msdn training

Unterrichtseinheit 12: Sichern der BizTalk Server 2000-Umgebung

Inhalt

Microsoft

Hinweise für Kursleiter

Präsentation:
45 Minuten

Übungseinheit:
45 Minuten

In dieser Unterrichtseinheit werden den Kursteilnehmern die Kenntnisse und Fähigkeiten zum Sichern einer Microsoft® BizTalk™ Server 2000-Umgebung vermittelt. Dazu werden Server, Servergruppen und Austauschvorgänge gesichert.

Am Ende dieser Unterrichtseinheit werden die Kursteilnehmer in der Lage sein, die folgenden Aufgaben auszuführen:

- Beschreiben der Microsoft Windows® 2000-Features, die von BizTalk Server 2000 zum Sichern von Daten und Komponenten verwendet werden.
- Konfigurieren von Benutzerkonten und Richtlinien für einen sicheren Zugriff.
- Verwenden der Übertragungsmethoden, die BizTalk Server 2000 zum Sichern von Daten unterstützt.
- Verwenden von Zertifikaten in BizTalk Server 2000.
- Sichern des Zugriffs durch einen Firewall.

Unterlagen und Vorbereitung

In diesem Abschnitt werden die erforderlichen Unterlagen und vorbereitenden Aufgaben erläutert, die nötig sind, um diese Unterrichtseinheit zu unterrichten.

Erforderliche Unterlagen

Um diese Unterrichtseinheit zu unterrichten, benötigen Sie folgende Unterlagen:

- Die Microsoft Word-Datei **2387A_12.doc**
- Die Microsoft PowerPoint®-Datei **2387A_12.ppt**
- Übungseinheit 12: Überprüfen der Sicherheitseinstellungen

Vorbereitende Aufgaben

Zur Vorbereitung dieser Unterrichtseinheit gehen Sie folgendermaßen vor:

- Lesen Sie alle Unterlagen für diese Unterrichtseinheit.
- Arbeiten Sie die Übungseinheit durch.
- Lesen Sie die Fragen zur Lernzielkontrolle, und bereiten Sie sich auf Erläuterungen vor, die über die zur Verfügung gestellten Antworten hinausgehen.
- Gehen Sie alle relevanten Informationen in den BizTalk Server 2000-Hilfedateien und im BizTalk Server 2000 Deployment Guide durch.

Strategie für die Unterrichtseinheit

Verwenden Sie die folgende Strategie, um diese Unterrichtseinheit zu präsentieren:

- Einführung in das Sichern der BizTalk Server 2000-Umgebung

  Erklären Sie den Kursteilnehmern, dass BizTalk Server 2000 die Sicherheitsfeatures von Windows 2000 und Microsoft SQL Server™ verwendet, um es Unternehmen zu ermöglichen, Daten auf eine sichere Weise mit Unternehmensgruppen innerhalb der Organisation und über das Internet auszutauschen. Erläutern Sie, dass die Kursteilnehmer die Sicherheitsfeatures verwenden können, die in Windows 2000 zur Verfügung stehen, um die BizTalk Server 2000-Umgebung zu sichern. Sie können dazu Zugriff und Richtlinien auf Administratorebene definieren, sichere Übertragungsmethoden und Zertifikate verwenden und den Zugriff durch Firewalls sichern.

  Richten Sie die Aufmerksamkeit der Kursteilnehmer auf die Tabelle, in der die Sicherheitsfeatures von Windows 2000 und deren Verwendung zum Sichern der BizTalk Server 2000-Umgebung beschrieben werden.

- Verwenden von Konten und Richtlinien

  Erläutern Sie, dass die Kursteilnehmer zum Sichern der BizTalk Server 2000-Umgebung die Gruppe **BizTalk Server-Administratoren**, die Gruppe **Windows 2000-Administratoren** und Dienstkonten konfigurieren müssen. Außerdem müssen die Kursteilnehmer lokale Richtlinien konfigurieren, um die Sicherheitsoptionen für ein Benutzer- oder Dienstkonto festzulegen.

- Verwenden von Übertragungsmethoden zum Sichern von Daten

  Erläutern Sie den Kursteilnehmern, dass sie die Übertragungsmethode bereitstellen werden, die beim Entwickeln des automatisierten Geschäftsprozesses ausgewählt wurde. Beschreiben Sie die vier Übertragungsmethoden, die die Kursteilnehmer für den sicheren Transport ausgehender und eingehender Daten konfigurieren können. Erläutern Sie den Kursteilnehmern, dass sie in der Bereitstellungsphase eine sichere Übertragungsmethode konfigurieren müssen, wenn dies nicht bereits in der Entwicklungsphase geschehen ist.

- Verwenden von Zertifikaten zum Sichern von Daten

  Erklären Sie den Kursteilnehmern, dass sie mit Hilfe von Zertifikaten den Austausch von Informationen in ungesicherten Netzwerken wie z. B. dem Internet authentifizieren und sichern können. Erwähnen Sie, dass sie Zertifikate für einen Benutzer, einen Computer oder einen Dienst verwalten können. Erläutern Sie, dass bei der Bereitstellung des automatisierten Geschäftsprozesses die Kanal- und Portkonfiguration auf dem Entwurf und der Konfiguration des Entwicklers basieren muss.

  Erläutern Sie, dass die Kursteilnehmer die Kanäle und Ports signieren und verschlüsseln müssen. Erläutern Sie außerdem, dass sie BizTalk-Messaging-Manager verwenden können, um bestimmte Kanäle und Ports so zu konfigurieren, dass sie bestimmte Zertifikate verwenden.

- Sichern des Zugriffs durch Firewalls

  Erläutern Sie, warum es nötig ist, Firewalls zu konfigurieren. Die Kursteilnehmer müssen wissen, welche Ports des Firewalls für BizTalk Server 2000 offen sein müssen und welche Konfigurationen für BizTalk Server 2000 am besten geeignet sind. Beschreiben Sie die Ports, die offen sein müssen. Besprechen Sie mit den Kursteilnehmern die am besten geeigneten Konfigurationen. Erläutern Sie außerdem, inwiefern diese Konfigurationen den Sicherheitsanforderungen der jeweiligen Organisation entsprechen.

Anpassungsinformationen

Dieser Abschnitt beschreibt die Anforderungen zum Einrichten der Übungseinheiten für eine Unterrichtseinheit sowie die Konfigurationsänderungen, die während der Übungseinheiten an den Kursteilnehmercomputern vorgenommen werden. Diese Informationen sollen Ihnen beim Replizieren oder Anpassen der Schulungsunterlagen für Training und Zertifizierung helfen.

Einrichten der Übungseinheit

In der folgenden Liste werden die Anforderungen zum Einrichten der Übungseinheit in dieser Unterrichtseinheit beschrieben:

Anforderung 1

Für die Übungseinheit in dieser Unterrichtseinheit müssen BizTalk Server 2000 und die erforderliche Software installiert werden, um die BizTalk Server 2000-Umgebung zu sichern. Führen Sie die folgenden Aktionen aus, damit die Kursteilnehmercomputer diese Anforderungen erfüllen:

- Schließen Sie Unterrichtseinheit 2, „Installieren von BizTalk Server 2000“, des Kurses 2387A, *Entwickeln und Bereitstellen von Microsoft BizTalk Server 2000-Lösungen*, ab.
- Schließen Sie Unterrichtseinheit 9, „Bereitstellen und Verwalten von BizTalk Server 2000-Lösungen“, des Kurses 2387A, *Entwickeln und Bereitstellen von Microsoft BizTalk Server 2000-Lösungen*, ab.

Ergebnisse der Übungseinheit

Auf den Kursteilnehmercomputern gibt es keine Konfigurationsänderungen, die die Replikation oder Anpassung betreffen.

Übersicht

Thema
Geben Sie eine Übersicht über die Themen und Lernziele dieser Unterrichtseinheit.

Einstieg
In dieser Unterrichtseinheit lernen Sie, wie die BizTalk Server 2000-Umgebung gesichert wird.

- **Einführung in das Sichern der BizTalk Server 2000-Umgebung**
- **Verwenden von Konten und Richtlinien**
- **Verwenden von Übertragungsmethoden zum Sichern von Daten**
- **Verwenden von Zertifikaten zum Sichern von Daten**
- **Sichern des Zugriffs durch Firewalls**

************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

Organisationen, in denen Microsoft® BizTalk™ Server 2000 für Geschäftstransaktionen innerhalb der Organisation und mit anderen Organisationen verwendet wird, müssen davon ausgehen können, dass die Sicherheit der Daten in diesen Transaktionen gewährleistet ist. Der Administrator- und Benutzerzugriff muss so konfiguriert sein, dass der entsprechende Zugriff zulässig ist, nicht autorisierter Zugriff dagegen verhindert wird. Sie müssen die Integrität und Vertraulichkeit der Daten und Komponenten von Geschäftstransaktionen aufrechterhalten, die mit Handelspartnern über öffentliche Netzwerke durchgeführt werden.

Sie können die Sicherheitsfeatures verwenden, die in Microsoft Windows® 2000 zur Verfügung stehen, um die BizTalk Server 2000-Umgebung zu sichern. Sie können hierfür Zugriff und Richtlinien auf Administratorebene definieren, sichere Übertragungsmethoden und Zertifikate verwenden und den Zugriff durch Firewalls sichern.

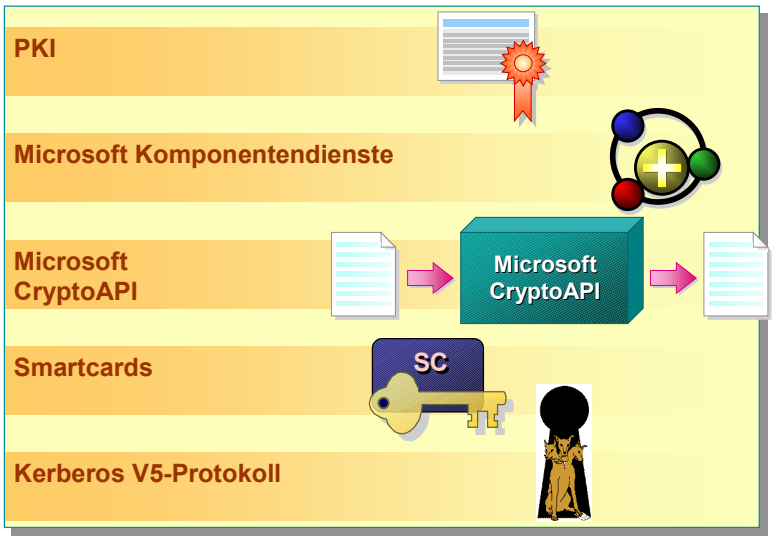
Am Ende dieser Unterrichtseinheit werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Beschreiben der Windows 2000-Features, die von BizTalk Server 2000 zum Sichern von Daten und Komponenten verwendet werden.
- Konfigurieren von Benutzerkonten und Richtlinien für einen sicheren Zugriff.
- Verwenden der Übertragungsmethoden, die BizTalk Server 2000 zum Sichern von Daten unterstützt.
- Verwenden von Zertifikaten in BizTalk Server 2000.
- Sichern des Zugriffs durch einen Firewall.

Einführung in das Sichern der BizTalk Server 2000-Umgebung

Thema
Stellen Sie die Sicherheitsfeatures von Windows 2000 und SQL Server vor, und beschreiben Sie, wie diese Features zum Sichern der BizTalk Server 2000-Umgebung verwendet werden.

Einstieg
Sie können die Sicherheitsfeatures von Windows 2000 und SQL Server verwenden, um den Austausch von Daten in und zwischen Organisationen zu sichern.



************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

BizTalk Server 2000 verwendet die Sicherheitsfeatures von Windows 2000 und Microsoft SQL Server™, um es Unternehmen zu ermöglichen, Daten auf eine sichere Weise mit Unternehmensgruppen innerhalb der Organisation und über das Internet auszutauschen.

BizTalk Server 2000 verwendet zur Gewährleistung der Sicherheit Folgendes:

- Windows 2000-Sicherheitsdienste

  BizTalk Server 2000 stellt zahlreiche Authentifizierungs- und Verschlüsselungskomponenten bereit, die die Windows 2000-Sicherheitsdienste verwenden.

- SQL Server-Sicherheit

  BizTalk Server basiert hauptsächlich auf der SQL Server-Anmeldungssicherheit, um die Sicherheit der Daten in der BizTalk-Messaging-Verwaltungsdatenbank zu gewährleisten. Die Standard-Persistenzdatenbank für die Orchestrierung von BizTalk basiert jedoch auf der Windows 2000-Authentifizierung. Beim Erstellen einer COM-Komponente (Component Object Model), die als Host für Ablaufplaninstanzen und deren Persistenzdatenbank für die Orchestrierung dient, können Sie auswählen, ob Sie die SQL Server- oder die Windows 2000-Authentifizierung verwenden möchten.

