



**Site24x7**

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 BST) | US Time Zone (10:00 PDT)

## Sessions split up:

**Session 1 - Introduction and Deep Dive into Website Monitoring (Mon, Oct 10, 2022)**

**Session 2 - Infrastructure Monitoring and Custom Plugins (Tue, Oct 11, 2022)**

**Session 3 - Network & Virtualization Monitoring and Log Management (Wed, Oct 12, 2022)**

**Session 4 - Application Performance Monitoring and Real User Monitoring (Thu, Oct 13, 2022)**

**Session 5 - Reports, Dashboards, Advanced Configurations, Alerting, and More (Fri, Oct 14, 2022)**



# Scope of the session

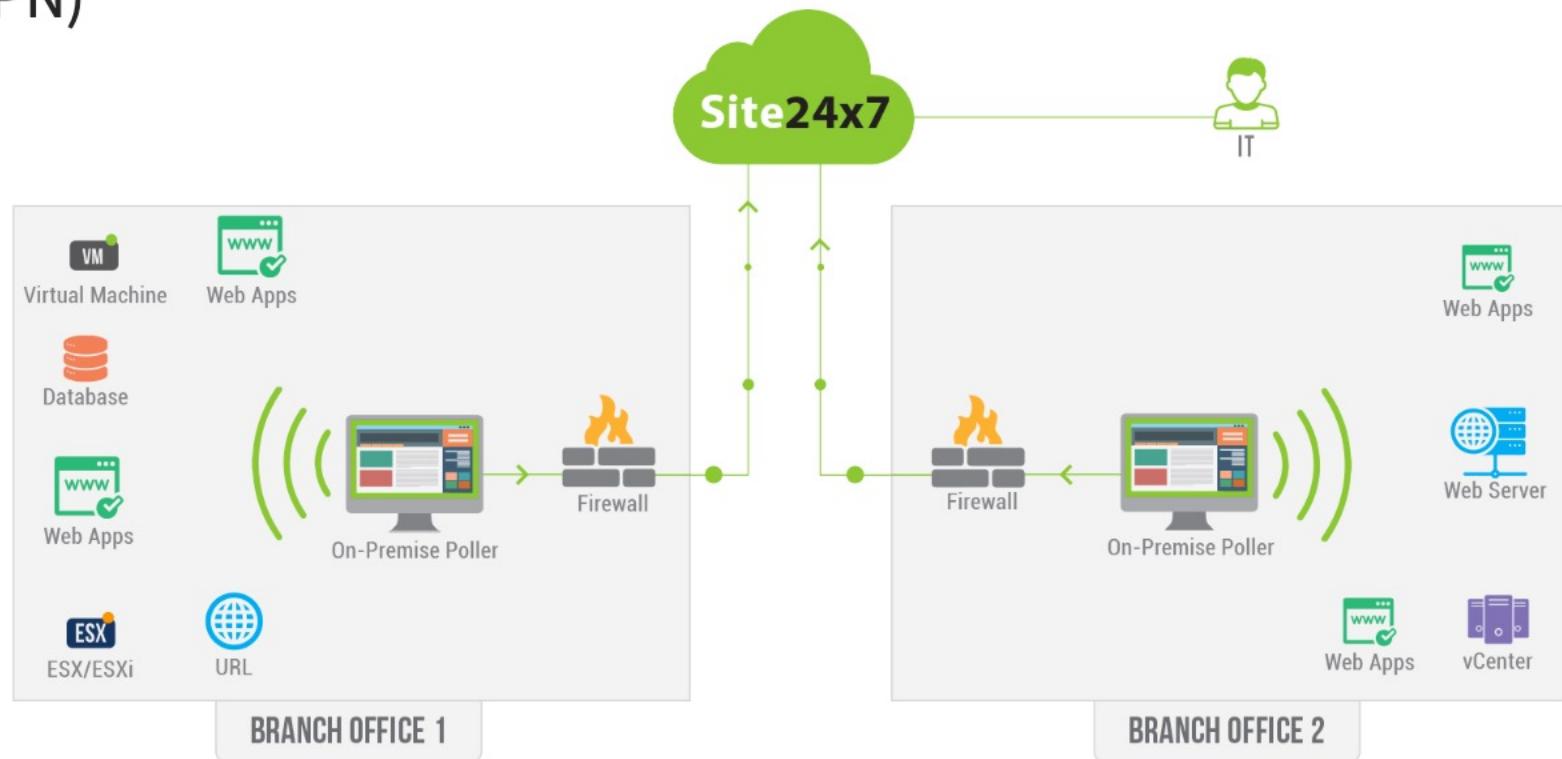
- ⇢ Overview of On-Premise Poller
- ⇢ Network Monitoring
- ⇢ NetFlow Analyzer
- ⇢ Network Configuration Manager
- ⇢ VoIP Monitoring
- ⇢ VMware Monitoring
- ⇢ Nutanix Monitoring
- ⇢ VMware Horizon Monitoring
- ⇢ AppLogs Monitoring



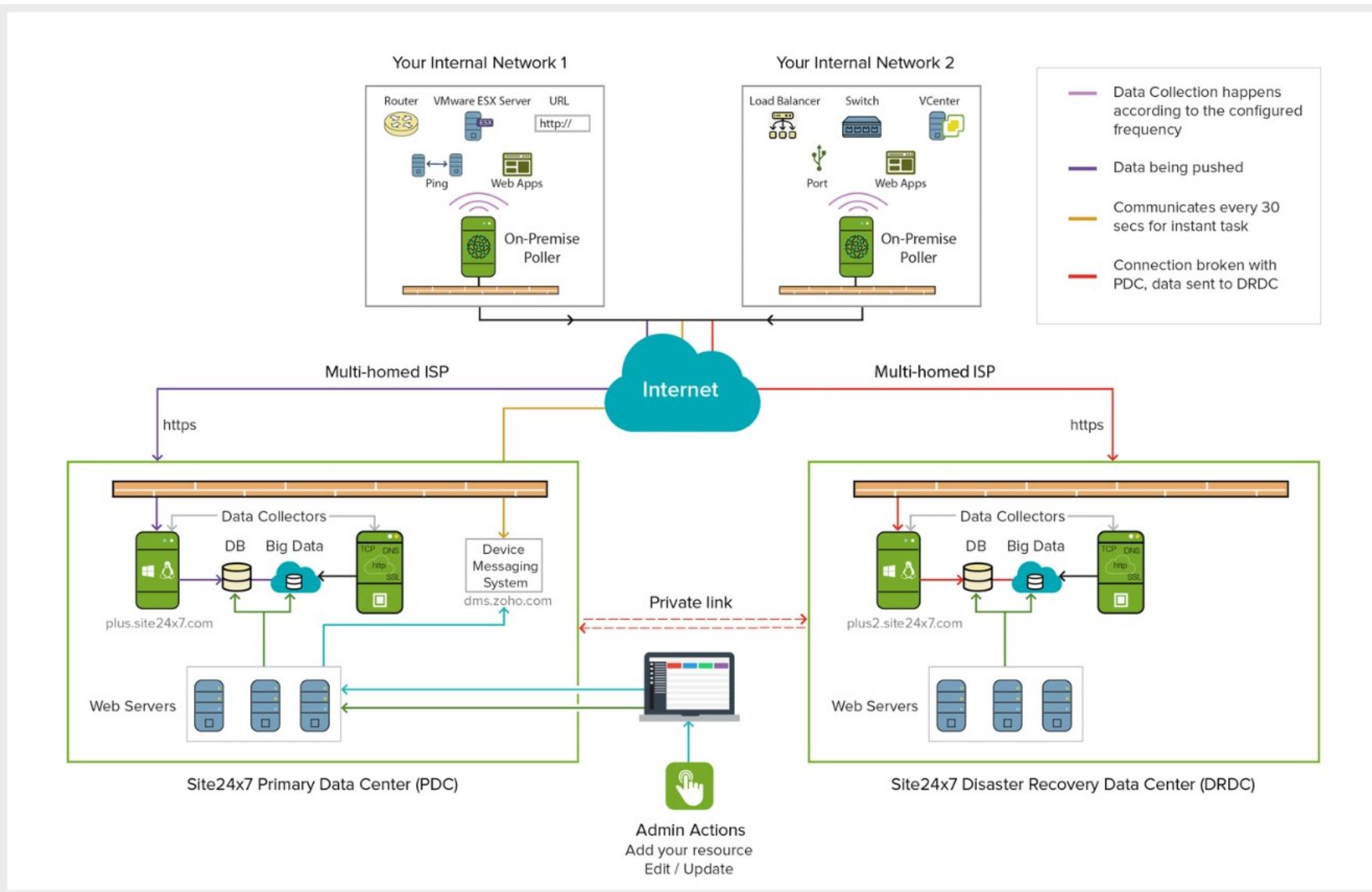
# Overview of On-Premise Poller

# 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

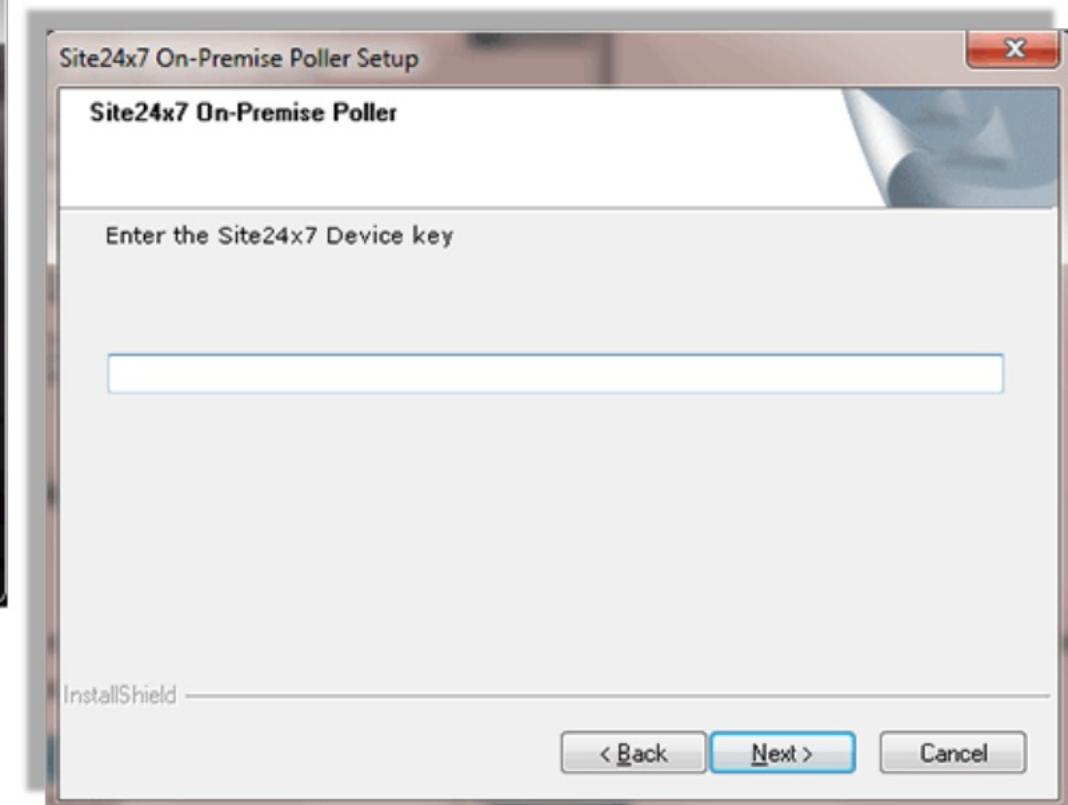
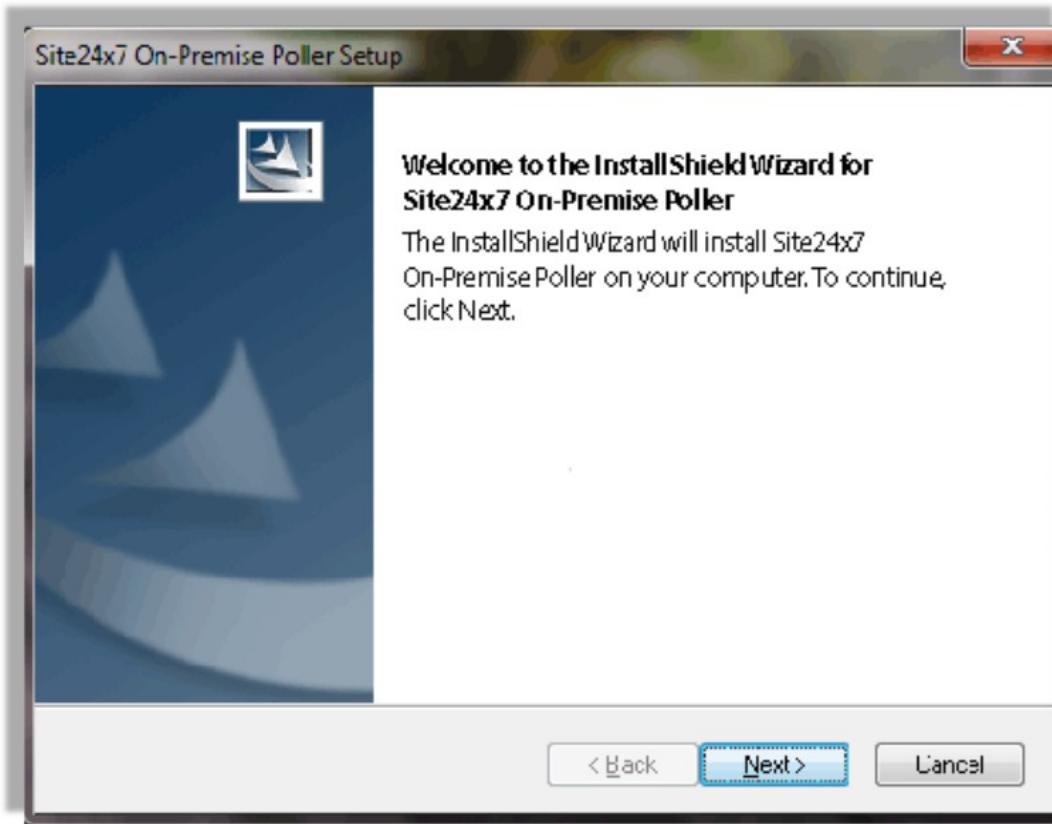
> plus2.site24x7.com

