



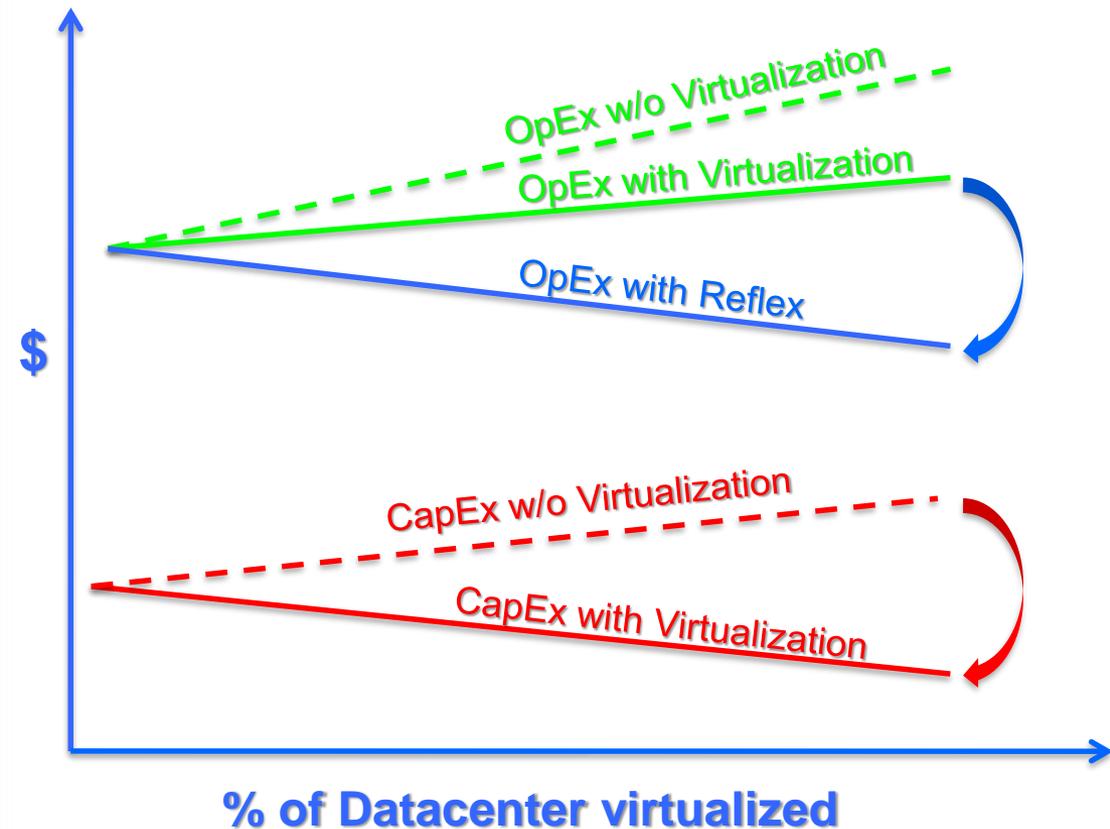
Management & Security For Virtualization & Cloud Infrastructures



Reflex History

- ❑ 2000 – Reflex Security Founded to focus on network security
- ❑ 2001 – First Intrusion Prevention System (IPS) shipped
- ❑ 2006 – First virtualization product released (Virtual Security Appliance)
- ❑ February 2008 – Decision to focus exclusively on virtualization & Cloud
- ❑ **April 2008 – Seed investment in the new virtualization business – Complete restart of and restructuring of the company – Reflex Systems LLC**
- ❑ April 2008 – New CEO, Pete Privateer starts
- ❑ August 2008 – First release of Reflex's Virtualization Management Center (VMC)
- ❑ September 2008 – Reflex's VMC wins best virtualization security & best of show at VM World
- ❑ December 2008 – Reflex Systems achieves first \$1M in sales
- ❑ **March 31, 2009 – Reflex Systems LLC closes \$8.5M Series A funding round**
- ❑ **Today – Over 80 customers and Growing!**

Virtualization Benefits & Challenges



Examples:

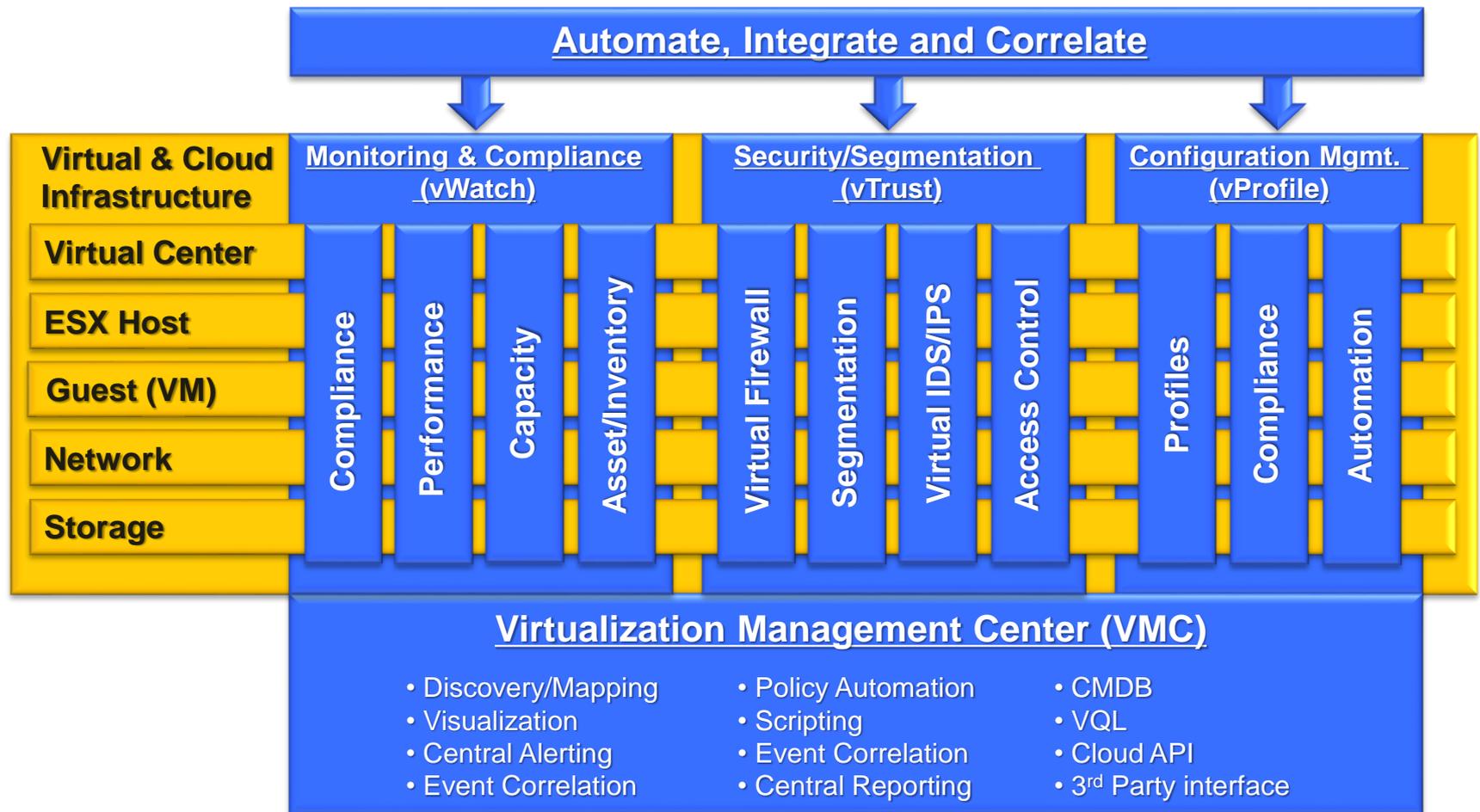
Citi: Virtual Infrastructure Management
Reflex will Save 30 FTE/Year with vProfile alone

