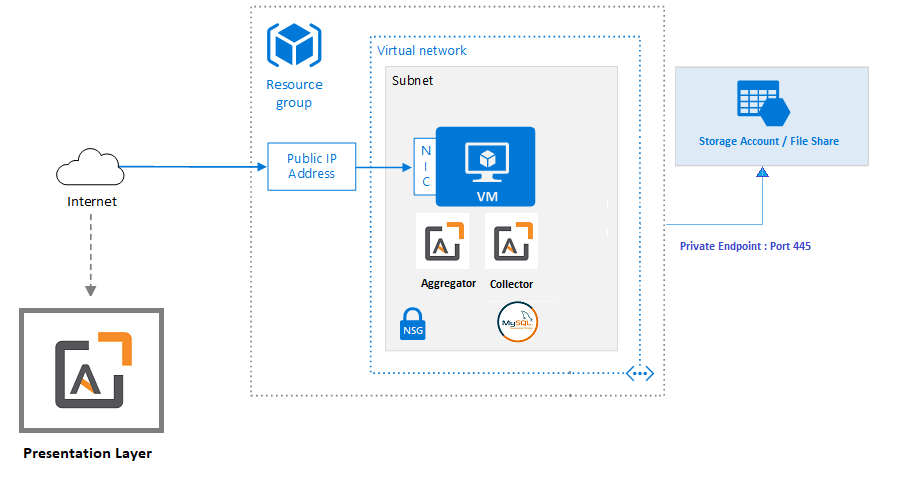
# Setup for Microsoft Azure Storage Account for use with Aparavi Agent/Collector

# Purpose

Microsoft Storage Account and its file share services can be connected via the Server Message Block (SMB) protocol using the Aparavi Agent/Collector and configured to search for unstructured data. The benefit of this method is the great flexibility in designing an individual infrastructure architecture, which can also bring cost advantages.

The following description of the setup assumes that an Aparavi Agent or Collector is already installed on a supported operating system and connected and online in the Aparavi Presentation Layer. After successfully setting up the Microsoft Azure storage account with a public endpoint using port 445, only the path and credentials for the storage account need to be specified. The data is then scanned either automatically or manually from the Aparavi Presentation Layer, as required.

# Use/Architecture

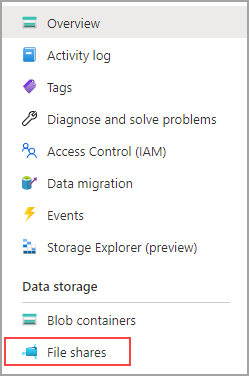


# Setup

This article assumes that you have already created an Azure subscription. If you don't already have a subscription, then create a [free account](https://azure.microsoft.com/de-de/free/?WT.mc_id=A261C142F) before you begin.

