

# Mastering Service Orchestration: How Saxo Blueprint Leverages Kubernetes Operators and GitOps

Jimmi Hested



# Saxo Bank

- **Founded in Copenhagen in 1992**
- **Pioneered Online Trading in 1998**
- Global Presence: Trusted by over 1 million clients worldwide, with **USD 100 billion** in client assets and operations in 15 countries.
- **Platform Excellence:** Regulated access to 71,000+ financial instruments on award-winning platforms.

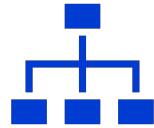


# whoami

- Jimmi Hested - Developer Platform Architect
- 3+ years with Kubernetes development
- 1+ year building Kubernetes operators
- Formerly part of Saxo Bank's Cloud Center of Excellence
- 10+ years of DevOps experience
- 15+ Developer
- PowerPoint Wizard
- Family, biking, and table tennis



# Blueprint Overview



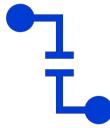
## Centralized Configuration

The Service Definition serves as a single source of truth for each service, making it easier to manage and audit configurations.



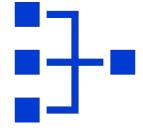
## Automation

The Blueprint automates the provisioning and management of services, reducing manual intervention and the risk of human errors.



## Continuous Reconciliation

Following the Kubernetes Operator pattern ensures that services always align with the desired state.



## Version Control

Version control for Service Definition files enables change tracking and auditing.



## CI/CD Integration

Seamless integration with CI/CD pipelines streamlines the deployment process.



# Why Service Blueprint?



# Classic Service Management

- Manual identity and role assignments.
- Complex firewall configurations.
- DNS name setup.
- Challenges with decommissioning services.
- Security risks and inefficiencies.

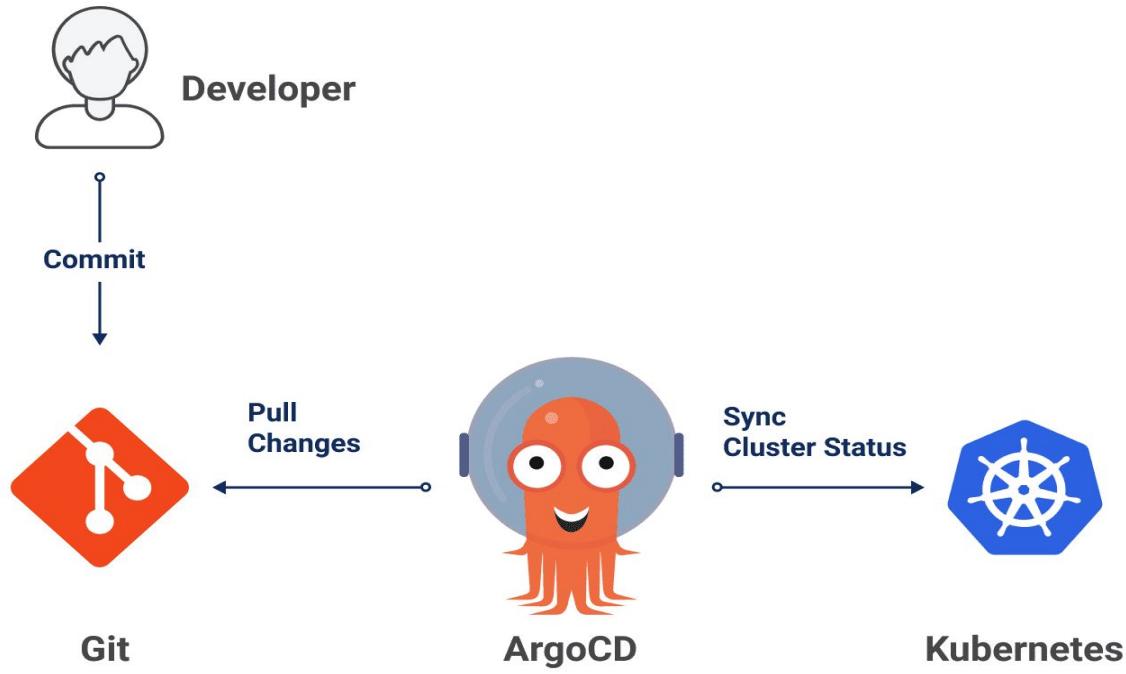


# Classic Resource Deployment

- Complex and Inconsistent Process
- Drift-Prone
- Manual and Slow
- Poor feedback
- Difficult Disaster Recovery

