BIG-IP DNS

WHAT'S INSIDE

Hyperscale and Protect Your DNS While Optimizing Global App Delivery

Scaling and securing every environment helps protect your business from site outages and improves DNS and application performance. Securing DNS infrastructures from the latest distributed denial-of-service (DDoS) attacks and protecting DNS query responses from cache-poisoning redirects will help keep your business online and viable. To fully achieve these goals, you need efficient ways to monitor DNS infrastructure and application health, and to scale on-demand.

F5® BIG-IP® DNS distributes DNS and user application requests based on business policies, data center and cloud service conditions, user location, and application performance. The BIG-IP platform delivers F5's high-performance DNS services with visibility, reporting, and analysis; hyperscales and secures DNS responses geographically to survive DDoS attacks; delivers a real-time DNSSEC solution; and ensures high availability of global applications in all cloud environments.

KEY BENEFITS

Hyperscale DNS up to 100 million RPS with a fully loaded chassis
BIG-IP DNS hyperscales authoritative DNS up to 100 million query responses per second (RPS) and controls DNS traffic. It ensures that users are connected to the best site and delivers on-demand scaling for DNS and global apps.

Protect against DNS attacks and ensure availability
Ensure DNS and application availability and protection during DNS DDoS attacks or volume spikes. Mitigate DNS threats by blocking access to malicious IP domains.

Improve global application performance
Send app users to the cloud or on-premises site with the best performance based on application, geolocation, business, and network conditions.

Deploy flexibly, scale as you grow, and manage efficiently
BIG-IP DNS delivers flexible global application management in virtual and multi-cloud environments. The web-based UI provides easy DNS configuration with centralized menus; advanced logging, statistics, and reporting along with export to 3rd party analytics.

ICSA labs CERTIFIED FIREWALL - CORPORATE

UNMATCHED DNS PERFORMANCE

BIG-IP DNS delivers hyperscale performance that can handle even the busiest apps and websites. When apps have a volume spike in DNS queries due to legitimate requests or DDoS attacks, BIG-IP DNS manages requests with multicore processing and F5 DNS Express™, dramatically increasing authoritative DNS performance up to 50 million RPS to quickly respond to all queries.

This scalability helps your organization provide the best quality of service (QoS) for your users while eliminating poor application performance. DNS Express improves standard DNS server functions by offloading DNS responses as an authoritative DNS server. BIG-IP DNS accepts zone transfers of DNS records from the primary DNS server and answers DNS queries authoritatively.

Benefits and features of multicore processing and DNS Express include:

- High-speed response and DDoS attack protection with in-memory DNS
- Authoritative DNS replication in multiple BIG-IP or DNS service deployments for faster responses
- Authoritative DNS and DNSSEC in multi-clouds for disaster recovery and fast, secure responses
- Scalable DNS performance for quality of app and service experience
- The ability to consolidate DNS servers and increase ROI

In cases of very high volumes for apps and services or a DNS DDoS attack, BIG-IP DNS with DNS Express enabled plus in Rapid Response Mode (RRM) hyperscales up to 100 million RPS. It extends availability with unmatched performance and security—absorbing and responding to queries up to 200 percent of the normal limits. See page 17 for performance metrics and details.

DNS CACHING AND RESOLVING

DNS latency can be reduced by enabling a DNS cache on BIG-IP DNS and having it respond immediately to client requests. BIG-IP DNS can consolidate the cache and increase the cache hit rate. This reduces DNS latency up to 80 percent, with F5 DNS Caching reducing the number of DNS queries for the same site. When used in hardware on the F5 VIPRION® platform, DNS caching hyperscales for ultimate query response performance and delivers linear scalability across multi-bladed chassis. In addition to caching, BIG-IP DNS allows the device to do its own DNS resolving without requiring the use of an upstream DNS resolver.

Caching profiles available to select for multiple caches include:

- Transparent cache
- BIG-IP DNS site between client and DNS internal/external
- Hot cache
- Caching resolver
- No cache response - BIG-IP DNS sends out requests with responses returned for resolving and caching
- Validating caching resolver

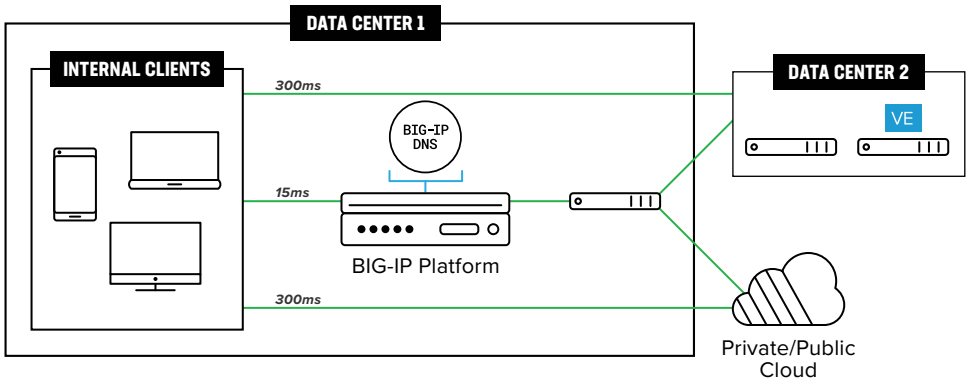


Figure 1: BIG-IP DNS supports all common DNS deployments that are either authoritative or locally resolved DNS. Specific zone requests not cached are forwarded to name servers for faster DNS resolving, allowing users to receive expedient responses.

BIG-IP DNS reduces the average DNS response time and latency for mobile and desktop devices from an average of 300 milliseconds (ms) and 100 ms respectively to as little as 15 ms, depending on workloads.

SECURE APPLICATIONS

DNS denial-of-service attacks, cache poisoning, and DNS hijacking threaten the availability and security of your applications. BIG-IP DNS protects against DNS attacks and enables you to create polices that provide an added layer of protection for your applications and data.

DNS attack protection features include:

- Hardened device—BIG-IP DNS is ICSA Labs Certified as a network firewall, and resists common teardrop, ICMP, and daemon attacks.
- DNS attack protection—BIG-IP DNS offers built-in protocol validation in software to automatically drop high-volume UDP, DNS query, NXDOMAIN floods, and malformed packets. You can use BIG-IP DNS in hardware to mitigate these high-volume attacks.

