LOGPOINT

# Integrations

## Unix

V5.1.0

# CONTENTS


**1 Unix Application** **1**

**2 Installing the Application** **6**
2.1 Prerequisites . . . 6
2.2 Installing the Unix Application in LogPoint . . . 6

**3 Configuring the Application** **7**
3.1 Adding a Normalization Policy for Unix Application . . . 7
3.2 Adding Unix as a Device in LogPoint . . . 8
3.3 Configuring the Syslog Collector for Unix . . . 10

**4 Unix Analytics** **13**
4.1 Unix Dashboards . . . 13
4.1.1 Adding the Unix Dashboards . . . 13
4.1.2 Unix Widgets . . . 16
4.2 Unix Alerts . . . 19
4.2.1 LP_Unix Possible Bruteforce Attack . . . 19
4.2.2 LP_Unix Kernel Logging Stopped . . . 19
4.2.3 LP_Unix User Deleted . . . 20
4.2.4 LP_Unix Password Expiry Changed for User . . . 20
4.2.5 LP_Unix Group Deleted . . . 20
4.2.6 LP_Unix Security Violation . . . 21
4.2.7 LP_Unix User Account Unlocked . . . 21
4.2.8 LP_Unix Excessive Denied Connection . . . 21
4.2.9 LP_Unix User Removed from Privileged Group . . . 22
4.2.10 LP_Unix Privilege Escalation Failed . . . 22
4.2.11 LP_Unix User Session Alert . . . 23
4.3 Unix Labels . . . 23
4.4 Unix Report Templates . . . 25
4.5 Using Unix Report Templates . . . 25

**5 Uninstallation** **28**
5.1 Uninstalling the Unix Application in LogPoint . . . 28

CHAPTER

ONE

# UNIX APPLICATION

The **Unix** application for LogPoint SIEM allows you to monitor and identify threats in your organization using the Unix data. LogPoint aggregates and normalizes the Unix logs so you can analyze the information through dashboards and security reports. Unix's dashboard provides visualization of event details for authentication requests, privilege escalation, and user account management of the Unix environment detected in your network. The dashboard enables you to monitor the security status of your organization. You can customize the dashboards to suit your needs and perform in-depth analysis by adjusting the data and searches.

1. **Dashboard Packages**
    - LP_Unix Overview
    - LP_Unix Privilege Escalation
    - LP_UNIX: AUTHENTICATION
    - LP_Unix: User Account Management
2. **Normalization Packages**
    - LP_Unix Syscall
    - LP_Unix Ftpd
    - LP_Unix Zookeeper
    - LP_Unix Vasd
    - LP_Unix clurgmgrd
    - LP_Unix Iptables
    - LP_Unix Logger
    - LP_Unix Ftp
    - LP_Unix Xntpd
    - LP_Unix Redis Server
    - LP_Unix Chkpwd
    - LP_Unix IPsec

- LP_Unix Kubelet
- LP_Unix Generic
- LP_Unix adcli
- LP_Unix Dockerd
- LP_Unix Chef Client
- LP_Unix SNMP Traps
- LP_Unix Auditd
- LP_Unix Crond
- LP_Unix Pure Ftpd
- LP_Unix Inetd
- LP_Unix SNMP
- LP_Unix Dhclient
- LP_Unix Cron
- LP_Unix Infinity
- LP_Unix Vparmodify
- LP_Unix VS Ftpd
- LP_Unix Rsandbox
- LP_Unix Runuser
- LP_Unix Devd
- LP_Unix Proftpd
- LP_Solaris OS
- LP_Unix SSL Proxy
- LP_Unix SCC
- LP_Unix Audispd
- LP_UNIX NFS
- LP_Unix nslcd
- LP_Unix Httpd
- LP_Unix Mountd
- LP_Unix dnsmasq
- LP_Unix Run-parts
- LP_Unix Kafka
- LP_Unix Ipmserver
- LP_Unix check nrpe
- LP_Unix Anacron

- LP_Unix php
- LP_Unix Xpand
- LP_Unix Routed
- LP_Unix Bash
- LP_UNIX Nscd
- LP_Unix Lvm
- LP_Unix Pengine
- LP_Unix Stonith NG
- LP_Unix Goferd
- LP_Unix Nagios
- LP_Unix IPMIEVD
- LP_Unix SAP
- LP_Unix Vmunix
- LP_Unix Savd
- LP_Unix Winbindd
- LP_Unix Syslog NG
- LP_Unix SU
- LP_Unix l4d
- LP_Unix Rsyslogd
- LP_Unix Rhnsd
- LP_Unix puppet-agent
- LP_Unix Suhosin
- LP_Unix Sudo
- LP_Unix ptymonitor
- LP_Unix Sfd
- LP_Unix Smbd
- LP_Unix passwd
- LP_Unix sssd
- LP_Unix Lrmd
- LP_Unix InotifyWait
- LP_Unix UCARP
- LP_Red Hat Linux
- LP_Unix rear
- LP_Unix NTPD

- LP_Unix RpcMountd
- LP_Unix Lighttpd
- LP_Unix Cimserver
- LP_Unix Cmclconfd
- LP_Unix Lvmpud
- LP_Unix NS
- LP_Unix ndo2db
- LP_Kernel
- LP_Unix Agetty
- LP_Unix Sudoscriptd
- LP_Docker
- LP_Unix Rshd
- LP_Unix xinetd
- LP_Unix SSHD
- LP_Unix Cifs Upcall
- LP_Unix Auditlog
- LP_Unix Sftp Server
- LP_Unix rgmanager
- LP_Unix PAM Tally
- LP_Unix subscription-manager
- LP_Unix Syslogd
- LP_Common Unix System
- LP_Unix Systemd
- LP_Unix Yum
- LP_Unix Snmpd
- LP_Unix Named
- LP_Unix Newrelic Infra
- LP_Unix Crmd

3. **Alert Packages**

- LP_Unix Possible Bruteforce Attack
- LP_Unix Kernel Logging Stopped
- LP_Unix User Deleted
- LP_Unix Password Expiry Changed for User

- LP_Unix Group Deleted
- LP_Unix Privilege Escalation Failed
- LP_Unix Security Violation
- LP_Unix User Account Unlocked
- LP_Unix Excessive Denied Connection
- LP_Unix User Session Alert
- LP_Unix User Removed from Privileged Group

4. **Label Packages**

    - LP_Unix SSHD
    - LP_Common Unix Systems
    - LP_Unix

5. **Compiled Normalizers**

    - UnixCompiledNormalizer
    - UnixAuditLogNormalizer

6. **Report Packages**

    - LP_Unix: User Privilege Escalation
    - LP_Unix: User Account Management
    - LP_UNIX: AUTHENTICATION

7. **Knowledge Base Lists**

    - ADMINS
    - ADMIN_GROUPS

CHAPTER

TWO

# INSTALLING THE APPLICATION

## 2.1 Prerequisites

LogPoint v6.7.4 or later

## 2.2 Installing the Unix Application in LogPoint

1. Go to *Settings >> System >> Applications*.
2. Click **Import**.
3. **Browse** the downloaded Unix pak file.
4. Click **Upload**.

After installing the application, you can find it under *Settings >> System >> Plugins*.

