#### $\mathsf{IBM}^{\circledast}\mathsf{WebSphere}^{\circledast}\mathsf{Application}$ Server V7– LAB EXERCISE

# WebSphere Application Server security auditing

Vhat this exercise is about	
ab requirements	
Vhat you should be able to do2	)
ntroduction2	)
Exercise instructions	\$
Part 1: Create an audit User ID	ŀ
Part 2: Configure and enable security auditing	\$
Part 3: View the audit logs	) -
Part 4: (Optional) Create a new event filter17	,
Part 5: (Optional) Digitally sign the audit log entries	\$
Part 6: (Optional) Encrypt the audit logs	,
Part 7: (Optional) Verbose logging and reporting	
Vhat you did in this exercise	;

### What this exercise is about

The objective of this lab is to introduce some of the new security auditing features in WebSphere Application Server Network Deployment V7 edition on distributed platforms. This exercise is split into two main sections. The first half goes through the process of enabling security auditing, setting basic audit configurations, and viewing the audit reports. The second half, which is optional, goes through some slightly more advanced features of the auditing functionality, including encrypting and digitally signing the audit logs.

### Lab requirements

The list of system and software required for the student to complete the lab.

- A system that meets that requirements for running WebSphere Application Server Version 7, with approximately 500 MB of disk space for creating profiles
- The most current version of WebSphere Application Server V7
- An application server profiles with administrative security enabled, and with the administrative console and the default application deployed.

### What you should be able to do

At the end of this lab you should be able to:

- Enable security auditing
- Configure security auditing for different administrative users
- Generate and view security audit report
- Configure new event filters
- Configure digital signing for the audit logs
- Configure encryption settings for security auditing

#### Introduction

WebSphere Application Server Version 7 builds on improvements made in Version 6.1. A few of the major enhancements introduced in this release are the capabilities to:

#### Part 1: Create an audit User ID

Since it may be desirable to distinguish those console users that have administrative access from those that have auditing console, a separate administrator user is created and mapped to the Audit role. This user is then used to configure and enable auditing features.

#### Part 2: Configure and enable WebSphere security auditing

This portion of the exercise configures and enables the auditing service. Before actually enabling the auditing, you need to configure how notifications will take place. For this exercise, you configure auditing to report the events to a log file.

#### Part 3: View the audit logs

After enabling the auditing, you verify that events are being reported to the log file. You also generate an html report, which is more readable that the text based log files.

#### Part 4: (Optional) Create a new event filter

Security auditing reports only four types of events by default, but there are many additional events which can be configured as well. This section adds an additional event filter, and maps it to the configurations for the service provider and event factory.

#### Part 5: (Optional) Digitally sign the audit log entries

In order to ensure the integrity of the log entries, digital signing can be configured. Once signing is enabled, the log entries are also 64-bit encoded. This portion of the exercise enables digital signing for the audit logs.

#### Part 6: (Optional) Encrypt the audit logs

This part adds encryption on top of the digital signing. This requires the addition of a new keystore and certificate which will be specific to encrypting the audit logs. Once that keystore exists, the encryption is enabled and verified.

#### Part 7: (Optional) Verbose logging and reporting

The final section of the lab enables verbose audit logging. This provides some additional information in the log entries that were not available previously. You also produce a new "complete" html audit report.

### **Exercise instructions**

Instructions and subsequent documentation use symbolic references to directories which are listed as follows:

Reference Variable		
<was_home></was_home>	C:\Program Files\IBM\WebSphere\AppServer	Linux /opt/WebSphere/AppServer
		AIX /usr/WebSphere/AppServer
<temp></temp>	C:\temp	/tmp
<hostname></hostname>	Host name or host address for the machine where the profiles are being created	Host name or host address for the machine where the profiles are being created

### Part 1: Create an audit User ID

WebSphere Application Server has the ability to grant administrative users different roles to distinguish between the sorts of access they have within a cell or application server. With WebSphere Application Server version 7, a new role of Auditor has been added and is required to configure and enable any of the auditing features. By having a separate role for auditing, it is possible to distinguish between administrative users and those users you want to grant access to auditing functions.

This part of the lab creates a new administrative user called wsaudit and maps them to the auditor role.

- 1. Start by ensuring that the application server is running.
- \_\_\_\_2. Open an administrative console and verify that administrative security is enabled.

🥹 Integrated Solutions Console - Mozilla Fir	efox	
Eile Edit View Go Bookmarks Iools	Help	¢
🗇 • 🖒 • 🥰 🛞 🚷 🗋 http	os://was7host01:9043/ibm/console/secure/securelogon.do	<u>a</u> ⊙ ∞ <u>C</u>
Integrated Solutions Console Welcome wsden	10 Help   Logou	· IBM.
View: All tasks	Cell=was7host01Node02Cell, Profile=Audit Global security	Close page
Welcome     Guided Activities		
	Global security	
	Use this panel to configure administration and the default application security functions and is used as a default security policy for user applications. Securit	y policy. This security configuration applies to ty domains can be defined to override and c
Applications	applications.	
Gervices		
	Security Configuration Wizard Security Configuration Report	
Security Security Security Security domains Administrative Authorization Groups SSL certificate and key management Security auditing Bus security	Administrative security  Enable administrative security  Administrative user roles  Administrative group roles  Administrative authentication  Application security	Authentication Authentication mechanisms and expirat C LTPA C Kerberos and LTPA Kerberos configuration C SWAM (deprecated): No authentica
Environment	Enable application security	Authentication cache settings
		Web and SIP security
	Java 2 security	RMI/IIOP security
	$\square$ Use Java 2 security to restrict application access to local resources	Java Authentication and Authorizatic
	₩ Warn if applications are granted custom permissions	Use realm-qualified user names
	Restrict access to resource authentication data	
10DI		
-	User account repository Current realm definition	Security domains     External authorization providers
Done		was7host01:9043 🦰

- \_\_\_\_a. If administrative security is not enabled, enable it (using a file-based repository) and restart the server.
- \_\_\_\_3. For security reasons, it is not necessarily desirable to have your administrators be able to configure and control the audit settings. The primary security user has implicit rights to the audit functionality, but other administrators do not (unless they have explicitly had the Audit role granted to their user). This step goes through adding a new user named **wsaudit** and assigning it to the **Auditor**.
  - \_\_\_\_a. In the administrative console, under Users and Groups, click Manage Users.
  - \_\_\_\_b. Click **Search** to verify that **wsaudit** does not already exist.

lanage Users				
Search for Users				
Search by *Search for *Maximum results User ID  * 100				
Search				
Create Delete				
Page 1 of 1 Total: 0				

- \_\_\_\_ c. Click **Create** to add the new user. On the next screen enter:
  - wsaudit for the User ID
  - WAS for the First name
  - Auditor for the Last name
  - wsdemo for the Password and confirmation password

