LiveAction | SOLUTION BRIEF
A BlueCat Company

LiveNX Assurance – Network Security F5 BIG-IP LTM

Network Observability and Health

Automating Best Practices and Operational Device Issue Detection for Your Load Balancers

Without automation, IT operations teams would spend countless hours gathering diagnostics and device data to keep load balancers up and running. IT teams that manage load balancers often have limited resources, resulting in an even greater need for automated diagnostics and issue detection. The typical network engineer spends a notable portion of their time identifying and remediating known errors.

IT operations teams can avoid costly outages if they receive advance notice about common issues that can lead to bigger problems. These issues might include hidden configuration drift, forgotten ongoing maintenance tasks, or a lack of adherence to vendor, industry, and/or high availability best practices.

This solution brief presents how LiveNX Assurance - Network Security automates detection of operational device issues, which are often hidden, in your load balancers. This brief provides specific examples from a variety of use cases for F5 BIG-IP Local Traffic Manager (LTM) customers to simplify Day 2 operations, adhere to best practices, and ensure maximum reliability. It also covers key differentiators from other solutions and key solution benefits.

Solution Overview

LiveNX Assurance - Network Security avoids network disruption with automation. Think of it as a virtual expert that can expand team skills and is on duty 24/7.

LiveNX Assurance - Network Security provides deep visibility into your load balancers to flag early warning signs of issues. With our domain expertise codified into LiveNX Assurance - Network Security, the platform knows what to look for, analyzing your load balancers to ensure they are healthy.

Should it find something, the platform proactively alerts IT operations teams that there might be a service failure—or any level of degradation of service—coming. Our auto-triage capability will investigate a problem without any human intervention. It gathers additional contextual diagnostic information, analyzes, and performs common troubleshooting tasks and root cause analysis.

Then, LiveNX Assurance - Network Security provides a list of recommended remediation steps that IT operations teams can use as a guide to help address the problem. IT operations teams gain load balancer-specific knowledge from issue descriptions and recommended remediations built from the real-world experience of certified networking experts.

Effectively, we've automated best practices to help you improve the efficiency of your network operations, reduce mean time to resolution, and prevent costly disruptions.

Challenge

Undetected issues with load balancers can cause service degradation for your network or lead to an outage. Existing monitoring tools are reactive, only notifying users of an issue after it occurs, and do not provide actionable next steps.

Solution

LiveNX Assurance - Network Security proactively alerts F5 BIG-IP LTM users to issues and provides remediation steps that IT operations teams can use to resolve problems before they cause significant damage.

Benefits

- Proactively identify issues to avoid outages
- Optimize the performance of load balancer infrastructure
- Reduce mean time to resolution
- Work more effectively

Six Types of Use Cases

For F5 BIG-IP LTM customers, moving beyond the reactive mindset when things go awry is within reach. In this section, we outline six scenarios that you might encounter, with specific real-world examples of detected issues. Each explores how LiveNX Assurance - Network Security can help ensure that your load balancers are working as intended. Once issues are detected, LiveNX Assurance - Network Security provides actionable information to help IT operations teams address them. They can troubleshoot issues by following the remediation steps authored by F5 Certified Professionals.

USE CASE 1 Health and Capacity Checks

LiveNX Assurance - Network Security continuously checks the health of a range of components at both the virtual and physical layers. The goal is for IT operations teams to minimize the impact of issues and avoid bigger problems before they happen.

Sample common issues detected, based on real experience, include:

- Pool member unavailable or latency too high
- Pool operating at low capacity
- Server down
- Virtual server down, offline, or no objects
- SNAT pool near maximum allocated, exhaustion, or indefinite timeouts
- Network port speed or duplex (including TX or RX packet drops or collisions)
- DNS lookup failures or response time too high
- High memory usage or out of memory
- Critical processes down (also in a virtual system)

