Quest

Quest® InTrust 11.4.2

Setting Up Gathering of Syslog Data

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, and Join the Innovation are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

IMPORTANT, **NOTE**, **TIP**, **MOBILE**, or **VIDEO**: An information icon indicates supporting information.

InTrust Setting Up Gathering of Syslog Data
Updated - September 2020
Version - 11.4.2

Contents

Setting Up Gathering of Syslog Data

You can use the InTrust Deployment Manager console to collect and manage Syslog data that is received by InTrust Server. To enable Syslog data capture, you need to set up a Syslog collection, as follows:

- Specify the InTrust server that should listen for Syslog messages
- Specify the devices you want to audit
- Specify the repository where you want to store the collected Syslog data

You can add, delete and edit collections at any time.

The first time you run InTrust Deployment Manager, you are directed to the welcome page, where you are prompted to create a collection. Take the opportunity to create your Syslog collection.

You can create more collections at any time. For that, right-click **Collections** and select **New Syslog Collection**, and then follow the wizard steps.

Common Tasks for Syslog Collections

To add a Syslog collection

1. In the InTrust Deployment Manager console, go to the **Collections** view.
2. Right-click **Collections** and select **New Syslog Collection**.
3. In the **New Syslog Collection** wizard, specify a name and a description for the collection.
4. On the **Set Up Collection** step, specify the InTrust server from which you want to get Syslog audit data and repository. You can collect Syslog data from all devices that send Syslog messages to the InTrust server or specify certain devices by selecting one of the following options:
    a. **All Syslog data received by InTrust server**
    b. **Syslog data only from devices you specify on the next step**
5. If you select the **Syslog data only from devices you specify on the next step** option, add the devices you want on the next **Specify Syslog Devices** step. For that click the **Add** button and select **Devices**. In the **Specify Syslog Devices** dialog box, you can add devices from the list or specify the IP address (DNS name) of the certain device.
   Also you can upload a text file that contain a list of device IPs, for that click **Add** and select the **Import from file** option. A list file uses the plain text format. Each IP address must be a separate line in the file.

To add devices to a collection

Use any of the following methods:

- In the wizard that opens when you edit a Syslog collection, change the devices list on the **Specify Syslog Devices** step as described in the previous procedure.
- Select the devices you need in the **Syslog devices not in a collection** search folder in the navigation pane and click **Add to collection**, and then select the collection you need.

CAUTION: You cannot add a device from the **Syslog devices not in a collection** search folder to a collection if this collection and this device are related to different InTrust servers.

To delete Syslog devices from a collection

1. Right-click the Syslog collection and select **Edit Collection**.
2. In the wizard that opens, go to the **Specify Syslog Devices** step.
3. In the list of devices, select the devices you do not need, and click **Remove**.

To start a new repository

You can create a repository when you create a new Syslog collection or edit an existing collection, on the **Set Up Collection** step of the wizard. For finer-grained management of repositories, use the Storage view (for details, see Managing Repositories).

Passing Messages On

If both Syslog listening and forwarding are enabled for a repository at once, then incoming Syslog messages are forwarded unchanged. This happens independently of writing the messages to the repository.

Analyzing Syslog Collections

There are two predefined search folders for Syslog devices: **Syslog devices by collection** and **Syslog devices not in a collection**. Use them to locate the devices you need; for example, if you cannot find your device in any existing Syslog collection, it is probably available in the **Syslog devices not in a collection** search folder.

For all Syslog devices contained in the **Syslog devices not in a collection** search folder, the **Received** field shows the the time when the InTrust server last received an event from the device. For devices that are included in collections, the corresponding field is called **Timestamp**, and it contains the time when a Syslog message was last generated by the device (or, if this cannot be determined, the time when the InTrust server last received an event from the device).

A device can have the **Collecting** or **Not Collecting** status. If the InTrust server does not receive events from the device for a week, the device changes status to **Not Collecting**.

When a Syslog collection is selected, the right pane shows a table with information about the collection members. The table supports multi-level grouping of devices, so that you can organize them in tree-like views using any criteria. For example, to quickly find out which devices are currently not collecting any data, you can group computers by source status, then by device name.

To use multi-level grouping, drag table column names from the devices list to the area above the list. The device list changes accordingly.

