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

Ein Webserver muss für SSL konfiguriert sein, damit HTTPS-Verbindungen von Clientanwendungen unterstützt werden. In dieser Vorgehensweise wird erläutert, wie SSL auf einem Webserver konfiguriert wird.

Vorgehensweise: Einrichten von SSL auf einem Webserver

SSL (Secure Sockets Layer) ist eine Sammlung von Verschlüsselungstechnologien, die Authentifizierung, Vertraulichkeit und Datenintegrität ermöglichen. SSL ist das zwischen Webbrowsern und Webservern am häufigsten eingesetzte Verfahren zur Errichtung eines sicheren Kommunikationskanals. SSL kann zudem auch zwischen Clientanwendungen und Webdiensten zum Einsatz kommen.

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.

- Microsoft® Windows® 2000 Server (mit Service Pack 2) als Betriebssystem
- Microsoft Zertifikatdienste (erforderlich, wenn Sie eigene Zertifikate erzeugen möchten)

Die in dieser Vorgehensweise erläuterten Verfahren setzen zudem Kenntnisse der IIS-Konfiguration voraus.

Zusammenfassung

Diese Vorgehensweise enthält folgende Verfahren:

1. Erzeugen einer Zertifikatsanforderung
2. Übermitteln einer Zertifikatsanforderung
3. Ausstellen des Zertifikats
4. Installieren des Zertifikats auf dem Webserver
5. Konfigurieren von Ressourcen zum Anfordern von SSL-Zugriff

1. Erzeugen einer Zertifikatsanforderung

In diesem Verfahren wird eine neue Zertifikatsanforderung erstellt, die zwecks Verarbeitung an eine Zertifizierungsstelle (Certificate Authority, CA) übermittelt werden kann. Nach erfolgreicher Anforderung sendet die Zertifizierungsstelle eine Datei zurück, die ein geprüftes Zertifikat enthält.

▶ **So generieren Sie eine Zertifikatsanforderung**

1. Starten Sie das IIS-MMC-Snap-In (Microsoft Management Console).
2. Erweitern Sie den Knoten mit dem Namen Ihres Webservers, und wählen Sie die Website aus, für die Sie ein Zertifikat installieren möchten.
3. Klicken Sie mit der rechten Maustaste auf die Website und dann auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Verzeichnissicherheit**.
5. Klicken Sie im Bereich **Sichere Kommunikation** auf die Schaltfläche **Serverzertifikat**, um den Assistenten für Webserverzertifikate zu starten.

   Hinweis: Wenn die Schaltfläche **Serverzertifikat** nicht verfügbar ist, haben Sie wahrscheinlich ein virtuelles Verzeichnis, ein Verzeichnis oder eine Datei ausgewählt. Führen Sie Schritt 2 erneut durch, und wählen Sie eine Website aus.

6. Klicken Sie auf **Weiter**, um das Begrüßungsdialogfeld zu schließen.
7. Klicken Sie auf **Neues Zertifikat erstellen** und dann auf **Weiter**.
8. Das nun gezeigte Dialogfeld bietet die beiden folgenden Optionen:
   - Anforderung jetzt vorbereiten, aber später senden
     Diese Option ist immer verfügbar.
   - Anforderung sofort an eine Onlinezertifizierungsstelle senden
     Diese Option ist nur verfügbar, wenn der Webserver auf einen oder mehrere Microsoft Zertifikatserver in einer Windows 2000-Domäne zugreifen kann, der bzw. die für die Ausgabe von Webserverzertifikaten konfiguriert ist/sind. Zu einem späteren Zeitpunkt im Anforderungsverfahren erhalten Sie die Möglichkeit, eine Zertifizierungsstelle aus einer Liste zu wählen, an die die Anforderung übermittelt werden soll.

   Klicken Sie auf **Anforderung jetzt vorbereiten, aber später senden**, und klicken Sie dann auf **Weiter**.
9. Geben Sie einen aussagekräftigen Namen für das Zertifikat in das Feld **Name** ein, geben Sie die Bitlänge des Schlüssels in das Feld **Bitlänge** ein, und klicken Sie dann auf **Weiter**.

   Der Assistent verwendet den Namen der aktuellen Website als Standardnamen. Dieser wird zwar nicht im Zertifikat verwendet, dient jedoch als angezeigter Name zur Orientierung der Administratoren.
10. Geben Sie den Namen einer Organisation (wie beispielsweise Contoso) in das Feld **Organisation** und eine Organisationseinheit (wie Vertriebsabteilung) in das Feld **Organisationseinheit** ein, und klicken Sie dann auf **Weiter**.

