

REPORT

Infoblox reporting and analytics

TABLE OF CONTENTS

1	INF	OBLOX REPORTING AND ANALYTICS OVERVIEW	5
2	но	ME DASHBOARDS AND PREDICTIVE REPORTS	6
	2.1	Home Dashboard	6
	2.2	System Capacity Prediction Trend	7
	2.3	System Capacity Predictive Trend	8
	2.4	IPAM Prediction Dashboard	9
3	DE\	VICES (DISCOVERY) DASHBOARDS	10
	3.1	Inactive IP Addresses	10
	3.2	Port Capacity Utilization by Device	11
	3.3	Port Capacity Trend	12
	3.4	Port Capacity Delta by Device	13
	3.5	Device Components	14
	3.6	Device Inventory	15
	3.7	Device Interface Inventory	16
	3.8	End Host History	17
	3.9	IP Address Inventory	18
	3.10	Network Inventory	19
4	DH	CP DASHBOARDS	20
	4.1	DHCP Lease History	20
	4.2	DHCP Message Rate Trend	21
	4.3	DHCP Top Lease Clients	22
	4.4	DHCPv4 Usage Trend	23
	4.5	DHCPv4 Usage Statistics	24
	4.6	DHCPv4 Range Utilization Trend	25
	4.7	DHCPv4 Top Utilized Networks	26

4.8	Top Device Classes	27
4.9	Device Class Trend	28
4.10	Device Trend	29
4.11	Top Devices Identified	30
4.12	Top Devices Denied an IP Address	31
4.13	Device Fingerprint Change Detected	32
DNS	S DASHBOARDS	33
5.1	DDNS Update Rate Trend	33
5.2	DNS Top Requested Domain Names	34
5.3	DNS Replies Trend	35
5.4	DNS Cache Hit Rate Trend	36
5.5	DNS Query Rate by Query Type	37
5.6	DNS Response Latency Trend	38
5.7	DNS Top Clients	39
5.8	DNS Query Rate By Member	40
5.9	DNS Daily Query Rate by Member	41
5.10	DNS Daily Peak Hour Query Rate by Member	42
5.11	DNS Statistics per Zone	43
5.12	DNS Statistics per DNS View	44
5.13	DNS Top Clients per Domain	45
5.14	DNS Top NXDOMAIN – NOERROR (no data)	46
5.15	DNS Top SERVFAIL Errors Sent/Received	47
5.16	DNS Top Timed-Out Recursive Queries	48
5.17	DNS Query Trend Per IP Block Group	49
5.18	DNS Domains Queried By Client*	50
5.19	DNS Domain Query Trend*	51
5.20	DNS Scavenged Object Count Trend	52
5.21	Top DNS Clients by Query Type*	53
5.22	Top DNS Clients Querying MX Records*	54
ECC	DSYSTEM DASHBOARDS	55
6.1	User Login History	55
6.2	Subscription Data	56
6.3	Publish Data	57
	 4.9 4.10 4.11 4.12 4.13 DNS 5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8 5.9 5.10 5.11 5.12 5.13 5.14 5.15 5.16 5.17 5.18 5.16 5.17 5.16 5.17 5.18 5.19 5.20 5.21 5.22 ECC 6.1 6.2 	 4.9 Device Class Trend 4.10 Device Trend 4.11 Top Devices Identified 4.12 Top Devices Denied an IP Address 4.13 Device Fingerprint Change Detected DEVENTION DINS Update Rate Trend 5. DNS Update Rate Trend 5. DNS Replies Trend 5. DNS Query Rate by Query Type 6. DNS Reponse Latency Trend 5. DNS Query Rate by Member 6. DNS Query Rate By Member 7. DNS Query Rate By Member 8. DNS Query Rate By Member 9. DNS Daily Query Rate by Member 9. DNS Daily Query Rate by Member 10. DNS Statistics per Zone 11 DNS Statistics per Zone 12 DNS Top Clients Der Domain 13 DNS Query Rate By Member 14 DNS Statistics per Zone 15 DNS Query Trend Per IP Block Group 16 DNS Top Timed-Out Recursive Queries 17 DNS Query Trend Per IP Block Group 18 DNS Domain Queried By Client* 19 DNS Clients by Query Trend 10 DNS Clients by Query Trend 11 DNS Scavenged Object Count Trend 12. Top DNS Clients by Query Trend* 13. DNS Clients by Query Trend* 14. User Legin History 15. Just Scavenged Dipet Count Trend 15. DNS Clients by Query Trend* 16. User Legin History 17. User Legin History 18. Suboription Data

7	INT	ERNAL DASHBOARDS	58
	7.1	Reporting Index Usage Statistics	58
	7.2	Reporting Volume Usage Trend Per Category	59
	7.3	Reporting Volume Usage Trend Per Member	60
	7.4	Reporting License Usage	61
8		ADDRESS MANAGERMENT DASHBOARDS	62
	8.1	IPAM v4 Network Usage Statistics	62
	8.2	IPAM v4 Network Usage Trend	63
	8.3	IPAM v4 Top Utilized Networks	64
	8.4	IPAM v4 Device Networks	65
9	SEC	CURITY (DNS) DASHBOARDS	66
	9.1	DNS Top RPZ Hits	66
	9.2	DNS Top RPZ Hits by Client	67
	9.3	FireEye Alerts Report	68
	9.4	Top DNS Firewall Hits	69
	9.5	Malicious Activity by Client	70
	9.6	Threat Protection Event Count by Time	71
	9.7	Threat Protection Event Count by Severity Trend	72
	9.8	Threat Protection Event Count by Rule	73
	9.9	Threat Protection Event Count by Member	74
	9.10	Threat Protection Event Count by Member Trend	75
	9.11	Threat Protection Event Count by Category	76
	9.12	Threat Protection Top Rules Logged by Source	77
	9.13	Threat Protection Top Rules Logged	78
	9.14	DNS Top Tunneling Activity	79
	9.15	DNS Tunneling Traffic by Category	80
	9.16	Top Malware and DNS Tunneling Events by Client	81
10	DN	S TRAFFIC CONTROLS DASHBOARDS	82
	10.1	DNS Traffic Control Resource Availability Status	82
	10.2	DNS Traffic Control Resource Availability Trend	83
	10.3	DNS Traffic Control Resource Pool Availability Status	84
	10.4	DNS Traffic Control Resource Pool Availability Trend	85
	10.5	DNS Traffic Control Response Distribution Trend	86
	10.6	DNS Traffic Resource Pool Availability Trend	87
	10.7	DNS Traffic Response Distribution Trend	88
	10.8	DNS Traffic Resource SNMP Trend	89

11	SYSTEM/APPLIANCE DASHBOARDS	90
	11.1 CPU Utilization Trend	90
	11.2 Memory Utilization Trend	91
	11.3 Traffic Rate by Member	92
12	AUDIT LOG DASHBOARD	93
	12.1 Audit Log Events	93
	12.2 User Login History	94
13	CLOUD DASHBOARD	95
	13.1 VM Address History	95
	13.2 License Pool Utilization	96

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



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:

Last 1 day ~	iction Trend fore ediling (id Member member.com (IB-VM-1410)	Model Type O v	CPU Utilization Threshold (e.g. 90 *) 80	DB Objects Threshold (e.g. 20000 *) 440000	QPS Threshold (e.g. 20000 *) 30000.0	LPS Threshold (e.g. 20000 *) 210.0	Hide Fitters Edit v More Inf Prediction Data ratio(e g. ratio 2 will display 2 times the current data.) Subwet 1 Q v	• ± •
CPU Threshold								
Max CPU Utilization		80		CPU Threshold	Prediction	WA		
CPU Trend Prediction				Time				- Actual - Prediction - Threshold
DB Objects Threshold								
Max DB Objects Utilization		N/A		DB Objects Th	eshold Prediction	N/A		۸
DB Objects Trend Prediction 100 10 10 10 10 10 10 10 10 10 10 10 10				No results found.				۸

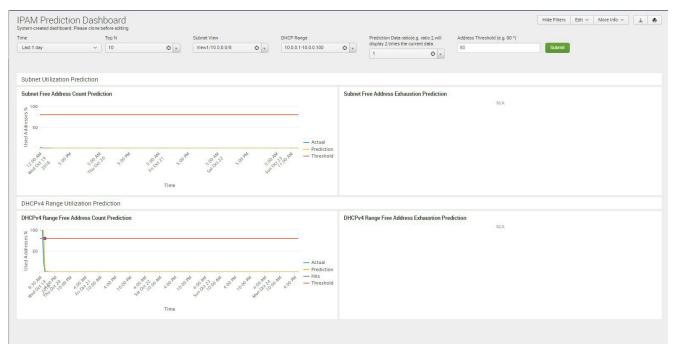
2.3 System Capacity Predictive Trend

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

System Capacity Prediction Trend System created distibuting Prese clone before atting Time Grid Member Model Type CPU Utilization Threshold (e.g. 50 *) Last 1 day v mem-repot com (B-800) v Solution Prediction Data ratiole grand 2 will splay 2 times the current data) 1 v v	Hide Filters Edit v More Info v Image: The Shold (e.g. 20000 *) LPS Threshold (e.g. 20000 *) Image: The Shold (e.g. 20000 *)<
CPU Threshold	
Max CPU Utilization	CPU Threshold Prediction
80	September 09 2016 15:00
CPU Trend Prediction	e Amat - Amat - Prediction - Hits - Threshold
DB Objects Threshold	
Mex DB Objects Utilization IB-800:33,000	DB Objects Threshold Prediction

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



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

me			Network View	v	Device Name				
Las	: 32 days	~	All	© •	All	Submit			
	IP 0	Last MA	AC/DUID 0	Type 0		Device Name 🗸	Device Type 0	Port / Interface 0	Network View 0
1	172.16.10.4			Host/Discovery		swr-c-04	Router		Company 1
2	172.16.50.1	00:1b:54	4:92:b6:c0	Host/Discovery		swr-c-02.infoblox.com	Router		Company 1
3	10.0.0.1	00:00:00	0:00:00:00	Fixed Address/A R	ecord/Discovery	juniper_srx			Company 1
4	192.168.1.15	00:50:56	6:9c:7c:cb	Host/Discovery		f5gtm1.infoblox.com	Load Balancer		Company 1
5	192.168.1.10	00:50:56	6:ba:43:63	Host/A Record/PT	R Record/Discovery	demogm1	VNIOS		Company 1
6	10.66.20.129	c2:05:06	5:05 <mark>:00:0</mark> 0	Host/Discovery		branch2	Switch-Router		Company 1
7	192.168.1.190	ca:04:08	8:09:00:08	Fixed Address		VRF-Router	Router		Company 1
8	10.0.17.1	00:0f:23	8:88:0a:c5	Host/Discovery		SWR-C-05			Company 1
9	10.197.7.2	00:1a:a2	2:af:9e:08	Host/Discovery		R-C-01			Company 1
10	172.16.10.6			Host/Discovery		R-C-01	Router		Company 1

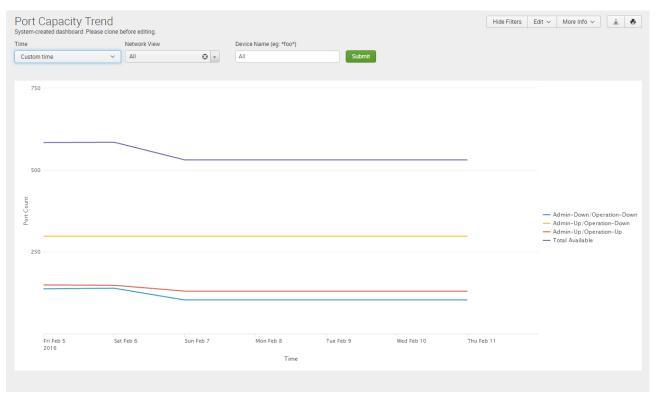
3.2 Port Capacity Utilization by Device

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

	Network View	Device Name	2			
istom time 🗸 🗸	All	B v All	Submit			
Device Name 0	Admin-Up/Op	eration-Up 0	Admin-Down/Operation-Down 0	Admin-Up/Operation-Down 0	Total Available 0	Network View 0
Campus1		2	2	0	4	Company 1
Campus2		2	2	0	4	Company 1
F5demo2.infoblox.com		5	0	0	5	Company 1
R-C-01		1	0	2	3	Company 1
bld1.infoblox.com		8	2	8	18	Company 1
bld2.infoblox.com		8	2	8	18	Company 1
branch2		1	2	0	3	Company 1
branch3		1	1	0	2	Company 1
branch5		1	1	0	2	Company 1
branch54		1	1	0	2	Company 1

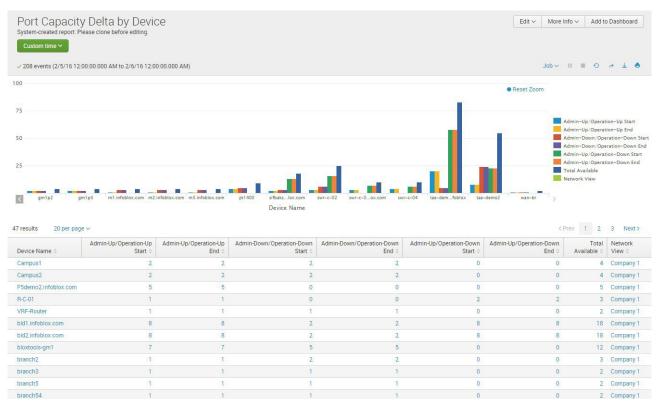
3.3 Port Capacity Trend

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



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



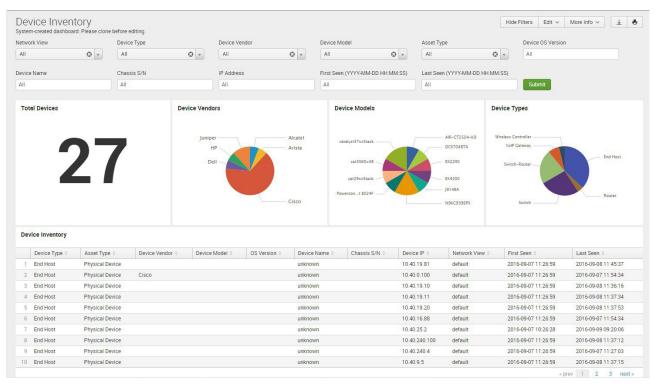
3.5 Device Components

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

etwo	rk View		Device Vendor		Device Model			Class Dev			Device Vers	Device Version				Device Name						
All		© ×	All	• •	All	0	-	All		<u>ب</u>	All				All							
evice	IP Address		S/N																			
AII			All		Submit																	
Dev	ice Compoi	nents																				
	Device IP 0	Network View	Device Name 0		Device Model 0	Device Vendor 0	OS Vers	sion o	Name 0	Description 0		Class 0	S/N 0	Model 0	Hardwa Rev 0	re	Firmware Rev 0		oftware ev 0			
1	10.40.16.8	default	AugustaLab-Arista-DCS- 7048T.inca.infoblox.com		DCS7048TA	Arista	4.9.0	6		Power Supply Fan C	ower Supply Fan Container											
2	10.40.16.8	default	AugustaLab-Arista-DCS- 7048T.inca.infoblox.com		DCS7048TA	Arista	4.9.6	6		Power Supply Sensor Container		container										
3	10.40.16.8	default	AugustaLab-Arista-DCS- 7048T.inca.infoblox.com		DCS7048TA	Arista	4.9.6	6		Power Supply Slot C	Power Supply Slot Container											
4	10.40.16.8	default	AugustaLab-Arista-DCS- 7048T.inca.infoblox.com		DCS7048TA	Arista	4.9.0	6		Fan Tray Slot Conta	ner	container										
5	10.40.16.8	default	AugustaLab-Arista-DCS- 7048T.inca.infoblox.com		DCS7048TA	Arista	4.9.6	6		Xcvr Slot Container		container										
6	10.40.16.8	default	AugustaLab-Arista-DCS- 7048T.inca.infoblox.com		DCS7048TA	Arista	4.9.6	6		Port Container		container										
7	10.40.16.8	default	AugustaLab-Arista-DCS- 7048T.inca.infoblox.com		DCS7048TA	Arista	4.9.0	6		Sensor Container		container										
8	10.40.16.8	default	AugustaLab-Arista-DCS- 7048T.inca.infoblox.com		DCS7048TA	Arista	4.9.6	6		Chip Container	Chip Container											
9	10.40.16.8	default	AugustaLab-Arista-DCS- 7048T.inca.infoblox.com		DCS7048TA	Arista	4.9.6	6		PowerSupply2 Fan		fan										
10	10.40.16.8	default	AugustaLab-Arista-DCS- 7048T.inca.infoblox.com		DCS7048TA	Arista	4.9.0	6		PowerSupply2 outpo sensor	it voltage	sensor										

