Erstellen sicherer ASP.NET-Anwendungen

Authentifizierung, Autorisierung und sichere Kommunikation

Auf der Orientierungsseite finden Sie einen Ausgangspunkt und eine vollständige Übersicht zum *Erstellen sicherer ASP.NET-Anwendungen*.

Zusammenfassung

Für Anwendungen ist die Fähigkeit zum Sichern der Daten, die an einen SQL Server-Datenbankserver übergeben und von diesem abgerufen werden, oftmals von ausschlaggebender Bedeutung. Mit SQL Server 2000 können Sie unter Verwendung von SSL einen verschlüsselten Kommunikationskanal einrichten. In dieser Vorgehensweise wird erläutert, wie auf dem Datenbankserver ein Zertifikat installiert wird, wie SQL Server für SSL konfiguriert wird und wie Sie sicherstellen können, dass der Kanal sicher ist.

Vorgehensweise: Verwenden von SSL zum Sichern der Kommunikation mit SQL Server 2000

Zum Sichern der Kommunikationsverbindung zwischen Clients (Direktaufrufer) und Microsoft SQL Server™ 2000 kann das SSL-Protokoll (Secure Sockets Layer) verwendet werden. Wenn Sie SQL Server für SSL konfigurieren, können sämtliche zwischen Client und Server (und umgekehrt) übertragenen Daten verschlüsselt werden, um sicherzustellen, dass die Vertraulichkeit der Daten bei der Übertragung zwischen Client und SQL Server gewahrt bleibt.

Hinweise

- Zum Zwecke der Sicherung des Datenbankverkehrs steht mit SSL eine Alternative für IPSec zur Verfügung.

  Weitere Informationen über die Verwendung von IPSec zum Sichern des Datenbankverkehrs finden Sie unter "Vorgehensweise: Verwenden von IPSec zum Sichern der Kommunikation zwischen zwei Servern" im Abschnitt "Referenz" dieses Handbuchs.
- Im Gegensatz zu IPSec sind mit SSL keine Konfigurationsänderungen erforderlich, wenn sich die IP-Adressen von Clients oder Servern ändern.
- Damit SSL funktioniert, müssen Sie auf dem Datenbankservercomputer ein Serverzertifikat installieren. Der Clientcomputer muss ebenfalls über ein Stammzertifizierungsstellenzertifikat von der gleichen Zertifizierungsstelle verfügen.
- Auf den Clients müssen die SQL Server 2000-Verbindungsbibliotheken installiert sein. Frühere Versionen oder generische Bibliotheken funktionieren nicht.
- SSL funktioniert nur für TCP/IP (das empfohlene Kommunikationsprotokoll für SQL Server) und Named Pipes.

- Sie können den Server so konfigurieren, dass die Verwendung der Verschlüsselung für alle Verbindungen erzwungen wird.
- Auf dem Client bestehen die folgenden Möglichkeiten:
  - Erzwingen der Verwendung der Verschlüsselung für alle ausgehenden Verbindungen.
  - Ermöglichen, dass Clientanwendungen anhand der Verbindungszeichenfolge auswählen, ob die Verschlüsselung für einzelne Verbindungen verwendet werden soll.

Anforderungen

Im Folgenden finden Sie eine Liste der empfohlenen Hardware und Software und eine Beschreibung der Netzwerkinfrastruktur, der Fähigkeiten und Kenntnisse sowie der Service Packs, die Sie benötigen.

- Zwei Computer mit Microsoft Windows® 2000 Server als Betriebssystem.
- SQL Server 2000 auf dem Datenbankservercomputer. Im vorliegenden Beispiel wird davon ausgegangen, dass der SQL Server-Dienst als lokaler Systemdienst ausgeführt wird. Wenn sich das Zertifikat im lokalen Computerspeicher befindet, sollte SSL ungeachtet des Kontos funktionieren, unter dem SQL ausgeführt wird.
- Microsoft Data Access Components (MDAC) 2.6 oder höher oder die SQL Server 2000-Clientverbindungsbibliotheken auf dem Clientcomputer.
- Für das vorliegende Beispiel sollte der Zugriff auf die Microsoft Zertifikatdienste unter Windows 2000 möglich sein, damit Serverauthentifizierungszertifikate erstellt werden können. Dies ist jedoch nicht zwingend erforderlich.

