IBM Security Verify Access
Version 10.0.0
June 2020

Advanced Access Control Auditing

Contents

Tables... v

Chapter 1. Advanced Access Control auditing events.. 1

Chapter 2. IBM_SECURITY_AUTHN_events... 5

Chapter 3. IBM_SECURITY_TRUST events... 9

Chapter 4. IBM_SECURITY_RUNTIME events... 13

Chapter 5. IBM_SECURITY_CBA_AUDIT_MGMT events...................................... 15

Chapter 6. IBM_SECURITY_CBA_AUDIT_RTE events.. 21

Chapter 7. IBM_SECURITY_RTSS_AUDIT_AUTHZ events.................................... 23

Chapter 8. Deploying pending changes... 29

Index... 31

Tables

1. Attributes and elements of the ContextDataElements element......1

2. Attributes for the SourceComponentId element......2

3. Attributes for the Situation element...... 3

4. Attributes for the Outcome element......4

5. Elements for an IBM_SECURITY_AUTHN event...... 5

6. Elements for an IBM_SECURITY_TRUST event......9

7. Elements for an IBM_SECURITY_RUNTIME event...... 13

8. Elements used in IBM_ SECURITY_CBA_AUDIT_MGMT events......15

9. Elements used in IBM_SECURITY_CBA_AUDIT_RTE events......21

10. Properties used in IBM_SECURITY_RTSS_AUDIT_AUTHZ events......23

Chapter 1. Advanced Access Control auditing events

This section lists the audit elements that are available for each audit event type.

Use the instructions in Configuring auditing on the appliance to configure auditing on the appliance.

Advanced Access Control supports the following auditing events:

- IBM_SECURITY_TRUST
- IBM_SECURITY_RUNTIME
- IBM_SECURITY_CBA_AUDIT_MGMT
- IBM_SECURITY_CBA_AUDIT_RTE
- IBM_SECURITY_RTSS_AUDIT_AUTHZ

This section describes the available elements for each event type.

Common elements for all events

The following elements are included with all security events:

- ContextDataElements
- SourceComponentIdelements
- Situation
- Outcome

ContextDataElements

The contextId value, which is specified on the type attribute, is included in the ContextDataElements element to correlate all events that are associated with a single transaction.

Table 1. Attributes and elements of the ContextDataElements element

Attribute	**Value**
name	Security Event Factory The XPath is: `CommonBaseEvent/contextDataElements/@name`
type	eventTrailId The XPath is: `CommonBaseEvent/contextDataElements/@type`
contextId	This element is a container element for the eventTrailId value; it does not have an XPath value.
eventTrailId	The event trail identifier value, for example, FIM_116320b90110104ab7ce9df3453615a1+729829786 The XPath is: `CommonBaseEvent/contextDataElements/[@type='eventTrailId']/contextId`

The following are XML-formatted examples of CBE event headers containing entries for the ContextDataElements element. These entries illustrate how separate events are correlated for a single transaction.

```
<CommonBaseEvent
    creationTime="2007-01-31T20:59:57.625Z"
    extensionName="IBM_SECURITY_TRUST"
    globalInstanceId="CE4454A122E10AB044A1DBB16E020E1D80"
    sequenceNumber="1" version="1.0.1">
    <contextDataElements name="Security Event Factory"     type="eventTrailId">
        <contextId>FIM_79f4e4c801101db5aba48cd8e0212be7+656317861</contextId>
    </contextDataElements>
...
</CommonBaseEvent>
```

```
<CommonBaseEvent
    creationTime="2007-01-31T20:59:57.765Z"
    extensionName="IBM_SECURITY_TRUST"
    globalInstanceId="CE4454A122E10AB044A1DBB16E02213050"
    sequenceNumber="2" version="1.0.1">
    <contextDataElements name="Security Event Factory" type="eventTrailId">
        <contextId>FIM_79f4e4c801101db5aba48cd8e0212be7+656317861</contextId>
    </contextDataElements>
...
</CommonBaseEvent>
```

SourceComponentId element

The SourceComponentId is an identifier that represents the source that generates the event.

Table 2. Attributes for the SourceComponentId element

Attribute	Value
application	IBM® Security Verify Access The XPath is: `CommonBaseEvent/sourceComponentId/@application`
component	The XPath is: `CommonBaseEvent/sourceComponentId/@component`
componentIdType	ProductName The XPath is: `CommonBaseEvent/sourceComponentId/@componentIdType`
componentType	http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes The XPath is: `CommonBaseEvent/sourceComponentId/@componentType`
executionEnvironment	<OS name>#<OS Architecture>#<OS.version> The XPath is: `CommonBaseEvent/sourceComponentId/@executionEnvironment`

Table 2. Attributes for the SourceComponentId element (continued)

Attribute	Value

location	<hostname>
	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='registryInfo']/children`
	`[@name='location']/values`

locationType	FQHostname
	The XPath is:
	`CommonBaseEvent/sourceComponentId/`
	`@locationType`

subComponent	<classname>
	The XPath is:
	`CommonBaseEvent/sourceComponentId/`
	`@subComponent`

Situation element
The Situation element describes the circumstance that caused the audit event.

