

Simplifying Cloud Data Protection

NetBackup Intelligent Cloud Policy Engine automates protection.

VERITAS™

OVERVIEW

If organizations were previously reluctant to embrace the cloud, the recent COVID-19 health crisis has forced them to pivot, reinvent and develop new capabilities to meet the needs of the socially distanced era that includes tele-medicine, eLearning, virtual retail experiences and government-to-citizen services, to name a few. The pay-as-you-go cloud model gives companies the flexibility to dynamically provision cloud resources to meet peak usage needs and scale down those resources to manage cloud infrastructure costs. Cloud vendors typically guarantee their service, however, not the safety of your data. Companies need to revisit their business continuity/disaster recovery plans to ensure their new cloud architectures and information are adequately protected.

**ALWAYS
PROTECTED...**

**NO CLOUD
LEFT BEHIND**

As organizations scale their cloud investments, they also need to protect, measure and monitor a wide variety of services, resources and assets. Departments may use their own criteria to logically group together cloud resources using tags. Cloud resources do not automatically inherit tags, which must be assigned by the application, the individual launching the resource or an administrator. Each tag consists of a name and a value pair, and organizations can use multiple tags to reference a specific asset. A good tagging strategy helps identify assets based on department, function, application owner or other similar criteria.

A good cloud-native data protection platform must be capable of identifying tags on newly discovered assets and protecting this data to ensure it complies with the information lifecycle policies of the business. In short, this strategy delivers no surprises because your cloud data is always protected.

PROTECT CLOUD ASSETS WITH NETBACKUP INTELLIGENT GROUPS

Veritas NetBackup™ supports the backup and recovery of workloads within cloud environments by leveraging cloud-native snapshot technology on Google Cloud Platform (GCP), Microsoft Azure and Amazon Web Services (AWS). Cloud or IT architects can use NetBackup 9.1 to create and manage intelligent groups of cloud assets based on a set of filters using simple queries. As an organization adds to or removes cloud resources from the environment, NetBackup automatically selects the discovered assets based on simple SQL-based queries and adds them to the designated intelligent group. These groups can be defined for AWS, Azure, Azure Stack and GCP cloud providers starting in NetBackup 9.1 (see Figure 1).

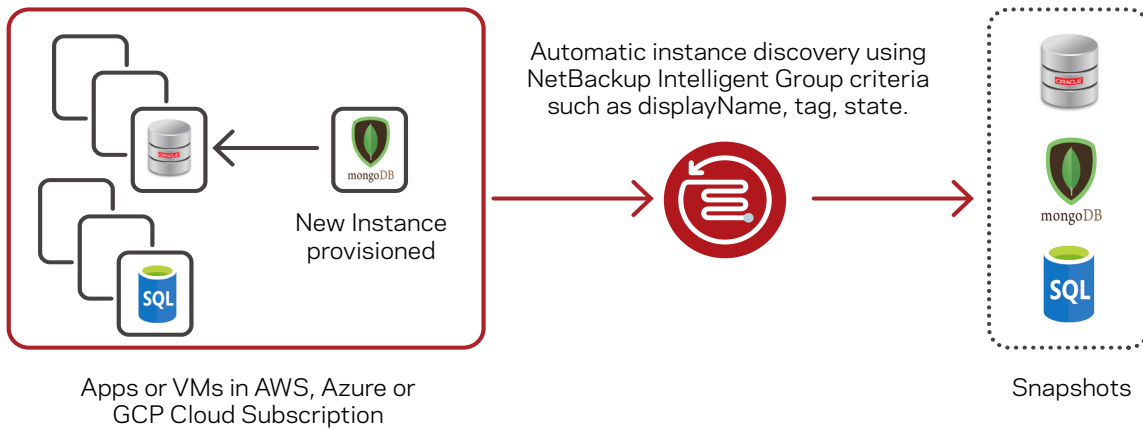


Figure 1. An overview of NetBackup intelligent groups for cloud assets.

Once defined, organizations also need to associate intelligent groups with protection plans that describe how the data is to be protected. These plans enable workflow customization with options to enable granular files and folder recovery or protect platform as a service (PaaS) application workloads on supported cloud platforms.

Using role-based access control (RBAC), the cloud administrator or IT architect can be enabled for self-service in NetBackup. This designation helps with both visibility and control of data protection for cloud assets. Privileged users can preview the asset list in an intelligent group at any time to see which will be protected during the next job run. They can also alter the intelligent group criteria as well as post-processing attributes.

These users can easily automate the creation of an intelligent group for the cloud using our API capabilities or configure it using the NetBackup user interface (see Figure 2).

Asset types include virtual machines (VMs) and supported PaaS applications. Each intelligent group provides a filtered selection of cloud assets within a specific region or zone and an account ID for the chosen cloud provider. The account ID requested corresponds to the Subscription ID for Azure, the Account ID for AWS and the Project ID for GCP.

