BeyondTrust

BeyondInsight 23.2
Event Forwarder Message Fields

TC:10/4/2023

Table of Contents

Event Forwarder Message Fields

There are a number of syslog formats supported by BeyondInsight, including newline-delimited, tab-delimited, LEEF, CEF, and a custom JSON structure for added parsing options. This document provides details on the following:

- Message components and format
- Persistent and variable fields within each message
- Event field mappings, event name, event type values, and event category values for Password Safe events
- Hardware, monitored services, and performance counter events for U-Series Appliance
- Sample syslog output formats

Overall Message structure

The newline-delimited and JSON syslog message structure is outlined below. CEF, LEEF, FireEye TAP, Splunk HTTP EC, and other implementations adhere to the message structures as required by their specifications.

Message Components

```
[priority] [syslog sender time] [syslog sender IP] [message body]
```

- **Priority:** Calculated using the event severity and syslog facility.
- **Syslog Sender Time** (yyyy-MM-ddTHH:mm:ss): UTC date and time when the event was forwarded.

> ***Note:*** *If there appears to be a discrepancy with the time of an event, make sure the receiver is configured to use UTC.*

- **Syslog Sender IP:** The IP address of the sender as an IPv4 address or IPv6 address.
- **Message Body:** The current syslog message body implementation is newline-delimited.

Message Format

```
<priority>yyyy-MM-ddTHH:mm:ssZ 10.10.10.10 Key=Value
```

Example: *Sample Message Format*

```
<0>2016-06-13T11:38:21Z 10.101.25.115 AgentId=Retina …
```

> ***Note:*** *The Event Forwarder only scrapes and forwards events from the database. A comprehensive list of all Syslog Event Messages is currently unavailable.*

Persistent Fields

The following keys can be expected within each message.

Field	Value Type	Description
Event Date	DateTime	Event date (UTC)
Server Date	DateTime	DateTime of server event forwarding processing (UTC)
RefType	String	Event reference Id
Agent Desc	String	The last known relaying agent (for example, *Application Bus 3.0*)
Agent ID	String	The source or originating agent
Agent Ver	String	The version of the agent
Source Host	String	The machine name of the agent (or IP address if the machine name is not available)
Source IP	String	The IP address of the agent
OS	String	The operating system of the agent
Category	String	Event Category. This can be any number of verbs (T49152, U11234, Group, Audits, etc.)
Event Name	String	The name of the event
Event Desc	String	Additional descriptive details for the event. This varies in level of detail based on the event source, etc.
Event Severity	Integer	In general, severity ranges from 0-10, where Information = 0, low = 3, medium = 6, and high = 9
Event Subject	String	Subject Identity at the root of the event. This can be a scanned asset (for example, IP or Hostname), an action (for example, *Application launch*)
Event Type	Integer	[Reserved for future use]
User	String	The computer / machine user associated with the event
Workgroup ID	String	The workgroup ID (for example,*BeyondTrust Workgroup*)
Workgroup Desc	String	The workgroup name (for example, *BeyondTrust*)
Workgroup Location	String	The workgroup location (for example, *Default Location*)

Variable Fields

Additional fields may be present following the persistent fields already mentioned. These are message type dependent and can vary over time and can be enabled and disabled using the **Event Filters** option within an event forwarder connector in BeyondInsight.

