International Journal of Science, Engineering and Technology
An Open Access Journal

Centralized Logging, Backup User and Management

Swapnil Pawar, Pratik Deshmukh, Sandhya Mhetre, Megha Anuse, Vaishnvi Pujari

Abstract

The purpose of the paper is to research on centralized logging, backup and user management Centralized Logging is a computing done at central location. Logs area unit used for various functions, like recording user activities, track authentication tries, and alternative security events. As a result of increasing variety of threats against networks and systems, the amount of security logs will increase. However, several organizations that employment in a very distributed atmosphere faces following problems: log generation and storage.Moreover, guaranteeing that security, system and network directors analyse log information in a good approach is another issue. During this analysis, we tend to propose associate degree approach for receiving, storing log events, backup of logs & user management. Besides, we exhibit an answer plan that securely enables associations in appropriated situations to send review log exchanges from various nearby systems to one brought together server. The process of backing up, refers to the copying and archiving of computer logs so it may be used to restore the original after a data loss event. Users and groups are used on Linux for access control that is to control access to system's files, directories and peripherals.

Keywords—Centralized Logging, Audit Log, Centralized Server

Introduction

It is vital to identify what devices and services were affected when a specific incident has occurred in the network in order to support incident investigation. The logs are valuable for intrusion detection and analysis.Log files are going to be very useful for troubleshooting or once yearning for unauthorized log in tries to the system. It helps to managing & accessing logs at central location. Information loss is that the most important issues, the foremost common cause's area unit physical failure of your portable computer, frequent accidental error or accidents like fire thus, we tend to taking backup. & we tend to do user management for the aim of security by limiting access in positive specific ways that during which. In this research, we propose a system for receiving, storing logs, log backup & user management.

LITERATURE SURVEY

Centralized Logging

Monitoring several service on one server poses some difficulties.

Watching several service on several servers needs an entire new approach of thinking and a brand new set of tools. We cannot, anymore, log into a node and appearance at logs. There area unit too several logs to seem at. On high of that, they're distributed among several servers

Logging:

Logs are unit an essential a part of any system, they furnish you info concerning what a system is doing moreover what happened.

Nearly each method running on a system generates logs in some type. Usually, these logs area unit written to files on native disks work could be a means that of pursuit events that happen once some software system runs.

- **Backup:**

© 2017, This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

One of the most neglected tasks of system administration is creating backup copies of files on a daily basis. The backup copies square measure very important in 3 instances: once the system malfunctions, files square measure lost, once a ruinous like a fireplace or earthquake happens and once a user or the computer user deletes or corrupts a file by chance

Backup Utilities:-

A number of utilities will assist you make a copy the machine, and maximum paintings with any media. Maximum Linux backup utilities location unit supported one in all the archive programs —tar or cpio & mdash and augment these basic packages with accounting guide for dealing with backups handily

User management:-

Managing Users via GUI

1. Adding Users

2. Deleting Users

3. Modifying Users

Tools available for centralized logging:-

1. Rsyslog
2. Logcheck
3. Logwatch

Drawbacks of above tools:-

1) Rsyslog:-

Rsyslog is an open-source software utility used on UNIX and Unix-like computer systems for forwarding log messages in an IP network. It implements the basic syslog protocol.[2] Rsyslog works with terminal and it doesn't have program and it don't take backup of logs at a centralized server.

2) Logcheck:-

Logcheck is a software package that is designed to automatically run and check system log files for security violations and unusual activity, it utilizes a program called logtail that remembers the last position it read from the log file.[3] As like Rsyslog, Logcheck works with terminal and it solely offers alerting of errors and warnings. It doesn't have user management too.

3) Logwatch:-

Our Linux systems run logwatch utility by default. Problem is that by default these daily emails are too noisy and contain a lot of superfluous information (HTTP errors, daily disk usage, etc.) which are already monitored by other services (Nagios, Cacti, central syslog, etc.). For 100 systems, the email load is unbearable. People ignore the emails, which means that we may miss problems which are picked up by logwatch.[4]

PROBLEM LIFE CYCLE

Problem Identification

When your system grows to multiple hosts, managing the logs and accessing them will get difficult. Looking for a selected error across many log files on many servers is tough while not sensible tools. That's why a typical approach to the current drawback is to setup centralized work. So multiple logs will aggregative in an exceedingly central location. User management could be an important a part of maintaining a secure system. Ineffective user and privilege management usually lead several systems into being compromised. Data loss will happen in many ways, the foremost common causes are physical failure of your machine, accidental error, felony or disasters like fire. Therefore, it's necessary that you just perceive however you'll be able to shield your server through easy and effective user account management techniques

Problem Selection

There are Separate applications available for centralized logging, backup and user management. Till now no any application available with centralized logging, backup and user management together .we are providing this three functionality in one application. System administrator can do centralized logging. Backup and user management from remote server, no need to go at particular place and do the work. So that this application will be very useful for system administrator.