CHAPTER

THREE

# CONFIGURING THE APPLICATION

## 3.1 Adding a Normalization Policy for Unix Application

1. Go to *Settings >> Configuration >> Normalization Policies*.
2. Click **Add**.
3. Enter a **Policy Name**.
4. Select the **Compiled Normalizer** for Unix.
5. Click **Submit**.

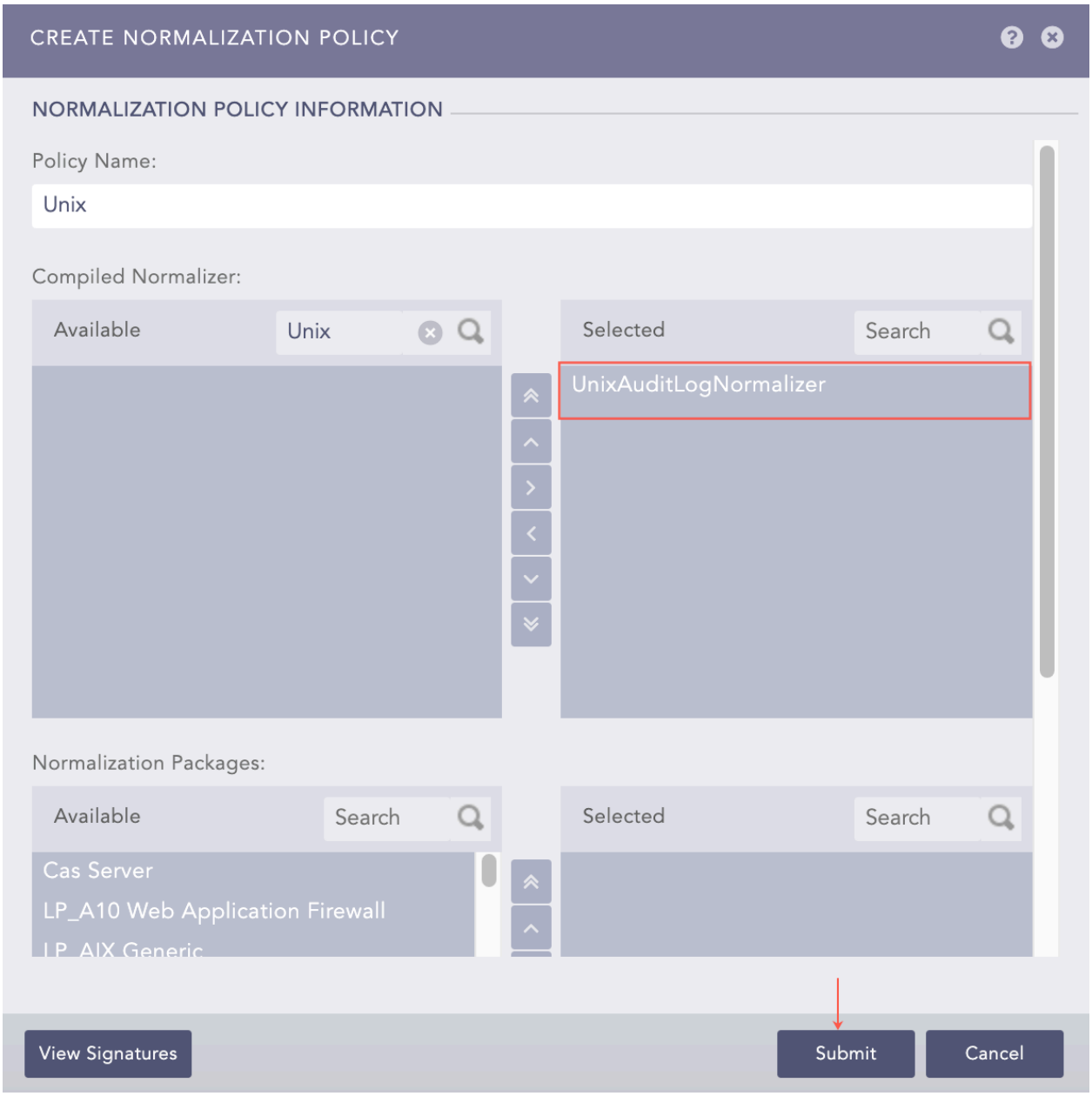



Fig. 1: Adding a Normalization Policy

## 3.2 Adding Unix as a Device in LogPoint

1. Go to *Settings >> Configuration >> Devices*.
2. Click **Add**.

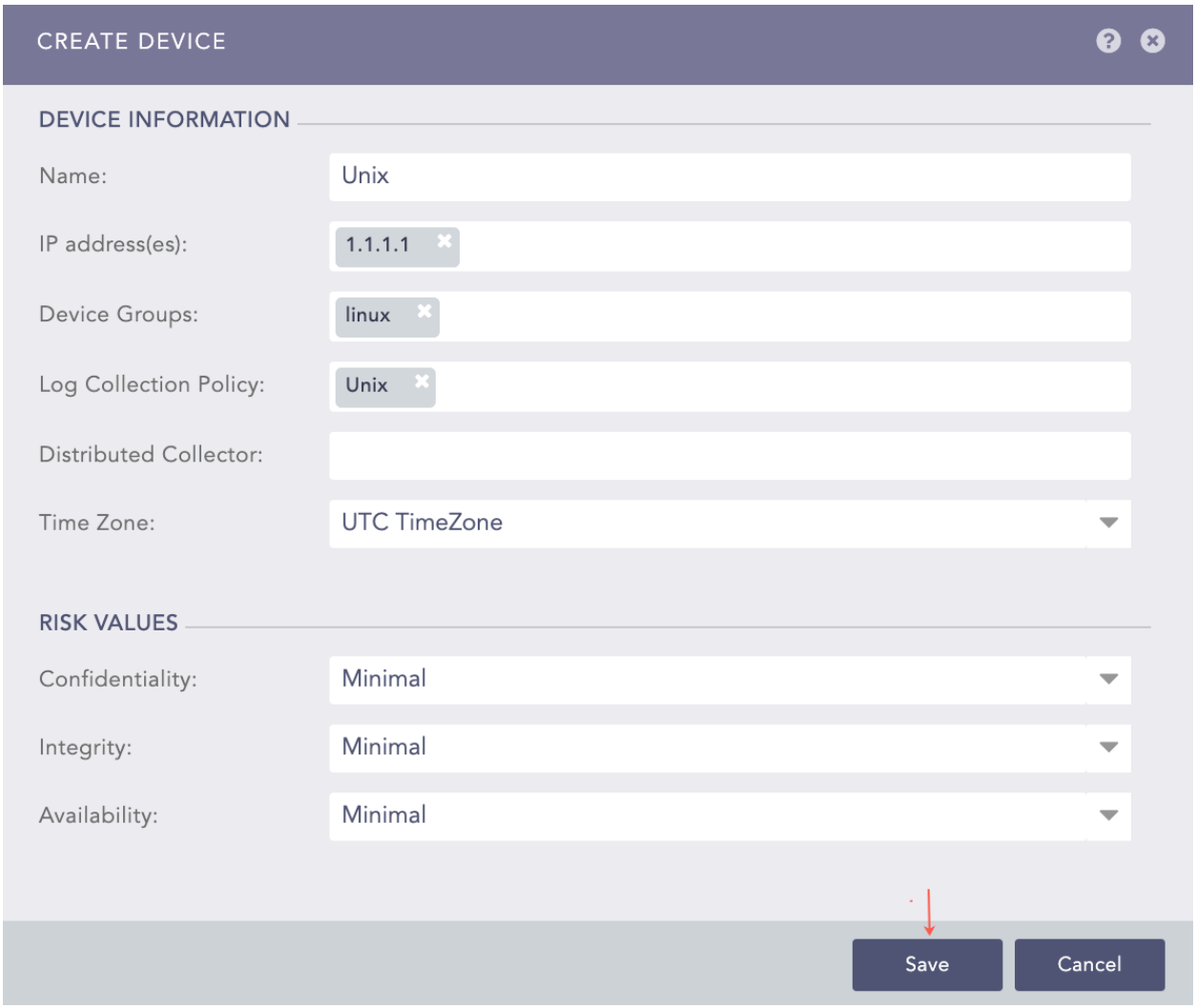



Fig. 2: Creating Unix as a Device

3. Enter a device **Name**.
4. Enter the **IP address(es)** of the Unix server.
5. Select the **Device Groups**.
6. Select an appropriate **Log Collection Policy** for the logs.
7. Enter a collector or a forwarder in the **Distributed Collector**.

