Enhancing you Azure resources security with PIM

Olav Tvedt

SparebankenVest

Twitter: @olavtwitt

LinkedIn: https://www.linkedin.com/in/otvedt/

Podkast: BlåSkjerm Brødrende

MVP Dagen

Takk til våre sponsorer

Microsoft

audiocodes

glasspaper

POINT : TAKEN

EPOS

aztek

Evidi

KPMG

CloudWay

spirhed

Noroff
School of technology
and digital media

blinQ

amesto
Fortytwo

SparebankenVest

IT styring

INNOFACTOR

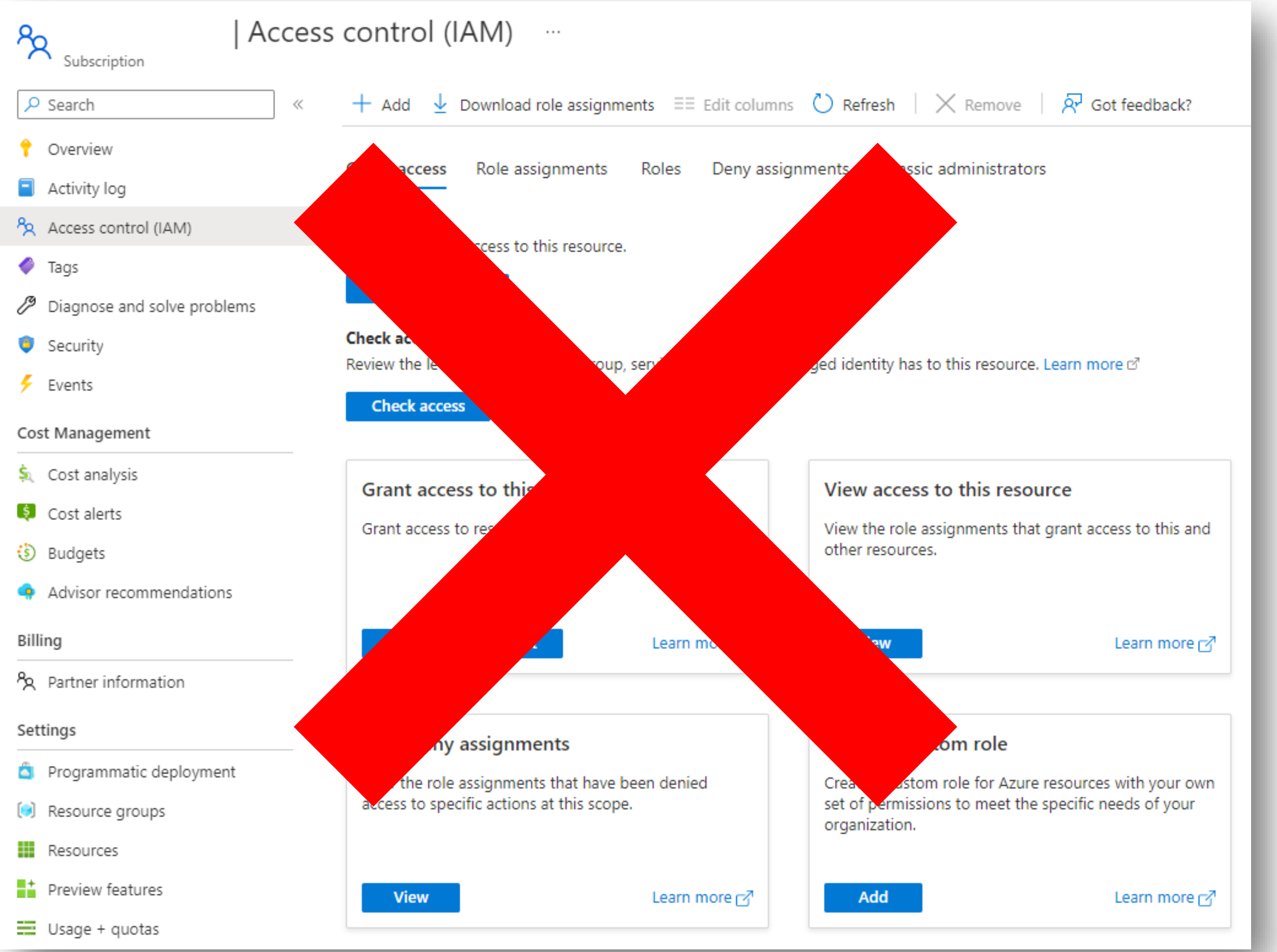
Agenda

- ? Why
- ✓ Getting started
- Setup
- Reporting/Monitoring

Why?

What are PIM?

PIM is NOT!



cess to this resource.

Check ac

Review the le oup, ser ged identity has to this resource. Learn more

Grant access to thi

Grant access to res

View access to this resource

View the role assignments that grant access to this and other resources.

ny assignments

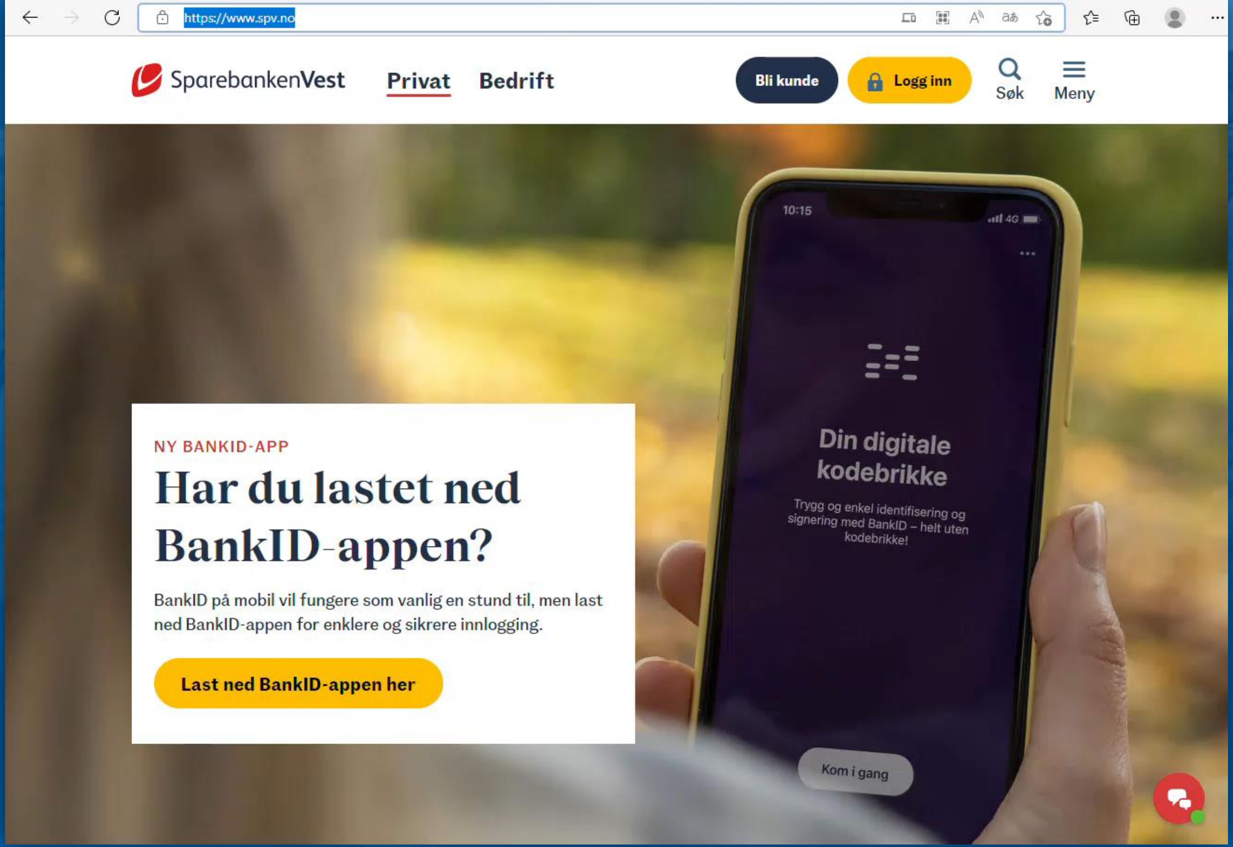
the role assignments that have been denied access to specific actions at this scope.

om role

Crea stom role for Azure resources with your own set of permissions to meet the specific needs of your organization.

