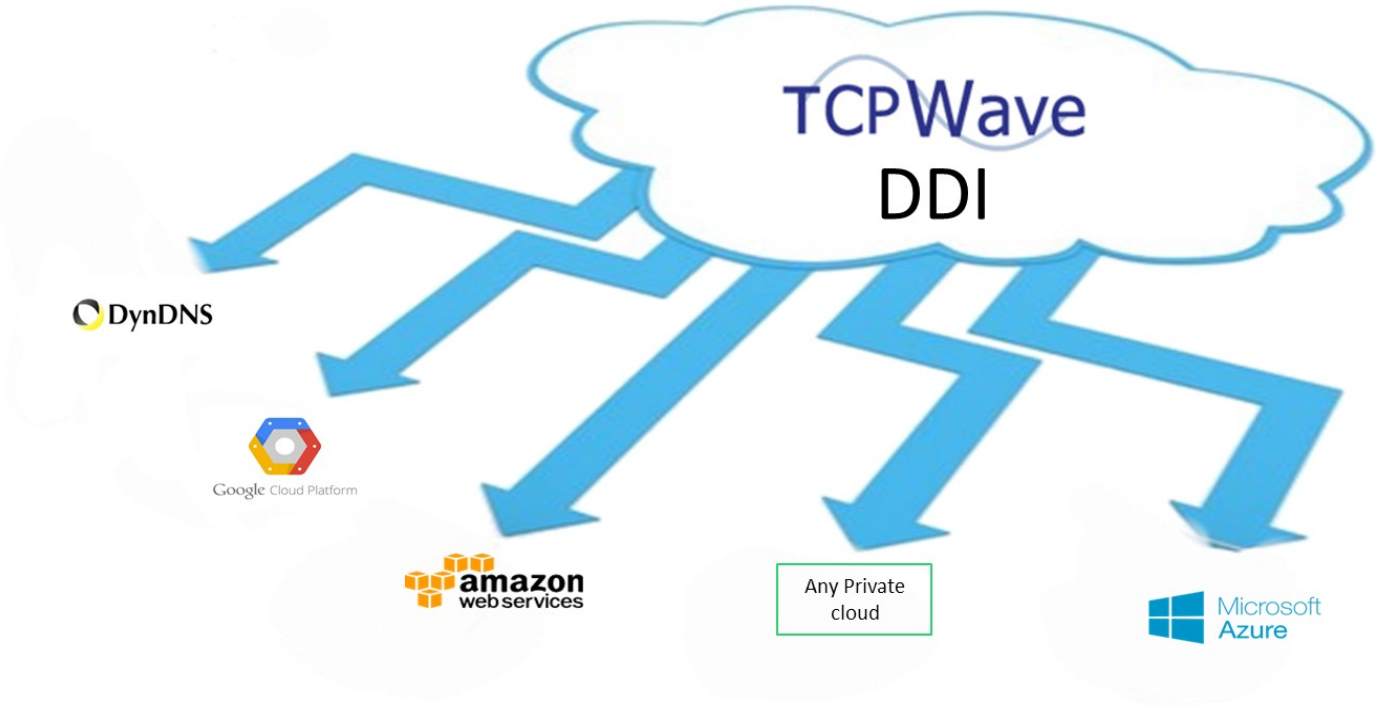
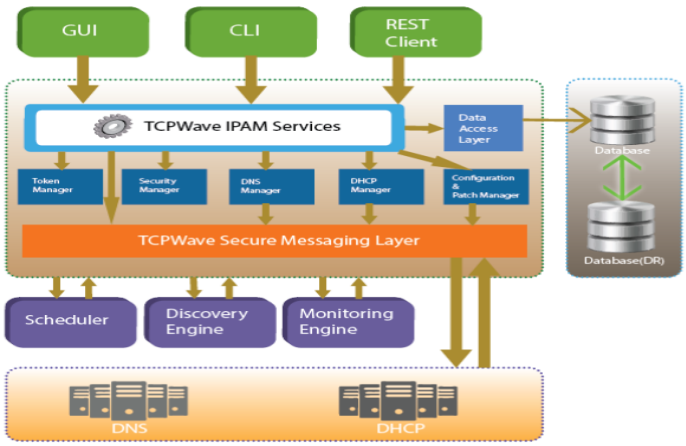
# Built in the cloud
# To manage the cloud



