

vmworld 2013  
10TH ANNUAL

# DEFT CONVENTION

**VAPP5618**

**Virtualize Active Directory – The Right Way!**

**Deji Akomolafe, VMware**

**Alex Fontana, VMware**

# Agenda

- **Active Directory Overview**
- **Why virtualize Active Directory?**
- **Best Practices**
- **New Features**

# Active Directory Overview

---

- **This is not an Active Directory class**
- **Windows Active Directory Multi-master Replication Conundrum**
  - Write Originates from any Domain Controller
    - RODC is “special”
    - Schema Update is “special”
  - Selective Partnership
    - The Case for Optimal Replication Topology
  - Changes **MUST** Converge
    - Eventually
    - Preferably On-Time
- **The Additional Complexity of Multi-Domain Infrastructure**
  - The Infrastructure Master
  - The Global Catalog

# Active Directory Overview

---

## ■ How Do They Do That? – Overview of AD Replication

- The Directory Service Agent GUID
  - Unique to a Domain Controller
  - Persistent over the life of a Domain Controller
  - Used in USNs to track DC's originating updates
- The InvocationID
  - Used by DSA to identify a DC's instance of the AD database
  - Can change over time (e.g. during a DC restore operation)
- Update Sequence Number (USN), aka “Logical Clock”
  - Used by DCs to track updates sent or received
  - Increases per write transaction on each DC
  - Globally unique in Forest
- USN + InvocationID => Replicable Transactions

## ■ What about Timestamps?

- Conflict Resolution – Check the Stamps
  - Stamp = Version + Originating Time + Originating DSA

# Why Virtualize Active Directory?

# Why Virtualize AD?

Virtualization is main-stream

Active Directory virtualization is FULLY supported

Active Directory characteristics are virtualization-friendly

Domain Controllers are interchangeable

Why not to virtualize Active Directory?

**“Virtualize First” – the new normal**  
**No longer a “black magic”**

**All roles are suitable candidates**  
**Can’t spell “Cloud” w/o “Virtual”**

**Distributed, Multi-master**  
**Low I/O and resource requirements**

**OK, maybe not the RODC ☺**  
**Facilitates rapid provisioning**

**The fear of the “stolen vmdk”**  
**How about the “stolen server”?**  
**Privilege Escalation\***

# Best Practices

# Best Practices for Virtualizing Domain Controllers

## *Design for Resilience*

### The “low-hanging fruits”

Deploy across multiple datacenters  
Multiple geographical locations and AD Sites  
Distribute the FSMO roles  
Use **EFFECTIVE** Role-Based Access Control  
Enforce Well-Defined Administrative Practices

### Leverage VMware Availability Features

#### VMware HA

#### VMware DRS Rules

- Use Anti-affinity rules to keep DCs separated
- Use Host-Guest affinity rules to keep DCs on specific Hosts

#### vMotion

### What’s in a Name?

~ 75% of AD-related support calls attributable to DNS “issues”

**AD DEPENDS** on effective name resolution

- Clients and DCs reference objects by name/GUID
- Internal AD processes depend on DNS

**The “Repl Perform Initial Synchronizations = 0” Curse Word**

**DNS on DC or IPAM?**

- Physical IPAM complicates failover and recovery
- Avoid pointing DC to ONLY itself for DNS
- Distribute DNS servers across multiple sites
- Include loopback address in DNS list
- Include ALL Suffixes – or use GlobalNames