- Windows-Verwaltungsinstrumentation (Windows Management Instrumentation, WMI)

  Die BizTalk Server-Verwaltungskonsole verwendet WMI in Windows 2000.

Zu den Windows 2000-Sicherheitsfeatures, die BizTalk Server 2000 zum Sichern von Daten und Komponenten verwendet, gehören PKI (Public-Key Infrastructure), Microsoft Komponentendienste, Microsoft Cryptography Application Programming Interface (CryptoAPI), Smartcards und das Kerberos V5-Protokoll (Version 5).

Weitere Sicherheitsfunktionen von Windows 2000, die BizTalk Server 2000 verwenden kann, umfassen Unterstützung für offene PKI-Standards und sichere Protokolle, wie z. B. IPSec (Internet Protocol Security), L2TP (Layer-2-Tunneling-Protokoll), SSL/TLS (Secure Sockets Layer/Transport Layer Security) und S/MIME (Secure Multipurpose Internet Mail Extensions), damit ein Netzwerk schnell und sicher für Lieferanten und Handelspartner erweitert werden kann.

In der folgenden Tabelle werden die Sicherheitsfeatures von Windows 2000 und deren Verwendung zum Sichern der BizTalk Server 2000-Umgebung beschrieben.

Sicherheitsfeature	Sichert	Konfigurationspunkt	Konfigurations-programm
PKI	Dokumente (Signieren oder Verschlüsseln)	Ports und Kanäle	BizTalk-Messaging-Manager
Microsoft Komponentendienste	COM+-Komponenten	**Komponentendienste\ Computer\Arbeitsplatz**	Komponentendienste
Microsoft CryptoAPI	BizTalk Server 2000-Daten	Ports und Kanäle	BizTalk-Messaging-Manager
		Komponentendienste\ Computer\Arbeitsplatz	Komponentendienste
		Eigenschaften von VPN-Verbindungen (Virtuelles Privates Netzwerk), von DFÜ- und von LAN-Verbindungen (Local Area Network, lokales Netzwerk)	Netzwerk- und DFÜ-Verbindungen
		Nachrichtenwarteschlange	
Smartcards	Zertifikatbasierte Features für Netzwerk-anmeldungen, bei denen EAP (Extensible Application Protocol) verwendet wird	Eigenschaften von VPN-, DFÜ-, und LAN-Verbindungen	Netzwerk- und DFÜ-Verbindungen
Kerberos V5-Protokoll	Nachrichten	Nachrichtenwarteschlange	BizTalk-Messaging-Manager

Verwenden von Konten und Richtlinien

Thema
Beschreiben Sie, wie Administratorengruppen, Anmeldeeigenschaften, Dienstkonten und lokale Richtlinien konfiguriert werden.

Einstieg
Sie müssen die Administratorengruppen, Anmeldeeigenschaften, Dienstkonten und lokalen Richtlinien konfigurieren, um die BizTalk Server 2000-Umgebung zu sichern.

- **Administratorengruppen**
- **Anmeldeeigenschaften und Dienstkonten**
- **Lokale Richtlinien**

************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

Mit Benutzerkonten werden die Benutzer in einem Netzwerk identifiziert und authentifiziert. Die Administratorengruppen sind Gruppen, die über die erforderlichen Berechtigungen verfügen, andere Benutzerkonten zu verwalten. Ein Mitglied einer Administratorengruppe kann Benutzerkonten kontrollieren, indem Benutzern und Gruppen Zugriff auf Ressourcen im Netzwerk gewährt wird. Lokale Richtlinien bieten eine Möglichkeit, einem Benutzer den erforderlichen Zugriff zu gewähren.

Zum Sichern der BizTalk Server 2000-Umgebung müssen Sie die Gruppe **BizTalk Server-Administratoren**, die Gruppe **Windows 2000-Administratoren** und Dienstkonten konfigurieren. Außerdem müssen Sie lokale Richtlinien konfigurieren, um die Sicherheitsoptionen für ein Benutzer- oder Dienstkonto festzulegen.

Administratorengruppen

Thema
Erläutern Sie die Zugriffsebenen, die mit dem Verwalten von Servern und Servergruppen verbunden sind.

Einstieg
Um die BizTalk Server-Verwaltung anzuzeigen und zu verwenden, müssen Sie Mitglied der Gruppe **BizTalk Server-Administratoren** sein.

Zugriff	BizTalk Server 2000-Administratoren	Windows 2000-Administratoren
Hinzufügen und Entfernen von Servergruppen	X	X
Anzeigen und Ändern von Gruppeneigenschaften	X	X
Verwalten aller Warteschlangen und der Einträge	X	X
Hinzufügen und Entfernen von Empfangsfunktionen	X	X
Anzeigen und Ändern der Eigenschaften von Empfangsfunktionen	X	X
Hinzufügen und Entfernen von Servern in einer Servergruppe		X
Anzeigen und Ändern von Servereigenschaften		X
Anzeigen des Serverstatus		X
Freigeben von Austauschvorgängen auf einem Server		X

************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

In einer BizTalk Server 2000-Umgebung können Sie eines der folgenden beiden Gruppenkonten verwenden, um den Administratorzugriff auf BizTalk-Server zu sichern: **BizTalk Server-Administratoren** und **Windows 2000-Administratoren**. Wenn ein Konto zu einer oder zu beiden Gruppen gehört, verfügt der Benutzer des Kontos über die notwendigen Berechtigungen, erforderliche Administratoraufgaben durchzuführen.

Um das Tool BizTalk Server-Verwaltung anzuzeigen und zu verwenden, müssen Sie Mitglied der Gruppe **BizTalk Server-Administratoren** sein. Wenn Sie nicht als BizTalk Server-Administrator angemeldet sind, können Sie keine Elemente im Ordner **Microsoft BizTalk Server 2000** anzeigen. Wenn Sie Mitglied der Gruppe **BizTalk Server-Administratoren**, jedoch nicht Mitglied der Gruppe **Windows 2000-Administratoren** sind, können Sie nur die Aufgaben ausführen, die in der vorherigen Abbildung dargestellt sind.

Wenn Sie eine Servergruppe verwalten, müssen Sie auf jedem Server der Gruppe über Windows 2000-Administratorrechte verfügen. Die Verwaltungskonsole gibt eine Liste aller Server zurück, die der Gruppe zugeordnet sind, und gibt den Status der Server an. Wenn also auf einem oder mehreren Servern die Windows 2000-Administratorrechte geändert wurden und Sie für den Server nicht mehr über Administratorrechte verfügen, wird als Status für diese Server **Zugriff verweigert** zurückgegeben.

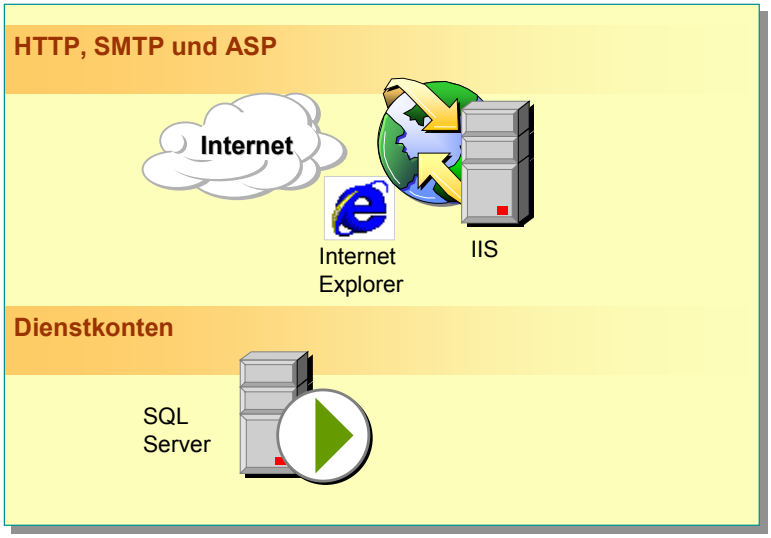
Wenn Sie sowohl Mitglied der Gruppe **BizTalk Server-Administratoren** als auch der Gruppe **Windows 2000-Administratoren** sind, können Sie alle Aufgaben ausführen, die in der vorherigen Abbildung dargestellt sind.

Anmerkung Während der Installation wird der Benutzer, der die BizTalk Server 2000-Installation ausführt, zur Gruppe **BizTalk Server-Administratoren** hinzugefügt. Mit Hilfe der Systemprogramme in der Computerverwaltung können Sie Benutzer zu den Gruppen **BizTalk Server-Administratoren** und **Windows 2000-Administratoren** hinzufügen.

Anmeldeeigenschaften und Dienstkonten

Thema
Beschreiben Sie, wie Anmeldeeigenschaften zum Sichern von Nachrichten an und von Websites verwendet werden, und erläutern Sie die Vorteile der Verwendung von Dienstkonten.

Einstieg
Sie verwenden Anmeldeeigenschaften für Nachrichten, die über HTTP, SMTP und ASP empfangen werden.



************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

Um eine BizTalk Server 2000-Umgebung zu sichern, müssen Sie die Windows 2000-Anmeldeeigenschaften sichern. Diese Eigenschaften steuern, ob sich ein Benutzer bei einem bestimmten Computer anmelden kann. Anmeldeeigenschaften erfordern die Angabe eines Benutzernamens und Kennworts, bevor auf Ressourcen wie eine Dateifreigabe oder Nachrichtenwarteschlange zugegriffen werden kann.

Sie verwenden Anmeldeeigenschaften für Nachrichten, die über HTTP (Hypertext Transfer Protocol), SMTP (Simple Mail Transfer Protocol) und ASP-Seiten (Active Server Pages) empfangen werden. Sie verwenden Anmeldeeigenschaften außerdem, um die Sicherheit des Dienstkontos zu gewährleisten.

HTTP, SMTP und ASP

Über HTTP oder SMTP empfangene Nachrichten verwenden Anmeldeeigenschaften, um die Sicherheit zu gewährleisten. Eine ASP-Seite, auf die über HTTP zugegriffen wird, kann z. B. die Eingabe eines Benutzernamens und Kennworts erfordern, ehe der Inhalt der Webseite angezeigt wird.

Dienstkonten

Ein Dienstkonto ist ein reguläres Benutzerkonto mit bestimmten Eigenschaften, durch die es als ein Teil des Betriebssystems fungieren kann. Ein interaktives Benutzerkonto ist das Konto des Benutzers, der während der Installation von BizTalk Server 2000 angemeldet ist. Ein Dienstkonto ähnelt einem interaktiven Benutzerkonto, da beide Konten einem Benutzer den Zugriff auf Computer- und Netzwerkressourcen ermöglichen.

Wenn Sie ein interaktives Benutzerkonto verwenden, kann die Anwendung nur ausgeführt werden, wenn der entsprechende Benutzer angemeldet ist. Wenn daher BizTalk Server 2000 mit einem interaktiven Benutzerkonto eingerichtet wurde, bricht das Programm ab, wenn sich der angegebene Benutzer vom Server abmeldet.

Das Auswählen einer interaktiven Benutzeridentität birgt Sicherheitsrisiken, da die Anwendung unter der Identität des angemeldeten Benutzers ohne dessen Wissen oder Zustimmung ausgeführt werden kann. Wenn z. B. die Anwendung auf einem Computer ausgeführt wird, während ein Administrator angemeldet ist, wird die Anwendung unter der Identität des Administrators ausgeführt und nimmt als solche möglicherweise Aufrufe im Auftrag von Clients vor.

Wenn die Identität auf ein Dienstkonto festgelegt ist, kann das Dienstkonto als Teil des Betriebssystems fungieren und den Benutzern den Zugriff auf Anwendungen auf einem Server ermöglichen, auch wenn der Benutzer nicht am Computer angemeldet ist.

Anmerkung COM+-Anwendungen müssen ebenfalls mit einer Identität konfiguriert werden. Die Standardkonfiguration ist für die Identität **Interaktiver Benutzer - der zurzeit angemeldete Benutzer** eingerichtet. Deshalb kann eine COM+-Anwendung ausgeführt werden, wenn ein beliebiger Benutzer angemeldet ist. Geben Sie andernfalls zum Anmelden ein Benutzerkonto für die COM-Komponente an. Das Konto muss über das Recht zum Anmelden als Batchauftrag verfügen.

