

ManageEngine
Site24x7

Certification



STUDY MATERIAL

Contents

1. [About Site24x7](#)
2. [Basic overview: Monitors and the homepage](#)
3. [Monitoring digital experience](#)
 - a. [Website](#)
 - b. [Synthetic transaction monitoring](#)
 - c. [Other internet services](#)
 - d. [Security monitoring](#)
 - e. [Real user monitoring](#)
4. [Infrastructure monitoring](#)
 - a. [Server monitoring](#)
 - [Agent-based server monitoring](#)
 - [Agentless server monitoring](#)
 - b. [Cloud services monitoring](#)
 - [Amazon Web Services \(AWS\)](#)
 - [Microsoft Azure](#)
 - [Google Cloud Platform \(GCP\)](#)
 - c. [Virtualization monitoring](#)
 - d. [Kubernetes monitoring](#)
 - e. [Docker monitoring](#)
 - f. [Database monitoring](#)
 - g. [Cron monitoring](#)
 - h. [Heartbeat monitoring](#)
5. [Network monitoring](#)
6. [Application performance monitoring and troubleshooting](#)
 - a. [Supported platforms](#)
 - [Java application monitoring](#)
 - [.NET application monitoring](#)
 - [PHP application monitoring](#)
 - [Ruby application monitoring](#)
 - [Node.js application monitoring](#)
 - [Python application monitoring](#)
 - b. [APM features](#)
 - c. [Mobile application monitoring](#)
7. [Application log management](#)

8. [Microsoft application performance monitoring](#)
9. [Plugin integrations: Out-of-the-box monitoring for 100+ apps](#)
10. [Metrics](#)
11. [Platform features](#)
 - a. [User and alert management](#)
 - b. [Monitor groups and tags](#)
 - c. [Configuration profiles](#)
 - d. [Bulk action](#)
 - e. [Configuration rules](#)
 - f. [Alerts](#)
 - g. [Anomaly dashboard](#)
 - h. [IT automation](#)
 - i. [Alarm management](#)
 - j. [Third-party integrations](#)
 - k. [Dashboards](#)
 - l. [Reports](#)
 - m. [Teams management](#)
 - n. [Schedule maintenance](#)
12. [AIOps](#)
13. [Mobile and TV apps](#)
14. [StatusIQ](#)
15. [CloudSpend](#)
16. [Digital Risk Analyzer](#)
17. [MSP plan for Managed Services Providers](#)
18. [Plans and pricing](#)
19. [Security](#)

1. About Site24x7

Site24x7 is an all-in-one, AI-powered, and cloud-based monitoring tool for IT and DevOps teams that offers website, server, network, application performance, cloud, and real user monitoring from over 130 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.

2. 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, virtual machines (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. 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.

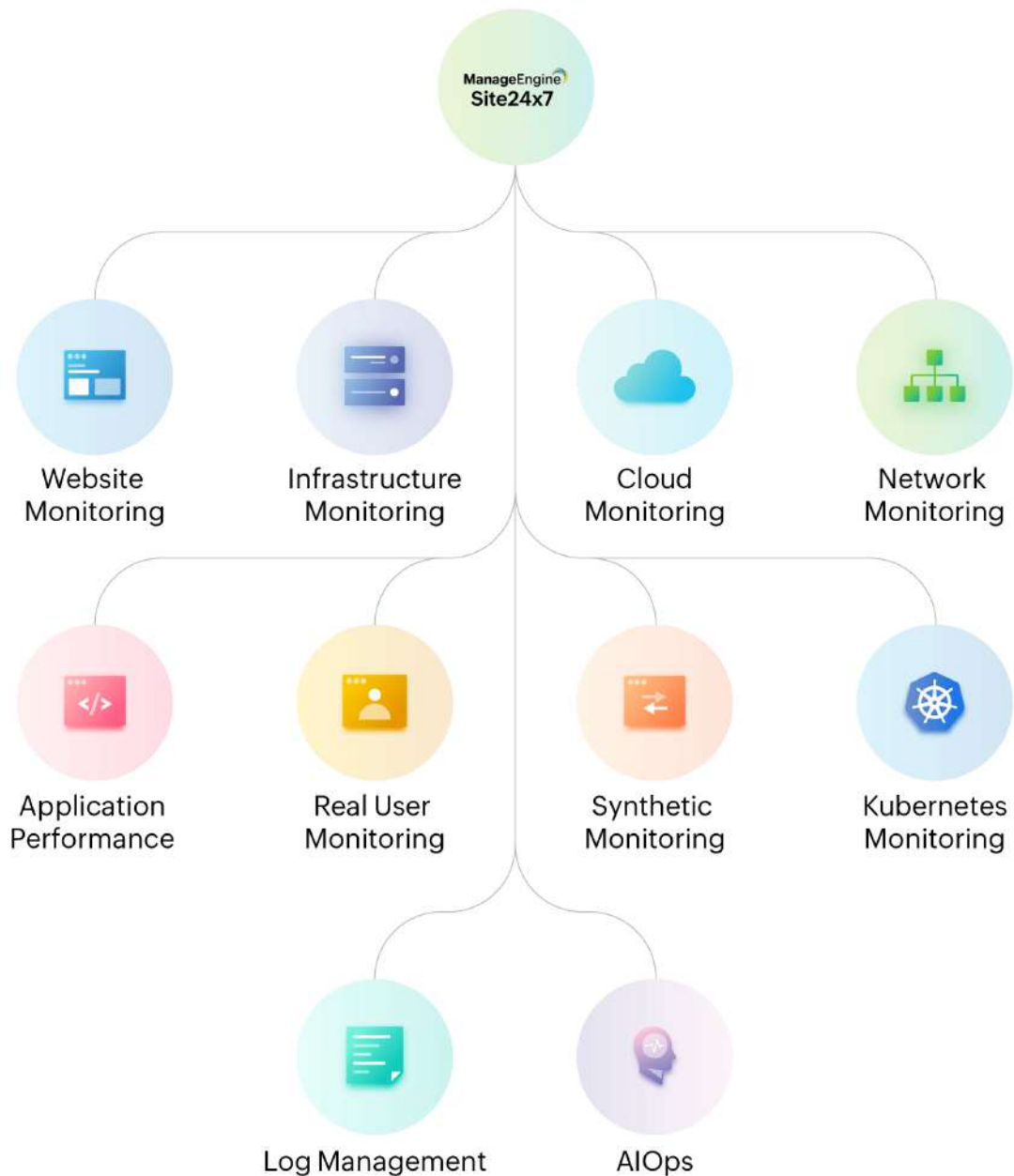


Figure 1: Site24x7 - overview

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 VMs.

With the High Availability On-Premise Poller, 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 downed On-Premise Pollers.

3. Monitoring digital experience

3.a. Website

Site24x7 acts as a continuous URL monitoring service by keeping a constant watch over specific websites and tracks the availability of websites at preconfigured intervals spanning from 30 seconds to once in a day. A website monitor verifies the availability of addressable, standard HTTP or HTTPS URLs from over 130 global locations, as well as from behind your firewall using On-Premise Poller. Uptime is usually depicted as percentage in Site24x7.

You can:

- Enable Site24x7 to resolve the website IPs using the domain authoritative name servers 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 frequently and receive instant alerts if websites are down from any of the monitoring location.
- Monitor websites that use HTTP/1.1 or HTTP/2
- Ensure the integrity of your websites with the help of content checks.
- Perform continuous monitoring of your URLs from sitemaps or sheets and get your newly APIs also monitored.

Gain visibility into your website's response time and other split-up including DNS time, connection time, SSL handshake time, first byte time, and download 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 on SSL/TLS protocol version and cipher suite details like key exchange, bulk encryption, and hash function from the Poll Now report. During a Down/Trouble outage, you can receive an in-depth root cause analysis (RCA) report after the monitor reports an outage lasting for 150 seconds or longer. The RCA report offers basic details about your monitor, outage, and rechecks; it includes the following details:

Checks from the primary location and re-checks from the secondary location

- Ping analysis
- DNS analysis
- TCP traceroute
- cURL Checks
- MTR report
- MTR-based network route
- APM Traces
- Visibility into your RUM-related metrics
- Screenshots from the website

3.b. Synthetic transaction monitoring

Web applications

Web application user flows can be easily monitored using Site24x7's Synthetic 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 130 global monitoring locations or from a private

location (using the On-Premise Poller for Linux). You can configure resolutions according to the device and record transactions for tablets, iPads, or mobile devices besides desktop devices. You can also monitor applications with MFA or TOTP. In addition to a list of metrics, you can also obtain screenshots to cross-verify the steps in the transaction, a waterfall chart with page-level details, options to compare the HTML, compare screenshots, and an exhaustive root cause analysis report. You can also obtain APM Traces related information, data based on RUM analysis, and much more.

In addition to monitoring web applications, you can use the SaaS Synthetics monitor to track the availability and performance of SaaS-based applications, such as Microsoft Outlook and Salesforce. This monitor tracks metrics such as transaction details, event timeline, and page load time based on various locations, ensuring the efficient operation of SaaS applications.

REST applications

Site24x7's REST API Transaction monitor can track 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 complete monitoring the workflow. You can also import steps from HAR, OpenAPI 3.0, cURL, Postman, and WSDL to monitor them using Site24x7.

3.c. Other internet services

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 on a real browser (you can choose your preferred browser) to analyze all its resources and offers Lighthouse report to drill deep into the performance of your websites. 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 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 list of domains to be blocked to restrict monitoring of these domains. You can add domains at monitor level or account level. You can also validate all the individual elements on a page by setting the required configuration.

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/XPath/JSONPath assertions. Additionally, you can test and validate your JSON response against the specified JSON schema. You can also monitor your GraphQL endpoints. Basic, Webtoken, OAuth, and AWS authentications are supported for authenticating your endpoints. 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 service

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 server

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 configured 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, SRV, and more. You can also check whether the resolved record matches the configured search value. You can debug your DNS-related issues by verifying the DNS responses from our root cause analysis report.

