

OFFIZIELLES MICROSOFT LEARNING - PRODUKT

10225A

**Installieren und Konfigurieren von
Windows® 7 Client**

Assistenteninhalte

Die in diesem Dokument enthaltenen Angaben und Daten, einschließlich URLs und anderer Verweise auf Internetwebsites, können ohne vorherige Ankündigung geändert werden. Die in den Beispielen verwendeten Namen von Firmen, Organisationen, Produkten, Domänen, E-Mail-Adressen, Logos, Personen sowie Orten und Ereignissen sind frei erfunden, soweit nichts anderes angegeben ist. Jede Ähnlichkeit mit tatsächlichen Firmen, Organisationen, Produkten, Domänen, E-Mail-Adressen, Logos, Personen, Orten und Ereignissen ist rein zufällig. Die Benutzer sind für das Einhalten aller geltenden Urheberrechtsgesetze verantwortlich. Unabhängig von der Anwendbarkeit der entsprechenden Urheberrechtsgesetze darf ohne ausdrückliche schriftliche Erlaubnis der Microsoft Corporation kein Teil dieses Dokuments für irgendwelche Zwecke vervielfältigt oder in einem Datenempfangssystem gespeichert oder darin eingelesen werden, unabhängig davon, auf welche Art und Weise oder mit welchen Mitteln (elektronisch, mechanisch, durch Fotokopieren, Aufzeichnen usw.) dies geschieht.

Microsoft Corporation kann Inhaber von Patenten oder Patentanträgen, Marken, Urheberrechten oder anderen gewerblichen Schutzrechten sein, die den Inhalt dieses Dokuments betreffen. Das Bereitstellen dieses Dokuments gibt Ihnen jedoch keinen Anspruch auf diese Patente, Marken, Urheberrechte oder auf sonstiges geistiges Eigentum, es sei denn, dies wird ausdrücklich in den schriftlichen Lizenzverträgen von Microsoft eingeräumt.

Die Namen von Herstellern und Produkten sowie URLs werden nur zu Informationszwecken bereitgestellt, und Microsoft schließt im Zusammenhang mit den Herstellern oder der Verwendung der Produkte mit Microsoft-Technologien jede Gewährleistung aus, sei sie ausdrücklich, konkludent oder gesetzlich geregelt. Die Nennung eines Herstellers oder Produkts impliziert nicht, dass Microsoft den Hersteller oder das Produkt unterstützt. Es können Hyperlinks zu Sites von Drittanbietern aufgeführt werden. Diese Sites stehen nicht unter der Verwaltung von Microsoft. Microsoft ist nicht verantwortlich für den Inhalt von Websites, die durch Hyperlinks verbunden sind, für Hyperlinks auf diesen Websites oder für die Änderungen bzw. Aktualisierungen solcher Websites. Microsoft ist nicht für Webcasting oder andere Übertragungsformen verantwortlich, die von anderen durch Hyperlinks verbundenen Websites empfangen werden. Die Tatsache, dass Microsoft Hyperlinks von anderen Websites einschließt, bedeutet nicht, dass Microsoft mit dem Inhalt dieser Sites oder den Produkten übereinstimmt. Microsoft stellt Ihnen diese Links vielmehr nur als Service zur Verfügung.

© 2009 Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft und die unter <http://www.microsoft.com/about/legal/en/us/IntellectualProperty/Trademarks/EN-US.aspx> aufgeführten Marken sind Marken der Unternehmen der Microsoft-Gruppe. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber.

Produktnummer: 10225A

Veröffentlicht: 08/2011

MICROSOFT-LIZENZBESTIMMUNGEN

OFFICIAL MICROSOFT LEARNING PRODUCTS COURSEWARE – STUDENT EDITION – Vorabversionen und endgültige Versionen

Diese Lizenzbestimmungen sind ein Vertrag zwischen Microsoft Corporation und Ihnen. Bitte lesen Sie die Lizenzbestimmungen aufmerksam durch. Sie gelten für die oben genannten lizenzierten Inhalte und gegebenenfalls für die Medien, auf denen Sie diese erhalten haben, sowie für alle von Microsoft diesbezüglich angebotenen

- Updates
- Ergänzungen
- Internetbasierten Dienste
- Supportleistungen

Liegen letztgenannten Elementen eigene Bestimmungen bei, gelten diese eigenen Bestimmungen.

Durch die Verwendung der lizenzierten Inhalte erkennen Sie diese Bestimmungen an. Falls Sie die Bestimmungen nicht akzeptieren, sind Sie nicht berechtigt, die lizenzierten Inhalte zu verwenden.

Wenn Sie diese Lizenzbestimmungen einhalten, verfügen Sie über die nachfolgend aufgeführten Rechte.

1. ÜBERBLICK.

Lizenzierte Inhalte. Die lizenzierten Inhalte umfassen Software, gedruckte Materialien, akademische Materialien (im Online- oder elektronischen Format) und dazugehörige Medien.

Lizenzmodell. Die lizenzierten Inhalte werden auf der Basis pro Kopie pro Gerät lizenziert.

2. RECHTE ZUR INSTALLATION UND NUTZUNG.

- Lizenziertes Gerät.** Das lizenzierte Gerät ist das Gerät, auf dem Sie die lizenzierten Inhalte verwenden. Sie sind berechtigt, eine Kopie der lizenzierten Inhalte auf dem lizenzierten Gerät zu installieren und zu verwenden.
- Tragbares Gerät.** Sie sind berechtigt, eine weitere Kopie auf einem tragbaren Gerät zur Verwendung durch die einzige Hauptnutzerin oder den einzigen Hauptnutzer des lizenzierten Geräts zu installieren.
- Trennung von Komponenten.** Die Komponenten der lizenzierten Inhalte werden als eine Einheit lizenziert. Sie sind nicht berechtigt, die Komponenten zu trennen und auf unterschiedlichen Geräten zu installieren.
- Drittanbieterprogramme.** Die lizenzierten Inhalte können Drittanbieterprogramme enthalten. Diese Lizenzbestimmungen gelten für Ihre Verwendung dieser Drittanbieterprogramme, es sei denn, diesen Programmen liegen andere Bestimmungen bei.

3. VORABVERSIONEN.

Wenn es sich bei den lizenzierten Inhalten um eine Vorabversion („Betaversion“) handelt, finden zusätzlich zu den anderen Bestimmungen in diesem Vertrag die folgenden Bestimmungen ebenfalls Anwendung:

- Lizenzierte Vorabinhalte.** Bei diesen lizenzierten Inhalten handelt es sich um eine Vorabversion. Die Informationen und/oder die Funktionsweise der endgültigen Version kann sich von der der Vorabversion unterscheiden. Wir sind berechtigt, Änderungen an der endgültigen Version für den Handel vorzunehmen. Des Weiteren sind wir berechtigt, keine Handelsausgabe auf den Markt zu bringen. Sie werden alle Kursteilnehmer, die an einer Autorisierten Schulungssitzung teilnehmen, sowie alle Kursleiter,

die Schulungen in solchen Autorisierten Schulungssitzungen bereitstellen, deutlich und auffällig über das Vorgenannte sowie darüber informieren, dass weder Sie noch Microsoft einer Verpflichtung unterliegen, ihnen weitere Inhalte bereitzustellen, einschließlich, aber nicht beschränkt auf die endgültige Version der Lizenzierten Inhalte für den Kurs.

- b. Feedback.** Wenn Sie sich damit einverstanden erklären, Microsoft Feedback zu den lizenzierten Inhalten zu geben, berechtigen Sie Microsoft, Ihr Feedback zu verwenden, an Dritte weiterzugeben und für kommerzielle Zwecke und in jeglicher Weise und für jeglichen Zweck zu nutzen, ohne dafür Gebühren zu berechnen. Des Weiteren treten Sie jegliche Patentrechte an Drittparteien für deren Produkte, Technologien und Dienste ab, die zur Verwendung mit oder als Schnittstelle für spezifische Teile einer Microsoft-Software, von lizenzierten Inhalten von Microsoft oder eines Microsoft-Dienstes dienen, für den bzw. die Ihr Feedback verwendet wurde. Sie geben kein Feedback, das unter einen Lizenzvertrag fällt, der es erforderlich macht, dass Microsoft ihre Software oder Dokumentation für Drittparteien lizenziert, weil wir Ihr Feedback für diese verwenden. Diese Rechte sind über die Laufzeit dieses Vertrags hinaus gültig.
- c. Vertrauliche Informationen.** Die lizenzierten Inhalte, einschließlich aller Viewer, Benutzeroberflächen, Features und Dokumentation, die möglicherweise in den lizenzierten Inhalten enthalten sind, sind vertrauliche Informationen und Eigentum von Microsoft und deren Lieferanten.
- i. Nutzung.** Sie dürfen diese vertraulichen Informationen erst fünf Jahre nach der Installation der lizenzierten Inhalte bzw. ihrer Kommerzialisierung, je nachdem, welcher Zeitpunkt früher ist, an Dritte weitergeben. Sie dürfen vertrauliche Informationen nur an Ihre Mitarbeiter und Berater weitergeben, die diese Informationen zur Erfüllung ihrer Aufgaben benötigen. Sie müssen schriftliche Erklärungen von diesen einholen, die besagen, dass sie die vertraulichen Informationen mindestens in dem durch diesen Vertrag festgelegten Maße schützen.
- ii. Fortgeltung.** Ihre Pflicht, die vertraulichen Informationen zu schützen, besteht über die Laufzeit dieses Vertrags hinaus.
- iii. Ausschluss.** Sie dürfen vertrauliche Informationen weitergeben, um einer gerichtlichen Verfügung oder behördlichen Anordnung nachzukommen. Vorher müssen Sie Microsoft jedoch schriftlich davon unterrichten und somit die Möglichkeit geben, eine Schutzanordnung anzustreben oder die Informationen auf andere Weise zu schützen. Zu den vertraulichen Informationen gehören nicht Informationen, die
- ohne Verschulden öffentlich bekannt werden,
 - Sie von einer Drittpartei erhalten haben, die damit nicht ihre Vertraulichkeitsverpflichtungen gegenüber Microsoft oder ihren Lieferanten verletzt hat,
 - Sie eigenständig entwickelt haben.
- d. Laufzeit.** Die Laufzeit dieses Vertrags für Vorabversionen dauert bis zu (i) dem Datum, das nach Auskunft von Microsoft das Enddatum für die Nutzung der Betaversion ist, oder (ii) der Kommerzialisierung der endgültigen Version der lizenzierten Inhalte, wobei das frühere Ereignis maßgeblich ist („Beta-Laufzeit“).
- e. Nutzung.** Sie werden die Nutzung aller Kopien der Betaversion bei Ablauf oder Kündigung der Beta-Laufzeit einstellen und alle Kopien derselben, die sich in Ihrem Besitz oder unter Ihrer Kontrolle befinden, vernichten.
- f. Kopien.** Microsoft wird Autorisierte Lernzentren informieren, wenn sie berechtigt sind, Kopien der Betaversion (entweder als gedruckte und/oder CD-Version) anzufertigen und diese Kopien an Kursteilnehmer und/oder Kursleiter weiterzugeben. Wenn Microsoft eine solche Weitergabe erlaubt, werden Sie alle zusätzlichen Bestimmungen einhalten, die Microsoft Ihnen für solche Kopien und eine solche Weitergabe bereitstellt.

