



Free Online Training - Day 3



# Intro about the training program

All modules of Site24x7 will be covered in 5 sessions.

We offer this training program in three time zones for your convenience.

AUS Time Zone (10:00 AEDT) | UK Time Zone (10:00 GMT) | US Time Zone (10:00 PST)

## Sessions split up:

**Session 1 - Introduction and Deep Dive into Website Monitoring (Mon, April 17, 2023)**

**Session 2 - Infrastructure Monitoring and Custom Plugins (Tue, April 18, 2023)**

**Session 3 - Network & Virtualization Monitoring and Log Management (Wed, April 19, 2023)**

**Session 4 - Application Performance Monitoring and Real User Monitoring (Thu, April 20, 2023)**

**Session 5 - Reports, Dashboards, Advanced Configurations, Alerting, and More (Fri, April 21, 2023)**



# Scope of the session

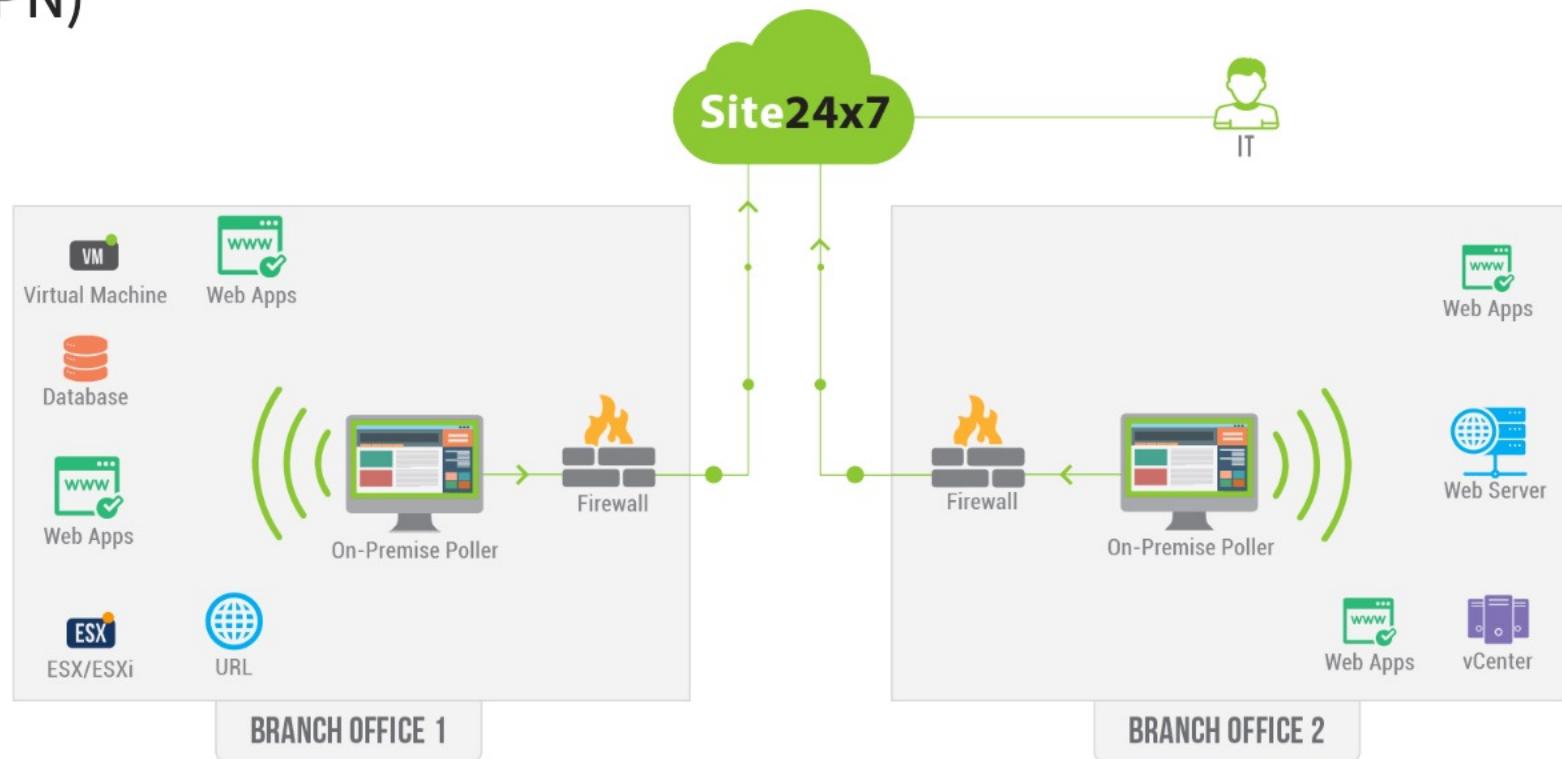
- Overview of On-Premise Poller
- Network Monitoring
- NetFlow Analyzer
- Network Configuration Manager
- VoIP Monitoring
- Cisco Meraki Monitoring
- VMware Monitoring
- Nutanix Monitoring
- VMware Horizon Monitoring
- AppLogs Monitoring



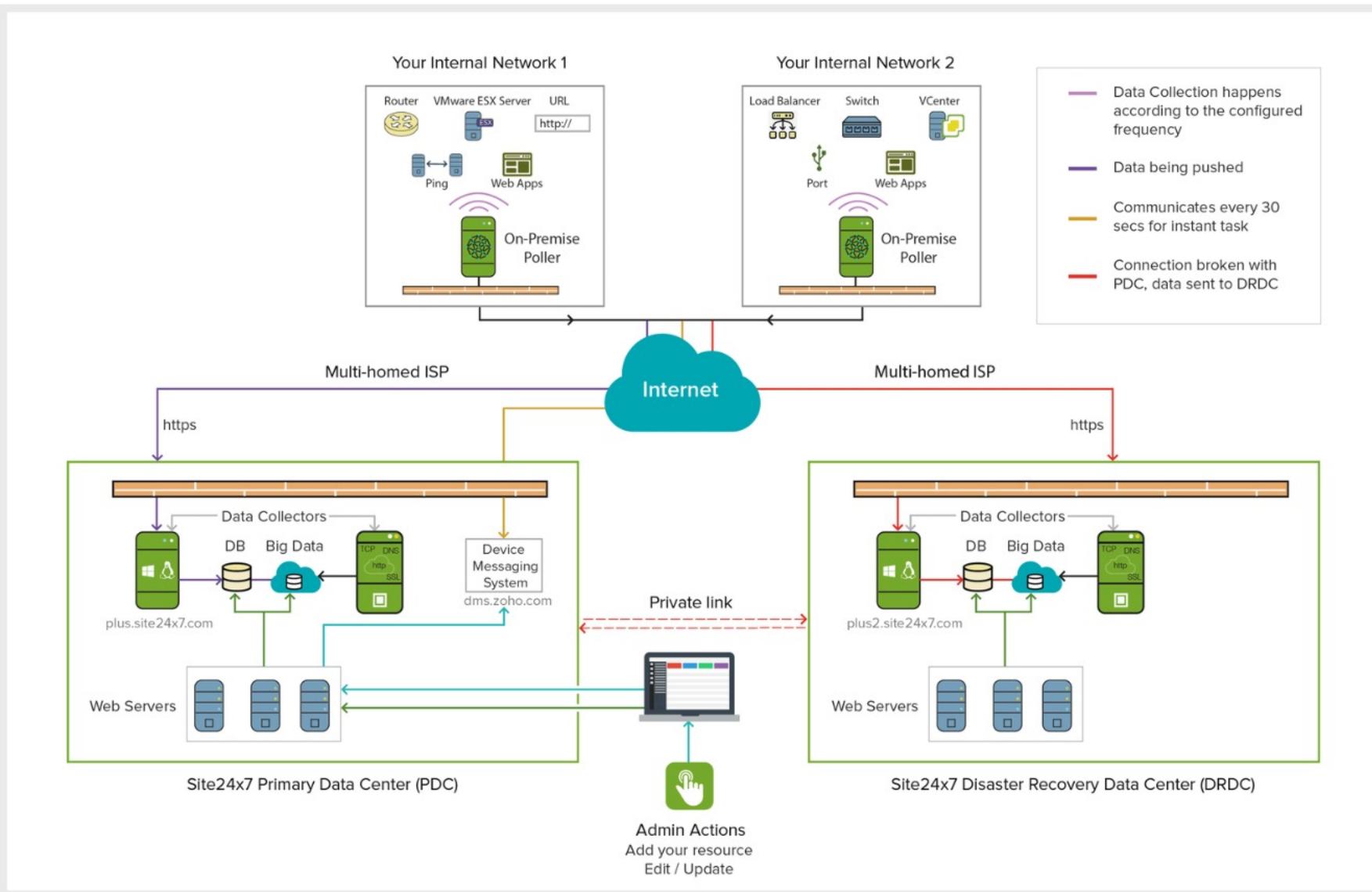
# Overview of On-Premise Poller

# On-Premise Poller - Introduction

- On-Premise Poller, our lightweight agent, helps monitor your internal network and resources behind your firewall or virtual private network (VPN)



# Architecture





# Minimum Requirements

Parameters	Minimum requirements
OS	All Windows and Linux operating systems, including 32-bit and 64-bit
RAM	8 GB
Processor speed	2 GHz
Disk space	80 GB



# Ports and Domains to be whitelisted

→ Ports

=80

= 443

→ Domains

> plus.site24x7.com

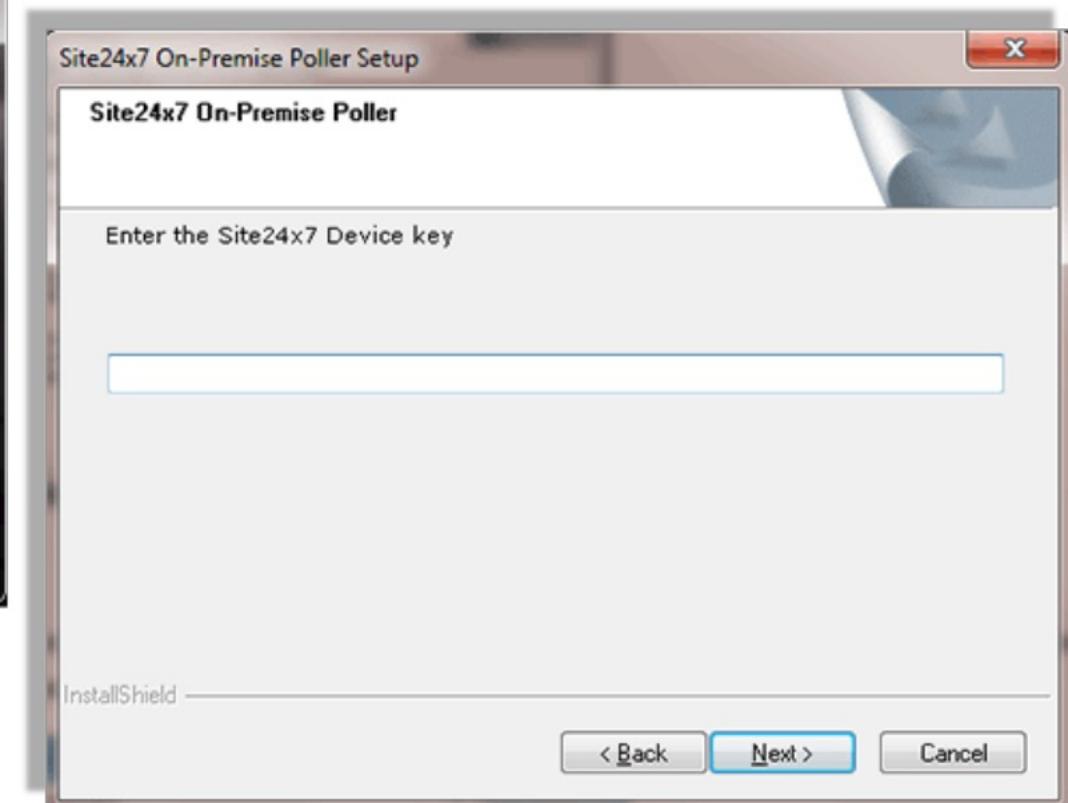
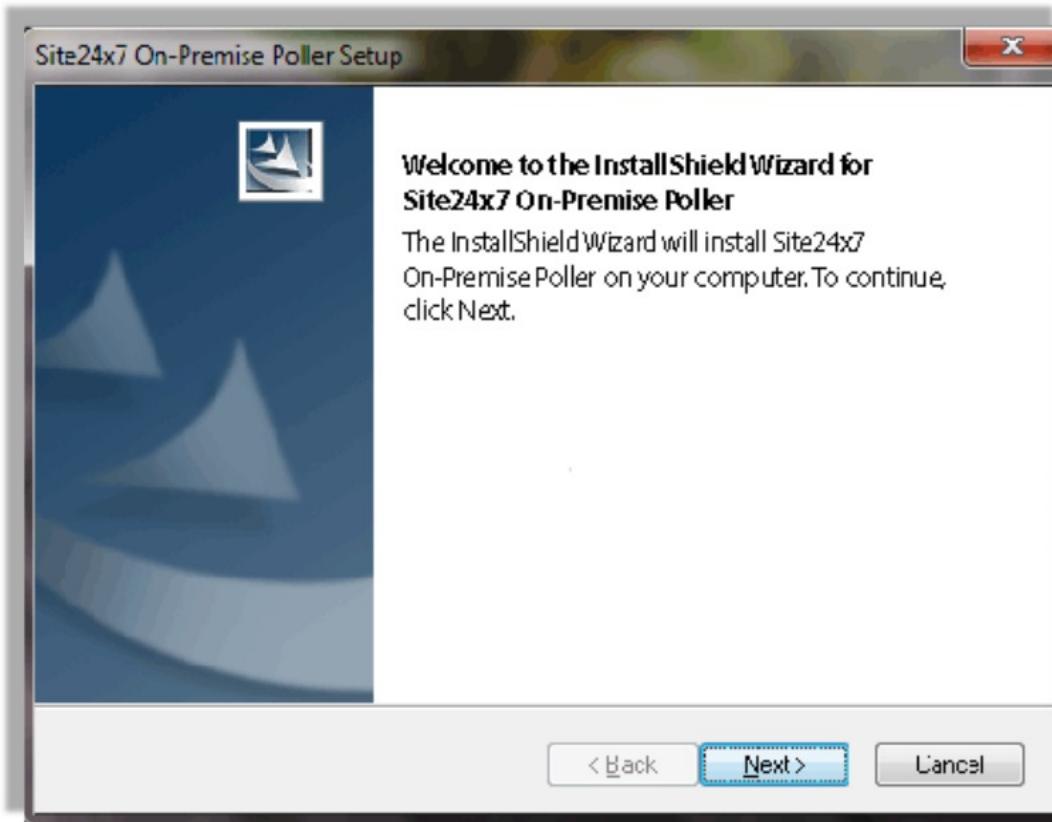
> plus2.site24x7.com

> pluspoller.site24x7.com

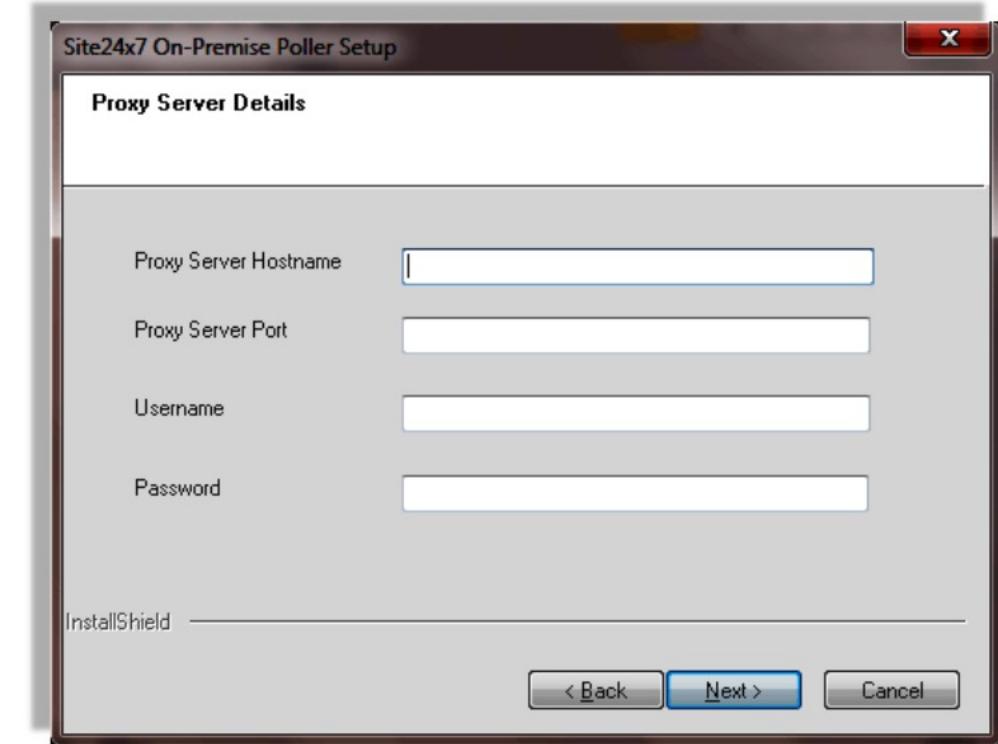
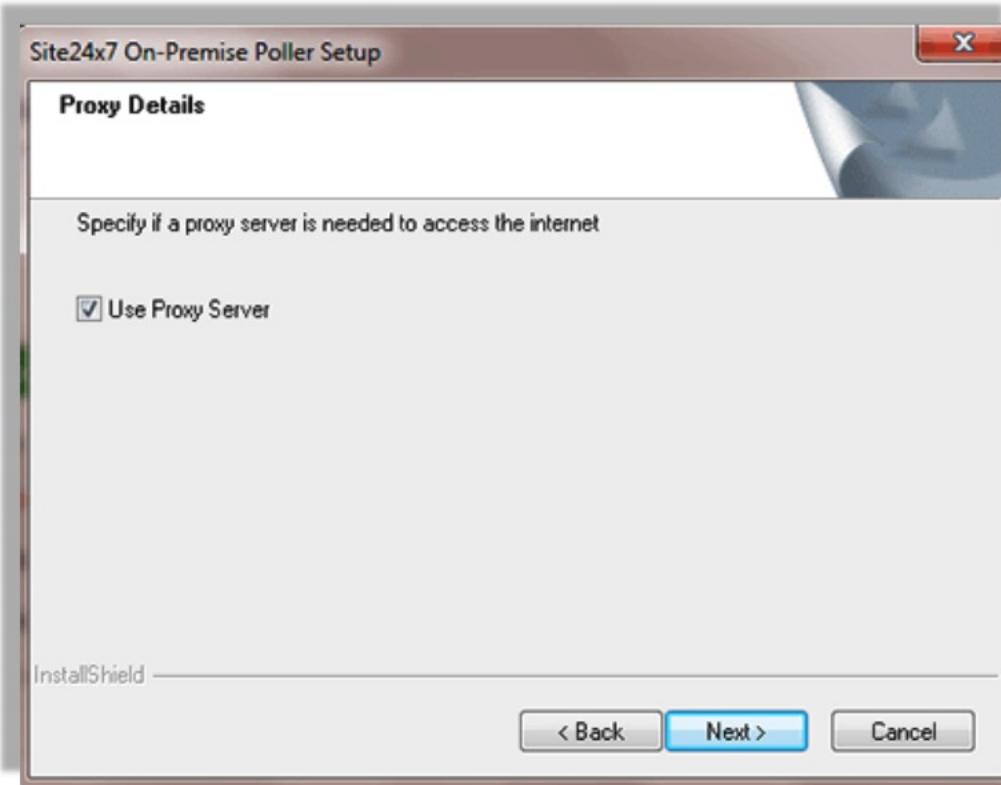
> plusnetwork.site24x7.com

> staticdownloads.site24x7.com

# Adding On-Premise Poller for Windows



# Configuring Proxy





# Adding On-Premise Poller for Linux

- Execute the following commands in your terminal to install the On-Premise Poller
- 64 bit OS:  
sudo wget  
[http://staticdownloads.site24x7.com/probe/Site24x7OnPremisePoller\\_64bit.bin](http://staticdownloads.site24x7.com/probe/Site24x7OnPremisePoller_64bit.bin)  
sudo chmod 755 Site24x7OnPremisePoller\_64bit.bin  
sudo ./Site24x7OnPremisePoller\_64bit.bin
- 32 bit OS:  
sudo wget http://staticdownloads.site24x7.com/probe/Site24x7OnPremisePoller.bin  
sudo chmod 755 Site24x7OnPremisePoller.bin  
sudo ./Site24x7OnPremisePoller.bin
- Run the installer to install the On-Premise Poller by using your account's device key in the installation wizard



# High Availability On-Premise Poller

- When an On-Premise Poller or its Network Module goes down, the resources associated with it will not be monitored until the On-Premise Poller is backed up
- This is where Site24x7's new High Availability feature comes in handy; you can associate another On-Premise Poller to act as a standby On-Premise Poller in case of downtime
- This *failover mechanism* ensures that monitoring is never interrupted by downtime of On-Premise Pollers



# Working of HA Poller

- When there is a change in the availability status of the On-Premise Poller or the Network Module, Site24x7 initiates a status check for the next three consecutive polls
- If the status does not return to Up, the monitoring resources associated with that On-Premise Poller will then be monitored from the standby On-Premise Poller



# Prerequisites

- The On-Premise Poller that is being associated as standby On-Premise Poller must not be in a down or suspended state
- The On-Premise Poller version should be 4.3.0 or above
- The On-Premise Poller should not have any monitor associated with it
- The standby On-Premise Poller must be of the same OS flavor as the primary On-Premise Poller
- The standby On-Premise Poller should not have any other On-Premise Poller associated as standby to it
- The On-Premise Poller should not be associated with another location profile (For example, the On-Premise Poller must not be associated with a location profile that contains global locations or multiple On-Premise Pollers)

