TCPWave IP Address Management System®

Release Notes

Version 11.33P1

February 2023

TCPWave

TCPWave® Inc
600 Alexander Road
Princeton, NJ 08540
USA
Phone: 888-831-8276
Email: support@tcpwave.com
Website: www.tcpwave.com

Table of Contents

Introduction

These release notes summarize the new features, improvements, and stability fixes included in the TCPWave DDI v11.33P1 release. In this release. TCPWave has introduced support for the following significant features:

- Application Delivery Controller (ADC) management solution ensures the availability of business-critical enterprise applications and global server load balancing across diverse environments with minimum network latency and downtime. Additionally, it provides continuous security for applications and infrastructure against web attacks and other key threats.
- Kea DHCP is the next generation of IPv4/IPv6 DHCP servers from the Internet Systems Consortium (ISC). Kea DHCP offers a newer extensible modular design with advanced features such as a dynamically loaded Hooks Module, support for Dynamic DNS, reconfiguration via REST, and many more features.

  Note: Customers are encouraged to begin testing and rolling out Kea in their own environments since Kea replaces the older ISC DHCP.

Customers will need to have new licenses for v11.33P1. Please contact TCPWave Support to request new licenses prior to installing or upgrading to v11.33P1.

Feature Requests/Enhancements

Application Delivery Controller (ADC) Management

TW-FR-953: ADC Management

TCPWave's Application Delivery Controller (ADC) management comprises three major components - GSLB (Global Server Load Balancer), SLB (Server Load Balancer), and WAF (Web Application Firewall). TCPWave's GSLB technology provides intelligent DNS responses based on the configured GSLB Traffic Rule types, such as Extension Attributes, Geolocations, Subnet, and default rules. TCPWave's SLB technology provides load balancing and high availability services to TCP and HTTP-based applications. SLB is placed between the client and the backend pool of servers. When operating in TCP mode, it provides layer 4 load balancing. In HTTP mode, it provides layer 7 load balancing. Clients send their requests to the virtual IP address of a frontend server. The frontend server then distributes the incoming traffic to the set backend pool to prevent any single server from overloading. In the event of any server failure, the other servers handle the traffic. WAF provides a highly scalable security solution by analyzing incoming HTTP traffic and blocks key threats such as SQL injections, Cross-site scripting (XSS), Sensitive data exposure, etc.

Added ADC Management menu link under the Network Management section, which has the following

sub-menu links:

- **ADC Appliances**: These appliances are managed by the TCPWave IPAM. GSLB services are run on ADC appliances that provide intelligent DNS responses based on configured GSLB rules.
- **GSLB Rule Set**: Using this section, you can configure the GSLB rules based on the extension attribute, geolocation, subnet, or default rules.
- **SLB Configurations**: Using this section, you can configure frontend(s) that defines how requests are forwarded to backend/backend pools.
- **SLB Overview**: This interface provides a complete visualization of how the ADC appliances are connected in a single pane of glass.
- **SLB Response Page**: This interface provides the HTTP response status code based on the request.
- **SLB Rule Set**: You can configure rules to route requests to the desired backend using this section.
- **SLB Templates**: You can configure the process level parameters and other parameters and associate them with ADC appliances.

TCPWave's ADC management solution also integrates into Fault Management, Performance Management, Configuration Assurance. Added ADC Version Matrix and ADC Settings Matrix in the Configuration Assurance section.

Navigation:

Network Management >> ADC Management

Infrastructure Management >> Configuration Assurance >> ADC Version Matrix, ADC Settings Matrix

Infrastructure Management >> Configuration Assurance >> IPv4 Policy Compliance >> ADC Policy Compliance

Infrastructure Management >> Performance Management >> TCPWave SLB Statistics

ISC Kea DHCP

TW-FR-76: Provide ISC Kea Support for DHCP

Integrated ISC Kea DHCP 2.2.0 version with TCPWave IPAM with the following enhancements:

- Add, edit, and delete operation of Kea DHCP appliances.
- Associating the Kea DHCP appliance with the subnets.
- Creation and deletion of scopes and DHCP manual objects.
- Auto DHCP incremental updates, full synchronization, and full pull from remote with acknowledgment status messages.
- Auto lease updates to IPAM and publishes auto DDNS adds and deletes for lease objects.
- Ability to view and sync active leases on appliances and subnet level.

- Support the configuration assurance checks, monitoring alerts, version matrix checks, and system summary analysis.

IPv6 Functionality

TW-FR-977: IPv6 Reverse Zones Modifications

Enhanced the IPv6 functionality to support various functionalities in the IPv6 Reverse Zone page:

- **Auto Force Sync**: Performing auto force sync operation on objects, object RRs, zone RRs, reverse zone RRs, IPv6 objects, IPv6 object RRs, place holder objects import sends DDNS updates to all the bulk records.
- **Exclude From Sync**: This feature excludes the zone from DNS full sync, and zone force sync operation fails.
- **DNSSEC**: Using this interface, you can view all the DNSSEC keys, ZSK (Zone Signing Key), and KSK (Key Signing Key) of all the IPAM managed zones in the order of zone name.
- **Monitoring**: This feature allows you to check various monitoring services such as Zone KSK expiry, zone configuration, etc.
- **Force Sync**: This feature updates the zone file on the managed remotes with the data available in the IPAM and reloads the zone.
- **Freeze**: This feature suspends dynamic updates of the selected reverse zones. The system prevents you from performing freeze operations if no zone template is associated.
- **Thaw**: DNS sync resets the frozen status of a given reverse zone back to a thawed state.
- **Zone Status**: This feature allows you to view the status of the selected zone, which also provides information about monitoring, active directory, and restricted zone.
- **Support for PTR & NS Resource Records**: Extended the IPv6 functionality for reverse DNS lookups and NS records.
- **Incremental Updates**: This feature supports incremental zone transfer (IXFR).

Threat Intelligence

TW-FR-968: Entropy Value in Anomaly Detection

Added a new number field Entropy as part of anomaly detection. It is a statistical parameter that measures the amount of information produced on average for each letter of a DNS query.

