LOGPOINT

Integrations

Unix

V5.4.2 (latest)

CONTENTS

CHAPTER ONE

UNIX

Unix normalizes *Unix* events and enables you to analyze *Unix* data. It includes the Syslog Collector based *Linux* log source template, simplifying log source configuration with pre-defined settings. The log source template ensures consistency in collecting, processing and analyzing *Unix* logs for precise security event analysis and reporting.

Logpoint aggregates and normalizes the *Unix* logs so you can analyze the information through dashboards and security reports. Unix dashboards visualize event details for authentication requests, privilege escalation and user account management of the Unix environment detected in your network. You can further customize the data and searches to perform in-depth analysis.

You can configure Unix from *Log Source Template* or *Devices*. We recommend using the log source template.

Unix supported devices/sources are listed in Log Source.

Unix Components

1. **Dashboard Packages**

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

2. **Normalization Packages**

   - LP_Unix Dovecot
   - LP_Unix Scponly
   - LP_Unix Nullmailer
   - LP_Unix Iptables
   - LP_Unix Syscall
   - LP_Unix Ftpd
   - LP_Unix Zookeeper

- LP_Unix Vasd
- LP_Unix Etcd
- LP_Unix Rtkit
- LP_Unix SQL Query
- 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
- LP_Dell Data Domain

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 Possible DNS Server Modified
    - 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**

    - UnixSysmonCompiledNormalizer
    - 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 UNIX

Prerequisite

- Logpoint v6.7.0 or later
- Logpoint v7.4.0 or later for log source template.

To install Unix:

1. Download the .pak file from the Help Center.
2. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
3. Click **Import**.
4. **Browse** to the downloaded .pak file.
5. Click **Upload**.

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

CHAPTER

THREE

UNINSTALLING UNIX

You must remove Unix configuration to uninstall it. If configured from Devices, you must remove *Devices*, *Processing Policies* and *Normalization Policies*. Otherwise, remove all the log sources created using the Unix templates. To learn how to remove the log sources, go to Deleting Log Source.

To remove Devices:

1. Go to *Settings >> Configuration* from the navigation bar and click **Devices**.
2. Click the **Delete** icon from **Actions** of the device name for Unix.
3. Click **Yes**.

To remove Processing Policies:

If you have configured **Log Collection Policies**, you need to remove them.

1. Go to *Settings >> Configuration* from the navigation bar and click **Processing Policies**.
2. Click the **Delete** icon from **Actions** of the policy name for Unix.
3. Click **Yes**.

To remove Normalization Policies:

1. Go to *Settings >> Configuration* from the navigation bar and click **Normalization Policies**.
2. Click the **Delete** icon from **Actions** of the policy name for Unix.
3. Click **Yes**.

To uninstall Unix:

1. Go to *Settings >> System Settings* from the navigation bar and click **Applications**.
2. Click the **Uninstall** icon from **Actions** of Unix.
3. Click **Yes**.

CHAPTER

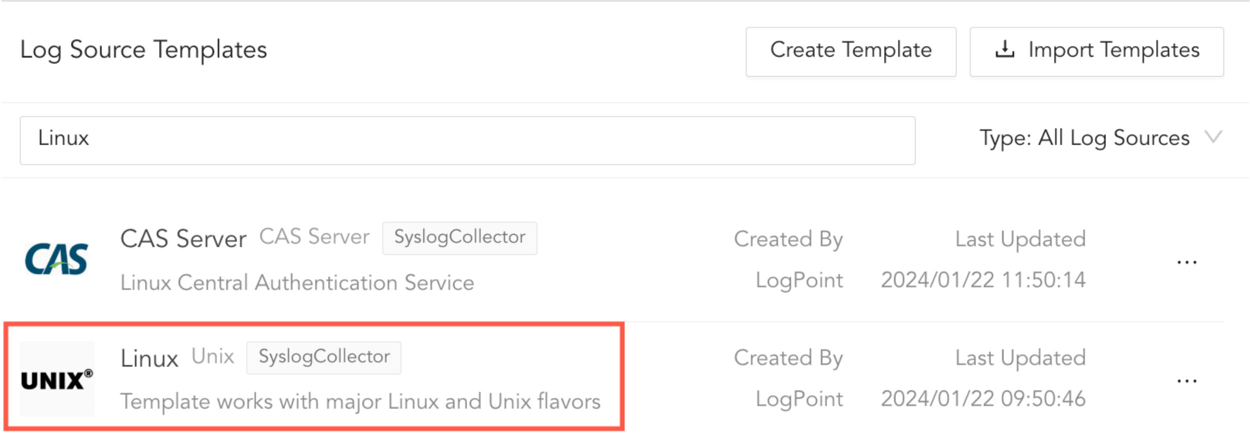
FOUR

CONFIGURING UNIX

Log sources for Unix can be configured using *Log Source Template* or *Devices*. Log Source Template is recommended to minimize setup requirements and eliminate normalization issues.

4.1 Using Log Source Template

You must create a log source using the log source template to receive the normalized *Unix* logs. Go to Creating Log Source via a Template to learn more.



CAS Server CAS Server SyslogCollector
Linux Central Authentication Service
Created By LogPoint
Last Updated 2024/01/22 11:50:14

Linux Unix SyslogCollector
Template works with major Linux and Unix flavors
Created By LogPoint
Last Updated 2024/01/22 09:50:46

Fig. 1: Selecting Linux

4.2 Using Devices

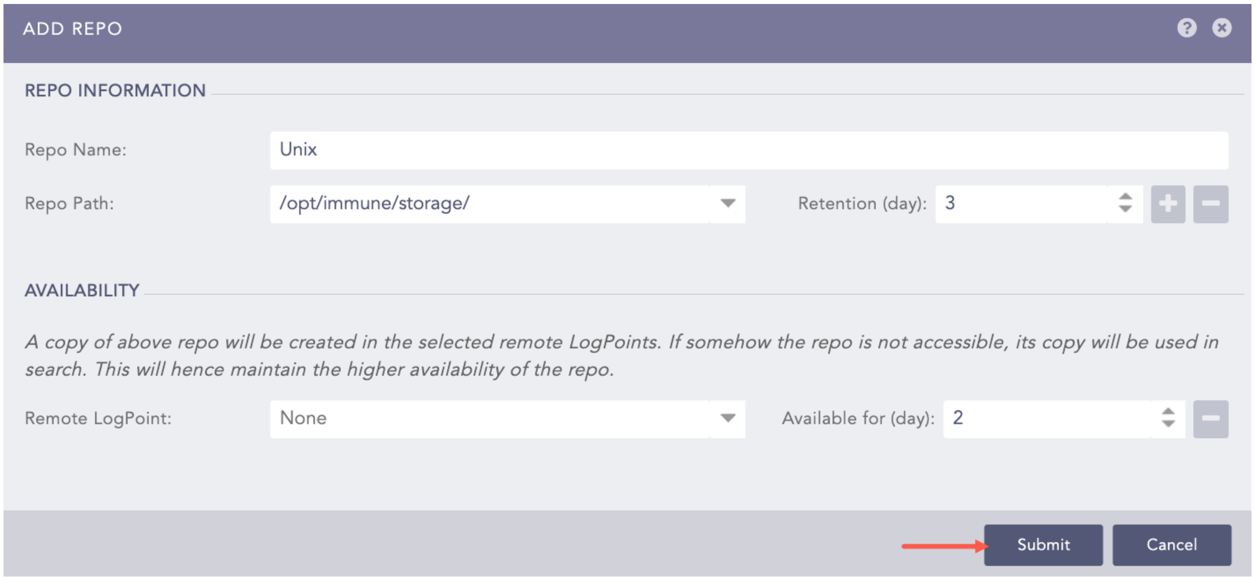
4.2.1 Configuring a Repo for Unix

1. Go to *Settings >> Configuration* from the navigation bar and click **Repos**.
2. Click **Add**.

3. Enter a **Repo Name**.
4. Select a **Repo Path** to store incoming logs.
5. Set a **Retention Day** to keep logs in a repository before they are automatically deleted.

