KubeCon

CloudNativeCon

North America 2024

SPIFFE Deployments in Non-K8s Environments

Nadin El-Yabroudi (Founding Engineer, SPIRL)
Eli Nesterov (CTO, SPIRL)

Who We Are

Nadin El-Yabroudi

nadin@spirl.com
@nadinelyab

- Software Engineer at SPIRL
- Previously security and systems engineer at Cloudflare

I like to go on runs, hike, and travel!

Eli Nesterov

eli@spirl.com
@elinesterov

- Co-founder and CTO @ SPIRL
- Co-author “Solving the bottom Turtle”
- Built world-largest SPIFFE deployment (beyond 1M nodes)

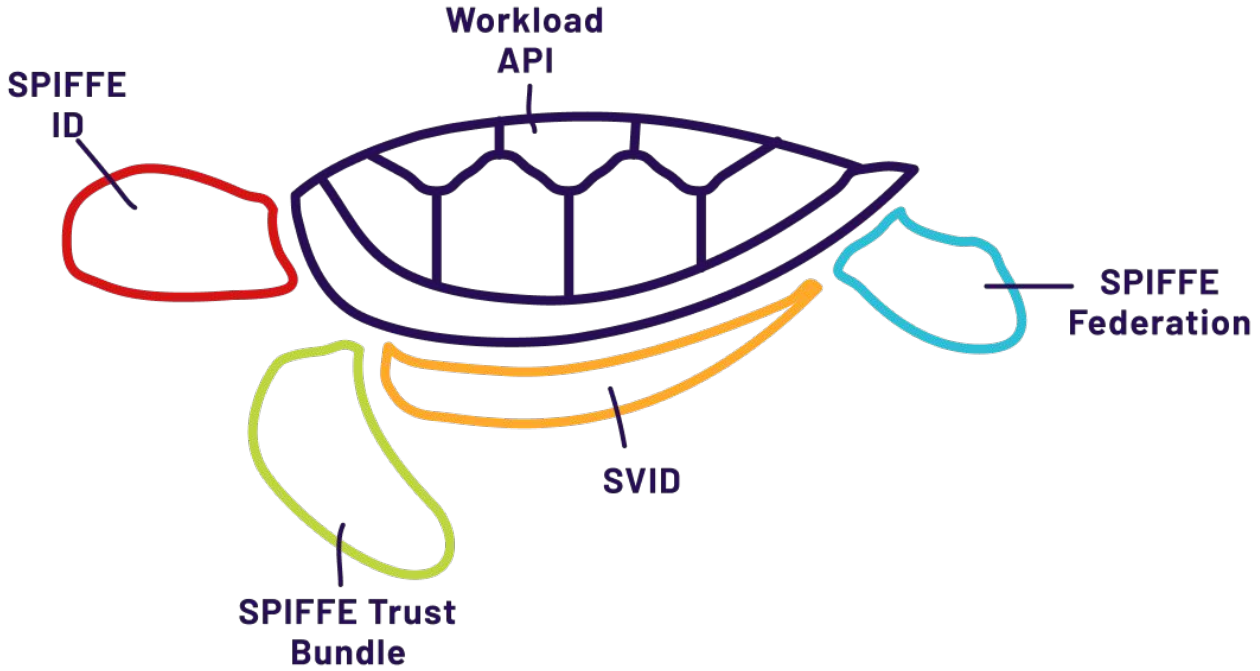
Quick Recap

What is SPIFFE?

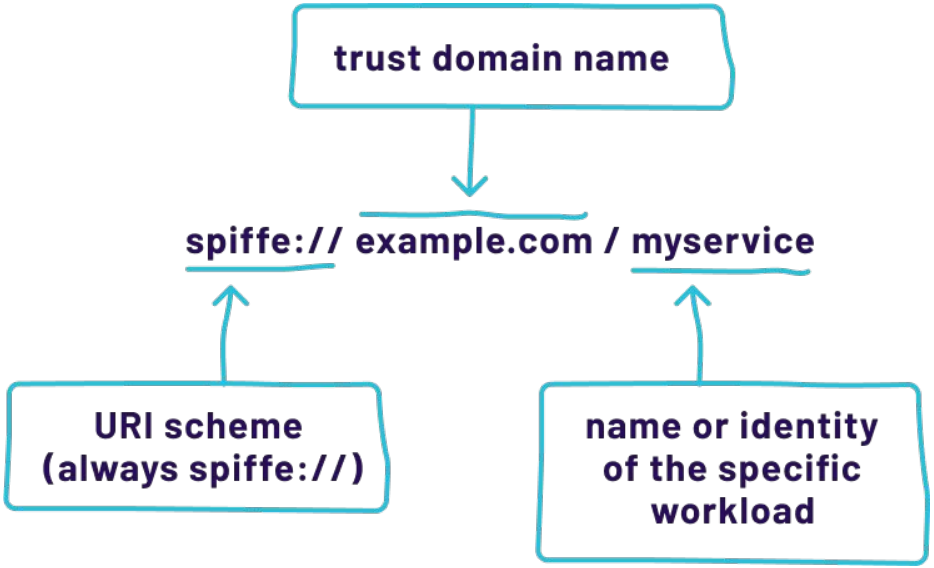
Secure
Production
Identity
Framework
For
Everyone

