Quest® InTrust 11.4.2

Preparing for Auditing Cisco PIX Firewall

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

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.**

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

InTrust Preparing for Auditing Cisco PIX Firewall
Updated - September 2020
Version - 11.4.2

Contents

Cisco PIX Firewall Auditing Overview 4

Getting Started with Cisco PIX Auditing 5

About us 6

Contacting Quest 6

Technical support resources 6

Cisco PIX Firewall Auditing Overview

The Firewalls Knowledge Pack expands the auditing and reporting capabilities of InTrust to Cisco PIX. The necessary data is provided by the Cisco PIX log in plain text format.

Use the following InTrust objects to work with data related to Cisco PIX Firewall:

- “Cisco PIX text Log” data source
- “Cisco PIX Firewall: All Events” gathering policy
- “Cisco PIX Firewall: All Events” import policy
- “Cisco PIX Firewall log daily collection” task
- “Cisco PIX Firewall weekly reporting” task
- “All syslog servers for Cisco PIX firewalls” site

The Knowledge Pack includes the Cisco PIX report pack. You can schedule the reports with the “Cisco PIX Firewall weekly reporting” task.

Getting Started with Cisco PIX Auditing

The predefined Cisco PIX data source works with Cisco PIX Firewall log data in ASCII format. The log files are located on a Syslog server, which receives Syslog messages from the Cisco PIX Firewall computer.

The data source works with the following log formats:

1. <date/time> <facility>.<severity> <hostname> <message>
2. <date>,<time>,<host>,<facility>,<severity>,<DateTime_generated>: <message>

An example of a message in the log is as follows:

```
%PIX-6-605005: Login permitted from 192.168.0.3/2629 to inside:192.168.0.1/https for
user "enable_15"
```

The format depends on the **syslogd** daemon used and its settings. You may need to change the data source to suit your log format.

To configure gathering of the Cisco PIX Firewall log

1. On the Cisco Firewall computer, configure sending of Syslog messages to a Syslog server, which will act as an intermediary computer. For detailed information about the settings, see Cisco PIX documentation.
2. Install the InTrust agent on the Syslog server to gather the log. The agent is not required if the log files are located in a share on a Windows computer or an SMB share on a Unix computer.
3. In InTrust Manager, edit the Cisco PIX data source. Specify the log file name and location; you can use regular expressions and wildcards.
   If you want to gather without an agent, specify the path using the %COMPUTER_NAME% variable and a share name (**\\%COMPUTER_NAME%\*share_name***).
4. Make sure the “All Syslog servers for Cisco PIX firewalls” site includes the intermediary computer.
   If the log is located in an SMB share on a Unix host, and you want to gather the log without an agent, you need to manually create a site under the Microsoft Windows Network node, and include the Unix computer in it. This is necessary because InTrust currently supports gathering from network shares only in Microsoft Windows Environment sites; this workaround makes InTrust aware of the share even though the processed computer is not actually running Windows.
5. Schedule the “Cisco PIX Firewall log daily collection” task. Make sure the gathering job within this task uses the “Cisco PIX Firewall: All Events” gathering policy.
   For agentless gathering from an SMB share on a Unix host, you need to create a separate gathering policy under the **Gathering | Gathering Policies | Microsoft Windows Network** node and use the policy in the gathering job instead of “Cisco PIX Firewall: All Events”. In this scenario, the **Use agents to execute this job on target computers** option must be turned off for the gathering job.
6. Schedule the “Cisco PIX Firewall log weekly reporting” task. Configure the reporting job within this task to create the reports you need.

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