Note: You can add and remove multiple **Repo Path** and **Retention Day**.

6. Select a **Remote LogPoint** and set a **Available for (day)**.
7. Click **Submit**.



ADD REPO

REPO INFORMATION

Repo Name: Unix

Repo Path: /opt/immune/storage/ Retention (day): 3

AVAILABILITY

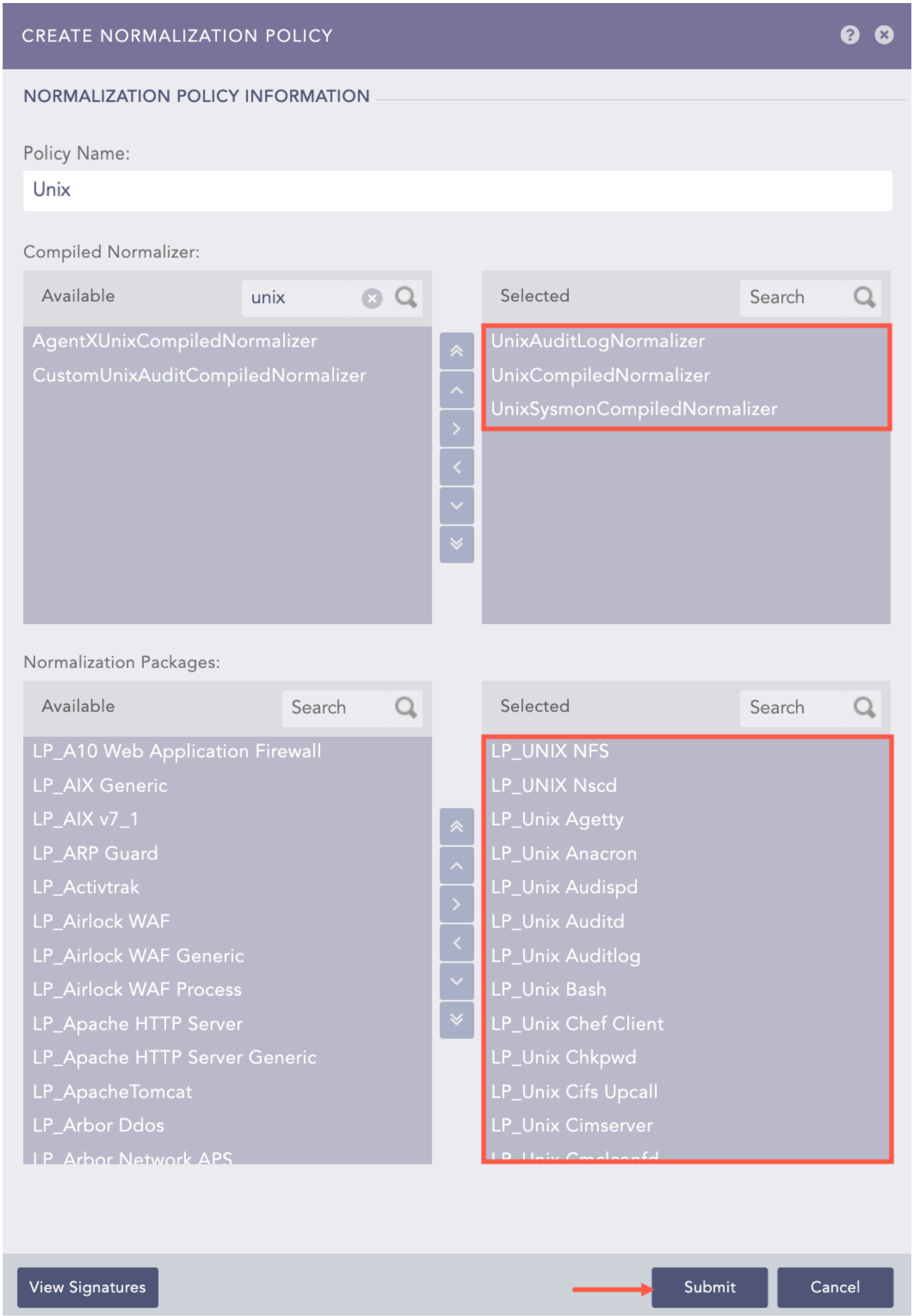
A copy of above repo will be created in the selected remote LogPoints. If somehow the repo is not accessible, its copy will be used in search. This will hence maintain the higher availability of the repo.

Remote LogPoint: None Available for (day): 2

Fig. 2: Adding a Repo

4.2.2 Adding a Normalization Policy for Unix

1. Go to *Settings >> Configuration* from the navigation bar and click **Normalization Policies**.
2. Click **Add**.
3. Enter a **Policy Name**.
4. Select the **Compiled Normalizers** and **Normalization Packages** for Unix.
5. Click **Submit**.



CREATE NORMALIZATION POLICY

NORMALIZATION POLICY INFORMATION

Policy Name: Unix

Compiled Normalizer:

Available: unix

- AgentXUnixCompiledNormalizer
- CustomUnixAuditCompiledNormalizer

Selected:

- UnixAuditLogNormalizer
- UnixCompiledNormalizer
- UnixSysmonCompiledNormalizer

Normalization Packages:

Available:

- LP_A10 Web Application Firewall
- LP_AIX Generic
- LP_AIX v7_1
- LP_ARP Guard
- LP_Activtrak
- LP_Airlock WAF
- LP_Airlock WAF Generic
- LP_Airlock WAF Process
- LP_Apache HTTP Server
- LP_Apache HTTP Server Generic
- LP_ApacheTomcat
- LP_Arbor Ddos
- LP_Arbor Network APS

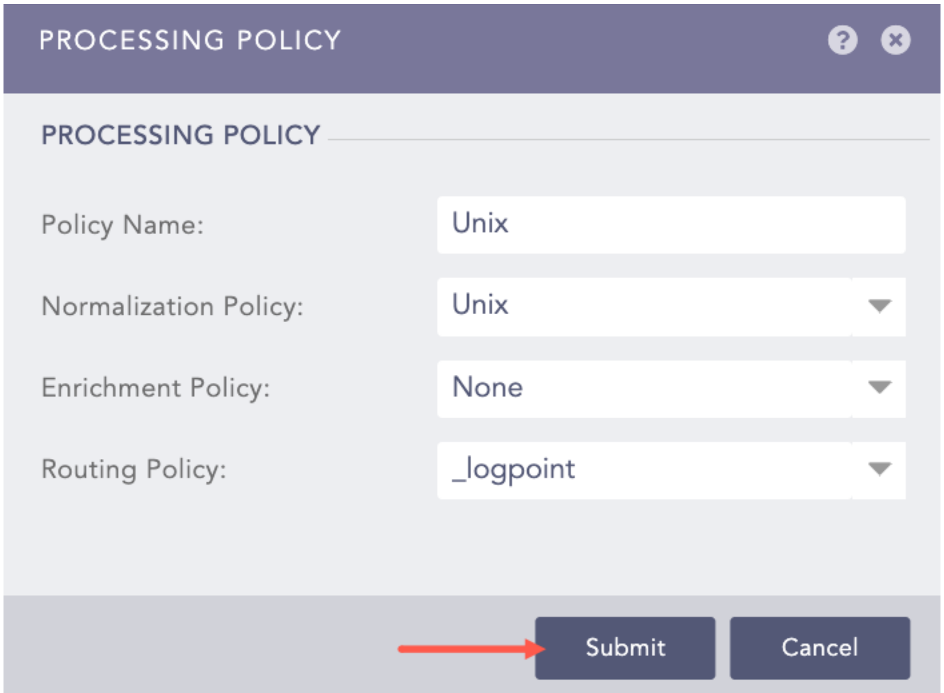
Selected:

- LP_UNIX NFS
- LP_UNIX Nscd
- LP_Unix Agetty
- LP_Unix Anacron
- LP_Unix Audispd
- LP_Unix Auditd
- LP_Unix Auditlog
- LP_Unix Bash
- LP_Unix Chef Client
- LP_Unix Chkpwd
- LP_Unix Cifs Upcall
- LP_Unix Cimserver
- LP_Unix Cmsdconfd

Fig. 3: Adding a Normalization Policy

4.2.3 Configuring a Processing Policy for Unix

1. Go to *Settings >> Configuration* from the navigation bar and click **Processing Policies**.
2. Click **Add** .
3. Enter a **Policy Name**.
4. Select the previously created **Normalization Policy**.
5. Select the **Enrichment Policy**.
6. Select the **Routing Policy**.
7. Click **Submit**.



PROCESSING POLICY

PROCESSING POLICY

Policy Name: Unix

Normalization Policy: Unix

Enrichment Policy: None

Routing Policy: _logpoint

Fig. 4: Adding a Processing Policy

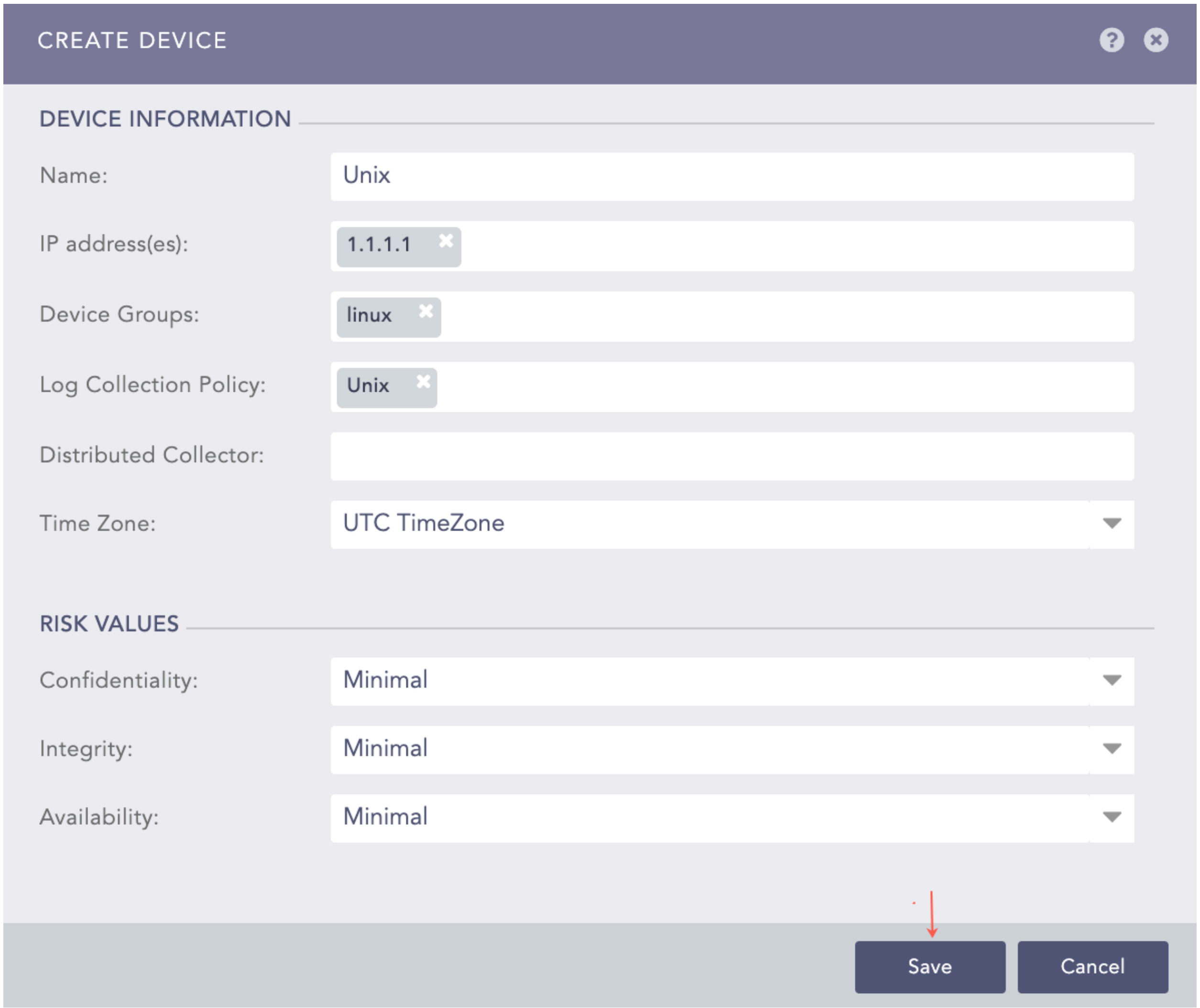
4.2.4 Adding Unix as a Device in Logpoint

1. Go to *Settings >> Configuration* from the navigation bar and click **Devices**.
2. Click **Add**.
3. Enter a device **Name**.
4. Enter the *Unix* server **IP address(es)**.

5. Select the **Device Groups**.
6. Select an appropriate **Log Collection Policy** for the logs.
7. Select a collector or a forwarder from the **Distributed Collector** drop-down.

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

8. Select a **Time Zone**. The timezone of the device must be same as 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**.



Name:	Unix
IP address(es):	1.1.1.1
Device Groups:	linux
Log Collection Policy:	Unix
Distributed Collector:	
Time Zone:	UTC TimeZone

Confidentiality:	Minimal
Integrity:	Minimal
Availability:	Minimal

Fig. 5: Creating Unix as a Device

4.2.5 Configuring the Syslog Collector for Unix

1. Go to *Settings >> Configuration* from the navigation bar and click **Devices**.
2. Click the **Add** icon from **Actions** of the previously added device.
3. Click **Syslog Collector**.

Note: You can select a different collector depending on your requirements and added device. To learn more about available collectors go to collectors. If you require assistance, contact our support team.

