Commvault®

Cloud Rewind™
Formerly Appranix

WHITE PAPER

Cyber Resilience With Commvault Cloud Rewind

Proof of Concept and Success Criteria

Table of Contents

CONTENTS

WHITE PAPER

Overview

Cloud-enabled enterprises have rapidly shifted to a decentralized operating model for their applications and services.

Software architectures have also become more distributed, making use of readily available cloud resources across cloud zones and regions. Site Reliability Engineers have adopted more dynamic and faster release cycles through DevOps practices to meet increased customer demands. Furthermore, programmable cloud resources have enabled environments to scale automatically to meet the performance requirements of critical business applications such as Point of Sale (PoS) systems.

On the negative side, though, these changes have created massive challenges for the shared operations service teams that manage resilience with backup, recovery and disaster recovery, security, and cost. The most pressing question now, especially when cloud environments are prone to increased cyberattacks, is how these dynamic, auto-scaled application environments can recover and rebuild quickly from downtimes using cloud-native infrastructure so promised business SLAs can be maintained.

This document describes how Commvault Cloud Rewind Cyber Resilience SaaS works for cloud application environments.

COMMVAULT CLOUD REWIND

Commvault Cloud Rewind is a comprehensive cyber and cloud resilience solution with cloud-native backup, long term retention with deduplication, replication, and disaster recovery capabilities. Commvault Cloud Rewind ensures not only data resiliency but also the resiliency of the entire distributed and dynamic cloud application environment with all the configurations and dependencies of distributed.

Supported Cloud Platforms

- AWS
- GCP
- Azure
- Kubernetes

COMMVAULT CLOUD REWIND POC

Commvault Cloud Rewind delivers cloud and cyber resilience with an entire cloud environment backup and recovery of resources, data, services, and dependencies at any point-in-time in any cloud region with short and long-term data retention capabilities. This PoC document explains the process of conducting a PoC with specific details and success criteria.

CLOUD ENVIRONMENT DISCOVERY

Modern enterprises cannot afford the risk of not protecting critical cloud resources. Cloud Rewind provides a comprehensive discovery of cloud environment resources so businesses can understand what to protect and what they can afford not to protect. Cloud Rewind agentless service connects multi-cloud accounts for continuous automated discovery and cloud resource dependency mapping. There is nothing to install and no infrastructure to provision. Consolidated cloud resource reports are generated as per the discovery of the cloud environment.

CLOUD ENVIRONMENT PROTECTION

Cloud configurations and dependencies will be continuously backed up in an immutable vault away from the production cloud to withstand even the worst outages and ransomware attacks. Commvault Cloud Rewind's Dual-vault Cloud Time Machine uses an Application-Infrastructure-Centered approach to protect both cloud configurations and application data together in-sync so when the recovery is triggered, application environment resources, application images, containers, cloud services and dependencies can be recovered together.

CLOUD CONFIGURATION DRIFTS

For CISO and Cloud Ops teams, two point-in-time cloud configurations across stacks can be compared to understand drifts and anomalies that could indicate a cyberattack. For example, an unexplained firewall/security group change across all the cloud environments would indicate an anomaly that was not expected by the operations or security teams would indicate a security threat.

APPLICATION DATA BACKUP

Commvault Cloud Rewind backs up your distributed application data spread across multiple services. Based on company policies, Cloud Rewind can retain application backup copies in the same region or to another region or to another tenant. All the application data backup copies will be forever incremental to reduce the RPO and strictly meet the RPO policies.

APPLICATION DATA REPLICATION

Commvault Cloud Rewind can also replicate application data of distributed services to other selected cloud regions. Customers can apply retention policies to keep replicated application data for point-in-time recoveries as well. These replicated copies will be in-sync with the production region backup copies. Customers can optimize the location of data copies based on the business requirements.

GRANULAR RECOVERIES

Commvault Cloud Rewind automatically writes cloud native Recovery-as-Code™ for granular recoveries. For example, you can recover a single VM or database and Cloud Rewind will automatically identify corresponding cloud network resources so the VMs and databases can become quickly operational. No more runbooks, complicated scripts, and risky manual assembly of stacks and services are required.