Problem Definition

Relevance:-

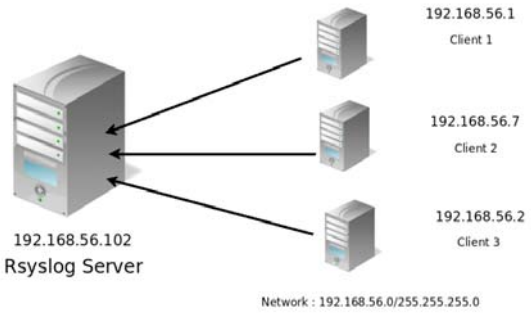
Most of the tools and utilities available for the centralized logging and backup of the clients are terminal based while we do user management through terminal only. Also some tools available are web-based and takes lot of money to store the backup of log data to the cloud. This application provides centralized logging, backup of the logs and

user management with better user interface for Linux users.

Objectives:-

1. To create GUI based application for centralized logging, Backup and User Management for Linux clients.
2. To take backup of logs at low cost.
3. To provide secured and easy access to required logs and User's Account.

Problem Analysis:



System Architecture

Why centralized logging?

When your system grows to multiple hosts, managing the logs and accessing them will get difficult. Sorting out a selected error across many log files on many servers is troublesome while not sensible tools. A typical approach to the present downside is to setup a centralized work answer so multiple logs is collective during a central location.

Why Backup?

- Data misfortune can occur from multiple points of view, the most widely recognized causes are physical failure of your PC, coincidental mistake, robbery or disasters like fire.
- Files can accidently be deleted or become corrupt.
- Customers want Access to data 24*7.

Why User Management?

- User management is done for the purpose of security by limiting access in certain specific ways.
- To verify the identification of each and every specific user utilizing a pc method.
- To permit the per-individual tailoring of resources and access privileges.

End Users

This project can be used by any system administrator for storing logs, maintaining the backup and managing users

IMPLEMENTATIOIN AND RESULT ANALYSIS

We are using glade framework for developing GUI for this application. We are using python language for implementation.

Python

Python is a widely used high-level, general, taken, language. Python is a multi-paradigm programming language: object-oriented programming and structured programming are fully supported, and many language features support functional programming and aspect-oriented programming (including by metaprogrammingand metaobjects (magic methods))[1]

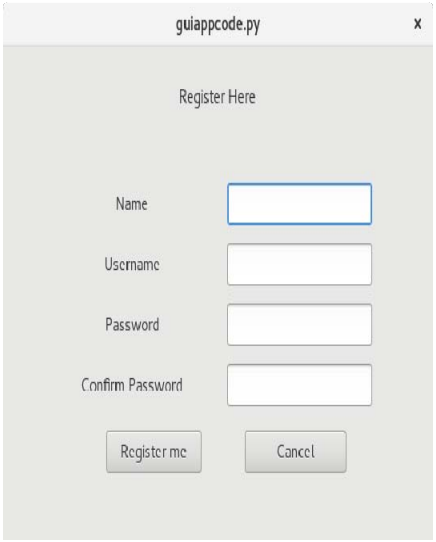


Fig 1: Registration Window

This is Registration window for Administrator.

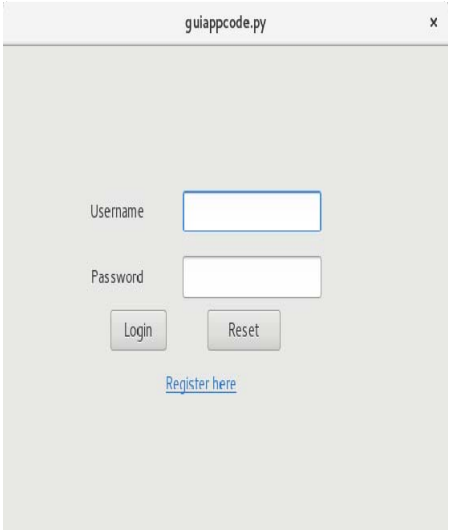


Fig2: Login page

This is Login & Registration page for Administrator.

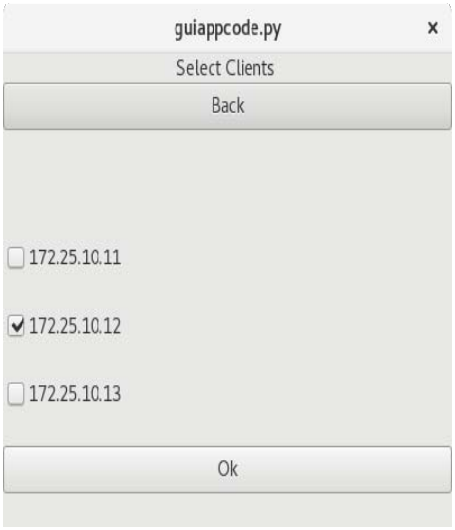


Fig 3:Client Selection Window

This window help administrator to select client on which operations to be perform.