Table 3. Attributes for the Situation element

Attribute	Value

categoryName	ReportSituation
	The XPath is:
	`CommonBaseEvent/situation/`
	`@categoryName`

reasoningScope	INTERNAL
	The XPath is:
	`CommonBaseEvent/situation/situationType/`
	`@reasoningScope`

reportCategory	SECURITY
	The XPath is:
	`CommonBaseEvent/situation/situationType/`
	`@reportCategory`

Outcome element
The Outcome element is the result of the action for which the security event is being generated.

Table 4. Attributes for the Outcome element

Attribute	Value

failureReason	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='outcome']/children`
	`[@name='failureReason']/values`

majorStatus	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='outcome']/children`
	`[@name='majorStatus']/values`

result	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='outcome']/children`
	`[@name='result']/values`

Note: Advanced Access Control does not use the **ReporterComponentId** field.

Chapter 2. IBM_SECURITY_AUTHN_events

This event type is generated by the authentication service when it authenticates a user accessing a protected resource.

The following table lists the elements that can be shown in the output of an IBM_SECURITY_AUTHN event. All elements are included in the output, unless indicated otherwise.

Table 5. Elements for an IBM_SECURITY_AUTHN event

Element	**Description**
action	Optionally specifies the HTTP method on the requested resource or the operation that is performed by the provider of the authentication service. The XPath is: `CommonBaseEvent/extendedDataElements [@name='action']/values`

authnProvider	The provider of the authentication service.
	Sample data:
	`com.tivoli.am.fim.authsvc.protocol.delegate.AuthSvcDelegate`
	`com.tivoli.am.fim.authsvc.action.authenticator.hotp.HOTPAuthnticator`
	The XPath is:
	`CommonBaseEvent/extendedDataElements [@name='authnProvider']/values`

authnScope	Optionally specifies the transaction identifier of the authentication policy. Sample data: `94434b2a-748e-42fe-af3d-67db04aa4ba0` The XPath is: `CommonBaseEvent/extendedDataElements [@name='authnScope']/values`

authnType	The URI identifier of the authentication policy.
	Sample data:
	`urn:ibm:security:authentication:asf:password_hotp`
	The XPath is:
	`CommonBaseEvent/extendedDataElements [@name='authnType']/values`

partner	The authentication service does not utilize this element and will appear in the IBM_SECURITY_AUTHN event as ‘`Not Available`’. The XPath is: `CommonBaseEvent/extendedDataElements [@name='partner']/values`

Table 5. Elements for an IBM_SECURITY_AUTHN event (continued)

Element	**Description**

progName	Optionally specifies the URL of the requested resource.
	Sample data: `http://www.example.com`
	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='progName']/values`

tokenType	The authentication service does not utilize this element and will appear in the IBM_SECURITY_AUTHN event as ‘`Not Available`’.
	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='tokenType']/values`

trustRelationship	The authentication service does not utilize this element and will appear in the IBM_SECURITY_AUTHN event as '`Not Available`’.
	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='trustRelationship']/values`

userInfo.appUserName	Optionally specifies information about the user who is authenticating.
	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='userInfoList']/children[1]/children`
	`[@name='appUserName']/values`

userInfo.attributes	Optionally specifies the following types of additional information about user data that are audited during authentication:
	`licenseFileMetadata`
	Metadata that is defined in the license agreement.
	`licenseFileName`
	The license file name.
	`userAction`
	The action that the user takes when the End-User License Agreement authentication mechanism presents the license agreement. The user can accept the license agreement or decline the license agreement.
	The XPath is:
	` CommonBaseEvent/extendedDataElements`
	`[@name='userInfoList']/children [@name='userInfo']`
	`/children [@name='attributes']/children`

xmlTokenType	The authentication service does not utilize this element and will appear in the IBM_SECURITY_AUTHN event as ‘`Not Available`’.
	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='xmlTokenType']/values`