The DNS Server monitor tracks the response time of your DNS server and the average response time from every monitoring location. The following parameters are captured and listed on the *Monitor 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 DNSSEC validation, Site24x7 authenticates the DNS responses and validates the security.

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. Only servers deemed to be accurate by the client are used for synchronization. You can provide an arbitrary drift threshold to detect a false-ticker. 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. 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. The monitor will be considered Up if at least one packet is received. However, if no packs are received, the monitor will be considered Down.

TCP port

Check the connectivity of your TCP ports from over 130 global locations. You can also validate the response of text-based protocols and run Port Status Checks. Receive alerts in case of downtime or if there is a content mismatch in the response. You can opt to receive alerts when your port is available. You can opt to get notified when the port is closed or when the port is not listening and when the port is open or when the port is listening.

Mail server

Site24x7's Mail Delivery monitor checks your inbound and outbound mail servers by verifying delivery to both internal and external mailboxes. It lets you know more about the mail-user experience by testing every aspect of the email delivery process and capturing the email round-trip-time from over 130 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. It creates an uninterrupted connection between two devices and updates the content without having to wait for a request from the user, thereby providing low latency 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 corrective actions.

UDP

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.

gRPC

gRPC is an open-source, high-performance remote procedure call (RPC) framework that helps in creating scalable APIs and also enables faster client-server communication. With Site24x7's gRPC monitoring, you can run health checks to ensure the availability of your gRPC services and the functionality of all the related services. We support unary RPCs, client-side and server-side streaming RPCs.

You can also track whether the client-server communication is working well by ensuring that the data is rendering and confirming whether the gRPC endpoints are available.

File upload

Say for instance, that you've a support portal where customers can raise their concerns, upload load files, or images. With Site24x7's File Upload monitoring, you can ensure whether the files are getting uploaded without errors, by checking the availability of your API endpoints.

File Upload monitor regularly checks the availability and response of your API endpoints over IPv4 or IPv6 enabled locations. It supports multipart data (text and files) in the request body.

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 an in-depth visibility into the availability and latency in the routing path between your network and any location server.

With Site24x7 ISP latency monitoring, you can:

- Obtain the latency of each path from various locations and view a global latency map.
- Gain insights on performance metrics such as jitter, latency, hops, downtime, availability, and hop count.
- Obtain a detailed hop-to-hop view and Autonomous System (AS) number view.
- Visualize the data transfer using traceroute.
- Pinpoint connectivity loss and faulty interfaces.
- Troubleshoot network issues.
- Check if ISPs are abiding by their SLA.
- Get notified in case of any latency-related issues or delays in the network.

3.d. Security monitoring

Real-time Blocklist (RBL) check

Getting blocklisted can affect your brand's reputation and your relationship with 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 instill 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 Google's Web Risk list (a repository that contains all the webpages are blacklisted) to notify whether your site is listed there or not. 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. This monitor allows you to add unlimited URLs for Brand Reputation check. The default check frequency is set as one hour. You can view a detailed security report for your Brand Reputation monitor and can share it as well.

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. You can view a detailed security report for your Website Defacement monitor and can share it as well.

Expiration checks

SSL/TLS certificate

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), certificate chain related issues, Online Certificate Status Protocol (OCSP) 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. You can check the vulnerabilities, the insecure ciphers, and protocols associated with the certificate. You can also view and share a detailed report as well for your SSL/TLS certificate monitor.

Domain expiry

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. You can also ensure the integrity of your domain with the help of content checks by verifying WHOIS records.

3.e. Real user monitoring

Real User Monitoring (RUM) gives you visibility into the behind-the-scene performance of your web application, along with accurate insights 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 single page applications (SPA) framework and optimize them for better customer experience.

Web vitals

Web Vitals are modern user-centric metrics developed by Google that measure a

user's experience loading a webpage. These measurements assess how quickly a web page's content loads, how quickly a browser responds to a user's input, and how stable the content loads in the browser. These factors will be taken into account when Google ranks your web pages for mobile devices.

Currently, Site24x7 RUM measures four web vitals.

- i. **Cumulative layout shift**- This score is used to determine the "visual stability" of a page. The lower the CLS score, the better the visual stability.
- ii. **First input delay**- This score is used to measure the time between when a user interacts with your site for the first time (i.e. when they click a link, tap a button, or press a key) and when the browser can reply to that interaction.
- iii. **Largest contentful paint**- It measures the time from when the page starts loading to when the largest text block or image element is rendered on the screen.
- iv. **First contentful paint**- It measures the time from when the page starts loading to when any part of the page's content is rendered on the screen.
- v. **Interaction to next paint**- It measures a page's overall responsiveness to user interactions by assessing the latency of all click, tap, and keyboard engagements that occur during the course of a user's visit to a page. The final INP value is the longest interaction recorded after excluding outliers.
- vi. **Time to first byte**- It measures the time between when a resource request is made and when the first byte of response begins to arrive.

User sessions

Analyze the behavior of your website users using user sessions. You can also understand how users navigate through your website, and learn how much time they spend viewing each webpage, and in each session.

Filterable performance

Analyze your website performance by filtering it based on various parameters, including browsers, devices, countries, users, domains, and Internet service providers (ISPs) using filterable performance. This helps you identify granular details that impact your website performance, and the end-user's experience.

JavaScript errors

Site24x7's JavaScript Errors feature facilitates monitoring and debugging in modern applications.

- Users can view error metrics, filter errors based on various parameters, and analyze error details such as device, browser, and affected users.
- The tool provides a stack trace with the ability to de-obfuscate minified code and pinpoint the exact line of error.
- Automatic source map detection and manual upload options enhance debugging.
- Users can upload source maps and JS source files, view recent actions as breadcrumbs, and access detailed error reports.
- The feature simplifies debugging in scenarios where cryptic minified code makes error identification challenging.

Waterfall analysis

The waterfall chart provides invaluable insight into the list of resources made to load a page and the time taken for each. It allows you to see how a page is loaded and which requests took the longest time, enabling you to pinpoint where to focus on performance optimization for that page.

Auto RUM injection

Enable RUM effortlessly in your application through the Auto RUM Injection feature, which will be automatically activated for Java and PHP agents. The RUM monitor will be in the name format `<APM_name>-RUM`. To view the RUM metrics collected for your Java application, select **RUM** icon > Find your application, and click it.

4. Infrastructure monitoring

With Site24x7, monitor the health and performance of your servers, the applications running on them, and also the allied resources in them like directories, files, ports, and logs. Supported OS platforms are: Windows, Linux (all major flavors), FreeBSD, and macOS.

4.a. Server monitoring

Agent-based server monitoring

Windows server monitoring

Monitor your Windows servers and measure more than 80 critical health and 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 on 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 the polling interval of data collection from one-minute, five-minute, 10 minutes, 15 minutes, 30 minutes, 1 hour, 3 hours, 6 hours, 12 hours, to one day.
- 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, and 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 in-depth understanding with the help of insightful reports like inventory report, top 5/10 processes based on CPU and memory utilization, and many more.
- Cut-down manual intervention with the IT-Automation feature.

Linux server monitoring

Monitor your Linux servers and measure more than 80 critical performance metrics including CPU steal time, load average, 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 the polling interval of data collection from one-minute, five-minute, 10 mins, 15 mins, 30 mins, 1 hour, 3 hours, 6 hours, 12 hours, to one day.
- Bulk-install the agent using Chef, Puppet, SaltStack, Ansible, and more.
- Automate services or processes on the go using your mobile device.
- Auto-discover and monitor Docker containers and SMART disks. This option can be disabled.
- Choose from more than 100 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 report.
- Cut-down manual intervention with the IT-Automation feature.

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.

4.b. Cloud services monitoring

Site24x7 supports monitoring for the following cloud platforms:

- Amazon Web Services
- Microsoft Azure
- Google Cloud Platform

Amazon Web Services (AWS)

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 ElastiCache
- AWS DynamoDB
- AWS Elastic Load Balancing (ELB)
- Amazon Elastic Beanstalk
- Amazon Elastic Block Storage (EBS)
- Amazon CloudFront
- Amazon Elastic Container Service (ECS)
- 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

- Amazon Redshift
- AmazonElastic File Storage (EFS)
- Amazon Simple Email Service (SES)
- Web Application Firewall (WAF)
- AWS AppSync
- AWS Backup
- Amazon EBS Volume
- AWS Batch
- Amazon EBS Snapshot
- AWS Secrets Manager
- AWS Elastic IP
- AWS Glue
- RabbitMQ
- Lightsail
- Amazon GuardDuty
- Amazon FSx
- Lambda@Edge
- DocumentDB
- Gateway Load Balancer
- Amazon Inspector
- SFTP
- Systems Manager
- Amazon AppStream 2.0
- AWS Health
- AWS Trusted Advisor
- Amazon VPC
- Amazon RDS Proxy
- Amazon MSK

Features:

- Uptime monitoring for AWS resources
- Inventory reports
- In-built 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 simplify administration of AWS resources
- Service Quotas feature to view and manage quotas directly from the Site24x7 web client.
- View all the associated monitored resources for your key monitored services.
- Organize your data using Tags to discover AWS monitors and enable uptime monitoring.
- Forecast future values of a performance metric and manage your cloud infrastructure.

- Create default threshold profiles, customize your Guidance Report, and alert the right personnel using with advanced configurations.
- Gain better understanding of your Virtual Private Cloud components such as regions, availability zones, subnets, network interfaces, and protocols with Site24x7's Amazon Virtual Private Cloud integration.
- View, add, or integrate your cost accounts and business units with Site24x7 using ManageEngine CloudSpend.
- Plan, process, and procure additional resources based on the metrics-related data collected with Capacity Planning for monitor groups.

