TIBCO LogLogic® Log Management Intelligence

TIBCO LogLogic® Enterprise Virtual Appliance

TIBCO LogLogic® Enterprise Virtual Appliance - Container Edition

Syslog Alert Format Quick Reference

Version 6.4.0
February 2022

Contents

Overview

Alerts are an important way of sending immediate notifications on events. The TIBCO LogLogic® Log Management Intelligence appliance has three ways of sending out alerts:

- using email
- SNMP trap
- Syslog format

This document specifies the format of Syslog alert messages sent by the LogLogic® LMI appliance to Syslog receivers. You can integrate your systems and applications with the LogLogic LMI appliance by parsing and analyzing the received alert messages.

Note:
LogLogic LMI has been used to represent LogLogic LMI, LogLogic EVA, and LogLogic EVA - Container Edition. All processes and procedures applicable to LogLogic LMI are also applicable to LogLogic EVA and LogLogic EVA - Container Edition, unless explicitly stated otherwise.

Format of Syslog Messages

Each Syslog message is of the format:

```
SYSLOG_HEADER LogLogic_ID Common_Alert_Message_Attributes Alert_
Specific_Message_Attributes
```

The common and specific message attributes are a set of name/value pairs (Name="Value") that conform to the following rules:

- The order of the name/value pairs is NOT significant.
- Syslog messages sent/received by LogLogic LMI are limited to 65535 characters.
- One or more spaces are allowed between each name/value pair.
- The number of spaces in a value is always significant.

- New lines (\n) and binary characters are not possible in Syslog alert messages. Binary characters are converted to `\xNN`, where NN is the hex value of the binary character. If there is a new line value, then it becomes `\x0A` in the final Syslog alert message.
- All values appear between quotation marks ("Value").
- Double quotation marks ("") are escaped by a backslash (\") if found in the attribute value.
- To specify names not part of the LogLogic specifications, you must specify them as follows: name (starts with a character), followed by numbers, characters, and underscores.

TIBCO LogLogic® reserves the right to change the message format in future revisions to suit the need of our customers and development partners. The format has been designed to support some types of future extensions while maintaining backward compatibility. Possible types of changes include:

- The addition of name/value pairs to be inserted at any location in the message
- The text of the Summary attribute may change for readability or to provide additional information

See the following sections:

- SYSLOG HEADER Components
- LogLogic ID
- Common Alert Message Attributes
- Alert-Specific Message Attributes

SYSLOG HEADER Components

The SYSLOG_HEADER conforms to RFC3164. The format is:

```
PRIORITY TIME_STAMP HD_LOGAPP_IP
```

where

- `PRIORITY` ::= <133>

  > **Note:** LogLogic LMI currently does not enable users to specify the Syslog severity or facility on a per-alert basis. Therefore, for all alerts, we use a fixed Syslog priority value of <133>, which indicates the facility "local0" and a severity level of "notice".

- `TIME_STAMP` ::= MONTH DATE HOUR ':' MINUTE ':' SECOND YEAR
- `HD_LOGAPP_IP` :: = IP address of the LogLogic LMI appliance

LogLogic ID

LogLogic_ID is a string of the following format:

```
%LOGLOGIC-X-05XXYY:
```

where

- `X` - Single digit representing the Syslog severity. At this time, the value is always 5.
- `05XXYY` - Unique six digit LogLogicID code, where:
  - `XX` - AlertType
  - `YY`– AlertSubType

LogLogic ID and associated AlertTypes and Alert Subtypes

The following table provides a list of unique LogLogicID codes and their associated Alert Type and Alert Subtypes, if applicable.

LogLogic ID	Alert Type	Alert Subtype
50100	ADAPTIVE_BASELINE_ALERT	
50200	CISCO_PIX/ASA_MESSAGES_ALERT	
50300	MESSAGE_VOLUME_ALERT	
50400	NETWORK_POLICY_ALERT	
50500	PRE_DEFINED_SEARCH_FILTER_ ALERT	
50600	RATIO_BASED_ALERT	
50701	SYSTEM_ALERT	CPU_TEMPERATURE_ALERT