# Monitoring from Standby On-Premise Poller

S24X7-NW-C4  

On-Premise Poller 

Last 24 Hours 

[Summary](#) [Network Module](#) [Outages](#) [Inventory](#) [Log Report](#)

100 % Availability	5 % JVM CPU	12 Associated Monitors	0 Downtimes	4.3.0 Version
-----------------------	----------------	---------------------------	----------------	------------------

**Root Cause Analysis:** Network Module is down.  
Create Request in ServiceDesk Plus [On-Demand](#) | [On-Premise](#) | [MSP](#)

**On-Premise Poller high availability**

Primary On-Premise Poller	Standby On-Premise Poller	Current high availability status
 S24X7-NW-C4 (This On-Premise poller)	 S24X7-NW-C3	Monitoring from Standby On-Premise poller

**Associated Monitors**

Monitor display name	Status	Performance	Last Polled
ESX [REDACTED]			12:21 PM
[REDACTED]		11.0 %	12:19 PM
datastore1			12:19 PM
VM demo-vm-root1			12:19 PM
VM demo-vm-root2			12:18 PM
VM demo-vm-rp1-v3			12:19 PM
VM demo-vm-v2			12:18 PM

# High Availability Status

Site24x7

Help Assistant

Inventory

User & Alert Management

Configuration Profiles

IT Automation Templates

Server Monitor

AppLogs

On-Premise Poller

High Availability

AWS

Mobile Network Poller

Azure

Operations

My Account

GCP

Subscriptions

Report Settings

Share

Developer

Milestones

Third-Party Integrations

Tags

Downloads

Advisor

Admin  
10:32

Search Monitors/Groups/Tags

High Availability

Primary On-Premise Poller	Standby On-Premise Poller	Current High Availability Status	Poll Now
Zyker-QA-1	Configure	-	↻
S247-US-b1	Configure	-	↻
S24X7-ANZ-P3	Configure	-	↻
Zyker-3	Zyker 1A	Monitoring from Primary On-Premise Poller	↻
Zyker-US-1C	Configure	-	↻
Zyker-remote	Configure	-	↻

High Availability Status

Configurations

Primary On-Premise Poller	Standby On-Premise Poller
S24X7-NW-C1	S24X7-NW-C3

Check Now

Monitors With Issue

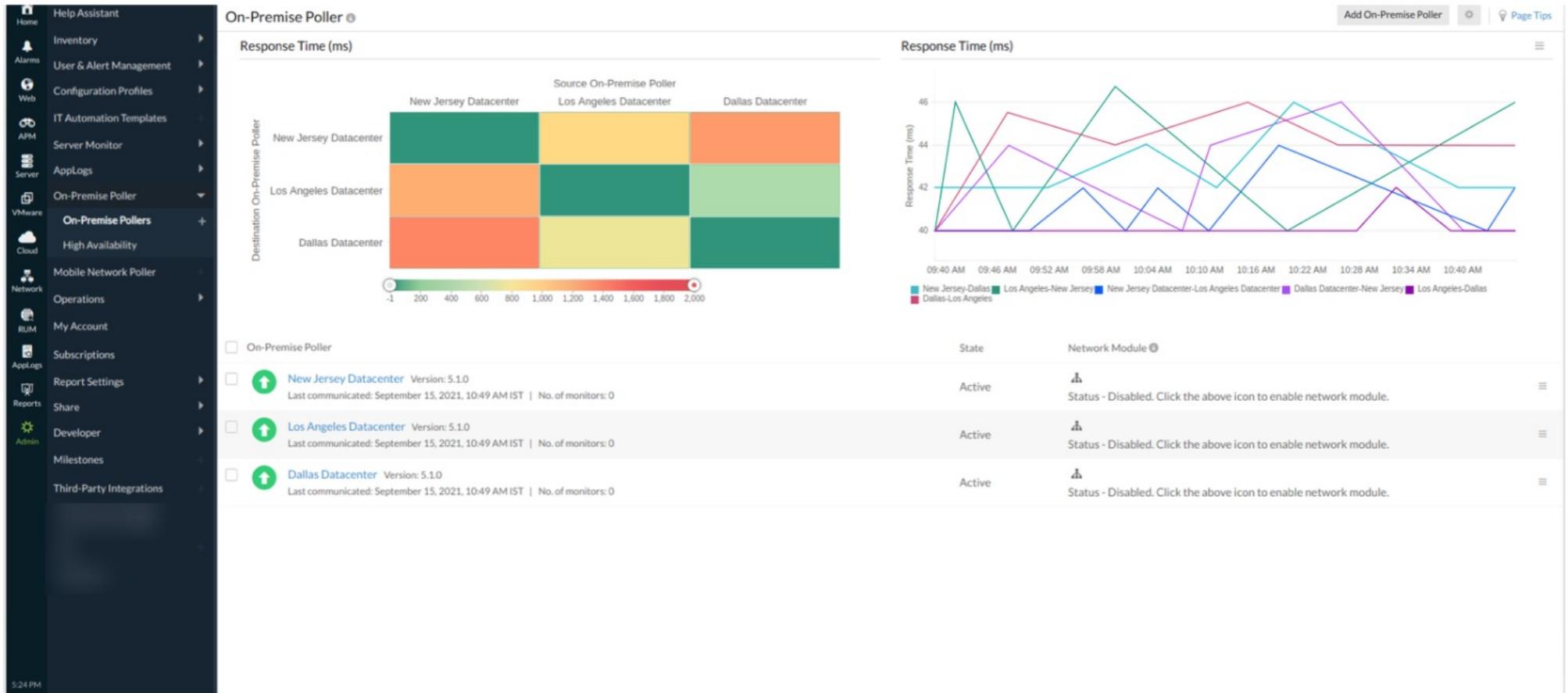
Monitor name	Monitor Type	Reason	Last updated
datastore	Datastore	Error in data collection.	Aug 7, 2019 12:09:06 PM
AP-03	Network Device	Device is not responding to the SNMP credential.	Aug 7, 2019 12:10:10 PM
Wireless AP-07	Network Device	Device is not responding to the SNMP credential.	Aug 7, 2019 12:10:10 PM
Wireless AP-02	Network Device	Device is not responding to the SNMP credential.	Aug 7, 2019 12:10:10 PM
Wireless AP-01	Network Device	Device is not reachable.	Aug 7, 2019 12:10:10 PM
SITE-W8-AIO-1	Network Device	Device is not reachable.	Aug 7, 2019 12:10:10 PM
VMware ESX/ESXi Server	VMware ESX/ESXi Server	Invalid User Name/Password.	Aug 7, 2019 12:09:06 PM



# Latency Dashboard

- Understand the availability, latency, and connectivity patterns between the geographically distributed On-Premise Pollers in your account
- Polls every 5 mins and calculates the response time between the other On-Premise Pollers

# Latency Dashboard





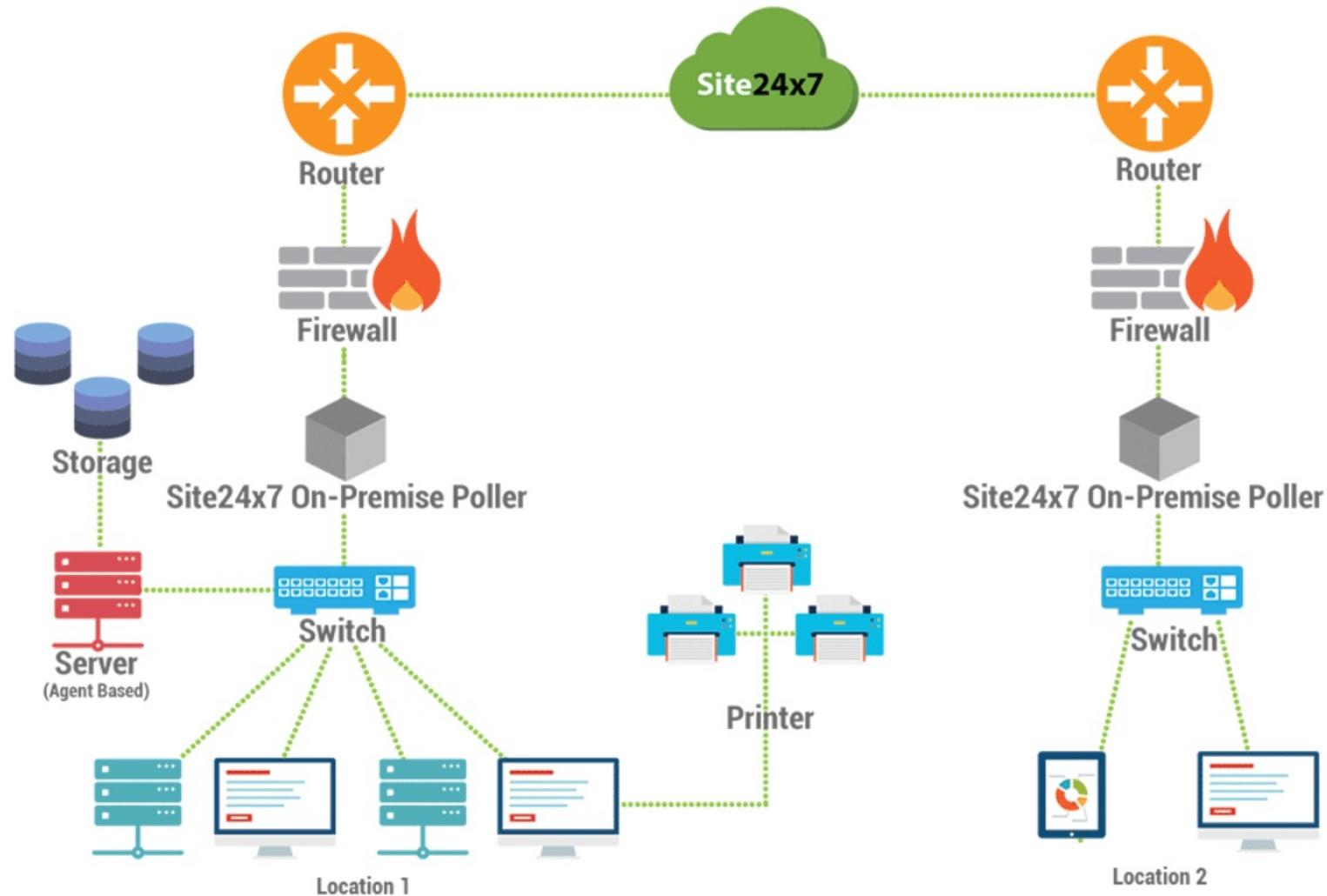
# Network Monitoring



# Network Monitoring - Introduction

- Built on the technical expertise of ManageEngine OpManager - with more than 15 years of experience in providing smarter, integrated network management solution
- Scalability - Monitor 1000s of Network devices
- Support for over 450 vendors and more than 10000 device types
- Automatic network discovery
- Robust monitoring for complex, distributed Networks
- Deep insights using SNMP performance counters

# Network Monitoring Architecture



# Enable Network Module

**Site24x7**

	Help Assistant	On-Premise Poller ⓘ	
Home	Inventory	On-Premise Poller	Network
Web	User & Alert Management	sushma-3222 (v1.4.4)	 Status - Up
Server	Configuration Profiles	Last updated on -   No. of monitors - 0	
Server	Server Monitor	site24x7-support2 (v1.4.3) 	 Status - Up
APM	On-Premise Poller	Last updated on -   No. of monitors - 12	 Status - Up
Alarms	Mobile Network Poller	SITE-W8-AIO-1 (v1.4.3) 	 Status - Up
Reports	Operations	Last updated on -   No. of monitors - 11	
Admin	My Account	JARAVIND-0557-T (v1.4.4)	 Status - Down
Admin	Subscriptions	Last updated on -   No. of monitors - 0	
Admin	Report Settings		

# Adding a Network Monitor Step 1

Network Discovery

Quick Help

Step 1 Step 2 Step 3 Step 4 Step 5 Step 6

On-Premise Poller Credentials Details Device Filters Interface Filters Discover

You need an [On-Premise Poller](#) to monitor your network devices.  
Choose an On-Premise Poller which has Network Module enabled in it.  
Ensure that the chosen On-Premise Poller and your network device are in the same network.

On-Premise Poller Name	IP Address	Number of Associated Monitors / Interfaces	Network Module ⓘ
site24x7poller	127.0.0.2	0 / 0	Status - Down
S24X7-NW-U3.csez.zohocorp.com	172.24.149.36	0 / 0	Status - Down
<b>S24X7-NW-U3</b>	172.24.149.36	8 / 1727	Status - Up
8825-test	192.168.56.1	0 / 0	Status - Down
8825-u20	172.24.143.178	0 / 0	Status - Down

Add a new On-Premise Poller

Next

# Adding a Network Monitor Step 2

Network Discovery

Step 1 Step 2 Step 3 Step 4 Step 5 Step 6

On-Premise Poller Credentials Details Device Filters Interface Filters Discover

Quick Help

Credentials help Site24x7 communicate via SNMP and fetch data for monitoring.  
Choose proper credentials according to your SNMP version.

<input type="checkbox"/>	Name	Type	Description	Action
<input checked="" type="checkbox"/>	Credential	SNMP v3	Credential	/
<input type="checkbox"/>	Training_SNMP	SNMP v1/v2	Training SNMP Printer	/
<input type="checkbox"/>	Public	SNMP v1/v2	-	/
<input type="checkbox"/>	ITOM	SNMP v1/v2	-	/
<input type="checkbox"/>	Traps_cred	SNMP v1/v2	-	/
<input type="checkbox"/>	VOIP	SNMP v1/v2	-	/
<input type="checkbox"/>	v3	SNMP v3	-	/

Add a new SNMP Credential

Back Next

# Adding a Network Monitor Step 3

Network Discovery

Step 1 Step 2 Step 3 Step 4 Step 5 Step 6

On-Premise Poller Credentials Details Device Filters Interface Filters Discover

You can discover and monitor a single device or a whole network.  
Select your discovery mode and enter details for discovery.

Discovery Mode  Add Device  Add Network

Discovery Type  Use IP Range  Use CIDR

IP Type  IPv4  IPv6

Start IP

End IP

NetMask

Tags

Back Next

# Adding a Network Monitor Step 4

Add Network Discovery Rule X

Name	Interface
Interface Types	Ethernet, Fast Ethernet
Admin State	Up, Down, Testing
Operational State	Up, Down, Testing, Unknown and <a href="#">1 more</a>
Description	To filter interfaces during discovery

[Save Rule](#)

# Adding a Network Monitor Step 5

Network Discovery

Step 1 Step 2 Step 3 Step 4 Step 5

On-Premise Poller Credentials Details Interface Filters Discover

Recheck your entries and click Discover to proceed.

On-Premise Poller	S24X7-NW-C1
Type	Network Device
IP Version	v4
Display Name	Switch
Host Name / IP Address	192.168.49.106
Credentials	Public
Discover Unknown Devices	No
Rule Selected	No rule selected

Back Discover



# Network Monitoring Setup - Auto Discovery

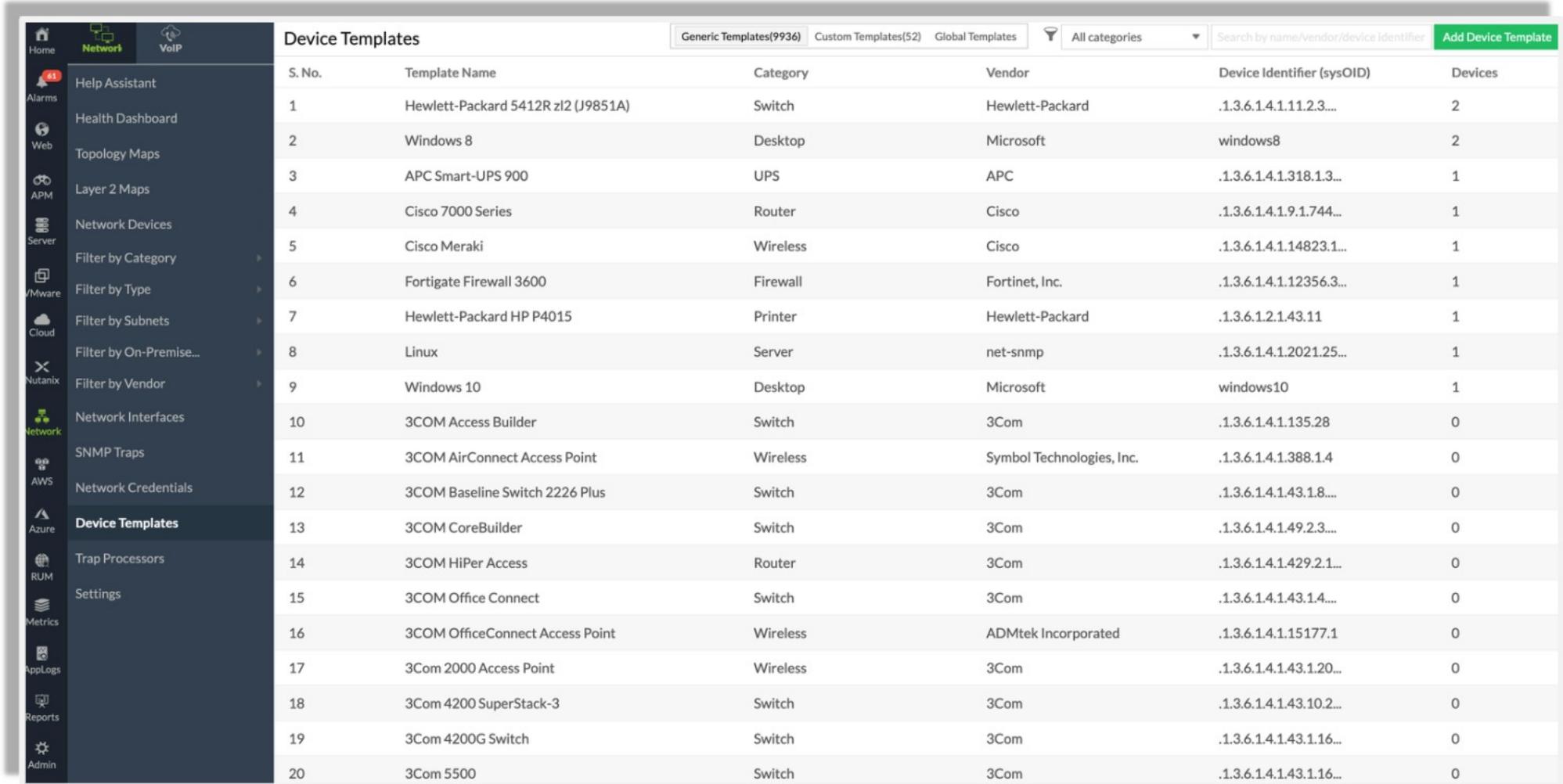
- Automatically discover all the devices present within a provided IP range or within a whole network using SNMP
- Once the devices are discovered, device templates are automatically associated
- Performance metrics of the device and interface status will be immediately displayed in the web console



## Supported vendors (Partial list)

- Alcatel, Barracuda Networks, Cisco, Canon Inc., Citrix Systems, Compaq, D-Link, Dell Inc., Epson, FortiGate, Hewlett Packard, Huawei, IBM, Intel Corporation, Juniper Networks, WatchGuard
- Additionally, with Site24x7 you can monitor new devices of any vendors by specifying the correct sysOID of the particular device

# Device Templates for Auto Discovery



The screenshot shows a network monitoring application's interface. On the left is a sidebar with various monitoring tabs: Home, Network (highlighted), VoIP, Alarms, Web, APM, Server, VMware, Cloud, Nutanix, Network (with Network Interfaces, SNMP Traps, AWS, Azure, Device Templates, Trap Processors, RUM, Metrics, AppLogs, Reports, Admin), and Admin. The main area is titled "Device Templates" and contains a table with the following data:

S. No.	Template Name	Category	Vendor	Device Identifier (sysOID)	Devices
1	Hewlett-Packard 5412R zl2 (J9851A)	Switch	Hewlett-Packard	.1.3.6.1.4.1.11.2.3....	2
2	Windows 8	Desktop	Microsoft	windows8	2
3	APC Smart-UPS 900	UPS	APC	.1.3.6.1.4.1.318.1.3...	1
4	Cisco 7000 Series	Router	Cisco	.1.3.6.1.4.1.9.1.744...	1
5	Cisco Meraki	Wireless	Cisco	.1.3.6.1.4.1.14823.1...	1
6	Fortigate Firewall 3600	Firewall	Fortinet, Inc.	.1.3.6.1.4.1.12356.3...	1
7	Hewlett-Packard HP P4015	Printer	Hewlett-Packard	.1.3.6.1.2.1.43.11	1
8	Linux	Server	net-snmp	.1.3.6.1.4.1.2021.25...	1
9	Windows 10	Desktop	Microsoft	windows10	1
10	3COM Access Builder	Switch	3Com	.1.3.6.1.4.1.135.28	0
11	3COM AirConnect Access Point	Wireless	Symbol Technologies, Inc.	.1.3.6.1.4.1.388.1.4	0
12	3COM Baseline Switch 2226 Plus	Switch	3Com	.1.3.6.1.4.1.43.1.8....	0
13	3COM CoreBuilder	Switch	3Com	.1.3.6.1.4.1.49.2.3...	0
14	3COM HiPer Access	Router	3Com	.1.3.6.1.4.1.429.2.1...	0
15	3COM Office Connect	Switch	3Com	.1.3.6.1.4.1.43.1.4....	0
16	3COM OfficeConnect Access Point	Wireless	ADMtek Incorporated	.1.3.6.1.4.1.15177.1	0
17	3Com 2000 Access Point	Wireless	3Com	.1.3.6.1.4.1.43.1.20...	0
18	3Com 4200 SuperStack-3	Switch	3Com	.1.3.6.1.4.1.43.10.2...	0
19	3Com 4200G Switch	Switch	3Com	.1.3.6.1.4.1.43.1.16...	0
20	3Com 5500	Switch	3Com	.1.3.6.1.4.1.43.1.16...	0



# Performance Counters

- View Performance Counters associated with the device like temperature stats, memory, CPU Utilization, etc
- Add Tabular Performance Counters manually or by using the in-built MIB browser
- Create a *Table View* by including two or more performance counters to view together in a table format and add alerts to see which tabular performance counter generates alerts
- For monitoring special attributes apart from the basic performance counters provided by the vendor, add Custom Performance Counters from generic MIBs or Custom MIBs

# Performance Counters

The screenshot shows the Site24x7 interface for monitoring an HP Switch (10.10.10.1). The left sidebar contains navigation links for Home, Network, NetFlow, NCM, Meralid, Help Assistant, Health Dashboard, Topology Maps, Layer 2 Maps, Network Devices, Filter by Category, Filter by Type, Filter by Subnets, Filter by On-Premise..., Filter by Vendor, Network Interfaces, SNMP Traps, VoIP Monitors, Network Credentials, Device Templates, Trap Processors, and Settings. The main content area displays performance metrics in cards:

Metric	Value
SysUpTime (Hours)	5,803
Network Interfaces (Nos)	244
IP Routing discards (Nos)	0
CPU Utilization ( Percentage)	7
Memory Utilization (Percentage)	27
Memory Used (bytes)	192,184,976

At the bottom, a note states: "Dashboard View created for N-PLZ-EAST-1F-YELLOW on July 6, 2022 5:21 PM Asia/Calcutta for the time period: July 5, 2022 5:21 PM Asia/Calcutta to July 6, 2022 5:21 PM Asia/Calcutta."

