Vmware vCloud Director 1.5 & vShield 5 – What's New

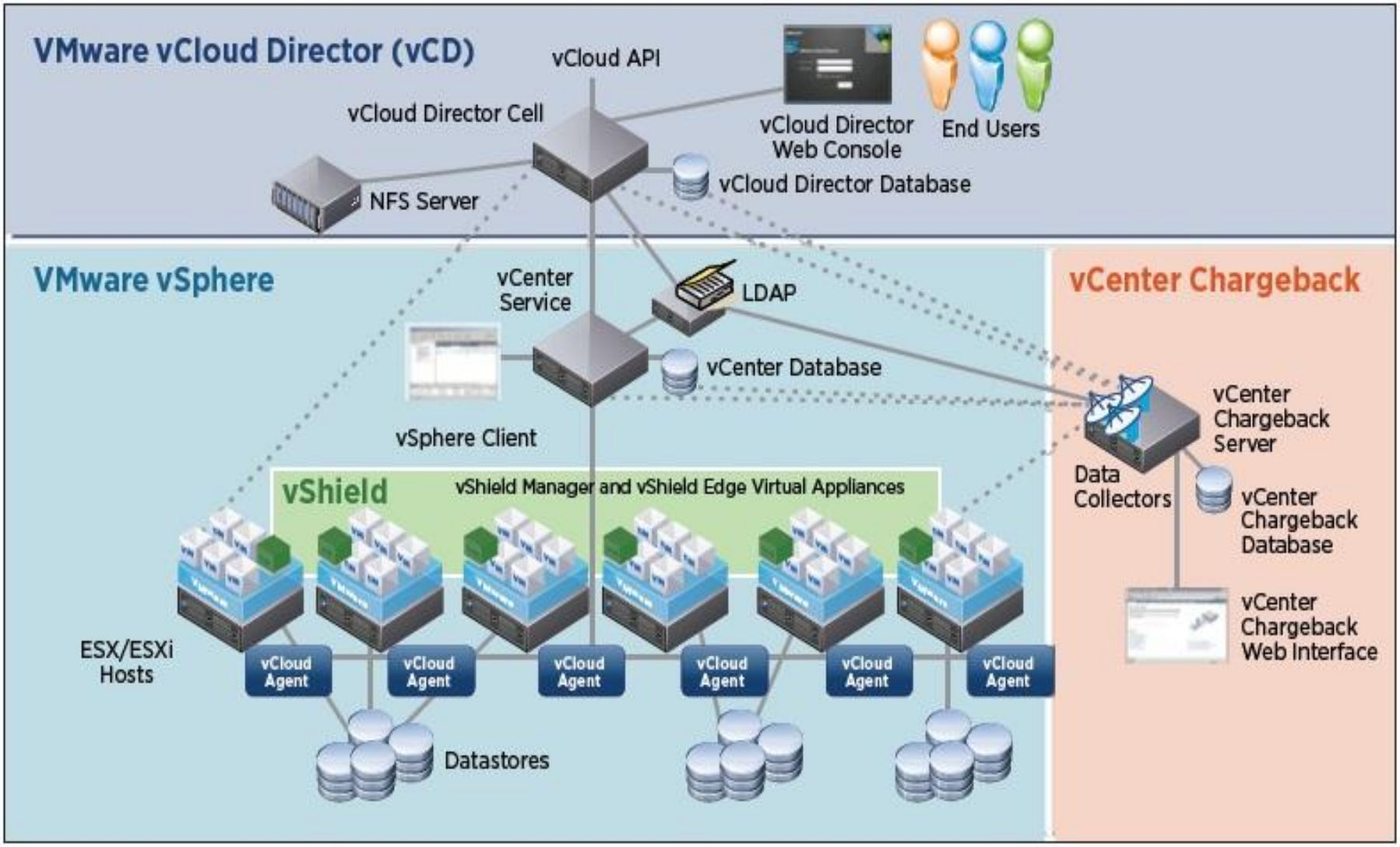
Maciej Kot

Senior System Engineer

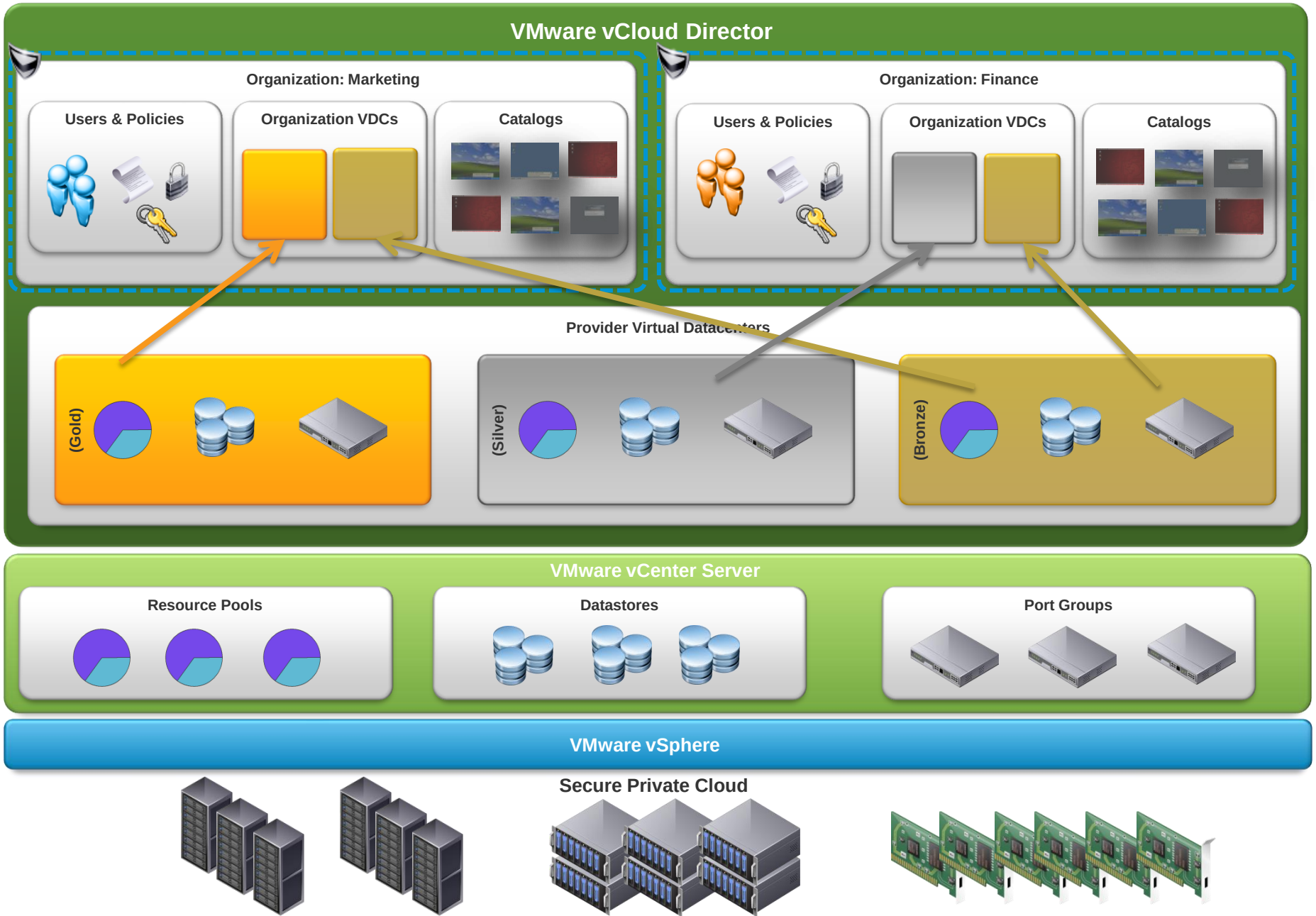
Agenda:

- **Introduction**
- vCloud Director 1.5 – What's new?
- Vmware vShield 5 Family – What's new?
- Implementing VMware Cloud Computing – Best Practices
- Q & A

Private cloud – VMware vCloud Director



Private cloud – VMware vCloud Director



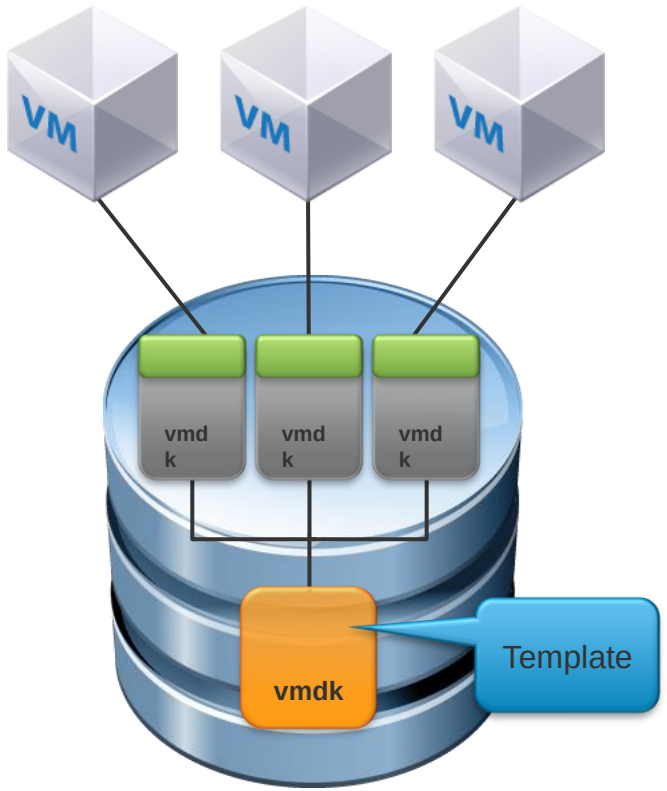
Agenda:

- Introduction
- **vCloud Director 1.5 – What's new?**
- Vmware vShield 5 Family – What's new?
- Implementing VMware Cloud Computing – Best Practices
- Q & A

VMware vCloud Director 1.5

- Fast Provisioning
- vApp Custom Properties
- Expanded vCloud API
- Microsoft SQL Server Support
- Cisco Nexus 1000 Support
- vShield Edge VPN integration

Fast Provisioning using Linked Clones For Improved Agility



Overview

- Provisions new VMs from a template or clone existing VMs without replicating the entire image
- Instead, links the images (clones) so that common elements are stored only once

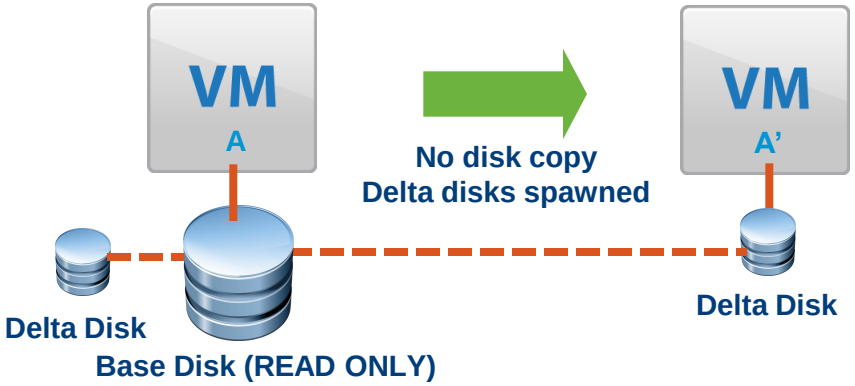
Benefits

- Dramatically speeds up provisioning time from >2 minutes to <5 seconds
- Reduces storage footprint (and cost) by over 60%

