TAC 9710 - Virtualizing a Windows Active Directory Domain Infrastructure

Chris Skinner

Technical Instructor
Education Services

VMware, Inc.

VMWORLD 2006

Why Virtualize Active Directory?

- Hardware Consolidation
- Test and Development
- Security Control

Hardware Consolidation

- Combine multiple, single use boxes
- Standardization – eliminate imaging problems
- Reduce Product Activation issues

Test and Development

- Policy Testing
- Schema Changes
- Migration/Upgrade testing
- Domain reconfigurations
- Deployment testing
- Disaster recovery planning

Security control

- Physical access
- Administrative delegations
- Separate applications from Active Directory databases

Supported Operating Systems

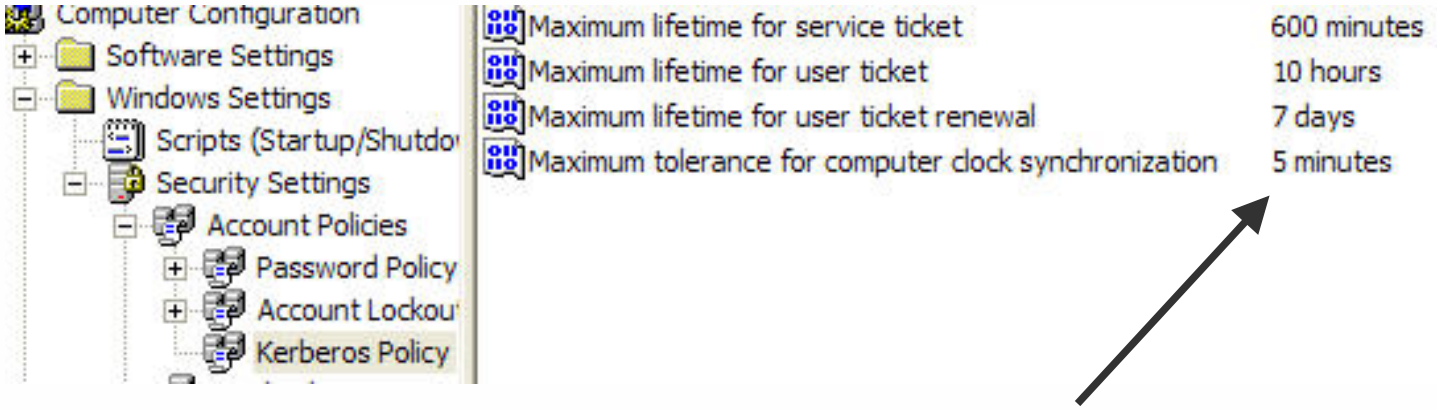
- Windows 2000
- Windows 2003 & R2
- Native Mode or Mixed Mode

Challenges to Virtualizing Active Directory

- Clock synchronization
- Network performance
- Multi-master replication model
- Security
- Potential single point of failure
- Disaster recovery

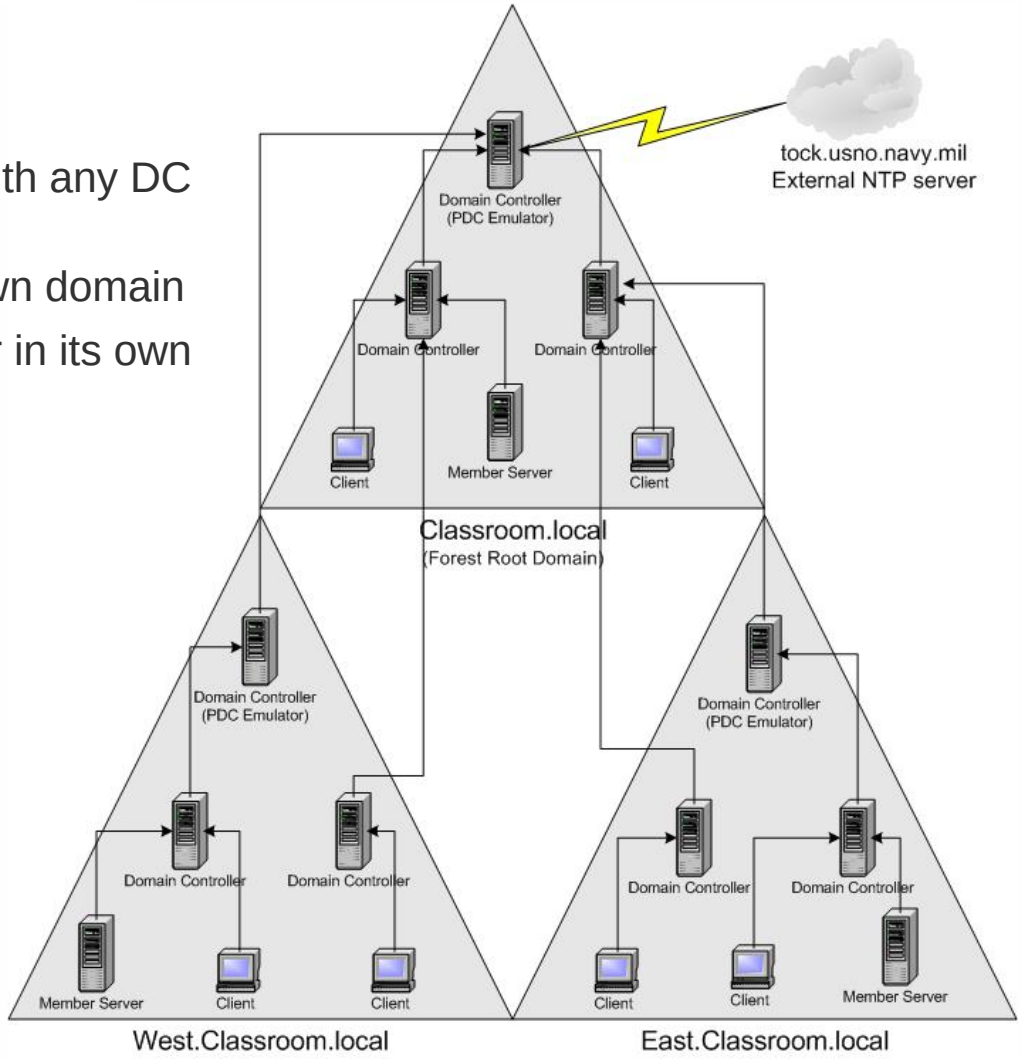
Clock Synchronization – Why So Important?