> pluspoller.site24x7.com

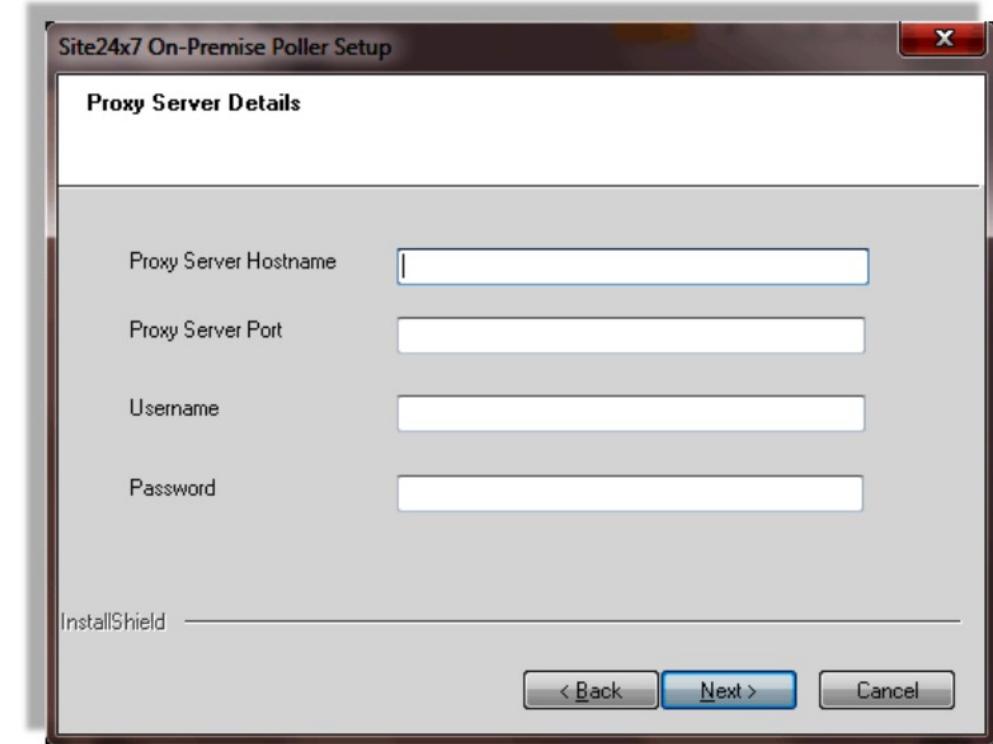
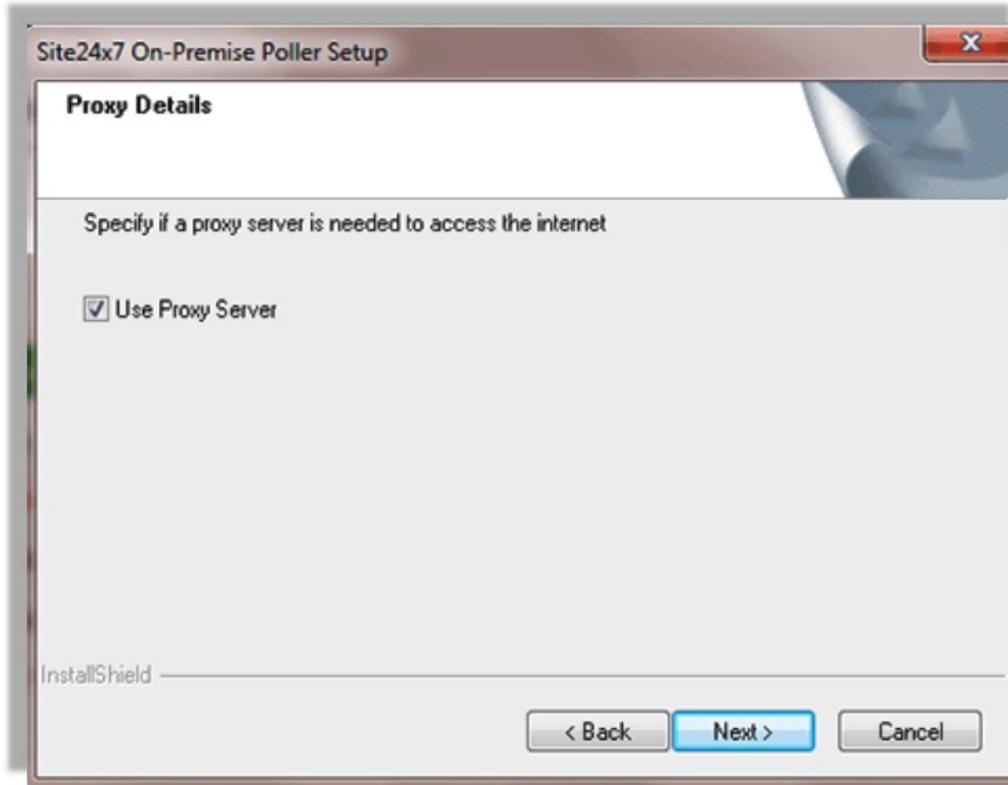
> plusnetwork.site24x7.com

> 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

The screenshot shows the Site24x7 On-Premise Poller monitoring interface for the module S24X7-NW-C4. The top navigation bar includes 'Summary' (selected), 'Network Module', 'Outages', 'Inventory', and 'Log Report'. A dropdown menu shows 'Last 24 Hours'. The main summary section displays:

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

A message indicates a 'Root Cause Analysis: Network Module is down.' with links to 'Create Request in ServiceDesk Plus' and 'On-Demand | On-Premise | MSP'.

The 'On-Premise Poller high availability' section shows the Primary On-Premise Poller (S24X7-NW-C4) and the Standby On-Premise Poller (S24X7-NW-C3), both in green status.

The 'Associated Monitors' section lists the following items:

Monitor display name	Status	Performance	Last Polled
ESX 172.21.112.41	Green		12:21 PM
192.168.222.58AS	Green	11.0 %	12:19 PM
datastore1	Green		12:19 PM
VM demo-vm-root1	Red		12:19 PM
VM demo-vm-root2	Red		12:18 PM
VM demo-vm-rp1-v3	Red		12:19 PM
VM demo-vm-v2	Red		12:18 PM

# High Availability Status

The screenshot displays the Site24x7 monitoring platform interface. On the left, a dark sidebar menu lists various monitoring categories such as Home, Inventory, User & Alert Management, Configuration Profiles, IT Automation Templates, Server Monitor, AppLogs, On-Premise Poller (selected), and many others. The main content area is titled "High Availability" and shows a table of poller configurations. The table has columns for Primary On-Premise Poller, Standby On-Premise Poller, Current High Availability Status, and Poll Now button. The pollers listed are: Zylker-QA-1 (Standby), S247-US-b1 (Standby), S24X7-ANZ-P3 (Standby), Zylker-3 (Monitoring from Primary), Zylker-US-1C (Standby), and Zylker-remote (Standby). A modal window titled "High Availability Status" is open, showing configurations for the Primary On-Premise Poller (S24X7-NW-C1) and the Standby On-Premise Poller (S24X7-NW-C3), with a "Check Now" button. Below the modal is a table titled "Monitors With Issue" listing network devices and their statuses.

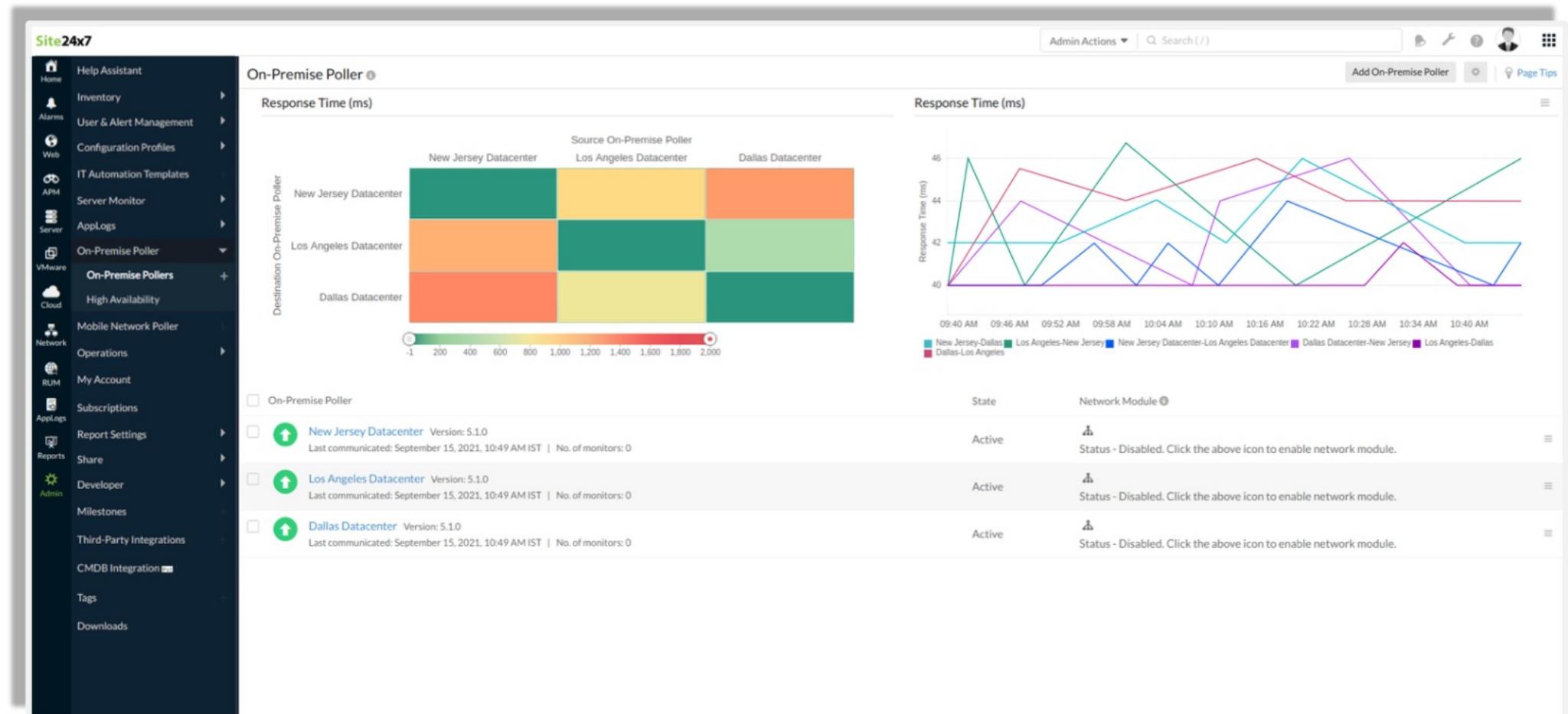
Monitor name	Monitor Type	Reason	Last updated
datastore	Datastore	Error in data collection.	Aug 7, 2019 12:09:06 PM
AP-03	Network Device	Device is not responding to the SNMP credential.	Aug 7, 2019 12:10:10 PM
Wireless AP-07	Network Device	Device is not responding to the SNMP credential.	Aug 7, 2019 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
192.168.50.222	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





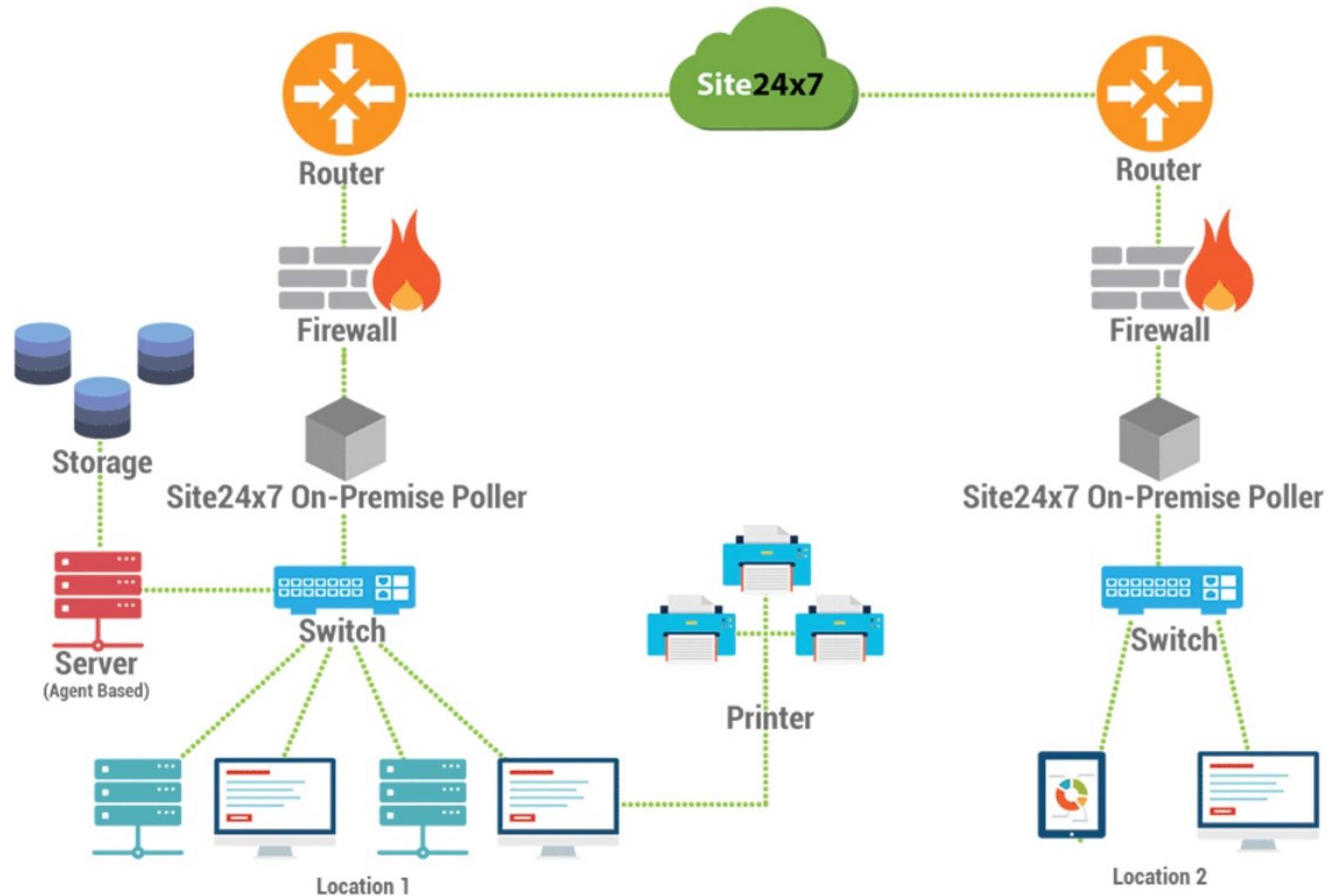
# Network Monitoring



# 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

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

# Adding a Network Monitor Step 1

Network Discovery

Step 1 Step 2 Step 3 Step 4 Step 5

On-Premise Poller Credentials Details Interface Filters Discover

You need an [On-Premise Poller](#) to monitor your network devices.

