Quest®

Quest® InTrust 11.4

Preparing for Auditing Trend Micro InterScan Web Security

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 Preparing for Auditing Trend Micro InterScan Web Security
Updated - October 2018
Version - 11.4

Contents

Knowledge Pack Overview

The InTrust Knowledge Pack for Trend Micro InterScan Web Security Virtual Appliance works with Syslog messages forwarded from Trend Micro InterScan Web Security virtual appliances to Linux hosts. These messages are treated as events, which InTrust can collect and monitor for.

For the complete list of supported events, see Audited Events.

Requirements

InTrust supports gathering and real-time monitoring of Syslog messages from InterScan Web Security Virtual Appliance 6.5.

Auditing uses a Linux host as an intermediary. InTrust supports the following Linux distributions for this purpose:

- Red Hat Enterprise Linux 7, 6.6, 6.5, 6.4, 6.3, 5, 4
- Oracle Linux 7, 6.6, 6.5, 6.4, 6.3

InterScan Web Security auditing may work on other distributions supported by InTrust, but this was not tested.

To prepare a Linux host, you need to install an InTrust agent and adjust the configuration of the Syslog flavor used. Currently, agents must be installed manually on each Linux host you want to cover.

Installation

The Linux Knowledge Pack is installed on top of an existing InTrust installation. The following objects are included:

- "IWSVA through Oracle Linux Syslog" data source
- "IWSVA hosts" site
- "IWSVA: All Syslog Events" gathering policy
- "IWSVA Syslog consolidation" consolidation policy
- "IWSVA Syslog collection" task, containing "IWSVA Syslog collection" gathering job
- "Trend Micro IWSVA Security" real-time monitoring policy
- Real-time monitoring rules:
    - Virus detected
    - Spyware detected
    - Command and control callback detected
    - Data loss prevention detected

Installing Agents

InTrust agents must be installed manually on Linux hosts. For details, see Installing Agents Manually on Linux Computers.

Syslog Configuration

InTrust takes advantage of the Syslog logging system on Linux computers. It is implemented by the Syslog daemon, which accepts messages from various sources that support logging, and either writes these messages to files or passes them on to other hosts in the network.

You need to permit the Syslog daemon to receive logs from the Trend Micro virtual appliance on the proxy Red Hat host. For that, perform the *Enabling Reception of External Syslog Messages* procedure described in the Syslog Configuration topic. After this, you should be ready to receive events from the appliance.

InTrust Configuration

After you have taken all the necessary configuration steps on the target Linux hosts, the InTrust server takes over all auditing and real-time monitoring operations. Linux auditing and real-time monitoring is similar to working with any other system supported by InTrust. Use the InTrust Manager console to set up audit data gathering and monitoring.

There is only one important difference that refers to active scheduling of the InTrust tasks. For information see the warning note below.

> **CAUTION: An active schedule on an InTrust task is required to make the agent cache events. If the schedule is disabled, no events are stored. The "IWSVA through Oracle Linux Syslog" data source uses event caching, so it is recommended that you use at least one task for the cache-enabled data sources that run regularly. If you want to gather data only on demand, you must still enable the schedule for your task or tasks, but set it to a point in the future or in the past.**

The other operations do not have special requirements, and you can perform them as described in the Auditing Guide and Real-Time Monitoring Guide.

Data Source Details

The "IWSVA through Oracle Linux Syslog" data source represents InterScan Web Security Syslog audit trails. It analyzes the flow of data forwarded to the Syslog daemon and makes meaningful event records from the data.

The data source uses a list of regular expressions. When the data source is working, it applies the expressions, in the order specified, to each message. The order of the regular expressions matters because message processing stops as soon as the message matches one of the expressions. During parsing, pairs of parentheses are used in regular expressions to break messages up into numbered fields.

