Designing Virtualization and Cloud Services into a High Availability, Multi-Tiered, Multi-Location Data Center

I migrated our northern data center to the cloud.

But the cloud stopped working and I can’t find the phone number for our cloud guy.

So... whatever.

You lost our data center?

That’s one way to look at it.

Brian Henry
Senior Systems Engineer
bhenry@bellarmine.edu

Mike Mattei
Professor of IT & former Dean IT and Prof Studies
mmattei@bellarmine.edu

Eric Satterly
Director of Information Technology
esatterly@bellarmine.edu
Learning Outcomes Session 10A

By the end of the session, participants will be able to:

• Explain the importance of tail-risk events that tend to be excluded from traditional DR-BC plans
• Plan for the consequences of undesirable events, not the risk of the events occurring
• Set a recovery time objective for each tier of a multi-tier strategy that is aligned with a user “tolerance” paradigm
• Select an initial processing and storage method for each location of a multi-location DR-BC strategy
• Fine tune the first pass of the “grid” to minimize technology costs within the RTO for each tier of the strategy
Some of Bellarmine’s Recent Tail-Risk Events
or just more of Murphy’s Law…

• Water line break on floor above warm data center
• Lost core switch during last afternoon of finals – two hours to restore backup switch
• Internet down five hours even w/two paths off campus
• Cigarette butt burned through fiber to key campus bldg.
• Lightning fried entire telephone switch
• Lost email for 4 days
• Wind storm – no power to campus for two days
• Ice storm – no power for five days, students sent home
• Sys Admin went home and shot wife, then …
Foundational Definitions:

- Production site – an organization’s active or primary production computing site
- Hot site – an active duplication of the organization’s live systems
- Warm site – a site with systems and communications ready to use, just need to restore data
- Cold site – a place to store data, has adequate space and infrastructure
- Mobile site – a self-contained, transportable office custom fitted with IT and communications equipment

from Government Finance Review, August 2012, pg. 53
Computing Sites at Bellarmine:

Bellarmine University - Data Center Strategy

**PRODUCTION SITE**
Brown Library Data Center

*All production systems will run in this space*
- Virtualization Hosts
- Storage Networks
- Phone System
- Firewall
- Core Network Switching

**HOT SITE**
Horrigan Hall Data Center

*Operations at this facility will be possible with the loss of the Production Data Center*
- Real-time RPO via SAN technology
- Able to run Production load at above 70% capacity
- Development and Staging hosts will run here to verify operability of the center

**WARM SITE**
Allen Hall Data Closet

*Houses the backups for campus computing, specifically backup servers will run here in proxy mode*
- Systems could be brought online to offer production computing; additional server hardware the site could be used to run more campus systems
- Management and monitoring tools will run in this location so that we have an external monitor of our computing centers

**COLD SITE**
Peak-10 Data Center

*Off-site Cloud, the purpose of this center is to house selected backup and archive data tied to very specific RPO targets.*
- This facility will not have the capacity to run systems for the university, but could be pressed into service with additional resources from the provider
Relating Computing Sites to “The Grid”:

<table>
<thead>
<tr>
<th>Local</th>
<th>Offsite</th>
<th>Local</th>
<th>Offsite</th>
</tr>
</thead>
<tbody>
<tr>
<td>Physical</td>
<td>Virtual</td>
<td>Physical</td>
<td>Virtual</td>
</tr>
<tr>
<td>Prod</td>
<td>Hot</td>
<td>Warm</td>
<td>Cold</td>
</tr>
<tr>
<td>Prod</td>
<td>Hot</td>
<td>Warm</td>
<td>Cold</td>
</tr>
<tr>
<td>Prod</td>
<td>Hot</td>
<td>Warm</td>
<td>Cold</td>
</tr>
<tr>
<td>Prod</td>
<td>Hot</td>
<td>Warm</td>
<td>Cold</td>
</tr>
<tr>
<td>Prod</td>
<td>Hot</td>
<td>Warm</td>
<td>Cold</td>
</tr>
<tr>
<td>Prod</td>
<td>Hot</td>
<td>Warm</td>
<td>Cold</td>
</tr>
</tbody>
</table>