4. ZUSÄTZLICHE LIZENZANFORDERUNGEN UND/ODER NUTZUNGSRECHTE.

- a. Medienelemente und Vorlagen.** Sie sind berechtigt, Bilder, ClipArt, Animationen, Ton, Musik, Shapes, Videoclips und Vorlagen, die mit den lizenzierten Inhalten bereitgestellt werden, ausschließlich zu Ihrer persönlichen Schulungsverwendung zu nutzen. Wenn Sie diese Medienelemente oder Vorlagen zu irgendeinem anderen Zweck verwenden möchten, besuchen Sie www.microsoft.com/permission, um zu erfahren, ob eine entsprechende Verwendung gestattet ist.
- b. Akademische Materialien.** Wenn die lizenzierten Inhalte akademische Materialien enthalten (z. B. Whitepapers, praktische Übungen, Tests, Datenblätter und FAQs), sind Sie berechtigt, die akademischen Materialien zu kopieren und zu verwenden. Sie sind nicht berechtigt, Änderungen an den akademischen Materialien vorzunehmen, und Sie sind nicht berechtigt, ein vollständiges Buch (weder in elektronischer noch in gedruckter Version) zu drucken. Wenn Sie akademische Materialien vervielfältigen, erklären Sie sich mit Folgendem einverstanden:
- Die Verwendung der akademischen Materialien erfolgt nur zur Ihrer persönlichen Referenz- oder Schulungsverwendung.
 - Sie werden die akademischen Materialien nicht erneut veröffentlichen und nicht auf einem Netzwerkcomputer erneut veröffentlichen und nicht über irgendein Medium senden.
 - Sie werden den Originalurheberrechtshinweis der akademischen Materialien oder einen Urheberrechtshinweis zugunsten von Microsoft einschließen, der dem unten dargestellten Format entspricht:

Format des Vermerks:

© 2008 Nachdruck nur zur persönlichen Referenzverwendung mit Genehmigung von Microsoft Corporation. Alle Rechte vorbehalten.

Microsoft und Windows sind Marken oder eingetragene Marken von Microsoft Corporation in den USA und/oder anderen Ländern. Andere in diesen Unterlagen genannte Produkt- und Firmennamen können Marken der jeweiligen Eigentümer sein.

- c. Vertreibbarer Code.** Die lizenzierten Inhalte können Code enthalten, den Sie in von Ihnen entwickelten Programmen vertreiben dürfen, wenn Sie die nachfolgenden Bestimmungen einhalten.
- i. Recht zur Nutzung und zum Vertrieb.** Bei dem nachfolgend aufgelisteten Code und den nachfolgend aufgelisteten Textdateien handelt es sich um „vertreibbaren Code“.
- REDIST.TXT-Dateien. Sie sind berechtigt, die Objektcodeform des in den Dateien namens REDIST.TXT aufgelisteten Codes zu kopieren und zu vertreiben.
 - Mustercode. Sie sind berechtigt, die Quell- und Objektcodeform des als „Muster“ gekennzeichneten Codes zu ändern, zu kopieren und zu vertreiben.
 - Vertrieb durch Dritte. Sie sind berechtigt, Distributoren Ihrer Programme zu erlauben, den vertreibbaren Code als Teil dieser Programme zu kopieren und zu vertreiben.
- ii. Vertriebsbedingungen.** Für vertreibbaren Code, den Sie vertreiben, sind Sie verpflichtet:
- diesem in Ihren Programmen wesentliche primäre Funktionalität hinzuzufügen
 - von Distributoren und externen Endbenutzern die Zustimmung zu Bestimmungen zu verlangen, die einen mindestens gleichwertigen Schutz für ihn bieten wie dieser Vertrag
 - Ihren gültigen Urheberrechtshinweis auf Ihren Programmen anzubringen

- Microsoft von allen Ansprüchen freizustellen und gegen alle Ansprüche zu verteidigen, einschließlich Anwaltsgebühren, die mit dem Vertrieb oder der Verwendung Ihrer Programme in Zusammenhang stehen.

iii. Vertriebsbeschränkungen. Sie sind nicht dazu berechtigt:

- Urheberrechts-, Markenrechts- oder Patentinweise im vertreibbaren Code zu ändern
- die Marken von Microsoft in den Namen Ihrer Programme oder auf eine Weise zu verwenden, die nahe legt, dass Ihre Programme von Microsoft stammen oder von Microsoft empfohlen werden
- vertreibbaren Code zur Ausführung auf einer anderen Plattform als der Windows-Plattform zu vertreiben
- vertreibbaren Code in bösartige, täuschende oder rechtswidrige Programme aufzunehmen
- den Quellcode von vertreibbarem Code so zu ändern oder zu vertreiben, dass irgendein Teil von ihm einer ausgeschlossenen Lizenz unterliegt. Eine ausgeschlossene Lizenz ist eine Lizenz, die als Bedingung für eine Verwendung, Änderung oder einen Vertrieb erfordert, dass:
 - der Code in Quellcodeform offen gelegt oder vertrieben wird oder
 - andere das Recht haben, ihn zu ändern.

5. INTERNETBASIERTE DIENSTE. Microsoft stellt möglicherweise internetbasierte Dienste mit den lizenzierten Inhalten bereit. Microsoft ist berechtigt, diese jederzeit zu ändern oder zu kündigen. Sie sind nicht berechtigt, diese Dienste auf eine Weise zu verwenden, die diese Dienste beschädigen oder ihre Verwendung durch andere beeinträchtigen könnte. Sie sind nicht berechtigt, die Dienste zu verwenden, um zu versuchen, auf irgendeine Weise nicht autorisierten Zugriff auf Dienste, Daten, Accounts oder Netzwerke zu erlangen.

6. GÜLTIGKEITSBEREICH DER LIZENZ. Die lizenzierten Inhalte werden lizenziert, nicht verkauft. Dieser Vertrag gibt Ihnen nur einige Rechte zur Verwendung der lizenzierten Inhalte. Microsoft behält sich alle anderen Rechte vor. Sie dürfen die lizenzierten Inhalte nur wie in diesem Vertrag ausdrücklich gestattet verwenden, es sei denn, das anwendbare Recht gibt Ihnen ungeachtet dieser Einschränkung umfassendere Rechte. Dabei sind Sie verpflichtet, alle technischen Beschränkungen der lizenzierten Inhalte einzuhalten, die Ihnen nur spezielle Verwendungen gestatten. Sie sind nicht dazu berechtigt:

- Ergebnisse von Vergleichstests der lizenzierten Inhalte ohne vorherige schriftliche Genehmigung von Microsoft an Dritte weiterzugeben
- technische Beschränkungen der lizenzierten Inhalte zu umgehen
- die lizenzierten Inhalte zurückzuentwickeln (Reverse Engineering), zu dekompileieren oder zu disassemblieren, es sei denn, dass (und nur insoweit) es durch das anwendbare Recht ungeachtet dieser Einschränkung ausdrücklich gestattet ist
- eine größere Anzahl von Kopien der lizenzierten Inhalte als in diesem Vertrag angegeben oder vom anwendbaren Recht ungeachtet dieser Einschränkung ausdrücklich gestattet anzufertigen
- die lizenzierten Inhalte zu veröffentlichen, damit andere sie kopieren können
- die als 'Beta' oder 'Vorabversion' gekennzeichneten lizenzierten Inhalte an Dritte zu übertragen,
- anderen zu erlauben, auf die lizenzierten Inhalte zuzugreifen oder sie zu verwenden,
- die lizenzierten Inhalte zu vermieten, zu verleasen oder zu verleihen
- die lizenzierten Inhalte für kommerzielle Hostingdienste für lizenzierte Inhalte zu verwenden.

- Rechte zum Zugriff auf die Serversoftware, die möglicherweise im Lieferumfang der lizenzierten Inhalte enthalten ist, einschließlich der virtuellen Festplatten, geben Ihnen kein Recht, Patente von Microsoft oder anderes geistiges Eigentum von Microsoft in Software oder Geräten zu implementieren, die möglicherweise auf den Server zugreifen.
- 7. SICHERUNGSKOPIE.** Sie sind berechtigt, eine Sicherungskopie der lizenzierten Inhalte anzufertigen. Sie dürfen diese nur zur erneuten Installation der lizenzierten Inhalte verwenden.
 - 8. ÜBERTRAGUNG AUF EIN ANDERES GERÄT.** Sie sind berechtigt, die lizenzierten Inhalte zu deinstallieren und auf einem anderen Gerät zu Ihrer persönlichen Schulungsverwendung zu installieren. Sie sind nicht berechtigt, dies zu tun, um diese Lizenz auf mehreren Geräten gemeinsam zu verwenden.
 - 9. ÜBERTRAGUNG AN DRITTE.** Sie sind nicht berechtigt, diejenigen Versionen, die als 'Beta' oder 'Vorabversion' gekennzeichnet sind, an Dritte zu übertragen. Für endgültige Versionen finden die folgenden Bestimmungen Anwendung: Der erste Nutzer der lizenzierten Inhalte ist berechtigt, diese mit diesem Vertrag direkt an Dritte zu übertragen. Vor der Übertragung muss sich die andere Partei damit einverstanden erklären, dass dieser Vertrag für die Übertragung und Verwendung der lizenzierten Inhalte gilt. Der erste Nutzer ist verpflichtet, die lizenzierten Inhalte zu deinstallieren, bevor er sie separat vom Gerät überträgt. Der erste Nutzer ist nicht berechtigt, Kopien zurückzubehalten.
 - 10. AUSFUHRBESCHRÄNKUNGEN.** Die lizenzierten Inhalte unterliegen den Exportgesetzen und -regelungen der USA sowie des Landes, aus dem sie ausgeführt werden. Sie sind verpflichtet, alle nationalen und internationalen Exportgesetze und -regelungen einzuhalten, die für die lizenzierten Inhalte gelten. Zu diesen Gesetzen gehören Einschränkungen im Hinblick auf Bestimmungsorte, Endbenutzer und Endbenutzung. Weitere Informationen finden Sie unter www.microsoft.com/exporting, oder wenden Sie sich an das verbundene Unternehmen von Microsoft in Ihrem Land, siehe unter www.microsoft.com/worldwide oder für Deutschland unter www.microsoft.com/germany oder telefonisch unter (49) (0) 89-3176-0.
 - 11. NICHT ZUM WEITERVERKAUF BESTIMMTE SOFTWARE/LIZENZIERTE INHALTE („Not for Resale“ oder „NFR“).** Software oder lizenzierte Inhalte, die als „Nicht zum Weiterverkauf bestimmt“ oder „NFR“ (Not for Resale) gekennzeichnet ist bzw. sind, dürfen Sie nicht verkaufen.
 - 12. SCHULVERSION („Academic Edition“ oder „AE“).** Um lizenzierte Inhalte zu verwenden, die als „Schulversion“ oder „AE“ (Academic Edition) gekennzeichnet sind, müssen Sie „eine berechtigte Benutzerin oder ein berechtigter Benutzer einer anerkannten Ausbildungseinrichtung“ sein. Wenn Sie nicht wissen, ob Sie eine berechtigte Benutzerin oder ein berechtigter Benutzer einer anerkannten Ausbildungseinrichtung sind, besuchen Sie <http://www.microsoft.com/germany/bildung>, oder wenden Sie sich an Microsoft oder an das verbundene Unternehmen von Microsoft in Ihrem Land.
 - 13. GESAMTER VERTRAG.** Dieser Vertrag sowie die Bestimmungen für von Ihnen verwendete Ergänzungen, Updates, internetbasierte Dienste und Supportleistungen stellen den gesamten Vertrag für die lizenzierten Inhalte und die Supportleistungen dar.
 - 14. ANWENDBARES RECHT.**
 - a. Vereinigte Staaten.** Wenn Sie die lizenzierten Inhalte in den Vereinigten Staaten erworben haben, regelt das Gesetz des Staates Washington die Auslegung dieses Vertrags und gilt für Ansprüche, die aus einer Vertragsverletzung entstehen, ungeachtet von Prinzipien über Gesetzeskonflikte. Die Gesetze des Staates Ihres Wohnortes regeln alle anderen Ansprüche, einschließlich Ansprüche aus den Verbraucherschutzgesetzen des Staates, aus Gesetzen gegen unlauteren Wettbewerb und aus Schadenersatzverfahren.
 - b. Außerhalb der Vereinigten Staaten.** Wenn Sie die lizenzierten Inhalte in einem anderen Land erworben haben, gelten die Gesetze dieses Landes.