## The TCPWave IPAM Solution

TCPWave's IP Address Management software for DNS, DHCP and IP Address Management (DDI) includes a full featured and integrable IPAM solution that helps network administrators eliminate network conflicts and outages, track critical assets, ensure network security and providing reports based on a wide range of parameters, including IP address status (dynamic, static, available, reserved, etc.), networks, subnets, and admin activities. TCPWave IP Address Management allows the Network Personnel to automate the process of allocating and de-allocating IP address resources. This automation is both efficient and intelligent. The IPAM can dynamically manage the available address space by complying with the Organization's IP Address and Security policies. TCPWave's IPAM provides an intuitive Graphical Web User Interface for managing DNS, DHCP, IP Network as well as all related services. TCPWave DDI can manage multiple external DNS hosting services, manage TCPWave DNS in the cloud as well as multiple DNS vendors to minimize a myriad of DNS attacks. Older DDI providers have numerous product deficiencies, which cause issues as enterprises scale and newer technologies rely more on advanced fundamental DNS and DHCP protocols. The architecture and design of the TCPWave DDI is built using state of the art technology.




## Fully published interfaces

TCPWave has a fully published **REST** API. The REST API can be used to communicate with all external REST interfaces. TCPWave provides Pre-configured REST communication with all of the most popular public and private cloud providers allowing customers to stay focused on network obligations. TCPWave's RESTful API comes with extensive documentation and examples.

For legacy communication TCPWave provides a robust command Line Interface (**CLI )** .

**VMware plugin** is available if a customer needs to communicate with VMware Orchestrator.

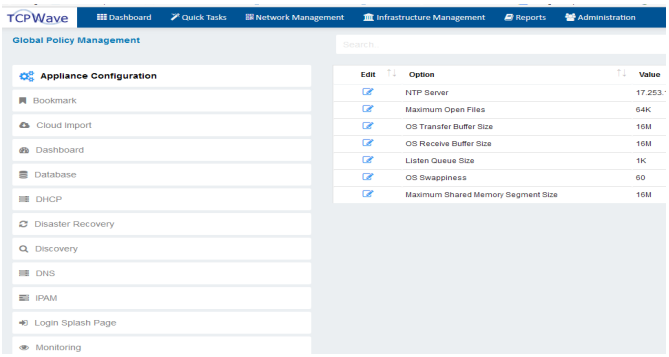
**VMware Discovery** enables discovery of the virtual instances in the Vmware Infrastructure. The discovered objects can then be added to the desired subnets in TCPWave.

## Built With The Latest Technology

TCPWave's IPAM is built from scratch using the latest technologies including robust jQuery framework and Java. One of the primary benefits of TCPWave's IPAM is the ability to handle cross browser issues seamlessly. TCPWave's IPAM has been engineered to work with all browsers and all smart phones and tablets. TCPWave's IPAM, built using the latest Java technology is much faster and can seamlessly integrate into the existing automation via RESTful API calls.

## Simplified Dashboard

TCPWave's IPAM provides fault management, performance management, config assurance, patch management and IPAM software in one bundle. There is no need to purchase monitoring software to manage your DNS Infrastructure. TCPWave's IPAM integrates with customer provided EMC SMARTS and automatically sends SNMP alerts when critical events arise in IPAM operation. Scheduled changes can be managed more efficiently and roll backs take place automatically if the change implementation fails. TCPWave also provides a powerful dashboard to monitor all the core components of the DDI infrastructure managed by the TCPWave IPAM with extensive graphing capabilities for performance management metrics. TCPWave's DNS and DHCP appliances are automatically added to the fault and performance monitoring.




## Auto Discovery

Auto Discovery is designed for organizations with complex and dynamic network infrastructure. It automatically discovers your network topology and updates itself when new subnets are discovered on the network. The networks and subnets can be configured to be scanned periodically to detect the changes in the network nodes and then update the objects data. It can discover all the network devices and their configuration via ICMP, SNMP and NetBIOS protocols and consolidate the newly collected data with the existing data.