- DNS load balancing—The BIG-IP platform can be used to front-end static DNS servers. If the DNS request is for a name controlled by the BIG-IP platform, F5 DNS services will answer the request.
- Security control—F5 iRules® for DNS can help you create policies that block requests from rogue sites.
- Packet filtering—BIG-IP DNS uses packet filtering to limit or deny websites' access based on source, destination, or port.

DNS firewall

DNS DDoS, cache poisoning of LDNS, and other unwanted DNS attacks and volume spikes can cause DNS outage and lost productivity. These attacks and traffic spikes increase volume dramatically and can take down DNS servers.

BIG-IP DNS, with security, scale, performance, and control functionality, provides DNS firewall benefits. It shields DNS from attacks such as reflection or amplification DDoS attacks and other undesired DNS queries and responses that reduce DNS performance.

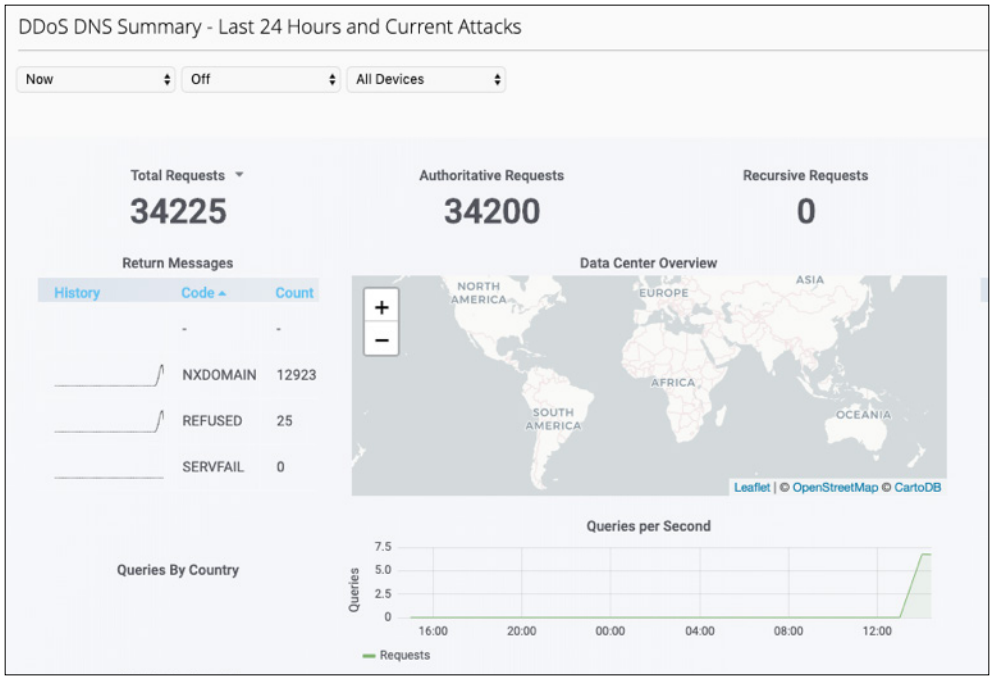


Figure 2: Visualize DNS DDoS attacks, the top 25 attack URLs, Queries Per Second (QPS) and by country as available, and other DNS traffic such as Reponses Per Second (RPS) by record types for a full picture of your DNS performance and unwanted attacks.

In addition, you can mitigate complex DNS security threats by blocking access to malicious IP domains with Response Policy Zones. With BIG-IP DNS, you can install a third-party domain filtering service such as SURBL or Spamhaus and prevent client infection or intercept infected responses to known sources of malware and viruses. F5 DNS firewall services reduce the costs of infection resolution and increase user productivity.

F5 DNS SERVICES INCLUDE:

- Protocol inspection and validation
- DNS record type ACL*
- High-performance authoritative DNS, which scales responses exponentially
- Authoritative DNS hyperscaling up to 200% to absorb DDoS attacks
- Reducing latency and hyperscaling DNS caching
- DNS load balancing
- Stateful inspection (never accepts unsolicited responses)
- ICSA Labs certification (can be deployed in the DMZ)
- The ability to scale across devices using IP Anycast
- Secure responses (DNSSEC)
- DNSSEC response rate limits
- DNS over HTTPS support resolves queries and mitigates attacks
- Complete DNS control using DNS iRules
- DDoS threshold alerting*
- Threat mitigation by blocking access to malicious IP domains
- DNS logging and reporting
- Hardened F5 DNS code (not BIND protocol)

*Requires provisioning BIG-IP® Advanced Firewall Manager™ to access functionality.

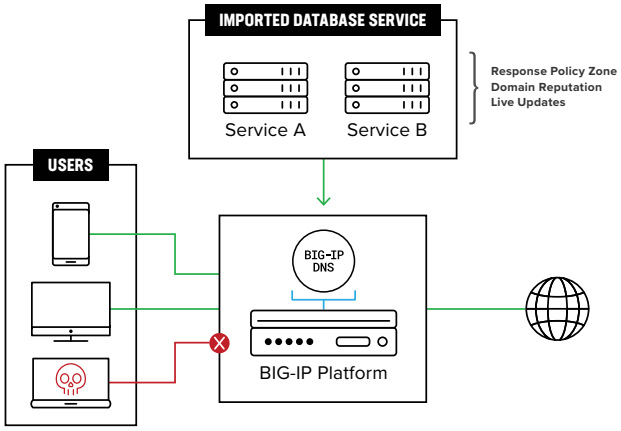


Figure 3: Lower your risk of malware and virus communication and mitigate DNS threats by blocking access to malicious IP domains with a domain reputation service such as SURBL or Spamhaus.