E*Trade: Virtual Infrastructure Management
daily trouble shooting:
1 FTE to manage every 20 physical Servers
1 FTE to manage ever 50-100 virtual servers
Using Reflex: 1 FTE can manage 2-500 virtual Servers

Medquist, Regions Bank, Bank of Canada:
Certified "compensating control" to meet Compliance and audit guidelines

Schwans, Saavis, Cisco & Infor:
Virtual security, segmentation, and monitoring
Simplifies and reduces networking costs and
Enables rapid trouble shooting and performance Tuning.

Reflex Virtual/Cloud Infrastructure Management & Security Platform

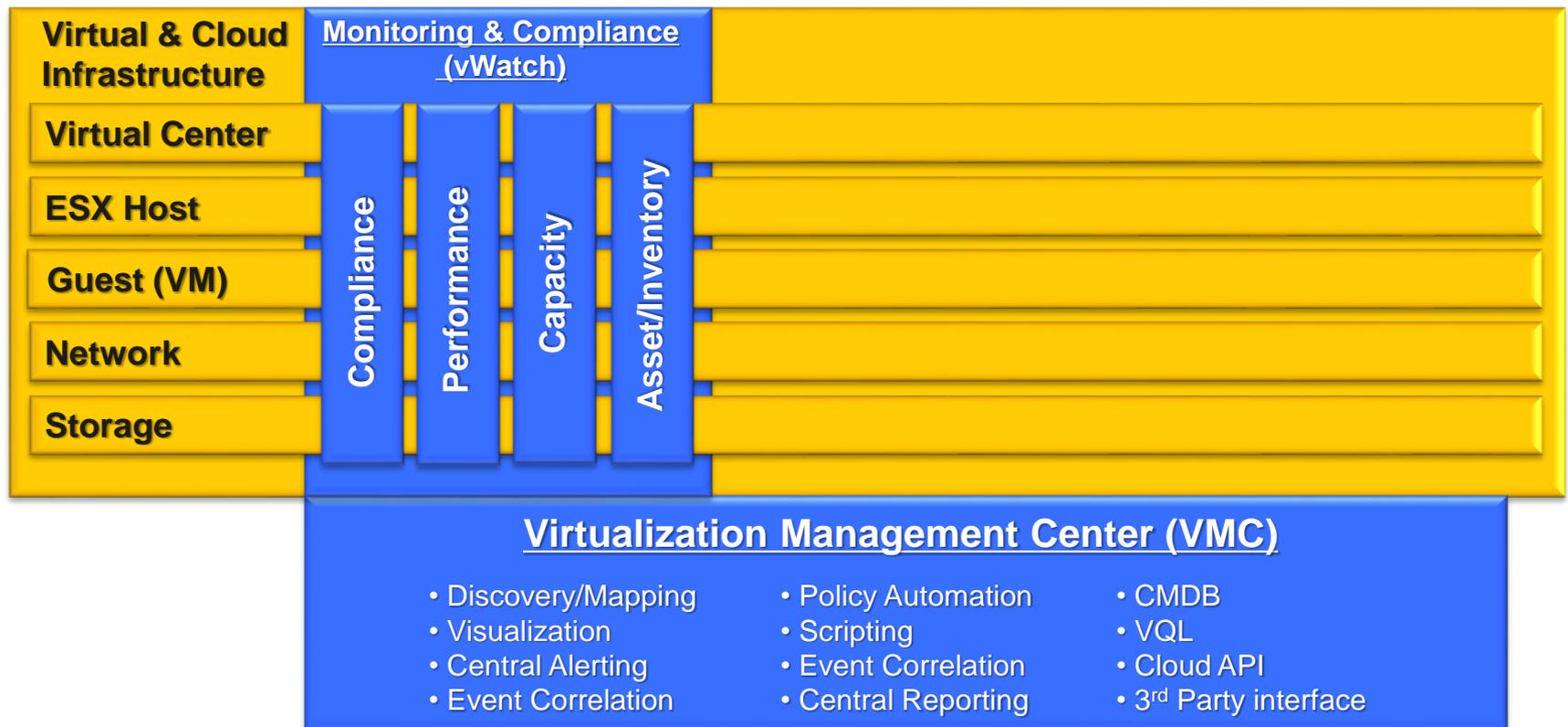


Virtualization Management & Security

The screenshot displays the Reflex Virtualization Management Center interface, which is divided into several functional areas:

- Track Changes:** A table showing configuration changes with columns for Name, Change, New Value, User, and Revis. Callout: "Change Control & Configuration Monitoring".
- Virtual Security (FW/IDS/IPS):** A section for security alerts, showing event types like "Microsoft DNS WPAD Sp" and "ACK Scan". Callout: "Virtual Security (FW/IDS/IPS)".
- VM Performance:** A 3D area chart showing "Memory Usage (Average)" over time from Tuesday to Saturday. Callout: "CPU, Memory, Network, & Storage Performance".
- Virtual Infrastructure Discovery and Mapping:** A central network diagram showing "VM Network VMs (2)", "ProdNet VMs", and "172.16.2.100 Networks". Callout: "Virtual Infrastructure Discovery and Mapping".
- Auditing & Compliance:** A timeline view showing events from August 3rd to August 16th, 2009. Callout: "Auditing & Compliance".
- Software Asset Management:** A list of installed applications and their versions, including VMware Tools, vCenter Server, and various Windows updates. Callout: "Software Asset Management".
- All Alarms:** A table at the bottom listing alarms such as "Host Has changed", "Virtual Switch Has changed", and "Virtual Machine Memory Usage".

