Breaking Managed Identity Barriers in Azure Services

David Fiser, Nitesh Surana

- From Sikkim, India
- Senior Threat Researcher (Cloud) TREND MICRO™
- Presented at Black Hat USA, HITB, HackInParis...
- Vulnerabilities in cloud services via Zero Day Initiative
- X: @_niteshsurana || Web: niteshsurana.com

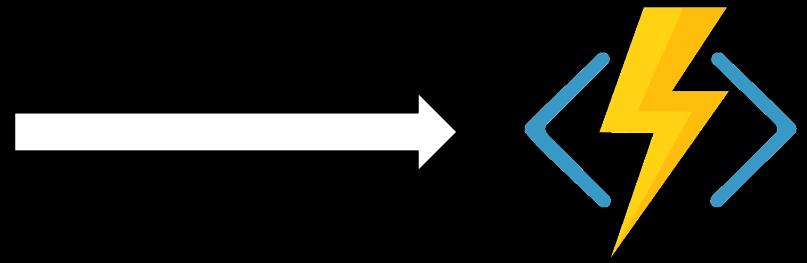
Microsoft Azure Service Fabric WAagent Exposure of Resource to Wr
Disclosure Vulnerability

ZDI-23-002
ZDI-CAN-18519

CVE ID	CVE-2023-21531
CVSS SCORE	5.3, (AV:L/AC:H/PR:H/UI:N/S:C/C:H/I:N/A:N)
AFFECTED VENDORS	Microsoft
AFFECTED PRODUCTS	Azure
VULNERABILITY DETAILS	This vulnerability allows local attackers to disclose sensitive information on Micr ability to execute high-privileged code within a container on the target system in The specific flaw exists within the WAagent daemon. The issue results from insu attacker can leverage this vulnerability to disclose stored credentials, leading to
ADDITIONAL DETAILS	Microsoft has issued an update to correct this vulnerability. More details can be https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-21531
DISCLOSURE TIMELINE	2022-09-20 - Vulnerability reported to vendor 2023-01-18 - Coordinated public release of advisory
CREDIT	David Fiser (Trend Micro - Project Nebula)

The Art

Azure Functions



Azure Machine Learning

Managed Identities

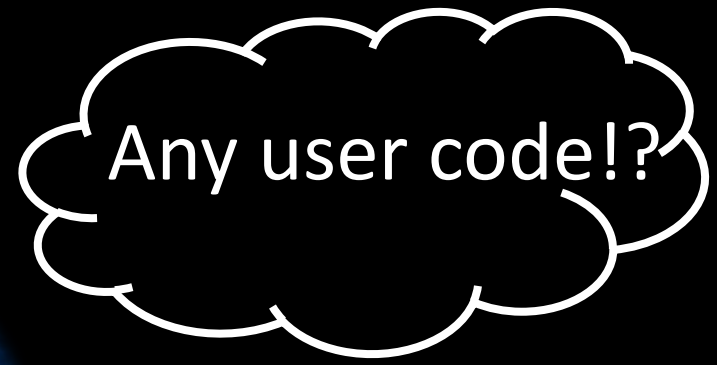
The Artists

EPISODE I: Azure Functions

Azure Functions

- Serverless platform
- User code inside CSP

Azure Functions



- Running user code

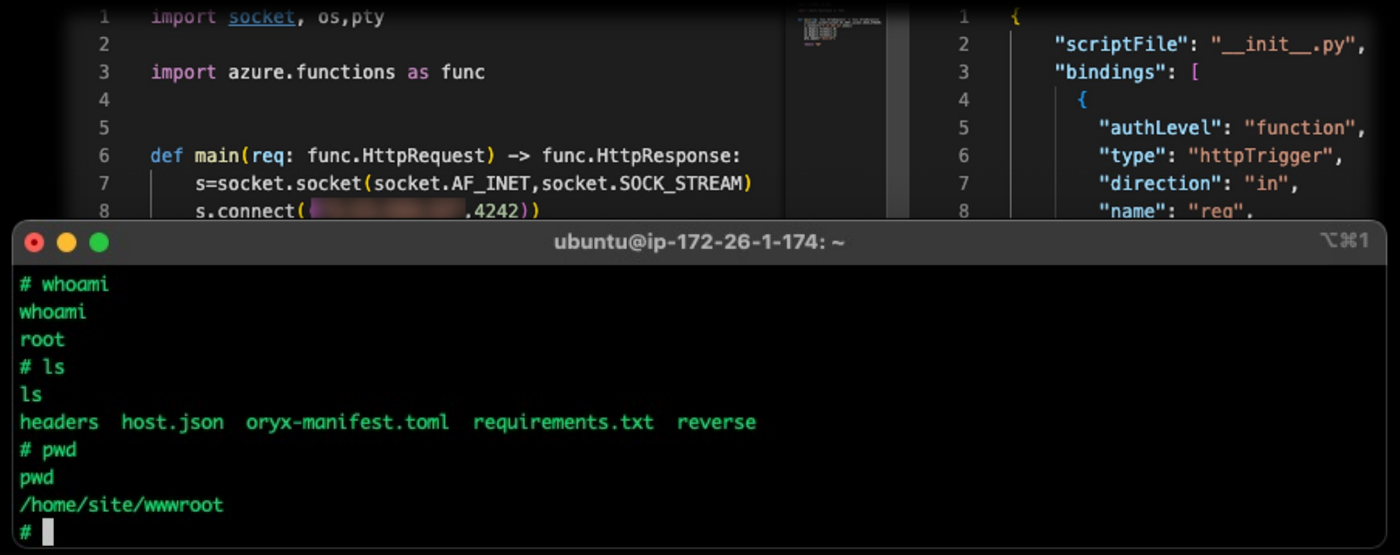
```
import azure.functions as func
import os


def main(req: func.HttpRequest) -> func.HttpResponse:
val = req.params.get('msg')

return check_output("echo '{0}'".format(val), shell=True)
```

Azure Functions

- Authentication
- Triggers

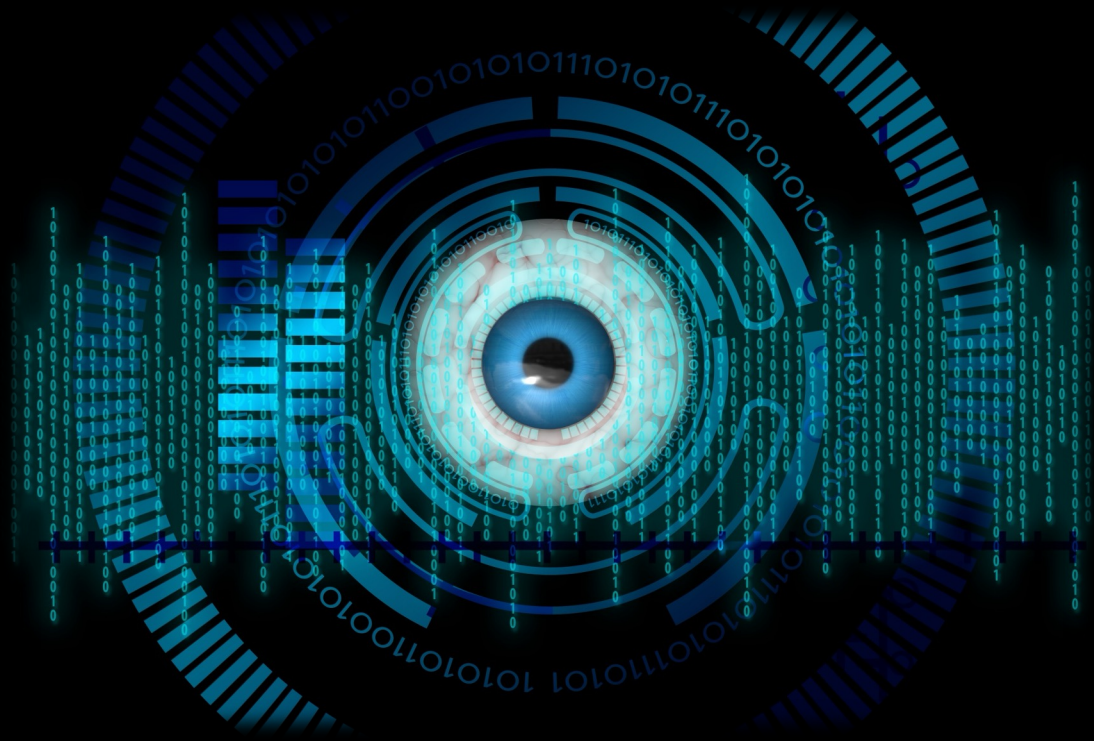
Research

- Simulation of compromise
- Analysis of environment
- Configuration changes



Authentication

- Tokens
- Client certificate
- Custom logic



Triggers

C# Copy

```
[Function("CosmosTrigger")]
public void Run([CosmosDBTrigger(
    databaseName: "ToDoItems",
    containerName:"TriggerItems",
    Connection = "CosmosDBConnection",
    LeaseContainerName = "leases",
    CreateLeaseContainerIfNotExists = true)] IReadOnlyList<ToDoItem> todoItems,
    FunctionContext context)
{
    if (todoItems is not null && todoItems.Any())
    {
        foreach (var doc in todoItems)
        {
            _logger.LogInformation("ToDoItem: {desc}", doc.Description);
        }
    }
}
```

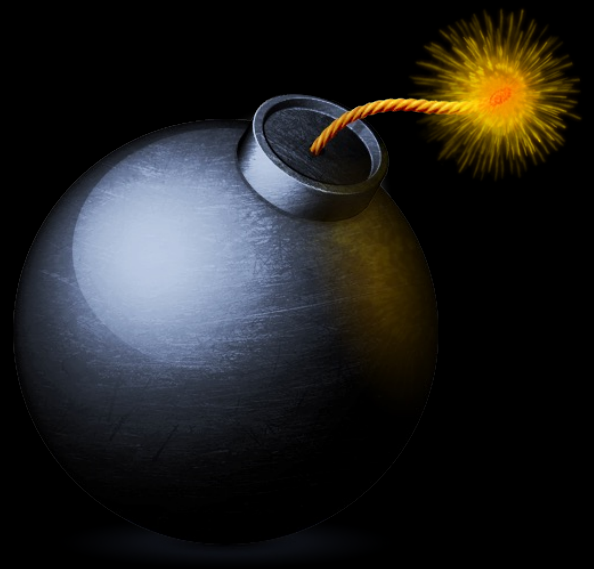
Timeouts

5 m

4.5 m

Environment analysis

- whoami
- mount, capsh
- env

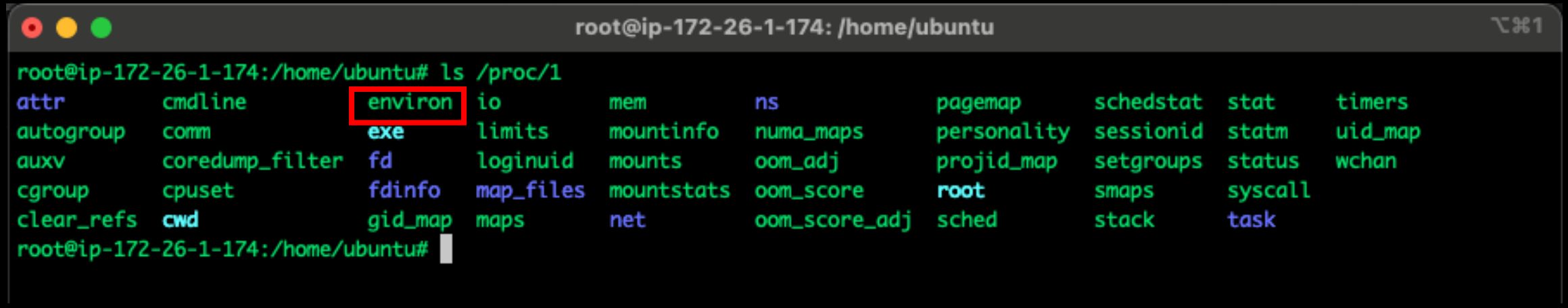


Environment variables

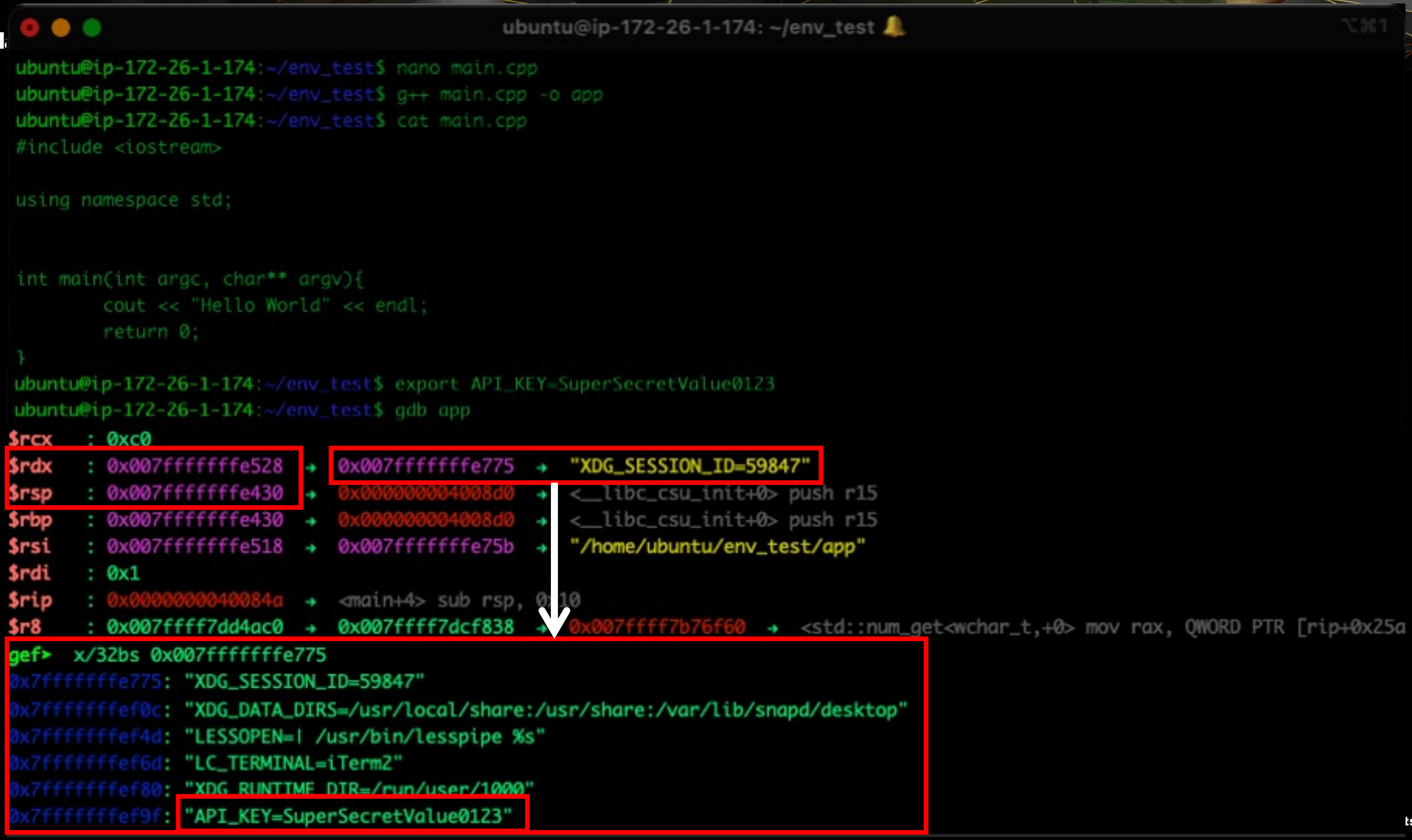
- Popular practice in DevOps
- Often stores secrets
  - References as a **!!! VAULT !!!**

Environment variables

- Fundamentals



unless a new table **passed as arguments**


ubuntu@ip-172-26-1-174: ~/env_test
ubuntu@ip-172-26-1-174:~/env_test$ nano main.cpp
ubuntu@ip-172-26-1-174:~/env_test$ g++ main.cpp -o app
ubuntu@ip-172-26-1-174:~/env_test$ cat main.cpp
#include <iostream>
using namespace std;
int main(int argc, char** argv){
cout << "Hello World" << endl;
return 0;
}
ubuntu@ip-172-26-1-174:~/env_test$ export API_KEY=SuperSecretValue0123
ubuntu@ip-172-26-1-174:~/env_test$ gdb app
$rcx : 0xc0
$rdx : 0x007fffffffe528 → 0x007fffffffe775 → "XDG_SESSION_ID=59847"
$rsp : 0x007fffffffe430 → 0x0000000004008d0 → <__libc_csu_init+0> push r15
$rbp : 0x007fffffffe430 → 0x0000000004008d0 → <__libc_csu_init+0> push r15
$rsi : 0x007fffffffe518 → 0x007fffffffe75b → "/home/ubuntu/env_test/app"
$rdi : 0x1
$rip : 0x0000000040084a → <main+4> sub rsp, 0x10
$r8 : 0x007ffff7dd4ac0 → 0x007ffff7dcf838 → 0x007ffff7b76f60 → <std::num_get<wchar_t,+0> mov rax, QWORD PTR [rip+0x25a
gef➤ x/32bs 0x007fffffffe775
0x7fffffffe775: "XDG_SESSION_ID=59847"
0x7fffffffef0c: "XDG_DATA_DIRS=/usr/local/share:/usr/share:/var/lib/snapd/desktop"
0x7fffffffef4d: "LESSOPEN=| /usr/bin/lesspipe %s"
0x7fffffffef6d: "LC_TERMINAL=iTerm2"
0x7fffffffef80: "XDG_RUNTIME_DIR=/run/user/1000"
0x7fffffffef9f: "API_KEY=SuperSecretValue0123"

