DCIG TOP 5
Enterprise AWS Cloud Backup Solutions

by DCIG President and Founder, Jerome M Wendt

TOP 5 Enterprise AWS Cloud Backup Solutions*

Cobalt Iron Compass

Commvault Backup and Recovery

IBM Spectrum Protect Plus

Unitrends Backup

Veritas NetBackup

** Listed in Alphabetical Order*

SOLUTIONS EVALUATED:

Arcserve Unified Data Protection (UDP)

Asigra Cloud Backup

Clumio Backup for AWS Native Services

Cobalt Iron Compass

Cohesity DataProtect

Commvault Backup and Recovery

Dell EMC Avamar

Dell EMC Networker

Druva Phoenix

IBM Spectrum Protect Plus

Rubrik Cloud Data Management

Unitrends Backup

Veritas NetBackup

SOLUTION FEATURES EVALUATED:

- Backup administration
- Backup capabilities
- Configuration, licensing, and pricing
- Recovery and restores
- Snapshot administration
- Support

AWS a Major Beneficiary of Enterprise Public Cloud Adoption

The percentage of companies running their application workloads on public cloud platforms continues to grow. Consider:

- 30 percent of corporate application workloads currently run on public cloud platforms[1]
- Public cloud platforms will host more than 50% of enterprise workloads and data by 2021[2]
- Most companies expect to accelerate public cloud usage due to the COVID-19 pandemic[3]

These statistics reflect what other surveys also say: enterprise adoption of public cloud platforms continues to grow unabated. Among these platforms, Amazon Web Services (AWS) represents one of this trend's primary beneficiaries. AWS already owns nearly 50% of the public cloud platform market and outdistances its nearest competitor by more than 3:1.[4]

Enterprises select AWS over its competitors for many reasons. It offers over 100 platform services from basic compute and storage services to artificial intelligence, containers, and Kubernetes. It has data centers throughout the world. Over 10 percent of enterprises already host some or all their application workloads on AWS. Taken together, these benefits make a compelling argument for enterprises to adopt and embrace AWS.

Backup Still a Requirement in the AWS Cloud

AWS offers many features enterprises want from a public cloud platform to include high availability, redundancy, security, and many more. Despite all the benefits AWS offers, enterprises must keep one principle in mind: they retain responsibility for their data.

This puts the onus on enterprises to backup and recover their data. Should their data get corrupted, deleted, lost, or encrypted by ransomware, they need a solution in place to protect it.

AWS does offer its own backup software. However, it is a separate offering optimized for virtual machine backup to which enterprises must subscribe. Many enterprises will have application and data requiring specific backup and recovery features beyond what AWS's backup software offers. This will necessitate they acquire a third-party solution that meets their AWS backup and recovery needs.

The State of Enterprise AWS Cloud Backup Solutions

Most of the solutions that meet enterprise backup and recovery requirements for the AWS cloud got started doing on-premises backup. This start gave them the core functionality that enterprises still need as they move existing applications to the cloud.

Enterprises deploy these backup solutions in the AWS cloud the same way they do on-premises, with minor differences. They obtain an appropriately sized Elastic Cloud Compute (EC2) instance from AWS to host the backup software. They license, install, and maintain the backup solution themselves. They configure it to back up their applications hosted in the AWS cloud. In many respects, they manage this backup software in the cloud the same way they do now.

These enterprise AWS cloud backup solutions do, however, face a challenge going forward. Fewer enterprises want to manage backup software the same way they did in the past. Instead, they want to subscribe and pay for backup software like they do other services in the AWS cloud.

They also want backup software architected and available as a cloud-native service. Delivered this way, the backup software automatically scales up or down based on demand. The provider also handles all the backup software's ongoing maintenance, such as fixes, patches, and upgrades. This frees enterprise to focus on using the backup software while removing the task of maintaining it.

Of the thirteen enterprise solutions DCIG evaluated, two already deliver their software as cloud-native

[1] https://virtualizationreview.com/articles/2020/01/17/cloud-workloads.aspx. Referenced 8/12/2020.

[2] https://resources.flexera.com/web/pdf/report-state-of-the-cloud-2020.pdf. Referenced 8/12/2020. Pg. 10.

[3] Ibid. Pg. 10

[4] https://www.forbes.com/sites/jeanbaptiste/2019/08/02/amazon-owns-nearly-half-of-the-public-cloud-infrastructure-market-worth-over-32-billion-report/#377293c229e0. Referenced 8/12/2020.

