2021

StealthAUDIT®

AnyData_AzureBlobs User Guide v1.0

300 Spectrum Center Drive, Suite 200, Irvine, California | (949) 407-5125

Contents

Copyright 2021 NETWRIX ALL RIGHTS RESERVED

Introduction

This document is designed to enable a user to install, configure, and execute AnyData_AzureBlobs in their environment. AnyData_AzureBlobs connects to an Azure Storage tenant and scans files stored in blob storage (“hot” access tier) for sensitive data, including images using Optical Character Recognition (OCR).

AnyData then aggregates sensitive data scan results into a view within the StealthAUDIT Access Information Center (AIC), which will show the subscriptions, resource groups, storage accounts, containers, and blob hierarchy of the scanned Azure Storage tenant, which files contain sensitive data, which sensitive data criteria were found, and, optionally, the specific sensitive strings of text that were found within each blob.

IMPORTANT: AnyData jobs do not support StealthAUDIT's job history functionality. For each AnyData job, ensure job history has been disabled (which will override global job history settings). Failure to disable job history for an AnyData job may result in data inaccuracies after multiple runs.

Copyright 2021 NETWRIX ALL RIGHTS RESERVED

AnyData for Azure Storage (Blobs)

This document describes the process for installing and configuring AnyData_AzureBlobs into an environment where the StealthAUDIT Management Platform and AIC are already installed and running.

Prerequisites

Prior to adding the AnyData_AzureBlobs job to your StealthAUDIT environment, confirm you have administrator rights on the StealthAUDIT server, as well as enough rights to download or copy files to the server.

You will need:

1. StealthAUDIT 11.5.0.127+
2. Access to StealthAUDIT server & SQL Server administrator accounts.
3. The following PowerShell modules installed on the StealthAUDIT server:
   a. Az.Accounts
   b. Az.Storage
   c. Az.Resources
4. Access to an Azure Active Directory user with permission to set IAM roles on desired resources.
5. Access to the target Azure tenant via Azure's REST API, from the StealthAUDIT server.
6. An Azure Active Directory app registration with the following roles assigned to the resources intended to be scanned by AnyData (by default, Azure resources inherit roles from parent resources).
   a. Role assignment: Reader
   b. Role assignment: Reader and Data Access

Configuration

Creating an App Registration in Azure

To scan Azure Storage (Blobs) with a least privilege model, an app registration is required with the **Reader** and **Reader and Data Access** roles assigned to it for the resources intended to be scanned by AnyData.

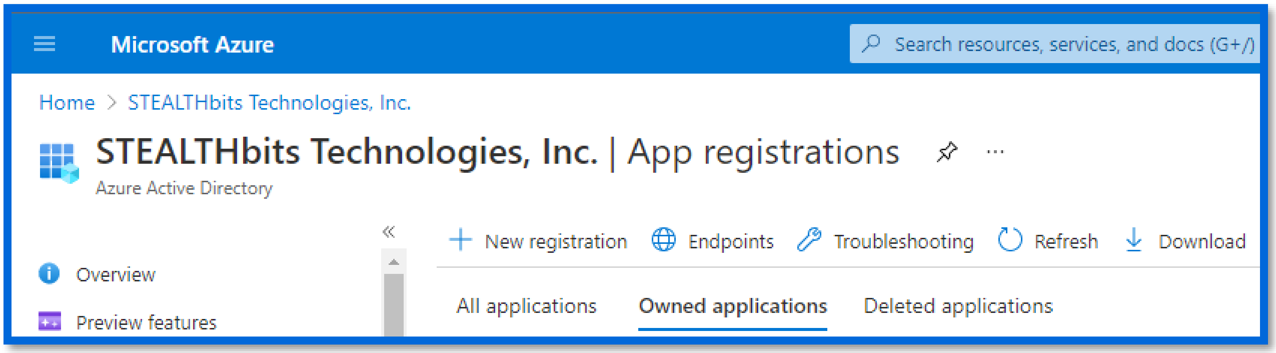
This role can be assigned using the **Access control (IAM)** option for a resource object in Azure, such as a Management Group, Subscription, Resource Group, Storage Account, or Container.