AUTOMATED RECOVERY TESTING

Commvault Cloud Rewind can automatically run recovery testing based on specified policies for compliance. These automated tests can be set up to run daily, weekly or monthly. After the recovery tests are complete based on Cloud Time Machine copies, all the cloud resources that were created for testing will be automatically deleted to save costs. There will be recovery test reports created so operational teams can be confident about application recoveries after a cyberattack or a cloud regional failure or zonal disaster.

REDUCE COSTS FOR TEST RECOVERIES

Commvault Cloud Rewind provides the capability to rebuild entire cloud infrastructure, applications, and application data using the Recovery-as-Code™ using spot/preemptible instances that could potentially reduce the cost by up to 80% for test recoveries. This capability is available for GCP workloads today.

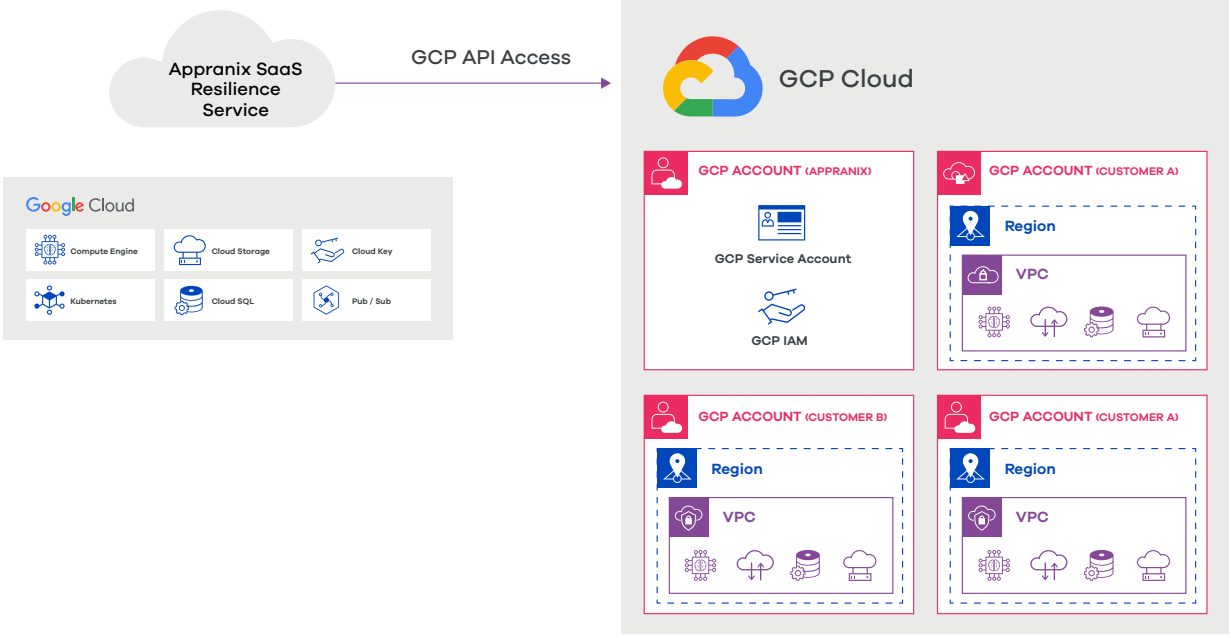
ON-DEMAND REBUILDS WITH RECOVERY-AS-CODE FOR DR

Companies can "turn back the clock" on cloud infrastructure, applications, cloud services and application data to a precise moment in time before an outage or attack occurs. Rebuild allows for disaster recovery without any pre-created infrastructure to tremendously save cloud infrastructure costs. Since Commvault Cloud Rewind Copilot rebuilds using RaC™ to get backup and replicated data recovered fast along with cloud services - IaaS, PaaS, Containers and their dependencies, you can get back your entire application environments with less or no human intervention or complicated scripts.

CLOUD REWIND SECURE SAAS ARCHITECTURE

Cloud Rewind SaaS runs predominately in Google Cloud across multiple zones and regions using GCP high-FedRAMP services. Cloud Rewind is SOC 2 Type II compliant as certified by AICPA. Refer to https://trust.Cloud Rewind.cloud to know how the Cloud Rewind SaaS platform is secured and continuously monitored for several security frameworks' compliance.

Cloud Rewind securely connects to cloud environments using cloud-native API and discovers all the supported resources running within cloud projects. All API calls made by Cloud Rewind are highly secure and encrypted with 256-bit encryption. All the configuration data are encrypted and secured with 256-bit encryption.