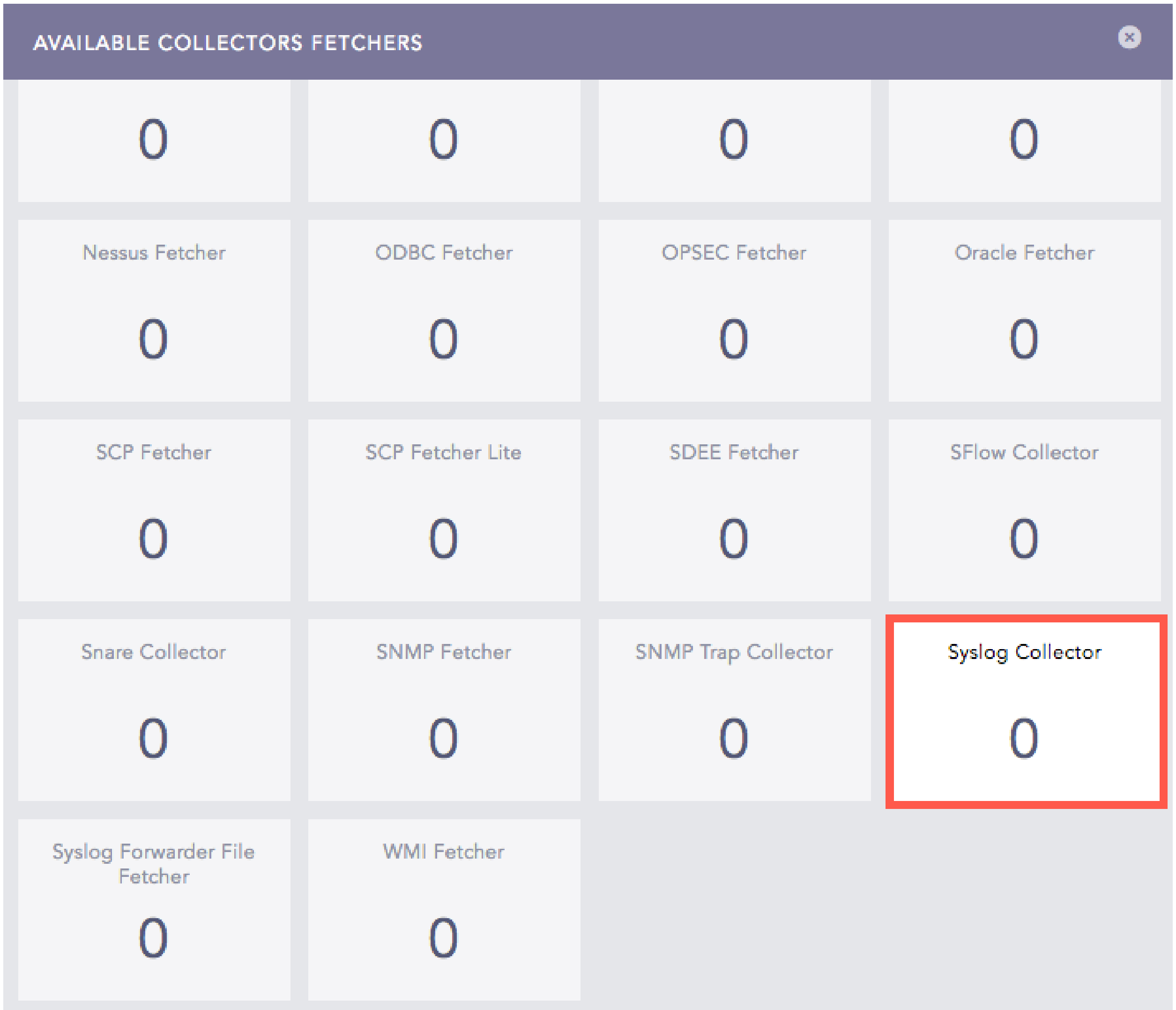
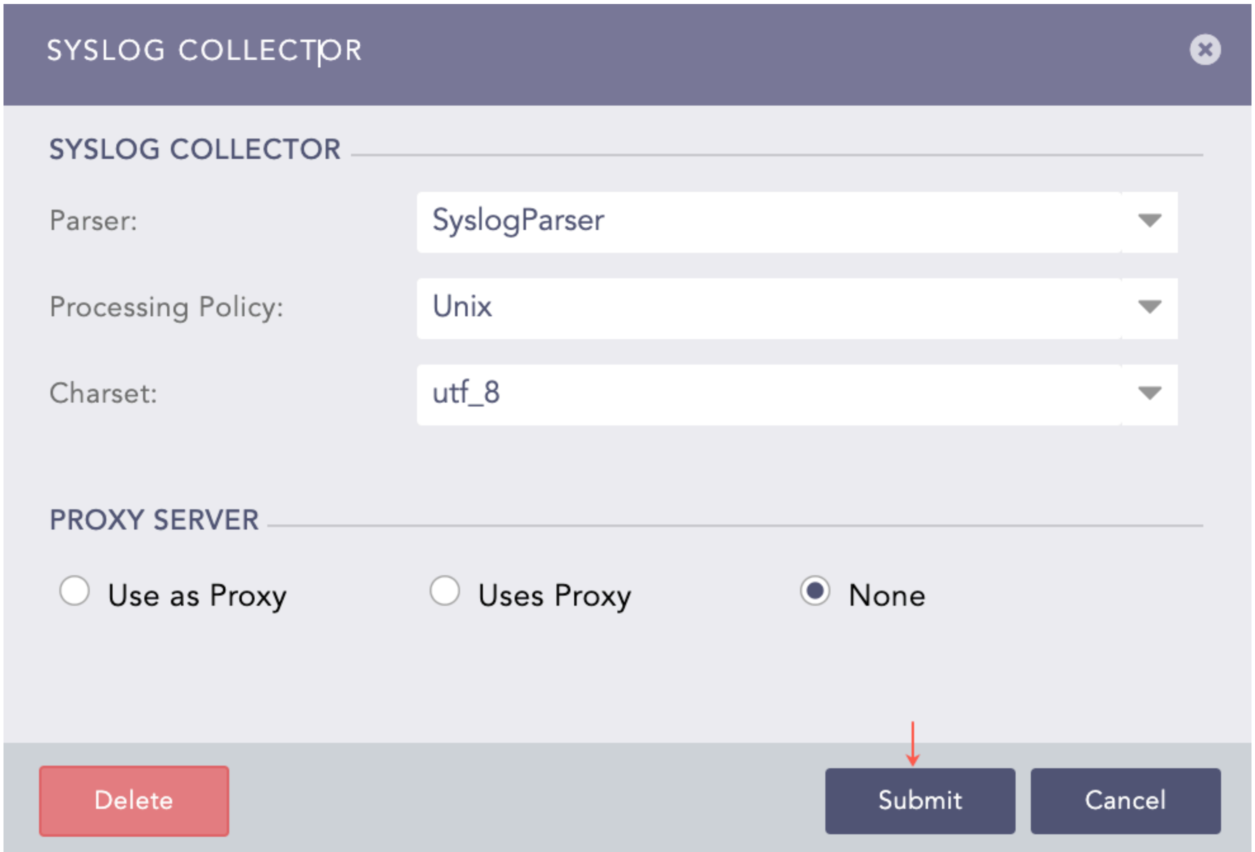


Fig. 6: Selecting a Collector

4. Select **Syslog Parser** as **Parser**.

5. Select the previously created **Processing Policy**.
6. Select the **Charset**.
7. In **Proxy Server**, select **None**
8. Click **Submit**.



SYSLOG COLLECTOR

SYSLOG COLLECTOR

Parser: SyslogParser

Processing Policy: Unix

Charset: utf_8

PROXY SERVER

○ Use as Proxy ○ Uses Proxy ● None

Fig. 7: Configuring Syslog Collector

CHAPTER

FIVE

UNIX ANALYTICS

5.1 Unix Dashboards

5.1.1 LP_Unix Overview

This dashboard consists of the following widgets:

Widget Name	Description
Top 10 Process Running	The top ten Unix processes running in the Logpoint for the administrator to see what is running, the resources that processes are using, how the system is affected by the load and how memory is being used.
Events Timetrend	A time trend of the Unix events generated based on event severity or event type to analyze the performance of Logpoint over time.
Top 10 Commands Used	The top ten most used Unix commands, such as sudo allowing direct communication with the Logpoint via a terminal, hence being very interactive and giving the user direct control over the Logpoint resources.
Top 10 Sudo Commands	The top ten sudo commands allow you to run programs with the security privileges of another user (by default, as the superuser).
Top 10 Sources in Denied Connection	The top ten denied source addresses from accessing Unix networks to protect your system.
Top 10 Users in Successful Logins	The top ten users who successfully logged in allowing the administrator to view the user account name, date and login time.

