TCPWave IP Address Management System®

Release Notes

Version 11.32P4

August 2022

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 state the new features, improvements, and stability fixes included in the TCPWave DDI v11.32P4 release are summarized below. The intended audience for this information consists of those who need to understand the changes in this release, including administrators responsible for upgrading TCPWave IPAM and remote appliances.

Feature Requests/Enhancements

Information Security Upgrades

TW-FR-840: Jackson upgrade to v2.13.2

Upgraded the Jackson version to v2.13.2, and a few of the changes of the upgraded version are listed below:

- Java 8 forms the baseline for almost all modules such as minus jackson-annotations, jackson-core streaming API, json, and jackson-jr.
- Introduced a new set of components - JAXB, JAX-RS, JSON-P.

TW-FR-844: BIND upgrade to v9.16.30

Upgraded the BIND version from v9.16.27 to v9.16.30, and a few of the changes of the upgraded version are listed below:

- Designed the fetches-per-server quota to auto-adjust when an authoritative server times out too frequently.
- Addressed the issue of DNSSEC-signed catalog zones that were not processed correctly.

TW-FR- 850: NSD upgrade to v4.5.0

Upgraded the NSD version to v4.5.0, and a few of the changes of the upgraded version are listed below:

- Added IXFR out functionality which enables the NSD to respond to IXFR queries and serve IXFR transfers downstream.
- Fixed minor bugs related to code analyzer large value with assertion, spelling error in a comment in svcbparam_lookup_key, etc.
- Updated cirrus script FreeBSD version.

TW-FR- 851: UNBOUND upgrade to v1.16.0

Upgraded the UNBOUND version to v1.16.0, and a few of the changes of the upgraded version are listed below:

- Added essential support for Extended DNS Errors (EDE).
- Fixed minor bugs related to cache invalidation issue with CNAME+A, ensured uniform handling of spaces and tabs when parsing RRs, etc.

TW-FR- 852: OpenSSL upgrade to v1.1.1p

Upgraded the OpenSSL version from 1.1.1 to v1.1.1p, which fixed the AES OCB failure issue to encrypt some bytes on 32-bit x86 platforms.

TW-FR- 853: MariaDB upgrade to v10.2.44

The MariaDB version is upgraded from v10.2.40 to v10.2.44, including all the security, bug, and optimization fixes.

TW-FR- 854: Net SNMP upgrade to v5.9.1

The Net SNMP version is upgraded to v5.9.1, allowing monitoring of a broader set of hosts and devices.

TW-FR-856: Splunk forwarder to v9.0.0

The Splunk forwarder version to v9.0.0 provides a new user interface that allows administrators to author, preview, and deploy ingest-time rules for filtering, masking, and routing events, new features related to role-based field filtering, and health report config tuning, etc.

DNS Threat Management

TW-FR-741: XGBoost Model

TCPWave's DNS TITAN is upgraded with the state-of-the-art machine learning (ML) model – **XGBoost** (eXtreme Gradient Boosting). Using this model, you can detect and mitigate DNS anomalies. When you enable anomaly detection using XGBoost within the TCPWave application, the system initializes the detection service, sniffs the traffic, logs the suspicious traffic, and generates alerts.

Navigation: Network Management >> DNS Management >> DNS Security >> DNS Threat Management >> NSM Template >> Add/Edit >> Enable Anomaly Detection >> XGBoost Model

TW-FR-721: DNS ACL Blackhole Mechanism

TCPWave's DNS TITAN functionality is enhanced to automatically block anomalous traffic on DNS Caches using the Blackhole ACL option. In the TCPWave IPAM application, if a source IP is declared malicious by the Network Security Monitoring (NSM) platform, it is added to the blackhole option section of the DNS appliance configuration. To block the anomalous traffic, enable the following global options:

- Automatically block anomalous traffic on DNS caches: By default, this global option is set to No; you must set it to Yes to block the anomalous traffic.
- Anomalous traffic blocking methodologies using Blackhole ACL, Suricata Rule, Switch-Port Shutdown.

Once the above global options are set to Yes, you can remove the blocked sources after the specified time interval (hours) using the DNS Network Security Monitoring Autoblock Purge Interval global option. By default, the time interval is 24hrs.