## Switch Port Discovery

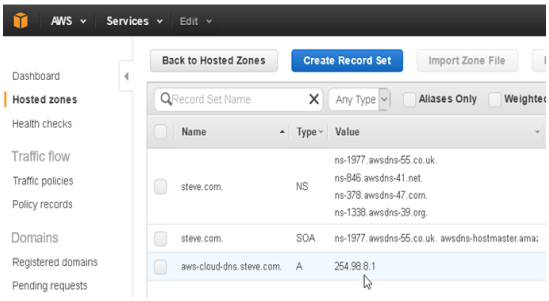
Switch Port Discovery Is designed to discover switches in a given subnet and the devices connected to those switches. As part of the discovery, the vlan and port details will also be discovered. IP Address, Mac Address, Switch Name, Port Name and Port Duplex will be collected for each device. These devices can then be added to TCPWave IPAM subnets.

## Cloud Discovery

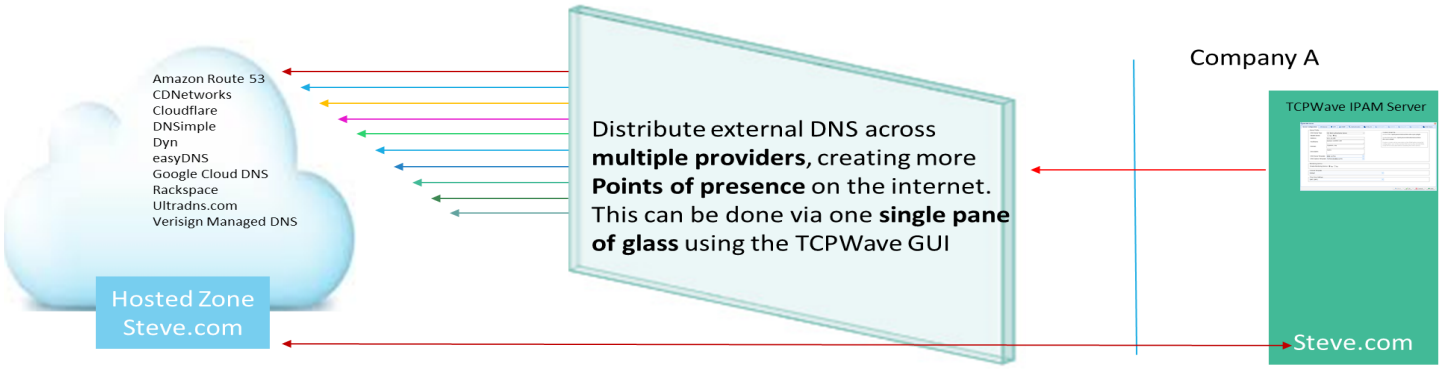
TCPWave can fully discover subnets, objects and DNS resource records and then update the TCPWave DDI system.

## Unsurpassed Cloud management

TCPWave has pre-configured it's Rest interface to communicate with most of the top cloud providers and is easily configured for any private cloud. IPAM can host zones in multiple cloud providers or run the TCPWave DNS server in the cloud. The ability to start up many more DNS servers by cloning in the TCPWave GUI or manage and update zones in cloud providers with many points of entry around the world is necessary to withstand the intensity of todays malicious DDOS attacks.




DNS Zones hosted in Multiple providers in the Cloud – Managed by TCPWave in a single pane of glass allows dynamic increase and decrease of DNS band-with without major OpEx purchases of DNS servers that mostly sit idle.

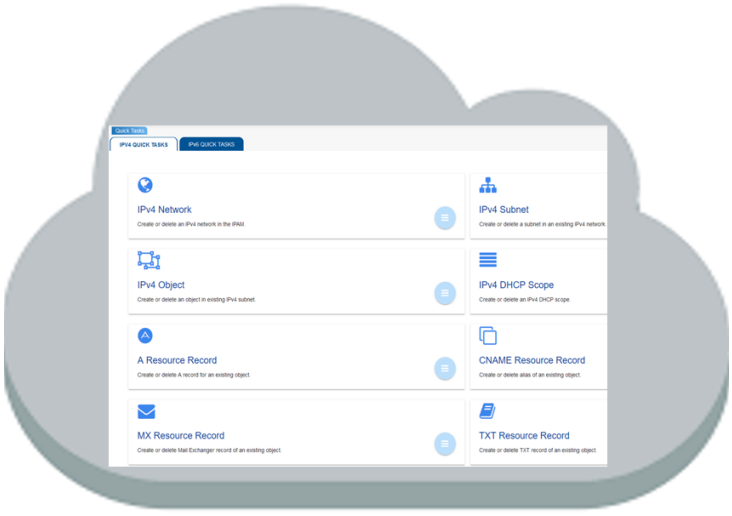



Clone X number of TCPWave DNS Slaves Using the TCPWave GUI when extended bandwidth is needed.