Environment

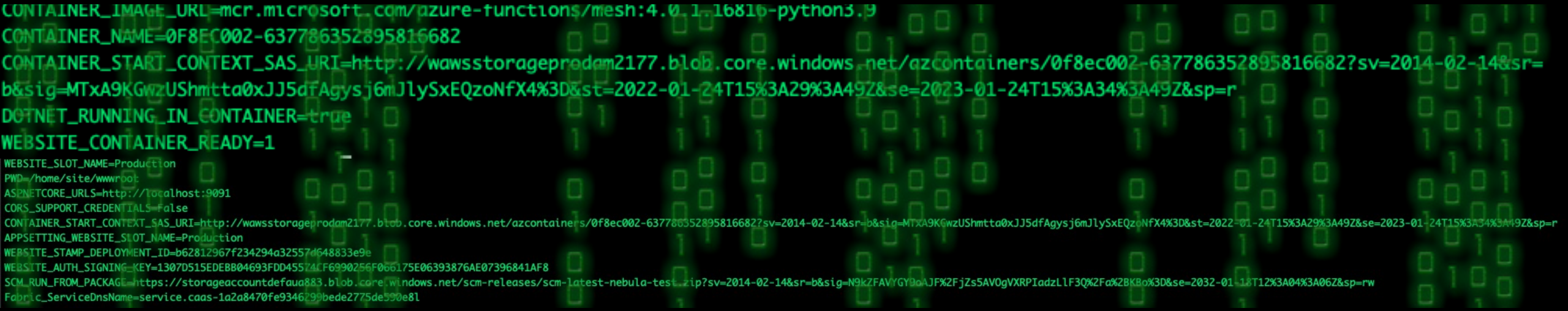
```
/*
 * present useful information to the program by shovelling it onto the new
 * process's stack
 */
static int create_elf_fdpic_tables(struct linux_binprm *bprm,
                                   struct mm_struct *mm,
                                   struct elf_fdpic_params *exec_params,
                                   struct elf_fdpic_params *interp_params)
{
/* fill in the envv[] array */
current->mm->env_start = (unsigned long) p;
for (loop = bprm->envc; loop > 0; loop--) {
    if (put_user((elf_caddr_t)(unsigned long) p, envp++))
        return -EFAULT;
    len = strnlen_user(p, MAX_ARG_STRLEN);
    if (!len || len > MAX_ARG_STRLEN)
        return -EINVAL;
    p += len;
}
```

https://github.com/torvalds/linux/blob/23956900041d968f9ad0f30db6dede4daccd7aa9/fs/binfmt_elf_fdpic.c#L64

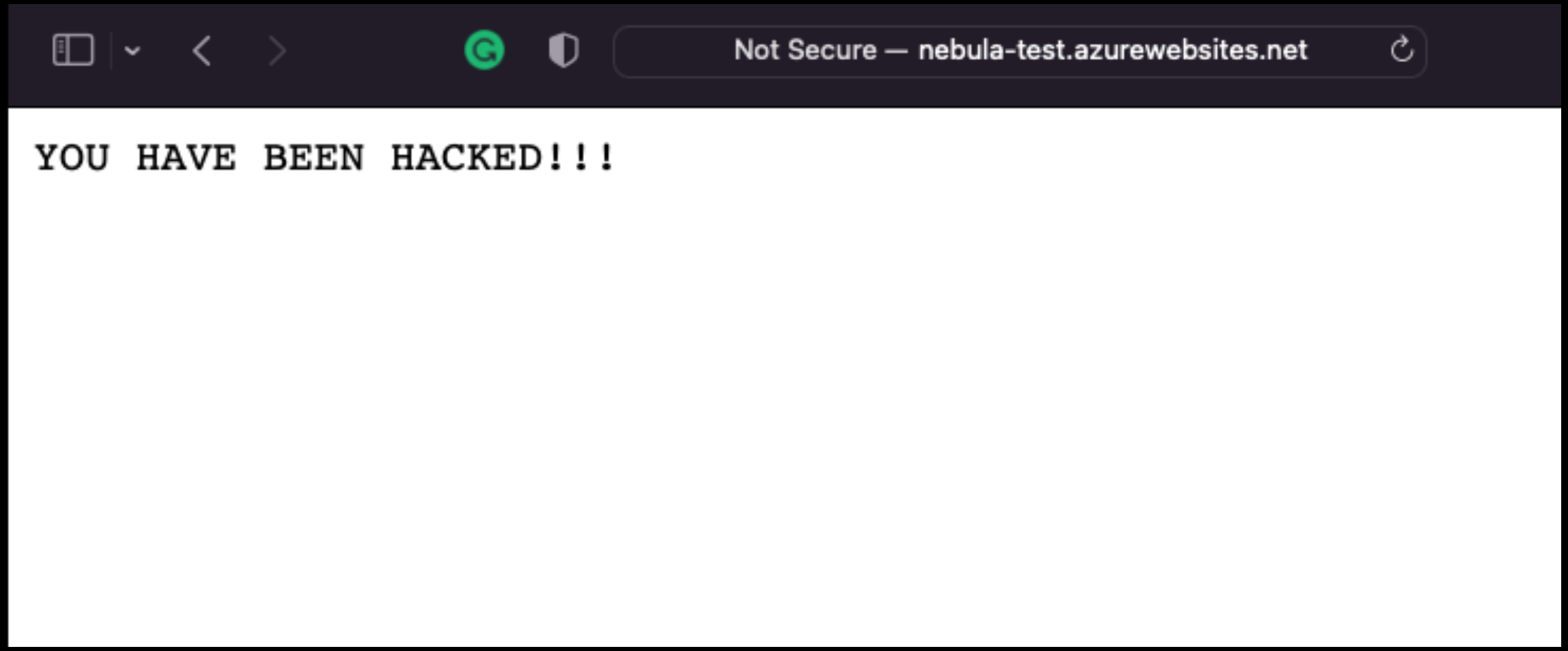
AzureWebJobsStorage

CONTAINER_ENCRYPTION_KEY

CONTAINER_START_CONTEXT_SAS_URI



AzureWebJobsStorage



CONTAINER_START_CONTEXT_SAS_URI

```
{
    "encryptedContext" : "AES_IV . payload . SHA256"
}
```

CONTAINER_ENCRYPTION_KEY

Recipe

From Base64

Alphabet: A-Za-z0-9+/=

Remove non-alphabet chars

AES Decrypt

Key: jaXOvBRs4jvnYKSghsOIbt07B5+leYmnTd1BhM… BASE64

IV: Lk8nHZ/2m+6TGuK0pfhtNA== BASE64

Mode	Input	Output
CBC	Raw	Raw

Input

length: 9196
lines: 1

/cYdq+AnpWjICTECMSDgT5SsgFPGgm6ouZIL2DHqQVF92aun+3ZGuz79neYZQNaC6Zq4htv2WPL1u/0Z7g0WJIDreYyLVME7alLzS
WNd4cAzWL/bBHZSH8iedjLUVasR90U8qYoN1TR1Y5mqCPesCHFDmDOqUozQUHYmco290YqnpGFLlFtlY7UzQUXvdEiEkDsDSQreIA
NoeFRcIvnEZ/Hkaa4yeyg2l4b1TBz71cT7Lf/TFG3F0783HzpwgvEelbu+HWAWVfd8WK9MOeOy8q4eHKvqWa9uqXBTSfLbNr2oUms
GSWPFwQTZPYcL4dUmiNm2yusw1fkwa6dJmPC7pXcSh5e4CDec8/RCVizmWNQufkg1Yp7B19QKUf0K4noQR233zdsbkXlXO7pL6jpj
4hWDOdmipcF6tlcVbMTf4BfPZYyyD1HdYtHLalndF7jxrJsu+QwjBXm7G088p2KJLbWromnM3QOI+VqKSOYRMsoLjXoUK9wfMvcsB
XjKkRT7cAjgvNRq6YKGNyhDa21+IHkC6J+bTaXiGirWA8WL1zaHbUe9aGk5Ay9rr/hVVrGWiPO79SdN7Ff8a2+P9zVdKNrLXKd5lA
qS4x8BmX0/zHmnigMC+0SHEK3C2IVQ1z1Pydp9p2ziDEc3IrzsZ86bM6JWxaKdFfHrQ8lXt7EOFMD/H26gIaIQXHEzbFBKuZf0y2j
RYRMhU49SehAeAdID72DBbSM1O/v4ggkLYOzCFy4MVQhj0erDWhvU+iFLtfoQQ7ptQ4Z04MrxrCADtrepbv4HV/jv6iBCLn50UMeS
oA5FJARqlvpJV/tPSDudlJNqrRAq8ugcCf77/pgZ6SuT34Dor9zdNxDXg93minjSYnEL2M8Uzc3Zxv+DevBI3SeA4Alo5Pw8FvJihI
94Z1qDHCvQ7vLUWyNqOuQw3TAUOEuaT4mUmIjzzhMuAjBUDUOEymrH1ldxuTE5YEMhsK1tBGYPbdYzqDYMbENeou+OGibn8mjLr2i7
nD4x6ATtdDO9Cw8+fIjAQqRskuazEOyyPf+ingAkj7GjjwaL85TlFZSpOykJN6t+BoQQALavdTV0tnQwyd8xBQU9dp56iMPJBAiU+I
BNYXkY6L9GwJQ03AEDGq40d2qacSndXsagIUElbsB7FfUqIc06D7YlnQxV0UcQ7m0S8QL3ijyHKWQEZszq1N6gAKoQGr2/3RddDqV
HGorLHwl7uRARny3BzugRlH+VxGwDRnw/qrdMvS6vQn3ogAvn877aIX6/DDGm1cNtV2xfM8XOsWNFb+X4a8tNHhE4Cv5R2qgylMsPv
t5bwVJP5//1JUbfCjoHJqmXOK4axP9E6zH27lFD9R6o3Vp0bOK9x0tuSPLujpoefyqiuJIFEdUJBDkwC82bmAXLSKEfgsutTDdDy8C
LAJblPBMlxH3H3iSl8+JuoQ1mmI2CfFZwDHDs0i2Ei2a5RLiko0aZVhweElPNLIw2mDm/5XJ4iZunlxKi8xLtqODdBvjjCAl9WfXDr
t5+I3gi6czwxv3i6Ypa+YSXrDKJEGIXEwB3v1BL3JLUhSPL3FbKq72Z6LixL6nhd+i/nI2+fKAak2m//dj8ACDRv4fYU0X3J15CatE
NMdyLsaKeo9UW7Ef+6s6BeFv2EhAoK/VipGPX+DyPw61VvQaH0Sqk/oKzPo40CoRBDiOyoN4WanvLNOn7SwgzDzvXfiYnI0FyuGTHV
ysQcXXKs1CBNynm70vV9H1vECy2B5UpvEfbknFarwlPX/Q4eqvkRt8L26gKT8JpkBXCJTm/GGaUIgX/ajBUbQz1al+YA02Cy9cVxUH

Output

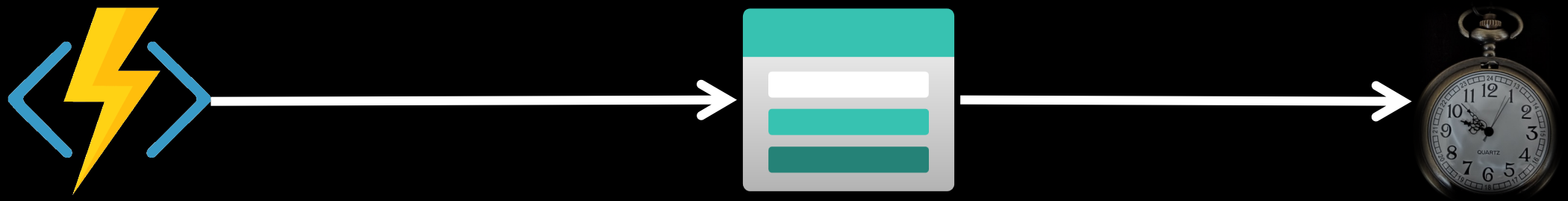
start: 0 time: 3ms
end: 6891 length: 6891
length: 6891 lines: 1

{"SiteId":767064730,"SiteName":"nebula-test","EncryptedEnvironment":"3 | VizDzTy3Oag/PHD1E7gwWg== |
VizDzTy3Oag/PHD1E7gwWqhXzQpeguHXICV7FYHwuYGqVJF2pJiekzHg7Se9pFMSsM3HNtx4Suy499UIqF8Fe9AhoiJMbE3aD2+3bC
Nm5tK4ogMk8fgGtiLQgELuSugTYq8HoQaG5p+CGGFNIbwhhQbj2kVyfewdlAESgXADxUPW6+criRqdJgqvjF6/66kxGJqL3UoQEGk3
MedtHb03J8+0KXFq1Ws5SNBjpc0rwgRHToIBd1WFrrAO9G1AFim3EgHUxB5euM1B81bn9CfKuR5nw2Cdt8WpktoEWLa7vPwbE62EFp
1m69PZIC3L686IN0+nFT1wMqP9UraBeQo+/OWQTrfjUeTDEBIjbKArLAO5/1yBfYfWDXIg5PGmWoi4HedSYnbobScX5n1iwp99BiPr
+MPiU6km35FWWRp/qqujeChHQPXC9i/ICPO6Wg4UxXlhQbDlMtwkEl5dH1soCMXTknuLSLAW/96WOQN5yhxqjtLQVqh4NzLmwwrhjg
UwPaknHWH0oTYSXW70Vww88UDgYcqncIIjPwl3d7SawBXVO93t0L+EdQDSvMTK1pFr+h/xuK3s93Q4L+An7OR6WUSeI7KYOVfwPG2r
1Zm4tzBJxzSnlTbaYTm7NkuKH6e1ZIeAZhatY4XFf55d+yzSIMBRO3Th5SojwmB0wCEBOgLhEApnLKPy4FNygU/ZOVvd6gfNDpc/ZI
ZaBuIUMulZk/kEwC6JyKmQfO0wef2t4ApQMlpC8DWNgI2pGU83iMf2meVUMEyxjpEZh2xdjJiHN9djvSjxpS4Q+4NT2G4n1EimPXSC
0XhJ8UwSxZEsD8jASXd7TJ3muZ5ssinNcT2KIQKEgjqEQ75nYs1hMMP2AuQSzsl7e9ePuRt0dw0azTj6uHmmA56IllE5VaRZL/dF3I
cVhTWL5j6LiKq6CXl7Lhc/t1arOoYwATN+HBOkgXPFABJfJ8npFZzumvQTH4UK04xmXbksWNUJ69JAi8ooQiezSzfxatW9PRVL1edV
MmN6VPe1XdivOJTGwgkgmqj1e8MnZZvfgaBo3GvCMarOykXdzKmuRF5WLMHwjcF5NV765pgN81FNz9ur2eNvH768sMa1p9BXUa27Ye
AZLC28IqTL6OZQq0eILglFGoDjotTNho/DtT3tQhF1SEMqVS/IAmBvow+f/VArfincjGwp045udB8XjTeksVRQuyGHJvX78QcwKYWr
2WjmLMOK7YuxAVfvxi0QejIDwPlFsBxauyMP4cljGNCnY1LvQIHPeQoV2XzjtTQD2piBm702X6icE5QKi8lB+vG7e5+0UW2WIDGjtO
dePnYgbZekgEhjTggpOrPJaC8GtJ/D7y4drEqvvsB5PpTKRK1Xd9OJRM2YHp6odYlc5LPYvU05ZDrFAGAJYOjFWwxTLG3YNCiLcFeO

