



I am the VIP

Global Azure Meetup #Bergen

Bluescreen Brothers edition



SparebankenVest

Fortytwo.io

WE ARE FORTYTWO

We solve our customers challenges. Problems. We are the solution. We are technology. Using the best tools, we ensure that our customers can rely on their operations, safely, securely, in the cloud.



We`re not just experts

We're like the cosmic hitchhikers of the cloud. Our squad, versed in DevOps, Cloud Native, Security, and beyond, is on a mission to turn challenges into victories across the galaxy.



We`re not just building cloud solutions

We're navigating the cosmic waves of innovation. Step into our realm, where the solutions we craft in the Microsoft Cloud ecosystem are as robust as they are out-of-this-world.

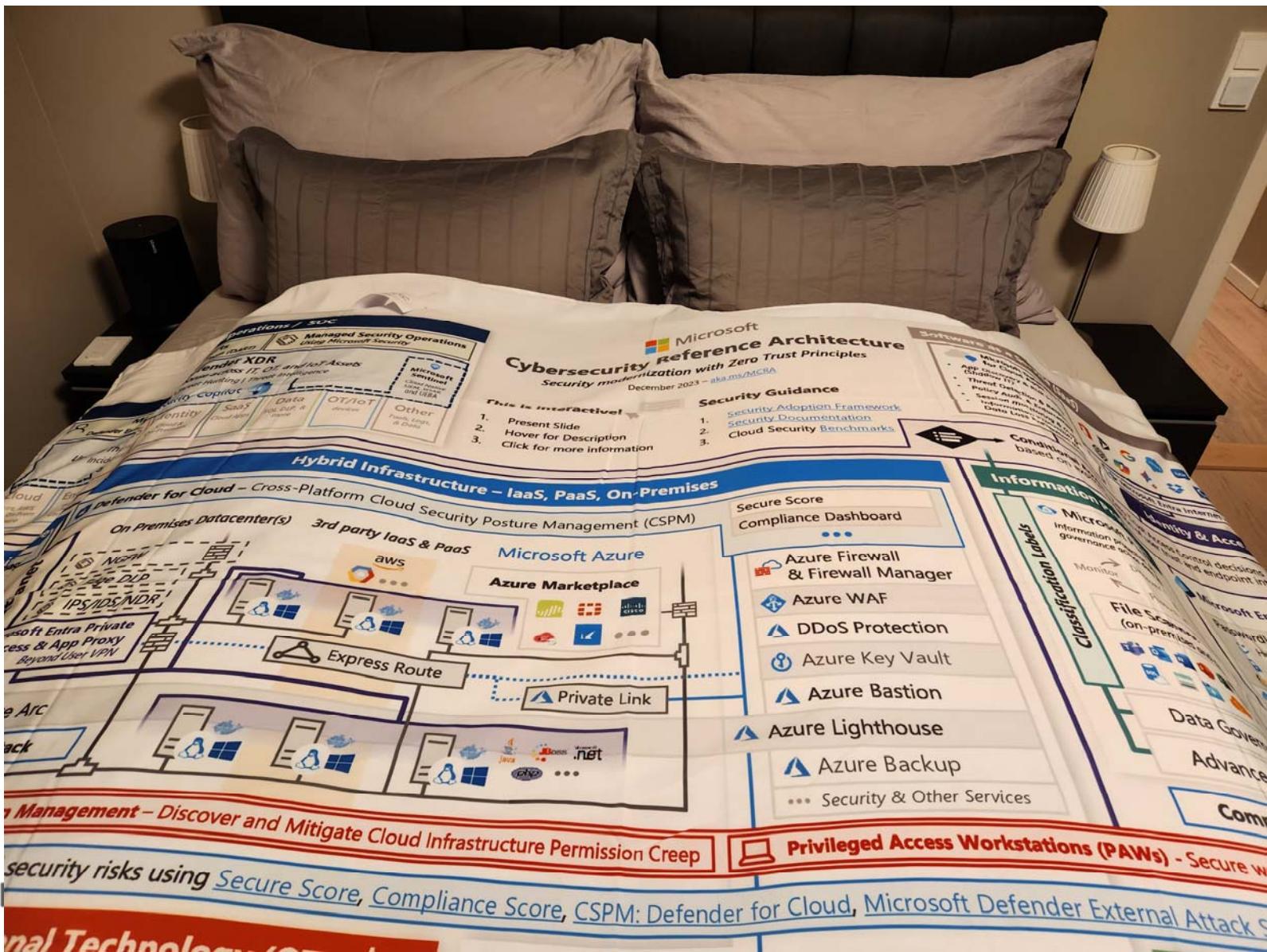


We`re not your ordinary service provider

We're intergalactic partners in your journey to success. Dive into collaboration, and unlock a galaxy of expertise to navigate the cloud with unwavering confidence.

