Quest® InTrust 11.4.2

Preparing for Auditing and Monitoring Active Roles

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 and Monitoring Active Roles
Updated - September 2020
Version - 11.4.2

Contents

Active Roles Auditing and Monitoring Overview **5**
Compatibility 5

What You Can Do **6**
Tracking Administrative Activity Outside Active Roles 6
Managing Audit Data 7
Archiving Data 7
Reporting 7
Using InTrust Tasks 7
Complementing Audit Data 8
Monitoring Active Roles Policy Compliance 9
Tracking Active Roles Operation 10

Putting It to Work **11**
Installing the Knowledge Pack 11
Data Gathering and Reporting 11
Setting Up Gathering and Reporting with InTrust Manager 11
Jobs and Tasks 11
Reports 12
Example 13
Real-Time Monitoring of Business-Critical Events 14
Setting Up Monitoring with InTrust Manager 14
Viewing Alerts in InTrust Monitoring Console 14

Use Cases **16**
Checking Policy Compliance 16
Reporting on Account Management 17
Investigating Service Failure 17
Data Archiving and Analysis 18

Knowledge Pack Objects **19**
Site 19
Notification Group 19
Rules 19
Data Sources 19
Real-Time Monitoring Policy 20
Gathering Policies 20
Import Policy 20

Tasks 20
Repository Viewer Searches 20
Reports 21

Known Issues in Knowledge Pack 22

About us 23
Contacting Quest 23
Technical support resources 23

Active Roles Auditing and Monitoring Overview

The Knowledge Pack for Active Roles is a link between InTrust on the one hand and Active Roles on the other hand. The Knowledge Pack enables you to use the InTrust workflow to control the operation of Active Roles.

The Knowledge Pack is essentially a collection of InTrust objects such as rules, sites, policies, tasks and reports. These objects are interdependent, and they blend in with other predefined InTrust objects you may have installed.

After you have set up the Knowledge Pack, you can work with the following objects using InTrust:

- Rules
- Tasks
- Gathering policies
- Real-time policies
- Data providers
- Reports
- Sites

Using objects included in the Knowledge Pack, you can work with events that Active Roles records to its log. This log provides extended information about security events compared with the Security log.

Compatibility

The Knowledge Pack works with data provided by One Identity Active Roles 7.*.

What You Can Do

The Knowledge Pack adds significantly to the value of Active Roles. In an enterprise where both Active Roles and InTrust are deployed, each of these products plays a central part. Active Roles is designed to be the Active Directory administration center for the environment, whereas InTrust is the main facility for auditing and ensuring policy compliance. The Knowledge Pack brings these administrative functions closer together, making administration easier and more direct.

The related topics describe particular benefits that you get by deploying the Knowledge Pack:

- Tracking Administrative Activity Outside Active Roles
- Managing Audit Data
- Complementing Audit Data
- Monitoring Active Roles Policy Compliance
- Tracking Active Roles Operation

Tracking Administrative Activity Outside Active Roles

Active Roles is meant to be the control center for Active Directory administration. Accordingly, once you have deployed Active Roles, you should pay attention to any administrative activity that circumvents it. The Knowledge Pack enables you to find out whether any administrative actions are performed or attempted with other tools, such as the Active Directory Users and Computers MMC snap-in.

Administrative actions taken outside Active Roles may have different implications. This depends on whether the account that was used is one of the accounts reserved for the Active Roles service.

In a typical environment with Active Roles deployed, Active Directory-native permissions cannot be granted directly. Here, the term permissions includes membership in certain groups whose members have permissions on Active Directory objects. Only Active Roles accounts can delegate these permissions, but they are supposed to do it on behalf of Active Roles administrators by applying administrative templates (or roles) rather than dealing with individual permissions. One way of delegating Active Directory-native permissions on an individual basis is by using the Active Directory Users and Computers MMC snap-in.

In such cases, other accounts do not get direct access to Active Directory administration. If an account is not reserved for use with Active Roles, then administrative actions by that account fail. In such cases, you should investigate to find out who tried to get unauthorized access.