SPIFFE Specification

Secure
Production
Identity
Framework
For
Everyone



SPIFFE ID



spiffe://example.com/us-central/instance-id/service-name

spiffe://example.com/us-central/prod-cluster/ns/checkoutservice

SVID

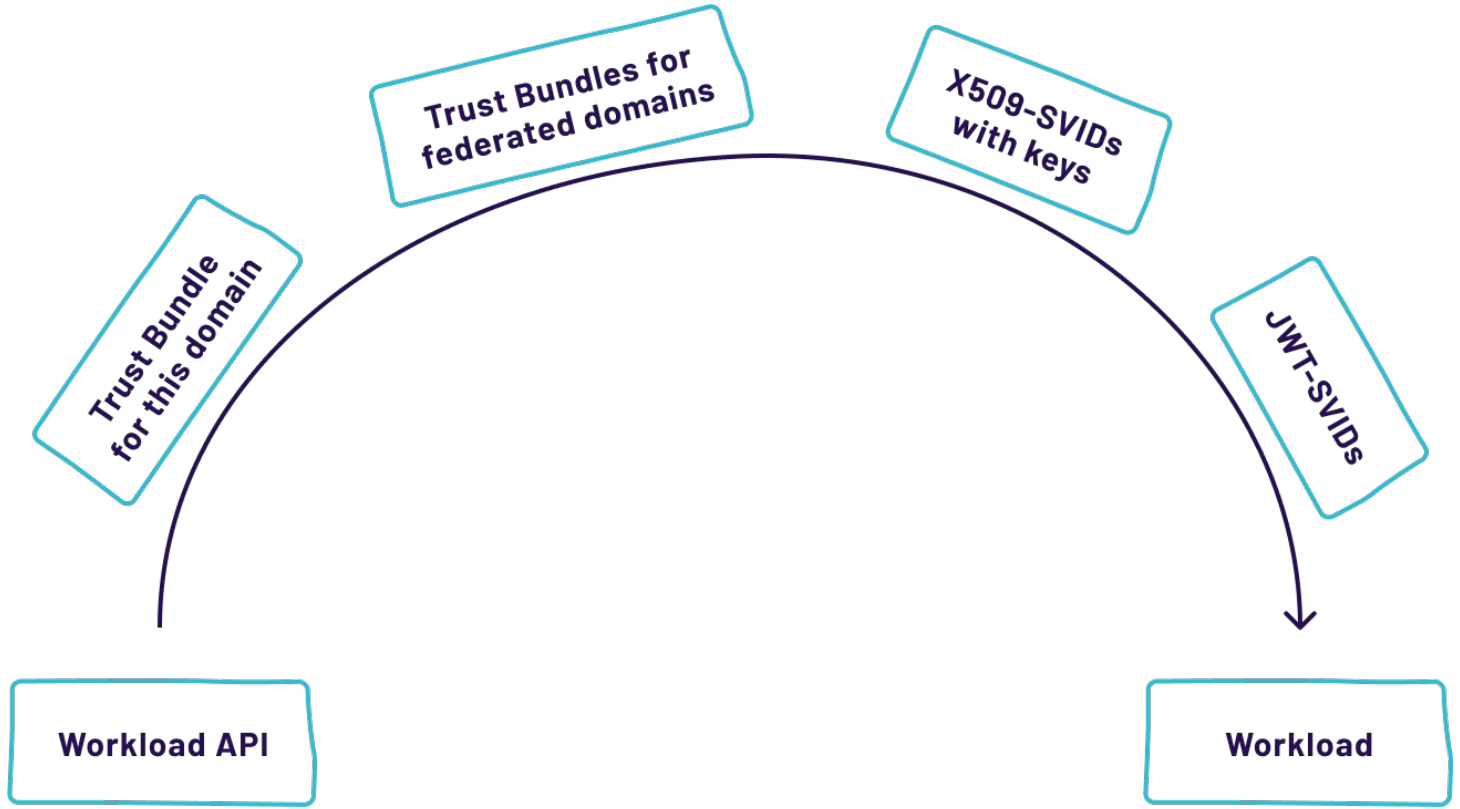
spiffe://example.com/myservice

X.509

JWT

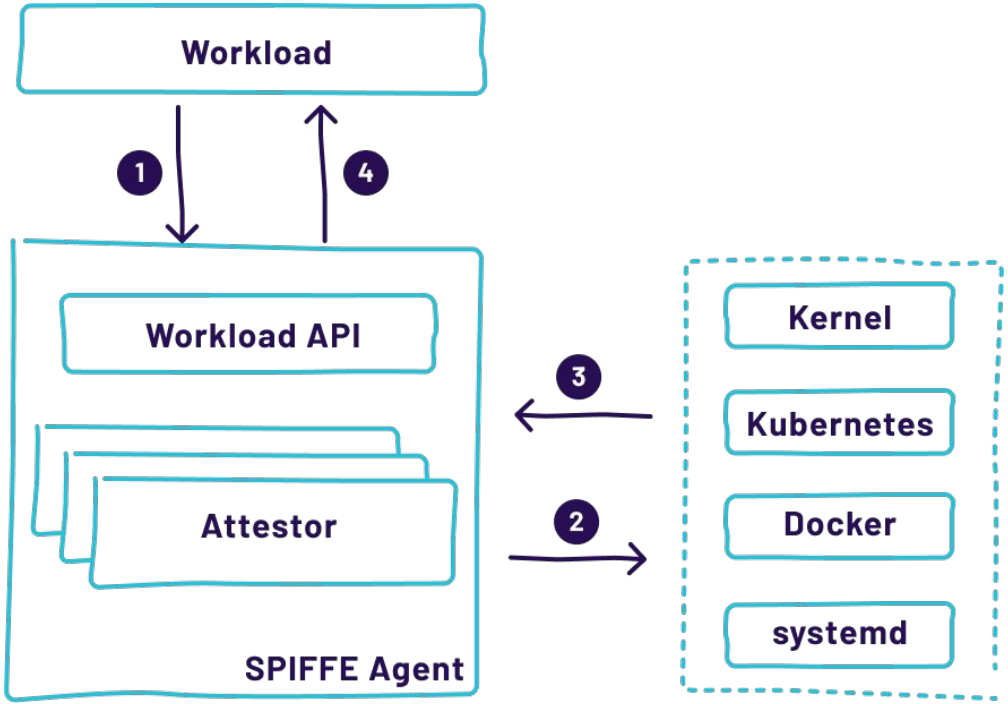
SPIFFE Trust Bundle

Workload API



Workload Attestation

Process by which the identity of a workload is determined and an SVID is issued as a result