Lokale Richtlinien

Thema
Beschreiben Sie, wie lokale Richtlinien verwendet werden.

Einstieg
Sie können Konfigurationseinstellungen lokaler Richtlinien dazu verwenden, die BizTalk Server 2000-Umgebung weiter zu sichern.

************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

Sie können Konfigurationseinstellungen lokaler Richtlinien dazu verwenden, die BizTalk Server 2000-Umgebung weiter zu sichern. **Lokale Richtlinien**, eine Auswahlmöglichkeit der Konsole **Lokale Sicherheitseinstellungen**, wird verwendet, um die Sicherheitsoptionen eines Benutzer- oder Dienstkontos festzulegen.

Anmerkung Um lokale Richtlinien festzulegen, zeigen Sie im Startmenü auf **Einstellungen**, klicken Sie auf **Systemsteuerung**, und doppelklicken Sie zuerst auf **Verwaltung** und dann auf **Lokale Sicherheitsrichtlinie**. Erweitern Sie anschließend den Ordner **Lokale Richtlinien**.

Lokale Richtlinien basieren auf dem Computer, an dem ein Benutzer angemeldet ist, sowie auf den Rechten, über die der Benutzer für den entsprechenden Computer verfügt. Mit lokalen Richtlinieneinstellungen werden Benutzerprivilegien und -rechte definiert. Außerdem werden sie verwendet, um die Datenintegrität aufrechtzuerhalten. Sie gelten jedoch nur für einen bestimmten Bereich und können durch globale oder Gruppenrichtlinien außer Kraft gesetzt werden. Beispielsweise könnte eine Einstellung für eine lokale Richtlinie, mit der eine minimale Kennwortlänge von 7 Zeichen festgelegt wird, von einer Gruppen- oder Domänenrichtlinie außer Kraft gesetzt werden, die mindestens 10 Zeichen für ein Kennwort erfordert.

Anmerkung Weitere Informationen zu lokalen Richtlinien finden Sie in Unterrichtseinheit 5, „Sichern von Windows 2000-basierten Computern“, des Kurses 2169A, *Entwerfen eines sicheren Microsoft Windows 2000-Netzwerkes*, und in Unterrichtseinheit 8, „Verwenden von Gruppenrichtlinien zum Verwalten von Benutzerumgebungen“, des Kurses 2175A, *Implementieren und Verwalten von Microsoft Windows 2000-Verzeichnisdiensten*.

Benutzerprivilegien und -rechte

Mit lokalen Richtlinien werden die Privilegien und Rechte von BizTalk Server 2000-Benutzern definiert. Sie können lokale Richtlinien verwenden, um Optionen für Überwachungsrichtlinien, Zuweisungen von Benutzerrechten und Sicherheit zu konfigurieren.

Datenintegrität

In der Konsole **Lokale Sicherheitseinstellungen** können weitere Richtlinien konfiguriert werden, um die Integrität der Daten in BizTalk Server 2000 aufrechtzuerhalten. Sie können beispielsweise Kontorichtlinien verwenden, um Kennwortrichtlinien und Kontosperrungsrichtlinien zu konfigurieren.

Anmerkung Weitere Informationen zu lokalen Richtlinienprivilegien und -rechten finden Sie in der BizTalk Server 2000-Hilfe.

Bereich lokaler Richtlinien

Wenn Sie die BizTalk Server 2000-Umgebung sichern, müssen Sie den Bereich der lokalen Richtlinieneinstellungen kennen, den Sie zum Sichern eines einzelnen BizTalk-Servers verwenden.

Lokale Richtlinien gelten per Definition nur lokal auf einem Computer. Wenn diese Einstellungen in ein Gruppenrichtlinienobjekt im Verzeichnisdienst Active Directory™ importiert werden, wirken sie sich auf die lokalen Sicherheitseinstellungen aller Computerkonten aus, auf die dieses Gruppenrichtlinienobjekt angewendet wird. Aus diesem Grund muss die Rangfolge für Sicherheitsrichtlinien beachtet werden.

Sicherheitsrichtlinien, die Gruppenrichtlinien zugeordnet sind, setzen auf der lokalen Ebene definierte Richtlinien außer Kraft. Auf ähnliche Weise setzen Richtlinien der Domäne lokal definierte Richtlinien außer Kraft. In jedem Fall gelten die Rechte für das Benutzerkonto nicht mehr, wenn diese Privilegien durch vorhandene lokale Richtlinieneinstellungen außer Kraft gesetzt werden.

Anmerkung Legen Sie lokale Richtlinien nicht für öffentliche Schlüssel fest. Öffentliche Schlüssel stellen einen Sicherheitsschutz für BizTalk Server 2000 bereit. Öffentliche Schlüssel sind eine Komponente der Zertifikate, die zum Ver- und Entschlüsseln von Daten verwendet werden. Wenn zu einem öffentlichen Schlüssel weitere Richtlinien hinzugefügt werden, kann BizTalk Server 2000 das zugeordnete Zertifikat nicht verwenden.

Übungseinheit 12: Überprüfen der Sicherheitseinstellungen

Thema
Geben Sie eine Einführung in die Übungseinheit.

Einstieg
In dieser Unterrichtseinheit überprüfen Sie Sicherheitseinstellungen, indem Sie die lokalen, Anmelde- und Systemkontorichtlinien anzeigen.

************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

Erläutern Sie die Lernziele der Übungseinheit.

Lernziele

Am Ende dieser Übungseinheit werden Sie in der Lage sein, die folgenden Aufgaben auszuführen:

- Anzeigen von Sicherheitseinstellungen in den Komponentendiensten und in Message Queuing.
- Anzeigen und Hinzufügen von Benutzern in den Gruppen **BizTalk Server-Administratoren** und **Windows 2000-Administratoren**.
- Erkennen der Unterschiede zwischen den Zugriffsrechten für Konten, die Mitglied einer der beiden Administratorengruppen sind.
- Anzeigen der Sicherheitseinstellungen für SQL Server 2000-Systemadministratoren und der Anmeldeeinstellungen für den BizTalk-Messagingdienst.
- Anzeigen und Bearbeiten einer lokalen Richtlinie.

Voraussetzung

Um diese Übungseinheit zu bearbeiten, müssen Sie über Kenntnisse in Bezug auf die Windows 2000-Benutzeroberfläche verfügen.

Einrichten der Übungseinheit

Um diese Übungseinheit zu bearbeiten, muss auf dem Computer Folgendes installiert sein:

- Microsoft Windows 2000 Server, Microsoft Windows 2000 Advanced Server oder Microsoft Windows 2000 Professional mit dem NTFS-Dateisystem und Service Pack 1 (SP1 und Hotfixes).
- BizTalk Server 2000 und die erforderliche zusätzliche Software.
- Microsoft Internet Explorer, Version 5.

Szenario

Als Handelspartner verwenden Northwind Traders und Contoso Ltd. automatisierte BizTalk Server 2000-Geschäftsprozesse und Servergruppen, um Geschäftsdokumente zu verarbeiten. Als Systemadministrator müssen Sie die BizTalk Server 2000-Umgebung sichern.

Als Vorbereitung auf die Sicherung der Umgebung müssen Sie die aktuellen Sicherheitseinstellungen der Komponentendienste und von Message Queuing anzeigen, Benutzer in den Gruppen **BizTalk Server-Administratoren** und **Windows 2000-Administratoren** anzeigen und hinzufügen und die Unterschiede zwischen den Zugriffsrechten dieser Konten kennen. Außerdem müssen Sie die Sicherheitseinstellungen für den SQL Server 2000-Systemadministrator und die Anmeldeeinstellungen für den BizTalk-Messagingdienst anzeigen und eine lokale Richtlinie anzeigen und bearbeiten.

Veranschlagte Zeit für die Übungseinheit: 45 Minuten

Übung 1
Anzeigen von Sicherheitseinstellungen in den Komponentendiensten und in Message Queuing

In dieser Übung zeigen Sie die aktuellen Sicherheitseinstellungen in den Komponentendiensten und in Message Queuing an.

Aufgaben	Einzelne Schritte
1. Melden Sie sich als **Administrator** am Computer an.	• Melden Sie sich als **Administrator** mit dem Kennwort **password** an.
2. Zeigen Sie die Sicherheitseinstellungen für die COM+-Anwendungen BizTalk Server Interchange Application und XLANG Scheduler an.	**a.** Zeigen Sie im Startmenü auf **Einstellungen**, und klicken Sie dann auf **Systemsteuerung**. **b.** Doppelklicken Sie auf **Verwaltung**, und doppelklicken Sie dann auf **Komponentendienste**. **c.** Maximieren Sie das Fenster **Komponentendienste**. **d.** Erweitern Sie **Komponentendienste** im linken Bereich des Fensters **Komponentendienste**, erweitern Sie **Computer**, erweitern Sie **Arbeitsplatz**, und erweitern Sie dann **COM+-Anwendungen**. **e.** Erweitern Sie **BizTalk Server Interchange Application** und **XLANG Scheduler** unter **COM+-Anwendungen**. **f.** Erweitern Sie **Komponenten** unter **BizTalk Server Interchange Application**, und erweitern Sie dann alle Komponenten und Ordner unter **Komponenten**, um den Inhalt des Ordners **Methoden** anzuzeigen. **g.** Klicken Sie unter **BizTalk Server Interchange Application** auf **Rollen**, um den Inhalt des Ordners **Rollen** anzuzeigen. **h.** Erweitern Sie **Komponenten** unter **XLANG Scheduler**, und erweitern Sie dann alle Komponenten und Ordner unter **Komponenten**, um den Inhalt des Ordners **Methoden** für alle Schnittstellen anzuzeigen. **i.** Erweitern Sie **Rollen** unter **XLANG Scheduler**, und erweitern Sie dann alle Komponenten und Ordner unter **Rollen**, um den Inhalt des Ordners **Benutzer** für alle Rollen anzuzeigen. **j.** Schließen Sie alle Fenster.
3. Zeigen Sie die Sicherheitseinstellungen für die Nachrichtenwarteschlangen an.	**a.** Öffnen Sie die Systemsteuerung. **b.** Doppelklicken Sie auf **Verwaltung**, und doppelklicken Sie dann auf **Computerverwaltung**. **c.** Maximieren Sie das Fenster **Computerverwaltung**. **d.** Erweitern Sie **Dienste und Anwendungen** im linken Bereich des Fensters **Computerverwaltung**, erweitern Sie **Message Queuing**, und erweitern Sie dann **Private Warteschlangen**. **e.** Klicken Sie unter **Private Warteschlangen** mit der rechten Maustaste auf **ContosoPOQueue**. *Wenn **ContosoPOQueue** nicht aufgeführt ist, befinden Sie sich nicht auf dem Server von Contoso Ltd. Klicken Sie dann stattdessen mit der rechten Maustaste auf **admin_queue$**.*

3. *(Fortsetzung)*

f. Klicken Sie auf **Eigenschaften**.

g. Zeigen Sie im Eigenschaftendialogfeld auf der Registerkarte **Sicherheitseinstellungen** die Sicherheitseinstellungen an.

*Auf der Registerkarte **Sicherheitseinstellungen** werden die Benutzer und Gruppen, die auf die Warteschlange zugreifen können, sowie die entsprechenden Berechtigungen für die Benutzer und Gruppen angezeigt. Notieren Sie sich die Benutzer und Gruppen, damit Sie die Frage zur Übung beantworten können.*

h. Klicken Sie auf **Erweitert**, und klicken Sie dann auf die Registerkarten **Berechtigungen** und **Überwachung**, um die darauf angezeigten Einträge anzuzeigen.

i. Beachten Sie den Eintrag unter **Aktueller Besitzer dieses Elements** und die Benutzer und Gruppen unter **Besitzer ändern auf** auf der Registerkarte **Besitzer**.

j. Klicken Sie zweimal auf **Abbrechen**, und schließen Sie dann alle Fenster.

Nennen Sie die Message Queuing-Benutzer und -Gruppen und deren Berechtigungen. Geben Sie ein Beispiel dafür, wann diese Einstellungen geändert werden sollten.

Übung 2
Anzeigen und Hinzufügen von Benutzern zu den Administratorengruppen

In dieser Übung zeigen Sie Benutzer in den Gruppen **BizTalk Server-Administratoren** und **Windows 2000-Administratoren** an und fügen Benutzer hinzu. Sie können Benutzern den Zugriff auf die BizTalk Server 2000-Verwaltungsfunktionen gewähren, indem Sie die Benutzer zu einer oder zu beiden Administratorengruppen hinzufügen.