Continued on next page

Table 1 – continued from previous page

Widget Name	Description
Top 10 Users in Failed Logins	The top ten users who failed to log in indicated invalid login attempts, forgot their password or mistyped it.
Top 10 Sources in Successful User Logins	The top ten source addresses in successful user logins.
Top 10 Sources in Failed User Logins	The top ten source addresses in failed user logins.
User Login Status	The user login status may be a successful or failed login.

5.1.2 LP_Unix Privilege Escalation

This dashboard consists of the following widgets:

Widget Name	Description
Session Duration	The session duration from when a user arrives, interacts and exits a Unix system.
Root Privilege Command Execution	The commands executed that require permissions not granted to a standard UNIX user account. These commands include root session start timestamp, root session end timestamp, user, command execute timestamp and command.
Top 10 Users in Privilege Escalation	The top ten users who gained unauthorized admin or root level privileges in a Unix system. It enables the administrator to discover opportunities to improve the Unix privilege management and security to reduce the risk of a cyber attack.
Top 10 Command Executed	The top ten executed Unix commands that administrators check for successful execution.

5.1.3 LP_Unix:Authentication

This dashboard consists of the following widgets:

Widget Name	Description
Top 10 Successful Administrative Logins	The top ten successful administrative logins with rights to control or restrict the activity of other users. You need a list of ADMINS to run this query.
Top 10 Users in Successful Login	The top ten users with valid credentials successfully logged in to gain access to the Unix system.
Users in Successful Login - List	The list of successful users logins using valid user credentials, action and source address.
Top 10 Users in Failed Login	The top ten users with invalid or expired credentials failed to login so administartor can trace the source of the login attempts and a sign of brute force attack.
Users in Failed Login - List	The list of failed user logins by a user, action and source address.
Top 10 Failed Administrative Logins	The top ten administrative users (ADMINS, root or administrator) failed login attempts as the Unix system didn't recognize the authentication details. You need a list of ADMINS to run this query.
Top 10 User Login Activities	The top ten successful or failed login activities so the administrator better determines which user behavior is legitimate to prevent brute force attacks in the Unix system.

5.1.4 LP_Unix:User Account Management

This dashboard consists of the following widgets:

Widget Name	Description
Created Accounts - List	The list of created accounts to access the Unix system or any service running on the Unix system for an administrator to authenticate, trace, log and monitor its services.
User Accounts Created	The created user accounts with a user name and password and assigned permission levels.
User Accounts Deleted	The deleted user accounts barred from accessing data, services, systems and network resources.

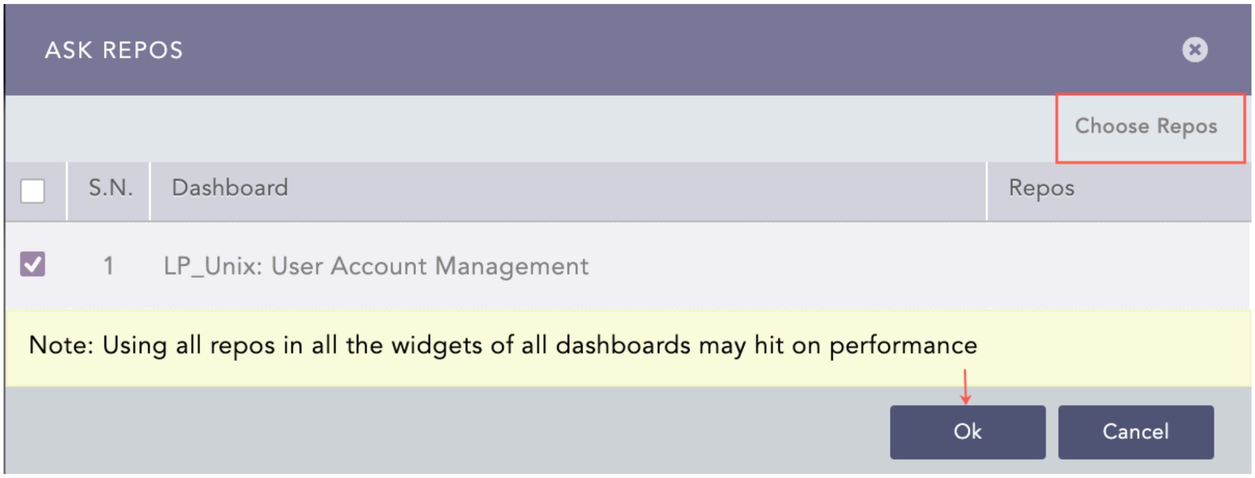
Continued on next page

Table 4 – continued from previous page

Widget Name	Description
Activities in User Account Management	The activities in the user account management, such as user adds or group adds. It allows administrators to group users and define flexible access policies.
Activities in User Account Management - List	The list of activities in user account management by user and action.
Top 10 Actions in User Account Management	The top ten actions performed in the user account management.
User Account Password Change	The changed user account password to ensure account security, prevent the default password problem and for the administrator to authenticate the user.
Locked User Account	The locked user account when the number of incorrect password entries exceeds the maximum number allowed by the account password policy.
User Account Unlocked	Accounts reset by an administrator.
User Account Locked/Unlocked - Status	The locked or unlocked user account's status by user, action and object.
Newly Created Group - List	The list of a newly created group in Unix.
Deleted Group - List	The list of deleted groups from Unix.
Group User Deletion - List	The users deleted or removed from a group in Unix.
User Added in Group	The users added to a group in Unix.

5.1.5 Adding the Unix Dashboards

1. Go to *Settings >> Knowledge Base* from the navigation bar and click **Dashboards**.
2. Select **VENDOR DASHBOARD** from the drop-down.
3. Click the **Use** icon from **Actions** of the required dashboard.
4. Click **Choose Repos**.

