Cloud Native Certificate Management

Key findings from Venafi research, exploring how cert-manager is used in Kubernetes production environments.

Venafi

cert-manager is one of the most widely used open source projects in the cloud native ecosystem

Cloud native machine identity management using cert-manager with Venafi TLS Protect for Kubernetes is critical for modern DevSecOps.

Venafi is the inventor and market leader of machine identity management. The team that originally invented cert-manager and continues to be its primary contributor is part of Venafi. In 2020, cert-manager was donated to the CNCF (Cloud Native Computing Foundation).

7000+ Slack Members

9000+ Github Stars

CLOUD NATIVE
COMPUTING FOUNDATION

Open source cloud native machine identity management using cert-manager

cert-manager is a very popular open source project that is part of the Cloud Native Computing Foundation and is purposely built to give developer teams effortless certificate management when deploying workloads to Kubernetes clusters.

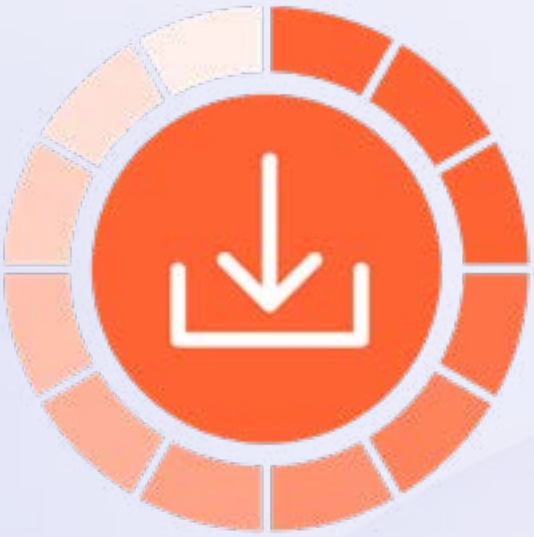
cert-manager is also a powerful and extensible X.509 certificate controller for Kubernetes and OpenShift workloads. It obtains certificates from a variety of Issuers—both popular public Issuers as well as private Issuers—ensures the certificates are valid and up-to-date, and will attempt to renew certificates at a configured time before expiration.

TLS certificates used to protect Kubernetes ingresses are an example of a machine identity. In addition, since most cloud native applications are based on a microservices architecture, mTLS certificates are used to protect pod-to-pod communication within a Kubernetes cluster. These also are examples of machine identities.

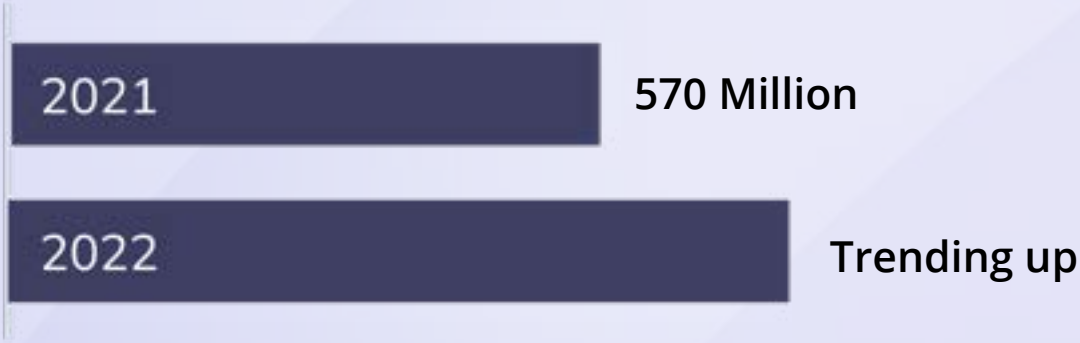
cert-manager is one of the most widely used open source projects in the cloud native ecosystem

In 2021, there were more than 570 million downloads of cert-manager. That is more than half a billion downloads of cert-manager deploying to Kubernetes clusters, or an average of more than 1.5 million downloads a day and this trend is growing even more strongly in 2022. Venafi estimates around 70% of all Kubernetes clusters in existence use cert-manager to ensure workloads are protected using TLS and mTLS encryption.