Monitoring & Compliance - vWatch



Topology Mapping

The screenshot displays the Reflex Virtualization Management Center interface. The main window shows a network topology map for 'esx-9.demo.reflex'. The map includes components like 'vSphere', 'vSwitch0', 'vSwitch0', 'vmnic0', 'vmnic1', 'vTrust-esx-9.demo.reflex', 'vmervice-vswitch', and 'data1 VMs' (Datastore, NagProduct, Porter). A third-party vSwitch 'n1 kv-1:vmnic1' is connected to 'n1 kv-1'. A callout points to this vSwitch with the text 'Third Party vSwitch'. Another callout points to the 'vTrust-esx-9.demo.reflex' component with the text 'VMs connected to the vSwitch and secured by Reflex vTrust'. On the right, an information panel for 'n1 kv-1' is shown, including details like Name, Parent, Distributed, Type, Version, and Tags. Below this, a 'Performance Data' section shows graphs for CPU (0.26%), Memory (34.99%), Disk (2 KB/s), and Network (0 KB/s). A callout points to this panel with the text 'Info panel shows the performance of the Object'. The interface also shows a timeline at the bottom and a status bar with the user 'mike@vmc-1.demo.reflex'.

Information

- Name: n1 kv-1
- Parent: DC1
- Distributed: Yes
- Type: Cisco Nexus 1000V
- Version: Cisco Nexus 1000V
- Tags:

Contains

- Unused_Or_Quarantine_Uplink
- Unused_Or_Quarantine_Veth
- system-uplink
- vm-uplink
- data1

Performance Data

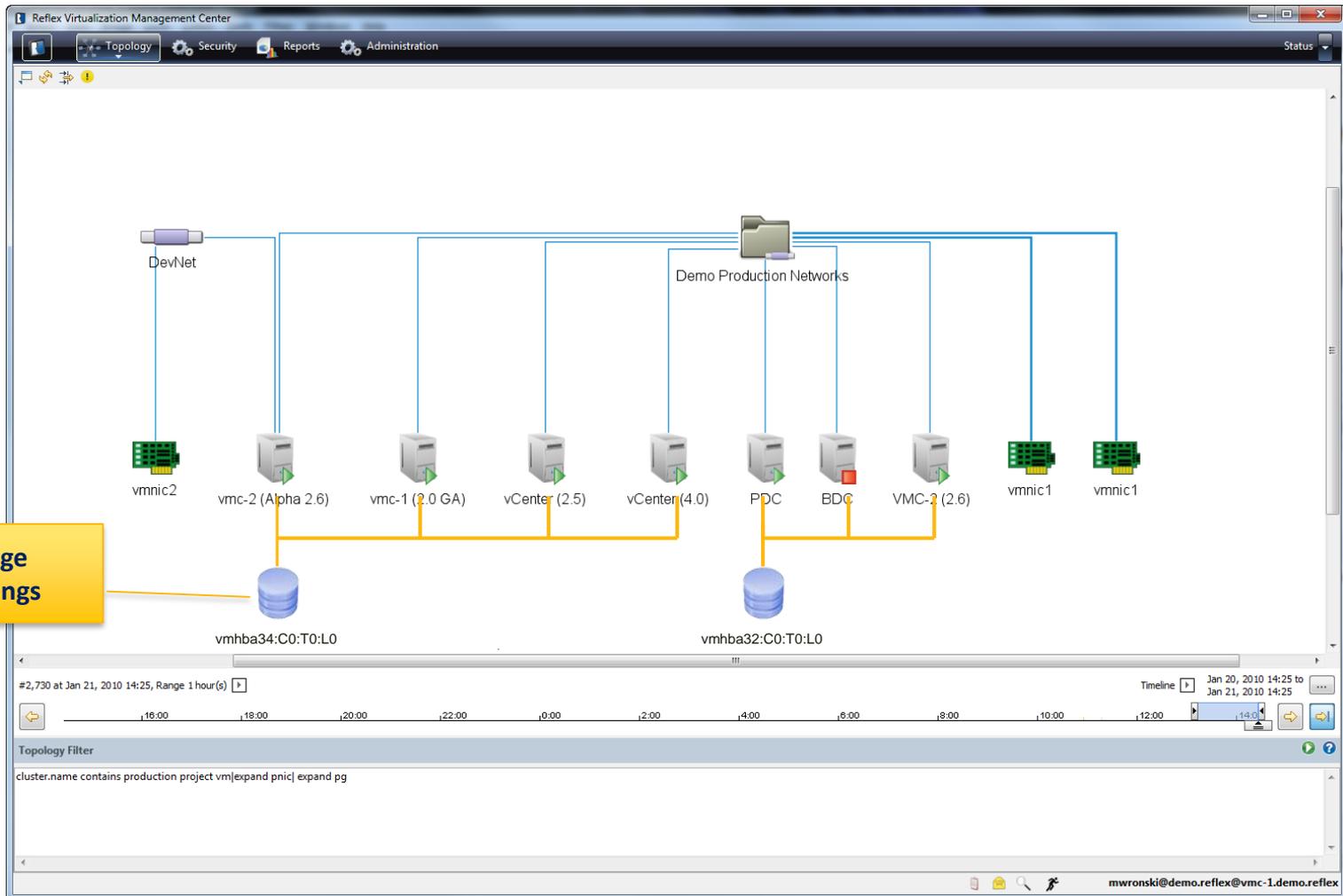
- CPU: 0.26 %
- Memory: 34.99 %
- Disk: 2 KB/s
- Network: 0 KB/s

Third Party vSwitch

VMs connected to the vSwitch and secured by Reflex vTrust

Info panel shows the performance of the Object

Storage : Visibility



Visibility, Correlation & Troubleshooting

What, Where, When, Why something went wrong
Assign to users for resolution

Topology Alarms					
Object	Name	Current	Highest	Last Updated	Closed
cable.reflex	Virtual Machine Memory Usage	✓	⚠	2009-02-19 14:59:28	2009-02-19 14:59:28
cable.reflex	Virtual Machine CPU Usage	✓	⚠	2009-02-19 14:52:28	2009-02-19 14:52:28
cable.reflex	Virtual Machine CPU Usage	✓	✗	2009-02-19 14:31:28	2009-02-19 14:31:28

Transitions

2009-02-19 14:28:28 ✓ to ✗
 2009-02-19 14:31:28 ✗ to ✓

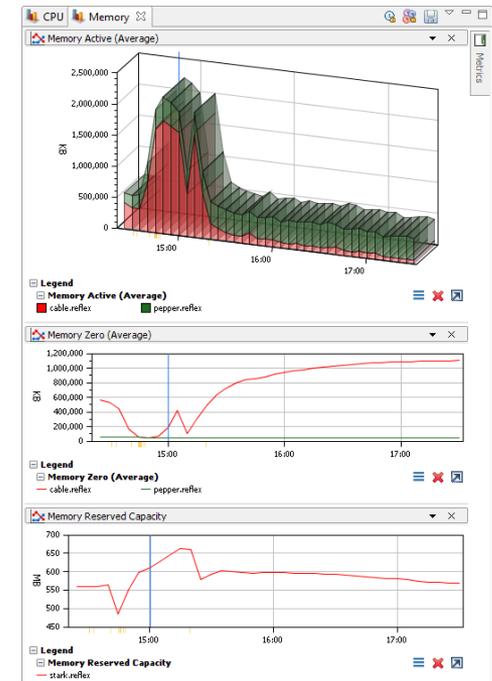
Definition

Yellow when virtual machine CPU Usage (Average) is above 75% and Red when virtual machine CPU Usage (Average) is above 90%.