Sample of an IBM_SECURITY_AUTHN event

The following example shows one event generated by the runtime for a two-factor authentication policy requiring both username password and one-time password authentications:

```
<CommonBaseEvent
  creationTime="2014-02-15T18:50:05.026Z"
  extensionName="IBM_SECURITY_AUTHN"
  globalInstanceId="FIM36e24f6301441708947ceef443526"
  sequenceNumber="2"
  version="1.1">
  <contextDataElements
    name="Security Event Factory"
    type="eventTrailId">
        <contextId>FIM_36e24f62014415f59913eef443526e68+1246005647</contextId>
  </contextDataElements>
  <extendedDataElements name="userInfoList" type="noValue">
   <children name="userInfo" type="noValue">
     <children name="registryUserName" type="string">
       <values>Not Available</values>
     </children>
     <children name="appUserName" type="string">
       <values>test_user</values>
     </children>
   </children>
 </extendedDataElements>
 <extendedDataElements name="tokenType" type="string">
   <values>Not Available</values>
 </extendedDataElements>
 <extendedDataElements name="authnProvider" type="string">
   <values>com.tivoli.am.fim.authsvc.action.authenticator.hotp.HOTPAuthenticator</values>
 </extendedDataElements>
 <extendedDataElements name="action" type="string">
      <values>verify</values>
 </extendedDataElements>
 <extendedDataElements name="authnType" type="string">
      <values>urn:ibm:security:authentication:asf:password_hotp</values>
 </extendedDataElements>
 <extendedDataElements name="outcome" type="noValue">
      <children name="result" type="string">
        <values>SUCCESSFUL</values>
      </children>
      <children name="majorStatus" type="int">
        <values>0</values>
      </children>
 </extendedDataElements>
 <extendedDataElements name="trustRelationship" type="string">
      <values>Not Available</values>
 </extendedDataElements>
 <extendedDataElements name="progName" type="string">
      <values>Not Available</values>
 </extendedDataElements>
 <extendedDataElements name="authnScope" type="string">
      <values>Not Available</values>
 </extendedDataElements>
 <sourceComponentId
      application="IBM Security Verify Access"
      component="Authentication and Federated Identity"
      componentIdType="ProductName"
      executionEnvironment="Linux[amd64]#2.6.32-279.14.1.30.iss7_3.x86_64"
      location="example"
      locationType="FQHostname"
      subComponent="com.tivoli.am.fim.authsvc.action.authenticator.hotp.HOTPAuthenticator"
      threadId="Default Executor-thread-60"
      componentType="http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes"/>
  <situation categoryName="ReportSituation">
     <situationType
       xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
       xsi:type="ReportSituation"
       reasoningScope="INTERNAL"
       reportCategory="SECURITY"/>
  </situation>
</CommonBaseEvent>
```

Chapter 3. IBM_SECURITY_TRUST events

This event type is generated by the trust server when it validates a token, issues a token, maps an identity, or authorizes a Web service call.

The following table lists the elements that can be shown in the output of an IBM_SECURITY_TRUST event.

Table 6. Elements for an IBM_SECURITY_TRUST event

Element	**Description**

accessDecision	For the authorization module, it is the result of the authorization decision. This element is filled out only when the action is authorized.
	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='accessDecision']/values`

action	The action being performed. Possible actions are:
	• authorize
	• issue
	• map
	• validate
	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='action']/values`

appliesTo	The destination or resource that the request or token applies to.
	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='appliesTo']/values`

issuer	The party responsible for issuing the token.
	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='issuer']/values`

moduleName	The module in the STS module chain that the action is taken on.
	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='moduleName']/values`

ruleName	The rule name used for the mapping module. This element is filled out only when specified action is set to *map*.
	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='ruleName']/values`

Table 6. Elements for an IBM_SECURITY_TRUST event (continued)

Element	Description
token	The incoming token that the action is being taken on. Only the first 1024 characters of the token are set. When the action is set to *map*, this element represents the incoming principal. The XPath is: `CommonBaseEvent/extendedDataElements [@name='token']/values`
tokenInfo	The internal representation of the user information *after* changes are made by the module. Only the first 1024 characters of the token are set. When action is set to *map*, this element represents the outgoing principal. When the action is set to *authorize*, this element represents the principal for whom the access decision was made. The XPath is: `CommonBaseEvent/extendedDataElements [@name='tokenInfo']/values`
tokenType	The type of token the module is using. The XPath is: `CommonBaseEvent/extendedDataElements [@name='tokenType']/values`

Samples of IBM_SECURITY_TRUST events

The following example shows an event generated by a Trust request.

```
<CommonBaseEvent creationTime="2013-07-19T06:21:05.256Z"
extensionName="IBM_SECURITY_TRUST"
globalInstanceId="FIMf596c16e013f12d38eb0b66d4d925"
sequenceNumber="1" version="1.1">
    <contextDataElements name="Security Event Factory"
type="eventTrailId">
        <contextId>FIM_f596bda0013f188f9983b66d4d92542a+971185751</contextId>
    </contextDataElements>
    <extendedDataElements name="tokenType" type="string">
        <values>Not Available</values>
    </extendedDataElements>
    <extendedDataElements name="issuer" type="string">
        <values>/otpfed/otp/get/delivery/options/issuer</values>
    </extendedDataElements>
    <extendedDataElements name="token" type="string">
        <values>user1 [ Attribute 1 name   [ value 1 user1 ] ]</values>
    </extendedDataElements>
    <extendedDataElements name="ruleName" type="string">
        <values>otp_get_methods.js </values>
    </extendedDataElements>
    <extendedDataElements name="moduleName" type="string">
        <values>com.tivoli.am.fim.trustserver.sts.modules.STSMapDefault</values>
    </extendedDataElements>
    <extendedDataElements name="appliesTo" type="string">
        <values>/otpfed/otp/get/delivery/options/appliesto</values>
    </extendedDataElements>
    <extendedDataElements name="action" type="string">
        <values>Map</values>
    </extendedDataElements>
    <extendedDataElements name="tokenInfo" type="string">
        <values>user1 [ Attribute 1 name   [ value 1 user1 ] ]</values>
    </extendedDataElements>
    <extendedDataElements name="outcome" type="noValue">
        <children name="result" type="string">
            <values>SUCCESSFUL</values>
        </children>
        <children name="majorStatus" type="int">
            <values>0</values>
        </children>
    </extendedDataElements>
    <sourceComponentId application="IBM Security Verify Access"
component="Authentication and Federated Identity"
componentIdType="ProductName"
executionEnvironment="Linux[amd64]#2.6.32-279.14.1.30.iss7_3.x86_64"
location="localhost" locationType="FQHostname"
subComponent="com.tivoli.am.fim.trustserver.sts.modules.STSMapDefault"
threadId="Default Executor-thread-6"
componentType="http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes"/>
    <situation categoryName="ReportSituation">
        <situationType xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="ReportSituation" reasoningScope="INTERNAL" reportCategory="SECURITY"/>
    </situation>
</CommonBaseEvent>
```

