BCNET

EduCloud Server

Sanja LeBlanc, Manager, UBC IT Systems (sanja.leblanc@ubc.ca)
Chris Krusch, Systems Architect, UBC IT Systems (chris.krusch@ubc.ca)
Randell Ong, Systems Administrator, UBC IT Systems (randell.ong@ubc.ca)

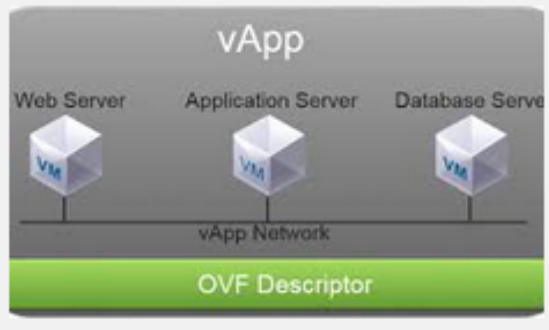
Agenda

1	Managing your EduCloud Server Virtual Datacentre
2	Capacity and Performance Dashboards
3	Rightsizing your Workloads
4	Authentication
5	Roadmap
6	Feedback
7	Questions

Managing vApps

vApps

- Standard unit of deployment in EduCloud
- Virtual application comprised of VMs, networks, and policies



- Policies include start/stop actions, start up/shutdown order

Managing vApps

vApps (continued)

- Create vApp templates for cloning
- Export vApps
- Snapshot
- Migrate across virtual data centers
- Assign permissions

Managing Catalogs

- Content repository for vApp templates and media files in an organization
- vApp templates are comprised of one or more VM templates
- users can provision vApps/VMs from the catalog templates/images
- Users can publish vApps/VMs to the catalog for others to use

Managing Catalogs (continued)

- Catalog templates currently available from public catalog
  - ❑ Red Hat Enterprise Linux 6
  - ❑ Red Hat Enterprise Linux 7
  - ❑ Ubuntu 12.04 LTS
  - ❑ Ubuntu 14.04
  - ❑ Windows 7 Enterprise
  - ❑ Windows 8.1 Enterprise
  - ❑ Windows Server 2008 R2 Standard
  - ❑ Windows Server 2012 R2 Standard

Managing Catalogs (continued)

Uploading templates

Supported formats:

- Open Virtualization Format (.ovf, .ova)
- CD/DVD images (.iso)
- Floppy images (.img, .vfd, .flp)
- Existing vApps in virtual data center

BCNET

Managing Networks

Types of Networks

1. External – connection to the outside world
2. Org Network -
    a) Isolated – VMs can only talk to other VMs in the same org
    b) Routed – connected to the external network through an edge appliance
    c) Direct – direct connection to the external network