Navigation: Administration >> Configuration Management >> Global Policy Management >> Automatically block anomalous traffic on DNS cache.

Administration >> Configuration Management >> Global Policy Management >> Anomalous Traffic Blocking Methodologies >> Blackhole ACL

Administration >> Configuration Management >> Global Policy Management >> DNS Network Security Monitoring Autoblock Purge Interval

TW-FR-815: Forecasting Charts Using Machine Learning

TCPWave's monitoring framework now uses the **Seasonal Autoregressive Integrated Moving Average** (SARIMA) Time Series Machine Learning model to analyze real-time network telemetry data and forecast the metrics. Performance metrics such as CPU, Disk and Memory Usages, Queries Per Second (QPS), and Leases Per Second (LPS) are forecasted based on the daily, weekly, and monthly frequencies. On setting the global option **Enable ML Forecasting Charts** to Yes, the system displays the ML forecasted data in the grey shade. To view the instant plots, you must execute the following schedule jobs for the first time after setting the global option to Yes.

- CPUQPSLPSForecastDaily
- CPUQPSLPSForecastHourly
- CPUQPSLPSDailybestparamwriter
- CPUQPSLPSHourlybestparamwriter

Navigation: Infrastructure Management >> Performance Management >> IPAM Statistics >> Resource Utilization >> CPU Utilization, Memory Utilization, Disk Utilization

Infrastructure Management >> Performance Management >> DNS Statistics >> CPU, Disk, Memory Utilizations QPS

Infrastructure Management >> Performance Management >> DNS Statistics >> CPU, Disk, Memory Utilizations LPS

Administration >> Configuration Management >> Global Policy Management >> Enable ML Forecasting Charts

TW-FR-837: TCPWave Outlier Detection

Added a new global option **Enable TCPWave Outlier Detection** for CPU, Memory, Disk, QPS, and LPS in the Global Policy Management. TCPWave's monitoring framework uses Median Absolute Deviation (MAD) algorithm to detect outliers in performance metrics of DDI (CPU, Disk & Memory usage), DNS (QPS), and DHCP (LPS) appliances, respectively. The outlier detection process is initiated based on the global policy configuration. By default, the global option is set to No. When the global option to Yes and if there are any outliers related to performance metrics for consecutive 15 minutes, the system generates a critical alert in the Current Alarms section.

Navigation: Infrastructure Management >> Fault Management >> Current Alarms >> CRITICAL

Administration >> Configuration Management >> Global Policy Management >> Enable TCPWave Outlier Detection

TW-FR-839: Auto Turn-off Switch Ports of Malicious Systems Using Threat Intelligence

TCPWave's DNS TITAN functionality is enhanced to automatically shut down the infected applications' switch ports using TCPWave's IPAM Network Security Monitoring (NSM) platform. The auto-detection

of the malicious source IPs is done using Atlantis or XGBoost machine learning models that are part of anomaly detection and generate alerts related to auto block and switch port shut down in the Current Alarms section.

Navigation: Administration >> Configuration Management >> Global Policy Management >> Automatically block anomalous traffic on DNS cache

Administration >> Configuration Management >> Global Policy Management >> Anomalous Traffic Blocking Methodologies >> Switch-Port Shutdown

Remote High Availability

TW-FR-792: Add support for Remote HA

Added a new feature to form a cluster of two remote appliances to provide uninterrupted DNS and/or DHCP services. When the users form a cluster using two nodes, the underlying services are provided using a virtual IP, which interacts with the cluster's active member node. So, when a failover occurs, the passive node takes over and provides the services without interruption.

Navigation: Network Management >> DNS Management >> TCPWave IPv4 DNS/DHCP Appliances >> Grid >> Context menu option >> Administration >> Cluster Administration

Fault Management

TW-FR-709: Automated Email Alert when a DNSSEC KSK Expires Within 30 days

Added **DNSSEC_KSK_EXPIRY_CHECK** monitoring check in the monitoring services interface. To perform the check, ***MonitoringCertExpiryChecker*** scheduled job is executed every day at 00.05 AM. Enable and Disable context menu options are added in the search results grid. The monitoring check fetches all the zone KSK values and checks the expiry days. The system generates a critical alert if the value is less than the critical threshold defined in the monitored service. If the value is between critical and warning thresholds, the system generates a warning alert, and an ok alert is generated if the value is less than the warning threshold. When the service is disabled, the alerts associated with this service get deleted, and the scheduled job is not executed.