LogLogic ID	Alert Type	Alert Subtype
50702	SYSTEM_ALERT	DISK_USAGE_ALERT
50703	SYSTEM_ALERT	DROPPED_MESSAGE_ALERT
50704	SYSTEM_ALERT	FAILOVER_ALERT
50705	SYSTEM_ALERT	NETWORK_CONNECTION_SPEED_ALERT
50706	SYSTEM_ALERT	NETWORK_INTERFACE_ALERT
50707	SYSTEM_ALERT	RAID_DISK_FAILURE_ALERT
50708	SYSTEM_ALERT	SYNCHRONIZATION_FAILURE_ALERT
50709	SYSTEM_ALERT	TCP_FORWARD_CONNECTION_ALERT
50710	SYSTEM_ALERT	MIGRATION_COMPLETE_ALERT
50711	SYSTEM_ALERT	TCP_FORWARD_FALLING_BEHIND_ALERT
50712	SYSTEM_ALERT	RESOURCE_EXHAUSTION_ALERT
50800	VPN_CONNECTIONS_ALERT	
50900	VPN_MESSAGES_ALERT	
51001	VPN_STATISTICS_ALERT	VPN_CONNECTIONS
51002	VPN_STATISTICS_ALERT	DENIED_VPN_CONNECTION
51003	VPN_STATISTICS_ALERT	VPN_CONNECTION_DURATION
51004	VPN_STATISTICS_ALERT	BYTES_RECEIVED
51005	VPN_STATISTICS_ALERT	BYTES_SENT

Common Alert Message Attributes

Name	Value / Description
AlertPriority	("HIGH" | "MEDIUM" | "LOW")
AlertType	("ADAPTIVE_BASELINE_ALERT" | "CISCO_PIX/ASA_MESSAGES_ ALERT" | "MESSAGE_VOLUME_ALERT" | "NETWORK_POLICY_ALERT" | "PRE_DEFINED_SEARCH_FILTER_ALERT" | "RATIO_BASED_ALERT" | "SYSTEM_ALERT" | VPN_CONNECTIONS_ALERT" | "VPN_ MESSAGES_ALERT" | "VPN_STATISTICS_ALERT")
AlertName	Name of the alert
GeneratedBy	IP address of the LogLogic LMI appliance that generated the alert
ForDevices	Comma-separated list of devices or device group names
ForDeviceIPs	Comma-separated list of IP addresses for the devices that triggered the alert
ConfiguredForDevices (Optional)	Comma-separated list of devices or device group names
AlertableEventsCount	Number of events (integer)
DetailsURL (not available in v3.2.x)	URL of the alert

Alert-Specific Message Attributes

The following sections identify the alert-specific message attributes for the alert types.

ADAPTIVE_BASELINE_ALERT

Message attributes and sample message of ADAPTIVE_BASELINE_ALERT

Name	Value / Description
MsgRate	Message rate percentage (integer in percent)
(Low | High)Threshold	Low or high threshold for the message rate (integer in percent)

Sample Message

```
<133> Mar 15 11:05:59 2009 10.1.1.165 %LOGLOGIC-5-050100:
AlertPriority="LOW" AlertType="ADAPTIVE_BASELINE_ALERT"
AlertName="relVol" GeneratedBy="10.1.1.165" ForDevices="10.1.1.125_
1,10.1.1.165_17,10.1.1.124_1,10.1.1.92_7,te
st5_7,test4_6,10.1.1.100_1,10.1.1.95_4,sqajuniperfw.1.10.in-addr.a rpa_
4,10.1.1.96_2,10.1.1.240_2,LocalHost"
ForDeviceIPs="10.1.1.125,10.1.1.165,10.1.1.124,10.1.1.92,10.1.1.82
,10.1.1.80,10.1.1.100,10.1.1.95,10.1.1.98,10.1.1.96,10.1.1.240,127
.0.0.1"
ConfiguredForDevices="10.1.1.125_1,10.1.1.165_17,10.1.1.124_1,10.1
.1.92_7,test5_7,test4_6,10.1.1.100_1,10.1.1.95_4,sqajuniperfw.1.10
.in-addr.arpa_4,10.1.1.96_2,10.1.1.240_2,LocalHost" MsgRate="193"
HighThreshold="101" AlertableEventsCount="0"
```