- Active Directory operations are critically time dependent
- MS Kerberos implementation allows a 5 minute tolerance
- File Replication Services (FRS) synchronizes scripts, database changes/updates, policies based, in part, on time-stamping



Time Server Hierarchies

- Child PDC emulators can sync with any DC in the parent domain
- Clients sync with any DC in its own domain
- DCs can sync with PDC emulator in its own domain or any DC in parent

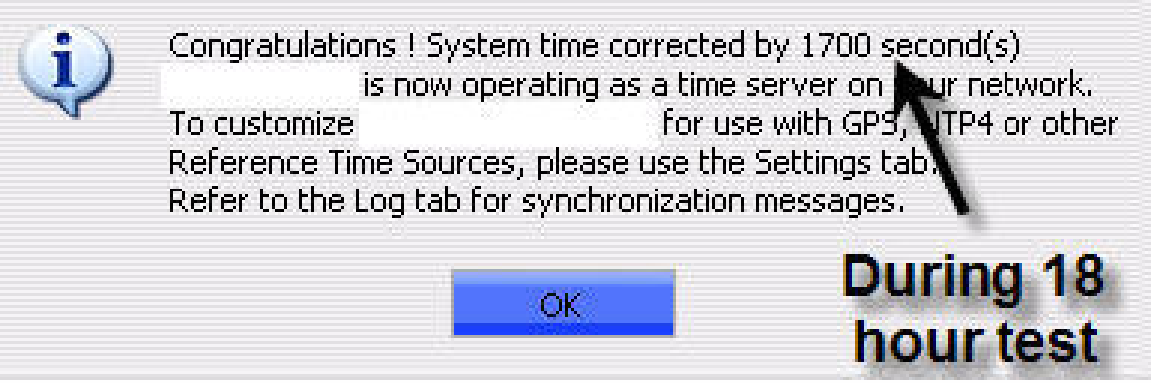


Source: Microsoft Corporation

Clock Synchronization – Virtualization Issues

- No CPU cycles needed – none given!
- Clock drifts can be significant in a relatively short period
- Idle cycles in a virtual machine is an Active Directory domain's worst enemy
- How do you combat time synchronization issues?

More than a 28 minute drift!



Clock Synching – Option A – Using W32Time

- Use Windows Time Service – NOT VMware Tools
- Define an alternative external time source for “master” time server

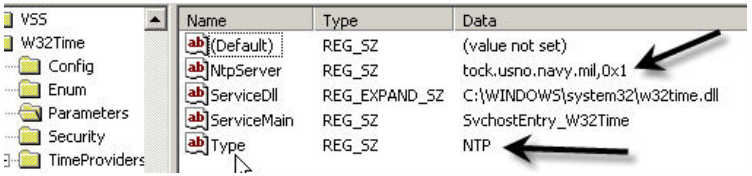
1. Modify Registry settings on the PDC emulator for the forest root domain:

   `HKLM\System\CurrentControlSet\Services\W32Time\Parameters`

   - Change **Type RED_SZ** value from **NT5DS** to **NTP**
   - Change **NtpServer** value from **time.windows.com,0x1** to an external stratum 1 time source, i.e. **tock.usno.navy.mil,0x1**

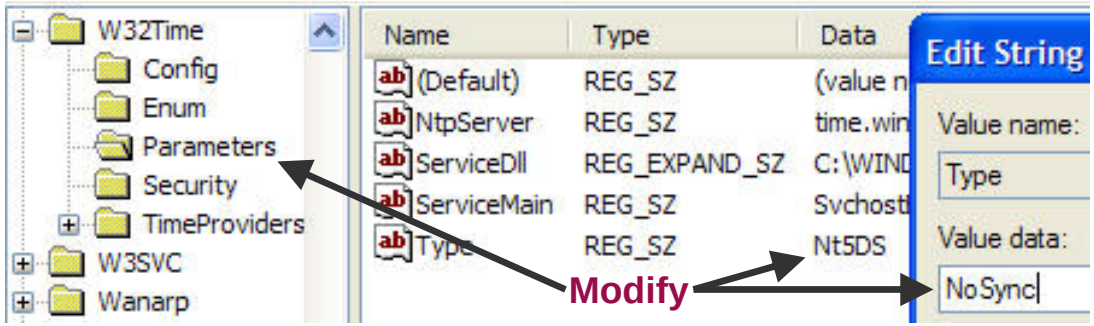
   `HKLM\System\CurrentControlSet\Services\W32Time\Config`

   - Change **AnnounceFlags REG_DWORD** from **10** to **5**
2. Stop and restart Time Service – **net stop w32time → net start w32time**
3. Manually force update → **w32tm /resync /rediscover**



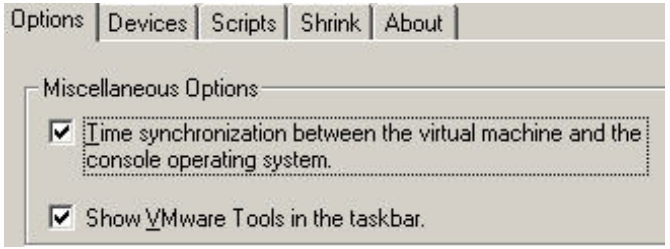
Clock Synching – Option B – Using VMware Tools

- Modify Windows Time Service – Use VMware Tools
  - Implement Domain Controllers Group Policy to modify registry:



- Enable ESX server NTP daemon to sync with external stratum 1 NTP source
  - VMware Knowledge Base ID# 1339
- Use VMware Tools Time Synchronization within the virtual machine

NOTE: VMware Tools time sync is designed to play "catch-up", not slow down!

