Quest

Quest® InTrust 11.3.1

Preparing for Auditing and Monitoring Microsoft IIS

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 Microsoft IIS
Updated - November 2017
Version - 11.3.1

Contents

IIS Auditing Overview

InTrust with the Knowledge Pack for Microsoft IIS allows you to gather and monitor for events generated by Microsoft Internet Information Services (IIS). This information allows you to stay informed about who has been using the server and how many times your online information was accessed.

You can collect, report, and monitor for events generated by Microsoft IIS versions 7.0 and later. Gathering (but not monitoring) of events generated by Microsoft FTP Service is also supported.

IMPORTANT: For gathering and real-time monitoring to work on 64-bit Windows, IIS must be running in 32-bit mode.

InTrust can process the event data written by IIS to the following logs:

- Microsoft IIS WWW Log
- Microsoft IIS FTP Log
- Windows Security Log (events generated by IIS)

Installing the Knowledge Pack for Microsoft IIS

Support for IIS auditing and real-time monitoring is provided by the Knowledge Pack for Microsoft IIS. The Knowledge Pack must be installed on top of an existing InTrust installation.

Configuring Service Logging for IIS and FTP Service

1. In Internet Information Services Manager, in the left pane, click the necessary site or server.
2. In the right pane, click **Logging**.
3. On the screen that opens, set the Format option to **W3C**.
4. Configure other logging options as necessary.

Known Issues with IIS 7.0 and FTP Service 7.5

The following issues exist with gathering and real-time monitoring of IIS 7.0 and FTP Service 7.5 logs:

1. The "Oversized request" real-time monitoring rule does not work for these logs.
2. When gathering uses agent-side log backup, filtering by the **sc-bytes**, **cs-bytes** and **time-taken** fields does not work in the following audit data filters:
    - MS IIS: Web Site: Failed Access
    - MS IIS: Web Site: Restricted Access
    - MS IIS FTP Site Log
    - MS IIS: Web Site: Warning-code Access
    - MS IIS: FTP Site: Successful Logons
    - MS IIS: Web Site: Successful Access
    - MS IIS: FTP Site: Failed Logons
    - MS IIS: FTP Site: Upload
    - MS IIS: FTP Site: All Logons
    - MS IIS Web Site Log
    - MS IIS: Web Site: Not Found Errors
    - MS IIS: FTP Site: Download
3. If gathering uses agent-side log backup, the "Web site total statistics" and "WEB site daily traffic [chart]" reports cannot be generated from the resulting events.
4. Real-time monitoring and gathering of FTP logs with the agent-side audit log backup enabled does not work.
5. Gathering of WWW log in UTF-8 format does not work if **Do not create new log files** logging option is selected.

How to Gather Event Data with InTrust

1. In InTrust Manager, select **Configuration | Sites | Microsoft Windows Network**, and make sure the **All IIS Servers** site includes your IIS servers.
2. To automatically install agents on the site computers, select **Install Agents** from site's shortcut menu. Agentless gathering peculiarities are described later.
3. Select the **IIS Daily Collection** task, or configure a new task you need, with a gathering job involving the necessary gathering policy and site. In the task properties, select the **Schedule enabled** option.
4. Select the **IIS Weekly Reporting** task, or configure a new reporting task you need, and enable its schedule in the similar way.

CAUTION: If you change the location of IIS log files between gathering sessions, make sure the old log files are available in the new location.

Gathering Data Using Agents

To minimize impact on the network when communicating data from target computer to InTrust server, agents are recommended for data gathering.

The following rights and permissions must be assigned to the InTrust agent account if the agent is not running under the **LocalSystem** account:

- Read permission to the **HKLM\SYSTEM\CurrentControlSet\Control\ TimeZoneInformation** registry key.
- **Read** and **List Folder Contents** permissions to log file folders; the **Delete** permission must also be granted if the agent-side log backup is enabled and the **Clear the backup after gathering** option is turned on for the data source.

Gathering Data Without Agents

To gather IIS events without agents:

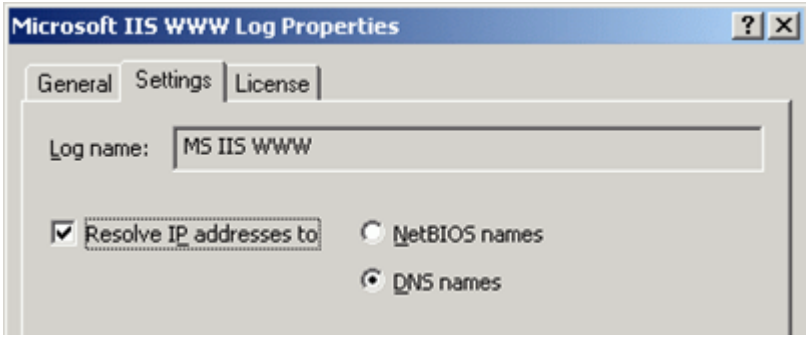
- Microsoft IIS Administrative Components must be installed on the InTrust server.
- On the processed computer, the Remote Registry Service is required.