This report is based on a survey of cert-manager users conducted by Venafi to explore how this popular open source project is being used in production environments. It identifies key security vulnerabilities that may be apparent in Kubernetes production infrastructure with recommendations on how to address security risks.



1.5 Million cert-manager downloads daily

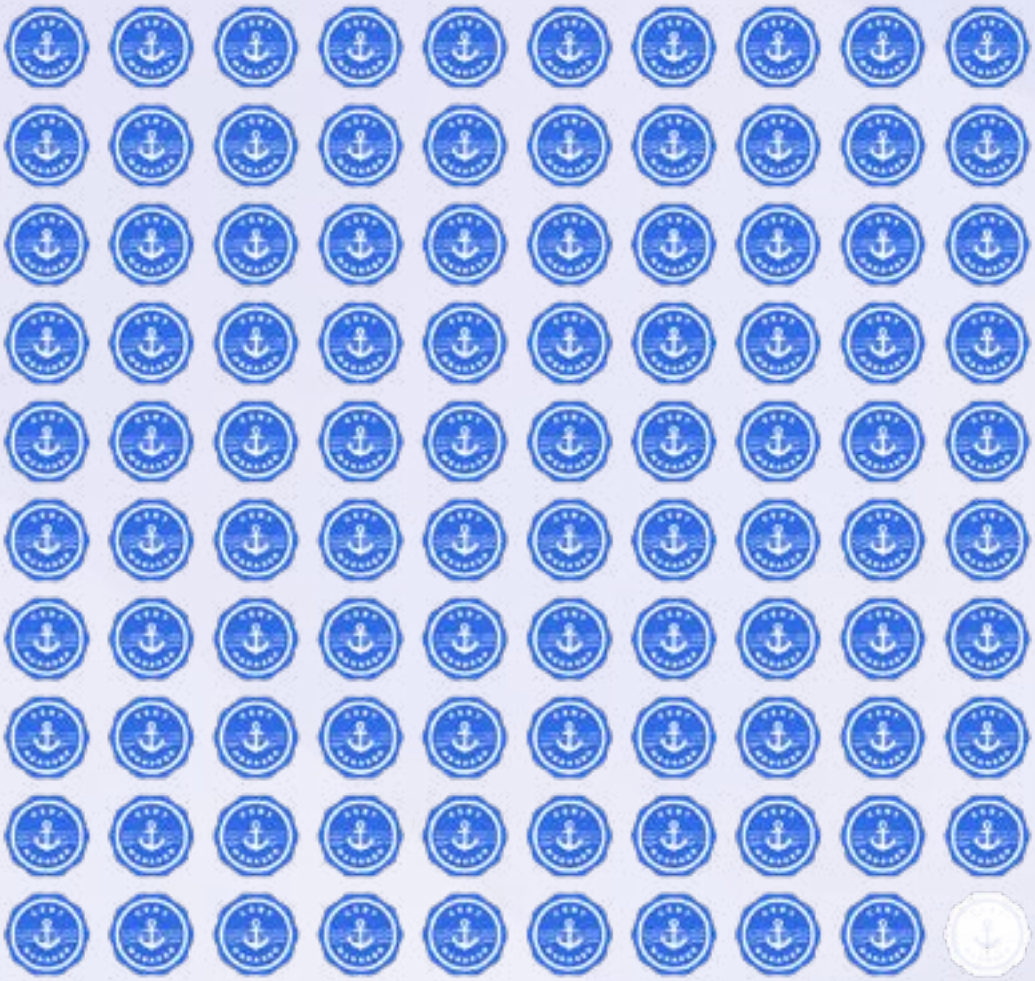


cert-manager has a 99% approval rating and is very clearly appreciated by users across all types of infrastructure

TLS Protect for Kubernetes provides cloud native machine identity management for organizations that are deploying cert-manager across multiple clusters. It provides platform teams and security teams detailed observability and hardened security protection for Kubernetes workloads that use cert-manager for machine identity management in cloud native environments.