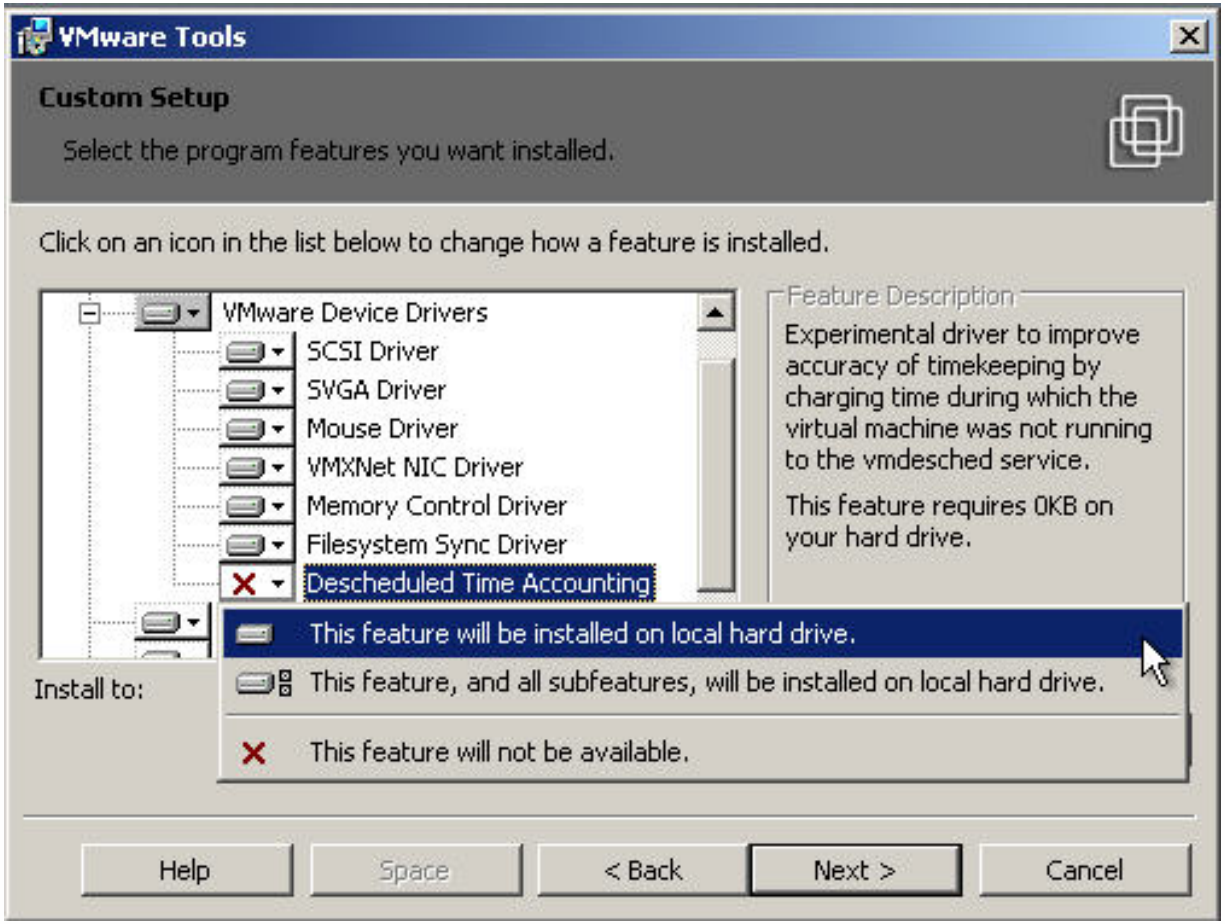


New Clock Synching – Descheduled Time Accounting

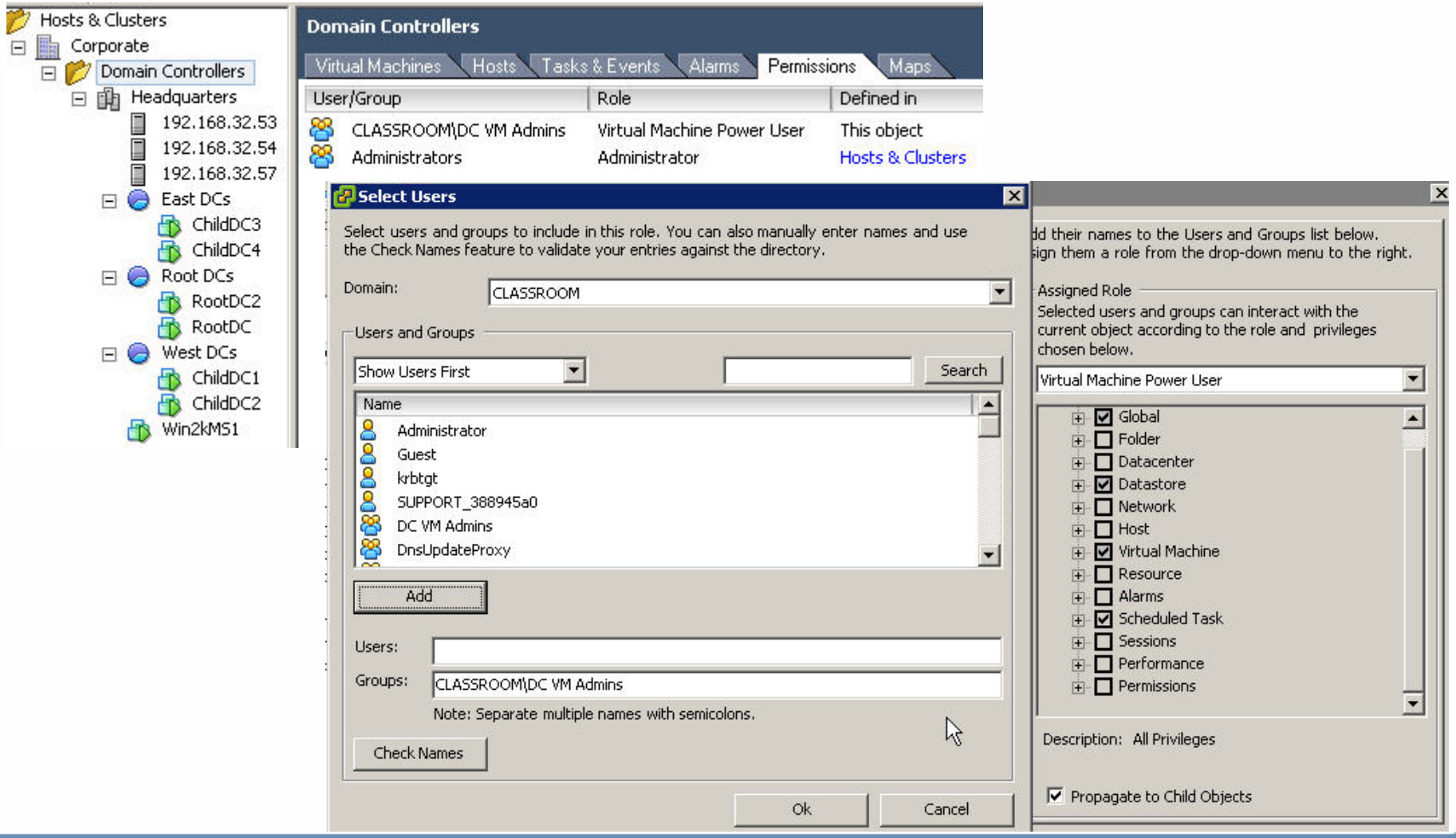
- VMware Tools experimental component
- Custom component for ESX 3.x VMs
- Currently for uniprocessor Windows and Linux VMs
- Improved accuracy for guest OSes CPU time accounting
- Allows quicker “catch-up” of time for guest OS
- Launches a VMDesched thread or process

