Cloud Backup

November 2, 2017
New Service Template: Cloud Backup

Purpose / Objective:

As an increasing number of HUIT and customer-managed workloads move to cloud (IaaS) providers, the need for a cloud backup solution that replicates on-premises features is acute. The Cloud Backup offering in Cloud Services is an evolution of the HUIT Backup Service that extends data protection services to AWS-hosted workloads – reducing costs, increasing flexibility, and improving recoverability.

Users:
ITS DevOps and AWS instance owners requiring backup services

Value / Benefits:

• Features – Point-in-time backups, AMI management, tag propagation, tag based management, central backup visibility, flexible backup/recovery options, DR copy, RDS, Aurora, Redshift support, and "The Freezer"

• Encrypted - All access to the CPM tool is encrypted and all AWS accounts credentials are encrypted at rest.

• Resilient - Cloud Backup utilizes secure cloud based storage (AWS S3) for lower cost and improved durability.

• Flexible - Customer-defined backup schedules and retention policies may be defined if standard offerings are insufficient.

• AWS native services - Backup/Recovery of AWS instances using standard AWS services
New Service Template: Cloud Backup

Service offering will provide:
- Support for CPM tool, including operations and maintenance
- Standard policy and tagging management
- Monitoring of CPM performance
- Flexibility to match data protection to information value
- Training and other knowledge artifacts to support users

Offering Owner: Ron Hawkins / David LaPorte

Provider Group: ITS – Data Center Operations & Production Control

Support Model:
- Tier 1: Data Center Operations & Production Control
- Tier 2: ITS Platform team
- Tier 3: Vendor

Dependencies: AWS computation (EC2), storage (S3), and connectivity (DirectConnect) services and Cloud Protection Manager
Appendix
Business Analysis: Process Overview

- Validate the problem statement (slide 6)
- Identify stakeholders and potential users (slide 7)
- Gather information on current state, process(es), and context (e.g., organizational, financial) (slide 8)
- Interview stakeholders and users to understand priorities, criteria, challenges, and desired outcomes (slides 9-11)
- Determine scope of problem to address (slide 12)
- Evaluate possible solutions (slide 13)
- Conduct financial analysis (e.g., who pays/who’s willing to pay) (slide 14)
- Assess whether HUIT should and could provide a solution (slide 15)
Business Analysis: Problem Statement

The current HUIT cloud backup solution is a fragmented set of legacy and home-grown tools that lack scalability and result in unnecessary complexity.

The new Cloud Backup Offering using the CPM tool will be:

- More cost-effective
- Able to provide basic self-service functionality as well as white-glove support options
- Resilient, scalable, and flexible
- Easier to manage
- Reliant on standard AWS services
## Business Analysis: Stakeholders and Users

<table>
<thead>
<tr>
<th>Stakeholder/User</th>
<th>Reason for Inclusion</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology &amp; Security Cloud Strategy Workgroup</td>
<td>Develops plans, standards, and technology best practices to guide the cloud migration, incorporate Enterprise Architecture processes into the definition of standards, and work closely with existing Security governance structures.</td>
</tr>
<tr>
<td>ITS DevOps group</td>
<td>Understands end user and customer requirements, and are key advisors on infrastructure decisions and dependencies of cloud resources.</td>
</tr>
<tr>
<td>HUIT managed accounts</td>
<td>Current HUIT and non-HUIT cloud application owners and managers.</td>
</tr>
</tbody>
</table>
Business Analysis: Current State, Processes and Context

Current solution is a fragmented set of legacy and home-grown tools including:

• EMC Networker
• AMI Management Tool (AMT)
• Adhoc backup scripts
## Business Analysis: Requirements – MVP

### Standards: Does the tool comply with current HUIT and Cloud standards, processes, and/or practices?

- Facilitate HUIT service level guarantees
- Leverage existing HUIT Tools (e.g., Splunk, Nagios)
- Integrate with IAM and Security polices and standards (phase 2)
- Implement Cloud standards for tagging
- Elastic solution for future needs (i.e., more apps)
- Implement HUIT standards for governance (i.e., controls and auditing)

