



Trust in Tech Cologne

Meetup

Securing your privileged identity and access in Azure (Active Directory)

Thomas Naunheim
(July 28th, 2020)

About Me

Thomas Naunheim

Cloud Engineer
Koblenz, Germany

 @Thomas_Live

 Thomas@Naunheim.net

 www.cloud-architekt.net



Securing your privileged identity and access

More than just vaulting and protecting admin passwords



Privileged Identity



Privileged Access



Secure Access Workstation

Level of Isolation and Separation
= Your Balance of Security, Complexity and Usability



Privileged Service Principals (Automation/DevOps Pipelines)



Protection of Privileged Identities

Protecting Privileged Identities

Foundation of Administrative Accounts



Microsoft Account



Separation of work and privileged accounts

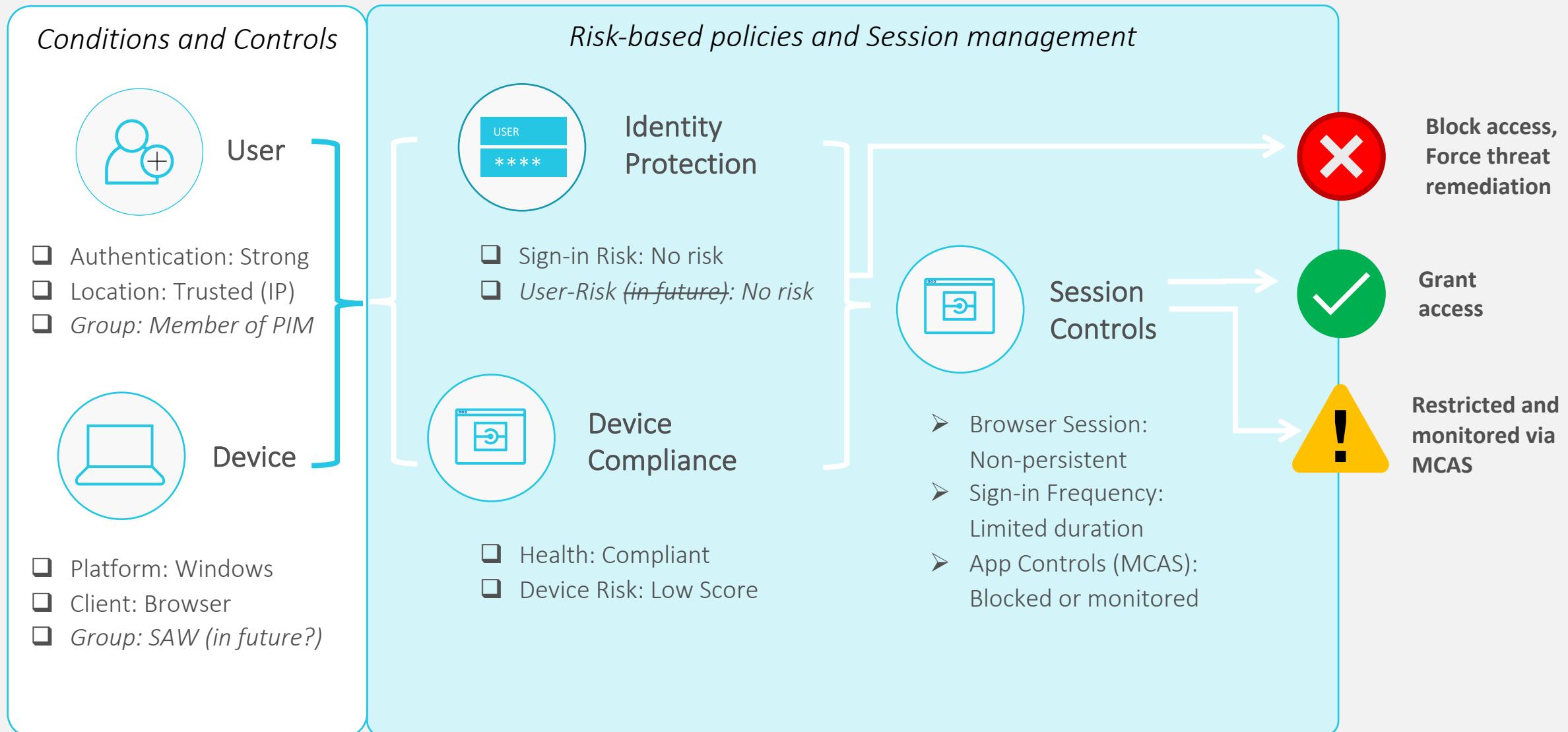
- ✓ Do not use unmanaged (personal) accounts
- ✓ Separate your work and privileged account(s)
- ✓ Do not sync from (AD) on-premises
- ✓ Separated custom domain name space
- ✓ Implement identity lifecycle and access review
- ✓ Remove licenses of productivity workloads
- ✓ Forwarded mail address

Secured and hardened Azure AD Tenant

- ✓ Synchronizing from secured Active Directory
- ✓ Monitor and response for suspicious activities
- ✓ Isolation of work- and privileged resources
- ✓ Strong baseline and tenant-level security

Protecting Privileged Identities

Design of Conditional Access for Privileged Identities



Create a resource
Home
Card
...
Library
Maintenance
Security
Sentinel
Insights
Monitor
Virtual machines
Cost Management + Billing
Policy
Advisor
Security Center
Subscriptions

< Dashboard > Security > Conditional Access | Policies >

CA10 - All privileged users / All Cloud Apps: Require MFA

Conditional access policy



Control user access based on conditional access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Name *

CA10 - All privileged users / All Cloud Ap...

Assignments

Users and groups ⓘ

Specific users included and specifi...

Cloud apps or actions ⓘ

All cloud apps

Conditions ⓘ

1 condition selected

Access controls

Grant ⓘ

1 control selected

Session ⓘ

0 controls selected

Control user access based on users and groups assignment for all users, specific groups of users, directory roles, or external guest users [Learn more](#)

None

All users

Select users and groups

All guest and external users ⓘ

Directory roles ⓘ

Select

Security operator and 51 more

Application administrator ...

Application developer ...

Authentication administrator ...

Azure DevOps administrator ...

Azure Information Protection admin... ...

B2C IEF Keyset administrator ...

B2C IEF Policy administrator ...

Billing administrator ...