Navigation: Infrastructure Management >> Fault Management >> Monitoring Services >> Threshold Name >> DNSSEC_KSK_Expiry_Check

TW-FR-771: Send IPAM alerts via Messaging Apps

Added a new feature in TCPWave's IPAM Alarm Subscriptions section, wherein the network administrators get notified about the critical or warning alerts based on the monitoring service category and components (DNS, DHCP, IPAM, Network, etc.) through the following messaging platforms.

- Email
- Google Chat

- Microsoft Teams
- Pager Duty
- Slack
- Telegram

Navigation: Infrastructure Management >> Fault Management >> Alarm Subscriptions >> Add/Edit >> Messaging Properties >> Messaging Apps

TW-FR-746: Monitoring with Force Recheck

Added **Force Recheck** context menu option in the Current Alarms section that permits you to manually re-invoke a monitoring check and update an alert's status. When you perform force recheck, the monitoring engine sends the updated alert into the existing notification queue from which notifications are inserted into the database as per the **Monitoring Notification Processing Interval** defined in the Global Policy Management. By default, the processing interval is 2 minutes. You must refresh the Current Alarms section to view the latest alert.

Navigation: Infrastructure Management >> Fault Management >> Current Alarms >> Context Menu >> Force Recheck

Administration >> Configuration Management >> Global Policy Management >> Monitoring Notification Processing Interval

Network Discovery

TW-FR-587: Discovery Tasks Tab - Subnet

Added **Discovery Tasks** tab in the Subnet page which enables you to view the discovery tasks specific to a subnet and associated discovery results within a subnet.

Navigation: Network Management >> IPv4 Address Space >> IPv4 Networks >> IPv4 Subnets >> Edit >> Discovery Tasks

TW-FR-700: Global Option: Run Discovery - All Networks

Introduced a new global option **Enable Auto Discovery** to perform the auto-discovery of all the networks, subnets, and objects when it is set to Yes. By default, the option is set to No.

Navigation: Administration >> Configuration Management >> Global Policy Management >> Enable Auto Discovery

TW-FR-759: Import Device Credentials

Added **Import** option in the Device Credentials and Exclusions page which allows you to import the device information such as device address, device type, vendor, platform, IP address, exclusion type etc.

Navigation: Network Management >> IPv4 Network Discovery >> Discovery Agent >> Edit >> Device Credentials /Exclusions >> Import

Dashboard

TW-FR-865: Capacity Planning Dashboard

Added the **Capacity Planning Dashboard** in the Dashboard section, which allows you to get a quick snapshot of the top parameters such as CPU Usage, Disk Utilization, Memory Usage, DNS QPS, and DHCP LPS across the DDI infrastructure. It helps you to analyze, monitor, and alter network capacity patterns of your organization.

Navigation: Dashboard >> Capacity Planning Dashboard

Network Management

TW-FR-336: Centralized Syslog-NG Configuration Through Templates

Added the **Global DNS Syslog-NG Configuration** page under the DNS Configuration section. You can simultaneously update the configurations on all IPv4 and IPv6 DNS appliances using this interface. If you update the Global DNS Syslog-NG configuration, the system overrides the existing Syslog-NG settings specific to individual DNS appliances.

Added the **Global DHCP Syslog-NG Configuration** page under the DHCP Configuration section. Using this option, you can simultaneously update the configurations on all IPv4 and IPv6 DHCP appliances. If you update the Global DHCP Syslog-NG configuration, the system overrides the existing Syslog-NG settings specific to individual DHCP appliances.