### Cloud Backups: Does the tool create backups?

- Backup based on schedule or time event
- Backup on-demand
- Automated AMI Creation
- AMI Retention
- Associate AMI to the application and environment
- Automated EBS Snapshot Creation Encrypted and Unencrypted
- EBS Snapshot Retention
- Unlimited storage of backup artifacts
- Associate snapshot to the application and environment
- Backup activity logs
- Backup notifications
## Business Analysis: Requirements – MVP

### Cloud Recovery: Does the tool facilitate recovery of instances?
- Recovery of entire application to last backed up state
- Recovery using AMIs
- Recovery for self healing
- Recovery using EBS snapshots
- Associate recovery to the application and environment
- Recovery notifications
- Recovery logs
- Automated via scripting

### Configuration and Management: How do we configure and administrate the tool?
- Configuration Driven Management
- Support for multiple AWS accounts and multiple environments in an AWS Account
- Control number of backups
- Control retention for backups
- Control who gets notified of activity
- Configuration UI tool
## Business Analysis: Requirements – MVP

### Operational Support: What features and information will allow us to effectively and efficiently use the platform?

- Unlimited support for users, AWS accounts, instances (dependent on licensing agreement)
- Easy to setup and install
- Easy to scale and handle high volume of simultaneous requests for processing
- Documentation or runbook on how to configure
- Highly available

### Technical Support: When we need help, advise, a fix, or a new feature, what should we do and who can we contact?

- Documentation
- Dedicated Team of Experts
- Availability of Tool Updates and Patches
- Responsive Release Cycle
- Notifications
Business Analysis: Determine Scope

- Support for CPM tool, including operations and maintenance
- Standard policy and tagging management
- CPM performance monitoring
- Best practices and standards for managing storage costs
- Training and other knowledge artifacts to support users
- HarvardKey integration (phase 2)
- Service available to HUIT and Schools
Business Analysis: Evaluate Solutions

The following products were evaluated:

• Cloud Protection Manager - CPM (selected)
• CloudBerry
• Cloudian
• CommVault
• Ctera
• Dell EMC Networker
• Druva
• Skeddly
• Veeam
Business Analysis: Financial Model

Cost Model: In progress

- Per-instance CPM license cost (~$33)
- Pass-through S3 costs (variable)
- Human resources (0.5 FTE)
Does It Qualify as a New Service?

A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs or risks. ITIL v3, Service Design

An IT Service exhibits the following characteristics:

• Fulfills one or more needs of the customer ✔
• Supports the customer’s business objectives ✔
• Is perceived by the customer as a coherent whole or consumable product ✔

When trying to determine whether an offering is a service, consider the following:

• If someone can request and purchase it, it is probably a service.
• If it can be viewed as an add-on or an option of a service, it should be considered a part of that service and not a service of its own
• Applications, themselves, are not services. They enable services that may be provided by someone else.
## Evaluating a Potential New Service: Backup

### Strategy
- Ongoing customer outreach to understand and define cloud backup requirements
- Iterative approach given current gap in operational requirements vs state of art
- Define rollout strategy
- Pilot service launch

### Future State
- Deploy cloud backup solution to address immediate needs for simplicity and scalability in support of migration efforts
- Continue to evaluate marketplace for holistic (e.g., on-premises and cloud-native) replacement solutions

### Current State
- Inconsistent approaches to cloud backup under development
- Lack of self-service and automation
- Intensive resourcing driven by complexity
- Perceived as high cost
- Current cloud backup approach has on-premises dependency and lacks cloud-native features

### Gaps
- Cloud backup market is immature
- Native cloud provider-based solutions lack enterprise-class features
- Re-establishing customer value proposition
### Proposed Service Definition

**Purpose / Objective:** The Cloud Backup offering in Cloud Services is an evolution of the HUIT Backup Service that extends data protection services to AWS-hosted workloads – reducing costs, increasing flexibility, and improving recoverability.

**Users:** HUIT, Harvard University schools, departments, and affiliates with assets on the cloud

**Value / Benefits:**

- Cloud Backup provides customer defined backup scheduling of point-in-time, crash-consistent snapshots of instance data. These snapshots may be recovered on-demand by customers.
- Incremental - Only instance data that has changed is backed up, reducing storage requirements and cost.
- Encrypted - All access to the CPM tool is encrypted and all AWS accounts credentials are encrypted at rest.
- Resilient - Cloud Backup utilizes secure cloud based storage (AWS S3) for and lower cost and improved durability.
- Flexible - Customer-defined backup schedules and retention policies may be defined if defaults are insufficient.