# Time Keeping

---

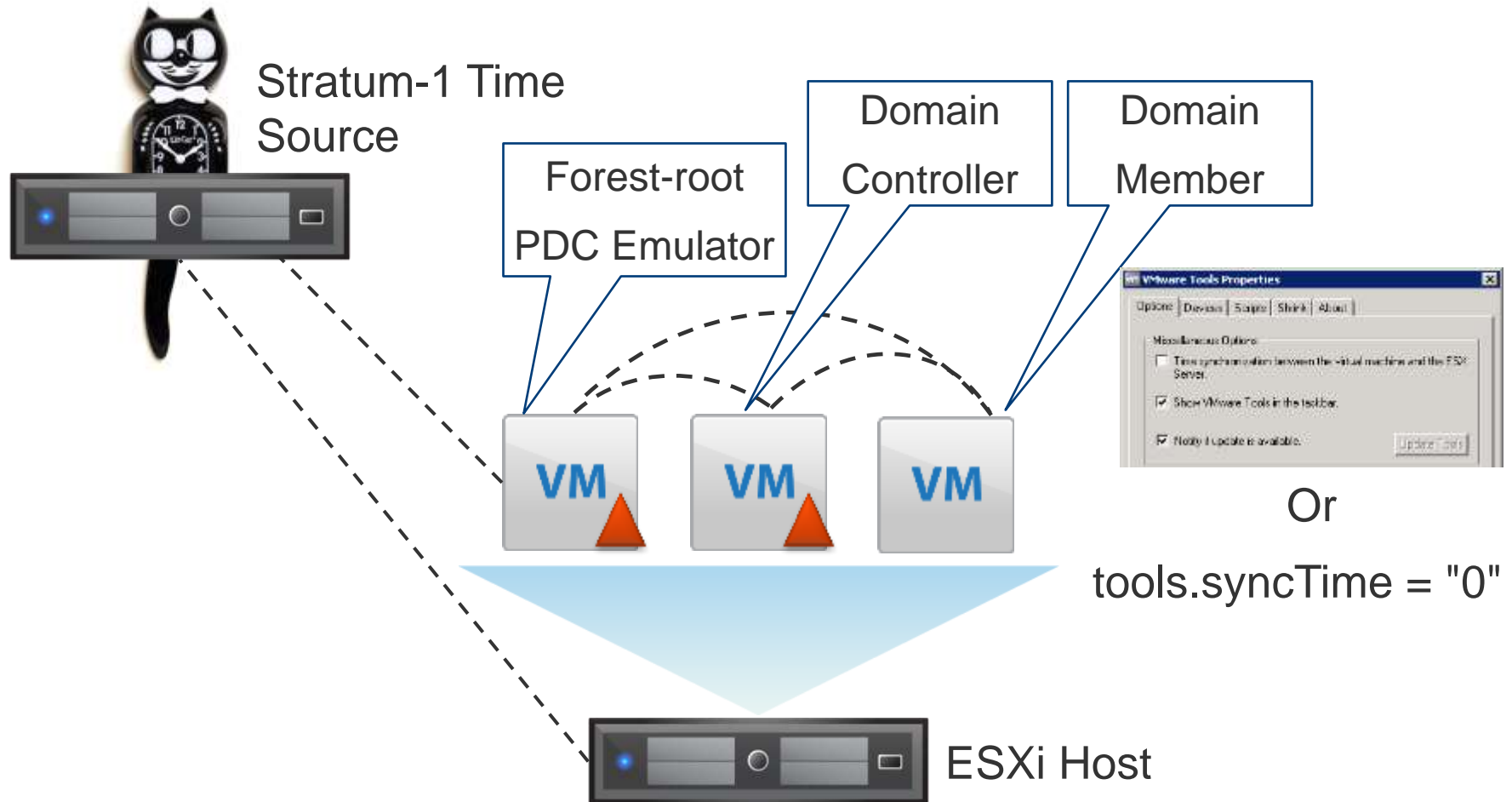
- **ACCURATE timekeeping is essential to AD**
  - Conflict resolution “tie breaker”
  - Kerberos authentication
  - W32Time is “good enough”
- **Operating Systems use timer interrupts (ticks) to track elapsed time**
  - Relies on CPU availability for accuracy
- **Tickless timekeeping avoids problem of CPU saturation**
  - Uses units of elapsed time since boot-up
  - Depends on fast, reliable “hardware counter”
- **Host resource over-allocation will lead to contention**
  - Guest may be idle and not schedule timer interrupts
  - Guest unable to schedule CPU time for interrupts
  - This leads to interrupt backlogs – and clock “drift”
  - Guest may over-compensate for “drift” by discarding backlogs – Ping-Pong!