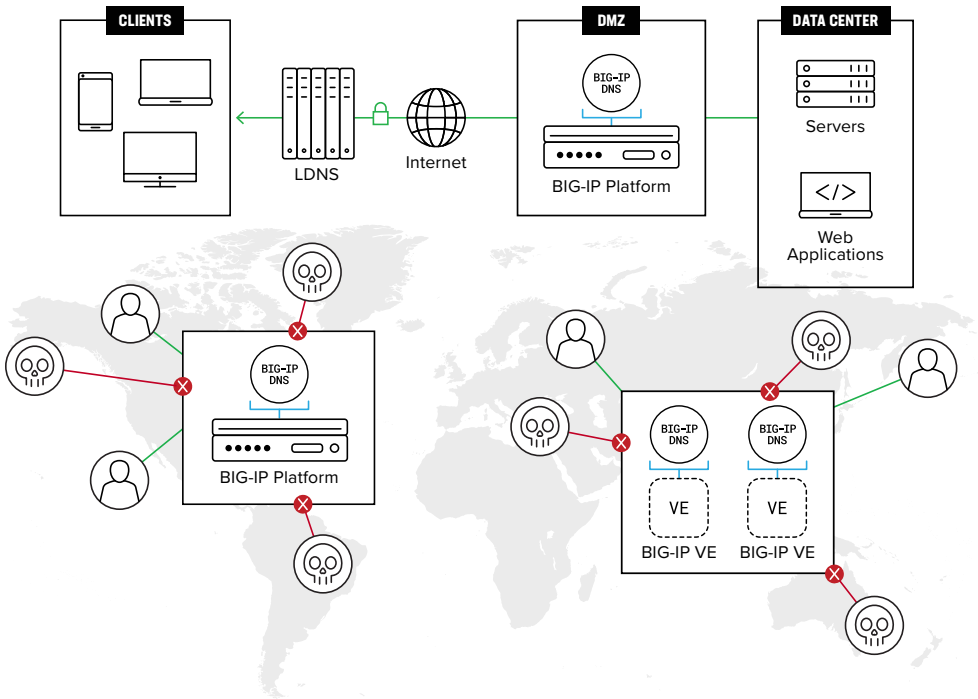


Figure 4: BIG-IP DNS keeps apps available with firewall services protecting DNS infrastructure from high-volume attacks and malformed packets.

Complete DNSSEC signing

With BIG-IP DNSSEC support, you can digitally sign and encrypt your DNS query responses. This enables the resolver to determine the authenticity of the response, preventing DNS hijacking and cache poisoning. In addition, receive all the benefits of global server load balancing while also securing your DNS query responses. Alternatively, if a zone has already been signed, BIG-IP DNS manages static DNSSEC responses for higher performance.

Centralized DNSSEC key management

Many IT organizations have or want to standardize on FIPS-compliant devices and secure DNSSEC keys. You can use BIG-IP DNS with FIPS cards that provide 140-2 support for securing your keys. In addition, BIG-IP DNS integrates and uses hardware security modules (HSMs) from Thales for implementation, centralized management, and secure handling of DNSSEC keys, reducing OpEx and delivering consolidation and FIPS compliance.

Top-level domain support for DNSSEC

For DNS administrators who want to delegate to other secure sub-domains, BIG-IP DNS allows easy management of DNSSEC as a top-level domain, becoming a parent zone.

DNSSEC validation

In most networks, DNS resolvers offload DNSSEC record requests and crypto calculations to validate that the DNS response being received is correctly signed. DNSSEC responses coming into the network require high CPU loads on DNS resolving servers.

DNS over HTTPS

DNS over HTTPS (DOH) is encrypted DNS using SSL for full protection. It is fully enabled by popular web browsers and can create delays and security issues for service providers and enterprises who are not able to terminate and respond to these DNS inquires. F5 BIG-IP DNS allows your network to unencrypt and resolve DNS queries over HTTPS without impacting responses-per-second (RPS). In addition, DoH support removes HTTPS as a DNS Spoofing vector for malicious amplification attacks and protects the last mile with DNS message encapsulation.

DNS over TLS

DNS over TLS (DoT) ensures that DNS requests and responses are not tampered with or forged via on-path attacks. DoT adds TLS encryption on top of the transmission control protocol (TCP), which is used for DNS queries. DoT is a protocol that authenticates communication between a DNS client and a DNS server. It uses cryptographic signatures for secured transmission. DNS over TLS or DoT, is a standard for encrypting DNS queries to keep them secure and private. DoT uses the same security protocol, TLS to encrypt and authenticate communications.

ECDSA keys

BIG-IP DNS provides support for Elliptic Curve Digital Signature Algorithm (ECDSA) keys for DNSSEC. In addition to complying with modern security requirements of a wide range of industries, ECDSA provides the same level of cryptographic strength as the RSA keys BIG-IP currently supports, but with much smaller keys. This provides a significant increase in security strength when using similar key sizes and allows for faster signing and verification.

DEPLOY F5 DISTRIBUTED CLOUD BOT DEFENSE DIRECTLY FROM YOUR BIG-IP

Bots cause significant financial pain through scraping that slows performance, scalping and inventory hoarding that frustrate loyal customers, enumerating gift card codes to steal balances, creating fake accounts to commit fraud, and credential stuffing—the testing of stolen credentials—that leads to account takeovers.

Today's advanced persistent bots are more sophisticated than ever. To stay ahead of attackers, F5 Distributed Cloud Bot Defense uses rich client-side signal collection, industry-leading code obfuscation, aggregate telemetry collection, and AI for unparalleled long-term efficacy and near-zero false positives while maintaining access for good bots. And because F5 defends the most targeted sites on the web—including those of the world's largest banks, retailers, and airlines—F5 is ready when these attacks target your organization.

Deploy Distributed Cloud Bot Defense directly from BIG-IP or through a connector that's right for your application, with support services tailored to your needs, from self-service to managed service.

Advanced global load balancing

BIG-IP DNS includes the industry's most advanced traffic distribution capabilities to match the needs of any organization or globally deployed application.

- Round robin
- Global availability
- LDNS persistence
- Application availability
- Geography
- Virtual server capacity
- Least connections
- Packets per second
- Round trip time
- Hops
- Packet completion rate
- User-defined QoS
- Dynamic ratio
- LDNS
- Ratio
- Kilobytes per second

With BIG-IP DNSSEC validation, administrators can easily offload and validate DNSSEC on the client side using BIG-IP DNS for resolving. This results in superior DNS performance and a dramatic increase in the site response to users.