Choose an On-Premise Poller installed in the network to be monitored which also has network module enabled in it.

On-Premise Poller Name	Network Module <small>i</small>	IP Address	Number of Associated Monitors
<span>●</span> site24x7-support2	<span>✗</span> Status - Down	192.168.223.34	39
<span>●</span> S24X7-NW-U6	<span>✗</span> Status - Down	172.21.184.234	0
<span>●</span> S24X7-NW-U6	<span>✗</span> Status - Down	172.24.152.149	0
<span>●</span> S24X7-NW-C1	<span>✓</span> Status - Up	172.24.148.53	44

# Adding a Network Monitor Step 2

Network Discovery

Step 1 Step 2 Step 3 Step 4 Step 5

On-Premise Poller Credentials Details Interface Filters Discover

Page Tips

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"/>	Public	SNMP v1/v2	Default 'public' read community.	
<input type="checkbox"/>	SNMPV3	SNMP v3	Opmanager	
<input type="checkbox"/>	virtualIP	SNMP v1/v2		
<input type="checkbox"/>	Q2	SNMP v1/v2	Q2	
<input type="checkbox"/>	SNMPv3_1	SNMP v3	SNMP3User test credential	
<input type="checkbox"/>	public8001	SNMP v1/v2		
<input type="checkbox"/>	public_duplicate	SNMP v1/v2		

# Adding a Network Monitor Step 3

Network Discovery

Step 1 Step 2 Step 3 Step 4 Step 5

On-Premise Poller Credentials Details 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

Display Name Switch

Host Name / IP Address 192.168.49.106

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

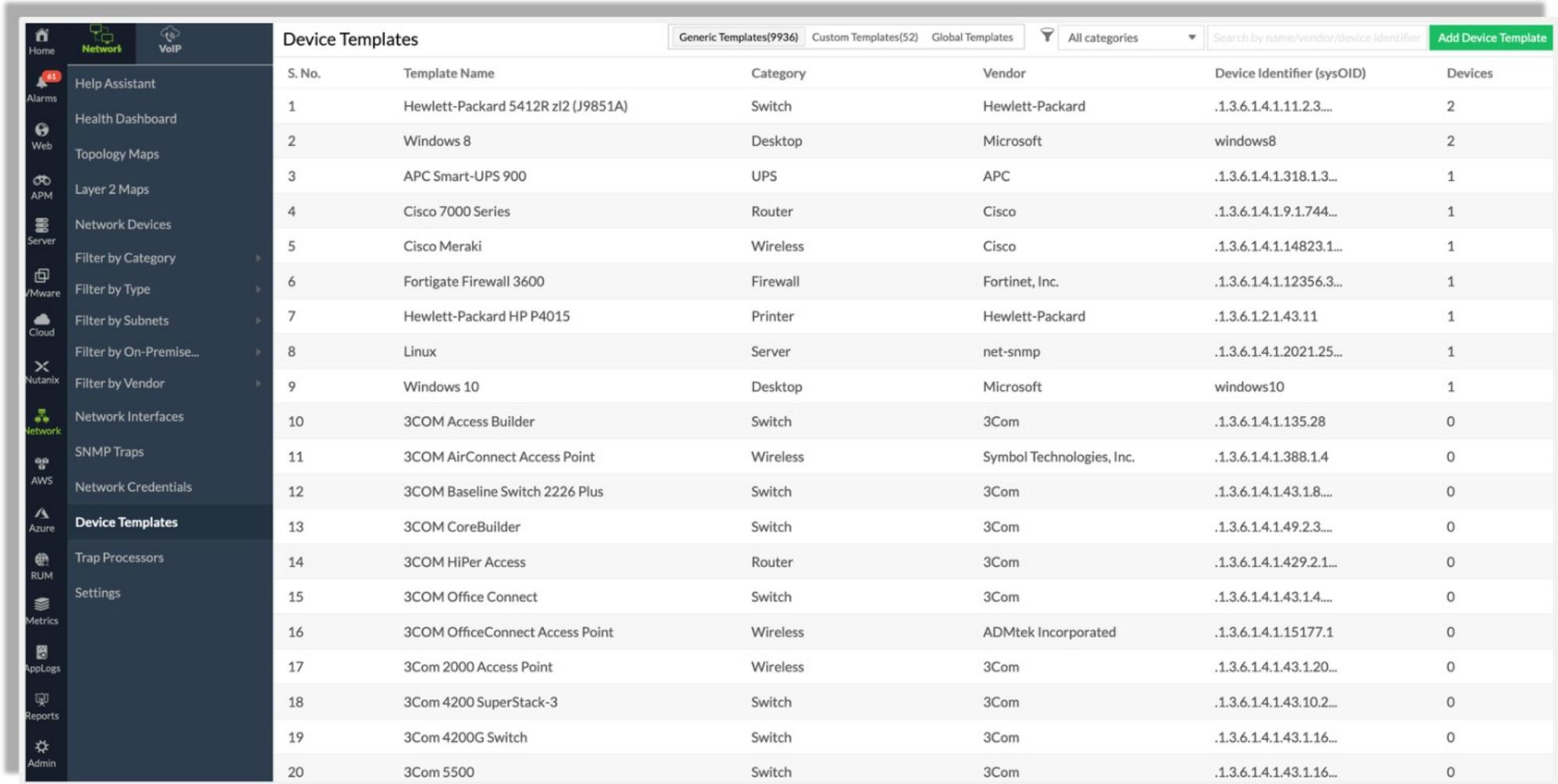
- Automatically discover all the devices present within a provided IP range or within a whole network using SNMP
- Once the devices are discovered, device templates are automatically associated
- Performance metrics of the device and interface status will be immediately displayed in the web console



## 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, AWS, Azure, RUM, Metrics, AppLogs, Reports, 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. The left sidebar contains navigation links for Home, Alarms, Web, APM, Server, VMware, Cloud, Network, RUM, AppLogs, Reports, Admin, and Edit. The main content area displays performance metrics for the device 10.10.10.1 (Network Device). The 'Performance Counters' tab is selected. Key metrics shown include:

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

Cisco Temperature

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

Used Memory

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

Free Memory

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

CPU Utilization (5 min)

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 shows 'Site24x7' and a search bar. The top right has a 'Register here' button, 'Plans and Pricing', and a help icon. The device being monitored is a 'Router' at 10.10.10.1, identified as a 'Network Device'. The timeline is set to 'Last 24 Hours'. The navigation tabs include Device Performance, Interfaces, Traps, Performance Counters (selected), Tabular Performance Counters, Router Performance, Outages, and More. The 'Tabular Performance Counters' section displays a table titled 'ifTable' with columns: Index, ifDescr, ifType, ifMtu, ifSpeed, ifPhysAddress, ifAdminStatus, ifOperStatus, and ifLastChange. The table lists 14 rows of network interface data.

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

Add Custom Performance Counters

**MIB BROWSER**

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

**SNMP OID**  **Test**

**Name**

**Description**

**Unit**

**Type**  Numeric  String

**Save Absolute**  Yes  No

**Format Value**  Yes  No

**Show in Monitor Summary Page**  Yes  No

**Add** **Reset**

**Vendor** All

**MIB** IANA-ENTITY-MIB

mib-2  
+ TEXTUALCONVENTION

## 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.

# Adding Custom Performance Counters - Tabular

Add Custom Performance Counters

MIB BROWSER

GENERAL MIBS CUSTOM MIBS

Vendor All

MIB IANA-ENTITY-MIB

+ mib-2  
TEXTUALCONVENTION

SCALAR TABULAR TABLE VIEW

SNMP OID .1.3.6.1.2.1 Test

Name mib-2

Description

Unit --

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.

# Adding Custom Performance Counters - Table View

Add Custom Performance Counters

The screenshot shows the 'Add Custom Performance Counters' interface. On the left is a tree view of performance counter categories under 'enterprises/storage/storageSystem'. A node named 'SystemIfTable' is selected. On the right, there are tabs for SCALAR, TABULAR, and TABLE VIEW. The TABLE VIEW tab is selected, showing a table titled 'Tabular Performance Counters'. The table has columns for S.No, Name, SNMP OID, Unit, Add To Table View (checkbox), and Action (button). Four rows are listed:

S.No	Name	SNMP OID	Unit	Add To Table View	Action
1	IfDescr	.1.3.6.1.4.1.24681.1.2.	String	<input checked="" type="checkbox"/>	
2	IfPacketsReceived	.1.3.6.1.4.1.24681.1.2.	Counter	<input checked="" type="checkbox"/>	
3	IfPacketsSent	.1.3.6.1.4.1.24681.1.2.	Counter	<input checked="" type="checkbox"/>	
4	IfErrorPackets	.1.3.6.1.4.1.24681.1.2.	Counter	<input checked="" type="checkbox"/>	

Below the table, there is a section titled 'Show in Monitor Summary Page' with 'Yes' and 'No' buttons. The 'Yes' button is selected.

## 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

**MIB BROWSER**

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

Vendor: QNAP  
MIB: NAS-MIB

**TABLE VIEW**

Name: SystemFanTable

Show in Monitor Summary Page: Yes

**Tabular Performance Counters**

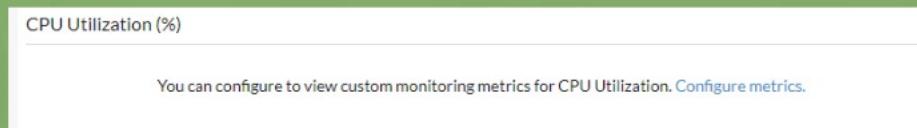
S.No	Name	Unit	SNMP OID	Add To Table View	Action
1	SysFanDescr	String	.1.3.6.1.4.1.24681.1.2.15.1.2	<input checked="" type="checkbox"/>	
2	SysFanSpeed	String	.1.3.6.1.4.1.24681.1.2.15.1.3	<input checked="" type="checkbox"/>	

Column of the Table View to be displayed in the Alert: SysFanDescr

Add Reset

# Adding Custom Monitor Metrics

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



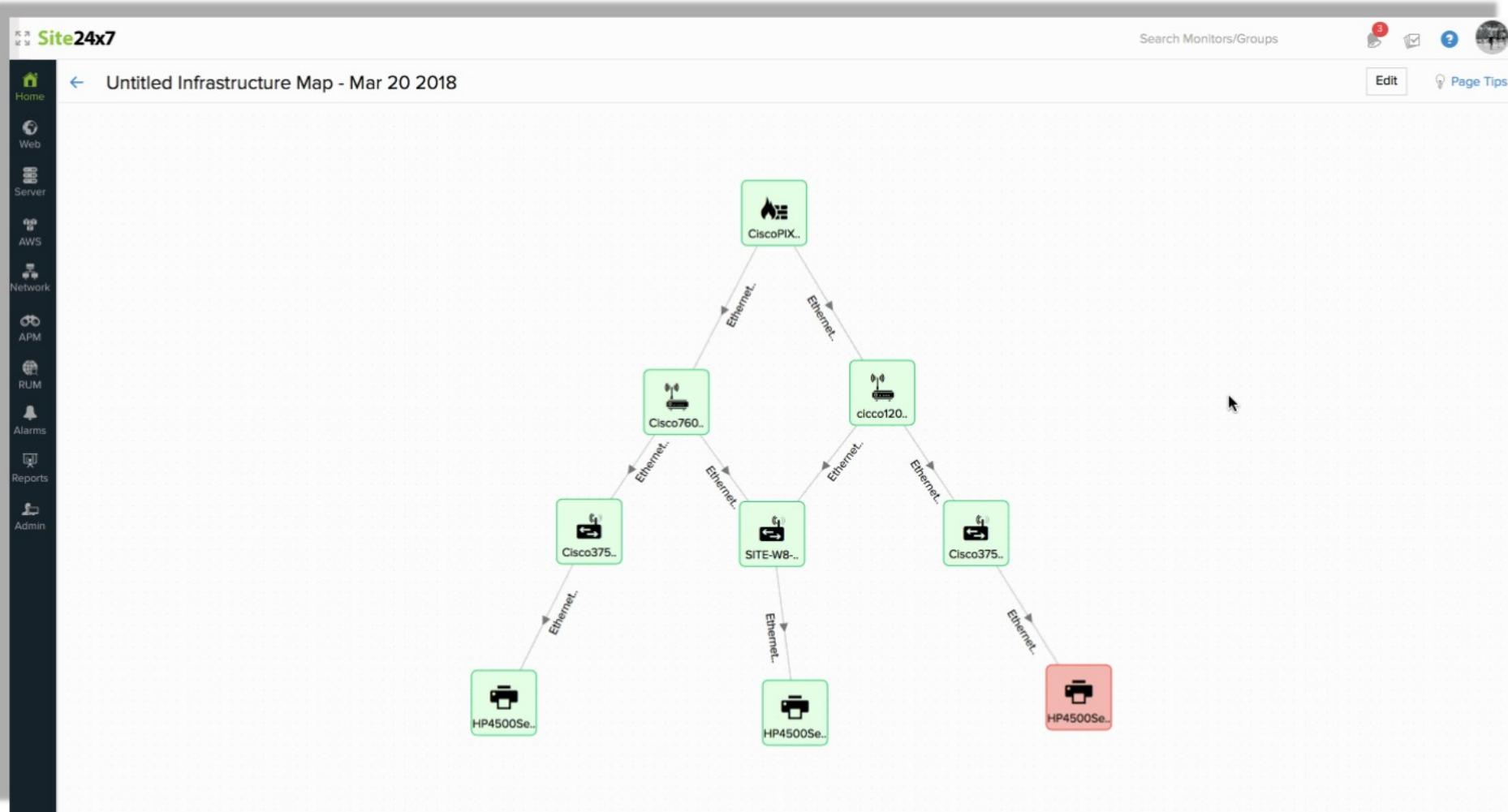
## Add Custom Monitor Metrics

Custom Monitor Metrics ⓘ X

CPU Utilization	<input type="text" value="None"/> <span style="border: 1px solid #ccc; padding: 2px 5px;">Test</span>
Memory Utilization	<input type="text" value="None"/> <span style="border: 1px solid #ccc; padding: 2px 5px;">Test</span>
Manufacturer	<input type="text" value="None"/> <span style="border: 1px solid #ccc; padding: 2px 5px;">Test</span>
Serial Number	<input type="text" value="None"/> <span style="border: 1px solid #ccc; padding: 2px 5px;">Test</span>
Model Name	<input type="text" value="None"/> <span style="border: 1px solid #ccc; padding: 2px 5px;">Test</span>