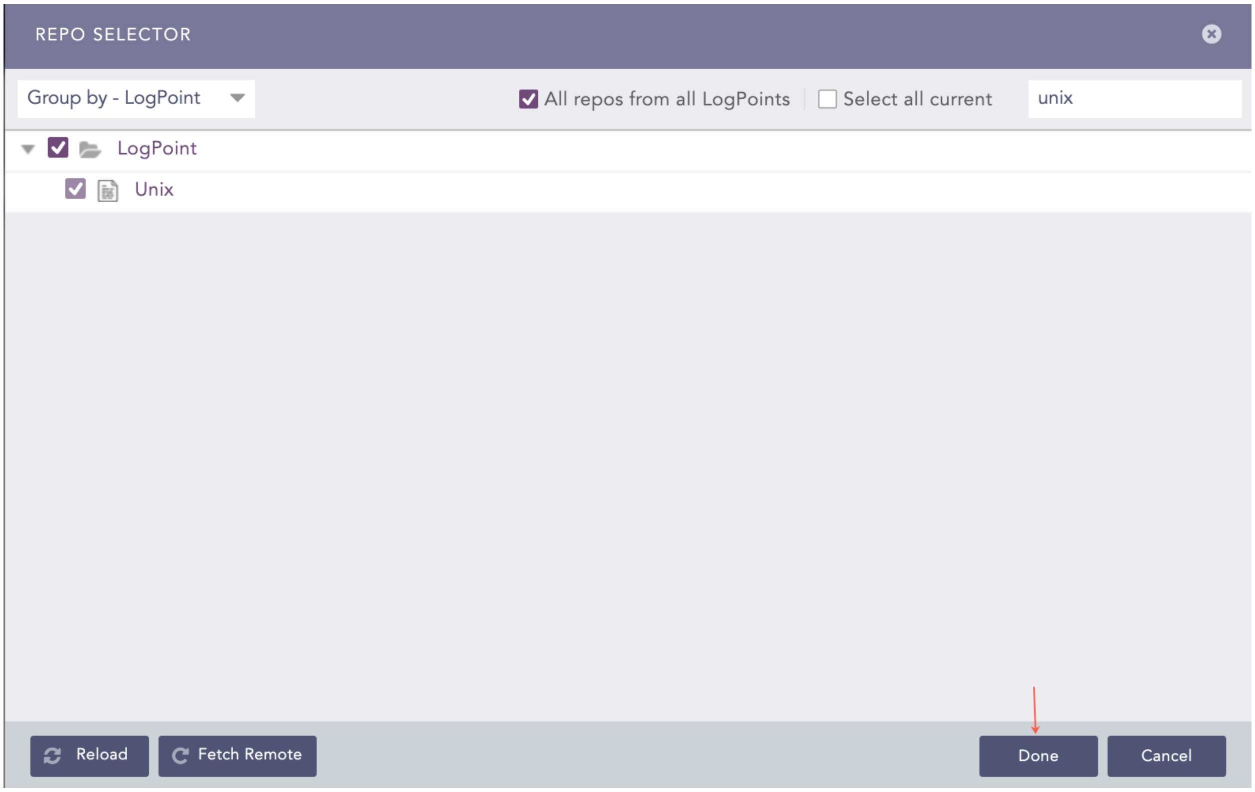


□	S.N.	Dashboard	Repos
☑	1	LP_Unix: User Account Management	

Note: Using all repos in all the widgets of all dashboards may hit on performance

Fig. 1: Selecting a Repo

5. Select the *repo configured* to store the Unix logs and click **Done**.



☑ All repos from all LogPoints □ Select all current unix

☑ LogPoint
☑ Unix

Fig. 2: Selecting a Repo

6. Select the dashboard and click **Ok**.

You can find the Unix dashboards under **Dashboards**.

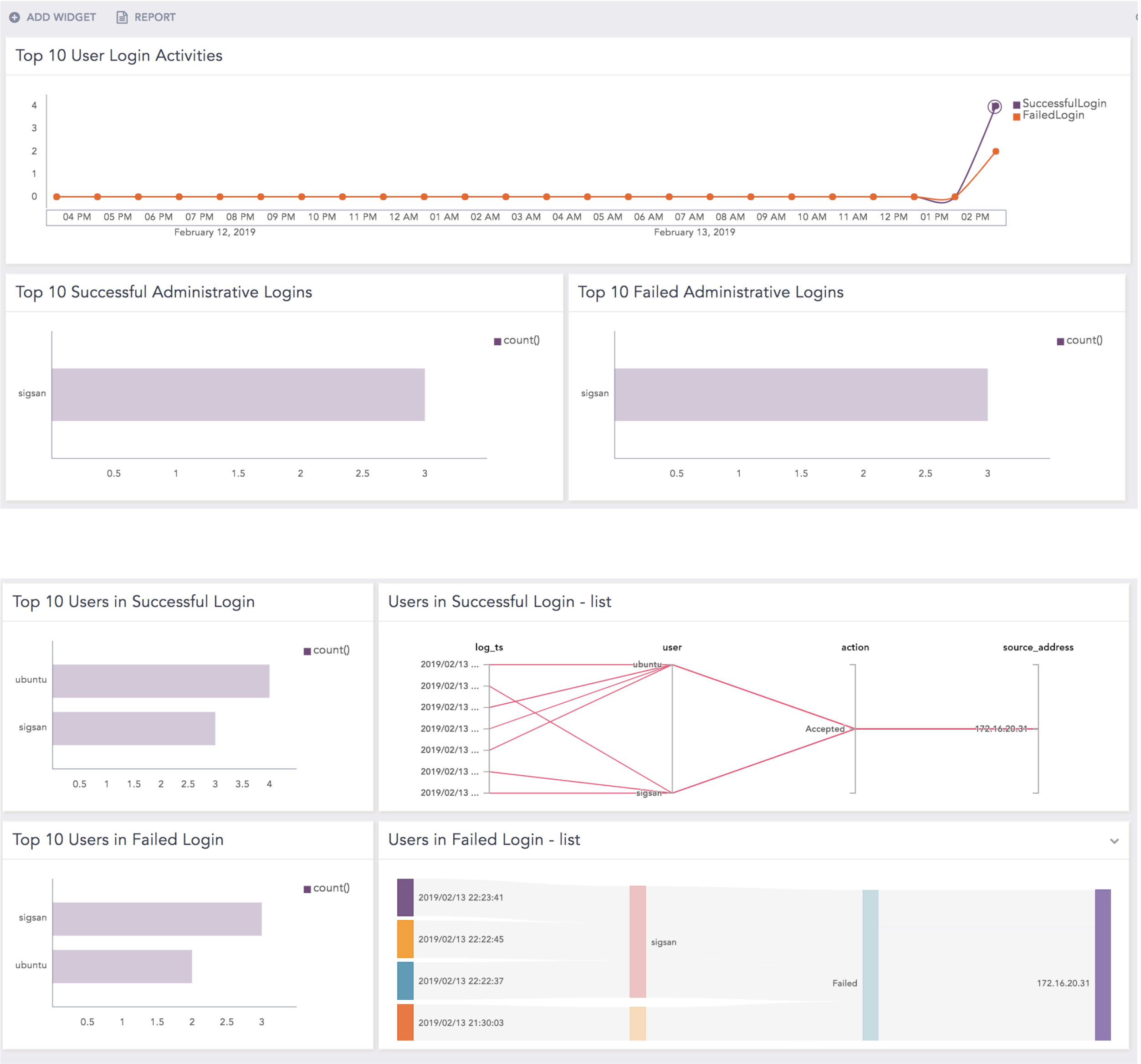


Fig. 3: Unix Dashboard

5.2 Unix Alerts

Alerts available in Unix are:

5.2.1 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
```

5.2.2 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"
```

5.2.3 LP_Unix User Deleted

- **Trigger Condition:** A user account is deleted.
- **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=*
```

5.2.4 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=*
```

5.2.5 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=*
```

5.2.6 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
```

5.2.7 LP_Unix Possible DNS Server Modified

- **Trigger condition:** Unauthorized default Application Layer Protocol and DNS server modification is 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=File label=Info label=Path (path="/etc/resolv.conf" OR path="/etc/hosts")
```

5.2.8 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 OR label=Delete) group=*
```

5.2.9 LP_Unix User Session Alert

- **Trigger condition:** Authentication for a user is successful and session of a previous user is exited.
- **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=Login label=Open label=Session label=Successful label=User
↪label=Start) OR (norm_id=Unix label=Session label=User)
```

5.2.10 LP_Unix User Removed from Privileged Group

- **Trigger condition:** A user account is removed from the privileged group.
- **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 label=User
↪(group=sudo)
```

5.3 Unix Labels

Labels available in *LP_Unix* are:

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.
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.

