This presentation will explain the security auditing capabilities added in WebSphere Application Server version 7.

Agenda

- Security auditing feature
- Generating reports

This presentation will begin by explaining a new feature that allows security data to be collected based on configured filters. The presentation will then explain how to use the stored data to generate audit reports for this security data.

Section

Security auditing

This next section explains the new security auditing feature in WebSphere Application Server V7.

Security auditing overview

- Designed to provide audit records that can be used to ensure the integrity of a secured computing environment
- Captures authentication, authorization, system management, and other security events into logged audit event records
  - Provide audit trail that can be used for accountability
  - Used for vulnerability analysis
  - Provide a mechanism which can be used to prove compliance with regulatory laws

Security auditing is designed to create and provide auditing records that can be used to ensure the integrity of a secured environment. Auditing can be configured to capture data on authentication, authorization and other security events. This data is then stored in audit even records which provide an audit trail which can be used for vulnerability analysis, to identify accountability for key events and to provide a mechanism to comply with certain regulatory laws.

Secure auditing feature

- WebSphere Application Server security auditing feature provides the option to generate reports based on different events
  - Authentication, authorization, resource access, and others
  - Filters can be used to capture a subset of events tailored to the audited environment
- Overhead of audit event collection should be minimal

WebSphere Application Server security auditing has filters that can used to used to tailor the data collected for auditing purposes. Filters can be used to gather data on authentication, authorization, resource access or other types of security events that you want to be tracked. There is some overhead associated with enabling auditing, but work has been done to keep the overhead minimal. It is best to test the overhead in your specific environment based on the filters selected.

Secure auditing feature (continued)

- Two plug-in points are available
  - Audit Event Factory which captures the audit data
  - Audit Service Provider which takes the captured data and outputs it to a backend repository
  - Default plug-in implementations are shipped and output the audit records to a binary audit log
- WebSphere Application Server security auditing feature provides plug-in points for third party solutions
- Provider implementation plug-in support for writing audit records to SMF on the z/OS® platform

There are two plug-in points provided with the auditing feature. The audit event factory captures the auditing data, and the audit service provider takes captured data and outputs it to some backend repository. Default implementations are shipped with WebSphere Application Server version 7 and can be used for auditing purposes, or solutions from other vendors that work with this implementation can be investigated.

Audit data

- The audit data collected can be protected against tampering
  - Mechanisms to encrypt and sign the data are available
- Encryption is managed by the auditor
  - The certificate used to encrypt the data records is managed within the audit subsystem, in audit.xml
- Signing is managed by WebSphere Application Server
  - The certificate used to sign the data records is managed with WebSphere Application Server, in security.xml

The audit data collected by the secured auditing feature can be protected from tampering using mechanisms to encrypt and sign the data. Encryption of the data is managed by the auditor, with the security certificate used managed by the audit subsystem and configured in audit.xml. Signing of the data is managed by WebSphere Application Server, which stores information about the certificate used in security.xml.

Section

Generating reports

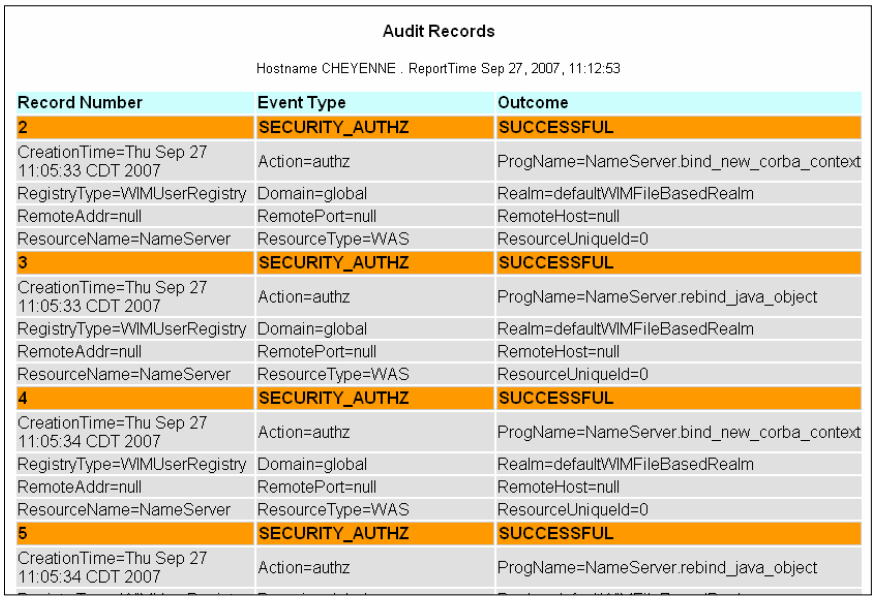
This next section explains how to generate reports for the security auditing feature in WebSphere Application Server V7.

Audit reader

- An audit reader is provided to read a generated IBM binary audit log
  - Can generate an HTML report from the audit data
  - Capability to read from an unencrypted and unsigned, encrypted and unsigned, unencrypted and signed, and encrypted and signed logs is supported
  - Invoked as an AdminTask
- $AdminTask binaryAuditLogReader {-fileName <String> -reportMode <String> -eventFilter <String> -outcomeFilter <String> -sequenceFilter <String> -timeStampFilter <String> -keyStorePassword <String> -outputLocation <String> -dataPoints <String>}

A command line tool is provided to generate reports from the audit data that has been collected. This tool can generate an HTML based report from the auditing data. It has the ability to read signed and encrypted data as well. An example of the admintask used to invoke the audit reader is shown here, to learn more about the command invoke it with the –help option.