- 15. RECHTSKRAFT.** Dieser Vertrag beschreibt bestimmte gesetzliche Rechte. Möglicherweise haben Sie unter den Gesetzen Ihres Landes weitergehende Rechte. Möglicherweise verfügen Sie außerdem über Rechte im Hinblick auf die Partei, von der Sie die lizenzierten Inhalte erworben haben. Dieser Vertrag ändert nicht Ihre Rechte, die sich aus den Gesetzen Ihres Landes ergeben, sofern die Gesetze Ihres Landes dies nicht zulassen.
- 16. AUSSCHLUSS VON GARANTIE. DIE LIZENZIERTEN INHALTE WERDEN „WIE BESEHEN“ LIZENZIERT. SIE TRAGEN DAS MIT DER NUTZUNG VERBUNDENE RISIKO. MICROSOFT GEWÄHRT KEINE AUSDRÜCKLICHEN GEWÄHRLEISTUNGEN ODER GARANTIE. MÖGLICHERWEISE HABEN SIE UNTER DEN ÖRTLICH ANWENDBAREN GESETZEN ZUSÄTZLICHE VERBRAUCHERRECHTE, DIE DURCH DIESEN VERTRAG NICHT ABGEÄNDERT WERDEN KÖNNEN. IM DURCH DAS ÖRTLICH ANWENDBARE RECHT GESTATTETEN UMFANG SCHLIESST MICROSOFT IMPLIZIERTE GARANTIE FÜR DIE GEBRAUCHSTAUGLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND NICHTVERLETZUNG VON RECHTEN DRITTER AUS.**
- 17. BESCHRÄNKUNG UND AUSSCHLUSS DES SCHADENERSATZES. SIE KÖNNEN VON MICROSOFT UND DEREN LIEFERANTEN NUR EINEN ERSATZ FÜR DIREKTE SCHÄDEN BIS ZU EINEM BETRAG VON 5 US-DOLLAR ERHALTEN. SIE KÖNNEN KEINEN ERSATZ FÜR ANDERE SCHÄDEN ERHALTEN, EINSCHLIESSLICH FOLGESCHÄDEN, SCHÄDEN AUS ENTGANGENEM GEWINN, SPEZIELLE, INDIREKTE ODER BEILÄUFIG ENTSTANDENE SCHÄDEN.**

Diese Beschränkung gilt für:

- jeden Gegenstand im Zusammenhang mit den lizenzierten Inhalten, Software, Diensten, Inhalten (einschließlich Code) auf Internetseiten von Drittanbietern oder Programmen von Drittanbietern
- Ansprüche aus Vertragsverletzungen, Verletzungen der Garantie oder der Gewährleistung, verschuldensunabhängiger Haftung, Fahrlässigkeit oder anderen unerlaubten Handlungen im durch das anwendbare Recht gestatteten Umfang.

Sie hat auch dann Gültigkeit, wenn Microsoft von der Möglichkeit der Schäden gewusst hat oder hätte wissen müssen. Obige Beschränkung und obiger Ausschluss gelten möglicherweise nicht für Sie, weil Ihr Land den Ausschluss oder die Beschränkung von beiläufig entstandenen Schäden, Folgeschäden oder sonstigen Schäden nicht gestattet.

Wenn Sie die Software in DEUTSCHLAND oder in ÖSTERREICH erworben haben, findet die Beschränkung im vorstehenden Absatz „Beschränkung und Ausschluss des Schadenersatzes“ auf Sie keine Anwendung. Stattdessen gelten für Schadenersatz oder Ersatz vergeblicher Aufwendungen, gleich aus welchem Rechtsgrund einschließlich unerlaubter Handlung, die folgenden Regelungen:

Microsoft haftet bei Vorsatz, grober Fahrlässigkeit, bei Ansprüchen nach dem Produkthaftungsgesetz sowie bei Verletzung von Leben, Körper oder der Gesundheit nach den gesetzlichen Vorschriften.

Microsoft haftet nicht für leichte Fahrlässigkeit. Wenn Sie die Software jedoch in **Deutschland** erworben haben, haftet Microsoft auch für leichte Fahrlässigkeit, wenn Microsoft eine wesentliche Vertragspflicht verletzt. In diesen Fällen ist die Haftung von Microsoft auf typische und vorhersehbare Schäden beschränkt. In allen anderen Fällen haftet Microsoft auch in Deutschland nicht für leichte Fahrlässigkeit.

Unterrichtseinheit 1

Windows 7: Installation, Upgrade und Migration

Inhalt:

Lektion 1: Vorbereiten der Installation von Windows 7	10
Lektion 2: Ausführen einer Neuinstallation von Windows 7	13
Lektion 3: Windows 7: Upgrade und Migration	17
Lektion 4: Ausführen einer abbildbasierten Installation von Windows 7	19
Lektion 5: Konfigurieren der Anwendungskompatibilität	24
Lernzielkontrollen und Kernpunkte der Unterrichtseinheit	26
Fragen und Antworten zur Lernzielkontrolle	29

Lektion 1

Vorbereiten der Installation von Windows 7

Inhalt:

Fragen und Antworten

11

Fragen und Antworten

Hauptfeatures von Windows 7

Frage: Welche der Hauptfeatures von Windows 7 sind für Ihre Organisation hilfreich?

Antwort: Die Antwort kann unterschiedlich ausfallen, im Allgemeinen sind jedoch alle wichtigen Features von Windows 7 im Hinblick auf Benutzerfreundlichkeit, Sicherheit, Verwaltbarkeit, Bereitstellung und Produktivität hilfreich.

Editionen von Windows 7

Frage 1: Welche Edition von Windows 7 sollte in den folgenden Szenarien ausgewählt werden?

Szenario 1: Ihre Organisation umfasst nur wenige Benutzer. Derzeit ist kein zentraler Dateiserver vorhanden, und die Computer befinden sich nicht in einer Domäne.

Szenario 2: Die Organisation verfügt über mehr als hundert Benutzer die in mehreren Büros im ganzen Land verstreut arbeiten. Zudem haben Sie mehrere Benutzer, die häufig reisen.

Antwort: Wählen Sie Windows 7 Professional für Szenario 1 und Windows 7 Enterprise für Szenario 2.

Szenario 1: Wählen Sie für eine Geschäftsumgebung entweder Windows 7 Professional oder Windows 7 Enterprise. Windows 7 Home Premium, Windows 7 Home Basic und Windows 7 Starter sind für Privatbenutzer bestimmt. Da Sie nur wenige Benutzer haben, ist Windows 7 Professional die beste Wahl.

Szenario 2: Wählen Sie Windows 7 Enterprise mit Features, wie z. B. BranchCache und DirectAccess, um die Produktivität der mobilen Benutzern zu erhöhen.

Frage 2: Was ist der Unterschied zwischen der Enterprise- und der Ultimate-Edition von Windows 7?

Antwort: Es gibt keinen Unterschied zwischen der Enterprise- und der Ultimate-Edition bezüglich der Features. Windows 7 Enterprise ist über Microsoft Software Assurance mit Volumenlizenzierung verfügbar, und Windows 7 Ultimate ist im Einzelhandel erhältlich. Es gibt keinen Upgradepfad zwischen den beiden Editionen.

Hardwareanforderungen für die Installation von Windows 7

Frage: Welche Computerspezifikation ist in Ihrer Organisation derzeit vorherrschend? Vergleichen Sie diese Spezifikation mit den üblichen Spezifikationen zum Zeitpunkt der Veröffentlichung von Windows Vista. Gehen Sie davon aus, dass Windows 7 auf den vorhandenen Computern in Ihrer Organisation bereitgestellt werden kann?

Antwort: Die Antwort kann unterschiedlich ausfallen. Vor mehreren Jahren, als Windows Vista veröffentlicht wurde, wurden die Hardwareanforderungen als ziemlich hoch eingestuft. Da die Windows 7-Hardwareanforderungen mit denen von Windows Vista identisch sind, kann Windows 7 auf den Computern in den meisten Organisationen installiert werden.

Optionen beim Installieren von Windows 7

Frage: Welcher Installationstyp wird in den folgenden Szenarien verwendet?

Szenario 1: Die Benutzer verwenden Computer, die mindestens drei Jahre alt sind, und Ihre Organisation plant, Windows 7 auf vielen neuen Computern bereitzustellen.

Szenario 2: In Ihrer Organisation gibt es nur wenige Benutzer mit zumeist neuen Computern, auf denen jedoch viele Anwendungen installiert und eine große Menge an Daten gespeichert sind.

