TCPWave IP Address Management System®

Release Notes

Version 11.33P2

August 31, 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

Document Change History

Revision Date	Summary of Changes
August 31 2023	Added the following tickets: TW-CR-5691, TW-FR-985, TW-SR-1371, TW-CR-5409, TW-FR-1038, TW-SR-1395, TW-CR-5509, TW-CR-5874, TW-SR-1283, TW-SR-977, TW-CR-6244

Introduction

These release notes summarize the new features, improvements, and stability fixes included in the TCPWave DDI v11.33P2 release.

Notes: Contact support@tcpwave.com for the following:

- ADC Integration.
- Alice Chatbot Service License.
- Organization-specific ACLs: When upgrading to 11.33P2, existing ACLs, which are currently not organization-specific, will be available in all organizationsIt. It helps you to create organization specific ACLs.
- If you come across any issues with DNSSEC enabled zones.

Feature Requests/Enhancements

ADC Management

TW-FR-1061: ADC Management

Implemented the following features:

- ADC Dashboard and Application Management Support: ADC Dashboard offers a robust interface for managing, monitoring, and troubleshooting Application Delivery Controllers (ADCs), ensuring seamless functionality and uptime of crucial applications.
- Implementations for ADCs and GSLB Appliances: It extends to implementing ADC Top Talkers and Recursive DNS Resolver for GSLB appliances. These are integral parts of the network infrastructure to track significant data flow and manage DNS queries effectively. Additionally, you can enable GSLB services on DNS cache appliances.
- Load Balancing and Health Checks: With customizable GSLB Load Balancing algorithms, the system ensures efficient network traffic distribution, while configurable GSLB Health Checks enable reliable GSLB responses.
- Licensing and Patch Management Support: This system provides streamlined processes for ADC appliance licensing and comprehensive patch management support, ensuring that all ADC appliances are secure and up-to-date.
- Client IP Reservation and Protocol Supports: The platform offers client IP reservation in HTTP mode and support for the H2 protocol and HSTS for frontend members in the SLB frontend.
- Cookie Persistence and Cluster Functionality: Dynamic cookies enhance user session tracking, improving the cookie persistence feature. Also, cluster functionality for the ADC appliances is provided to improve the system's efficiency and reliability.

- SSL Certificate Monitoring and Firewall Template: The platform includes SSL Certificate expiration monitoring for the SLB VIP SSL Certificate and a Firewall template for the ADC appliance, enhancing network security.
- Association of Appliance Groups: The association of appliance groups with ADC appliances allows efficient management of different ADC appliances in a unified manner.
- GSLB Traffic Control, WAF Features, and Service Management: GSLB traffic control based on subnet groups and WAF template-related features improve the system's security and manageability. Also, service management from the UI for the ADC appliance has been added for easier control.
- Network Monitoring and Schedule Operations: The ADC Dashboard support incorporates network bandwidth usage and real-time traffic analysis grid in the ADC appliance context menu. Scheduling operations for Sync, Add, Edit, and Delete operations of ADC appliances are also included to enhance system management efficiency.
- ADC Monitoring: The system provides comprehensive ADC Monitoring, offering insights into the performance and health of the ADC appliances, ensuring continuous, optimum performance.
- SLB Statistics: SLB Statistics effortlessly monitor and evaluate the health status of the ADC appliances. It provides insights into crucial system parameters, including CPU utilization, memory utilization, traffic, and administrative logs, as well as frontend and backend server parameters, such as heartbeat and session rate, enabling comprehensive analysis and assessment.

Navigation:

Network Management >> ADC Management >> ADC Appliances >> ADC Cluster

Network Management >> ADC Management >> ADC Appliances >> ADC Health Check Template

Network Management >> ADC Management >> Application Management >> Applications

Network Management >> ADC Management >> SLB Templates >> SLB WAF Template

Infrastructure Management >> Performance management >> TCPWave SLB Statistics

TW-FR-1023: AI-ML WAF Support

Added SLB WAF template under SLB templates section. WAF stands for Web Application Firewall (WAF). TCPWave's AI/ML-based WAF, a hybrid architecture, combines the power of signature and anomaly-based detection. The solution offers comprehensive protection against known attacks and emerging threats. With IP blocking, customization options, and rule management features, TCPWave’s WAF ensures efficient and tailored security for web applications. Leveraging AI/ML models DistilBERT and Logistic Regression, TCPWave WAF achieves high accuracy while optimizing CPU resources.

Navigation: Network Management >> ADC Management >> SLB Templates >> SLB WAF Template >> Add WAF Template

TW-FR-1035: NICs and VIPs Monitoring

Added new Monitored Service CHECK_NIC_INTERFACES to enable or disable the monitoring check. By default, check is enabled. The check is performed on TCPWave IPAM, DNS, DHCP, and ADC appliances every 5 minutes.

Navigation: Infrastructure Management >> Fault Management >> Monitored Services >> Check_NIC_Interfaces

TW-FR-1074: ADC Appliance Audit Report

Added ADC Appliance Audit Report in ADC Reports section. This report provides comprehensive audit information about the operations performed on a specific ADC appliance or all appliances by an administrator. The report helps network administrators track changes and activity related to ADC appliances and ensure that the configuration and operation of the ADC system are secure and stable.

Navigation: Reports >> ADC Reports >> ADC Appliance Audit

TW-FR-1087: SLB Option Template Audit Report

Added SLB Option Template Audit Report in ADC Reports section. This report provides a comprehensive account of an administrator's actions and events on the SLB option template(s). This report provides information such as additions, modifications, deletions, and other relevant details. It helps maintain accountability, ensure compliance, and identify potential configuration errors or unauthorized modifications.

Navigation: Reports >> ADC Reports >> SLB Option Template Audit

TW-FR-1114: GSLB Traffic Control Rule Report

Added GSLB Traffic Control Rule Report in ADC Reports. This report provides valuable information about the activities carried out by an administrator about GSLB Traffic Control Rules and Rule sets. This report specifically focuses on adding, editing, and deleting GSLB Traffic Control Rules and Rule sets. In addition, the GSLB Traffic Rule Set Report plays a role in identifying potential configuration errors or unauthorized modifications.

Navigation: Reports >> ADC Reports >> GSLB Traffic Control Rule

TW-FR-1055: SLB Health Status Report

Added SLB Health Status Report in SLB Health Status Report. This report offers visibility into server availability and performance, which helps you identify any load-balancing service-related issues. The report encompasses essential details like server status (up or down), response times, and alerts concerning server health. This valuable information facilitates troubleshooting, highlights problematic servers or applications, and assists in making informed decisions regarding server maintenance or upgrades.

Navigation: Reports >> ADC Reports >> SLB Health Status

TW-FR-1054: Top SLB Appliances Connections Report

Added Top SLB Appliances Connections Report. This report monitors and manages the performance and availability of heavily utilized SLB Appliances by clients or users. It allows you to optimize performance and ensure availability proactively. This involves resource allocation, such as increased memory or CPU capacity, or load balancing to prevent overwhelming any single server. Additionally, tracking these metrics aids in identifying security threats, like denial-of-service attacks, by detecting abnormal traffic patterns and enabling swift responses to prevent potential security incidents.

