OVERVIEW OF

SPIRE

solo.io

PETER JAUSOVEC

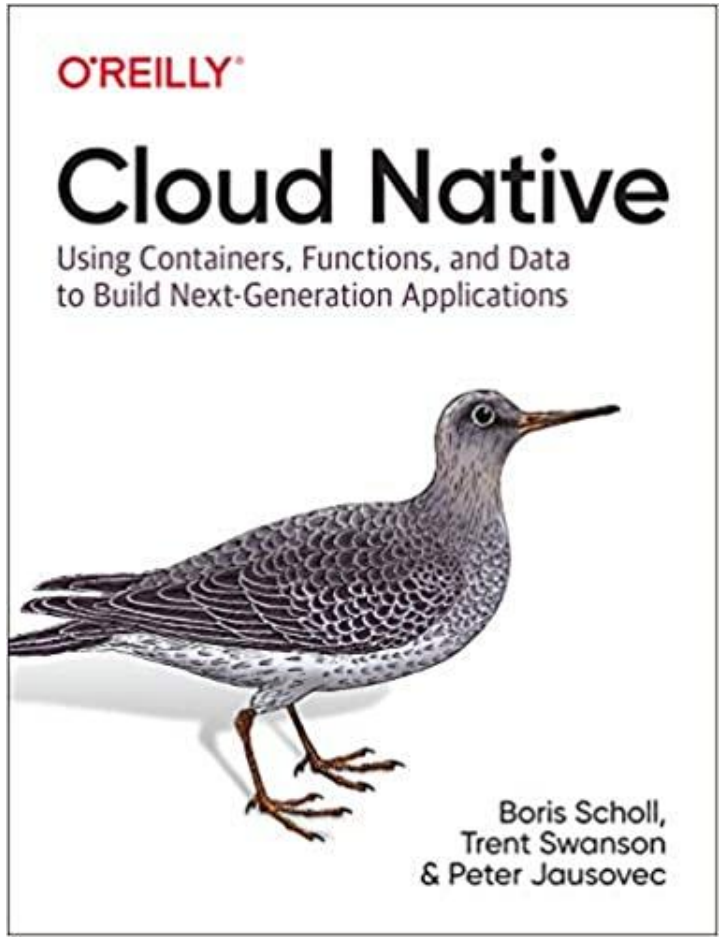
Platform Advocate, Solo.io

@pjausovec

peter.jausovec@solo.io

https://learncloudnative.com

https://www.linkedin.com/in/pjausovec/



solo.io

Agenda

01 What is SPIRE?

02 How do SPIFFE / SPIRE work?

03 Using SPIRE with Istio

solo.io

What is SPIRE?

Production-ready implementation of **SPIFFE** APIs that perform node and workload **attestation** to securely **issue SVIDs** to workloads and **verify SVIDs** of other workloads based on some conditions.

solo.io

SPIFFE: Three Core Components

SPIFFE ID

A string to uniquely and specifically identify a workload.

```
spiffe://cluster.local/ns/default/sa/sleep
```

SPIFFE Verifiable Identity Document (SVID)

Used by a workload to prove its identity to a resource or caller

Workload API

Used by a workload to receive its identity, private key/cert, and trust bundle.

solo.io

SPIFFE ID in x.509 SVID

- Identity in Istio = based on service accounts, trust domain, and namespace
- SPIFFE ID is encoded in SAN field (Subject Alternative Name)
- x.509 certificate:

```
X509v3 Authority Key Identifier:
    keyid:45:13:7D:E0:94:F6:42:8F:F0:66:E3:45:DB:67:82:F8:D8:81:89:F3
X509v3 Subject Alternative Name: critical
    URI:spiffe://cluster.local/ns/default/sa/sleep
```


solo.io

SPIFFE vs SPIRE

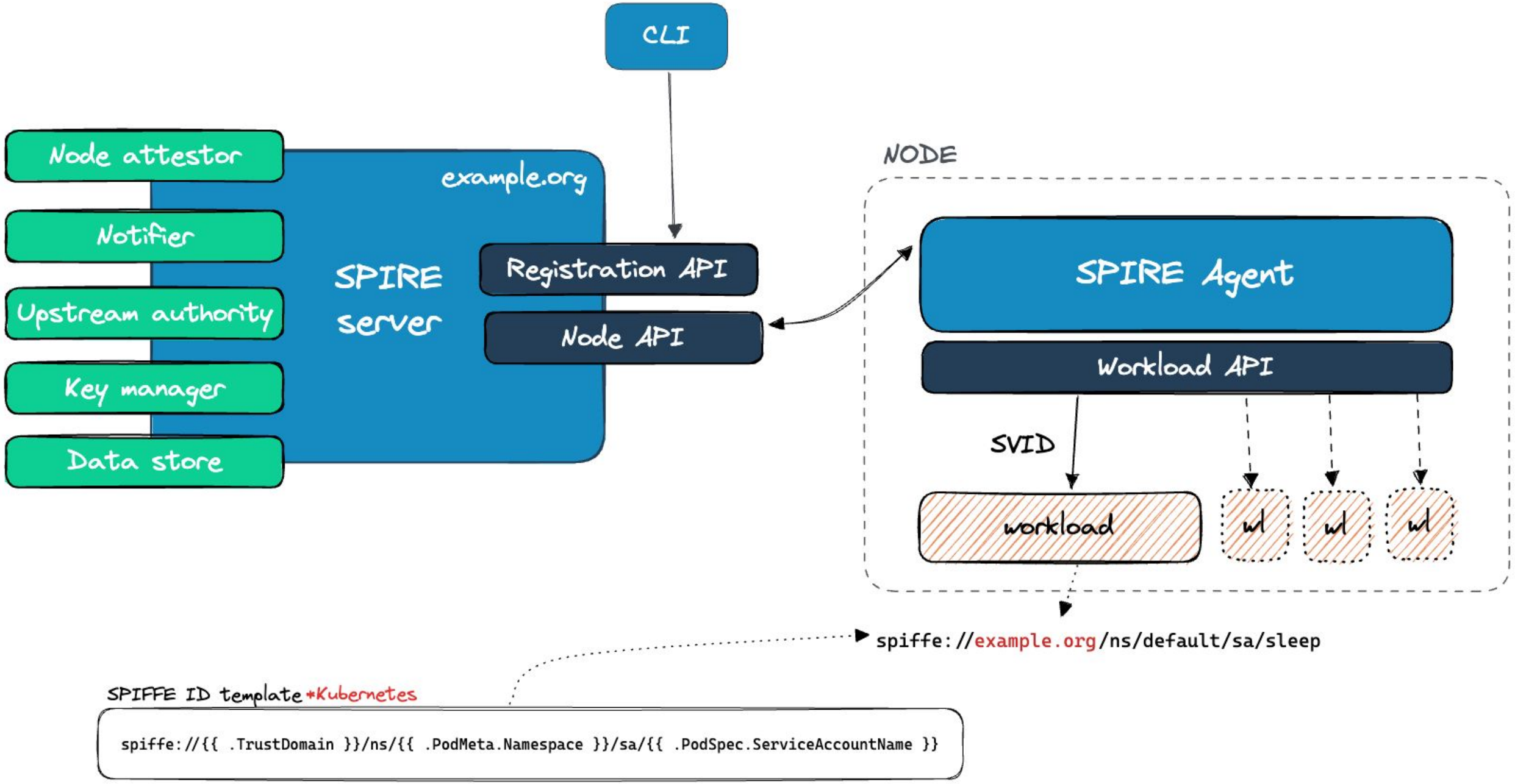
A set of open-source standards for securely identifying software systems

