SQL SAFE FOR THE HYBRID CLOUD

SQL SAFE FOR THE HYBRID CLOUD

As organizations migrate their data to the cloud, database administrators need to consistently manage data on-premise and in the cloud with existing staff and tools. Typical concerns with migration to the cloud are moving data to the cloud without impacting performance, determining the best settings, configuring for high availability and disaster recovery, balancing performance and cost, and managing data in the cloud and on-premise without learning multiple tools.

There is no need to fear the cloud when managing the performance and availability of data in the cloud and on premise with a single tool. By eliminating the steep learning curve associated with new tools for the cloud, free up time for new organizational needs, adopt data in the cloud confidently, and avoid making critical errors with data in the cloud.

Automate backups for SQL Server and recover data from backups without restoring with SQL Safe Backup.

With IDERA SQL Safe Backup, automate backups and restores of Microsoft SQL Server, and recover data without restoring. SQL Safe Backup runs on cloud virtual machines with Microsoft Windows. It can access mapped cloud drives. It backs to and restores from instances of SQL Server on cloud virtual machines, and the cloud databases Amazon Simple Storage Service (S3) and Microsoft Azure Blob Storage.

Install on Cloud Virtual Machines

SQL Safe Backup runs on cloud virtual machines with Windows –
such as Amazon Elastic Compute Cloud (EC2) and Azure Virtual Machines.

Refer also to the product documentation Installation and deployment.
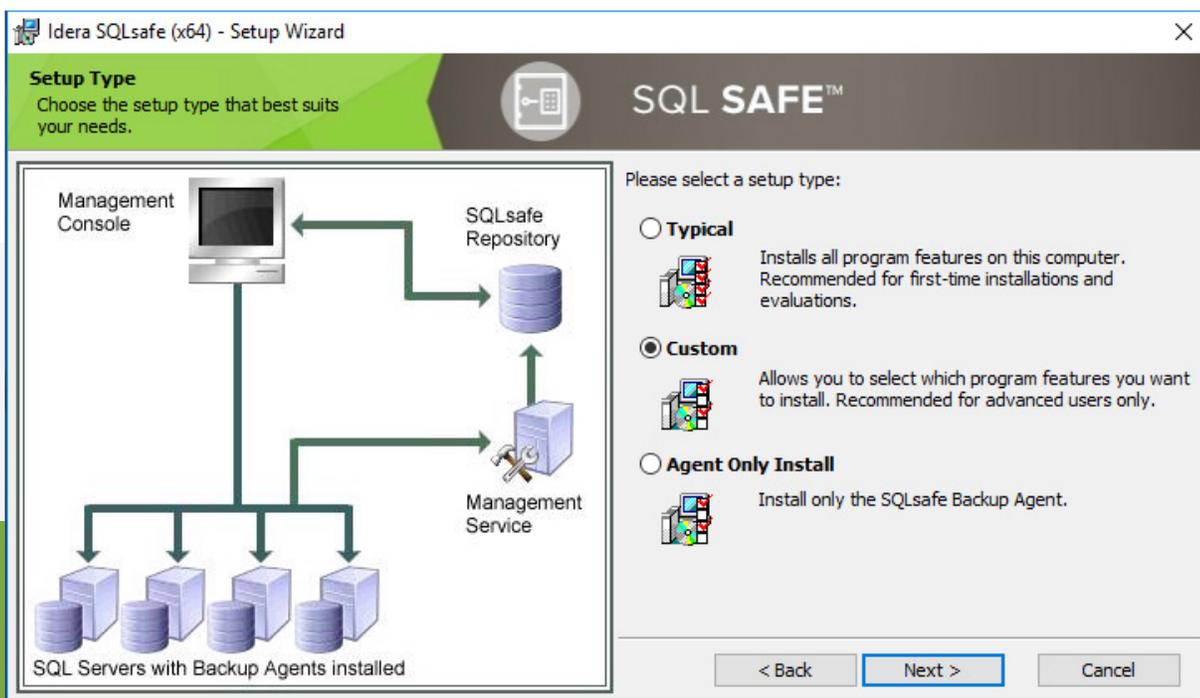
The Setup wizard.

Access Mapped Cloud Drives

SQL Safe Backup can access cloud storage that third-party software map as network drives or removable drives on Windows. Examples of such third-party software include [CloudBerry Drive](#) and [Mountain Duck](#) for Amazon S3 and Azure Blob Storage.

