

MVP Dagen

mvpdagen.no



I NEED TO KNOW WHY MOVING
OUR APP TO THE CLOUD DIDN'T
AUTOMATICALLY SOLVE ALL OUR
PROBLEMS.



Dilbert.com @ScottAdamsSays

YOU WOULDN'T
LET ME RE-
ARCHITECT THE
APP TO BE
CLOUD-NATIVE.

JUST PUT IT
IN
CONTAINERS.



11-08-17 © 2017 Scott Adams, Inc./Dist. by Andrews McMeel

YOU CAN'T
SOLVE A
PROBLEM JUST
BY SAYING
TECHY THINGS. KUBERNETES.





AKS Automatic riktig valg for deg?

Martin Ehrnst & Anders Kristiansen

kubectl describe pod presenters



Anders Kristiansen
Lead Security Architect STB CDC
MVP Security SIEM & XDR,
Identity & Access



Martin Ehrnst
Principal Architect @ Simplifai
MVP DevOps & Azure Kubernetes

AKS Automatic med sikkerhetsbriller

- - Nice, nå jeg jeg slipper jeg endelig manage clustere
- Alle AKS Automatic features finnes i vanlig Standard AKS.



Automatic fra platform siden



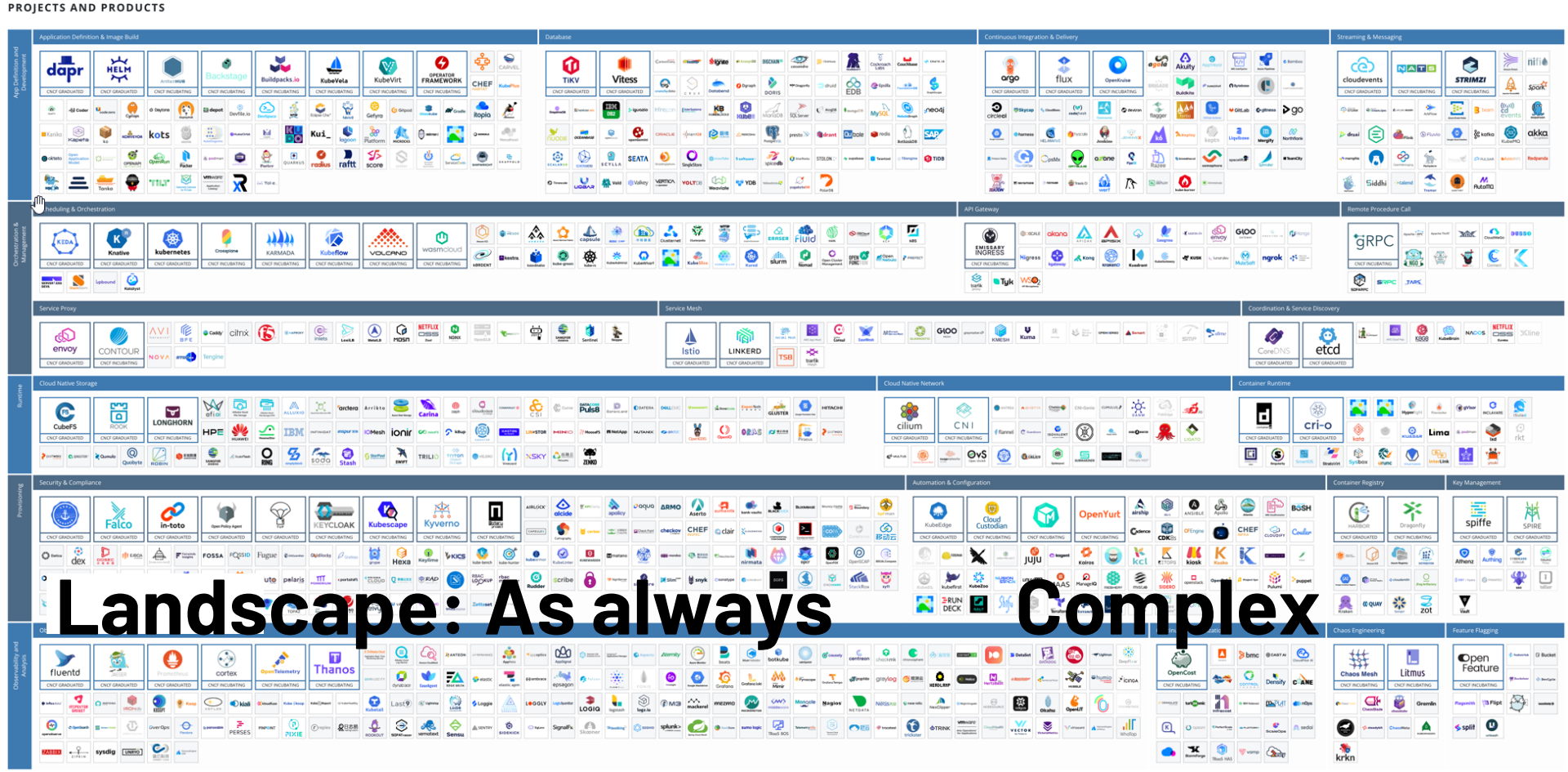
Jeg er lei, sliten og for gammel til Kubernetes.