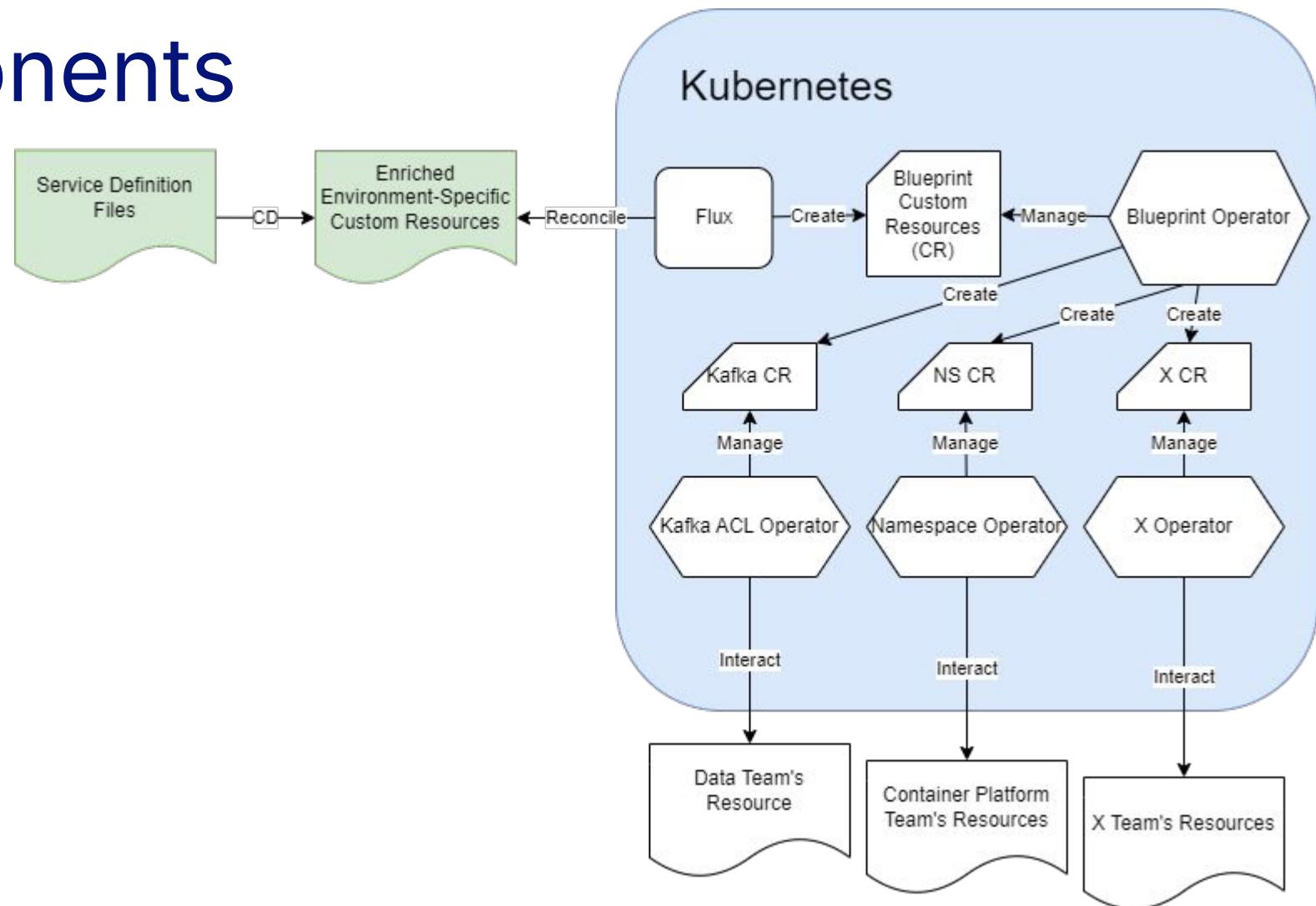


# Kubernetes and GitOps



# Blueprint Components

- Service Catalog (YAML)
- Blueprint Operator
- Custom Ressource Definition
- Kubernetes Operator
- External API / Existing Automation



# Service Catalog

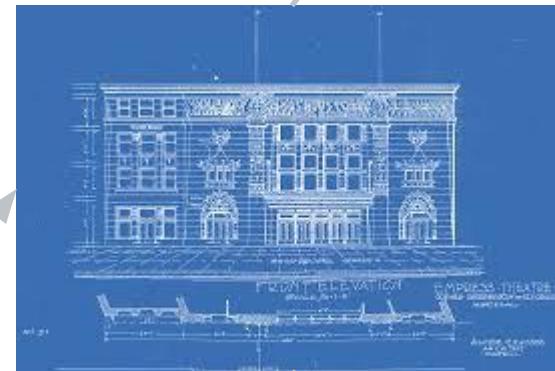
- Central repository hosted in GIT
- Based on Backstage format
- Built-in approvals via Pull Request Validation
- Environment Invariant representation

```
1 # yaml-language-server: $schema=https://git/artifacts/schema.json
2 apiVersion: backstage.io/v1alpha1
3 kind: Component
4 metadata:
5   annotations:
6     dev.azure.com/project-repo: PlatformKnowledgebase
7   description: Service collection for various platform services, including
8     PlatformKnowledgebase, PlatformContent, and PlatformWebsite.
9   name: PlatformKnowledgebase
0 spec:
1   lifecycle: production
2   owner: group:KnowledgeBaseDevelopers
3   saxo:
4     groups:
5       deployment: group:KnowledgeBaseDevelopers
6       managedBy: user:xyz
7       ownedBy: user:xyz
8       system: PlatformKnowledgebase
9       type: service
```