Decrypted context

- Authentication tokens
- **Managed identity proxy settings**

Managed Identities

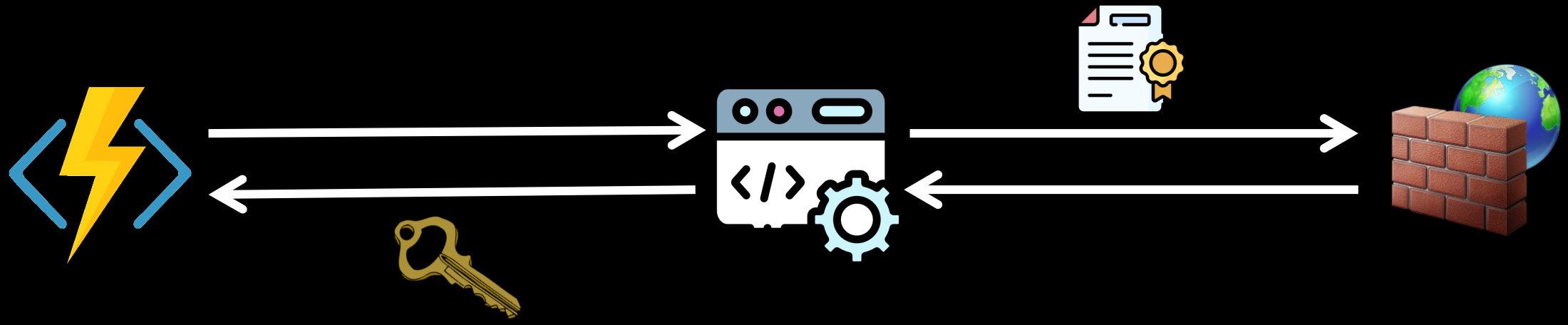


~~STORAGE_ACCOUNT_CREDENTIALS~~

Managed Identities

```
> GET /msi/token?resource=https://management.azure.com&api-version=2019-08-01 HTTP/1.1
> Host: localhost:8081
> User-Agent: curl/7.74.0
> Accept: */*
> X-IDENTITY-HEADER: 70DBF9CB04554E9E8E210A70CD4D2974

* Mark bundle as not supporting multiuse
< HTTP/1.1 200 OK
< Date: Thu, 31 Mar 2022 13:06:34 GMT
< Content-Type: application/json; charset=utf-8
< Server: Kestrel
< Transfer-Encoding: chunked

{"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6ImpTMVhvMU9XRGpfNTJ2YndHTmc
wNDc1M2EtYWU1Yi00MmQ0LWE4NmQtZDZmMDU0NjBmOWU0LyIsImlhdCI6MTY0ODczMTY5NSwibmJmIjoxNjQ4NzM
ciI6IjIiLCJpZHAiOiJodHRwczovL3N0cy53aW5kb3dzLm5ldC8zZTA0NzUzYS1hZTViLTQyZDQtYTg2ZC1kNmYw
```

Managed Identities



Findings

- Environment variables
- Proxy parameters
- **Valid JWT tokens <u>outside Azure</u>**

```
david_fiser@CZ-64PZE33B LeakPoC % ls
Microsoft.AspNetCore.Mvc.Versioning.dll                System.Composition.AttributedModel.dll  log4net.dll                test1.pdb
Microsoft.Extensions.Logging.Abstractions.dll          TokenServiceContainer.dll               test1.deps.json            test1.runtimeconfig.dev.json
Microsoft.IdentityModel.Clients.ActiveDirectory.dll    TokenServiceContainer.pdb               test1.dll                  test1.runtimeconfig.json
README.txt                                             leak.py                                 test1.exe
david_fiser@CZ-64PZE33B LeakPoC % python3 leak.py
```

Why?

- Environment variables popularity
- Not knowing fundamentals
- Ignoring the risks

What do you suggest David?

Why?

```
int k = (argc + 5) * sizeof(char*);
```


```
return ret;
```

< Back

Mistaken Identity: Extracting Managed Identity Credentials from Azure Function Apps

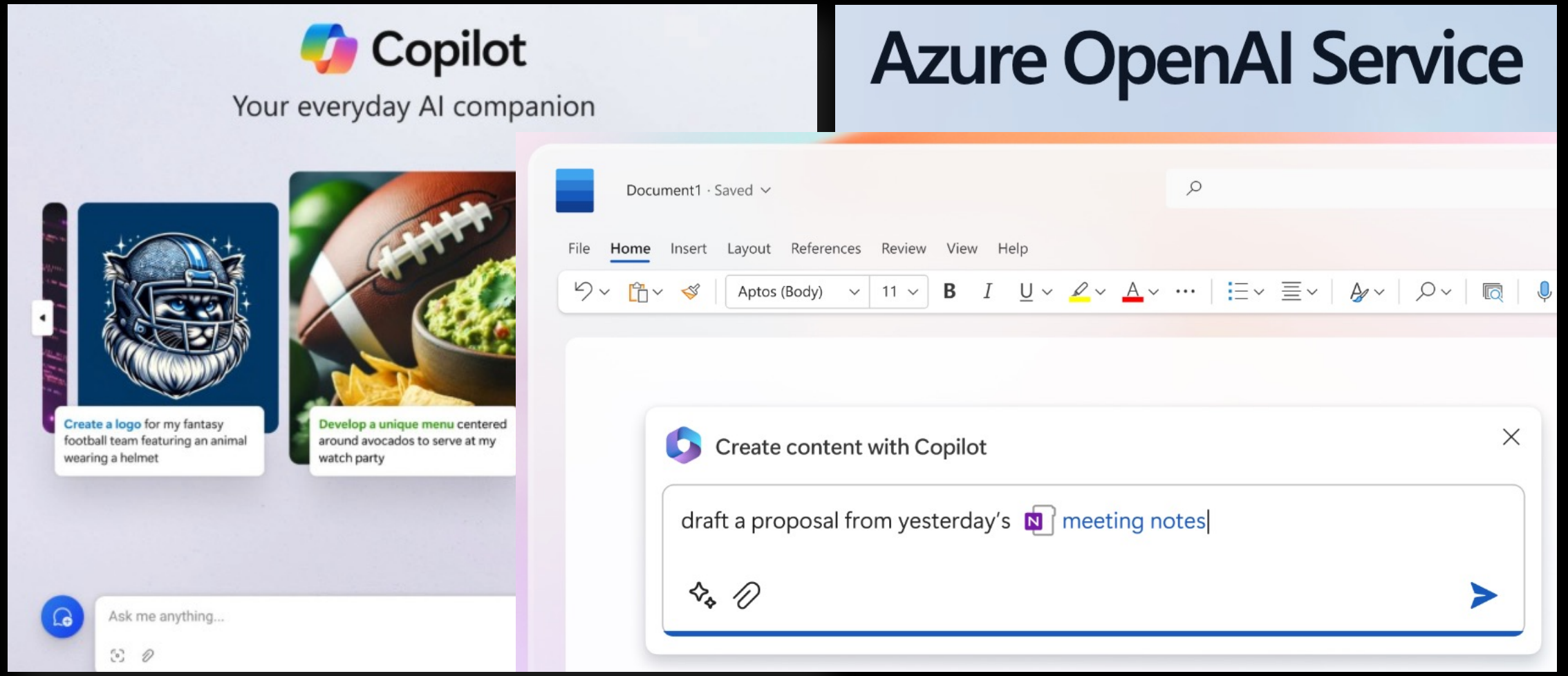
November 16, 2023 | Karl Fosaaen

TECHNICAL BLOG CLOUD PENETRATION TESTING

As we were preparing our slides and tools for our DEF CON Cloud Village Talk (What the Function: A Deep Dive into Azure Function App Security), Thomas Elling and I stumbled onto an extension of some existing research that we disclosed on the NetSPI blog in March of 2023. We had started working on a function that could be added to a Linux container-based Function App to decrypt the container startup context that is passed to the container on startup. As we got further into building the function, we found that the decrypted startup context disclosed more information than we had previously realized.

June 1

EPISODE II: Azure ML


Copilot
Your everyday AI companion
Azure OpenAI Service
Create a logo for my fantasy football team featuring an animal wearing a helmet
Develop a unique menu centered around avocados to serve at my watch party
Ask me anything...
Document1 · Saved
File
Home
Insert
Layout
References
Review
View
Help
Aptos (Body)
11
Create content with Copilot
draft a proposal from yesterday's meeting notes

Applied AI Services

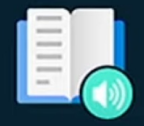

Bot Service


Cognitive Search


Form Recognizer


Video Indexer


Metrics Advisor


Immersive Reader

Cognitive Services


Vision


Speech


Language

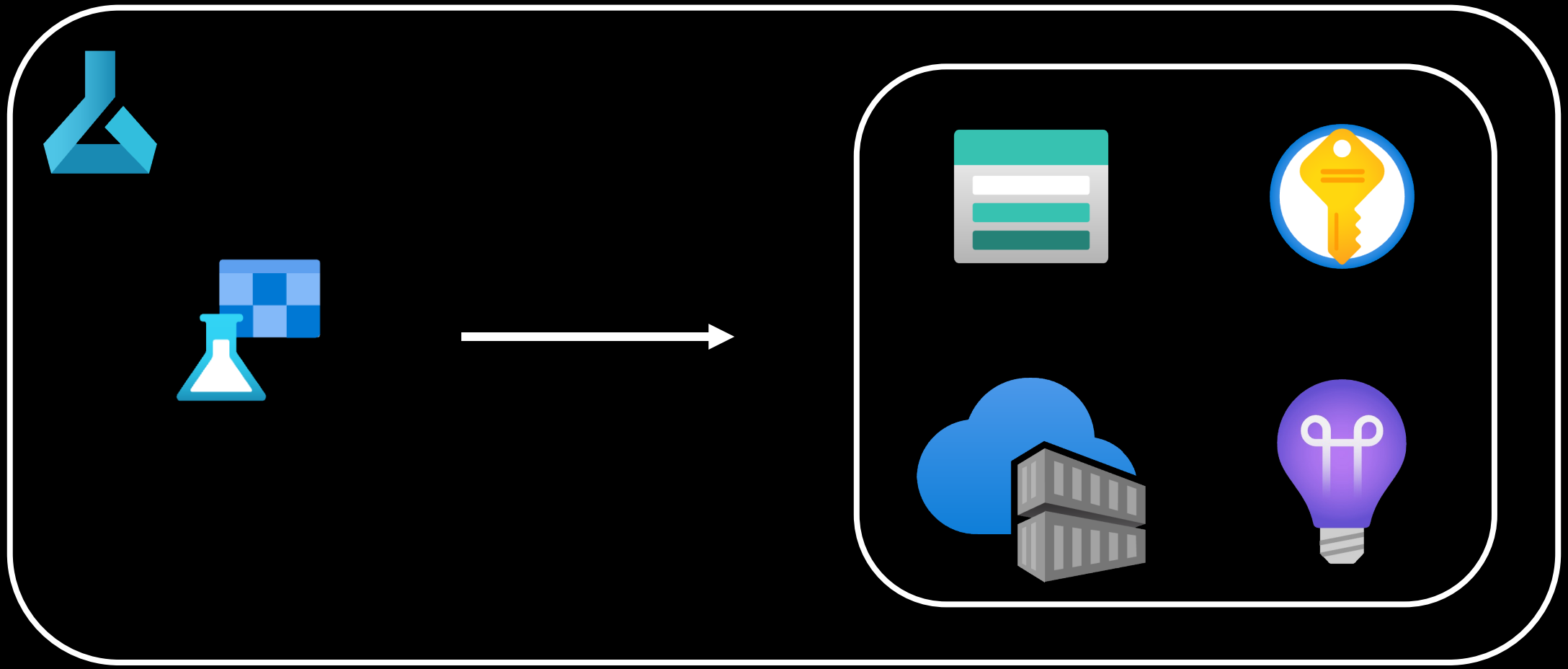

Decision


Azure OpenAI Service

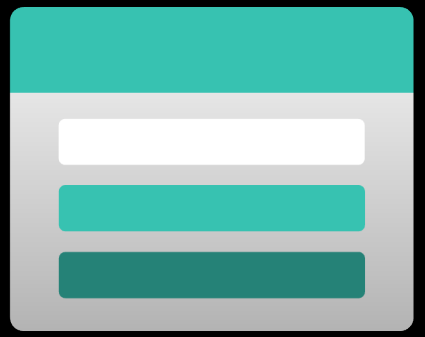
Azure Machine Learning

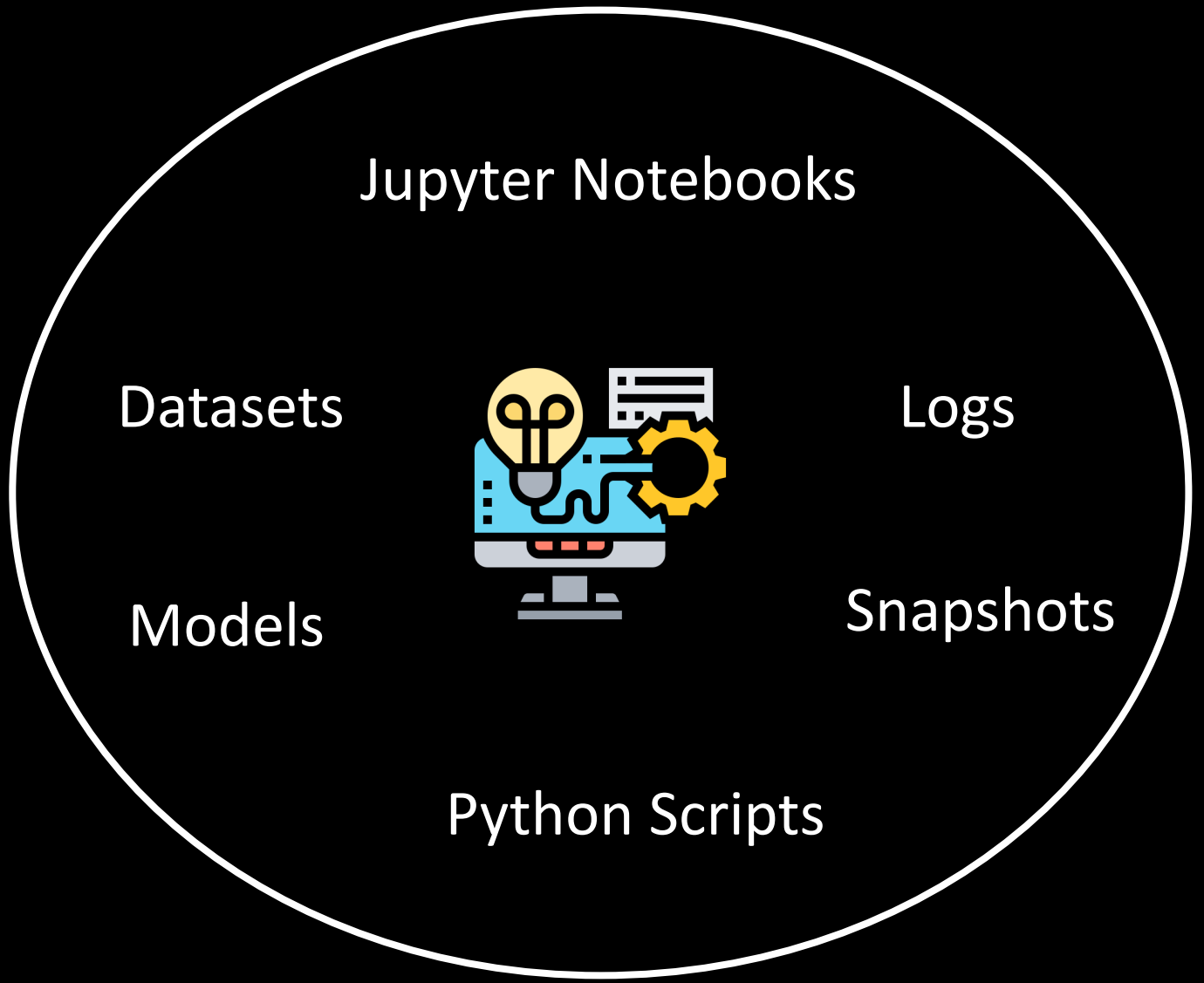
Prepare & Preprocess | Build, Train & Consume | Deploy & Scale | Manage & Monitor