Navigation: Reports >> ADC Reports >> SLB Appliances with Highest & Lowest Client Connections

TW-FR-1068: ADC Top Talker Report

Added ADC Top Talker Report in ADC Reports. Additionally, monitoring top talkers allows you to proactively plan for capacity, ensuring our network can handle increasing traffic demands.

Navigation: Reports >> ADC Reports >> ADC Top Talker

TW-FR-1056: Frontend & Backend Statistics ADC Report

Added Fronted & Backend Statistics ADC Report in ADC Reports. This report provides valuable insights into the performance and behavior of your application infrastructure. It allows you to monitor and analyze the traffic, requests, and response times for both frontend and backend components, helping you optimize the delivery of your applications.

Navigation: Reports >> ADC Reports >> Frontend & Backend Statistics ADC

TW-FR-1080: SLB Appliances Template Audit Report

Added SLB Appliances Template Audit Report in ADC Reports. The SLB Appliance Template Audit Report provides a comprehensive account of an administrator's actions and events on the SLB Appliance template(s). This report is an invaluable audit trail, providing information such as additions, modifications, deletions, and other relevant details. It helps maintain accountability, ensure compliance, and identify potential configuration errors or unauthorized modifications.

Navigation: Reports >> ADC Reports >> ADC Appliances Template Audit

TW-FR-1072: WAF Attack Analysis Report

Added WAF Attack Analysis Report in ADC Reports. This report provides information that delves into the various attack types employed against a web application, meticulously detailing the count of each attack type encountered. This information empowers you to fortify your security measures based on the insightful findings, ultimately elevating the overall protection of your web application to unprecedented levels of excellence.

Navigation: Reports >> ADC Reports >> WAF Attack Analysis

TW-FR-1095: WAF Template Audit Report

Added WAF Template Audit Report in ADC Reports. The WAF (Web Application Firewall) Template Audit provides administrator-related actions and events specific to one WAF template or all templates. This comprehensive report ensures that every change such as addition, modification, deletion, or other relevant detail is captured and recorded precisely. It helps maintain accountability, ensure compliance, and identify potential configuration errors or unauthorized modifications.

Navigation: Reports >> ADC Reports >> WAF Template Audit Report

TW-FR-1130: Monitor SSL Cert Expiration

Added the backend logic to monitor the VIP SSL certificate expiry.

TW-FR-1104: Preserve Client IP Feature In The SLB Frontend Configuration

Added Preserve Client IP Address checkbox while adding and editing the SLB Frontend Configurations. By enabling the checkbox, the client's IP address is retained instead of the load balancer's address.

Navigation: Network Management >> ADC Management >> SLB Frontend Configuration >> Add/Edit SLB Frontend Configuration>> Properties tab >> Preserve Client IP Address checkbox

TW-FR-1124: Auto Create Object For VIP In The SLB Frontend Configuration

Added auto-create object for VIP while editing the SLB Configurations. It allows you to select the domain name from the dropdown to auto-create an object with VIP.

Navigation: Network Management >> SLB Configuration >> Editing SLB Configuration >> Frontend Members tab >> Domain Name dropdown

TW-FR-1117: Scheduled Feature ADC Appliance

Added Scheduled option while adding, editing, and deleting ADC appliance sections. It allows you to set the scheduled time for the operations.

Navigation: Network Management >> ADC Management >> ADC Appliances >> Create/Edit/Delete Appliances >> Schedule

TW-FR-1118: Response Pages For Server Load Balancing (SLB)

Modified the error pages according to the error codes specified in the Edit SLB Response Page. This feature enables personalized error page customization for various error codes, particularly when the server is experiencing downtime or is inaccessible. This page encompasses a range of defined error codes.

Navigation: Network Management >> ADC Management >> SLB Response >> Edit

TW-FR-1098: ADC Monitoring Checks

Added New Monitored Services to enable/disable the monitoring checks. By default, all monitoring checks are enabled.

- ADC_CLUSTER_NAME: It allows you to check the name of the ADC cluster configured in the IPAM vs. the name in /etc/keepalived/keepalived.conf file in the ADC appliance. If any difference is detected, the system generates a CRITICAL alert in the IPAM. An OK alert is

generated if there is no difference. The ADC cluster name is configured while creating an ADC cluster in the IPAM.

- ADC_CLUSTER_STATE: It allows you to check the state of the ADC appliance in the cluster. This is checked as the state configured in the IPAM vs. the state in /etc/keepalived/keepalived.conf file in the ADC appliance. If any difference is detected, the system generates a CRITICAL alert in the IPAM. An OK alert is generated if there is no difference. The state of the ADC appliance is defined while adding the appliance to the ADC cluster in the TCPWave IPAM.
- ADC_CLUSTER_INTERFACE: To check the interface of the ADC appliance used in the cluster. This is checked as interface configured in the IPAM vs. the interface existing in /etc/keepalived/keepalived.conf file in the ADC appliance. If any difference is detected, the system generates a CRITICAL alert in the IPAM. An OK alert is generated if there is no difference. The interface of the ADC appliance in the cluster is defined while adding the appliance to the ADC cluster in the TCPWave IPAM.
- ADC_CLUSTER_VIPS: To check the VIPs of the ADC appliance used in the cluster. This will be checked as VIPs configured in the IPAM vs. those existing in /etc/keepalived/keepalived.conf file in the ADC appliance. If any difference is detected, the system generates a CRITICAL alert in the IPAM. An OK alert is generated if there is no difference. VIPs are associated with Front Ends and the ADC appliance in the TCPWave IPAM.
- ADC_VIPS_STATE: To check if the VIPs are up/pingable from the ADC appliance. VIPs are associated with Front Ends and the ADC appliance in the TCPWave IPAM.
- TCPWAVE_SLB: To check whether haproxy service is running in the ADC appliance. If the service is not running, a CRITICAL alert is generated in the IPAM else, an OK alert.
- TCPWAVE_GSLB: To check whether the timsgslb service is running in the ADC appliance. This check is done only if the GSLB is enabled on the ADC appliance. If the service is not running, a CRITICAL alert is generated in the IPAM else, an OK alert.
- TCPWAVE_GSLBDNS: To check whether the timsgslbdns service is running in the ADC appliance. This check is done only if the GSLB is enabled on the ADC appliance. If the service is not running, a CRITICAL alert is sent to IPAM else, an OK alert.

The checks are performed in the ADC appliances every 5 minutes.

Navigation: Infrastructure Management >> Fault Management >> Monitored Services

DNS Management

TW-FR-472: Organization Specific ACLs

Added organization-specific dropdown while creating ACLs. It allows you to specify the organization. This field is mandatory for adding or cloning the ACLs. If the organization is not specified for a particular ACL, then the system allows you to select the organization from the dropdown in the ACL edit page. If the organization is specified for a particular ACL, the field is disabled, restricting you from modifying it.