Automatic fra platform siden



og jeg bidrar ikke til selskapets bunnlinje.

mvpdagen.no





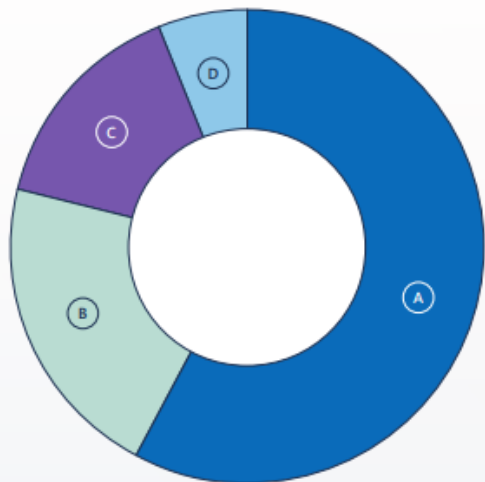
"Perfection is lots of little things done right"

-- Marco Pierre White

Container security in focus

Cloud threat infection types

100 days January-April 2025

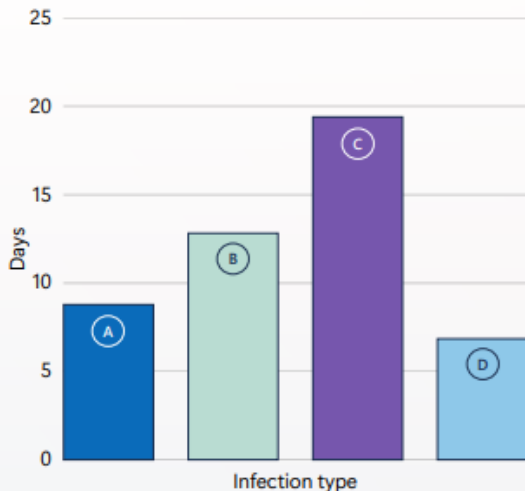


%

A. Crypto miner	58
B. Credential theft	21
C. Known attack tools	15
D. Web shells	6

Median infection time by infection type

100 days in January-April 2025



Days

A. Crypto miner	8.7
B. Credential theft	12.7
C. Known attack tools	19.3
D. Web shells	6.8

Most compromised containers are attacked within the first 48 hours of deployment. This emphasizes the critical need for immediate runtime protection.

Cryptomining dominates the attack landscape.

Cryptojacking is the most prevalent threat in Kubernetes environments, exhibiting the fastest median time to compromise—less than two days post-deployment.

Credential theft attacks take longer to manifest.

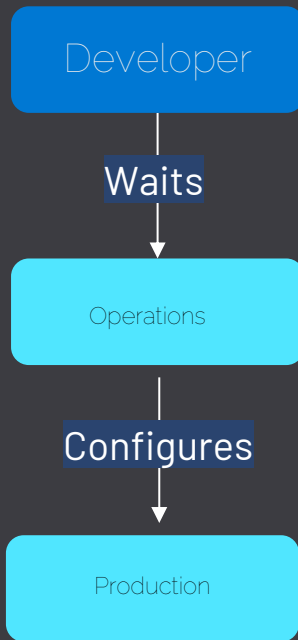
These attacks, the second most common type observed, had the highest median infection time, occurring approximately 3.5 days after container creation.