Navigation: Network Management >> DNS Management >> DNS Security >> DNS Threat Management >> Network Security Monitoring (NSM) template >> Add/Edit >> NSM Configuration >> Enable Anomaly Detection >> Entropy

TW-FR-960: Atlantis Model for DNS Over HTTPS (DoH) queries

Atlantis - A deep learning model integrated with TCPWave's Network Security Monitoring (NSM)

template safeguards the DNS appliances from attacks such as the DGA, DNS Tunnelling, etc. Previously, this model is used to sniff the HTTP packets. Now, the model is enhanced to sniff the DoH packets using a newly added field - Enable DoH.

Note: Enabling DoH requires high CPU usage and impacts the appliance's performance.

Navigation: Network Management >> DNS Management >> DNS Security >> DNS Threat Management >> Network Security Monitoring (NSM) template >> Add/Edit >> Enable Anomaly Detection >> Enable DoH

TW-FR-891: Advanced Threat Intelligence Dashboard

Added **Advanced Threat Intelligence** dashboard in the Dashboard menu link. It includes the count of Queries Per Second (QPS), Anomalies Per Second, Remotes, and Alerts in the form of counters and has the following widgets:

- Top QPS & APS data
- Anomalous Source Geo Map
- DGA Pie Chart
- Outliers Grid
- Anomalous Query Distribution Suricata
- Intrusion Alerts Suricata
- Top 10 Forward Zones

Added a new schedule job **ATISDashboardScheduler** which executes every 30 minutes and stores the data related to the above-mentioned widgets and counters in the database. Whenever the rest call operations are performed, the system retrieves the information from the database and projects it on the respective dashboard widgets.

Navigation: Dashboard >> dropdown >> Advanced Threat Intelligence

Discovery

TW-FR-952: Discovery Dashboard

Added Discovery dashboard in the Dashboard section. It is a central repository to monitor ongoing discovery operations. It includes the count of the Routers, Switches, Firewalls, Router Subnets, Switch Subnets, and Subnet Mismatches represented in the form of counters and has the following widgets:

- Distribution by Device
- Distribution by Vendor
- Top 10 Switch Port Traffic Utilization
- Top and Least Busiest Poller
- Top 10 Devices Uptime

- Discovered Devices Details
- Distribution by OS Version
- Discovery Logs

Navigation: Dashboard >> dropdown >> Discovery

Information Security Upgrades

TW-FR-845: ISC DHCP, NSD & UNBOUND Updates

Upgraded **ISC DHCP** from v4.4.2 to v 4.4.3P1. The latest version includes two bug fixes which are listed below:

- Corrected a reference count leak when the server builds responses to leasequery packets.
- Corrected a memory leak when unpacking a packet with an FQDN option (81) containing a label with a length greater than 63 bytes.

Upgraded **NSD** from v4.5.0 to v 4.6.1. The latest version includes two bug fixes which are listed below:

- The Application-Layer Protocol Negotiation (alpn) is set for DOT connections.
- The Service Binding (SVCB) type supports the dohpath parameter.

Upgraded **UNBOUND** from v1.16.0 to v1.17.0. The latest version includes various bug fixes, of which a few are listed below:

- Fixed ratelimit inconsistency.
- Fixed proxy length debug output printout typecasts.

TW-FR-867/SR-934: BIND Updates

Upgraded **BIND** from v9.16.30 to v9.18.9. The latest version includes feature changes and bug fixes, of which a few are listed below:

- The NXDOMAIN records are no longer retained past the standard negative cache TTL, even if the stale-cache-enable option is set to yes. This is to ensure there is a reduction in unnecessary memory consumption.
- The coresize, datasize, files, and stacksize options have been deprecated.
- The number of HTTP headers allowed in requests sent to the named's statistics channel has increased from 10 to 100, accommodating some browsers that send more than ten headers by default.
- The issue of the named could crash due to an assertion failure when an HTTP connection to the statistics channel was closed prematurely has been fixed.

TW-FR-892: MariaDB upgrade to version 10.6.10

Upgraded MariaDB version from v10.2.44 to v10.6.10. The latest version of MariaDB includes changelogs and bug fixes; a few of the bug fixes are listed below:

- Recovery or backup of instant ALTER TABLE is incorrect.
- Full-text index corruption if shutdown before changes is fully flushed.
- JSON_VALUE () does not parse NULL properties properly.

TW-CR-5252: Suricata upgrade to version 6.0.8

Upgraded Suricata version from v6.0.4 to v6.0.8. The latest version of Suricata includes significant features and default settings; a few of the features and default settings are listed below:

- New protocols mqtt rfb are enabled by default.
- SSH client fingerprinting for SSH clients.
- Initial support of HTTP/2.
- FTP is updated with a maximum command request and response line length of 4096 bytes.

TW-CR-5253: Zeek upgrade to version 5.1.1

Upgraded Zeek version from v4.0.0 to v5.1.1. The latest version includes minor bug fixes, of which a few are listed:

- Fixed a potential stall in Broker's internal data pipeline.
- An IPv6 packet can cause Zeek to overflow memory and potentially crash. Due to the possibility of receiving these packets from remote hosts, this is a DoS risk. The fix included is better length checking and reporting a weird for violations.

TW-FR-978: Jetty Upgrade to 10.0.11

Upgraded Jetty version from v9.4.44 to v10.0.11. The latest version includes significant modifications, of which a few are listed:

- A new API for managing Configuration within a WebAppContext.
- Replaced Classic jetty logging facade with slf4j-api usage.
- Usage of jetty-home with a proper ${jetty.base}.
- Replaced old base functionality with demo jetty-start module.
- Removed jetty-all uber artifact.
- Support for WebSocket over HTTP/2 (client and server).
- Improvised Jetty HttpClient.
- Supports dynamic protocol upgrades (http/2 and http/1.1).
- Refactored session management.

Note: The minimum required Java version for Jetty 10 is now Java 11.

TW-FR-979: timsscheduler upgrade

Upgraded the embed-jetty-related jar files and backend logic as part of the timsscheduler project.

