Site24x7 Certification

SCPA

Site24x7 Certified User • Site24x7 Certified User • Site24x7 Certified User • Site24x7 Certified User •

STUDY MATERIAL

Contents

- Real User Monitoring

- Security Monitoring

- Synthetic Transaction Monitoring

  - Web Applications

  - REST Applications

- Expiration Checks

  - SSL

  - Domain

CHAPTER 4

Infrastructure Monitoring

- Windows Server Monitoring

- Linux Server Monitoring

- Agentless server monitoring

- Cloud Services Monitoring

  - Amazon Web Services (AWS)

  - Microsoft Azure

  - Google Cloud Platform Monitoring (GCP)

- VMware Monitoring

- Nutanix Monitoring

- Kubernetes Monitoring

- Docker Monitoring

- Network Monitoring

About Site24x7

Site24x7 is an all-in-one, cloud-based monitoring tool for IT and DevOps teams that offers website, server, network, application performance, cloud, and real user monitoring from over 100 locations around the globe. With constant updates and new feature releases catering to customers' needs, Site24x7 offers a complete monitoring package with instant alerts, reports, and mobile app support.

Basic Overview: Monitors and the Homepage

Monitors are the basic units of monitoring in Site24x7, which give you the flexibility to test your IT resources. Classified as basic and advanced, monitors allow you to proactively examine the availability and various performance trends of your internet resources, servers, network resources, cloud resources, VMs, applications, and other endpoints.

The homepage that opens when you log in to Site24x7 lists all your monitors, with the option to navigate to different tabs. It offers a basic overview of your monitors and available alert credits.
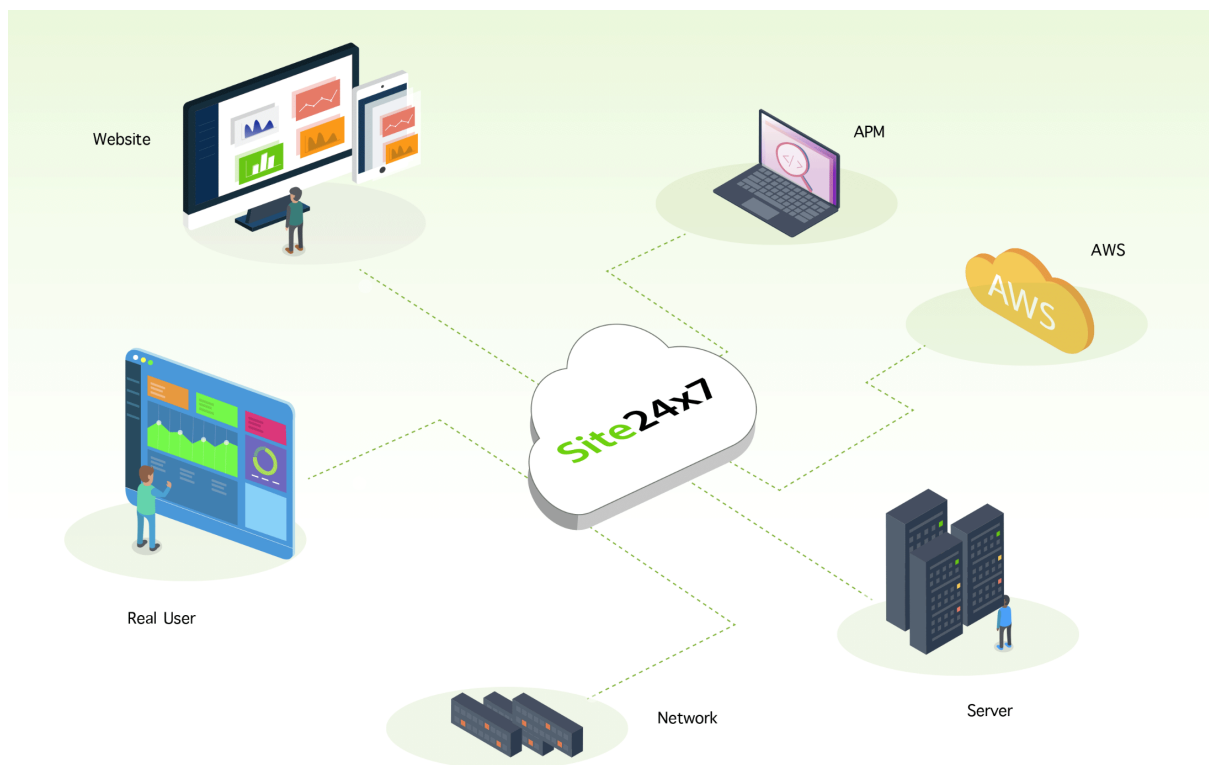
Figure 1: Site24x7 - overview

You can view details of monitors that require corrective actions directly from this page.Using the enhanced Search bar, you can search your resources in the Site24x7 web client, perform selected actions, and use quick, command-based, or query-based searches to filter resources or tabs.

Site24x7 offers a comprehensive set of APIs for remote operations. Site24x7 mandates users include their Zoho Auth Token in headers for successful API authentication

On-Premise Poller

On-Premise Poller is a lightweight agent that helps monitor your internal network and any resources behind your firewall. This allows you to keep track of the resources behind a virtual private network (VPN). On-Premise Poller monitors data center components and intranet applications like blogs, payroll applications, ERP systems, network devices, and database servers. This agent can be installed in various branch offices within a distributed organization and can be used to monitor the user experience. You can install On-Premise Poller on Windows and Linux machines (both 32-bit and 64-bit) as well as on virtual machines.
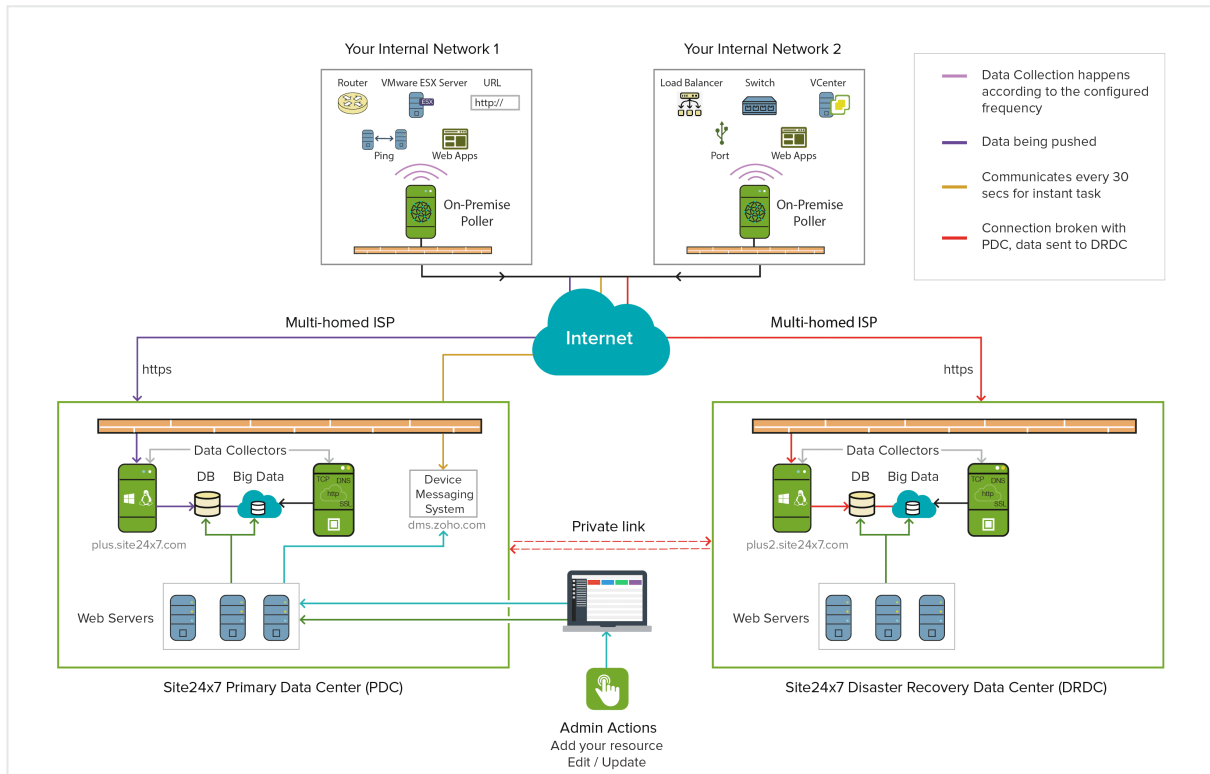
Figure 2: On-Premise Poller architecture

Monitoring Internet Services

— Uptime Monitoring

◆ Website

Site24x7 acts as a continuous URL monitoring service that keeps constant watch over a specified website and tracks the availability of the website at intervals spanning from once a minute to once a day. Its Website Monitor verifies the availability of addressable, standard HTTP and HTTPS URLs from over 110 global locations, as well as from behind your firewall using On-Premise Poller.

You can enable Site24x7 to resolve the website IP using the domain's authoritative name server instead of the default system resolver. Monitor your dual-stack endpoints from both IPv4 and IPv6-supported locations to identify possible connectivity issues. Check the uptime every 30 seconds and receive instant alerts if websites are down from any of the monitored locations using Site24x7 Website Monitoring. Uptime is usually depicted as a percentage in Site24x7.

◆ Web Page Speed (Browser)

Site24x7's advanced Web Page Speed (Browser) provides a split up of your website components like HTML, JavaScript, CSS, and images—as well as their corresponding load time, response time, status, component size, and more—using a waterfall model. It loads your webpage in a real browser to analyze all its resources and offers a PageSpeed Insights report. You can obtain information related to core web vitals like first contentful paint(FCP), largest contentful paint(LCP),

and cumulative layout shift(CLS). Additionally, Site24x7's browser agent will correctly identify and show you the HTTP protocol (version 1.1/2.0) that was used to render your resource. You can also configure resolutions according to the device and record transactions for tablets and mobile devices besides desktop devices.

You can build a block domains list to restrict monitoring of these domains. You can add domains at the Monitor level or Account level.

◆ **REST API**

The REST API Monitor regularly checks the availability of your REST API endpoints over IPv4 or IPv6-enabled locations and alerts you if the API response values fail to be validated by the specified RegEx/X-Path/JSONPath assertions. Additionally, you can test and validate your JSON response against the specified JSON schema. You can enable Site24x7 to resolve the endpoint IP using the domain's authoritative name server instead of the default system resolver. To import REST API endpoints in bulk, simply upload your predefined HAR/Swagger (JSON)/CSV file into Site24x7.

◆ **SOAP Web Services**

The SOAP Web Service Monitor regularly checks the availability and performance of your SOAP-based web services. It alerts you whenever the response (XML) does not bear the specified SOAP attribute name, or when the SOAP attribute value provided in response validation fails to be validated by its corresponding SOAP attribute name.

◆ **DNS**

The DNS Server Monitor regularly checks the availability of your

domain name servers and alerts you instantly when the DNS lookups are faulty, or when the socket connection time to the DNS Server exceeds the set limit. That way, you can ensure forward lookups are working and your domain names are resolving correctly. Site24x7 supports different DNS record lookup types, including A, AAAA, CNAME, NS, MX, SOA, PTR, and SRV. You can also check whether the resolved record name matches the configured search value.

◆ **NTP**

The Network Time Protocol (NTP) client typically uses three or more NTP servers to synchronize its clock. Using three or more servers enables you to detect an inaccurate server, also called a falseticker. Only servers deemed to be accurate by the client (called truechimers) are used for synchronization. You can provide an arbitrary drift threshold to detect a falseticker. Site24x7 lets you monitor the availability of the primary server alone and raise an alert if the secondary servers drift from the primary server.

◆ **Ping**

Site24x7's Ping Monitor detects the round-trip latency to any host. It measures the round-trip time for packets sent from the local host to the destination computer, including the local host's own interfaces. Three ICMP packets are sent per poll; if at least one packet is received, this monitor will be considered UP. However, if no packs are received, the monitor will be considered DOWN.

◆ **TCP Port**

Check the connectivity of any TCP ports from over 100 global locations. You can also validate the response of text-based protocols. Recieve

alerts in case of downtime or if there is a content mismatch in the response.

◆ **Mail Server**

Site24x7's Mail Delivery Monitor checks your inbound and outbound mail servers by verifying delivery to both internal and external mail-boxes. It lets you know more about the mail-user experience by test-ing every aspect of the email delivery process and capturing the emailround-trip time from over 110 global locations, as well as from behind a firewall using On-Premise Poller.