Event Category	Event Description	Agent ID	Event Type ID	Event ID
BeyondInsight Application Audit		appaudit		
BeyondTrust Discovery Agent		Retina		
Clarity		mlwr		
Endpoint Privilege Management for Mac & Windows	Application Request Elevation Application Launched Custom Rule Applied Shell Rule Applied ActiveX - Control Rule Applied ActiveX - Application Request Elevation UAC Prompt Denied Rule Applied Passive Rule Applied Validate Policy Policy Applied	pbw, pbmac pbw, pbmac pbw, pbmac pbw, pbmac pbw, pbmac pbw, pbmac pbw, pbmac pbw, pbmac pbw, pbmac pbw, pbmac pbw, pbmac	28691 28692 28693 28694 28695 28696 28697 28698 28699 28702 28703	PBW-EVENT-28691 PBW-EVENT-28692 PBW-EVENT-28693 PBW-EVENT-28694 PBW-EVENT-28695 PBW-EVENT-28696 PBW-EVENT-28697 PBW-EVENT-28698 PBW-EVENT-28699 PBW-EVENT-28702 PBW-EVENT-28703
Endpoint Privilege Management for Unix & Linux	Accept Finish Keystroke Reject Register Update	pbul pbul pbul pbul pbul pbul	01 02 03 04 05 06	PBUL-EVENT-01 PBUL-EVENT-02 PBUL-EVENT-03 PBUL-EVENT-04 PBUL-EVENT-05 PBUL-EVENT-06
File Integrity Monitoring		flm		
General Appliance Health		GenAppHealth		
Password Safe		pbps		
Privilege Management Reporting	Starts Logins Protection Processes	pmr		01 02 03 04

Note: *Privilege Management Reporting is available only when the Privilege Management Reporting plugin is installed and configured.*

Events

Password Safe Event Field Mappings

The table below provides the value type and description for each Password Safe field found in events.

Field	Value Type	Description
Event Date	DateTime	Event date (UTC)
Server Date	DateTime	DateTime of server event forwarding processing (UTC)
Agent ID	String	PBPS
Source Host	String	The machine name of BeyondInsight instance
Source IP	String	The IP address of BeyondInsight instance
Event Name	String	Role used
Event Desc	String	Object Type + Operation (for example, **Functional Account Add**)
Event Severity	Integer	0 = failed, 1 = success
Event Subject	String	IP address of the browser that initiated the event
User	String	Username associated with the event
Workgroup ID	String	Where applicable, workgroup ID of the associated asset
Workgroup Desc	String	Where applicable, workgroup description of the associated asset
LogSystemID	Integer	PMMLogSytem table reference ID
LogTime	DateTime	MM/dd/yyyy HH:mm:ss
UserName	String	Username associated with the event
UserID	String	User ID associated with the event
RoleUsed	String	Role used
ObjectTypeID	Integer	Object Type reference ID
ObjectType	String	Object Type (i.e. Function Account)
ObjectID	Integer	Object reference ID
Operation	String	Operation (for example, **Add**, **Update**)
Failed	Boolean	True / False
Target	String	Describes the asset acted upon (for example, **FAccount=testuser1 FAlias=testuser1 FDomain=testdomain1 PFid=25**)
Details	String	Miscellaneous additional information

Event Triggers

Event Name and Event Type Values

The following are potential values that can be found in application audit messages for **Event Name**, in addition to their corresponding **Event Type** value shown in parentheses. Events are based on action taken.

> **Note:** *This list may change over time and is not guaranteed to include every possible value.*

"Event Name" (Event Type)

Default (0)	*Login* (1)	*Logout* (2)	*Add* (3)
Edit (4)	*Delete* (5)	*Read* (6)	*Assign* (11)
Rename (12)	*Schedule* (14)	*Abort Job* (17)	*Delete Job* (18)
Reset (19)	*Import* (20)	*Copy* (23)	*Generate* (24)
Session End (25)	*Bulk Password Change* (26)	*Bulk Domain Account Unlink* (27)	*Validate* (28)
Update (30)	*Download* (35)	*Unlock* (36)	*Bulk Move Credential* (37)

Event Category Values

The following are potential values that can be found for **Category** in application audit messages.

> **Note:** *This list may change over time and is not guaranteed to include every possible value.*