**Note:** It is optional to select the **Device Groups**, the **Log Collection Policy**, and the **Distributed Collector**.

8. Select a **Time Zone**.

**Note:** The timezone of the device must be the same as that of its log source.

9. Configure the **Risk Values** for **Confidentiality**, **Integrity**, and **Availability** used to calculate the risk levels of the alerts generated from the device.
10. Click **Submit**.

## 3.3 Configuring the Syslog Collector for Unix

1. Click **Syslog Collector** on the *Available Collectors Fetchers* panel.

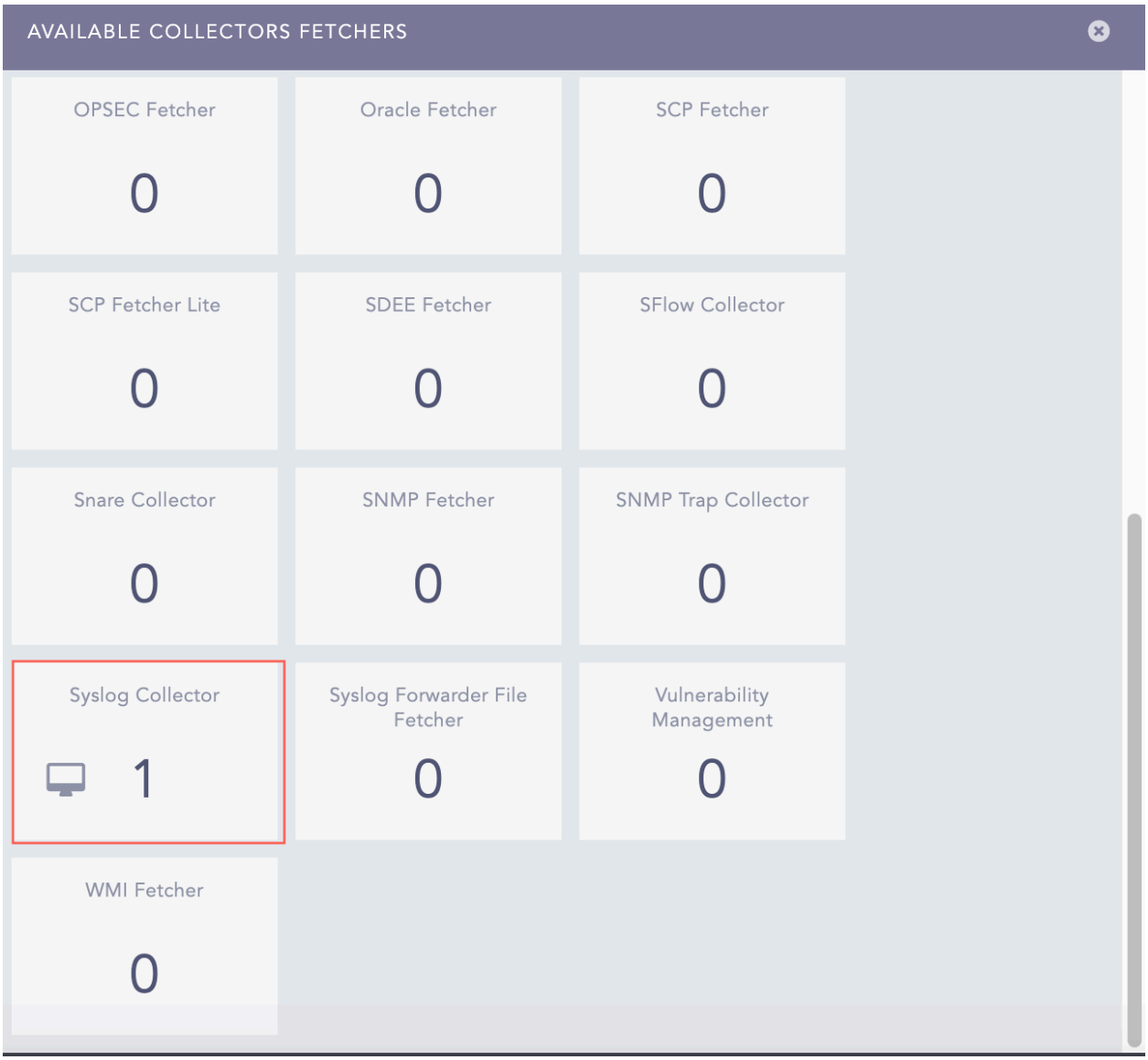



Fig. 3: Available Collectors Fetchers Panel

2. Select the **Syslog Parser**.

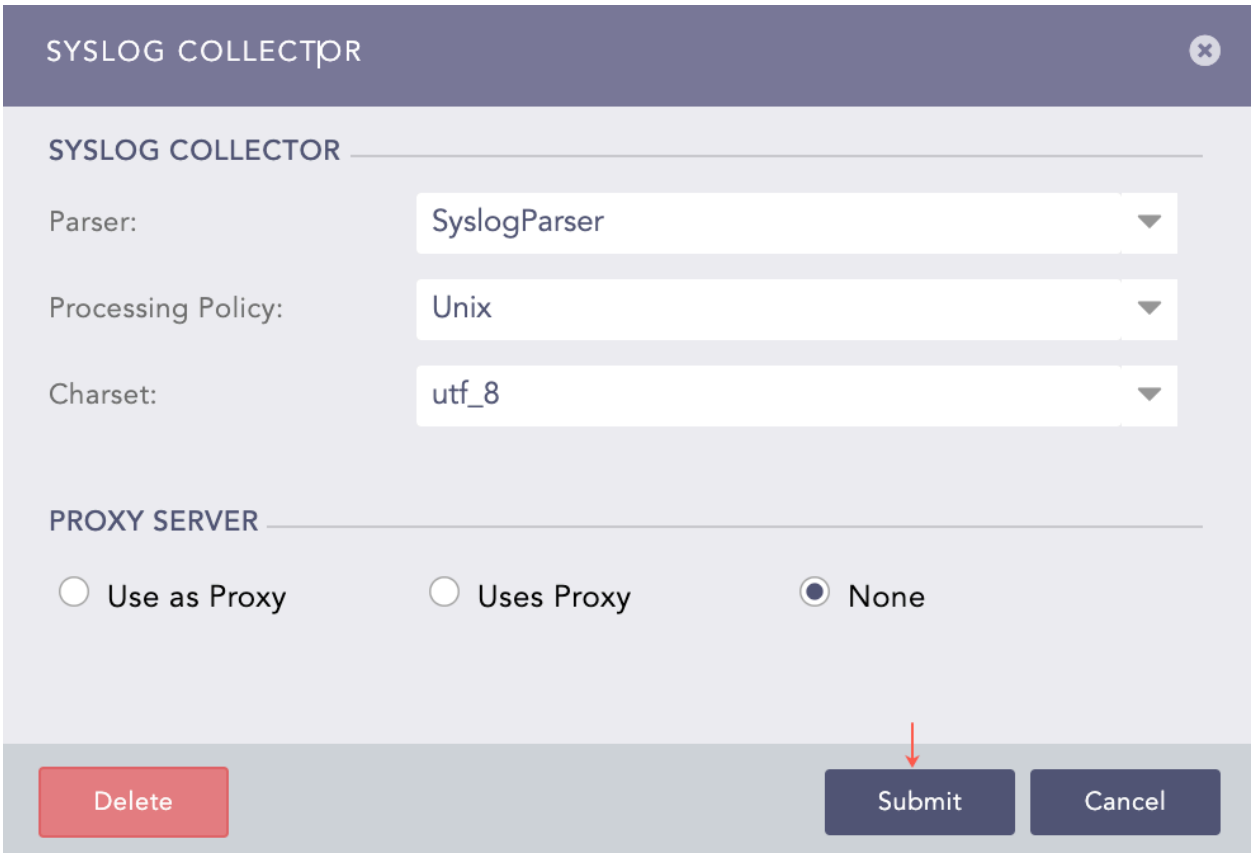



Fig. 4: Syslog Collector Panel

3. Select the **Processing Policy** which contains the previously added *normalization policy*.
4. Select the **Charset**.
5. Select *None* as **Proxy Server**.
6. Click **Submit**.

CHAPTER

FOUR

# UNIX ANALYTICS

## 4.1 Unix Dashboards

### 4.1.1 Adding the Unix Dashboards

1. Go to *Settings >> Knowledge Base >> Dashboards*.
2. Select **Vendor Dashboard** from the drop-down.
3. Click **Add**.

