I am THE VIP

mvpdagen.no

SparebankenVest

Takk til våre sponsorer

mvpdagen.no

SparebankenVest

Olav Tvedt

SparebankenVest

- x17 – Cloud Security
- youtube.com/@bluescreenbrothers
- /in/otvedt
- olavtwitt

MVP Dagen

SparebankenVest

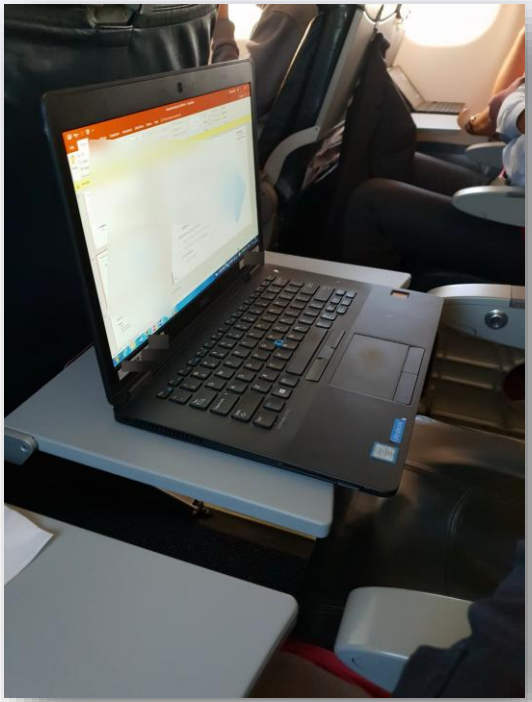
VIP

Person, Privileges eller Permission

MVP Dagen

SparebankenVest

Hvem er brukerne dine i dag?



MI

Manglende Intelligens

Hvem er brukerne dine i dag?

- Vanlig?
- Utvidet?
- Admin?

Hvem er du i dag?

Olav?
DemOlav?
Sky Admin Olav?
Legacy Admin Olav?
All of the above?

JEA / Roller

Hvorfor og hvordan

MVP Dagen

SparebankenVest

Customized or Built-in, spiller det noen rolle(r)?

112

611

MVP Dagen

SparebankenVest

Azure Resources – Default Owner


```
{
  "assignableScopes": [
    "/"
  ],
  "description": "Grants full access to manage all resources, including the ability to assign roles in Azure RBAC.",
  "id": "/providers/Microsoft.Authorization/roleDefinitions/8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
  "name": "8e3af657-a8ff-443c-a75c-2fe8c4bcb635",
  "permissions": [
    {
      "actions": [
        "*"
      ],
      "notActions": [],
      "dataActions": [],
      "notDataActions": []
    }
  ],
  "roleName": "Owner",
  "roleType": "BuiltInRole",
  "type": "Microsoft.Authorization/roleDefinitions"
}
```


MVP Dagen

SparebankenVest

Azure Resources – Default Contributor


```
{
  "assignableScopes": [
    "/"
  ],
  "description": "Grants full access to manage all resources,but does not allow you to assign roles in Azure RBAC, manage assignments in Azure Blueprints, or share image galleries.",
  "id": "/providers/Microsoft.Authorization/roleDefinitions/b24988ac-6180-42a0-ab88-20f7382dd24c",
  "name": "b24988ac-6180-42a0-ab88-20f7382dd24c",
  "permissions": [
    {
      "actions": [
        "*"
      ],
      "notActions": [
        "Microsoft.Authorization/*/Delete",
        "Microsoft.Authorization/*/Write",
        "Microsoft.Authorization/elevateAccess/Action",
        "Microsoft.Blueprint/blueprintAssignments/write",
        "Microsoft.Blueprint/blueprintAssignments/delete",
        "Microsoft.Compute/galleries/share/action",
        "Microsoft.Purview/consents/write",
        "Microsoft.Purview/consents/delete"
      ],
      "dataActions": [],
      "notDataActions": []
    }
  ],
  "roleName": "Contributor",
  "roleType": "BuiltInRole",
  "type": "Microsoft.Authorization/roleDefinitions"
}
```

Mine «notActions» for de fleste Owners

```
"notActions": [
                "Microsoft.Purview/consents/write",
                "Microsoft.Purview/consents/delete",
                "Microsoft.Network/virtualNetworks/write",
                "Microsoft.Network/virtualNetworks/delete",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/write",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/delete",
                “Microsoft.network/vpngateways/*",
                "Microsoft.Network/azurefirewalls/*",
                "Microsoft.Network/expressRouteCircuits/*",
                "Microsoft.Network/vpnsites/*"
                 ],
```

MVP Dagen

SparebankenVest

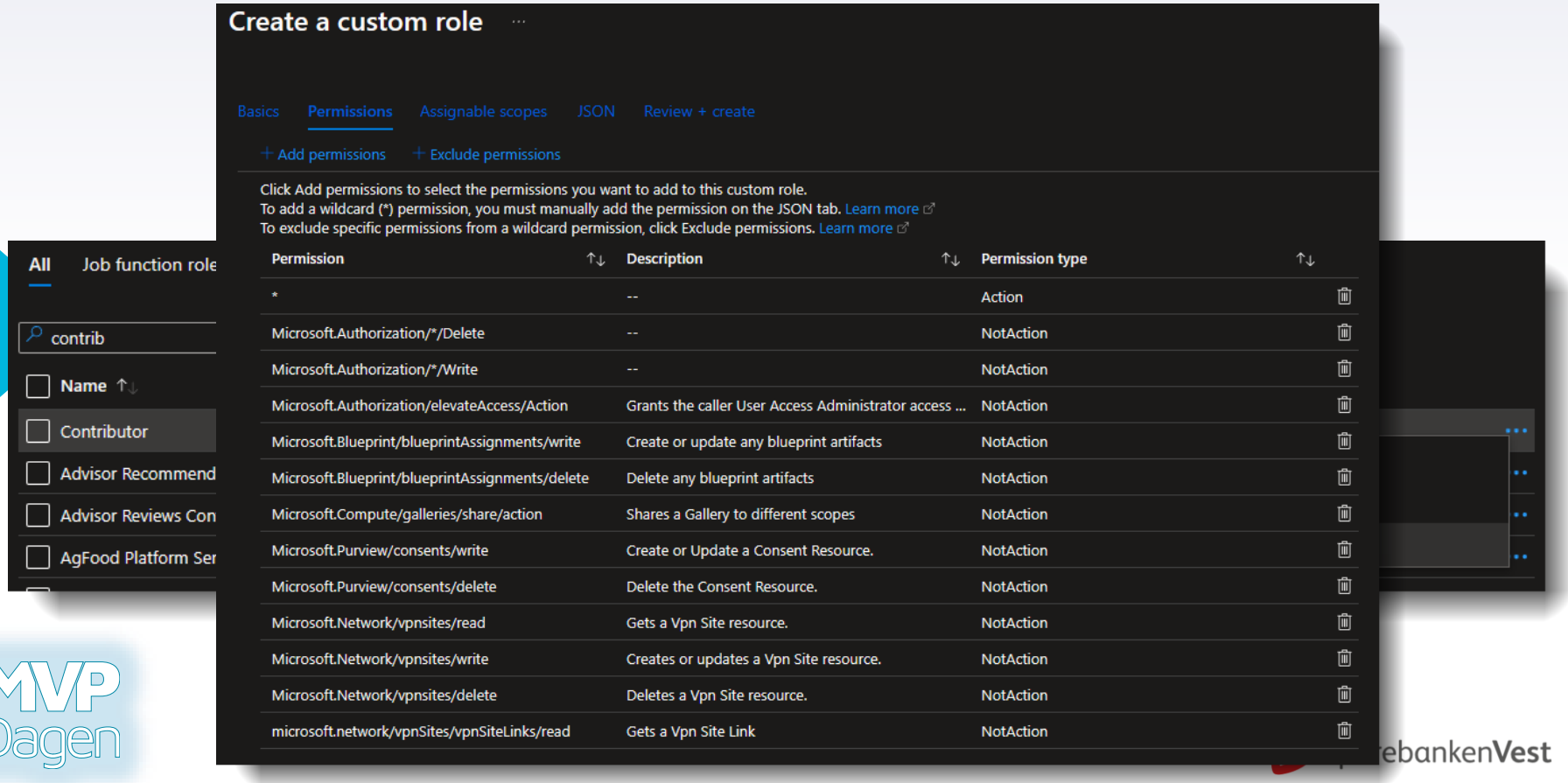
Mine «notActions» for Contributor

```
"notActions": [
                “Microsoft.Authorization/*/Delete",
                "Microsoft.Authorization/*/Write",
                 "Microsoft.Authorization/elevateAccess/Action",
                "Microsoft.Blueprint/blueprintAssignments/write",
                "Microsoft.Blueprint/blueprintAssignments/delete",
                "Microsoft.Compute/galleries/share/action",
                "Microsoft.Purview/consents/write",
                "Microsoft.Purview/consents/delete",
                "Microsoft.Network/virtualNetworks/write",
                "Microsoft.Network/virtualNetworks/delete",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/write",
                "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/delete",
                “Microsoft.network/vpngateways/*",
                "Microsoft.Network/azurefirewalls/*",
                "Microsoft.Network/expressRouteCircuits/*",
                "Microsoft.Network/vpnsites/*"
                 ],
```

