CYBERARK

SOLUTION BRIEF

CYBERARK CONJUR ENTERPRISE SECURES ANSIBLE BY RED HAT DEVOPS AUTOMATION ENVIRONMENTS

Key Features and Benefits

- Consistently secure and manage passwords and other secrets used by Ansible
- Implement role-based access controls to assign distinct privileges to different users
- Keep secrets out of repositories, code and user-accessible storage to reduce attack surfaces
- Securely deliver secrets managed by CyberArk to Ansible hosts
- Avoid duplicating secrets management functionality across multiple platforms with inconsistent maturity levels
- Audit privileged activity on Ansible hosts

ANSIBLE by Red Hat

CyberArk Conjur Enterprise helps Ansible by Red Hat customers boost security, mitigate risks and improve compliance by protecting and managing secrets used throughout the DevOps automation environment.

CyberArk Conjur Enterprise lets DevOps and InfoSec professionals proactively secure and manage user and machine credentials based on administratively defined policies. The comprehensive secrets management solution protects passwords and other secrets used by users, Ansible, and other DevOps and continuous integration (CI) and continuous delivery (CD) tools. By centralizing and automating secrets management, Conjur Enterprise reduces security vulnerabilities and minimizes attack surfaces, while streamlining operations.

DevOps Secrets Management Challenges

In the dynamic DevOps environment, CI/CD scripts, applications, and microservices are continuously created, executed, and disabled. Each CI/CD tool relies on authentication secrets, which are scattered across physical and virtual machines, and too often hard-coded into application code and playbooks, making them nearly impossible to track and manage.

Worse still, credentials are often issued by build team members, independently of the security organization. Secrets often remain unchanged for months or even years after release. Former employees, contractors and development partners often maintain access to critical applications and systems long after termination, exposing the business to security breaches, malicious attacks and confidential data theft.

Secure and Manage Secrets throughout the CI/CD Pipeline

The integrated CyberArk/Red Hat solution is designed to safeguard and manage secrets used by machines and people throughout the DevOps pipeline. The policy driven solution provides protection, control and manageability by enabling passwords, certificates, API keys, tokens, and SSH keys to be stored securely—out of repositories, out of source code, and off of user-accessible storage systems.

The integrated solution bolsters security by removing hard-coded and unmanaged credentials from scripts and playbooks, and introducing role-based access controls. Centralized, tamper-resistant audit logs are designed to simplify compliance attestation and reporting activities.

Joint Solution Provides Seamless Integration

Conjur integrates seamlessly with Ansible, helping IT teams, DevOps staff and security professionals centralize and simplify the management of security credentials across the application lifecycle. The integrated solution automatically creates, secures and manages credentials used by Ansible playbooks, and is designed to help organizations:

Partner Products

- Red Hat Ansible Automation (Commercial Solutions)
- Ansible (Open Source Solution)

CyberArk Products:

- CyberArk Conjur Enterprise
- CyberArk Conjur Open Source (www.conjur.org)
- CyberArk Core Privileged Access Security Solution (Optional)

Solution Components

CyberArk Conjur Enterprise: Enterprise-ready secrets management solution for cloud and DevOps.

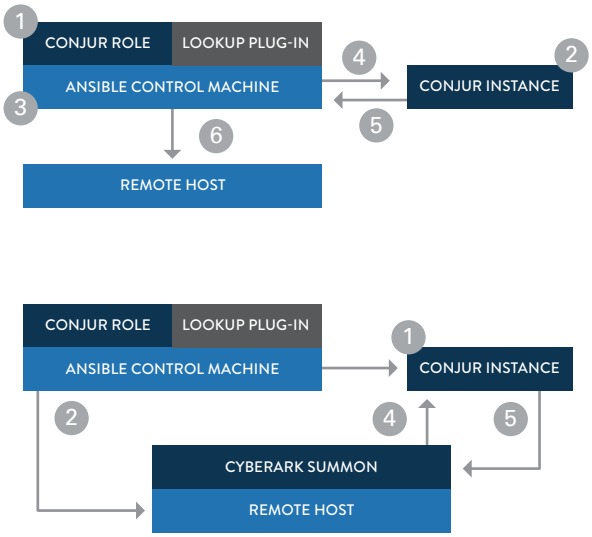
CyberArk Conjur Ansible Role: Enables Ansible control machine to establish Conjur identities via Ansible plays.

CyberArk Conjur Ansible Lookup Plug-in: Enables Ansible control machine to reference secrets secured by Conjur, in Ansible plays.

CyberArk Summon: Enables Ansible remote hosts to authenticate to Conjur and inject secrets into processes.

- Enforce best security practices including encryption and least privileged access
- Use machine identities with role-based access controls to enable granular authentication control
- Produce on-demand reports to support compliance audits
- Securely deliver secrets managed by CyberArk to Ansible hosts
- Avoid duplicating secrets management functionality across multiple platforms with differing maturity level and creating islands of security

The following diagram describes the solution components and workflows.



Use Conjur Lookup Plug-in to Authenticate Ansible Control Machine

1. Install Conjur Role and Lookup Plug-in
2. Load a Conjur policy that grants the Ansible control machine privileges on secrets
3. Run a playbook containing references to secrets stored in Conjur
4. Authenticate the control machine to Conjur
5. Issue the secret
6. Playbook runs containing secret

Use CyberArk Summon to Authenticate Remote Host

1. Load a Conjur policy that grants a class of remote hosts privileges on secrets
2. Run a play assigning a Conjur identity to a remote host
3. Install Summon on the remote host
4. Authenticate the remote host to Conjur
5. Issue the secret

Zero Disruption for Developers

Conjur is specifically designed to minimize the impact of security on development and IT operations teams by streamlining security management. The integrated CyberArk/Red Hat solution lets development organizations improve their security posture and reduce risks, without disrupting operations or impairing service velocity.

About CyberArk

CyberArk is the only security company that proactively stops the most advanced cyber threats – those that exploit insider privileges to attack the heart of the enterprise. The company has pioneered a new category of targeted security solutions to protect against cyber threats before attacks can escalate and do irreparable business damage.

About Red Hat

Red Hat is the world's leading provider of open source software solutions, using a community-powered approach to provide reliable and high-performing cloud, Linux, middleware, storage and virtualization technologies. Red Hat also offers award-winning support, training, and consulting services. As a connective hub in a global network of enterprises, partners, and open source communities, Red Hat helps create relevant, innovative technologies that liberate resources for growth and prepare customers for the future of IT.

ANSIBLE
by Red Hat