noscito Services

Technical Overview

April 2004

400 Thames Valley Park Drive
Thames Valley Park
Reading
Berkshire
RG6 1PT
T +44(0) 87 0351 5922 F +44(0) 87 0351 5923 www.noscito.com

INTRODUCTION

Noscito offers IT monitoring services delivered over the Internet. These agentless remote monitoring services are managed by a central Noscito portal situated at a secure data centre. This means that these solutions have little impact on the client's infrastructure.

These services are proactive. They alert designated users when there is a potential problem rather than expecting support staff to log on to the monitoring system on a regular basis. No additional hardware, training or installation costs are involved.

This document outlines the two Noscito IT Monitoring services. Noscito REMOTE can monitor the entire IT infrastructure including hardware, operating systems and applications. Noscito USER monitors Websites and Web based applications.

The technical configuration is described in detail including how the system generates user alerts to potential problems and automatic generation of reports.

Noscito REMOTE and Noscito USER are highly customisable so that every client can experience an IT Monitoring service that supports their business needs accurately.

Noscito takes the responsibility for the maintenance and continuity of these services.

SERVICES

Noscito offers flexible monitoring by providing two discrete services. This way the customer only pays for the functionality that adds value to their IT infrastructure.

noscito REMOTE

This is an agent free, system, network and application monitoring service. It enables customers to establish the performance and availability of the IT infrastructure by alerting users to potential problems via Email and/or SMS messages before systems become critical. Noscito REMOTE supports most popular operating system and subsystem environments. No software needs to be installed on the customer's production servers. Easy to use templates enable management parameters to be customised to meet individual customer Service Level Agreements (SLAs). Customers can view how applications are performing and determine whether service level objectives are being met.

noscito USER

This service monitors Websites and Web based applications. It tests the performance and availability of static, dynamic and personalised dynamic Web pages and can verify entire transactions passing through CRM systems, databases, ERP systems and bespoke applications.

All of the monitored elements can be configured with thresholds that the service will adhere to when alerting designated users in the event of a breach by Email and/or SMS messages. It is also possible to configure SLAs for individually monitored components as well as overall availability.

TECHNICAL CONFIGURATION

Noscito monitors "elements". Depending on the service that you select, Noscito is able to monitor hardware, applications and Web transactions.

An infrastructure element refers to any device that is IP addressable.

A Web transaction element monitors the performance and availability of HTTP and HTTPS Web transactions.

Let's look in more detail as to how Noscito services are delivered:

System Integration Portal (SIP)

The SIP is a Web based application that runs on the Noscito portal. This portal is located and managed at a secure data centre.

At the SIP, elements are configured and organised into services. Reports can be viewed and notifications can be set up. The configuration can be crafted by the end user or by a Noscito consultant.

Remote Service Monitor (RSM)

This is a "light" application that collects performance data and relays it to the SIP. The RSM is downloaded from the SIP and installed on the user's network. It must have IP addressability to those infrastructure elements that are monitored. The RSM can also monitor end user applications.

Although not necessary, a customer may choose to install multiple RSMs within the infrastructure. This might be elected for one or more of the following reasons:

- Redundancy. If a box running a RSM goes down, monitoring will not be affected.
- Load balancing. If a large network is being monitored, it might make sense to have more than one RSM.
- Topology. If the monitored network is distributed, it might be appropriate to deploy multiple RSMs.

A Global RSM is a shared RSM that is located outside the customer's network. It is used to monitor WEB sites including page display, path and page times. Noscito's Global RSMs reside in various locations and IP networks for customers' use.

The RSM supports the following remote monitoring protocols:

What is monitored / data collected	Protocol
• MS Windows operating systems • MS Exchange • IIS • MS SQL Server • Other Windows-based solutions	PerfMon
Specific criteria in the Windows application, system and security event logs	WMI (alternative for monitoring Windows event logs)
Unix/Linux operating systems	rstatd, Secure Shell, SNMP
Network devices, operating systems and applications	SNMP
PATROL Knowledge Modules	PATROL protocol
Oracle database Sybase	SQL*Net
Response time and availability of HTTP/HTTPS requests	HTTP/HTTPS
Domain Name System (DNS) Lookup time	DNS
Network connectivity of an element	Ping
Text log files	File system