# Time Keeping – The Proper Way

---

- **vSphere includes time-keeping mechanism**
- **VMware Tools is the delivery vehicle**
  - Resets Guest's clock to match Host's on boot-up
    - Even if Guest-Host clock synchronization is disabled
  - Reset Guest's clock when resuming from suspension or snapshot restore
    - This behavior can be disabled
- **Synch with Host or Use Windows domain time hierarchy?**
  - We have had a change of heart
    - Default guest time synchronization option changed in vSphere
    - Domain-joined Windows guests should use native time sync option
    - Domain Controllers should NOT be synced with vSphere hosts \*
    - Unless when running VMKernel-hosted NTP daemon in vSphere (ESXi)
    - vSphere hosts should NOT be synced with virtualized DCs
    - Follow Microsoft's time sync configuration best practices
- **VMware Tools STILL performs on-startup guest time correction \***

# Proper Time Keeping – For Visual Learners



<http://support.microsoft.com/kb/816042>

<http://kb.vmware.com/kb/1318>

<http://www.vmware.com/files/pdf/techpaper/Timekeeping-In-VirtualMachines.pdf>

# Historical Problems with Virtualizing Domain Controllers

---

- **Virtual Disk – To cache or not to cache?**
  - Not ~~our problem~~ a vSphere issue ☺
  - Force Unit Access – <http://support.microsoft.com/kb/888794/en-us>
  - Virtual Disk Corruption in Hyper-V – <http://support.microsoft.com/kb/2853952>
- **AD is a distributed directory service that relies on a clock-based replication scheme**
  - Each domain controller keeps track of its own transactions and the transactions of every other domain controller via Update Sequence Numbers and InvocationIDs
  - A domain controller which has been reverted to a previously taken snapshot, or restored from a VM level backup will attempt to reuse USNs for new transactions – USN Rollback
  - The local DC will believe its transactions are legit, while other domain controllers know they are not and refuse to allow incoming replication
- **The fix? VM GenerationID**

# VM Generation ID

---

- **Windows Server 2012 provides a way for hypervisor vendors to expose a 128-bit generation ID counter to the VM guest**
  - Generation ID is communicated from the hypervisor to the guest through the VM GenerationID Counter Driver (not VMware Tools)
- **VM GenerationID supported in vSphere 5.0 Update 2 and later**
  - Exposed in VMX file as *vm.genid*
  - Added to all VMs configured as Windows Server 2012
- **VM GenerationID is updated by the hypervisor**
  - VM clone, new VM from copied VMDK, snapshot revert, restore from VM-level backup, replicated VM (vSphere Replication or Array-based)
- **VM GenerationID tracked via new Active Directory attribute on domain controller objects – *msDS-GenerationId***
  - Attribute is not replicated to other domain controllers

# VM GenerationID Screenshots

The screenshot displays the VMware Workstation interface with the 'W12-DC1 Properties' dialog box open. The 'Attributes' tab is selected, showing a list of attributes for the virtual machine. The 'msDS-GenerationId' attribute is highlighted, showing a value of '100<000R'. The 'Operating System' tab is also visible, showing 'Microsoft Windows Server 2012 (64-bit)'. In the bottom left, a PuTTY terminal window shows the command 'vm.genid = "5963699947071140"' and 'vm.genidX = "-72060497887599"'. The 'Settings' tab on the right shows 'Disable acceleration' checked.