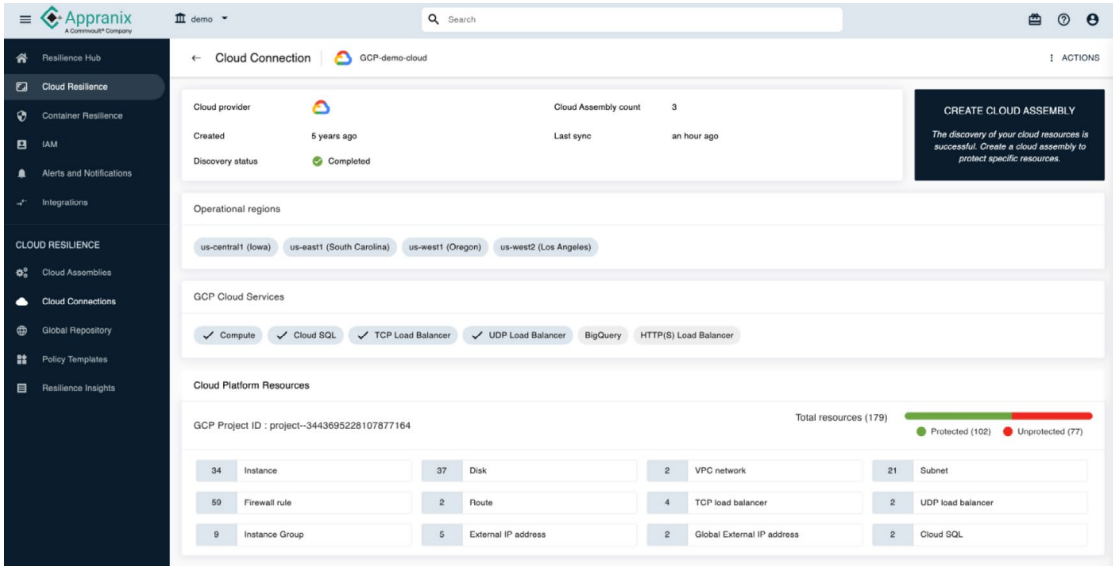


COMMVAULT CLOUD REWIND POC DETAILS

To start the PoC process the customer will have to sign up and create an account and assign permissions with Commvault Cloud Rewind to discover all the PoC resources. Commvault recommends using a development or test environment for the PoC.

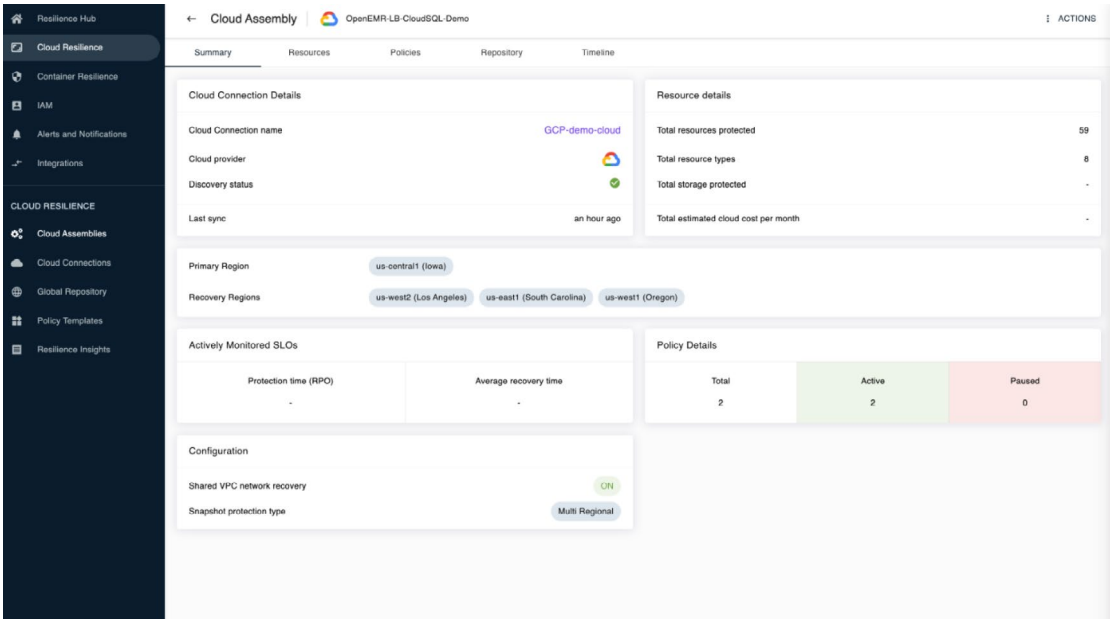
CUSTOMER CLOUD CONNECTION(S)

Customer to provide cloud permissions to connect the cloud environment(s) for discovery. A detailed permissions list is provided here. Cloud Rewind only takes the configurations as read only from customer environments. Here is an example of a Cloud Connection after the discovery is completed.