Navigation: Network Management >> DNS Management >> DNS Configuration >> Global DNS Syslog-NG Configuration

Navigation: Network Management >> DHCP Management >> DHCP Settings >> Global DHCP Syslog-NG Configuration

TW-FR-407: Centralized TACACS+ Configuration Through Templates

Added **Global DNS TACACS+ Configuration** and **Global DHCP TACACS+ Configuration** pages in DNS & DHCP Configurations section. Using these respective interfaces, you can simultaneously update the LDAP and TACACS+ settings on all IPv4 and IPv6 DNS and DHCP appliances.

Navigation: Network Management >> DNS Management >> DNS Configuration >> Global DNS TACACS+ Configuration

Navigation: Network Management >> DHCP Management >> DHCP Settings >> Global DHCP TACACS+ Configuration

TW-FR-578: Ability to view the size/number of pending DDNS updates from Remotes

Added **External DDNS Updates** context menu option in TCPWave DNS IPv4 appliances grid section. On clicking the option, you can view the count of the pending external updates on the remote appliances.

Note: The system won't be able to fetch and display the count of the pending updates if the script is not present on the remote. This feature has its main usage when the IPAM is down.

Navigation: Network Management >> DNS Management >> DNS Appliances >> TCPWave DNS IPv4 appliances >> Context Menu >> Information >> External DDNS Updates

TW-FR-592: Improve Results page for Import Wizard

Improved the results page of the Import Wizard section in terms of validation messages.

Navigation: Network Management >> Import Wizard

TW-FR-611: Update Config option

Added **Update Config** context menu option in TCPWave DNS IPv4 appliances grid section. On clicking the option, the system displays a validation message to perform DNS configuration on the selected appliance. On clicking Yes, the system updates the named.conf and rndc.conf for the BIND, unbound.conf for UNBOUND and nsd.conf for the NSD appliances respectively.

Navigation: Network Management >> DNS Management >> DNS Appliances >> TCPWave DNS IPv4 appliances >> Context Menu >> Administration >> DNS Config >> Update Config

TW-FR-604: Support of a BGP ASN database table

Since Border Gateway Protocol uses ASN to identify the system, TCPWave added **Autonomous System Number** (ASN) page in the IPv4 Address Space section. You can perform add, edit and delete operations from the TCPWave's ASN interface.

Navigation: Network Management >> DNS Management >> DNS Appliances >> TCPWave DNS IPv4 appliances >> Context Menu >> Administration >> DNS Config >> Update Config

TW-FR-686: Import/Export Wizard for Autonomous System Number

Added **Autonomous System Number** function in the import and export wizards, to allow the bulk import/export the data related to ASNs of various organizations or a specific organization.

Navigation: Network Management >> Data Wizards >> Import/Export Wizard >> Autonomous System Number

TW-FR-693: View Active Leases In DHCP Scopes Tab

Added **Active Leases** icon in DHCP Scopes tab and Global Search page. On clicking the icon, the system displays the total count of active leases of the selected subnet.

Navigation: Network Management >> IPv4 Address Space >> IPv4 Networks >> IPv4 Subnets >> Edit >> DHCP Scopes tab >> Active Leases

Dashboard >> Blue Ribbon >> Global Search >> IPv4 Subnets >> Edit >> Active Leases

TW-FR-702: Query Alternate DNS Servers

When the Query Alternate DNS Servers feature is configured, a TCPWave DNS Proxy Appliance that is authoritative for a zone being queried will query one or more alternate DNS servers instead of returning an NXDOMAIN response to a DNS client. Customers can use this feature in cases in which they have an internal authoritative DNS Appliance and want it to be able to query one or more other DNS appliances that are authoritative for the same zone or zones. These other DNS servers could be from business partners or, for example, third parties in a public cloud computing service, such as vendors in the Amazon Web Services (AWS) Marketplace.

Navigation: Network Management >> DNS Management >> DNS Proxy Zones >> Query Alternate Resolvers

TW-FR-718: TTL should be Null, not 1200 by default

Previously, the default value displayed in the TTL field was 1200 in IPv4 Objects, IPv6 Objects, IPv4/IPv6 Reverse Zone, DNS Root Zone, DNS Proxy Root Zone, and Zone Normal RRs pages. Now, the default value is changed to NULL.

TW-FR-719: Get rid of Communication-key

Previously, server-level TSIG was used to encrypt the notifications and other communications. Now the functionality is modified, and notifications are based on the IP address.

