



Defining the Undefined: **What is Tier Zero? – Part 3**

Thomas Naunheim, Andy Robbins, Jonas B. Knudsen

Agenda

- Recap
- Today's scope: Entra ID
- Enterprise Access Model
- Default Tier Zero Nodes in BloodHound
- EntraOps
- Entra ID Roles

Who are we?

Thomas Naunheim

*Cyber Security Architect
(glueckkanja)*



Andy Robbins

*Principal Product Architect
(SpecterOps)*



Jonas Bülow Knudsen

*Product Architect
(SpecterOps)*



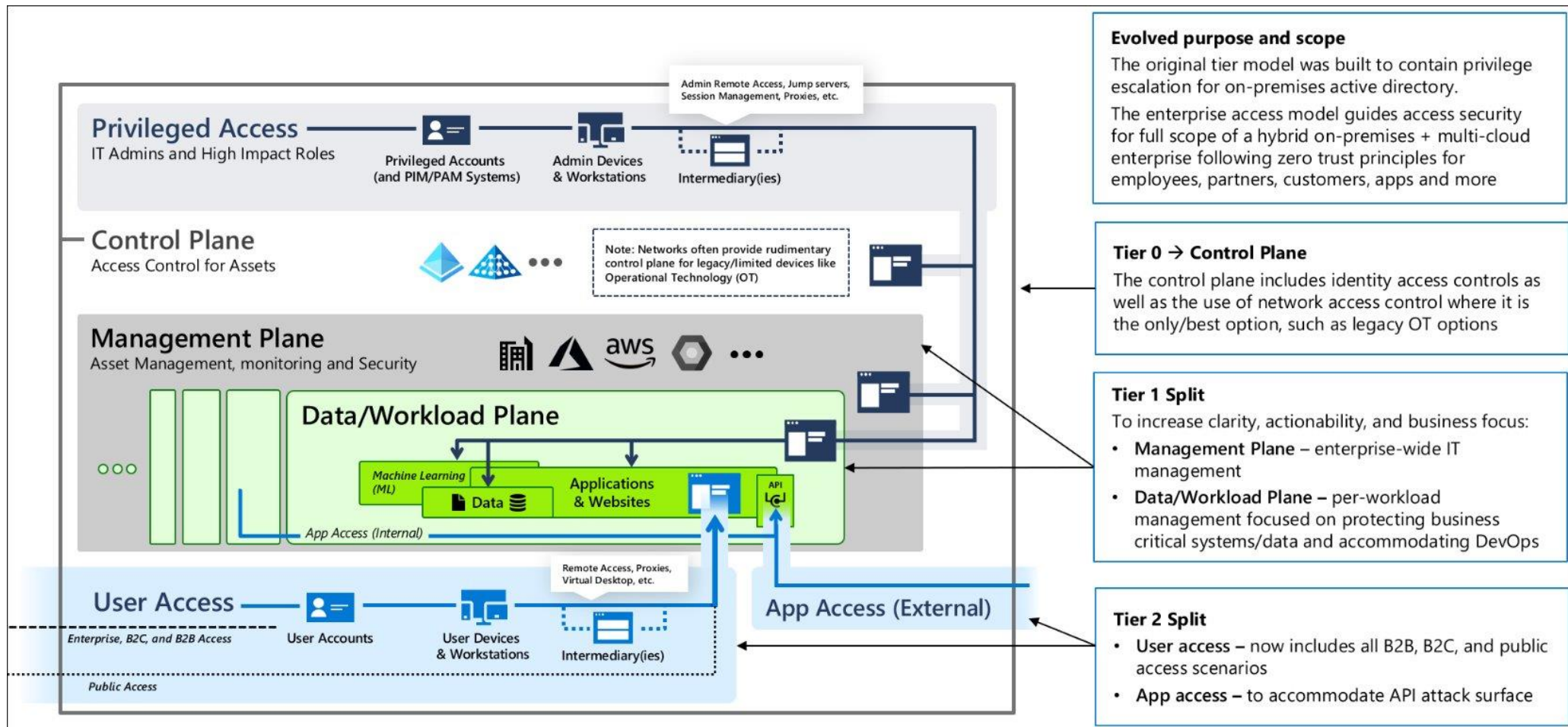
Recap

Recap – Part 1 & 2

- History of Tier Zero
- Purpose of the *What is Tier Zero* series
- Our definition of Tier Zero:
Tier Zero is a set of assets in control of enterprise identities and their security dependencies
 - *Control: A relationship that can contribute to compromising the controlled asset or impact its operability*
 - *Security dependency: A component whose security impacts another component's security*
- Microsoft's original list of Tier Zero AD groups
- More on-prem AD objects

