Table of Contents

Safety System Monitoring

SSM stands for Safety System Monitoring. See Monitoring Systems for a complete description. **===Introduction===** Today the Safety System Monitoring (SSM) is An integrated system for monitoring all safety and access systems of GS/ASE in a coherent and reliable manner: LACS, SUSI, CSAM, SIP, etc. All the functionalities and definitions can be found in the EDMS: 1099499.

The aim of this project is research and test different software and architectures in order to improve the present system.

Any Monitoring System must be capable of monitoring hundred of servers and thousands of services. It must also be easy to deploy with as much automation as possible, such that new servers can be provisioned and added to the monitoring pool with little administrative overhead and the capability of scripting changes and commands to the server.

===Monitoring Systems=== Presently there is hundred of Monitoring System in the market. Open-source and Proprietary software. There is Windows and Linux based, with and without database support, etc. A complete list can be found here: http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems

Basically a monitoring system describes the use of a system that constantly monitors computers, PLC's, UTL's, etc. looking for slow or falling components and that notifies the maintenance team in case of outages. The system has to be able to give enough information and tools to the maintenance team to repair the system before that becomes critical for the normal operations.

The 3 systems that are going to be evaluated are: **Nagios, Zabbix and Zenoss**. All three are open-source software and have a global recognition in the monitoring community with regular updates and several plug-ins for the different networks and hardware equipment.

===Purpose of the evaluation=== We will evaluate the three systems based on the following criteria: - Ability to scale to hundreds of host checks and thousands of service checks . - Ease of importing host and service checks from a script. - Ease of modifying a configuration or scheduled checks, particularly the ability to do mass changes to many nodes at once . - API which can be accessed via a command line . - Ability to do distributed checks from multiple monitoring servers. - Reporting capabilities . - Ability to create Snow tickets for critical alerts . - Industry acceptance, availability of expertise, and community support - Ability to schedule planned maintenance periods and store work comments for hosts - Ability to create graphics for ease and quick localisation of problems.

===Methodology=== ==Hardware== The hardware foreseen for the test is a HP ProLiant DL300 Server that is a versatile and general-purpose 1- 2 processor rack mount server. It's perfect for enterprise data center and sophisticated SMB environments, database applications, and front-end network applications.

The server will be installed in the 212-2 building in a space dedicated.

Will be provided with 2 Ethernet cards in order to connect the GP Network and the TS network. **==Hypervisor Software==** To be able to test in parallel all the systems and allow easy and quick software installations, Vmware will be installed on the server. VMware software provides a completely virtualised set of hardware to the guest operating system. Vmware software virtualises the hardware for a video adapter, a network adapter, and hard disk adapters. The host provides pass-through drivers for guest USB, serial, and parallel devices.

In this way, VMware virtual machines become highly portable between computers, because every host looks nearly identical to the guest. In practice, a system administrator can pause operations on a virtual machine guest, move or copy that guest to another physical computer, and there resume execution exactly at the point

of suspension. **==Monitoring Software==** Nagios, Zabbix and Zenoss will be installed in 3 virtual machines with the operating system required. The 3 systems need additional plug-ins to performs the checks. Some of them need databases support that will be installed in the server. **==Equipment to survey==** Mainly the clients will be Windows machines, PLC's, UTL's and Linux machines. Some equipment from each subsystem will be selected for the test. The systems to check are CSAM, LACS, LASS, SIP, SPS and the PS. **===Conclusions===** At the end of the tests a rapport will be written with the pros and cons of each system and will be presented a planning for the deployment of a new version of the SSM. **===Documents==** * {{:ssm_update_report.odt|Original Document SSM}} * {{:ssm_update_report.pdf|Pdf}}

This topic: SSM > WebHome
Topic revision: r6 - 2018-02-08 - TonoRiesco

Copyright &© 2008-2024 by the contributing authors. All material on this collaboration platform is the property of the contributing authors.
or Ideas, requests, problems regarding TWiki? use Discourse or Send feedback