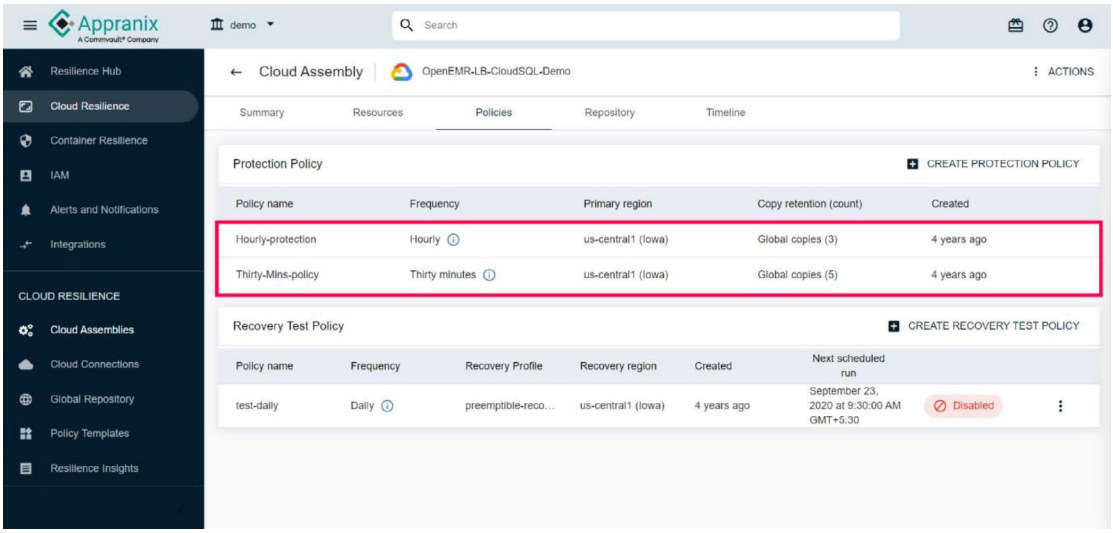
CLOUD ASSEMBLY

Cloud Assemblies can be created per cloud application. Cloud Assemblies are dependent cloud resources that correspond to a customer cloud application. DevOps teams can tag the high-level resources such as VMs or databases PaaS services to protection in their pipelines. The following picture provides an example of such a Cloud Assembly.