Audit reader report



Audit Records

Hostname CHEYENNE . ReportTime Sep 27, 2007, 11:12:53

Record Number	Event Type	Outcome
2	SECURITY_AUTHZ	SUCCESSFUL
CreationTime=Thu Sep 27 11:05:33 CDT 2007	Action=authz	ProgName=NameServer.bind_new_corba_context
RegistryType=WIMUserRegistry	Domain=global	Realm=defaultWIMFileBasedRealm
RemoteAddr=null	RemotePort=null	RemoteHost=null
ResourceName=NameServer	ResourceType=WAS	ResourceUniqueId=0
3	SECURITY_AUTHZ	SUCCESSFUL
CreationTime=Thu Sep 27 11:05:33 CDT 2007	Action=authz	ProgName=NameServer.rebind_java_object
RegistryType=WIMUserRegistry	Domain=global	Realm=defaultWIMFileBasedRealm
RemoteAddr=null	RemotePort=null	RemoteHost=null
ResourceName=NameServer	ResourceType=WAS	ResourceUniqueId=0
4	SECURITY_AUTHZ	SUCCESSFUL
CreationTime=Thu Sep 27 11:05:34 CDT 2007	Action=authz	ProgName=NameServer.bind_new_corba_context
RegistryType=WIMUserRegistry	Domain=global	Realm=defaultWIMFileBasedRealm
RemoteAddr=null	RemotePort=null	RemoteHost=null
ResourceName=NameServer	ResourceType=WAS	ResourceUniqueId=0
5	SECURITY_AUTHZ	SUCCESSFUL
CreationTime=Thu Sep 27 11:05:34 CDT 2007	Action=authz	ProgName=NameServer.rebind_java_object

This is an example of a report generated by the audit reader command line tool. Events are broken out and information is displayed about each type of event.

Auditor role

- A new auditor role has been added to allow the auditing security role to be separated from the administrative security role
  - During installation the administrator is included in the auditor role
  - Not supported in fine-grained administration
- Enable/disable auditing, configure the auditing feature, define the security events to be captured
- The auditor role is used to grant additional users the same role

A new security role is also introduced with the security audit feature. This is done so that the auditing security role can be separate from the administrative security role in an environment. At installation time the default administrative user is granted the auditor role; this can then be changed to setup a separate user with the auditor role, which has the ability to grant the auditor security role to other users and to manage the auditing configuration. The auditor role is not yet supported in the fine-grained security administration feature.

Section

Summary

Following is the summary for the presentation.

Summary

- Security auditing feature allows you to capture and maintain audit controls over your environments

WebSphere Application Server has introduced several new features for security. Security auditing allows you to gather security information about your environment and generate reports based on that information. These reports provide a mechanism which can be used to examine security events that have occurred in the environment.

Feedback

Your feedback is valuable

You can help improve the quality of IBM Education Assistant content to better meet your needs by providing feedback.

- Did you find this module useful?
- Did it help you solve a problem or answer a question?
- Do you have suggestions for improvements?

Click to send e-mail feedback:

mailto:iea@us.ibm.com?subject=Feedback_about_WASv7_SecurityAuditingOverview.ppt

This module is also available in PDF format at: ../WASv7_SecurityAuditingOverview.pdf

You can help improve the quality of IBM Education Assistant content by providing feedback.

Trademarks, copyrights, and disclaimers

The following terms are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both:

IBM WebSphere z/OS

A current list of other IBM trademarks is available on the Web at http://www.ibm.com/legal/copytrade.shtml

Product data has been reviewed for accuracy as of the date of initial publication. Product data is subject to change without notice. This document could include technical inaccuracies or typographical errors. IBM may make improvements or changes in the products or programs described herein at any time without notice. Any statements regarding IBM's future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only. References in this document to IBM products, programs, or services does not imply that IBM intends to make such products, programs or services available in all countries in which IBM operates or does business. Any reference to an IBM Program Product in this document is not intended to state or imply that only that program product may be used. Any functionally equivalent program, that does not infringe IBM's intellectual property rights, may be used instead.

Information is provided "AS IS" without warranty of any kind. THE INFORMATION PROVIDED IN THIS DOCUMENT IS DISTRIBUTED "AS IS" WITHOUT ANY WARRANTY, EITHER EXPRESS OR IMPLIED. IBM EXPRESSLY DISCLAIMS ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NONINFRINGEMENT. IBM shall have no responsibility to update this information. IBM products are warranted, if at all, according to the terms and conditions of the agreements (for example, IBM Customer Agreement, Statement of Limited Warranty, International Program License Agreement, etc.) under which they are provided. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products in connection with this publication and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products.

IBM makes no representations or warranties, express or implied, regarding non-IBM products and services.

The provision of the information contained herein is not intended to, and does not, grant any right or license under any IBM patents or copyrights. Inquiries regarding patent or copyright licenses should be made, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

Performance is based on measurements and projections using standard IBM benchmarks in a controlled environment. All customer examples described are presented as illustrations of how those customers have used IBM products and the results they may have achieved. The actual throughput or performance that any user will experience will vary depending upon considerations such as the amount of multiprogramming in the user's job stream, the I/O configuration, the storage configuration, and the workload processed. Therefore, no assurance can be given that an individual user will achieve throughput or performance improvements equivalent to the ratios stated here.

Note to U.S. Government Users - Documentation related to restricted rights-Use, duplication or disclosure is subject to restrictions set forth in GSA ADP Schedule Contract and IBM Corp.