F5 Distributed Cloud Services Release Notes

06.26.26

JULY 2026 RELEASE

The product release notes for F5® Distributed Cloud Services provide monthly updates on new features and enhancements included in each release. This month's release was completed on July 12th, 2026. Please reference the Changelog documentation for more information.

APPLICATION SECURITY

API Security

API1 - BOLA and enumeration findings are now more precise, with broader user identification and method-level context in every incident
This release improves BOLA and enumeration detection with expanded user identification for JWT tokens and method-aware incident analysis. Identity resolution now covers additional and custom token locations in requests, aligning user identification with authentication discovery. Detection logic also accounts for the specific HTTP methods involved, so findings better reflect how a resource is being accessed. This provides clearer, more accurate incident context for investigating authorization issues.

API3 Broken Object Property Level Authorization (BOPLA) detection now covers property-access patterns out of the box and validates both requests and responses
This release expands BOPLA detection to cover a wider range of property-access patterns with less reliance on restrictive schema configuration. The service now validates both requests and responses to identify more cases where users may attempt to access or manipulate object properties beyond intended permissions. This improves coverage and helps security teams detect authorization issues more effectively.

API4 Incident Detection for Excessive API Resource Usage
This release adds detection for suspicious API activity that may indicate excessive or abusive resource usage. The capability identifies endpoints where unusual request patterns, resource-heavy activity, or abnormal runtime behavior may create risk for backend services or application availability. Detected incidents provide response context in Security Analytics to help security teams determine whether stronger limits, validation, or protection policies are needed.

API6 Detection of Sensitive Business-Flow Abuse
This release introduces detection for automated abuse targeting sensitive business flows such as checkout, account creation, ticket purchasing, and fund transfers. The service can now classify API endpoints involved in these flows and monitor them for patterns that indicate misuse. When abusive activity is observed, an API6 incident is generated with context. This provides better visibility into business-critical endpoints and helps detect abuse before it causes business impact.

API10 Discovery and Drift Detection for External Redirects and Callback URLs
This release adds discovery for external API dependencies and drift detection for callback and redirect domains. By analyzing headers, fields, and specification constructs, the service identifies APIs that rely on external services, maps their destinations, and flags them per API. It also continuously monitors those dependencies and alerts security teams when an API starts using a new external callback or redirect domain. This improves API governance and helps reduce risk from third-party integrations.

Per-Domain Schema and Definition Export
API schemas, endpoints, and sensitive data discovery can now be scoped under each unique FQDN, and API definitions can be downloaded per domain, with exports that exclude endpoints belonging to other domains. This makes it easier to focus analysis on a specific environment and manage API definitions by application, environment, or team.

API Metrics & Widgets for BIG-IP Integration
In hybrid deployments where Distributed Cloud Services ingests logs from BIG-IP for API discovery, the service already provides table and graphical views of the learned API inventory. This release expands that view with key API metrics widgets at the top, bringing visibility for BIG-IP-discovered APIs closer to the SaaS-only HTTP load balancer experience. Within the API Endpoints tab, the complete set of metrics for BIG-IP-sourced traffic is now available, including sensitive data summary, API call distribution, and most-active APIs.

Web App Scanning

New Attack Surface Reconnaissance (Recon) WAF Detection Feature
The platform now automatically fingerprints WAFs protecting discovered web services, providing critical visibility into WAF coverage across your external attack surface. With a recon scan, the platform identifies and maps WAF products and vendors (e.g., F5 BIG-IP, Cloudflare, AWS WAF, Akamai etc.), displaying protection status. This enables your teams to quickly identify unprotected assets, audit WAF coverage across the attack surface, and validate the effectiveness of deployed WAFs. By understanding protection gaps, tracking WAF deployments, and identifying misconfigurations or vendor inconsistencies, you can ensure web applications remain secure and resilient against potential threats.

CVE-to-WAF Attack Signature Mapping
Web App Scanning now automatically maps CVEs to F5 WAF attack signatures. This enhancement helps bridge the gap between vulnerability detection and protection by surfacing WAF attack signature details for CVE-based findings directly within the user interface. When the scanner detects a vulnerability tied to a known CVE, it automatically identifies corresponding F5 Distributed Cloud WAF attack signatures, providing you actionable protection guidance. This includes Signature ID, attack type, risk level, accuracy, and detailed remediation steps—all without requiring manual cross-referencing or leaving the scanning interface. This helps accelerate time to protection, enabling vulnerabilities to be mitigated with WAF signatures as stopgap measures while permanent fixes are implemented.

