REPORT

Infoblox reporting and analytics

TABLE OF CONTENTS

1 INFOBLOX REPORTING AND ANALYTICS OVERVIEW

Infoblox has provided the industry-leading platform for real-time views and management DNS, DHCP and IP Address Management (IPAM) for the past decade. Infoblox Reporting and Analytics integrates with the patented Infoblox Grid™ technology and enhances the real-time management with an extensive and customizable historical reporting engine as well as a predictive analytics engine.

Infoblox Reporting & Analytics delivers actionable network intelligence by providing the ability to collect, analyze, and visualize granular core network data and perform free-form searches, produce interactive dashboards and reports with drill down capabilities, and view predictive analytics. IT teams can now do detailed investigation of events, identify anomalies, easily collect compliance audit data, and share reports and dashboards with the organization at large. The solution's predictive analytics helps enterprises model future patterns of network behavior and create more accurate capacity planning thresholds. Reports can be captured and shared via the Infoblox community giving users access to a vast pool of ideas, benefitting from other's best practices.

With Infoblox, you have the power and management capability to manage DDI deployments with the most reliable and secure services, the best real-time management views and robust, customizable reporting – all within a single platform.

This sample report booklet includes many of the pre-built reports available with Infoblox Reporting and Analytics today. The reports are grouped by:

- DNS reports
- Security (DNS) reports
- DHCP reports
- IPAM reports
- Device reports
- Integration reports
- Cloud reports
- Discover reports

Each sample report includes the following information:

- Description of the report
- Data presented
- Sample report graphic

For additional information on Infoblox Reporting and Analytics or other Infoblox products, please contact your local Infoblox representative or call 1-408-625-4200 ext. 2.

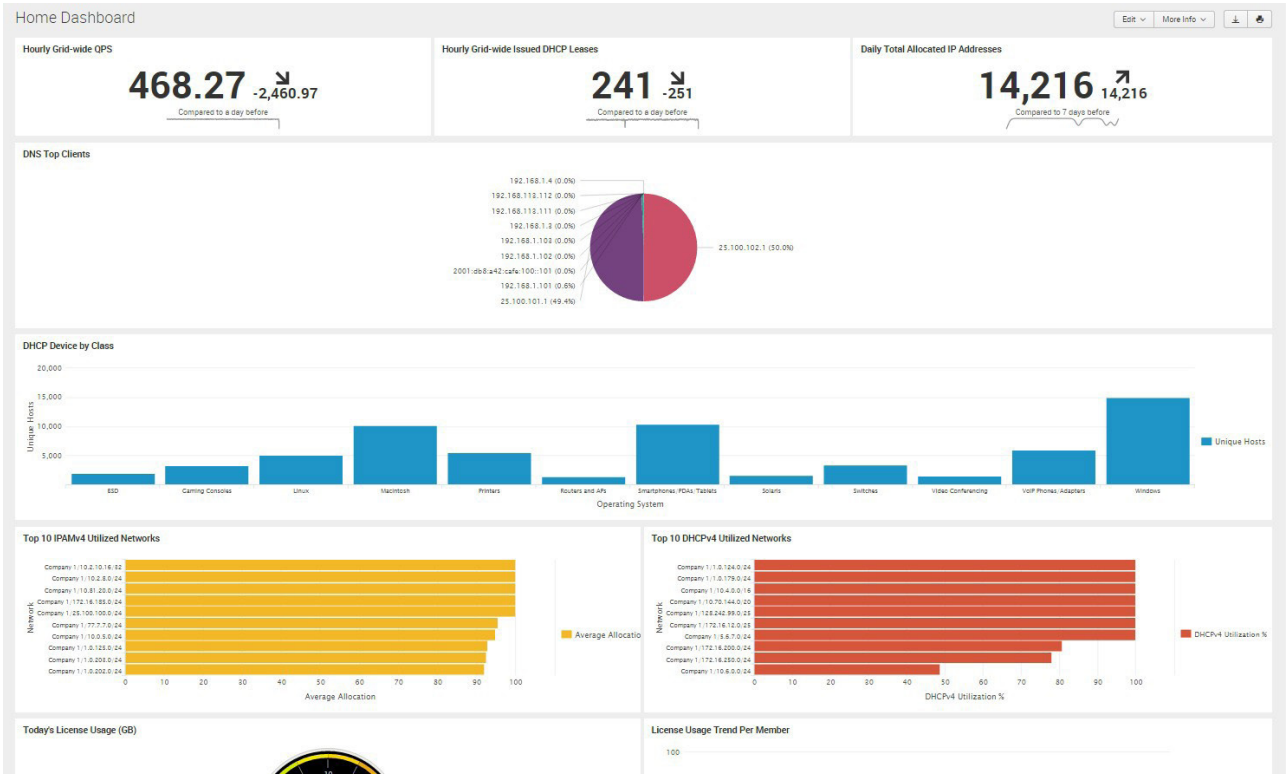
Please note Infoblox Reporting and Analytics will have continuous updates to existing reports and add new capabilities over time. This sample report book lists the available reports in the current release of the solution. Customers not on the current release and/or not utilizing all of the products, features, or capabilities may not receive all available reports. This is a sample reporting book and the reports listed here may be reformatted, changed and/or be removed.

2 HOME DASHBOARDS AND PREDICTIVE REPORTS

2.1 Home Dashboard

Description	Home Dashboard highlights critical DDI components on a single report.
Overview	This report is a one-stop dashboard for several critical reports on a single view providing a snapshot of status and potential issues. Users can drill down into any report for more detail.
Data presented	• Hourly Grid-wide QPS • Hourly Grid-wide Issued DHCP Leases • Daily Total Allocated IP Addresses • DNS Top Clients • DHCP Device by Class • Top 10 IPAMv4 Utilized Networks • Top 10 DHCPv4 Utilized Networks • Today's License Usage (GB) • License Usage Trend By Member

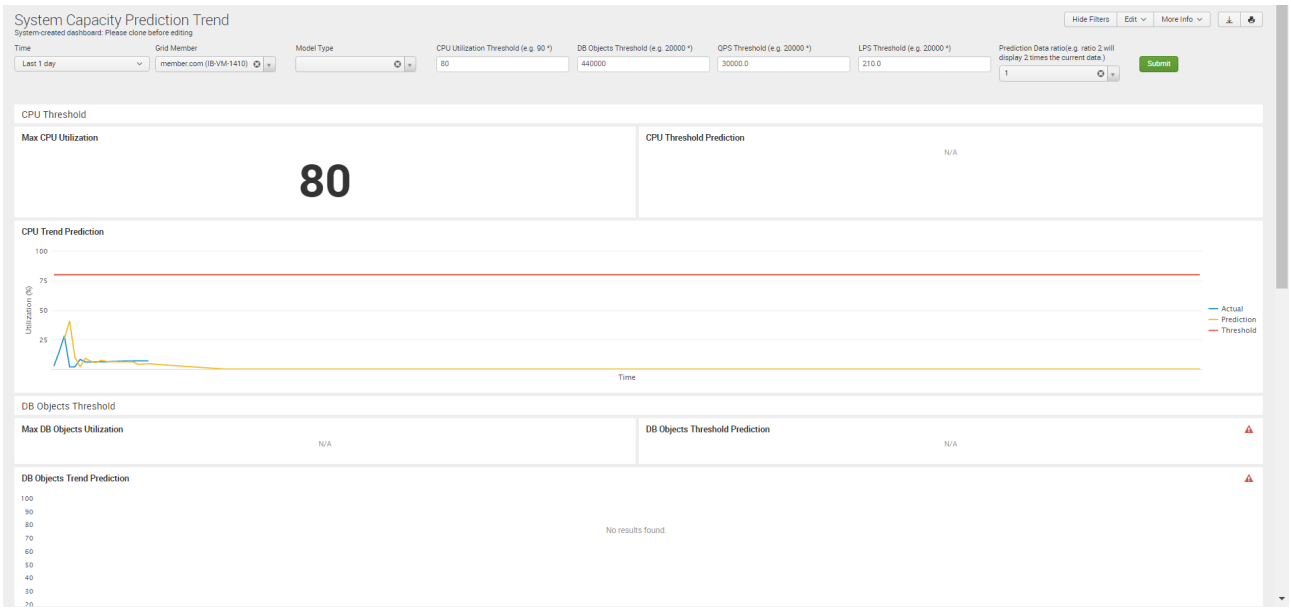
Sample report:



2.2 System Capacity Prediction Trend

Description	Dashboard view that provides predictive projections for system requirements.
Overview	This report leverages the rich current and historical DDI data and a predictive algorithm to help users identify with core services are likely to exceed the current capacity such as when QPS or DHCP LPS should be upgraded to reduce the risk of under provisioning.
Data presented	• Max CPU utilization • CPU threshold prediction • CPU trend prediction • Max DB objects utilization • DB objects threshold prediction • DB objects trend prediction • Database max QPS • QPS threshold prediction • QPS prediction • DHCP thresholds • LPS threshold predictions • DHCP activity prediction

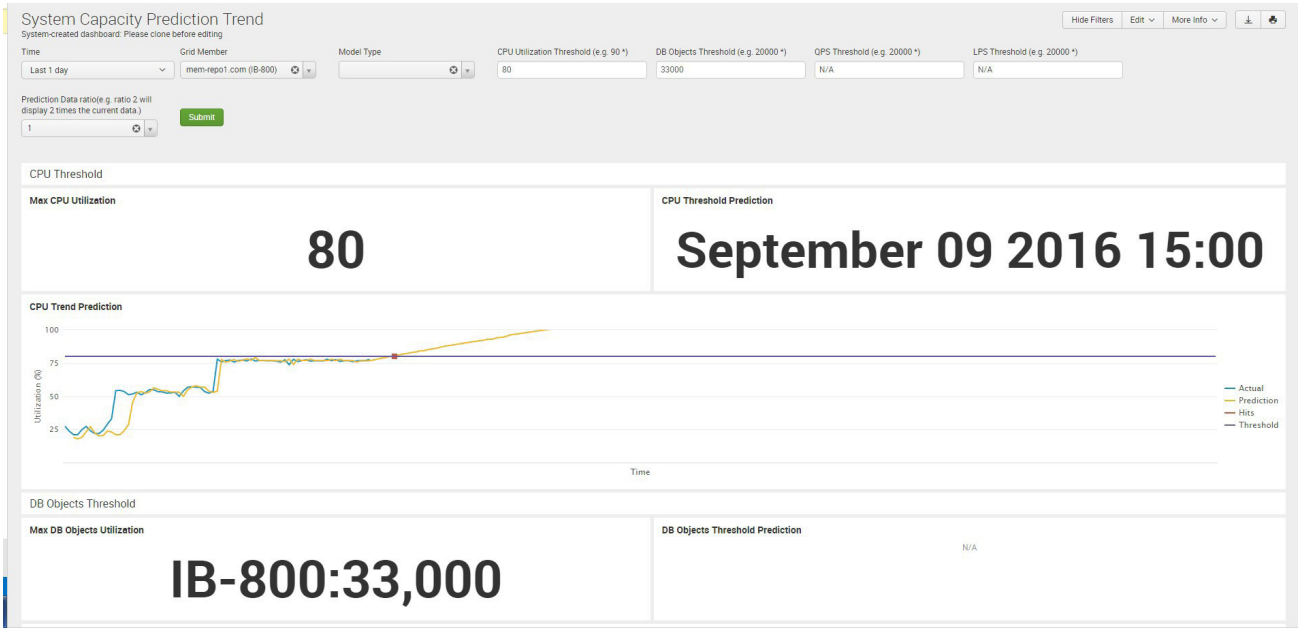
Sample report:



2.3 System Capacity Predictive Trend

Description	Dashboard view that provides predictive projections for system requirements.
Overview	This report leverages the rich current and historical DDI data and a predictive algorithm to help users identify with core services are likely to exceed the current capacity such as CPU Threshold and Database Objects should be upgraded to reduce the risk of under provisioning.
Data presented	• Max CPU Utilization • CPU Utilization Prediction • CPU Trend Prediction • Max DB Objects Utilization • DB Object Threshold Prediction

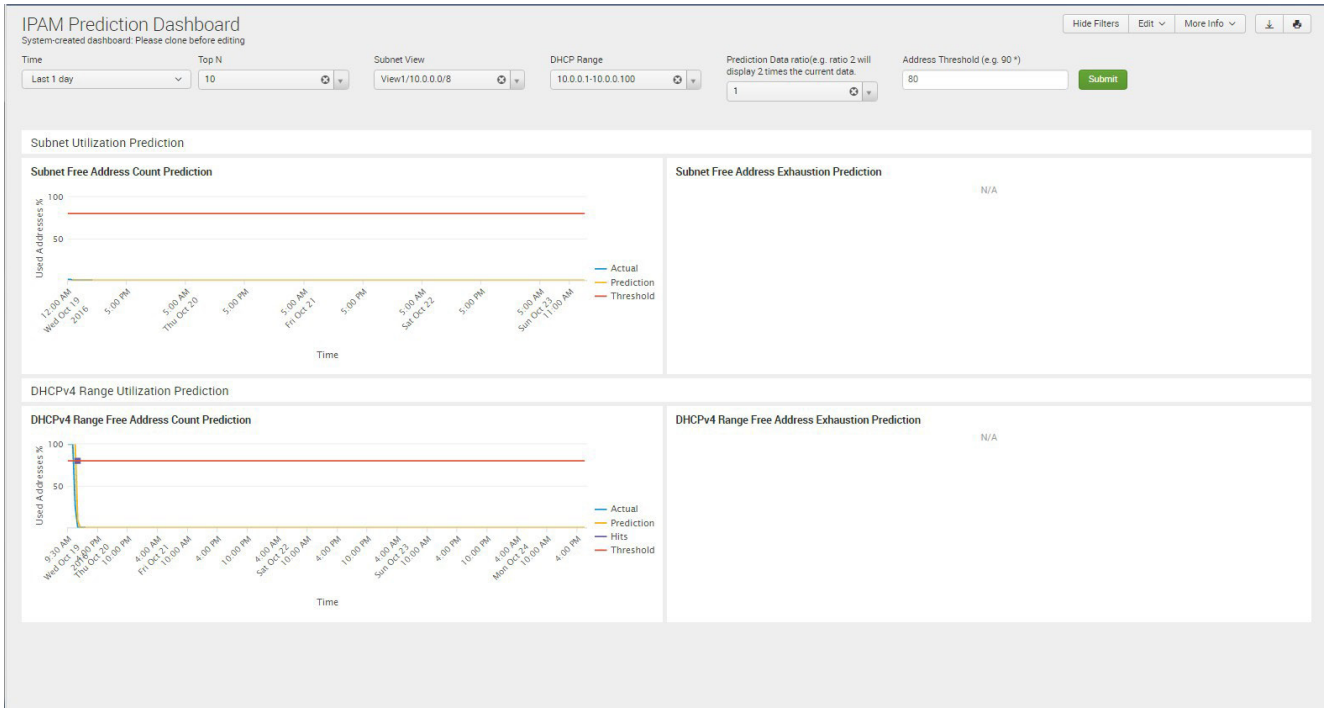
Sample report:



2.4 IPAM Prediction Dashboard

Description	Dashboard view that provides predictive projections for IP address management requirements.
Overview	This report leverages the rich current and historical IP address management data and a predictive algorithm to help users identify with core services are likely to exceed the current capacity such as when subnets and ranges should be upgraded to reduce the risk of under provisioning.
Data presented	• Subnet Free Address Count Prediction • Subnet Free Address Exhaustion Prediction • DHCPv4 Range Address Count Prediction • DHCPv4 Range Free Address Exhaustion Prediction

Sample report:

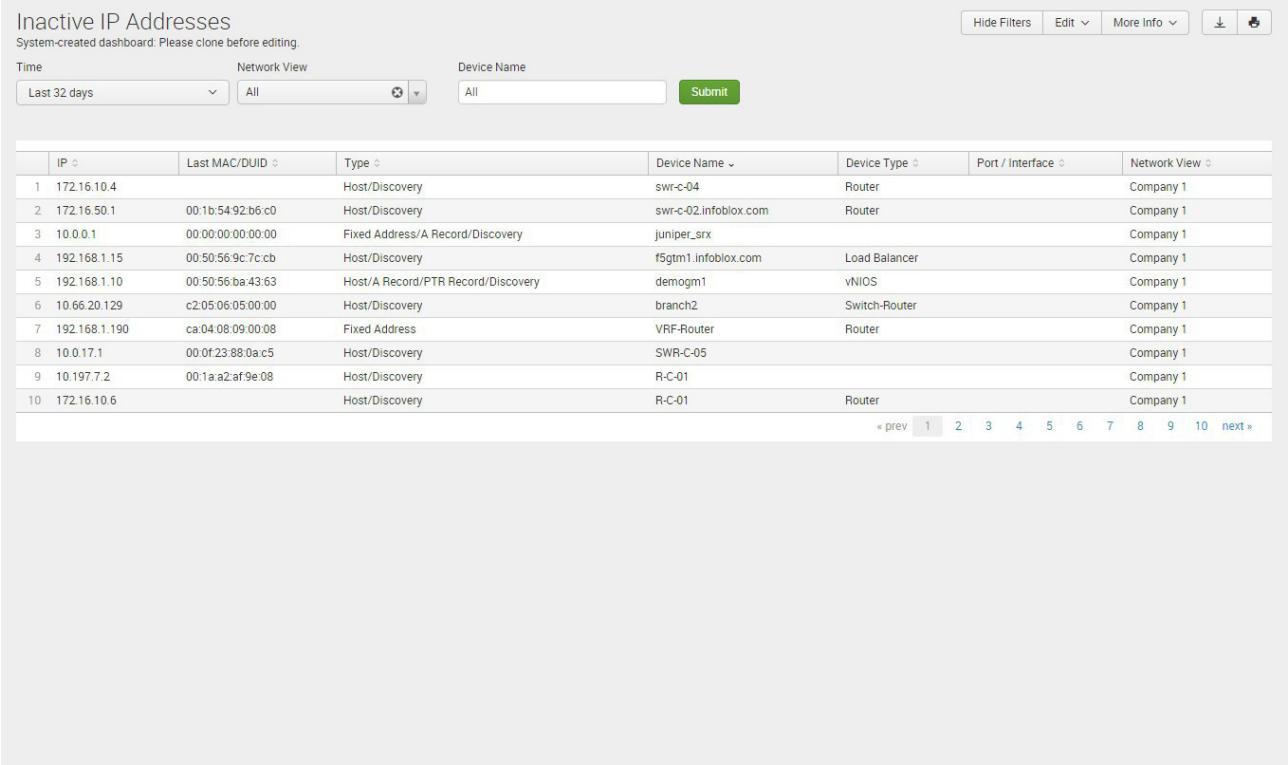


3 DEVICES (DISCOVERY) DASHBOARDS

3.1 Inactive IP Addresses

Description	Identifies IP Addresses that are inactive
Overview	Monitors and tracks the last time IP addresses were used and reports on all IP addresses that are inactive. This view allows users to clean up unused IP addresses which reclaims IP addresses for future requirements, shrinks the data requirements and improves visibility. This report is available for customers with Infoblox Network Insight.
Data presented	• IP Address • Last MAC/DUID • Type • Device Name • Device Type • Port/Interface • Network View

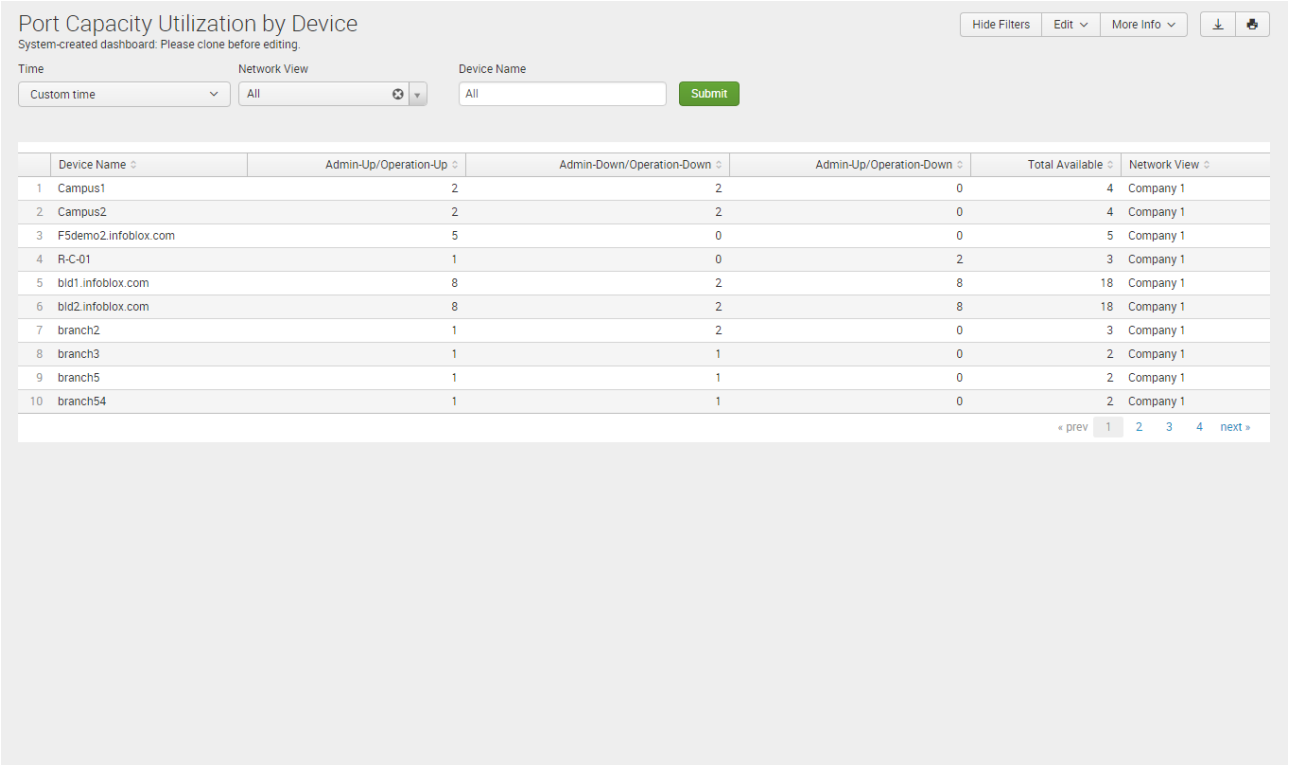
Sample report:



3.2 Port Capacity Utilization by Device

Description	Tracks Port Capacity Utilization by Device
Overview	Tracks the port capacity by monitoring end-hosts connected to switch ports. The detailed views of operation and admin up/down status with total port counts help with faster troubleshooting and improved capacity planning with up-to-date visibility. This report is available for customers with Infoblox Network Insight.
Data presented	• Device Name • Admin Up, Operation Up Start • Admin Up, Operation Up End • Admin Down, Operation Down Start • Admin Down, Operation Down End • Admin Up, Operation Down Start • Admin Up, Operation Down End • Total Available • Network View

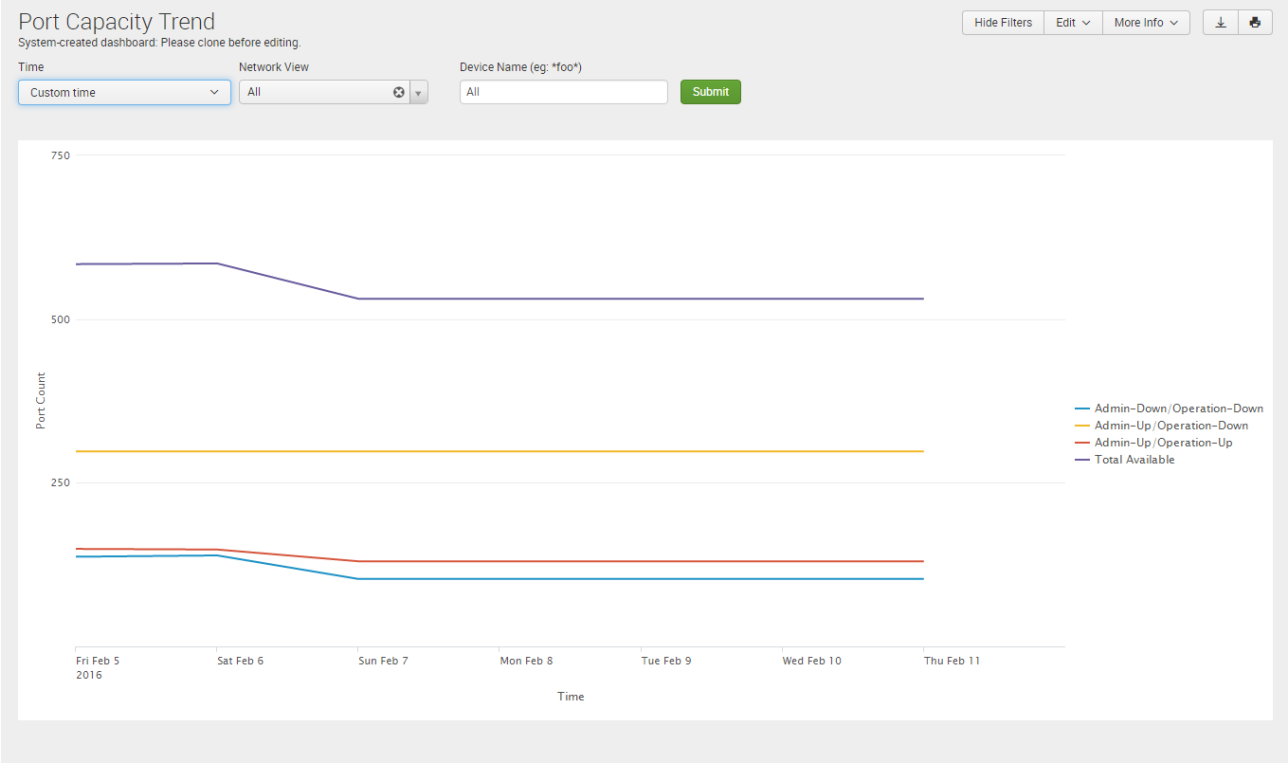
Sample report:



3.3 Port Capacity Trend

Description	Monitors Port Capacity Utilization over time with historical visibility
Overview	Tracks the port capacity by monitoring end-hosts connected to switch ports over time. The trending views of operation and admin up/down status highlights utilization over time to plan better with enhanced visualization. This report is available for customers with Infoblox Network Insight.
Data presented	• Admin Up, Operation Up • Admin Down, Operation Down • Admin Up, Operation Down • Total Available

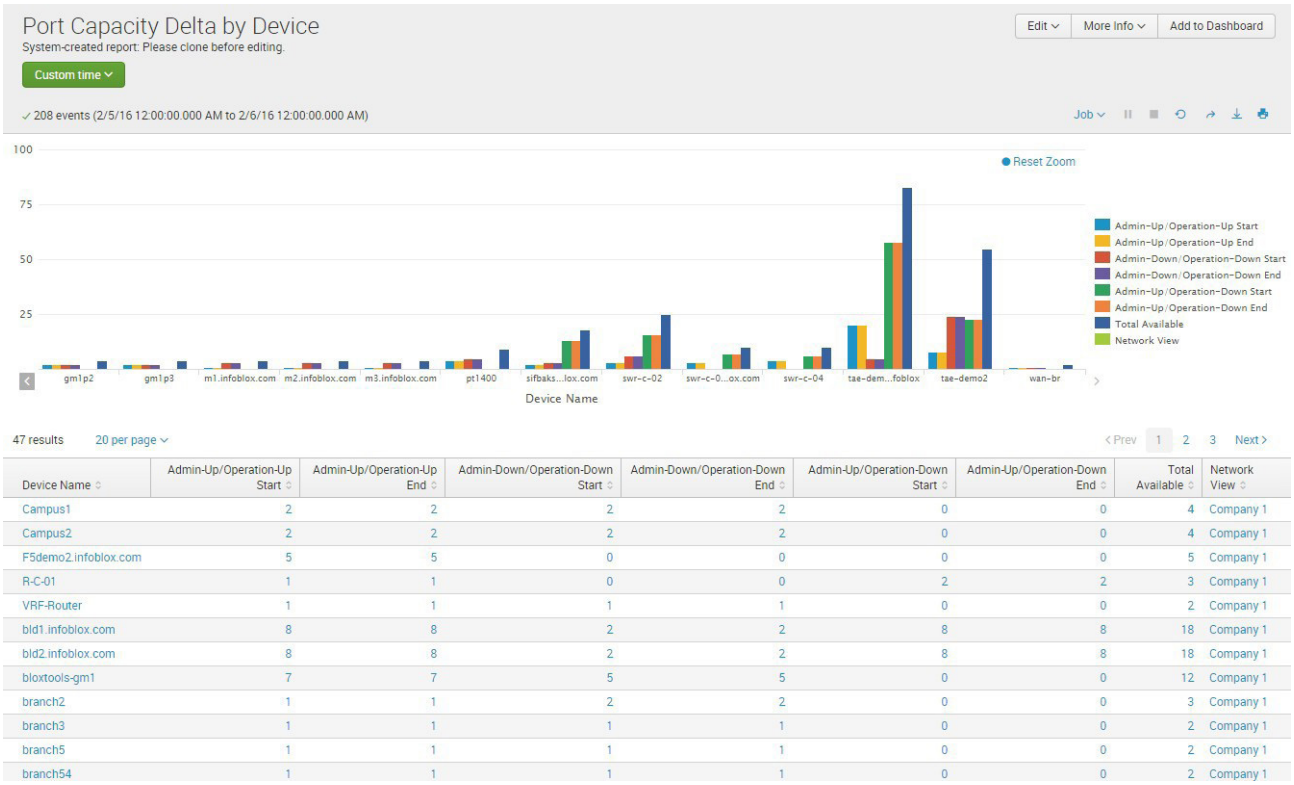
Sample report:



3.4 Port Capacity Delta by Device

Description	Tracks the change in Port Capacity by Device over time
Overview	Monitors the port capacity over time and identifies the delta over time between admin and operation up/down status. The data helps identify which devices have had the biggest or smallest changes in status over a defined period which helps with capacity planning. This report is available for customers with Infoblox Network Insight.
Data presented	• Device Name • Admin Up/Operation Up • Admin Down, Operation Down • Admin Up, Operation Down • Total Available • Network View

Sample report:

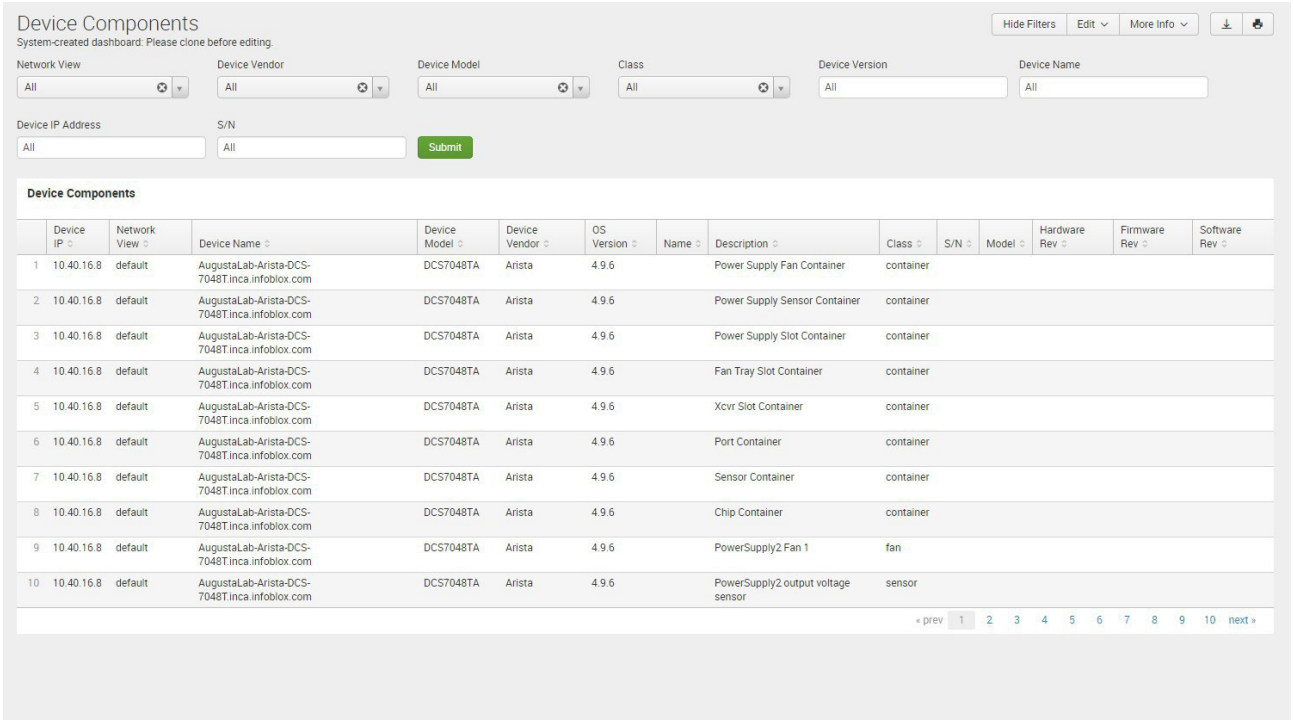


Device Name	Admin-Up/Operation-Up Start	Admin-Up/Operation-Up End	Admin-Down/Operation-Down Start	Admin-Down/Operation-Down End	Admin-Up/Operation-Down Start	Admin-Up/Operation-Down End	Total Available	Network View
Campus1	2	2	2	2	0	0	4	Company 1
Campus2	2	2	2	2	0	0	4	Company 1
F5demo2.infoblox.com	5	5	0	0	0	0	5	Company 1
R-C-01	1	1	0	0	2	2	3	Company 1
VRF-Router	1	1	1	1	0	0	2	Company 1
bld1.infoblox.com	8	8	2	2	8	8	18	Company 1
bld2.infoblox.com	8	8	2	2	8	8	18	Company 1
bloxtools-gm1	7	7	5	5	0	0	12	Company 1
branch2	1	1	2	2	0	0	3	Company 1
branch3	1	1	1	1	0	0	2	Company 1
branch5	1	1	1	1	0	0	2	Company 1
branch54	1	1	1	1	0	0	2	Company 1

3.5 Device Components

Description	Tracks the device components discovered
Overview	Identifies and highlights the top device components be used across the organization's IT infrastructure to help with planning, troubleshooting and auditing requirements.
Data presented	• Device IP • Network View • Device Name • Device Model • Device Vendor • OS Version • Name • Description • Class • Serial Number • Model • Hardware Rev • Firmware Rev • Software Rev

Sample report:



Device Components

System-created dashboard: Please clone before editing.

Hide Filters | Edit | More Info

Network View: All | Device Vendor: All | Device Model: All | Class: All | Device Version: All | Device Name: All

Device IP Address: All | S/N: All | Submit

Device Components

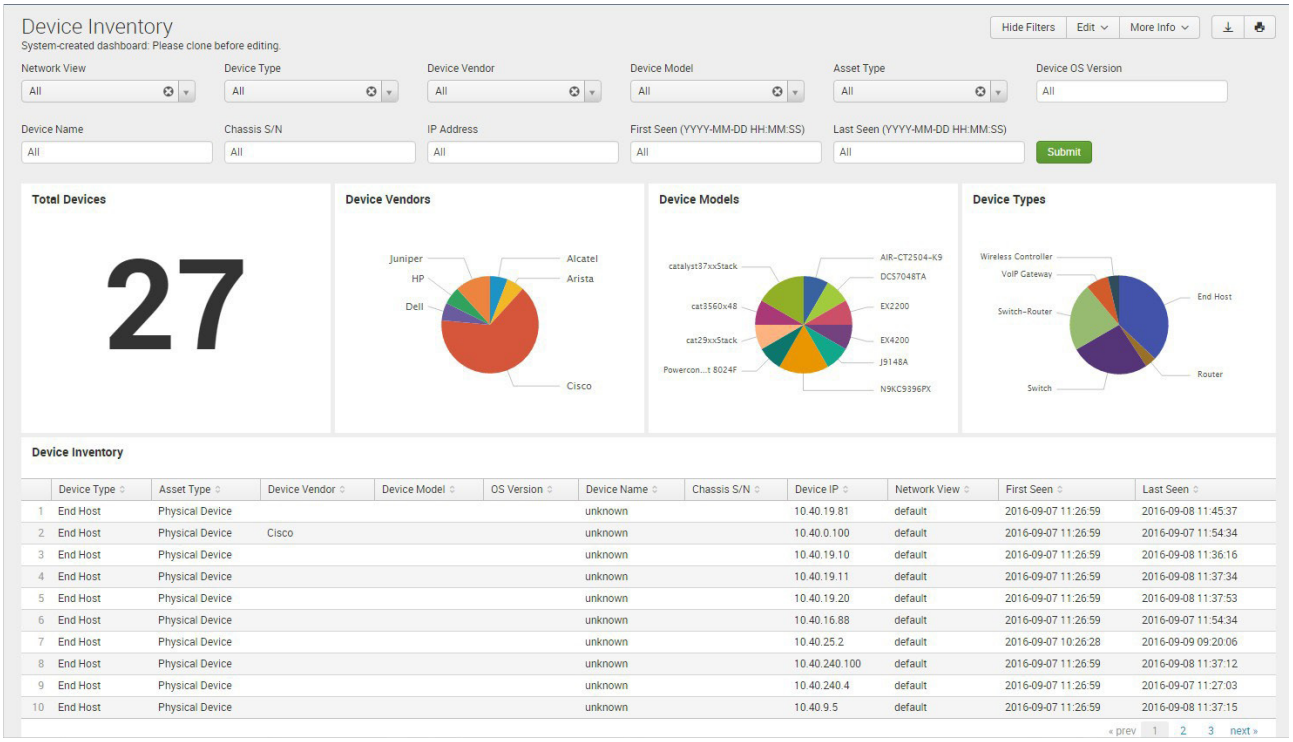
	Device IP	Network View	Device Name	Device Model	Device Vendor	OS Version	Name	Description	Class	S/N	Model	Hardware Rev	Firmware Rev	Software Rev
1	10.40.16.8	default	AugustaLab-Arista-DCS-7048T.inca.infoblox.com	DCS7048TA	Arista	4.9.6		Power Supply Fan Container	container					
2	10.40.16.8	default	AugustaLab-Arista-DCS-7048T.inca.infoblox.com	DCS7048TA	Arista	4.9.6		Power Supply Sensor Container	container					
3	10.40.16.8	default	AugustaLab-Arista-DCS-7048T.inca.infoblox.com	DCS7048TA	Arista	4.9.6		Power Supply Slot Container	container					
4	10.40.16.8	default	AugustaLab-Arista-DCS-7048T.inca.infoblox.com	DCS7048TA	Arista	4.9.6		Fan Tray Slot Container	container					
5	10.40.16.8	default	AugustaLab-Arista-DCS-7048T.inca.infoblox.com	DCS7048TA	Arista	4.9.6		Xcvr Slot Container	container					
6	10.40.16.8	default	AugustaLab-Arista-DCS-7048T.inca.infoblox.com	DCS7048TA	Arista	4.9.6		Port Container	container					
7	10.40.16.8	default	AugustaLab-Arista-DCS-7048T.inca.infoblox.com	DCS7048TA	Arista	4.9.6		Sensor Container	container					
8	10.40.16.8	default	AugustaLab-Arista-DCS-7048T.inca.infoblox.com	DCS7048TA	Arista	4.9.6		Chip Container	container					
9	10.40.16.8	default	AugustaLab-Arista-DCS-7048T.inca.infoblox.com	DCS7048TA	Arista	4.9.6		PowerSupply2 Fan 1	fan					
10	10.40.16.8	default	AugustaLab-Arista-DCS-7048T.inca.infoblox.com	DCS7048TA	Arista	4.9.6		PowerSupply2 output voltage sensor	sensor					

« prev 1 2 3 4 5 6 7 8 9 10 next »

3.6 Device Inventory

Description	Dashboard of device inventory and components
Overview	Identifies and highlights the key device parameters found during discovery and used for inventory purposes. But tracking the vendors, models, and types, the report helps users understand the current environment as well as identify if unplanned or unsupported devices/vendors touch the network.
Data presented	• Total Devices • Device Vendors • Device Models • Device Types • Device Inventory

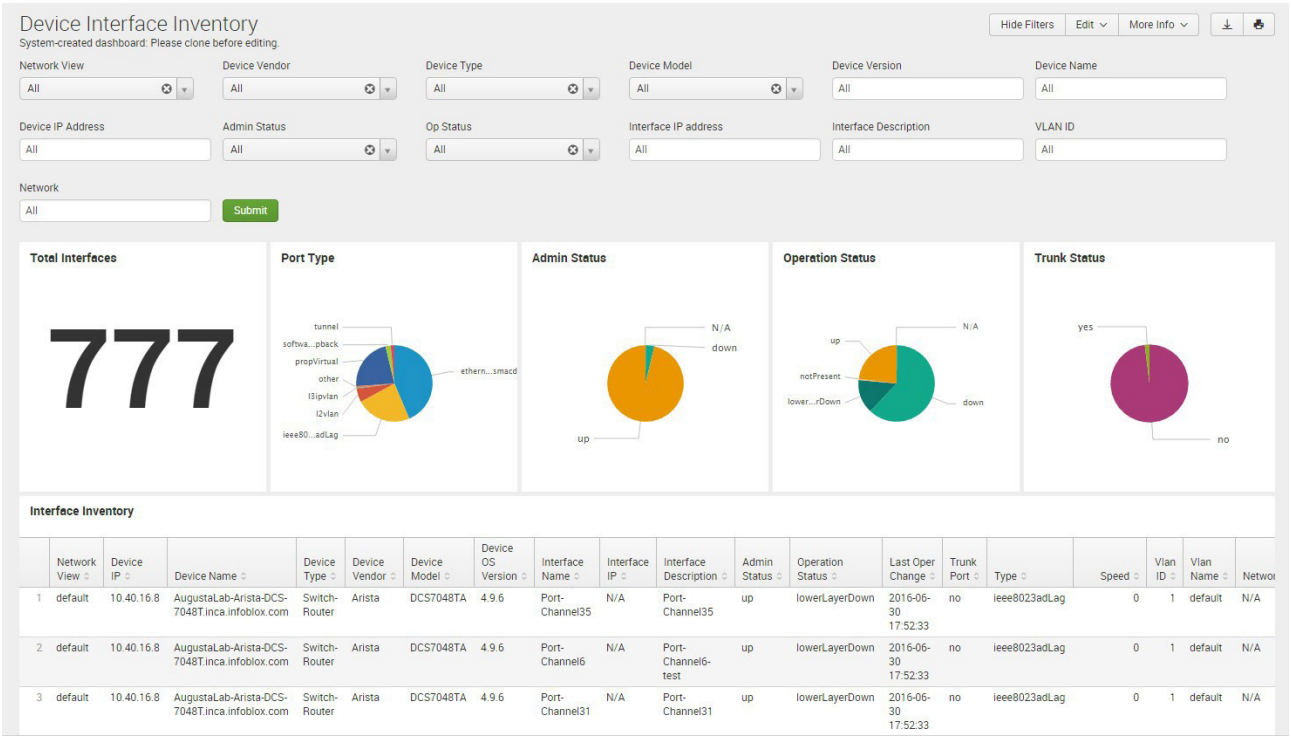
Sample report:



3.7 Device Interface Inventory

Description	Tracks the devices and the interface inventory of each device
Overview	Discovers and tracks both the devices discovered as well as the interfaces, port types, admin status, operation status, trunk status, and interface inventory. This report helps with auditing, compliance, and troubleshooting the devices and their respective interfaces.
Data presented	• Total Interfaces • Port Types • Admin Status • Operation Status • Trunk Status • Interface Inventory

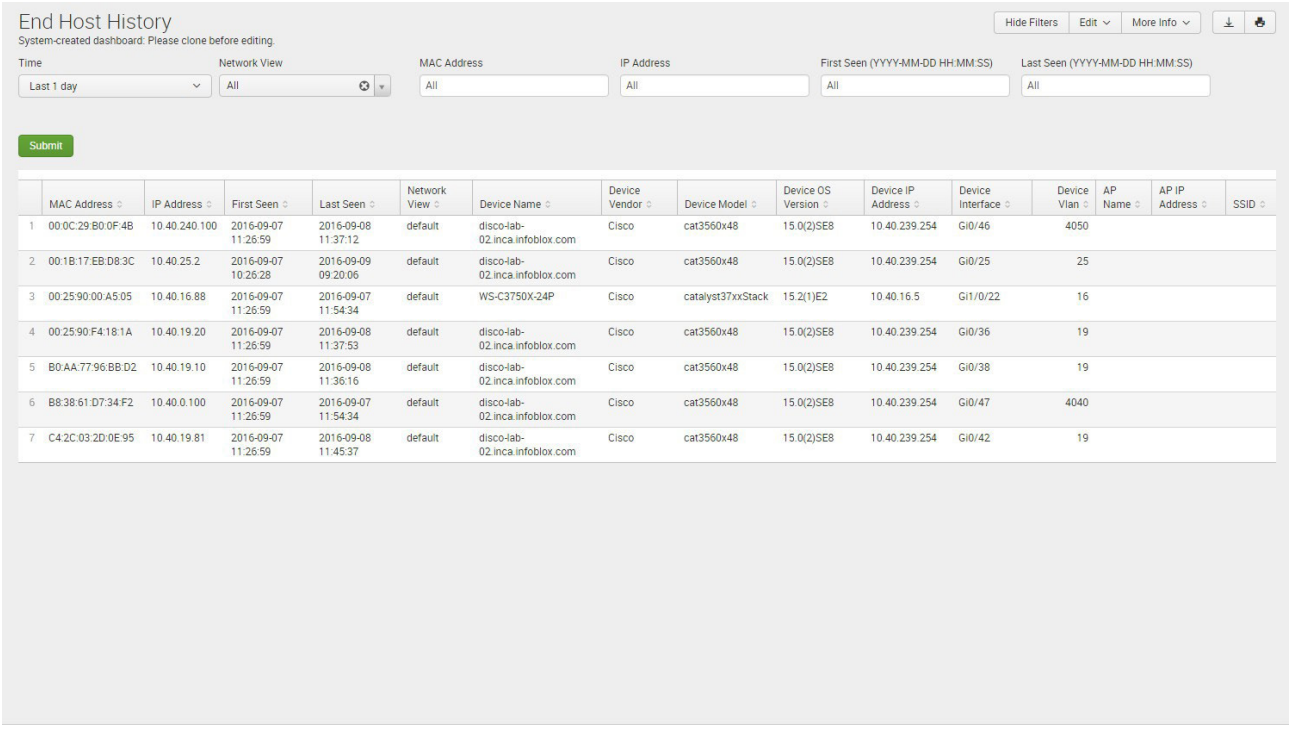
Sample report:



3.8 End Host History

Description	Tracks the detailed end host history
Overview	Discovers, monitors, and tracks the detailed history of each discovered end host. This report would help identify which end hosts are connected, with specific details so the IT team can have better day-to-day management, troubleshooting, security, and auditing capabilities.
Data presented	• MAC Address • IP Address • First Seen • Last Seen • Network View • Device Name • Device Vendor • Device Model • Device OS Version • Device IP Address • Device Interface • Device VLAN • AP Name • AP IP Address • SSID

Sample report:



End Host History

System-created dashboard: Please clone before editing.