# Tabular Performance Counters

The screenshot displays a dashboard with four separate tables, each representing a different type of performance counter:

- Cisco Temperature**: Shows temperature readings in Celsius for various components. The data is as follows:

Name	Value (Celsius)	Action
Intake Right	14	▶ ⚒
Exhaust Left	24	▶ ⚒
Exhaust Right	18	▶ ⚒
CPU	40	▶ ⚒
Power Supply	34	▶ ⚒
Intake Left	12	▶ ⚒

- Used Memory**: Shows memory usage in KBytes. The data is as follows:

Name	Value (KBytes)	Action
.1	175,345	✎
.2	13,006	✎

- Free Memory**: Shows free memory in KBytes. The data is as follows:

Name	Value (KBytes)	Action
.1	68,359	✎
.2	23,857	✎

- CPU Utilization (5 min)**: Shows CPU utilization as a percentage. The data is as follows:

Name	Value (Percentage)	Action
.1	17	✎

# Table View for Performance Counters

The screenshot shows the Site24x7 network monitoring interface. The left sidebar navigation includes Home, Alarms, Web, APM, Server, VMware, Cloud, Network (selected), RUM, AppLogs, Reports, Admin, Edit, and Settings. The main header displays "Site24x7" and a search bar. The top right features a "Register here" button, "Plans and Pricing", and a help icon. Below the header, the device details for a "Router" at IP 10.10.10.1 are shown, along with a "Last 24 Hours" time range selector.

The navigation tabs include Device Performance, Interfaces, Traps, Performance Counters, Tabular Performance Counters (selected), Router Performance, Outages, and More. The "Tabular Performance Counters" section contains a table titled "ifTable".

Index	ifDescr	ifType	ifMtu	ifSpeed	ifPhysAddress	ifAdminStatus	ifOperStatus	ifLastChange
.1	Backplane-GigabitEthernet0/3	6 (ethernet-csmacd)	9,576	1,000,000,000	44 d3 ca 39 42 c3	1 (up)	1 (up)	2,211
.2	GigabitEthernet0/0	6 (ethernet-csmacd)	1,500	1,000,000,000	44 d3 ca 39 42 c0	1 (up)	2 (down)	2,211
.3	GigabitEthernet0/1	6 (ethernet-csmacd)	1,500	1,000,000	44 d3 ca 39 42 c1	1 (up)	1 (up)	3,723,031,115
.4	GigabitEthernet0/2	6 (ethernet-csmacd)	1,500	1,000,000,000	44 d3 ca 39 42 c2	1 (up)	1 (up)	3,852,402,616
.5	Embedded-Service-Engine0/0	6 (ethernet-csmacd)	1,500	10,000,000	00 00 00 00 00 00	1 (up)	2 (down)	213,335,213
.6	Null0	1 (other)	1,500	4,294,967,295		1 (up)	1 (up)	0
.20	Loopback51	24 (softwareLoopback)	1,514	4,294,967,295		1 (up)	1 (up)	2,468
.21	Loopback50	24 (softwareLoopback)	1,514	4,294,967,295		1 (up)	1 (up)	3,841,868,301
.11	Loopback0	24 (softwareLoopback)	1,514	4,294,967,295		1 (up)	1 (up)	3,987,692,883
.13	GigabitEthernet0/1.1	135	1,500	100,000,000	44 d3 ca 39 42 c1	1 (up)	1 (up)	3,723,031,015
.14	Loopback10	24 (softwareLoopback)	1,514	4,294,967,295		2 (down)	2 (down)	2,353

# Adding Custom Performance Counters - Scalar

**MIB BROWSER**

**GENERAL MIBS** **CUSTOM MIBS**

Vendor: RFC-Standard-MIBS

MIB: RFC1213-MIB

+ org

**SCALAR** **TABULAR** **TABLE VIEW**

SNMP OID:  Test

Name:

Description:

Unit:

Functional Expression:  None

Type:  Numeric  String

Save Absolute:  Yes  No

Format Value:  Yes  No

Show in Monitor Summary Page:  Yes  No

**Add** **Reset**

**Add Custom Performance Counters**

- Add custom performance counters to monitor any metric provided by your vendor in addition to default metrics available in Site24x7. Enter the SNMP OID and get started.
- The OIDs can be of the types numeric, string, or mathematical expressions.
- The performance counters can be either scalar or tabular. Scalar performance counters fetch individual values while the tabular performance counters fetch a column of values from a table.
- You can also create a table view and view multiple tabular performance counters grouped as a table.

**Help Links**

[Device Templates](#) | [Custom SNMP counters](#) | [Tabular Performance Counters](#)

# Adding Custom Performance Counters - Tabular

**MIB BROWSER**

**GENERAL MIBS** **CUSTOM MIBS**

Vendor: RFC-Standard-MIBS

MIB: RFC1213-MIB

+ org

**TABULAR** **SCALAR** **TABLE VIEW**

SNMP OID:  Test

Name:

Description:

Unit:

Functional Expression:  None

Type:  Numeric  String

Save Absolute:  Yes  No

Format Value:  Yes  No

Show in Monitor Summary Page:  Yes  No

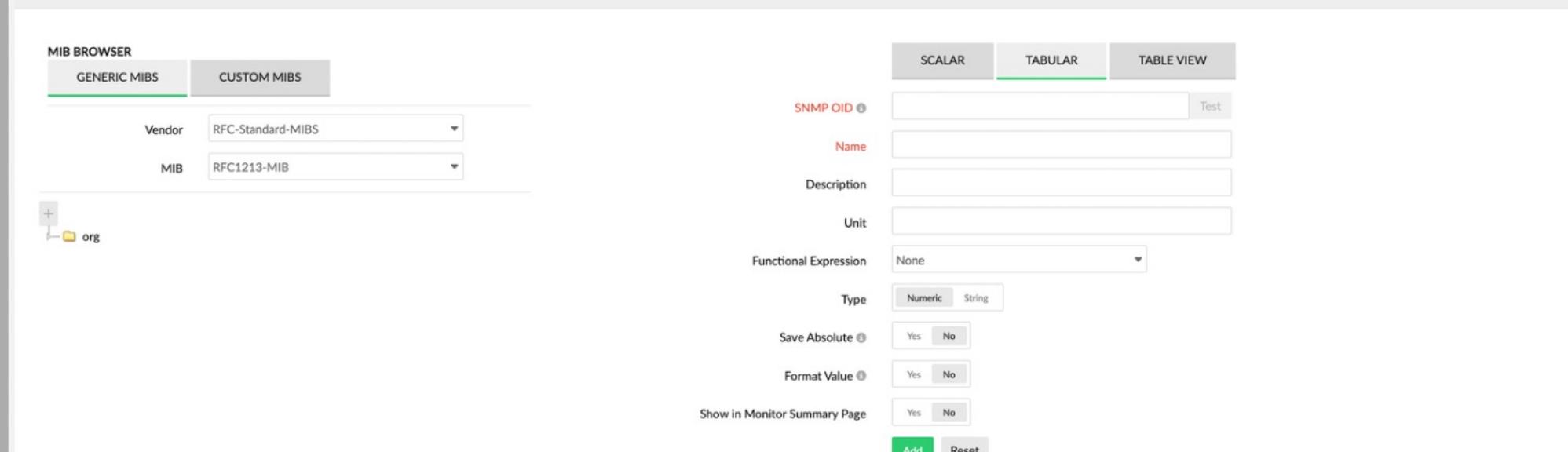
**Add** **Reset**

**Add Custom Performance Counters**

- Add custom performance counters to monitor any metric provided by your vendor in addition to default metrics available in Site24x7. Enter the SNMP OID and get started.
- The OIDs can be of the types numeric, string, or mathematical expressions.
- The performance counters can be either scalar or tabular. Scalar performance counters fetch individual values while the tabular performance counters fetch a column of values from a table.
- You can also create a table view and view multiple tabular performance counters grouped as a table.

**Help Links**

[Device Templates](#) | [Custom SNMP counters](#) | [Tabular Performance Counters](#)



# Adding Custom Performance Counters - Table View

The screenshot shows the configuration interface for adding custom performance counters. On the left, a hierarchical tree view displays MIB objects under the 'interfaces' section, specifically focusing on the 'ifTable' entry. On the right, the 'TABLE VIEW' tab is selected, showing a form to define a new table counter named 'ifTable'. The form includes options to 'Show in Monitor Summary Page' (set to 'Yes') and 'Show Index Column' (set to 'Yes'). Below this is a table titled 'Tabular Performance Counters' with four rows, each representing a column from the 'ifTable' MIB entry. The table has columns for S.No, Name, SNMP OID, and Unit. Each row also includes a 'Add To Table View' checkbox (all checked) and an 'Action' button.

S.No	Name	SNMP OID	Unit	Add To Table View	Action
1	ifDescr	.1.3.6.1.2.1.2.2.1.2	String	<input checked="" type="checkbox"/>	
2	ifType	.1.3.6.1.2.1.2.2.1.3	INTEGER	<input checked="" type="checkbox"/>	
3	ifMtu	.1.3.6.1.2.1.2.2.1.4	Integer	<input checked="" type="checkbox"/>	
4	ifSpeed	.1.3.6.1.2.1.2.2.1.5	Gauge	<input checked="" type="checkbox"/>	

**Add Custom Performance Counters**

- Add custom performance counters to monitor any metric provided by your vendor in addition to default metrics available in Site24x7. Enter the SNMP OID and get started.
- The OIDs can be of the types numeric, string, or mathematical expressions.
- The performance counters can be either scalar or tabular. Scalar performance counters fetch individual values while the tabular performance counters fetch a column of values from a table.
- You can also create a table view and view multiple tabular performance counters grouped as a table.

**Help Links**

[Device Templates](#) | [Custom SNMP counters](#) | [Tabular Performance Counters](#)

# Adding Custom Performance Counters - Table View (Cont..)

Add Custom Performance Counters

- ifInUnknownProtos
- ifOutOctets
- ifOutUcastPkts
- ifOutNUcastPkts
- ifOutDiscards
- ifOutErrors
- ifOutQLen
- ifSpecific

- at
- atTable
- atEntry
- atIndex
- atPhysAddress
- atNetAddress

- ip
- ipForwarding
- ipDefaultTTL
- ipInReceives
- ipInHdrErrors
- ipInAddrErrors

**SCALAR** **TABULAR** **TABLE VIEW**

Name

Show in Monitor Summary Page  Yes  No

Show Index Column  Yes  No

S.No	Name	SNMP OID	Unit	Add To Table View	Action
1	atPhysAddress	.1.3.6.1.2.1.3.1.1.2	PhysAddress	<input checked="" type="checkbox"/>	

Column of the Table View to be displayed in the Alert

**Add** **Reset**

**Add Custom Performance Counters**

- Add custom performance counters to monitor any metric provided by your vendor in addition to default metrics available in Site24x7. Enter the SNMP OID and get started.
- The OIDs can be of the types numeric, string, or mathematical expressions.
- The performance counters can be either scalar or tabular. Scalar performance counters fetch individual values while the tabular performance counters fetch a column of values from a table.
- You can also create a table view and view multiple tabular performance counters grouped as a table.

**Help Links**

[Device Templates](#) | [Custom SNMP counters](#) | [Tabular Performance Counters](#)

**Save** **Cancel**

# Adding Custom Monitor Metrics

If the Performance Counter value is not fetched with the default OIDs -



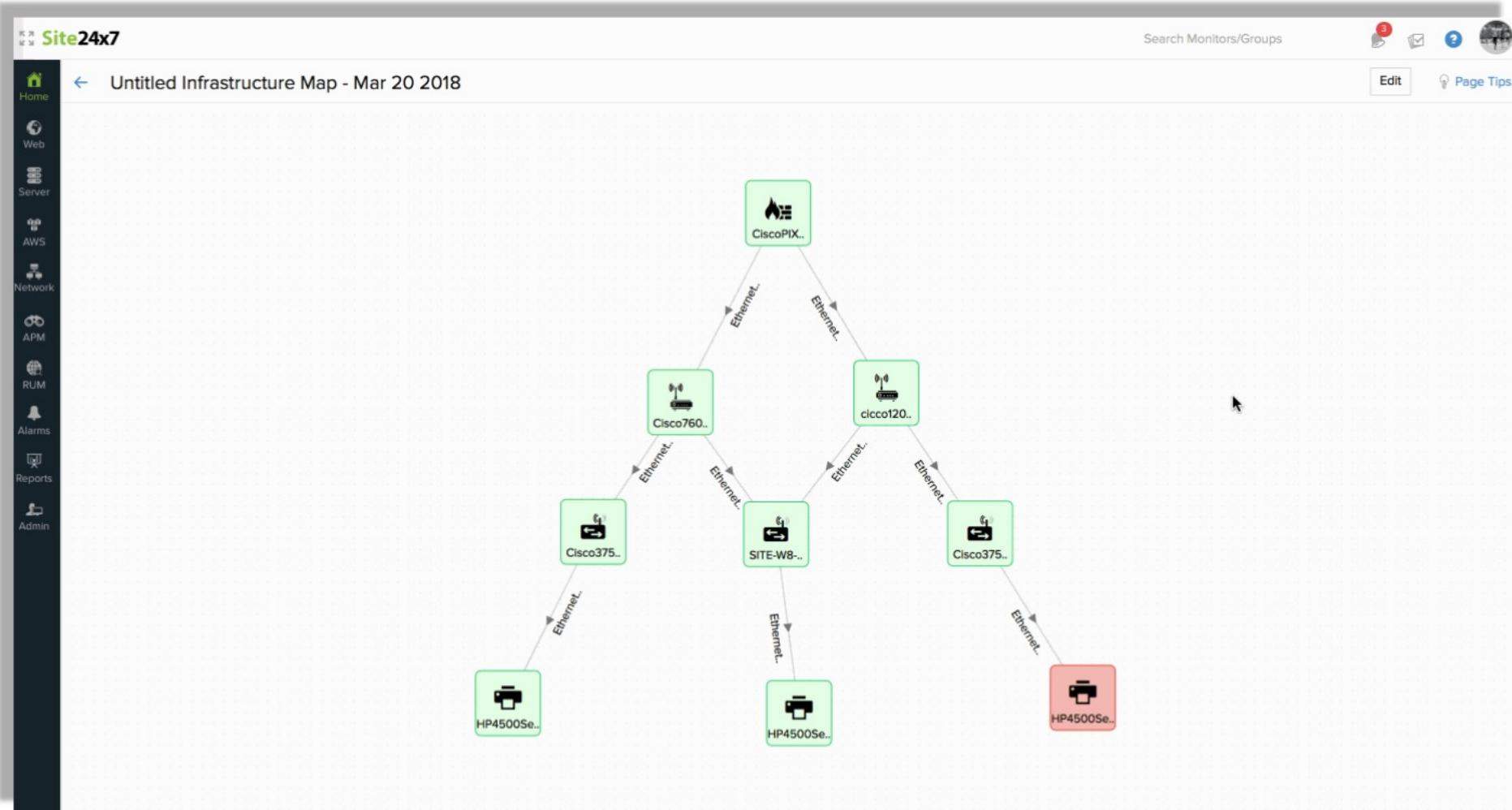
## Add Custom Monitor Metrics

Custom Monitor Metrics ⓘ X

CPU Utilization	None	<span style="border: 1px solid #ccc; padding: 2px;">Test</span>
Memory Utilization	None	<span style="border: 1px solid #ccc; padding: 2px;">Test</span>
Manufacturer	None	<span style="border: 1px solid #ccc; padding: 2px;">Test</span>
Serial Number	None	<span style="border: 1px solid #ccc; padding: 2px;">Test</span>
Model Name	None	<span style="border: 1px solid #ccc; padding: 2px;">Test</span>

Save Cancel

# Viewing Details from Layer 2 Maps





# SNMP Traps

- Get instant notifications on detection of hardware and network issues using traps
- Site24x7 On-Premise Poller listens to traps from network devices via port UDP 162
- Set the trap destination host address as the IP address or the host name of the respective On-Premise Poller
- Set the trap destination port to be 162
- Save the configuration



# Switch Stack Monitoring

- Monitor your switch stacks and the switches connected to them with switch stack monitoring
- Drilled down monitoring at switch-level to check its health, performance, and status
- Visualize the status of every switch and its connection on the data ring

# Switch Stack Monitoring Metrics Collected

Cisco 3850 Switch Last 24 Hours

10.10.10.3 Network Device

Device Performance **Stack** Interfaces Traps Performance Counters Tabular Performance Counters Outages More ▾

### Stack Data Ring

The diagram illustrates a stack data ring consisting of 8 Cisco 3850 switches. The switches are labeled Switch 1 through Switch 8. They are arranged in a circular pattern where each switch is connected to its immediate neighbors, forming a closed loop.