Download our cert-manager infographic

Venafi
TLS Protect for Kubernetes

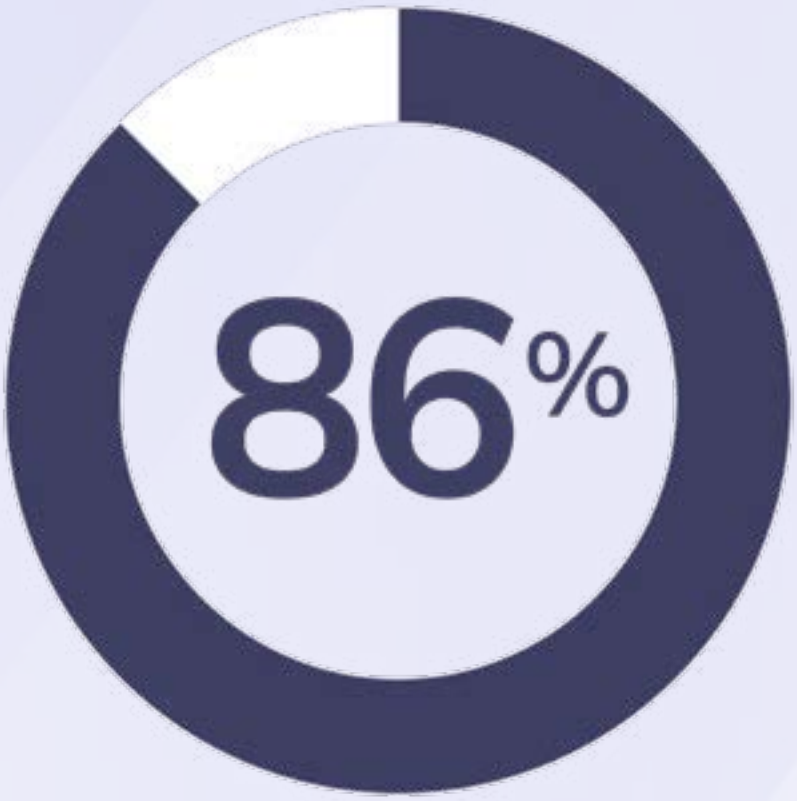


99%

cert-manager is vital for modern DevSecOps

cert-manager is used by developers and platform engineers, yet security teams in organizations that are deploying Kubernetes infrastructure are largely unaware of the vital role cert-manager plays in the security set-up for operating production clusters.

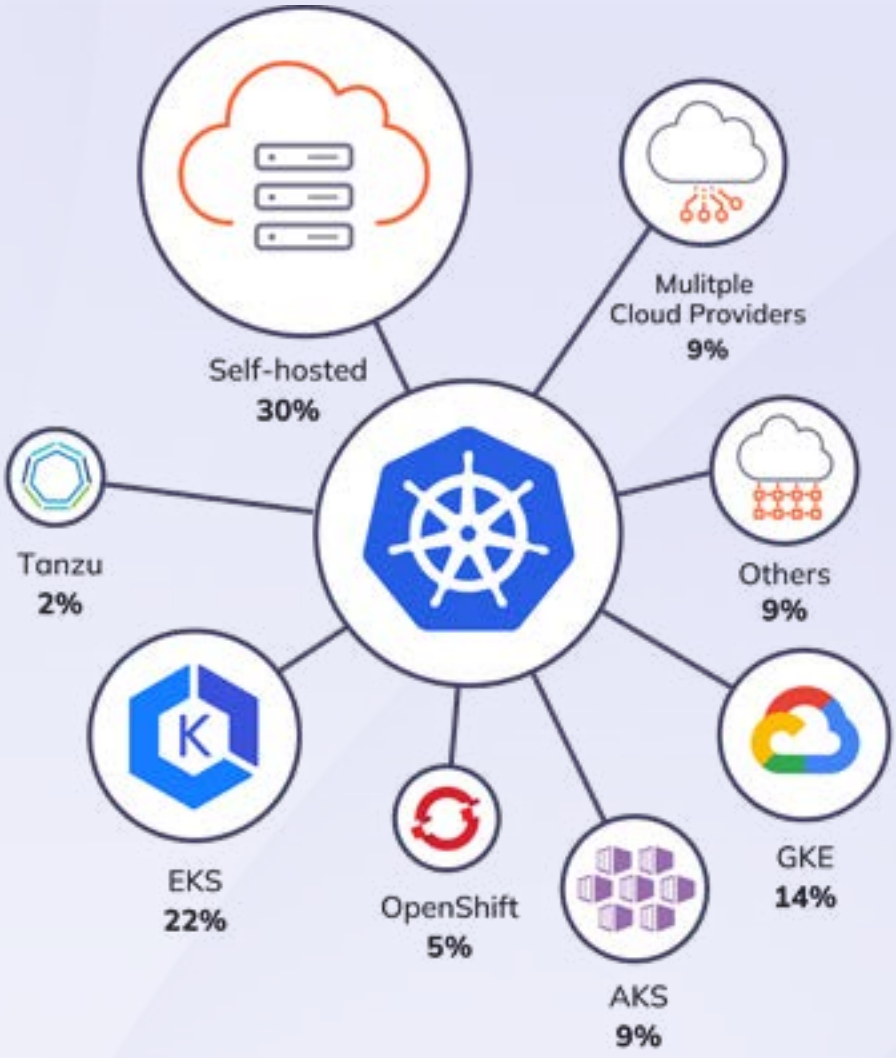
For the vast majority of organizations using Kubernetes, cert-manager is used as policy for each new production cluster, reflecting its strength as a critical tool for bootstrapping each new cluster. Consistency in the way new clusters are created—and avoiding "snowflake" clusters, so that each cluster can be supported uniformly—is important to ensure efficient cluster operations, which will reduce the overall toil for SRE teams.