Enable policy

Report-only On Off

Save

Governance and Protection of Privileged Identities



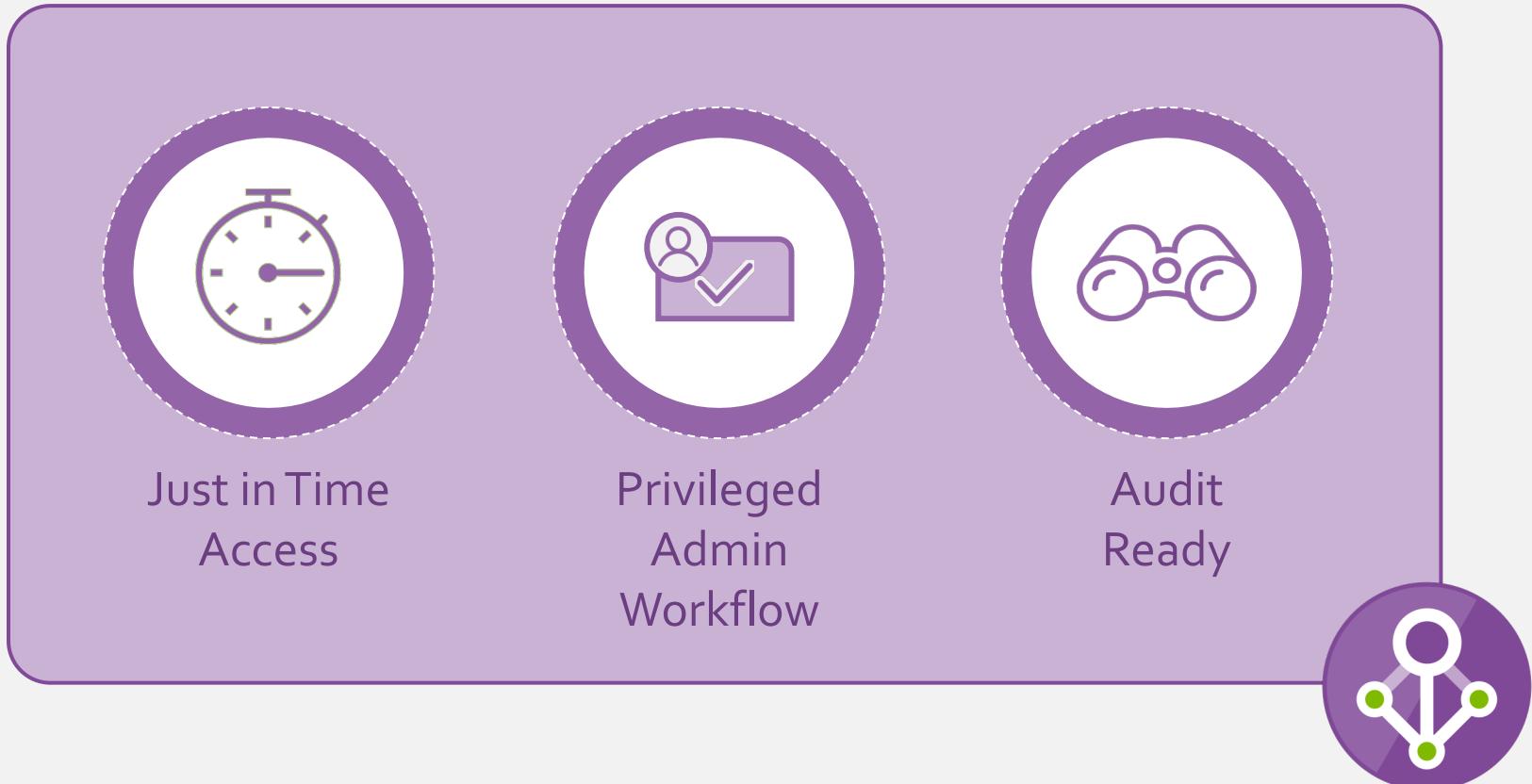
Securing Privileged Access

Securing Privileged Access

Zero Standing Privileged Access for your organization

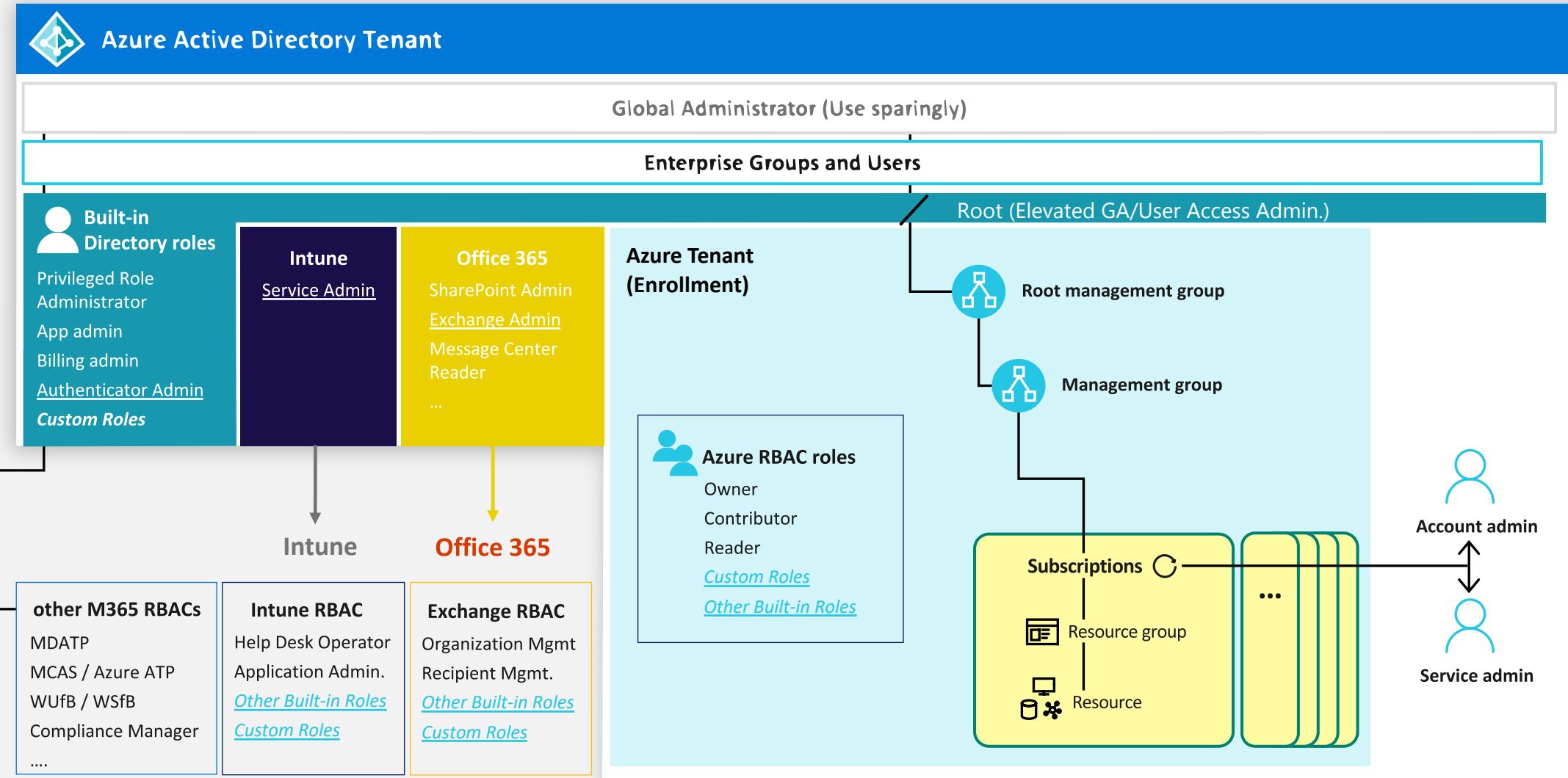


Granular Task
Scoped Access
(Just Enough)



Securing Privileged Access

Understanding Azure and Azure AD RBAC

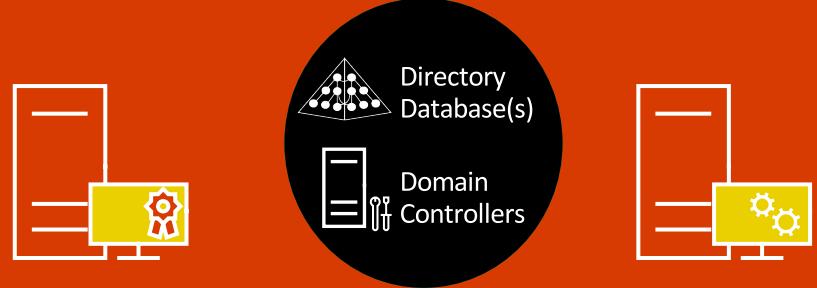


Securing Privileged Access

Tiering of Administrative Accounts and Permissions

Tier 0 (Identity)

Domain &
Enterprise Admins



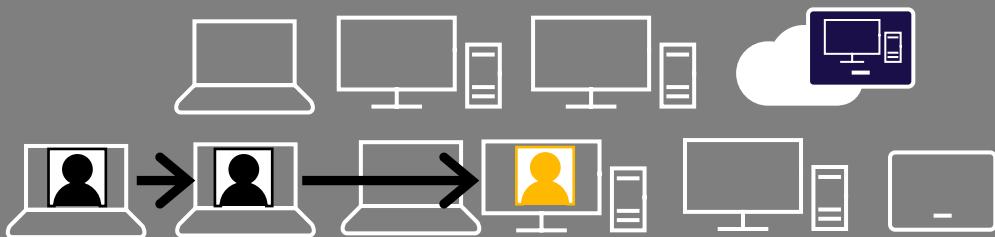
Tier 1 (Server)

Server Admins



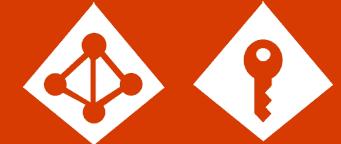
Tier 2 (Clients)

Workstation &
Device Admins



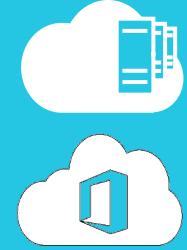
Tier 0 (Identity)

Global Admins
Authenticator Admin



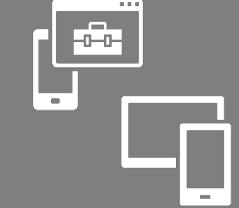
Tier 1 (Resources)

VM Contributor (IaaS)
Exchange Admin (SaaS)



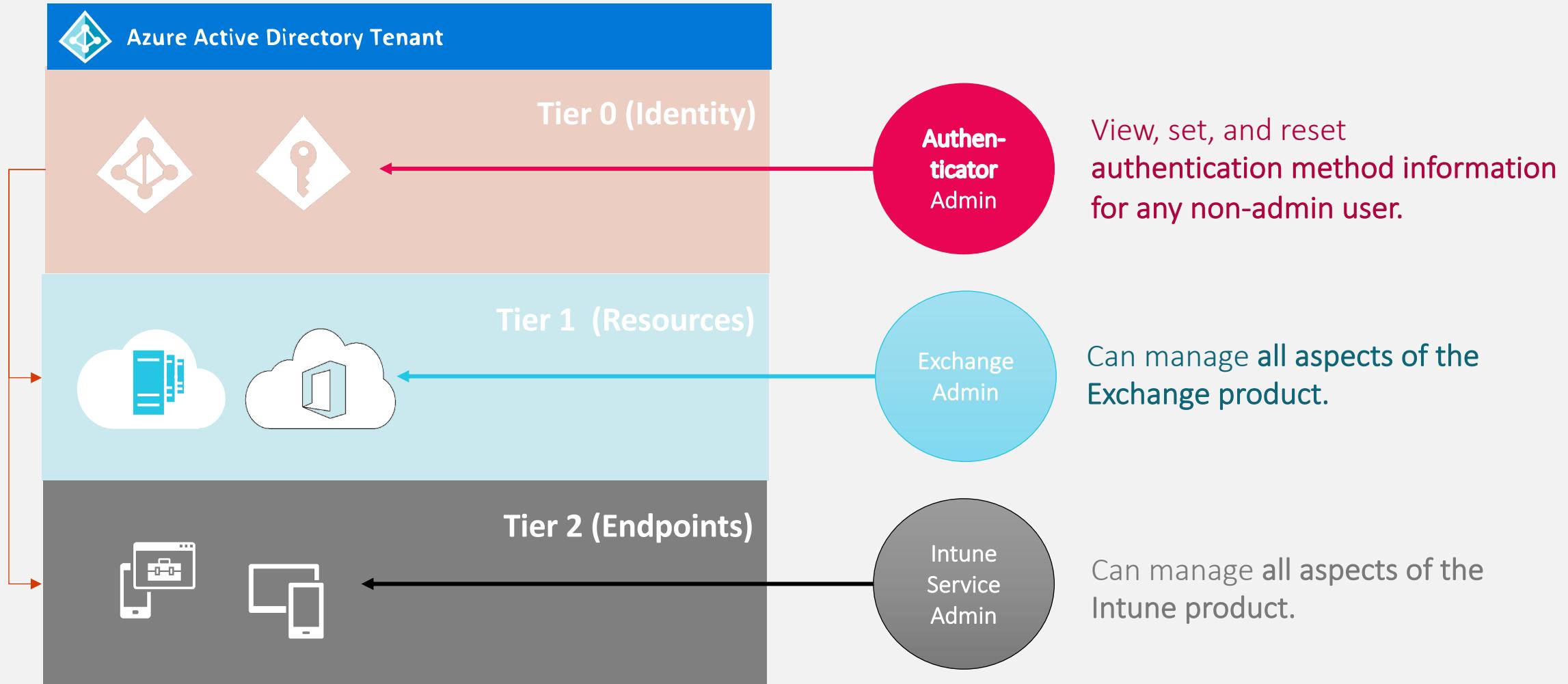
Tier 2 (Endpoints)

Intune Service Admin
MDATP “Admin”?



Securing Privileged Access

Azure AD: Tiering of Administrative Accounts and Permissions



Create a resource

Home

Card

Identity

Governance

Security

Sentinel

Tune

Monitor

Virtual machines

Cost Management + Billing

Policy

Advisor

Security Center

Subscriptions

Dashboard > Identity Governance > Privileged Identity Management >

Cloud-Architekt.net | Roles

Privileged Identity Management | Azure AD roles

Quick start

Overview

Tasks

Pending requests

Approve requests

Review access

Manage

Roles

Assignments

Alerts

Access reviews

Settings

Activity

Resource audit

My audit

Add assignments Refresh Export

Search by role name

Role

Description

Application Administrator

Users with this role can create and manage all aspects of app registrations and enterprise apps.

Application Developer

this role can create application registrations independent of the 'Users can register applications' setting.

Authentication Administrator

Can access, view, set and reset authentication method information for any non-admin user.

Azure DevOps Administrator

Can manage A DevOps organization policy and settings.

Azure Information Protection Administrator

Users with this role have user rights only on the Azure Information Protection service.

B2C IEF Keyset Administrator

Manage secrets for a B2C tenant.

B2C IEF Policy Administrator

Creates and manages policies for a B2C tenant.

Billing Administrator

Makes purchases, manages subscriptions.

Cloud Application Administrator

Users with this role can manage cloud applications.

Cloud Device Administrator

Full access to manage devices.

Compliance Administrator

Users with this role have management permissions.

Compliance Data Administrator

Creates and manages compliance data.

Conditional Access Administrator

Users with this role have the ability to manage Azure Active Directory conditional access settings.

Dynamics 365 Administrator

Users with this role have global permissions within Microsoft Dynamics 365.

Customer LockBox Access Approver

Can approve or reject customer requests to access customer data.

Desktop Analytics Administrator

Users in this role will have access to manage Desktop Analytics.

Device Administrators

Users with this role become local machine administrators on all Windows devices that are joined to Azure Active

Directory Readers

Allows access to various read-only tasks in the directory.

Exchange Administrator

Users with this role have global permissions within Microsoft Exchange Online.

External ID User Flow Administrator

Create and manage all aspects of user flows.

External ID User Flow Attribute Administrator

Create and manage the attribute schema available to all user flows.

External Identity Provider Administrator

Configure identity providers for use in direct federation.