Essential concepts for successful integration between your AWS account and Site24x7

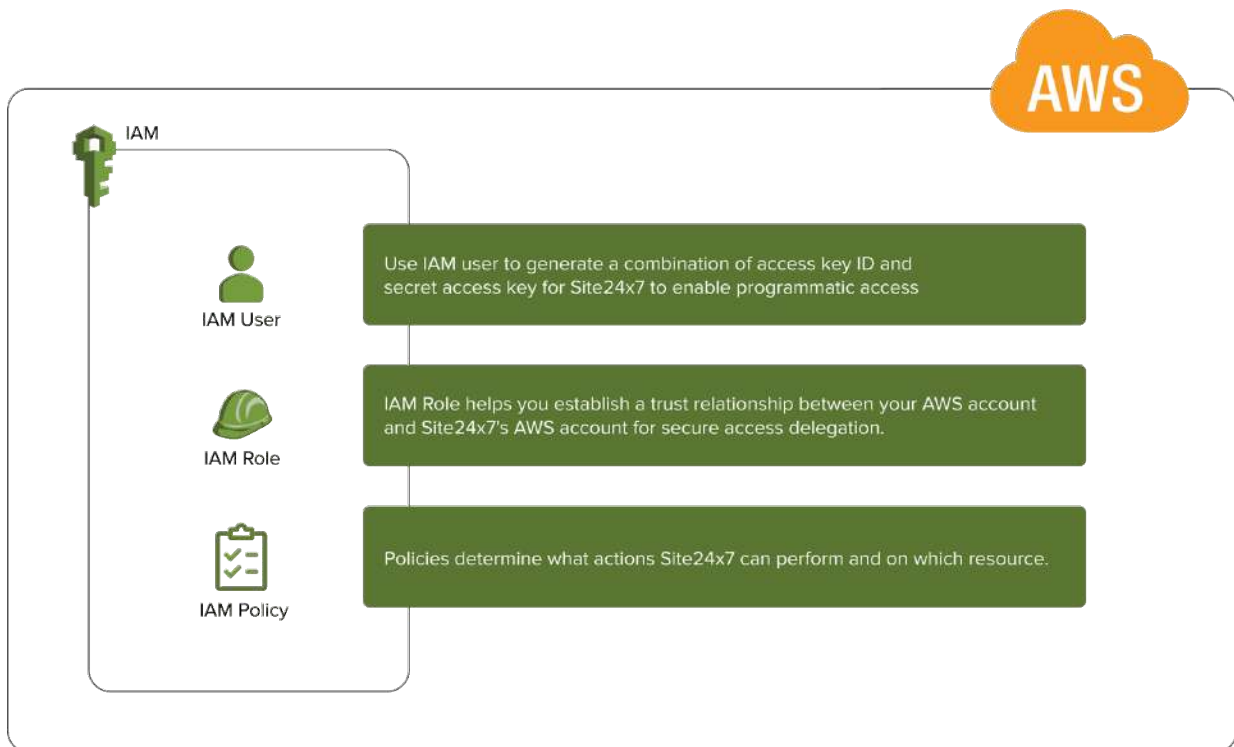


Figure 2: Essential concepts for AWS integration

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 (ReadOnlyAccess) 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.

Cloud Formation IAM role-based access

Site24x7 uses an AWS CloudFormation template to automatically create an IAM role so that you can effortlessly integrate your AWS account with Site24x7. The AWS CloudFormation stack, created with the Site24x7 template, generates the IAM role with the provided configurations and a Lambda function. The Lambda function securely sends the generated role ARN for integration using Site24x7 API key.

Once the role ARN details are fetched, you can configure settings (such as the default threshold profiles for each supported AWS service), mute resource termination alerts, and customize the Guidance Report using the Advanced Configuration option.

AWS Control Tower lifecycle events-based access

You can enable access to your existing and new AWS accounts with AWS Control Tower lifecycle events. Site24x7 uses AWS Control Tower lifecycle events to automatically discover all the accounts in your organization, including new accounts.

The Site24x7-AWS Control Tower integration helps to save time and increase efficiency when managing multiple accounts. For instance, if you create a new account in AWS using Control Tower, the same account gets automatically integrated with Site24x7 without any manual intervention.

AWS IAM Identity Center-based access

AWS IAM Identity Center enables access to your AWS accounts with a consistent single sign-on experience and helps to integrate multiple AWS accounts with Site24x7.

The integration with IAM Identity Center helps you manage all integrated AWS accounts from a single location and enhance productivity and user satisfaction with a set of AWS IAM Identity Center user credentials that integrate multiple AWS accounts into Site24x7.

Microsoft Azure

Microsoft Azure Monitoring monitors over 100 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 different Azure services including Virtual Machines, Scale Sets, Storage Accounts, Cosmos DB, and more.

- Virtual Machines
- Disks
- Kubernetes Services
- Virtual Machine Scale Sets
- Virtual Machines (Classic)
- Fabric Clusters
- Batch Accounts
- App Services
- App Service Plans
- Functions
- Data Factories (V2)
- Power BI Embedded
- HDInsight Clusters
- Data Factory Pipelines
- Log Analytics Workspaces
- Analysis Services
- Event Hubs
- Data Lake Analytics
- Stream Analytics Jobs
- SQL Servers
- PostgreSQL Servers
- Queue Storage
- Search Services
- Machine Learning
- Cognitive Services
- Stream Analytics Jobs
- Device Provisioning Services
- Logic Apps
- Maps Accounts

- Continuous WebJobs
- API Management Services
- Triggered WebJobs
- App Services
- App Service Plans
- CDN Profiles
- Deployment Slots
- SignalR
- Notification Hubs
- Media Services
- Network Interfaces
- DNS Zones
- Firewalls
- Network Watcher Connections
- Load Balancers
- Public IP Address
- Application Gateways
- Virtual Network Gateways
- VPN Gateways
- Storage Sync Services
- Document DB
- Database for MySQL Servers
- SQL Database
- Cosmos DB
- SQL Elastic Pools
- Database for MariaDB Servers
- Redis
- Data Factories (V2)
- SQL Managed Instances
- Service Bus
- Relays
- API Management Services
- Service Bus Queues
- Event Grid Topics
- Service Bus Topics
- Logic Apps
- Table Storage
- Data Lake
- Storage Accounts (Classic)
- Graph
- IoT Hubs
- Kubernetes Services
- Container Instances
- Fabric Clusters
- Batch Accounts
- Container Registries
- Automation Accounts
- Application Insights
- Key Vaults
- Autoscale Settings
- Virtual Networks
- Host Pools
- Network Connections
- Traffic Manager Profiles
- Express Route Circuits

- CDN Profiles
- Recovery Services
- Storage Accounts
- Blob Storage
- Vaults
- File Share

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.
- See which resources are dependent on one another. Keep a record of the dependent 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 resource health issues and ensure reliable deployments and high availability of your services using Azure Deployment Manager (ADM) Health Check.
- View all the activity logs from your Azure account in one console from

Site24x7 Azure Activity Logs.

- Create your own app in the Microsoft Azure portal and assign the necessary permissions.
- Update your Client Secret Expiry to get notified before the client secret expires. Note that if the client secret expires, the data collection will not happen for your Azure resources.
- Assign and schedule IT automation for your resources so that the remedial actions are kickstarted as soon as there is a breach in the set threshold.

Google Cloud Platform (GCP)

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-discovery and resource termination options to match your elastic scaling cloud setup.
- Setup monitoring at both individual project level and organization levels.
- Monitor Google Compute Engine (GCE), Google App Engine (GAE), Google Kubernetes Engine, VPC, Cloud IAM, Cloud Audit Logging, Cloud SQL, BigQuery, and more.

Services

- Persistent Disk (Disk)
- Cloud Storage (Storage)
- Memorystore (Redis)
- Filestore
- Cloud Functions
- App Engine
- Pub/Sub Topic
- Dataflow
- Cloud Router
- Cloud Load Balancing
- Cloud Networking
- Google Kubernetes Engine
- Cloud Run
- Compute Engine (VM Instance)
- Google Cloud KMS (Key Management Service)
- Google Cloud Certificate Authority Service
- Cloud Spanner
- Firebase Realtime Database
- Cloud SQL
- Cloud VPN
- Cloud DNS
- Cloud Interconnect

- Support to monitor the cloud resources at both project level and organization level.
- Guidance reports to streamline and optimize your cloud resources usage.
- 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.
- Utilize Guidance Reports to ensure your Google Cloud resources are optimally used, safe, and efficient.
- Track events that affect your project, monitor operation logs, system logs, activity logs etc. and know all the actions performed in the GCP console.

4.c. Virtualization monitoring

Automatically discover and map your entire vSphere environment, from data centers to 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.
- VMware Snapshot: The availability of snapshots, the total number of snapshots, the space they occupy, and downtime details.
- VMware Cluster: Effective Storage Capacity, Distributed Resource Scheduler (DRS) Configuration, DRS Faults, DRS Migrations, Total Storage Consumed, VM Operations, Memory Usage, and more in the user's environment.
- 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 hyperconverged 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.
- **Nutanix Storage Container:** Monitor key performance indicators, such as storage capacity, latency, and bandwidth, to gain control over the health and performance of your Nutanix storage containers.

4.d. 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:

- Site24x7 Kubernetes monitoring is supported in the following platforms: Azure Kubernetes Service, Amazon Elastic Kubernetes Service, Google Kubernetes Engine, Red Hat OpenShift, AWS Fargate, Rancher Kubernetes Engine, Digital Ocean, Oracle Kubernetes Engine, MicroK8s, Kind, and K3s.
- 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.
- Get a complete view of your Kubernetes resources by viewing metrics at pod, container, node, daemonset, and replicaset levels.
- Gain a comprehensive view of all your resources with the exclusive cluster, namespace, node, pod, container, deployment, daemonsets, replicasets and statefulsets dashboards.
- Collect and analyze the pod, audit, and event logs in the Kubernetes

environment to spot negligible errors, and avoid node-pod failures and downtime.

- Plan your capacity by using the forecast data for crucial metrics like CPU usage and utilization and memory usage and utilization at all three levels: nodes, pods, and clusters.

4.e. 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 in-depth analytics for the docker host.
- 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.

4.f. Database monitoring

Keep tabs on and enhance the health and efficiency of your database using Site24x7's specialized database monitoring solution. Site24x7 Database Monitoring provides monitoring solutions for Postgres, Amazon RDS for PostgreSQL, Aurora PostgreSQL, MySQL, MySQL NDB Cluster, Amazon RDS for MySQL, Aurora MySQL, Microsoft SQL Server, and Microsoft SQL Insight monitoring.

