directly on physical hardware. Critical server roles include the following: Global catalog servers, Domain Name System (DNS) servers, Operations master roles, also known as flexible single master operations (FSMO)"

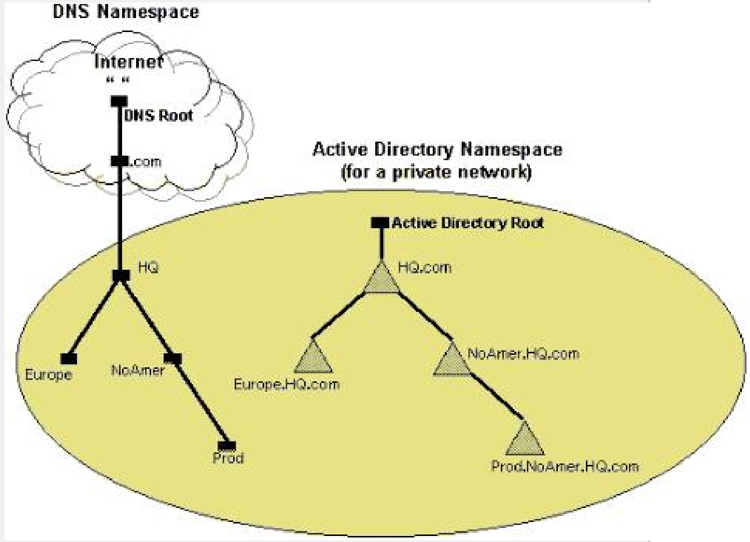
All of these server types have been virtualized and there is no reason not to. Why do Microsoft insist on keeping this on physical? Either you can make an educated guess, or ask them to provide data to back up the conjecture?

For **Why?** The reasons to virtualize are many, here are a few of my favourites - check out this VMTN thread for a longer version of below: Should DC, AD, DNS, DHCP servers be in VMware env?

- Build the AD applications on standard OS instances - you might be doing a great job of this already, but virtual machines help this enormously.
- **Eat your own dogfood** - how can you virtualize that Siebel app when you don't virtualize the servers you own - assuming sales own Siebel and you own the infrastructure apps...
- Leveraging virtualization to **make YOUR job easier** - need to deploy another AD server? Heard of VM templates? What about leveraging DRS and HA...
- Your old AD server is probably running on **OLD hardware** (3 or 5 years old?) - you COULD P2V that old machine directly onto VMware if you are scared of rebuilding it... and don't forget that the AD instance running slowly on that OLD hardware will run like lightening in a VM on the latest hardware - who said virtual machines were slow?!
- If you need **a way to migrate back** from virtual to physical to satisfy your vendor's crazy support statements, here's one you might **never** need: Virtual Machine to Physical Machine Migration
- If you are doing a **server consolidation project** - trying to save DC space - then the AD servers are probably taking up quite a bit of room... instead of eight AD pizza boxes using two NICs therefore 16 switch ports - they can use 8 or less! (assuming two ESX servers with redundant connections for 2 networks, or instead of 16 power sockets, use just 4... the list goes on
- Don't take my word for it - **read the testimonials** in this VMTN community article, started by Michael Knight, Discuss: Virtualisation of Active Directory Infrastructure ?
-
  - **kix1979** - About 15,000 users in about 10 countries all getting AD, DNS, DHCP from Domain controllers that are all virtualized
  - **mimpella** - Win 2003 AD support about 5000 users. Combination of Hardware and VM DCs. New DCs are Virtual. 14 Physical 11 VM
  - **sbeaver** - At my last life we had about 90-95% of all server virtualized. At the beging we had all DC running as VM's in over 26 offices world wide supporting between 5000 and 7000 users. We had well over 600 virtual machines in the Enterprise when I left.
  - **MR-T** - At our place we've got around 20,000 machines in the AD and we run a mix of physical and virtual. I'm not aware of any issues as a result of the virtual machines. Over the coming months I plan to introduce a few more DC's in the virtual world and begin to switch off the physical.

Remember, you don't have to go ALL VIRTUAL or ALL PHYSICAL - you can run a blend and get used to the feel of things... but I bet you $10 that you will soon be running all AD in virtual machines...