Global Administrator

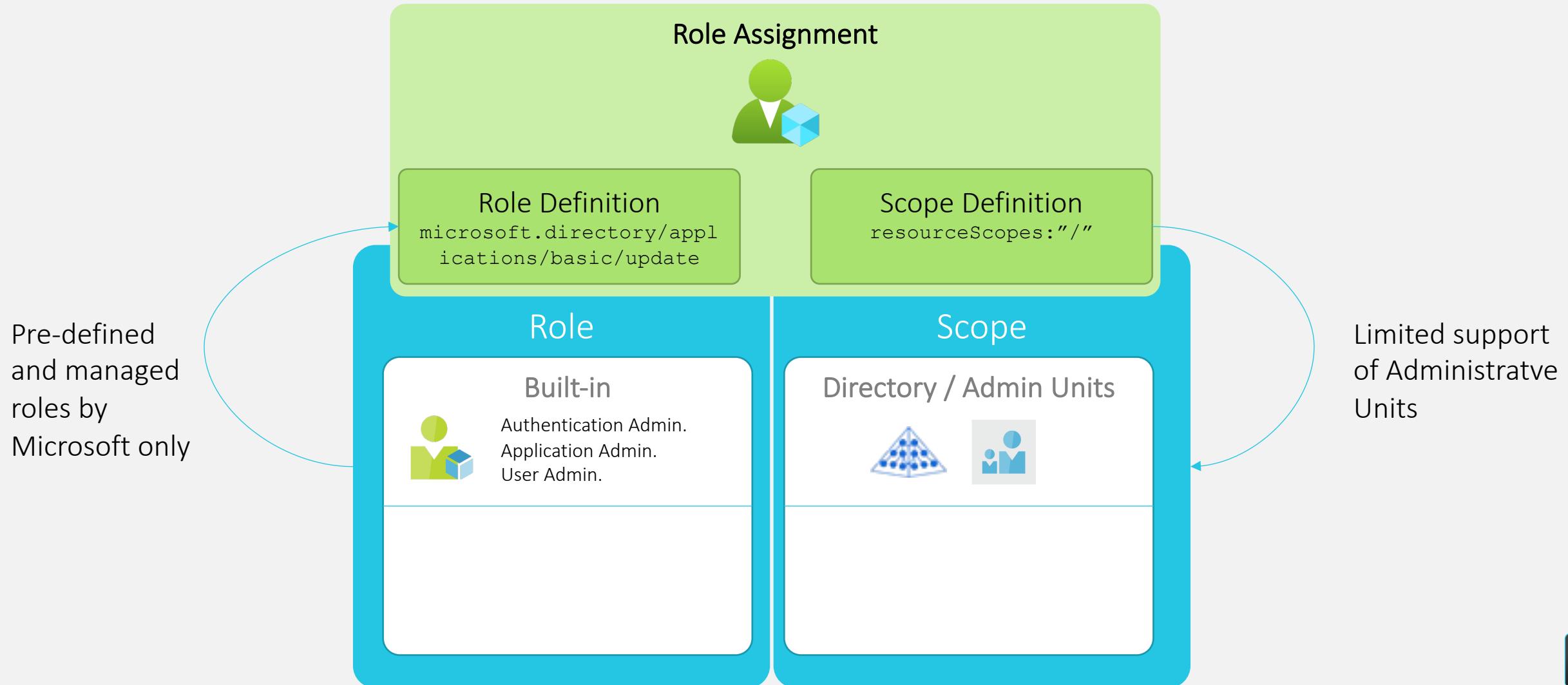
Users with this role have access to all administrative features in Azure Active

Directory

Challenges and Limitations in Delegation of Directory roles

Securing Privileged Access

Reduce scope and permission of Azure AD Roles

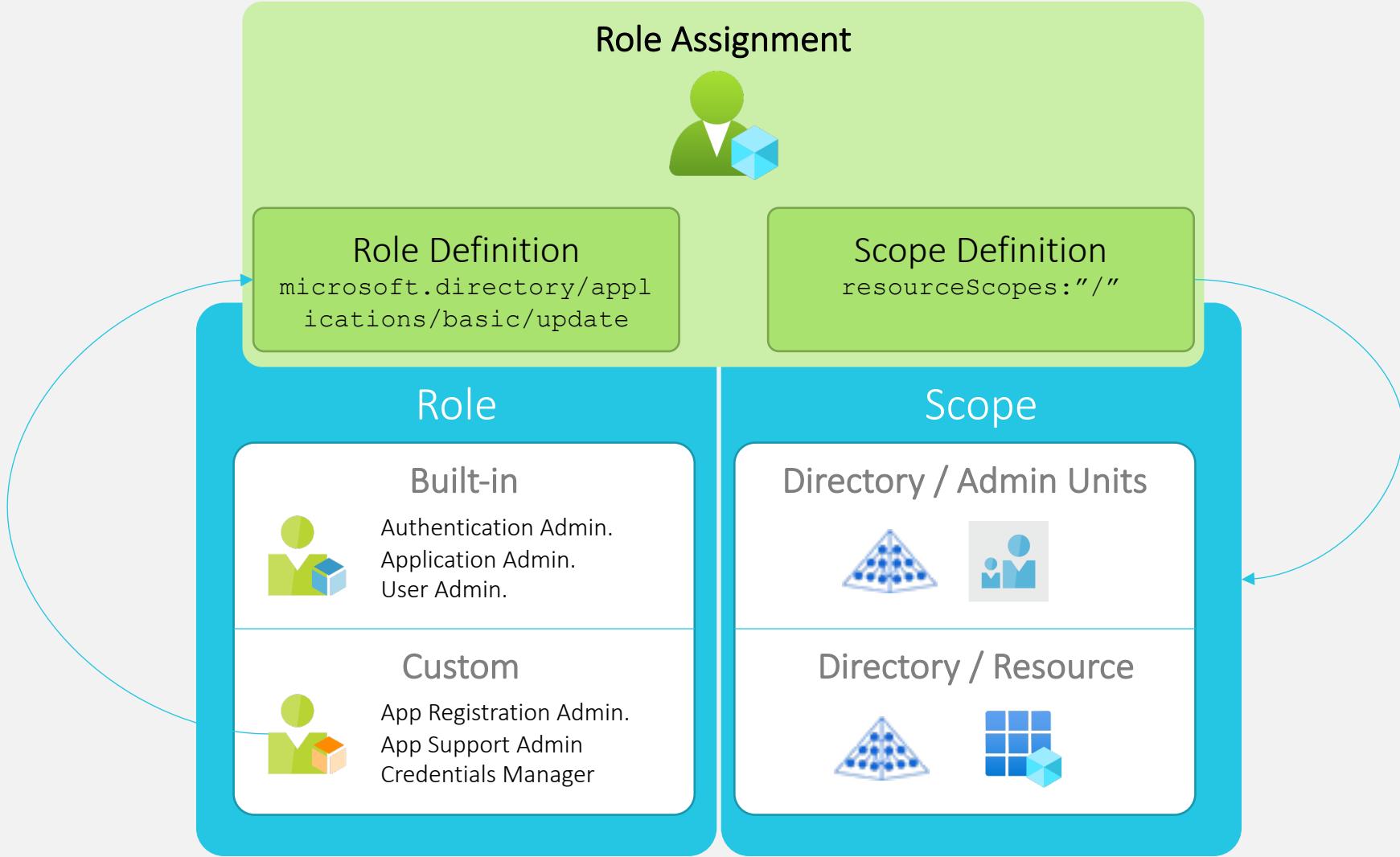


Securing Privileged Access

Reduce scope and permission of Azure AD Roles

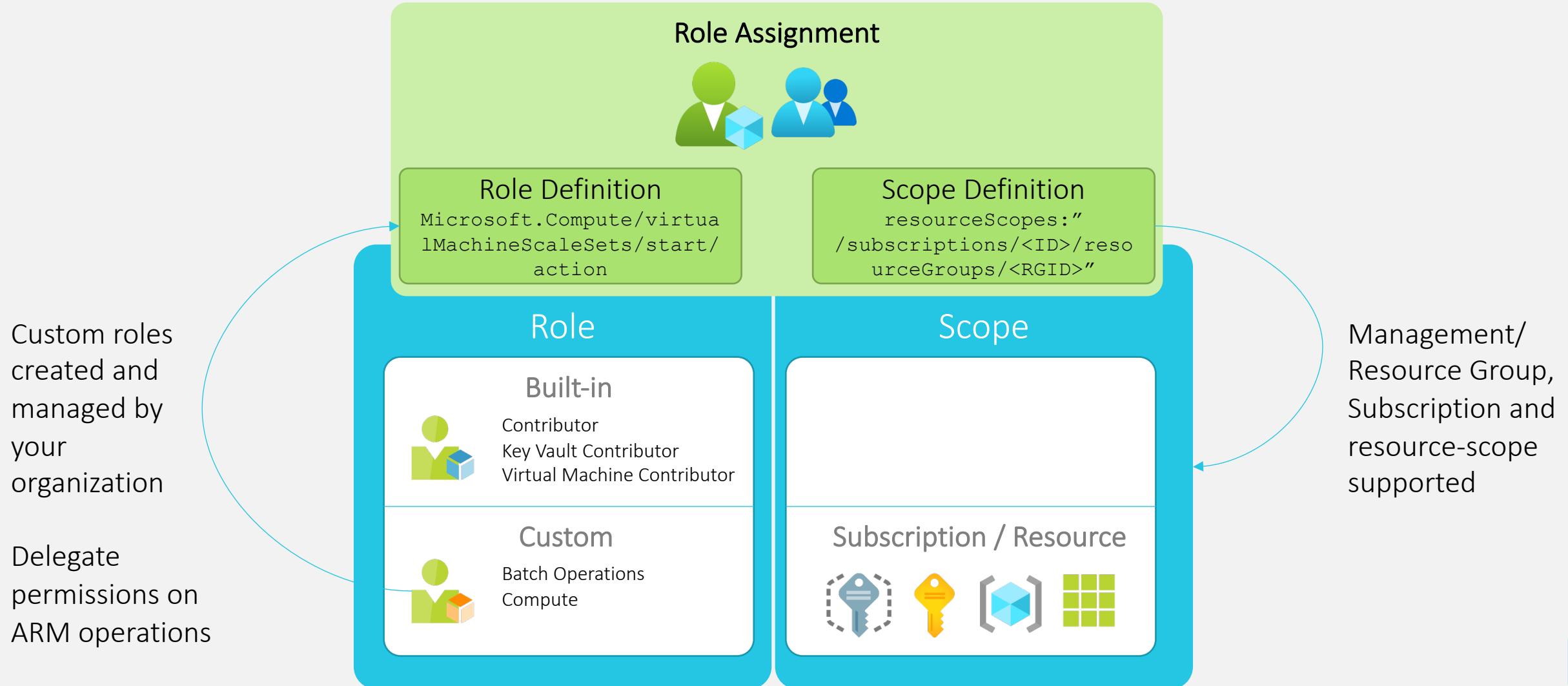
Custom roles created and managed by your organization