DCIG: Empowering the IT industry with actionable analysis.™

AWS offerings. As they introduce features to better protect applications lifted-and-shifted to the cloud, they will become more attractive to enterprises. In the meantime, expect current providers to make their software available as a cloud-native offering in the coming years.

Distinguishing Features of Enterprise AWS Cloud Backup Solutions

DCIG identified over 30 solutions in the marketplace that offer backup capabilities for the AWS cloud. Of these, DCIG identified and classified thirteen of them as meeting DCIG's definition of an enterprise AWS cloud backup solution. These thirteen solutions target large enterprise environments in their user and administration documents. Attributes that help distinguish these solutions from those targeted at small and midsize enterprises (SMEs) include support for the following:

1. ***Enterprise level support.*** The levels of support enterprise backup solutions offer perhaps most distinguishes them from solutions targeted as SMEs. They each give enterprises multiple ways to contact them (chat, email, phone, web) with near immediate response times. In contrast, SME offerings may only offer a subset of these contact mechanisms and slower response times when contacted.
2. ***Hybrid backup and recovery.*** Enterprises often support a hybrid environment with some applications running on-premises and others in the AWS cloud. They can use most of the enterprise AWS cloud backup solutions to protect data across these two environments.
3. ***Protect cloud-based SaaS applications.*** Some applications enterprises once used on-premise they now subscribe to as cloud-based SaaS offerings. Over 70 percent of the solutions could protect SaaS applications such as Google G Suite, Microsoft Office 365, or Salesforce.
4. ***Protect non-AWS databases.*** The non-AWS databases that each one protects varies by solution. Most will minimally protect Microsoft SQL Server, MySQL, Oracle Database and SAP HANA.

Similarities between the TOP 5 Enterprise AWS Cloud Backup Solutions

In addition to the features listed above that all enterprise AWS cloud backup solutions generally share, the TOP 5 solutions have the following traits in common. They include:

- ***Index protected data.*** More enterprises desire deeper insight into their protected data as well as to comply with various government regulations. Each solution indexes the data it protects to provide this visibility and compliance that enterprises seek.
- ***Options to take frequent snapshots***. Applications differ in their respective recovery point objectives (RPOs) and recovery time objectives (RTOs). To meet these varying requirements, every TOP 5 solution may create application snapshots as frequently as every 15 minutes. Further, they all recognize and integrate with Amazon Elastic Block Store (EBS) to create and store these snapshots.
- ***Protect VMware applications running in VMware Cloud on AWS.*** A recent survey showed that VMware Cloud on AWS is already the cloud fifth most used by enterprises. Further, it could jump into the number four or number three position based upon current trends.[5] Each of these TOP 5 solutions gives enterprises the flexibility to protect the VMware applications running in VMware Cloud on AWS.

Next Gen Enterprise AWS Cloud Backup Solution Features

Using backup software hosted in the AWS cloud affords new ways for enterprises to back up and recover their applications. Note that enterprises may only find these capabilities available on some of the solutions evaluated.

Providers remain in the early stages of optimizing their software to back up and recover applications and data hosted in AWS. As a result, the breadth and type of features they offer that leverage AWS's resources still vary. However, here are some features a few solutions already offer that enterprises may find appealing.

1. **Store backup data In Amazon S3.** Using Amazon's simple storage services (S3) as a primary backup target for these solutions becomes more practical. AWS S3 storage resides in the same physical location as the applications so backups to S3 and recoveries from it may complete more quickly. Once they store backup data on S3, enterprises may take advantage of S3's various features. These include tiering, versioning, and data immutability. Further, a few solutions offer the option to manage these more advanced S3 features through their management console.
2. **Protect AWS RDS databases.** Using Amazon's relational database service (RDS), enterprises may subscribe to any of six different relational databases like other AWS services. However, the responsibility to manage, back up, and recover the data stored in these RDS databases still falls on enterprises. Many of these enterprise backup solutions offer options to back up and recover these AWS RDS databases.
3. **All-inclusive, subscription-based pricing.** A few solutions already model their pricing structure after AWS's pay-as-you go model. While each one's pricing structure varies, those that do offer it calculate their pricing based upon some mix of variables. Enterprises should minimally expect to pay monthly based upon how much data they backup and how many VMs they protect. They may pay extra for services such as disaster recovery and premium levels of support.
4. **AWS IAM integration.** More enterprises want to give applications owners ownership over scheduling their backup and recovery jobs. A few backup solutions already support and integrate with AWS's Identity and Access Management (IAM) feature. Through this integration with IAM, they can use the application owners' AWS logins to assign them roles in the software.