Designing Active Directory to run in Virtual Machines



OK - you've got over the hump of 'Should I, or shouldn't I?"

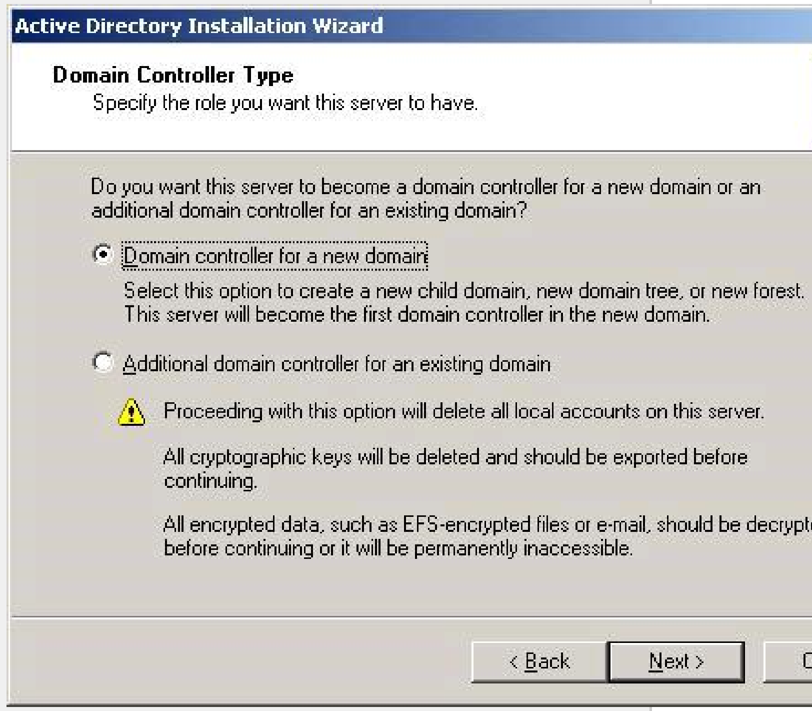
Now for the good news - you don't need to redesign your IT infrastructure to run AD in a virtual machine; just like any other application that you can virtualize it's just like running it in a physical machine. In fact, this is rule #1 - follow your normal plan, design, sizing for AD - but this time you are taking into account virtual networking (do you have a special network for AD network traffic? If so, is there a virtual switch connected to that network and available to the virtual machine?. But because you are using virtual machines, if you find out later that you got the design wrong you can just delete your VM and redo it again - the power of virtual!

Here are some design considerations:

- Consider creating a dedicated virtual switch for replication traffic between AD instances.
- Use a single vCPU virtual machine, not 2- or 4-vCPU - unless you have data to support the capacity increase to more processes.
- Draw up the network connections to show inbound and outbound network connections so you have a good, detailed diagram showing how the replication traffic works between nodes.
- If you are planning a slow, steady migration from physical to virtual - ie. take over or add virtual AD instances one server at a time - then this kind of risk averse approach might also warrant changing the weight and/or priority of the DNS SRV records for virtual machines
- Create a separate virtual disk for Active Directory database, log files, and SYSVOL

- Consider VM Permissioning - you probably want to restrict access to the AD VMs, so that probably means sticking them in their own folder with restrictions on who can see them, never mind perform operations on them. Guy Chapman has started a great document here on Proven Practice: VMware Infrastructure Permissioning from Sungard.
- Use DRS anti-affinity rules to make sure all your AD servers don't end up on one piece of hardware!
- As part of your availability commitments, leverage HA to recover your VMs instantly - don't forget that you can now have VM-level recovery, not just host-level.
- For DR, are you designing with Site Recovery Manager in mind?

Installing or Migrating Active Directory in Virtual Machines



Domain Controller Type

Specify the role you want this server to have.

Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?

● Domain controller for a new domain

Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.

○ Additional domain controller for an existing domain

⚠ Proceeding with this option will delete all local accounts on this server.

All cryptographic keys will be deleted and should be exported before continuing.