Fortytwo.io

The VIP experience!



Spark

two.io

TLA's

Being geeks, we quickly realized that the problem with TLAs is that there are only 17,576 unique TLAs in a 26-letter alphabet

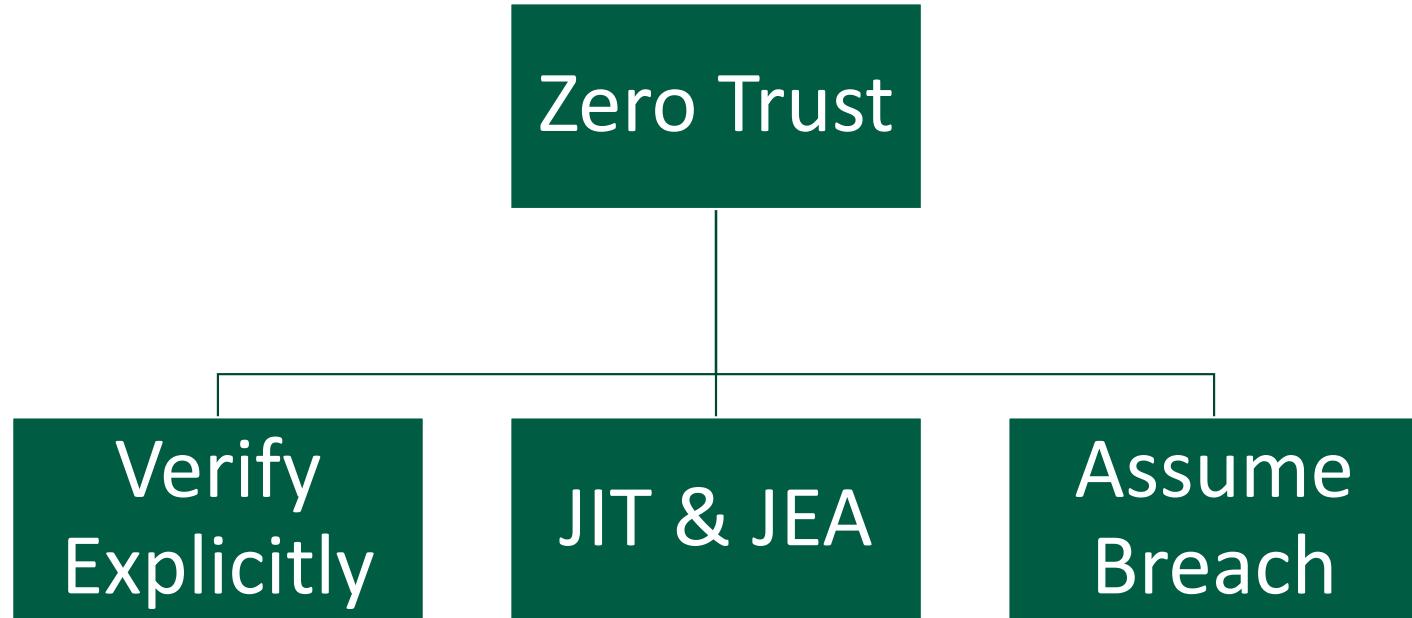
DNS
JIT
JEA
LOL

SOAP
ISDN
ADSL
ROFL

(...)In a 1998 newsletter article, I declared them to be FLAPs. This stands for four-Letter Acronym package, and of course, FLAP itself is a FLAP

Microsoft have used them all up the summer before last.

