Service Auditing Behavior

.NET Framework 4.5 Este tópico ainda não foi avaliado como

This sample demonstrates how to use the ServiceSecurityAuditBehavior to enable auditing of security events during service operations. This sample is based on the Getting Started Sample. The service and client have been configured using the wsHttpBinding Element. The **mode** attribute of the Security element has been set to **Message** and **clientCredentialType** has been set to **Windows**. In this sample, the client is a console application (.exe) and the service is hosted by Internet Information Services (IIS).

Note:

The setup procedure and build instructions for this sample are located at the end of this topic.

The service configuration file uses the **serviceSecurityAudit** element to configure auditing.

```
<behaviors>
  <serviceBehaviors>
    <behavior name="CalculatorServiceBehavior">
      ...
<!-- serviceSecurityAudit allows specification of audit location      and whether t
     <serviceSecurityAudit auditLogLocation ="Default" messageAuthenticationAuditLe
    </behavior>
  </serviceBehaviors>
</behaviors>
```

When you run the sample, the operation requests and responses are displayed in the client console window. Press ENTER in the console window to shut down the client.

The resulting audit logs can be seen by running the Event Viewer. By default, on Windows XP the audit events can be seen in the Application Log while on Windows Server 2003 and Windows Vista, the audit events can be seen in the Security Log. On Windows Server 2008 and Windows 7, the audit events can be seen in the Applications and Services logs. The location of audit events can be specified by setting the **auditLogLocation** attribute to “Application” or “Security”. For more information, see How to: Audit Windows Communication Foundation Security Events. If the events are written in the Security Log the LocalSecurityPolicy-> Enable Object Access should be set for "Success" and "Failure".

When looking at the event log, the source of the audit events is "ServiceModel Audit 3.0.0.0". Message authentication audit records have a category of "MessageAuthentication" while service authorization audit records have a category of “ServiceAuthorization”.

Message authentication audit events cover whether the message was tampered with, whether the message has expired, and whether the client can authenticate to the service. They provide information about whether the authentication succeeded or failed along with the identity of the client, and the endpoint the message was sent to along with the action associated with the message.

Service authorization audit events cover the authorization decision made by a service authorization manager. They provide information about whether authorization succeeded or failed along with the identity of the client, the endpoint the message was sent to, the action associated with the message, and the identifier of of the client, the endpoint the message was sent to, the action associated with the message, the identifier of the authorization context that was generated from the incoming message, and the type of the authorization manager that made the access decision.

To set up, build, and run the sample

1. Ensure that you have performed the One-Time Setup Procedure for the Windows Communication Foundation Samples.

2. To build the C# or Visual Basic .NET edition of the solution, follow the instructions in Building the Windows Communication Foundation Samples.

3. To run the sample in a single- or cross-computer configuration, follow the instructions in Running the Windows Communication Foundation Samples.

See Also

Tasks

How to: Audit Windows Communication Foundation Security Events

Concepts

Auditing Security Events

Contribuições da comunidade