Labels available in *LP_Unix SSHD* are:

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

Labels available in *LP_Common Unix Systems* are:

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.
Fail	Events with the *failed* status.

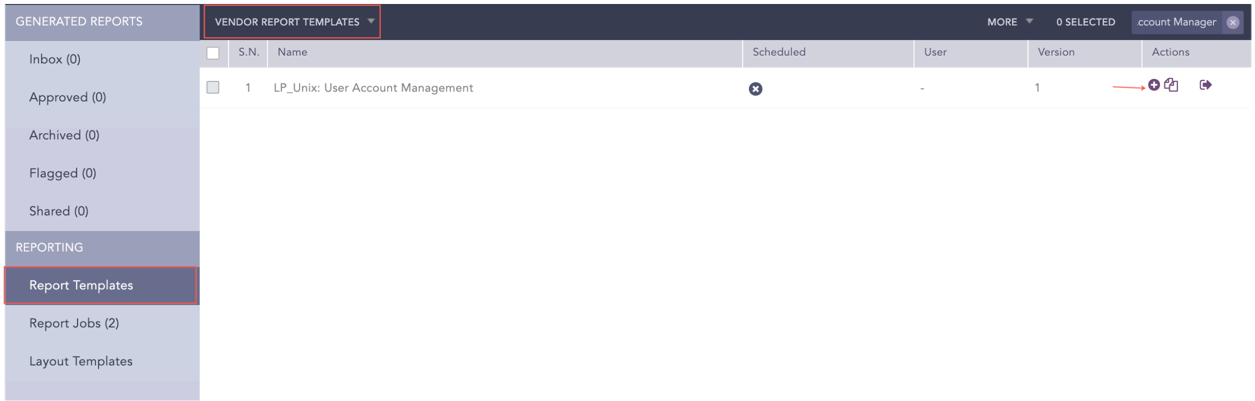
Labels available in *LP_Unix Systemd* are:

Labels	Description
Session, Start	Session start events.

5.4 Unix Report Templates

5.4.1 Using Unix Report Templates

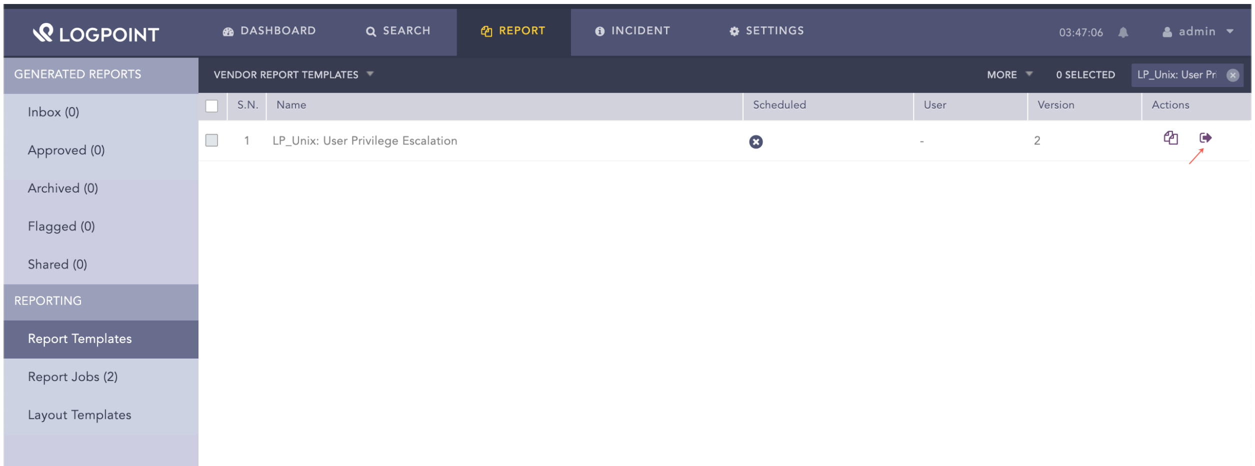
1. Go to *Report >> Report Template >> Vendor Report Templates*.



S.N.	Name	Scheduled	User	Version	Actions
1	LP_Unix: User Account Management	⊗	-	1	

Fig. 4: Using the Unix Report Template

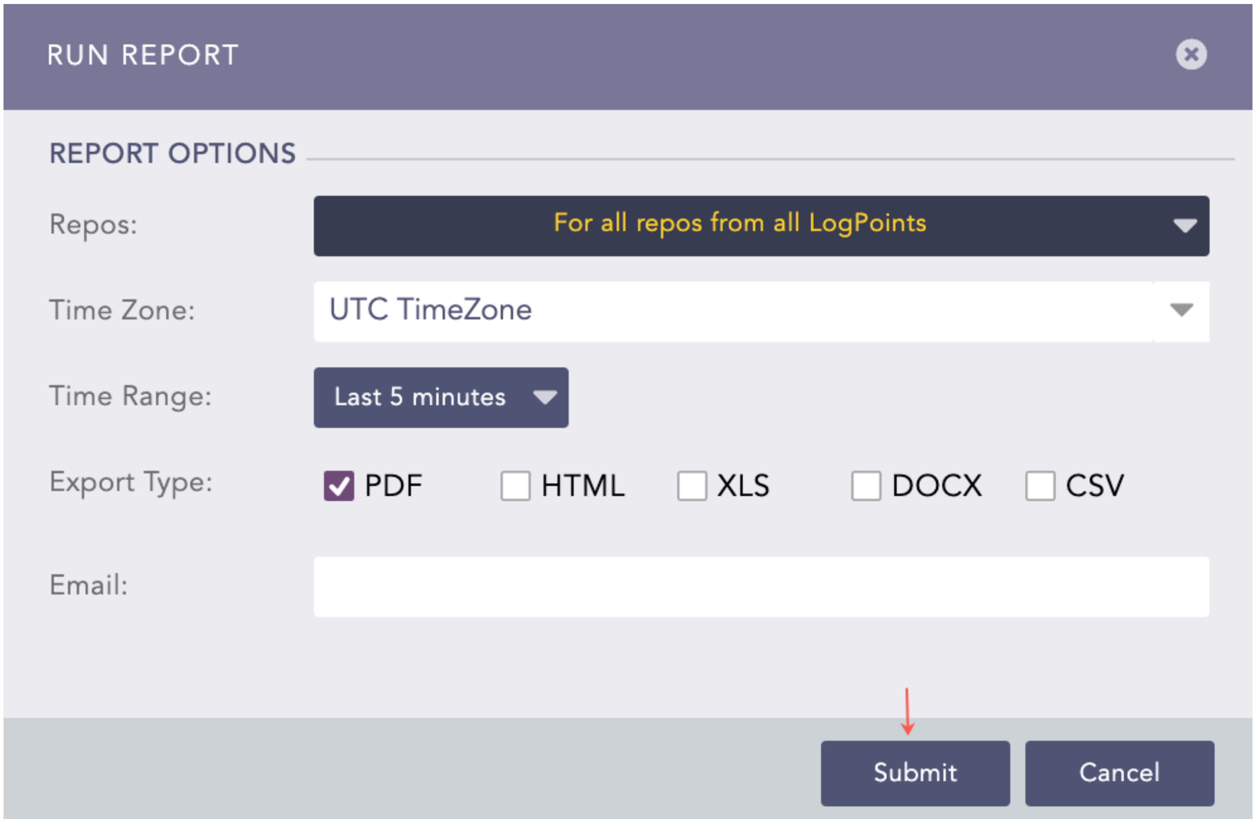
2. Click **Add** from the **Actions** column.