ZT, VE, JIT, JEA & AB går inn i en bar

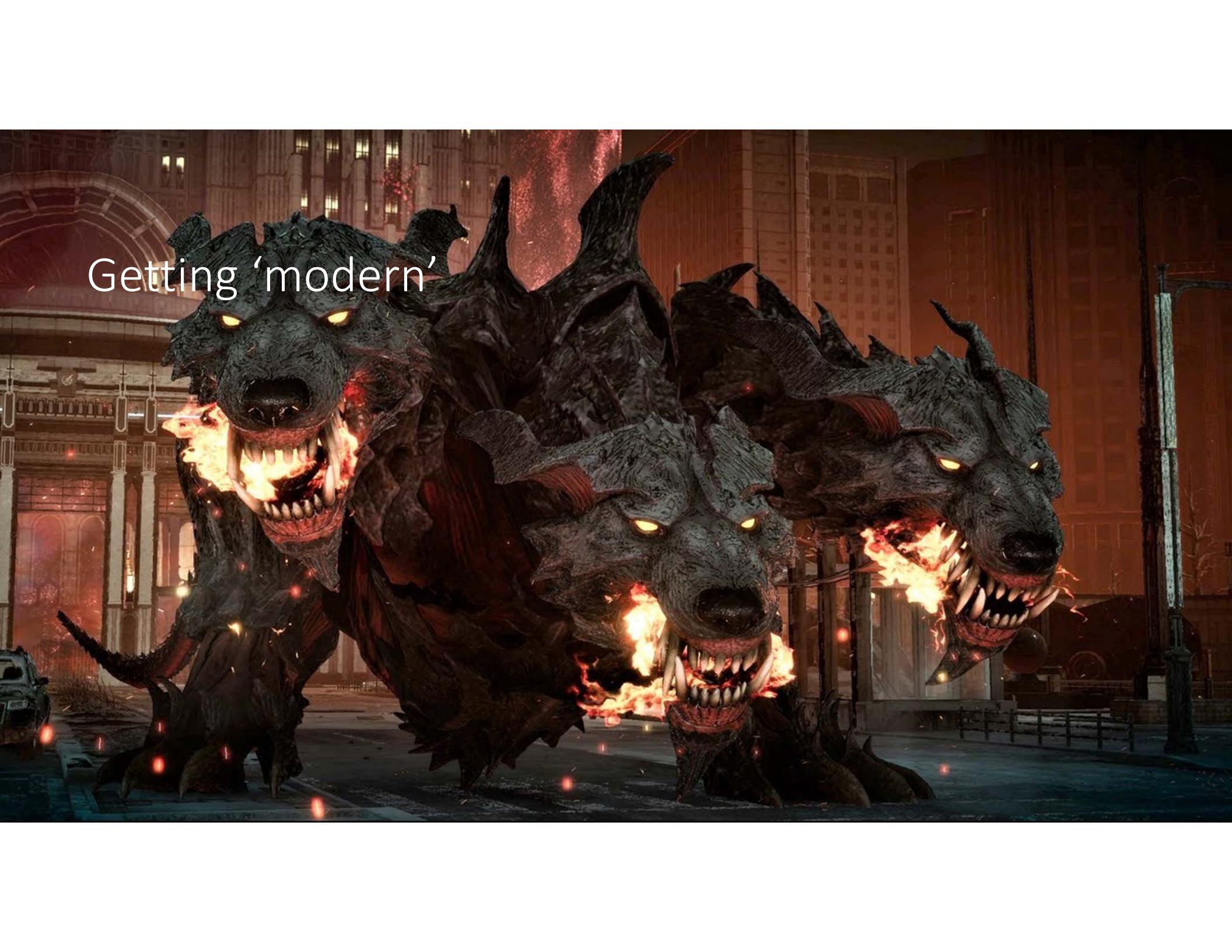


Who are you?



What are you accessing?



A massive, dark, multi-headed怪兽 (怪獣) stands in a city street at night. The creature has several heads, each with glowing yellow eyes and a mouth full of sharp, white teeth. It appears to be breathing fire from its mouths. The background shows a city skyline with lit buildings and a bridge.

Getting 'modern'

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

99



529

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"  
}
```

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"  
}
```

notActions

```
"notActions": [  
    "Microsoft.Network/virtualNetworks/write",  
    "Microsoft.Network/virtualNetworks/delete",  
    "Microsoft.Network/vpnGateways/*",  
    "Microsoft.Network/azurefirewalls/*",  
    "Microsoft.Network/expressRouteCircuits/*",  
    "Microsoft.Network/routeTables/write",  
    "Microsoft.Network/routeTables/delete",  
    "Microsoft.Network/routeTables/routes/write",  
    "Microsoft.Network/routeTables/routes/delete",  
    "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/write",  
    "Microsoft.Network/virtualNetworks/virtualNetworkPeerings/delete",  
    "Microsoft.Network/vpnSites/*"  
,
```

Customizing the Portal way

Create a custom role ...