SQL Safe Backup supports the following location types for automatic and manual backups: A single file on the local computer or a network share, multiple striped files on different locations on the local computer or a network share, Amazon S3, and Azure Blob Storage. Consequently, it is possible to back up to and restore from a network drive that is mapped to the cloud or directly to the cloud.

Refer to the section "Support Amazon S3 and Azure Blob Storage" on the next page for details concerning how to specify the locations of the backup files.
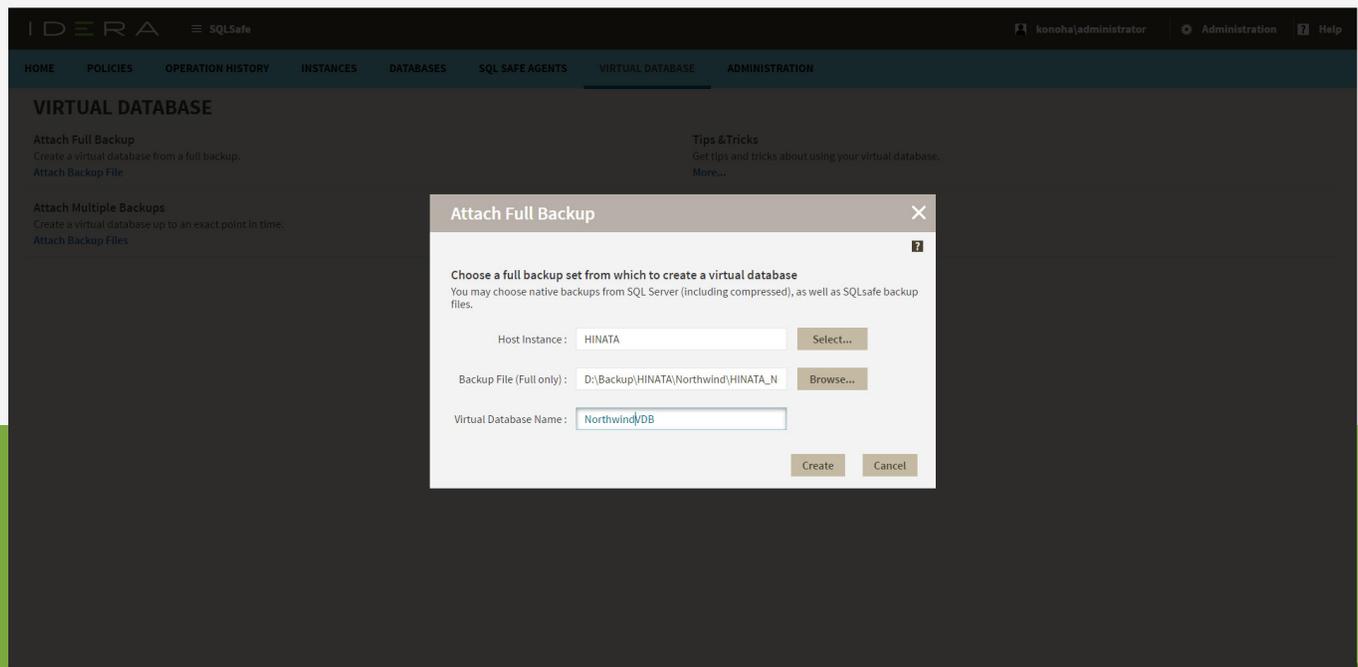
Access cloud drives as network drives.

Support SQL Server on Cloud Virtual Machines

SQL Safe Backup supports backing up to and restoring from instances of SQL Server running on cloud virtual machines (such as Amazon EC2 and Azure Virtual Machines).

Connect to instances of SQL Server on physical machines, virtual machines, and cloud virtual machines.

Support Amazon S3 and Azure Blob Storage

Backups

SQL Safe Backup supports the following location types for automatic and manual backups:
A single file on the local computer or a network share, multiple striped files on different locations
on the local computer or a network share, Amazon S3, and Azure Blob Storage. For automatic
backups, use the "Locations" tab of the "Backup Policy" wizard to specify the location of the backup
files for each operation included in the backup policy. For manual backups, use the "Locations"
tab of the "Backup" wizard to specify the location of the backup files for each operation included
in the backup.

