

Implement Advanced Server Access

Duration: 2 days (8hrs/day)

Prerequisites: Okta Essentials or minimum experience in Okta. Experience with SSH and RDP protocols. Experience managing Linux and Windows servers.

Course Objective: In this course, you will get hands-on practice using an Okta org to configure identity first, zero-trust access management for your cloud and on-premise infrastructure.

Lab Requirement: Koenig DC

Module 1 - Introduction TO ASA

Define the concepts behind Advanced Server Access

Describe ASA components

Understand how Okta Identity Cloud is leveraged for server access

Module 2 - ASA Architecture

Understand ASA architecture

Describe bastions and gateways

Understand server and client agents

Describe networking requirements

Module 3 - Team Configuration

Create a Team (ASA tenant)

Integrate with Okta Org for SAML SSO and provisioning

Module 4 – Provisioning

Understand SCIM provisioning

Configure provisioning to Linux and Windows servers

Understand team roles

Customize user attributes

Module 5 - Server Enrollment

Install ASA agents

Configure enrollment tokens

Understand agent configuration options

Configure a gateway

Module 6 – Policies

Configure access policies

Create a sudo entitlement

Describe the client approval process

Configure client preauthorizations

Module 7 – Clients

Describe client enrollment

Install the client agent on Windows and Linux

Use the command line interface

Connect to Linux and Windows servers with various tools

Module 8 – API

Configure an API service account

Describe several API endpoints

Set up Postman with the ASA collection

Module 9 – Cloud Servers

Understand cloud accounts

Deploy and enroll an AWS server with Terraform and user data

Module 10 - Monitoring and Troubleshooting

Understand event logging

Access SSH session logs

Understand how to configure log forwarding

Describe how to resolve common authentication and authorization issues