Only few role permissions supported



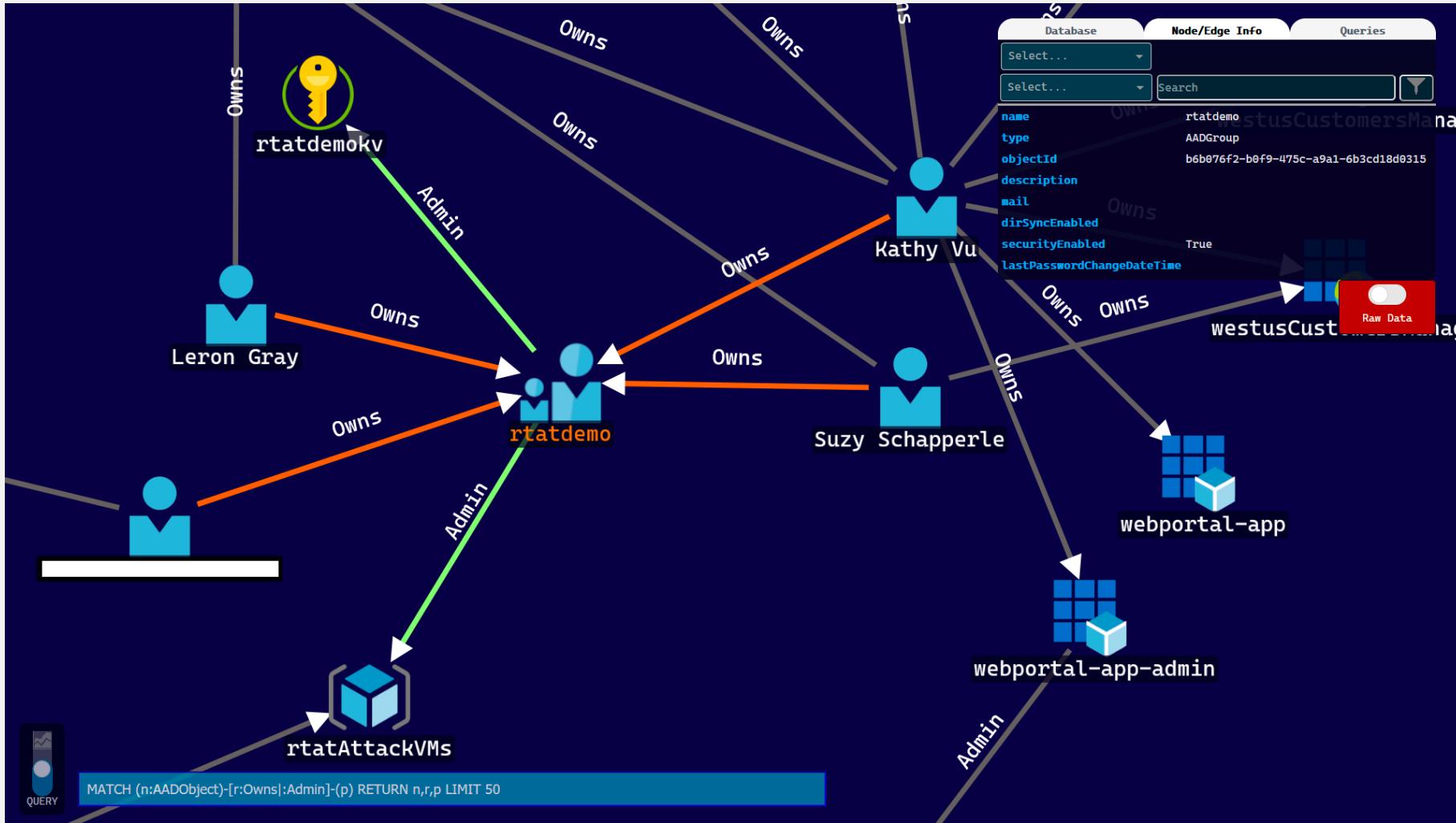
Securing Privileged Access

Reduce scope and permission of Azure RBAC



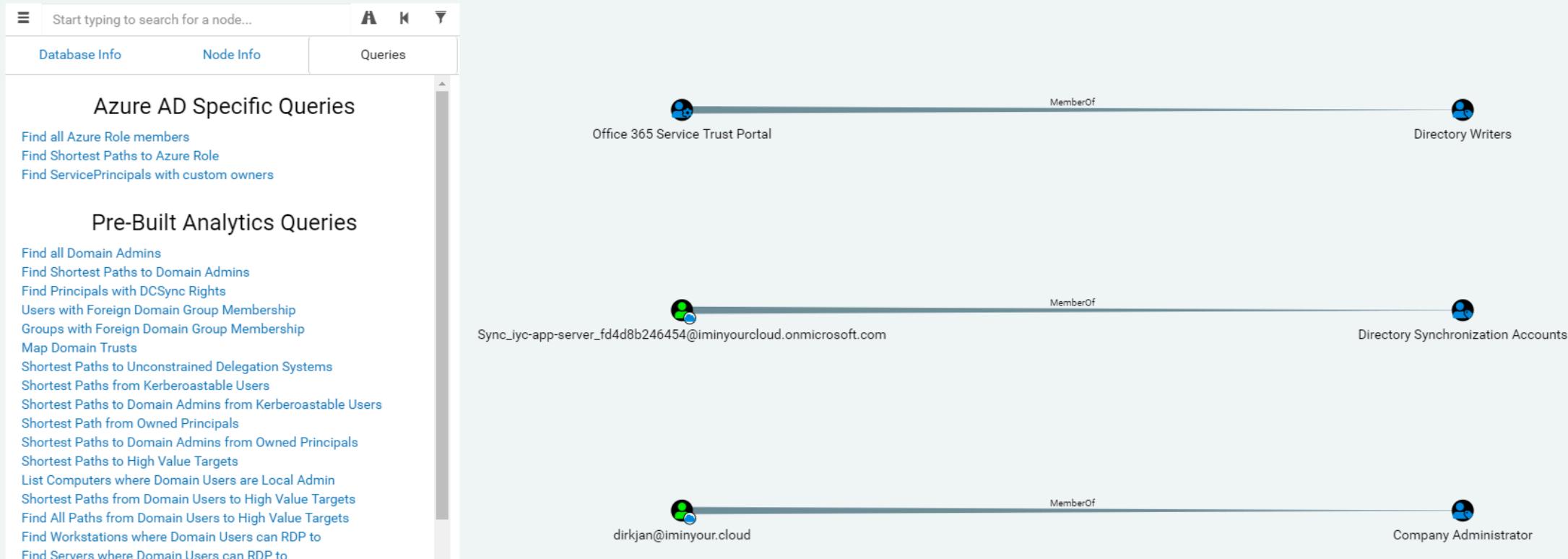
Securing Privileged Access

Stormspotter (Released in May 2020)



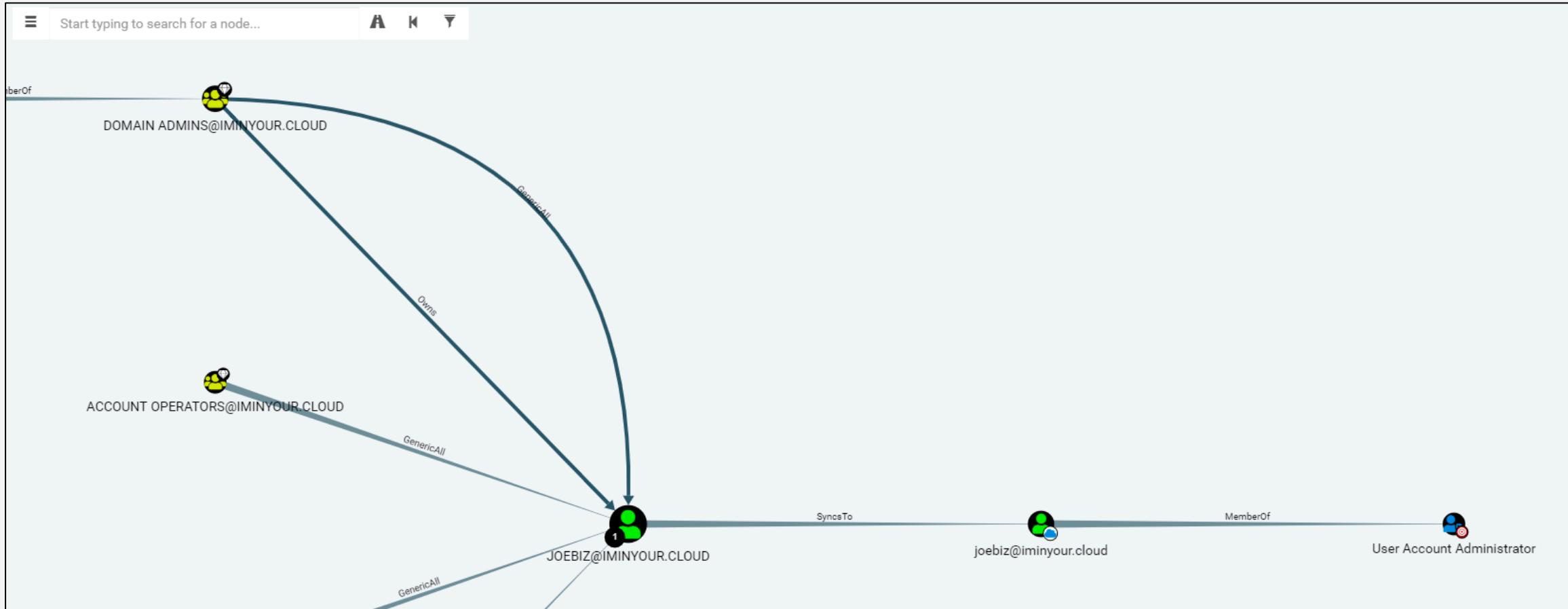
Securing Privileged Access

ROADtools (released in April 2020)