# Blueprint Operator



```
1 # yaml-language-server: $schema=https://git.artifacts/schema.json
2 apiVersion: backstage.io/v1alpha1
3 kind: Component
4 metadata:
5   annotations:
6     dev.azure.com/project-repo: PlatformKnowledgebase
7     description: Service collection for various platform services, including
8       PlatformKnowledgebase, PlatformContent, and PlatformWebsite.
9     name: PlatformKnowledgebase
10    spec:
11      lifecycle: production
12      owner: group:KnowledgeBaseDevelopers
13      sans:
14        groups:
15          deployment: group:KnowledgeBaseDevelopers
16          managedBy: user:xyz
17          ownedBy: user:xyz
18        system: PlatformKnowledgebase
19        type: service
```



gRPC

kafka

Microsoft  
Entra ID

SAXO  
BE INVESTED

"One  
click"

# Blueprint

```
1  apiVersion: backstage.io/v1alpha1
2  kind: Component
3  metadata:
4    annotations:
5      kubernetes.io/namespace: trading
6    description: This client is used for trading
7    name: Public.Trading.Client
8  spec:
9    consumesApis:
10   - instruments-v2
11   - trading_client-trades
12   - projections/read
13  lifecycle: production
14  owner: group:Trading
15  saxo:
16    groups:
17      support: group:Trading
18    managedBy: user:JaneDoe
19    ownedBy: user:JohnDoe
20    shortName: tradeclient
21  system: Trading
22  type: service
23
```



# Blueprint

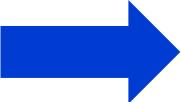
```
1 apiVersion: backstage.io/v1alpha1
2 kind: Component
3 metadata:
4   annotations:
5     kubernetes.io/namespace: trading
6   description: This client is used for trading
7   name: Public.Trading.Client
8 spec:
9   consumesApis:
10    - instruments-v2
11    - trading_client-trades
12    - projections/read
13   lifecycle: production
14   owner: group:Trading
15   saxo:
16     groups:
17       support: group:Trading
18     managedBy: user:JaneDoe
19     ownedBy: user:JohnDoe
20     shortName: tradeclient
21   system: Trading
22   type: service
23
```

Namespace: trading



# Blueprint

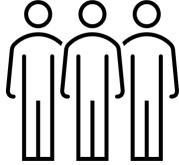
```
1  apiVersion: backstage.io/v1alpha1
2  kind: Component
3  metadata:
4    annotations:
5      kubernetes.io/namespace: trading
6    description: This client is used for trading
7    name: Public.Trading.Client
8  spec:
9    consumesApis:
10   - instruments-v2
11   - trading_client-trades
12   - projections/read
13  lifecycle: production
14  owner: group:Trading
15  saxo:
16    groups:
17      support: group:Trading
18    managedBy: user:JaneDoe
19    ownedBy: user:JohnDoe
20    shortName: tradeclient
21  system: Trading
22  type: service
23
```



You, 3 months ago | 2 authors (Kristian Bø)

```
apiVersion: infra.dk/v1
kind: NamespaceRequest
metadata:
  name: namespace-trading
  namespace: default
spec:
  name: trading
  serviceNow:
    number: APM000
    managedBy: JohnDoe
```





Namespace: trading



```
Context: laks006nl          <0> all   <a> Atta
Cluster: laks006nl           <1> default <ctrl-d> Delete
User: clusterUser_lgr006aksnl_laks006nl <d> Desc
K9s Rev: v0.32.5 ↗ v0.32.7 <e> Edit
K8s Rev: v1.29.7             <f> Help
CPU: 24%                   <shift-j> Jump
MEM: 40%
```

NAME	PF	READY	STATUS	RESTARTS	CP
blueprint-engine-svc-28868185-cmfr	*	0/1	Completed	0	
blueprint-engine-svc-28868190-44c4t	●	0/1	Completed	0	
blueprint-engine-svc-28868195-wbkgf	●	0/1	Completed	0	
operators-activedirectory-5f86b96fdb-czh9l	●	2/2	Running	0 19	
operators-activedirectory-5f86b96fdb-fj858	●	2/2	Running	0	
operators-blueprint-d5c5dcfc-dmtpt	●	2/2	Running	0	
operators-blueprint-d5c5dcfc-jn2wb	●	2/2	Running	0	
operators-certificate-c44f749b4-jsg8s	●	2/2	Running	0	
operators-certificatedb-758745df66-zbrvc	●	2/2	Running	0	
operators-kafkaacls-758745df66-dqcc2	●	2/2	Running	1	
operators-kafkaacls-758745df66-fswfn	●	2/2	Running	3	
operators-namespacerequests-7985b8869d-5lfxl	●	2/2	Running	0	
operators-sqlidentity-864b5d8f89-7hpbt	●	2/2	Running	0	
operators-sqlidentity-864b5d8f89-44zpj	●	2/2	Running	0	
operators-sqlidentity-864b5d8f89-gms9q	●	2/2	Running	0	

