# Protecting Azure resources with Recovery Services vault

We've implemented Azure Recovery Services vault to provide data protection services for our growing Azure virtual machine infrastructure. Recovery Services vault is a cloud-based PaaS solution—by using it, our employees can quickly obtain access to data protection for Azure resources. It's flexible and adaptable enough to meet the needs of all our business groups, and it can evolve into an even more comprehensive data protection solution in the future.

## Data protection services at Microsoft

Our data protection services team manages data protection for all Core Services Engineering (CSE, formerly Microsoft IT). We oversee the backup and recovery of almost 9 petabytes (PB), or 9 million gigabytes (GB), of on-premises data for the organization. Primarily, we use Microsoft System Center Data Protection Manager for our on-premises workloads. We use it for the backup and recovery of:

- Physical servers, files, and folders.
- Virtual machines, files, and folders.
- Application workloads, such as SQL Server and SharePoint.

### Adapting for Microsoft Azure

In the past, our corporate infrastructure was hosted in on-premises datacenters. However, Azure has become the default environment for all CSE solutions. When we develop new solutions, we look at Azure first. By the end of fiscal year 2018, almost 90 percent of our CSE resources will be hosted in Azure. With our organization rapidly migrating and deploying CSE solutions to Azure, the demand for data protection in the cloud has also increased. Although our on-premises data protection methods using System Center Data Protection Manager can be extended into Azure, backing up cloud data to on-premises datacenters introduced several problems that we wanted to address.

Backup and recovery of Azure data depends on network bandwidth between the datacenter and Azure. Backup and recovery times can be significantly impacted by fluctuations in bandwidth, and they are non-functional if the connection to Azure is unavailable. CSE manages 12,000 Azure infrastructure as a service (IaaS) virtual machines in subscriptions. So we recognized the need to develop a solution for data protection. We wanted the solution to provide appropriate service for our Azure users. At the same time, we wanted a manageable and maintainable solution that we can provide for our business groups using Azure now and in the future.

## Protecting data in Azure IaaS

We recognized the need to develop a solution with a high-level approach to protecting data in Azure. To fulfil our new solution, we set several goals:

- Create a solution that enables our employees to quickly obtain access to data protection services for Azure IaaS resources.
- Provide the quickest possible backup and recovery window.
- Leverage built-in Azure components with the least requirement for customization.
- Be flexible enough to meet the data protection needs of all our business groups.
- Be adaptable to future changes in Azure data protection functionality.
- Lower cost by reducing Azure ExpressRoute consumption to back up Azure workloads on-premise.

From these goals, we recognized how our solution in Azure would take form. First, we decided that we wouldn't provide a specific, highly managed service that we would have to mold in an attempt to satisfy all our business groups. Instead, we wanted to provide guidance, standards, and governance around how the business groups should and could use an Azure technology for data protection to reduce overhead and complexity. It would also allow business groups to adapt the solution to fit their needs and create a solution that works best for their organization. Then, based on the governance and guidance, we provided toolsets and support based on Azure best practices and how our business needed to use the technology. We used Microsoft Azure Backup, an Azure-based service to back up and restore data in the Microsoft cloud. It uses Azure Recovery Services vault, a durable, highly available, and massively scalable cloud storage service for protecting Azure IaaS virtual machines.

## Using Azure Recovery Services vault for data protection

Azure Recovery Services vault is an Azure Resource Manager resource to manage your backup and disaster recovery needs natively in the cloud. Recovery Services vault gives us a consistent and unlimited backup for Azure virtual machines at the file, folder, and virtual machine levels. It also provides file and folder backup for on-premises devices.