Message Parsing Specifics

InTrust parses the Syslog messages it captures to store a useful representation of them in the repository. Only UDP v4 is used for receiving messages, and they can use either ASCII or UTF-8.

Messages are expected to conform to either RFC 3164 or RFC 5424. The fields of an event entry in the repository are filled in from the fields of a Syslog message.

A message is parsed until the end or until a mismatch occurs. The parser breaks down the message into as many insertion strings as it can. No matter how many fields InTrust is able to parse successfully—all of them, just the first three or none at all—the entire message text is saved in the Description field. This enables you to find the message in Repository Viewer (by using the **Any field** parameter) or IT Security Search even if the fields are not mapped properly.

RFC 3164 Specifics

The following pattern is defined in RFC 3164:

```
<PRI>TIMESTAMP HOSTNAME TAG: MSG
```

An example of a valid message is as follows:

```
<34>Oct 14 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8
```

The **PRI** field indicates the facility and severity. For details, see Treatment of Facility and Severity Information.

A message has the following parts:

Field	Details
PRI	Indicates the facility and severity. For details, see Treatment of Facility and Severity Information.
TIMESTAMP	See Treatment of Timestamps (RFC 3164).
HOSTNAME	The name of the host as returned by the **hostname** command. If it is unknown, the host puts its own IP address in this field.
TAG	This is a piece of data that can help classify the message. It is often followed by the process ID in square brackets. If the process ID is not used, it is followed by a colon.
MSG	The body of the message.

Treatment of Timestamps (RFC 3164)

If the timestamp cannot be parsed, the **Time** event field stores a part of the time that the event was written to the repository (in the InTrust server's time zone). Note that this field is supposed to contain local times. The GMT timestamp is derived from the parsed value. The message contains no time zone information, so it is important that the Syslog device and the InTrust server should best be located in the same time zone; otherwise, the local and GMT timestamps will be wrong.

The RFC 3164 format does not specify the year in the timestamp. However, when capturing messages, InTrust must supply the year to form a valid event date. Normally, this only matters for a fraction of a second at midnight on January 1st, because the year can change while a message is in transit.

In rare cases, messages are accumulated and need to be submitted after a delay. For example, some applications that can send Syslog will hold events until Syslog forwarding is configured. When these stored messages cross a calendar year, they can end up with an incorrect timestamp that appears to be in the future when in reality they are from the past.

When InTrust receives a Syslog message without the year, it assumes the message has the current year value. However, it can decide to change the year. If this timestamp appears to be more than six months in the future (same year), InTrust changes it to the previous year. For example, in March 2018 you get messages from November. There's no same-year date six months before March, and November 2018 is more than six months ahead, so the resulting date is in November 2017.

RFC 5424 Specifics

The following pattern is defined in RFC 5424 (the header is **bolded**):

<PRI>VERSION TIMESTAMP HOSTNAME APP-NAME PROCID MSGID STRUCTURED-DATA MSG

A message has the following parts:

Field	Details
PRI	Indicates the facility and severity. For details, see Treatment of Facility and Severity Information.
VERSION	Syslog version. The presence of a digit after the **PRI** field is how InTrust can tell this is an RFC 5424-compliant message. However, it doesn't matter which digit it is.
TIMESTAMP	See Treatment of Timestamps (RFC 5424).
HOSTNAME	This can be an FQDN, IPv4 address, IPv6 address or conventional hostname. It can also be omitted with “-”. Examples of valid host names: • Machinename • Myhost.domain.com • 10.30.44.135 • fe80::5d3b:41f:38d2:a1b1%13
APP-NAME	This field identifies the application that sent the message. It can be omitted with “-”. InTrust does not process this data.
PROCID	This field is often used to provide the process name or process ID associated with a Syslog system. It can be omitted with “-”. InTrust does not process this data.
MSGID	This field should identify the type of message. For example, a firewall might use the MSGID "TCPIN" for incoming TCP traffic and the MSGID "TCPOUT" for outgoing TCP traffic. It can be omitted with “-”. InTrust does not process this data.
STRUCTURED-DATA	This is a collection of arbitrary key-value pairs. It can be omitted with “-”. InTrust does not process this data.