Zusammenfassung

Diese Vorgehensweise enthält folgende Verfahren:

1. Installieren eines Serverauthentifizierungszertifikats
2. Sicherstellen, dass das Zertifikat installiert wurde
3. Installieren des Zertifikats der ausstellenden Zertifizierungsstelle auf dem Client
4. Erzwingen, dass alle Clients SSL verwenden
5. Ermöglichen der clientseitigen Festlegung, ob SSL verwendet werden soll
6. Sicherstellen, dass die Kommunikation verschlüsselt wird

1. Installieren eines Serverauthentifizierungszertifikats

SSL setzt voraus, dass der Server über ein Serverauthentifizierungszertifikat verfügt. Dieses Zertifikat muss von einer Zertifizierungsstelle (Certificate Authority, CA) ausgestellt worden sein, die für die verbindenden Clients als vertrauenswürdig gilt.

▶ So installieren Sie ein Serverzertifikat

1. Melden Sie sich unter Verwendung eines Administratorkontos am Datenbankservercomputer an.
2. Starten Sie Internet Explorer, und navigieren Sie zu den Microsoft Zertifikatdiensten, z. B.:

   ```
   http://MyCA/certsrv
   ```

3. Klicken Sie auf **Zertifikat anfordern** und dann auf **Weiter**.
4. Klicken Sie auf **Erweiterte Anforderung** und dann auf **Weiter**.
5. Klicken Sie auf **Senden Sie ein Zertifikatsanforderungsformular an diese Zertifizierungsstelle** und dann auf **Weiter**.

6. Füllen Sie das Zertifikatsanforderungsformular aus, und machen Sie hierbei die folgenden Angaben:
   a. Geben Sie im Feld **Name** den vollqualifizierten Domänennamen des Computers ein, auf dem SQL Server ausgeführt wird. Beispiel:

      ```
      sql01.nwtraders.com
      ```

   b. Klicken Sie im Feld **Beabsichtigte Zwecke** (oder **Typ des erforderlichen Zertifikats**) auf **Serverauthentifizierungszertifikat**.
   c. Klicken Sie für den Kryptografiedienstanbieter (Cryptographic Service Provider, CSP) auf den Microsoft RSA/Schannel-Kryptografiedienstanbieter.

      Hinweis: Sie können auch Microsoft Base Cryptographic Provider, Version 1.0, und die Microsoft Enhanced Cryptographic Providers verwenden. Der Microsoft Strong Cryptographic Provider kann nicht eingesetzt werden.

   d. Aktivieren Sie das Kontrollkästchen **Lokalen Speicher verwenden**.

      Hinweis: Wählen Sie NICHT **Verstärkte Sicherheit für den privaten Schlüssel aktivieren**.

7. Klicken Sie auf **Senden**, um die Anforderung zu übermitteln.
   Wenn der Zertifikatserver automatisch Zertifikate ausstellt, können Sie das Zertifikat jetzt installieren. Andernfalls können Sie das Zertifikat erst installieren, nachdem es vom Zertifizierungsstellenadministrator ausgestellt wurde, indem Sie zu den Microsoft Zertifikatdiensten navigieren und **Auf eine ausstehende Zertifikatsanforderung überprüfen** auswählen.

2. Sicherstellen, dass das Zertifikat installiert wurde

Mit diesem Verfahren wird sichergestellt, dass das Serverzertifikat erfolgreich installiert wurde.