Securing Privileged Access

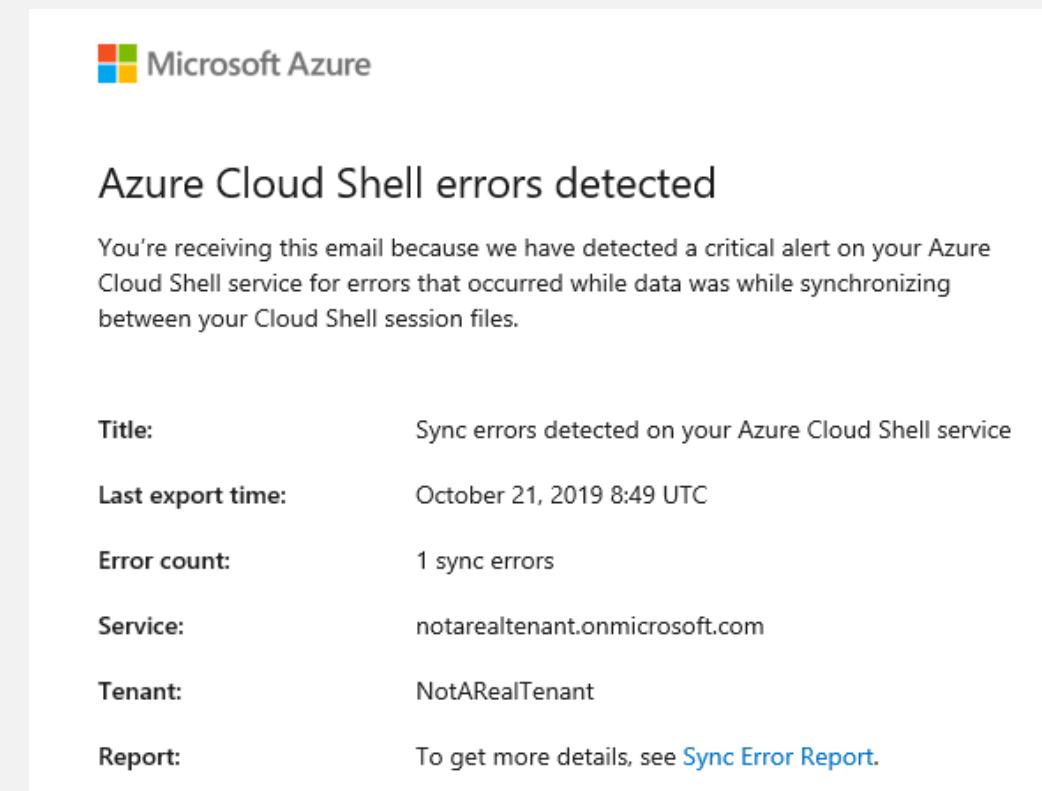
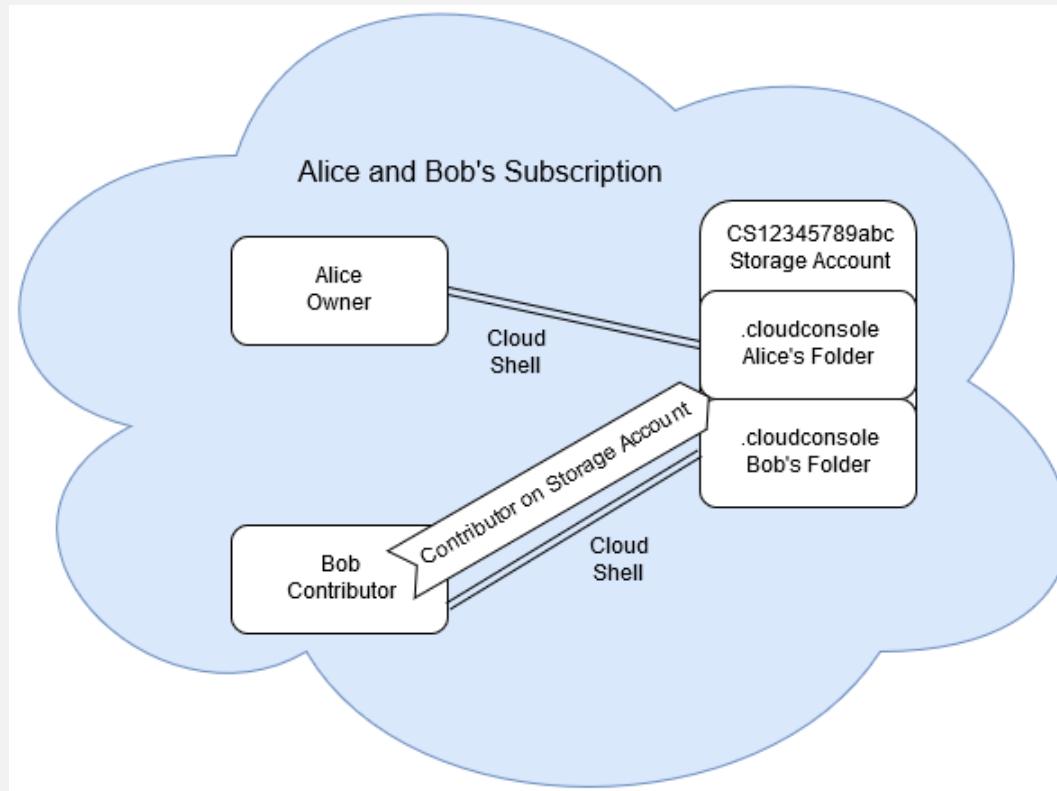
ROADtools (released in April 2020)



Securing Privileged Access

Privilege Escalation from Storage Contributor

- Azure Privilege Escalation via Azure Cloud Shell:
[Blog post by Karl Fosaaen \(NetSPI\)](#)



Securing Privileged Access

Privilege Escalation from Storage Contributor

- Azure Privilege Escalation via Cloud Shell:

```
$token = (curl http://localhost:50342/oauth2/token --data  
"resource=https://management.azure.com/" -H Metadata:true -s)
```

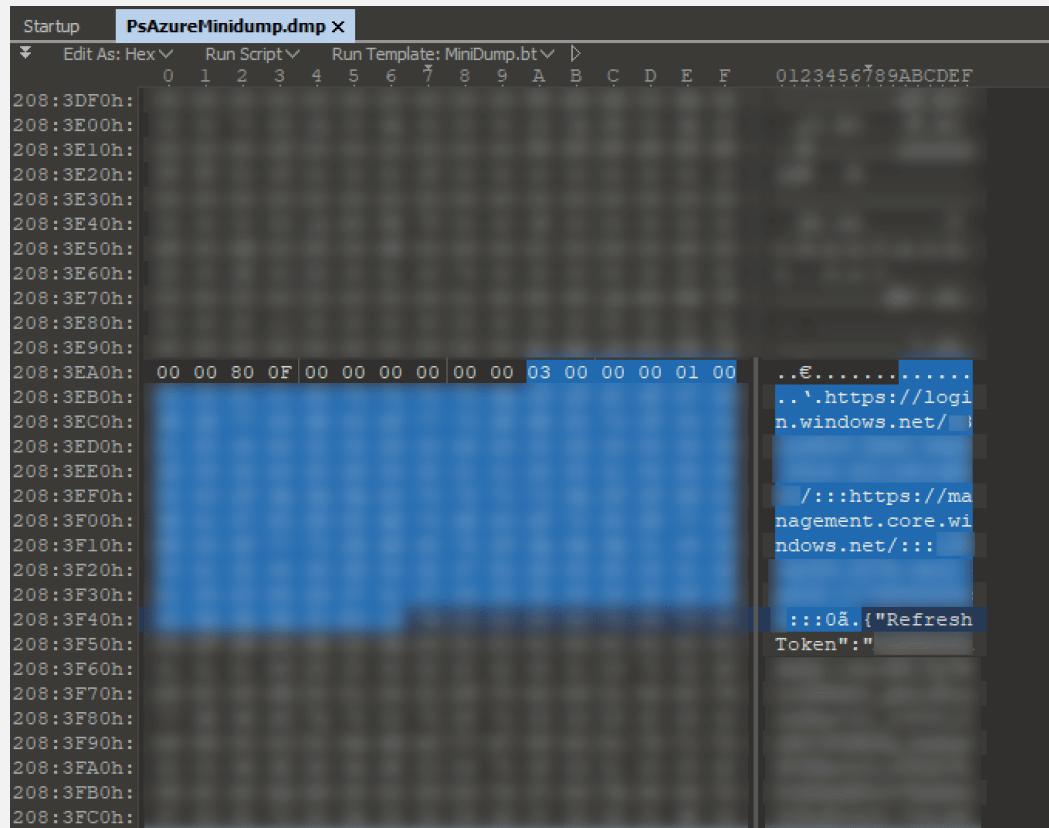
- Microsoft Security Response Center (MSRC) response:

“...confirming that this is the currently designed behavior. We have expanded our guidance on this issue here – <https://docs.microsoft.com/en-us/azure/cloud-shell/persisting-shell-storage#securing-storage-access> and the team will look into possible design changes related to storage accounts.”

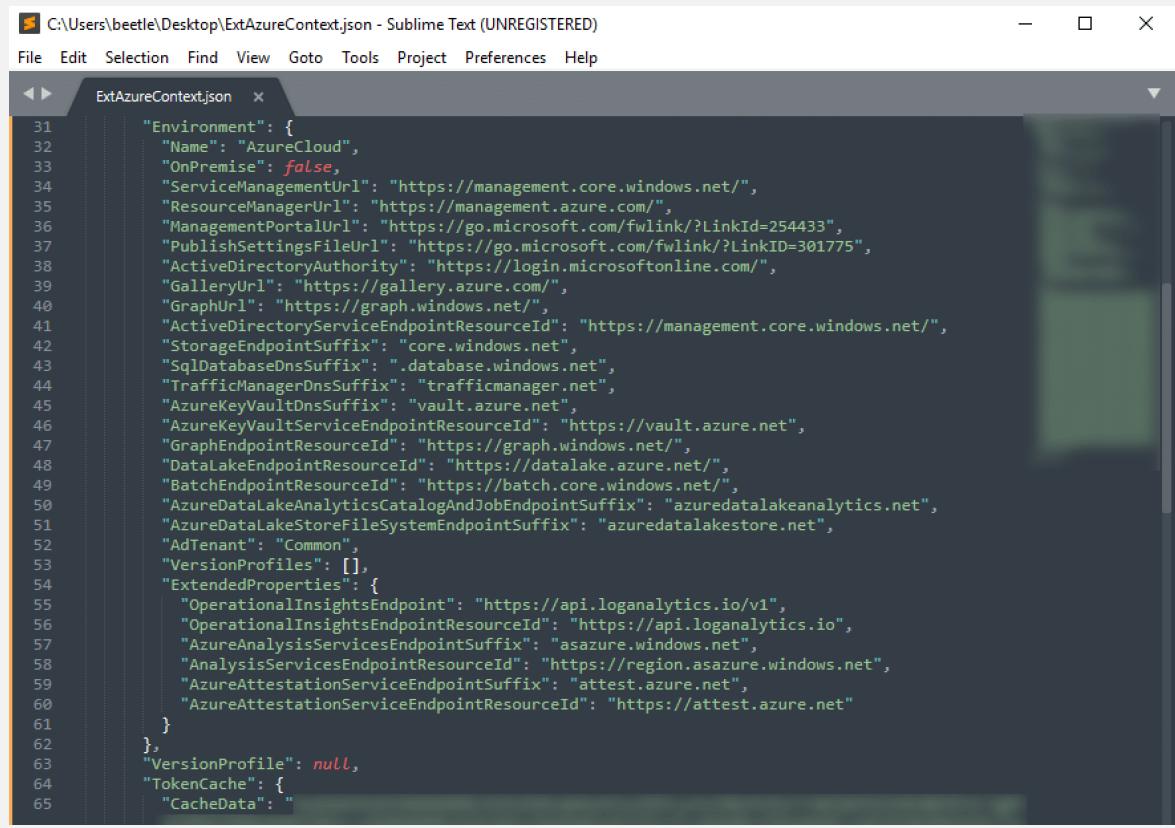
Securing Privileged Access

Privilege Escalation from Device Administrator

- Disconnected Azure PowerShell Sessions: Dumping from PowerShell Memory:
[Blog post by R.J. McDown \(Lares\)](#)



The screenshot shows a memory dump of a PowerShell session in Immunity Debugger. The dump is titled "PsAzureMinidump.dmp". The left pane displays memory addresses from 208:3DF0h to 208:3FC0h, with the current view centered around address 208:3EA0h. The right pane shows the raw hex and ASCII data. A specific memory location at 208:3EA0h contains the URL "https://management.core.windows.net/" and a refresh token. The refresh token is partially visible as "...0ä.{\"RefreshToken\":\"". The memory dump interface includes various tools like "Edit As: Hex", "Run Script", and "Run Template".