    Hinweis: Diese Angaben erscheinen in der Zertifikatsanforderung, also sollten Sie sie auf Richtigkeit prüfen. Die Zertifizierungsstelle überprüft zudem diese Informationen und setzt sie in das Zertifikat. Besucher Ihrer Website möchten diese Informationen möglicherweise anzeigen, um zu entscheiden, ob dieses Zertifikat von ihnen akzeptiert werden sollte.

11. Geben Sie im Feld **Gemeinsamer Name (CN)** einen gemeinsamen Namen für die Site ein, und klicken Sie dann auf **Weiter**.

Wichtig: Der gemeinsame Name ist eine der wichtigsten Angaben, die ebenfalls in das Zertifikat übernommen wird. Hierbei handelt es sich um den DNS-Namen der Website (d. h. den Namen, den der Benutzer eingibt, wenn er Ihre Site besuchen möchte). Wenn der Zertifikatname nicht mit dem Sitenamen übereinstimmt, wird ein Problem mit dem Zertifikat gemeldet, wenn Benutzer die Site besuchen.

Wenn sich die Site im Web befindet und der Name **www.contoso.com** lautet, sollten Sie auch diesen Namen als gemeinsamen Namen angeben.

Wenn es sich um eine interne Site handelt und die Benutzer die Auswahl nach Computername treffen, geben Sie den NetBIOS- oder DNS-Namen des Computers ein.

12. Geben Sie die entsprechenden Informationen in die Felder **Land/Region**, **Bundesland/Kanton** und **Ort** ein, und klicken Sie auf **Weiter**.
13. Geben Sie einen Dateinamen für die Zertifikatsanforderung ein.
    Die Datei enthält Informationen wie die folgenden:

```
-----BEGIN NEW CERTIFICATE REQUEST-----
MIIDZjCCAs8CAQAwgYoxNjA0BgNVBAMTLW1penJvY2tsYXB0b3Aubm9ydGhhbWVy…
-----END NEW CERTIFICATE REQUEST-----
```

    Dies ist eine Base-64-codierte Darstellung Ihrer Zertifikatsanforderung. Die Anforderung enthält die im Assistenten gemachten Angaben sowie Ihren öffentlichen Schlüssel. Darüber hinaus enthält sie Informationen, die mit dem privaten Schlüssel signiert sind.

    Die Anforderungsdatei wird an die Zertifizierungsstelle gesendet. Die Zertifizierungsstelle verwendet anschließend die Angaben zum öffentlichen Schlüssel aus der Zertifikatsanforderung, um die mit dem privaten Schlüssel signierten Informationen zu überprüfen. Die Zertifizierungsstelle prüft zudem die mit der Anforderung übermittelten Informationen.

    Nachdem Sie die Anforderung an die Zertifizierungsstelle gesendet haben, sendet diese ein Zertifikat zurück, das in einer Datei enthalten ist. Sie starten Ihrerseits dann den Assistenten für Webserverzertifikate erneut.
14. Klicken Sie auf **Weiter**. Der Assistent zeigt nun eine Zusammenfassung der in der Zertifikatsanforderung enthaltenen Angaben an.
15. Klicken Sie auf **Weiter** und dann auf **Fertig stellen**, um den Anforderungsprozess abzuschließen.
    Die Zertifikatsanforderung kann nun zwecks Überprüfung und Verarbeitung an die Zertifizierungsstelle gesendet werden. Nachdem Sie von dieser eine Antwort enthalten haben, können Sie fortfahren und das in der Antwort enthaltene Zertifikat – wiederum mithilfe des IIS-Zertifikatassistenten – auf dem Webserver installieren.

2. Übermitteln einer Zertifikatsanforderung

In diesem Verfahren wird auf die Microsoft Zertifikatdienste zurückgegriffen, um die Zertifikatsanforderung zu übermitteln, die im vorherigen Verfahren erzeugt wurde.

▶ **So übermitteln Sie eine Zertifikatsanforderung**

1. Öffnen Sie die im vorherigen Verfahren erstellte Zertifikatdatei in Notepad, und kopieren Sie den gesamten Inhalt in die Zwischenablage.
2. Starten Sie Internet Explorer, und navigieren Sie zu **http://***Hostname***/CertSrv**, wobei *Hostname* für den Namen des Computers steht, auf dem die Microsoft Zertifikatdienste ausgeführt werden.
3. Klicken Sie auf **Zertifikat anfordern** und dann auf **Weiter**.
4. Klicken Sie auf der Seite **Anforderungstyp wählen** auf **Erweiterte Anforderung**, und klicken Sie dann auf **Weiter**.