▶ **So stellen Sie sicher, dass das Zertifikat installiert wurde**

1. Klicken Sie auf der Taskleiste auf **Start** und dann auf **Ausführen**.
2. Geben Sie **mmc** ein, und klicken Sie auf **OK**.
3. Klicken Sie im Menü **Datei** auf **Snap-In hinzufügen/entfernen**.
4. Klicken Sie auf **Hinzufügen**.
5. Klicken Sie auf **Zertifikate** und dann auf **Hinzufügen**.
6. Klicken Sie auf **Computerkonto** und dann auf **Weiter**.
7. Vergewissern Sie sich, dass **Lokaler Computer (Computer, auf dem diese Konsole ausgeführt wird)** aktiviert ist, und klicken Sie dann auf **Fertig stellen**.
8. Klicken Sie auf **Schließen** und dann auf **OK**.
9. Erweitern Sie in der Strukturansicht im linken Fensterbereich den Knoten **Zertifikate (Lokaler Computer)**, erweitern Sie **Eigene Zertifikate**, und wählen Sie dann **Zertifikate**.
10. Vergewissern Sie sich, dass es in Verbindung mit dem im vorherigen Verfahren angegebenen vollqualifizierten Domänennamen nur exakt ein Zertifikat gibt.
    Sie können auf das Zertifikat doppelklicken, um Details hierzu anzuzeigen.

3. Installieren des Zertifikats der ausstellenden Zertifizierungsstelle auf dem Clientcomputer

Nachdem das Zertifikat installiert und der SQL Server-Dienst neu gestartet wurde, kann SQL Server SSL mit Clients die Gegebenheiten aushandeln. Clients, die SSL für die Herstellung der Verbindung zu SQL Server verwenden sollen, müssen folgende Voraussetzungen erfüllen:

- MDAC 2.6 oder die SQL Server 2000-Verbindungsbibliotheken müssen installiert sein.
- Der Aussteller des SQL Server-Zertifikats muss als vertrauenswürdig gelten.

▶ So installieren Sie das Zertifikat der ausstellenden Zertifizierungsstelle auf dem Clientcomputer

1. Melden Sie sich als Administrator am Clientcomputer an.
2. Starten Sie Internet Explorer, und navigieren Sie zu den Microsoft Zertifikatdiensten, z. B.:

   ```
   http://MyCA/certsrv
   ```

3. Klicken Sie auf **Zertifizierungsstellenzertifikat oder Zertifikatsperrliste abrufen**, und klicken Sie dann auf **Weiter**.
4. Klicken Sie auf **Diesen Zertifizierungsstellen-Zertifikatspfad installieren**, und klicken Sie dann im Bestätigungsdialogfeld zum Installieren des Stammzertifikats auf **Ja**.

4. Erzwingen, dass alle Clients SSL verwenden

Sie können den Server so konfigurieren, dass die Verwendung von SSL für alle Clients obligatorisch ist (wie im vorliegenden Verfahren erläutert). Sie können jedoch auch festlegen, dass die Clients auf Basis einzelner Verbindungen wählen können, ob SSL verwendet werden soll oder nicht (wie im nächsten Verfahren beschrieben). Die Vorteile einer Konfiguration des Servers für die obligatorische Verwendung von SSL seitens der Clients sind die folgenden:

- Die Sicherheit der gesamten Kommunikation wird garantiert.
- Alle unsicheren Verbindungen werden zurückgewiesen.

Es gibt jedoch auch Nachteile:

- Auf allen Clients muss MDAC 2.6 oder müssen die SQL Server 2000-Verbindungsbibliotheken installiert sein; mit älteren oder generischen Bibliotheken können keine Verbindungen hergestellt werden.
- Bei Verbindungen, die nicht sicher sein müssen, kommt es aufgrund der zusätzlichen Verschlüsselung zu geringfügigen Leistungseinbußen.

▶ So erzwingen Sie die Verwendung von SSL für alle Clients

1. Klicken Sie auf dem Computer, auf dem SQL Server ausgeführt wird, in der Programmgruppe **Microsoft SQL Server** auf **SQL Server-Netzwerkkonfiguration**.
2. Klicken Sie auf **Protokollverschlüsselung erzwingen**.
3. Vergewissern Sie sich, dass TCP/IP und/oder Named Pipes aktiviert ist.
   Von anderen Protokollen wird SSL nicht unterstützt.
4. Klicken Sie auf **OK**, um die SQL Server-Netzwerkkonfiguration zu schließen, und klicken Sie dann im Meldungsfenster der SQL Server-Netzwerkkonfiguration nochmals auf **OK**.
5. Starten Sie den SQL Server-Dienst neu.