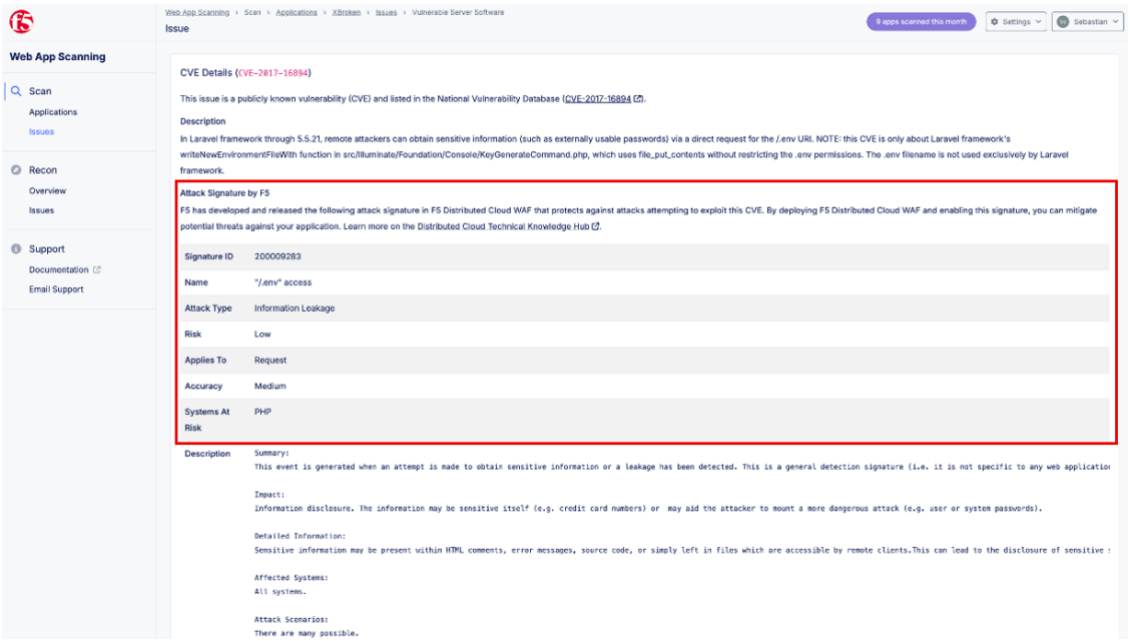

Figure 1: Signature mapping in Web App Scanning to CVE

Web Application Firewall

AI-enabled WAF numerical risk scoring

This release introduces AI-enabled numerical risk scoring for WAF security events. Risk scores help quantify relative severity, making it easier for security teams to prioritize investigations and focus on the most impactful threats.