Guest Operating System

- ☒ Windows
- ☐ Linux
- ☐ Other

Version:

Microsoft Windows Server 2012 (64-bit)

W12-DC1 Properties

General	Operating System	Member Of	Delegation	Location
Managed By	Object	Security	Dial-in	Attribute Editor

Attributes:

Attribute	Value
localPolicyFlags	0
logonCount	1721
msDS-GenerationId	100<000R
msDS-SupportedEncr...	0x1C = ( RC4_HMAC_MD5   AES128_CTS_
name	W12-DC1
objectCategory	CN=Computer,CN=Schema,CN=Configuratio
objectClass	top; person; organizationalPerson; user; com
objectGUID	102908c1-22c0-4c49-9640-8ffa27e25482
objectSid	S-1-5-21-270845870-183488998-241929798
operatingSystem	Windows Server 2012 Datacenter
operatingSystemVersi...	6.2 (9200)
primaryGroupID	516 = ( GROUP_RID_CONTROLLERS )
pwdLastSet	8/5/2013 4:24:03 PM Pacific Daylight Time
replPropertyMetaData	AttID Ver Loc.USN Org.DSA

tsa-bl460-1.vmware.com - PuTTY

```
/vmfs/volumes/4d94102a-5a169  
vm.genid = "5963699947071140"  
vm.genidX = "-72060497887599"  
/vmfs/volumes/4d94102a-5a169
```

Settings

☒ Disable acceleration

Experimental features or as instructed by

- VM GenerationID allows for two new features: domain controller cloning and domain controller safeguard

# Domain Controller Cloning

---

- **DC Cloning allows fast, safe deployment of new domain controllers using hypervisor based cloning techniques**
  - Includes clone and copy VMDK
- **DC Cloning Sequence**
  - Source DC is prepared for cloning, this includes adding the DC to the cloneable domain controllers AD group, checking for non-cloneable software and creating the DCCloneConfig.xml
  - Source DC is shut down
  - Source DC VM is cloned using hypervisor based cloning operations
  - New DC is powered on and VM GenerationID is evaluated
  - New VM GenerationID triggers DC Safeguard – RID Pool discard, invocationID reset
  - New VM checks for existence of file DCCloneConfig.xml
  - If exists, the cloning process proceeds and new DC is promoted using the existing AD database and SYSVOL contents

# Domain Controller Cloning Example

vSphere Host

```
Administrator: Windows PowerShell

Windows PowerShell
Copyright (C) 2012 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> New-ADDCCloneConfigFile -Static -IPv4Address "192.168.11.42" -IPv4DNSResolver "192.168.11.40" -IPv4SubnetMask "255.255.255.0" -CloneComputerName "W2K12-DC03" -IPv4DefaultGateway "192.168.11.1"
Running in 'Local' mode.
Starting PDC test: Verifying that the domain controller hosting the PDC FSMO role is running Windows Server 2012 or later...
Passed: The domain controller hosting the PDC FSMO role (W2K12-DC01.id-lab.loc) was located and running Windows Server 2012 or later.

Verifying authorization: Checking if this domain controller is a member of the 'Cloneable Domain Controllers' group...
Located the local domain controller: (W2K12-DC02.id-lab.loc).
Querying the 'Cloneable Domain Controllers' group...
Pass: The local domain controller is a member of the 'Cloneable Domain Controllers' group.

Starting test: Validating the cloning allow list.
NOTE: C:\Windows\NTDS\CustomDCCloneAllowList.xml is being used as the defined inclusion list.
No excluded applications were detected.
Pass: No excluded applications were detected.

No valid clone configuration files were found at any of the supported locations.
All preliminary validation checks passed.

Starting creation of the clone configuration file...
Finding the path to the Directory Service database...
The clone configuration file was generated at:
C:\Windows\NTDS\DCCloneConfig.xml
Generating the clone configuration file content...
The clone configuration file has been created.

PS C:\Windows\system32> _
```