Refer also to the product documentation Selecting location for the "Backup Policy" wizard
and Selecting the location of your backup files for the "Backup" wizard of the web console,
and Select location for the "Backup Policy" wizard and Select location for manual backup
for the "Backup" wizard of the desktop console.
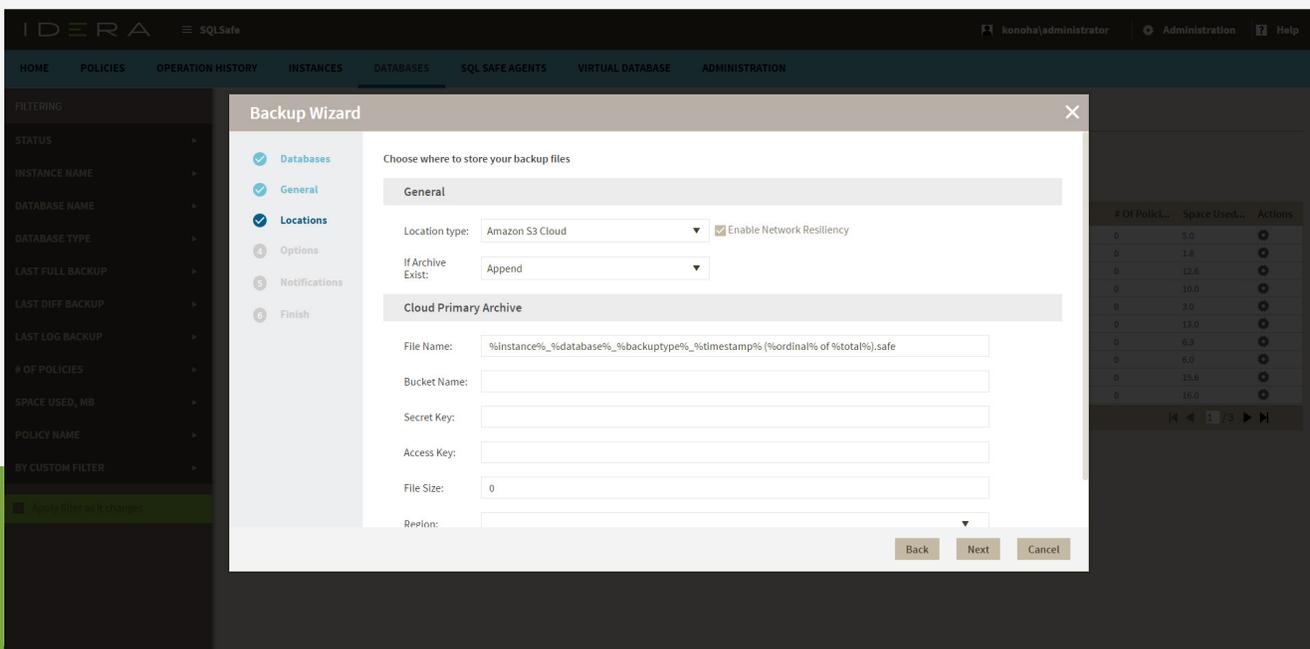
The "Locations" tab of the "Backup" wizard.

Restores

SQL Safe Backup supports the following location types for automatic and manual restores, and manually restoring object level recovery: A repository, a local drive or network share on a local file system, a network share on a remote file system, Amazon S3, and Azure Blob Storage. For automatic restores, use the "Source" tab of the "Restore Policy" wizard to specify the location of the backup files. For manual restores, use the "Databases" tab of the "Restore" wizard to specify the location of the backup files.