Save Cancel

# Viewing Details from Topology 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

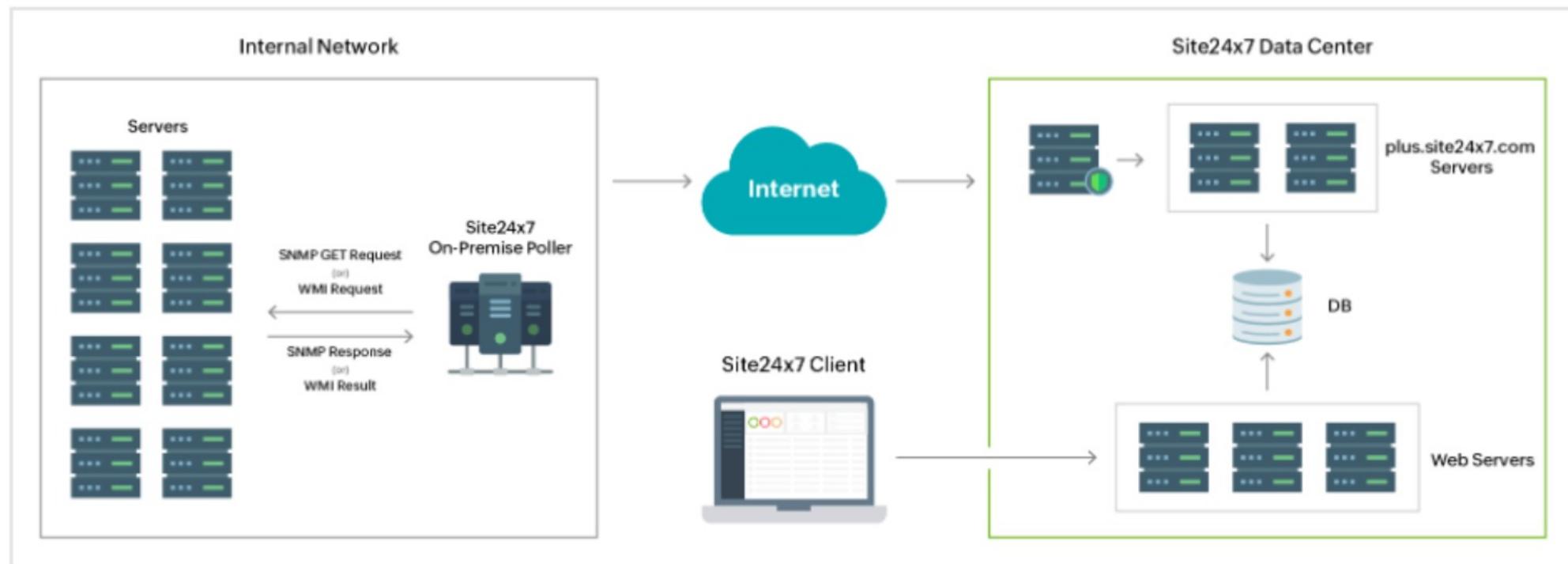
### Stack Switch Details

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 web 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 sections like Monitors, Configuration Profiles, and IT Automation Templates. The main content 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 with fields for "Hostname/IP Address" (10.10.10.3), "SSH/Telnet Credential" (CiscoRouterSSH), and "SNMP Credential" (Public). A "Connect" button is present. Below this, a message states "Site24x7 has connected to your device successfully. Choose a Source Interface and execute the below commands." A dropdown for "Source Interface" is set to "One". Under "Export Commands", the configuration includes "ip flow-export destination 172.24.147.201 9996" and "ip flow-export source One in flow-export version 5".

# 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, 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. The sub-tasks under Step 4 are "On-Premise Poller", "Flow Export Mode", "Flow Export Configuration", and "Choose Devices". 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