Chapter 4. IBM_SECURITY_RUNTIME events

This event type is generated when the runtime is started.

The following table lists the elements that can be shown in the output of an IBM_SECURITY_RUNTIME event.

Table 7. Elements for an IBM_SECURITY_RUNTIME event

Element	Description

Domain	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='Domain']/values`

IsMgmtAudit	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='IsMgmtAudit']/values`

nameInApp	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='resourceInfo']/children`
	`[@name='nameInApp']/values`

nameInPolicy	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='resourceInfo']/children`
	`[@name='nameInPolicy']/values`

type	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='resourceInfo']/children`
	`[@name='type']/values`

uniqueID	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='resourceInfo']/children`
	`[@name='uniqueID']/values`

action	The XPath is:
	`CommonBaseEvent/extendedDataElements`
	`[@name='action']/values`

Samples of IBM_SECURITY_RUNTIME events

The following example shows an events generated by a runtime request.

```
<CommonBaseEvent
creationTime="2013-07-19T06:20:18.361Z"
extensionName="IBM_SECURITY_RUNTIME"
globalInstanceId="FIMf5960a71013f15479e82b66d4d925"
sequenceNumber="0"
version="1.1">
```

```
    <contextDataElements name="Security Event Factory"
type="eventTrailId">
        <contextId>FIM_f5960938013f1eba8b40b66d4d92542a+1655973824</contextId>
    </contextDataElements>
    <extendedDataElements name="Domain" type="string">
        <values>Not Available</values>
    </extendedDataElements>
    <extendedDataElements name="IsMgmtAudit" type="boolean">
        <values>false</values>
    </extendedDataElements>
    <extendedDataElements name="resourceInfo" type="noValue">
        <children name="nameInApp" type="string">
            <values/>
        </children>
        <children name="nameInPolicy" type="string">
            <values/>
        </children>
        <children name="type" type="string">
            <values>application</values>
        </children>
        <children name="uniqueId" type="long">
            <values>0</values>
        </children>
    </extendedDataElements>
    <extendedDataElements name="action" type="string">
        <values>auditStart</values>
    </extendedDataElements>
    <extendedDataElements name="outcome" type="noValue">
        <children name="result" type="string">
            <values>SUCCESSFUL</values>
        </children>
        <children name="majorStatus" type="int">
            <values>0</values>
        </children>
    </extendedDataElements>
    <sourceComponentId application="IBM Security Verify Access"
component="Authentication and Federated Identity"
componentIdType="ProductName"
executionEnvironment="Linux[amd64]#2.6.32-279.14.1.30.iss7_3.x86_64"
location="localhost" locationType="FQHostname"
subComponent="com.tivoli.am.fim.audit.event.impl.RuntimeAuditAdapterImpl"
threadId="Start Level Event Dispatcher"
componentType="http://www.ibm.com/namespaces/autonomic/Tivoli_componentTypes"/>
    <situation categoryName="ReportSituation">
        <situationType xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xsi:type="ReportSituation" reasoningScope="INTERNAL" reportCategory="SECURITY"/>
    </situation>
</CommonBaseEvent>
```

Chapter 5. IBM_SECURITY_CBA_AUDIT_MGMT events

This event type identifies the security context-based management events, such as the creation of risk profiles.

The following table lists the elements that can be displayed in the output of a `IBM_SECURITY_CBA_AUDIT_MGMT` event. All elements are included in the output, unless indicated otherwise.

Table 8. Elements used in IBM_ SECURITY_CBA_AUDIT_MGMT events

Element	**Description**
creationTime	Specifies the date and time when the event was issued. For example: `2013-09-11T19:18:04.140Z` The letter Z in the sample that is shown indicates the UTC format. All time stamps are issued in UTC format. There is no provision for specifying local time. This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type.
actionInfo	Provides information about the management action that is performed on a resource. This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type.