Navigation: Network Management >> DNS Management >> DNS Security >> DNS Access Control Lists

TW-FR-804: MNAME Option

Added MNAME dropdown option in the SOA Record Attributes while adding and editing zone templates. It allows you to select one slave for SOA generation. During DNS full sync and Zone Force sync processes, the zone files are generated using the SOA record selected from the zone template. This selected SOA record is used to populate the MNAME field in the SOA section of the zone file. The SOA selection process includes designating a stealth appliance as the primary name server. When multiple slaves are chosen for a stealth master, the current logic randomly selects one slave for the SOA section. By default, the master's fully qualified domain name (FQDN).

Navigation: Network Management >> DNS Management >> DNS Zone Templates >> Create Zone Template >> Basic Zone Information tab >> SOA Record Attributes >> MNAME dropdown option

TW-FR-879: Provided SNMP OID For Serial Number Or Service Tag

TCPWave has recently updated its SNMP MIB file, incorporating the relevant OID for Service Tag information. This newly added OID, .1.3.6.1.4.1.39572.1.14.1.7.4.0, provides detailed data about the service tag.

TW-FR-935/ TW-CR-5874: Zone Exclusion, Force Sync Enhancement, & Bulk Operation Support

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 for 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 are required to 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-941: Schedule Operations For Resource Records

Added Schedule option in add, edit, and delete resource record popup window at the zone, object, proxy root zone, and root zone level. On clicking this option, the system displays a Schedule Add Operation popup window to set the schedule operation by providing the job ID, date, and time for adding, editing, and deleting resource records at zone, object, and root zone levels.

Navigation:

Network Management >> DNS Management >> Managed DNS Zones >> Edit Zone >> Resource Records tab >> Add/Edit/Delete >> Schedule

Network Management >> DNS Management >> DNS Proxy Zones >> DNS Proxy Root Zone >> DNS Proxy Root Zone Resource Records >> Add/Edit/Delete >> Schedule

Network Management >> DNS Management >> DNS Zones >> Managed DNS IPv4 Reverse Zone >> Resource Records >> Add/Edit/Delete >> Schedule

Network Management >> DNS Management >> IPv4 Address Space>> IPv4 Networks >> IPv4 Subnets >> IPv4 Objects >> Resource Records >> Add/Edit/Delete >> Schedule

TW-FR-945: RPZ Support For Unbound

Added RPZ support for unbound appliances. It allows you to associate the RPZ template to a DNS appliance of unbound type; then, a full sync is initiated to update the configurations on the remote unbound appliance and generate the configs in unbound.conf. When an RPZ template is changed with either masters or zone names, then IPAM sends updates to all the appliances that are using the selected RPZ template.

Navigation: Network Management >> DNS Management >> DNS Security >> DNS Threat Management

TW-FR-951: Logging Facility For DDNS Related Logs

Implemented additional logging functionalities on both the IPAM and remote sides to monitor the Dynamic DNS (DDNS) updates within a newly created log file. This enhanced log file facilitates the examination of the DDNS update process and aiding in identifying and resolving any potential issues where updates might not have been successfully processed.

TW-FR-971/ 1067: Secondary Zone Support - NS1, Akamai, Neustar & Cloudflare

Added support for Akamai, NS1, Neustar & Cloudflare as slaves to TCPWave DNS Masters. TSIG Key is needed for the zone transfers between the slave cloud providers and TCPWave DNS masters. Added Slave Cloud Providers Grid in the Cloud Providers tab. It allows you to select the slave cloud providers. When this zone template is associated with a zone, the system sends a secondary zone created to the cloud providers. Added TSIG Key context menu option in the Provider Credentials page. On clicking this option, the system displays a TSIG Key popup window where you can enter the TSIG Key name, which TCPWave DNS masters use to transfer the zone data to the secondary cloud providers. Added Slave Cloud Provider TSIG Key Name dropdown field in the Managed Zone and Reverse Zone pages to accept the zone-specific TSIG keys.

Navigation:

Network Management >> DNS Management >> DNS Templates >> DNS Zone Templates >> Create >> Cloud DNS Providers tab >> Slave Cloud Providers Grid

Network Management >> Cloud Management >> Provider Credentials >> Context menu >> TSIG Key

Network Management >> DNS Management >> DNS Zones >> Managed DNS Zones >> Create/Edit >> Slave Cloud Provider TSIG Key Name field

Network Management >> DNS Management >> DNS Zones >> Managed DNS IPv4 Reverse Zones >> Create/ Edit >> Slave Cloud Provider TSIG Key Name field

TW-FR-988: DNSSEC Signing Changed In ISC BIND 9.18.10

In prior versions, the auto-dnssec and inline-signing parameters for automatic DNSSEC maintenance were used, but starting from the 9.18.10 release, these options have been deprecated and eventually removed in subsequent 9.19.* versions, although the 9.18.* versions continue to support them with potential warnings in named-check.conf and named.log. Starting from BIND version 9.16.*, a more robust alternative is introduced - the dnssec-policy parameter, which revolutionizes key creation and maintenance when a zone is DNSSEC-enabled, eliminating the reliance on the deprecated parameters. The existing IPAM functionality is maintained for key creation, copying to remotes, and key rollover management while adapting to the new DNSSEC signing approach by removing the deprecated auto-dnssec and inline-signing parameters from our named.conf configuration and incorporating the new syntax to support the dnssec-policy parameter, ensuring a smooth and efficient transition.

TW-FR-1004: Upgrade The Xbill Java DNS

Existing JavaDNS upgraded to the latest version to fix the security vulnerabilities with the old jar file.

TW-FR-1022: Undo Support For Object & Zone RRs

Added Undo icon in the Resource Records grid of Managed DNS Zone, Managed DNS IPv4 Reverse Zones, DNS Proxy Root Zone, DNS Root Zone, and Object pages. By clicking this icon, it redirects to the recycle bin page. This page lets you view the add/edit/delete operations performed on the specific

resource record. This page allows you to restore or undo specific resource records by clicking the restore option.

Navigation:

Network Management >> DNS Management >> DNS Zones >> Managed DNS Zones >> Edit Managed DNS Zones >> Resource Records grid >> Undo icon

Network Management >> DNS Management >> Managed DNS IPv4 Reverse Zones >> Edit Managed DNS IPv4 Reverse Zones grid >> Undo icon

Network Management >> DNS Management >> DNS Proxy Root Zone >> DNS Proxy Root Zone Resource Records >> Undo icon

Network Management >> DNS Management >> DNS Root Zone >> Internal root zone external resource records grid >> Undo icon

Network Management >> DNS Management >> Object >> Undo icon

TW-FR-1038: Loading Icon To RPZ Page

Implemented the inclusion of a loading icon on the RPZ page while editing RPZ policies. This loading icon indicates the transmission of incremental updates to DNS remotes.

Navigation: DNS Management >> DNS Security >> DNS Threat Management >> RPZ Polices tab

TW-FR-1064: Remote Cluster Support For DNS+DHCP Appliances

Enhanced remote cluster functionality that supports a combined DNS and DHCP cluster. This enhancement enables DNS and DHCP remote clusters to be established on the same set of member appliances.