Copyright 2021 NETWRIX ALL RIGHTS RESERVED

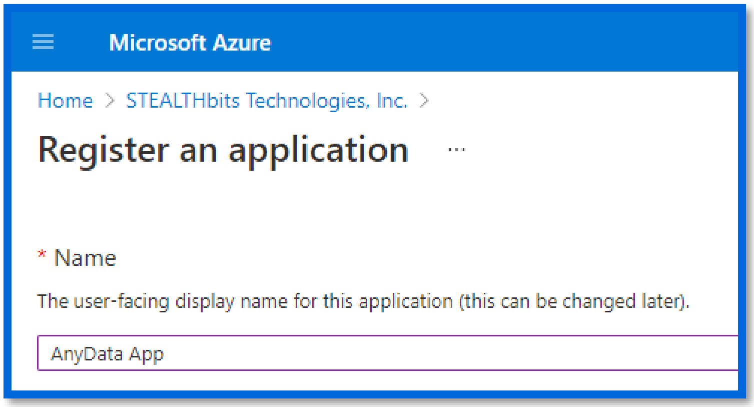
It's recommended to assign this role at the Management Group level in order to scan all files in all blobs in an Azure tenant, however IAM roles can be assigned to the app registration at any level to fit an organizations security and scoping needs.

Step 1 – Log-in to the Azure Portal with an account that has admin privileges in your Azure tenant.

Step 2 – Navigate to **Azure Active Directory > App Registrations** in the left sidebar and create a **New Registration**. This will be the service account used to read data in each blob.



The app can have any name and other settings can be left as defaults. Click **Register** when finished.



* Name

The user-facing display name for this application (this can be changed later).

AnyData App

Step 3 – In the Azure search bar, search for the resource object you'd like to grant this app registration **Reader** and **Reader and Data Access** to.

Depending on where you give the app registration these roles in the hierarchy of Azure, this will grant the app registration read access to all blobs underneath that scope.

In Azure (and for the purposes of AnyData), the resource hierarchy is:

Management Group > Subscription > Resource Group > Resource > Container > Blob

This is exemplified in broader terms in the image below.

Copyright 2021 NETWRIX ALL RIGHTS RESERVED

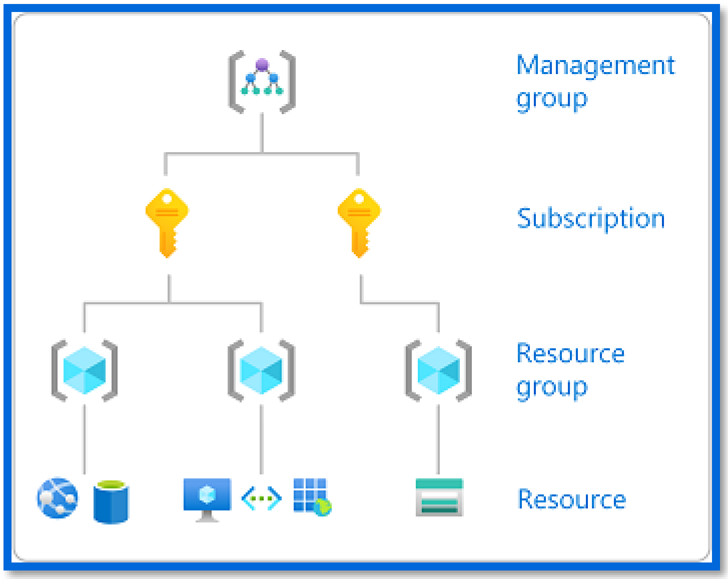
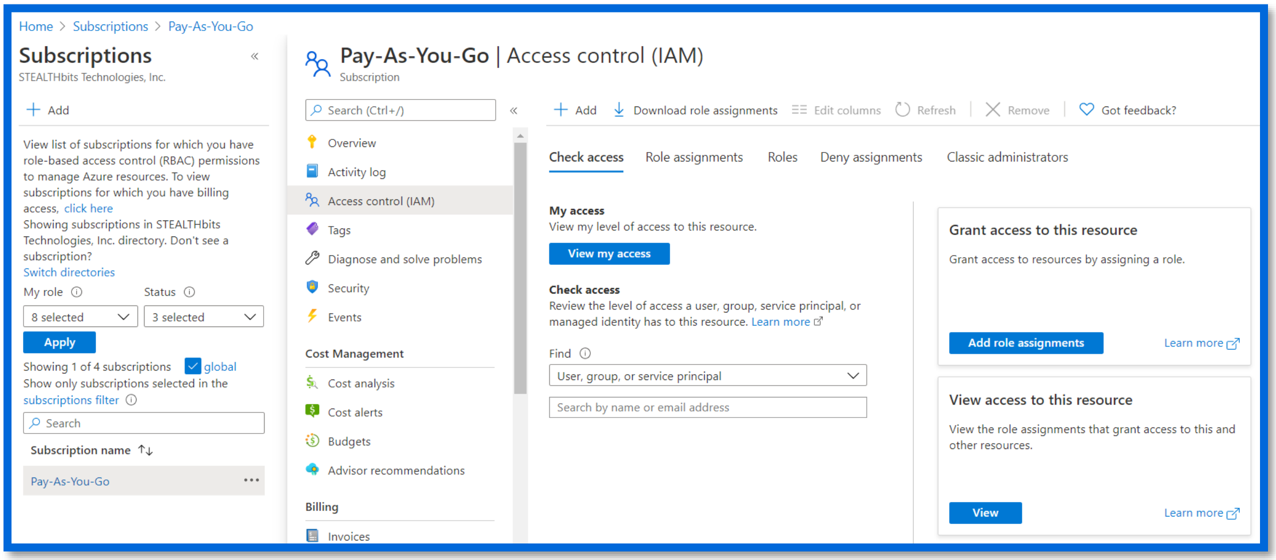