TW-FR-989: Open SSL updates

Upgraded Open SSL from v1.1.1p to v1.1.1t. The latest version has major CVE fixes, of which a few are listed below:

- Fixed timing Oracle in RSA Decryption
- Fixed Use-after-free following BIO_new_NDEF

TW-FR-992: Open SSH Updates

Upgraded Open SSH to v9.2.0.

Network Management

TW-FR-571: Improvise format for renamed DHCP Objects

Added a new global option **DHCP Duplicate Client Name Delimiter,** which has the following dropdown values:

- IP String
- User Defined

IP String configures the system to use the string that adds the leading zeros to the octets of the IP address.

User Defined configures the system to use the defined delimiter to concatenate the octets of the IP address. The obtained constructed string is used as the prefix for the duplicate DHCP hostnames.

Navigation: Administration >> Global Policy Management >> DHCP >> DHCP Duplicate Client Name Delimiter

TW-FR-691/FR-685: Ability to map A record's IP address to the corresponding object in IPAM

Added View All Resource Records check box in the Resource Records tab of the Managed DNS Zones section. On selecting the checkbox, the system displays all the zone-level RRs, object-level RRs, Domain Controller RRs, and NS RRs. If the checkbox is unchecked, the system displays the zone-level RRs.

Navigation: Network Management >> DNS Management >> DNS Zones >> Managed DNS Zones >> Edit Managed DNS Zone >> Resource Records tab >> Resource Records grid >> View All Resource Records checkbox

TW-FR-717: Allow domain NS records to be entered directly in the Zone Resource records

Previously, the system prevented you from adding a domain at zone level NS resource record. Now, the functionality is modified to allow the domain at the zone-level NS resource record.

Navigation: Network Management >> DNS Management >> DNS Zones >> Managed DNS Zones >> Edit Managed DNS Zone >> Resource Records tab >> Resource Record Type >> NS Record >> Owner Name >> Domain

TW-FR-775: Ability to override DHCP Options at the Subnet profile - To include all common options to a template & just different options at the Subnet profile.

Added a new tab DHCP IPv4 option in the IPv4 Subnets properties page that displays all the DHCP IPv4

options. This provides an ability to override the DHCP options at the subnet level.

Navigation: Network Management >> IPv4 Network Address Space >> IPv4 Networks >> IPv4 Subnets >> DHCP IPv4 Options

TW-FR-804/CR-5369: Defining SOA when a primary nameserver is configured as stealth

Added MNAME field in the DNS Zone Templates page. By default, the system has the selected primary master as the drop-down value. Additionally, it contains all the selected slaves of the corresponding master(s), which is/are configured as a stealth appliance. You can select one of the slaves FQDN values for the SOA generation or select Default to the selected master appliance option from the drop-down.

Navigation: Network Management >> DNS Management >> DNS Zones >> Managed DNS Zones >> Add/Edit/Clone >> SOA Attributes >> MNAME

TW-FR-806 Ability to use a non-standard port for SSH

Previously, the default port for SSH client connections was 22. Now, the functionality is enhanced, and you can change the default port. Added a Port field under the SSH Port settings that allows you to enter a default port number and values between 1024 and 32,767.

Navigation:

Network Management >> IPAM Management >> IPv4 IPAM Appliances >> PAM Settings >> SSH Port Settings >> Port

Network Management >> DNS Management >> DNS Appliances >> TCPWave DNS IPv4 Appliances >> PAM Settings >> SSH Port Settings >> Port

Network Management >> DHCP Management >> TCPWave DHCP IPv4 Appliances >> PAM Settings >> SSH Port Settings >> Port

TW-FR-822: Ability to flush cache on multiple DNS appliances

Enhanced Flush functionality allows you to delete the cached data of a particular zone or record from multiple appliances with recursion enabled. The flush operations are applicable for BIND Auth + BIND Cache & UNBOUND combinations.

Navigation: Network Management >> DNS Management >> DNS Appliances >> TCPWave DNS IPv4 Appliances >> Content Menu >> Flush

TW-FR-835: Option to select DNS master (name, domain, and interface) in case the DNS remote has multiple interfaces

Added a DNS Interface tab that allows you to add the DNS interface and listen-on interfaces for the DNS process. By default, DNS listens on all the interfaces defined on the remote, and the management interface name and IP are used in the zone file generation.

Navigation: Network Management >> DNS Management >> DNS Appliances >> TCPWave DNS IPv4 Appliances >> Edit >> DNS Interface

TW-FR-849: Null DHCP hostnames are keeping the placeholder names and are not renamed by the IPAM

Added **DHCP Empty Client Hostname Appender** global option in Global Policy Management. This option generates an object name pattern based on the following drop-down values when a client hostname has an empty value.

- Placeholder
- MAC address

On selecting the placeholder value, the system uses the existing hostname as the object name. On selecting the MAC address, the system uses the combination of the string and MAC address of the object as the hostname.

Navigation: Administration >> Configuration Management >> Global Policy Management >> DHCP >> DHCP Empty Client Hostname Appender

TW-FR-857: Add an option to import whitelisted and blacklisted domains into the NSM template

Previously, you could add only one whitelisted or one blacklisted domain in the Network Security Monitoring Template section. Now the functionality is enhanced to import multiple whitelisted and blacklisted domains in the NSM template.

Navigation: Network Management >> DNS Management >> DNS Security >> DNS Threat Management >> NSM Template >> Add/Edit >> Whitelisted & Blacklisted Domains >> Import >> Select file

TW-FR-871: TCPWave DNS Application logs (All relevant logs) should have all necessary logs logged by default (Without enabling debugging)

Irrespective of the global option **Enable Debug Log Level** is set to Yes/No. By default, the system logs all the critical logs as informational logs.

TW-FR-888: Increase the max value of 'High water mark to purge older entries in object history table' from 200,000 to 4,000,000

Previously, the maximum value of the global option High watermark to purge older entries in the object history table was 200,000. Now, the value is increased to 4,000,000.

Previously, the maximum value of the global option High watermark to purge older entries in the audit history table was 1,000,000. Now, the value has increased to 4,000,000.

Note: Any value above 200,000 requires at least 128 GB Memory and 4 GB heap size.