**Self-service**

- Define own policies and schedules (pending HarvardKey integration)

**Managed**

- Support for CPM tool, including operations and maintenance
- Standard policy and tagging management
- Monitor CPM performance
- Best practices and standards for managing storage costs
- Training and other knowledge artifacts to support users
Proposed Service Definition (cont.)

Service Owner: Ron Hawkins and David LaPorte

Provider Group: Infrastructure Technology Services

Service Support
- Tier 1: Data Center Operations & Production Control
- Tier 2: ITS Platform team
- Tier 3: Vendor

On-call and Escalations:
- After-hours coverage: standard on-call procedure

End User Communications:
- Proactive consultative engagement
- Self-service reporting
- Automated Notification/Alerts

Service Dependencies:
- “One-Down” Services this Service depends on
  - Cloud providers – AWS computation (EC2), storage (S3), and connectivity (DirectConnect) services and Cloud Protection Manager
- “One-Up” Services that depend on this Client Service
  - HUIT service providers, Non-HUIT service providers
## Service Design Partners

<table>
<thead>
<tr>
<th>Design Partner</th>
<th>Why them? What do you need from them?</th>
<th>Engagement Approach</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology &amp; Security Cloud Strategy Workgroup</td>
<td>The Technology and Security Workgroup will develop plans, standards, and technology best practices to guide the cloud migration, incorporate Enterprise Architecture processes into the definition of standards, and work closely with existing Security governance structures.</td>
<td>Meet regularly to review progress, identify issues, and provide consultation.</td>
</tr>
<tr>
<td>ITS DevOps</td>
<td>ITS DevOps understand end user and customer requirements, and are key advisors on infrastructure decisions and dependencies of cloud resources.</td>
<td>Continuous engagement through participation in meetings, product reviews, and CPM pilot, provide feedback to approach.</td>
</tr>
<tr>
<td>Services Workgroup</td>
<td>The Services Workgroup helps develop a comprehensive strategy and plan to introduce new cloud services to the Harvard Community in support of a cohesive, University-wide cloud presence. The Workgroup will create service definitions, define a simple request/fulfillment processes, determine timelines for new and deprecating services, and articulate processes for service approval and exceptions.</td>
<td>Meet regularly to review progress, identify issues, and provide consultation.</td>
</tr>
</tbody>
</table>
Establish Financial Models

We are working with finance on HUIT billing model but moving towards an annual per instance backup service fee which will include cost of license, AWS CPM instance, and overhead.
Document Service Delivery

Timeline for service Development and Launch

- Phase 1 – CPM implementation – October 2017
- Phase 2 – Service preparation, design, and roll-out to pilot users – October to November 2017
- Phase 3 – General HUIT roll-out – December 2017
- Phase 4 – Expanded Roll-out to University – FY Q3

Available to

- HUIT, Harvard University schools, departments, and affiliates with assets on the cloud

Requirements and Limitations

- AWS-based workloads may make use of the Cloud Backup services, workloads located on-premises and at other cloud providers are not eligible.
- Self-service access to the CPM tool assumes basic familiarity with the tool and the vendor-provided documentation
- Customer must provide the CPM tool with access to the appropriate AWS account using a role definition provided upon initial service request.
- Customer is responsible for defining backup scheduling and is responsible for any AWS storage charges that result from those business decisions.
- Windows may require installation of an agent to realize more advanced features, specifically application quiescence.

Policies regarding Use of Service

- Data protected and retained by Cloud Backup services in accordance with data classification level.

Potential Risks

- TBD
Document Service Delivery

**Service Team**
The Service Team is accountable for service operations. Responsible for strategy and development of services-functional group of HUIT members that can provide subject matter expertise to the Service Owner.