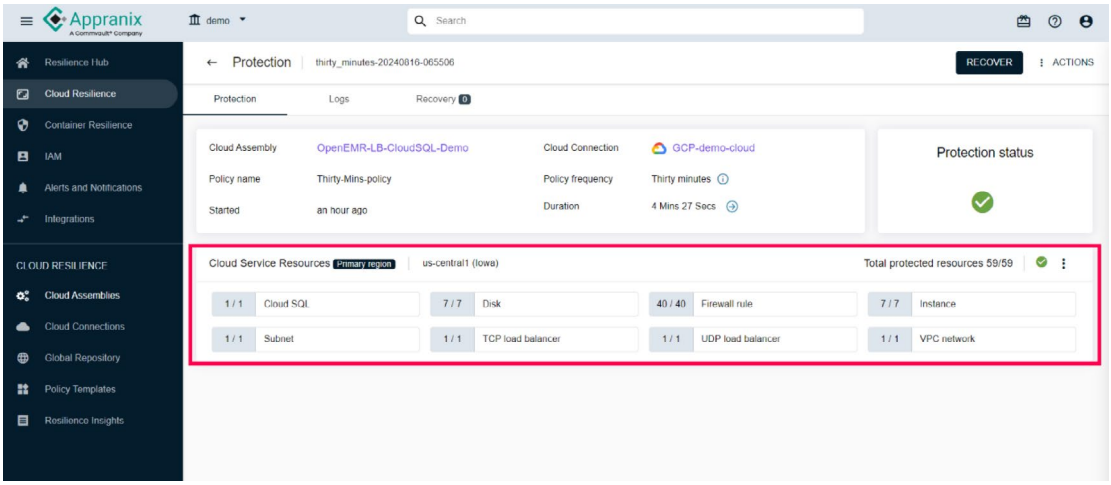
APPLICATION-CENTRIC POLICIES

SRE teams can set up application-centric policies under Cloud Assemblies to back up all the resources. These resources within a Cloud Assembly can dynamically change. A single policy can enforce backup as well as replication SLAs. Within GCP, cross-region replication within a continent appears globally so you can quickly rebuild or recover across to another region. Below is an example of the consolidated policy setup.



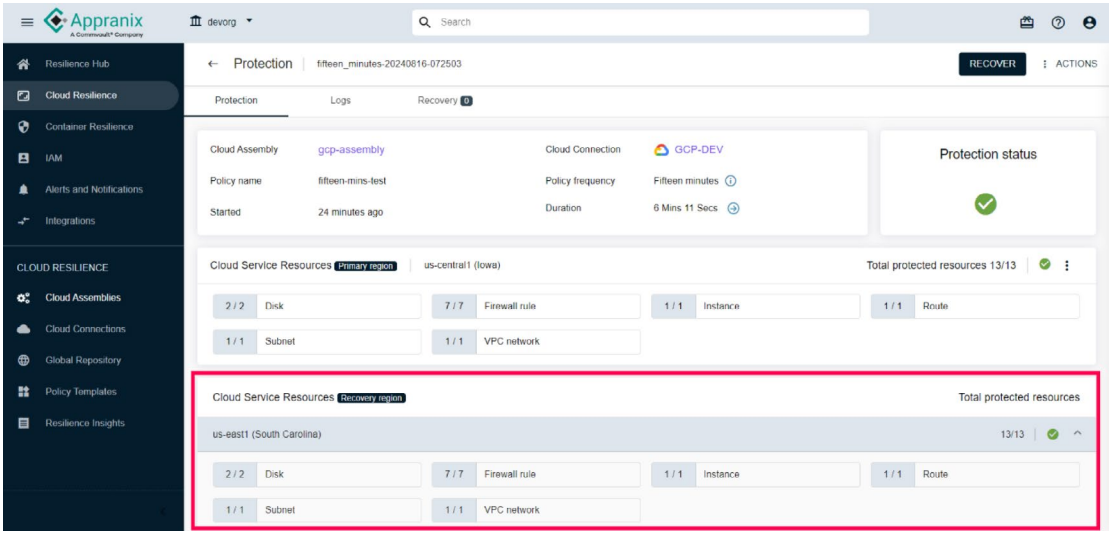
CLOUD-NATIVE BACKUP

Application data will be backed up in the same region for quick VM or other individual resources recovery within the same VPC where the production is running or across to another VPC. One can recover these selected resources or the entire Cloud Assembly across to another Availability Zone as well. Below is an example of cloud-native backup and the associated RPO SLA.