   Bei allen nachfolgenden Clientverbindungen muss nun zwangsläufig SSL verwendet werden, ungeachtet dessen, ob sichere Verbindungen angegeben werden oder nicht.

5. Ermöglichen der clientseitigen Festlegung, ob SSL verwendet werden soll

In diesem Verfahren wird die SSL-Konfiguration erläutert, die es Clients ermöglicht, zu wählen, ob SSL verwendet werden soll. Sie können entweder die Clientbibliotheken so konfigurieren, dass bei allen Verbindungen SSL verwendet werden muss, oder Sie können einzelnen Anwendungen auf Basis von Einzelverbindungen die Auswahl der Verbindungsart ermöglichen. Die Vorteile der Konfiguration des Clients für die Auswahl der Verbindungsart sind die folgenden:

- Der von SSL verursachte Overhead tritt nur bei Verbindungen auf, für die SSL wirklich erforderlich ist.
- Clients, die SSL in Verbindung mit SQL Server nicht unterstützen, können dennoch die Verbindung herstellen.

Bevor Sie sich für diesen Ansatz entscheiden, sollten Sie jedoch prüfen, ob Sie unsichere Verbindungen wirklich zulassen möchten.

▶ **So nehmen Sie eine Neukonfiguration des Servers vor**

1. Führen Sie auf dem SQL Server-Computer die SQL Server-Netzwerkkonfiguration aus.
2. Deaktivieren Sie das Kontrollkästchen **Protokollverschlüsselung erzwingen**.
3. Starten Sie den SQL Server-Dienst neu.
4. Kehren Sie zum Clientcomputer zurück.

▶ **So verwenden Sie SSL für alle Clientverbindungen**

Bei diesem Ansatz konfigurieren Sie die Clientbibliotheken so, dass SSL für alle Verbindungen verwendet wird. Dies bedeutet, dass auf Servern mit SQL Server, die die Verschlüsselung nicht unterstützen, und auf Servern mit einer älteren Version als SQL Server 2000 nicht mehr zugegriffen werden kann.

1. Klicken Sie in der Programmgruppe **Microsoft SQL Server** auf **SQL Server-Clientkonfiguration**.
2. Vergewissern Sie sich, dass TCP/IP und/oder Named Pipes aktiviert ist.
3. Wählen Sie **Protokollverschlüsselung erzwingen**.

▶ **So lassen Sie Anwendungen wählen, ob Verschlüsselung verwendet werden soll**

Bei diesem Ansatz verwenden Anwendungen die Verbindungszeichenfolge, um festzulegen, ob Verschlüsselung verwendet werden soll. Auf diese Weise kann jede Anwendung die Verschlüsselung nur dann verwenden, wenn diese wirklich erforderlich ist.

1. Wenn Sie den OLE-DB-Datenanbieter für die Herstellung der Verbindung zu SQL Server verwenden, setzen Sie **Use Encryption for Data** wie im nachstehenden Beispiel einer OLE-DB-Verbindungszeichenfolge gezeigt auf **true**.

```
"Provider=SQLOLEDB.1;Integrated Security=SSPI;Persist Security Info=False;Initial
Catalog=Northwind;Data Source=sql01;Use Encryption for Data=True"
```

2. Wenn Sie den SQL Server .NET-Datenanbieter für die Herstellung der Verbindung zu SQL Server verwenden, setzen Sie **Encrypt** wie im folgenden Beispiel gezeigt auf **true**.

```
"Server=sql01;Integrated Security=SSPI;Persist Security
Info=False;Database=Northwind;Encrypt=True"
```

6. Sicherstellen, dass die Kommunikation verschlüsselt wird

In diesem Verfahren wird mithilfe des Netzwerkmonitors sichergestellt, dass die Datenströme zwischen Anwendungsserver und Datenbankserver verschlüsselt werden. Sie beginnen mit dem Senden von Daten im Klartext und aktivieren dann die Verschlüsselung, indem Sie zunächst den Server und dann den Client konfigurieren.