<table>
<thead>
<tr>
<th>Functional Team</th>
<th>Individual</th>
<th>Area of Expertise</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Desk</td>
<td>N/A</td>
<td>Intake of incidents relating to service. Troubleshooting according to standard Troubleshooting Guide knowledge</td>
</tr>
<tr>
<td>Application Team</td>
<td>Data Center Operations &amp; Production Control ITS Platform Services</td>
<td>In-depth service and technical knowledge, incident and problem resolution. Escalation to Service Owners.</td>
</tr>
<tr>
<td>Service Delivery Managers</td>
<td>Dave LaPorte Ron Hawkins</td>
<td>Accountable for service operations. Responsible for strategy and development of service.</td>
</tr>
</tbody>
</table>
Document Service Delivery

Service Requests

• Customer submits ServiceNow ticket to Data Center Operations & Production Control team

Knowledge

• Vendor-provided documentation: https://n2ws.com/documentation/cpm-user-guide

• ServiceNow knowledgebase to be updated with frequently asked questions and commonly experienced issues

Major Incidents

• Major Incident – any system on which the service is dependent (CPM, AWS)

• Upon discovery of an incident, on-call personnel are to be notified immediately and by phone call to 844-HUITNOC (844-484-8662) and by email to noconcall@harvard.edu. On-call person will assume responsibility for sending relevant notifications, and as primary point of contact for Customer, ITSM, and Client Services. On-call person will initiate a conference bridge when circumstances require. Incident responder must update ITSM on thirty minute intervals, at a minimum. Incident responder must update noconcall@harvard.edu with a firm “all clear” when the incident is resolved. Incident responder is responsible for performing any post-incident review activities, as required by the HUIT Incident & Problem management protocols.

• Customers alerted through same notification process as dependent system notification.
Document Service Delivery

Technology and Vendors used for Service Delivery

• Service provided using the N2WS Cloud Protection Manager (CPM) tool.

Service Dependencies

• “One-Down” Services this Service depends on
  – Cloud providers – AWS computation (EC2), storage (S3), and connectivity (DirectConnect) services and Cloud Protection Manager

• “One-Up” Services that depend on this Client Service
  – HUIT service providers, Non-HUIT service providers

Service Level Agreements

• Service expected to support per-instance backup scheduling and restoration of files or entire instances.

Underpinning Contracts

• A two year subscription to the N2WS Cloud tool has been purchased.
Document Service Delivery

Metrics

<table>
<thead>
<tr>
<th>KPI</th>
<th>Target</th>
<th>How Measured</th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability</td>
<td>December 2017</td>
<td>Cloud Backup Services available to HUIT DevOps team</td>
</tr>
<tr>
<td>Mean time to resolve Incidents</td>
<td>Within 1 Business day</td>
<td>Days to resolution</td>
</tr>
<tr>
<td>Time to fulfill request</td>
<td>Within 2 Business day</td>
<td>Time to close request ticket</td>
</tr>
<tr>
<td>Customer satisfaction survey</td>
<td>95% “Satisfied” or better rating</td>
<td>Customer relationship management records</td>
</tr>
</tbody>
</table>
Service Design Checklist: Part 1

Service Attributes

- Description ✔
- Key Features and Benefits ✔
- Offerings ✔
- New or Replacement? ✔
- Service Stakeholders ✔
- Available to ✔
- Requirements and Limitations ✔
- Policies regarding Use of Service ✔
- Compliance and/or Regulatory Requirements ✔
- Potential Risks ✔

Service Transition

- Timeline for Service Development & Launch ✔
Service Design Checklist: Part 2

Service Operations

- Service Team ✔
- Service Support ✔
- Service Requests ✔
- Knowledge ✔
- Major Incidents ✔
- Technology used for Service Delivery ✔
- Service Dependencies ✔
  - “One-Down” this Service depends on
  - “One-Up” that depend on this Service

Service Level Management

- Service Level Targets ✔
- Service Level Agreements ✔
- Operating Level Agreements ✔
- Underpinning Contracts ✔
- Metrics ✔

Financial model

- Internal
- External
Cloud Backup Phased Rollout

**Phase 1**
Controlled HUIT Rollout
- Provide a default set of CPM policies based on backup policies currently in use
- Ensure all production and development assets moving to the cloud are tagged with a CPM policy
- Provide custom CPM policy service upon request
- Provide restore services upon request

**Phase 2**
Eliminate redundant backups
- Identify where AMT or Networker are being used, ensure there is a CPM tag in place and then remove those configurations

**Phase 3**
Enhanced Self-service
- Improve authentication/authorization model
- Self-service policy creation and restoration
Service Handbook

Service Handbook -