> **CAUTION: It is not recommended that you modify predefined regular expressions in the data source. However, you can experiment with a copy of the predefined data source if necessary. Do not include a lot of complex regular expressions in the data source, because that may slow down Syslog processing significantly.**

InterScan Web Security Virtual Appliance Configuration

After you have set up the Syslog daemon, as described in Syslog Configuration, and adjusted the gathering settings in InTrust, as described in InTrust Configuration, configure forwarding of InterScan Web Security Virtual Appliance logs to the Linux host. The Linux host with an installed InTrust agent will act as a Syslog listener.

For information on how to configure the logs to be sent to the Syslog server, refer to InterScan Web Security Virtual Appliance documentation.

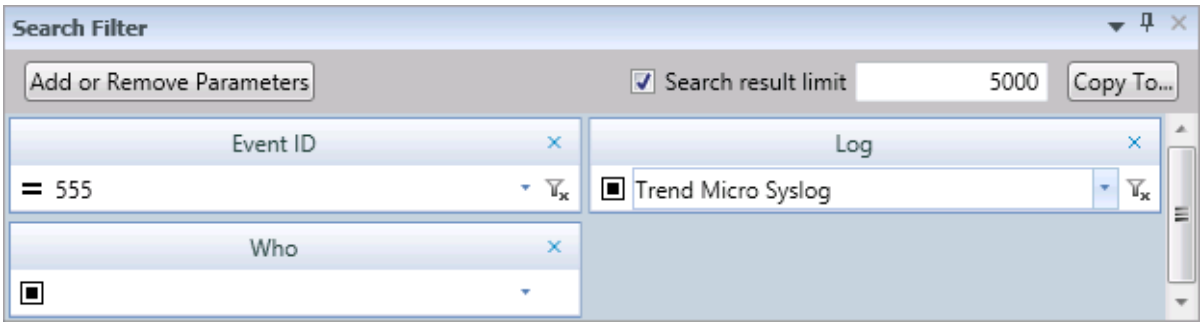
Use Scenarios

For these scenarios to work, first include the necessary Linux host or hosts the "IWSVA hosts" site.

Tracking URL Access

After you have made sure that InTrust collects virtual appliance logs to the repository, you can view the logs in InTrust Repository Viewer. Suppose you want to focus on URL access. For that purpose, you can create a custom Repository Viewer search folder which includes event ID 555 from the and use the Who field from Normalized Strings as well as any other filter parameters as follows:

1. In InTrust Repository Viewer create a new search folder. For that, right-click **Custom Search Folders** and select **Create Search**.
2. In the Search Filter pane, click **Add or Remove Parameters**, switch from **Normalized Strings** to **All** and enable **Event ID**, **Log** and **Who**.
3. In the **Event ID** field, specify **555**.
4. In the **Log** field, specify **Trend Micro Syslog**.
5. In the **Who** field, specify the users whose URL access you want to track.



Now you can track URL access by these users. Click **Go** to view available events. You can configure the configure the layout of the result grid as necessary. For more details, see Searching for Events in Repository Viewer.

Monitoring for Viruses

In this scenario, you configure InTrust to raise alerts whenever a virtual appliance detects a virus. Take the following steps in InTrust Manager:

1. Open the properties of the **Trend Micro IWSVA Security | Detection log | Virus detected** real-time monitoring rule and enable the rule.

2. Open the properties of the **Trend Micro IWSVA Security** real-time monitoring policy, go to the **E-mail** tab and specify the operators that should be notified when the alerts are raised. If the people you want to notify are not listed, you can manage notification operators as described in Configuring Notification Groups and Operators.
3. Activate the **Trend Micro IWSVA Security** real-time monitoring policy.
4. Click the **Commit** button in the toolbar to apply your configuration changes.

After this, the specified operators will get email notifications every time the virtual appliance sends a virus detection message to the monitored Linux host, and InTrust will trigger alerts, which you can view and manage in Monitoring Console.

Audited Events

This topic lists Trend Micro InterScan Web Security Virtual Appliance events that InTrust recognizes during task-based gathering and real-time monitoring.

