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

ASP.NET-Webanwendungen werden in der Regel unter Verwendung des integrierten ASPNET-Kontos ausgeführt. Es kann sich allerdings die Notwendigkeit ergeben, stattdessen ein benutzerdefiniertes Konto zu verwenden. Nachstehend wird erläutert, wie ein mit minimalen Rechten ausgestattetes Konto zum Ausführen von ASP.NET-Webanwendungen erstellt wird.

Vorgehensweise: Erstellen eines benutzerdefinierten Kontos zum Ausführen von ASP.NET

Diese Vorgehensweise beschreibt, wie ein mit minimalen Rechten ausgestattetes lokales Konto zum Ausführen des ASP.NET-Workerprozesses (**aspnet_wp.exe**) oder für Wechselidentitäten in virtuellen Verzeichnissen erstellt wird. Mit den hier beschriebenen Verfahren wird zwar ein lokales Konto erstellt, die Konzepte gelten jedoch gleichermaßen für ein Domänenkonto.

Identität des ASP.NET-Workerprozesses

Das zum Zeitpunkt der Installation angelegte Standardkonto zum Ausführen von ASP.NET ist ein lokales Konto mit minimalen Rechten und wird in **machine.config** wie folgt definiert:

```
<processModel enable="true" userName="machine" password="AutoGenerate" />
```

Dieses Konto wird im Container **Lokale Benutzer und Gruppen** als "ASPNET" aufgeführt und verfügt über ein starkes Kennwort, das in der Local Security Authority (LSA) gesichert ist.

Wenn Sie unter Verwendung der ASP.NET-Prozessidentität auf Netzwerkressourcen wie eine Datenbank zugreifen müssen, haben Sie die folgenden Möglichkeiten:

- Sie können ein Domänenkonto verwenden.
- Sie können "gespiegelte" lokale Konten verwenden (d. h. Konten mit übereinstimmenden Benutzernamen und Kennwörtern auf zwei Computern). Diese Vorgehensweise ist zwingend, wenn sich die Computer in unterschiedlichen Domänen ohne Vertrauensstellung befinden oder wenn sich zwischen den Computern ein Firewall befindet und Sie die für die NTLM- oder Kerberos-Authentifizierung benötigten Anschlüsse nicht öffnen können.

Die einfachste Vorgehensweise besteht darin, das Kennwort des ASPNET-Kontos in einen dem Webserver bekannten Wert zu ändern und dann ein Konto mit Namen ASPNET mit dem gleichen Kennwort auf dem Zielcomputer zu erstellen. Auf dem Webserver müssen Sie zuerst das Kennwort des ASPNET-Kontos im Container **Lokale Benutzer und Gruppen** ändern und dann **AutoGenerate** in **machine.config** durch das neue Kennwort ersetzen.

```
<processModel enable="true" userName="machine"
              password="YourStrongPassword" />
```

Mit den in dieser Vorgehensweise erläuterten Schritten können Sie ein lokales Konto mit minimalen Rechten erstellen.

Identitätswechsel zu festen Identitäten

Mithilfe der folgenden Einstellung in **web.config** können Sie feste Identitäten für bestimmte virtuelle Verzeichnisse festlegen.

```
<identity impersonate="true" userName="YourAccount"
          password="YourStrongPassword" />
```

Dieses Verfahren wird in der Regel verwendet, wenn Sie auf dem gleichen Webserver mehrere Websites verwalten, die unter unterschiedlichen Identitäten ausgeführt werden müssen, also beispielsweise beim Anwendungshosting.

Nachstehend wird gezeigt, wie ein lokales Konto mit minimalen Rechten angelegt wird. Wenn es in erster Linie um die Verwaltung geht, können Sie auch ein eingeschränktes Domänenkonto mit minimalen Rechten und einem starken Kennwort verwenden.

Hinweise

Bei den Überlegungen bezüglich des Kontos zum Ausführen von ASP.NET sollten Sie Folgendes berücksichtigen:

- ASP.NET führt nicht standardmäßig einen Identitätswechsel durch. Demzufolge wird bei jedem Ressourcenzugriff seitens der Webanwendung die ASP.NET-Prozessidentität verwendet. In diesem Fall müssen Windows-Ressourcen über eine Zugriffsteuerungsliste (Access Control List, ACL) verfügen, die den Zugriff auf das ASP.NET-Prozesskonto ermöglicht.
- Wenn Sie den Identitätswechsel aktivieren, greift die Anwendung unter Verwendung des Sicherheitskontextes des ursprünglichen Aufrufers oder des anonymen Internetbenutzerkontos (standardmäßig IUSR_MACHINE) auf Ressourcen zu, wenn IIS für die anonyme Authentifizierung konfiguriert ist. In diesem Fall müssen die Ressourcen über ACLs basierend auf der Identität des ursprünglichen Aufrufers (oder IUSR_MACHINE) verfügen.
- Halten Sie sich bei der Erstellung eines benutzerdefinierten Kontos immer an das Prinzip der minimalen Rechte, d. h. gewähren Sie jeweils nur das Minimum der erforderlichen Rechte und Berechtigungen.
- Vermeiden Sie es, ASP.NET unter Verwendung des Kontos SYSTEM auszuführen.
- Sehen Sie davon ab, dem Konto das Recht **Als Teil des Betriebssystems handeln** zu gewähren.

Zusammenfassung

Diese Vorgehensweise enthält folgende Verfahren:

1. Erstellen eines neuen lokalen Kontos
2. Zuweisen von minimalen Rechten
3. Zuweisen von NTFS-Berechtigungen

4. Konfigurieren von ASP.NET für die Ausführung unter Verwendung des neuen Kontos

1. Erstellen eines neuen lokalen Kontos

Mit diesem Verfahren wird ein neues lokales Konto erstellt. Das neue Konto wird standardmäßig der lokalen Gruppe **Benutzer** hinzugefügt.

} So erstellen Sie ein neues lokales Konto

1. Erstellen Sie in lokales Konto (zum Beispiel "CustomASPNET").

   Verwenden Sie unbedingt ein starkes Kennwort für das Konto. Ein starkes Kennwort umfasst mindestens sieben Zeichen und setzt sich aus einer Mischung aus Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen wie *, ? oder $ zusammen.
2. Deaktivieren Sie die Option **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**.
3. Aktivieren Sie die Option **Kennwort läuft nie ab**.

2. Zuweisen von minimalen Rechten

Mit diesem Verfahren werden die minimalen Rechte zugewiesen, die zum Ausführen von ASP.NET erforderlich sind.

υ So weisen Sie minimale Rechte zu

1. Starten Sie das Tool **Lokale Sicherheitsrichtlinie** aus der Programmgruppe **Verwaltung**.
2. Erweitern Sie **Lokale Sicherheitsrichtlinie**, und wählen Sie **Zuweisen von Benutzerrechten**.

   Im rechten Fensterausschnitt wird eine Liste der Rechte angezeigt.
3. Weisen Sie dem neuen Konto die folgenden Rechte zu:
   - Auf diesen Computer vom Netzwerk aus zugreifen
   - Lokale Anmeldung verweigern
   - Anmelden als Stapelverarbeitungsauftrag
   - Als Dienst anmelden

   Hinweis: Wenn Sie einem Konto ein Recht zuweisen möchten, doppelklicken Sie auf das Recht und klicken dann auf **Hinzufügen**, um das gewünschte Konto auswählen zu können.
4. Schließen Sie das Tool.

3. Zuweisen von NTFS-Berechtigungen

Mit diesem Verfahren werden dem benutzerdefinierten ASP.NET-Konto die erforderlichen NTFS-Berechtigungen im lokalen Dateisystem gewährt.

Hinweis: Die Schritte in diesem Verfahren beziehen sich auf das Dateisystem auf dem Webserver (und nicht auf einem Remotecomputer, auf dem Sie evtl. das Konto zum Zwecke der Netzwerkauthentifizierung duplizieren).

υ So weisen Sie NTFS-Berechtigungen zu

1. Starten Sie Windows-Explorer, und weisen Sie für die in Tabelle 1 aufgeführten Ordner die geeigneten Berechtigungen zu.

   Das in Tabelle 1 genannte Konto für den Wechsel zu einer festen Identität bezieht sich auf das Konto, das optional unter Verwendung des <**identity**>-Elements in **web.config** wie nachstehend gezeigt konfiguriert werden kann.

```
<identity impersonate="true" userName="YourImpersonatedIdentity"
```

```
password="YourStrongPassword" />
```

