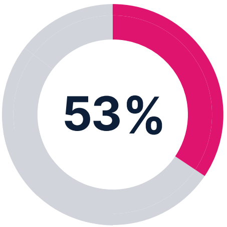
BLUECAT™ | Explainer

Missing signs of impending network downtime?

Quickly get ahead of three top DDI issues



of network outages and performance issues could be eliminated with better network management tools, according to IT professionals.

Source:
Network Management Megatrends 2024, Enterprise Management Associates

Disk space runs low on DNS and DHCP servers: A creeping network issue

DNS and DHCP servers heavily rely on disk space to function correctly. Often, disk utilization can be an afterthought until vast amounts of data—including zone files, caches, lease databases, configuration files, and logs—eat away at precious storage. When disk space runs low, network teams face server latency issues, server crashes, IP address assignment failures, and corrupted data.

BlueCat Infrastructure Assurance helps prevent these issues from happening by continuously measuring your disk space utilization metrics. When it detects an issue, Infrastructure Assurance conducts auto-triage and root cause analysis in real time and offers up recommended remediation steps. It provides a range of alerts to help diagnose disk space utilization issues such as accumulated WAL file sizes, database replication errors, and deployment failures. With these near-real time alerts and recommended remediation steps, IT operations teams can address issues early, ensuring their DNS and DHCP infrastructure remains stable and secure.

Broken IPAM, DNS, or DHCP connections: A culprit in disguise

Misconfigurations are often the culprit behind IP address management (IPAM) and DNS or DHCP communication breakdowns. When these connections break, DNS records aren't updated, DHCP leases fail, and IP conflicts and downtime arise.

However, sometimes looks can be deceiving. The culprit could also be restrictive firewalls that block essential ports and disrupt communication between servers.

Infrastructure Assurance can quickly detect connection issues across DNS, DHCP, and IP address management (DDI) and security infrastructure to offer actionable remediation steps.

Uncovering the source of misconfigurations—such as blocking port 647—reduces the time to remediate DHCP failover connection failures, avoiding costly network downtime.

> **“Business operations halted when our critical Wi-Fi devices could not connect due to DHCP being exhausted.”**
>
> Network administrator,
> Financial services

DHCP range exhaustion: A ticking time bomb for your network

DHCP range exhaustion occurs when a DHCP pool runs out of IP addresses to assign to devices on a network. It can happen when there are too many devices on the network or when IP addresses aren't recycled from devices that have left the network.

When the DHCP pool runs dry, new devices can't connect to the network and devices already on the network suffer IP renewal conflicts. This results in connectivity issues and potential network downtime.

Infrastructure Assurance provides proactive alerts on DHCP range utilization issues. With these proactive alerts as a guide, IT operations teams can expand the pool, adjust lease times, and reorganize subnets to diffuse issues before they spiral out of control.

BLUECAT™

Learn more