Antwort: Es sind verschiedene Antworten möglich. Die Auswahl des Installationstyps wird möglicherweise nicht nur von diesen Faktoren entschieden. Im Allgemeinen wird empfohlen, eine Neuinstallation und dann eine Migration der Benutzereinstellungen und -daten durchzuführen. Vermeiden Sie das Upgrade außer bei sehr wenigen Benutzern oder Computern. In Szenario 1 sollten Sie neue Hardware für die Organisation kaufen, eine Neuinstallation von Windows 7 ausführen und die notwendigen Benutzereinstellungen und -daten migrieren. In Szenario 2 sollten Sie ein direktes Upgrade auf Windows 7 durchführen.

Lektion 2

Ausführen einer Neuinstallation von Windows 7

Inhalt:

Fragen und Antworten	14
Detaillierte Demoschritte	16

Fragen und Antworten

Diskussion: Überlegungen zur Neuinstallation

Frage: Wann sollten Sie eine Neuinstallation von Windows ausführen?

Antwort: Die Antworten können unterschiedlich ausfallen, bedenken Sie jedoch die folgenden allgemeinen Umstände.

Überlegungen zur Neuinstallation

In den folgenden Fällen müssen Sie eine Neuinstallation ausführen:

- Es ist kein Betriebssystem auf dem Computer installiert.
- Das installierte Betriebssystem unterstützt kein Upgrade auf Windows 7.
- Der Computer verfügt über mehrere Partitionen und muss eine Mehrfach-Boot-Konfiguration unterstützen, die Windows 7 und das aktuelle Betriebssystem verwendet.

Eine Neuinstallation ist die bevorzugte Installationsmethode. Bei einer Neuinstallation wird sichergestellt, dass alle Ihre Systeme über die gleiche Konfiguration verfügen und alle Anwendungen, Dateien und Einstellungen zurückgesetzt werden.

Methoden zum Ausführen einer Neuinstallation

Frage: In welchen Situationen werden die einzelnen Methoden für eine Neuinstallation des Windows-Betriebssystems verwendet?

Antwort: Die Windows-Installation von der Produkt-DVD ist am einfachsten. Im Allgemeinen wird diese Methode in einer Heim- oder kleinen Firmenumgebung oder zur Installation eines Referenzcomputers verwendet. Sie können die Installationsdateien auf einer Netzwerkfreigabe speichern, damit die Windows-Installation vom Netzwerk aus auf Computern ohne DVD-Laufwerk ausgeführt werden kann. Bei der Windows-Installation von einer Netzwerkfreigabe müssen Sie auch keine Installationsmedien verwalten. Wenn Sie Windows in einem Großunternehmen installieren und die Umgebung standardisieren möchten, installieren Sie Windows mit einem Abbild.

Diskussion: Häufige Installationsfehler

Frage: Welche potenziellen Probleme könnten beim Installieren von Windows auftreten?

Antwort: Es sind verschiedene Antworten möglich. In der folgenden Tabelle werden mehrere Installationsprobleme und Lösungen beschrieben, mit denen bestimmte Probleme identifiziert und gelöst werden können.

Problem	Lösung
Das Installationsmedium ist beschädigt.	Testen Sie die CD oder DVD auf einem anderen System.
Ein BIOS-Upgrade ist erforderlich.	Überprüfen Sie auf der Internetseite des Computerherstellers, ob ein BIOS-Upgrade für Windows 7 verfügbar ist.

Die Hardware wurde falsch installiert.	Prüfen Sie sämtliche Meldungen, die während der Startphase angezeigt werden. Stellen Sie bei der Installation zusätzlicher Hardware (z. B. Grafikkarten und Speichermodule) sicher, dass diese ordnungsgemäß installiert wird.
Die Hardware entspricht nicht den Mindestanforderungen.	Suchen Sie im Windows-Katalog nach Produkten, die für Microsoft Windows entwickelt wurden, und stellen Sie sicher, dass die Hardware den Mindestanforderungen für die zu installierende Windows 7-Edition entspricht.
Während des Setups treten Fehlermeldungen auf.	Notieren Sie sämtliche Meldungen sorgfältig, und suchen Sie in der Microsoft Knowledge Base nach einer Erklärung der Meldungen.

Demo: Konfigurieren des Computernamens und der Domänen-/Arbeitsgruppeneinstellungen

Frage: Wann sollte das primäre DNS-Suffix so konfiguriert werden, dass es sich von der Active Directory-Domäne unterscheidet?

Antwort: In den meisten Fällen konfigurieren Sie das primäre DNS-Suffix nicht unterschiedlich von der Active Directory-Domäne. Dies wird nur in Großunternehmen mit einer komplexen DNS-Struktur gemacht, die von der Active Directory DNS-Struktur unabhängig ist. Sie könnten beispielsweise ein anderes primäres DNS-Suffix konfigurieren, um Anwendungen zu unterstützen, die in einer alternativen DNS-Domäne suchen müssen.

Detaillierte Demoschritte

Demo: Konfigurieren des Computernamens und der Domänen-/Arbeitsgruppeneinstellungen

Detaillierte Demoschritte

1. Melden Sie sich am virtuellen Computer 10225-LON-CL1 als **CONTOSO\Administrator** mit dem Kennwort **Pa\$\$w0rd**.
2. Klicken Sie auf **Start** und dann auf **Systemsteuerung**.
3. Klicken Sie auf **System und Sicherheit** und dann auf **System**.
4. Klicken Sie im Bereich **Einstellungen für Computernamen, Domäne und Arbeitsgruppe** auf **Einstellungen ändern**.
5. Klicken Sie im Fenster **Systemeigenschaften** auf die Schaltfläche **Ändern**. Beachten Sie, dass die Schaltfläche **Netzwerk-ID** dieselbe Aufgabe mit einem Assistenten ausführt.
6. Klicken Sie im Fenster **Ändern des Computernamens bzw. der Domäne** auf **Arbeitsgruppe**, und geben Sie „**WORKGROUP**“ ein. Dies ist der Name der Arbeitsgruppe, der beigetreten werden soll.
7. Klicken Sie auf **OK**.
8. Klicken Sie auf **OK**, um die Warnung zu bestätigen.
9. Klicken Sie auf **OK**, um die Willkommensnachricht zu schließen.
10. Klicken Sie auf **OK**, um die Benachrichtigung über den Neustart zu schließen.
11. Klicken Sie im Fenster **Systemeigenschaften** auf die Schaltfläche **Ändern**. Beachten Sie, dass die Schaltfläche **Netzwerk-ID** dieselbe Aufgabe mit einem Assistenten ausführt.
12. Klicken Sie im Fenster **Ändern des Computernamens bzw. der Domäne** auf **Domäne**, und geben Sie „**Contoso.com**“ ein. Dies ist der Name der Domäne, der beigetreten werden soll.
13. Klicken Sie auf die Schaltfläche **Details**. Verwenden Sie das primäre DNS-Suffix, um den Computer nach DNS-Domänen außerhalb der beizutretenden Active Directory®-Domäne suchen zu lassen. Der NetBIOS-Name wird für die Abwärtskompatibilität mit älteren Anwendungen verwendet.
14. Klicken Sie auf die Schaltfläche **Abbrechen**.
15. Klicken Sie im Fenster **Ändern des Computernamens bzw. der Domäne** auf **OK**.
16. Wenn Sie dazu aufgefordert werden, geben Sie im Feld **Windows-Sicherheit** die Zeichenfolge „**Administrator**“ mit dem Kennwort **Pa\$\$w0rd** ein.
17. Klicken Sie drei Mal auf **OK** und dann auf **Schließen**.
18. Klicken Sie auf **Jetzt neu starten**.
19. Wenn das System neu gestartet wurde, melden Sie sich als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.

Lektion 3

Windows 7: Upgrade und Migration

Inhalt:

Fragen und Antworten

18

Fragen und Antworten

Überlegungen zum Upgraden auf und Migrieren zu Windows 7

Frage: Sie stellen Windows 7 für die gesamte Organisation bereit. Würden Sie sich in den folgenden Szenarien für ein Upgrade oder eine Migration entscheiden?

Szenario 1: Die Organisation verfügt über eine standardisierte Umgebung. Mehrere Server stellen Speicherplatz bereit, und die Computer der Organisation sind nicht älter als zwei Jahre.

Szenario 2: Die Organisation verfügt über eine standardisierte Umgebung. Mehrere Server stellen Speicherplatz bereit, und Sie planen, vorhandene Computer zu ersetzen, wenn diese mehr als drei Jahre alt sind.

Szenario 3: Sie verfügen über keinen zusätzlichen Speicherplatz, und die Computer in der Organisation sind weniger als zwei Jahre alt. Außerdem gibt es in der Organisation nur fünf Benutzer, und Sie möchten vorhandene Anwendungen auf den Benutzercomputern nicht neu installieren.

Antwort: Szenario 1: Führen Sie eine Wipe-and-Load-Migration aus. Um eine standardisierte Umgebung zu erreichen, führen Sie eine Neuinstallation und danach eine Migration aus. In diesem Szenario haben Sie Speicherplatz, Sie planen jedoch nicht, die vorhandene Hardware zu ersetzen.

Szenario 2: Führen Sie eine parallele Migration aus. Um eine standardisierte Umgebung zu erreichen, führen Sie eine Neuinstallation und danach eine Migration aus. In diesem Szenario haben Sie Speicherplatz und planen, die vorhandene Hardware zu ersetzen.

Szenario 3: Ausführen einer direkten Aktualisierung. In diesem Szenario haben Sie keinen Speicherplatz, der für eine Migration erforderlich ist. Bei einer Migration müssen Sie zudem alle vorhandenen Anwendungen neu installieren.

Tools zum Migrieren von Benutzerdaten und Einstellungen

Frage: Wie migrieren Sie Anwendungen zu Windows 7?

Antwort: Sie können Anwendungseinstellungen migrieren, jedoch nicht die Anwendungen selbst. Sie müssen die Anwendungen vor dem Wiederherstellen der Anwendungseinstellungen auf dem Zielcomputer neu installieren.

Lektion 4

Ausführen einer abbildbasierten Installation von Windows 7

Inhalt:

Fragen und Antworten	20
Detaillierte Demoschritte	21

Fragen und Antworten

Demo: Erstellen einer Antwortdatei mit Windows SIM

Frage: Warum sollten Sie eine Antwortdatei verwenden, anstatt die Installation von Windows 7 manuell durchzuführen?

Antwort: Eine Antwortdatei wird verwendet, um den Installationsvorgang für Geschwindigkeit und Konsistenz zu automatisieren. Wenn Sie eine Antwortdatei verwenden, können Sie sicher sein, dass die Installationen identisch sind. Das Automatisieren des Installationsvorgangs ist effizienter, wenn mehrere Computer gleichzeitig konfiguriert werden.