Refer also to the product documentation Selecting databases you want to restore for the "Restore Policy" wizard, and Selecting the databases you want to restore and Restoring Object Level Recovery for the "Restore" wizard of the web console, and Select the database you want to restore for the "Restore Policy" wizard and Select the databases you want to restore for the "Restore" wizard of thevdesktop console.
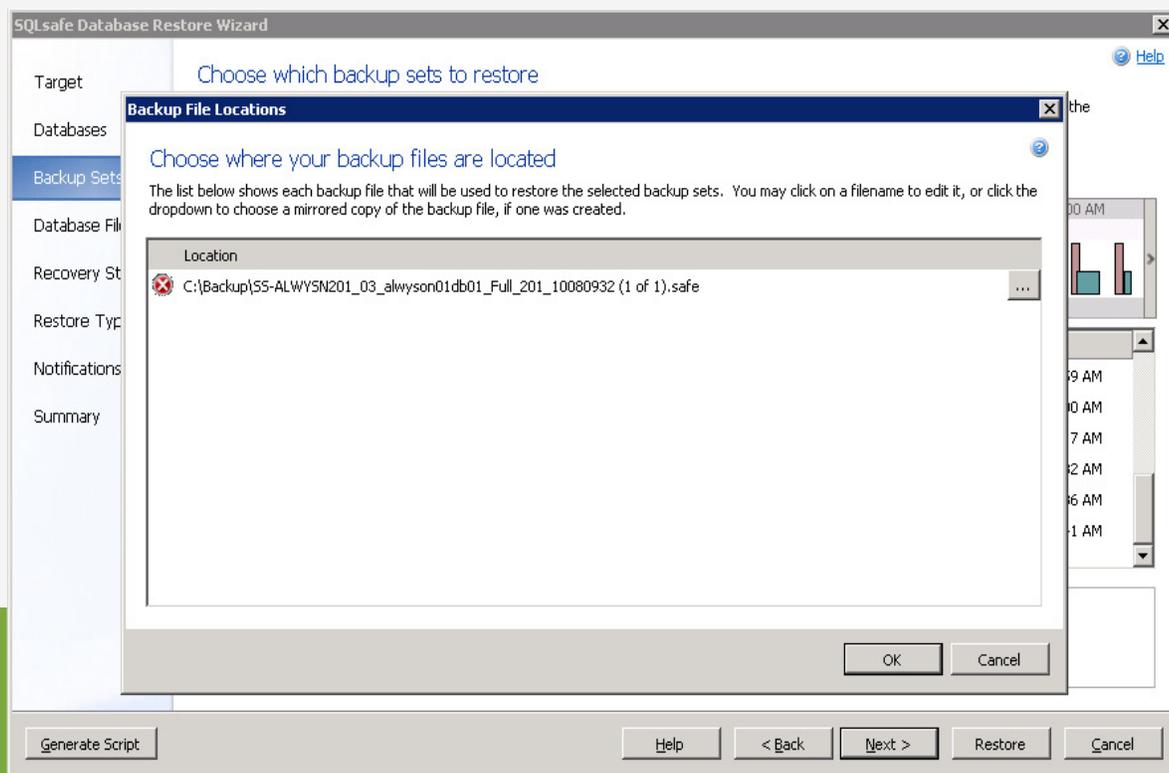
The "Backup File Locations" window of the "Backup Sets" tab of the "Restore" wizard.

Virtual Databases

For attaching full backups and for attaching multiple backups, use the "Attach full backup" option and the "Attach multiple backups" option, respectively, of the "Virtual Database" tab to specify the location of the backup files.

Refer also to the product documentation Attach Full Backup and Attach Multiple Backups for the web console.
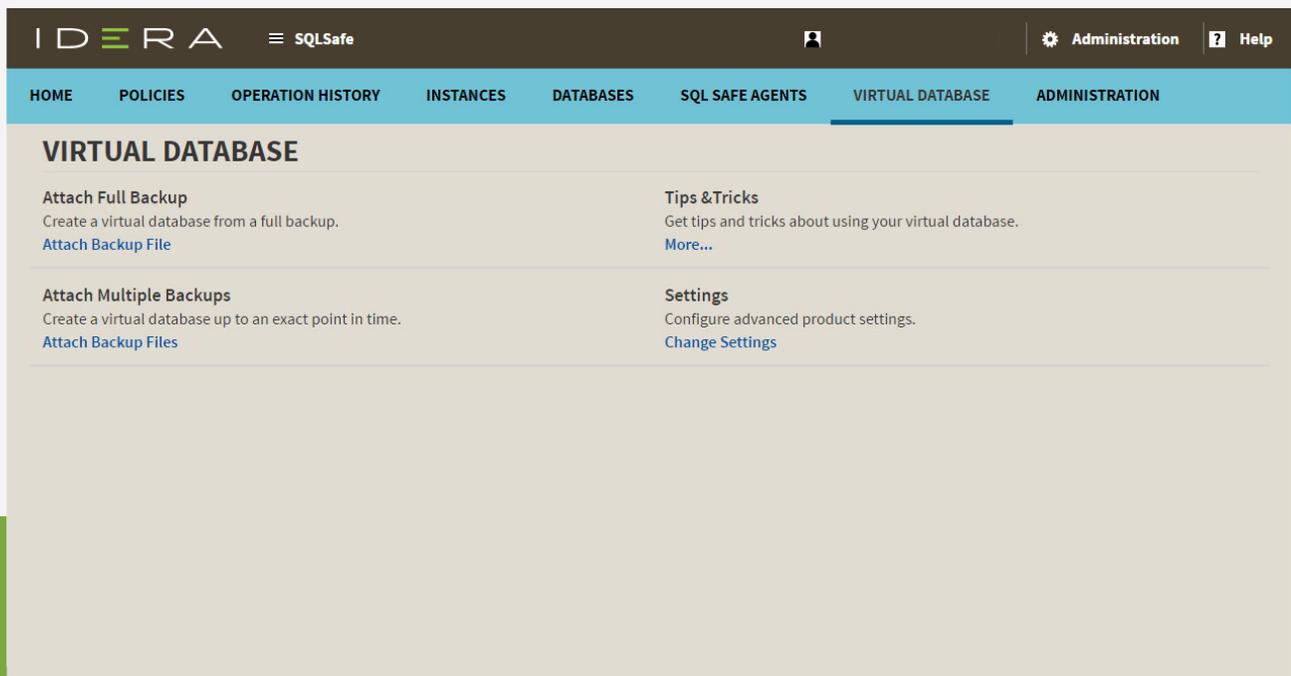
The "Virtual Database" tab.