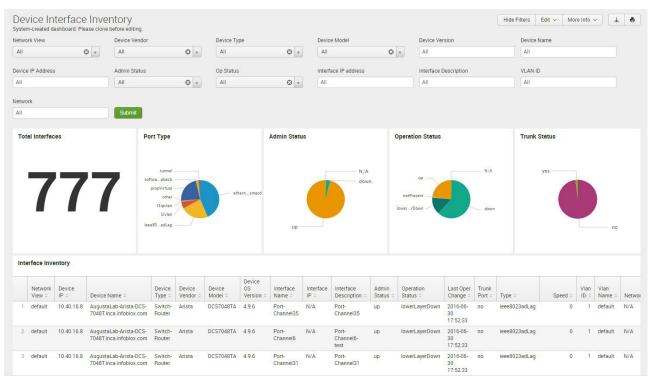
3.6 Device Inventory

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



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



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 Vendor Device Model Device OS Version Device IP Address Device Interface Device VLAN AP Name AP IP Address SSID

	d Host Hist		fore editing.										Ŧ	-			
ime			Network View		MAC Add	Iress	IP Addres	s		First Seen (YYYY- <mark>MM-DD H</mark>	Last Seen	MM:SS)					
La	st 1 day	~]	All	© -	All		All			All		All					
Su	bmit																
			1		Network		Device		Device C	S Device IP	Device	0.	rice AF		APIP		
	MAC Address 0	IP Address 0	First Seen 0	Last Seen 0	View 0	Device Name 0	Vendor 0	Device Model 0	Version		Interface			ime 0	Address 0	s	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)S	E8 10.40.239.254	Gi0/46	4	050				
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)S	E8 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)E	2 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)S	E8 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)S	E8 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)S	E8 10.40.239.254	Gi0/47	4	040				
7	C4:2C:03:2D:0E:95	10.40.19.81	2016-09-07	2016-09-08	default	disco-lab- 02.inca.infoblox.com	Cisco	cat3560x48	15.0(2)S	E8 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:

100% ▼ -/-sec @ 28.8 Khns ▼ 138K/- PNG-24 ▼

Time	e			Networ	k View	Address		Netmask			Management Platform						
Al	ll tim	ie	~	All	© ,	All		All				Ø v		© ,			
/lan	Nan	ne		Vlan ID		First Seen after (YYYY-MM-DD		Last Seen before (YYY	Y-MM-DD								
All			⊙ _▼	All	© ,	HH:MM:SS)		HH:MM:SS)		Submit	omit						
	Ian Name Ali Address Address				All		All		_								
	4	Address 0	Ne	etmask 0	First Seen 0	Last Seen 0	Net	work View 0	Utilization	n % 🌣	Managed 0	Managemer	nt Platform 0	Vlan Name	0	v	/lan IC
1	1 9	93.29.56.1	32			def	ault	100		True			VLAN3000			30	
2	2 5	56.125.36.0	30				RED		100		True			global			
3	3 5	58.125.36.0	30 30				GREEN				True			VLAN0823			8
4	4 5	58.125.35.0	30 30				GREEN				50.0 True			VLAN0821			8
5	5 1	97.23.56.0		24	2017-02-20 11:14:42	2017-03-13 07:38:30	GRI	EEN		0.3	True	Network Ins	ight	CE2-1			1
6	5 1	72.22.80.7		32			MG	MT	1	100.0	True			default			
7	7 1	94.24.56.0		24	2017-02-20 11:22:29	2017-02-20 12:06:55	GRI	EEN		0.3	True			default			
8	8 2	2.5.10.0		24	2017-02-20 11:23:09	2017-03-13 07:38:58	defa	ault		0.0	False	Network Ins	ight				
9	2	2.5.40.0		24	2017-02-20 11:01:30	2017-03-13 07:42:48	defa	ault		0.0	False	Network Ins	ight				
) 2	2.5.50.0		24	2017-02-20 11:15:51	2017-03-13 07:39:14	def	ault		0.0	False	Network Ins	ight				

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

me		Networ	k View	Address		Netmask	Ma	nagement Platform		Managed				
All time	~	All	© ,	All		All	A	JI	© •	All		© •		
an Name		Vlan ID		First Seen after (YYYY-MM-DD		Last Seen before (YYYY-MM-DD								
All	© .	All	© ,	HH:MM:SS)		HH:MM:SS)		Submit						
				All		All		_						
Address 0	Ne	etmask :	First Seen 0	Last Seen 0	Netw	ork View ≎ Ut	ilization %	○ Managed ○	Manageme	nt Platform ः		Vlan Nam	ne o	Vlan ID
1 93.29.56.1		32			defau	lt	100.0	0 True				VLAN300	0	300
2 56.125.36.0		30			RED		100.0	0 True				global		90
3 58.125.36.0		30			GREE	N	50.0	0 True				VLAN082	3	82
4 58.125.35.0		30			GREE	N	50.0	0 True				VLAN082	1	82
5 197.23.56.0		24	2017-02-20 11:14:42	2017-03-13 07:38:30	GREE	N	0.3	3 True	Network Ins	sight		CE2-1		10
6 172.22.80.7		32			MGM	r	100.0	0 True				default		
7 194.24.56.0		24	2017-02-20 11:22:29	2017-02-20 12:06:55	GREE	N	0.3	3 True				default		
8 2.5.10.0		24	2017-02-20 11:23:09	2017-03-13 07:38:58	defau	lt	0.0	0 False	Network Ins	sight				
9 2.5.40.0		24	2017-02-20 11:01:30	2017-03-13 07:42:48	defau	lt	0.0	0 False	Network Ins	sight				
10 2.5.50.0		24	2017-02-20 11:15:51	2017-03-13 07:39:14	defau	lt	0.0	0 False	Network Ins	sight				
									×	prev 1	2 3	4 5 6	7 8 9) 10 next »

4 DHCP DASHBOARDS

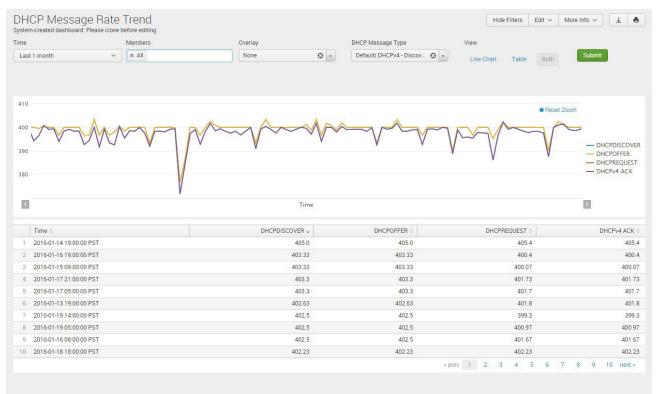
4.1 DHCP Lease History

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

Fime		Members		M	ember IP		Lease IP		Protocol				
Last 1 week ~					AII.		All	All Lease Start (YYYY-MM-DD HH:MM:SS)		Both O v			
					AC or DUID		Lease Start (Y)						
All	© .	All			AII.		All		All				
ingerprint		Device Class											
All	© .	All	6		Submit								
Time 0	Member 4		Member IP 0	Protocol ©	Action 0	Lease IP 0	MAC/DUID 0	Host Name 0	Lease Start ©	Lease End ©	Fingerprint		
Time 0	Member 4		Member IP 0	Protocol ©	Action 1	Lease IP 0	MAC/DUID ::	Host Name 0	Lease Start ::	Lease End 0	Fingerprint		
					Action			rioot itanic v	Leade blant v				
01/25/2016 05:56:45	master.inf	oblox.com		IPV4	Freed	3.2.17.84	2f:47:28:49:58:43		2016-01-25 05:51:45	2016-01-25 05:56:45	No Match		
01/25/2016 05:56:45 01/25/2016 05:56:45										2016-01-25 05:56:45 2016-01-25 05:56:45			
	master.inf	oblox.com		IPV4	Freed	3.2.17.84	2f:47:28:49:58:43		2016-01-25 05:51:45		No Match		
01/25/2016 05:56:45	master.inf master.inf	oblox.com oblox.com		IPV4 IPV4	Freed Freed	3.2.17.84 3.2.17.85	2f:47:28:49:58:43 e7:66:f9:36:84:fc		2016-01-25 05:51:45 2016-01-25 05:51:45	2016-01-25 05:56:45	No Match No Match		
01/25/2016 05:56:45 01/25/2016 05:56:45	master.inf master.inf master.inf	oblox.com oblox.com oblox.com		IPV4 IPV4 IPV4	Freed Freed Freed	3.2.17.84 3.2.17.85 3.2.17.88	2f:47:28:49:58:43 e7:66:f9:36:84:fc 30:62:53:13:fb:4b		2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45	2016-01-25 05:56:45 2016-01-25 05:56:45	No Match No Match No Match		
01/25/2016 05:56:45 01/25/2016 05:56:45 01/25/2016 05:56:45	master.inf master.inf master.inf master.inf	oblox.com oblox.com oblox.com oblox.com		IPV4 IPV4 IPV4 IPV4	Freed Freed Freed Freed	3.2.17.84 3.2.17.85 3.2.17.88 3.2.17.86	2f:47:28:49:58:43 e7:66:f9:36:84:fc 30:62:53:13:fb:4b fb:40:b1:39:59:ba		2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45	2016-01-25 05:56:45 2016-01-25 05:56:45 2016-01-25 05:56:45	No Match No Match No Match No Match		
01/25/2016 05:56:45 01/25/2016 05:56:45 01/25/2016 05:56:45 01/25/2016 05:56:45	master.inf master.inf master.inf master.inf	oblox.com oblox.com oblox.com oblox.com oblox.com		IPV4 IPV4 IPV4 IPV4 IPV4 IPV4	Freed Freed Freed Freed Freed	3.2.17.84 3.2.17.85 3.2.17.88 3.2.17.86 3.2.17.86 3.2.17.87	2f:47:28:49:58:43 e7:66:f9:36:84:fc 30:62:53:13:fb:4b fb:40:b1:39:59:ba ec:71:6f:34:00:28		2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45	2016-01-25 05:56:45 2016-01-25 05:56:45 2016-01-25 05:56:45 2016-01-25 05:56:45	No Match No Match No Match No Match No Match		
01/25/2016 05:56:45 01/25/2016 05:56:45 01/25/2016 05:56:45 01/25/2016 05:56:45 01/25/2016 05:51:45	master.inf master.inf master.inf master.inf master.inf	oblox.com oblox.com oblox.com oblox.com oblox.com oblox.com		IPV4 IPV4 IPV4 IPV4 IPV4 IPV4 IPV4	Freed Freed Freed Freed Freed Issued	3.2.17.84 3.2.17.85 3.2.17.88 3.2.17.86 3.2.17.86 3.2.17.87 3.2.17.84	2f.47:28:49:58:43 e7:66:f9:36:84:fc 30:62:53:13:fb:4b fb:40:b1:39:59:ba ec:71:6f:34:00:28 2f:47:28:49:58:43		2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45	2016-01-25 05:56:45 2016-01-25 05:56:45 2016-01-25 05:56:45 2016-01-25 05:56:45 2016-01-25 05:56:45	No Match No Match No Match No Match No Match No Match		
01/25/2016 05:56:45 01/25/2016 05:56:45 01/25/2016 05:56:45 01/25/2016 05:56:45 01/25/2016 05:51:45 01/25/2016 05:51:45	master.inf master.inf master.inf master.inf master.inf master.inf	oblox.com oblox.com oblox.com oblox.com oblox.com oblox.com oblox.com		IPV4 IPV4 IPV4 IPV4 IPV4 IPV4 IPV4 IPV4	Freed Freed Freed Freed Freed Issued Issued	3.2.17.84 3.2.17.85 3.2.17.88 3.2.17.86 3.2.17.86 3.2.17.87 3.2.17.84 3.2.17.85	2f:47:28:49:58:43 e7:66:19:36:84:fc 30:62:53:13:fb:4b fb:40:b1:39:59:ba ec:71:6f:34:00:28 2f:47:28:49:58:43 e7:66:19:36:84:fc		2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45 2016-01-25 05:51:45	2016-01-25 05 56:45 2016-01-25 05 56:45 2016-01-25 05 56:45 2016-01-25 05 56:45 2016-01-25 05 56:45 2016-01-25 05 56:45	No Match No Match No Match No Match No Match No Match		

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



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

ne	Top N	Members	Report On	Fingerprint	
Last 1 day	~ 20	🕲 👻 🕅 🗶	All	All	© -
vice Class					
NI ©	✓ Submit				
MAC/DUID 0		Issued 0	Renewed 0	Freed 0	MAC/DUID Tota
1 19:42:68:44:2c:4a		2	0	2	
2 30:8f:fc:37:50:26		2	0	2	
3 49:b0:d4:38:82:df		2	0	2	
4 5e:aa:00:04:74:92		2	0	2	
5 79:d2:6e:0f:42:05		2	0	2	
6 a5:30:44:0e:2d:e3		2	0	2	
		2	0	2	
7 b0:85:b6:5b:01:06		2	0	2	
7 b0:85:b6:5b:01:06 8 cf:21:c3:3f:37:0b 9 e1:15:dc:25:dc:22		2	0	2	

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

stem-created dashboard: Please clone I	-						
ne	Members	Microsoft Servers		DHCP Range (eg: *10.120.20.2*)	Network (eg: *.168.1.*)		
.ast 1 month V	× All	All Search produced no res	© .	All	All		
w ine Chart Table Both	Submit						
600,000						• Reset Zoom	
Count							
200,000	16:00:00 PST	2016-01-08 20:00:00 PST	Time	2016-01-09 00:00:00 PST	2016-01-09 (04:00:00 PST	
200,000	16:00:00 PST	2016-01-08 20:00:00 PST	Time	2016-01-09 00:00:00 PST Dynamic v	2016-01-09 (Static 0	04:00:00 PST	- Static - Free
200,000	16:00:00 PST	2016-01-08 20:00:00 PST	Time			04:00:00 PST	- Static - Free
200,000 2016-01-08 Time 0 2016-01-18 08:00:00 PST	16:00:00 PST	2016-01-08 20:00:00 PST	Time	Dynamic 🗸	Static 0	04:00:00 PST	Static Free Free 72442
200,000 2016-01-08 Time 0 2016-01-18 08:00:00 PST 2016-01-16 20:00:00 PST	16:00:00 PST	2016-01-08 20:00:00 PST	Time	Dynamic 🗸 1018.5	Static 0 0.0	04:00:00 PST	Static Free 72442 724428
200,000 2016-01-08 Time 0 2016-01-18 08:00:00 PST 2016-01-16 20:00:00 PST 2016-01-14 12:00:00 PST	16:00:00 PST	2016-01-08 20:00:00 PST	Time	Dynamic 🗸 1018.5 1018.25	Static 0 0.0 0.0	04:00:00 PST	 Static Free Free 724428 724428 724428
200,000 2016-01-08 2016-01-18 08:00:00 PST 2016-01-16 08:00:00 PST 3 2016-01-14 12:00:00 PST 4 2016-01-14 08:00:00 PST	16:00:00 PST	2016-01-08 20:00:00 PST	Time	Dynamic - 1018.5 1018.25 1014.25	Static 0 0.0 0.0 0.0	04:00:00 PST	 Static Free Free 72442 724422 724432 724432 724432
200,000 2016-01-08 2016-01-18 08:00:00 PST 2016-01-16 20:00:00 PST 2016-01-14 12:00:00 PST 4 2016-01-14 08:00:00 PST 5 2016-01-15 12:00:00 PST	16:00:00 PST	2016-01-08 20:00:00 PST	Time	Dynamic - 1018.5 1018.25 1014.25 1014.25	Static 0 0.0 0.0 0.0 0.0	04:00:00 PST	 Static Free 72442 724432 724432 724439
200,000 2016-01-08 2016-01-18 08:00:00 PST 2016-01-16 08:00:00 PST 2016-01-14 08:00:00 PST 3016-01-14 08:00:00 PST 4016-01-14 08:00:00 PST 5016-01-15 12:00:00 PST 5016-01-18 04:00:00 PST	16:00:00 PST	2016-01-08 20:00:00 PST	Time	Dynamic - 1018.5 1018.25 1014.25 1012.5 1007.75	Static 0 0.0 0.0 0.0 0.0 0.0	04:00:00 PST	 Static Free Free 72442 724432 724439 7244439
200,000 2016-01-08 2016-01-18 2016-01-18 2016-01-18 2016-01-14 2000 2016-01-14 2000 2015 2016-01-14 2000 2015 2016-01-18 2010 2015 2016-01-18 2015	16:00:00 PST	2016-01-08 20:00:00 PST	Time	Dynamic - 1018.5 1018.25 1014.25 1012.5 1007.75 1006.5	Static 0 0.0 0.0 0.0 0.0 0.0 0.0 0.0	04:00:00 PST	 Static Free Free 72442 724432 724432 724439 724443 724444 724444
200,000 2016-01-08 I 2016-01-1808:00:00 PST 2 2016-01-18:08:00:00 PST 2 2016-01-16:20:00:00 PST 3 2016-01-14:12:00:00 PST 4 2016-01-14:12:00:00 PST 5 2016-01-15:12:00:00 PST 6 2016-01-18:04:00:00 PST 7 2016-01-18:00:00 0PST	16:00:00 PST	2016-01-08 20:00:00 PST	Time	Dynamic - 1018.5 1018.25 1014.25 1012.5 1007.75 1006.5 1004.0	Static 0 0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0	04:00:00 PST	

