

Here's Some S\*\*\* I Learned:  
Enumerating Azure  
AD and ARM



# whoami

- **Leron Gray**
  - Azure Red Team @ Microsoft
  - aka daddycocoaman
    - <https://daddycocoaman.dev>
    - <https://github.com/daddycocoaman>
  - aka Ohm-I (*pronounced oh-my*)
    - Nerdcore rapper
    - <https://mcohmi.com>
  - Ten-year Navy veteran
  - Lover of Python and Pythonic things

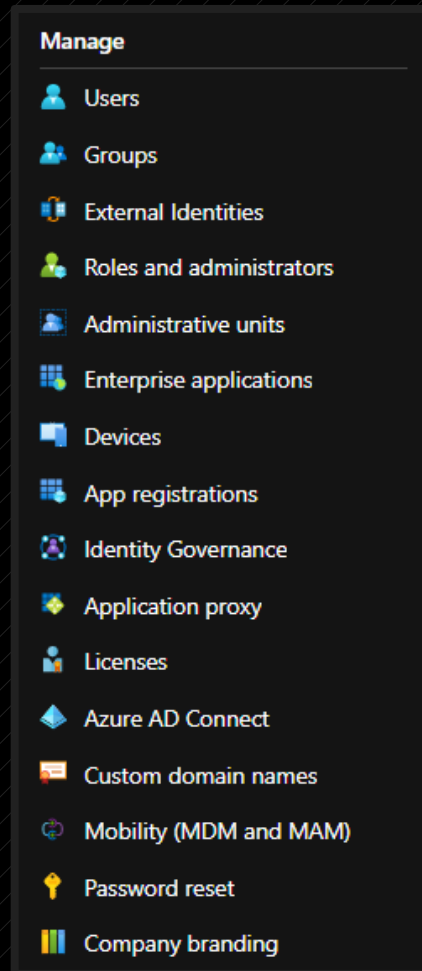
# Agenda

- Azure Active Directory
- Azure Resource Manager
- Tools for interacting with AAD and ARM
- Stormspotter

# Azure Active Directory

The image features a solid blue background. In the bottom right corner, there are several overlapping geometric shapes: a dark grey triangle pointing towards the top right, a medium blue trapezoidal shape, and a dark blue trapezoidal shape, all creating a layered, architectural effect.

# Azure Active Directory



- Cloud-based identity and access management service, which helps your employees sign in and access resources.
- So basically...

SORTA LIKE ACTIVE DIRECTORY....BUT IN AZURE!

**WOW!**

# AAD Objects

## Users

- Standard user/member identity.

## Groups

- A group of objects (users, groups, service principals, etc).

## Applications

- Used as a template to create one or more service principal objects.

## Service Principals

- Local representation, or application instance, of a global application object in a single tenant or directory.

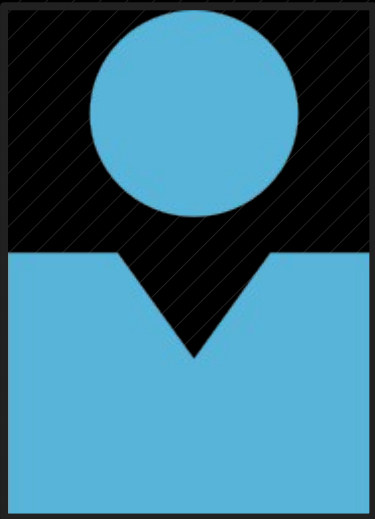
## Devices

- Managed devices can be added to AAD

## Roles

- Defines permissions for AAD objects
- Examples: Global/Company Administrator, User Account Administrator, Directory Members

# AAD Users



- Standard identity for a user.
- Users can be internal or external
  - **Internal:** <alias>@<tenant>.onmicrosoft.com
  - **External:** <alias>\_<HomeTenant>#EXT#@<tenant>.onmicrosoft.com
  - Example:

Leron.Gray@stormspotter.onmicrosoft.com

Leron.Gray\_microsoft.com#EXT#@stormspotter.onmicrosoft.com

# Kelly Santana

Kelly.Santana@stormspotter.onmicrosoft.com



[User Sign-ins](#)

[Group memberships](#)

1

Sep 20

Sep 27

Oct 4

Oct 11

## Identity

Name

Kelly Santana

First name

Kelly

Last name

Santana

User Principal Name

Kelly.Santana@stormspotter.onmicrosoft.com

User type

Member

Object ID

d880ee73-a1fa-4055-bbc3-2ae3bf200d59

Source

Azure Active Directory

## Job info

Job title

-- --

Department

-- --

Manager

Company name

-- --

Employee ID

-- --

## Settings

Block sign in

Yes

Usage location

United States

## Contact info

Street address

23099 Mckee Shores Apt. 962

State or province

WW

Country or region

US

City

Crystalfort

ZIP or postal code

-- --

Office phone

731-884-2213

Email

-- --

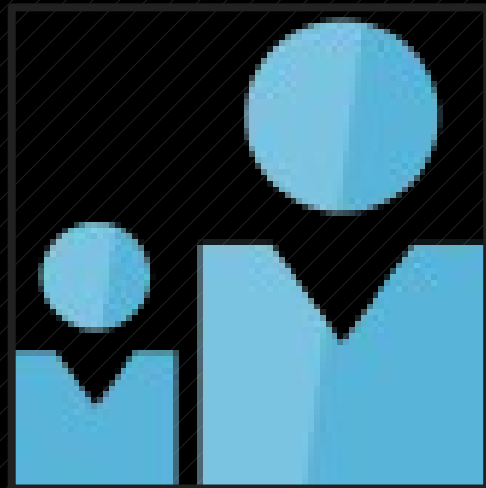
Alternate email

-- --

Proxy address



# AAD Groups



## SA Sales

Membership type: Assigned

Source: Cloud

Type: Security

Object Id: bbce3dd3-f5e6-4496-a8ed-0da219551b9f

Creation date: 6/9/2020, 1:24:37 PM

**Direct members**

6 Total    5 User(s)    1 Group(s)    0 Device(s)    0 Other(s)

**Group memberships**    **Owners**    **Total members**

0    0    9

# Direct Members

**Direct members** All members

Search by name + Add filters

Name	Type
<input type="checkbox"/> CH Caroline Harris	User
<input type="checkbox"/> KA Katherine Austin	User
<input type="checkbox"/> JY Jason Young	User
<input type="checkbox"/> SC Sales Cashiers	Group
<input type="checkbox"/> KS Kelly Santana	User
<input type="checkbox"/> KT Kyle Torres	User