## Simple DDI managed in the cloud

A} TCPWave DDI Managed Service in the Cloud

B} TCPWave DDI running in the cloud managed by customer staff




## External DNS Diversification

External DNS diversification is **mandatory** in todays net-works. Whether it is multiple DNS cloud hosting or dual DNS servers running different code. TCPWave can mange all of this in a single pane of glass.

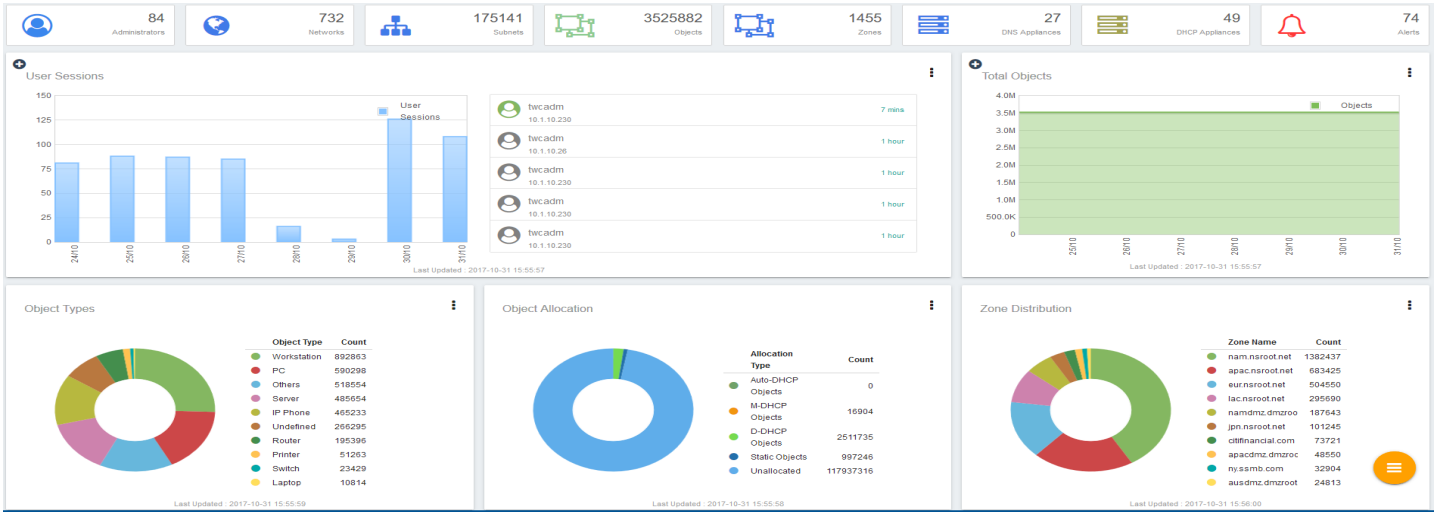

## Terraform Cloud Workflow Integration

Automated DDI workflow from customers internal applications to customers cloud instances while updating TCPWave.

- Add, Modify and Delete subnets and objects
- Create VPC with custom DHCP Options Set
- Create VPC with next available IP block with given mask
- Create VPC with given IP block
- Create next available Subnet in AWS in given VPC

## Network and Health Management

TCPWave's IPAM enforces strict database integrity checks. Its smart logic checks the sanity of the DNS and DHCP configuration files before sending them to the remote DNS and DHCP devices. This ensures that the remote devices do not crash after getting an update from DDI. Thus it eliminates manual DNS and DHCP updates. DNS updates take place in real time and DHCP configurations are updated automatically when new scopes are defined. Powerful metrics used by the dashboard assist in identifying bottlenecks in the network.