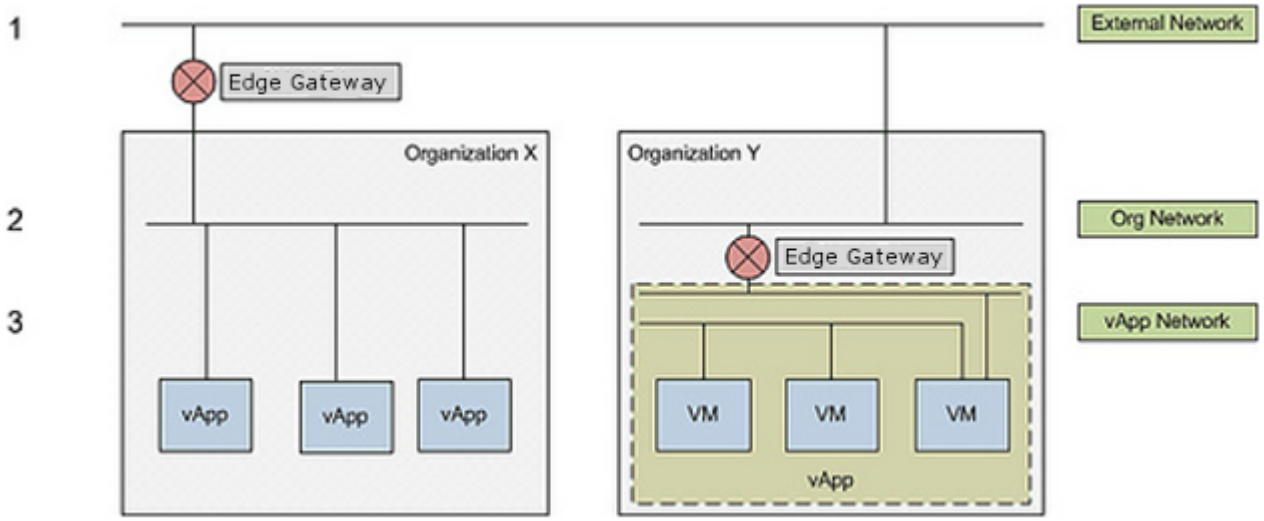
Managing Networks

Types of Networks

3. vApp Network -
    a) Isolated – VMs can only talk to other VMs in the same vApp
    b) Routed – connected to the org network through an edge appliance
    c) Direct – direct connection to the external network