Azure Machine Learning

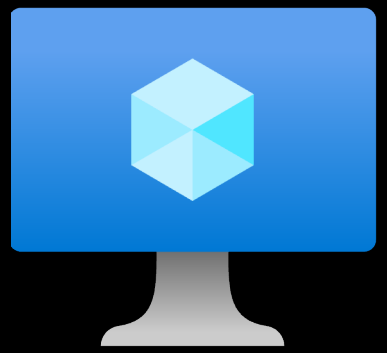


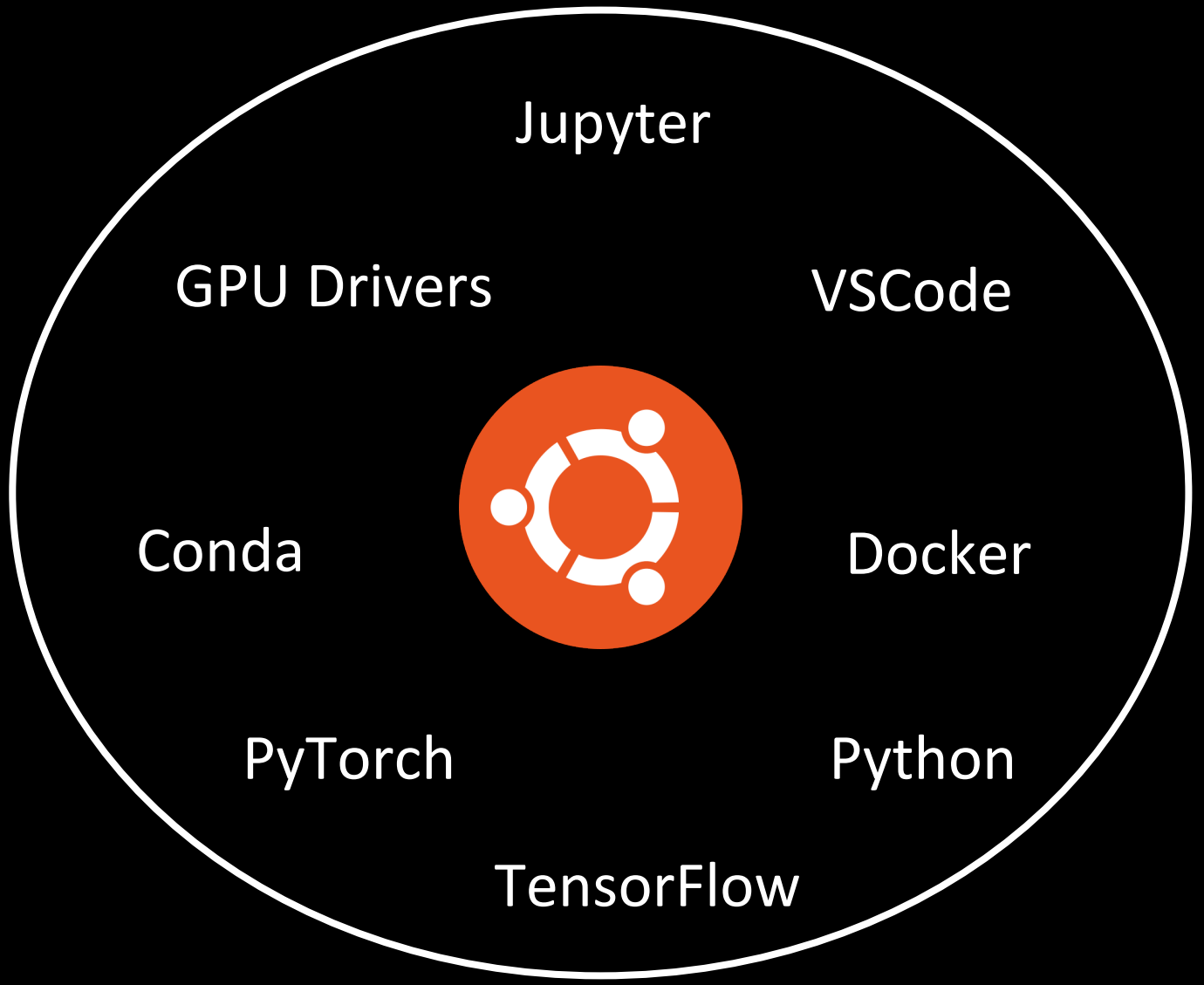
Storage Account



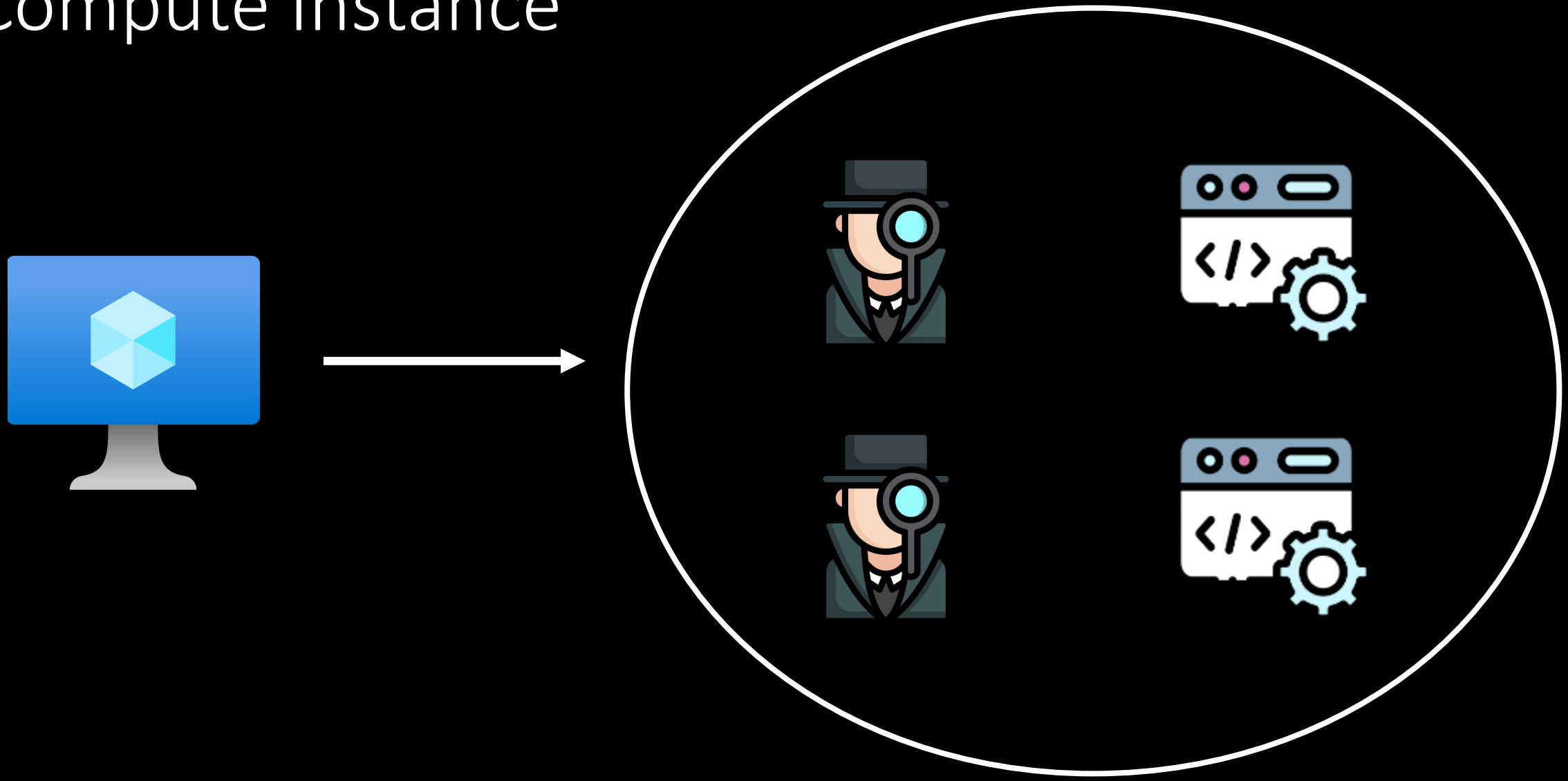


Compute Instance



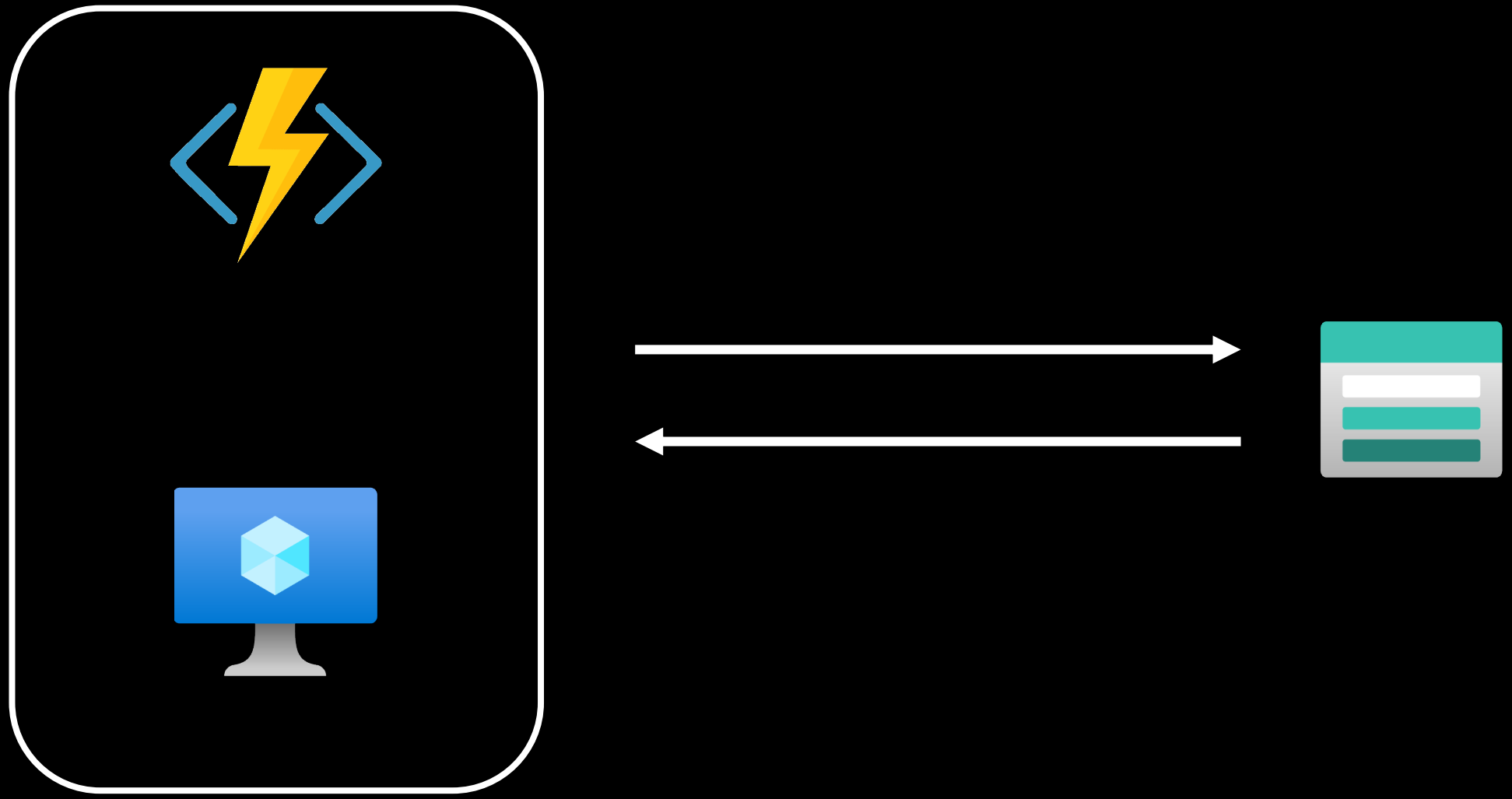


Compute Instance



Approach

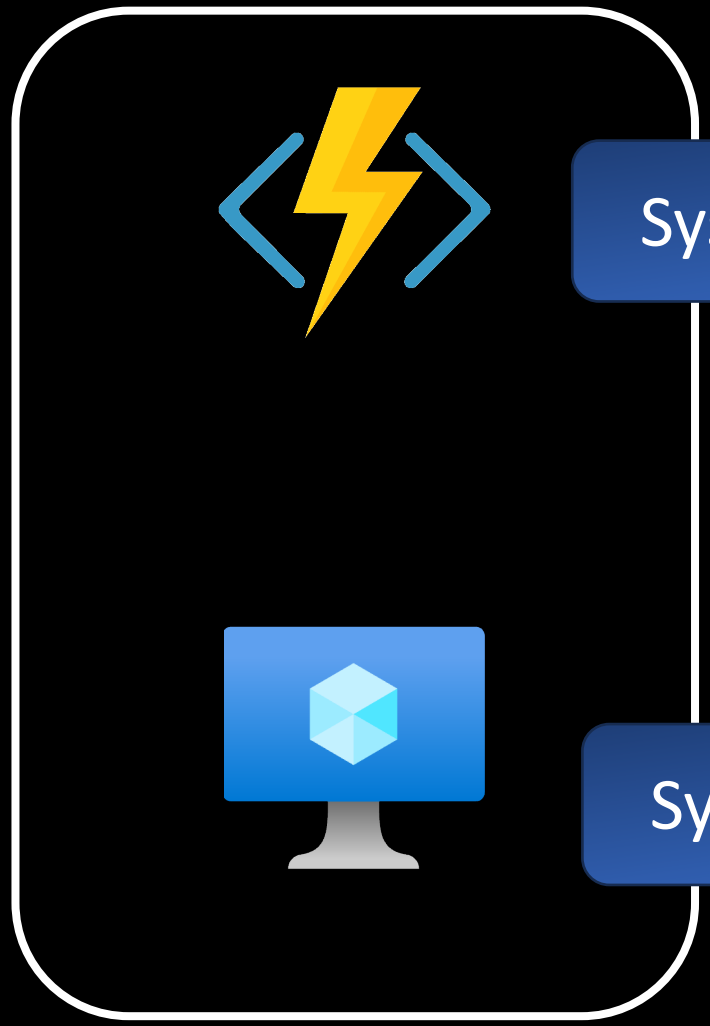
- Inspect network traffic
- Running processes
- Reverse CSP agents
- Examine default logs




Storage Account's Access Key


Managed Identities
imgflip.com


User Assigned Managed Identity



System Assigned Managed Identity

System Assigned Managed Identity

Sign in with a managed identity

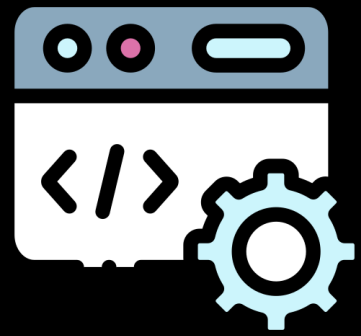
On resources configured for managed identities for Azure resources, you can sign in using the managed identity. Signing in with the resource's identity is done through the `--identity` flag.

Azure CLI | Copy | Open Cloudshell

```
az login --identity
```

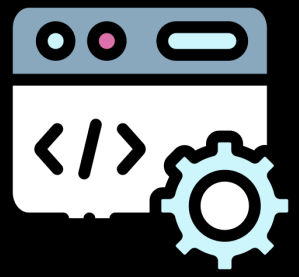
az login --identity

GET /MSI/auth/?resource=https://management.core.windows.net/&api-version=2017-09-01 HTTP/1.1
Host: 127.0.0.1:46808
User-Agent: python-requests/2.31.0
Accept-Encoding: gzip, deflate
Accept: */*
Connection: keep-alive
secret: 6cvsqlMIRvIyURbztZ3P



identityresponderd

identityresponderd



```
[Unit]
Description=Azure Batch AI Identity Responder Daemon
```

```
EnvironmentFile=-/etc/environment
EnvironmentFile=-/etc/environment.sso
EnvironmentFile=-/mnt/batch/tasks/startup/wd/dsi/dsixdsenv
WorkingDirectory=/mnt/batch/tasks/startup/wd
```

identityresponderd

/etc/environment.sso

```
APPSETTING_WEBSITE_SITE_NAME=AMLComputeInstance
MSI_ENDPOINT=http://127.0.0.1:46808/MSI/auth
MSI_SECRET=6cvsqlMIRvIyURbztZ3P
OBO_ENDPOINT=http://127.0.0.1:46808/OBO/token
DEFAULT_IDENTITY_CLIENT_ID=clientId
```

/mnt/azmnt/.nbvm

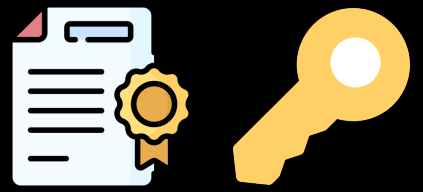
```
instance=<CI_NAME>
domainsuffix=<REGION>.instances.azureml.ms
tokenurl=https://<REGION>.cert.api.azureml.ms/nbip/token/subscription
s/<SUB_ID>/resourceGroups/<RG_NAME>/workspaces/<WS_NAME>/computes/<CI_NAME>
certurl=https://<REGION>.cert.api.azureml.ms/nbip/token
```

Outbound Traffic from identityresponderd

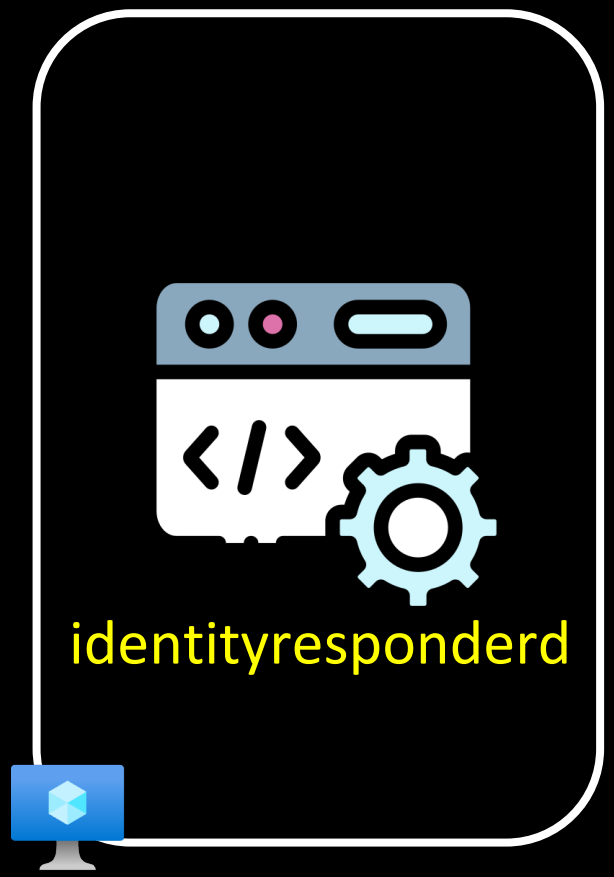
POST
/nbip/token/subscriptions/<SUB>/resourceGroups/<RG>/workspaces/<WS>/computes/<CI_NAME>