Demo: Erstellen eines startfähigen Windows PE-Mediums

Frage: Auf welche Weise verwenden Sie die erstellte ISO-Datei?

Antwort: In der Regel wird die ISO-Datei im nächsten Schritt als startfähige CD oder DVD gebrannt. Diese kann dann verwendet werden, um Abbildvorgänge auszuführen.

Demo: Konfigurieren von VHDs

Frage: Können Sie eine Windows 7-basierte VHD, die für das Ausführen auf einem virtuellen Computer konfiguriert wurde, so konfigurieren, dass dieselbe VHD als systemeigener Start ausgeführt wird?

Antwort: Ja. Bevor eine Windows 7-basierte VHD, die für das Ausführen auf einem virtuellen Computer konfiguriert wurde, als systemeigener Start ausgeführt werden kann, müssen Sie zunächst systemspezifische Daten mit Sysprep aus der Windows-Installation entfernen.

Detaillierte Demoschritte

Demo: Erstellen einer Antwortdatei mit Windows SIM

Detaillierte Demoschritte

Erstellen einer Antwortdatei mit Windows SIM

1. Melden Sie sich am virtuellen Computer 10225-LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd**.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Microsoft Windows AIK** und dann auf **Windows System Image Manager**.
3. Klicken Sie im Bereich **Windows-Abbild** mit der rechten Maustaste auf **Windows-Abbild oder Katalogdatei auswählen**, und klicken Sie dann auf **Windows-Abbild auswählen**.
4. Navigieren Sie zum Ordner **E:\Labfiles\Mod01\Sources**, klicken Sie auf **install_Windows 7 ENTERPRISE.clg**, und dann auf **Open**.

Hinweis: Wenn für diese Edition von Windows 7 keine Katalogdatei vorhanden ist, werden Sie aufgefordert, eine Katalogdatei zu erstellen. Der Erstellungsvorgang dauert mehrere Minuten. In dieser Demo werden Sie nicht aufgefordert, eine Katalogdatei zu erstellen, da sie bereits für Sie erstellt wurde.

5. Klicken Sie im Bereich **Antwortdatei** mit der rechten Maustaste auf **Antwortdatei erstellen oder öffnen**, und klicken Sie dann auf **Neue Antwortdatei**.
6. Erweitern Sie im Bereich **Windows-Abbild** den Knoten **Komponenten**, führen Sie einen Bildlauf nach unten aus, und erweitern Sie **x86_Microsoft-Windows-Setup**. Diese Gruppe von Einstellungen wird hauptsächlich in der windowsPE-Phase einer unbeaufsichtigten Installation verwendet. Beachten Sie, dass Datenträgerkonfiguration dazugehören.
7. Erweitern Sie **UserData**, und klicken Sie mit der rechten Maustaste auf **ProductKey**. Beachten Sie, dass diese Einstellung nur in der windowsPE-Phase angewendet werden kann. Sie wird zu einer unbeaufsichtigten Installation verwendet, bei der Windows 7 von der Windows 7-Installations-DVD aus der Datei install.wim installiert wird.
8. Führen Sie einen Bildlauf nach unten durch, und klicken Sie auf **x86_Microsoft-Windows-Shell-Setup**. Beachten Sie, dass die Option für den Product Key hier verfügbar ist und im Eigenschaftenbereich angezeigt wird.
9. Klicken Sie mit der rechten Maustaste auf **x86_Microsoft-Windows-Shell-Setup**, und klicken Sie auf **Einstellung zu Pass 4 specialize hinzufügen**. Diese Einstellungen werden übernommen, nachdem ein Betriebssystem mit Sysprep verallgemeinert wurde.
10. Geben Sie im Bereich **Eigenschaften von Microsoft-Windows-Shell-Setup** im Feld **ProductKey** den Eintrag „**11111-22222-33333-44444-55555**“ ein, und drücken Sie die **EINGABETASTE**. Wenn in dieser Antwortdatei ein Produktschlüssel angegeben wird, muss dieser bei der Installation eines neuen Abbilds nicht eingegeben werden.

11. Schließen Sie den **Windows System Image Manager**, und speichern Sie die Änderungen nicht.

Hinweis: Weitere Informationen finden Sie in „Technische Referenz zu Windows System Image Manager“ unter <http://go.microsoft.com/fwlink/?LinkID=154216>.

Demo: Erstellen eines startfähigen Windows PE-Mediums

Detaillierte Demoschritte

Erstellen eines startfähigen Windows PE-Mediums

1. Melden Sie sich am virtuellen Computer 10225-LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd**.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Microsoft Windows AIK**, und klicken Sie dann auf **Eingabeaufforderung für Bereitstellungstools**.
3. Geben Sie an der Eingabeaufforderung „**copy.cmd amd64 E:\winpe_amd64**“ ein, und drücken Sie die EINGABETASTE. Dieser Befehl kopiert die notwendigen Dateien in den Ordner E:\winpe_amd64 folder. Wenn der Ordner nicht vorhanden ist, wird er erstellt.
4. Geben Sie an der Eingabeaufforderung „**copy „C:\Programme\Windows AIK\Tools\amd64\imagex.exe“ E:\winpe_amd64\iso**“ ein, und drücken Sie dann die EINGABETASTE. Hierdurch werden den Dateien das ImageX-Tool für die ISO hinzugefügt.
5. Geben Sie an der Eingabeaufforderung „**oscdimg -n -bE:\winpe_amd64\etfsboot.com E:\winpe_amd64\iso E:\winpe_amd64\winpe_amd64.iso**“ ein, und drücken Sie dann die EINGABETASTE. Dieser Befehl erstellt die ISO-Datei mit Windows PE.

Hinweis: Weitere Informationen zu „copy“, „copy“ und „oscdimg“ finden Sie unter:
<http://go.microsoft.com/fwlink/?LinkID=154217>
<http://go.microsoft.com/fwlink/?LinkID=154218>
<http://go.microsoft.com/fwlink/?LinkID=154219>

Demo: Bearbeiten von Abbildern mit DISM

Detaillierte Demoschritte

Bearbeiten von Abbildern mit DISM

1. Melden Sie sich am virtuellen Computer 10225A-LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd**.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Microsoft Windows AIK**, und klicken Sie dann auf **Eingabeaufforderung für Bereitstellungstools**.
3. Geben Sie an der Eingabeaufforderung „**dism**“ ein, und drücken Sie die EINGABETASTE. Die Hilfeinformationen für den Befehl werden angezeigt.
4. Geben Sie an der Eingabeaufforderung „**md C:\img**“ ein, und drücken Sie dann die EINGABETASTE.
5. Geben Sie an der Eingabeaufforderung „**dism /mount-wim /wimfile:E:\Labfiles\Mod01\Sources\install.wim /name: „Windows 7 ENTERPRISE“ /mountdir:C:\img**“ ein, und drücken Sie die EINGABETASTE.

6. Wenn die Abbildbereitstellung abgeschlossen ist, geben Sie an der Eingabeaufforderung „**dism /get-mountedwiminfo**“ ein, und drücken Sie die EINGABETASTE. Hierdurch werden Informationen zum bereitgestellten Abbild angezeigt. Beachten Sie, dass eine Indexnummer statt des Namens angezeigt wird.
7. Geben Sie „**cd C:\img**“ ein, und drücken Sie die EINGABETASTE.
8. Geben Sie an der Eingabeaufforderung „**dir**“ ein, und drücken Sie die EINGABETASTE. Sie können die Installationsdateien für Windows 7 ENTERPRISE anzeigen und ändern.
9. Geben Sie an der Eingabeaufforderung „**cd **“ ein, und drücken Sie die EINGABETASTE.
10. Geben Sie an der Eingabeaufforderung „**dism /image:C:\img /?**“ ein, und drücken Sie die EINGABETASTE. Hierdurch werden die verfügbaren Optionen für die Wartung eines Abbilds angezeigt, wie z. B. das Hinzufügen eines Treibers oder Features.
11. Geben Sie an der Eingabeaufforderung „**dism /image:C:\img /add-driver /driver:E:\LabFiles\Mod01\vx6000\vx6000.inf**“ ein, und drücken Sie die EINGABETASTE. Hierdurch wird dem Abbild der Treiber für die VX6000-Lifecam hinzugefügt, damit diese für alle mit diesem Abbild konfigurierten Computer verfügbar ist.
12. Geben Sie an der Eingabeaufforderung „**dism /unmount-wim /mountdir:C:\img /discard**“ ein, und drücken Sie die EINGABETASTE. Verwenden Sie die Option **/commit**, um die Änderungen zu speichern.
13. Schließen Sie alle geöffneten Fenster.

Lektion 5

Konfigurieren der Anwendungskompatibilität

Inhalt:

Fragen und Antworten

25

Fragen und Antworten

Aktualisieren von Shims

Frage: In welchen Situationen verwenden Sie einen Kompatibilitätspatch?

Antwort: Die Antwort kann unterschiedlich ausfallen. Der Kompatibilitätspatch wird in mehreren Szenarien eingesetzt, wenn beispielsweise ein Kompatibilitätsproblem in einer Anwendung besteht, deren Anbieter nicht mehr vorhanden ist, wenn eine Anwendung intern erstellt wurde, wenn eine Anwendung vorhanden ist, für die in naher Zukunft eine kompatible Version freigegeben werden soll, oder wenn eine Anwendung, unabhängig von ihrer Version, nicht entscheidend für die Organisation ist.

Lernzielkontrollen und Kernpunkte der Unterrichtseinheit

Fragen zur Lernzielkontrolle

Sie haben sich dazu entschlossen, Windows 7 in der Organisation bereitzustellen. Sie arbeiten vom Hauptsitz der Organisation aus. Die Organisation verfügt über fünf Zweigstellen im selben Land, in denen jeweils weniger als zehn Benutzer arbeiten. Insgesamt arbeiten im Hauptsitz der Organisation hundert Mitarbeiter. Außerdem gibt es landesweit mehrere Benutzer, die von zu Hause oder unterwegs arbeiten. Die Organisation plant zudem, in der nahen Zukunft in die Nachbarländer zu expandieren. Dadurch werden Sprachen eingeführt, die sich von der im Hauptsitz der Organisation unterscheiden.

Die Organisation verfügt über eine standardisierte und verwaltete IT-Umgebung mit Windows Server 2008 R2 und Active Directory. Fast alle Benutzer verwenden Windows XP mit Service Pack 3. Einige wenige verfügen über Windows Vista mit Service Pack 2.

Frage 1: Welche Edition von Windows 7 eignet sich am besten für Ihre Organisation?

Antwort: Wählen Sie in Geschäftsszenarien entweder Windows 7 Professional oder Windows 7 Enterprise aus. Diese zwei Editionen sind auf Unternehmen ausgerichtet und unterstützen Domänenbeitritte sowie Active Directory.