DEMO

Activation



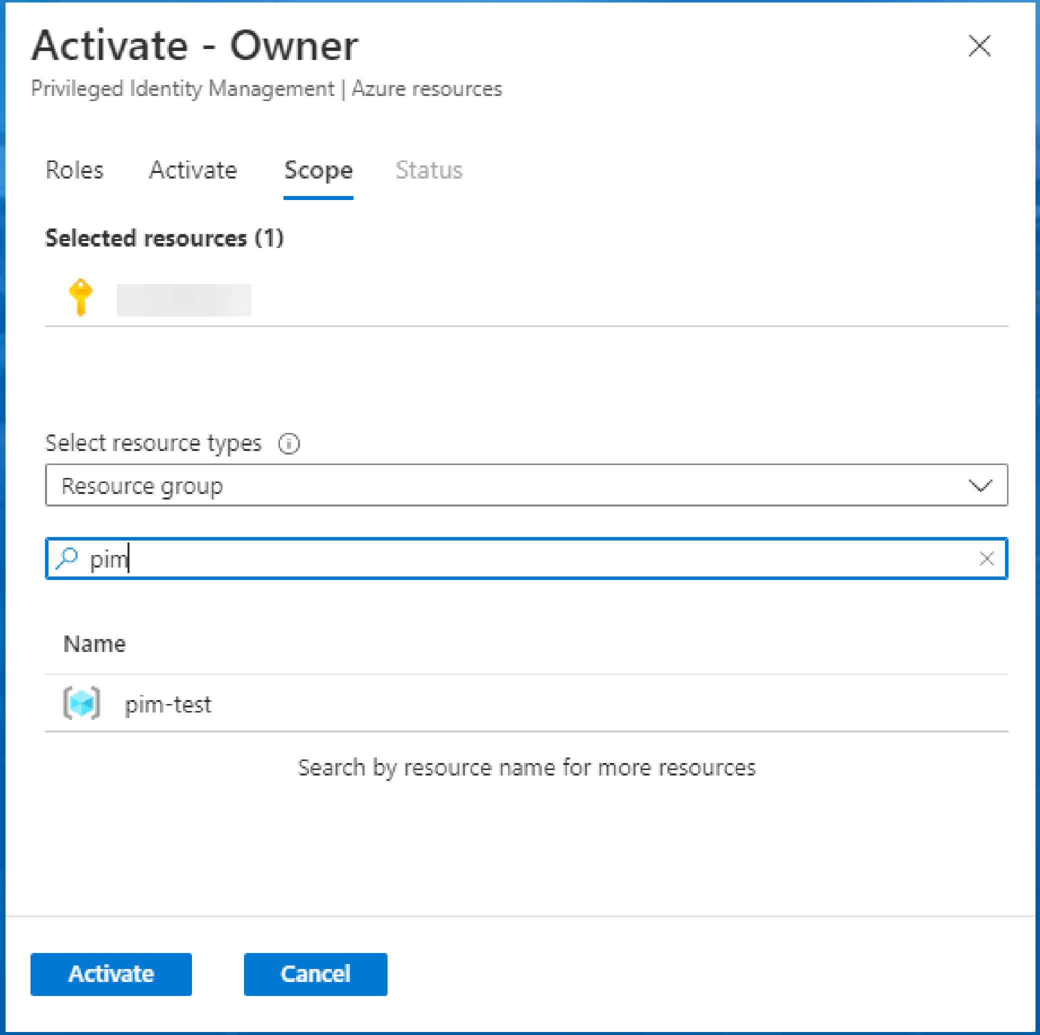
NY BANKID-APP

Har du lastet ned BankID-appen?

BankID på mobil vil fungere som vanlig en stund til, men last ned BankID-appen for enklere og sikrere innlogging.

DEMO

Activation



Activate - Owner

Privileged Identity Management | Azure resources

Roles | Activate | **Scope** | Status

Selected resources (1)

[redacted]

Select resource types ⓘ

Resource group

pim

Name

pim-test

Search by resource name for more resources

Why?

- Prevent:
  - Unauthorized use of escalated permissions
  - Script/malware misuse of escalated permissions
  - User/scripts accidents
- Log escalated role usage and users

	Risko time/week	A year
No PIM	168	7896
8 Hours PIM	40	1880
2 Hours PIM	10	470

Getting started

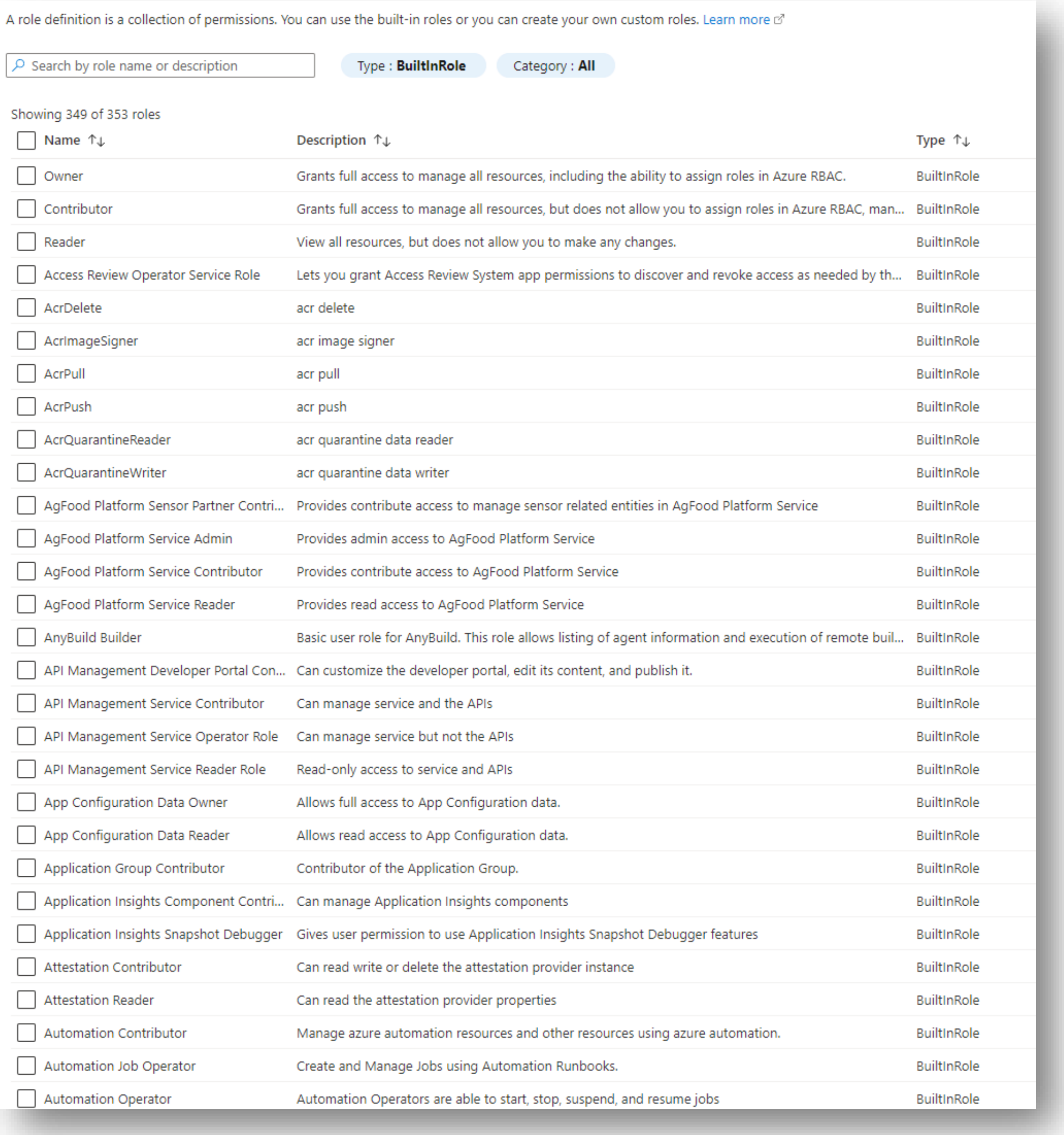
Stats and Scope

15.08.2022

Number of built-in roles 349

Scope:

- Define what roles to protect
- Collect exiting groups and users
- Set allowed length of privileged access



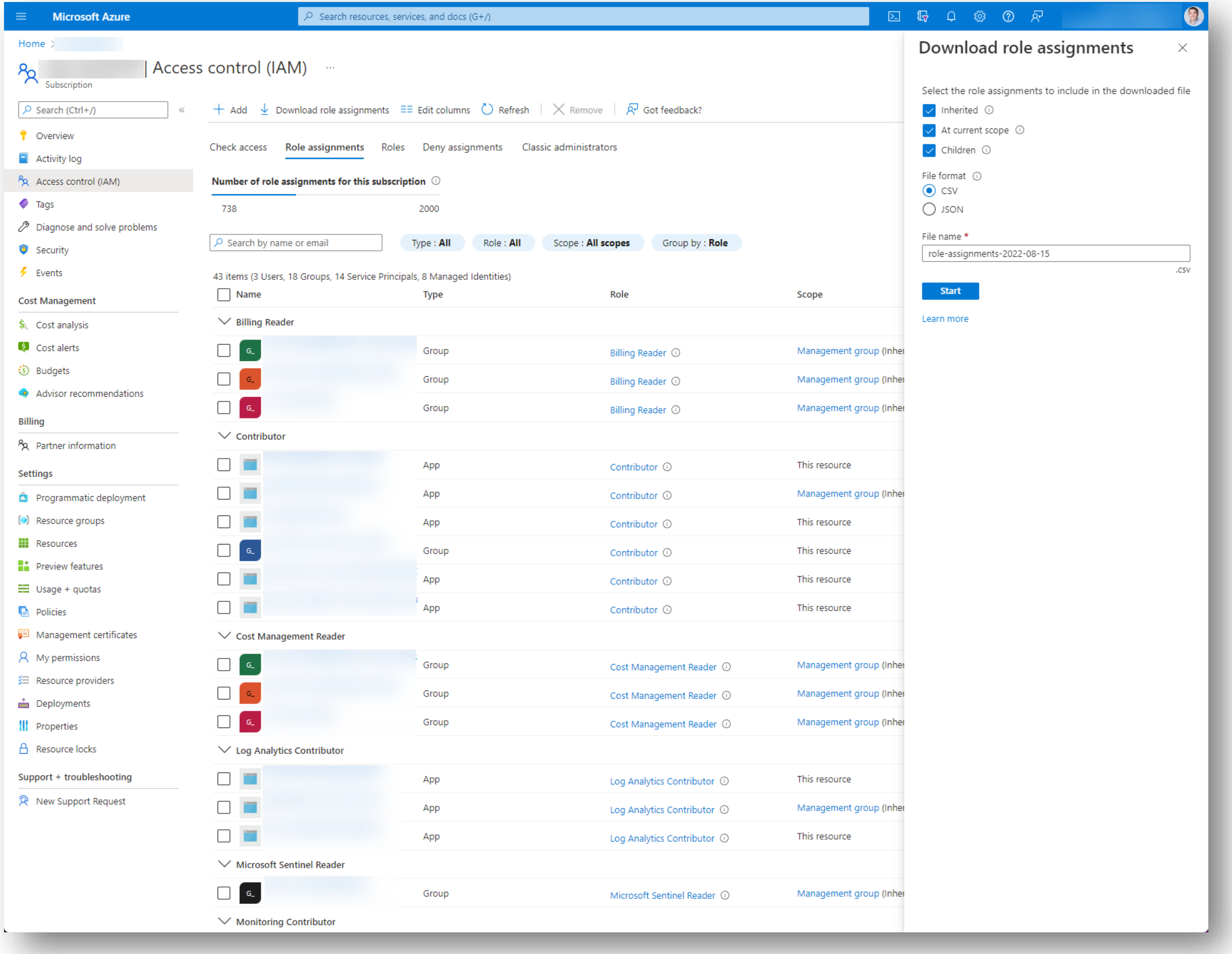
A role definition is a collection of permissions. You can use the built-in roles or you can create your own custom roles. Learn more

Search by role name or description | Type : **BuiltInRole** | Category : **All**

Showing 349 of 353 roles

□	**Name** ↑↓	**Description** ↑↓	**Type** ↑↓
□	Owner	Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.	BuiltInRole
□	Contributor	Grants full access to manage all resources, but does not allow you to assign roles in Azure RBAC, man...	BuiltInRole
□	Reader	View all resources, but does not allow you to make any changes.	BuiltInRole
□	Access Review Operator Service Role	Lets you grant Access Review System app permissions to discover and revoke access as needed by th...	BuiltInRole
□	AcrDelete	acr delete	BuiltInRole
□	AcrImageSigner	acr image signer	BuiltInRole
□	AcrPull	acr pull	BuiltInRole
□	AcrPush	acr push	BuiltInRole
□	AcrQuarantineReader	acr quarantine data reader	BuiltInRole
□	AcrQuarantineWriter	acr quarantine data writer	BuiltInRole
□	AgFood Platform Sensor Partner Contri...	Provides contribute access to manage sensor related entities in AgFood Platform Service	BuiltInRole
□	AgFood Platform Service Admin	Provides admin access to AgFood Platform Service	BuiltInRole
□	AgFood Platform Service Contributor	Provides contribute access to AgFood Platform Service	BuiltInRole
□	AgFood Platform Service Reader	Provides read access to AgFood Platform Service	BuiltInRole
□	AnyBuild Builder	Basic user role for AnyBuild. This role allows listing of agent information and execution of remote buil...	BuiltInRole
□	API Management Developer Portal Con...	Can customize the developer portal, edit its content, and publish it.	BuiltInRole
□	API Management Service Contributor	Can manage service and the APIs	BuiltInRole
□	API Management Service Operator Role	Can manage service but not the APIs	BuiltInRole
□	API Management Service Reader Role	Read-only access to service and APIs	BuiltInRole
□	App Configuration Data Owner	Allows full access to App Configuration data.	BuiltInRole
□	App Configuration Data Reader	Allows read access to App Configuration data.	BuiltInRole
□	Application Group Contributor	Contributor of the Application Group.	BuiltInRole
□	Application Insights Component Contri...	Can manage Application Insights components	BuiltInRole
□	Application Insights Snapshot Debugger	Gives user permission to use Application Insights Snapshot Debugger features	BuiltInRole
□	Attestation Contributor	Can read write or delete the attestation provider instance	BuiltInRole
□	Attestation Reader	Can read the attestation provider properties	BuiltInRole
□	Automation Contributor	Manage azure automation resources and other resources using azure automation.	BuiltInRole
□	Automation Job Operator	Create and Manage Jobs using Automation Runbooks.	BuiltInRole
□	Automation Operator	Automation Operators are able to start, stop, suspend, and resume jobs	BuiltInRole

Portal Way



[redacted] | Access control (IAM) ···
Subscription

Number of role assignments for this subscription ⓘ

738 2000

Search by name or email

Type : **All** Role : **All** Scope : **All scopes** Group by : **Role**

43 items (3 Users, 18 Groups, 14 Service Principals, 8 Managed Identities)

□ Name	Type	Role	Scope
Billing Reader			
□ [redacted]	Group	Billing Reader ⓘ	Management group (Inher
□ [redacted]	Group	Billing Reader ⓘ	Management group (Inher
□ [redacted]	Group	Billing Reader ⓘ	Management group (Inher
Contributor			
□ [redacted]	App	Contributor ⓘ	This resource
□ [redacted]	App	Contributor ⓘ	Management group (Inher
□ [redacted]	App	Contributor ⓘ	This resource
□ [redacted]	Group	Contributor ⓘ	This resource
□ [redacted]	App	Contributor ⓘ	This resource
□ [redacted]	App	Contributor ⓘ	This resource
Cost Management Reader			
□ [redacted]	Group	Cost Management Reader ⓘ	Management group (Inher
□ [redacted]	Group	Cost Management Reader ⓘ	Management group (Inher
□ [redacted]	Group	Cost Management Reader ⓘ	Management group (Inher
Log Analytics Contributor			
□ [redacted]	App	Log Analytics Contributor ⓘ	This resource
□ [redacted]	App	Log Analytics Contributor ⓘ	Management group (Inher
□ [redacted]	App	Log Analytics Contributor ⓘ	This resource
Microsoft Sentinel Reader			
□ [redacted]	Group	Microsoft Sentinel Reader ⓘ	Management group (Inher
Monitoring Contributor			