CISCO_PIX/ASA_MESSAGES_ALERT

Message attributes and sample message of CISCO_PIX/ASA_MESSAGES_ALERT

Name	Value / Description
Message	PIX/ASA message
(Low | High)Threshold	Low or high threshold for the message count (integer)
DurationSeconds	Duration in seconds(integer)
MsgCriticality	PIX/ASA message criticality(integer)
MsgCode	PIX/ASA message code (integer)

Sample Message

```
<133> Mar 15 11:15:22 2009 10.1.1.165 %LOGLOGIC-5-050200:
AlertPriority="HIGH" AlertType="CISCO_PIX/ASA_MESSAGES_ALERT"
```

```
AlertName="pixAlert" GeneratedBy="10.1.1.165" ForDevices="10.1.1.240_2"
ForDeviceIPs="10.1.1.240" ConfiguredForDevices="10.1.1.96_2,10.1.1.240_
2" Message="<1>Mar 6 09:35:38 bemidjisu-pix.r.mnscu.edu %PIX-4-106023:
Deny tcp src outside:164.58.100.125/9609 dst inside:199.17.199.190/81 by
access-group \"INBOUND-ITG\" " HighThreshold="5" DurationSeconds="60"
MsgCriticality="4" MsgCode="106023" AlertableEventsCount="0"
```

MESSAGE_VOLUME_ALERT

Message attributes and sample message of MESSAGE_VOLUME_ALERT

Name	Value / Description
MsgRate	Message per second (integer)
(Low | High)Threshold	Low or high threshold for the message per second (integer)

Sample Message

```
<133> Mar 15 11:31:06 2009 10.1.1.165 %LOGLOGIC-5-050300:
AlertPriority="LOW" AlertType="MESSAGE_VOLUME_ALERT"
AlertName="volAlert" GeneratedBy="10.1.1.165" ForDevices="10.1.1.125_
1,10.1.1.165_17,10.1.1.124_1,10.1.1.92_7,te
st5_7,test4_6,10.1.1.100_1,10.1.1.95_4,sqajuniperfw.1.10.in-addr.a
rpa_4,10.1.1.96_2,10.1.1.240_2,LocalHost"
ForDeviceIPs="10.1.1.125,10.1.1.165,10.1.1.124,10.1.1.92,10.1.1.82
,10.1.1.80,10.1.1.100,10.1.1.95,10.1.1.98,10.1.1.96,10.1.1.240,127
.0.0.1"
ConfiguredForDevices="10.1.1.125_1,10.1.1.165_17,10.1.1.124_1,10.1
.1.92_7,test5_7,test4_6,10.1.1.100_1,10.1.1.95_4,sqajuniperfw.1.10
.i n-addr.arpa_4,10.1.1.96_2,10.1.1.240_2,LocalHost" MsgRate="1280"
HighThreshold="1000" AlertableEventsCount="8"
```

NETWORK_POLICY_ALERT

Message attributes and sample message of NETWORK_POLICY_ALERT

Name	Value / Description
NetworkPolicy	Network policy name
NetworkDevice	Log source IP address
SrcIP	Message source IP address
SrcPort	Message source port
DestIP	Message destination IP address
DestPort	Message destination port
Protocol	Message protocol
Action	("ACCEPTED" | "DENIED")

Sample Message

```
<133> Mar 15 11:35:15 2009 10.1.1.165 %LOGLOGIC-5-050400:
AlertPriority="HIGH" AlertType="NETWORK_POLICY_ALERT"
AlertName="PolicyAlert" GeneratedBy="10.1.1.165" ForDevices="10.1.1.95_
4" ForDeviceIPs="10.1.1.95" ConfiguredForDevices="10.1.1.95_
4,sqajuniperfw.1.10.in-addr.arpa_4
,10.1.1.96_2,10.1.1.240_2" NetworkPolicy="PolicyAlert"
NetworkDevice="10.1.1.95" SrcIP="10.100.0.1" SrcPort="0"
DestIP="224.0.0.18" DestPort="0" Protocol="icmp" Action="DENIED"
AlertableEventsCount="287033"
```

PRE_DEFINED_SEARCH_FILTER_ALERT

Message attributes and sample message of PRE_DEFINED_SEARCH_FILTER_ALERT

Name	Value / Description
FilterMatch	Search filter pattern
TriggeringMessage	Last triggering message
(Low | High)Threshold	Low or high threshold (integer)
DurationSeconds	Duration in seconds (integer)