Hide Filters | Edit | More Info

Time: Last 1 day | Network View: All | MAC Address: All | IP Address: All | First Seen (YYYY-MM-DD HH:MM:SS): All | Last Seen (YYYY-MM-DD HH:MM:SS): All

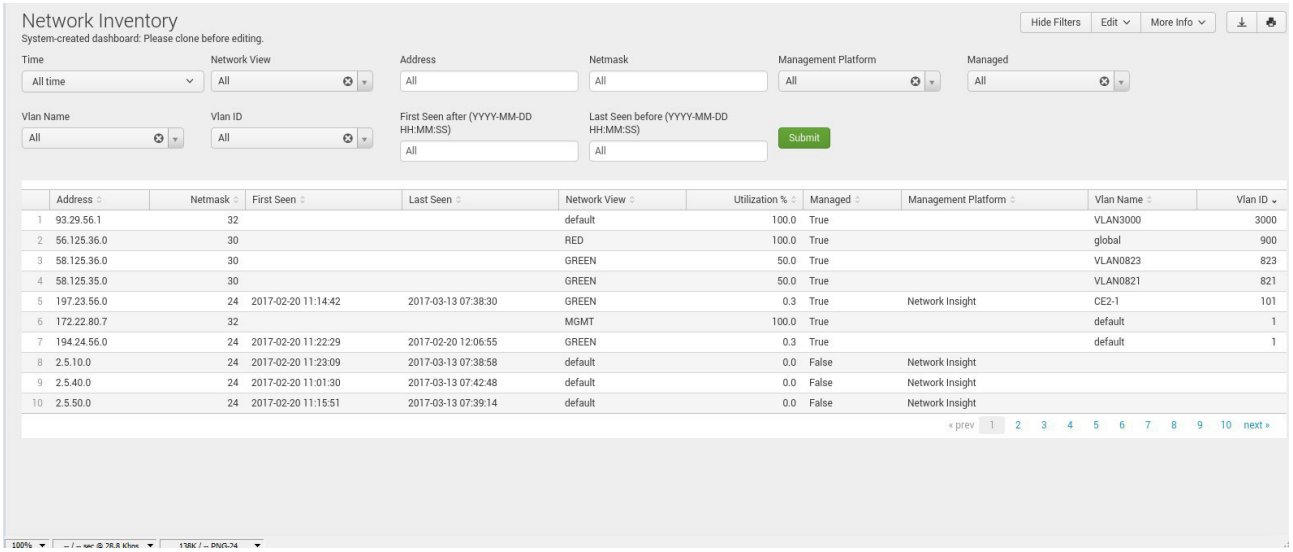
Submit

	MAC Address	IP Address	First Seen	Last Seen	Network View	Device Name	Device Vendor	Device Model	Device OS Version	Device IP Address	Device Interface	Device Vlan	AP Name	AP IP Address	SSID
1	00:0C:29:B0:0F:4B	10.40.240.100	2016-09-07 11:26:59	2016-09-08 11:37:12	default	disco-lab-02.inca.infoblox.com	Cisco	cat3560x48	15.0(2)SE8	10.40.239.254	Gi0/46	4050			
2	00:1B:17:EB:D8:3C	10.40.25.2	2016-09-07 10:26:28	2016-09-09 09:20:06	default	disco-lab-02.inca.infoblox.com	Cisco	cat3560x48	15.0(2)SE8	10.40.239.254	Gi0/25	25			
3	00:25:90:00:A5:05	10.40.16.88	2016-09-07 11:26:59	2016-09-07 11:54:34	default	WS-C3750X-24P	Cisco	catalyst37xxStack	15.2(1)E2	10.40.16.5	Gi1/0/22	16			
4	00:25:90:F4:18:1A	10.40.19.20	2016-09-07 11:26:59	2016-09-08 11:37:53	default	disco-lab-02.inca.infoblox.com	Cisco	cat3560x48	15.0(2)SE8	10.40.239.254	Gi0/36	19			
5	B0:AA:77:96:BB:D2	10.40.19.10	2016-09-07 11:26:59	2016-09-08 11:36:16	default	disco-lab-02.inca.infoblox.com	Cisco	cat3560x48	15.0(2)SE8	10.40.239.254	Gi0/38	19			
6	B8:38:61:D7:34:F2	10.40.0.100	2016-09-07 11:26:59	2016-09-07 11:54:34	default	disco-lab-02.inca.infoblox.com	Cisco	cat3560x48	15.0(2)SE8	10.40.239.254	Gi0/47	4040			
7	C4:2C:03:2D:0E:95	10.40.19.81	2016-09-07 11:26:59	2016-09-08 11:45:37	default	disco-lab-02.inca.infoblox.com	Cisco	cat3560x48	15.0(2)SE8	10.40.239.254	Gi0/42	19			

3.9 IP Address Inventory

Description	Tracks inventory of IP addresses across the network
Overview	Discovers, monitors, and tracks the detailed history of each IP address including when it was first and last seen as well as how the IP was discovered. This report would help identify and troubleshoot IP address issues by providing a complete view of where the IPs are located as well as network views.
Data presented	• IP address • Discovered name • First seen • Last seen • Network view • Managed • Management platform • VLAN name • VLAN ID

Sample report:

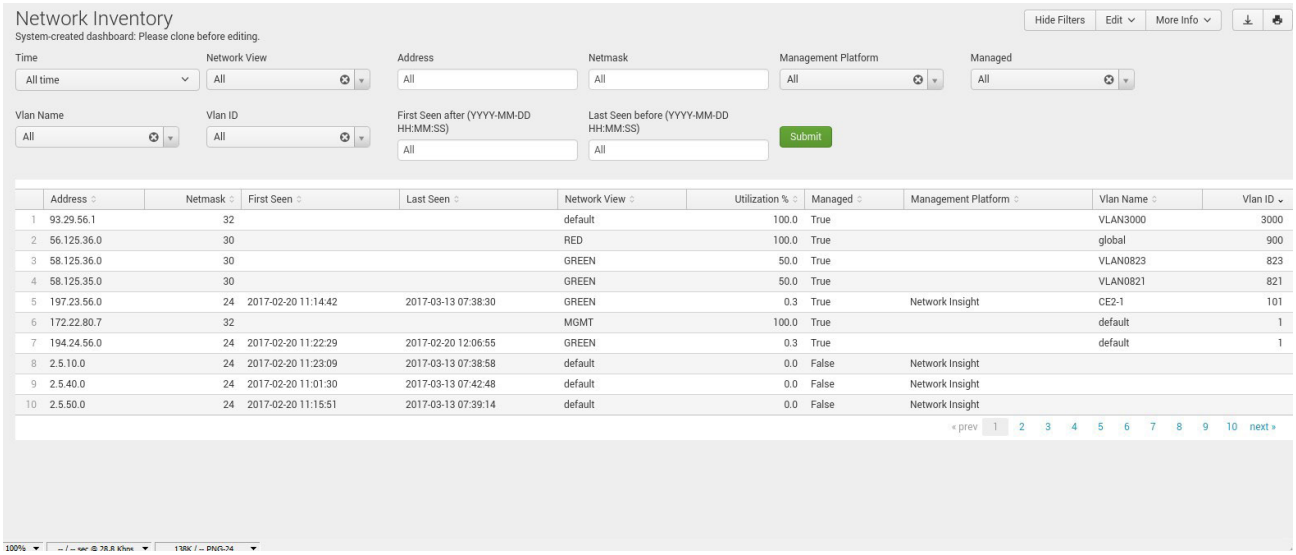


	Address	Netmask	First Seen	Last Seen	Network View	Utilization %	Managed	Management Platform	Vlan Name	Vlan ID
1	93.29.56.1	32			default	100.0	True		VLAN3000	3000
2	56.125.36.0	30			RED	100.0	True		global	900
3	58.125.36.0	30			GREEN	50.0	True		VLAN0823	823
4	58.125.35.0	30			GREEN	50.0	True		VLAN0821	821
5	197.23.56.0	24	2017-02-20 11:14:42	2017-03-13 07:38:30	GREEN	0.3	True	Network Insight	CE2-1	101
6	172.22.80.7	32			MGMT	100.0	True		default	1
7	194.24.56.0	24	2017-02-20 11:22:29	2017-02-20 12:06:55	GREEN	0.3	True		default	1
8	2.5.10.0	24	2017-02-20 11:23:09	2017-03-13 07:38:58	default	0.0	False	Network Insight		
9	2.5.40.0	24	2017-02-20 11:01:30	2017-03-13 07:42:48	default	0.0	False	Network Insight		
10	2.5.50.0	24	2017-02-20 11:15:51	2017-03-13 07:39:14	default	0.0	False	Network Insight		

3.10 Network Inventory

Description	Tracks the inventory of discovered networks
Overview	Discovers, monitors, and tracks the detailed history of each discovered network and the corresponding inventory. This report would help identify discovered networks withspecific details so the IT team can have better day-to-day management, troubleshooting, security, and auditing capabilities.
Data presented	• Address • Netmask • First seen • Last seen • Network view • Utilization % • Managed • Management platform • VLAN name • VLAN ID

Sample report:

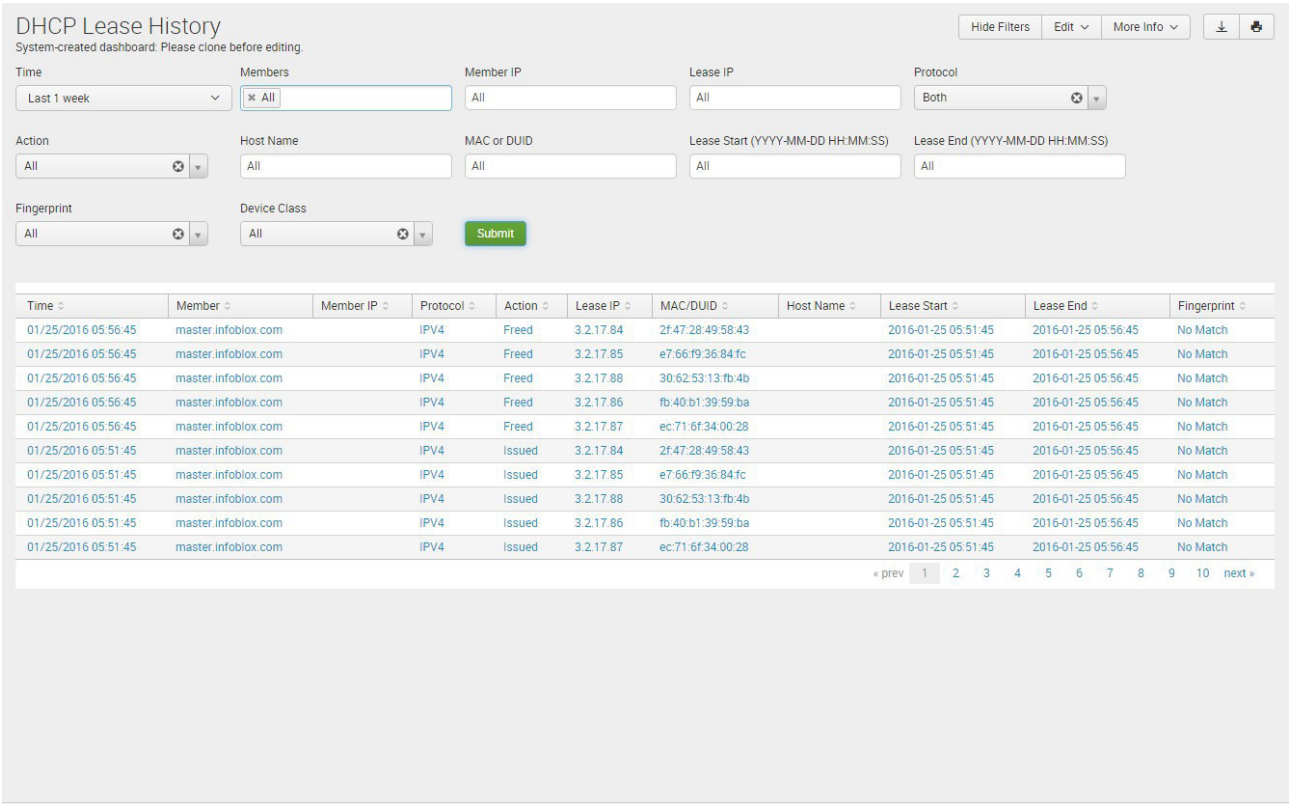


4 DHCP DASHBOARDS

4.1 DHCP Lease History

Description	Shows DHCP history for the given timeframe.
Overview	Provides time-sequenced list of which MAC address requested an IP address and when. Assists with troubleshooting or compliance tracking and auditing.
Data presented	• Time • Members • Member IP • Lease IP • Protocol • Action • Hostname • MAC/DUID • Lease Start • Lease End • Fingerprint • Device Class

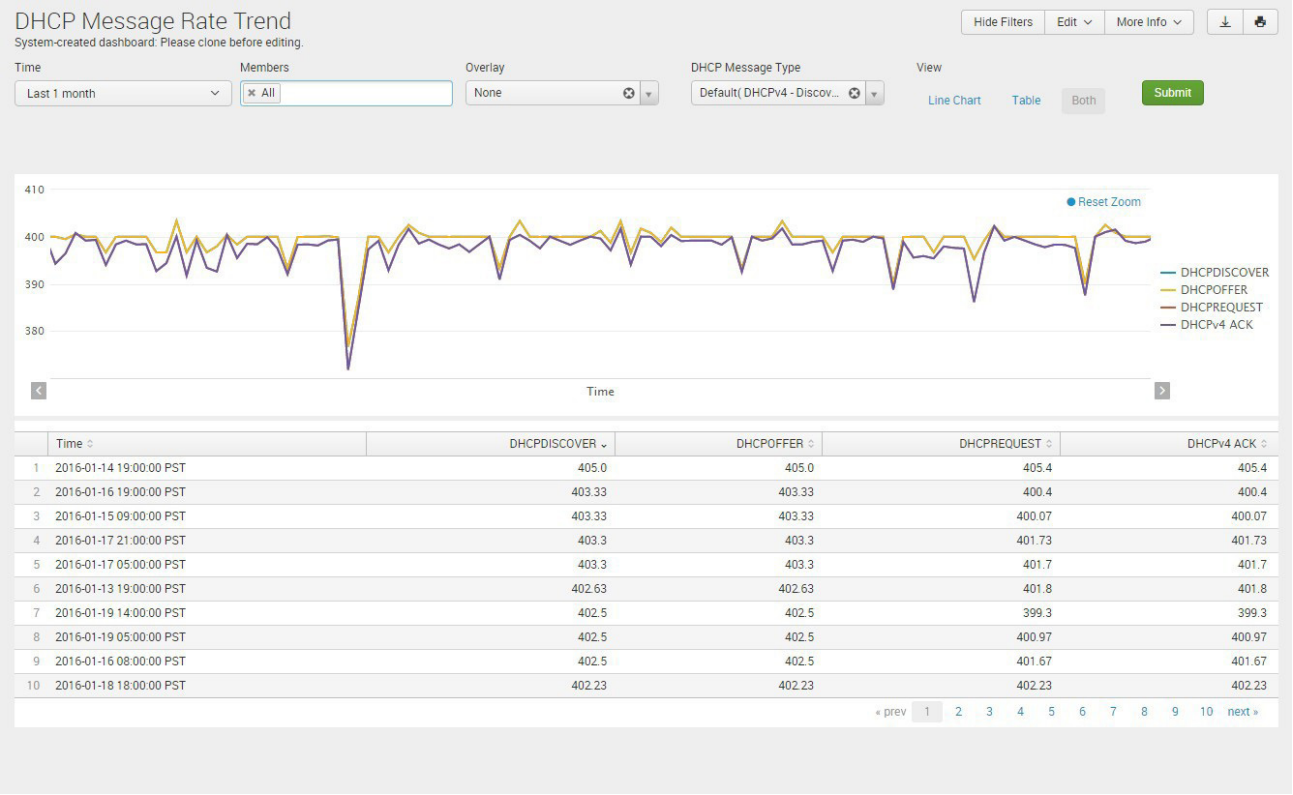
Sample report:



4.2 DHCP Message Rate Trend

Description	DHCP messages rate trend by IP protocol (4 or 6).
Overview	Trends DHCP message rate over time broken down by message time. Helps find unplanned or dangerous activities such as abnormal levels caused by a request storm.
Data presented	• Time • DHCPDISCOVER • DHCPOFFER • DHCPREQUEST • DHCPPACK

Sample report:



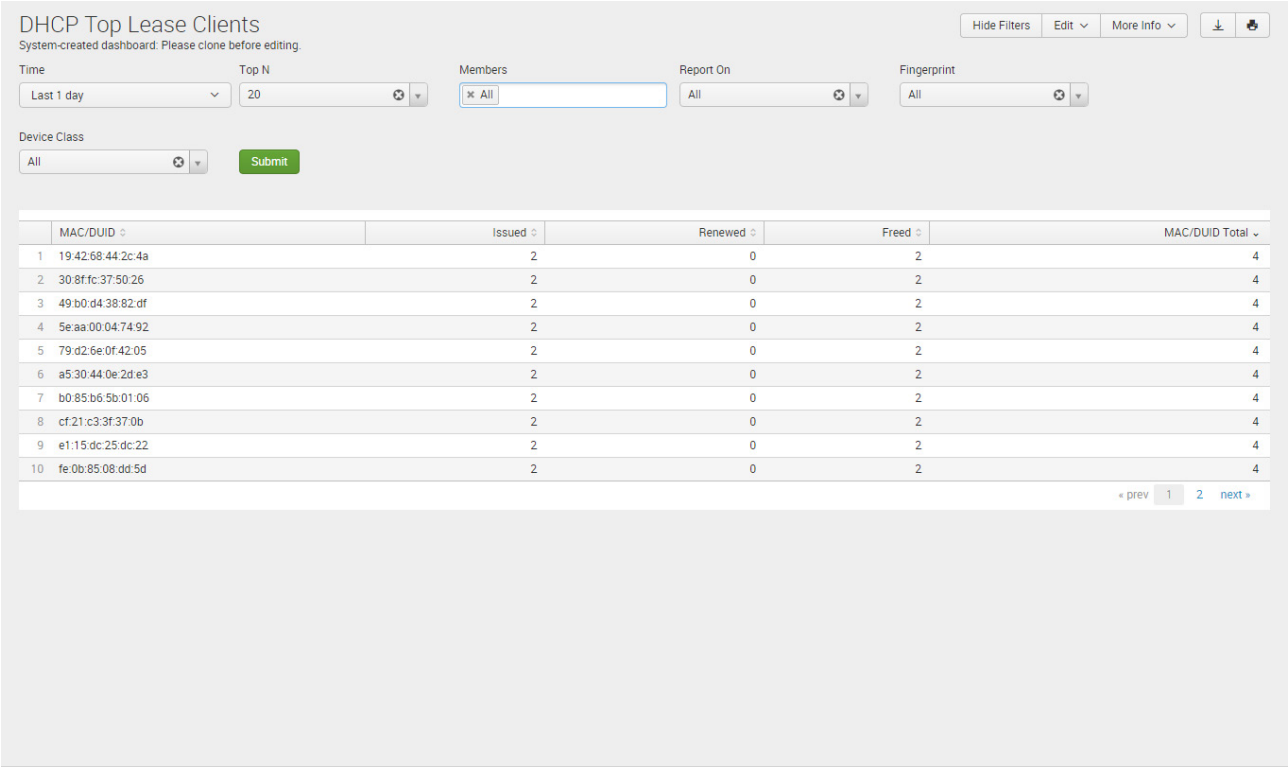
	Time	DHCPDISCOVER	DHCPOFFER	DHCPREQUEST	DHCPv4 ACK
1	2016-01-14 19:00:00 PST	405.0	405.0	405.4	405.4
2	2016-01-16 19:00:00 PST	403.33	403.33	400.4	400.4
3	2016-01-15 09:00:00 PST	403.33	403.33	400.07	400.07
4	2016-01-17 21:00:00 PST	403.3	403.3	401.73	401.73
5	2016-01-17 05:00:00 PST	403.3	403.3	401.7	401.7
6	2016-01-13 19:00:00 PST	402.63	402.63	401.8	401.8
7	2016-01-19 14:00:00 PST	402.5	402.5	399.3	399.3
8	2016-01-19 05:00:00 PST	402.5	402.5	400.97	400.97
9	2016-01-16 08:00:00 PST	402.5	402.5	401.67	401.67
10	2016-01-18 18:00:00 PST	402.23	402.23	402.23	402.23

« prev 1 2 3 4 5 6 7 8 9 10 next »

4.3 DHCP Top Lease Clients

Description	Top DHCP activity by MAC/DUID address
Overview	Shows the top N generators of DHCP by message type. Helps identify heavy internal users or pinpoint security risks of unplanned activity.
Data presented	• MAC/DUID • Issued • Renewed • Freed • MAC/DUID Total • Fingerprint

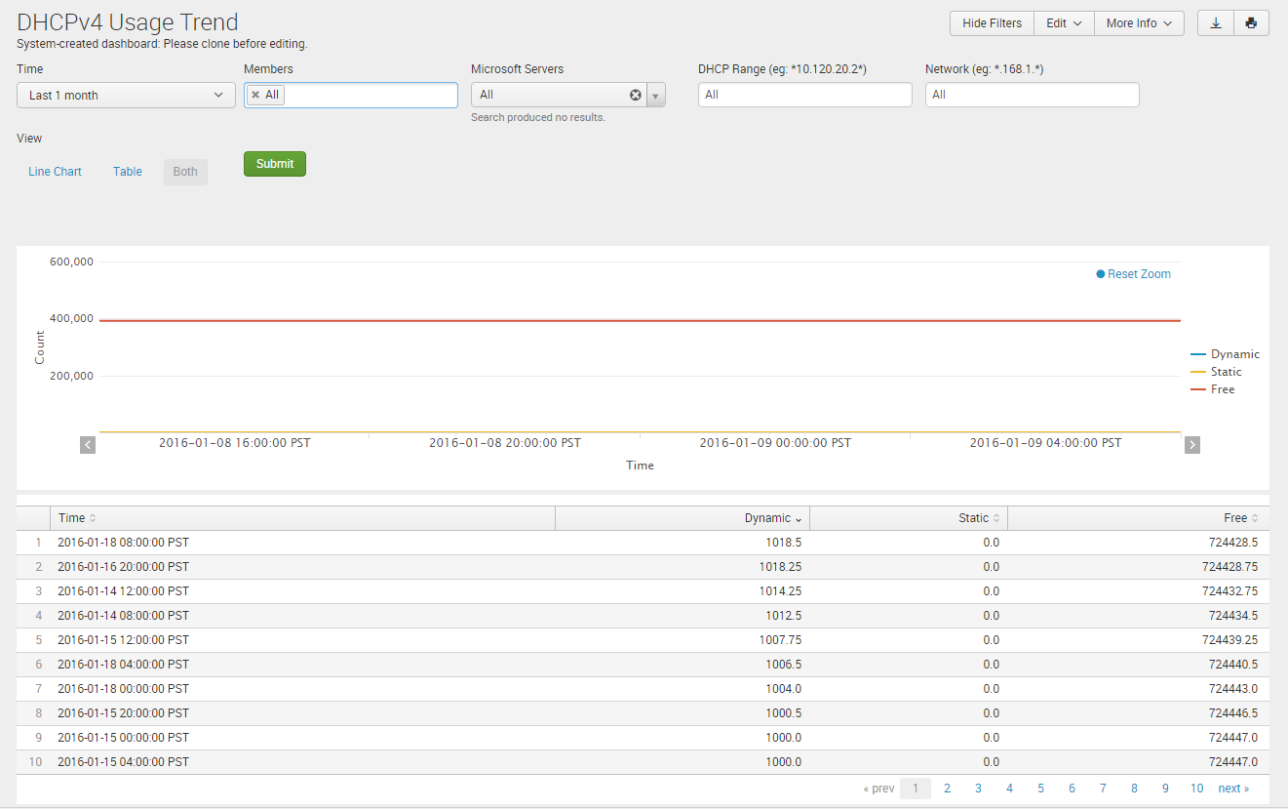
Sample report:



4.4 DHCPv4 Usage Trend

Description	DHCPv4 usage overall – for a given time window and IPv4 network address range provide usage snapshot
Overview	Shows DHCP utilization trends across an entire IP address space or selection range and trends over time. Helps identify utilization changes and improves planning to handle ongoing variations.
Data presented	• Time • Dynamic • Static • Free

Sample report:



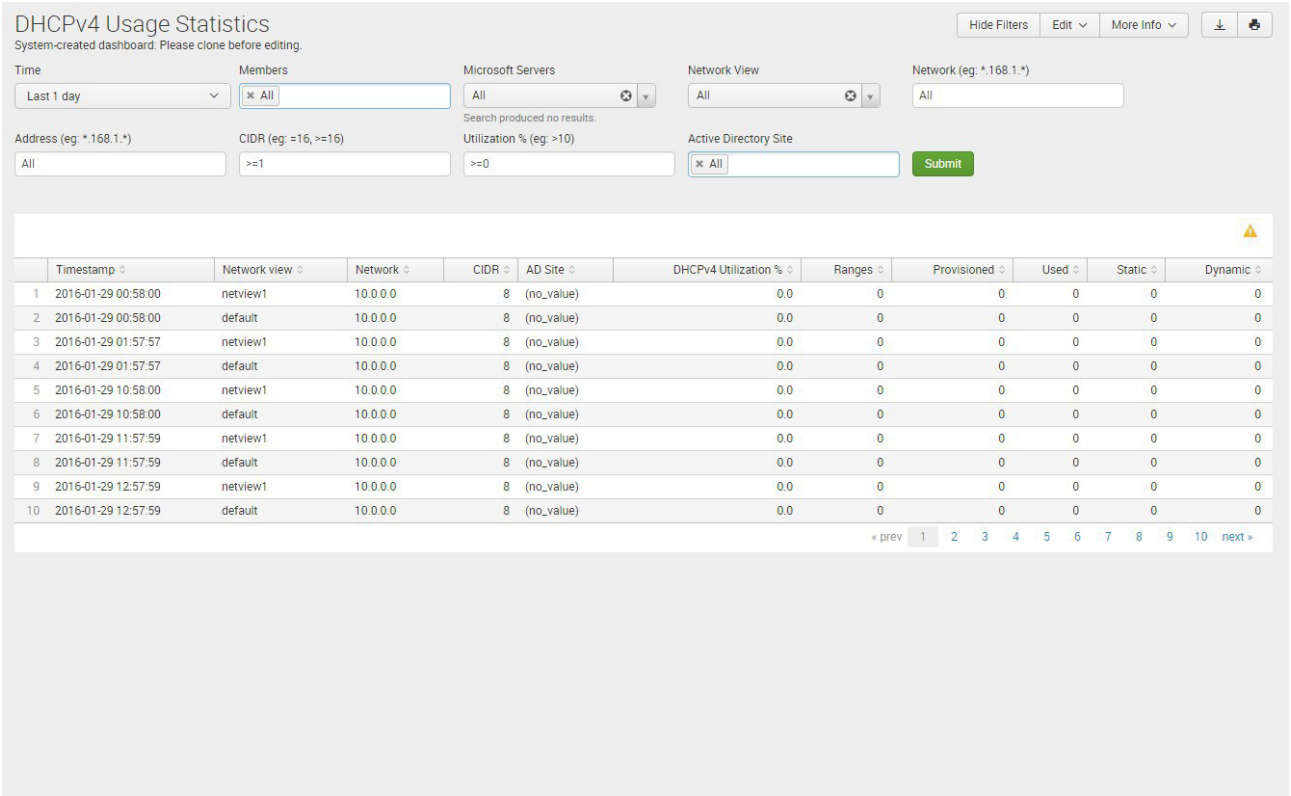
	Time	Dynamic	Static	Free
1	2016-01-18 08:00:00 PST	1018.5	0.0	724428.5
2	2016-01-16 20:00:00 PST	1018.25	0.0	724428.75
3	2016-01-14 12:00:00 PST	1014.25	0.0	724432.75
4	2016-01-14 08:00:00 PST	1012.5	0.0	724434.5
5	2016-01-15 12:00:00 PST	1007.75	0.0	724439.25
6	2016-01-18 04:00:00 PST	1006.5	0.0	724440.5
7	2016-01-18 00:00:00 PST	1004.0	0.0	724443.0
8	2016-01-15 20:00:00 PST	1000.5	0.0	724446.5
9	2016-01-15 00:00:00 PST	1000.0	0.0	724447.0
10	2016-01-15 04:00:00 PST	1000.0	0.0	724447.0

« prev 1 2 3 4 5 6 7 8 9 10 next »

4.5 DHCPv4 Usage Statistics

Description	DHCP usage overall – for a given time window and IPv4 network address range provide usage snapshot
Overview	Shows the DHCP usage and activity over time for a selected IP address range. Provides detailed visibility into usage at any point in time which assists with troubleshooting or compliance auditing requirements.
Data presented	• Timestamps • Network View • Network • CIDR • AD Site • DHCPv4 Utilization • Ranges • Provisioned • Dynamic • Static • Free • Used

Sample report:

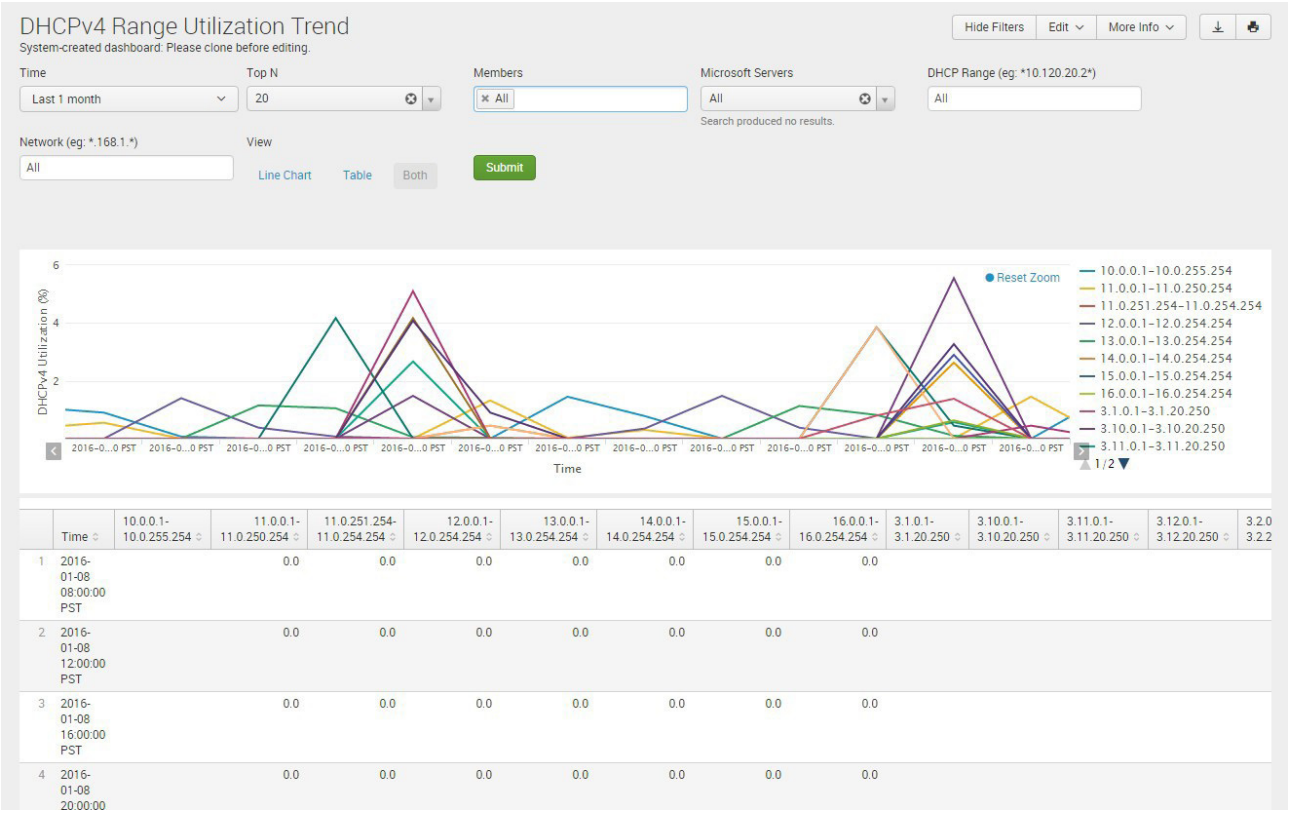


	Timestamp	Network view	Network	CIDR	AD Site	DHCPv4 Utilization %	Ranges	Provisioned	Used	Static	Dynamic
1	2016-01-29 00:58:00	netview1	10.0.0.0	8	(no_value)	0.0	0	0	0	0	0
2	2016-01-29 00:58:00	default	10.0.0.0	8	(no_value)	0.0	0	0	0	0	0
3	2016-01-29 01:57:57	netview1	10.0.0.0	8	(no_value)	0.0	0	0	0	0	0
4	2016-01-29 01:57:57	default	10.0.0.0	8	(no_value)	0.0	0	0	0	0	0
5	2016-01-29 10:58:00	netview1	10.0.0.0	8	(no_value)	0.0	0	0	0	0	0
6	2016-01-29 10:58:00	default	10.0.0.0	8	(no_value)	0.0	0	0	0	0	0
7	2016-01-29 11:57:59	netview1	10.0.0.0	8	(no_value)	0.0	0	0	0	0	0
8	2016-01-29 11:57:59	default	10.0.0.0	8	(no_value)	0.0	0	0	0	0	0
9	2016-01-29 12:57:59	netview1	10.0.0.0	8	(no_value)	0.0	0	0	0	0	0
10	2016-01-29 12:57:59	default	10.0.0.0	8	(no_value)	0.0	0	0	0	0	0

4.6 DHCPv4 Range Utilization Trend

Description	DHCP utilization by IPv4 network range and time frame
Overview	Highlights the DHCP range utilization for selected address ranges over time. Allows for better tracking and trending of DHCP resources to avoid overutilization.
Data presented	• Time • Dynamic • Static • Free

Sample report:

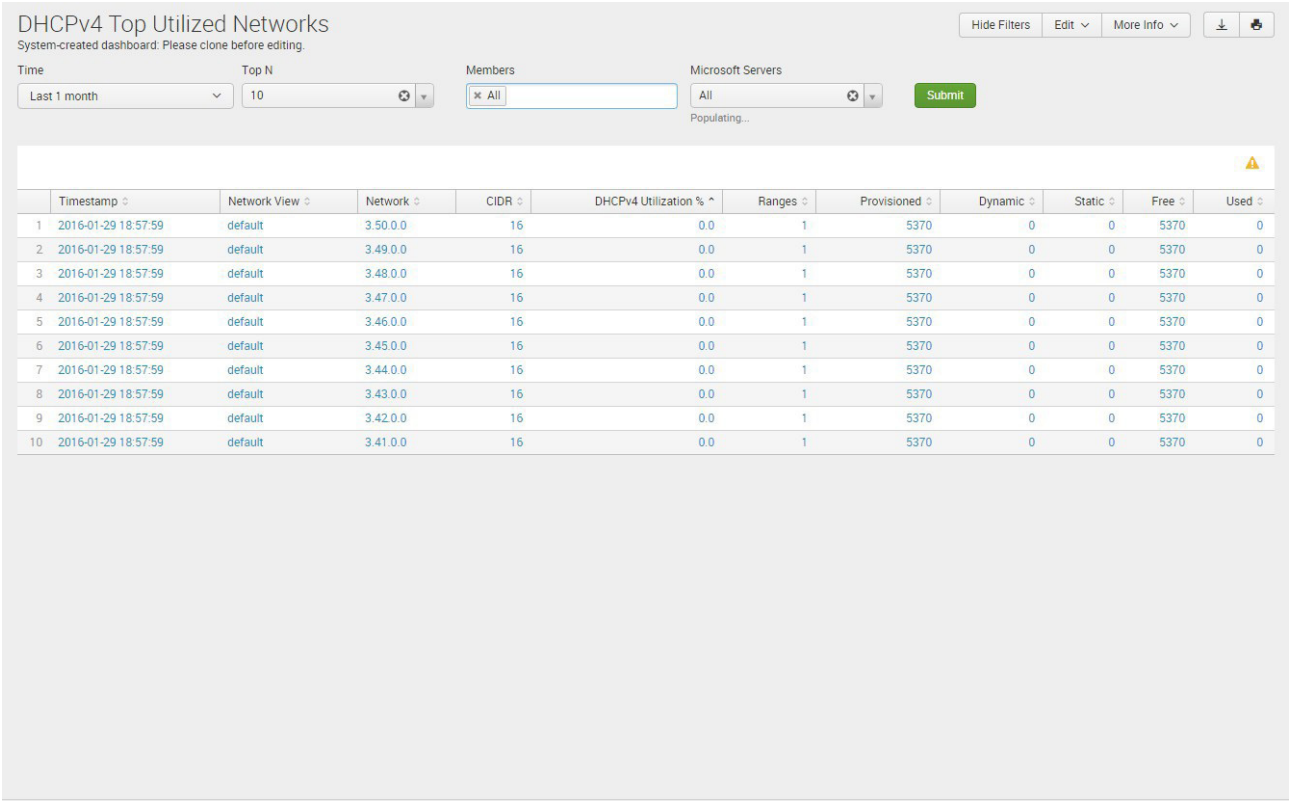


	Time	10.0.0.1-10.0.255.254	11.0.0.1-11.0.250.254	11.0.251.254-11.0.254.254	12.0.0.1-12.0.254.254	13.0.0.1-13.0.254.254	14.0.0.1-14.0.254.254	15.0.0.1-15.0.254.254	16.0.0.1-16.0.254.254	3.1.0.1-3.1.20.250	3.10.0.1-3.10.20.250	3.11.0.1-3.11.20.250	3.12.0.1-3.12.20.250	3.2.0 3.2.2
1	2016-01-08 08:00:00 PST		0.0	0.0	0.0	0.0	0.0	0.0	0.0					
2	2016-01-08 12:00:00 PST		0.0	0.0	0.0	0.0	0.0	0.0	0.0					
3	2016-01-08 16:00:00 PST		0.0	0.0	0.0	0.0	0.0	0.0	0.0					
4	2016-01-08 20:00:00		0.0	0.0	0.0	0.0	0.0	0.0	0.0					

4.7 DHCPv4 Top Utilized Networks

Description	Tracks the utilization of DHCP by subnet
Overview	Shows the most utilized subnets in terms of IP address consumption including the DHCP range in each subnet. Helps track usage trends over time and plan for future resource allocation.
Data presented	• Timestamp • Network View • Network • CIDR • DHCPv4 Utilization % • Ranges • Provisioned • Dynamic • Static • Free • Used

Sample report:

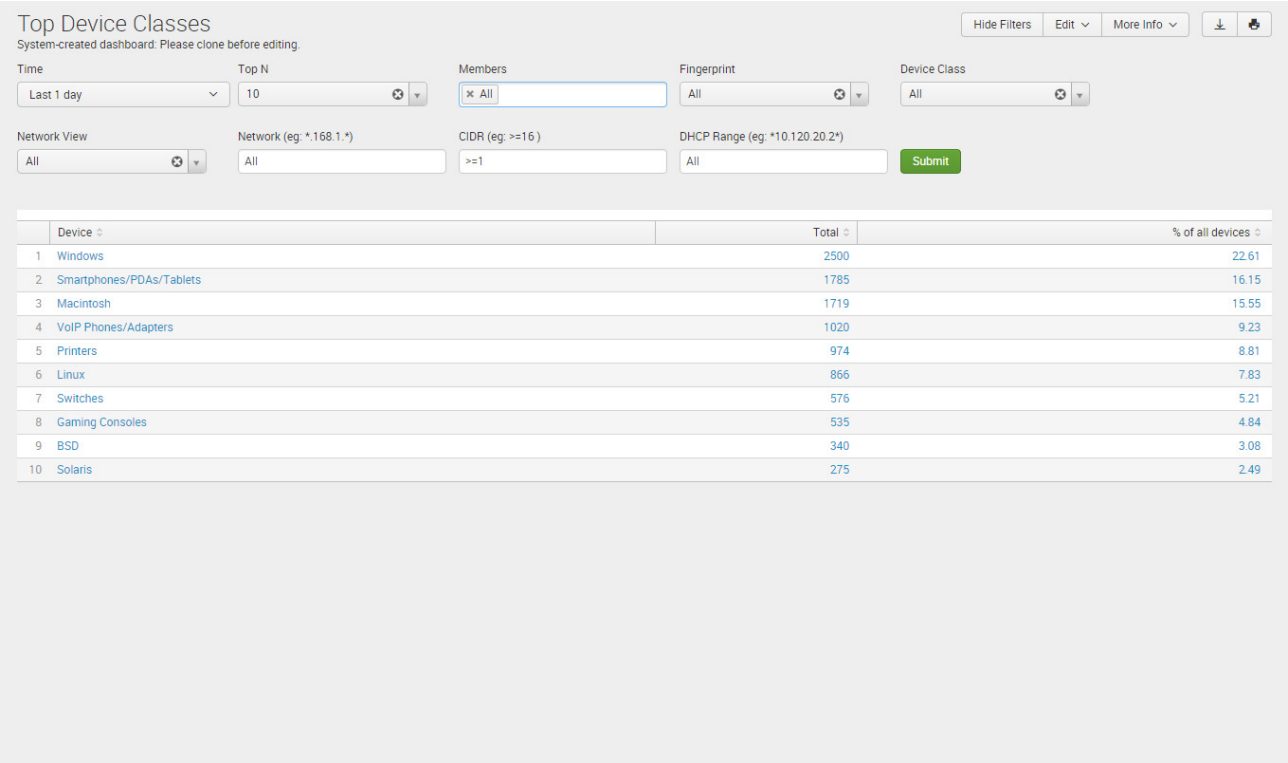


	Timestamp	Network View	Network	CIDR	DHCPv4 Utilization %	Ranges	Provisioned	Dynamic	Static	Free	Used
1	2016-01-29 18:57:59	default	3.50.0.0	16	0.0	1	5370	0	0	5370	0
2	2016-01-29 18:57:59	default	3.49.0.0	16	0.0	1	5370	0	0	5370	0
3	2016-01-29 18:57:59	default	3.48.0.0	16	0.0	1	5370	0	0	5370	0
4	2016-01-29 18:57:59	default	3.47.0.0	16	0.0	1	5370	0	0	5370	0
5	2016-01-29 18:57:59	default	3.46.0.0	16	0.0	1	5370	0	0	5370	0
6	2016-01-29 18:57:59	default	3.45.0.0	16	0.0	1	5370	0	0	5370	0
7	2016-01-29 18:57:59	default	3.44.0.0	16	0.0	1	5370	0	0	5370	0
8	2016-01-29 18:57:59	default	3.43.0.0	16	0.0	1	5370	0	0	5370	0
9	2016-01-29 18:57:59	default	3.42.0.0	16	0.0	1	5370	0	0	5370	0
10	2016-01-29 18:57:59	default	3.41.0.0	16	0.0	1	5370	0	0	5370	0