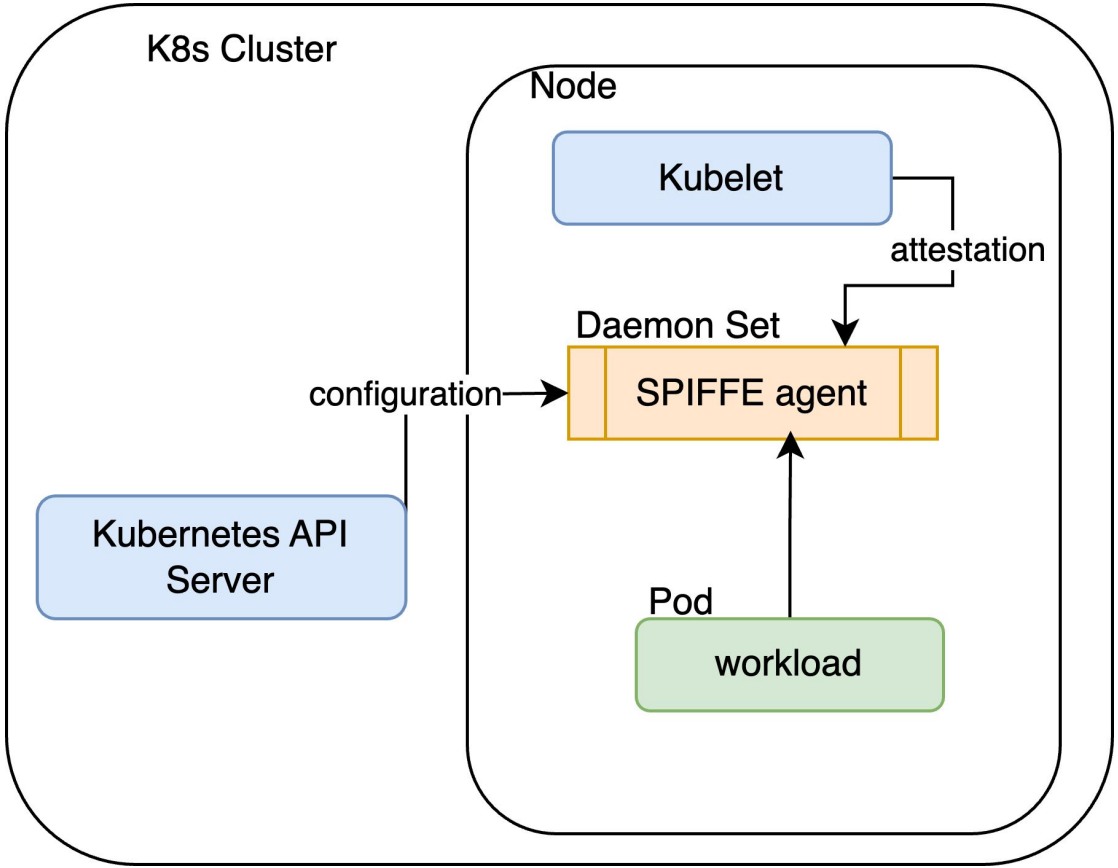
1. The workload calls the Workload API to get an SVID
2. Based on process data, the agent interrogates the platform.
3. The agent determines the attributes of the workload.
4. The agent obtains the identity of the workload and returns it.

SPIFFE In the Real World - For Everyone?