GLOBALLY AVAILABLE APPLICATIONS

BIG-IP DNS offers global application availability and sophisticated health monitoring that support a wide variety of application types, giving organizations the flexibility to adapt quickly and stay competitive.

These global availability and health monitoring features include:

- Global load balancing—BIG-IP DNS provides comprehensive, high-performance application management for hybrid environments.
- Dynamic ratio load balancing—BIG-IP DNS routes users to the best resource based on site and network metrics (for example, based on the number of hops between the client and the local DNS).
- Wide area persistence—To ensure user connections persist across apps and data centers, BIG-IP DNS synchronizes data, propagates local DNS, and maintains session integrity.
- Geographic load balancing—BIG-IP DNS includes an IP database identifying location at the continent, country, and state/province level to connect users to the closest app or service for the best performance.
- Custom topology mapping—With BIG-IP DNS, organizations can set up custom topology maps. By defining and saving custom region groupings, you can configure topology based on intranet app traffic policies that match your internal infrastructure.
- Infrastructure monitoring—BIG-IP DNS checks entire infrastructure health, eliminating single points of failure and routing app traffic away from poorly performing sites.

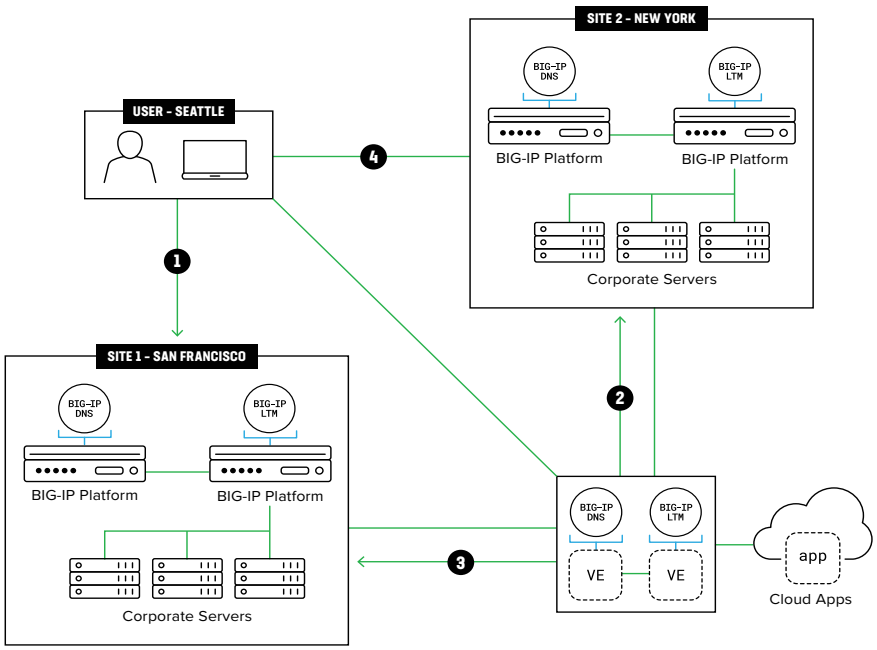


Figure 5: BIG-IP DNS ensures users are always connected to the best site. 1 User queries local DNS to resolve domain, and local DNS queries BIG-IP DNS. 2 BIG-IP DNS uses metrics collected for each site and identifies the best server. 3 BIG-IP DNS responds to local DNS with IP address. 4 User is connected to best site on premises or in multi-cloud.

Application health monitoring

BIG-IP DNS improves the application experience by intelligently monitoring the availability of resources. It expands application resilience by flexibly selecting and using the best available BIG-IP solutions for health monitoring. BIG-IP DNS reduces application downtime and enables easy availability with multiple settings in application monitoring.

Today's sophisticated applications require intelligent health checks to determine availability. Instead of relying on a single health check, BIG-IP DNS aggregates multiple monitors so that you can check the application state at multiple levels. This results in the highest availability, improves reliability, and eliminates false positives to reduce management overhead.

BIG-IP DNS provides pre-defined, out-of-the-box health monitoring support for more than 18 different applications, including SAP, Oracle, LDAP, and mySQL. BIG-IP DNS performs targeted monitoring of these applications to accurately determine their health, reduce downtime, and improve the user experience.

Disaster recovery/business continuity planning

In addition to performing comprehensive site availability checks, you can define the conditions for shifting all traffic to a backup data center, failing over an entire site, or controlling only the affected applications.

SIMPLE MANAGEMENT

Managing a distributed, multiple-site network from a single point is an enormous challenge. BIG-IP DNS provides tools that give you a global view of your infrastructure with the means to manage the network and add polices to ensure the highest availability for your business-critical applications. Manage global infrastructure from a centralized UI with features including:

- Web-based user interface.
- Streamlined and centralized DNS and GSLB menus for fast configuration.
- Efficient list and object management for complete visibility of global resources.
- Unique naming of objects to reduce administration and build business policies.
- Enhanced management of distributed applications as part of one collective group.
- Context-sensitive help for information on objects, commands, and configuration examples.