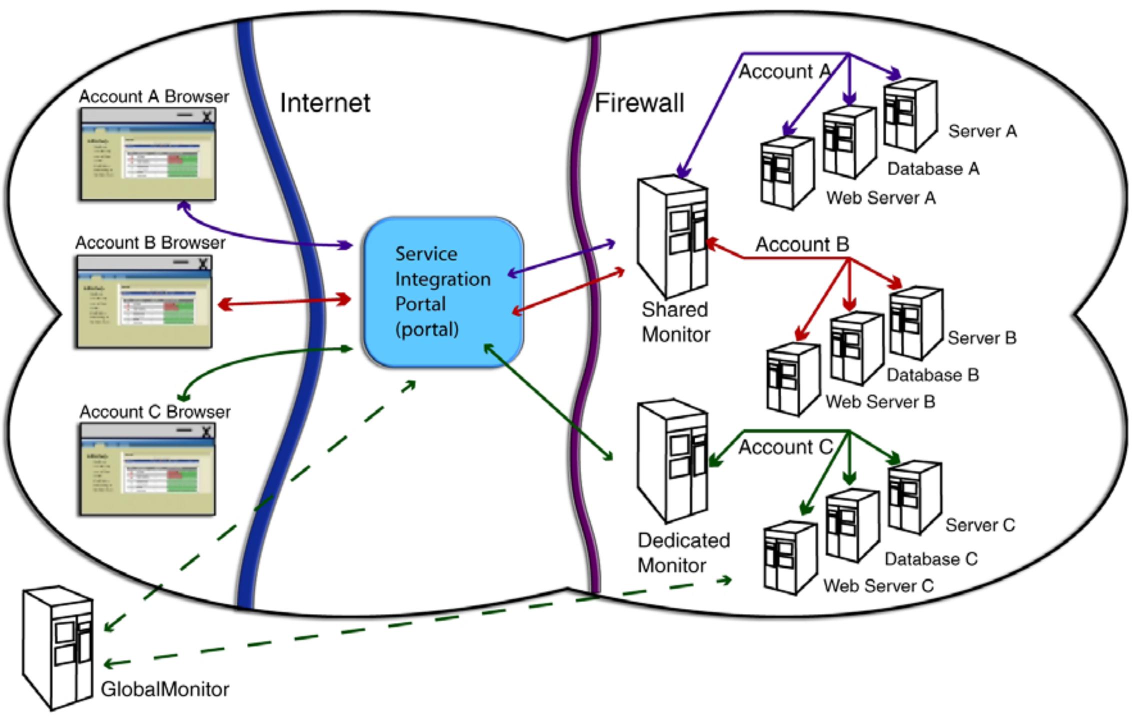
Each RSM can monitor hundreds of elements. Typically the RSM will retrieve parameters from an element once a minute. (This monitoring interval can be customised.) The RSM also has a manager application that sits in the Microsoft Windows system tray. This enables the user to control the RSM and obtain diagnostic and communication information.

Communication between the SIP and RSM

The RSM communicates the following information to the SIP using HTTP and HTTPS:

- Verification of RSM-to-SIP communication. The RSM tries to connect to the SIP every minute to ensure there is a connection between the components.
- Warnings and alerts to the SIP for processing. When the RSM detects a threshold violation, it will immediately send this data to the SIP.
- Parameter data to the SIP for processing service reports. The RSM sends collected performance data at user-defined intervals. These intervals are set at element configuration time (1, 5, 10, 15 or 30 minutes). This data is used for service and history reporting.

The data is compressed and encrypted prior to being sent.



WARNINGS/ ALERTS/ CRITICAL ALERTS

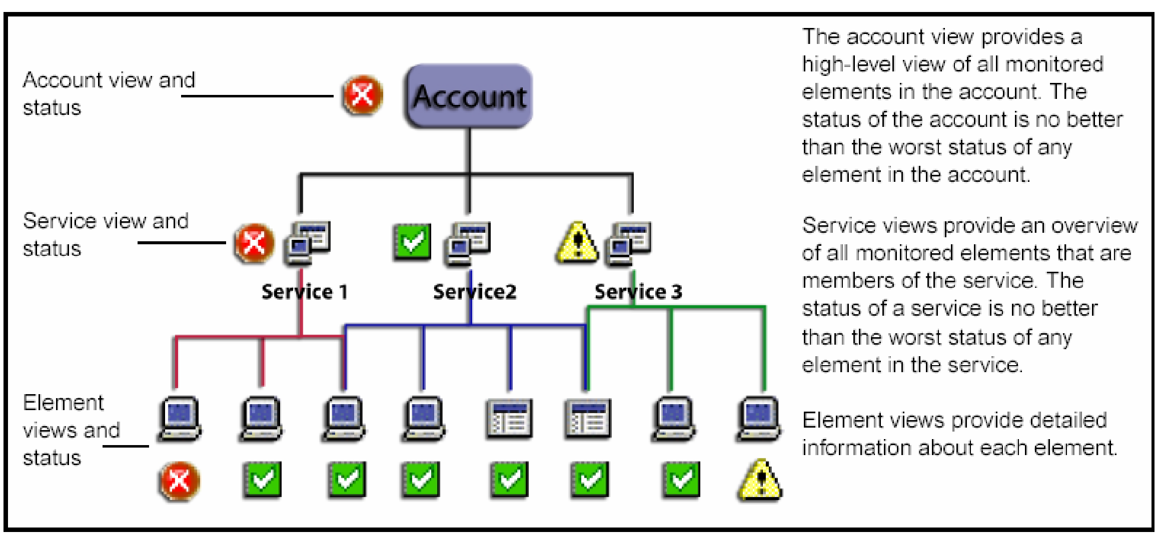
When conditions occur that causes an element to violate an alert rule, the program triggers a notification. The customer determines;

- The type of condition to trigger a notification
- Who receives this notification, delivered via Email and/or SMS messages
- The length of time Noscito waits before sending notification.