Clock Synching – Descheduled Time Accounting (2)

- Perform a Custom installation of VMware Tools in Windows guest OS



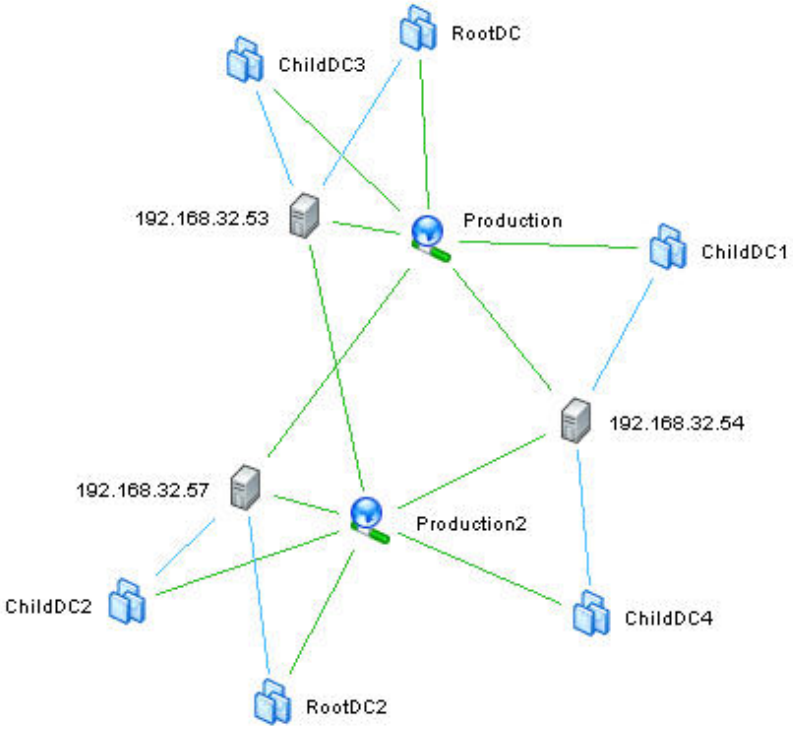
ESX 3.x/VC 2.x Security - VM Access Control

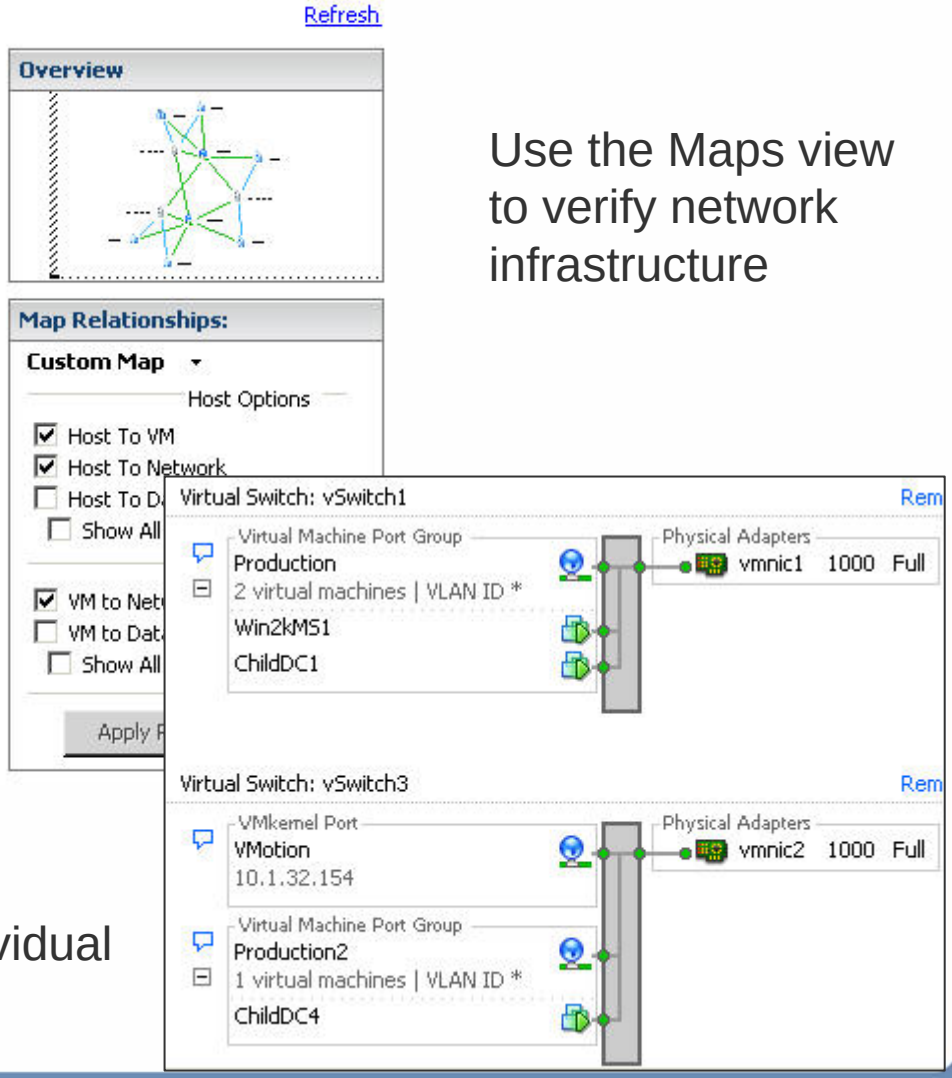


Transitioning from Physical to Virtual

- Start with a fresh system state backup for recovery
- Consider creating a dedicated virtual switch or virtual machine port group to isolate replication traffic
- Generally single processor virtual machines are adequate for domain controllers
- Create a separate virtual disk for Active Directory database, log files, and SYSVOL
- Validate inbound/outbound connections between physical and virtual machines
- Allow 24-48 hours for replication to complete
- Change the weight and/or priority of the DNS SRV records for virtual machines
- Monitor the logon requests to ensure virtual machines are successfully responding
- Decommission physical domain controllers