## IPv4 and IPv6 Support

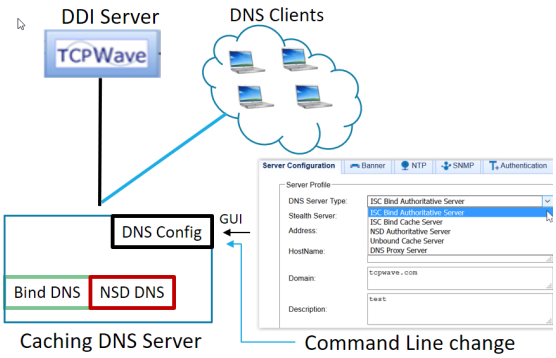
TCPWave's IPAM solution supports both IPv4 and IPv6 out of the box. No additional license is needed for IPv6.

## DNSSEC

The DNSSEC rich set of features include automatic key generation, zone signing, and scheduled DNSSEC key rollover.

## Dual DNS

When the primary BIND DNS becomes compromised, the monitoring service alerts the administrator who can shut down the BIND DNS and bring up the Unbound DNS for Caching or the NSD DNS for Authoritative.




## Segregation of Duties

Segregation of Duties are Control Activities that reduce the risk of error and malicious DNS/DHCP activities or human errors, through proper division of tasks between employees. As DNS and DHCP relate to the core functionality of mission critical network services, it is the proper Segregation of Duties in the TCPWave IPAM that prevents the potential for *employee circumvention of controls*. Using the TCPWave IPAM, User Administrators can only create user accounts and cannot alter DNS/DHCP data. Power and Normal accounts can alter DNS/DHCP data but they cannot define user accounts. All the user actions are audited. The various types of administrators and their descriptions listed below:

- FADM – Functional Admin, All functionality
- UADM – User Admin, Has access to user administration functionality only
- SADM – Super Admin, Access to all functionality with in the organization, except User administration
- PADM – Power Admin, Has access to Zone/Domain/Server/ Network/Subnet/Scope /Template/Object
- NADM – Normal Admin, Manage permitted network resources within the organization
- RADM – Read-only Admin , Read only access to the resources within the organization

## High Availability and Scalability

TCPWave's IPAM is a highly scalable and reliable IP address management solution. It ensures strict database and configuration integrity checks. The solution is built with high availability and disaster recovery management to ensure the continuity of business critical services. In case of catastrophic failure scenarios, a secondary server automatically takes over the primary server's role without interrupting the enterprise network.

## Information Security

TCPWave's IPAM supports TACACS+, Active Directory, Radius, PAM, and Single Sign On authentication mechanisms. TCPWave's appliances have passed the most stringent ethical hacking and penetration tests where our competition failed. When BIND exploits take place, TCPWave's IPAM protects your mission critical DNS infrastructure because it provides a non-BIND solution in addition to BIND to fend off DNS exploits.


TCPWave's IPAM offering is an innovative security-as-a-service bundled product that delivers core network infrastructure solutions that help organizations protect their mission critical networks from DNS attacks and enable them to effectively meet the complex and evolving regulatory compliance and data governance mandates that have been spawned from highly publicized data breaches. TCPWave, a best in class appliance provider, is delivering an integrated suite of on-demand data protection solutions spanning DNS threat management, regulatory compliance, data governance and secure B2B communications—all of which are based on a common security-as-a-service platform. Simply put, our solutions help organizations to:

- Keep DNS DDOS attacks out of their environments.
- Prevent the theft or inadvertent loss of sensitive information.
- Collect, securely retain, govern and discover sensitive data for compliance and litigation support.
- Securely communicate and collaborate on sensitive data

Traditional DNS is vulnerable to multiple security exploits. Managing DNS with DNSSEC or GSS-TSIG has many operational overheads. Sending DNS updates using UDP port 53 has been proven as an insecure way to operate the mission critical DNS infrastructure. TCPWave has designed a revolutionary **method of securing dynamic changes using a robust security model**. Changes made in the IP Address Management web interface are sent using a secure conduit from the management server to the remote DNS server. A powerful logic developed in Java examines the contents of the update, determines the authenticity of the source IP Address, and verifies if the IPAM server sent the message and then processes the message. After updating the master DNS, the secure conduit service sends an acknowledgement back to the management server. If the acknowledgement is not received, the management server sends a retry. This communication uses a TCP port with a 1024 bit encryption key.