Image courtesy of Microsoft's online Azure documentation

To allow the app registration read access to all blobs in the broadest scope, search for **Management Group**. These steps can be applied to any of the resource object IAM scopes in Azure.

Step 4 – In the resource object, click on **Access control (IAM)** > **Check access** > **Add role assignments**.



Home > Subscriptions > Pay-As-You-Go

Subscriptions
STEALTHbits Technologies, Inc.

+ Add

View list of subscriptions for which you have role-based access control (RBAC) permissions to manage Azure resources. To view subscriptions for which you have billing access, click here

Showing subscriptions in STEALTHbits Technologies, Inc. directory. Don't see a subscription? Switch directories

My role: 8 selected
Status: 3 selected

Apply

Showing 1 of 4 subscriptions ☑ global

Show only subscriptions selected in the subscriptions filter

Search

Subscription name

Pay-As-You-Go

Pay-As-You-Go | Access control (IAM)
Subscription

Search (Ctrl+/)

Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Security
Events

Cost Management
Cost analysis
Cost alerts
Budgets
Advisor recommendations

Billing
Invoices

+ Add | Download role assignments | Edit columns | Refresh | Remove | Got feedback?

Check access | Role assignments | Roles | Deny assignments | Classic administrators

My access
View my level of access to this resource.
View my access

Check access
Review the level of access a user, group, service principal, or managed identity has to this resource. Learn more

Find: User, group, or service principal
Search by name or email address

Grant access to this resource
Grant access to resources by assigning a role.
Add role assignments | Learn more

View access to this resource
View the role assignments that grant access to this and other resources.
View | Learn more

Step 5 – For **Role**, select **Reader**. For **Assign access to**, select **User, group, or service principal**. For **Select Members**, search for the app registration created in Step 2 and select it to grant it the **Reader** role for the current resource object.

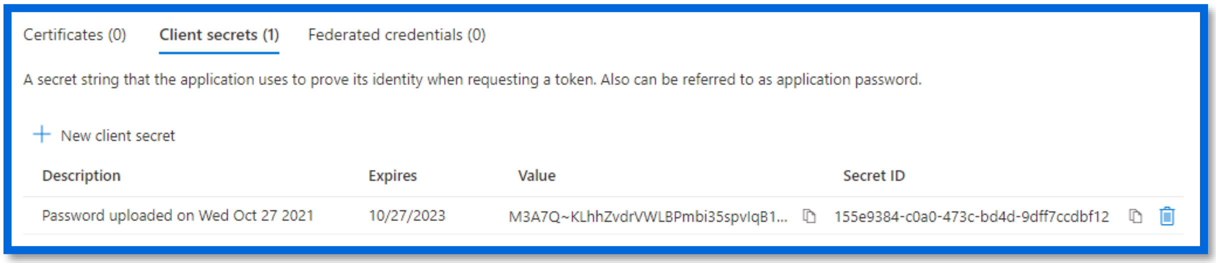
Copyright 2021 NETWRIX ALL RIGHTS RESERVED

Repeat these steps for the same app registration and resource object, but this time assign the **Reader and Data Access** role. The app registration created in Step 2 now has read access to all blobs under the current resource object in the Azure hierarchy.

Step 6 – Before continuing, the app registration's Client ID and Client Secret need to be noted. Navigate back to **Azure Active Directory > App Registrations** and click on the app registration created earlier. On the **Overview** page, note the app registration's **Application (Client) ID** and **Directory (Tenant) ID**.