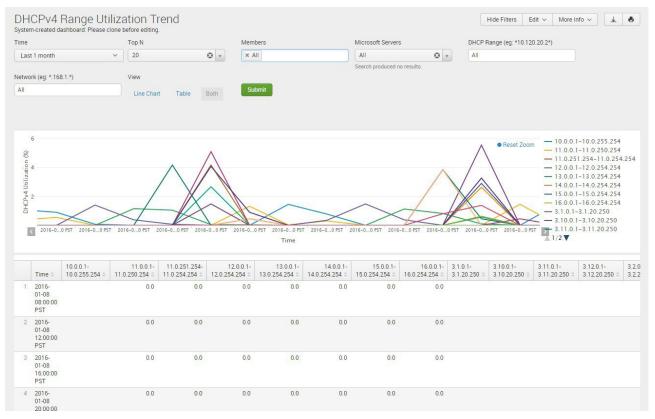
4.5 DHCPv4 Usage Statistics

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

		Members		Microsoft	Servers	Network View		Network (eg: *.168.1.)	*)		
Las	t 1 day	× All		All	• •	All	⊙ v	All			
ddre	dress (eg: *.168.1.*) CIDR (eg: =16,		=16)	Search produced no results. Utilization % (eg: >10)		Active Directory Site	Active Directory Site				
All		>=1		>=0		× All		Submit			
											-
	Timestamp 0	Network view 0	Network 0	CIDR 0	AD Site 0	DHCPv4 Utilization % 0	Ranges 0	Provisioned 0	Used 0	Static 0	Dynamic
1	2016-01-29 00:58:00	netview1	10.0.0.0	8	(no_value)	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	
	2016-01-29 01:57:57	netview1	10.0.0.0	8	(no_value)	0.0	0	0	0	0	
3		default	10.0.0.0	8	(no_value)	0.0	0	0	0	0	
3	2016-01-29 01:57:57				(no_value)	0.0	0	0	0	0	
	2016-01-29 01:57:57 2016-01-29 10:58:00	netview1	10.0.0.0	8	(0	
4		netview1 default	10.0.0.0	8		0.0	0	0	0	0	
4	2016-01-29 10:58:00					0.0	0	0	0	0	
4	2016-01-29 10:58:00 2016-01-29 10:58:00	default	10.0.0.0	8	(no_value)						
4 5 6 7	2016-01-29 10:58:00 2016-01-29 10:58:00 2016-01-29 11:57:59	default netview1	10.0.0.0 10.0.0	8	(no_value) (no_value)	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



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

ime		Top N		Members	Microso	oft Servers					
Las	t 1 month	✓ 10	• •	× All	All		😮 👻 Subn	nit			
					Populatio	ng		_			
	Timestamp 0	Network View 0	Network 0	CIDR 0	DHCPv4 Utilization % ^	Ranges 0	Provisioned 0	Dynamic 0	Static 0	Free 0	Used
1	2016-01-29 18:57:59	default	3.50.0.0	16	0.0	1	5370	0	0	5370	
2	2016-01-29 18:57:59	default	3.49.0.0	16	0.0	1	5370	0	0	5370	
3	2016-01-29 18:57:59	default	3.48.0.0	16	0.0	1	5370	0	0	5370	
4	2016-01-29 18:57:59	default	3.47.0.0	16	0.0	1	5370	0	0	5370	
5	2016-01-29 18:57:59	default	3.46.0.0	16	0.0	1	5370	0	0	5370	
6	2016-01-29 18:57:59	default	3.45.0.0	16	0.0	1	5370	0	0	5370	
7	2016-01-29 18:57:59	default	3.44.0.0	16	0.0	1	5370	0	0	5370	
8	2016-01-29 18:57:59	default	3.43.0.0	16	0.0	1	5370	0	0	5370	
9	2016-01-29 18:57:59	default	3.42.0.0	16	0.0	1	5370	0	0	5370	
10	2016-01-29 18:57:59	default	3.41.0.0	16	0.0	1	5370	0	0	5370	

4.8 Top Device Classes

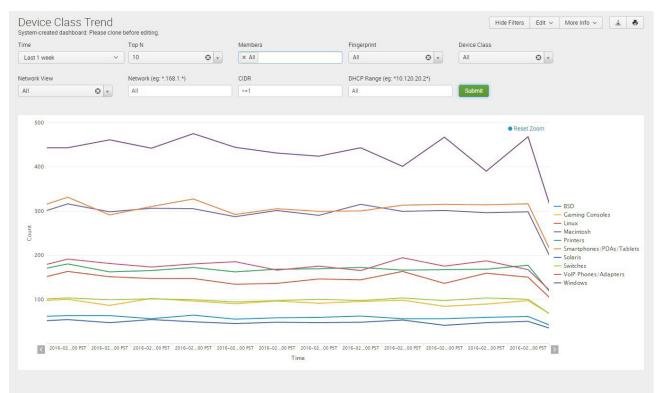
Description	Top Device Classes
Overview	Identifies and highlights the top device operating systems broken down by classes that receive DHCP leases. Helps identify which manufacturers and operating systems are being used so IT can identify non-supported devices or plan for future requirements.
Data presented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

Sample report:

	Device Classes	before editing.					Hide Filt	ters Edit ~	More Info 🗸	7
Time		Top N		Members	Fingerprint		Device Class			
Las	t 1 day 🗸 🗸 🗸	10	Θv	× All	All	• •	All	• •		
Netwo	ork View	Network (eg: *.16	8.1.*)	CIDR (eg: >=16)	DHCP Range (eg:	*10.120.20.2*)				
All	© .	All		>=1	All		Submit			
	Device 0					Total 0			% of	f all devices 0
1	Windows					2500				22.61
2	Smartphones/PDAs/Tablets					1785				16.15
3	Macintosh					1719				15.55
4	VoIP Phones/Adapters					1020				9.23
5	Printers					974				8.81
6	Linux					866				7.83
7	Switches					576				5.21
8	Gaming Consoles					535				4.84
9	BSD					340				3.08
10	Solaris					275				2.49

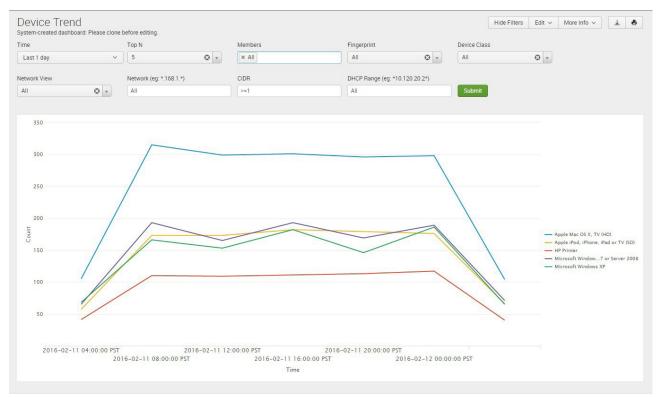
4.9 Device Class Trend

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	TimestampDevice CountDevice Class



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	TimestampDevice CountDevice Class



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	FingerprintTotal% of all devices

Sample report:

	Devices Identified							Hide Filters	Edit 🗸	More Info 🗸	Ŧ	
Time		Top N		Fingerprint		Network View	Ne	etwork (eg: *.168.1.*)				
Las	t 1 day 🗸 🗸 🗸	10	• •	All	•	All	😔 🔻 🖉	All				
CIDR ('eg: >=8)	DHCP Range (eg: *10	.120.20.2*)									
>=1		All		Submit								
	Fingerprint 0						Tota	il ¢		% of	all devices 0	
1	Apple Mac OS X, TV (HD)						17	26			16	
2	Microsoft Windows Vista/7 or Ser	ver 2008					10	040			9	
3	Apple iPod, iPhone, iPad or TV (SD))					10)14			9	
4	Microsoft Windows XP						9	966			9	
5	HP Printer						6	541			6	
6	Microsoft Windows 8 or 8.1 (Versi	ion 6.2)					4	195			4	
7	Chrome OS						3	373			3	
8	FreeBSD						3	340			3	
9	Lexmark Printer						3	332			3	
10	HP ProCurve						3	815			3	

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

Time		Top N	Members	Network View	Network (eg:)	*.168.1.*)		
Las	t 1 week 🗸 🗸 🗸	10 🕲 🔻	× All	All	▼ All			
	(eg: >=8)	Fingerprint	Device Class					
>=1		All 🕲 🔻	All 🕲 🗸	Submit				
	MAC/DUID 0	Device Type 0	Device Class 0	Network 0	Attempts 0	Last Attempt ©		
1	00:cc:e2:7c:ea:07	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:41 PS	Т	
2	03:7b:74:02:98:6a	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:31 PS	т	
3	10:40:b3:55:c9:1e	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:35 PS	т	
	10:f4:da:14:dc:19	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:21 PS	Т	
4		nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:19 PS	т	
4	13:9d:55:5b:5e:08	nomateri				C. STATE OF REPORT OF STATES		
4 5 6	13:9d:55:5b:5e:08 19:7f:9b:6d:c7:df	nomatch	Modified or Deleted	192.168.1.0	1	2016-02-06 20:46:43 PS	T	
4 5 6 7			Modified or Deleted Modified or Deleted	192.168.1.0 192.168.1.0	1	2016-02-06 20:46:43 PS 2016-02-06 20:46:21 PS		
4 5 6 7 8	19:7f:9b:6d:c7:df	nomatch			1		T	
7	19:7f:9b:6d:c7:df 1c:4c:e4:24:d9:f3	nomatch nomatch	Modified or Deleted	192.168.1.0	1 1 1 1	2016-02-06 20:46:21 PS	T T	

4.13 Device Fingerprint Change Detected

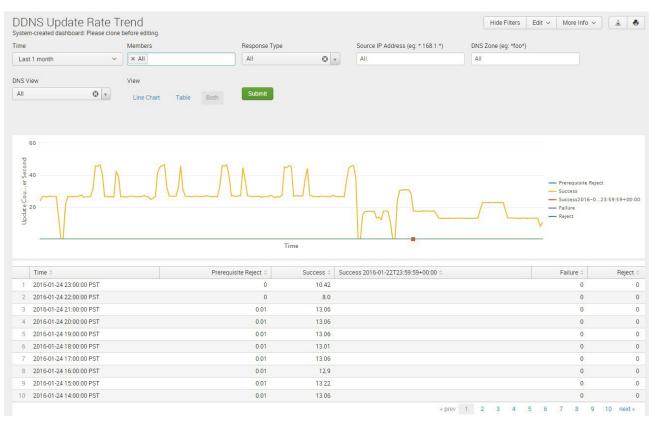
Description	Tracks when a device changes fingerprint type
Overview	Identifies and highlights when the device identified using DHCP Fingerprinting has changed. Helps identify attempts to misrepresent a device through a method called MAC Spoofing. It can also be used to identify when a desktop is using 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

lime		Members		Network Vie	W	Network (eg: *.168.1.*)	CIDR	(eg: >=16)		
Last 1 day	~	X All		All	© -	All	>=1			
HCP Range (eg: *2.1.0	0.1*)	Previous Fing	gerprint	Current Fing	erprint	Previous Device Class	Curre	nt Device Class		
All		All	© -	All	© v	All	* All	© v		
Time 0	MAC/D	UID 0 C	Current Device Type ©		Current Device Class 0	Previous Device Type 0		Previous Device Class 0	Lease IP 0	Action
Time 0 1 02/12/2016 01			Current Device Type 0 Apple Mac OS X, TV (HD)		Current Device Class O Macintosh	Previous Device Type Microsoft Windows Vista/7 or	Server 2008	Previous Device Class O Windows	Lease IP 0 172.16.100.85	Action
	:17:22 e1:15:d	::25:dc:22 A					Server 2008			
1 02/12/2016 01	17:22 e1:15:d :02:32 a5:30:4	:25:dc:22 A 4:0e:2d:e3 H	Apple Mac OS X, TV (HD)	V (SD)	Macintosh	Microsoft Windows Vista/7 or Microsoft Windows XP		Windows	172.16.100.85	Issued
1 02/12/2016 01 2 02/12/2016 01	17:22 e1:15:d :02:32 a5:30:4 :02:27 5e:aa:0	2:25:dc:22 A 4:0e:2d:e3 H 0:04:74:92 A	Apple Mac OS X, TV (HD) HP ProCurve	V (SD)	Macintosh Switches	Microsoft Windows Vista/7 or Microsoft Windows XP		Windows Windows	172.16.100.85 172.16.100.55	Issued Issued
1 02/12/2016 01 2 02/12/2016 01 3 02/12/2016 01	e1:15:d 02:32 a5:30:4 02:27 5e:aa:0 02:22 49:b0:d	2:25:dc:22 A 4:0e:2d:e3 H 0:04:74:92 A 4:38:82:df A	Apple Mac OS X, TV (HD) HP ProCurve Apple iPod, iPhone, iPad or T	V (SD)	Macintosh Switches Smartphones/PDAs/Tablets	Microsoft Windows Vista/7 or Microsoft Windows XP Cisco/Linksys SPA series IP F		Windows Windows VoIP Phones/Adapters	172.16.100.85 172.16.100.55 172.16.100.71	Issued Issued Issued
1 02/12/2016 01 2 02/12/2016 01 3 02/12/2016 01 4 02/12/2016 01	17:22 e1:15:d 102:32 a5:30:4 102:27 5e:aa:0 102:22 49:b0:d 147:43 fe:0b:85	2:25:dc:22 A 4:0e:2d:e3 H 0:04:74:92 A 4:38:82:df A :08:dd:5d 0	Apple Mac OS X, TV (HD) HP ProCurve Apple iPod, iPhone, iPad or T Apple Mac OS X, TV (HD)		Macintosh Switches Smartphones/PDAs/Tablets Macintosh	Microsoft Windows Vista/7 or Microsoft Windows XP Clsco/Linksys SPA series IP F Siemens optiPoint 410/420	hone	Windows Windows VoIP Phones/Adapters VoIP Phones/Adapters	172.16.100.85 172.16.100.55 172.16.100.71 172.16.100.52	Issued Issued Issued Issued
1 02/12/2016 01 2 02/12/2016 01 3 02/12/2016 01 4 02/12/2016 01 5 02/12/2016 00	e1:15:d :02:32 a5:30:4 :02:27 5e:aa.0 :02:22 49:b0:d :02:22 49:b0:d :47:43 fe:0b:85 :47:39 79:d2:6	2:25:dc:22 A 4:0e:2d:e3 H 0:04:74:92 A 4:38:82:df A 0:08:dd:5d O e:0f:42:05 N	Apple Mac OS X, TV (HD) HP ProCurve Apple IPod, IPhone, IPad or T Apple Mac OS X, TV (HD) OpenSolaris		Macintosh Switches Smartphones/PDAs/Tablets Macintosh Solaris	Microsoft Windows VIsta/7 or Microsoft Windows XP Cisco/Linksys SPA series IP F Siemens optiPoint 410/420 Microsoft Windows XP	hone	Windows Windows VoIP Phones/Adapters VoIP Phones/Adapters Windows	172.16.100.85 172.16.100.55 172.16.100.71 172.16.100.52 172.16.100.161	Issued Issued Issued Issued Issued
1 02/12/2016 01 2 02/12/2016 01 3 02/12/2016 01 4 02/12/2016 01 5 02/12/2016 00 6 02/12/2016 00	e1:15:22 e1:15:3 e1:15:30:4 e1:23:22 a5:30:4 e1:22:27 5e:aa.0 e1:22:22 49:b0:3 e1:47:43 fe:0b:88 e1:47:39 79:32:6 e1:47:34 19:42:6	c:25:dc:22 A 4:0e:2d:e3 H 0:04:74:92 A 4:38:82:df A 6:08:dd:5d O e:0f:42:05 N 8:44:2c:4a L	Apple Mac OS X, TV (HD) HP ProCurve Apple IPod, IPhone, IPad or T Apple Mac OS X, TV (HD) OpenSolaris dicrosoft Windows 8 or 8.1 (Macintosh Switches Smartphones/PDAs/Tablets Macintosh Solaris Windows	Microsoft Windows Vista/7 or Microsoft Windows XP Cisco/Linksys SPA series IP F Siemens optiPolint 410/420 Microsoft Windows XP Cisco/Linksys SPA series IP F	hone	Windows Windows VoIP Phones/Adapters VoIP Phones/Adapters Windows VoIP Phones/Adapters	172.16.100.85 172.16.100.55 172.16.100.71 172.16.100.52 172.16.100.161 172.16.100.194	Issued Issued Issued Issued Issued Issued
1 02/12/2016 01 2 02/12/2016 01 3 02/12/2016 01 4 02/12/2016 01 5 02/12/2016 00 6 02/12/2016 00 7 02/12/2016 00	17:22 e1:15:d 02:32 a5:30:4 02:27 5e:aa.0 02:22 49:b0:8 :47:33 fe:0b:8 :47:34 19:42:6 :47:32 30:8ffc	2:25:dc:22 A 4:0e:2d:e3 H 0:04:74:92 A 4:38:82:df A 0:08:dd:5d 0 e:0f:42:05 N 8:44:2c:4a L 1:37:50:26 A	Apple Mac OS X, TV (HD) HP ProCurve Apple IPod, IPhone, IPad or T Apple Mac OS X, TV (HD) OpenSolaris Microsoft Windows 8 or 8.1 (.exmark Printer		Macintosh Switches Smartphones/PDAs/Tablets Macintosh Solaris Windows Printers	Microsoft Windows Vista/7 or Microsoft Windows XP Cisco/Linksys SPA series IP F Siemens optiPolint 410/420 Microsoft Windows XP Cisco/Linksys SPA series IP F Siemens optiPoint 410/420	hone	Windows Windows VolP Phones/Adapters VolP Phones/Adapters Windows VolP Phones/Adapters VolP Phones/Adapters	172.16.100.85 172.16.100.55 172.16.100.51 172.16.100.52 172.16.100.161 172.16.100.194 172.16.100.155	Issued Issued Issued Issued Issued Issued