Host: <REGION>.cert.api.azureml.ms

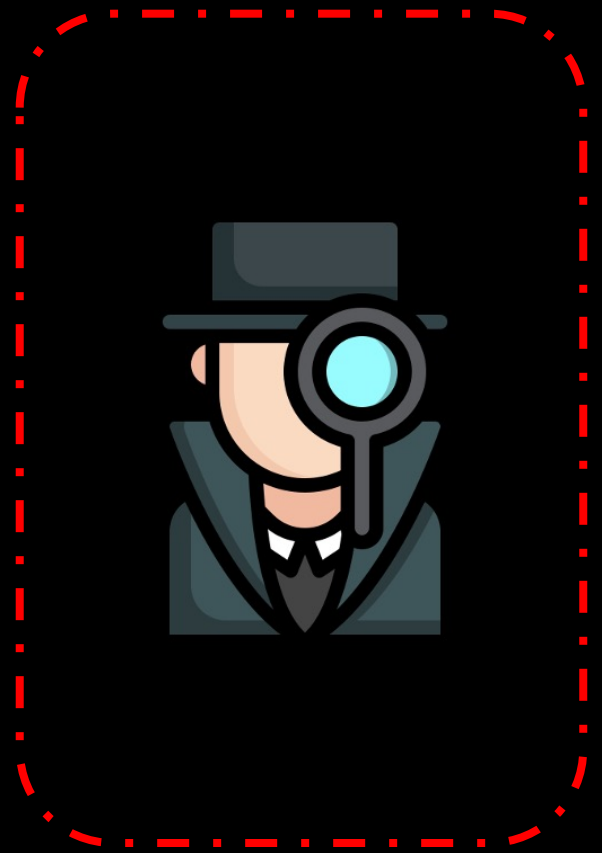
certThumbprint=<THUMBPRINT>
instanceId=<CI_NAME>
resource=https%3A%2F%2Fmanagement.core.windows.net%2F

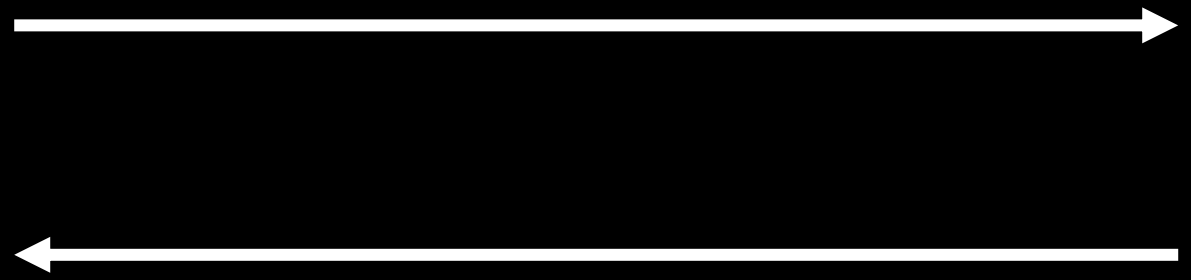


*/mnt/batch/tasks/startup/certs/*sha1-<THUMBPRINT>.{pem,key}

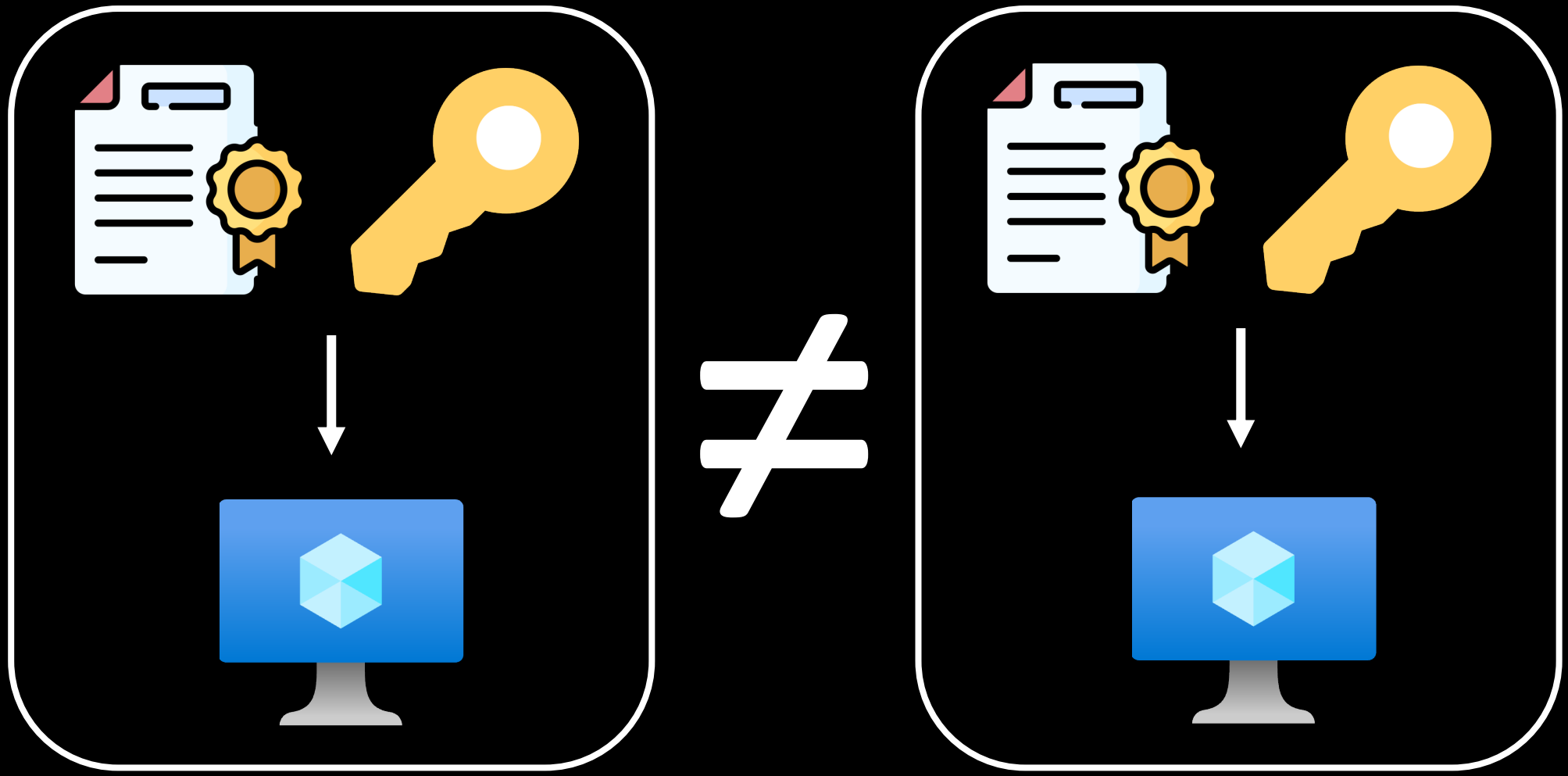


200 OK with M.I. JWT



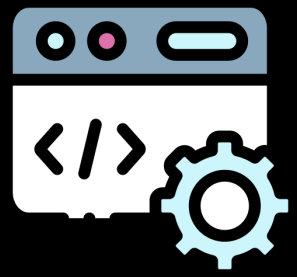


401 Unauthorized



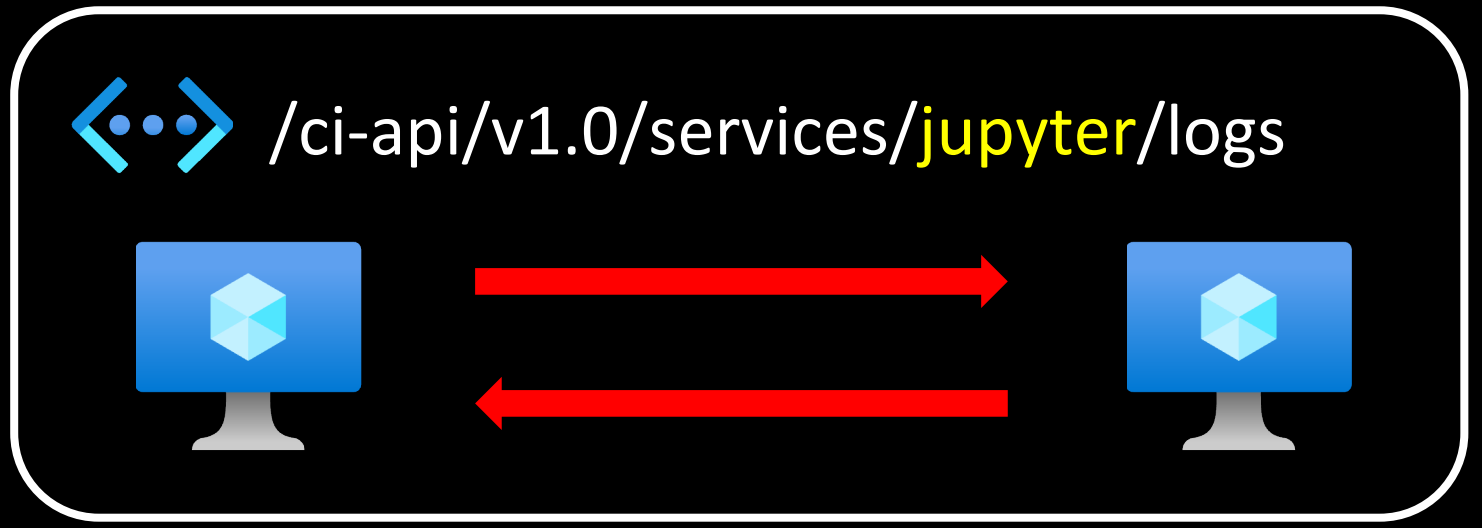
Let’s see *everything*

dsimountagent



```
[Unit]
Description=Azure Batch AI DSI Mounting Agent

[Service]
Type=simple
TimeoutStartSec=0
Restart=always
LimitNOFILE=65536
LimitCORE=infinity
CPUSchedulingScheduler=best-effort
CPUSchedulingPriority=0
EnvironmentFile=/mnt/batch/tasks/startup/wd/dsi/dsimountagentenv
WorkingDirectory=/mnt/batch/tasks/startup/wd/dsi
ExecStart=/mnt/batch/tasks/startup/wd/dsimountagent
StandardOutput=syslog
StandardError=syslog
SyslogIdentifier=dsimountagent

[Install]
WantedBy=multi-user.target
```

MLSEC Spying The Scientist



azureuser : TTY=pts/0 ; PWD=/ ; USER=root ;
COMMAND=/usr/bin/cat /etc/shadow

MLSEC Spying The Scientist

Azure Machine Learning Information Disclosure Vulnerability

CVE-2023-28312
Security Vulnerability

Released: Apr 11, 2023 Last updated: Aug 22, 2023

Assigning CNA: Microsoft

CVE-2023-28312

Impact: Information Disclosure Max Severity: Important

CVSS:3.1 6.5 / 5.7

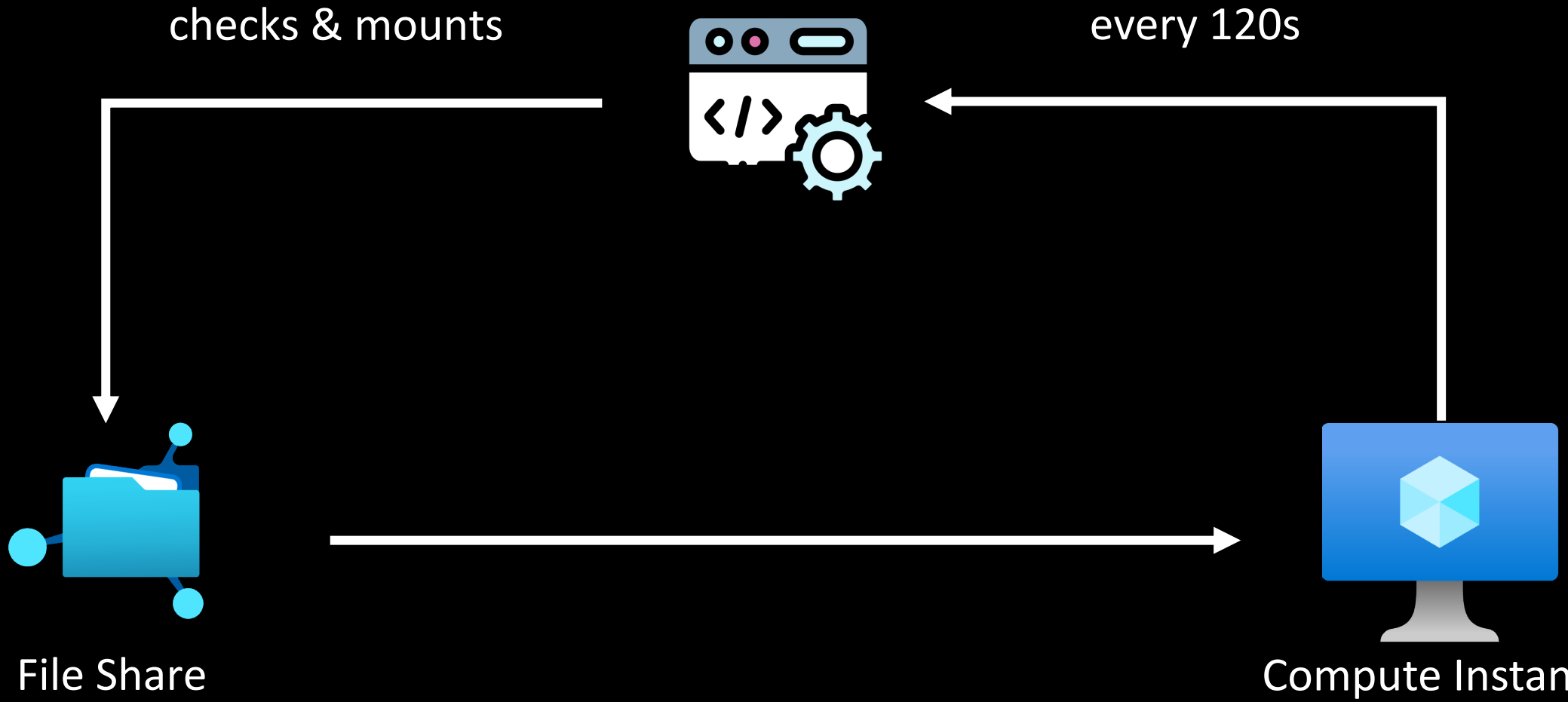
https://msrc.microsoft.com/update-guide/vulnerability/CVE-2023-28312

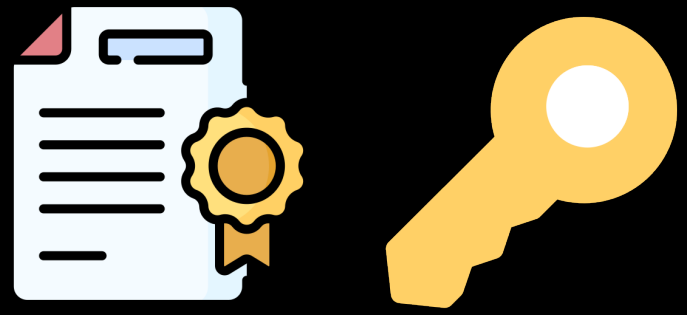
Config of dsimountagent

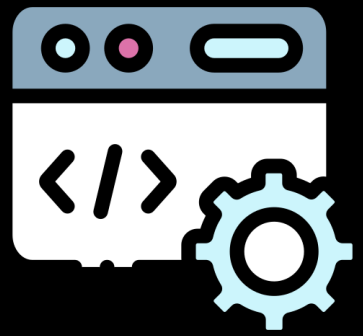
```
AZ_LS_ENCRYPTED_SYMMETRIC_KEY=eyJraWQiOiJCNUQxMTc0MTRDOUYxODA1MEI4M0YyRE
AZ_BATCHAI_CLUSTER_CERTIFICATE_PEM=-----BEGIN PRIVATE KEY-----;localKey
AZ_BATCHAI_CLUSTER_PRIVATE_KEY_PEM=-----BEGIN PRIVATE KEY-----;localKey
AZ_BATCHAI_XDS_ENDPOINT=https://eastasia.cert.api.azureml.ms/xdsbatchai
```