# Unrolled Members

Direct members **All members**

Search by name + Add filters

Name	Type
CH Caroline Harris	User
KA Katherine Austin	User
JA Johnny Anderson	User
KH Kristen Howell	User
JY Jason Young	User
SC Sales Cashiers	Group
DF Dave Frank	User
KS Kelly Santana	User
KT Kyle Torres	User

Home > stormspotter > Groups > Sales

### Sales | Members

Group

« + Add members Remove Refresh

This page includes previews available for your evaluation.

Overview  
Diagnose and solve problems

Manage

- Properties
- Members**
- Owners
- Administrative units
- Group memberships
- Applications
- Licenses
- Azure role assignments

**Direct members**

	Name
<input type="checkbox"/>	CH Caroline Harris
<input type="checkbox"/>	JY Jason Young
<input type="checkbox"/>	KA Katherine Austin
<input type="checkbox"/>	KS Kelly Santana
<input type="checkbox"/>	KT Kyle Torres
<input type="checkbox"/>	SC Sales Cashiers

Home > stormspotter > Groups > Sales

### Sales | Owners

Group

« + Add owners Remove Refresh | Columns Preview features

This page includes previews available for your evaluation. View previews →

Overview  
Diagnose and solve problems

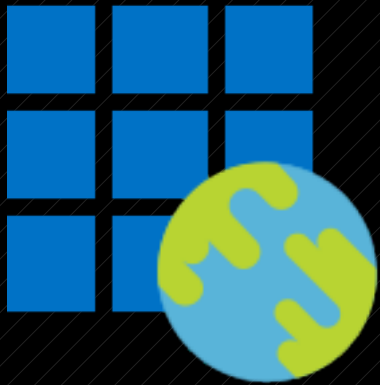
Manage

- Properties
- Members
- Owners**
- Administrative units
- Group memberships

	Name	Type
<input type="checkbox"/>	KS Kelly Santana	User
<input type="checkbox"/>	SalesAADSPN	Service Principal

- Groups can have owners who don't have to be members of the group.

# AAD Applications



- Used as a template to create service principals for authentication.
- Applications can be single tenant or multi-tenant.
- Multi-tenant apps will be homed in the tenant they were created in, but the service principal will be created in the target tenant.

# SalesAADSPN | Properties

Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems

## Manage

- Properties
- Owners
- Roles and administrators (Pre...
- Users and groups
- Single sign-on
- Provisioning
- Application proxy
- Self-service

Save Discard Delete | Got feedback?

Enabled for users to sign-in? ⓘ

Yes No

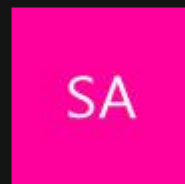
Name \* ⓘ

SalesAADSPN ✓

Homepage URL ⓘ



Logo ⓘ



Select a file



Application ID ⓘ

ce88c3f2-ea42-4667-9d37-f908178382ef



Object ID ⓘ

9d03d772-4645-4a32-8057-b876748f84a5



User assignment required? ⓘ

Yes No

Visible to users? ⓘ

Yes No

# AAD Service Principals



- Instance of an AAD application *somewhere*.
- Essentially a service account. Credentials can be added to log in as the identity.
  - Password
  - Certificates
- Creating an SPN directly will also create an application

# Application

Home > stormspotter > Enterprise applications >

**SalesAADSPN | Overview**  
Enterprise Application

- Overview
- Deployment Plan
- Diagnose and solve problems

**Manage**

- Properties
- Owners

### Properties

SA

Name ⓘ  
SalesAADSPN

Application ID ⓘ  
ce88c3f2-ea42-4667-9d37-f...

Object ID ⓘ  
9d03d772-4645-4a32-8057...

# Service Principal

Home > stormspotter >

**SalesAADSPN**

Search (Ctrl+/)

Delete Endpoints Preview features

Got a second? We would love your feedback on Microsoft identity

### Essentials

Display name : SalesAADSPN

Application (client) ID : ce88c3f2-ea42-4667-9d37-f908178382ef

Directory (tenant) ID : 087a8387-325b-444f-aa20-4258f6d6828c

Object ID : a10d46b1-fcb9-43c1-bce6-5eeda0565c30

Starting June 30th, 2020 we will no longer add any new features to

Overview

Quickstart

Integration assistant | Preview

### Manage

- Branding
- Authentication
- Certificates & secrets

# Devices

- AAD joined or registered device.
  - **Joined** – Typically corporate resource
  - **Registered** – Typically “Bring Your Own Device”



4 Devices

























Name	Enabled	OS	Version	Join Type
<input type="checkbox"/> [Redacted]	<input checked="" type="checkbox"/> Yes	Windows	10.0.18363.778	Azure AD joined
<input type="checkbox"/> legra-win-dev	<input checked="" type="checkbox"/> Yes	Windows	10.0.18362.0	Azure AD registered
<input type="checkbox"/> legra_Android_ [Redacted]	<input checked="" type="checkbox"/> Yes	Android	10.0	Azure AD registered
<input type="checkbox"/> legra_AndroidForW...	<input checked="" type="checkbox"/> Yes	AndroidForWork	10.0	Azure AD registered



# AAD Roles



- Define permissions for other AAD Objects.
- Built-in roles have a predefined set of permissions.
- Custom roles can be added but permissions should be audited to ensure roles aren't too permissive.