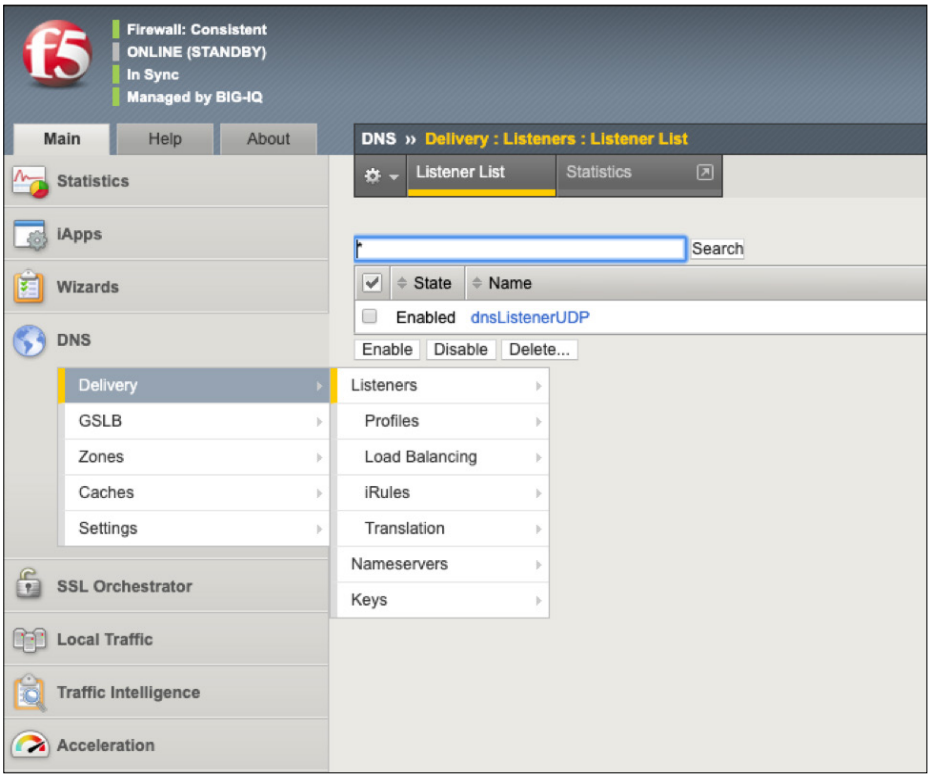


Figure 6: Reduce DNS delivery deployment time with centralized and easy-to-find configuration and management sequences.

- **Powerful command-line interface**—The TMSH command-line interface delivers integrated search, context-sensitive help, and batch-mode transactions.
- **Automated setup and synchronization**—Autosync automates and secures multiple BIG-IP DNS devices, eliminating difficult hierarchical management common to DNS.
- **Improves scale and analysis with unlimited N+1 devices**—In a failover situation, when BIG-IP DNS services are part of a Device Service Cluster (DSC) group, the BIG-IP solution performs at its peak capacity—across all appliances or virtual editions synced with DNS and GSLB services. BIG-IP DNS provides highly scalable apps and services, performing smart analysis on all incoming traffic to better understand patterns and anomalies.
- **Scalable and optimized GSLB configurations**—Incremental Sync delivers high performance for large deployments. With more devices synced, configuration changes transpire rapidly. For large deployments with GSLB configurations and rapid user changes, you can protect changes by manually saving when most convenient.
- **Configuration retrieval**—AutoDiscovery enables retrieved configurations from distributed BIG-IP instances, removing repeat configurations across devices.
- **Data center and sync groups**—Create logical groups of network equipment to ensure efficient use of monitoring and metrics collection for intelligently sharing with members in the logical group.

- **Distributed application management**—You can define dependencies between application services and manage them as a group, building scalable traffic distribution policies and improving efficiency with granular control of objects.
- **iRules**—Use the F5 iRules scripting language to customize the distribution of global traffic. BIG-IP DNS looks deep inside DNS traffic to customize app traffic to the desired data center, pool, or virtual server. This reduces latency, increases attack protection, and improves performance.
- **Customize traffic with QoS**—Design traffic decisions and easily develop custom load balancing algorithms using quality of service metrics in iRules, such as round-trip time, hops, hit ratio, packet rate, topology, and more.
- **DNS iRules**—Manage DNS queries, responses, and actions for a fast, customized DNS infrastructure. For instance, configure DNS iRules with filtering for protection and reporting.
- **F5 ZoneRunner**™—ZoneRunner is an integrated DNS zone file management tool that simplifies and reduces the risk of misconfiguration. Built on the latest version of BIND, ZoneRunner provides:
    - Auto population of commonly used protocols.
    - Validation/error checking for zone file entries.
    - Zone importation from an external server or a file.
    - Automatic reverse lookups.
    - Easy creation, editing, and searching of all records.
    - Easy management of NAPTR records for LTE and 4G requirements.

Load balancing across container environments

When migrating to public cloud and containers, engineers and architects need a robust solution for load balancing between clusters (global load balancing) across multi-cloud deployments. F5 BIG-IP DNS targets applications in container clusters for scale, routing, and security services by enabling Server Name Indication (SNI) support when using HTTPS monitor.

DNS health monitor

The DNS health monitor available in BIG-IP DNS and BIG-IP® Local Traffic Manager™ (LTM) monitors DNS server health and helps configure DNS based on reporting. The DNS health monitor detects whether the servers are operating at peak performance and helps in reconfiguring for optimal responses.

High-speed logging

You can easily manage DNS and global app logging for fast network visibility and planning. High-speed logging of DNS queries and responses, syslog, and global server load balancing decision logs improve information on data to enable fast network recognition with quick, deep search and display.

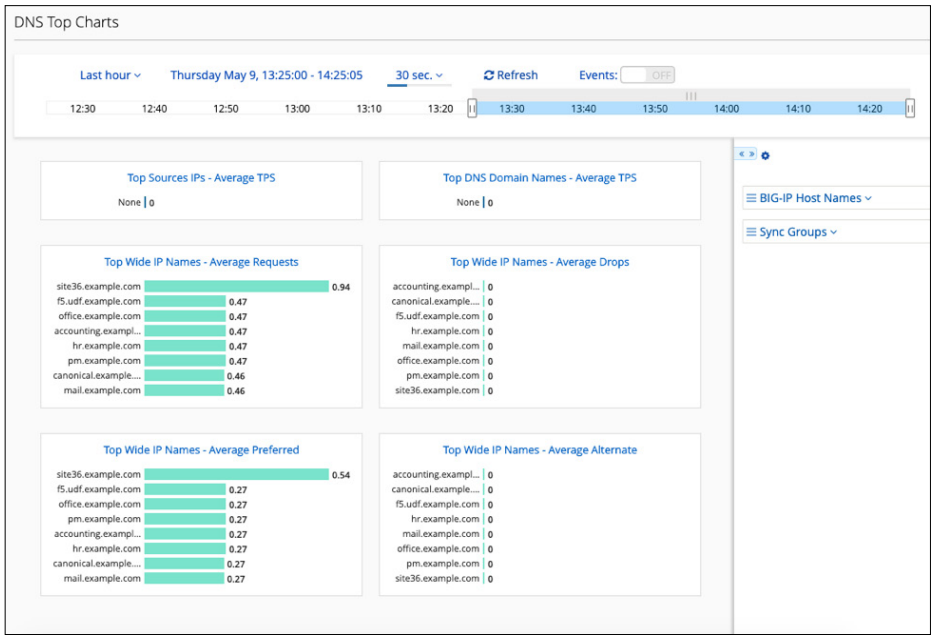


Figure 7: Understand your DNS health from seconds to years comparing the top source IPs, Domain and wide IP names and the TPS for reporting.