General Preferences

For general preferences for all subsequent backups and restores, specify the settings for Amazon S3 and Azure Blob Storage in the "Cloud Settings" tab and the "Azure Settings" tab, respectively, of the "Configure General Preferences" option of the "Administration" tab of the web console, and the "Cloud Settings" option of the "Management Console Preferences" window of the "Tools" menu of the desktop console.

Refer also to the product documentation Cloud Settings and Azure Settings for the web console, and Configure Console preferences for the desktop console.
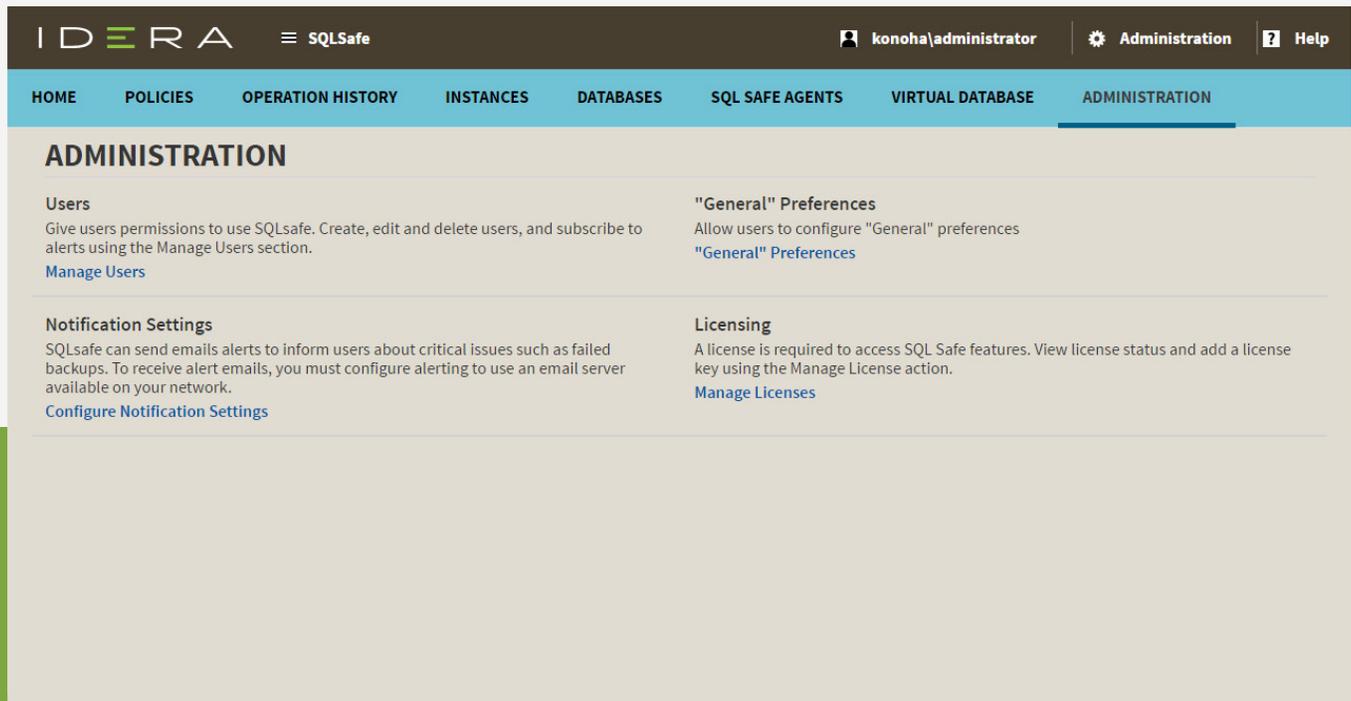
The "Administration" tab.