If the account is an Active Roles account, this may mean someone with access to the account performed the administrative action using a tool other than Active Roles. This can be done in an attempt to conceal the action or keep Active Roles from preventing it. Look into the matter to find out whether it is a case of impersonation or privilege abuse.

In some non-typical situations certain special-purpose administrative accounts retain the privileges to perform management outside Active Roles. Actions by these accounts should also be tracked to ensure that administrative measures do not violate the corporate policy.

Managing Audit Data

Archiving Data
Reporting
Using InTrust Tasks

Archiving Data

InTrust is a complete auditing and reporting solution.

The Knowledge Pack enables you to efficiently store and archive data related to Active Roles. By gathering the data to InTrust repositories, you store data in a compact and flexible way, while keeping it available for further use.

You achieve this by using InTrust gathering jobs (which you can set up in InTrust Manager) or real-time event collection (which you can set up in InTrust Deployment Manager). For information about creating and modifying jobs and tasks, see the Auditing Guide. For information about real-time collection, see Getting Started with InTrust.

In addition to long-term archiving, you can use InTrust repositories to consolidate Active Roles audit trails from multiple departments of your enterprise if your Active Roles administration is decentralized. In this way, you centralize both the archiving and the reporting. Consolidation jobs in InTrust serve this purpose.

When you use InTrust to manage Active Roles audit data, there is no restriction on the number of separate Active Roles-managed portions of the environment.

Reporting

To get reports on administrative activity performed with Active Roles and outside it, use InTrust tasks to gather the necessary data and schedule reports. The most common use for reports is to focus on the activity of particular users or track who makes particular changes to Active Directory.

Using InTrust Tasks

The Knowledge Pack comes with tasks that address both auditing and reporting needs. Use the tasks as follows:

- The “Active Roles: Daily events collection” task collects the ARAdminService log from Active Roles servers. It stores the gathered data in the default repository. This task archives data. One of the reasons for it is compliance with regulations.
- The “Active Roles: Weekly reporting” task depends on the previous tasks for data. It uses all data from Active Roles logs and some data—related to account management—from the Security log. The task imports data for reports from the repository and creates those reports.

You do not necessarily have to work with these predefined tasks. You may want to use them as templates for your own tasks: copy them and make the necessary adjustments to the copies.

Complementing Audit Data

Even though Active Roles logging is very detailed, there are situations when additional data helps. Change Auditor for Active Directory complements Active Roles audit with events from its own log to more completely and accurately reflect what happens in the environment. It is recommended that you deploy Change Auditor for Active Directory for comprehensive audit and additional benefits such as prevention of unwanted changes.

The following are examples of cases where Active Roles data is not enough:

- A user logs on to a domain controller to perform some administrative action. Active Roles does not capture this logon event.
- A user directly accesses and modifies an Active Directory object without using Active Roles administrative templates. Active Roles is not aware of the change.
- An administrator uses the Active Directory Users and Computers MMC snap-in to directly grant permissions to certain users. The set of permissions for the users contradicts roles defined by Active Roles, but Active Roles has no way of disallowing the changes and keeping the roles consistent.

These actions are not allowed in environments administered using Active Roles. For more information, see the Tracking Administrative Activity Outside Active Roles topic.

In your particular environment, other situations may come up when you also need data from Change Auditor for Active Directory logs on domain controllers for detailed analysis. InTrust gathering jobs provide an easy way to get that data, and reporting jobs incorporate it in reports.

InTrust can also collect and consolidate data from other sources such as the Security log, Application log, Directory Service log and Exchange tracking log. This gives you more capabilities for implementing audit procedures and ensuring regulation compliance.

Monitoring Active Roles Policy Compliance

Maintaining corporate administrative policies is one of the most important tasks in Active Roles. Active Roles prevents violation of policies it defines. If policies are violated outside Active Roles, it detects the violations. In either case, Active Roles makes detailed log records.

You must manually schedule policy compliance checking.

The Knowledge Pack ensures that you are notified of policy violations, whether attempted or successful. For example, you can monitor situations when there are multiple attempts to access certain resources. The most likely explanation is that some person or application keeps trying to gain access to the resource and failing at each attempt.

Normally, such situations are detected after the event and investigated by analyzing logs or reports. The Knowledge Pack provides monitoring rules that notify you of policy violations in real time.