Navigation:

Network Management >> DNS Management >> DNS Appliances >> Context menu option >> Cluster Administration

Network Management >> DHCP Management >> DHCP Appliances >> Context menu option >> Cluster Administration

TW-FR-1097: Support For DNSDiag

Added DNSPing context menu option in the TCPWave IPv4 DNS Appliances page. On clicking this option, the system displays the DNSPing popup window. You can use the hostname, record type, and number of pings to try and flag. This option pings the DNS resolver by sending an arbitrary DNS query a given number of times and calculates minimum, maximum, and average response times.

The DNSPing page is also added in DNS Tools of the Infrastructure Management.

Navigation:

Network Management >> DNS Management >> DNS Appliances >> TCPWave IPv4 DNS Appliances >> Context menu options >> Information >> DNSDiag >> DNSPing

Infrastructure Management >> DNS Tools >> DNSDiag >> DNSPing page

TW-FR-1134: Add Entity-level Permission Support For NSM, Firewall, & RPZ Templates

Implemented the ability to grant record-level permission for NSM, Firewall, and RPZ templates during administrator permission creation. These granular functions empower administrators to take actions at the individual record level.

Navigation: Administration >> Security management >> Administrator Permission

TW-FR-1185: Zone RR Count Validation On IPAM & Remote During DNS Full Sync On The Appliance

Enhanced the zone Resource Record (RR) count validation in the IPAM system. This strategic advancement ensures data synchronization between the local and the remote systems.

Added the following global options:

Enable RR Count Validation During DNS Sync:

- Description: When 'Enable RR Count Validation During DNS Sync' is set to 'Yes,' DNS sync validates RR count in IPAM-generated and remote zone files twice before copying them to named folders. Discrepancies trigger sync cancellation to ensure data integrity.

Max RR Count Difference in DNS Sync: IPAM vs. Remote Zone Files:

- Description: This parameter empowers you to define the permissible maximum difference in RR counts between IPAM and remote zone files during synchronization. The default value has been set at 1000, with a range spanning from 0 to 100000.

Activating the enable RR count validation during the DNS Sync option initiates zone RR count validation locally and remotely. The IPAM system meticulously validates comparing the generated data with the remote data across all zones.

DHCP Management

TW-FR-823: Add An Option For The User To Perform Only The DHCP Service Sync

Added DHCP Sync context menu option in the DHCP IPv4 Appliances. It performs DHCP Sync, which only changes the DHCP configuration and restarts the DHCP service. Renamed the existing Sync option to Full Sync in the context menu of the DHCP IPv4 appliances. Added DHCP Sync All in the DHCP IPv4 appliances page. It performs full sync operation on one or multiple appliances. Renamed Sync All icon to Full Sync All in the DHCP IPv4 appliances page.

Navigation:

Network Management >> DHCP Management >> DHCP Appliance >> TCPWave DHCP IPv4 Appliances >> Context menu >> DHCP Sync

Network Management >> DHCP Management >> DHCP Appliance >> TCPWave DHCP IPv4 Appliances >> DHCP IPv4 Appliances >> DHCP Sync All

Network Management >> DHCP Management >> DHCP Appliance >> TCPWave DHCP IPv4 Appliances >> DHCP IPv4 Appliances >> Full Sync All

TW-FR-994: Enhancements To Kea-DHCP Functionalities

Introduced a range of Kea-DHCP enhancements:

- DHCP Failover Support for Kea-DHCP Appliance: We now support DHCP failover peers for the Kea-DHCP appliance, both with and without certificates.
- Enhanced Subnet Failover Association: Support for the failover association within the subnet. This includes adding, editing, and importing failover associations and comes with an IPv4 Subnet Template.
- Incremental and Full Configuration Updates: Flexibility to perform both incremental updates and complete configuration changes with failover sections.
- Improved Logging and Log Rotation: Introduced log rotations and a new log at /var/log/kea-dhcp4-packets.log for enhanced tracking and system maintenance.
- Failover Client Class Association for Scopes: The IPAM auto associates the respective appliances with scopes in the failover section, offering better network management.
- Customizable Options: Allows you to define custom options and option spaces, enabling a more personalized experience.
- In-Built Multi-Threading Support: In-built support for multi-threading in high availability and failover modes.
- Audit and Statistical Reports: Ability to gain insights into your Kea-DHCP appliance's performance with our audit and statistical reports feature.
- Optimized Lease Parsing and Configuration Generation: Optimized the lease parsing flow and made changes to the configuration generation for improved performance.
- Support for DHCP Auto Objects: The new update includes support for DHCP Auto objects, enhancing network automation.
- Central Logging Support: To streamline log management, central logging support has been updated.

Navigation: Network Management >> DHCP Management >> DHCP Settings>> DHCP Failover Peers >> Create DHCP Failover Peer >> DHCP Appliance Type >> TCPWave KEA DHCP

TW-FR-1029: Preventing Duplicate MAC Addresses Within A Subnet

Added global option Allow Duplicate MAC Addresses in a Subnet in the Global Policy management page. By default, the value is set to Yes. The IP Address Management checks and verifies all the object additions and updates. When the value is set to No, the validation process ensures that no two objects within the same subnet have the same MAC address.

Navigation:

Administration >> Configuration Management >> Global Policy Management >> Allow Duplicate MAC Addresses in a Subnet

TW-FR-1039: Confirmation Message To Restart OR Reload DHCP Service

Added a new note message in the confirmation popup window that the DHCP service on the respective associated appliance must be restarted or reloaded when the add, edit, and delete operations are performed on all the DHCP core elements like IPv4 DHCP Subnet, IPv4 Option Template, IPv4 DHCP Appliance, IPv4 DHCP Objects, and Failover peer.

TW-FR-1046: Streamlined Options At Template Level

Modified parser logic to add unique DHCP options at the subnet level, which is common at the template level.

ChatBot Integration

TW-FR-171: Alice Chatbot

Introduced TCPWave's DDI & ADC AI chatbot - Alice. It is empowered by cutting-edge Natural Language Processing (NLP) technology. It swiftly addresses your queries and simplifies complex DDI and ADC operations, such as adding or deleting networks, subnets, objects, Resource Records, and DHCP Scopes.

To view the Alice bot across the application, you must set the global option Enable Alice DDI-Bot to Yes. By default, the option is set to No. Additionally, the global option would be updated for Alice Chatbot if the license is configured for Alice Chatbot service.

Navigation: TCPWave IPAM login >> Lower right across all IPAM pages

Network Management

TW-FR-673: Added Object Type Of 5G Phone

Added a 5G Phone option in the object type dropdown field while adding/updating IPv4 object/IPv6 object.

Navigation:

Network Management >> IPv4 Address space >>IPv4 Networks >> Subnet >> Create Object >> Object Type dropdown menu option

Network Management >> IPv6 Pools >> IPv6 Blocks >> IPv6 Subnets >> IPv6 Objects >> Create IPv6 Object >> Object Type dropdown menu option

TW-FR-803: Organization Level Authentication

Added the Authentication Configuration tab while editing the Organization. This tab is enabled when the global option Organization Level Authentication Configuration is set to Yes. By default, the option is set to No. Once the option is enabled, the system displays Authentication Types and Configuration Options. When you choose an authentication type, the organization's specific configuration determines the options for setting it up. However, if you don't specify the authentication type, the system resorts to using the global settings.

