Stay Open. OX

CHECKLIST

Is your DNS ready for 5G?

For the last few years, 5G networks have been deployed around the world, usually starting with the RAN. They come with improved bandwidth for subscribers and their devices, wholesale architectural changes towards an SDN/NFV-based network and other specific goals for new services such as VR/AR.

However, typical legacy DNS deployments do not support 5G latency targets or architectural requirements. This quick checklist will let you find out how well your DNS installation is equipped for 5G requirements. If you want to learn more about the requirements that 5G has for DNS installations, check out our free whitepaper 'DNS in a 5G network'. Please feel free to contact us if you would like to discuss anything further or need support in making your DNS ready for 5G.

Deployment

☑ Support for Virtual Network Functions (VNFs)

☑ Cloud-Native Network Functions (CNFs) deployment

If you are still installing DNS software manually on bare metal, your competitors will easily outrun you in the 5G race. DNS software must be capable of being run on Virtual Machines (VMs). Luckily, most DNS installations today support VNF. For 5G, it is crucial that your solution at least supports NFV.

NFV is one of the primary architectural components of a 5G network, enabling network slicing, orchestration of VNFs and more. However, to cope with current and future trends, traditional approaches, including NFV, are not efficient and agile enough to meet today's needs. This is why more and more network operators are looking to cloud-native solutions for next generation network infrastructure. Cloud-native DNS means the ability to run in containerized infrastructure and brings highly scalable and distributed DNS within reach, while simplifying deployment and scaling by the operations teams.

Performance Measurement

☑ Measure end-to-end latency as seen by subscribers using probes installed throughout the network

DNS performance is extremely important but can be hard to measure. The most critical metrics to measure are the 99.9% latency experienced by real subscribers on your network, but these are typically not the metrics that are available to you as the operator of a DNS platform. If you only measure average latency, you will miss the spikes that will cause dissatisfaction amongst your subscribers, which is why measuring the 'long-tail' of latency is so important. This is especially true for those 5G ready devices, which require low latency.

Measuring latency only at the DNS servers, can also give a false impression: for example, if there is a problem with the RAN, or with the interaction between the RAN equipment and the WAN equipment. Your subscribers could experience very high latency that your KPIs completely miss. DNS solutions, especially those used in 5G networks, should always measure end-to-end latency as experienced by your subscribers.

Low Latency

☑ Support for edge DNS deployment near the end-user

☑ Support for tiered caching

☑ Provide DNS aware load balancing to optimize cache hits

A key component of enhancing the user experience with 5G is delivering fast content to users, for example, for video streaming services. For this, the content is located as close to the end-user as possible, typically near the edge of the network. This also requires DNS software to be deployed on the edge. In addition, the DNS solution needs to ensure that users end up being directed to the most local content server. A load balancer on the edge can take over this function and, at the same time ensure an equal distribution of traffic.

Once the DNS service has retrieved the localized answer from the content provider, it should cache the result appropriately for the end-user, meaning that future DNS lookups from the same user or other users in the same locality will be delivered from the cache and thus deliver content even faster. Tiered caching should provide an optimal balance between fast localized DNS responses and minimized latency for domains that are looked up less frequently.

Operations options

☑ Deployment automation options using Helm and Kubernetes

☑ Monitoring and Reporting possibility using OpenMetrics and Grafana

☑ Availability of on-demand DNS instances to support network slicing

☑ Day 1 and 2 Configuration options and Lifecycle Management

5G comes with a whole new set of requirements for DNS. For example, services will have to be deployed automatically across hundreds or even thousands of nodes, where configuration changes or upgrades need to be rolled out seamlessly and without downtime, and ops teams should be alerted to service, performance or latency issues. This can only be achieved through automated and orchestrated deployment, network slicing and configuration and lifecycle functionality to manage and monitor all these activities.