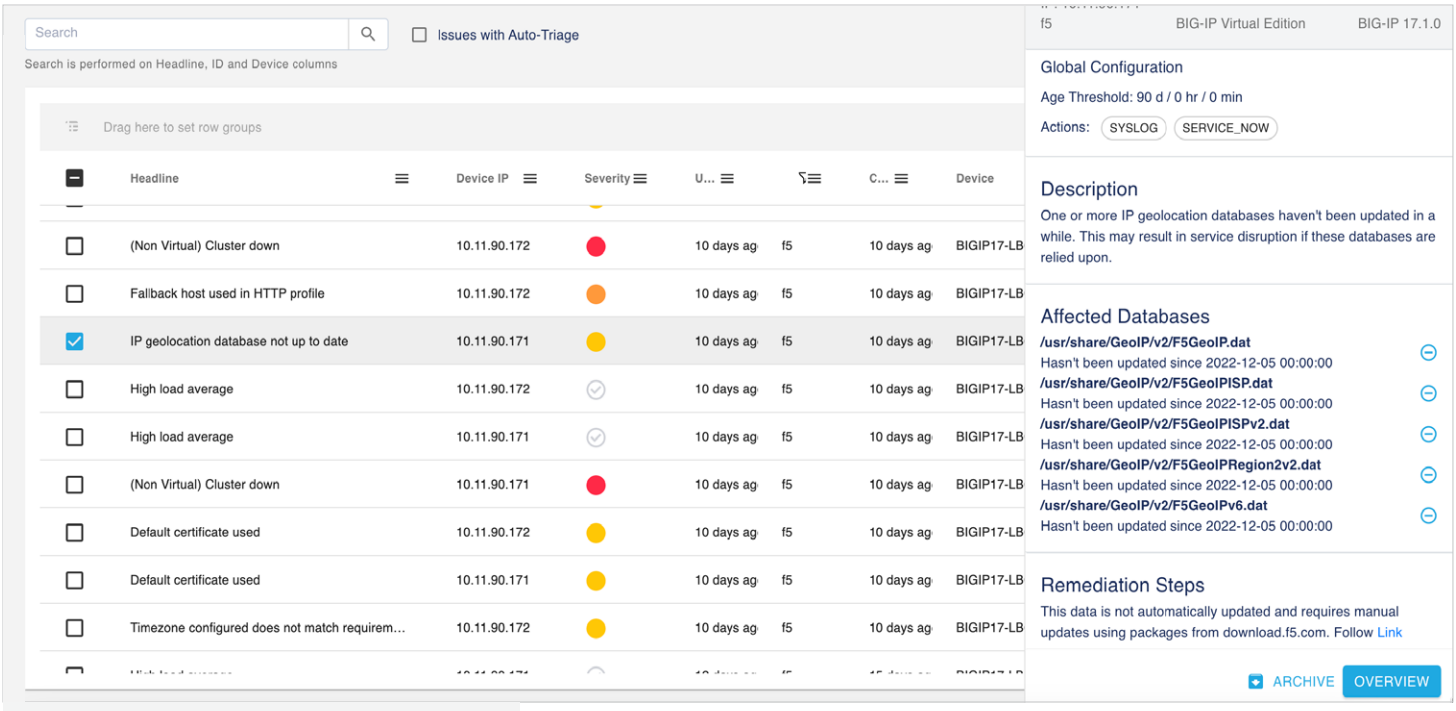


Figure 1. Sample F5 BIG-IP LTM Alerts

USE CASE 2 External Critical Services and Dependencies

Load balancers have near real-time dependency on many applications and external services. It is important to monitor the connection to these critical services. LiveNX Assurance - Network Security's automation features ensure, through regular testing, that communication with these applications and external services is always available.

For basic system operation, clustering, and most forms of troubleshooting and logging, accurate time synchronization and related timestamps are crucial. Additionally, and for most forms of external system reachability, name resolution is also key. LiveNX Assurance - Network Security checks for both NTP sync issues and DNS lookup failures while also checking remote syslog (TCP) reachability.

Figure 2. External Critical Services

When configured, RADIUS—a protocol for authentication, authorization, and accounting (AAA)—must also be accessible to facilitate authenticated user sessions or operator device access. LiveNX Assurance - Network Security checks for AAA reachability and the validity of pre-shared keys for configured endpoints.

On the client side, geolocation is increasingly important for serving users compliant or customized content. F5's IP geolocation database requires updates to ensure the correct and relevant content reaches the right destination. LiveNX Assurance - Network Security detects an out-of-date or non-functioning geolocation database and provides guidance on how to update it.

LiveNX Assurance - Network Security also checks access to F5's BIG-IQ Centralized Management. Alerts can be generated, as they can be for all checks, via actions that utilize a range of methods such as email, SNMP, syslog, or via ServiceNow integration.

USE CASE 3 Misconfigurations and Best Practices

Misconfiguration of devices, virtual servers, member pools, or any dependent services can play a significant role in unplanned downtime and impact the seamless delivery of your critical applications. Easily correctable errors can disrupt the flow of high-value traffic and compromise the reliability of your network infrastructure. LiveNX Assurance - Network Security continuously detects misconfigurations by verifying against a gold standard for your network. It continuosly assesses devices for alignment with configuration recommendations from F5 and seasoned practictioners.