## Certified IPAM drivers

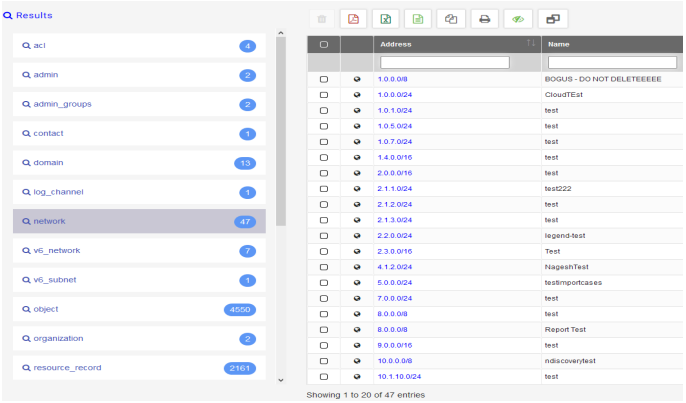
Available for customer provided **EMC Smarts, Infovista, Alterpoint** and **HPNA.** Integration with **HP Arcsight (SIEM)** for allter security logs.

## Audit and Traceability

TCPWave's IPAM comes with an extensive audit capability, which provides accurate forensics for IP Audit, subnet audit, network audit, domain audit etc. You can customize the auditing policies to audit what the Security team is interested in for better audit reviewing. The Login audit enables detection of unauthorized intrusions in to the system. A combination of failure and success authentication audits help determine when the breach of security occurred. Isolation and preservation of the security event log helps track users who gained unauthorized admin privileges.

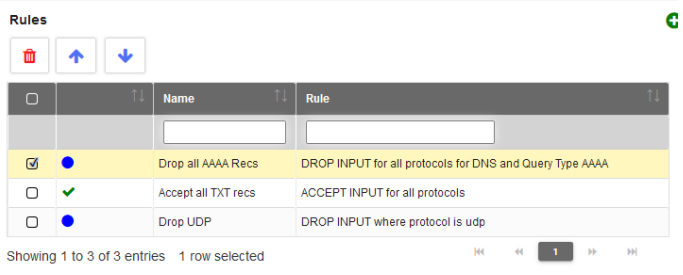

## Search Engine

TCPWave's IPAM solution provides a powerful search engine. It can be used to search literally anything in the IPAM constellation.