Download role assignments

Select the role assignments to include in the downloaded file

☑ Inherited ⓘ

☑ At current scope ⓘ

☑ Children ⓘ

File format ⓘ

● CSV

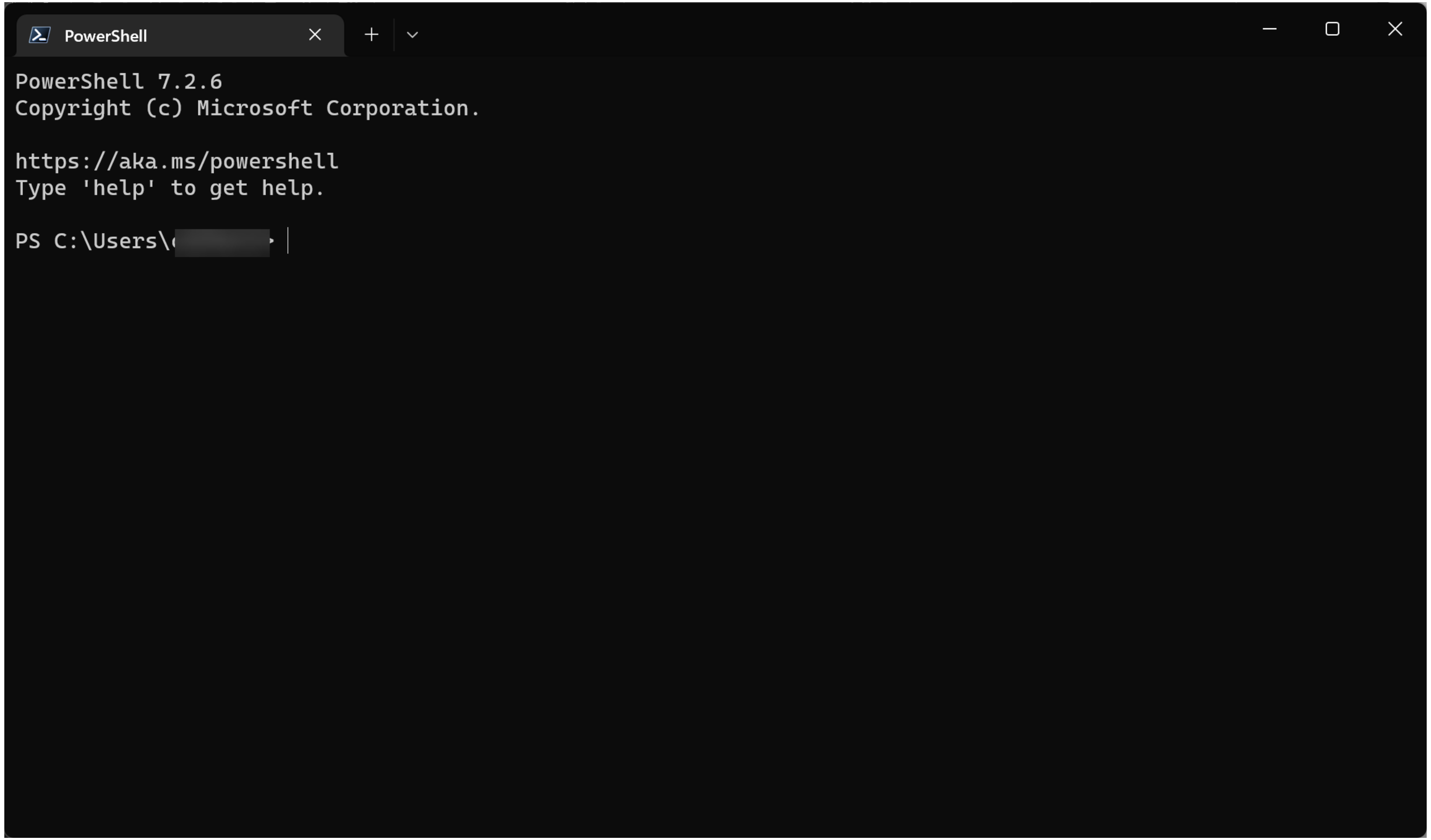
○ JSON

File name *

role-assignments-2022-08-15 .csv

MVP-Dagen

The Right Way



```
PowerShell 7.2.6
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.

PS C:\Users\[redacted]
```

Roles in use

```
Get-AzRoleAssignment | Select RoleDefinitionName | Sort-Object * | select * -Unique
```

Remember: Set-AzContext -SubscriptionName <your subscription>

Get info about user

Get-AzRoleAssignment -SignInName <your@user.com> -ExpandPrincipalGroups | select DisplayName, RoleDefinitionName, Scope

Remember: Set-AzContext -SubscriptionName <your subscription>

Get info about a group

$Group01 = Get-AzureADGroup -SearchString “<Group you are searching for>“
(Or use –Filter)

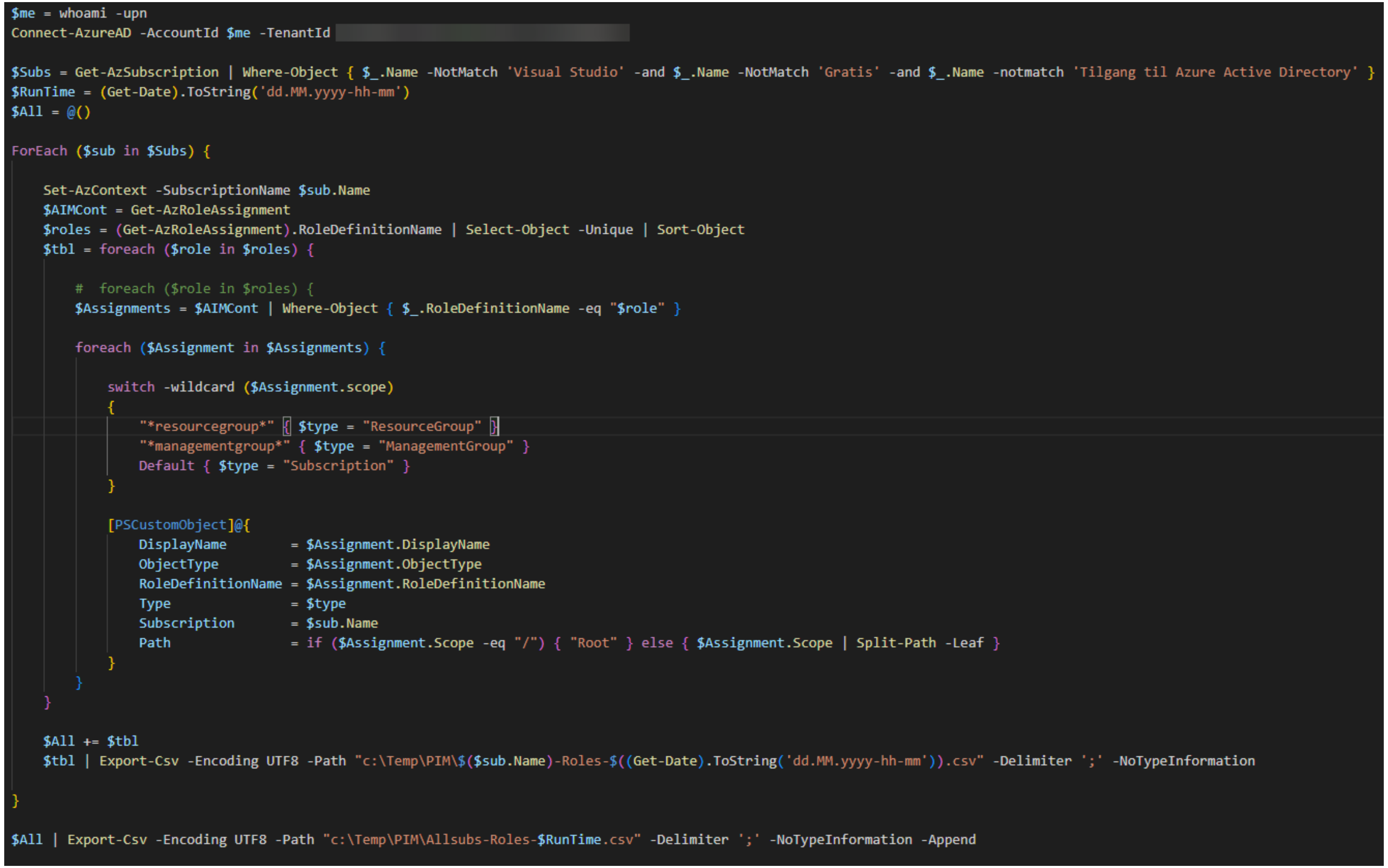
Get-AzRoleAssignment -ObjectId $Group01.ObjectId |
select DisplayName, RoleDefinitionName, Scope | fl