See what changed and who changed it

Track Changes						
Name	Change Type	Property	Old Value	New Value	User	Modification time
VMS						
Datacenter1						
stark.reflex						
cable.reflex						
Network Adapter 1	Modified	Guest VNIC Network Name	VM Network	VM Network Secured	Administrator	2009-02-19 14:48:18

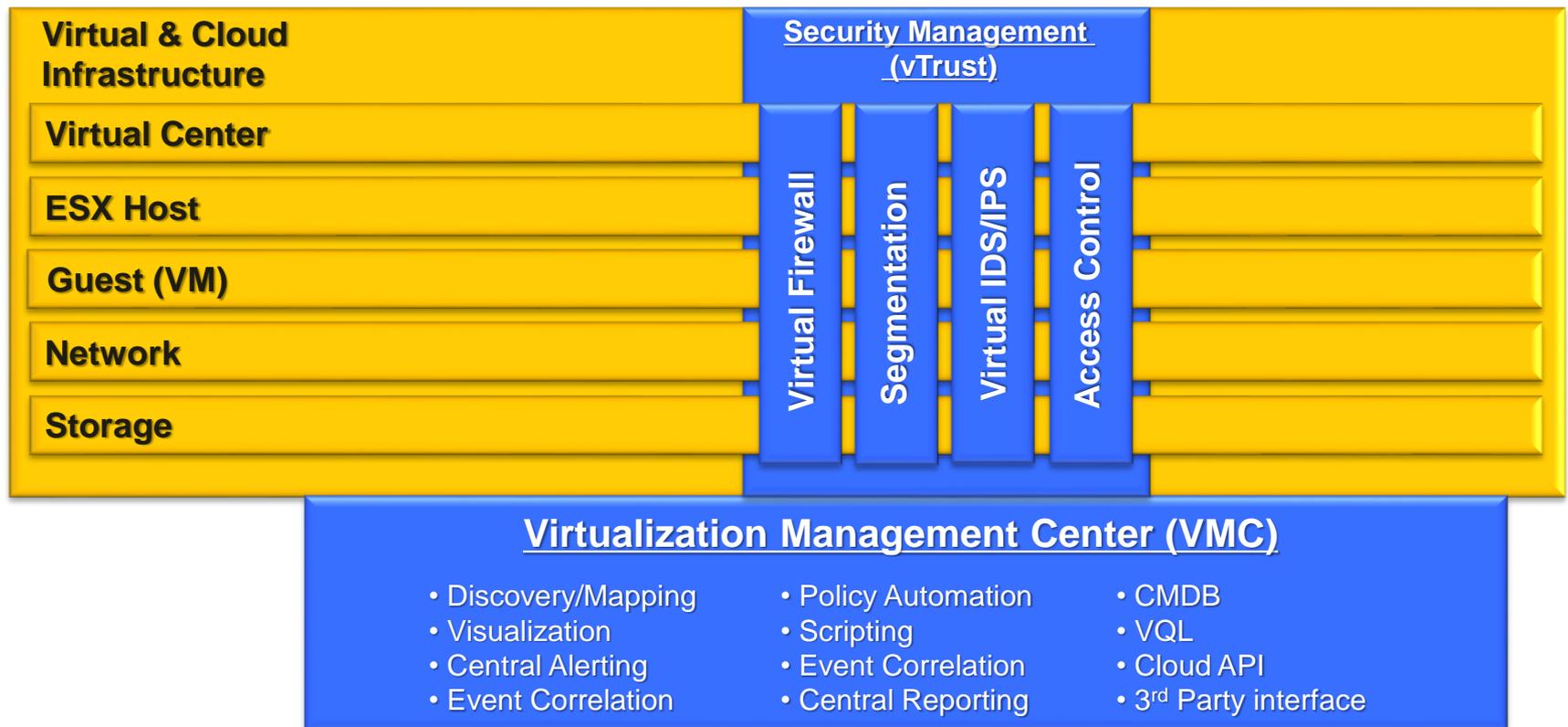
See what affect changes had on other systems historically



Over 150 Performance Metrics



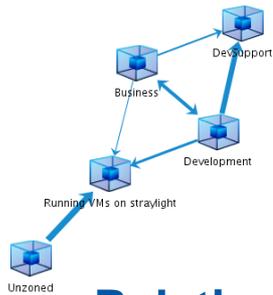
Security Management - vTrust



Segment The Virtual Infrastructure

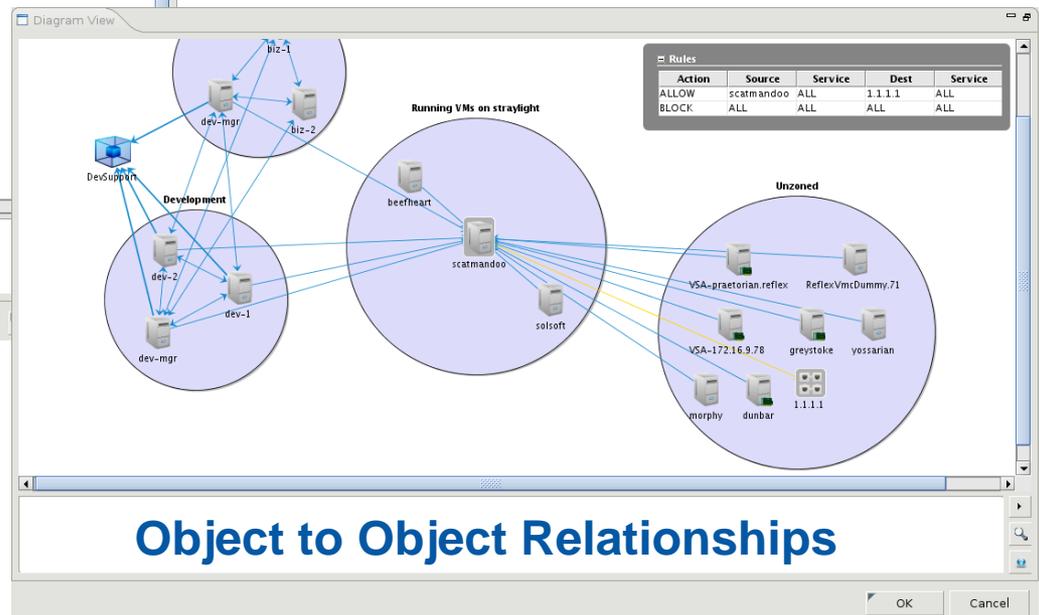
Dynamically partition the virtual infrastructure using software, not hardware

Zone to Zone Relationships



Create Trust Zones or groups of virtual objects with different network communication policies.