Today's scope: Entra ID

Enterprise Access Model



Default Tier Zero Nodes in BloodHound

Default Tier Zero Nodes in BloodHound

- The Entra ID tenant object
- The following Entra ID admin roles:
 - Global Administrator
 - Privileged Role Administrator
 - Privileged Authentication Administrator
 - Partner Tier2 Support
 - Any principal assigned one of the above roles

Default Tier Zero Nodes in BloodHound

- Any service principal with one of the following MS Graph application role assignments:
 - RoleManagement.ReadWrite.Directory
 - AppRoleAssignment.ReadWrite.All

EntraOps

Classification for Entra ID Privileged Roles

Classification of Action and Scope

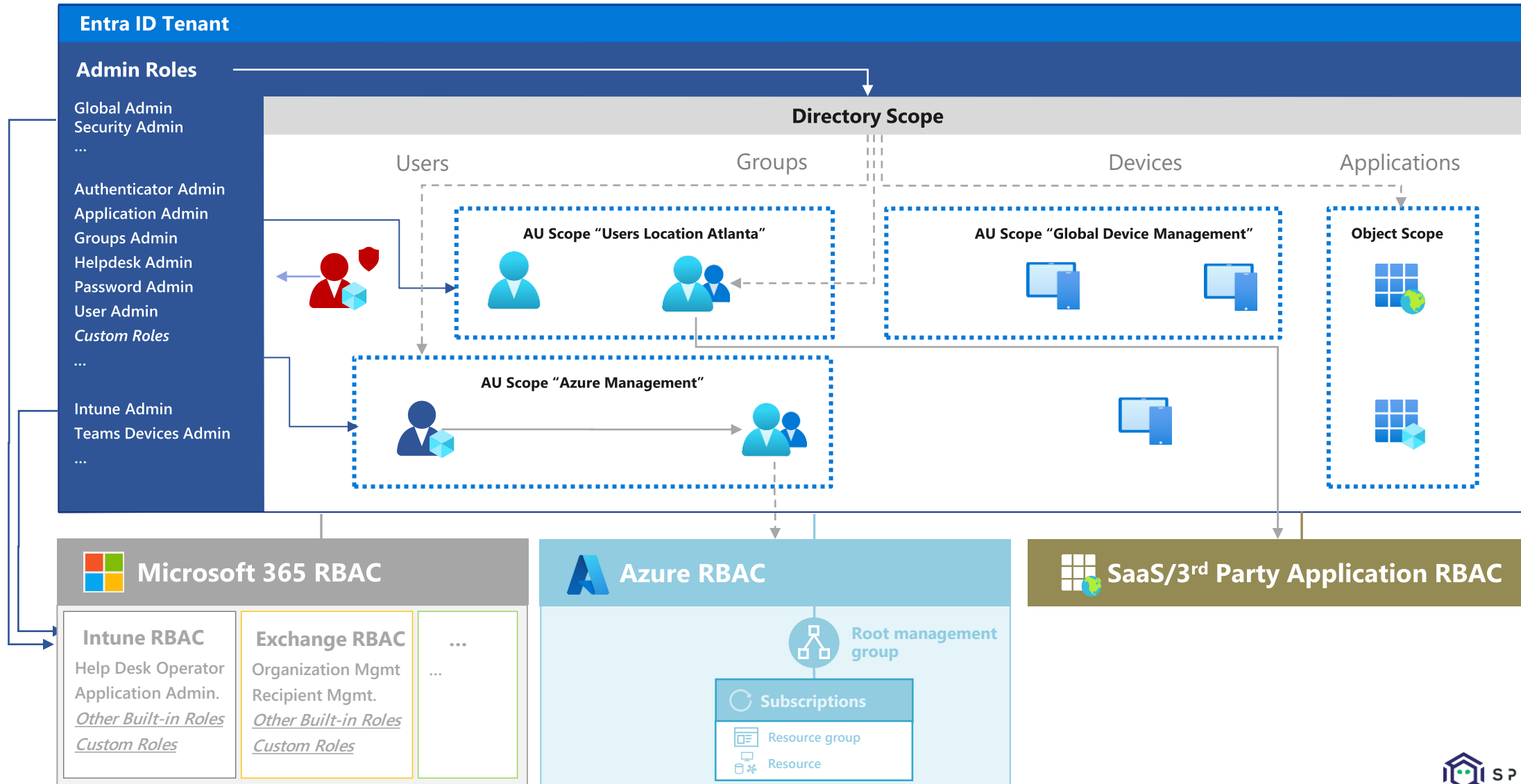
```
"EAMTierLevelName": "ControlPlane",
"TierLevelDefinition": [
  {
    "Category": "Microsoft.AzureAD",
    "Service": "User Management",

    "RoleAssignmentScopeName": [
      "/administrativeUnits/3f225776-fb03-4f3c",
      "/",
    ],
    "RoleDefinitionActions": [
      "microsoft.directory/users/password/update"
      ...
    ]
  }
]
```