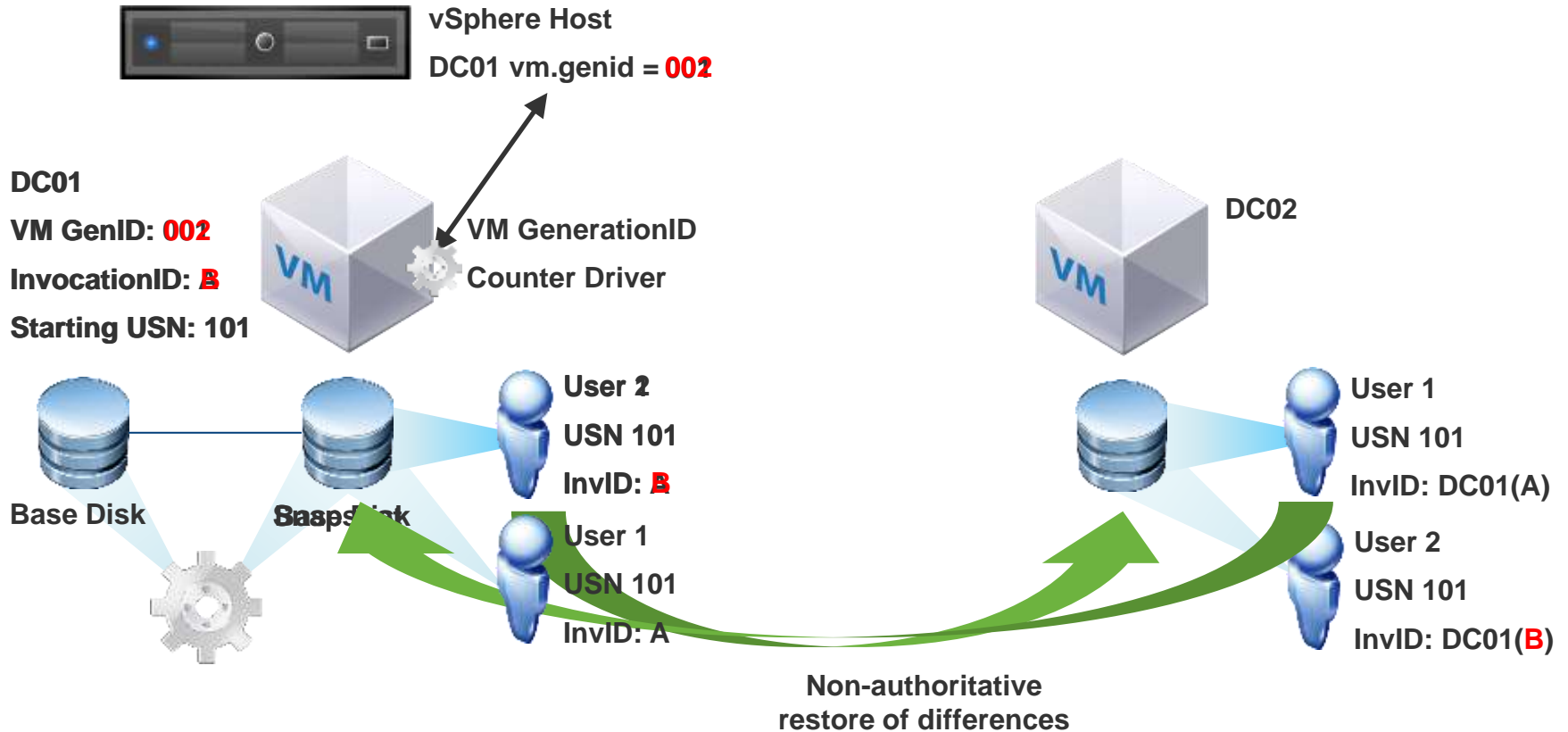
# Domain Controller Cloning Demo

# Domain Controller Safeguard

---

- **DC Safeguard allows a DC that has been reverted from a snapshot, or restored from VM backup to continue to function as a member of the directory service**
  - VM GenerationID is evaluated during boot sequence and before updates are committed to active directory
- **After revert/restore:**
  - Boot-up or new AD update triggers VM GenerationID to be compared to value of msDS-GenerationId in local AD database
  - If the values differ:
    - The local RID pool is invalidated
    - New invocationID is set for the local AD database
  - New changes can be committed to the database and synchronized outbound
  - Changes lost due to revert/restore and synchronized back inbound
- **After VM Clone or Copy (without proper prep)**
  - DC is rebooted into directory service restore mode (DSRM)