Amazon S3

When selecting Amazon S3 Cloud as the location for backup files, specify the following fields:

- Append/overwrite: Select to append the backup archive to an existing one or to overwrite it.

- Bucket name: Define the name of the Amazon S3 bucket to store the backup.

- Secret key: Specify the secret key generated in the security credentials of the Amazon S3 web console. Refer also to the AWS documentation "Managing Access Keys for Your AWS Account".

- Access key: Specify the access key generated in the security credentials of the Amazon S3 web console. Refer also to the AWS documentation "Managing Access Keys for Your AWS Account".

- File size: Specify the minimal parts of the backup file in bytes to send to the Amazon S3 bucket simultaneously.

- Region: Select the region to store the backup. Refer also to the AWS documentation "Amazon Simple Storage Service (Amazon S3)".

- File name: Define the name of the location to store the backup.

Refer also to the product documentation Selecting location and Cloud Settings for the web console, and Configure Console preferences for the desktop console.
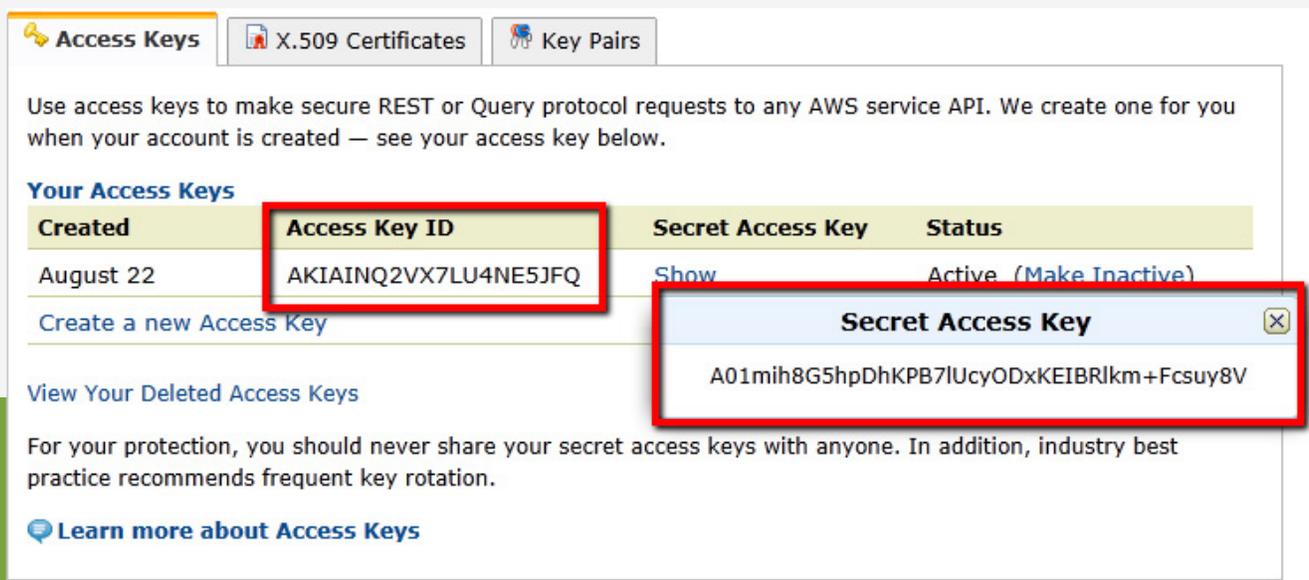
The access key ID and secret access key in the Amazon S3 web console.

Amazon S3 Regions

OREGON 3 2
N. CALIFORNIA 3
AWS GOVCLOUD
OHIO (Coming soon) 5
UK (Coming soon)
N. VIRGINIA
IRELAND 3 2
FRANKFURT
SÃO PAULO 3
INDIA (Coming soon)
NINGXIA (Coming soon)
BEIJING 2 2
SEOUL 3
TOKYO
SINGAPORE 2
SYDNEY 2