5 DNS DASHBOARDS

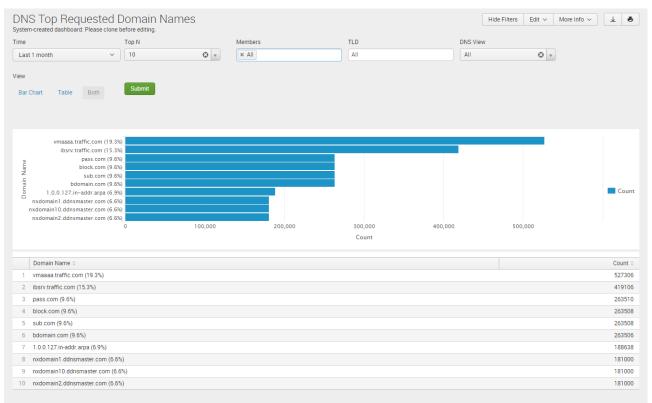
5.1 DDNS Update Rate Trend

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



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)



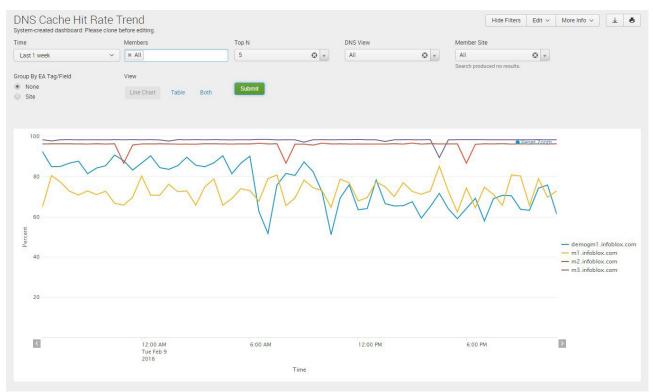
5.3 DNS Replies Trend

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

em-created dashboard: Please clone before editing.						
e Members	Response Type	View				
ist 1 week 🗸 🗸 🖌 🖌	All	🙂 🔻 Line C	nart Table Bot	Submit		
3,000						
5,000					 Reset Z 	oom
2 2,000 1,000						— failur
					Λ	— nxdo — nxrrs
					1	
						- othe
1,000					\	
ž 1,000		~				- refer
1,000		`				- refer
<		Time				- other - refer - succe
		Time				refer
	failure ≎	Time nxdomain 0	nxrrset 0	other 0	referral 0	refer
	failure ≎ 0.0		nxrrset ≎ 0.0	other 0 0.0	referral 0 0.0	> refer - succe
Time :		nxdomain 🗅				> refer - succe
Time : 2016-01-29 09:30:00 PST 2016-01-29 09:00:00 PST	0.0 0.0 0.0	nxdomain 🗇 0.0	0.0	0.0	0.0	> refer - succe
Time : 2016-01-29 09:30:00 PST 2016-01-29 09:00:00 PST 2016-01-29 08:30:00 PST	0.0	nxdomain 0 0.0 0.0	0.0	0.0	0.0	> refer - succe
Time : 2016-01-29 09:30:00 PST 2016-01-29 09:30:00 PST 2016-01-29 08:30:00 PST 2016-01-29 08:30:00 PST 2016-01-29 08:30:00 PST	0.0 0.0 0.0	nxdomain 0 0.0 0.0 0.0	0.0 0.0 0.0	0.0 1.0 0.0	0.0 0.0 0.0	> refer - succe
Time : 2016-01-29 09:30 00 PST 2016-01-29 09:30 00 PST 2016-01-29 08:30 00 PST 2016-01-29 08:30 00 PST 2016-01-29 08:00 00 PST 2016-01-29 07:30 00 PST	0.0 0.0 0.0 0.0	nxdomain 0 0.0 0.0 0.0 0.0	0.0 0.0 0.0 0.0	0.0 1.0 0.0 1.0	0.0 0.0 0.0 0.0	> refer - succe
Time : 2016-01-29 09:30:00 PST 2016-01-29 09:00:00 PST 2016-01-29 08:30:00 PST	0.0 0.0 0.0 0.0 0.0	nxdomain ○ 0.0 0.0 0.0 0.0 0.0	0.0 0.0 0.0 0.0 0.0 0.0	0.0 1.0 0.0 1.0 0.0	0.0 0.0 0.0 0.0 0.0 0.0	Succe
Time : 2016-01-29 09:30:00 PST 2016-01-29 09:30:00 PST 2016-01-29 08:30:00 PST 2016-01-29 08:00:00 PST 2016-01-29 07:30:00 PST 2016-01-29 07:30:00 PST 2016-01-29 07:30:00 PST	0.0 0.0 0.0 0.0 0.0 0.0	nxdomain ○ 0.0 0.0 0.0 0.0 0.0 0.0	0.0 0.0 0.0 0.0 0.0 0.0	0.0 1.0 0.0 1.0 0.0 1.0	0.0 0.0 0.0 0.0 0.0 0.0	refer
Time: 2016-01-29.09.30.00 PST 2016-01-29.09.30.00 PST 2016-01-29.08.30.00 PST 2016-01-29.08.30.00 PST 2016-01-29.07.30.00 PST 2016-01-29.07.30.00 PST 2016-01-29.07.30.00 PST 2016-01-29.07.30.00 PST 2016-01-29.07.30.00 PST 2016-01-29.07.30.00 PST	0.0 0.0 0.0 0.0 0.0 0.0 0.0	nxdomain ○ 0.0 0.0 0.0 0.0 0.0 0.0 0.0	0.0 0.0 0.0 0.0 0.0 0.0 0.0 0.0	0.0 1.0 0.0 1.0 0.0 1.0 0.0	0.0 0.0 0.0 0.0 0.0 0.0 0.0	Succe

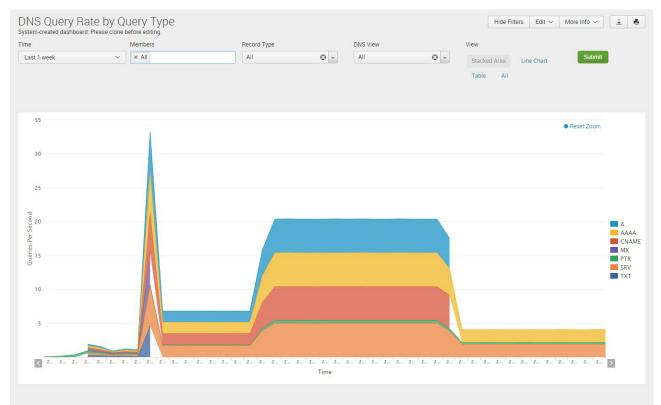
5.4 DNS Cache Hit Rate Trend

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



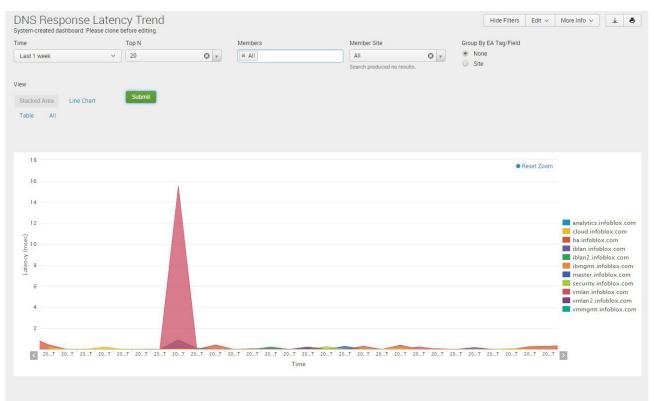
5.5 DNS Query Rate by Query Type

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



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



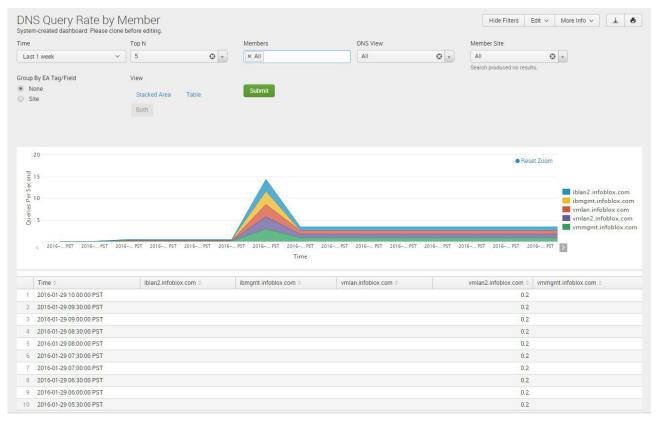
5.7 DNS Top Clients

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 addressesNumber of queries generated

NS Top Clients stem-created dashboard: Plea	ise clone bef	ore editing.						H	ide Filters	Edit 🗸	More Info v	Ŧ
ne		op N		Members		DNS Vie	w	View				
ast 1 week	~	10	• •	× All		All	e	Bar Chart	Table	Both	Submit	
10.34.209.20 (94.3%) 10.34.209.3 (1.1%) 10.34.209.5 (1.1%) 10.34.209.6 (1.1%) 10.34.209.17 (0.7%) 10.34.209.17 (0.7%) 10.34.209.11 (0.4%) 10.34.209.11 (0.4%) 10.34.209.16 (0.1%) 10.34.209.16 (0.1%) 10.34.209.18 (0.1%)		200,000	400,000	600,000	800,000	1,000,000	1,200,000	1,400,000 1,6	00,000	1,800,0	00	Que
						Queries						
Client 0												Querie
10.34.209.20 (94.3%)												1728
2 10.34.209.3 (1.1%)												20
3 10.34.209.5 (1.1%)												20
10.34.209.6 (1.1%)												19
5 10.34.209.17 (0.7%)												13
10.34.209.12 (0.6%)												11
7 10.34.209.14 (0.5%)												8
8 10.34.209.11 (0.4%)												7
0 10.34.209.16 (0.1%)												1
												1

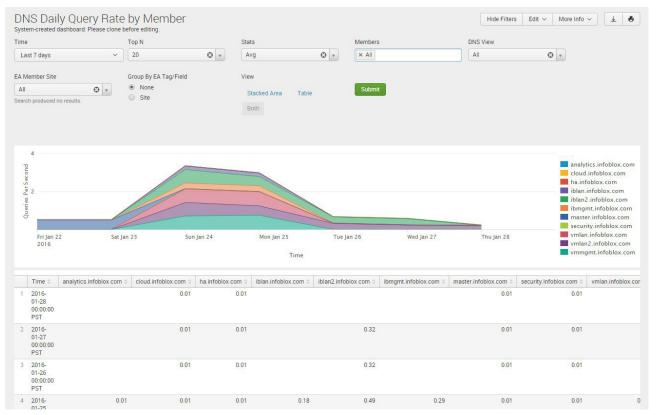
5.8 DNS Query Rate By Member

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	MemberQPSTime



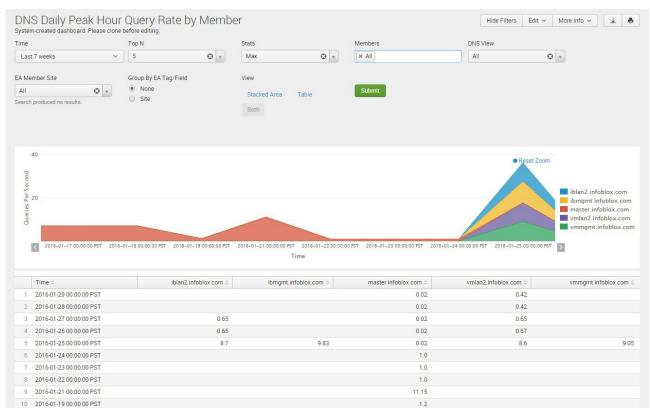
5.9 DNS Daily Query Rate by Member

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



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	TimeQPSMember



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

me			Grid Primary			Microsof	t Primary		DNS V	iew		Zon	e Name (eg: *	.google.com)			
Las	st 1 day	~	× All			All		© ,	All		٢	* All					
onel	Function		Signed			Search pre	oduced no resu	ilts.									
All	runction	© ,	All		• •	Submit											
							-										
							.		AAAA	CNAME	DNAME	DNSKEY	DS	MX	NAPTR	NSEC	NSEC3
	Timestamp 0	Zone 0	Function 0	Signed 0	Hosts 0	LBDN 0	Total Records 0	A Records 0	Records 0	Records 0	Records 0	Records 0	NSEC3 Re				
1	2016-01-28 22:02:42 PST	master.reporting.o	com Forward- Mapping	No	0	0	6	3	1	0	0	0	0	0	0	0	
2	2016-01-28 22:02:42 PST	reporting.com	Forward- Mapping	No	0	0	3	0	0	0	0	0	0	0	0	0	
3	2016-01-28 22:02:42 PST	member1_9.com	Forward- Mapping	No	0	0	52	10	10	10	0	0	0	10	0	0	
4	2016-01-28 22:02:42 PST	member1_8.com	Forward- Mapping	No	0	0	52	10	10	10	0	0	0	10	0	0	
5	2016-01-28 22:02:42 PST	member1_7.com	Forward- Mapping	No	0	0	52	10	10	10	0	0	0	10	0	0	
6	2016-01-28 22:02:42 PST	member1_6.com	Forward- Mapping	No	0	0	52	10	10	10	0	0	0	10	0	0	
7	2016-01-28 22:02:42 PST	member1_5.com	Forward- Mapping	No	0	0	52	10	10	10	0	0	0	10	0	0	
8	2016-01-28 22:02:42 PST	member1_4.com	Forward- Mapping	No	0	0	52	10	10	10	0	0	0	10	0	0	
9	2016-01-28 22:02:42 PST	member1_3.com	Forward- Mapping	No	0	0	52	10	10	10	0	0	0	10	0	0	
10	2016-01-28 22:02:42 PST	member1_23.com	Forward- Mapping	No	0	0	18	4	3	3	0	0	0	3	0	0	
																	1