Integrated Solutions Console - Mozilla	a Firefox				<u>-0×</u>
Eile Edit View <u>G</u> o Bookmarks <u>T</u> ool:	s <u>H</u> elp				0
🗘 • 🏟 • 🛃 😣 🚷 🗈	https://was7host01:9043/ibm/console/secure/securelogon.do				
Integrated Solutions Console Welcome ws	demo		Help   Logout		IDM.
View: All tasks	Manage Users				
Welcome	Manage Users				2 = 0
Guided Activities					
	Create a User				
Applications	*User ID				
	wsaudit	Group Membership			
🗄 Resources	* First name	*Last name			
	WAS	Auditor			
Environment	E-mail				
System administration					
🗆 Users and Groups	* Password *****	* Confirm password *****			
<ul> <li>Administrative user roles</li> <li>Administrative group roles</li> <li>Manage Users</li> <li>Manage Groups</li> </ul>	Create Cancel				
⊞ Monitoring and Tuning			N		
			$\mathbb{R}$		
•	×				
Done				was7ho	st01:9043 👸 🏾

\_\_\_\_ d. Click Create again and then Close.

\_\_\_\_\_4. Assign the Auditor role to wsaudit.

\_\_\_\_a. Using the administrative console, click Administrative user roles under Users and Groups.

\_\_\_ b. Click Add.



\_\_\_\_ c. Select the Auditor role under the Roles list. Then click the Search button to display the list of known users. From the list of users, select wsaudit in the Available box and click the right arrow to add them to the Mapped to role.



\_\_\_\_ d. Click **OK** and **Save** the changes.

### Part 2: Configure and enable security auditing

Now that an auditor user exists, this part of the exercise configures and enables WebSphere security auditing. Before auditing can be enabled, several configuration settings need to be set so that the audit service knows what to do with the audit events.

This initial part of the exercise turns on the basic auditing functions and sends the output to a log file.

- \_\_\_\_1. Before enabling security auditing, there are some configuration setting that need to be set.
  - \_\_\_\_a. In the administrative console, click Security auditing under Security.
  - \_\_\_\_b. Before enabling the auditing, it is necessary to determine what happens with the audit records. Start by clicking **Audit monitor** under **Related Items**.
  - \_\_\_\_ c. Under **Notifications**, click **New**.
  - \_\_\_\_d. This screen defined the notification specifics. Enter Log\_Notification for the Notification name and check the Message log box. You can also configure e-mail notifications if needed.

😻 Integrated Solutions Console - Mozilla	Firefox	
Eile Edit View Go Bookmarks Iools	Help	<u> </u>
🔷 • 🌳 • 🥰 🔕 🚷 🔯	ttps://was7host01:9043/ibm/console/secure/securelogon.do	<u>⊖</u> © ∞ [C,
Integrated Solutions Console Welcome woo		TEM.
View: All tasks	Cell=was7host01Node02Cell, Profile=Audit	Close page
= Welcome	Security auditing	? - Help -
⊞ Guided Activities     ■	Security auditing > Audit monitor > Notifications	Field help
Gervers	Specifies the generic notification definitions that are used in certificate expiration	Specifies that this configuration intends to
	monitors. General Properties	log certificate expiration information to the
	Notification name	message log file.
Resources	Log_Notification	Page help More information about
🖂 Security	🗹 Message log	this page
<ul> <li>Global security</li> <li>Security domains</li> <li>Administrative Authorization Groups</li> <li>SSL certificate and key management</li> <li>Security auditing</li> <li>Bus security</li> </ul>	E-mail address to add	Command Assistance <u>View administrative</u> <u>scripting command for last</u> <u>action</u>
⊞ Environment	Remove	
	Outgoing mail (SMTP) server	
🖯 Users and Groups		
<ul> <li>Administrative user roles</li> <li>Administrative group roles</li> <li>Manage Users</li> <li>Manage Groups</li> </ul>	Apply OK Reset Cancel	
🕀 Monitoring and Tuning		
🗄 Troubleshooting 🗸 💂		
*I I F		
Done		was7host01:9043 😁 🥢

\_\_\_\_e. Click **OK** and **Save** the changes.

\_\_\_\_ f. Now that a notification definition exists, it is possible to configure auditing to use that notification. On the same screen, check the **Enable monitoring** box and verify that **Log\_Notification** has been selected in the **Monitor notification** pull-down list.



\_\_\_\_ g. Click **OK** and **Save** the changes. This returns you to the main **Security auditing** page.

- \_\_ 2. Now that the configuration settings have been completed, it is possible to enable auditing.
  - \_\_\_\_ a. At this point, check the Enable security auditing box. From the Audit subsystem failure action pull-down, select Log warning. And from the Primary auditor user name, select wsaudit.



**NOTE:** The Audit subsystem failure action dropdown menu has the following options:

**No warning**: The **No warning** action specifies that the auditor will not be notified of a failure in the audit subsystem. The product will continue processing but audit reporting will be disabled.

**Log warning**: The Log warning action specifies that the auditor will be notified of a failure in the audit subsystem. The product will continue processing but audit reporting will be disabled.

**Terminate server**: The Terminate server action specifies the application server to gracefully quiesce when an unrecoverable error occurs in the auditing subsystem. If e-mail notifications are configured, the auditor will be sent a notification that an error has occurred. If logging to the system log is configured, the notification of the failure will be logged to the system file.

\_\_\_\_b. Click Apply and Save the changes.

- \_\_\_\_\_ 3. **Restart the server** to have these security changes take effect.
  - \_\_\_\_a. In order for these changes to take effect, the server needs to be restarted. If this were running in a federated environment, the nodes would first be resynchronized, and then all processes in the cell would be restart.
  - \_\_\_\_b. For this exercise, **stop** the server and then **start** it again.

### Part 3: View the audit logs

Security auditing is now enabled. This part of the exercise goes through the process of viewing the audit data.

The fastest way to view the data is to simply look at the log file that is generated, but that can be difficult to read. The other way to view the data is to use wsadmin to generate an html report. This part of the exercise goes through both of these options.

- \_\_\_\_\_1. View the log records with a text editor.
  - \_\_\_\_a. Using **Windows Explorer**, go to the logs directory for the server and open the file called **BinaryAudit\_<cellName>\_<nodeName>\_server1.log** in a text editor.

