HashiCorp® Integration Overview

HashiCorp Vault™ integration within WALLIX Bastion

November 2021

Paris-based WALLIX a software company providing cybersecurity solutions, WALLIX is the European specialist in Identity and Access Security. WALLIX's unified solutions portfolio enables companies to respond to today's data protection challenges. WALLIX solutions guarantee detection of and resilience to cyberattacks, which enables business continuity. The solutions also ensure compliance with regulatory requirements regarding access to IT infrastructures and critical data. The portfolio of unified solutions is distributed through a network of more than 270 resellers and integrators worldwide. Listed on Euronext (ALLIX), WALLIX supports more than 1,500 organizations in securing their digital transformation. WALLIX is a founding member of the HEXATRUST group and has been included in the Futur40, the first ranking of fast-growing companies on the stock exchange published by Forbes France and is part of the Tech 40 index.

San Francisco-based HashiCorp®, a leader in multi-cloud infrastructure automation software. The HashiCorp software suite enables organizations to adopt consistent workflows to provision, secure, connect, and run any infrastructure for any application. HashiCorp open source tools Vagrant, Packer, Terraform, Vault, Consul, and Nomad are downloaded tens of millions of times each year and are broadly adopted by the Global 2000. Enterprise versions of these products enhance the open-source tools with features that promote collaboration, operations, governance, and multi-data center functionality.

HashiCorp Vault™ integration within WALLIX Bastion

The HashiCorp Vault™ of your organization can be used as a secret provider by your WALLIX Bastion so that you can benefit from the strengths of both solutions. To do so, we will see how you need to configure both solutions to make the integration working.

Configuration in the HashiCorp Vault™ secret management solution

You must configure the HashiCorp Vault™ with the following parameters:

- Type: Key/Value (KV)
- Engine version: Version 1

You need to configure your secrets within the HashiCorp Vault™ with the following format:

- Vault root
  - Name of the secret engine
    - Account name in WALLIX Bastion
      - Login (field "login")
      - Password (field "password")
      - SSH certificate (field "ssh_certificate")
      - SSH key (field "ssh_key")
    - Other account name in WALLIX Bastion
      - Login (field "login")
      - Password (field "password")
      - SSH certificate (field "ssh_certificate")
      - SSH key (field "ssh_key")
    - […]

Each secret engine must be associated with a domain and at least one credential (password or SSH key) is required for each login. The SSH key must be entered in the OpenSSH or PEM formats. The certificate corresponds to the content of a signed public key which can be downloaded from the Web interface of WALLIX Bastion. Account data within the solution is UTF-8-encoded.

Configuration in WALLIX Bastion

To use the HashiCorp Vault™ inside WALLIX Bastion, a dedicated global domain must be created as follows:

- **API URL**: URL of the REST API to access the HashiCorp Vault™.
- **Secret engine path**: access path to the vault secret engine.
- **Token**: token to access the HashiCorp Vault™ through the "Token" authentication method. Token must be entered twice (for confirmation).
- **Username**: login of the account to access the vault through the "Userpass" authentication method. This login must correspond to the username of an account in the HashiCorp Vault™ secret management solution.
- **Password**: password of the account to access the vault through the "Userpass" authentication method. If a password is entered, it must be entered again for confirmation.
- **PKCS#12 file**: browse a path to upload a PKCS#12 file to provide the private and public keys to access the vault through the "TLS Certificate" authentication method.
- **PKCS#12 file passphrase**: passphrase to unlock the keys provided via the PKCS#12 file for the "TLS Certificate" authentication method. Passphrase must be entered twice (for confirmation).
- **Role name**: name of the role associated with the Certificate Authority (or "CA") on the server of the HashiCorp Vault™ secret management solution.