- **Primary Data Center**: Local, Physical, Prod, Hot, Warm, Cold
- **Cloud Service Provider**: Local, Virtual, Prod, Hot, Warm, Cold
- **HOT SITE**: SECONDARY DATA CENTER, Local, Physical, Prod, Hot, Warm, Cold
- **WARM SITE**: DATA BACKUP CLOSET, Local, Virtual, Prod, Hot, Warm, Cold
- **COLD SITE**: CO-LOCATION SERVICE PROVIDER, Local, Physical, Prod, Hot, Warm, Cold
Typical (and not so typical) Disaster Recovery – Business Continuity (DR-BC) Definitions:

- **Uncertainty** – future outcomes not known or variable
- **Risk** – uncertainties with possible *undesirable outcomes*
- **Event** – a thing that happens, especially one of importance
- **RTO** – recovery time objective
- **RPO** – recovery point objective
- **Consequence** – a result or effect of an action or event
- **Tail risk event** – probability of occurrence is less than 0.03%, virtually nil (beyond three standard deviations from the mean)
Session Roadmap

- Virtualization Technologies
- Define your 10 most critical applications
- Cloud Computing and Storage Concepts
- Define your storage capacities
- Discuss strategically integrating Virtualization and Cloud for Recovery
- Define your current Computing Sites and map your applications
- Plan multi-locations under consequences arising from the various “tolerance” tiers
Key Component #1 - Virtualization
Decoupling a “system” from its native environment and transplanting it in a new ecosystem.
Virtualization... It Isn’t New

• Supercomputers have made use of virtual machines for decades – the 1960’s to be exact

• But virtualization of servers is relatively young and has RAPIDLY EVOLVED in just the last 5 years

• There are many approaches offered by many companies
What can be Virtualized?

- **Desktops**
  - VDI
  - Terminal Services
  - Desktop as a Service

- **Servers**
  - VMware
  - Microsoft Hyper-V
  - Xen

- **Storage**
  - Hitachi TagmaStore
  - IBM SVS (SAN Volume Controller)

- **Networks**
  - Virtual Network Stack
Server Virtualization

• There are several types or flavors of Server Virtualization
• Again, the technology has really matured of late
• A key piece of Server Virtualization is the…

_hypervisor_

Web definitions

In computing, a hypervisor or virtual machine monitor (VMM) is a piece of computer software, firmware or hardware that creates and runs virtual machines.

http://en.wikipedia.org/wiki/Hypervisor
Visualizing Server Virtualization
Server Virtualization

Traditional Architecture

- Application
- Application
- Application

OPERATING SYSTEM

HARDWARE

- Application
- Application
- Application

OPERATING SYSTEM

HARDWARE
Early hypervisors fooled guest operating systems into believing they were operating on real hardware rather than virtual. This ensured that early hypervisors would be compatible with operating systems that lacked virtualization awareness.

Full Virtualization

APPLICATION APPLICATION APPLICATION
Unaware
OPERATING
SYSTEM

APPLICATION APPLICATION APPLICATION
Unaware
OPERATING
SYSTEM

VIRTUALIZATION SOFTWARE

HARDWARE
Later software hypervisors provided *guest operating systems* better access to resources within the hardware, but the operating systems had to be modified to make use of the resources.
Virtualization moved into the hardware and special processors were created to handle the virtualization, this allowed modified and un-modified OS’s to work.