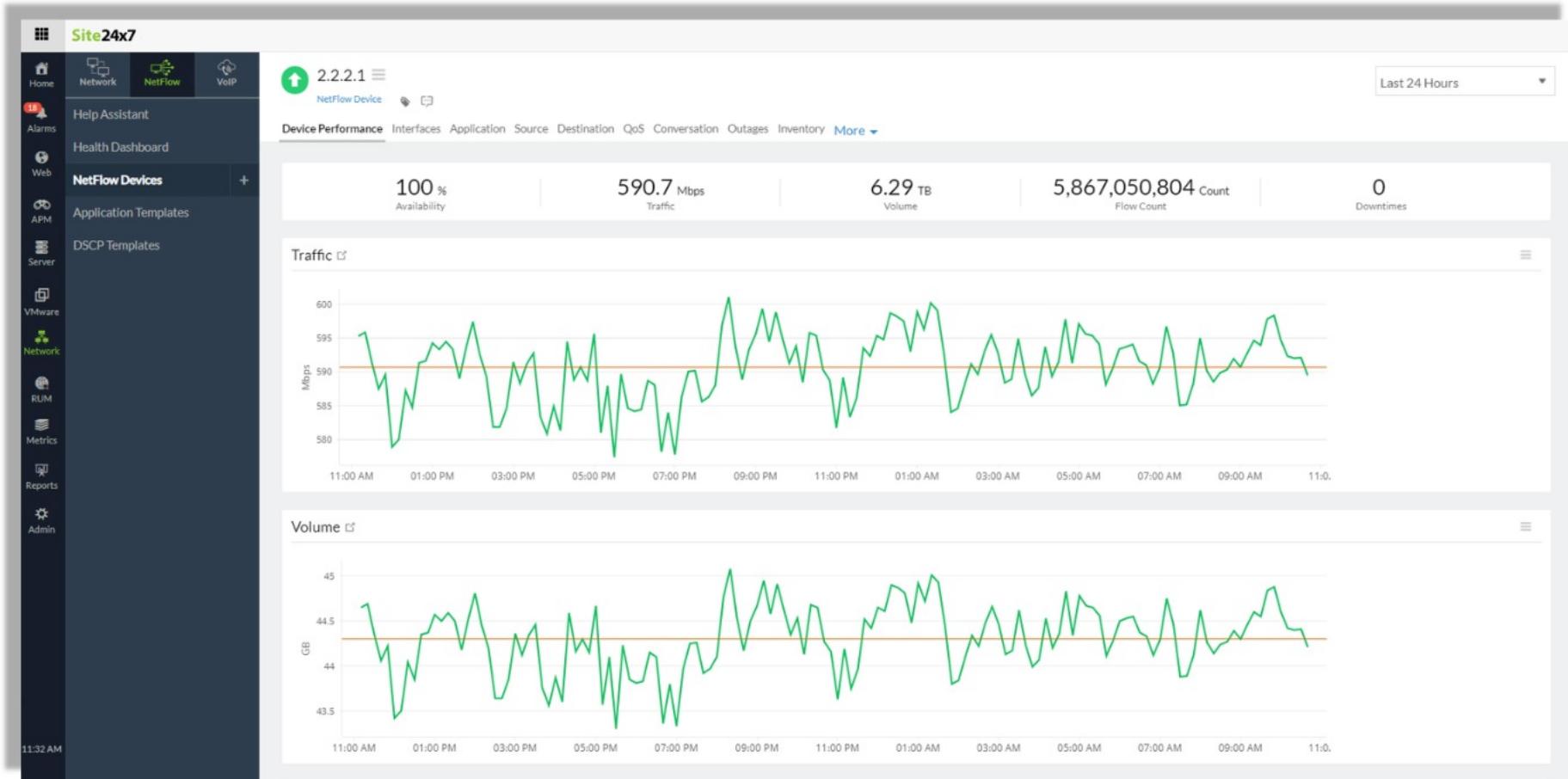
Back Next



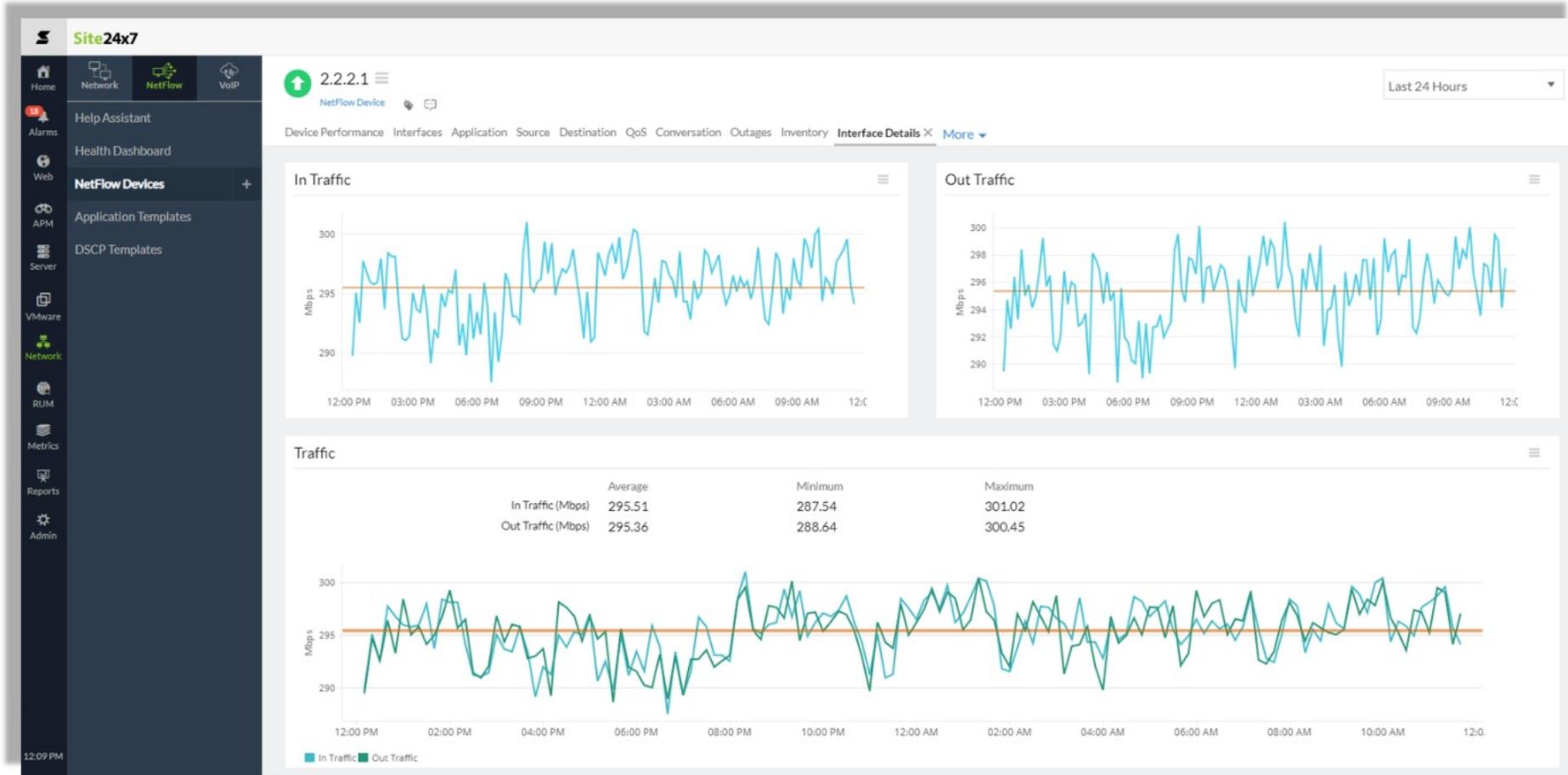
# Supported Templates

- …→ Application Templates
- …→ DSCP Templates

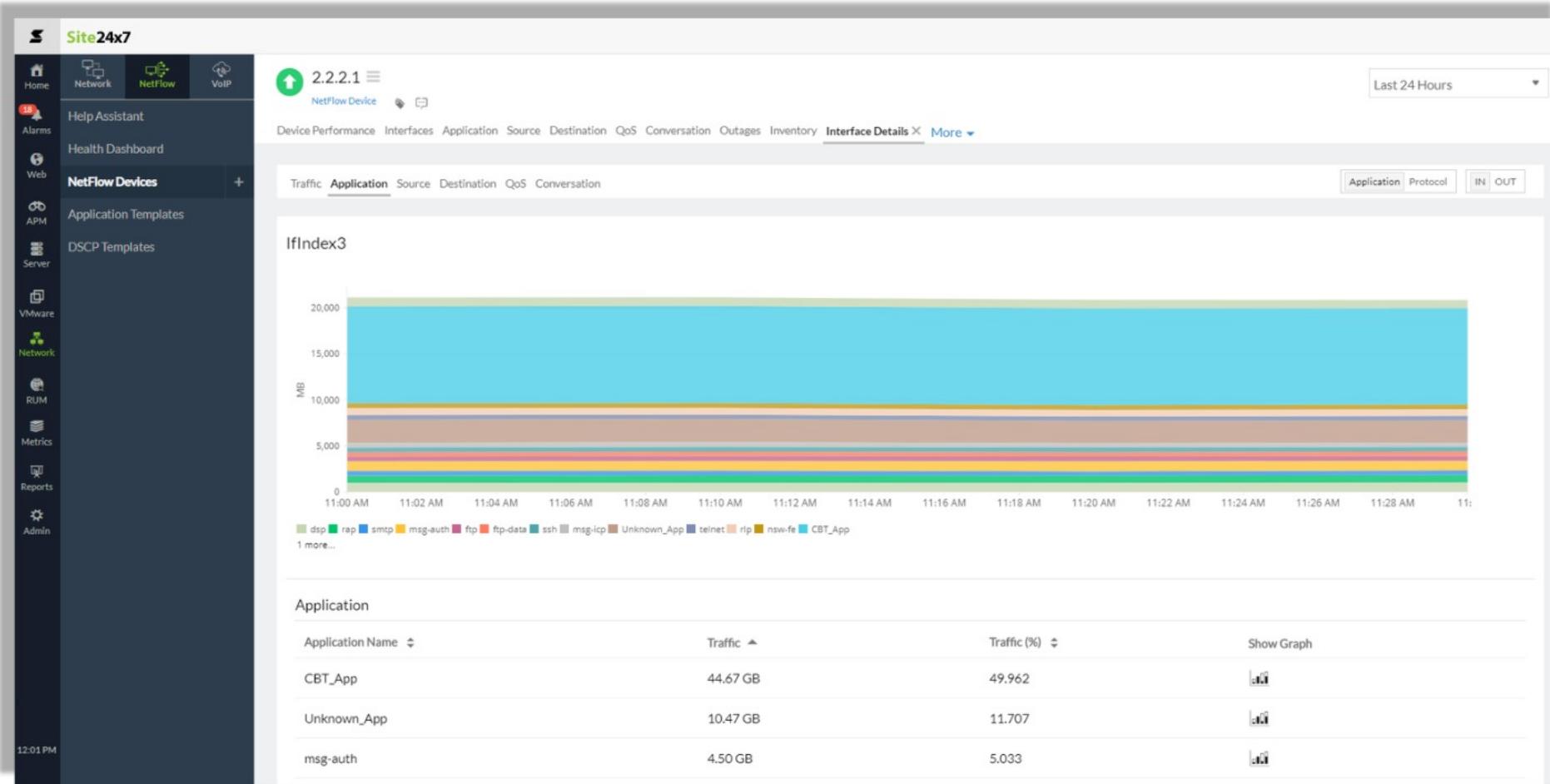
# NetFlow: Device Metrics



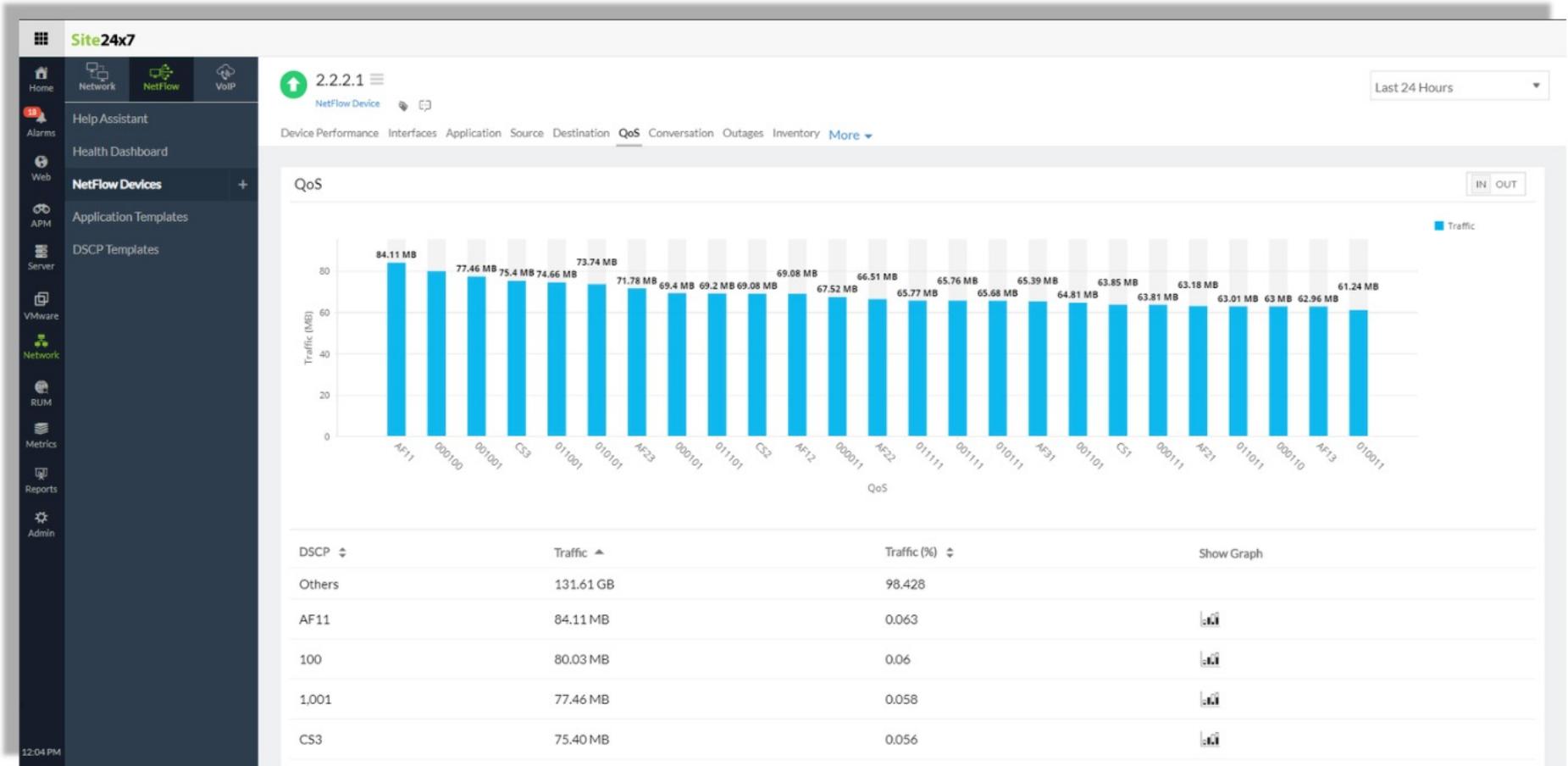
# NetFlow: Interface Metrics



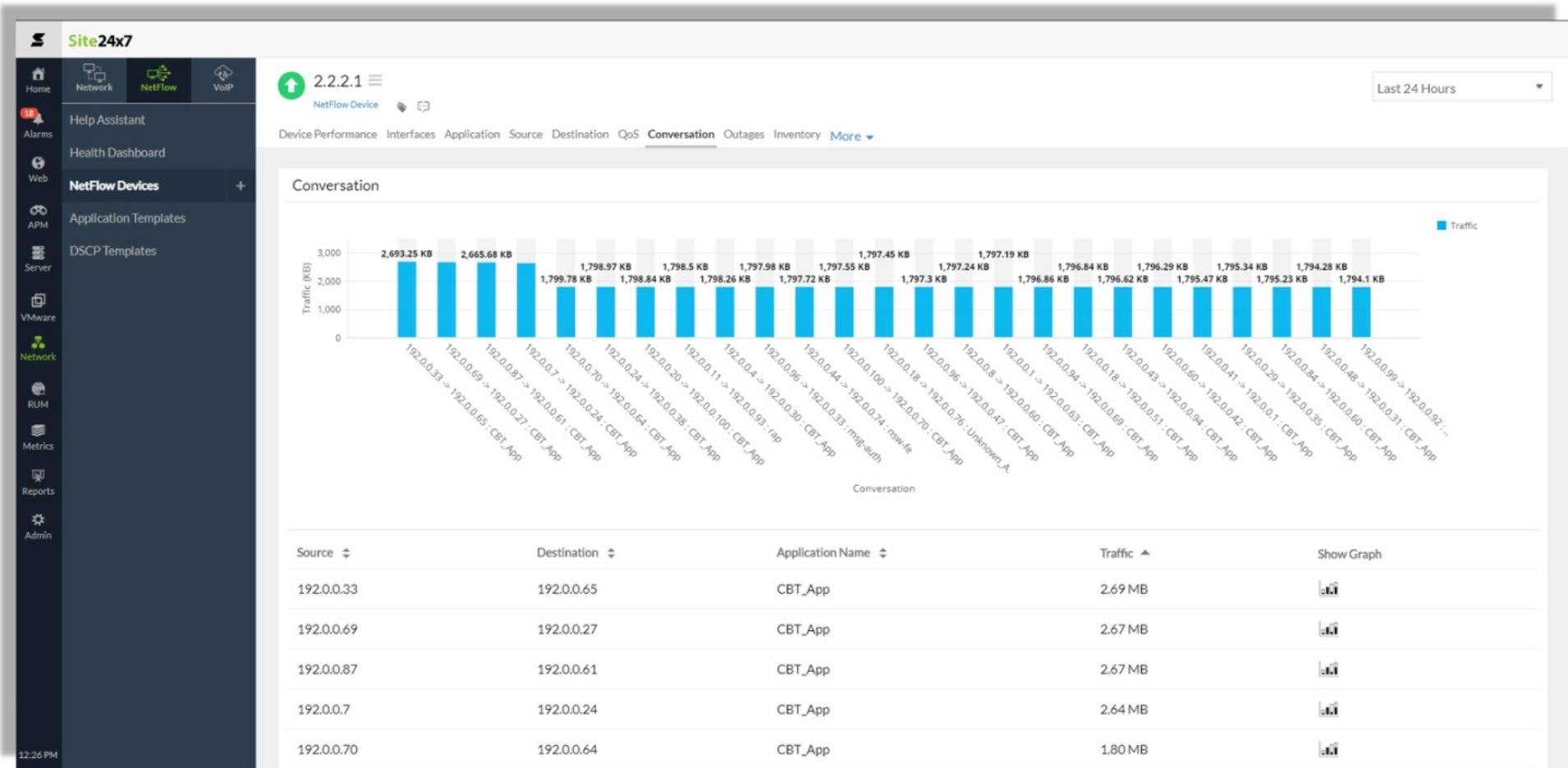
# NetFlow: Application Metrics



# 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 options like Home, Network, NetFlow, NCM, and APM. The 'Device Templates' option is selected and highlighted in blue. The main content area is titled 'Device Template: Cisco IOS Router'. It shows vendor information ('Vendor: Cisco'), operating system ('OS @: iOS'), and a description ('Description: For all Cisco IOS Routers'). Below this, there are four sections: 'Backup Running Configuration', 'Backup Startup Configuration', 'Disable Syslog Change Detection', and 'Enable Syslog Change Detection'. Each section lists commands, timeout values (all set to 20000 ms), and line feed types (all set to LF). The 'Device Templates' option in the sidebar is highlighted in blue.

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

# Device Configuration

**Site24x7**

All Monitors | Search (/)

Help Assistant

NCM Devices

Device Templates

NCM Credentials

**Device Configurations**

Configuration Changes

Compare Configurations

Settings

Cloud

Network

RUM

Metrics

Reports

Admin

Network

NetFlow

NCM Pro

Meraki Pro

### Device Configurations

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	≡

# Current configurations

The screenshot shows a left sidebar with various monitoring categories like MSP, Home, Alarms, Web, APM, Server, VMware, Cloud, Network, RUM, Metrics, and Reports. Under the 'Current Configurations' section, there is a list of monitors with their details. A context menu is open over the last monitor in the list, with a red box highlighting the three-dot options icon.

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.

# 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 from version 1, last changed on Oct 28 at 19:44:13 IST 2021. The R.H.S section shows a configuration for device 10.10.10.18 with a running configuration from version 3, last changed on Oct 29 at 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:

- Line 3: Building configuration... (Red)
- Line 4: (Blank)
- Line 5: Current configuration: (Red)
- Line 10: ! (Blue)
- Line 11: hostname Cisco360044 (Blue)
- Line 12: ! (Blue)
- Line 16: !prompt Cisco360044# (Blue)
- Line 19: ip address 10.10.10.14 (Blue)
- Line 20: cdp enable (Blue)
- Line 21: mtu 1500 (Blue)
- Line 25: cdp enable (Blue)
- Line 28: interface Serial0 (Blue)
- Line 29: ip address 10.10.10.14 (Blue)
- Line 30: mtu 1800 (Blue)
- Line 31: ! (Blue)
- Line 32: interface Serial0 (Blue)
- Line 33: ip address 127.0.0.1 (Blue)
- Line 34: mtu 1800 (Blue)
- Line 35: ! (Blue)
- Line 36: interface Serial1 (Blue)
- Line 37: ip address 10.10.10.14 (Blue)
- Line 38: mtu 1500 (Blue)
- Line 39: ! (Blue)

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

A purple callout box on the right side of the diff view area contains the text: '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.
- Devices Monitored:** 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:** A line chart showing packet loss percentage over time. The Y-axis ranges from 0 to 100. The X-axis shows dates from 07:11 to 12:41. The chart shows a constant baseline around 50% packet loss.
- Response Time of mx01-dl1:** A line chart showing response time in milliseconds (ms) over time. The Y-axis ranges from 0 to 10. The X-axis shows dates from 07:11 to 12:41. The chart shows a constant baseline around 8 ms with occasional spikes reaching up to 10 ms.



# 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

# 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, 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, 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



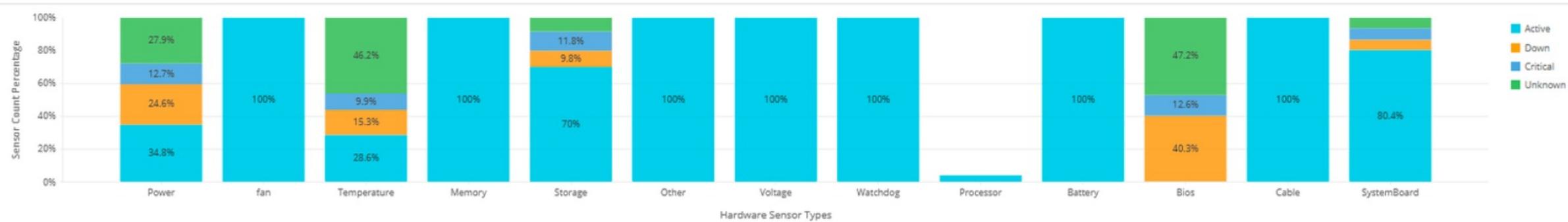
# VMware Hardware Monitoring

- 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



# Log Profile

Log Profile <small>i</small>				Add Log Profile	<small>💡</small> Page Tips
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>				Add Log Type	<small>💡</small> Page Tips
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 \$Me	\$UserAgent\$ \$Referer\$ \$StatusCode:long\$ \$SubStatusCode:long\$ \$WindowsStatusCode:long\$		Enabled	

# Custom Log type

Display Name i Custom Application

Log Type name is an unique identifier for logs following the same format. NOTE: The name should not have spaces or any special characters and cannot be edited later.

Retention (days) i 30

Maximum Upload Limit (GB) i

Auto Discovery i Enable Disable

Sample Logs i Minimum 3 Lines Required

Log Pattern i eg:\$LogTime:date:yyyy-MM-dd HH:mm:ss,SSS\$ \$LogLevel\$ \$BytesTransferred:number\$ \$message\$ ?