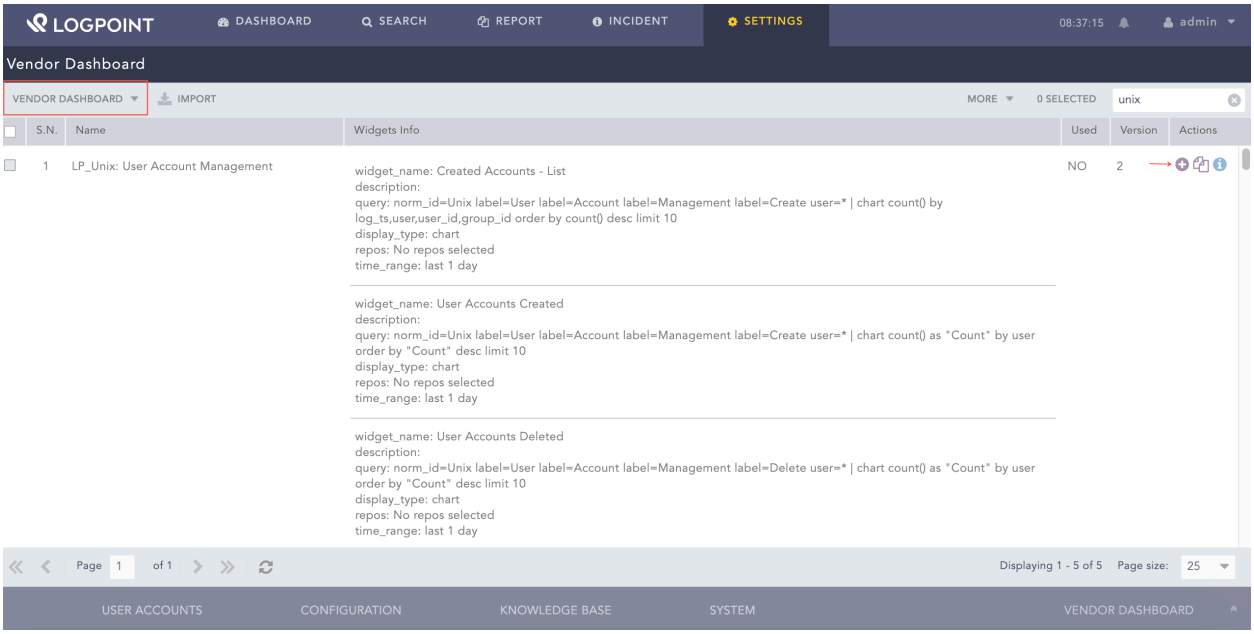



Fig. 1: Adding the Unix Dashboard

3. Click **Choose Repos**.

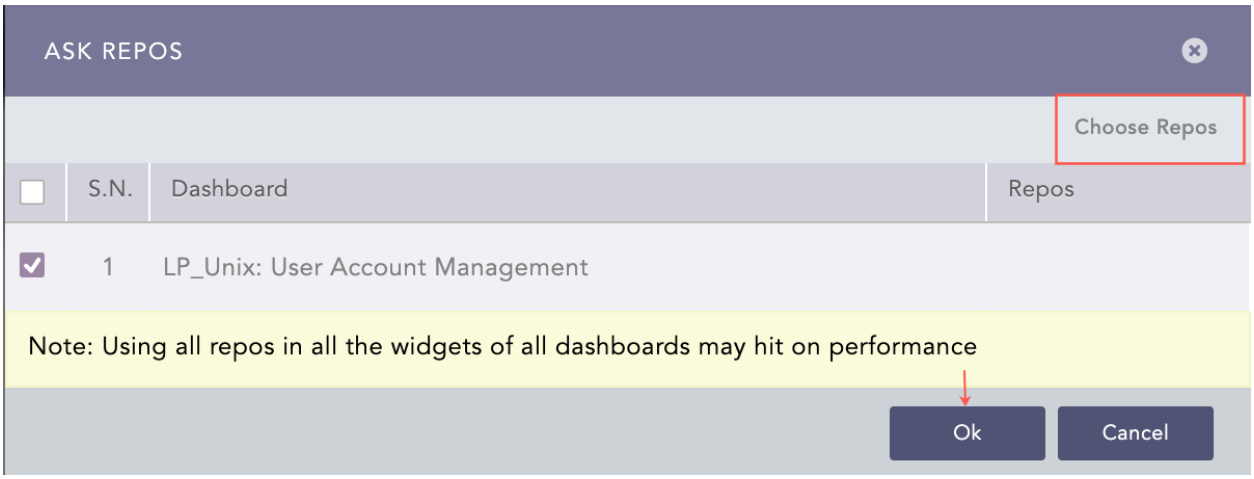



Fig. 2: Selecting a Repo

4. Select the repo and click **Done**.