Tabelle 1: Erforderliche NTFS-Berechtigungen

Ordner	Erforderliche Berechtigung	Konto	Kommentare
C:\WINNT\Microsoft.NET\Framework\<Version>\Temporary ASP.NET Files	Vollzugriff	Prozesskonto und Konten für den Wechsel zu einer festen Identität	Dies ist die dynamische Kompilierungsposition von ASP.NET. Der Anwendungscode wird für jede Anwendung in einem getrennten Verzeichnis in diesem Ordner erzeugt. Zum Ändern dieser Standardposition kann das **tempdir**-Attribut des <**compilation**>-Elements verwendet werden.
C:\WINNT\Temp	Lesen/ Schreiben/ Löschen	Prozesskonto	Von Webdiensten zum Erzeugen von Serialisierungsproxys verwendeter Speicherort. Beachten Sie, dass die Berechtigung zum Löschen unter Verwendung der Schaltfläche **Erweitert** auf der Registerkarte **Sicherheitseinstellungen** des Windows-Explorer-Dialogfeldes **Eigenschaften von [Ordner]** festgelegt wird.
Anwendungsordner	Lesen	Prozesskonto	Die Position der Dateien Ihrer Webanwendung (d. h. das virtuelle Stammverzeichnis der Anwendung, zum Beispiel **c:\inetpub\wwwroot\webapp1**). Die Gruppe **Benutzer** verfügt standardmäßig über die entsprechenden Zugriffsrechte.
%installroot%-Hierarchie (**C:\WINNT\Microsoft.Net\Framework\v1.0.3705**)	Lesen	Prozesskonto und Konten für den Wechsel zu einer festen Identität	ASP.NET muss in der Lage sein, auf .NET Framework-Assemblys zugreifen zu können. Die Gruppe **Benutzer** verfügt standardmäßig über die entsprechenden

			Zugriffsrechte.
C:\WINNT\Assembly	Lesen	Prozesskonto und Konten für den Wechsel zu einer festen Identität	Dies ist der globale Assemblycache. Die Bearbeitung der ACLs für diesen Ordner kann nicht direkt von Windows-Explorer aus erfolgen. Verwenden Sie stattdessen ein Befehls-fenster, und führen Sie den folgenden Befehl aus: **cacls %windir%\assembly /e /t /p domain\useraccount:R** Alternativ können Sie vor der Verwendung von Windows-Explorer auch die Registrierung der Datei **shfusion.dll** mit dem folgenden Befehl aufheben: **regsvr32 –u shfusion.dll** Nach der Festlegung von Berechtigungen mit Windows-Explorer registrieren Sie die Datei **shfusion.dll** mit dem folgenden Befehl erneut: **regsvr32 shfusion.dll**
Websitestamm: **C:\inetpub\wwwroot** oder der Pfad, auf den die Standardwebsite verweist	Lesen	Prozesskonto	ASP.NET liest Konfigura-tionsdateien und überwacht Dateiänderungen in diesem Ordner.
C:\WINNT\system32	Lesen	Prozesskonto	Für System-DLLs, die vom Framework geladen werden.
Übergeordnete Verzeichnisse (Kontext)	Ordner auflisten/Lesen	Prozesskonto	Für Dateiänderungsbenach-richtigungen und den C#-Compiler.

4. Konfigurieren von ASP.NET für die Ausführung unter Verwendung des neuen Kontos

Mit diesem Verfahren wird **machine.config** bearbeitet und ASP.NET so konfiguriert, dass es unter Verwendung des neuen Kontos ausgeführt werden kann.

υ So konfigurieren Sie ASP.NET für die Ausführung unter Verwendung des neuen Kontos

1. Öffnen Sie **machine.config** mit Visual Studio.NET oder Notepad.

Die Datei **machine.config** befindet sich im folgenden Ordner:

```
C:\WINNT\Microsoft.NET\Framework\v1.0.3705\CONFIG
```

2. Suchen Sie das <**processModel**>-Element, und legen Sie die Attribute für Benutzername und die Kennwortattribute so fest, dass sie dem neuen benutzerdefinierten Konto entsprechen.

```
Default: <!-- userName="machine" password="AutoGenerate" -->
Becomes: <!-- userName="CustomASPNET" password="YourStrongPassword" -->
```

3. Speichern Sie die Änderungen an **machine.config**.

Hinweis: Mit dem .NET Framework Version 1.0 gibt es keine Möglichkeit, das Speichern des Kennworts im Klartext zu umgehen. Zwar ist das Speichern von Anmeldeinformationen im Klartext generell nicht empfehlenswert, jedoch wird die Datei **machine.config** als sicherer erachtet, da sie sich außerhalb des Webbereichs befindet. Sie sollten **machine.config** vor unnötigem Zugriff schützen, indem Sie eine entsprechend konfigurierte ACL verwenden.

In Windows Server 2003 werden Anmeldeinformationen verschlüsselt, um besseren Schutz zu bieten.