# Blueprint

```
1 apiVersion: backstage.io/v1alpha1
2 kind: Component
3 metadata:
4   annotations:
5     kubernetes.io/namespace: trading
6   description: This client is used for trading
7   name: Public.Trading.Client
8 spec:
9   consumesApis:
10    - instruments-v2
11    - trading_client-trades
12    - projections/read
13   lifecycle: production
14   owner: group:Trading
15   saxo:
16     groups:
17       support: group:Trading
18       managedBy: user:JaneDoe
19       ownedBy: user:JohnDoe
20     shortName: tradeclient
21   system: Trading
22   type: service
23
```

Namespace: trading



Identity: tradeclient



# Blueprint

```
1 apiVersion: backstage.io/v1alpha1
2 kind: Component
3 metadata:
4   annotations:
5     kubernetes.io/namespace: trading
6   description: This client is used for trading
7   name: Public.Trading.Client
8 spec:
9   consumesApis:
10    - instruments-v2
11    - trading_client-trades
12    - projections/read
13   lifecycle: production
14   owner: group:Trading
15   saxo:
16     groups:
17       support: group:Trading
18       managedBy: user:JaneDoe
19       ownedBy: user:JohnDoe
20     shortName: tradeclient
21   system: Trading
22   type: service
23
```

Namespace: trading



Identity: tradeclient



Microsoft  
Entra ID

Topic: instruments-v2



SAXO  
BE INVESTED

# Blueprint

```
1  apiVersion: backstage.io/v1alpha1
2  kind: Component
3  metadata:
4    annotations:
5      kubernetes.io/namespace: trading
6      description: This client is used for trading
7      name: Public.Trading.Client
8
9    spec:
10   consumesApis:
11     - instruments-v2
12     - trading_client-trades
13     - projections/read
14   lifecycle: production
15   owner: group:Trading
16   saxo:
17     groups:
18       support: group:Trading
19       managedBy: user:JaneDoe
20       ownedBy: user:JohnDoe
21     shortName: tradeclient
22   system: Trading
23   type: service
```

Namespace: trading



Identity: tradeclient



Microsoft  
Entra ID

Topic: instruments-v2



Database: trading



# Blueprint

```
1  apiVersion: backstage.io/v1alpha1
2  kind: Component
3  metadata:
4    annotations:
5      kubernetes.io/namespace: trading
6      description: This client is used for trading
7      name: Public.Trading.Client
8
9    spec:
10   consumesApis:
11     - instruments-v2
12     - trading_client-trades
13     - projections/read
14
15   lifecycle: production
16   owner: group:Trading
17   saxo:
18     groups:
19       support: group:Trading
20       managedBy: user:JaneDoe
21       ownedBy: user:JohnDoe
22       shortName: tradeclient
23
24   system: Trading
25   type: service
```