Navigation: Administration >> Configuration Management >> Global Policy Management >> IPAM

TW-FR-894 Ability to have subnets in more than one subnet group

Previously, one subnet was associated with one subnet group. Now, the functionality is enhanced to have one subnet associated with multiple subnet groups. Added multi-select subnet group drop-down field in the Subnets and Subnet Template sections.

Navigation:

IPv4 Address Space >> IPv4 Networks >> IPv4 Subnets >> Add/Edit >>Subnet Group dropdown

IPv4 Address Space >> IPv4 Subnet Templates >> Add/Edit >> Subnet Group dropdown

TW-FR-904: Support for DNS over HTTPS (DoH)

Added support for DNS over HTTPS (DoH) functionality with which the encryption is provided between the DNS client and server. It ensures that the malicious actors cannot alter the DNS traffic.

Navigation: Network Management >> DNS Management >> DNS Appliances >> TCPWave DNS IPv4 Appliances >> Enable DoH

TW-FR-935: Exclude zones from DNS full sync and zone force sync & support for disabling auto force sync of a zone when bulk operations done

Added Auto Force Sync and Exclude from Sync sub-menu options in the Administration context menu option with Boolean data values as Yes or No for each option.

Exclude From Sync Functionality

- On setting the option to Yes, the system excludes the zone from DNS full sync, and zone force sync fails. Performing auto force sync operations on objects, object RRs, zone RRs, reverse zone RRs, IPv6 objects, IPv6 object RRs, place holder objects import sends DDNS updates to all the bulk records instead of zone force sync operation.
- On setting the option to No, you can perform full sync and zone force from the GUI. Whenever a network and a subnet are deleted, the system fails to perform zone force sync operation. You must manually perform the zone force sync option by disabling the Exclude From Sync operation.

Auto Force Sync Functionality

On setting the option to No, all the bulk operations like objects, object RRs, zone RRs, reverse zone RRs, IPv6 objects, IPv6 object RRs, and place holder objects imports send DDNS updates for all the bulk records instead of zone force sync.

Navigation:

Managed DNS Zones >> Right-click Zone >> Administration >> Auto Force Sync and Exclude From Sync

Managed DNS IPv4 Reverse Zones >> Right-click Zone >> Administration >> Auto Force Sync and Exclude From Sync

Managed DNS IPv6 Reverse Zones >> Right-click Zone >> Administration >> Auto Force Sync and Exclude From Sync

TW-FR-939: Ability to control and specify the "forwarders" on a per DNS view basis

Previously, the forward and forwarders options at the DNS Option Template level were applied to all the views and zones in the appliance. Now, the functionality is modified to override the forward, and forwarders options at the view level and hence added two new drop-down fields, **Forward** and **Forwarders,** in the DNS Views add and edit pages.

The forward field has two values: **Only** and **First**. If you select **Only**, the server is responsible for forwarding queries. If you select **First** which is a default value, it sends the queries to the forwarder, and if not answered, it attempts to answer the query. In the Forwarders field, you can define a list of IP address(es) and optional port numbers to which queries are forwarded.

Navigation: Network Management >> DNS Management >> DNS Zones >> DNS Views >> Add/Edit >> Forward & Forwarders

TW-FR-958: CLI's for Zone Sync Exclude and Auto force sync

Added the following CLIs for Auto Force Sync and Exclude From Sync features:

- setzoneexcludesync
- setzoneautoforcesync

TW-FR-980: Network Hierarchy

Enhanced the network hierarchy topology diagram. Using this interface, you can manage network hierarchy in an organization. The network space is organized as a hierarchy of network blocks. You can perform various operations such as adding address space, adding blocks, etc., using the icons or from the context menu options at each level in the hierarchy. By default, the system displays a maximum of five address blocks based on the global organization selection.

Navigation: Network Management >> Network Hierarchy >> Overview

TW-FR-989: Add a progress indicator for DNS/DHCP sync operations

Added Progress Indicator for DNS & DHCP sync operations that allow you to view the status of the actions, such as initialization of sync operation, generation of the config file, and full sync status.

Navigation:

Network Management >> DNS Management >> DNS Appliances >> TCPWave DNS IPv4 Appliances >> Live Appliance >> Context Menu Options >> Administration >> DNS Configuration >> DNS Sync /Full Sync

Network Management >> DHCP Management >> DHCP Appliances >> TCPWave DHCP IPv4 Appliances >> Live Appliance >> Context Menu Options >> Administration >> DHCP Configuration >> DHCP Sync /Full Sync

TW-FR-993: Callhome.zip download

Added context menu option Callhome Download in the IPAM/DNS/DHCP appliances sections that allow to download the data related to callhome.

Navigation:

Network Management >> DNS Management >> DNS Appliances >> TCPWave DNS IPv4 Appliances

Network Management >> DHCP Management >> DHCP Appliances >> TCPWave DHCP IPv4 Appliances

Network Management >> IPAM Management >> IPAM Appliances >> IPv4 IPAM Appliances

Remote High Availability

TW-FR-903: Checks for patch level comparison

Added validation to check the member node's patch levels while resetting the remote HA cluster. If the member nodes are at a different level, the UI displays a warning and an option to either continue with the reset or cancel the operation. Added new context menu options Reset Cluster State and Reset Cluster Services in DNS and DHCP Appliances page. Using the Reset Cluster State option, you can reset the cluster resource/service fail count. Using the Restart Cluster Services option, you can restart the cluster services on both member nodes.

Navigation:

Network Management >> DNS Management >> DNS Appliances >> TCPWave DNS IPv4 Appliances >> Right-Click DNS Appliance >> Context menu options >> Administration >> Cluster Administration >> Reset Cluster State, Reset Cluster Services

Network Management >> DHCP Management >> DHCP Appliances >> TCPWave DHCP IPv4 Appliances >> Right-Click DHCP Appliance >> Context menu options >> Administration >> Cluster Administration >> Reset Cluster State, Reset Cluster Services

Global Policy Management

TW-FR-817: SAML/Azure authentication with FQDN

Added a new global option **SAML Fully Qualified Name of the IPAM** in the Global Policy Management, which fetches the FQDN name for SAML authentication.