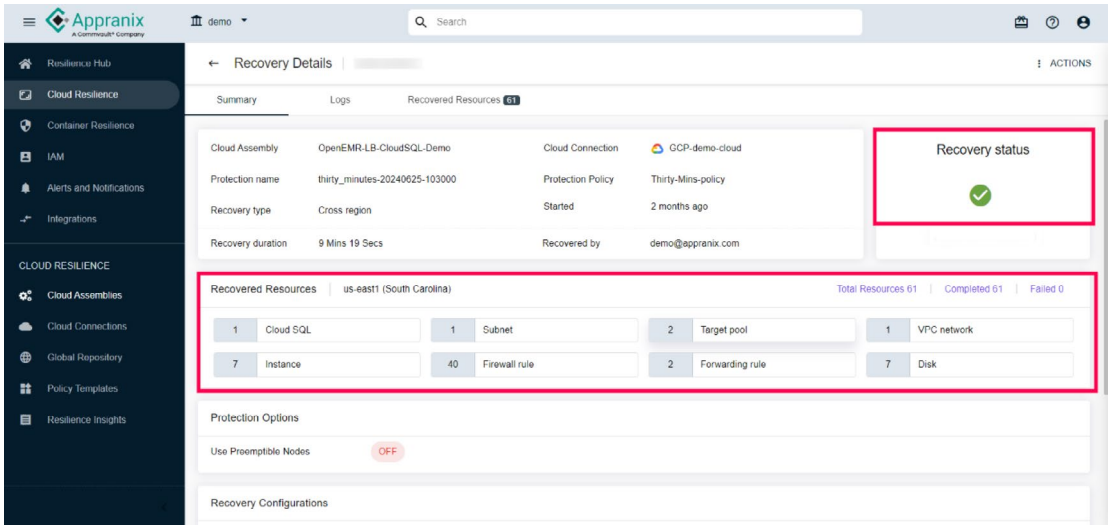
CLOUD-NATIVE REPLICATION

Customers can opt for regional or multi-regional snapshot replication copies. It depends on what the customer decides to optimize between the cost and resilience flexibility. Cloud Rewind will automatically select appropriate regions for replication and RPO SLAs will be available similar to the screen shown below.