Account Lockout	*Address Group*	*Application Session*	*Assets*	*Attribute*
Attribute Type	*BeyondInsight Password Policy*	*BeyondInsight Configuration Tool*	*Change Password*	*Client Certificate*
Cloud Connector	*Configure*	*Credential*	*Databases*	*Direct Connect*
Direct Connect Failure	*Directory Query*	*Domain Management*	*EPM Exclusion*	*EPM Policy Logout*
EPM Policy User	*EPM Rule*	*Event Forwarder*	*JIRA Ticket System*	*Login Failure*
Managed Account Alias	*Organization*	*Plugin Setting*	*PMM Access Policy*	*PMM Access Policy Schedule*
PMM Account	*PMM API Authentication Rule Failure*	*PMM API Registration*	*PMM API SignOut*	*PMM Application*
PMM Change Email Template	*PMM Connection Profile*	*PMM Connection Profile Filter*	*PMM DSS Key Policies*	*PMM Functional Account*
PMM Login	*Pre-Login Banner*	*PMM Login Failure*	*PMM Managed Account*	*PMM Managed System*
PMM Mask Remedy Connector	*PMM Oracle Internet Directory*	*PMM Password Rule*	*Propagation Action*	*Purging Options*
Remedy Connector Mapping	*Sailpoint STI*	*Scan*	*SCIM*	*ServiceNow Connector*
ServiceNow Export	*ServiceNow Export Mapping*	*ServiceNow Import*	*ServiceNow Ticket System Mapping*	*ServiceNow Ticket System*
Session Monitoring	*Smart Rule*	*System Options*	*Secrets Safe*	*Secrets Safe Credential*

Secrets Safe Folder	*Third Party Connector*	*Ticket*	*TOTP Authentication Failure*	*TOTP Device Enrolled*
User	*User Group*	*User Group - Smart Rule Role*	*Worker Node*	*Workgroup*

U-Series Appliance SNMP Events

There are 4 event names:

- EventName = PerformanceAlert / EventID = variable (for example, U-Series Appliance-HARDWARE-001)
- EventName = ServiceErrorAlert / EventID = U-Series Appliance-SERVICE-001
- EventName = HardwareFaultAlert / EventID = variable (for example, U-Series Appliance-HARDWARE-001)
- EventName = DailyPerformanceSummary / EventID = U-Series Appliance-PERFDAILY-001

The sources that trigger the events can be categorized as follows:

- **Hardware Events**: Any of the hardware events raised by Dell's OpenManage.
- **Monitored Services**: A variety of events around monitored services, such as:
    - Crashes
    - A Service's running state isn't as expected (for example, running when it should be stopped or vice-versa, or when the previously alerted service is then found to be running in the correct state).
    - Service controller manager generates any of the following events in the event log (crashes or did-not-start type of events): *7034*, *7000*, *7013*, *7023*, *7024*, *7031*, *7032*, *7034*, *7043*.
- **Performance Counters**: Events when the various performance monitor counters cross the user-configured thresholds (low, med, or hi and reset).

Possible Hardware Events

batterywarn	batteryfail	fanwarn	fanfail	hardwarelogwarn
hardwarelogfull	intrusion	memprefail	memfail	systempowerwarn
systempowerfail	powersupply	powersupplywarn	processorwarn	processorfail
redundegrad	redunlost	tempwarn	tempfail	voltwarn
voltfail	watchdogasr	storagesyswarn	storagesysfail	storagectrlwarn
storagectrlfail	pdiskwarn	pdiskfail	vdiskwarn	vdiskfail
enclosurewarn	enclosurefail	storagectrlbatterywarn	storagectrlbatteryfail	systempeakpower

List of Monitored Services

EventServer	ManagementConsole	StandaloneEventServer	BIDatabase	Database
PasswordSafe	StandalonePasswordSafe	PatchManagement	ThirdPartyPatch	Retina
ARCube	ARReporting	AutoUpdates	EUS	Updater

List of Performance Counters

SQL Memory usage (% used of the allocated SQL Server memory limit)	SQL Server's CPU usage	Total CPU usage
Disk free on each drive	Physical Disk Avg Disk sec write C:	Physical Disk Current Disk Queue Length
Memory Pages/sec SQLServer Batch Requests/Sec	Memory Cache Bytes SQLServer SQL Compilations/Sec	Paging File_Percent_Usage SQLServer SQL_ReCompilations/Sec
SQLServer User Connections	SQLServer LockWaits/Sec	SQLServer PageSplits/Sec
SQLServer ProcessesBlock	SQLServer CheckpointPages/Sec	