Navigation: Administration >> Configuration Management >> Global Policy Management

TW-FR-961: DNS Response Monitor

Added the following global options to monitor the DNS responses when the DNS resolution has failed.

- Alert for NXDOMAIN/SERVFAIL Responses
  - **Description**: Generates an alert when the count of the DNS Responses (NXDOMAIN, SERVFAIL, FORMERR, NOTIMP, REFUSED) exceeds the value specified in **Threshold for NXDOMAIN/SERVFAIL Responses** global option.
  - **Boolean Values**: Yes / No
  - **Default Value**: No
- Threshold limit for NXDOMAIN/SERVFAIL Responses
  - **Description**: Specify the value of the DNS Responses count per hour above which an alert is generated.
  - **Values**: Between 1 and 100000
  - **Default Value**: 60

Navigation:

Administration >> Configuration Management >> Global Policy Management >> DNS >> Alert for NXDOMAIN/SERVFAIL Responses

Administration >> Configuration Management >> Global Policy Management >> DNS >> Threshold limit for NXDOMAIN/SERVFAIL Responses

Reports Management

TW-FR-883: Extended Attribute Audit

Added Extended Attribute Audit report in the Event Reports. These are the set of names or values associated with an entity. This report displays the information related to the actions performed on the extensions by the network administrators.

Navigation: Reports >> Event Reports >> Extended Attribute Audit

TW-FR-821: DNS Queried Alternate Domains

Added DNS Queried Alternate Domains report in the DNS Query Reports. This report displays information about the frequently queried domains to TCPWave appliances forwarded to the proxy appliances. It helps you assign proper resource distribution and identify what applications are accessed.

Navigation: Reports >> DNS Reports >> DNS Query Reports >> DNS Most Queried Alternate Domains Report

TW-FR-995: Modified Microsoft Active Users report to fetch users from Domain Controllers

Microsoft Active Users report provides AD domain user information if the TCPWave appliance is connected to a domain controller. This information helps the network administrators to understand how and by whom the network resources are consumed. The data is displayed in the reports grid based on the newly added global option **Microsoft AD Users Poll Time Interval (minutes)**, enabled when the global option **Enable Microsoft AD Users Polling** is set to Yes.

Navigation:

Reports >> DHCP Reports >> Microsoft Active Users Report

Administration >> Global Policy Management >> Microsoft AD Users Poll Time Interval (minutes)

Administration >> Global Policy Management >> Enable Microsoft AD Users Polling

Fault Management

TW-FR-772: Benchmark alert for QPS, Alerts on resolution time

Added **Set QPS Thresholds** context menu option in the Monitored Appliances section. Using this option, you can set the High/Low QPS threshold values to check for the OK or CRITICAL alerts. On setting the values, the DNS_QPS_MONITOR service is enabled, and you can view the alerts in the Current Alarms section.

Added two new fields, Critical Threshold, and Warning Threshold, in the CHECK_DIG_QUERY_RESPONSE monitored service that allows you to monitor the query resolution

time. This service check is applicable to internal cache DNS appliances.

Navigation:

Infrastructure Management >> Fault Management >> Monitored Services >> Service Name >> DNS QPS Monitor

Infrastructure Management >> Fault Management >> Monitored Appliances >> Context Menu >> Set QPS Thresholds

Infrastructure Management >> Fault Management >> Current Alarms >> Service >> High_DNS_QPS_Monitor /Low_DNS_QPS_Monitor

TW-FR-830: Add Force Recheck Support for Multiple alerts and the CLIs.

Previously, force recheck functionality was enabled for an individual alert. Now the functionality is enhanced to support multi-select of alerts.

Navigation: Infrastructure Management >> Fault Management >> Current Alarms >> Single select/multi-select >> Force Recheck

TW-FR-918: Add monitoring to check the checksum of dhcpd.conf on remote vs IPAM

Added new monitored service DHCP_CONF_CHECKSUM that allows you to monitor the checksum value of the DHCP configuration file on IPAM and the respective remote DHCP appliances. This check is performed on an hourly basis.

Navigation: Infrastructure Management >> Fault Management >> Monitored Service >> DHCP_CONF_CHECKSUM

Configuration Assurance

TW-FR-928: HPNA Integration - Script to provide the version of the patch needed

Added Patch version configuration check in DNS, DHCP, and IPAM policy compliance sections which compare the actual and expected parameters and generate an alert if there is a mismatch in the parameters.

Navigation:

Infrastructure Management >> Configuration Assurance >> IPv4 DHCP Policy Compliance

Infrastructure Management >> Configuration Assurance >> IPv4 DNS Policy Compliance

Infrastructure Management >> Configuration Assurance >> IPv4 IPAM Policy Compliance

TW-CR-5478 Add a config assurance check

Added dhcpd_interfaces configuration check in the DHCP policy compliance section, which compares the actual and expected parameters and generates an alert if there is a mismatch in the parameters.

Navigation:

Infrastructure Management >> Configuration Assurance >> IPv4 DHCP Policy Compliance

Performance Management

TW-FR-800: Add Support to Windows Event Logs

Added Windows Logs option in the Log type drop-down. On selecting this option, the system displays the Category field with the following drop-down values:

- **Application**: On selecting this drop-down value, the system displays the information logged by the application hosted on the local machine. Example: It displays the information related to the type of resource records, TTL value, etc.
- **Security**: On selecting this drop-down value, the system displays the information related to the login attempts of the user, which could be either a successful event or a failure event; it also displays the elevated privileges and other audited events.
- **Setup**: On selecting this drop-down value, the system displays the information related to messages generated while installing and upgrading the Windows OS.
- **DNS Server**: On selecting this drop-down value, the system displays logs related to DNS Server Service, like zone files, shutdown, errors related to AD, etc.

Navigation: Infrastructure Management >> Performance Management >> Microsoft DNS Statistics >> Logs >> Windows Logs

TW-FR-956: Microsoft DNS Statistics – DNS Audit Logs

Added DNS Audit Logs option in the Log type drop-down. On selecting this option, the system displays the information about the zone or resource record settings that are modified. These include events such as dynamic updates, zone transfers, and DNSSEC zone signing and unsigning.