Object to Object Relationships



Next Generation Virtual Firewall

The screenshot displays the ACL Management interface, which is divided into several sections:

- Zones:** A list of zones including All, CRM, DMZ, ERP, Internal, and Internet.
- Policies:** A list of policies including WebApplication.
- Services:** A list of services including Default Header, WebApplication, DMZ Policy, and Default Footer.
- Zones (bottom):** A list of zones including CRM, ERP, and Internet.
- WebApplication rules:** A table of rules with columns for Action, Source, Destination, Source services, Dest services, and Log. The table is currently empty.
- Diagram View:** A network diagram showing three zones: CRM, ERP, and Internet. The Internet zone is connected to the CRM and ERP zones. The CRM zone contains a SharedDB, AppSvr1, WebSvr1, and AppSvr4. The ERP zone contains a WebSvr2, AppSvr2, AppSvr3, and SharedDB.

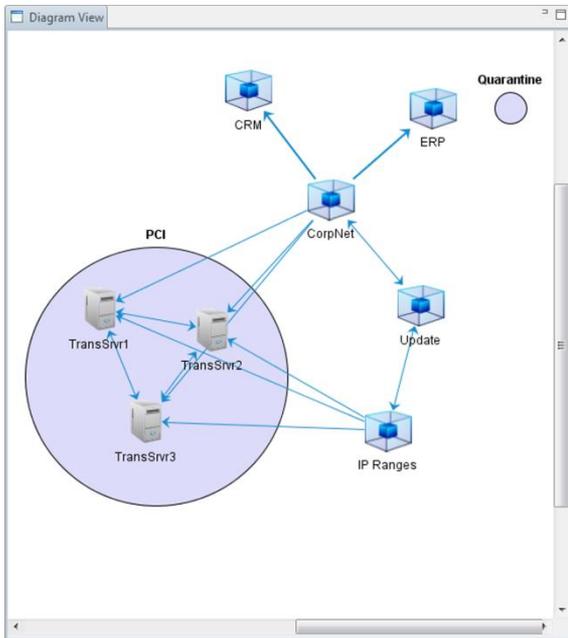
Action	Source	Destination	Source services	Dest services	Log
	zone:Internet	tag:web	ALL	web	
	tag:web	tag:app	ALL	web	
	tag:app	tag:db	ALL	Oracle	

Filter Diagram

OK Cancel

Automating Security Compliance

PCI Zone - Credit Cards Transaction Servers



Email alarm with detail Information about the PCI violation

Alert: Unencrypted traffic on PCI Network

ReflexVMC@reflexsystems.com

Sent: Wed 8/26/2009 3:48 PM

To: Hezi Moore

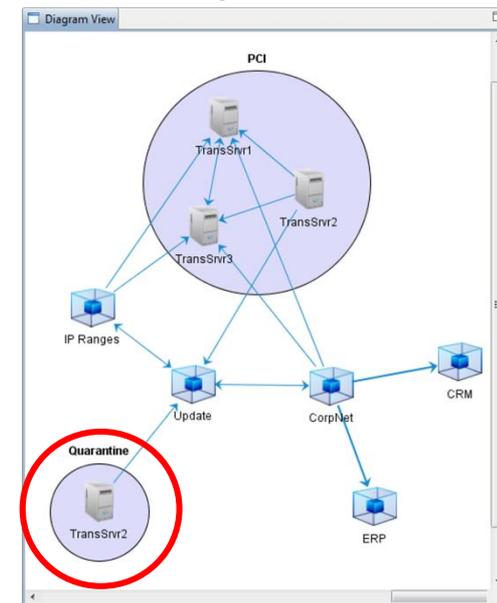
The following guests have violated PCI DSS Requirement 2.3

[PCI-DSS] 2.3 Encrypt all non-console administrative access administrative access.

* Guest TransSrvr2 on host esx-6.demo.reflex.

** Guests have been quarantined.

Quarantine the PCI Server that violated compliance



PCI Violation Alarm DSS 2.3 unencrypted HTTP communication

Object	Name	Current	Highest	Assigned to	Last Updated	Closed	Transitions
TransSrvr2	PCI Violation	●	⊗		2009-08-26 16:30:29	2009-08-26 16:30:29	2009-08-26 15:17:27 ? to ⊗
TransSrvr2	PCI Violation	●	⊗		2009-08-26 16:30:29	2009-08-26 16:30:29	2009-08-26 16:30:29 ⊗ to ●
TransSrvr2	PCI Violation	●	⊗		2009-08-26 16:30:29	2009-08-26 16:30:29	

Definition
Violation of DSS 2.3: Guest TransSrvr2 on esx-6.demo.reflex is communicating unencrypted HTTP.