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

		tics per DN board: Please clone												Hide Fi	ters Edit	✓ More In	fo 🗸 🔄	1 9
Time	2		Members			D	NS View											
La	ist 1 month	~	× All				All		• •	Subm	nit							
	Timestamp 0	View ≎	Forward Mapping Zones ©	IPv4 Reverse Mapping Zones ©	IPv6 Reverse Mapping Zones 0	Signed Zones ≎	Hosts ©	LBDN 0	Total Records ≎	A Records ≎	AAAA Records ≎	CNAME Records ≎	DNAME Records ≎	DNSKEY Records ©	DS Records 0	MX Records ≎	NAPTR Records ≎	NSI Records
1	2016-01-28 22:02:42 PST	default.netview1	1	1	1	0	0	0	3340	29	0	0	0	0	0	0	0	
2	2016-01-28 22:02:42 PST	default	36	6	2	0	0	1	9182	317	233	225	1	0	0	224	0	
4																		•

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

ime	Top N	Members	DNS View	Domair	n Name (eg:*foo*)	
Last 1 day	× 20	🕲 👻 🔀 All	All	🛛 👻 🛛 All		
LD						
All	Culuria					
411	Submit					
Domain 0		Client ©				Qu
1 cisco.com		192.168.1.101				1
		192.168.1.101				
2 infoblox.com						
		25.100.102.1				
3 cisco.com		25.100.102.1 25.100.101.1				
3 cisco.com 4 cisco.com						
3 cisco.com 4 cisco.com 5 cisco.com		25.100.101.1				
2 infoblox.com 3 cisco.com 4 cisco.com 5 cisco.com 6 infoblox.com 7 infoblox.com		25.100.101.1 2001:db8:a42:cafe:100::101				

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 nameNumber of queries

ime	Top N		Members		DNS View		Replay Type			
Last 1 day 🗸 🗸 🗸	10	• •	× All		All	• •	NXDOMAIN	0		
iew										
Bar Chart Table Both	Submit									
vic.example.net. (83.6%) www.infoblox.net. (7.6%) bar.example.com. (0.6%) www.demo3.com. (6.8%) bar.example.com. (0.5%) www.remarkost.com. (0.3%) click4search.info. (0.1%) www.google-login.com. (0.1%) speed-pay.ru. (0.1%) active.googleupdate.hk. (0.1%)	100,000	200,00	0 300,000	400,000	500,000 Queries	600,000	700,000	800,000	900,000	Queri
Domain Name 0										Queries
1 vic.example.net. (83.6%)										88320
2 www.infoblox.net. (7.6%)										7983
3 www.demo3.com. (6.8%)										7224
4 bar.example.com. (0.6%)										596
5 www.remaxhost.com. (0.3%)										28
6 mysecurityupdates.info. (0.2%)										178
7 click4search.info. (0.1%)										13
8 www.google-login.com. (0.1%)										13
										12
9 speed-pay.ru. (0.1%)										

5.15 DNS Top SERVFAIL Errors Sent/Received

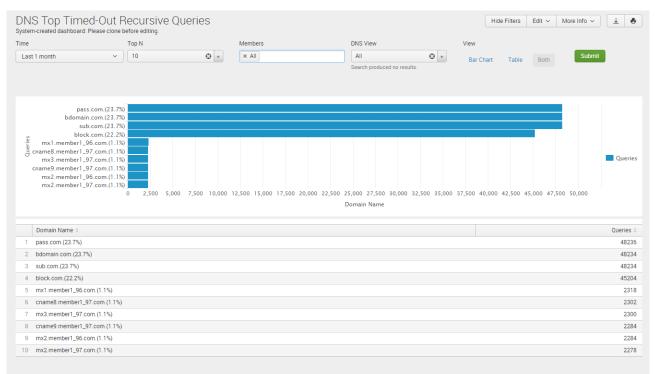
Description	Shows queries that received or sent SERVFAIL responses	
Overview	Allows users to see if issues reside within their DNS servers or upstream name servers by showing queries that receive/send SERVFAIL responses from upstream name serves.	
Data presented	Domain nameNumber of queries (sent or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

	before editing.											
1e	Top N		Members			5 View		View				
ast 1 month V	10	© v	× All		AI		• •	Bar Chart	Table	Both	Submit	
					гор	ulating						
ONS Top SERVFAIL Errors Se	nt											
INS Top SERVFAIL Errors Sent												
bdomain.com.(24.4%												
block.com.(24.4%												
sub.com.(24.4%												
aaaa6.member1_100.com.(0.4%												
aaaa6.member1_41.com.(0.4% aaaa7.member1_100.com.(0.4%												Que
arec5.member1_100.com.(0.4%												
arec6.member1_100.com.(0.4% aaaa1.member1_24.com.(0.4%												
adad1.member1_24.com.(0.4%	0 1,000	2,000	3,000	4,000	5,000 6,	,000 7,0	00 8,000	9,000	10,000	11,	000	
					Domai	in Name						
Domain Name 0												Queri
bdomain.com.(24.4%)												11
block.com.(24.4%)												11
sub.com.(24.4%)												11
pass.com.(24.4%)												11
aaaa6.member1_100.com.(0.4%)												
aaaa6.member1_41.com.(0.4%)												
aaaa6.member1_100.com.(0.4%) aaaa6.member1_41.com.(0.4%) aaaa7.member1_100.com.(0.4%) arec5.member1_100.com.(0.4%)												

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 nameNumber of queries

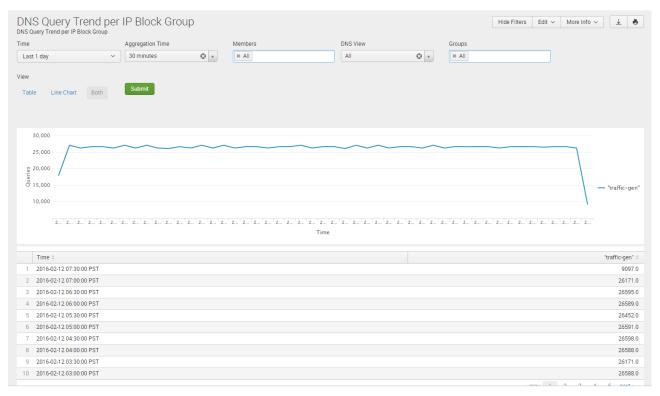
Sample report:



infoblox.

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	TimeGroupQuery count



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

me	Source	P Address (eg: 192.168.1.2)	Domain Name (eg: www.company.com)	Query Type		Members		DNS View		
Last 1 month	✓ 1.1.15	5.128	All	All	•	× All		All		• •
Submit										
Timestamp 0		Source IP Address 0	Domain Name 🗘	Query Type 0	Me	mber 0		View 0		
2016-02-22 08:12:20.90	08:12:20.90 1.1.15.128		simple6.com	A member-perf-lab-01		mber-perf-lab-015.com	m default.test1-view		test1-view	
2016-02-22 05:40:37.695		1.1.15.128	simple5.com	A	member-perf-lab-015.com			default.test1-view		
2016-02-22 05:40:37.695		1.1.15.128	simple5.com	А	me	member-perf-lab-015.com		default.test1-view		
2016-02-22 05:37:42.564		1.1.15.128	simple4.com	A	me	mber-perf-lab-015.com		default.test1-view		
2016-02-22 05:37:42.563		1.1.15.128	simple4.com	A	me	mber-perf-lab-015.com	m		default.test1-view	
2016-02-19 12:07:39.787		1.1.15.128	simple3.com	A	me	mber-perf-lab-015.com	n		default.test1-view	
2016-02-19 12:07:39.787		1.1.15.128	simple3.com	A	me	mber-perf-lab-015.com			default.test1-view	
2016-02-19 12:07:39.784		1.1.15.128	simple3.com	A	me	mber-perf-lab-015.com	n		test1-view	
2016-02-19 12:07:39.784		1.1.15.128	simple3.com	A	me	mber-perf-lab-015.com		default	test1-view	
		1.1.15.128	simple3.com	A		mber-perf-lab-015.com			test1-view	

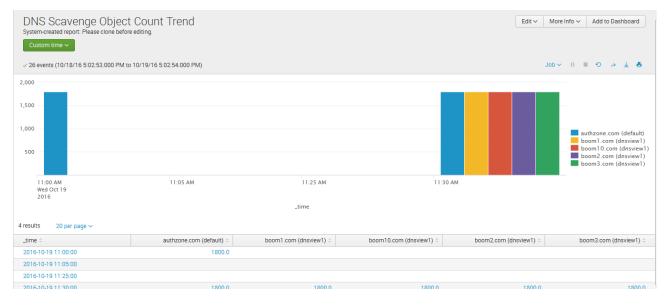
5.19 DNS Domain Query Trend*

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 In	*Please note the Infoblox Data Connector is required for this report.			

	Members		Domain Name (Mandatory Field) (eg:	Source IP Address (eg: 192.168.1.2)	Query Type	DNS	3 View
ist 1 month	✓ × All		www.company.com) simple3.com	1.1.15.128	All	O v Al	•
y Source	View						
e	Line Chart	Bar Chart	Submit				
	Both						
7,500							
5,000							
5,000						\wedge	
2.500						$\langle \rangle$	
					/		— co
					/		
		Sun Jan 31	Sun Feb 7	Sun	Feb 14	Sun	Feb 21
Sun Jan 24 2016							

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	TimeCount trend



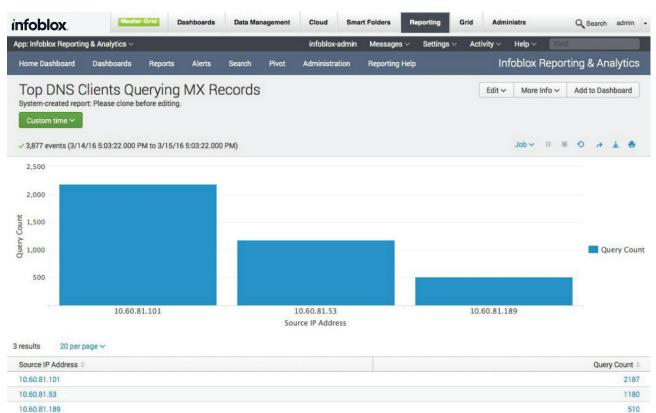
5.21 Top DNS Clients by Query Type*

s report is populated by the Data Connector. It enables administrators to search for nular queries and filter by type and source.
imestamp Iomain Name 1ember iew
1

ne TopN	Query Typ	2	Query Source		Source IP Address (eg: 192.168.1.2)				
Last 1 month v 10	😧 👻 🔺	•	Internal	•	All		Sub	mit		
Source IP Address 0									Qu	ery Coun
10.32.2.156										55
DNS Queries for Source IP Address 10.32.2.156										
-	-									
Timestamp ©		nain Name 0		Member 0				View 0 default		
2016-02-22 06:15:47.109 2016-02-22 06:14:25.652		.com		gm-vm-10-27.c				default		
2016-02-22 06:14:25:652		.com		gm-vm-10-27.c				default		
2016-02-22 06:14:25:652		.com		gm-vm-10-27.c				default		
2016-02-22 06:14:21:394		i.com		gm-vm-10-27.c				default		
2016-02-22 03:49:51.772		.com		gm-vm-10-27.c				default		
2016-02-22 03:49:51.771		com		gm-vm-10-27.c				default		
2016-02-22 03:43:03.319		.com		gm-vm-10-27.c				default		
2016-02-22 03:43:03.318		.com		gm-vm-10-27.c				default		
2016-02-19 10:08:01.234	sim	ole3.com		gm-vm-10-27.c				default		
				-	« prev 1	2 3 4	5 6	7 8	9 1	0 next
	0.155									
DHCP Lease History for Source IP Address = 10.32	.2.156									
			ults found.							

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 IPQuery Count
*Please note the Ir	nfoblox Data Connector is required for this 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

ast Update	ed	IP Address		User Name	User	Status		
Last 1 we	eek ~	All		All	All	© .	Submit	
Last	t Updated 0	User Name 0	Domain 0	IP Address 0	First Seen 0	Logout Time 0	Last Seen 0	User Status 0
1 2016	6-01-28 20:35:24	u01_000328	ad-30	10.102.30.125	2016-01-28 20:12:4	4	2016-01-28 20:12:44	TIMEOUT
2 2016	6-01-28 20:35:24	u01_000327	ad-30	10.102.30.125	2016-01-28 19:44:3	7	2016-01-28 19:44:37	TIMEOUT
3 2016	6-01-28 20:35:24	u01_000326	ad-30	10.102.30.125	2016-01-28 20:19:0	2	2016-01-28 20:19:02	TIMEOUT
4 2016	6-01-28 20:35:24	u01_000325	ad-30	10.102.30.125	2016-01-28 20:24:1	7	2016-01-28 20:24:17	TIMEOUT
5 2016	6-01-28 20:35:24	u01_000324	ad-30	10.102.30.125	2016-01-28 20:19:5	2	2016-01-28 20:19:52	TIMEOUT
6 2016	6-01-28 20:35:24	u01_000323	ad-30	10.102.30.125	2016-01-28 20:05:5	8	2016-01-28 20:05:58	TIMEOUT
7 2016	6-01-28 20:35:24	u01_000322	ad-30	10.102.30.125	2016-01-28 19:30:3	4	2016-01-28 19:30:34	TIMEOUT
8 2016	6-01-28 20:35:24	u01_000321	ad-30	10.102.30.125	2016-01-28 19:25:5	6	2016-01-28 19:25:56	TIMEOUT
9 2016	6-01-28 20:35:24	u01_000320	ad-30	10.102.30.125	2016-01-28 19:39:3	8	2016-01-28 19:39:38	TIMEOUT
10 2016	6-01-28 20:35:24	u01_000319	ad-30	10.102.30.125	2016-01-28 20:03:0	1	2016-01-28 20:03:01	TIMEOUT

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

Subscription		before editing.							Hide Filters	Edit v More Info v	
LAN ID		IP Address (e.g. *.168.1	1.*)								
All		All	Sub	amit							
User Name 0	Domain 0	Cisco ISE SSID 0	VLAN Name 0	VLAN ID 0	Cisco ISE Session State 0	Cisco ISE Endpoint profile 0	Cisco ISE Security Group 0	Discovered At 0	Cisco ISE EPS Status 0	IP Address 0	GUID
1 qa	ft-ac.com				STARTED	Cisco-Switch	SGT_TestServers	2016-10-18 09:19:13	NONE	10.0.0.6	qa
2 qa	ft-ac.com				STARTED	Cisco-Switch	SGT_TestServers	2016-10-18 09:19:13	NONE	10.0.0.6	qa
3 qa	ft-ac.com				STARTED	Cisco-Switch	SGT_TestServers	2016-10-18 09:19:13	NONE	10.0.0.6	qa
4 qa	ft-ac.com				STARTED	Cisco-Switch	SGT_TestServers	2016-10-18 09:19:13	NONE	10.0.0.6	qa
5 qa	ft-ac.com				STARTED	Cisco-Switch	SGT_TestServers	2016-10-18 09:19:13	NONE	10.0.0.6	qa
6 qa	ft-ac.com				STARTED	Cisco-Switch	SGT_TestServers	2016-10-18 09:19:13	NONE	10.0.0.6	qa
7 qa	ft-ac.com				STARTED	Cisco-Switch	SGT_TestServers	2016-10-18 09:18:26	NONE	10.0.0.5	qa
8 qa	ft-ac.com				STARTED	Cisco-Switch	SGT_TestServers	2016-10-18 09:18:07	NONE	10.0.0.4	qa
9 qa	ft-ac.com				STARTED	Cisco-Switch	SGT_TestServers	2016-10-18 09:17:39	NONE	10.0.0.3	qa
10 qa	ft-ac.com				STARTED	Cisco-Switch	SGT_TestServers	2016-10-18 09:13:26	NONE	10.0.0.2	qa

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:

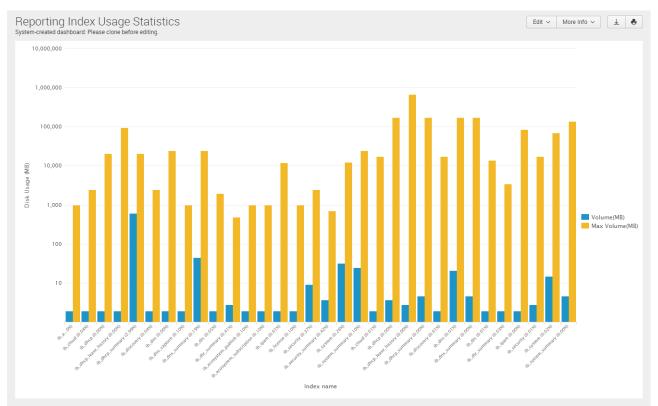
Publish Data stem-created dashboard: Please clone b	efore editing.					Hide Filters Edit 🗸	More Into V	*
st Updated	IP Address (e.g. *.168.1.*)	Target IP Address (e.g. *.168.1.*)	View					
Last 1 week 🗸 🗸	All	All	Bar Chart Line Chart	Submit				
			Pie Chart Stacked Area					
			Table All					
Last updated 0		IP Address 0	TARGET I	P Address 0	Publish Type 0			
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			

infoblox.