TW-FR-725: RR Support in Cloud Providers

Added the support for the following resource records in the respective cloud providers.

Cloud Providers	Resource Records
AWS	CAA, SPF
Azure	CAA
DynDNS	DNAME, CAA, SPF, DS, LOC, SSHFP, TLSA, IPSECKEY
Google	CAA, DS, SPF, TLSA, SSHFP, IPSECKEY

TW-FR-734: Object Grid Enhancements to show all RRs, Views

Added **Reference Column** in the IPv4 Objects grid. On clicking the reference link, the system displays the details of the IP address references, such as type of RR, class, TTL, etc., in the IP Address Associations pop-up.

Navigation: Network Management >> IPv4 Networks >> IPv4 Subnets >> IPv4 Objects >> References

TW-FR-736: Parallel Processing of zone bulk updates from IPAM

Previously, the serial processing technique was used to process the zone updates. Now the functionality is deprecated, and zone updates are performed through parallel processing, which helps reduce the time for the zone template updates; hence, the optimization is improvised.

TW-FR-846: DDI Migration Wizard

Added the **DDI Migration Wizard** page in the Data Wizard section. This interface provides the functionality to import the data from zone files and XML, as per the BIND and MS file format, into the TCPWave environment.

Navigation: Network Management >> Data Wizards >> DDI Migration Wizard

Reports Management

TW-FR-706: DNS Daily Peak Hour Query Rate By Appliance Report

Added **DNS Daily Peak Hour Query Rate By Appliance** report in DNS Reports section. This report displays the peak DNS Query rate at the busiest hour within a day.

Navigation: Reports >> DNS Reports >> DNS Daily Peak Hour Query Rate By Appliance

TW-FR-713: IPv6 DHCP Option Template Audit

Added **IPv6 DHCP Option Template Audit** report in IPv6 DHCP Reports section that provides complete audit information regarding operations performed on the DHCP IPv6 Option Template by an administrator.

Navigation: Reports >> IPv6 DHCP Reports >> IPv6 DHCP Option Template Audit

TW-FR-714: IPv6 DHCP Appliance Audit

Added **IPv6 DHCP Appliance Audit** report in IPv6 DHCP Reports section that provides complete audit information about the operations performed by an administrator on a specific IPv6 DHCP appliance or All appliances.

Navigation: Reports >> DHCP Reports >> IPv6 DHCP Reports >> IPv6 DHCP Appliance Audit

TW-FR-715: IPv6 DNS Appliance Audit

Added **IPv6 DNS Appliance Audit** in IPv6 DNS Reports section that provides complete audit information regarding the operations performed by an administrator on a specific IPv6 DNS appliance or all appliances.

Navigation: Reports >> DNS Reports >> IPv6 DNS Reports >> IPv6 Appliance Audit

TW-FR-716: IPv6 Subnet Template Audit

Added **IPv6 Subnet Template Audit** report that provides complete audit information regarding operations performed by an administrator on a specific IPv6 subnet template or all subnet templates.

Navigation: Reports >> Address Space Reports >> IPv6 Reports >> IPv6 Subnet Template

TW-FR-745: AD User to TCPWave IP Address Mapping report

Added **Microsoft Active Users** report in the DHCP reports section that displays the Active Directory (AD) domain user data whenever the TCPWave appliance is connected to an MS server. Using the statistics, the network teams can view all the active users currently logged in to AD domain services.

Navigation: Reports >> DHCP Reports >> Microsoft Active Users Report

TW-FR-747: IPv6 Reverse Zones Audit

Added **IPv6 Reverse Zones Audit** report in IPv6 DNS Reports section that provides complete audit information regarding operations performed by an administrator on a specific IPv6 reverse zone or all zones. The IPAM retrieves and displays the zone audit information for a specified time provided by the user.

Navigation: Reports >> DNS Reports >> IPv6 DNS Reports >> IPv6 Reverse Zones Audit

TW-FR-748: IPv4 Subnet Template Audit

Added **IPv4 Subnet Template Audit** report in IPv4 Reports section that provides complete audit information regarding operations performed by an administrator on a specific IPv4 subnet template or all subnet templates.