A section of environment variables used by DSIMountAgent

Purpose of dsimountagent



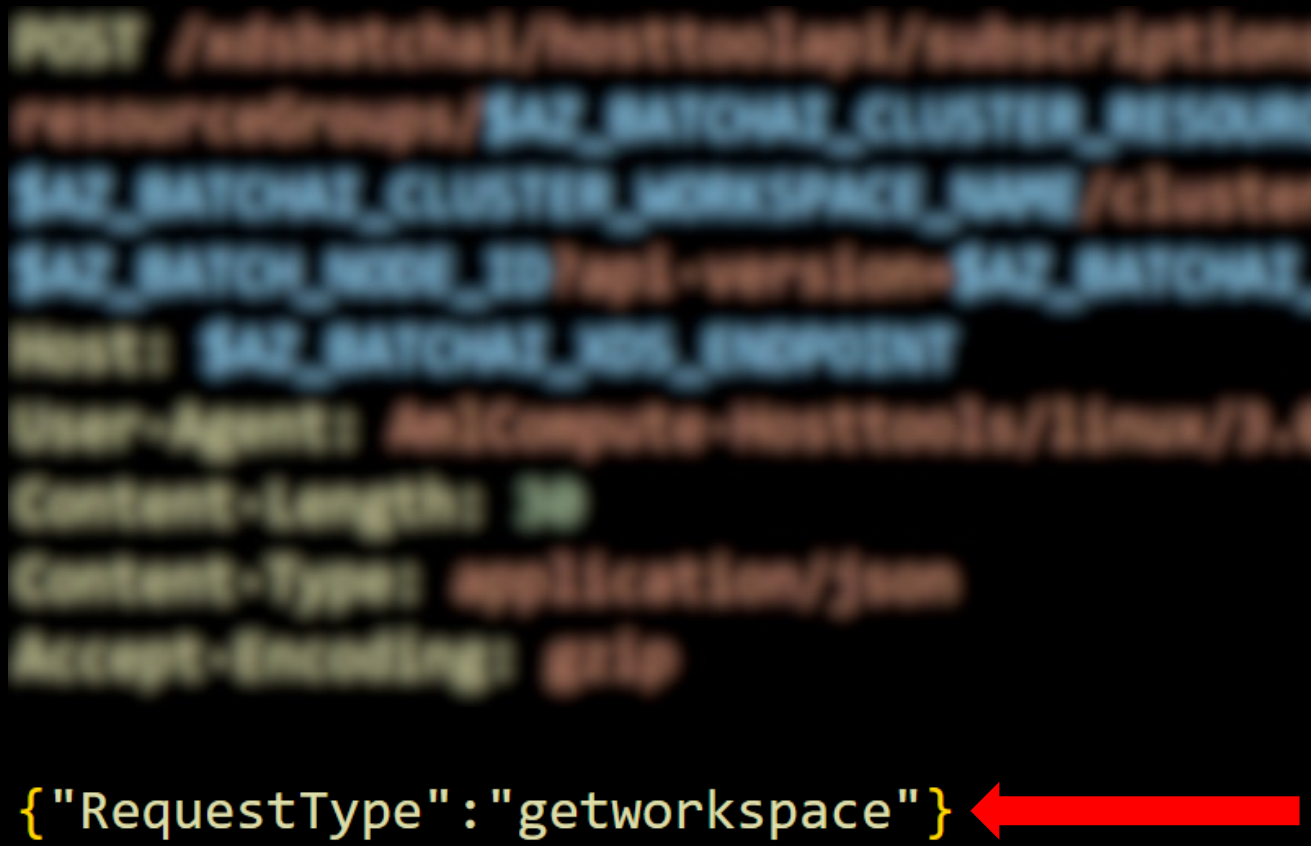




dsimountagent

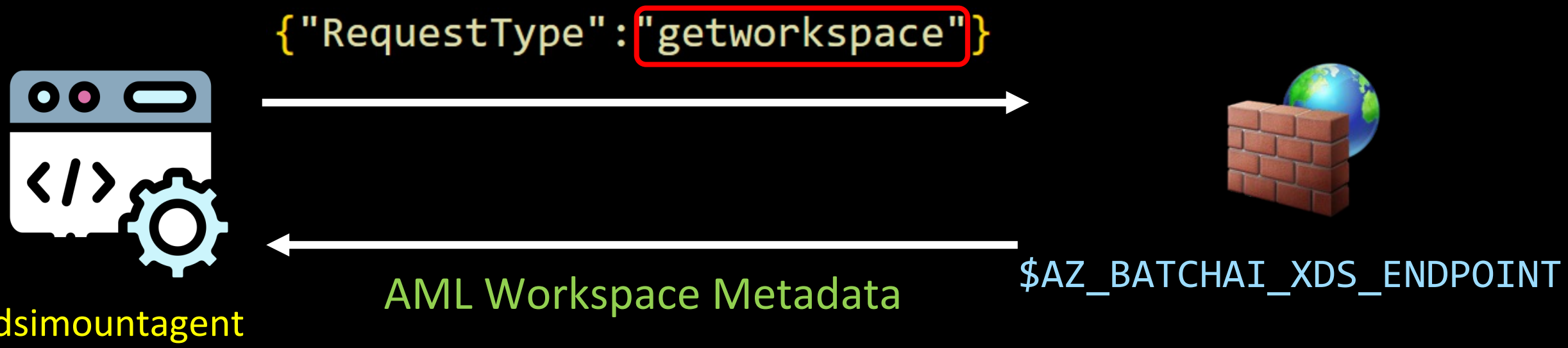
$AZ_BATCHAI_XDS_ENDPOINT

Outbound Traffic from dsimountagent



Fetching AML Workspace Information

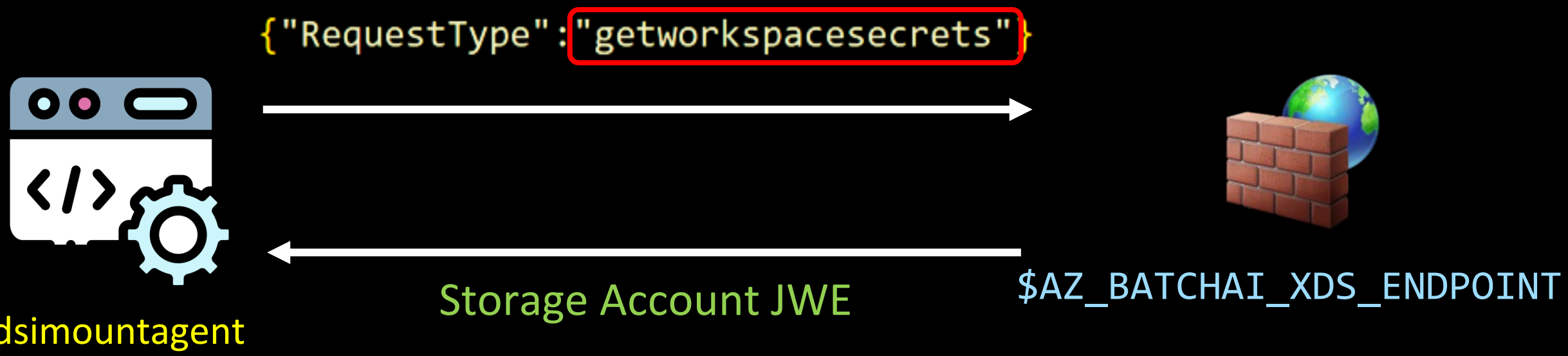
fn: hosttools/clients.**GetWorkspaceInfo**



```
"name": "amldemo",
"id": "/subscriptions/[redacted]re
"location": "eastasia",
"tags": {},
"properties": {
  "friendlyName": "amldemo",
  "description": "",
  "storageAccount": "/subscriptions/[redacted]
  "keyVault": "/subscriptions/[redacted]
  "applicationInsights": "/subscriptions/[redacted]
  "hbiWorkspace": false,
  "tenantId": "[redacted]",
  "imageBuildCompute": null,
  "provisioningState": "Succeeded",
  "containerRegistry": "/subscriptions/[redacted]
  "creationTime": "[redacted]",
  "subscriptionResourceGroupMoveState": null,
  "subscriptionState": null,
  "subscriptionStatusChangeTimeStampUtc": null,
```

Fetching Storage Account Key

fn: hosttools/clients.**GetWorkspaceSecrets**



```
{
  "errorCode":"Success",
  "response":"{\"AccountName\":\"<redacted>\",
  \"AccountKeyJWE\":\"eyJraWQiOiI2ZDhiMmVlOC0wN2ZlLTRlM2ItOTJiYy00MWIyMmFhZDM1ZWEiLCJhbGciOiJkaXIiL
  CJlbmMiOiJBMjU2Q0JDLUhTNTEyIn0..qN9urvrXK1SpyNIaJRdt_A.
  GirzYmKVSPoPXUdSDHMvKO9xIo9xMtjQifszY77ymnRrCatI_gYtsEyhoQLWwhk5Klfn2KbBvD9gF5bM3_1vXsvWeu-DHzbUC
  NznJ6Ca4z0i5Xg6jOBCuee60CM8ZFK1.Z9zMViTPXs2zefaO5qD2LNzphG1OkDuIhgGohz-wVFk\",
  \"SasTokenJWE\":null}"
}
```


$AZ_LS_ENCRYPTED_SYMMETRIC_KEY

$AZ_BATCHAI_CLUSTER_PRIVATE_KEY_PEM

Decrypted Symmetric Key

dsimountagentenv/dsiidlestopagentenv

Decrypted Symmetric Key

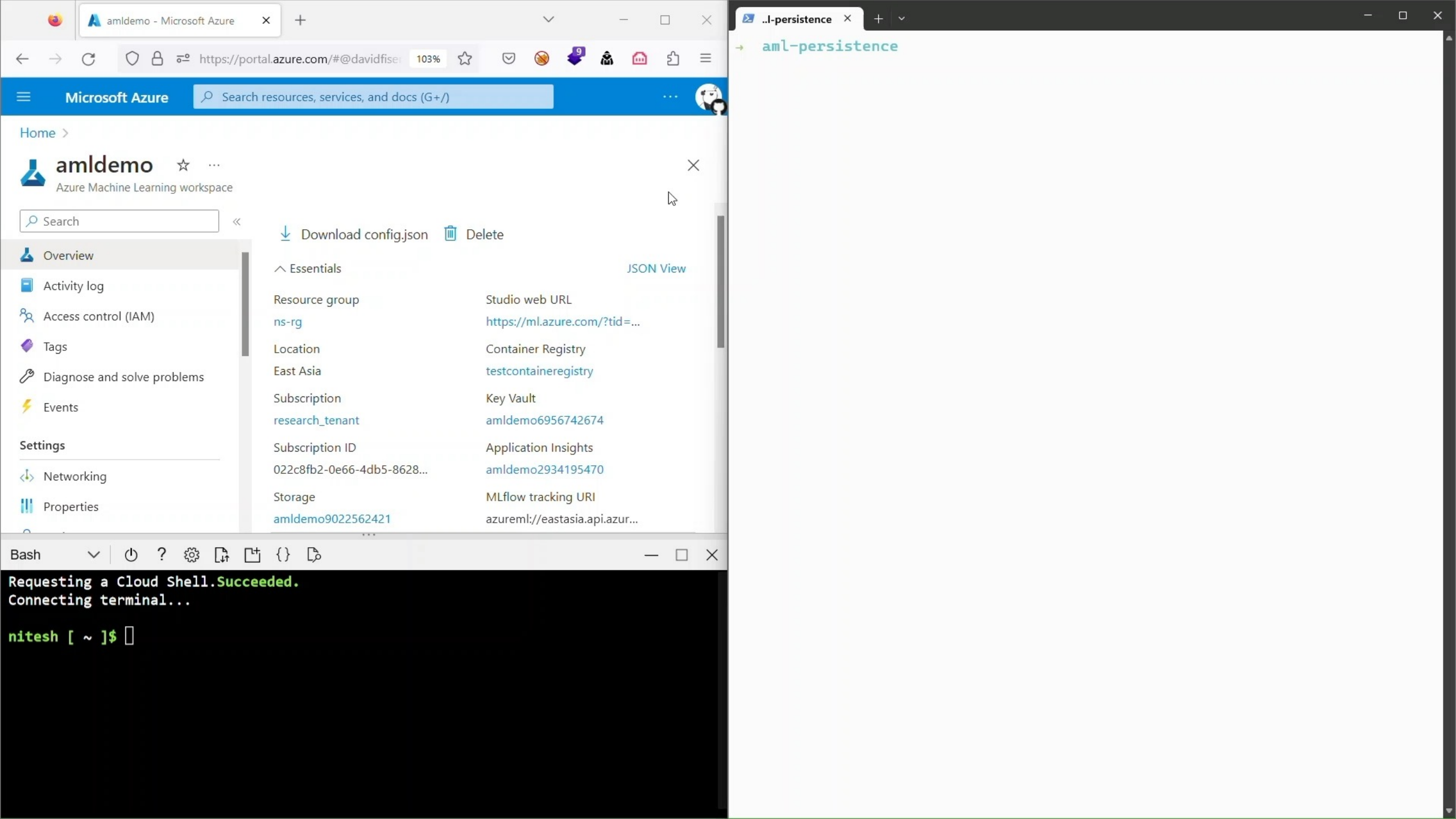
JWE of Storage Account Access Key

Storage Account Access Key

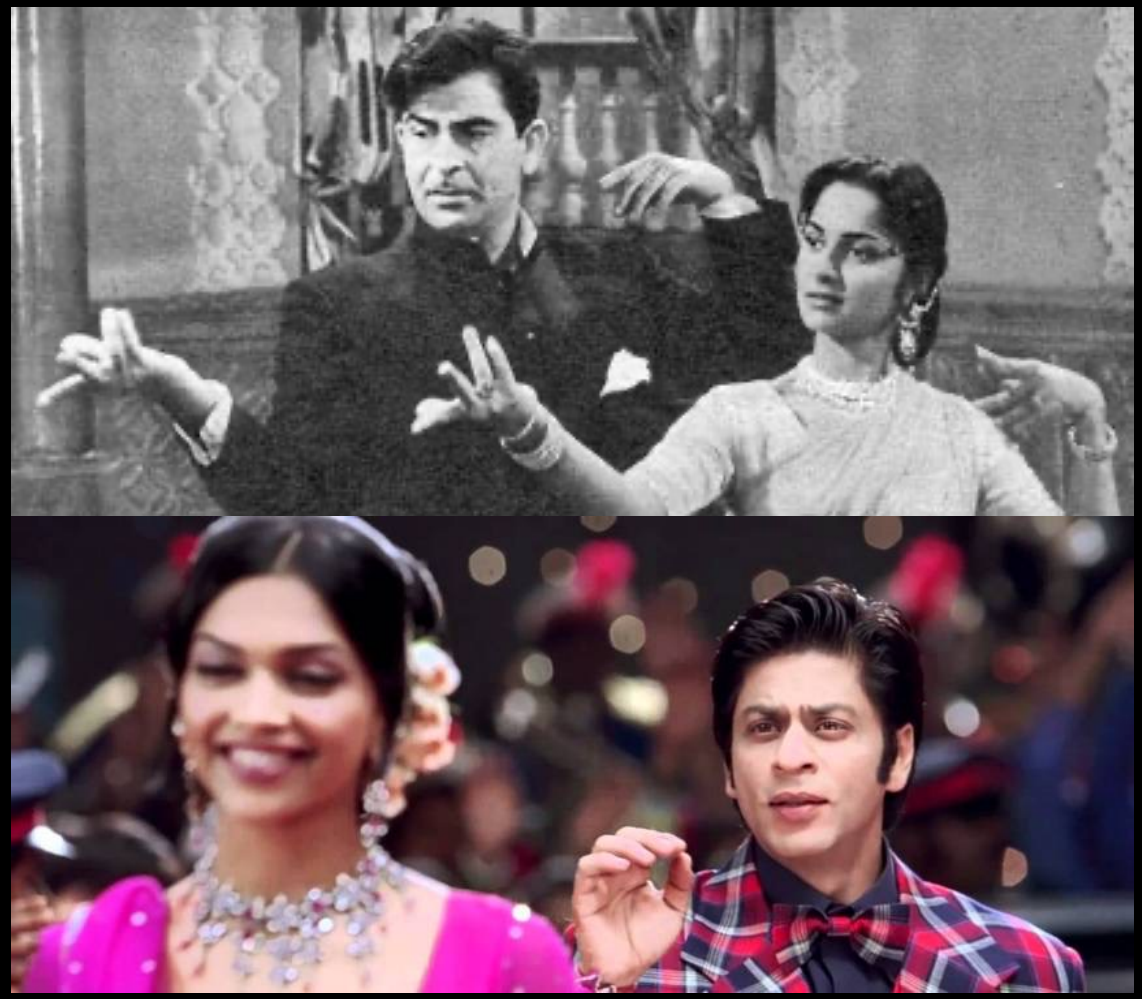
Attack Scenario

Storage Account Access Key

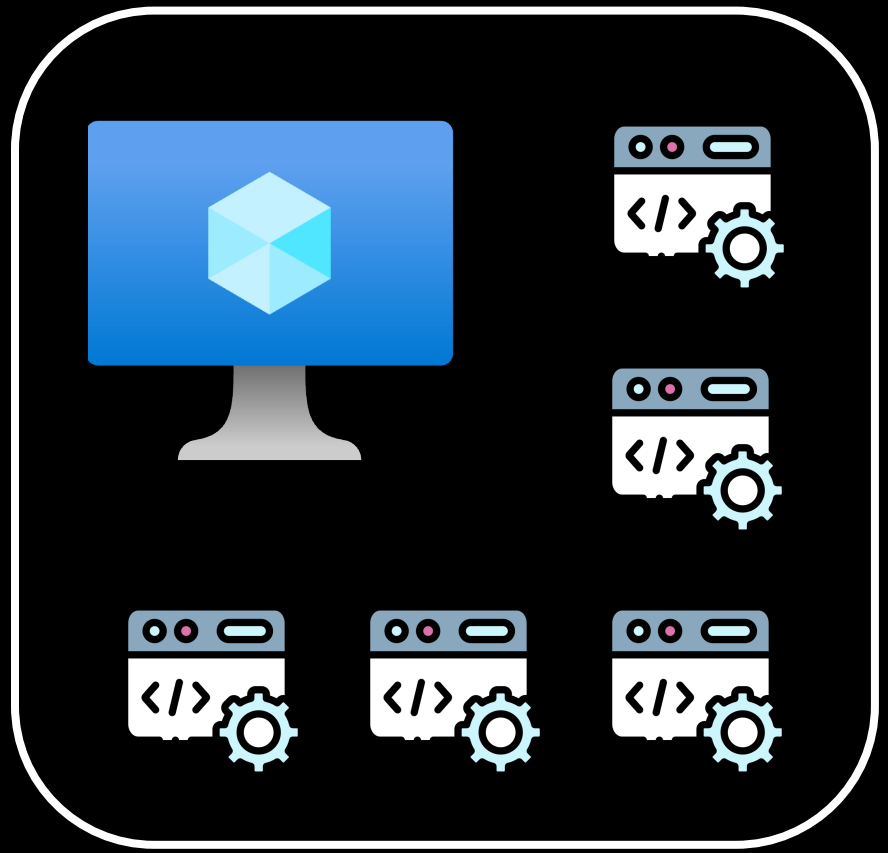
Does rotating the key help?