5. Klicken Sie auf der Seite **Erweiterte Zertifikatsanforderungen** auf **Senden Sie eine Zertifikatsanforderung ein, die eine Base64-codierte PKCS10-Datei verwendet**, und klicken Sie dann auf **Weiter**.
6. Klicken Sie auf der Seite **Gespeicherte Anforderung einsenden** auf das Textfeld zur Base64-codierten Zertifikatsanforderung (PKCS #10 oder #7). Drücken Sie dann **STRG+V**, um die Zertifikatsanforderung einzufügen, die Sie im Vorfeld in die Zwischenablage kopiert haben.
7. Klicken Sie im Kombinationsfeld **Zertifikatvorlagen** auf **Webserver**.
8. Klicken Sie auf **Senden**.
9. Schließen Sie Internet Explorer.

3. Ausstellen des Zertifikats

▶ **So stellen Sie das Zertifikat aus**

1. Starten Sie das Tool **Zertifizierungsstellen** aus der Programmgruppe **Verwaltung**.
2. Erweitern Sie Ihre Zertifizierungsstelle, und wählen Sie den Ordner **Ausstehende Anforderungen**.
3. Wählen Sie die Zertifikatsanforderung, die Sie soeben übermittelt haben.
4. Zeigen Sie im Menü **Aktion** auf **Alle Tasks**, und klicken Sie auf **Ausstellen**.
5. Vergewissern Sie sich, dass das Zertifikat im Ordner **Ausgestellte Zertifikate** angezeigt wird, und doppelklicken Sie dann darauf, um es anzuzeigen.
6. Klicken Sie auf der Registerkarte **Details** auf **In Datei kopieren**, und speichern Sie das Zertifikat als Base-64-codiertes X.509-Zertifikat.
7. Schließen Sie das Eigenschaftenfenster des Zertifikats.
8. Schließen Sie das Tool **Zertifizierungsstellen**.

4. Installieren des Zertifikats auf dem Webserver

In diesem Verfahren wird das im vorstehenden Verfahren ausgestellte Zertifikat auf dem Webserver installiert.

▶ **So installieren Sie das Zertifikat auf dem Webserver**

1. Starten Sie die Internet-Informationsdienste, sofern diese nicht bereits ausgeführt werden.
2. Erweitern Sie den Knoten mit dem Namen Ihres Servers, und wählen Sie die Website aus, für die Sie ein Zertifikat installieren möchten.
3. Klicken Sie mit der rechten Maustaste auf die Website und dann auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Verzeichnissicherheit**.
5. Klicken Sie auf **Serverzertifikat**, um den Assistenten für Webserverzertifikate zu starten.
6. Klicken Sie auf **Ausstehende Anforderung verarbeiten und Zertifikat installieren**, und klicken Sie dann auf **Weiter**.
7. Geben Sie den Pfad und den Namen der Datei ein, die die Antwort der Zertifizierungsstelle enthält, und klicken Sie auf **Weiter**.
8. Werfen Sie einen Blick in die Zertifikatübersicht, klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**.

   Das Zertifikat ist nun auf dem Webserver installiert.

5. Konfigurieren von Ressourcen zum Anfordern des SSL-Zugriffs

In diesem Verfahren wird ein virtuelles Verzeichnis mithilfe des Internetdienste-Managers so konfiguriert, dass SSL für den Zugriff gefordert wird. Sie können festlegen, dass SSL für bestimmte Dateien, Verzeichnisse oder virtuelle Verzeichnisse verlangt wird. Die Clients müssen dann das HTTPS-Protokoll verwenden, um auf in dieser Weise konfigurierte Ressourcen zugreifen zu können.

▶ **So konfigurieren Sie Ressourcen für die Verwendung des SSL-Zugriffs**

1. Starten Sie die Internet-Informationsdienste, sofern diese nicht bereits ausgeführt werden.
2. Erweitern Sie den Namen Ihres Servers und der Website. (Hierbei muss es sich um eine Website handeln, für die ein Zertifikat installiert wurde.)
3. Klicken Sie mit der rechten Maustaste auf ein virtuelles Verzeichnis, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf die Registerkarte **Verzeichnissicherheit**.
5. Klicken Sie unter **Sichere Kommunikation** auf **Bearbeiten**.
6. Klicken Sie auf **Sicheren Kanal verlangen (SSL)**.
   Clients, die auf dieses virtuelle Verzeichnis zugreifen möchten, müssen nun HTTPS verwenden.
7. Klicken Sie auf **OK** und dann erneut auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.
8. Schließen Sie die Internet-Informationsdienste.