Highlights:

- Monitor your database availability and delve into its elements for deeper insights.
- Proactively identify issues before they escalate.
- Understand the underlying causes of performance degradation.
- Automate corrective measures for seamless maintenance.

Gain a centralized view of your database's health and ensure the smooth operation of your database environment.

4.g. 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.

4.h. 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 can 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.

5. Network monitoring

Monitor your entire network to ensure the health and performance of your network devices and interfaces. Automatically discover your devices, track and analyze network traffic (NetFlow), and manage device configurations (Network Configuration Manager (NCM)). 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:

- Auto-discovery of network devices, filter out devices while discovering devices in the entire network, discover interfaces based on type and status.
- Supports multiple credentials during device discovery.
- Automatic layer 2 discovery and mapping.
- Support for over 450 vendors and 11,000 device templates, with the option to import global device templates created by other users.
- Custom SNMP monitoring for any device with SNMP support
- Performance counters for monitoring SNMP OIDs and custom SNMP OIDs in scalar, tabular, and table view formats.
- 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.
- SNMP trap monitoring.
- View devices in NOC view, and create topology maps for any devices or groups
- 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.
- Track the connected and rogue access points, analyze the radios, and check the number of access points connected to a single SSID through Cisco WLC monitoring. Assess the quality of WAN links and VoIP call services throughout the call path using Cisco IPSLA-based monitoring.
- Complete visibility into network traffic and bandwidth performance, including in-depth details such as conversations between interfaces. Site24x7 supports different flow technologies like NetFlow, JFlow, sFlow, IPFIX, NetStream, and AppFlow.
- Network Configuration Manager (NCM) helps monitor configuration changes,

compare configuration versions, automate device configuration backups and restore backups as needed.

- Check for firmware vulnerabilities, view categorization (Critical, Important, Moderate, and Low) and check if patch updates are available based on data from National Institute of Standards and Technology (NIST).
- Ensure network configuration compliance by tracking adherence to industry standards like Cisco IOS, SOX, HIPAA, or the PCI DSS and any custom organizational policies.
- Execute commands across multiple devices using configuration templates or configlets. Use variables to define dynamic elements, allowing them to act as input variables and take values based on the execution context.
- Cisco Meraki monitoring via SNMP. Cisco Meraki Map view for devices monitored using REST-API.
- Cisco ACI monitoring via REST-API that can track super spine, spine, and leaf nodes along with endpoint groups and tenants.

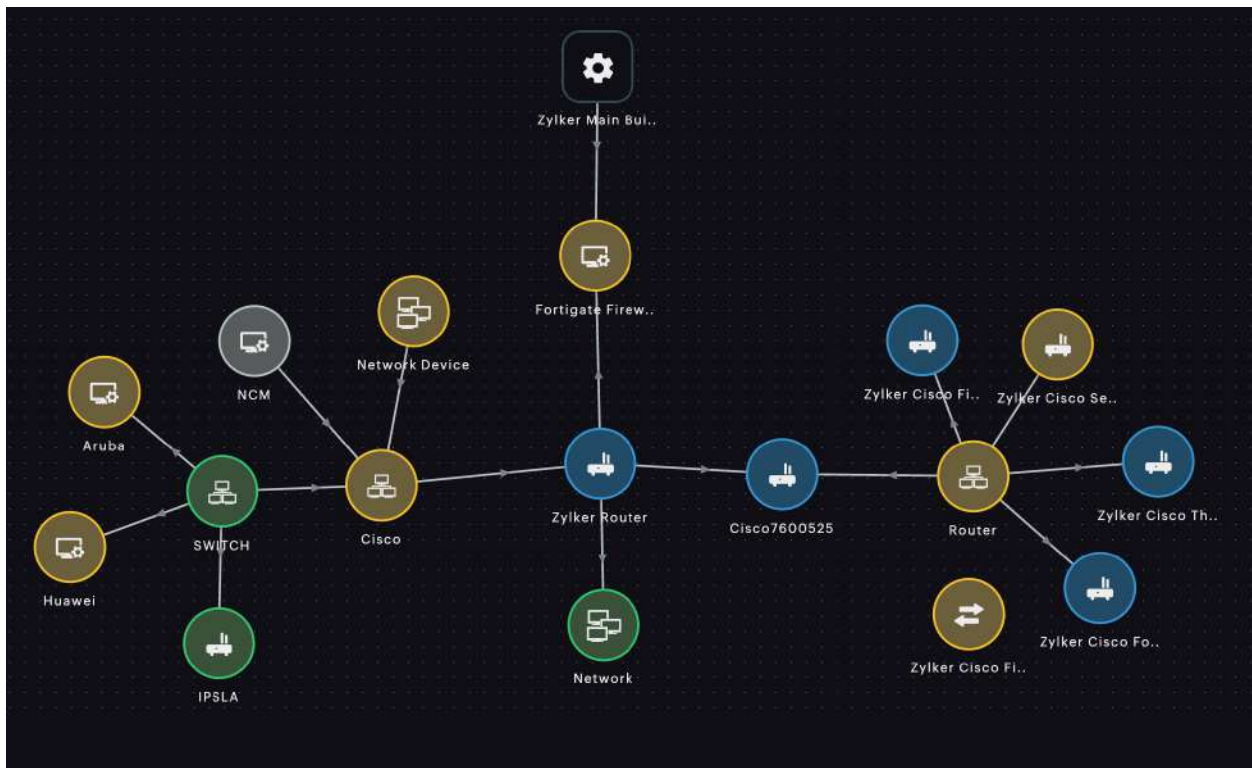


Figure 3: Network Topology Mapper

6. Application performance monitoring and troubleshooting

Site24x7 APM Insight gives DevOps teams complete visibility into application 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 individual web transactions and highlights issues no matter where they originate.

Features:

1. Gives you the complete picture of how your application connects and communicates with external components.
2. Allows you to track and measure important metrics including apdex score, appserver throughput, response time, exceptions and more.
3. Easily identifies slow queries and eliminates potential bottlenecks.
4. Monitors background transactions and captures exceptions at their point of occurrence.
5. Offers a comprehensive view of database operations including database calls and database usage.
6. Tracks custom application components.

6.a. Supported platforms:

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

Requirements:

- The APM Insight Java agent is supported on application servers running Java 1.6 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 5.4 and above.

- Support is provided from Node.js version 4 and above.
- The Python agent is supported on Python 3.5.0 or higher.

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.

Application servers supported: Tomcat, GlassFish, WildFly, WebLogic, Springboot, JIRA, JBoss AS, JBoss EAS, Jetty, WebLogic, WebSphere, AWS Beanstalk and so on.

.NET application monitoring

Site24x7 APM Insight allows you to monitor .NET and .NET Core applications. The .NET agent can monitor slow methods in your 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.

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.

Webservers supported: IIS, Apache2, NGINX or any other FPM based webserver.

Frameworks supported: Codeigniter, CakePHP, Laravel, Drupal, Joomla, WordPress, Magento, Symfony

Databases supported: Redis, Memcache, MySQL drivers, SQLite and PDO based db queries.

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.

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.

Frameworks supported: Express, Koa, Hapi.

Databases supported: MySQL, PostgreSQL, MSSQL, MongoDB, Oracle DB.

Python application monitoring

The APM Insight Python agent allows you to monitor and optimize the performance of your Python application. The agent provides you with information on the response time, throughput, database operations, and errors of your application. You can also keep track of these metrics over time to identify where to optimize them for enhanced performance.

By default, the APM Insight Python agent captures incoming web requests of Web Server Gateway Interface (WSGI)- and Asynchronous Server Gateway Interface (ASGI)-based applications for supported frameworks and modules. For a more detailed analysis, you can utilize the custom instrumentation APIs. This enables you to analyze specific transactions or code blocks in your applications.

Supported frameworks: Bottle, CherryPy, Django, Flask, Pyramid, FastAPI, and Starlette

Supported databases and components: PyMySQL, Psycopg2, Pymemcache, Redis, SQLite, Cassandra, Jinja2, Genshi, Mako, PyMongo, PyMssql, PyODBC, OracleDB, and cx_Oracle

Supported HTTP libraries: http.client, httplib2, httpx, urllib, urllib3 and requests

Supported async libraries: aioredis, aredis, asyncpg, aiomysql

6.b. APM features

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, PHP and Node.js applications.

Milestone marker

Milestone Marker helps you to record significant events like build deployments, product updates, feature enhancements, and infrastructure upgrades.

With milestone marker, you can:

- Mark your infrastructure updates on a timeline.
- Compare your product performance before and after an update.
- View marked updates over a period.

Milestone markers can be created at individual monitor level for website, server or APM monitors.

APM key transactions

You can add business-critical transactions as Key Transactions and track their performance separately. This helps you assess the performance metrics of important transactions at a glance instead of having to search for them in the pool of web transactions. By marking Key Transactions, you can set specific thresholds, receive alerts, and track performance reports for critical transactions.

Licensing: Each Key Transaction is considered a separate, basic monitor, and is charged the price of a basic monitor.

Application dependency maps (Service maps)

Application Dependency Maps give you a complete overview of your application infrastructure along with its connection to other dependent resources.

Application dependency maps can be visualized in the following views.

- Map view
- Graph view
- Tabular view

Thread profiling

Thread profiling enables you to identify and isolate bottlenecks in your code stack. In Site24x7 APM Insight, all thread profiles collected in the chosen time window are listed, along with the thread count, CPU time and memory details. Each thread profile consists of a list of threads that were running when the application was being profiled.

Upon clicking a specific thread profile, one can view:

- High CPU consuming threads, along with its thread ID, CPU time and memory allocated details.
- Time-consuming methods which could potentially affect application's performance.
- Invocation count of every method.

Memory leak detection

Allows you to detect and address memory leaks before they seriously affect your Java application's performance.

The On-Demand Memory Profiling in the Memory Leak Detection tab tracks the collection and identifies potential leaks using a linear regression model. You can also identify the root cause of the leak by tracking the growth of the objects in the collection over a period of time.

