

The header graphic features a dark blue background with a central white icon of a cloud containing a shield and a key. This icon is connected by white lines to several smaller white cloud icons positioned around it. The overall design is clean and modern, emphasizing cloud security.

Security and Distributed Cloud Services Release Notes

July 2023

Welcome to the product release notes for F5® Distributed Cloud Services. Each month, the product team will provide additional details on key features and enhancements in every release.

Bot & Risk Management

Mobile App Shield

New Mobile App Security Product Now Live

Customers can now purchase F5 Distributed Cloud Mobile App Shield (XC Mobile App Shield) to lower mobile app security risks that result in compliance violations, financial loss, data leakage, fraud, customer churn, and reputational harm. This mobile app security solution safeguards mobile apps and prevents tampering (RASP), data exfiltration, and API abuse with proactive protection from malware, bots, unauthorized access, and man-in-the-middle attacks.

Distributed Cloud Mobile App Security blends bot defense with app shielding to protect your mobile apps at runtime and at rest, ensuring your mobile apps are tamper-resistant and constantly monitored so you can meet mobile compliance requirements for payments (e.g., EMVCo SBMP, PSD2, and PCI), privacy (GDPR and CCPA), and healthcare (HIPAA). Deploy and scale bot defense with mobile app shielding via a single, low-code, SDK integration that accelerates time-to-value and reduces engineering effort. Contact your account manager to learn more.

Web Application and API Protection

WAAP

Export Security Events and Incidents from the Console to CSV Format

Users can now export security events and incidents (up to 500 logs at a time) from the Distributed Cloud Console in a CSV file, which enables flexibility in how users want to consume this data, based on their desired incident and event management response workflow(s). On top of the [Global Log Receiver](#) functionality to stream logs to various third-party log collection tools, this capability provides another option for users to manage their logs, for analysis and investigations.

Updated WAAP Dashboard: Announcing Trends for Security Dashboards

The WAAP Security dashboards for both namespaces and individual load balancer views now supports trends for metrics such as security events, threat campaigns, IP reputation, etc. This will enable users to view the change in metrics (up or down) for the selected date time range compared with the previous period, along with the sentiment (positive, negative or neutral), allowing users to more clearly understand how their security posture is evolving over time.

Enhanced Filter Options for Web App and API Protection (WAAP) Security Analytics

Two new operators (present and not present) are now supported for filters on the Security Events and Incidents pages. This update enables users to more easily search and filter through security events and incidents to narrow views to identify specific violation, event types, and/or application attributes. This more granular filtering can speed up investigation time, narrow down potential issues, and improve users' ability to respond quickly.

Application and Network Performance

DNS

Migration of the Delegated Domain into Primary DNS Management

With this release, we are merging the Delegated Domain feature into the Primary DNS section of F5 Distributed Cloud Services. This allows for easier management, as it is now possible to have DNS records for an HTTP Load-Balancer automatically created, while letting customers manage the content of this DNS zone. Records automatically created appear in a new RRSets group called "x-ves-io-managed" that is in read-only mode.

DNS Load Balancer

Display Details about Why a DNS Load Balancer Health Check Failed

This release adds more information in the DNS Load Balancer dashboard about the reason a health check failed -- for example, a connection refused, or received a string not matching the configured string. With this update, users are provided more insights for troubleshooting.

The screenshot shows the 'DNS Load Balancers' overview page for 'lb1pool'. The 'Health' section displays 'Degraded' in yellow. Below it, the 'Pools Overview' shows 0 Healthy, 0 Unhealthy, 1 Degraded, and 0 Disabled, with a total of 1. A table below lists the pool 'lbp1' with an ICMP health monitor, a degraded status, 1 healthy member, 1 unhealthy member, 0 degraded members, and 0 disabled members.

Name	Health Monitor	Status	Healthy Members	Unhealthy Memb...	Degraded Me...	Disabled Members
lbp1	ICMP	Degraded	1	1	0	0

Figure 1: Here is how a DNS Load Balancer Health Check failure is displayed in the product overview dashboard.

The screenshot shows the 'Members' page for 'lb1pool', displaying 2 items. A table lists the members with their IP endpoints, health monitors, member status, and reasons for failure.

IP Endpoint	Health Monitor	Member Status	Reason
[Redacted]	ICMP	Unhealthy	ICMP ping failure for health check from at l...
[Redacted]	ICMP	Healthy	—

Figure 2: Here is how a DNS Load Balancer Health Check failure is displayed in the "Members" dashboard.

Automatic Certificate Generation for Load Balancers Advertised on Customer Edge Sites

The F5 Distributed Cloud Platform can now auto-generate certificates for Load Balancers that are advertised on Customer Edge (CE) sites. This includes support for Load Balancers advertised on private networks such as SLO/SLI as well as Load Balancers advertised to the Internet directly from the CE site. Note: In this phase, support for DNS domain delegation is not available. This will be added soon.

Global Log Receiver

Added One New Target for Global Log Receiver

This release adds support for IBM QRadar as target for the Global Log Receiver feature. This allows customers using those vendors to send their logs more easily, rather than having to use the generic HTTPS endpoint.

Multi-Cloud Networking

Network Connect

Uptime Improvement for Services Hosted on CEs During a Software Update

F5 Distributed Cloud Services has made several improvements to our CE software update process to improve the uptime of services hosted on CEs during upgrade. With this release, we have reduced the downtime for services hosted on CEs by about three times during a CE upgrade.

App Connect

Rich Dashboards for Multi-Cloud App Connect

The Multi-Cloud App Connect service is refreshed with rich dashboards focused on application delivery. Application and network operators can now observe and take action on applications delivered across their multi-cloud network fabric with an app health and performance dashboard.

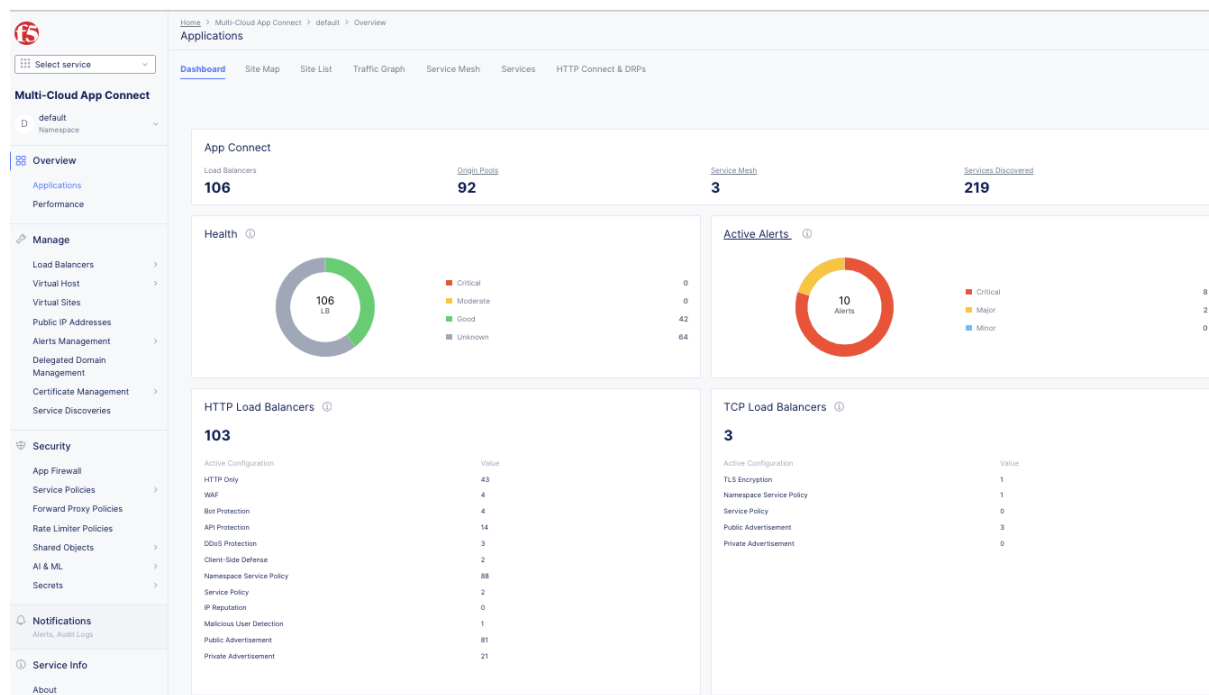


Figure 3: Multi-Cloud App Connect now provides dashboards focused on application delivery, such as the example above that offers metrics on application health and performance.

Please see the full [F5 Distributed Cloud Changelog](#) for additional information, including more new enhancements plus known issues and caveats. We hope you find the information contained in these release notes useful. If you have any feedback, please email: CS_DistributedCloudTeam@f5.com