CASE STUDY

SBA Info Supports a Leading Banking Customer with NagiosXI for Measuring their Availability Across Geography

The Client

Incorporated in 1904, our customer is a 110+ years old Indian bank. They provide a gamut of technical services such as net banking, mobile banking, self-service kiosks, bulk note acceptors, and point of sales. To cater to the needs of a wide range of customers, the bank has a wide offering of savings and deposit products. It also offers many loan products to service the financial needs of small individual customers as well as large industries. They have a strong network of 496 computerized branches and 1292+ ATMs which are spread throughout India.

Business Need

A 3rd party partner was managing our customer's network infrastructure and has their monitoring tool. Our customer faced the below challenges with the 3rd party partner,

1. Most of their leased lines to their branches/ nodal points have an ISDN dialup as a standby. And ISDN will be triggered if the primary link fails.

   One of the key challenges was in finding the actual no. of hours ISDN was 'UP'
2. Only upon request they were able to get the incidents of link failures to branches & their UP status from 3rd party partner
3. Executive monthly reporting was not meeting the management's expectation
4. NOC screen, alerts & escalations were not able to be used efficiently for pinpointing the faulty link
5. Not flexible to add non-network hosts like Windows/ Linux servers

The Solution

After understanding the customer's business requirements. SBA (as an authorized NagiosXI partner) proposed to implement NagiosXI to solve their monitoring challenges.

- The monitoring application was installed on an IBM x3850 server (local RAID protected disk drives) over a centos OS platform
- There was a separate RAID volume for backups where scheduled backups were stored temporarily which will be archived to tape regularly
- Initially, all the routers & core switches (using SNMP v3) were added for monitoring. Later all ATMs were added to be checked for availability
- The various hosts were grouped based on nodal affinities. Also, to take reports & SLA for the ISP lines, like services were grouped together
- Notifications were set to trigger based on alert event thresholds. Also, escalations points were set at scheduled intervals (for failed hosts/ services) to send mail escalations to a specific set of people

During the initial period, 1000+ hosts & 2000+ services were configured (including critical ATMs) and created separate users for the set of services they need to monitor and manage (multi-tenancy).

Tools Used

Nagios XI

Highlights of Nagios

- It provides monitoring of all mission-critical infrastructure components including applications, services, operating systems, network protocols, systems metrics, and network infrastructure. Hundreds of third-party add-ons provide for monitoring of virtually all in-house and external applications, services, and systems
- It uses the powerful Nagios Core 4 monitoring engine to provide users with efficient, scalable monitoring
- With the help of advanced graphs, administrators can easily view network incidents and resolve them before they become major catastrophes
- Automated, integrated trending and capacity planning graphs in Nagios XI allow organizations to plan for upgrades
- Its dashboard provides a customizable high-level overview of hosts, services, and network devices

Results

Our customer was able to reap the benefits of the new monitoring solution within a couple of months after the implementation & fine-tuning phase. They also planned to add Windows/ Linux servers, mail server queues, etc. for monitoring in the future and tag them to the users of the respective services for monitoring/ management.