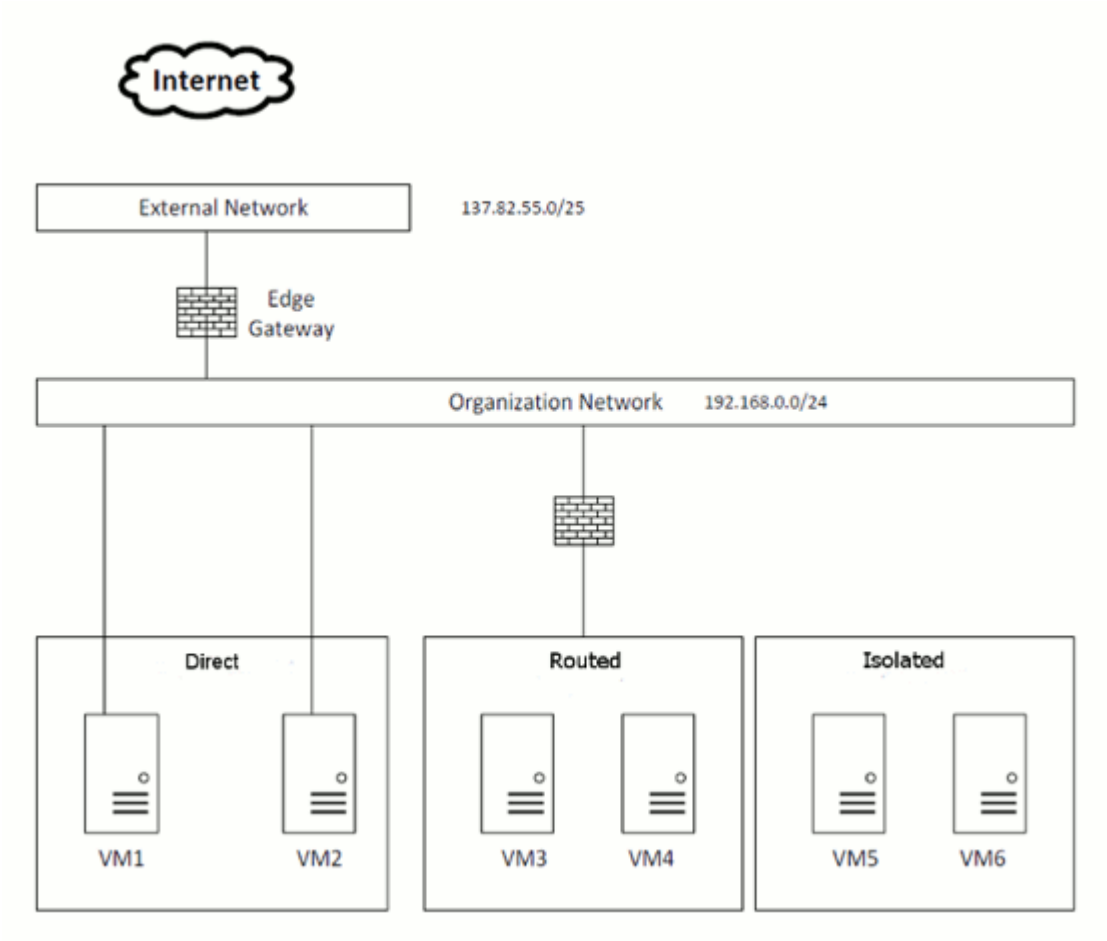
Managing Networks

Types of Networks



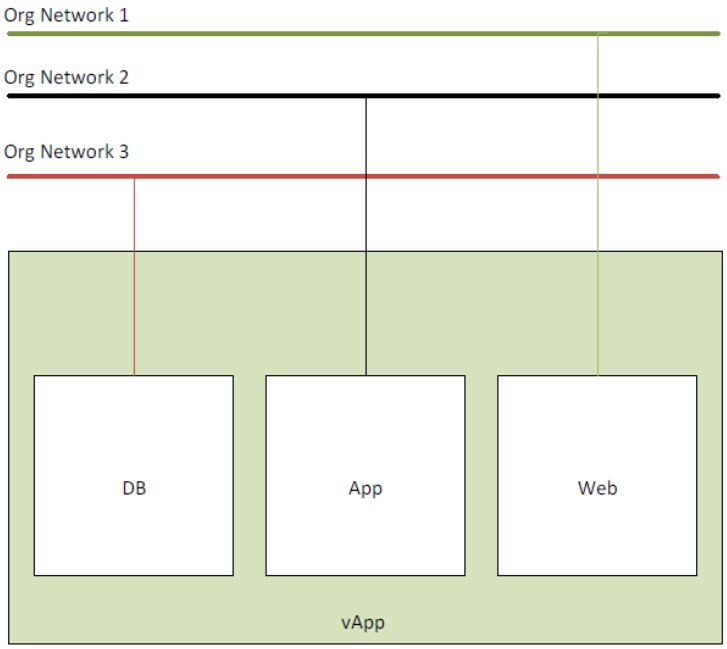
Managing Networks

vApp Networks



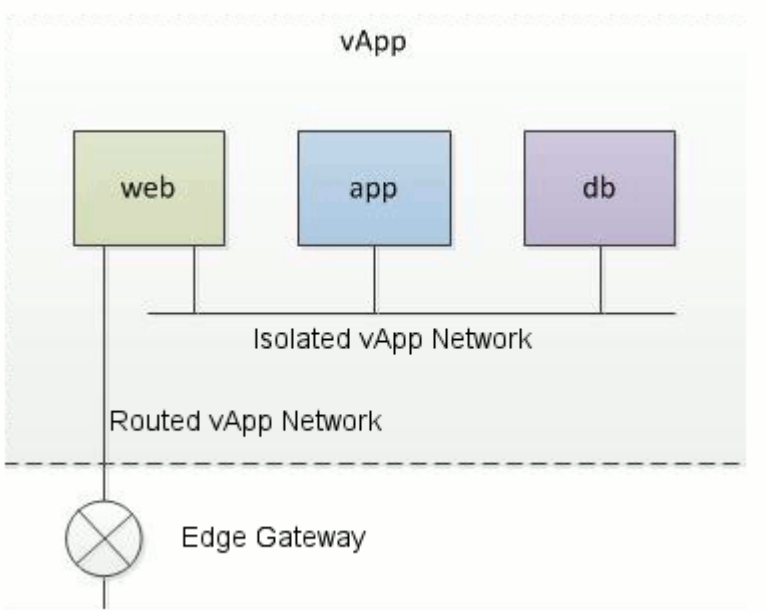
Managing Networks

Example 1



Managing Networks

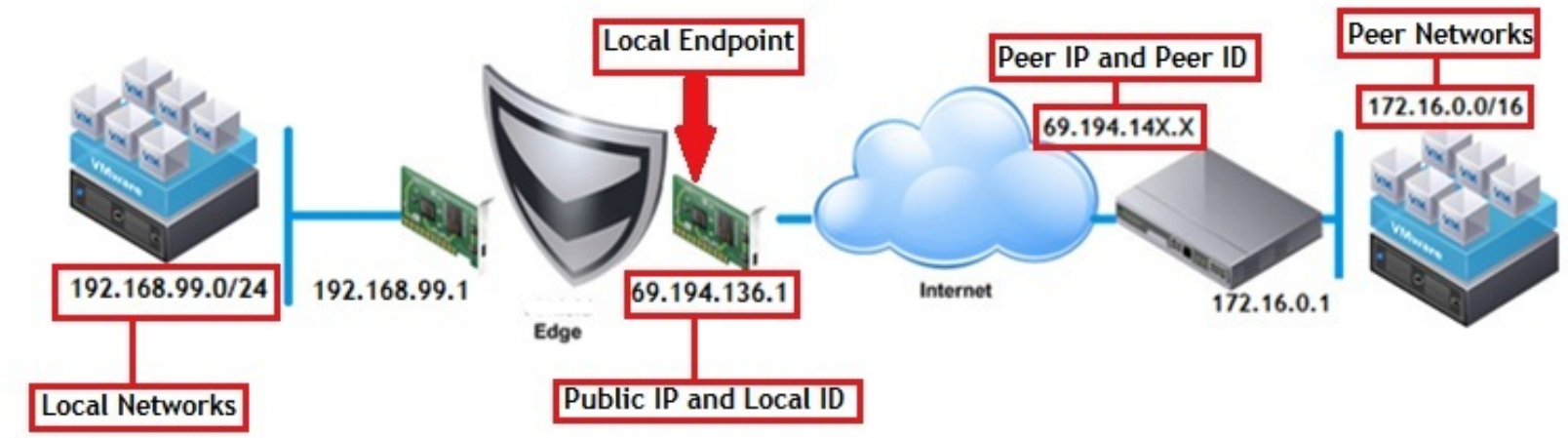
Example 2



IPSec VPN

- Establish VPN between local network and EduCloud private network
- Servers in local network can talk to EduCloud hosted VMs through the IPsec tunnel

IPSec VPN


Local Endpoint
Peer IP and Peer ID
69.194.14X.X
Peer Networks
172.16.0.0/16
192.168.99.0/24
192.168.99.1
69.194.136.1
Internet
172.16.0.1
Edge
Local Networks
Public IP and Local ID

IPSec VPN Setup

- Different vendors have different settings for their VPN devices
- Successfully deployed with Palo Alto, Cisco, Juniper
- Open firewall TCP ports 50/51, UDP ports 500/4500

BCNET

IPSec VPN Setup Resources

- http://vcloud.vmware.com/using-vcloud-air/tutorials/creating-an-ipsec-vpn
- https://kb.vmware.com/selfservice/microsites/search.do?language=en_US&cmd=displayKC&externalId=2051370

Best Practices

- Avoid special characters in VM name
- Ensure VMware Tools is installed, running, and up to date
- Supported operating systems vs. operating system guest customization support
- When provisioning VMs, start small, add more resources as needed

Troubleshooting

- Cannot power on VMs – not enough resources
- No network connectivity into or out of the virtual data centre
- Can’t login to VMs for the first time with automatically generated password

Dashboards

- VMware vRealize Operations Manager
- Monitors virtual data center
- Various dashboards displaying real time data and metrics for capacity planning and performance monitoring purposes
  - CPU
  - Memory
  - Storage
- URL: https://dashboard.educloud.ubc.ca
- suggestions

Rightsizing your Workloads

Rightsizing

- Rightsizing is process of ensuring appropriate resources are assigned to a VM to meet demand.
- Over allocating VM resources can have a negative impact on both a VM's performance and the performance, efficiency and achievable density of the underlying infrastructure.
- An ongoing process done on a regular cycle.