The Mail Delivery Monitor sends emails to a designated SMTP server (similar to an email client), retrieves the emails using IMAP and POP3 protocols, and measures the round-trip time. For validating the email round-trip time, you can either use your own server configurations or Site24x7's SMTP and POP3/IMAP server configurations.

◆ **WebSocket**

WebSocket helps establish a two-way, open communication between a web browser and a server. WebSocket creates an uninterrupted connection between two devices and updates the content without having to wait for a request from the user thereby providing low laten-cy communication, along with delivering a dynamic and real-time web experience. Site24x7 monitors your WebSocket endpoints to identify service interruptions and sends notification about service disruption and unusual spikes in response times helping you take quick correc-tive actions.

◆ **UDP Monitoring**

With UDP monitoring you can track the availability of your User Datagram Protocol (UDP) ports from different locations. UDP is a connection-less protocol, effective in time-sensitive applications like real-time systems. With the help of a Site24x7 UDP monitor, you can get alerted about any downtime or when there is a content mismatch in the response. With the Basic Monitor available in the Starter pack, you can also monitor your dual stack infrastructure.

◆ **False Alert Protection**

Site24x7 has taken a few measures to mitigate false downtime alerts:

• **Rechecks from alternate locations:** Outages are only reported after downtime is verified from alternate locations.

• **Advanced threshold settings:** You can use the Strategy option in Threshold Settings for individual attributes of your monitor. Once an attribute value fails to conform to the specified condition set by the user, a TROUBLE alert is instantly triggered. Some of the monitoring strategies that can be applied to the attributes include poll count, poll average, time duration, and average time.

• **Browser-based check:** After the rechecks are completed, Site24x7 does a final check on the status of your website via a web browser screenshot. If the website is found available in this browser-based check, it will be considered UP and no alert notification will be sent.

• **Network sanity check:** A network sanity check is done to make sure that Site24x7's network in the monitoring location is working.

◆ **ISP Latency Monitoring**

Obtain the availability and latency between multiple On-Premise Pollers in your account with an intuitive latency dashboard. Monitoring ISP latency is critical for network admins to:

- Identify the best and shortest network path based on reachability and latency.
- Visualize the data transfer using traceroute.
- Pinpoint connectivity loss and faulty interfaces.
- Troubleshoot network issues.
- Check if ISPs are abiding by their SLA.

▬ Performance Monitoring

◆ **Website**

Gain visibility into your website response time, including DNS time, connection time, first byte time, download time, and SSL handshake time. Analyze how your website responds when accessed from various global locations and take swift corrective actions in case of downtime. Gather in-depth information from the Poll Now Report on SSL/TLS protocol version and cipher suite details like key exchange, bulk encryption, and hash function.

During a DOWN/TROUBLE outage, you'll receive an in-depth root cause analysis (RCA) report after the monitor reports an outage lasting 150 seconds or longer. The RCA report offers basic details about your monitor, outage, and recheck; it includes the following details:

- Checks from the primary location and re-checks from the secondary location
- Ping analysis
- DNS analysis
- TCP traceroute
- MTR report
- MTR-based network route
- Conclusion

◆ **DNS**

The DNS Server Monitor tracks the response time of your DNS server and the average response time from every monitoring location. These critical parameters are captured and listed in the details page:

- *Response time*, which outlines the domain resolution time of the DNS server in milliseconds and the average response time from every monitoring location.
- *Availability and response time* by location provides the availability of the DNS server and DNS resolution time in milliseconds.
- *DNS security: Domain Name System Security Extensions (DNSSEC)* technology is used to protect your domain against external hijacks by digitally signing data so you'll know it's valid. After enabling the DNSEC validation, Site24x7 authenticates the DNS responses and validates the security.

▬ Real User Monitoring

Real User Monitoring (RUM) gives you visibility into the

behind-the-scene performance of your web application, along with accurate insight into the end-user experience. RUM visualizes application interaction patterns to give you an in-depth understanding of the problems affecting users accessing websites and applications in real time. You also get to analyze application performance from every aspect like browser, platform, geography, and ISP.

In short, RUM provides key insights into key performance metrics, right from the initiation of the URL till the request is served back to the browser, enabling developers to tailor their applications to optimize for end-user experience.With the help of RUM, you can also monitor the performance of applications (Single Page Applications) built on SPA framework and optimize them for better customer experience.
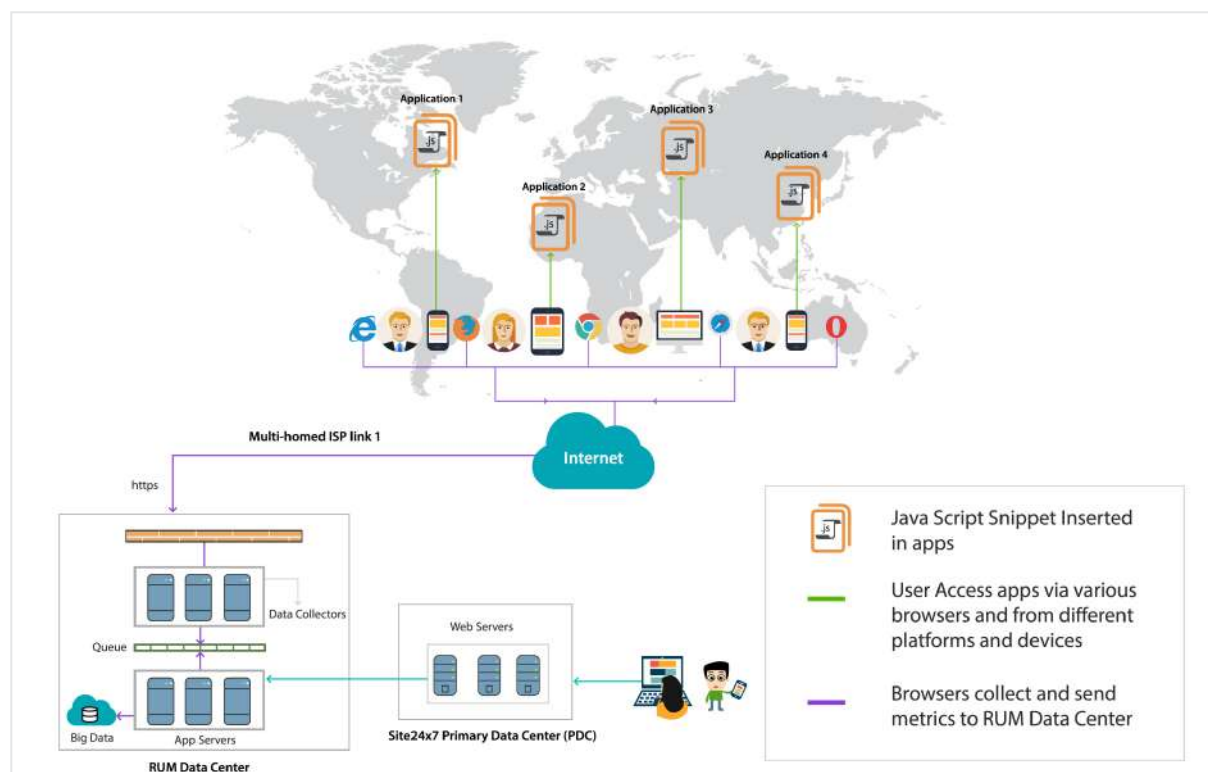

Figure 3: RUM - architecture

Security Monitoring

◆ Real-time Blocklist (RBL) Check

Getting blocklisted can affect your brand and your relationship with your customers. Real-time Blocklist monitoring checks and confirms whether your hostname or IP addresses are blocklisted against popular DNS-based blocklists in real-time. It thereby helps you to ensure confidence in your customers that they can contact you safely, through email, your website, and social media without risking their security.

◆ Brand Reputation

Brand Reputation Monitor checks your website against Web Risk list and notifies if your website is affected. Since any website containing malware or suspicious for phishing activity is seen as a threat to the online community and is often penalized by search engines, any insight from this monitoring will ensure that your site is free of any such malicious code and retains your brand's reputation intact. The monitor allows you to add unlimited URLs for Brand Reputation check. The default check frequency is set as one hour.

◆ Website Defacement Monitoring

Website defacement refers to an attack on your website that alters your website's visual appearance with potentially hazardous content, graphics, and malicious code insertions. With Site24x7's Website Defacement Monitoring, you can periodically monitor the integrity of your webpage and check for modifications to content and critical elements, such as image files, scripts, anchors, links, and iframes.

If a mismatch is detected during a poll, Site24x7 immediately notifies you with an alert, so the problem can be addressed before your customers are at risk. You can also monitor any unintentional or unauthorized changes to company websites by company employees. You can only monitor your websites for defacement from your configured primary monitoring location.

.Synthetic Transaction Monitoring

◆ **Web Applications**
Web application user flows can be easily monitored using Site24x7's synthetic transaction monitors: Web Transaction Monitor and Web Transaction (Browser) Monitor.

The *Web Transaction Monitor* uses a downloadable transaction tool to record all user steps in your web application in their exact sequence. These transactions then get replayed at regular intervals of time, and notifications are sent when any error is detected. Site24x7 also simulates these actions continuously, scanning for signs of trouble.

The *Web Transaction (Browser) Monitor* allows you to track the availability and performance of your web transactions using an actual web browser like Firefox or Chrome. Site24x7's robust recorder tool records web transactions and plays them back through a real browser from 100 global monitoring locations or from a private location (using the On-Premise Poller for Linux). You can import Selenium-based test cases into the recorder tool to set up new monitors. You can configure resolutions according to the device and record transactions for

tablets and mobile devices besides desktop devices.

By creating a block domains list for your web application, you can restrict monitoring of these domains. The block domains list can be created at the Monitor level or Account level.

◆ **REST Applications**
Site24x7's REST API Transaction Monitor can monitor workflows in REST applications. You can create a monitor directly from the Site24x7 web client without requiring any recorder. Once the monitor is set up, each transaction step will either be an HTML request or a REST API call. Site24x7 performs synthetic monitoring of web application workflows without the overhead of running a real browser.

You can monitor a sequence of 25 endpoint URLs and even allow parameter forwarding in your step sequence. Parameter forwarding lets you capture the transaction to fetch the token/parameter from the service and pass it to any successive steps of the same monitor to successfully validate the endpoint.

— **Expiration Checks**

◆ **SSL/TLS**
SSL/TLS certificates encrypt the data transferred to and from the website of the certificate holder. Site24x7's SSL/TLS Certificate Monitor performs multiple checks like secure socket layer certificate validity (to notify you about the expiration of your domain's SSL/TLS certificate in advance), OCSP checks (to inform you about any revoked certificates), and blacklisted checks

(to inform you about any revoked certificates), and blacklisted checks (to notify you about any potential blacklisted certifying authority). Additionally, you can also set up a SHA-1 fingerprint threshold to detect any potential certificate tampering. This way, you can provide a safe environment for your website visitors while also enhancing the credibility of your website.

◆ **Domain**

The Domain Expiry Monitor lets you monitor your domain name and notifies you at a preset time period prior to the domain's expiration so you can easily renew and maintain ownership of your domain address. You can also configure the expiration notification threshold to meet your specific needs.

Infrastructure Monitoring

— Windows Server Monitoring

Monitor your Windows servers and measure more than 50 critical performance metrics including CPU, memory, disk utilization, thread and handle count of services and processes, and bandwidth utilization—all from a unified dashboard.

The Windows monitoring agent needs to be installed in the respective servers to start monitoring. The agent is a native C/C++ executable file, run as either a Site24x7 Windows Agent service or a MonitoringAgent.exe process.

Features:

- Choose one-minute or five-minute polling.
- Bulk install the agent using Active Directory, remote commands, PowerShell DSC, and more.
- Start and stop services or processes on the go using your mobile device.
- Auto-discover and start monitoring Microsoft applications, including SQL, IIS, Exchange, Hyper-V, Active Directory, Windows Backup, Windows Updates and Failover Cluster. This option can also be disabled.
- Choose from more than 100 ready-to-use plugin integrations, along with custom script monitoring using VB, Python, PowerShell, Batch, and DLL.

- Monitor internal resources including event logs, files, directories.
- Set alerts for individual attributes like services or processes; disks; or the entire server.
- Diagnose connectivity issues using a detailed root cause analysis report.
- Explore and gain an in-depth understanding with the help of insightful Inventory reports.

Linux Server Monitoring

Monitor your Linux servers and measure more than 50 critical performance metrics including CPU steal time, idle time, user space time, interrupts time, nice time, wait time, and system time—all from a unified dashboard.

