Solution Brief | BlueCat Infrastructure Assurance for Integrity

BLUECAT™

Challenge

Undetected issues with DNS, DHCP, and IP address management infrastructure can slow your network down 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

BlueCat Infrastructure Assurance proactively alerts Integrity enterprise customers to issues and provides remediation steps that admins can use to resolve problems before they cause significant damage.

Benefits

- Proactively identify issues to avoid downtime and outages
- Optimize the performance of your DDI infrastructure
- Automate troubleshooting and receive remediation steps
- Improve the efficiency of your IT operations team

Request a live demo

DDI Day 2 operations and best practices

Without automation, IT operations teams would spend countless hours gathering diagnostics and device data to keep DNS, DHCP, and IP address management (together known as DDI) infrastructure up and running. IT teams that manage DDI infrastructure often have limited resources, resulting in an even greater need for automated diagnostics and issue detection. The typical network administrator spends a notable portion of their time identifying and remediating known errors.

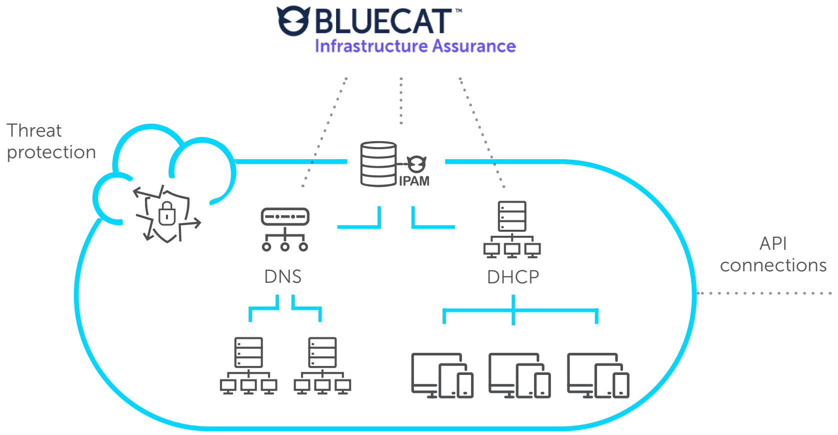
IT operations teams can avoid costly outages if they receive advanced notice about common issues that can lead to bigger problems. These issues might include hidden configuration skew, forgotten ongoing maintenance steps, or a lack of adherence to vendor or industry best practices.

For Integrity enterprise customers, this solution brief presents how BlueCat Infrastructure Assurance automates detection of operational device issues, which are often hidden, in your DDI environment. This brief provides specific examples from four types of use cases. It also covers key differentiators from other solutions and key solution benefits.

Solution overview

BlueCat Infrastructure Assurance avoids network disruption with automation. Think of it as a virtual DDI expert, on duty 24/7.

Infrastructure Assurance provides deep visibility into BlueCat Integrity enterprise environments, including its key BlueCat Address Manager and BlueCat DNS/DHCP Server (BDDS) components, to flag early warning signs of issues. With our domain expertise codified into BlueCat Infrastructure Assurance, the platform knows what to look for, interrogating your systems to ensure they are healthy. This includes knowledge of capabilities and features of the BlueCat implementation of DDI and its entire management layer.



Should it find something, the platform proactively alerts customers 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 interventions. It gathers additional contextual diagnostic information, analyzes, and performs common troubleshooting tasks and root cause analysis.

Then, BlueCat Information Assurance provides a list of recommended remediation steps that admins can use as a guide to help address the problem. As a result, IT operations teams can gain BlueCat-specific knowledge from issue descriptions and recommended remediations built from the real-world experience of BlueCat experts.

Effectively, we've automated BlueCat best practices to help you improve the efficiency of your Day 2 operations, keep service delivery available at all times, and prevent costly disruptions.

Four types of potential use cases

For BlueCat Integrity enterprise customers, moving beyond the reactive mindset when things go awry is within reach. In this section, we outline four types of scenarios that you might encounter, with specific real-world examples. Each explores how BlueCat Infrastructure Assurance can help ensure that your DDI infrastructure is working as intended and that your organization's DNS services are uninterrupted.

Use case 1: Stateful health checking

We've codified BlueCat's decades of DDI expertise in Infrastructure Assurance. With it, Infrastructure Assurance continuously assesses the health of Address Manager and BDDSes by comparing expected device configurations against the current status. The goal is to find lurking issues and address them before they impact services.

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

- DNS lookup failure
- DNS queries failure is higher than expected
- DNS serial number falling too far behind—if changes have not been propagated to the secondary server, a zone can be removed
- Notification processing falling behind—DNS going further out of sync with Address Manager, resulting in incorrect information being presented
- NTP sync failure
- Concurrent connections are too high
- Kernel connection limit has been modified
- Kernel connection tracking is nearing limit

Use case 2: The network factor

Address Manager or BDDSes are often not the cause of many issues. Instead, changes in other devices within the broader networking environment are often the culprit.