All encrypted data, such as EFS-encrypted files or e-mail, should be decrypt

before continuing or it will be permanently inaccessible.

One of the most important features is time synchronisation. You will hear old, crusty virtual machine folks talk about time drift and time synchronisation. Time used to drift in a VM (ie. the clock would go backwards, or even forwards) because of a few reasons - either the VM was so idle that it never got scheduled on a CPU to have its clock updated, or the OS kernel inside the VM was bad at time keeping, or even the underlying hardware clock didn't run correctly. Nowadays things are much improved - check out these resources:

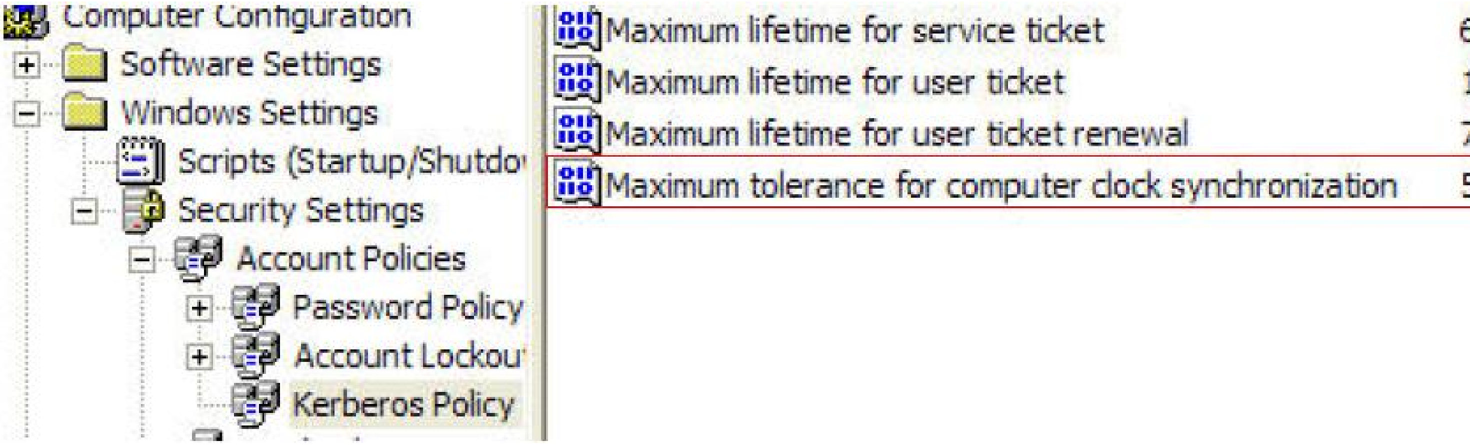
- VMtools Deschedule Time Accounting
- • Summary
  - • This document explains how to install and monitor VMDesched on Linux and Windows guest operating systems. It also describes timer interrupt virtualization issues resolved by VMDesched and how VMDesched works.
  - Outline

- Installing VMDesched on Linux Guest Operating Systems
- Installing VMDesched on Windows Guest Operating Systems
- Timer Interrupt Virtualization Issues Resolved by VMDesched
- How VMDesched Works

- Timekeeping in a VM
    - Summary
        - Because virtual machines work by time#sharing host physical hardware, a virtual machine cannot exactly duplicate the timing behavior of a physical machine. VMware virtual machines use several techniques to minimize and conceal differences in timing behavior, but the differences can still sometimes cause timekeeping inaccuracies and other problems in software running in a virtual machine. This information guide describes how timekeeping hardware works in physical machines, how typical guest operating systems use this hardware to keep time, and how VMware products virtualize the hardware.
    - Outline
        - Timekeeping Basics
        - Time and Frequency Units
        - PC Timer Hardware
        - VMware Timer Virtualization
        - Timekeeping in Specific Operating Systems
        - Synchronizing Virtual Machines and Hosts with Real Time
        - Time and Performance Measurements Within a Virtual Machine
        - Resource Pressure
        - Troubleshooting
        - Resources
- How to configure an authoritative time server in Windows Server 2003 (http://support.microsoft.com/kb/816042)
    - Summary
        - Windows includes W32Time, the Time Service tool that is required by the Kerberos authentication protocol. The purpose of the Windows Time service is to make sure that all computers that are running Microsoft Windows 2000 or later versions in an organization use a common time.
    - Outline
        - Configuring the Windows Time service to use an internal hardware clock
        - Configuring the Windows Time service to use an external time source
        - Troubleshooting
        - Reliable time source configuration
        - Manually-specified synchronization
        - All available synchronization mechanisms
        - Windows Time service registry entries
- VMware Sync and Windows Service (1318)
    - Summary