- The account that will be used for access to the site computers during gathering (specified explicitly in the site's settings, or inherited from InTrust server or task) requires the following:
    a. **Access this computer from the network** right.
    b. **Deny access to this computer from network** right must be disabled.
    c. Membership in the local **Administrators** group.
    d. Read permission to the **HKLM\SYSTEM\CurrentControlSet\Control\ TimeZoneInformation** registry key.
    e. Read permission to the **HKLM\SYSTEM\CurrentControlSet\Control\ Nls\Language** registry key.
    f. **Read** and **List Folder Contents** permissions on log file folders; the **Delete** permission must also be granted if the agent-side log backup is enabled and the **Clear the backup after gathering** option is turned on for the data source.

IP Address Resolution

If specified by InTrust settings, IP addresses found in the log are resolved to host names, and InTrust saves them both (IP addresses and host names) into the log, appending them to original fields. This can significantly slow down the gathering process; so this option is disabled by default. If necessary, you can enable this option in the following way:

1. In InTrust Manager, select **Configuration | Data Sources**.
2. On the right pane, select the IIS log you need, for example, Microsoft IIS WWW Log
3. From its shortcut menu, select **Properties**, on the **Settings** tab select **Resolve IP addresses to** and specify whether to resolve them into NetBIOS names or DNS names:



How to Monitor for Critical Events

To monitor for critical events, InTrust agents are used on the computers included in the target site. If the agents are not yet installed, they will be deployed automatically as soon as you activate a real-time monitoring policy.

To simplify the configuration of the real-time monitoring workflow, InTrust Knowledge Pack for Microsoft IIS offers predefined monitoring rules and policies.

IMPORTANT: For real-time monitoring to work on 64-bit Windows, IIS must be running in 32-bit mode.

To configure IIS monitoring with InTrust

1. In InTrust Manager, carry out the following:
    a. Enable the rule that will handle the events you need, for example, 'Unauthorized web-page access attempt', or any other rule from **Real-Time Monitoring | Rules | IIS RTM Rules | Common Attacks**.
    b. Activate a monitoring policy that will bind this rule to your InTrust site, that is the **Real-Time Monitoring | Policies | IIS Security** policy.
    c. If you want to get an email notification upon alert generation, in the **Configuration | Personnel**, select **Notification Groups**, select the necessary group and specify the desired recipients.
    d. Select the site you will monitor (All IIS Servers), and from its shortcut menu, select **Properties**. Click **Security**, and make sure the list of accounts includes users you want to be able to work with the alerts (as alert readers or alert managers). Check the same for the rule group containing the rule you are using.
2. In Monitoring Console, do the following:
    a. Open the profile you want to work with, or create a profile by running Monitoring Console Administration from the Start menu.
    b. Configure an alert view to display the necessary alerts.

For detailed information on configuring gathering and monitoring processes, refer to the InTrust Auditing Guide and InTrust Real-Time Monitoring Guide.

InTrust Knowledge Pack for Microsoft IIS

The Knowledge Pack for Microsoft IIS offers a set of predefined InTrust objects that will help you configure the gathering and monitoring of event data from your IIS servers. The following objects are included:

- Gathering policies:
  - IIS: Security
    Collects all IIS security events to both a repository and a database.
  - IIS: Health
    Collects all IIS health events both to a repository and a database.
  - IIS: Usage: WWW
    Collects IIS Web Site log both to a repository and a database.
  - IIS: Usage: FTP
    Collects IIS FTP Site log both to a repository and a database.
- Import policies:
  - IIS: Security
    Imports all IIS security events to a database.
  - IIS: Health
    Imports all IIS health events to a database.
  - IIS: Usage: WWW
    Imports events from IIS Web Site log to a database.
  - IIS: Usage: FTP
    Imports events from IIS FTP Site log to a database.
- Jobs:
  - IIS Security events collection
    Collection of all the IIS security events to the default repository and the default database.
  - IIS Web Site Reporting
    Weekly reporting of IIS Web Site usage and security events.
  - IIS FTP Reporting
    Weekly reporting of IIS FTP Site usage and security events.
- Tasks:
  - IIS Daily collection
    Daily collection of all the IIS events to the default repository and the default database.
  - IIS Weekly Reporting
    Weekly reporting of IIS statistics and the most critical events.
- “All IIS servers” site
- “IIS Security” real-time monitoring policy
  Applies real-time monitoring rules related to IIS security.

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