BinaryAudit - Notepad
File Edit Format View Help
Files\IBM\webSphere\AppServer\java\bin;C:\Program Files\IBM\webSphere\AppServer\java\jre\bin;C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System3 2\wbem
Current trace specification = *=info
<pre>current trace spectrication = ~=Into ************************************</pre>
26 17:20:17 EDT 2008   GlobalInstanceId = 0   FirstCaller = pull   Realm = defaultWIMFileBasedRealm   RegistryType = null   Url = N/A (Dseq = 2) Event Type = SECURITY_AUTHN   Outcome = UNSUCCESSFUL   OutcomeReason = DENIED   OutcomeReasonCode = 15   SessionId = Ubq-wi-J2zFAYNJXVQOelv   RemoteAddr = 192.168.128.142   RemotePort = 2429   RemoteHost = 192.168.128.142   ProgName = /navigatorCmd.do   Action = webAuth   RegistryUserName = null   AppUserName = null   AccessDecision = denied   ResourceName = GET   ResourceType = web   ResourceUniqueId = 0   PermissionSChecked = null   PermissionSGranted = null   RolesChecked = N/A   RolesGranted = null   EventTrailId = 457691007   CreationTime = Thu Jun 26 17:24:44 EDT 2008   GlobalInstanceId = 0   FirstCaller = null   Realm = defaultWIMFileBasedRealm   RegistryType = WIMUserRegistry   AuthnType = challengeResponse   Provider = WebSphere   ProviderStatus = providerSuccess(DSeq = 3) Event Type = SECURITY_AUTHN   Outcome = UNSUCCESSFUL   OutcomeReason = DENIED   OutcomeReasonCode = 15   SessionId = Ubq-wi-J2zFAYNJXVQOelv   RemoteAddr = 192.168.128.142   RemotePort = 2429   RemoteHost = 192.168.128.142   ProgName = /navigatorCmd.do   Action = webAuth   RegistryUserName = null   AppUserName = null   AccessDecision = denied   ResourceName = GET   ResourceType = web   ResourceUniqueId = 0   PermissionSchecked = null   PermissionSchame = GET   ResourceType = web   ResourceUniqueId = 0   PermissionSchecked = null   PermissionSchame = GET

\_\_\_\_\_ b. Notice the sequence numbers. Those are the individual audit records, but this format certainly is not easy to read. If a better text editor is used, the output can be slightly more readable, but still not easy to read.

```
************ Start Display Current Environment ************
.
WebSphere Platform 7.0.0.0 [ND 7.0.0.0 h0823.03] running with process name was7host01Node02Cell\was7host01Nod
Detailed IFix information: No Interim Fixes applied to this build
Host Operating System is Windows XP, version 5.1 build 2600 Service Pack 3
Java version = J2RE 1.6.0 IBM J9 2.4 Windows XP x86-32 jvmwi3260-20080523 19691 (JIT enabled, AOT enabled)
J9VM - 20080523_019691_1HdSMr
JIT - r9 20080522 1822
GC - 20080521_AC, Java Compiler = j9jit24, Java VM name = IBM J9 VM
was.install.root = C:\Program Files\IBM\WebSphere\AppServer
user.install.root = C:\Program Files\IBM\WebSphere\AppServer\profiles\Audit
Java Home = C:\Program Files\IBM\WebSphere\AppServer\java\jre
ws.ext.dirs = C:\Program Files\IBM\WebSphere\AppServer/java/lib;C:\Program Files\IBM\WebSphere\AppServer\prof
Classpath = C:\Program Files\IBM\WebSphere\AppServer\profiles\Audit/properties;C:\Program Files\IBM\WebSphere
Java Library path = C:\Program Files\IBM\WebSphere\AppServer\java\jre\bin;.;C:\Program Files\IBM\WebSphere\Ap
Current trace specification = *=info
************** End Display Current Environment **************
Seq = 0 | Event Type = SECURITY_RESOURCE_ACCESS | Outcome = SUCCESSFUL | OutcomeReason = SUCCESS | OutcomeRea
Seq = 1 | Event Type = SECURITY RESOURCE ACCESS | Outcome = SUCCESSFUL | OutcomeReason = SUCCESS | OutcomeRea
Seq = 2 | Event Type = SECURITY AUTHN | Outcome = UNSUCCESSFUL | OutcomeReason = DENIED | OutcomeReasonCode =
Seq = 3 | Event Type = SECURITY_AUTHN | Outcome = UNSUCCESSFUL | OutcomeReason = DENIED | OutcomeReasonCode =
Seq = 4 | Event Type = SECURITY AUTHN | Outcome = SUCCESSFUL | OutcomeReason = REDIRECT | OutcomeReasonCode =
Seq = 5 | Event Type = SECURITY RESOURCE ACCESS | Outcome = SUCCESSFUL | OutcomeReason = SUCCESS | OutcomeRea
Seq = 6 | Event Type = SECURITY_RESOURCE_ACCESS | Outcome = SUCCESSFUL | OutcomeReason = SUCCESS | OutcomeRea
Seq = 7 | Event Type = SECURITY AUTHN | Outcome = SUCCESSFUL | OutcomeReason = SUCCESS | OutcomeReasonCode =
Seq = 8 | Event Type = SECURITY_AUTHN | Outcome = SUCCESSFUL | OutcomeReason = SUCCESS | OutcomeReasonCode =
Seq = 9 | Event Type = SECURITY AUTHN | Outcome = SUCCESSFUL | OutcomeReason = SUCCESS | OutcomeReasonCode =
Seq = 10 | Event Type = SECURITY_AUTHN | Outcome = SUCCESSFUL | OutcomeReason = SUCCESS | OutcomeReasonCode =
Seq = 11 | Event Type = SECURITY AUTHN | Outcome = SUCCESSFUL | OutcomeReason = SUCCESS | OutcomeReasonCode =
Seq = 12 | Event Type = SECURITY AUTHN | Outcome = SUCCESSFUL | OutcomeReason = SUCCESS | OutcomeReasonCode =
Seq = 13 | Event Type = SECURITY_AUTHN | Outcome = SUCCESSFUL | OutcomeReason = SUCCESS | OutcomeReasonCode =
•
```

\_\_\_\_ c. It is also possible to use **tail -f** to track the entries added to the log file in real time.

- 2. Verify that auditing is actually logging events that need to be reported.
  - \_\_\_\_a. Open a new browser instance to the administrative console.
  - \_\_\_\_b. When prompted for a username and password, enter BADUSER and wsdemo

Integrated Solutions Console	Integrated Solutions Console
Log in to the console.	
BADUSER Password:	Login failed. Check the user ID and password and try again.
	OK

\_\_\_\_c. Reopen the **BinaryAudit\_<cellName>\_<nodeName>\_server1.log** in a text editor and search for **BADUSER**. There will be several instances and it becomes clear that the login attempt failed.