4.8 Top Device Classes

Description	Top Device Classes
Overview	Identifies and highlights the top device operating systems broken down by classes that receive DHCP leases. Helps identify which manufacturers and operating systems are being used so IT can identify non-supported devices or plan for future requirements.
Data presented	• Device Class • Total • % of all devices

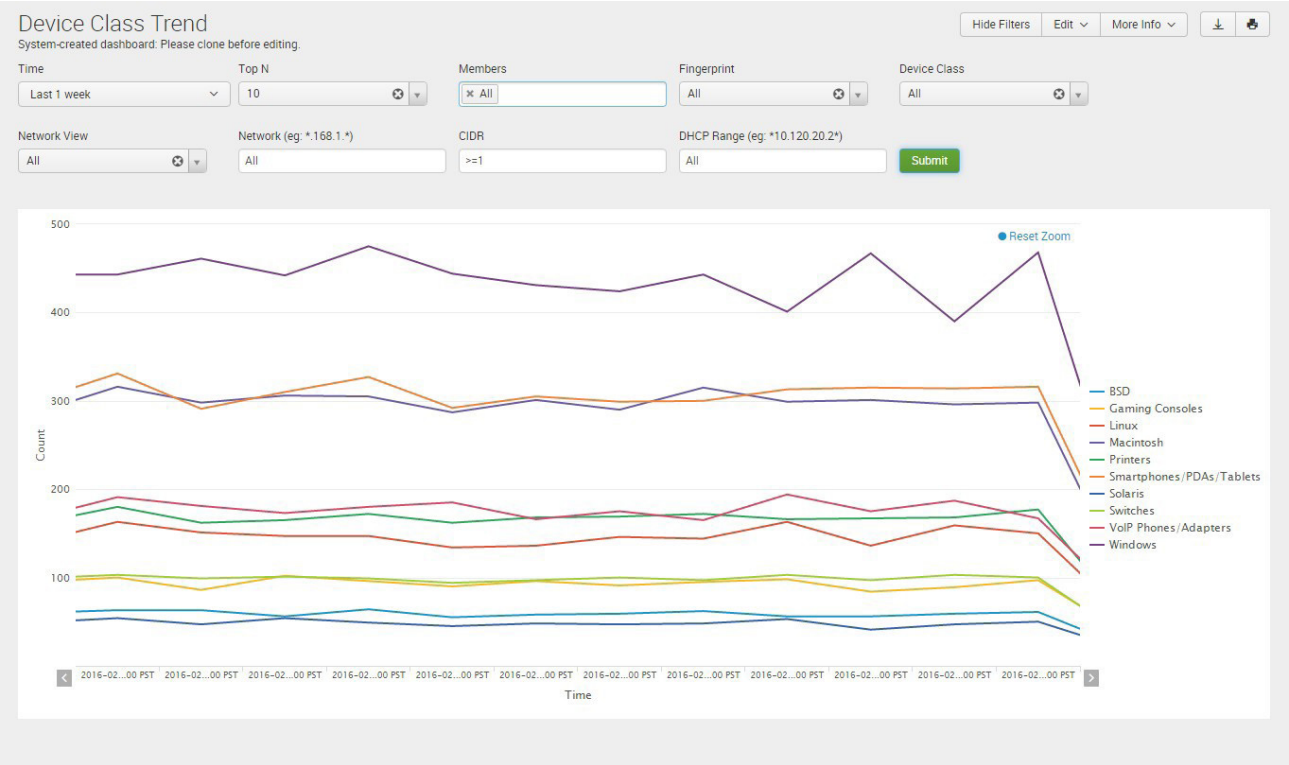
Sample report:



4.9 Device Class Trend

Description	Tracks the device class trend over time
Overview	Identifies and highlights the top device operating systems broken down by class that receive DHCP leases over time. Helps identify which device classes are being used so IT can find trends, identify non-supported devices or plan for future requirements.
Data presented	• Timestamp • Device Count • Device Class

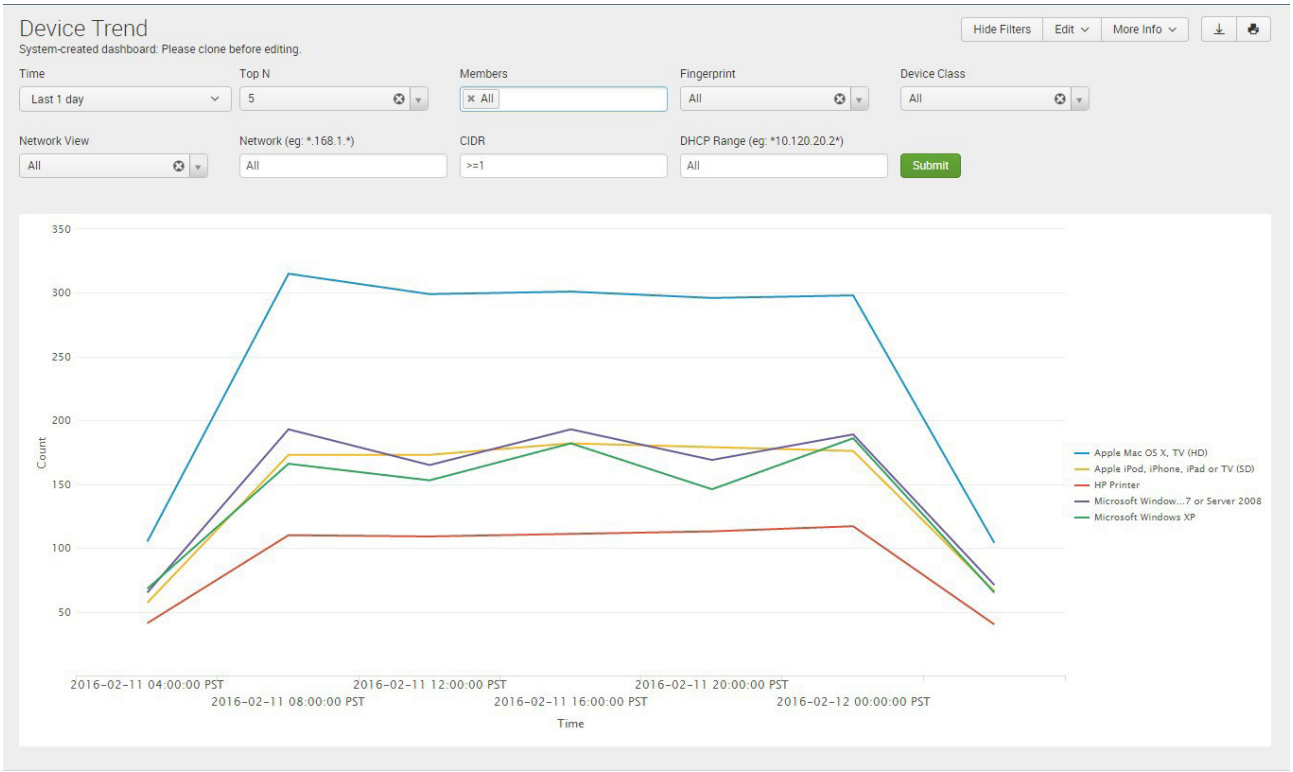
Sample report:



4.10 Device Trend

Description	Tracks the device type trend over time
Overview	Identifies and highlights the top device operating systems that receive DHCP leases over time. Helps identify which manufacturers and operating systems are being used so IT can find trends in usage, identify non-supported devices or plan for future requirements.
Data presented	• Timestamp • Device Count • Device Class

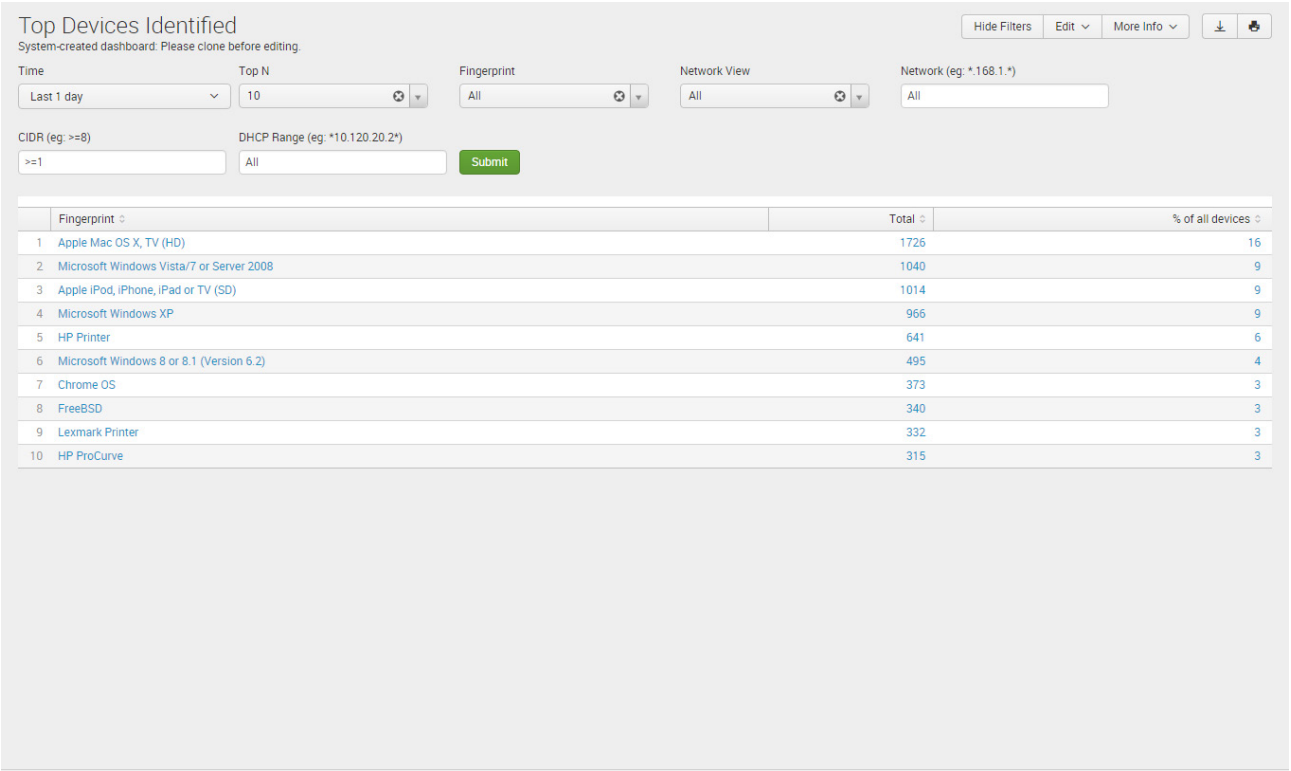
Sample report:



4.11 Top Devices Identified

Description	Tracks the devices identified
Overview	Identifies and highlights the top device operating systems that receive DHCP leases. Helps identify which manufacturers and operating systems are being used so IT can find trends in usage, identify non-supported devices or plan for future requirements.
Data presented	• Fingerprint • Total • % of all devices

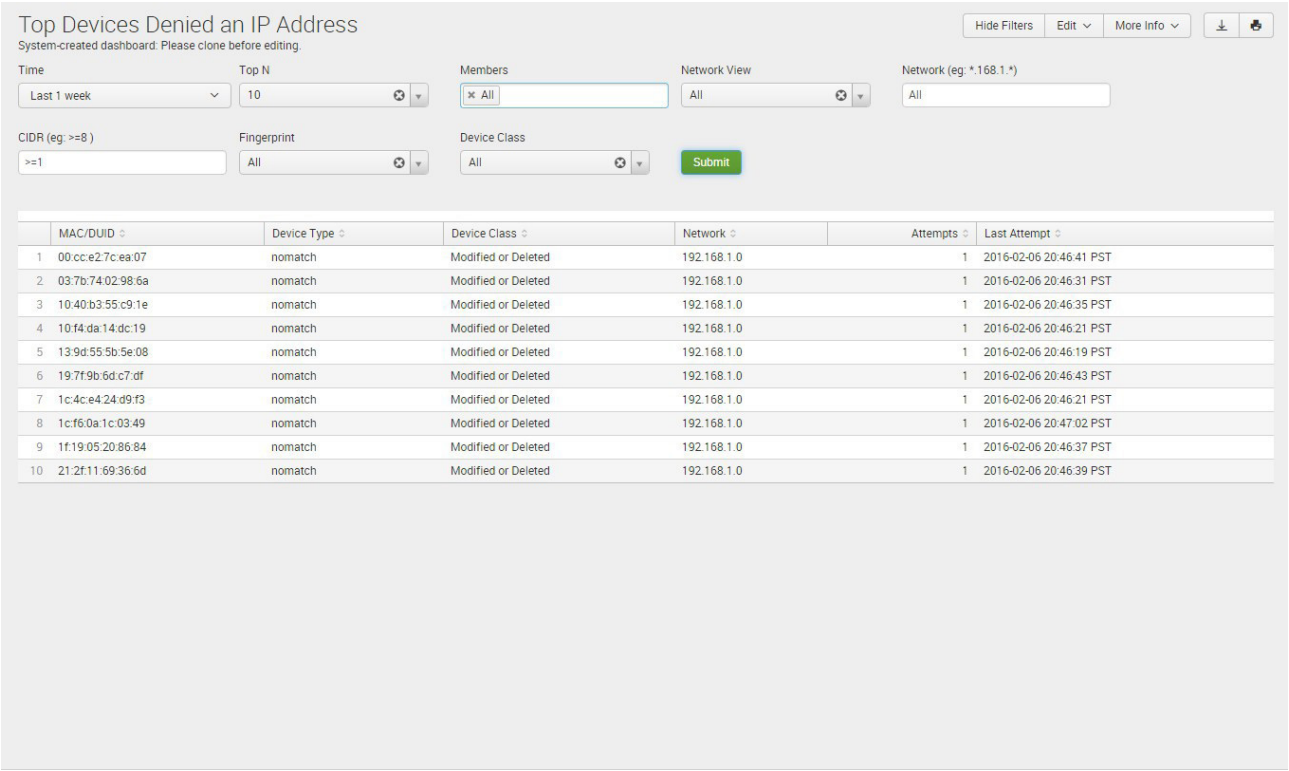
Sample report:



4.12 Top Devices Denied an IP Address

Description	Tracks devices that were denied an IP address
Overview	Identifies the top number of devices that were denied an IP address using DHCPv4 Fingerprint Filters. Helps pinpoint potential problem areas regarding the attempted use of devices that do not comply to corporate use policy.
Data presented	• MAC/DUID • Fingerprint • Device Class • Network • Attempts • Last Attempt

Sample report:

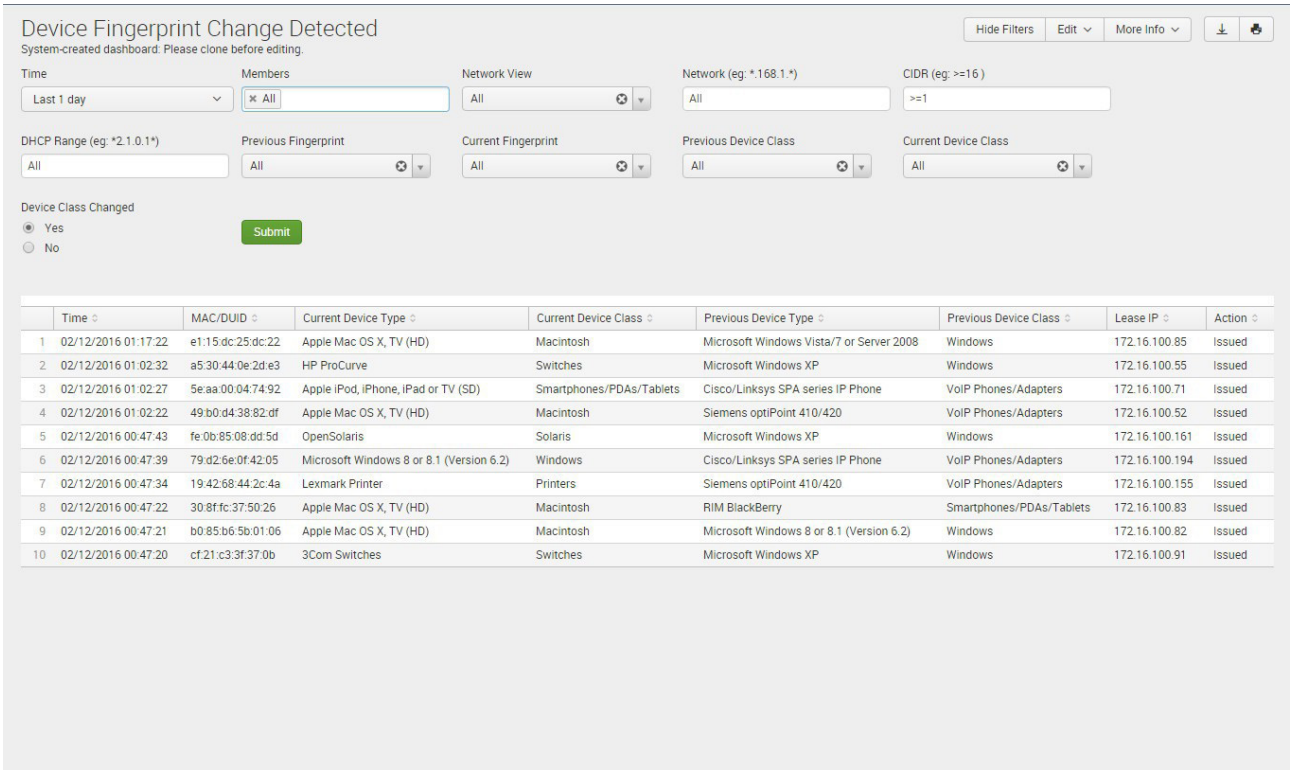


	MAC/DUID	Device Type	Device Class	Network	Attempts	Last Attempt
1	00:cc:e2:7c:ea:07	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:41 PST
2	03:7b:74:02:98:6a	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:31 PST
3	10:40:b3:55:c9:1e	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:35 PST
4	10:f4:da:14:dc:19	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:21 PST
5	13:9d:55:5b:5e:08	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:19 PST
6	19:7f:9b:6d:c7:df	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:43 PST
7	1c:4c:e4:24:d9:f3	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:21 PST
8	1c:f6:0a:1c:03:49	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:47:02 PST
9	1f:19:05:20:86:84	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:37 PST
10	21:2f:11:69:36:6d	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:39 PST

4.13 Device Fingerprint Change Detected

Description	Tracks when a device changes fingerprint type
Overview	Identifies and highlights when the device identified using DHCP Fingerprinting has changed. Helps identify attempts to misrepresent a device through a method called MAC Spoofing. It can also be used to identify when a desktop is using Virtual Machine software or software such as Apple's Bootcamp.
Data presented	• Time • MAC/DUID • Current Device Type • Current Device Class • Previous Device Type • Previous Device Class • Lease IP • Action

Sample report:



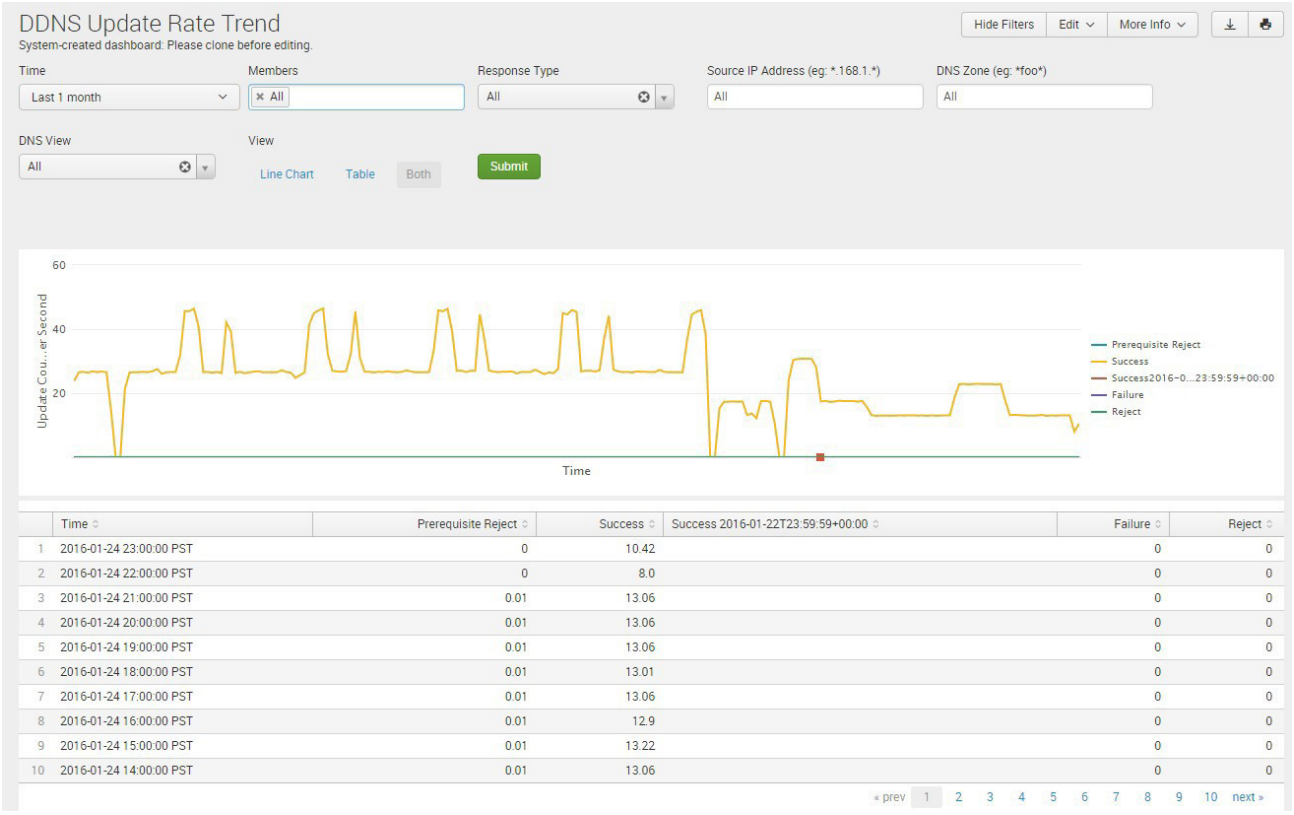
	Time	MAC/DUID	Current Device Type	Current Device Class	Previous Device Type	Previous Device Class	Lease IP	Action
1	02/12/2016 01:17:22	e1:15:dc:25:dc:22	Apple Mac OS X, TV (HD)	Macintosh	Microsoft Windows Vista/7 or Server 2008	Windows	172.16.100.85	Issued
2	02/12/2016 01:02:32	a5:30:44:0e:2d:e3	HP ProCurve	Switches	Microsoft Windows XP	Windows	172.16.100.55	Issued
3	02/12/2016 01:02:27	5e:aa:00:04:74:92	Apple iPod, iPhone, iPad or TV (SD)	Smartphones/PDAs/Tablets	Cisco/Linksys SPA series IP Phone	VoIP Phones/Adapters	172.16.100.71	Issued
4	02/12/2016 01:02:22	49:b0:d4:38:82:df	Apple Mac OS X, TV (HD)	Macintosh	Siemens optiPoint 410/420	VoIP Phones/Adapters	172.16.100.52	Issued
5	02/12/2016 00:47:43	fe:0b:85:08:dd:5d	OpenSolaris	Solaris	Microsoft Windows XP	Windows	172.16.100.161	Issued
6	02/12/2016 00:47:39	79:d2:6e:0f:42:05	Microsoft Windows 8 or 8.1 (Version 6.2)	Windows	Cisco/Linksys SPA series IP Phone	VoIP Phones/Adapters	172.16.100.194	Issued
7	02/12/2016 00:47:34	19:42:68:44:2c:4a	Lexmark Printer	Printers	Siemens optiPoint 410/420	VoIP Phones/Adapters	172.16.100.155	Issued
8	02/12/2016 00:47:22	30:8f:fc:37:50:26	Apple Mac OS X, TV (HD)	Macintosh	RIM BlackBerry	Smartphones/PDAs/Tablets	172.16.100.83	Issued
9	02/12/2016 00:47:21	b0:85:b6:5b:01:06	Apple Mac OS X, TV (HD)	Macintosh	Microsoft Windows 8 or 8.1 (Version 6.2)	Windows	172.16.100.82	Issued
10	02/12/2016 00:47:20	cf:21:c3:3f:37:0b	3Com Switches	Switches	Microsoft Windows XP	Windows	172.16.100.91	Issued

5 DNS DASHBOARDS

5.1 DDNS Update Rate Trend

Description	Shows DDNS update count by response type
Overview	Shows the specific DDNS updates (by type) received by a selected IP address over a given time period. Allows better tracking and trending for planning.
Data presented	• Timestamp • Success • Failure • Reject • Prerequisite Reject

Sample report:



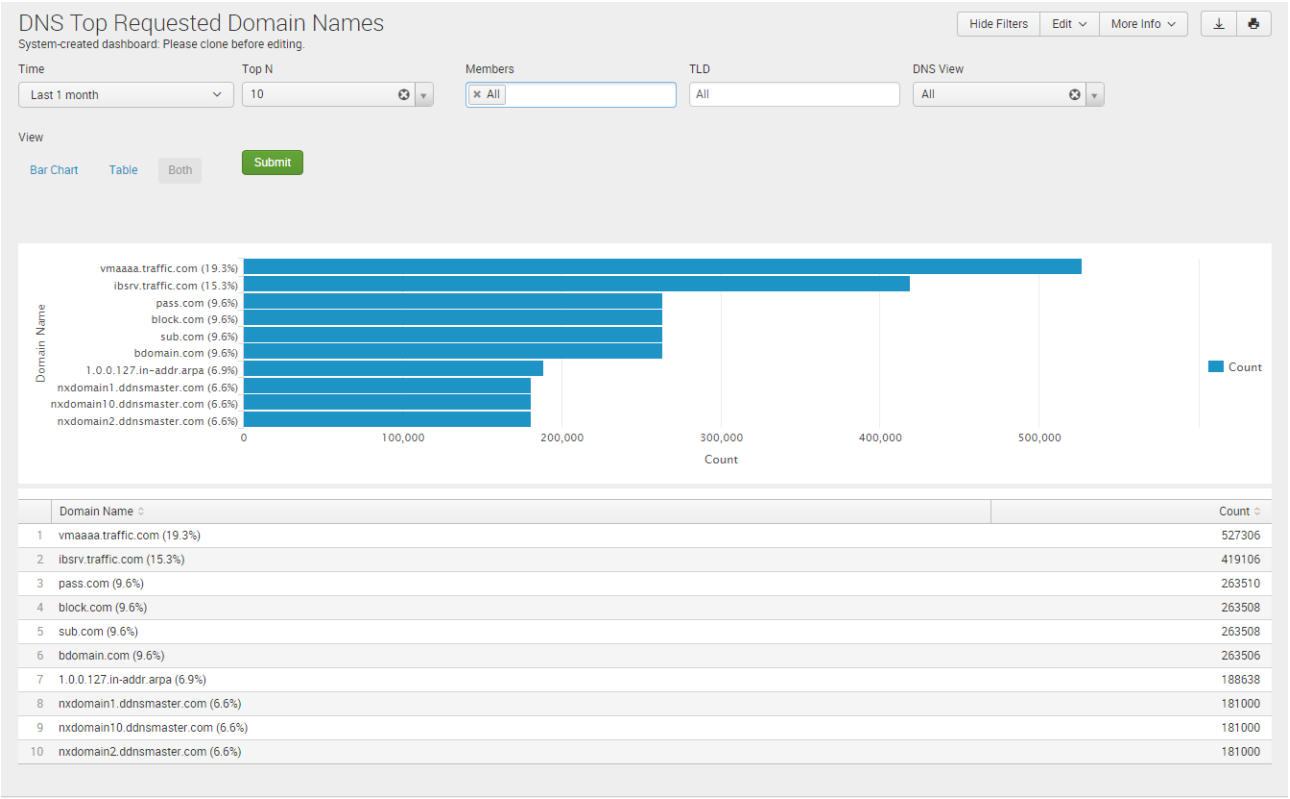
	Time	Prerequisite Reject	Success	Success 2016-01-22T23:59:59+00:00	Failure	Reject
1	2016-01-24 23:00:00 PST	0	10.42		0	0
2	2016-01-24 22:00:00 PST	0	8.0		0	0
3	2016-01-24 21:00:00 PST	0.01	13.06		0	0
4	2016-01-24 20:00:00 PST	0.01	13.06		0	0
5	2016-01-24 19:00:00 PST	0.01	13.06		0	0
6	2016-01-24 18:00:00 PST	0.01	13.01		0	0
7	2016-01-24 17:00:00 PST	0.01	13.06		0	0
8	2016-01-24 16:00:00 PST	0.01	12.9		0	0
9	2016-01-24 15:00:00 PST	0.01	13.22		0	0
10	2016-01-24 14:00:00 PST	0.01	13.06		0	0

« prev 1 2 3 4 5 6 7 8 9 10 next »

5.2 DNS Top Requested Domain Names

Description	List Top Requested Domain Names
Overview	Provides visibility of the top domains being requested (based on filter settings) to help assign proper distribution of resources and identify where users are going or what applications they are accessing.
Data presented	• Domain Names (Fully Qualified Domain Names) • Query Counts per DNS Domain Name • Query Percentage (for the time frame)

Sample report:

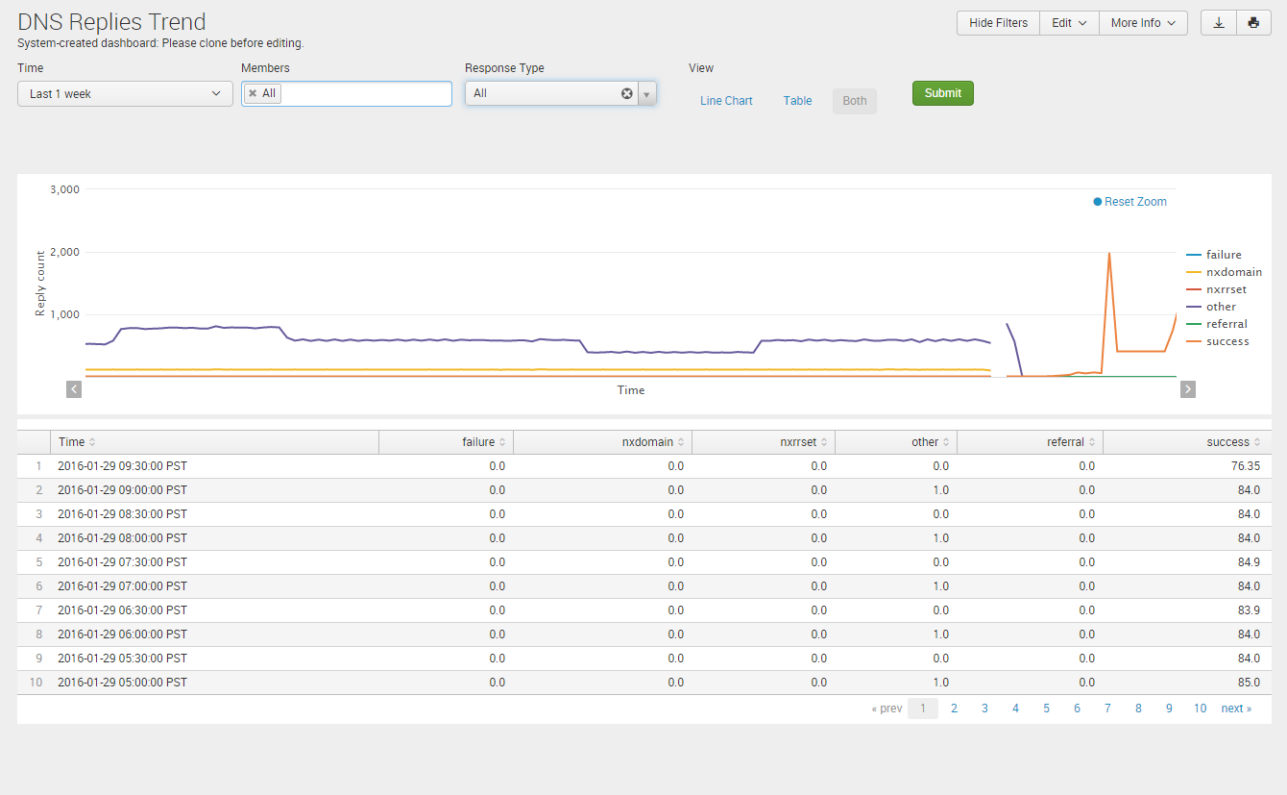


	Domain Name	Count
1	vmaaaa.traffic.com (19.3%)	527306
2	ibsrv.traffic.com (15.3%)	419106
3	pass.com (9.6%)	263510
4	block.com (9.6%)	263508
5	sub.com (9.6%)	263508
6	bdomain.com (9.6%)	263506
7	1.0.0.127.in-addr.arpa (6.9%)	188638
8	nxdomain1.ddnsmaster.com (6.6%)	181000
9	nxdomain10.ddnsmaster.com (6.6%)	181000
10	nxdomain2.ddnsmaster.com (6.6%)	181000

5.3 DNS Replies Trend

Description	List DNS Query Replies by Reply Code
Overview	Provides insight into how effectively DNS queries are being processed. This report can be used to measure successful queries and to identify changes in the number of failed or unsuccessful queries.
Data presented	Query Reply Count by Reply Code • Failure • Success • Referral • NXRRset • NXDomain • Refused • Other

Sample report:



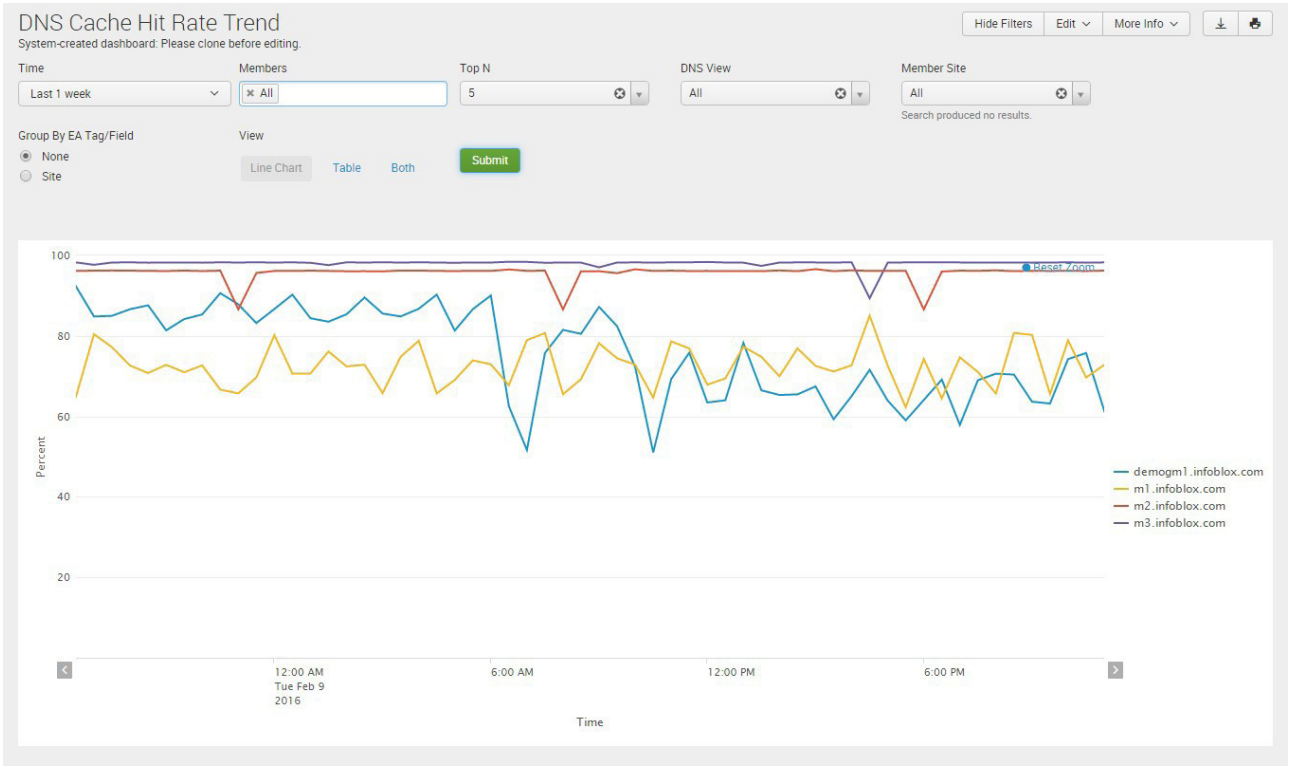
	Time	failure	nxdomain	nxrrset	other	referral	success
1	2016-01-29 09:30:00 PST	0.0	0.0	0.0	0.0	0.0	76.35
2	2016-01-29 09:00:00 PST	0.0	0.0	0.0	1.0	0.0	84.0
3	2016-01-29 08:30:00 PST	0.0	0.0	0.0	0.0	0.0	84.0
4	2016-01-29 08:00:00 PST	0.0	0.0	0.0	1.0	0.0	84.0
5	2016-01-29 07:30:00 PST	0.0	0.0	0.0	0.0	0.0	84.9
6	2016-01-29 07:00:00 PST	0.0	0.0	0.0	1.0	0.0	84.0
7	2016-01-29 06:30:00 PST	0.0	0.0	0.0	0.0	0.0	83.9
8	2016-01-29 06:00:00 PST	0.0	0.0	0.0	1.0	0.0	84.0
9	2016-01-29 05:30:00 PST	0.0	0.0	0.0	0.0	0.0	84.0
10	2016-01-29 05:00:00 PST	0.0	0.0	0.0	1.0	0.0	85.0

« prev 1 2 3 4 5 6 7 8 9 10 next »

5.4 DNS Cache Hit Rate Trend

Description	Cache hit ratio by server
Overview	Provides DNS cache hit ratio over time for DNS servers. Helps identify how server is performing, what percent of queries are already in cache and what percent of queries is unique.
Data presented	• Server Node • Cache hit rate (%) • By unit of time

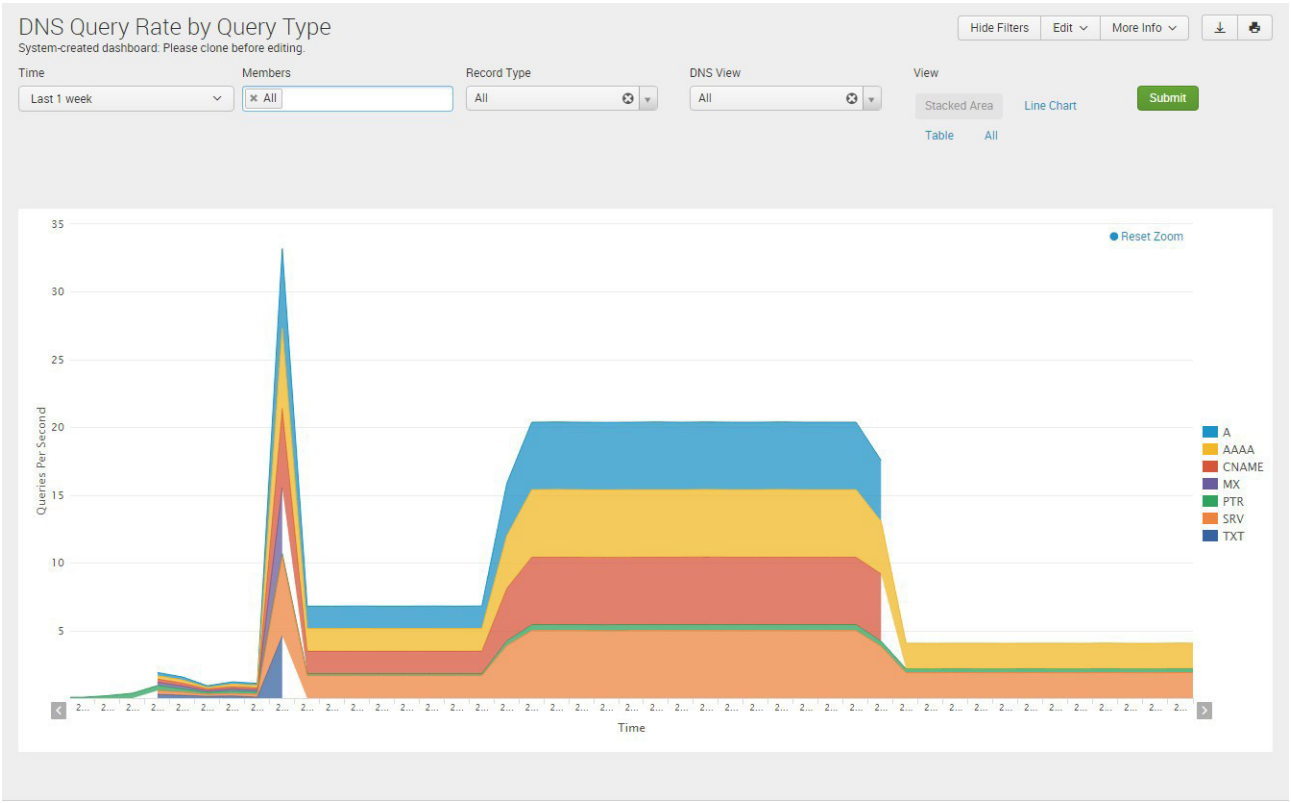
Sample report:



5.5 DNS Query Rate by Query Type

Description	List DNS Query Rates by Query Type
Overview	Shows the types of DNS requests by volume over time for DNS servers. Helps pinpoint trends in requests by users across the infrastructure.
Data presented	Query Types (Total, Average, Maximum) • AAAA • CNAME • NS • ANY • A • MX • PTR • SOA • TKEY • Other

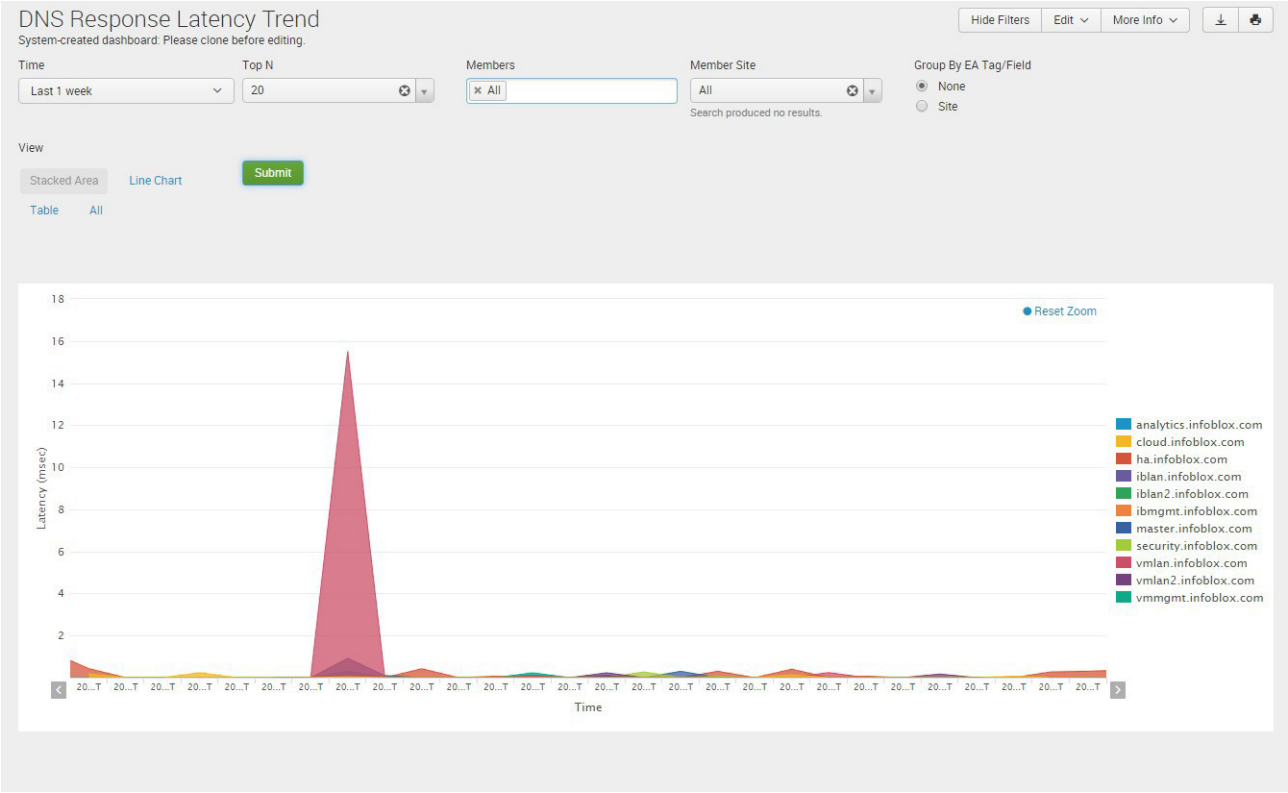
Sample report:



5.6 DNS Response Latency Trend

Description	Map DNS Latency Response time for all or selected cache servers.
Overview	Provides the DNS latency or round-trip response time for DNS queries. This data helps identify potential “slow” or problem areas based on filters.
Data presented	• Overall DNS response latency in milliseconds

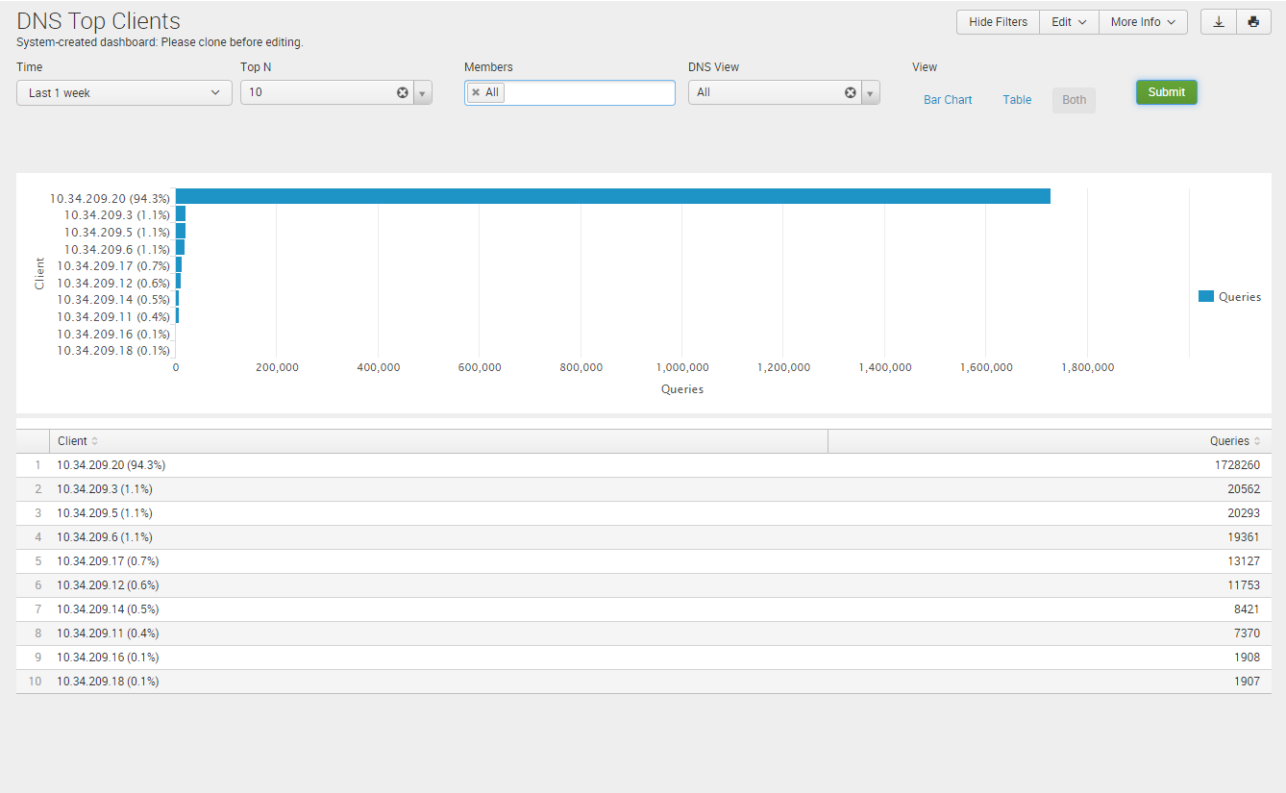
Sample report:



5.7 DNS Top Clients

Description	Shows clients with the most DNS queries
Overview	Highlights the top N requestors – shows which clients are sending the most queries over a selected time period. Helps identify top talkers and potential risk areas.
Data presented	• Source IP addresses • Number of queries generated

Sample report:

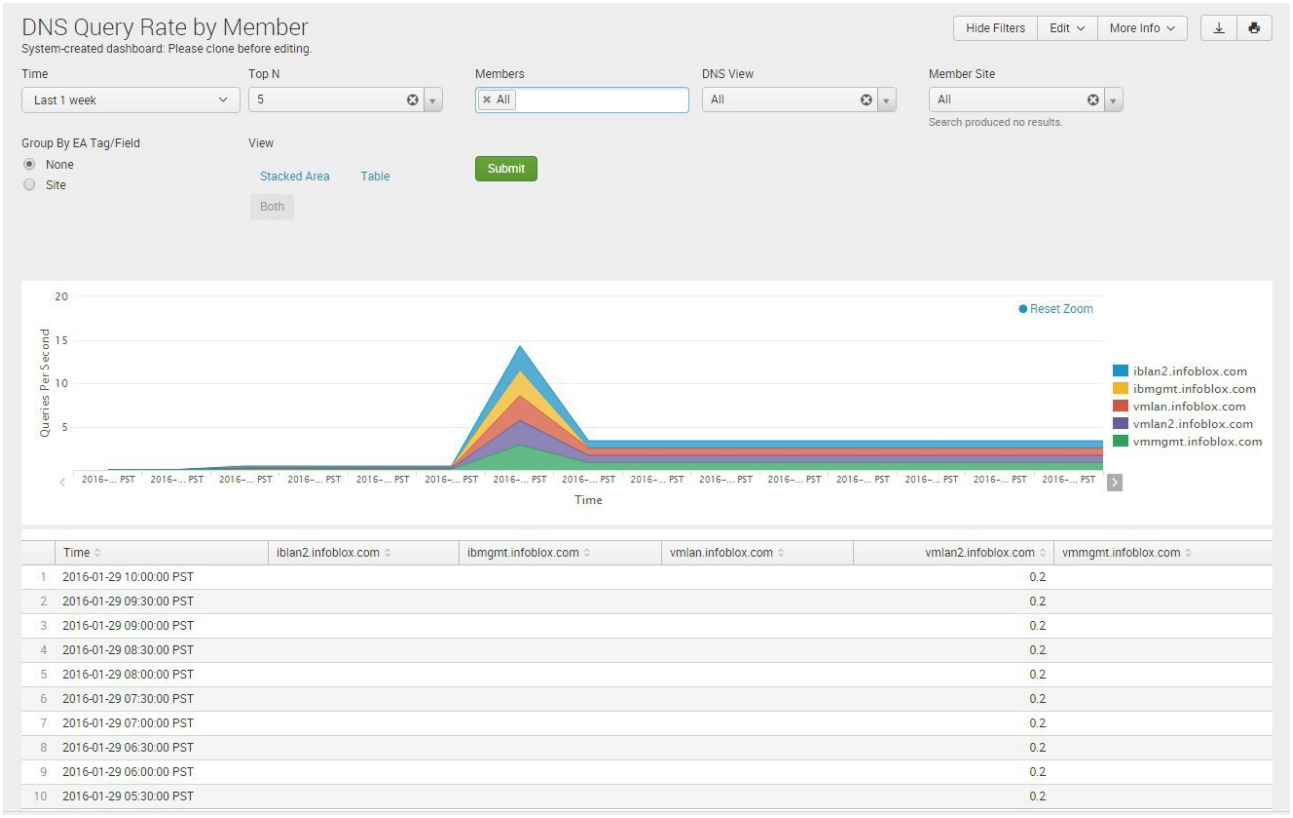


	Client	Queries
1	10.34.209.20 (94.3%)	1728260
2	10.34.209.3 (1.1%)	20562
3	10.34.209.5 (1.1%)	20293
4	10.34.209.6 (1.1%)	19361
5	10.34.209.17 (0.7%)	13127
6	10.34.209.12 (0.6%)	11753
7	10.34.209.14 (0.5%)	8421
8	10.34.209.11 (0.4%)	7370
9	10.34.209.16 (0.1%)	1908
10	10.34.209.18 (0.1%)	1907

5.8 DNS Query Rate By Member

Description	Shows trend of DNS QPS by member
Overview	Shows the queries per seconds and how much load is being generated and which devices are carrying the load. Helps plan better for capacity and reduce the risk of overloading DNS devices.
Data presented	• Member • QPS • Time

Sample report:

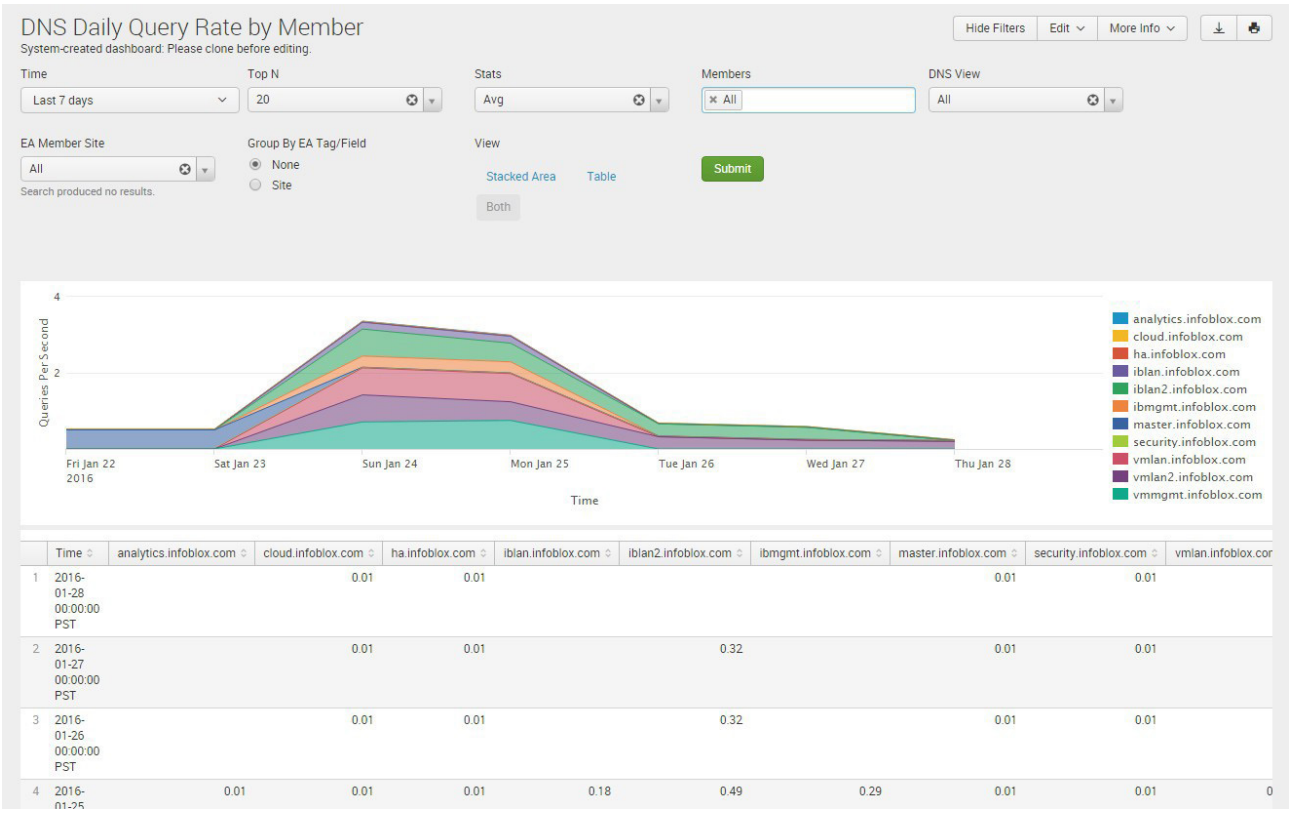


	Time	iblan2.infoblox.com	ibmgmt.infoblox.com	vmlan.infoblox.com	vmlan2.infoblox.com	vmmgmt.infoblox.com
1	2016-01-29 10:00:00 PST				0.2	
2	2016-01-29 09:30:00 PST				0.2	
3	2016-01-29 09:00:00 PST				0.2	
4	2016-01-29 08:30:00 PST				0.2	
5	2016-01-29 08:00:00 PST				0.2	
6	2016-01-29 07:30:00 PST				0.2	
7	2016-01-29 07:00:00 PST				0.2	
8	2016-01-29 06:30:00 PST				0.2	
9	2016-01-29 06:00:00 PST				0.2	
10	2016-01-29 05:30:00 PST				0.2	

5.9 DNS Daily Query Rate by Member

Description	Shows daily average or daily maximum query rate trend by member.
Overview	Shows the daily average or daily maximum query rate by server. It displays a single value per day per server. This report shows how much load is being generated and which devices are carrying the load. Helps plan better for capacity and reduce the risk of overloading DNS devices.
Data presented	• Member names • DNS Queries Per Second per member • Time

Sample report:

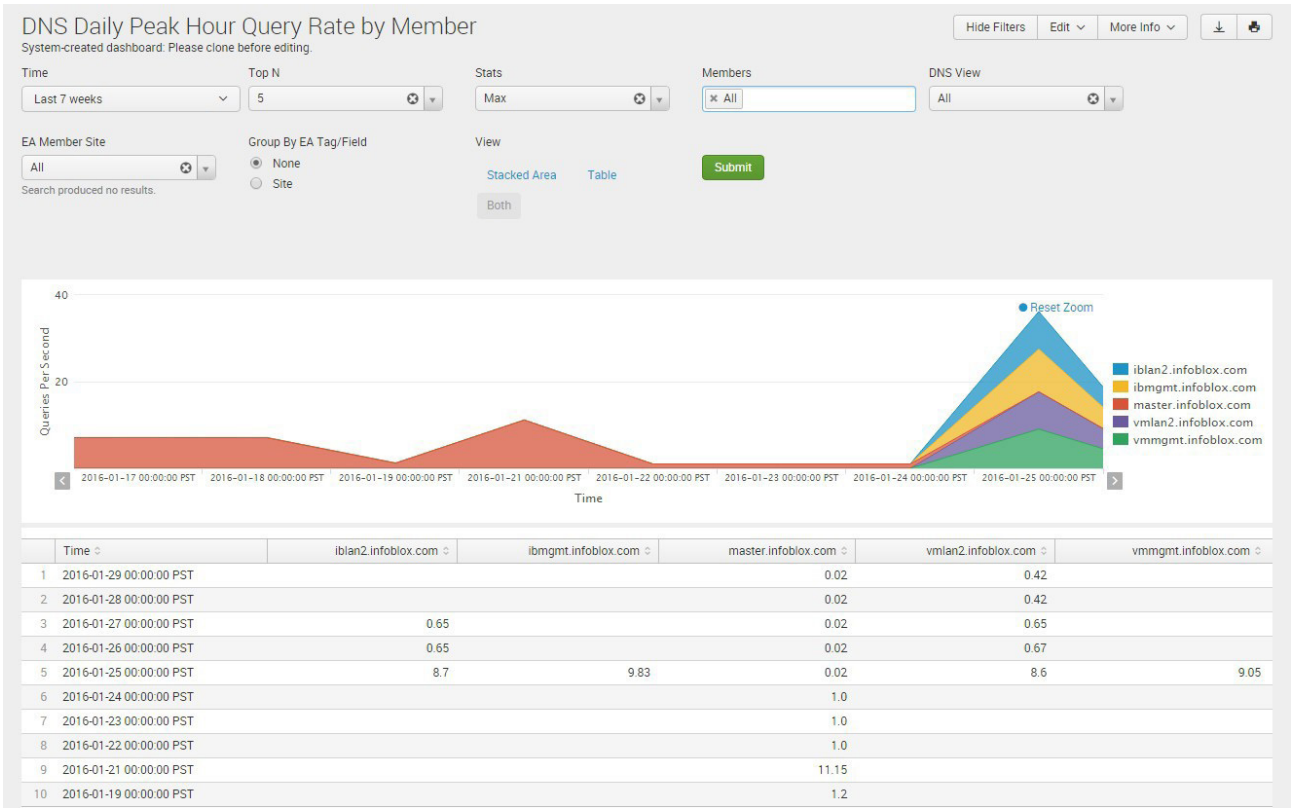


	Time	analytics.infoblox.com	cloud.infoblox.com	ha.infoblox.com	iblan.infoblox.com	iblan2.infoblox.com	ibmgmt.infoblox.com	master.infoblox.com	security.infoblox.com	vmlan.infoblox.com
1	2016-01-28 00:00:00 PST		0.01	0.01				0.01	0.01	
2	2016-01-27 00:00:00 PST		0.01	0.01		0.32		0.01	0.01	
3	2016-01-26 00:00:00 PST		0.01	0.01		0.32		0.01	0.01	
4	2016-01-25	0.01	0.01	0.01	0.18	0.49	0.29	0.01	0.01	0

5.10 DNS Daily Peak Hour Query Rate by Member

Description	Shows the maximum or average QPS for the peak hour of the day by member
Overview	Tracks the queries per seconds over a peak hour and how much load is being generated and which devices are carrying the load. The peak hour measurement helps plan better for the highest volume load capacity requirements by providing the max hourly query rate instead of averaging over an entire day. This view reduces the risk of overloading DNS devices when they are in the most demand.
Data presented	• Time • QPS • Member

Sample report:

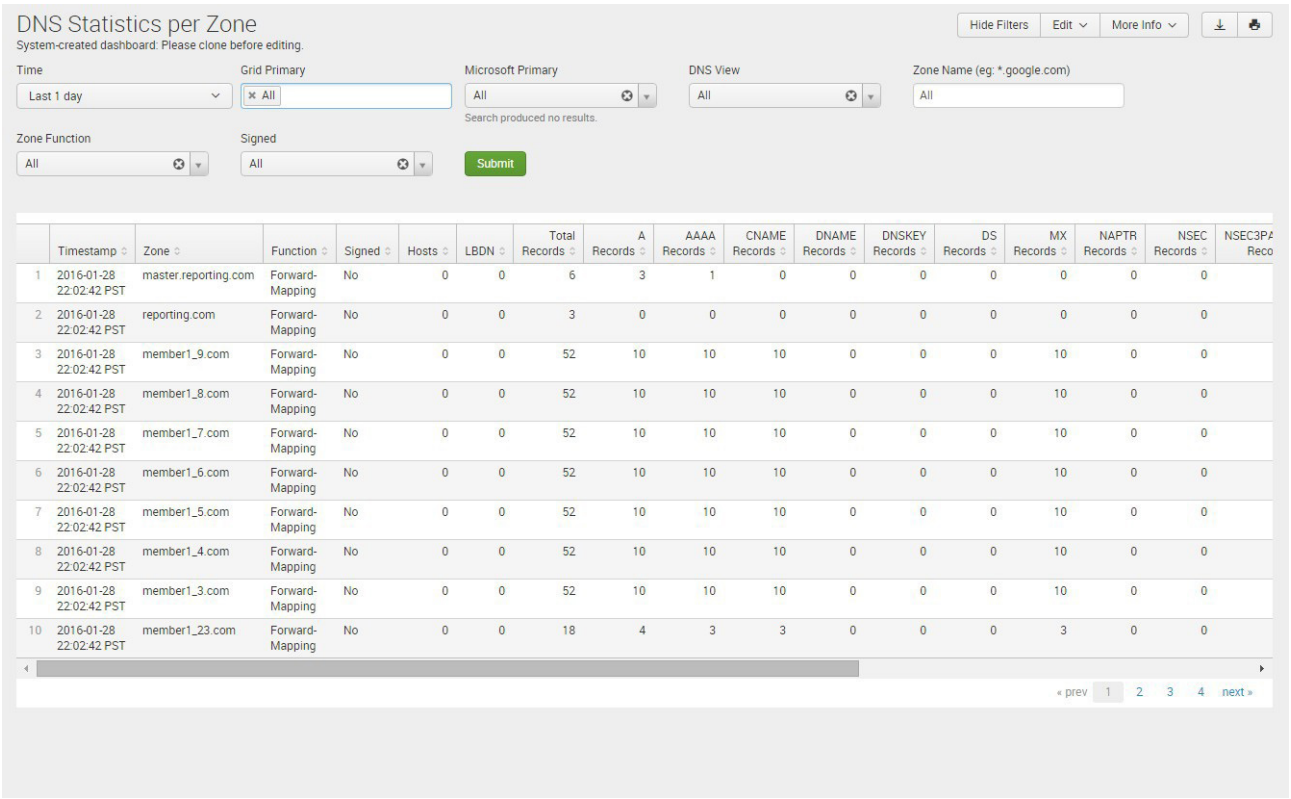


	Time	iblan2.infoblox.com	ibmgmt.infoblox.com	master.infoblox.com	vmlan2.infoblox.com	vmmgmt.infoblox.com
1	2016-01-29 00:00:00 PST			0.02	0.42	
2	2016-01-28 00:00:00 PST			0.02	0.42	
3	2016-01-27 00:00:00 PST	0.65		0.02	0.65	
4	2016-01-26 00:00:00 PST	0.65		0.02	0.67	
5	2016-01-25 00:00:00 PST	8.7	9.83	0.02	8.6	9.05
6	2016-01-24 00:00:00 PST			1.0		
7	2016-01-23 00:00:00 PST			1.0		
8	2016-01-22 00:00:00 PST			1.0		
9	2016-01-21 00:00:00 PST			11.15		
10	2016-01-19 00:00:00 PST			1.2		

5.11 DNS Statistics per Zone

Description	Tracks DNS statistics per zone
Overview	This report allows the user to quickly determine the number of resource records assigned to any zone by resource record type. The statistics provided by this report can be used for more effective planning.
Data presented	• Timestamp • Zone • Function (Forward-Mapping, IPv4 Reverse-Mapping, IPv6 Reverse-Mapping) • Signed • Hosts • LBDN • Total Records • Count of the following records: A Records, AAAA Records, CNAME Records, DNAME Records, DNSKEY Records, MX Records, NAPTR Records, NSEC Records, NSEC3PARAM Records, NSEC3 Records, NS Records, PTR Records, RRSIG Records, SOA Records, SRV Records, TXT Records and Other Records

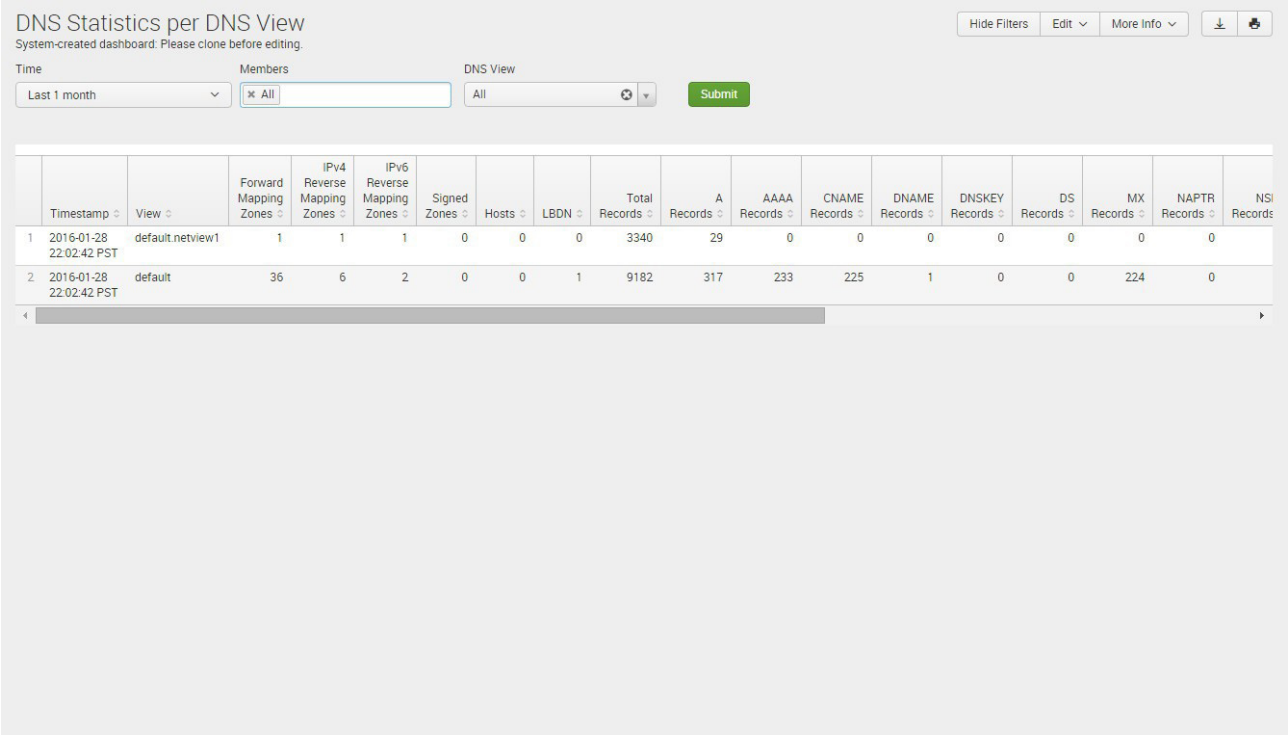
Sample report:



5.12 DNS Statistics per DNS View

Description	Tracks DNS statistics per DNS view
Overview	Since every DNS view can have multiple zones and each zone can have multiple records, this report highlights the statistics based on every DNS View or Member. This report allows you to identify how many Zones and DNS records a member or a DNS view is serving and use these statistics for more effective planning.
Data presented	• Timestamp • View • Forward-mapping zones • IPV4 Reverse Mapping • IPV6 Reverse Mapping • Signed Zones • Hosts • LBDN • Total records • Count of the following records: A Records, AAAA Records, CNAME Records, DNAME Records, DNSKEY Records, MX Records, NAPTR Records, NSEC Records, NSEC3PARAM Records, NSEC3 Records, NS Records, PTR Records, RRSIG Records, SOA Records, SRV Records, TXT Records and Other Records

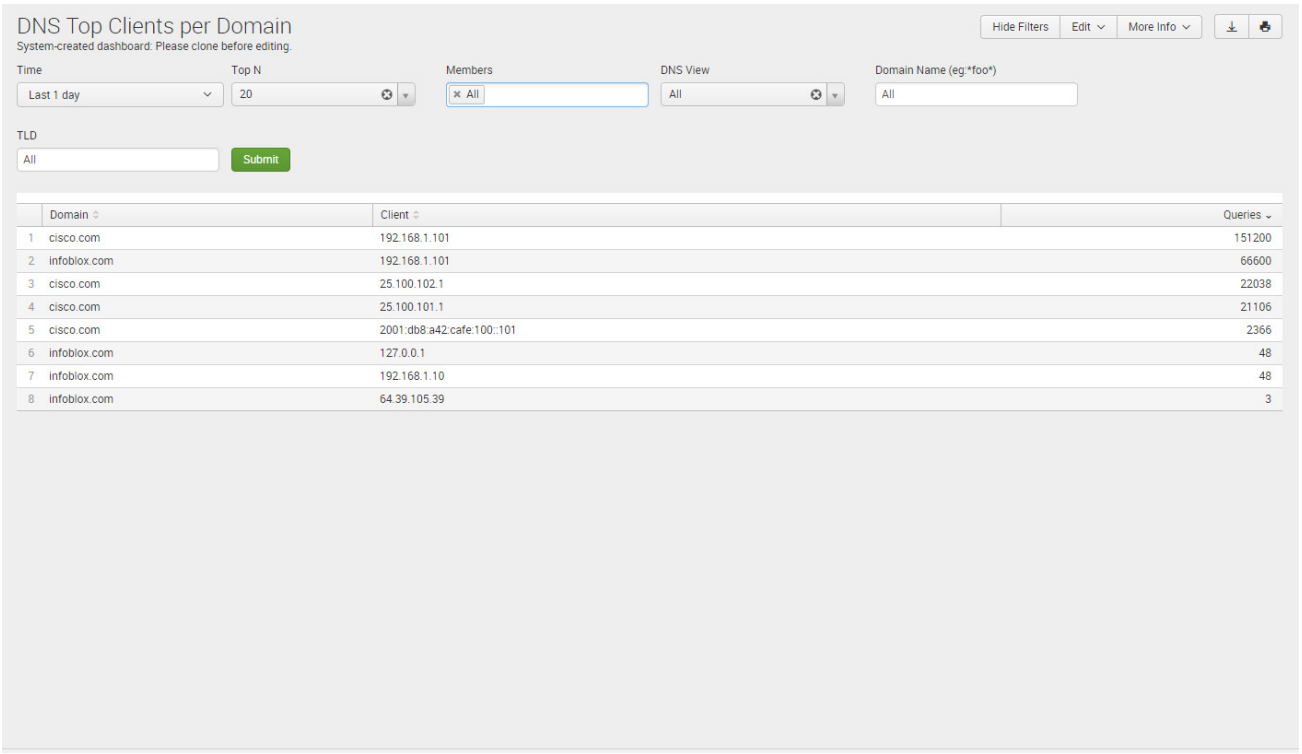
Sample report:



5.13 DNS Top Clients per Domain

Description	Lists the top N clients and number of queries for all or the specified DNS domains
Overview	Identify top users of specific applications, see clients querying a list of malicious domains and track clients to specific domains to improve performance and reduce risk.
Data presented	• Domain Names (Fully Qualified Domain Names) • Query Counts per DNS Domain Name • Client

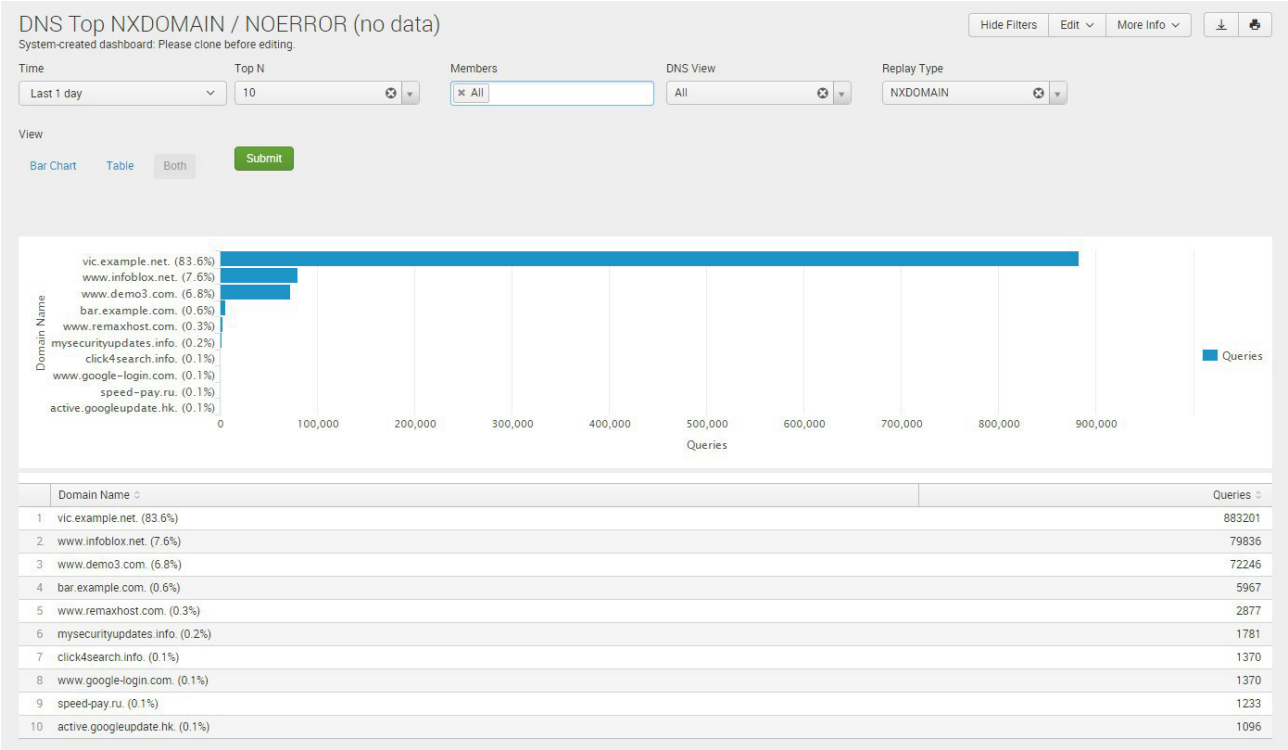
Sample report:



5.14 DNS Top NXDOMAIN – NOERROR (no data)

Description	Lists DNS queries that result in NXDOMAIN or NOERROR (no data) response
Overview	Identifies queries to servers that have been renamed or removed and finds mis-configurations by showing DNS queries that result in NXDOMAIN and NOERROR(no data) responses
Data presented	• Domain name • Number of queries

Sample report:

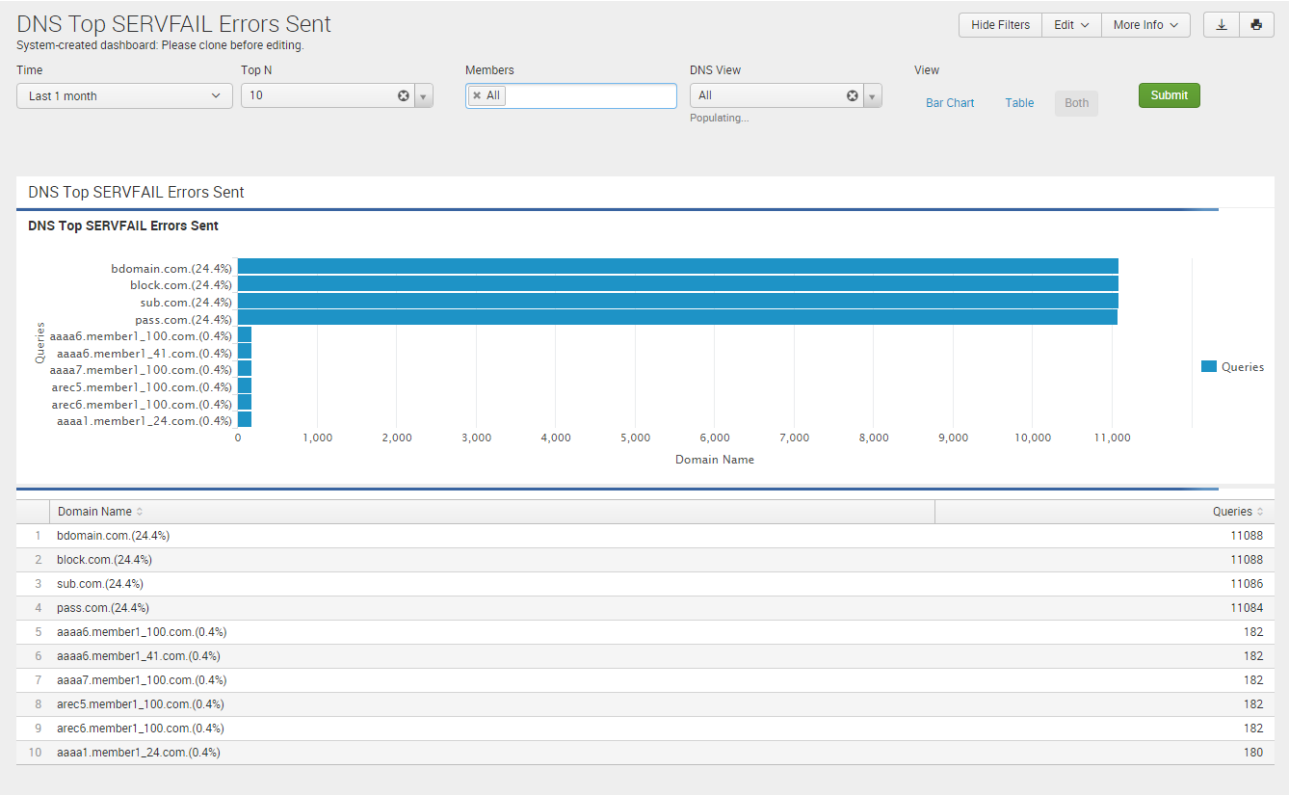


	Domain Name	Queries
1	vic.example.net. (83.6%)	883201
2	www.infoblox.net. (7.6%)	79836
3	www.demo3.com. (6.8%)	72246
4	bar.example.com. (0.6%)	5967
5	www.remaxhost.com. (0.3%)	2877
6	mysecurityupdates.info. (0.2%)	1781
7	click4search.info. (0.1%)	1370
8	www.google-login.com. (0.1%)	1370
9	speed-pay.ru. (0.1%)	1233
10	active.googleupdate.hk. (0.1%)	1096

5.15 DNS Top SERVFAIL Errors Sent/Received

Description	Shows queries that received or sent SERVFAIL responses
Overview	Allows users to see if issues reside within their DNS servers or upstream name servers by showing queries that receive/send SERVFAIL responses from upstream name serves.
Data presented	• Domain name • Number of queries (sent or received)

Sample report:

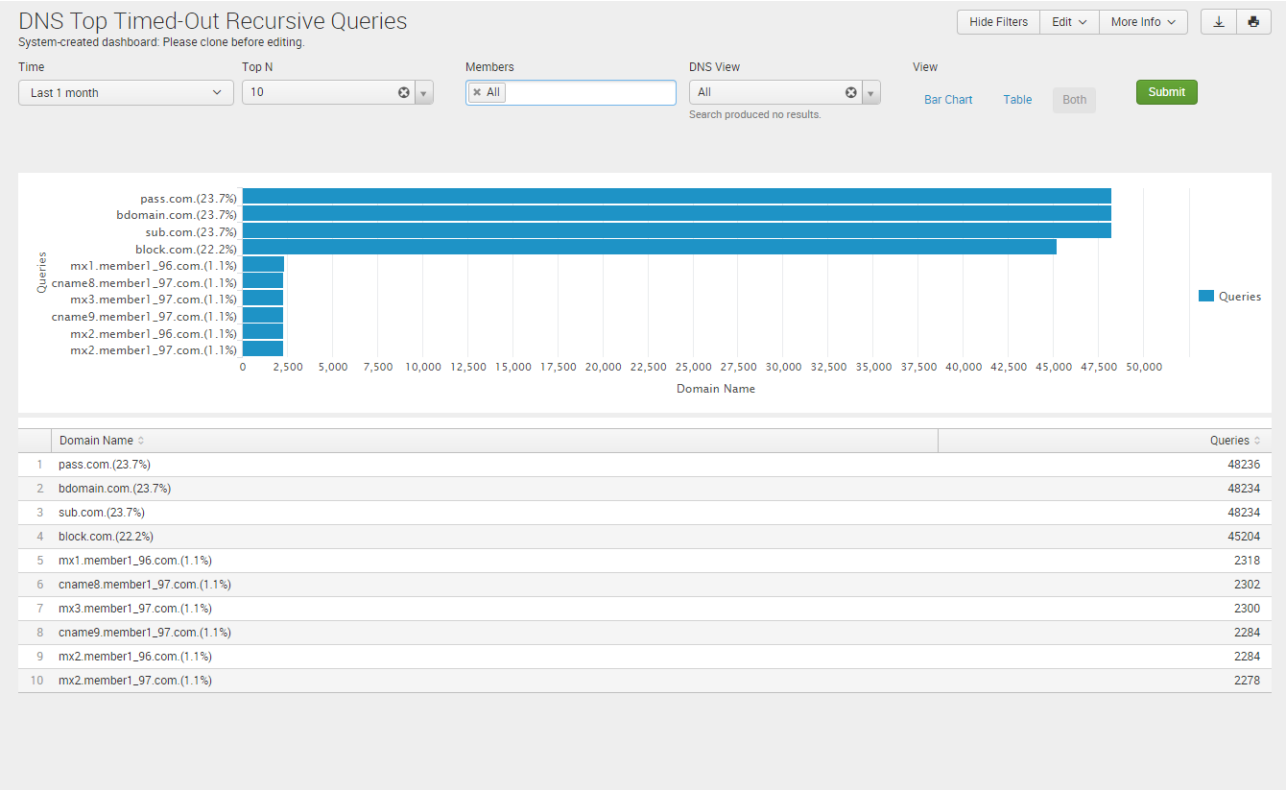


	Domain Name	Queries
1	bdomain.com.(24.4%)	11088
2	block.com.(24.4%)	11088
3	sub.com.(24.4%)	11086
4	pass.com.(24.4%)	11084
5	aaaa6.member1_100.com.(0.4%)	182
6	aaaa6.member1_41.com.(0.4%)	182
7	aaaa7.member1_100.com.(0.4%)	182
8	arec5.member1_100.com.(0.4%)	182
9	arec6.member1_100.com.(0.4%)	182
10	aaaa1.member1_24.com.(0.4%)	180

5.16 DNS Top Timed-Out Recursive Queries

Description	Lists DNS queries that time out
Overview	Reduces troubleshooting time by showing the top DNS queries that resulted in Infoblox name servers timing out when sending queries to upstream name servers.
Data presented	• Domain name • Number of queries

Sample report:

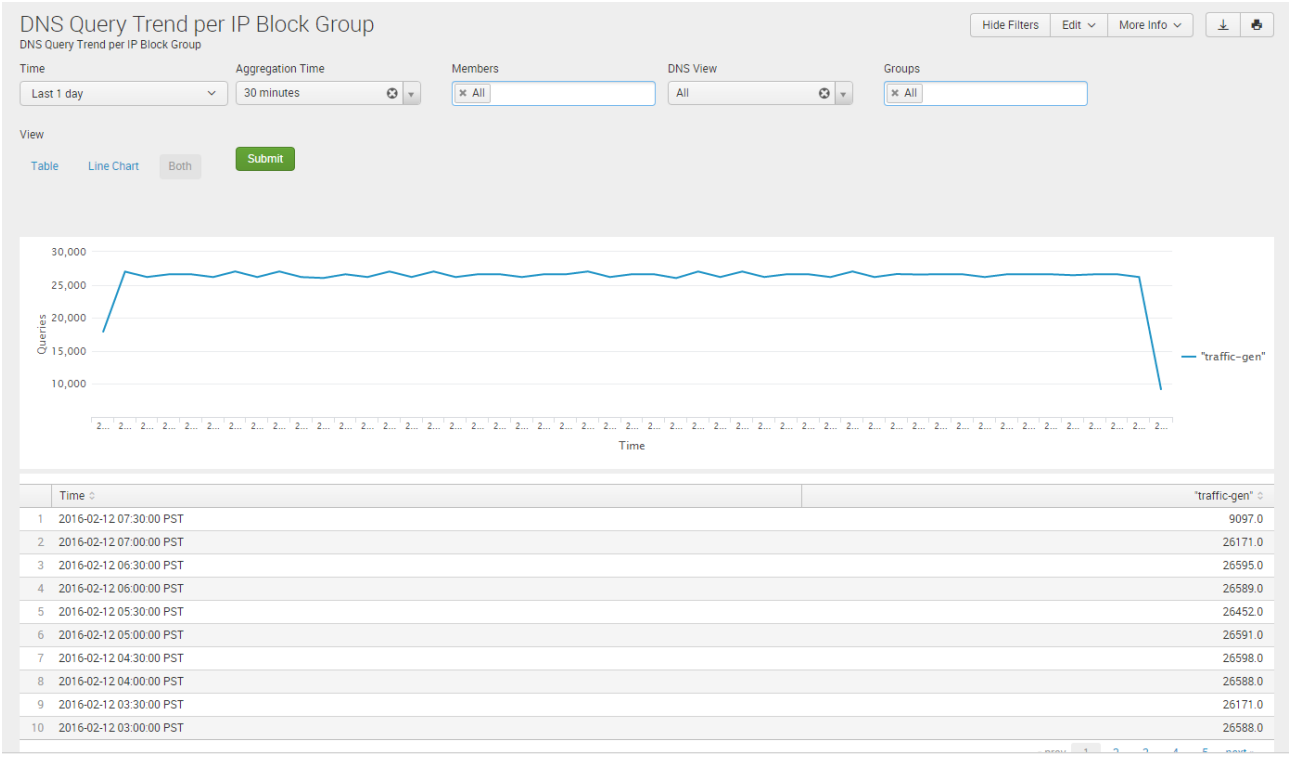


	Domain Name	Queries
1	pass.com.(23.7%)	48236
2	bdomain.com.(23.7%)	48234
3	sub.com.(23.7%)	48234
4	block.com.(22.2%)	45204
5	mx1.member1_96.com.(1.1%)	2318
6	cname8.member1_97.com.(1.1%)	2302
7	mx3.member1_97.com.(1.1%)	2300
8	cname9.member1_97.com.(1.1%)	2284
9	mx2.member1_96.com.(1.1%)	2284
10	mx2.member1_97.com.(1.1%)	2278

5.17 DNS Query Trend Per IP Block Group

Description	DNS Query Trend Per IP Block Group
Overview	Reduces time to identify issues by identifying the top DNS queries by selected IP Block Group. This allows for detailed filtering on a selected group or multiple groups. In addition, the enterprise or service provider can plan better for future growth requirements by tracking usage or top talkers across different regions.
Data presented	• Time • Group • Query count

Sample report:

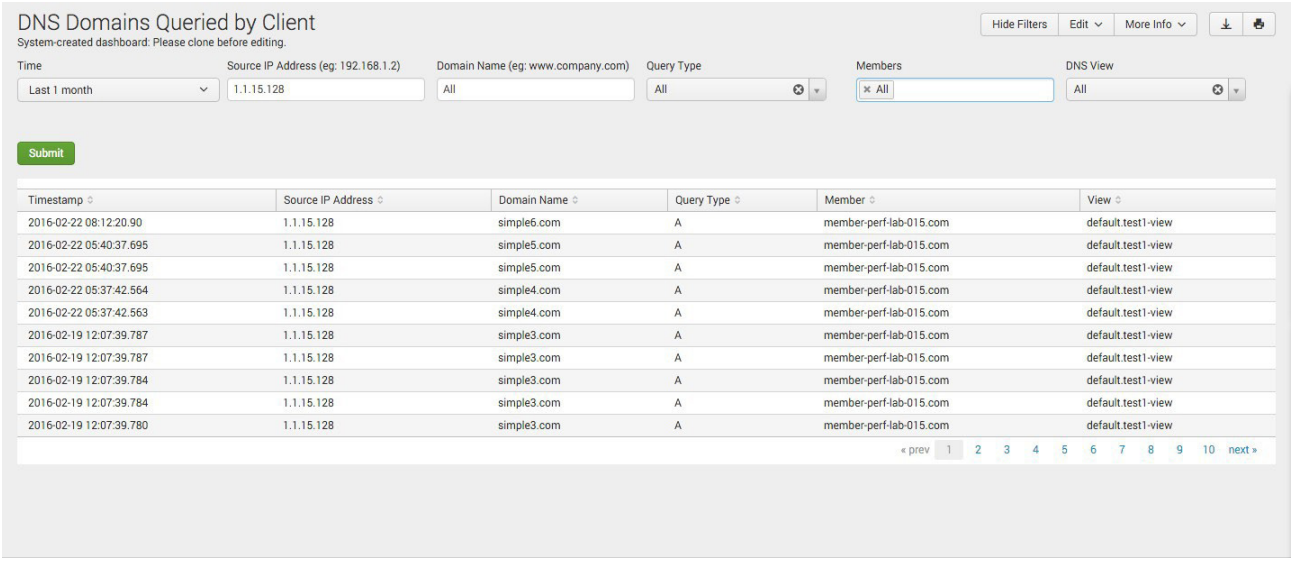


	Time	"traffic-gen"
1	2016-02-12 07:30:00 PST	9097.0
2	2016-02-12 07:00:00 PST	26171.0
3	2016-02-12 06:30:00 PST	26595.0
4	2016-02-12 06:00:00 PST	26589.0
5	2016-02-12 05:30:00 PST	26452.0
6	2016-02-12 05:00:00 PST	26591.0
7	2016-02-12 04:30:00 PST	26598.0
8	2016-02-12 04:00:00 PST	26588.0
9	2016-02-12 03:30:00 PST	26171.0
10	2016-02-12 03:00:00 PST	26588.0

5.18 DNS Domains Queried By Client*

Description	Lists the DNS domains being queried by the client
Overview	Displays the DNS domains that are being queried from both the internal and external sources.
Data presented	• Timestamp • Source IP address • Domain name • Query type • Member • View
*Please note the Infoblox Data Connector is required for this report.	