Linked Clones in vCD 1.5 vs. Full Clones

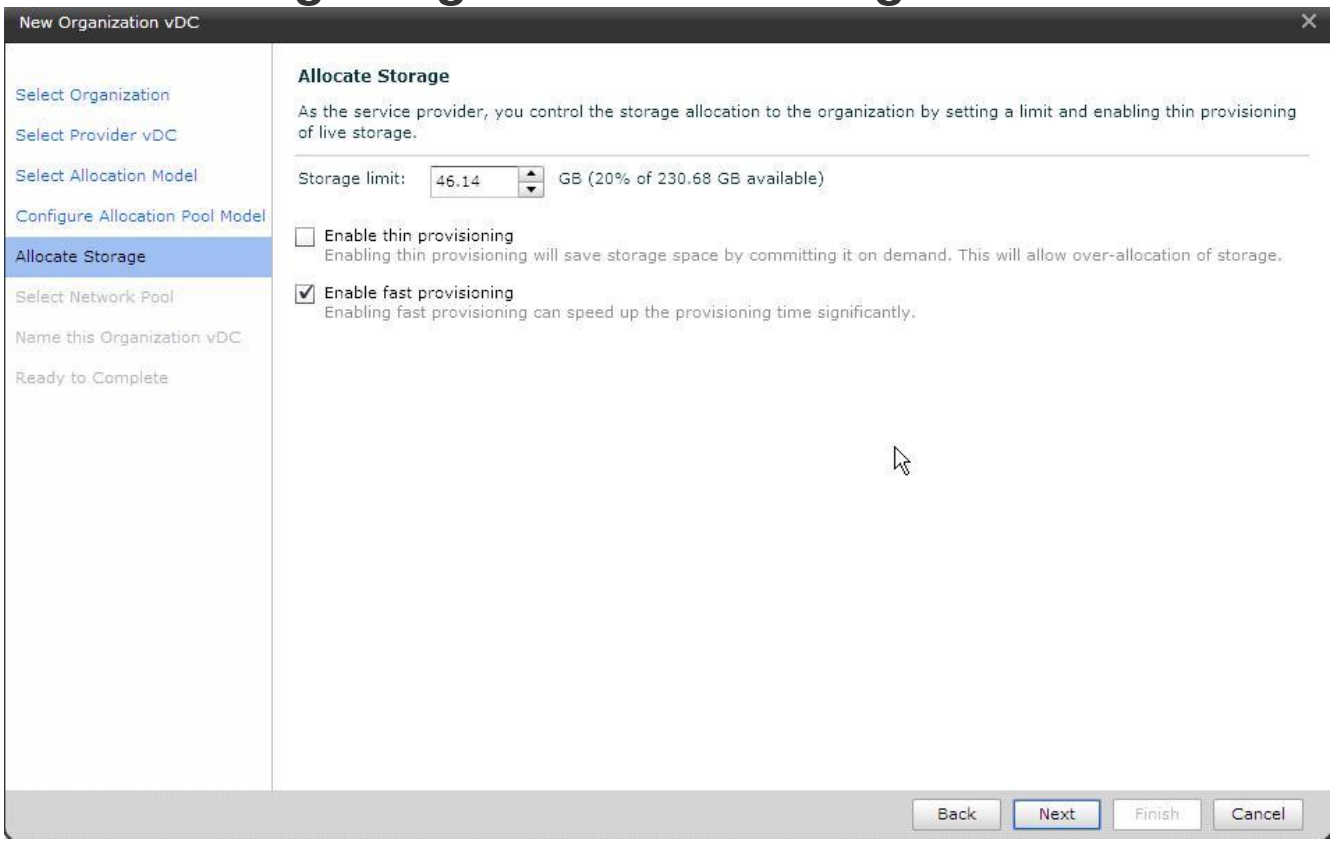
Full Clone (Default)

Fast Provisioning



Enabling Linked Clones Is Easy

- **Single click operation done by vCloud Administrator**
  - Creating new Organization vDC
  - Modifying existing Org vDC
- **Automated Billing integration with Chargeback**



Use cases for Linked Clones

- **Use fast provisioning to accelerate vApp deployment time**
  - **Production and Pre-production workloads**
    - Instantly clone production or pre-production workloads
  - **Test and Dev workloads**
    - Use linked clones when users spin up multiple copies of vApps to save time
    - Use in conjunction with “Network Fencing” to deploy fully isolated test/dev environments in a matter of seconds
  - **Demo workloads**
    - Use linked clones to quickly provision demo environments for field staff. Demo environments provisioned in minutes
  - **Support desk**
    - Provision multiple copies of vApp templates to troubleshoot customer issues. Support can react faster to incoming issues increasing customer satisfaction
- **Use fast provisioning to conserve storage**
  - vCloud administrators can enable fast provisioning on an existing organization virtual datacenter to reduce storage footprint of vApps

Management of Linked clones

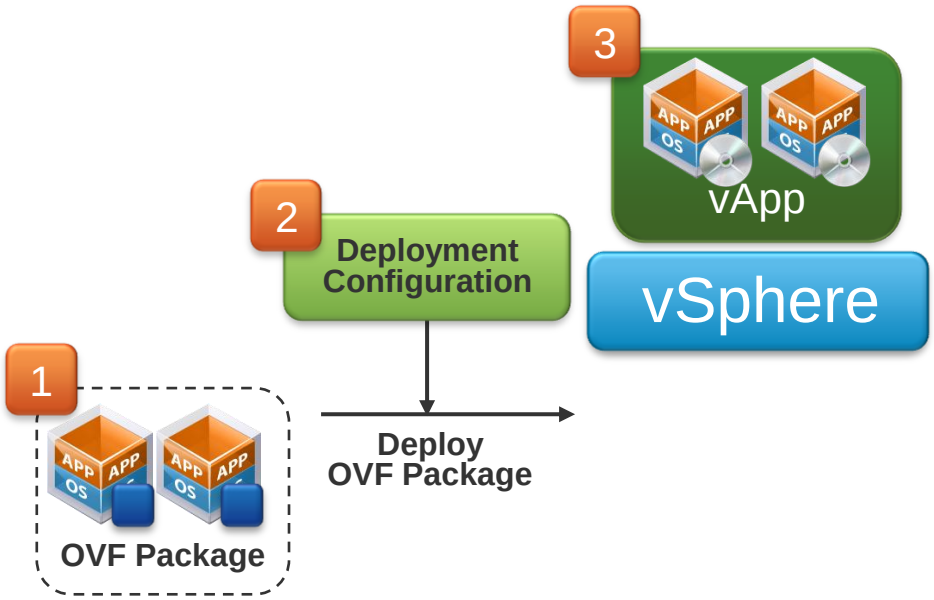
- **Migration of linked clones**
  - Use vCD API to migrate VM to alternate datastore
  - Leverages Storage vMotion to migrate and tree structure is maintained
  - Works for both powered on and powered off VMs
  - Note: Using Storage vMotion directly from vSphere client will flatten the disks, so do not use.
- **VM tree consolidation**
  - Use vCD API to consolidate powered off VM trees to chain length zero
  - Will not work if VMs have any user created snapshots.

UI support for migration and consolidation not available in the current release. These are not common operational tasks

Known limitations for Fast Provisioning

- **Eight node VMFS limitation**
  - Ensure that the storage datastores with linked clone trees are zoned to no more than **eight hosts so DRS does not move the VMs to a ninth host**.
  - Alternatively use NFS to allow trees to be accessed by hosts in clusters larger than eight nodes
- **No support for VAAI (vStorage APIs for Array Integration)**
- **Linked clones requires upgrade to vSphere 5.0**
  - Mixed mode (vSphere 4.0/4.1 and vSphere 5.0 in the same cluster **not supported for linked clones**)

vApp Custom Guest Properties



Overview

- Allows developers and other users to easily pass user data into guest OSes using OVF descriptors.
- Parameters available using VMware tools, on an ISO, or in the XML for the vApp

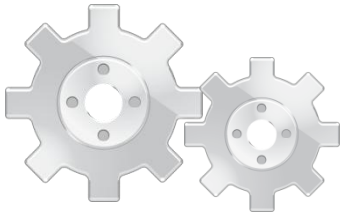
Benefits

- Easier post-deployment configuration & provisioning of identity to VMs & vApps
- Provides functionality to bootstrap a wide variety of guest customization solution

Detail and Use cases

- **User data can be defined at vApp level and at VM level**
  - User data defined at vApp level are propagated to all VMs in the vApp
  - User data defined at VM level take precedence if same key is defined at both vApp and VM level
- **Use Cases**
  - Initializing personalization procedures such as Kickstart or Windows Automated Installer;
  - Establishing security keys/authorization credentials for remote access, for instance ssh-keys;
  - Provide configuration/identity to bootstrap configuration management systems/automation systems, for instance configuring chef, SCM, etc.
  - Passing executable scripts to VMs to enable further customization
  - Pass variables to post-deploy scripts such as usernames, database information, or any other per-guest customization information
  - Include information about which load balancer to connect to when deploying auto-scaling applications

Expanded vCloud APIs and SDKs



Programmatic Control and Integrations

Overview

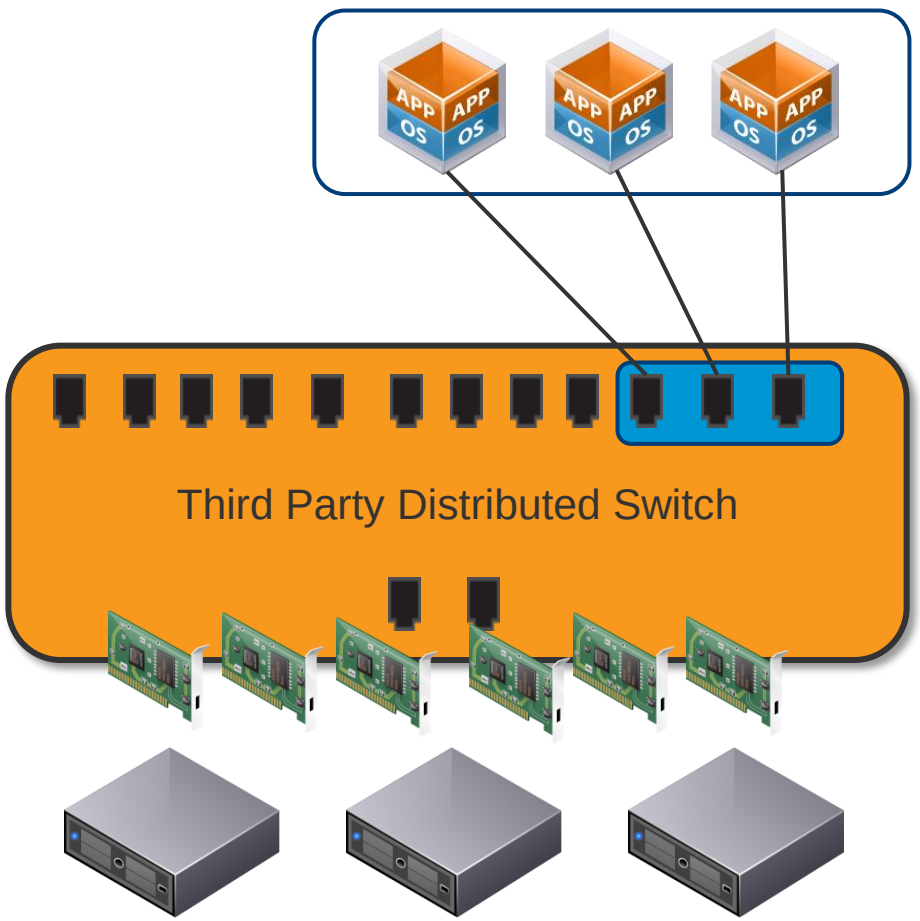
- vCloud SDKs for Java, PHP, .NET
- Additional commands added to the vCloud API namespace to include all GUI-accessible actions