The Linux Server Monitoring agent is written in Python and has two components: the Site24x7Agent and the Site24x7AgentWatchdog that run as two separate processes. Both root users and non-root users can install the Linux agent.

Features:
- Choose one-minute or five-minute polling.
- Bulk-install the agent using Chef, Puppet, SaltStack, Ansible, and more.
- Start and stop services or processes on the go using your mobile device.
- Auto-discover and monitor Docker containers. This option can be disabled.
- Choose from more than 50 ready-to-use plugin integrations including MySQL, NGINX, or build your own plugin using Python and Shell scripts.
- Monitor internal resources including syslogs, files, directories.

- Set alerts for individual attributes like services or processes; disks; or the entire server.
- Explore and get a deep understanding of your server environment with the help of insightful Inventory reports.
- Diagnose connectivity issues using a detailed root cause analysis

▬ Agentless Server Monitoring

Monitor your servers agentless using Site24x7 On-Premise Poller. Simply configure SNMP on your Windows, Linux, macOS, Oracle Solaris, Dell iDRAC, IBM AIX, HP iLO, HP UX, or other servers, to get started. You can monitor a single server or all the servers in a given IP range for important metrics like response time, packet loss, services, processes, and disk related metrics using performance counters and tabular performance counters. You can also configure to receive instant downtime alerts by configuring threshold profiles.

▬ Cloud Services Monitoring

Site24x7 supports monitoring for the following cloud platforms:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

◆ Amazon Web Services Monitoring
Data Collection: Site24x7 collects resource usage metrics and metadata for supported AWS services by accessing various AWS service APIs, like CloudWatch, at regular intervals.

Supported Services:

• Amazon Elastic Compute Cloud (EC2)

• Amazon Relational Database Service (RDS)

• Amazon Simple Storage Service (S3)

• Amazon Simple Notification Service (SNS)

• Amazon Simple Queue Service (SQS)

• Amazon Kinesis

• Amazon ElasticCache

• AWS DynamoDB

• AWS Elastic Load Balancing (ELB)

• Amazon Elastic Beanstalk

• Amazon Elastic Block Storage (EBS)

• Amazon CloudFront

• Amazon Elastic Container Service (ECS)

• Amazon Redshift

• Amazon Elastic File Storage (EFS)

• Amazon Simple Email Service (SES)

• Web Application Firewall (WAF)

• CloudSearch

• Certificate Manager

• Elastic Kubernetes Service (EKS)

• Amazon MQ

• Storage Gateway

• Transit Gateway

• Database Migration Service (DMS)

• Direct Connect

• VPC-VPN connection

• API Gateway

• Step Functions

• Key Management Service (KMS)

- Route 53
- Elasticsearch
- NAT Gateway
- Elastic MapReduce
- WorkSpaces
- Neptune
- Lightsail
- Amazon GuardDuty
- Amazon FSx
- Lambda@Edge
- DocumentDB
- Gateway Load Balancer
- Amazon Inspector
- SFTP
- Systems Manager

Features:

- Uptime monitoring for AWS resources
- Inventory reports
- Inbuilt AWS best practices through the Guidance report
- Instance type recommendations that work on top of the Guidance report
- AI-powered anomaly reporting with dashboard
- Custom dashboards and reporting
- Metric profile to choose specific CloudWatch metrics to monitor
- Schedule automations across AWS resources for manual tasks
- NOC dashboard
- AWS log analytics for a reduced MTTR
- Infrastructure dashboard

• Business view to organize and simply administration of AWS resources

• Service Quotas feature to view and manage quotas directly from the Site24x7 web client

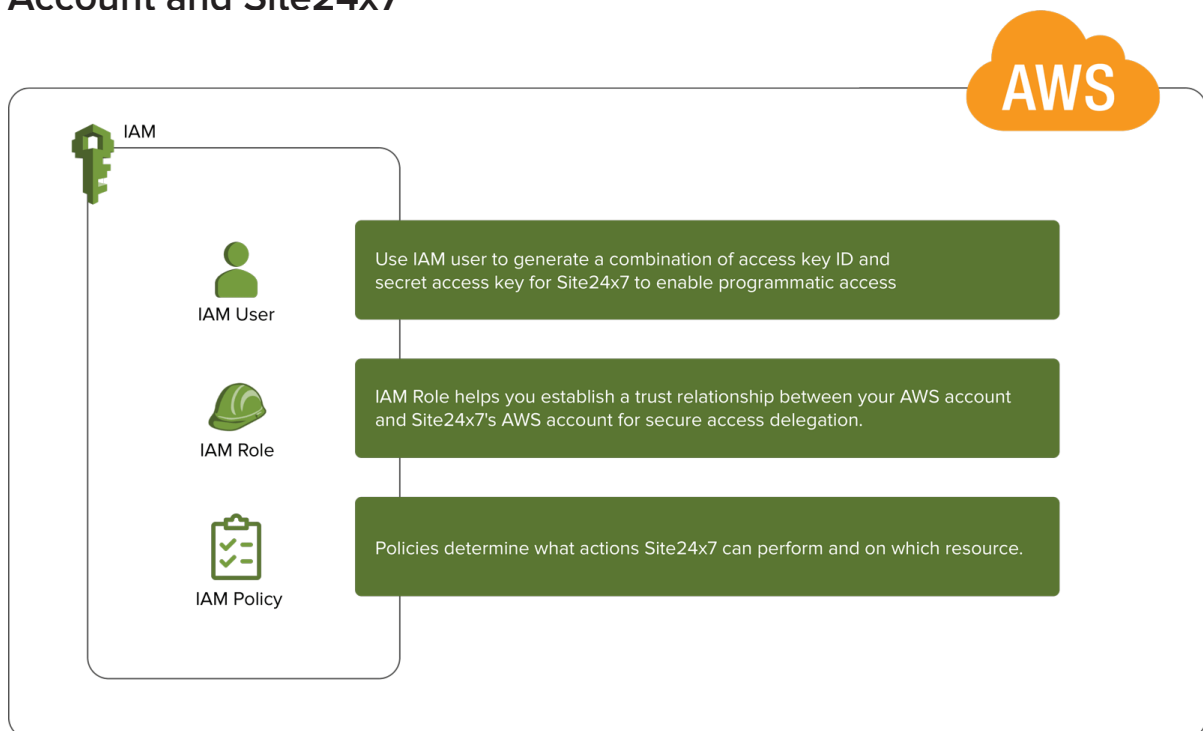## Essential Concepts for Successful Integration Between Your AWS Account and Site24x7

IAM

IAM User

Use IAM user to generate a combination of access key ID and secret access key for Site24x7 to enable programmatic access

IAM Role

IAM Role helps you establish a trust relationship between your AWS account and Site24x7's AWS account for secure access delegation.

IAM Policy

Policies determine what actions Site24x7 can perform and on which resource.

Figure 4: Essential concepts for AWS integration

Region

The AWS infrastructure is hosted in multiple locations worldwide. These locations are composed of Regions and Availability Zones (AZs), where each Region is a separate geographic area. With Site24x7, you can collect metrics on usage and performance for resources deployed in the following Regions:

• AWS Standard Regions
• AWS GovCloud Region
• AWS China Region

AWS IAM Entity

An IAM entity is an AWS identity that you create to represent people or third parties who want to access your account. There are different types of entities: IAM users, groups, and roles. An AWS account holder can delegate access to Site24x7 either by creating an IAM user or role.

AWS IAM Policies

Policies determine what actions an IAM user or role can or cannot do in AWS. We recommend using the AWS managed policy (ReadOnly-Access) to grant permission to Site24x7.

IAM Users

An IAM user is an AWS identity with attached policies that authorize AWS operations.

When you add Site24x7 as a new IAM user, choose "Programmatic access" as the Access type. This enables an Access Key ID and Secret Access Key which can be used to make programmatic requests to the AWS service APIs.

IAM Roles

An IAM role is similar to an IAM user in that it's an AWS identity with attached policies. However, instead of being assigned to a single person, an IAM role can be assumed by anyone who needs it. Using IAM roles, there's no sharing of long-term security credentials like an Access Key ID and Secret Access Key.

In Site24x7's case, the AWS account holder creates a cross-account

IAM role between their account and Site24x7's AWS account. When Site24x7 assumes the role, it's assigned temporary security credentials. Another important aspect of IAM roles is the concept of an External ID, which is an alphanumeric key provided in the Site24x7 console. This additional piece of information ensures that no one other than Site24x7 can assume its IAM role.

◆ **Microsoft Azure Monitoring**

Microsoft Azure Monitoring monitors over 80+ Azure Service types in near real time. Auto-discover, monitor and analyze the performance of your entire Azure environment.

Site24x7 collects performance metrics and metadata for supported Azure service types by using Microsoft APIs. Set up alerts, associate tags with resources, automate actions and analyze trends in customizable dashboards. Site24x7's agent extensions offer performance metrics like CPU, memory, disk usage, and database calls, along with more than 50 other metrics for Windows, Linux, and .NET platforms

List of Azure Services Monitored by Site24x7

Site24x7 monitors 80+ Azure services including Virtual Machines, Scale Sets, Storage Accounts, Cosmos DB, and more.

Categories	Services	
Compute	• Virtual Machines • Disks • Kubernetes Services • Virtual Machine Scale Sets • Virtual Machines (Classic)	• Fabric Clusters • Batch Accounts • App Services • App Service Plans

Categories	Services	
Web	• Functions • Continuous WebJobs • Triggered WebJobs • API Management Services • App Services • App Service Plans	• CDN Profiles • Deployment Slots • SignalR • Notification Hubs • Media Services
Networking	• Network Interfaces • DNS Zones • Firewalls • Network Watcher Connections • Load Balancers • Public IP Address • Application Gateways	• Virtual Network Gateways • VPN Gateways • CDN Profiles • Virtual Networks • Network Connections • Traffic Manager Profiles • Express Route Circuits
Databases	• SQL Servers • PostgreSQL Servers • Document DB • Database for MySQL Servers • SQL Database • Cosmos DB	• SQL Elastic Pools • Database for Maria DB Servers • Redis • Data Factories (V2) • SQL Managed Instances

Categories	Services	
Storage	• Storage Accounts • Storage Accounts (Classic) • Recovery Services Vaults • Blob Storage • Table Storage	• Data Lake • Queue Storage • File Share • Storage Sync Services
Containers	• Kubernetes Services • Container Instances • Fabric Clusters	• Batch Accounts • Container Registries
Analytics	• Log Analytics Workspaces • Data Factories (V2) • Power BI Embedded • HDInsight Clusters • Data Factory Pipelines	• Analysis Services • Event Hubs • Data Lake Analytics • Stream Analytics Jobs
Integration	• Service Bus • Relays • API Management Services • Service Bus Queues	• Event Grid Topics • Service Bus Topics • Logic Apps
AI+Machine Learning	• Search Services • Machine Learning	• Cognitive Services

Categories	Services	
Internet of Things	• Stream Analytics Jobs • Device Provisioning Services • Logic Apps	• Maps Accounts • Graph • IoT Hubs
Management + Governance	• Automation Accounts	
DevOps	• Application Insights	
Security	• Key Vaults	
Other	• Autoscale Settings • Host Pools	

Features:

• Auto-identify and stop problematic resources using instant alert responses and IT Automation tools.

• Check on the availability of your entire Azure stack, Azure resource usage, and the performance of Azure resources using exclusive dashboards.

• Perform bulk actions on virtual machines and install the server monitoring agent for in-depth monitoring of your VMs.

- Remove Azure terminated resources from Site24x7 monitoring using Resource Termination Settings, which will help you in managing cost.
- Filter resources based on subscription, resource group, service, and location for better visibility in the Infrastructure/Inventory/ Management dashboard.
- See which resources are dependent on one another. Keep a record of the dependant resources to figure out the reason behind the downtime of parent resources.
- Detect unusual monitoring patterns and outliers using the Business View under Monitor Groups.
- Get best practice recommendations to optimize costs, increase the performance and reliability of your Azure services using Guidance report.
- Modify configuration profiles, perform monitor-level actions like delete/suspend, import changes, and apply them across Azure subscriptions, resource groups, and locations in one go.
- Monitor the health of your services to detect any service health issues and ensure reliable deployments and high availability of your services using Azure Deployment Manager (ADM) Health Check.
- View all the logs from your Azure account in one console from Site24x7 Activity Logs.
- Create your own app in the Microsoft Azure portal and assign the necessary permissions.