Aufgaben	Einzelne Schritte
1. Erstellen Sie drei Benutzerkonten: **BTAdmin1**, **WinAdmin1** und **BTWinAdmin1**.	**a.** Öffnen Sie die Systemsteuerung. **b.** Doppelklicken Sie auf **Verwaltung**, und doppelklicken Sie dann auf **Computerverwaltung**. **c.** Maximieren Sie das Fenster **Computerverwaltung**. **d.** Erweitern Sie **Lokale Benutzer und Gruppen** im linken Bereich des Fensters **Computerverwaltung** unter **Systemprogramme**. **e.** Klicken Sie mit der rechten Maustaste auf **Benutzer**, und klicken Sie dann auf **Neuer Benutzer**. **f.** Geben Sie in den entsprechenden Feldern die folgenden Informationen ein: • **Benutzername**: **BTAdmin1** • **Vollständiger Name**: **BTAdmin1** • **Beschreibung**: <leer> • **Kennwort**: **password** • **Kennwort bestätigen**: **password** **g.** Deaktivieren Sie das Kontrollkästchen **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**. **h.** Aktivieren Sie das Kontrollkästchen **Kennwort läuft nie ab**, und klicken Sie dann auf **Erstellen**. **i.** Geben Sie in den entsprechenden Feldern die folgenden Informationen ein: • **Benutzername**: **WinAdmin1** • **Vollständiger Name**: **WinAdmin1** • **Beschreibung**: <leer> • **Kennwort**: **password** • **Kennwort bestätigen**: **password** **j.** Deaktivieren Sie das Kontrollkästchen **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**. **k.** Aktivieren Sie das Kontrollkästchen **Kennwort läuft nie ab**, und klicken Sie dann auf **Erstellen**.

1. *(Fortsetzung)*	**l.** Geben Sie in den entsprechenden Feldern die folgenden Informationen ein: • **Benutzername**: **BTWinAdmin1** • **Vollständiger Name**: **BTWinAdmin1** • **Beschreibung**: <leer> • **Kennwort**: **password** • **Kennwort bestätigen**: **password** **m.** Deaktivieren Sie das Kontrollkästchen **Benutzer muss Kennwort bei der nächsten Anmeldung ändern**. **n.** Aktivieren Sie das Kontrollkästchen **Kennwort läuft nie ab**. **o.** Klicken Sie auf **Erstellen**, und klicken Sie dann auf **Schließen**.
2. Nehmen Sie die Benutzerkonten **WinAdmin1** und **BTWinAdmin1** in die Gruppe **Windows 2000-Administratoren** und die Benutzerkonten **BTAdmin1** und **BTWinAdmin1** in die Gruppe **BizTalk Server-Administratoren** auf.	**a.** Klicken Sie im linken Bereich des Fensters **Computerverwaltung** unter **Lokale Benutzer und Gruppen** auf **Gruppen**. **b.** Doppelklicken Sie im rechten Bereich des Fenster **Computerverwaltung** auf **Administratoren**. **c.** Klicken Sie im Dialogfeld **Eigenschaften von Administratoren** auf **Hinzufügen**. **d.** Scrollen Sie im Dialogfeld **Benutzer oder Gruppen auswählen** in der Liste **Name** zu **WinAdmin1**, doppelklicken Sie auf **WinAdmin1**, und klicken Sie dann auf **OK**. **e.** Klicken Sie im Dialogfeld **Eigenschaften von Administratoren** auf **Hinzufügen**. **f.** Scrollen Sie im Dialogfeld **Benutzer oder Gruppen auswählen** in der Liste **Name** zu **BTWinAdmin1**, doppelklicken Sie auf **BTWinAdmin1**, und klicken Sie dann auf **OK**. **g.** Doppelklicken Sie im rechten Bereich des Fensters **Computerverwaltung** auf **BizTalk Server-Administratoren**. *Die Beschreibung lautet wie folgt:* ***Mitglieder können Microsoft BizTalk Server 2000 vollständig verwalten****. Standardmäßig sind das Administratorkonto und die Gruppe* ***VORDEFINIERT\Administratoren*** *Mitglieder der Gruppe* ***BizTalk Server-Administratoren****.* **h.** Klicken Sie im Dialogfeld **Eigenschaften von BizTalk Server-Administratoren** auf **Hinzufügen**. **i.** Scrollen Sie im Dialogfeld **Benutzer oder Gruppen auswählen** in der Liste **Name** zu **BTAdmin1**, doppelklicken Sie auf **BTAdmin1**, und klicken Sie dann auf **OK**. **j.** Klicken Sie im Dialogfeld **Eigenschaften von BizTalk Server-Administratoren** auf **Hinzufügen**. **k.** Scrollen Sie im Dialogfeld **Benutzer oder Gruppen auswählen** in der Liste **Name** zu **BTWinAdmin1**, doppelklicken Sie auf **BTWinAdmin1**, und klicken Sie dann auf **OK**. **l.** Schließen Sie alle Fenster.

Verfügt **WinAdmin1** über BizTalk Server 2000-Administratorprivilegien? Falls ja, warum? Falls nicht, warum nicht?

Übung 3
Verwenden von Konten der Administratorengruppe

Melden Sie sich in dieser Übung mit Hilfe eines Kontos an, das zur Gruppe **BizTalk Server-Administratoren** oder zur Gruppe **Windows 2000-Administratoren** gehört. Beachten Sie die Unterschiede zwischen den Zugriffsrechten der beiden Konten.

Aufgaben	Einzelne Schritte
1. Melden Sie sich als **BTAdmin1** am Computer an.	• Melden Sie sich als **BTAdmin1** mit dem Kennwort **password** an.
2. Zeigen Sie den BizTalk Server-Status an.	**a.** Klicken Sie auf **Start**, zeigen Sie auf **Programme**, zeigen Sie auf **Microsoft BizTalk Server 2000**, und klicken Sie dann auf **BizTalk Server-Verwaltung**. **b.** Maximieren Sie das Fenster **BizTalk Server-Verwaltung**. **c.** Erweitern Sie **Microsoft BizTalk Server 2000** im linken Bereich des Fensters **BizTalk Server-Verwaltung**, und erweitern Sie anschließend **BizTalk Server-Gruppe**. **d.** Klicken Sie im linken Bereich auf den Servernamen des Servers. *Der Status des Servers ist **Zugriff verweigert**.* **e.** Klicken Sie mit der rechten Maustaste auf den Servernamen des Servers. *Es ist kein Eintrag **Eigenschaften** verfügbar, wenn Sie mit der rechten Maustaste auf den Servernamen klicken. Auch die Option **Alle Tasks** oder **Alle Tasks/Austauschvorgänge freigeben** ist nicht verfügbar. Außerdem ist keine Option zum Löschen des Servers vorhanden.* **f.** Schließen Sie alle Fenster.
3. Melden Sie sich als **WinAdmin1** am Computer an.	• Melden Sie sich als **WinAdmin1** mit dem Kennwort **password** an.
4. Zeigen Sie den BizTalk Server-Status an.	**a.** Öffnen Sie die BizTalk Server-Verwaltung. **b.** Maximieren Sie das Fenster **BizTalk Server-Verwaltung**. **c.** Erweitern Sie **Microsoft BizTalk Server 2000** im linken Bereich des Fensters **BizTalk Server-Verwaltung**. *Es wird folgender Fehler der BizTalk Server-Verwaltung angezeigt: „Instanzen von MicrosoftBizTalkServer_Group können nicht aufgezählt werden: Der Zugriff auf die BizTalk Server-Verwaltungskonsole wird aufgrund eines Fehlers im Authentifizierungsvorgang verweigert. Der Benutzer ist nicht Mitglied der BizTalk Server-Verwaltungsgruppe.“* **d.** Klicken Sie auf **OK**.

4. *(Fortsetzung)*	**e.** Klicken Sie auf **Microsoft BizTalk Server 2000**. *Es wird folgender Fehler der BizTalk Server-Verwaltung angezeigt: „Keine ausreichende Berechtigung: Der Zugriff auf die BizTalk Server-Verwaltungskonsole wird aufgrund eines Fehlers beim Authentifizierungsvorgang verweigert. Der Benutzer ist nicht Mitglied der BizTalk Server-Verwaltungsgruppe.“* **f.** Klicken Sie auf **OK**. **g.** Schließen Sie alle Fenster.
5. Melden Sie sich als **BTWinAdmin1** am Computer an.	• Melden Sie sich als **BTWinAdmin1** mit dem Kennwort **password** an.
6. Zeigen Sie den BizTalk Server-Status an.	**a.** Öffnen Sie die BizTalk Server-Verwaltung. **b.** Maximieren Sie das Fenster **BizTalk Server-Verwaltung**. **c.** Erweitern Sie **Microsoft BizTalk Server 2000** im linken Bereich des Fensters **BizTalk Server-Verwaltung**, und erweitern Sie anschließend **BizTalk Server-Gruppe**. **d.** Klicken Sie im linken Bereich auf den Servernamen des Servers. *Der Status des Servers ist **Wird ausgeführt**.* **e.** Klicken Sie mit der rechten Maustaste auf den Servernamen des Servers. *Es ist ein Eintrag **Eigenschaften** verfügbar, wenn Sie mit der rechten Maustaste auf den Servernamen klicken. Auch die Optionen **Alle Tasks** und **Alle Tasks/Austauschvorgänge freigeben** sind verfügbar. Außerdem ist eine Option zum Löschen des Servers vorhanden.* **f.** Schließen Sie alle Fenster.

Übung 4
Anzeigen der Sicherheitseinstellungen für den Systemadministrator und Bearbeiten einer lokalen Richtlinie

In dieser Übung zeigen Sie die Sicherheitseinstellungen für den SQL Server 2000-Systemadministrator und die Anmeldeeinstellungen für den BizTalk-Messagingdienst an. Außerdem zeigen Sie eine lokale Richtlinie an, und bearbeiten diese.

Aufgaben	Einzelne Schritte
1. Zeigen Sie die Sicherheitseinstellungen für den SQL Server 2000-Systemadministrator an.	**a.** Zeigen Sie im Startmenü auf **Programme**, zeigen Sie auf **Microsoft SQL Server**, und klicken Sie dann auf **Enterprise Manager**. **b.** Maximieren Sie im Fenster **SQL Server Enterprise Manager** den Konsolenstamm. **c.** Erweitern Sie **Microsoft SQL Server** im linken Bereich des Fensters **SQL Server Enterprise Manager**, erweitern Sie **SQL Server-Gruppe**, und erweitern Sie anschließend den Eintrag für Ihren Server. **d.** Erweitern Sie unter dem Eintrag für Ihren Server **Sicherheit**, und klicken Sie dann auf **Benutzernamen**. **e.** Klicken Sie im rechten Bereich mit der rechten Maustaste auf **sa**, und klicken Sie dann auf **Eigenschaften**. **f.** Zeigen Sie auf der Registerkarte **Allgemein** die allgemeinen Einstellungen für das Systemadministratorkonto an. **g.** Zeigen Sie auf der Registerkarte **Serverrollen** die Einstellungen für Serverrollen für das Systemadministratorkonto an. **h.** Zeigen Sie auf der Registerkarte **Datenbankzugriff** die Einstellungen für den Datenbankzugriff für das Systemadministratorkonto an. **i.** Schließen Sie alle Fenster.
2. Zeigen Sie die Anmeldeeinstellungen für den BizTalk-Messagingdienst an.	**a.** Zeigen Sie im Startmenü auf **Einstellungen**, und klicken Sie dann auf **Systemsteuerung**. **b.** Doppelklicken Sie auf **Verwaltung**, und doppelklicken Sie dann auf **Computerverwaltung**. **c.** Maximieren Sie das Fenster **Computerverwaltung**. **d.** Erweitern Sie im linken Bereich **Dienste und Anwendungen**, und klicken Sie dann auf **Dienste**. **e.** Klicken Sie im rechten Bereich mit der rechten Maustaste auf **BizTalk-Messagingdienst**, und klicken Sie dann auf **Eigenschaften**. **f.** Klicken Sie im Dialogfeld **Eigenschaften von BizTalk-Messagingdienst (Lokaler Computer)** auf die Registerkarte **Anmelden**.  *Der BizTalk-Messagingdienst ist so konfiguriert, dass er mit dem lokalen Systemkonto angemeldet werden.* **g.** Schließen Sie alle Fenster.