vs

debian

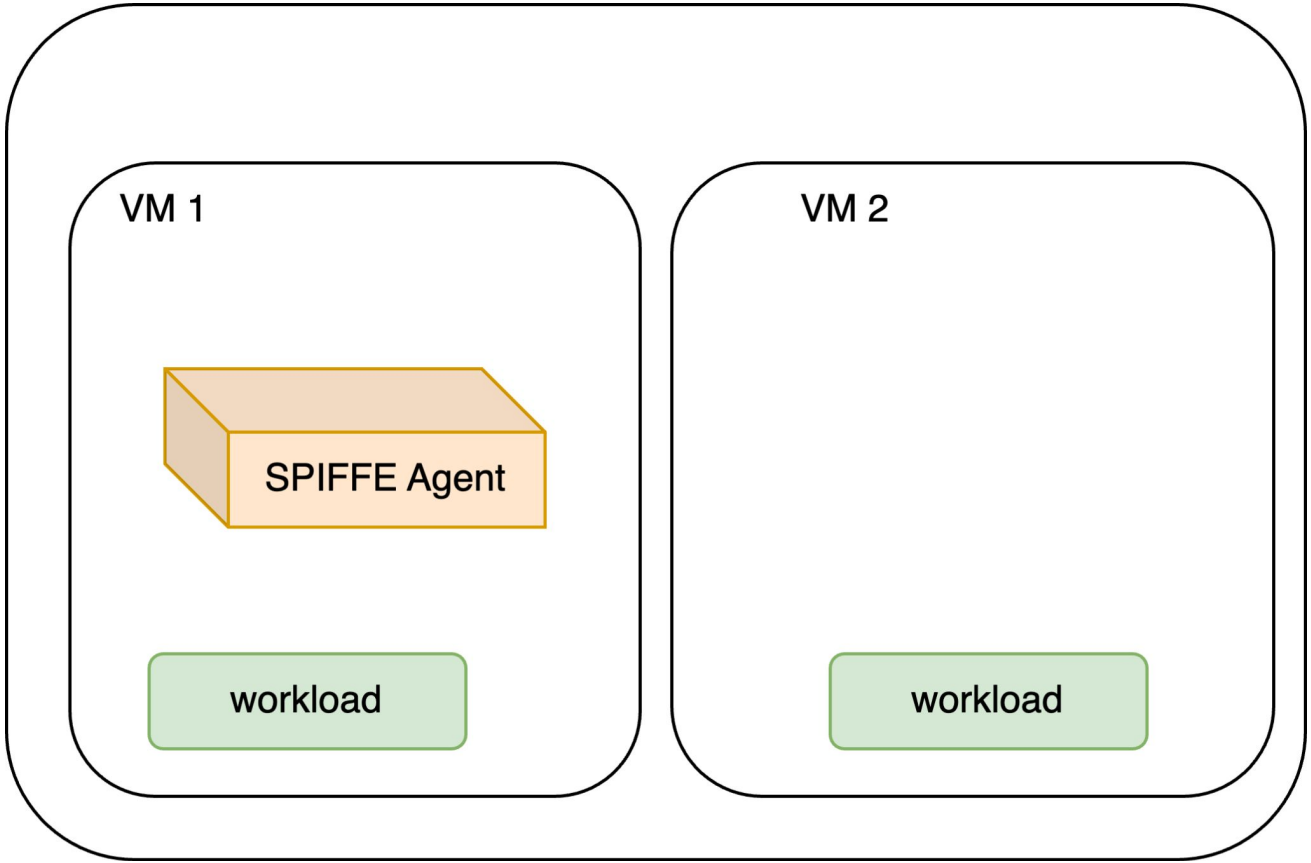
Kubernetes SPIFFE Deployment



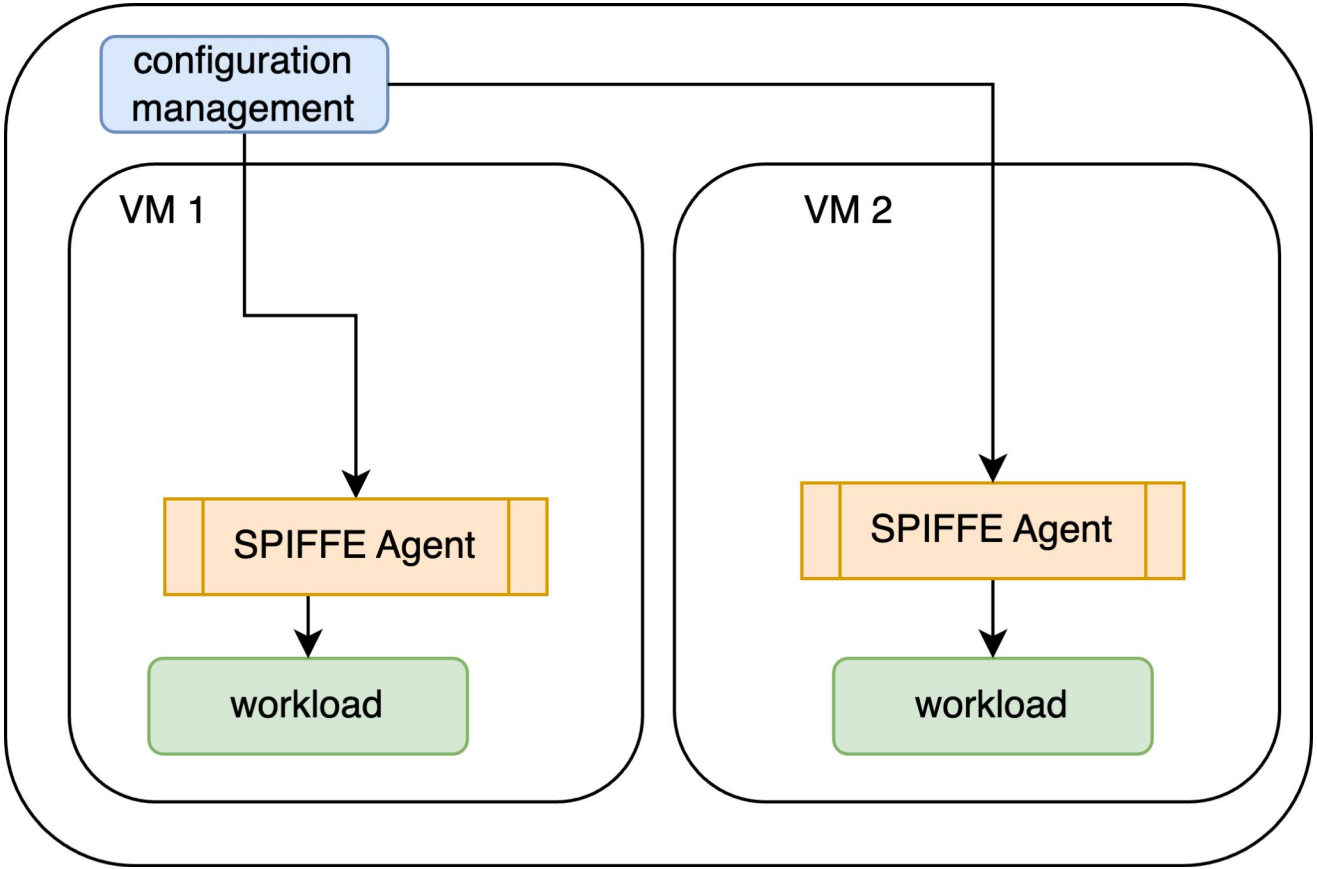
Agent Deployment on K8s Features

Feature	K8s	Linux
Agent binary	Container Image	?
Run agent on every node	DaemonSet	?
Agent Configuration File on each node	DaemonSet	?
Restart agent on failures	DaemonSet	?
Privileged access for attestation	Security Context	?