Navigation: Infrastructure Management >> Performance Management >> Microsoft DNS Statistics >> Logs >> DNS Audit Logs

TW-FR-957: Microsoft DHCP Statistics – Logs

Added Logs tab in the Microsoft DHCP Statistics page. On selecting this tab, the system displays the following fields:

- DHCP Appliance
- Log Start Date, Time
- Log End Date, Time

On clicking Generate, the system displays the information related to the DHCP server operational events, such as deletion of scope, scope configurations, scope modifications, etc.

Navigation:

Infrastructure Management >> Performance Management >> Microsoft DHCP Statistics >> Logs

Miscellaneous

TW-FR-964: Enhanced REST API

Added a new REST API call /rest/xtn/getSubnetNetworkDetailsByExtensions. It retrieves the subnet details using the extension name and value.

Customer Change Requests/Support Requests

Ticket ID	Description
TW-SR-783	Added a new scheduled job **ReclaimDHCPExpiredObjects**, which periodically clears the expired leases data. By default, the job is executed every 24 hours and reclaims all the DHCP expired object information from the IPAM, followed by publishing the deleted DDNS updated to the respective DNS appliance to remove the expired lease information from the appliance. **Navigation**: Administration >> Scheduler Management >> ReclaimDHCPExpiredObject
TW-SR-850	The issue of APIs to pull the next free IP address did not consider the Reference columns within the object grid into consideration before pulling the next IP has been fixed.
TW-SR-853	Previously, different custom administrators who belonged to the same administrator group but different organizations were not able to perform global search functionality. Now, the backend logic is modified to fix the global search functionality issue.
TW-SR-859	The issue of new entries created at the object level reflects in both internal & external zones has been fixed.
TW-SR-865	The issue of editing a TXT record ending in duplicate entries has been fixed.
TW-SR-876	Previously, the duplicate DHCP object name was validated using the short name of the object. Now, the logic is modified such that the name is considered as duplicate only if the FQDNS are the same for the object with a different IP address.
TW-SR-883	Delete operation failed on the object-level resource records from the DNS. Modified the backend logic to ensure that the object level resource records were deleted from the DNS.
TW-SR-895	Modified stored procedure to create reverse lookup entries while importing the IPv4 bulk object import.
TW-SR-898	Modified the column values in the SQL ALTER table to fix the address block issue.
TW-SR-924	Modified the schema to accept the NS records with owner name even if the domain exists.
TW-SR-949	Users were unable to view the non-managed zones in the named.conf from the GUI. To address this issue, backend logic is added, which ensures the information of the non-managed zones in the config file.
TW-SR-989	The issue of Dynamic DNS updates not making it to the master IPAM has been fixed.

Ticket ID	Description
TW-SR-990	The issue of DNS & DHCP remote servers constantly loosing connection status has been fixed.
TW-SR-1036	Added a new global option **RPZ Query Stats Table Rows,** that allows you to specify the number of rows to keep in the rpz query stats table. The minimum value is 5000, and the maximum value is 1 million. **Navigation**: Administration >> Global Policy Management >> RPZ Query Stats Table Rows
TW-SR-1056	Modified stored procedure and backend logic to fix the issue of adding a non-managed DNS zone.
TW-SR-1111	Modified the backend logic to fix the issue of the NS records to display the DNS interface name instead of the duplicate NS record name while generating the zone file.
TW-FR-596	It provided the ability to support DNS Charts over SNMPv3.
TW-FR-779	Object resource record import CLI supports DNS views column
TW-FR-925	Added hash code to license agreement page for tracking purposes.
TW-CR-4832	The issue of creating CNAME RR has been fixed.
TW-CR-4833	Usage of port 647 DHCP Failover traffic as DHCP Listening interface.
TW-CR-4957	The issue of the import wizard GUI displaying incorrect information has been fixed.
TW-CR-4989	API /object/getNextFreeIPandAllocate does not evaluate secondaryDomains
TW-CR-5025	The issue of screen sessions getting killed when trying to create an object to a zone with a long name has been fixed
TW-CR-5026	The issue of apex DNS entries not created at the object level has been fixed.
TW-CR-5032	The issue of the Splunk forwarder not sending any logs from the log directory has been fixed.
TW-CR-5045/FR-943	Modified backend logic to support RPZ functionality when the DNS views global option is enabled.
TW-CR-5077	The issue of dynamic PTR entries not replicating to the IPAM has been fixed.
TW-CR-5081	The issue of TXT record's rdata getting < \" > as prefix & suffix when such entries are created enclosed in double quotes has been fixed.
TW-CR-5084	DHCP Restarts Optimization: Added a backend logic to optimize the DHCP service restarts whenever you perform the bulk operations on IPv4 subnets and IPv4 DHCP Option Templates.
TW-CR-5100	The issue of object level DNS resource records not populating the DNS view value ended up in resolution failures have been fixed.
TW-CR-5128	The issue of the SNMP v3 discovery operation has been fixed.

Ticket ID	Description
TW-CR-5144	The issue of full DNS sync not propagating DNS records to remotes with large date sets has been fixed.
TW-CR-5145	CAA Bug: Added validation to accept hyphen characters in the owner's name field of the CAA resource record at the zone level.
TW-CR-5158	Previously, for a DHCP duplicate object name, the DDNS updates sent by IPAM to Microsoft DNS appliances led to multiple subzones within it, leading to incorrect DNS resolution. Now, the backend logic is modified to address the DHCP duplicate object name to ensure that multiple sub-zones are not created.
TW-CR-5209	Modified the backend logic to fix the reverse lookup issue at the object level for the PTR records.
TW-CR-5211/SR-989	Added SQLite database on the remote appliances to store the dynamic DNS updates when the IPAM is not reachable and replicate the updates when the IPAM is up and running. The following global options are added in the Global Policy Management section to optimize the External DDNS Updates: **External Updates Purge from SQLite**: This purges the oldest entries from the SQLite database on the remote. ▪ Default value: 7 days ▪ Minimum value: 1 day ▪ Maximum value: 30 days **External Updates Queue Purge Limit**: The queue size limit default value is increased to 0.5M and the maximum value to 2M. **Navigation**: Administration >> Configuration Management >> Global Policy Management
TW-CR-5212	The issue of DNS remotes trying to establish a connection with multiple IPAMs even though the IPAM preference is set manually has led to the restarting of the broken client has been fixed.
TW-CR-5222	Updated Configure script.
TW-CR-5224	The issue of deleting the TXT record that has quotes in CLI has been fixed.
TW-CR-5226	Previously, the TTL value at the object level was 1200 seconds. Now the functionality is enhanced at the object level to accept the TTL value provided at the zone level. Additionally, you can also modify the TTL value at the object level. **Navigation**: Network Management >> IPv4 Address Space >> IPv4 Networks >> IPv4 Subnets >> IPv4 Objects >> Edit
TW-CR-5227	When the TTL is not updated with any value, the system defaults to zero resulting in