Next, click on **Certificates & Secrets**. Click **New Client Secret**. Enter any name for the secret, set the expiration time, and click **Add**. Now note the **Value** of the newly created secret (not to be confused with the Secret ID).

IMPORTANT: A secret's value can only be viewed in Azure once, so if this information is lost then a new secret will need to be created.



A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value	Secret ID
Password uploaded on Wed Oct 27 2021	10/27/2023	M3A7Q~KLhhZvdrVWLBPmbi35spvlqB1...	155e9384-c0a0-473c-bd4d-9dff7ccdbf12

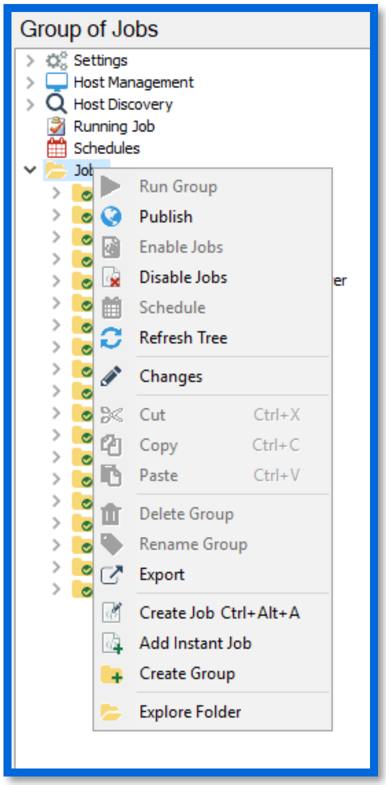
Implementation

This section will walk through how to extract the package downloaded from the Stealthbits website, how to import the AnyData_AzureBlobs job to StealthAUDIT, and how to configure and run the job to scan for sensitive data in Azure Storage (Blobs).

Extracting the Downloaded AnyData_AzureBlobs Job

Step 1 – Create a new Group in the StealthAUDIT job hierarchy by right-clicking **Jobs** and clicking **Create Group**. Name the group however you chose, for example: **AnyData Connectors**

Copyright 2021 NETWRIX ALL RIGHTS RESERVED



Step 2 – Right-click on the new Group and click **Explore Folder**. The directory that opens is where the **AnyData_AzureBlobs** job that has been downloaded will be placed. Extract the job to this location.

Step 3 – Right-click on the new **Group** and click **Refresh Tree**. The **AnyData_AzureBlobs** job should now be visible within the previously created Group in StealthAUDIT.

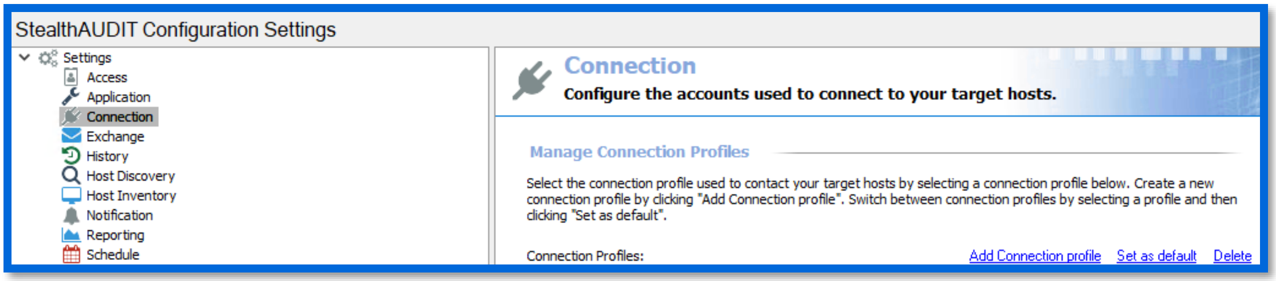
CAUTION: If the job does not appear in StealthAUDIT after refreshing the group, make sure the Windows **Read-only** property has not been set on the job's folder. If so, remove it and refresh the group once more to view the job in StealthAUDIT.

Configuring the AnyData_AzureBlobs Job

Now that the downloaded job has been imported to StealthAUDIT, you can configure it to scan for sensitive data in blobs in Azure Storage using the app registration configured in the **Creating an App Registration in Azure** step.

Step 1 – Add a new set of credentials by navigating in the StealthAUDIT hierarchy to Settings > Connection. Click **Add Connection Profile**.

