Welcome to InTrust Knowledge Pack for AIX

InTrust Knowledge Pack for AIX adds the capability of native (agent based) gathering from and real-time monitoring of the following audit trails on IBM AIX 5L 5.3 and V6 6.1 systems:

- Syslog messages
- Configuration file modifications
- Text logs of any format (gathering only)
- AIX audit log

CAUTION:

An agent running on an AIX machine catches only the local messages; it does not catch messages redirected from other computers over the network.

Resolved Issues and Enhancements

The following is a list of issues addressed and enhancements implemented in this release of the Knowledge Pack.

Table 1: Agents installation and uninstallation resolved issues

Resolved Issue	Issue ID
The Uninstall.sh script fails to remove some directories under the agent installation path that are not empty. You will have to manually remove those directories after uninstalling the agent from an AIX system with the Uninstall.sh script.	CR0182113
The adcscm_package.aix_ppc.sh script displays the following message during the agent installation: `./request: not found` This message does not affect the agent installation and is safe to ignore.	CR0182045

Known Issues

The following is a list of issues known to exist at the time of InTrust Knowledge Pack for AIX release.

Table 2: Upgrade known issues

Known Issue	Issue ID
Changes you might have made to predefined objects related to processing AIX machines (like job names and some other parameters) will be lost upon upgrade. It is recommended that you use copies of predefined objects (policies, jobs, etc.), rather than original objects themselves, to customize their parameters as you need.	CR0220429

Table 3: Real-time monitoring known issues

Known Issue	Issue ID

When InTrust monitors an AIX system with a real-time monitoring rule based on the "AIX Text Files Monitoring" data source and aimed at a set of text files, like the "Text file modified" predefined rule, and one of the text files specified for monitoring exceeds 2MB in size, the rule stops processing other files down the list. The confusing event is logged to the InTrust event log on the corresponding InTrust Server computer:
`Event ID: 8325 Type: Error Source: InTrust Monitoring Engine Operation: Internal Event Computer: host0123`
`Description: Data source 'AIX Text Files Monitoring' (ID = {8F031B9E-ECB6-4DDF-B63C-9582A629748F}) failed to collect events.`
`Error text: ADC Error: Function not implemented (ADCCanUnloadNow)`
Avoid monitoring text files that may exceed overgrow 2MB.
	CR0204065, CR0204074

When InTrust monitors an AIX system with the "Group created" and "User added to the group" real-time monitoring rules at the same time, and the group with users in it is created on that system, only the "Group created" rule generates an alert and the "User added to the group" rule does not. Likewise, when both the "Group removed" and "User removed from the group" real-time monitoring rules apply to an AIX system, and the group with users in it is removed from that system, only the "Group removed" rule generates an alert and the "User removed from the group" rule does not.	CR0203085

Upgrade and Compatibility

InTrust 11.3.1 Knowledge Pack for AIX supports upgrade from Knowledge Pack for AIX 5L for InTrust versions 10.4.1 and later.

CAUTION:

1. Make sure you have read a recommendation related to CR0220429 in the Known Issues sections of this document.
2. Agents installed on AIX computers must be manually upgraded for InTrust Knowledge Pack for AIX to work properly. You should manually uninstall an existing agent and then manually install the new AIX agent and register it on appropriate InTrust servers. You can find the updated agent in the ***<InTrust_Server_installation_path>*\Server\ADC\Agent\aix_ppc** folder after you install InTrust 11.3.1 Knowledge Pack for AIX.

System Requirements

Before installing InTrust Knowledge Pack for AIX, ensure your system meets the following minimum hardware and software requirements:

Server side

Table 4: Server side requirements

Requirement	Details
Platform	See system requirements for Quest InTrust Server 11.3.1
Memory	
Operating system	
Additional Software & Services	Quest InTrust Server 11.3.1

Agent side

Table 5: Agent side requirements

Requirement	Details
Platform/architecture	PowerPC_POWER5
Memory	Any of the following: • IBM AIX 5L 5.3 • IBM AIX V6.1 • IBM AIX V7.1
Operating system	• At least 260MB (280MB recommended) for agent files • Sufficient space for the event cache (default location is /var/InTrust)
Additional Software & Services	IBM C++ Runtime Environment Components for AIX version 8.0 and higher (available at http://www-01.ibm.com/support/docview.wss?uid=swg24015708)

Report pack

Table 6: Report pack requirements

Requirement	Details
Additional Software & Services	Microsoft SQL Server 2005—2012 SP1 Reporting Services

Getting Started

- Contents of Release Package
- Installation Instructions

Contents of Release Package

The InTrust Knowledge Pack for AIX release package contains the following components:

- Quest InTrust Knowledge Pack for AIX
- Quest InTrust for AIX Report Pack
- Product documentation, including the Preparing for Auditing and Monitoring IBM AIX document

Installation Instructions

Refer to Preparing for Auditing and Monitoring IBM AIX for instructions on the product installation.

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

© 2018 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

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.

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

InTrust Knowledge Pack for AIX Readme
Updated - September 2018
Version - 11.3.1