(legend) Region & Number of Availability Zones

New Region Coming Soon
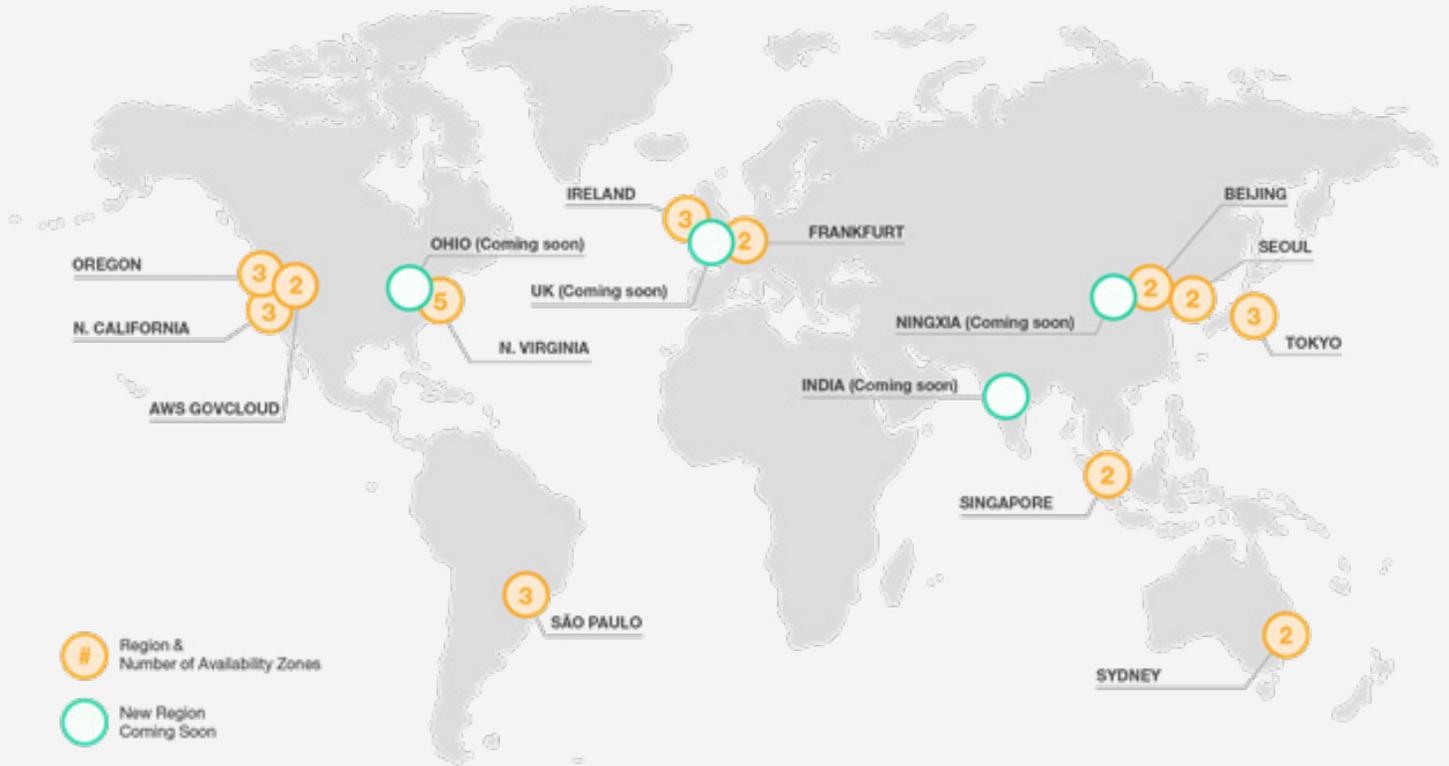
Azure Blob Storage

When selecting Azure Blob Storage as the location for backup files, specify following fields:

- **Container name:** Define the name of the Azure container to store the backup. Every blob in Azure Blob Storage must reside in a container. The container forms part of the name of the blob. Refer also to the Microsoft documentation Quickstart: Upload, download, and list blobs using .NET.

- **Azure storage account name:** Specify the name of the account of the storage account. Every object stored in Azure Storage has a unique URL address. The storage account name forms the subdomain of that address. Refer also to the Microsoft documentation Create a storage account > Storage account endpoints.

- **Azure access key:** Specify the access key to the Azure Storage Account. Refer also to the Microsoft documentation Create a storage account > View and copy storage access keys.