Basics Permissions Assignable scopes JSON Review + create

+ Add permissions + Exclude permissions

Click Add permissions to select the permissions you want to add to this custom role.
To add a wildcard (*) permission, you must manually add the permission on the JSON tab. [Learn more](#)
To exclude specific permissions from a wildcard permission, click Exclude permissions. [Learn more](#)

Permission	Description	Permission type
*	--	Action
Microsoft.Authorization/*/Delete	--	NotAction
Microsoft.Authorization/*/Write	--	NotAction
Microsoft.Authorization/elevateAccess/Action	Grants the caller User Access Administrator access ...	NotAction
Microsoft.Blueprint/blueprintAssignments/write	Create or update any blueprint artifacts	NotAction
Microsoft.Blueprint/blueprintAssignments/delete	Delete any blueprint artifacts	NotAction
Microsoft.Compute/galleries/share/action	Shares a Gallery to different scopes	NotAction
Microsoft.Purview/consents/write	Create or Update a Consent Resource.	NotAction
Microsoft.Purview/consents/delete	Delete the Consent Resource.	NotAction
Microsoft.Network/vpnsites/read	Gets a Vpn Site resource.	NotAction
Microsoft.Network/vpnsites/write	Creates or updates a Vpn Site resource.	NotAction
Microsoft.Network/vpnsites/delete	Deletes a Vpn Site resource.	NotAction
microsoft.network/vpnSites/vpnSiteLinks/read	Gets a Vpn Site Link	NotAction



Sparebeam

.ertytwo.io

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>

What about Entra ID?

Your Role: Global Administrator and 1 other roles					
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 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					
Role	Description	Privileged	Type	Ass... ↑↓	Type
<input type="checkbox"/> Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Authentication Administrator	Can access to view, set and reset authentication method information for any non-admin user.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Authentication Extensibility Administrator	Customize sign in and sign up experiences for users by creating and managing custom authentication extensions.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> B2C IEF Keyset Administrator	Can manage secrets for federation and encryption in the Identity Experience Framework (IEF).	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Cloud Application Administrator	Can create and manage all aspects of app registrations and enterprise apps except App Proxy.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Cloud Device Administrator	Limited access to manage devices in Microsoft Entra ID.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Conditional Access Administrator	Can manage Conditional Access capabilities.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Directory Writers	Can read and write basic directory information. For granting access to applications, not intended for users.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Domain Name Administrator	Can manage domain names in cloud and on-premises.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> External Identity Provider Administrator	Can configure identity providers for use in direct federation.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Global Administrator	Can manage all aspects of Microsoft Entra ID and Microsoft services that use Microsoft Entra identities.	PRIVILEGED	Built-in	2	
<input type="checkbox"/> Global Reader	Can read everything that a Global Administrator can, but not update anything.	PRIVILEGED	Built-in	2	
<input type="checkbox"/> Helpdesk Administrator	Can reset passwords for non-administrators and Helpdesk Administrators.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Hybrid Identity Administrator	Can manage AD to Microsoft Entra cloud provisioning, Microsoft Entra Connect, and federation settings.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Intune Administrator	Can manage all aspects of the Intune product.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Lifecycle Workflows Administrator	Create and manage all aspects of workflows and tasks associated with Lifecycle Workflows in Microsoft Entra ID.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Password Administrator	Can reset passwords for non-administrators and Password Administrators.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Privileged Authentication Administrator	Can access to view, set and reset authentication method information for any user (admin or non-admin).	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Privileged Role Administrator	Can manage role assignments in Microsoft Entra ID, and all aspects of Privileged Identity Management.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Security Administrator	Can read security information and reports, and manage configuration in Microsoft Entra ID and Office 365.	PRIVILEGED	Built-in	1	
<input type="checkbox"/> Security Operator	Creates and manages security events.	PRIVILEGED	Built-in	0	
<input type="checkbox"/> Security Reader	Can read security information and reports in Microsoft Entra ID and Microsoft 365.	PRIVILEGED	Built-in	0	

Customize?

Home >

Roles and administrators | All roles

solaat

+ New custom role Delete custom role Download assignments Refresh Preview features Go

All roles Protected actions Diagnose and solve problems

Activity Access reviews Audit logs

Troubleshooting + Support New support request

Administrative roles

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

Learn more about Microsoft Entra ID role-based access control

Search by name or description Add filters

Role	Description	Privileged
<input type="checkbox"/> Application Administrator	Can create and manage all aspects of app registrations and enterprise apps.	PRIVILEGED
<input type="checkbox"/> Application Developer	Can create application registrations independent of the 'Users can register applications' setting.	PRIVILEGED
<input type="checkbox"/> Attack Payload Author	Can create attack payloads that an administrator can initiate later.	