Sample Message

```
<133> Mar 15 11:43:29 2009 10.1.1.165 %LOGLOGIC-5-050500:
AlertPriority="HIGH" AlertType="PRE_DEFINED_SEARCH_FILTER_ALERT"
AlertName="wordAlert" GeneratedBy="10.1.1.165" ForDevices="All Syslog
Sources"
ForDeviceIPs="10.1.1.5,10.1.1.80,10.1.1.82,10.1.1.96,10.1.1.92,10.
1.1.95,10.1.1.98,10.1.1.100,10.1.1.124,10.1.1.125,10.1.1.165,10.1.
1.240,127.0.0.1" ConfiguredForDevices="All Syslog Sources"
FilterMatch="inbound" TriggeringMessage="<1>Mar 10 15:37:50 metro-
gateway.r.mnscu.edu %PIX-6-302013: Built inbound TCP connection
544430255 for outside:67.28.27.217/4030
(67.28.27.217/4030) to dmz1:199.17.241.217/80 (199.17.241.217/80)
" HighThreshold="2" DurationSeconds="60" AlertableEventsCount="2577"
```

RATIO_BASED_ALERT

Message attributes and sample message of RATIO_BASED_ALERT

Name	Value / Description
MsgRate	Percentage of messages (integer)
(Low | High)Threshold	Low or high threshold for the message rate (integer in percent)

Sample Message

```
<133> Mar 15 16:27:09 2009 10.1.1.165 %LOGLOGIC-5-050600:
AlertPriority="LOW" AlertType="RATIO_BASED_ALERT" AlertName="ratioVol"
GeneratedBy="10.1.1.165" ForDevices="10.1.1.125_1,10.1.1.165_
17,10.1.1.124_1,10.1.1.100_1,1
0.1.1.95_4,sqajuniperfw.1.10.in-addr.arpa_4,10.1.1.96_2,10.1.1.240
_2,LocalHost"
ForDeviceIPs="10.1.1.125,10.1.1.165,10.1.1.124,10.1.1.100,10.1.1.9
5,10.1.1.98,10.1.1.96,10.1.1.240,127.0.0.1"
ConfiguredForDevices="10.1.1.125_1,10.1.1.165_17,10.1.1.124_1,10.1
.1.100_1,10.1.1.95_4,sqajuniperfw.1.10.in-addr.arpa_4,10.1.1.96_2,
10.1.1.240_2,LocalHost" MsgRate="0" LowThreshold="2"
AlertableEventsCount="36"
```

SYSTEM_ALERT

The SYSTEM_ALERT alerts are of the following subtypes.

- CPU_TEMPERATURE_ALERT
- MIGRATION_COMPLETE_ALERT
- DISK_USAGE_ALERT
- DROPPED_MESSAGE_ALERT
- FAILOVER_ALERT
- NETWORK_CONNECTION_SPEED_ALERT
- NETWORK_INTERFACE_ALERT
- RAID_DISK_FAILURE_ALERT
- RESOURCE_EXHAUSTION_ALERT
- SYNCHRONIZATION_FAILURE_ALERT
- TCP_FORWARD_CONNECTION_ALERT
- TCP_FORWARD_FALLING_BEHIND_ALERT

CPU_TEMPERATURE_ALERT

Message attributes and sample message of CPU_TEMPERATURE_ALERT

Name	Value / Description
AlertSubType	CPU_TEMPERATURE_ALERT
Summary	High CPU temperature

Sample Message

```
<133> Mar 15 11:51:32 2009 10.1.1.165 %LOGLOGIC-5-050701:
AlertPriority="LOW" AlertType="SYSTEM_ALERT" AlertName="cpuTempAlert"
GeneratedBy="10.1.1.165" ForDevices="10.1.1.165_17"
ForDeviceIPs="10.1.1.165" Summary="High CPU temperature"
AlertSubType="CPU_TEMPERATURE_ALERT" AlertableEventsCount="0"
```

MIGRATION_COMPLETE_ALERT

Message attributes and sample message of MIGRATION_COMPLETE_ALERT

Name	Value / Description
AlertSubType	MIGRATION_COMPLETE_ALERT
Summary	Data Migration complete