Navigation: Administration >> Configuration Management >> Organizations >> Edit Organization >> Authentication Configuration tab

Administration >> Global Policy management >> Organization Level Authentication Configuration

TW-FR-805: Merge & Split Networks

Added Merge option in the IPv4 Networks page. It allows you to merge two or more selected networks into one large network of available ranges. When the merge operation is performed, the selected network subnets are moved to the newly created network. Added Split option in the IPv4 Networks page. It allows you to perform a network split of selected network into smaller networks. When the split operation is performed, the selected network is distributed based on the new network ranges. New networks created after the split are named by concatenating the parent network name and ID of the network separated by '-. '

Integrating merge and split operations with the IA permission module is accomplished through a new IPv4 Network Delete/Split/Merge function. By default, all FADMs possess the capability to execute it.

Navigation:

Network Management >> IPv4 Address Space >> IPv4 Networks >> Context menu >> Merge

Network Management >> IPv4 Address Space >> IPv4 Networks >> Context menu >> Split

Network Management >> IPv4 Address Space >> IPv4 Networks >> Merge icon

Network Management >> IPv4 Address Space >> IPv4 Networks >> Split icon

TW-FR-947: Use Of Splunk HTTP Event Collector

Added Send Logs to Splunk HEC check box in the Central Logging page. By enabling this check box, the system displays the Splunk Host, HTTP Port, and HEC Token fields, using which you can send the IPAM logs to the Splunk HEC on the specified port. You are required to Enable Central Logging on the individual DNS/DHCP appliances.

Navigation: Administration Management >> Configuration Management >> Central Logging >> Send Logs to Splunk HEC checkbox

TW-FR-980: Network Hierarchy Enhancement

Added one more level hierarchy to represent objects hierarchically grouped by their class codes. Clicking on the group, the system displays the respective objects.

Navigation: Network Management >> Network Hierarchy >> Overview

TW-FR-984: Ability To Change Network & Subnet Mask

Added Mask slider option while editing the IPv4 Networks and IPv4 subnets. This option allows you to modify networks and subnets dynamically with the available ranges. The increase or decrease of the network size is based on the number of available IP addresses. You can re-adjust the mask length for the current networks and subnets from the Edit IPv4 Networks and Subnets page.

Navigation:

Network Management >> IP4 Address Space >> IPv4 Networks / IPv4 Subnets >> Edit Network /Subnet >> Mask slider

Network Management >> IP4 Address Space >> IPv4 Networks >> Edit Network >> Auto Create Reverse Zone checkbox

TW-FR-985: Extensible Attributes For Network Blocks

Added Extension attribute while creating and ending the address block page. It allows you to assign the extension values to the address block. Enable extension attributes to the address block while creating the extended attribute management page. Once this option is enabled, the system displays the added extension attribute in the add and edit address block.

Navigation:

Network Management >> Network Hierarchy >> Address Blocks >> Create Address Block >> Extension attribute

Administration >> Configuration Management >> Extended Attribute Management >> Create Extension Attribute Management >> Address Block Checkbox

TW-FR-1002: Workflow Management Support For Custom Admin User

Added Workflow Management Stage and Workflow Management Approve support for Custom Admin (CADM) users in the Administration Roles page. It allows CADM users to stage or approve the workflows. Modified the existing global option Enable Simple Workflow Management to specify that a Custom Admin can also stage or approve workflows, depending upon the workflow permissions. By default, the NADM/PADM users can stage workflows, and FADM/SADM users can approve or deny workflows.

Navigation: Administration >> Security Management >> Administrator Roles >> Custom Admin

TW-FR-1015: Reference Column In IPv6 Object Grid

Added a reference column in the IPv6 Object page. By clicking the specific reference record, an IP Address Associations popup window displays to view the number of records associated with the IP address.

Navigation: Network Management >> IPv6 Address Space >> IPv6 Pools >> IPv6 Blocks >> IPv6 Subnets >> IPv6 Objects >> References

TW-FR-1016: VRF To Device Mapping Report

Added VRF to Device Mapping Report in Discovery Report. This report displays the configured routers list for the selected virtual routing and forwarding (VRF). Additionally, it helps you understand the network topology, monitor the devices' status, and ensure efficient resource allocation. This enhanced visibility allows businesses to make informed decisions.

Navigation: Reports >> Discovery Reports >> VRF to Device Mapping Report

TW-FR-1027: IPv6 Subnet Split Feature

Added Split context menu option/icon in the IPv6 Subnet page. It allows you to perform a subnet split of selected subnets into smaller subnets. When the split operation is performed, the selected subnet is distributed based on the new subnet ranges.

Navigation: Network Management >> IPv6 Address Space >> IPv6 Pools >> IPv6 Blocks >> Ipv6 Subnets >> Context menu >> Split

TW-FR-1030: NameSpace Hierarchy

Added Namespace Hierarchy sub-menu link under Network Management. The namespace hierarchy simplifies DDI management, ensuring efficient control over network infrastructure. On clicking the menu link, the system displays the NameSpace Hierarchy UI, where you can easily visualize and navigate to parent-child zones. Added context menu options such as adding resource records, viewing zone templates, and performing force sync. The namespace hierarchy simplifies DNS management, ensuring efficient control over network infrastructure.

Navigation: Network Management >> NameSpace Hierarchy

TW-FR-1051: Validation Message While Creating Child Address Block

Implemented an error popup window feature while adding a Child Address Block page. This feature facilitates the addition of child address blocks in a sequential and ascending manner. In cases where the correct order is not followed, the system promptly triggers an error popup window for notification.

Navigation: Network Management >> Network Hierarchy >> Address Block>> Create Block >> Create Address Block

TW-FR-1052: Description Field in Adding Block

Added Description field in Add Seed Block popup window. The field defines the purpose of the seed block.

Navigation: Network Management >> Network Hierarchy >> Address Block >> Create Address Block >> Add Seed Block popup window >> Description field

TW-FR-1063: Cache Issues

Added a refresh icon in the network hierarchy page. It allows you to refresh the java cache.

Navigation: Network Management >> Network Hierarchy >> Overview >> Refresh icon

TW-FR-1065: Add Workflow Support For Network Split & Manage

Ability to stage a workflow for splitting/merging of network for PADM/NADM/CADM(custom admin with required permissions) users. The approval users can approve or deny the workflow.

Navigation:

Network Management >> IPv4 Address Space >> IPv4 Networks >> Split/ Merge options

Network Management >> IPv4 Address Space >> IPv4 Networks >> Split/ Merge Context menu options

TW-FR-1085: Remote SNMP Metrics & MIB Updates For DNS & DHCP Appliances

The remote SNMP metrics and MIB updates for DNS and DHCP appliances have been enabled. The following metrics are now enabled.