Ticket ID	Description
	the failed cache resolution. Modified the backend logic to ensure the zone's TTL value is updated at the object level RR.
TW-CR-5259	Added new schedule type options Daily, Weekly, and Monthly in the Schedule Email popup window. Using these options, you can schedule the email to the selected contacts on a daily, weekly, and monthly basis. A scheduled task is created in the scheduler management and is executed based on the schedule type. **Navigation**: Administration >> Reports >> Generate >> Email icon >> Email Report >> Selected Contact >> Schedule Email
TW-CR-5260	Modified Global NTP Offset Report by adding the columns: Type, When, Poll, Reach, Jitter, and NTP Authentication. **Navigation**: Report >> Event Reports >> Global NTP Offset Report
TW-CR-5277	Added validation to accept hyphen characters in the owner's name field at the zone level. **Navigation**: Network Management >> DNS Management >> DNS Zones >> Managed DNS Zones >> Resource Records tab >> Owner Name
TW-SR-1017/CR-5308	Resource record type CAA is failing to load in the zone DB file.
TW-CR-5309	Previously, the owner's name field was prepopulated with the zone name in the Managed DNS Zones page. Now, the functionality is enhanced to include the sub-domains in the owner's name field. **Navigation**: Network Management >> DNS Management >> Managed DNS Zones >> Add/Edit >> Resource Records >> Record Type >> CAA >> Owner Name
TW-CR-5335	The issue of organization export if a subnet or object file is not created has been fixed.
TW-CR-5362	Modified the backend validation to ensure that the owner's name format accepts the underscore character after the dot at the zone level RR. Example: test._domainkey
TW-CR-5368	Modified the backend logic to accept the blank line in the description field of the resource records. **Navigation**: Network Management >> DNS Management >> Managed DNS Zones >> Resource Records tab >> Resource Record >> Description field
TW-CR-5373	Previously, the owner's name field did not accept the FQDN. Now, the functionality is enhanced to accept FQDN in the owner's name field. **Navigation**: Network Management >> DNS Management >> Managed DNS Zones >> Add/Edit >> Resource Records >> Record Type >> SPF

Ticket ID	Description
TW-CR-5374	Previously, the character length of the public key was 255. Now, modified the backend logic and added validation to allow 499 characters in the public key field. **Navigation**: Network Management >> DNS Management >> Managed DNS Zones >> Add/Edit >> Resource Records >> Record Type >> DKIM
TW-CR-5387	The issue of the user is not able to modify or delete the record as it is associated with one or more CNAME resource record(s)." while trying to add an extra DNS view to an RR.
TW-CR-5414	The issue of Getting the error "Table 'tims.v6_external_master_last_sync_status' doesn't exist." when the user selects a different organization from the "Create Non-Managed DNS Zone" form has been fixed.
TW-CR-5428	Modified the backend logic to optimize the Microsoft sync issue.
TW-CR-5474	The network delete force sync of forward and reverse zones has been fixed.
TW-CR-5489	Resolved discovery-related issues.
TW-CR-5541	The issue of DDNS updates has been fixed.
TW-CR-5566	Added a backend logic to fix the IPv6 DNS full sync issue and IPv6 reverse zone.db file truncation issue.
TW-CR-5569	The conflicting gateway issue was resolved in the config script.

CLI Updates

#	Description
1	Added the following CLI's: ▪ addslbfrontend ▪ addfrontendmembers ▪ addpoolassociations ▪ addslbaclrulecontents ▪ addslbaclruleset ▪ adddnsdohtmpl ▪ adddhcppingpoller ▪ addbackendnode ▪ addslbadvrule ▪ addslbadvruleacl ▪ addslbbackend ▪ addipv6rr ▪ deletednsdohtmpl ▪ deletepoolassociations ▪ deletefrontendmembers ▪ deleteslbfrontend ▪ deleteslbaclruleset ▪ deleteslbaclrulecontents ▪ deletedhcppingpoller ▪ downloadipv6dhcpconfig ▪ downloadipv6dnsconfig ▪ deleteipv6rr ▪ editbackendnode ▪ editslbbackend ▪ editslbadvrule ▪ editaclruleset

#	Description
	▪ editslbadvruleacl ▪ editaclrulecontents ▪ editslbfrontendmembers ▪ editpoolassociations ▪ editslbfrontend ▪ editdnsdohtmpl ▪ editdhcppingpoller ▪ editipv6rr ▪ exportmicrosoftdhcpserver ▪ exportproxyrootzone ▪ forcerecheckalert ▪ getslbappliance ▪ getslbappliancetmpl ▪ getslbopttmpl ▪ importmicrosoftdhcpserver ▪ importproxyrootzone ▪ listdhcppingpoller ▪ listpoolassociations ▪ listslbvip ▪ listslbserver ▪ listslbservertmpl ▪ listslbopttmpl ▪ listslbfrontend ▪ listslbbackend ▪ listslbbackendnode ▪ listslbadvrule ▪ listslbadvruleacl ▪ listipv6rr