Once the On-Demand Memory Profiling process is completed, all objects collected during the specified time are listed along with the associated metrics.

If any of the memory objects has a leak, you can drill down deeper into it by clicking on the respective record to identify the actual cause of the memory leak.

To troubleshoot and prevent similar memory leak issues in the future, you can use:

- **Content inspection:** This tab tells you what data the collection object is holding in the application so that you can begin troubleshooting. It allows you to keep track of the histograms of all the elements in a specific collection.
- **Access tracking:** This tab displays the actual code paths that access the collection object.

Async request tracking

The traces captured in APM Insight provide visibility into how asynchronous

tasks are executed concurrently across your Java application.

We show the following metrics for async calls:

- **Async call status:** Completed, Failed, Cancelled
- **Async thread information:** Thread name, Thread ID, CPU time, Memory allocated
- **Threadpool wait time:** The waiting time of an async task for a new thread assignment
- **Wait time in caller thread:** The waiting time of the main thread for the async job to finish (if `join()` is invoked)

Server integration

APM Insight-Server Monitor 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.

OpenAI observability

Site24x7 offers OpenAI Observability, which gives full visibility into your OpenAI implementation.

Gain valuable insights into your OpenAI usage, perform model-wise cost analysis, log prompts and responses, identify errors, and more—all to track the performance and utilization of your OpenAI implementation in real time.

Note: Currently only applies to Node.js and Python applications.

Node VM (NVM)

Gain insight into useful runtime data for troubleshooting performance issues and monitoring the health of your Node.js application with NVM metrics such as GC Pause Time, GC Pause Frequency, Memory Usage, CPU Utilization, Event Loop Ticks Per Minute, and Max CPU time per tick.

Next.js application

Next.js is a JavaScript framework that optimizes the performance of Node.js applications. It allows you to develop server-side rendered applications and middleware.

With the help of the *APM Insight Next.js package*, the Node.js agent can monitor back-end observability. On the back end, you can monitor the usual application key metrics and Next.js-specific metrics. If you want to monitor the front-end metrics such as web vitals, AJAX calls, and pageviews, you need to inject the RUM script into the header or footer of the index page or a common page of your application or website that you would like to monitor.

6.c. Mobile application monitoring

Site24x7 Mobile APM 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.

Additionally, it assesses mobile vitals, offering valuable insights into the responsiveness, stability, and resource usage of your mobile application. This information helps in pinpointing and prioritizing significant performance issues, allowing for a quick resolution by tracing problems back to their source.

Site24x7 Mobile APM also supports Crash Analytics. You can get a holistic view of crash details like the number of crashes, the devices where the crash occurred, the number of users affected by the crash, and the corresponding app version. You can also compare the percentage of crashes that occurred over a given time period to the number of devices and users that did not crash during that time period.

Mobile APM is available for Android, iOS, React Native, and Flutter applications.

7. Application log management

AppLogs is the 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, MonoLog, Log4net, and NLog, and from over 100 applications including IIS, Apache, Syslogs, Windows event logs, Salesforce logs, Kubernetes audit logs, Elasticsearch slow 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. Using

multiple log pattern support, you can combine different log patterns in a single log type and visualize the data on a single dashboard. You can create a custom parsing rule using derived field support to extract useful information from the log field.

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.

You can use various search and filter options to refine your search results, such as

- Relative time period to search based on relative times such as days, hours, or minutes in the date picker.
- Log type view to build a customized view that helps you focus on the relevant debugging information.
- Related log template to compare multiple fields between two log types.

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

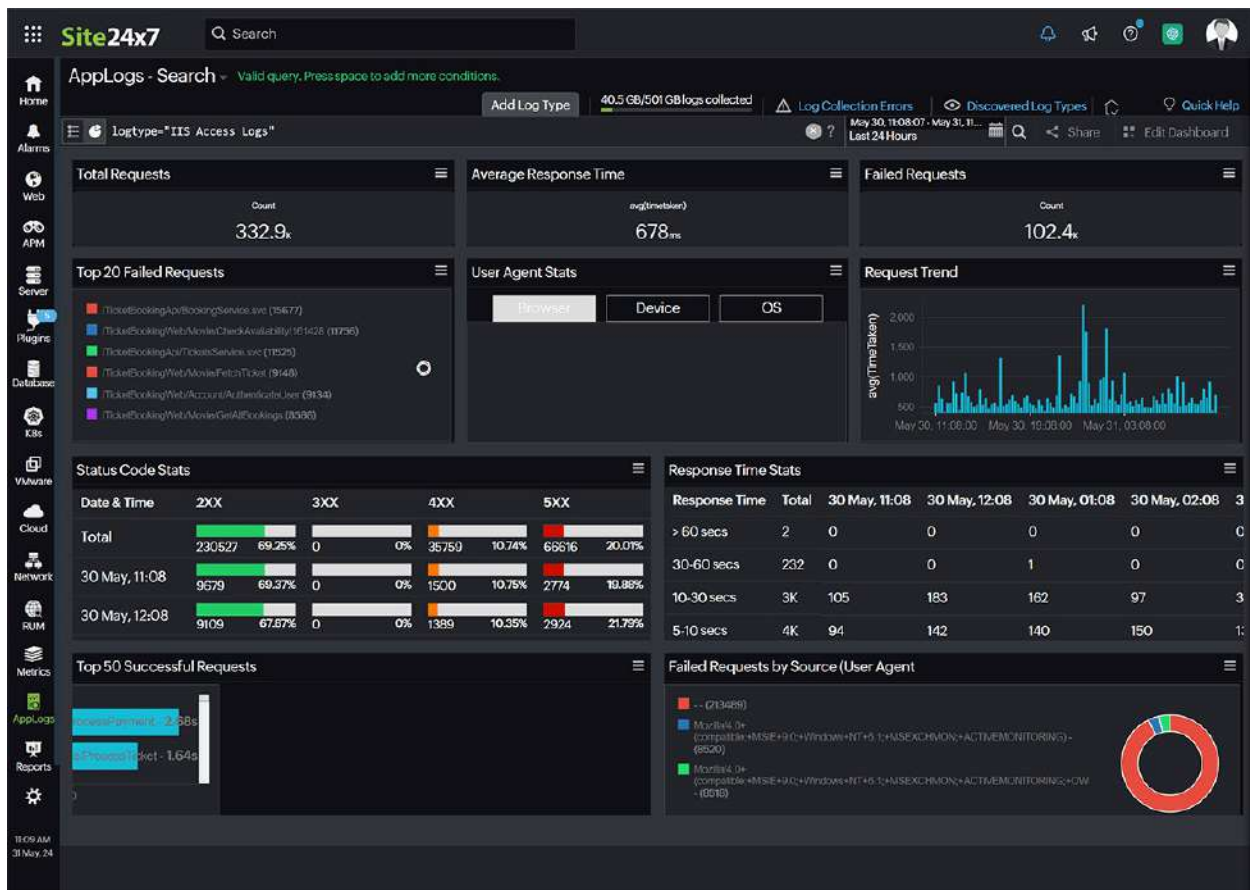


Figure 4: AppLogs - query language search

8. 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, there's no need to install the Windows monitoring agent, 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.

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.

9. Plugin integrations: out-of-the-box monitoring for 100+ apps and custom script monitoring

Network and server administrators often require specific monitoring data that goes beyond the scope of vendors' standard monitoring solutions. Leverage over 100 ready-to-install plugin integrations to monitor applications, hosts, devices, services, protocols, and more. 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 need to install the Site24x7 Windows/Linux Server Monitoring agent to add plugin monitors.

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 duplicating plugin codes with different names and reduce manual effort.

- 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.

10. Metrics

Utilize Site24x7 to view your Prometheus and StatsD metrics with intuitive dashboards and easily comprehensible reports. Integrate Site24x7 Linux server monitoring agent and Prometheus or StatsD to view metrics like Counter, Gauge, and more.

With Site24x7 integration, you can:

- View performance and availability reports
- Auto remediate with IT automation
- Get instant alerts during downtimes
- Easily understand metrics with enhanced visibility

11. Platform features

11.a. 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. Alert contacts can receive alerts but they will not have login access to web client. Set up email, SMS, or Call notifications. You can organize individuals into groups to receive alerts and reports based on their organizational team or department. 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 for adding users and assisting relevant roles. You can quickly respond to incidents and outages round-the-clock by opting to receive alerts during selected shifts via On-Call Schedule.

You can manage the information related to a single user for all three products from

one place Site24x7 for monitoring, StatusIQ for incident communication, and CloudSpend for cloud cost management.

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**. Whoever 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. An admin with monitor-group-level permissions can edit or delete monitors they can access.
- **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:** 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 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 Benchmark Report, Read-Only users need permission to view reports. However, Read-Only users can perform actions like Poll Now, and export and email reports.

11.b. 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 Subgroups up to level five under a main Monitor Group, and visualize all your monitored resources using a Business View. Moreover, you can create reports, perform bulk action or schedule maintenance for your Subgroups.

Capacity planning

You can use the capacity planning feature for analytical data for a group of monitors. With this feature, you can determine the capacity required to optimize resources for a particular operation or workload. This allows you to plan, process, and procure additional resources based on the metrics-related data collected.

Health checks

Site24x7's Health Check feature assesses the availability and health of the Monitor Group or Subgroup and is used to identify any issues or potential problems that could affect the particular operation or workload of the Monitor Group. With the Health Check feature, you can view, analyze, and manage the status of your monitor group along with its availability. Whenever a resource undergoes a status change, you receive a detailed RCA and can analyze the impact at Monitor Group level. The resource status change is instantly propagated to the Monitor Group and gives you a combined alert at Monitor Group level resulting in alert noise reduction.

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.

11.c. Configuration profiles

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

Location profiles

Location Profiles make it easy to set monitoring locations consistently across various monitors such as Internet Services monitors, Network monitors, and VMware monitors. Site24x7 monitors from 120+ locations. 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.