CPU Used %, Total Memory, Memory Used, Memory Free, Disk Used %, A, AAAA, CNAME, SOA, MX, PTR, SRV, NS, SUCCESS, SRVFAIL, FORMERR, NXDOMAIN, RECURSION, DHCPDISCOVER, DHCPREQUEST, DHCPACK, DHCPOFFER, DHCPINFORM, DHCPNACK, DHCPDECLINE, DHCPRELEASE

TW-FR-3148: Add Workflow Management Support For IPv6

Supported Workflow Management for the IPv6 Pools, IPv6 Blocks, IPv6 Object, IPv6 Subnet Groups, DHCP IPv6 Scopes, and IPv6 Subnet. Those with Workflow Management Approve Permission, like FADM/SADM/CADM, can utilize these options to stage workflow by Adding/Edit/Delete/ Add All, Multi Add, and Subnet Split options.

Navigation:

Network Management >> IPv6 Address Space >> IPv6 Pools >> IPv6 Blocks >> IPv6 Subnets >> IPv6 Objects >> Add/Edit/Delete option

Network Management >> IPv6 Address Space >> IPv6 Pools >> IPv6 Blocks >> IPv6 Subnets >> Add/delete/edit & Add All, Multi Add and Subnet Split option

Network Management >> IPv6 Address Space >> IPv6 Pools >> IPv6 Blocks >> Add/delete/Edit option

Network Management >> IPv6 Address Space >> IPv6 Pools >> Add/delete/Edit option

Network Management >> DHCP Management>> DHCP Scopes >> DHCP IPv6 Scopes >> Add/Delete/ Edit

Component Upgrades

TW-FR-1082: NSD Upgrade

Upgraded NSD to 4.7 version. The latest version of it includes features and bug fixes, of which a few are listed below:

- Added bash autocompletion script for nsd-control.
- Fixed to compile without ssl with dnstap-tls code.
- Dnstap tls code fixes.

TW-FR-1083: UNBOUND Upgrade

Upgraded Unbound 1.17.1 version. The latest version of it includes features and bug fixes, of which a few are listed below:

- Added max-query-restarts option. Exposes an internal configuration, but the default value retains Unbound's behavior.
- Added keep-cache option to unbound-control reload to keep caches.
- Fixed cachedb that does not store failures in the external cache.
- Fixed windows compile for libunbound subprocess reap comm point closes.

TW-FR-1086: BIND Upgrade

Update BIND from v9.18.9 to v9.18.16. The latest version of it features and bug fixes, of which a few are listed below:

- The overmem cleaning process has been improved, to prevent the cache from significantly exceeding the configured max-cache-size limit.
- The system test suite can now be executed with pytest along with pytest-xdist for parallel execution.

TW-FR-1142: Splunk Forwarder

Upgraded Splunk Forwarder from v9.0.4 to 9.1.0.1, which includes clearing the notification to dismiss the error.

TW-FR-1143: Zeek Upgrade

Upgraded Zeek from v5.1.1 to v5.2.1. The latest version of it includes the bug fixes, of which a few are listed below:

- Fixed the crash issue on the Linux system during parsing.
- The issue of the AF_Packet plugin masking the tp_vlan_tci values received from the kernel is fixed.

TW-FR-1144: Suricata Upgrade

Upgraded Suricata from v6.0.8 to v7.0.0. The latest version of it includes new features and fixes a number of important issues, of which a few are listed below:

- Added HTTP/HTTP2 new keywords for header inspection.

- Added VLAN support extended from 2 to 3 layers.
- Improved hash calculation using Rust crypto.

TW-FR-1145: Openssh Upgrade

Upgraded Openssh from v9.2 to 9.3. The latest version of it includes a security fix.

TW-FR-1146: Kernel Upgrade

Upgraded Kernel from v5.7.9 to v6.3.2. The latest version of it includes the bug-fix release and fixing a number of important issues, of which a few are listed below:

- Fixed deadlock in ksmbd_find_crypto_ctx().
- Added missing locking to protect against concurrent rx/status calls.

Global Options

Added the following global options:

Name	Description
Allow Duplicate MAC Addresses in a Subnet	Controls the presence of duplicate MAC addresses in a subnet in the system.
Configuring In-Memory Storage of DDNS Updates for Remote Retrieval	The option allows specifying the number of DDNS updates per zone to be stored in memory after publishing them to remote systems. This feature enables the IPAM to retain a certain number of updates in its memory. When a remote system requests missing updates, the IPAM can read from the stored queue and resend them to the remote, ensuring comprehensive synchronization. Accepts a value between 1000 and 1000000.
Delete GSLB NS Records	This option allows for deleting GSLB NS records when the appliance goes inactive. If you choose Yes, the GSLB NS records will be deleted, while selecting No will prevent the system from deleting the GSLB NS records.
Enable Debug Logging for DDNS Messages	Log DNS Dynamic updates debug messages.
Enable Alice DDI-Bot	Enables Alice DDI-Bot interface in the TCPWave IPAM. Default option is set to No.

Name	Description
Enhanced DDNS Update Propagation with Update Counters	The option allows for the activation or deactivation of the enhanced DDNS update propagation logic, which utilizes update counters. Enabling this option ensures that each DDNS update includes a counter mechanism to ensure its successful transmission and proper update on the remote DNS appliance.
Enable RR Count Validation During DNS Sync	When 'Enable RR Count Validation During DNS Sync' is set to 'Yes', DNS sync validates RR count in IPAM-generated and remote zone files twice before copying to named folders. Discrepancies trigger sync cancellation to ensure data integrity.
Maximum DNS Sync Timeout for Clearing Queued DDNS Updates (Minutes)	Maximum DNS sync timeout to efficiently clear queued Dynamic DNS (DDNS) updates on non-managed IPAMs during DNS synchronization. Accepts a value between 5 and 120 (Minutes).
Max RR Count Difference in DNS Sync: IPAM vs. Remote Zone Files	Define max RR count difference between IPAM & remote zones during DNS sync for data accuracy. Accepts a value between 0 and 100000.
Number of days to preserve ADC reports table data	Number of days to preserve ADC reports table data. Accepts a value between 1 and 365.
Organization Level Authentication Configuration.	By default, the option is set to No. When the global option is set to Yes, the authentication configuration at the organization level is enabled.
Save ADC Reports Data	Enabling the global option allows for implementing a feature that facilitates the storage of ADC Audit data in the database.