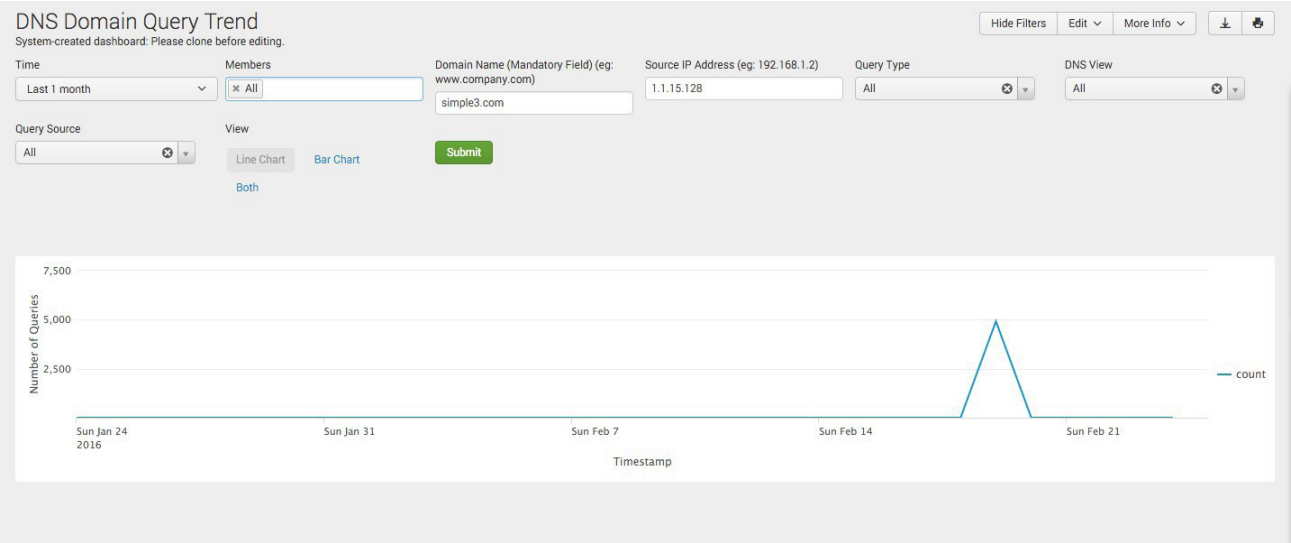
Sample report:



5.19 DNS Domain Query Trend*

Description	Lists the trend of DNS queries for specific domains
Overview	Displays the DNS query trends for queries generated from both the internal and external sources.
Data presented	• Query trend over time
*Please note the Infoblox Data Connector is required for this report.	

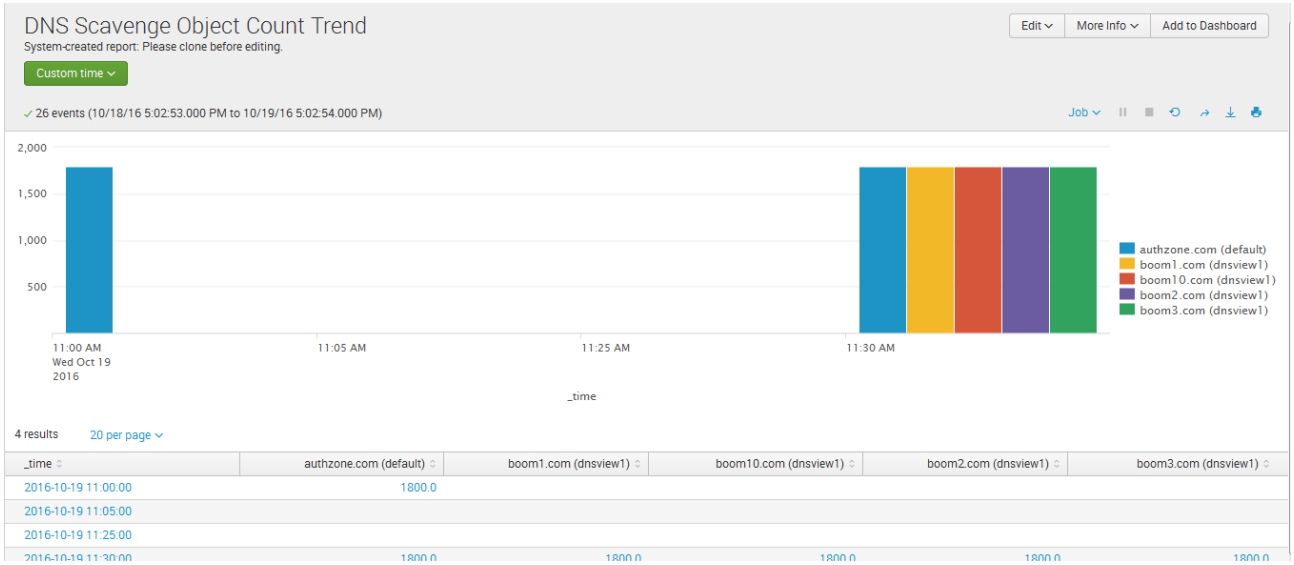
Sample report:



5.20 DNS Scavenged Object Count Trend

Description	Displays the number of removed stale DNS records per zone or DNS view over time
Overview	This report show the trend of scavenged DNS objects over time. This report is only populated if the scavenging feature is enabled, and there are records that meet the scavenging criteria.
Data presented	• Time • Count trend

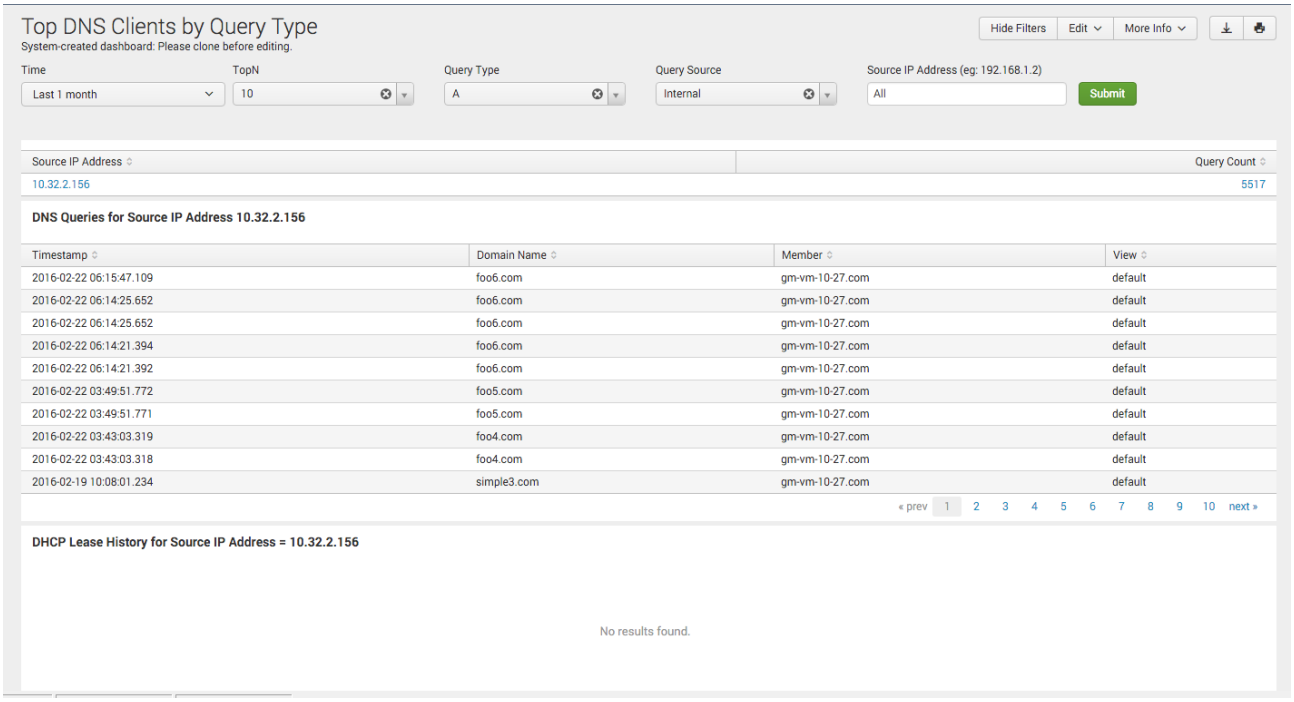
Sample report:



5.21 Top DNS Clients by Query Type*

Description	Displays the top DNS resource records that have been queried per client
Overview	This report is populated by the Data Connector. It enables administrators to search for granular queries and filter by type and source.
Data presented	• Timestamp • Domain Name • Member • View
*Please note the Infoblox Data Connector is required for this report.	

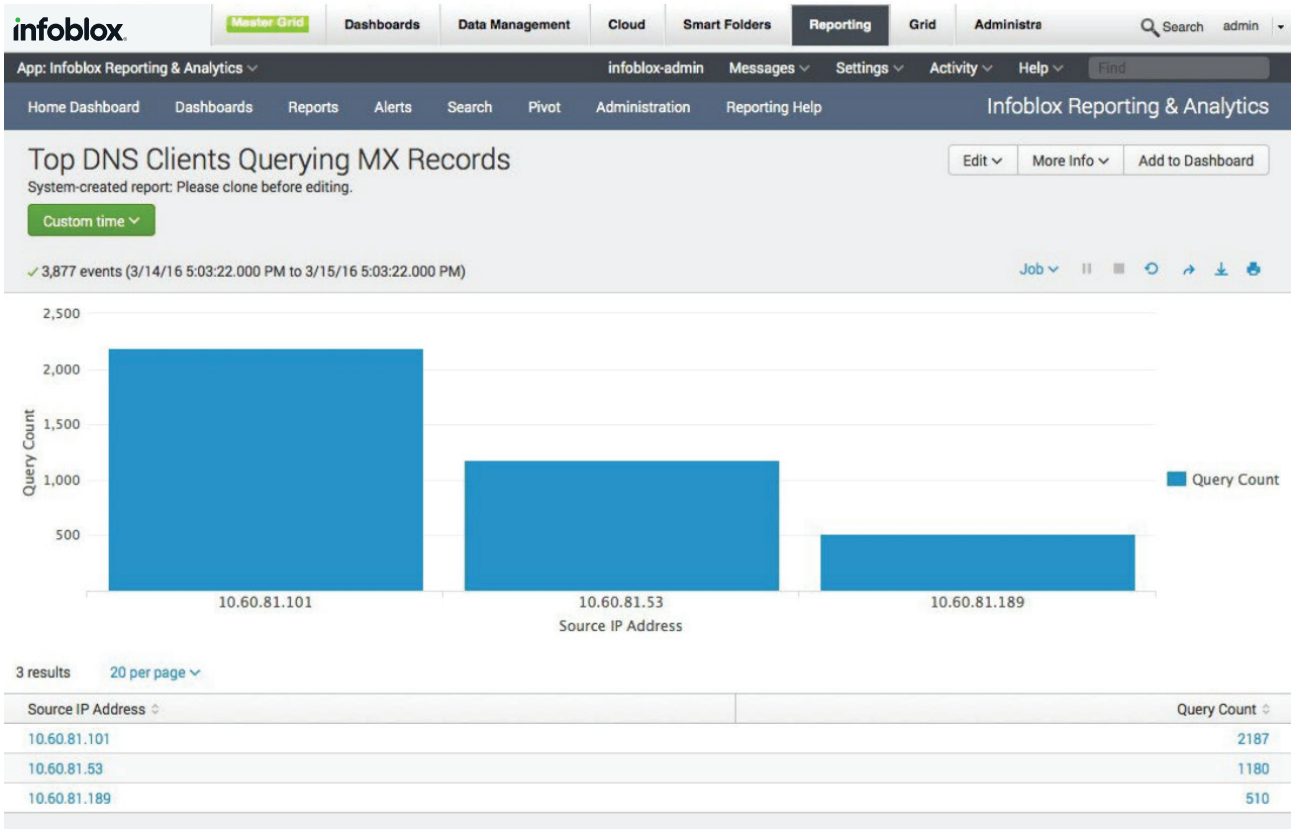
Sample report:



5.22 Top DNS Clients Querying MX Records*

Description	Displays the top MX records that have been queried per client
Overview	This report is populated by the Data Connector. It allows administrators to find unauthorized uses of external email, which could indicate personal email on corporate networks or the presence of spambots. It is expected that administrators know which IPs are valid email servers in order to identify invalid mail servers.
Data presented	• Source IP • Query Count
*Please note the Infoblox Data Connector is required for this report.	

Sample report:

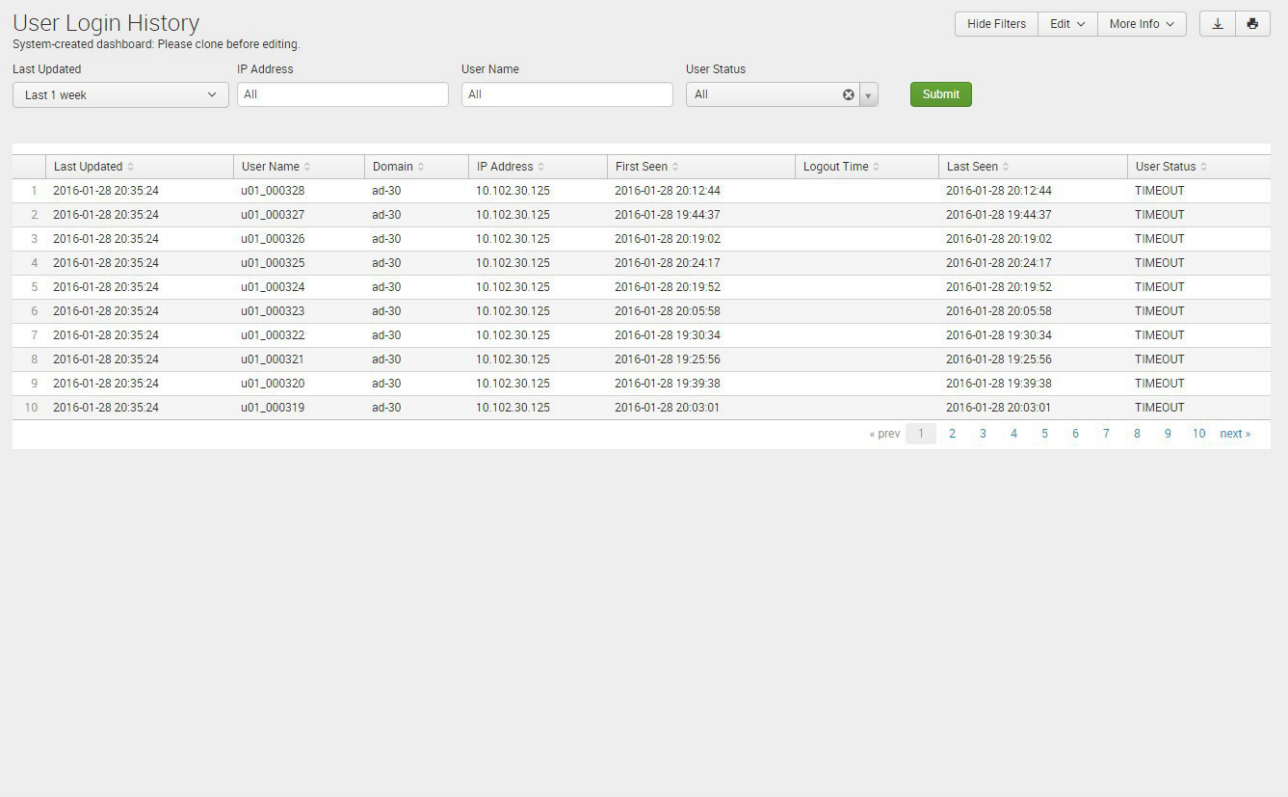


6 ECOSYSTEM DASHBOARDS

6.1 User Login History

Description	Tracks user logins over time.
Overview	Monitors and documents user logins over time with the ability to filter. Helps track who logged in when and where for troubleshooting and auditing.
Data presented	• User • Domain • IP Address • First Seen • Logout Time • Last Seen • User Status

Sample report:



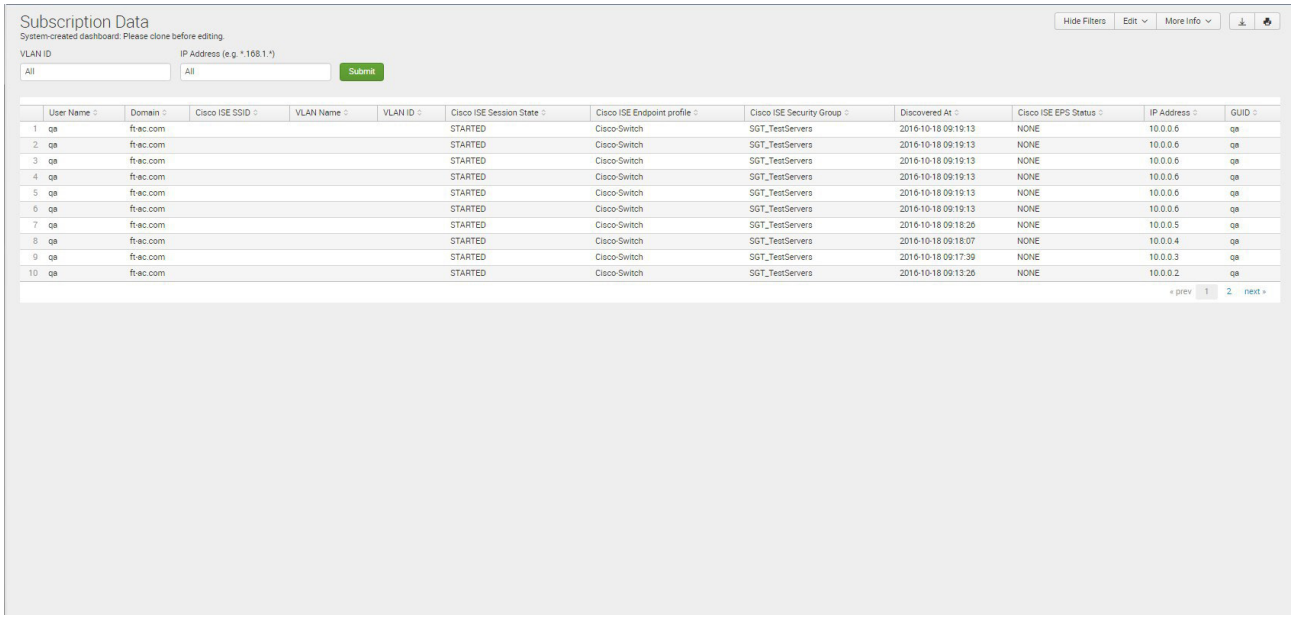
	Last Updated	User Name	Domain	IP Address	First Seen	Logout Time	Last Seen	User Status
1	2016-01-28 20:35:24	u01_000328	ad-30	10.102.30.125	2016-01-28 20:12:44		2016-01-28 20:12:44	TIMEOUT
2	2016-01-28 20:35:24	u01_000327	ad-30	10.102.30.125	2016-01-28 19:44:37		2016-01-28 19:44:37	TIMEOUT
3	2016-01-28 20:35:24	u01_000326	ad-30	10.102.30.125	2016-01-28 20:19:02		2016-01-28 20:19:02	TIMEOUT
4	2016-01-28 20:35:24	u01_000325	ad-30	10.102.30.125	2016-01-28 20:24:17		2016-01-28 20:24:17	TIMEOUT
5	2016-01-28 20:35:24	u01_000324	ad-30	10.102.30.125	2016-01-28 20:19:52		2016-01-28 20:19:52	TIMEOUT
6	2016-01-28 20:35:24	u01_000323	ad-30	10.102.30.125	2016-01-28 20:05:58		2016-01-28 20:05:58	TIMEOUT
7	2016-01-28 20:35:24	u01_000322	ad-30	10.102.30.125	2016-01-28 19:30:34		2016-01-28 19:30:34	TIMEOUT
8	2016-01-28 20:35:24	u01_000321	ad-30	10.102.30.125	2016-01-28 19:25:56		2016-01-28 19:25:56	TIMEOUT
9	2016-01-28 20:35:24	u01_000320	ad-30	10.102.30.125	2016-01-28 19:39:38		2016-01-28 19:39:38	TIMEOUT
10	2016-01-28 20:35:24	u01_000319	ad-30	10.102.30.125	2016-01-28 20:03:01		2016-01-28 20:03:01	TIMEOUT

« prev 1 2 3 4 5 6 7 8 9 10 next »

6.2 Subscription Data

Description	Tracks the user and device identity captured by the Cisco ISE for the subscribed member.
Overview	Displays user name, domain name, VLAN ID, Device operating system, and last discovered timestamp.
Data presented	• User name • Domain • SSID • VLAN Name • VLAN ID • Device OS • Session State • Security Group • Discovered At • Quarantined Status • IP Address • Grid ID

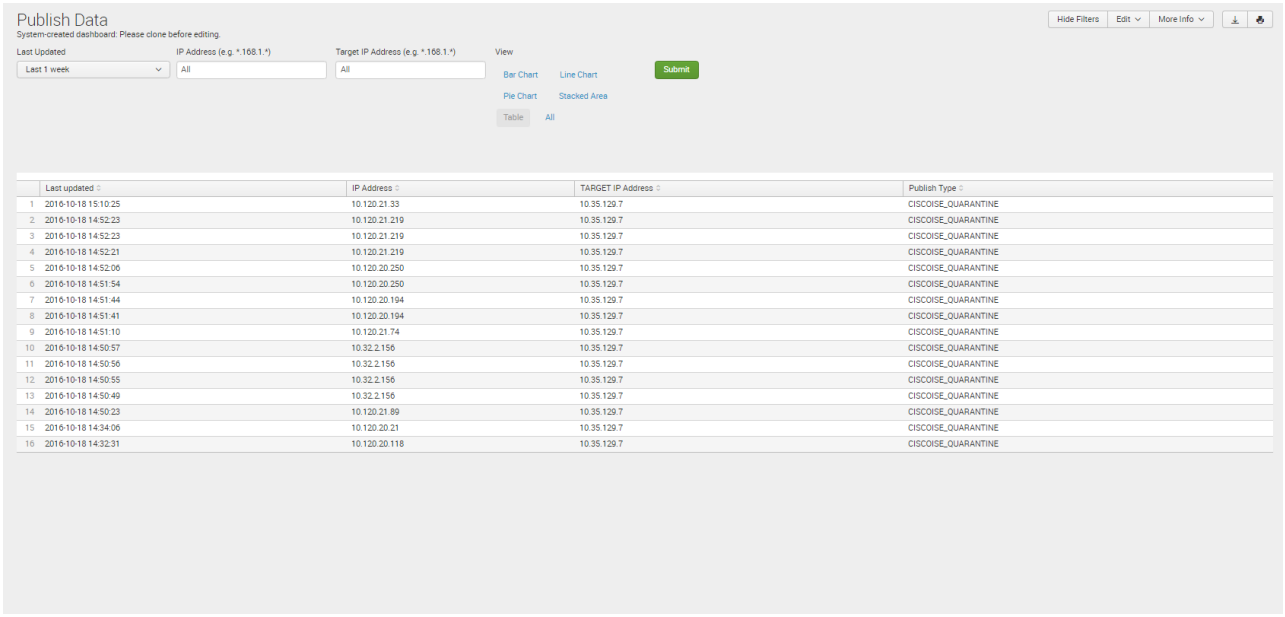
Sample report:



6.3 Publish Data

Description	Highlights the information and data shared with the Cisco ISE ecosystem
Overview	Displays the RPZ, Security ADP, IPAM and DHCP lease information that is shared with the Cisco IS
Data presented	• Last Updated • IP Address • Target Address • Publish Type • Contents

Sample report:



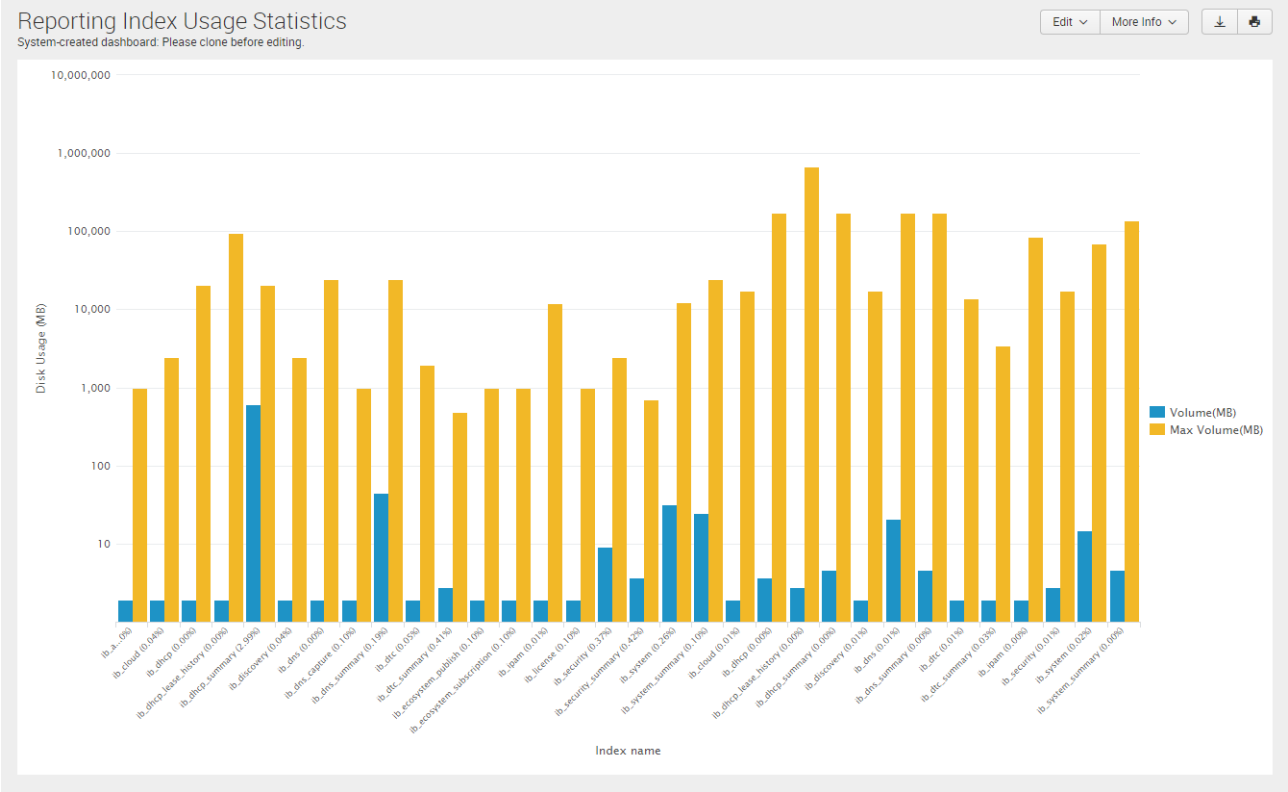
	Last updated	IP Address	TARGET IP Address	Publish Type
1	2016-10-18 15:10:25	10.120.21.33	10.35.129.7	CISCOISE_QUARANTINE
2	2016-10-18 14:52:23	10.120.21.219	10.35.129.7	CISCOISE_QUARANTINE
3	2016-10-18 14:52:23	10.120.21.219	10.35.129.7	CISCOISE_QUARANTINE
4	2016-10-18 14:52:21	10.120.21.219	10.35.129.7	CISCOISE_QUARANTINE
5	2016-10-18 14:52:06	10.120.20.250	10.35.129.7	CISCOISE_QUARANTINE
6	2016-10-18 14:51:54	10.120.20.250	10.35.129.7	CISCOISE_QUARANTINE
7	2016-10-18 14:51:44	10.120.20.194	10.35.129.7	CISCOISE_QUARANTINE
8	2016-10-18 14:51:41	10.120.20.194	10.35.129.7	CISCOISE_QUARANTINE
9	2016-10-18 14:51:10	10.120.21.74	10.35.129.7	CISCOISE_QUARANTINE
10	2016-10-18 14:50:57	10.32.2.156	10.35.129.7	CISCOISE_QUARANTINE
11	2016-10-18 14:50:56	10.32.2.156	10.35.129.7	CISCOISE_QUARANTINE
12	2016-10-18 14:50:55	10.32.2.156	10.35.129.7	CISCOISE_QUARANTINE
13	2016-10-18 14:50:49	10.32.2.156	10.35.129.7	CISCOISE_QUARANTINE
14	2016-10-18 14:50:23	10.120.21.89	10.35.129.7	CISCOISE_QUARANTINE
15	2016-10-18 14:34:06	10.120.20.21	10.35.129.7	CISCOISE_QUARANTINE
16	2016-10-18 14:32:31	10.120.20.118	10.35.129.7	CISCOISE_QUARANTINE

7 INTERNAL DASHBOARDS

7.1 Reporting Index Usage Statistics

Description	Tracks the index usage statistics for different reporting types.
Overview	Shows the maximum volume available and the current used volume for the different reporting types. Helps fine tune the configurable parameters for maximizing reporting visibility.
Data presented	• Index Name • Disk Usage

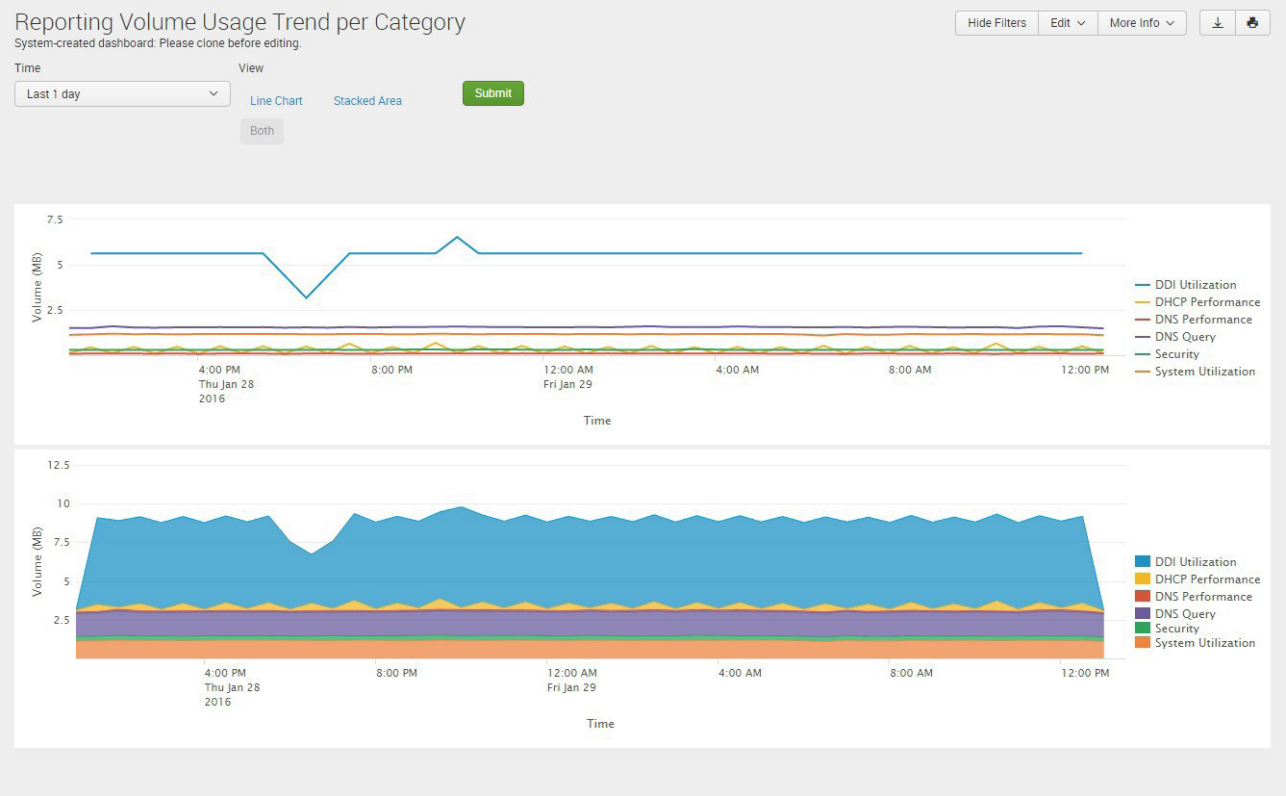
Sample report:



7.2 Reporting Volume Usage Trend Per Category

Description	Monitors the volume of reporting traffic by category over time.
Overview	Highlights the volume of reporting traffic by individual category over time. Helps identify if particular categories are using an abnormal amount of reporting usage which helps troubleshoot and/or fine tune the configurable parameters.
Data presented	• Volume (MB) • Time

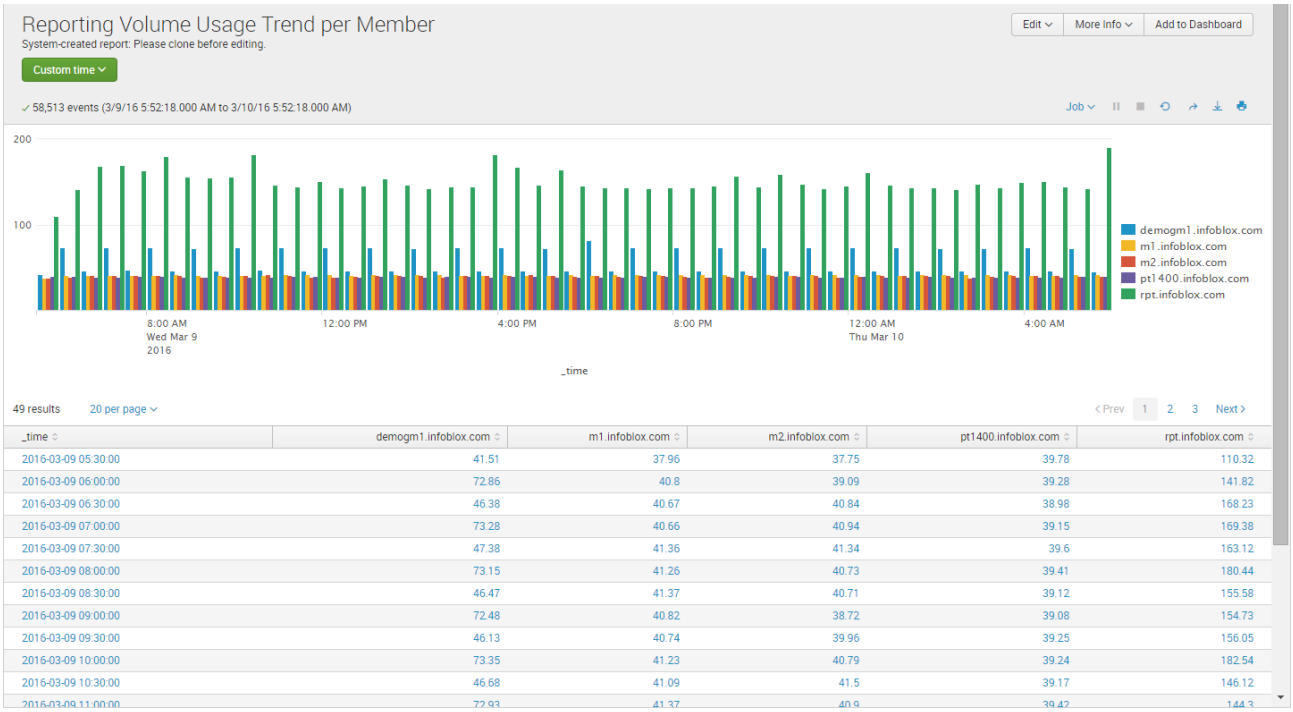
Sample report:



7.3 Reporting Volume Usage Trend Per Member

Description	Tracks the volume of reporting traffic by member over time.
Overview	Highlights the volume of reporting traffic by individual member with trending over time. Helps identify if a particular member is using an abnormal amount of reporting usage which helps troubleshoot.
Data presented	• Volume (MB) • Member • Time

Sample report:

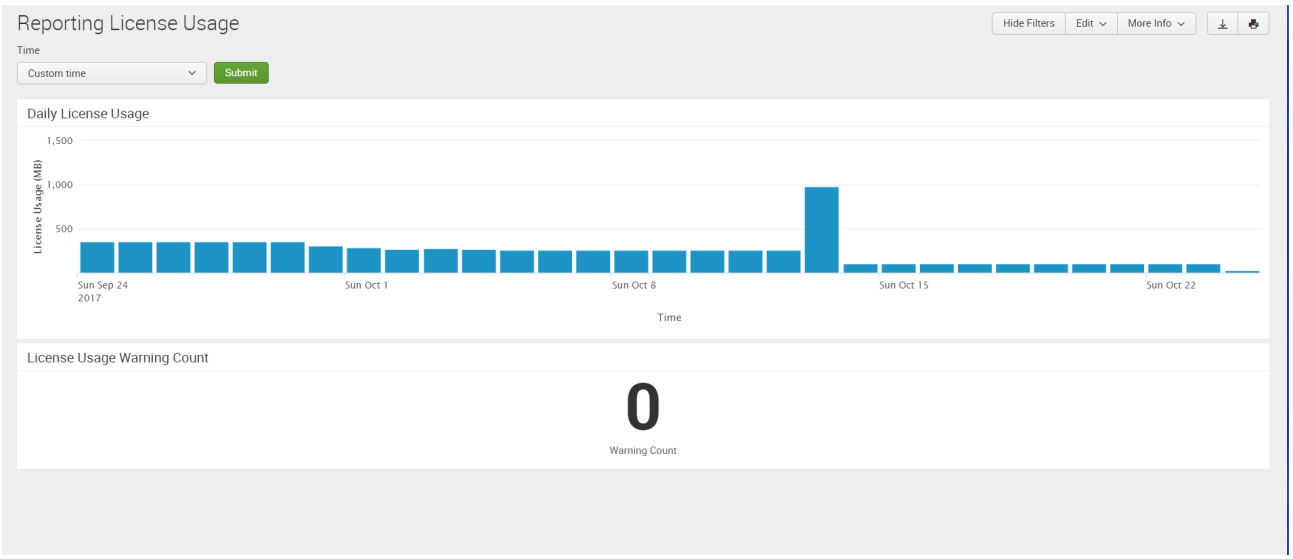


_time	demogm1.infoblox.com	m1.infoblox.com	m2.infoblox.com	pt1400.infoblox.com	rpt.infoblox.com
2016-03-09 05:30:00	41.51	37.96	37.75	39.78	110.32
2016-03-09 06:00:00	72.86	40.8	39.09	39.28	141.82
2016-03-09 06:30:00	46.38	40.67	40.84	38.98	168.23
2016-03-09 07:00:00	73.28	40.66	40.94	39.15	169.38
2016-03-09 07:30:00	47.38	41.36	41.34	39.6	163.12
2016-03-09 08:00:00	73.15	41.26	40.73	39.41	180.44
2016-03-09 08:30:00	46.47	41.37	40.71	39.12	155.58
2016-03-09 09:00:00	72.48	40.82	38.72	39.08	154.73
2016-03-09 09:30:00	46.13	40.74	39.96	39.25	156.05
2016-03-09 10:00:00	73.35	41.23	40.79	39.24	182.54
2016-03-09 10:30:00	46.68	41.09	41.5	39.17	146.12
2016-03-09 11:00:00	72.93	41.37	40.9	39.42	144.3

7.4 Reporting License Usage

Description	Tracks the amount of indexing used by day.
Overview	Highlights the total usage of indexing by day for Reporting and Analytics. This report is used to identify if the data collected is exceeding the indexing capacity and if additional capacity is needed for today and future growth.
Data presented	• Licensing usage (MB) • Date • Time

Sample report:

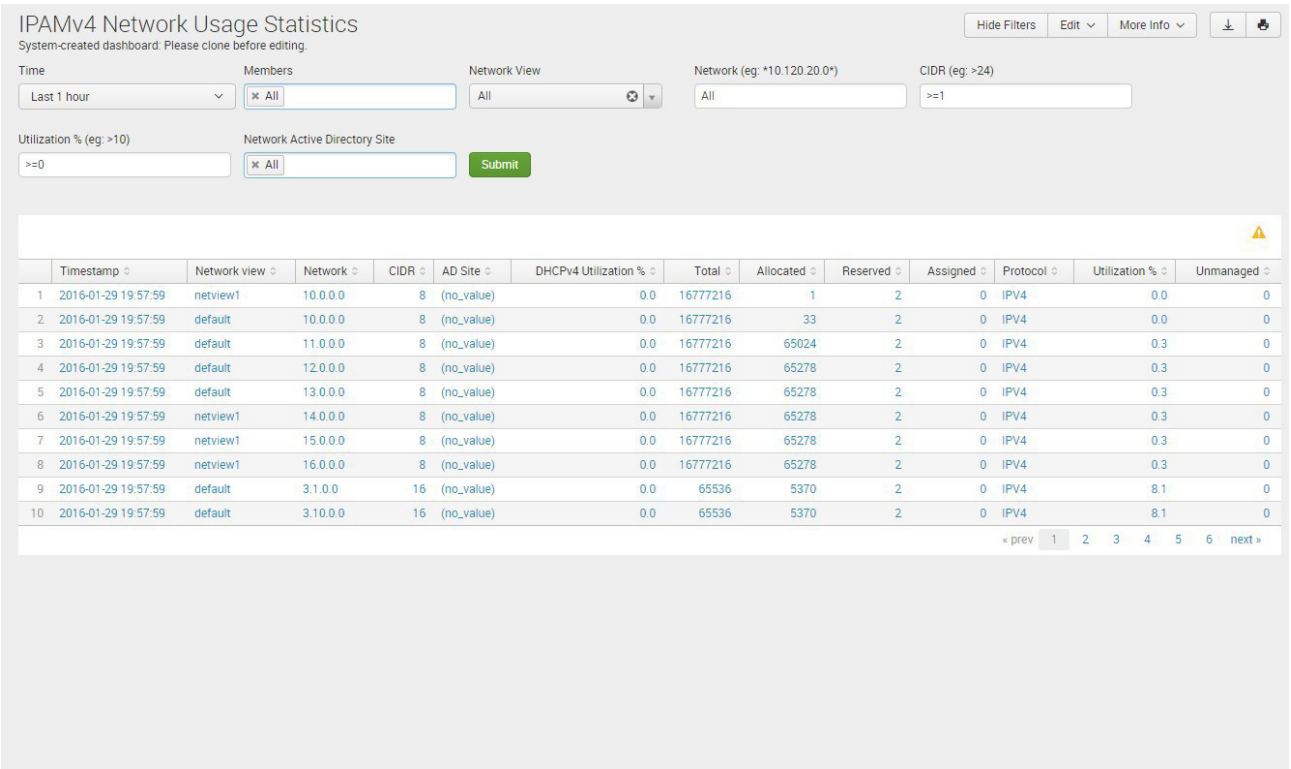


8 IP ADDRESS MANAGERMENT DASHBOARDS

8.1 IPAM v4 Network Usage Statistics

Description	Tracks usage statistics for IPv4 networks
Overview	Provides detailed views of usage based on individual networks/subnets. Helps administrators plan for network/subnet capacity and track usage over time.
Data presented	• Timestamp • Network view • Network • CIDR • AD Site • DHCPv4 utilization % • Total • Allocated • Reserved • Assigned • Protocol • Utilization % • Unmanaged

Sample report:

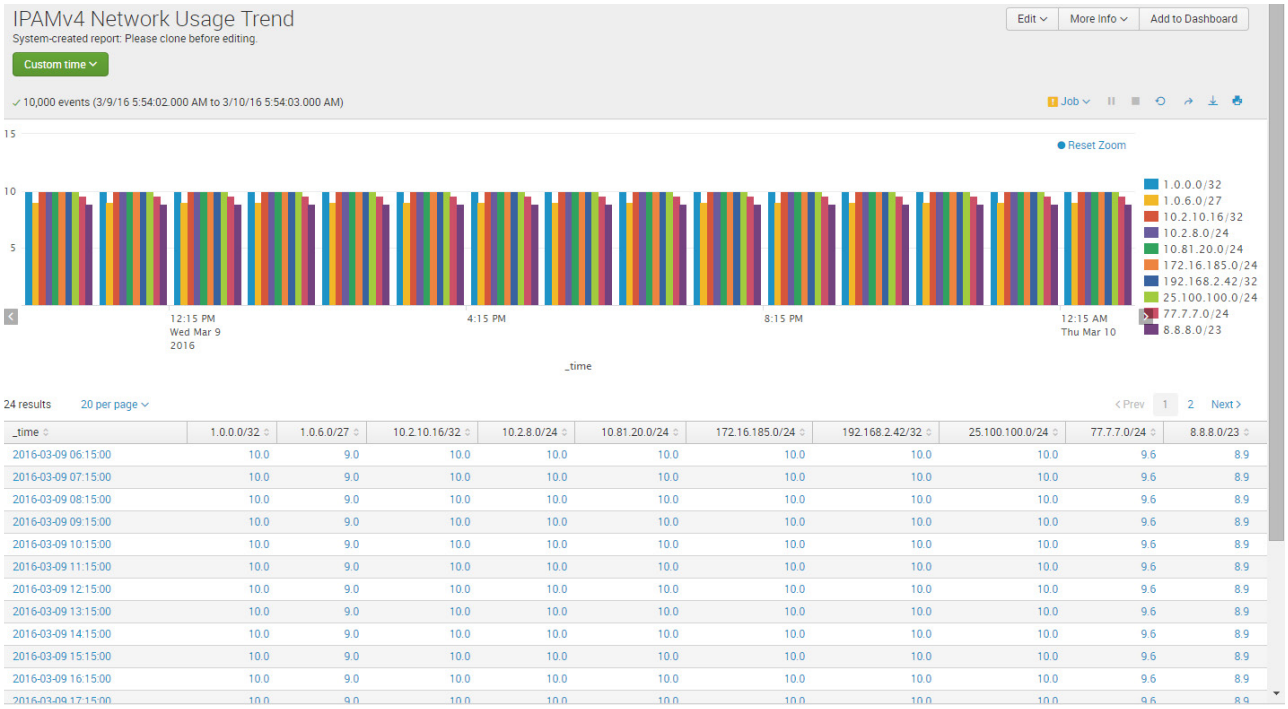


	Timestamp	Network view	Network	CIDR	AD Site	DHCPv4 Utilization %	Total	Allocated	Reserved	Assigned	Protocol	Utilization %	Unmanaged
1	2016-01-29 19:57:59	netview1	10.0.0.0	8	(no_value)	0.0	16777216	1	2	0	IPV4	0.0	0
2	2016-01-29 19:57:59	default	10.0.0.0	8	(no_value)	0.0	16777216	33	2	0	IPV4	0.0	0
3	2016-01-29 19:57:59	default	11.0.0.0	8	(no_value)	0.0	16777216	65024	2	0	IPV4	0.3	0
4	2016-01-29 19:57:59	default	12.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	0
5	2016-01-29 19:57:59	default	13.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	0
6	2016-01-29 19:57:59	netview1	14.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	0
7	2016-01-29 19:57:59	netview1	15.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	0
8	2016-01-29 19:57:59	netview1	16.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	0
9	2016-01-29 19:57:59	default	3.1.0.0	16	(no_value)	0.0	65536	5370	2	0	IPV4	8.1	0
10	2016-01-29 19:57:59	default	3.10.0.0	16	(no_value)	0.0	65536	5370	2	0	IPV4	8.1	0

8.2 IPAM v4 Network Usage Trend

Description	Tracks usage trend for IPv4 networks
Overview	Provides detailed views of usage trends over time based on individual networks/ subnets. Helps administrators plan for network/subnet capacity and identify trends over time.
Data presented	• Time • Usage %

Sample report:



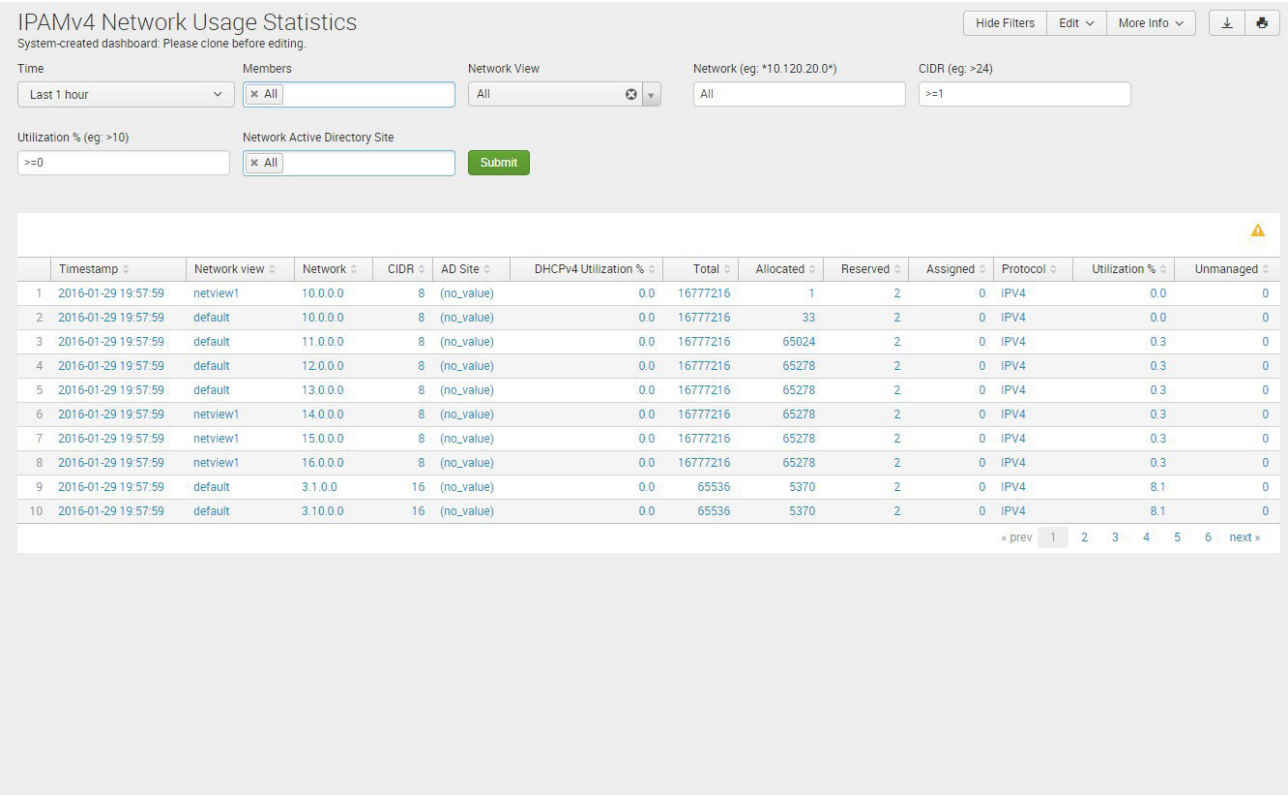
24 results 20 per page Prev 1 2 Next

_time	1.0.0.0/32	1.0.6.0/27	10.2.10.16/32	10.2.8.0/24	10.81.20.0/24	172.16.185.0/24	192.168.2.42/32	25.100.100.0/24	77.7.7.0/24	8.8.8.0/23
2016-03-09 06:15:00	10.0	9.0	10.0	10.0	10.0	10.0	10.0	10.0	9.6	8.9
2016-03-09 07:15:00	10.0	9.0	10.0	10.0	10.0	10.0	10.0	10.0	9.6	8.9
2016-03-09 08:15:00	10.0	9.0	10.0	10.0	10.0	10.0	10.0	10.0	9.6	8.9
2016-03-09 09:15:00	10.0	9.0	10.0	10.0	10.0	10.0	10.0	10.0	9.6	8.9
2016-03-09 10:15:00	10.0	9.0	10.0	10.0	10.0	10.0	10.0	10.0	9.6	8.9
2016-03-09 11:15:00	10.0	9.0	10.0	10.0	10.0	10.0	10.0	10.0	9.6	8.9
2016-03-09 12:15:00	10.0	9.0	10.0	10.0	10.0	10.0	10.0	10.0	9.6	8.9
2016-03-09 13:15:00	10.0	9.0	10.0	10.0	10.0	10.0	10.0	10.0	9.6	8.9
2016-03-09 14:15:00	10.0	9.0	10.0	10.0	10.0	10.0	10.0	10.0	9.6	8.9
2016-03-09 15:15:00	10.0	9.0	10.0	10.0	10.0	10.0	10.0	10.0	9.6	8.9
2016-03-09 16:15:00	10.0	9.0	10.0	10.0	10.0	10.0	10.0	10.0	9.6	8.9
2016-03-09 17:15:00	10.0	9.0	10.0	10.0	10.0	10.0	10.0	10.0	9.6	8.9

8.3 IPAM v4 Top Utilized Networks

Description	Provides statistics on top utilized networks
Overview	Provides view into the top utilized subnets measured by utilization metrics. Helps slice and dice the data into usable formats for improved planning.
Data presented	• Timestamp • Network view • Network • CIDR size • AD Site • Utilization % • Total • Assigned • Reserved • Unmanaged

Sample report:



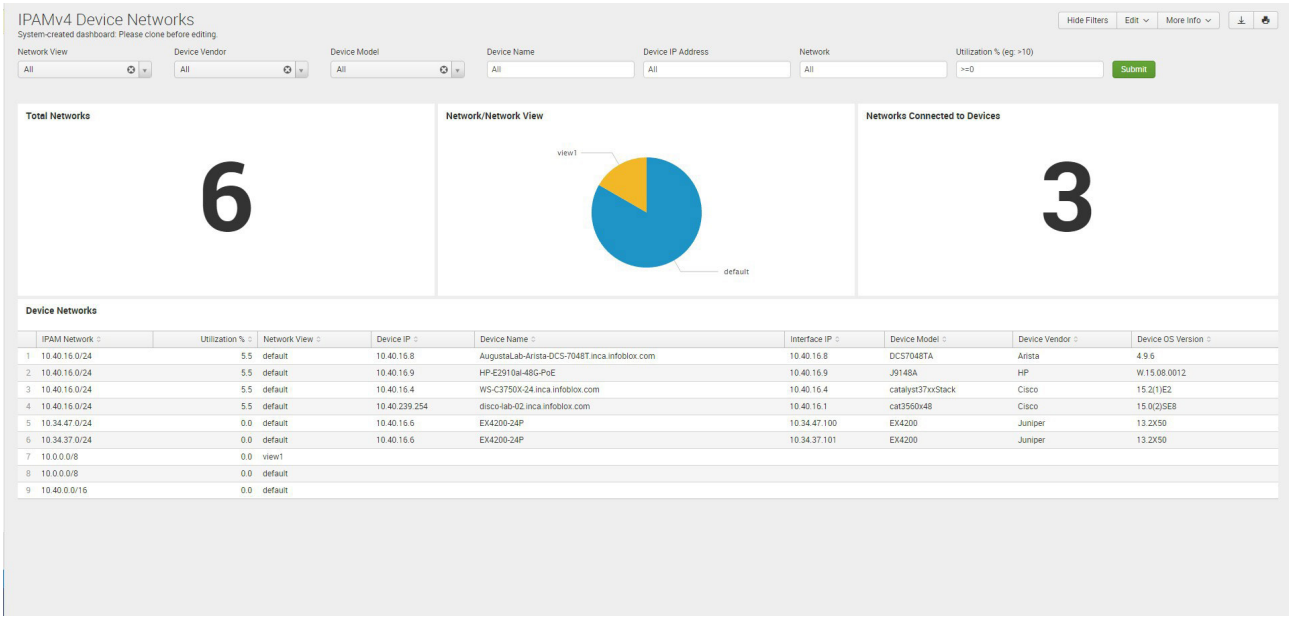
	Timestamp	Network view	Network	CIDR	AD Site	DHCPv4 Utilization %	Total	Allocated	Reserved	Assigned	Protocol	Utilization %	Unmanaged
1	2016-01-29 19:57:59	netview1	10.0.0.0	8	(no_value)	0.0	16777216	1	2	0	IPV4	0.0	0
2	2016-01-29 19:57:59	default	10.0.0.0	8	(no_value)	0.0	16777216	33	2	0	IPV4	0.0	0
3	2016-01-29 19:57:59	default	11.0.0.0	8	(no_value)	0.0	16777216	65024	2	0	IPV4	0.3	0
4	2016-01-29 19:57:59	default	12.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	0
5	2016-01-29 19:57:59	default	13.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	0
6	2016-01-29 19:57:59	netview1	14.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	0
7	2016-01-29 19:57:59	netview1	15.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	0
8	2016-01-29 19:57:59	netview1	16.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	0
9	2016-01-29 19:57:59	default	3.1.0.0	16	(no_value)	0.0	65536	5370	2	0	IPV4	8.1	0
10	2016-01-29 19:57:59	default	3.10.0.0	16	(no_value)	0.0	65536	5370	2	0	IPV4	8.1	0

« prev 1 2 3 4 5 6 next »

8.4 IPAM v4 Device Networks

Description	Tracks the number and type of networks for IPAM v4
Overview	Allows users to monitor the number of networks tracked by the IPAM database with a network view and drill down into device specifics including IP, name, interface IP, model, vendor, and OS version. This helps with troubleshooting and audit requirements.
Data presented	• IPAM Network • Utilization • Network View • Device IP • Device Name • Interface IP • Device Model • Device Vendor • Device OS Version

Sample report:

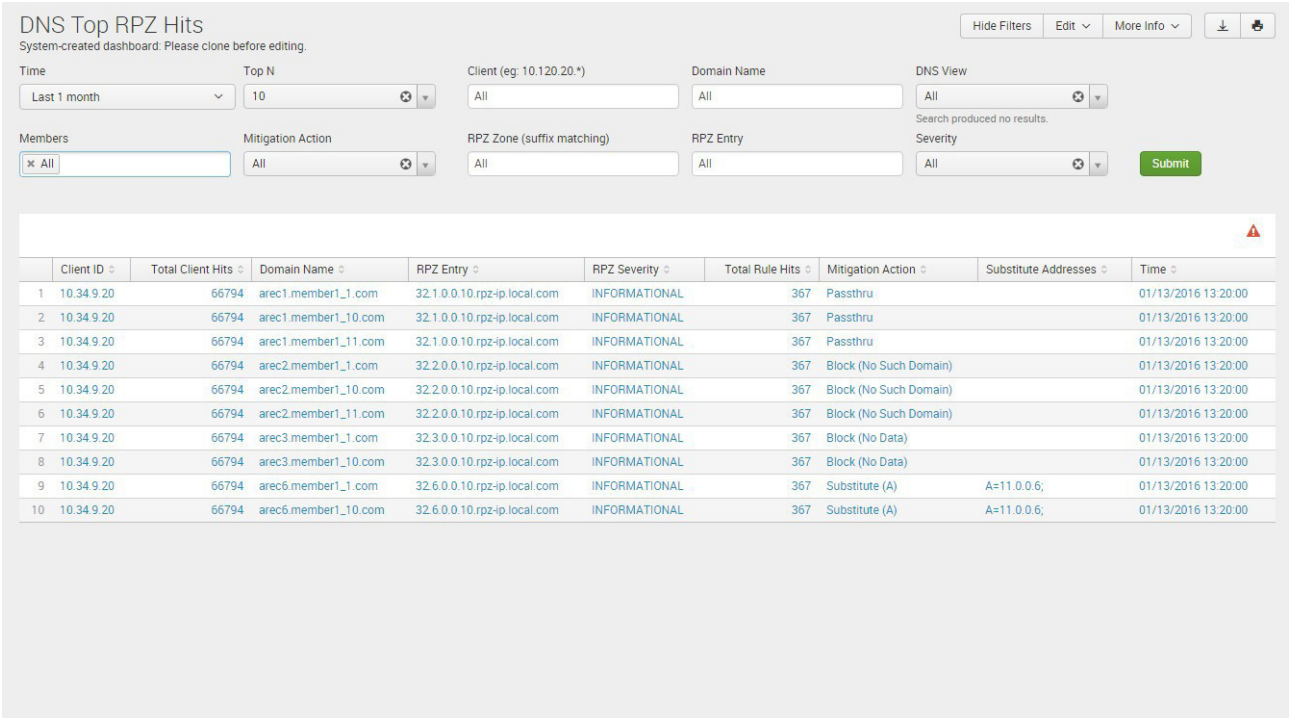


9 SECURITY (DNS) DASHBOARDS

9.1 DNS Top RPZ Hits

Description	Lists the top hits to domains defined in the Response Policy Zone
Overview	Identifies domains in the RPZ which have the most hits that have been on qualified as malicious domains. Report is designed to shorten the time to identify malware impacts by tracking when attempts are made to reach domains on the RPZ list including number of hits and time. This report is available for customers with Infoblox ActiveTrust.
Data presented	• Client ID • Total Client Hits • Domain Name • Severity • RPZ Entry • Total Rule Hits • Mitigation Action • Substitute Addresses • Time • RPZ Rule • First Identified • Description

Sample report:



DNS Top RPZ Hits

System-created dashboard. Please clone before editing.

Hide Filters | Edit | More Info

Time: Last 1 month | Top N: 10 | Client (eg: 10.120.20.*): All | Domain Name: All | DNS View: All

Search produced no results.

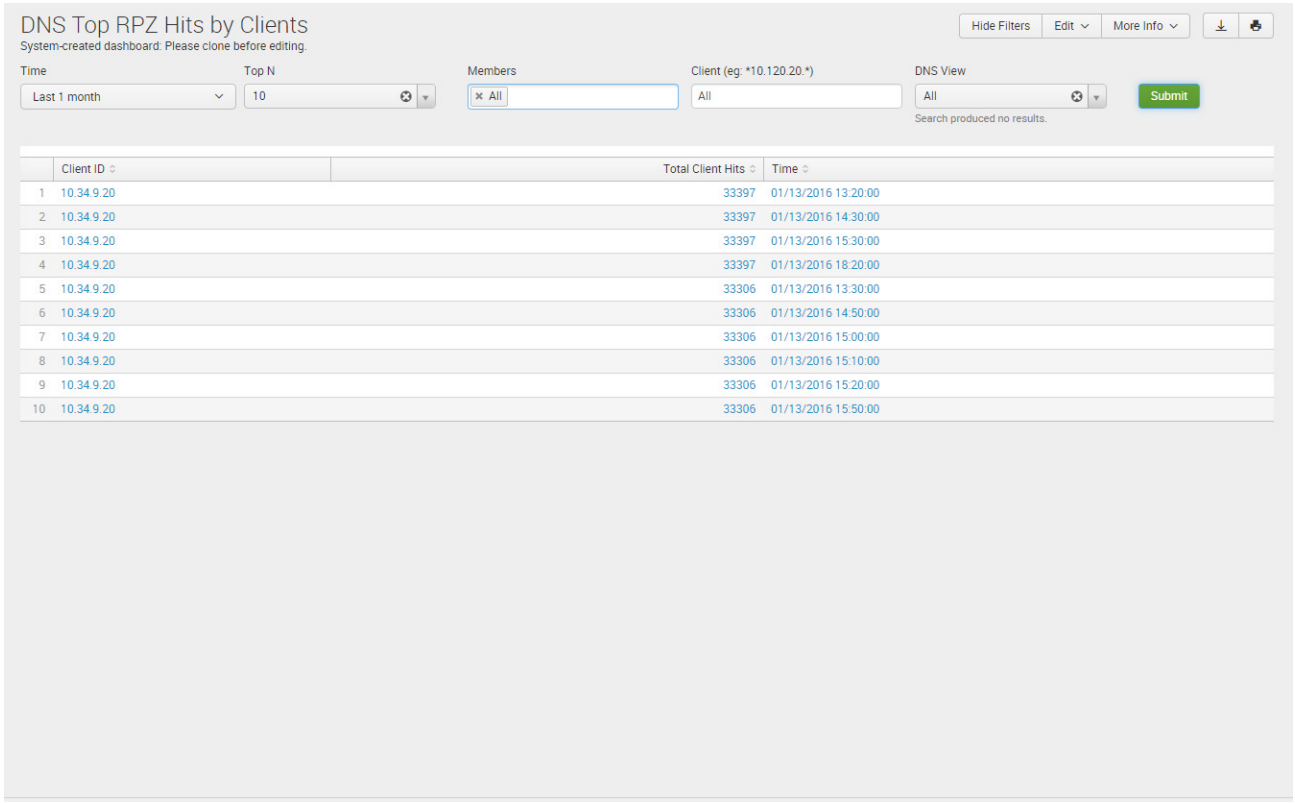
Members: All | Mitigation Action: All | RPZ Zone (suffix matching): All | RPZ Entry: All | Severity: All | Submit

	Client ID	Total Client Hits	Domain Name	RPZ Entry	RPZ Severity	Total Rule Hits	Mitigation Action	Substitute Addresses	Time
1	10.34.9.20	66794	arec1.member1_1.com	32.1.0.0.10.rpz-ip.local.com	INFORMATIONAL	367	Passthru		01/13/2016 13:20:00
2	10.34.9.20	66794	arec1.member1_10.com	32.1.0.0.10.rpz-ip.local.com	INFORMATIONAL	367	Passthru		01/13/2016 13:20:00
3	10.34.9.20	66794	arec1.member1_11.com	32.1.0.0.10.rpz-ip.local.com	INFORMATIONAL	367	Passthru		01/13/2016 13:20:00
4	10.34.9.20	66794	arec2.member1_1.com	32.2.0.0.10.rpz-ip.local.com	INFORMATIONAL	367	Block (No Such Domain)		01/13/2016 13:20:00
5	10.34.9.20	66794	arec2.member1_10.com	32.2.0.0.10.rpz-ip.local.com	INFORMATIONAL	367	Block (No Such Domain)		01/13/2016 13:20:00
6	10.34.9.20	66794	arec2.member1_11.com	32.2.0.0.10.rpz-ip.local.com	INFORMATIONAL	367	Block (No Such Domain)		01/13/2016 13:20:00
7	10.34.9.20	66794	arec3.member1_1.com	32.3.0.0.10.rpz-ip.local.com	INFORMATIONAL	367	Block (No Data)		01/13/2016 13:20:00
8	10.34.9.20	66794	arec3.member1_10.com	32.3.0.0.10.rpz-ip.local.com	INFORMATIONAL	367	Block (No Data)		01/13/2016 13:20:00
9	10.34.9.20	66794	arec6.member1_1.com	32.6.0.0.10.rpz-ip.local.com	INFORMATIONAL	367	Substitute (A)	A=11.0.0.6;	01/13/2016 13:20:00
10	10.34.9.20	66794	arec6.member1_10.com	32.6.0.0.10.rpz-ip.local.com	INFORMATIONAL	367	Substitute (A)	A=11.0.0.6;	01/13/2016 13:20:00

9.2 DNS Top RPZ Hits by Client

Description	Lists the top client IDs and hits to domains defined in the Response Policy Zone
Overview	Tracks when client IDs attempt to reach domains on the RPZ list including number of hits and time which shortens time to identify clients impacted by malware by identifying who may be infected. This report is available for customers with Infoblox Advanced ActiveTrust.
Data presented	• Client ID –Total Client Hits • Total Client Hits • Time

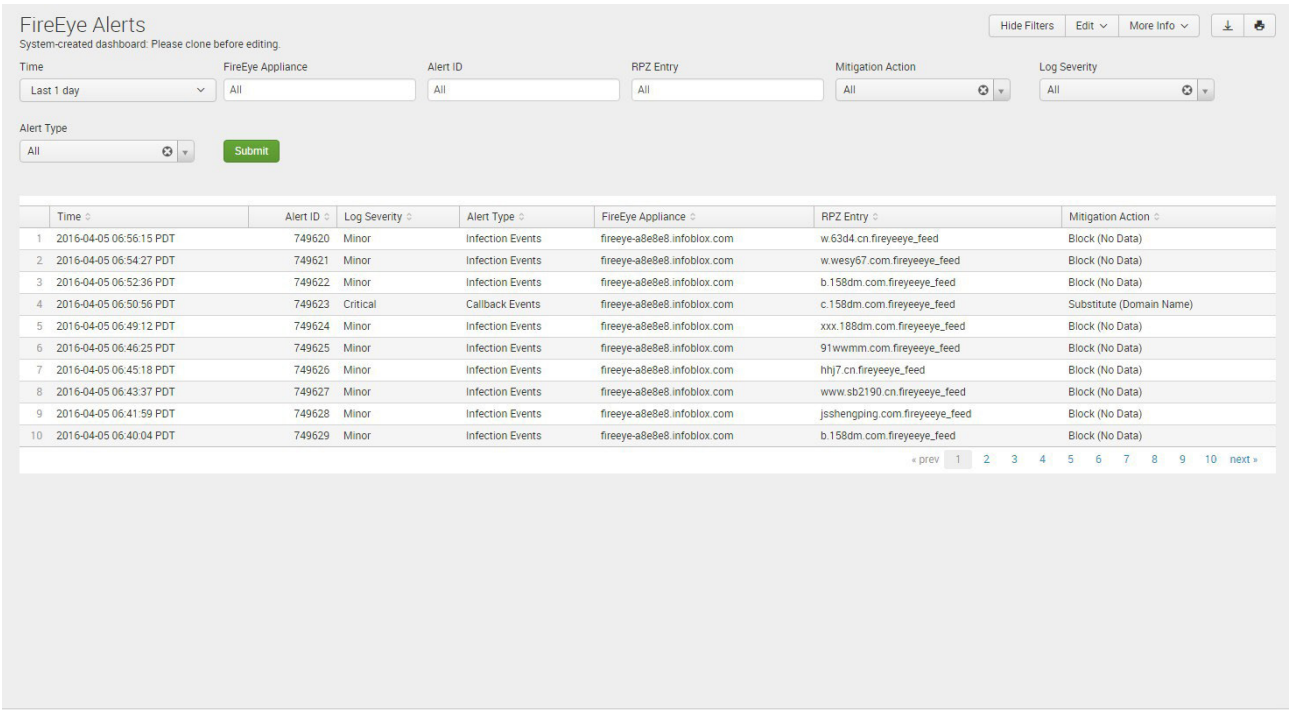
Sample report:



9.3 FireEye Alerts Report

Description	Tracks logs and alerts from FireEye appliance
Overview	Provides date/time, alert ID and log severity for FireEye block alerts provided via the Infoblox Cybersecurity Ecosystem License. Validates operation of ActiveTrust and FireEye NX appliances. This report is available for customers with Infoblox ActiveTrust and Cybersecurity Ecosystem License.
Data presented	• Time • Alert ID • Log Severity • Alert Type • FireEye Appliance • RPZ Entry • Mitigation Action

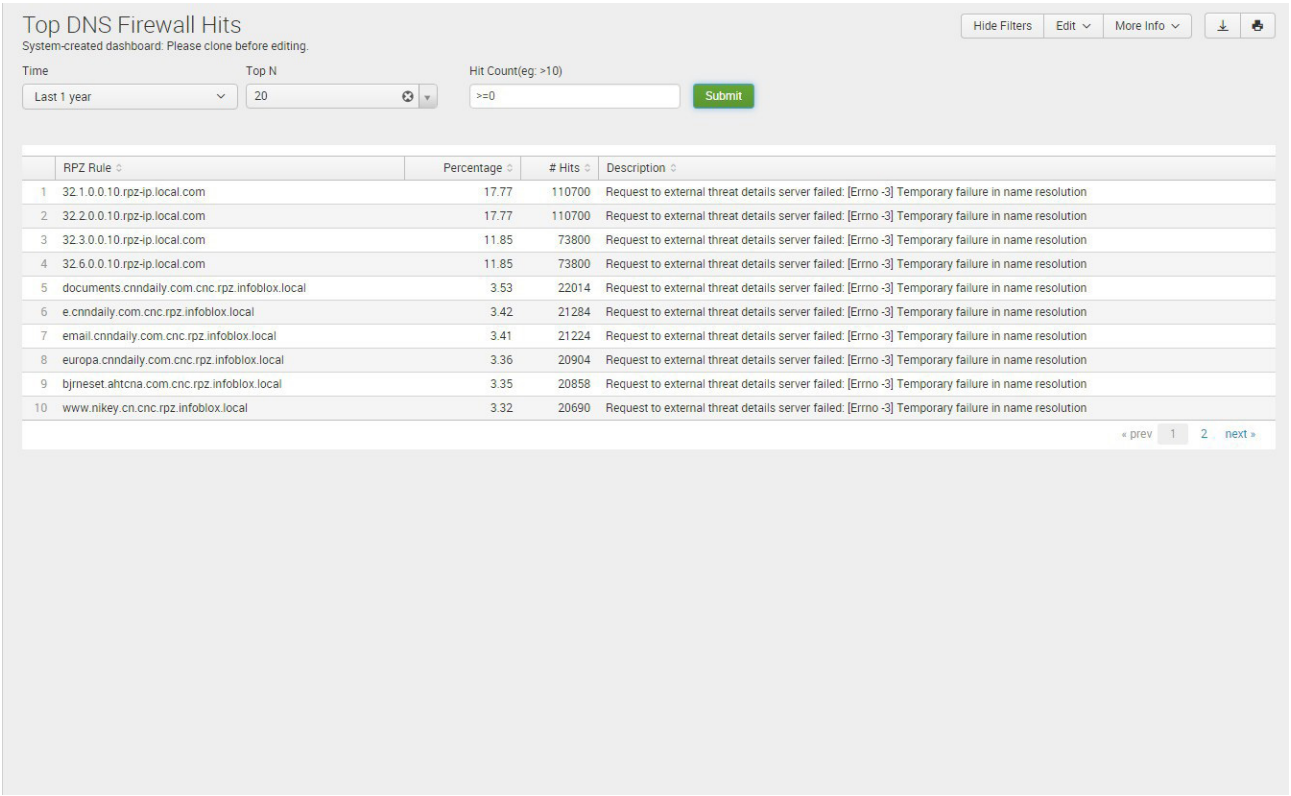
Sample report:



9.4 Top DNS Firewall Hits

Description	Lists the top RPZ rules triggered over a given time frame
Overview	Provides visibility into which RPZ rules are being triggered most often, including percentage of RPZ rules hits per rule and description of the threat that triggered the RPZ rules. This report is available for customers with Infoblox ActiveTrust.
Data presented	• RPZ rule • Percentage of RPZ rules hits • Number of Hits • Description of threat that triggered RPZ rule

Sample report:



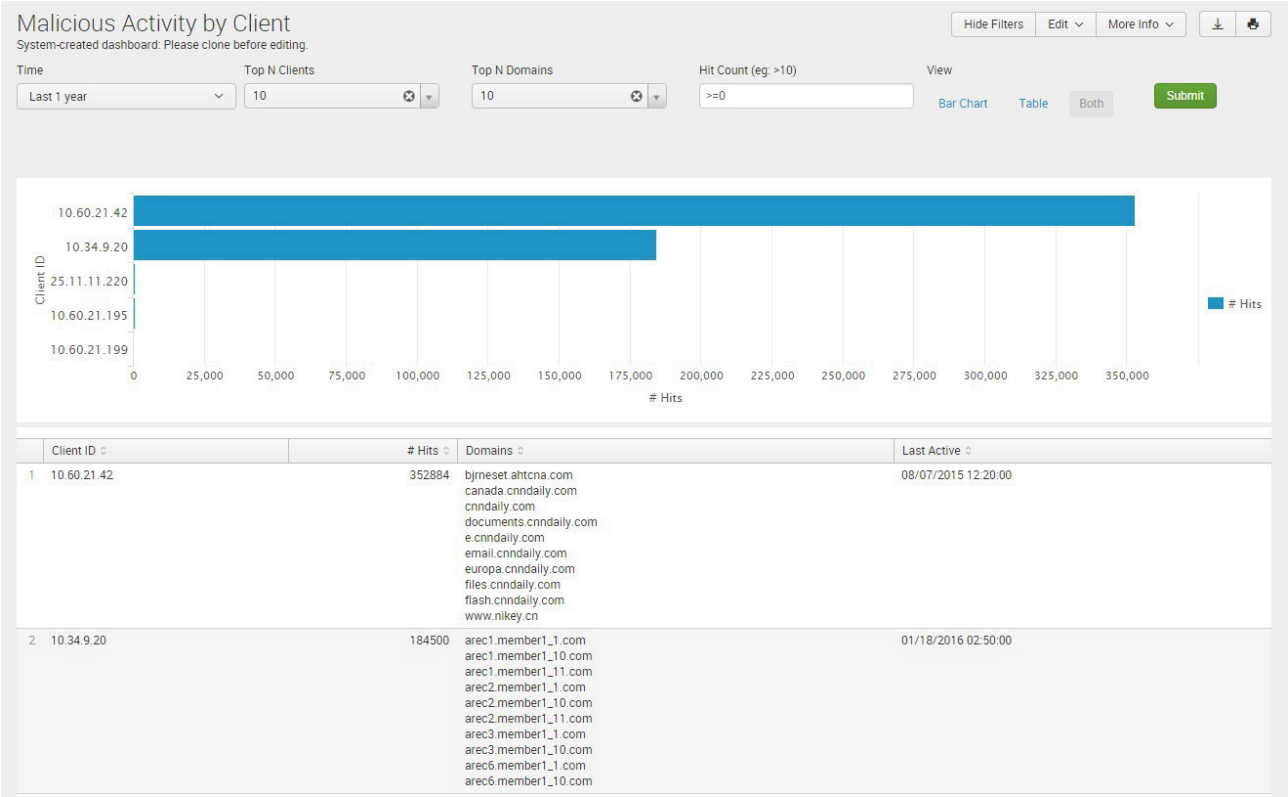
	RPZ Rule	Percentage	# Hits	Description
1	32.1.0.0.10.rpz-ip.local.com	17.77	110700	Request to external threat details server failed: [Errno -3] Temporary failure in name resolution
2	32.2.0.0.10.rpz-ip.local.com	17.77	110700	Request to external threat details server failed: [Errno -3] Temporary failure in name resolution
3	32.3.0.0.10.rpz-ip.local.com	11.85	73800	Request to external threat details server failed: [Errno -3] Temporary failure in name resolution
4	32.6.0.0.10.rpz-ip.local.com	11.85	73800	Request to external threat details server failed: [Errno -3] Temporary failure in name resolution
5	documents.cnndaily.com.cnc.rpz.infoblox.local	3.53	22014	Request to external threat details server failed: [Errno -3] Temporary failure in name resolution
6	e.cnndaily.com.cnc.rpz.infoblox.local	3.42	21284	Request to external threat details server failed: [Errno -3] Temporary failure in name resolution
7	email.cnndaily.com.cnc.rpz.infoblox.local	3.41	21224	Request to external threat details server failed: [Errno -3] Temporary failure in name resolution
8	europa.cnndaily.com.cnc.rpz.infoblox.local	3.36	20904	Request to external threat details server failed: [Errno -3] Temporary failure in name resolution
9	bjrneset.ahtcna.com.cnc.rpz.infoblox.local	3.35	20858	Request to external threat details server failed: [Errno -3] Temporary failure in name resolution
10	www.nikey.cn.cnc.rpz.infoblox.local	3.32	20690	Request to external threat details server failed: [Errno -3] Temporary failure in name resolution

« prev 1 2 next »

9.5 Malicious Activity by Client

Description	Shows clients with the most malicious activities
Overview	Highlights which clients are performing malicious activities in a particular time frame. This report is available for customers with Infoblox ActiveTrust.
Data presented	• Client ID • Number of hits • Domain • Last Active

Sample report:

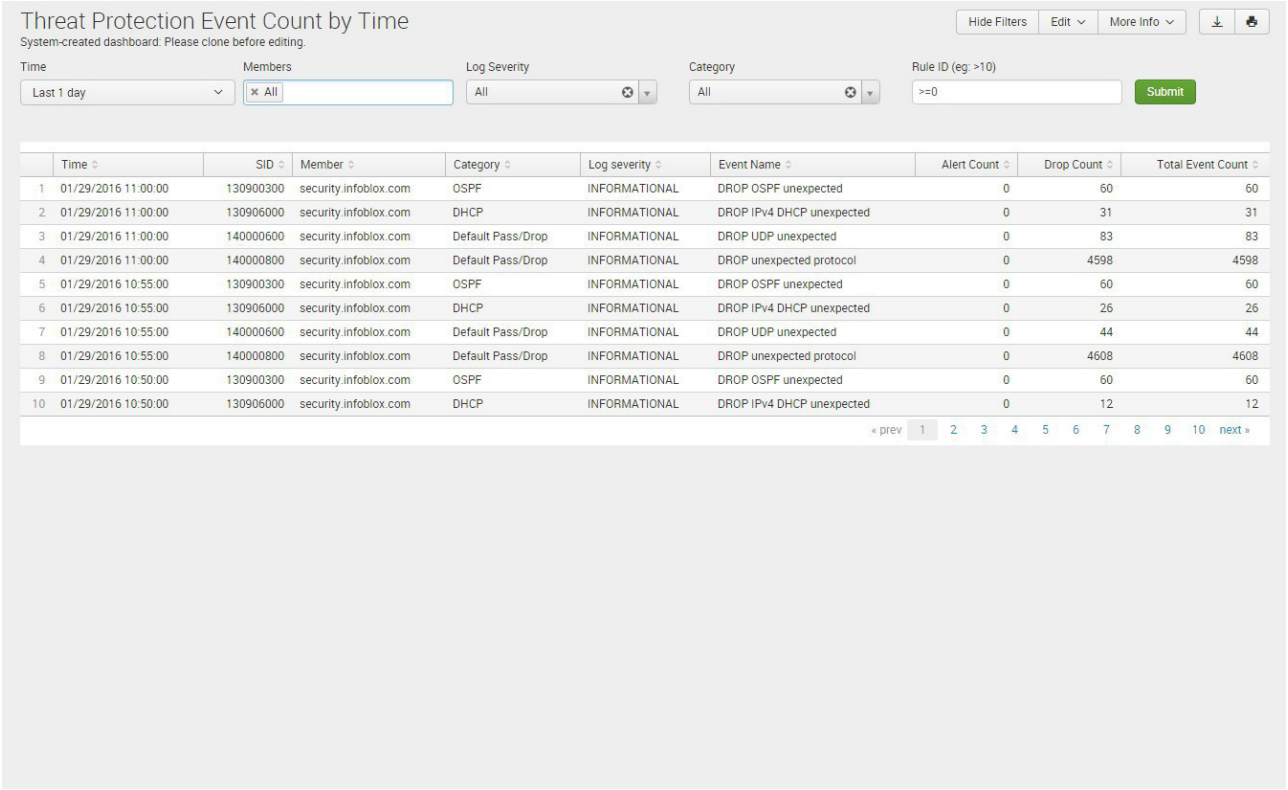


	Client ID	# Hits	Domains	Last Active
1	10.60.21.42	352884	bjrneset.ahtcna.com canada.cnndaily.com cnndaily.com documents.cnndaily.com e.cnndaily.com email.cnndaily.com europa.cnndaily.com files.cnndaily.com flash.cnndaily.com www.nikey.cn	08/07/2015 12:20:00
2	10.34.9.20	184500	arec1.member1_1.com arec1.member1_10.com arec1.member1_11.com arec2.member1_1.com arec2.member1_10.com arec2.member1_11.com arec3.member1_1.com arec3.member1_10.com arec6.member1_1.com arec6.member1_10.com	01/18/2016 02:50:00

9.6 Threat Protection Event Count by Time

Description	List of attacks that happened across the network ordered by timestamp
Overview	Helps identify if an attack is short lived or is a prolonged threat, if attacks are happening at different points in the network at the same time etc. This report is available for customers with Infoblox Advanced DNS Protection.
Data presented	• Time • SID • Member • Category • Log Severity • Event Name • Alert Count • Drop Count • Total Event Count

Sample report:



Threat Protection Event Count by Time

System-created dashboard. Please clone before editing.

