ADMIN-332

Securing Cloudera on premises

Course Overview

Course Type
Instructor-Led Training

Level
Advanced
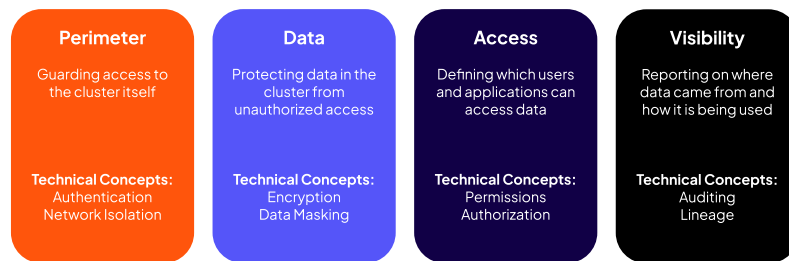
Duration
4 days

Platform
Cloudera on premises

Topics Covered
- Architecture for secure Cloudera Clusters
- Implementation of directory services
  - LDAP
  - KDC
- Deployment of Auto-TLS and Kerberos
- Theory and installation of:
  - Apache Ranger
  - Apache Atlas
  - Ranger Key Management Service
  - Apache Knox Gateway
- Building Ranger Resource Policies
- Creating Atlas Classifications
- Building Ranger Tag Policies

About This Training

The Cloudera platform is intended to meet the most demanding technical audit standards. The significant improvements in Cloudera architecture and components make Cloudera "Secure by Design." This four-day hands-on course is presented as a project plan for Cloudera administrators to build fully secured Cloudera clusters.

Perimeter	Data	Access	Visibility
Guarding access to the cluster itself	Protecting data in the cluster from unauthorized access	Defining which users and applications can access data	Reporting on where data came from and how it is being used
Technical Concepts: Authentication Network Isolation	**Technical Concepts:** Encryption Data Masking	**Technical Concepts:** Permissions Authorization	**Technical Concepts:** Auditing Lineage

The course begins with implementing Perimeter Security by installing host level security and Kerberos. Next, students protect Data by implementing Transport Layer Security using Auto-TLS and data encryption using Key Management System and Key Trustee Server (KMS/KTS). Following this, in the third stage, students control access for users and to data using Apache Ranger and Apache Atlas. The fourth stage focuses on visibility practices, teaching students how to audit systems, users, and data usage. Finally, the course introduces Cloudera practices for Risk Management in a fully secured Cloudera platform. This course is 60% exercise and 40% lecture.

Who Should Take This Course?

This immersion course is designed for Linux Administrators transitioning to Cloudera Administrator roles. Students must have proficiency in Linux (e.g., navigating the file system, using basic commands) and Linux text editors (e.g., vi, nano). Familiarity with Directory Services, Transport Layer Security, Kerberos, and SQL select statements is recommended. Prior experience with Cloudera products is required. Students must have reliable internet access to connect to the classroom environments hosted on Amazon Web Services.

ADMIN-332

Securing Cloudera on premises

Cloudera Secure by Design

- Cloudera Security Models
- Cloudera Security Pillars
- Cloudera Security Levels

Project Planning for Cloudera

- The Importance of Project Planning
- Outline of Project Plan
- Roles and Responsibilities of a Cloudera Administrator

Directory Services

- Comparing Directory Services
- Lightweight Directory Access Protocol
- FreeIPA or Active Directory

Manage Identities on Cloudera

- Identity Management Architecture
- The purpose of PAM
- Cloudera Manager and PAM

Isolated Networks

- Architecture for Network Security
- Building an Isolated Network

Quality Controlled Hosts

- Cloudera Requirements for Hosts
- Recommendations for deployment hosts

Protect Data in Motion

- Theory for Security Protocols (TLS and SASL)
- Tools: openssl and keytool
- Architecture for Enterprise Certificate Authorities
- Deploying TLS using Auto-TLS
- Deploying SASL

Authentication with Kerberos

- Architecture for Kerberos
- Kerberos CLI
- Deploying Kerberos
- Managing Cloudera services within Kerberos

Shared Data Experience (SDX)

- Architecture for Apache Ranger
- Deploying Ranger
- Deploying Infra Solr
- Deploying Atlas

Data at Rest

- Theory for KMS/KTS
- Deploying KMS/KTS
- Encrypting Data at Rest

Single Sign-On with Knox Gateway

- Architecture for Knox Gateway
- Installing Knox Gateway
- Deploying Knox Gateway SSO
- Accessing services through Knox Gateway

Authorization with Ranger

- Creating Ranger KMS Encryption Zones
- Creating Ranger Security Zones
- Creating Ranger resource policies

Classify Data with Atlas

- Ranger Policies for Atlas
- Searching Atlas
- Classifying Data with Tags
- Creating Ranger Tag Policies
- Creating Ranger Masking Policies

VERSION 2.0.0

ADMIN-332

Securing Cloudera on premises

Audit Cloudera

- Auditing access on hosts
- Auditing users with Ranger
- Auditing lineage with Atlas

Commission Cloudera

- Validating Security Level 2
- Checklist for commissioning Cloudera

Achieving Compliance

- Regulatory Compliance
- Roadmap to Security Level 3