IBM Security Verify Privilege DevOps Vault

Balance speed, agility and security.

Rapid, iterative DevOps workflows often expose many security vulnerabilities directly tied to privilege management. Every container, server, and application can have privileged access, dramatically expanding the attack surface for intruders looking for an entry point. It's difficult to balance high-speed, dynamic DevOps practices and RPA deployments with necessary security policies. IBM's Verify Privilege DevOps Vault automates secrets management to provide DevOps teams the speed and agility needed to stay productive without sacrificing security. It addresses all scenarios where secrets are exchanged between machines, including databases and applications for software and infrastructure deployment, testing, orchestration, configuration, and Robotic Process Automation.

Enable greater agility, ease of use, and reduced overhead

- Manage secrets at the speed and scale of DevOps pipelines and RPA deployments.
- Adopt DevOps and RPA principles securely without the infrastructure burden of provisioning on-premises vault instances.
- Eliminate the risk of disparate vault instances and decrease cost of ownership with a SaaS solution.

Highlights

- Minimize Risk: Automate secrets management with consistent, centralized, and auditable processes

- Improve Security: Protect secrets to harden your attack surface and build resilience

- Meet Compliance Mandates: Pass audits and avoid significant financial penalties

- Issue X.509 and SSH certificates, enabling automated certificate signing and distribution.

Get started rapidly

- Cloud-based solution with REST API and command-line interface helps you get started fast.
- Connect to any platform in your DevOps pipeline or RPA deployment, and take advantage of infinite scalability.

Maximize productivity of development, security, and operations teams

- Automate the deprovisioning of secrets when they are no longer needed.
- Minimize privileged account sprawl.
- Allow flexibility with a platform-agnostic solution.
- Eliminate the need to build and maintain your own infrastructure.

De-risk operations within dynamic, elastic environments

- Harden attack surface by controlling privileged access.
- Eliminate the need to hard-code secrets within code and scripts.
- Provide centralized, unified, auditable management and enforcement of secrets access.
- Remove standing access to critical infrastructure with dynamic secrets.

Embrace modern DevOps and RPA principles easily and securely.

IBM Security Verify Privilege DevOps Vault is a high-velocity vault capable of high-speed secrets creation, archiving, and retrieval. It centralizes management, enforces access controls, and provides automated logging trails. You can minimize privilege account sprawl and harden your attack surface to lower risk without sacrificing productivity.

Key Features:

Protect the secrets that DevOps teams and RPA tools need to access applications, services, and IT resources with:

• Advanced automation
• Infinite scalability
• High availability and disaster recovery
• Local caching
• Cloud authentication
• OpenID Connect authentication
• Dynamic secrets for IaaS
• Certificate issuance
• Languages/tool support
• Integration with IBM Security Verify Privilege Vault and SIEM tools
• Sandbox tenant available

```
        (1) File store (default)
        (2) None (no caching)
        (3) Pass (linux only)
        (4) Windows Credential Manager (windows only)
Selection:
Please enter directory for file store (default:/root/.thy):
Please enter cache strategy for secrets:
        (1) Never (default)
        (2) Server then cache
        (3) Cache then server
        (4) Cache then server, but allow expired cache if server unreachable
Selection:
Please enter auth type:
        (1) Password (default)
        (2) Client Credential
        (3) AWS IAM (federated)
        (4) Azure (federated)

Selection:
Please enter username for password auth: admin
Please enter password for password auth:
Please enter password for password auth (confirm):
root@collector:~/thycotic# ./thy auth
{
    "accessToken": "eyJhbGciOiJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJhZG1pbiI6dHJ1ZSwidGVuYW50IjoiYWNhcnJvbGwiLCJleHAiOjE1NDk4NTAxOTQsI
    LhdCI6MTU0OTg0NjU5NCwiaXNzIjoic3Ryb25paG9sZCIsIm5iZiI6MTU0OTg0NjU5NCwic3ViIjoidXNlcnM6YWRtaW4ifQ.XHBip-1xx3TavVBpiMmfkWvEK-3
    P7KAenfhzySKhrAgVdcRIhSZcZieOnCxJT6BbZYr1zam9cv46CdxgeI_5xGrSi44DdMGUU36aYQnJpuXndUP7YyqiXqlpMXOBQ4Src1z-tnTHah0Thg0BJ78hZK0
    _TwCYRm2bBEhQfeOb_4VDplTlNI6HPHHOfDuUOQ8vYlo1AnuQlyILLAbUi4iipgWj-blOW6BWFomp7BuVQLUJYWZOH791yex2alOzommuXh72ZBgqHDzo3RfzOi2
    F3ev1OWbrnrDut0uZbU_2tqyUfW8FVDjEz1uwoOvOLDqD4EqGoQA8wlXzPlNUa3A",
    "expiresIn": 3600,
    "granted": "2019-02-11T00:45:13.258727771Z",
    "refreshToken": "_QtCy4GAz6vEgvXLO_O5lZDSkW6mhXqh",
    "tokenType": "bearer"
}
root@collector:~/thycotic# ./thy secret read main
{"attributes":null,"data":{"password":"nothing2"},"id":"d94a8203-b70f-4a0f-b9ac-e1881b4f04fd","path":"main"}root@collector:~
thycotic# ./thy secret read main -b
{
    "attributes": null,
    "data": {
        "password": "nothing2"
```

Why IBM?

Of the dozens of vendors that offer IAM solutions and services, only IBM infuses deep identity context and expertise into your program, empowering you to give the right people the right access at the right time. That's why IBM is also the only vendor that leads in identity governance and administration (IGA), access management, privileged access management and professional and managed services. With the industry's broadest portfolio of IAM solutions and more than 7,000+ experts focused on supporting your transformation, we can help tackle your toughest identity challenges.

IBM

All statements regarding IBM's future direction and intent are subject to change or withdrawal without notice and represent goals and objectives only.

For more information

To learn more about the IBM Security Identity & Access Management portfolio please visit our main page: https://www.ibm.com/security/identity-access-management

For more information on IBM's Privileged Access Management portfolio please visit: https://www.ibm.com/security/identity-access-management/privileged-access-management