Enterprise Computing Solutions - Education Services

TRAINING OFFERING

You can reach us at:

Arrow Enterprise Computing Solutions Ltd, Part 1st Floor, Suite 1D/1, Central House, Otley Road, Harrogate, HG3 1UG

Email: educationteam.ecs.uk@arrow.com
Phone: 0870 251 1000

F5 Distributed Cloud Services Bundle

CODE:	LENGTH:	PRICE:
F5N_F5XC-BDLE	40 Hours (5 days)	£3,995.00

Description

F5 Distributed Cloud Services Bundle (instructor-led) is a comprehensive course which will prepare you for deploying F5XC networking, security, and application management services. It includes the full course content from both the Administering Applications in F5 Distributed Cloud Services and Securing Applications and APIs with F5 Distributed Cloud Services courses.

F5 Distributed Cloud Services (F5XC) learning experience mimics real-world applications, including adapting to and tackling outages and performance effects.
F5XC provides a SaaS-based solution for managing data centers, cloud, and hybrid cloud container-based customer applications. It is implemented as a collection of hundreds of Kubernetes microservices, geographically distributed across the globe, accessed via a browser-based console.
F5XC manages, maintains, and scales the platform and microservices. Customer solutions for network infrastructure and application management are delivered by interconnecting these services. F5XC SaaS is not monolithic and unchanging. It is live on the Internet, dynamic, and subject to regular updates.

Prerequisites

There are no prerequisites before attending this course, but the following knowledge is helpful:

- Experience with any cloud provider
- Basic networking skills including a basic understanding of routing, firewalls (application and network layer), proxies and load balancers
- Basic understanding of Kubernetes, pods, and containerization concepts

Programme

Administering Applications in F5 Distributed Cloud Services
Chapter 1: Introduction

- Resources
- Benefits of F5XC
- How F5XC works
- Primary F5XC Deployment Types

Chapter 2: (labs) Intro to Training Environment and F5XC Console

- Accessing Training Environment
- Intro to Console
- Creating Namespace
- Building Site Infrastructure
- Configuring Cloud Credentials
- Creating Cloud Site

Chapter 3: Site and Infrastructure Management

- Tenants and Namespaces
- Labels and Key Pairs
- Virtual Sites
- Load Balancing and Origin Pools
- Architecture of Infrastructure Objects
- Examples of Objects used in Production

Chapter 4: (labs) Using F5XC Objects to prepare AWS Application

- Creating and Sending Alerts
- Viewing Site Status
- Creating Origin Pool for TCP Load Balancer
- Creating Delegated DNS Domain
- Creating TCP Load Balancer

Chapter 5: How F5XC Uses Kubernetes

- Kubernetes (K8s) Overview
- The Need for Kubernetes
- Containers, Pods, Nodes, Services, Clusters
- Virtual K8s

Chapter 6: (labs) Creating vK8s and Alerts on F5XC Gateway

- Use F5 Simulator to Deliver Modern App at the Edge
- Creating vK8s on F5XC Gateway
- Exploring Basic Kubernetes Commands

Chapter 7: Introduction to Distributed Cloud Mesh

- Services vs Service Mesh
- Components of Service Mesh
- Service Mesh and Sidecar Proxies
- F5XC Cloud Mesh
- Mesh vs App Stack
- App Stack and Mesh Working Together

Chapter 8: (labs) Expose, Access, Protect, Reroute, and Troubleshoot AWS site

- Creating Origin Pool and Health Check for HTTP(s) Load Balancer
- Creating HTTP Load Balancer and View Application
- Activating WAF
- Creating Routing Configuration
- Deploying Virtual K8s Workload for Application
- Automation with Terraform
- Viewing Data in Dashboards
- Challenge Lab: Deploy and Troubleshoot Replica site
- Challenge Lab: Access AWS Instance via SSH