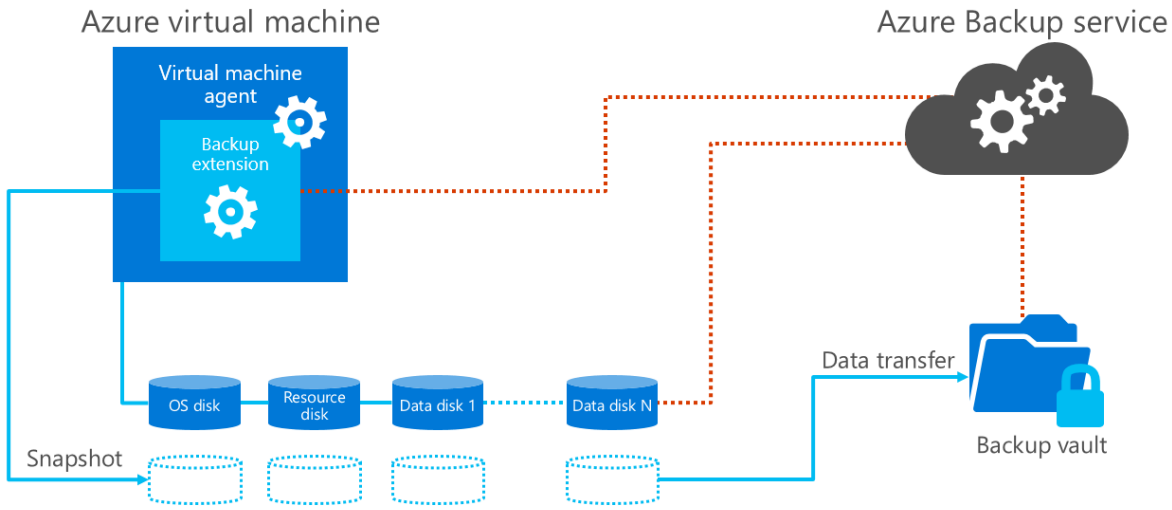


*Figure 1. Primary functions of the Azure Recovery Services vault*

### Important Azure Recovery Services vault features

Azure Recovery Services vault has some important features and functionality that fulfilled several of our goals for data protection. By using these features, we quickly positioned Recovery Services vault as a data protection solution for our business groups. We identified important functionality such as:

- It stores data in Azure datacenters, so backup, recovery, and general data movement happens quickly between virtual machines and the Recovery Services vault.
- It provides built-in functionality for both file and folder backup and the backup of entire virtual machines.
- It fulfills many of our requirements in its default state. It required less customization, and it's a solution that's extensible and more flexible to grow with Azure functionality.
- It uses familiar backup and recovery methods and user interfaces.
- It meets GDPR requirements in that when data resides in the Recovery Service vault, that data is encrypted and protected against malware and ranswomware attacks.

# Creating Recovery Services vault guidance and governance

Using the Recovery Services vault as our standard source for backup and recovery, we created a set of guidelines and governance standards for business groups to follow when using Recovery Services vault for data protection.

## Basic standards

We developed standards to help guide our business units in the optimal use of Recovery Services vault. This included preventing using Recovery Services vault in situations that wouldn't serve the business groups' needs. Among the standards we set, the most important included:

- **A 30-day default retention period for data.** This retention length gave us the best balance between acceptable recovery scenarios and the most efficient use of Recovery Services vault storage and the associated costs.
- **Use Recovery Services vault as an opt-in service.** Business groups aren't mandated to use Recovery Services vault, or to back up certain sets of data. We found that business groups know their data best and can make the best choices on what they back up and how.
- **Use Recovery Services vault to back up mainly IaaS workloads.** If data changes infrequently and you have enterprise-scale amounts of data to be backed up for regular use, our recommendation is not to regularly back up on-premises physical or virtual machines to Azure because it can adversely impact network latency and bandwidth. We do back up small amounts of on-premises data when the case fits, but the greatest value in using Recovery Services vault is when it's used to back up Azure resources within Azure.
- **Treat all data as high priority and high impact.** This standard ensures that we're using sound backup and recovery practices. Nothing gets treated with less security than it should.