Support Requests

Ticket ID	Description
TW-SR-382	Modified the code to resolve the BGP route issue from neighbors. The system's BGP and Zebra services startup order is fixed and cannot be altered.
TW-SR-949	Implemented backend logic to address the issue of non-managed zone data not replicated in the named.conf files when downloading the configurations from the GUI. This logic ensures that the non-managed zones are included in the configuration file.
TW-SR-1239	Added DDNS Update Counters context menu option in the Managed DNS Zones Page. On clicking this option, the system displays the zone's current DDNS update counters on IPAM and Remotes. On adding the resource records to the specified managed DNS zone, the DDNS update counter value is increased on IPAM and remote. Added the following global options: Enhanced DDNS Update Propagation with Update Counters: This option allows activating or deactivating the enhanced DDNS update propagation logic, which utilizes update counters. Enabling this option ensures that each DDNS update includes a counter mechanism for successful transmission and proper update on the remote DNS server. By default, the value is set to No. Configuring In-Memory Storage of DDNS Updates for Remote Retrieval: This option specifies the number of DDNS updates per zone to be stored in memory after publishing them to remote systems. It enables the IPAM to retain a certain number of updates in its memory. When a remote system requests missing updates, the IPAM reads from the stored queue and resends them to the remote, ensuring comprehensive synchronization. By default, the value is set to 10000. Navigation: Administration >> Configuration Management >> Global Policy Management >> Enhanced DDNS Update Propagation with Update Counters Administration >> Configuration Management >> Global Policy Management >> Configuring In-Memory Storage of DDNS Updates for Remote Retrieval Network Management >> DNS Management >> Managed DNS Zones >> Context menu option >> DDNS Update Counters
TW-SR-1283	Modified backend logic to fix the discovery engine issues.

Ticket ID	Description
TW-SR-1311	Fixed multiple network hierarchy issues reported at the block, network & subnet level.
TW-SR-1328	Implemented a backend logic that ensures the preservation of the existing IPs while appending the newly added ones.
TW-SR-1337	Provided a data SQL file after converting and importing in TCPWave IPAM.
TW-SR-1354	Modified the backend logic to take the network mask which is the same as the actual router subnet mask and added an option in the UI so that you can control this behavior.
TW-SR-1360	Added Download icon in the DNS Statistics Log tab. It allows you to download all logs with respective dates and times. Additionally, this option is also added in the DHCP and IPAM Statistics Log tab. **Navigation:** Infrastructure management >> Performance Management >> TCPWave DNS/DHCP/IPAM Statistics >> Logs tab >> Download icon
TW-SR-1371	Previously, upon completion of RPZ updates, our process involved performing full DNS synchronization internally across all DNS remotes. To enhance efficiency, incremental logic was implemented. However, the incremental process exhibited slowness due to the significant number of remotes requiring updates. To address this, multithreading logic is implemented that allows parallel transmission of incremental updates to remotes.
TW-SR-1376	Modified the backend logic changes to download the Suspicious Query Log (ML)" log.
TW-SR-1393	Modified the backend logic to display the Adhoc Admin Audit by Name report.
TW-SR-1395	Removed validation constraints linked to RRL parameters, enabling the editing of other parameters.
TW-SR-1396	The issue of DNS statistics for the DNS query and DNS response charts has been fixed for the DNS proxy appliances.
TW-SR-1397	Modified the backend logic and schema changes to the IPAM Subnet Split.
TW-SR-1401	Updated DB and backend logic to fix the deleteadminpermission CLI issue.
TW-SR-1412	Added a backend check to avoid adding the permission for the non-permittable function.
TW-SR-1447	Added a script file to reload syslog-ng configuration on file rotation.

Ticket ID	Description
TW-SR-1452	In previous versions, the merging process lacked consideration for the secondary domain. This issue has been successfully resolved by implementing a backend check in the stored procedure, ensuring accurate subnet merging.
TW-SR-1468	The issue of DHCP configuration generation failing due to syntax errors has been fixed by Updating the backend validation to the MAC address for DHCP objects.

Change Requests

Ticket ID	Description
TW-CR-5117	Introduction of new validation for PTR records during bulk import.
TW-CR-5221/TW-SR-977	Modified frontend validations to enable the utilization of special characters within the Create Non-Managed Zone page for zones. This enhancement permits the creation of non-managed DNS zone names that incorporate special characters. **Navigation:** DNS Management >> DNS Zones >> Non-Managed DNS Zones >> Create Non-Managed DNS Zones >> Basic Zone information tab >> Name
TW-CR-5409	The issue of the search API, when pointed to a member IPAM in an HA cluster, has been fixed.
TW-CR-5428	Modified the backend logic to enable batch execution of commands within a PowerShell script, accommodating 1000 commands per batch. This adjustment has led to a significant decrease in request volume, resulting in a notable enhancement of CPU utilization optimization for the Microsoft server.
TW-CR-5577	Implemented an efficient approach while updating the RPZ policy file. When the RPZ Policy file is updated, the system sends incremental updates to the remote systems. This ensures that the changes made to the RPZ Policy file are transmitted to the remotes, significantly reducing the network traffic and processing overhead. The remote systems apply incremental updates to their RPZ Policy file, keeping them in sync with the latest changes. This approach minimizes the downtime and resource consumption associated with full syncs while maintaining consistency and accuracy across all remote systems.
TW-CR-5509/TW-CR-5691	Updated the backend logic to fix the subnet to object inheritance extension attribute issue.
TW-CR-5774	In the zone's template page, there's a field called MNAME. Previously, only the

Ticket ID	Description
	Fully Qualified Domain Name of the master server was accepted as valid input. If the master servers included a stealth master, MNAME was set to the master server's FQDN. If not, MNAME was 'Default.' Now, enhanced the options for MNAME to accept any valid FQDN when using a stealth master among the selected master servers.
TW-CR-5779	Deleted the dependency of the network not getting deleted when there is an ACL reference to the network.
TW-CR-5790	Updated backend and DB logic to support adding administrative permissions for AD sites and services function.
TW-CR-5827	Modified backend logic to support 255 characters length for a subnet group.
TW-CR-5857	The vendor-class-identifier string has been missing in the configuration file. Generation as part of the regression code changes for the subnet-level DHCP options support.
TW-CR-5875	The reservation objects of the IPv4 subnet are not being added to the list if we have only manual objects defined in the IPv4 subnet and made respective database changes to get into the config generation list.
TW-CR-5885	Modified backend logic to sort IP address of address blocks in ascending order.
TW-CR-5894	Modified frontend logic to create the network from the address block page.
TW-CR-5938	Modified the backend code to resolve the issue related to firmware patch deployment, causing the system to experience command hang issues when applying firmware patches.
TW-CR-6039	Provided a refresh button to refresh the Java cache.
TW-CR-6059	Added an option for references of IPv6 Object at Global search.
TW-CR-6092	Modified code to support files exceeding 1GB in size. Additionally, it fixed the problem with firmware patch uploads, where the user interface was incapable of accepting files larger than 100MB.
TW-CR-6095	Modified the backend logic to display complete data of scheduled DHCP Lease report.
TW-CR-6157	Added support to give permissions to the IPv4 Subnet based on their IPv4 subnet group. After selecting a subnet group, the system displays the grid with the respective subnet. Selecting the subnet from the grid allows you to assign permission to the administrator or administrator group.