Network Connections



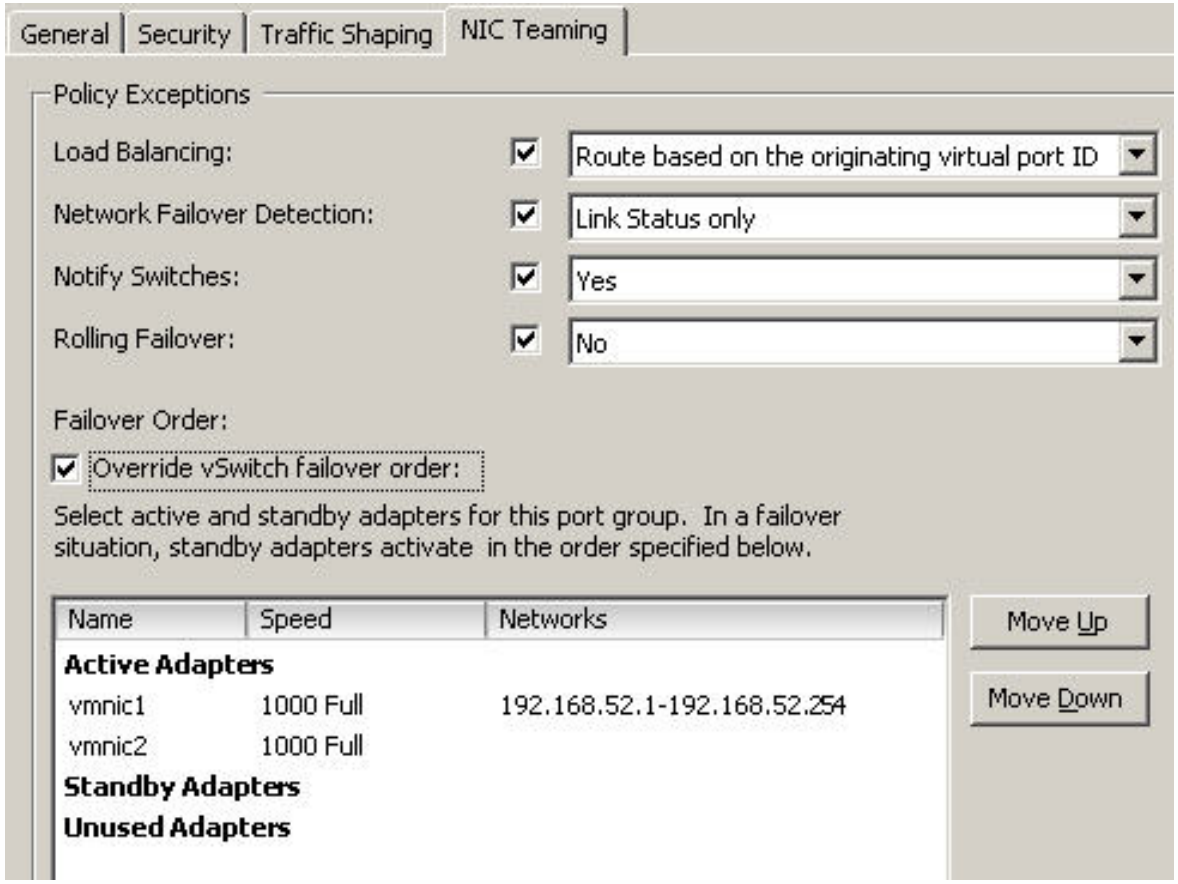


Use the Maps view to verify network infrastructure

Create separate VM port groups connected to individual NICs

Advanced Switch Settings - Networking

- ESX Server 3.x provides some more sophisticated network settings



Using Replication Monitor

- Validating Inbound Connections

Active Directory Replication Monitor

File Edit Action View Help

Monitored Servers:

Monitored Servers
- Default-First-Site-Name
  - dc1
    - DC=classroom,DC=local
    - CN=Configuration,DC=classroom,DC=local
    - CN=Schema,CN=Configuration,DC=classroom,DC=local
    - 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,DC=local
    - 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,DC=local
    - DC=childa,DC=classroom,DC=local
  - child2
    - CN=Configuration,DC=classroom,DC=local
    - CN=Schema,CN=Configuration,DC=classroom,DC=local
    - DC=childb,DC=classroom,DC=local

Update Automatically

Log: C:\Documents and Settings\Administrator\My Documents\Default-First-Site-Name-

Status as of: 9/3/2006 12:12:07 PM

Server Properties

General | Server Flags | FSMO Roles | Credentials

Inbound Replication Connections | TCP/IP Configuration

Below is a list of the inbound connection objects established for this domain controller:

Connection Name	Server Name	Admin-Generated?
0538dddd-32ad-49cd-9...	Default-First-Site-Na...	AUTO
360e077a-2da0-4043-8...	Default-First-Site-Na...	AUTO
ef98af74-fcb6-4738-a2...	Default-First-Site-Na...	AUTO

Below is an advanced description of why the inbound connection objects were establishe

Connection Name: 0538dddd-32ad-49cd-92e9-160bccf56312

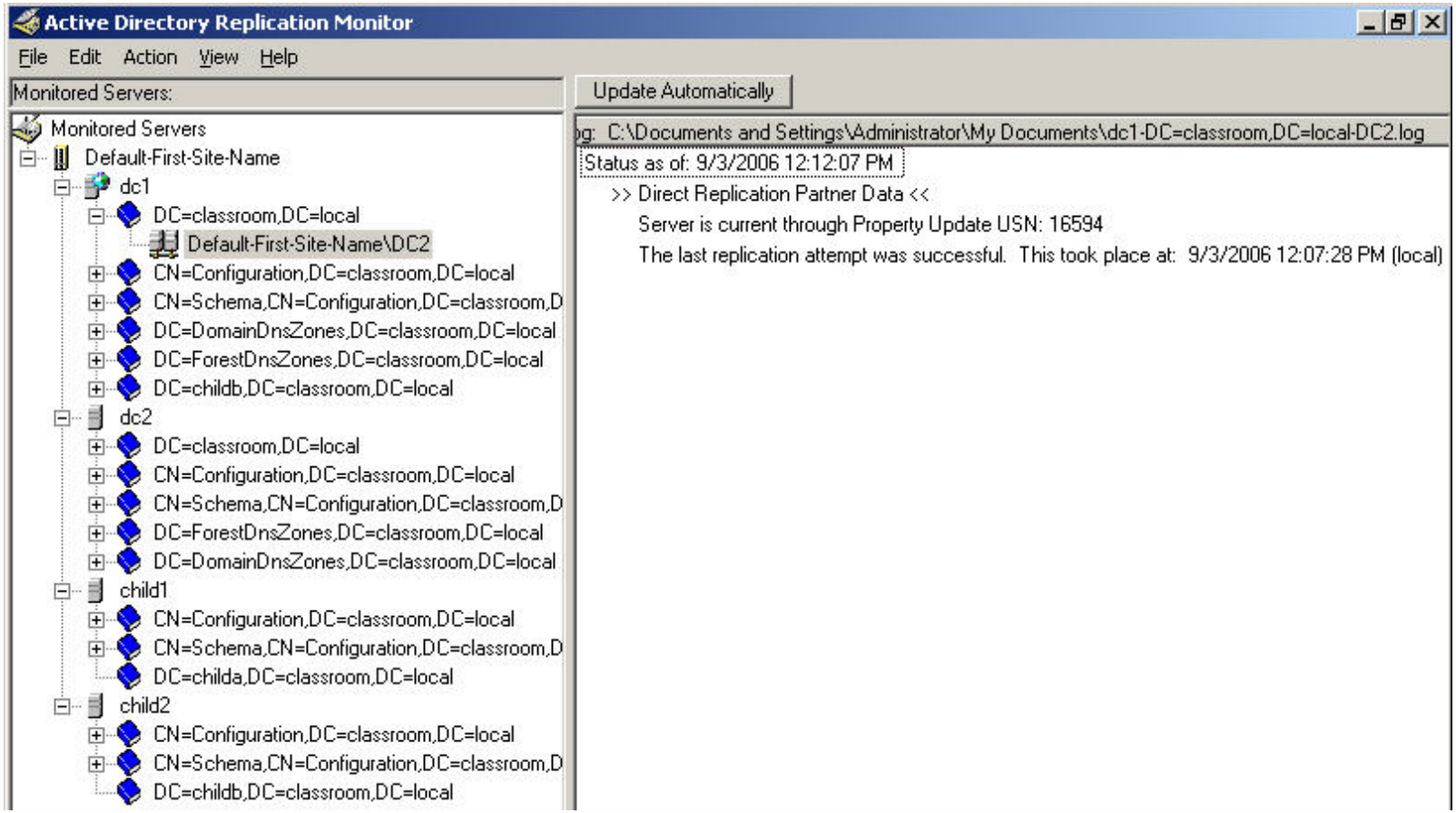
Replication Partner: Default-First-Site-Name\DC2
Administrator Generated?: AUTO