MVP Dagen

SparebankenVest

Customizing the Portal way



MVP Dagen

ebankenVest

The missing «*»

```
Get-AzRoleDefinition Contributor | ConvertTo-Json
New-AzRoleDefinition -InputFile "C:\CustomRoles\Contributor-NoNetwork.json"
```

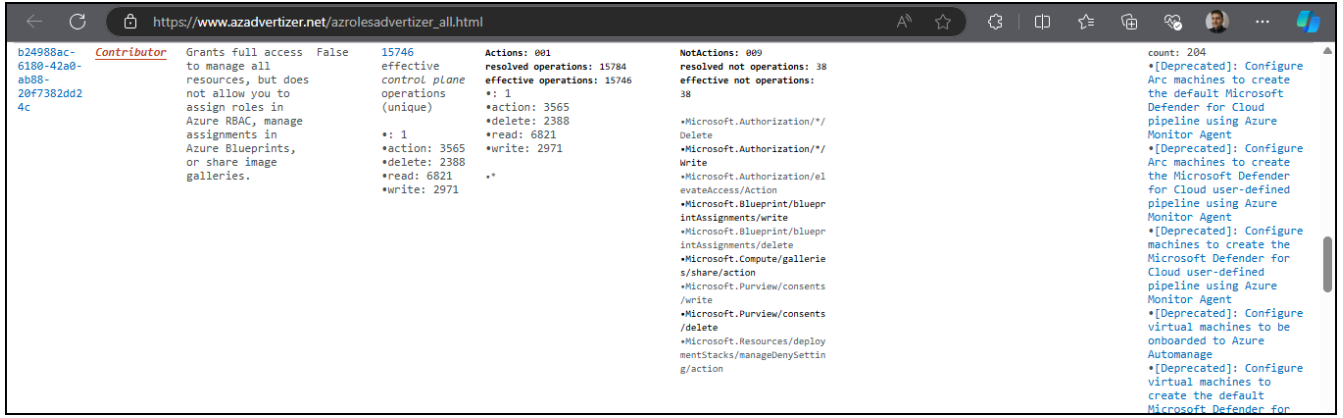
https://learn.microsoft.com/en-us/azure/role-based-access-control/custom-roles

MVP Dagen

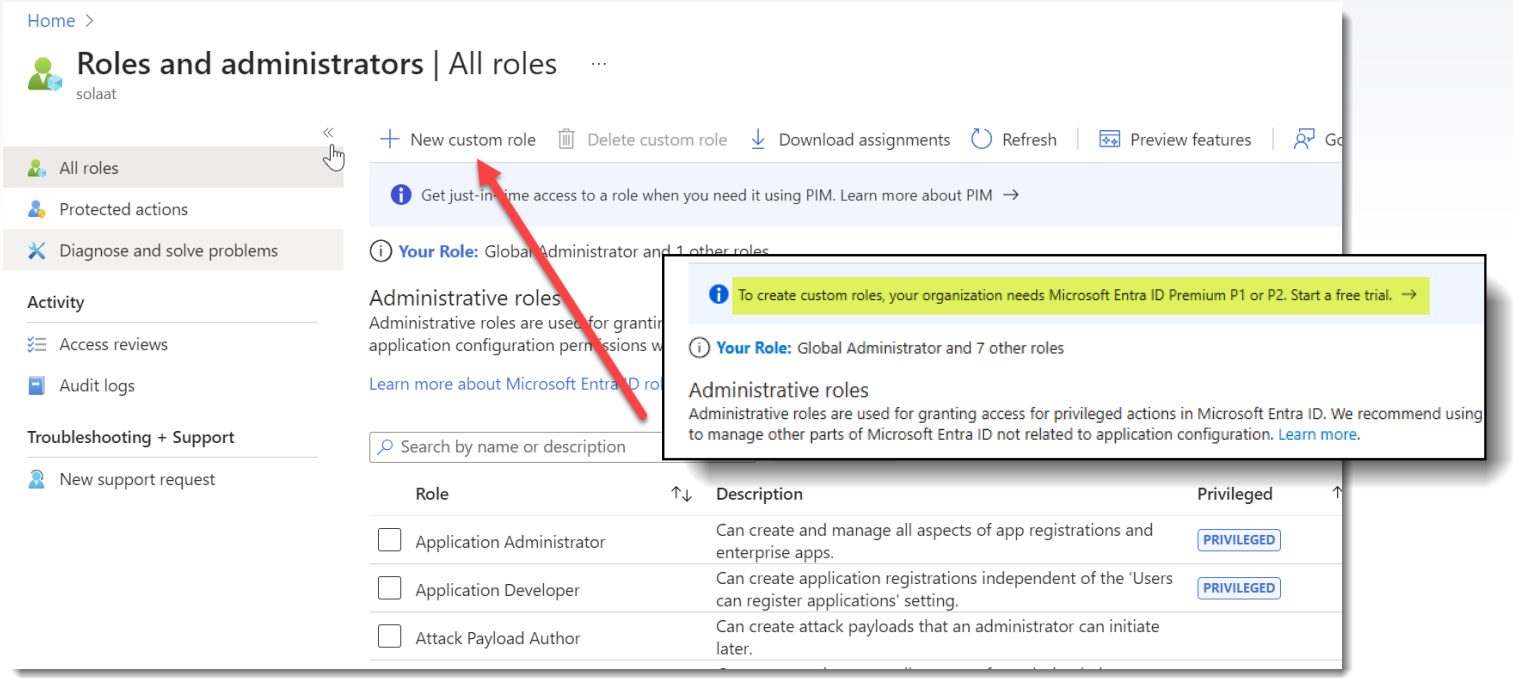
SparebankenVest

Hjelpemiddel

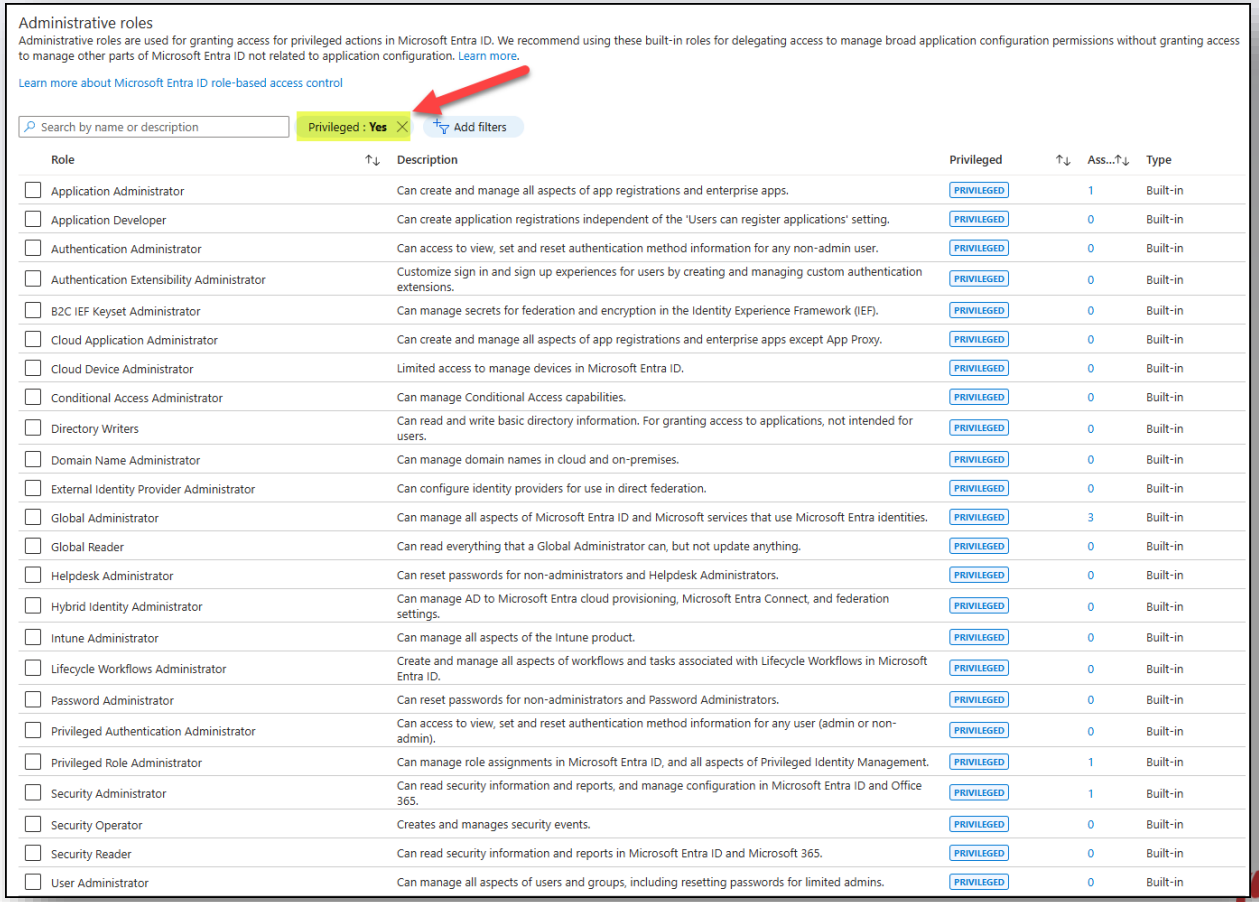
[AzRolesAdvertizer (azadvertizer.net)]



Entra ID Custom roller



Entra ID Privileged roller



Administrative roles

Administrative roles are used for granting access for privileged actions in Microsoft Entra ID. We recommend using these built-in roles for delegating access to manage broad application configuration permissions without granting access to manage other parts of Microsoft Entra ID not related to application configuration. Learn more.