Sie haben mehrere Zweigstellen und mehrere mobile Mitarbeiter. Wählen Sie in diesem Szenario Windows 7 Enterprise aus, um Features wie z. B. DirectAccess, BranchCache und VPN-Verbindungswiederherstellung zu nutzen. Dadurch wird sich die Produktivität der Zweigstelle und der mobilen Mitarbeiter vergrößern.

Außerdem unterstützt Windows 7 Enterprise alle verfügbaren Benutzeroberflächensprachen, was sich als vorteilhaft erweisen kann, wenn Ihre Organisation in benachbarte Länder expandiert.

Frage 2: Welche Installationsmethode wählen Sie aus?

Antwort: Die Organisation verfügt über eine standardisierte und verwaltete IT-Umgebung, und es gibt eine große Anzahl von Computern, die an der Bereitstellung teilnehmen. Obwohl einige Benutzer, die Windows Vista mit Service Pack 2 verwenden, direkt auf Windows 7 upgraden können, müssen Sie dennoch eine Neuinstallation von Windows 7 und eine anschließende Migration durchführen, um Benutzereinstellungen und Daten beizubehalten. Dadurch wird sichergestellt, dass alle Benutzer über dieselbe Konfiguration verfügen und sämtliche Anwendungen, Dateien und Einstellungen zurückgesetzt werden.

Ziehen Sie in Betracht, die Windows-Neuinstallation mit einem Standardabbildverfahren auszuführen. Sie können das Abbild mit Bereitstellungstools bereitstellen, wie z. B. Windows-Bereitstellungsdiensten (WDS) oder dem Microsoft Deployment Toolkit (MDT).

Frage 3: Wenn eine Migration erforderlich ist: Für welches Migrationstool entscheiden Sie sich?

Antwort: In diesem Szenario arbeiten Sie mit vielen Computern. Wählen Sie das User State Migration Tool (USMT) aus, das Ihnen beim Migrieren von Benutzereinstellungen und Daten hilft.

Häufige Probleme bei der Installation von Windows 7

Problem	Tipps zur Problembehandlung
Das Installationsmedium ist beschädigt.	Testen Sie die CD oder DVD auf einem anderen System.
Ein BIOS-Upgrade ist erforderlich.	Überprüfen Sie auf der Internetseite des Computerherstellers, ob ein BIOS-Upgrade für Windows 7 verfügbar ist.
Die Hardware wurde falsch installiert.	Prüfen Sie sämtliche Meldungen, die während der Startphase angezeigt werden. Stellen Sie bei der Installation zusätzlicher Hardware (z. B. Grafikkarten und Speichermodule) sicher, dass diese ordnungsgemäß installiert wird.
Die Hardware entspricht nicht den Mindestanforderungen.	Suchen Sie im Windows-Katalog nach Produkten, die für Microsoft Windows entwickelt wurden, und stellen Sie sicher, dass die Hardware den Mindestanforderungen für die zu installierende Windows 7-Edition entspricht.
Während des Setups treten Fehlermeldungen auf.	Notieren Sie sämtliche Meldungen sorgfältig, und suchen Sie in der Microsoft Knowledge Base nach einer Erklärung der Meldungen.

Häufige Anwendungskompatibilitätsprobleme

Issue	Troubleshooting Tip
Die Anwendung kann unter Windows 7 nicht installiert oder ausgeführt werden. Die Anwendung kann installiert und ausgeführt werden, sie verhält sich jedoch nicht ordnungsgemäß.	<ul style="list-style-type: none"> • Upgraden der Anwendung auf eine kompatible Version • Anwenden von Updates oder Service Packs • Verwenden der Anwendungskompatibilitätsfeatures • Ändern der Anwendungskonfiguration durch Erstellen von Anwendungspatches • Ausführen der Anwendung in einer virtualisierten Umgebung • Auswählen einer anderen Anwendung, die die gleiche Geschäftsfunktion erfüllt

Best Practices zu Windows 7: Installation, Upgrade und Migration

- Sichern Sie vor einem Upgrade des Betriebssystems zunächst immer Ihre Daten.
- Installieren Sie Windows mit einem Abbild, um eine standardisierte Computerumgebung zu erhalten.
- Bewerten Sie die Systemanforderungen und die Anwendungskompatibilität, bevor Sie ein Betriebssystem aktualisieren.
- Führen Sie **Sysprep /generalize** aus, bevor Sie ein Windows-Abbild auf einen anderen Computer übertragen.
- Verwenden Sie beim Aufzeichnen eines Abbilds die **ImageX-Option /flags**, um die Metadaten zu erstellen, die für das Abbild gelten sollen.
- Erstellen Sie architekturspezifische Abschnitte für die einzelnen Konfigurationsdurchläufe einer Antwortdatei.

Tools

Tool	Verwendung	Bezugsquelle
Windows-Setup	Installieren von Windows oder Aktualisieren früherer Windows-Versionen	Windows 7-Produkt-DVD
Windows Upgrade Advisor	Bewerten der Durchführbarkeit eines Upgrades auf Windows 7	Microsoft Download Center
Microsoft Assessment and Planning Toolkit	Bewerten der Upgradebereitschaft der Organisation für Windows 7	Microsoft Download Center
Windows-EasyTransfer	Migrieren der Benutzereinstellungen und Daten mit einer parallelen Migration für einen einzelnen oder für wenige Computer	Windows 7-Produkt-DVD
Windows Automated Installation Kit (Windows AIK)	Unterstützen der Bereitstellung des Windows-Betriebssystems	Microsoft Download Center
User State Migration Tool	Migrieren der Benutzereinstellungen und Daten für eine große Anzahl von Computern	Windows AIK
Windows SIM	Erstellen von Antwortdateien für eine unbeaufsichtigte Installation	Windows AIK
ImageX	Aufzeichnen, Erstellen, Bearbeiten und Anwenden der WIM-Datei	Windows AIK
Windows PE	Installieren und Bereitstellen des Windows-Betriebssystems	Windows 7-Produkt-DVD
Sysprep	Vorbereiten der Windows-Installation für die Datenträgerabbilderstellung, für Systemtests oder für die Übermittlung	Windows AIK
Diskpart	Konfigurieren der Festplatte	Windows 7
WDS	Bereitstellen von Windows über das Netzwerk	Microsoft Download Center für Windows Server 2003 SP1-Serverrolle in Windows Server 2008 und Windows Server 2008 R2
DISM	Warten und Verwalten von Windows-Abbildern	Windows 7 Windows AIK
Anwendungskompatibilitäts-Toolkit	Inventarisieren und Analysieren der Anwendungskompatibilität der Organisation	Microsoft Download Center
Compatibility Administrator-Tool	Erstellen von Anwendungspatches	ACT

Fragen und Antworten zur Lernzielkontrolle

Frage: Warum wird Sysprep vor dem Aufzeichnen eines Abbilds verwendet?

Antwort: Sysprep wird zur Verallgemeinerung des Betriebssystems verwendet. Dadurch werden hardwarespezifische Informationen wie z. B. Treiber entfernt, damit diese neu erkannt werden können, wenn das Abbild auf die neue Hardware angewendet wird. Computerspezifische Konfigurationseinstellungen für das Betriebssystem, wie z. B. SID-Nummern und der Computername, werden ebenfalls entfernt. Dies verhindert Netzwerkkonflikte.

Frage: Warum ist Windows PE als Teil der Abbilderstellung erforderlich?

Antwort: Wenn Sie ein Betriebssystemabbild aufzeichnen oder anwenden, benötigt ImageX Vollzugriff auf die Festplatte. Windows PE wird unabhängig von dem auf dem Computer installierten Betriebssystem ausgeführt und ermöglicht daher den Vollzugriff auf die Festplatte. Wenn Sie eine andere Version als Windows PE verwenden, sind einige Dateien des Betriebssystems in Verwendung, wenn Sie versuchen, ein Abbild aufzuzeichnen oder anzuwenden, und der Vorgang schlägt fehl.

Unterrichtseinheit 2

Konfigurieren von Datenträgern und Gerätetreibern

Inhalt:

Lektion 1: Partitionieren von Datenträgern in Windows 7	31
Lektion 2: Verwalten von Datenträgervolumen	34
Lektion 3: Verwalten von Datenträgern in Windows 7	39
Lektion 4: Installieren und Konfigurieren von Gerätetreibern	43
Lernzielkontrollen und Kernpunkte der Unterrichtseinheit	47
Fragen und Antworten zur Lernzielkontrolle	53

Lektion 1

Partitionieren von Datenträgern in Windows 7

Inhalt:

Fragen und Antworten	32
Detaillierte Demoschritte	33

Fragen und Antworten

Was ist ein MBR-Datenträger?

Frage: Welche Einschränkungen bestehen für einen MBR-partitionierten Datenträger? Sind Sie in Ihrem Unternehmen auf diese Einschränkungen gestoßen, und wenn ja, was haben Sie getan, um diese zu umgehen?

Antwort: Die Einschränkungen bestehen darin, dass MBR-partitionierte Datenträger auf vier Partitionen begrenzt sind, eine maximale Partitionsgröße von 2 TB haben und keine Datenredundanz bieten.

Was ist ein GPT-Datenträger?

Frage: Wie wird ein MBR von einer GPT-partitionierten Festplatte auf einem 64-Bit-Windows 7-Betriebssystem verwendet?

Antwort: Auf einem GPT-partitionierten Datenträger enthält der Bereich 0 einen Legacy-Schutz-MBR. Der Schutz-MBR enthält eine primäre Partition, die den gesamten Datenträger umfasst. Der Schutz-MBR schützt GPT-Datenträger älterer MBR-Datenträgertools z. B. Microsoft MS-DOS FDISK oder Microsoft Windows NT-Datenträgeradministrator. Diese Tools zeigen einen GPT-Datenträger durch die Interpretation des geschützten MBR als eine einzige, umfassende (möglicherweise nicht erkannte) Partition an, anstatt den Datenträger fälschlicherweise für unpartitioniert zu halten. Ältere Software, die GPT nicht kennt, interpretiert beim Zugriff auf einen GPT-Datenträger nur den geschützten MBR.

Datenträgerverwaltungstools

Frage: Welche Auswirkung hat das Konvertieren eines Basisdatenträgers in einen dynamischen Datenträger (und umgekehrt) auf die vorhandenen Daten?

Antwort: Basisdatenträger können ohne Datenverlust in dynamische Datenträger konvertiert werden. Ein dynamischer Datenträger kann jedoch nicht in einen Basisdatenträger umgewandelt werden, ohne dass zuvor alle Volumes gelöscht werden.

Demo: Konvertieren einer MBR-Partition in eine GPT-Partition

Frage: Welches Tool würden Sie für das Konvertieren eines neuen Datenträgers in GPT bevorzugen, das Datenträgerverwaltungs-Snap-In oder das „diskpart.exe“-Befehlszeilentool?

