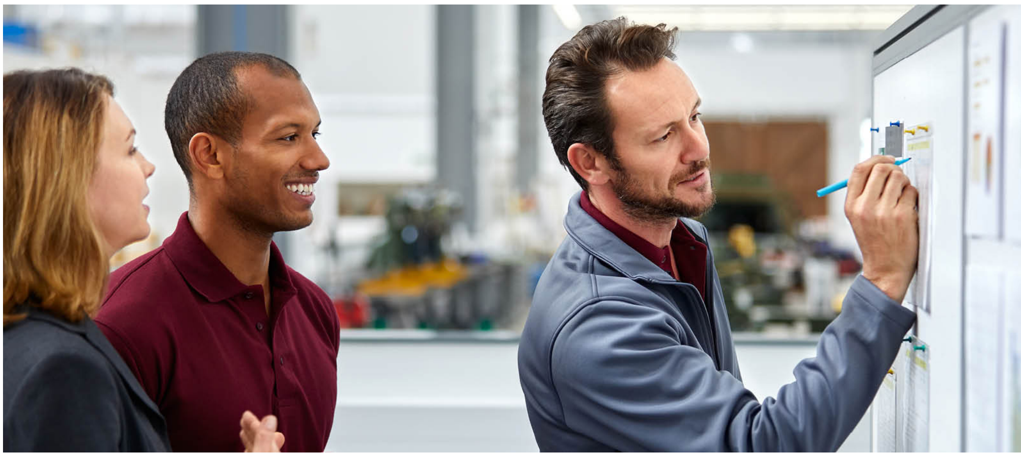
PROJECT COSIGNO—EASILY AND SECURELY EXTEND KERBEROS TO THE CLOUD



THE PROBLEM

As organizations adopt cloud-based infrastructure, application services running in the cloud must be able to establish trusted communication with on-premises systems of record. To allow rapid cloud adoption without compromising security, IT security and engineering teams want to extend their existing security investments into cloud environments without significant modification to existing tooling, practices, or client libraries. Extending existing Kerberos-based authentication becomes a priority.

However, the following obstacles often stymie extending existing Kerberos-based authentication into cloud- and container-based environments:

Manually provisioned credentials are incompatible with cloud automation: Services that participate in Kerberos authentication must first establish a connection to the Kerberos-enabled identity provider (IdP) using a keytab—a long-lived credential. Any actor who obtains this credential can impersonate this service and often do so undetected. In traditional environments, a trusted human operator generates this credential manually and delivers it to the node running the service. However, in cloud- or container-based environments, where nodes and/or services are provisioned dynamically (for example, because of elastic scaling in the public cloud, or dynamic scheduling in a container orchestrator), this process must necessarily be automated. In turn, this requires complete trust in the automation process as well as the workload itself, and any human operator who interacts with it.

Long-lived credentials become an attractive target: Since keytabs are long-lived credentials, they become an attractive target for a malicious actor because they can be used to impersonate a service long after it has been exfiltrated.

Providing network line-of-sight between an IdP and cloud service is complex and poses a risk: In traditional Kerberos authentication, a source service requires a network line-of-sight not only to the destination service it is calling but also to the Kerberos IdP itself (for example, an Active Directory deployment). This can be logistically challenging (given the dynamic nature of cloud networking) and demands that the security team perform additional investigation of the workload and its security privileges, which slows time to delivery.

Load spikes on the IdP disrupt service performance: In traditional environments, a Kerberos keytab is typically exchanged for a short-lived ticket-granting ticket when the service starts or first authenticates a cryptographically expensive operation. However, provisioning services rapidly through automation, elastic scaling, or dynamic scheduling can lead to unexpected load spikes on the IdP, which can have a widespread impact on services dependent on that provider.

Limited auditability of the ticket issuance makes compliance difficult: Compliance and security best practices often require detailed auditing of when and where authentication credentials are issued, which entitlements they confer, and for how long credentials are valid. Conventional IdPs auditing Kerberos ticket issuance typically rely on recording the IP address of the principal user that requested the ticket. In cloud- or container-based deployments, an IP address is not a useful, stable identifier for auditability.

SOLUTION OVERVIEW

Project Cosigno, an industry-first service identity platform, allows you to extend Kerberos-based authentication infrastructure easily and securely to the cloud. The solution securely issues short-lived credentials from on-premises IdPs such as Active Directory to cloud- and container-based services. It also enables cloud services to access on-premises services without exposing IdPs to the public internet or breaking or changing existing risk policies.

Make the right purchase decision. Contact our presales specialists.

Chat Email Call

Get updates

HOW DOES IT WORK?

Project Cosigno achieves the previous results through two core capabilities:

- **Multifactor service authentication based on industry standards (SPIFFE):** Project Cosigno performs a zero-trust attestation process that leans on a configurable union of trusted third parties. It includes cloud provider control planes, container orchestrators, signatures from CI/CD pipelines and trusted OS kernels, hardware security modules, and existing machine identity frameworks to provide a strongly attested identity for cloud (and optionally, on-premises) services. Service identity is thus conferred by a detailed set of identifying attributes of the service in question, rather than by the presence of a service ticket or an IP address. Project Cosigno thus provides a highly trusted identity in dynamic cloud- and container-based environments, and avoids the pitfalls and complexities of conventional secrets management. The identities that Project Cosigno issues conform to the Secure Production Identity Framework for Everyone (SPIFFE) open standard, which is backed by the Cloud Native Computing Foundation (CNCF). Organizations can use these identities to authenticate services in a wide variety of applications.
- **Identity brokering from a Kerberos identity provider to SPIFFE-identified services:** Having established a service's identity through multifactor authentication, an application must then be able to deliver a scoped, short-lived Kerberos ticket to it. Project Cosigno includes an identity brokering capability in which a SPIFFE-identified service may obtain a short-lived Kerberos service ticket from an identity provider. A lightweight, secure Project Cosigno Connector maintains trust between the Project Cosigno server and the IdP, such that these sensitive long-lived credentials need not be delivered to target services directly. It also handles direct interactions with the Kerberos identity provider to generate short-lived service tickets.

Short-lived credentials are then delivered directly to the service via a channel secured by the multifactor authentication process described earlier.

BENEFITS

Strengthen your security posture and protect your existing investments: Multifactor policies establish greater trust in provisioned identities. Short-lived credentials reduce threat radius. The ability to extend your existing on-premises IdPs—such as Active Directory—to cloud and container services strengthens your security posture, reduces the risk of compromise, and helps eliminates the need to rewrite code or rearchitect for cloud and container platforms.

Boost staff and developer productivity: API-driven, automated controls mean that your developers spend less time writing code for security controls or waiting for tickets; and operations teams can deploy, operate, and scale authentication easily across dynamic, heterogeneous infrastructures.

Speed cloud and container adoption: Project Cosigno leverages a common, scalable identity model that works with your existing IdP and is designed for cloud- and container-based environments, to authorize services seamlessly and securely across any platform. It reduces time to market from weeks to minutes. It helps eliminate manual processes and development efforts to authorize a service across multiple platforms. Automated, uniform service identity management reduces application onboarding times from weeks to minutes.

LEARN MORE AT

hpe.com/us/en/software/service-identity-management.html

Hewlett Packard Enterprise

a50002405ENW, August 2020