Learn more about Microsoft Entra ID role-based access control

Search by name or description | Privileged : Yes | Add filters

Role	Description	Privileged	Ass...	Type
Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED	1	Built-in
Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED	0	Built-in
Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.	PRIVILEGED	0	Built-in
Authentication Extensibility Administrator	Customize sign in and sign up experiences for users by creating and managing custom authentication extensions.	PRIVILEGED	0	Built-in
B2C IEF Keyset Administrator	Can manage secrets for federation and encryption in the Identity Experience Framework (IEF).	PRIVILEGED	0	Built-in
Cloud Application Administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.	PRIVILEGED	0	Built-in
Cloud Device Administrator	Limited access to manage devices in Microsoft Entra ID.	PRIVILEGED	0	Built-in
Conditional Access Administrator	Can manage Conditional Access capabilities.	PRIVILEGED	0	Built-in
Directory Writers	Can read and write basic directory information. For granting access to applications, not intended for users.	PRIVILEGED	0	Built-in
Domain Name Administrator	Can manage domain names in cloud and on-premises.	PRIVILEGED	0	Built-in
External Identity Provider Administrator	Can configure identity providers for use in direct federation.	PRIVILEGED	0	Built-in
Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	PRIVILEGED	3	Built-in
Global Reader	Can read everything that a Global Administrator can, but not update anything.	PRIVILEGED	0	Built-in
Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.	PRIVILEGED	0	Built-in
Hybrid Identity Administrator	Can manage AD to Microsoft Entra cloud provisioning, Microsoft Entra Connect, and federation settings.	PRIVILEGED	0	Built-in
Intune Administrator	Can manage all aspects of the Intune product.	PRIVILEGED	0	Built-in
Lifecycle Workflows Administrator	Create and manage all aspects of workflows and tasks associated with Lifecycle Workflows in Microsoft Entra ID.	PRIVILEGED	0	Built-in
Password Administrator	Can reset passwords for non-administrators and Password Administrators.	PRIVILEGED	0	Built-in
Privileged Authentication Administrator	Can access to view, set and reset authentication method information for any user (admin or non-admin).	PRIVILEGED	0	Built-in
Privileged Role Administrator	Can manage role assignments in Microsoft Entra ID, and all aspects of Privileged Identity Management.	PRIVILEGED	1	Built-in
Security Administrator	Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.	PRIVILEGED	1	Built-in
Security Operator	Creates and manages security events.	PRIVILEGED	0	Built-in
Security Reader	Can read security information and reports in Microsoft Entra ID and Microsoft 365.	PRIVILEGED	0	Built-in
User Administrator	Can manage all aspects of users and groups, including resetting passwords for limited admins.	PRIVILEGED	0	Built-in