Benefits

- Enables broader integration and scripting using the API

vCloud API tasks now on parity with the vCD UI

Third Party Distributed Switch Integration



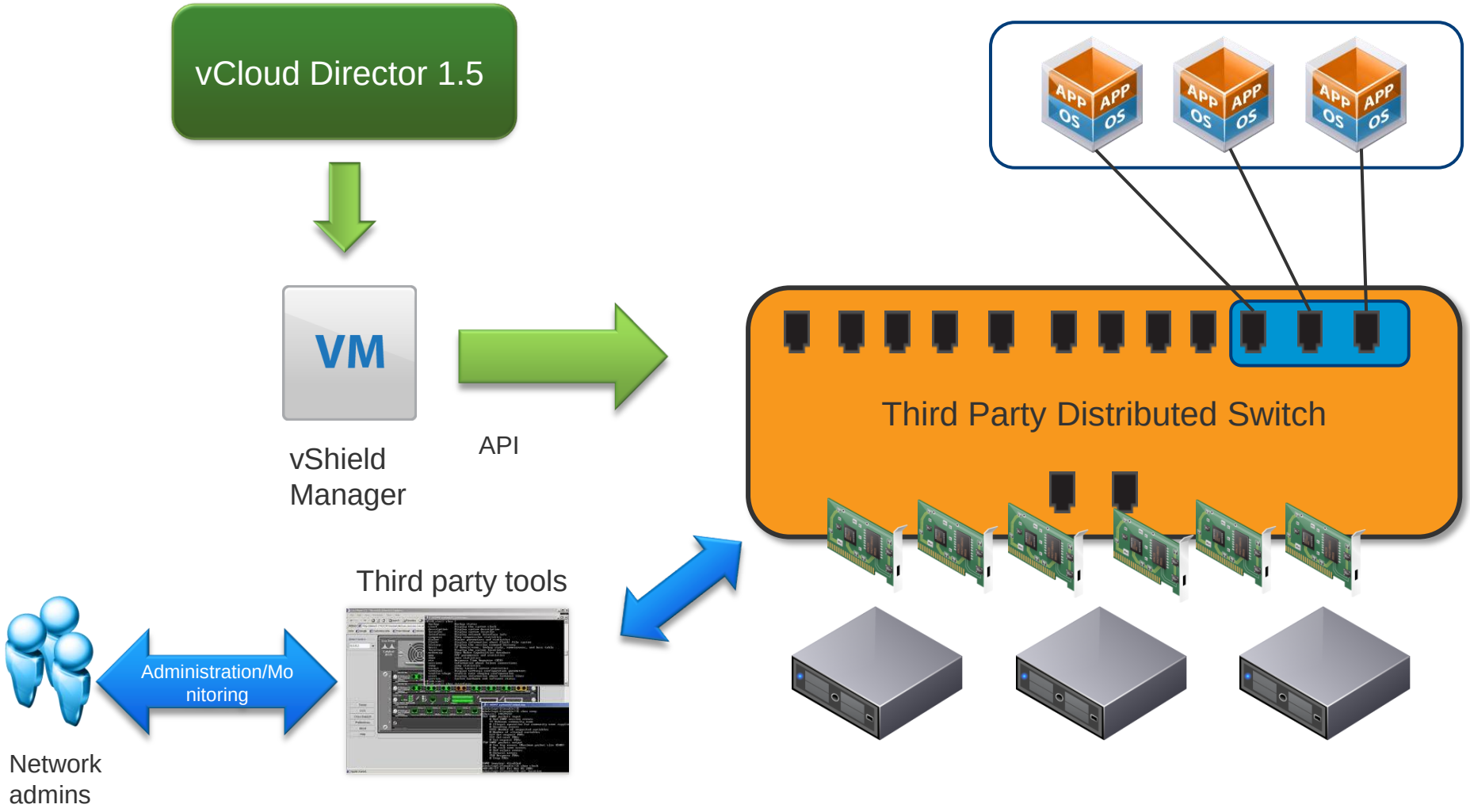
Overview

- Support for broader range of network pool types in third party distributed switches
- Support VLAN-backed networks and vCloud Director Network Isolation backed networks (VCDNI)

Benefits

- Leverage third party switches – automatic portgroup creation now enabled
- Leverage third party tools for network monitoring in conjunction with vCloud deployments.

Manage your cloud networking using standard tools

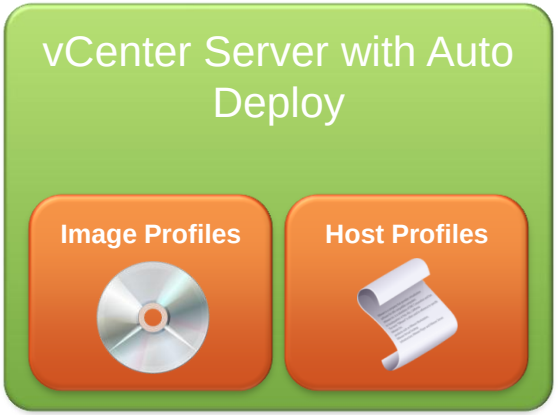


Microsoft SQL Server Support

- **Supported Databases**
  - Oracle 10g Std/Ent Release 2
  - Oracle 11g Std/Ent
  - Oracle 11g R2
  - Microsoft SQL 2005 Std/Ent SP4
  - Microsoft SQL 2008 Exp/Std/Ent (64-bit)

vSphere 5 support

vCloud Director 1.5



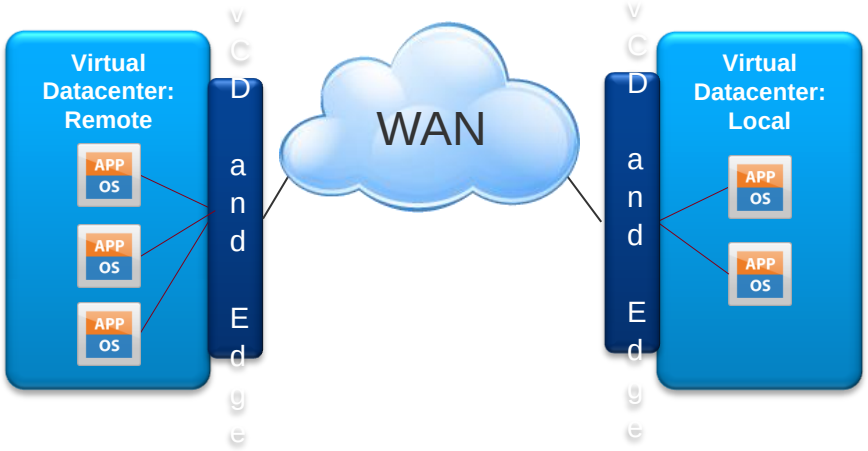
Overview

- vCloud Director adds support for vSphere 5 platform
  - vSphere Auto Deploy support
  - Support for virtual hardware v8
    - 32 vCPU
    - 1 TB vRAM

Benefits

- Faster deployment of physical infrastructure
- Run the most demanding workloads in vCloud Director

Expanded vShield Integration



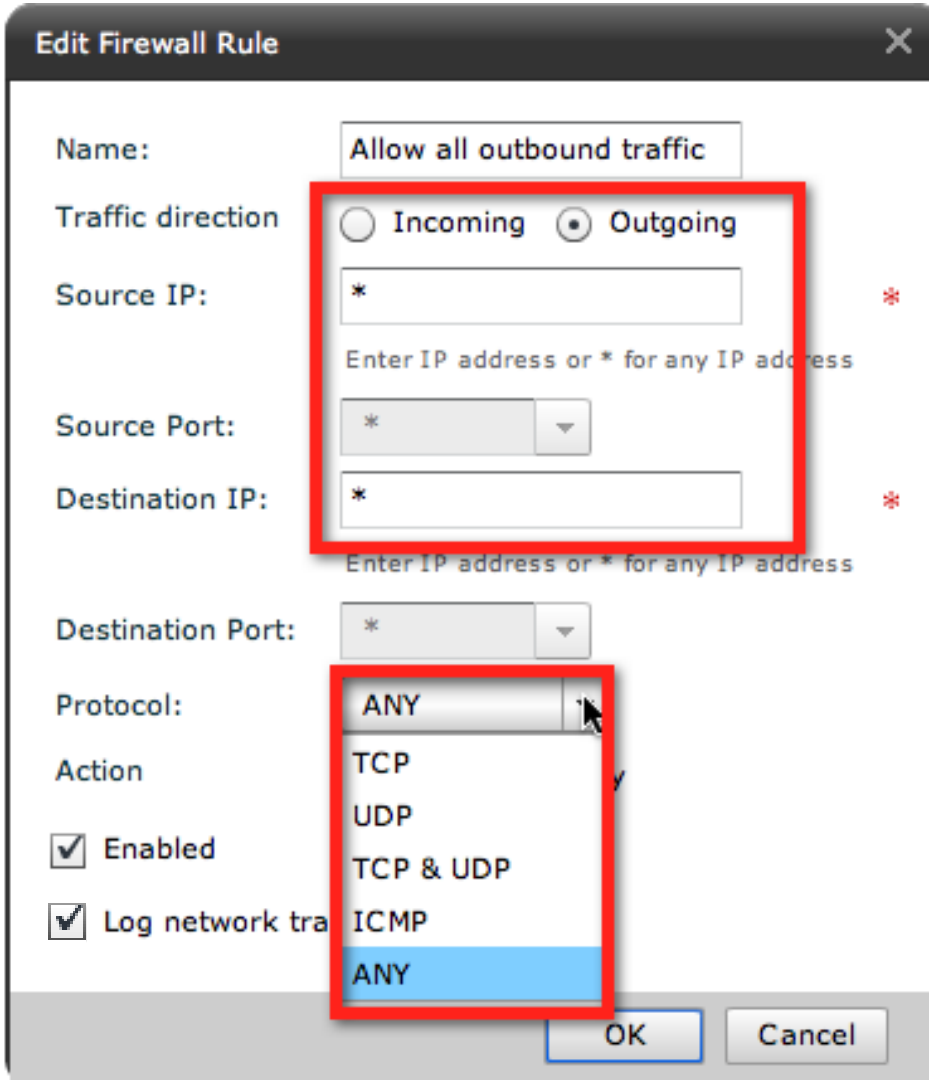
Overview

- Integration with vShield IPSec VPN capabilities through both API & UI
- Expanded firewall capabilities to include full 5-tuple firewalls and static routing