Copyright 2021 NETWRIX ALL RIGHTS RESERVED



Connection

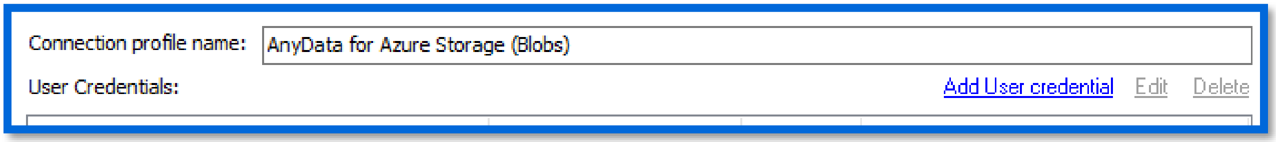
Configure the accounts used to connect to your target hosts.

Manage Connection Profiles

Select the connection profile used to contact your target hosts by selecting a connection profile below. Create a new connection profile by clicking "Add Connection profile". Switch between connection profiles by selecting a profile and then clicking "Set as default".

Connection Profiles:

Step 2 – Name the profile, for example: **AnyData for Azure Storage (Blobs).** Click **Add User Credential**.



Connection profile name: AnyData for Azure Storage (Blobs)

User Credentials:

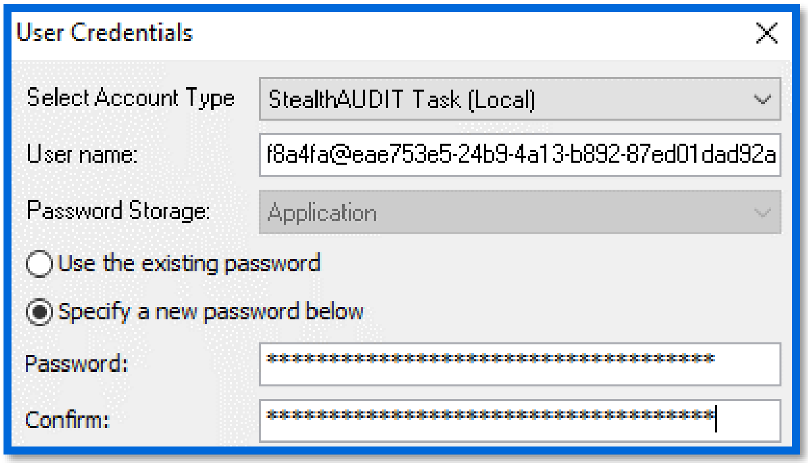
Step 3 – For this first credential's Account Type, select **Active Directory Account**. The User Name and Password should be for a user with the ability to authenticate to the SQL Server database used by StealthAUDIT. Click **OK** when finished.

IMPORTANT: It's important for the **Active Directory Account** to be the first credential in the list for this Connection Profile. If it's not, use the **Move Up** button to adjust this credential's position.

Step 4 – Click **Add User Credential** again. For this credential's Account Type, select **StealthAUDIT Task (Local).** For the Username, enter the app registration's **Client ID** and **Tenant ID**, separate by an "@" symbol.

For example: bf9551a0-f2d3-441e-b47c-2ec901f8a4fa@eae753e5-24b9-4a13-b892-87ed01dad92a

For the password, enter the app registration's **Client Secret (Value)**. Click **OK** when finished, then **Save**.



Select Account Type: StealthAUDIT Task (Local)

User name: f8a4fa@eae753e5-24b9-4a13-b892-87ed01dad92a

Password Storage: Application

○ Use the existing password

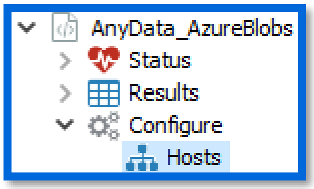
● Specify a new password below

Password: **

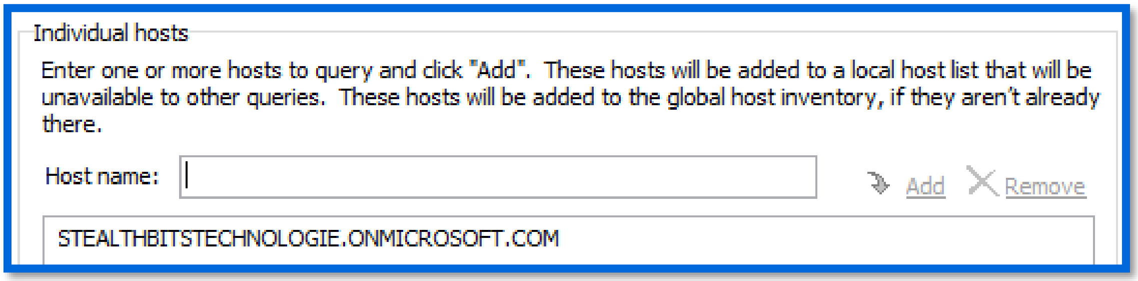
Confirm: **

Copyright 2021 NETWRIX ALL RIGHTS RESERVED

Step 5 – Navigate back to the AnyData_AzureBlobs job and navigate to the job's Host configuration via **<Job Name>** > **Configure** > **Hosts**.