Table 8. Elements used in IBM_ SECURITY_CBA_AUDIT_MGMT events (continued)

Element	Description
actionInfo action-id	Specifies the action that caused this management event. Possible actions include: ***API protection client related events*** API_PROTECTION_CLIENT_CREATE_EVENT, API_PROTECTION_CLIENT_DELETE_EVENT, API_PROTECTION_CLIENT_SEARCH_EVENT, API_PROTECTION_CLIENT_SECRET_GENERATE_EVENT, API_PROTECTION_CLIENT_UPDATE_EVENT ***API protection definition related events*** API_PROTECTION_DEFINITION_CREATE_EVENT, API_PROTECTION_DEFINITION_DELETE_EVENT, API_PROTECTION_DEFINITION_SEARCH_EVENT, API_PROTECTION_DEFINITION_UPDATE_EVENT ***Attribute matcher related events*** ATTRIBUTE_MATCHER_CREATE_EVENT, ATTRIBUTE_MATCHER_DELETE_EVENT, ATTRIBUTE_MATCHER_SEARCH_EVENT, ATTRIBUTE_MATCHER_UPDATE_EVENT ***Attribute related events*** ATTRIBUTE_CREATE_EVENT, ATTRIBUTE_DELETE_EVENT, ATTRIBUTE_SEARCH_EVENT, ATTRIBUTE_UPDATE_EVENT ***Audit related events*** AUDIT_SEARCH_EVENT, AUDIT_UPDATE_EVENT ***Authentication mechanism instances related events*** AUTH_MECH_INSTANCE_UPDATE_EVENT, AUTH_MECH_INSTANCE_SEARCH_EVENT ***Authentication mechanism types related events*** AUTH_MECH_TYPE_SEARCH_EVENT ***Authentication policy related events*** AUTH_POLICY_CREATE_EVENT, AUTH_POLICY_UPDATE_EVENT, AUTH_POLICY_DELETE_EVENT, AUTH_POLICY_SEARCH_EVENT ***Bundle related events*** BUNDLE_SEARCH_EVENT, BUNDLE_CREATE_EVENT, BUNDLE_UPDATE_EVENT, BUNDLE_DELETE_EVENT, BUNDLE_EXPORT_EVENT, BUNDLE_IMPORT_EVENT ***Device related events*** DEVICE_DELETE_EVENT, DEVICE_SEARCH_EVENT, DEVICES_FOR_USER_SEARCH_EVENT, DEVICE_USER_ID_SEARCH_EVENT ***Extension instances related events*** EXTENSION_INSTANCE_SEARCH_EVENT, EXTENSION_INSTANCE_CREATE_EVENT, EXTENSION_INSTANCE_UPDATE_EVENT, EXTENSION_INSTANCE_DELETE_EVENT ***Extension related events*** EXTENSION_SEARCH_EVENT ***Geolocation data related events*** GEOLOCATION_DATA_CANCEL_IMPORT_EVENT, GEOLOCATION_DATA_IMPORT_EVENT, GEOLOCATION_DATA_STATUS_IMPORT_EVENT ***HVDB related events*** HVDB_DELETE_ALL_DATA_EVENT, HVDB_DELETE_USER_DATA_EVENT, HVDB_CANCEL_DELETE_DATA_EVENT, HVDB_DELETE_DEVICES_EVENT, HVDB_STATUS_DELETE_DATA_EVENT, HVDB_DELETE_USER_FROM_DB ***Mapping rule related events*** MAPPING_RULE_EXPORT_EVENT, MAPPING_RULE_IMPORT_EVENT , MAPPING_RULE_SEARCH_EVENT, MAPPING_RULE_UPDATE_EVENT, MAPPING_RULE_CREATE_EVENT, MAPPING_RULE_DELETE_EVENT ***Obligation related events*** OBLIGATION_CREATE_EVENT, OBLIGATION_DELETE_EVENT, OBLIGATION_SEARCH_EVENT, OBLIGATION_UPDATE_EVENT

Table 8. Elements used in IBM_ SECURITY_CBA_AUDIT_MGMT events (continued)

Element	Description
outcome	Specifies the outcome of the action for which the security event is generated. This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type
outcome failureReason	Provides more information about the outcome. This element is included in the output when the result is FAILURE. XPath: `CommonBaseEvent/extendedDataElements /[@name=’outcome’]/children[@name=’failureReason’ ]/values`
outcome result	Specifies the overall status of the event that is commonly used for filtering. The following values are possible for the status of this element: • `FAILURE` • `SUCCESSFUL` XPath: `CommonBaseEvent/extendedDataElements /[@name=’outcome’]/children[@name=’result’]/values`
userInfoList	Provides information about the user who accesses the resource. This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type.
userInfoList appUserName	Specifies the name of the user. XPath: `CommonBaseEvent/extendedDataElements /[@name=’userInfoList’]/children[@name=’appUserName’]/values`
resourceInfo	Provides information about the resource that is accessed. This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type.
resourceInfo RESTInvocationURI	Specifies the URI of the REST interface that is accessed for this management event. XPath: `CommonBaseEvent/extendedDataElements /[@name=’resourceInfo’]/children[@name=’RESTInvocationURI’]/values`
resourceInfo nameOfPolicy	Specifies the policies and policy sets that are associated with the policy attachment for the resource as specified by the nameOfResource property. This element is included in the output for policy attachment action-ids. XPath: `CommonBaseEvent/extendedDataElements /[@name=’resourceInfo’]/children[@name=’nameOfPolicy’]/values`
resourceInfo nameOfResource	Specifies the name of the resource for a policy attachment. For example: `/WebSEAL/security-default/index.html` This element is included in the output for policy attachment action-ids. XPath: `CommonBaseEvent/extendedDataElements /[@name=’resourceInfo’]/children[@name=’nameOfResource’]/values`