[5] https://www.flexera.com/blog/industry-trends/trend-of-cloud-computing-2020/. Referenced 8/14/2020.

All TOP 5 solutions also support the following traits:

- Back up and restore individual VMs at the file, folder, volume, and VM image levels
- Encrypt data at-rest and in-flight
- Generate alerts on backup job errors and failures
- Index protected data
- License their solution in the AWS cloud using a bring your own license (BYOL) model
- Make their solution available in all compatible AWS regions
- Perform cloud-to-cloud (C2C), instant, and virtual-to-virtual (V2V) recoveries
- Perform differential, full, and incremental backups
- Perform secure erasure of deleted data
- Protect Microsoft Active Directory and Exchange applications hosted in the AWS cloud
- Vault backups

Differences between the TOP 5 Enterprise AWS Cloud Backup Solutions

The TOP 5 solutions differ in how they deliver their respective offering in the AWS cloud in at least the following five ways:

- ***Automated VM conversion to AMI-compliant VMs.*** Although all these solutions perform VM backup, they do not yet all automatically convert protected VMs to Amazon Machine Image (AMI) compliant VMs. Enterprises lifting and shifting applications to the AWS cloud or looking to change how they host their VMs in AWS may find this feature desirable.
- ***Available as a SaaS offering.*** Only two of these TOP 5 solutions make their software available as SaaS offerings. They each host their SaaS offering outside of the AWS cloud.
- ***Integration with single sign-on (SSO) solutions.*** More enterprises use SSO solutions such as Okta or OneLogin to centralize, consolidate, and simplify user administration. Three of the TOP 5 solutions have already integrated their software with these SSO offerings.
- ***Backup solution management interface.*** While all the solutions provide a GUI to manage their own software, only one currently integrates with AWS IAM. However, four TOP 5 solutions already integrate with third party cloud management software such as CloudAware, CloudCheckr, or ServiceNow.
- ***Protection of AWS databases.*** Having their origins in protecting on-premises databases, only two currently protect any of AWS databases. If enterprises currently use any AWS databases, they will need to verify a solution can back up and recover them.

TOP 5 Enterprise AWS Cloud Backup Solution Profiles

Each of the TOP 5 Enterprise AWS Cloud Backup Solution profiles highlights at least three ways each one differentiates itself. These differentiators represent some of the best methods that backup solutions offer to back up and recover data in the AWS cloud. Within each solution, enterprises will find distinctive features that may better meet their respective needs.

Cobalt Iron Compass

Cobalt Iron Compass continues to display its prowess in the enterprise backup and recovery market. Previously identified by DCIG as a TOP 5 enterprise anti-ransomware solution, DCIG now ranks it a TOP 5 enterprise AWS cloud backup solution. Enterprises may deploy Compass in multiple ways in AWS and gain access to all its features through an all-inclusive licensing option. Ways that Cobalt Iron differentiates itself from other TOP 5 enterprise AWS cloud backup solutions include:

- ***Protects Amazon RDS database instances.*** Cobalt Iron represents one of the few enterprise AWS backup solutions that protects AWS RDS database instances. Using RDS, enterprises obtain the benefits of relational databases and leave their backend management tasks to AWS. Further, relational databases still represent the most common database enterprise developers select when creating new applications.[6] Compass' support for AWS RDS frees enterprises moving into the cloud to adopt AWS RDS. It simultaneously offers applications born in the cloud access to an enterprise caliber backup solution.
- ***Analytics engine to improve backup and recovery.*** Cobalt Iron grants every Compass user access to its analytics engine. This software constantly evaluates how Compass backups perform across all enterprise environments, to include their backups in the AWS cloud. Using this information, it may then automatically act. These actions may include optimizing when backups run, resolving backup storage issues, and monitoring the infrastructure for the presence of ransomware.
- ***Supports backup across multiple public and private cloud.*** Cobalt Iron differentiates itself from almost all other backup solution by offering backups in multiple public and private clouds. Others generally support at most one or two public clouds in addition to providing backup for on-premises applications. In addition to AWS, Cobalt Iron Compass also protects applications running in the Alibaba Cloud, Google Cloud, IBM Cloud, and Microsoft Azure. Since many enterprises plan to utilize multiple clouds, they may use Compass to back up applications across all of them.