of new production clusters install cert-manager by default

Security Best Practices

- Security teams needs to be more aware of the existence of cert-manager and the role it plays in production environments.
- Security policy should insist cert-manager is deployed as standard policy for all production environments.
- Venafi can provide expertise to help implement policies along with “hardened” signed builds of cert-manager for effective security.



Nearly 40% of cert-manager users reported they do not use any particular public cloud as their primary provider

Security Best Practices

- Running cert-manager to secure Kubernetes workloads on hybrid clouds will keep developer processes consistent.
- Venafi can help determine an effective strategy to manage machine identities across multiple cloud platforms.
- TLS Protect for Kubernetes is built on top of cert-manager and will provide observability across all cloud native environments.

Self hosted Kubernetes with hybrid clouds is increasingly popular

The majority of organizations feel confident in running Kubernetes on self-hosted infrastructure using hybrid clouds, as opposed to relying on a managed service from a Cloud Service Provider (CSP). A strength of cert-manager is it's high suitability to easily secure workloads across different Kubernetes environments, irrespective of the underlying infrastructure, whether it is public cloud infrastructure or on-premise data centers. Given cert-manager is designed to be cloud agnostic, it is very common to see it used so prominently across multiple cloud providers and self-hosted environments.

When using hybrid or multi-cloud infrastructure, it is important to consider how machine identities will be managed across multiple cloud platform environments. If using each platform's own tools, an enterprise will not have observability across all cloud native infrastructure and will not be able to ensure consistency or control of security policy across all Kubernetes platforms.

Service mesh solutions are driving the use of mTLS for private workloads alongside TLS for Ingress protection

95% of users reported Ingress TLS using as the primary use case for cert-manager in production clusters but many are also using cert-manager to additionally support requirements for mTLS operation. A large number are clearly extending their Kubernetes environments and using cert-manager to support webhook admission controllers.

cert-manager is becoming more widely used to easily integrate private enterprise PKI, using popular service mesh solutions such as Istio and Linkerd. Using service mesh solutions have become popular because they have the capacity to secure and enforce strict mTLS between machine identities running in the cluster.

