How to Achieve Agility and Redundancy in the Hybrid Cloud
Speakers

Bryan Bond
SR System Admin
eMeter, A Siemens Business
@VMJEDI

Pat O’Day
Chief Technology Officer
Bluelock
Terms/Definitions

- RaaS
- BaaS
- RTO
- RPO
- Application
- Declaration
- The Plan
Traditional Disaster Recovery

**Primary Location**

Very expensive use of capital and human resources

**Recovery Location**

New Approach

**Primary Location**

Pay only for storage & replication

**Recovery Location**
Which approach is best for me?

- Driving factors:
- RTO/RPO requirements
- BW availability/cost
- How much am I protecting?
- What am I protecting against?
- Need for a third site if primary or secondary unavailable for long periods
RTO/RPO Requirements

• How long can the application be unavailable?

• How much data can be lost in the recovery window?

• Will there be a performance impact in the recovery site?
Bandwidth/Throughput considerations

- How big will the pipe need to be?
- Secure Tunnel/PtoP
- How will outage affect BW and access
How much am I protecting?

- Total data set size at rest
- Rate of Change
- Replication time for ROC
- (RTO/RPO)
- What systems/application are actually critical?
What am I protecting against?

- People
- Connectivity
- Power
- Physical location
- (Fire, Flood, Earthquake)
Need for a 3rd site?

- If my primary or Secondary location is offline for XXX, what will I do?
- Effort level to secure new site
- Will my solution support Multipoint?
- Can I move from site to site easily?
Hybrid solution

- RaaS and BaaS blended approach
- Plan from back to front:
  - What will I need to bring this application online?
  - What infrastructure do I need in place prior to a failure?
- (AD, DNS, SMTP, Monitoring, etc.)
Hybrid solution

• Define protection levels
• Come up with a number then throw out all but 4
  • 1= No one cares
  • 2= Probably unique data, but not important/critical to daily business operation
  • 3= important/unique data but availability not critical
  • 4= we loose money every minute this is down
Hybrid solution

• **1= No one cares**
  - Maybe storage based snapshots for convenience, definitely not copied off site

• **2= Probably unique data, but not important/critical to daily business operation**
  - Storage based snapshots, array based replication, offsite BaaS.
  - Less RTO less RPO
Hybrid solution

- **3= important/unique data but availability not critical**
  - Test data, Non critical/time sensitive business data, Data warehousing
  - Storage based backups
  - Array based replication
  - Offsite Backup (BaaS)
- **4= we loose money every minute this is down**
  - Source code, customer data, archives, etc.
  - Storage based backups
How do I do it?

- Look for solutions that meld with current technologies in place
- Look for partners that understand your needs and can adapt to them rather than forcing you into a mold
- Avoid large upfront investments
- Leverage backend solutions wherever possible (array based replication, tools)
Planning phase

• Do I have all the pieces I need?
• Test to find out
• Keep all protection levels separate, no mixing of types
• Develop the run book as you proceed through the planning phase
• Test, test, test, test
Declaration time

• Who can make a failover declaration?
• What are the declaration parameter?
• How long do I have before I have to make a declaration?
• “I concur”
• “Hold on to your butts”
Post declaration/failback

- Test failback
- May need a separate run book, not just go backward through the list.
- How long can I operate in recovery site?
- How long to reseed in reverse?
- RTO/RPO expectations on failback
Montgomery Scott method of engineering

- Do NOT promise what you MIGHT be able to do
- Promise in writing what you are 100% capable of doing
- If you are 75% confident, maybe mention this at time of declaration (reduced RTO/RPO from SLA, etc.)
- If you are below 75%, keep it to yourself.
- Surprise them with more than you promised.
Key items

• Get RTO/PRO defined based on actually ability to perform
• Fight to keep applications/systems off the top tier of protection
• Get buy in from the top down on all aspects
• Keep run book complete and up to date after each test