◆ **Google Cloud Platform Monitoring**

Auto-discover and monitor all your Google cloud services, identify performance bottlenecks, and address issues instantly.

Prerequisites:

• Ensure the role Viewer is provided to the service account associated with the project.

• To start/stop VMs under Management Actions, ensure Compute Admin role is provided.

• Upload a valid Service Account JSON File to authenticate Site24x7 for performing resource discovery.

Features:

• Auto-discover and monitor Google Compute Engine (GCE), Google App Engine (GAE), Google Kubernetes Engine, VPC, Cloud IAM, Cloud Audit Logging, Cloud SQL, BigQuery, and more.

• Get a NOC view of all the GCP resources discovered from your account using the Infrastructure Dashboard.

• View the daily usage of critical GCP resources for a set of service types in the Inventory Dashboard.

• Start/stop VMs, delete your resources, and filter resources based on service types, location, and monitor status for better visibility.

• Track events that affect your project, monitor operation logs, system logs, activity logs etc. and know all the actions performed in the GCP console.

─ VMware Monitoring

Automatically discover and map your entire vSphere environment, from data centers to virtual machines (VMs), in real time; just install On-Premise Poller in the network where your virtual infrastructure is located to get started. Monitor your virtual resources for their availability and the different performance metrics listed below.

- vCenters: Clusters, datacenters, and other virtual components.
- VMware ESX/ESXi hosts: CPU, memory, hardware sensors, network utilization, disk utilization, and other host details.
- VMware VMs: CPU, memory, network utilization, disk utilization, and other VM details.
- VMware datastores: Space split-up (snapshots, disk files, free space, swap memory), log file size, LUN information, and other VM metrics.
- VMware resource pools: Monitor VMs that are powered on or off, CPU and memory reservations and limits, and child resource pool metrics to avoid resource contention in CPU and RAM.
- VMware ESXi Hardware Monitoring: Monitor the hardware sensors.
- AI-powered insights for datastore and VM space metrics.

You can also monitor VMware Horizons with Site24x7's VMware VDI monitoring. This includes monitoring the associated resources, tracking the connections established over different sessions, and alerting admins based on the thresholds configured for various metrics.

Nutanix Monitoring

Monitor your Nutanix infrastructure thoroughly for the health and performance of all the resources and processes in every cluster, host, and VM. Analyze the Nutanix Acropolis hypervisor, controller VM, storage controllers, and containers using different metrics. Automatically discover the hosts and VMs associated with your cluster, and monitor the infrastructure at every node.

Features:

Nutanix Cluster: Keep track of the performance of every disk, content cache, and storage controller in your Nutanix cluster. Managing your clusters is simple with stats and graphs on data transfer rates, latencies, I/O operations, and deduplication.

Nutanix Host: Monitor the bandwidth, latency, and I/O operations for every disk, hypervisor, and storage controller in your Nutanix host. Also, analyze the logical and physical memory used and saved in the content cache.

Nutanix VM: Achieve a deep understanding of your Nutanix VMs by monitoring every VM at the child level. Monitor storage containers, virtual disks, and virtual network interface controllers (NICs), along with controller I/O operations, bandwidth, and latency.

Kubernetes Monitoring

Get a comprehensive view of the health and performance of your Kubernetes clusters by monitoring the various components of your Kubernetes infrastructure.

Features:

• Set up custom alerts based on the state of essential Kubernetes components like kube-apiserver,kube-scheduler, kube-controller-manager, and etcd.

• Track service latency and throughput to ensure that the apps running in your Kubernetes environment are performing at their best.

• Keep track of all terminated pods in a worker node and how much more load can be distributed per node.

• Receive notifications before the application goes down so you may respond ahead of time before end users are impacted.

Docker Monitoring

Monitor a Docker container either by auto-discovering it as an application once the Linux agent is installed, or by installing it as a separate agent to monitor the underlying hosts.

Features:
• Get the Docker agent from Docker Hub or from the Site24x7 web client.
• Bulk-install the Docker agent using AWS ECS or Kubernetes.
• Track dynamic, rapidly scaling containers with container CPU usage, memory, size, output, uptime, overall status, and other performance metrics.

Network Monitoring

Monitor your entire network to ensure the health and performance of your network devices and interfaces. Automatically discover your SNMP devices, and continuously monitor critical metrics such as CPU, memory utilization, buffer hit stats, bandwidth utilization, response time, and packet loss. Licensing is based on the number of interfaces that are monitored by Site24x7.

Supported devices:
Routers, switches, firewalls, load balancers, printers, wireless devices,

WAN accelerators, UPSs, storage devices, and anything with SNMP support.

Features:

• Support for 450 vendors and 10,000 device templates. With custom

• SNMP monitoring, monitor any device with SNMP support.

• Support for devices with more than one credential.

• One-minute status polls.

• Complete visibility into network traffic and bandwidth performance.

• Site24x7 supports different flow technologies like NetFlow, JFlow, sFlow, IPFIX, NetStream, and AppFlow along with support for different vendors in the market.

• Performance counters for monitoring SNMP OIDs and custom SNMP OIDs. Tabular performance counters for monitoring tabular OIDs.

• Upload custom MIBs from your system and use them to add custom performance counters, giving you the flexibility to add performance metrics of your choice.

• Automatic layer 2 discovery and mapping.

• SNMP trap processing.

• NOC view, network health dashboard, and topology maps for visual aids.

• Ping and traceroute options to test the reachability of a network device.

• Visualize the topology and interconnection of your stack switch using the stack data ring. Track the health of the switches in your stack by monitoring their hardware sensors.

• VPN monitoring.

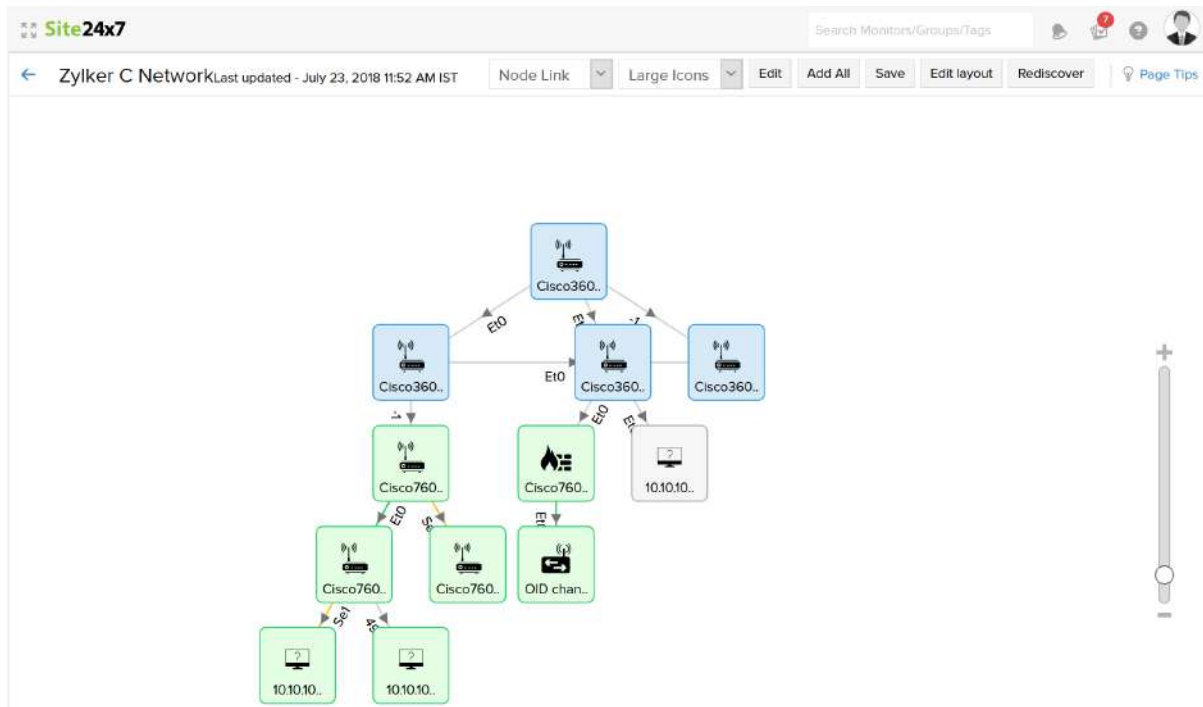• Assess the quality of VoIP call services through out the call path using Cisco IPSLA-based VoIP monitoring.

Figure 5: Layer 2 Network Map

Cron Monitoring

Monitor cron jobs, micro-services, backups, daemons, and any other scheduled tasks with a simple no-coding setup. Troubleshoot cron failures quickly and get alerts before a cron failure impacts your system.

Features:

• Add a cron job for monitoring in minutes. Just give it a name, specify the cron expression, and select who to notify.

• Gain better visibility into your jobs by viewing their availability and performance over time.

• Use cron expressions for greater flexibility in defining cron jobs, and define fixed time schedules.

• Use either Crontab, Bash, Python, PowerShell, or Ruby to push data to Site24x7 from your endpoints.

- Receive alerts when jobs, workers, or services run longer than expected. Use unique ping URLs to send alerts for a particular time period.

▬ Heartbeat Monitoring

Monitor to know if your scripts, agents, workers, daemons are able to communicate as expected. With a simple HTTP request to the {display name} endpoint of the URL, you will know if your task is able to communicate with your server or not. You can also set up thresholds and be alerted when your servers don't ping back. Use either Bash, Python, PowerShell, or Ruby to push data to Site24x7 from your endpoints.

Application Performance Monitoring

Site24x7 APM Insight gives DevOps teams complete visibility into application server performance, along with various components of a web application. This tool is perfect for IT operations, developers, and application teams looking to collaborate and ensure high application uptime; it provides end-to-end insight into the performance of individ-ual web transactions and highlights issues no matter where they origi-nate.
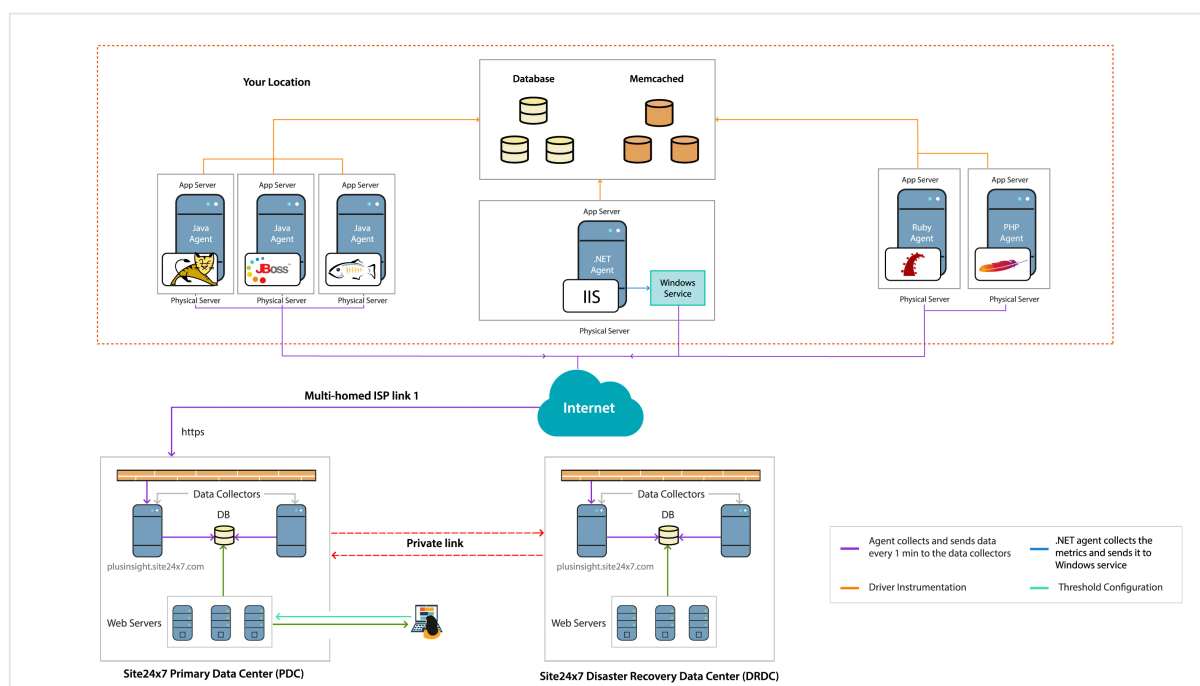

Figure 6: APM architecture

Key features:

• Gives you the complete picture of how your application connects and communicates with external components.