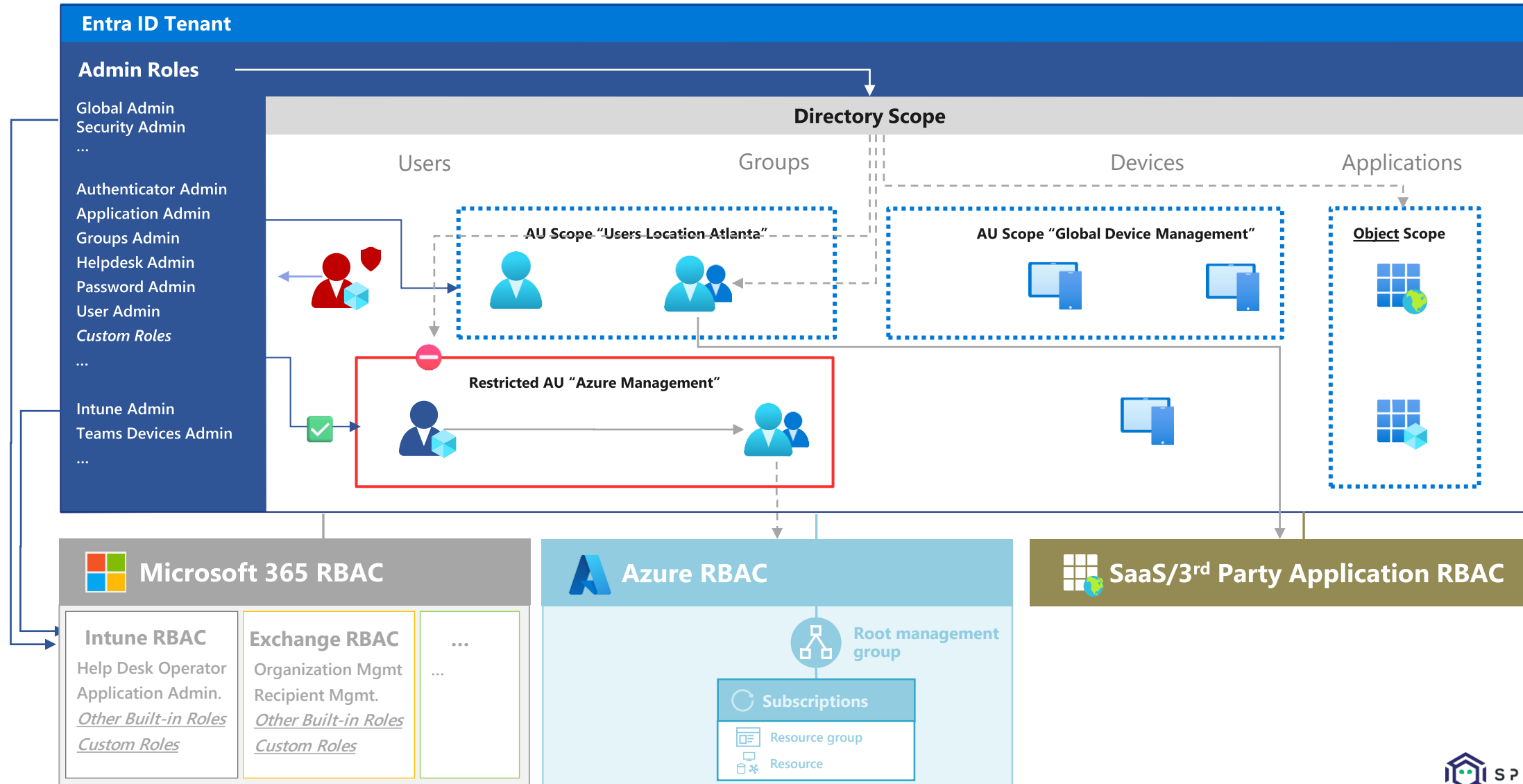
Classification of Privileged Principal

```
"ObjectAdminTierLevelName": "ControlPlane",
"ObjectDisplayName": "admThom0",
"Classification": [
  {
    "AdminTierLevelName": "ControlPlane",
    "Service": "User Management"
  }
]
"RoleAssignments": [
  {
    "RoleAssignmentScopeName": "/",
    "RoleAssignmentType": "Transitive",
    "TransitiveByObject": "prg_Tier0.IdentityOps",
    "RoleDefinitionName": "Helpdesk Administrator",
    "PIMAssignmentType": "Eligible"
  }
]
```