Threshold and availability profiles

Threshold and Availability Profiles help the alerting 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(s) 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. You can use Zia-based threshold

feature to set a threshold value for your resource based on which we detect any unusual aberrations or spikes in resource performance.

Notification profile

Notification Profile helps you configure status-based alerting period and notification medium options for Down/Trouble/Critical notification delays. You can opt to receive alerts at multiple frequencies configured in the persistent alerts section through the third-party services supported in Site24x7 along with email, SMS, voice call, and Site24x7 mobile application push notifications. Moreover, it will provide you with the option to set multiple escalation times, upon crossing which escalation alerts will be raised. Some of the settings in Notification Profile include:

- **Alert configuration** - Configure alert notification modes of your preference. You can also configure the business hours and the status changes for which you would like to receive alerts.
- **Notification delay** - You can use this option to choose to delay receiving alert notifications for Down, Trouble, or Critical status changes for a specific number of polls. If you're not configuring the notification delay, you'll start receiving alert notifications immediately.
- **Persistent alert** - Obtain continuous notifications until you acknowledge the Down/Critical/Trouble alarms with Persistent Alerts. You can receive alerts based on the poll count you've configured in the Notify After Every field.
- **Escalation settings** - Escalation acts as notifications to user alert groups about the monitors that are still down and need to be resolved. You can set more than one escalation time, crossing which an escalation alert will be triggered. You can also opt to trigger an IT automation after the escalation.

Credential profile

Credential Profile is a secure, encrypted 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 across datacenters, 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
- Kubernetes and Docker
- FreeBSD server agent
- MacOS 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
- Nodejs for APM insight
- Python for APM insight,
- .NET core for APM insight
- Cron
- Zapier Integration

11.d. Bulk actions

Bulk Actions in Site24x7 help you perform a particular admin action on multiple monitors at once. 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. Currently, we support 10k monitors at a time. Operations like Append, Overwrite, or Remove can be performed for tags, monitor groups, IT Automation, and user alert groups.

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.

11.e. 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 with editing multiple monitors to associate different monitor groups or adding a different tag can be a tedious process.

11.f. Alerts

Alerting is a crucial aspect of monitoring your infrastructure. Alerts warn you when there is an outage or when the website or service does not meet the required performance standards, which helps you respond quickly to fix the issue. Site24x7 delivers alerts for various status changes such as Up, Down, Trouble, and Critical.

Alerts need to be carefully planned and configured. If alert thresholds are too low, the monitoring team will get alerts too frequently 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 or/and critical alert should be triggered.

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, Site24x7 mobile application or custom Webhooks.

11.g. Anomaly dashboard

Site24x7's AI-powered Anomaly Dashboard detects unusual 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.

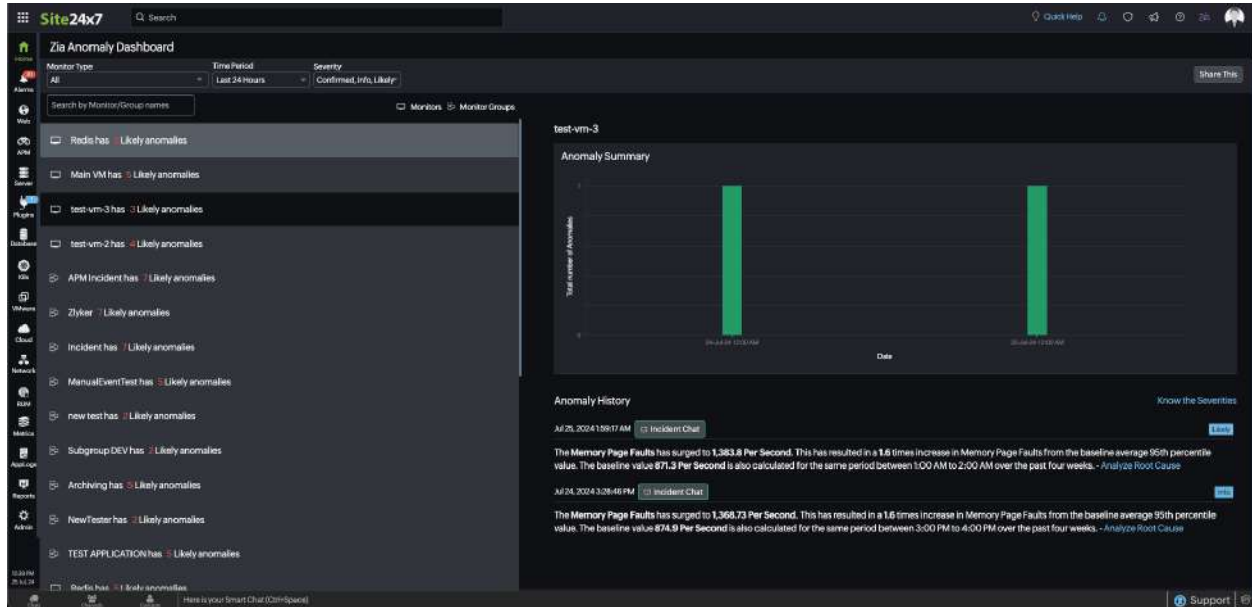


Figure 5: Anomaly dashboard

11.h. IT automation

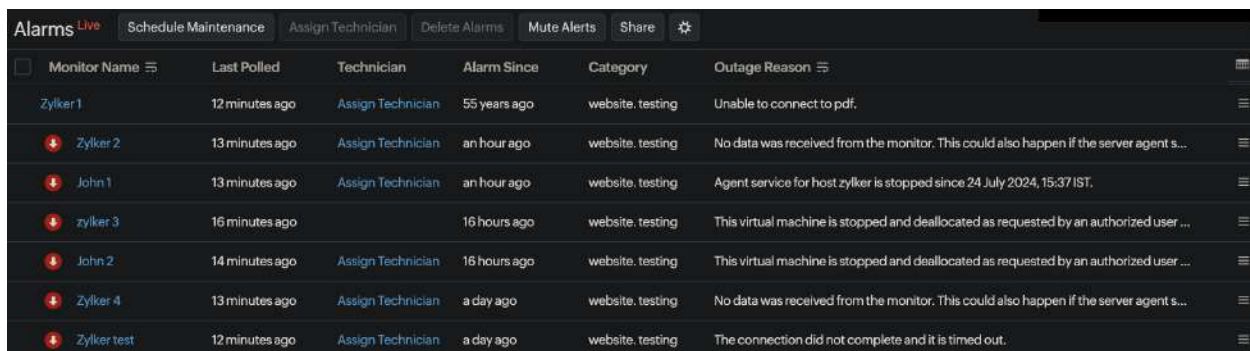
IT process automation reduces downtime from manual processes and human error, leading to faster deployment. In a lot of cases, automation increases efficiency and decreases costs.

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. 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.

11.i. 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 severity. Based on the selected toggle button, e.g. Current Alarms, you can view all monitors that are currently in Down, Trouble, Critical, or Maintenance 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.



Monitor Name	Last Polled	Technician	Alarm Since	Category	Outage Reason
Zylker1	12 minutes ago	Assign Technician	55 years ago	website, testing	Unable to connect to pdf.
Zylker 2	13 minutes ago	Assign Technician	an hour ago	website, testing	No data was received from the monitor. This could also happen if the server agent s...
John1	13 minutes ago	Assign Technician	an hour ago	website, testing	Agent service for host zylker is stopped since 24 July 2024, 15:37 IST.
zylker 3	16 minutes ago		16 hours ago	website, testing	This virtual machine is stopped and deallocated as requested by an authorized user ...
John2	14 minutes ago	Assign Technician	16 hours ago	website, testing	This virtual machine is stopped and deallocated as requested by an authorized user ...
Zylker 4	13 minutes ago	Assign Technician	a day ago	website, testing	No data was received from the monitor. This could also happen if the server agent s...
Zylker test	12 minutes ago	Assign Technician	a day ago	website, testing	The connection did not complete and it is timed out.

Figure 6: 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. You can suppress alerts for a specific set of monitors, monitor groups, or even for all resources in your account.

11.j. Third-party integrations

Site24x7 offers native integrations with diverse collaboration tools.

- IT Service Management (ITSM) tools help with facilitating tasks and work flows such as Webhooks, PagerDuty, ServiceNow, Opsgenie, etc.
- Collaboration tools that streamline communication and creative processes such as Slack, Microsoft Teams, Discord, etc.

- Workflow tools are information tools used to optimize workflow such as Zapier, Amazon Event Bridge, etc.
- Analytics tools are resources that provide for access to information for research and evaluation purposes such as Zoho Analytics.

11.k. Dashboards

Dashboards in Site24x7 are broadly categorized as system dashboards and user-defined 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.

User-defined dashboards

These include Custom Dashboards, Business Views, and Infrastructure Maps. You have to manually create them 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.

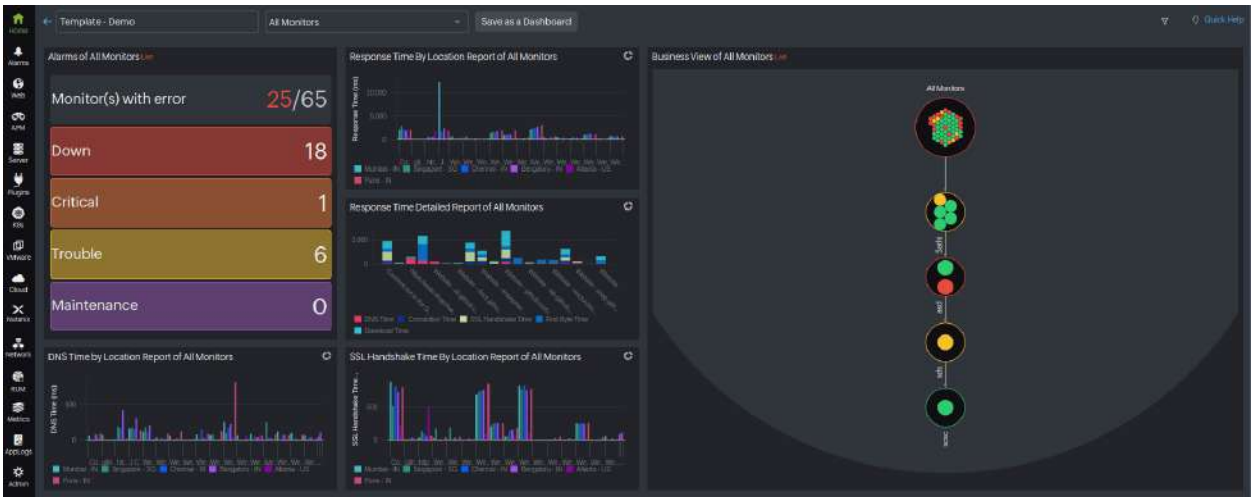


Figure 7: Custom Dashboards

- **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 filter out details about the availability of individual monitors easily, monitor groups, and subgroups. You can automatically build Business Views based on system-generated monitor groups or using default templates provided by Site24x7.