BinaryAudit - Notepad
File Edit Format View Help
RemotePort = 2466   RemoteHost = localhost   ProgName = /images/Error.gif   Action = resourceAccess   RegistryUsenName = defaultWIMFileBasedRealm/wsdemo   AppUserName = baduser   AccessDecision = accessSuccess   ResourceName = GET   ResourceType = web   ResourceUniqueId = 0   PermissionsChecked = null   PermissionsGranted = null   RolesChecked = unprotected   RolesGranted = unprotected   EventTrailId = 877113022   CreationTime = Thu Jun 26 17:39:55 EDT 2008   GlobalInstanceId = 0   FirstCaller = null   Realm = defaultWIMFileBasedRealm   RegistryType = WIMUserRegistry   url = /images/Error.gif ISeq = 26   Event Type = SECURITY_RESOURCE_ACCESS   Outcome = SUCCESSFuL   OutcomeReason = SUCCESS   outcomeReasonCode = 6   SessionId = PTFrXRjdTwaTI22-rIVgck   RemoteAddr = 127.0.0.1   RemotePort = 2466   RemoteHost = localhost   ProgName = /logon.jsp   Action = resourceAccess   RegistryUserName = defaultWIMFileBasedRealm/wsdemo   AppUserName = baduser   AccessDecision = accessSuccess   ResourceName = POST   ResourceType = web   ResourceUniqueId = 0   PermissionsChecked = null   PermissionsGranted = null   RolesChecked = unprotected   RolesGranted = unprotected   EventTrailId = 877113022   CreationTime = Thu Jun 26 17:42:49 EDT 2008   GlobalInstanceId = 0   FirstCaller = null   Realm = defaultWIMFileBasedRealm   RegistryType = WIMUserRegistry   Url = /logon.jsp ISeq = 27   Event Type = SECURITY_AUTHN   Outcome = UNSUCESSFUL   OutcomeReason = REDIRECT   OutcomeReasoncode = 15   Ses§ionId = PTFrXRjdTwaTI22-rIVgck   RemoteAddr = 127.0.0.1   RemotePort = 2479   RemoteHost = localhost   ProgName = isClite   Action = formlogie   RegistryUserName = defaultWIMFileBasedRealm/wsdemo   AppUserName = BADUSER   AccessDecision = authRedirect   ResourceName = POST   ResourceType = web   ResourceMaleI = 0   PermissionSChecked = null PermissionSChecked = null   Realm = the JUN 26 17:44:28 EDT 2008   GlobalInstanceId = 0   FirstCaller = null   Realm = defaultWIMFileBasedRealm / SecourceType = WEUSERSE   OutcomReason

- \_ 3. View the log entries using the Audit Log Reader. This is an interface available through wsadmin which will convert the audit log entries into an html report.
  - \_\_\_\_a. Using a command window, go to the bin directory for your profile. Enter the command:

wsadmin -lang jython -username wsaudit -password wsdemo

\_\_\_\_b. Once the wsadmin shell has started, enter the following command to generate an html report AdminTask.binaryAuditLogReader('-interactive')

- \_\_\_\_ c. The interactive mode will prompt for input for the following questions. Enter the following:
  - filename:

<profile\_root>\logs\server1\BinaryAudit\_<cellName>\_<nodeName>\_server1.log

- outputLocation: C:\basicAuditReport.html
- Key Store Password: <br/>
  <b
- Data points: <br/>
   <br/>
- Timestamp filter: <blank>
- Report mode selection: basic
- Events filter: <br/>
   <br/
- Outcomes filter: <br/>
   <br/>
- Sequence filter: <br/>
   <b
- Select [F, C]: F

\_\_\_\_d. At this point an html file by the name of **basicAuditReport.html** is generated. With a Windows Explorer window, browse to the C:\ directory and double click **basicAuditReport.html**.

	Audit	Records
	Hostname was7host01 . Re	portTime Jun 30, 2008, 15:05:50
Record Number	Event Type	Outcome
0	SECURITY_RESOURCE_ACCES	S SUCCESS
CreationTime=Thu Jun 26 17:20:17 EDT 2008	Action=preinvoke MBean	ProgName=Server (module)
RemoteAddr=null	RemotePort=null	RemoteHost=null
ResourceName=getState	ResourceType=SM_MBEAN	ResourceUniqueId=0
1	SECURITY_RESOURCE_ACCES	S SUCCESS
CreationTime=Thu Jun 26 17 20 17 EDT 2008	Action=preinvoke MBean	ProgName=Server (module)
RemoteAddr=null	RemotePort=null	RemoteHost=null
ResourceName=getState	ResourceType=SM_MBEAN	ResourceUniqueId=0
2	SECURITY_AUTHN	DENIED
CreationTime=Thu Jun 26 17:24:44 EDT 2008	Action=webAuth	ProgName=/navigatorCmd.do
RemoteAddr=192.168.128.142	RemotePort=2429	RemoteHost=192.168.128.142
ResourceName=GET	ResourceType=web	ResourceUniqueId=0
3	SECURITY_AUTHN	DENIED
CreationTime=Thu Jun 26 17:24:44 EDT 2008	Action=webAuth	ProgName=/navigatorCmd.do
RemoteAddr=192.168.128.142	RemotePort=2429	RemoteHost=192.168.128.142
ResourceName=GET	ResourceType≕web	ResourceUniqueId=0

### Part 4: (Optional) Create a new event filter

At this point, security auditing is configured and enabled and the logs have been viewed both through a text interface and an HTML report. Those are the most basic steps for getting started with auditing.

The rest of the exercise goes through some additional features including configuring additional filters and encryption of the audit data. Since these features might not be of interest to all students, these parts have been marked as optional.

In this part of the exercise, an additional event filter is created. This filter tells the audit service to audit any authorization failures.

- 1. The first step will be to add and configure the new event filter.
  - \_\_\_\_a. Using the administrative console, log in as **wsaudit**. Go to the **Security auditing** page, and click **Event type filters** under **Related Items**.
  - \_\_\_\_b. There are four default filters, including authentication success, denied and redirect. There is also one resource\_access filter. To create a new filter, click **New**.

ecurity a	uditing ? -				
<u>Security auditing</u> > Event type filters					
	the audit filters configured f ype and outcome are to be fi		n, including what auditable		
🕀 Prefe	erences				
New	Delete				
Select	Name 🛟	Enable 🗘	Events and Outcomes 🗘		
You ca	n monitor the following reso	urces:			
	DefaultAuditSpecification 1	true	AUTHN:SUCCESS		
	DefaultAuditSpecification_2	true	AUTHN: DENIED		
	DefaultAuditSpecification 3	true	RESOURCE_ACCESS:SUCCESS		
	DefaultAuditSpecification 4	true	AUTHN:REDIRECT		
Total 4	ŧ				

\_\_\_\_ c. Enter Authorization\_Event for the Name. Select SECURITY\_AUTHZ from the Selectable events region and click the right arrow to move it into the Enabled events. Then select DENIED from the Selectable events outcomes and click the right arrow to move it into the Enabled event outcomes.