    - The most accurate way to keep guest operating system time synchronized with real time is to use the VMware Tools time synchronization function. You should not use the Windows Time service or other form of clock synchronization meant for physical machines to set the time in the guest operating system. Unlike a physical machine, a virtual machine is not always loaded and running on a CPU. A virtual machine's clock can't run when the virtual machine is not running. When the virtual machine gets to run on a CPU again, the virtual machine's clock needs to catch up to real time. The Windows Time service attempts to synchronize the virtual clock to an external time source on the network; it is not aware of the unusual clock behavior of a virtual machine, however, so it does not synchronize accurately. In some cases, the Windows Time service can do more harm than good. The VMware Tools time synchronization feature is aware of the built-in clock catch-up function in a virtual machine and can accurately synchronize the guest's clock to the host's clock.
  - Outline
    - VMware Tools time synchronization in the guest
    - When You Must Run Windows Time Service
- Installing and Configuring NTP on VMware ESX Server (1339)
  - Outline
    - Editing /etc/ntp.conf
    - Editing /etc/ntp/step-tickers
    - Editing /etc/hosts
    - ESX 3.0 Only: Enabling NTP Client for Firewall
    - Restarting and Monitoring the NTP Service
    - ESX Sever 2.0.0

Why is time so important? AD operations are time sensitive, File Replication Services use time-stamping, and AD servers use an MIT Kerberos derived authentication system - and Kerberos tickets are time sensitive... so AD is time sensitive:


Computer Configuration
Software Settings
Windows Settings
Scripts (Startup/Shutdo
Security Settings
Account Policies
Password Policy
Account Lockou
Kerberos Policy
Maximum lifetime for service ticket
Maximum lifetime for user ticket
Maximum lifetime for user ticket renewal
Maximum tolerance for computer clock synchronization

The current recommended practice for time keeping is External Clock <- ESX Server <- Virtual Machine <- Windows OS <- Active Directory

1. Use NTP on the ESX host to keep the host time in sync with an external clock - you should have an NTP source in your organization (see below on how to check).
2. Use VMtools inside the Virtual Machine to synchronise the guest with the host - do NOT use NTP inside the guest. How do you know if you are using NTP inside the guest? (see below to check)

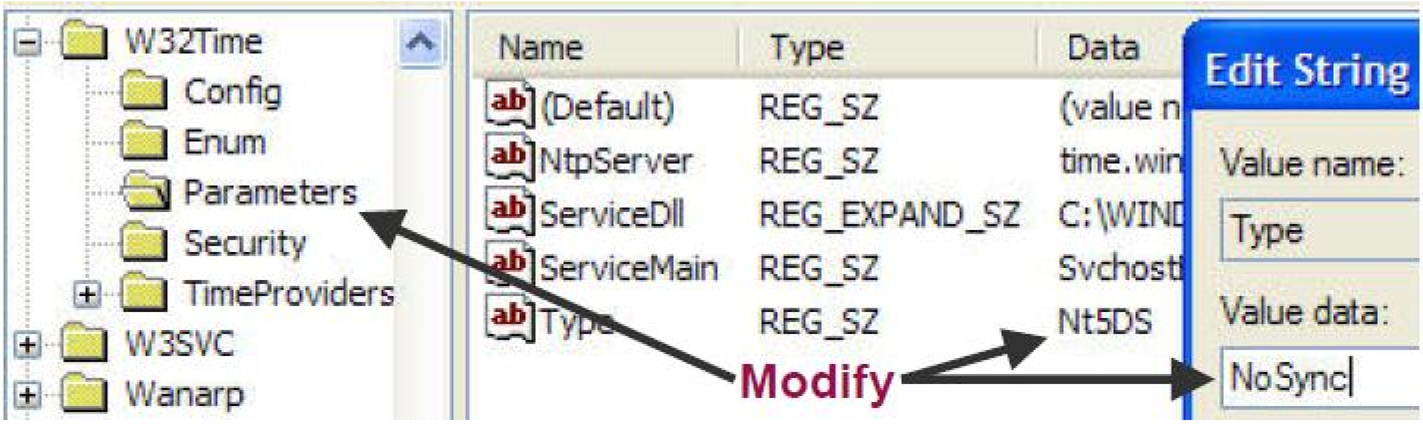
Tip: Where do I find the NTP source in my organization?