Benefits

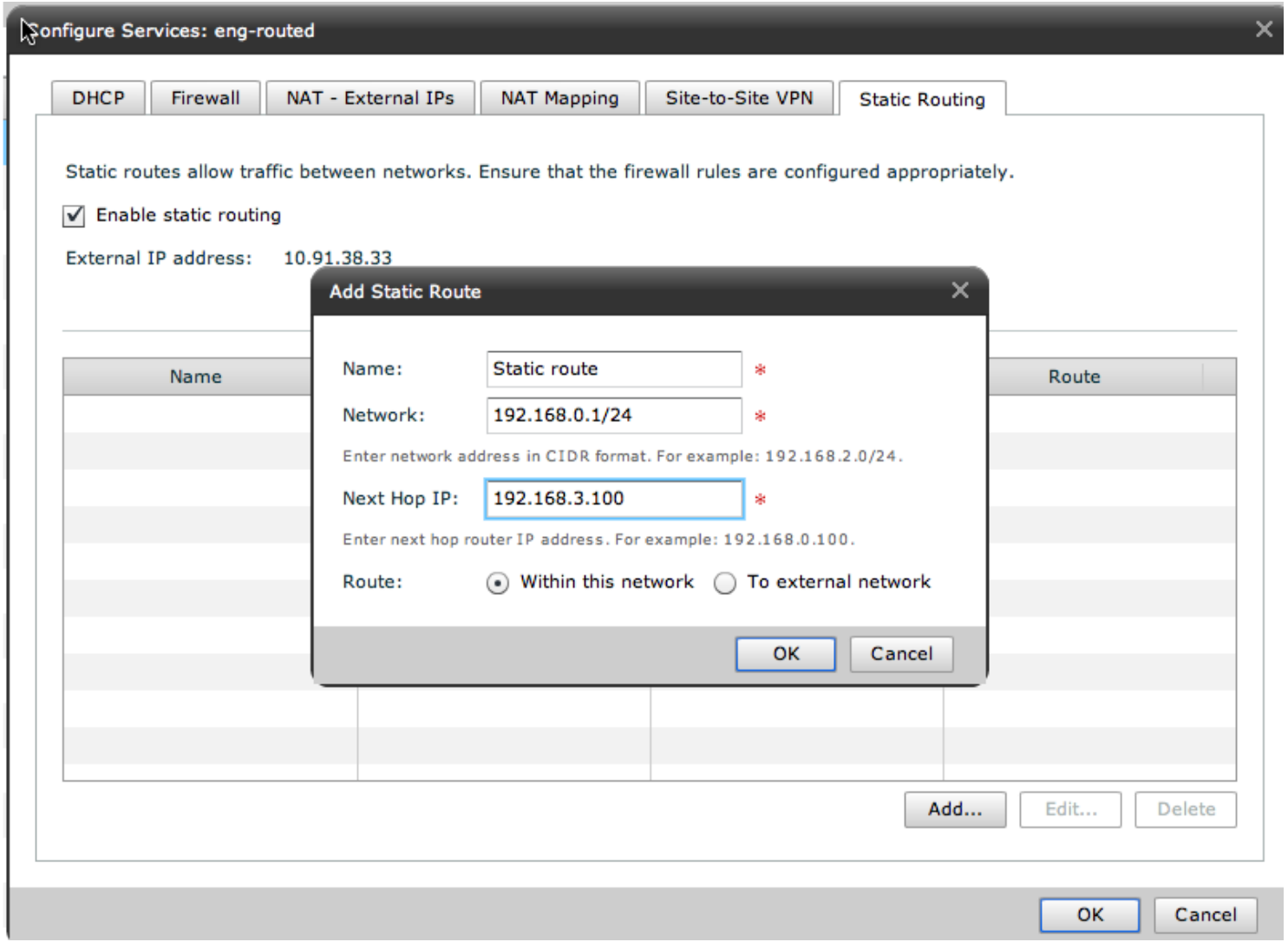
- Organization administrators can easily configure private networking enclave connected between datacenters (private and public)
- 5-tuple firewalls allows fully flexible network access management—control source & destination.

Five Tuple Firewalls



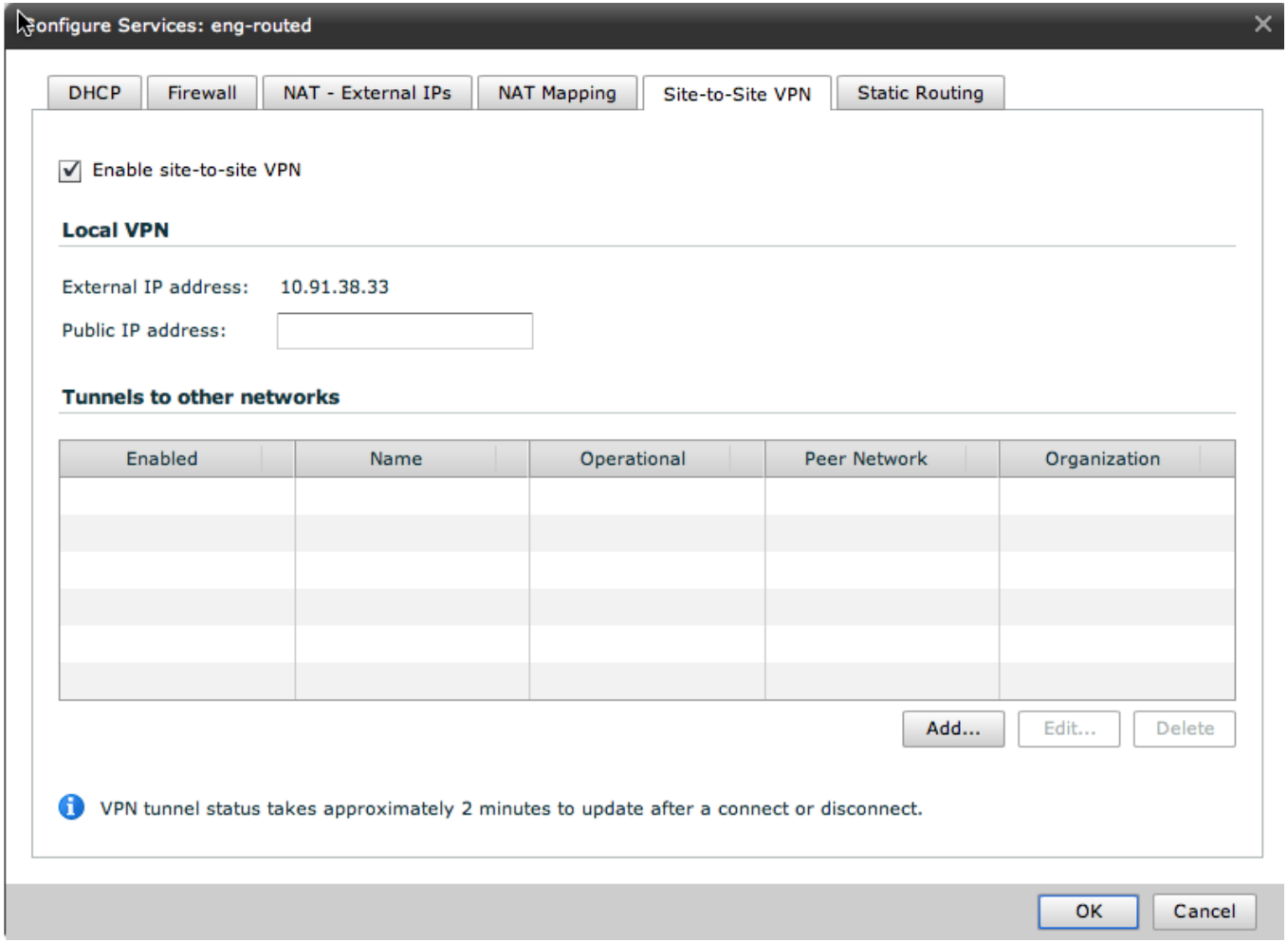
- **Create complex firewall rules for enhanced security**
  - Firewall rules now can be configured for <source address, source port, protocol, destination port, destination address>
  - Support for ICMP protocol in addition to tcp and udp
  - Define syslog targets enabling vSE logging.

Static Routing

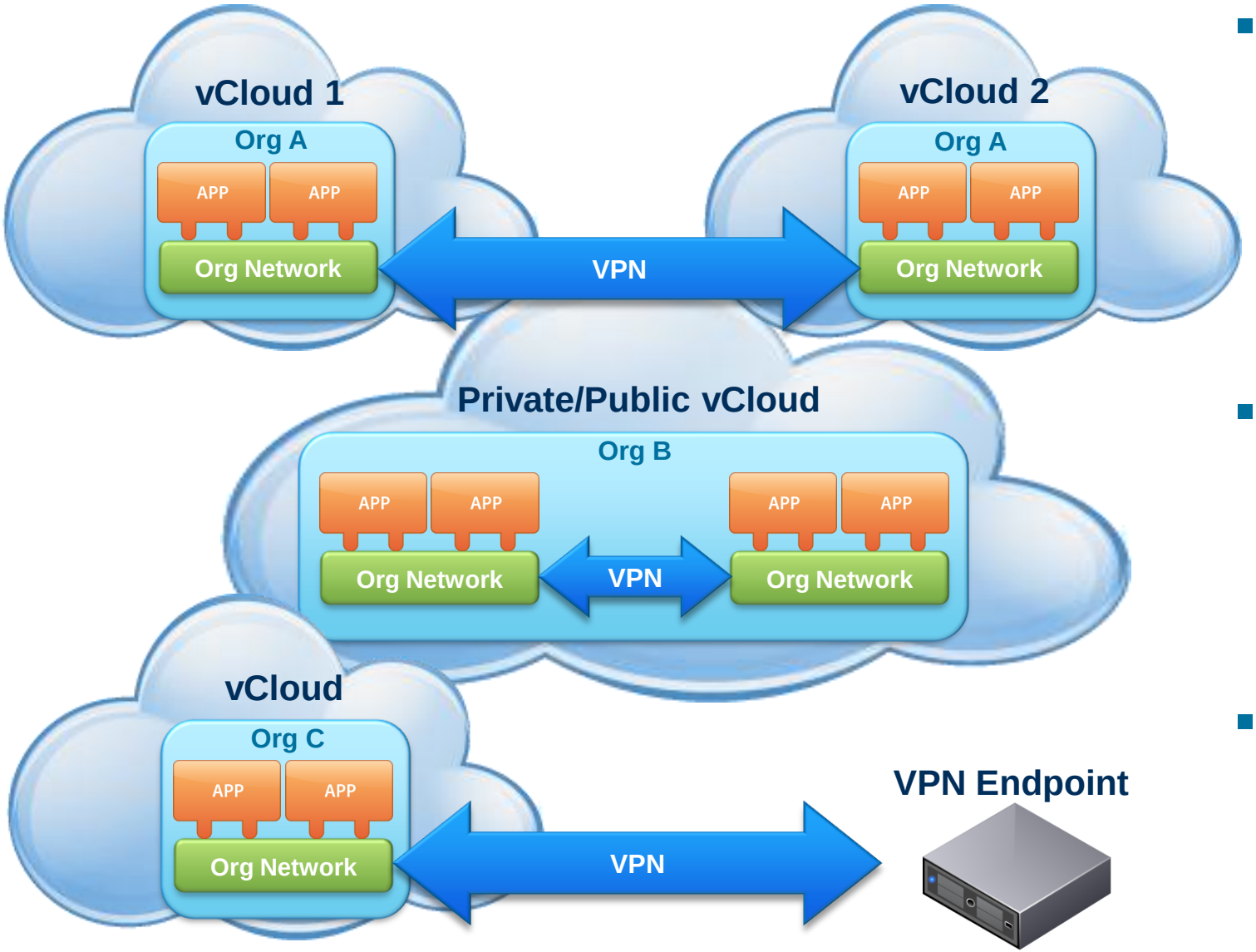


IPSec Site to Site VPN

- **Enable Site to Site VPN connections using vCloud Director**
  - Configured by the organization administrator on a routed org network