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 NameDisk Usage



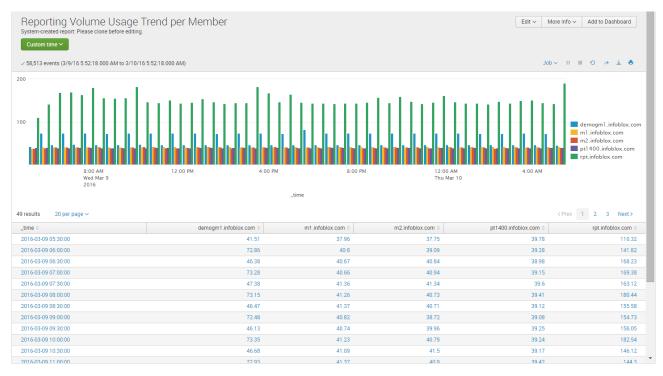
7.2 Reporting Volume Usage Trend Per Category

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



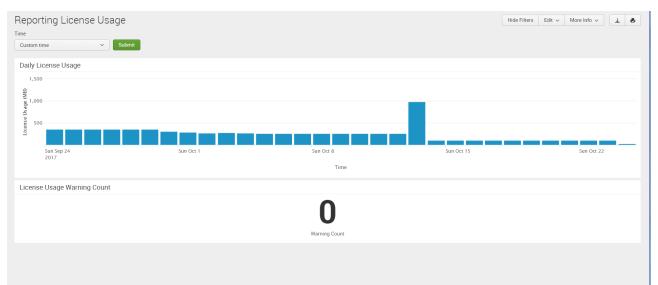
7.3 Reporting Volume Usage Trend Per Member

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)MemberTime



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



8 IP ADDRESS MANAGERMENT DASHBOARDS

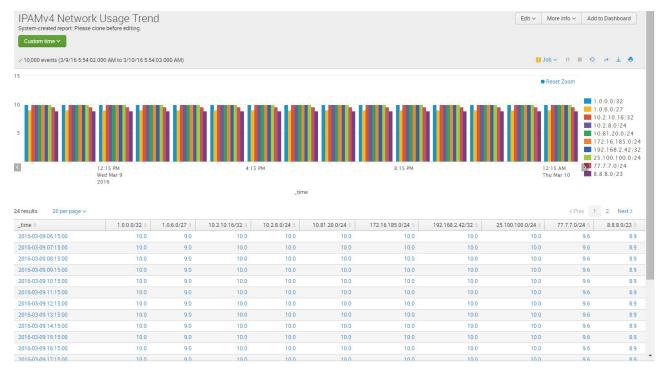
8.1 IPAM v4 Network Usage Statistics

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

ime		Member	s		Network	View	Network (eg: *10.120.20.0	*)	CIDR (eg: >24)			
Las	1 hour	~ X All			All	⊖ v	All			>=1			
tiliza	tion % (eg: >10)	Network	Active Directory	Site									
>=0	aon io (eg ro)	× All	Active Directory	one	Subm	it							
													4
	Timestamp 0	Network view 0	Network 0	CIDR 0	AD Site 0	DHCPv4 Utilization % 0	Total 0	Allocated 0	Reserved 0	Assigned 0	Protocol 0	Utilization % 0	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	
	2016-01-29 19:57:59	default	10.0.0.0	8	(no_value)	0.0	16777216	33	2	0	IPV4	0.0	
2					(no_value)	0.0	16777216	65024	2	0	IPV4	0.3	
2	2016-01-29 19:57:59	default	11.0.0.0	8	(mo_renec)								
	2016-01-29 19:57:59 2016-01-29 19:57:59	default default	11.0.0.0		(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	
3				8		0.0	16777216 16777216	65278 65278	2		IPV4 IPV4	0.3 0.3	
3	2016-01-29 19:57:59	default	12.0.0.0	8	(no_value)					0			
3 4 5	2016-01-29 19:57:59 2016-01-29 19:57:59	default default	12.0.0.0 13.0.0.0	8 8 8	(no_value) (no_value)	0.0	16777216	65278	2	0	IPV4	0.3	
3 4 5	2016-01-29 19:57:59 2016-01-29 19:57:59 2016-01-29 19:57:59	default default netview1	12.0.0.0 13.0.0.0 14.0.0.0	8 8 8 8	(no_value) (no_value) (no_value)	0.0 0.0	16777216 16777216	65278 65278	2	0 0 0	IPV4 IPV4	0.3 0.3	
3 4 5 6 7	2016-01-29 19:57:59 2016-01-29 19:57:59 2016-01-29 19:57:59 2016-01-29 19:57:59	default default netview1 netview1	12.0.0.0 13.0.0.0 14.0.00 15.0.0.0	8 8 8 8 8	(no_value) (no_value) (no_value) (no_value) (no_value)	0.0 0.0 0.0	16777216 16777216 16777216	65278 65278 65278	2 2 2	0 0 0	IPV4 IPV4 IPV4	0.3 0.3 0.3	

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	TimeUsage %



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

Time		Mem	bers		Network	View	Network	eg: *10.120.20.0	*)	CIDR (eg: >24)		
Las	t 1 hour	~) (× /	11		All	© .	All			>=1			
Itiliza	tion % (eg: >10)	Netw	ork Active Directory	Site									
>=0		×			Subm	it							
													4
	Timestamp ©	Network view	Network 0	CIDB 0	AD Site 0	DHCPv4 Utilization % 0	Total ©	Allocated ©	Reserved 0	Assigned ©	Protocol 0	Utilization % 0	Unmanaged
1	2016-01-29 19:57:59	netview1	10.0.0.0			0.0	16777216	1	2	1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1		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	
3	2016-01-29 19:57:59	default	11.0.0.0	8	(no_value)	0.0	16777216	65024	2	0	IPV4	0.3	
	2016-01-29 19:57:59	default	12.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	
4	2016-01-29 19:57:59	default	13.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	
4		netview1	14.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	
	2016-01-29 19:57:59	netview1	15.0.0.0	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	
5	2016-01-29 19:57:59 2016-01-29 19:57:59		40000	8	(no_value)	0.0	16777216	65278	2	0	IPV4	0.3	
5		netview1	16.0.0.0										
5 6 7	Ition % (eg:>10) Network Active Directory Site Xall Submit Timestamp c Network View c Network c CIDR c DHCPv4 Utilization % c Total c Allocated c Reserved c Assigned c Protocol c Utilization % c Unmanaged c 2016-01-29 19:57:59 netview1 10.0.0 8 (no_value) 0.0 1677216 1 2 0 IPV4 0.0 <td< td=""></td<>												

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 QS Version

twork View	Device Vendor	Dev	ice Model	Device Name	Device IP Address	Network	Utilizatio	in % (eq: >10)		
All 💿 🔻	All	O v Al			All	All	>=0		Submit	
		-								
Total Networks				work/Network View			Networks Connected to Devices			
					defaul	t				
Device Networks	Dilectics 9: 4	Maturel (Teur -	Davido 18 A	Perios Nomo -	defaul		Device Model o	Device Mender 1	Period DE Marcha o	
IPAM Network ©		Network View 0	Device IP o	Device Name o		Interface IP 0	Device Model ©	Device Vendor ©	Device OS Version 0	
IPAM Network 0 10.40.16.0/24	5.5	default	10.40.16.8	AugustaLab-Arista-DCS-7048T.inca		Interface IP 0 10.40.16.8	DCS7048TA	Arista	4.9.6	
IPAM Network 0 10.40.16.0/24 2 10.40.16.0/24	5.5 5.5	default default	10.40.16.8 10.40.16.9	AugustaLab-Arista-DCS-7048T.inca HP-E2910al-48G-PoE		Interface IP 0 10.40.16.8 10.40.16.9	DCS7048TA J9148A	Arista HP	4.9.6 W.15.08.0012	
IPAM Network 0 10.40.16.0/24 10.40.16.0/24 10.40.16.0/24 10.40.16.0/24	5.5 5.5 5.5	default default default	10.40.16.8 10.40.16.9 10.40.16.4	AugustaLab-Arista-DCS-7048T.inca HP-E2910al-48G-PoE WS-C3750X-24.inca.infoblox.com		Interface IP 0 10.40.16.8 10.40.16.9 10.40.16.4	DCS7048TA J9148A catalyst37xxStack	Arista HP Cisco	4.9.6 W.15.08.0012 15.2(1)E2	
IPAM Network 0 10.40.16.0/24 2.10.40.16.0/24 3.10.40.16.0/24 4.10.40.16.0/24	5.5 5.5 5.5 5.5	default default default default	10.40.16.8 10.40.16.9 10.40.16.4 10.40.239.254	AugustaLab-Arista-DCS-7048T.inca HP-E2910al-48G-PoE WS-C3750X-24 inca infobiox.com disco-lab-02 inca infobiox.com		Interface IP 0 10.40.16.8 10.40.16.9 10.40.16.4 10.40.16.1	DCS7048TA J9148A catalyst37xxStack cat3560x48	Arista HP Cisco Cisco	4.9.6 W.15.08.0012 15.2(1)E2 15.0(2)SE8	
IPAM Network 0 10.40.16.0/24 2 10.40.16.0/24 3 10.40.16.0/24 4 10.40.16.0/24 5 10.34.47.0/24	5.5 5.5 5.5 5.5 0.0	default default default default default	10.40.16.8 10.40.16.9 10.40.16.4 10.40.239.254 10.40.16.6	AugustaLab-Arista-DCS-7048T.inca. HP-E2910al-48G-PoE WS-C3750X-24.inca.infoblox.com disco-lab-02.inca.infoblox.com EX4200-24P		Interface IP 0 10.40.16.8 10.40.16.9 10.40.16.4 10.40.16.1 10.34.47.100	DCS7048TA J9148A catalyst37xxStack cat3560x48 EX4200	Arista HP Cisco Cisco Juniper	4.9.6 W.15.08.0012 15.2(1)E2 15.0(2)SE8 13.2X50	
IPAM Network 0 10.40.16.0/24 10.40.16.0/24 10.40.16.0/24 10.40.16.0/24 10.40.16.0/24 10.34.47.0/24	5.5 5.5 5.5 5.5 0.0 0.0	default default default default default default	10.40.16.8 10.40.16.9 10.40.16.4 10.40.239.254	AugustaLab-Arista-DCS-7048T.inca HP-E2910al-48G-PoE WS-C3750X-24 inca infobiox.com disco-lab-02 inca infobiox.com		Interface IP 0 10.40.16.8 10.40.16.9 10.40.16.4 10.40.16.1	DCS7048TA J9148A catalyst37xxStack cat3560x48	Arista HP Cisco Cisco	4.9.6 W.15.08.0012 15.2(1)E2 15.0(2)SE8	
	5.5 5.5 5.5 0.0 0.0 0.0	default default default default default	10.40.16.8 10.40.16.9 10.40.16.4 10.40.239.254 10.40.16.6	AugustaLab-Arista-DCS-7048T.inca. HP-E2910al-48G-PoE WS-C3750X-24.inca.infoblox.com disco-lab-02.inca.infoblox.com EX4200-24P		Interface IP 0 10.40.16.8 10.40.16.9 10.40.16.4 10.40.16.1 10.34.47.100	DCS7048TA J9148A catalyst37xxStack cat3560x48 EX4200	Arista HP Cisco Cisco Juniper	4.9.6 W.15.08.0012 15.2(1)E2 15.0(2)SE8 13.2X50	

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

Time		Top N		Client (eg: 10.120.20.	*)	Domain Name		DNS View		
Last 1 month	~	10	🕲 👻 All		All		All		() v	
Members		Mitigation Action		RPZ Zone (suffix matching)		RPZ Entry		Search produced no results. Severity		
× All		All	0 v	All		All		All	O .	Submit
Client ID 0	Total Client Hits	Domain Name 0	RPZ En	itry 0	RPZ Severity 0	Total Rule Hits 0	Mitigation Actio	n o	Substitute Addresses 0	Time 0
A.S. (10.00							Contraction of the second	n o	Substitute Addresses 0	
1 10.34.9.20	66794	arec1.member1_1.com	32.1.0.0	0.10.rpz-ip.local.com	INFORMATIONAL	367	Passthru	n o	Substitute Addresses 0	01/13/2016 13:20:00
1 10.34.9.20 2 10.34.9.20	66794 66794	arec1.member1_1.com arec1.member1_10.com	32.1.0.0	0.10.rpz-ip.local.com 0.10.rpz-ip.local.com	INFORMATIONAL	367 367	Passthru Passthru	n 0	Substitute Addresses 0	01/13/2016 13:20:00
1 10.34.9.20	66794	arec1.member1_1.com arec1.member1_10.com	32.1.0.0	0.10.rpz-ip.local.com	INFORMATIONAL	367	Passthru	n ≎	Substitute Addresses 0	01/13/2016 13:20:00
1 10.34.9.20 2 10.34.9.20	66794 66794	arec1.member1_1.com arec1.member1_10.com arec1.member1_11.com	32.1.0.0 32.1.0.0 32.1.0.0	0.10.rpz-ip.local.com 0.10.rpz-ip.local.com	INFORMATIONAL	367 367	Passthru Passthru		Substitute Addresses 0	01/13/2016 13:20:00
1 10.34.9.20 2 10.34.9.20 3 10.34.9.20	66794 66794 66794	arec1.member1_1.com arec1.member1_10.com arec1.member1_11.com arec2.member1_1.com	32.1.0.0 32.1.0.0 32.1.0.0 32.2.0.0	0.10.rpz-ip.local.com 0.10.rpz-ip.local.com 0.10.rpz-ip.local.com	INFORMATIONAL INFORMATIONAL INFORMATIONAL	367 367 367	Passthru Passthru Passthru	Domain)	Substitute Addresses 0	01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00
1 10.34.9.20 2 10.34.9.20 3 10.34.9.20 4 10.34.9.20	66794 66794 66794 66794	arec1.member1_1.com arec1.member1_10.com arec1.member1_11.com arec2.member1_1.com arec2.member1_10.com	32.1.0.0 32.1.0.0 32.1.0.0 32.2.0.0 32.2.0.0	0.10.rpz-ip.local.com 0.10.rpz-ip.local.com 0.10.rpz-ip.local.com 0.10.rpz-ip.local.com	INFORMATIONAL INFORMATIONAL INFORMATIONAL INFORMATIONAL	367 367 367 367 367	Passthru Passthru Passthru Block (No Such	Domain) Domain)	Substitute Addresses 0	01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00
1 10.34.9.20 2 10.34.9.20 3 10.34.9.20 4 10.34.9.20 5 10.34.9.20	66794 66794 66794 66794 66794	arec1.member1_1.com arec1.member1_10.com arec1.member1_11.com arec2.member1_1.com arec2.member1_10.com arec2.member1_10.com	32.1.0.0 32.1.0.0 32.2.0.0 32.2.0.0 32.2.0.0 32.2.0.0	0.10.rpz-ip.local.com 0.10.rpz-ip.local.com 0.10.rpz-ip.local.com 0.10.rpz-ip.local.com 0.10.rpz-ip.local.com	INFORMATIONAL INFORMATIONAL INFORMATIONAL INFORMATIONAL	367 367 367 367 367 367	Passthru Passthru Passthru Block (No Such Block (No Such	Domain) Domain) Domain)	Substitute Addresses 0	01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00
1 10.34.9.20 2 10.34.9.20 3 10.34.9.20 4 10.34.9.20 5 10.34.9.20 6 10.34.9.20	66794 66794 66794 66794 66794 66794	arec1.member1_1.com arec1.member1_10.com arec1.member1_11.com arec2.member1_10.com arec2.member1_10.com arec2.member1_11.com	32.1.0.0 32.1.0.0 32.1.0.0 32.2.0.0 32.2.0.0 32.2.0.0 32.3.0.0	0.10.rpz-ip.local.com 0.10.rpz-ip.local.com 0.10.rpz-ip.local.com 0.10.rpz-ip.local.com 0.10.rpz-ip.local.com 0.10.rpz-ip.local.com	INFORMATIONAL INFORMATIONAL INFORMATIONAL INFORMATIONAL INFORMATIONAL	367 367 367 367 367 367 367	Passthru Passthru Passthru Block (No Such Block (No Such Block (No Such	Domain) Domain) Domain)	Substitute Addresses 0	01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00
1 10.34.9.20 2 10.34.9.20 3 10.34.9.20 4 10.34.9.20 5 10.34.9.20 6 10.34.9.20 7 10.34.9.20	66794 66794 66794 66794 66794 66794 66794	arec1.member1_1.com arec1.member1_10.com arec1.member1_11.com arec2.member1_10.com arec2.member1_10.com arec3.member1_11.com arec3.member1_10.com	32.1.0.0 32.1.0.0 32.2.0.0 32.2.0.0 32.2.0.0 32.2.0.0 32.3.0.0 32.3.0.0	0.10.rpz-ip local.com 0.10.rpz-ip local.com 0.10.rpz-ip local.com 0.10.rpz-ip local.com 0.10.rpz-ip local.com 0.10.rpz-ip local.com 0.10.rpz-ip.local.com	INFORMATIONAL INFORMATIONAL INFORMATIONAL INFORMATIONAL INFORMATIONAL INFORMATIONAL	367 367 367 367 367 367 367 367 367	Passthru Passthru Passthru Block (No Such Block (No Such Block (No Such Block (No Data)	Domain) Domain) Domain)	Substitute Addresses 0	01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00 01/13/2016 13:20:00 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:

ime		Top N		Members	Client (eg: *10	.120.20.*)	DNS View			
Last	t 1 month	× 10	() v	× All	All		All	© -	Submit	
							Search produced no results.			
	Client ID 0				Total Client Hits 0	Time 0				
1	10.34.9.20				33397	01/13/2016 13:20:00				
2	10.34.9.20				33397	01/13/2016 14:30:00				
3	10.34.9.20				33397	01/13/2016 15:30:00				
4	10.34.9.20				33397	01/13/2016 18:20:00				
5	10.34.9.20				33306	01/13/2016 13:30:00				
6	10.34.9.20				33306	01/13/2016 14:50:00				
7	10.34.9.20				33306	01/13/2016 15:00:00				
8	10.34.9.20				33306	01/13/2016 15:10:00				
9	10.34.9.20				33306	01/13/2016 15:20:00				
10	10.34.9.20				33306	01/13/2016 15:50:00				

infoblox.