For example, many problems can be traced to firewall policy changes. Perhaps someone inadvertently broke the connection between the primary and secondary DNS servers, causing zone transfer failure. These problems often go unnoticed. And eventually a zone expires, impacting DNS services.

With Infrastructure Assurance, you will receive proactive alerts relating to connectivity issues. No more waiting for a zone transfer failure, a DNS deployment failure, or a DHCP failover failure.

Sample connectivity issues detected might include:

- Connectivity broken between the two DHCP failover servers
- Communication from Address Manager to BDDSes not working
- Communication from BDDSes to Address Manager not working
- Communication from primary DNS server to secondary server not working for zone transfer
- Communication from primary Address Manager to secondary or tertiary Address Manager not working

Use case 3: High availability readiness

To prevent a single point of failure on your network, you made the investment to deploy redundant infrastructure to ensure always-on services. Unfortunately, despite the investment, failovers do not always go smoothly.

Infrastructure Assurance constantly detects high availability unreadiness from cross-device inconsistencies. This includes configuration state and ensuring adherence to best practices. Examples of high availability readiness issues that Infrastructure Assurance might detect and provide alerts for include:

- Alert if xHA service, xHA cluster, or cluster member is down
- Identify if xHA configuration is not synchronized
- Alert if xHA backbone is overlapping
- Alert if xHA backbone interface is not configured
- Identify if DHCP failover state has changed
- Ensure connectivity between the two DHCP failover servers is working
- Alert if DHCP failover server(s) is/are down
- Identify if DHCP failover state has changed

Beyond ensuring high availability readiness, Infrastructure Assurance ensures database replication is successful between the primary and secondary or tertiary Address Manager. It will also ensure that backups are successful. Notifications of database issues might include:

- Database replication is disabled
- Database replication stopped
- Database replication latency nearing critical limit or nearing warning limit
- Large, accumulated WAL file size or large number of accumulated WAL files
- Backup is not configured or is disabled
- Backup failed and another backup process is running
- Local or remote backup failed or is not configured

Use case 4: Misconfigurations

Device misconfiguration is another major cause of unplanned downtime. Certainly, configuration errors can create security gaps in your network, making it vulnerable to cyberattacks. Infrastructure Assurance continuously detects misconfigurations by verifying against a gold standard for your network. It even detects configuration drift from Address Manager. Misconfiguration issues that BlueCat Infrastructure Assurance might alert you of include:

- Configuration drift detected—DNS server configuration does not match Address Manager
- NTP server configured does not match requirement
- DNS server configured does not match requirement
- Syslog server configured does not match requirement
- Manual override enabled

Key differentiators

There are three major differences between BlueCat Infrastructure Assurance and other network monitoring and management solutions.

- For Integrity enterprise customers, we've codified our domain expertise into Infrastructure Assurance. When deploying Infrastructure Assurance in a BlueCat DDI environment, customers immediately receive notifications about misconfigurations, errors, and lack of adherence to best practices. Because Infrastructure Assurance knows what to look for, the platform can continually and preemptively identify issues to avoid bigger problems. Meanwhile, other network monitoring solutions lack specific, codified domain expertise.
- When it detects the symptoms of various potential problems, Infrastructure Assurance 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 analyses themselves. Automated detection and analysis of issues can prevent them from recurring and reduce downtime.
- Once root causes have been determined, Infrastructure Assurance 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 compiled from the real-world experience of BlueCat experts. These specific, actionable insights also reduce troubleshooting time.

Solution benefits

IT operations teams enjoy several benefits when using Blue Cat Infrastructure Assurance as a solution for hidden issue detection and recommended remediation. They include:

- Achieve zero downtime.
  Proactively identify misconfigurations, high availability inconsistencies, forgotten maintenance tasks, and other best practices to avoid outages.
- Optimize the performance of your BlueCat DDI infrastructure.
  Automation streamlines IT operations, allowing network teams to deliver optimal DDI services to your organization.
- Automate troubleshooting.
  Remediate DNS or DHCP issues by conducting automated root cause analysis, without human intervention.
- Work more efficiently.
  Infrastructure Assurance surfaces useful and actionable information that will immediately facilitate your IT operations team's work.

Next steps

Discover how BlueCat Infrastructure Assurance can reduce service tickets and avoid outages.

Request a live demo

Corporate Headquarters
4100 Yonge St. 3rd Floor, Toronto, ON, M2P 2B5
1-416-646-8400 | 1-866-895-6931

bluecat.com