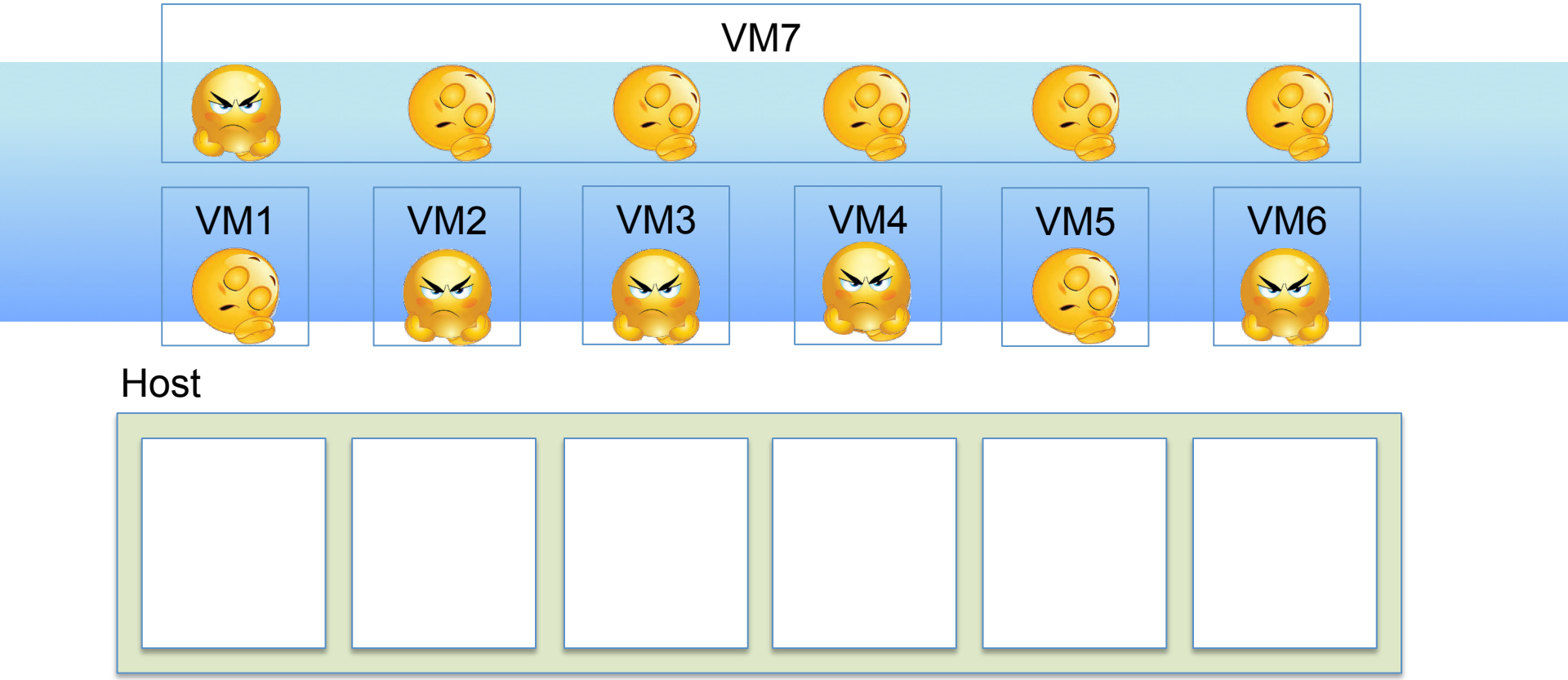
BCNET

Rightsizing

- Are all environments needed? Is it possible to maintain the application with fewer environments?
- Can infrequently used or reference only environments be powered off while not in use?
- Are there opportunities for elastic resourcing?
  - Does the service have only a few annual periods of high load?
  - Can resources be reduced (or some VM's shut down) during non-peak period?
- Are resources assigned efficiently

BCNET

CPU Resource Management



CPU Scheduling

- Large VM waits until all vCPU's can be scheduled – even if there is workload for only 1 vCPU.
- While Large VM is running, small VM's cannot be scheduled on the inactive CPU's
- Time spent waiting for scheduling is tracked as "CPU Ready" Metric.
- Even an idle VM must process clock interrupts - default is 64 times/sec (15.6ms). 1000 times/sec (1 ms) if high res timer activated.
- DRS (Distributed Resource Scheduler) may move workloads to better balance CPU demand across hosts.

CPU Sizing Guidelines

- To maximize host CPU utilization and efficiency, size number of CPU's just big enough to handle peak loads.
- Design applications for horizontal growth – Better 4 app servers with 2 vCPU than one app server with 8 vCPU.
- < 35% Average CPU busy – oversized.
- > 70% average CPU busy – undersized.

Memory Management

- Transparent Page Sharing – memory is scanned and multiple occurrences of identical pages are reduced to a single page.
- Ballooning – Mechanism to steal unallocated memory pages from one VM and assign to another. Requires VMware tools.
- Memory Compression – Page compressed before attempting page out – moved to compressed memory queue if compression > 2:1
- Swapping – Pages of virtual memory are swapped out to disk – by hypervisor (not guest OS).

Memory Management

- Memory management at hypervisor level done without any knowledge of application.
- Decisions can only be made based on how active a particular memory page has been.
- Ballooning, compression, swapping are only considered when memory demand exceeds availability.
- DRS (Distributed Resource Scheduler) may move workloads to better balance memory demands across hosts.