The screenshot shows a JSON configuration file named "ExtAzureContext.json" open in Sublime Text. The file contains settings for an Azure environment, including URLs for Service Management, Resource Manager, and Management Portal, as well as Active Directory and Graph endpoints. The "Environment" section specifies "Name": "AzureCloud" and "OnPremise": false. The "ActiveDirectoryAuthority" is set to "https://login.microsoftonline.com". The "GraphUrl" is "https://graph.windows.net/". The "StorageEndpointSuffix" is "core.windows.net", and the "SqlDatabaseDnsSuffix" is ".database.windows.net". The "TrafficManagerDnsSuffix" is "trafficmanager.net", and the "AzureKeyVaultDnsSuffix" is "vault.azure.net". The "AzureKeyVaultServiceEndpointResourceId" is "https://vault.azure.net", and the "GraphEndpointResourceId" is "https://graph.windows.net/". The "DataLakeEndpointResourceId" is "https://datalake.azure.net/", and the "BatchEndpointResourceId" is "https://batch.core.windows.net/". The "AzureDataLakeAnalyticsCatalogAndJobEndpointSuffix" is "azuredatalakeanalytics.net", and the "AzureDataLakeStoreFilesystemEndpointSuffix" is "azuredatalakestore.net". The "AdTenant" is "Common", and there are no version profiles defined. The "ExtendedProperties" section includes endpoints for Operational Insights and Analysis Services.

```
31     "Environment": {
32         "Name": "AzureCloud",
33         "OnPremise": false,
34         "ServiceManagementUrl": "https://management.core.windows.net/",
35         "ResourceManagerUrl": "https://management.azure.com/",
36         "ManagementPortalUrl": "https://go.microsoft.com/fwlink/?LinkId=254433",
37         "PublishSettingsFileUrl": "https://go.microsoft.com/fwlink/?LinkId=301775",
38         "ActiveDirectoryAuthority": "https://login.microsoftonline.com",
39         "GalleryUrl": "https://gallery.azure.com",
40         "GraphUrl": "https://graph.windows.net",
41         "ActiveDirectoryServiceEndpointResourceId": "https://management.core.windows.net",
42         "StorageEndpointSuffix": "core.windows.net",
43         "SqlDatabaseDnsSuffix": ".database.windows.net",
44         "TrafficManagerDnsSuffix": "trafficmanager.net",
45         "AzureKeyVaultDnsSuffix": "vault.azure.net",
46         "AzureKeyVaultServiceEndpointResourceId": "https://vault.azure.net",
47         "GraphEndpointResourceId": "https://graph.windows.net",
48         "DataLakeEndpointResourceId": "https://datalake.azure.net",
49         "BatchEndpointResourceId": "https://batch.core.windows.net",
50         "AzureDataLakeAnalyticsCatalogAndJobEndpointSuffix": "azuredatalakeanalytics.net",
51         "AzureDataLakeStoreFilesystemEndpointSuffix": "azuredatalakestore.net",
52         "AdTenant": "Common",
53         "VersionProfiles": [],
54         "ExtendedProperties": {
55             "OperationalInsightsEndpoint": "https://api.loganalytics.io/v1",
56             "OperationalInsightsEndpointResourceId": "https://api.loganalytics.io",
57             "AnalysisServicesEndpointSuffix": "asazure.windows.net",
58             "AnalysisServicesEndpointResourceId": "https://region.asazure.windows.net",
59             "AzureAttestationServiceEndpointSuffix": "attest.azure.net",
60             "AzureAttestationServiceEndpointResourceId": "https://attest.azure.net"
61         },
62     },
63     "VersionProfile": null,
64     "TokenCache": {
65         "CacheData": "
```

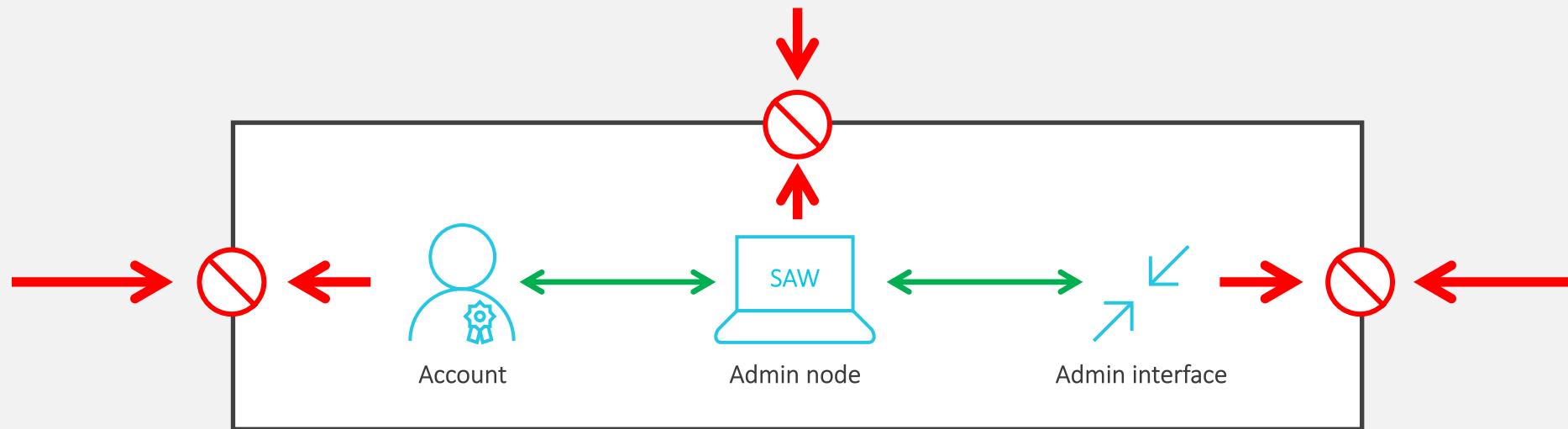
Source: [Disconnected Azure PowerShell Sessions \(Lares Blog\)](#)



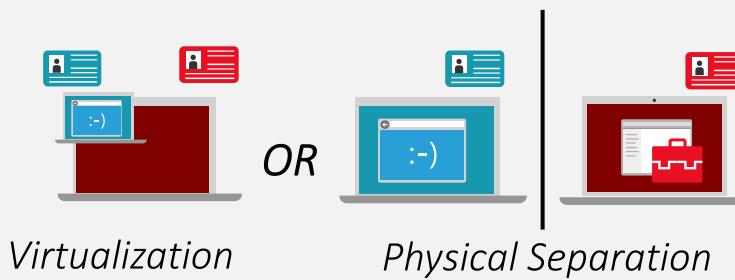
Securing your Access Workstation

Securing your access workstations (SAW)

Overview of Secure Admin Workstation



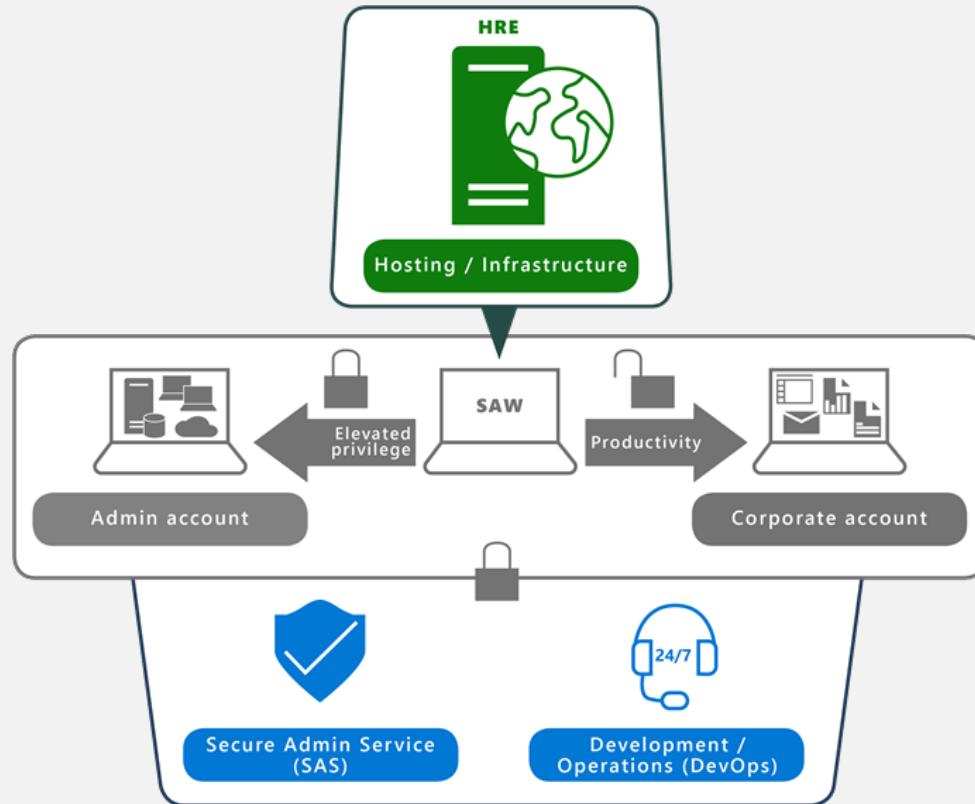
- [DISA STIG](#) requires Privilege Access Workstations (PAW) for Cloud Tenant Administration
- [CIS \(C4\)](#): Administrators shall use a dedicated, isolated machine for all administrative tasks



Securing your access workstations (SAW)

Secure access to Azure by Microsoft IT

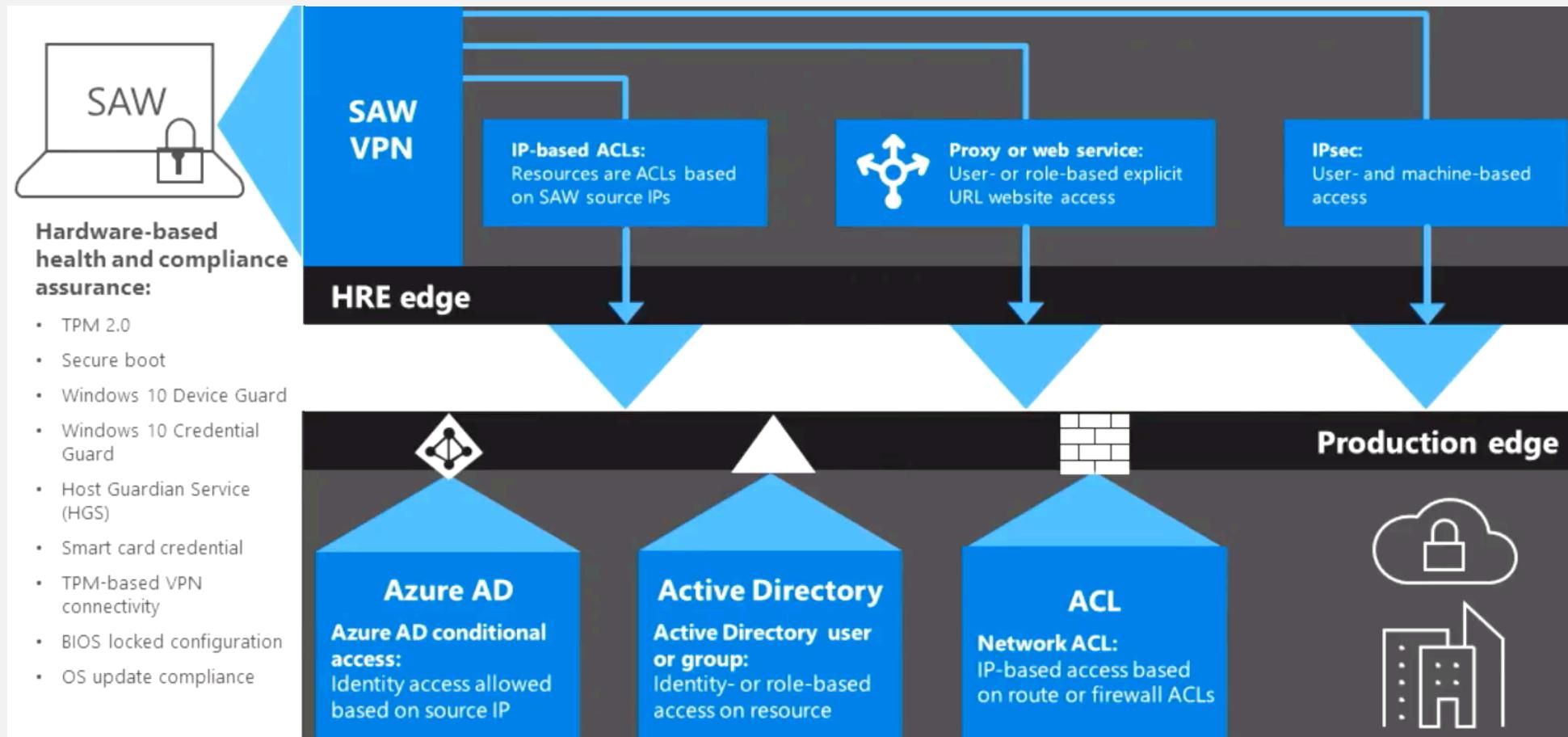
Secure Admin Workstation used for High Risk Environment [at Microsoft](#)