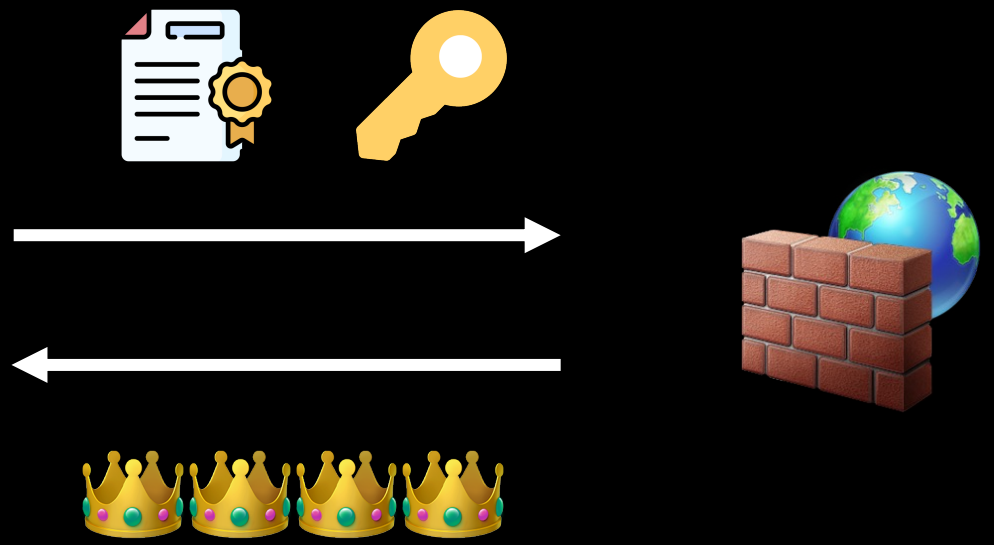

amldemo - Microsoft Azure
https://portal.azure.com/#@davidfiser
103%
Microsoft Azure
Search resources, services, and docs (G+/)
Home
amldemo
Azure Machine Learning workspace
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Events
Settings
Networking
Properties
Download config.json
Delete
Essentials
JSON View
Resource group
ns-rg
Location
East Asia
Subscription
research_tenant
Subscription ID
022c8fb2-0e66-4db5-8628...
Storage
amldemo9022562421
Studio web URL
https://ml.azure.com/?tid=...
Container Registry
testcontaineregistry
Key Vault
amldemo6956742674
Application Insights
amldemo2934195470
MLflow tracking URI
azureml://eastasia.api.azur...
Bash
Requesting a Cloud Shell.Succeeded.
Connecting terminal...
nitesh [~]$
..l-persistence
aml-persistence

Does the story end here?



Cloud Agents





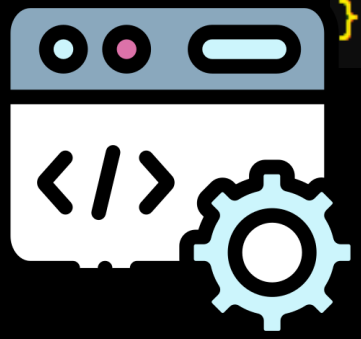
Fetching more {“RequestType”:”?”}

Address	Text
hosttools_clients_xdsApiCallerReal_generateRequestSchema+63	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_generateXDSApiRequestSchema+299	jmp hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_UpdateJobState+6C1	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_UpdateJobEndpointState+4B3	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_generatePostJobStuckSchema+2D9	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_GenerateSas+452	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_GenerateDataStoreCredentials+452	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_GetAADToken+20D	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_GetACRToken+20D	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_GetSecret+164	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_GetACRDetails+224	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_GetAppInsightsInstrumentationKey+4B	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_GetDsiUpdateSettings+4B	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_PostDsiUpdateSettings+60	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_GetWorkspaceSecrets+253	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_GetWorkspaceInfo+253	call hosttools_clients_generateXDSApiRequestSchema
hosttools_clients_CallXDSToRecoverJobWithUnhealthyNode+22D	call hosttools_clients_generateXDSApiRequestSchema

Fetching System Assigned MI JWT

fn: hosttools/clients.**GetAADToken**

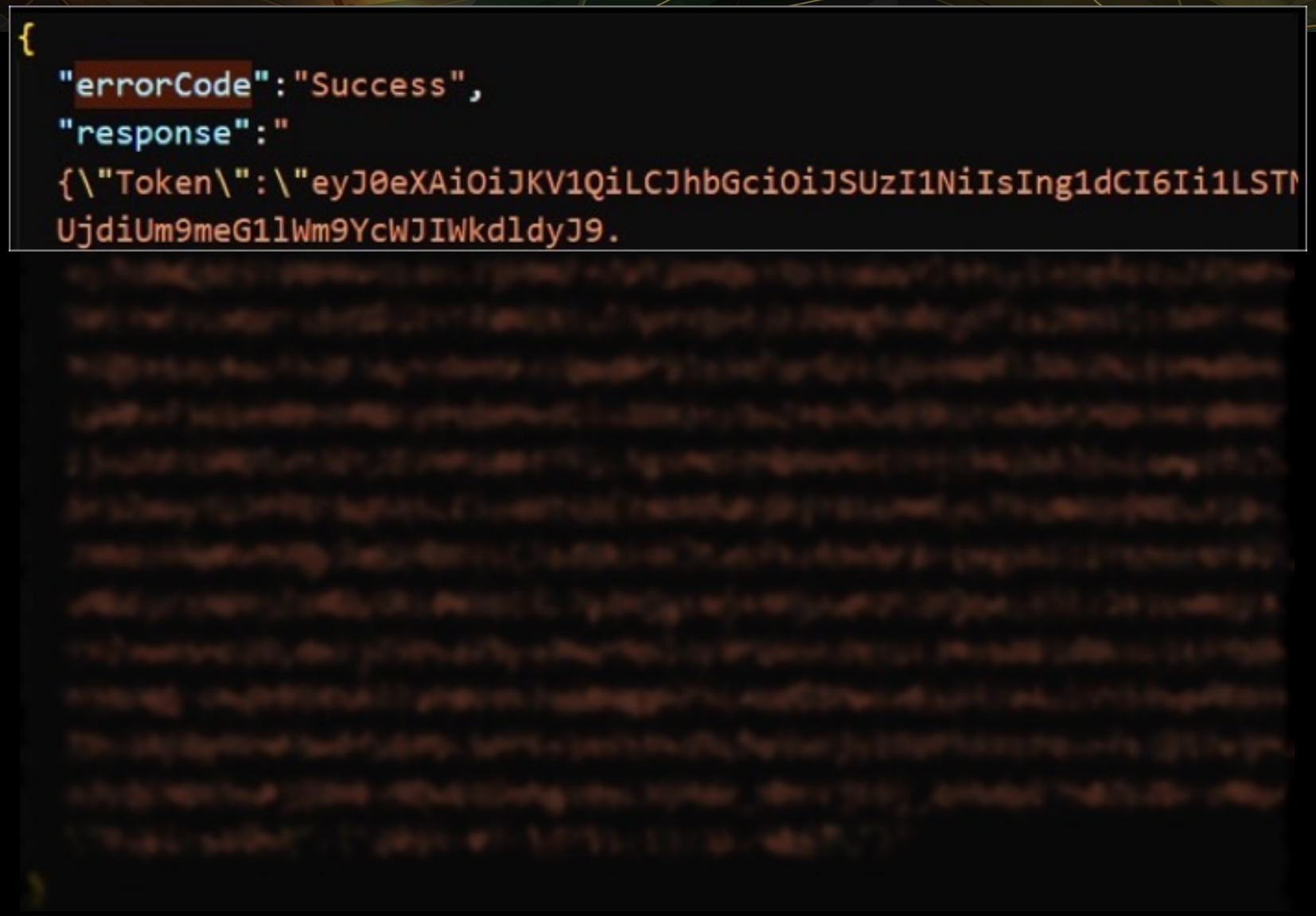
```
{
  "RequestType":"getaadtoken",
  "RequestBody":"{\"resource\":\"https://management.azure.com/\"}"
}
```



identityresponderd

$AZ_BATCHAI_XDS_ENDPOINT

Entra ID JWT of Managed Identity

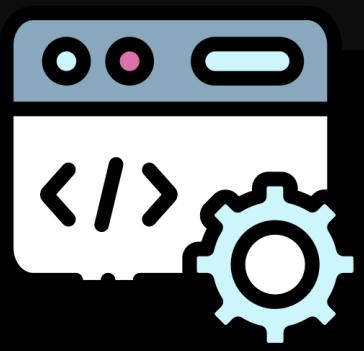


Entra ID JWT of System Assigned Managed Identity

Fetching User Assigned MI JWT

fn: hosttools/clients.**GetAADToken**

```
{
  "RequestType":"getaadtoken",
  "RequestBody":"{\"resource\":\"https://management.azure.com\",\"client_id\":\"REDACTED\"}"
}
```

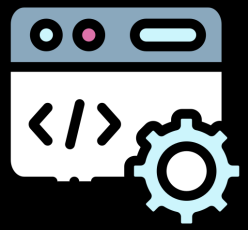


$AZ_BATCHAI_XDS_ENDPOINT

Entra ID JWT of Managed Identity

identityresponderd

Recap



$AZ_BATCHAI_XDS_ENDPOINT

'whoami' of AML Workspace
Storage Account Access Key
Managed Identity JWTs
…

But we can use the logs, right?

Legitimate Activity

```
from azureml.core.authentication import MsiAuthentication


client_id_value = os.getenv("DEFAULT_IDENTITY_CLIENT_ID") #id
msi_identity_config = {"client_id": client_id_value}
msi_auth = MsiAuthentication(identity_config=msi_identity_config)
jwt.decode(msi_auth.get_token().token,options={"verify_signature": False})
```

$ az login --identity

Fetching Managed Identity JWT from a Compute Instance

Malicious Activity

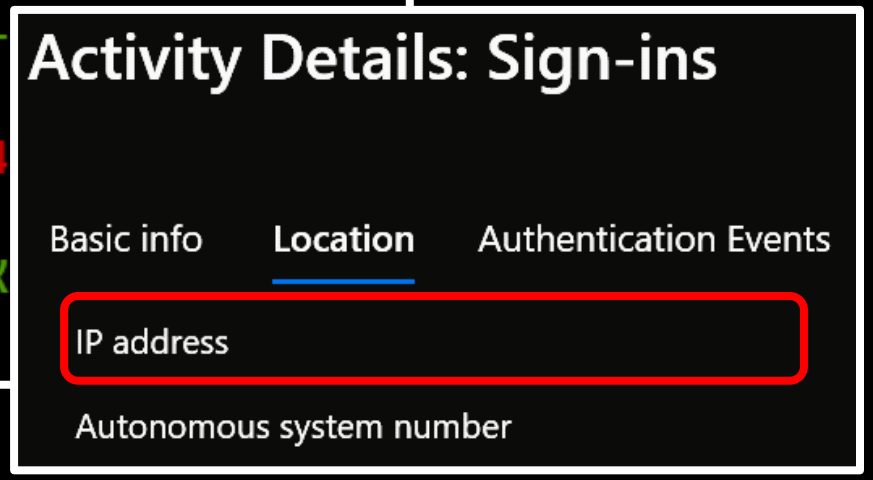

```
{
  "RequestType":"getaadtoken",
  "RequestBody":"{\"resource\":\"https://management.azure.com/\"}"
}
```

$AZ_BATCHAI_XDS_ENDPOINT

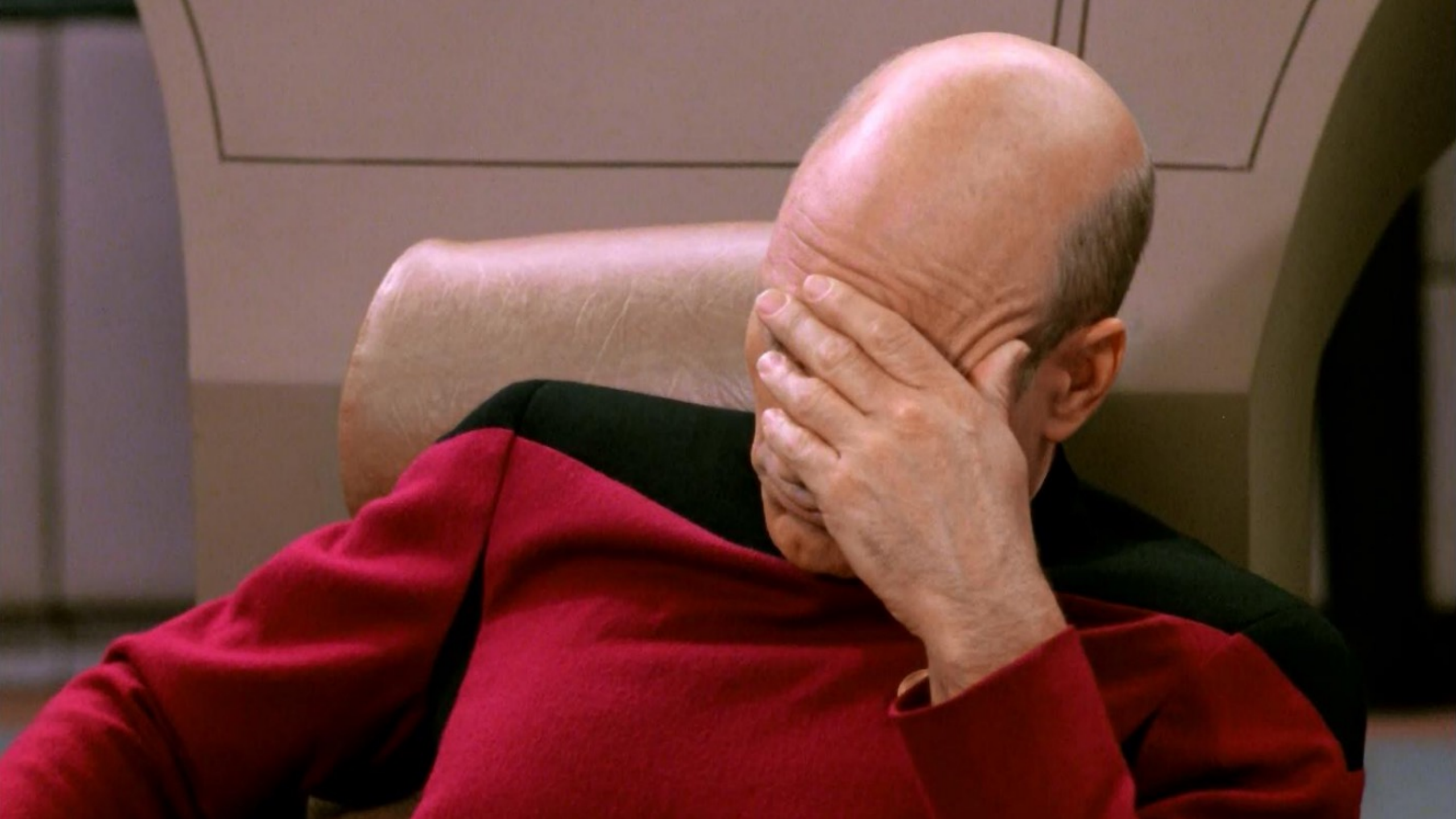
Entra ID JWT of Managed Identity

Generated Logs

```
→  Downloads diff Attacker.json Compute-Instance.json
2,3c2,3
<    "id": "17a0e470-7e40-4b76-aa3e-42f8f5bc4600",
<    "createdDateTime": "2023-07-15T11:07:07Z",
---
>    "id": "e089d82d-16f6-4f95-8878-f14a8a3ad300",
>    "createdDateTime": "2023-07-15T10:54:48Z",
13c13
<    "correlationId": "0d34d004-6b11-4523-801f-2194fb9b46b2",
---
>    "correlationId": "36c3b381-7baf-436d-8909-
48c48
<    "uniqueTokenIdentifier": "cOSgF0B-dkuqPkL4
---
>    "uniqueTokenIdentifier": "LdiJ4PYWlU-IePFK
→  Downloads
```



How to detect stolen certs?