Remember: Set-AzContext -SubscriptionName <your subscription>

DEMO

PowerShell

Script



```
$me = whoami -upn
Connect-AzureAD -AccountId $me -TenantId [redacted]

$Subs = Get-AzSubscription | Where-Object { $_.Name -NotMatch 'Visual Studio' -and $_.Name -NotMatch 'Gratis' -and $_.Name -notmatch 'Tilgang til Azure Active Directory' }
$RunTime = (Get-Date).ToString('dd.MM.yyyy-hh-mm')
$All = @()

ForEach ($sub in $Subs) {

    Set-AzContext -SubscriptionName $sub.Name
    $AIMCont = Get-AzRoleAssignment
    $roles = (Get-AzRoleAssignment).RoleDefinitionName | Select-Object -Unique | Sort-Object
    $tbl = foreach ($role in $roles) {

        #  foreach ($role in $roles) {
        $Assignments = $AIMCont | Where-Object { $_.RoleDefinitionName -eq "$role" }

        foreach ($Assignment in $Assignments) {

            switch -wildcard ($Assignment.scope)
            {
                "*resourcegroup*" { $type = "ResourceGroup" }
                "*managementgroup*" { $type = "ManagementGroup" }
                Default { $type = "Subscription" }
            }

            [PSCustomObject]@{
                DisplayName        = $Assignment.DisplayName
                ObjectType         = $Assignment.ObjectType
                RoleDefinitionName = $Assignment.RoleDefinitionName
                Type               = $type
                Subscription       = $sub.Name
                Path               = if ($Assignment.Scope -eq "/") { "Root" } else { $Assignment.Scope | Split-Path -Leaf }
            }
        }
    }

    $All += $tbl
    $tbl | Export-Csv -Encoding UTF8 -Path "c:\Temp\PIM\$($sub.Name)-Roles-$((Get-Date).ToString('dd.MM.yyyy-hh-mm')).csv" -Delimiter ';' -NoTypeInformation

}

$All | Export-Csv -Encoding UTF8 -Path "c:\Temp\PIM\Allsubs-Roles-$RunTime.csv" -Delimiter ';' -NoTypeInformation -Append
```

https://github.com/OTvedt/Scripts-For-Sharing/blob/master/Azure/PIM/Azure-resources/

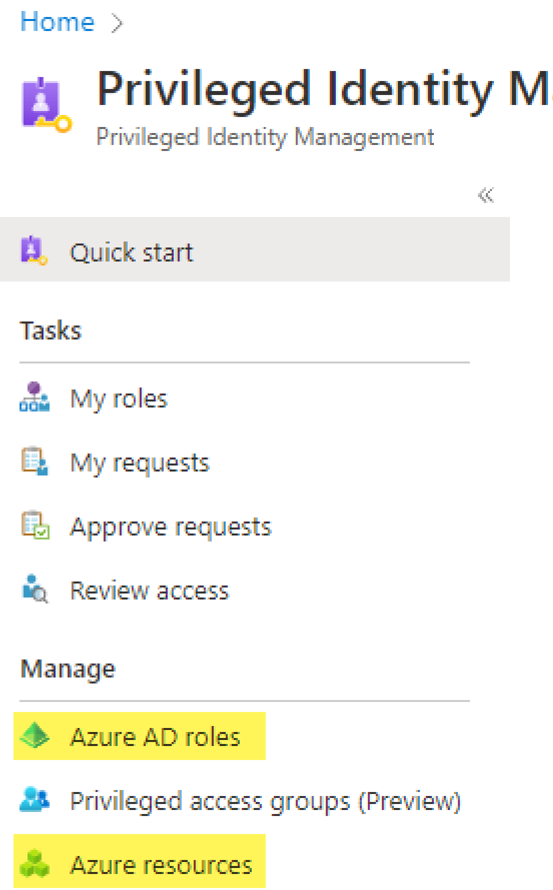
DEMO

Excel

Setup

Prepare the users / Support

Difference Between Azure AD Roles and Azure Resources



Home >

Privileged Identity Management

Privileged Identity Management

Quick start

Tasks

My roles

My requests

Approve requests

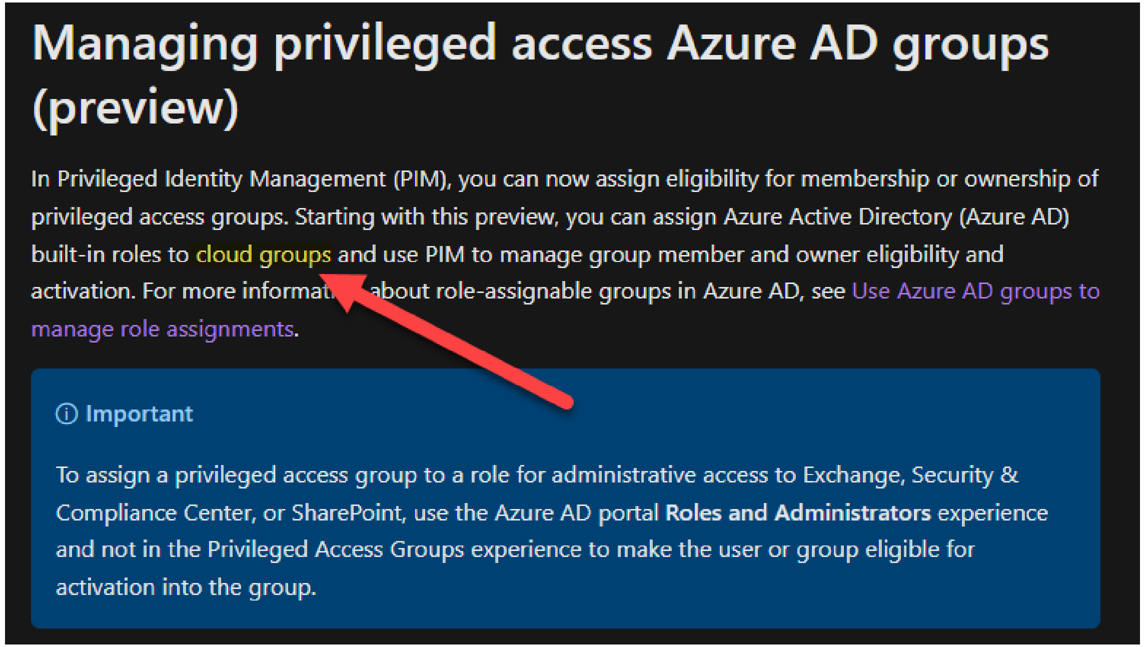
Review access

Manage

Azure AD roles

Privileged access groups (Preview)

Azure resources



Managing privileged access Azure AD groups (preview)

In Privileged Identity Management (PIM), you can now assign eligibility for membership or ownership of privileged access groups. Starting with this preview, you can assign Azure Active Directory (Azure AD) built-in roles to cloud groups and use PIM to manage group member and owner eligibility and activation. For more information about role-assignable groups in Azure AD, see Use Azure AD groups to manage role assignments.