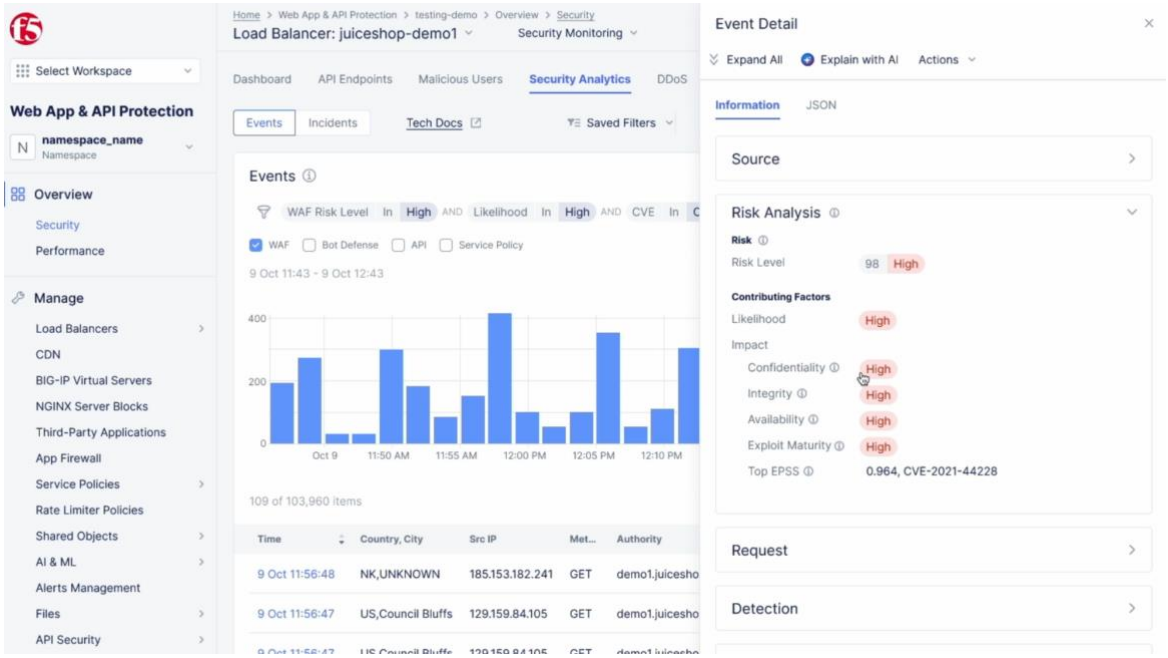

Figure 2: Numerical scoring added for risk analysis

APPLICATION DELIVERY

CDN

One-click CDN Enablement
We are excited to introduce one-click CDN enablement, a powerful solution designed to instantly accelerate application delivery and optimize performance without architectural overhauls. With simple one-click enablement for existing load balancers, customers can seamlessly serve traffic from the edge to achieve 50–80% faster user experiences and improve SEO rankings. Furthermore, adopting this CDN directly reduces origin compute and cloud egress costs while automatically enforcing your existing security policies without any coverage gaps.

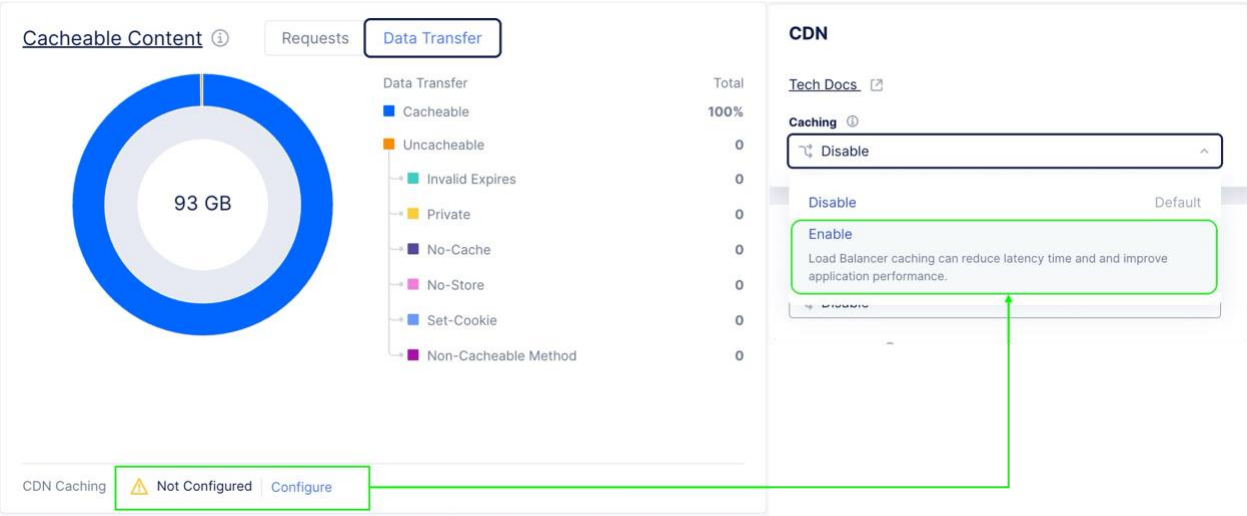

Figure 3: One-click enablement from the cacheability widget to enable CDN

Customer Edge (CE) Nodes

Single Domain Registration for Customer Edge Nodes
This release simplifies CE registration by requiring allowlisting only for the F5-owned wildcard domain when URL categorization is not enabled. This reduces firewall configuration complexity for common CE deployments while preserving flexibility for environments that require URL categorization.

IP reputation processing is now handled locally by Envoy, which performs IP database lookups and passes results to Opera, eliminating the need for external Webroot communication. URL categorization remains disabled by default and can be enabled in CE settings for Secure Mesh Site v2. When URL categorization is enabled, additional domains must be allowlisted as documented in the CE egress domain rules.

Reduced Downtime During CE Upgrades to Under 20 Seconds
This release reduces the downtime experienced by CE sites during an upgrade to under 20 seconds, down from multiple minutes. Shorter upgrades reduce traffic interruption during maintenance windows and help improve operational continuity.

CE Enterprise Readiness
This release reflects continued improvements to CE deployment speed, stability, and operations. Over the past 18 months, F5 Distributed Cloud Services has delivered measurable gains across deployment success, deployment time, traffic continuity, and upgrade reliability, including:

- 9x improvement in deployment success rate
- Sub-30 minute deployment time with a single IP to register
- 98% reduction in traffic downtime
- 99.9% upgrade success rate

Combined with proactive monitoring and real-time health visibility, these improvements make CE deployments more stable, faster to deploy, and easier to operate at enterprise scale.

DNS & DNSLB

XC DNS

Initiate Secondary Secure Transfer from the Distributed Cloud Console

Some primary DNS servers generate a NOTIFY messages for every record change. During periods of frequent updates, or when using a “chatty” primary, NOTIFY messages can be rate-limited, which may cause some notifications to be delayed or missed.