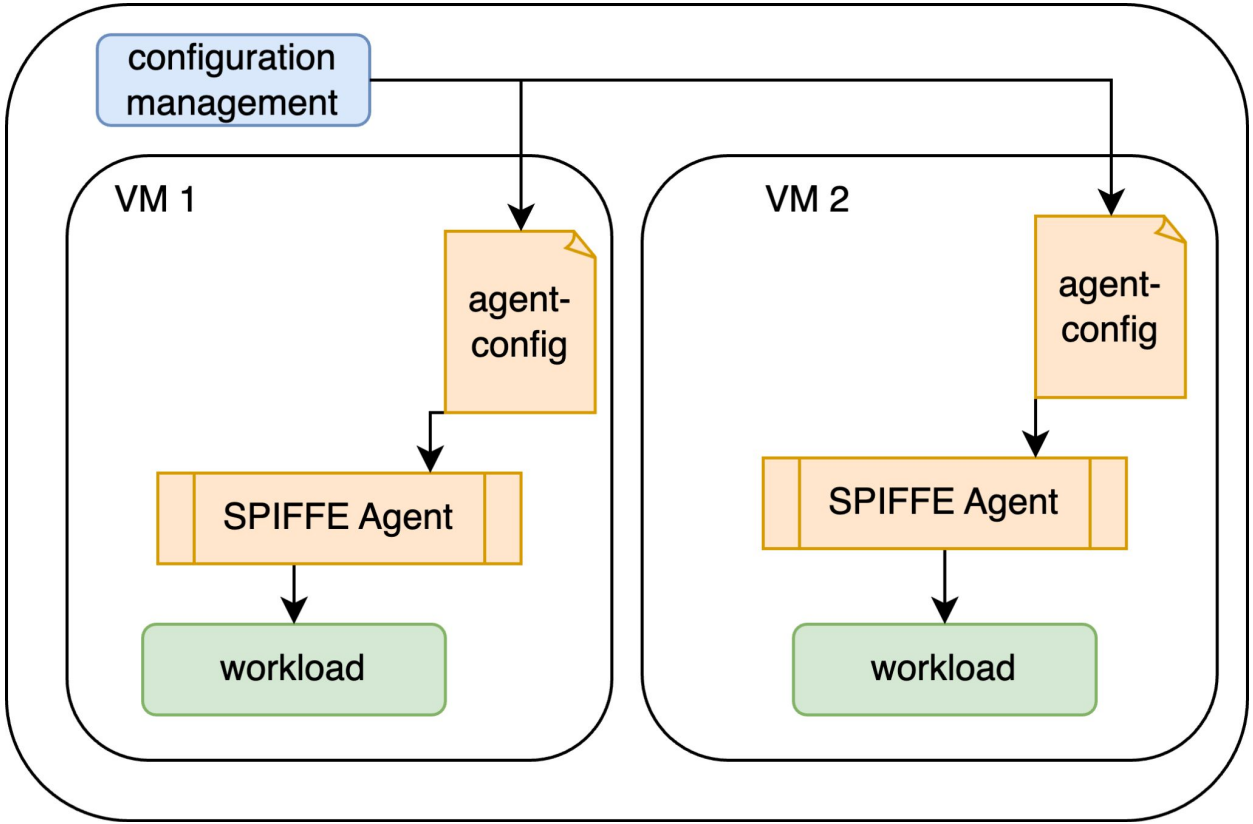
Linux Deployment: Package Agent



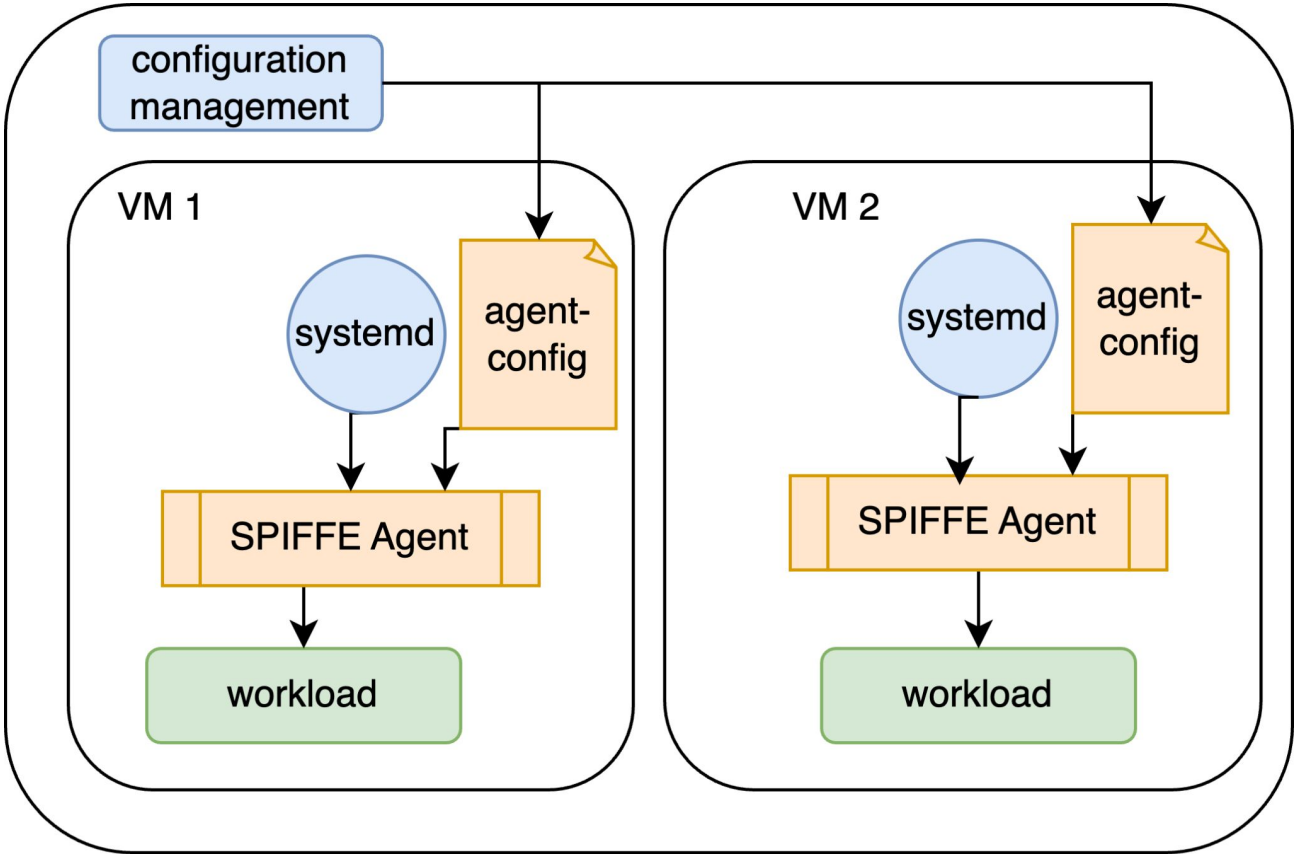
Linux Deployment: Agent



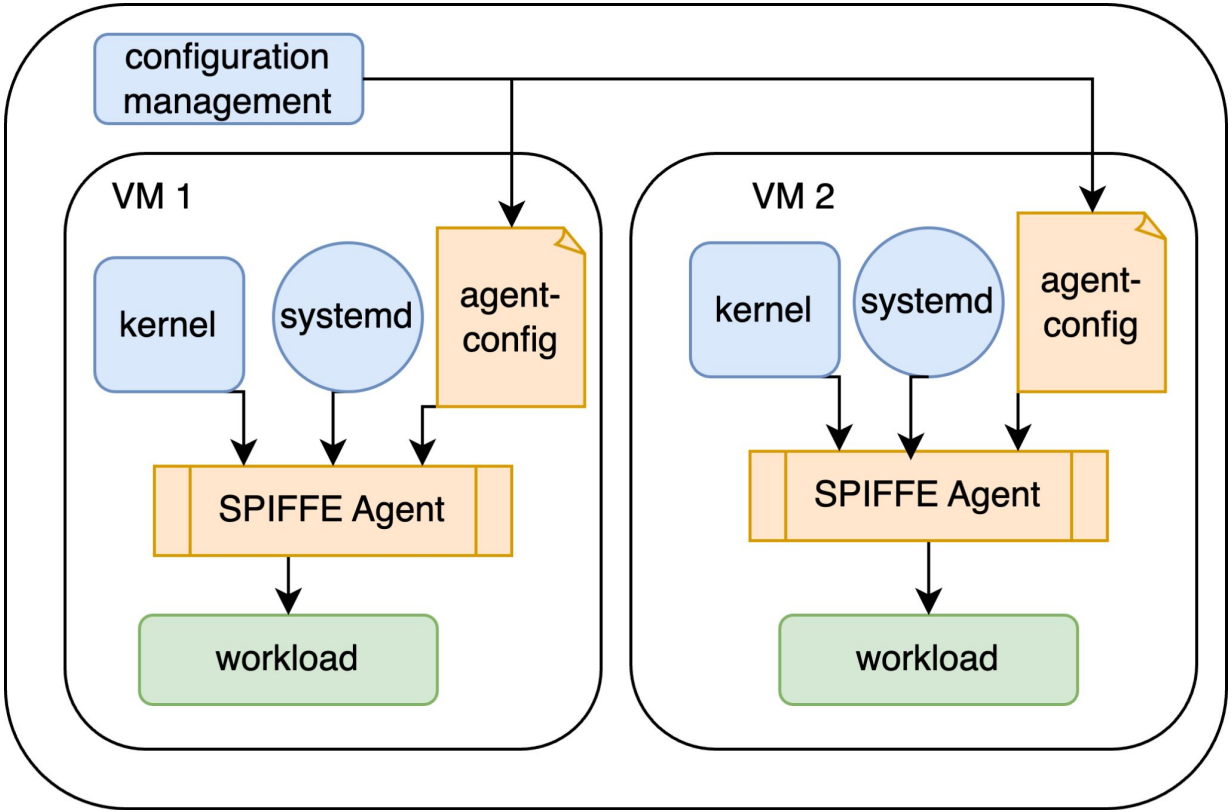
Linux Deployment: Agent Configuration



Linux Deployment: Restart Agent



Linux Deployment: Privileged Access



Agent Deployment K8s vs. Linux

Feature	K8s	Linux
Agent packaging	Container Image	Package for each Linux Flavor
Agent on every node	DaemonSet	Ansible, Puppet, Chef, etc.
Agent configuration file on every node	DaemonSet	Ansible, Puppet, Chef, etc.
Restart agent on failures	DaemonSet	systemd
Privileged access for attestation	Security Context	Root user or Linux capabilities

Workload Attestation

Kubernetes → Kubelet

Attested identifiers:

- Pod name
- Label name
- Namespace
- Cluster name
- Node name

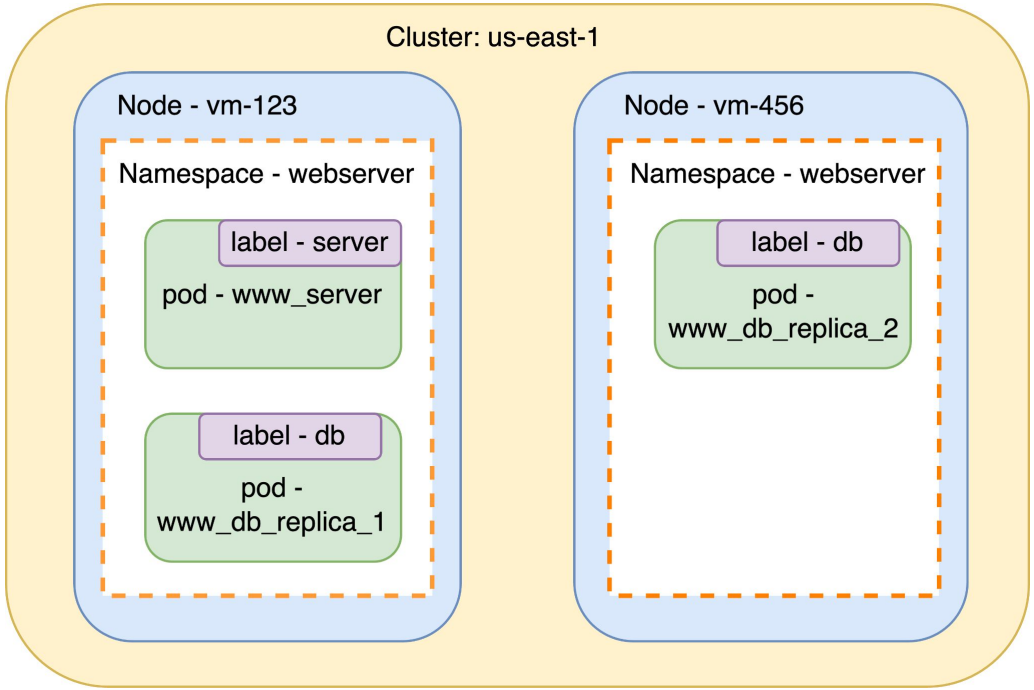
Linux → Kernel

Attested identifiers

- Hostname
- Linux User
- Linux Group
- Complete binary path or binary hash

Kubernetes Identifiers

- Pod name
- Label name
- Namespace
- Cluster name
- Node name

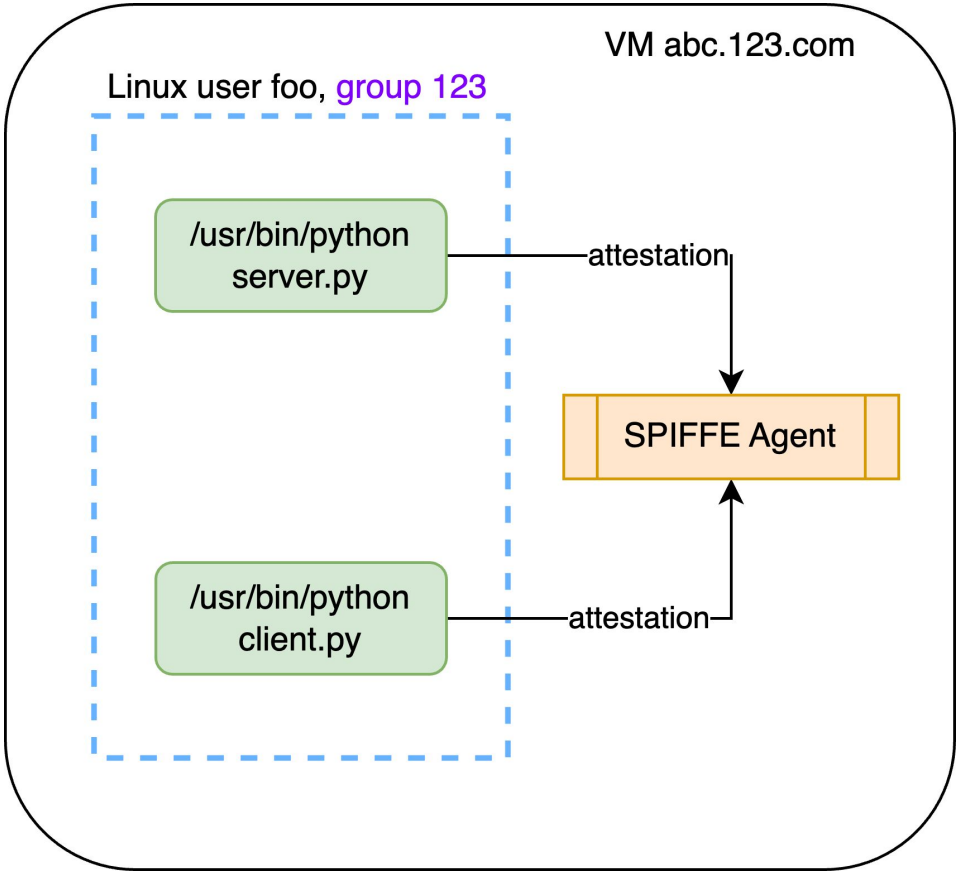


SPIFFE ID:
spiffe://trust-domain/node/vm-123
spiffe://trust-domain/node/vm-123/pod/www_server
spiffe://trust-domain/ns/webserver/label/db
spiffe://trust-domain/cluster/us-east-1/ns/webserver