Examples of valid messages:

- `<165>1 2015-05-11T22:14:15.003Z SUPERHOST1 myproc 8710 - - %% It's time to make the do-nuts.`
- `<165>1 2003-10-11T22:14:15.003Z mymachine.domain.com evntslog - ID47 [exampleSDID@32473 iut="3" eventSource="Application" eventID="1011"]`
  Message with structured data in the UTC time zone
- `<140>1 2003-10-11T22:14:15.003+3:00 10.30.44.245 evntslog - ID47`
  Message with a non-UTC time zone and IP address instead of host name

For an in-depth description of the format, see Section 6 of RFC 5424.

Treatment of Timestamps (RFC 5424)

The timestamp in a message can contain such details as the time zone and milliseconds. Millisecond information is lost when a message is converted to an event entry. It is also possible that the timestamp is omitted altogether, replaced by "-".

The following are examples of valid timestamps:

```
2015-05-12T19:20:50.52-04:00
2015-05-11T22:14:15.003Z
2015-05-24T05:14:15.000003-07:00
-
```

The following timestamps are malformed:

`2015-08-24T05:14:15.000000003-07:00`
Too many decimal places (there should be no more than six).

`08-24-2015T05:14:15-07:00`
The order of units in the date is wrong.

`2015/08/24T05:14:15-07:00`
You cannot use separators other than "–" and ":" in the time part.

If the timestamp cannot be parsed or it is omitted, InTrust substitutes the current time during event generation (in the InTrust server's time zone). The parsed (or substituted) timestamp goes to the **Date** and **Time** fields of the event. Note that messages are supposed to contain local times.

The GMT timestamp is derived from the resulting value, as follows:

- If the time zone is specified, it is used for offsetting the GMT timestamp.
- A message must have either time zone information or local offset information; if neither is available, the timestamp cannot be parsed.

Mapping of Event Fields

When InTrust generates an event entry based on a Syslog message, it uses the rules outlined in the table below. It shows what happens to the following example message:

- RFC 3164-compliant format
  `<34>Oct 14 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8`
- RFC 5424-compliant format
  `<34>1 2014-10-14T22:14:15+03:00 mymachine su - ID47 - 'su root' failed for lonvick on /dev/pts/8`

Event field	Value	In the example above
Log	Syslog	Syslog
Event Type	*Severity value, derived from the **PRI** field. For details, see Treatment of Facility and Severity Information.* *There are more severities than event types, and they are mapped as follows:* • *0–3: error* • *4: warning* • *5–7: information*	error
Source	Syslog Device	Syslog Device
Category	*Facility value, derived from the **PRI** field.*	security
Event ID	0	0
Date	*The date the event occurred or was put in the repository. For details, see Treatment of Timestamps (RFC 3164) or Treatment of Timestamps (RFC 5424).*	10/14/2014
Time	*For details, see Treatment of Timestamps (RFC 3164) or Treatment of Timestamps (RFC 5424).*	22:14:15
User	*Not used.*	
Computer	*The **HOSTNAME** field, if it can be parsed. This is the host where the event occurred.* *If the host name cannot be parsed or is omitted, then InTrust substitutes the IP address of the host that the message came from.*	mymachine
Description	*The entire message, restored from the insertion strings it was broken down into.*	<34>Oct 14 22:14:15 mymachine su: 'su root' failed for lonvick on /dev/pts/8 <34>1 2014-10-14T22:14:15+03:00 mymachine su - ID47 - 'su root' failed for lonvick on /dev/pts/8
Insertion String #1	*The host that sent the message; not necessarily the same host that the event occurred on.*	mymachine

Treatment of Facility and Severity Information

In both RFC 3164 and RFC 5424, the PRI field indicates the facility and severity. The following table shows how PRI values are interpreted:

Severity → Facility ↓	emergency	alert	critical	error	warning	notice	info	debug
kernel	0	1	2	3	4	5	6	7
user	8	9	10	11	12	13	14	15
mail	16	17	18	19	20	21	22	23
system	24	25	26	27	28	29	30	31
security	32	33	34	35	36	37	38	39
syslog	40	41	42	43	44	45	46	47
lpd	48	49	50	51	52	53	54	55
nntp	56	57	58	59	60	61	62	63
uucp	64	65	66	67	68	69	70	71
time	72	73	74	75	76	77	78	79
security	80	81	82	83	84	85	86	87
ftpd	88	89	90	91	92	93	94	95
ntpd	96	97	98	99	100	101	102	103
logaudit	104	105	106	107	108	109	110	111
logalert	112	113	114	115	116	117	118	119
clock	120	121	122	123	124	125	126	127
local0	128	129	130	131	132	133	134	135
local1	136	137	138	139	140	141	142	143
local2	144	145	146	147	148	149	150	151
local3	152	153	154	155	156	157	158	159
local4	160	161	162	163	164	165	166	167
local5	168	169	170	171	172	173	174	175
local6	176	177	178	179	180	181	182	183
local7	184	185	186	187	188	189	190	191

Treatment of Named Fields

Syslog messages can contain pieces of information that are semantically key–value pairs. There is no agreed-upon notation for such items, so the syntax may vary from provider to provider. InTrust attempts to analyze

incoming messages to spot key–value information.

During message parsing, InTrust first tries to detect a pattern that indicates the presence of keys. The pattern for a key is like this: separator followed by single word followed by assignment marker. These three elements are distinguished as follows:

- The separator is white space, a comma or a semicolon.
- The word is alphanumeric without spaces in the middle and doesn't start with a number or underscore.
- The assignment marker is a colon or equals sign. It may or may not contain white space to the left or right of it. As long as the use of white space is consistent, the assignment marker will be spotted.

If a combination of these features occurs repeatedly in a message, then InTrust considers it a pattern and treats the matching words as keys and the substrings to the right of them as values.

InTrust puts the discovered key–value pairs in the named strings of event records.

IMPORTANT:

- Sometimes a Syslog message contains a multi-value field expressed as multiple occurrences of the same key with different values. InTrust repository records cannot have multi-value fields, so in such cases the resulting value will be a concatenation of all the string values for the key.
- If a substring looks like a key–value pattern but is enclosed in quotation marks, it is not split into fields and can be treated as part of the value for some key.

Tags

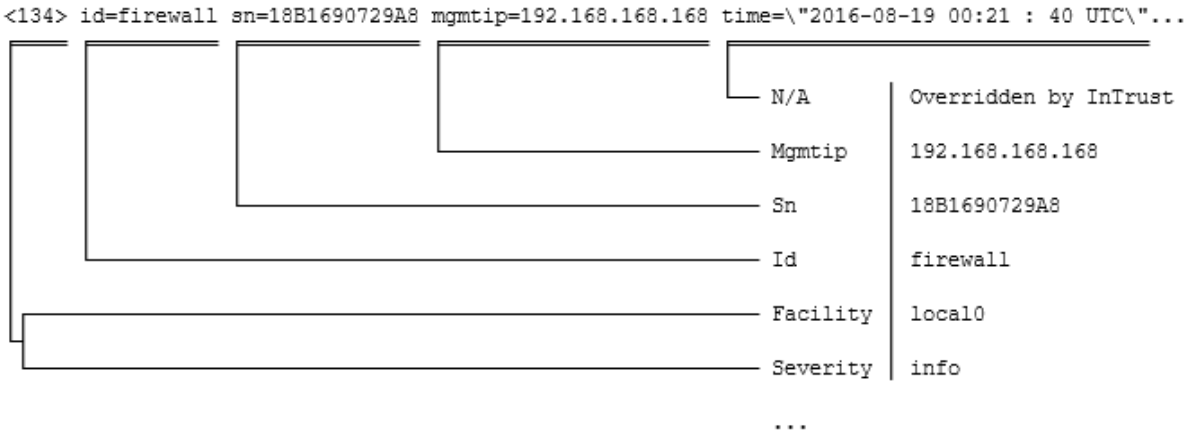
Messages from some Syslog providers include a piece of information that is traditionally referred to as a *tag*. It isn't usually marked in any way, and its position is defined by a set of rules. For example, in a message like "<54>Dec 31 23:51:36 sm-w2k12-001 SymantecServer: sm-w2k12-001,Local: 10.30.38.109,Local: 514..." the tag is **SymantecServer**.

InTrust detects such tags and puts them in the **Tag** field. If they match the key–value pattern, it also forms named fields from them.