Security auditing ? –
<u>Security auditing</u> > <u>Event type filters</u> > New
Defines the audit filters configured for the implementation, including what auditable event type and outcome are to be filtered.
General Properties
* Name Authorization_Event
Events to associate with an audit filter
Selectable events SECURITY_AUTHN SECURITY_AUTHN_CREDS_MODIFY SECURITY_AUTHN_DELEGATION SECURITY_AUTHN_MAPPING
Event outcomes to associate with an audit filter  Selectable event outcomes  SUCCESS INFO WARNING ERROR
Apply OK Reset Cancel

\_\_\_\_ d. Click **OK** and **Save** the changes.

- 2. Notice that there is a new event defined. But this event will not be audited until further configuration is complete. The next step is to configure the service provider.
  - \_\_\_\_a. Go back to the **Security auditing** page and click **Audit service provider**. There will be only one defined at this point, click **auditServiceProviderImpl\_1**.

ecurity auditing		2.
<u>Security auditing</u> > Audit service pr	ovider	
Audit service providers define the im are three types of audit service prov		on details of the service provider. There y file-based, SMF, and third party.
New 🔹 Delete		
Select Name 🛟	Туре 🗘	Event Formatting Module Class Name 💲
You can monitor the following reso	urces:	
auditServiceProviderImpl 1	Binary file-based emitter	
Total 1		

\_\_\_\_b. Notice that the Authorization\_Event that was just created is listed under the Selectable filters, but is not part of the Enabled filters list. Select the new filter and click the right arrow to move it to the Enabled filters list.

Security auditing ? –
<u>Security auditing</u> > <u>Audit service provider</u> > auditServiceProviderImpl_1
Audit service providers define the implementation details of the service provider. There are three types of audit service providers: binary file-based, SMF, and third party.
General Properties
* Name
auditServiceProviderImpl_1
* Audit log file location
\$(LOG_ROOT)
Audit log file size:
10 MB
Maximum number of audit log files
100
Event formatting module class name
Sele table filters
Authorization_Event
DefaultAuditSpecification_2
DefaultAuditSpecification_3 DefaultAuditSpecification_4
Apply OK Reset Cancel

\_\_\_\_ c. Click **OK** and **Save** the changes.

- \_\_\_\_\_ 3. Update the event factory configuration.
  - \_\_\_\_a. Return to the **Security auditing** page and click on **Audit event factory configuration**. There will be only one defined at this point, click **auditEventFactoryImpl\_1**.
  - \_\_\_\_b. Like in the service provider screen, move the **Authorization\_Event** to the **Enabled filters** for the event factory.

Security auditing ? –
<u>Security auditing</u> > <u>Audit event factory configuration</u> > auditEventFactoryImpl_1
Defines the audit event factories.
General Moperties
* Name
auditEventFactoryImpl_1
* Туре
IBM audit event factory
* Class name
com.ibm.ws.security.audit.AuditEventFactoryImpl
Audit service provider auditServiceProviderImpl_1
Selectable filters       * Enabled filters         Authorization_Event       DefaultAuditSpecification_1         DefaultAuditSpecification_2       DefaultAuditSpecification_3         DefaultAuditSpecification_4       VefaultAuditSpecification_4
Custom properties
Select Name Value New
Delete Delete
Apply OK Reset Cancel

\_\_\_\_ c. Click **OK** and **Save** the changes.

**Note:** The event factory is where the configuration is done to define what events are gathered. The service **provider** is where the configuration occurs to define which events are reported. See the Information Center for details on the numerous other event types that can be configure.

- \_\_\_\_4. Restart the application server and verify that these updates are doing what is expected.
  - \_\_\_\_\_a. **Restart the application server** in order for the changes to take effect.
  - \_\_\_\_b. Once the application server has been restart, look at the **BinaryAudit.log** file in the server's log directory. Take note of the latest sequence number.
  - \_\_\_\_\_ c. Now, attempt to stop the application server using **wsaudit** as the username. Since the **wsaudit** user is not a console administrator, this should fail.

🖾 Command Prompt	×I
C:\Program_Files\IBM\WebSnhere\AnnServer\profiles\Audit\bin>stopServer.bat_serve r1_username_wsaudit_password_wsdemo	]
ADMUØLIEL: LOOL INFORMATION IS DEING LÖGGED IN FILE C:\Program Files\IBM\WebSphere\AppServer\profiles\Audit\logs\server1\stopServer. log	
ADMU0128I: Starting tool with the Audit profile	
ADMU3100I: Reading configuration for server: server1	
ADMU0111E: Program exiting with envort jaway management JMRuntimeException:	
ADMN0022E: Access is denied for the stop operation on Server MBean	
ADMU4113E: Verity that username and password information is correct. If running tool from the command line, pass in the correct -username and -password. Alternatively, update the <conntype>.client.props file.</conntype>	
ADMU1211I: To obtain a full trace of the failure, use the -trace option.	
ADMU0211I: Error details may be seen in the file: C:\Program	
Files\IBM\WebSphere\AppServer\profiles\Audit\Iogs\server1\stopServer. log	
C:\Program Files\IBM\WebSphere\AppServer\profiles\Audit\bin>	

\_\_\_\_\_d. Once the stopServer command has failed, look at the **BinaryAudit.log** file again. Look for the **SECURITY\_AUTHZ** entry that shows the denial.

🔤 Command Prompt
Seq = 1   Event Type = SECURITY_RESOURCE_ACCESS   Outcome = SUCCESSFUL   Outcome Reason = SUCCESS   OutcomeReasonCode = 6   SessionId = N/A   RemoteAddr = null   RemotePort = null   RemoteHost = null   ProgName = Server (module)   Action = p reinvoke MBean   RegistryUserName = null   AppUserName = null   AccessDecision = authnSuccess   ResourceName = getState   ResourceType = SM_MBEAN   ResourceUniq ueId = 0   PermissionsChecked = null   PermissionsGranted = null   RolesChecked = N/A   RolesGranted = null   EventTrailId = 457691007   CreationTime = Mon Jun 30 17:34:56 EDT 2008   GlobalInstanceId = 0   FirstCaller = null   Realm = defau ItWFileBasedRealm   RegistruTume = null   IvP = N/A
Seq = 2
ort = null ; Remotehost = null ; rrogName = Server.stop:java.lang.Boolean:java.l ang.Integer ; Action = authz ; RegistryUserName = null ; AppUserName = defaultWI MFileBasedRealm/wsaudit ; AccessDecision = authzDenied ; ResourceName = Server ; ResourceType = WAS ; ResourceUniqueId = 0 ; PermissionsChecked = null ; Permiss ionsGranted = null ; RolesChecked = operator , administrator ; RolesGranted = nu l1 ; EventTrailId = 1079617506 ; CreationTime = Mon Jun 30 17:36:29 EDT 2008 ; G lobalInstanceId = 0 ; FirstCaller = null ; Realm = defaultWIMFileBasedRealm ; Re gistryType = WIMUserRegistry ; Provider = WebSphere ; ProviderStatus = providerS uccess ; PolicyName = null ; PolicyType = null
C:\Program Files\IBM\WebSphere\AppServer\profiles\Audit\bin>_

## Part 5: (Optional) Digitally sign the audit log entries

By default, the auditing data is stored in clear text. Although this provides useful information, it could potentially be tampered with. To help deal with this issue, the data can be digitally signed, encrypted or both. This part of the exercise turns on digital signatures for the audit data ensuring the integrity of the data.

