

Alliance LogAgent for IBM i

Solution Brief



Compliance Logging for the IBM i Platform

Regulatory compliance involves monitoring all of your Enterprise server logs in real time for security attacks and breaches. Alliance LogAgent for IBM i provides the real-time security event notification you need for your IBM i server. With Alliance LogAgent for IBM i you can implement a common Security Information and Event Management strategy for all of your Enterprise servers. An added benefit is the ability to control the size of audit logs and reclaim expensive disk storage space.

High Speed Event Management

Poor performance can consume CPU resources and slow event management, defeating your security strategy. On an entry level IBM i platform, Alliance LogAgent processed over 800 events per second with minimal impact on CPU.



Meet Compliance Regulations

Collect security system logs and transmit to a log collection server

Formats QAUDJRN Security Journal

Format to syslog (RFC3164) or Common Event Format (CEF)

Communicates Securely

Communicates with log collection servers and Security Information & Event (SIEM) solutions

High Performance

Event management protects CPU resources with high event processing speeds

Affordable Solution

Protects your investment in IBM i hardware and software

www.townsendsecurity.com

Introduction

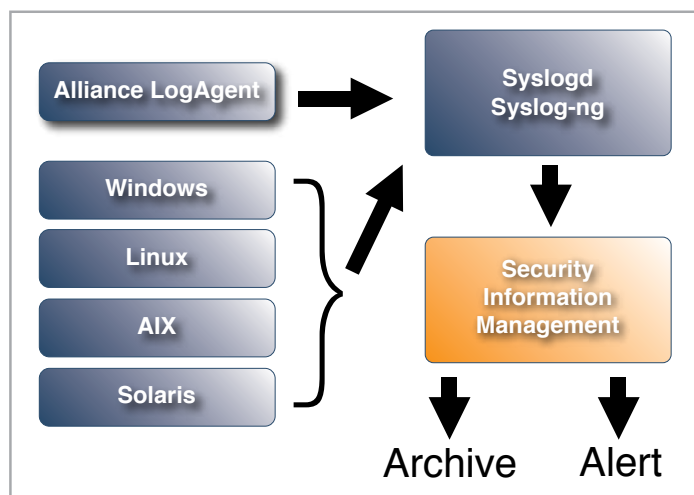
Alliance LogAgent for IBM i helps Enterprise customers bring their IBM I platforms into compliance with PCI, Sarbanes-Oxley (SOX), HIPAA and other regulations requiring active security monitoring of their servers. Alliance LogAgent automatically collects system security events, formats them into an open systems log format, and securely transmits them to a log server for consolidation with the security events from other servers.

Logs can be collected from the IBM i security journal QAUDJRN, system operator message queue, and system history file QHST. Log entries are converted from the internal IBM format to either syslog format (RFC 3164) or Common Event Format (CEF). Converted entries are then transmitted to a central log server or SIEM product for log collection, analysis, and alert management.

Alliance LogAgent for IBM i provides high performance event handling. On an entry level IBM i platform the application can process more than 800 log entries per second. This means that you can process the large number of events that are generated when IBM i security levels are at the highest settings.

System Logging and Compliance

Data security regulations require monitoring of corporate servers for potential security breaches. A typical server can contain thousands of potential security events collected daily in system logs. Additionally, a company may have servers in multiple locations. In order to manage these logs



and meet the requirement to monitor for security breaches, a company needs to consolidate logs from many servers into a single database and use sophisticated software to detect and report potential breaches.

In the past the **IBM i (AS/400 or iSeries)** customer did not have a way to bring security and application logs into a coherent strategy for log management and analysis. IBM I security events are stored in a proprietary format in a system journal that is not compatible with other server log formats. And security events created by user and vendor applications may not even write to the security journal. Making the management of logs more difficult, many new open systems applications such as the **Apache web server**, the **OpenSSH** secure shell application, the **MySQL database**, **PHP**, and other applications create system and security logs in the IFS directory in UNIX or Linux format.

The Alliance LogAgent for IBM i solution collects all of these events, converts them to a common, open standard for system logs, and transmits them to a central server using standard communications protocols. The Enterprise customer can now bring the IBM i platform into a common strategy for log consolidation and analysis to meet regulatory compliance requirements.

Log Format Standards

The open standard for system logs is defined by **RFC 3164**. This standard defines all of the information that should be included in a system log entry including the date and time stamp, the originating system, the application generating the log, and the text description of the security or system event. Applications that conform to this open standard for log entries work well with log monitoring and alerting software. The Alliance LogAgent solution formats all log information from the security journal, system operator message queue, and user applications into this standard format. This provides a view of the IBM i security environment that is compatible with open standards and third party software.

Security Information & Event Management (SIEM) Solutions

A number of software vendors have created solutions that provide proactive monitoring of system logs and send alerts when potential security breaches occur. Solutions like ArcSight ESM, Symantec SIM, LogLogic LX, Novell Sentinel, Q1Labs QRadar, TriGeo SIM, and CrossTec Activeworx can receive events from Alliance LogAgent and analyze system logs in real time to identify security threats. The Enterprise customer can use these solutions to manage the high volume of system log information generated from multiple servers. Because the IBM i security events are merged with security events from all other servers, these SIEM applications can identify suspicious patterns of activity. This results in a complete picture of your server network and better security management.



security audit journal receivers you retain on your system and decrease the amount of storage used. This provides a direct cost savings by reducing expensive IBM i storage.