API Upload i Enable Disable

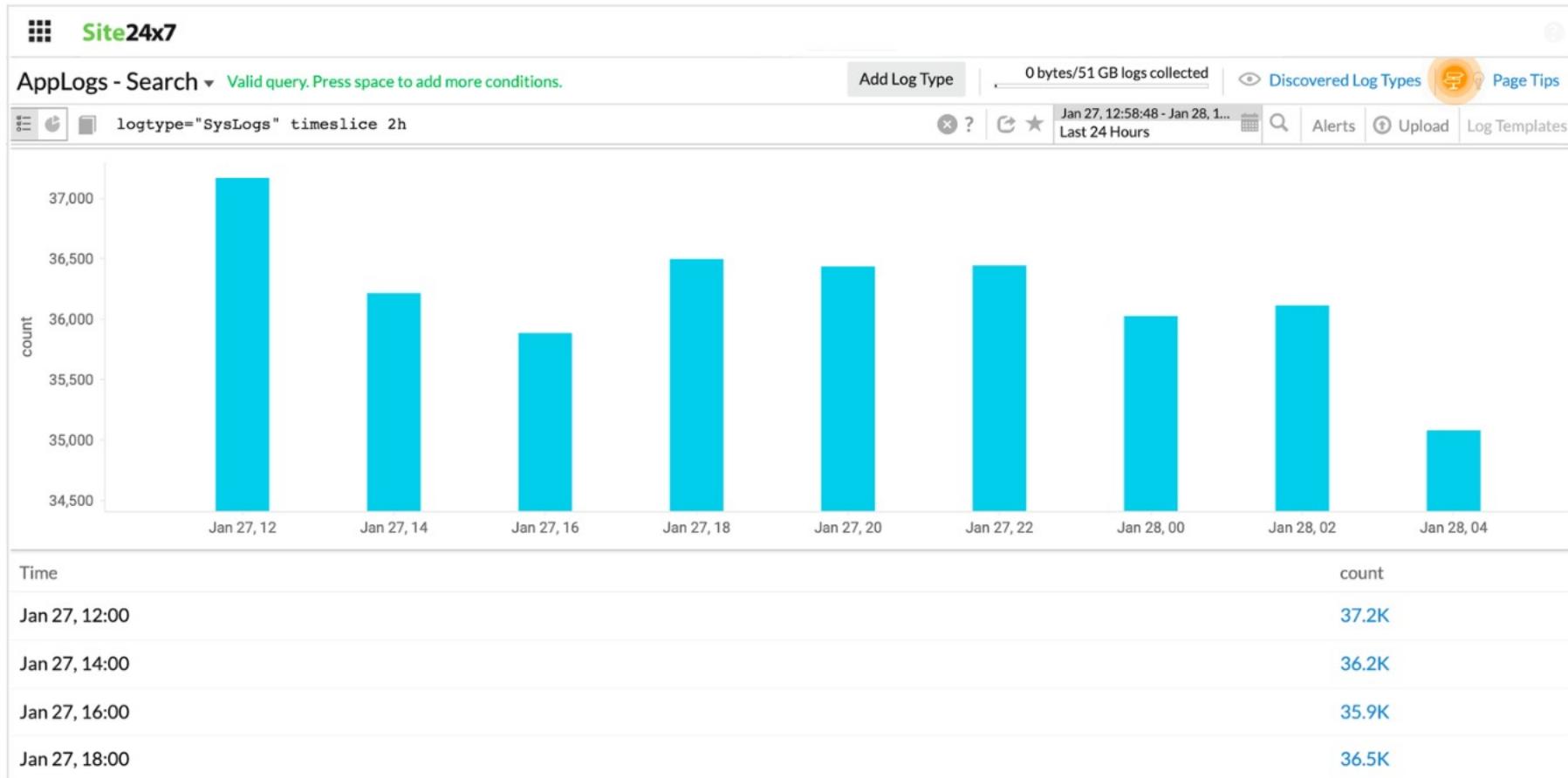


# AppLogs Query Language

- 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

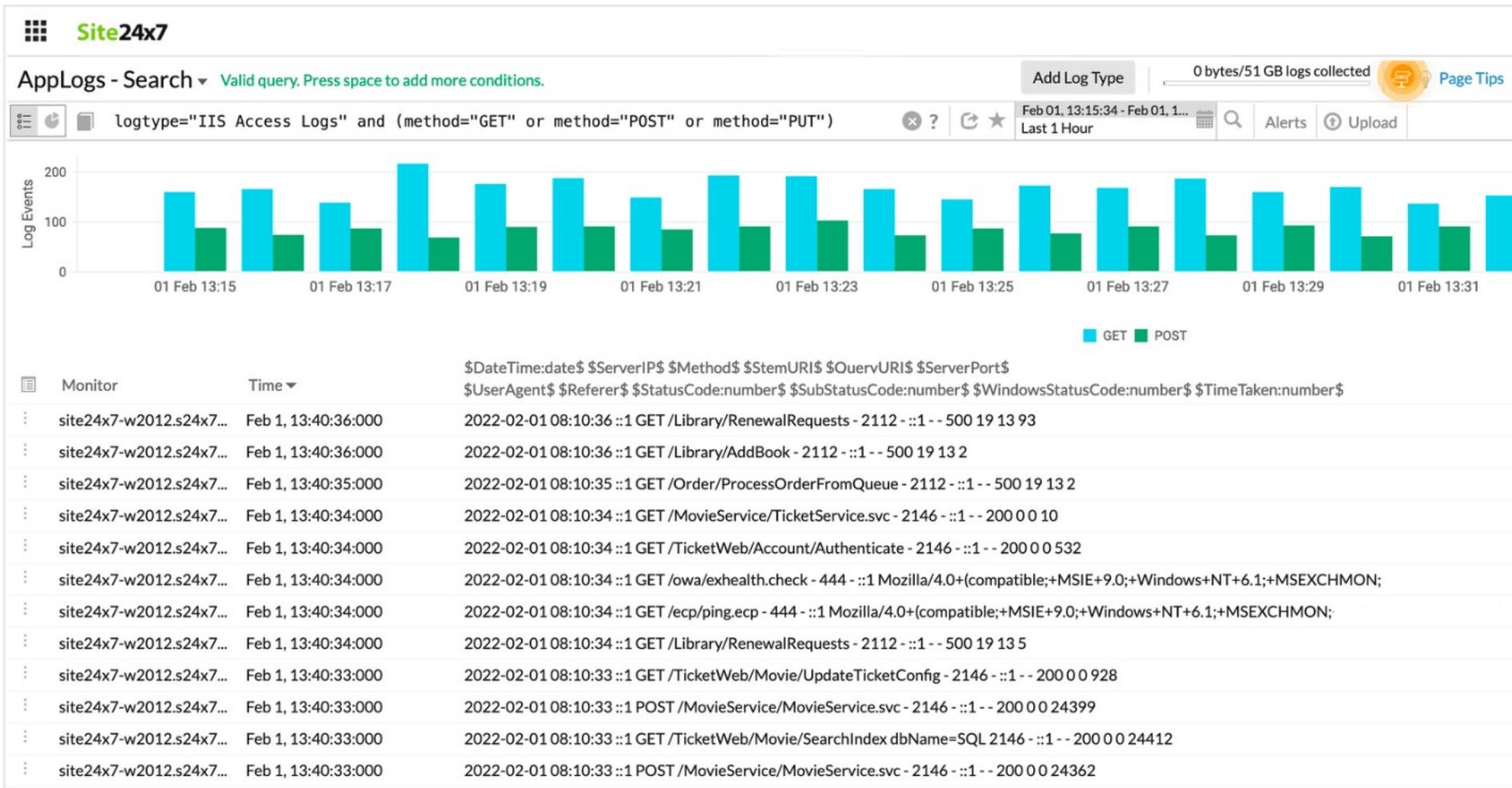


# Time Slice Report



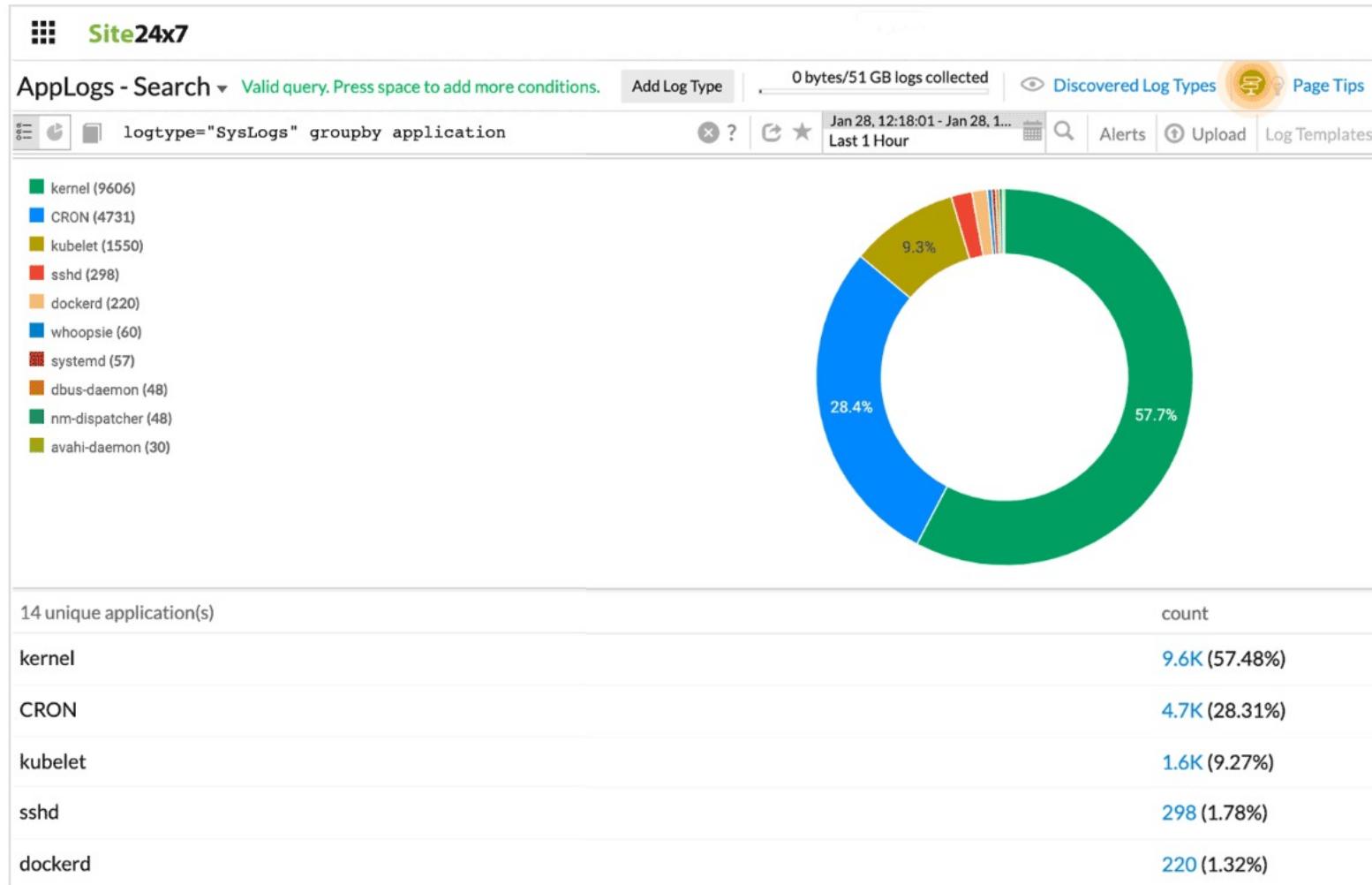


# Log Report



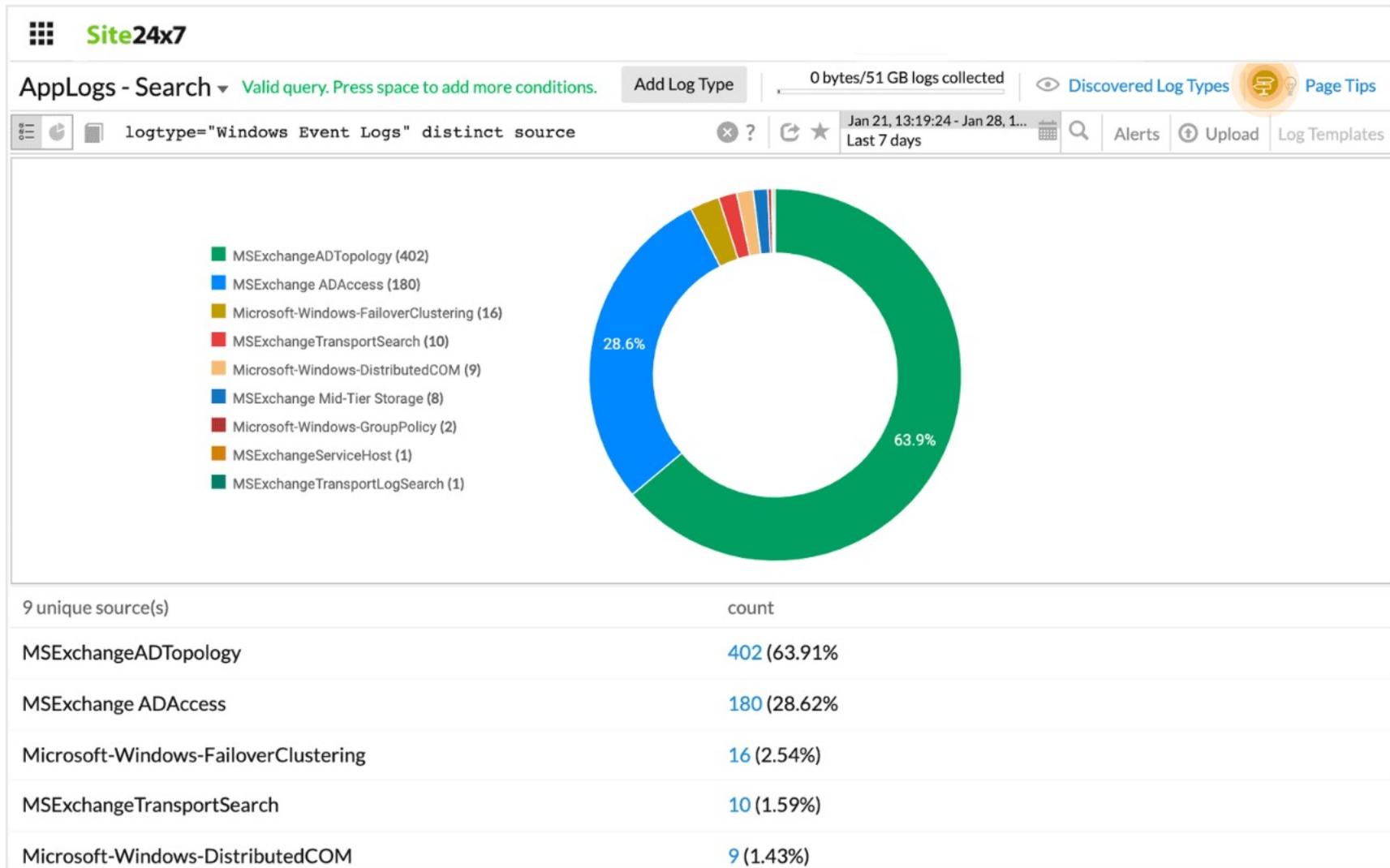


# Groupby Report

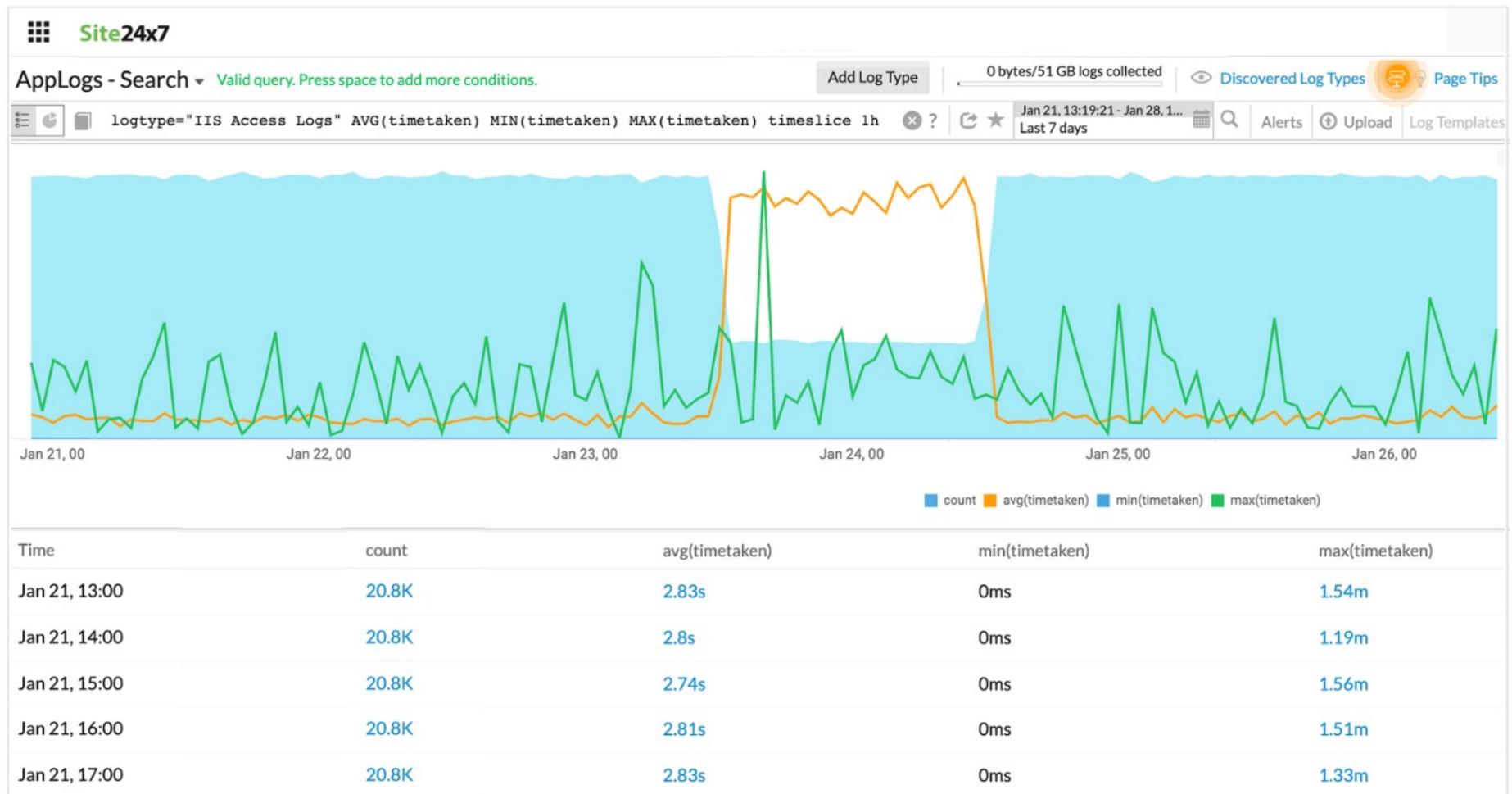




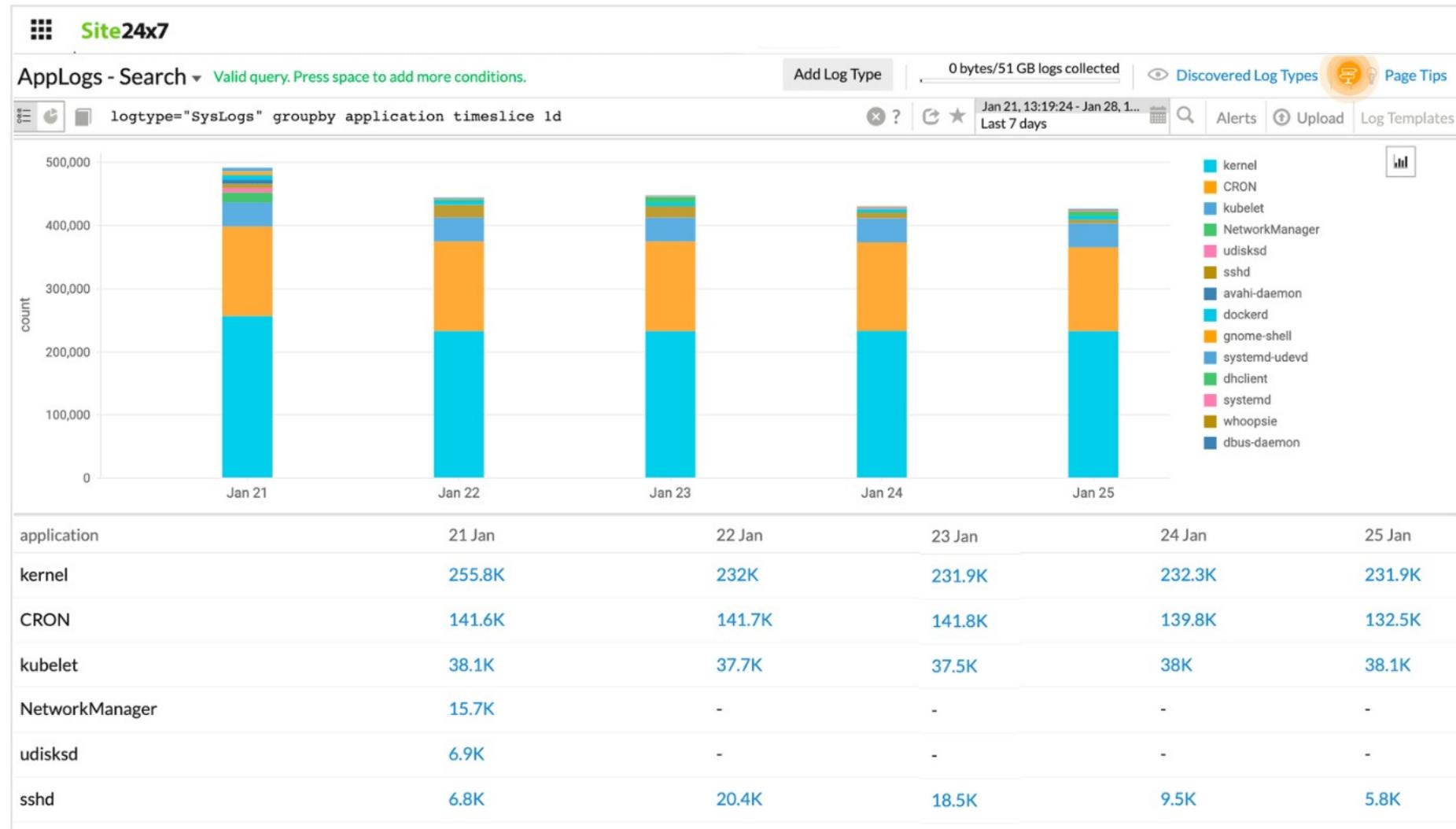
# Distinct Report



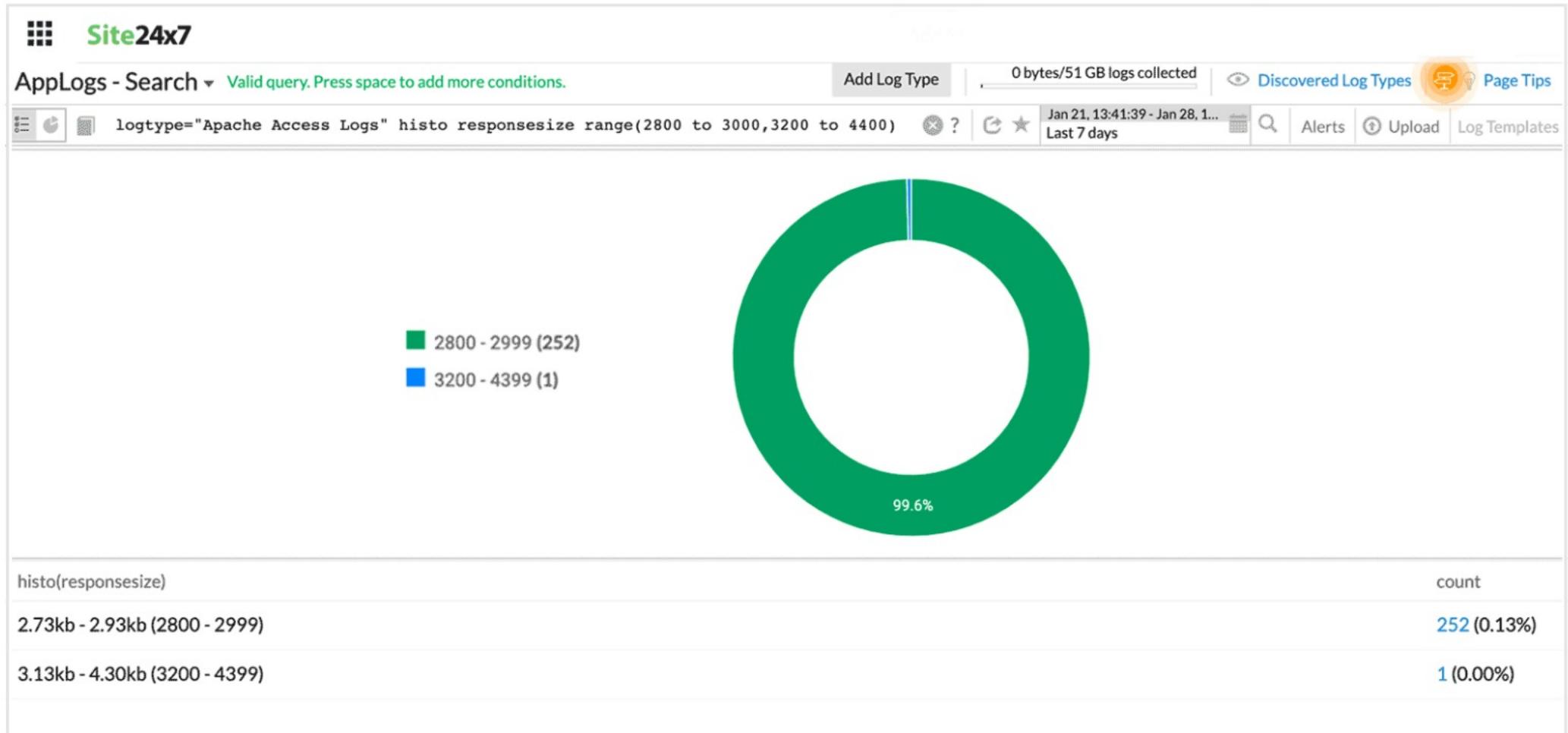
# Combining Timeslice and Aggregation Together



# Combining Groupby and Timeslice Together



# Histo with Range



# Key performance Indicator

The screenshot shows the Site24x7 application logs search interface. On the left, a sidebar lists monitoring categories: Home, Alarms, Web, APM, Server, VMware, Cloud, Network, RUM, and AppLogs (which is selected). 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 filters for time (Feb 01, 11:10:39 - Feb 02, 1... Last 24 Hours), log type (Add Log Type), and file size (0 bytes/51 GB logs collected). Below the search bar, a large KPI value is displayed: **268.7 K** (down 10.98% from 7 days ago: 301.9K). At the bottom, a note indicates "Showing 1 - 100 log events out of 201055".

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

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

Feb 01, 11:10:39 - Feb 02, 1... Last 24 Hours

Feb 01, 11:10:39 - Feb 02, 1... Last 24 Hours

Home  
Alarms  
Web  
APM  
Server  
VMware  
Cloud  
Network  
RUM  
AppLogs

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

logtype="IIS Access Logs"

Total Requests Count 500.5k Average Response Time avg(timetaken) 2.64s

Failed Requests Count 262.3k timetaken avg(timetaken) 2.64s

timetaken min(statuscode) 200 sum(windowsstatuscode) 220164725563747

Top 20 Failed Requests

- /rpc/rpcproxy.dll (35271)
- /powershell (34176)
- /Microsoft-Server-ActiveSync/Proxy (12762)
- /owa/proxylgion.owa (10992)
- /Library/EditBook (8451)
- /Account/MemberLogin (8447)
- /MovieService/BookingService.svc (7781)
- /Library/ReturnedBooks (7487)

User Agent Stats

Browser Device OS

UNKNOWN - 498,715

Request Trend

Browser Device OS

UNKNOWN - 498,715

Status Code Stats

Date & Time	2XX	3XX	4XX	5XX				
Total	234894	45.95%	8412	1.65%	126542	24.75%	141392	27.66%
06 Jul, 12:00	9906	45.95%	355	1.65%	5374	24.93%	5923	27.47%
06 Jul, 01:00	9766	45.86%	347	1.63%	5238	24.6%	5942	27.91%
06 Jul, 02:00	9850	45.96%	355	1.66%	5310	24.78%	5916	27.6%

Response Time Stats

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
> 60 secs	691	16	57	45	24	22	24	12
30-60 secs	26K	1160	1067	1110	1119	1070	1133	1124
10-30 secs	665	13	46	31	14	29	17	21
5-10 secs	1K	28	54	47	25	54	49	30

