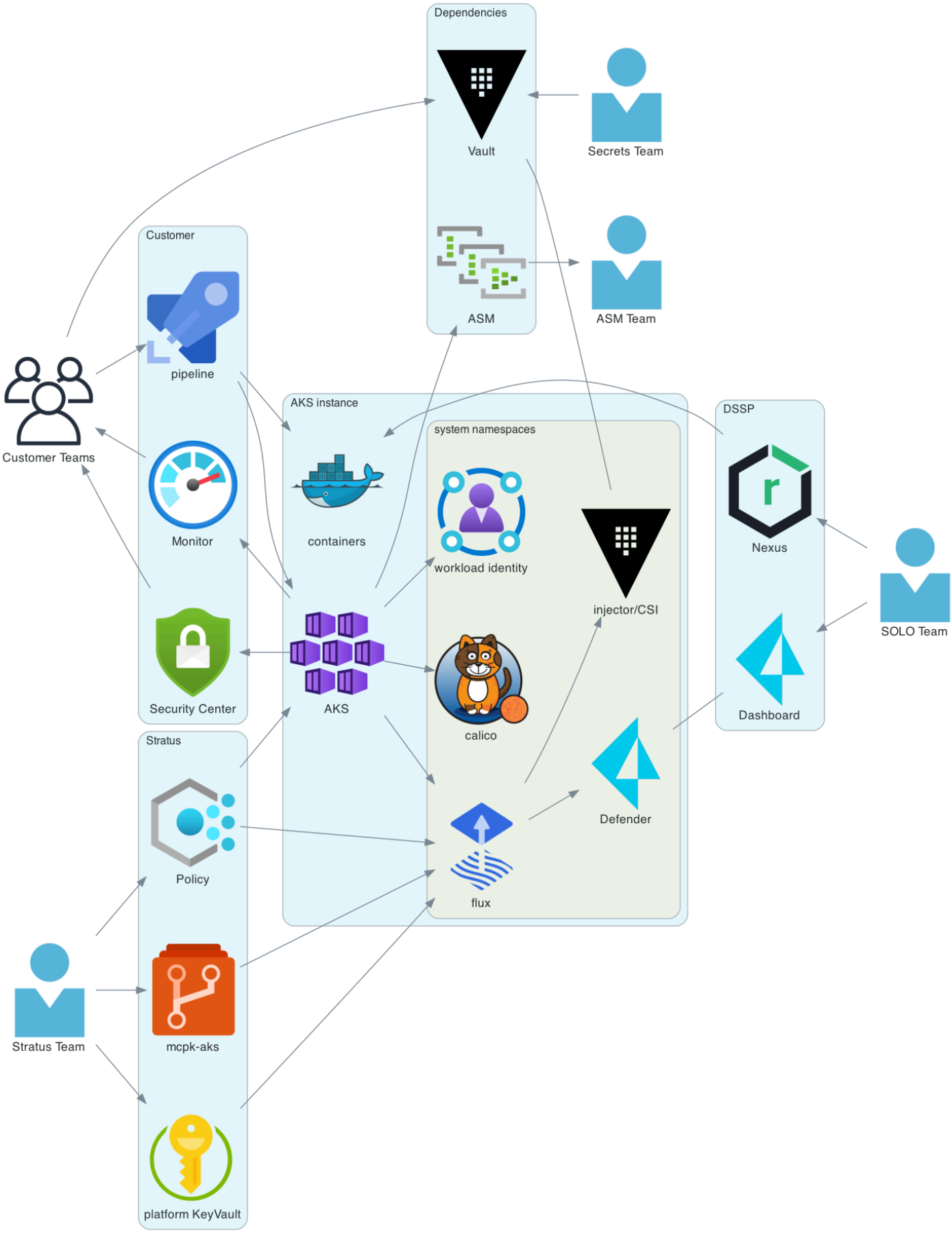
Mandatory Components

Last updated by | Michele Cereda | Nov 28, 2023 at 1:53 PM GMT+1

The FSCP Secure Context solution for AKS is intended to provide some guardrails while allowing Customers to use the most vanilla AKS cluster possible.
Such guardrails will enforce compliance by denying the application of non-compliant configurations and by automatically installing some mandatory components.