3. Zeigen Sie eine lokale Richtlinie an, und bearbeiten Sie diese.	**a.** Öffnen Sie die Systemsteuerung. **b.** Doppelklicken Sie auf **Verwaltung**, und doppelklicken Sie dann auf **Lokale Sicherheitsrichtlinie**. **c.** Maximieren Sie das Fenster **Lokale Sicherheitseinstellungen**. **d.** Erweitern Sie **Kontorichtlinien** im Fenster **Lokale Sicherheits-einstellungen**, und klicken Sie dann auf die Ordner **Kennwort-richtlinie** und **Kontosperrungsrichtlinien**, um deren Inhalt anzuzeigen. **e.** Erweitern Sie im linken Bereich **Lokale Richtlinien**, und klicken Sie dann auf **Überwachungsrichtlinie**. **f.** Doppelklicken Sie im rechten Bereich auf **Anmeldeereignisse überwachen**. **g.** Aktivieren Sie im Dialogfeld **Lokale Sicherheitsrichtlinie** unter **Einstellung der lokalen Richtlinie** die Kontrollkästchen **Erfolgreich** und **Fehlgeschlagen**, und klicken Sie dann auf **OK**. **h.** Doppelklicken Sie im rechten Bereich auf **Objektzugriffsversuche überwachen**. **i.** Aktivieren Sie im Dialogfeld **Lokale Sicherheitsrichtlinie** unter **Einstellung der lokalen Richtlinie** die Kontrollkästchen **Erfolgreich** und **Fehlgeschlagen**, und klicken Sie dann auf **OK**. **j.** Schließen Sie alle Fenster. **k.** Melden Sie sich ab, und melden Sie sich dann als **Administrator** mit dem Kennwort **password** an. **l.** Zeigen Sie im Startmenü auf **Programme**, zeigen Sie auf **Microsoft BizTalk Server 2000**, und klicken Sie dann auf **BizTalk Server-Verwaltung**. **m.** Maximieren Sie das Fenster **BizTalk Server-Verwaltung**. **n.** Erweitern Sie im linken Bereich **Ereignisanzeige (Lokal)**, und klicken Sie dann auf **Sicherheit**. *Das Protokoll **Sicherheit** enthält Ereignisse, die als Ergebnis von Richtlinienänderungen protokolliert werden. Die Ereignisse resultieren aus dem An- und Abmelden.* **o.** Schließen Sie alle Fenster.
4. Machen Sie die in Aufgabe 2 vorgenommenen Richtlinienänderungen rückgängig.	**a.** Öffnen Sie die Systemsteuerung. **b.** Doppelklicken Sie auf **Verwaltung**, und doppelklicken Sie dann auf **Lokale Sicherheitsrichtlinie**. **c.** Maximieren Sie das Fenster **Lokale Sicherheitseinstellungen**. **d.** Erweitern Sie **Kontorichtlinien** im Fenster **Lokale Sicherheits-einstellungen**, und klicken Sie dann auf die Ordner **Kennwort-richtlinie** und **Kontosperrungsrichtlinien**, um deren Inhalt anzuzeigen. **e.** Erweitern Sie im linken Bereich **Lokale Richtlinien**, und klicken Sie dann auf **Überwachungsrichtlinie**. **f.** Doppelklicken Sie im rechten Bereich auf **Anmeldeereignisse überwachen**.

4. *(Fortsetzung)*

g. Deaktivieren Sie im Dialogfeld **Lokale Sicherheitsrichtlinie** unter **Einstellung der lokalen Richtlinie** die Kontrollkästchen **Erfolgreich** und **Fehlgeschlagen**, und klicken Sie dann auf **OK**.

h. Doppelklicken Sie im rechten Bereich auf **Objektzugriffsversuche überwachen**.

i. Deaktivieren Sie im Dialogfeld **Lokale Sicherheitsrichtlinie** unter **Einstellung der lokalen Richtlinie** die Kontrollkästchen **Erfolgreich** und **Fehlgeschlagen**, und klicken Sie dann auf **OK**.

j. Schließen Sie alle Fenster.

k. Melden Sie sich ab, und melden Sie sich dann als **Administrator** mit dem Kennwort **password** an.

l. Öffnen Sie die BizTalk Server-Verwaltung.

m. Maximieren Sie das Fenster **BizTalk Server-Verwaltung**.

n. Erweitern Sie im linken Bereich **Ereignisanzeige (Lokal)**, und klicken Sie dann auf **Sicherheit**.

*Das Protokoll **Sicherheit** enthält Ereignisse, die als Ergebnis von Richtlinienänderungen protokolliert werden. Die Ereignisse werden nicht mehr durch An- und Abmelden ausgelöst.*

o. Schließen Sie alle Fenster.

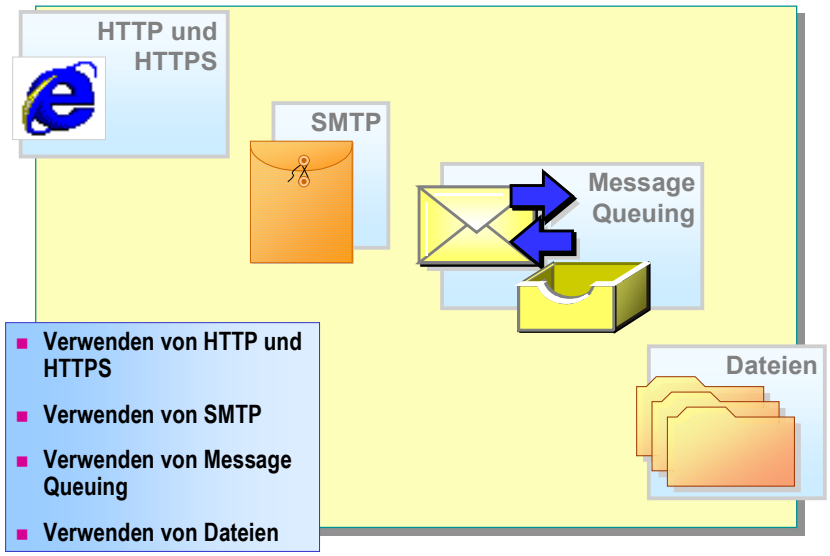
Welchen Einfluss hat das Ändern der Kontoeinstellungen für den SQL Server 2000-Systemadministrator auf die BizTalk Server 2000-Umgebung?

Welche Ereignisse wurden durch Änderungen an der lokalen Richtlinie verursacht?

Verwenden von Übertragungsmethoden zum Sichern von Daten

Thema
Geben Sie eine Einführung in die Themen, die sich auf das Sichern des Datenaustauschs mit Hilfe von Übertragungsmethoden beziehen.

Einstieg
Sie müssen außerdem die in der BizTalk Server 2000-Umgebung verwendete Übertragungsmethode sichern.
BizTalk Server 2000 unterstützt HTTP, HTTPS, SMTP, Message Queuing und Dateien.



************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

Sie müssen außerdem die in der BizTalk Server 2000-Umgebung verwendete Übertragungsmethode sichern. BizTalk Server 2000 unterstützt eine Hauptgruppe von Transportdiensten. Durch diese Transportdienste kann der Server Dokumente an Organisationen oder Anwendungen senden, unabhängig davon, ob die Anwendungen mit Hilfe einer COM-Schnittstelle direkt mit dem Server kommunizieren können. BizTalk Server 2000 unterstützt die folgenden Transportdienste: HTTP und HTTPS (Hypertext Transfer Protocol Secure), SMTP, Message Queuing, Version 2.0, und Dateien.

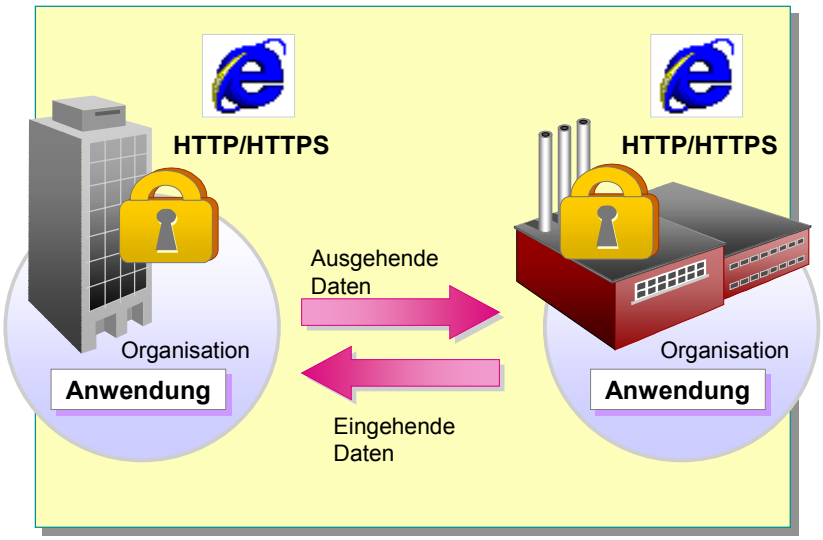
Sie werden die Übertragungsmethode bereitstellen, die der Entwickler beim Entwickeln des automatisierten Geschäftsprozesses ausgewählt hat. Sie können die vier Übertragungsmethoden so konfigurieren, dass ausgehende und eingehende Daten sicher transportiert werden.

Als Entwickler haben Sie möglicherweise die Übertragungsmethode bereits so konfiguriert, dass die Sicherheit gewährleistet ist. Sie müssen die Sicherheit der Übertragungsmethode überprüfen und gegebenenfalls Maßnahmen zum Sichern der Übertragungsmethode ergreifen.

Verwenden von HTTP und HTTPS

Thema
Beschreiben Sie die Verwendung von HTTP und HTTPS zum Sichern von Daten.

Einstieg
Sie können HTTP und HTTPS zum sicheren Transport von ausgehenden und eingehenden Daten verwenden.



************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

BizTalk Server 2000 kann HTTPS verwenden, um Daten auf sichere Weise innerhalb einer Organisation oder mit Handelspartnern über HTTP auszutauschen. Sie können diese beiden Transportdienste zum sicheren Transport von ausgehenden und eingehenden Daten verwenden.

Anmerkung Weitere Informationen zu HTTP und HTTPS finden Sie in der BizTalk Server 2000-Hilfe.

Sichern von ausgehenden Datenübertragungen

Sie können die HTTPS-Transportdienste verwenden, um sichere Daten an eine Anwendung oder einen Handelspartner zu senden. Die Sicherheit dieser Transportdienste basiert auf Zertifikaten, mit denen die Daten digital signiert und verschlüsselt werden.

Vor dem Senden von Daten über HTTPS sendet ein BizTalk Server-Administrator z. B. eine Kopie eines Clientzertifikats an einen Handelspartner. Der Handelspartner behält eine Kopie des Zertifikats im BizTalk Server 2000-Zertifikatspeicher. Von dem Zeitpunkt an wird das Zertifikat verwendet, um den Handelspartner zu authentifizieren, der Daten sendet.

Sichern von eingehenden Datenübertragungen

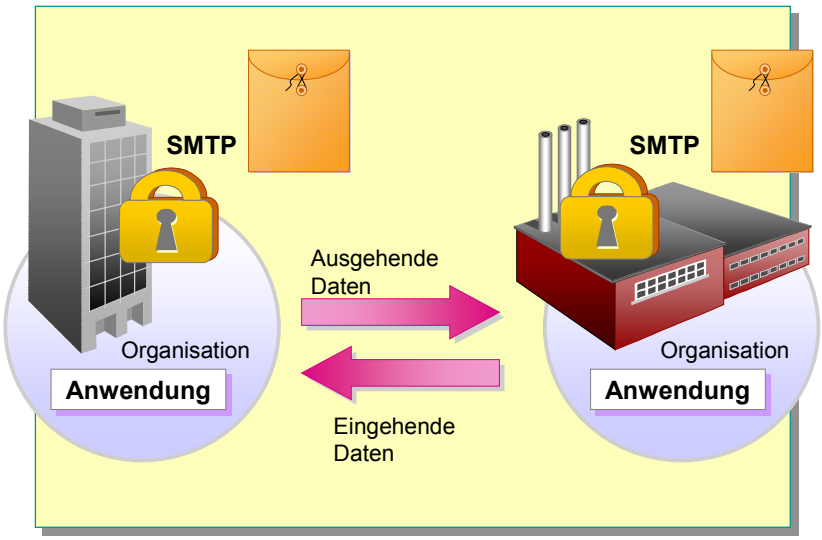
BizTalk Server 2000 kann Daten über HTTP mit Hilfe der Microsoft Internet-Informationsdienste (Internet Information Services, IIS) und ASP-Seiten empfangen. Beim Verwenden von HTTPS zum Verbinden mit IIS handeln Client und Browser ein gemeinsames Protokoll aus, um den Kanal zu sichern.

In Fällen, in denen Server und Client mehrere Protokolle gemeinsam haben, schützt IIS den Kanal mit einem unterstützten Protokoll, wie z. B. SSL. Die ASP-Seite dient als Mechanismus für das Senden von Daten an BizTalk Server 2000. Wenn die Daten sicher sind, werden Sie von BizTalk Server 2000 empfangen. Der ASP-Code verwendet die **Submit**-Methode oder die **SubmitSync**-Methode für einen Aufruf.

Verwenden von SMTP

Thema
Beschreiben Sie, wie SMTP gesichert wird.

Einstieg
Sie können SMTP verwenden, um ausgehende und eingehende Daten innerhalb einer Organisation oder mit einem Handelspartner sicher auszutauschen.



************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

SMTP ist ein Protokoll für das Senden von E-Mail-Nachrichten zwischen Servern, das für das Senden von E-Mail-Nachrichten über das Internet weit verbreitet ist. Sie können SMTP verwenden, um ausgehende und eingehende Daten innerhalb einer Organisation oder mit einem Handelspartner sicher auszutauschen.

Anmerkung Weitere Informationen zu SMTP finden Sie in der BizTalk Server 2000-Hilfe.

Sichern von ausgehenden Datenübertragungen

BizTalk Server 2000 implementiert ein Transportprotokoll, um Daten über SMTP zu senden. Die Mindestanforderung ist, dass die SMTP-Daten MIME-codiert sind. Durch diesen Vorgang kann BizTalk Server 2000 identifizieren, wo eine Datenmenge endet und die nächste beginnt. Die MIME-Codierung bietet jedoch keine Sicherheit.

Die sichere Version von MIME ist S/MIME. Dokumente, die mit Hilfe integrierter S/MIME-Codierungskomponenten verschlüsselt werden, stellen die Dokumentintegrität, die Authentifizierung des Absenders und die Datenverschlüsselung sicher. BizTalk Server 2000 erstellt ein S/MIME-Dokument mit der verschlüsselten Nachricht als Textkörper des Dokuments. Der MIME-codierten Nachricht muss ein Zertifikat zugeordnet werden, um diese Sicherheitsebene hinzuzufügen.

Sie können MIME-Codierung angeben, wenn Sie Messagingports in BizTalk-Messaging-Manager erstellen. Hier werden auch die Zertifikate angegeben.

Sichern von eingehenden Datenübertragungen

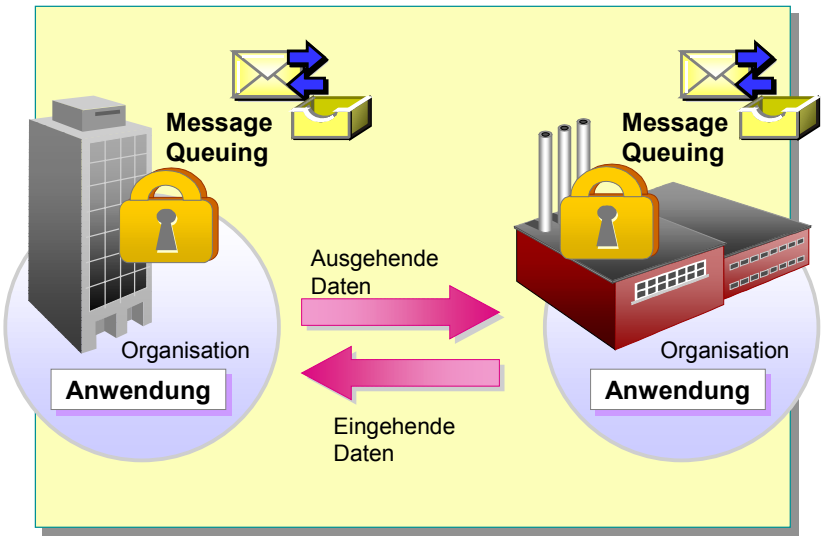
Sie müssen mit Hilfe von Microsoft Exchange Server ein Empfangskonto für BizTalk Server 2000 erstellen, um die Sicherheit auf der Empfängerseite von SMTP zu implementieren. Nach dem Einrichten des Kontos können Handelspartner ihre öffentlichen Schlüssel an Exchange Server senden, mit denen der Absender (Handelspartner) authentifiziert wird. Die öffentlichen Schlüssel werden zum Exchange Server-Zertifikatspeicher hinzugefügt.

Wenn Exchange Server eine Nachricht empfängt, sendet die **Submit**-Methode die Daten an BizTalk Server 2000. BizTalk Server 2000 vergleicht das Zertifikat mit dem öffentlichen Schlüssel. Bei einer Übereinstimmung entschlüsselt BizTalk Server 2000 die Daten und verarbeitet dann das Dokument.

Verwenden von Message Queuing

Thema
Beschreiben Sie, wie Message Queuing für den Austausch von Daten konfiguriert wird.

Einstieg
Sie können Message Queuing verwenden, um Nachrichten und deren Inhalt zu sichern.



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Message Queuing ist die wichtigste Anforderung für einen automatisierten Geschäftsprozess, in dem eine lose gekoppelte Architektur für die Übertragung und Verarbeitung von Dokumenten verwendet wird. Um Nachrichten und deren Inhalt zu sichern, müssen Sie sicherstellen, dass Message Queuing sicher ist. Message Queuing nutzt auch das in Windows 2000 enthaltene Sicherheitsprotokoll Kerberos V5 und unterstützt darüber hinaus die 128-Bit- und 40-Bit-Verschlüsselung.

Anmerkung Weitere Informationen zu Message Queuing finden Sie in Unterrichtseinheit 9, „Bereitstellen und Verwalten von BizTalk Server 2000-Lösungen“, des Kurses 2387A, *Entwickeln und Bereitstellen von Microsoft BizTalk Server 2000-Lösungen*.

Sie können Message Queuing konfigurieren, um ausgehende und eingehende Daten innerhalb einer Organisation oder mit einem Handelspartner sicher auszutauschen.

Sichern von ausgehenden Datenübertragungen

Wenn Sie Daten in Message Queuing speichern oder daraus abrufen, müssen Sie einen Benutzernamen und ein Kennwort verwenden. Message Queuing kann Daten speichern, die über ein Zertifikat verfügen. Mit Hilfe von BizTalk-Messaging-Manager können Benutzer ein Zertifikat für Daten angeben, die in einer Nachrichtenwarteschlange gespeichert sind.

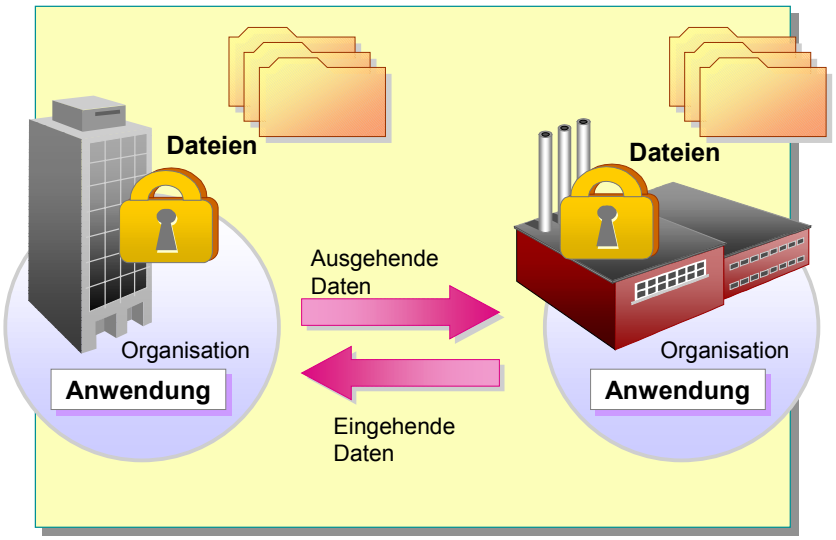
Sichern von eingehenden Datenübertragungen

Wenn Sie Anmeldeeigenschaften für eine Nachrichtenwarteschlange erstellen, müssen zum Abrufen der Daten ein Benutzername und ein Kennwort verwendet werden. Das Erstellen von Anmeldeeigenschaften stellt eine grundlegende Sicherheitsebene dar.

Verwenden von Dateien

Thema
Beschreiben Sie, wie die Dateispeicherung für den sicheren Austausch von Daten konfiguriert wird.

Einstieg
Um den Datenaustausch in BizTalk Server 2000 zu sichern, müssen Sie die Dateispeicherung konfigurieren, um sicherzustellen, dass die von den Empfangsfunktionen übernommenen Dateien sicher sind.



************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

Windows 2000 sichert Daten- und Systemschutz durch das Definieren einer Dateizugriffssteuerung. Das Windows-NTFS-Dateisystem ist erforderlich für BizTalk Server 2000 und kann verhindern, dass Benutzer wichtige System- oder Anwendungsdateien beschädigen. NTFS bietet ferner eine zuverlässige Sicherheit für die unterstützenden Dateien in einer Anwendung.

Sie können die Dateispeicherung so konfigurieren, dass ausgehende und eingehende Daten innerhalb einer Organisation und mit einem Handelspartner sicher ausgetauscht werden. BizTalk Server 2000 unterstützt Dateiempfangsfunktionen und Message Queuing-Empfangsfunktionen. Um den Datenaustausch in BizTalk Server 2000 zu sichern, müssen Sie deshalb die Dateispeicherung konfigurieren, um sicherzustellen, dass die von den Empfangsfunktionen übernommenen Dateien sicher sind.

Anmerkung Weitere Informationen zur Verwendung der Dateispeicherung als Übertragungsmethode finden Sie in der BizTalk Server 2000-Hilfe.

Sichern von ausgehenden Datenübertragungen

Die erste Sicherheitsebene für die Dateispeicherung ist ein Benutzername und ein Kennwort. Jeder Benutzer, der Daten in einem Ordner speichert oder daraus abruft, muss einen Benutzernamen und ein Kennwort verwenden. Darüber hinaus können in Ordnern Daten gespeichert werden, die über ein zugeordnetes Zertifikat verfügen. Erstellen Sie mit BizTalk-Messaging-Manager ein Zertifikat für die Daten, die in einem Ordner gespeichert werden sollen, um diese weitere Sicherheitsebene zu verwenden.

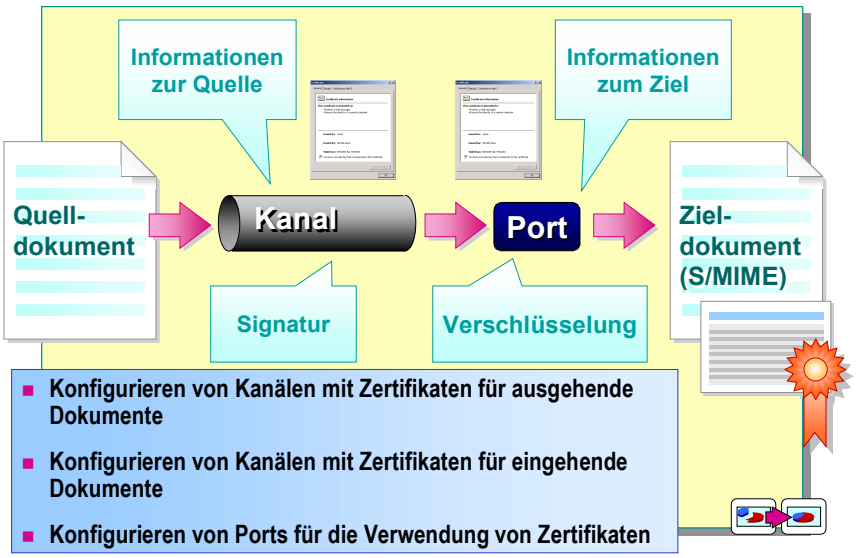
Sichern von eingehenden Datenübertragungen

Wenn auf einen Ordner Anmeldeeigenschaften angewendet wurden, müssen zum Abrufen der Daten ein Benutzername und ein Kennwort verwendet werden. Sie können für bestimmte Benutzer verschiedene Zugriffsstufen (Lesen, Löschen usw.) für das Dateiverzeichnis bestimmen. Eingehende Dokumente können auch digital signiert werden, um sicherzustellen, dass der Absender nicht leugnen kann, das Dokument gesendet zu haben.

◆ Verwenden von Zertifikaten zum Sichern von Daten

Thema
Beschreiben Sie, wie Kanäle und Ports so konfiguriert werden, dass sie Zertifikate zum Sichern von Daten verwenden.

Einstieg
Sie verwenden Zertifikate für die Authentifizierung und die Sicherheit des Austauschs von Informationen in ungesicherten Netzwerken. Sie können Zertifikate für einen Benutzer, einen Computer oder einen Dienst verwalten.