In the Hosts menu, locate the **Individual Hosts** section, type your Azure tenant's friendly name for the **Host Name**, and click **Add** then **Save**.



Individual hosts

Enter one or more hosts to query and click "Add". These hosts will be added to a local host list that will be unavailable to other queries. These hosts will be added to the global host inventory, if they aren't already there.

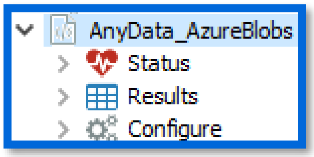
Host name:

STEALTHBITSTECHNOLOGIE.ONMICROSOFT.COM

Step 6 – The following parameters can also be configured for the job:

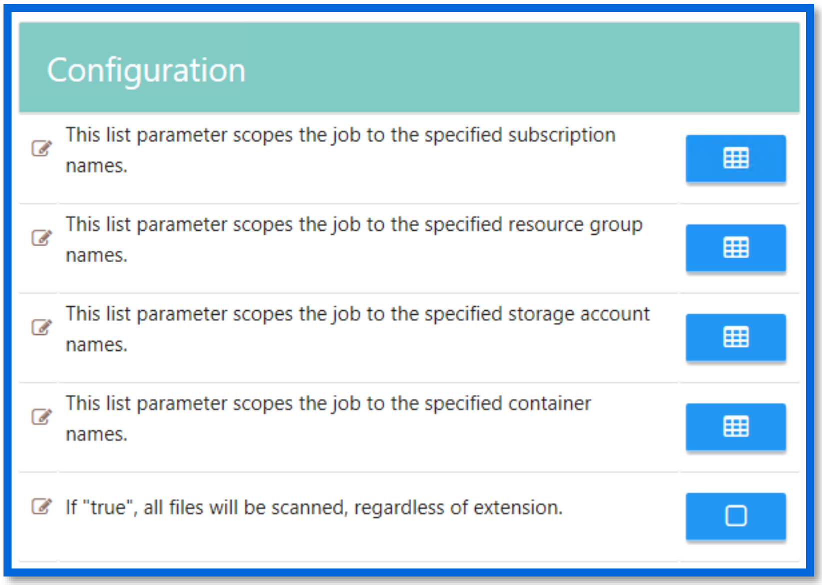
Container Name	This list parameter scopes the job to the specified container names.
Resource Group Name	This list parameter scopes the job to the specified resource group names.
Scan All File Types	If "true", all files will be scanned, regardless of extension.
Storage Account Name	This list parameter scopes the job to the specified storage account names. ***NOTE:*** *Only storage account short names should be used. Fully qualified name formats are not supported.* *For example, the format **<storage-account>.file.core.windows.net** is not supported, rather just the **<storage-account>** name is used for scoping.*
Subscription Name	This list parameter scopes the job to the specified subscription names.

To configure the parameters above, navigate to the job's node in the job tree.



Copyright 2021 NETWRIX ALL RIGHTS RESERVED

The parameters will be displayed along with other job information and can be modified in the **Configuration** section.



Configuration

This list parameter scopes the job to the specified subscription names.

This list parameter scopes the job to the specified resource group names.

This list parameter scopes the job to the specified storage account names.

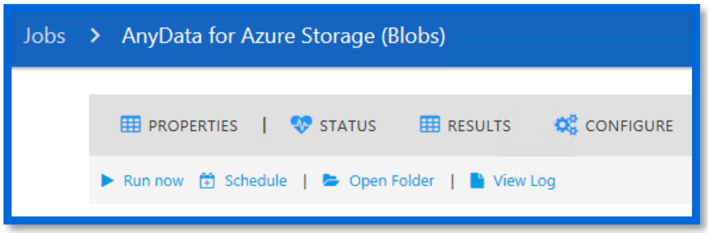
This list parameter scopes the job to the specified container names.

If "true", all files will be scanned, regardless of extension. □

Execution

CAUTION: AnyData_AzureBlobs only retains sensitive data matches from the most recent scan. All previous AnyData_AzureBlobs scan data, in both StealthAUDIT and the Access Information Center (AIC), is overwritten upon running a new AnyData_AzureBlobs scan.