Combining a modified OS with Hardware Virtualization results in Hybrid-Virtualization.
Compelling Arguments for Virtualization

- **Data Center Consolidation** – Reduce the number of physical servers and decrease the footprint
- **Outlive Obsolescence** – Older systems can be upgraded based on business needs rather than out of technical necessity
- **Live Migration** – The ability to move servers from host to host allows for maintenance to be done anytime
- **Snapshots** – Take point in time images of an entire server allows for updates to be done with little risk
- **High Availability** – Combining server and storage virtualization allows for servers to survive a host level crash
Plus... It’s Getting Much Easier to Virtualize

• Software exists that allows you to convert a physical server into a virtual machine, the process is called P-to-V and it’s very common

• With Hardware Assisted Virtualization almost any OS can be virtualized since OS modifications are not necessary to run in that virtual environment

• This means that systems CAN often be virtualized WITHOUT being upgraded or redeployed
Practical Considerations with Virtualization

- As with most areas of technology, there are trade-offs to consider
Backups and Snapshots

- Snapshots provide a way to easily roll-back to the exact state of a server at the specific point in time when the snapshot was taken.
- The Virtualization layer does this by maintaining a list of the changes to the application server at the time the snapshot was taken.
- The big advantage of this is that a snapshot can be made almost instantly and without impairing the production system.
- Additionally, the time and I/O needed to create the snapshot does not increase with the size of the data set, whereas the same for a direct backup is proportional to the size of the data set.
Backups and Snapshots

• Snapshots help you avoid prospective problems with your system, but are NOT a complete backup of the system - if the base image is corrupted, ALL snapshots will be useless

• The more Snapshots you take, the more you tax your host system as the host is maintaining a base image PLUS a list of changes

• Virtualization makes these easy to do, but use them with eyes wide open
Complex “Information Systems”

• While virtualization technologies were advancing, Information Systems became much more complex

• Now these are rarely contained within a single server, but are a collection of multiple servers, storage resources, and services spread across multiple networks

• How can virtualization be leveraged to deal with complex systems?
  • By adding Network Virtualization and Storage Virtualization to the mix
Network Virtualization

• It’s moving parts of the network from physical routers and switches to software defined network components
• Allows for network boundaries to exist in your virtualized ecosystem
• Requires more host level resources to operate efficiently
Storage Virtualization

• The conglomeration of multiple storage devices and/or networks behind a unified interface, presented as a single storage unit
Virtualization Key Points

• Virtualization of large chunks of your infrastructure is possible

• Enough tools now exist that allow you more time to focus on the “Business” aspects of the technology applications and services you deliver to your community

• While the future is never certain, one trend is collapsing Server, Storage, and Networking into appliances

• As Server, Network, and Storage Virtualization continue to converge, the concept of Software Defined Data Centers becomes possible
Software Defined Data Centers

Goal of the SDDC:

“"To see everything virtualized and everything delivered as a service through automated data center management software.”

-Pat Gelsinger, VMware CEO

This is a concept that many technologists are uneasy about

As Louis C.K. famously put it…

“Everything’s amazing and nobody’s happy.”
Table Exercise - List Your 10 Most Critical Services/Apps

• Paretto – 20% services fulfill 80% user needs
• Create list from user perspective
• Select ones that generate most complaints if service/app not available to user
• Think “Services”… Don’t include low level infrastructure hardware/software
Key Component #2 - Cloud
Cloud Tools and Considerations

- What the cloud is
- What types of clouds there are
- What kind of risks are there with the cloud
What Exactly is “The Cloud?”

- Definitions of “cloud” vary
- Generally a “cloud” service is a service that makes use of hardware and software in a manner that is delivered across a network
  - Typically involves the Internet
  - Usually involves:
    - Virtualization
    - Geographic Clustering
    - Load Balancing
    - Multi-Tenancy
What Types of Clouds Are There?

- **Public**
  - Amazon, Microsoft, Google, etc.

- **Private**
  - In house solutions for infrastructure, applications, and storage

- **Community**
  - A public cloud that is utilized by multiple organizations with similar requirements
    - Usually used by government organizations and universities

- **Hybrid**
  - A system that incorporates both Public and Private cloud elements.
Cloudy Resources

• Infrastructure
  • Public: Amazon & Microsoft
  • Private: VMWare vCloud & Microsoft Hyper V

• Storage
  • Public: DropBox, Box.Net
  • Private: Many commercial SAN providers

• Applications and Services
  • Public: Lots!
  • Private: Load balanced and replicated web services, VMware Thin App, Microsoft App-V
From Silos to Clouds

