AZURE BACKUP

Service description

Version: January 2025

any.cloud

Table of contents

About any.cloud

Azure Backup is delivered by any.cloud, a provider of simple and scalable cloud ISO-certified solutions on a global scale. any.cloud complies to strict control measures, high security demands and high transparency when it comes to the function and security of Azure Backup.

Established in 1998, any.cloud has a long history in the IT sector, and since the beginning the focus has always been helping customers secure their business ontinuity. With the backup and replication services any.cloud has been a constant player in the market since 2014 and has throughout the years received awards and acknowledgments. In 2021 any.cloud was awarded 'Most Significant VCSP Partner' by Veeam and in 2023 'Nordic Cloud Partner of the Year 2023' by IBM as well as the winner of ''IBM Partner Plus EMEA Award'' in the category of Modernization.

This has made any.cloud an innovative partner – not just following the market trends and products but creating them. Meaning the services are constantly being improved, refined, and developed to match the world of today.

Introduction to Azure Backup

This document provides a detailed functional and technical description of the service and features available for Azure Backup. Azure is Microsoft's public cloud computing platform, a strong multi-functional platform used for networking, storage, analytics, virtual computing and much more. Like all other solutions from Microsoft, Azure is also covered by the shared responsibility model. This means Microsoft is responsible for the infrastructure and the consumer using the platform is responsible for the data processed within the Microsoft environment. This means Microsoft is not accountable for lost data, and that the users need to have their own methods of backup.

Azure Backup is a seamless integration with Microsoft, where native object storage is used to enable backup storage repository. The Azure Backup service provides segregation of duties to the end-customer as the responsibility and access to the backup data is moved from the IT personnel to any.cloud. Data moved to the any.cloud backup service is besides restore capabilities completely separated from the Azure production environment and administrative access from the IT personnel.

TERMINOLOGY	
Microsoft Azure	Microsoft's public cloud computing platform.
Azure Backup	The solution.
Veeam Software	The provider of the backup software used as foundation for Azure Backup.
Microsoft	The provider of the service Azure backup.
any.cloud	The developer and provider of the service.
Backup	The copy of the Azure data.
Restore	The process of replacing a lost or deleted item from a backup.
Segregation of duties	Also referred to as SoD is where access to the data is handled by 3 part.
Resting state	Data when stored.
Transit	Data when processed.
Tenant	The customer environment within Microsoft Azure.
RPO	Recovery Point Objective, defines the acceptable amount of data that can be lost following a disaster.
RTO	Recovery Time Objective, defines the time it takes to recover data following a disaster.
VHD	Virtual hard drive

Functional description of Azure Backup

Azure Backup is managed from a single web-based interface. Azure Backup can be delivered in either a managed or unmanaged model:

Managed

any.cloud personnel manage and maintain the service fully. The managed solution has an additional fee, invoiced monthly. any.cloud has the responsibility of the following:

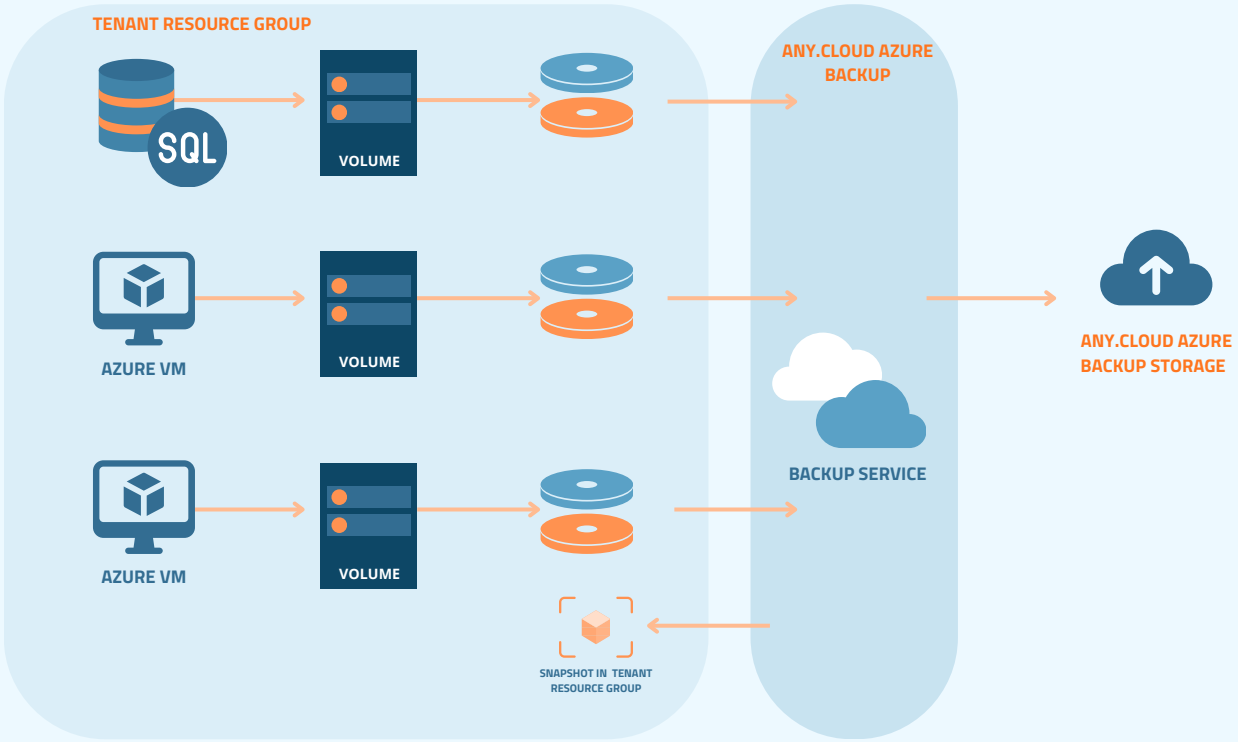
- Daily run of backup jobs with a goal of as many successful backups as possible
- Restores upon request (formal process agrees in-between parties) or Customer have access only to restore
- Responsibility for the backup platform
- Updates of the backup platform
- Uptime of the Azure Backup platform responsibility

Unmanaged

any.cloud personnel maintains the service. any.cloud has the responsibility of the following:

- Responsibility for the Azure Backup platform
- Updates of the backup platform
- Uptime of the Azure Backup platform responsibility

The backup process in technical detail



Azure Backup allows you to create the following types of snapshots and backups:

- Snapshots: managed and unmanaged VHDs of Microsoft Azure VMs, which includes the configuration of a VM
- Backups of managed and unmanaged VHDs of Microsoft Azure VMs, which includes the configuration of a VM

When you run a backup job, the any.cloud backup services will perform the following tasks:

- Retrieve the configuration of your Microsoft Azure VMs that are selected in the policy
- Create either a backup or snapshot for the Microsoft Azure VMs, depending on the policy configuration
- Backups – Both managed/unmanaged VHDs are saved to the configured Backup Repository.
- Snapshots
- Managed VHDs – snapshot saved to resource group of sources VM
- Unmanaged VHDs – snapshots saved to Azure Storage Account of source VHD

For both backups and snapshots, the VM configuration is saved to the Veeam Backup for Microsoft Azure configuration database. The any.cloud backup services, encrypt, and compresses data that you back up to backup repositories.

Backup sources

Azure Backup supports two Azure native instances, Azure Virtual Machines and Applications like Azure SQL Database service. Both are calculated based on a per-instance-model.

VM

Azure Backup produces cloud-native snapshots and image-level backups of VMs. To create backups of Azure VMs, Azure Backup creates backup jobs. A backup job is a collection of settings that define the way backup operations are performed – what to back up, retention periods, where to store it and when to start the backup jobs.

Applications: SQL instances, Postgres SQL.

To create backups of Azure SQL databases, Azure Backup creates backup jobs. A backup job is a collection of settings that define the way backup operations are performed – what to backup, retention periods, where to store it and when to start the backup job. One backup job can process multiple SQL databases within different or the same region.

Please note – Azure Backup does not support backup of databases hosted by Azure Arc-enabled SQL managed instances and SQL Servers on Azure Arc-enabled servers.

Fileshare

Azure Backup ensures the backup of Azure File Shares by automating the backup process and providing easy data recovery through policy-based backup. Backup data is stored in any.cloud Backup via Blob Storage, with security ensured through encryption during both transfer and storage. The solution scales according to demand and optimizes bandwidth and storage costs by transferring and storing only changed data.