Asking the network and security folks is probably your best bet. They should have a published standard on time keeping within your organization. Network devices like routers all need to be in sync, as should web servers, so if you know the team that manages these then they should have the answer. You existing AD servers might be configured using W32Time to sync with an NTP server - so if you check out the next tip, you can find out the NTP servers that way.

In an existing AD server, check out the Registry setting W32Time -> Parameters -> NtpServer value - it might be something like time.windows.com,0x1 - but hopefully it's something different like pool.your.domain.com,0x1.

Tip: How do you know if you are using NTP inside the guest?

Check out the following Registry setting. If W32Time -> Parameters -> Type = NTP then you are using NTP. This needs to be set to NoSync, and you need to enable VMtools.

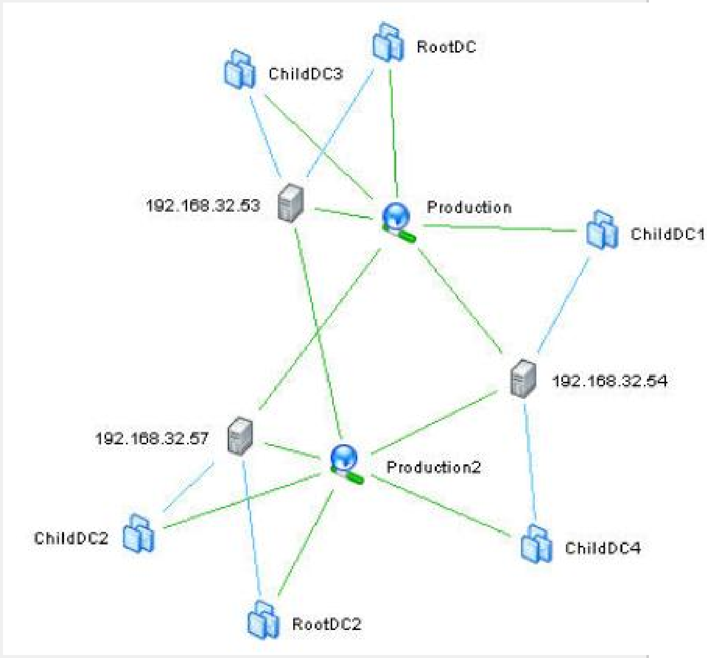


Name	Type	Data
(Default)	REG_SZ	(value n
NtpServer	REG_SZ	time.win
ServiceDll	REG_EXPAND_SZ	C:\WIND
ServiceMain	REG_SZ	Svchost
Type	REG_SZ	Nt5DS