To execute the job, highlight the **AnyData_AzureBlobs** job in the StealthAUDIT job hierarchy, and click **Run Now** below the breadcrumb trail and other job configuration options.



Jobs > AnyData for Azure Storage (Blobs)
PROPERTIES | STATUS RESULTS CONFIGURE
Run now Schedule | Open Folder | View Log

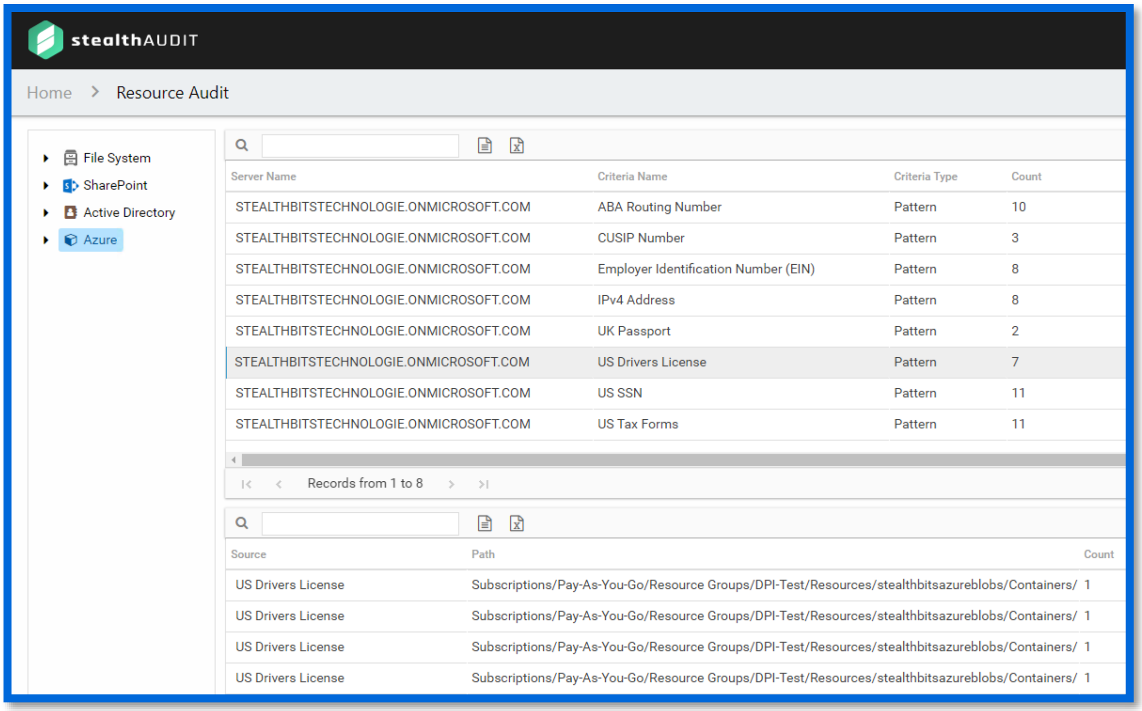
View Results

Sensitive data scan results from the **AnyData_AzureBlobs** job will be available for review in the **Access Information Center (AIC).**

Step 1 – Launch the AIC by double-clicking its icon on the StealthAUDIT server's desktop or by navigating to its URL. Log-in as required.

Copyright 2021 NETWRIX ALL RIGHTS RESERVED

Step 2 – Click on Resource Audit and navigate to “Azure” in the left sidebar. Expand the node, and nodes below it, to view details.