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

	FireEye Appliance	AI	ert ID	RPZ Entry	Mitigation Action	Log Severity
Last 1 day	~ All		All	All	All 🛛 🗸 🗸	All 🛛 🗸 🗸
ert Type						
All 😳 🔻	Submit					
Time 0	Alert ID 0	Log Severity 0	Alert Type 0	FireEye Appliance 0	RPZ Entry 0	Mitigation Action ©
1 2016-04-05 06:56:15 PDT	749620	Minor	Infection Events	fireeye-a8e8e8.infoblox.com w.63d4.cn.fireyeeye_feed		Block (No Data)
2 2016-04-05 06:54:27 PDT	749621	Minor	Infection Events	fireeye-a8e8e8.infoblox.com	w.wesy67.com.fireyeeye_feed	Block (No Data)
3 2016-04-05 06:52:36 PDT	749622	Minor	Infection Events	fireeye-a8e8e8.infoblox.com	b.158dm.com.fireyeeye_feed	Block (No Data)
4 2016-04-05 06:50:56 PDT	749623	Critical	Callback Events	fireeye-a8e8e8.infoblox.com	c.158dm.com.fireyeeye_feed	Substitute (Domain Name)
5 2016-04-05 06:49:12 PDT	749624	Minor	Infection Events	fireeye-a8e8e8.infoblox.com	xxx.188dm.com.fireyeeye_feed	Block (No Data)
5 2010-04-03 00.43.121 01	749625	Minor	Infection Events	fireeye-a8e8e8.infoblox.com	91wwmm.com.fireyeeye_feed	Block (No Data)
6 2016-04-05 06:46:25 PDT	749626	Minor	Infection Events	fireeye-a8e8e8.infoblox.com	hhj7.cn.fireyeeye_feed	Block (No Data)
	749020	Minor	Infection Events	fireeye-a8e8e8.infoblox.com	www.sb2190.cn.fireyeeye_feed	Block (No Data)
6 2016-04-05 06:46:25 PDT	749627	MITIO				
6 2016-04-05 06:46:25 PDT 7 2016-04-05 06:45:18 PDT		Minor	Infection Events	fireeye-a8e8e8.infoblox.com	jsshengping.com.fireyeeye_feed	Block (No Data)

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

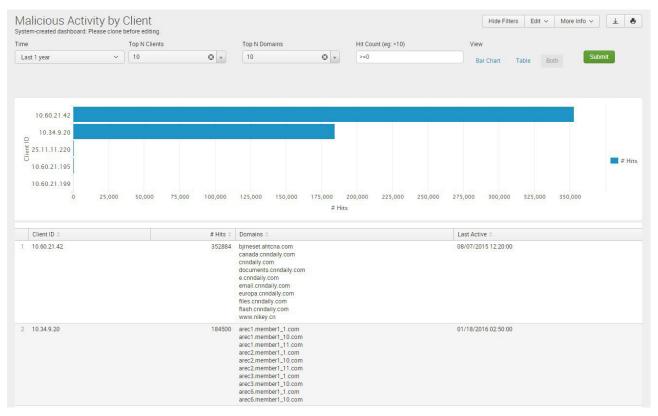
Sample report:

me	Top N	Hit	Count(eg: >1	0)		
Las	t 1 year 🗸 🔪 🔽 20	⊙ ▼ >=	=0		Submit	
	RPZ Rule 0	Percenta	age o	# Hits 0	Description 0	
1	32.1.0.0.10.rpz-ip.local.com	1	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	1	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	1	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	1	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	

infoblox.

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



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

9.6 Threat Protection Event Count by Time

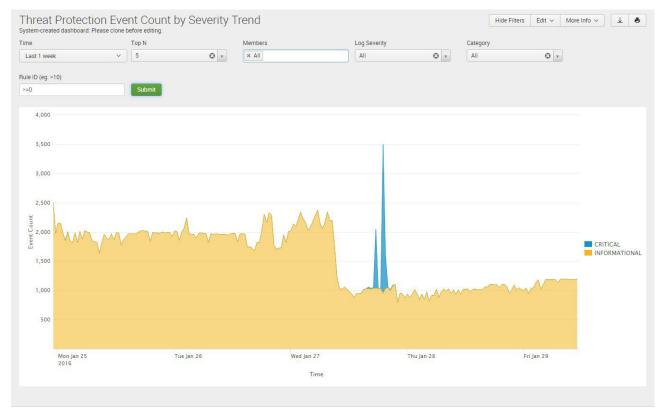
Sample report:

me		Members		Log Severity		Category	Rule ID (eg: >10)		
Last	t 1 day	~ X All		All	© ,	All 🛛 🔻	>=0		Submit
	Time 0	SID 0	Member 0	Category 0	Log severity 0	Event Name 🌣	Alert Count ©	Drop Count 0	Total Event Count
1	01/29/2016 11:00:00	130900300	security.infoblox.com	OSPF	INFORMATIONAL	DROP OSPF unexpected	0	60	6
2	01/29/2016 11:00:00	130906000	security.infoblox.com	DHCP	INFORMATIONAL	DROP IPv4 DHCP unexpected	0	31	3
3	01/29/2016 11:00:00	140000600	security.infoblox.com	Default Pass/Drop	INFORMATIONAL	DROP UDP unexpected	0	83	8
4	01/29/2016 11:00:00	140000800	security.infoblox.com	Default Pass/Drop	INFORMATIONAL	DROP unexpected protocol	0	4598	459
5	01/29/2016 10:55:00	130900300	security.infoblox.com	OSPF	INFORMATIONAL	DROP OSPF unexpected	0	60	6
6	01/29/2016 10:55:00	130906000	security.infoblox.com	DHCP	INFORMATIONAL	DROP IPv4 DHCP unexpected	0	26	2
7	01/29/2016 10:55:00	140000600	security.infoblox.com	Default Pass/Drop	INFORMATIONAL	DROP UDP unexpected	0	44	4
8	01/29/2016 10:55:00	140000800	security.infoblox.com	Default Pass/Drop	INFORMATIONAL	DROP unexpected protocol	0	4608	460
9	01/29/2016 10:50:00	130900300	security.infoblox.com	OSPF	INFORMATIONAL	DROP OSPF unexpected	0	60	6
10	01/29/2016 10:50:00	130906000	security.infoblox.com	DHCP	INFORMATIONAL	DROP IPv4 DHCP unexpected	0	12	1

infoblox.

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 countSeverity TypeTime



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:

Time		Members	Log Severity	Log Severity Category		Rule ID (eg: >10)		
Last 1 month	~	IIA × AII	All 🕹 ,	All	• ©	ALL		Submit
							700000000000	
SID 0	SID © Category © Log severity ©		Event Name ©			Alert Count ©	Drop Count ©	Total Event Count
140000800	000800 Default Pass/Drop INFORMATIONAL		DROP unexpected protocol			0	7858364	785836
130900300	130900300 OSPF INFORMATIONAL		DROP OSPF unexpected			0	158620	15862
140000600 Default Pass/Drop INFORMATIONAL		DROP UDP unexpected			0	115024	11502	
130906000 DHCP INFORMATIONAL		DROP IPv4 DHCP unexpected		0	64716	6471		
110100900 DNS Protocol Anomalies CRITICAL		EARLY DROP UDP query multiple questions or non query operation code			0	23833	2383	
130906100 DHCP INFORMATIONAL		DROP IPv6 DHCP unexpected		0	1225	122		
140000500 Default Pass/Drop INFORMATIONAL		Drop TCP unexpected			0	109	10	
140000500								

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:

Time	Members	Category	Rule ID (eg: >10)	EA Member Site	
Last 1 year	~ X All	All 😔 🔻	>=0	All 😧 🗸	
iroup By EA Tag/Field None Site	Submit				
				Informational Event Count ©	Total Event Count
Member 0	Critical Event Count ©	Major Event Count ©	Warning Event Count ©	Informational Event Count ©	Total Event Count
Member 0 1 ib4030.nios72	Critical Event Count 0 118265283	Major Event Count 0 11448	58156979	64958235774	6513466948

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	TimeMemberEvent Count



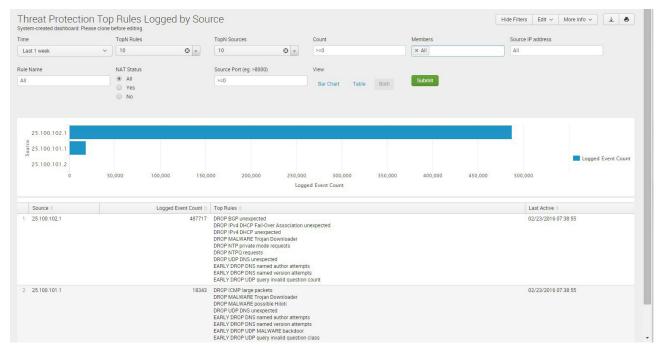
9.11 Threat Protection Event Count by Category

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

me	Members	Category				
Las	t 1 year 🗸 🗸 🖌 🗸 All	All	© v	Submit		
	Category ≎	Critical Event Count ©	Major Event Count ©	Warning Event Count 🗇	Informational Event Count 0	Total Event Count
1	Default Pass/Drop	0	0	0	64237480764	6423748076
2	TCP/UDP Floods	0	0	0	727470530	72747053
3	ICMP 117		0	0	0	11760829
4	DNS Cache Poisoning	0	0	58156979	0	581569
5	DHCP	0	0	0	1035232	10352
6	DNS Protocol Anomalies	674821	0	0	0	6748
7	BGP	0	0	0	285065	28500
8	OSPF	0	0	0	158620	15862
9	DNS Amplification and Reflection	512	11214	0	0	117:
10	DNS Tunneling	0	0	0	3627	363

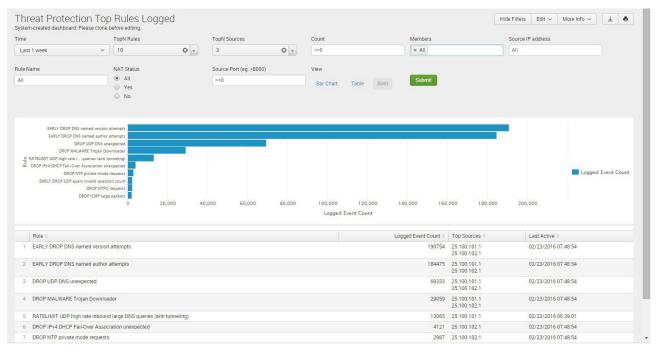
9.12 Threat Protection Top Rules Logged by Source

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



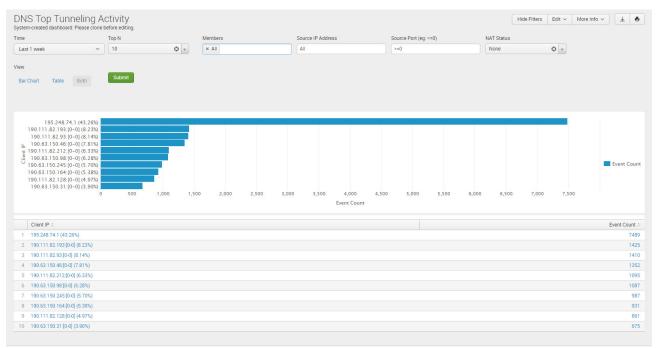
9.13 Threat Protection Top Rules Logged

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 namesEvent count per threat event



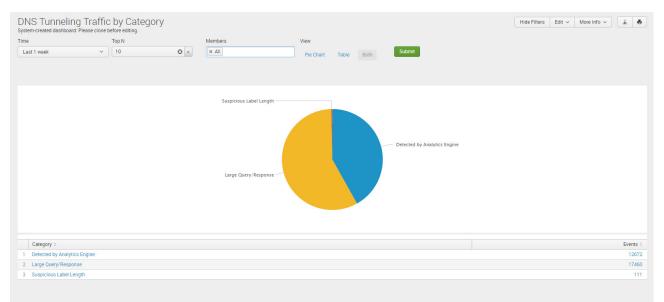
9.14 DNS Top Tunneling Activity

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



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



9.16 Top Malware and DNS Tunneling Events by Client

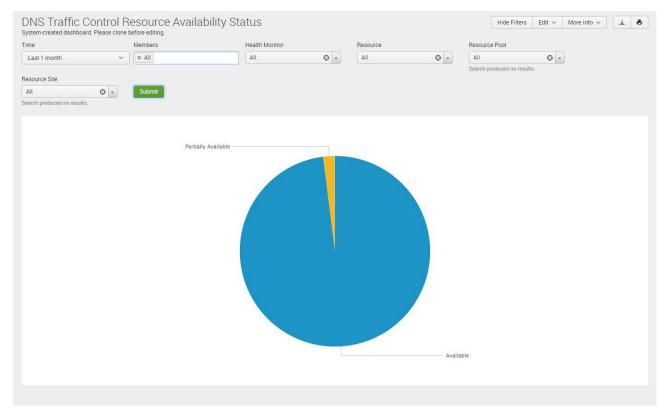
Description	Lists the clients that have the most number of outbound malicious queries (RPZ hits) and DNS tunneling events in a given time frame
Overview	Helps identify the top infected clients detected making outbound malicious queries and that were associated with DNS tunneling activities, so that the 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

Top Malware a	and DNS	6 Tunneling Ev	ents by Client					Hide Filters Edit ~	More Info v	Ŧ
ime		Members	Source IP address	NAT Status		Source Port (eg: >8000)				
Last 1 week	~	× All	All	All	© •	>=0	Submit			
Client IP 0			Total DNS Tunne	ing Events 0		Total Outbound maliciou	s queries 0	Last Seen 0		
195.248.74.1				71			7489	03/16/2016 10:50:00		
190.111.82.93				1410			217	03/18/2016 10:00:00		
190.111.82.193				1425			185	03/18/2016 10:00:00		
190.63.150.46				1352			241	03/18/2016 10:00:00		
190.63.150.245				987			233	03/18/2016 10:00:00		
190.111.82.212				1095			89	03/15/2016 10:30:00		
190.63.150.98				1087			88	03/15/2016 10:30:00		
190.111.82.128				861			234	03/18/2016 10:00:00		
190.63.150.164				931			150	03/18/2016 10:00:00		
190.63.150.31				675			216	03/18/2016 10:00:00		

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	AvailablePartially availableUnavailable