Snapshots

Azure Backup supports manually creation of snapshots of Azure VMs that are added to an existing backup job. Each snapshot is saved to the same Azure region where the protected Azure VM reside.

Please note – Azure Backup does not include any snapshots created manually within the backup chain and does not apply the configured retention policy settings to these snapshots. This means that the snapshots are kept within the tenants Microsoft Azure environment until removed manually.

RTO

Regarding backup Recovery Time Objective is an important factor. With Azure Backup, restoring is performed within Microsoft Azure, to ensure a fast recovery, and thereby minimizing the duration of downtime.

Frequency and Retention

Azure Backup starts the backup jobs automatically based on how the scheduler has been defined. The scheduler defines how often the Azure data is being backed up. The following can be chosen:

Frequency:

- Daily — the backup job will create restore points repeatedly throughout a day on specific days.
- Weekly — the backup job will create restore points once a day on specific days.
- Monthly — the backup job will create restore points once a month on a specific day.
- Yearly — the backup job will create restore points once a year on a specific day.

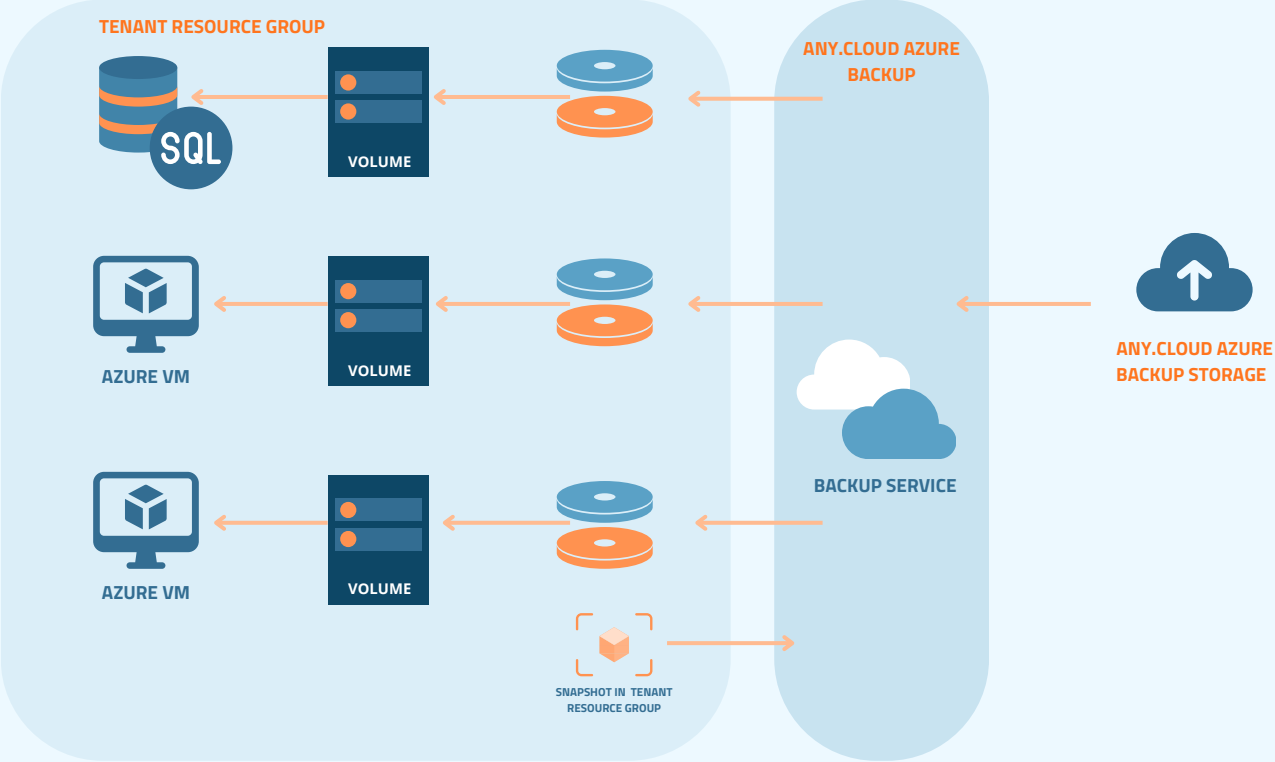
Retention:

- Defined by customer

Encryption

Azure Backup supports encryption End2End & at-rest. The encryption keys are handled by the any.cloud backup service. If advanced requirements for cryptographic keys are needed, Azure Backup supports Azure Key Vault cryptographic key.