MVP Dagen

SparebankenVest

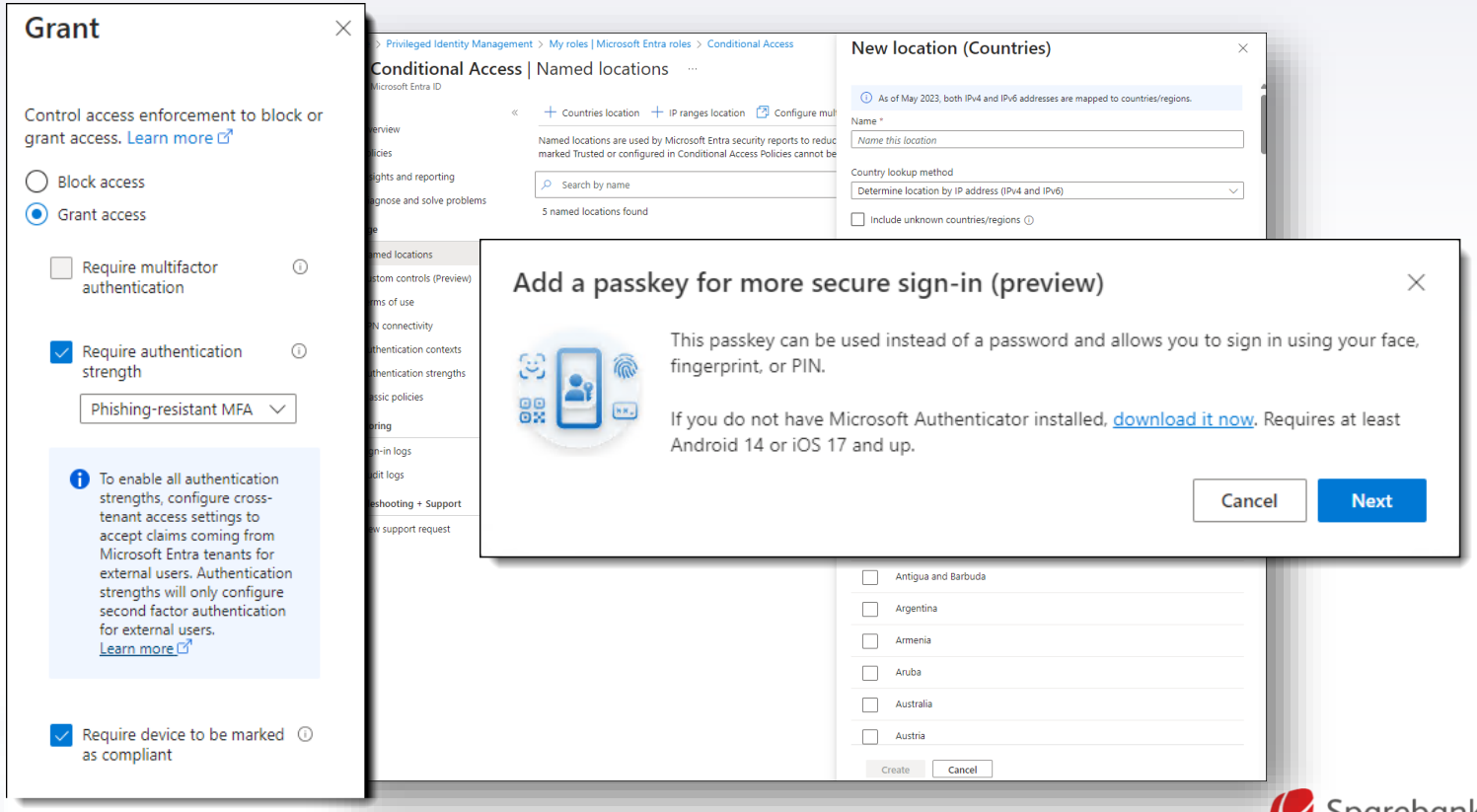
Demo

PowerShell:
Built-In & Custom

MVP Dagen

SparebankenVest

Protected actions / Conditional Access



MVP Dagen

SparebankenVest

JIT / PIM

Just in time / Privileged Identity Management

MVP Dagen