# Create a storage account and file share

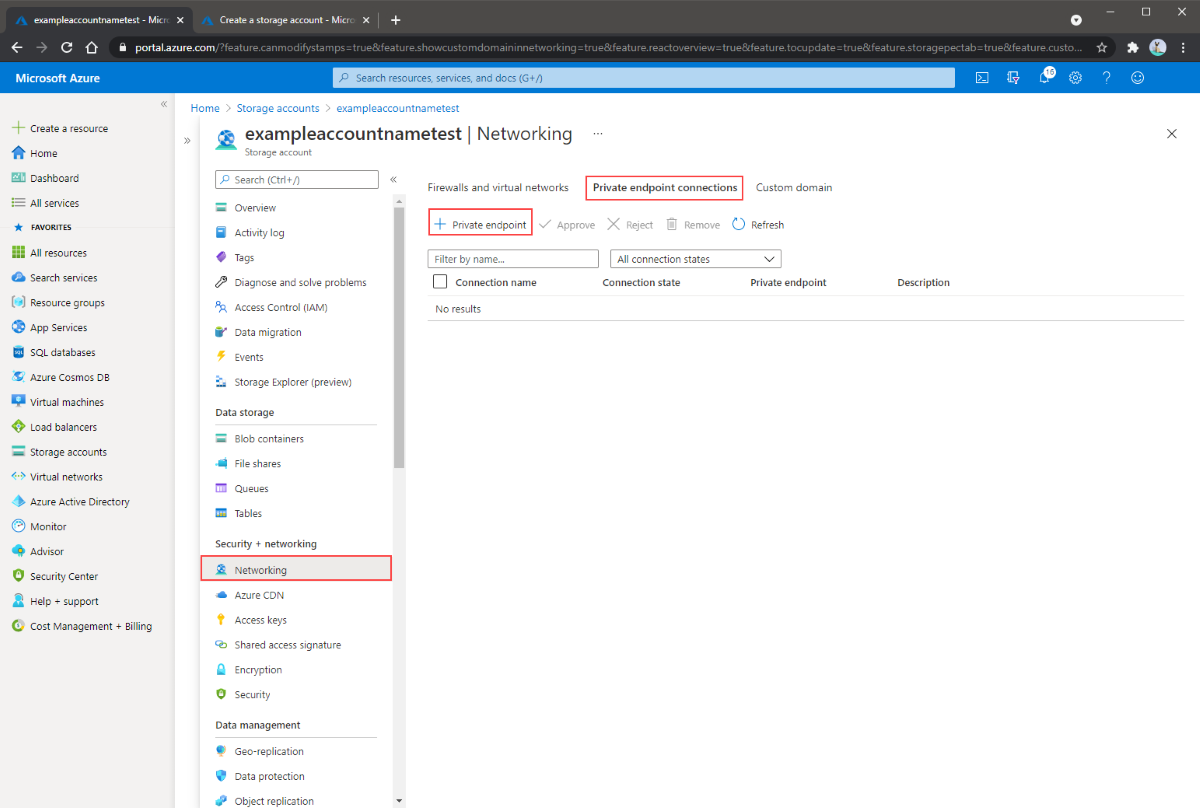
* 1. On the Azure portal menu, select All services. In the list of resources, type Storage Accounts. As you begin typing, the list filters based on your input. Select Storage Accounts.
  2. On the Storage Accounts window that appears, choose + New.
  3. On the Basics blade, select the subscription in which to create the storage account.
  4. Under the Resource group field, select your desired resource group, or create a new resource group. For more information on Azure resource groups, see Azure Resource Manager overview.
  5. Next, enter a name for your storage account. The name you choose must be unique across Azure. The name also must be between 3 and 24 characters in length and may include only numbers and lowercase letters.
  6. Select a region for your storage account or use the default region.
  7. Select a performance tier. The default tier is Standard.
  8. Specify how the storage account will be replicated. The default redundancy option is Geo-redundant storage (GRS). For more information about available replication options, see Azure Storage redundancy.
  9. Additional options are available on the Advanced, Networking, Data protection, and Tags blades. To use Azure Data Lake Storage, choose the Advanced blade, and then set Hierarchical namespace to Enabled. For more information, see Azure Data Lake Storage Gen2 Introduction.
  10. Select Review + Create to review your storage account settings and create the account.
  11. Select Create. Ein Bild, das Text enthält.

      Automatisch generierte Beschreibung
  12. When the Azure storage account deployment is complete, select Go to resource.
  13. Select File shares from the storage account pane. 
  14. Select File shares.
  15. Select + file share to create a new file share.

More information: [Create an Azure file share - Azure Files | Microsoft Docs](https://docs.microsoft.com/en-us/azure/storage/files/storage-how-to-create-file-share?tabs=azure-portal)

# Create a private endpoint

Creating a private endpoint for your storage account will result in the following Azure resources being deployed:

* A **private endpoint:** An Azure resource representing the storage account's private endpoint. You can think of this as a resource that connects a storage account and a network interface.
* A **network interface (NIC):** The network interface that maintains a private IP address within the specified virtual network/subnet. This is the exact same resource that gets deployed when you deploy a virtual machine, however instead of being assigned to a VM, it's owned by the private endpoint.
* A **private DNS zone:** If you've never deployed a private endpoint for this virtual network before, a new private DNS zone will be deployed for your virtual network. A DNS A record will also be created for the storage account in this DNS zone. If you've already deployed a private endpoint in this virtual network, a new A record for the storage account will be added to the existing DNS zone. Deploying a DNS zone is optional, however highly recommended, and required if you are mounting your Azure file shares with an AD service principal or using the FileREST API.
  1. Navigate to the storage account for which you would like to create a private endpoint. In the table of contents for the storage account, select Networking, Private endpoint connections, and then + Private endpoint to create a new private endpoint. 
  2. In the Basics blade, select the desired resource group, name, and region for your private endpoint. These can be whatever you want, they don't have to match the storage account in any way, although you must create the private endpoint in the same region as the virtual network you wish to create the private endpoint in. Ein Bild, das Text enthält.

     Automatisch generierte Beschreibung
  3. In the Resource blade, select the radio button for Connect to an Azure resource in my directory. Under Resource type, select Microsoft.Storage/storageAccounts for the resource type. The Resource field is the storage account with the Azure file share you wish to connect to. Target sub-resource is file, since this is for Azure Files.
  4. The Configuration blade allows you to select the specific virtual network and subnet you would like to add your private endpoint to. You must select a distinct subnet from the subnet you added your service endpoint to above. The Configuration blade also contains the information for creating/update the private DNS zone. We recommend using the default privatelink.file.core.windows.net zone. Ein Bild, das Text enthält.