#	Description
	▪ resetremoteclusterstate ▪ restartremotecluster ▪ setslbappliance ▪ setslbappliancetmpl ▪ setslbopttmpl ▪ setzoneexcludesync ▪ setzoneautoforcesync ▪ deleteslbbackendnode ▪ deleteslbadvrule ▪ deleteslbadvruleacl ▪ deleteslbbackend ▪ deleteslbappliance ▪ deletednsdohtmpl ▪ deleteslbappliancetmpl ▪ deleteslbopttmpl
2	Modified the following CLIs: ▪ adddnszonetmpl ▪ adddnsview ▪ adddnsdohtmpl ▪ editdnsview ▪ editdnszonetmpl ▪ setdnsserver

REST APIs

#	Operation	RESTAPI
Added REST APIs		
1	GET	/subnet/list-dhcp-params
		/slbOptionTemplate/get
		/slbOptionTemplate/page
		/object/get_dc_credentials
		/auditreports/dnsqueryalternatedomainrptlist
		/server/restartClusterServices
		/server/resetResourceFailCount
		/atis/geomap
		/atis/top10qpsaps
		/atis/outliersgrid
		/atis/atiscounter
		/atis/dgapiechart
		/atis/dnsqueryratebyzone
		/xtn/getSubnetNetworkDetailsByExtensions
		/monitor/getQpsThresholds
		/server/areMemsAtSamePatchLevel
		/server/getCurrentHeapSize
		/server/changeHeapSize
		/discoverydashboard/getDiscoveryEvents
		/discoverydashboard/getOSTodevicecount
		/discoverydashboard/discovereddevices
		/discoverydashboard/topleastbusypoller
		/discoverydashboard/devicelastuptime
		/dnsserver/dns_interfaces_get
		/server/callhomedownload
		/ms-charts/mswineventlogs/
		/auditreports/dnsqueryalternatedomainrptlist
		/adcRuleset/page
		/adcRuleset/getAssociatedList
		/adcRuleset/listbyorg
		/adcRuleset/aclElement/get
		/adcRuleset/aclElements/page
		/aclRuleset/search
		/gslbtrafficRules/page
		/newchart/gslbstats
		/newchart/gslbcharts
		/newchart/gslb
		/gslbTrafficRules/getAssociatedList
		/gslbTrafficRules/listbyorg
		/gslbTrafficRules/get
		/gslbTrafficRules/gtRule/get
		/gslbTrafficRules/getfiledata
		/gslbTrafficRules/gtRule/page
		/gslbTrafficRules/search
		/slbAclRule/page
		/slbAclRule/getAssociatedList

#	Operation	RESTAPI
		/slbAclRule/listbyorg
		/slbAclRule/get
		/slbAppliance/getLastSync
		/slbAppliance/getGslbRuleReferences
		/slbAppliance/getFrontends
		/slbAppliance/slb/config/download
		/slbAclRule/aclElement/get
		/slbAclRule/getfiledata
		/slbAclRule/aclElements/page
		/slbAclRule/search
		/slbAppliance/getRemoteVersions
		/slbAppliance/getLogs
		/slbAppliance/heartbeat
		/slbAppliance/getCurrentHeapSize
		/slbAppliance/getMRCParams
		/slbAppliance/getStatsHtml
		/slbAppliance/server-configuration
		/slbAppliance/page
		/slbAppliance/checkGslbIP
		/slbAppliance/ref-front-end-list
		/slbAppliance/update-heartbeat
		/slbAppliance/genconfig
		/slbAppliance/gslb/config/download
		/slbApplianceTemplate/get
		/slbApplianceTemplate/page
		/slbApplianceTemplate/add
		/slbBackEnd/node/page
		/slbBackEnd/node/get
		/slbBackEnd/page
		/slbBackEnd/Search
		/slbFrontEnd/Search
		/slbFrontEnd/getfiledata
		/slbFrontEnd/page
		/slbFrontEnd/get
		/slbFrontEnd/backend/page
		/slbFrontEnd/bind/page
		/slbFrontEnd/bind/get
		/slbFrontEnd/backend/get
		/slbFrontEnd/getFrontendRef/appliances
		/slbResponses/page
2	POST	/object/update_dc_credentials
		/object/add_dc_credentials
		server/changeHeapSize
		zone/excludeFromSync
		/zone/autoForceSync
		/monitor/setQpsMonitoring
		/adcRuleset/delete
		/adcRuleset/aclElement/delete
		/adcRuleset/aclElement/edit

#	Operation	RESTAPI
		/adcRuleset/edit
		/adcRuleset/aclElement/add
		/adcRuleset/add
		/gslbTrafficRules/delete
		/gslbTrafficRules/gtRule/delete
		/gslbTrafficRules/gtRule/edit
		/gslbTrafficRules/edit
		/gslbTrafficRules/gtRule/add
		/gslbTrafficRules/add
		/slbAclRule/add
		/slbAclRule/aclElement/add
		/slbAclRule/edit
		/slbAclRule/aclElement/edit
		/slbAclRule/aclElement/delete
		/slbAclRule/delete
		/slbAppliance/restart
		/slbAppliance/changeHeapSize
		/slbAppliance/edit
		/slbAppliance/editbgpcfg
		/slbAppliance/delete
		/slbAppliance/notification/add
		/slbAppliance/gslb/sync
		/slbAppliance/notification/delete
		/slbAppliance/add
		/slbApplianceTemplate/delete
		/slbApplianceTemplate/edit
		/slbApplianceTemplate/add
		/slbBackEnd/edit
		/slbBackEnd/node/edit
		/slbBackEnd/node/delete
		/slbBackEnd/node/add
		/slbBackEnd/delete
		/slbBackEnd/add
		/slbFrontEnd/bind/edit
		/slbFrontEnd/edit
		/slbFrontEnd/bind/add
		/slbFrontEnd/bind/delete
		/slbFrontEnd/backend/edit
		/slbFrontEnd/delete
		/slbFrontEnd/backend/add
		/slbFrontEnd/backend/delete
		/slbFrontEnd/add
		/slbOptionTemplate/edit
		/slbOptionTemplate/add
		/slbOptionTemplate/delete
Modified REST APIs		
1	GET	/object/getNextFreeIPandAllocate
2	POST	/monitor/recheckAlert
Deleted REST API		

#	Operation	RESTAPI
1	GET	subnet/listdomainservers