Tracking Active Roles Operation

You can track Active Roles server health, availability and performance in real time. This is done with InTrust rules, which help detect and resolve issues in a timely fashion and keep Active Roles functional.

Rules, through alerts, mainly provide information about the following:

- Situations when the Active Roles service is unavailable
- How the service uses available system resources
- Whether the conditions in the environment are suitable for the service's successful operation

Putting It to Work

The Active Roles Knowledge Pack lets you perform the following operations:

- Gather Active Roles-related audit data
- Report on the gathered data
- Get notified of Active Roles issues in real time

The workflow for these tasks is no different from working with data for other InTrust Knowledge Packs. It includes working in InTrust Manager, InTrust Monitoring Console and, optionally, Quest Knowledge Portal.

The following three sections deal with installing and using these InTrust components for the tasks:

- Installing the Knowledge Pack
- Data Gathering and Reporting
- Real-Time Monitoring of Business-Critical Events

Installing the Knowledge Pack

To set up the Knowledge Pack, run the **ActiveRoles_KP.*.*.*.*.msi** installation package from your InTrust distribution.

Data Gathering and Reporting

To gather audit data and include it in SSRS reports, use the InTrust Manager MMC snap-in. Alternatively, you can use real-time event collection in InTrust Deployment Manager and analyze events using Repository Viewer.

The following two topics deal with how to use these components for the task:

Setting Up Gathering and Reporting with InTrust Manager

The combination of InTrust and the Knowledge Pack for Active Roles lets you easily gather audit data and create reports on it. The most convenient way to accomplish both of these objectives is to use a single InTrust task. You configure this task in the InTrust Manager MMC snap-in.

This section concentrates on what you do with InTrust Manager that involves objects from the Active Roles Knowledge Pack. For detailed instructions on how to do it, see the Auditing Guide.

Jobs and Tasks

InTrust tasks are chains of specialized operations called jobs. To gather Active Roles-related audit data and report on it, you need a task that includes at least a properly configured gathering job and a reporting job.

The necessary tasks are provided for you in the Knowledge Pack: “Active Roles: Daily events collection” and “Active Roles: Weekly reporting”. In general, there are tasks intended for gathering and those meant for reporting. The collection tasks gather audit data to the repository. The reporting tasks import the necessary data to the database, compile reports using that database, and then clean up the database.

The default configuration requires that you simply set an appropriate schedule for the tasks. However, if you want to split the reporting workflow into several tasks, you can make copies of the predefined reporting tasks and edit the parameters of the reporting jobs.

When configuring gathering jobs, you must supply the following information:

- Where to get the data
  This is determined by your choice of an InTrust site, which is a collection of audited computers. The Knowledge Pack comes with predefined sites you can use.
  You need to populate the required sites as necessary and make sure that agents are installed on site computers. Agents are installed as soon as site members are first enumerated, but you can force agent installation at any time by right-clicking the site and selecting **Install Agents**.
- What data to gather
  This is defined by InTrust gathering policies. On the one hand, policies let you narrow down the choice of audited computers. On the other hand, they provide filters for data that arrives in InTrust data storages. The predefined gathering policies that come with the Knowledge Pack are "Active Roles: All Administration Service log events", "Active Roles: Change Auditor for AD log events", and "Active Roles: Security log events".
  There are also import policies that specify which data is brought from repositories into audit databases for reporting.
  You can gather everything in the Active Roles logs for analysis and bring in data from the Change Auditor log and Security log for additional capabilities.
- Where to store the data
  InTrust supports two types of audit data storage: repositories and audit databases. Repositories are for long-term archival of arbitrary amounts of data, and audit databases should store data for immediate reporting needs. You can gather to a repository and then import data for reports to a database by including an InTrust import job in the task. This is the recommended way, and the predefined tasks are built around this model. You can also gather to a repository and a database at once if you want.