Navigation: Reports >> Address Space Reports >> IPv4 Reports >> IPv4 Subnet Template Audit

TW-FR-761 New Scheduled Job

Added **DNSNamedLogsCollector** scheduled job in the Scheduler Tasks section that executes for every thirty-minute interval. Based on the logic, the records of events are displayed in the UI of the DNS SERVFAIL Responses report grid.

Navigation: Administration >> Scheduler Management >> Scheduled Tasks >> DNSNamedLogsCollector >> DNS SERVFAIL Reponses Report grid data

TW-FR-762: DNS SERVFAIL Responses Report

Added **DNS SERVFAIL responses** report in DNS Reports section that displays the domain names and the SERVFAIL counts for which the DNS resolution failed.

Navigation: Reports >> DNS Reports >> DNS Query Reports >> DNS SERVFAIL Responses

TW-FR-763: DNS Query Stats Report

Added **IPv6 Address Request** parameter in the DNS Query Statistics Report grid. This field displays the count of the IPv6 address that was able to communicate with the appliances. Additionally, the report displays information such as the count of all the messages sent to and received from the servers, the count of duplicate queries, dropped queries, etc.

Navigation: Reports >> DNS Reports >> DNS Query Reports >> DNS Query Statistics

TW-FR-774: IPv6 DHCP Appliance Pool Utilization Report

Added **IPv6 DHCP Appliance Pool Utilization** report in the IPv6 Reports section that displays the DHCP scope utilization of the active DHCP appliances in the IPAM.

Navigation: Reports >> Capacity Planning Reports >> IPv6 Reports >> IPv6 DHCP Appliance Pool Utilization Report

TW-FR-794: Report Name Modifications

Previously, sub-section reports names were succeeded by the word Report. The modifications are made to all the sub-section report names to avoid redundancy.

Navigation: Reports

TW-FR-795: DHCP IPv4 Daily Peak Hour LPS

Added **DHCP IPv4 Daily Peak Hour LPS** report in the DHCP reports section that displays the DORA (Discover Offer Request Acknowledgement) packets with LPS (Leases Per Second) details for the peak hour of the day based on the selected appliances and date range. Peak Time and LPS are displayed based on acknowledgment packets. This report helps you identify the load carried by each DHCP appliance during active hours to plan better for capacity and lessen the risk of overloading DHCP devices. It uses organization as a global drop-down.

Navigation: Reports >> Capacity Planning Reports >> IPv4 DHCP Reports >> DHCP IPv4 Daily Peak Hour LPS

TW-FR-813: Cloud Instance Provisioning Audit Report

Added **Cloud Instance Provisioning Audit** report in the Cloud Reports section that provides

information about the operations performed by the administrator on the cloud provider instances.

Navigation: Reports >> Cloud Reports >> Cloud Instance Provisioning Audit Report

TW-FR-841: Cosmetic Changes - Report Menu Links

If the disk space reaches a critical value, the main menu of the reports section of the TCPWave IPAM application is displayed in red.

Navigation: Dashboard >> Blue ribbon >> Reports menu

TW-FR-842: DNS Statistics Report per zone

Added **DNS Statistics Report Per Zone** report in DNS Zone Reports section that displays the number of resource records assigned to a zone by resource record type. It helps you plan better for capacity. It uses organization as a global drop-down.

Navigation: Reports >> DNS Reports >> DNS Zone Reports >> DNS Statistics Per Zone

TW-FR-859: Cloud Instance Provisioning Template Audit

Added **Cloud Instance Provisioning Template Audit** report in the Cloud Reports section that provides information about the operations performed by an administrator on the cloud provisioning template. It uses organization as a global drop-down.

Navigation: Reports >> Cloud Reports >> Cloud Instance Provisioning Template Audit Report

Common Functionality

TW-FR-778: Global Search For IPS Rules

Added global search functionality for NSM IPS rules based on the rule content. Enable and Disable context menu options are added in the NSM IPS search results grid. When the option is enabled, the system returns the rule to the Suricata rules file. On selecting the disable option, the system removes the Suricata rules file on the DNS appliances associated with the NSM template.