Namespace: trading



Identity: tradeclient



Microsoft  
Entra ID

Topic: instruments-v2



Database: trading



API: projections/read



SAXO  
BE INVESTED

# Blueprint

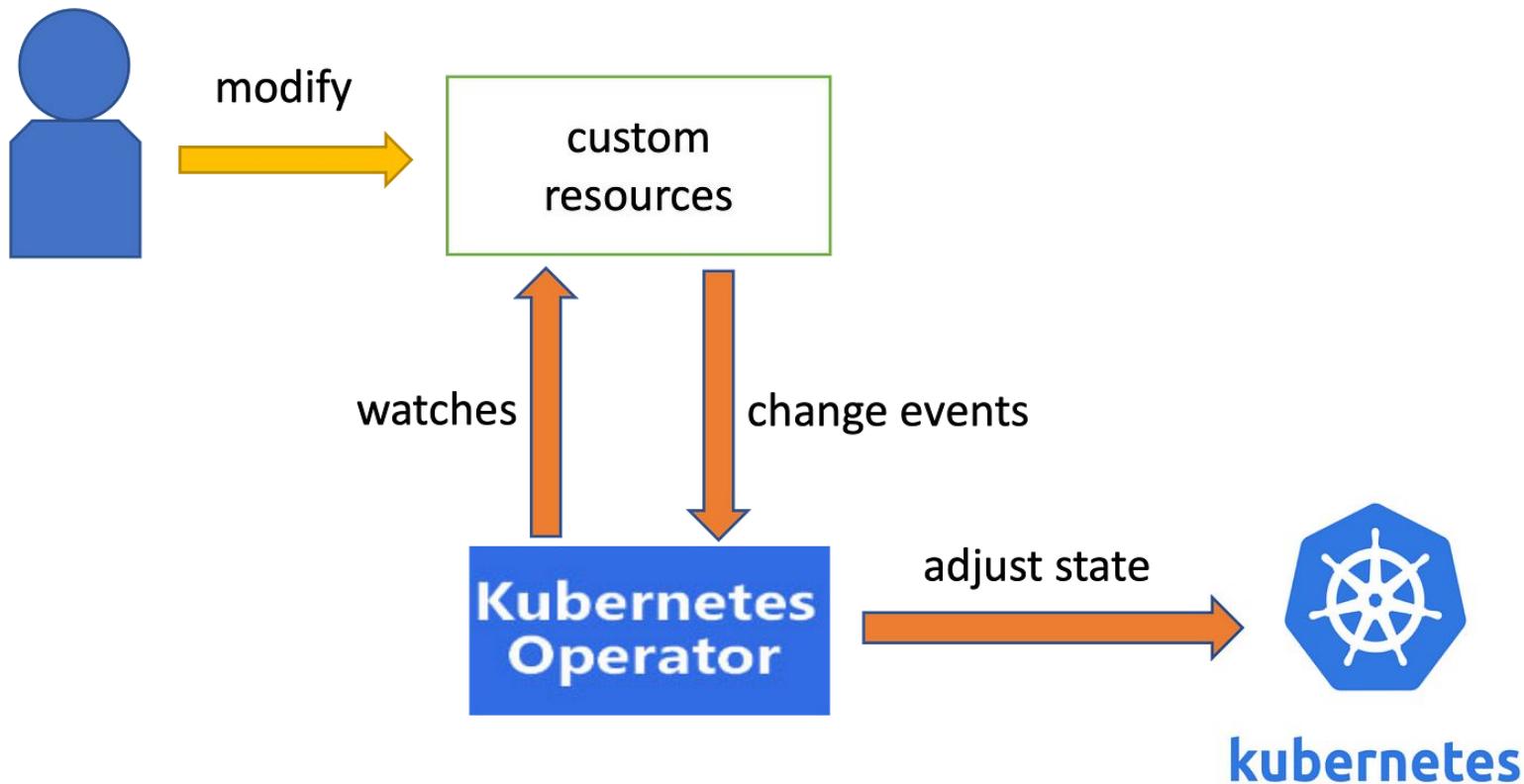
```
1 apiVersion: backstage.io/v1alpha1
2 kind: Component
3 metadata:
4   annotations:
5     kubernetes.io/namespace: trading
6   description: This client is used for trading
7   name: Public.Trading.Client
8 spec:
9   consumesApis:
10    - instruments-v2
11    - trading_client-trades
12    - projections/read
13   lifecycle: production
14   owner: group:Trading
15   saxo:
16     groups:
17       support: group:Trading
18     managedBy: user:JaneDoe
19     ownedBy: user:JohnDoe
20     shortName: tradeclient
21   system: Trading
22   type: service
23
```

```
1 apiVersion: backstage.io/v1alpha1
2 kind: API
3 metadata:
4   name: projections/read
5   spec:
6     type: grpc
7   ...
8 apiVersion: backstage.io/v1alpha1
9 kind: API
10 metadata:
11   name: instruments-v2
12   spec:
13     type: kafka
14   ...
15 apiVersion: backstage.io/v1alpha1
16 kind: API
17 metadata:
18   name: trading_client-trades
19   spec:
20     type: database
```

# Delegate Responsibility



# Operator Pattern



# Resource Operator

```
you, 5 months ago | 2 authors (you and one other)
1 apiVersion: sql.infra.dk/v1
2 kind: AzureSqlIdentity
3 metadata:
4   name: sqlidentity-access-request
5   namespace: default
6 spec:
7   server:
8     name: azure-sql-db
9     type: AzureSQLDatabase
10  database: Contoso
11  identity:
12    name: unique-client
13    type: ManagedIdentity
14  roles:
15    - name: Writer
16
```

```
public async Task<ReconcileResult<V2Alpha1AzureSqlIdentity>> ReconcileAsync(V2Alpha1AzureSqlIdentity entity, CancellationToken cancellationToken = default)
{
    AzureSqlDatabase azureSqlDatabase = await FindAzureSqlDatabaseOrThrowAsync(entity.Spec.Database, cancellationToken);
    return await ProvisionIdentities(entity, azureSqlDatabase, cancellationToken);
}

1 reference | Kristian Børner Jensen (KJEN), 53 days ago | 2 authors, 2 changes
public async Task<AzureSqlDatabase> FindAzureSqlDatabaseOrThrowAsync(string databaseName, CancellationToken cancellationToken = default)
{
    var databases = await _databaseRepository.ListByNameAsync(databaseName, cancellationToken);

    if (databases.Count() == 1)
    {
        return databases.Single();
    }
    else if (databases.Count() > 1)
    {
        var servers = string.Join(", ", databases.Select(x => x.GetServerName()).Distinct());
        throw new ReconcileException(
            EventStatusCodes.InternalError,
            $"Multiple databases found with name '{databaseName}'. Servers [{servers}]",
            AzSqlConditionReasons.MultipleServersFound,
            requeueAfter: TimeSpan.FromMinutes(20));
    }
    else
    {
        throw new ReconcileException(
            EventStatusCodes.UserError,
            $"No databases found with name '{databaseName}'",
            AzSqlConditionReasons.SqlDatabaseNotFound,
            requeueAfter: TimeSpan.FromMinutes(10));
    }
}

2 references | Kristian Børner Jensen (KJEN), 53 days ago | 2 authors, 2 changes
private async Task<ReconcileResult<V2Alpha1AzureSqlIdentity>> ProvisionIdentities(V2Alpha1AzureSqlIdentity entity, AzureSqlDatabase database, CancellationToken cancellationToken = default)
{
```