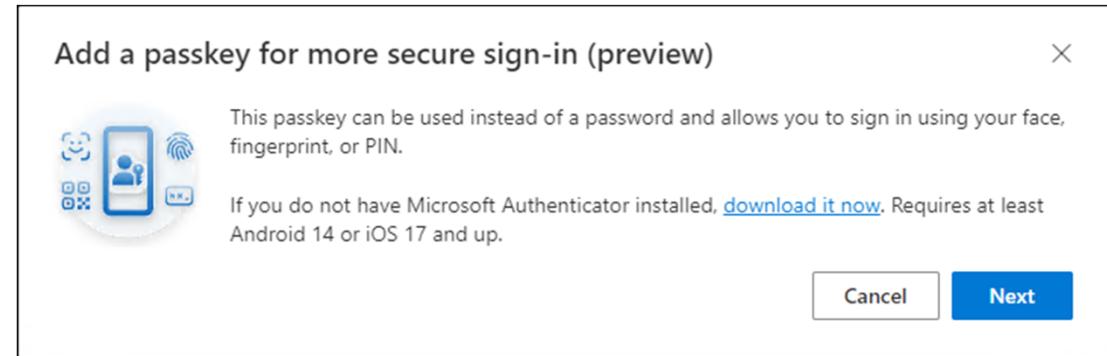
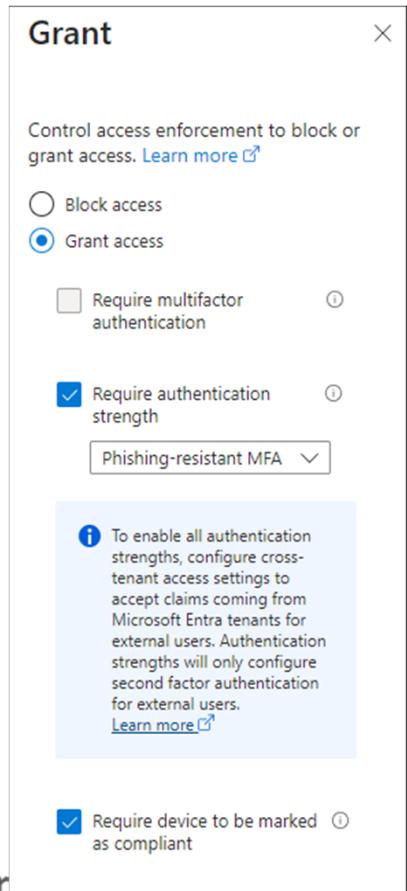
Non-local admin?

The screenshot shows the Microsoft Intune admin center interface. The left sidebar includes links for Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled "Create profile" for "Windows PC". The navigation bar at the top shows steps: Basics (green checkmark), Out-of-box experience (OOBE) (selected tab), Assignments, and Review + create. The "Out-of-box experience (OOBE)" section is configured for "User-Driven" deployment mode and "Microsoft Entra joined" device joining. It includes sections for Microsoft Software License Terms, Privacy settings, and Hide change account options. A note states that the default value for diagnostic data collection has changed for devices running Windows 10, version 1903 and later, or Windows 11. The "User account type" section is highlighted in yellow, showing "Administrator" selected over "Standard". Other configuration options include "Allow pre-provisioned deployment" (No), "Language (Region)" (Operating system default), "Automatically configure keyboard" (Yes), and "Apply device name template" (No). At the bottom, there are "Previous" and "Next" buttons.

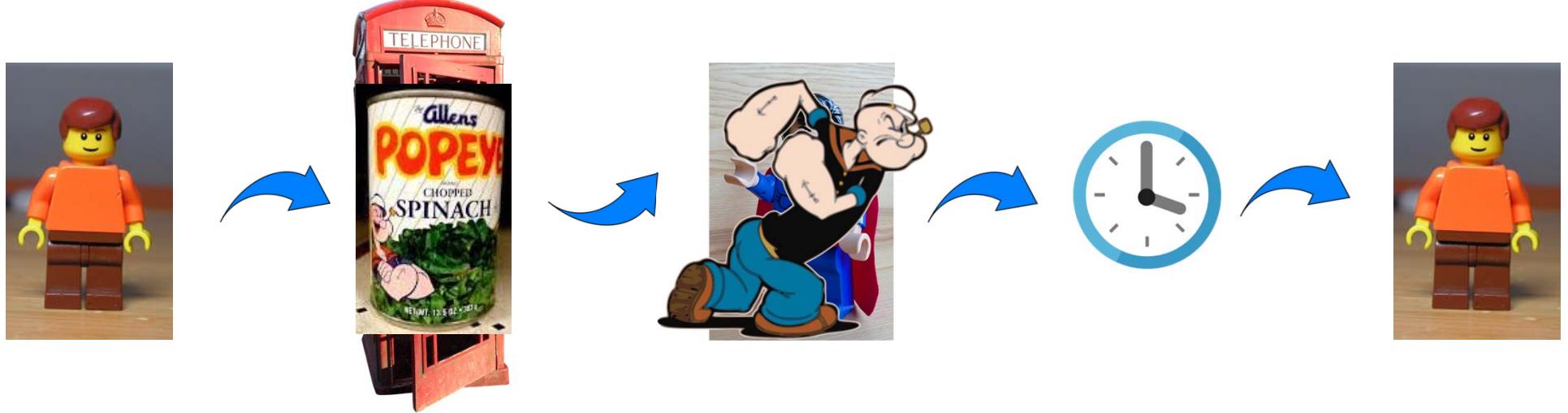
Limitations?