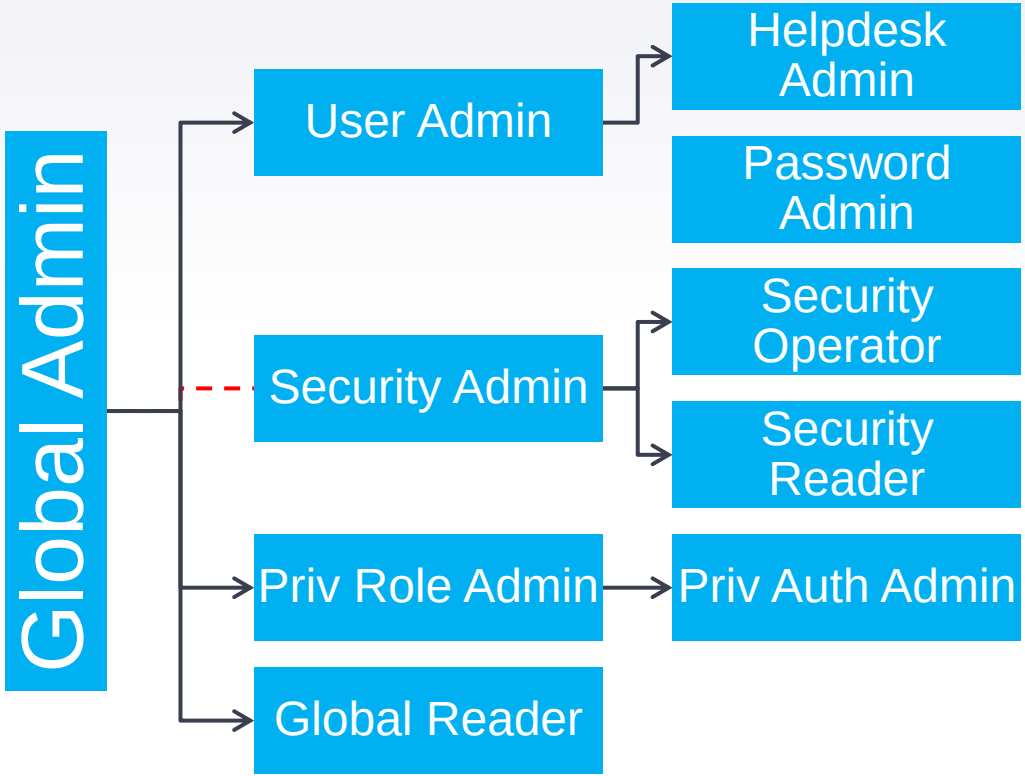
SparebankenVest

PIM

MVP Dagen

For mange koker?

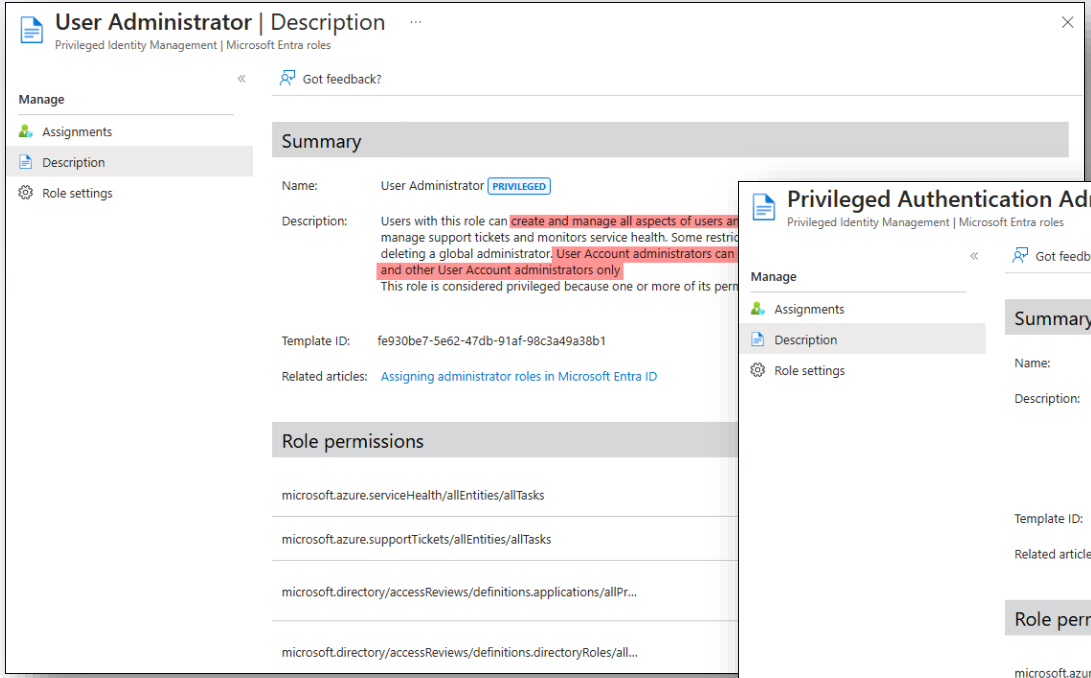
Forstå alle lag av Entra og Azure roller og tilganger

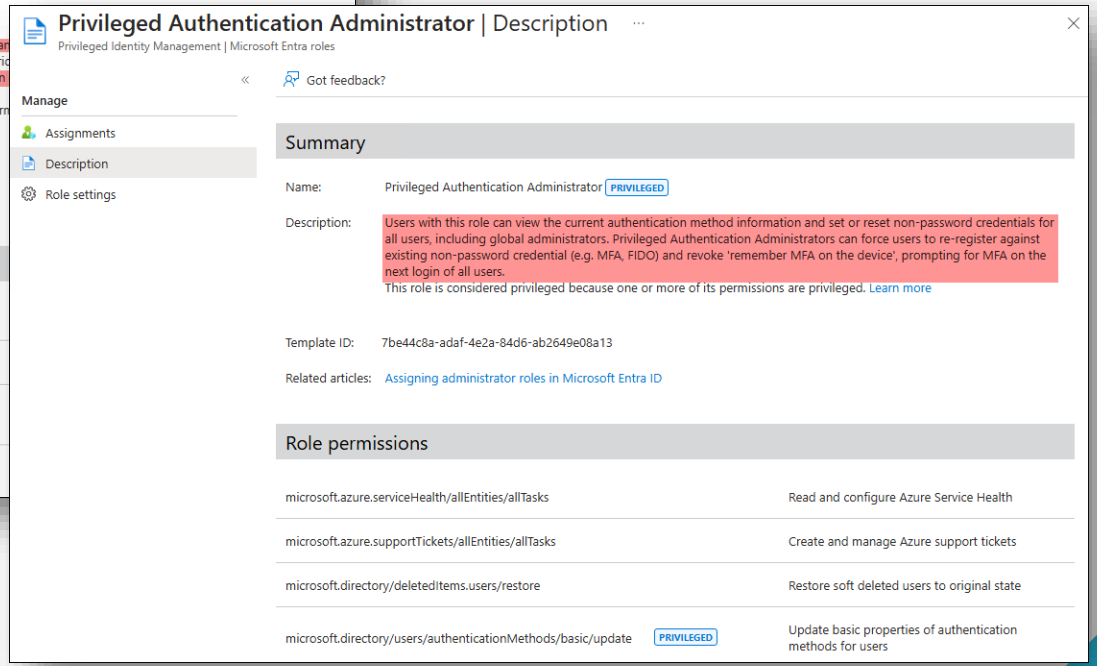


MVP Dagen

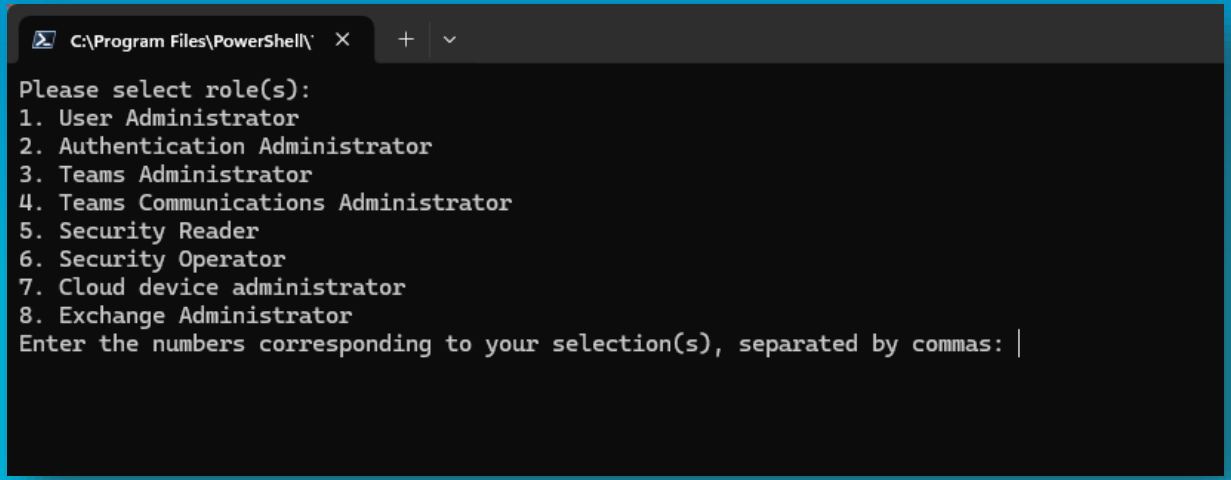
For mange koker?