Ticket ID	Description
	Navigation: Administration >> Security management >> Administrator Permission
TW-CR-6229	Modified backend logic to permit record level.
TW-CR-6244	Modified the backed logic to set the zone template default TTL value.
TW-CR-6261	Modified the backend logic to store the CAA record of the iodef tag.
TW-CR-6436	Modified the backend logic to prioritize the first name if the last name is missing and the last name if the first name is missing. This maintains user continuity when either name is absent. User creation is prohibited only if both names are missing.
TW-CR-6506	Modified the backend logic to fix the PTR traverse of the newly added records after DNS sync.
TW-SR-1508/TW-CR-6512/6513/6514	Fixed the issue of initiating parallel DNS Syncs using monit restart timsdns on remote and sync from UI. Enhanced the log feature to differentiate the logs between DNS full sync, force sync, and user name. Added a validation message to check if sync is in progress when full sync is initiated from Master IPAM if we create a record/object on member IPAM.
TW-CR-6737	Modified the backend logic related to ACL Edit, causing an incomplete DNS Config update. Subsequent attempts to perform DNS Sync fail, with no response from the remote.
TW-CR-6738	Modified the backend logic for DNS log channel editing, resulting in prolonged DNS Sync duration for remote systems, with no response following the log channel edit.

CLI Updates

#	Description
1	Added the following CLI's: ▪ addmsdhcpexclusionrange ▪ addadccluster ▪ addadchealthtemp ▪ addapplication ▪ deactivatesessiontoken ▪ deletemsdhcpexclusionrange ▪ deleteapplication ▪ deleteadccluster ▪ deleteadchealthtemp ▪ editadccluster ▪ exportmsdhcpexclusionranges ▪ exportipv6dhcpoptiontmpl ▪ editapplication ▪ formremotecluster ▪ formimportremotecluster ▪ generatesessiontoken ▪ importmsdhcpexclusionranges ▪ ipv6splitsubnet ▪ listldapusers ▪ listsessiontoken ▪ listmonitoredservices ▪ listadchealthtemp ▪ listapplication ▪ listadccluster ▪ mergenetwork ▪ resetremotecluster

#	Description
	▪ resteremoteslusterstate ▪ restartremotecluster ▪ setipv6revzoneautoforcesync ▪ setipv6revzoneexcludesync ▪ splitnetwork ▪ syncslbserver ▪ updatemsserverpwd ▪ validateupn ▪ updateremotecluster
2	Modified the following CLIs: ▪ addbackendnode ▪ addfrontendmembers ▪ addpoolassociations ▪ addslbfrontend ▪ addslbbackend ▪ adcappliance ▪ addgslbtrafficrule ▪ addslbbackend ▪ addrr ▪ deletefrontendmembers ▪ deleterr ▪ editpoolassociations ▪ editnetwork ▪ editsubnet ▪ editslbbackend ▪ editfrontendmembers ▪ editrr ▪ getdnsacl

#	Description
	▪ getzoneacl ▪ listdnsacl ▪ login ▪ setdnsacl ▪ setzoneexcludesync ▪ setzoneautoforcesync ▪ syncdhcpserver

REST APIs

#	Operation	REST API
Added the following REST APIs		
1	GET	/rest/adcdashboard/serverconnections
		/rest/adcdashboard/clientconnections
		/rest/newchart/adcconn
		/rest/adcdashboard/adccounter
		/rest/adcdashboard/top10cpuconsumers
		/rest/slbAppliance/getADCToptalkers
		/rest/v6server/get
		/rest/ipv6object/references
		/rest/v6dnsserver/search
		/rest/v6dnsserver/references
		/rest/object/getObjectsGroupByType
		/rest/namespace/hierarchy/initialize
		/rest/namespace/hierarchy/getParentZones
		/rest/namespace/hierarchy/getConnectedChilds
		/rest/namespace/hierarchy/getTemplateInfo
		/rest/namespace/hierarchy/getZoneStatus
		/rest/namespace/hierarchy/getRootOrg
		/rest/hierarchy/reloadHierarchyCache
		/rest/wafTemplate/list
		/rest/wafTemplate/get

#	Operation	REST API
		/rest/application/list
		/rest/application/get
		/rest/adcreports/adcreportlist
		/rest/adcreports/topslbapplianceconnrpt/
		/rest/adcreports/adctoptalkerrpt/
		/rest/adcreports/wafattackrpt/
		/rest/adcreports/alltemplatelist/
		/rest/adcreports/adcAuditreportgridlist
		/rest/adcreports/slboptiontempllist/
		/rest/adccluster/search
		/rest/adcHealthTemplate/get
		/rest/adcHealthTemplate/delete
		/rest/adccluster/list
		/rest/adccluster/get
		/rest/adccluster/delete
		/rest/adccluster/search-references
		/rest/application/search
		/rest/application/listbyorg
		/rest/application/references
		/rest/organization/get_auth_details
		/rest/organization/get_auth_options
		/rest/user/getOrganizations
		/rest/application/search-references
		/rest/slbAppliance/applianceInfo
		/rest/adcHealthTemplate/search-references
		/rest/slbAppliance/remoteDebugging
2	POST	/rest/namespace/hierarchy/load
		rest/network/split
		rest/network/merge
		/rest/dnstools/dnsdiag
		/rest/clouddnsprovider/tsigkeyupdate
		/rest/application/add

#	Operation	REST API
		/rest/application/edit
		/rest/application/delete
		/rest/wafTemplate/add
		/rest/wafTemplate/edit
		/rest/wafTemplate/delete
		/rest/organization/update_auth_option
		/rest/adcHealthTemplate/add
		/rest/adcHealthTemplate/edit
		/rest/adccluster/search
		/rest/adccluster/add
		/rest/adccluster/edit
Modified the REST APIs		
3	GET	/rest/object/rrlist
		/rest/reports/msactiveusersrptgrid
		/rest/reports/dhcpAppliancePoolUtilized
		/rest/home/getLogs
		/rest/clouddnsprovider/update_template
		/rest/acls/list
		/rest/acls/getreferences
		/rest/clouddnsprovider/update_template
		rest/acls/get
4	POST	rest/dhcpserver/generateConfig
		rest/dhcpserver/syncall
		rest/network/edit
		rest/subnet/edit
		/rest/v6scope/autoprovision
		/rest/v6scope/delete
		/rest/ipv6block/add
		/rest/ipv6block/delete
		/rest/ipv6block/edit
		/rest/ipv6object/add
		/rest/zone/update
		/rest/ipv6object/delete-multiple

#	Operation	REST API
		/rest/ipv6object/edit
		/rest/ipv6pool/add
		/rest/ipv6pool/delete
		/rest/clouddnsprovider/tsigkeyupdate
		/rest/ipv6pool/edit
		/rest/ipv6subnetgroup/add
		/rest/ipv6subnetgroup/deleteAll
		/rest/ipv6subnetgroup/update
		/rest/ipv6subnet/add
		/rest/authPermission/create
		/rest/ipv6subnet/addall
		/rest/ipv6subnet/multiadd
		/rest/ipv6subnet/split
		/rest/ipv6subnet/delete
		/rest/ipv6subnet/edit
		/rest/workflow/add
		/rest/workflow/modify
		/rest/workflow/delete
		/rest/network/merge
		/rest/dhcpserver/add
		/rest/dhcpserver/delete
		/rest/acls/create
		/rest/acls/update
		/rest/ipv6object/add
		/rest/ipv6block/edit