Securing your access workstations (SAW)

Secure access to Azure by Microsoft IT

Secure Admin Workstation used for High Risk Environment [at Microsoft](#)



Source: [Microsoft Docs \(„Protecting high-risk environments with secure admin workstations“\)](#)



admThom0
admthom0@cloud-architekt.net

Please enter your security key PIN

 PIN →

Change PIN

Sign-in options

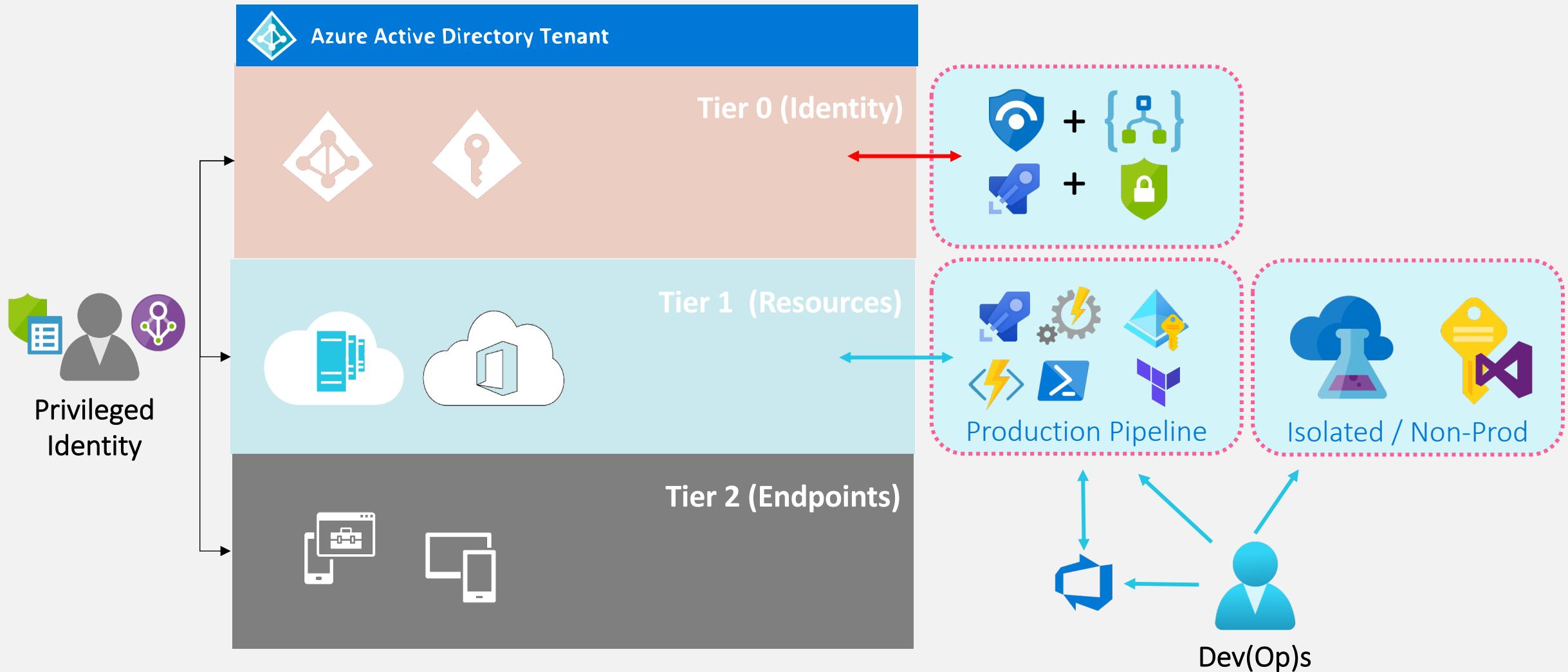
cloud...

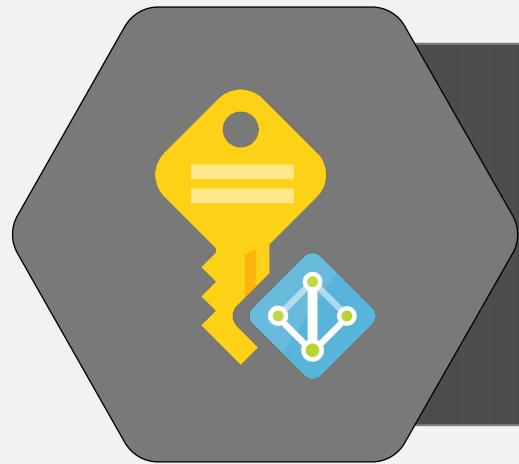
ENG ⌂ ⌁

Cloud-managed Secure Admin Workstation (SAW)

Securing Privileged Access

Tiering of Administrative Accounts and Permissions



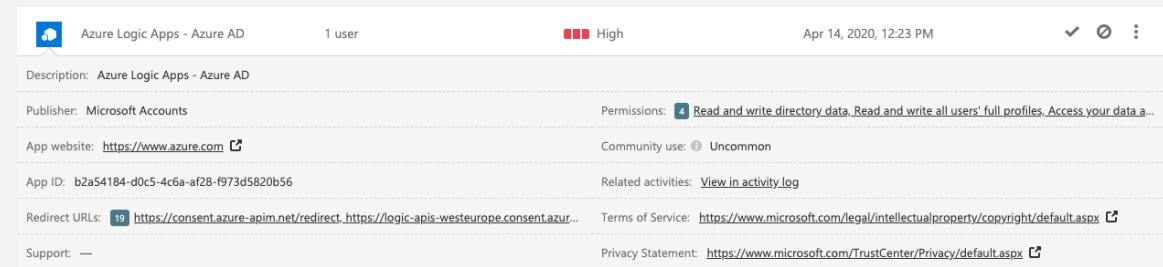


Audit and Protection of Service Principals

Audit and Protection of Service Principals

Risks of Service Principals

- Attack scenarios:
 - Delegated (OAuth2) vs. Application Permissions (without a signed-in user)
 - No security options (Conditional Access, MFA or IPC “Sign-in” risk policy)
 - No sign-in events
 - = Application Administrators (Tier1) or Owner can impersonate an “application identity”
 - = Backdooring Azure AD with service principals
- Defense and mitigations:
 - Inventory and monitoring
 - Assignments to Directory Roles
 - API permissions assignment
 - Owner of App Registration
 - “Application Administrator” as Custom Role / Scope
 - Configure expiration of ClientSecret and secure storing (Audited Key Vaults)



[Dashboard](#) > [Cloud-Architekt.net | App registrations](#) >

msidotnet-func | Certificates & secrets

- [Overview](#)
- [Quickstart](#)
- [Integration assistant \(preview\)](#)

Manage

- [Branding](#)
- [Authentication](#)
- [Certificates & secrets](#)
- [Token configuration](#)
- [API permissions](#)
- [Expose an API](#)
- [Owners](#)
- [Roles and administrators \(Preview\)](#)
- [Manifest](#)
- [Support + Troubleshooting](#)
- [Troubleshooting](#)
- [New support request](#)

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

	Upload certificate	Thumbprint	Start date	Expires
--	--------------------	------------	------------	---------

No certificates have been added for this application.

Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as app secrets.

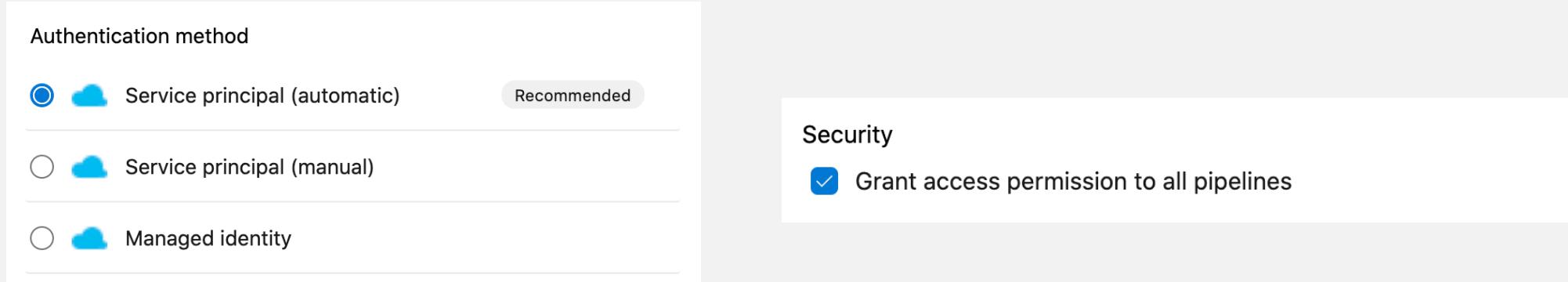
	New client secret	Description	Expires	Value
		No description	6/13/2030	Hidden

Securing secrets and „Managed Identities“ for Automation

Audit and Protection of Service Principals

Considerations of CD Pipelines in Azure DevOps

- Secrets and Service Principals in Pipeline
 - Accessing Azure Key Vault Secrets from your pipelines
 - Service Principal or Managed Identities in [Service Connections](#)



- Audit in Azure DevOps in [Public Preview](#)
 - Rest-API: https://auditservice.dev.azure.com/<OrgName>/_apis/audit/actions
 - Streaming of “Auditing Logs” → *EventHub, Log Analytics*
 - No correlation between Azure Activity and Pipeline Events → [My feature request](#)



Project Settings

IaC-WebApp

General

Overview

Teams

Permissions

Connections

Cards

Issues

Project configuration

Team configuration

GitHub connections

Repos

Repositories

Pipelines

Agent pools

Parallel jobs

Settings

Test management

Release retention

Service connections

XAML build services

Test

Retention

Security

MSDN Subscription

User permissions

Project

Organization



Undo



Save

Inheritance



[IaC-WebApp]\Endpoint Administrators



Administrator

Inherited



thomas



Administrator

Assigned

Pipeline permissions

No restrictions

Any pipeline may use this resource

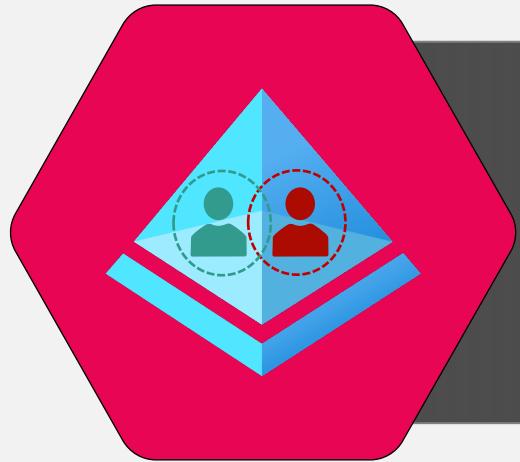
[Learn more](#)

Auditing of Service Connections in Azure DevOps

Only current project

Share service connection with other projects.

