# DevOps Secrets Management

## 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, and the growth of robotic process automation (RPA) further expands those entry points. It's difficult to balance high-speed, dynamic DevOps practices and RPA deployments with necessary security policies. Thycotic's DevOps Secrets Vault automates secrets management to provide DevOps teams the speed and agility needed to stay productive without sacrificing security.

### 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 or cloud vault instances

Eliminate the risk of disparate vault instances and lower cost of ownership with a SaaS solution

### Get started rapidly

Cloud-based solution with REST API and command-line interface help you get started fast

Connect to any platform in your DevOps pipeline or RPA deployment

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 privilege 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.

## DevOps Secrets Vault Benefits

### Minimize Risk

Automate secrets management with consistent and predictable processes

### Improve Security

Protect secrets to harden your attack surface and build resilience

### Meet Compliance Mandates

Pass audits and avoid significant financial penalties

---

**thycotic**

# DevOps Secrets Vault empowers organizations to embrace modern DevOps and RPA principles easily and securely.

DevOps Secrets 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.

```
                    (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": "eyJhbGci0iJSUzI1NiIsInR5cCI6IkpXVCJ9.eyJhZG1pbiI6dHJlZSwidGVuYW50IjoiYWNhcnJvbGwiLCJleHAiOjE1NDk4NTAx0TQsIm
lhdCI6MTU00Tg0NjU5NCwiaXNzIjoic3Ryb25naG9sZCIsIm5iZiI6MTU00Tg0NjU5NCwic3ViIjoidXNlcnM6YWRtaW4ifQ.XHBip-1xx3TavVBpiMmfkWvEK-3B
P7KAenfhzySKhrAgVdcRIhSZcZie0nCxJT6BbZYr1zam9cv46CdxgeI_5xGr5i44DdMGUU36aYQnJpuXndUP7YyqiXqlpMX0BQ4Src1z-tnTHah0ThgOBJ78hZK0F
_TwCYRm2bBEhQfe0b_4VDp1TlNI6HPHH0fDuU0Q8vY1o1AnuQ1yIl1AbUi4iipgWj-b10W6BWFomp7BuVQLUJYWZOH791yex2a10zommuXh72ZBgqHDzo3RfzOi2o
F3ev10WbrnrDut0uZbU_2tqyUfW8FVDjEz1uwo0v0LDqD4EqGoQA8wlXzPlNUa3A",
    "expiresIn": 3600,
    "granted": "2019-02-11T00:45:13.2587277771Z",
    "refreshToken": "_QtCy4GAz6vEgvXL0_051ZD5kW6mhXqh",
    "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"
    },
```

## Key Features

Protect the secrets that the 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
- Dynamic secrets for IaaS
- Certificate issuance
- Languages/tool support
- Sandbox tenant available

### Privileged Account Discovery, Protection, & Monitoring

Identify service, application, admin, and root accounts. Vault credentials, enforce policies, rotate secrets, delegate access, monitor and record sessions.

### Endpoint Privilege Elevation & Application Control

All-in-one solution for least privilege management, threat intelligence, and application whitelisting, greylisting, and blacklisting.

### High-Velocity Secrets Management for Applications, DevOps & RPA

High-velocity vault for automated secrets creation, archiving, and retrieval.

## Free version available at thycotic.com

Thycotic is focused on the most vulnerable attack vector – privilege. With Thycotic you can adopt a multi-layered approach that covers your privilege security needs from endpoints to credentials, ensuring protection at every step of an attacker's chain.

thycotic.com  |  sales@thycotic.com