• Allows you to track and measure important metrics including apdex score, appserver throughput, response time, exceptions and more.

• Easily identifies slow queries and eliminates potential bottlenecks.

• Monitors background transactions and captures exceptions at their point of occurrence.

• Offers a comprehensive view of database operations including database calls and database usage.

• Tracks custom application components. .

Supported platforms:

APM Insight supports applications built on Java, Ruby, .NET, PHP, and Node.js.

Requirements:

• The APM Insight Java agent is supported on application servers running Java 1.5 or above.

• .Net applications in Microsoft .Net Framework version 4.0 as well as IIS 7.0 and above.

• Ruby applications 1.8.7 and higher, and Ruby on Rails 3.0 and higher.

• The PHP agent is supported on Apache2 Web Server with Linux operating system running PHP version 5.3 and above.

  • Support is provided from Node.js version 4 and above.

Java Application Monitoring

Get in-depth analysis on your Java EE web transactions with performance metrics for all components. You can easily identify slow internal invocations (methods) in the Java code and view the entire web request pathway in a tree view. Monitor key JVM metrics like JVM CPU usage, runtime memory, GC count, GC time, and thread summary.

.NET Application Monitoring

The APM Insight .NET agent can monitor slow methods in your .NET code, track database calls and background transactions, and monitor user-defined methods. You can also monitor your .NET framework desktop applications along with Windows service performance. You can monitor and track a wide variety of components in your AWS and Azure environments, too.

Site24x7 also gives you an overall view of IIS servers, and the applications and IIS pools accessing those servers.

Ruby Application Monitoring

Deploying the Site24x7 APM Insight Ruby agent on a Rails platform gives you end-to-end awareness of performance issues in web transactions. To monitor Ruby application performance with Site24x7, you need to deploy a monitoring agent (a Ruby gem) in your application server. The agent collects application performance metrics and sends them to the central Site24x7 server at fixed intervals, e.g. every 60 seconds.

— PHP Application Monitoring

The APM Insight PHP agent can monitor your PHP applications deployed in both Windows and Linux platforms. You can monitor slow queries and easily identify the needle in the haystack.

— Node.js Application Monitoring

The APM Insight Node.js agent allows you to track all events and I/O operations in your Node applications. You can monitor the performance of asynchronous calls, analyze the time taken, and track triggered events and their sequences.

— Application Monitoring using One Agent

The APM insight One agent allows you to monitor and optimize the performance of your applications on Windows platforms (.NET, .NET Core, Java, and PHP). The agent automatically collects the performance metrics of the application and sends it to the central Site24x7 server at fixed intervals i.e., every 60 seconds.

— Distributed Tracing:

As applications become more complex, finding out errors and their root cause becomes difficult, especially with microservices and distributed architectures which has a myriad connections between the varied components. This is where distributed tracing comes handy.

Distributed tracing lets you map the exact path of a transaction across varied components, built in different platforms. This helps you find the origin of a transaction, the exact pain points and makes debugging easier.

Site24x7 APM Insight supports distributed tracing in Java, .NET and Node.js applications.

Server Integration

Site24x7 Server Integration feature helps you to get a complete picture of your application's performance along with the metrics of the connected servers. The server monitor and the APM instance monitor integration happens automatically in the Site24x7 console, if they have the same hostname.

Mobile APM

Site24x7 Mobile APM for iOS lets you track the performance of your native mobile applications on actual end-user devices. For example, a news reader application may perform the following operations internally:

- Navigate to a table view to show a list of articles.
- Load the list of articles using a REST API call.
- Cache the list of articles in an SQLite database.
- Download a thumbnail for each article.
- Cache the thumbnails to the filesystem.
- Build a complex UI, such as a custom table view cell style.

All of the above are potentially long-running operations that impact the user experience, so it's important to benchmark and optimize them across various devices. Site24x7 Mobile APM gathers and aggregates metrics from all your users across the globe by embedding an APM agent in your applications in the form of a library.

The APM agent measures the execution time of your code using transactions and components. In the previous example, the entire sequence of operations, from starting navigation to rendering the final UI, can be considered a transaction. Individual operations can be grouped into different component types such as HTTP, SQLite, filesystem, and UI. Simple operations can be measured using transactions, while complex operations can be measured using transactions with components.

Site24x7 Mobile APM is supported on both Android and iOS devices.

End-user Experience Monitoring

Enhance the end-user experience by integrating APM Insight and Site24x7's Real User Monitoring. With this integration, you get a holistic view of an application's performance from a single console. All critical metrics—such as application performance from the moment users access the application, the time taken in the back end to process the request, network latency, and the time consumed in rendering the response—are captured and displayed in a single console; Site24x7 can also track soft navigations. Additionally, both the browser and server times are integrated, allowing you to analyze all metrics together, which helps in fine-tuning app performance.

Microsoft Application Performance Monitoring

▬ Microsoft SQL Monitoring

Monitor SQL server status, database attributes, and SQL operations, and receive alerts about database performance spikes. SQL servers will be automatically discovered and added for monitoring once the Windows monitoring agent is installed. SQL Server Monitoring gives you a deep understanding of various memory and buffer manager details for optimal capacity planning. Drill down to performance details such as SQL compilations, longest transaction time of SQL instances, and database attributes.

Whether it's a stand-alone SQL server or a SQL cluster, the Windows agent will auto-discover and take it up as a single monitor license. You can get a single view for your SQL server cluster instead of having separate SQL monitors for active and passive nodes. Set instant alerts that notify you about any failover between the active and passive nodes. You can also view a detailed log report on all the failovers of your cluster.

▬ Microsoft IIS Monitoring

Monitor and analyze the resource usage of sites, apps, and application pools to avoid server problems. IIS servers are automatically discovered and added for monitoring once the Windows monitoring agent is installed.

Automate the start/stop of an application or site using IT automation. With IIS Monitoring, you can identify the top worker processes causing resource contentment issues, and monitor session details along with cached, queued, and failed requests to avoid application overload. You can also view detailed metrics such as CLR data and thread data connected to .NET.

▬ Microsoft Exchange Monitoring

Exchange Monitoring offers key stats like RPC request/response time for client access, unified messaging and hub transport, communication with hub transport store details, and database details to identify potential issues as well as their root cause. You can also monitor the various Exchange roles configured in your servers. Exchange servers are automatically discovered and added for monitoring once the Windows monitoring agent is installed. Site24x7 supports Exchange Server versions 2007, 2010, 2013, and 2016.

▬ Microsoft SharePoint Monitoring

Keep an eye on SharePoint's server metrics, services, queued requests, and overall health—all in one console. The SharePoint servers will be automatically discovered and added for monitoring once the Windows monitoring agent is installed. Site24x7 supports SharePoint Server versions 2007, 2010, 2013, and 2016.

▬ Microsoft Office 365 Monitoring

Site24x7 is an agentless way to monitor Office 365. In other words,

and users need not share their credentials directly with Site24x7. Once a user logs in through the Microsoft portal, Site24x7 is registered in that user's Office 365 account with read-only permission. Access tokens (generated from the Windows Graph API requests) are used to fetch data from the user's Office 365 account, and that information is then presented in the Site24x7 web client.

The user account provided in Site24x7 should be a licensed account and the user should have a Global Admin role in their Office 365 account. With Office 365 monitoring, you can view stats on the outgoing and incoming mail traffic of Microsoft Exchange servers; the usage of your SharePoint sites; instant messaging (IM), audio, and video conversations; and Skype (Lync) meetings.t

Microsoft BizTalk Monitoring

BizTalk Monitoring provides a complete picture of all parameters that are critical to the functioning of your BizTalk server, ensuring smooth performance. With BizTalk Monitoring, you get in-depth knowledge on the active state of orchestrations; metrics related to messaging performance, messages received/sent per second, and the active sessions manageable for any adapter; and host throttling metrics.

BizTalk servers are automatically discovered and added for monitoring once the Windows monitoring agent is installed. Site24x7 supports BizTalk Server version 2006 and above.

Microsoft Hyper-V Monitoring

Monitor your Microsoft Hyper-V servers and their guest virtual machines to increase their server uptime. Site24x7 ensures continued functioning of your Hyper-V environment and manages virtualization solutions from multiple vendors from a single console. Identify the CPU, memory load, disk usage, and network capacity of the applications to be included in your virtual infrastructure, and gather metrics on hypervisor, VMs, processor, network, storage, and more for both your host server and VMs. Automate the start, stop, and restart of Hyper-V VMs with Site24x7's IT Automation.

The Hyper-V servers are automatically discovered and added for monitoring once the Windows monitoring agent is installed. Site24x7 supports Hyper-V version 2008 and above.

Windows Updates Monitoring

Install a Windows update monitor to ensure that your servers are always up to date. Set attribute thresholds and get notified when the updates fail.

Windows Server Backup Monitoring

Add a backup monitor to your Windows server to keep track of backups, events, disc use, and policy scheduling data. Set attribute thresholds and get notified when the threshold is exceeded. The Site24x7 Windows agent is used to monitor Windows server backups, thus once the Windows agent is installed, they will be auto-discovered and put to the monitoring list.

Application Log Management

AppLogs is a Site24x7 log management service that helps you upload and manage your logs within a single dashboard across all your associated servers. AppLogs works with an existing Site24x7 Server Monitoring agent and open-source log collectors like Fluentd & Logstash. The logs are retained for 30 days. You can perform a query language search to search for logs, and then save any required searches. AppLogs Alerts allow you to set thresholds and associate AppLogs alerts to your predefined user alert groups, third-party ITSM, collaboration tools like Jira, PagerDuty and Slack so you can thwart critical operational issues right when they start. Also, you can configure IT Automations that allow you configure actions for log alerts and fix common incidents without any manual intervention.

By default, Site24x7 supports logs from frameworks like Log4j, Mono-Log, Log4net, and NLog, and from over 70 applications including IIS, Apache, Syslogs, Windows event logs and Redis. Cloud logs like Azure and AWS are as well, supported. The system, application, and security logs are also natively supported, and Site24x7 will support more log types in the future. You can also monitor other application logs by creating a custom log type and mapping it with a log profile that's associated with any required servers. If you require to access the old log data (>30 days), you can use our re-index feature to re-index logs.

AppLogs Scheduled Reports give you detailed insights with all your default log type widgets and saved searches for the log types you

choose. You can also view your saved search queries along with charts or tables in different widgets.

With AppLogs, you can also collect and manage events from Zoom Meetings, Video Webinar, Conference Rooms, and Chat, and analyze their availability and performance.
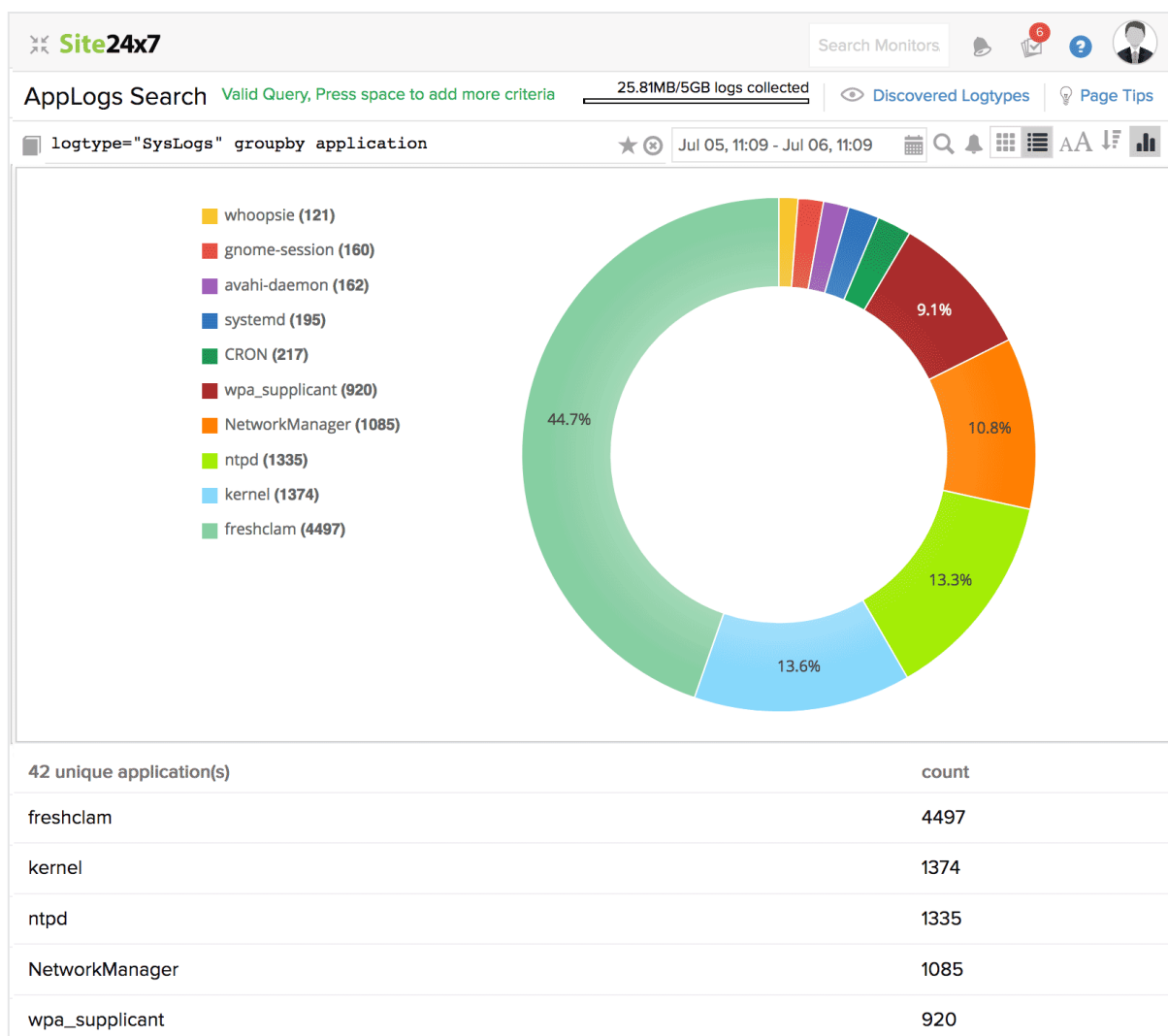