Long-tail attacks are a risk.

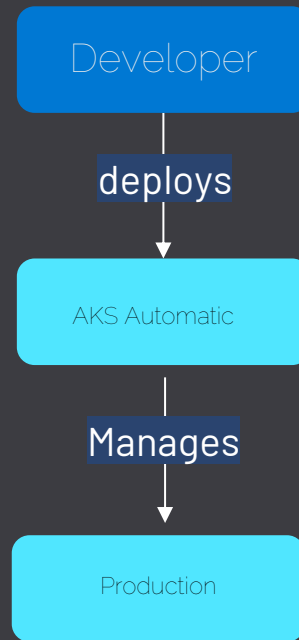
While most attacks occur early, outliers with significantly delayed infection highlight the importance of sustained monitoring beyond initial deployment.

Developer Experience

Idag



Etter



Kitchen Layout | Infrastructure

Order System |  Kubernetes Control Plane



Prep Stations /
Workload
Management



Quality control/
Security



Inventory /
Resources



Service /
Endpoints



Demo: Deployment Options

mvpdagen.no




Demo: NAP + KEDA

mvpdagen.no

Auto preconf vs default

Top Preconf instillinger vs standard

- 
- Node Autoprovisioning & Automatic Scaling
 - Standard Tier with Uptime SLA
 - Azure RBAC for Kubernetes
 - API Server VNet Integration
 - Workload Identity + OIDC
 - Deployment Safeguards*
 - Automatic Cluster Upgrades
 - Image Cleaner
 - Locked Node Resource Group

Bruker vi dette da?

Anders?

Martin?



Brukes I non-prod (CDC)

Ikke ennå

AKS Auto GA

Generally Available: AKS Automatic

Azure Kubernetes Service (AKS)










■ ■ ■ LAUNCHED

GENERAL AVAILABILITY
September 2025

Hva så? Hvorfor skulle vi bry oss..

mvpdagen.no

AKS Safeguards

Name ↕	Reference ID ↕	Effect type ↑
 Prints a message if a mutation is applied	printmutationsannotations	Audit
 Must Have Anti Affinity Rules or Topology Spread Constraints Set	podenforceantiaffinityinkube...	Deny
 Kubernetes clusters should use Container Storage Interface(CSI) driver StorageClass	ensurecsidriverstorageclass	Deny
 No AKS Specific Labels	restrictedlabelsinkubernetesc...	Deny
 Ensure cluster containers have readiness or liveness probes configured	ensureprobesconfiguredinku...	Deny
 Kubernetes cluster services should use unique selectors	uniqueserviceselectors	Deny
 Reserved System Pool Taints	restrictedtaintsinkubernetesc...	Deny
 Cannot Edit Individual Nodes	restrictednodeeditsinkuberne...	Deny
 Kubernetes cluster container images should not include latest image tag	imagesdonotuselatest	Deny

Probe Type

Purpose

Action on Failure

Liveness Probe

Checks if the application is **running and healthy** (e.g., not deadlocked).

Restarts the container to fix an internal issue.

Readiness Probe

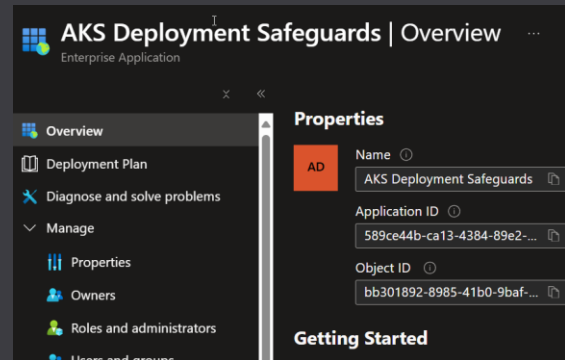
Checks if the application is **ready to serve traffic** (e.g., finished initializing).