## Dynamic DNS firewall

Robust firewall managed directly from the GUI



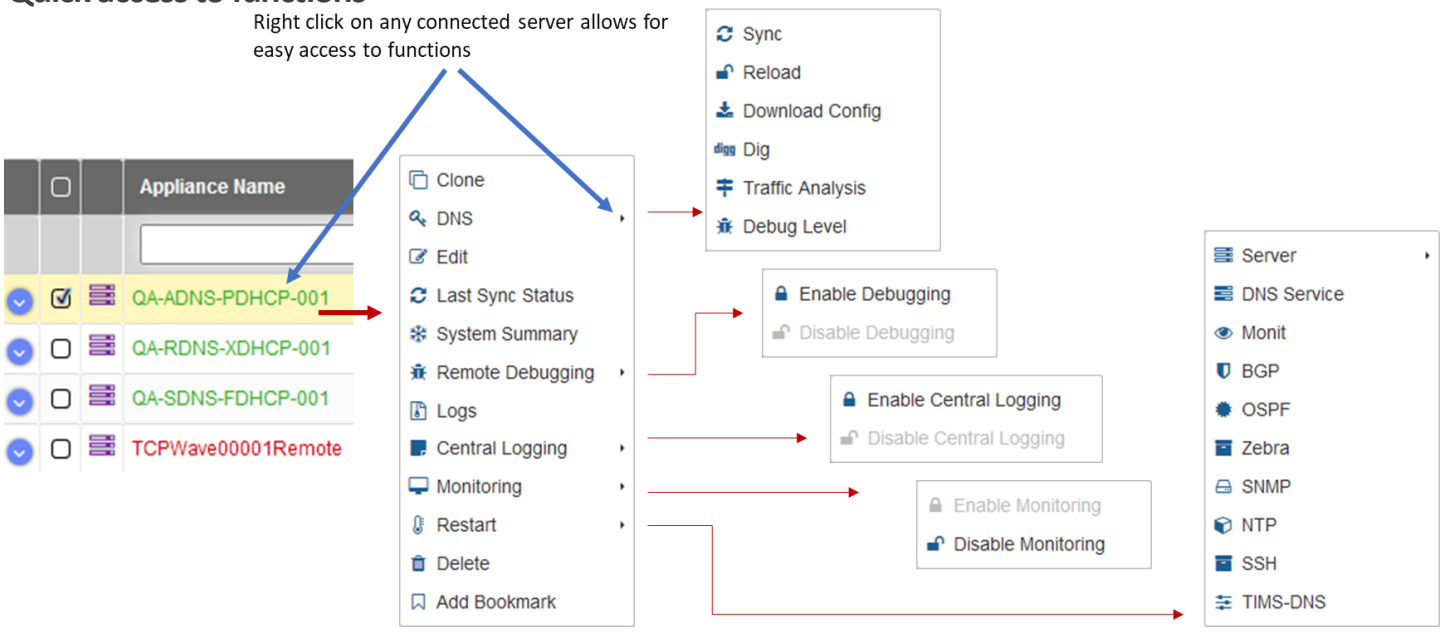

## ServiceNow integration

TCPWave Integrates ServiceNow trouble tickets with TCPWave DDI modifications performed by administrators. All modifications are audited by trouble ticket number. Easily undo all or some modifications by trouble ticket number. Easily search for any modifications made using a particular trouble ticket. A global policy can be used to make trouble ticket mandatory for all modifications.

## Robust Reporting

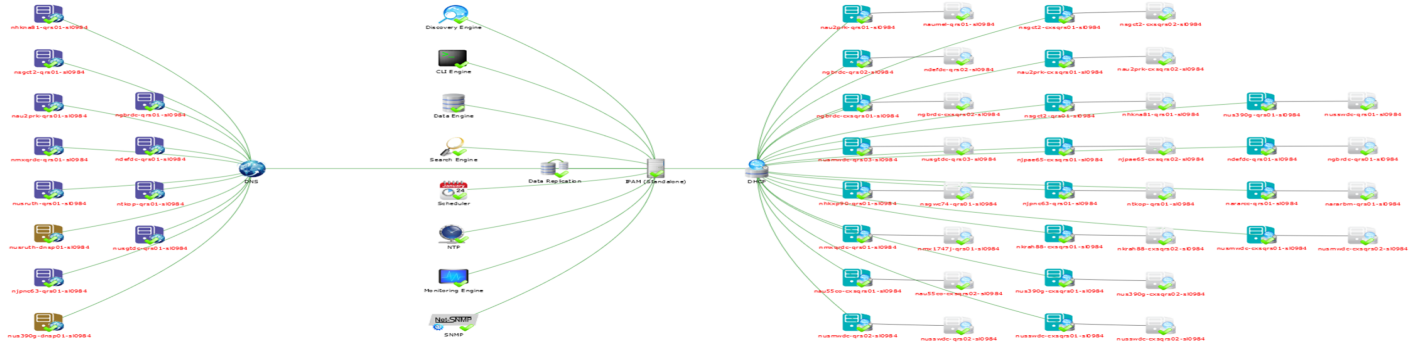

## Quick access to functions

Right click on any connected server allows for easy access to functions




## DDI Topology

Topology of all DNS, DHCP, IPAM servers and important services. If a server or service is down the name will be red, If up it will be green.



## TCPWave State of the Art Offered platforms

| | |
|---|---|
| TCPWave **DDI** Cloud offering | TCPWave DDI Management |
| TCPWave **DDI** Cloud offering hosted by a provider | TCPWave DDI |

## TCPWave Legacy Offered platforms

| | |
|---|---|
| TCPWave **DDI** purpose built Dell appliance | DELL |
| TCPWave D**DI** running on Customer provided HW | DELL, hp, IBM, Sun ORACLE, VitalQIP |
| TCPWave **DDI** running Virtually | vmware, KVM |


Contact Sales at TCPWave.com

TCPWave
World Headquarters
600 Alexander Road
Princeton, NJ – 08540