Figure 7: AppLogs - query language search

Plugins: Out-of-the-box monitoring for 100+ apps

Network and server administrators often require specific monitoring data that goes beyond the scope of vendors' standard monitoring solutions. In addition to more than 100 ready-to-use plugin integrations, you can also build your own plugin for Linux and Windows servers and monitor the data you need, the way you want. The first plugin added for a server monitor is free. After that, each plugin monitor is considered a basic monitor. Each plugin can have up to 50 attributes.

Requisites:

Define the attributes that you wish to monitor in a plugin template.

The plugin script should return a JSON object.

You have to install the Windows/Linux Server Monitoring agent to start using plugins.

Features:

• Write your own plugin using Python and Shell scripts for Linux and DLL, Batch, Python, PowerShell, and VB for Windows.

• Execute multiple configurations on a single plugin to avoid creating a new monitor with different names.

• Set thresholds to individual attributes and be alerted if the set values are exceeded.

• Customize the poll interval for data collection, from once per minute to once per day.

• Associate tags, automate repetitive tasks, and integrate with third-party integrations.

Metrics

— StatsD Integration

Gather and aggregate all the custom metrics from your applications, through StatsD and integrate it with Site24x7 in a single console. Configure thresholds and get instant alerts when the metrics violate the thresholds and schedule corrective measures using IT Automation.

Platform Features

━ User and Alert Management

Give users login access for Site24x7, customize the way each contact interacts with your Site24x7 account, and receive notifications about outages. Set up email, or phone-based alert modes. You can also export all your users and alert details in a CSV file. You can organize individuals into groups to receive alerts and reports based on their responsibility. You can even create unique attribute alert groups by consolidating various attributes from multiple monitor types. You must access the Admin > User and Alert Management section in the web client and dedicate a specific monitor status and time spans for delivering alerts to relevant users.

Common User Management

You can manage the information related to a single user for all three products from Site24x7- Site24x7 for monitoring, StatusIQ for incident communication, and CloudSpend for cloud cost management in a common user management platform. Whereas the previous user management model had a separate portal for each

Organization and Site24x7 Roles and Permissions

There are various roles and user privileges allocated to individual users in Site24x7. Users in organizations can assume various roles in Site24x7 based on specific requirements. If you're an Organization admin, you can assign or change the user organization roles using Zoho Directory. The roles available are categorized under

Zoho Organization account roles and Site24x7 user roles.

Zoho Organizations have two roles: Org admin and Org user. Who-ever signs up for Site24x7 will automatically be the Org admin. Site24x7 offers the following user roles:

• Super Admin: If you've created your Site24x7 account, you'll be the Super Admin for your organization and Site24x7 accounts.You'll have complete operational and management control over these accounts.

• Admin: The Admin role has many of the same privileges as the Super Admin role, except for in the subscription billing and On-Premise Poller modules.

• Operator: An Operator has read-only permissions to most of the modules. However, Operators can schedule, edit, or delete a new maintenance window, or create, update, and delete Custom reports and Global Benchmark Reports that they created. Operators can't modify maintenance windows created by other users.

• Spokesperson: A Spokesperson can post Status page announcements via the Public Status Pages. Additionally, a Spokesperson will also have read-only access to most of the modules of that particular Site24x7 account. A Spokesperson has read-only permission to Custom Reports and Global Benchmark Reports generated by all users. A Spokesperson has to be granted permission to access data from monitors in a Monitor Group.

• Billing Contact: A Billing Contact only has access to the Subscription module inside the Admin tab.

• Hosting Provider: A Hosting Provider can only schedule maintenance under the Admin tab; they don't have access permis-

- Hosting Provider: A Hosting Provider can only schedule mainte-nance under the Admin tab; they don't have access permissions for any other part of Site24x7.

- Read-Only: Read-Only users have read-only access to most of the modules in Site24x7. For a Custom Report and a Global Bench-mark Report, Read-Only users need permission to view reports. However, Read-Only users can perform actions like Poll Now, and export and email reports.

- Admin with group-level permission: An admin with moni-tor-group-level permissions can edit or delete monitors they can access.

Monitor Groups and Tags

◆ Monitor Groups

Monitor Groups enable you to seamlessly organize your monitored resources for easier administration. You can sort resources (monitors) by business application, geography, type, and resource ownership. Aside from general reporting, Monitor Groups offer insight into the real-time and historical operational trends of individual resources and groups during an outage. Additionally, you can also add nested Sub-groups up to level five under a main Monitor Group, and visualize all your monitored resources using a Business View.

◆ Tags

Tags offer a powerful yet intuitive way to classify and discover resources in your Site24x7 account in different ways, such as by resource type, user role, or environment. You get more flexibility to manage and sort your Site24x7 monitors (as well as their related

alerts and reports) by adding your own custom metadata in simple name-value pairs and associating them with your resources. Since Site24x7 has a hybrid tagging concept, a tag can consist of an arbitrary key name and an optional value, both of which you can define.

Configuration Profiles

Maintain the configurations for all your monitors in one place and apply settings to all monitors uniformly. You can create the following Configuration Profiles: Location Profiles, Notification Profiles, Threshold and Availability Profiles, Email Templates, Global Parameters, OAuth Providers, and Web Tokens.

Location Profiles

Location Profiles make it easy to set monitoring locations consistently across many websites or monitors. Based on your IT infrastructure, you have the freedom to choose from a wide range of IPv4 and IPv6-supported monitoring locations around the world. Based on your monitor type, you can also choose your configured On-Premise Pollers and mobile network pollers to monitor your resources.

Notification Profiles

Notification Profiles allow you to define your notification rule and let you tweak when alerts are generated and who receives them. You can define critical notification and escalation settings right here. Some of the settings include:

Downtime notification delay: Delay notifications by choosing to get notified after two to five continuous failures.

Persistent notifications: Receive continuous alerts based on the poll

count you've configured, until the errors are rectified for your DOWN/TROUBLE monitors.

• Escalation settings: Define an escalation policy, including contact groups and downtime duration before escalation.

Threshold and Availability Profiles

Threshold and Availability Profiles help the alarms engine decide if a specific resource has to be declared CRITICAL or TROUBLE. Configure Downtime Rules to reduce false alerts for monitors. Individual monitors have unique sets of threshold values that can be configured. Once defined, the threshold profile can be associated with a monitor to trigger default trouble alerts when the set threshold is breached. Using the advanced threshold settings, you can even set trouble or critical alert conditions for all parameters. For example, you can configure thresholds for response time spikes for both Primary and Secondary locations.

Credential Profile

Credential Profile is a secure library of sensitive data. You can store the key usernames and passwords of your resources here for easy use when you start monitoring. Credential Profile helps you to easily add and associate credentials with monitors so that you don't need to provide your third-party account details every time you add a resource for monitoring.

Email Templates

Email Templates help you customize the content of alert emails. You can associate an Email Template with a Notification Profile, which in turn is associated with a monitor.

Global Parameters

Global Parameters are custom name-value pairs that can be defined as part of your Site24x7 global configuration. Once defined, these parameters get embedded into the monitoring forms and text fields that you access, where they get assigned along with other default parameters. You can invoke a Global Parameter in these forms and text fields by simply entering a $ symbol and selecting the relevant parameter. The Global Parameter will be defined in the format ${PARAMETERNAME}. Once the form data gets rendered or is used, the defined parameter names get auto-replaced by the corresponding constant or dynamically generated values.

OAuth Providers

OAuth 2 is an open authorization framework that provides client applications secure delegated access over HTTP to a server resource on behalf of a resource owner. Site24x7 lets you set up multiple OAuth Providers for monitoring your API endpoints. Every OAuth Provider lets you generate a unique access token, which can be used to authorize Site24x7 to monitor your websites/endpoint APIs. While configuring monitoring forms for URLs, REST API, and SOAP workflows, you can use these preset OAuth access tokens for authentication purposes.

Web Tokens

A JSON Web Token (JWT) is an industry standard defined in RFC 7519 as a compact and self-contained way to create access tokens for securely transferring information between two parties. Register Site24x7 with your authentication server to monitor protected resources using Web Tokens.

◆ **Device Key**

A device key is a unique and secure alphanumeric key that allows the Site24x7 agent to collect performance metrics and push that data to Site24x7.com. This data is then presented as performance graphs and reports. To avoid the risk of a security breach, never share your device key with others. For an account with multiple sub-users, only the super admin and admin roles should have access to the device key.

Since device keys are unique, so no two Site24x7 accounts can have the same device key. The Site24x7 agents that use the device key are:
- Windows server agent
- Linux server agent
- FreeBSD server agent
- On-Premise Poller
- Mobile Network Poller
- Java agent for APM Insight
- .NET agent for APM Insight
- Ruby agent for APM Insight
- Site24x7 DeskApp
- Azure VM Extension
- Zapier integration

– Alerts

Alerting is a crucial aspect of monitoring your infrastructure. Alerts warn you when there is an outage or your tests show that the website or service is not meeting required performance standards, so you can respond quickly to fix the issue. Site24x7 delivers alerts for various status changes such as UP, DOWN, and TROUBLE.

Alerts need to be carefully planned and configured. On the one hand, if alert thresholds are too low, the monitoring team will get alerts too frequently and sometimes for issues that don't require action. If the alert thresholds are too high, customers may experience poor performance before the monitoring team is aware there's a problem. You can set advanced threshold settings to define when and for which attribute a trouble alert should be triggered. You can define Alert Settings in the User and Alert Management form to decide on the alerting modes and modify the notification profile settings to reduce false alerts.

To enable seamless alerting via SMS or phone call, you'll need to purchase alert credits from Site24x7. You can also deliver alerts to third-party apps using native integrations or custom web hooks.