### Stack Details

**Bandwidth :** Full Redundancy  
**Master Switch :** Switch 1 (FSGE635)  
**Down/Trouble Switches :** 0

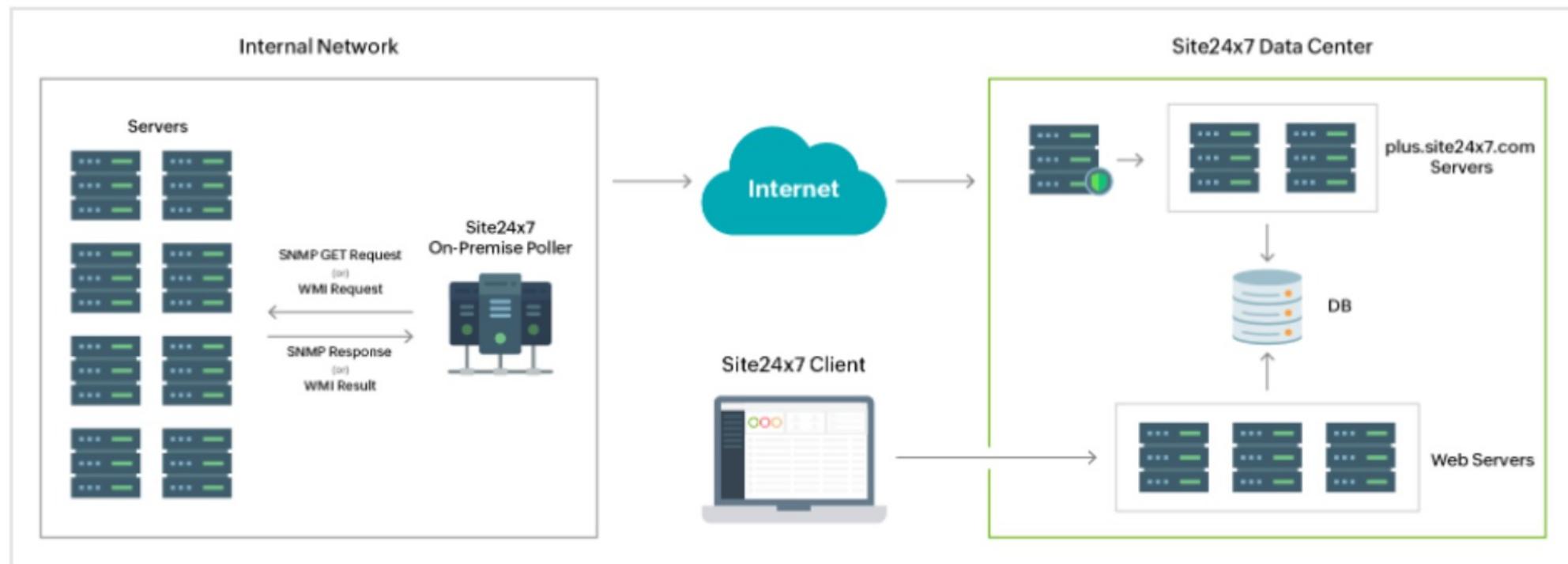
### Stack Switch Details

Switch Name	Role	State	MAC	Sw Priority	Hw Priority	Model	Serial No	Status	Action
Switch 1	Master	Ready	00 50 bf 07 ed 2d	2	0	WS-C3850-24P-S	FSGE635	<span style="color: green;">OK</span>	<span style="color: green;">Edit</span>
Switch 2	Member	Ready	24 50 a1 07 00 61	1	0	WS-C3850-24P-S	FOC2148	<span style="color: green;">OK</span>	<span style="color: green;">Edit</span>
Switch 3	Member	Ready	31 45 bf 07 11 12	1	0	WS-C3850-24P-S	G2Y6D	<span style="color: green;">OK</span>	<span style="color: green;">Edit</span>
Switch 4	Member	Ready	00 50 bf 07 ed 2d	1	0	WS-C3850-24P-S	SF36F	<span style="color: green;">OK</span>	<span style="color: green;">Edit</span>
Switch 5	Member	Ready	00 50 bf 07 ed 2d	1	0	WS-C3850-24P-S	HDG2D	<span style="color: green;">OK</span>	<span style="color: green;">Edit</span>
Switch 6	Member	Ready	00 50 bf 07 ed 2d	1	1	WS-C3850-24P-S	FW3J7	<span style="color: green;">OK</span>	<span style="color: green;">Edit</span>
Switch 7	Member	Ready	00 50 bf 07 ed 2d	1	1	WS-C3850-24P-S	SF36F	<span style="color: green;">OK</span>	<span style="color: green;">Edit</span>
Switch 8	Member	Ready	00 50 bf 07 ed 2d	1	1	MODEL	HFG46	<span style="color: green;">OK</span>	<span style="color: green;">Edit</span>

### Hardware Sensor Details

Sensor Name	Sensor Type	Sensor State	Sensor Value	Status	Action
Switch 1 - Temp Sensor 0	Temperature	Normal	20	<span style="color: green;">OK</span>	<span style="color: green;">Edit</span>
Switch 1 - Temp Sensor 1	Temperature	Normal	30	<span style="color: green;">OK</span>	<span style="color: green;">Edit</span>
Switch 1 - Temp Sensor 2	Temperature	Normal	39	<span style="color: green;">OK</span>	<span style="color: green;">Edit</span>

# SNMP and WMI based Agentless Server Monitoring



SNMP and WMI Server Monitoring Architecture



# NetFlow Analyzer



# NetFlow Analyzer - Introduction

- Obtain complete visibility into your network traffic and bandwidth performance in real time
- Identify traffic peaks, top applications, and conversations using different flow technologies so that you can analyze for what and by whom your bandwidth is being used



# Prerequisites

- To perform network traffic analysis using Site24x7, you must install an On-Premise Poller (version: 4.6.0 or above) in the network being monitored
- The devices should be able to export flows to Site24x7



# Supported Flows

→ NetFlow

→ J-Flow

→ SFlow

→ IPFIX

→ NetStream

→ AppFlow

→ CFlow



# Adding a device to monitor NetFlow

- ....> Choose an On-Premise Poller
- ....> Configure the devices to export flows  
(Flow export configuration - Automatic/Manual)
- ....> Choose devices and interfaces
- ....> Organize your monitors and configure profiles
- ....> Verify your entries and export flows for monitoring

# Adding a device to monitor NetFlow

The screenshot shows the Site24x7 interface for configuring a flow export. The left sidebar contains navigation links for Home, Alarms, Web, APM, Server, VMware, Network, RUM, Metrics, Reports, Admin, and various monitoring and management sections. The main area is titled "Flow Export" and shows a five-step process: Step 1 (On-Premise Poller), Step 2 (Flow Export Configuration, currently selected), Step 3 (Choose Devices), Step 4 (Configuration Profiles), and Step 5 (Add). The "Flow Export Configuration" step is detailed below:

**Automatic Flow Export** Manual Flow Export

Provide your device's host name, SSH/CLI, and SNMP credentials using which we will automatically configure your devices to export flows to Site24x7.

Skip this step if you have configured your devices to export flows already.

Hostname/IP Address: 10.10.10.3

SSH/Telnet Credential: CiscoRouterSSH

SNMP Credential: Public

Connect

Site24x7 has connected to your device successfully. Choose a Source Interface and execute the below commands.

Source Interface: One

Device Vendor/Type: Cisco\_IOS\_Router

Command Set: CiscoRouter\_FlowExport

Export Commands:

```
Config  
ip flow-export destination 172.24.147.201 9996  
ip flow-export source One  
in flow-export version 5
```

# Adding a device to monitor NetFlow

The screenshot shows the Site24x7 interface for configuring NetFlow monitoring. The left sidebar contains navigation links for Home, Help Assistant, Inventory, Alarms, Web, APM, Server, VMware, Cloud, Network, RUM, Reports, and Admin. The Admin section is currently selected. The main content area is titled "Flow Export" and displays a six-step wizard. Step 4, "Choose Devices", is active, indicated by a blue dot on the timeline. Below the timeline is a table titled "Select interfaces in each device." It lists devices and their interfaces, with checkboxes for selecting specific interfaces.

Device Name	IP Address	Device Type	Interface Count	Flow Type
2.2.2.2	2.2.2.2	Router	4	V9
Interface Name	Interface Type	Interface Index	In Speed	Out Speed
<input type="checkbox"/> IfIndex3	Others	3	1,000.00 K	1,000.00 K
<input checked="" type="checkbox"/> IfIndex1	Others	1	1,000.00 K	1,000.00 K
<input checked="" type="checkbox"/> IfIndex4	Others	4	1,000.00 K	1,000.00 K
<input type="checkbox"/> IfIndex2	Others	2	1,000.00 K	1,000.00 K
<input checked="" type="checkbox"/> 2.2.2.1	2.2.2.1	Router	4	V9
<input type="checkbox"/> 2.2.2.3	2.2.2.3	Router	4	V9
<input type="checkbox"/> 2.2.2.4	2.2.2.4	Router	4	V9

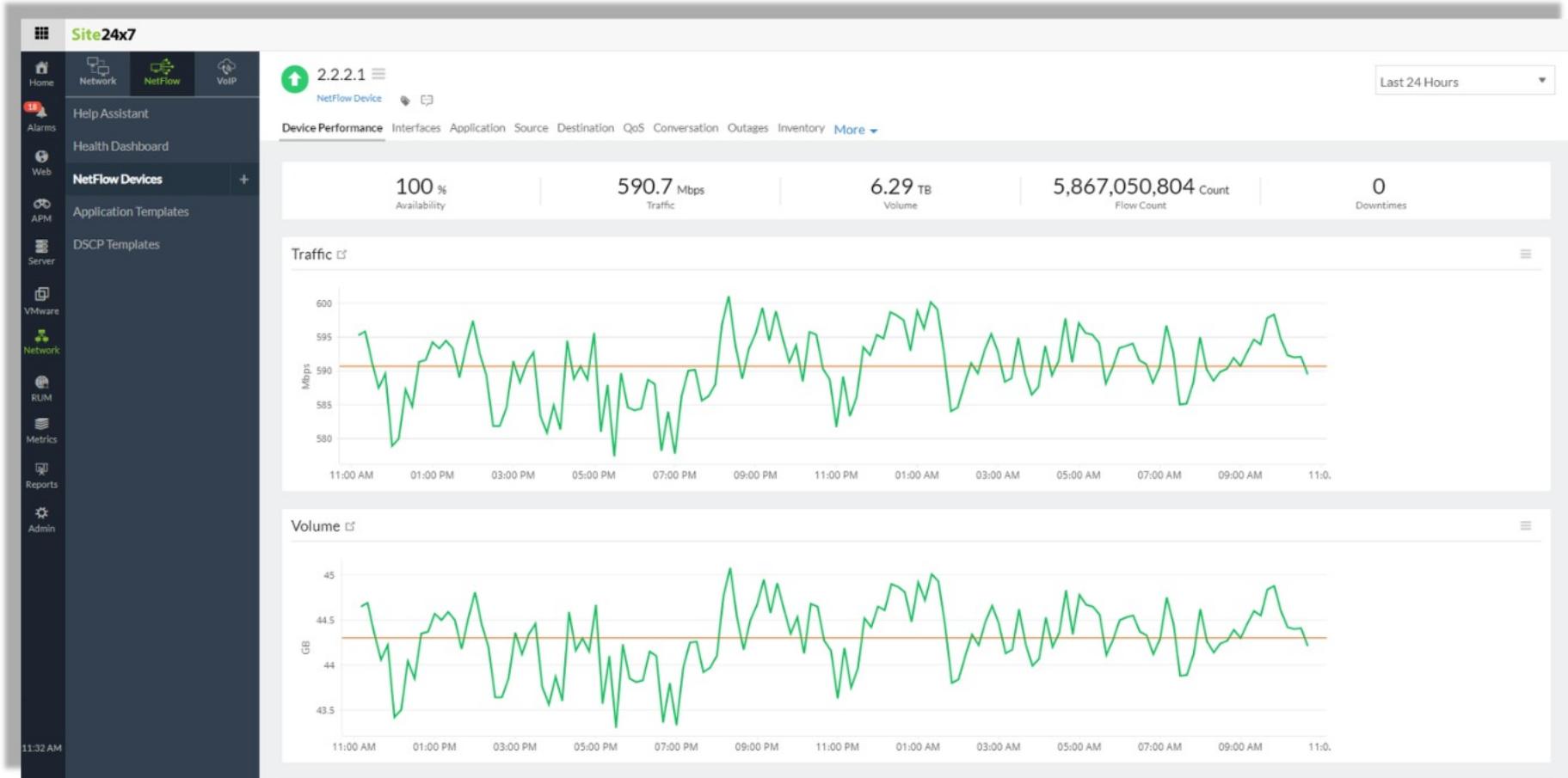
Buttons at the bottom right include "Back" and "Next".



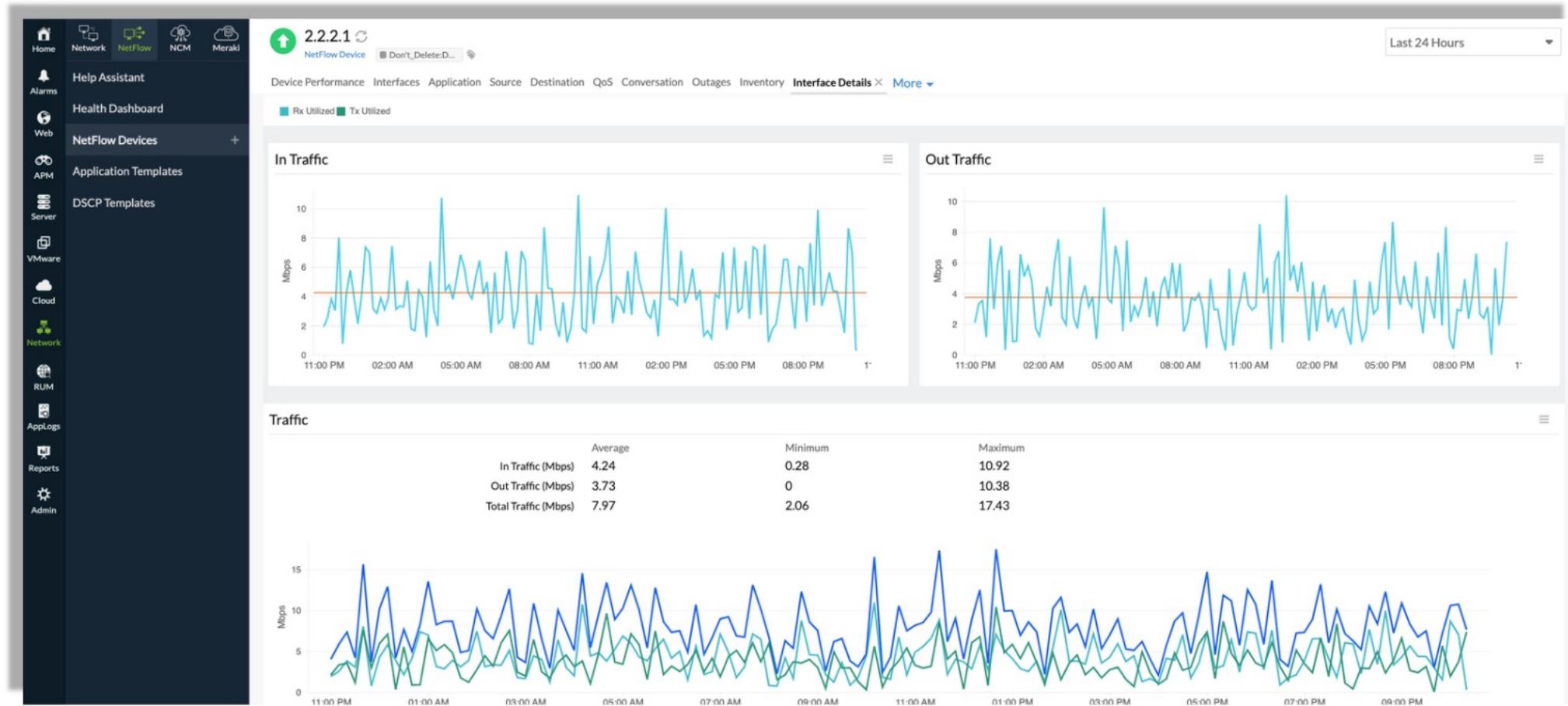
# Supported Templates

- …→ Application Templates
- …→ DSCP Templates

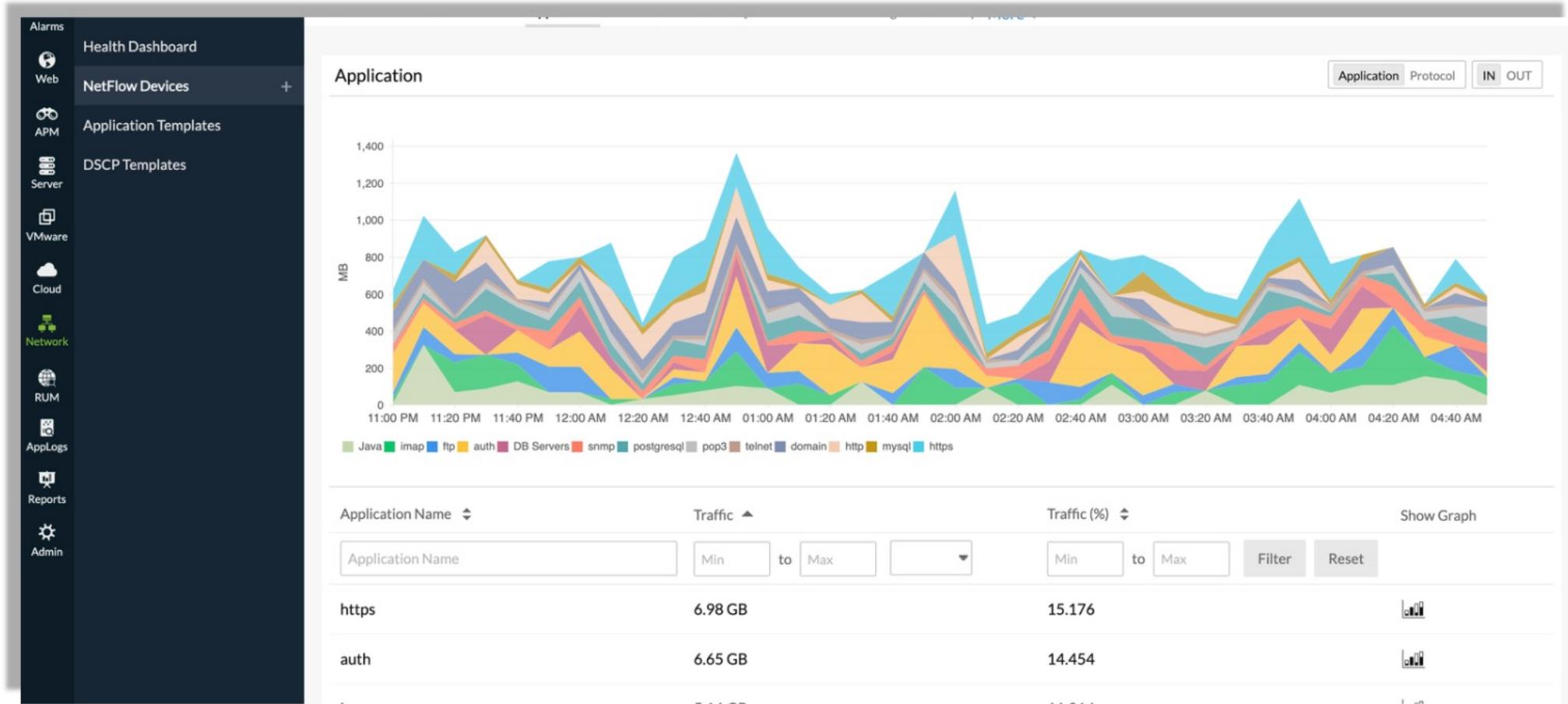
# NetFlow: Device Metrics



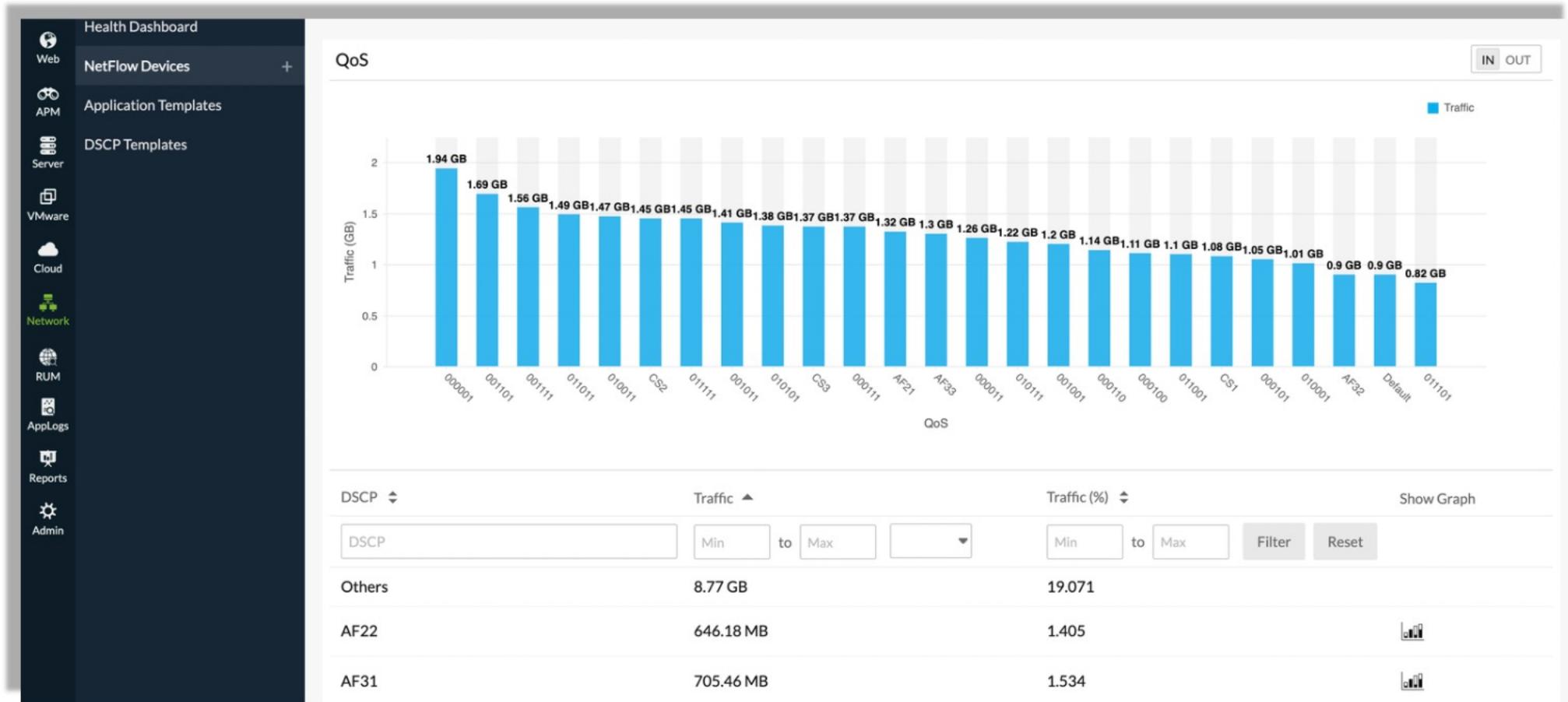
# NetFlow: Interface Metrics



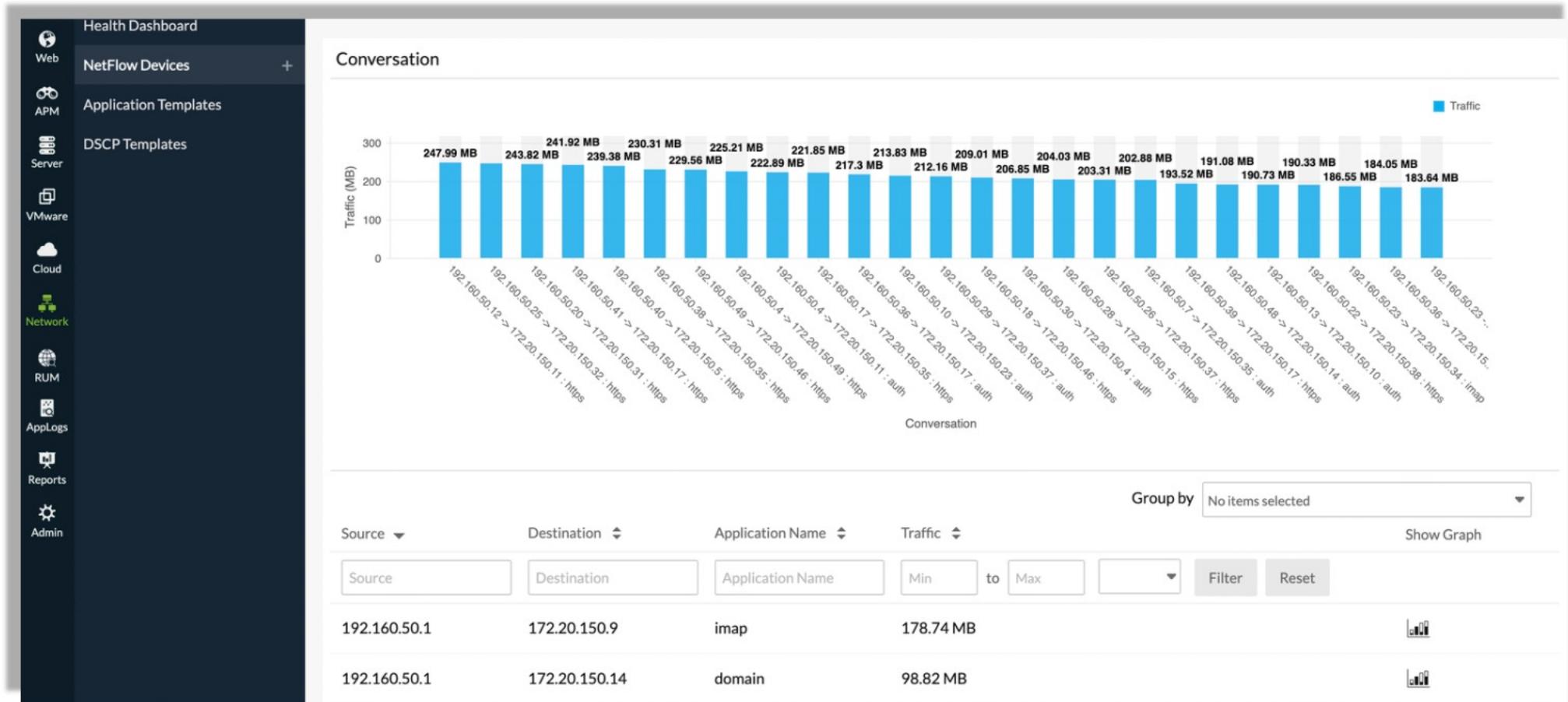
# NetFlow: Application Metrics



# NetFlow: QoS Metrics



# NetFlow: Conversation Metrics





# Network Configuration Manager



# Network Configuration Manager - Introduction

- Multi-vendor network device change and configuration management tool
- Allows you to
  - Continuously track and alert on the configuration changes
  - Compare configuration versions
  - Perform audits
  - Restore configurations
  - Automate device configuration backups