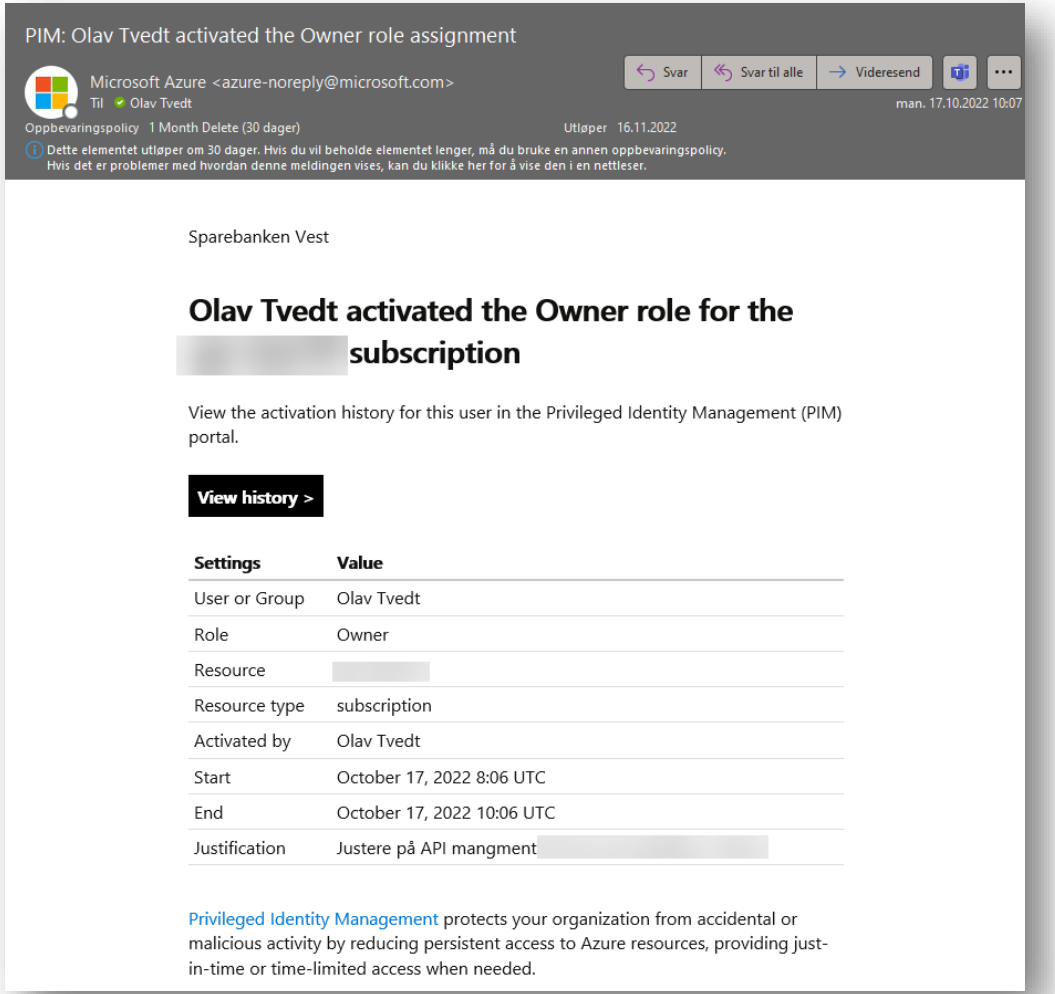
ⓘ Important

To assign a privileged access group to a role for administrative access to Exchange, Security & Compliance Center, or SharePoint, use the Azure AD portal **Roles and Administrators** experience and not in the Privileged Access Groups experience to make the user or group eligible for activation into the group.

DEMO

Setup

Reporting
/
Monitoring



PIM: Olav Tvedt activated the Owner role assignment

Microsoft Azure <azure-noreply@microsoft.com>
Til Olav Tvedt
man. 17.10.2022 10:07

Oppbevaringspolicy 1 Month Delete (30 dager) Utløper 16.11.2022

Dette elementet utløper om 30 dager. Hvis du vil beholde elementet lenger, må du bruke en annen oppbevaringspolicy.
Hvis det er problemer med hvordan denne meldingen vises, kan du klikke her for å vise den i en nettleser.

Sparebanken Vest

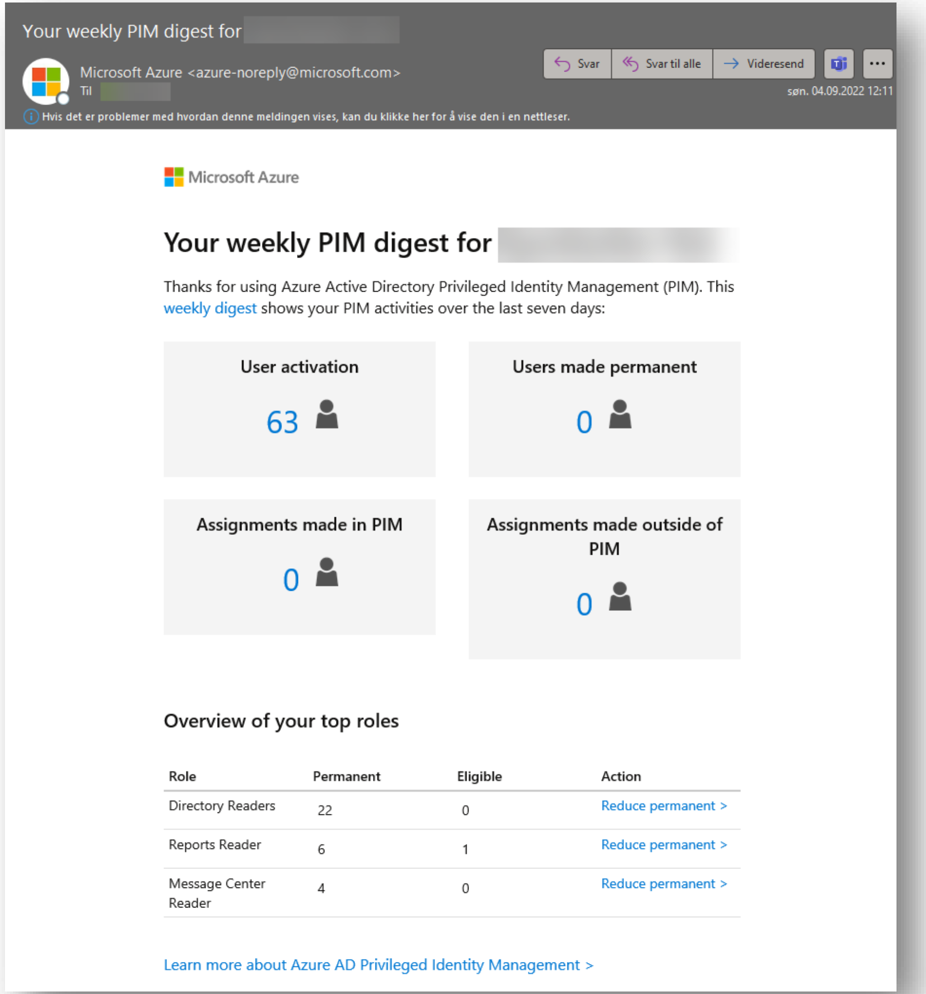
Olav Tvedt activated the Owner role for the [redacted] subscription

View the activation history for this user in the Privileged Identity Management (PIM) portal.

View history >

Settings	Value
User or Group	Olav Tvedt
Role	Owner
Resource	[redacted]
Resource type	subscription
Activated by	Olav Tvedt
Start	October 17, 2022 8:06 UTC
End	October 17, 2022 10:06 UTC
Justification	Justere på API mangment [redacted]

Privileged Identity Management protects your organization from accidental or malicious activity by reducing persistent access to Azure resources, providing just-in-time or time-limited access when needed.



Your weekly PIM digest for [redacted]

Microsoft Azure <azure-noreply@microsoft.com>
Til [redacted]
søn. 04.09.2022 12:11

Hvis det er problemer med hvordan denne meldingen vises, kan du klikke her for å vise den i en nettleser.

Microsoft Azure

Your weekly PIM digest for [redacted]

Thanks for using Azure Active Directory Privileged Identity Management (PIM). This weekly digest shows your PIM activities over the last seven days:

User activation	Users made permanent
63	0

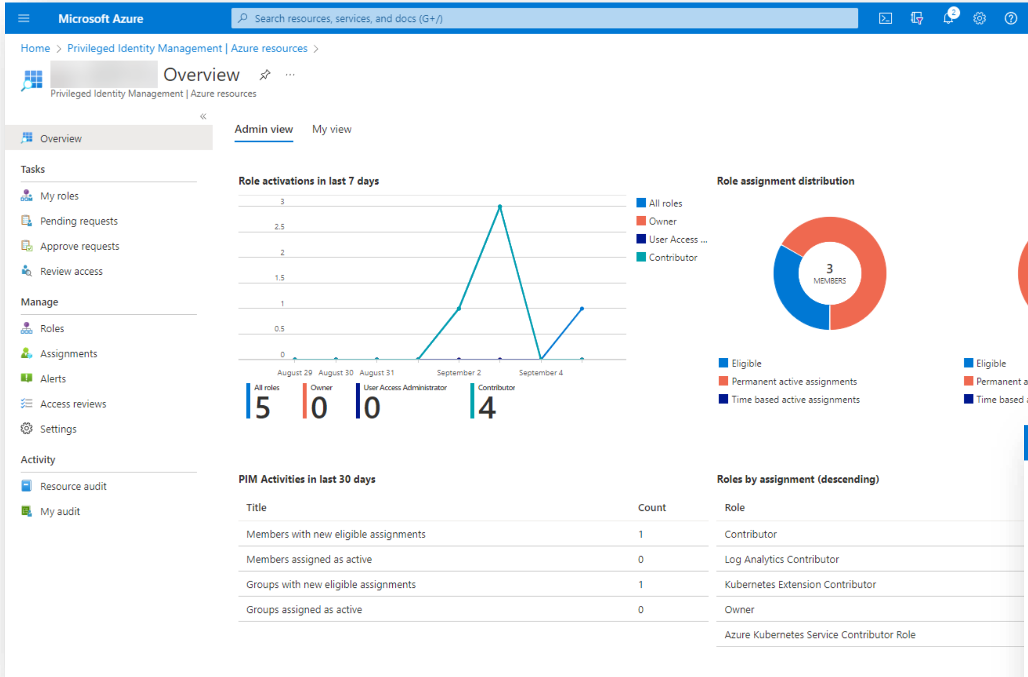
Assignments made in PIM	Assignments made outside of PIM
0	0

Overview of your top roles

Role	Permanent	Eligible	Action
Directory Readers	22	0	Reduce permanent >
Reports Reader	6	1	Reduce permanent >
Message Center Reader	4	0	Reduce permanent >

Learn more about Azure AD Privileged Identity Management >

MVP-Dagen

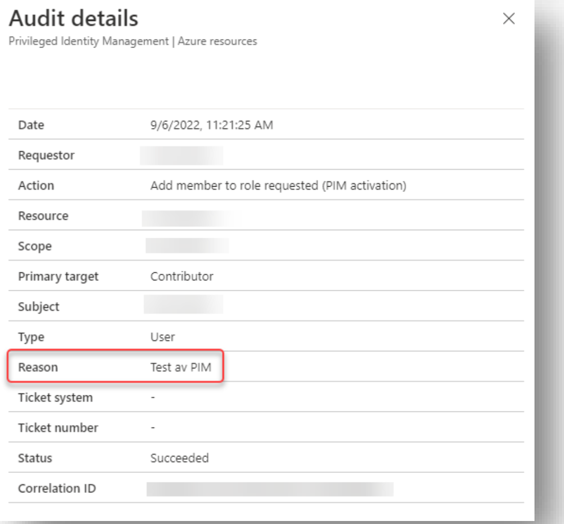


PIM Activities in last 30 days

Title	Count
Members with new eligible assignments	1
Members assigned as active	0
Groups with new eligible assignments	1
Groups assigned as active	0

Roles by assignment (descending)

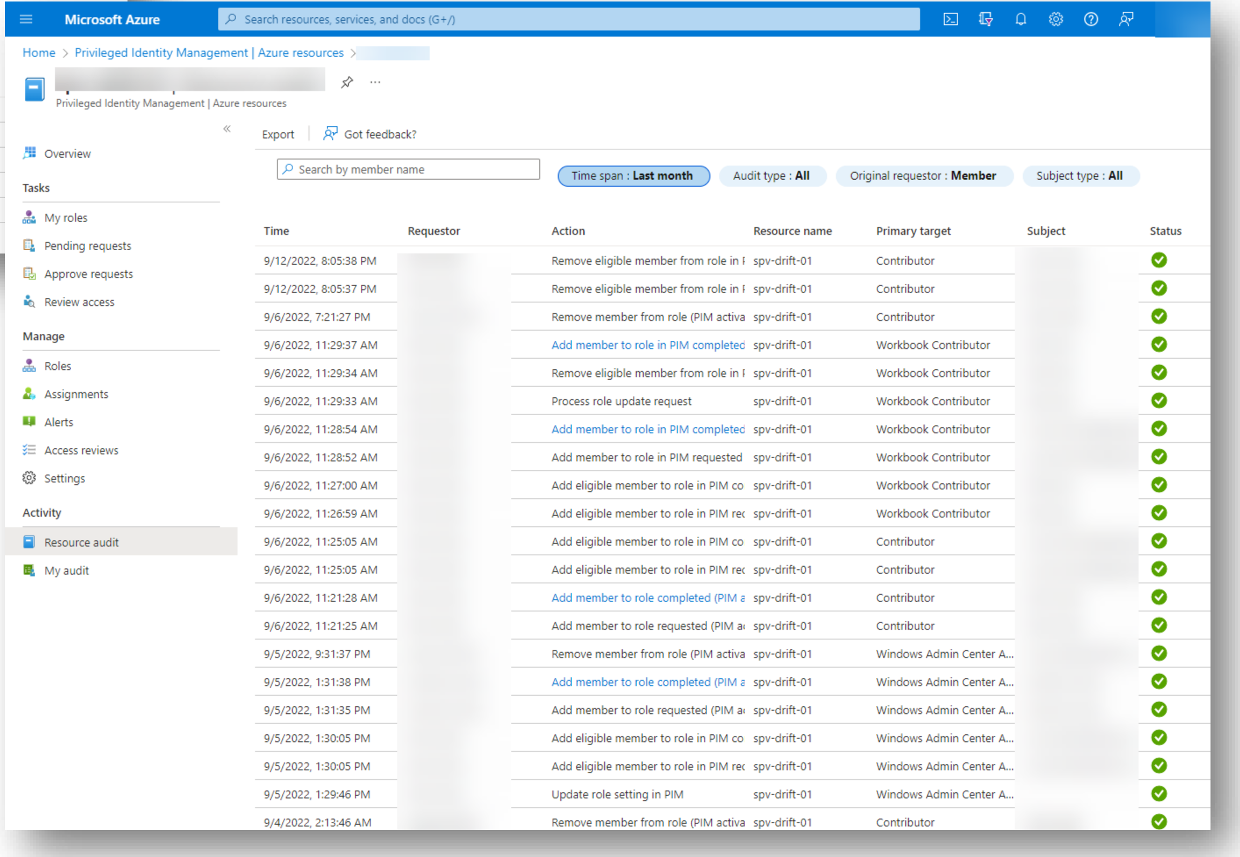
Role
Contributor
Log Analytics Contributor
Kubernetes Extension Contributor
Owner
Azure Kubernetes Service Contributor Role



Audit details

Privileged Identity Management | Azure resources

Date	9/6/2022, 11:21:25 AM
Requestor	[redacted]
Action	Add member to role requested (PIM activation)
Resource	[redacted]
Scope	[redacted]
Primary target	Contributor
Subject	[redacted]
Type	User
Reason	Test av PIM
Ticket system	-
Ticket number	-
Status	Succeeded
Correlation ID	[redacted]

