**Everything You Need to Know About DNS Monitoring**

In order to communicate, web pages, devices and applications need a common **naming system** which allows them to identify each other and send information. This is particularly important when the communication takes place over the Internet because of the large number of services and websites that need to be identified.

This is why the **Domain Name System** (DNS) is so important for businesses. It matches website pages and devices to an IP address that can be traced by other devices. With a large number of accessible websites and devices, DNS records all the IP addresses so an enterprise does not have to manually do it.

In this way, Domain Name System is a useful system for a business, but at times its performance can be affected due to a number of factors. To prevent this from happening, businesses should use [**DNS monitoring solutions**](https://www.virtualmetric.com/windows-monitoring) to ensure smooth operations of enterprise communications.

**How Does DNS Work?**

It’s important to know the DNS communications process and where a DNS request connects. Whenever a device inputs a domain name into a web browser, the browser then sends request to the **name server** for that domain’s associated IP address. Upon locating the IP, it allows the browser to open the associated website.

**Why DNS Monitoring?**

DNS monitoring is important to ensure that your employees are able to seamlessly connect to a website and use the resources over the internet up to full extent. For companies that rely on internet to operate, a DNS monitoring tool can ensure its effective performance by tracking **DNS requests** and DNS server.

**Why is DNS Monitoring Important?**

Let us now briefly look at what to expect from a effective DNS monitoring tool.

**Connectivity between Network and DNS Server**

This is a basic check which verifies your network’s connection to a DNS server. DNS monitoring tools regularly perform this check to test **connectivity** between a device and configured recursive and authoritative servers. This check is important because a DNS server can become unavailable at any point of time.

When your windows DNS monitoring tool sends test DNS requests, it identifies whenever a server is not responding. It also helps to verify that the domain name is correctly resolved every time. This check is performed with the help of a **network monitoring** tool which gives you information such as:

* How many times the recursive DNS server was out of service
* Failure in domain name resolution

**DNS Request Latency**

The time taken by a device to send a Domain Name System request and get an answer should be as brief as possible. DNS monitoring helps you discover any delays in your network by checking for any **latency** between the connections for your team to address.

**Tracking and Logging DNS Requests**

DNS monitoring can also discover and track **IP addresses** of DNS requests and log every website viewed by a device connected to your network. This helps your network team find out which websites your employees are visiting and how long it takes to complete the DNS request.

**DNS Security Check**

DNS protocols are not very secure and easily susceptible to attacks. A DNS server can be infected by malicious actors who feed false IP addresses intentionally to a device. This can lead users to an **infected website** instead of the actual legitimate website they intended to visit.

When a user accesses a website for the first time, the **monitoring solution** can check the IP address contents to identify any security threats. Since, website IP address can change, the monitoring tool can also verify any new address before it delivers website information to the user.

DNS security checks can help you identify **vulnerabilities** before they can be exploited. DNS monitoring can help you prevent a number of attacks including:

* Denial of Service (DoS) and Distributed Denial of Service (DDoS) Attacks
* Domain hijacking
* DNS Spoofing
* DNS Cache poisoning
* DNS tunneling
* DNS flood attacks
* Phantom Domain attacks
* Random subdomain attacks

**DNS Record Lookup**

Just like a Powershell DNS lookup query, a DNS monitoring tool also allows you to validate and check **DNS records** associated with a domain and shows them as received. If you have changed your DNS records or hosting, it will verify that the records you entered are correct so that there is no downtime.

DNS record lookup monitoring helps you in:

* Monitoring any changes that may have occurred in the DNS records
* Keeping updated copies of the records
* Generating history of all changes made
* Achieving control over your DNS service by receiving alerts whenever an unwanted change takes place and make corrections

Among other records, DNS record lookup fetches some important records such as

* SOA record: It changes serial number in case of a change in DNS entry. Monitoring SOA record can help in preventing an imminent attack
* MX and SRV records: These are key to preventing email systems from getting hacked. Monitoring these records prevents loss of communication routes.
* NS Records and Root Server: These records can ensure that **primary and backup records** for nameserver are not being interfered with.

**Tracking Volume of Outgoing Traffic**

You can monitor your **outbound traffic volume** by tracking domain name resolution requests. This can help you maintain a table of the most requested domains and create quotas for them which indicate request levels. In event of any volume exceeding the quota, the monitoring software can issue an alert for unusual number of requests.

**How Virtual Metric’s Windows DNS Server Monitoring Tool Can Help You?**

Without a monitoring mechanism in place, teams cannot do much to resolve issues that they cannot see. At the end of the day, **powerful DNS monitoring** adds another visibility layer which is vital for optimal performance of teams given the task of running their enterprise networks smoothly.

It’s always recommended to regularly run monitoring checks for detecting latency or disruption in service. Virtual Metric’s [**Windows DNS Server Monitoring**](https://www.virtualmetric.com/windows-monitoring)and performance tool is a comprehensive real-time agentless Windows infrastructure monitoring suite. You can set up smart notifications and alerts for severity levels, active hours, planned downtime and much more.

Our monitoring tool also allows you to check whether **TCP network connection** exists, and how it is performing. You can also carry uptime checks for SSL certificates and HTTPS requests, identify issues with your SSL certificates and get alerted when they are about to get expired.

Get a free 30-day trial of our windows DNS monitoring tool [here](https://www.virtualmetric.com/trial).