Securing Applications and APIs with F5 Distributed Cloud Services

- Introduction and Agenda
- Lesson Objectives
- Lesson Topics
- Overview of how F5XC WAAP protects web apps in any cloud, edge, or on-premises environment
- Defining core features and use cases

Module 1: Introduction to Distributed Cloud WAAP and WAF Deployment

- Exploring the security flow through application proxy
- Lab: Deploy Juice Shop (target application) on an HTTP load balancer and configure API endpoint discover.
- Create load balancer and connect origin pool to expose Juice Shop application
- Enable API discovery (so that we can discuss API protection and have ready examples)
- Run some traffic and review request log

Module 2: Overview of Web Application Processing

- Overview of web application communication elements
- Overview of HTTP message structure (headers and methods)
- Parsing HTTP requests
- Lab: Exploring the target application

Module 3: Overview of Web Application Vulnerabilities

- A taxonomy of attacks: the threat landscape
- Common exploits against web applications (OWASP Top 10, OWASP API)
- Lab: Exploiting web application vulnerabilities

- SQL injection
- Cross-site scripting
- Bypass security using a poison null byte
- Forceful browsing

Module 4: Mitigating Threats with Web Application Firewall Policies

- Defining web application firewall processing at layer 7
- Applying different protections to a load balancer
- Defining violations and false positives
- Reviewing RFC 2616 as it drives protocol compliance
- Differentiating positive and negative security
- Differentiating blocking and monitoring actions
- Reviewing security event logging
- Defining Threat Campaigns
- Defining Attack Signatures
- Lab: Create App Firewall, enable blocking mode, attach to load balancer
- Lab: Launch XSS attack and observe security processing in the log
- Lab: Launch SQL injection attack and observe security processing in the log
- Lab: Launch poison null byte attack and observe security processing in the log

Module 5: Manage Security Events with Exclusion Rules

- Defining exclusion rules
- Analyzing elements and contexts of exclusion rules
- Lab: Create an Exclusion Rule for Two Attack Signature IDs

Module 6: Mitigating Threats with Service Policies

- Differentiating protections at namespace vs. load balancer levels
- Exploring service policy rules, policies, and policy sets
- Handling traffic flow
- Enforcing layer 7 elements of HTTP processing
- Lab: Practicing service policy protections for geolocation enforcement, file types enforcement, method and path enforcement, and IP address enforcement

Module 7: Deploying Bot Defense

- Classifying and categorizing bots (good/suspicious/malicious)
- Reviewing bot signatures
- Configuring bot defense on the XC load balancer
- Lab: Mitigating an attack from an automated agent (python scripts for bad traffic and credential stuffing/brute force)

Module 8: Mitigate Threats using Machine Learning and Artificial Intelligence

- Defining Malicious User Detection
- TLS fingerprinting
- JavaScript challenges/client side defense
- Lab: Deploying Machine Learning

Module 9: Protecting Public APIs

- Defining an API
- Defining API specifications
- Defining a RESTful API
- Recognizing API endpoints
- Defining Shadow APIs
- Defining OpenAPI 3.0 and the Swagger specification
- Analyzing API routing in F5XC
- Analyzing API protection in F5XC
- App firewall (OWASP vulnerabilities)
- CAPTCHA/JS challenges
- Network firewall
- API usage characterizations
- User anomaly detection
- API rate limiting (threshold configuration)
- API Learning
- Endpoint learning
- Schema learning
- Behavioral firewall/business logic markup

- Lab: Machine Learning Lab
- Review discovered APIs
- Configure malicious users mitigation
- Configure user identification
- Configure load balancer
- Test XSS (without WAF policy)

Module 10: API Automation using Postman

- Introduction to Postman
- Defining environments
- Defining collections
- Reviewing variables
- Lab: Use a postman collection to create a WAF policy for a namespace
- Lab: Use a postman collection to create service policies for a shared namespace

Session Dates

On request. Please Contact Us

Additional Information

This training is also available as onsite training. Please contact us to find out more.