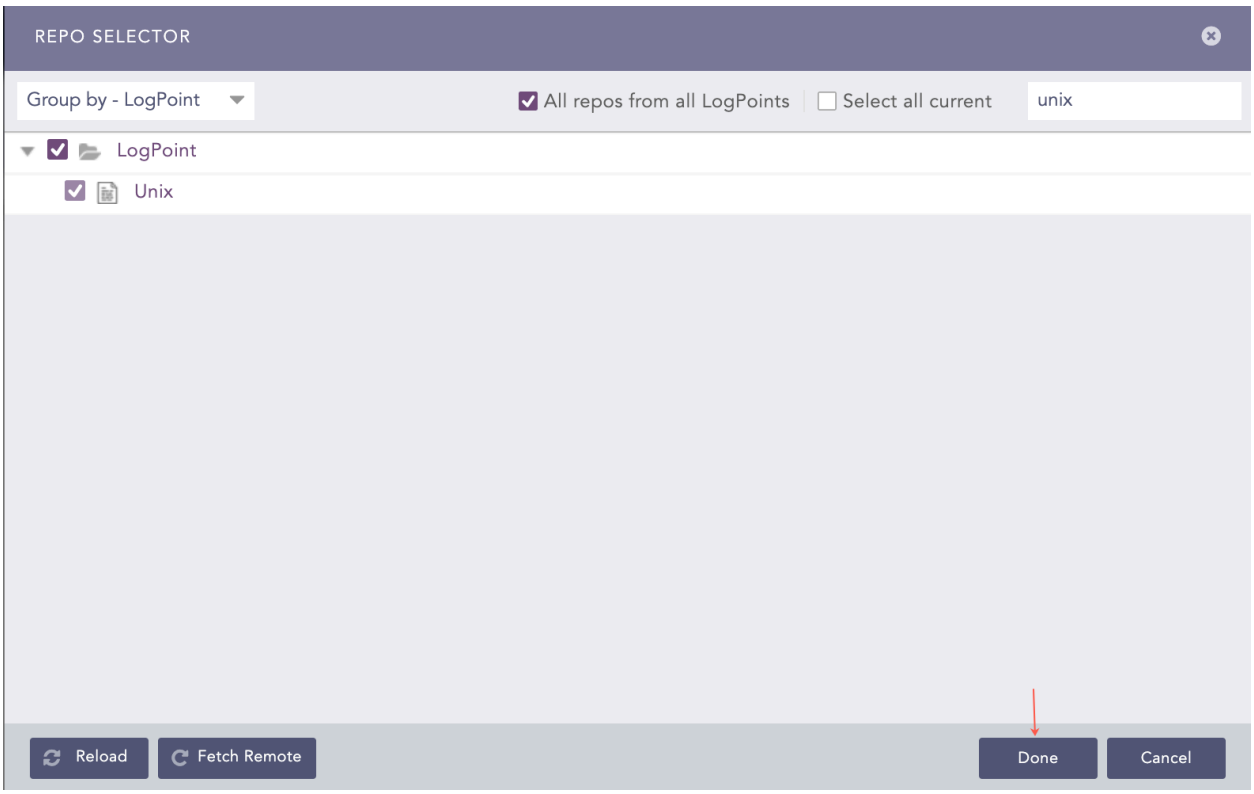



Fig. 3: Selecting a Repo

5. Click **Ok**.

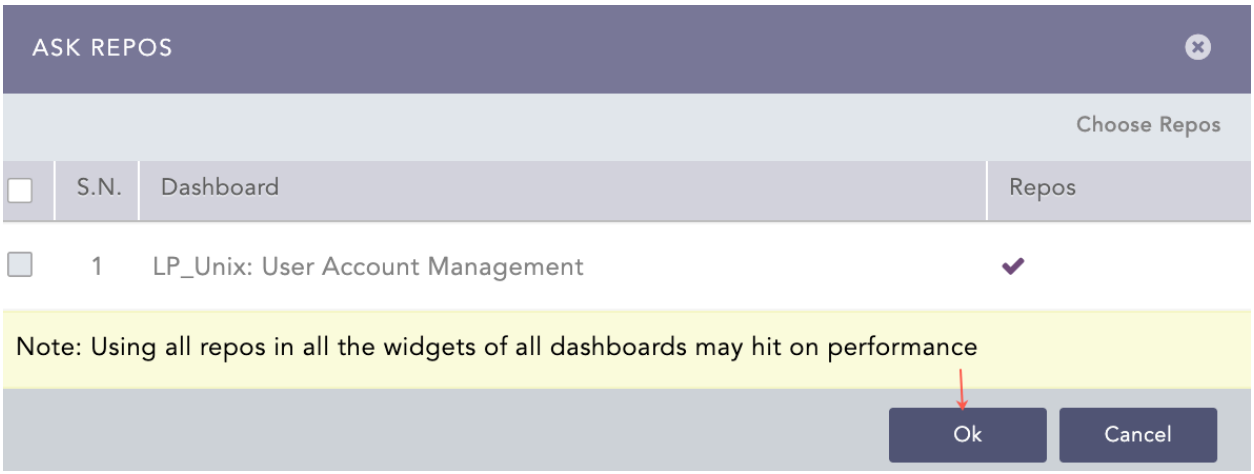
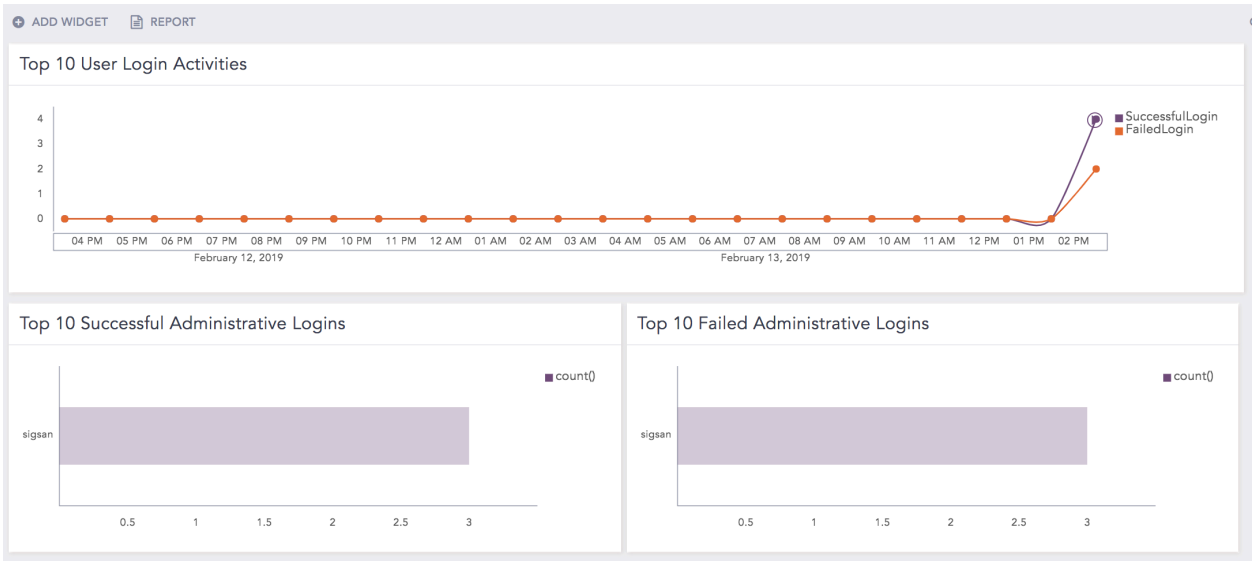



Fig. 4: Confirmation for Repo

You can find the Unix dashboards under *Dashboards*.