# What about monitoring?

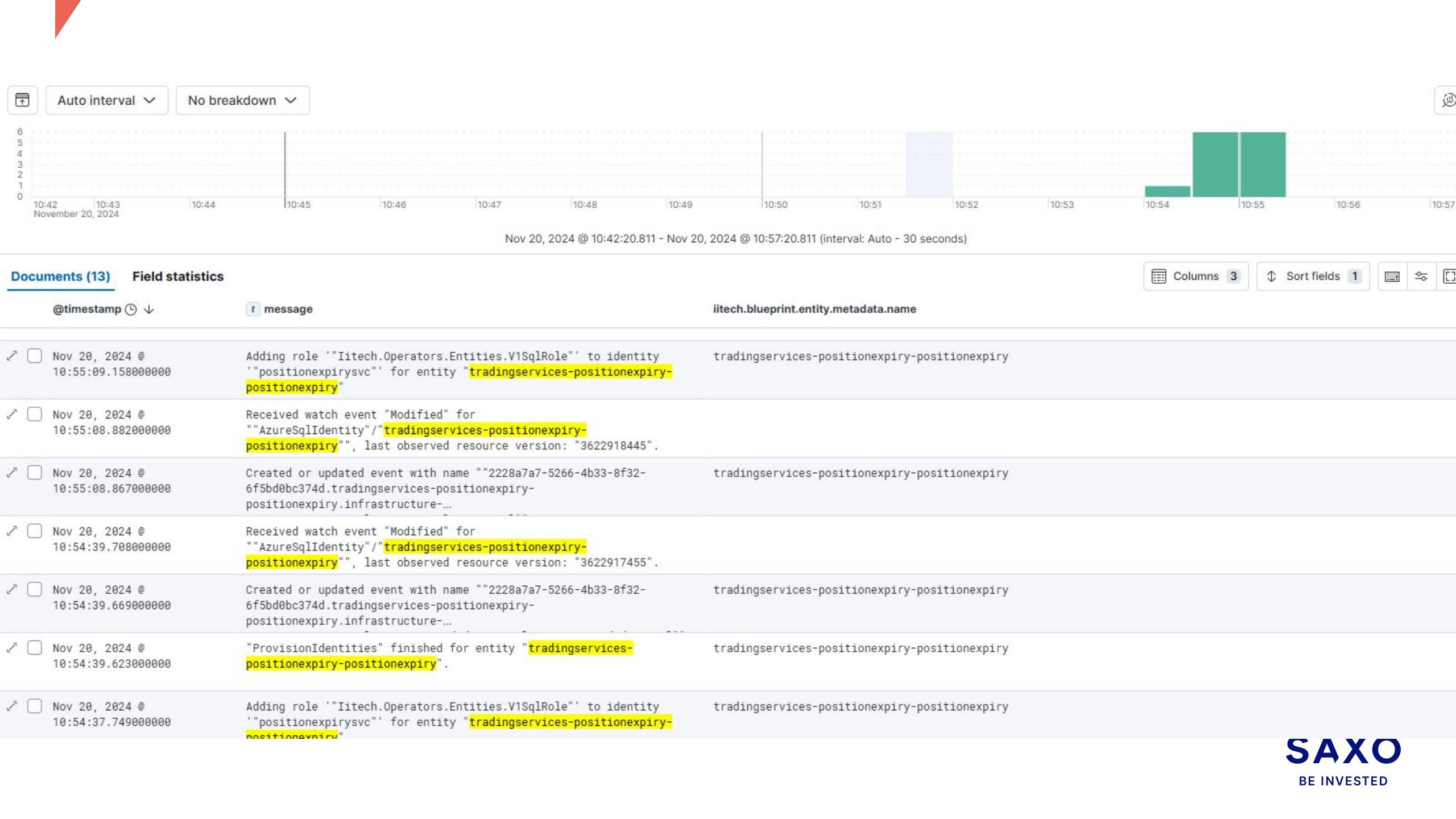
Cluster: daks006nl  
 User: clusterUser\_drg006aksnl\_daks006nl  
 K9s Rev: v0.32.5 ↳ v0.32.7  
 K8s Rev: v1.29.7  
 CPU: 35%  
 MEM: 29%