Bruker administrasjon





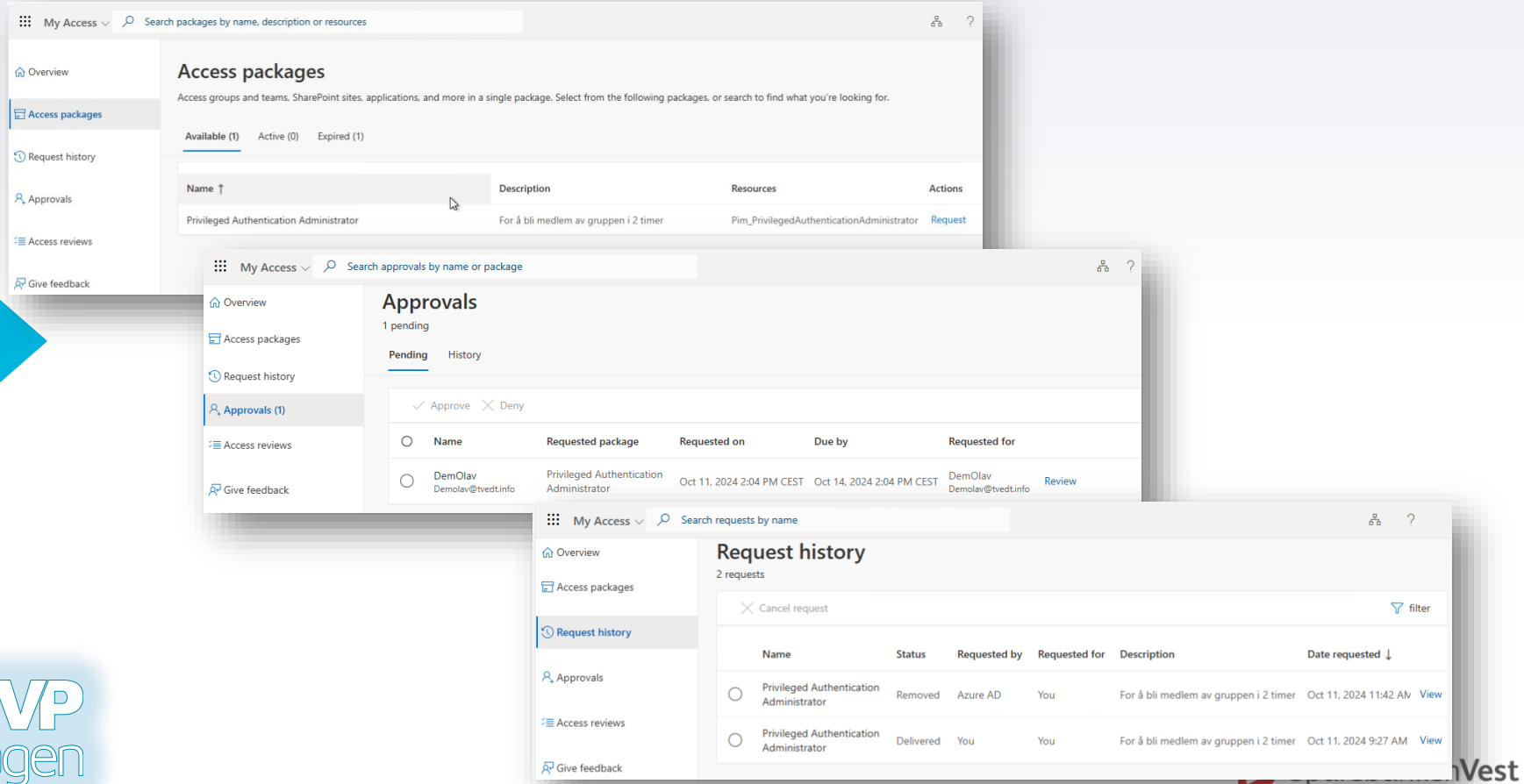
MVP Dagen



MVP Dagen

SparebankenVest

Access Packages



MVP Dagen

DEMO

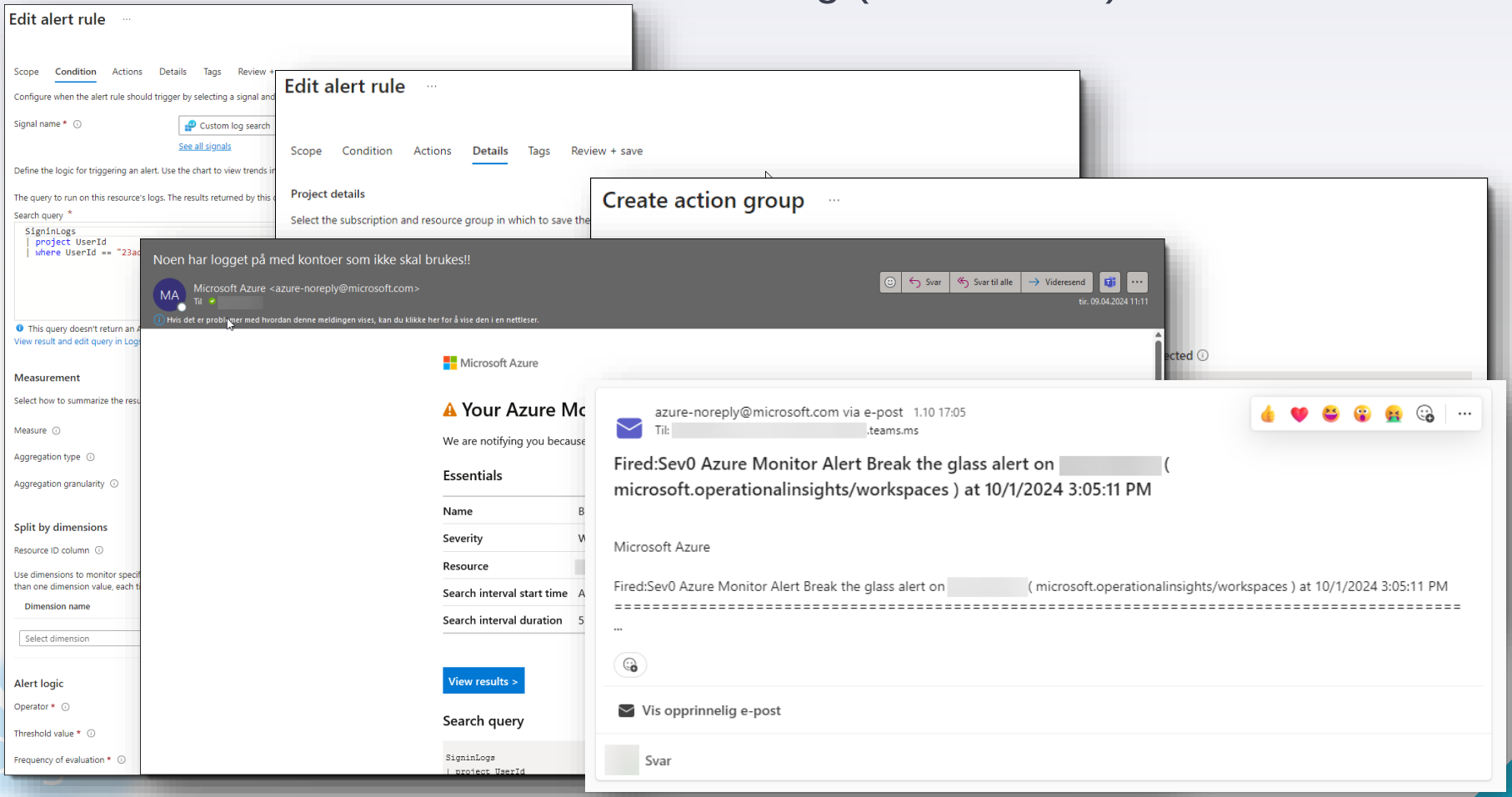
Access Packages

MVP Dagen

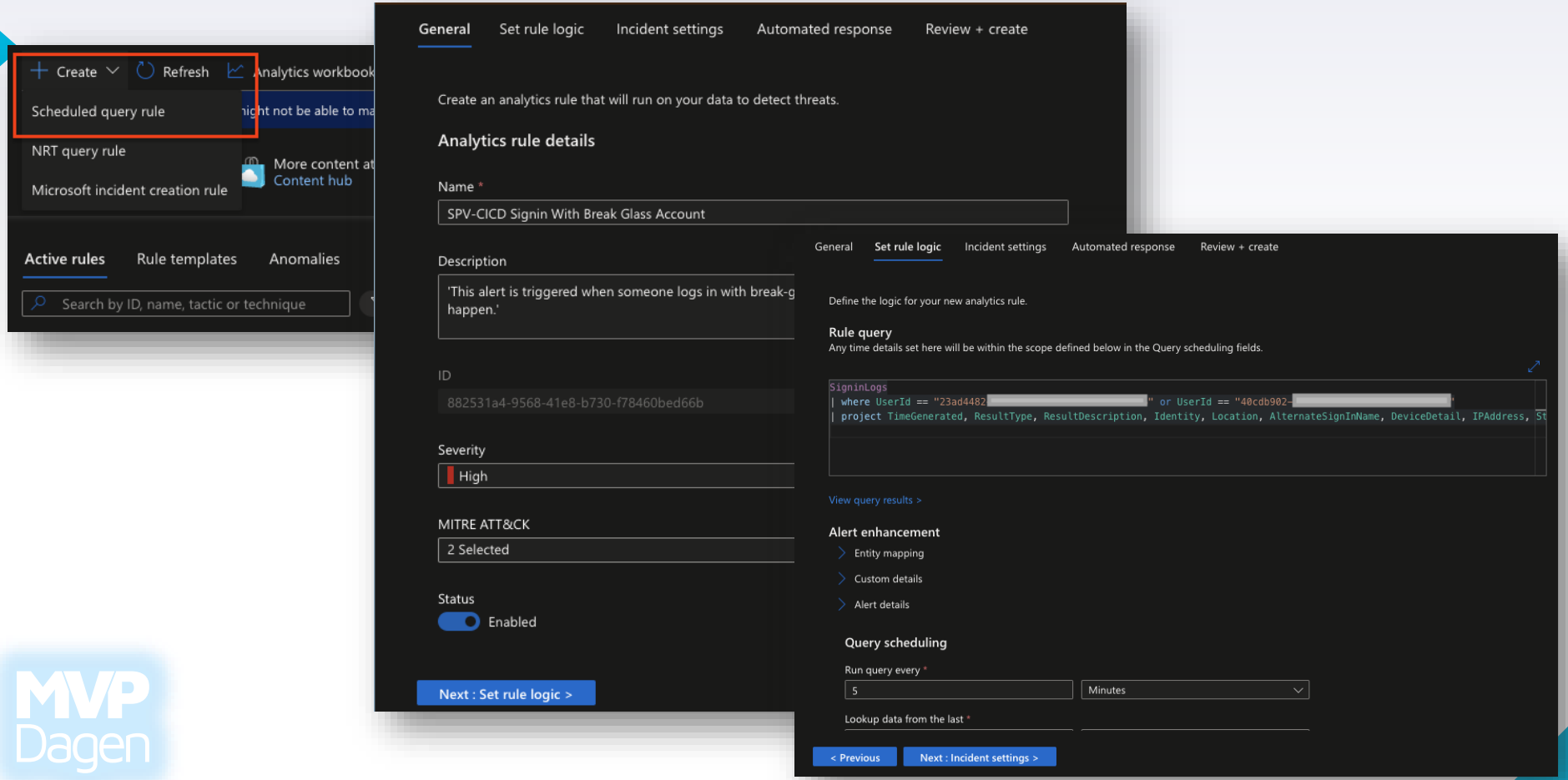
SparebankenVest

Overvåkning og innsikt

Account monitorering (VIPs / BGA)

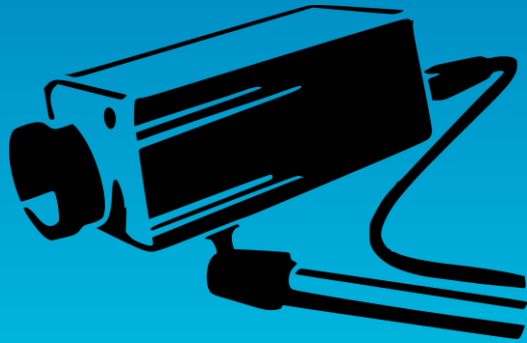


Account monitorering (VIPs / BGA)