Antwort: Betonen Sie, dass beide Möglichkeiten funktionieren, die Kursteilnehmer können jedoch eine Präferenz angeben.

Detaillierte Demoschritte

Demo: Konvertieren einer MBR-Partition in eine GPT-Partition

Detaillierte Demoschritte

Konvertieren eines Datenträgers in GPT mithilfe von „Diskpart.exe“

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, und klicken Sie dann auf **Zubehör**. Klicken Sie mit der rechten Maustaste auf Eingabeaufforderung, und klicken Sie dann auf **Als Administrator ausführen**.
3. Geben Sie an der Eingabeaufforderung **„DiskPart“** ein, und drücken Sie dann die EINGABETASTE.
4. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl **„list disk“** ein, und drücken Sie anschließend die EINGABETASTE.
5. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl **„select disk 2“** ein, und drücken Sie die EINGABETASTE.
6. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl **„convert gpt“** ein, und drücken Sie anschließend die EINGABETASTE.
7. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl **„exit“** ein, und drücken Sie die EINGABETASTE.

Konvertieren von Datenträger 3 in GPT mithilfe der Datenträgerverwaltung

1. Klicken Sie auf **Start**, klicken Sie mit der rechten Maustaste auf **Computer**, und klicken Sie dann auf **Verwalten**.
2. Klicken Sie in der Liste **Computerverwaltung (Lokal)** auf **Datenträgerverwaltung**.
3. Klicken Sie im Dialogfeld **Datenträgerinitialisierung** auf **GPT (GUID-Partitionstabelle)**, und klicken Sie anschließend auf **OK**.

Überprüfen des Datenträgertyps

1. Klicken Sie in der Datenträgerverwaltung mit der rechten Maustaste auf **Datenträger 2**, und überprüfen Sie dessen Typ.
2. Klicken Sie in der Datenträgerverwaltung mit der rechten Maustaste auf **Datenträger 3**, und überprüfen Sie dessen Typ.
3. Klicken Sie außerhalb des Kontextmenüs.

Lektion 2

Verwalten von Datenträgervolumen

Inhalt:

Fragen und Antworten	35
Detaillierte Demoschritte	36

Fragen und Antworten

Demo: Erstellen eines einfachen Volumes

Frage: Unter welchen Umständen verwenden Sie für ein neues Volume weniger als den gesamten verfügbaren Datenträgerspeicherplatz?

Antwort: Mehrere Antworten sind möglich, darunter das Partitionieren eines Datenträgers zur Unterstützung von Dualbootszenarien.

Was sind übergreifende Volumes und Stripesetvolumes?

Frage: Beschreiben Sie Szenarien, in denen Sie ein übergreifendes Volume erstellen würden, und solche, in denen Sie ein Stripesetvolume erstellen würden.

Antwort: Sie sollten übergreifende Volumes erstellen, wenn Sie mehrere Bereiche des verfügbaren Speichers auf zwei oder mehr Datenträgern zusammenfassen möchten. Erstellen Sie ein Stripesetvolume, wenn Sie die E/A-Leistung des Computers verbessern möchten.

Demo: Erstellen übergreifender Volumes und Stripesetvolumes

Frage: Worin liegt der Vorteil der Verwendung von Stripesetvolumes, und worin besteht auf der anderen Seite der größte Nachteil?

Antwort: Der Vorteil liegt in der besseren Leistung, der Nachteil in der verminderten Fehlertoleranz.

Demo: Ändern der Größe eines Volumes

Frage: Wann müssen Sie die Größe der Systempartition möglicherweise reduzieren?

Antwort: Mehrere Antworten sind möglich – Für die Aktivierung von BitLocker muss zum Beispiel eine unverschlüsselte Partition verfügbar sein. In manchen Fällen ist diese auf einem Computer nicht vorhanden, sodass sich eine Verkleinerung des Systemvolumes als sinnvoll erweisen könnte. Sie können erwähnen, dass durch Fragmentierung und die Platzierung bestimmter Dateitypen auf den Datenträgern (z. B. die Masterdateitabelle (MFT)) möglicherweise nicht der gesamte verfügbare Speicherplatz für ein neues Volume verwendet werden kann.

Detaillierte Demoschritte

Demo: Erstellen eines einfachen Volumes

Detaillierte Demoschritte

Erstellen eines einfachen Volumes mit der Datenträgerverwaltung

1. Klicken Sie gegebenenfalls auf LON-CL1 auf **Start**, klicken Sie mit der rechten Maustaste auf **Computer**, und klicken Sie anschließend auf **Verwalten**.
2. Klicken Sie in der Liste **Computerverwaltung (Lokal)** auf **Datenträgerverwaltung**.
3. Klicken Sie in der Datenträgerverwaltung von Datenträger 2 mit der rechten Maustaste auf **Nicht zugeordnet**, und klicken Sie anschließend auf **Neues einfaches Volume**.
4. Klicken Sie im **Assistenten zum Erstellen neuer einfacher Volumes** auf **Weiter**.
5. Geben Sie auf der Seite **Volumegröße festlegen** im Feld **Größe des einfachen Volumes in MB** den Wert „100“ ein, und klicken Sie auf **Weiter**.
6. Klicken Sie auf der Seite **Laufwerksbuchstaben oder -pfad zuordnen** auf **Weiter**.
7. Geben Sie auf der Seite **Partition formatieren** im Feld **Volumebezeichnung** die Zeichenfolge „Einfach“ ein, klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**.

Erstellen eines einfachen Volumes mithilfe von DiskPart.exe

1. Klicken Sie gegebenenfalls auf **Start**, zeigen Sie auf **Alle Programme**, und klicken Sie dann auf **Zubehör**. Klicken Sie mit der rechten Maustaste auf Eingabeaufforderung, und klicken Sie dann auf **Als Administrator ausführen**.
2. Geben Sie an der Eingabeaufforderung „DiskPart“ ein, und drücken Sie dann die EINGABETASTE.
3. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl „list disk“ ein, und drücken Sie anschließend die EINGABETASTE.
4. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl „select disk 3“ ein, und drücken Sie dann die EINGABETASTE.
5. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl „create partition primary size=100“ ein, und drücken Sie dann die EINGABETASTE.
6. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl „list partition“ ein, und drücken Sie dann die EINGABETASTE.
7. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl „select partition 2“ ein, und drücken Sie dann die EINGABETASTE.
8. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl „format fs=ntfs label=simple2 quick“ ein, und drücken Sie dann die EINGABETASTE.
9. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl „Assign“ ein, und drücken Sie dann die EINGABETASTE.

Demo: Erstellen übergreifender Volumes und Stripesetvolumes

Detaillierte Demoschritte

Erstellen eines übergreifenden Volumes

1. Klicken Sie in der Datenträgerverwaltung von LON-CL1 auf Datenträger 2 mit der rechten Maustaste auf **Nicht zugeordnet**, und klicken Sie dann auf **Neues übergreifendes Volume**.
2. Klicken Sie im Assistenten **Assistenten zum Erstellen neuer übergreifender Volumes** auf **Weiter**.
3. Geben Sie auf der Seite **Datenträger auswählen** im Feld **Speicherplatz in MB** den Wert „100“ ein.
4. Klicken Sie in der Liste **Verfügbar** auf **Datenträger 3**, und klicken Sie dann auf **Hinzufügen >**.
5. Klicken Sie in der Liste **Ausgewählt** auf **Datenträger 3**, geben Sie im Feld **Speicherplatz in MB** den Wert „250“ ein, und klicken Sie auf **Weiter**.
6. Klicken Sie auf der Seite **Laufwerksbuchstaben oder -pfad zuordnen** auf **Weiter**.
7. Geben Sie auf der Seite **Partition formatieren** im Feld **Volumebezeichnung** den Namen „Übergreifend“ ein, klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**.
8. Klicken Sie im Dialogfeld **Datenträgerverwaltung** auf **Ja**.

Erstellen eines Stripesetvolumes

1. Klicken Sie in der Datenträgerverwaltung auf **Datenträger 2**, und klicken Sie dann auf **Neues Stripesetvolume**.
2. Klicken Sie im **Assistenten zum Erstellen neuer Stripesetvolumes** auf **Weiter**.
3. Klicken Sie auf der Seite **Datenträger auswählen** in der Liste **Verfügbar** auf **Datenträger 3**, und klicken Sie anschließend auf **Hinzufügen >**.
4. Geben Sie auf der Seite **Datenträger auswählen** im Feld **Speicherplatz in MB** den Wert „512“ ein, und klicken Sie dann auf **Weiter**.
5. Klicken Sie auf der Seite **Laufwerksbuchstaben oder -pfad zuordnen** auf **Weiter**.
6. Geben Sie auf der Seite **Partition formatieren** im Feld **Volumebezeichnung** die Zeichenfolge „Stripeset“ ein, klicken Sie auf **Weiter**, und klicken Sie dann auf **Fertig stellen**.

Demo: Ändern der Größe eines Volumes

Detaillierte Demoschritte

Verkleinern eines Volumes mit Diskpart.exe

1. Wechseln Sie auf LON-CL1 in das Eingabeaufforderungsfenster.
2. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl „list disk“ ein, und drücken Sie anschließend die EINGABETASTE.
3. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl „select disk 2“ ein, und drücken Sie dann die EINGABETASTE.
4. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl „list volume“ ein, und drücken Sie anschließend die EINGABETASTE.

5. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl „**select volume 6**“ ein, und drücken Sie dann die EINGABETASTE.
6. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl „**shrink desired = 50**“ ein, und drücken Sie dann die EINGABETASTE.
7. Geben Sie an der Eingabeaufforderung DISKPART> den Befehl „**exit**“ ein, und drücken Sie die EINGABETASTE.
8. Wechseln Sie zur Datenträgerverwaltung, und zeigen Sie die neue Volumegröße an.

Erweitern eines Volumes mit der Datenträgerverwaltung

1. Klicken Sie in Datenträger 2 mit der rechten Maustaste auf das **Einfache Laufwerk (F:)**, und klicken Sie dann auf **Volume erweitern**.
2. Klicken Sie im **Assistenten zum Erweitern von Volumes** auf **Weiter**.
3. Geben Sie im Feld **Speicherplatz in MB** den Wert „**50**“ ein, klicken Sie auf **Weiter** und dann auf **Fertig stellen**.
4. Schließen Sie alle geöffneten Fenster.

Hinweis: Weitere Informationen über „diskpart“ finden Sie unter <http://go.microsoft.com/fwlink/?LinkId=153231>.

Lektion 3

Verwalten von Datenträgern in Windows 7

Inhalt:

Fragen und Antworten	40
Detaillierte Demoschritte	41

Fragen und Antworten

Was sind Datenträgerkontingente?

Frage: Wie können Sie mehr freien Speicherplatz zur Verfügung stellen, nachdem die Kontingentgrenze überschritten wurde?