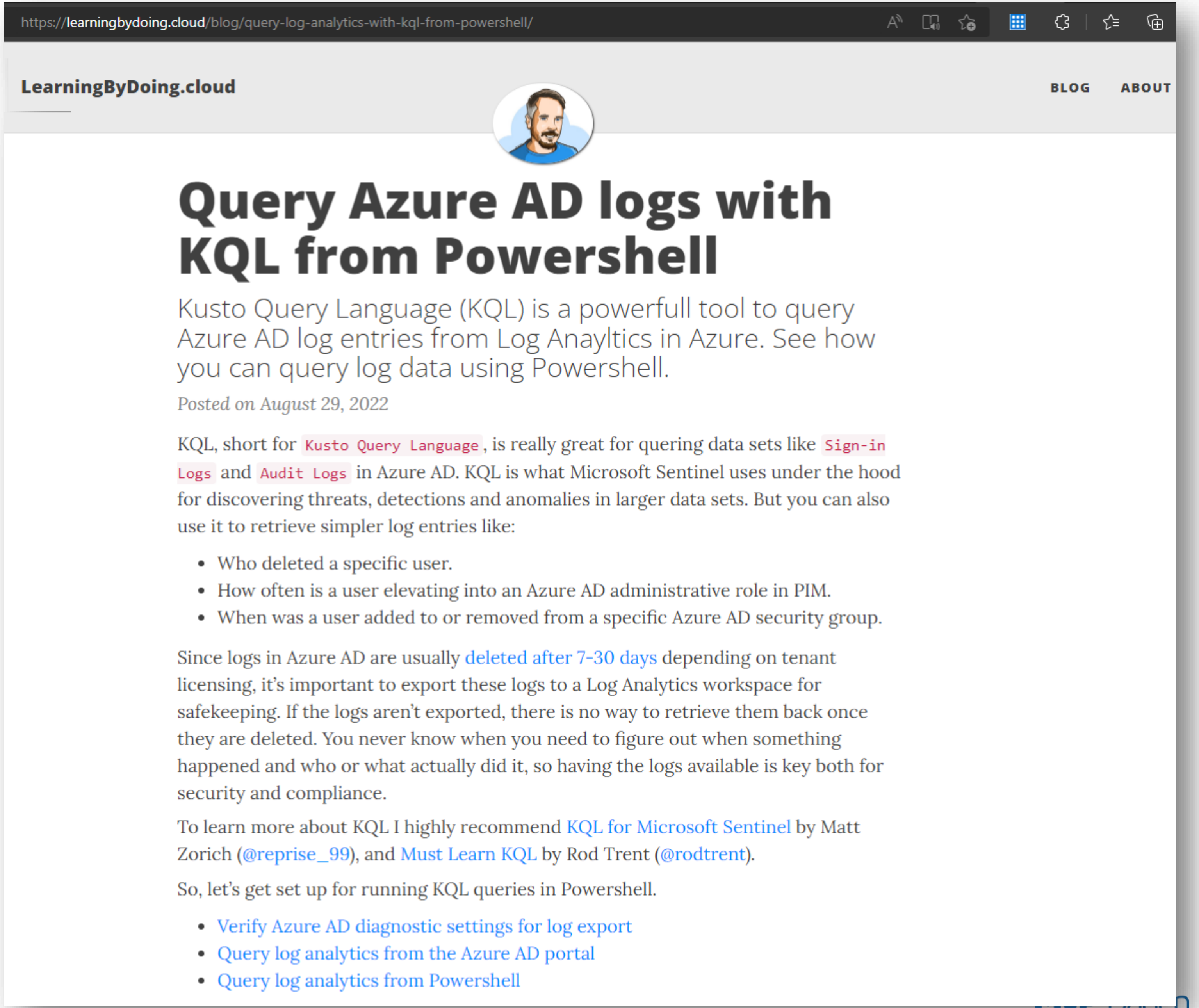


Time span : **Last month** Audit type : **All** Original requestor : **Member** Subject type : **All**

Time	Requestor	Action	Resource name	Primary target	Subject	Status
9/12/2022, 8:05:38 PM	[redacted]	Remove eligible member from role in I	spv-drift-01	Contributor	[redacted]	✓
9/12/2022, 8:05:37 PM	[redacted]	Remove eligible member from role in I	spv-drift-01	Contributor	[redacted]	✓
9/6/2022, 7:21:27 PM	[redacted]	Remove member from role (PIM activa	spv-drift-01	Contributor	[redacted]	✓
9/6/2022, 11:29:37 AM	[redacted]	Add member to role in PIM completed	spv-drift-01	Workbook Contributor	[redacted]	✓
9/6/2022, 11:29:34 AM	[redacted]	Remove eligible member from role in I	spv-drift-01	Workbook Contributor	[redacted]	✓
9/6/2022, 11:29:33 AM	[redacted]	Process role update request	spv-drift-01	Workbook Contributor	[redacted]	✓
9/6/2022, 11:28:54 AM	[redacted]	Add member to role in PIM completed	spv-drift-01	Workbook Contributor	[redacted]	✓
9/6/2022, 11:28:52 AM	[redacted]	Add member to role in PIM requested	spv-drift-01	Workbook Contributor	[redacted]	✓
9/6/2022, 11:27:00 AM	[redacted]	Add eligible member to role in PIM co	spv-drift-01	Workbook Contributor	[redacted]	✓
9/6/2022, 11:26:59 AM	[redacted]	Add eligible member to role in PIM rec	spv-drift-01	Workbook Contributor	[redacted]	✓
9/6/2022, 11:25:05 AM	[redacted]	Add eligible member to role in PIM co	spv-drift-01	Contributor	[redacted]	✓
9/6/2022, 11:25:05 AM	[redacted]	Add eligible member to role in PIM rec	spv-drift-01	Contributor	[redacted]	✓
9/6/2022, 11:21:28 AM	[redacted]	Add member to role completed (PIM a	spv-drift-01	Contributor	[redacted]	✓
9/6/2022, 11:21:25 AM	[redacted]	Add member to role requested (PIM a	spv-drift-01	Contributor	[redacted]	✓
9/5/2022, 9:31:37 PM	[redacted]	Remove member from role (PIM activa	spv-drift-01	Windows Admin Center A...	[redacted]	✓
9/5/2022, 1:31:38 PM	[redacted]	Add member to role completed (PIM a	spv-drift-01	Windows Admin Center A...	[redacted]	✓
9/5/2022, 1:31:35 PM	[redacted]	Add member to role requested (PIM a	spv-drift-01	Windows Admin Center A...	[redacted]	✓
9/5/2022, 1:30:05 PM	[redacted]	Add eligible member to role in PIM co	spv-drift-01	Windows Admin Center A...	[redacted]	✓
9/5/2022, 1:30:05 PM	[redacted]	Add eligible member to role in PIM rec	spv-drift-01	Windows Admin Center A...	[redacted]	✓
9/5/2022, 1:29:46 PM	[redacted]	Update role setting in PIM	spv-drift-01	Windows Admin Center A...	[redacted]	✓
9/4/2022, 2:13:46 AM	[redacted]	Remove member from role (PIM activa	spv-drift-01	Contributor	[redacted]	✓

https://learningbydoing.cloud

https://learningbydoing.cloud/blog/query-log-analytics-with-kql-from-powershell/



https://learningbydoing.cloud/blog/query-log-analytics-with-kql-from-powershell/
LearningByDoing.cloud
BLOG
ABOUT

Query Azure AD logs with KQL from Powershell

Kusto Query Language (KQL) is a powerfull tool to query Azure AD log entries from Log Anayltics in Azure. See how you can query log data using Powershell.

Posted on August 29, 2022

KQL, short for `Kusto Query Language`, is really great for quering data sets like `Sign-in Logs` and `Audit Logs` in Azure AD. KQL is what Microsoft Sentinel uses under the hood for discovering threats, detections and anomalies in larger data sets. But you can also use it to retrieve simpler log entries like:

- Who deleted a specific user.
- How often is a user elevating into an Azure AD administrative role in PIM.
- When was a user added to or removed from a specific Azure AD security group.

Since logs in Azure AD are usually deleted after 7-30 days depending on tenant licensing, it's important to export these logs to a Log Analytics workspace for safekeeping. If the logs aren't exported, there is no way to retrieve them back once they are deleted. You never know when you need to figure out when something happened and who or what actually did it, so having the logs available is key both for security and compliance.

To learn more about KQL I highly recommend KQL for Microsoft Sentinel by Matt Zorich (@reprise_99), and Must Learn KQL by Rod Trent (@rodtrent).

So, let's get set up for running KQL queries in Powershell.

- Verify Azure AD diagnostic settings for log export
- Query log analytics from the Azure AD portal
- Query log analytics from Powershell

Olav Tvedt

SparebankenVest

We recognize and value your exceptional contributions to technical communities worldwide
15 Years
10 Years
5 Years
MVP
Microsoft Most Valuable Professional

https://bit.ly/blueScreenTube

Twitter: @olavtwitt

LinkedIn: https://www.linkedin.com/in/otvedt

Podkast: BlåSkjerm Brødrende

Takk til våre sponsorer

Microsoft

audiocodes

glasspaper

POINT : TAKEN

EPOS

aztek

Evidi

KPMG

CloudWay

spirhed

Noroff
School of technology
and digital media

blinQ

amesto
Fortytwo

SparebankenVest

IT styring

INNOFACTOR

Tusen takk!

MVP-Dagen