10.2 DNS Traffic Control Resource Availability Trend

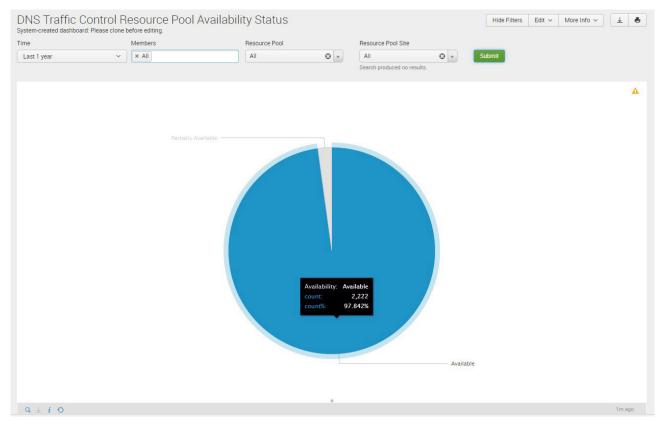
Description	Provides the resource availability of DNS Traffic Control over time with trending
Overview	Tracks the availability (or lack of availability) for DNS Traffic Control resources over time. Helps monitor changes over time to find trends that can impact performance.
Data presented	 Availability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

e	Members	Resource	1	Health Monitor	Resource Pool	
ast 1 month ~	× All	All	© .	All	All Search produced r	results.
ource Site	Group By EA Tag/Field	View				
۲ 🕄 ۲	 None Site 	Line Ch	art Table Both	Submit		
rch produced no results.						
100						Reset Zoom
80						
60 221						
60 Aligge Isov 40						— agowtham-s
Availability (%)						— agowtham-s

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	AvailablePartially availableUnavailable

Sample report:



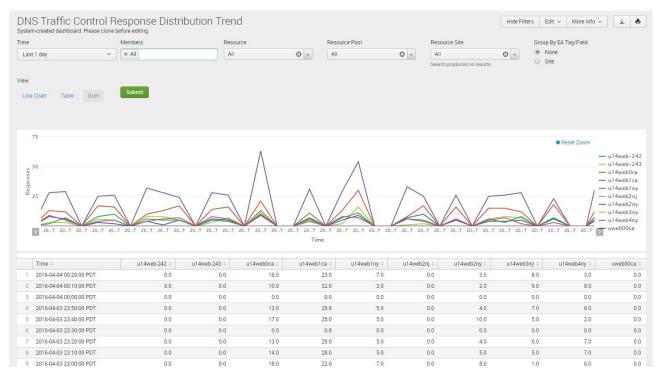
10.4 DNS Traffic Control Resource Pool Availability Trend

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

me	Members	Resource Pool	Resource Pool Site	Group By EA Tag/Field	
Last 1 year 🗸 🗸	× All	All	All O v Search produced no results.	 None Site 	
ew					
Line Chart Table Both	Submit				
					4
102				Reset Zoom	
e 100					-
ζi ζ					
88 a					-
000 96 001					— agowtham-p
2016-01-21 00:00:00 PST	2016-01-22 00:00:00 PST	2016-01-23 00:00:00 PST 2011 Time	5-01-24 00:00:00 PST 2016-01-25 00:00:0	0 PST 2016-01-26 00:00:00 PST	>
					agowtham-poo
Time 0					agonalampor
Time 0 2016-01-29 00:00:00 PST					-
1 2016-01-29 00:00:00 PST					10
2016-01-29 00:00:00 PST 2 2016-01-28 00:00:00 PST					10
2016-01-29 00:00:00 PST 2 2016-01-28 00:00:00 PST 3 2016-01-27 00:00:00 PST					10 10 99
2016-01-29 00:00 PST 2 2016-01-28 00:00:00 PST 3 2016-01-27 00:00:00 PST 4 2016-01-26 00:00:00 PST					10 10 99 99
1 2016-01-29 00:00:00 PST 2 2016-01-28 00:00:00 PST 3 2016-01-27 00:00:00 PST					10/ 10/ 99. 99.
1 2016-01-29 00:00:00 PST 2 2016-01-28 00:00:00 PST 3 2016-01-27 00:00:00 PST 4 2016-01-26 00:00:00 PST 5 2016-01-25 00:00:00 PST					100 100 99. 99. 100 100 100 99.

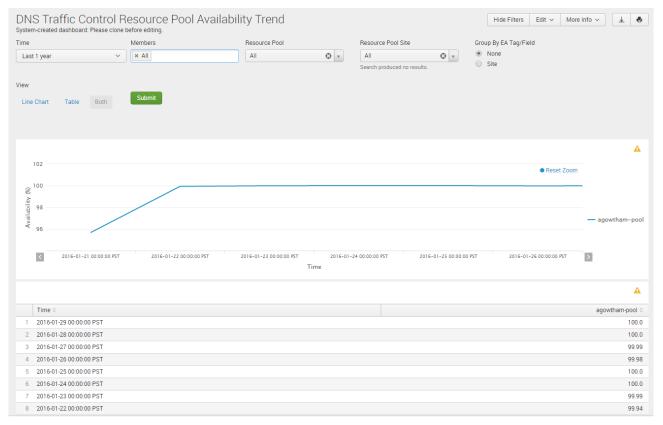
10.5 DNS Traffic Control Response Distribution Trend

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



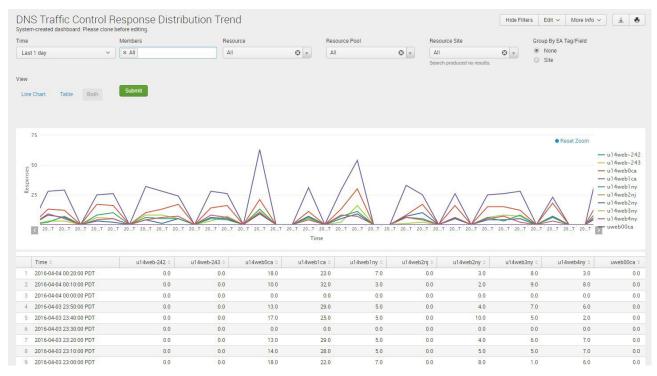
10.6 DNS Traffic Resource Pool Availability Trend

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



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	ResponsesTimeTraffic Control Resources



10.8 DNS Traffic Resource SNMP Trend

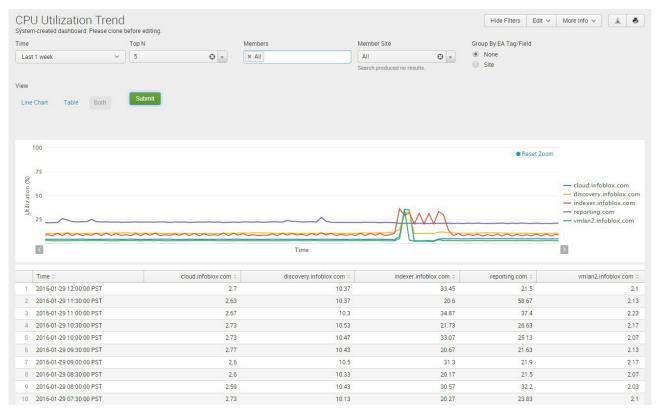
Description	Tracks SNMP resource information over time for DNS Traffic Control
Overview	Allows more granular view of SNMP data over time to better manage DNS Traffic Control across multiple appliances.
Data presented	SNMP data over time

DNS Traffic C			SNMF	P Trend										Hide Filters E	dit 🗸 Mor	e Info 🗸 👲
Time		Members			Resource Pool		Health Monitor		OID		Resource		Resource Site			
Last 1 day	~	IA X			All	0 v	All	• •	All	O .	All	© .	All	© .		
Group By EA Tag/Field		View											Search produced no			
None	• •				Submit											
Search produced no results.	- 10	Line Chart	Table	Both												
5.5																
5.5																
5																
4.5																
4																
3.5																
Value																
2.5																1.3.6.1.2.1.2.1.0
2																
2																
1.5																
1																
0.5																
								Time								

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



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	

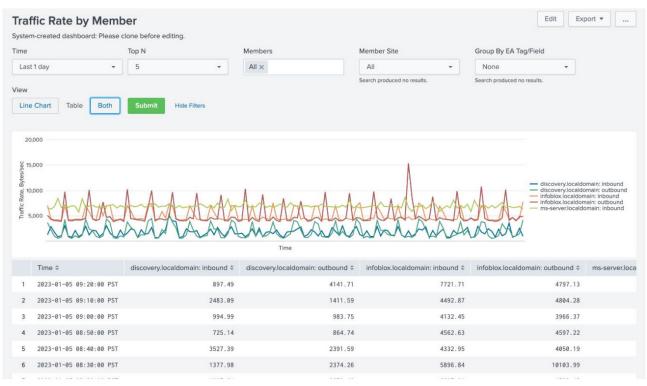
Sample report:

System Time Last View	nory Utilization T -created dashboard: Please of 1 day • Chart Table Both		Members All ×	Member Site All Search produced no results.	Group By EA Tag/Fie None Search produced no result	•
100 7* (%) uotpaziliji 50 25	5)		Time			 adp.localdomain discovery.localdomain infoblox.localdomain member2.localdomain ms-server.localdomain
	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:



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

Time Admin				Actio	n		Object Ty	pe	Object Name	Execution Status					
Last 1 day	~	All		All	٥	¥	All	© 7	All	All	© v				
lembers		Message													
× All		All		Sul	bmit										
Timestamp 0	Admin 0		Action ©	Object Type 0	Object Name 0	Executi Status		Message 0	sage 🌣						
2016-02-23 07:15:31 PST	mgowarty		Called		PrepareReportingUser	Normal		user="mgowarty"			demogm1.infoblox.c				
2016-02-23 07:15:30 PST	mgowarty		Called		IndexerStatus	Normal					demogm1.infoblox.co				
2016-02-23 07:15:29 PST	aobszynski Logout				Normal			ip=89.73.204.145 group=dl	Expiration	demogm1.infoblox.co					
2016-02-23 07:15:06 PST	\$SPLUNK-RI ADMIN\$	LUNK-REPORTING- Login_Allowed 11NS				Normal		to=AdminConnector ip=192	168.1.6 auth=LOCAL group=s	plunk-reporting-group apparently_via=API	demogm1.infoblox.co				
2016-02-23 07:15:06 PST	\$SPLUNK-RI ADMINS	EPORTING-	Called		GetSplunkLookups	Normal		file_type="all"			demogm1.infoblox.co				
2016-02-23 07:15:01 PST	\$SPLUNK-RI ADMIN\$	EPORTING-	Login_Allowed	1		Normal		to=AdminConnector VPN=F apparently_vla=API	Reporting Member auth=LOCAI	_ group=splunk-reporting-group	demogm1.infoblox.c				
2016-02-23 07:14:49 PST	07:14:49 mgowarty Login_Allowed			1		Normal		to=AdminConnector ip=108	demogm1.infoblox.co						
2016-02-23 07:14:43 PST	admin Login_Denied					Normal		to=AdminConnector ip=108	demogm1.infoblox.co						
2016-02-23 07:14:33 PST	admin	Login_Denied Normal to=AdminConnector ip=108.28.189.20 info=AD_Local apparently_via=GUI					demogm1.infoblox.co								
2016-02-23 07:14:28 PST	apatel		Logout			Normal		ip=50.162.99.196 group=dl	SE NA trigger_event=Session I	Expiration	demogm1.infoblox.co				
									« [nev 1 2 3 4 5 6 7	8 9 10 next				

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

st Updated	IP Address	User Name	User Status				
Last 1 week 🗸 🗸 🗸	All	All	All	🛛 👻 Submit			
Last Updated 0	User Name 0	Domain 0	IP Address 0	First Seen 0	Logout Time 0	Last Seen 0	User Status 0
1 2016-10-18 09:19:13	qa	ga ft-ac.com 10.0.0.6 2016-10-18.09:19:13				2016-10-18 09:19:13	TIMEOUT
2 2016-10-18 09:19:13	qa	ft-ac.com	10.0.0.6	2016-10-18 09:19:13		2016-10-18 09:19:13	TIMEOUT
3 2016-10-18 09:19:13	ga ft-sc.com 10.0.6 2016-10-18.09:19:13						TIMEOUT
4 2016-10-18 09:19:13	qa	ft-ac.com	10.0.0.6	2016-10-18 09:19:13		2016-10-18 09:19:13	TIMEOUT
5 2016-10-18 09:19:13	qa	ft-ac.com	10.0.0.6	2016-10-18 09:19:13		2016-10-18 09:19:13	TIMEOUT
6 2016-10-18 09:19:13	qa	ft-ac.com	10.0.0.6	2016-10-18 09:19:13		2016-10-18 09:19:13	TIMEOUT
7 2016-10-18 09:18:26	qa	ft-ac.com	10.0.0.5	2016-10-18 09:18:26		2016-10-18 09:18:26	TIMEOUT
8 2016-10-18 09:18:07	qa	ft-ac.com	10.0.0.4	2016-10-18 09:18:07		2016-10-18 09:18:07	TIMEOUT
9 2016-10-18 09:17:39	qa	ft-ac.com	10.0.0.3	2016-10-18 09:17:39		2016-10-18 09:17:39	TIMEOUT
0 2016-10-18 09:13:26	qa	ft-ac.com	10.0.0.2	2016-10-18 09:13:26		2016-10-18 09:13:26	TIMEOUT

13 CLOUD DASHBOARD

13.1 VM Address History

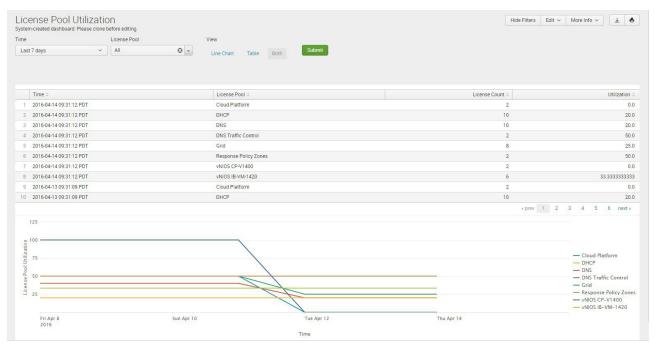
Description	Tracks the history of IP addresses of VMs provisioned
Overview	Provides detailed views of current and historical IP addresses (and other parameters) of VMs provisioned and destroyed. Helps administrators troubleshoot virtual instances faster with accurate visibility and meets audit/compliance 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

Time			Member	s		Network	(e.g. *.168	.1.*)	Network 1	/iew			Tenant ID			Tenant	Name		VLAN I	D				
Week to date	e	v	x All			All			All		¢	•	All			All			All					
ocation			Applicat	ion Type		Address	Туре		Private H	ostname			Public Hostn	ame		Private	Address (e.g. *.	168.1.*)	Public	Address (e.g.	*.168.1.*)			
All			All			All		• v	All				All			All			IIA					
Elastic Addres	s (e.g. *.168.	1.*)	Manage	ment Platform		Is Prime	ry Interface	,	VPC Nam	e			VPC Network	(e.g. *.1)	58.1.*)	VM Ho:	stname							
All			All			All		• •	All				All			All			Subr	nit				
Time 0	IP Address 0	Action ©	Address Type ©	MAC Address 0	CNAME(s)	o ID o	FQDN 0	VM Name/Instance Name 0	Network 0	Network View 0	Tenant ID 0 236	Tenant Name 0 236	Location 0	VLAN ID 0	Application Type 0	Private Hostname	Public Hostname 0	Private Address 0	Public Address 0	Elastic Address ©	Interface Name 0	Is Primary Interface 0	Management Platform 0 vm132ctest	VPC Nam
19:03:59																						No		
10/18/2016 19:03:08	20.0.0.10	Allocated		aa:11:11:11:11:16					20.0.0.0/28		236	236										No	vm132ctest	
10/18/2016 19:02:51	20.0.0.9	Allocated	Fixed	88:11:11:11:11:15				99	20.0.0.0/28	default	236	236										No	vm132ctest	
10/18/2016 19:02:31	20.0.0.8	Allocated	Fixed	88:11:11:11:11:14				99	20.0.0.0/28	default	236	236										No	vm132ctest	
10/18/2016 19:01:26	20.0.0.7	Allocated	Fixed	ee:11:11:11:11:13				99	20.0.0/28	default	236	236										No	vm132ctest	
10/18/2016	20.0.0.6	Allocated	Fixed	aa:11:11:11:11:12				99	20.0.0/28	default	236	236										No	vm132ctest	
			Fixed	aa:11:11:11:11:11					20.0.0.0/28		236	236										No	vm132ctest	

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:



infoblox.

Infoblox unites networking and security to deliver unmatched performance and protection. Trusted by Fortune 100 companies and emerging innovators, we provide real-time visibility and control over who and what connects to your network, so your organization runs faster and stops threats earlier. Corporate Headquarters 2390 Mission College Blvd, Ste. 501 Santa Clara, CA 95054

+1.408.986.4000 www.infoblox.com