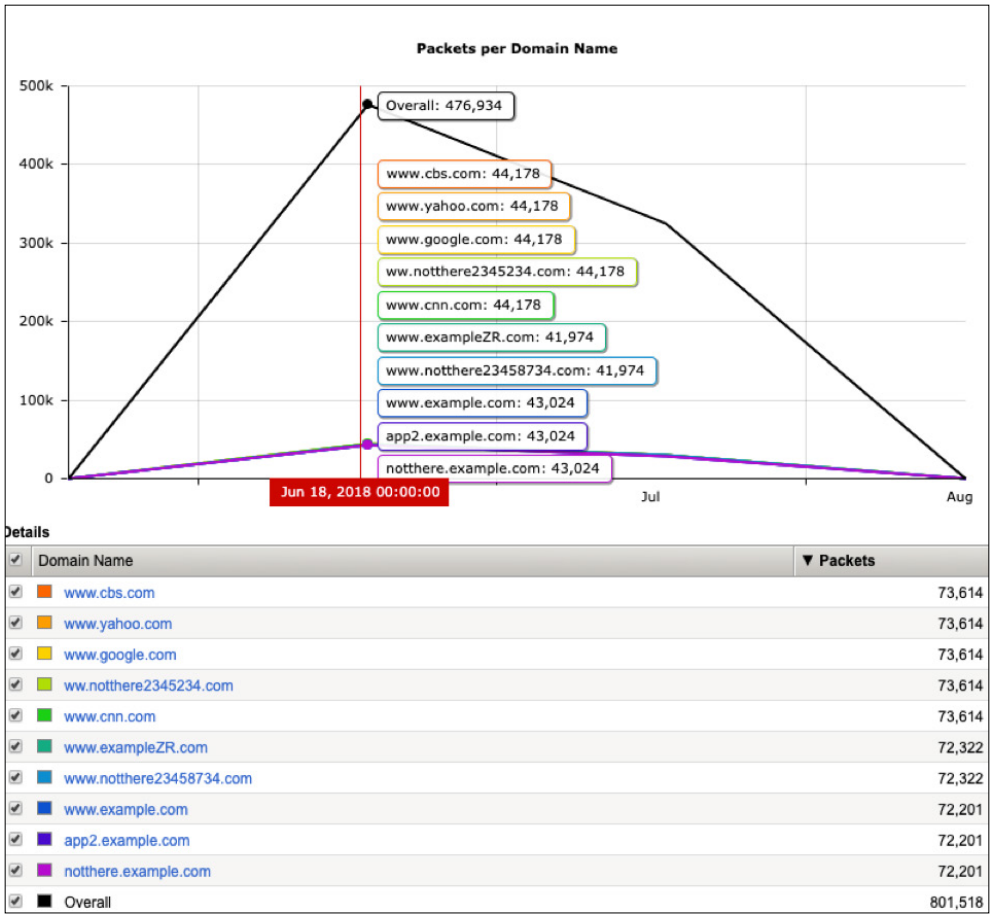
Enhanced DNS detailed statistics

BIG-IP DNS delivers advanced DNS statistics for administrators, with enhanced detailed data for profiles such as query type counts (A, CNAME, NS, RRSIG, AAAA, SRV, and “other” types) with requests, responses, and percentage counts. Stats are per profile and per device global count for fast visibility and capacity planning of DNS delivery infrastructure. DNS detail stats are viewable in DNS profile or in analytics reporting.

Advanced DNS reporting and analytics

F5 Analytics provides advanced DNS reporting and analysis of applications, virtual servers, query names, query types, client IPs, top requested names, and more for business intelligence, capacity planning, ROI reporting, troubleshooting, performance metrics, and tuning, enabling maximum optimization of the DNS and global app infrastructure.

Figure 8: Administrators can easily manage DNS using analytics with advanced reporting and analysis of actions for fast visibility of DNS delivery and infrastructure.



ADVANTAGES OF DNS VISIBILITY

- View and manage configuration and policies on DNS devices.
- Add BIG-IP DNS and BIG-IP LTM devices to existing sync groups.
- Analyze F5 iQuery® connection information to help identify DNS sync-group issues.
- View high-level statistics across your DNS infrastructure showing status of DNS sync groups and devices.
- View both real-time and historical DNS statistics.

BIG-IQ Centralized Management

F5® BIG-IQ® Centralized Management provides a central point of control for F5 physical and virtual devices and for the solutions that run on them. It simplifies management, helps ensure compliance, and gives you the tools you need to deliver your applications securely and effectively. BIG-IQ manages BIG-IP DNS licenses, policies, SSL certificates, images, and configurations.

BIG-IQ offers BIG-IP DNS centralized management including the ability to create, retrieve, update, and delete all global server load balancing (GSLB) objects; tools to deploy and rollback GSLB policies; and the ability to manage DNS listener and profile configurations.