Sample Message

```
<133> Jul 11 03:04:19 2011 10.8.0.153 %LOGLOGIC-5-050710:
AlertPriority="HIGH" AlertType="SYSTEM_ALERT" AlertName="data migration
complete 001" GeneratedBy="10.8.0.153" ForDevices="10.8.0.153_logapp"
ForDeviceIPs="10.8.0.153" Summary="Data Migration complete"
```

```
Details="Data Migration complete. It is safe to remove the source
appliance" AlertSubType="MIGRATION_COMPLETE_ALERT"
AlertableEventsCount="0"
```

DISK_USAGE_ALERT

Message attributes and sample message of DISK_USAGE_ALERT

Name	Value / Description
AlertSubType	DISK_USAGE_ALERT
Summary	High disk usage

Sample Message

```
<133> Mar 15 11:52:34 2009 10.1.1.165 %LOGLOGIC-5-050702:
AlertPriority="LOW" AlertType="SYSTEM_ALERT" AlertName="diskUsageAlert"
GeneratedBy="10.1.1.165" ForDevices="10.1.1.165_17"
ForDeviceIPs="10.1.1.165" Summary="High disk usage" AlertSubType="DISK_
USAGE_ALERT" AlertableEventsCount="0"
```

DROPPED_MESSAGE_ALERT

Message attributes and sample message of DROPPED_MESSAGE_ALERT

Name	Value / Description
AlertSubType	DROPPED_MESSAGE_ALERT
Summary	Dropped messages

Sample Message

```
<133> Mar 15 11:02:04 2009 10.1.1.165 %LOGLOGIC-5-050703:
AlertPriority="HIGH" AlertType="SYSTEM_ALERT" AlertName="msgDropAlert"
GeneratedBy="10.1.1.165" ForDevices="10.1.1.165_17"
ForDeviceIPs="10.1.1.165" Summary="Dropped messages"
AlertSubType="DROPPED_MESSAGE_ALERT" AlertableEventsCount="0"
```

FAILOVER_ALERT

Message attributes and sample message of FAILOVER_ALERT

Name	Value / Description
AlertSubType	FAILOVER_ALERT
Summary	Cluster failover

Sample Message

```
<133> Mar 14 16:59:59 2009 10.1.1.73 %LOGLOGIC-5-050704:
AlertPriority="HIGH" AlertType="SYSTEM_ALERT" AlertName="Failover-Alert"
GeneratedBy="10.1.1.73" ForDevices="10.1.1.69_17"
ForDeviceIPs="10.1.1.69" Summary="Cluster failover"
AlertSubType="FAILOVER_ALERT" AlertableEventsCount="0"
```

NETWORK_CONNECTION_SPEED_ALERT

Message attributes and sample message of NETWORK_CONNECTION_SPEED_ALERT

Name	Value / Description
AlertSubType	NETWORK_CONNECTION_SPEED_ALERT

Name	Value / Description
Summary	Low network speed

Sample Message

```
<133> Mar 15 17:05:36 2009 10.1.1.165 %LOGLOGIC-5-050705:
AlertPriority="LOW" AlertType="SYSTEM_ALERT" AlertName="netSpeedAlert"
GeneratedBy="10.1.1.165" ForDevices="10.1.1.165_17"
ForDeviceIPs="10.1.1.165" Summary="Low network speed"
AlertSubType="NETWORK_CONNECTION_SPEED_ALERT" AlertableEventsCount="0"
```

NETWORK_INTERFACE_ALERT

Message attributes and sample message of NETWORK_INTERFACE_ALERT

Name	Value / Description
AlertSubType	NETWORK_INTERFACE_ALERT
Summary	Network interface down

Sample Message

```
<133> Mar 14 16:34:17 2009 10.1.1.73 %LOGLOGIC-5-050706:
AlertPriority="MEDIUM" AlertType="SYSTEM_ALERT" AlertName="netIntfAlert"
GeneratedBy="10.1.1.73" ForDevices="10.1.1.69_17"
ForDeviceIPs="10.1.1.69" Summary="Network interface down"
AlertSubType="NETWORK_INTERFACE_ALERT" AlertableEventsCount="0"
```

RAID_DISK_FAILURE_ALERT

Message attributes and sample message of RAID_DISK_FAILURE_ALERT

Name	Value / Description
AlertSubType	RAID_DISK_FAILURE_ALERT
Summary	Raid disk failure