Hide Filters | Edit | More Info

Time: Last 1 day | Members: All | Log Severity: All | Category: All | Rule ID (eg: >10): >=0 | Submit

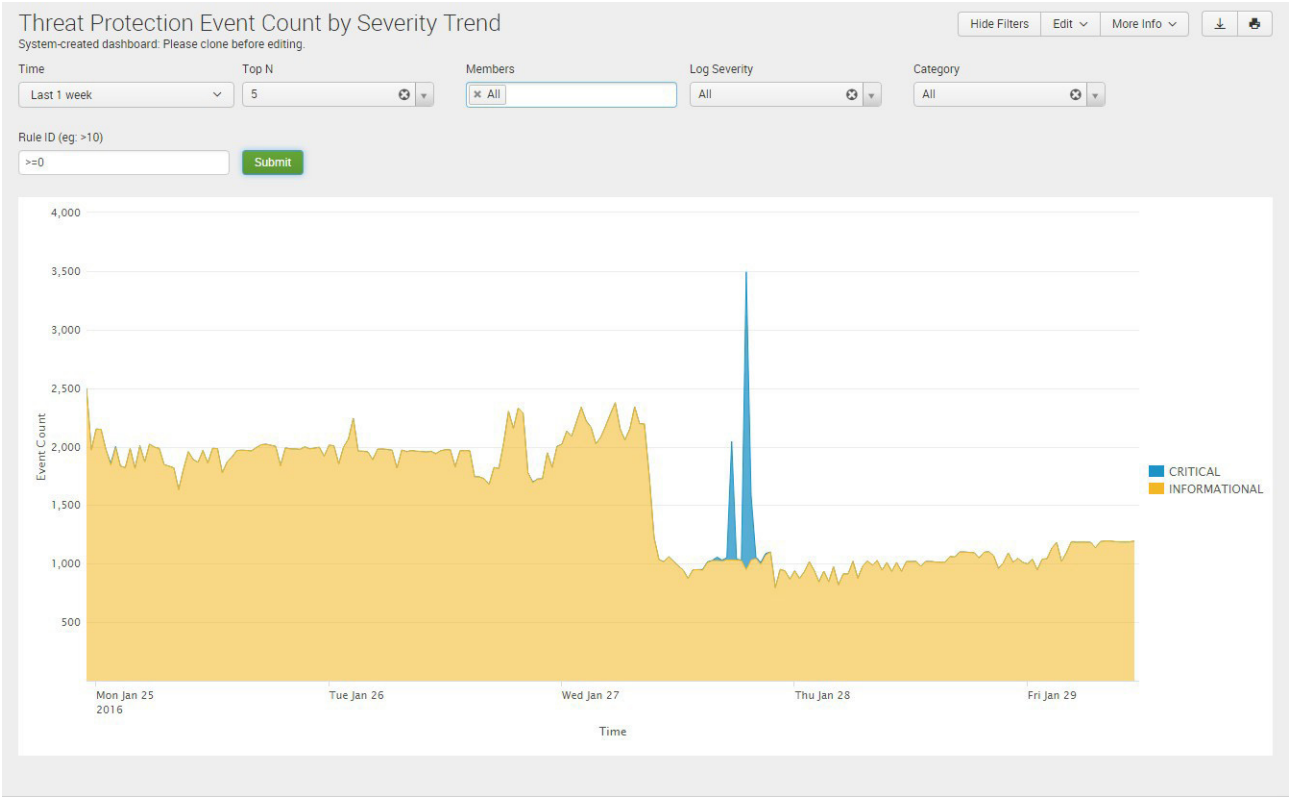
	Time	SID	Member	Category	Log severity	Event Name	Alert Count	Drop Count	Total Event Count
1	01/29/2016 11:00:00	130900300	security.infoblox.com	OSPF	INFORMATIONAL	DROP OSPF unexpected	0	60	60
2	01/29/2016 11:00:00	130906000	security.infoblox.com	DHCP	INFORMATIONAL	DROP IPv4 DHCP unexpected	0	31	31
3	01/29/2016 11:00:00	140000600	security.infoblox.com	Default Pass/Drop	INFORMATIONAL	DROP UDP unexpected	0	83	83
4	01/29/2016 11:00:00	140000800	security.infoblox.com	Default Pass/Drop	INFORMATIONAL	DROP unexpected protocol	0	4598	4598
5	01/29/2016 10:55:00	130900300	security.infoblox.com	OSPF	INFORMATIONAL	DROP OSPF unexpected	0	60	60
6	01/29/2016 10:55:00	130906000	security.infoblox.com	DHCP	INFORMATIONAL	DROP IPv4 DHCP unexpected	0	26	26
7	01/29/2016 10:55:00	140000600	security.infoblox.com	Default Pass/Drop	INFORMATIONAL	DROP UDP unexpected	0	44	44
8	01/29/2016 10:55:00	140000800	security.infoblox.com	Default Pass/Drop	INFORMATIONAL	DROP unexpected protocol	0	4608	4608
9	01/29/2016 10:50:00	130900300	security.infoblox.com	OSPF	INFORMATIONAL	DROP OSPF unexpected	0	60	60
10	01/29/2016 10:50:00	130906000	security.infoblox.com	DHCP	INFORMATIONAL	DROP IPv4 DHCP unexpected	0	12	12

« prev 1 2 3 4 5 6 7 8 9 10 next »

9.7 Threat Protection Event Count by Severity Trend

Description	Shows attacks categorized by severity
Overview	Provides graphical representation of all attacks categorized by severity levels (pre-defined) – critical, informational and major. Helps understand severity trends at different times, on different members, by category etc. to take corrective measures. This report is available for customers with Infoblox Advanced DNS Protection.
Data presented	• Event count • Severity Type • Time

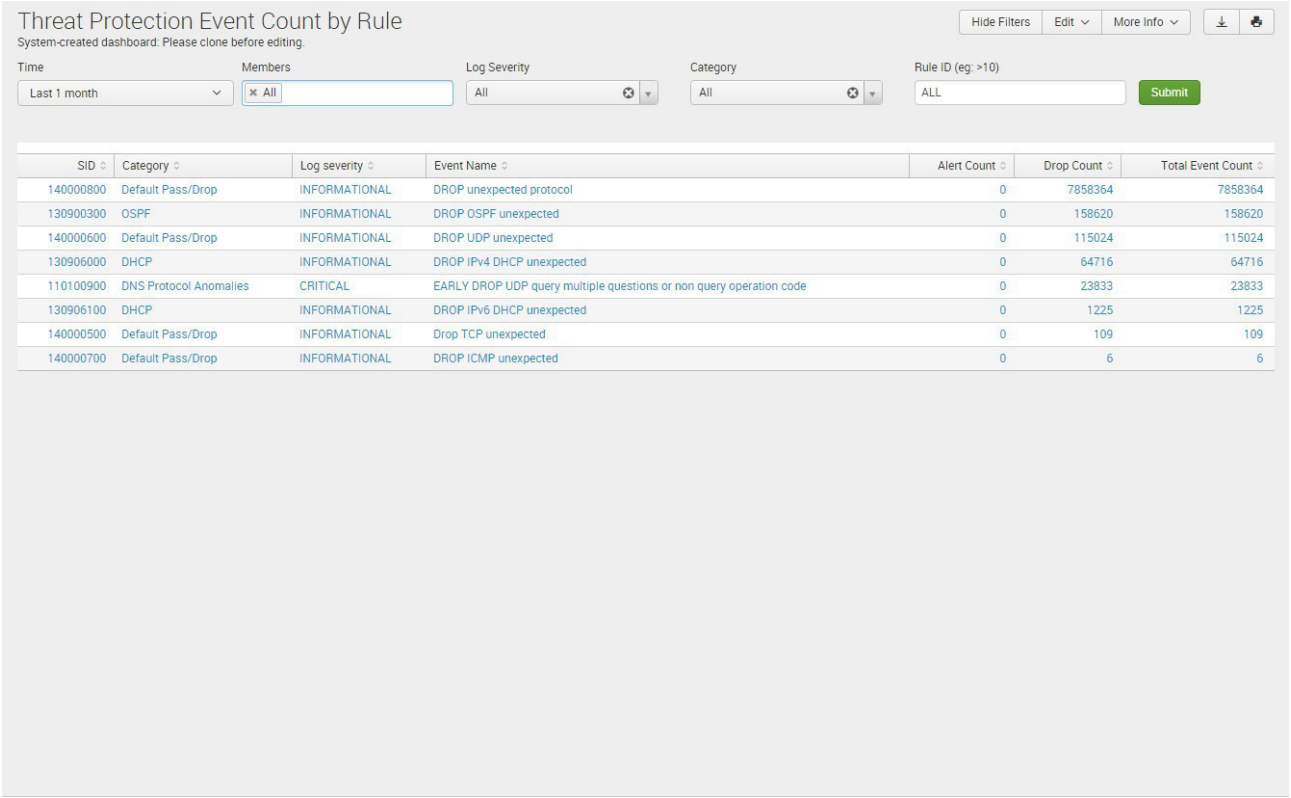
Sample report:



9.8 Threat Protection Event Count by Rule

Description	Shows attacks by pre-defined threat rules
Overview	Helps identify most used threat rules for protection, providing intelligence on common threats to DNS. This report is available for customers with Infoblox Advanced DNS Protection.
Data presented	• SID • Category • Log Severity • Event Name • Alert Count • Drop Count • Total Event Count

Sample report:

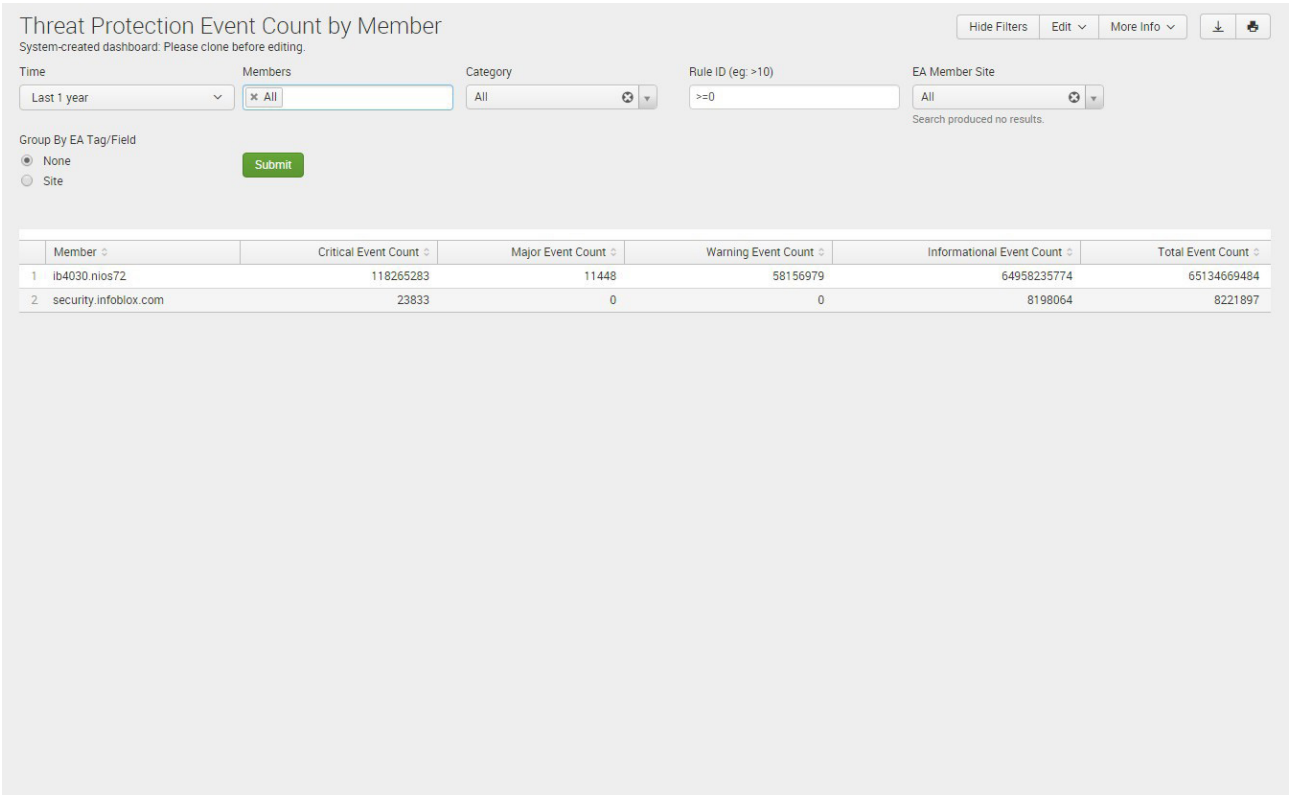


SID	Category	Log severity	Event Name	Alert Count	Drop Count	Total Event Count
140000800	Default Pass/Drop	INFORMATIONAL	DROP unexpected protocol	0	7858364	7858364
130900300	OSPF	INFORMATIONAL	DROP OSPF unexpected	0	158620	158620
140000600	Default Pass/Drop	INFORMATIONAL	DROP UDP unexpected	0	115024	115024
130906000	DHCP	INFORMATIONAL	DROP IPv4 DHCP unexpected	0	64716	64716
110100900	DNS Protocol Anomalies	CRITICAL	EARLY DROP UDP query multiple questions or non query operation code	0	23833	23833
130906100	DHCP	INFORMATIONAL	DROP IPv6 DHCP unexpected	0	1225	1225
140000500	Default Pass/Drop	INFORMATIONAL	Drop TCP unexpected	0	109	109
140000700	Default Pass/Drop	INFORMATIONAL	DROP ICMP unexpected	0	6	6

9.9 Threat Protection Event Count by Member

Description	Shows attacks happening on each member in the network
Overview	Helps identify severity of attacks happening on a member, and to pinpoint which member(s) are frequent targets for different kinds of attacks. This report is available for customers with Infoblox Advanced DNS Protection.
Data presented	• Member • Critical Event Count • Major Event Count • Warning Event Count • Informational Event Count • Total Event Count

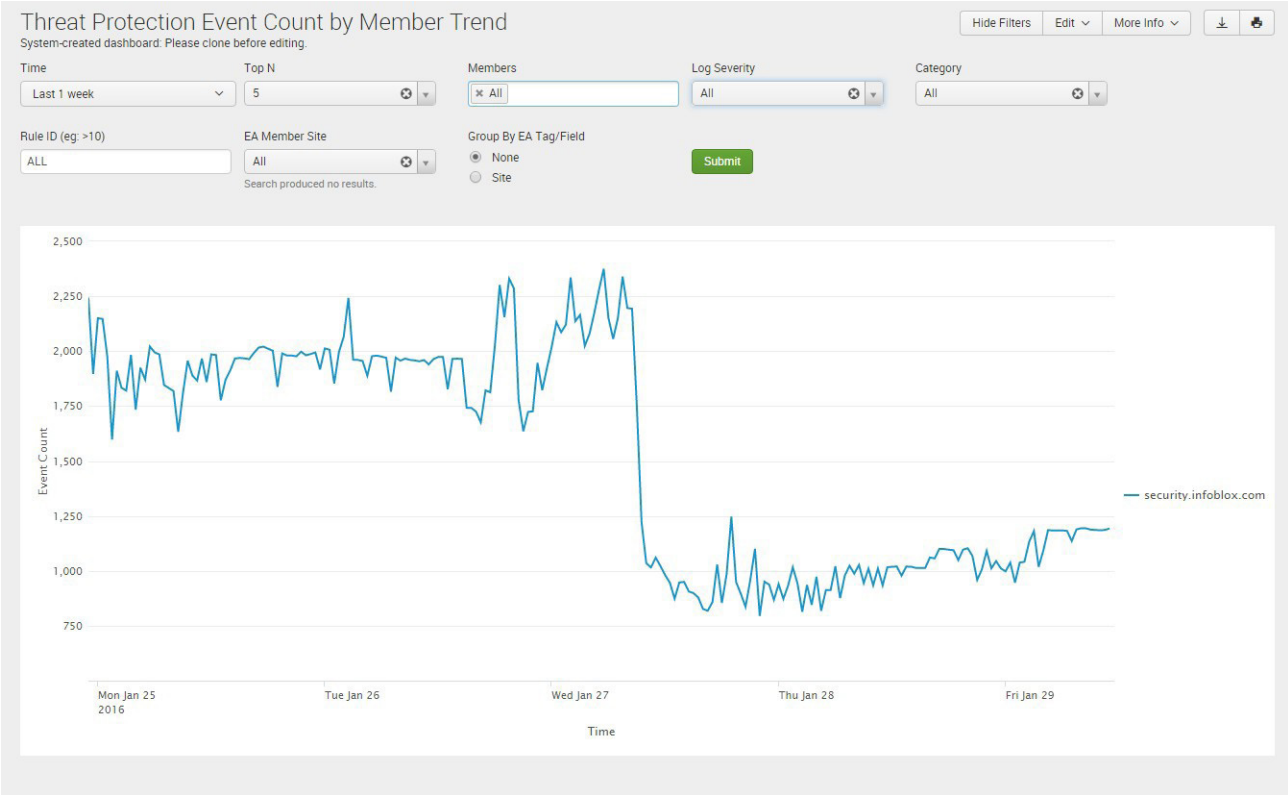
Sample report:



9.10 Threat Protection Event Count by Member Trend

Description	Shows members targeted the most with DNS attacks
Overview	Provides a graphical representation of Top N members that have been attacked over a selected time period. Helps identify points of risk in the network and take appropriate action. This report is available for customers with Infoblox Advanced DNS Protection.
Data presented	• Time • Member • Event Count

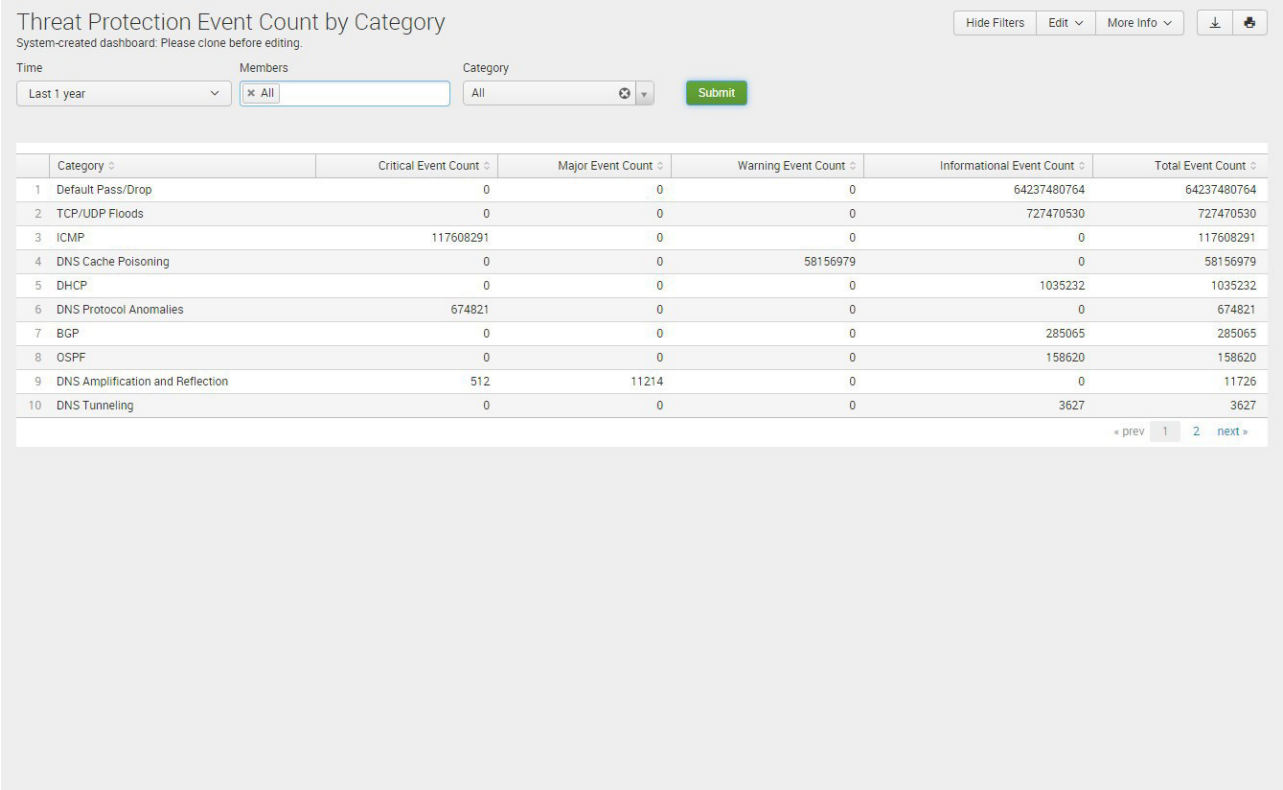
Sample report:



9.11 Threat Protection Event Count by Category

Description	Shows attacks by threat category
Overview	Helps identify which category of attacks is more frequent over a given time period or targeted to specific members. This report is available for customers with Infoblox Advanced DNS Protection.
Data presented	• Category • Critical Event Count • Major Event Count • Warning Event Count • Informational Event Count • Total Event Count

Sample report:



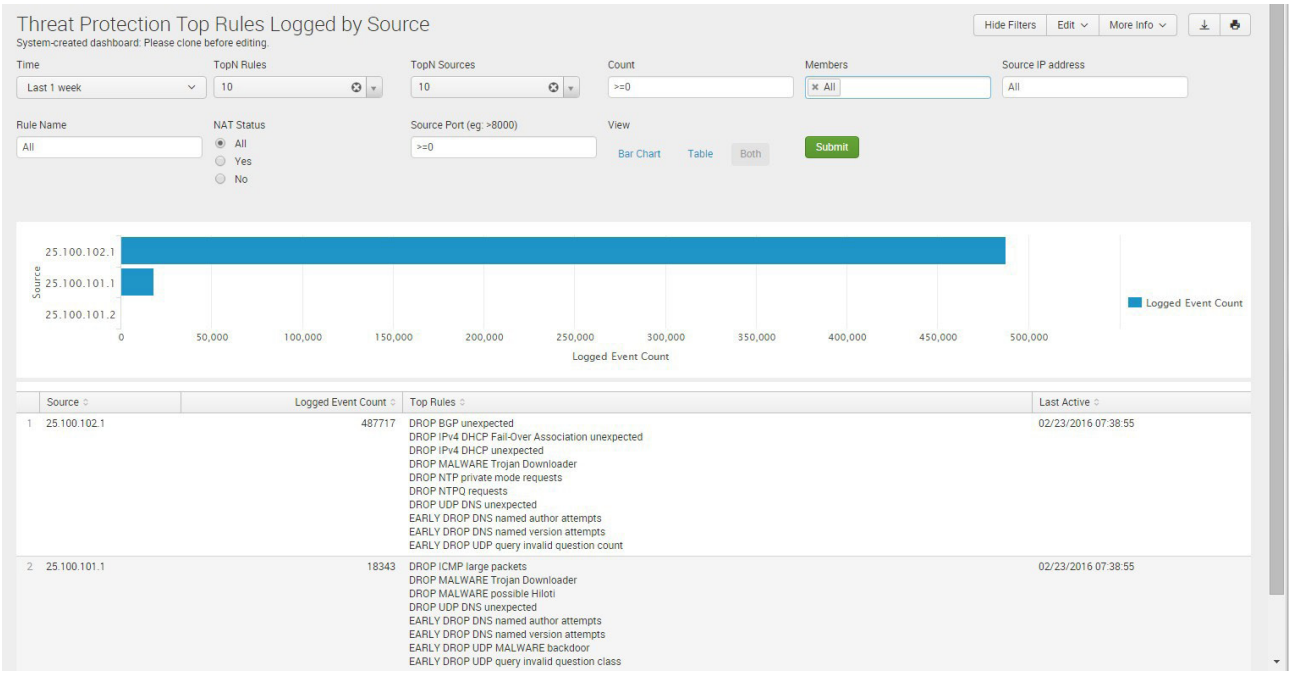
	Category	Critical Event Count	Major Event Count	Warning Event Count	Informational Event Count	Total Event Count
1	Default Pass/Drop	0	0	0	64237480764	64237480764
2	TCP/UDP Floods	0	0	0	727470530	727470530
3	ICMP	117608291	0	0	0	117608291
4	DNS Cache Poisoning	0	0	58156979	0	58156979
5	DHCP	0	0	0	1035232	1035232
6	DNS Protocol Anomalies	674821	0	0	0	674821
7	BGP	0	0	0	285065	285065
8	OSPF	0	0	0	158620	158620
9	DNS Amplification and Reflection	512	11214	0	0	11726
10	DNS Tunneling	0	0	0	3627	3627

« prev 1 2 next »

9.12 Threat Protection Top Rules Logged by Source

Description	Lists the top source IP s hitting each threat rule
Overview	Helps identify the clients that are attacking the server the most and which rules they trigger. This enables the administrator to tune thresholds of the rules better. This report is available for customers with Infoblox Advanced DNS Protection.
Data presented	• Source IP • Event Count per Source IP • Top Rules • Last Active

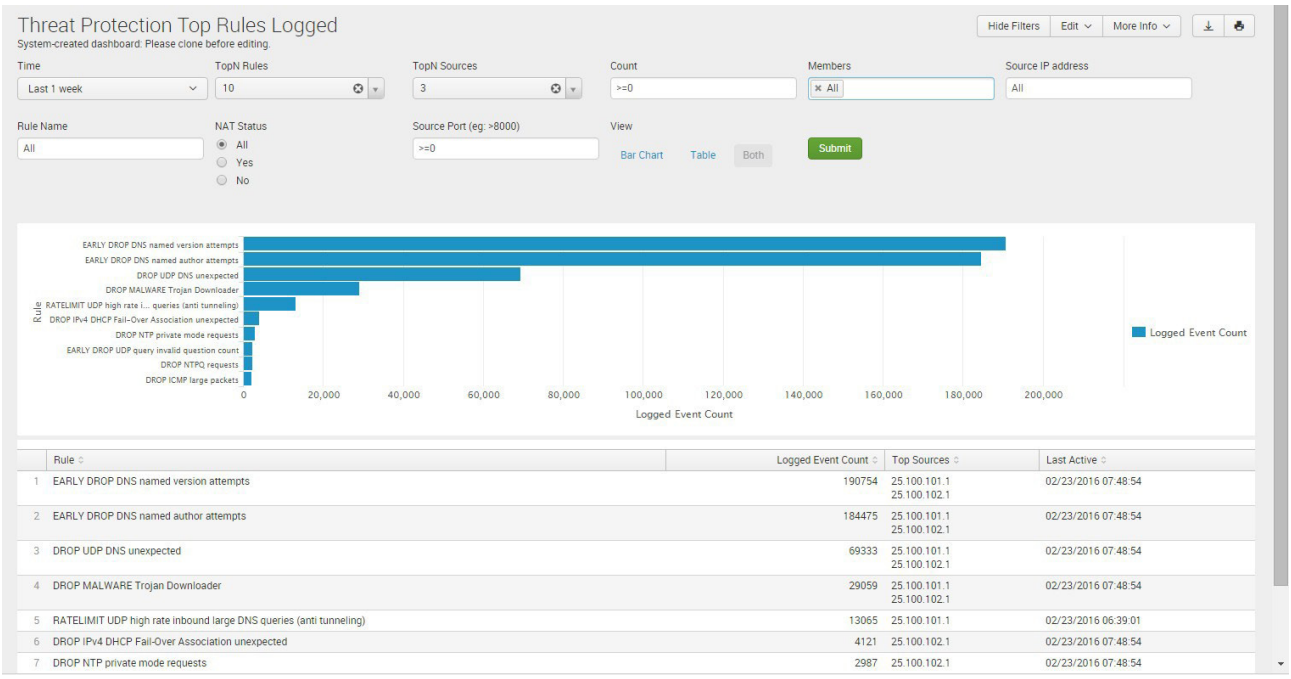
Sample report:



9.13 Threat Protection Top Rules Logged

Description	Lists the top threat rules hit by attacks
Overview	Helps identify the most triggered threat rules. This enables the administrator to know which attacks are more frequent and can tune thresholds for the corresponding threat rules. This report is available for customers with Infoblox Advanced DNS Protection.
Data presented	• Event names • Event count per threat event

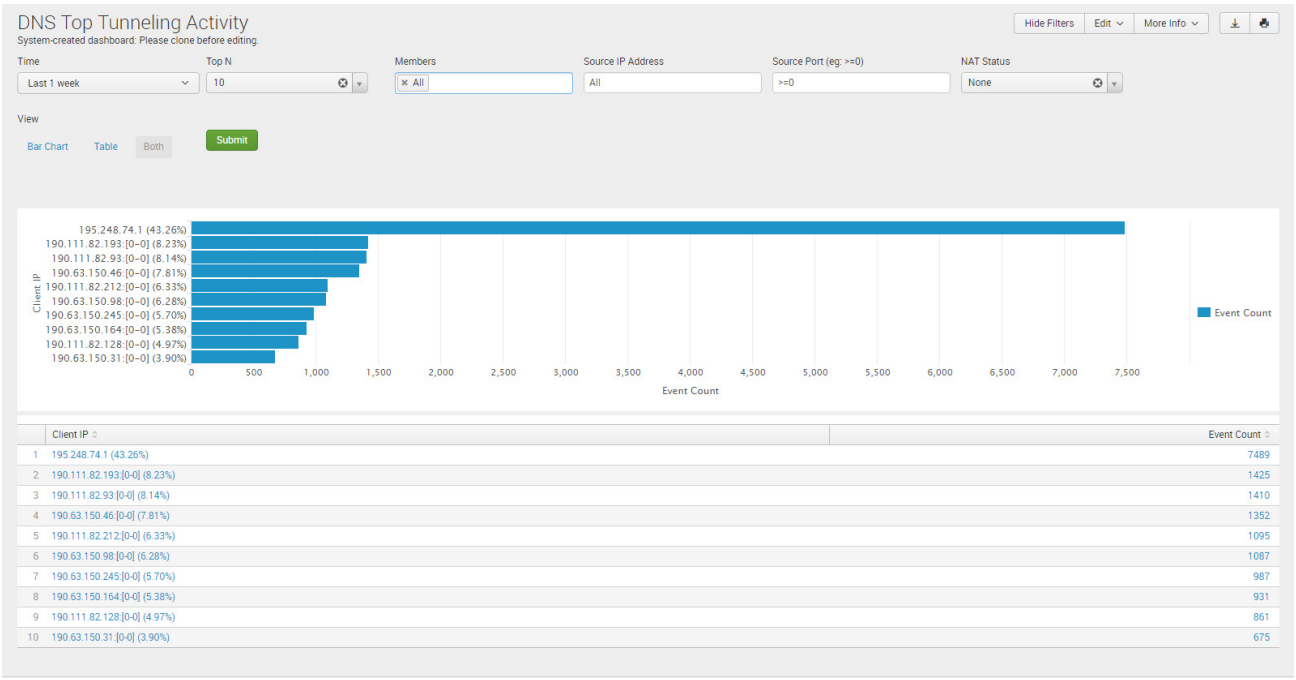
Sample report:



9.14 DNS Top Tunneling Activity

Description	Lists the clients that have the most number of DNS tunneling activities in a given time frame
Overview	Helps identify the clients most often performing DNS tunneling activities. This data can be used by the security team for investigation and/or taking an action on those clients. This report is available for customers with Infoblox Advanced DNS Protection.
Data presented	• Client IP • Event Count • Category • Last Seen

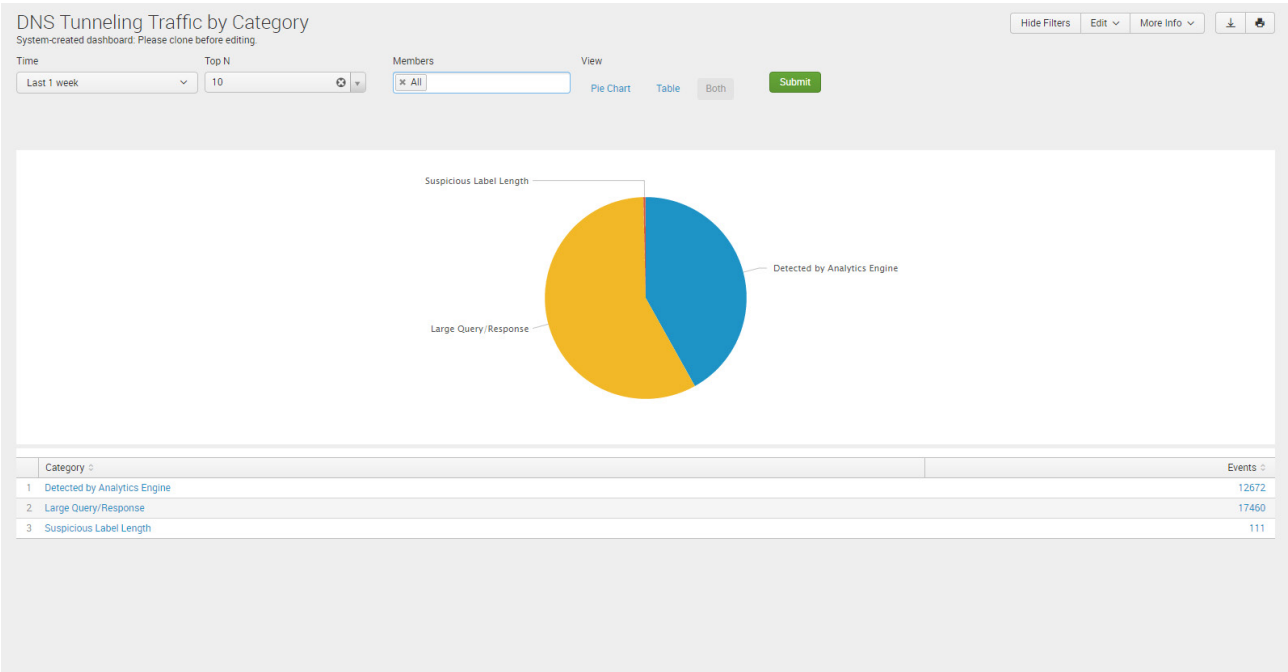
Sample report:



9.15 DNS Tunneling Traffic by Category

Description	Lists information about DNS tunneling activities by specific categories and the percentage of events by the category of DNS tunneling events in a given time frame
Overview	Helps provide visibility into the top categories of DNS tunneling activities to help prioritize risk mitigation efforts to counter DNS tunneling-based malware insertion, data exfiltration and anonymous IP traffic tunneling attempts. This report is available for customers with Infoblox Advanced DNS Protection.
Data presented	• Category • Category % • Description • Client IP • Rule SID • Event Count • Rule Description • Last Seen

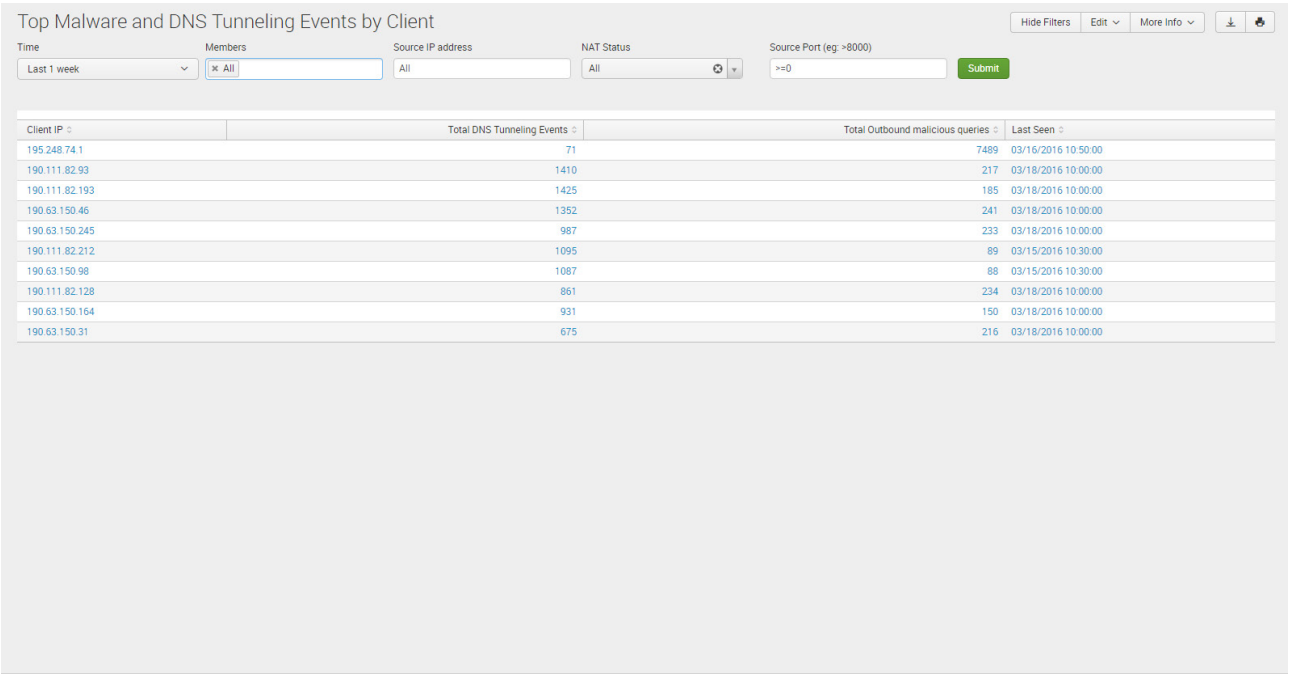
Sample report:



9.16 Top Malware and DNS Tunneling Events by Client

Description	Lists the clients that have the most number of outbound malicious queries (RPZ hits) and DNS tunneling events in a given time frame
Overview	Helps identify the top infected clients detected making outbound malicious queries and that were associated with DNS tunneling activities, so that the security team can more easily prioritize DNS-related security efforts, with a two-fold goal: to prevent spread of malware and prevent further damage from DNS tunnelingattempts, such as data exfiltration. This report is available for customers with Infoblox ActiveTrust.
Data presented	• Client IP • Total DNS Tunneling Events • Total Outbound Malicious Queries • Last Seen

Sample report:

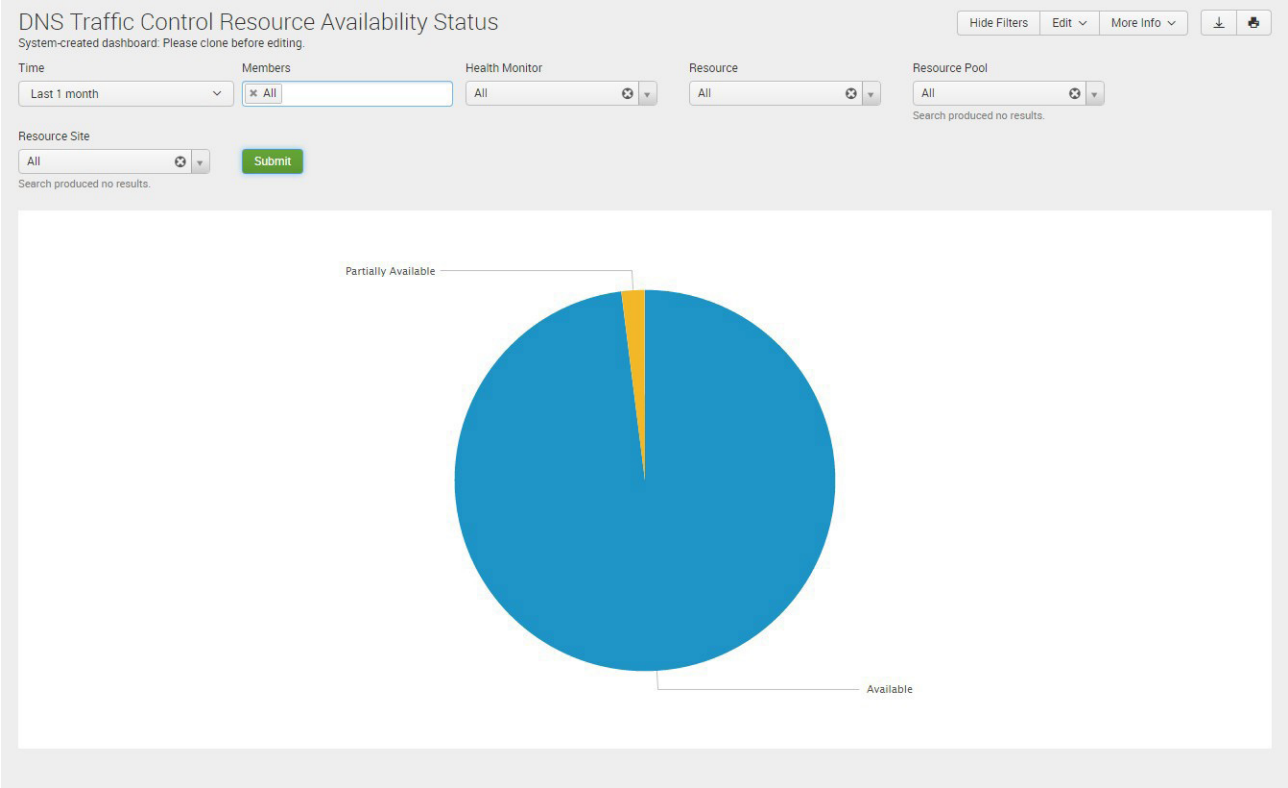


10 DNS TRAFFIC CONTROLS DASHBOARDS

10.1 DNS Traffic Control Resource Availability Status

Description	Tracks the resource availability of DNS Traffic Control with customizable time periods
Overview	Highlights the availability (or lack of availability) for DNS Traffic Control resources. Helps identify if limited or no availability of resources has impacts performance and shortens time to troubleshoot.
Data presented	• Available • Partially available • Unavailable

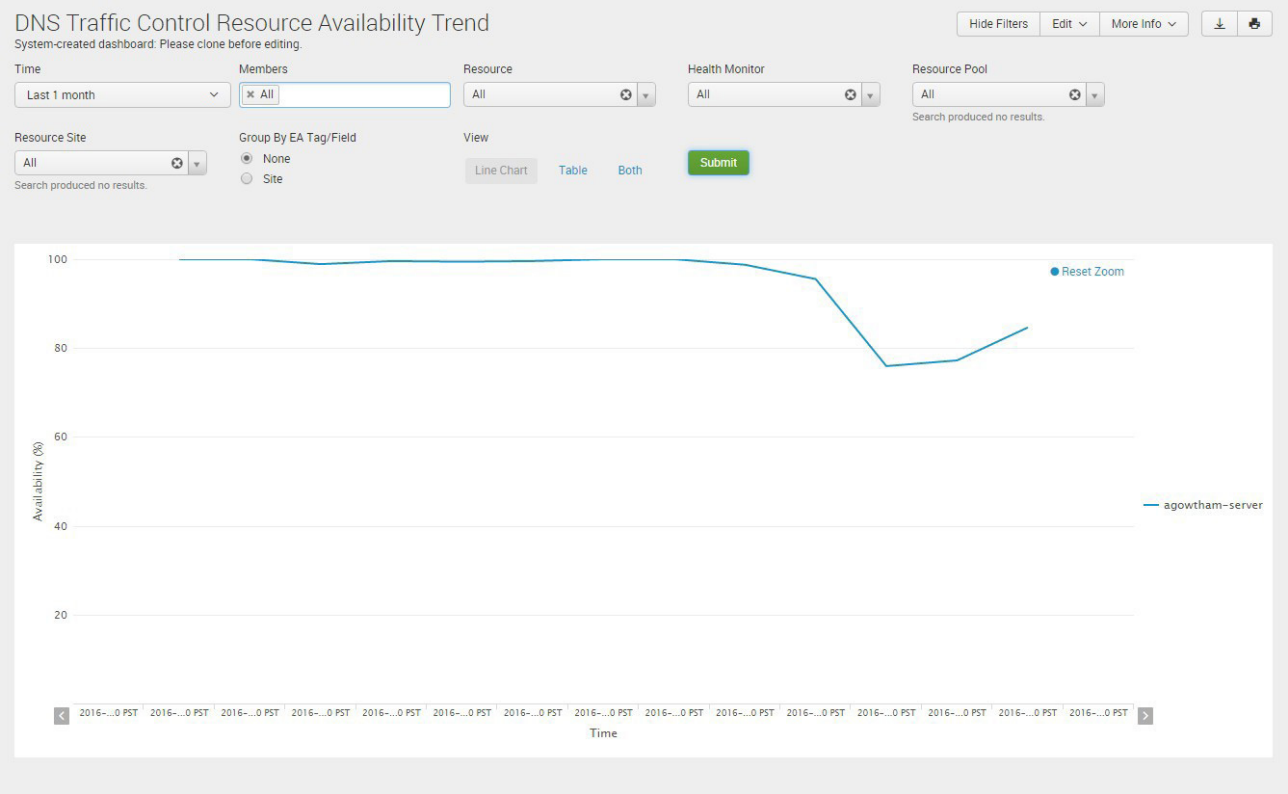
Sample report:



10.2 DNS Traffic Control Resource Availability Trend

Description	Provides the resource availability of DNS Traffic Control over time with trending
Overview	Tracks the availability (or lack of availability) for DNS Traffic Control resources over time. Helps monitor changes over time to find trends that can impact performance.
Data presented	• Availability % • Time • Traffic Control Resources