11.1. 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 Bottom 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
- Forecast Report

You can schedule a report or set your report-related configurations by navigating to **Admin > Report Settings** in the Site24x7 web client. Site24x7 offers Site24x7 offers daily, weekly, monthly, or quarterly scheduling options.

11.m. 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 account-level optimization and segregation of resources within teams.
- 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.

11.n. Scheduled maintenance

Schedule a maintenance window to collaborate effectively within your IT team. 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. You can choose monitors, monitor groups, or tags as the resource type. Add a maintenance automation to avoid being

alerted for every log back up. The maintenance period can be scheduled, until which the servers will remain marked as maintenance. This will ensure no false alerts are received until the logs are backed up and the application is rebooted.

12. AIOps

Utilizing Zia-powered AIOps, Site24x7 offers real-time insights, predictive issue identification, and automated resolution to enhance proactive monitoring and ensure optimal IT health and performance.

Anomaly detection

Site24x7's Anomaly Reporting, powered by Artificial Intelligence through the Zia framework, employs sophisticated algorithms such as Robust Principal Component Analysis (RPCA) and Matrix sketching to detect abnormal spikes or deviations in critical performance attributes like response time, CPU usage, and memory utilization. This feature promptly alerts users through detailed dashboards and email notifications, providing insights to fine-tune resource performance and safeguard infrastructure. Leveraging AI, the anomaly engine processes incoming data, generating events based on quantitative and qualitative comparison models. Analyzing data for as little as 7 days, the severity of anomalies is determined through domain scoring, categorizing anomalies as Confirmed, Likely, or Info, aiding in proactive issue resolution and infrastructure optimization.

Additionally, Zia-based threshold profiles dynamically adjust thresholds based on monitor behavior, eliminating the need for static thresholds and enabling immediate notification of anomalies. The Interpret Anomaly Dashboard facilitates easy interpretation of anomaly trends, allowing users to filter anomalies, share reports, and delve into root cause analysis for informed decision-making.

Forecast

Zia-based Forecast is a tool within Site24x7 that leverages advanced analytics and machine learning to provide accurate predictions and insights into monitor performance. Users can customize thresholds for specific attributes, enabling proactive monitoring and alerting for potential breaches. By analyzing historical data, Zia-based Forecast identifies patterns and trends, allowing users to anticipate

issues and take preemptive action. This feature empowers users to optimize resource management and ensure smooth operations through informed decision-making. Zia-based Forecast can be accessed in dashboards, reports, scheduled reports, and public reports, offering flexibility and visibility across monitoring platforms.

13. Mobile and TV apps

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.

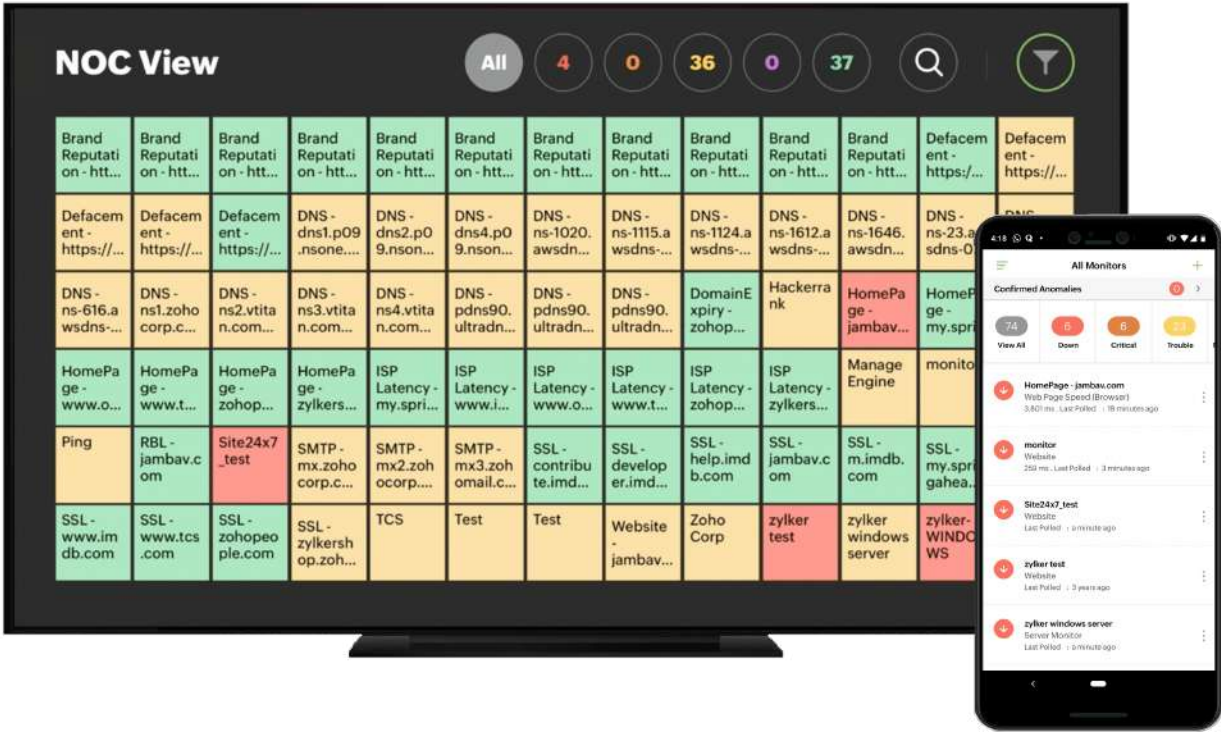


Figure 8: Site24x7 App

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.

Attend to critical issues by viewing them on the big screen when you are away with Android and Apple TV.

14. StatusIQ

StatusIQ is a status tool with which you can communicate to your customers about service downtime details, upcoming scheduled maintenances, your remediation plan, security or privacy breaches etc. with great ease. Customers will receive alerts via SMS, emails, etc. With StatusIQ, you can:

- Add components to represent the status of your service.
- Automate status updates for components using Site24x7, REST API, or via email.
- Create real-time incidents to update your customers.
- Post private notes to communicate with your team.
- Inform your users of any upcoming scheduled maintenance.
- Notify your subscribers about real-time incidents and scheduled maintenance through email or SMS.
- Write postmortem reports for resolved incidents.
- View the timeline of your incident history
- Display the service status to your customers from your websites using status widgets

You can equip your status page by syncing performance data captured via Site24x7 monitoring and publishing the maintenance configured in Site24x7 using your status pages. Additionally, you can post user experience data of your application or webpage via Site24x7 Real User Monitoring (RUM) in StatusIQ. You can obtain region-specific performance of components by integrating the RUM Apex dashboard.

Status page

You can communicate real-time incidents or schedule a maintenance using your status pages. Status pages are mainly used to ensure that users are updated about an incident that has happened or is about to happen. By keeping your users in the

loop, you can provide more transparency during communication.

Components

Components are the functional units of your service or IT infrastructure. For instance, your website, mobile application, APIs, servers, databases, etc., are all components. It is advisable to create a component for every functional or architectural division of your infrastructure. Resources or services used by the end user can be added as components.

The Import Monitors feature can help you import your monitors in bulk from Site24x7 as Components to StatusIQ. This can help reduce the time taken to create multiple components in StatusIQ and associate them to Site24x7 resources. If you own a Basic or Free page you can import 10 components. If you're using a Green plan, you can add up to 50 components.

Components groups

A component group can be formed by grouping similar functional services or resources. Creating a component group can help declutter the status page to give it a more organized and comprehensible look.

The status of a component group will always be the status of the component with the highest severity. Based on severity, component status has the following hierarchy:

- Major Outage
- Partial Outage
- Under Maintenance
- Degraded Performance
- Suspended

You can import Monitor Groups from Site 24x7 as Component Groups to StatusIQ in bulk. Once imported, you can view the monitor groups in the Component Summary section after 5-10 minutes.

Publishing a status page

You can publish your status page on our subdomain (you can also host it on your preferred domain). It can be accessed by clicking on **View Status Page** in your status page. StatusIQ offers you an option to change the time zone of your published status page.

Users can opt to view the data on the status page in their own preferred timezone and language. To configure, click the **Settings** icon on the top right side of your public status page and choose timezone and language. To access these features, the status page should have a Green page license.

Third-party components

Third-party components are services provided by third-party platforms, such as AWS or GCP. The Third-Party Components feature in StatusIQ allows you to add desired third-party services to your status page, helping you view real-time updates on services that are facing downtime.

StatusIQ fetches the status of the third-party components by continuously checking the RSS feed, Atom feed, and JSON APIs of the respective status pages of all the supported third-party services. This is done every five minutes to obtain the real-time status. Based on the status information, StatusIQ will automatically change the status of the corresponding component in your status page.

When the status of a third-party component changes, an email notification will be sent to StatusIQ account users/members with the following roles: StatusIQ Super Admin, StatusIQ Admin, and StatusIQ Spokesperson. To update your subscribers about the status change, add it as an incident on the respective status page and they'll be notified via email or SMS (based on your notification settings).

Customizing a status page

You can customize your status pages to suit your convenience. The following are the changes you can make in your status page.

- **Graphics:** Personalize your status pages with your logo and favicon to reflect

and match your branding.