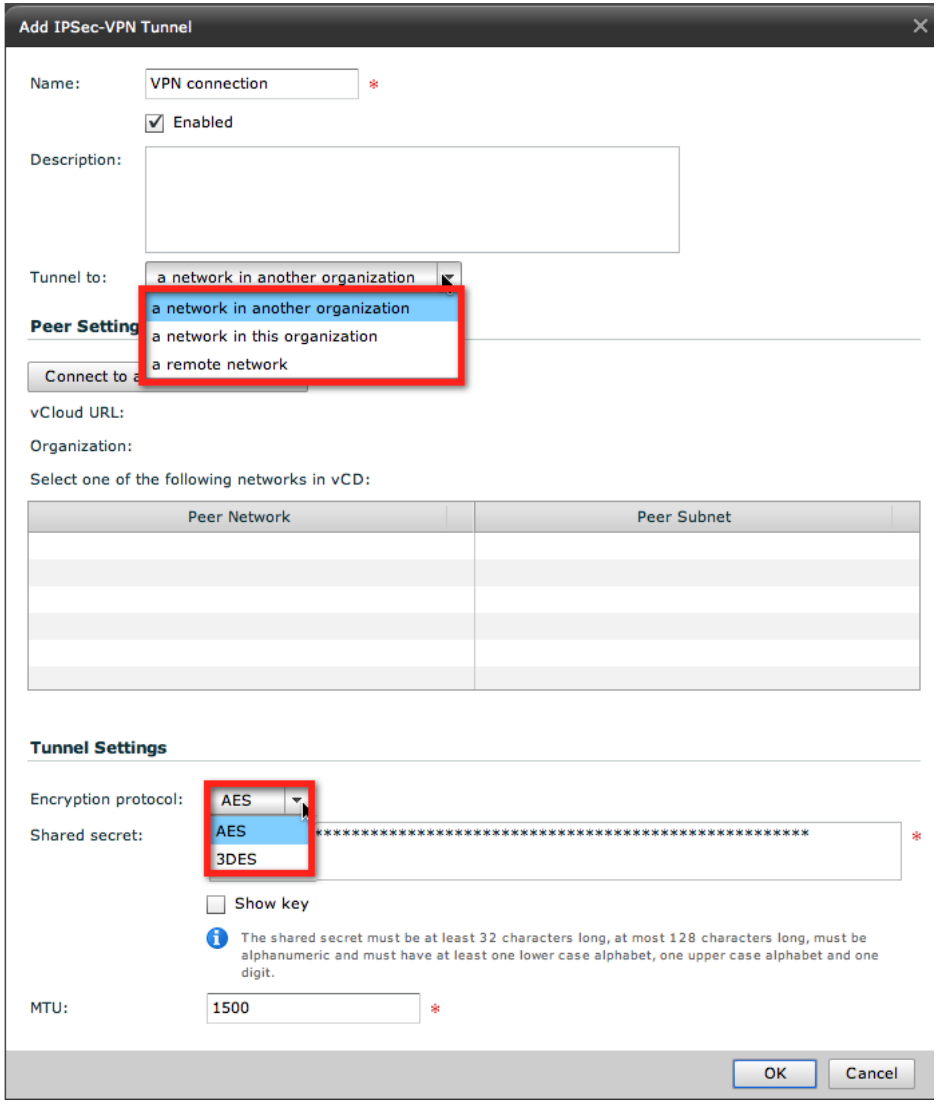


IPSec VPN tunnel configuration types



- Tunnel to network in another organization
- Tunnel to network in this organization
- Tunnel to a remote network

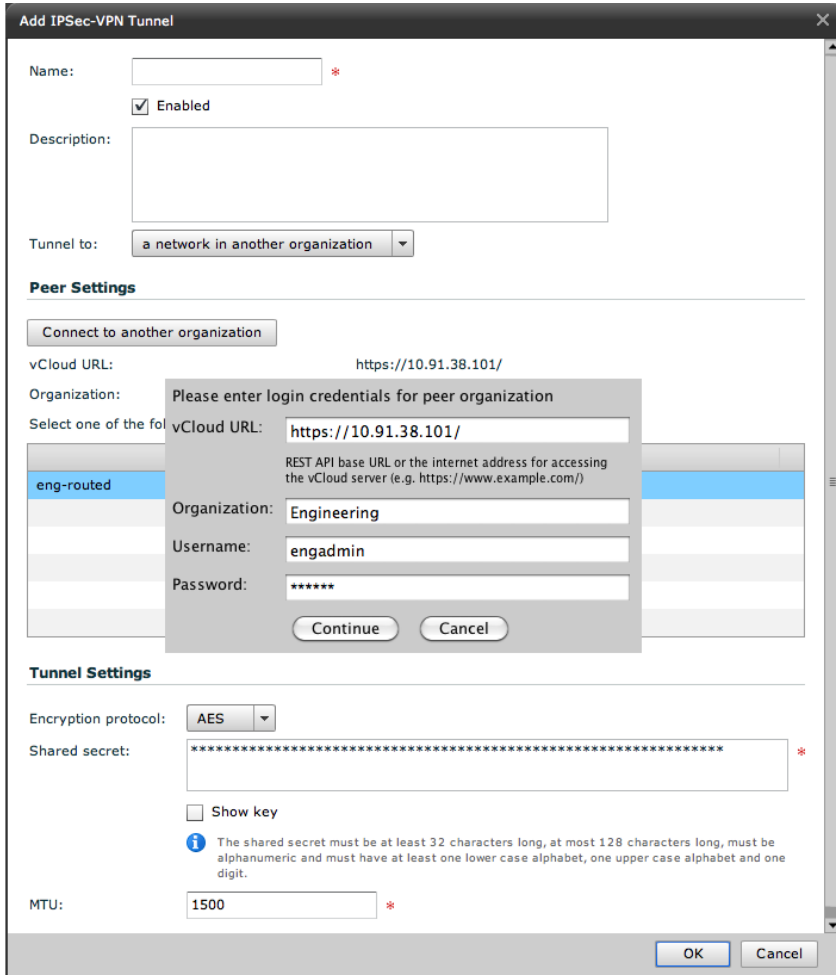
Types of VPN connections and Encryption Protocols



- **Choose from a network in**
  - Same organization
  - Different organization
  - VPN endpoint (remote network)

- **Choose encryption protocol**
  - AES
  - 3DES

Setting Up VPN Tunnels



- **Connecting to organization network to setup VPN tunnel is really easy**
  - vCloud URL
  - Organization Name
  - Credentials
- **Setup Site to Site VPN connections in a matter of minutes**
  - Self-service
  - No need to call or email the vCloud administrator

Agenda:

- Introduction
- vCloud Director 1.5 – What's new?
- **Vmware vShield 5 Family – What's new?**
- Implementing VMware Cloud Computing – Best Practices
- Q & A

Data Center needs to be secured at different levels–

Perimeter Security

- Perimeter security device (s) at the edge
- Firewall, VPN, Intrusion Prevention
- Load balancers

Keep the bad guys out

Internal Security

- VLAN or subnet based policies
- Interior or Web application Firewalls
- DLP, application identity aware policies