Sample Syslog Output Formats

> **Note:** *This is a small sample of event messages in various formats, not an all-encompassing set of every possible event.*

Syslog Format: Newline-delimited

```
<0>2015-12-05T11:22:53Z 10.124.101.11 Agent Desc: Application Bus 3.0
Event Date: 2016-06-13 10:14:35
Server Date: 2016-06-13 11:38:21
RefType: 16
Agent ID: retina
Agent Ver: 5.23.1.3108
Category: Processes
Source Host: WIN-4PBV285405S
Event Desc: svchost
Event Name: Process   772
OS: Windows,Microsoft,Windows,Server 2008 R2 Standard Edition (full installation) x64,Service
Pack 1
Event Severity: 0
Source IP: 10.200.31.203
Event Subject: 010.200.031.085
Event Type: 0
User: SYSTEM
Workgroup Desc: BeyondTrust
Workgroup ID: BeyondTrust Workgroup
Workgroup Location: Default Location
Process ID: 772 (0x304)
Parent Process ID: 492 (0x1EC)
Start Time: 5/12/2016 9:21:05 AM GMT-04
```

Syslog Format: Tab-delimited

```
<0>2016-12-05T11:22:53Z 10.101.25.167 Agent Desc: Application Bus 3.0Agent ID: retina
    Agent Ver: 5.25.2.3215Category: UserSource Host: WIN-N83HFCB9RNAEvent
Desc: Built-in account for guest access to the computer/domainEvent Name: GuestOS:
Windows,Microsoft,Windows,UnknownEvent Severity: 0Source IP: 10.101.25.167
Event Subject: 010.101.025.177Event Type: 0User: WIN-N83HFCB9RNA$
    Workgroup Desc: BeyondTrust        Workgroup ID: BeyondTrust Workgroup     Workgroup
Location: Default Location     Member of Group (01/001): Guests        Privilege (01/002)
: Guest        Account Disabled (01/003): True Last Logon (01/004): never      Last Logoff
(01/005): unknown      Expires (01/006): never         Max Storage (01/007): unlimited Bad
PW Count (01/008): 0   Number of Logons (01/009): 0    Logon Server (01/010): \\*      Country
 Code (01/011): 0      RID (01/012): 501       Password Expired (01/013): no   Source
(01/014): NetUserEnum  SID (01/015): S-1-5-21-2210307081-232491991-3792010023-501
```

JSON Syslog Format


```
<0>2016-06-13T11:38:21 10.101.25.115
{
          "formatVersion":"1.0",
          "vendor":"BeyondTrust",
          "product":"BeyondInsight",
          "version":"6.0.0",
          "agentid":"attack",
          "agentdesc":"Application Bus 3.0",
          "agentver":"Unknown",
          "category":"User",
          "severity":"0",
          "eventid":"RET-SCAN-007",
          "eventname":"beyondtrust",
          "eventdesc":"bt admin",
          "eventdate":"Jun 10 2016 03:05:04",
          "sourcehost":"mymachine-ws",
          "os":"Windows,Microsoft,Windows,Unknown",
          "souirceip":"172.168.101.202",
          "eventsubject":"172.168.101.222",
          "eventtype":"0",
          "user":"MYMACHINE-WS$",
          "workgroupid":"BeyondTrust Workgroup",
          "workgroupdesc":"BeyondTrust",
          "workgrouplocation":"Default Location",
          "nvps":
          {
                    "id":"c85dca8c-df30-4a70-98f8-c8a47f7fc2fa",
                    "evtdate":"6/10/2016 3:05:04 AM",
                    "clienthost":"mymachine-ws",
                    "eventseverity":"0",
                    "dllversion":"AppBus EMS v3.0 com xml",
                    "transactiongroup":"5B3A069BE0D84E7EA56F2A40EFDBE253",
                    "subjectdescription":"mymachine-ws",
                    "evtsubjbi":"2896693762",
                    "evtsrcipbi":"2896693762",
                    "referenceid":"7",
                    "evtdatatype":"SCAN",
                    "evtstatus":"True",
                    "badpwcount0101":"0",
                    "countrycode0101":"0",
                    "expires0101":"never ",
                    "fullname0101":"beyondtrust",
                    "lastlogoff0101":"unknown ",
                    "lastlogon0101":"Tue Jun 02 19:26:42 2015",
                    "logonserver0101":"\\\\*",
                    "maxstorage0101":"unlimited",
                    "memberofgroup0101":"Administrators, Performance Log Users, Users",
                    "numberoflogons0101":"7",
                    "passwordage0101":"412 days",
                    "passwordexpired0101":"no",
                    "privilege0101":"Administrator",
                    "rid0101":"1006",
```

```
                        "sid0101":"S-1-5-21-4152543990-75340177-3020034217-1006",
                        "source0101":"NetUserEnum"
            }
}
```