<input type="checkbox"/>	 Conditional Access administrator	Can manage conditional access capabilities.
<input type="checkbox"/>	 Customer LockBox access approver	Can approve Microsoft support requests to access customer organizational data.
<input type="checkbox"/>	 Desktop Analytics administrator	Can access and manage Desktop management tools and services.
<input type="checkbox"/>	 Directory readers	Can read basic directory information. Commonly used to grant directory read access to applications and guests.
<input type="checkbox"/>	 Directory writers	Can read and write basic directory information. For granting access to applications, not intended for users.
<input type="checkbox"/>	 Dynamics 365 administrator	Can manage all aspects of the Dynamics 365 product.
<input type="checkbox"/>	 Exchange administrator	Can manage all aspects of the Exchange product.
<input type="checkbox"/>	 External ID user flow administrator	Can create and manage all aspects of user flows.
<input type="checkbox"/>	 External ID user flow attribute administrator	Can create and manage the attribute schema available to all user flows.
<input type="checkbox"/>	 External Identity Provider administrator	Can configure identity providers for use in direct federation.
<input checked="" type="checkbox"/>	 Global administrator	Can manage all aspects of Azure AD and Microsoft services that use Azure AD identities.
<input type="checkbox"/>	 Global reader	Can read everything that a global administrator can, but not update anything.
<input type="checkbox"/>	 Groups administrator	Can manage all aspects of groups and group settings like naming and expiration policies.
<input type="checkbox"/>	 Guest inviter	Can invite guest users independent of the 'members can invite guests' setting.
<input type="checkbox"/>	 Helpdesk administrator	Can reset passwords for non-administrators and Helpdesk administrators.
<input type="checkbox"/>	 Hybrid identity administrator 	Can enable, deploy, configure, manage, monitor, and troubleshoot cloud provisioning and authentication services.
<input type="checkbox"/>	 Insights administrator 	Has administrative access in the Insights app.
<input type="checkbox"/>	 Insights business leader 	Can view and share dashboards and insights via the M365 Insights app.
<input type="checkbox"/>	 Intune administrator	Can manage all aspects of the Intune product.
<input type="checkbox"/>	 Kaizala administrator	Can manage settings for Microsoft Kaizala.
<input type="checkbox"/>	 License administrator	Ability to assign, remove and update license assignments.

# AAD Role Permissions

## Summary

**Name:** Helpdesk administrator

**Description:** Users with this role can change passwords, invalidate refresh tokens, manage service requests, and monitor service health. Invalidating a refresh token forces the user to sign in again. Helpdesk administrators can reset passwords and invalidate refresh tokens of other users who are non-administrators or assigned the following roles only:

- Directory Readers
- Guest Inviter
- Helpdesk Administrator
- Message Center Reader
- Password Administrator
- Reports Reader

**Template ID:** 729827e3-9c14-49f7-bb1b-9608f156bbb8

- Permissions have a namespace, an object in the namespace, sometimes properties, and an action.
- More information:  
<https://docs.microsoft.com/en-us/azure/active-directory/users-groups-roles/directory-assign-admin-roles>

## Role permissions

microsoft.directory/users/invalidateAllRefreshTokens	Invalidate all user refresh tokens in Azure Active Directory.
microsoft.directory/users/bitLockerRecoveryKeys/read	
microsoft.directory/users/password/update	Update passwords for all users in Azure Active Directory. See online documentation for more detail.
microsoft.azure.serviceHealth/allEntities/allTasks	Read and configure Azure Service Health.
microsoft.azure.supportTickets/allEntities/allTasks	Create and manage Azure support tickets for directory-level services.
microsoft.office365.webPortal/allEntities/standard/read	Read basic properties on all resources in microsoft.office365.webPortal.
microsoft.office365.serviceHealth/allEntities/allTasks	Read and configure Office 365 Service Health.
microsoft.office365.supportTickets/allEntities/allTasks	Create and manage Office 365 support tickets.

This role also grants the following [basic read permissions](#) to guests and service principals

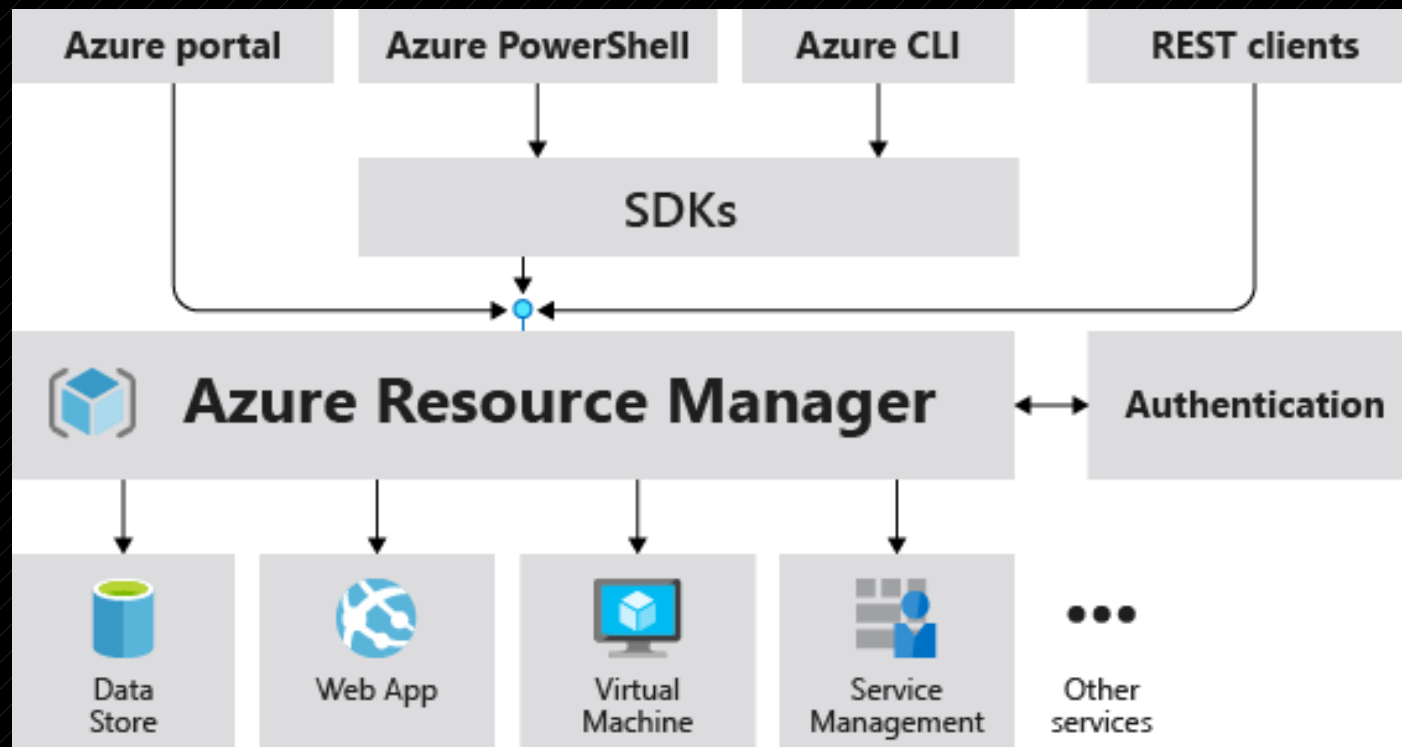
microsoft.directory/administrativeUnits/standard/read	Read basic properties on administrativeUnits in Azure Active Directory.
microsoft.directory/administrativeUnits/members/read	Read administrativeUnits.members property in Azure Active Directory.
microsoft.directory/applications/standard/read	Read standard properties of applications.
microsoft.directory/applications/owners/read	Read owners on all types of applications.
microsoft.directory/applications/policies/read	Read applications.policies property in Azure Active Directory.
microsoft.directory/contacts/standard/read	Read basic properties on contacts in Azure Active Directory.
microsoft.directory/contacts/memberOf/read	Read contacts.memberOf property in Azure Active Directory.
microsoft.directory/contracts/standard/read	Read basic properties on contracts in Azure Active Directory.
microsoft.directory/devices/standard/read	Read basic properties on devices in Azure Active Directory.