Sample Message

```
<133> Mar 14 13:35:48 2009 10.1.1.45 %LOGLOGIC-5-050707:
AlertPriority="HIGH" AlertType="SYSTEM_ALERT"
AlertName="sqaRaidDskFailAlert" GeneratedBy="10.1.1.45"
ForDevices="10.1.1.45_17" ForDeviceIPs="10.1.1.45" Summary="Raid disk
failure" AlertSubType="RAID_DISK_FAILURE_ALERT" AlertableEventsCount="4"
```

RESOURCE_EXHAUSTION_ALERT

Message attributes and sample message of RESOURCE_EXHAUSTION_ALERT

Name	Value / Description
AlertSubType	RESOURCE_EXHAUSTION_ALERT
Summary	Resource exhaustion, failed to load alert

Sample Message

```
<133> Jul 10 22:51:35 2011 10.8.0.154 %LOGLOGIC-5-050712:
AlertPriority="HIGH" AlertType="SYSTEM_ALERT" AlertName="resource
exhaustion 001" GeneratedBy="10.8.0.154" ForDevices="10.8.0.154_logapp"
ForDeviceIPs="10.8.0.154" Summary="Resource exhaustion, failed to load
alert" Details="Failed to load alert pre-03: out of memory."
AlertSubType="RESOURCE_EXHAUSTION_ALERT" AlertableEventsCount="0"
```

SYNCHRONIZATION_FAILURE_ALERT

Message attributes and sample message of SYNCHRONIZATION_FAILURE_ALERT

Name	Value / Description
AlertSubType	SYNCHRONIZATION_FAILURE_ALERT
Summary	Data sync error

Sample Message

```
<133> Mar 14 17:08:30 2009 10.1.1.73 %LOGLOGIC-5-050708:
AlertPriority="HIGH" AlertType="SYSTEM_ALERT" AlertName="Sync-Alert"
GeneratedBy="10.1.1.73"
ForDevices="10.1.1.69_17" ForDeviceIPs="10.1.1.69" Summary="Data sync
error" AlertSubType="SYNCHRONIZATION_FAILURE_ALERT"
AlertableEventsCount="0"
```

TCP_FORWARD_CONNECTION_ALERT

Message attributes and sample message of TCP_FORWARD_CONNECTION_ALERT

Name	Value / Description
AlertSubType	TCP_FORWARD_CONNECTION_ALERT
TunnelPeerIP Disconnected	TUNNEL_PEER_IP
Summary	TCP forward connection error

Sample Message

```
<133> Mar 15 11:52:59 2009 10.1.1.165 %LOGLOGIC-5-050709:
AlertPriority="HIGH" AlertType="SYSTEM_ALERT" AlertName="tcpFwdAlert"
GeneratedBy="10.1.1.165" ForDevices="10.1.1.165_17"
ForDeviceIPs="10.1.1.165" Summary="TCP forward connection error"
TunnelPeerIPDisconnected="10.1.1.212" AlertSubType="TCP_FORWARD_
CONNECTION_ALERT"
AlertableEventsCount="0"
```

TCP_FORWARD_FALLING_BEHIND_ALERT

Message attributes and sample message of TCP_FORWARD_FALLING_BEHIND_ALERT

Name	Value / Description
AlertSubType	TCP_FORWARD_FALLING_BEHIND_ALERT
Summary	TCP Forwarding Falling Behind

Sample Message

```
<133> Jul 10 20:29:43 2011 10.8.0.154 %LOGLOGIC-5-050711:
AlertPriority="HIGH" AlertType="SYSTEM_ALERT" AlertName="tcp forward
falling behind 001" GeneratedBy="10.8.0.154" ForDevices="10.8.0.154_
logapp" ForDeviceIPs="10.8.0.154" Summary="TCP Forwarding to 10.8.0.100
Falling Behind" AlertSubType="TCP_FORWARD_FALLING_BEHIND_ALERT"
AlertableEventsCount="0"
```

VPN_CONNECTIONS_ALERT

Message attributes and sample message of VPN_CONNECTIONS_ALERT

Name	Value / Description
VPNConnectivity	("DISCONNECTED" | "DENIED") User
	VPN User name
Group	VPN Group name
RemoteIP	Remote VPN IP address