Mandatory components which are enabled for AKS in FSCP 3.0 include:

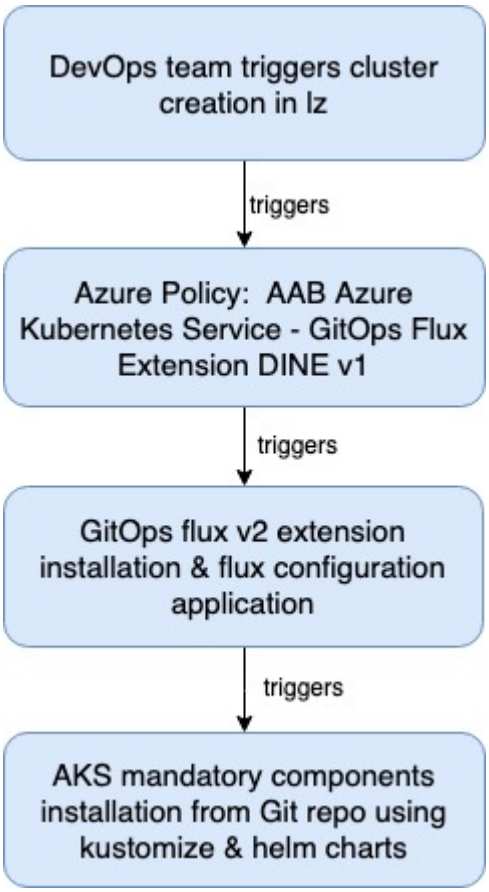
- The Azure Policy AKS **add-on** for Kubernetes.
- The GitOps Flux v2 AKS **extension**.
- Prisma Cloud Compute (ex Twistlock) agents.
  Only in A and P.
- Calico Network Policies (`deny-all`).
- ~~Fluent-bit~~
  suspended until the backend service is ready



FSCP 3.0 AKS - Components

Contents

Installation Flow



Prerequisites

Necessary resource providers and features are enabled on the subscription.

Features

- AKS-ExtensionManager

Providers

- Microsoft.Kubernetes

- Microsoft.ContainerService
- Microsoft.KubernetesConfiguration
- Microsoft.PolicyInsights

Mandatory Components

AKS add-on: Azure Policy for Kubernetes

Azure Policy for Kubernetes is an AKS *add-on* from Microsoft which deploys Gatekeeper and integrates the policies of Gatekeeper with Azure Policy.
Its installation is triggered by the cluster's `addonProfiles.azurePolicy.enabled` attribute, and it will be installed during cluster deployment. If for some reason it fails, the whole cluster deployment will fail.

AKS extension: GitOps Flux v2

The 'GitOps Flux v2' AKS *extension* lets us configure AKS to automatically and **cyclically** apply the contents of the git repository storing all mandatory applications.
This is preconfigured and installed on all clusters via the "AAB Azure Kubernetes Service - GitOps Flux Extension DINE v1" Azure Policy.

Prisma Cloud Compute agents

Prisma Cloud Compute agents are required for **runtime security** for 3.0 clusters.
The application is included in Flux's configuration, and it gets installed right after the cluster creation.

We are mainly interested in the following three features:

- Runtime protection
- Vulnerability management
- Visibility

Calico Network Policies

Calico is the tool of choice to secure the network with**in** clusters.

Flux will deploy a `deny-all` global network policy to restrict Pod-to-Pod communication within the same cluster.
Customers **will** need to **explicitly allow** each and every Pod-to-Pod / Pod-to-other network flow they require.

Fluent-bit

> *suspended until the backend service is ready*

The ASM and SSM teams need to receive logs centrally in order to be able to analyze application logs from a central location.
Fluent-bit is included in Flux's configuration, and it gets installed right after the cluster creation.