Privacy features

☑ Support of DNS over HTTPs (DoH)

☑ Support of DNS over TLS (DoT)

☑ Support of DNSSEC signing and validation

☑ Support of Query Name Minimization

If the DNS traffic of your subscribers is not protected, anyone monitoring a network would be able to see all of the DNS lookups that a given end-user or mobile device was making. This is a huge privacy issue as well as a potential security issue, if you consider that a MITM attack could also rewrite DNS answers.

There are three main technologies that address the security, privacy and integrity issues inherent in traditional plaintext DNS: DNS encryption via DoH or DoT, DNSSEC and Query Name Minimization. You should ensure that your DNS solution supports these technologies as not only performance and latency, but also security and privacy are important to your subscribers these days.

Security measures

☑ Detecting Phishing, Malware and Botnet Command & Control

☑ Blocking/filtering Phishing, Malware and Botnet Command & Control

☑ Alerts/Notifications for Phishing, Malware and Botnet Command & Control

DNS solutions should check lookup requests, block malicious content, such as phishing and malware, and notify subscribers and providers about the identified security issues. Of course, this has also been valid before 5G, but with much greater traffic rates and increased content consumption via non-traditional connected appliances, such as smart TVs, subscribers need help in protecting these devices against attacks.

IoT security

☑ Alert when IoT devices are potentially infected with malware

☑ Blocking/filtering Malware on IoT devices

☑ Prevents Botnet activation through IoT devices

☑ Protect your network from 'IoT' DNS based DDoS

The threat of malware-infected IoT devices causing damage to physical infrastructure, networks and even human life, is very real. The average subscriber is not able to ensure adequate protection for always connected IoT devices without any interface. Thus, detecting malware-infected IoT devices in the network is the only way to ensure that such devices do not continue to cause harm. This is achieved by using regularly updated threat intelligence feeds which contain information on the IP addresses and hostnames used to host malware Command and Control (C2) servers. By detecting the devices that attempt to connect to known C2 servers, their network access can be blocked, and the owner of the device can then be alerted. This also provides protection against Distributed Denial of Service (DDoS) attacks originated by botnets resulting from self-contained IoT devices communicating with each other.

Monitoring and analysis

☑ Big data analytics connector

☑ Long-term query logging & searching options

☑ End-to-end performance measurement

Monitoring and analyzing huge amounts of traffic requires new tools. DNS software needs to be able to be connected with solutions that can analyze big data. To feed big data analytics tools with useful and representative information, your DNS solution should be able to save queries long-term and provide a search functionality to scan the data. It should also be capable of monitoring and analyzing the most important DNS functions at any time, including performance measurements.

License model

☑ Subscriber-based licensing

☑ QpS-independent licensing

☑ Instance-independent licensing

To cope with future traffic levels from several connected traditional as well as IoT devices per subscriber, your DNS supplier should support subscriber-based licensing instead of a pricing model that is based on traffic or instances. Your DNS costs need to support whatever product innovations you will provide in the future. This is only possible if you have complete flexibility when it comes to deploying DNS software in whatever configuration and volume of instances you require. Increased traffic and additional software instances should not incur additional costs.

About OX PowerDNS

POWERDNS

PowerDNS is a leading provider of open source and commercial DNS software since 2001. OX PowerDNS is focused entirely on large-scale DNS service-providers, including mobile and fixed-line broadband operators, hosting, and cloud service providers.

Headquartered in the Netherlands, PowerDNS is part of the Open-Xchange group of companies, which are dedicated to keeping the internet open, safe, and free.

Learn more about our OX PowerDNS solutions.

About Open-Xchange

Stay Open. OX

Open-Xchange is a developer of secure and open communication and office productivity software, IMAP server software and DNS solutions. Since 2005, it has partnered with many of the world's largest Internet Service Providers (ISPs), telcos and carriers.

Open-Xchange products are used by 200 million people globally. They create vendor independence, and generate trust by providing full transparency and control over system governance through an OS business model.

To find out more visit our company page.