Commvault Backup and Recovery

Commvault Backup and Recovery demonstrates its ability to meet evolving enterprise backup needs. As enterprises adopt the AWS cloud, they may turn to Commvault to protect the applications and data they move to it. They will also find Commvault offers multiple options to protect AWS applications. Commvault offers the following features that help distinguish it from other enterprise AWS cloud backup solutions.

- ***Automated spin-up and shutdown of Commvault EC2 instances.*** Commvault uses EC2 instance in the AWS cloud to host its software with each of these instances incurring hourly costs. Commvault monitors its instances current and scheduled activity on AWS. Should Commvault not need the instances

[6] https://insights.stackoverflow.com/survey/2020. Referenced 8/14/2020.

hosting its software, it shuts them down until they are needed. This helps to reduce the EC2 costs incurred by Commvault.

- ***Migrate existing database applications to Amazon EC2 or RDS instances.*** Enterprises currently using MySQL, Oracle, PostgreSQL, or SQL Server databases often want to optimize them once in the AWS cloud. Using Commvault, they can more easily accomplish this task. They may migrate a database to an EC2 instance that more closely aligns with the database's underlying technical requirements. Alternatively, Commvault can migrate a database instance into Amazon RDS so Amazon may assume management of the underlying database.
- ***Protects multiple AWS databases.*** Once enterprises adopt the AWS cloud, they often want to use AWS databases such as Aurora, DocumentDB, DynamoDB, or RedShift. Commvault helps to facilitate and accelerate their adoption and use of these AWS databases. Commvault represents one of the few solutions that already protects these AWS databases.

IBM Spectrum Protect Plus

IBM Spectrum Protect Plus cracks the inaugural list of DCIG TOP 5 Enterprise AWS Cloud Backup Solutions. Available in the AWS marketplace, enterprises may deploy IBM Spectrum Protect Plus on Amazon Machine Images (AMIs). IBM makes an AWS CloudFormation template available to accelerate and simplify its provisioning and configuration in the AWS cloud. Spectrum Protect Plus offers the following features that help distinguish it from other TOP 5 offerings

- ***A hybrid deployment option.*** Enterprises adopting AWS may need to continue protecting applications on-premises in addition to those running in the AWS cloud. Using Spectrum Protect Plus, enterprises may first deploy its vSnap server in the AWS cloud. This serves as a backup target for VMs hosted in the AWS cloud. They may deploy vSnap server while continuing to run Spectrum Protect Plus on-premises.
- ***Protects logical application groupings of containers hosted in Kubernetes.*** In 2019, the Cloud Native Computing Foundation surveyed individuals in the software, technology, and professional services industries. It found 78 percent of them already use Kubernetes in production.[7] When deployed on-premises, IBM Spectrum Protect Plus protects persistent volumes in a Kubernetes environment. It can create SLA policies such as snapshots, backups, replication, and data retention. As enterprises build new applications using containers, developers can use these labels to protect logical application groupings instead of individual volumes. They may also back up and recover logical persistent volumes associated with Kubernetes namespaces.
- ***Supports multiple object stores for cost-effective data retention and archiving.*** Enterprises cannot always keep all their backup data in the AWS S3 storage cloud. Some need to bring this data back on-premises or store it in other cloud to satisfy application, archival, or compliance requirements. Using Spectrum Protect, they may copy data to other object stores, to include on-premises object stores. They can also use Spectrum Protect to further lower storage costs in Amazon S3 by placing data on S3 Glacier.

Unitrends Backup

Unitrends Backup builds upon its success in on-premises backup to tackle the new world of enterprise AWS cloud backup. DCIG has previously identified Unitrends as a TOP 5 provider of anti-ransomware and all-in-one disaster recovery solutions. Enterprises may also turn to Unitrends to back up and recover their applications and data in the AWS cloud. Key features that Unitrends offers to help distinguish it from other AWS cloud backup solutions include:

- ***Recovery assurance.*** Unitrends stands apart as one of the only providers to formally offer backup testing and verification. Recovery assurance grants enterprises the flexibility to regularly test and verify they can successfully recover from their backups.
- ***Unitrends conducts these recovery tests in its cloud, rather than the AWS cloud, for multiple reasons.*** This approach mitigates the additional compute and storage costs and configuration overhead that performing these tasks in the AWS cloud would incur. It also gives enterprises confidence they can recover outside the AWS cloud should it become unavailable, which does occur.
- ***Certified recoveries in the Unitrends Cloud.*** Recovering applications in the Unitrends cloud serves another important purpose: enterprises can certify their recoveries work. Unitrends can perform recoveries in its cloud on the enterprise's behalf to certify application and data recoveries work. Once recovered, Unitrends provides a certification the recovery worked. Third parties such as regulatory agencies accept this certification as proof that an enterprise can recover from a disaster.