Reports

Reports help you find out about any event from the Active Roles Administration log in detail. In particular, you can report on the following:

- Assignment of user privileges
- Object management (including account management) in general

When configuring InTrust reporting jobs, you have access to reports shipped with the Knowledge Pack. In addition to the choice of reports, the following settings are important for reporting jobs:

- The URL of the reporting server's Web service
- The database to be used as the data source for the reports; the database you specify must exist and have the structure of an InTrust database
- Optionally, the credentials for creating the reports
- The reports and filters you need

- Where to deliver the ready reports—email address, network share or a Reporting Server snapshot that you can view using Knowledge Portal.
- Optionally, the repository from which to import data that is missing from the database.
- Optionally, settings for notification about job completion by email
- The InTrust server where the job runs

Example

The simplest way to organize reporting is as follows:

1. Adjust the schedule of the “Active Roles: Daily events collection” task or a copy of this task.
2. Adjust the schedule of the “Active Roles: Weekly reporting” task or a copy of this task so that the task runs after the necessary data has been gathered.
3. Configure the list of reports you want to get by editing the reporting job in the reporting task.

Real-Time Monitoring of Business-Critical Events

As described in this guide, real-time monitoring facilities provided by the Knowledge Pack focus on the health and functionality of the Active Roles service.

InTrust Manager and InTrust Monitoring Console are the two components that enable you to work with real-time monitoring objects.

InTrust sends out alerts as soon as certain events or conditions occur. Alerts are viewable in InTrust Monitoring Console. Notifications about alerts can be email or net send messages.

For more details, see the following topics:

- Setting Up Monitoring with InTrust Manager
- Viewing Alerts in InTrust Monitoring Console

Setting Up Monitoring with InTrust Manager

InTrust Manager lets you set up real-time monitoring. Real-time monitoring is governed by InTrust rules. To get a rule to work successfully, make sure of the following:

- Agents are installed on the computers to be monitored.
- The rule is enabled.
- All the parameters necessary for the rule are specified.
- The rule is bound to an InTrust site by a real-time monitoring policy.
- The policy is active.

To enable notifications

- Ensure that notification messages are defined for rules and activated.
- For real-time monitoring policies, check that notification of the right recipients is turned on.

For an example of the described configuration, see the Checking Policy Compliance topic. For other settings, such as configuring response actions and scheduling monitoring, refer to the InTrust documentation.

Viewing Alerts in InTrust Monitoring Console

Monitoring Console provides a centralized Web interface for real-time monitoring alerts. People responsible for resolution of certain types of alerts can have corresponding profiles to view only the reports they need.

Before you can use InTrust Monitoring Console to work with rules from the Knowledge Pack, complete the following preparatory steps:

1. In InTrust Manager, configure the rules you are going to use. Make sure that the rules are set to send out alerts.

2. Still in InTrust Manager, assign inspectors to the sites you want to monitor and the rule groups that include the rules you want to use. Inspectors are the personnel who will be viewing alerts. In a default configuration, inspectors must be assigned to the “Active Roles: Servers” site. The same people must be inspectors for the rule groups that contain the rules you need. By specifying inspectors, you ensure that these people can view the alerts that the rules generate.

After this, make some changes to Monitoring Console configuration by creating the following:

- An alerting profile
  It defines who can read alerts and change their state.
- An alert view
  It specifies what alerts you are interested in.

Creating an Alerting Profile

Open the Monitoring Console Administration page. For that, click the Monitoring Console entry in the Start menu, and when the page loads, append "/Administration" to the URL in the address bar.

On the Administration page, click **New** in the left pane to start the New Alerting Profile Wizard.

The wizard lets you select the InTrust Server that generates the alerts and specify who views these alerts. You let your personnel view alerts by assigning the roles of alert readers and alert managers. To allow a user to view alerts, assign the alert reader role to the user account; to allow a user to add comments and to acknowledge and resolve alerts, assign the alert manager role. Alert records are available to users (alert readers and alert managers) only if their accounts are inspectors for both monitored sites and rule groups.

After a new profile has been successfully configured, you can customize alert views for this profile in Monitoring Console. To open Monitoring Console, you can click its entry in the Start menu.

Creating an Alert View

Creating alert views doesn't involve the Administration page. To create a view, open the regular Monitoring Console page (click the Monitoring Console entry in the Start menu).