# DC Safeguard Example



# DC Safegaurd Demo

# Considerations When Using DC Safeguard Features

---

- **Minimum vSphere/vCenter/ESXi version: 5.0 Update 2**
- **Always shutdown source domain controller prior to cloning**
  - No Hot-clone! Besides, it's not supported.
- **If cloning or safeguard is not working as expected, make sure the guest operating system setting on the VM is set to Windows Server 2012**
- **Remember to validate all software (think management/backup agents) for cloning**
- **Leave Cloneable Domain Controllers group empty in between clone operations**
- **If using Windows Backup make sure to delete the history on the clone, and take a fresh backup ASAP**

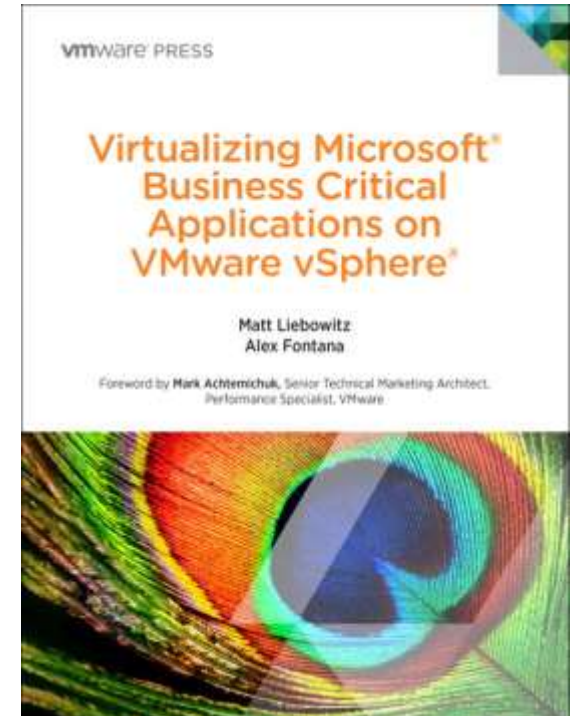
## Key Take Aways...

---

- Dangers which were once present when virtualizing DCs have mostly been resolved in Windows Server 2012
- Domain Controller virtualization is 100% supported
- The Multi-master, distributed, and low resource utilization characteristics of Active Directory make domain controllers virtualization-friendly
- Most of the best practices for virtualizing Active Directory, are not specific to VMware or virtualization at all, i.e. DNS, time keeping, etc.
- Active Directory is natively highly available, combine with vSphere High Availability to mitigate hardware failures
- Upgrade to Windows Server 2012 to bring domain controller safeguard and cloning to the party.

# Shameless Plug

- **New book available for VMworld 2013**
- **Topics include:**
  - Virtualizing business critical apps
  - Active Directory
  - Windows Failover Clustering
  - Exchange 2013
  - SQL 2012
  - SharePoint 2013
- **Available on-site at the VMworld Book Store**
- **Available online at Amazon and Pearson ([pearsonitcertification.com](http://pearsonitcertification.com))**
- **Book signing Wednesday 12:30-1:30pm**



# Q&A



vmworld 2013  
10<sup>TH</sup> ANNUAL

**THANK YOU**

**DEFY**  
**CONVENTION**

vmware®

vmworld 2013  
10TH ANNUAL

# FILL OUT A SURVEY

Every Completed Survey Is Entered Into  
a Drawing for a \$25 VMware  
Company Store Gift Certificate

vmware

DEFY  
CONVENTION



vmworld 2013  
10TH ANNUAL

# DEFT CONVENTION

**VAPP5618**

**Virtualize Active Directory – The Right Way!**

**Deji Akomolafe, VMware**

**Alex Fontana, VMware**