▶ **So stellen Sie sicher, dass die Kommunikation verschlüsselt wird**

1. Erstellen Sie auf dem Clientcomputer mit Visual Studio .NET in C# eine neue Konsolenanwendung mit Namen **SQLSecureClient**.
2. Kopieren Sie den folgenden Code in **Class1.cs**, und ersetzen Sie damit allen vorhandenen Code.

   Hinweis: Ersetzen Sie den Servernamen in der Verbindungszeichenfolge durch den Namen Ihres Datenbankservers.

```
using System;
using System.Data;
using System.Data.SqlClient;

namespace SQLSecureClient
{
  class Class1
  {
    [STAThread]
    static void Main(string[] args)
    {
      // Replace the server name in the following connection string with the
      // name of your database server
      SqlConnection conn = new SqlConnection(
        "server='sql01';database=NorthWind;Integrated Security='SSPI'");

      SqlCommand cmd = new SqlCommand("SELECT * FROM Products");
      try
      {
        conn.Open();
        cmd.Connection = conn;
        SqlDataReader reader = cmd.ExecuteReader();
        while (reader.Read())
        {
          Console.WriteLine("{0} {1}",
                     reader.GetInt32(0).ToString(),
                     reader.GetString(1) );
        }
        reader.Close();
      }
      catch( Exception ex)
      {
      }
      finally
      {
        conn.Close();
      }
    }
  }
}
```

3. Klicken Sie im Menü **Erstellen** auf **Projektmappe erstellen**.

4. Damit zwischen den beiden Computern eine Windows-Authentifizierung stattfinden kann, müssen Sie das Konto, mit dem Sie gegenwärtig interaktiv am Clientcomputer angemeldet sind, auf den Datenbankserver kopieren. Stellen Sie sicher, dass Benutzername und Kennwort die gleichen sind. Alternativ können Sie auch ein Domänenkonto verwenden, das von beiden Computern erkannt wird.

   Darüber hinaus müssen Sie mithilfe von SQL Server Enterprise Manager eine Datenbankanmeldung für das neu erstellte Konto sowie einen Datenbankbenutzer für diese Anmeldung an der Northwind-Datenbank anlegen.
5. Deaktivieren Sie auf dem Datenbankserver mithilfe der SQL Server-Netzwerkkonfiguration die Verwendung der Verschlüsselung, indem Sie sicherstellen, dass die Option **Protokollverschlüsselung erzwingen** deaktiviert ist.
6. Klicken Sie auf dem Datenbankserver in der Programmgruppe **Verwaltung** auf **Netzwerkmonitor**.

   Hinweis: Zum Lieferumfang von Windows 2000 Server gehört eine eingeschränkte Version des Netzwerkmonitors. Die Vollversion steht mit Microsoft SMS zur Verfügung.

   Wenn der Netzwerkmonitor noch nicht installiert wurde, wechseln Sie in der Systemsteuerung zu **Software**, klicken Sie auf **Windows-Komponenten hinzufügen/entfernen**, wählen Sie **Verwaltungs- und Überwachungsprogramme** aus der Liste **Windows-Komponenten**, klicken Sie auf **Details**, und wählen Sie dann **Netzwerkmonitorprogramme**. Klicken Sie auf **OK** und dann auf **Weiter**, um die eingeschränkte Version des Netzwerkmonitors zu installieren. Sie werden möglicherweise aufgefordert, die Windows 2000 Server-CD einzulegen.

   ---
7. Klicken Sie im Menü **Sammeln** auf **Filter**, um einen neuen Filter zu erstellen, der für die Anzeige des zwischen Datenbankserver und Clientcomputer übertragenen TCP/IP-Netzwerkverkehrs konfiguriert ist.
8. Klicken Sie auf die Schaltfläche **Sammlung starten**.
9. Kehren Sie zum Clientcomputer zurück, und führen Sie die Testkonsolenanwendung aus. Nun sollte eine Liste der Produkte in der Northwind-Datenbank im Konsolenfenster angezeigt werden.
10. Kehren Sie zum Datenbankserver zurück, und klicken Sie im Netzwerkmonitor auf die Schaltfläche **Sammlung beenden und anzeigen**.
11. Doppelklicken Sie auf den ersten gesammelten Rahmen, um die hierin enthaltenen Daten anzuzeigen.
12. Führen Sie in den gesammelten Rahmen einen Bildlauf nach unten durch. Sie sollten nun die SELECT-Anweisung im Klartext gefolgt von der Liste der Produkte sehen, die aus der Datenbank abgerufen wurde.
13. Erzwingen Sie nun die Verwendung der Verschlüsselung für alle Verbindungen, indem Sie den Server mit der SQL Server-Netzwerkkonfiguration konfigurieren.
    a. Aktivieren Sie mithilfe der SQL Server-Netzwerkkonfiguration die Option **Protokollverschlüsselung erzwingen**.
    b. Beenden und starten Sie den SQL Server-Dienst neu.
14. Kehren Sie zum Netzwerkmonitor zurück, und klicken Sie auf die Schaltfläche **Sammlung starten**. Klicken Sie im Dialogfeld **Datei speichern** auf **Nein**.
15. Kehren Sie zum Clientcomputer zurück, und führen Sie die Testkonsolenanwendung erneut aus.
16. Kehren Sie zum Datenbankserver zurück, und klicken Sie im Netzwerkmonitor auf **Sammlung beenden und anzeigen**.
17. Vergewissern Sie sich, dass die Daten nun nicht mehr lesbar sind (da sie verschlüsselt wurden).
18. Konfigurieren Sie den Server wieder so, dass keine Verschlüsselung mehr erzwungen wird:

a. Deaktivieren Sie mithilfe der SQL Server-Netzwerkkonfiguration die Option **Protokollverschlüsselung erzwingen**.

b. Beenden und starten Sie den SQL Server-Dienst neu.

19. Starten Sie im Netzwerkmonitor eine neue Sammlung, und führen Sie die Client-anwendung erneut aus. Vergewissern Sie sich, dass die Daten wieder im Klartext vorliegen.
20. Kehren Sie zum Clientcomputer zurück, und wählen Sie aus der Programmgruppe **Microsoft SQL Server** die **SQL Server-Clientkonfiguration**.
21. Aktivieren Sie die Option **Protokollverschlüsselung erzwingen**, und klicken Sie auf **OK**, um die SQL Server-Clientkonfiguration zu schließen.
22. Kehren Sie zum Netzwerkmonitor zurück, und klicken Sie auf die Schaltfläche **Sammlung starten**. Klicken Sie im Dialogfeld **Datei speichern** auf **Nein**.
23. Kehren Sie zum Clientcomputer zurück, und führen Sie die Testkonsolenanwendung erneut aus.
24. Kehren Sie zum Datenbankserver zurück, und klicken Sie im Netzwerkmonitor auf **Sammlung beenden und anzeigen**.
25. Vergewissern Sie sich, dass die Daten nun nicht mehr lesbar sind (da sie verschlüsselt wurden).
26. Beachten Sie, dass SQL Server in allen Fällen zu Beginn der Kommunikationssequenz sein Serverauthentifizierungszertifikat im Klartext an den Client sendet. Dies ist Teil des SSL-Protokolls. Beachten Sie, dass dies auch dann geschieht, wenn weder der Server noch der Client Verschlüsselung verlangen.

Weitere Ressourcen

Weitere Informationen über die Installation des Netzwerkmonitors unter Windows 2000 finden Sie in folgenden Artikeln in der Microsoft Knowledge Base:

- "HOW TO: Install Network Monitor in Windows 2000 (Q243270)" (US)
- "HOW TO: Enable SSL Encryption for SQL Server 2000 with Certificate Server"(Q276553)" (US)

Weitere Informationen über den Netzwerkmonitor finden Sie im Abschnitt "Network Monitor" des Microsoft Platform SDKs im MSDN (http://msdn.microsoft.com/library/default.asp?url=/library/en-us/netmon/netmon/network_monitor.asp, englischsprachig).