# Azure Resource Manager

The image features a solid blue background. In the bottom right corner, there are several overlapping geometric shapes: a dark grey triangle pointing towards the top right, a medium blue trapezoidal shape below it, and a dark blue trapezoidal shape at the bottom, all creating a layered, architectural effect.

# Azure Resource Manager

- Deployment and management service for Azure resources.
- Replaced Azure Service Manager (ASM) which is now known as “Classic”.



# ARM Terminology

## Tenant

- Represents an organization

## Subscription

- Logical collection of Resource Groups
- Usually separated for billing purposes

## Resource Group

- Logical collection of resources

## Resource

- Any manageable item in Azure. (i.e., Virtual Machines, Web Apps, Storage, Key Vaults)
- **Subscriptions and Resource Groups are also considered Resources.**

## Resource Provider

- A service that provides a type of resource. (i.e. Microsoft.Storage for a storage account).

## Role-Based Access Control (RBAC)

- Specifies a set of permissions a user may take on a specific resource. The resource is defined in a scope parameter.
- **Not the same as AAD Roles.**

# Resource Providers

Microsoft.Attestation	Azure Attestation Service
Microsoft.Authorization <sup>1</sup>	Azure Resource Manager
Microsoft.Automation	Automation
Microsoft.AutonomousSystems	Autonomous Systems
Microsoft.AVS	Azure VMware Solution
Microsoft.AzureActiveDirectory	Azure Active Directory B2C
Microsoft.AzureData	SQL Server registry
Microsoft.AzureStack	core
Microsoft.AzureStackHCI	Azure Stack HCI
Microsoft.Batch	Batch
Microsoft.Billing <sup>1</sup>	Cost Management and Billing
Microsoft.BingMaps	Bing Maps
Microsoft.Blockchain	Azure Blockchain Service
Microsoft.BlockchainTokens	Azure Blockchain Tokens
Microsoft.Blueprint	Azure Blueprints
Microsoft.BotService	Azure Bot Service
Microsoft.Cache	Azure Cache for Redis
Microsoft.Capacity	core
Microsoft.Cdn	Content Delivery Network
Microsoft.CertificateRegistration	App Service Certificates
Microsoft.ChangeAnalysis	Azure Monitor
Microsoft.ClassicCompute	Classic deployment model virtual machine
Microsoft.ClassicInfrastructureMigrate	Classic deployment model migration
Microsoft.ClassicNetwork	Classic deployment model virtual network
Microsoft.ClassicStorage	Classic deployment model storage

Microsoft.Services	core
Microsoft.SignalRService	Azure SignalR Service
Microsoft.SoftwarePlan	License
Microsoft.Solutions	Azure Managed Applications
Microsoft.Sql	Azure SQL Database Azure SQL Managed Instance Azure Synapse Analytics
Microsoft.SqlVirtualMachine	SQL Server on Azure Virtual Machines
Microsoft.Storage	Storage
Microsoft.StorageCache	Azure HPC Cache
Microsoft.StorageSync	Storage
Microsoft.StorSimple	StorSimple
Microsoft.StreamAnalytics	Azure Stream Analytics
Microsoft.Subscription	core
microsoft.support <sup>1</sup>	core
Microsoft.Synapse	Azure Synapse Analytics
Microsoft.TimeSeriesInsights	Azure Time Series Insights
Microsoft.Token	Token
Microsoft.VirtualMachinesImages	Azure Image Builder
microsoft.visualstudio	Azure DevOps
Microsoft.VMware	Azure VMware Solution
Microsoft.VMwareCloudSimple	Azure VMware Solution by CloudSimple
Microsoft.VSOnline	Azure DevOps
Microsoft.Web	App Service Azure Functions
Microsoft.WindowsDefenderATP	Microsoft Defender Advanced Threat Protection