Anomaly Dashboard

Site24x7's AI-powered Anomaly Dashboard uses Robust Principle Component Analysis and Matrix sketching algorithms to detect unsual spikes or aberrations in your monitor's critical performance attributes, such as response time, CPU utilization, and memory utilization. All the KPIs will be compared against seasonal benchmark values. It promptly notifies Operations and Dev teams about such spikes well in advance, so they can take corrective actions before the service fails. That way, Operations teams can fine-tune resource performance and safeguard from any unforeseen infrastructure issues. You can also share anomalies within your team via email or by generating a CSV or PDF file.
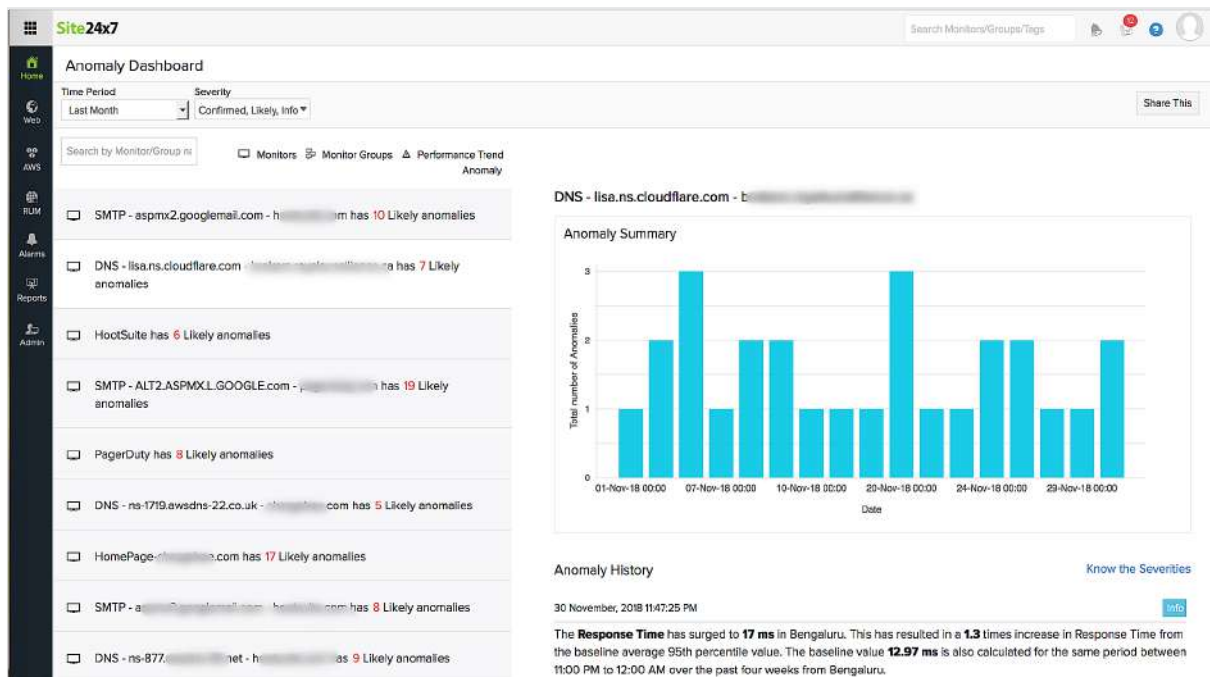
Figure 8: Anomaly dashboard

IT Automation

IT process automation, also known as run book automation (RBA), is the process of orchestrating and integrating tools, people, processes, and more through automated workflows. It reduces downtime from manual processes and human error, leading to faster deployment. In a lot of cases, automation increases efficiency and decreases costs.

All Site24x7 automations, except invoke URL, mark as maintenance, and the supported AWS service actions, require installing a server monitoring agent. The automations will be handled and executed by the Site24x7 IT Automation Engine, a part of Site24x7's data center. Available automation tools include server scripts, server commands, invoke URL, server reboot, starting/stopping of Windows services, IIS application pools or sites, Hyper-V VMs, EC2 instances, and RDS instances. You can also view the complete history and status of
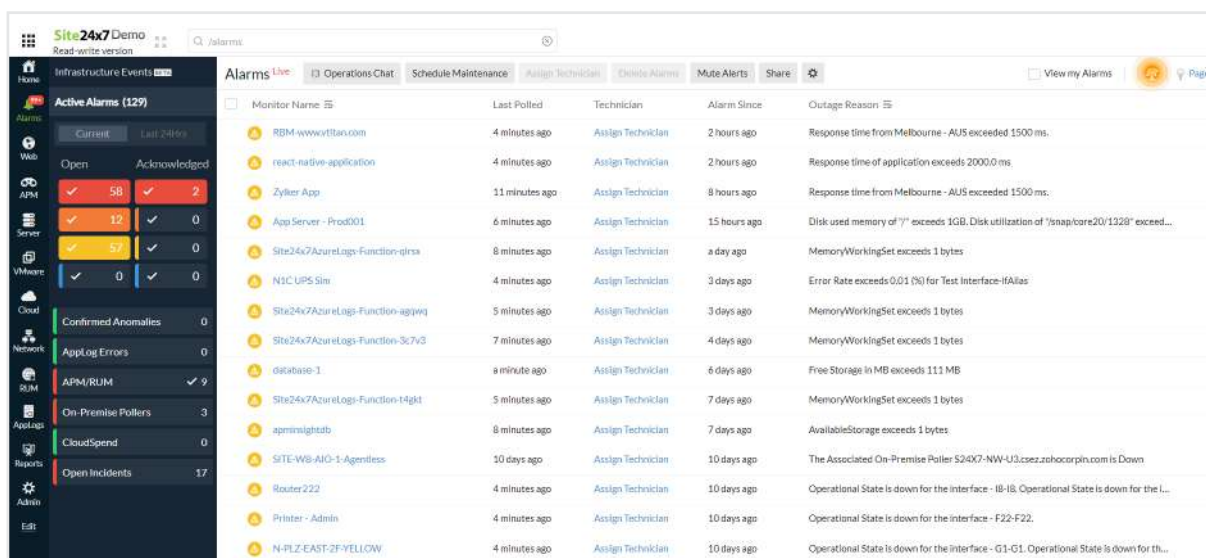
all executed automations by date. A maximum of 100 automations can be added per Site24x7 account.

Alarm Management

The Alarms view in Site24x7 lets you keep tabs on all the monitor issues in your configured account by grouping all alerts by monitor name and severity. Based on the selected toggle button, e.g. Current Alarms, you can view all monitors that are currently in DOWN or TROUBLE status. Classifying alarms based on severity level helps you pinpoint alarms that should be addressed first. Additionally, you can assign alarms to any technician according to your need.

You can filter your alarms based on their acknowledgement and severity status. Site24x7 super admins, admins, operators, and especially NOC Teams or IT Operations Managers can use Operations Chat to initiate account level discussions on IT operations.You can also share your alarms in CSV or PDF format.

Figure 9: The Alarms tab

If you're aware of an issue in your setup that you don't want to generate alerts in Site24x7, you can mute alerts to temporarily disable alerting for a specified period of time. You can suppress alerts for a specific set of monitors, monitor Groups, or even for all resources in your account.

Third-party Integrations

Site24x7 offers native integrations with popular collaboration tools, including Microsoft Teams, Slack, HipChat, and Stride. It also connects with ticketing platforms like ServiceDesk Plus (on-premises and cloud) and ServiceNow, as well as incident management platforms like PagerDuty, OpsGenie, or AlarmsOne. With all of these integrations, Site24x7 alerts are pushed to these other platforms for intelligent alarms handling. You can also use custom web hooks to push Site24x7 alerts to any third-party app.

Dashboards

Dashboards in Site24x7 are broadly categorized as system dashboards and non-system dashboards. Both are listed in the web client under Home > Dashboards.

System Dashboards

The primary system dashboards are the Operational Dashboard, NOC Dashboard, and the Anomaly Dashboard. These dashboards need not be configured manually; they're auto-generated based on the various monitor details analyzed by Site24x7.
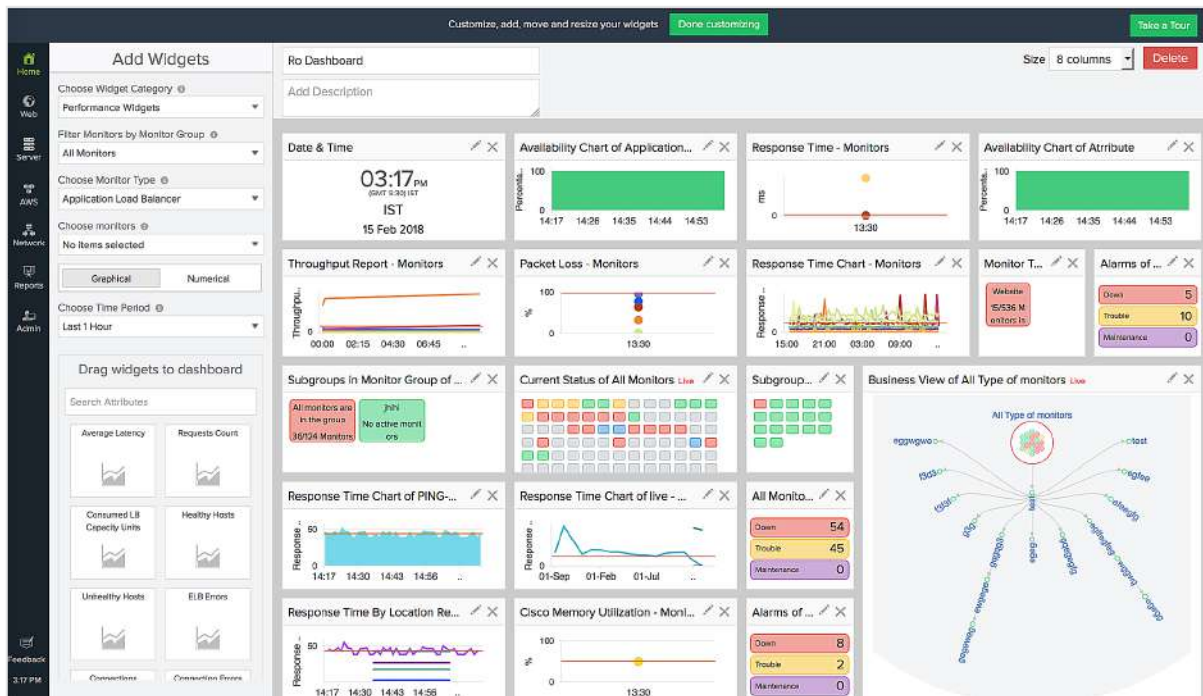
Figure 10: Dashbaords

Non-system Dashboards

Non-system dashboards include Custom Dashboards, Business Views, and Infrastructure Maps. You have to manually create non-system dashboards as per your needs. You also need to have a paid subscription plan to use non-system dashboards.

- Custom Dashboards: Custom Dashboards enable you to bring together various key metrics from every tier of your infrastructure. They help you portray data differently than Site24x7's default dashboards. You can create personalized dashboard views with dynamic widgets that can be dragged and dropped onto a common dashboard grid. You can add up to 100 widgets and create 100 custom dashboards. Custom Dashboards auto-refresh every minute.

- Infrastructure Maps: Infrastructure Maps let you manually create a schematic description of your network topology by logically arranging your physical nodes, network devices, interfaces, and links over a predefined or custom background.

This view renders a visualization of your devices, hosts, and their interlinkages, and provides the accurate status of the various resources for quick troubleshooting.

• Business Views: Business Views allow you to easily filter out details about the availability of individual monitors, Monitor Groups, and Subgroups. You can automatically build Business Views based on system-generated Monitor Groups or using default templates provided by Site24x7.

Reports

Site24x7 offers many in-depth reports on the availability and performance metrics that matter most. View the required metrics, intuitive graphs,or heat map widgets, and generate reports for a custom time period. Some of the reports are:

• Summary Report
• Availability Summary Report
• Busy Hours Report
• Health Trend Report
• Performance Report
• Top N Report
• Global Benchmark Report
• Custom Report
• Outages Report
• Security Report
    • SSL/TLS Grade Report
    • Brand Reputation Report
    • Real-time Blocklist Report
• Poll Now Report

The Summary report provides details about the average response time, overall availability, and number of downtime events. You can also generate SLA reports to ensure your hosting provider meets your defined SLAs.

You can go to Report settings in the web client to schedule a report; Site24x7 offers daily, weekly, or monthly scheduling options.

▬ Scheduled Maintenance and Bulk Actions

By default, all monitor alerts are suppressed during scheduled maintenance windows. However, you can increase your overall uptime by enabling monitoring during maintenance periods. Once monitoring is enabled during maintenance, the Maintenance Monitors View will accurately track and list the real-time status of your monitor during the maintenance window.

Bulk Actions in Site24x7 help you perform a particular admin action on multiple monitors at once, all without using APIs. Supported bulk actions include monitor activation, deletion, or suspension; modification of threshold groups, user alert groups, or location profiles; or even actions like adding tags to sort monitors into a smarter view.

Site24x7 also allows you to bulk import and export monitors using a CSV file. For the REST API Monitor, you can import the monitor configurations in CSV, JSON (Swagger definition), or HAR formats.

Configuration Rules

Use Configuration Rules to automate the configuration settings of your monitoring resources. You can also create custom rules to track configuration changes continuously and achieve the ideal configuration settings. This can help you in editing multiple monitors to associate different monitor groups or adding a different tag can be a tedious process.

MSP Plan for Managed Service Providers

Manage your customers' IT infrastructure efficiently with our secure, scalable, and affordable monitoring suite for Managed Service Provider and Cloud Service Provider.

