Simple Event Management Protocol (SEMP) and Event Management Protocol for Cloud Computing. SEMP is used in event management systems to monitor cloud computing networks, internet and mobile networks for autonomics (self-healing), corrective actions, and notification. It consists of a set of standards for event management, including an application layer protocol, a database schema, and a set of event based properties.

SEMP delivers management data in the form of properties on the managed systems, networks, applications, transactions and databases, which describe the system configuration. These properties can then be requested by management applications through SOAP (Simple Object Access Protocol) or REST.

Overview and basic concepts

In most cases SEMP (Simple Event Management Protocol) there are many servers, applications, cloud computing environments, utility computing services and mobile devices that require the correlation of events as well as the autonomics of the components. SEMP events are sent from components to a SEMP server located in most cases on the internet for event management. For example, a cloud computing Unix server instance submits a SEMP event to a utility computing service for correlation and autonomics of the situation for the correct response.

Protocol Details

The properties available via SEMP (Simple Event Management Protocol) are definitive for the purpose of usability of high count infrastructure components distributed across information system networks, cloud computing networks and mobile networks. The properties are description, group, time, source, sub source, severity, location, IP and status. An example for a semp event is included below.

"description", => error codes

"group", => network, application, systems

"IP", => 172.29.131.5

"location", => cloud/subnet/datacenter

"severity", => 1,2,3,4,5

"source", => esm system, application, ...

"subsource", => transactions

"time", => unixtimestamp

"status", => open/closed/archived/pending

The description typically includes error codes to process event management correctly. A description with the error code helps to pin point what the problem is and how to resolve the incident. HTTP 404 is the return code for not found indicating that the client was unable to communicate to the server based on what was requested.

The group defines which category the event is referring to. A group summarizes and categorizes for a logical separation of events. Examples for the group property can be network, application, database, system and transaction.

The IP specifies the host address located on a network also including networks for cloud computing, IT networks and mobile networks. An address enables a corrective action to be taken since the monitoring server can determine what component is submitting requests. An example for an IP is 172.29.131.5.

The location specifies the host location across cloud computing networks, IT networks and

mobile networks. A location enables a corrective action to be taken since the monitoring server can determine what component from which location is submitting requests. An example for an location is Cloud EC2, Data Center San Jose or Subnet 71.