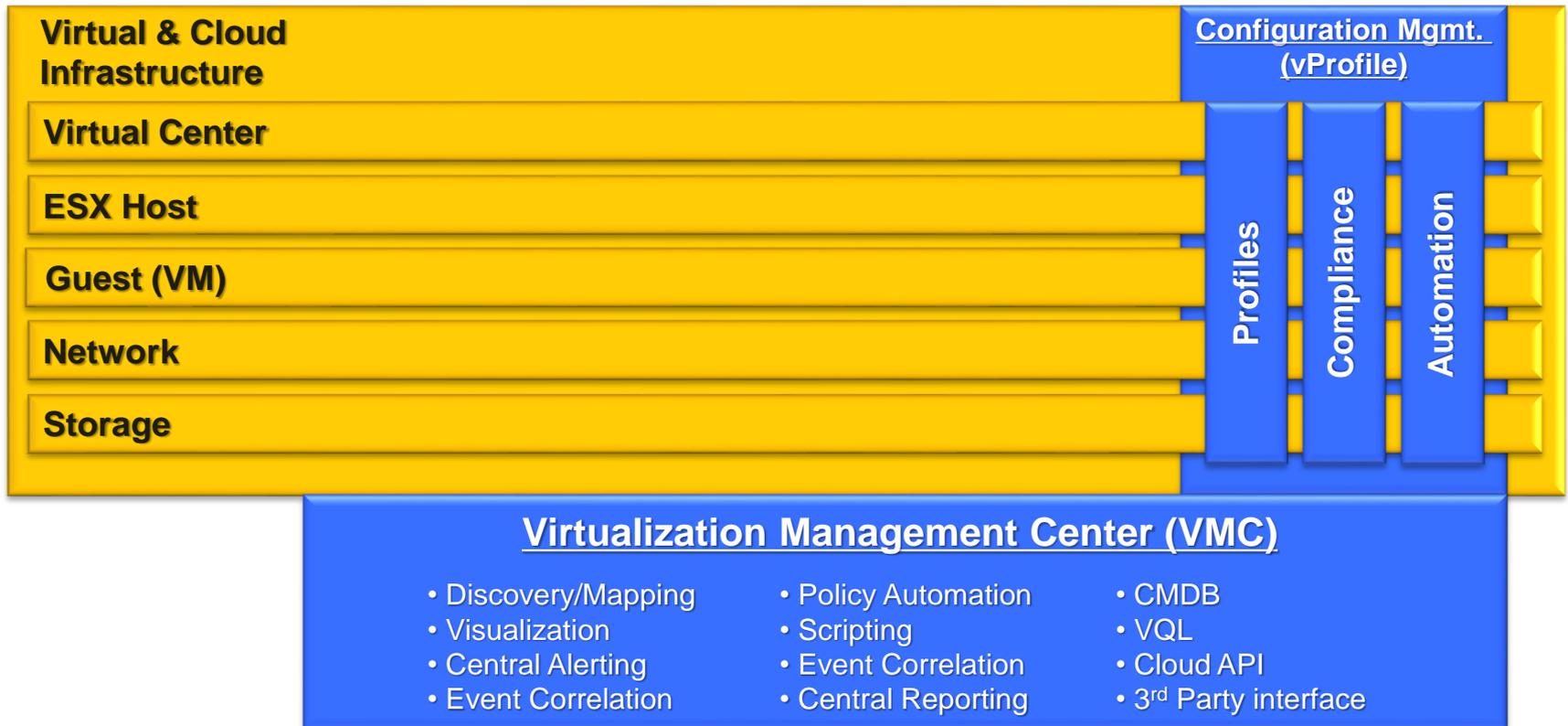
Extending Firewall to Storage

The screenshot displays the vTrust Workspace interface. On the left, there are panels for 'Zones' (listing All, Applications, CRM, DMZ, ERP, PCI, Production, Quarantine, sas70) and 'Policies' (listing PCI, DMZ, VDI). The main area shows a table of firewall rules and a 'Diagram View'.

Action	Source	Destination	Comment
Permit	vm.tags contains DB	vDisk_Share3:LUN2	
Permit	vm.tags contains WEB	vDisk_Share3:LUN4	
ALERT			email: operator@domain.com
SCRIPT			//reflex/scripts/QuarantineVM1

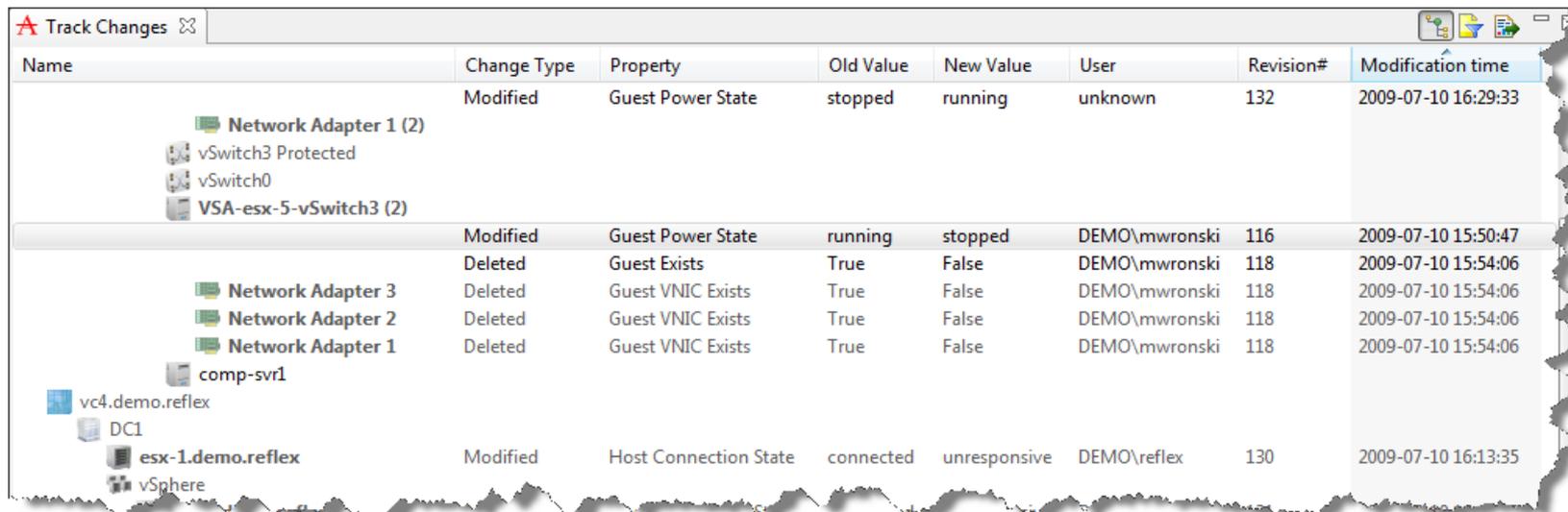
The 'Diagram View' illustrates a network topology with three main zones: vDisk_Share3, PCI, and DMZ. vDisk_Share3 contains four LUNs (LUN1, LUN2, LUN3, LUN4). PCI contains four servers: DbSrvr1_LV, DbSrvr2_LV, WebSrvr1, and WebSrvr2. DMZ contains a WebStore server. vDisk_Share4 contains three storage units. Below the zones, there are icons for Applications, Quarantine, Production, sas70, CRM, ERP, and All. At the bottom, there are 'Apply Filter' and 'Filter as I type' options, and 'Save' and 'Cancel' buttons.

Configuration Management - vProfile



Configuration Change Management

Track every change, at any point in time
Throughout the entire infrastructure



Name	Change Type	Property	Old Value	New Value	User	Revision#	Modification time
Network Adapter 1 (2) vSwitch3 Protected vSwitch0 VSA-esx-5-vSwitch3 (2)	Modified	Guest Power State	stopped	running	unknown	132	2009-07-10 16:29:33
	Modified	Guest Power State	running	stopped	DEMO\mwronski	116	2009-07-10 15:50:47
Network Adapter 3	Deleted	Guest Exists	True	False	DEMO\mwronski	118	2009-07-10 15:54:06
Network Adapter 2	Deleted	Guest VNIC Exists	True	False	DEMO\mwronski	118	2009-07-10 15:54:06
Network Adapter 1	Deleted	Guest VNIC Exists	True	False	DEMO\mwronski	118	2009-07-10 15:54:06
comp-svr1 vc4.demo.reflex DC1 esx-1.demo.reflex vSphere	Modified	Host Connection State	connected	unresponsive	DEMO\reflex	130	2009-07-10 16:13:35

Timeline-based monitoring to visualize the past



Host Configuration Visualization

- Visualize Differences
- Analytical Heat Map
- Ad-Hoc Remediation
- Multiple Profiles per Host
- Compare Hosts or Profiles
- Exclusion Masks

The screenshot displays the Reflex Virtualization Management Center interface. The main window is titled "Host Configuration" and shows a comparison of two hosts: "vmaster3.reflex" and "angelina.reflex". The interface includes a sidebar with navigation options for VMS, Host, Guest, and Migrations. The main area features a heat map visualization of configuration differences, with a tooltip showing the property "host.net_dns_search" and its values for both hosts. Below the heat map is a table for filtering fields and a field list.