The administrator is able to choose which certificate's private key is used to digitally sign the log entries. This then means that only the corresponding public key is needed to validate the signature. For an additional level of security, turning on digital signing also has the side effect of having the log entries 64-bit encoded.

- \_\_\_\_\_1. For this part of the exercise, administrative access is required for the console (not just auditor access).
  - \_\_\_\_a. In the administrative console window, logout as the wsaudit user.
  - \_\_\_\_b. Log in again as **wsdemo**, which has implicit access as an administrator.

- \_\_\_\_\_2. Turn on digital signing for the audit logs.
  - \_\_\_\_a. Return to the **Security auditing** page of the administrative console and click **Audit record signing configuration**.
  - \_\_\_\_\_b. Check the Enable signing box. Accept the default for the Managed keystore containing the signing certificate, which should be the NodeDefaultKeyStore. For the Certificate alias under Certificate in keystore, select default from the pulldown.

General Properties
Enable signing
Managed keystore containing the signing certificate
NodeDefaultKeyStore ((cell):was7host00Node02Cell:(node):was7host00Node03)
Certificate in keystore Certificate alias default 👽
Create a new certificate in the selected keystore file Certificate alias
Import the encryption certificate
Automatically generate certificate
Import a certificate
Key file name
Path
Type PKCS12
Key file password
Get Key File Aliases
Certificate alias to import
Apply OK Reset Cancel

- \_\_\_\_ c. Click **OK** and **Save** the changes.
- \_\_\_\_\_ d. **Restart the application server** to have the changes take affect.

- \_\_\_\_3. View the audit log and take note that the log entries are now encoded.
  - \_\_\_\_a. Using a text editor, open the new BinaryAudit.log file. Notice that the records are now encoded. The file header also includes specific information on the keys used for digitally signing the records.

📕 BinaryAudit.log - Notepad	<u>- 0 ×</u>
File Edit Format View Help	
2\wbem Current trace specification = *=info	
*********** End Display Current Environment *********** <signing information="">0 <signingsharedkey>gJ6Rj++g9eX4bfa5iITnefsIu642458Ze83rcuRVlkE=</signingsharedkey>0</signing>	
<pre> <signingcertalias>default</signingcertalias>0  <scope>(cell):was7host00Node02Cell:(node):was7host00Node03</scope>0</pre>	
<pre><signingkeystore>&gt;&gt;{CONFIG_ROOT}/cells/was7host00Node02Cell/nodes/was7host00Node03/key.p12 190799KeyStore&gt;u <signingcertificate>IBMJCE RSA Public Key:0modulus:0 99022190580965844396376938785802614365701053713946216263124748687662444467933731511679246</signingcertificate></signingkeystore></pre>	
67117047651685396310348351053840896397694388515672322390010525105350927530331203632059703 75657784987061549513152272871709669318938154846810974018205832788706557478452775983553804 532159476020889056961474849415130public exponent:065537000information>0	3894
<pre>degin&gt;l2vxiD0gMCB8IEv2zw50IFR5cGUgPSBTRUNVUklUwv9SRVNPvvJDRv9BQ0NFu1MgfCBPdxRjb21lID0gU1 0vr0uzv1CB8IE91dGNvbwvszwFzb24gPSBTvUNDRvNTIHwgT3v0Y29tzvJlyxNvbkNvzGUgPSA2IHwgU2vzc2lvbk D0gTi9BIHwgUmvtb3RlQwRkciA9IG51bGwgfCBSzw1vdGvQb3J0ID0gbnvsbCB8IFJlbw90zUhvc3QgPSBudwxsIH</pre>	klki
HJVZ05hbwUgPSBTZXJ2ZXIgKG1vZHVSZSkgfCBBY3Rpb24gPSBwcmvpbnZva2UgTUJ1vW4gfCBSZWdpC3RyeVvZZ> W11ID0gbnvsbCB8IEFwcFvZZXJ0vW11ID0gbnvsbCB8IEFjY2vzc0R1Y21zaw9uID0gYXV0aG5TdWNjZXNZIHwgUm 3vyY2v0YW11ID0gZ2v0U3RhdGUgfCBSZXNvdXJjZvR5cGUgPSBTTV9NQkVBTiB8IFJ1c291cmN1vW5pcXv1sWQgP	xJŌY m∨zb
HwgUGVybwlzc2lvbnNDaGVja2vkID0gbnVsbCB8IFBlcm1pc3Npb25zR3JhbnRlZCA9IG51bGwgfCBSb2xlc0NoZV WQgPSBoL0EgfCBSb2xlc0dyvw50ZWQgPSBudwxsIHwgRXZlbnRUcmFpbElkID0gMjE30Dg4NjQZIHwgQ3JlYXRpb2 W1lID0gVHVlIEp1bCAwMSAXOToxMzoxOSBFRFQgMjAwoCB8IEdsb2JhbEluc3RhbmNlSWQgPSAwIHwgRmlyc3RDYv	25Ua 📗
XIgPSBudwxsIHwgUmvhbG0gPSBkZwZhdwx0v0lNmmlsZUJhc2vkUmvhbG0gfCBSZwdpc3RyevR5cGUgPSBudwxsIH XJSID0gTi9BI4o8c2lpbmF0dXJlPnRRTAXTexH7HwAn50QGJDxloihw0we1GXsis5ij683rqXLAudDv6oy8L3NpZ2 HVyZT4€ <end><begin>J2VXID0gMSB8IEV2Zw50IFR5cGUqPSBTRUNVUklUwv9SRVNPVvJDRv9BQ0NFU1MqfCBPd&gt;</begin></end>	HwgV 25hd
211ID0g01vDq0vT002V1CB8IE91dGNvbwVsZwFzb24gPsBTVUNDRVNTIHwgT3V0Y29tZVJ1YXNvbkNvZGUgPSA2IF 2Vzc2lvbklkID0gT19BIHwgUmVtb3RlQwRkc1A9IG51bGwgfCBsZw1vdGvQb3J0ID0gbnVsbCB8IFJlbw90ZUhvc3	HwgU 3QgP
SBudwxsIHwgUHJVZ05hbwUğPSBTZXJ2ZXIgKG1vZHVsZSkğfCBBY3Rpb24gPSBwcmvpbnZva2UgTUJ1YW4gfCBSZV 3RyeVvZZXJ0YW11ID0gbnvsbCB8IEFwcFvZZXJ0YW11ID0gbnvsbCB8IEFjY2Vzc0R1Y21zaw9uID0gYXv0aG5Tdw XNZIHwgUmvzb3vyY2v0YW11ID0gZ2V0U3RhdGUgfCBSZXNvdXJjZvR5cGUgPSBTTV9NQkVBTiB8IFJ1c291cmN1vv	wNjZ
XVlSwQğPSAwIHwģUGVybwlzc2lvbnNDaGVja2vkID0gbnVsbCB8IFBlcm1pc3Npb25zR3JhbnRlZCA9IG51bGwgfC 2xlc0NoZWNrZwQgPSBoL0EgfCBSb2xlc0dyYw50ZwQgPSBudwxsIHwgRXZlbnRUcmFpbElkID0gMjE30Dg4NjQZIH 3JlYXRpb25Uaw1lID0gVHVlIEp1bCAwMSAXOToXMZoXOSBFRFQgMjAwoCB8IEdsb2JhbEluc3RhbmNlSwQgPSAwIH	CBSb   HwqQ
mlyc3RbYWxsZXIgPSBūdWxsIHwgUmVhbG0gPSBkZwZhdwx0V0lNRmlsZUJhc2VkUmVhbG0gfCBSZWdpc3RýeVR5cc SBudWxsIHwgVXJsID0g <u>Ti9BI</u> Ao8c2lnbmF0dXJlPo6Z9wHHkqUzx6i7Lqs5W2MlzCBLicp59NB2/40RQK+OqXLAuc	GUĀP 📗
oY8L3NpZ25hdHvyZT4< <end></end>	-