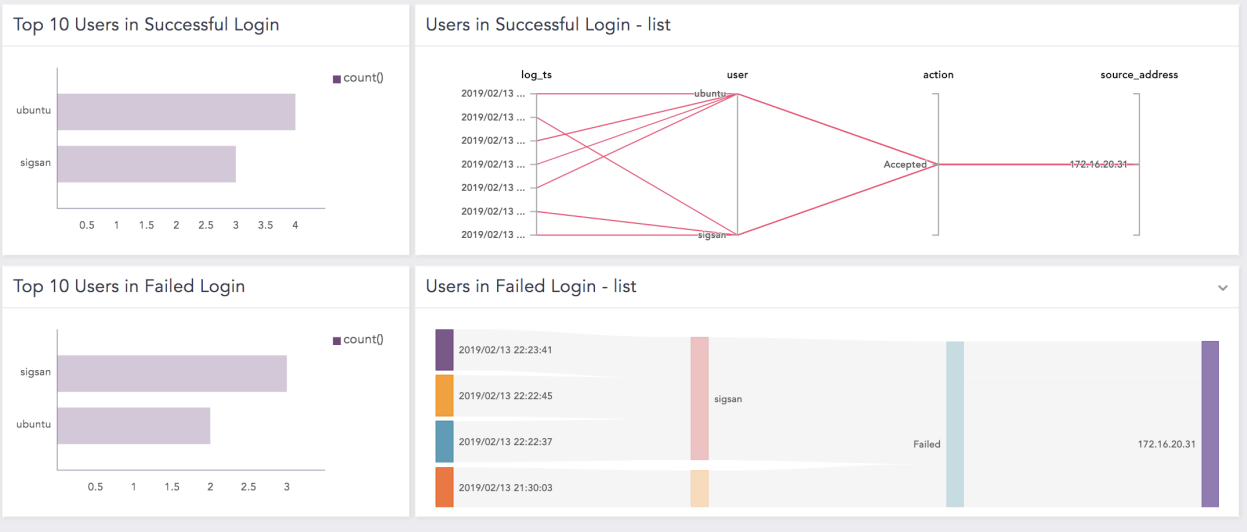



Fig. 5: Unix Dashboard

### 4.1.2 Unix Widgets

The following widgets are available in *LP_Unix Overview*:

| Widget Name | Description |
|---|---|
| Top 10 Process Running | The widget provides an overview of the top 10 Unix processes, such as parents or child processes, zombie or orphan processes, or even list running processes. |
| Events Timetrend | The widget displays a time trend of the Unix events. |
| Top 10 Commands Used | The widget displays the top 10 most used Unix commands, such as sudo. |
| Top 10 Sudo Commands | The widget provides an overview of the top 10 sudo commands that allows you to run programs with the security privileges of another user (by default, as the superuser). |
| Top 10 Sources in Denied Connection | The widget provides an overview of the top 10 denied source addresses. |
| Top 10 Users in Successful Logins | The widget provides an overview of the top 10 users who successfully logged in. |
| Top 10 Users in Failed Logins | The widget provides an overview of the top 10 users who failed to log in. |
| Top 10 Sources in Successful User Logins | The widget provides an overview of the top 10 source addresses in successful user logins. |

Continued on next page

Table 1 – continued from previous page

| Widget Name | Description |
|---|---|
| Top 10 Sources in Failed User Logins | The widget provides an overview of the top 10 source addresses in failed user logins. |
| User Login Status | The widget provides the status of user login, which may be a successful login or failed login. |

The following widgets are available in *LP_Unix Privilege Escalation*:

| Widget Name | Description |
|---|---|
| Session Duration | The widget provides an overview of Unix user session so you can see the full context of what happened through the session by session start timestamp, session end timestamp, user, root ID, and session ID. |
| Root Privilege Command Execution | The widget provides an overview of the commands executed that require privileges not granted to a standard UNIX user account by root session start timestamp, root session end timestamp, user, command execute timestamp, and command. |
| Top 10 Users in Privilege Escalation | The widget provides an overview of the top 10 users in privilege escalation who have gained elevated access to resources that are normally protected from an application or user. |
| Top 10 Command Executed | The widget provides an overview of the top 10 Unix commands executed. |

The following widgets are available in *LP_Unix:Authentication*:

| Widget Name | Description |
|---|---|
| Top 10 Successful Administrative Logins | The widget provides an overview of the top 10 successful administrative logins. You need the list ADMINS to run this query. |
| Top 10 Users in Successful Login | The widget provides an overview of the top 10 users who logged in successfully. |
| Users in Successful Login - List | The widget provides a detailed list of the successful user login by a user, action, and source address. |
| Top 10 Users in Failed Login | The widget provides an overview of the top 10 users who failed to log in successfully. |
| Users in Failed Login - List | The widget provides a detailed list of the failed user login by a user, action, and source address. |

Continued on next page

Table 3 – continued from previous page

| Widget Name | Description |
|---|---|
| Top 10 Failed Administrative Logins | The widget provides an overview of the top 10 admin users who failed to log in successfully. You need a list ADMINS to run this query. |
| Top 10 User Login Activities | The widget provides an overview of the top 10 successful user activities, such as successful login or failed login. |

The following widgets are available in *LP_Unix:User Account Management*:

| Widget Name | Description |
|---|---|
| Created Accounts - List | The widget provides a detailed list of created accounts. |
| User Accounts Created | The widget provides an overview of the created user accounts. |
| User Accounts Deleted | The widget provides an overview of the deleted user accounts. |
| Activities in User Account Management | The widget provides an overview of the activities in the user account management, such as user add or group add. |
| Activities in User Account Management - List | The widget provides a detailed list of activities in user account management by user and action. |
| Top 10 Actions in User Account Management | The widget provides an overview of the top 10 actions performed in the user account management. |
| User Account Password Change | The widget provides an overview of the changed user account password. |
| Locked User Account | The widget provides an overview of the locked user account due to a bad password. |
| User Account Unlocked | The widget provides an overview of the unlocked user account. |
| User Account Locked/Unlocked - Status | The widget provides an overview of the locked or unlocked user account's status by user, action, and object. |
| Newly Created Group - List | The widget provides a detailed list of a newly created group. |
| Deleted Group - List | The widget provides a detailed list of deleted groups. |
| Group User Deletion - List | The widget provides a detailed list of the users deleted or removed from a group. |
| User Added in Group | The widget provides an overview of the users added to a group. |

## 4.2 Unix Alerts

The following alerts are available in Unix:

### 4.2.1 LP_Unix Possible Bruteforce Attack

- **Trigger Condition:** An account is not present but is used repeatedly to login. This may be a brute force attack by a bot, malware, or threat agent.
- **ATT&CK Category:** Credential Access
- **ATT&CK Tag:** Brute Force
- **ATT&CK ID:** T1110
- **Minimum Log Source Requirement:** Unix
- **Query:**

```
norm_id=Unix ((label=Account label=Absent) OR (label=User label=Authentication
↪label=Fail)) user=* | chart count() as cnt by user | search cnt>10
```

### 4.2.2 LP_Unix Kernel Logging Stopped

- **Trigger Condition:** Unix Kernel stops logging that may violate the audit compliance of the organization.
- **ATT&CK Category:** Defense Evasion
- **ATT&CK Tag:** Impair Defenses, Indicator Blocking
- **ATT&CK ID:** T1562, T1562.006
- **Minimum Log Source Requirement:** Unix
- **Query:**

```
norm_id=Unix OR norm_id=Kernel label=Logging label=Stop "process"="kernel" action=
↪"stopped"
```