     Automatisch generierte Beschreibung

# [OPTIONAL] Verify connectivity

* 1. You can test your private endpoint by running the following commands from PowerShell. You must replace <storage-account-name> with the appropriate storage account name:

nslookup <storage-account-name>.file.core.windows.net

**Output:**

Server: UnKnown

Address: 10.2.4.4

Non-authoritative answer:

Name: storageaccount.privatelink.file.core.windows.net

Address: 192.168.0.5

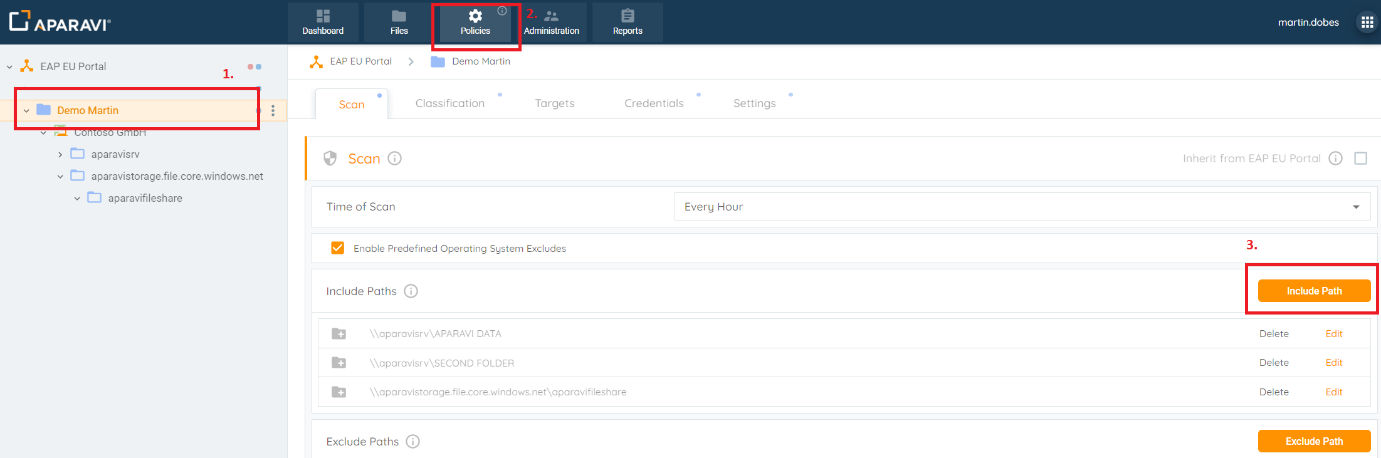
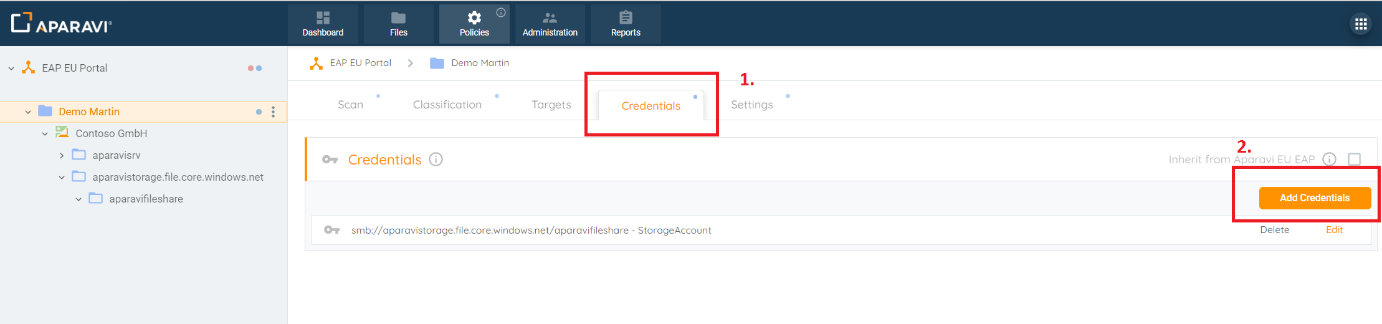
Aliases: storageaccount.file.core.windows.net