Removes the Pod from Service Endpoints, stopping traffic to the Pod but *without restarting the container*.

AKS Safeguard policy

- Preconf på AKS Automatic
- Eneste mate kontrollere disse på eller skru av er exclusions.

Probe Type	Purpose	Action on Failure
Liveness Probe	Checks if the application is running and healthy (e.g., not deadlocked).	Restarts the container to fix an internal issue.
Readiness Probe	Checks if the application is ready to serve traffic (e.g., finished initializing).	Removes the Pod from Service Endpoints , stopping traffic to the Pod but <i>without restarting the container</i> .



Name : AKS Deployment Safeguards Policy Assignment

Definition version (preview) : 1.9.*-preview

Description : This policy assignment is owned by Azure Kubernetes Service (AKS).

Update with cli?

Description ⓘ

This policy assignment is owned by Azure Kubernetes Service (AKS). To make modifications, use the Azure CLI as shown in the docs here: <https://aka.ms/aks/guardrails>.

```
az aks safeguards update -g t-aks -n t-secops-aks --excluded-ns cert-manager vectr
(RequestNotAllowedBecauseAssociatedClusterIsAutomaticCluster) The request is not allowed because t-secops-aks is an automatic cluster. Resource ID: "/subscriptions/b23edb10-7875-4205-b250-edfaa0753397/resourceGroups/t-aks/providers/Microsoft.ContainerService/managedClusters/t-secops-aks/providers/Microsoft.ContainerService/deploymentSafeguards/default". Correlation ID: "2b90ca95-f557-48ee-9446-9af70917202a". Operation ID: "84aca542-448-4aad-a243-b84cfc2deddb"
Code: RequestNotAllowedBecauseAssociatedClusterIsAutomaticCluster
Message: The request is not allowed because t-secops-aks is an automatic cluster. Resource ID: "/subscriptions/b23edb10-7875-4205-b250-edfaa0753397/resourceGroups/t-aks/providers/Microsoft.ContainerService/managedClusters/t-secops-aks/providers/Microsoft.ContainerService/deploymentSafeguards/default". Correlation ID: "2b90ca95-f557-48ee-9446-9af70917202a". Operation ID: "84aca542-6d48-4aad-a243-b84cfc2deddb"
```

✓ ⓘ Create policy assignment	Succeeded	an hour ago	Thu Oct 02 ...	CS NonProd Test SecOps	AKS Deployment
ⓘ Create policy assignment	Started	an hour ago	Thu Oct 02 ...	CS NonProd Test SecOps	AKS Deployment
✓ ⓘ Create policy assignment	Succeeded	an hour ago	Thu Oct 02 ...	CS NonProd Test SecOps	AKS Deployment
ⓘ Create policy assignment	Started	an hour ago	Thu Oct 02 ...	CS NonProd Test SecOps	AKS Deployment
✓ ⓘ Create policy assignment	Succeeded	a day ago	Wed Oct 01...	CS NonProd Test SecOps	admin-cloud-OD
ⓘ Create policy assignment	Started	a day ago	Wed Oct 01...	CS NonProd Test SecOps	admin-cloud-OD