Why is this even a vulnerability?

System-assigned. Some Azure resources, such as virtual machines allow you to enable a managed identity directly on the resource. When you enable a system-assigned managed identity:

- A service principal of a special type is created in Azure AD for the identity. The service principal is tied to the lifecycle of that Azure resource. When the Azure resource is deleted, Azure automatically deletes the service principal for you.
- By design, only that Azure resource can use this identity to request tokens from Azure AD.
- You authorize the managed identity to have access to one or more services.
- The name of the system-assigned service principal is always the same as the name of the Azure resource it is created for. For a deployment slot, the name of its system-assigned identity is `<app-name>/slots/<slot-name>`.

https://learn.microsoft.com/en-us/azure/active-directory/managed-identities-azure-resources/overview

This is trust.. But did you *verify*?

WHY NO IP ADDRESS

AZURE SUPPORT?

Call Azure Support! 🔥

Azure Managed Identity can obtain a token from Managed Identity endpoint from inside the Azure Virtual Network. The token acquisition endpoint for the managed identities 'http://169.254.169.254/metadata/identity/oauth2/token?api-version=2018-02-01&resource=https%3A%2F%2Fvault.azure.net&client_id=<UAMI CLIENT ID>' is not accessible from outside of the resource, hence the token acquisition call needs to come from the resource to which the managed identity is assigned.

Due to which the sign-in logs don't show any IP Address, but you can reference it to the private IP of the resource making the token acquisition call.

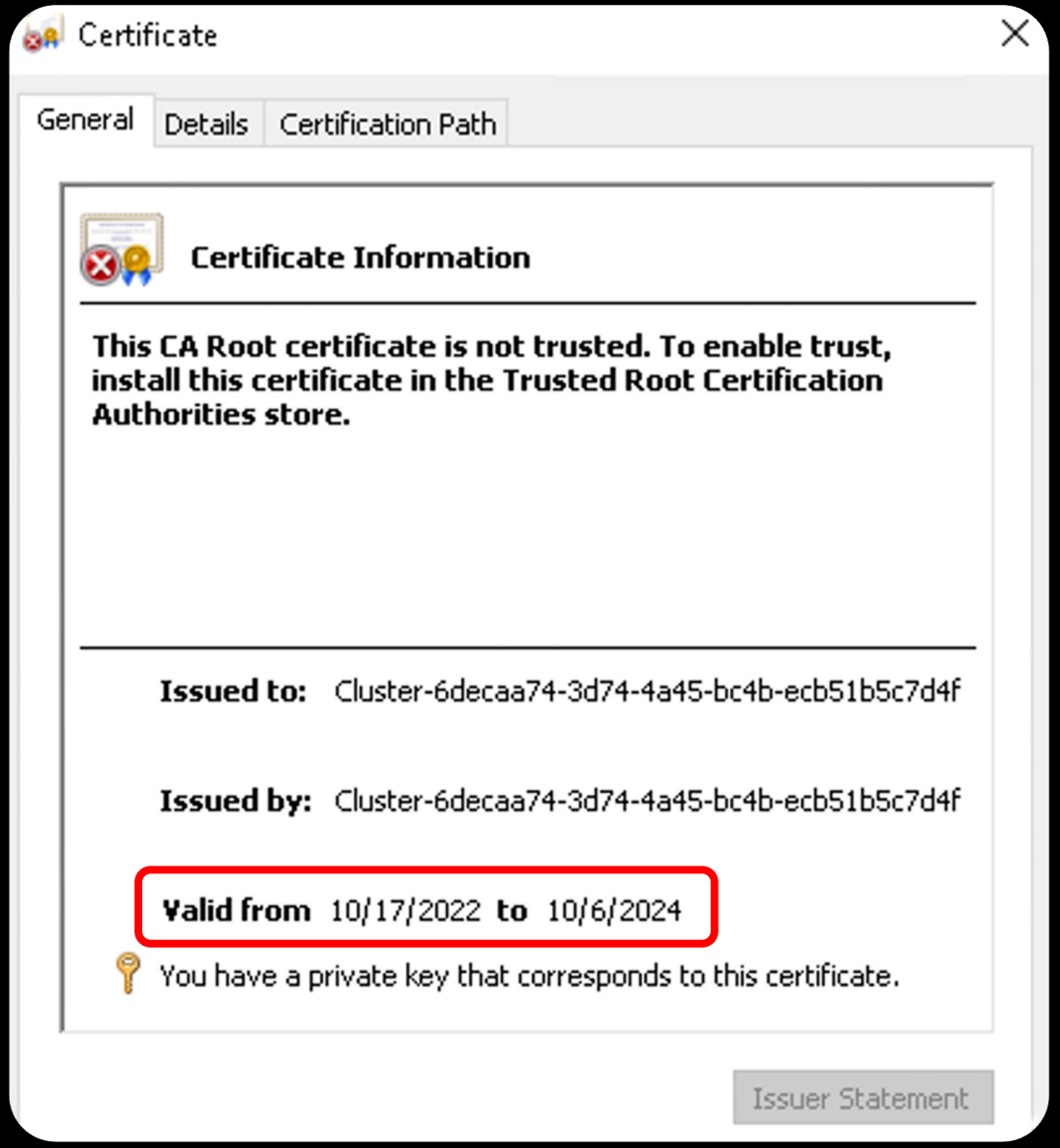
Call Azure Support! 🔥

Is it implied that public IP address of the resource from where a MI token has been fetched will not be visible in any of the log sources across Azure such as Microsoft Graph logs?

[A] No, Microsoft Entra doesn't record the IP address of the source while populating the sign-in. It is assumed that the sign-in happened from the targeted managed identity resource.

Persistence

- Fetch rotated keys, MI JWTs, etc.
- Certificate valid for two years
- Delete  if cert. compromised
- Logging discrepancies == 🔥



Disclosure Timeline

04/07/23 – ZDI reported the vulnerability to the vendor.
04/11/23 – The vendor acknowledged the report.
07/13/23 – ZDI asked for an update.
07/19/23 – The vendor asked us to join a call to discuss the report.
07/19/23 – ZDI joined the call and provided the vendor with additional details.
07/20/23 – The vendor states that they are considering this bug low severity and that they would release a fix in 30-45 days.
07/20/23 – The ZDI informed the vendor that the case is due on 08/05/23 and that we are publishing this case as a zero-day advisory on 08/09/23.

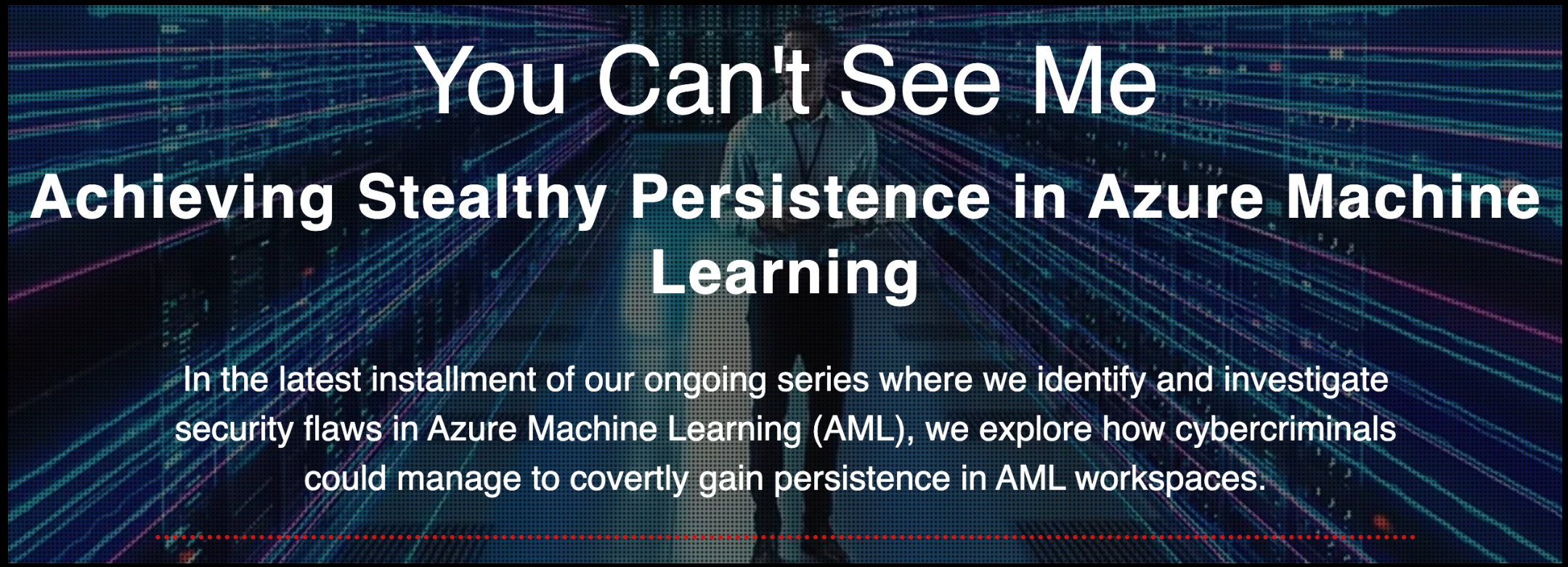
August 9th, 2023

(0Day) Microsoft Azure Machine Learning Compute Instance certificate Exposure of Resource to Wrong Sphere Information Disclosure Vulnerability

ZDI-23-1056
ZDI-CAN-20771

https://www.zerodayinitiative.com/advisories/ZDI-23-1056/

References


You Can't See Me
Achieving Stealthy Persistence in Azure Machine Learning
In the latest installment of our ongoing series where we identify and investigate security flaws in Azure Machine Learning (AML), we explore how cybercriminals could manage to covertly gain persistence in AML workspaces.

How many services support M.I.?

50+ Azure Services

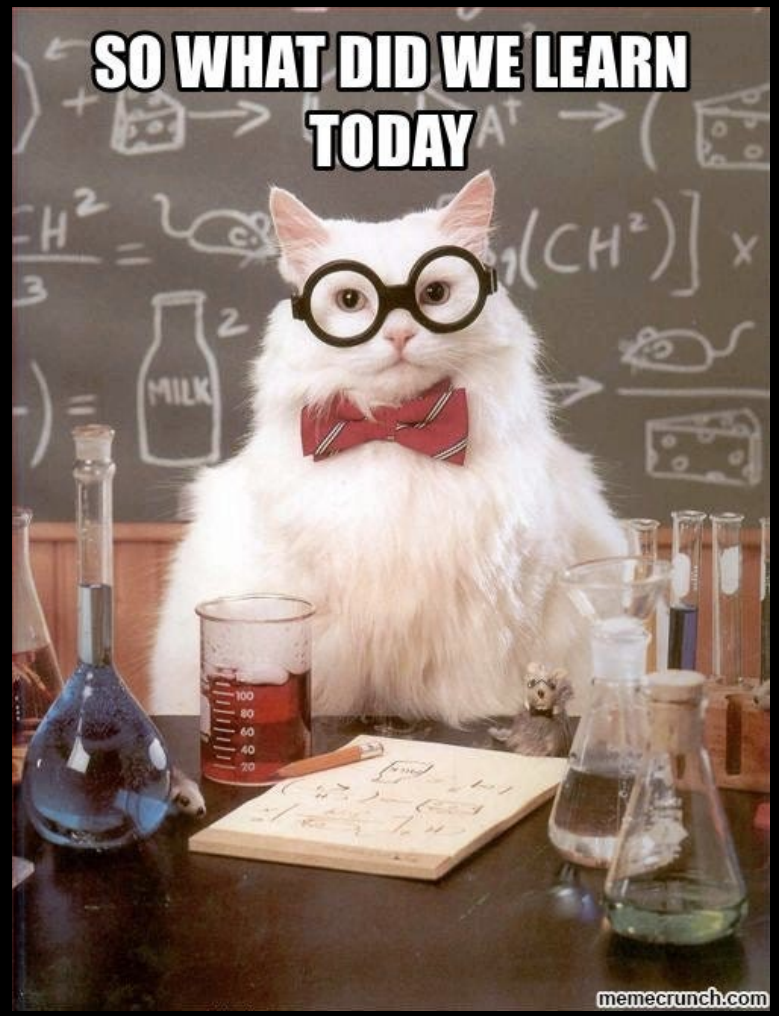
https://learn.microsoft.com/en-us/entra/identity/managed-identities-azure-resources/managed-identities-status#services-supporting-managed-identities

Future Scope: Azure Services x M.I. 🎯

API Management	Azure Container Instance	Azure Event Hubs
Application Gateway	Azure Container Registry	Azure Image Builder
Azure App Services	**Azure Machine Learning**	Azure IoT Hub
Azure Arc	Azure Data Box	Azure Kubernetes Service
Azure Automanage	Azure Data Explorer	Azure Logic Apps
Azure Automation	Azure Data Factory	Azure Log Analytics
Azure Batch	Azure Data Lake	Azure Media services
Azure Blueprints	Azure Data Share	Azure Service Fabric
Azure Cache	Azure DevTest Labs	Azure Stack Edge
Azure Container Apps	Azure Event Grid	Azure Virtual Machines

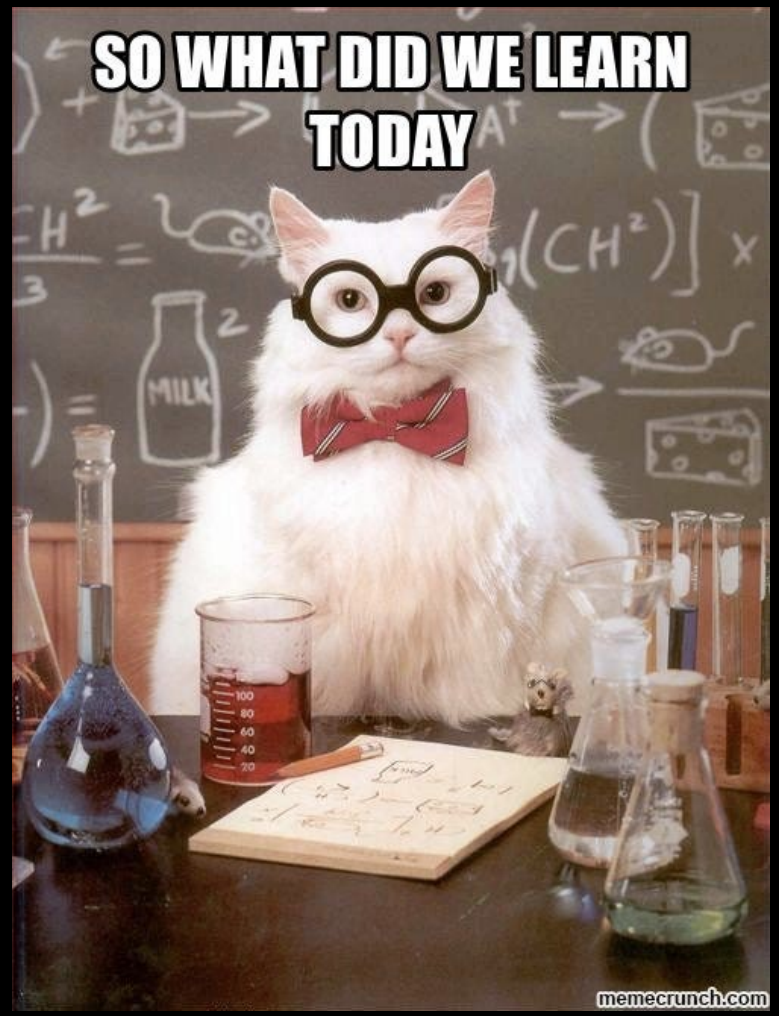
Takeaways

- Use environment variables carefully
- Threat model CSP services
- Least privilege for identities
- Examine Cloud APIs & find 🔥 bugs



Takeaways

- Test & Secure AuthN & AuthZ scopes
- Actionable logging for detection
- Assume Breach scenarios & edge cases
- Challenge official documentation



Acknowledgements

X: @thezdi

Q/A

Source: https://surveysparrow.com/blog/funny-customer-service-memes/

Find us 👇

niteshsurana.com

x.com/anu4is

⚡ Black Hat Sound Bytes ⚡

Assume breach x edge cases == variants of bugs

Challenge official documentation

Examine Cloud APIs & find 🔥 bugs