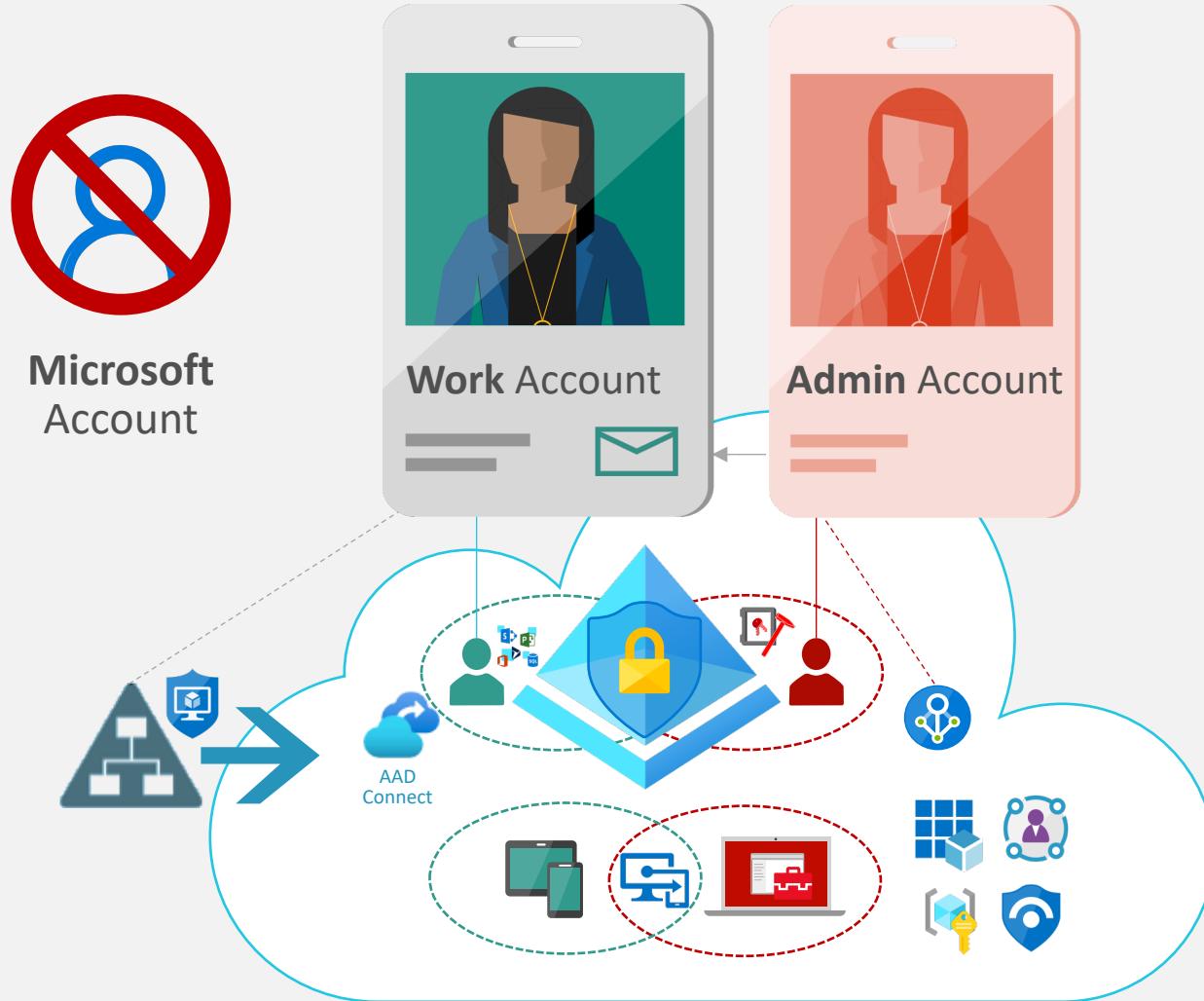
[Learn more](#)



Isolation & Protection on Inter-Tenant-Level

Protecting Privileged Identities

Considerations and Limitations



Privileged Accounts and Resources

- Consider limitations of Administrative Units
- Tenant-wide delegation by AAD / Azure RBAC
 - Separation of all privileged resources (Cloud Shell)

Secure Admin Workstations (SAW)

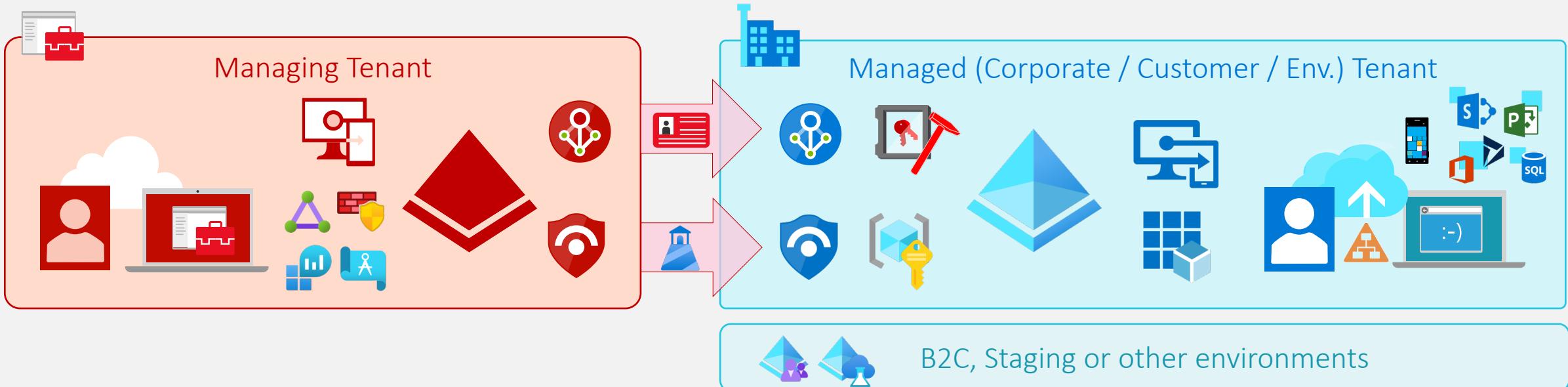
- Scoped and Intune RBAC roles separation between SAW and Standard Workplaces
- Client Certificate (via MCAS) or Trusted IP (VPN) to verify SAW device
- Deployment & Usability of Virtualization

Service Principals and DevOps

- Protection of secrets and automation tasks
- Audit and security concept of DevOps tools
- Using “Managed Identity” where possible

Protecting Privileged Identities

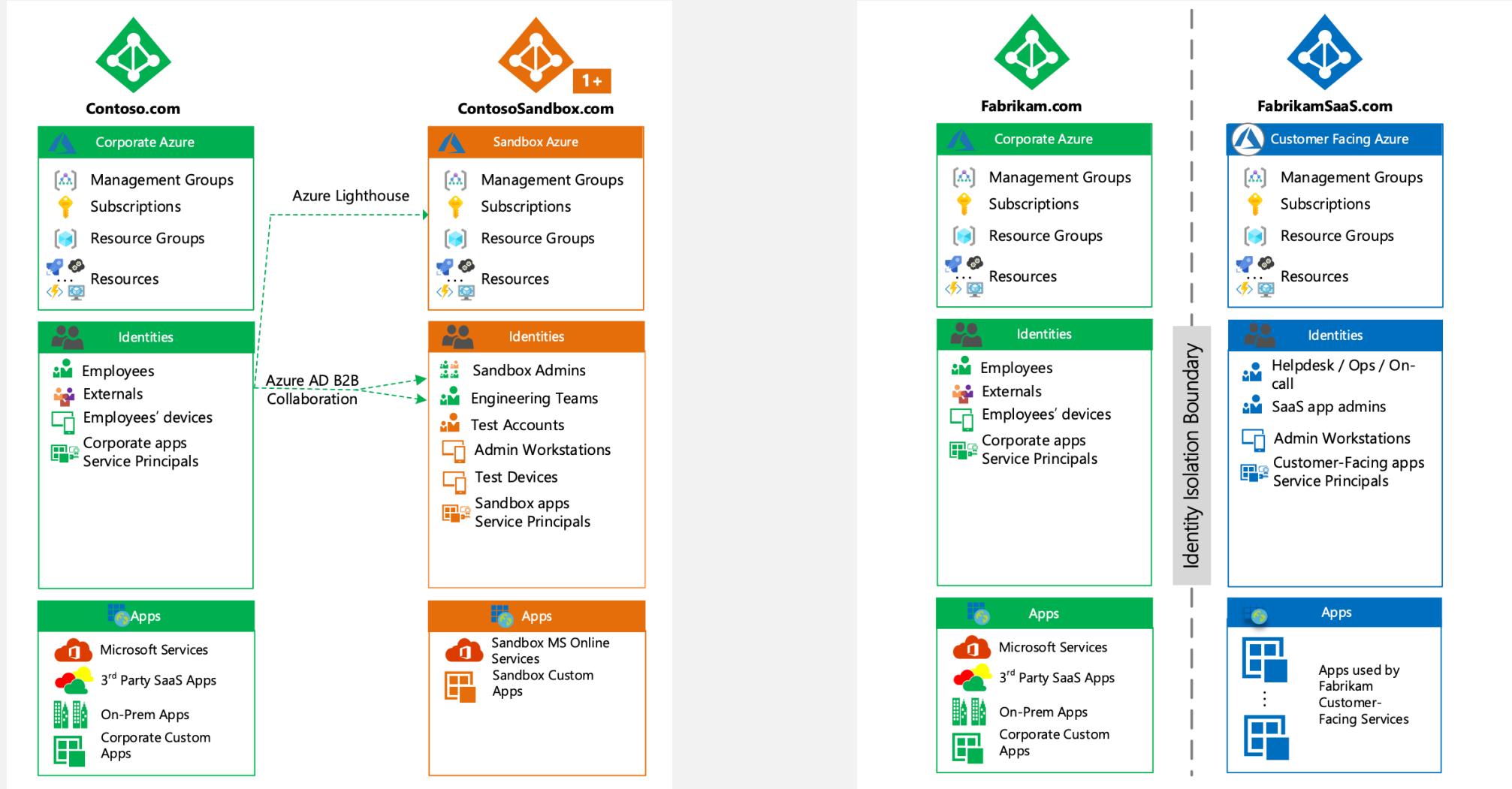
“Red Tenant” – Azure AD Tenant as security boundary



- No hybrid identity integration (no security risks by Azure AD Connect)
- **Privileged resources only** (security groups, apps, network, devices,...)
- Reduced attack surface, shared resources from secured environment
- Dependence on „**Azure AD B2B**“ feature, Doubled Identity Protection, FIDO2 & Security Policies
- Costs and Complexity (Licenses, Administrative Costs, Additional VNet Peering)
- Limited support by Microsoft (no PAM trust, „single tenant“ approach, avoid complexity)

Protecting Privileged Identities

“Sandbox/Staging Tenants” – Identity Isolation Boundary



Securing your privileged identity and access

More than just vaulting and protecting admin passwords



Privileged Identity

- Separated/isolated accounts from productive tasks
- Located in secured and monitored identity directory
- Strong and passwordless authentication options



Privileged Access

- “Least privileged” by defined and tiered RBAC design
- Zero Rights by default / Non-persistent access
- Regular review of privileged accounts and access



Secure Access Workstation

- Privileged access from hardened device only
- Secured admin interface and restricted user sessions
- Balance between usability and security of administrators



Privileged Service Principals

Auditing and protecting of secrets and privileged access in Automation tasks or DevOps Pipelines (CI/CD)

A close-up photograph of a person's hands typing on a silver laptop keyboard. The background is blurred, showing what appears to be a window or a bright screen.

Thank You

 @Thomas_Live

 Thomas@Naunheim.net

 www.cloud-architekt.net