LEEF Syslog Format

```
Jun 13 23:11:40 fe80::ad7a:8589:f107:158a%12
LEEF:1.0|BeyondTrust|BeyondInsight|6.0.0|RET-SCAN-009|cat=Modules      devTime=Jun
04 2016 02:08:58       devTimeFormat=MMM dd yyyy HH:mm:ss      sev=0
       src=10.200.31.212       resource=WIN-AR9FPF5LTJG        dst=10.200.31.84
       usrName=WIN-AR9FPF5LTJG$        groupID=BeyondTrust Workgroup
       AgentDesc=Application Bus 3.0   AgentID=retina  AgentVer=5.24.1.3126
       EventDesc=acrotray.exe  EventName=acrotray.exe
       Os=Windows,Microsoft,Windows,Unknown    EventType=0
       WorkgroupDesc=BeyondTrust       WorkgroupLocation=Default Location      Type=Module
       Name=acrotray.exe       Filename=C:\\Program Files\\Adobe\\Acrobat
11.0\\Acrobat\\acrotray.exe    MD5=E0DF6506C36AA207F41EFED13D876D83
       SHA1=11B87A57B626CCD760D121215C1B96AB72F06BAA   Version=11.0.6.70
       Company Name=Adobe Systems Inc. Description=AcroTray    Product=AcroTray -
Adobe Acrobat Distiller helper application.    Signer=Adobe Systems, Incorporated      Image
Size=3514368   Entry Address=0056F07E  Base Address=003C0000
       CertSerial=68ADD7AFFC72183C31865ACD3CB2D70C     CertIssuer=Symantec Class 3
Extended Validation Code Signing CA
```

CEF Syslog Format

```
Jun 13 16:09:00 WIN-TC570BCQDNA CEF:0|BeyondTrust|BeyondInsight|6.0.0|RET-SCAN-012|
IP Start Time|0|rt=Jun 13 2016 19:08:32 deviceExternalId=pbw_vulnerability cat=Status
src=10.200.31.81 shost=PATCHWIN764X suser=NT AUTHORITY\NETWORK SERVICE msg=2016-
06-13 16:08:33 dst=10.200.31.81 BeyondTrustBeyondInsightAgentDesc=PBW 7.0.2.79
BeyondTrustBeyondInsightAgentID=pbw_vulnerability
BeyondTrustBeyondInsightAgentVer=7.0.2.79 BeyondTrustBeyondInsightCategory=Status
BeyondTrustBeyondInsightClientHost=PATCHWIN764X
BeyondTrustBeyondInsightEventDesc=2016-06-13 16:08:33
BeyondTrustBeyondInsightEventName=IP Start Time BeyondTrustBeyondInsightOs=Windows 7
(X64), Service Pack 1 BeyondTrustBeyondInsightEventSeverity=0
BeyondTrustBeyondInsightSourceIp=10.200.31.81
BeyondTrustBeyondInsightEventSubject=10.200.31.81 BeyondTrustBeyondInsightEventType=0
BeyondTrustBeyondInsightUser=NT AUTHORITY\NETWORK SERVICE
BeyondTrustBeyondInsightWorkgroupDesc=BeyondTrust Workgroup
BeyondTrustBeyondInsightWorkgroupID=BeyondTrust Workgroup
BeyondTrustBeyondInsightWorkgroupLocation=Default Location
```