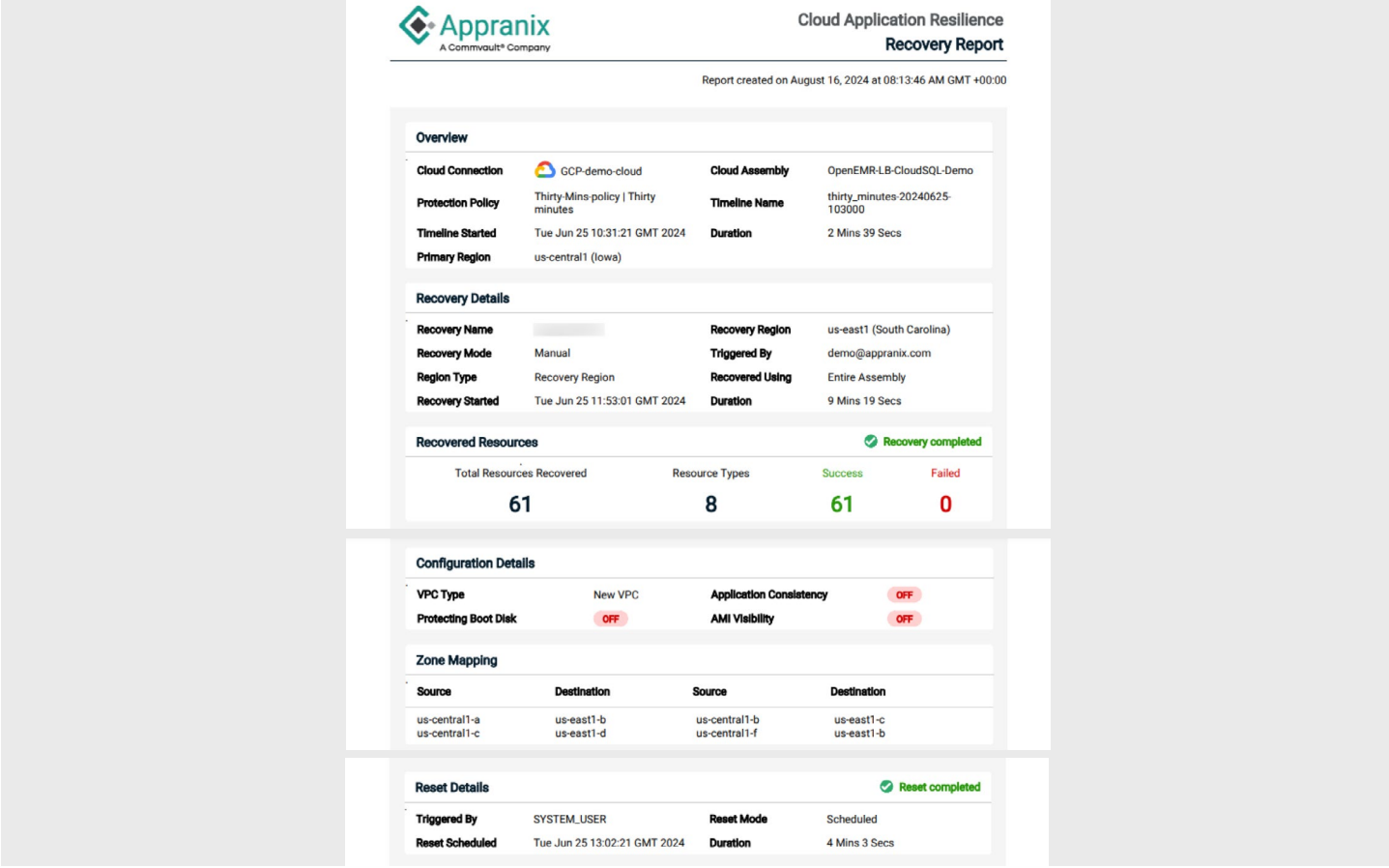
CLOUD APPLICATION RECOVERY

From Cloud Rewind Cloud Time Machine, application stacks can be recovered in the same region or across to other region(s) at a specific point-in-time based on the retention policies setup during the policy creation time. After the recovery, Cloud Rewind will show the total recovery time for the application stack with the details as shown below.



CLOUD REBUILD/RECOVERY REPORT(S)

After a successful recovery, the customer can download a detailed recovery report as shown below.



Appranix
A Commvault® Company

Cloud Application Resilience
Recovery Report

Report created on August 16, 2024 at 08:13:46 AM GMT +00:00

Overview

Cloud Connection	GCP-demo-cloud	Cloud Assembly	OpenEMR-LB-CloudSQL-Demo
Protection Policy	Thirty-Mins-policy | Thirty minutes	Timeline Name	thirty_minutes-20240625-103000
Timeline Started	Tue Jun 25 10:31:21 GMT 2024	Duration	2 Mins 39 Secs
Primary Region	us-central1 (Iowa)		

Recovery Details

Recovery Name		Recovery Region	us-east1 (South Carolina)
Recovery Mode	Manual	Triggered By	demo@appranix.com
Region Type	Recovery Region	Recovered Using	Entire Assembly
Recovery Started	Tue Jun 25 11:53:01 GMT 2024	Duration	9 Mins 19 Secs

Recovered Resources — Recovery completed

Total Resources Recovered	Resource Types	Success	Failed
61	8	61	0

Configuration Details

VPC Type	New VPC	Application Consistency	OFF
Protecting Boot Disk	OFF	AMI Visibility	OFF

Zone Mapping

Source	Destination	Source	Destination
us-central1-a us-central1-c	us-east1-b us-east1-d	us-central1-b us-central1-f	us-east1-c us-east1-b

Reset Details — Reset completed

Triggered By	SYSTEM_USER	Reset Mode	Scheduled
Reset Scheduled	Tue Jun 25 13:02:21 GMT 2024	Duration	4 Mins 3 Secs

REQUIRED CUSTOMER PERMISSIONS

Cloud Provider	Document link
AWS	https://docs.appranix.net/resilience-service/cloud-connections/connect-toaws/
GCP	https://docs.appranix.net/resilience-service/cloud-connections/connect-to-gcp/
Azure	https://docs.appranix.net/resilience-service/cloud-connections/connect-toazure/
EKS	https://docs.appranix.net/container-resilience/container-connection-aws/
GKE	https://docs.appranix.net/container-resilience/container-connection-gcp/
AKS	https://docs.appranix.net/container-resilience/container-connection-azure/

COMMVAULT CLOUD REWIND POC SUCCESS CRITERIA

Success Criteria	Success/Failure
Connecting Cloud Rewind with the customer Cloud Account/ Project/Subscription	
Discovery of all the Cloud Rewind supported cloud resources* in the cloud environment	
Assembly of application resources - creating custom automated Cloud Assemblies	
Recovery region(s) configuration	
Enabling protection and replication with customer policies	
Successful completion of protection and replication of first full and consecutive incrementals for data security in the timeline	
Test for successful recovery of application environment (same-region, cross-region, isolated recovery environment or recovery with precreated-network)	
Verification of the recovered application (customer responsibility)	
Reset of the recovered environment to clean up recovered resources	

CLOUD REWIND GLOBAL ANALYSTS REPORTS

- 2023 Storage Hype Cycle - https://www.gartner.com/interactive/hc/4527399?ref=solrAll&refval=381143410
- Gartner Cool Vendors in storage - https://www.gartner.com/document/3991388?ref=solrAll&refval=381143463&
- Gigaom Cloud-native Leader report - https://gigaom.com/report/gigaom-sonar-report-for-cloud-based-data-protection/