\_\_\_\_b. Now verify that the html reports can still be generated correctly. In a command window, start wsadmin from the profile's bin directory with the following command:

wsadmin -lang jython -username wsaudit -password wsdemo

\_\_\_\_ c. Once the wsadmin shell has started, enter the following command to generate an html report

AdminTask.binaryAuditLogReader('-interactive')

\_\_\_\_\_d. The interactive mode will prompt for input for the following questions. Enter the following:

filename:

<profile\_root>\logs\server1\BinaryAudit<cellName>\_<nodeName>\_server1.log

•	outputLocation:	C:\signedAuditReport.html
---	-----------------	---------------------------

•	Key Store Password:	<blank></blank>
•	Data points:	<blank></blank>
•	Timestamp filter:	<blank></blank>
•	Report mode selection:	basic
•	Events filter:	<blank></blank>

- Outcomes filter: <br/>
   <b
- Sequence filter: <br/>
   <br/>
- Select [F, C]:
- \_\_\_\_ e. Using Windows Explorer, go to C:\ and double click on signedAuditReport.html. This will open the HTML report in a browser. Notice that the entries in this report look exactly like they did before the signing was turned on.

#### Audit Records

Record Number	Event Type	Outcome
0	SECURITY_RESOURCE_ACCESS	SUCCESS
CreationTime=Tue Jul 01 19:13:19 EDT 2008	Action=preinvoke MBean	ProgName=Server (module)
RemoteAddr=null	RemotePort=null	RemoteHost=null
ResourceName=getState	ResourceType=SM_MBEAN	ResourceUniqueId=0
1	SECURITY_RESOURCE_ACCESS	SUCCESS
CreationTime=Tue Jul 01 19:13:19 EDT 2008	Action=preinvoke MBean	ProgName=Server (module)
RemoteAddr=null	RemotePort=null	RemoteHost=null
ResourceName=getState	ResourceType=SM_MBEAN	ResourceUniqueId=0
2	SECURITY_RESOURCE_ACCESS	SUCCESS
CreationTime=Tue Jul 01 23:24:20 EDT 2008	Action=preinvoke MBean	ProgName=Server (module)
RemoteAddr=null	RemotePort=null	RemoteHost=null
ResourceName=getProcessType	ResourceType=SM_MBEAN	ResourceUniqueId=0
3	SECURITY_RESOURCE_ACCESS	SUCCESS
CreationTime=Tue Jul 01 23:24:44 EDT 2008	Action=execute command	ProgName=com.ibm.websphere.management.cmdframe
RemoteAddr=null	RemotePort=null	RemoteHost=null
ResourceName=getNodeBaseProductVersion	ResourceType=SM_COMMAND	ResourceUniqueId=0
4	SECURITY_RESOURCE_ACCESS	SUCCESS
CreationTime=Tue Jul 01 23:26:49 EDT 2008	Action=execute command	ProgName=com.ibm.ws.security.audit.tools.binaryAudit
RemoteAddr=null	RemotePort=null	RemoteHost=null
ResourceName=binaryAuditLogReader	ResourceType=SM_COMMAND	ResourceUniqueId=0

#### Hostname was7host00 . ReportTime Jul 1, 2008, 23:26:51

### Part 6: (Optional) Encrypt the audit logs

If the intention is to not just protect the integrity of the data, but actually encrypt it, that is possible as well. In this part of the exercise, the log entries will be both encrypted and signed, but it certainly is possible to encrypt them and not sign them.

The first step toward encrypting the log entries is to create a new key store and certificate specifically for audit encryption.

- \_\_\_\_1. Log into the console as **wsaudit**.
  - \_\_\_\_a. This section requires being logged in as the **wsaudit** console user since it has auditor access.
- 2. Create a key store and certificate for audit encryption.
  - \_\_\_\_a. Using the administrative console, logged in as wsaudit, go to the Security auditing page. Click Audit encryption key stores and certificates under Related Items.
  - \_\_\_\_b. Click **New** to create a new key store and certificate.
  - \_\_ c. For the name, enter AuditKeyStore and fore the Path enter C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\properties\audit.p12. Enter wsdemo in the Password fields and accept the default Type of PKCS12.

rity auditing	
ecurity auditing > Audit encryption key stores and certificates > New efines the keystores used for storing the encryption certificate.	
General Properties * Name AuditKeyStore	The additional properties will not be available until the general properties fo this item are applied or saved.
* Path C:\Program Files\IBM\WebSphere\AppServer\profiles\AppSrv01\properties\audit.p:	Additional Properties
* Password ******  * Confirm password  ******	Personal certificates
Type PKCS12	
Apply OK Reviet Cancel	

- \_\_\_\_ d. Click **OK** and **Save** the changes.
- \_\_\_\_ e. Next the actual certificate needs to be created. Click the AuditKeyStore in the Audit encryption key stores and certificates page. On the right side, click Personal certificates under Additional Properties.
- \_\_\_\_\_f. Click **Create self-signed Certificate** to create the new certificate.