S.N.	Name	Scheduled	User	Version	Actions
1	LP_Unix: User Privilege Escalation	⊗	-	2	

Fig. 5: Using Unix Report Template

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



RUN REPORT

REPORT OPTIONS

Repos: For all repos from all LogPoints

Time Zone: UTC TimeZone

Time Range: Last 5 minutes

Export Type: ☑ PDF □ HTML □ XLS □ DOCX □ CSV

Email:

Fig. 6: 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.

Report templates available for Unix are:

- **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 formed 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

SIX

EXPECTED LOG SAMPLES

Unix Nullmailer

```
<30>Nov 16 05:01:50 xxx nullmailer-send[515886]: Rescanning queue.
```

Unix Scponly

```
<86>Nov 16 04:07:59 xxx scponly[1710658]: running: /usr/lib64/misc/sftp-server (username:
↪c10005(10005), IP/port: 1.1.1.1 59774 22)
```

Unix Dovecot

```
<22>Jan 03 09:18:08 daserver dovecot[609314]: imap-login: Login: user=
↪<MESSAGEIDORMAIL@example.com>, method=PLAIN, rip=1.1.1.1, lip=1.1.1.2,
↪mpid=977535, TLS, session=<HNTJkOPQD82sFgBz> <22>Jan 03 04:06:07 daserver
↪dovecot[609314]: imap-login: Login: user=<MESSAGEIDORMAIL@example.com>,
↪method=PLAIN, rip=1.1.1.3, lip=1.1.1.4, mpid=735023, secured, session=<a4/vNN/QLNd/
↪AAAB>
```

IPtable

```
<30>Apr 2116:23:01 xxxxx iptables.init[22335]: iptables: Setting chains to policy ACCEPT: filter [
↪OK ]
```

Meinberg NTP Server

```
Sep 7 21:11:39 xxxxx ntpd[7782]: proto: precision = 1.938 usec Mar 15 13:35:17 xxxxx
↪ntpd[12948]: precision = 3.000 usec
```

Unix Sysmon

```
<14>Oct 15 10:29:40 server-hostname-abc sysmon: <Event><System><Provider Name="Linux
↪Sysmon" Guid="{xxxxxxxxxxxxxxxxxxxxxxxxxxx}"/><EventID>3</EventID><Version>5</
↪Version><Level>4</Level><Task>3</Task><Opcode>0</Opcode><Keywords>
↪0x8000000000000000</Keywords><TimeCreated SystemTime="2021-10-15T10:29:40.
↪544390000Z"/><EventRecordID>12345</EventRecordID><Correlation/><Execution
↪ProcessID="15341" ThreadID="15352"/><Channel>Linux-Sysmon/Operational</Channel>
↪<Computer>server-hostname-abc</Computer><Security UserId="0"/></System>
↪<EventData><Data Name="RuleName">-</Data><Data Name="UtcTime">2021-10-15
↪10:29:40.541</Data><Data Name="ProcessGuid">{xxxx-xxxxx-xxxx-xxx-xxxx}</Data><Data
↪Name="ProcessId">1267</Data><Data Name="Image">/opt/ds_agent/ds_am</Data>
↪<Data Name="User">-</Data><Data Name="Protocol">udp</Data><Data Name=
↪"Initiated">true</Data><Data Name="SourceIsIpv6">false</Data><Data Name="SourceIp
```

(continues on next page)

(continued from previous page)

Unix Named

```
Aug 29 15:33:13 xxxxx named[464]: client 1.1.1.1#1036: query (cache) denied
```

Unix Xrdp

```
<30>Nov 28 16:11:02 xxx xrdp[28904]: [INFO ] Using default X.509 certificate: /etc/xrdp/cert.
↪pem <30>Nov 28 16:12:52 xxx xrdp[28941]: [INFO ] Using default X.509 key file: /etc/xrdp/key.
↪pem
```

Unix Solaris OS

```
Jul 2 09:30:52 xxx Had[1906]: [ID 702911 daemon.notice] VCS ERROR V-16-1-40174 TargetCount
↪dropped below zero for group xxxxx; setting to zero.
```

Unix Log

Expected Log Format

```
<datetime> <hostname> <process>[<process_id>]: <message_part>
```

Modified Log Format

```
<datetime> <hostname> <process> <process_id> - - <message_part>
```

```
2020-05-13T15:33:21.038630+03:00 xxxxx snmpd 56789 - - Connection from UDP: [1.1.1.1]:12345-
↪>[1.1.1.2]:123
```

Common Unix System

```
Jul 23 06:27:39 xxxxx? su[9233]: FAILED su for xxxxx by xxxxx
```

Unix SSHD

```
<166>Jun 2 14:41:27 ssss sshd[39844]: Starting session: shell on pts/0 for ddddd from 192.168.
↪12.6 port 59021 id 0
```

Unix Cron

```
[86]1 2020-05-13T15:25:01.256154+03:00 myserver-1 CRON 1357 - - pam_unix(cron:session):
↪session opened for user root by (uid=0)
```

Unix SU

```
<86>Jul 5 10:30:51 xxxxx su: pam_unix(su:session): session closed for user xxxxx
```

Unix Sudo

```
<85>Apr 19 08:58:13 xxxxx sudo: pam_unix(sudo:auth): authentication failure; logname=xxxxx
↪uid=603 euid=0 tty=/dev/pts/0 ruser=xxxxx rhost= user=xxxxx
```

Unix Crond

```
10.177.145.50/10.177.145.50 crond[11814]: xxxx_xxx[11814]: keytab: FILE:/etc/xxxxx.xxxxx
```

Unix Bash

```
10.177.145.50/10.177.145.50 crond[11814]: xxxx_xxx[11814]: keytab: FILE:/etc/xxxxx.xxxxx
```

Unix Passwd

```
<85>Jun 21 17:12:27 xxxxx passwd: pam_unix(passwd:************): password changed for xxxxx
```

Unix Auditd

```
<29>Nov 6 01:00:01 eru062 auditd[2908]: Audit daemon rotating log files
```

Unix Auditd Enriched

```
<13>Fri 26 05:31:58 ubuntu type=SYSCALL msg=audit(1645418719.167:47531): arch=c000003e
↪syscall=42 success=yes exit=0 a0=e a1=c0000f62ec a2=10 a3=7f512a7fbe50 items=0 ppid=1
↪pid=85231 auid=4294967295 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0
↪tty=(none) ses=4294967295 comm="filebeat" exe="/usr/share/filebeat/bin/filebeat" key=
↪"network_connect_4"ARCH=x86_64 SYSCALL=connect AUID="unset" UID="root" GID=
↪"root" EUID="root" SUID="root" FSUID="root" EGID="root" SGID="root" FSGID="root"
```

Unix Bash

```
May 23 16:55:41 xxxxx bash[31854]: xxxxx(7320):xxxxx(12345): df
```

Unix Runuser

```
<86>runuser: pam_unix(runuser-l:session): session opened for user xxxxx by (xxxxx)
```

Unix Smbd

```
<27>Apr 2 23:59:04 xxxxx smbd[28739]: nt_printing_init: error checking published printers:
↪WERR_ACCESS_DENIED
```

Unix Systemd

```
<30>Apr 26 11:08:00 xxxxx systemd: Starting Cleanup of Temporary Directories...
```

Unix Systemd

```
<30>Apr 26 11:08:00 xxxxx systemd: Starting Cleanup of Temporary Directories...
```