An alert rule consists of whom to notify, how to notify them, what elements and services they are responsible for and when to notify them.

The same rules can be applied to all elements in the account. Alternatively, different notification rules for each element or multiple notifications for each element can be implemented. This enables escalation procedures to be set up. For example, a company may want one of the members of its IT department to be notified about a problem immediately. However, if after 30 minutes the alert still occurs, the IT manager would be notified.

For Web transactions, customers can specify the number of locations that must detect an outage before it is considered a critical alarm. For example, customers may create a rule that requires only one location (RSM) to detect an outage before the element is considered in critical alarm. Alternatively, customers may choose to create a rule that requires three or more locations (RSMs) to detect an outage. By allowing this type of flexibility, customers can prevent sporadic network outages at single locations from affecting the overall availability. Additionally, notification rules can be set up to send alerts only when critical alarms are detected. This significantly reduces the likelihood of false alarms.



REPORTS

All of the following reports are customisable. They can be delivered to the designated users at prescribed intervals or requested ad-hoc.

Current Status Views.

These show a quick snapshot of the current services and elements. Possible states include normal, warning, alert and critical alert. These exceptions are rolled up to the account and service level. This allows the user to see if problems exist for the account. For example, if one parameter for one element detects a warning condition, yet the remaining parameters for other elements do not detect any problems, the status view of the service is "warning." Another example is if an element is in critical alert, then the service containing that element will also be in critical alert.

Current status views for the accounts and services have "quick view" graphic bars that display the overall health of the account or service. This enables IT organisations, Service Providers and their customers to see if there are problems and to determine the severity.

Service Measures reports

Service Measures reports show the availability and mean time to repair (MTTR) for accounts, services and elements. Both availability and MTTR are measured against defined service level objectives. Users can select options to compare multiple services and multiple elements in either Availability or MTTR reports.

Infrastructure element reports

The following reports are available:

- Availability. This report shows the percentage of time this element was free of any critical alarms.
- Mean Time To Repair. This report shows the average time a critical alarm has lasted. Timing stops when a critical alarm is fixed or when it drops to a lower alert state such as a warning.

Web transaction element reports

In addition to Availability and MTTR, the following reports can be produced:

- Path Time vs. Goals. This report shows the percentage of time this element's path was completed faster than, or equal to, the defined path-time goal.
- Page Time vs. Goals. This report shows the percentage of time the pages were downloaded faster than, or equal to, the defined page-time goal.
- Diagnostic reports. Information includes; total path time, slowest/ fastest five steps/ page time/ page component (DNS, first byte, resources). This information is shown as averages or for specific locations.

SECURITY

The following security measures have been implemented:

- All traffic, including log on credentials between the SIP and RSM is compressed and encrypted using HTTPS.
- The SIP uses Secure Socket Layer (SSL) IDs that enable the strongest SSL encryption with all versions of Microsoft and Netscape browsers. This SSL is the standard adopted worldwide by online merchants, banks, brokerages, insurers and healthcare organisations.
- Users are required to use passwords when logging onto the SIP.
- IP addresses, user names and passwords of portals and elements are stored encrypted in the SIP database.
- Two firewalls are installed at the Noscito SIP.

IMPLEMENTATION

The customer can elect to customise their Noscito implementation or request the services of Noscito for a nominal charge.

The following steps are executed using a simple graphical user interface:

- Download Remote Service Monitor(s) onto Windows 2000/2003 server(s) within the target infrastructure.
- Create services.
- Create elements. These can be done individually or in blocks.
- Set thresholds for critical warnings, alerts and those elected recipients.
- Set automatic report generation and target recipients.

APPENDIX – SYSTEM CONFIGURATION

RSM System Requirements

Resource	Requirement	Minimum[a]	Recommended[b]
platform	Intel Pentium III or equivalent	• minimum of 128 MB memory dedicated to the RSM • minimum 600-MHz processing speed • minimum 260 MB disk space	• minimum of 512 MB memory dedicated to the RSM • minimum 700-MHz processing speed • minimum 260 MB disk space
operating system	• Windows NT 4.0 (SP6a or later) • Windows 2000 (SP2 or later) • Windows XP		

[a] RSM computer that can monitor 100 Infrastructure *or* 25 Web page elements

[b] RSM computer that can monitor 1000 Infrastructure *or* 250 Web page elements