Venafi

TECHNICAL BRIEF

Using open source cert-manager with Venafi TLS Protect for Kubernetes

Infosec teams are discovering the open source cert-manager project is used universally in Kubernetes production clusters for machine identity management. TLS Protect for Kubernetes works with cert-manager and allows Infosec to extend their existing Venafi solution to deliver vital new capabilities for policy enforcement and governance over certificate issuance in Kubernetes clusters.

Better security for machine identity management using Kubernetes

Using Kubernetes can easily become highly complex, making it challenging for Infosec teams to manage machine identities effectively. To protect Kubernetes machine identities against outages or data breaches, understanding the differences between open source cert-manager and the additional value and security provided by the TLS Protect for Kubernetes offering is crucial. This document presents an informative comparison of the open source capabilities and highlights the additional security features available from Venafi to ensure the highest level of protection for cloud native applications.

TLS Protect for Kubernetes

Venafi TLS Protect for Kubernetes is a powerful and comprehensive solution for managing machine identities across multiple clusters to give Infosec teams important new capabilities to improve Kubernetes security.

- Full observability of all machine identities in clusters to better manage risk
- Extends security policies to validate certificate issuance in Kubernetes
- Stops untrusted certificates being deployed to clusters
- Enforces and automates security policies for developer teams

About the solutions mentioned in this paper

cert-manager: This refers to the open source project that is freely available from Cloud Native Computing Foundation (CNCF) as well as versions of it that may be supplied by cloud platform solutions or Kubernetes distribution providers.

Using Venafi TLS Protect with cert-manager: Venafi TLS Protect provides machine identity management of TLS certificates for data center applications and is used to work with cert-manager for machine identity issuance in Kubernetes clusters. Existing Venafi customers may know this product by its former name Trust Protection Platform (TPP).

TLS Protect for Kubernetes: This product solution is an extension of TLS Protect that provides additional capabilities for customers operating Kubernetes and OpenShift environments. It offers security assurances and add-ons for cert-manager to provide the highest standards for Kubernetes machine identity management.

Why open source cert-manager is used universally across Kubernetes

cert-manager is an open source project that was originally invented by Venafi for automating X.509 certificate management in Kubernetes environments. It is a powerful and very popular solution for simplifying the complex process of managing TLS certificates, allowing for easy issuance, renewal, and revocation of certificates. By providing a wide range of integrations with popular certificate authorities, including Let's Encrypt and HashiCorp Vault, and of course Venafi, DevOps teams can easily manage certificates from a variety of sources. cert-manager is used to automate the entire certificate management process and eliminates the need for manual certificate management. It allows DevOps teams to configure and manage certificate issuers, certificate requests, and certificates using Kubernetes resources, making it easy to integrate certificate management into cloud native infrastructure as code-based workflows.

Kubernetes machine identity management and support

Infosec teams can facilitate certified builds of cert-manager for enhanced security assurances and improved compliance. Venafi is the leading maintainer of the cert-manager open source project and is committed to ensuring that it remains the top choice for DevOps teams. With Venafi TLS Protect for Kubernetes, these teams can also benefit from expert guidance and support, enabling them to more easily operationalize cert-manager for multi-cluster production environments.

Machine identity management & support	Open source cert-manager	Venafi TLS Protect + cert-manager	Venafi TLS Protect for Kubernetes
Open source cert-manager distribution	Public repository (GitHub)	Public repository (GitHub)	Signed and distributed by Venafi
Automatic X.509 certificate issuance with Certificate Authority integrations	Yes	Yes	Yes
Certificate renewal and rotation	Yes	Yes	Yes
Certificate audit logging	Yes	Yes	Yes
Support multiple DNS providers using webhooks	Yes	Yes	Yes
Pod to pod mTLS csi-driver for using private Issuers	Yes	Yes	Yes
Pod to pod mTLS csi-driver for using SPIFFE with private Issuers	No	Yes	Yes
Istio-csr agent for using private Issuers in a service mesh	Yes	Yes	Yes
FIPS 140-2 compliant distribution of cert-manager	No	No	Yes
cert-manager long term support (LTS)	No	No	Yes (2 years)
Break/fix support and advice	Community based only	Community based only	SLA backed support from Venafi

Machine identity observability & security posture monitoring

Infosec teams can use Venafi TLS Protect for Kubernetes to observe and monitor certificate configuration status across clusters and identify and remove self-signed certificates. This also helps to ensure that certificate issuance comes from a trusted machine identity Issuer, which reduces the risk of rogue or uncontrolled developer activity. Additionally, since cert-manager can support various machine identity Issuers, Infosec needs extra capabilities to observe machine identity usage and ensure that certificate issuance complies with security policies.

Machine identity observability & security posture monitoring	Open source cert-manager	Venafi TLS Protect + cert-manager	Venafi TLS Protect for Kubernetes
Visibility of certificates across all clusters	No	Certificates issued by Venafi	Certificates from all Issuers
Observe certificate contexts for enhanced vulnerability assessment	No	No	Yes
Automated certificate reconciliation to relocate or revoke	No	No	Yes
Detect and alert certificate misconfiguration across all clusters	No	No	Yes
Detect and alert self-signed Certificate Authorities across all clusters	No	No	Yes
Detect and alert unvalidated certificate issuance across all clusters	No	No	Yes
cert-manager version control and health monitoring	No	No	Yes

Machine identity controls for policy & governance

In Kubernetes environments, it is important to enforce trust for all workload activity. Venafi TLS Protect for Kubernetes achieves this by implementing policy controls that ensure that developers adhere to Infosec's certificate issuance policies. Automation is critical for developer teams as it streamlines the workflow and helps ensure consistent policy enforcement. By integrating automated policy controls into the development process, Infosec can work more effectively with DevOps teams and deliver better security and governance.

Machine identity controls for policy & governance	Open source cert-manager	Venafi TLS Protect + cert-manager	Venafi TLS Protect for Kubernetes
Centralized secrets management for Kubernetes workloads	No	Public keys	Public and private keys
Policy controls for certificate issuance across all clusters	No	Yes	Yes
Developer guardrails for validating issuance in clusters	No	No	Yes
Automated token based secure access to cert-manager Issuers	No	No	Yes

Venafi is the cybersecurity market leader in identity management for machines. From the ground to the cloud, Venafi solutions automate the lifecycle of identities for all types of machines—from physical devices to software applications, APIs and containers. With more than 30 patents, Venafi delivers innovative solutions for the most demanding, security-conscious organizations in the world. **To learn more, visit venafi.com**