Table 8. Elements used in IBM_ SECURITY_CBA_AUDIT_MGMT events (continued)

Element	Description
restManagement	Provides optional information regarding the input JSON for this management request. This element is included in the output for some management audit events. This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type.
restManagement json	JSON for this management request. This element is included in the output for some management audit events. **Note:** To enable the inclusion of additional data in an audit event, the administrator must select **Enable verbose audit events** in the **Audit Configuration** panel. XPath: `CommonBaseEvent/extendedDataElements / [@name='restManagement']/children[@name='json']/values`
extensionName	Specifies the name of the event class that this event represents. The name indicates any additional elements that are expected to be present within the event. The value for context-based authorization management events is *IBM_SECURITY_CBA_AUDIT_MGMT*. This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type.
globalInstanceId	Specifies the primary identifier for the event. This property must be globally unique and can be used as the primary key for the event. For example: `f0c93637-ada2-4afb-9687-47a7ec1fa3a7` This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type.
msg	Specifies more information when the outcome is `SUCCESSFUL`. This element: • Is optional. • Is a container element. • Does not have a valid XPath. A valid XPath requires a `values` declaration. • Uses the children of the ComponentIdentification element type.
reporterComponentId	This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type.
reporterComponentId application	Specifies the name of the application that reports the event. For context-based authorization events, the value is set to *IBM Security Verify Access*.
reporterComponentId component	Specifies the logical identity of a component. For context-based authorization events, the value is set to *Context-Based Authorization*.
reporterComponentId componentIdType	Specifies the format and meaning of the component that is identified by this component identification. For example: *ProductName*

Table 8. Elements used in IBM_ SECURITY_CBA_AUDIT_MGMT events (continued)

Element	**Description**
reporterComponentId location	Specifies the physical address that corresponds to the location of a component. For example: *host name*, *IP address*, or *MAC address*.
reporterComponentId locationType	Specifies the format and meaning of the value in the location property. For context-based authorization events, the value is set to *FQHostname*.
sourceComponentId	Identifies the component that is affected or was impacted by the event. This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type.
sourceComponentId component	Specifies the logical identity of a component.
sourceComponentId componentIdType	Specifies the format and meaning of the component that is identified by this component identification. For example: *ProductName*
sourceComponentId location	Specifies the physical address that corresponds to the location of a component. For example: *host name*, *IP address*, or *MAC address*.
sourceComponentId locationType	Specifies the format and meaning of the value in the location property. For context-based authorization events, the value is set to *FQHostname*.

Chapter 6. IBM_SECURITY_CBA_AUDIT_RTE events

This event type identifies the security context-based authorization events, such as device registration.

The following table lists the elements that can be shown in the output of an IBM_SECURITY_CBA_AUDIT_RTE event. All elements are included in the output, unless indicated otherwise.

Table 9. Elements used in IBM_SECURITY_CBA_AUDIT_RTE events

Element	Description
creationTime	Specifies the date and time when the event was issued. For example: 2013-09-11T19:18:04.140Z The letter Z in the sample that is shown indicates the UTC format. All time stamps are issued in UTC format. There is no provision for specifying local time. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.
actionInfo	Provides information about the management action that is performed on a resource. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type.
actionInfo action-id	Specifies the action that caused this event. Possible actions include: • CALCULATE_RISK_SCORE_EVENT • DEVICE_DELETION_EVENT • DEVICE_REGISTRATION_EVENT • JAVASCRIPT_EVENT XPath: CommonBaseEvent/extendedDataElements /[@name= ’ actionInfo’]/children[@name=’ urn:oasis:names:tc:xacml:1.0:action:action-id’]/ values
outcome	Specifies the outcome of the action for which the security event is generated. This element is a container element and has no valid XPath. A valid XPath requires a values declaration. This container element uses the children of the ComponentIdentification element type
outcome failureReason	Provides additional information about the outcome. Included in the output when the result is FAILURE. XPath: CommonBaseEvent/extendedDataElements / [@name=’outcome’]/children[@name=’failureReason’]/ values

Table 9. Elements used in IBM_SECURITY_CBA_AUDIT_RTE events (continued)

Element	**Description**
outcome result	Specifies the overall status of the event that is commonly used for filtering. The following values are possible for the status: • `FAILURE` • `SUCCESSFUL` XPath: `CommonBaseEvent/extendedDataElements / [@name='outcome']/children[@name='result']/values`
userInfoList	Provides information about the user who accesses the resource. This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type.
userInfoList appUserName	Specifies the name of the user. XPath: `CommonBaseEvent/extendedDataElements / [@name='userInfoList']/children[@name='appUserName']/ values`
extensionName	Specifies the name of the event class that this event represents. The name indicates any additional elements that are expected to be present within the event. The value for context-based authorization runtime events is *IBM_SECURITY_CBA_AUDIT_RTE*. This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type.
globalInstanceId	Specifies the primary identifier for the event. This property must be globally unique and can be used as the primary key for the event. For example: `f0c93637-ada2-4afb-9687-47a7ec1fa3a7` This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type.
msg	Specifies additional information when the outcome is `SUCCESSFUL`. This element is a container element and has no valid XPath. A valid XPath requires a `values` declaration. This container element uses the children of the ComponentIdentification element type.