Navigation: Global Search >> Search Term >> NSM IPS Rules

TW-FR-783: Responsive Left Side Menu Bar

Added responsive left side menu bar in all the operational screens of TCPWave IPAM application. The side menu bar has expandable and collapsible views. In the collapsible view, you can view the icons of the main sections, and on the mouse hover, you can view the sub-sections of the main sections.

The system displays the top-level menu items in the accordion format in the expandable view. On clicking the top-level menu items, the system displays the respective sub-menu items.

TW-FR-723: Need API call to pull subnets based on % utilization & get utilization value in specific parameters

Added subnet/listSubnetsUsingAllocation RESTAPI, which retrieves the information IPv4 subnets of a specific network based on the utilized percentage of the subnet.

TW-FR-824: Unable to get correct admin details using the rest API

Added user/getUserDetailsByLoginName RESTAPI call, which retrieves the users' data along with their

first and last name, admin groups, and list of the functions associated with the groups, etc. based on the login name details.

Change Request

TW-CR-3854: Interactive Network Topology

Added interactive network topology diagrams in the Architecture Overview page. You can view the system information with a double click on a live appliance. The right-click provides a context menu option, which includes Dig, Last Sync Status, Restart DNS Service, Sync, etc.

Navigation: Infrastructure Management >> Architecture Overview

TW-CR-4947: DDNS Updates Issue

Added a new scheduled job **ZoneSerialConsistencyChecker** in the Scheduled Tasks section. It is executed every 30 minutes. It fetches the list of organizations, zones defined in the organization, and associated masters and slaves. It checks whether all the slave's serial numbers are in line with masters for all the zones. If there is any inconsistency (configurable through the global option **Zone Serial Delta Difference**), then the scheduled job ensures that slaves are updated with their masters.

Navigation: Administration >> Scheduler Management >> Scheduled Tasks >> ZoneSerialConsistencyChecker

Bug Fixes

Ticket ID	Description
TW-CR-3033	Fixed an issue of zone serial number increment to allow a maximum of 4294967295.
TW-CR-4327	Fixed an issue for subnet/getSubnetDetails in the secondary domain.
TW-CR-4339	Fixed an issue with the data export wizard option in IPAM appliances in v11.31P8.
TW-CR-4383	Fixed an issue of inconsistent data response for subnet objects across the different APIs.
TW-CR-4384	Fixed an issue of incorrect data returned from API subnet/getSubnetDetails and API search/search for attribute 'object_count'.
TW-CR-4394	The issue of qef.jar generating incorrect rows to g_zone_rrs.csv for TXT records with multiple strings has been fixed.
TW-CR-4466	The issue of 'TIMS-1351: User Id cannot be null' for API 'object/list' returns has been fixed.
TW-CR-4476	Fixed the issue of changes to zone templates without full sync and deletion of db files.
TW-CR-4598	Fixed an issue of exportreversezonetmpl data.
TW-CR-4655	Fixed an issue of secondary domains displayed incorrectly on some subnets and cannot be modified in the GUI.
TW-CR-4662	Fixed an issue of replication DDNS updates to another DNS master received directly from the client.
TW-CR-4695	Fixed an issue of the default route that is dropped when an appliance reboots from patching.
TW-CR-4696	The issue of remote license key fails for service-tag-based license keys in Data wizard import has been fixed.
TW-CR-4730	Fixed an issue for the removal of child domain validations alert.
TW-CR-4732	Fixed an issue with uploading the keytab with the same DC IP and different DNS appliances.
TW-CR-4782	Fixed the issue for Auditing when the critical alert is disabled and OK when it is enabled.
TW-CR-4785	Fixed the red X error message issue and named.conf in DNS Sync master and slave appliances to the zone templates on child zones.
TW-CR-4803	Fixed an issue in creating an MX record in GUI.
TW-CR-4830	Fixed the issue of deleting the object in the secondary object.
TW-CR-4832	Fixed the issue of creating a CNAME record.
TW-CR-5026	Unable to create Apex DNS entries at the Object level.