- A Traditional application
- Database is Local

Connection to 10.0.0.1

Connection to 172.16.0.1

- Still Traditional
- Database is separate
  - Likely behind firewall

© Bellarmine University 2013
Breaking that out into a cloud

172.16.0.1
172.16.1.1
172.16.1.2
172.16.2.1
172.16.2.2
172.16.0.1
172.16.1.1
172.16.1.2

Connection to 10.0.0.1
Scale It Up to a Geographic Cluster

Public Cloud Overview

- Variable Costs
- Management
- Anytime, Anywhere
- Internet Dependent
- Hidden traps
Public Cloud Case Study: Practice Fusion

• Affordable Care Act has provision to incentivize health care providers to move to electronic records

• School nurse at a school finds a service that will help do it for them called Practice Fusion – for FREE

• Nurse requests uploading ALL student data to the cloud server from our student record system
Public Cloud Case Study: Practice Fusion

- IT Staff examined the terms and conditions and find lines such as:
  - “When you submit Content on our Services, you grant us and those we work with a worldwide, royalty-free right to store, host, reproduce, create derivative works of (such as translations, adaptations, reformatted versions and anonymized or de-identified versions), publish, publicly perform, display, use and distribute such Content”
Security and Stability in the Public Cloud

- Security
  - How many full time security staff do YOU have
  - How many people have access to your data?
- Shared access
Notable Cloud Outages

Some Microsoft Outage Dates:
- 9/9/2011, DNS Misconfiguration
- 2/29/2012, Leap Year Bug
- 7/26/2012, Cause unknown
- 2/11/2013, “Procedural Error”
- 2/22/2013, Expired SSL Certificate

Some Amazon Outage Dates:
- 10/5/2009, Denial of Service Attack
- 4/21/2001, Cause unknown
- 8/10/2011, Storms knock out Dublin data center
- 6/30/2012, Storms knock out Virginia data center
- 7/3/2012, Storms and generator bugs at Virginia DC
- 10/22/2012, Storms take out Virginia DC
- 12/26/2012, Cause Unknown
Costly Services

- Pricing structures for cloud services vary
- Hosting services are often based on usage
- Applications are often priced per user
Private Clouds

- Storage
- Infrastructure
- Clustered and Balanced
- Outage Preparation
- Costs
Sorting your Storage

- Network
- Replication
- Speed
  - Network
  - Nodes
  - Heads
  - Drives
Improve your Network

• Datacenter communication speeds are critical
  • By 2015 you will see more demand for 10 Gb/s!
• Single points of failure are deadly
Fix Your Single Points of Failure

• The most critical piece of a cloud deployment is to fix the network

• Anything that a Private cloud service should be designed in a N+1 setup
  • N+2, Nx2, etc. can yield more stability
  • There are naturally more costs!

• Buy Blades or Boxes?
Cluster, Balance, Webalize, and Virtualize

- Clustered and load balanced services are by design failure resistant
- Web-delivered applications are easiest to cluster and load balance
- Infrastructure Virtualization is often leveraged as part of this to speed up deployments and disaster recovery
Costs of a Private Cloud

- Hardware
- Hypervisor Licensing
- Operating system licensing
- Application licensing
- Database licensing
- Manpower
Condensation on the Cloud

• The definition of the Cloud is nebulous
• The cloud is not 100% guaranteed
• It can be significantly more costly to run on the cloud than in-house
• Cloud providers often have more resources than you do
• You may have your own private cloud.
Cloud and Virtualization Tools provide a myriad of DR options but …

What is the best way to “put the pieces together”?

Developing a Strategy
Our Initial Strategy...

• Two data centers on campus
• Locate in separate buildings
• Virtualize all physical servers and employ multiple hosts
• Utilize synchronous SAN technology
• Mirror data centers so that one takes over if the other is lost
…Had Some Holes

• If there is no true disaster but DCs lose communication with each other… which one is primary? Do we need a third DC for quorum?

• Which layer in the stack is in charge? VM, SAN, Application?

• What if errant process deletes a virtual machine or application data base?

• In an Active-Active design, how are you certain where the freshest data are so that an accurate RPO can be understood?