Chapter 7. IBM_SECURITY_RTSS_AUDIT_AUTHZ events

This event type identifies the authorization decision events for runtime security services.

Runtime security services generates an authorization decision event record if both of the following conditions occur:

- The runtime security services component is asked for an access decision
- Auditing is enabled

In addition to the base Common Base Event content, runtime security services authorization decision records contain authorization-specific properties. These authorization-specific properties are defined in the Common Base Event Extensions for Security Events specification with the ExtendedDataElement.

The following table lists the event properties that are included in the output of an IBM_SECURITY_RTSS_AUDIT_AUTHZ event record. All elements are included in the output, unless indicated otherwise.

Table 10. Properties used in IBM_SECURITY_RTSS_AUDIT_AUTHZ events

Element	**Description and values**
accessDecision	Present when the result is SUCCESSFUL This property specifies the decision of the authorization call. Possible element values include: • `Permit` • `Deny` • `NotApplicable` • `Indeterminate` If a `Permit` decision is returned with obligations, then a ConditionalPermit decision is recorded in the event.
accessDecisionReason	Present when accessDecision is DENY This property provides more information about the denial of the access decision.
action	Not always in output. This property specifies the action that caused the authorization event.
outcome	Specifies the outcome of the action for which the security event is being generated. This ExtendedDataElement element does not have a value declaration. This container element uses the children of the outcomeType element type.
outcome failureReason	Not always in output. This property provides more information about the outcome.
outcome majorStatus	Specifies the major status code.
outcome minorStatus	Not always in output. This property specifies the minor status code.

Table 10. Properties used in IBM_SECURITY_RTSS_AUDIT_AUTHZ events (continued)

Element	Description and values
outcome result	Specifies the overall status of the event. This element is also used for filtering. Element values are UNSUCCESSFUL if an error condition occurs that prevents standard processing. Element values are SUCCESSFUL when the error condition starts standard processing.
permissionInfo	Provides information about access permissions. This ExtendedDataElement element has no value declaration. This container element uses the children of the PermissionInfoType element type.
permissionInfo checked	Specifies permissions that are checked during the authorization call.
permissionInfo denied	Not always in output. This property specifies the permissions that are denied among the permissions that are requested.
permissionInfo granted	Not always in output. This property specifies permissions that are granted.
policyInfo	Not always in output. This property provides information about policies that are attached to the resource or the container of a resource. This ExtendedDataElement element does not have a value declaration. This container element uses the children of the PolicyInfoType element type.
policyInfo attributes	Not always in output. This property specifies attributes that are associated with a policy.
policyInfo description	Not always in output. This property provides a description of the policy.
policyInfoname	Not always in output. This property specifies the name of the policy.
policyInfo type	Not always in output. This property specifies the type of the policy.
registryInfo	Not always in output. This property provides information about the registry that is involved in the authentication. This ExtendedDataElement element does not have a value declaration. This container element uses the children of the RegistryInfoType element type.
registryInfo serverLocation	Not always in output. This property specifies where the registry server is located.
resourceInfo	Provides information about the resource that is accessed. This ExtendedDataElement element has no a value declaration. This container element uses the children of the resourceInfoType element type.

Table 10. Properties used in IBM_SECURITY_RTSS_AUDIT_AUTHZ events (continued)

Element	**Description and values**
resourceInfo attributes	Specifies the attributes for the resource.
resourceInfo nameInApp	Not always in output. This property specifies the name of the resource in the context of the application.
resourceInfo nameInPolicy	Specifies the name of the resource when it applies a policy to the resource.
resourceInfo type	Specifies the type of the resource.
userInfo	Provides information about each user in the delegation chain. This ExtendedDataElement element has no a value declaration. This container element uses the children of the UserInfoType element type.
userInfo appUserName	Present when the accessing subject is authenticated. This property specifies the name of a user within an application.
userInfo attributes	Not always in output. This property provides more user information.
userInfo callerList	Not always in output. This property specifies a list of names that represents the identities of a user.
userInfo location	Not always in output. This property specifies the location of the user.
userInfo locationType	Not always in output. This property specifies the type of location.
userInfo realm	Not always in output. This property specifies the registry partition to which the user belongs.
userInfo registryUserName	Not always in output. This property specifies the name of the user in the registry.
userInfo sessionId	Not always in output. This property specifies the ID for the session that belongs to the user.
userInfo uniqueId	Not always in output. This property specifies the unique identifier that belongs to the user within an application.
creationTime	Specifies the date and time when the event was issued. For example: `2008-09-11T19:18:04.140Z` The letter Z in the example indicates the UTC format. All time stamps are issued in UTC format. There is no provision for specifying local time.
contextDataElement	Specifies the ContextDataElement type, which defines the contexts that each event references. This element contains data that assists with problem diagnostic procedures by correlating messages or events that are generated during the execution of a unit of work.
contextDataElement type	Specifies the data type of the contextValue property.