Veritas NetBackup

Veritas brings its rich background in enterprise backup to bear in successfully adapting NetBackup to meet enterprise AWS cloud backup requirements. NetBackup brings along its backup capabilities that enterprises continue to need as they lift-and-shift them to the AWS cloud. As it does so, NetBackup offers new features enterprises need to facilitate their move to the AWS cloud. Technologies and solutions that help set Veritas NetBackup apart in providing backup in the AWS cloud include:

- ***Standardizes backup data before storing it on Amazon S3 buckets.*** Enterprises typically know they will incur a monthly per GB fee when storing data on Amazon S3. However, they may forget that as their applications store or retrieve data from S3, they may incur ingress and egress fees. To alleviate these costs, NetBackup breaks data down to a 64MB chunk of deduplicated data prior to storing it in an S3 bucket. In this way, every GET or PUT request NetBackup issues to an S3 bucket sends or retrieves the same amount of data.
- ***Application data migration to the AWS cloud.*** To facilitate migrating application data from on-premises to the AWS cloud, NetBackup 8.2 introduced image sharing into its CloudCatalyst feature. CloudCatalyst enables NetBackup to store on-premises backups on AWS S3 object stores. Its image sharing capabilities make the S3 bucket where NetBackup stores backups self-descriptive. In so doing, the bucket becomes available for reuse by instances other than the one that created and used it. This facilitates moving on-premises applications to the AWS cloud and bringing them online since their data already resides there.

[7] https://www.cncf.io/wp-content/uploads/2020/03/CNCF_Survey_Report.pdf/ Referenced 7/28/2020.

- ***Orchestrating complex application migrations to the AWS cloud.*** Enterprises may have multiple interdependent applications they want to migrate to the cloud. Keeping them in sync as they migrate applications to the AWS cloud requires a more sophisticated approach. In these situations, enterprises may use NetBackup Resiliency. This includes automatic deployments of NetBackup in AWS that may access CloudCatalyst data stores on S3 object stores.

Enterprise AWS Cloud Backup Solutions Inclusion Criteria

- Protect applications and data residing in the Amazon Web Services (AWS) cloud
- Meets backup and recovery requirements of large enterprises
- Solution is shipping and available by July 1, 2020
- Information available for DCIG to make an informed, defensible decision

DCIG Disclosures

Vendors of some of the solutions covered in this DCIG TOP 5 report are or have been DCIG clients. This is not to imply that their solution was given preferential treatment in this report. In that vein, there are some facts to keep in mind when considering the information contained in this TOP 5 report and its merit.

- No vendor paid DCIG any fee to research this topic or arrive at predetermined conclusions.
- DCIG did not guarantee any vendor that its solution would be included in this TOP 5 report.
- DCIG did not imply or guarantee that a specific solution would receive a TOP 5 designation.
- All research is based upon publicly available information, information provided by the vendor, and/or the expertise of those evaluating the information.
- DCIG conducted no hands-on testing to validate how or if the features worked as described.
- It is a misuse of this TOP 5 report to compare solutions included in this report against solutions not included in it.

No vendor was privy to how DCIG weighted individual features. In every case the vendor only found out the rankings of its solution after the analysis was complete. To arrive at the TOP 5 solutions included in this report, DCIG went through a seven-step process to come to the most objective conclusions possible.

1. DCIG established which features would be evaluated.
2. The features were grouped into five general categories.
3. A DCIG analyst internally examined the feature data for each solution and completed a survey for it based upon the analyst's own knowledge of the solution and publicly available information.
4. DCIG identified solutions that met DCIG's definition for an Enterprise AWS Cloud Backup Solution.
5. DCIG weighted each feature to establish a scoring rubric.
6. DCIG evaluated each solution based on information gathered in its survey.
7. Solutions were ranked using standard scoring techniques. ■

About DCIG

DCIG empowers the IT industry with actionable analysis that equips individuals within organizations to conduct technology assessments. DCIG delivers informed, insightful, third party analysis and commentary on IT technology. DCIG develops custom and licensed content in the form of blog entries, executive white papers, podcasts, competitive intelligence reports, webinars, white papers, and videos. More information is available at **www.dcig.com.**