Click **New** to start the New Alert View Wizard. This wizard lets you select the rules and sites that you want to monitor, and saves your preferences as an alert view. For an existing view, you can configure filters based on alert state and generation time and other alert properties. Within a view, you can examine alert statistics and analyze the alerts in detail. For more information, refer to the Monitoring Console help.

You can create as many alert views as you need for organizing your alert resolution workflow.

Use Cases

This chapter describes several common use scenarios for the Knowledge Pack. The related topics describe general methods to achieve typical tasks and do not contain detailed instructions on procedures:

- Checking Policy Compliance
- Reporting on Account Management
- Investigating Service Failure
- Data Archiving and Analysis

For detailed instructions about working with InTrust configuration objects, refer to the Auditing Guide.

Checking Policy Compliance

This scenario is possible if the environment is configured so as to allow certain users to perform administrative actions outside Active Roles. Suppose you want to monitor changes to mailbox aliases in your environment that bypass Active Roles.

For example, suppose that there is a distinct policy for mailbox naming, and Active Roles imposes this policy. However, certain personnel can manage mailboxes without using Active Roles. You need to make sure that any mailbox management actions that these users perform comply with the policy and that no controversial changes are made inadvertently.

Configure the “Active Roles: Policy compliance check” rule to send email notifications to your Active Roles operators, as follows:

1. Make sure that the “Active Roles Operators” notification group is populated with accounts that must receive the notifications.
2. Open the properties of the “Active Roles: Policy compliance check” rule.
3. On the General tab, make sure that **Enabled** is selected.
4. On the Matching tab, select the check box next to the parameter in the list and specify the organizational units you want to monitor in the Containers parameter.
5. The list should contain few items. If the list is too large, rule matching takes a very long time.
6. Click **OK**.
7. Open the properties of the “Active Roles: Administration Service Policy” Policy.
8. Check that “Active Roles: Servers” is listed on the Sites tab, and the “Active Roles: Policy compliance check” rule (or the rule group that contains that rule) is listed on the Rules tab..
9. Select **Activate** on the **General** tab.
10. Click **OK**.
11. Commit the changes you have made by clicking the **Commit** button on the toolbar.

After that, you will receive notifications whenever a policy violation occurs for an object in the monitored OUs. Watch out for messages about mailbox alias changes.

Reporting on Account Management

In this scenario, you schedule a report on account management actions performed outside Active Roles. The information for the report comes from the Change Auditor for AD log and Security log on to the domain controllers of the domain you are interested in and from the ARAdminService log on the Active Roles servers in that domain.

To configure this workflow

1. Make sure the “Active Roles: Weekly reporting” task runs after all the required data has been gathered by the “Active Roles: Daily events collection”.
2. If necessary, edit the reporting job within the “Active Roles: Weekly reporting” task. For example, you can change filter settings for the “Account management performed outside Active Roles (Security Log)” report and specify the preferred output format for reports.
3. Optionally, add a notification job that informs you of task completion.

Now your report storage will contain a detailed report prepared automatically on schedule.

If you prefer to leave the default settings in the predefined task, make a copy of it and use the copy instead.

Investigating Service Failure

This scenario is common when the Active Roles service fails and you need to find out the reason. It is possible that the failure is due to a denial of service attack or abnormal activity going on. The symptom of such a situation is a large number of failure audit events in the environment.

You can monitor such situations by deploying the following rules:

- “Active Roles Service: General response”
- “Active Roles: Multiple failure audit”

Configure alerts from these two rules to be shown in InTrust Monitoring Console. When “Active Roles Service: General response” tells you that the service is not responding, check whether the alert is accompanied by the “Active Roles: Multiple failure audit” alert.

If both of these alerts are generated during a short period of time, investigate why the failure events occurred.

To implement this monitoring, prepare Monitoring Console for the task as described in the Viewing Alerts in InTrust Monitoring Console topic. When creating the alert view, include the two rules listed previously and the “Active Roles: Servers” site.

Remember that your alert viewers and managers must be inspectors for the group that holds the two rules and for the monitored site. Include the rules in the alert view you create.

If this situation is detected, you can further investigate the issue by preparing the “Active Roles all server events” SSRS report and analyzing it in InTrust Knowledge Portal. The report’s EventID filter lets you narrow down the scope of events to be included, and the Date Range filter refines the time period for the report.