# AppLogs Alerts

The screenshot displays the Site24x7 AppLogs interface. On the left, there's a sidebar with various monitoring categories like Home, Alarms, Web, APM, Server, VMware, Cloud, Metrics, AppLogs, Reports, Admin, and Help. The main area shows a search bar with the query "logtype='Windows Event Logs'". Below it is a chart titled "Log Events" showing event counts over time from Jan 16 to Jan 17. To the right of the chart is a detailed log table listing events from IP 179.50.90.226, including timestamp, event ID, type, and level. Overlaid on the interface is a modal window titled "Create Alert". The modal contains fields for "Display Name" (set to "Windows Alert"), "Search Query" (set to "logtype='Windows Event Logs'"), "Alert Type" (set to "Count Based Alert"), "Check Frequency" (set to "15 Minutes"), and "Attribute" (set to "count"). A red box highlights the "Threshold Configuration" section, which includes two rows of conditions: "Condition > Threshold 1 Notify As Trouble Automation Server" and "Condition >= 10 Notify As Critical Automation No items selected". Below this is the "Configuration Profiles" section with a "Notification Profile" set to "Default Notification". The "User Alert Group" section has checkboxes for "Admin Group" (checked), "Application T...", and "Network Team" (unchecked). There are also "Tags" and "Third-Party Integrations" sections, with "Slack Integration" checked under "Services". 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, there's a navigation sidebar with various monitoring and management options like Home, Inventory, User & Alert Management, Configuration Profiles, IT Automation Templates, Server Monitor, AppLogs (selected), Log Profile, Log Types, Saved Searches, Alerts, Settings, On-Premise Poller, Mobile Network Poller, Operations, My Account, Control Panel Settings, Subscriptions, Report Settings, Share, Developer, Milestones, Third-Party Integrations, CMDB Integration, Tags, and Downloads. The main area is titled "Edit Log Type" and shows "RequestURI - Field Configurations". It lists fields such as MachineIP, RemoteLogName, RemoteUser, Method, RequestURI, Protocol, Status, ResponseSize, Referer, UserAgent, and TimeTaken. For each field, there are options to "Hide this Field from Search Result" (Yes or No), "Character Length for Groupby" (input field), "Enable Masking" (Yes or No, with regex patterns like apiKey=(\.)& API\_KEY), and "Enable Hashing" (Yes or No, with regex patterns like &email=(\.)s). Below these settings, there's a section for "Filter Log Lines at Source" with "Select Log Line only if this Field" (Matches or Doesn't Match) and "Any of These Values" (input field). There's also an option to "Ignore this Field at Source" (Yes or No). At the bottom, there's an "Apply" button, a note about field type being immutable, and a note about API Upload (Enable or Disable). A message at the bottom states: "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." The right side of the screen shows a log entry with masked fields.