The restore process in technical detail



Entire VM restore

In case of worst-case-scenario Azure Backup supports restoring an entire Azure VM from a cloud-native snapshot or image-level backup. One or more Azure VMs can be restored at once, to the original location or to a new location.

Disk restore

Azure Backup supports restoring virtual disks of VMs from cloud-native snapshots or image-level backups. Restores back to the original location or a new location is supported.

File-level recovery

Azure Backup can recover corrupted or missing files of an Azure VM from a cloud-native snapshot or image-level backup. The following file systems are supported:

- Microsoft Windows systems — FAT, FAT32, NTFS.
- Linux systems — ext2, ext3, ext4, XFS, Btrfs.

Azure Backup supports file-level restore only for Microsoft Windows basic volumes.

Please note – If Azure Disk encryption is enabled for the selected virtual disk/VM, any.cloud Backup will not be able to restore the file-level operation.

Azure SQL restore

Azure Backup allows you to restore an Azure SQL database. You can restore one or more databases at once to the original location or to a new location. One restore session can only restore the Azure SQL databases located on the same SQL server. If a different database is needed, a new restore session is required.

Compliance

The purpose of this document is to inform any.cloud A/S's distributors, partners and auditors about the requirements listed in the international standard for assurance engagements regarding assurance reports on controls at a service organization. any.cloud is an ISO 27001 certified company with an SLA formed by the regulations and requirements based on ISO 27001. any.cloud is a certified member of the Cloud Security Alliance (CSA STAR) and has an ISAE 3000 assurance report made by an independent external auditor every year.

Azure Backup is developed by any.cloud, and the service complies with the General Data Protection Regulation and standards listed above. With Azure Backup your Azure workloads are protected by both industry and best-practices standards with military grade encryption and security built-in and with SoD and air-gapped protection. Access to the Azure Backup and the data are kept to a minimum philosophy. Access to the actual data is not possible by the customer or reseller, without a formal written request that has built-in validation processes to ensure that any kind of access only happens to the authorized persons.

ISO 27001

any.cloud is certified within the ISO 27001 framework. Working with the framework of standards in how to manage their information and data. As a cornerstone in any.cloud's business, risk-management is key to all actions any.cloud performs.

ISAE 3000

any.cloud holds an independent auditor's report. The ISAE 3000 is a control report that controls any.cloud under the ISO standards and GDPR legislation. This generates a fully public report that confirms any.cloud's actions and internal processes.

CSA

The membership of CSA is an addition to the official certifications and auditing reports. By being a member of CSA any.cloud holds an CAIQ – a questionnaire that answers most security and compliance questions that any.cloud partners and customers have.

Pricing

Azure Backup has 3 pricing points:

PRICING POINT 1:

The number of instances (VM and/or SQL)

PRICING POINT 2:

The number of allocated TBs in backup

PRICING POINT 3:

Number of workers is defined by daily amount of incoming/outgoing data, number of R/W and how many daily backups needed.

Additional cost on Workers can occur if R/W exceeds 250.000 R/W per day and size of data moved per worker exceeds 1 TB pr day.

Choosing Azure Backup

- Protect your data with secure cloudnative backup
- Quickly overcome any data loss using full- and filelevel recovery
- Azure Backup workloads with SoD and air-gapping built-in natively
- Secure your data away from the MS tenant and Protect from insider treats and other malicious attacks

Azure is delivered in a backup model, which allow for one Azure tenant to back up to another Azure tenant. Making sure Azure data residing in the Microsoft environment is safely backed up This ensures data availability and allows for restore in case of lost or deleted data. More importantly, it allows for segregation of duties as well as air-gapped backups.

LET'S STAY CONNECTED

Anycloud A/S
Hedegaardsvej 88
2300 Copenhagen S
Denmark

CVR: DK31161509
E-mail: sales@anycloud.dk

any.cloud