For more information about using reports, see the Data Gathering and Reporting topic.

Alternatively, you can analyze events in Repository Viewer or IT Security Search. This means working with events stored in an InTrust repository instead of the audit database. For details, see the following:

- Searching for Events in Repository Viewer
- IT Security Search User Guide

Data Archiving and Analysis

This scenario represents the regular practice of gathering and archiving audit data, and then analyzing it. This is not a course of action for emergency situations.

InTrust provides you with long-term storage for Active Roles-related audit data. Keeping all the data in databases is impractical, so you use InTrust repositories for long-term storage.

You gather the audit data to InTrust repositories and import recent portions of it to audit databases to build reports. You are interested in data related to Active Directory object management.

To implement this scenario

1. Create a separate InTrust audit database for this purpose. You should not use your regular database in this case, because only one task should depend on it.
2. Create a new InTrust task and schedule it to run as often as you need it to.
3. In the new task, create a cleanup job than clears all data from the special audit database you have created. This job ensures that the database is emptied before any new data arrives in it.
4. Create a successor import job that imports data you are going to analyze. This job must import only Active Roles Administration log data.
5. Create a successor notification job to inform you of task completion.
6. When you get notified that the data has becomes available, see the “Active Roles all server events” report in Quest Knowledge Portal.

Using report filters, you can easily determine which events need attention and analyze them in depth.

Knowledge Pack Objects

Site

- Active Roles: Servers

Notification Group

- Active Roles Operators

Rules

- Administration Services
  - Active Roles Service: General response
  - Active Roles Service: Physical memory usage
  - Active Roles Service: Reserved virtual memory
  - Active Roles: License system failure
  - Active Roles: Administration Service internal error
  - Active Roles: Critical error on startup
  - Active Roles: Event with Error severity
  - Active Roles: Event with Warning severity
  - Active Roles: Multiple failure audit
  - Active Roles: Policy compliance check
  - Active Roles: Replication monitoring

Data Sources

- Active Roles Administration Log
- Active Roles Service: General Response - Script
- Active Roles Service: Physical memory usage - Script
- Active Roles Service: Reserved virtual memory - Script
- Active Roles: Change Auditor for AD log
- Active Roles: Policy compliance check - Script
- Active Roles: Replication monitoring - Script

Real-Time Monitoring Policy

- Active Roles: Administration Service Policy

Gathering Policies

- Active Roles: All Administration Service log events
- Active Roles: Change Auditorfor AD log events
- Active Roles: Security log events

Import Policy

- Active Roles: All Events

Tasks

- Active Roles: Daily events collection
- Active Roles: Weekly reporting

Repository Viewer Searches

- Active Roles
    - All events produced by Active Roles
    - All operations and operation requests
    - Operation requests for computers
    - Operation requests for groups
    - Operation requests for miscellaneous objects
    - Operation requests for users
    - Operations on computers
    - Operations on groups
    - Operations on miscellaneous objects
    - Operations on users

Reports

- Active Roles\Active Directory Management Bypassing Active Roles
  - Account management performed outside Active Roles (Security Log)
  - All activity within and outside of Active Roles
- Active Roles\Active Directory Management using Active Roles
  - Active Roles Deprovisioning of User Accounts
  - Active Roles Directory object management
  - Active Roles Directory object management summary by Initiator
  - Active Roles Group Management by Initiator
  - Active Roles Group Membership Management by Initiator
  - Active Roles User Accounts Management
  - Active Roles User attribute management
- Active Roles\Active Roles Events
  - Active Roles all Server events
  - Active Roles event statistics by Computer
  - Active Roles events by eventID
  - Active Roles startup failures

Known Issues in Knowledge Pack

The following is a list of issues known to exist at the time of the InTrust 11.4.2 Knowledge Pack for Active Roles release.

Known Issue	Issue ID
The **AR Server WI: Availability** real-time monitoring rule is matched if the Web Interface site uses any TCP port different from the default one (80), as if the Web Interface were not available.	B113361
The **AR Server WI: Availability** real-time monitoring rule does not work with Active Roles Server of versions prior to 6.0.3.	ST43222

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