\_\_\_\_g. Enter AuditEncryptionCertificate for the Alias and ibm.com for the Common name.

General Properties
* Alias AuditEncryptionCertificate
Version X509 V3 💌
Key size 1024 💽 bits
* Common name ibm.com
* Validity period 365 days
Organization
Organization unit
Locality
State/Province
Zip code
Country or region (none)
Apply OK Reset Cancel

\_\_\_ h. Click **OK**.

- \_\_\_\_ 3. Turn on encryption for the audit logs.
  - \_\_\_\_a. Return to the Security auditing page and click Audit record encryption configuration.
  - \_\_\_\_b. Check the Enable encryption box. Accept the default keystore of AuditKeyStore and the default Certificate alias of auditencryptioncertificate.

General Properties
Enable encryption
The Audit keystore containing the encryption certificate. AuditKeyStore
• Certificate in keystore
Certificate alias
auditencryptioncertificate
C Create a new certificate in the selected keystore file Certificate alias
Certificate allas
6
Automatically generate certificate
Import a certificate
Key file name
Path
Type
PKCS12
Key file password
Get Key File Aliases
Certificate alias to import
Apply OK Reset Cancel

- \_\_\_\_ c. Click OK and Save the changes.
- \_\_\_\_\_d. Restart the application server to have the changes take effect.
- 4. View the audit log and take note that the log entries are now encrypted.
  - \_\_\_\_a. Using a text editor, open the new BinaryAudit.log file. Notice that the file header now includes encryption certificate information; otherwise the individual entries look much the same as they did when the records were merely signed.
  - \_\_\_\_b. Now verify that the html reports can still be generated correctly. In a command window, start wsadmin from the profile's bin directory with the following command:

wsadmin -lang jython -username wsaudit -password wsdemo

\_\_\_\_ c. Once the wsadmin shell has started, enter the following command to generate an HTML report AdminTask.binaryAuditLogReader('-interactive')

- \_\_\_\_d. The interactive mode will prompt for input for the following questions. Enter the following (note this time the key Store Password is required):
  - filename:

#### <profile\_root>\logs\server1\BinaryAudit\_<cellName>\_<nodeName>\_server1.log

- outputLocation: C:\encryptedAuditReport.html
- Key Store Password: wsdemo
- Data points: <br/>
   <br/>
- Timestamp filter: <br/>
   <
- Report mode selection: basic
- Events filter: <br/>
   <br/>
- Outcomes filter: <br/>
   <br/>
- Select [F, C]: F
- \_\_\_\_ e. Using Windows Explorer, go to C:\ and double click encryptedAuditReport.html. This will open the HTML report in a browser. Notice that the entries in this report look exactly like they did before the signing and encryption was turned on.

### Part 7: (Optional) Verbose logging and reporting

Finally, for comparison, this section of the exercise turns on verbose audit logging and generates a report with the complete mode.

- \_\_\_\_\_1. Turn on verbose logging for security auditing.
  - \_\_\_\_a. In the administrative console, return to the **Security auditing** page.
  - \_\_\_\_b. Check the **Enable verbose auditing** box.

ssure the integrity of the business o	o gather and store auditable event records to help computing environment.
General Properties	Related Items
Enable security auditing	Event type filters
Audit subsystem failure action	<ul> <li><u>Audit service provider</u></li> <li><u>Audit event factory configuration</u></li> </ul>
Primary auditor user name wsaudit 💌	<ul> <li><u>Audit encryption key stores and</u> <u>certificates</u></li> <li><u>Audit record encryption configuration</u></li> </ul>
Enable batching of events	<ul> <li>Audit record signing configuration</li> <li>Audit monitor</li> </ul>
Enable verbose auditing	
Apply Reset	

- \_\_\_\_ c. Click **Apply** and **Save** the changes.
- 2. In order to read the log files in clear text, disable both signing and encryption.
  - \_\_\_\_a. In the Security auditing page, click Audit record encryption configuration.
  - \_\_\_\_b. Uncheck Enable encryption and click OK.
  - \_\_\_ c. Save the changes.
  - \_\_\_\_ d. In order to turn off signing, you will need to be logged into the console as an administrator user. Logout of the wsaudit session and login as wsdemo.
  - \_\_\_\_e. Return to the Security auditing page and click Audit record signing configuration.
  - \_\_\_\_ f. Uncheck Enable signing and click OK.

\_\_\_\_ g. Save the change.

- \_\_\_\_\_3. Restart the application server to have these changes take effect.
- 4. Open the **BinaryAudit.log** in a text editor. Notice that the entries have additional information in them.
- 5. Next, using wsadmin, generate an html report using the same process as before, but enter **complete** for the **reportMode** and **C:\completeAuditReport.**html for the **outputLocation**.
- \_\_\_\_6. Open the new audit report and notice that it also has more information than was available with the basic reportMode.

st00 . ReportTime Jul 2, 2008, 00:45:06       Outcome       ESOURCE_ACCESS       SUCCESS       oke MBean       ProgName=Server (module)
ESOURCE_ACCESS SUCCESS bke MBean ProgName=Server (module)
ke MBean ProgName=Server (module)
о ( ,
I Realm=defaultWIMFileBasedRealm
ull RemoteHost=null
=SM_MBEAN ResourceUniqueId=0
17888643 GlobalInstanceId=0
ProviderStatus=null
=null MappedUserName=null
II IdentityName=null
TerminateReason=null
null PolicyType=null
ranted=null RolesChecked=N/A
II MgmtCommand=null
ueld=null Url=N/A
ESOURCE_ACCESS SUCCESS
oke MBean ProgName=Server (module)
I Realm=defaultWIMFileBasedRealm
ull RemoteHost=null
=SM_MBEAN ResourceUniqueId=0
17888643 GlobalInstanceId=0
ProviderStatus=null
=null MappedUserName=null
II IdentityName=null
TerminateReason=null
null PolicyType=null
ranted=null RolesChecked=N/A
II MgmtCommand=null
ueld=null Url=N/A

# What you did in this exercise

In this lab you learned how to enable security auditing for WebSphere Application Server Network Deployment V7. You created an auditor user, configured and enabled auditing, and viewed the text based log files and the generated html report. In the optional parts of this exercise, you created a new event filter, digitally signed the audit log entries and the encrypted them. Finally, you switched the auditing level to verbose and generated a "complete" audit report. This page is left intentionally blank.