## Established SLAs

We also created a set of service level agreements (SLAs) for data protection that our business groups could use as a basis with respect to protecting their data. These SLAs provide the business groups with best practices that they are free to adopt. These SLAs included:

- **98 percent backup success.** 98 percent of all backups will be completed successfully with one recovery point per day for 30 days.
- **100 percent recovery success.** All recoveries will be completed. We didn't establish recovery time objectives, but we guaranteed that recovery processes would be started within four hours of the restore request.

## Power BI reporting

Liaising with the product group, we used Extensible Data Model solutions provided with Azure Backup and ingested corporate data to create a federated reporting model in Power BI. The reports can be consumed by employees at any level in the company to view backup health.

# Recovery Services vault implementation

Our implementation procedures are based on standard Recovery Services vault procedures. Our business groups are free to use any of the existing tools to manage their backup environment, but we also provide pre-planning considerations for using Recovery Services vault.

## Pre-planning

We provide the following pre-planning tips to our business groups for their implementation:

1. Make sure that users understand the guidelines and governance standards.

2. Choose the region where users want the backups to be stored. It's important that users decide this before they start protecting their data. With the current release of Recovery Services vault, users can't back up virtual machines to a different region. Also, billing rates and availability can vary between regions.
3. Protect only what users need. There's a cost involved with each Recovery Services vault that users create. They may have hundreds of virtual machines, but should back up the ones that they think are important—where data loss could impact the business.
4. Carefully choose the retention period. Just because storage is unlimited doesn't mean users can retain data for as long as they want. There are two major factors involved:
    - **Corporate retention policy.** Corporate Records Management dictates retention policies for long-term backups.
    - **Cost of storage.** You are billed for the amount of storage you use in Azure, so you should weigh the benefits of retaining data for longer periods with the cost you'll incur from the required storage.

### Usage options for Recovery Services vault

We offer three primary methods for data protection using Recovery Services vault:

- **File and folder backup and recovery.** You can protect files and folders from within the operating system of your virtual machine using the Azure Backup agent. The agent is installed and managed for each virtual machine. Business groups can use the agent to back up individual files and folders or entire volumes, either as scheduled backups, or on demand.
- **Azure IaaS virtual machine backup and recovery.** With virtual machine recovery, you can back up the virtual machine state to a fully recoverable snapshot in Azure. It provides the most immediate and complete option for full virtual machine recovery. And it can be done using either Azure Portal or Azure PowerShell. With the latest release, you can even perform an item-level recovery of an Azure virtual machine deployed using the Azure Resource Manager model.
- **SQL running on IaaS VMs**. Recently, the product group introduced workload backup for SQL running on IaaS VMs. It uses the same native SQL APIs to do the backups and provides the added advantage of being able to manage all of it through the Azure portal. Seamless discovery and agentless protection has made it one of the best solutions available.

## Looking ahead

The Recovery Services vault gives us a strong feature set and an easy-to-use data protection service for our business groups to protect their Azure IaaS virtual machines. We're anticipating several changes to the way we provide Azure Backup services in the near future. As the offering matures, new Azure features that are related to virtual backup and Azure Recovery Services vault will become available. Some of these include:

- Long-term retention. We're looking at establishing long-term retention policies for data stored in Azure Recovery Services vault.
- Backup for virtual machines that require Sarbanes-Oxley (SOX) compliance. Currently, reporting and monitoring features are still evolving toward an end-to-end monitoring and reporting solution that we require for SOX compliance.
- Application-level data protection. We want to implement backup and recovery for application-based data, such as Exchange and SharePoint, which will be an agentless solution.
- Agentless file and folder backup for files and folders in Azure IaaS virtual machines.
- Incorporating backup and recovery for Azure PaaS services using Recovery Services vault.

# For more information

To get started with Azure Backup to protect your data with a cloud-based backup as a service, see the Backup page on Microsoft Azure.

## Microsoft

microsoft.com/ITShowcase

Azure Backup Documentation