In the Linux World

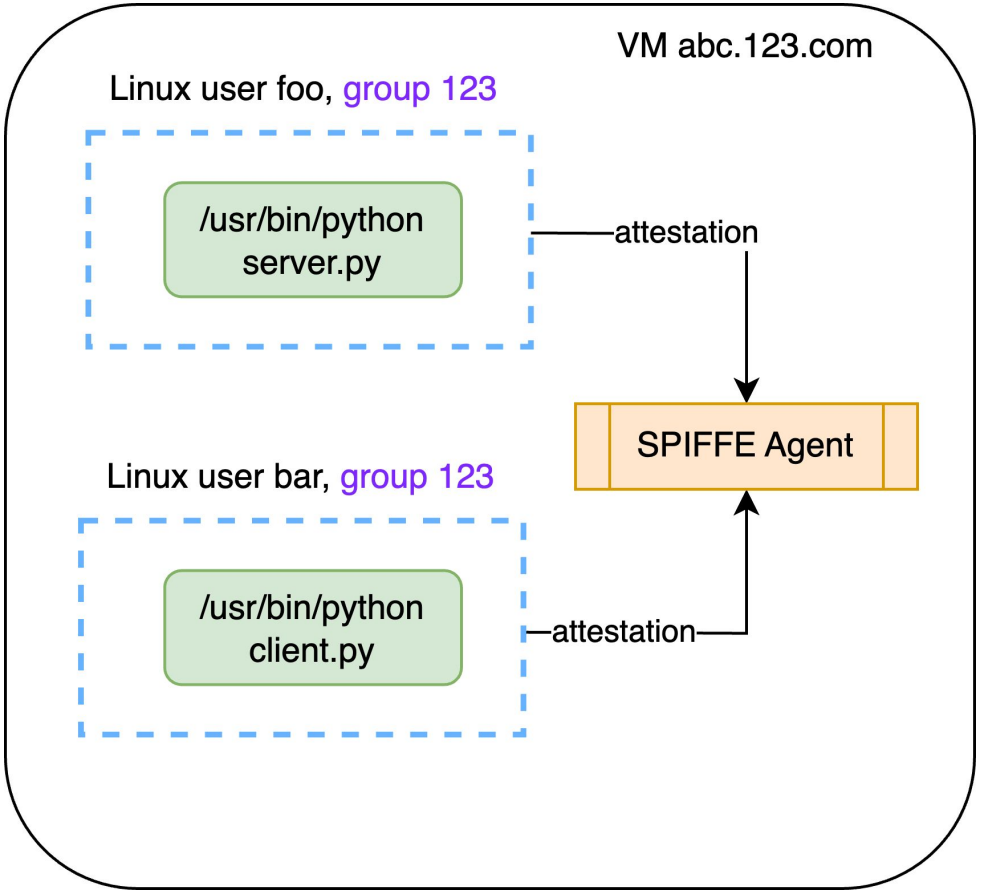
- Hostname
- Linux User
- Linux Group
- Complete binary path
- Hash of binary

SPIFFE ID:
spiffe://trust-domain/user/foo/binary/usr/bin/python
spiffe://trust-domain/user/foo/group/123



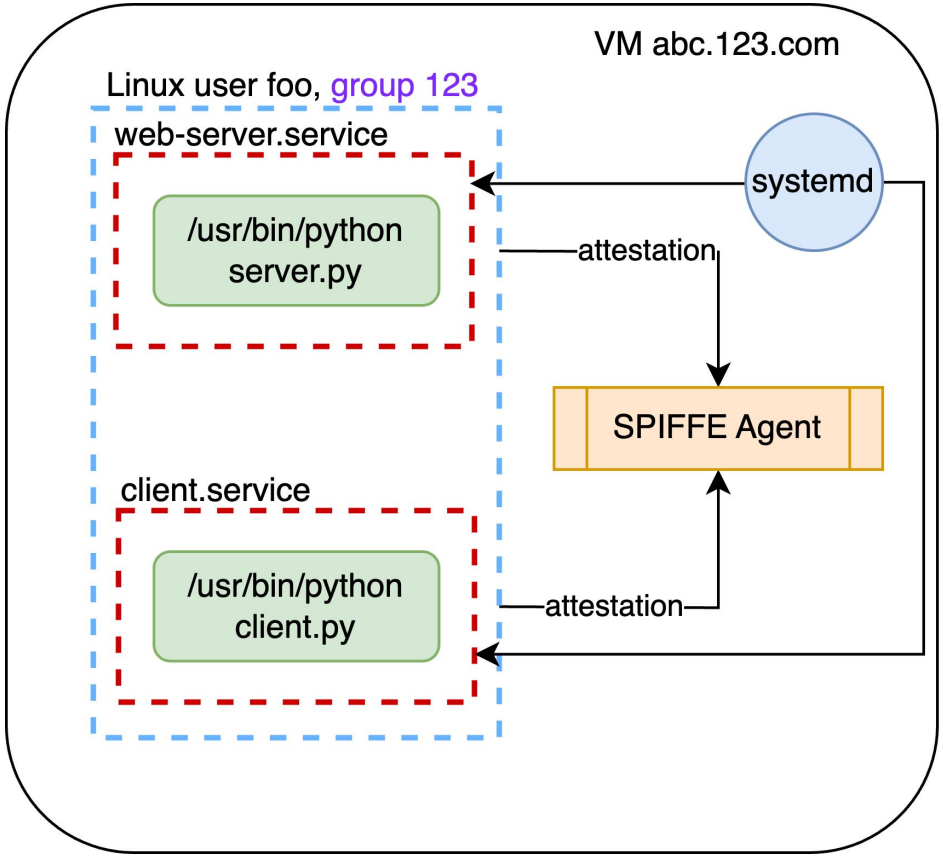
Option 1: Two Linux Users/Group

SPIFFE ID:
spiffe://trust-domain/user/foo/binary/usr/bin/python
spiffe://trust-domain/user/bar/binary/usr/bin/python



Option 2: Other platform attributes

SPIFFE ID:
spiffe://trust-domain/user/foo/systemd/web-server
spiffe://trust-domain/user/foo/systemd/client



How to Choose a SPIFFE ID?

Guiding Principle: SPIFFE ID should support Authz Policies

How to Choose a SPIFFE ID?

Option 1: Based on org structure

- One K8s namespace per service
- One systemd service per team
- One VM per team

How to Choose a SPIFFE ID?

Option 2: Based on security boundaries

Same Linux user/group

=

Same Linux permissions

=

Same security posture

=

Same SPIFFE ID

KubeCon CloudNativeCon North America 2024

spiffe

Additional Resources:

- Website: spiffe.io
- spiffe.io/book
- How to construct SPIFFE IDs
- spirl.com

Want to give us feedback?
Scan this QR Code

SPIRL