VEEAM PROPARTNER

What's New:

Veeam Backup *for Google Cloud* v3

Releasing in Q2 2022, Veeam Backup *for Google Cloud* v3 adds Google Cloud-native backup and recovery for MySQL, as well as numerous enhancements to security and user experience.

Capability	MYSQL Backup Control	Role-based Access Control (RBAC)
What it does	Automate native backup of MySQL databases on Google Cloud, which features flexible policy-based protection and recovery options.	Veeam enables the assignment of specific roles and permissions to different users within Veeam Backup for Google Cloud. This allows organizations to delegate specific tasks to certain groups of users, improving operational efficiencies while also securing backup data from unauthorized access.
Customer goals, problems, and needs	Many companies are looking to leverage cloud-hosted databases due to their scalability and ease of management. This makes MySQL support a highly demanded feature in Google Cloud. Like all databases both on-prem and in the cloud, backup and recovery of this data is the responsibility of the user – not Google – to ensure maximum availability for the database and the applications that rely on them.	Security is at the forefront of almost every IT professional's priorities, especially in the light of the growing volume of cybersecurity threats and breaches. Need an easy way to ensure only the right people have secure access to Veeam backups configuration, policies, and encrypted backups.
Diagnose with these questions	Do you run MySQL on Google Cloud? How do you backup and protect these MySQL databases? Does this mean you spend too much of your time and resources ensuring your MySQL data is protected and can be recoverable? What would the impact to your business be if you were not able to easily restore your MySQL data?	How do you currently manage access to Google Cloud data protection in your organization? What's your strategy to make sure only the right people in your organization have access to Google Cloud backups configuration? Does that mean it is complicated to ensure only the right people have access to your Google Cloud data? Does this limit your ability to delegate tasks related to backup policies only to a specific group of users (for example, only restore some resources)? How does this impact the security of your Google Cloud data? What is the impact to your business?
Position with usage scenarios	**Automate native backup of MySQL databases on Google Cloud**, which features flexible policy-based protection and recovery options.	**Delegate data protection-specific permissions to users** to maximize operational efficiencies while ensuring greater security.

VEEAM PROPARTNER

What's New:

Veeam Backup *for Microsoft AWS* v5

Releasing in Q2 2022, Veeam Backup *for AWS* v5 expands AWS-native support in these areas:

Capability	Amazon Aurora Backup	Enhanced Amazon EFS Backup	Configuration backup & restore
What it does	Amazon Aurora is a MySQL and PostgreSQL relational database built for the cloud and is part of the Amazon RDS offering. This new feature allows users to natively protect Amazon Aurora using native snapshots. Recovery involves full database recovery to the original location or to a new location.	Amazon Elastic File Systems (Amazon EFS) creates a catalog of guest files to enable browsing, searching and easier restore of individual files. Veeam Backup *for AWS* supports cloud-native backup of Amazon EFS, with v5 including enhanced file-level indexing.	Veeam Backup *for AWS* can now create a backup of its full configuration on a backup repository.
Customer goals, problems, and needs	AWS provides over 200 services that users can consume, with Amazon Aurora being one of the most popular due to its speed. Just like a data on AWS, Amazon Aurora databases also need to be protected.	Enhanced file-level indexing for Amazon EFS backup improves the speed and efficiency when locating and restoring individual files and folders stored in backups.	Enables organizations with easy recovery options of the Veeam Backup *for AWS* appliance, also useful for redeployments, migrations, testing and more.
Diagnose with these questions	What relational database services in AWS do you use? Do you use Amazon Aurora? How would it impact your business apps and services if you lost or experienced an outage of your Amazon Aurora data?	What is your backup strategy for AWS? Do you use Amazon EFS Backup? Are you able to locate and recover individual files and folders in your Amazon EFS backups? If so, how easy or fast is this?	What is your strategy if your backup server fails for some reason? Do you regularly perform configuration backups of your backup infrastructure? How easy is it to recover your backup infrastructure?
Position with usage scenarios	Natively protect Amazon Aurora databases, featuring **flexible policy-based scheduling,** and **lightning-fast recovery to an exact point-in-time in seconds**.	**Achieve even quicker and easier restores** of Amazon EFS files and folders through **enhanced file-level indexing** of file system backups.	**Create backups** of Veeam Backup *for AWS* and its configuration, ideal for **redeploying** from scratch, quick **migration** procedures, **testing** and more.

VEEAM PROPARTNER

What's New:

Veeam Backup *for Microsoft Azure* v4

Releasing in Q2 2022, Veeam Backup *for Microsoft Azure* v4 expands Azure-native support to include Azure Files backup and recovery

Capability	Azure Files Backup & Recovery
What it does	This new feature allows users to natively backup and recover their Azure Files using a fully automated and secure solution for even the largest file systems.
Customer goals, problems, and needs	Many organizations are turning to Azure Files for new file share deployments as well as migrating on-prem Windows file servers as it offers simple, secure, and serverless cloud file shares. Like all file shares both on-prem and in the cloud, backup and recovery of this data is the responsibility of the user — not Microsoft — to ensure maximum availability for the data and the applications that rely on them.
Diagnose with these questions	How do you backup and protect your Azure Files deployments? Does this mean you spend too much of your time and resources ensuring your Azure Files data is protected and can be recovered? What would the impact to your business be if you were not able to easily restore your Azure Files data?
Position with usage scenarios	**Extend Azure-native backup and recovery** to Azure Files, a fully automated and secure solution for even the largest file systems.