An open-source, production-ready implementation of the SPIFFE APIs

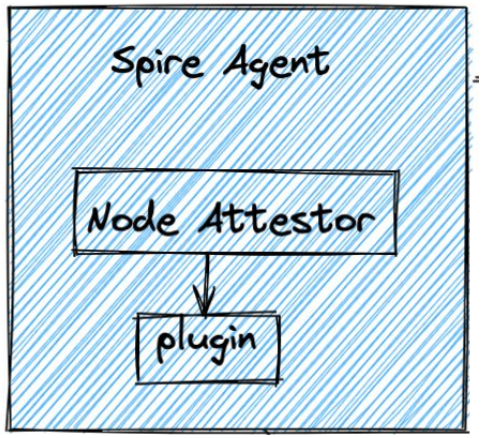
solo.io

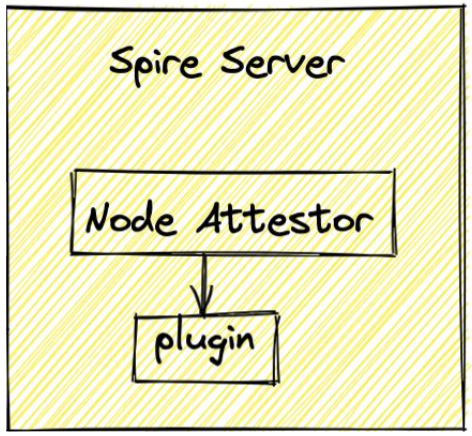
How SPIRE works?