<1> default <2> Describe  
 <e> Edit <?> Help  
 <y> YAML



### Blueprints(infrastructure-automation)[853]

NAME↑	READY	REASON	AGE
clientmanagement-client360view	True	ReconciliationSucceeded	57d
clientmanagement-clientmanagementoperationsapp	True	ReconciliationSucceeded	97d
clientmanagement-clientmanagementtrading-api	True	ReconciliationSucceeded	97d
clientmanagement-enterprise-idgenerator	True	ReconciliationSucceeded	57d
clientmanagement-enterprise-kyc-clientmatchingservice	True	ReconciliationSucceeded	97d
clientmanagement-enterprise-kyc-identitydocumentprocessing	True	ReconciliationSucceeded	57d
clientmanagement-enterprise-onboarding	True	ReconciliationSucceeded	97d
clientmanagement-enterprise-renewal	True	ReconciliationSucceeded	97d
clientmanagement-partnerclientmanagement	True	ReconciliationSucceeded	97d
clientmanagement-partydataintegration	True	ReconciliationSucceeded	57d
clientmanagement-qualityassuranceandcontrol	True	ReconciliationSucceeded	97d
clientmanagement-trading	True	ReconciliationSucceeded	97d
clientmanagement-trading-configuration	True	ReconciliationSucceeded	57d
clientpricing-feemanagementoperationsapp	True	ReconciliationSucceeded	57d
clientpricing-feesmanagement	True	ReconciliationSucceeded	97d
clientpricing-feesmanagementextension	True	ReconciliationSucceeded	57d
clientpricing-globaltaxoperationsapp	True	ReconciliationSucceeded	57d
clientpricing-marginrequirementnfe	True	ReconciliationSucceeded	57d
clientpricing-pricingandaccountconfigurationoperationsapp	True	ReconciliationSucceeded	57d
clientpricing-rewardmanagementsystem	True	ReconciliationSucceeded	97d
clientpricing-rewardmanagementsystem-offerservice	True	ReconciliationSucceeded	57d
closeoutbridgeservice	True	ReconciliationSucceeded	57d
cloudautomation	True	ReconciliationSucceeded	57d
cloudcontrols	True	ReconciliationSucceeded	57d
cloudinfra-appserviceenvironment	True	ReconciliationSucceeded	57d
cloudinfra-virtualnetwork	True	ReconciliationSucceeded	57d



Kind

Component

Type

all

PERSONAL

Owned 0

Starred 3

SAXO BANK

All 890

OWNER

LIFECYCLE

## All components (890)

Filter

NAME	SYSTEM	OWNER	TYPE	LIFECYCLE	DESCRIPTION	TAGS	ACTIONS
Accounting.FinanceProcessManagementApp	AccountingHub	AccountingHub Support	service	production	This is front end...		
ADKeys	ActiveDirectory	EPEDevOps Support	service	pre-production	Make AD Key...		
AIResearch.DatabricksWorkspace	ACE	DataEngineeringBDS Support	service	production	For analytical...		
AirflowSharedService	AirflowShared Services	EPEDataIntegration Support	service	production	Airflow is an ope...		
AM.Audit.Service	AMProjection	AssetManagement Support	service	implementing	A business servi...		
Am.Projects.Grpc.Service	AMProjection	AssetManagement Support	service	implementing	This business...		
Am.Projects.OAPIOService	AMProjection	AssetManagement Support	service	production	This business...		
AM.Projecti...	AMProjection	AssetManagement Support	service	implementing	This business...		