# Prerequisites

- On-Premise Poller version 5.2.0 or above

# System Requirements

Maximum no. of devices per On-Premise Poller Processor	RAM	Disk space for aggregate data
100	4 processors	8 GB 100 GB or higher
500	8 processors	16 GB 100 GB or higher

## Port Requirements

Port health	Default port number
TFTP port	69
SSHD port	22
Telnet port	23
Syslog server	514



# Enable Network Configuration Manager

- Log in to your Site24x7 account
- Navigate to Network > NCM > Settings
- Once the Manage NCM page pops up, choose an On-Premise Poller from the drop-down
- Toggle to Enable
- Wait 5-10 minutes
- Navigate to Admin > On-Premise Poller and ensure that the On-Premise Poller and the network module are running

# Add devices

Site24x7 /admin-actions

Help Assistant

Inventory

- Add Monitor
- Monitors
- Monitor Groups
- Import Monitors
- Export Monitors
- Configuration Rules

Bulk Action

User & Alert Management

Cloud

Network

- IT Automation Templates
- Server Monitor
- AppLogs
- On-Premise Poller
- Mobile Network Poller

RUM

Metrics

AppLogs

Operations

Reports

My Account

Control Panel Settings

Subscriptions

Report Settings

Share

Developer

14:35

## Edit NCM Device

Display Name: Zylker HP Switch

Host Name: 192.168.49.4

IP Address: 192.168.49.4

Vendor: HP

Device Template: HP Procurve Switch

Protocol: SSH - TFTP

Primary Credential: HP\_Switch\_SSH (SSH)

+ Test Credential

SNMP Credential: Public

+ +

Check Frequency: 1 hr

Monitoring Locations: Profile S24X7-NW-U3.csez.zohocorpin.com

+ S24X7-NW-U3.csez.zohocorpin.com

Monitor Groups: No items selected

Dependent on Monitor: No items selected

Save Cancel Suspend Delete Page Tips

Configuration Profiles

# Device templates

The screenshot shows the Site24x7 interface for managing device templates. The left sidebar has a dark theme with various monitoring categories like Home, Network, NetFlow, NCM, APM, Server, VMware, Cloud, Network, RUM, Reports, Admin, and Edit. The 'Device Templates' option is selected. The main content area is titled 'Device Template: Cisco IOS Router'. It shows vendor information (Cisco), OS (IOS), and a description ('For all Cisco IOS Routers'). Below this, there are sections for 'Backup Running Configuration', 'Backup Startup Configuration', 'Disable Syslog Change Detection', and 'Enable Syslog Change Detection', each listing commands, timeout values (20000 ms), and line feed types (LF or LineFeed). The bottom left corner shows the time as 2:24 PM.

Command	Timeout (ms)	LineFeed
terminal length 0	20000	LF
show running-config	20000	LF

Command	Timeout (ms)	LineFeed
terminal length 0	20000	LF
show startup-config	20000	LF

Command	Timeout (ms)	LineFeed
configure terminal	20000	LF
no logging \${UserInput:HostIpAddress}	20000	LF
end	20000	LF

Command	Timeout (ms)	LineFeed
configure terminal	20000	LF
logging on	20000	LF
logging \${UserInput:HostIpAddress}	20000	LF
logging trap \${UserInput:LoggingLevel}	20000	LF
end	20000	LF

# Current configurations

Search by monitor name/config type/version | Page Tips

Monitor Name	Type	Version	Captured On	Change Type	Action
10.10.10.16	Startup	2	Mon Nov 01 19:17:52 IST 2021	Authorized	≡
10.10.10.16	Running	2	Mon Nov 01 19:17:52 IST 2021	Authorized	≡
10.10.10.18	Running-Baseline	1	Fri Oct 29 11:33:47 IST 2021	Authorized	≡
10.10.10.18	Running	3	Fri Oct 29 11:33:47 IST 2021	Authorized	≡
10.10.10.18	Startup-Baseline	1	Fri Oct 29 11:33:47 IST 2021	Authorized	≡
10.10.10.18	Startup	3	Fri Oct 29 11:33:47 IST 2021	Authorized	≡
10.10.10.14	Startup	2	Fri Oct 29 10:48:29 IST 2021	Authorized	≡
10.10.10.16	Running-Baseline	1	Fri Oct 29 10:48:29 IST 2021	Authorized	≡
10.10.10.14	Running	2	Fri Oct 29 10:48:29 IST 2021	Authorized	≡
10.10.10.16	Startup-Baseline	1	Fri Oct 29 10:48:29 IST 2021	Authorized	≡
10.10.10.14	Startup-Baseline	1	Thu Oct 28 19:44:13 IST 2021	Authorized	≡
10.10.10.14	Running-Baseline	1	Thu Oct 28 19:44:13 IST 2021	Authorized	≡

Click the hamburger icon to view options.

- Mark as unauthorized
- Edit description
- Compare with startup
- Compare with running
- Compare with previous
- Compare with any
- Upload configuration

# Compare configurations

The screenshot shows the 'Compare Configurations' feature in Site24x7. On the left, there's a sidebar with various monitoring tabs: Home, Alarms, Web, APM, Server, VMware, Cloud, Network (highlighted in green), RUM, Metrics, Reports, Admin, and Edit. The timestamp at the bottom is 11:35 AM.

The main interface has two sections: L.H.S (Left Hand Side) and R.H.S (Right Hand Side). Both sections have dropdown menus for 'Select Device', 'Select Config Type', and 'Select Version'. The L.H.S section shows a configuration for device 10.10.10.14 with a startup-baseline configuration, version 1, and a changed date of Thu Oct 28 19:44:13 IST 2021. The R.H.S section shows a configuration for device 10.10.10.18 with a running configuration, version 3, and a changed date of Fri Oct 29 11:33:47 IST 2021.

The central area is titled 'Diff View' and displays a list of configuration differences. The list is color-coded: red for additions, blue for modifications, and orange for deletions. The differences are:

- L.H.S (1)
  - 3 Building configuration...
  - 4
  - 5 Current configuration:
  - 10 !
  - 11 hostname Cisco360044
  - 12 !
  - 16 !prompt Cisco360044#
  - 19 ip address 10.10.10.14
  - 20 cdp enable
  - 21 mtu 1500
  - 25 cdp enable
  - 28 interface Serial0
  - 29 ip address 10.10.10.14
  - 30 mtu 1800
  - 31 !
  - 32 interface Serial0
  - 33 ip address 127.0.0.1
  - 34 mtu 1800
  - 35 !
  - 36 interface Serial1
  - 37 ip address 10.10.10.14
  - 38 mtu 1500
  - 39 !
- R.H.S (2)
  - !hostname Cisco360046
  - !prompt Cisco360046#1
  - ip address 10.10.10.18
  - no cdp enable
  - mtu 15001
  - no cdp enable
  - ip route 0.0.0.0 0.0.0.0 10.10.10.18

At the top right, there are checkboxes for 'Added (0)', 'Modified (84)', and 'Deleted (3)'. Below them are two buttons: 'Diff Only' (highlighted with a red border) and 'All Lines'.

A purple callout box on the right side of the interface says: 'View differences or all lines between two configurations.'



# VoIP Monitoring



# VoIP Monitoring

- With Site24x7, you can assess the quality of VoIP call services throughout the call path using Cisco Internet Protocol Service Level Agreement (IPSLA)
- Analyzing the network and the call transmission across the call path will help to troubleshoot and rectify issues



# Prerequisites

- Install Site24x7 On-Premise Poller
- Both the source and the destination devices should be a Cisco switch, firewall, or router
- The Cisco Internetwork Operating System (IOS) version should be 12.4 or later
- Enable IPSLA in the destination device
- The source device and the interface should be monitored by Site24x7 with SNMP read-write community credentials



# Cisco Meraki Monitoring

# SNMP-based

Meraki Cloud Controller  

10.10.10.1 Network Device 

Last 24 Hours 

Device Performance Interfaces Traps Performance Counters **Tabular Performance Counters** Outages More ▾

Tabular Performance Counters Add Performance Counters Threshold Configuration Bulk Action Last 24 Hours Last Polled Active Suspended

Devices						
Device Name	Device Status	Connected Clients	Mesh Status	Device Serial	Device MAC	Device Product Description
Florida-GW01	1 (Online)	12	0 (Gateway)	WX26-S2ZY-YUUZ	73 74 72 69 6e 70	Gateway Appliance
Florida-AP02	1 (Online)	18	0 (Gateway)	WXU3-UE2D-OSNK	73 74 72 69 6e 6f	Access Point
Florida-AP01	1 (Online)	23	0 (Gateway)	WXNH-N705-8RIV	73 74 72 69 6e 6e	Access Point
Texas-AP02	1 (Online)	10	0 (Gateway)	WXWP-C0D4-HYN0	73 74 72 69 6e 69	Access Point
Texas-AP01	1 (Online)	24	0 (Gateway)	WX3W-Y5WU-2TLN	73 74 72 69 6e 68	Access Point
Florida-SW01	1 (Online)	2	0 (Gateway)	WXXQ-R142-PD3R	73 74 72 69 6e 71	Switch
Texas-SW02	1 (Online)	18	0 (Gateway)	WXFJ-SJL8-V7WU	73 74 72 69 6e 6d	Switch
Texas-SW01	1 (Online)	10	0 (Gateway)	WXM3-23R7-NQ5E	73 74 72 69 6e 6c	Switch
Texas-GW01	1 (Online)	3	0 (Gateway)	WXY5-U1LD-CWK2	73 74 72 69 6e 6b	Gateway Appliance
Texas-AP03	1 (Online)	2	0 (Gateway)	WXTW-BRQY-5X8N	73 74 72 69 6e 6a	Access Point

# REST API-based

The dashboard displays the status of various Meraki devices and networks:

- Monitors in Monitor Type:** Meraki Camera, Meraki Organization, Meraki Security Appliance, Meraki Switch & Meraki Wireless.
- Status Legend:** Green indicates healthy status, while red indicates an issue.
- Device Status:**
  - 1st Floor AP, 2nd Floor AP, ap01-dl3, Basement AP, Basement switch1, Bedroom Switch, Big Office Switch, BigCat, CLUS18-SmartCity, DevNetAssoc, First Floor Switch, Forest City - Other, Front Desk Surveillance, Meraki Five, ms01-dl1, ms01-dl2, ms01-dl3, MX-Zylker-01, MX-Zylker-02, mx01-dl1, mx01-dl2, Office AP, Reception Surveillance, Second Floor Switch, Sun Room, Terminal Tower - IDF2-AP13.
  - test, Vegas Balcony MR84, Vegas Living Room MR84, Zylker Organization.
- Performance Metrics:**
  - Packet Loss of mx01-dl1: Shows a flat line at 0% loss from 07:11 to 12:41.
  - Response Time of mx01-dl1: Shows a constant response time around 8ms with minor fluctuations.



# Prerequisites

- The Meraki REST API key generated in your Cisco Meraki dashboard needs to be granted read-only access to Site24x7.

# Add Meraki organization & Devices to be monitored

Meraki Monitoring 💡 Page Tips

Step 1 Step 2 Step 3 Step 4

Details Choose Meraki Organization Select Meraki Devices Discover

Choose the organization to be monitored.  
Click Next to view the devices available in the organization.

Organization Name	Organization ID	Organization URL
<input checked="" type="radio"/> DeLab		
<input type="radio"/> DevNet Sandbox		
<input type="radio"/> My organization		
<input type="radio"/> Xirg		
<input type="radio"/> "New Network"		
<input type="radio"/> Test_org		

# Add Meraki organization & Devices to be monitored

Meraki Monitoring

[Page Tips](#)

Step 1



Details

Step 2



Choose Meraki Organization

Step 3



Select Meraki Devices

Step 4



Discover

Choose the devices to be monitored.

The devices added will be monitored using Cisco Meraki REST APIs.

<input checked="" type="checkbox"/>	Status	Name	Device Serial	Device Model	Network Name
<input checked="" type="checkbox"/>				MR84	Lyoli
<input checked="" type="checkbox"/>				MS220-8P	Lyoli
<input checked="" type="checkbox"/>				MS220-8P	Lyoli
<input checked="" type="checkbox"/>				MR52	Lyoli
<input checked="" type="checkbox"/>				MR52	Lyoli
<input checked="" type="checkbox"/>				MR52	Lyoli
<input checked="" type="checkbox"/>				MR52	Lyoli
<input checked="" type="checkbox"/>				MS250-48FP	Lyoli
<input checked="" type="checkbox"/>				MX250	Lyoli
<input checked="" type="checkbox"/>				MV71	Vegas Apartment



# VMware Monitoring



# VMware Monitoring - Introduction

- Automatically discover and map your entire vSphere environment, from data centers to VMs, in real time
- Monitor different CPU, memory, disk, and network metrics from time to time to understand how each component is performing
- Obtain performance metrics at the host level, VM level, and guest OS level, and correlate them for complete VMware performance monitoring
- Avoid resource contention and optimize resource allocation so you can ensure your capacity planning is also accurate

# VMware vCenter Monitoring

- Auto-discover your entire virtual infrastructure through VMware vCenter and visualize critical metrics in one view
- Prerequisites:
  - > Site24x7 On-Premise Poller
  - > Access to Managed Object Browser
  - > VMware Read-only or Administrator roles to monitor vCenter

VMware resources	Privilege	Reason
vCenter	No additional privileges are required	
ESX/ESXi host	No additional privileges are required	
Virtual machine (VM)	<i>Interact.PowerOff</i> , <i>Interact.PowerOn</i> , and <i>Interact.Reset</i> for the connected ESX/ESXi host	To stop, start, and reset VMs for the Site24x7 console
Datastore	<i>Browse</i> and <i>Config</i> for all connected ESX/ESXi hosts	To perform basic monitoring
Resource pool	No additional privileges are required	
All types	<i>System.Read</i> , <i>System.View</i> , and <i>System.Anonymous</i>	Default privileges for <b>Read Only</b> role.

- Reference:<https://support.site24x7.com/portal/en/kb/articles/vmware-privileges-required>

# Different types of polling for VMware resources

- **VMware vCenter-based polling :** Here, you can provide your vCenter credentials, and Site24x7 use the same to monitor all the associated ESX/ESXi host, VMs, datastores, Snapshots, hardware, and resource pools
- vCenter-based polling works from On-Premise Poller version 4.6.4. Hence, upgrade your On-Premise Poller to this version or the latest
  
- **VMware ESX/ESXi-based polling :** In this case, you need to create user credentials at each ESX/ESXi host level and enable the required privileges
- This has to be done at the individual ESX/ESXi host level to monitor the ESX/ESXi host and its associated VMs, datastores, Snapshots, hardware, and resource pools
- You can choose the type of polling while adding the ESX/ESXi host monitors



# VMware ESX/ESXi Monitoring

- Gain in-depth insights on critical performance metrics of CPU, memory, disk, datastore, and network of your ESX/ESXi servers
- You can also add your VMware datastores and resource pools for monitoring while adding ESX/ESXi hosts
- Prerequisites:
  - > Site24x7 On-Premise Poller
  - > Access to Managed Object Browser
  - > VMware Read-only or Administrator roles to monitor ESX/ESXi servers



# VMware VM Monitoring

- Track the performance of your virtual environment and gain exhaustive reports on disk I/O, datastore, network and memory of virtual servers
- You will need to add an ESX/ESXi host first, and this will in turn discover the VMs mapped to it
- Prerequisites:
  - > Site24x7 On-Premise Poller
  - > VMware Read Only or Administrator roles along with Interact.PowerOff, Interact.PowerOn, and Interact.Reset privileges for the connected ESX/ESXi host

# VMware VM Monitor and Server Monitor Integration

→ If you're monitoring your VMware virtual machines (VMs) via both Site24x7 VMware Monitoring and the server agent, you can integrate both for a unified view of VM metrics, as well as guest OS metrics

## → **Benefits**

By integrating your VM and server monitors, you'll be able to view the following additional metrics for your VMware VM monitor:

- > CPU, memory, thread count, and handle count of all your Windows services
- > CPU and memory use, number of instances, thread count, and handle count of all your processes
- > Additional guest OS network-level metrics like data sent, data received, packets sent, packets received, and bandwidth
- > You can also perform URL checks, port checks, file checks, directory checks, and NFS checks
- > From the Tools tab, you can execute commands and WMI queries
- > You will also receive support for Site24x7 AppLogs



# How to integrate?

- To integrate, your VM should be monitored both via the server agent and Site24x7 VMware Monitoring
  - 1. Go to the VMware tab
  - 2. Click on the desired VM monitor name
  - 3. Go to the Processes tab
  - 4. Click Integrate
- If your VM isn't monitored using the server agent, you need to download the server agent and add a server monitor
- Once installed, your server monitor will automatically integrate with the VMware VM monitor



# VMware Datastore Monitoring

- View the virtual machines that use your datastore the most in terms of key metrics like latencies, operations per second, occupied space, allocated space, and disk space management
- Prerequisites:
  - > Site24x7 On-Premise Poller
  - > VMware Read Only or Administrator roles along with Browse and Config privileges for that particular VMware ESX/ESXi host



# VMware Resource Pool Monitoring

- Optimize and manage the resources allocated to virtual machines (VMs) with VMware Resource Pool monitoring. Avoid resource contention in your CPU and RAM by monitoring all your critical resource pool metrics
- Prerequisites:
  - > Site24x7 On-Premise Poller
  - > VMware Read Only or Administrator roles for that particular VMware ESX/ESXi host



# VMware Snapshot Monitoring

- Add all the snapshots associated with your datastore for monitoring so that you can effectively manage your space requirements
- Using Site24x7's Snapshot Monitoring feature, you can monitor the snapshots that belong to the virtual machines that are a part of that datastore
- It also allows you to monitor the performance at each snapshot-level and configure thresholds for each of them
- Prerequisites:
  - > Site24x7 On-Premise Poller version 4.6.4. or above
  - > [VMware Datastore.Browse privileges](#) required for datastore monitoring



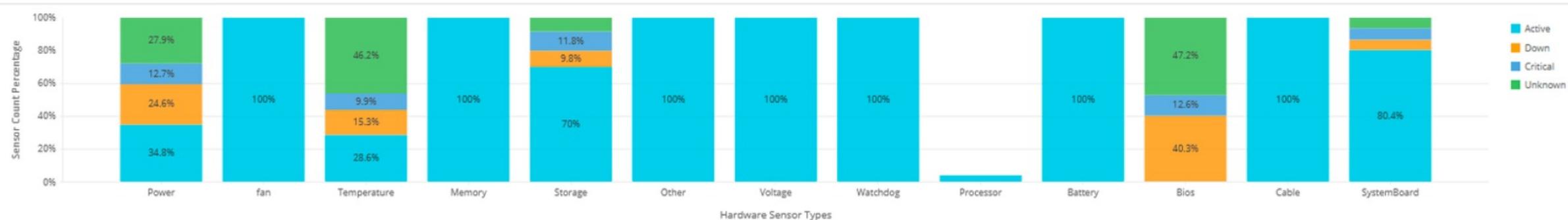
# VMware Hardware Monitoring

- Monitor your ESX/ESXi hardware sensors like cables, systemboards, and Bios and get detailed analysis including the status and count of all the hardware sensors
- Prerequisites:
  - > Site24x7 On-Premise Poller version 5.1.1 and above
  - > VMware Read Only or Administrator role for that particular VMware ESX/ESXi host



