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

Die Kerberos-Delegierung ermöglicht die Weitergabe einer authentifizierten Identität durch mehrere physikalische Schichten einer Anwendung für die nachgeordnete Authentifizierung und Autorisierung. Die nachstehende Vorgehensweise erläutert die hierfür erforderlichen Konfigurationsschritte.

Vorgehensweise: Implementieren der Kerberos-Delegierung unter Windows 2000

Standardmäßig verwendet das Betriebssystem Microsoft® Windows® 2000 das Kerberos-Protokoll für die Authentifizierung. In dieser Vorgehensweise wird die Konfiguration der Kerberos-Delegierung beschrieben, eines leistungsfähigen Features, das es dem Server bei Übernahme der Identität des Clients ermöglicht, anstelle des Clients auf Remoteressourcen zuzugreifen.

Wichtig: Die Delegierung ist eine äußerst leistungsfähige Funktion, die unter Windows 2000 keinerlei Beschränkungen unterliegt. Sie sollte daher mit großer Vorsicht eingesetzt werden. Bei Computern, die für die Unterstützung der Delegierung konfiguriert sind, sollte der Zugriff permanent überwacht werden, um einen Missbrauch der Funktion zu vermeiden.

Für Windows Server 2003 ist eine eingeschränkte Delegierungsfunktion vorgesehen.

Wenn der Server die Identität eines Clients annimmt, erzeugt die Kerberos-Authentifizierung ein Token auf der Ebene **Delegate** (das in der Lage ist, auf Netzwerk-Authentifizierungsanforderungen von Remotecomputern zu antworten), wenn die folgenden Voraussetzungen erfüllt sind:

1. Das Clientkonto, dessen Identität der Server annimmt, ist nicht als vertraulich gekennzeichnet und kann im Verzeichnisdienst Microsoft Active Directory® nicht delegiert werden.
2. Dem Prozesskonto des Servers (d. h. dem Benutzerkonto, unter dem der Serverprozess ausgeführt wird, oder dem Computerkonto, wenn der Prozess unter dem lokalen Konto SYSTEM ausgeführt wird), wird in Active Directory zu Delegierungszwecken vertraut.

Hinweise

- Damit die Kerberos-Delegierung erfolgreich durchgeführt werden kann, müssen sich alle Computer (Clients und Server) in einer gemeinsamen Active Directory-Gesamtstruktur befinden.
- Wenn der Identitätswechsel innerhalb von Serviced Components erfolgt und Sie den Aufruferkontext durch eine Enterprise Services-Anwendung weitergeben möchten, muss der Anwendungsserver, der als Host für Enterprise Services dient, über Hotfix Rollup 18.1 oder höher verfügen.

  Weitere Informationen finden Sie in INFO: Availability of Windows 2000 Post-Service Pack 2 COM+ Hotfix Rollup Package 18.1 (US).

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:

- Windows 2000 Server mit Active Directory.

Zusammenfassung

Diese Vorgehensweise enthält folgende Verfahren:

1. Sicherstellen, dass das Clientkonto für die Delegierung konfiguriert ist
2. Sicherstellen, dass dem Prozesskonto des Servers zu Delegierungszwecken vertraut wird

1. Sicherstellen, dass das Clientkonto für die Delegierung konfiguriert ist

Mit diesem Verfahren können Sie sich vergewissern, dass das Clientkonto delegiert werden kann.

▶ **So vergewissern Sie sich, dass das Clientkonto für die Delegierung konfiguriert ist**

1. Melden Sie sich unter Verwendung eines Administratorkontos am Domänencontroller an.
2. Klicken Sie auf der Taskleiste auf **Start**, zeigen Sie auf **Programme** und dann auf **Verwaltung**, und klicken Sie anschließend auf **Active Directory-Benutzer und -Computer**.
3. Klicken Sie in Ihrer Domäne auf den Ordner **Benutzer**.
4. Klicken Sie mit der rechten Maustaste auf das zu delegierende Benutzerkonto, und klicken Sie dann auf **Eigenschaften**.
5. Klicken Sie auf die Registerkarte **Konto**.
6. Vergewissern Sie sich in der Liste **Kontooptionen**, dass die Option **Konto ist vertraulich und kann nicht delegiert werden** deaktiviert ist.
7. Klicken Sie auf **OK**, um das Dialogfeld **Eigenschaften** zu schließen.

2. Sicherstellen, dass dem Prozesskonto des Servers zu Delegierungszwecken vertraut wird

Mit diesem Verfahren wird geprüft, dass es dem Konto, das zum Ausführen des Serverprozesses verwendet wird (d. h. das Konto, das den Identitätswechsel durchführt), gestattet ist, Clientkonten zu delegieren. Sie müssen das Benutzerkonto konfigurieren, unter dem der Serverprozess ausgeführt wird. Wenn der Prozess unter dem lokalen Konto SYSTEM ausgeführt wird, müssen Sie das Computerkonto konfigurieren. Führen Sie das jeweils

zutreffende Verfahren durch, und zwar abhängig davon, ob der Serverprozess unter einem Windows-Benutzerkonto oder unter einem lokalen SYSTEM-Konto ausgeführt wird.

▶ **So vergewissern Sie sich, dass dem Prozesskonto des Servers zu Delegierungszwecken vertraut wird, wenn der Serverprozess unter einem Windows-Benutzerkonto ausgeführt wird**

1. Klicken Sie im Ordner **Benutzer** von **Active Directory-Benutzer und –Computer** mit der rechten Maustaste auf das Benutzerkonto, das für das Ausführen des Serverprozesses verwendet wird, der die Identität des Clients annimmt, und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie auf die Registerkarte **Konto**.
3. Klicken Sie in der Liste **Kontooptionen** auf **Konto wird für Delegierungszwecke vertraut**.

▶ **So vergewissern Sie sich, dass dem Prozesskonto des Servers zu Delegierungszwecken vertraut wird, wenn der Serverprozess unter dem lokalen Konto SYSTEM ausgeführt wird**

1. Klicken Sie in **Active Directory-Benutzer und –Computer** mit der rechten Maustaste auf den Ordner **Computer** und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie mit der rechten Maustaste auf den Servercomputer (auf dem der Prozess, der die Identität des Clients annimmt, ausgeführt wird), und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie auf der Seite **Allgemein** auf **Computer für Delegierungszwecke vertrauen**.

Referenzen

- Eine Liste der Dateien, die vom COM+ Hotfix Package 18.1 aus dem Windows 2000 Post-Service Pack 2 (SP2) betroffen sind, finden Sie im Artikel Q313582, "INFO: Availability of Windows 2000 Post-Service Pack 2 COM+ Hotfix Rollup Package 18.1" (US) in der Microsoft Knowledge Base.
- Wenn Sie wissen möchten, wie ein vollständiges Delegierungsszenario konfiguriert wird, das ASP.NET, Enterprise Services und SQL Server einschließt, lesen Sie "Übermitteln des ursprünglichen Aufrufers an die Datenbank" in Kapitel 5, "Intranetsicherheit".