Value name:
Type

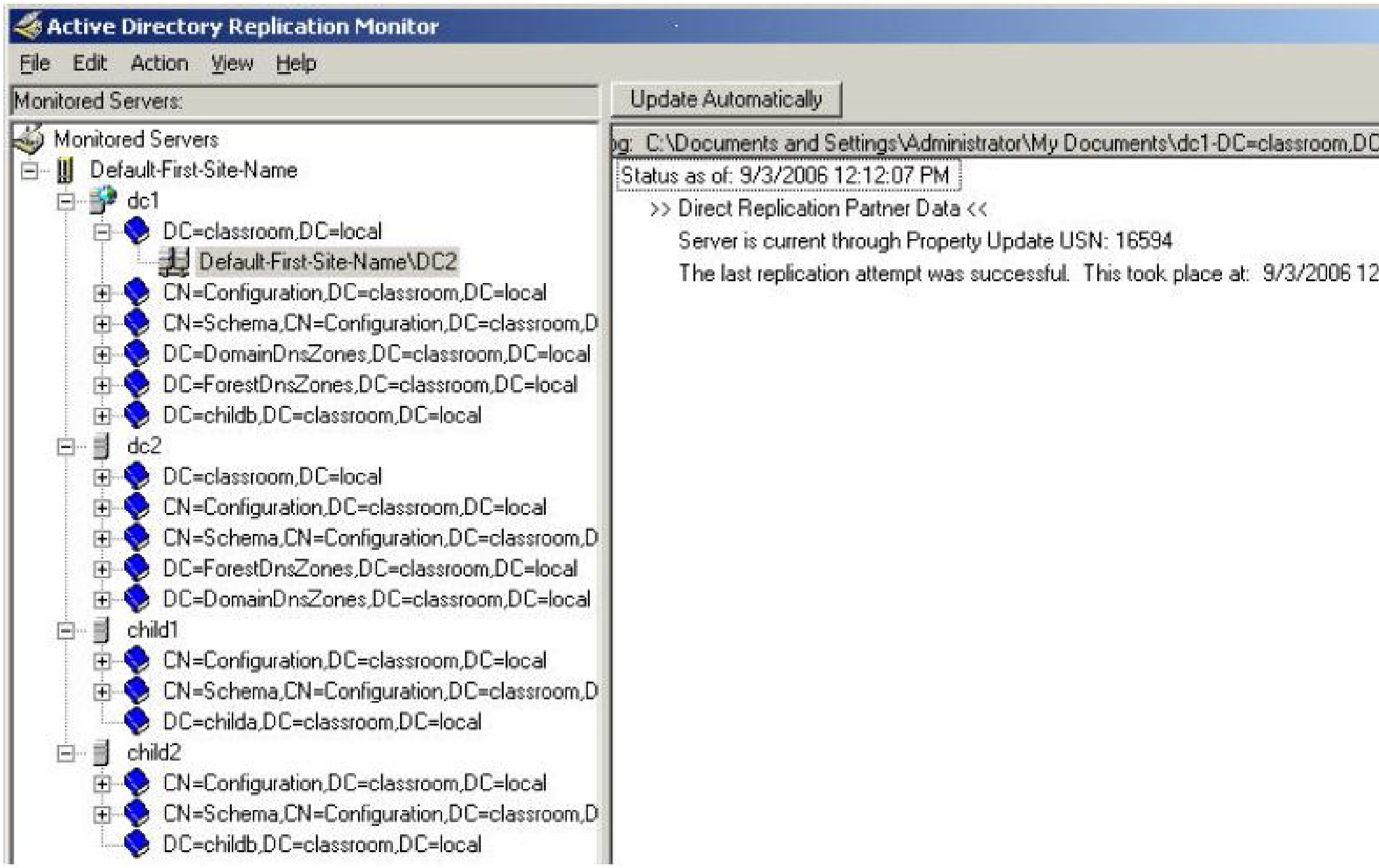
Value data:
NoSync

Testing / QA of AD in VMs



Here's a checklist of what to QA and check before you go live with AD (not all are specific to virtual machines, but provided here for completeness).

- Use VirtualCenters Network Maps to verify the network configuration
- Verify the Virtual Machine configuraitons meet the spec - 1vCPU, 512MB, 10GB Disk, 2 vNIC - whatever your standard is.
  - Is someone creating 2vCPU AD VMs?
- Use Replication Monitoring to confirm the inbound/outbound connections.