BCNET

Memory Sizing

- Just large enough to meet application peak demands.
- Grow in smaller increments (not powers of 2!)
- Take into account guest OS memory usage information (how much application, file system buffer, etc)
- Take into account application specific sizing requirements (e.g. java stack sizes).
- “Memory Demand” metric – indicator of memory pages being actively accessed.
- Allocated and Used metrics.

Tools

- https://dashboard.educloud.ubc.ca
- Set to retain 1 years worth of history
  Granularity – 5 minute intervals
- VMWare Document:
  VM Right-Sizing Best Practice Guide

Org Authentication/Authorization Options

- Local (default)
- VCD System LDAP Service
- Custom LDAP Service
- Federation – SAML 2.0 Identity Provider

BCNET

Local Accounts

- Organization administrator creates individual accounts and assigns them credentials/roles
- Accounts/credentials/privileges – all stored in vCloud Director database
- Groups cannot be used
- Tedious for maintaining larger number of users
- Any automation requires use of vCD API
- Can co-exist with other account types

VCD System LDAP Service

- Use the cloud provider LDAP service
  restrict to specific OU
- Not available:
  Licensing
  Configuration
  Protection of Privacy

BCNET

Custom LDAP Service

- Organization provides its own LDAP service
- Groups can be used for:
  - Granting access and assigning roles
  - Sharing vApps
- Easier to leverage existing identity & access management processes
- Design Considerations:
  - Local vs Remote, Security, Availability

Federation

- Leverage SAML 2.0 Services
  - Active Directory Federation Services
  - Shibboleth
  - Ping
  - … Many More
- Import Users/Groups
- Easier to leverage existing identity & access management processes
- Testing with Shibboleth pending

LDAP – Supported Services

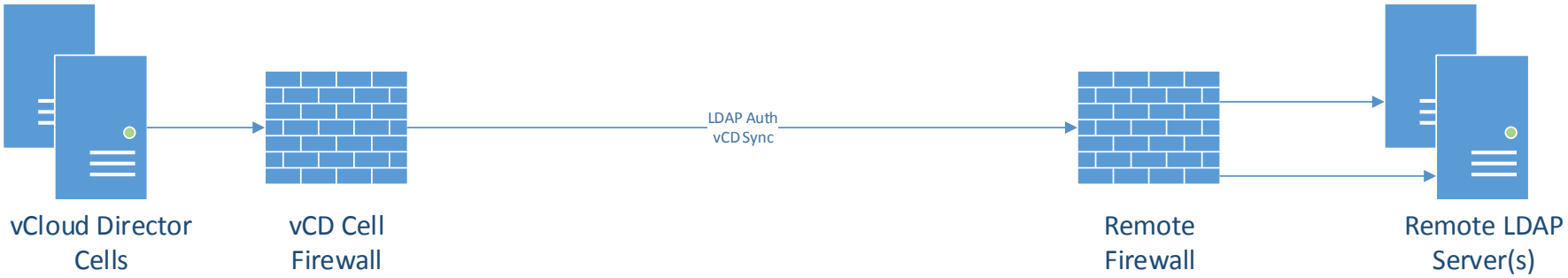
Platform	LDAP Server	Authentication Methods
Windows Server 2003	Active Directory	Simple, Simple SSL, Kerberos, Kerberos SSL
Windows Server 2008	Active Directory	Simple
Windows Server 2008 R2	Active Directory	Simple, Simple SSL, Kerberos, Kerberos SSL
Windows Server 2012	Active Directory	Simple, Simple SSL, Kerberos, Kerberos SSL
Linux	OpenLDAP	Simple, Simple SSL

Other LDAP3 servers may work (no VMWare Support).