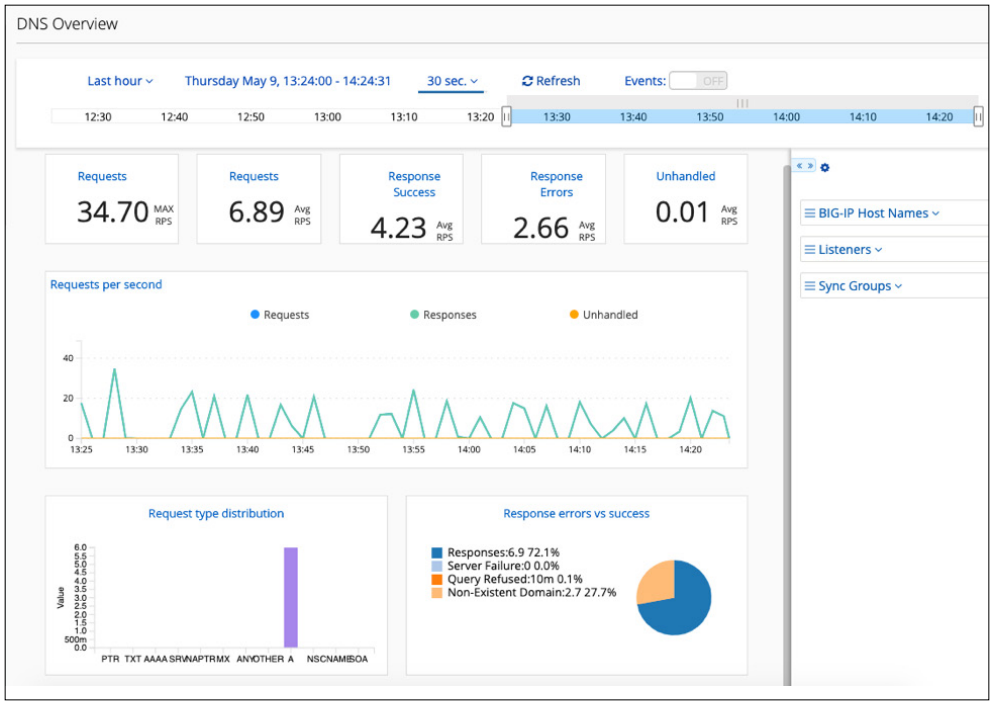


Figure 9: BIG-IQ integration showcases advanced DNS visibility with requests, responses, and unhandled query insights for in-depth analytics.

NETWORK INTEGRATION

BIG-IP DNS is designed to fit into your current network and into your plans for the future. Integration features include:

- **SNMP management application support**—BIG-IP DNS integrates its MIBs and an SNMP agent with DNS. This enables SNMP management applications to read statistical data about BIG-IP DNS performance.
- **Third-party integration**—BIG-IP DNS communicates and integrates with a broad array of network devices. This includes support for various types of remote hosts, such as SNMP agents, third-party caches, servers, routers, and load balancers to diagnose the health of network endpoints.
- **IPv6/IPv4 support**—Ease the transition to IPv6 by providing DNS gateway and translation services for hybrid IPv6 and IPv4 solutions and managing IPv6 and IPv4 DNS servers. BIG-IP LTM configured with NAT64 transforms IPv6 to IPv4 for those IPv4-only environments.

- **IP Anycast integration**—DNS query volumes directed to one IP address, whether legitimate or during a DoS attack, are easily managed by distributing the load among multiple geographic BIG-IP DNS devices. Network managers realize these benefits:
  - Improved user performance and reliability
  - Reduced network latency for DNS transactions
  - Ability to scale DNS infrastructure to manage DNS request load to one IP address
  - Lower rates of dropped query packets, reducing DNS timeouts/retries
  - Increased revenue because more users are serviced and brand equity is protected

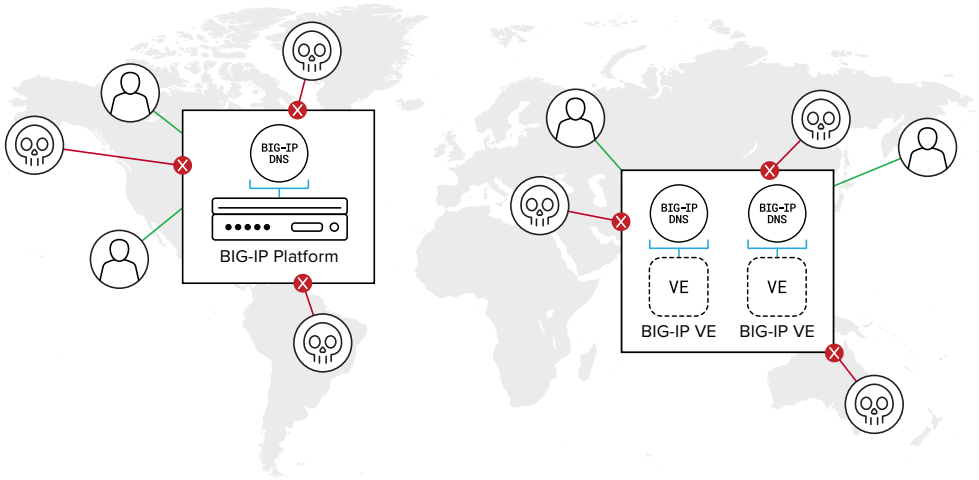


Figure 10: BIG-IP DNS and IP Anycast integration distributes the DNS request load by directing single IP requests to multiple local devices.

- **Global server load balancing in virtual and cloud environments**—Easily spin up virtual instances of BIG-IP DNS. Provide flexible DNS delivery and global application availability by routing users to applications in physical, virtual, and cloud environments.

ARCHITECTURE

The advanced architecture of BIG-IP DNS gives you total flexibility to control application delivery without creating traffic bottlenecks.

The BIG-IP DNS architecture includes:

- **TMOS**®—The F5 operating system, TMOS, provides a unified system for optimal DNS and application delivery, giving you total visibility, flexibility, and control across all BIG-IP services.
- **Query and response performance and scalability**—Linearly scale on larger platforms and multi-bladed chassis for increased performance by integrating functions in TMOS. BIG-IP DNS is can be provisioned for platforms that support F5 Virtual Clustered Multiprocessing™ (vCMP®).

BIG-IP PLATFORMS

Only F5's next-generation, cloud-ready ADC platform provides DevOps-like agility with the scale, security depth, and investment protection needed for both established and emerging apps. The new BIG-IP® iSeries appliances deliver quick and easy programmability, ecosystem-friendly orchestration, and record-breaking, software-defined hardware performance. Customers can now accelerate private clouds and secure critical data at scale while lowering TCO and future-proofing their application infrastructures. F5 solutions can be rapidly deployed via integrations with open source configuration management tools and orchestration systems.