Sample Message

```
<133> Mar 15 12:47:36 2009 10.1.1.165 %LOGLOGIC-5-050800:
AlertPriority="MEDIUM" AlertType="VPN_CONNECTIONS_ALERT"
AlertName="vpnConnalert" GeneratedBy="10.1.1.165" ForDevices="10.1.1.92_
7,test5_7,test4_6,10.1.1.100_1"
ForDeviceIPs="10.1.1.92,10.1.1.82,10.1.1.80,10.1.1.100"
ConfiguredForDevices="10.1.1.92_7,test5_7,test4_6,10.1.1.100_1"
VPNConnectivity="DISCONNECTED" User="swhitworth" Group=""
RemoteIP="65.5.224.151" AlertableEventsCount="1"
```

VPN_MESSAGES_ALERT

Message attributes and sample message of VPN_MESSAGES_ALERT

Name	Value / Description
VPNMsgArea	VPN message area
VPNMsgSeverity	VPN message severity
VPNMsgCode	VPN message code
VPNMsg	VPN message

Sample Message

```
<133> Mar 15 13:55:10 2009 10.1.1.165 %LOGLOGIC-5-050900:
AlertPriority="MEDIUM" AlertType="VPN_MESSAGES_ALERT"
AlertName="vpnMsgAlert" GeneratedBy="10.1.1.165" ForDevices="test4_6"
ForDeviceIPs="10.1.1.80" ConfiguredForDevices="test4_6" VPNMsgArea="IKE"
VPNMsgSeverity="6" VPNMsgCode="128" VPNMsg="%IKE-6-128: RPT=4585:
Connection attempt to VCPIP redirected to VCA peer 164.111.101.18 via
load balancing "AlertableEventsCount="0"
```

VPN_STATISTICS_ALERT

Message attributes and sample message of VPN_STATISTICS_ALERT

Name	Value / Description
AlertSubType	("VPN_CONNECTIONS"| "DENIED_VPN_CONNECTIONS" | "VPN_ CONNECTION_DURATION" | "BYTES_RECEIVED" | "BYTES_SENT")
Frequency	("PER_SECOND" | "PER_MINUTE" | "PER_HOUR" | "PER_DAY" | "PER_WEEK" | "PER_MONTH")
Relationship	("<" | ">" | "=" | "INCREASED_BY_MORE_THAN" | "DECREASED_BY_MORE_ THAN")
Threshold	Number of times a match occurred
User	VPN User name
Group	VPN Group name
RemoteIP	Remote VPN IP address

Sample Message

```
<133> Mar 15 16:03:12 2009 10.1.1.165 %LOGLOGIC-5-051001:
AlertPriority="MEDIUM" AlertType="VPN_STATISTICS_ALERT"
AlertName="vpnStatAlert" GeneratedBy="10.1.1.165" ForDevices="test4_6"
ForDeviceIPs="10.1.1.80" ConfiguredForDevices="test4_6"
AlertSubType="VPN_CONNECTIONS" Frequency="PER_MINUTE" Relationship=">"
Threshold="2" User="" Group="llvpn" RemoteIP="0.0.0.0"
AlertableEventsCount="14"
```

TIBCO Documentation and Support Services

For information about this product, you can read the documentation, contact TIBCO Support, and join TIBCO Community.

How to Access TIBCO Documentation

Documentation for TIBCO products is available on the TIBCO Product Documentation website, mainly in HTML and PDF formats.

The TIBCO Product Documentation website is updated frequently and is more current than any other documentation included with the product.

Product-Specific Documentation

The following documentation for this product is available on the TIBCO LogLogic® Log Management Intelligence Product Documentation page.

- *TIBCO LogLogic® Log Management Intelligence Release Notes*
- *TIBCO LogLogic® Log Management Intelligence Administration*
- *TIBCO LogLogic® Log Management Intelligence Configuration and Upgrade*
- *TIBCO LogLogic® Log Management Intelligence Hardware Installation Guide*
- *TIBCO LogLogic® Log Management Intelligence Log Source Report Mapping*
- *TIBCO LogLogic® Log Management Intelligence Security Guidelines*
- *TIBCO LogLogic® Log Management Intelligence SSD Hardware Field Installation*
- *TIBCO LogLogic® Log Management Intelligence Syslog Alert Message Format Quick Reference*
- *TIBCO LogLogic® Log Management Intelligence User Guide*
- *TIBCO LogLogic® Log Management Intelligence XML Import/Export Entities Reference*
- *TIBCO LogLogic® Enterprise Virtual Appliance Quick Start*

Other TIBCO Product Documentation

The following documents for TIBCO LogLogic® Log Source Packages are available on the TIBCO eDelivery website or TIBCO Support website after logging in.

