MYSURVEILLANCE

Installation Manual

Version 1.1

OPEN SOURCE COMPETENCY CENTRE (OSCC) MAMPU

Level 3, APT E302-E304
Enterprise Building, Persiaran APEC
63000 Cyberjaya
Selangor
Tel: (6)03-8319 1200
Fax: (6)03-8319 3206
E-mail: helpdesk@oscc.org.my
http://opensource.mampu.gov.my

Table of Contents

INTRODUCTION

MySurveillance is a security monitoring system application that collects and analyzes security reports from all network devices and system applications such as firewalls, databases, web servers and switches. MySurveillance client-server architecture helps organizations/individuals to monitor all security alerts for devices or applications from a central (MySurveillance server).

Each client that need to be monitored will be installed with a MySurveillance sensor which will collect the security event logs and Intrusion Detection Message Exchange Format (IDMEF) will translate the log to a common language using IDMEF before sending it to the MySurveillance server for analysis. Report of all security events will be displayed at the MySurveillance Console.

Complex and large organizations such as governmental agencies benefit from the flexibility that MySurveillance offers them. In Addition to being compatible with all security systems in the market, there are different configuration variations that are possible with MySurveillance such as filtering system and sensor error detection system with status reporting.

OBJECTIVES

The resources and features available in the MySurveillance would allow the Public Sector agencies to achieve the following objectives:

- To collect and analyze security event logs from various network and system devices.
- To centrally monitor overall network and system security.
- To identify critical security events rapidly and effectively.

FEATURES

Features available in MySurveillance are:

- Able to support log files generated by various devices and applications available in the market.
- Real-time analysis of events received from MySurveillance Sensor.
- Built-in event log filter enables only critical and error messages to be displayed at central server.
- Data can be collected and corellated from sensors deployed on supported devices.

ARCHITECTURE

There are four major components in MySurveillance which are ***MySurveillance Sensors/Agents***, ***MySurveillance Server***, ***MySuveillance Data Store*** and ***MySurveillance Console***.

- ***Sensors/Agents*** at the client-server (prelude-lml) are responsible for intrusion detection, and report events in a centralized fashion using a Transport Layer Security (TLS)
- All the report of security events will be collect and analyze at ***MySurveillance Server*** (prelude-manager).
- MySurveillance uses Intrusion Detection Message Exchange Format (IDMEF) as the common language for reporting events. The server can then process these events and deliver them to a ***MySurveillance Data Store***.
- The ***MySurveillance Console*** can then be used to view these events log reading the information from the MySurveillance Data Store.

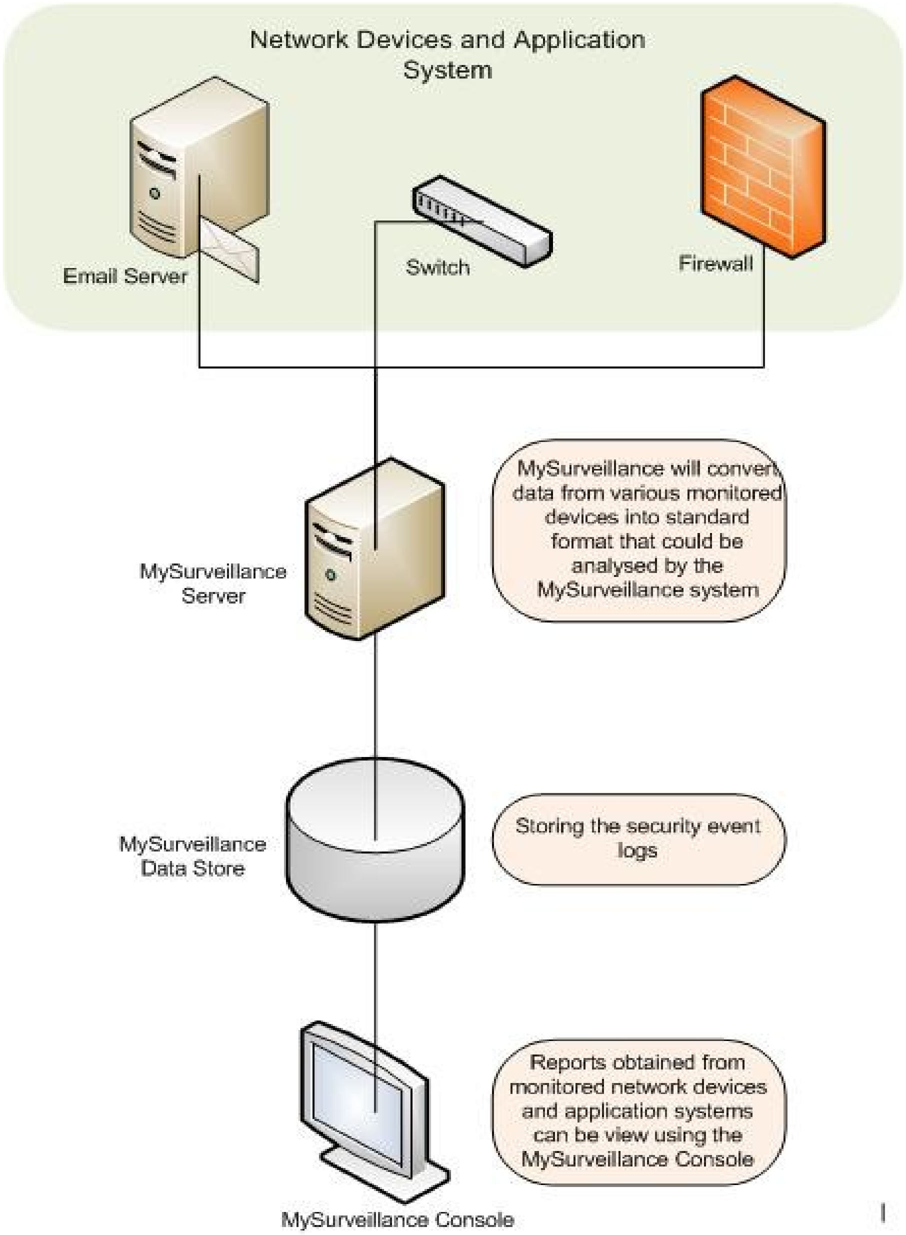
Network Devices and Application System
Email Server
Switch
Firewall
MySurveillance Server
MySurveillance will convert data from various monitored devices into standard format that could be analysed by the MySurveillance system
MySurveillance Data Store
Storing the security event logs
Reports obtained from monitored network devices and application systems can be view using the MySurveillance Console
MySurveillance Console

Figure 4.1 : Architecture Diagram

MySurveillance is compatible with various network and system devices in the market regardless whether it is proprietary or open source. Below are some examples of MySurveillance logs compatibility with various network and system devices.

Firewall, Routers & VPN	BIG-IP®, Check Point®, CISCO® ASA, CISCO® IOS, CISCO® Router, CISCO® VPN, D-Link®, Ipchains, IpFw, Juniper Networks® NetScreen, Linksys® WAP11, ModSecurity®, Netfilter, SonicGuard SonicWall®
Switchs	CISCO® CSS
IDS	CISCO® IPS, Portsentry, Shadow, Tripwire®
Monitoring	APC®-EMU, ArpWatch, Dell® OpenManage, Nagios®
AntiVirus/AntiSpam	ClamAV®, P3Scan, SpamAssassin
Database	Microsoft® SQL Server, Oracle®
SMTP/POP Server	Exim, Postfix®, Qpopper®, Sendmail®, Vpopmail
FTP Server	ProFTPD, WU-FTPD
Web Server	Apache®
Vulnerability Scanner	Nessus®
Honeypots	Honeyd, Honeytrap, Kojoney
Authentication	OpenSSH
Applications	Asterisk, Cacti, Libsafe, Shadow Utils, Squid, Sudo
OS (security tools)	GrSecurity, PaX, SELinux
Miscellaneous	Unix® specific logs, Webmin, Windows® Server, Arbor, Linux® bonding, Microsoft® Cluster Service, NetApp® ONTAP®, NTSyslog, OpenHostAPD, Rishi, Suhosin

Table 4.1 : Logs Compatibility

SYSTEM REQUIREMENT

Below are the minimum requirements needed to install MySurveillance:

Hardware

- **Model**: Pentium IV
- **Memory**: 512MB RAM
- **Storage**: 20GB HD
- **Network Interface Card**: 1 or 2

Software

- **Operating System**: CentOS 5
- **Web Server** : Apache
- **Database** : Mysql

DEPENDENCIES

MySurveillance-server

```
================================================================
Package                  Arch        Version            Repository        Size
==================================================================
Installing:
 mysurveillance-server   i386        1.1-1.oscc         oscc-repo         2.2 k
Installing for dependencies:
 libprelude              i386        0.9.17.2-1         oscc-repo         985 k
 libprelude-python       i386        0.9.17.2-1         oscc-repo         520 k
 libpreludedb            i386        0.9.14.1-1         oscc-repo         196 k
 libpreludedb-mysql      i386        0.9.14.1-1         oscc-repo         28 k
 libpreludedb-python     i386        0.9.14.1-1         oscc-repo         90 k
 mysurveillance-client   i386        1.0-2.oscc         oscc-repo         1.9 k
 oscc-bayesian           noarch      0.0.2-4.oscc       oscc-repo         2.2 M
 oscc-tracking           noarch      0.0.2-1.oscc       oscc-repo         29 k
 perl-Archive-Tar        noarch      1.30-1.fc6         base              47 k
 perl-Compress-Zlib      i386        1.42-1.fc6         base              52 k
 perl-Digest-HMAC        noarch      1.01-15            base              12 k
 perl-Digest-SHA1        i386        2.11-1.2.1         base              48 k
 perl-HTML-Parser        i386        3.56-1             oscc-repo         124 k
 perl-IO-Socket-INET6    noarch      2.51-2.fc6         base              13 k
 perl-IO-Socket-SSL      noarch      1.07-2.el5.rf      oscc-repo         43 k
 perl-IO-Zlib            noarch      1.04-4.2.1         base              15 k
 perl-Net-DNS            i386        0.61-1.el5.rf      oscc-repo         276 k
 perl-Net-Daemon         noarch      0.43-1             oscc-repo         44 k
 perl-Net-IP            noarch    1.25-2.fc6          base         31 k
 perl-Net-SSLeay        i386      1.30-4.fc6          base         195 k
 perl-Socket6           i386      0.19-3.fc6          base         22 k
 perl-libwww-perl       noarch    5.805-1.1.1         base         376 k
 prelude-lml            i386      0.9.12.2-5          oscc-repo    187 k
 prelude-manager        i386      0.9.12.1-1          oscc-repo    192 k
 prewikka               noarch    0.9.14-1            oscc-repo    420 k
 python-cheetah         i386    2.0-0.1.rc8.el5.rf    oscc-repo    423 k
 spamassassin           i386      3.2.4-1.el5         base         1.0 M
```

MySurveillance-client

```
==================================================================Pac
kage                    Arch      Version             Repository   Size
==================================================================
Installing:
 mysurveillance-client  i386      1.0-2.oscc          oscc-repo    1.9 k
Installing for dependencies:
 libprelude             i386      0.9.17.2-1          oscc-repo    985 k
 oscc-tracking          noarch    0.0.2-1.oscc        oscc-repo    29 k
 prelude-lml            i386      0.9.12.2-5          oscc-repo    187 k
```

OSS TECHNOLOGIES

CentOS 5

CentOS is an Enterprise class Linux Distribution derived from sources freely provided to the public by a prominent North American Enterprise Linux vendor. CentOS is perfect for servers and cluster nodes where newer software is not a requirement. CentOS preferred software updating tool is based on yum, although support for use of an uptodate variant exist. Each may be used to download and install both additional packages and their dependencies, and also to obtain and apply periodic and special (security) updates from repositories on the CentOS Mirror Network.

This following steps show how to install CentOS 5.

1. Place the DVD/CDROM in your DVD/CDROM drive and boot your system from the DVD/CDROM. If the DVD/CDROM drive is found and the driver loaded, the installer will present you with the option to perform a media check on the DVD/CDROM. This will take some time, and you may option to skip over this step.
2. Welcome screen will be appear and click 'Next' to proceed.
3. Language selection Select the language and it will become the default language for the operating system once it is installed. Selecting the appropriate language also helps target your timezone configuration later in the installation. The installation program tries to define the appropriate time zone based on what you specify on this screen. Once you select the appropriate language, click 'Next' to continue.
4. Keyboard Layout Selection Select the correct layout type for the keyboard you would prefer to use for the installation and as the system default. Click 'Next' to continue installation.

5. Setup your disk partitioning, the first three option will perform automatic partitioning while 'Create customs layout' will perform manual partition.
6. For Network configuration, the installation program will automatically detects any network devices and its hostname. You can edit its configuration or just click 'Next' to continue.
7. Set your time zone by selecting the city closest to your computer's physical location. Select 'System Clock uses UTC' if your system is set to UTC.
8. Set root password. This is the most important steps because root account is used for system administration.
9. You can customize software selection of your system or do it after installation.
10. A screen preparing the installation will be appear. For your reference, a complete log of your installation can be found in /root/install.log once you reboot your system.
11. This step is when the installation program installing all the packages. How quickly this happens depends on the number of packages you have selected and your computer's speed.
12. Now your installation is complete. The installation program prompts you to prepare your system for reboot.
13. Then, start your CentOS Linux system in run level 5 (graphical run level), the Setup Agent is presented, which guides you through the CentOS Linux configuration. Using this tool, you can set up your system time and date, install software and more.

For more info about CentOS, check website at http://www.centos.org/

Apache HTTP Server (MySurveillance Web Console)

The Apache HTTP Server is the most popular Open Source and widely used web server in the world. The Apache HTTP server is known to be a stable and extensible server.

MySQL (MySurveillance Data Storage)

MySQL is a very popular and widely used Open Source database that is known for its robustness and ease of use. Some features available are multiple storage, query caching, Secure Sockets Layer (SSL) support and many more.

Prelude-manager

Prelude Manager is the main program of MySurveillance system. It is a multithreaded server which handles connections from the MySurveillance sensors. It is able to register local or remote sensors, enable the operator to configure them remotely, receive and store alerts in a database or any format supported by reporting plugins, thus providing centralized logging and analysis. It also provides relaying capabilities for failover and replication. The Intrusion Detection Message Exchange Format (IDMEF) standard is used for alert representation. Support for filtering plugins allows you to hook in different places in the Manager to define custom criteria for alert relaying and logging.

Prelude-lml

The Prelude Log Monitoring Lackey (LML) is the host-based sensor program component. It can act as a centralized log collector for local or remote systems. It can run as a network server listening on a syslog port or analyze log files. It supports logfiles in the Berkeley Software Distribution (BSD) syslog format and is able to analyze any logfile by using the Perl Compatible Regular Expressions (PCRE) library. It can send an alert to the Prelude Manager when a suspicious log entry is detected.

Libprelude Library

Libprelude is the library that provides the framework used to access the Prelude system. It handles secure communications with the MySurveillance sensor, and provides an Application Programming Interface (API) to create Intrusion Detection Message Exchange Format (IDMEF) based events. It also provides important features like fail-over (by saving to a local file for later retransmission later and usage of a fallback route), in case one of the MySurveillance servers goes down. Moreover, it gives you the ability to create sensors that read events received by one or more MySurveillance servers.

Libpreludedb Library

The PreludeDB Library provides an abstraction layer based upon the type and the format of the database used to store Intrusion Detection Message Exchange Format (IDMEF) alerts. It allows developers to use the MySurveillance Data Store easily and efficiently without worrying about Structured Query Language (SQL), and to access the MySurveillance Data Store independently of the type/format of the database.

Prewikka

Prewikka is a web-based management console for MySurveillance. Some of the features available in Prewikka are contextual filtering, aggregation and permission management.

INSTALLATION STEPS

There are two steps of installation involved with installation of the admin-server with an IP of 192.168.0.1 and a client-server with an IP of 192.168.0.2 to the system.

Section 1: Installing the MySurveillance server

1) To sync date and time at the server to an NTP server, run the command:

```
ntpdate pool.ntp.org (If ntpdate is not available, install it using the
                      command; yum install ntp)

service ntpd start

chkconfig ntpd on
```

2) Install/Enable the OSCC repos:

```
rpm -Uvh http://repos.oscc.org.my/centos/5/os/i386/CentOS/oscc-repos-0.0.1-1.noarch.rpm

rpm -Uvh http://repos.oscc.org.my/repos2/centos/5/oscc/i386/CentOS/oscc-repos2-0.0.1-1.noarch.rpm
```

3) Install mysurveillance-server

```
yum install mysurveillance-server
```

4) Change configurations in the */etc/prelude-manager/prelude-manager.conf* file

```
        listen = SERVER_IP

              (eg: 192.168.0.1)
```

5) Add prelude-manager to the system by run this command

```
        prelude-admin add "prelude-manager" --uid 0 --gid 0
```

6) Start prelude-manager service by run this command

```
        service prelude-manager start
```

7) After the installation is complete, open web browser.

```
        http://SERVER_IP/mysurveillance

              (eg: http://localhost/mysurveillance)

           or (eg: http://192.168.0.1/mysurveillance)
```

Use the default login (admin**) and password (**admin**), but it is highly recommended to change the password on the first the login.

Section 2: Adding client to the system

1) To sync date and time at the client-server to ntp time, run command:

```
ntpdate pool.ntp.org (If ntpdate is not available, install it using the
                        command; yum install ntp)

service ntpd start

chkconfig ntpd on
```

2) Install/Enable OSCC repos

```
rpm -Uvh http://repos.oscc.org.my/centos/5/os/i386/CentOS/oscc-repos-0.0.1-1.noarch.rpm

rpm -Uvh http://repos.oscc.org.my/repos2/centos/5/oscc/i386/CentOS/oscc-repos2-0.0.1-1.noarch.rpm
```

3) Install mysurveillance-client

```
yum install mysurveillance-client
```

4) Change the following in the config files:

4.1) /etc/prelude/default/client.conf

```
server-addr = IP_ADMIN_SERVER
```

```
        (eg: 192.168.0.1)
```

4.2) /etc/prelude/default/global.conf

```
analyzer-name = NAME

        (eg: test)

  node-name = MACHINE_NAME

        (eg: oscc1)

  node-location = COMPANY_NAME

         (eg: OSCC)

  node-category = REFER_NODE_TYPE

         (eg: unknown)


  [Node-Address]

  address = IP_ADDRESS

        (eg: 192.168.0.2)
```

4.3) /etc/prelude-lml/prelude-lml.conf

Uncomment these commands in the config file

```
[format=syslog]

time-format = "%b %d %H:%M:%S"

prefix-regex = "^(?P<timestamp>.{15}) (?P<hostname>\S+) (?:(?
P<process>\S+?)(?:\[(?P<pid>[0-9]+) \])?: )?"
file = /var/log/messages

file = /var/log/secure

file = /var/log/httpd/access_log
```

5) Add client to the system by run this command

```
        prelude-admin  register  prelude-lml  "idmef:w  admin:r"  IP_ADMIN-SERVER
        --uid 0 --gid 0

            (eg: prelude-admin register prelude-lml "idmef:w admin:r"
            192.168.0.1 --uid 0 --gid 0)
```

**It will prompt for one-shot password provided from admin-server (please refer to the Installation step at the server #1 before you proceed to the next step).

7) Start prelude-lml service by run this command

```
        service prelude-lml start
```

Installation step at the server

1) Register client to the server by run this command

```
        prelude-admin registration-server prelude-manager
```

**Use the password given for configuration #5 at the client machine.

MAINTENANCE

The following should be checked on a regular basis:

Network connections

The administrator should verify the server is reachable from the public network to avoid service interruption. Network monitoring is beyond the scope of these manual.

Log files

With the log files, it is possible to identify and monitor hardware and software problems on the servers. The log files should be checked at least once a week. All log files in /var/log/ directory.

Services

Used to start, stop or cancel a service on a local or remote computer. It is also a tool to set up recovery actions to take place if a service should fail. Should be checked in case of service failure.

e.g: *#/etc/init.d/[service_name] start/stop/status*

Package update/patch

Check that the latest package update/patches has been installed on the servers. It should be checked and done at least once a month.

Disk Space

to verify that there is always enough space on the most mission critical servers. It should be done at least once a week. Use *df -lh* command.

Password change

Password should be changed periodically, at least every three months.

Service update

Check for services update for the main components in MySurveillance such as libprelude, libpreludedb, prewikka and prelude_lml.