Host Configuration

Properties Filter: [Host->net_dns_servers.172.16.8.1]

Compare: Cluster VC-Master

Exclusion Masks:

- Data Storage
- Read-Only
- Hardware
- Host Advanced
- Host Primary
- Host Specific

Property: host.net_dns_search

Differences:

- vmaster3.reflex: reflex, reflexsystems.com
- angelina.reflex: reflex

Common Value: reflex, reflexsecurity.com

Drop Data Fields Here	host.net_dns_servers.172.17.0.18	prnc.vitrnic1.duplex
host.ntp_servers	Not set	FULL
ntp.reflex	1	2

Field List (Drag Items to the Pivot Grid):

- datastore.NetApp Software Repository.remote_host
- host.fw_enabled_services
- host.fw_enabled_services.Automated Availability Manager
- host.fw_enabled_services.CDM SLP
- host.fw_enabled_services.CDM Secure Server
- host.fw_enabled_services.CDM Server
- host.fw_enabled_services.NTP Client
- host.fw_enabled_services.SSH Server

Buttons: Add To, Row Area, Export to Excel

Host Configuration : Remediation

Reflex Virtualization Management Center - 2 day(s) until expiration

Topology Security Reports Configuration Management Administration Status

Host Configuration

Host Properties Filter

VQL: `cluster.name = VDI23`

Profiles:

- Profile_Global
- Profile_US
- Profile_EULA

Apply Filter

Compare all hosts in the cluster named VDI23

Baseline(s) to compare against

Visual "Heat Map" of differences between hosts and baselines. Where spots are "hot" there are differences. The hotter the areas, the greater the differences are.

Areas where the hosts/profiles/baselines differ. Every cell is a unique property on a host

User clicked hot spot showing view of property name and common/differing values on hosts

Quick Property name filter

This is a Pivot Table to compare/contrast properties from hosts/profiles(baselines)

Drop Filter Fields Here

Drop Data Fields Here

Property	host.advanced_properties.NFS.MaxVolumes	Differences
angelina.reflex	4	
diablo.reflex	16	
testify.reflex	2	
Common Value	8	

NFS.MaxVolumes per row

By Host Version in the columns

host.advanced_properties.NFS.MaxVolumes	host.version	host.advanced_properties.NFS.HeartbeatTimeout
5	VMware ESX 4.0.0 build-164009	VMware ESX Server 3.5.0 build-110181
8	5	1

Over 1500 Host properties to compare against. DragNDrop into Pivot Table

Field List (Drag Items to the Pivot Grid):

- host.advanced_properties.NFS.DiskFileLockUpdateFreq
- host.advanced_properties.NFS.DiskFileLockUpdateDelta
- host.advanced_properties.NFS.HeartbeatFrequency
- host.advanced_properties.NFS.HeartbeatMaxFailures
- host.advanced_properties.NFS.IndirectSend
- host.advanced_properties.NFS.LockDisable
- host.advanced_properties.NFS.LockRenewMaxFailureNumber
- host.advanced_properties.NFS.LockUpdateTimeout
- host.advanced_properties.NFS.ReceiveBufferSize
- host.advanced_properties.NFS.SendBufferSize
- host.advanced_properties.NFS.SyncRetries
- host.advanced_properties.NFS.UDPRetransmitDelay
- host.advanced_properties.NFS.VolumeRemountFrequency

Add To Row Area

Show only differences

isergeev@172.16.8.150

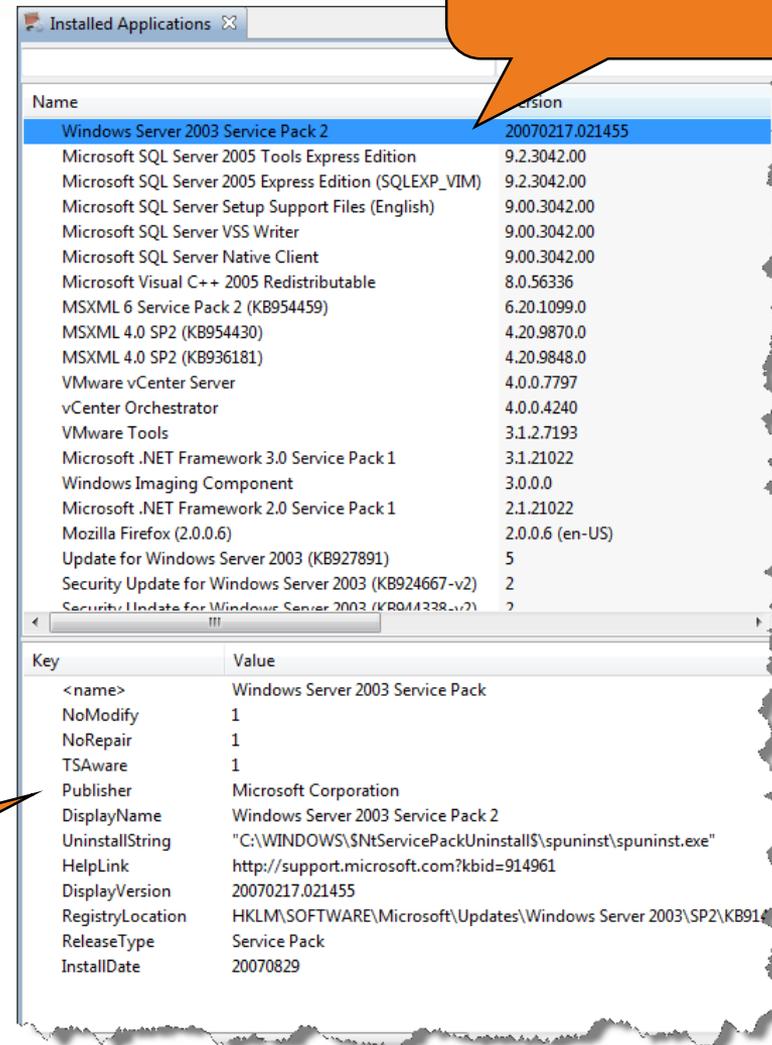
Software Asset Management

List of software assets on a VM

Track and monitor installed applications on VMs

- No Agents to Install
- Independent of Power State
- Policy Criteria
 - NAC
 - Posture Checking
 - Maintain Compliance

Software asset details (version, install date, etc.)



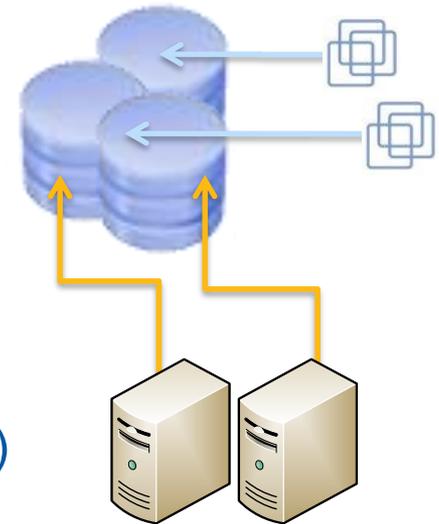
The screenshot shows the 'Installed Applications' window in Windows. The top part is a list of applications with columns for Name and Version. The bottom part is a 'Key-Value' table providing details for the selected application, 'Windows Server 2003 Service Pack 2'.