Delegation and scoping of Entra ID roles



Delegation and scoping of Entra ID roles



Group types for privileged assignments

	Preferred use case/scenario	Restricted group object	Restriction applies to <u>user</u> members
Security Groups (without PIM)	Non-high privileged assignments	✗ No restriction	✗ No restriction
Security Group with PIM for Groups	Just-In-Time Access outside of Azure and Entra ID RBAC	✗ No restriction	✗ No restriction
Security Groups in Restricted AU	Assignment to sensitive policies or none-PIM groups	✓ RMAU-scoped Admins	✗ No restriction,
Role-Assignable Security Groups	Assigning Entra ID roles (or other high-privileges)	✓ GA, Privileged Role Admin, Owners, <i>RoleManagement.-ReadWrite.Directory</i>	⚠ Restricted to GA and Privileged Auth. Admin when active/permanent member

Demo:

EntraOps Classification and Use Cases

Entra ID Roles

Entra ID Roles

Is Not Tier Zero



It Depends



Is Tier Zero



Security Administrator

Is Not Tier Zero



It Depends



Is Tier Zero



Security
Administrator

Knowledge Administrator

Is Not Tier Zero



It Depends



Is Tier Zero



Knowledge Administrator

Intune Administrator

Is Not Tier Zero



It Depends



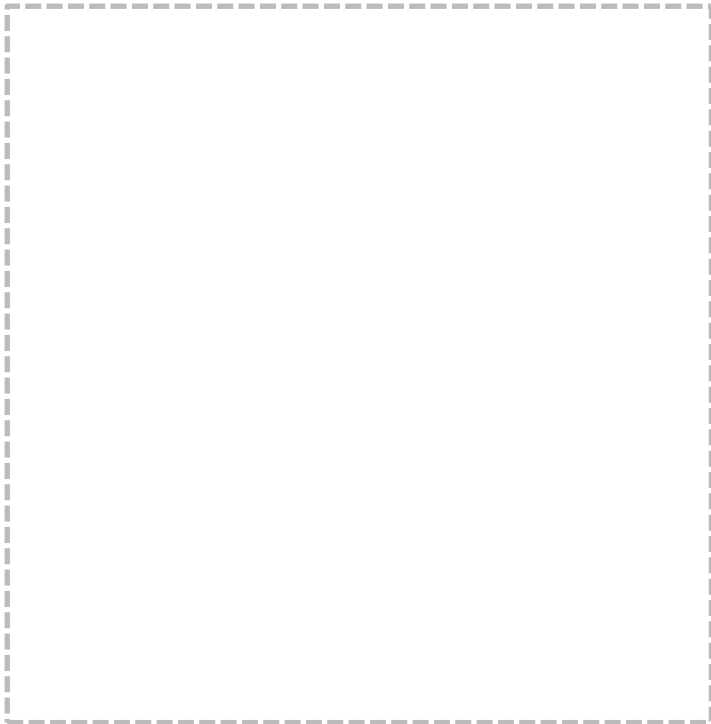
Is Tier Zero



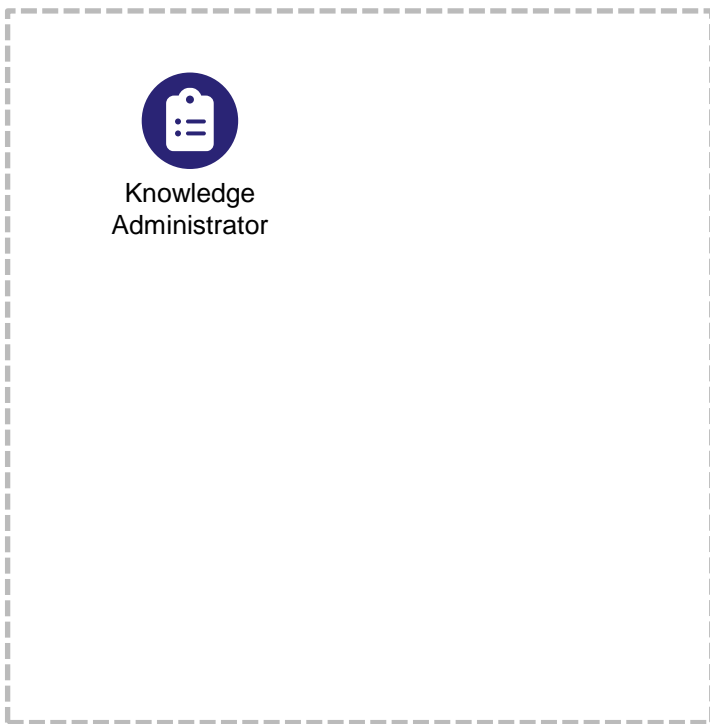
Intune
Administrator

Application Administrator

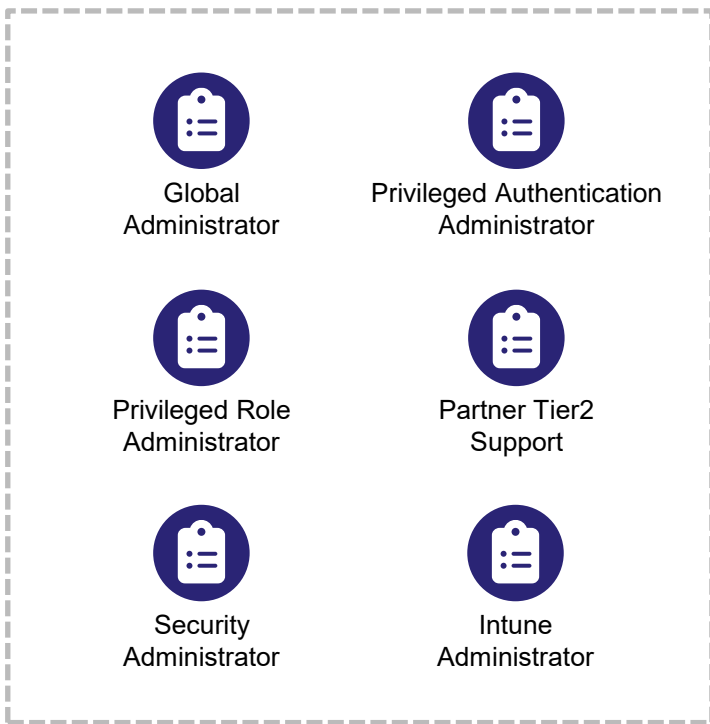