# Control Plane vs Data Plane

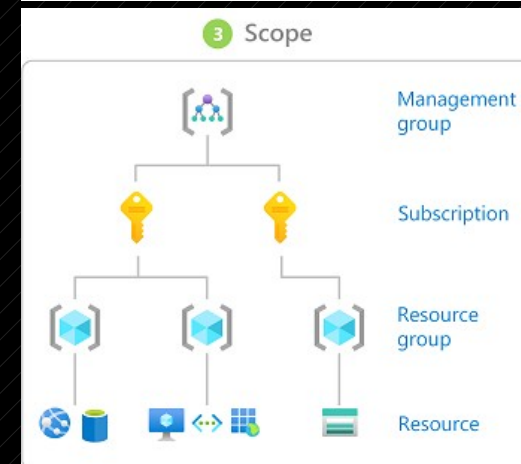
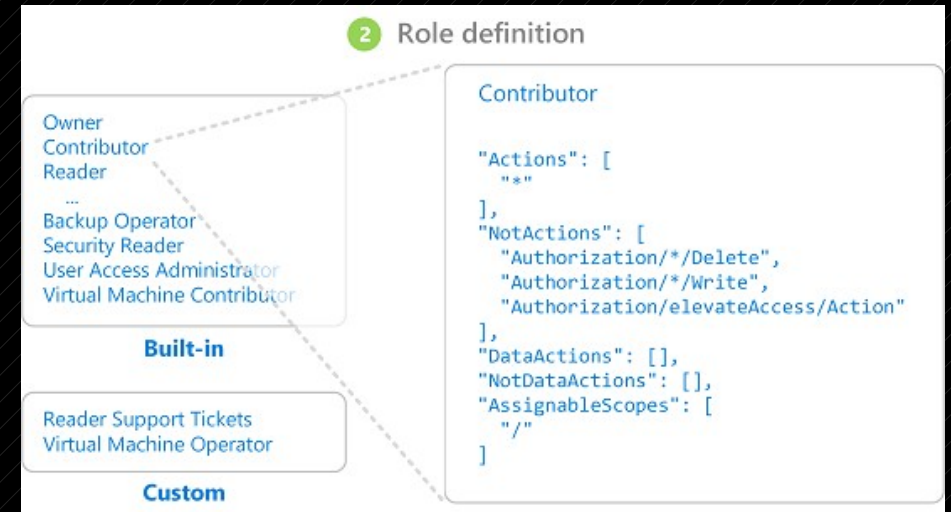
- Operations are divided into two categories: Control (aka Management) and Data.
- The control plane is for managing the resource with ARM. Requests for the control plane are sent to the relevant resource provider.
- The data plane is for managing the operations of the resource within the resource.

Control Plane	Data Plane
Create/Delete a virtual machine	RDP to the virtual machine
Create/Delete a storage account	Read/write data to the storage account
Create/Delete a database	Query the database

**THIS IS AN IMPORTANT CONCEPT FOR RBAC!**

# ARM Role-Based Access Control

- Authorization system built on ARM that provides access management of Azure resources.
- An RBAC role assignment is based on three parts:
  - **Security principal** – An AAD object such as User, Group, Service Principal, Managed Identity.
  - **Role definition** – Collection of permissions.
  - **Scope** - Set of resources that the access applies to.



# General RBAC roles

Built-in role	Description
<b>General</b>	
Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC.
Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.
Reader	View all resources, but does not allow you to make any changes.

# Specific RBAC roles

Storage File Data SMB Share Contributor	Allows for read, write, and delete access on files/directories in Azure file shares. This role has no built-in equivalent on Windows file servers.
Storage File Data SMB Share Elevated Contributor	Allows for read, write, delete, and modify ACLs on files/directories in Azure file shares. This role is equivalent to a file share ACL of change on Windows file servers.
Storage File Data SMB Share Reader	Allows for read access on files/directories in Azure file shares. This role is equivalent to a file share ACL of read on Windows file servers.
Storage Queue Data Contributor	Read, write, and delete Azure Storage queues and queue messages. To learn which actions are required for a given data operation, see <a href="#">Permissions for calling blob and queue data operations</a> .
Storage Queue Data Message Processor	Peek, retrieve, and delete a message from an Azure Storage queue. To learn which actions are required for a given data operation, see <a href="#">Permissions for calling blob and queue data operations</a> .

# Role Definitions

- Role Definitions can affect both Management and Data planes.
- **Management** – actions/not actions  
**Data** – data actions/not data actions
- **Management access is not inherited to your data!**
  - The permissions to read the containers in a Storage account **does not** give you the permission to read the blobs in the containers in the account.

JSON

```
{
  "assignableScopes": [
    "/"
  ],
  "description": "Allows for read access to Azure Storage blob containers and data",
  "id": "/subscriptions/{subscriptionId}/providers/Microsoft.Authorization/roleDefinitions/",
  "name": "2a2b9908-6ea1-4ae2-8e65-a410df84e7d1",
  "permissions": [
    {
      "actions": [
        "Microsoft.Storage/storageAccounts/blobServices/containers/read",
        "Microsoft.Storage/storageAccounts/blobServices/generateUserDelegationKey/action"
      ],
      "notActions": [],
      "dataActions": [
        "Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read"
      ],
      "notDataActions": []
    }
  ],
  "roleName": "Storage Blob Data Reader",
  "roleType": "BuiltInRole",
  "type": "Microsoft.Authorization/roleDefinitions"
}
```

# Actions/Permissions/Operations

Get Blob Metadata	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read
Set Blob Metadata	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write
Lease Blob	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write
Snapshot Blob	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write or Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action
Copy Blob	For destination blob: Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write or Microsoft.Storage/storageAccounts/blobServices/containers/blobs/add/action (when writing a new blob to the destination) For source blob in the same storage account: Microsoft.Storage/storageAccounts/blobServices/containers/blobs/read For source blob in a different storage account: Available as anonymous, or include valid SAS token
Abort Copy Blob	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/write
Delete Blob	Microsoft.Storage/storageAccounts/blobServices/containers/blobs/delete

# Actions/Permissions/Operations

## Storage Queue Data Reader

Read and list Azure Storage queues and queue messages. To learn which actions are required for a given data operation, see [Permissions for calling blob and queue data operations](#).

- Sometimes names of roles can be misleading.