In addition to the iSeries, F5 offers VIPRION modular chassis and blade systems designed specifically for performance and for true on-demand, linear scalability without business disruption. The new VELOS platform is the next generation of F5's industry-leading chassis-based systems, which delivers unprecedented performance, scalability, and customization in a single ADC system. BIG-IP® virtual edition (VE) software runs on commodity servers and supports the broadest range of hypervisors and performance requirements. VEs provide agility, mobility, and fast deployment of app services in software-defined data centers and cloud environments.

The next-generation Application Delivery Controller (ADC) solution, F5 rSeries, bridges the gap between traditional and modern infrastructures with a rearchitected, API-first platform designed to meet the needs of your traditional and emerging applications. The new F5 rSeries delivers unprecedented levels of performance, a fully automatable architecture, and the highest reliability, security, and access control for your critical applications.

See the BIG-IP System Hardware, VIPRION, VELOS, and Virtual Edition data sheets for details. For information about specific module support for each platform, see the latest release notes on AskF5. For the full list of supported hypervisors, refer to the VE Supported Hypervisors Matrix.

In addition, F5 offers BIG-IQ® Centralized Management for single-pane-of-glass management of all F5 devices for enabling orchestration of F5 application delivery policies.

BIG-IP iSeries Appliances

VIPRION Chassis

rSeries Appliances

VELOS Chassis

BIG-IP Virtual Editions

F5 CLOUD SERVICES

Now you can easily provision and configure the services your apps need in minutes. Built in a pay-as-you-go model, F5 Cloud Services offer predictable pricing, flexibility and the ability to auto-scale to meet changing demand. Have your on-premises DNS services and zone transferred to F5 Cloud Services:

- **DNS Cloud Service**—Easily provision and configure DNS services with a few clicks; begin responding to queries within minutes of activation.
- **DNS Load Balancer Cloud Service**—Ensure high availability and application performance with the simple, intelligent F5 DNS Load Balancer Cloud Service.

DNS ON-DEMAND SCALING

Administrators have the option to add DNS and GSLB on-demand scaling with rate limit and object limit capacity as desired to BIG-IP DNS or BIG-IP LTM appliances. This option supports requirements for exact traffic performance, resulting in lower CapEx and OpEx. On-demand scaling includes the following services: DNS, GSLB, and DNSSEC. User interface statistics show rated capacity of instances, such as query RPS and object limits, which deliver fast traffic detail for easy capacity planning. Contact your regional F5 sales representative or reseller for more information.

DNS QUERY RPS MAXIMUM PERFORMANCE

BIG-IP DNS services deliver query response per second (RPS) with high performance scalability. The table below lists many BIG-IP platforms with DNS Express enabled for authoritative DNS query response with the maximum capabilities per platform.

Platform	Max Query RPS
Virtual Edition	250,000*
r2600	590,000
r2800	1,100,000
r4600	1,800,000
r4800	2,500,000
r5600	2,700,000
r5800	3,800,000
r5900	4,900,000
r10600	5,000,000
r10800	5,700,000
r10900	6,900,000
i2600	240,000
i2800	500,000
i4600	480,000
i4800	880,000
i5600	1,000,000
i5800, i5820 FIPS	1,500,000
i7600	1,500,000
i7800, i7820 FIPS	2,300,000
10150s NEBS	990,000
10350v FIPS, NEBS	1,800,000
i10600	2,000,000
i10800	2,900,000
i11400-DS	1,200,000
i11600 (DS)	1,800,000
i11800 (DS)	4,500,000
i15600	4,100,000
i15800	8,100,000
VELOS CX410 Full Chassis (8 blades)	
VELOS BX110 Blade	2,500,000
VIPRION 2200 Full Chassis (2 blades) VIPRION 2400 Full Chassis (4 blades)	
VIPRION B2250 Blade	2,100,000
VIPRION 4480 Full Chassis (4 blades) VIPRION 4800 Full Chassis (8 blades)	
VIPRION B4450 Blade	6,400,000

*BIG-IP DNS Virtual Edition is available in increments of 250,000 RPS. For 5050s and above, Rapid Response Mode (RRM—see page 2) delivers up to 200 percent of normal max query RPS when turned on. See F5 Sales or reseller for details.

SIMPLIFIED LICENSING

Meeting your applications' needs in a dynamic environment has never been easier. F5's provides you with the flexibility to provision advanced modules on-demand, at the best value.

- Decide what solutions are right for your application's environment with F5's solutions.
- Specify the subscriptions you need across hybrid-cloud environments.
- Provision the modules needed to run your applications with F5's Good, Better, Best offerings.
- Spin up or down any solution needed with Enterprise Licensing Agreements.
- Implement complete application flexibility with the ability to deploy your modules on a virtual or physical platform.

F5 GLOBAL SERVICES

F5 Global Services offers world-class support, training, and consulting to help you get the most from your F5 investment. Whether it's providing fast answers to questions, training internal teams, or handling entire implementations from design to deployment, F5 Global Services can help ensure your applications are always secure, fast, and available. For more information about F5 Global Services, contact consulting@f5.com or visit F5 Professional Services.

DEVCENTRAL

The F5 DevCentral™ technical community is an active and engaged source for the best technical, how-to articles, discussion forums, shared code, media, and more related to DNS delivery and global app networking.

MORE INFORMATION

To learn more about BIG-IP DNS, search on f5.com to find these and other resources.

Web pages

DNS Delivery
Global Server Load Balancing
DevCentral

Data sheet

BIG-IP System Hardware Data sheet
BIG-IP Virtual Editions
VIPRION
VELOS
rSeries Hardware Data sheet

Articles and videos

Intro to DNS services and global server load balancing (video)
DNS is key to connected customers
Addressing Cloud-based DNS—It's time to move
Encrypted DNS - Mitigating the Impact of DoT and DoH for Service Providers
What Is a DNS Amplification Attack?

Case studies

Bank improves user experience with always available, fast, and secure access to banking services using F5
SaaS provider ensures high uptime and resiliency for critical customer apps with F5
Everbridge manages traffic and security across global cloud providers and local data center
Shawbrook Bank enlists F5 to accelerate and scale digital transformation

DC0223 | DS-CORE-1059852307