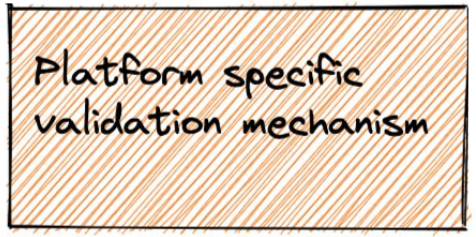
solo.io



Node Attestation







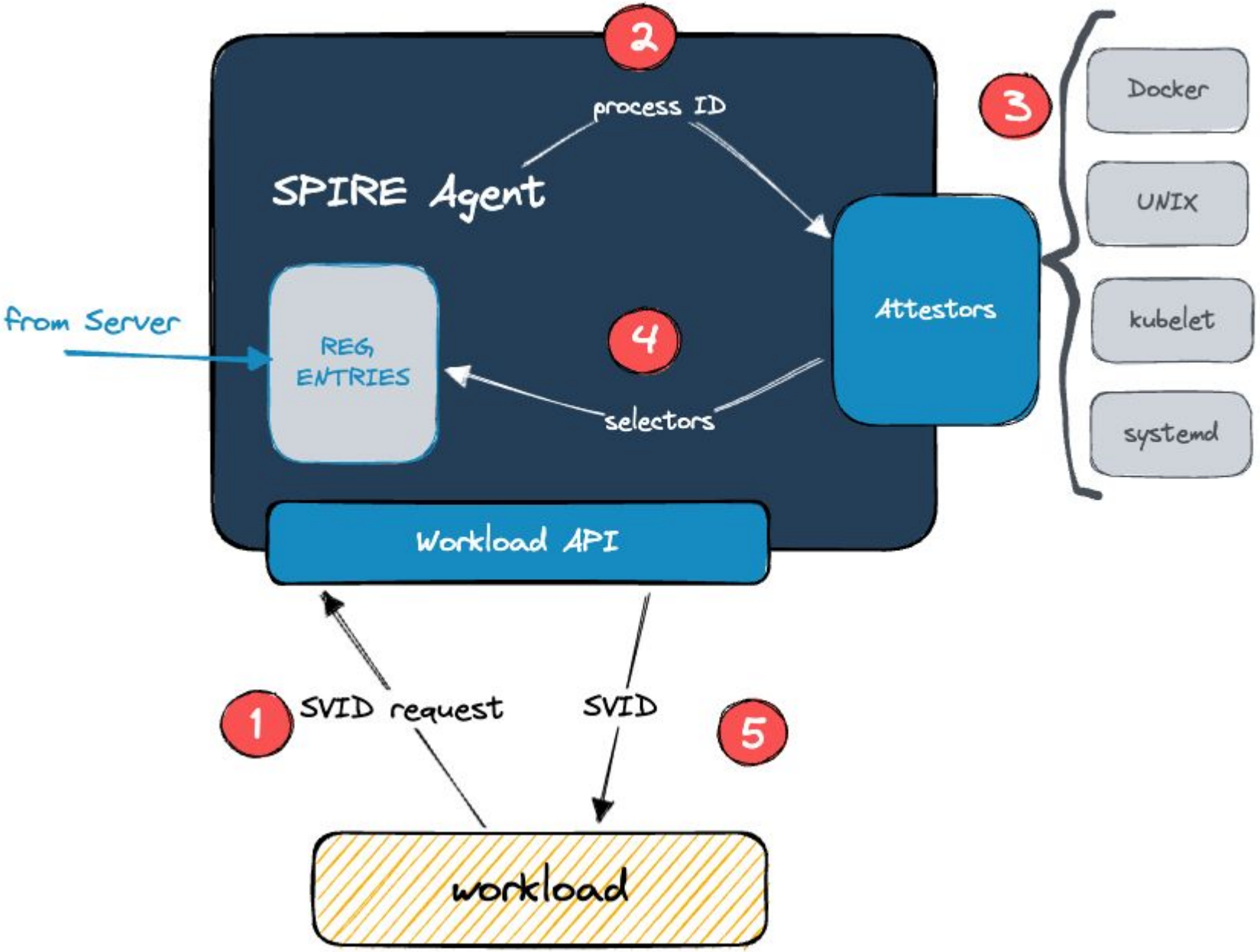
solo.io

Node Attestation

- Uses node attestors (AWS, GCP, Azure, HSM) → SPIFFE ID & SVID for the agent

```
Entry ID         : 62ebacd3-eaaa-4b21-b52e-79ba09da2adf
SPIFFE ID        : spiffe://example.org/k8s-workload-registrar/demo-cluster/node/k3s-peterj-istio-9e0a-ec4355-node-pool-e972-imoph
Parent ID        : spiffe://example.org/spire/server
Revision         : 0
TTL              : default
Selector         : k8s_psat:agent_node_uid:266b3555-9979-4ba2-8ed8-f902cb70b8e2
Selector         : k8s_psat:cluster:demo-cluster
```


solo.io



solo.io

Workload Attestation

- Uses workload attestors (Docker, Unix, K8s) to determine the properties of the workload (e.g uid, gid, service account in K8s, …)
- Discovered properties are returned as selectors to the agent
- Agent determines the identity by comparing the selectors to registration entries

```
Entry ID         : 5d260de3-d8b3-4911-8ddc-4edfd6e5ec46
SPIFFE ID        : spiffe://hoot.solo.io/ns/default/sa/sleep
Parent ID        : spiffe://hoot.solo.io/k8s-workload-registrar/spire-demo/node/k3s-spire-demo-b371-c25841-node-pool-589b-hhgm5
Revision         : 1
TTL              : default
Selector         : k8s:node-name:k3s-spire-demo-b371-c25841-node-pool-589b-hhgm5
Selector         : k8s:ns:default
Selector         : k8s:pod-uid:4356c73f-b279-4ed7-8ae6-80f34abd0ddc
DNS name         : sleep-7679b5cf67-qprlj
DNS name         : sleep.default.svc
```