Is Not Tier Zero



It Depends



Is Tier Zero



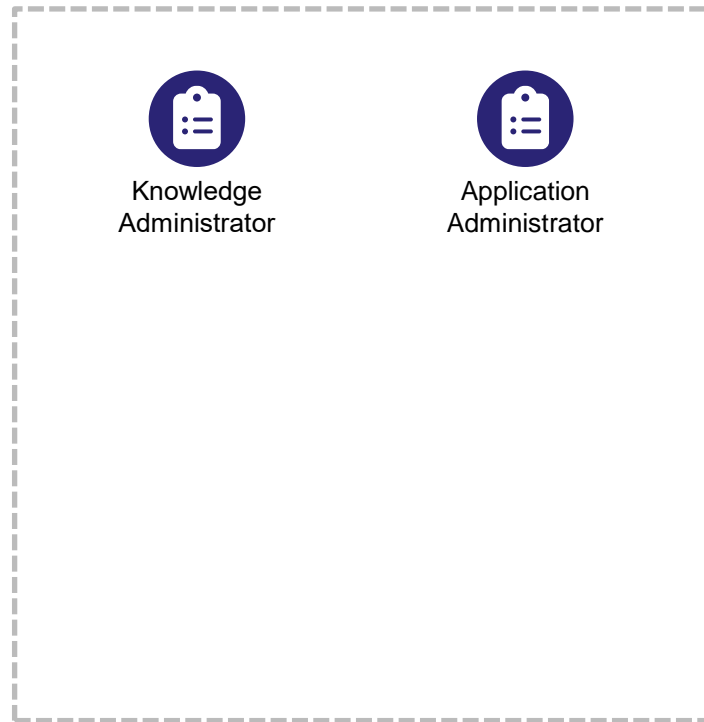
Application Administrator

Application Administrator

Is Not Tier Zero



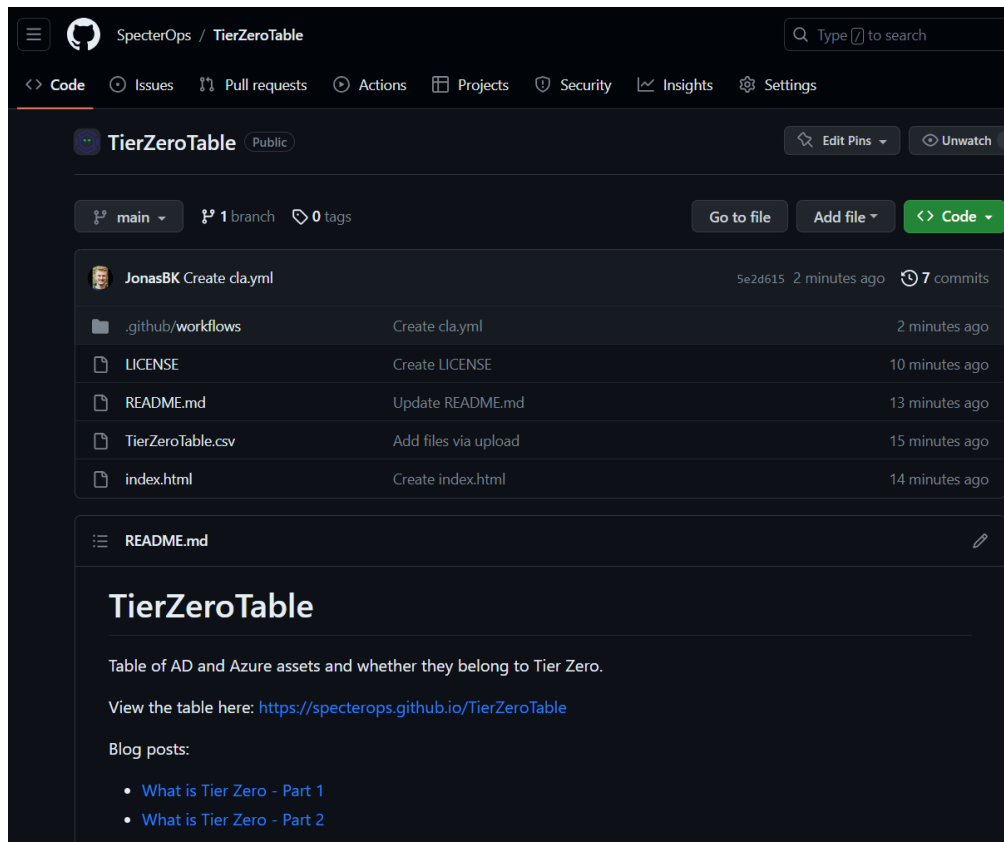
It Depends



Is Tier Zero



Tier Zero Table



SpecterOps / TierZeroTable

Type to search

<> Code Issues Pull requests Actions Projects Security Insights Settings

TierZeroTable Public

Edit Pins Unwatch

main 1 branch 0 tags

Go to file Add file Code

JonasBK Create clayml 5e2d615 2 minutes ago 7 commits

- .github/workflows Create clayml 2 minutes ago
- LICENSE Create LICENSE 10 minutes ago
- README.md Update README.md 13 minutes ago
- TierZeroTable.csv Add files via upload 15 minutes ago
- index.html Create index.html 14 minutes ago

README.md

TierZeroTable

Table of AD and Azure assets and whether they belong to Tier Zero.

View the table here: <https://specterops.github.io/TierZeroTable>

Blog posts:

- What is Tier Zero - Part 1
- What is Tier Zero - Part 2

Name	Type	IdP	Identification	Description	Known Tier Zero compromise abuse	Is Tier Zero	Reasoning	Microsoft Privileged access security roles	AdminSDHolder protected	External links
Account Operators	DC group	Active Directory	SID: S-1-5-32-549	The Account Operators group	DEPENDS	YES	The Account Operators group	YES	YES	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/understanding-ad-ds#groups