Reasons for this connection:

Directory Partition (DC=DomainDnsZones,DC=classroom,DC=local)
Replicated because the replication partner is a ring neighbor.

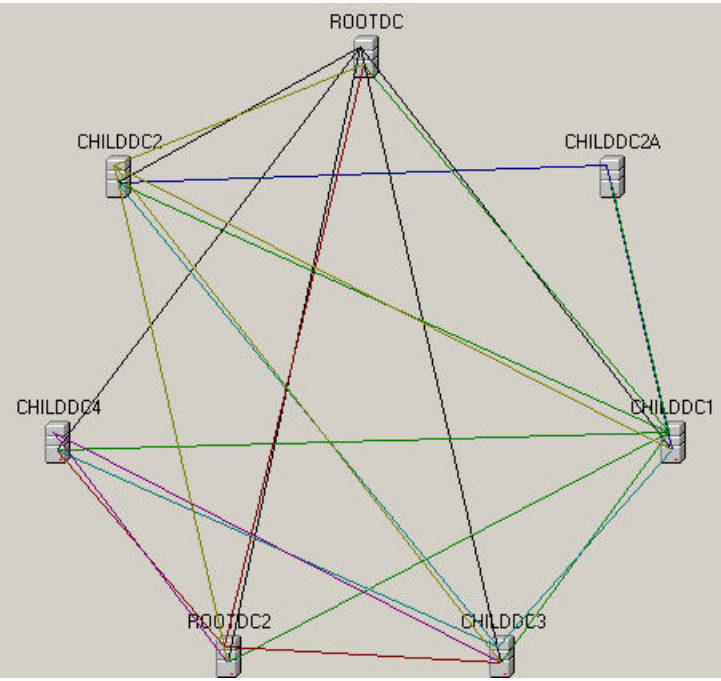
Using Replication Monitor (2)

- Successful Replication

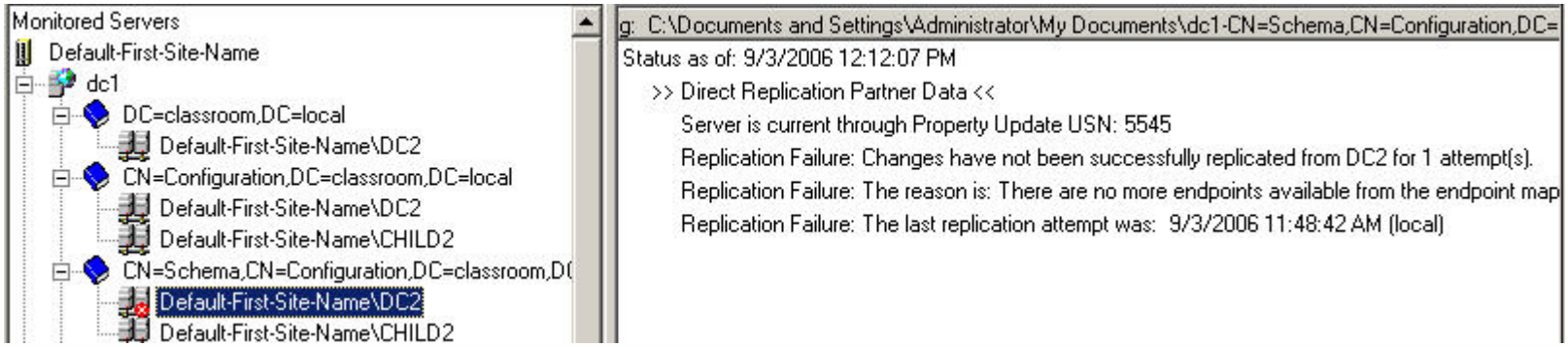


Replication Topology

- Checking Replication Topology



- Look for replication errors



DNS Modifications

- Modify the weight and/or priority of the DNS SRV records
- Specifically offload the authentication requests from the PDC emulator when possible
- DNS **weight** is the proportional distribution of requests among DNS servers
- DNS **priority** is the likelihood a server will receive a request
- PDC emulators should have one or both adjusted accordingly by adding:

  `HKLM\System\CurrentControlSet\Services\Netlogon\Parameters`

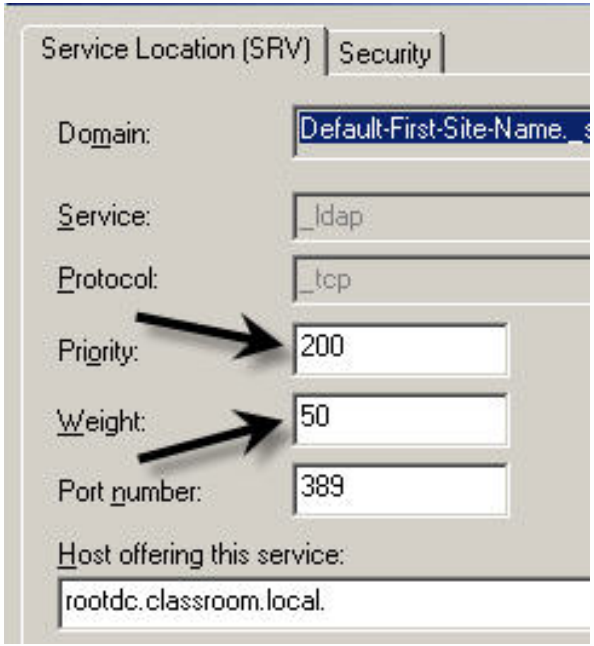
  - **LdapSrvWeight DWORD** decimal value of **25** or **50**

  `HKLM\System\CurrentControlSet\Services\Netlogon\Parameters`

  - **LdapSrvPriority DWORD** decimal value to **100** or **200**
- Physical domain controllers should be adjusted similarly to PDC emulator to decrease DNS dependencies on them

DNS Modifications

- Can also be changed within DNS manager
- Registry changes do not require a reboot

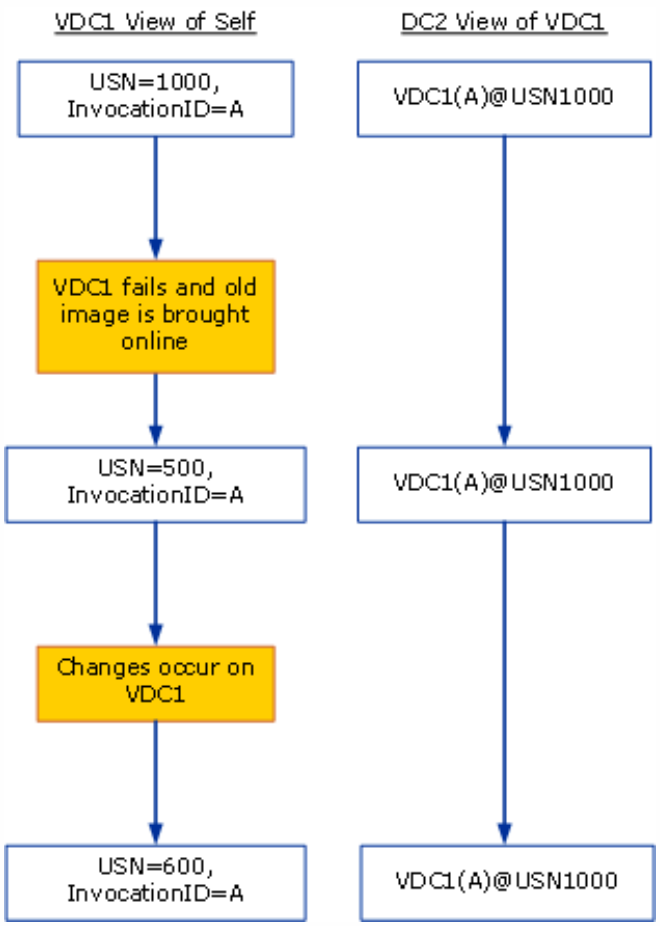


Disaster Recovery

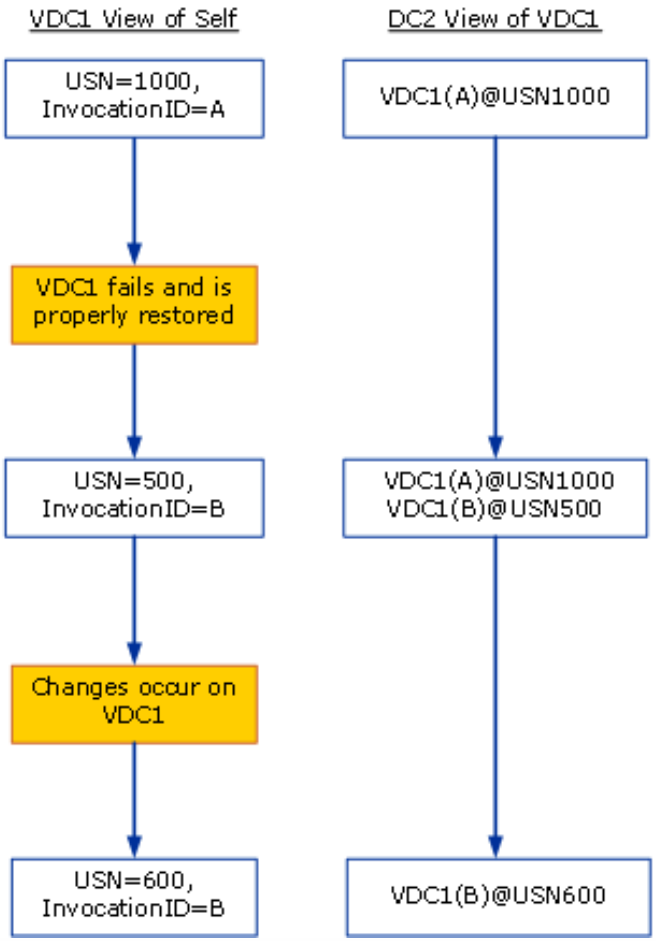
- Perform consistent system state backups
  - Eliminates hardware incapability when performing restore
- Follow Microsoft recommendations on FSMO role placement
  - http://support.microsoft.com/kb/223346
- All Active Directory restorations should be performed using authoritative and non-authoritative technique
  - Do not recover an Active Directory database from a backup copy of an old virtual disk!