Example 1

```
<134> id=firewall sn=18B1690729A8 mgmtip=192.168.168.168 time=\"2016-08-19 00:21 : 40
UTC\" fw=10.205.123.15 m=96 n=24789 i=60 lic=0 pt=8080.8443 usestandbysa=0 dyn=n.e
ai=1 fwlan=192.168.168.168 conns=18
```

Here is how the fields are extracted:



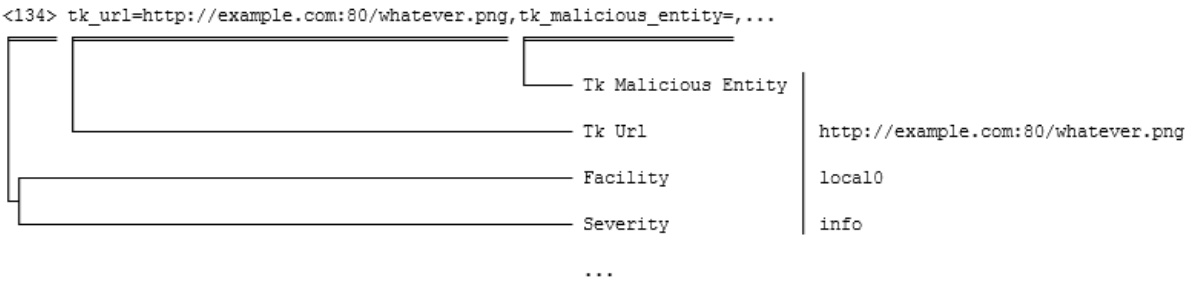
The parser decides that a white space means a separator, and an equals sign without white space on either side is the assignment marker. Therefore, the following fields are discovered:

Facility	local0
Severity	info
Where	10.30.35.174
Ai	1
Conns	18
Dyn	n.e
Fw	10.205.123.15
Fwlan	192.168.168.168
I	60
Id	firewall
Lic	0
M	96
Mgmtip	192.168.168.168
N	24789
Pt	8080.8443
Sn	18B1690729A8
Usestandbysa	0
When	9/5/2018 5:18:32 PM

Example 2

```
<134> tk_url=http://example.com:80/whatever.png,tk_malicious_entity=,tk_file_name=,tk_
entity_name=,tk_action=,tk_scan_type=WebReputation,tk_blocked_by=policy,tk_rule_
name=IJVIRUS,tk_opp_id=0,tk_group_name=None,tk_category=Web Reputation - Very Low,tk_
uid=0000002836-626130ec1beb9bfdaab2,tk_filter_action=3
```

Here is how the fields are extracted:



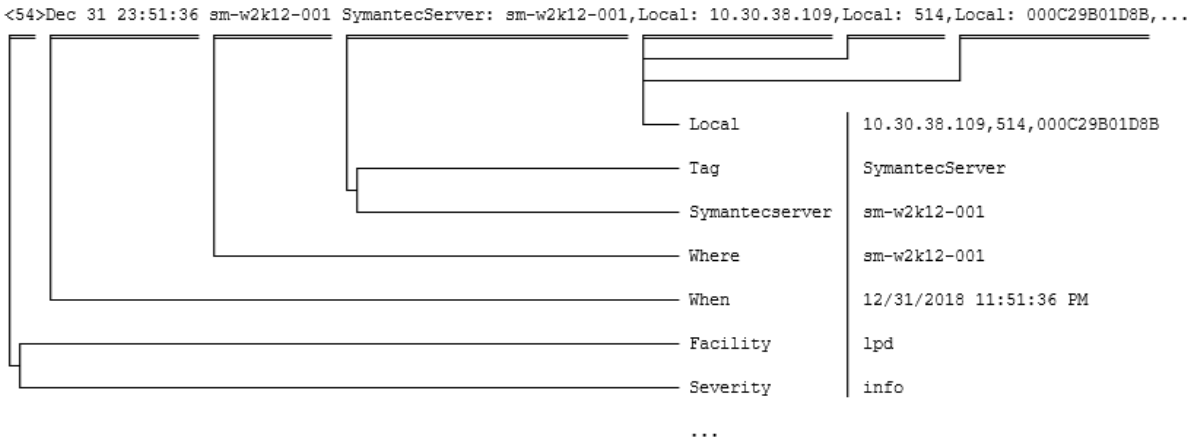
A comma is recognized as the separator, and an equals sign without white space on either side is the assignment marker. Some fields (such as **tk_action** and **tk_malicious_entity**) are detected and receive empty values. The following non-empty fields are discovered:

Facility	local0
Severity	info
Where	10.30.35.174
Tk Blocked By	policy
Tk Category	Web Reputation - Very Low
Tk Filter Action	3
Tk Group Name	None
Tk Opp Id	0
Tk Rule Name	IJVIRUS
Tk Scan Type	WebReputation
Tk Uid	0000002836-626130ec1beb9bfdaab2
Tk Url	http://example.com:80/whatever.png
When	9/5/2018 5:18:24 PM

Example 3

```
<54>Dec 31 23:51:36 sm-w2k12-001 SymantecServer: sm-w2k12-001,Local:
10.30.38.109,Local: 514,Local: 000C29B01D8B,Remote: 10.30.44.167,Remote: ,Remote:
58800,Remote: 0003BAF4AAD9,UDP,Inbound,Begin: 2017-12-31 23:57:38,End: 2017-12-31
23:57:39,Occurrences: 3,Application: ,Rule: Block all other IP traffic and
log,Location: Default,User: Administrator,Domain: SM-W2K12-001,Action: Blocked
```

Here is how the fields are extracted:



Here a colon followed by white space is assumed to be the assignment marker and the separator is a comma. The **Local** and **Remote** fields occur multiple times, so both of them get concatenated values. The resulting named strings are as follows:

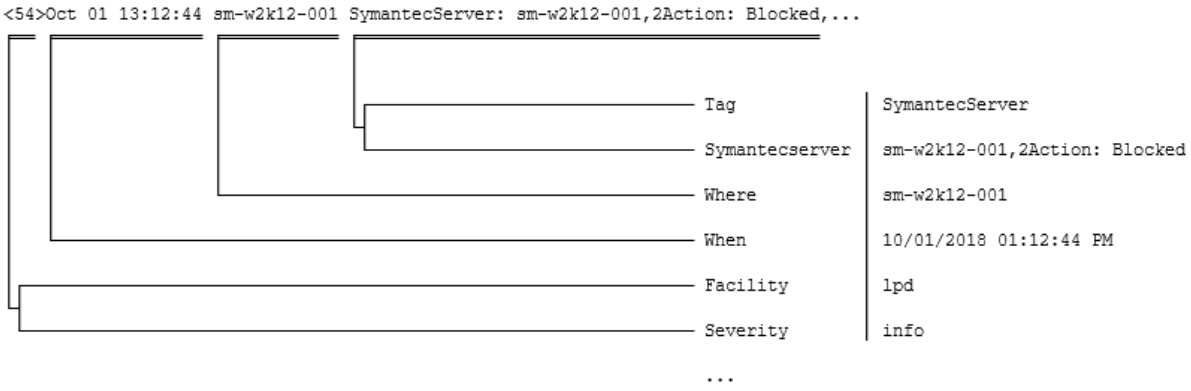
Facility	lpd
Severity	info
Where	sm-w2k12-001
Action	Blocked
Domain	sm-w2k12-001
Location	Default
Rule	Block all other IP traffic and log
Begin	2017-12-31 23:57:38
End	2017-12-31 23:57:39
Local	10.30.38.109, 514, 000C29B01D8B
Occurrences	3
Remote	10.30.44.167, , 58800, 0003BAF4AAD9,UDP,Inbound
Symantecserver	sm-w2k12-001
User	Administrator
When	12/31/2018 11:51:36 PM

Example 4

```
<54>Oct 01 13:12:44 sm-w2k12-001 SymantecServer: sm-w2k12-001,2Action: Blocked,Local:
10.30.38.109,Local: 514,Local: 000C29B01D8B,Remote: 10.30.44.167,Remote: ,Remote:
58800,Remote: 0003BAF4AAD9,UDP,Inbound,Begin: 2017-12-31 23:57:38,End: 2017-12-31
```

```
23:57:39,Application: ,Rule: Block all other IP traffic and log,Location:
Default,User: Administrator,Domain: SM-W2K12-001
```

In this example, see what happens to the substring **2Action** that could be a key if it didn't start with a digit:



Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions
- Chat with support engineers online
- View services to assist you with your product