

ADMIN-332: Building Secure Clusters

CDP is Secure by Design

Course Overview

Course Type

Instructor-led training course

Level

Intermediate

Duration

4 days

Platform

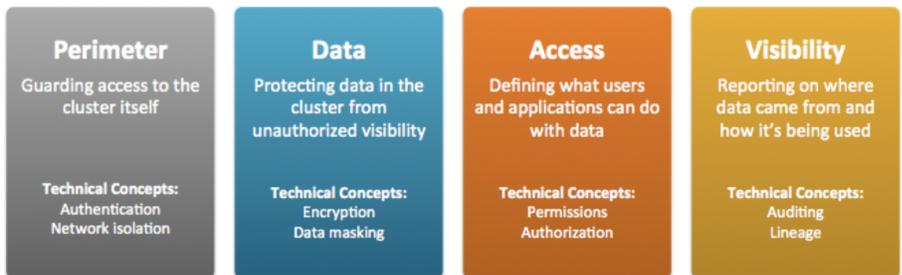
CDP Private Cloud Base

Topics Covered

- Architecture for CDP Clusters
- Requirements for an isolated network
- Comparison of Active Directory to Identity, Policy, and Audit
- Theory and installation of
 - Kerberos
 - Auto-TLS
 - Ranger
 - Atlas
 - Ranger Key Management Service
 - Knox Gateway
- Building Ranger Resource Policies
- Creating Atlas Classifications
- Building Ranger Tag Policies

About This Training

The significant improvements in CDP architecture and tools makes CDP “Secure by Design.” The Cloudera Data Platform is intended to meet the most demanding technical audit standards. This four-day hands-on course is presented as a project plan for CDP administrators to achieve technical audit standards.



The first project stage is implementing Perimeter Security by installing host level security and Kerberos. The second project stage protects Data by implementing Transport Layer Security using Auto-TLS and data encryption using Key Management System and Key Trustee Server (KMS/KTS). The third project stage controls Access for users and to data using Ranger and Atlas. The fourth stage teaches Visibility practices for auditing systems, users, and data usage. This project stage also analyzes applications in terms of vulnerabilities and introduces CDP practices for Risk Management in a fully secured Cloudera Data Platform. This course is 60% exercise and 40% lecture.

Who Should Take This Course?

This immersion course is intended for Linux Administrators who are taking up roles as CDP Administrators. We recommend a minimum of 3 to 5 years of system administration experience in industry. Students must have proficiency in Linux CLI. Knowledge of Directory Services, Transport Layer Security, Kerberos, and SQL select statements is helpful. Prior experience with Cloudera products is expected, experience with CDH or HDP is sufficient. Students must have access to the Internet to reach Amazon Web Services.

CDP Admin: Security by Design

Training Outline (Page 2 of 2)

Security Management

- CDP Security Models
- CDP Security Pillars
- CDP Security Levels

Project Planning

- The Importance of Project Planning
- Roles and Responsibilities

Isolated Networks

- Architecture for Network Security
- Building an Isolated Network

Identity Management

- FreeIPA or Active Directory
- Identity Management Architecture
- Pluggable Authentication Modules
- Lightweight Directory Access Protocol
- Cloudera Manager Roles
- Managing Super Users

Quality Controlled Hosts

- CDP Requirements for Hosts
- Recommendations for deployment hosts

Encrypt Network Traffic

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

Authentication with Kerberos

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

Shared Data Experience (SDX)

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

Data at Rest

- Theory for KMS with KTS
- Deploying KMS with 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 Data Encryption Zones
- Creating Ranger Security Zones
- Creating Ranger resource policies
- Creating Ranger masking policies

Classify Data with Atlas

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

Audit CDP

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

Commission CDP

- Validating Security Level 2
- Checklist for commissioning CDP

Achieving Compliance

- Regulatory Compliance
- Roadmap to Security Level 3