PARTNER PROGRAM GUIDE

F5 Partner CNF Certification Program Guide

A guide for F5 and its partners to validate successful set-up, on-boarding, integration, deployment, and lifecycle management of CNFs in a cloud-native environment to ensure base interoperability and integration.

GARTNER ESTIMATES THAT 90% OF GLOBAL ORGANIZATIONS WILL BE RUNNING CONTAINERIZED APPLICATIONS IN PRODUCTION BY 2026—UP FROM 40% IN 2021. IN ADDITION, BY 2026, 20% OF ALL ENTERPRISE APPLICATIONS WILL RUN IN CONTAINERS—UP FROM FEWER THAN 10% IN 2020.

F5 Partner CNF Certification Program - What Does It Do?

The F5 Partner CNF Certification Program is designed to vet the functionality and interoperability of any new cloud-native network function (CNF) partners who plan to run on F5 cloud-native infrastructures. Following industry standard practices, we provide the most likely use cases, scenarios, and testing objectives to validate successful set-up, onboarding, integration, deployment, and lifecycle management in a service mesh (Carrier-Grade Aspen Mesh (CGAM)) and service proxy (F5 BIG-IP® Next™ Service Proxy for Kubernetes (SPK)) architecture prior to entering customer labs and deployments.

To scale better to the data-heavy needs of consumers and enterprises, telco providers are now migrating to cloud-native network architectures. Vendors who want to use the new ecosystems need to confirm interoperability, functionality, and security prior to deployment.

The F5 portfolio of cloud-native solutions enables service providers to build and deploy a highly flexible, scalable, performant, and secure network to meet the demands of today's application-based economy, which relies heavily on microservices. There are also new tools built into this architecture that provide for cluster visibility, management, and automation of security policies.

How to assure customers that the proposed cloud-native solution will work?

Faced with an array of different options, approaches, and untried vendors, service providers want to minimize risk and be assured that the cloud-native products and solutions they are investing in:

- Have simple deployments
- Interoperate successfully with key products and solutions
- Can successfully minimize integration issues
- Can be optimized for performance and efficiency
- Can maximize security policies and the security posture for both the CNF and the platform

Our rigorous auditing process will provide your customers with confidence that your CNF solution will meet these criteria. Testing your CNF solution on either of F5's SPK and CGAM solutions—or both—ensures that your products interoperate effectively, securely, and at optimum performance. And as an additional option, F5 can provide professional services support for the solution (when the paid program is selected).

Certification Program Details and Use Cases

The partner performs the testing with specified F5 support and input. F5 currently offers two certification program options.

Free Tier, Partner Certified, and Non-Supported

With the first certification program option, F5 provides:

- Access to evaluation software (i.e., SPK and CGAM)
- Access to self-service technical resources in F5 DevCentral
- Alliance Program administration contact
- F5 logo usage rights
- F5 event participation

Paid for Supported

Includes the same support as Free Tier, plus:

- Certification supported by F5
- Alliance Team support
- F5 Support and Professional Services
- Participation in customer workshops

PROGRAM PREREQUISITES

Prerequisites for all: Signed application, mutual non-disclosure agreement (MNDA), certification agreement

Prerequisites for BIG-IP Next Service Proxy for Kubernetes

Kubernetes 1.21 and 1.23, with one of the following platforms:

- Red Hat OpenShift Container Platform Certification - version 4.7 and later
- Calico CNI plug-in (future)
- Wind River Linux version LTS 18 (future)
- Calico CNI plug-in with VMware TCP Suite 2.2 (future)

Prerequisites for Carrier-Grade Aspen Mesh 1.11.8-am2 release

- Red Hat OpenShift Container Platform 4.7+ (Kubernetes 1.20)
  - It is recommended that you use Helm 3.8 for this release
  - F5 Aspen Mesh requires third-party JSON Web Tokens to be enabled in your K8s cluster
- Red Hat OpenShift Certification - version 4.6 and later
  - Software compatibility analysis
  - Documentation
  - Lab Set-up (hardware and software in place)
  - Resources assigned
    - Technical proof-of-concept (POC)
    - Business POC