## DataActions

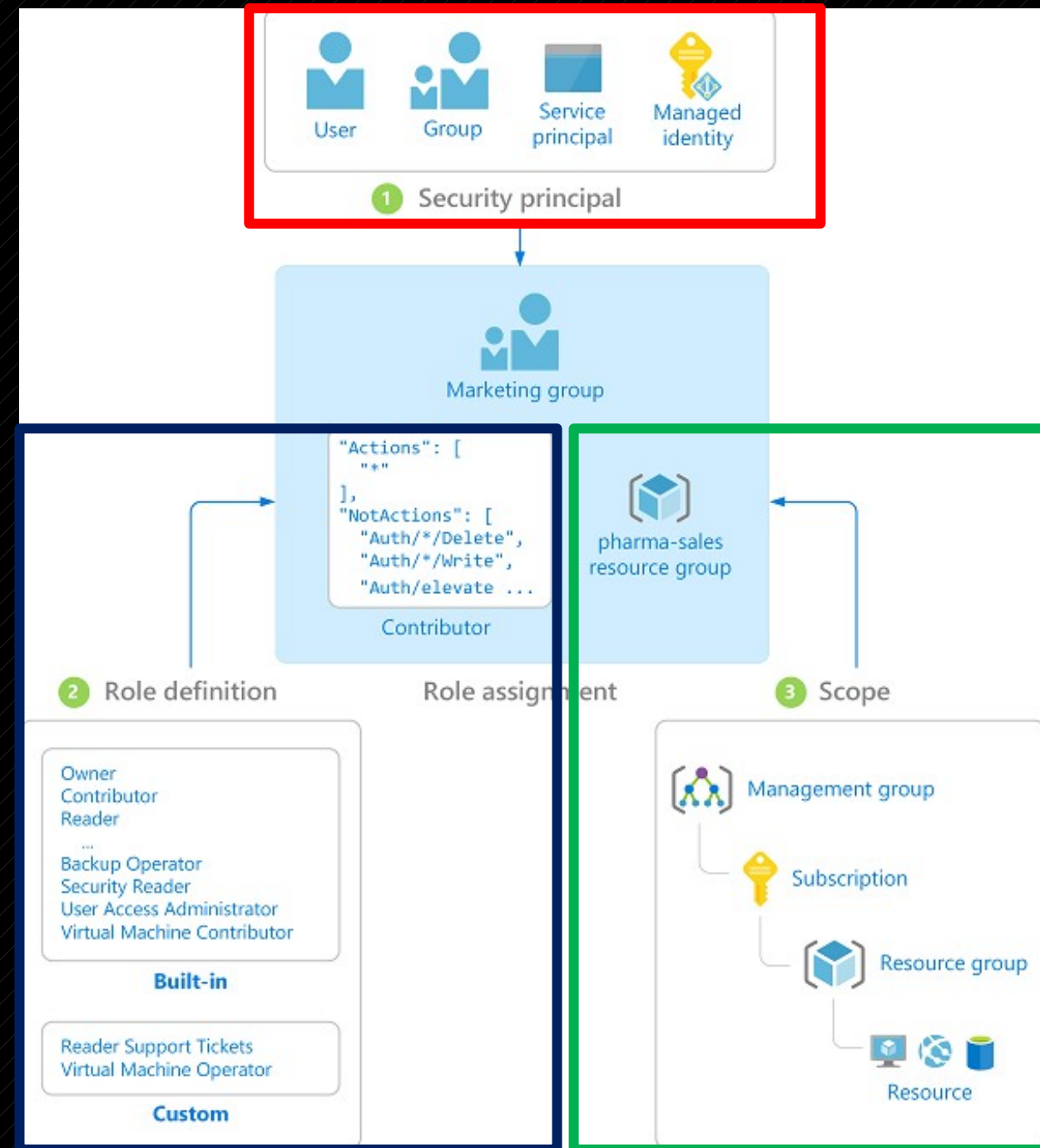
`Microsoft.Storage/storageAccounts/queueServices/queues/messages/read` Peek or retrieve one or more messages from a queue.

`Get Messages` `Microsoft.Storage/storageAccounts/queueServices/queues/messages/process/action` or `(Microsoft.Storage/storageAccounts/queueServices/queues/messages/delete and Microsoft.Storage/storageAccounts/queueServices/queues/messages/read)`

```
"permissions": [
  {
    "actions": [
      "Microsoft.Storage/storageAccounts/queueServices/queues/read"
    ],
    "notActions": [],
    "dataActions": [
      "Microsoft.Storage/storageAccounts/queueServices/queues/messages/read"
    ],
    "notDataActions": []
  }
],
"roleName": "Storage Queue Data Reader",
```

```
"permissions": [
  {
    "actions": [],
    "notActions": [],
    "dataActions": [
      "Microsoft.Storage/storageAccounts/queueServices/queues/messages/read",
      "Microsoft.Storage/storageAccounts/queueServices/queues/messages/process/action"
    ],
    "notDataActions": []
  }
],
"roleName": "Storage Queue Data Message Processor",
```

1. AAD Objects are a part of the **Marketing Group**.
2. The **Marketing Group** is assigned **Contributor** access with a scope for the **pharma-sales resource group**.
3. The **Marketing Group** has full access to all resources in the **pharma-sales resource group** but cannot assign RBAC roles to others.



# Interacting with AAD and ARM

The background is a solid blue color. In the bottom right corner, there are several overlapping geometric shapes. A dark grey triangle points towards the top right. Below it, a blue trapezoidal shape is partially visible. At the bottom, a dark grey trapezoidal shape is also present, creating a layered, architectural effect.