- **File name:** Define the name of the location of the primary backup archive.
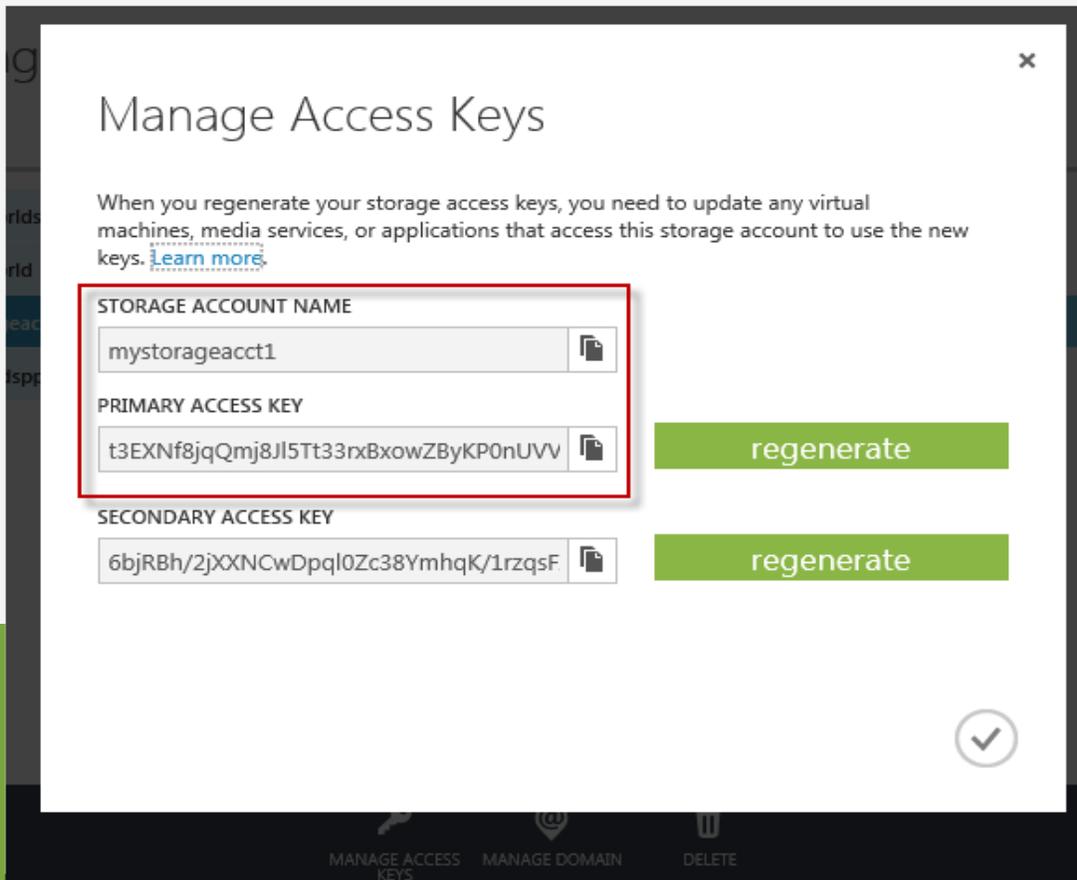
The storage account name and access key for Azure Blob Storage.

Azure Blob Storage, Continued.

Network Resiliency

When enabling the network resiliency settings and using Azure Blob Storage for backup operations, only the following parameters are applicable:

- **Retry Interval:** Specify the waiting period before retrying the backup operation.
- **Total Retry Interval:** Specify the total time for retrying the backup operation before stopping it.

In restore operations, the resiliency settings remain enabled.

Naming Conventions for Containers

Follow the following naming conventions for the names of the containers:

- The name of the container needs to be a valid domain name system name.
- The name of the container needs to start with a letter or number and can contain only letters, numbers, and the dash "-" character
- Immediately precede and follow every dash "-" character by a letter or number. The names of containers cannot contain consecutive dashes.
- All letters need be in lowercase.
- The name of the container needs to have a character length from three to 63.

Blob Names and Blob Sizes

The maximum size for a blob is 70 MB. When a backup file has a size of (for example) 160 MB, SQL Safe Backup creates multiple blobs using the naming format "<blobname>.safe_<i>" where "<i>" represents the counter for the blob.

When the blob name is (for example) "testdb", the three blobs created in the container will have the names "testdb.safe_1(70MB)", "testdb.safe_2(70MB)", and "testdb.safe_3(20MB)".

Refer also to the product documentation Selecting location and Azure Settings for the web console, and Configure Console preferences for the desktop console.

SQL SAFE BACKUP

With SQL Safe Backup, automate backups of entire SQL Server environments, choose from multiple options for recovery, ensure organizational compliance with backup and recovery policies, reduce failures due to temporary network problems, and turn backup files into virtual databases to query and modify data without restoring, and much more. Install and deploy SQL Safe Backup to meet the unique needs of any SQL Server environment.

Start for FREE

Manage backups, restores, and virtual databases for SQL Server with SQL Safe Backup.