Detection Log

Virus Found

Original ID: EVT_VIRUS_FOUND | LOG_CRIT

InTrust event ID: 547

Fields:

Field name in original event	Field description	Insertion string in InTrust event
tk_username	User ID (client IP address)	6
tk_date_field	Date and time	7
tk_protocol	Protocol	8
tk_url	URL	9
tk_malicious_entity	Types of malware	10
tk_file_name	File name	11
tk_entity_name	Detected malware name	12
tk_action	Processing	13
tk_scan_type	Scan type	14
tk_blocked_by	[unused]	15
tk_rule_name	Rule (policy) name	16
tk_opp_id	[unused]	17
tk_group_name	Group name (if LDAP is available)	18
tk_category	Category	19
tk_uid	Internal ID	20

Spyware Found

Original ID: EVT_SPYWARE_FOUND | LOG_CRIT

InTrust event ID: 548

Fields: same as for Virus Found

Data Loss Prevention

Original ID: EVT_DLP_FOUND | LOG_CRIT

InTrust event ID: 549

Fields:

Field name in original event	Field description	Insertion string in InTrust event
tk_username	User ID (client IP address)	6
tk_date_field	Date and time	7
tk_entity_name	Template name	12
tk_rule_name	Rule (policy) name	16
tk_group_name	Group name (if LDAP is available)	18
tk_scan_type	Scan type	14
tk_action	Processing	13
tk_protocol	Protocol	8
tk_url	URL	9
tk_malicious_entity	Matched content	10
tk_file_name	File name	11
tk_uid	Internal ID	20

Command and Control Callback

Original ID: EVT_C&C_CALLBACK_FOUND | LOG_CRIT

InTrust event ID: 550

Fields:

Field name in original event	Field description	Insertion string in InTrust event
tk_username	User ID (client IP address)	6
tk_date_field	Date and time	7
tk_protocol	Protocol	8
tk_url	URL	9
tk_domain	Domain	15
tk_device_name	Device name (host name)	11
tk_rule_name	Rule (policy) name	16
tk_group_name	Group name (if LDAP is available)	18
tk_client_ip	Client IP address	13
tk_server_ip	Server IP address	14
tk_destination_port	Destination port	12
tk_ccca_source	Detection source: • 0: Web reputation • 1: Virtual analyzer (sandbox) • 2: Other than virtual analyzer (sandbox)	17
tk_risk_level	Risk level: • 0: Unknown • 1: Low • 2: Medium • 3: High	19
tk_filter_action	Filtering action: • 0: Authorize • 1: Block • 2: Monitor	21

URL Access Log

URL Blocking

Original ID: EVT_URL_BLOCKING | LOG_CRIT

InTrust event ID: 551

Fields:

Field name in original event	Field description	Insertion string in InTrust event
tk_username	User ID (client IP address)	6
tk_date_field	Date and time	7
tk_protocol	Protocol	8
tk_url	URL	9
tk_malicious_entity	[unused]	10
tk_file_name	File name	11
tk_entity_name	[unused]	12
tk_action	[unused]	13
tk_scan_type	Search type	14
tk_blocked_by	Reason for blocking	15
tk_rule_name	Rule (policy) name	16
tk_opp_id	[unused]	17
tk_group_name	Group name (if LDAP is available)	18
tk_category	Category	19
tk_uid	Internal ID	20
tk_filter_action	Filtering action: • 0: Block by URL filter without HTTP inspection • 1: Block by URL filter with HTTP inspection • 2: Monitor • 3: Warn • 4: Warn and continue	21

URL Monitoring

Original ID: EVT_URL_MONITORING | LOG_CRIT
InTrust event ID: 552
Fields: same as for URL Blocking

URL Warning

Original ID: EVT_URL_WARNING | LOG_CRIT
InTrust event ID: 553
Fields: same as for URL Blocking