The MSP plan offers a number of unique features:

• Monitor multiple customers in silos in a multi-tenant set-up.

• Easy subscription handling.

• Scalable, cost-effective model.

• Real-time alerting and false alerts protection.

• Deep visibility and control into your customers' IT infrastructure environments.
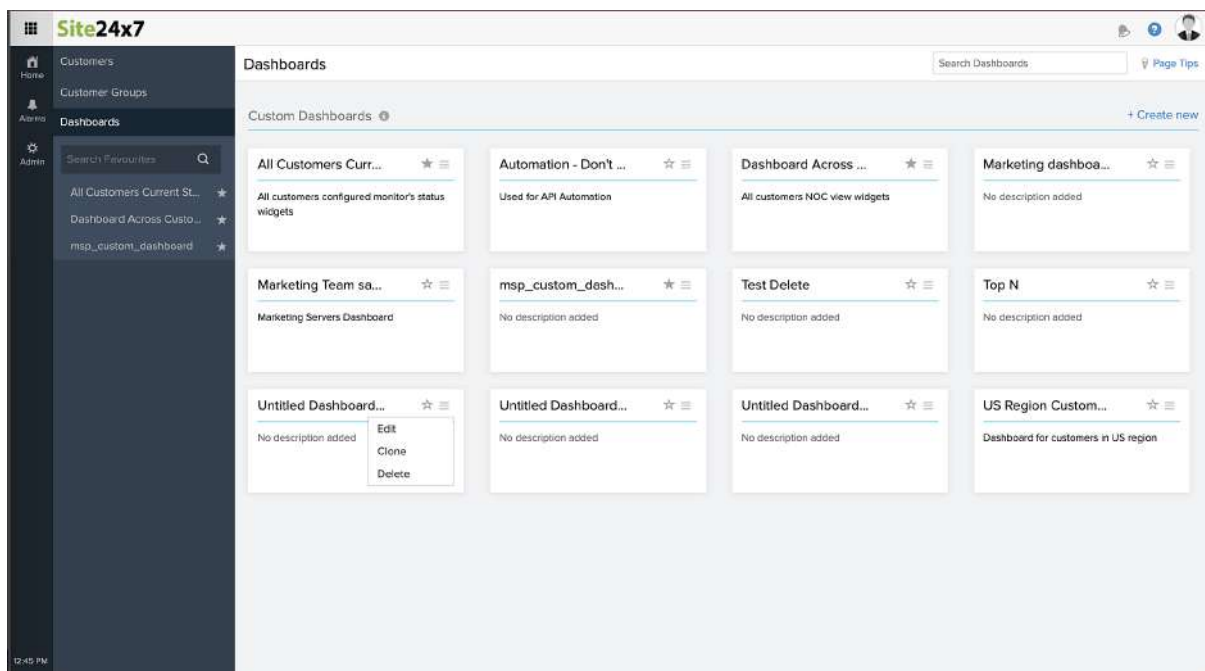
• MSP white-labelling opportunities

Figure 11: The MSP plan

Teams Management

Segregate and streamline IT monitoring among different teams or units in your organization from a single console using teams management or business units in Site24x7. It helps you organize and administer individual monitoring accounts based on the business application, geography, type, and resource ownership.

- Better resource and account-level optimization.
- Easy management of subscription and billing process for all your business units from a single console.
- Centralized pricing and global-level and distributed purchase of licenses.
- Scalable and cost-effective model to manage multiple business units efficiently.

StatusIQ

StatusIQ is a status and incident communication platform that helps inform your customers about updates on active incidents and planned maintenance. Communicating real-time status can reduce the pressure on your support team during unexpected outages. The features offered by StatusIQ are:

- Setting important resources as components to keep a track of their status.
- Real-time incident creation to keep your customers updated.
- Private Notes to communicate with your team.
- Postmortem reports to share a detailed analysis of incidents.
- Status automation via Site24x7, Rest API, or email.
- Notify subscribers via email or SMS.
- Make your pages private pages using passwords/IP restriction.
- Status page customization with custom domain, custom sender domain, logo & favicon.
- Incident and maintenance templates.
- Personalize your status page and the elements on it to reflect your brand colors using color customization.
- Create templates in prior to save time during incident and maintenance creation.
- Showcase status to your users by embedding graphical status widgets on your website.

CloudSpend

Understanding how and where you are accruing costs, identifying cost drivers, or keeping costs down can become difficult once you start to scale your cloud platforms. You can tackle these challenges easily with Site24x7 CloudSpend by visualizing runaway expenditures to implement budget controls in your FinOps journey and by performing cloud cost analytics for your resources. Optimize your cloud ecosystem with a drilled-down view of the cloud bills, and understand where the costs are accrued.

- Set up budget limits for cloud accounts or business units and stay on top of your expenses.
- Group and organize the cloud cost with custom search options leveraged via tags.
- Ensure accountability of the cloud bills and efficiently manage chargebacks.
- Exhaustive dashboards with graphical and numerical representations of your cloud expenses.
- Efficient alarm management by integrating with Site24x7.
- Schedule reports on a regular basis and keep a tab on usage.
- Automate your resource usage based on spending via IT automation.
- Forecast your spending patterns to uncover potential futuristic expenses.
- Customize your reports based on your requirements.
- Manage access using flexible user management options.

Mobile App

Site24x7 offers native iOS and Android apps as free supplemental tools to Site24x7 users. With the Site24x7 mobile app, you can monitor availability and performance of websites, servers, web applications, cloud services, VMs, and networks while on the move, and receive actionable alerts during an outage in your technology stack. You can track the entire outage history and troubleshoot incidents using detailed RCA reports in the app. You can also track SLA compliance.
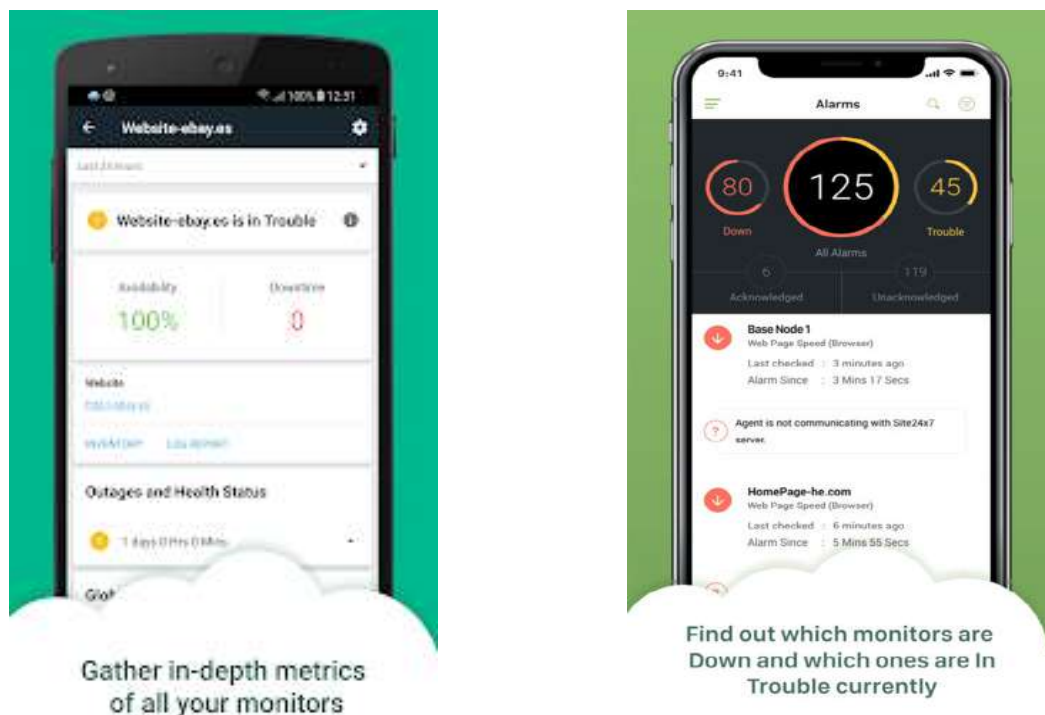

Figure 13: Site24x7 Mobile App

The apps are so comprehensive that you can perform most administrative actions from the app itself. If you receive a push alert on your app stating that a monitoring service has stopped on your server, you can instantly restart the monitoring service from the app.

Plans and Pricing

Site24x7's pricing model is completely based on the number of monitors you add. Each monitor is defined as either an advanced or basic monitor, and each pack has a predefined number of basic and advanced monitors that customers can add. The different packs that are available are provided below:

- **Starter:** The perfect solution for small-scale or individual business owners.
- **Pro:** The ideal solution for medium-scale businesses that want to monitor multiple monitors with advanced capabilities.
- **Classic:** Provides close to double the number of monitors available in the Pro pack. Ideal for large businesses trying to migrate to Site24x7.
- **Enterprise:** The largest pack available in Site24x7. Ideal for businesses with a large number of resources to monitor.
- **MSP:** Other than the four packs mentioned above, Site24x7 also provides a custom MSP plan for managed service providers. This pack supports monitoring different customer accounts from a single unified dashboard.

The idea behind having different packs with predefined number of monitors and other features is to ensure that we provide a variety of different offerings as per the requirements of the end user. Also if a user has already purchased a pack with a set number of monitors, they can purchase add-ons to increase their monitor count without having to purchase a larger pack.

The idea behind having different packs with predefined number of monitors and other features is to ensure that we provide a variety of different offerings as per the requirements of the end user. Also if a user has already purchased a pack with a set number of monitors, they can purchase add-ons to increase their monitor count without having to purchase a larger pack.

A monitor is characterized as either basic or advanced strictly based on the complexity of the monitoring or the number of in-depth metrics provided. Below is the complete list of all basic and advanced monitors

Basic Monitors	Advanced Monitors
Website (HTTP/HTTPS)	Web transaction (Browser)
DNS	Web page speed (Browser)
Ping	Website Defacement
FTP Server	Mail Delivery
SMTP Server	FTP Transfer
SOAP Web Service	APM Insight (Each JVM/.NET/ Ruby/Node.js instance)
Rest API	Microsoft Sharepoint
Port (Custom protocol)	Micrsoft Biztalk
POP Server	Microsoft Active Directory
Windows/Linux/FreeBSD/OS X Servers (Agent based)	Microsoft Failover Clusters
Microsoft IIS	Microsoft SQL
VMware VM Instances	Microsoft Hyper-V
VMware ESX Hosts	Microsoft Exchange Servers

VMware Datastores	
Cron/Heartbeat	
AWS EC2/RDS/ DynamoDB/SNS/ELB instances	

In addition to basic and advanced monitors, Real User Monitoring, AppLogs, and Network Monitoring are priced separately in each pack. If the license for any customer pack has been exceeded (e.g. the pre-defined pack limit has been reached), then customers can purchase add-ons and continue monitoring similar to monitor addons mentioned earlier.

Also, although all packs offer free email alerts, there is a fixed cap on the number of SMS/voice alerts that can be received. Similar to monitors, once this limit has been reached, customers can purchase add-ons to keep receiving SMS/voice alerts.

Security

Site24x7 is a service offered by Zoho Corporation. With nearly 8 million users worldwide accessing Zoho services, individuals, small, medium and large organizations count on Zoho security and data protection to meet their needs. We take security very seriously and have developed a comprehensive set of practices, technologies and policies to help ensure your data is secure. They include:

- Site24x7 ISO/IEC 27001 certified; SOC 2 Type II compliance
- OWASP as secure coding practice. Penetration test once every 6 months by our internal hacking team. Vulnerability scan every week.
- Undergoes an industry standard security audit every year, where an evaluation of the design and operating effectiveness of controls with respect to AICPA's Trust Services Principles are diligently done.
- Distributed Grid Architecture Data Protection and Back-up 24x7x365
- Security 128/256-bit SSL.
- GDPR compliant

We've dedicated data centers in important regions around the world:

United States: www.site24x7.com

European Union: www.site24x7.eu (Amsterdam, Dublin)

China: www.site24x7.cn

India: www.site24x7.in (Chennai, Mumbai)

Site24x7

Read detailed instructions for installing, configuring and using Site24x7 for your various monitoring needs.

READ HELP DOCS

Browse through our frequently asked questions and their standard solutions to quickly resolve the most common problems affecting your monitoring.

BROWSE KBASES

Our tutorials provide a step-by-step walk through various steps, right from set up to configuring alerts.

CHECK TUTORIALS

Contact our product experts for queries related to our certification program.

CONTACT NOW