use a service mesh in production with cert-manager

Security Best Practices

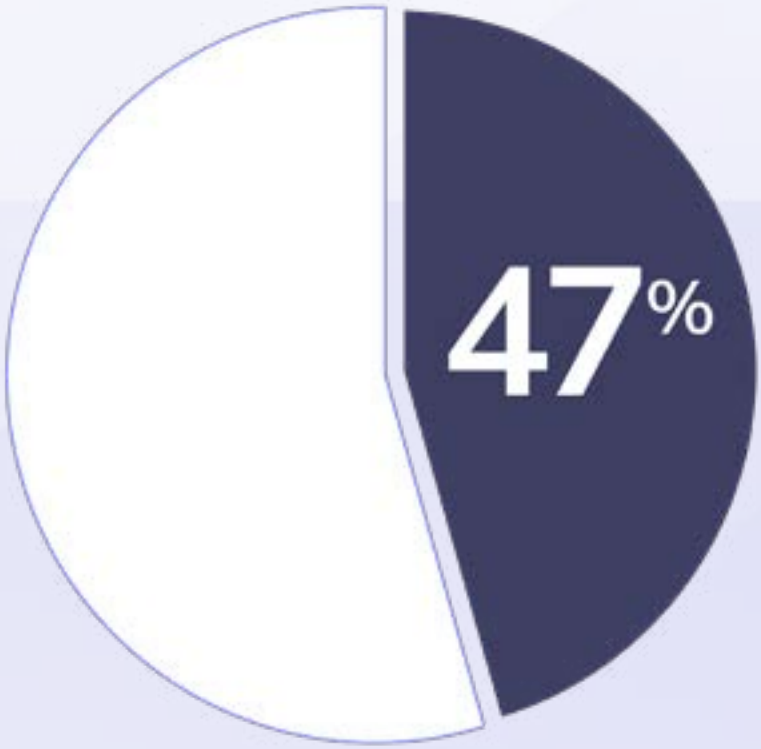
- Service mesh solutions can use cert-manager to integrate with their preferred private PKI provider.
- TLS Protect for Kubernetes will enforce strict security policies and deliver observability for all mesh workloads.
- Venafi provides expertise and support to help organizations shift their service mesh strategy into full production.

Not properly maintaining cert-manager in production is a security risk

Individual production clusters will be using cert-manager to issue and renew hundreds of certificates on an ever-increasing volume. For most organizations, the number of cluster numbers is growing, so it is vital to ensure each instance of cert-manager in production clusters is running the latest version. Running inconsistent versions of cert-manager across multiple clusters will imply potential toil and cost for SRE teams and create “security drift”.

Mind the Security Gap

Around 47% of all cert-manager instances in production clusters are not being proactively maintained with regular updates. At the same time, 86% deploy cert-manager as standard practice for each new production cluster. This implies a “security gap” where running inconsistent versions of the same tool across multiple clusters creates a real security risk. Security teams need to insist that all instances of cert-manager are properly maintained and running the latest released version which will ensure absolute consistency in the way all certificates are issued across all clusters.