Administrators	DC group	Active Directory	SID: S-1-5-32-544	Members of the Administrators	YES	YES	The Administrators	YES	YES	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/understanding-ad-ds#groups
Backup Operators	DC group	Active Directory	SID: S-1-5-32-551	Members of the Backup Operators	YES	YES	The Backup Operators group	YES	YES	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/understanding-ad-ds#groups
Cryptographic Operators	DC group	Active Directory	SID: S-1-5-32-569	Members of this group are	NO	YES	The Cryptographic	YES	NO	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/understanding-ad-ds#groups
Distributed COM Users	DC group	Active Directory	SID: S-1-5-32-562	Members of the Distributed COM	NO	YES	The Distributed COM Users group	YES	NO	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/understanding-ad-ds#groups
Domain Admins	AD group	Active Directory	SID: S-1-5-21-<domain>-512	Members of the Domain Admins	YES	YES	The Domain Admins group has	YES	YES	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/understanding-ad-ds#groups
Domain Controllers	AD group	Active Directory	SID: S-1-5-21-<domain>-516	The Domain Controllers group	NO	YES	The Domain Controllers group	YES	YES	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/understanding-ad-ds#groups
Enterprise Admins	AD group	Active Directory	SID: S-1-5-21-<root>	The Enterprise Admins group	YES	YES	The Enterprise Admins group has	YES	YES	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/understanding-ad-ds#groups
Group Policy Creator Owners	AD group	Active Directory	SID: S-1-5-21-<domain>-520	This group is authorized to	NO	NO	The Group Policy Creator Owners	YES	NO	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/understanding-ad-ds#groups
Print Operators	DC group	Active Directory	SID: S-1-5-32-550	Members of this group can	DEPENDS	YES	The Print Operators group	YES	YES	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/understanding-ad-ds#groups
Read-only Domain	AD group	Active Directory	SID: S-1-5-21-<domain>-521	This group is composed of the	NO	NO	The Read-only Domain	YES	YES	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/understanding-ad-ds#groups
Schema Admins	AD group	Active Directory	SID: S-1-5-21-<root>	Members of the Schema Admins	DEPENDS	YES	The Schema Admins group has	YES	YES	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/understanding-ad-ds#groups
Server Operators	DC group	Active Directory	SID: S-1-5-32-549	Members of the Server Operators	DEPENDS	YES	The Server Operators group	YES	YES	https://learn.microsoft.com/en-us/windows-server/identity/ad-ds/understanding-ad-ds#groups

- <https://github.com/SpecterOps/TierZeroTable>
- Submit contributions or refinements

Questions