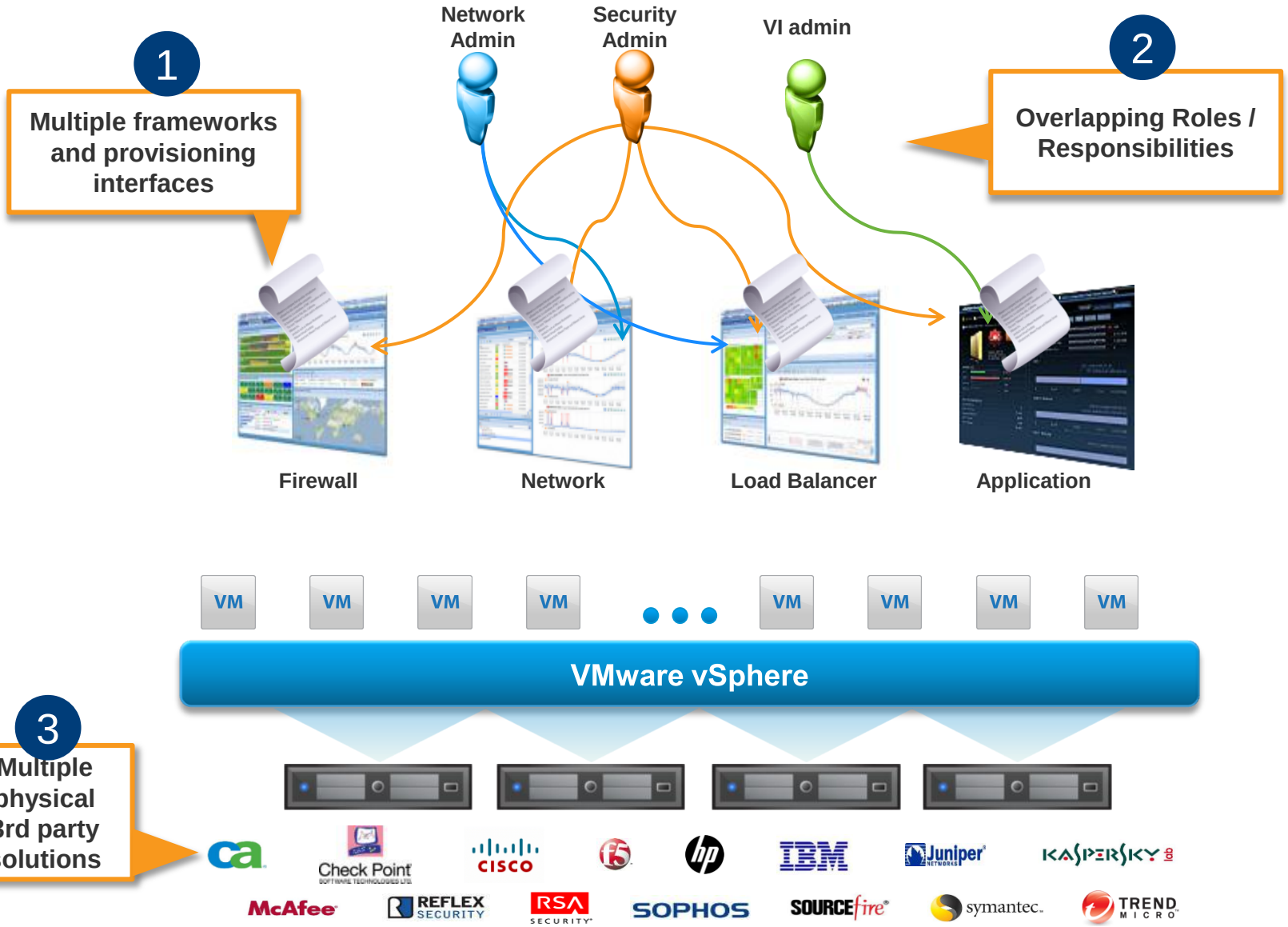
Segmentation of applications, servers

End Point Security

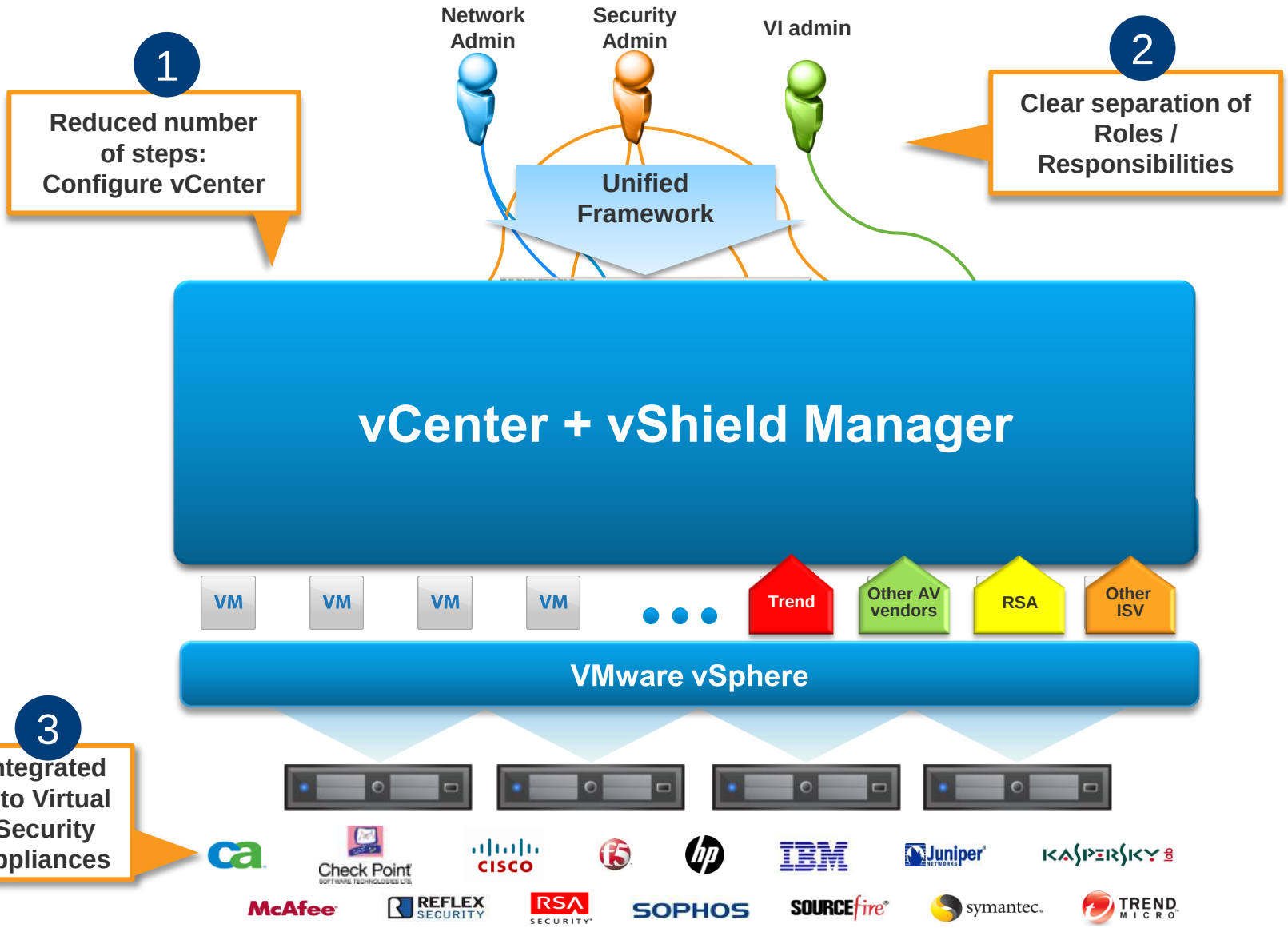
- Desktop AV agents,
- Host based intrusion
- DLP agents for privacy

End Point Protection

VMware Transforms Security from Complex…

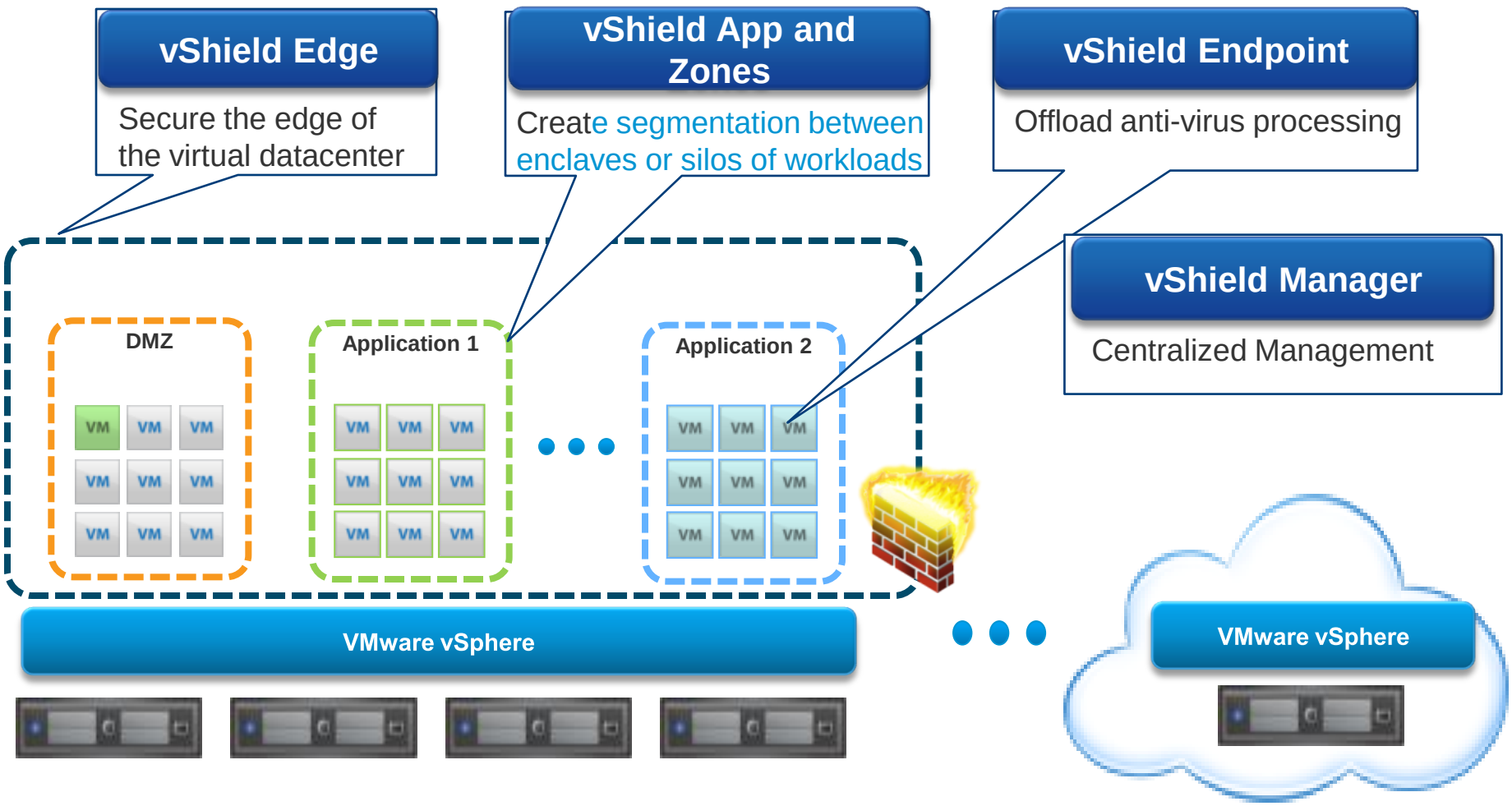


…To Disruptively Simple



vShield Products Family

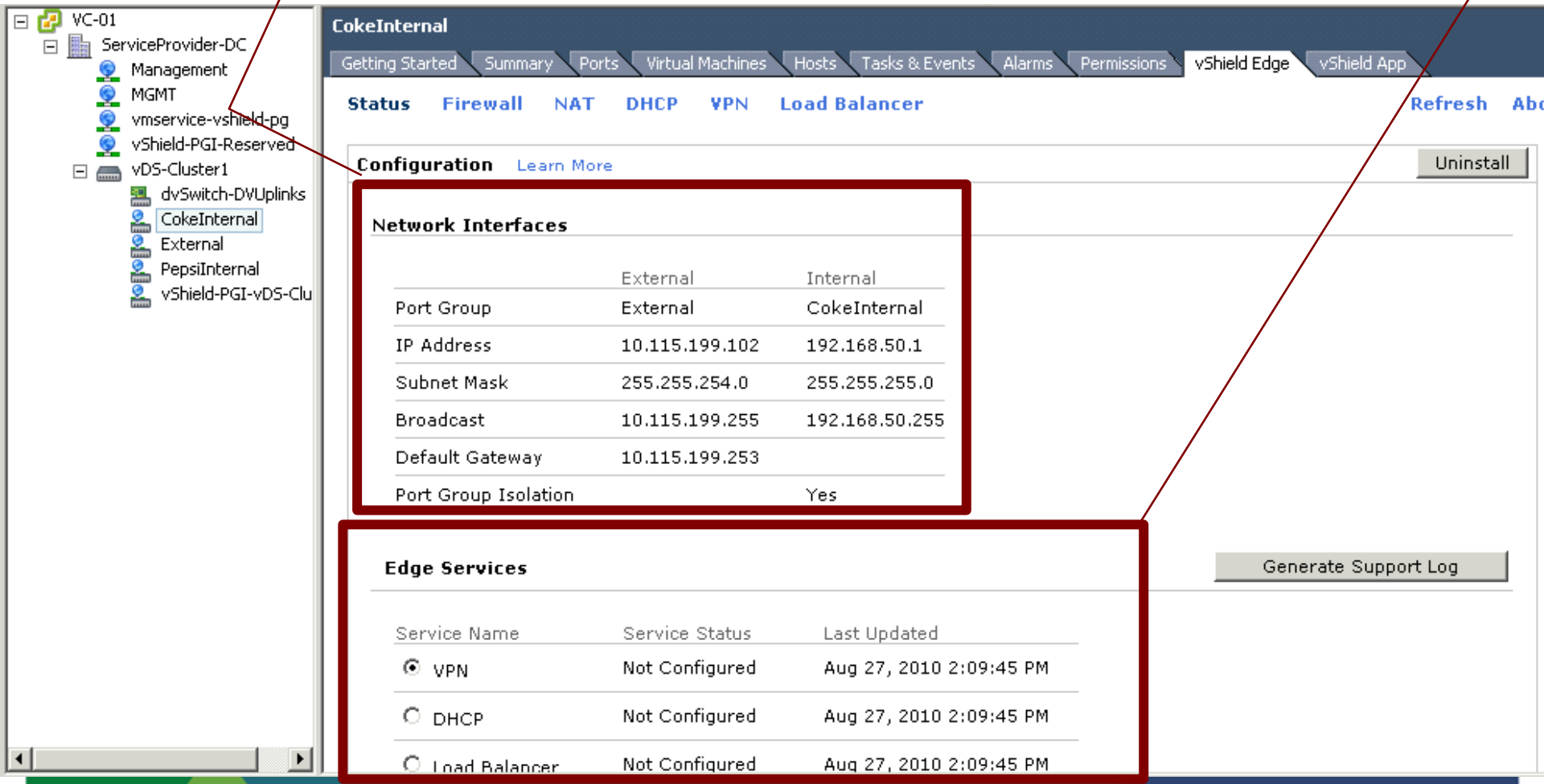
Securing the Private Cloud End to End: from the Edge to the Endpoint



vShield Edge

External and internal (private) address space

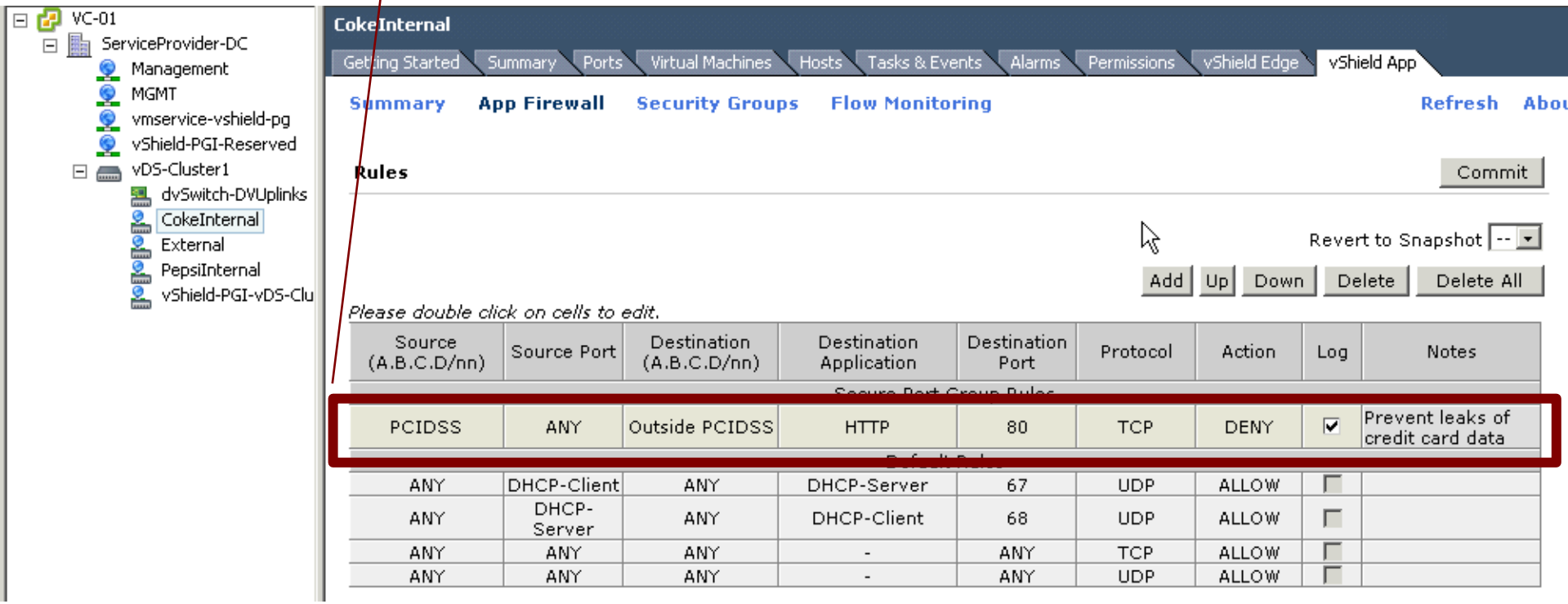
vShield Edge virtual appliance can be configured to provide VPN, DHCP, Load Balancing and more



vShield App

Secure traffic between virtual machines, within port group

Use Security Groups created earlier to define firewall policies without constraints of rules based on IP addresses