Misconfigurations and best practices that LiveNX Assurance - Network Security might detect and provide notifications for include:

- OS software level does not meet the standard
- Time zone is incorrect
- Static routing table has changed
- DNS, BIG-IQ, NTP, or RADIUS configuration missing or does not match requirement
- Virtual server is offline and not disabled
- Automap is enabled
- Default node monitor is not configured
- Deprecated 'matchclass' command in iRules

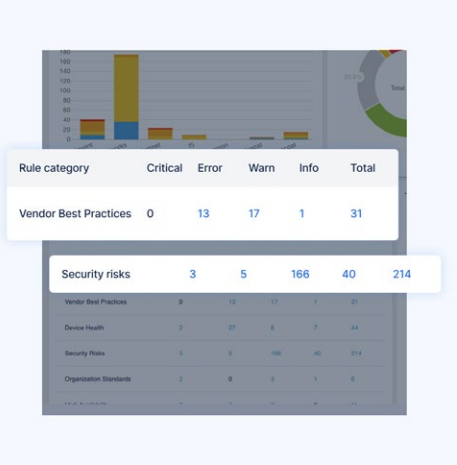
USE CASE 4 High Availability Readiness

To ensure the delivery of critical applications and services and to prevent a single point of failure on your network, you made the investment to deploy redundant infrastructure. Ensuring high availability readiness is crucial. LiveNX Assurance - Network Security constantly detects high availability unreadiness from cross-device inconsistencies.

Examples of high availability readiness issues that LiveNX Assurance - Network Security might detect and provide alerts for include:

- Virtual or physical cluster down
- Cluster member no longer active
- Cluster configuration not synched
- OS name or version mismatch across clusters
- Connected networks, features, or routing do not match across clusters
- IPv4 subnets or interface (MTU, speed, or duplex) does not match across clusters
- Cluster has preemption enabled
- Cluster member domain name mismatch

USE CASE 5 Auto-Detect Security Risks



Security is not just the purview of dedicated security teams but key to the work of IT operations teams, too. Mitigating security risks is an ongoing effort and bolstered by adhering to predefined compliance requirements.

Sample security checks LiveNX Assurance - Network Security performs to detect security risks include:

- Virtual forwarding server listening with a destination of all virtual LANs
- Default certificate used
- Weak cipher or protocol used with SSL profiles
- Clear text SNMP (v1 or v2c) versions used
- CVE vulnerability found in version
- Unencrypted cookie persistence files were found

USE CASE 6 Automate Easily Forgotten Maintenance Tasks

Infrastructure operations requires ongoing maintenance. Many maintenance tasks are unavoidable, and others are sometimes overlooked until it's too late. To ensure overall system health and optimal functioning, tasks that need to be performed regularly or intermittently—such as configuration backups or certificate renewals—can be initiated or checked for and subsequently alerted on.

How often has one of these issues led to problems with a production service?

- Certificate expiration or nearing expiration
- Failed device configuration backup
- Uptime exceeds a configured threshold
- License usage limit approaching
- Hardware or software end of support is nearing

Infrastructure Assurance provides automated checks and proactive alerts for maintenance tasks so that IT operations teams can stay in control and don't get tripped up by any surprises.

Key Differentiators

There are four major differences between LiveNX Assurance - Network Security and other network monitoring and management solutions.

1. Our automation elements are developed by our community of experts. By bringing expertise from our community, load balancer vendors, and Fortune 1,000 customers, we can gather the most relevant and important device knowledge. Crowdsourcing brings together ideas and expertise that would not otherwise be available.
2. When deploying LiveNX Assurance - Network Security for load balancers, customers immediately receive notifications about misconfigurations, errors, security risks, vulnerabilities, and lack of adherence to best practices. Because LiveNX Assurance - Network Security knows what to look for, the platform can continually and preemptively identify issues to avoid bigger problems. Other network monitoring solutions lack specific, codified domain expertise.
3. When it detects the symptoms of various potential problems, LiveNX Assurance - Network Security automates the troubleshooting process to determine root causes. Other network monitoring and management solutions provide alerts but stop there. It's left to IT operations teams to conduct troubleshooting and root cause analysis themselves. Automated detection and analysis of issues can prevent them from recurring and reduce downtime.
4. Once root causes have been determined, LiveNX Assurance - Network Security goes further than other monitoring solutions by providing a list of actionable remediation steps that IT operations teams can take. IT operations teams gain specific knowledge from the issue descriptions and recommended remediations.

Solution Benefits

IT operations teams enjoy several benefits when using LiveNX Assurance - Network Security as a solution for hidden issue detection and recommended remediation. They include:

- **Avoid downtime.** Proactively identify misconfigurations, high availability inconsistencies, forgotten maintenance tasks, and other best practices to avoid outages.
- **Optimize the performance of your load balancer infrastructure.** Automation streamlines IT operations, allowing IT teams to deliver optimal load balancing to your organization.
- **Reduce mean time to resolution.** Accelerate troubleshooting by conducting automated root cause analysis, without human intervention.
- **Work more efficiently.** LiveNX Assurance - Network Security surfaces useful and actionable information that will immediately facilitate your IT operations team's work.

LiveAction, a BlueCat Networks company, provides end-to-end visibility of network and application performance from a single pane of glass. We provide enterprises with confidence that the network is meeting business objectives, full network visibility for better decisions, and reduced cost to operate the network.

www.liveaction.com | 901 Campisi Way, Suite 222 Campbell, CA 95008 | USA +1 (888) 881-1116