solo.io

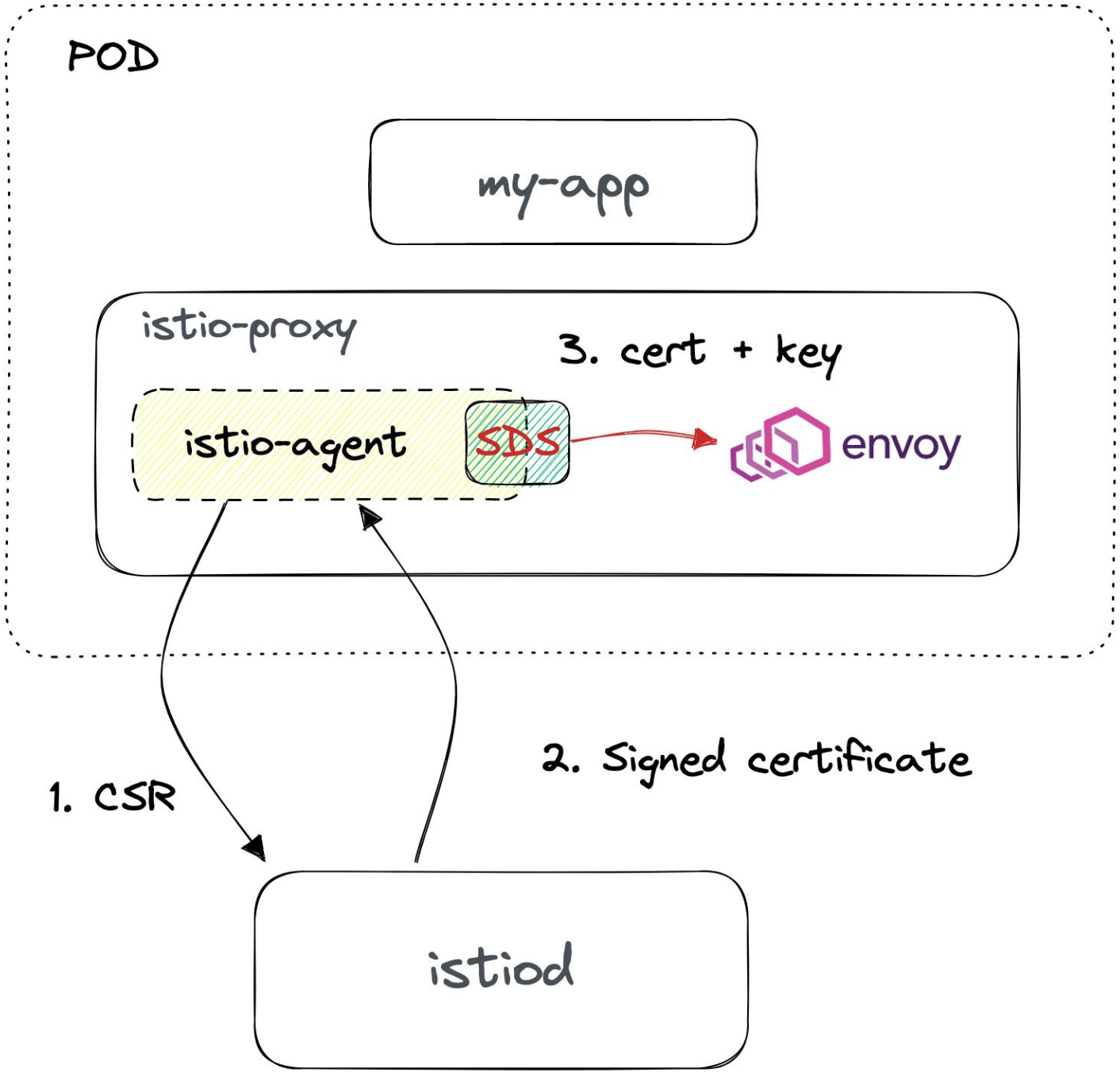
SPIRE with Istio

solo.io

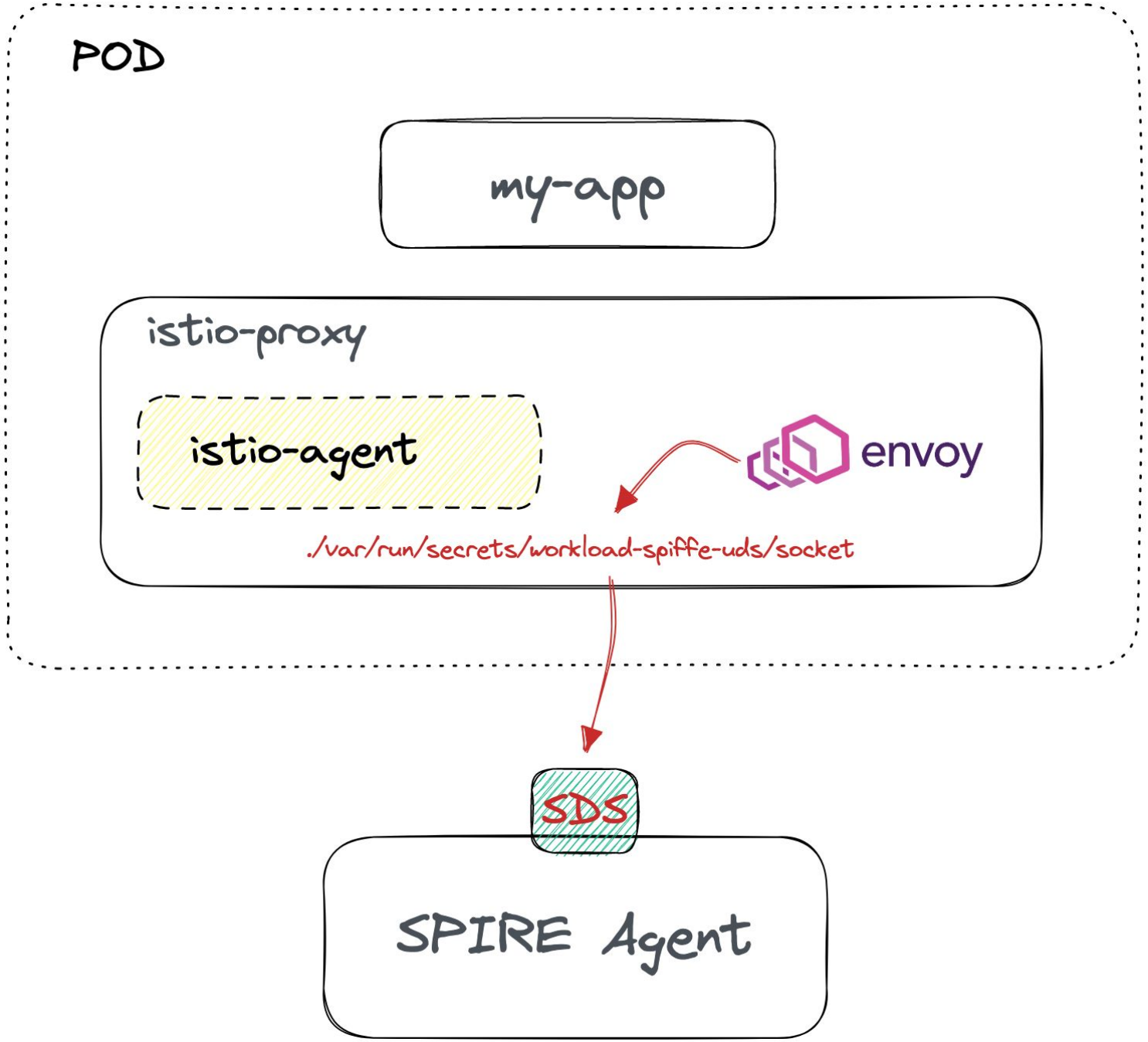
Breaking Down a Workload in Istio

Most of our workloads will be deployed as k8s pods

solo.io

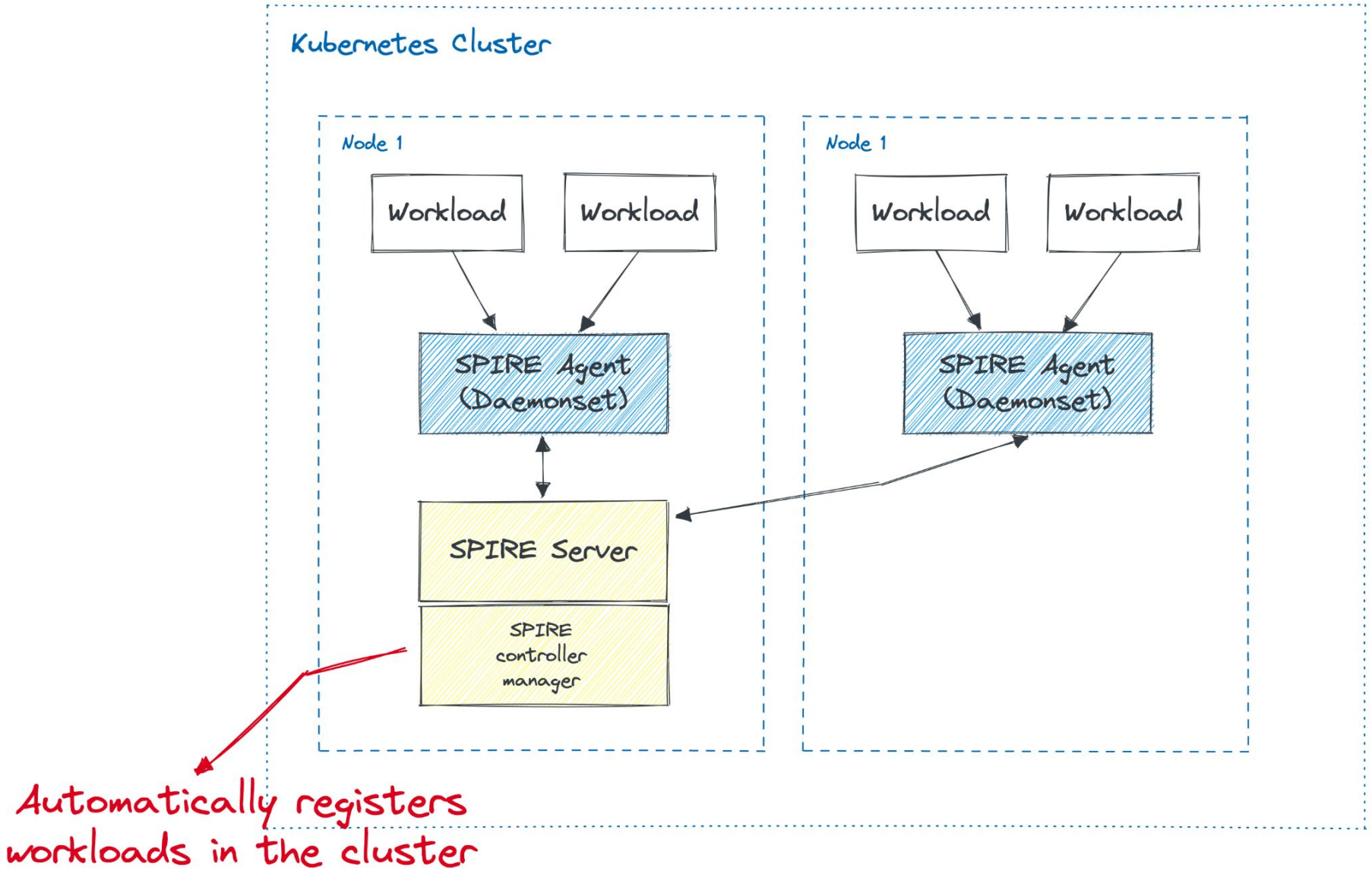


solo.io



solo.io

Kubernetes setup



solo.io

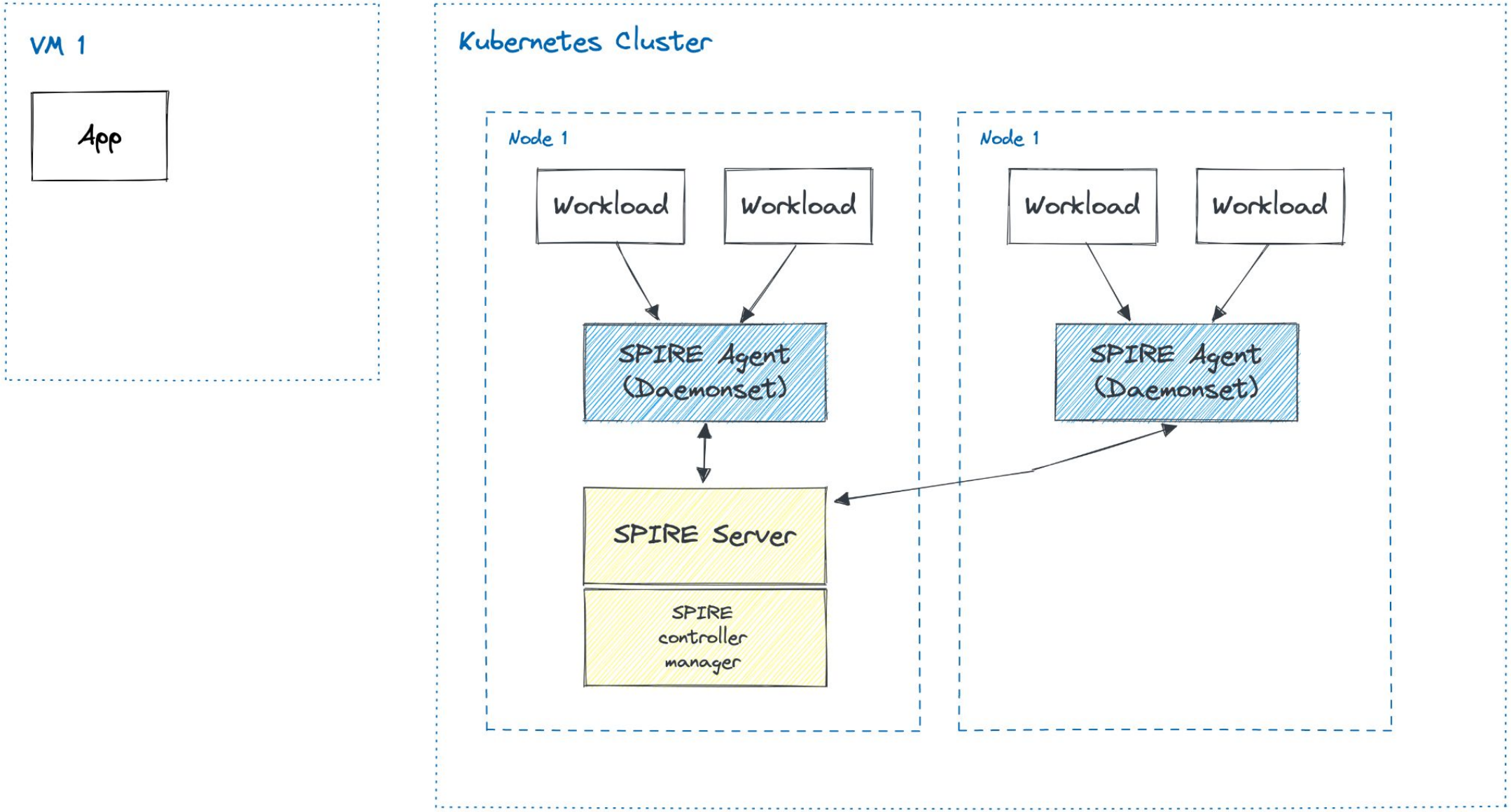
DEMO

solo.io