The screenshot shows the Microsoft Intune admin center interface. The left sidebar includes links for Home, Dashboard, All services, Devices, Apps, Endpoint security, Reports, Users, Groups, Tenant administration, and Troubleshooting + support. The main content area is titled 'Add assignments' under 'Privileged Identity Management | Microsoft Entra roles'. It shows a 'Membership' tab selected and a 'Setting' tab. A message box says, 'You can also assign roles to groups now. Learn more'. Below it, 'Resource' is set to 'solaat' and 'Resource type' is 'Directory'. A yellow-highlighted dropdown menu under 'Select role' shows 'Microsoft Entra Joined Device Local Administrator'. The 'Scope type' dropdown is set to 'Directory'. Under 'Select member(s)', it says '1 Member(s) selected' and shows 'Alexander Solaat Rødland' with a 'Remove' link. At the bottom are 'Next >' and 'Cancel' buttons.

Protected actions / Conditional Access



JIT What?



JIT & JEA fundamentals



DEMO TIME

Two side-by-side screenshots of Microsoft 365 and Microsoft Entra admin center. The left screenshot shows the Microsoft 365 homepage with a 'Welcome to Microsoft 365' message and a 'Quick access' sidebar. The right screenshot shows the 'Privileged Identity Management | Quick start' page in the Microsoft Entra admin center, which includes sections for 'Manage your privileged access' and 'Manage access'.

Audit Log Details		
Activity	Target(s)	Modified Properties
Activity		
Date	3/15/2024, 2:36 PM	
Activity Type	Remove service principal	
Correlation ID	a9521bd8-b2ae-4a45-996b-4e1a581dcae1	
Category	ApplicationManagement	
Status	success	
Status reason		
User Agent		
Initiated by (actor)		
Type	User	
Display Name		
Object ID	[REDACTED]	
User Principal Name	[REDACTED]	
Additional Details		
User-Agent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/122.0.0.0 Safari/537.36 Edg/122.0.0.0	
AppId	85fcd61c-7adb-4218-92cc-ead61fe65cab	

Account monitorering (VIPs / BGA)

The screenshot shows the Azure portal interface for managing alert rules. A modal window titled "Edit alert rule" is open, showing the "Details" tab. The search query is set to:

```
SigninLogs  
| project UserId  
| where UserId == "23ad"
```

The alert has triggered, and a message box displays:

Noen har logget på med kontøer som ikke skal brukes!!

Microsoft Azure <azure-noreply@microsoft.com>

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

Azure Monitor alert details:

⚠ Your Azure Monitor alert was triggered

We are notifying you because there are 4 counts of "Break the glass alert".

Essentials

Name	Break the glass alert
Severity	Warning
Resource	[Redacted]
Search interval start time	April 9, 2024 9:05:15 UTC
Search interval duration	5 min

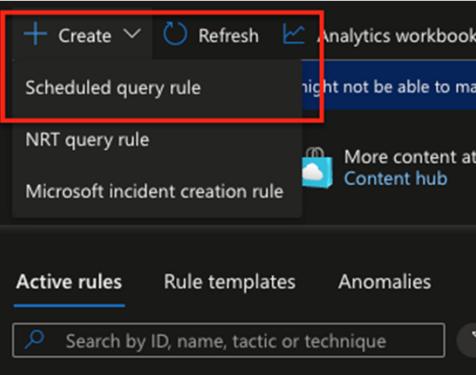
View results >

Search query

```
SigninLogs  
| project UserId
```

Fortytwo.io

Account monitoring (VIPs / BGA)



The screenshot shows the Microsoft Sentinel interface for creating a new analytics rule. A red box highlights the 'Scheduled query rule' option in the left sidebar.

General Set rule logic Incident settings Automated response Review + create

Create an analytics rule that will run on your data to detect threats.

Analytics rule details

Name * SPV-CICD Signin With Break Glass Account

Description This alert is triggered when someone logs in with break-g happen.'