New Features in vShield 5.0

- **Sensitive Data Discovery to meet standards & regulations**
  - Accurately discover and report sensitive data in unstructured files
  - Segment off VMs with sensitive data in separate trust zones
- **Strong and efficient protection against network intrusions**
  - Ability to quarantine compromised VMs
  - Layer 2 Firewall
- **Efficient Anti-Virus**
  - Offloaded anti-virus protection for server and desktop applications
  - Leverage 3rd party anti-virus solutions

Sensitive Data Discovery to Meet Standards & Regulations

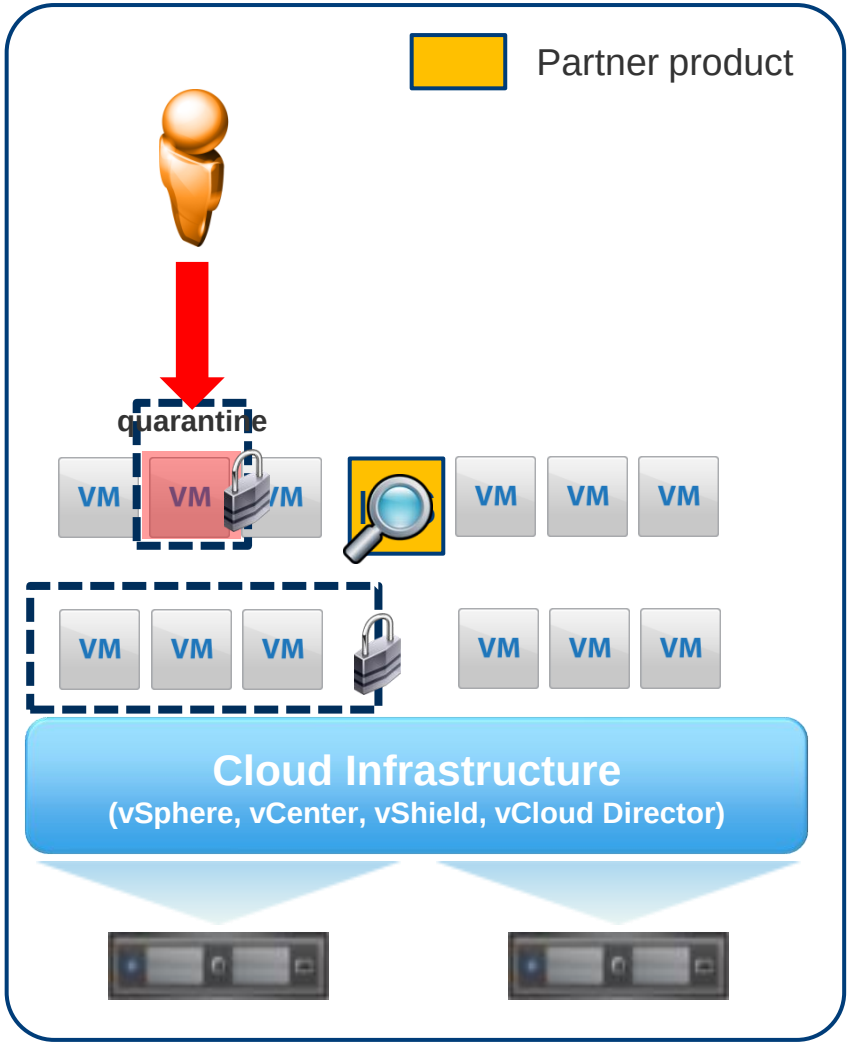
Overview

- More than 80 pre-defined templates for country/industry specific regulations
- Accurately discover and report sensitive data in unstructured files with analysis engine
- Segment off VMs with sensitive data in separate trust zones

Benefits

- Quickly identify sensitive data exposures
- Reduce risk of non-compliance and reputation damage
- Improve performance by offloading data discovery functions to a virtual appliance

Strong and Efficient Protection Against Network Intrusions



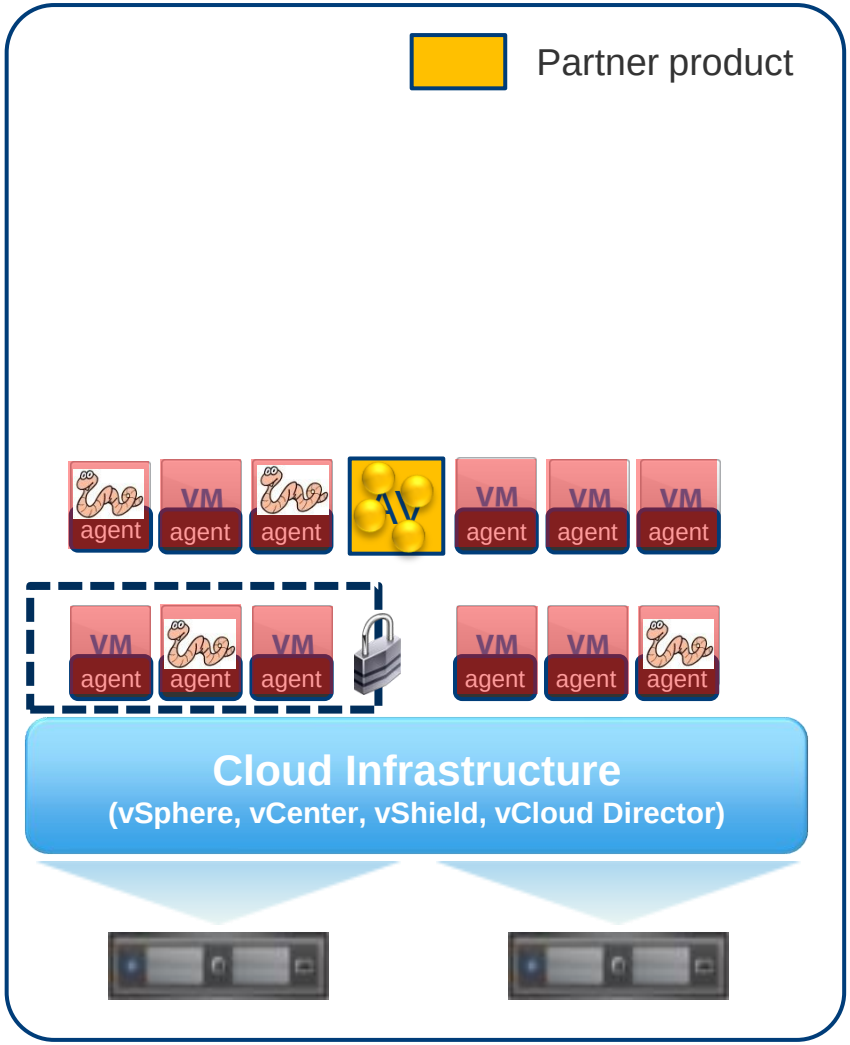
Overview

- Leverage 3rd party intrusion detection solutions (IDS) to identify network based threats
- Automatically isolate compromised VMs

Benefits

- Contain network intrusions and prevent them from spreading in the environment

Efficient Anti-virus Solution to Protect Virtual Machines



Overview

- Offloaded anti-virus protection for desktop and server applications
- Leverage 3rd party anti-virus solutions

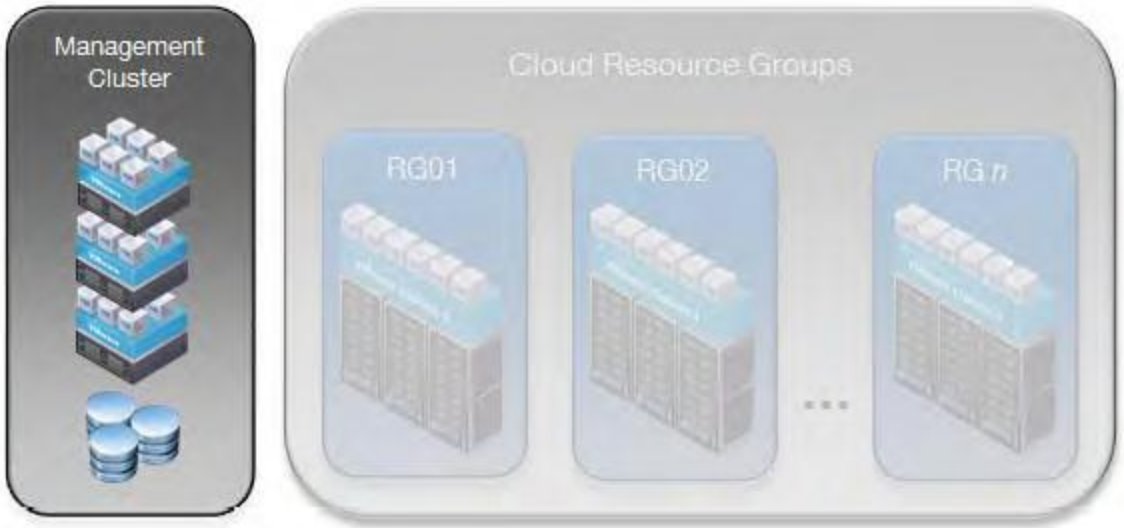
Benefits

- Eliminate anti-virus storms
- Rapid provisioning: deploy and patch
- Reduce risk and improve performance by eliminating agents susceptible to attack
- Lower cost and complexity to protect virtual machines against malware

Agenda:

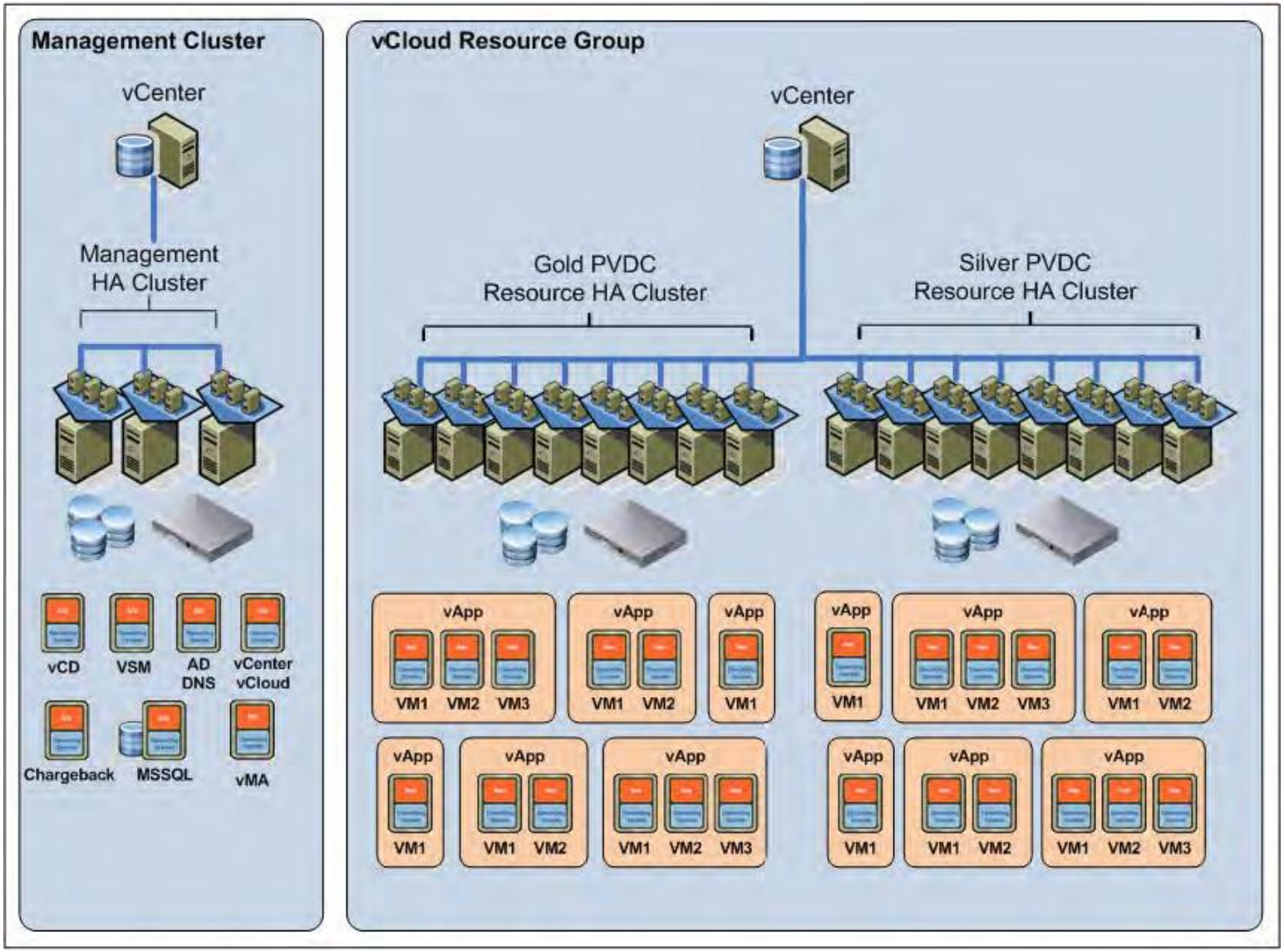
- Introduction
- vCloud Director 1.5 – What's new?
- Vmware vShield 5 Family – What's new?
- **Implementing VMware Cloud Computing – Best Practices**
- Q & A

VMware Cloud Computing – Best Practice

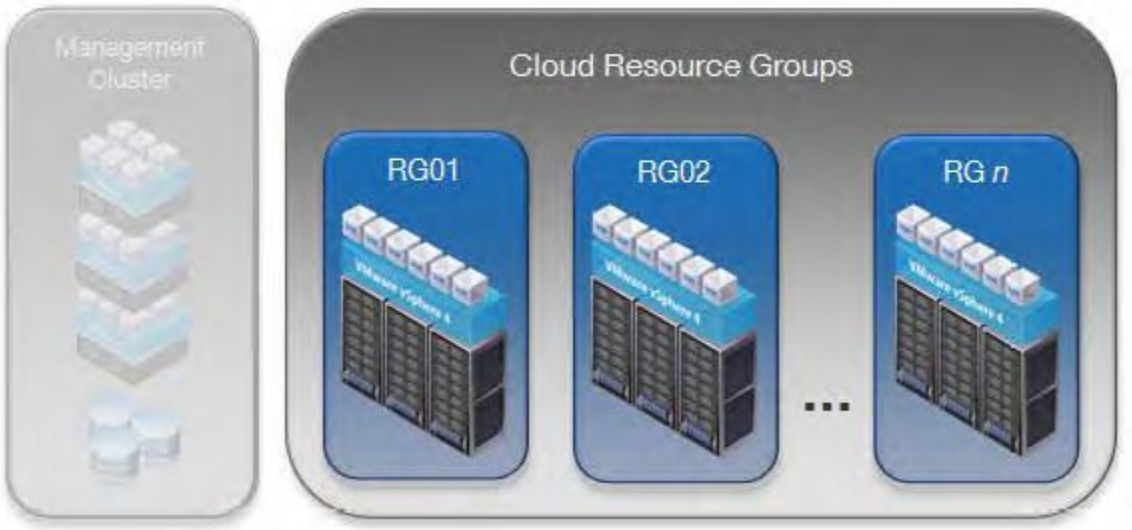


- vCenter Server 5.0 or vCenter Server appliance, ESXi 5.0 hosts
- vCenter Server database,
- vCloud Director 1.5,
- vCloud Director database.
- vShield Manager 5.0 (one per resource group vCenter Server.)
- vCenter Chargeback Server 1.6.2.
- vCenter Chargeback database and data collectors.
- VMware vCenter™ Update Manager.
- vCenter Orchestrator.
- LDAP, NTP, DHCP, DNS, Syslog

VMware Cloud Computing – Best Practice

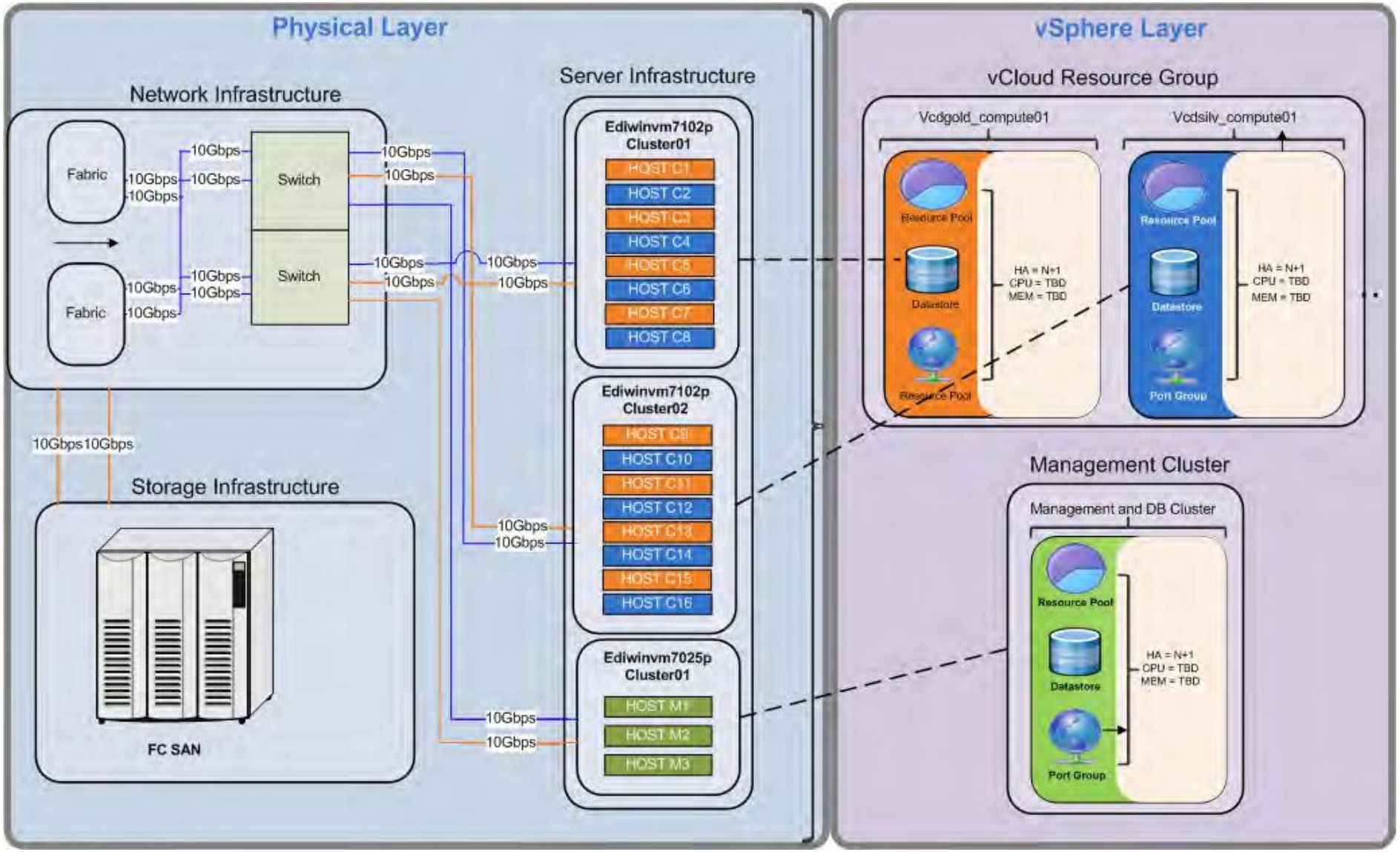


VMware Cloud Computing – Best Practice



- The total number of hosts in an HA/DRS cluster remains 32 – **do not exeed eight hosts** in a cluster if using fast provisioning (linked clones) and VMFS datastores,
- increase the number of vSphere Distributed Switch ports per host from the default value to the maximum of 4096,
- Increase the maximum transmission unit (MTU) size to 1600 for all devices residing in the transport network for vCloud Director network isolation,
- **vShield Edge does not support IPv6,**
- The license for vShield Edge included with vCloud Director (*vShield for vCloud Director)* ***does not include features such as VPN and load balancing capabilities, which are part of the fully licensed vShield Edge****,*
- Currently, vCloud Director **does not have integration with vShield App**. Using vShield App in conjunction with vCloud Director is a supported configuration, but requires careful design of the vCloud infrastructure,
- Currently vCloud Director **does not have integration with vShield Endpoint.**

VMware Cloud Computing – Best Practice



VMware vShield

<table>
<tr><td>Deployment</td><td>• one vShield Manager per vCenter Server
• one vShield App per ESX™ host</td><td>• one vShield Edge per port group
• One vShield Endpoint per ESX™ host</td></tr>
<tr><td>Hardware</td><td>Memory: 8GB
NIC: 2 gigabit NICs per ESX host</td><td>Disk space
• 8GB – for one vShield Manager
• 5GB – per vShield App per ESX host
• 100MB – vShield Edge
• Varies – for partner SVM (anti-virus)</td></tr>
<tr><td>Software</td><td colspan="2">• vCenter, vSphere Licensing: 4.0 U1*, 4.1, 5
• All packages except Essentials (Essentials Plus onwards OK)</td></tr>
<tr><td rowspan="2">Client and User Access</td><td>VMware vSphere Client
Privileges
• add, power on virtual machines
• Access to datastore with virtual machine files
• Copy files to this datastore</td><td rowspan="2">Web-based access
Supported browsers
• Internet Explorer 6.x and later
• Mozilla Firefox 1.x and later
• Safari 1.x or 2.x

Enable cookies for access to vShield Manager</td></tr>
<tr><td>Guest Virtual Machines (vShield Endpoint)
Thin client driver in supported OS
SCSI controller</td></tr>
</table>

Q & A