

CA Privileged Access Manager 3.X: Manage Access to UNIX/Linux Servers



PRODUCT RELEASE

CA Privileged Access Manager (PAM) 3.0.1 and greater

COURSE TYPE, LENGTH & CODE

- Web-Based Training (WBT)
- Thirty (0:30) minutes
- Course Code: 04PIM20460

PREREQUISITES

- None
- Attendees should have some knowledge of security, authentication systems and basic networking concepts.

Course Overview

Enterprise organizations need a Next Generation Privileged Access Management Platform – enabling them to protect and manage systems and privileged users across hybrid environments, all from a single point of control.

This course topic describes how to create access policies with the various UNIX/Linux connector components included in CA PAM. Begin by using the Discovery feature to search for Linux devices on the network and take those Devices under management. Next, create access policies with manual login. Finally, fully automate the logon process with vaulted credentials.

What You Will Learn

- Discover devices on the network
- Configure manual and automated login to UNIX devices

For Managers

CA Privileged Access Management will enable your team to properly manage users and entitlements, control IT systems, and conform to government regulations, which helps you to reduce costs, raise productivity, and increase user satisfaction.

WHO SHOULD ATTEND

- System Administrator
- Security Administrator
- Application Administrator
- IT Security Analyst
- IT Security Auditor
- IT Architect
- Technical Support Analyst
- Partner
- Sales

Course Agenda

| Manage Access to UNIX/Linux Servers | |
|-------------------------------------|--|
|-------------------------------------|--|

- | | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| <ul style="list-style-type: none">▪ Use the Discovery feature to scan an IP address range for Devices▪ Create an Access Policy for manual logon to UNIX Devices▪ Vault credentials and use them in an Access Policy for automated logon to UNIX Devices | |
|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|



Visit www.ca.com/education to explore the many course offerings, training options, and education solutions available to meet your skill development needs, budget, and travel requirements.