Using SPIRE to enable mTLS between a mesh and external VMs

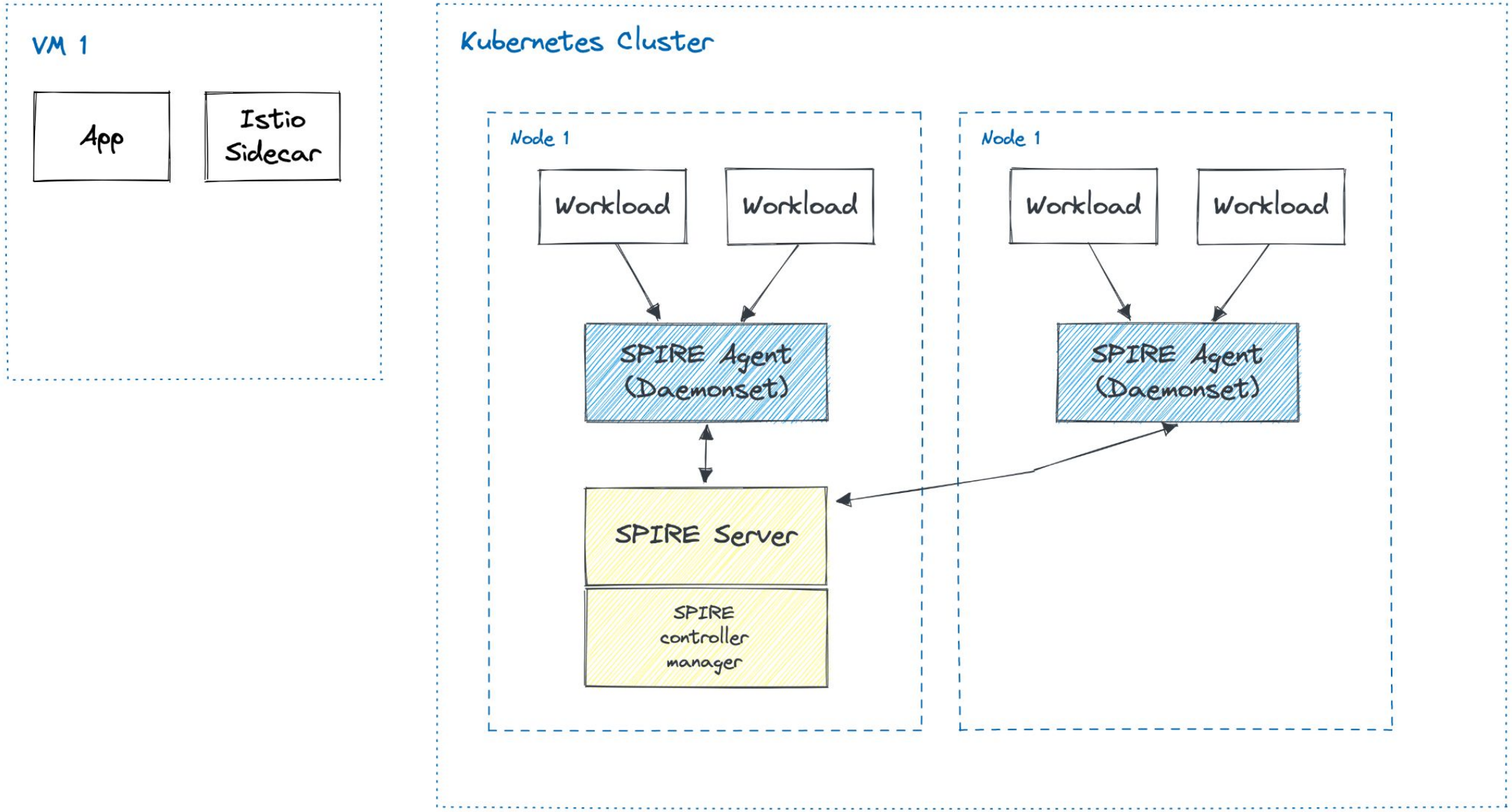
solo.io

Adding a VM to our setup



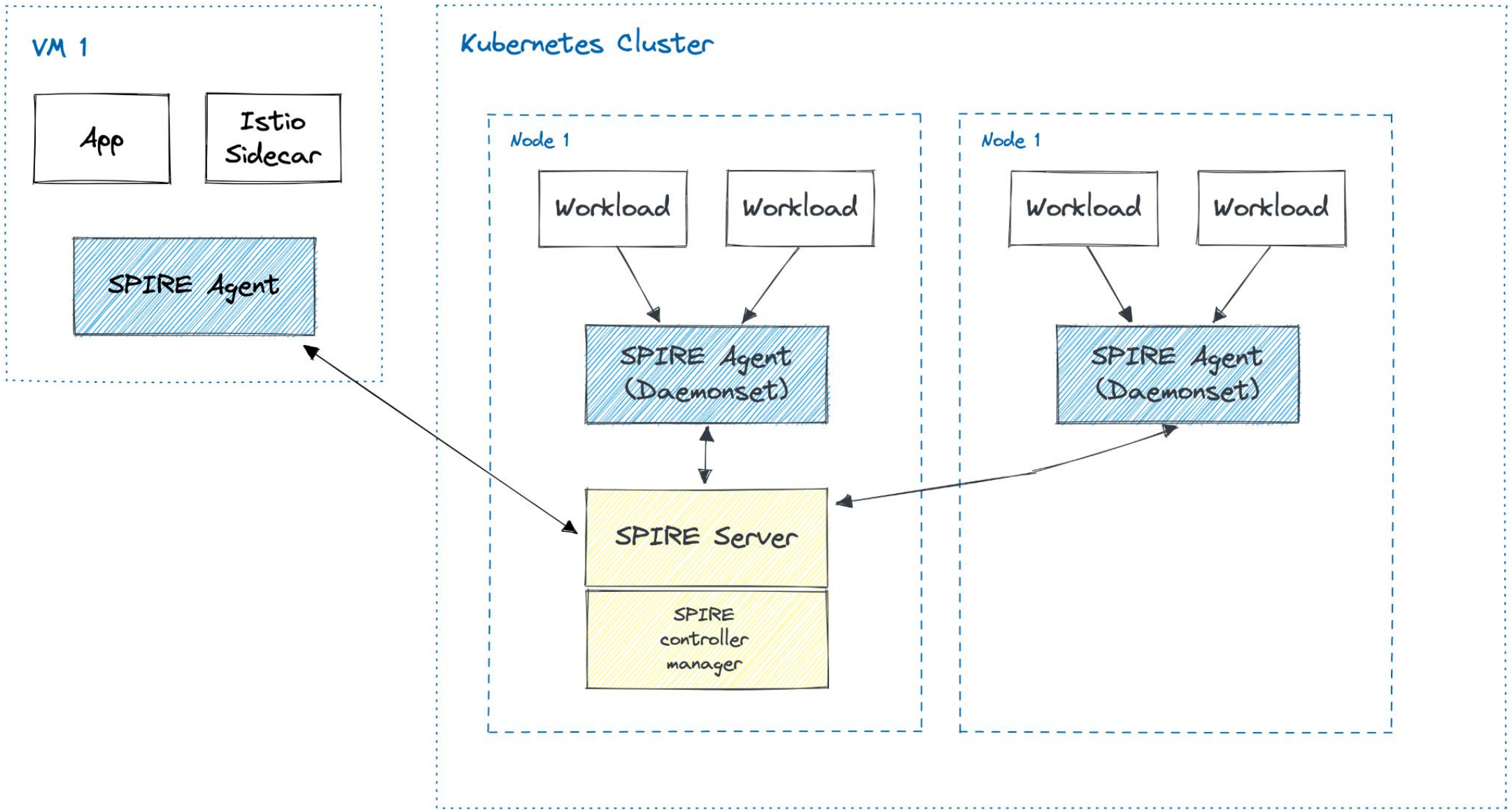
solo.io

Adding a VM to our setup

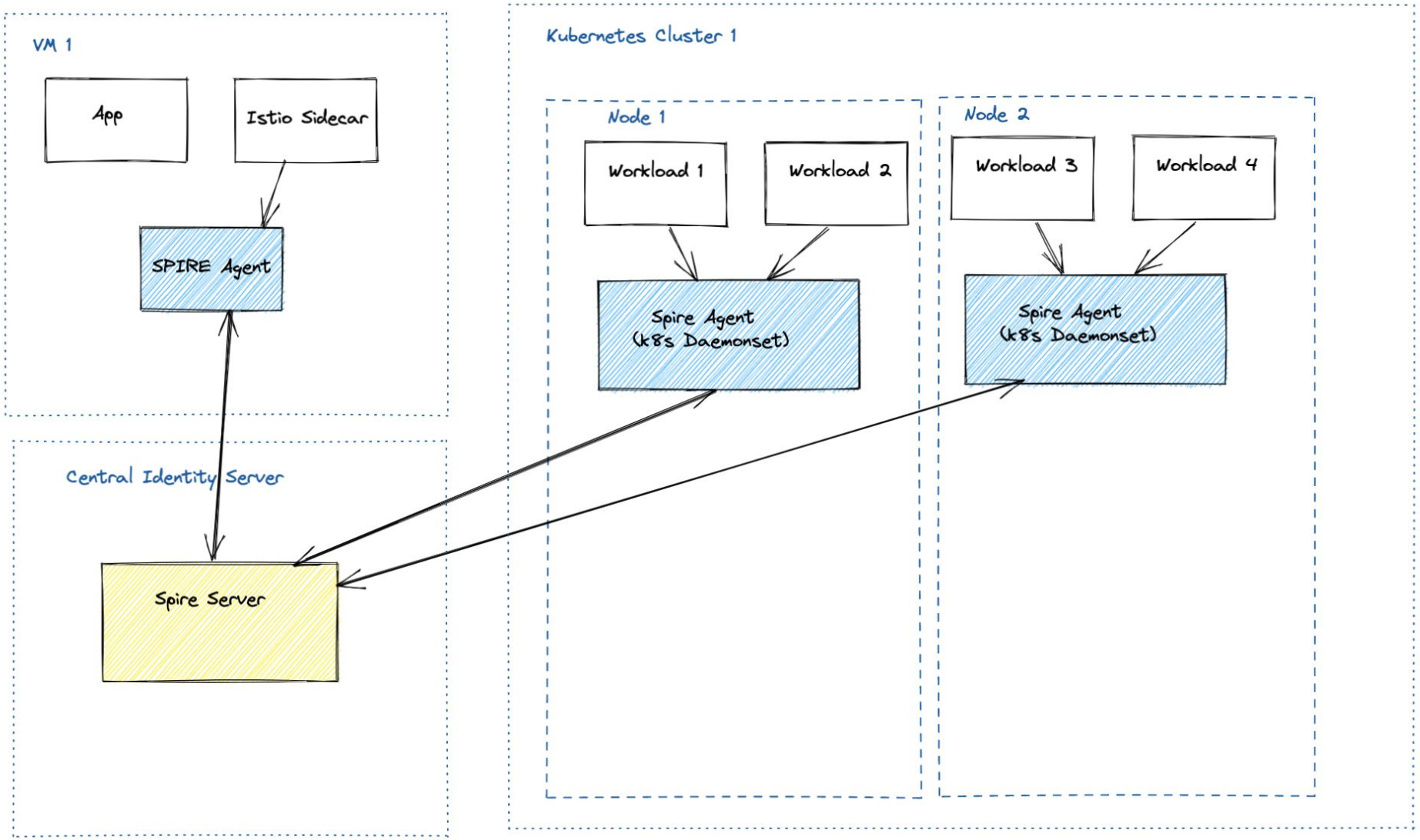


solo.io

Adding a VM to our setup

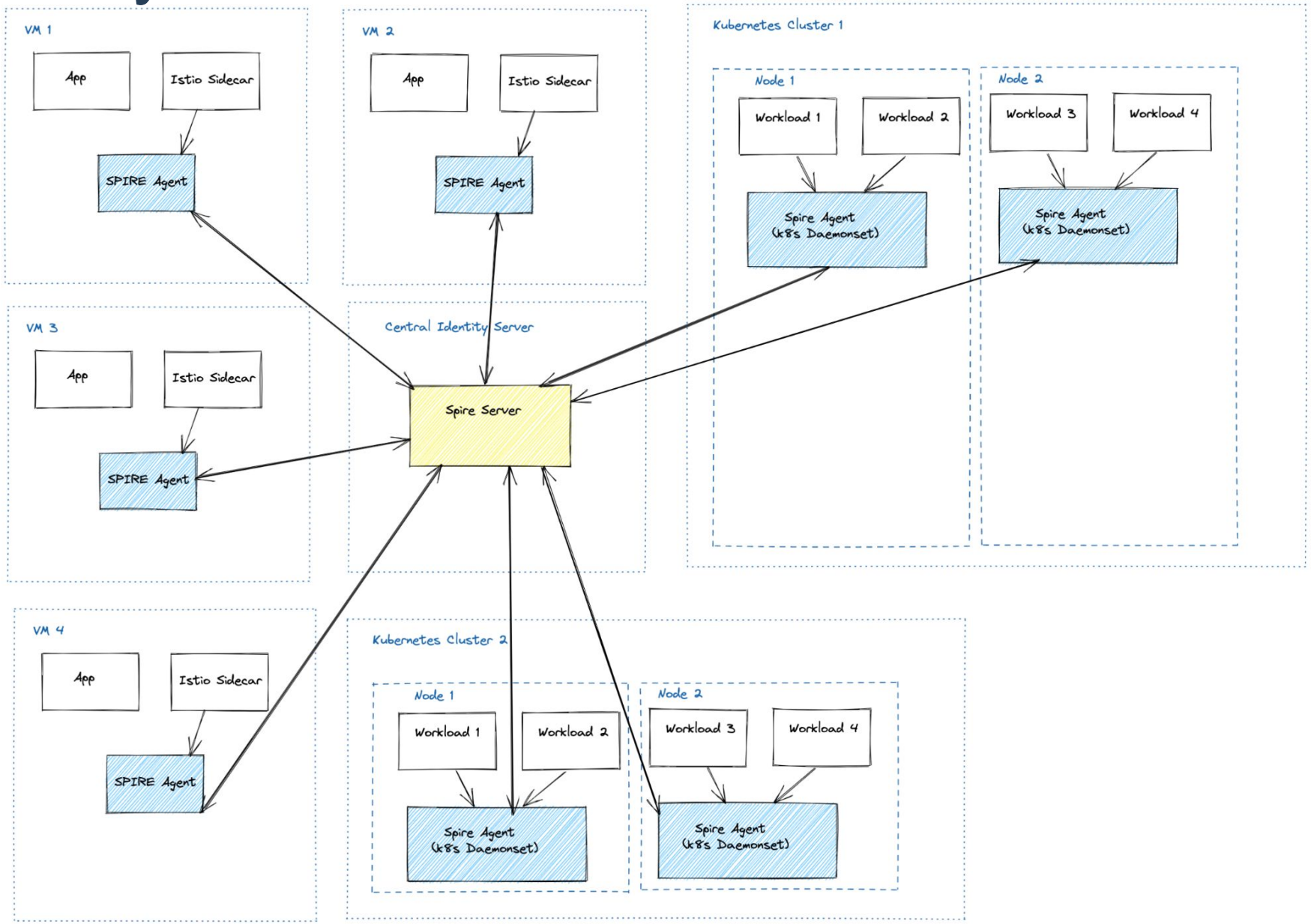


SPIRE is platform agnostic



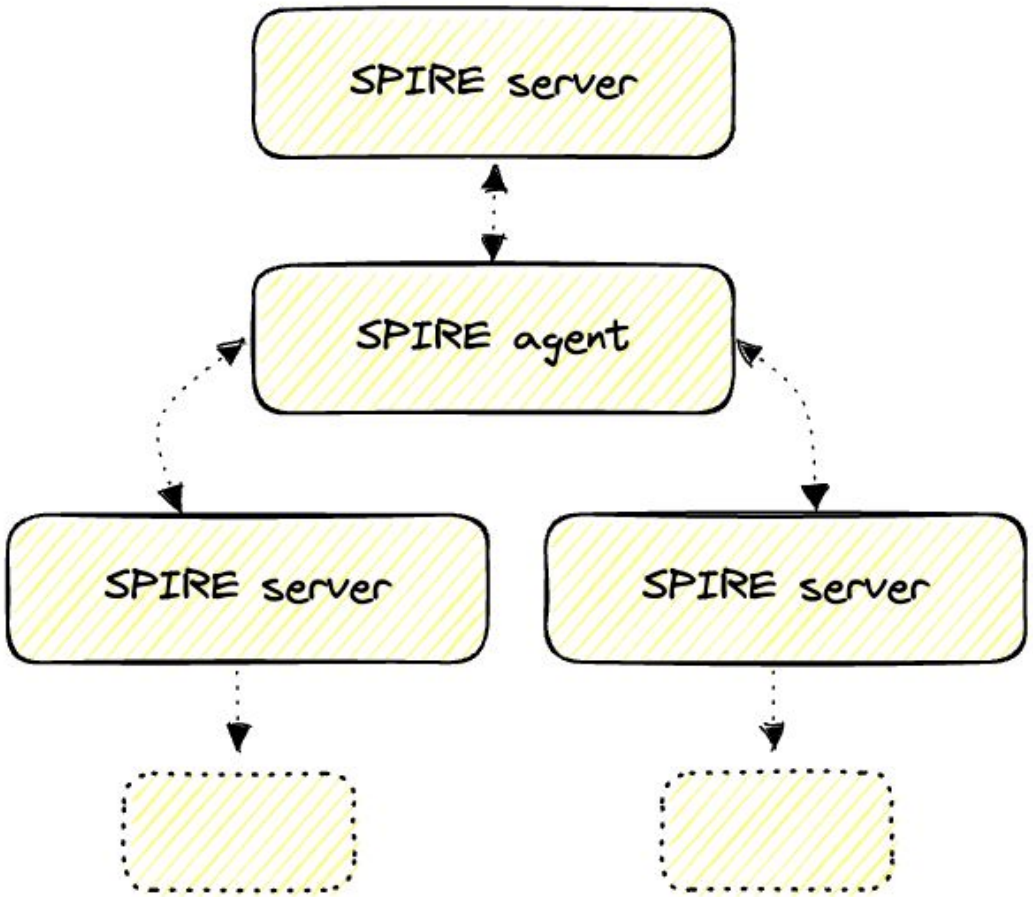
