Quest®

Quest® InTrust 11.3.1

Preparing for Auditing Recovery Manager for Active Directory

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 Recovery Manager for Active Directory
Updated - September 2017
Version - 11.3.1

Contents

Recovery Manager for Active Directory Auditing Overview

The Recovery Manager for Active Directory Knowledge Pack expands the auditing and reporting capabilities of InTrust to Dell™ Recovery Manager for Active Directory. It lets you gather events about Recovery Manager for Active Directory sessions and make reports on these events. You can also analyze diagnostic information, which is gathered to the repository.

Requirements

The Knowledge Pack is compatible with SQL Server 2005 Reporting Services or later. It works with Recovery Manager for Active Directory 7.9 or later.

Setup

The Knowledge Pack is installed as part of the main InTrust installation.

InTrust Objects

InTrust setup includes the following InTrust objects related to Recovery Manager for Active Directory:

- “RMAD Events from Application Log” filter for the “Windows Application Log” data source
- “RMAD Events: RMAD host and agent events” gathering policy:
- “RMAD Events: RMAD host and agent events” import policy
- “RMAD events daily collection” task
- Sites:
    - RMAD site (Host)
    - RMAD site (DCs)

After installation, the policies are immediately ready for use. The task does not require additional configuration either, but you should consider working with a copy of the task so that the original task contains backup configuration.

Only the predefined sites need tweaking to make the workflow fit your environment, as follows:

1. Populate the “RMAD site (DCs)” site with the domain controllers in your environment.
2. Include the Recovery Manager for Active Directory host computers in the “RMAD site (Host)” site.

Report Pack

The Recovery Manager for Active Directory report pack includes only the “Backup Jobs History” report. After you have completed the InTrust installation wizard, the report appears in the new **InTrust | InTrust for Servers and Applications | Dell RMAD** report set in Knowledge Portal.

Collecting Recovery Manager for Active Directory Data

The “RMAD events daily collection” task includes a job that gathers all of the data that the Knowledge Pack is designed for.

The task’s schedule is disabled by default. To enable the schedule, open the task’s properties and select the **Schedule enabled** option. The default schedule specifies that collection takes place daily. If necessary, adjust the schedule and rename the task appropriately.

Instead of working with the predefined task directly, you can make a copy of it and use the copy. This way you will have a configuration reference in case you inadvertently make some undesirable changes to the task.

To log information about backup sessions in the Windows Application log

1. In the console tree, right-click the collection whose backup sessions you want to record to the Application log.
2. Click the **Log** tab, select the **Application Log** check box, and select **Everything** from the **What to record** list.

Analyzing Event Data

The predefined gathering jobs collect more events to the repository than to the audit database, because not all Recovery Manager for Active Directory events are needed for the “Backup Jobs History” report. The “RMAD Events: RMAD host and agent events” import policy is also configured to accept only those events that are needed for the report.

If you want to analyze Recovery Manager for Active Directory audit data that is not used in the report (for example, diagnostic data), you can use InTrust Repository Viewer, as follows:

1. Connect to the repository with the necessary data.
2. Configure the search parameters to filter events by source, and specify the following sources:
    - Recovery Manager for AD
    - Dell Backup Agent
3. Use the grouping and view filtering options in Repository Viewer as necessary.

For details about using Repository Viewer, see its online help.

Reporting

Using an InTrust Reporting Job

If you want to automatically create and store reports on schedule, add a final reporting job to the “RMAD events daily collection” task, or create a separate task with a different schedule specifically for reporting.

If you decide to create a separate task, match its schedule to the Recovery Manager for Active Directory backup session schedule.

For details about working with InTrust sites, tasks, and jobs, see the Auditing Guide.

Viewing the Report in Knowledge Portal

Knowledge Portal lets you work with reports interactively. This data view application enables you to:

- Organize the structure of the folders that reports are stored in
- Apply report properties to a number of reports at a time
- Customize reports view by modifying sort order within reports

To start working with the Knowledge Portal it is required to specify some of the security settings and data source properties.

Before you can view reports, configure the data source to connect to the product database. Data sources are databases that store the information used in the reports.

It is also required to configure access rights to provide the report users with access to reports they need. These rights are assigned through specifying appropriate SQL Reporting Services role to a user or group account.

After Knowledge Portal is properly configured, open the InTrust Manager and launch the task that includes a reporting job with the “Backup Jobs History” report. Then in Knowledge Portal click the **Reports** tab in the left tabbed pane and select the report. To view the report, select the **View Report** option in the right pane.

For detailed information see Leveraging Microsoft SQL Server Reporting Services Integration for Advanced Reporting.

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