# VMware Hardware Monitoring

Hardware Sensor Status Split-up





# Nutanix Monitoring



# Nutanix Monitoring - Introduction

- Nutanix is a hyper-converged infrastructure solution that combines compute, virtualization, storage, networking, and security
- It can host and store virtual machines (VMs)
- A Nutanix Controller VM runs on each node, enabling the pooling of local storage from all nodes in the cluster
- Each node runs a standard hypervisor and contains processors, memory, and local storage (solid state drives and hard disks)
- It's important to monitor Nutanix clusters, hosts, and virtual machines
- Site24x7 monitors all of these from a single console
- Prerequisites: Site24x7 On-Premise Poller version 4.4.4 or above



# Nutanix Cluster Monitoring

- A Nutanix Virtual Computing Platform is a scale-out hyper-converged storage and compute platform
- Nutanix nodes collectively form a Nutanix cluster; each node contains CPU, memory, RAM, and storage, and they also run hypervisors. On each of these nodes runs a controller VM
- Gain in-depth insights on all key performance metrics of CPUs, memory, disks, content cache, and storage controllers
- You can monitor your Nutanix hosts and virtual machines by simply enabling auto-discovery while adding Nutanix clusters for monitoring



# Nutanix Host Monitoring

- Monitor Nutanix hosts and obtain metric-level data on all components like CPU, memory, storage, input-output operations, bandwidth, and latency
- You can also set thresholds and receive alerts when any of the thresholds are breached



# Nutanix VM Monitoring

- Monitor Nutanix virtual machines (VMs) and obtain metric-level data on all components like CPU ready time, storage, memory, storage containers, virtual disks, and virtual NICs
- You can also set thresholds and receive alerts when any of the thresholds are breached



# VMware Horizon Monitoring



# VMware Horizon Monitoring - Introduction

- VMware Horizon is a solution that simplifies the management and delivery of virtual desktops and apps on-premises, in the cloud, or in a hybrid or multi-cloud configuration through a single platform to end users
- Add VMware Horizon monitor to discover all the instances of View Connection Server, and monitor the performance of various resources associated with your virtual desktop infrastructure (VDI)



# Prerequisites

- …→ Site24x7 On-Premise Poller with version 4.4.6 and above
- …→ [Enable VMware PowerCLI Module](#)



# Interpret VMware Horizon Performance

- Analyze the performance of a VMware Horizon by viewing the connections in machines, servers, and event databases
- Summary: A glimpse of the number of associated resources and sessions
- Machines: Shows the number of machines connected
- Servers: Shows the View Connection Server details and vCenter Server details
- Events database: The details of the events database
- Settings: Lists the global settings



# AppLogs Monitoring



# View Unstructured Log Data in a Structured Way



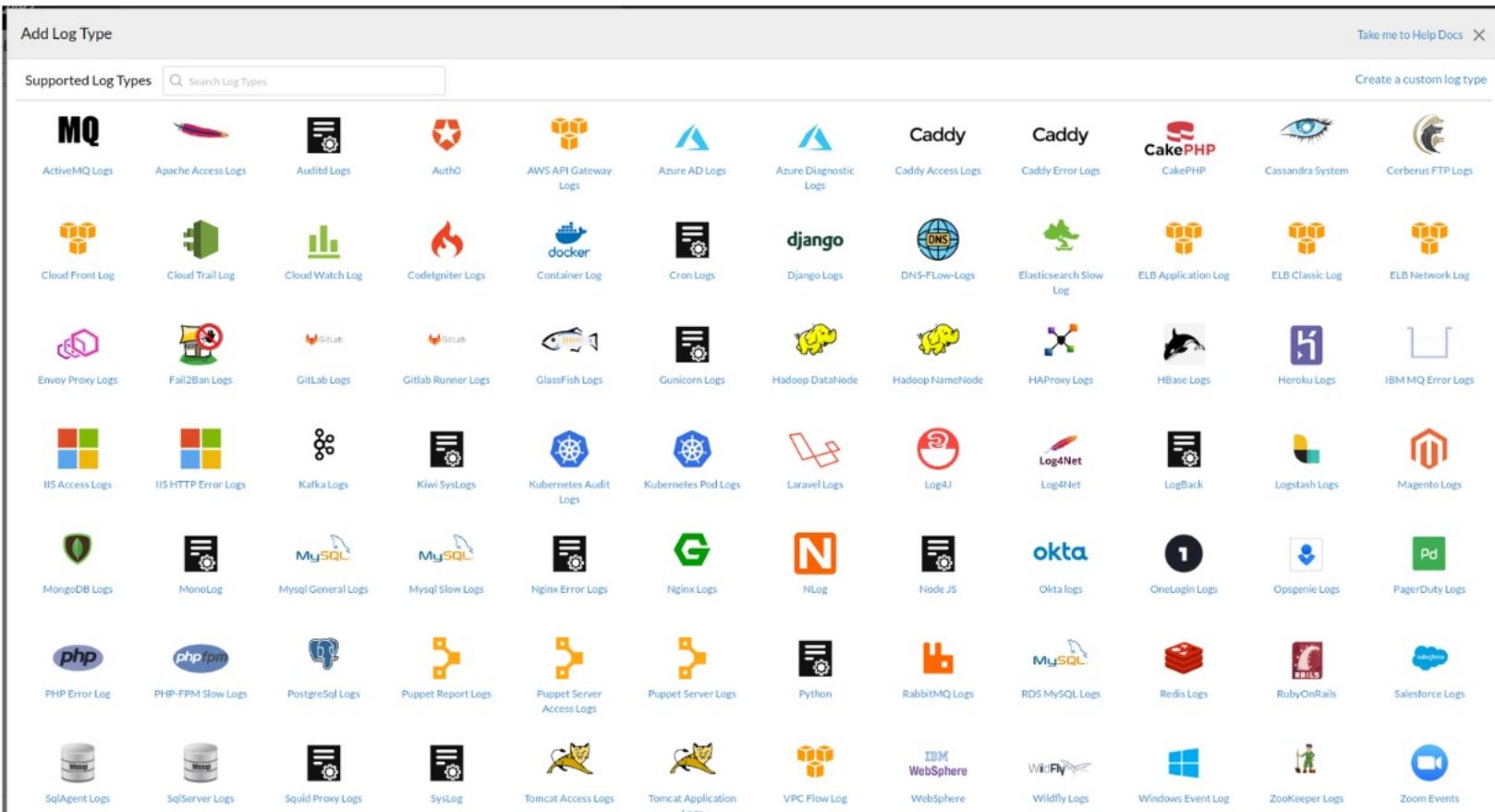
# Highlights

- Consolidate logs across servers
- Out-of-the-box support for common application, server, network device logs
- Provision to add any custom logs
- Alerting based on configured threshold
- Query language style - ease of use
- Different report types for different query types
- Dedicated dashboard of each log types

# Out-of-the-box Support for Common Applications



# Supported Log Types



“AppLogs supports over 100 log types by default including AWS & AZURE”

# Log Profile

Log Profile <small>i</small>			
Log Profiles	Log Types	Included Files	Excluded Files
apacheaccesslog Monitors : 1	apacheaccesslog	/etc/httpd/logs*/access_log*,/etc/httpd/logs*/access_log-*	
s247agent Monitors : 1	s247agent	/root/s247agent/ManageEngine/EUMAgent/logs/agentlog*.txt,/root/s247agent/ManageEngine/EUMAgent/logs/agentlog*	
iisaccesslogs Monitors : 1	iisaccesslogs		
Log Types <small>i</small>			
Log Type	Log Pattern	Auto Discovery	
S247AgentAccess Monitors : 1	tomcataccess	\$RemoteHost\$ \$RemoteLogName\$ \$RemoteUser\$	
redislog Monitors : 1	redislog	[\$Date:\$date\$] "\$RequestFirstLine\$" \$Status\$ \$ResponseSize:long\$ "\$Referer\$" "\$UserAgent\$"	Enabled
SqlServer Monitors : 1	sqlserver	[\$DateTime:\$date:EEE MMM dd HH:mm:ss z YYYY]\$[\$ThreadName\$][\$ThreadId\$]:\$Message\$	Enabled
test	\$Dat	\$DateTime:\$date\$ \$ServerIP\$ \$Method\$ \$StemURI\$ \$QueryURI\$ \$ServerPort\$ \$UserName\$ \$ClientIP\$	
redislog	\$PID	\$UserAgent\$ \$Referer\$ \$StatusCode:long\$ \$SubStatusCode:long\$ \$WindowsStatusCode:long\$	Enabled
iisaccesslogs	\$Me		



# Types of Log Sources

- …→ Local File
- …→ [Remote File](#)
- …→ Windows Event Logs
- …→ [Amazon Lambda](#)
- …→ [Azure Functions](#)
- …→ Log Collectors - [Logstash](#) | [Fluentd](#)

*Collect Logs from [Network](#) Devices*

# Custom Log type

The screenshot shows the 'Add Log Type' configuration page. On the left, a sidebar menu lists various monitoring categories like Home, Alarms, Web, APM, Server, Plugins, VMware, Cloud, Network, RUM, Metrics, Logs, Reports, and Admin. The 'Logs' section is currently selected.

The main form has the following fields:

- Log Type:** Custom Log Type
- Display Name:** Java-Logs
- Auto Discovery:** Enable (button)
- Sample Logs:** A code block containing a log entry:

```
{"log": "20-Mar-2023 13:31:40.377 INFO [main] org.apache.catalina.core.AprLifecycleListener.initializeSSL  
OpenSSL successfully initialized [OpenSSL 1.1.0l 10 Sep 2019]\n", "stream": "stderr", "time": "2023-03-  
20T13:31:40.377353037Z"}
```
- Matched Pattern:** default
- Log Pattern:** A table showing a single pattern named 'default':

Name	Pattern
default	json \$log:pattern:\$Datetime:date:dd-MMM-yyyy HH:mm:ss.SSSS \$LogLevel:word\$ [\$ThreadName\$] \$ClassName\$ \$Message\$
- Sample Output:** A table showing field mappings:

Field Name	Value from Sample Log 1 - Matched pattern : default	Edit Field Configurations
Datetime	20-Mar-2023 13:31:40.377	
LogLevel	INFO	
ThreadName	main	
ClassName	org.apache.catalina.core.AprLifecycleListener.initializeSSL	
Message	OpenSSL successfully initialized [OpenSSL 1.1.0l 10 Sep 2019]<NewLine>	



# Multiple Log Pattern

Combining different patterns of logs under a single log type



# Multiple Patterns



# Multiple Patterns...



# Derived Fields

To extract meaningful information from the message fields

# Derived Field Configuration

[Thu Aug 12 14:52:23 IST 2022|DEBUG|39]:SSL Handshake Time <https://zylker.com> :42

[Thu May 12 14:37:51 IST 2022|DEBUG|30]: Object.wait break after up notification received...

[Thu May 12 14:37:51 IST 2022|DEBUG|42]: Up Notification received... breaking the waiting thread....

---

[\$Datetime:date:EEE MMM dd HH:mm:ss z yyyy\$|\$LogLevel\$|\$Time\$]:\$Message\$

---

[Thu Aug 12 14:52:23 IST 2022|DEBUG|39]: HttpConnection : After successful gzip extraction  
downloaded response(22015) was extracted to 80132 of content-length

[Thu Aug 12 14:52:23 IST 2022|DEBUG|39]: HttpConnection : Failed to connect

---

[\$Datetime:date:EEE MMM dd HH:mm:ss z yyyy\$|\$LogLevel\$|\$Time\$]:\$Message\$

---



# Derived Field Configuration...

## Derived Fields ?

Display Name

First Rule

RegEx ?

SSL\shandshake\sTime\s(?<Domain>.\*\s:\s(?<SSLTime>\d+)

Domain

String

SSLTime

Number

Milliseconds (ms)

Tip: Create a RegEx with the *named capturing group* syntax (?<name>) capturing text) and validate your RegEx using our [free tool](#)



# Adding Derived Fields in dashboard



# AppLogs Query Language

- Collect, consolidate, index, and search logs to gain actionable insights using Site24x7 AppLogs
- Easy to understand language search by filtering out invalid values and obtain actionable results quickly

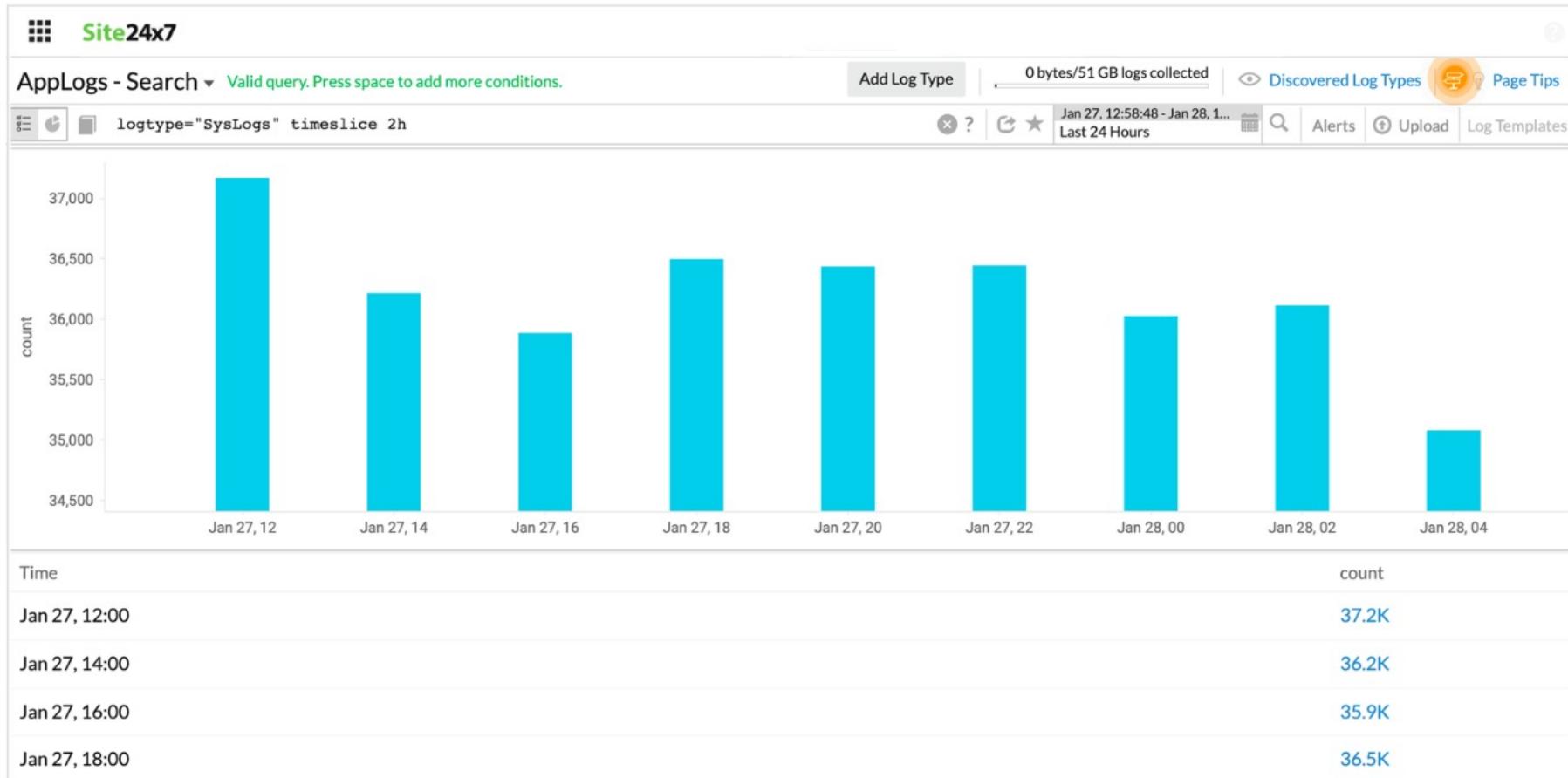
# Query Language

Support [keywords](#) in query language

or	and	contains	notcontains
isempty	isnotempty	in	notin
like	startswith	>,<,>=,<=,=,!=	not
count	min	max	sum
avg	sd	percentile	ratio
count_distinct	groupby, having	histo, range	timeslice
tophits	sort	before	include exclude
monitor_name	monitor_group	tags	