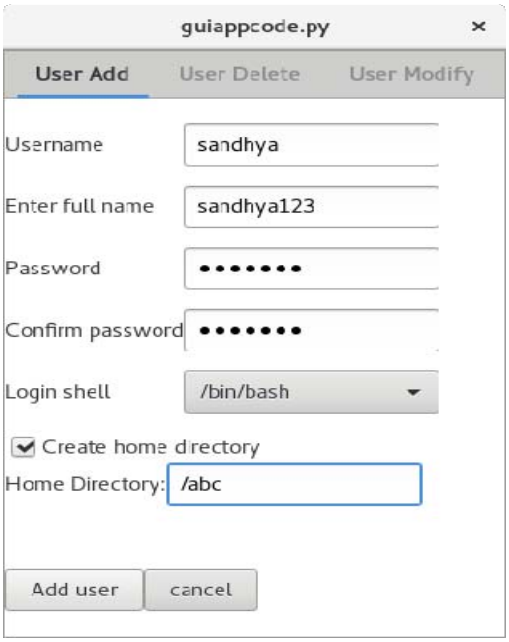


Fig 3: Adding User Window

Above Window contains 3 options 1-User Add. 2-User Delete. 3- User Modify. This window will add the users on clients that is connected in LAN via remote machine

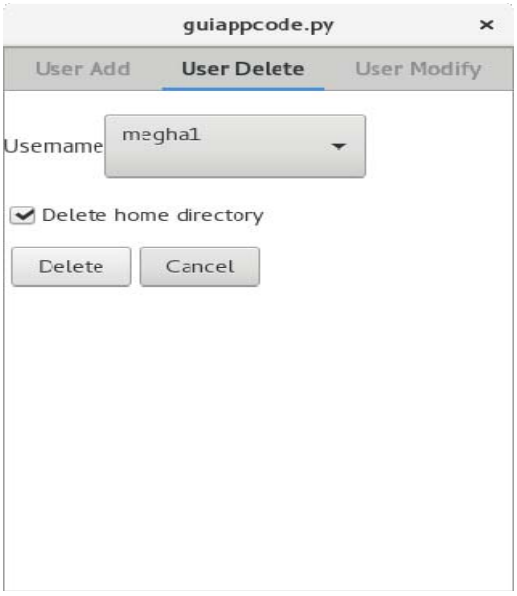


Fig4: Deleting User Window

This will delete the users which are available on remote machines connected in LAN

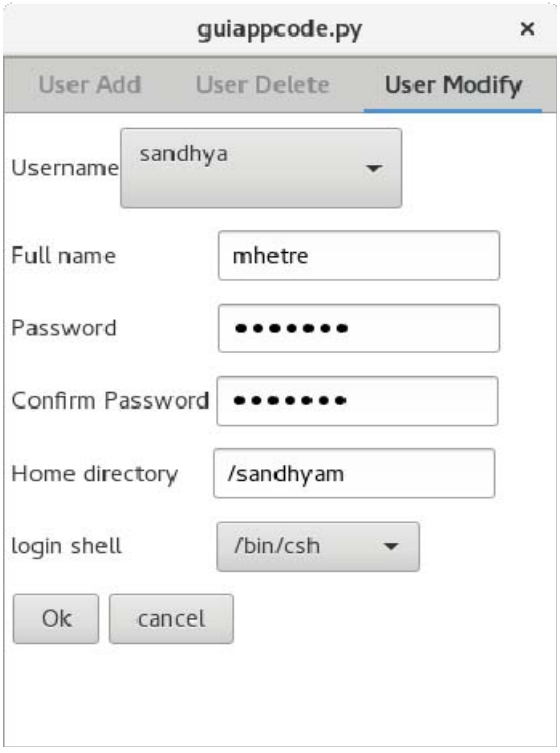


Fig 5: Modifying User Window

This window can be used to modify the existing users available on the remote machines connected in LAN

Fig 6: Backup Window

After selecting particular client it will be redirected to this window which select destination folder to take backup window. The dropdown list allows you to select the destination folder for saving the backup of remote machine connected in LAN.

CONCLUSION AND FUTURE WORK

Project is developing graphical user interface primarily based application for centralized work, backup and user management.

Future Work:

In future we can do following in our GUI:

1. Analysis of log files
2. Error reporting with solution
3. Nagios for service status details

References

[1].https://en.wikipedia.org/wiki/Python_(programming language)

[2] https://en.wikipedia.org/wiki/Rsyslog

[3] http://linoxide.com/tools/monitor-system-log-activity/

[4] https://serverfault.com/questions/293226/linux-logwatch8-is-too-noisy-how-can-i-control-the-noise-level/293233