With this release, DNS now lets administrators manually trigger an AXFR zone transfer from the console after they complete changes on their primary DNS server. For example, if an administrator makes 10 edits on the primary, they can make those changes first and then initiate a single zone transfer from the console to synchronize the secondary.

This capability helps teams consolidate change activity, reduce reliance on individual NOTIFY messages, and keep their DNS records (as a secondary) in sync more efficiently.

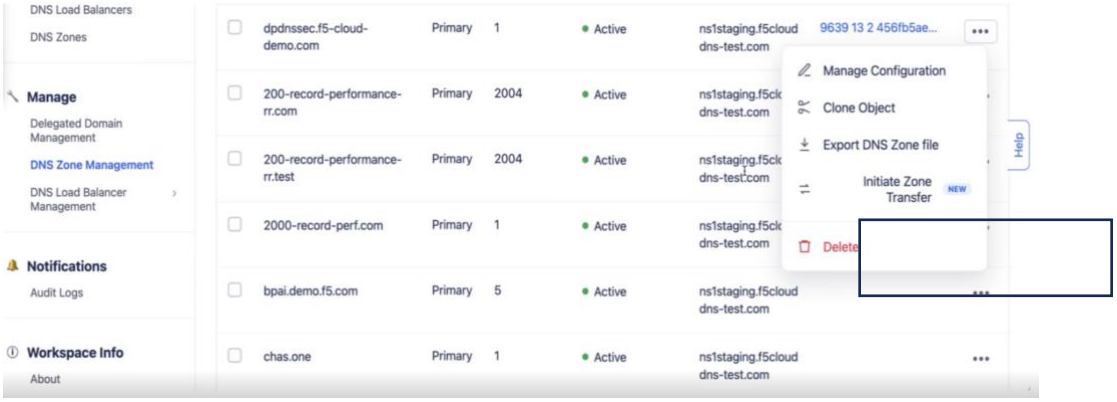

Figure 4: “Initiate Zone Transfer” action, allowing for single zone transfers

FQDN-Based Health Checks for CNAME Pool Members (with SNI / Host Header Support)

DNSLB health checks have been enhanced to support CNAME pools. This enables a more precise way to validate application health to improve global availability and extends DNSLB use cases for applications hosted behind CDN/SaaS provider CNAMEs. DNSLB health checks can now include SNI and/or host header information for your application. This makes health checks validate the actual application behind a hostname, so DNSLB traffic steering is based on true end-user reachability. This reduces false health results and improves the reliability of global failover and availability for CDN/SaaS and virtual-hosted environments.

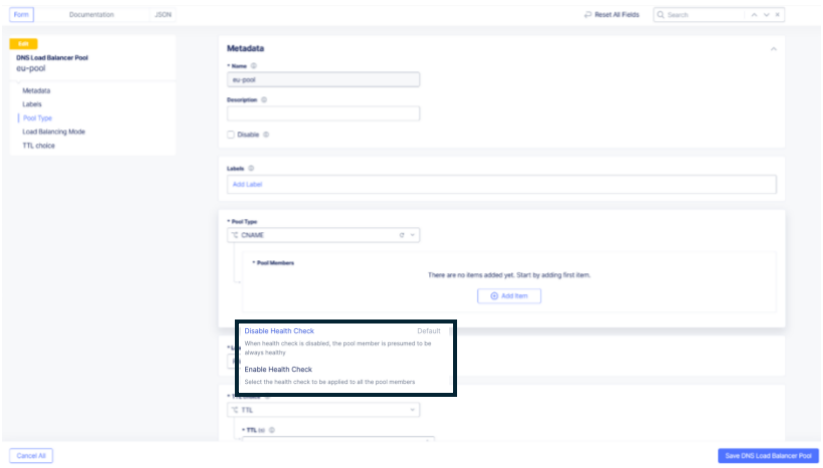

Figure 5: DNS Load Balancer Pool Dashboard with addition of CNAME health check

GENERAL UPDATES

Persistent Storage Region is now visible in the UI
This release adds region visibility for Persistent Storage resources in the user interface. Displaying the associated region improves storage placement visibility and makes it easier to verify regional configuration at a glance.

Real-Time Incident Procedures
This release adds support for managing Real-Time Incident Procedures (RTIP) directly in tenant administration. Users with tenant owner privileges can add, view, and edit RTIP content in the console, with changes saved immediately upon selecting **Save**. Support access remains read-only. RTIP is available under **Administration > Tenant Settings > Incident Procedures**, helping teams maintain incident response guidance in a centralized location.

***

Please see the full **Release Changelog** for additional information, including more new enhancements plus known issues and caveats. The information in these release notes is intended to help readers stay current on the latest updates. Feedback may be sent to **CS_DistributedCloudTeam@f5.com**.