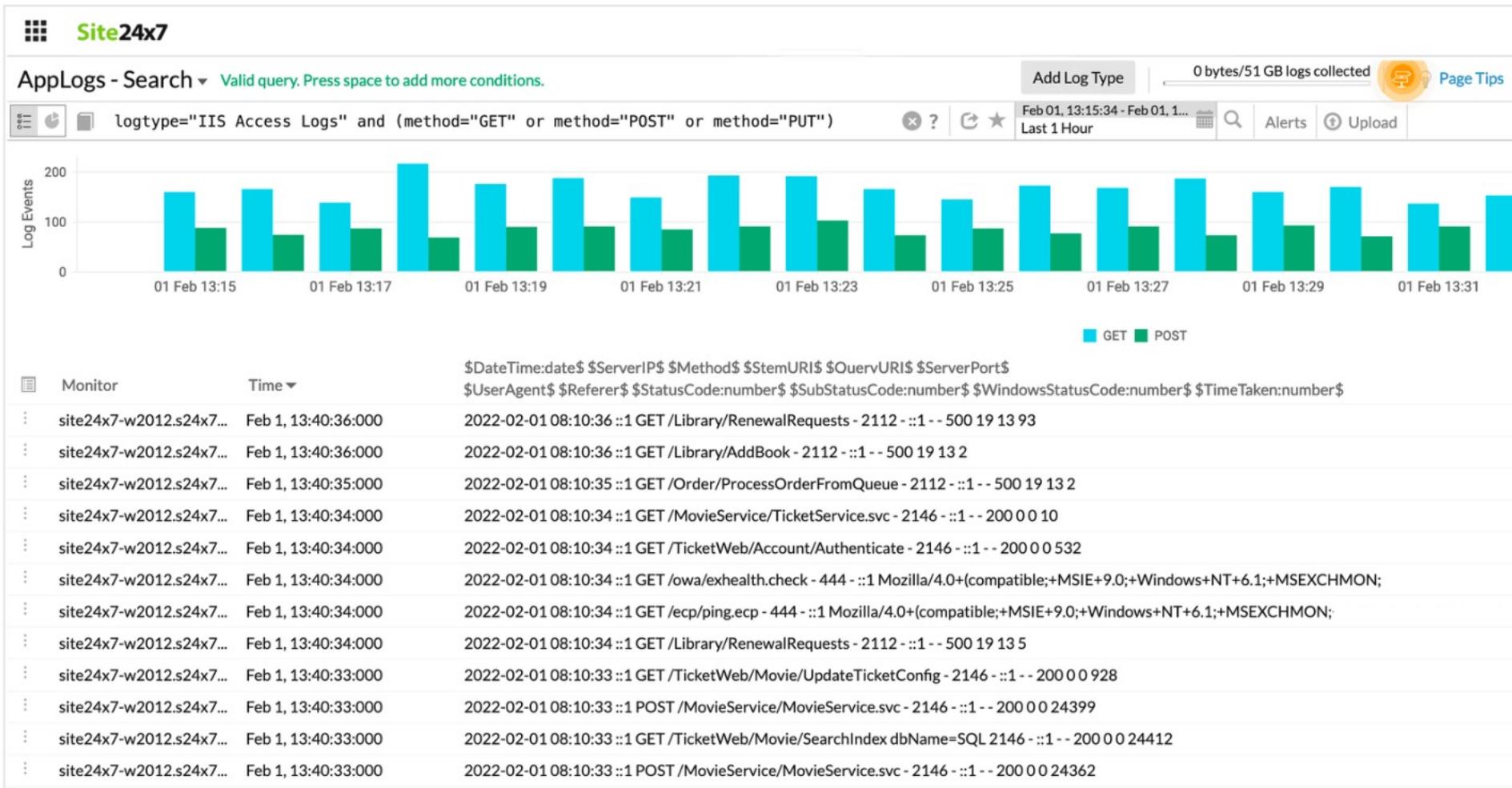


# Time Slice Report



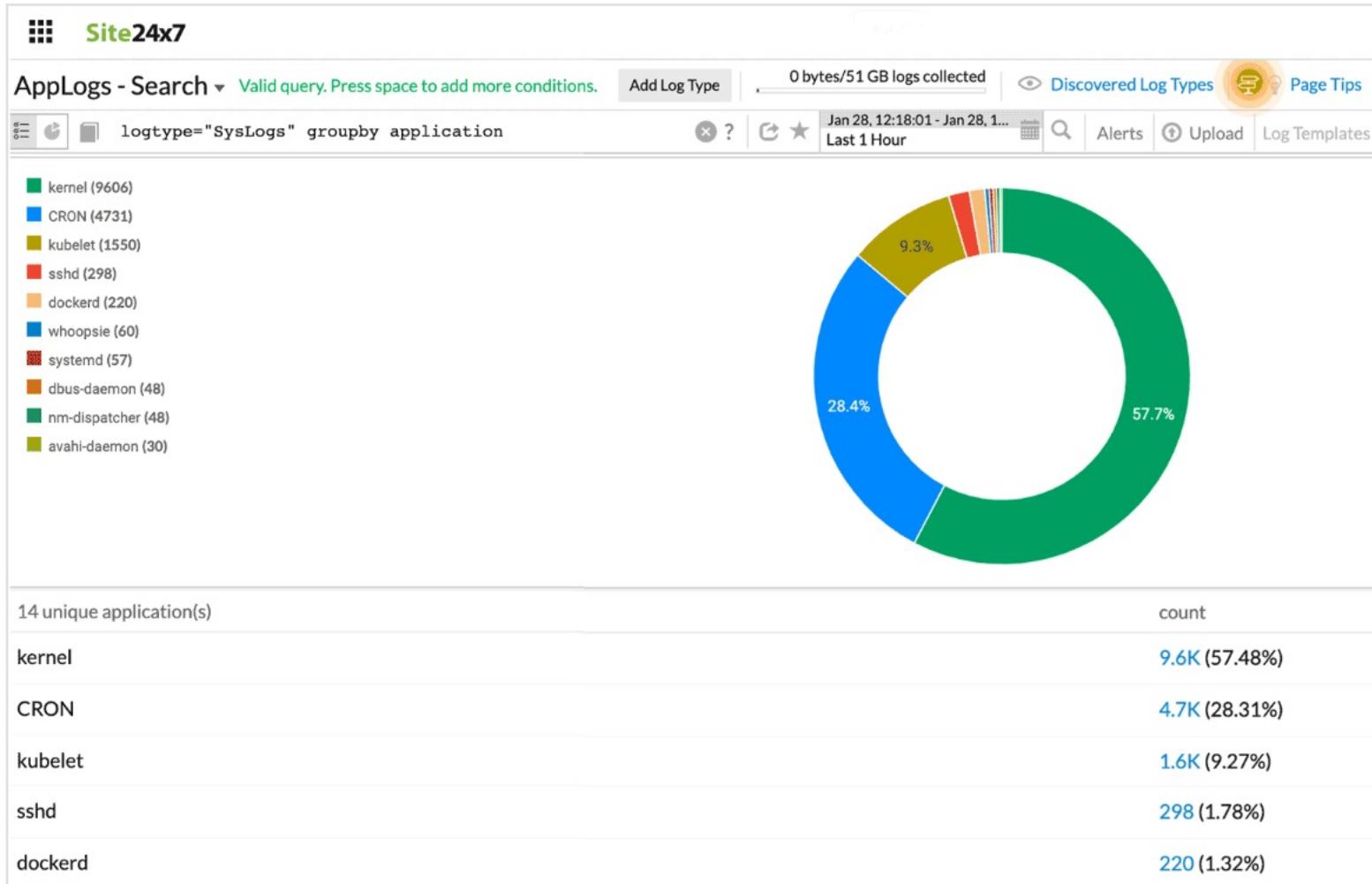


# Log Report

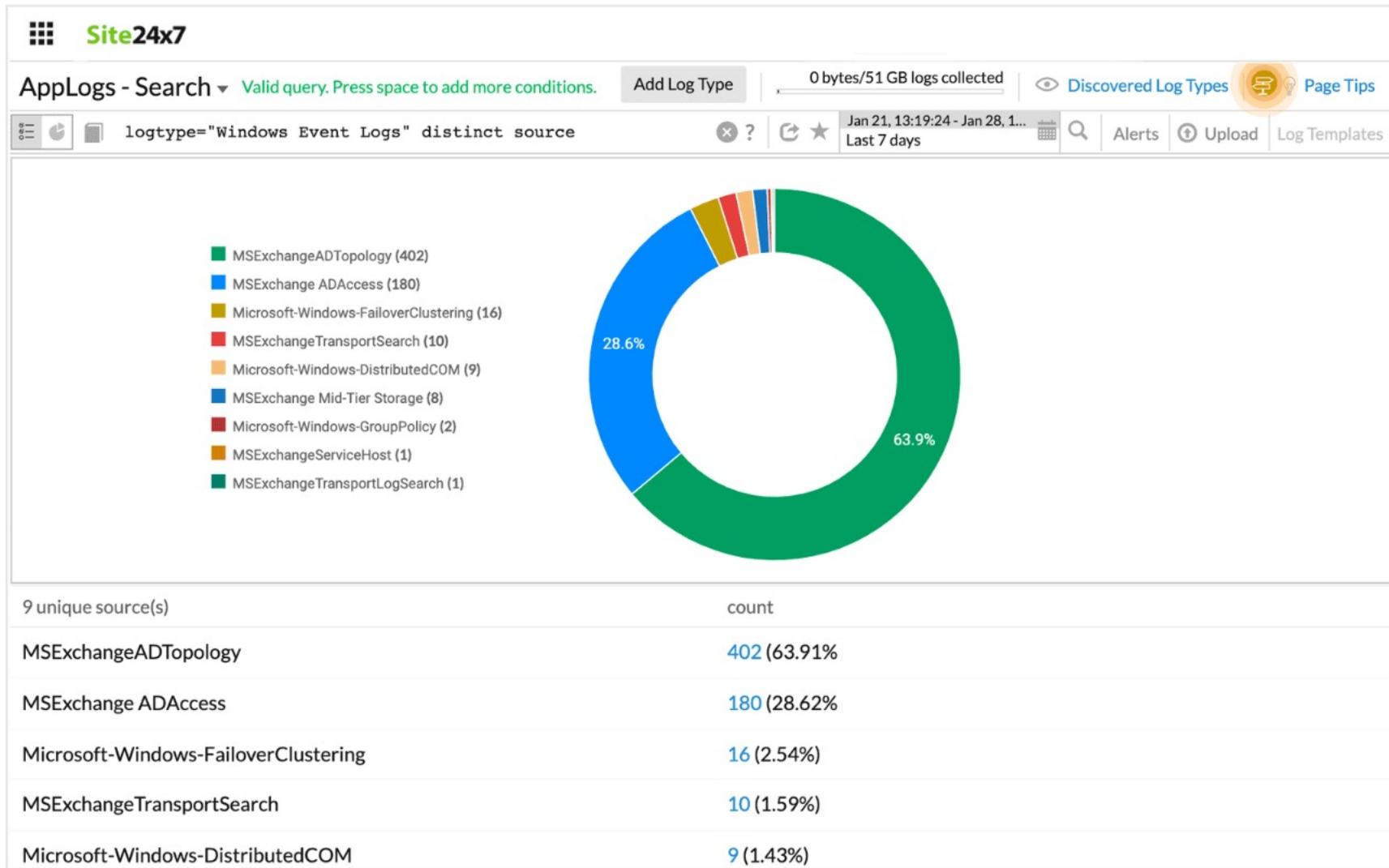




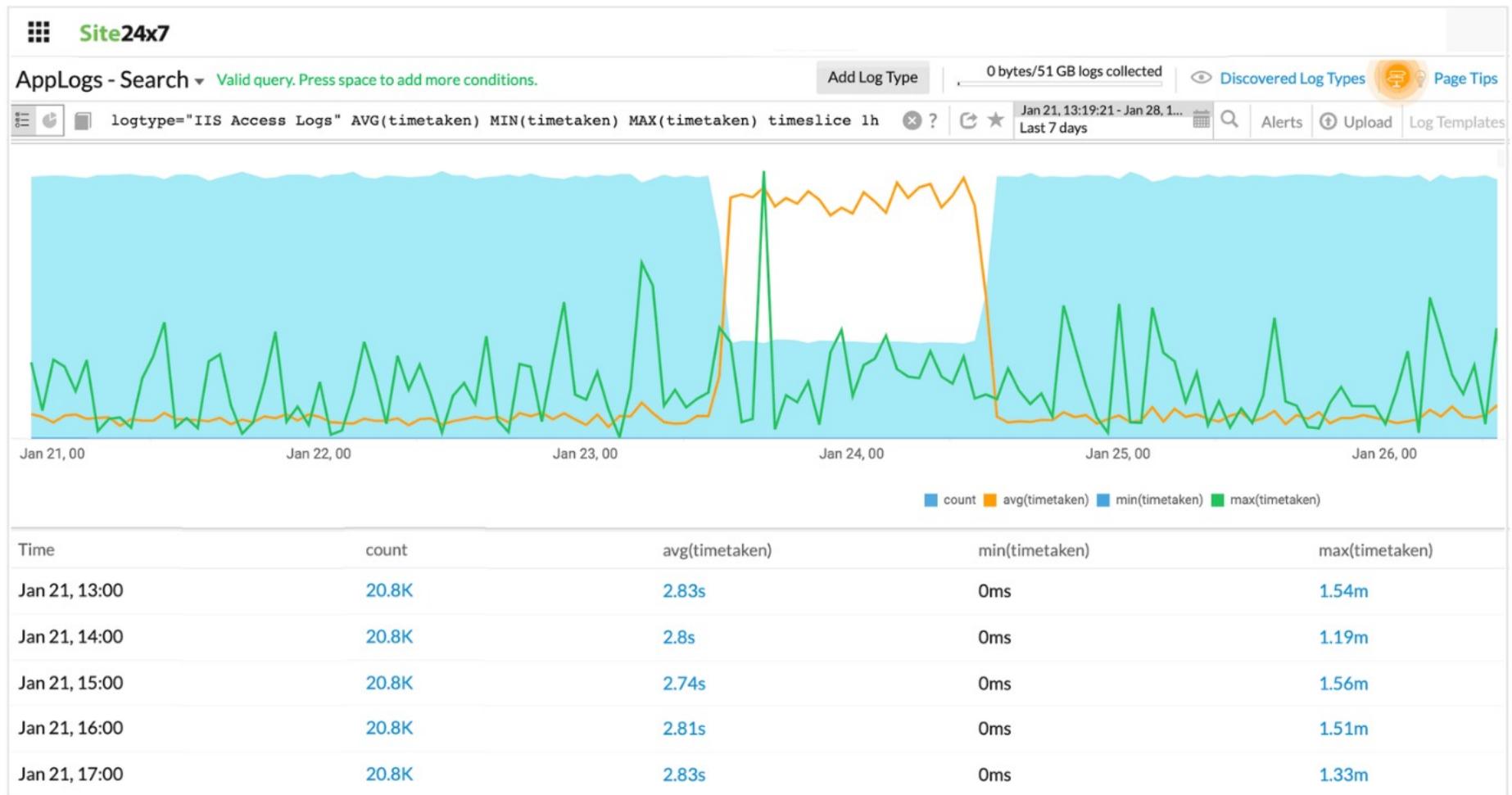
# Groupby Report



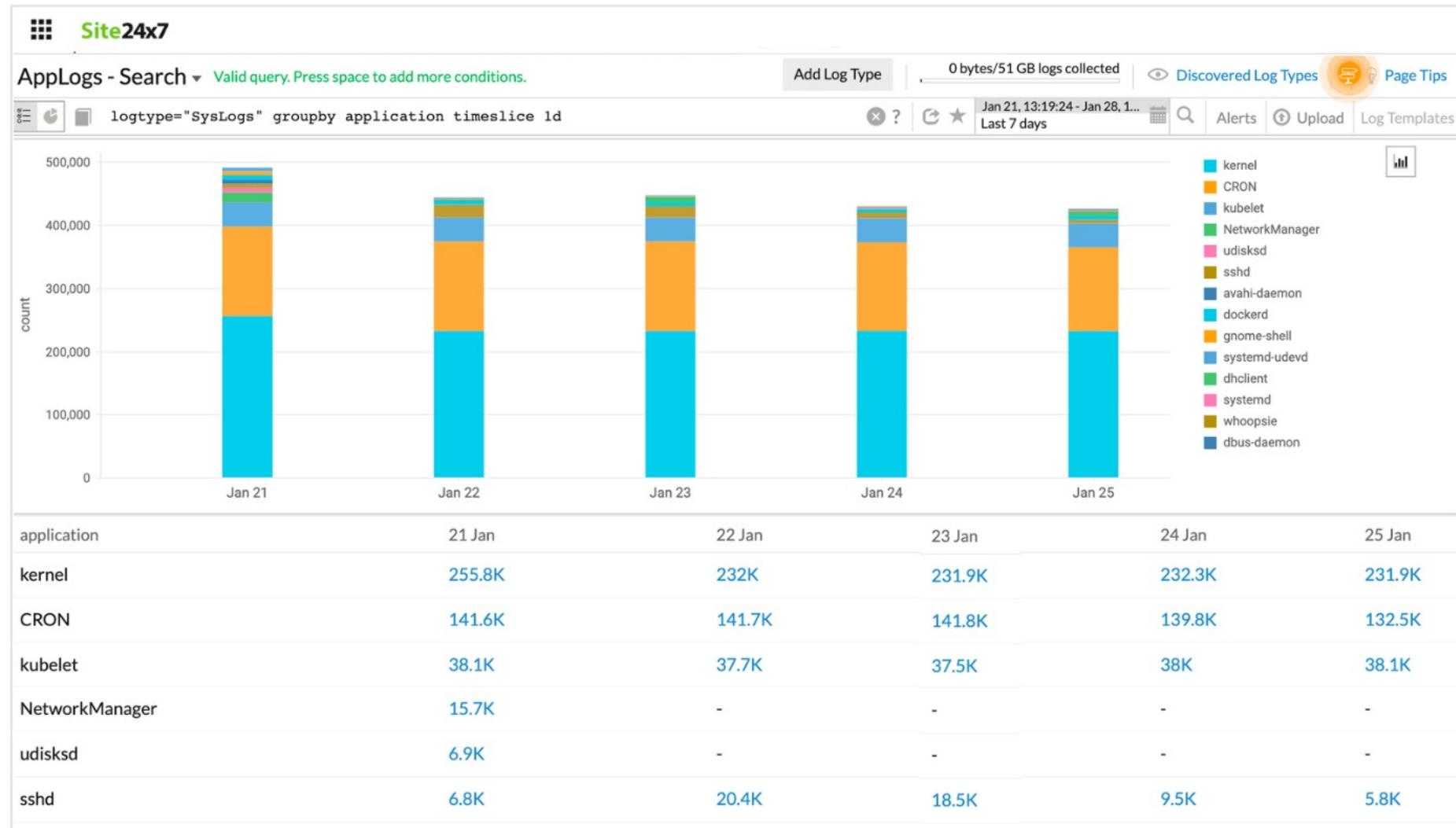
# Distinct Report



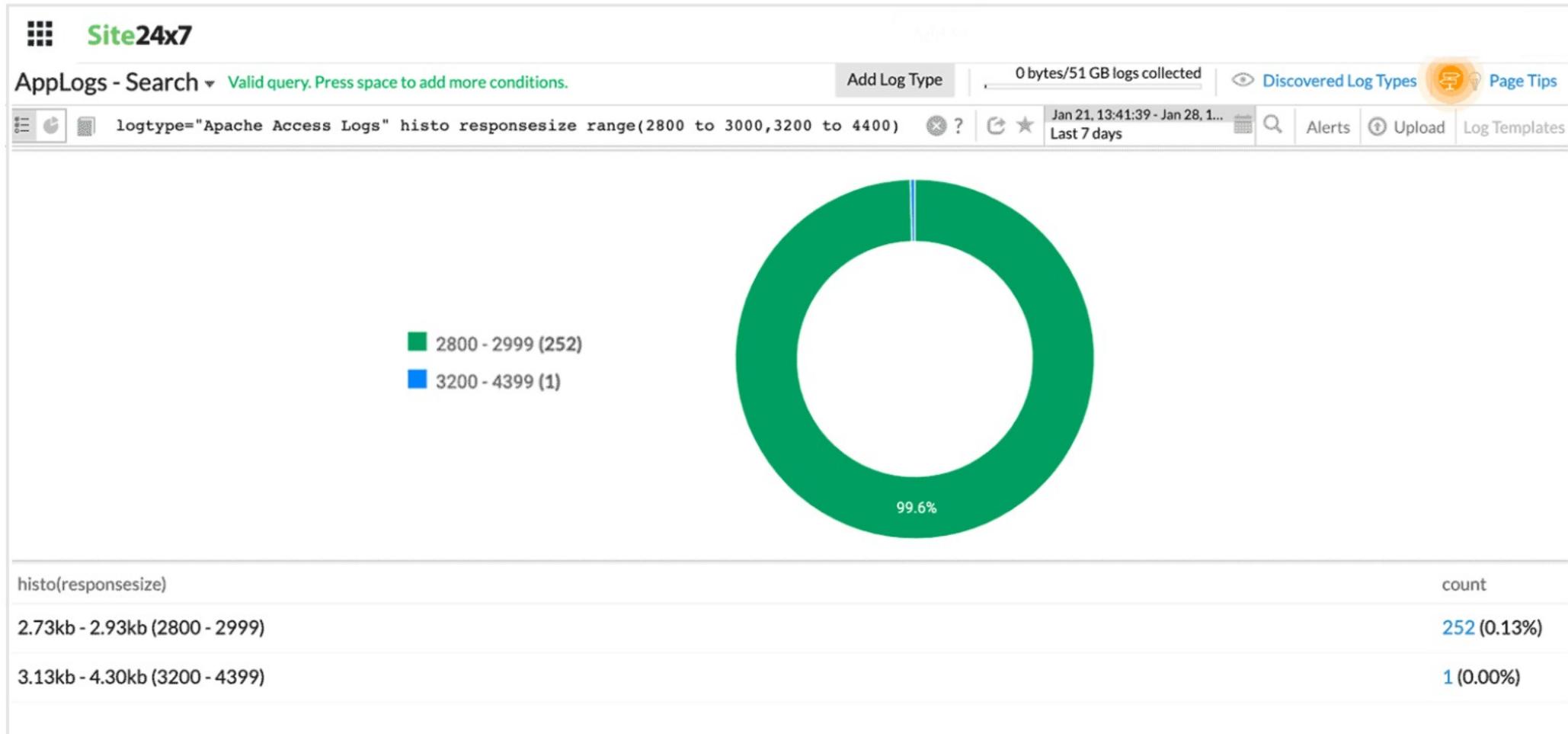
# Combining Timeslice and Aggregation Together



# Combining Groupby and Timeslice Together



# Histo with Range



# TopHits Query

The screenshot shows the Site24x7 log search interface. The top navigation bar includes the logo, a search bar, and various icons for account management and help. The main header displays "AppLogs - Search" and a query message: "Valid query. Press space to add more conditions." Below this is a search bar containing the query: "logtype='Kafka-Topic-Status' tophits(topicname,offset,lag) groupby topicname". The results table has columns: "topicname", "count", "offset", and "lag". The data shows five unique topic names, each with a count of 3 (20.00%), offset values ranging from 2837530 to 6837430, and lag values ranging from 22 to 342. A footer bar at the bottom includes links for "Chats", "Channels", "Contacts", and "Support".

topicname	count	offset	lag
Zylker-Order	3 (20.00%)	6837430	22
Zylker-Payment	3 (20.00%)	2837530	176
Zylker-Purchase	3 (20.00%)	5854430	34
Zylker-Shipment	3 (20.00%)	4864430	342
Zylker-Tracking	3 (20.00%)	3874430	270

Used to get current value of the grouped item. This is mainly useful for metric kind of logs

# Key performance Indicator

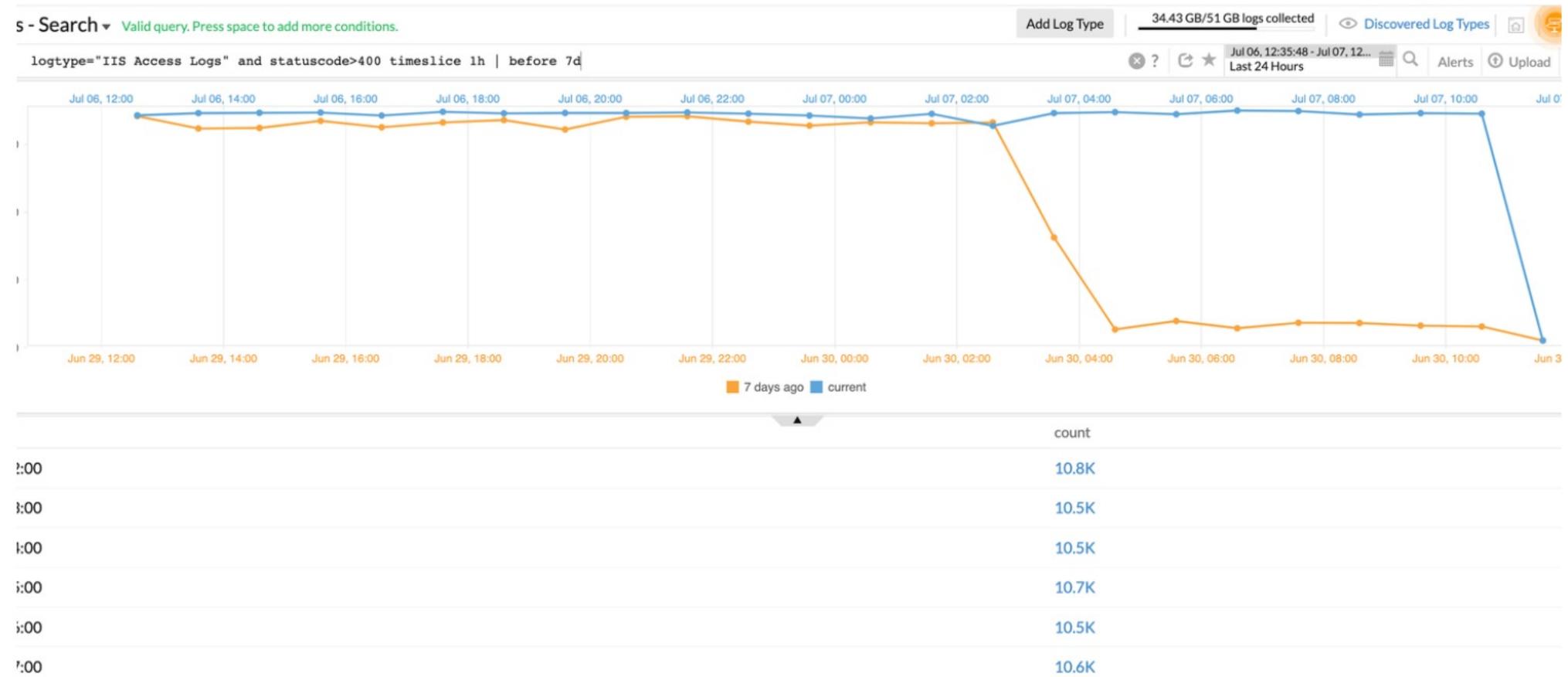
The screenshot shows the Site24x7 application logs search interface. On the left, a vertical sidebar lists monitoring categories: Home, Alarms, Web, APM, Server, VMware, Cloud, Network, RUM, and AppLogs. The AppLogs icon is highlighted with a green border. The main search bar displays the query: `logtype="IIS Access Logs" and statuscode>200 count | before 7d`. To the right of the search bar are buttons for 'Add Log Type', '0 bytes/51 GB logs collected', and 'Page Tips'. Below the search bar, a time range selector shows 'Feb 01, 11:10:39 - Feb 02, 1...' and 'Last 24 Hours'. Further right are buttons for 'Alerts', 'Upload', and 'Log Templates'. In the center, a large KPI value is displayed: **268.7 K** with a downward arrow and **-10.98%**. Below this, a smaller text indicates the data is from **7 days ago : 301.9K**. At the bottom of the interface, a footer bar shows the message **Showing 1 - 100 log events out of 201055**.