ID 882531a4-9568-41e8-b730-f78460bed66b

Severity High

MITRE ATT&CK 2 Selected

Status Enabled

Next : Set rule logic >

Rule query

Any time details set here will be within the scope defined below in the Query scheduling fields.

```
SignInLogs  
| where UserId == "23ad4482-[REDACTED]" or UserId == "40cdb902-[REDACTED]"  
| project TimeGenerated, ResultType, ResultDescription, Identity, Location, AlternateSignInName, DeviceDetail, IPAddress, St
```

View query results >

Alert enhancement

- > Entity mapping
- > Custom details
- > Alert details

Query scheduling

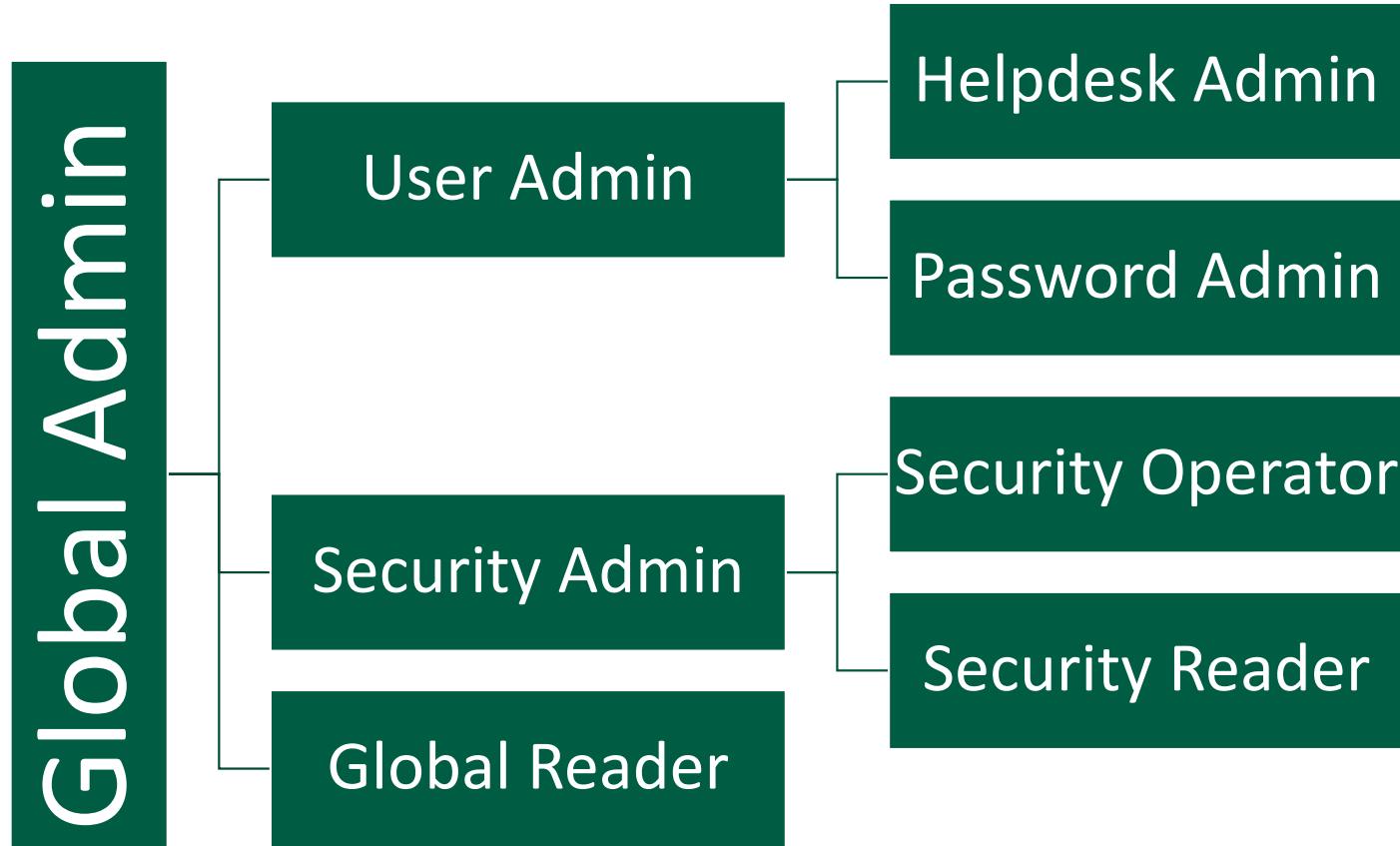
Run query every * 5 Minutes

Lookup data from the last *

< Previous Next : Incident settings >

Too many cooks?