DEMO

PIM

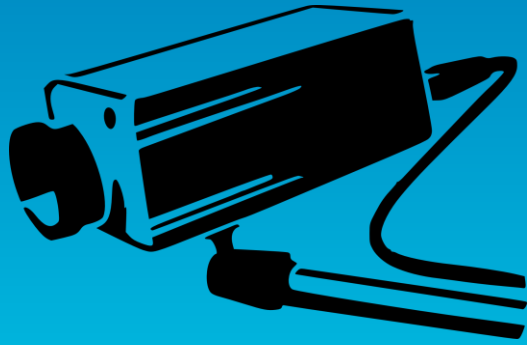


MVP Dagen

SparebankenVest

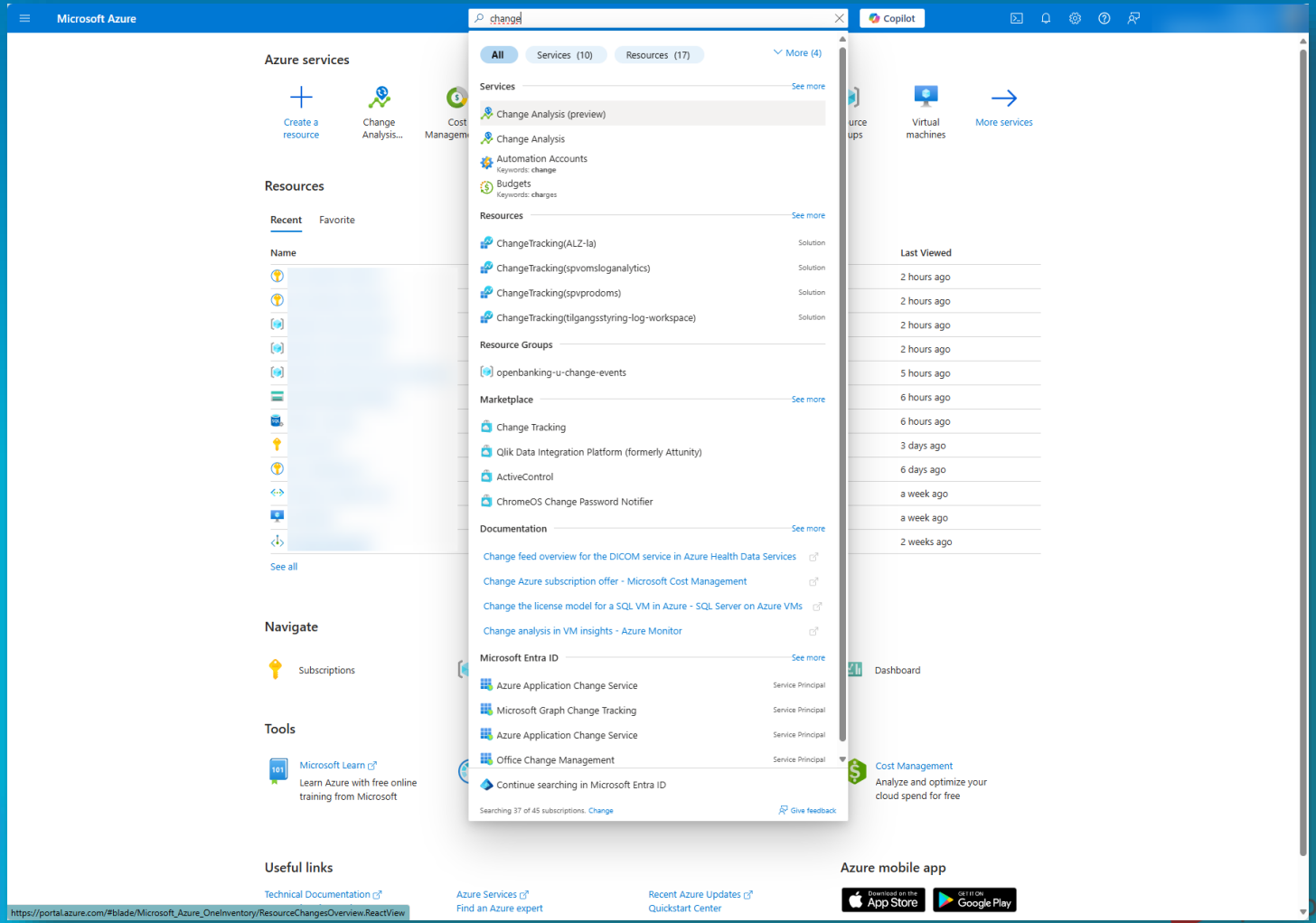
DEMO

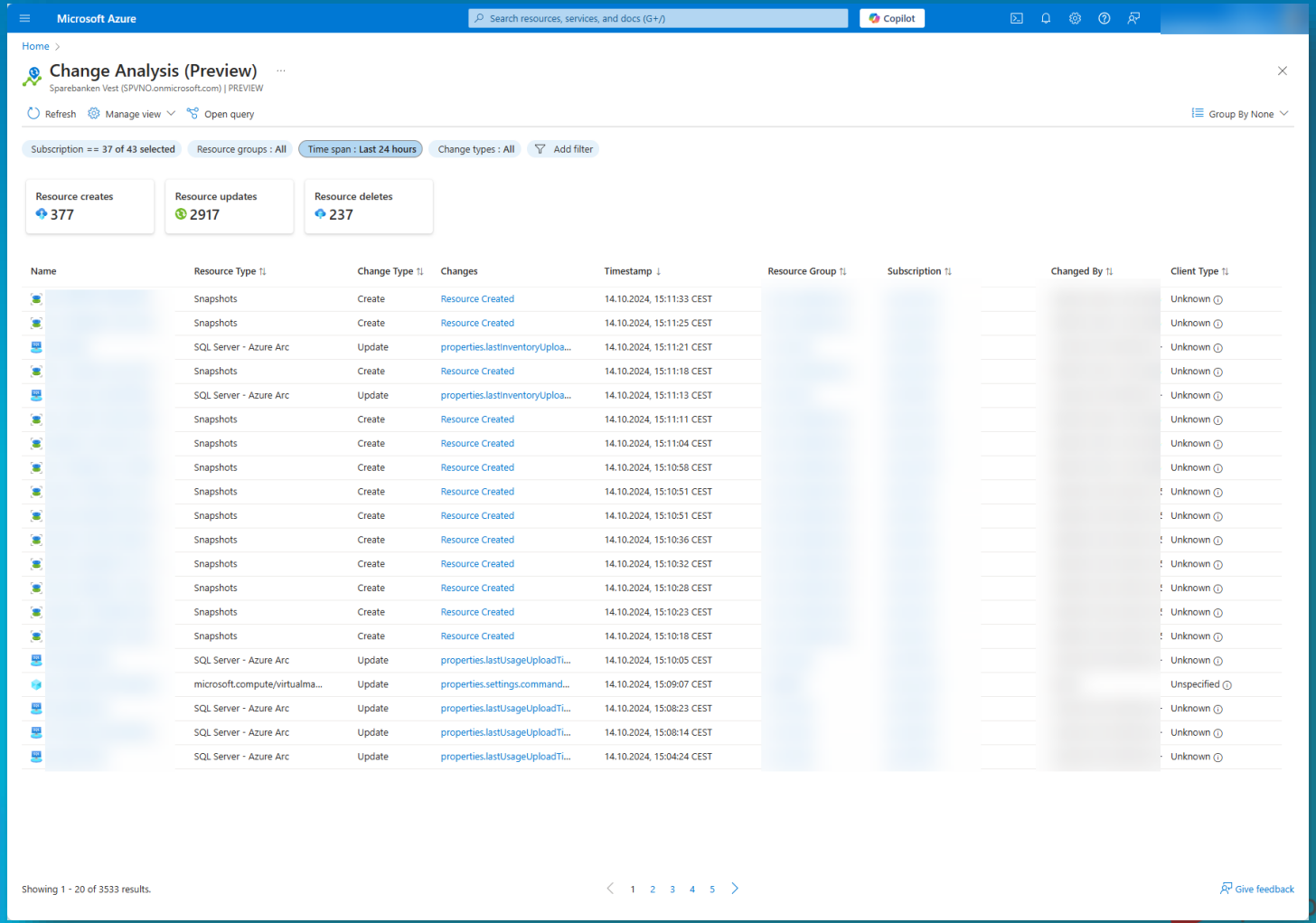
Azure endringer



MVP Dagen

SparebankenVest


Microsoft Azure
change
Copilot
All
Services (10)
Resources (17)
More (4)
Services
See more
Change Analysis (preview)
Change Analysis
Automation Accounts
Keywords: change
Budgets
Keywords: charges
Resources
See more
ChangeTracking(ALZ-la)
Solution
ChangeTracking(spvomsloganalytics)
Solution
ChangeTracking(spvprodoms)
Solution
ChangeTracking(tilgangsstyring-log-workspace)
Solution
Resource Groups
openbanking-u-change-events
Marketplace
See more
Change Tracking
Qlik Data Integration Platform (formerly Attunity)
ActiveControl
ChromeOS Change Password Notifier
Documentation
See more
Change feed overview for the DICOM service in Azure Health Data Services
Change Azure subscription offer - Microsoft Cost Management
Change the license model for a SQL VM in Azure - SQL Server on Azure VMs
Change analysis in VM insights - Azure Monitor
Microsoft Entra ID
See more
Azure Application Change Service
Service Principal
Microsoft Graph Change Tracking
Service Principal
Azure Application Change Service
Service Principal
Office Change Management
Service Principal
Continue searching in Microsoft Entra ID
Searching 37 of 45 subscriptions. Change
Give feedback
Azure services
Create a resource
Change Analysis...
Virtual machines
More services
Resources
Recent
Favorite
Name
Last Viewed
2 hours ago
2 hours ago
2 hours ago
2 hours ago
5 hours ago
6 hours ago
6 hours ago
3 days ago
6 days ago
a week ago
a week ago
2 weeks ago
See all
Navigate
Subscriptions
Dashboard
Tools
Microsoft Learn
Learn Azure with free online training from Microsoft
Cost Management
Analyze and optimize your cloud spend for free
Useful links
Technical Documentation
Azure Services
Find an Azure expert
Recent Azure Updates
Quickstart Center
Azure mobile app
Download on the App Store
GET IT ON Google Play
https://portal.azure.com/#blade/Microsoft_Azure_OneInventory/ResourceChangesOverview.ReactView



Microsoft Azure

Search resources, services, and docs (G+/)

Copilot

Home >

Change Analysis (Preview)

Sparebanken Vest (SPVNO.onmicrosoft.com) | PREVIEW

Refresh | Manage view | Open query | Group By None

Subscription == 37 of 43 selected | Resource groups : All | Time span : Last 24 hours | Change types : All | Add filter

Resource creates	Resource updates	Resource deletes
377	2917	237

Name	Resource Type	Change Type	Changes	Timestamp	Resource Group	Subscription	Changed By	Client Type
	Snapshots	Create	Resource Created	14.10.2024, 15:11:33 CEST				Unknown
	Snapshots	Create	Resource Created	14.10.2024, 15:11:25 CEST				Unknown
	SQL Server - Azure Arc	Update	properties.lastInventoryUploa...	14.10.2024, 15:11:21 CEST				Unknown
	Snapshots	Create	Resource Created	14.10.2024, 15:11:18 CEST				Unknown
	SQL Server - Azure Arc	Update	properties.lastInventoryUploa...	14.10.2024, 15:11:13 CEST				Unknown
	Snapshots	Create	Resource Created	14.10.2024, 15:11:11 CEST				Unknown
	Snapshots	Create	Resource Created	14.10.2024, 15:11:04 CEST				Unknown
	Snapshots	Create	Resource Created	14.10.2024, 15:10:58 CEST				Unknown
	Snapshots	Create	Resource Created	14.10.2024, 15:10:51 CEST				Unknown
	Snapshots	Create	Resource Created	14.10.2024, 15:10:51 CEST				Unknown
	Snapshots	Create	Resource Created	14.10.2024, 15:10:36 CEST				Unknown
	Snapshots	Create	Resource Created	14.10.2024, 15:10:32 CEST				Unknown
	Snapshots	Create	Resource Created	14.10.2024, 15:10:28 CEST				Unknown
	Snapshots	Create	Resource Created	14.10.2024, 15:10:23 CEST				Unknown
	Snapshots	Create	Resource Created	14.10.2024, 15:10:18 CEST				Unknown
	SQL Server - Azure Arc	Update	properties.lastUsageUploadTi...	14.10.2024, 15:10:05 CEST				Unknown
	microsoft.compute/virtualma...	Update	properties.settings.command...	14.10.2024, 15:09:07 CEST				Unspecified
	SQL Server - Azure Arc	Update	properties.lastUsageUploadTi...	14.10.2024, 15:08:23 CEST				Unknown
	SQL Server - Azure Arc	Update	properties.lastUsageUploadTi...	14.10.2024, 15:08:14 CEST				Unknown
	SQL Server - Azure Arc	Update	properties.lastUsageUploadTi...	14.10.2024, 15:04:24 CEST				Unknown

