Education

Cloud Backup Recovery and Restore Requirements

Ashar Baig, Asigra
Chairman, SNIA Cloud Backup Recovery and Restore (BURR) Special Interest Group (SIG)

SNIA Legal Notice

- The material contained in this tutorial is copyrighted by the SNIA unless otherwise noted.
- Member companies and individual members may use this material in presentations and literature under the following conditions:
  - Any slide or slides used must be reproduced in their entirety without modification
  - The SNIA must be acknowledged as the source of any material used in the body of any document containing material from these presentations.
- This presentation is a project of the SNIA Education Committee.
- Neither the author nor the presenter is an attorney and nothing in this presentation is intended to be, or should be construed as legal advice or an opinion of counsel. If you need legal advice or a legal opinion please contact your attorney.
- The information presented herein represents the author's personal opinion and current understanding of the relevant issues involved. The author, the presenter, and the SNIA do not assume any responsibility or liability for damages arising out of any reliance on or use of this information.

NO WARRANTIES, EXPRESS OR IMPLIED. USE AT YOUR OWN RISK.

Agenda

- What is Cloud Backup Recovery and Restore (BURR)?
- Cloud BURR Definition
- Cloud BURR Benefits
- Cloud BURR Standards
- Summary

What is Cloud BURR?

What is Cloud BURR?

- Cloud BURR (Backup Recovery & Restore) involves backing up data offsite to a data centre (Organization's central data center or Service Provider's data center), over a WAN, using standard internet protocols
- Hardware infrastructure is shared by the provider's "customers"
  - Increased efficiencies
  - Reduced costs due to syndication and sharing
- Cloud BURR is an inexpensive and flexible way of accessing storage on an as needed basis that's highly available and secure i.e. elastic capacity.

How can I utilize Cloud BURR?

1. **Public Cloud** – requires organizations to leverage 3rd party infrastructure for their BURR needs
2. **Hybrid Cloud** – requires organizations to leverage a combination of in-house and 3rd party infrastructure for their BURR needs
3. **Private Cloud** – requires organizations to leverage in-house infrastructure for their BURR needs

Cloud BURR Characteristics.

- Multi-tenant
- Shared infrastructure
- User transparency
  - Incredibly easy to use
- Scalable & resource elastic
  - Flexible resources-on-demand
- Pay-as-you-go cost-effective pricing - IaaS
- Accessible as a loosely-coupled service
- Economies of scale
- Private, Hybrid and/or Private / Off-Premise

SNIA's Cloud BURR Definition.

- Service-Based
  - BURR application hosted & operated at a central location
  - SP manages the BURR application, hardware, resources & security settings
  - End users can fine tune SLAs, policies, business rules, & access control
- Ubiquitous Access
  - Standard networking protocols to transfer data between customer & SP sites
  - Subscribers can backup data to any location that can access the service
- Scalable and Elastic
  - Hardware resources available to subscribers on-demand
- Metered by Use
  - Utility-based cost model – hardware resource usage can be monitored, controlled & reported
- Shared and Secure
  - Data and configuration are kept virtually separate in a scalable, shared infrastructure
  - Data mobility/portability between cloud repositories

Cloud BURR – Optimized For.

- Economies of scale through on-demand and elastic infrastructure
- Utility pricing
- Consumption tracking, monitoring & reporting
- Secure – e.g. SAS 70 audited, encrypted, FIPS 140-2 certified, etc.
- MSP Focus and expertise
- Flexibility – OPEX Vs. CAPEX

Cloud BURR – User Requirements.

- Be non disruptive
- Provide granularity for RPOs
- Provide granularity for RTOs
- Provide fast recoveries locally
- Provide fast off-site recoveries – Disaster Recovery
- Policy and/schedule driven
- Automated – little or no human intervention
- Not application disruptive – no scheduled downtime
- No lock-in
- Data mobility / data portability

Cloud BURR – Requirements. (Cont' d.)

- Cost less
- Secure
  - Data must be encrypted at all times – FIPS 140-2
  - Designed for multi-tenant environments
- Less complex to install, manage and deploy
- Reduce operational expenditures
- Protect servers, desktops and laptops – on the LAN & mobile
- Expand resources & capabilities elastically, cost-effectively
  - Backup virtualized & physical environments
  - Support of Public, Private, Hybrid clouds

Typical Cloud BURR User Errors.

- Focus on backup and not recovery
  - No Recovery and Restore Assurance (R2A)
- Limited resources to manage data backups & recoveries
- Finite (Private Cloud) vs. infinite (Public Cloud) storage resources
- No storage tiering
- Using technology that was not designed for the cloud era
- Treat all backups the same – old vs. new data

Who is Protecting Your Data?