URL Warning and Continue

Original ID: EVT_URL_WARN_AND_CONTINUING | LOG_CRIT
InTrust event ID: 554
Fields: same as for URL Blocking

URL Access Tracking

Original ID: EVT_URL_ACCESS_TRACKING | LOG_INFO

InTrust event ID: 555

Fields:

Field name in original event	Field description	Insertion string in InTrust event
tk_username	User ID (client IP address)	6
tk_url	URL	9
tk_size	File size	10
tk_date_field	Date	7
tk_protocol	Protocol	8
tk_mime_content	MIME content type	17
tk_server	Server (host name)	12
tk_client_ip	Client IP address	13
tk_server_ip	Server IP address	14
tk_domain	Domain	15
tk_path	Path	16
tk_file_name	File name	11
tk_operation	Request method	18
tk_uid	Internal identification ID	20
tk_category	Category ID For details about category mapping, see **/etc/iscan/urlfcMapping.ini**	19
tk_category_type	Category type • 0: Initial category • 1: Custom category	21

FTP Log

FTP Get

Original ID: EVT_FTP_GET | LOG_INFO
InTrust event ID: 556
Fields: same as for URL Access Tracking

FTP Put

Original ID: EVT_FTP_PUT | LOG_INFO
InTrust event ID: 557
Fields: same as for URL Access Tracking

Application Control Log

Protocol Block

Original ID: EVT_APP_CONTROL_BLOCK | LOG_CRIT

InTrust event ID: 558

Fields:

Field name in original event	Field description	Insertion string in InTrust event
tk_username	User ID (client IP address)	6
tk_date_field	Date and time	7
tk_category	Category	19
tk_protocol	Application name	8
tk_rule_name	Rule (policy) name	16
tk_group_name	Group name (if LDAP is available)	18
tk_client_ip	Client IP address	13

System Log

Performance Event

Original ID: EVT_PERFORMANCE | LOG_INFO

InTrust event ID: 559

Fields:

Field name in original event	Field description	Insertion string in InTrust event
tk_server	Server (host name)	12
tk_date_field	Date and time	7
tk_metric_id	Measured metric	8
tk_metric_value	Measured value	9

System Information Event (Success)

Original ID: EVT_SYSEVENT_AU_SUCC | LOG_INFO

InTrust event ID: 560

Fields:

Field name in original event	Field description	Insertion string in InTrust event
tk_server	Server (host name)	12
tk_date_field	Date and time	7
tk_source	Event source	9
tk_description	Description	8

System Information Event (Failure)

Original ID: EVT_SYSEVENT_AU_FAIL | LOG_xxx

InTrust event ID: 561

Fields: same as for System Information Event (Success)

Audit Log

Audit Event

Original ID: EVT_AUDITING | LOG_WARNING

InTrust event ID: 562

Fields:

Field name in original event	Field description	Insertion string in InTrust event
tk_user	User login	6
tk_date_field	Date and time	7
tk_description	Description	8

We are more than just a name

We are on a quest to make your information technology work harder for you. That is why we build community-driven software solutions that help you spend less time on IT administration and more time on business innovation. We help you modernize your data center, get you to the cloud quicker and provide the expertise, security and accessibility you need to grow your data-driven business. Combined with Quest's invitation to the global community to be a part of its innovation, and our firm commitment to ensuring customer satisfaction, we continue to deliver solutions that have a real impact on our customers today and leave a legacy we are proud of. We are challenging the status quo by transforming into a new software company. And as your partner, we work tirelessly to make sure your information technology is designed for you and by you. This is our mission, and we are in this together. Welcome to a new Quest. You are invited to Join the Innovation™.

Our brand, our vision. Together.

Our logo reflects our story: innovation, community and support. An important part of this story begins with the letter Q. It is a perfect circle, representing our commitment to technological precision and strength. The space in the Q itself symbolizes our need to add the missing piece — you — to the community, to the new Quest.

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