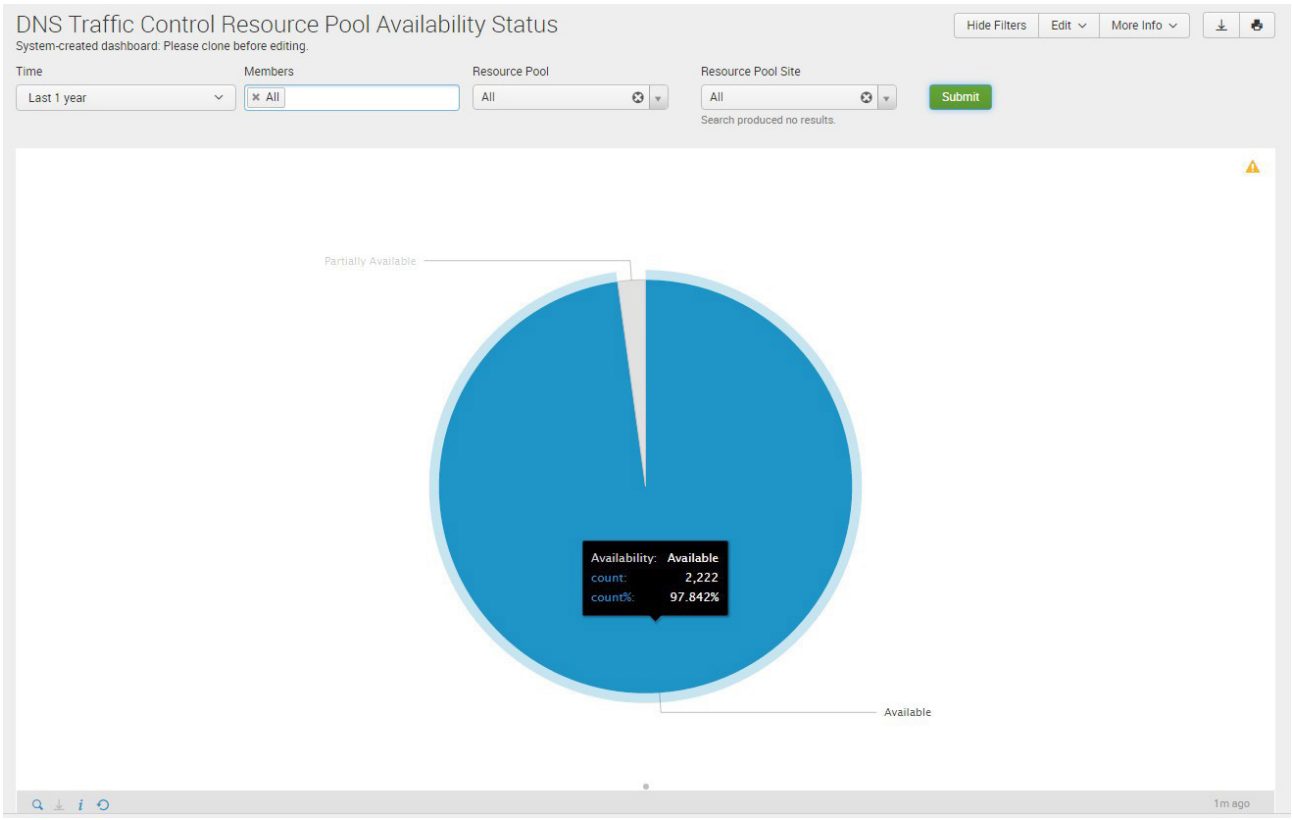
Sample report:



10.3 DNS Traffic Control Resource Pool Availability Status

Description	Tracks the resource pool availability of DNS Traffic Control with customizable time periods
Overview	Monitors the availability status for DNS Traffic Control resources for the resource pool. Helps identify if limited or no availability of resources within a particular pool has an impact performance and shortens time to troubleshoot.
Data presented	• Available • Partially available • Unavailable

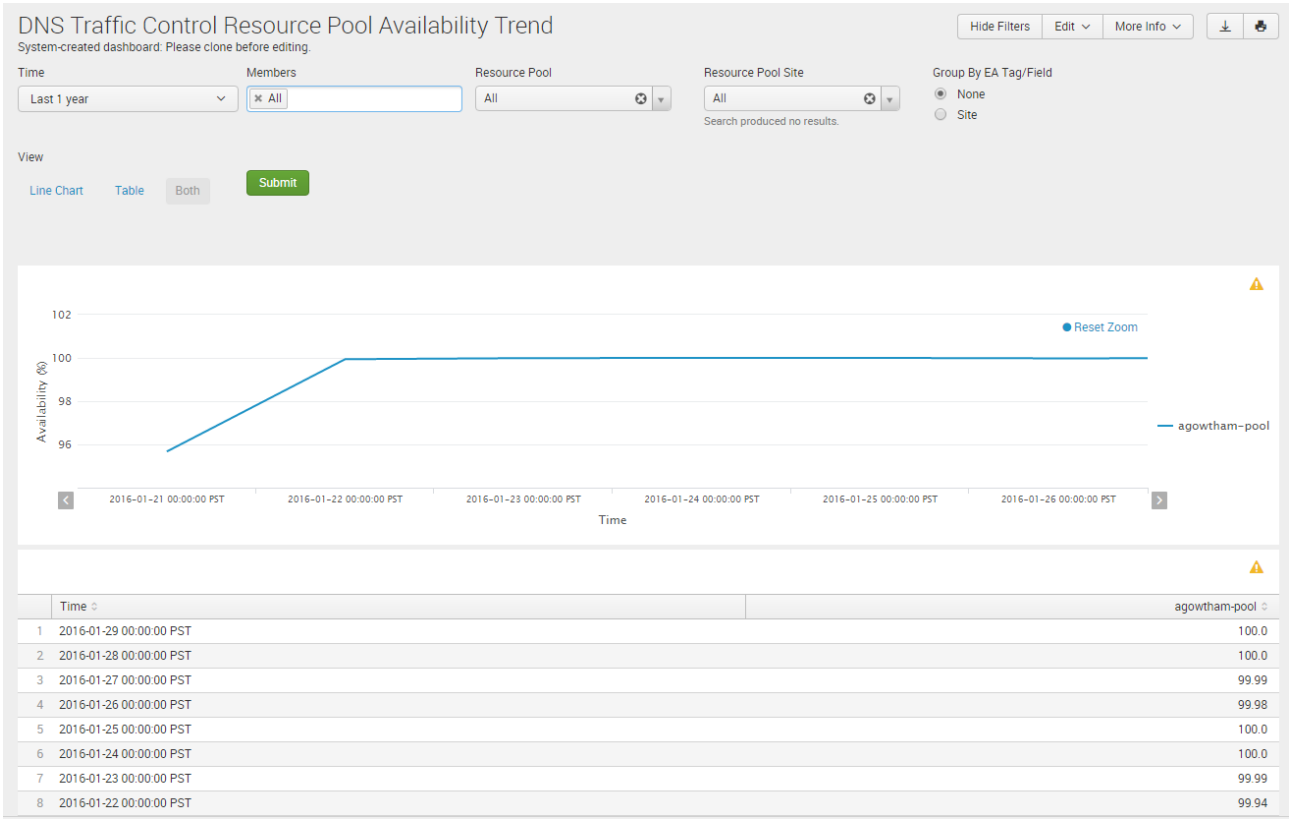
Sample report:



10.4 DNS Traffic Control Resource Pool Availability Trend

Description	Provides the resource pool availability of DNS Traffic Control over time with trending
Overview	Tracks the availability status for DNS Traffic Control resources for the resource pool over time. Helps identify trends where limited or no availability of resources within a particular pool has impacted performance and shortens time to troubleshoot.
Data presented	• Availability % • Time • Traffic Control Resources

Sample report:

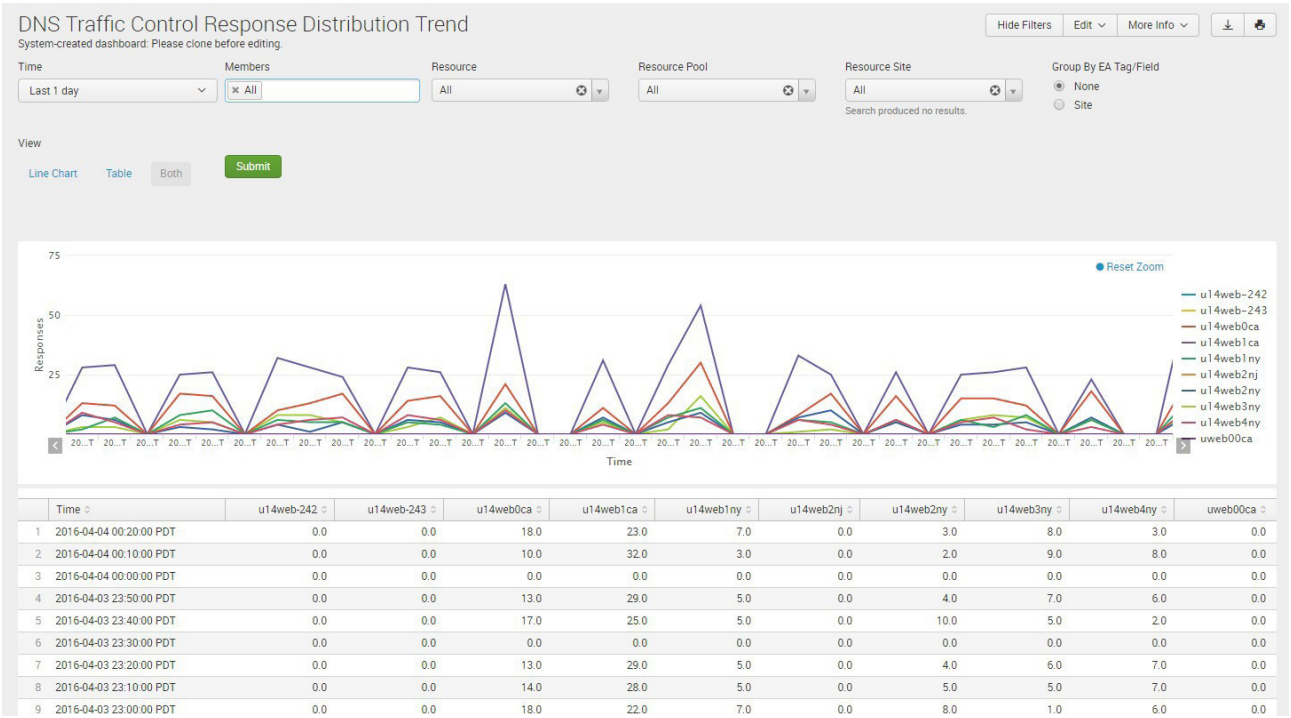


	Time	agowtham-pool
1	2016-01-29 00:00:00 PST	100.0
2	2016-01-28 00:00:00 PST	100.0
3	2016-01-27 00:00:00 PST	99.99
4	2016-01-26 00:00:00 PST	99.98
5	2016-01-25 00:00:00 PST	100.0
6	2016-01-24 00:00:00 PST	100.0
7	2016-01-23 00:00:00 PST	99.99
8	2016-01-22 00:00:00 PST	99.94

10.5 DNS Traffic Control Response Distribution Trend

Description	Tracks the responses of DNS Traffic Control over time with trending
Overview	Monitors the response distribution trends for DNS Traffic Control resources over time. Helps pinpoint of a trend of abnormal distribution has impacted performance.
Data presented	• Responses • Time • Traffic Control Resources

Sample report:

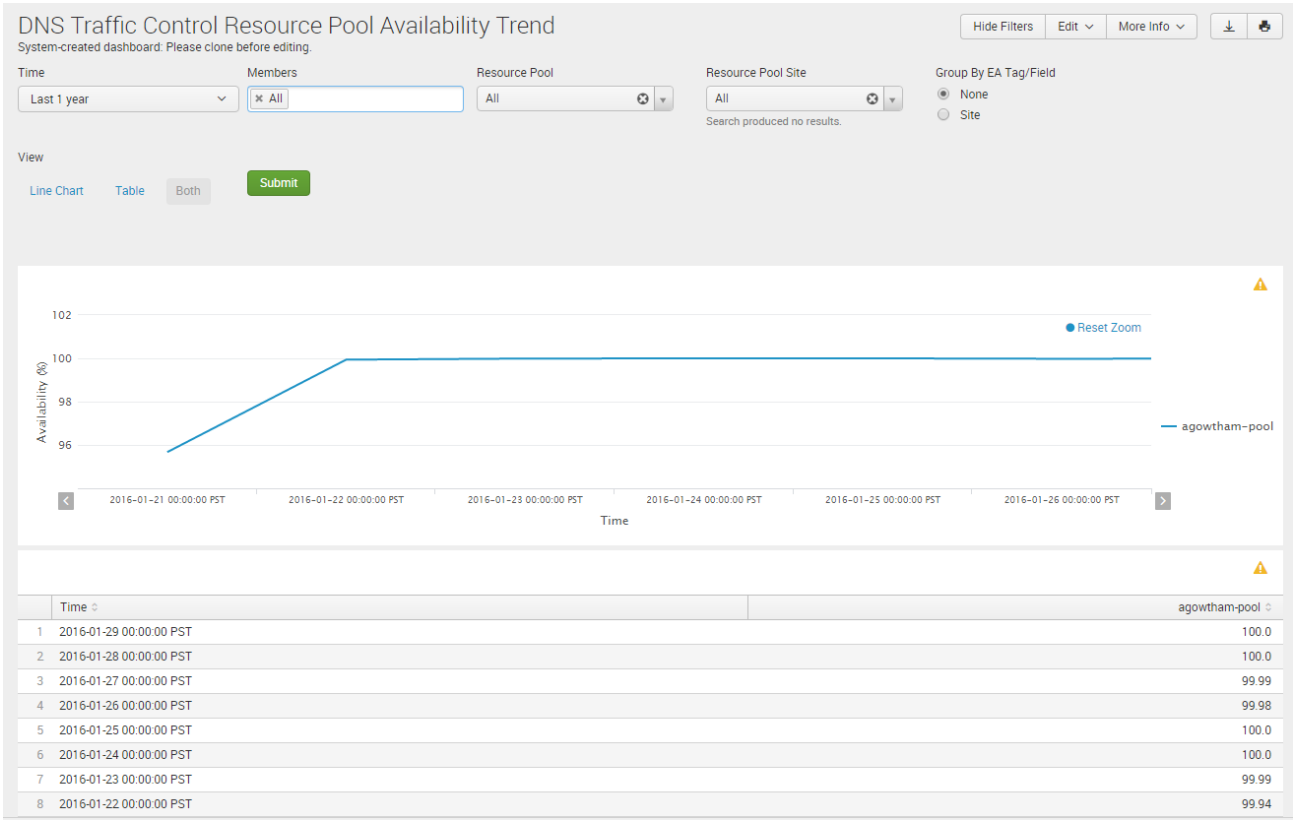


	Time	u14web-242	u14web-243	u14web0ca	u14web1ca	u14web1ny	u14web2nj	u14web2ny	u14web3ny	u14web4ny	uweb00ca
1	2016-04-04 00:20:00 PDT	0.0	0.0	18.0	23.0	7.0	0.0	3.0	8.0	3.0	0.0
2	2016-04-04 00:10:00 PDT	0.0	0.0	10.0	32.0	3.0	0.0	2.0	9.0	8.0	0.0
3	2016-04-04 00:00:00 PDT	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
4	2016-04-03 23:50:00 PDT	0.0	0.0	13.0	29.0	5.0	0.0	4.0	7.0	6.0	0.0
5	2016-04-03 23:40:00 PDT	0.0	0.0	17.0	25.0	5.0	0.0	10.0	5.0	2.0	0.0
6	2016-04-03 23:30:00 PDT	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
7	2016-04-03 23:20:00 PDT	0.0	0.0	13.0	29.0	5.0	0.0	4.0	6.0	7.0	0.0
8	2016-04-03 23:10:00 PDT	0.0	0.0	14.0	28.0	5.0	0.0	5.0	5.0	7.0	0.0
9	2016-04-03 23:00:00 PDT	0.0	0.0	18.0	22.0	7.0	0.0	8.0	1.0	6.0	0.0

10.6 DNS Traffic Resource Pool Availability Trend

Description	Provides the resource pool availability of DNS Traffic Control over time with trending
Overview	Tracks the availability status for DNS Traffic Control resources for the resource pool over time. Helps identify trends where limited or no availability of resources within a particular pool has impacted performance and shortens time to troubleshoot.
Data presented	• Availability % • Time • Traffic Control Resources

Sample report:

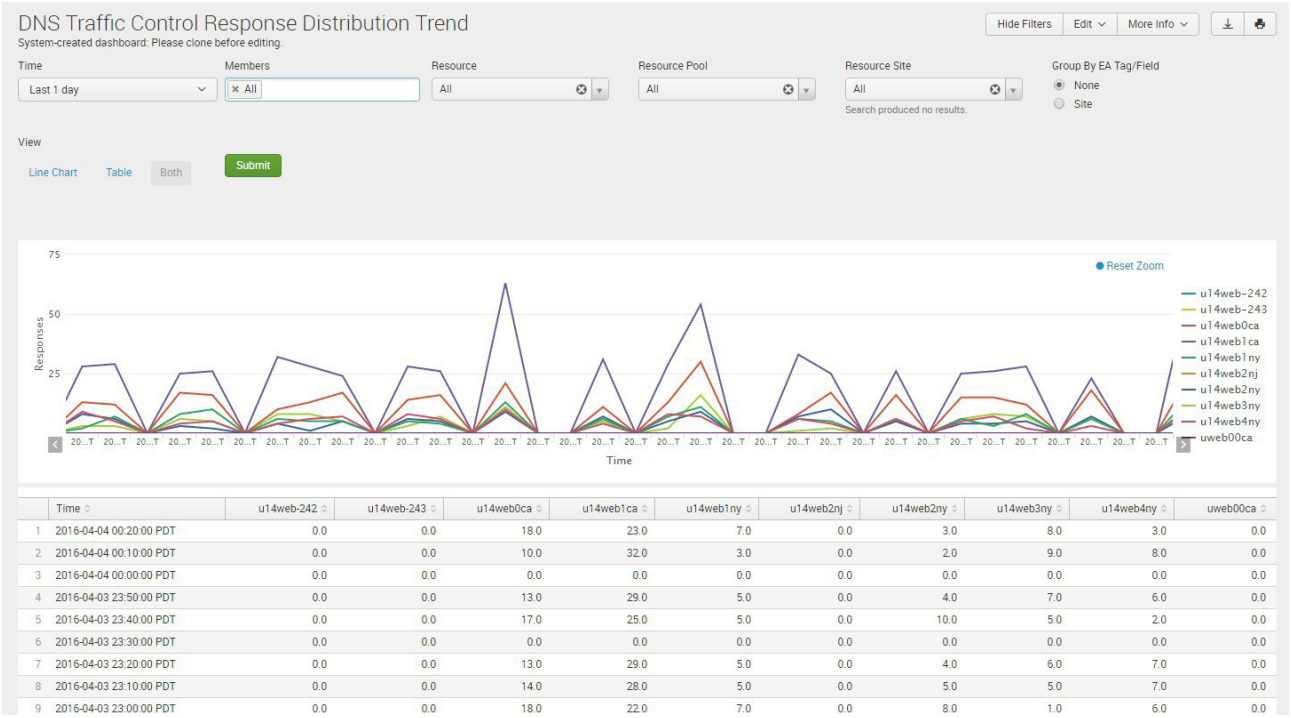


	Time	agowtham-pool
1	2016-01-29 00:00:00 PST	100.0
2	2016-01-28 00:00:00 PST	100.0
3	2016-01-27 00:00:00 PST	99.99
4	2016-01-26 00:00:00 PST	99.98
5	2016-01-25 00:00:00 PST	100.0
6	2016-01-24 00:00:00 PST	100.0
7	2016-01-23 00:00:00 PST	99.99
8	2016-01-22 00:00:00 PST	99.94

10.7 DNS Traffic Response Distribution Trend

Description	Tracks the responses of DNS Traffic Control over time with trending
Overview	Monitors the response distribution trends for DNS Traffic Control resources over time. Helps pinpoint of a trend of abnormal distribution has impacted performance.
Data presented	• Responses • Time • Traffic Control Resources

Sample report:

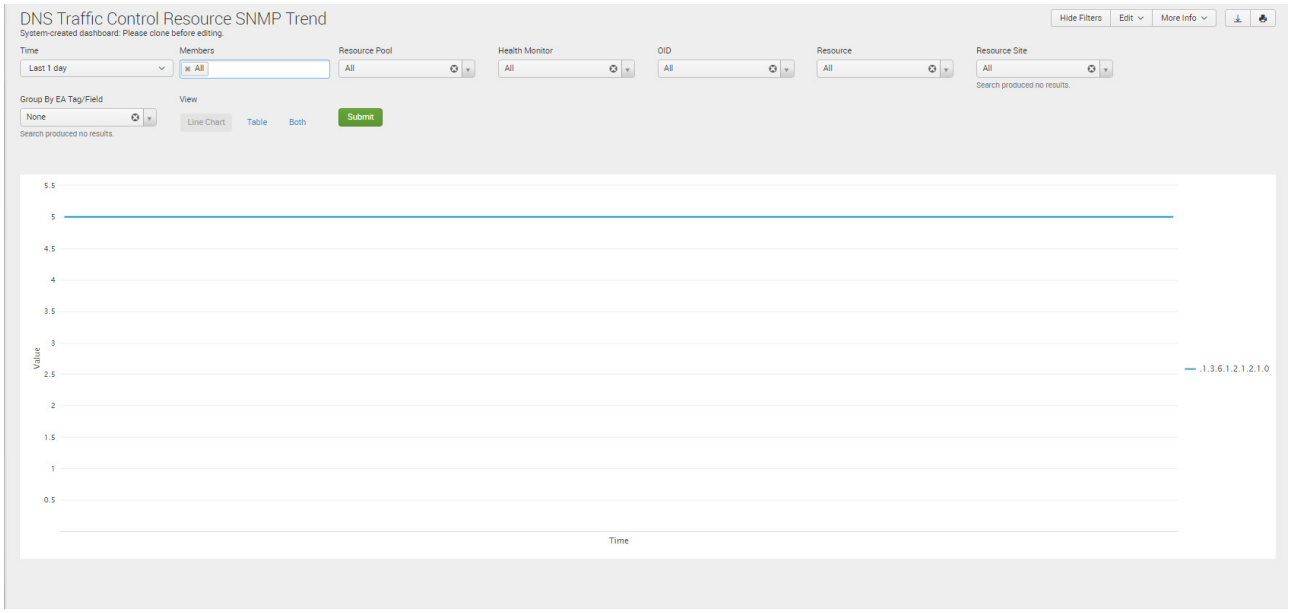


	Time	u14web-242	u14web-243	u14web0ca	u14web1ca	u14web1ny	u14web2nj	u14web2ny	u14web3ny	u14web4ny	uweb00ca
1	2016-04-04 00:20:00 PDT	0.0	0.0	18.0	23.0	7.0	0.0	3.0	8.0	3.0	0.0
2	2016-04-04 00:10:00 PDT	0.0	0.0	10.0	32.0	3.0	0.0	2.0	9.0	8.0	0.0
3	2016-04-04 00:00:00 PDT	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
4	2016-04-03 23:50:00 PDT	0.0	0.0	13.0	29.0	5.0	0.0	4.0	7.0	6.0	0.0
5	2016-04-03 23:40:00 PDT	0.0	0.0	17.0	25.0	5.0	0.0	10.0	5.0	2.0	0.0
6	2016-04-03 23:30:00 PDT	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0	0.0
7	2016-04-03 23:20:00 PDT	0.0	0.0	13.0	29.0	5.0	0.0	4.0	6.0	7.0	0.0
8	2016-04-03 23:10:00 PDT	0.0	0.0	14.0	28.0	5.0	0.0	5.0	5.0	7.0	0.0
9	2016-04-03 23:00:00 PDT	0.0	0.0	18.0	22.0	7.0	0.0	8.0	1.0	6.0	0.0

10.8 DNS Traffic Resource SNMP Trend

Description	Tracks SNMP resource information over time for DNS Traffic Control
Overview	Allows more granular view of SNMP data over time to better manage DNS Traffic Control across multiple appliances.
Data presented	• SNMP data over time

Sample report:

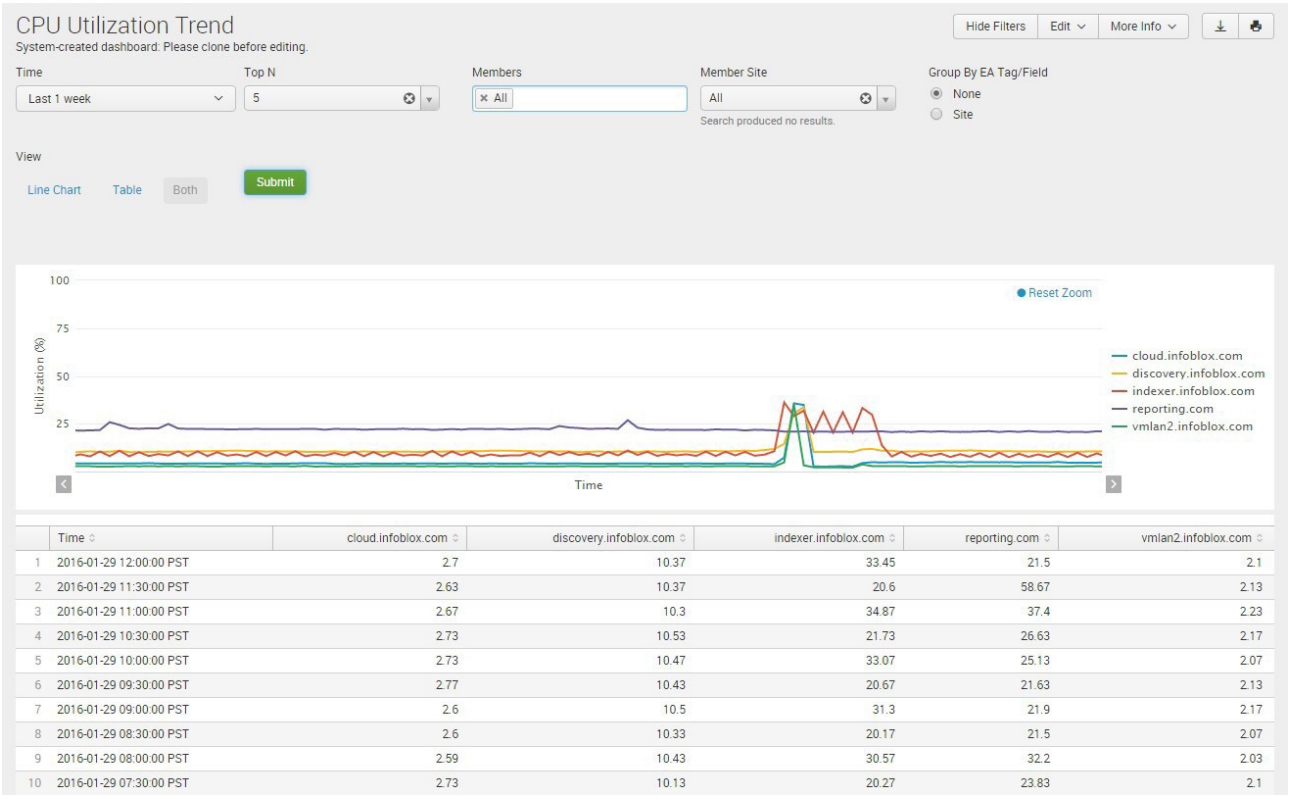


11 SYSTEM/APPLIANCE DASHBOARDS

11.1 CPU Utilization Trend

Description	CPU Utilization trend for a given appliance.
Overview	Provides CPU utilization by appliance over time. Helps pinpoint potential risk areas where additional resources may be required and assists with planning for future requirements by seeing trends over time.
Data presented	• CPU Utilization per Infoblox Member

Sample report:

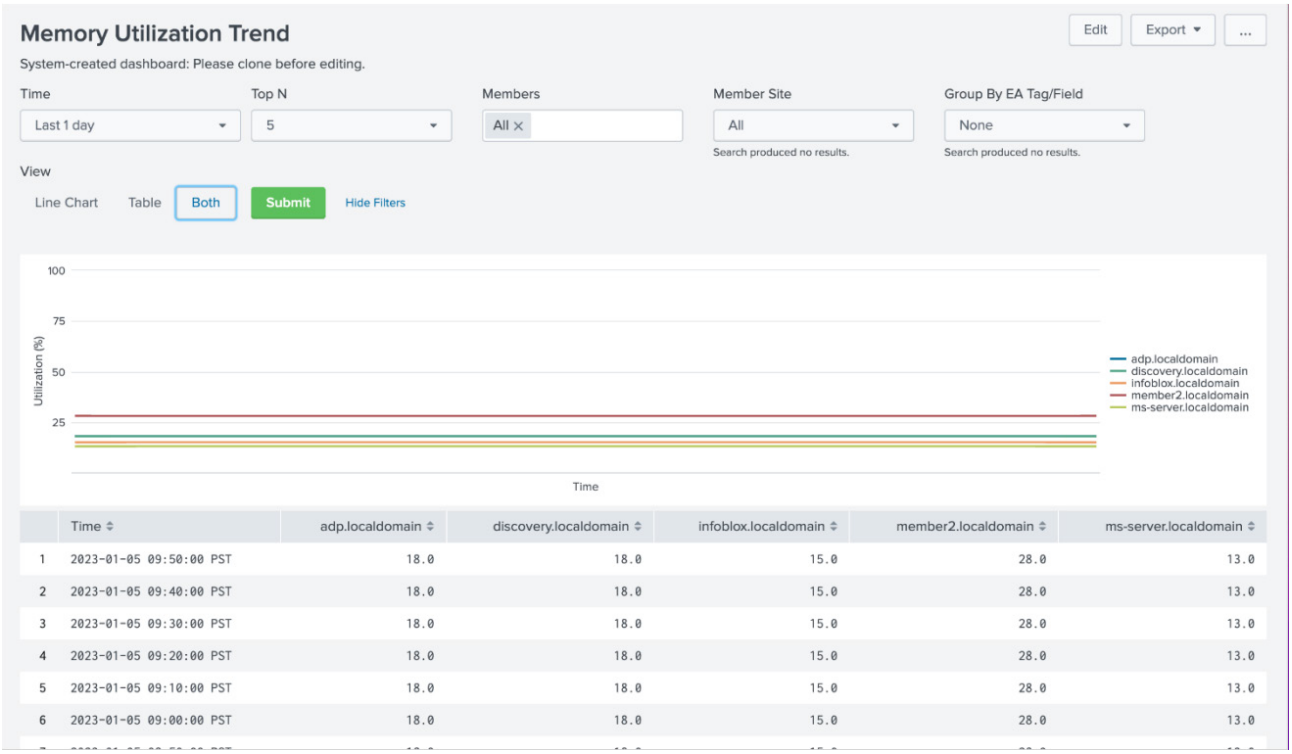


	Time	cloud.infoblox.com	discovery.infoblox.com	indexer.infoblox.com	reporting.com	vmlan2.infoblox.com
1	2016-01-29 12:00:00 PST	2.7	10.37	33.45	21.5	2.1
2	2016-01-29 11:30:00 PST	2.63	10.37	20.6	58.67	2.13
3	2016-01-29 11:00:00 PST	2.67	10.3	34.87	37.4	2.23
4	2016-01-29 10:30:00 PST	2.73	10.53	21.73	26.63	2.17
5	2016-01-29 10:00:00 PST	2.73	10.47	33.07	25.13	2.07
6	2016-01-29 09:30:00 PST	2.77	10.43	20.67	21.63	2.13
7	2016-01-29 09:00:00 PST	2.6	10.5	31.3	21.9	2.17
8	2016-01-29 08:30:00 PST	2.6	10.33	20.17	21.5	2.07
9	2016-01-29 08:00:00 PST	2.59	10.43	30.57	32.2	2.03
10	2016-01-29 07:30:00 PST	2.73	10.13	20.27	23.83	2.1

11.2 Memory Utilization Trend

Description	Memory Utilization trend for a given appliance.
Overview	Provides memory utilization by device over time. Helps pinpoint potential risk areas where additional resources may be required and assists with planning for future requirements by seeing trends over time.
Data presented	• Memory Utilization per Infoblox Member

Sample report:

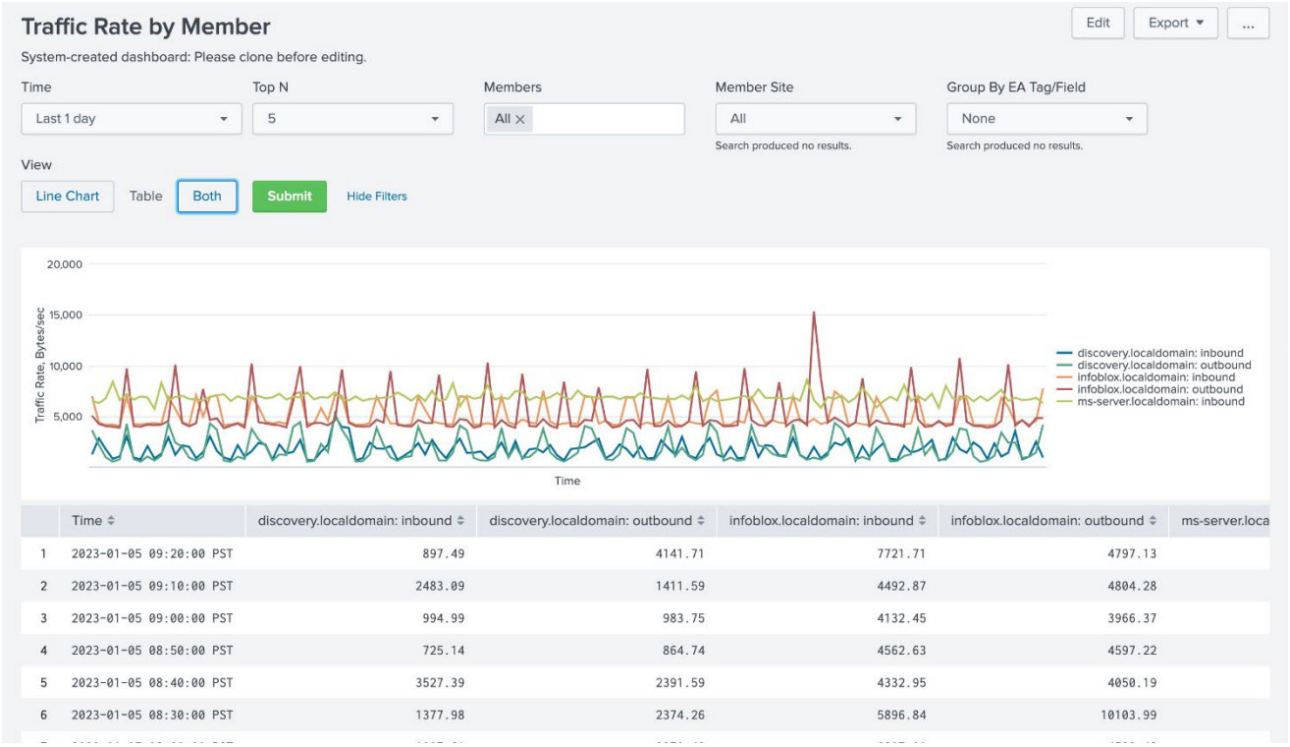


	Time	adp.localdomain	discovery.localdomain	infoblox.localdomain	member2.localdomain	ms-server.localdomain
1	2023-01-05 09:50:00 PST	18.0	18.0	15.0	28.0	13.0
2	2023-01-05 09:40:00 PST	18.0	18.0	15.0	28.0	13.0
3	2023-01-05 09:30:00 PST	18.0	18.0	15.0	28.0	13.0
4	2023-01-05 09:20:00 PST	18.0	18.0	15.0	28.0	13.0
5	2023-01-05 09:10:00 PST	18.0	18.0	15.0	28.0	13.0
6	2023-01-05 09:00:00 PST	18.0	18.0	15.0	28.0	13.0

11.3 Traffic Rate by Member

Description	Traffic rate associated with appliance service interface.
Overview	Shows traffic rate in and out of LAN port over time with selected appliances. Helps plan for current and future requirements with more detailed data.
Data presented	• Inbound traffic to all Interface (Bits / sec) • Outbound traffic to all Interface (Bits / sec)

Sample report:



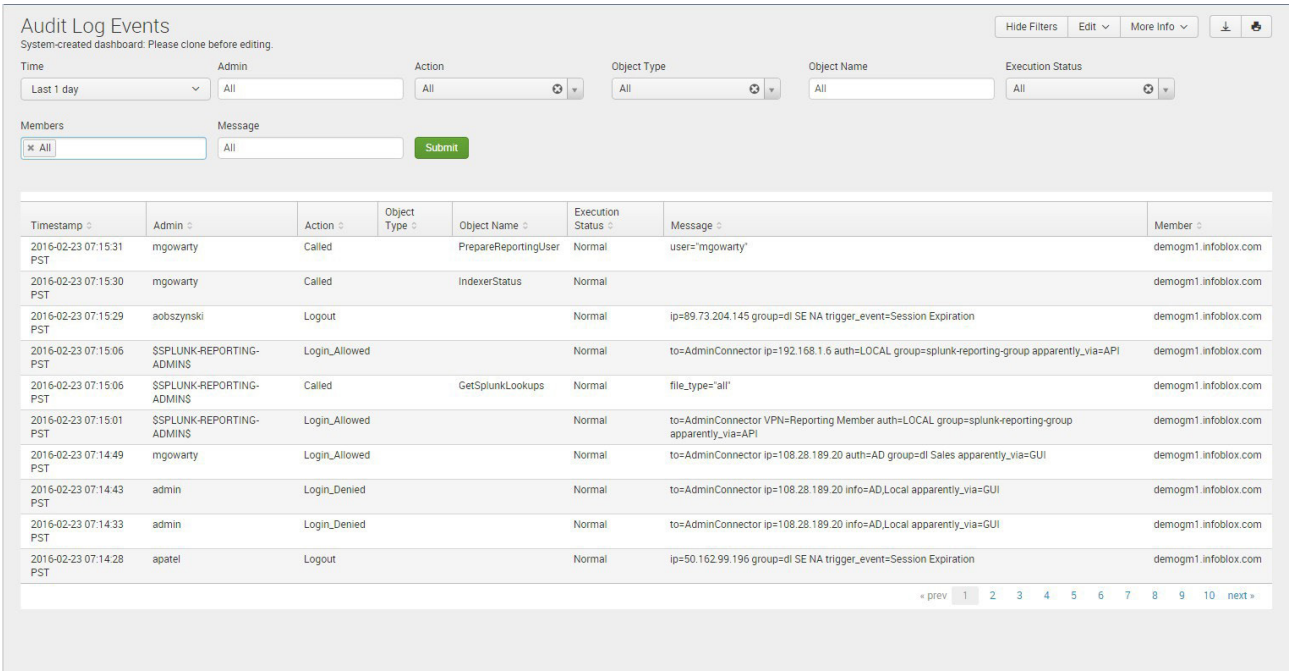
	Time	discovery.localdomain: inbound	discovery.localdomain: outbound	infoblox.localdomain: inbound	infoblox.localdomain: outbound	ms-server.loca
1	2023-01-05 09:20:00 PST	897.49	4141.71	7721.71	4797.13	
2	2023-01-05 09:10:00 PST	2483.09	1411.59	4492.87	4804.28	
3	2023-01-05 09:00:00 PST	994.99	983.75	4132.45	3966.37	
4	2023-01-05 08:50:00 PST	725.14	864.74	4562.63	4597.22	
5	2023-01-05 08:40:00 PST	3527.39	2391.59	4332.95	4050.19	
6	2023-01-05 08:30:00 PST	1377.98	2374.26	5896.84	10103.99	

12 AUDIT LOG DASHBOARD

12.1 Audit Log Events

Description	Tracks and document audits logs across the platform
Overview	Provides information about the administrator-initiated events such as login events, logout events, service restarts, appliance reboots, write operations such as the addition, modification, and deletion of objects, etc.
Data presented	• Timestamp • Admin • Action • Object Type • Object Name • Execution Status • Message • Members

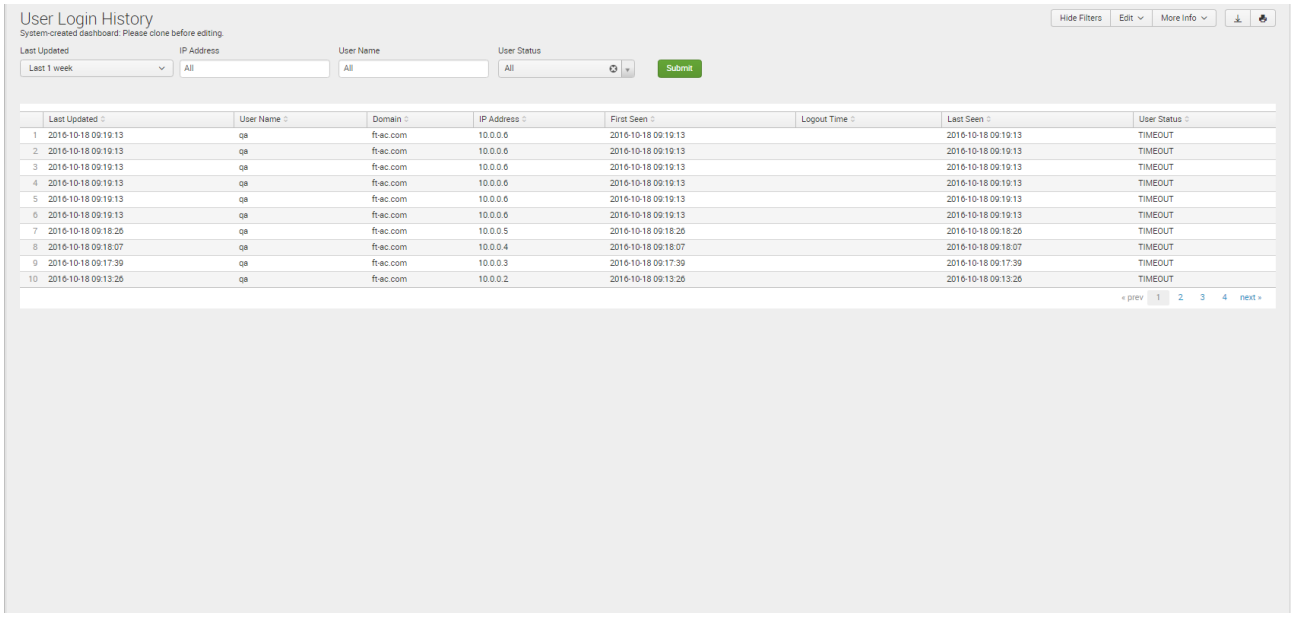
Sample report:



12.2 User Login History

Description	Tracks and documents user logins across the platform
Overview	Helps Infoblox administrators identify who logged into the platform at different points in time.
Data presented	• Timestamp • User name • Domain • IP address • First seen • Logout time • Last seen • User status

Sample report:

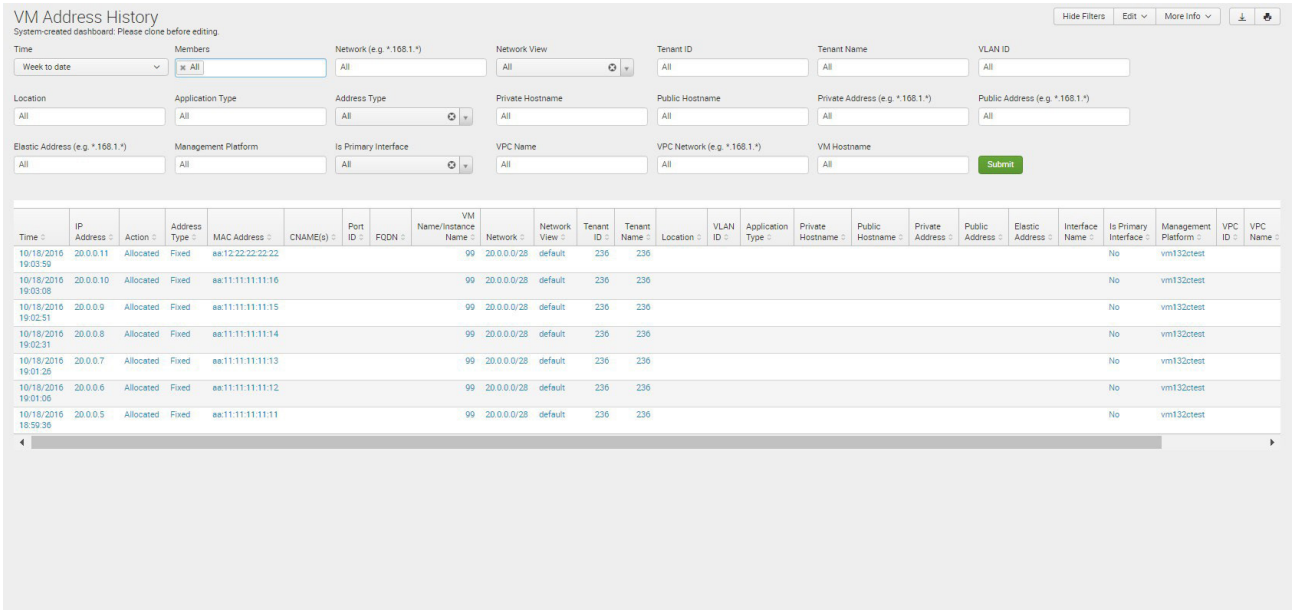


13 CLOUD DASHBOARD

13.1 VM Address History

Description	Tracks the history of IP addresses of VMs provisioned
Overview	Provides detailed views of current and historical IP addresses (and other parameters) of VMs provisioned and destroyed. Helps administrators troubleshoot virtual instances faster with accurate visibility and meets audit/compliance tracking needs.
Data presented	• Client IP • Total DNS Tunneling Events • Total Outbound Malicious Queries • Last Seen • Host Name • MAC/DUID • Lease State/Lease End • Top 3 RPZ Rules • Top 3 DNS Tunneling Events • Device Name • Port/Interface

Sample report:



13.2 License Pool Utilization

Description	Tracks the utilization of the dynamic licenses in a given time frame
Overview	Provides d the total number of dynamic licenses available, percentage of pooled license allocation over time and other related information for each license pool.
Data presented	• Period/Date • License Pool • Total License Count • Utilization %

Sample report: