

Integrations

Unix

V5.2.1

CONTENTS

1	Unix	1
2	Installing Unix	6
3	Configuring Unix	7
3.1	Adding a Normalization Policy for Unix	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	15
4.2	Unix Alerts	18
4.2.1	LP_Unix Possible Bruteforce Attack	18
4.2.2	LP_Unix Kernel Logging Stopped	18
4.2.3	LP_Unix User Deleted	19
4.2.4	LP_Unix Password Expiry Changed for User	19
4.2.5	LP_Unix User Account Unlocked	19
4.2.6	LP_Unix Excessive Denied Connection	20
4.2.7	LP_Unix Possible DNS Server Modified	20
4.2.8	LP_Unix Group Deleted	21
4.2.9	LP_Unix User Session Alert	21
4.2.10	LP_Unix User Removed from Privileged Group	21
4.3	Unix Labels	22
4.4	Unix Report Templates	24
4.5	Using Unix Report Templates	24
5	Uninstalling Unix	27
6	Log Samples	28

UNIX

Unix allows you to monitor and identify threats in your organization using Unix data. LogPoint aggregates and normalizes the Unix logs so you can analyze the information through dashboards and security reports. Unix dashboards and reports provide visualization of event details for authentication requests, privilege escalation, and user account management of the Unix environment detected in your network.

Unix consists of the following 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 Etc
- 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 lpmserver
- 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 Cmcldconfd
- 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 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

INSTALLING UNIX

Prerequisite

LogPoint v6.7.4 or later

To install Unix:

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

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

CONFIGURING UNIX

3.1 Adding a Normalization Policy for Unix

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

CREATE NORMALIZATION POLICY

NORMALIZATION POLICY INFORMATION

Policy Name:

Compiled Normalizer:

Available		Selected
Unix	⬆	UnixAuditLogNormalizer
	⬆	
	⬆	
	⬆	
	⬆	
	⬆	
	⬆	

Normalization Packages:

Available		Selected
Cas Server	⬆	
LP_A10 Web Application Firewall	⬆	
LP_AIX Generic	⬆	

View Signatures **Submit** Cancel

Fig. 1: Adding a Normalization Policy

3.2 Adding Unix as a Device in LogPoint

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

CREATE DEVICE?×

DEVICE INFORMATION

Name:

Unix

IP address(es):

1.1.1.1 ×

Device Groups:

linux ×

Log Collection Policy:

Unix ×

Distributed Collector:

Time Zone:

UTC TimeZone ▼

RISK VALUES

Confidentiality:

Minimal ▼

Integrity:

Minimal ▼

Availability:

Minimal ▼

Save

Cancel

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 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**.

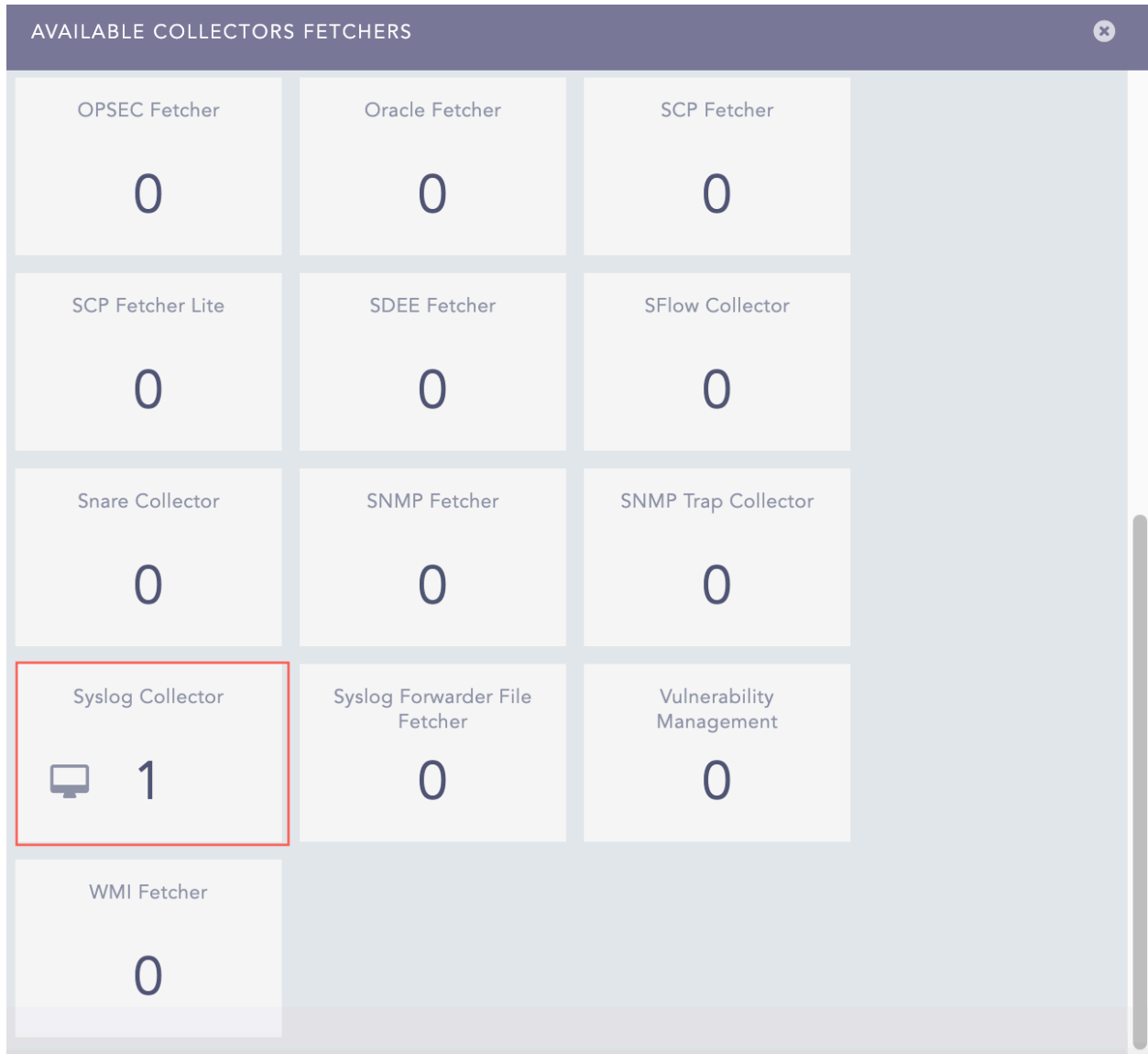


Fig. 3: Available Collectors Fetchers Panel

2. Select the **Syslog Parser**.
3. Select the **Processing Policy** which contains the previously added *normalization policy*.
4. Select the **Charset**.
5. In **PROXY SERVER**, click **None**.
6. Click **Submit**.

SYSLOG COLLECTOR

SYSLOG COLLECTOR

Parser:
SyslogParser

Processing Policy:
Unix

Charset:
utf_8

PROXY SERVER

☐ Use as Proxy
☐ Uses Proxy
☒ None

Delete

Submit

Cancel

Fig. 4: Configuring Syslog Collector

3.3. Configuring the Syslog Collector for Unix

12

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** from the **Actions** column.

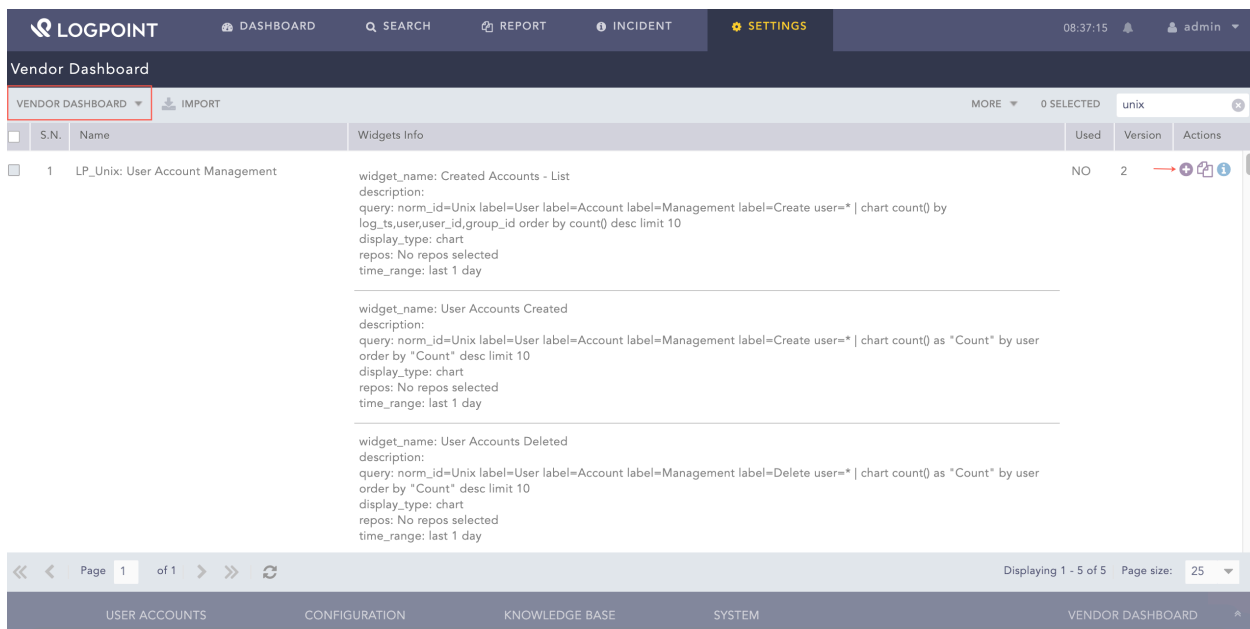


Fig. 1: Adding the Unix Dashboard

3. Click **Choose Repos**.

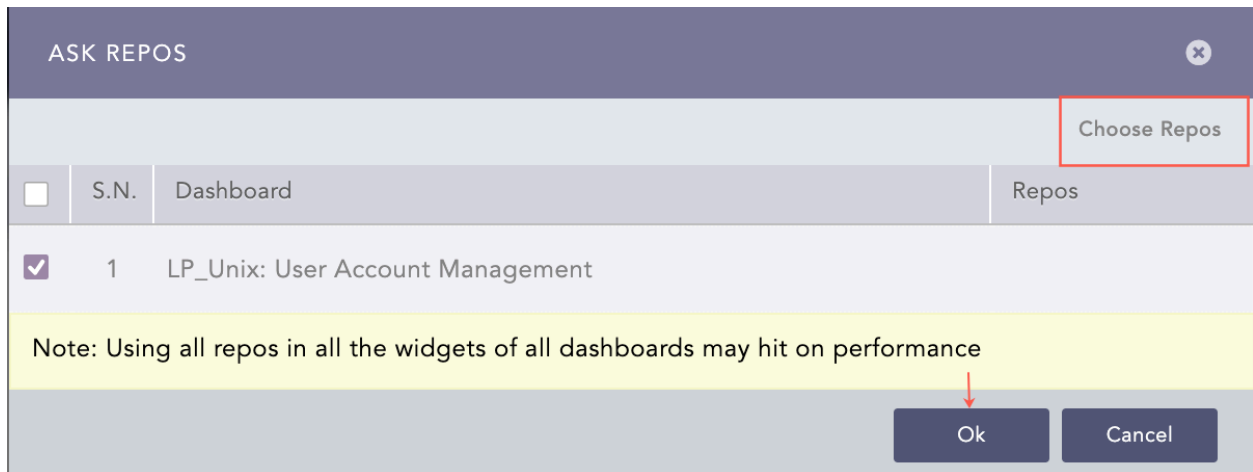


Fig. 2: Selecting a Repo

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

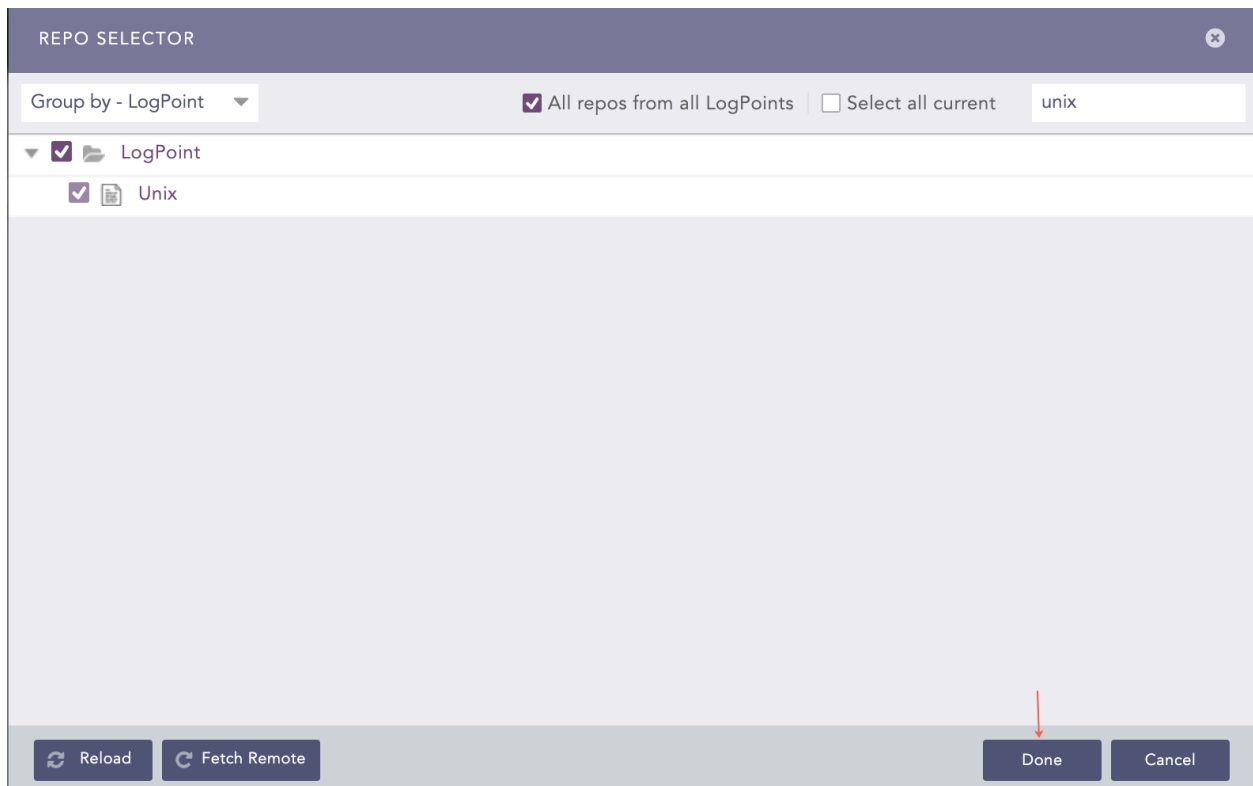


Fig. 3: Selecting a Repo

5. Click **Ok**.

You can find the Unix dashboards under *Dashboards*.

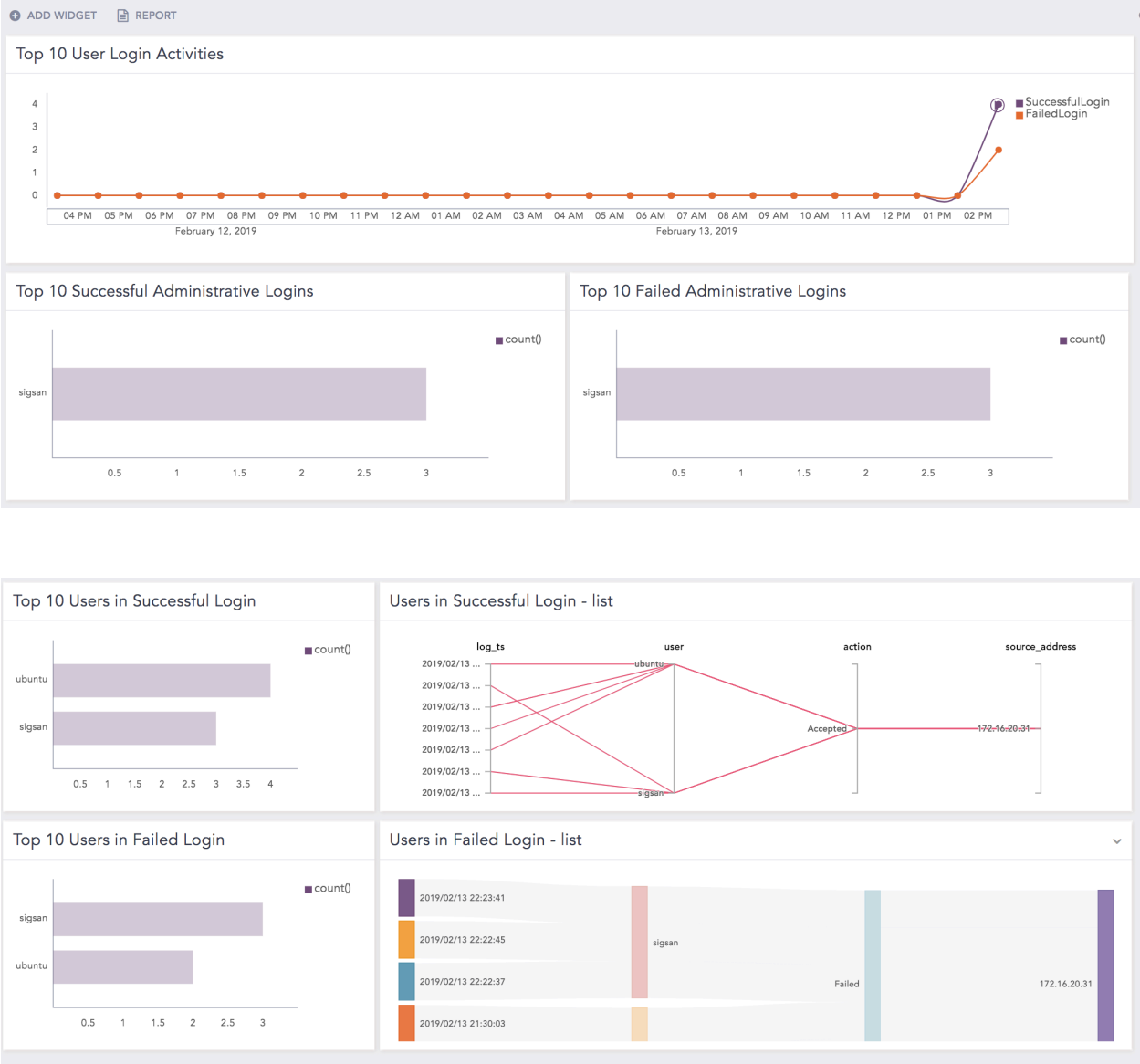


Fig. 4: Unix Dashboard

4.1.2 Unix Widgets

Widgets available in *LP_Unix Overview* provide:

Widget Name	Description
Top 10 Process Running	An overview of the top 10 Unix processes, such as parents or child process, zombie or orphan process, or list running process.
Events Timetrend	A time trend of the Unix events.

Continued on next page

Table 1 – continued from previous page

Widget Name	Description
Top 10 Commands Used	An overview of the top 10 most used Unix commands, such as sudo.
Top 10 Sudo Commands	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	An overview of the top 10 denied source addresses.
Top 10 Users in Successful Logins	An overview of the top 10 users who successfully logged in.
Top 10 Users in Failed Logins	An overview of the top 10 users who failed to log in.
Top 10 Sources in Successful User Logins	An overview of the top 10 source addresses in successful user logins.
Top 10 Sources in Failed User Logins	An overview of the top 10 source addresses in failed user logins.
User Login Status	An overview of the user login status, which may be a successful login or failed login.

Widgets available in *LP_Unix Privilege Escalation* provide:

Widget Name	Description
Session Duration	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	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	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	An overview of the top 10 executed Unix commands.

Widgets available in *LP_Unix:Authentication* provide:

Widget Name	Description
Top 10 Successful Administrative Logins	An overview of the top 10 successful administrative logins. You need a list of ADMINS to run this query.
Top 10 Users in Successful Login	An overview of the top 10 users who logged in successfully.
Users in Successful Login - List	A detailed list of the successful user logins by a user, action, and source address.
Top 10 Users in Failed Login	An overview of the top 10 users who failed to log in successfully.
Users in Failed Login - List	A detailed list of the failed user logins by a user, action, and source address.
Top 10 Failed Administrative Logins	An overview of the top 10 admin users who could not log in successfully. You need a list of ADMINS to run this query.
Top 10 User Login Activities	An overview of the top 10 successful user activities, such as successful login or failed login.

Widgets available in *LP_Unix:User Account Management* provide:

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

4.2 Unix Alerts

Alerts available in Unix are:

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:** 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=*
```

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 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=*
```

4.2.6 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
```

4.2.7 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")
```

4.2.8 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=**

4.2.9 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)*

4.2.10 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)
```

4.3 Unix Labels

Labels available in *LP_Unix* are:

Labels	Description
Cron, Job	Events with the <i>pam_unix(cron:session)</i> message.
Cron, Job	Events with the <i>/USR/SBIN/CRON</i> message.
Cron, Job	Events with the <i>CRON</i> or <i>cron</i> process.
NSCD	Events with the <i>nscd</i> process.
Successful	Events with the <i>Successful</i> , <i>Success</i> , or <i>Login successful</i> status.
Fail	Events with the <i>Failed</i> , <i>Fail</i> , or <i>Login failed</i> status.
Login	Events with the object in <i>authentication</i> , <i>keyboardinteractive/pam</i> , <i>publickey</i> , or <i>password</i> .
User, Login, Successful	Events with the <i>Accepted Password</i> , <i>Accepted publickey</i> , or <i>Session opened</i> .
User, Login, Fail	Events with the <i>Authentication Failure</i> or <i>Failed Password</i> .
User, Logoff	Events with the <i>Session closed</i> message.
User, Account, Management, Password, Change	Events with the <i>Password changed</i> message.
User, Account, Management, Remove	Events with the <i>Delete user</i> message.
User, Account, Management, Create	Events with the <i>A new user</i> message.
Privilege, Access	Events with the <i>sudo</i> or <i>su</i> process.
Service, Start	Events with the <i>Starting</i> or <i>Start</i> action for all Unix services.
Service, Restart	Events with the <i>Re-starting</i> , <i>Restarting</i> , or <i>Restart</i> action for all Unix services.

Continued on next page

Table 5 – continued from previous page

Labels	Description
Service, Stop	Events with the <i>Stop</i> or <i>Stopping</i> action for all Unix services.
FTP	Events with the <i>ftp</i> or <i>ftpd</i> process.
ssh	Events with the <i>sshd</i> process.
Command, Execute	Events with the Unix command.
Remove	Events with the <i>Delete</i> or <i>Deleted</i> action.
Modify	Events with the <i>Replace</i> action.
Start, Change, Edit	Events with the <i>Beign Edit</i> action.
Add	Events with the <i>Account added</i> action.
Remove	Events with the <i>Account removed</i> action.

Labels available in *LP_Unix SSHD* are:

Labels	Description
Session, Close	Events with the <i>closed</i> action or the <i>closed</i> status.
Session, Open	Events with the <i>opened</i> action or the <i>opened</i> status.

Labels available in *LP_Common Unix Systems* are:

Labels	Description
Open	Events with the <i>opened</i> message.
Close	Events with the <i>closed</i> action
Add	Events with the <i>added</i> action.
Delete	Events with the <i>deleted</i> action.
User, Delete	Events with the <i>userdel</i> process.
User, Add	Events with the <i>useradd</i> process.
Add	Events with the <i>account added</i> action.
Remove	Events with the <i>removed</i> action.
Successful	Events with the <i>successful</i> status.
Fail	Events with the <i>failed</i> status.

Labels available in *LP_Unix Systemd* are:

Labels	Description
Session, Start	Session start events.

4.4 Unix Report Templates

4.5 Using Unix Report Templates

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

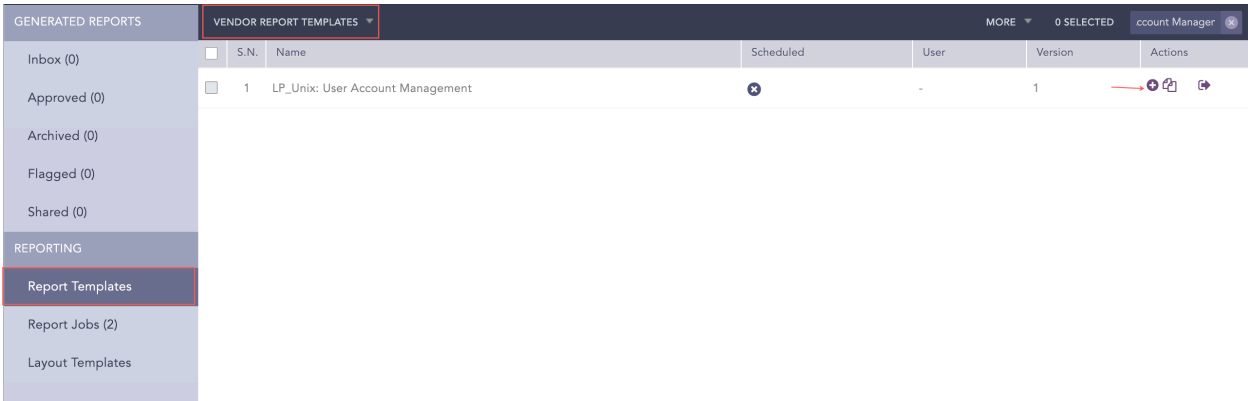


Fig. 5: Using the Unix Report Template

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

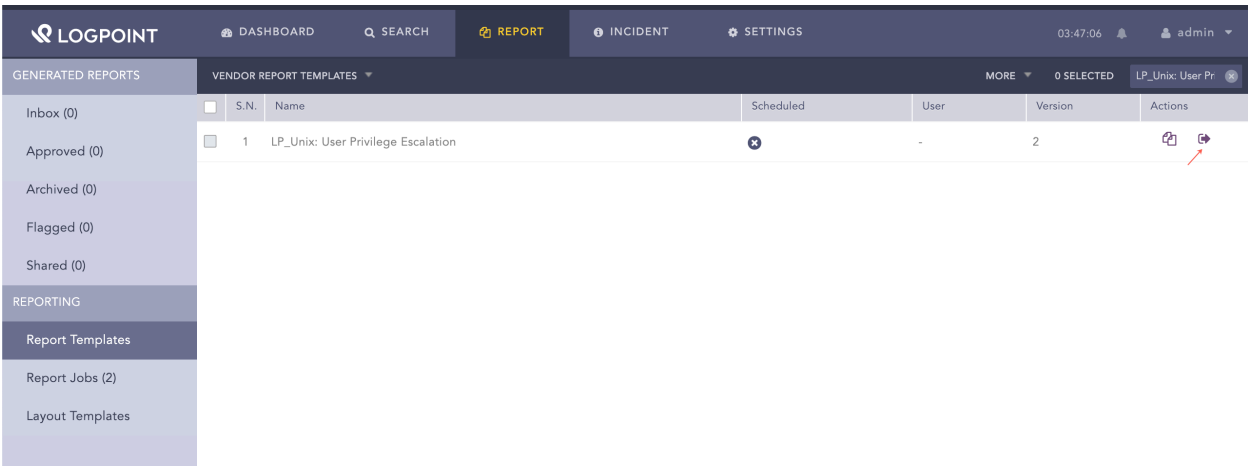


Fig. 6: Using Unix Report Template

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

Fig. 7: 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.

UNINSTALLING UNIX

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

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

LOG SAMPLES

Expected Log Format Sample

Unix Nullmailer

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

Expected Log Format Sample

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)
```

Expected Log Format Sample

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=<HNTJkOPQD8sFgBz> <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>
```

Expected Log Format Sample

IPtable

```
<30>Apr 21 16:23:01 xxxxx iptables.init[22335]: iptables: Setting chains to policy ACCEPT: filter [?  
↪OK ]
```

Expected Log Format Sample

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
```

Expected Log Format Sample

Unix Sysmon

```
<14>Oct 15 10:29:40 server-hostname-abc sysmon: <Event><System><Provider Name="Linux[?]
→ Sysmon" Guid="{xxxxxxxxxxxxxxxxxxxxxxxxxxxx}" /><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-xxxx-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
→ ">1.1.1.1</Data><Data Name="SourceHostname">-</Data><Data Name="SourcePort">
→ 12345</Data><Data Name="SourcePortName">-</Data><Data Name="DestinationIsIpv6
→ ">false</Data><Data Name="DestinationIp">1.1.1.2</Data><Data Name=
→ "DestinationHostname">-</Data><Data Name="DestinationPort">53</Data><Data Name=
→ "DestinationPortName">-</Data></EventData></Event>
```

Expected Log Format Sample

Unix Named

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

Expected Log Format Sample

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
```

Expected Log Format Sample

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.
```

Expected Log Format Sample

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
```

Expected Log Format Sample

Common Unix System

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

Expected Log Format Sample

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
```

Expected Log Format Sample

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)
```

Expected Log Format Sample

Unix SU

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

Expected Log Format Sample

Unix Sudo

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

Expected Log Format Sample

Unix Crond

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

Expected Log Format Sample

Unix Bash

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

Expected Log Format Sample

Unix Passwd

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

Expected Log Format Sample

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"
```

Expected Log Format Sample

Unix Bash

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

Expected Log Format Sample

Unix Runuser

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

Expected Log Format Sample

Unix Smbd

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

Expected Log Format Sample

Unix Systemd

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

Expected Log Format Sample

Unix Systemd

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