Disaster Recovery Scenarios

Improper Restore of VM



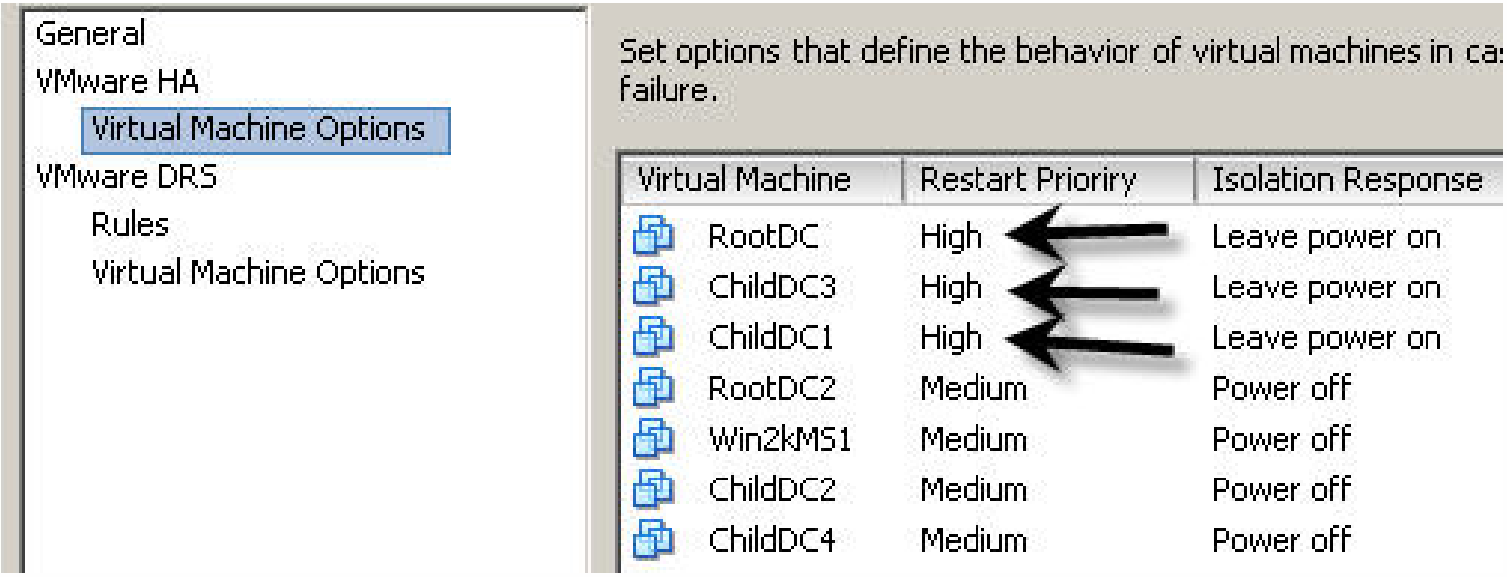
Proper Restore of VM



Source: Microsoft Corporation

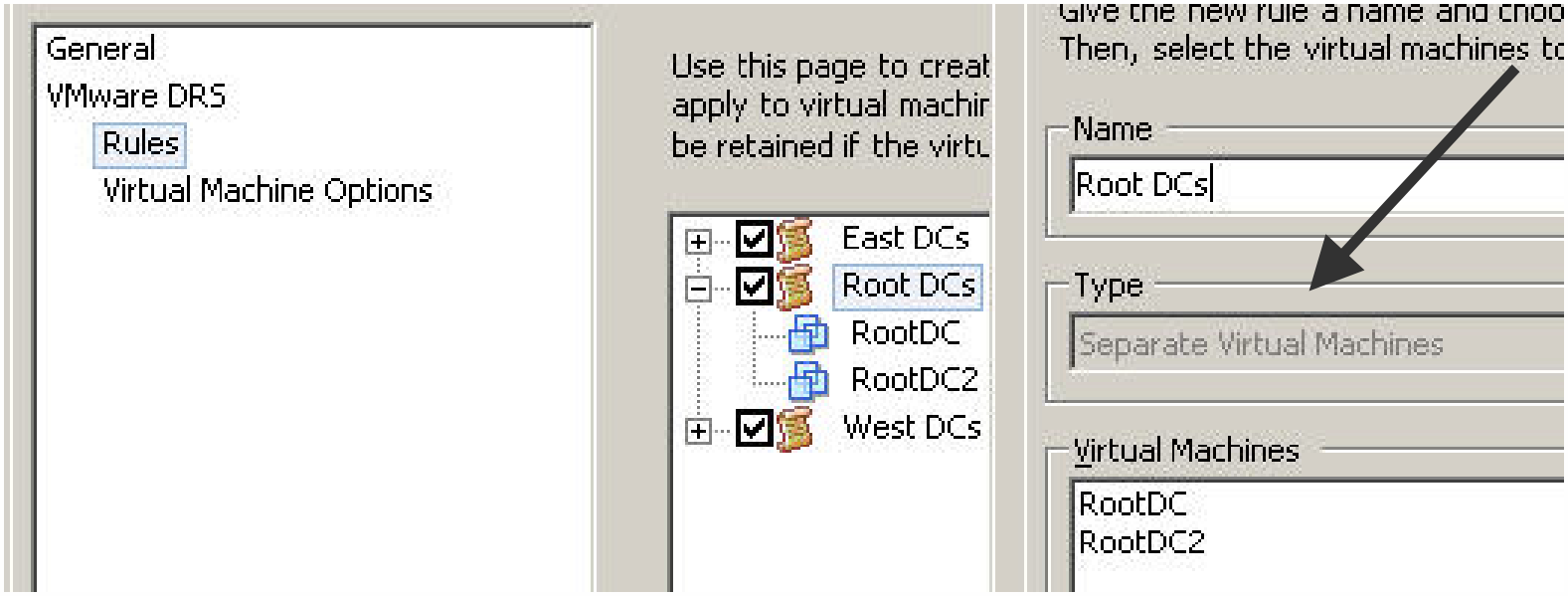
Disaster Preparedness – ESX 3.x/VirtualCenter 2.x

- VMware provides solutions for automatically restarting virtual machines
- Implement VMware HA as a high availability to ensure virtual machine domain controllers restart in the event an ESX server fails



Disaster Preparedness – ESX 3.x/VirtualCenter 2.x

- Combined with VMware DRS Anti-affinity rules can ensure domain controller VMs are segregated



Additional Information

- VMware Time Sync and Windows Time Service
  - VMware Knowledge Base ID# 1318
- Installing and Configuring NTP on VMware ESX Server
  - VMware Knowledge Base ID# 1339
- VMware Descheduled Time Accounting
  - http://www.vmware.com/pdf/vi3_esx_vmdesched.pdf
- How to detect and recover from a USN rollback in Windows Server 2003
  - http://support.microsoft.com/kb/875495
- How to detect and recover from a USN rollback in Windows 2000 Server
  - http://support.microsoft.com/kb/885875
- Support policy for Microsoft software running in non-Microsoft hardware virtualization software
  - http://support.microsoft.com/kb/897615
- How to configure an authoritative time server in Windows Server 2003
  - http://support.microsoft.com/kb/816042

Best Practices

- Avoid snapshots or REDOs for domain controller virtual machines
- Do not suspend domain controller virtual machines for long periods
- Consistent and regular system state backups still very important

Summary

- System State backups regularly
- Time Synchronization
- Disaster Recovery Plan
- High Availability
- Monitor Replication Traffic
- Modify DNS SRV records to redirect log on authentications to VMs
- Go back and constantly re-evaluate your strategy!!!

Thank you!!

VMWORLD 2006

Questions?