268.7 K ↓10.98%

7 days ago : 301.9K

Showing 1 - 100 log events out of 201055

# Key performance Indicator (Overtime)



# Recent and saved Searches

Site24x7

AppLogs - Search ▾ Valid query. Press space to add more conditions.

Add Log Type 0 bytes/51 GB logs collected Page Tips

logtype="

Home Alarms Web APM Server VMware Cloud Network RUM AppLogs Reports Admin

Saved Searches - 0/67

Display Name
1196 events
aaaa
Apm exception
Audit Failure
Azure count
Azure Failed Status
Azure Test Query
Azure-Test

Recent Searches - 1/21

logtype="IIS Access Logs" AVG(timetaken) MIN(timetaken) MAX(timetaken) groupby stemuri
logtype="Windows Event Logs" COUNT_DISTINCT(source)
logtype="Windows Event Logs" and source CONTAINS "Microsoft-Windows" count
logtype="IIS Access Logs" count   before 2d
logtype="IIS Access Logs" avg(timetaken) timeslice 1d
logtype="Windows Event Logs" and source STARTSWITH "Micro"
logtype="Windows Event Logs" and source LIKE "Microsoft*FailoverClustering"
logtype="SvsLogs"   exclude(pid)

Clear recent searches | Close

# App log Dashboard

AppLogs - Search ▾ Valid query. Press space to add more conditions.

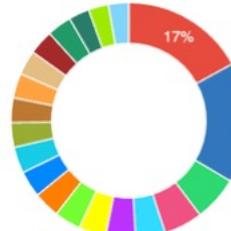
Add Log Type 34.43 GB/51 GB logs collected

Discovered Log Types Page Tips

Jul 06, 12:30:50 - Jul 07, 12... Last 24 Hours

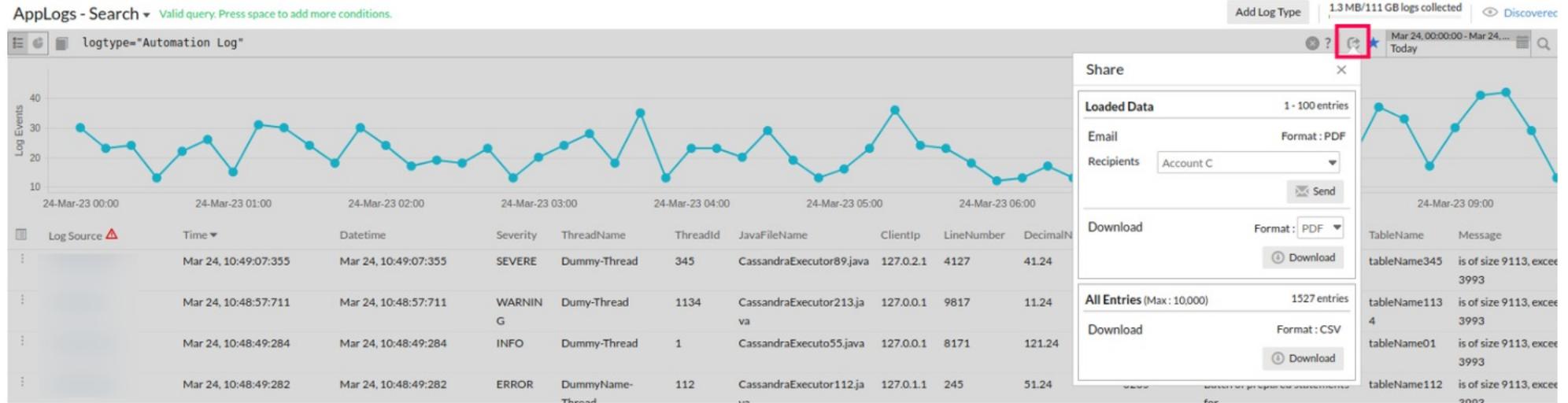
Share Edit Dashboard

Total Requests	Average Response Time	Failed Requests	timetaken	timetaken	sum
Count 500.5k	avg(timetaken) 2.64s	Count 262.3k	avg(timetaken) 2.64s	min(statuscode) 200	sum(windowsstatuscode) 220164725563747

Top 20 Failed Requests		User Agent Stats	Request Trend		
Browser	Device	OS	Browser	Device	OS
		UNKNOWN - 498,715	UNKNOWN - 498,715		

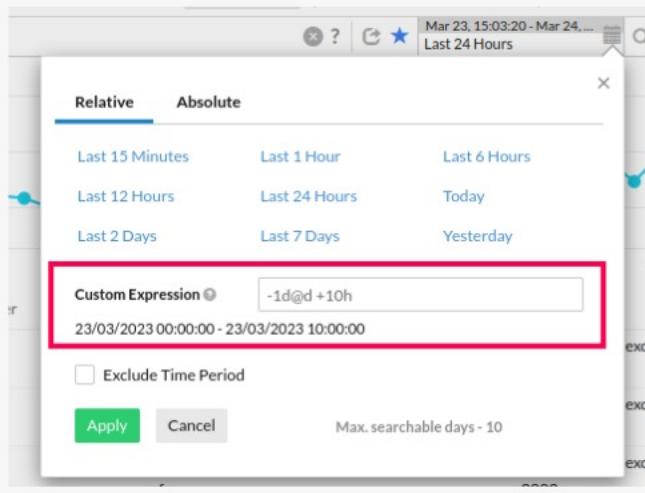
Status Code Stats							Response Time Stats																	
Date & Time	2XX	3XX	4XX	5XX								Response Time	Total	06 Jul, 12:00	06 Jul, 01:00	06 Jul, 02:00	06 Jul, 03:00	06 Jul, 04:00	06 Jul, 05:00	06 Ju				
Total	234894	45.95%	8412	1.65%	126542	24.75%	141392	27.66%								> 60 secs	691	16	57	45	24	22	24	12
06 Jul, 12:00	9906	45.95%	355	1.65%	5374	24.93%	5923	27.47%								30-60 secs	26K	1160	1067	1110	1119	1070	1133	1124
06 Jul, 01:00	9766	45.86%	347	1.63%	5238	24.6%	5942	27.91%								10-30 secs	665	13	46	31	14	29	17	21
06 Jul, 02:00	9850	45.96%	355	1.66%	5310	24.78%	5916	27.6%								5-10 secs	1K	28	54	47	25	54	49	30

# Export Search Result

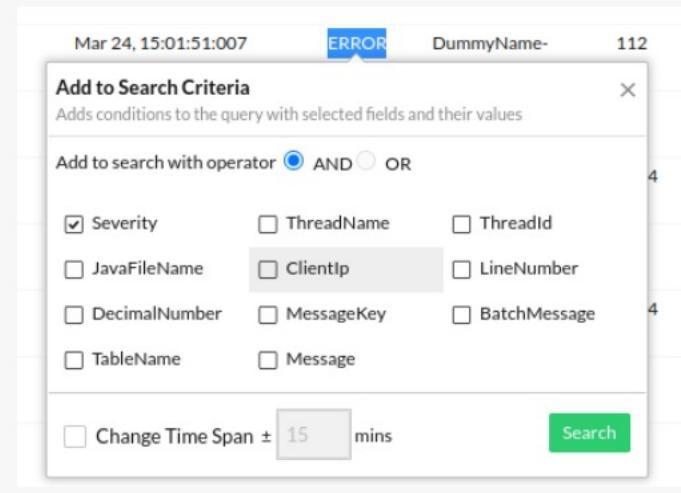


We can export the search result as CSV or PDF format. Limitation : Maximum 10K log lines  
Also we have python script to download the logs via REST API

# Search Options



Relative Time Search



Add Conditions to Search

# AppLogs Alerts

The screenshot displays the Site24x7 AppLogs interface. On the left, a sidebar lists various monitoring categories like Home, Alarms, Web, APNs, Server, VMware, Cloud, Network, AWS, BUM, Metrics, Apps, Reports, Admin, and Edit. The main area shows a search bar with the query "logtype='Windows Event Logs'". Below it is a chart titled "Log Events" showing a sharp spike on Jan 17 at 15:22. To the right, a detailed "Alerts" modal is open, allowing the creation of a new alert named "Windows Alert". The modal includes fields for "Search Query" (logtype="Windows Event Logs"), "Alert Type" (Count Based Alert selected), "Check Frequency" (15 Minutes), and "Attribute" (count). A red box highlights the "Threshold Configuration" section, which contains two conditions: one for a count greater than 1 (Notify As: Trouble, Automation: Server) and another for a count greater than or equal to 10 (Notify As: Critical, Automation: No items selected). Other sections include "Configuration Profiles" (Notification Profile: Default Notification), "User Alert Group" (Admin Group checked, Application Team and Network Team unchecked), "Tags" (Select Tags), and "Third-Party Integrations" (Slack Integration checked). At the bottom of the modal is a "Save" button.

# Masking and Hashing Log Data

→ Hide sensitive data while sending your logs to Site24x7 AppLogs

The screenshot shows the Site24x7 AppLogs interface. On the left, a modal window titled "RequestURI - Field Configurations" is open, allowing users to configure various log fields like RequestURI, Method, and UserAgent. On the right, the main log viewer displays log entries with sensitive information like URLs and user agents masked or hashed.

**RequestURI - Field Configurations**

- Machinelp: Display Name RequestURI
- RemoteLogName: Hide this Field from Search Result (Yes)
- RemoteUser: Character Length for Groupby
- Method: RequestURI (Enable Masking: Yes, apiKey=("{")& API\_KEY)
- Protocol
- Status
- ResponseSize
- Referer: Select Log Line only if This Field (Matches)
- UserAgent: Any of These Values (Type and press Enter to add values to filter)
- TimeTaken: Ignore this Field at Source (Yes)

**Log Lines**

UserAgent	TimeTaken (μs)	Log Line
"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36"	982712	"Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36"
	1192712	logo.png

The field type for a particular field name cannot be changed after creation of a log type. You have to use a different field name if you want a different field type.

**API Upload** (Enable, Disable)

You can configure your application to POST data directly to AppLogs at this URL. This is not a web page, so don't open it in your browser.



# Related Log Templates

- Compare multiple fields in one log type with another by creating a template
- Simply define the template with a name by providing the necessary fields to be included
- This allows you to follow that particular field in another log type

# Related Log Templates

**Site24x7**

AppLogs - Search ▾ Valid query. Press space to add more conditions.

logtype="Site-Access-Log"

The chart displays three bars representing log events at different times on November 16, 2020. The y-axis is labeled 'Log Events' and ranges from 0 to 150. The x-axis shows times: 16-Nov-20 05:35, 16-Nov-20 06:05, and 16-Nov-20 06:35. The first bar reaches approximately 165, the second reaches approximately 90, and the third reaches approximately 30.

Time	Log Events
16-Nov-20 05:35	~165
16-Nov-20 06:05	~90
16-Nov-20 06:35	~30

Monitor Time ▾ \$ReqId\$ sas \$Host\$ \$ZLOC\$ \$ZUID\$ \$ZOID\$  
\$internalIp\$ \$SessionId\$ \$TicketDigest\$

Nov 16, 10:29:34:272 74 sas 172.20.45.1 -- "16-11-2020 23:59:34:

Fields to Filter

Related Log Templates

Follow Application Log

logtype="Site-Application-Log" and threadid=\${threadid} and host=\${host}

Add Related Log Template

Nov 16, 10:27:58:201 60731599 - "16-11-2020 af00d10d252d2946  
Nov 16, 10:27:58:201 60731599 - "16-11-2020 af00d10d252d2946



# Log Type Views

---

Too much data may make it difficult to focus on the relevant information during troubleshooting

---

“

”



# Schedule Reports - AppLog Dashboard

---

This report give you detailed insights into all configured widgets for the log types

---



# AppLogs Usage Summary

---

Usage alert mail will send to configured user on 60%,80%,90% and 100%

---



# AppLogs Monitoring and Third-party Integration Support

AppLogs - Search - Valid query. Press space to add more conditions.

logtype="Windows Event Logs"

Log Events

Time ▾ Date/Time EventID Type Level

Log Source	Time	Date/Time	EventID	Type	Level
	Jan 17, 16:48:01.769	Jan 17, 16:48:01.769	1001	Application	Info
	Jan 17, 16:40:56.369	Jan 17, 16:40:56.369	1001	Application	Info
	Jan 17, 16:30:49.554	Jan 17, 16:30:49.554	1001	Application	Info
	Jan 17, 16:30:32.215	Jan 17, 16:30:32.215	1001	Application	Info
	Jan 17, 16:25:27.165	Jan 17, 16:25:27.165	1001	Application	Info
	Jan 17, 16:22:47.260	Jan 17, 16:22:47.260	4725	Application	Warn
	Jan 17, 16:20:19.551	Jan 17, 16:20:19.551	1001	Application	Info
	Jan 17, 16:15:15.493	Jan 17, 16:15:15.493	1001	Application	Info
	Jan 17, 16:10:12.326	Jan 17, 16:10:12.326	1001	Application	Info
	Jan 17, 16:05:08.861	Jan 17, 16:05:08.861	1001	Application	Info
	Jan 17, 15:59:55.313	Jan 17, 15:59:55.313	1001	Application	Info
	Jan 17, 15:54:49.995	Jan 17, 15:54:49.995	1001	Application	Info
	Jan 17, 15:52:39.898	Jan 17, 15:52:39.898	4725	Application	Warn
	Jan 17, 15:49:43.711	Jan 17, 15:49:43.711	1001	Application	Info
	Jan 17, 15:44:35.495	Jan 17, 15:44:35.495	1001	Application	Info
	Jan 17, 15:39:22.862	Jan 17, 15:39:22.862	1001	Application	Info
	Jan 17, 15:34:02.947	Jan 17, 15:34:02.947	1001	Application	Info
	Jan 17, 15:28:56.590	Jan 17, 15:28:56.590	1001	Application	Info
	Jan 17, 15:23:51.481	Jan 17, 15:23:51.481	1001	Application	Info

Security Auditing

Alerts

Create Alert

Display Name: Windows Alert

Search Query: logtype="Windows Event Logs"

Alert Type: Count Based Alert

Check Frequency: 15 Minutes

Attribute: count

Threshold Configuration

Condition	Threshold	Notify As	Automation
>	1	Trouble	Server
>=	10	Critical	No items selected

Configuration Profiles

Notification Profile: Default Notification

User Alert Group: Admin Group, Application T..., Network Team

Tags: Select Tags, Add Tag

Third-Party Integrations

Services: Slack Integration

Save

99.24 MB / 5 GB logs collected

Jan 16, 16:30:22.008 - Jan 17, 15:59:55.313

Last 24 Hours

Alerts

Upcoming Log Types

Log Types

Showing 1 - 100 log events out of 2000



# Benefits

- Receive alerts through third-party ITSM and collaboration tools like Jira, PagerDuty, Slack, Microsoft Teams, and others along with the email, voice call, and SMS alerts that are available currently
- Once you configure an alert for a Log Type in AppLogs, your Log Type will be treated as a monitor and any search query can be configured for alerting. This allows you to view your Log Type along with its status from the Home > Monitors page
- View and manage your alerts from the Alarms and Outages tabs along with other monitors
- If you have a planned maintenance for your servers, you can simply configure the server as undergoing maintenance and mute AppLogs Alerts for a particular duration
- Other monitor-level features like Notification Profiles and IT Automation that allow you configure actions for log alerts and fix common incidents without any manual intervention



## 2023 Q1 updates

- Applogs now supports Kubernetes audit logs, Node.js logs, and Python logs.
- AppLogs now includes percents, percentile, and tophits in the supported operator's list.
- Bulk Update Credential option for ESXi to vCenter-based polling
- VMware cluster monitoring GA



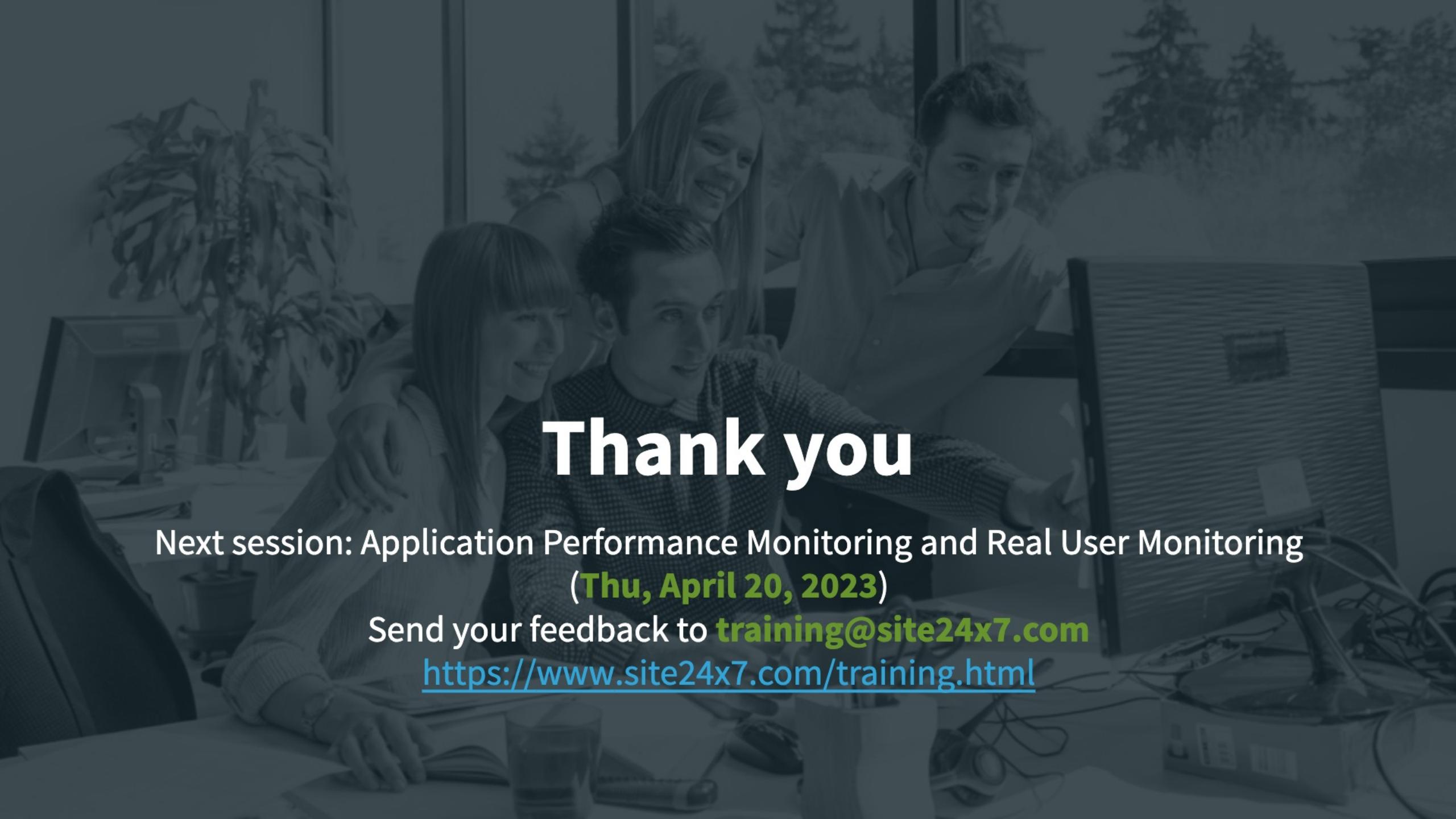
# Best Practices

- We always recommend you to use the latest version of On-Premise Poller for better performance
- Use High Availability On-Premise Poller
- Set thresholds and monitor the performance metrics effectively
- Install server agent in VMs to view both the VM metrics as well as guest OS metrics in a single unified console (integrated VM monitor console)



# Learnings from the session

- Learned about On-Premise Poller and High Availability On-Premise Poller
- Installation of Network Monitoring, NetFlow Analyzer, NCM, Meraki Monitoring and VMware Monitoring
- Overview of VoIP Monitoring, Nutanix Monitoring and VMware Horizon Monitoring
- About AppLogs Monitoring

A black and white photograph of four people in an office environment. Three women are in the foreground, leaning over a desk and looking at a computer monitor. A man is visible behind them, also looking towards the screen. They are all smiling. The office has large windows in the background showing trees. There are plants on the desk and papers scattered around.

# Thank you

Next session: Application Performance Monitoring and Real User Monitoring  
**(Thu, April 20, 2023)**

Send your feedback to **[training@site24x7.com](mailto:training@site24x7.com)**  
**<https://www.site24x7.com/training.html>**