Project Title: Using Nagios to Monitor Wireless Omnilocks

Submitter's Name: Peter McMillan, ITS UC Santa Cruz
Project Leaders: Peter McMillan, Terry Figel

Summary

Physical security growth over the past four years has been dramatic; a 550% growth increase in the installation of wireless Omnilocks and 450% growth in the installation of door access systems are being supported by 1.75 FTE. Much of this growth is due to units trying to increase their efficiency by eliminating brass key management. The long-term impact is that the ITS PSS group has to maintain additional networking infrastructure and programming to support wireless Omnilocks in over twenty different campus facilities with 1.75FTE.

Wireless Omnilocks use proprietary software to configure and provide information about the status of the locks. On our campus, ITS Physical Security Systems team manages the application environment and works with the campus lock shop and clients to achieve optimum results. The campus lock shop has the responsibility for replacing batteries and performing initial installations. Monitoring the locks for battery levels and other operational issues is the responsibility of a local facilities security coordinator (FSC).

Project Description

Problem Definition

Information Technology Services has been spending its limited resources to help monitor the health of the locks across the campus. Our project is to leverage our experience with using the Nagios monitoring software to monitor the health of the locks across campus and provide alert messaging that can reduce the risk of a lock failure due to low battery voltage. When batteries fail, access to Omnilock doors is impacted for students, faculty and staff and life-safety personnel.

Prior to this project our process was to rely upon the FSC to perform daily checks of the batteries in their facilities. Upon detecting a low battery situation, the FSC is to create a Campus Facilities work order to the lock shop for battery replacement.

Project Goals

Our goal was to investigate using the open source product Nagios and expertise in the School of Engineering to help develop a solution for monitoring the health of the Omnilocks; provide web-based reports and email alerts to the stakeholders in a proactive manner. Beyond these initial goals, we hope to use the data to develop and track metrics to help us position our resources more efficiently. Upon successful testing, we would seek to utilize the School of Engineering's Nagios implementation to run this service.

Our Approach

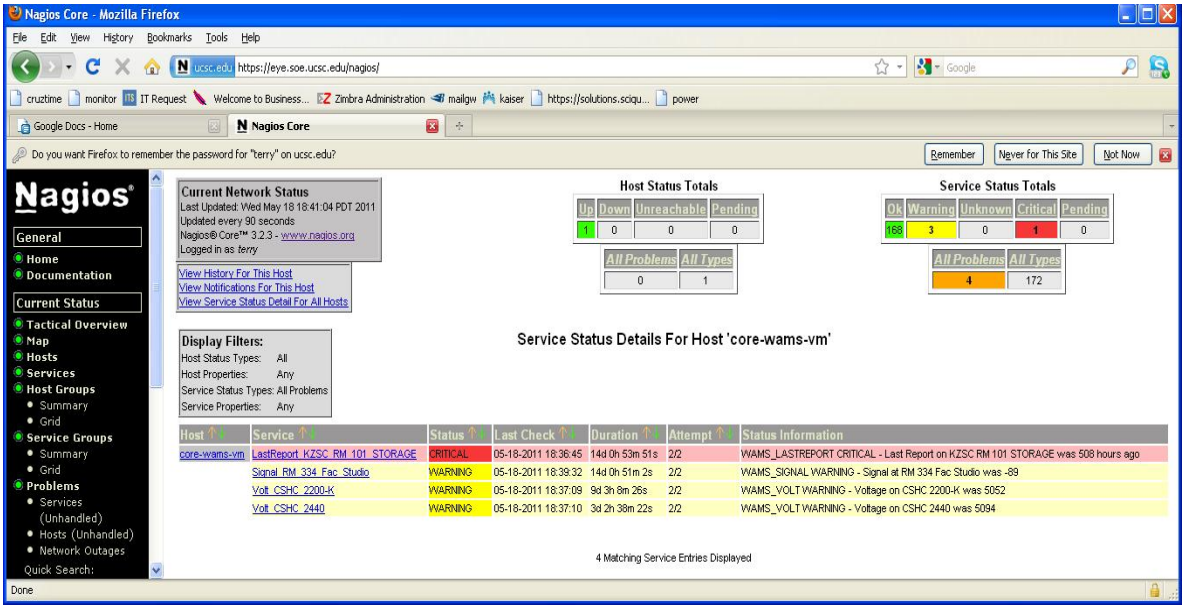
We solicited some help from our ITS staff in School of Engineering to see if they could make Nagios talk to wireless Omnilocks. Originally we were attempting to see if we could use SNMP to talk directly to the locks or the WAPS. When that was not an option we looked at both the web and telnet interfaces for the WAP, but were disappointed by the reporting capabilities on those interfaces. What we found was that we could create a SQL query to run as a scheduled job on the server that manages the WAPS. The output of the SQL query can be fed to Nagios. Nagios can interpret the data and based on thresholds generate appropriate alerts.

We created 3 separate tests in the nagios server, that parse the output from the Database:
1.) Battery life
2.) Signal strength
3.) Last report date

The initial roll out was done in School of Engineering on the facilites omnilock server, and then copied to the central server. As part of the process of familiarizing ourselves with the database behind the WAPS, we were able to write other scripts to help migrate the collection of campus omnilock servers onto the central VM.

We are still trying to narrow down the correct parameters of when to alarm on each of those criteria. Currently when one of the monitors hit the critical point, we alert the ITS team. The end goal will be to alert the facilities managers directly, and possibly the lockshop.
This allows ITS to provide a tool to help our clients(facilities managers) save time, without transferring a workload onto ITS staff.

Nagios has built in reporting features to see long term statistics on the services it monitors.



Success Criteria

We measure the success of this project by the number of batteries that are replaced prior to failure. We further measure the effectiveness of the solution through the automation of creating

Campus Facilities work orders via automated email that also alert the client and the ITS PSS team. In addition, the ability to gather data and plot it will provide additional decision making data for ITS Physical Security Systems group, individual Facilities Security Coordinators, University Police, students, faculty and staff.

Currently we are monitoring 47 locks in School of Engineering and 58 locks for the rest of campus. As we consolidate all of the servers into the central VM that number will grow considerably.

Technology Utilized

The wireless Omnilock product utilizes a product called Wireless Access Management System (WAMS) and runs in our virtual environment. This server software communicates with wireless access points that are referred to as Portal Gateways. Portal Gateways communicate with lock mechanisms. Data entered at the server is pushed to the Portal Gateway and out to the individual locks.

Our Nagios service is hosted and sponsored with the School of Engineering and runs in a Virtualized jail environment on FreeBsd.

Timeframe of Implementation

We were able to refine the problem and prototype a solution in Spring Quarter 2011.

Objective Customer Satisfaction

The Field Operations technicians and NOC analysts have been plagued with the thought (and reality) of being locked out of critical telecommunications closets. One of the worries is the possible failure of the battery powered locks currently used in some of these areas. Great job Terry and Peter. Geoff