AKS auto – networking/ingress

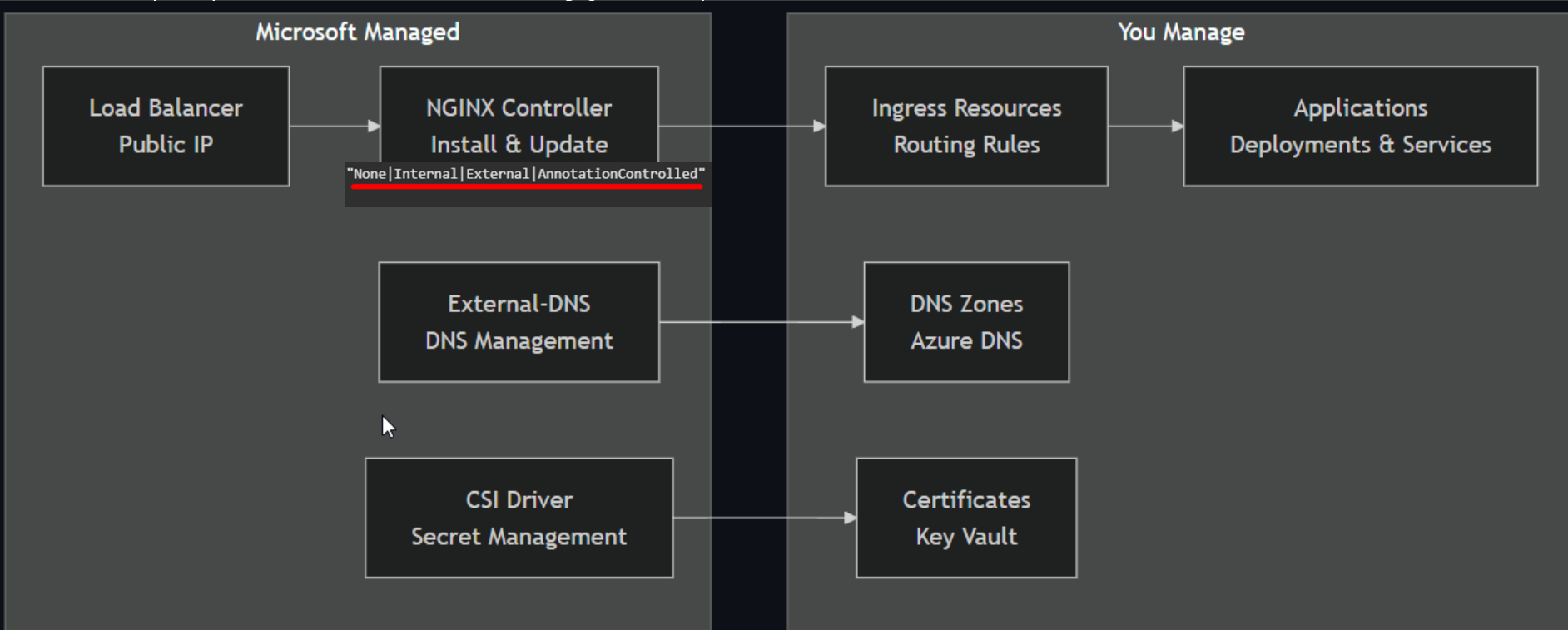
Nginx som standard – rett på internet uten WAF