RequestURI - Field Configurations

MachineIP Display Name RequestURI

RemoteLogName Hide this Field from Search Result Yes No

RemoteUser Character Length for Groupby

Method

RequestURI Enable Masking Yes No apiKey=(\.)& API\_KEY Expressions that you want masked must be expressed as a capture group in the regex

Protocol

Status

ResponseSize

Referer Select Log Line only if this Field Matches Doesn't Match

UserAgent Any of These Values Type and press Enter to add values to filter

TimeTaken Ignore this Field at Source Yes No

Apply

UserAgent "Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36" "Mozilla/5.0 (X11; Linux x86\_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/66.0.3359.139 Safari/537.36"

TimeTaken (μs) 982712 1192712

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"

Dashboard | 4.19 GB/51 GB logs collected | Discovered Log Types | Page Tips | Nov 16, 05:05 - Nov 17, 05:05 | Last 24 Hours | ? | Alerts | Upload | Log Templates

Log Events

16-Nov-20 05:35 16-Nov-20 06:05 16-Nov-20 06:35 16-Nov-20 09:35 16-Nov-20 09:50 16-Nov-20 10:05 16-Nov-20 10:20

Monitor Time ▾ \$ReqId\$ \$as \$Host\$ \$ZLOC\$ \$ZUID\$ \$ZOID\$ "\$TIMESTAMP:date\$" \$ResponseTime:number\$ \$Method\$ \$Encoding\$ \$StatusCode:number\$ \$RequestURL\$ \$ThreadId\$ \$RemoteIP:ip\$ \$internalIp\$ \$SessionId\$ \$TicketDigit\$

magesh-1870 Nov 16, 10:29:24.272 74 sas 172.20.45.1 - "16-11-2020 23:59:34:272" 5 GET UTF-8 404 /app/applog/modules/applog/related-logs/applog-related-logs-services.js 564 10.59.0.178 --

Fields to Filter

Related Log Templates

Follow Application Log

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

Add Related Log Template

magesh-1870 Nov 16, 10:29:32.966 68 sas 172.20.45.1 -- "16-11-2020 23:59:32:966" 3 GET UTF-8 404 /app/applog/modules/applog/related-logs/applog-related-logs-controller.js 580 10.59.0.178 --

magesh-1870 Nov 16, 10:29:32.966 67 sas 172.20.45.1 -- "16-11-2020 23:59:32:966" 3 GET UTF-8 404 /app/applog/modules/applog/related-logs/applog-related-logs-services.js 557 10.59.0.178 --

magesh-1870 Nov 16, 10:29:32.641 66 sas 172.20.45.1 -- "16-11-2020 23:59:32:641" 4 GET UTF-8 404 /app/applog/modules/applog/related-logs/applog-related-logs-directive.js 579 10.59.0.178 --

magesh-1870 Nov 16, 10:29:32.631 65 sas 172.20.45.1 - 60731599 - "16-11-2020 23:59:32:631" 15 GET UTF-8 304 /app/applog/modules/applog/infrastructure-events/applog-infraevents-directives.js 578 10.59.0.178 --

magesh-1870 Nov 16, 10:29:32.380 64 sas 172.20.45.1 - 60731599 - "16-11-2020 23:59:32:380" 12 GET UTF-8 304 /app/applog/modules/applog/parser-hint.js 577 10.59.0.178 -- ba0e73adfa8d0311af00d10d252d2946

magesh-1870 Nov 16, 10:29:32.358 63 sas 172.20.45.1 - 60731599 - "16-11-2020 23:59:32:358" 14 GET UTF-8 304 /app/applog/modules/applog/applog-directive.js 576 10.59.0.178 -- ba0e73adfa8d0311af00d10d252d2946

magesh-1870 Nov 16, 10:29:32.105 62 sas 172.20.45.1 - 60731599 - "16-11-2020 23:59:32:105" 12 GET UTF-8 304 /app/applog/modules/applog/applog-controller.js 575 10.59.0.178 -- ba0e73adfa8d0311af00d10d252d2946

magesh-1870 Nov 16, 10:29:32.083 61 sas 172.20.45.1 - 60731599 - "16-11-2020 23:59:32:083" 15 GET UTF-8 304 /app/applog/modules/applog/applog-filters.js 574 10.59.0.178 -- ba0e73adfa8d0311af00d10d252d2946

magesh-1870 Nov 16, 10:29:31.785 60 sas 172.20.45.1 - 60731599 - "16-11-2020 23:59:31:785" 18 GET UTF-8 304 /app/applog/modules/applog/applog-services.js 573 10.59.0.178 -- ba0e73adfa8d0311af00d10d252d2946

magesh-1870 Nov 16, 10:29:31.785 59 sas 172.20.45.1 - 60731599 - "16-11-2020 23:59:31:785" 17 GET UTF-8 304 /app/applog/modules/applog/applog-router.js 572 10.59.0.178 -- ba0e73adfa8d0311af00d10d252d2946

Showing 1 - 100 log events out of 432 ×

The screenshot shows the Site24x7 interface for monitoring application logs. A specific log entry for 'magesh-1870' on Nov 16, 10:29:24.272 is highlighted. Below the log entry, there are sections for 'Fields to Filter', 'Related Log Templates', and 'Follow Application Log'. The 'Related Log Templates' section is expanded, showing several other log entries from the same host and timestamp, which are related to the original log entry. The interface includes a sidebar with various monitoring modules like Home, Alarms, Web, APM, Server, VMware, Cloud, Network, AWS, Azure, RUM, Metrics, and AppLogs. At the bottom right, there is a watermark for 'Site24x7'.

# AppLogs Monitoring and Third-party Integration Support

The screenshot displays the Site24x7 AppLogs monitoring interface. On the left, a sidebar lists various monitoring categories like Home, Alarms, View, APM, Server, VMware, Cloud, Network, AWS, RUM, Metrics, Log, Reports, Admin, and Edit. The main area shows a search bar for "AppLogs - Search" with the query "logtype='Windows Event Logs'". Below it is a chart titled "Log Events" showing a sharp spike from 16-Jan-22 16:52 to 17-Jan-22 15:22. To the right of the chart is a detailed view of an alert configuration for "Windows Alert". The alert is set to trigger on "logtype='Windows Event Logs'" with a "Count Based Alert" type, checked every 15 Minutes, and counting the attribute "count". It defines two conditions: one for "Trouble" (threshold > 1) and another for "Critical" (threshold >= 10). The "Configuration Profiles" section uses the "Default Notification". Under "Third-Party Integrations", the "Services" section includes "Slack Integration". At the bottom, a table lists 2003 log events from Jan 17, 16:40 to 17:51, with columns for Log Source, Time, DateTime, EventId, Type, Level, and Message. The message column shows entries such as "179.50.90.226 Jan 17, 16:40:56:369 Jan 17, 16:40:56:369 1001 Application Info", "179.50.90.226 Jan 17, 16:35:49:554 Jan 17, 16:35:49:554 1001 Application Info", and "179.50.90.226 Jan 17, 16:25:27:165 Jan 17, 16:25:27:165 1001 Application Info". A "Save" button is at the bottom right of the alert configuration.



# 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



## 2022 Q3 updates

- Support for multiple log patterns, derived fields, key-value, and XML logs in AppLogs
- Manage your vSphere clusters effectively with Site24x7
- Managing AppLogs from MSP portal



# 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



Crafted at ZOHO Corp.

## Seminar

# Beyond Monitoring: Leverage AIOps for observability

Tuesday, 15 Nov 2022  
Sydney, Australia

Thursday, 17 Nov 2022  
Melbourne, Australia





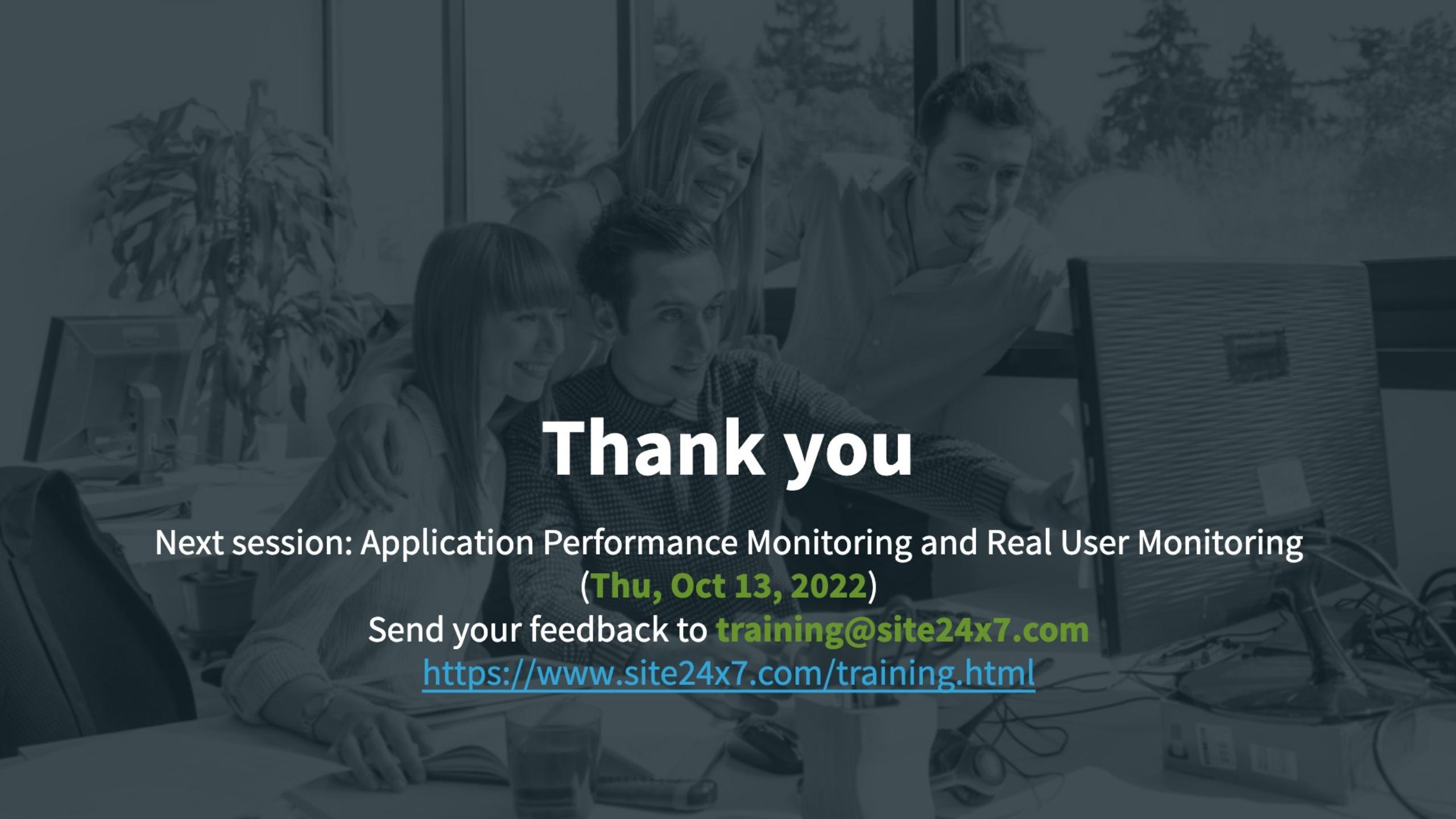
# Agenda

09:00 AM	 <b>Registration</b>  30 minutes
09:30 AM	 <b>★ Site24x7 observability platform: A shift from reactive to proactive monitoring</b>  45 minutes
10:15 AM	 <b>★ Digital experience management strategies for the modern enterprise</b>  45 minutes
11:00 AM	 <b>Break</b>  15 minutes
11:15 AM	 <b>★ Leverage AIOps for remote infrastructure monitoring in multi-cloud environments</b>  30 minutes
11:45 AM	 <b>★ Analyze, control, and track your spending on AWS and Azure cloud services</b>  15 minutes
12:00 PM	 <b>★ Certification</b>  30 minutes
12:30 PM	 <b>★ Lunch and Networking</b>  45 minutes



# Agenda / Registration Link

→ For Agenda and Registration : Click [this link](#)

A black and white photograph of four people in an office environment. Three women are in the foreground, leaning over a desk to look at a computer screen. A man is visible behind them. They are all smiling. The background shows office equipment and a window with trees outside.

# Thank you

Next session: Application Performance Monitoring and Real User Monitoring  
**(Thu, Oct 13, 2022)**

Send your feedback to **training@site24x7.com**  
<https://www.site24x7.com/training.html>