Active Directory Replication Monitor
File Edit Action View Help
Monitored Servers:
Update Automatically

```
Monitored Servers
  Default-First-Site-Name
    dc1
      DC=classroom,DC=local
        Default-First-Site-Name\DC2
      CN=Configuration,DC=classroom,DC=local
      CN=Schema,CN=Configuration,DC=classroom,D
      DC=DomainDnsZones,DC=classroom,DC=local
      DC=ForestDnsZones,DC=classroom,DC=local
      DC=childb,DC=classroom,DC=local
    dc2
      DC=classroom,DC=local
      CN=Configuration,DC=classroom,DC=local
      CN=Schema,CN=Configuration,DC=classroom,D
      DC=ForestDnsZones,DC=classroom,DC=local
      DC=DomainDnsZones,DC=classroom,DC=local
    child1
      CN=Configuration,DC=classroom,DC=local
      CN=Schema,CN=Configuration,DC=classroom,D
      DC=childa,DC=classroom,DC=local
    child2
      CN=Configuration,DC=classroom,DC=local
      CN=Schema,CN=Configuration,DC=classroom,D
      DC=childb,DC=classroom,DC=local
```

```
g:  C:\Documents and Settings\Administrator\My Documents\dc1-DC=classroom,DC
Status as of: 9/3/2006 12:12:07 PM
   >> Direct Replication Partner Data <<
      Server is current through Property Update USN: 16594
      The last replication attempt was successful.  This took place at:  9/3/2006 12
```

- Policy Testing
  - When you apply a group policy, is the AD instance being updated?
- Schema Changes
  - Are schema changes being applied to your AD instance?
- Migration/Upgrade testing
  - Test your P2V migration and/or an upgrade of your instance, leverage the virtualization tools like Converter and snapshots.
- Domain reconfigurations
  - Does your AD instance take part in AD reconfigurations?
- Deployment testing
  - Test the process to deploy your AD server, and to roll back the deployment.
- Disaster recovery planning
  - See the last section in this document

Operating AD in VMs

Common operational tasks checklist. Remember, that whilst YOU might adhere to these - how do you make sure everyone else does? This is the kind of operational consistency that separates the best from the rest. For example, how do you stop someone adding a redo log, then committing it - which is bad news for an AD server?

- Monitor the logon requests to ensure virtual machines are successfully responding
  - EXPLANATION
- Decommission physical domain controllers
  - Do not add to server sprawl by just adding more virtual AD servers; plan and manage the turn off of physical AD servers and measure the impact of your move from physical to virtual (power/ports/space/money saved).
- Perform regular system state backups, check that they complete correctly
  - Are you following the Microsoft standard, is this automated and is it monitored for success? How do you know that the last backup worked?
- Avoid snapshots or REDOsfor domain controller virtual machines
  - Is this part of your published operational policy, that all staff sign up to? How do you stop people (including yourself) from adding REDO logs to virtual machines? How do you monitor for REDO logs (electrify the fence!).
- Do not suspend domain controller virtual machines for long periods
  - Is this part of your published operational policy, that all staff sign up to? How do you stop people suspending AD virtual machines? How do you monitor for suspended virtual machines (electrify the fence!)
- Consistent and regular system state backups still very important
  - Make sure VMs are **not** outside of the normal backup system, if that system is working and best practice. If VMs are treated as an "exception" you might have problem.

Disaster Recovery

Here are some considerations for DR with AD:

- FSMO placement and optimization on Active Directory domain controllers
  - Summary
    - Active Directory domain controllers support multi-master updates for the replication of objects (such as user and computer accounts) in the Active Directory. In a multi-master model, objects and their properties can originate on any domain controller in the domain and become "authoritative" with replication. This article describes the placement of Active Directory Flexible Single-Master (FSMO) roles in the domain and forest.
  - Outline
    - FSMO availability and placement
    - General Recommendations for FSMO placement
- All Active Directory restorations should be performed using authoritative and non-authoritative technique
  - Do not recover an Active Directory database from a backup copy of an old virtual disk!
- Perform PROPER restores of AD instances, not improper
  - When an AD instance fails, do not restore from an old image, use the correct, approved and recommended recovery process
- Have you configered DRS anti-affinity rules to make sure all your AD servers don't end up on one piece of hardware!
- Do you use VMware HA to recover your VMs instantly - don't forget that you can now have VM-level recovery, not just host-level.
- For DR, are you designing with Site Recovery Manager in mind?