CERTIFICATION WORKFLOW

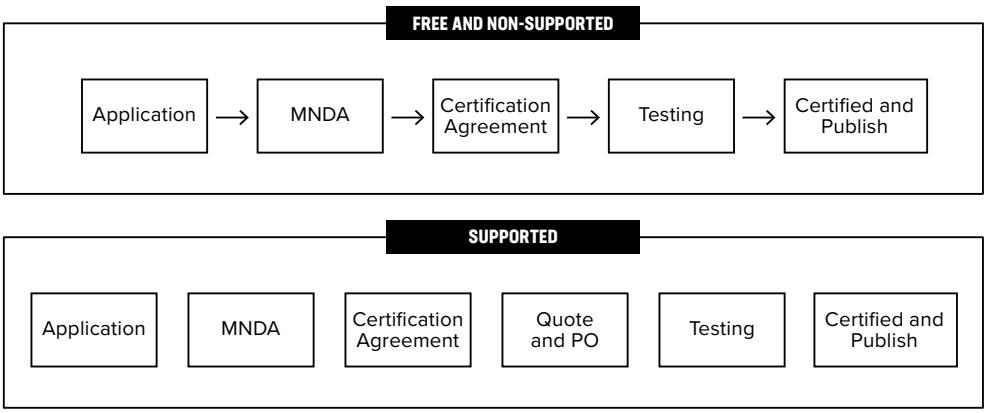

Figure 1: Rigorous auditing and personalization ensures that your chosen CNF solution interoperates effectively, securely, and at optimum performance.

TESTING PROCESS

Fill out the F5 Partner Application.

1. Prerequisite entry criteria met

- Lab set-up (hardware in place)
- Resources assigned
- MNDA signed

2. Pre-testing preparation call

- Review set-up
- Test plan guidelines and review
- Q&A

3. Testing (within 90 business days)

- Partner tests and validates CNF functionality based on test plan

4. Test report submission

5. F5 verification

- F5 verifies that CNF integrates with BIG-IP Next SPK and F5 Carrier-Grade Aspen Mesh infrastructure test plans

6. Certification granted

7. Lifecycle commitment

- Continuous certification to ensure interoperability across release

USE CASES

At this time the program will specifically provide testing for four different deployment scenarios:

1. Custom Ingress Gateway ingress-egress load balancing for multi-pod deployments

- Ingress-egress to and from single IP
- Ingress-egress to and from multiple IPs

2. Service Mesh Mutual Transport Layer Security (mTLS)

- Sidecar (SC) to SC within the mesh
- Non-SC to non-SC in-mesh
- SC to non-SC in-mesh and out-mesh
- Non-SC to SC out-mesh to in-mesh
- SC to non-SC in-mesh to non-K8 envoy
- Non-SC to SC non-K8 envoy to in-mesh

3. Authentication of Cloud-native Network Function (CNF) Service

4. CNF authentication token verification in service mesh

Program Benefits

- Reduces deployment time and complexity; minimizes risk of incompatibility by exposing initial CNF environment setup and integration issues
- Validates that the CNFs can be successfully onboarded and deployed
- Tests CNFs in a cloud-native environment to ensure they do not break after the deployment
- Provides confidence that CNFs work right away for the service provider customer
- Allows service providers to build repeatable reference architectures and blueprints for faster time-to-market
- Streamlines support costs
- The service provider's customer labs can work on more use cases to create multiple tested and certified reference architectures

Business value

- Verified on leading Kubernetes and Container PaaS distributors (e.g., OpenShift, Wind River, F5)
- Security scanning for better security practices
- Rapid on-boarding for faster time-to-market
- Continuous certification for continual infrastructure validation
- Lifecycle management with F5 and Container Platform Partner(s)
- Competitive differentiation through certification
- Increased revenue through certified products

Get Started Now

Get certified now to strengthen customer confidence in your solution. Complete an application form.

©2022 F5, Inc. All rights reserved. F5, and the F5 logo are trademarks of F5, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com.
Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, expressed or implied, claimed by F5, Inc.
DC0922 | PG-949495659