Knowing the many layers of JEA M365- rights



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

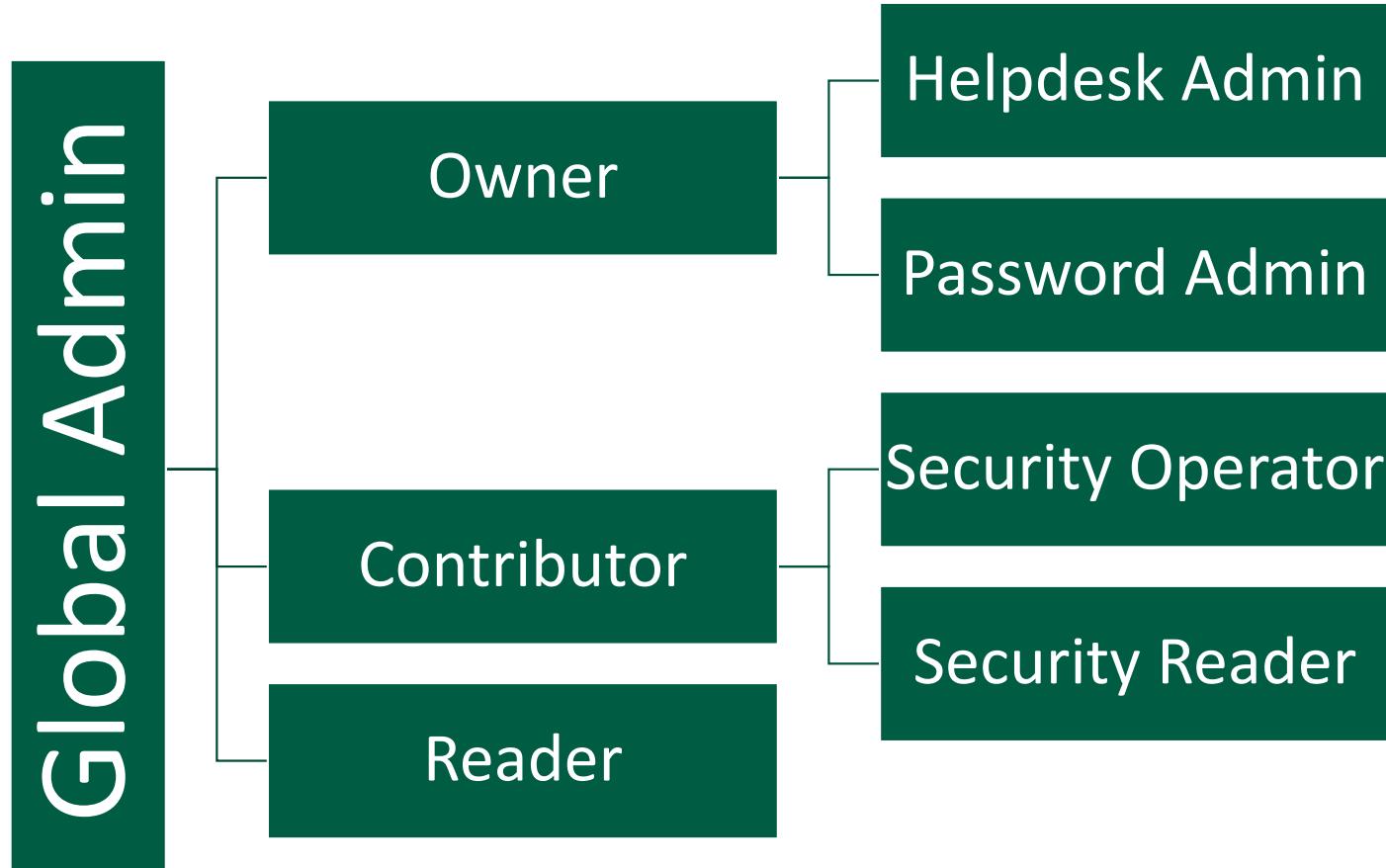
99



529

Too many cooks?

Knowing the many layers of JEA Azure rights





Alexander Solaat Rødland
Principal Cloud Engineer @ Fortytwo

- ✉ • alexander@solaat.no
- ▶ • youtube.com/@bluescreenbrothers
- in • [/in/alexsolaat](https://www.linkedin.com/in/alexsolaat)



Fortytwo.io



Olav Tvedt
Cloud dude @ Sparebanken Vest

- ✉ • olav@tvedt.info
- ▶ • youtube.com/@bluescreenbrothers
- in • [/in/otvedt](https://www.linkedin.com/in/otvedt)



Fortytwo.io

:)

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>



Fortytwo.io