- *TIBCO LogLogic® Log Source Packages Release Notes*
- *TIBCO LogLogic® Log Source Packages Installation and Upgrade*
- *TIBCO LogLogic® Log Source Packages Log Configuration Guides*
- *TIBCO LogLogic® Log Source Packages Log Collector Guides*

How to Contact TIBCO Support

Get an overview of TIBCO Support. You can contact TIBCO Support in the following ways:

- For accessing the Support Knowledge Base and getting personalized content about products you are interested in, visit the TIBCO Support website.
- For creating a Support case, you must have a valid maintenance or support contract with TIBCO. You also need a user name and password to log in to TIBCO Support website. If you do not have a user name, you can request one by clicking **Register** on the website.

How to Join TIBCO Community

TIBCO Community is the official channel for TIBCO customers, partners, and employee subject matter experts to share and access their collective experience. TIBCO Community offers access to Q&A forums, product wikis, and best practices. It also offers access to extensions, adapters, solution accelerators, and tools that extend and enable customers to gain full value from TIBCO products. In addition, users can submit and vote on feature requests from within the TIBCO Ideas Portal. For a free registration, go to TIBCO Community.

Legal and Third-Party Notices

SOME TIBCO SOFTWARE EMBEDS OR BUNDLES OTHER TIBCO SOFTWARE. USE OF SUCH EMBEDDED OR BUNDLED TIBCO SOFTWARE IS SOLELY TO ENABLE THE FUNCTIONALITY (OR PROVIDE LIMITED ADD-ON FUNCTIONALITY) OF THE LICENSED TIBCO SOFTWARE. THE EMBEDDED OR BUNDLED SOFTWARE IS NOT LICENSED TO BE USED OR ACCESSED BY ANY OTHER TIBCO SOFTWARE OR FOR ANY OTHER PURPOSE.

USE OF TIBCO SOFTWARE AND THIS DOCUMENT IS SUBJECT TO THE TERMS AND CONDITIONS OF A LICENSE AGREEMENT FOUND IN EITHER A SEPARATELY EXECUTED SOFTWARE LICENSE AGREEMENT, OR, IF THERE IS NO SUCH SEPARATE AGREEMENT, THE CLICKWRAP END USER LICENSE AGREEMENT WHICH IS DISPLAYED DURING DOWNLOAD OR INSTALLATION OF THE SOFTWARE (AND WHICH IS DUPLICATED IN THE LICENSE FILE) OR IF THERE IS NO SUCH SOFTWARE LICENSE AGREEMENT OR CLICKWRAP END USER LICENSE AGREEMENT, THE LICENSE(S) LOCATED IN THE “LICENSE” FILE(S) OF THE SOFTWARE. USE OF THIS DOCUMENT IS SUBJECT TO THOSE TERMS AND CONDITIONS, AND YOUR USE HEREOF SHALL CONSTITUTE ACCEPTANCE OF AND AN AGREEMENT TO BE BOUND BY THE SAME.

TIBCO, the TIBCO logo, the TIBCO O logo, and LogLogic are either registered trademarks or trademarks of TIBCO Software Inc. in the United States and/or other countries.

All other product and company names and marks mentioned in this document are the property of their respective owners and are mentioned for identification purposes only.

This software may be available on multiple operating systems. However, not all operating system platforms for a specific software version are released at the same time. See the readme file for the availability of this software version on a specific operating system platform.

THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT.

THIS DOCUMENT COULD INCLUDE TECHNICAL INACCURACIES OR TYPOGRAPHICAL ERRORS. CHANGES ARE PERIODICALLY ADDED TO THE INFORMATION HEREIN; THESE CHANGES WILL BE INCORPORATED IN NEW EDITIONS OF THIS DOCUMENT. TIBCO SOFTWARE INC. MAY MAKE IMPROVEMENTS AND/OR CHANGES IN THE PRODUCT(S) AND/OR THE PROGRAM(S) DESCRIBED IN THIS DOCUMENT AT ANY TIME.