### 4.2.3 LP_Unix User Deleted

- **Trigger Condition:** Deletion of a user account.
- **ATT&CK Category:** Impact
- **ATT&CK Tag:** Account Access Removal
- **ATT&CK ID:** T1531
- **Minimum Log Source Requirement:** Unix
- **Query:**

```
norm_id=Unix label=User label=Account label=Management label=Delete label=Remove
↪user=*
```

### 4.2.4 LP_Unix Password Expiry Changed for User

- **Trigger condition:** Information on password expiry information is changed for a user.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Unix
- **Query:**

```
norm_id=Unix label=User label=Password label=Expire label=Account
↪label=Management label=Change user=*
```

### 4.2.5 LP_Unix Group Deleted

- **Trigger condition:** A group is deleted.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Unix

- **Query:**

```
norm_id=Unix label=Group label=Management label=Remove group=*
```

### 4.2.6 LP_Unix Security Violation

- **Trigger condition:** Security violation is detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Vmware
- **Query:**

```
norm_id=Unix label=Security label=Violation message=*
```

### 4.2.7 LP_Unix User Account Unlocked

- **Trigger condition:** Unlocked user account detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Unix
- **Query:**

```
norm_id=Unix label=User label=Account label=Management label=Unlock user=*
```

### 4.2.8 LP_Unix Excessive Denied Connection

- **Trigger condition:** An excessive denied connection from the same source is detected i.e., 100 denied connections within two minutes.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A

- **Minimum Log Source Requirement:** Unix
- **Query:**

```
norm_id=Unix label=Connection label=Deny | chart count() as cnt by source_address |
↪search cnt>100
```

### 4.2.9 LP_Unix User Removed from Privileged Group

- **Trigger condition:** A user account is removed from the privileged group. For this alert to work, you must update the list *ADMIN_GROUPS*, with the name of privileged groups.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Unix
- **Query:**

```
norm_id=Unix label=User label=Group label=Management label=Member label=Remove
↪user=* (group=admin OR group IN ADMIN_GROUPS)
```

### 4.2.10 LP_Unix Privilege Escalation Failed

- **Trigger condition:** The user account tries to escalate the privilege and fails.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Unix
- **Query:**

```
norm_id=Unix label=User label=Fail (label=Login OR label=Authentication) user=root
↪caller_user=*
```

### 4.2.11 LP_Unix User Session Alert

- **Trigger condition:** A user session detected.
- **ATT&CK Category:** N/A
- **ATT&CK Tag:** N/A
- **ATT&CK ID:** N/A
- **Minimum Log Source Requirement:** Unix
- **Query:**

```
[norm_id=Unix "successful su for" user=root user=* process_id=*] as s1 join [norm_
↪id=Unix command=exit role_id=* session_id=*] as s2 on s1.user=s2.user and s1.process_
↪id=s2.role_id |
rename s1.log_ts as start_ts, s2.log_ts as end_ts, user as User, s2.role_id as role_id, s2.
↪session_id as session_id | chart count() by start_ts, end_ts, User, role_id, session_id
```

## 4.3 Unix Labels

The following labels are available in *LP_Unix*:

| Labels | Description |
|---|---|
| Cron, Job | Events with the *pam_unix(cron:session)* message. |
| Cron, Job | Events with the */USR/SBIN/CRON* message. |
| Cron, Job | Events with the *CRON* or *cron* process. |
| NSCD | Events with the *nscd* process. |
| Successful | Events with the *Successful, Success*, or *Login successful* status. |
| Fail | Events with the *Failed, Fail, or Login failed* status. |
| Login | Events with the object in *authentication, keyboardinteractive/pam, publickey*, or *password*. |
| User, Login, Successful | Events with the *Accepted Password, Accepted publickey*, or *Session opened*. |
| User, Login, Fail | Events with the *Authentication Failure* or *Failed Password*. |
| User, Logoff | Events with the *Session closed* message. |
| User, Account, Management, Password, Change | Events with the *Password changed* message. |

Continued on next page

Table 5 – continued from previous page

| Labels | Description |
|---|---|
| User, Account, Management, Remove | Events with the *Delete user* message. |
| User, Account, Management, Create | Events with the *A new user* message. |
| Privilege, Access | Events with the *sudo* or *su* process. |
| Service, Start | Events with the *Starting* or *Start* action for all Unix services. |
| Service, Restart | Events with the *Re-starting*, *Restarting*, or *Restart* action for all Unix services. |
| Service, Stop | Events with the *Stop* or *Stopping* action for all Unix services. |
| FTP | Events with the *ftp* or *ftpd* process. |
| ssh | Events with the *sshd* process. |
| Command, Execute | Events with the Unix command. |
| Remove | Events with the *Delete* or *Deleted* action. |
| Modify | Events with the *Replace* action. |
| Start, Change, Edit | Events with the *Beign Edit* action. |
| Add | Events with the *Account added* action. |
| Remove | Events with the *Account removed* action. |

The following labels are available in *LP_Unix SSHD*:

| Labels | Description |
|---|---|
| Session, Close | Events with the *closed* action or the *closed* status. |
| Session, Open | Events with the *opened* action or the *opened* status. |

The following labels are available in *LP_Common Unix Systems*:

| Labels | Description |
|---|---|
| Open | Events with the *opened* message. |
| Close | Events with the *closed* action |
| Add | Events with the *added* action. |
| Delete | Events with the *deleted* action. |
| User, Delete | Events with the *userdel* process. |
| User, Add | Events with the *useradd* process. |
| Add | Events with the *account added* action. |
| Remove | Events with the *removed* action. |
| Successful | Events with the *successful* status. |