************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

Sie können Zertifikate für die Authentifizierung und die Sicherheit des Austauschs von Informationen in ungesicherten Netzwerken, wie z. B. dem Internet, verwenden. Sie können Zertifikate für einen Benutzer, einen Computer oder einen Dienst verwalten.

Der Entwickler erstellt und konfiguriert Kanäle und Ports beim Erstellen und Kompilieren des automatisierten Geschäftsprozesses. Der Entwickler kann außerdem Zertifikate verwenden, um beim Entwurf die Kanäle und Ports zu signieren und zu verschlüsseln. Bei der Bereitstellung des automatisierten Geschäftsprozesses muss die Kanal- und Portkonfiguration auf dem Entwurf und der Konfiguration des Entwicklers basieren.

Da Ihre Bereitstellung dem Entwurf des Entwicklers entsprechen muss, müssen Sie die Kanäle und Ports signieren und verschlüsseln. Verwenden Sie BizTalk-Messaging-Manager, um bestimmte Kanäle und Ports so zu konfigurieren, dass sie bestimmte Zertifikate verwenden.

Digitale Zertifikate binden einen kryptografischen Schlüssel an ein oder mehrere Attribute eines Benutzers. Zertifikate können zum Signieren (eindeutige Identifikation eines Benutzers) oder zum Verschlüsseln (Codieren) von Informationen verwendet werden. Die von Zertifizierungsstellen ausgestellten Zertifikate schützen das Internet, indem die Authentizität von Netzwerknachrichten zugesichert wird.

Anmerkung Weitere Informationen zu PKI und Zertifikaten finden Sie in der BizTalk Server 2000-Hilfe und in Unterrichtseinheit 14, „Entwerfen einer PKI“, des Kurses 2169A, *Entwerfen eines sicheren Microsoft Windows 2000-Netzwerkes*.

Um Zertifikate zum Sichern von Daten in der BizTalk Server 2000-Umgebung zu verwenden, müssen Sie wissen, wie Sie Zertifikate für Daten in BizTalk Server 2000 erhalten und verwenden. Außerdem müssen Sie die Unterschiede zwischen Computerschlüsseln und Benutzerschlüsseln kennen.

Verwenden von Zertifikaten in BizTalk Server 2000

BizTalk Server 2000 ist in hohem Maße auf die Sicherheit angewiesen, die durch Zertifikate bereitgestellt wird. Durch die Verwendung öffentlicher Schlüssel zur Verschlüsselung der Daten und privater Schlüssel zur Datenentschlüsselung kann BizTalk Server 2000 vertrauenswürdige Daten senden und gewährleisten, dass die verarbeiteten Daten sicher sind.

Die zur MMC (Microsoft Management Console) gehörenden Richtlinien öffentlicher Schlüssel ermöglichen die Konfiguration von Agents für die Wiederherstellung verschlüsselter Daten für das verschlüsselnde Dateisystem (Encrypting File System, EFS), domänenweite Stammzertifizierungsstellen, vertraute Zertifizierungsstellen usw. Zertifikate enthalten ferner digitale Signaturen, die auf Dokumente angewendet und bei eingehenden Dokumenten mit Hilfe der systemeigenen Unterstützung von BizTalk Server 2000 für digitale Signaturen überprüft werden können.

Sie können Zertifikate in BizTalk Server 2000 mit Hilfe von BizTalk-Messaging-Manager konfigurieren. Zertifikate erleichtern die Ver- und Entschlüsselung von Daten sowie ihre digitale Signatur. Transportdienste in BizTalk Server 2000 unterstützen die Technologie der Verschlüsselung öffentlicher Schlüssel für alle Dokumente, die von BizTalk Server 2000 übertragen werden. BizTalk Server 2000 unterstützt außerdem die Entschlüsselung und Signaturüberprüfung für alle empfangenen Dokumente.

Computerschlüssel im Vergleich zu Benutzerschlüsseln

Beim Abrufen von Zertifikaten sollten dem Computer zugeordnete Computerschlüssel anstelle von Benutzerschlüsseln, die dem angemeldeten Benutzer zugeordnet sind, verwendet werden.

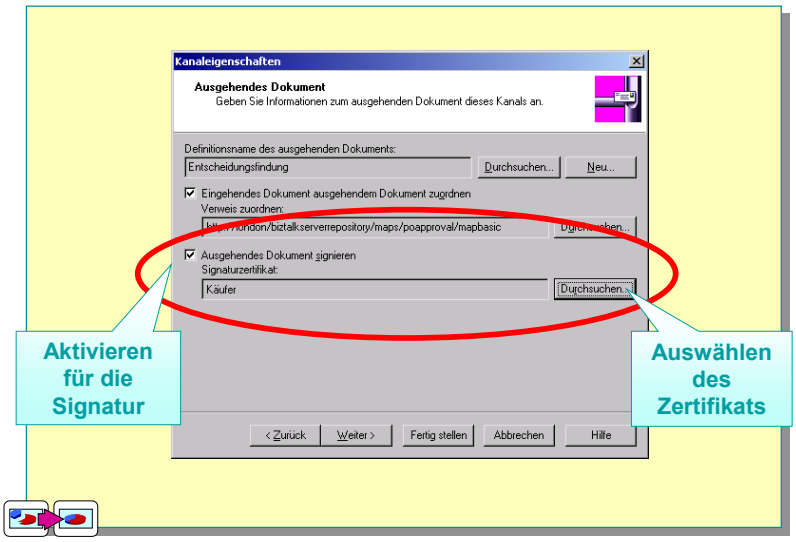
Wenn ein aktuell an einem Server angemeldeter Benutzer ein Zertifikat mit Benutzerschlüsseln abruft, kann nur dieser Benutzer auf das Zertifikat zugreifen, da der Benutzerschlüssel des Zertifikats die Anmeldeinformationen des Benutzers enthält. Wenn demnach Benutzer auf Zertifikate mit Benutzerschlüsseln in BizTalk Server 2000 zugreifen müssen, muss BizTalk Server im Kontext dieses Benutzers ausgeführt werden. Damit alle Benutzer sich bei BizTalk Server 2000 anmelden und auf Schlüssel zugreifen können, müssen Zertifikate über Computerschlüssel verfügen.

Damit BizTalk Server 2000 auf **Zertifikate (Lokaler Computer)** zugreifen kann, muss BizTalk Server 2000 als LocalSystem oder Administrator ausgeführt werden. Wenn Benutzerschlüssel verwendet werden, muss BizTalk Server im Kontext eines Benutzers ausgeführt werden, der auch Administrator sein muss.

Konfigurieren von Kanälen mit Zertifikaten für ausgehende Dokumente

Thema
Beschreiben Sie, wie Kanäle mit Zertifikaten für ausgehende Dokumente konfiguriert werden.

Einstieg
Sie können ein Zertifikat angeben, um die ausgehenden Dokumente für einen Kanal zu signieren.



************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

Sie können ein Zertifikat angeben, um die ausgehenden Dokumente für einen Kanal zu signieren.

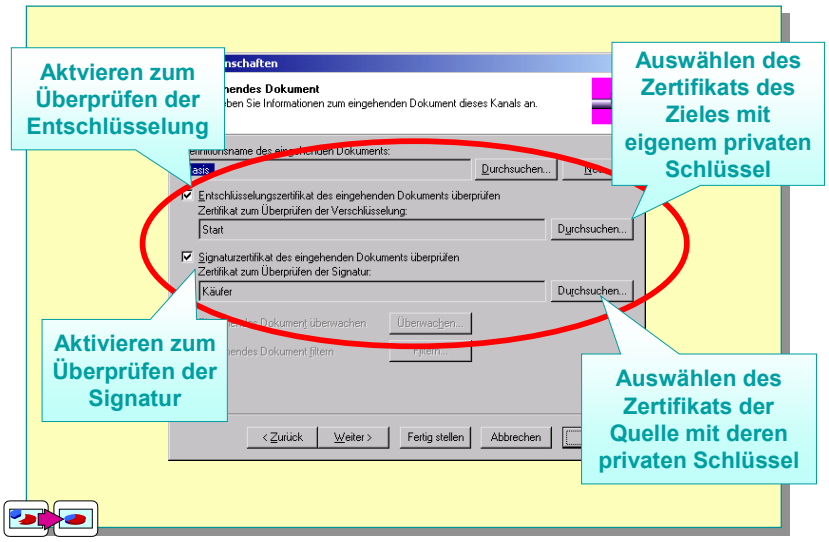
Um ein Zertifikat für das ausgehende Dokument für einen bestimmten Kanal anzugeben, können Sie BizTalk-Messaging-Manager verwenden und die Eigenschaften des Kanals konfigurieren, für den die Dokumente signiert werden müssen. So konfigurieren Sie die Eigenschaften:

1. Aktivieren Sie auf der Seite **Ausgehendes Dokument** des Kanal-Assistenten das Kontrollkästchen **Ausgehendes Dokument signieren**.
2. Klicken Sie rechts neben dem Feld **Signaturzertifikat** auf **Durchsuchen**.
3. Klicken Sie im Dialogfeld **Signaturzertifikat auswählen** in der Liste **Zertifikatsname** auf einen Zertifikatsnamen, und klicken Sie dann auf **OK**.

Konfigurieren von Kanälen mit Zertifikaten für eingehende Dokumente

Thema
Beschreiben Sie, wie Kanäle mit Zertifikaten für eingehende Dokumente konfiguriert werden.

Einstieg
Sie können Zertifikatsinformationen für eingehende Dokumente für einen Kanal angeben.



************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

Sie können Zertifikatsinformationen für eingehende Dokumente für einen Kanal angeben. Sie können Folgendes angeben:

- Die Entschlüsselung muss überprüft und das Zertifikat des Zieles angegeben werden.
- Eine Signatur muss überprüft und das Zertifikat der Quelle des Dokuments angegeben werden.

Sie verwenden dazu BizTalk-Messaging-Manager und konfigurieren die Eigenschaften für den Kanal, für dessen Dokumente Signaturen erforderlich sind.

So wählen Sie ein Zertifikat zum Überprüfen der Entschlüsselung aus:

1. Aktivieren Sie auf der Seite **Eingehendes Dokument** des Kanal-Assistenten das Kontrollkästchen **Entschlüsselungszertifikat des eingehenden Dokuments überprüfen**.
2. Klicken Sie anschließend rechts neben dem Feld **Zertifikat zum Überprüfen der Verschlüsselung** auf **Durchsuchen**.
3. Klicken Sie im Dialogfeld **Zertifikat zum Überprüfen der Entschlüsselung auswählen** in der Liste **Zertifikatsname** auf einen Zertifikatsnamen, und klicken Sie dann auf **OK**.

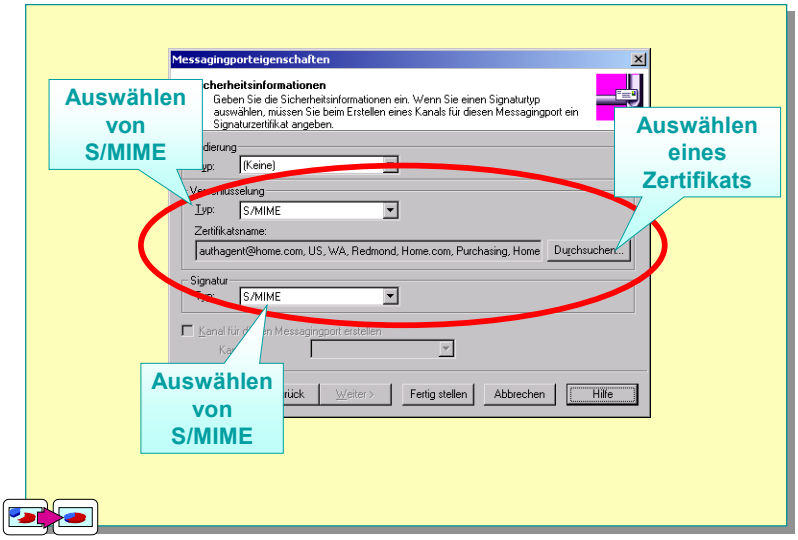
So wählen Sie ein Zertifikat zum Überprüfen der Signatur eingehender Dokumente aus:

1. Aktivieren Sie auf der Seite **Eingehendes Dokument** des Kanal-Assistenten das Kontrollkästchen **Signaturzertifikat des eingehenden Dokuments überprüfen**.
2. Klicken Sie anschließend rechts neben dem Feld **Zertifikat zum Überprüfen der Signatur** auf **Durchsuchen**.
3. Klicken Sie im Dialogfeld **Zertifikat zum Überprüfen der Signatur auswählen** in der Liste **Zertifikatsname** auf einen Zertifikatsnamen, und klicken Sie dann auf **OK**.