# Azure Portal

Azure Public  
[portal.azure.com](https://portal.azure.com)

US Government  
[portal.azure.us](https://portal.azure.us)

Germany  
[portal.microsoftazure.de](https://portal.microsoftazure.de)

China  
[portal.azure.cn](https://portal.azure.cn)

The screenshot displays the Microsoft Azure Portal interface. At the top, there is a navigation bar with the text "Microsoft Azure (Preview)" and a search bar containing "Search resources, services, and docs (G+/)". Below the navigation bar, the main content area is divided into several sections:

- Azure services:** This section contains a grid of service tiles. The first row includes "Create a resource" (with a plus icon), "Subscriptions" (with a key icon), "Azure Active Directory" (with a blue diamond icon), "Virtual machines" (with a monitor icon), "App Services" (with a blue globe icon), "Storage accounts" (with a green and white striped icon), and "SQL databases" (with a blue cylinder icon). The second row includes "Azure Database for PostgreSQL..." (with a blue cylinder icon), "Azure Cosmos DB" (with a blue planet icon), and "More services" (with a blue arrow icon).
- Navigate:** This section contains three tiles: "Subscriptions" (with a yellow key icon), "Resource groups" (with a blue cube icon), and "All resources" (with a green grid icon).
- Dashboard:** This section contains one tile: "Dashboard" (with a green bar chart icon).
- Tools:** This section contains three tiles: "Microsoft Learn" (with a blue book icon and a link icon), "Azure Monitor" (with a blue clock icon), and "Security Center" (with a green shield icon).

# Azure CLI

- Written in Python.
- Login with **az login** command
- Access tokens saved in `~/.azure/accessTokens.json`.

```
az>> keyvault list
[
  {
    "id": "/subscriptions/4719d83b-2b61-4ed8-8d46-39b6109a1496/resourceGroups,
    "location": "eastus",
    "name": "lotsOcreds",
    "resourceGroup": "glo",
    "tags": {},
    "type": "Microsoft.KeyVault/vaults"
  },
  {
    "id": "/subscriptions/4719d83b-2b61-4ed8-8d46-39b6109a1496/resourceGroups,
    "location": "northcentralus",
    "name": "SSITKeyVault",
    "resourceGroup": "IT-Dept-rg",
    "tags": {},
    "type": "Microsoft.KeyVault/vaults"
  },
  {
    "id": "/subscriptions/4719d83b-2b61-4ed8-8d46-39b6109a1496/resourceGroups,
    "location": "centralus",
    "name": "ssmanagementkv",
    "resourceGroup": "SSManagement-rg",
    "tags": {},
    "type": "Microsoft.KeyVault/vaults"
  }
]
```

```
az>> ad user show --id kelly.santana@stormspotter.onmicrosoft.com
{
  "accountEnabled": false,
  "ageGroup": null,
  "assignedLicenses": [],
  "assignedPlans": [],
  "city": "Crystalfort",
  "companyName": null,
  "consentProvidedForMinor": null,
  "country": "US",
  "createdDateTime": "2020-06-08T19:21:19Z",
  "creationType": null,
  "deletionTimestamp": null,
  "department": null,
  "dirSyncEnabled": null,
  "displayName": "Kelly Santana",
  "employeeId": null,
  "facsimileTelephoneNumber": null,
  "givenName": "Kelly",
  "immutableId": null,
  "isCompromised": null,
  "jobTitle": null,
  "lastDirSyncTime": null,
  "legalAgeGroupClassification": null,
  "mail": null,
  "mailNickname": "Kelly.Santana",
  "mobile": "143-456-3465",
  "objectId": "d880ee73-a1fa-4055-bbc3-2ae3bf200d59",
  "objectType": "User",
  "odata.metadata": "https://graph.windows.net/087a8387-325b-444f-aa20-4258f6d6828c/",
  "odata.type": "Microsoft.DirectoryServices.User",
  "onPremisesDistinguishedName": null,
  "onPremisesSecurityIdentifier": null,
  "otherMails": [],
  "passwordPolicies": null,
  "passwordProfile": {
    "enforceChangePasswordPolicy": false,
    "forceChangePasswordNextLogin": true,
    "password": null
  }
},
```

# PowerShell

## Az PowerShell

Newest version for interacting with Azure.

- Cannot coexist with AzureRM module.
- Login with `Connect-AzAccount`.

## AzureRM

Older version for interacting with Azure.

- Cannot coexist with Az PowerShell.
- Login with `Connect-AzureRmAccount`

## AzureAD

Interacts with Azure Active Directory

- Current versions interact with Microsoft Graph.
- Works in PowerShell Core.

## MSOnline

Deprecated in favor of AzureAD

- Does not work in PowerShell Core.

## Azure PowerShell

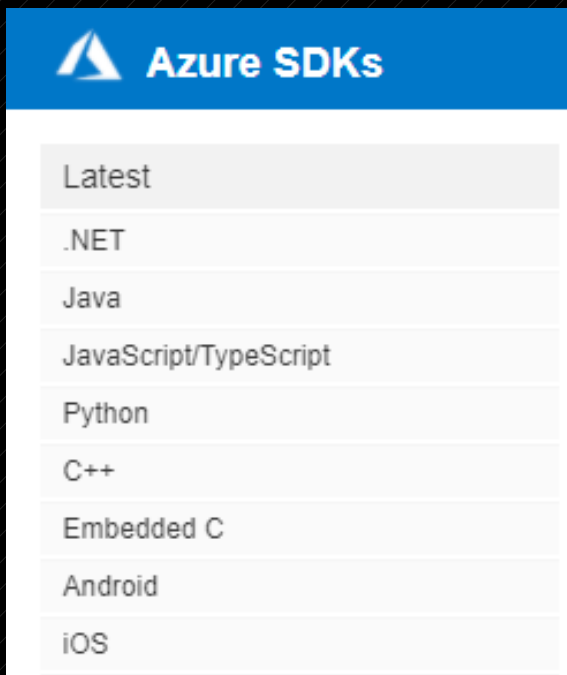
Used for classic resources

- Some organizations still have classic resources or use classic management certificates

# Azure SDKs

<https://azure.github.io/azure-sdk/>

- SDKs come in a variety of languages.
- Generally broken up into management libraries and client (data plane) libraries.
- There's been a lot of refactoring so make sure you test before implementing updated libraries.



A screenshot of the Python SDKs page on the Azure SDKs website. The page title is "Python". There are three tabs: "Client Libraries", "Management Libraries", and "All". Below the tabs is a table with columns: Display Name, Package, MS Docs, GH Docs, Source, and Notes. The table lists several SDKs with their respective package names and versions.