# Interesting.Service ☆

Owner  
CorpAct Support

Lifecycle  
production

⋮

OVERVIEW

CI/CD

API

DEPENDENCIES

DOCS

KUBERNETES

BLUEPRINT

PULL REQUESTS

## Blueprints by Cluster

### Development

2 resources 4 / 5 conditions ready X ▾

### Test

2 resources 4 / 5 conditions ready X ▾

### Sim

1 resources 1 / 1 conditions ready ✓ ▾

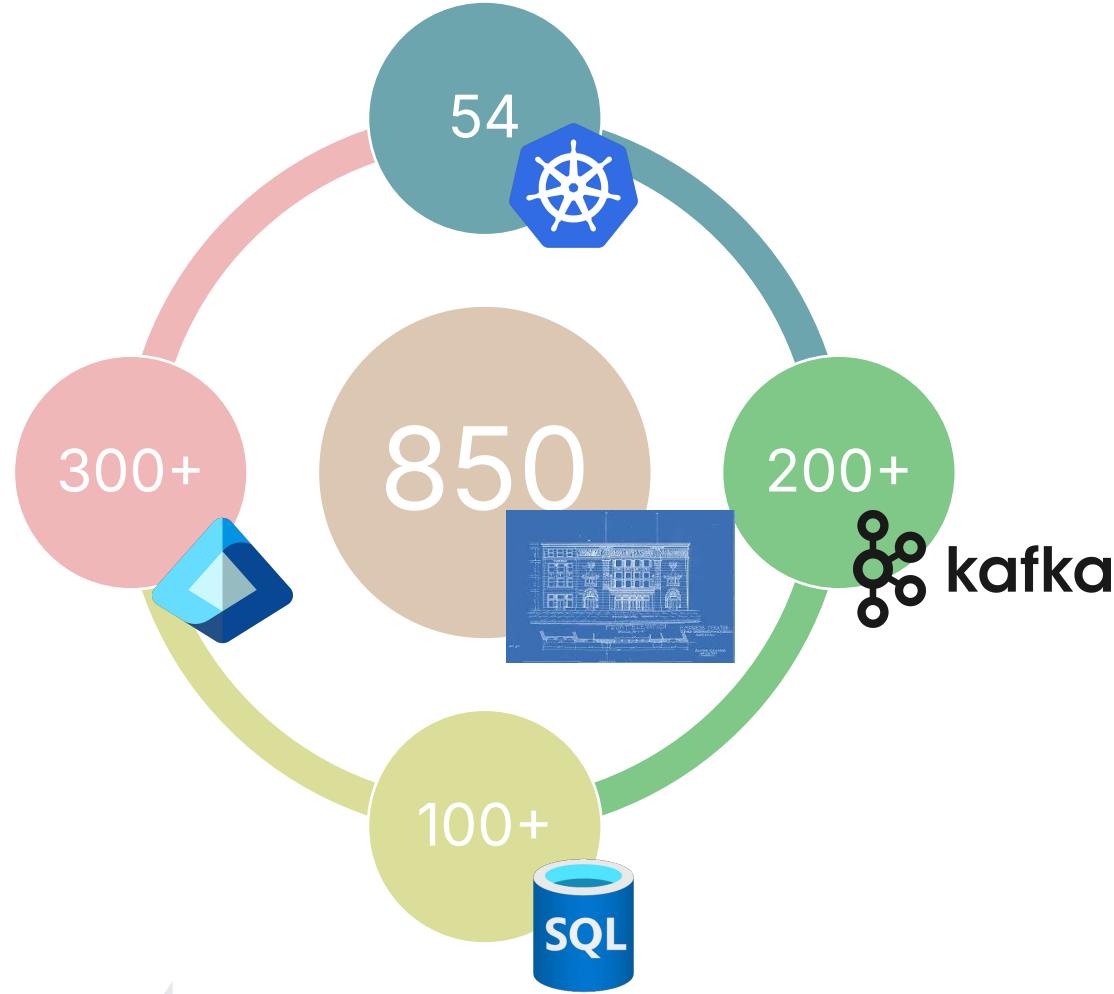
### Live

3 resources 7 / 8 conditions ready X ▲

### Blueprint

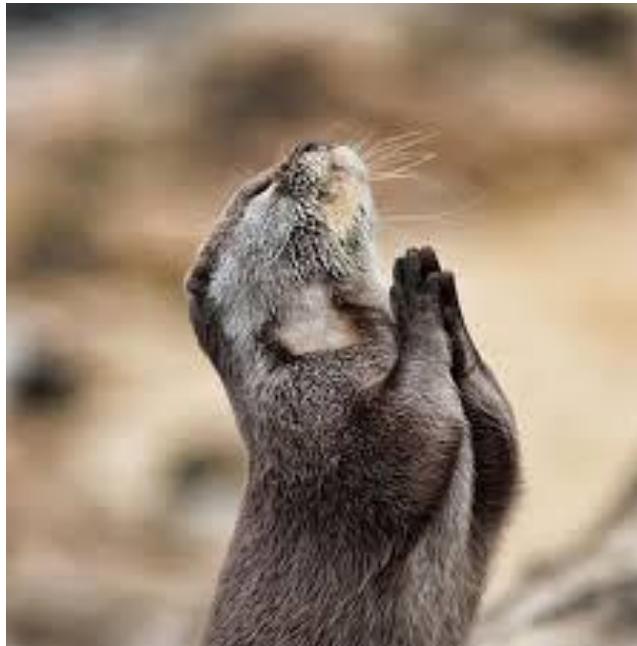
1 resources 5 / 6 conditions ready X ▾

# Current State

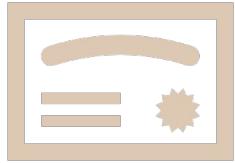


# Demo

If the internet god is with me...



# Next Step



Certificate



DNS



Firewall

# Classic Service Management

- Manual identity and role assignments.
- Complex firewall configurations.
- DNS name setup.
- Challenges with decommissioning services.
- Security risks and inefficiencies.



# Classic Service Management

- Identity and role assignments auto provisioned.
- Firewall automation.
- DNS automation.
- ~~Challenges with decommissioning services.~~
- ~~Security risks and inefficiencies.~~



# Classic Resource Deployment

- Complex and Inconsistent Process
- Drift-Prone
- Manual and Slow
- Poor feedback
- Difficult Disaster Recovery



# Classic Resource Deployment

- Simple and consistent Process
- ~~Drift Prone~~
- ~~Manual and Slow~~
- Timely feedback
- ~~Difficult Disaster Recovery~~