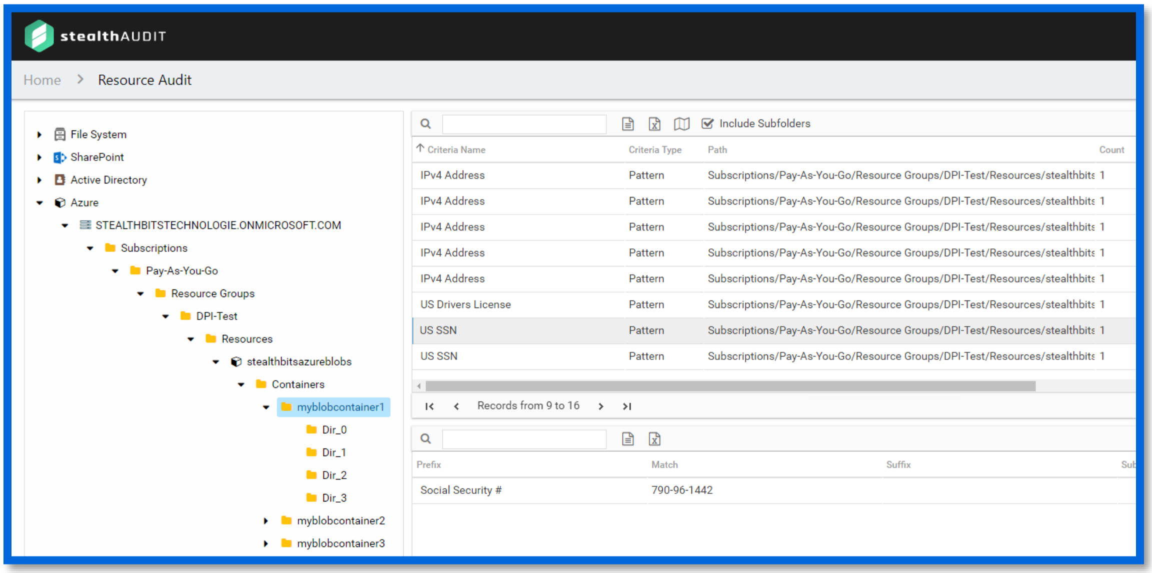


Server Name	Criteria Name	Criteria Type	Count
STEALTHBITSTECHNOLOGIE.ONMICROSOFT.COM	ABA Routing Number	Pattern	10
STEALTHBITSTECHNOLOGIE.ONMICROSOFT.COM	CUSIP Number	Pattern	3
STEALTHBITSTECHNOLOGIE.ONMICROSOFT.COM	Employer Identification Number (EIN)	Pattern	8
STEALTHBITSTECHNOLOGIE.ONMICROSOFT.COM	IPv4 Address	Pattern	8
STEALTHBITSTECHNOLOGIE.ONMICROSOFT.COM	UK Passport	Pattern	2
STEALTHBITSTECHNOLOGIE.ONMICROSOFT.COM	US Drivers License	Pattern	7
STEALTHBITSTECHNOLOGIE.ONMICROSOFT.COM	US SSN	Pattern	11
STEALTHBITSTECHNOLOGIE.ONMICROSOFT.COM	US Tax Forms	Pattern	11

Records from 1 to 8

Source	Path	Count
US Drivers License	Subscriptions/Pay-As-You-Go/Resource Groups/DPI-Test/Resources/stealthbitsazureblobs/Containers/	1
US Drivers License	Subscriptions/Pay-As-You-Go/Resource Groups/DPI-Test/Resources/stealthbitsazureblobs/Containers/	1
US Drivers License	Subscriptions/Pay-As-You-Go/Resource Groups/DPI-Test/Resources/stealthbitsazureblobs/Containers/	1
US Drivers License	Subscriptions/Pay-As-You-Go/Resource Groups/DPI-Test/Resources/stealthbitsazureblobs/Containers/	1

Information is broken down in a hierarchical view by Azure > Subscriptions > Storage Accounts > Containers > Blobs > Folders. Clicking on a scope allows you to select Sensitive Data reports in the AIC’s right sidebar, which shows sensitive data found at that hierarchical level and below.



Criteria Name	Criteria Type	Path	Count
IPv4 Address	Pattern	Subscriptions/Pay-As-You-Go/Resource Groups/DPI-Test/Resources/stealthbits	1
IPv4 Address	Pattern	Subscriptions/Pay-As-You-Go/Resource Groups/DPI-Test/Resources/stealthbits	1
IPv4 Address	Pattern	Subscriptions/Pay-As-You-Go/Resource Groups/DPI-Test/Resources/stealthbits	1
IPv4 Address	Pattern	Subscriptions/Pay-As-You-Go/Resource Groups/DPI-Test/Resources/stealthbits	1
IPv4 Address	Pattern	Subscriptions/Pay-As-You-Go/Resource Groups/DPI-Test/Resources/stealthbits	1
US Drivers License	Pattern	Subscriptions/Pay-As-You-Go/Resource Groups/DPI-Test/Resources/stealthbits	1
US SSN	Pattern	Subscriptions/Pay-As-You-Go/Resource Groups/DPI-Test/Resources/stealthbits	1
US SSN	Pattern	Subscriptions/Pay-As-You-Go/Resource Groups/DPI-Test/Resources/stealthbits	1

Records from 9 to 16

Prefix	Match	Suffix	Sub
Social Security #	790-96-1442		

Copyright 2021 NETWRIX ALL RIGHTS RESERVED