- Often delegated to junior or entry level personnel
  - Lack data protection knowledge or experience
  - Experienced IT personnel rarely volunteer for this job
- Self fulfilling prophecy
  - Thankless job
  - High failure rate makes responsibility unpopular
  - Experienced personnel avoid like the plague
  - Inexperienced personnel more likely to make mistakes
    - Increases probability of failures

Cloud BURR Future Challenges.

- Slow adoption of:
  - Cloud BURR standards
  - Pay-per-use business model of the Public Cloud / SaaS business model of the Public Cloud
- Security concerns
- Lack of demonstrated cost advantage
- Price

Today only about 5 - 15% of businesses have turned to Public Cloud Computing.
James Staten, VP, Principal Analyst, Forrester Research.

Most of these challenges can be mitigated by standards, price and end-user education

Problems Cloud BURR Solves?

Urgent End User BURR Problems.

- Failed recoveries and restores
  - No recovery assurance
  - Highly limited testing
- Recoveries and Restores are difficult and time consuming
- Increased liability
  - Fines for non-compliance from regulatory authorities
  - Job security
  - Fiduciary risk

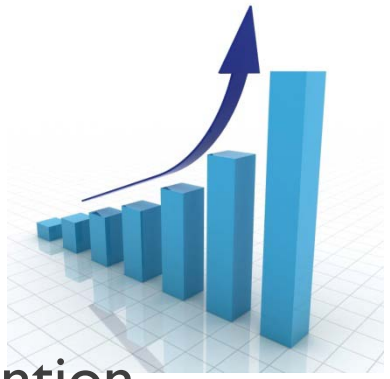
- Backup is the means to an end but not the end
- The worst time to find out that you cannot recover your data is when you have to recover your data

Important End User BURR Problems.

- Backups & Restores are Manually intensive
  - Missed backup windows, compliance
  - Difficult to add, operate, manage, upgrade, fix, etc.
- Highly application disruptive
- Escalating burden & costs
  - Infrastructure, storage, admins, bigger RPOs, much longer RTOs
  - Multiple point systems with no integration
  - Soaring pressure, plummeting morale
  - Protecting the data of mobile workforce

Market Conditions Exacerbating Cloud BURR Problems.

- Data growth – Too much data, too little time
- High dependence on digital content
  - Downtime and data loss tolerance is low
- Compliance & security requirements
  - Uncompromising demands for privacy and retention
  - eDiscovery
  - Off-premise copies to aid Disaster Recovery (DR)
- Economic downturn and recovery impacting headcount
  - Limited resources to manage it all



30x increase in storage requirements over the next decade.

How Cloud BURR Addresses Today's BURR Problems.

- Restores and recoveries are always urgent
- Cloud BURR offers quick & efficient Recovery and Restore Assurance (R2A)
  - Reduces fiduciary risk and liability
- Off-premises copies aid Disaster Recovery (DR) significantly reduces organisational risk, exposure and storage infrastructure costs
- Offers an incredibly broad range of granularity that goes from very fine grain with continuous data protection (captures every write file/message/email-level backup/restore), to very coarse grain daily backups

Cloud BURR Benefits

Cloud BURR Benefits
For Cloud Service Providers

- Magnification of MSPs size and scope
- Operational efficiencies
  - Economic downturn, forcing organizations to entertain ITaaS
- Bigger reward
  - MSPs can acquire new Cloud BURR-based recurring revenue with little effort
- Low or few barriers to entry
- Fewer capital expenditures to purchase/build storage vault
  - Store customer backed up data in the public cloud – minimal capital investment

Cloud BURR Benefits
For End Users

- Peace of mind via Service Provider SLAs
- Ease-of-use, interoperability and flexibility of the data protection strategy
- Security – Multi-layered security is provided by the technology and by the public cloud providers
- Reduced downtimes
- Improved RTOs and RPOs
- Cost savings
- Increased focus on their core business

Cloud BURR can make a significant difference to an organization's IT performance, human productivity and cost savings

Refer to the Hands-On Lab

Hands-On LAB COMPUTERWORLD SNIA SNW

Check out the Hands-On Lab:

Cloud Storage

Q&A / Feedback

- Please send any questions or comments on this presentation to SNIA: trackcloudtechnologies@snia.org

Many thanks to the following individuals for their contributions to this tutorial.

- SNIA Education Committee

Ashar Baig

Download SNIA CSI's Private and Hybrid storage clouds whitepaper at
http://www.snia.org/forums/csi/Private-HybridCloudWhitePaper.pdf

http://snia.org/cloud

http://snia-europe.org/cloud

Don't forget to Join/visit the Cloud Backup LinkedIn Group

THANK YOU!