Table 10. Properties used in IBM_SECURITY_RTSS_AUDIT_AUTHZ events (continued)

Element	**Description and values**
contextDataElement name	Specifies the name of the application that created the contextDataElement.
contextDataElement contextValue	Specifies the value of the context regarding the implementation of the context.
extensionName	Specifies the name of the event class that the extensionName event represents. The extensionName event indicates more elements that are expected to be present within the event. The value for runtime security services is the following value: IBM_SECURITY_RTSS_ AUDIT_AUTHZ
globalInstanceId	Specifies the primary identifier for the event. This property must be globally unique and can be used as the primary key for the event. For example:`f5e6bcc5-d1e8-4638- 8f84-3ba29ca950b2`
msg	Provides the text that accompanies the event. This element is typically the resolved message string in human readable format that is rendered for a specific locale. The following example uses runtime security services data: `Subject cn=wasadmin,c=us` requests access to the `http://localhost:9081/rtss/test/jaxws/echo/EchoService` protected resource.
situation	Specifies the situation that caused the event to be reported.
situation categoryName	Specifies the category type of the situation that caused the event to be reported.
situation situationType	Specifies the type of situation that caused the event to be reported.
situation reportCategory	Specifies the category of the reported situation. This element is used if the value that belongs to the element is STATUS.
situation reasoningScope	Defines whether this situation has either of the following impacts: • Internal-only impact. • Potential external impact. This element is used if the element value is either of the following values: • `INTERNAL` • `EXTERNAL`
sourceComponentId	Identifies the component that is impacted by the event. This element has no a value declaration. This container element uses the children of the ComponentIdType element type.
sourceComponentId application	Specifies the name of the application. The value that belongs to this element is the following: IBM runtime security services
sourceComponentId component	Specifies the logical identity of a component.

Table 10. Properties used in IBM_SECURITY_RTSS_AUDIT_AUTHZ events (continued)

Element	Description and values
sourceComponentId componentIdType	Specifies the format of the component and meaning of the component that is identified by this componentIdentification. For example: `ProductName`
sourceComponentId componentType	Specifies a well-defined name that is used to characterize all of the instances that belong to this component.
sourceComponentIdlocation	Specifies the physical address that corresponds to the location of a component. For example: Host name, IP address, or MAC address.
sourceComponentIdlocationType	Present if available. This property specifies the format and meaning of the value in the location property. For runtime security services, the value is set to `Not available` if the meaning of the location element value is not determined. The following is sample runtime security services data: `ipAddress`.
sourceComponentId processId	Not always in output. This property identifies the process ID of the running component or subcomponent that generated the event.
sourceComponentId subComponent	Not always in output. This property specifies a further distinction for the logical component property of the event.
version	Specifies a string that identifies the version of the event. The element value is `2.0`.

Chapter 8. Deploying pending changes

Some configuration and administration changes require an extra deployment step.

About this task

When you use the graphical user interface on the appliance to specify changes, some configuration and administration tasks take effect immediately. Other tasks require a deployment step to take effect. For these tasks, the appliance gives you a choice of deploying immediately or deploying later. When you must make multiple changes, you can wait until all changes are complete, and then deploy all of them at one time.

When a deployment step is required, the user interface presents a message that says that there is an undeployed change. The number of pending changes is displayed in the message, and increments for each change you make.

Note: If any of the changes require the runtime server to be restarted, the restart occurs automatically when you select **Deploy**. The runtime server will then be unavailable for a period of time until the restart completes.

Procedure

1. When you finish making configuration changes, select **Click here to review the changes or apply them to the system**.

   The **Deploy Pending Changes** window is displayed.
2. Select one of the following options:

Option	Description
Cancel	Do not deploy the changes now. Retain the undeployed configuration changes. The appliance user interface returns to the previous panel.
Roll Back	Abandon configuration changes. A message is displayed, stating that the pending changes were reverted. The appliance user interface returns to the previous panel.
Deploy	Deploy all configuration changes. When you select **Deploy**, a system message is displayed, stating that the changes were deployed. If any of the changes require the runtime server to be restarted, the restart occurs automatically when you select **Deploy**. The runtime server will then be unavailable for a period of time until the restart completes.

Index

A

audit
    events 1
audit events
    common elements 1
    IBM_SECURITY_CBA_AUDIT_RTE events 21
authorization events
    IBM_SECURITY_CBA_AUDIT_RTE events 21

C

common elements
    audit events 1

D

deploying changes 29

E

events
    IBM_SECURITY_CBA_AUDIT_RTE events 21
    IBM_SECURITY_RUNTIME 13
    IBM_SECURITY_TRUST 9

I

IBM_SECURITY_AUTHN events 5
IBM_SECURITY_CBA_AUDIT_MGMT events 15
IBM_SECURITY_CBA_AUDIT_RTE events 21
IBM_SECURITY_RTSS_AUDIT_AUTHZ events 23
IBM_SECURITY_RUNTIME
    description 13
IBM_SECURITY_TRUST
    description 9

P

pending changes 29

S

security runtime
    events 13
security trust
    events 9

IBM®