Quest®

Quest® InTrust 11.3

Preparing for Auditing CheckPoint Firewall

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 Preparing for Auditing CheckPoint Firewall
Updated - May 2017
Version - 11.3

Contents

CheckPoint Firewall Auditing Overview

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

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

- “CheckPoint Firewall-1 text Log” data source
- “CheckPoint Firewall: All Events” gathering policy
- “CheckPoint Firewall: All Events” import policy
- “CheckPoint Firewall log daily collection” task
- “CheckPoint Firewall weekly reporting” task
- “All CheckPoint firewalls” site

The Knowledge Pack also provides the CheckPoint Firewall report pack. You can schedule the reports with the “CheckPoint Firewall weekly reporting” task.

Getting Started with CheckPoint Auditing

The predefined CheckPoint data source is configured for logs exported by CheckPoint in ASCII format. The data source works with two log formats created by the following methods:

- Manual export from the CheckPoint Firewall GUI
- CheckPoint's standalone export utility

To configure gathering of the CheckPoint log

1. Do one of the following:
    - Manually export the log to a location that is available to an InTrust agent or directly to the InTrust gathering engine.
    - Create a schedule for the CheckPoint export utility that exports the log to a location that is available to an InTrust agent or directly to the InTrust gathering engine. A sample script for Windows is provided further in this document. For UNIX computers, the script is similar as far as export options go, but with a different syntax.

1. In InTrust Manager, edit the CheckPoint 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***). You can supply the name of a special Windows share or a regular Windows or SMB share, depending on where CheckPoint stores or exports logs in your environment.
2. Make sure the "All CheckPoint firewalls" site includes the computer where the log is located.
   If you want to gather CheckPoint logs from an SMB share on a Unix host without an agent, make sure that this host is a member of an InTrust site in the Microsoft Windows Environment container. 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.
3. Schedule the "CheckPoint Firewall log daily collection" task. Make sure the gathering job within this task uses the "CheckPoint Firewall: All Events" gathering policy.
   For agentless gathering from an SMB share, the gathering job must be configured for the site described in the previous step. You also need to create a separate gathering policy under the **Gathering | Gathering Policies | Microsoft Windows Network** node and use it in the gathering job instead of "CheckPoint 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.
4. Schedule the "CheckPoint Firewall log weekly reporting" task. Configure the reporting job within this task to create the reports you need.

Sample Export Schedule Script

```
@echo off
REM Setting Variables
SET EXPORTDIR=c:\checkpoint_export
if exist %EXPORTDIR% goto 2
:1
echo.
echo - Error, [%EXPORTDIR%] does not exist, creating directory...
md %EXPORTDIR%
goto 2
:2
for /F "tokens=2-4 delims=/ " %%i in ('date /t') do (
set Month=%%i
set Day=%%j
set Year=%%k
)
REM Switching logs
echo.
echo - Switching log...
%FWDIR%\bin\fw logswitch cpfw1_%Year%%Month%%Day%.log
REM Removing previously exported logs
echo.
echo - Removing previously exported logs...
rem del %EXPORTDIR%\*.log
REM Exporting logs
echo.
echo - Exporting log...
echo.
fwm logexport -i %FWDIR%\log\cpfw1_%Year%%Month%%Day%.log -d "|" -n -o
%EXPORTDIR%\cpfw1_exported_%Year%%Month%%Day%.log
```

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 https://www.quest.com/company/contact-us.aspx or call +1-949-754-8000.

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