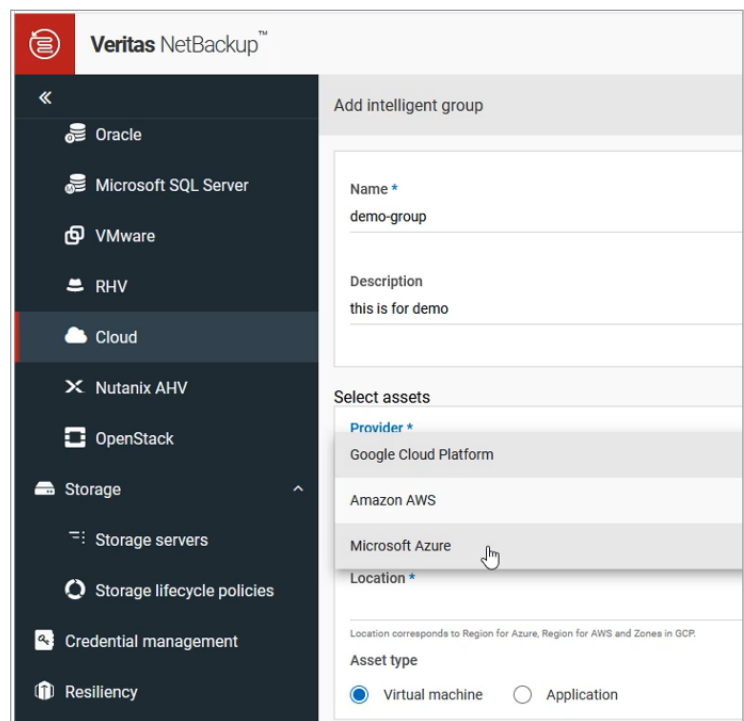


Figure 2. Application resilience under VMware with Veritas InfoScale.

Admins can easily build queries using NetBackup's visual editor and offer a Preview function to ensure all intended cloud resources are protected. Figure 3 shows how to use tags and displayName attributes to display a filtered list of assets. Administrators can also review protected assets and update the query to alter its scope. The asset's instance type, common asset attributes, and operational state are other attributes that the administrator can use for filtering. The query-based selection process is dynamic. Figure 4 gives an example of the query syntax and representative list of assets matching the query. The query can be consumed via RESTful APIs to help automate data protection workflows.

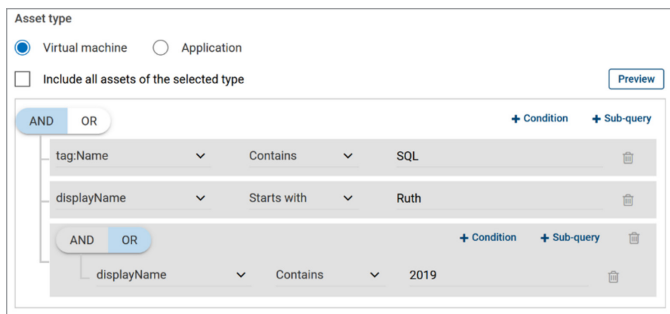


Figure 3. The visual SQL query builder for a NetBackup intelligent group.

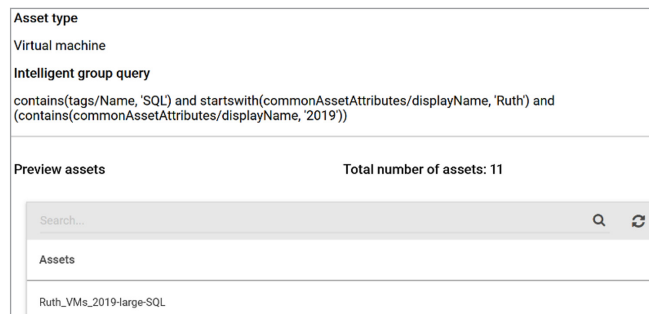


Figure 4. An example of a NetBackup intelligent group query and asset list.

CONCLUSION

The automatic discovery of new assets and intelligent filtering drastically reduce the level of effort required for automating data protection for cloud assets and staying compliant as enterprises continuously adopt multicloud applications and infrastructure.

To learn how easy it is to protect cloud resources, download a copy of Veritas NetBackup™ 9.1 from our [trialware page](#). Existing customers can download a copy from the [Veritas Download Center](#).

Veritas NetBackup enables organizations of all sizes with robust, cloud-native technologies that protect the business on every step along the cloud transformation journey. Learn more at veritas.com/netbackup.

ABOUT VERITAS

Veritas Technologies is a global leader in data protection and availability. Over 50,000 enterprises—including 87 percent of the Fortune Global 500—rely on us to abstract IT complexity and simplify data management. The Veritas Enterprise Data Services Platform automates the protection and orchestrates the recovery of data everywhere it lives, ensures 24/7 availability of business-critical applications, and provides enterprises with the insights they need to comply with evolving data regulations. With a reputation for reliability at scale and a deployment model to fit any need, Veritas Enterprise Data Services Platform supports more than 800 different data sources, over 100 different operating systems, more than 1,400 storage targets, and more than 60 different cloud platforms. Learn more at www.veritas.com. Follow us on Twitter at [@veritastechllc](https://twitter.com/veritastechllc).

2625 Augustine Drive, Santa Clara, CA 95054
 +1 (866) 837 4827
www.veritas.com

For specific country offices and contact numbers, please visit our website.
www.veritas.com/company/contact