• What if we lose both data centers?

There has to be a better (and cheaper) way
Define your computing sites by selecting the characteristics that define the location.
Consider where your critical applications fit within each computing site.
Table Exercise

- Use the blank grids in your handouts
- Label x and y axes with your current environment
- Place top 10 apps in the appropriate cells on the grid given your current operating environment
- Assume the campus and IT services are operating normally
- Walk around and help
Suppose a bad event hits your data center and produces damage

Do you focus your efforts on how that event caused the damage or how you get back in operation?

Shouldn’t that reaction to an event inform your preparation before the event?
We Learned, Focus on Consequences not Events

Brad Brekke, vice president of Assets Protection for Target Corporation, shared some of his organization’s methods for preparing for the unpredictable.

“You can’t plan for everything. Instead, we plan for consequences. What happens if you lose communication, transportation, energy?”

Planning for consequences, as Brekke puts it, is one way of broadening the organization’s ability to respond to unlikely events.
To Begin Our Approach, First Consider Campus Operating Conditions

1. Campus is operating normally, everything appears normal to users

2. Minor event on campus. Most offices open and most classes are being held but most people can see or are impacted by some unfortunate event

3. Major event impacts campus. Everyone can see or is seriously impacted by an event that most likely has closed the campus
Factor a User Tolerance Level Into RTO Based on the Campus Operating Condition

- More tolerance generally comes from the more “spectacular” event
- The more widespread the impact will mean more tolerance
- Greater Tolerance equals more Time to Recover

<table>
<thead>
<tr>
<th>Level of Tolerance</th>
<th>Tolerance Measured In</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Minutes? Hours?</td>
</tr>
<tr>
<td>Medium</td>
<td>Hours? Days?</td>
</tr>
<tr>
<td>High</td>
<td>Days? Weeks?</td>
</tr>
</tbody>
</table>
Table Exercise - Set RTO for Each Condition

- Assume many of the top 10 services are not available to users
- Quantify campus (not IT) operating conditions to inform the Level of User Tolerance
- Set a RTO for your campus in each of the three cells below

<table>
<thead>
<tr>
<th>Campus Operating Conditions</th>
<th>Minor Disruption to Normal Campus Operation</th>
<th>Major Disruption to Normal Campus Operation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low User Tolerance</td>
<td>?? Minutes or ?? Hours</td>
<td>?? Hours or ?? Days</td>
</tr>
<tr>
<td>Medium User Tolerance</td>
<td>?? Minutes or ?? Hours</td>
<td>?? Hours or ?? Days</td>
</tr>
<tr>
<td>High User Tolerance</td>
<td>?? Minutes or ?? Hours</td>
<td>?? Hours or ?? Days</td>
</tr>
</tbody>
</table>
Design the Data Centers

• Need to design location(s) that meet the RTOs for the 10 Apps
Designing Virtualization and Cloud Services into a High Availability, Multi-Tiered, Multi-Location Data Center
Bellarmine University - Data Center Strategy

**PRODUCTION SITE**
Brown Library Data Center

All production systems will run in this space
- Virtualization Hosts
- Storage Networks
- Phone System
- Firewall
- Core Network Switching

**HOT SITE**
Horrigan Hall Data Center

Operations at this facility will be possible with the loss of the Production Data Center
Real-time RPO via SAN technology
Able to run Production load at above 70% capacity
Development and Staging hosts will run here to verify operability of the center

**WARM SITE**
Allen Hall Data Closet

Houses the backups for campus computing, specifically backup servers will run here in proxy mode
Systems could be brought online to offer production computing; additional server hardware the site could be used to run more campus systems
Management and monitoring tools will run in this location so that we have an external monitor of our computing centers

**COLD SITE**
Peak-10 Data Center

Off-site Cloud, the purpose of this center is to house selected backup and archive data tied to very specific RPO targets.
This facility will not have the capacity to run systems for the university, but could be pressed into service with additional resources from the provider
Designing Virtualization and Cloud Services into a High Availability, Multi-Tiered, Multi-Location Data Center