App-Routing option in AKS

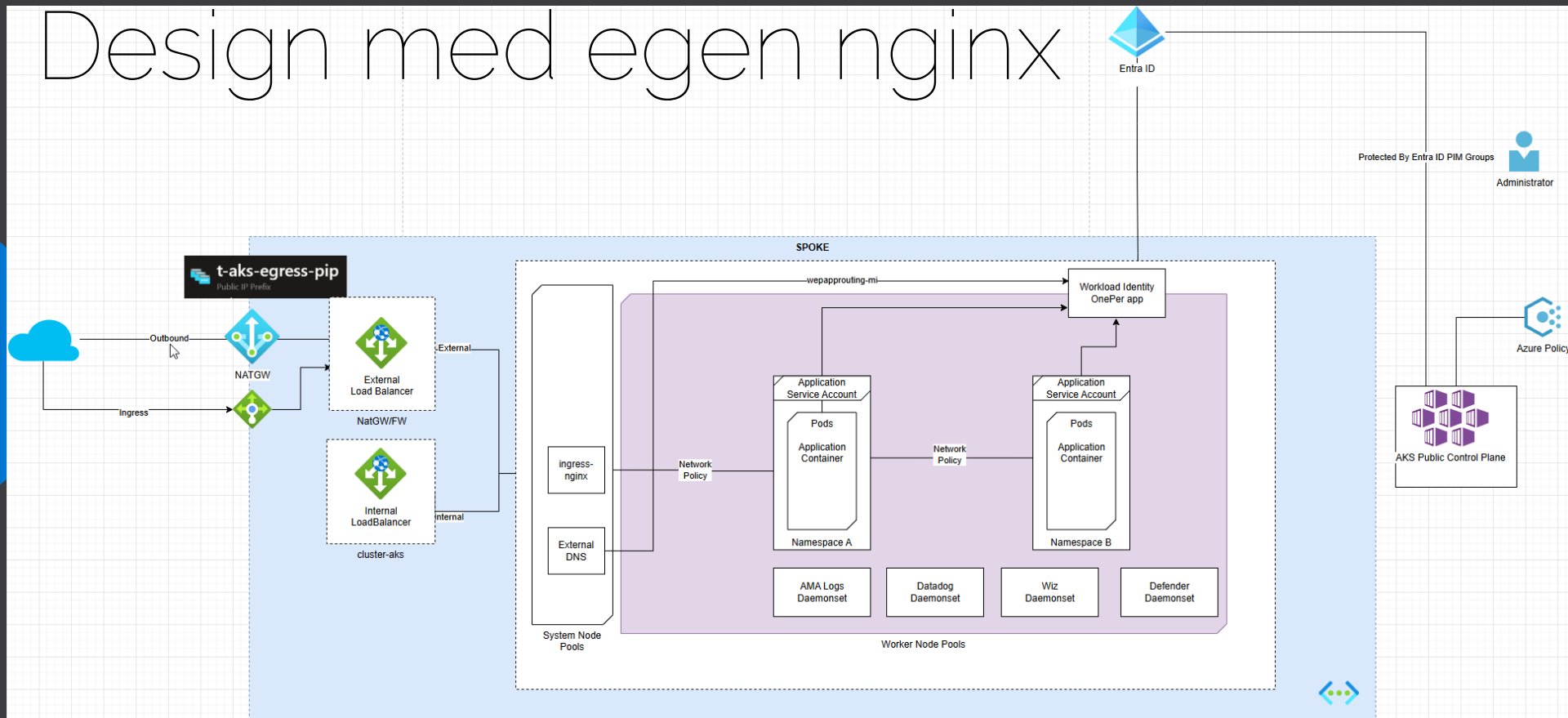
Det er flere valg via code enn portalen

Må være klar for å gå over til Gateway API

App-routing option



Design med egen nginx



AKS VS GKE Versjoner

Latest: 1.33.3

Rapid: 1.34

Sweden Central

[1.33.3](#), [1.33.2](#), [1.33.1](#), [1.33.0](#)
[1.32.7](#), [1.32.6](#), [1.32.5](#), [1.32.4](#), [1.32.3](#)
[1.31.11](#), [1.31.10](#), [1.31.9](#), [1.31.8](#), [1.31.7](#)
[1.30.100\(LTS\)](#), [1.30.14\(LTS\)](#)
[1.29.100\(LTS\)](#), [1.29.15\(LTS\)](#)
[1.28.102\(LTS\)](#), [1.28.101\(LTS\)](#)

Minor version (release date)	Rapid		Regular		Stable	
	Available ¹	Auto Upgrade ²	Available ¹	Auto Upgrade ²	Available ¹	Auto Upgrade ²
1.28	2023-09-04	2024-01-05	2023-11-30	2024-06-11	2024-01-05	2024-07-23
1.29	2024-01-05	2024-04-15	2024-01-25	2024-07-09	2024-06-11	2024-08-09
1.30	2024-04-29	2024-07-30	2024-07-30	2024-09-17	2024-08-13	2024-09-24
1.31	2024-08-20	2024-09-17	2024-10-22	2025-03-11	2025-01-28	2025-04-29
1.32	2024-12-17	2025-03-11	2025-02-11	2025-05-13	2025-03-04	2025-07-22
1.33	2025-05-06	2025-06-10	2025-06-03	2025-09-09	2025-07-22	2025-10-14
1.34	2025-09-02	2025-10-21 ⁵	2025-10-21 ⁵	2026-01 ⁴	2025-12 ⁴	2026-Q1 ⁴


Bør du velge AKS automatic?



Ja, men pass på et par ting

mvpdagen.no

Bør du velge AKS automatic?

- 
- Ingress, vurder om standard er sikker nok for dere.
 - Eksisterende deployments må tilpasses.

Bør du velge AKS automatic?



AKS Automatic er Microsoft sin mening
om hvordan Kubernetes bør se ut

Bør du velge AKS automatic?



... om du ikke liker den, dropp det.