solo.io

One identity server to rule them all

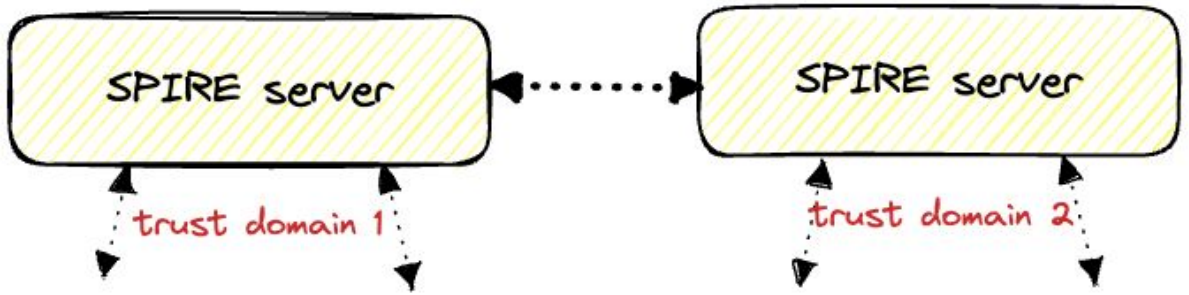


solo.io

Nested SPIRE



Federated SPIRE



solo.io

Wrap up

- Creating, maintaining and rotating certs for workloads is a lot of work
- SPIRE enables you to deploy mTLS across your workloads by:
  - Attest workload identity at runtime
  - Delivers workload-specific short-lived certs
- How?
  1. Install SPIRE server and SPIRE agents on each VM/node
  2. Configure node and workload attestation
  3. Register workloads with the server
  4. Retrieve SVIDs from SPIRE agent API (use SDK or Envoy proxy for example)

solo.io

Thank You!

Useful resources / further reading

- SPIFFE spec - https://github.com/spiffe/spiffe/blob/main/standards/SPIFFE.md
- Official SPIFFE docs - https://spiffe.io/docs/latest/spiffe-about/overview/
- SPIRE architecture & components - https://spiffe.io/docs/latest/spire-about/spire-concepts
- Scaling SPIRE - https://spiffe.io/docs/latest/planning/scaling_spire
- Istio cert management - https://istio.io/latest/docs/concepts/security/#pki
- Istio SPIRE integration - https://istio.io/latest/docs/ops/integrations/spire

solo.io