CLI Updates

#	Description
1	Added the following CLI's: ▪ addipv6dnsreversezone ▪ deleteipv6subnettmpl ▪ deleteipv6dnsserver ▪ deleteipv6dnsreversezone ▪ exportipv6dhcpserver ▪ exportipv6dnsserver ▪ editipv6dnsreversezone ▪ exportsubnettemplate ▪ getipv6dnsserver ▪ getipv6subnettmpl ▪ importipv6dhcpserver ▪ importsubnettemplate ▪ importipv6dnsserver ▪ listipv6subnettmpl ▪ listipv6dnsserver ▪ listipv6dnsreversezone ▪ setipv6subnettmpl ▪ setipv6remotemonitor ▪ setipv6remotedebug ▪ setipv6remotecntrllog ▪ setipv6dnsserver ▪ syncipv6dnsserver ▪ syncipv6dhcpserver

RESTAPIs

#	Operation	RESTAPI
1	Added the following GET calls:	
	GET	xtn/getSubnetNetworkDetailsByExtensions
		discovery_agent/agentMap2
		discovery_agent/natpoolList
		discovery_agent/getvmware_elements
		discovery_agent/firewallvrf/list
		discovery_agent/getNeighbors
		discovery_agent/getSubnetsByDevice
		daswitch/vlan/subnetelementpage
		daswitch/switchDetailsByElementIp
		discovery_appliance/search
		discovery_appliance/discovery_device/list
		discovery_appliance/discovery_exclusion/list
		reports/disksizestatus
		reports/dnsstatisticsperzoneaudit
		reports/dnsservfailresponsesRpt
		DNSDefaults/getSyslogngConfig
		DHCPDefaults/getSyslogngConfig
		DNSDefaults/getTacacsConfig
		DHCPDefaults/getTacacsConfig
		reports/cloudreportlist
		reports/dhcpAppliancePoolUtilized
		reports/dnsdailypeakqueryRpt
		reports/dhcpdailypeakqueryRpt
		v6auditreports/livev6appliancelist
		server/windowsServerslist
		queryAltResolvers/list
		queryAltResolvers/get
		v6auditreports/v6dhcpoptiontmpllist
		server/getClusterInfo
		server/getClusterStatus
		dnsserver/reconfig
		dnsserver/zonelist
		alarmSubscription/list
		v6auditreports/v6dnsserverslist

#	Operation	RESTAPI
		v6auditreports/v6revzonelist
		v6auditreports/reportchartlist
		v6auditreports/ipv6dhcpserverlist
		auditreports / v4SubnetTemplatelist
		capacityplanning/cumutilization
		capacityplanning/top10consumers
		capacityplanning/top10qps
		capacityplanning/top10lps
		capacityplanning/dnstoptalkers
2	Added the following POST calls:	
	POST	discovery_agent_task/acceptDevice
		discovery_agent_task/acceptRouterSubnet
		discovery_agent_task/acceptFirewallSubnet
		discovery_agent_task/acceptSwitchSubnet
		discovery_agent_task/acceptVrf
		discovery_agent_task/getConfigDifference
		discovery_agent/firewall/natpool_multiadd
		discovery_agent/vmware_element/multiadd
		discovery_agent/vmware/multiadd
		discovery_agent/firewallvrf/multiadd
		discovery_appliance/discovery_device/multiadd
		discovery_appliance/discovery_device/multidelete
		discovery_appliance/discovery_device/update
		discovery_appliance/discovery_exclusion/multiadd
		discovery_appliance/discovery_exclusion/multidelete
		discovery_appliance/discovery_exclusion/update
		DNSDefaults/updateSyslogngConfig
		DHCPDefaults/updateSyslogngConfig
		DNSDefaults/updateTacacsConfig
		DHCPDefaults/updateTacacsConfig
		globals/updatefadmaccess
		reports/msactiveusersrptgrid
		xtn/attr_object_val
		queryAltResolvers/add
		queryAltResolvers/edit
		queryAltResolvers/multidelete
		monitor/recheckAlert

#	Operation	RESTAPI
		v6templates/delete/ids
		v6templates/create
		v6templates/update
		dnsserver/formCluster
		dnsserver/updateCluster
		dnsserver/resetCluster
		alarmSubscription/add
		alarmSubscription/delete
		dashboard/widget/updateConfig