Continued on next page

Table 7 – continued from previous page

| Labels | Description |
|---|---|
| Fail | Events with the *failed* status. |

## 4.4 Unix Report Templates

## 4.5 Using Unix Report Templates

1. Go to *Report >> Report Template>>Vendor Report Templates*.

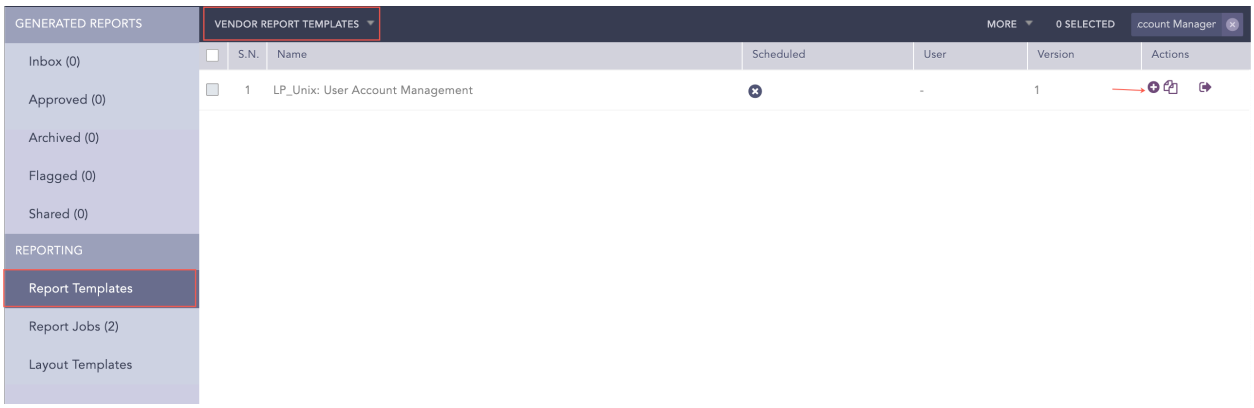



Fig. 6: Using the Unix Report Template

2. Click **Add** under the **Actions** column.

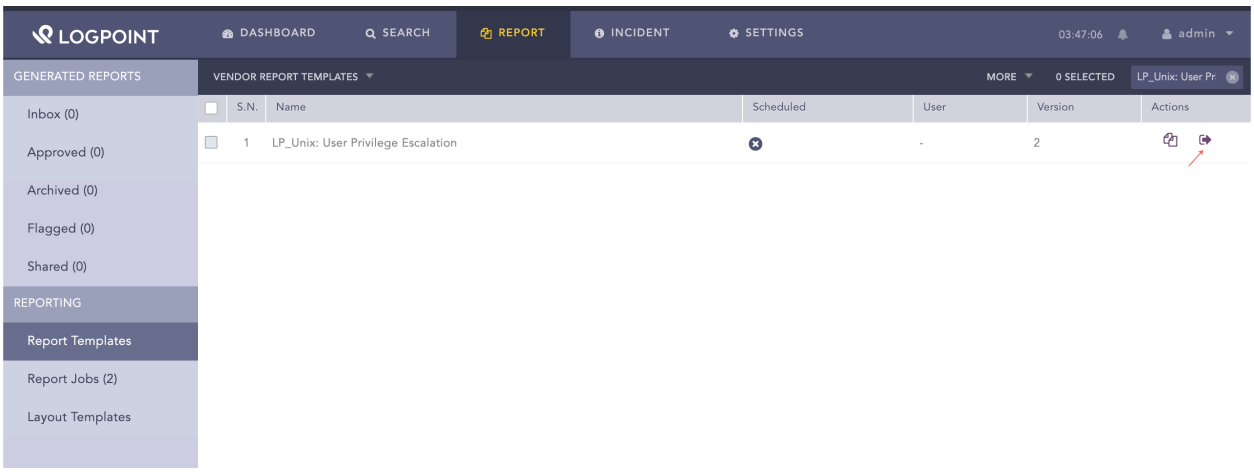



Fig. 7: Using Unix Report Template

3. Click **Run this Report** under the **Actions** column.

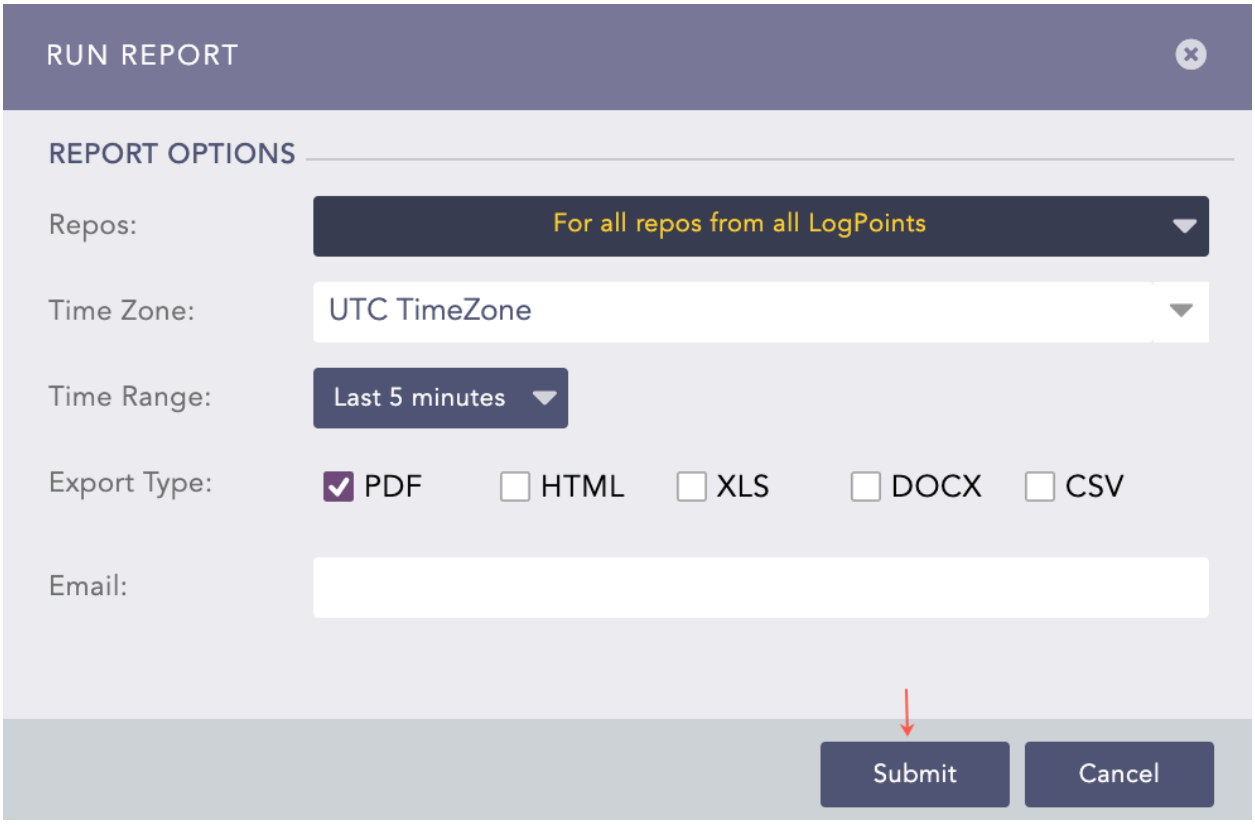



Fig. 8: Running Unix Report Template

4. Select **Repos**, **Time Zone**, **Time Range**, **Export Type**, and enter the **Email** address.
5. Click **Submit**.

You can view the reports being generated under **Report Jobs** and download the generated reports from **Inbox** with *.pdf* extension by clicking *PDF* under the **Download** section.

A report contains widgets enabling you to analyze the data in different formats like graphs, time trends, lists, and text. Reports are time-bound, which means they are incident summaries over a period of time, for example, the last 24 hours or last five minutes. While generating a report, you can customize the calendar period according to your needs. The following are the Unix report templates:

- **LP_Unix: User Privilege Escalation** is the incident summary report that provides statistical information on the session duration, commands executed, users in privilege escalation, and root privilege command execution in different formats, such as graphs and lists.
- **LP_Unix: User Account Management** is the incident summary report that provides statistical information on the user account created or deleted, activities in user

account management, user account locked or unlocked, newly created group or deleted group, and account status in different formats, such as graphs or lists.

- **LP_Unix: Authentication** is the incident summary report that provides statistical information on the successful or unsuccessful administrative logins and user login activities in different formats, such as graphs or lists.

CHAPTER

FIVE

# UNINSTALLATION

## 5.1 Uninstalling the Unix Application in LogPoint

1. Go to *Settings >> System >> Applications*.
2. Click the **Uninstall** icon under the **Actions** column.

**Note:** You must remove the **Unix** configurations to delete the application.