Name	Version
Windows Server 2003 Service Pack 2	20070217.021455
Microsoft SQL Server 2005 Tools Express Edition	9.2.3042.00
Microsoft SQL Server 2005 Express Edition (SQLEXP_VIM)	9.2.3042.00
Microsoft SQL Server Setup Support Files (English)	9.00.3042.00
Microsoft SQL Server VSS Writer	9.00.3042.00
Microsoft SQL Server Native Client	9.00.3042.00
Microsoft Visual C++ 2005 Redistributable	8.0.56336
MSXML 6 Service Pack 2 (KB954459)	6.20.1099.0
MSXML 4.0 SP2 (KB954430)	4.20.9870.0
MSXML 4.0 SP2 (KB936181)	4.20.9848.0
VMware vCenter Server	4.0.0.7797
vCenter Orchestrator	4.0.0.4240
VMware Tools	3.1.2.7193
Microsoft .NET Framework 3.0 Service Pack 1	3.1.21022
Windows Imaging Component	3.0.0.0
Microsoft .NET Framework 2.0 Service Pack 1	2.1.21022
Mozilla Firefox (2.0.0.6)	2.0.0.6 (en-US)
Update for Windows Server 2003 (KB927891)	5
Security Update for Windows Server 2003 (KB924667-v2)	2
Security Update for Windows Server 2003 (KB914338-v2)	2

Key	Value
<name>	Windows Server 2003 Service Pack
NoModify	1
NoRepair	1
TSAware	1
Publisher	Microsoft Corporation
DisplayName	Windows Server 2003 Service Pack 2
UninstallString	"C:\WINDOWS\SNTServicePackUninstall\spuninst\spuninst.exe"
HelpLink	http://support.microsoft.com?kbid=914961
DisplayVersion	20070217.021455
RegistryLocation	HKLM\SOFTWARE\Microsoft\Updates\Windows Server 2003\SP2\KB914338-v2
ReleaseType	Service Pack
InstallDate	20070829

Storage : Tracking and Policy

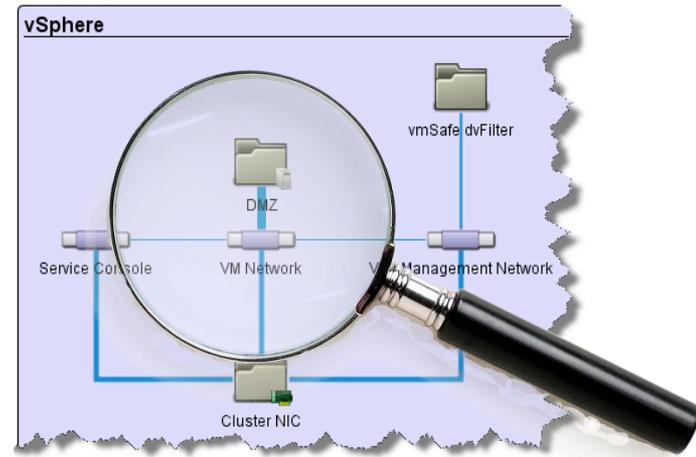
- Comprehend all storage relationships
 - LUN to VM
 - HBA to VM
 - VMFS to VM
 - Snapshots
 - VM OS Partitions
 - VMFS Disk Utilization (Reserved Space)
 - VM OS Partition Disk Utilization (Actual Utilization)
- Use Cases
 - Security and Infrastructure Policy
 - Asset Classification
 - VQL Queries
 - Show all VMs with multiple OS partitions
 - Show all VMs on a particular datastore
 - Show all VM's with OS partitions at over 80% capacity
 - Show all LUNS at over 80% capacity
 - Show all VM's linked to a specific VMFS file



Reflex VMC: VQooL

Virtualization Query Language

- Patent Pending
- Natural Search (Google)
- Structured Search (SQL)
- Zone Definition
- Policy Binding
- Data Classification



Screenshot of the VQL interface showing a query and its results.

Query Editor
pg.promisc = true project vm without vm.vsa = true

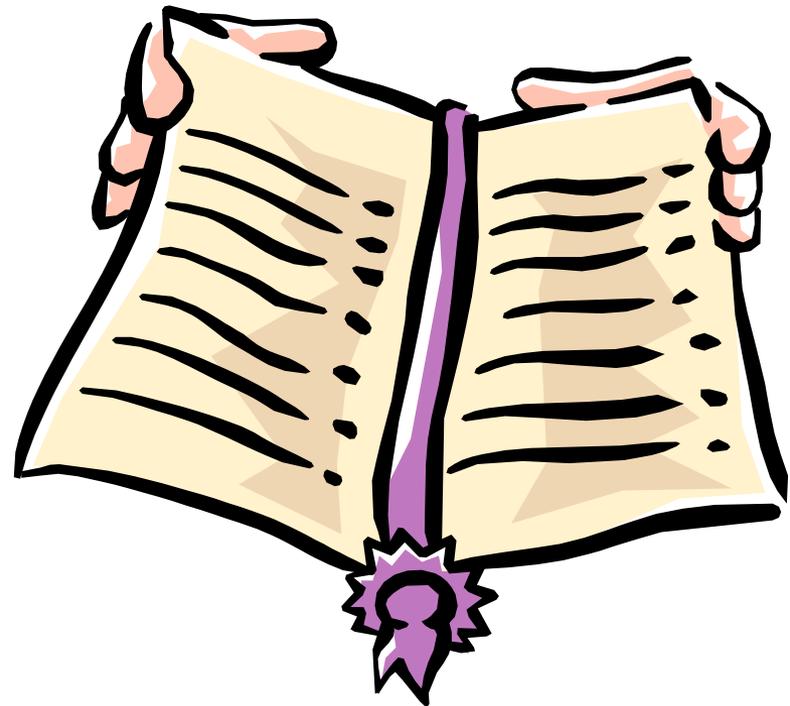
Query results 1 results (0.026 seconds)

Name	Type
TestHost	Virtual Machine

Name	Value
config_id	1309
cpu	2
cpu_limit	-1
cpu_res	0
cpu_shares	2000
date	Tue Sep 22 14:59:14 EDT 2009
exists	true

Service Catalog Capabilities

- Per Guest
 - Firewall, IDS/IPS, WAF, DLP
 - Software Inventory
 - Configuration management
 - Profile management
 - File Integrity
 - OS Compliance
 - Performance Statistics
 - Process Monitoring
 - Performance monitoring
 - Scheduled Reports
 - Event correlation & alerting
 - Policy Automation
 - Etc.



Reflex Industry Awareness



VIRTUALSTRATEGY MAGAZINE
the source for virtualization technology news

NETWORKWORLD



Gartner®

CTOEDGE



POWERING THE NEW IT GENERATION
VIRTUALIZATION
REVIEW