Case Study

Flux7
an NTT DATA Company

AWS Premier Consulting Partner - DevOps | Migration | Security

Payment System Provider Automates Security with Dynamic Secret Keeper

Financial Services Firm Achieves Security Goals with HashiCorp Vault

Profile

This financial services organization provides its customers with a variety of financial instruments to manage their wealth. From credit cards to banking and personal, home and student loans, this household brand is trusted by millions of Americans. This payment system provider is publicly traded on the NYSE, is part of the S&P 500, and is a member of the Fortune 500.

Business Needs

- Establish secret management that ensures security and compliance
- High Availability

Challenge

As a publicly-traded company managing highly sensitive personal financial data, the company is subject to multiple security regulations and has an overall climate that embraces assertive risk management. However, the financial services firm was relying on a solution for secret management that did not meet the demands of these high-security needs. For example, secret leaks were difficult to detect, it didn't support dynamic secrets and it was difficult to rotate secrets frequently. Having researched a solution, this organization sought a high availability design with HashiCorp Consul and Vault that would result in near-zero downtime for its applications and users while addressing these specific concerns.

Solution

This payment card provider reached out to the Flux7 DevOps consulting team, a HashiCorp partner, to assist. The DevOps consulting service team went to work, helping this organization install and configure a high availability Consul and Vault cluster on top of its existing infrastructure.

The project had 3 goals:

1. Guide the organization's architects and developers during installation and configuration of Vault & Consul:

Together, the teams broke the project down into several week-long sprints, each of which had specific tasks and goals that mapped to the ultimate outcome. As part of this implementation structure, there was a strong focus on teaching the customer the skills it needed to maintain and build upon their solution.

As such, the two teams worked hand-in-hand to install and configure Vault and Consul for the organization, with the customer learning from Flux7 security consultants along the way how to create and configure it moving forward.

We started with a basic, secure installation of Vault with a Consul back-end configured for a few users to be able to administer the platform. Next, we created policies that allowed this firm's IT operations team to take requests for access to an AWS RDS (MySQL/MariaDB) database instance, and issue ephemeral/leased credentials with subsequent expiration. Vault dynamically creates secrets that expire within a given time-period, which is important for meeting specific regulatory and security requirements.

We completed this phase with a highly available federated installation of Vault and Consul that allows administrators, end-users, and applications to have zero downtime due to unavailability.

2. Instruct the company's teams how to use Vault, various backends and the workflows for each one.

Secret backends are the components in Vault which store and generate secrets. We had several backends we were working with at this organization, including Consul, MySQL, Generic Secret, RabbitMQ, PKI, LDAP, and AppRole. While some secret backends, like Generic Secrets, simply store and read secrets verbatim, others, like RabbitMQ, create dynamic secrets, or secrets that are made on-demand.

The Vault authentication backend allows authentication using an existing LDAP server and user/password credentials. This allows Vault to be integrated into environments using LDAP without duplicating the user/pass configuration in multiple places. For AppRole, Vault allows machines and services (apps) to authenticate with Vault via a series of administratively defined roles, thus removing the need to share private keys with all users needing access to infrastructure, and further enforcing the company's security policies.

3. Establishing Security Automation.

In automating security, it was important to this organization that its application developers could build and deploy their applications to Cloud Foundry from their continuous integration workflows. As a result, we worked with this firm to establish a process whereby Developers could push their applications from the CI pipeline to Cloud Foundry (or any deployment target) without exposing credentials to either Jenkins or the end-user.

In addition, secret rotation had been a security concern for this company. As a result, we used Vault's capabilities for automatic rotation to ensure that we were able to handle rekeys and rotation of keys in this highly available deployment.

At the end of the project, cybersecurity engineers were able to automatically rotate any and all keys used to secure Vault and were able to revoke any and all issued secrets. Another key part of the project was to make sure we established an automatic rotation of root account credentials for middleware services without manual intervention and with minimal application downtime. Our architecture ensured that the Consul-template securely communicated with Vault, cycling root credentials based on lease expiration.

Benefits

Vault secret management is a solution of choice when building highly secure and highly available systems. By proactively building a cloud security architecture throughout the AWS IT management process, this firm has decreased risk from manual management. The firm's high availability design for Consul and Vault means that the system has zero downtime for applications and users. In addition, we configured a disaster recovery (DR) site for Consul so Consul clients can failover to the DR site and still continue to function, should it become necessary.

This solution addressed this financial service organization's secret management concerns. We provided a fail-safe mechanism to protect Vault and all of its secrets in a deployment that supported both static and dynamic secrets while easily rotating secrets frequently. The company achieved all these security benefits while also seeing an increase in ease-of-use.

About Flux7

Flux7, an NTT DATA Company, is an IT services firm that helps enterprises reduce the complexities of a new or evolving cloud automation strategy. Agile and DevOps-native, Flux7's robust services portfolio prioritizes a fast path to ROI that meets the immediate needs of technical and innovation teams focused on transformation while forging a secure and stable pathway for security and operational excellence. Learn how Flux7 helps businesses bring solutions to market faster at https://www.flux7.com