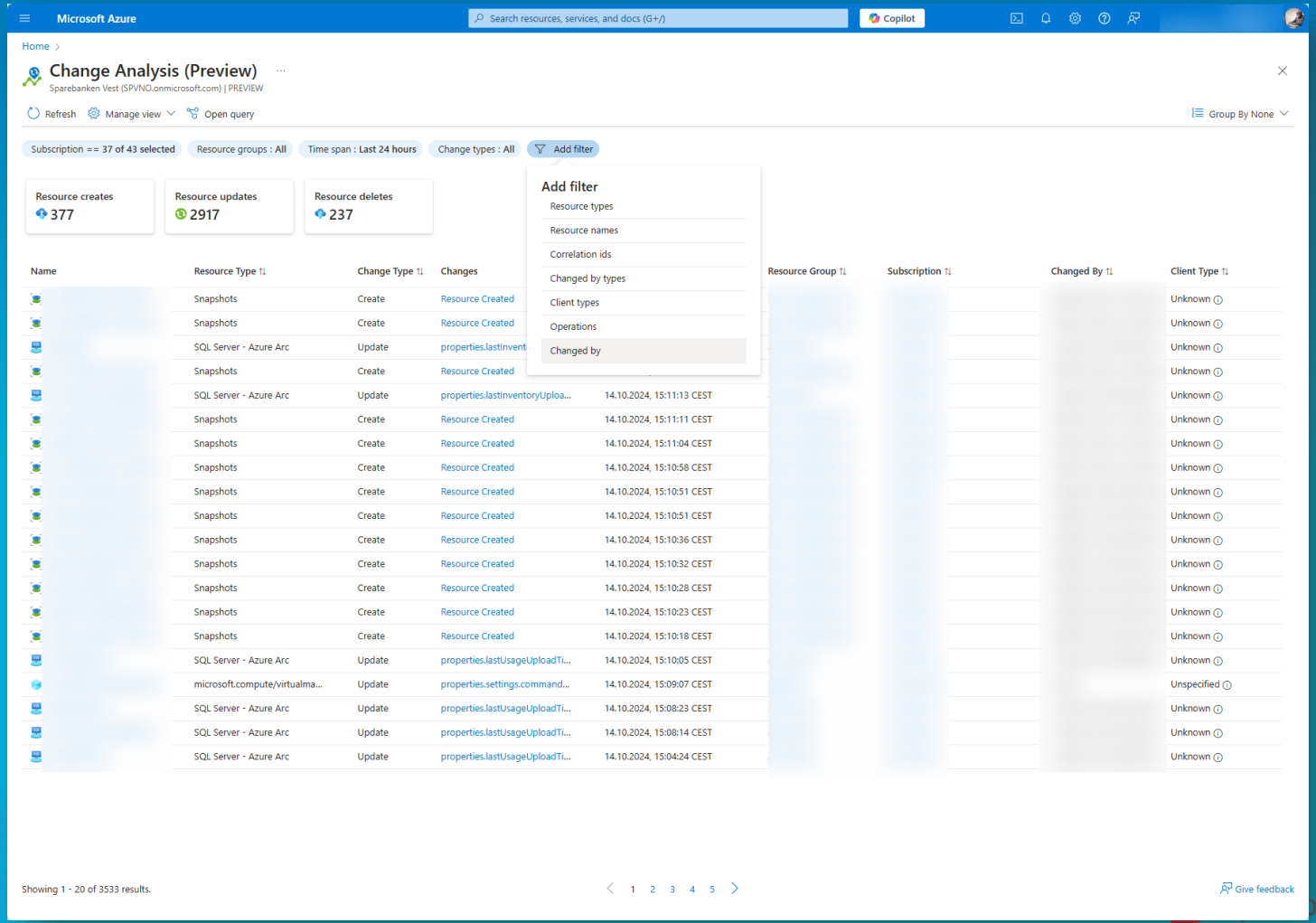
Showing 1 - 20 of 3533 results.

1 2 3 4 5

Give feedback

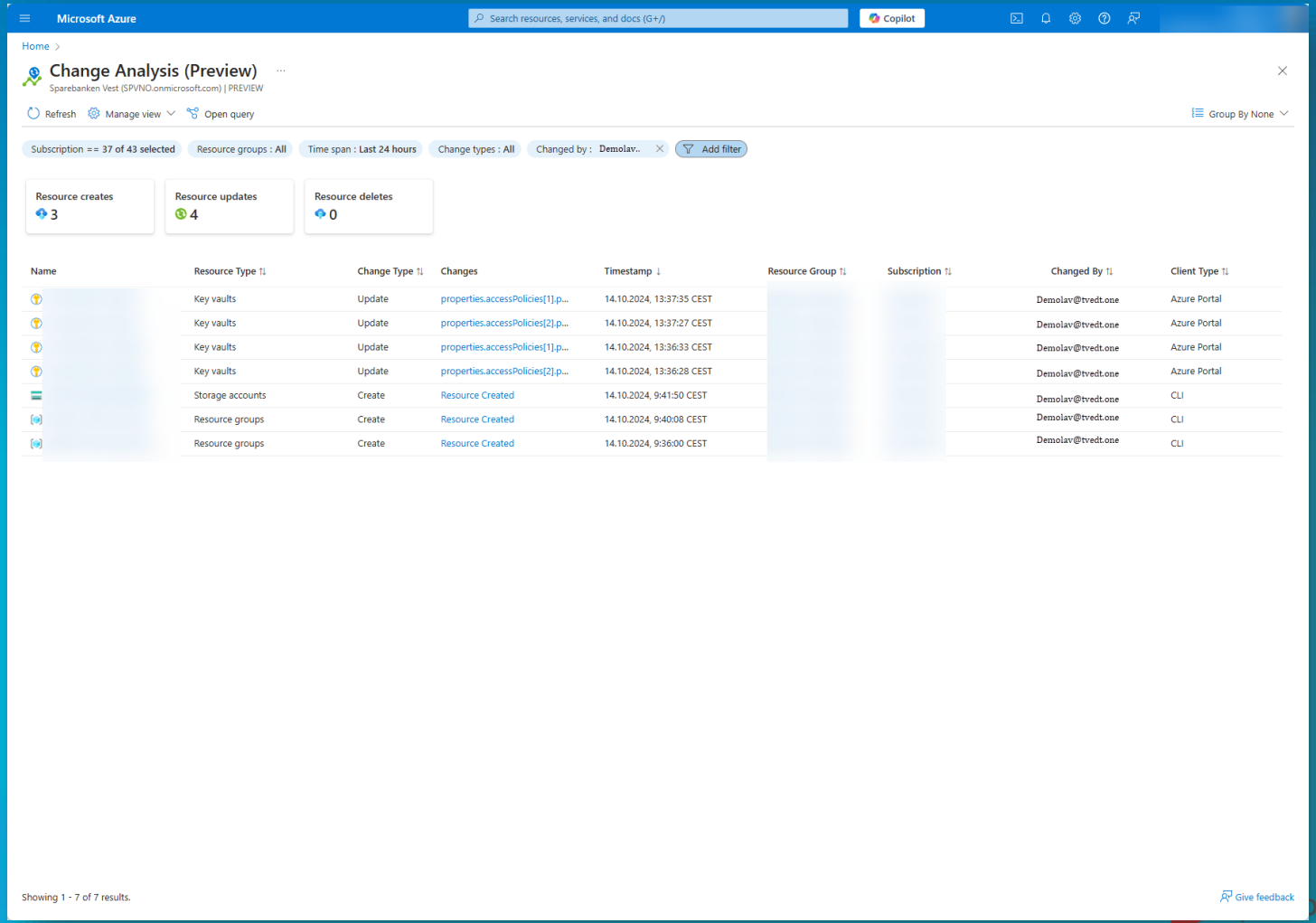
MVP Dagen

bankenVest



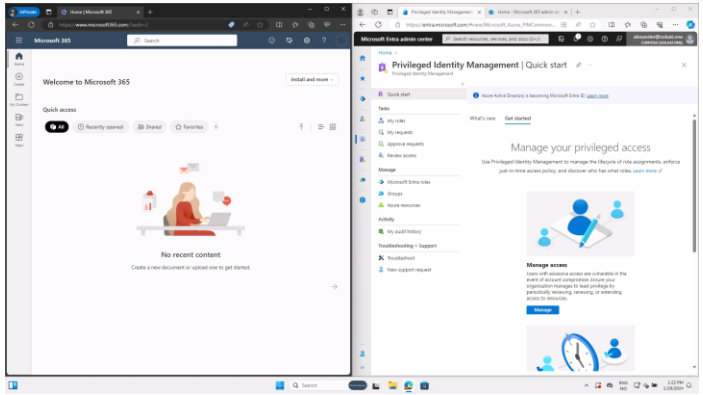
MVP Dagen

bankenVest


Microsoft Azure
Search resources, services, and docs (G+/)
Copilot
Home
Change Analysis (Preview)
Sparebanken Vest (SPVNO.onmicrosoft.com) | PREVIEW
Refresh
Manage view
Open query
Group By None
Subscription == 37 of 43 selected
Resource groups : All
Time span : Last 24 hours
Change types : All
Changed by : Demolav..
Add filter
Resource creates
3
Resource updates
4
Resource deletes
0
Name
Resource Type
Change Type
Changes
Timestamp
Resource Group
Subscription
Changed By
Client Type
Key vaults Update properties.accessPolicies[1].p... 14.10.2024, 13:37:35 CEST Demolav@tvedt.one Azure Portal
Key vaults Update properties.accessPolicies[2].p... 14.10.2024, 13:37:27 CEST Demolav@tvedt.one Azure Portal
Key vaults Update properties.accessPolicies[1].p... 14.10.2024, 13:36:33 CEST Demolav@tvedt.one Azure Portal
Key vaults Update properties.accessPolicies[2].p... 14.10.2024, 13:36:28 CEST Demolav@tvedt.one Azure Portal
Storage accounts Create Resource Created 14.10.2024, 9:41:50 CEST Demolav@tvedt.one CLI
Resource groups Create Resource Created 14.10.2024, 9:40:08 CEST Demolav@tvedt.one CLI
Resource groups Create Resource Created 14.10.2024, 9:36:00 CEST Demolav@tvedt.one CLI
Showing 1 - 7 of 7 results.
Give feedback

Privileged Role Administrator

DEMO TIME



MVP Dagen

:)

Your PC ran into a problem that it couldn't handle

Contact The Bluesscreen Brothers!

The BluesScreen Brothers

https://www.youtube.com/@bluescreenbrothers

https://www.linkedin.com/company/blaskjerm-brodrene

https://shows.acast.com/blaskjerm

SparebankenVest