Konfigurieren von Ports für die Verwendung von Zertifikaten

Thema
Beschreiben Sie, wie Ports für die Verwendung von Zertifikaten konfiguriert werden.

Einstieg
Sie können Sicherheitsinformationen für einen Port angeben.



************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

Sie können Sicherheitsinformationen für einen Port angeben. Sie können Folgendes angeben:

- S/MIME muss für die Verschlüsselung verwendet und ein entsprechendes Zertifikat ausgewählt werden.
- S/MIME muss für einen Signaturtyp verwendet werden.

Sie verwenden dazu BizTalk-Messaging-Manager und konfigurieren die Eigenschaften für den Port.

So wählen Sie ein Zertifikat zur Verwendung für die Verschlüsselung aus:

1. Klicken Sie im Messagingport-Assistenten auf der Seite **Sicherheitsinformationen** unter **Verschlüsselung** in der Liste **Typ** auf **S/MIME** und dann auf **Durchsuchen**.
2. Klicken Sie im Dialogfeld **Verschlüsselungszertifikat auswählen** in der Liste **Zertifikatsname** auf einen Zertifikatsnamen, und klicken Sie dann auf **OK**.

So wählen Sie einen Signaturtyp aus:

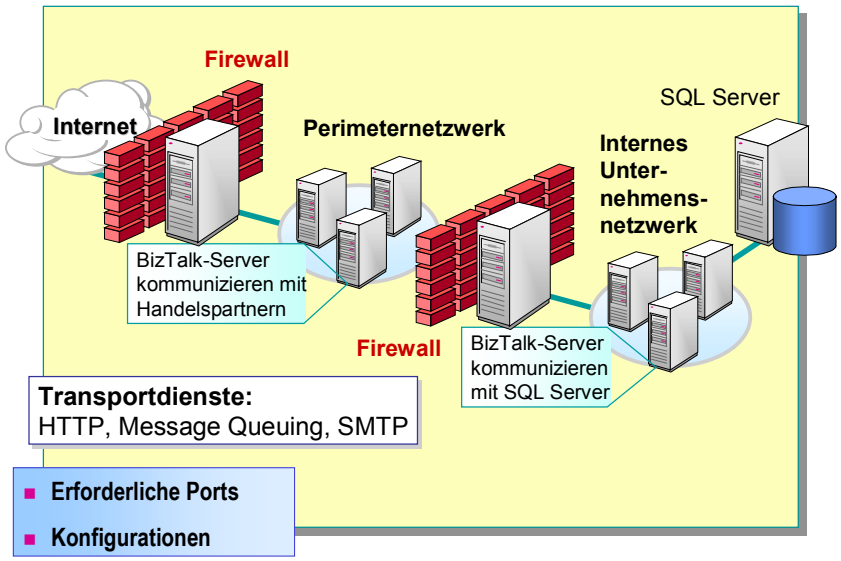
- Klicken Sie im Messagingport-Assistenten auf der Seite **Sicherheits-informationen** unter **Signatur** in der Liste **Typ** auf eine der folgenden Optionen:
  - **(Keine)**. Keine Signatur wird angegeben. Dies ist die Standard-einstellung.
  - **S/MIME**. Eine Signatur mit S/MIME wird angegeben.
  - **Benutzerdefiniert**. Gibt die Codierung an, die eine benutzerdefinierte Signaturkomponente verwendet.

Anmerkung Sie können nur dann eine benutzerdefinierte Signaturkomponente angeben und den Klassenbezeichner (Class Identifier, CLSID) konfigurieren, wenn Sie das BizTalk-Messaging-Konfigurationsobjektmodell verwenden.

Sichern des Zugriffs durch Firewalls

Thema
Beschreiben Sie, wie sicherer Zugriff durch einen Firewall bereitgestellt wird, indem Ports implementiert werden.

Einstieg
Unabhängig davon, ob Sie den Firewall selbst konfigurieren, müssen Sie wissen, welche Ports des Firewalls für BizTalk Server 2000 offen sein müssen und welche Konfigurationen für BizTalk Server 2000 am besten geeignet sind.



**********NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG**********

Ein weiterer Aspekt der BizTalk Server 2000-Umgebung, den Sie für die Sicherheit der Umgebung konfigurieren müssen, ist der Firewall. Unabhängig davon, ob Sie den Firewall selbst konfigurieren oder eine Konfigurationsänderung des Firewalls anfordern, müssen Sie wissen, welche Ports des Firewalls für BizTalk Server 2000 offen sein müssen und welche Konfigurationen für BizTalk Server 2000 am besten geeignet sind.

Anmerkung Firewalls bieten Unterstützung bei der Sicherung interner Netzwerke, führen jedoch zu Wartezeiten und unter Umständen zu Einzelpunkt-Versagen. Selbst wenn ein Mechanismus für den Lastenausgleich verwendet wird, um das Einzelpunkt-Versagen zu vermeiden, kann ein Firewall die Netzwerkleistung reduzieren.

Erforderliche Ports

Damit die BizTalk-Server miteinander und mit den Handelspartnern kommunizieren können, müssen Ports in mindestens einem Firewall offen sein. Die Ports, die offen sein müssen, hängen von den verwendeten Transportdiensten und der ausgewählten Firewallkonfiguration ab.

Für die folgenden in BizTalk Server 2000 verwendeten Transportdienste gelten folgende Ports:

- SMTP: TCP-Port 25 (Transmission Control Protocol)
- HTTP: TCP-Port 80

Anmerkung Für den Firewall des Unternehmens können Ports zu Protokollen neu zugewiesen werden. Weitere Informationen zur Zuweisung von Ports zu Protokollen finden Sie in der IANA-Registrierung (Internet Assigned Numbers Authority) zugewiesener Protokoll- und Portnummern unter **http://www.iana.org/numbers.htm**. Weitere Informationen zum Konfigurieren von Firewalls für bestimmte Protokolle und Ports finden Sie in Unterrichtseinheit 3, „Einrichten des sicheren Internetzugriffs“, des Kurses 2161A, *Microsoft Internet Security & Acceleration Server einsetzen und verwalten*.

Konfigurationen

Beim Konfigurieren einer BizTalk Server 2000-Umgebung sind im Wesentlichen zwei Konfigurationen empfehlenswert. Die ausgewählte Konfiguration sollte diejenige sein, die am besten mit der Sicherheitsarchitektur des Unternehmens übereinstimmt. Die folgenden beiden Konfigurationen werden empfohlen:

- Konfiguration A. Die BizTalk-Server befinden sich in einem Perimeternetzwerk und einem internen Unternehmensnetzwerk.
- Konfiguration B. Die BizTalk-Server befinden sich nur in einem Unternehmensnetzwerk.

BizTalk-Server in einem Perimeternetzwerk und einem internen Unternehmensnetzwerk

Installieren Sie die BizTalk-Server mit Ausnahme der Server, die mit den Handelspartnern kommunizieren, in einem internen Netzwerk. Installieren Sie die Server, die Sie für die direkte Kommunikation mit den Handelspartnern verwenden, in einem Perimeternetzwerk des Unternehmens.

Das Perimeternetzwerk ist die Begrenzung zwischen dem Internet und einer externen Sicherheitsbegrenzung des internen Netzwerkes. Die externe Sicherheitsbegrenzung ist normalerweise eine Kombination aus Firewalls und Bastionshosts, die Gateways zwischen inneren und äußeren Netzwerken darstellen.

Eine Firma, die eigene Internetdienste verwalten und den nicht autorisierten Zugriff auf ihr privates Netzwerk auf ein Mindestmaß reduzieren möchte, verwendet ein Perimeternetzwerk. Die Server im Perimeternetzwerk sollten lokale Transportdienste verwenden, wie z. B. HTTP, Message Queuing oder SMTP. In dieser Umgebung durchlaufen alle eingehenden und/oder ausgehenden Transaktionen einen Firewall. Die Server im Perimeternetzwerk senden Dokumente über einen weiteren Firewall an SQL Server.

Diese Konfiguration ermöglicht Servern im Perimeternetzwerk, wie z. B. BizTalk Server 2000 und ein HTTP-Webserver, über einen internen Firewall mit SQL Server zu kommunizieren.

BizTalk-Server nur in einem Unternehmensnetzwerk

Installieren Sie die BizTalk-Server nur in einem Unternehmensnetzwerk. Handelspartner, die Dokumente über das Internet austauschen, senden ihre Daten mit Hilfe von SMTP/HTTP-Servern im Perimeternetzwerk (erster Schutzfirewall). Diese Server senden die Daten dann über einen zweiten Firewall an die Server im Firmennetzwerk.

Anmerkung Durch beide Konfigurationen wird die Leistung beeinträchtigt. Um einen nennenswerten Leistungsabfall zu vermeiden, können Sie den Firewall so einrichten, dass eine bestimmte Anzahl von Transaktionen zwischen der Organisation und ihren Handelspartnern möglich ist. Weitere Informationen zur Firewallkonfiguration finden Sie in Unterrichtseinheit 6, „Konfigurieren eines Firewalls“, des Kurses 2161A, *Microsoft Internet Security & Acceleration Server einsetzen und verwalten*.

Lernzielkontrolle

Thema
Vertiefen Sie die Lernziele dieser Unterrichtseinheit, indem Sie die Kernpunkte wiederholen.

Einstieg
Die Fragen zur Lernzielkontrolle beziehen sich auf einige der Schlüsselkonzepte, die Inhalt dieser Unterrichtseinheit sind.

- **Einführung in das Sichern der BizTalk Server 2000-Umgebung**
- **Verwenden von Konten und Richtlinien**
- **Verwenden von Übertragungsmethoden zum Sichern von Daten**
- **Verwenden von Zertifikaten zum Sichern von Daten**
- **Sichern des Zugriffs durch Firewalls**

************NUR FÜR DIE VERWENDUNG DURCH DEN KURSLEITER ZULÄSSIG************

1. Sie sind der BizTalk Server-Administrator von Contoso Ltd., und Sie untersuchen Methoden zum Sichern der BizTalk Server 2000-Umgebung. Welche drei Optionen zum Sichern der Umgebung bietet BizTalk Server 2000?

   Windows 2000-Sicherheitsdienste, SQL Server-Sicherheit und Windows-Verwaltungsinstrumentation in Windows 2000.

2. Welche Windows 2000-Sicherheitsfeatures werden in BizTalk Server 2000 genutzt, die Sie zum Sichern der Umgebung verwenden können?

   PKI, Microsoft Komponentendienste, CryptoAPI, Smartcards und das Kerberos V5-Protokoll.

3. Sie haben gerade für Ihren BizTalk-Server ein Benutzerkonto zur Gruppe **BizTalk Server-Administratoren** hinzugefügt. Welche zusätzlichen BizTalk Server 2000-Funktionen könnte der Benutzer des Kontos ausführen, wenn Sie das Konto auch zur Gruppe **Windows 2000-Administratoren** hinzufügen?

   Hinzufügen und Entfernen von Servern in einer Servergruppe, Anzeigen und Ändern von Servereigenschaften, Anzeigen des Serverstatus und Freigeben von Austauschvorgängen auf einem Server.

4. Sie verwenden Message Queuing als Übertragungsmethode. Womit können Sie Message Queuing sichern?

   Sie können eine Benutzer-ID und ein Kennwort oder ein Zertifikat zum Speichern oder Abrufen von Daten in Message Queuing verwenden.

5. Sie implementieren die Zertifikatskonfiguration, die der Entwickler in der Testumgebung erstellt hat. Welche BizTalk-Messaging-Verwaltungsobjekte wurden wahrscheinlich so konfiguriert, dass sie im automatisierten Geschäftsprozess des Entwicklers Zertifikate verwenden?

   Ein Zertifikat zum Signieren ausgehender Dokumente für einen Kanal.

   Zertifikate zum Überprüfen der Entschlüsselung (Ziel) und der Signatur (Quelle) eingehender Dokumente für einen Kanal.

   Zertifikate für einen Port für Verschlüsselung und Signatur mit S/MIME.

6. Sie müssen eine Anforderung an den Firewalladministrator senden, um sicherzustellen, dass bestimmte Ports im inneren Firewall für die BizTalk Server 2000-Implementierung offen sind, um Informationen an die Handelspartner zu übertragen und von den Handelspartnern zu empfangen. Nennen Sie die Übertragungsmethode und den entsprechenden TCP-Port, die bzw. der in der Anforderung angezeigt wird.

   SMTP: TCP-Port 25.

   HTTP: TCP-Port 80.