**Bellarmine University - Data Center Strategy**

**PRODUCTION SITE**
Brown Library Data Center

**HOT SITE**
Horrigan Hall Data Center

**WARM SITE**
Allen Hall Data Closet

**COLD SITE**
Peak-10 Data Center

Internet

Physically Diverse Paths

300 Mbps

100 Mbps
Bellarmine University - Data Center Strategy

**PRODUCTION SITE**
Brown Library Data Center

**HOT SITE**
Horrigan Hall Data Center

**WARM SITE**
Allen Hall Data Closet

**COLD SITE**
Peak-10 Data Center

Bellarmine Campus Network

- 20 Gbps
- Assorted Bandwidth
- ~25%
- ~75%

- 2 Gbps

Designing Virtualization and Cloud Services into a High Availability, Multi-Tiered, Multi-Location Data Center

© Bellarmine University 2013
Bellarmine Strategy for Low Tolerance

Scenario

This type of disaster will not be obvious to the community except in the loss of IT services.

Probably an equipment failure, misconfiguration, or logic error.

Users will have little patience given a lack of visual evidence that there is a problem.

Strategy

Manually initiated recovery to the Hot Site which is a passive data center with a replicated SAN. SAN technology allows for near real-time replication resulting is a very recent RPO.
Table Exercise:

- Put a big X through one of the cells containing a majority of your apps.
- Define one or two locations (a cell on the grid) with the characteristics circled that can handle recovery based upon the RTOs you set for the user tolerance with campus operating normally.
Bellarmine University - Data Center Strategy

**PRODUCTION SITE**
Brown Library Data Center

**HOT SITE**
Horrigan Hall Data Center

**WARM SITE**
Allen Hall Data Closet

**COLD SITE**
Peak-10 Data Center
Designing Virtualization and Cloud Services into a High Availability, Multi-Tiered, Multi-Location Data Center
Table Exercise:

• Draw a line for each app to a cell where the app can be recovered
• Label the line with the amount of time it will take to get the app running to user satisfaction
• When estimating time, consider the number of apps that must be recovered and the order of recovery
• Did you meet the RTO set in the previous exercise? If not adjust the data center processing and/or storage parameters
Bellarmine Strategy for Minor Event Tolerance

Scenario

This type of disaster will be obvious to many in the community, e.g. there will be emergency personnel, potential evacuations, etc. Probably a fire, flood, or threat; likely not technically initiated. Users will have some patience as they will likely be focused on gathering information about the event over completing their work.

Strategy

Maintain a Cold Site that will provide a recovery location. Assume that some parts of one of the campus data centers can be gathered and taken to the Cold Site.
Bellarmine Strategy for Major Event Tolerance

Scenario
This type of disaster will be blatantly obvious to the community. Probably a wide scale “Act of God” type disaster large amounts of the school are rendered inoperable. All operations are impaired. Users will have a great deal of patience and will mainly be focused on wanting information.

Strategy
Cold site recovery strategy is the preferred approach, but if that is not possible rebuilding infrastructure in the Cloud would be the approach.
Table Exercise for Minor/Major Event Tolerance

• Select a clean sheet for this exercise
• Label production location and hot/warm location
• Place the top 10 apps in the appropriate cells
• Test: place a big X on 2-3 cells that contain most of the apps
• Draw lines to cells that will restore each lost app
• Label the lines in priority order with the RTO
• Evaluate the ability of the design and adjust until the design is aligned with user expectations (tolerance)
In Conclusion

• There is no “Right” answer
• Rapid changes in technology make for many options in the recovery space
• When developing your strategy, think consequences and not events and probabilities.
• Consider user perception and tolerance and set appropriate RTOs
• There will always be new tools and technologies, so implement a process that allows for testing, evaluation and adaptation of your strategy
• Walk before you run, start with one location-tier combination and evolve to meet the needs of your campus
Thank You for a Great Morning

Follow-up questions and comments, please email:

Technical or operational issues: bhenry@bellarmine.edu
Tactical or implementation issues: esatterly@bellarmine.edu
Strategic or philosophical issues: mmattei@bellarmine.edu