- **Custom Domain:** You can host status pages on your preferred domains that matches your business units.
- **Customize Email:** Customize the From and Reply-to email addresses for your status page.
- **Customize Colors:** Customize status pages to reflect the colors of your brand.

Customize email notifications

StatusIQ allows you to customize emails sent to your subscribers. This feature is available only for users with a Green status page subscription.

There are two types of customization:

- **Simple customization**

Simple customization also allows you to customize the color of the primary font, the secondary font, the background of the email, button backgrounds, button text colors, and more. The colors you picked in Customize Colors will be reflected in your emails.

- **Advanced customization**

Advanced customization gives you additional control over the changes you can make in your emails. For example, you can modify colors, modify email content, add images, and more. Also, you can rearrange the fields and constants in the email body as desired. To view the complete list of constants, click View Constants. Using constants, you can add new fields to your email content.

Customize HTML and CSS

The Customize HTML and CSS feature in StatusIQ allows users to tailor the appearance and layout of their status pages according to their preferences. Users can access the layout editor to make changes to the custom CSS, custom header HTML, and custom footer HTML. These changes provide flexibility in restructuring

the status page, including modifying the design elements, reordering sections, adding custom headers or footers, and adjusting fonts and colors. The feature offers a live preview of modifications and allows users to publish changes once satisfied. Additionally, users can customize the status from operational to any desired status, reorder components, change banner text, add banner images, and more using provided sample code snippets. This feature is available for users with a Blue plan.

Incident communication

You can create an incident to communicate with your customers in case of an unexpected outage. You can even choose to change the status of the component without creating an incident. As the status of the incident progresses, the status of the components can be changed accordingly.

Creating an incident helps you to communicate details about the health of a component or about any component outages to your users.

Status widgets

You can embed a graphical Status Widget on your website to display the status for your users. This feature is available only for Green Status Page users. The widget types are:

- **Basic:** This widget displays the overall status of your website.
- **Badge:** This widget lets you customize the status label and displays it as a prominent badge on your website.

The Basic and Badge widgets display the overall status of the components in your status page. If multiple components are facing downtime simultaneously, the one with the highest severity will be updated.

- **Sticky:** You can customize the display of this floating widget. You can choose a position on your website to stick the widget and it will stay in position, even when the site is being scrolled. The sticky widget will appear only if there are any active incidents, or any upcoming maintenance. It will be hidden if all components in the status page are operational.

15. 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.
- Forecast your cloud costs and budget values configured in CloudSpend. You can also view a budget forecast comparison of the current month against the budgeted value for your account.
- Monitor your cost account expenses or budget in your preferred currency to understand your spending patterns on a regional basis.
- Group and organize the cloud cost with custom search options leveraged via tags and rightsize your resources.
- Gain in-depth analysis of how your AWS, Azure, or GCP cost account is accruing cloud costs with Resource Explorer. You can group and view your cloud costs by account, region, service, resource group, or tag.
- Gain effective chargebacks in a multi-cloud setup by grouping and understanding cloud costs by different teams, projects, departments, subscriptions, resource groups, services, system-defined, and user-defined tags.
- 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.
- Obtain auto-created reports based on tags such as Region, Service, and Billed accounts for every existing integrated cost account.
- Obtain a granular view of the anomalies in cost detected for your cloud accounts. CloudSpend uses artificial intelligence (AI) to detect anomalies as soon as they occur. It collects and analyzes the cloud cost of the past 180 days to predict any unusual spikes in your cloud costs.
- Gain a comprehensive overview of all active cost accounts in CloudSpend and helps you understand your multi-cloud spending with the Summary Report.

You can set a custom date range, view cloud discounts, and schedule reports for your cost accounts. The Summary Report supports PDF and CSV formats.

ManageEngine CloudSpend mobile app

ManageEngine CloudSpend offers native iOS and Android apps as free supplemental tools to ManageEngine CloudSpend users. With the ManageEngine CloudSpend mobile app, optimize your cloud costs through adopting best practices like implementing chargebacks, reserving capacity, and rightsizing resources on the go.

The apps are so comprehensive that you can quickly access information about your cloud infrastructure, review alerts and notifications, identify and eliminate cloud resource wastage on your multi-cloud environment.

16. Digital Risk Analyzer

The Digital Risk Analyzer offers a robust solution for assessing and bolstering digital security. By analyzing various risk factors within the IT environment, it generates a cyber score for applications, providing users with insights to mitigate potential threats. Users can submit domain URLs for comprehensive scanning, enabling them to evaluate overall website security, including email settings, SSL certificate validity, and defacement risks. With features such as customizable reports, on-demand scans, and notification alerts, users can stay informed of their security posture and take proactive measures to safeguard their digital assets. Digital Risk Analyzer empowers users to identify vulnerabilities, enhance security, and maintain a secure platform in the face of evolving cybersecurity challenges.

Assertions

Assertions in the Digital Risk Analyzer serve as targeted checks to evaluate the security posture of your domain comprehensively. These checks encompass various facets of domain security, including DNS performance and brand reputation, providing users with valuable insights into potential vulnerabilities. By assessing assertions across domains, users can gauge the overall security of their digital assets and identify areas for improvement. The main assertion classifications cover the following areas offering users a structured approach to enhancing their

cybersecurity defenses.

- Domain security
- Email security
- Network security
- Application security

Industry index

The Industry Index feature in Digital Risk Analyzer provides users with insights into their domain's performance relative to others in their industry. Leveraging AI technology, it continuously scans high-traffic domains, categorizes them by industry, and updates benchmark scores regularly. Users can easily access the Industry Index section, select their industry of interest, and view metrics such as top domains and category averages (Domain Security, Email Security, Application Security, and Network Security). This empowers users to benchmark their domain's security, identify areas for improvement, and proactively mitigate risks within their industry landscape.

17. MSP Plan for Managed Service Providers

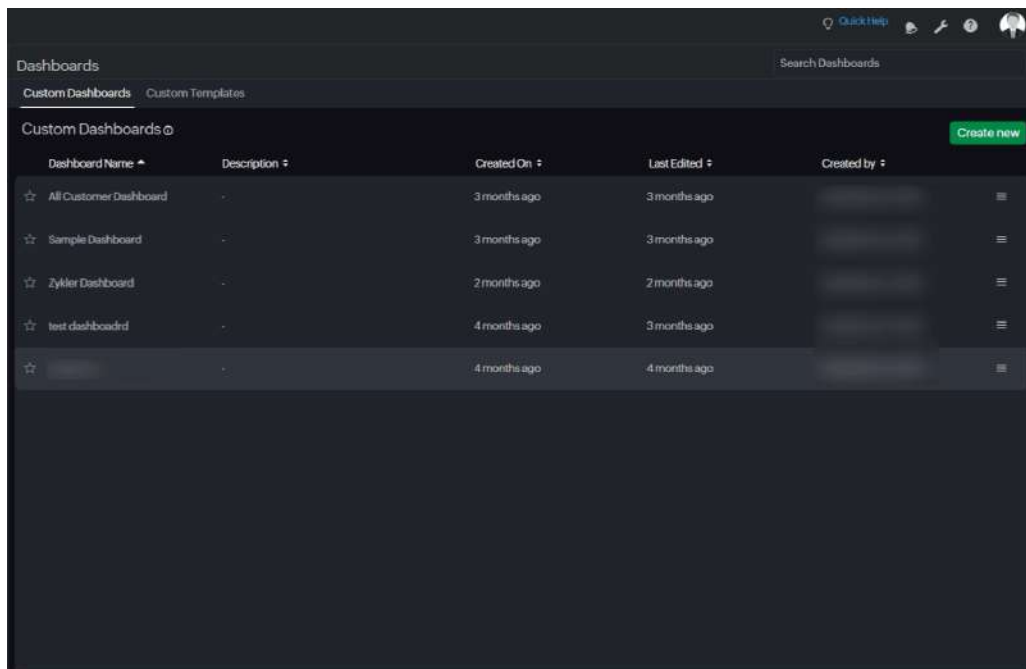


Figure 9: The MSP plan

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
- In-depth reports for admins to view granular details related to the resources of each customer.
- Outage Reports

18. 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.

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)	Microsoft Biztalk
SSL/TLS Certificate Monitor	Microsoft Active Directory
Brand Reputation	Microsoft Failover Clusters
Real-time Blocklist Check	Microsoft SQL
Domain Expiry	Microsoft Hyper-V
REST API Transaction	Microsoft Exchange Servers
POP Server	VMware VDI Horizon
UDP Monitor	ISP Latency Monitor
File Upload Monitor	
gRPC Monitor	
Windows/Linux/FreeBSD/OS X Servers (Agent based)	
Plugin Integrations	
Microsoft IIS	
VMware VM	
VMware ESX/ESXi Host	
VMware Datastore	
VMware Datastore Snapshot	

VMware Cluster	
VMware Resource pool	
Nutanix Cluster	
Nutanix Host	
Nutanix VM	
Nutanix Storage Container	
Cron/Heartbeat	
AWS EC2/RDS/DynamoDB/SNS/ELB instances	

In addition to basic and advanced monitors, Real User Monitoring, AppLogs, Network Monitoring, NetFlow and Network Configuration Manager (NCM) are priced separately in each pack. If the license for any customer pack has been exceeded (e.g. the predefined 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.

19. 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 (Seattle, Dallas)

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

China: www.site24x7.cn (Shanghai, Beijing)

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

Australia: www.site24x7.net.au (Sydney, Melbourne)

Japan: www.site24x7.jp (Tokyo, Osaka)

Canada: customer-sp.site24x7host.ca (Toronto, Montreal)

Saudi Arabia: customer-sp.site24x7host.sa (Riyadh, Jeddah)

To learn more about Site24x7:

Site24x7 Academy: <https://www.site24x7.com/academy.html>

Help docs: <https://www.site24x7.com/help/overview.html>

Knowledge bases: <https://support.site24x7.com/portal/helpcenter/site24x7>

Tutorials: <https://www.site24x7.com/help/tutorials/>

Contact: certifications@site24x7.com