Obj	Object	Type	Attribute	Size	Text
-	ADDRCU0024	*JHRRCU		12345344	
-	ADDRCU0025	*JHRRCU		8388608	
-	ADDRCU0026	*JHRRCU		3665928	
-	ADDRCU0027	*JHRRCU		11296768	
-	ADDRCU0028	*JHRRCU		11296768	
-	ADDRCU0029	*JHRRCU		12345344	
-	ADDRCU0030	*JHRRCU		9465856	

Because you are storing log events on a central server you also satisfy compliance requirements for saving log history.

IBM i Security Audit Journal

IBM i security administrators can enable the collection of a wide variety of security events by changing system settings. Once enabled, the security events are collected in the security journal QAUDJRN and include invalid user name and password attempts, denial of access to database files and programs, and user generated entries. These events have a proprietary format typical of IBM i journal entries.



Alliance LogAgent runs in the background to extract QAUDJRN security journal entries in real time. The journal entries are converted from internal IBM i format to Syslog format based on RFC 3164. Once converted to Syslog format the journal entries can be sent to a log consolidation system for analysis. In order to minimize the impact on network resources Alliance provides the ability to filter the security events to include only the types of events you want to monitor.

Managing Audit Journal Storage

The IBM i security log journal receivers can occupy many gigabytes of disk space when allowed to accumulate over time. By sending the log journal entries to a central management server you can decrease the number of

IBM i Operator Messages

Another source of system security event messages is the system operator's message queue QSYSOPR. Many user and ISV software solutions report security errors to the system operator. These messages can provide important



information about potential security breaches. Alliance LogAgent can read the messages from the QSYSOPR message queue in real time and format the messages to the standard Syslog format. Once formatted Alliance can send the messages to a consolidation server for analysis.

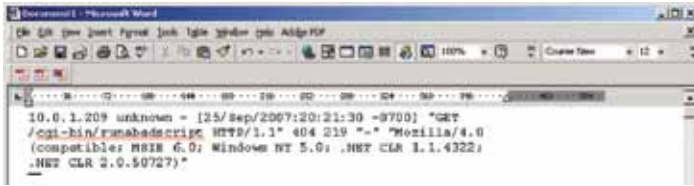
IBM i User Application Logging

To facilitate the generation of log events Alliance LogAgent provides program interfaces for generating events. A command interface provides the ability to create a log entry in the standard Syslog event format. You can also use a bindable service program in your ILE applications to generate log events directly from user applications. These log events give you the ability to create log events with the severity and descriptions that you want. Any user or ISV application can use these program interfaces to create system log entries.

IBM Apache, OpenSSH, MySQL, and PGP Application Logs

As IBM brings more open systems applications to the IBM i there are more potential security problems to manage. For example, the default web server on the IBM i is the Apache server, an open systems web server from the Apache Software Foundation. Recently IBM brought the open source MySQL database and the web application language

PHP to the IBM i. All of these applications present security challenges for the IBM i user.



These open source applications can be enabled to write security events to standard system log files in the IFS file system. However, these applications do not directly integrate with the native IBM I security journal. When important security event information is logged to these system logs it can be easily overlooked. Alliance LogAgent, combined with the Syslog-ng application for the IBM i, can provide the log monitoring that you need for security management.

Alliance LogAgent Log Formats

Alliance LogAgent supports the open standard for system log events defined by RFC 3164. This format provides a standard representation of system log events and makes it easier to analyze logs generated on a variety of systems. In addition to the open standard for system logs, Alliance supports the ArcSight Common Event Format (CEF). Customers using the ArcSight ESM product can receive system log events in CEF format for analysis in the native ArcSight format.

Alliance Communications with Syslogd

The Syslogd application is the most common system log server on Linux and UNIX systems. For companies using a Syslogd server to consolidate log information, Alliance LogAgent provides a TCP UDP communications interface to automatically send log events to Syslogd. The communications client can be automatically started when the IBM i is started to provide real time reporting.

Alliance Communications with Syslog-ng

Syslog-ng is the next generation of system log communications. As a replacement for Syslogd the application provides better communications, more robust support for logging formats, and automatic conversion of logs to the standard RFC 3164 format. Syslog-ng also

provides advanced filtering options to better manage which log entries are sent to a remote server. Syslog-ng is available in an open source edition and in a commercial version known as Syslog-ng Premium Edition. The Premier Edition of Syslog-ng provides secure SSL/TLS communications of log events, disk buffering, and other features for the Enterprise customer. Townsend Security provides sales and support for Syslog-ng.

Alliance Integration with AES Encryption

Alliance AES encryption products on the IBM i platform provide a number of user and application authentication methods to insure the appropriate access to sensitive data. When security policies result in a denial of access to an end user or application, log events are created in the IBM security audit journal. Users of the Alliance AES encryption and Alliance LogAgent solutions for the IBM i will have immediate notification of these types of security events.

Alliance Integration with FTP & XML Web Services

Alliance solutions that secure data in motion such as Alliance FTP Manager, Alliance XML, and Alliance AS2 Integrator have been enhanced to write security events to the IBM security journal to support event notification through Alliance LogAgent. When combined with Alliance AES encryption to secure data at rest the Enterprise customer can deploy a complete solution for security event management for data at rest and for data in motion.

Product Information

Alliance LogAgent for IBM i is licensed on a per partition basis with discounts for multiple licenses. A fully functional free trial is available for evaluation. You can also request a free consultation and additional product information.

Townsend Security

Townsend Security provides data encryption & tokenization, key management, secure communications, and compliance logging solutions to Enterprise customers on a variety of server platforms including IBM i, IBM z, Windows, Linux, and UNIX. The company can be reached on the web at www.townsendsecurity.com, or (800) 357-1019.