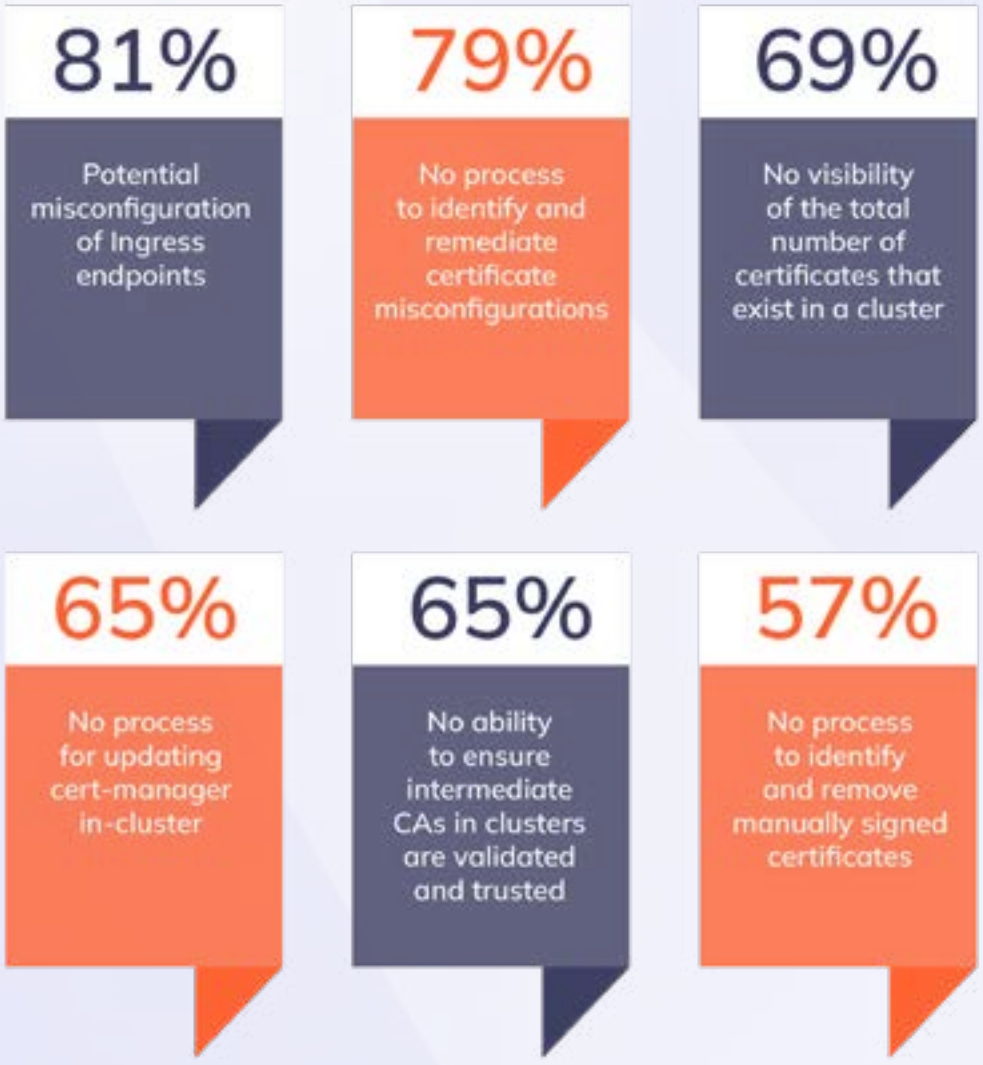


of organizations are NOT running the latest version of cert-manager

Security Best Practices

- TLS Protect for Kubernetes should be used to make sure cert-manager is proactively maintained and running consistently for all production clusters.
- Running outdated versions for cert-manager in production is a security risk that can be easily addressed with the correct tooling.
- Better cert-manager maintenance will significantly reduce the level of toil for SRE teams and reduce exposure to outages.

Machine identity security vulnerabilities that are most relevant when using Kubernetes:



Certificate misconfigurations are a major security concern when using Kubernetes

The danger of not having specific monitoring of Ingress endpoints, and of not being able to remediate certificate misconfigurations, stand out as key areas of potential risk from a whopping 81% of users. Whilst other risks are also apparent, 57% indicated the existence of manually signed certificates in production clusters, indicating poor security practices are evident.

Security Best Practices

- Security teams need to better manage the major concerns highlighted around certificate misconfiguration.
- TLS Protect for Kubernetes provides full visibility of certificate configuration status and will prevent outages and security breaches from misconfigurations.
- Manually signed certificates must be removed from production clusters.

TLS Protect for Kubernetes delivers effective security controls for cloud native environments using cert-manager

Insist cert-manager maintenance is part of the security policy.

Relying on different development teams to maintain cert-manager is a clear risk that TLS Protect for Kubernetes can solve by ensuring all product clusters are consistency running the same version of cert-manager.

Monitor and observe all machine identities operating in production environments.

TLS Protect for Kubernetes monitors the configuration status of all machine identities across all production clusters and provides remediation advice for SRE teams when issues are identified.

Venafi
TLS Protect for Kubernetes

Remove manually signing certificates from production environments.

Security teams should reinforce the need for best practice methods and use TLS Protect for Kubernetes to audit, identify and remove the existence for manually signed certificates in production clusters.

Machine identity management using a service mesh is foundational for zero trust.

Widespread service mesh workload protection for Kubernetes environments can be achieved using cert-manager to integrate their enterprise private PKI solutions with TLS Protect for Kubernetes, providing observability for all mesh workloads.

Survey results as of July 2022

Jetstack, a Venafi company, conducted this survey during March - July 2022 using an online survey form in the cert-manager open source project. 196 responses were received.

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**

CLOUD NATIVE COMPUTING FOUNDATION

Venafi