Display Name	Package	MS Docs	GH Docs	Source	Notes
App Configuration	<a href="#">pypi</a> <a href="#">1.1.1</a>	<a href="#">msdocs</a> <a href="#">1.1.1</a>	<a href="#">ghdocs</a> <a href="#">1.1.1</a>	<a href="#">github</a> <a href="#">1.1.1</a>	
azure-ai-metricsadvisor	<a href="#">pypi</a> <a href="#">1.0.0b1</a>	<a href="#">msdocs</a> <a href="#">1.0.0b1</a>	<a href="#">ghdocs</a> <a href="#">1.0.0b1</a>	<a href="#">github</a> <a href="#">1.0.0b1</a>	
Cognitive Search	<a href="#">pypi</a> <a href="#">11.0.0</a> <a href="#">pypi</a> <a href="#">11.1.0b3</a>	<a href="#">msdocs</a> <a href="#">11.0.0</a>	<a href="#">ghdocs</a> <a href="#">11.0.0</a> <a href="#">ghdocs</a> <a href="#">11.1.0b3</a>	<a href="#">github</a> <a href="#">11.0.0</a> <a href="#">github</a> <a href="#">11.1.0b3</a>	Replaces: azure-search
Communication Administration	<a href="#">pypi</a> <a href="#">1.0.0b2</a>	<a href="#">msdocs</a> <a href="#">1.0.0b2</a>	<a href="#">ghdocs</a> <a href="#">1.0.0b2</a>	<a href="#">github</a> <a href="#">1.0.0b2</a>	
Communication Chat	<a href="#">pypi</a> <a href="#">1.0.0b2</a>	<a href="#">msdocs</a> <a href="#">1.0.0b2</a>	<a href="#">ghdocs</a> <a href="#">1.0.0b2</a>	<a href="#">github</a> <a href="#">1.0.0b2</a>	
Communication Sms	<a href="#">pypi</a> <a href="#">1.0.0b3</a>	<a href="#">msdocs</a> <a href="#">1.0.0b3</a>	<a href="#">ghdocs</a> <a href="#">1.0.0b3</a>	<a href="#">github</a> <a href="#">1.0.0b3</a>	

# Azure REST APIs

- There's a lot of APIs.
- Read the docs, fam.
  - <https://docs.microsoft.com/en-us/rest/api/azure/>

## Examples

### GetSecrets

#### Sample Request

HTTP

Copy

```
GET https://myvault.vault.azure.net//secrets?maxresults=1&api-version=7.1
```

#### Sample Response

Status code: 200

JSON

Copy

```
{
  "value": [
    {
      "contentType": "plainText",
      "id": "https://myvault.vault.azure.net/secrets/listsecrettest0",
      "attributes": {
        "enabled": true,
        "created": 1482189047,
        "updated": 1482189047
      }
    }
  ],
  "nextLink": "https://myvault.vault.azure.net:443/secrets?api-version=7.1&$skiptoken=eyJ0ZXh0TWYya2VyIjoimE40CFNREF3TU"
}
```

Stormspotter



# What is Stormspotter?

- Stormspotter creates an “attack graph” of Azure AD and Azure Resource Manager.
  - Neo4j
  - Python
  - VueJS frontend
- It enables red teams and pentesters to visualize the attack surface and pivot opportunities within a tenant.
- Can also be used by defenders to audit themselves.
- **Not an official Microsoft product. Just a tool by a red team. Still in beta. 😊**



STORMSPOTTER

<https://github.com/Azure/Stormspotter>

## Why does it exist?

- Understanding how a configuration can affect resources is crucial to the security of an environment.
- Relationships are easier to understand when they can be visualized.
- Tools like **Bloodhound** for displaying relationships in Active Directory have proven that graphs work for security.
  - <https://bloodhound.readthedocs.io/en/latest/>
  - <https://github.com/BloodHoundAD/BloodHound>



# Would you rather...

## Command Line Output

```
az>> ad sp owner list --id 9d03d772-4645-4a32-8057-b876748f84a5 --output jsonc
```

```
[  
  {  
    "accountEnabled": false,  
    "ageGroup": null,  
    "assignedLicenses": [],  
    "assignedPlans": [],  
    "city": "Crystalfort",  
    "companyName": null,  
    "consentProvidedForMinor": null,  
    "country": "US",  
    "createdDateTime": "2020-06-08T19:21:19Z",  
    "creationType": null,  
    "deletionTimestamp": null,  
    "department": null,  
    "dirSyncEnabled": null,  
    "displayName": "Kelly Santana",  
    "employeeId": null,  
    "facsimileTelephoneNumber": null,  
    "givenName": "Kelly",  
    "immutableId": null,  
    "isCompromised": null,  
    "jobTitle": null,  
    "lastDirSyncTime": null,  
    "legalAgeGroupClassification": null,  
    "mail": null,  
    "mailNickname": "Kelly.Santana",  
    "mobile": "143-456-3465",  
    "objectId": "d880ee73-a1fa-4055-bbc3-2ae3bf200d59",  
    "objectType": "User",  
    "odata.type": "Microsoft.DirectoryServices.User",  
  }  
]
```

## Stormspotter



# Requirements for Using Stormspotter

- AAD
  - Must have read access to either Azure AD (legacy) or Microsoft Graph
  - Azure AD - <https://graph.windows.net> (Primary attempt)
  - MS Graph – <https://graph.microsoft.com> (Backup)
- ARM
  - Must have reader access at least at a subscription level
  - Enumeration of resources occurs the subscription level
- Currently only Azure CLI and Service Principal logins supported

# DEMO

- Found creds for a user named Kelly Santana.
- Kelly access to read AAD and some Azure resources.
- Can we find a path for lateral movement using Stormspotter?

# Things to Consider

- AAD and ARM permissions can be complex.
- Regularly audit permissions to check for changes.
- Follow the Least Privilege rules.
  - You don't need access to an entire subscription or resource group to access a resource as a user.
  - Users who manage resources should only be given access to the resources they need.

Questions?

**Leron Gray**

**Social Media - @mcohmi**

**Email - [daddycooaman@gmail.com](mailto:daddycooaman@gmail.com)**

**LinkedIn - <https://www.linkedin.com/in/leron-gray>**

**- Put "GrayHat RTV" when adding**