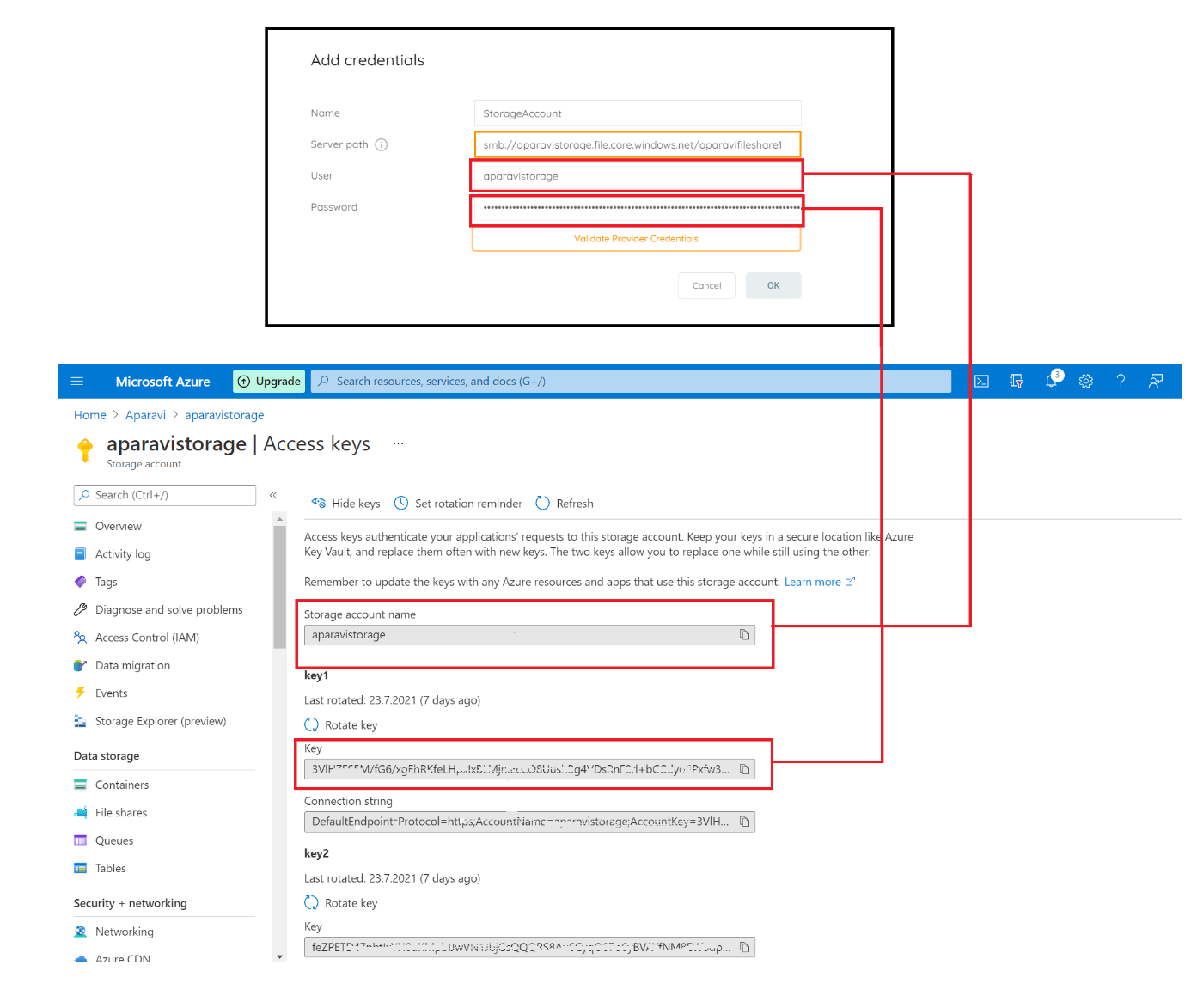
# Setup Of Aparavi Agent / Collector

This article assumes that you have already successfully installed an Aparavi Aggregator and a Collector, or an Agent and that the corresponding client is online.

# Definition of the crendentials in Aparavi Presentation Layer for the use with Microsoft Azure Storage Account

1. Log in to the Aparavi Presentation Layer
2. Check the status of the Agent / Collector and make sure that it is onlineEin Bild, das Text enthält.

   Automatisch generierte Beschreibung
3. Chose your client and select “Policies”. Then, chose “Include Path”.
4. The correct path definitions follow this rule: \\<NAME OF THE STORAGE ACCOUNT>.file.core.windows.net\<NAME OF THE FILE SHARE>, example: [\\aparavistorage.file.core.windows.net\aparavifileshare](file:///\\aparavistorage.file.core.windows.net\aparavifileshare)
5. After this step, set the correct credentials for the storage account.
6. Switch to “Credentials” and click the button “Add Credentials”.
7. The “User” corresponds to the name of the Azure Storage Account. The “Password” requires the “Key” of the Azure Storage Account which can be find in the Azure Portal.



Now, it is possible to migrate your test data to the Azure Storage Account and connect the data with the Aparavi Platform.

You can use the Microsoft Storage Account Explorer for data migration. [Azure Storage Explorer – cloud storage management | Microsoft Azure](https://azure.microsoft.com/en-us/features/storage-explorer/#overview)