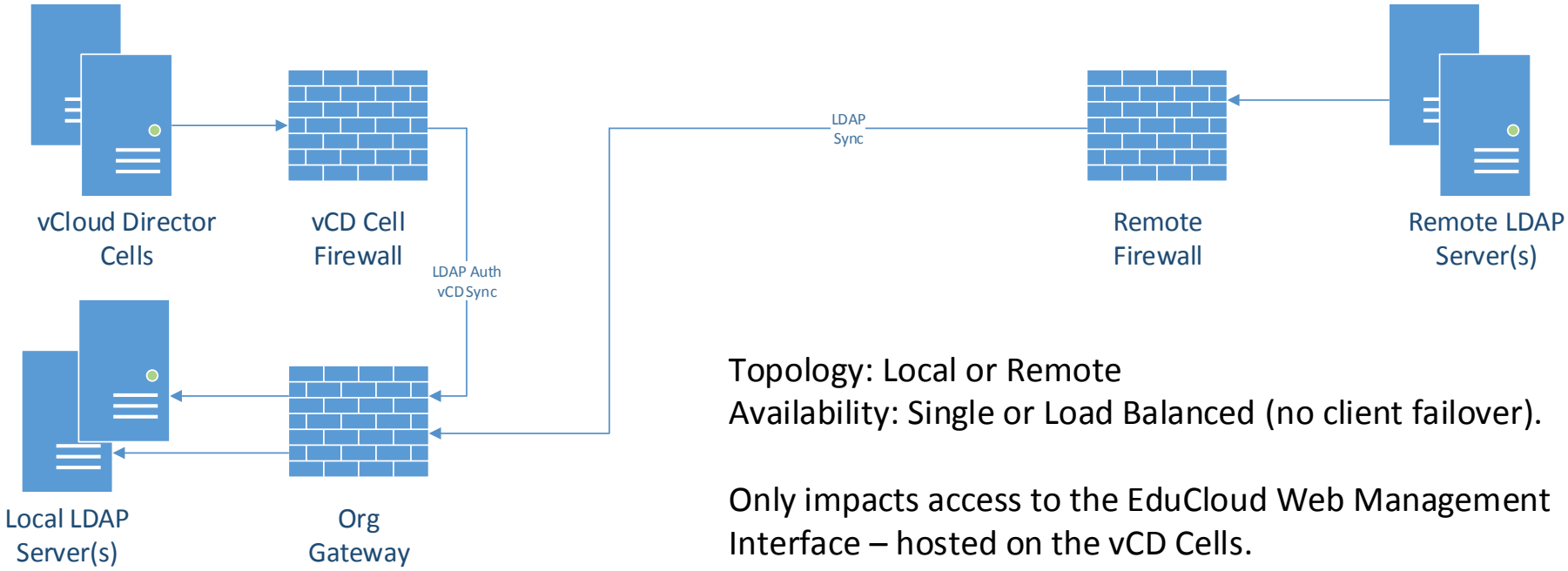
Active Directory – tested

389 Directory Server – testing in progress

Remote LDAP Server



Local LDAP Server



Topology: Local or Remote
Availability: Single or Load Balanced (no client failover).

Only impacts access to the EduCloud Web Management Interface – hosted on the vCD Cells.

LDAP – Guidelines/Restrictions

- Use encryption – LDAPS only (no StartTLS)
- Restrict LDAP access to EduCloud vCD Cells
- Supports only 1 base Dn for user and group searches. (Can impact directory design)
- Nested group membership not supported
- Avoid user name conflicts between local and LDAP accounts.
- Must be configured by EduCloud Sys Admins

LDAP – Users/Groups

- Import LDAP groups
  Assign associated EduCloud roles.
- Imported group members are allowed to log in.
  Account created automatically on first use.
- Permissions assigned based on group roles.
  If multiple roles – permissions are merged.
- Authentication/Permissions – real-time at login.
  Other attributes – synchronized nightly

LDAP – Users/Groups – Cont'd

- Accounts are moved to Lost & Found when no longer a member of a group that grants access.
- "Password Policies" (Under Settings→Policies) are also applied to LDAP accounts:
  - Enable/Disable lockout
  - Invalid logins before lockout
  - Account lockout interval (in minutes0

Roadmap – The Past

- Maintenance scheduled over the weekend of April 16-17
- Upgraded the entire EduCloud Server stack
  - vCloud Director 8.0.1
  - NSX 6.2.2
  - vCenter Server 5.5u3b
  - ESXi 5.5u3b

Roadmap – Current State

- vCloud Director 8.0.1
- Increased browser support, new client integration plugin
- Guest OS customization for windows 10
- Improved support for RHEL, CentOS
- Newer version of VMWare tools (communication will be sent out how and when to upgrade)

The Future

- Positioned well for the next releases of vCloud Director and vSphere
- Backup Storage RFP in process for new backup target
- Self-service backup and restore
- Second location – depends on funding

Feedback

- Communication
  - Was communication adequate throughout the maintenance process?
  - Are there any changes you would like to see?
- Support and Documentation
  - What kind of documentation is missing?
  - Would a different format be better?

BCNET

Questions