Antwort: Im Folgenden finden Sie Ideen, wie nach dem Überschreiten der Kontingentgrenze mehr Speicherplatz zur Verfügung gestellt werden kann:

- Löschen unnötiger Dateien
- Übernehmen der Eigentümerschaft für nicht benutzerspezifische Dateien durch einen anderen Benutzer
- Erhöhen der Kontingentgrenze, wenn die Volumegröße und die Richtliniengenehmigungen dies zulassen

Demo: Konfigurieren von Datenträgerkontingenten (optional)

Frage: Kann die Kontingentverwaltung in Ihren Unternehmen sinnvoll eingesetzt werden?

Antwort: Mehrere Antworten sind möglich. In den meisten Fällen ist es nicht erforderlich, die Datenträgerverwendung für Computer, auf denen Windows 7 ausgeführt wird, einzuschränken. Dies könnte jedoch sinnvoll sein, wenn mehrere Benutzer den gleichen Computer verwenden, oder wenn in einer Arbeitsgruppe Peer-to-Peer-Netzwerkfunktionen ausgeführt werden. Kontingente werden in der Regel auf Servern implementiert.

Detaillierte Demoschritte

Demo: Konfigurieren von Datenträgerkontingenten (optional)

Detaillierte Demoschritte

Erstellen von Kontingenten auf einem Volume

1. Klicken Sie auf LON-CL1 auf **Start** und anschließend auf **Computer**.
2. Klicken Sie mit der rechten Maustaste auf **Stripeset (I:)**, und klicken Sie dann auf **Eigenschaften**.
3. Klicken Sie im Dialogfeld **Eigenschaften von Stripeset (I:)** auf die Registerkarte **Kontingent**.
4. Aktivieren Sie das Kontrollkästchen **Kontingent** auf der Registerkarte **Kontingentverwaltung aktivieren**.
5. Aktivieren Sie das Kontrollkästchen **Speicherplatz bei Überschreitung der Kontingentgrenze verweigern**.
6. Klicken Sie auf **Speicherplatz beschränken auf**, geben Sie im angrenzenden Feld den Wert „6“ ein, und klicken Sie dann in der Liste **KB** auf **MB**.
7. Geben Sie im Feld **Warnstufe festlegen auf** den Wert „4“ ein, und klicken Sie dann in der Liste **KB** auf **MB**.
8. Aktivieren Sie das Kontrollkästchen **Ereignis bei Warnstufenüberschreitung protokollieren**, und klicken Sie anschließend auf **OK**.
9. Überprüfen Sie die Nachricht im Dialogfeld **Datenträgerkontingent**, und klicken Sie dann auf **OK**.

Erstellen von Testdateien

1. Öffnen Sie ein Eingabeaufforderungsfenster.
2. Geben Sie an der Eingabeaufforderung „i:“ ein, und drücken Sie dann die EINGABETASTE.
3. Geben Sie an der Eingabeaufforderung „fsutil file createnew 2mb-file 2097152“ ein, und drücken Sie dann die EINGABETASTE.
4. Geben Sie an der Eingabeaufforderung „fsutil file createnew 1kb-file 1024“ ein, und drücken Sie dann die EINGABETASTE.
5. Schließen Sie das Fenster Eingabeaufforderung.

Testen der konfigurierten Kontingente durch Erstellen von Dateien mithilfe eines Standardbenutzerkontos

1. Melden Sie sich ab, und melden Sie sich dann beim virtuellen Computer LON-CL1 als **Contoso\Alan** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start** und auf **Computer**, und doppelklicken Sie anschließend auf **Stripeset (I:)**.
3. Klicken Sie auf der Symbolleiste auf **Neuer Ordner**.
4. Geben Sie „**Alans Dateien**“ ein, und drücken Sie dann die EINGABETASTE.
5. Klicken Sie in der Dateiliste mit der rechten Maustaste auf **2mb-file**, ziehen Sie sie in Alans Dateien, und klicken Sie dann auf **Hierher kopieren**.
6. Doppelklicken Sie auf **Alans Dateien**.

7. Klicken Sie mit der rechten Maustaste auf **2mb-file**, und klicken Sie anschließend auf **Kopieren**.
8. Drücken Sie STRG+V.
9. Klicken Sie in der Adressleiste auf **Stripeset (I:)**.
10. Klicken Sie in der Dateiliste mit der rechten Maustaste auf **1kb-file**, ziehen Sie sie in Alans Dateien, und klicken Sie dann auf **Hierher kopieren**.
11. Doppelklicken Sie auf Alans Dateien.
12. Klicken Sie mit der rechten Maustaste auf **2mb-file**, und klicken Sie anschließend auf **Kopieren**.
13. Drücken Sie STRG+V.
14. Überprüfen Sie die Nachricht im Dialogfeld **Element kopieren**, und klicken Sie dann auf **Abbrechen**.

Überprüfen von Kontingentwarnungen und Ereignisprotokollmeldungen

1. Melden Sie sich ab, und melden Sie sich dann beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start** und dann auf **Computer**.
3. Klicken Sie mit der rechten Maustaste auf **Stripeset (I:)**, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie im Dialogfeld **Eigenschaften von Stripeset (I:)** auf die Registerkarte **Kontingent**, und klicken Sie dann auf **Kontingenteinträge**.
5. Doppelklicken Sie unter **Kontingenteinträge für Stripeset (I:)** in der Spalte **Anmeldename** auf **Contoso\Alan**.
6. Klicken Sie im Dialogfeld **Kontingenteinstellungen für Alan Brewer (CONTOSO\alan)** auf **OK**.
7. Schließen Sie die **Kontingenteinträge für Stripeset (I:)**.
8. Schließen Sie **Eigenschaften von Stripeset (I:) Stripeset (G:)**.
9. Klicken Sie auf **Start**, und geben Sie im Feld **Suche** das Wort „**Ereignis**“ ein.
10. Klicken Sie in der Liste **Programme** auf **Ereignisanzeige**.
11. Erweitern Sie in der Liste **Ereignisanzeige (Lokal)** die **Windows-Protokolle**, und klicken Sie dann auf **System**.
12. Klicken Sie mit der rechten Maustaste auf **System**, und klicken Sie dann auf **Aktuelles Protokoll filtern**.
13. Geben Sie im Feld **<Alle Ereignis-IDs>** den Wert „**36**“ ein, und klicken Sie anschließend auf **OK**.
14. Überprüfen Sie den aufgeführten Eintrag.
15. Schließen Sie alle geöffneten Fenster.

Lektion 4

Installieren und Konfigurieren von Gerätetreibern

Inhalt:

Fragen und Antworten	44
Detaillierte Demoschritte	45

Fragen und Antworten

Installieren von Geräten und Treibern

Frage: In welchen Schritten wird ein Treiber mithilfe des Tools Pnputil.exe im Treiberspeicher installiert?

Antwort: Folgende Schritte sind erforderlich:

1. Identifizieren Sie den Namen des Gerätetreibers.
2. Starten Sie das Tool Pnputil.exe über eine Eingabeaufforderung mit erhöhten Rechten.
3. Verwenden Sie den Parameter -a zusammen mit dem Pfad und dem Namen des Treibers, um den Treiber zum Treiberspeicher hinzuzufügen.
4. Notieren Sie den neu zugewiesenen Treibernamen einschließlich der Nummer.

Demo: Verwalten von Treibern

Frage: Welche Optionen zum Ausführen einer Treiberwiederherstellung haben Sie, wenn Ihr Computer aufgrund eines Treiberproblems nicht normal startet?

Antwort: Versuchen Sie, den Computer im abgesicherten Modus zu starten und die Treiber wiederherzustellen.

Detaillierte Demoschritte

Demo: Verwalten von Treibern

Detaillierte Demoschritte

Aktualisieren eines Gerätetreibers

1. Klicken Sie auf LON-CL1 auf **Start**, klicken Sie mit der rechten Maustaste auf **Computer**, und klicken Sie dann auf **Verwalten**.
2. Klicken Sie in der Computerverwaltung auf **Geräte-Manager**.
3. Erweitern Sie **Tastaturen**, klicken Sie mit der rechten Maustaste auf **Standardtastatur (PS/2)**, und klicken Sie anschließend auf **Treibersoftware aktualisieren**.
4. Klicken Sie im Dialogfeld **Treibersoftware aktualisieren – Standardtastatur (PS/2)** auf **Auf dem Computer nach Treibersoftware suchen**.
5. Klicken Sie auf der Seite **Auf dem Computer nach Treibersoftware suchen** auf **Aus einer Liste von Gerätetreibern auf dem Computer auswählen**.
6. Klicken Sie in der Liste **Kompatible Hardware anzeigen** auf **Erweiterte PC/AT-PS/2-Tastatur (101/102 Tasten)**, und klicken Sie anschließend auf **Weiter**.
7. Klicken Sie auf **Schließen**.
8. Klicken Sie im Dialogfeld **Geänderte Systemeinstellungen** auf **Ja**, um den Computer neu zu starten.

Wiederherstellen eines Gerätetreibers

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, klicken Sie mit der rechten Maustaste auf **Computer**, und klicken Sie dann auf **Verwalten**.
3. Klicken Sie in der Computerverwaltung auf **Geräte-Manager**.
4. Erweitern Sie **Tastaturen**, klicken Sie mit der rechten Maustaste auf **Erweiterte PC/AT-PS/2-Tastatur (101/102 Tasten)**, und klicken Sie dann auf **Eigenschaften**.
5. Klicken Sie im Dialogfeld **Eigenschaften von Erweiterte PC/AT-PS/2-Tastatur (101/102 Tasten)** auf die Registerkarte **Treiber**.
6. Klicken Sie auf **Vorheriger Treiber**.
7. Klicken Sie im Dialogfeld **Zurücksetzen des Treiberpakets** auf **Ja**.
8. Klicken Sie auf **Schließen**, und klicken Sie dann im Dialogfeld **Geänderte Systemeinstellungen** auf **Ja**, um den Computer neu zu starten.
9. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
10. Klicken Sie auf **Start**, klicken Sie mit der rechten Maustaste auf **Computer**, und klicken Sie dann auf **Verwalten**.
11. Klicken Sie in der Computerverwaltung auf **Geräte-Manager**.

12. Erweitern Sie **Tastaturen**, und klicken Sie dann auf **Standardtastatur (PS/2)**.
13. Überprüfen Sie, ob der Treiber erfolgreich zurückgesetzt wurde.
14. Schließen Sie die Computerverwaltung.

Installieren eines Treibers im Treiberspeicher

1. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Zubehör**, und klicken Sie dann mit der rechten Maustaste auf **Eingabeaufforderung**.
2. Klicken Sie auf **Als Administrator ausführen**.
3. Geben Sie an der Eingabeaufforderung „**E:**“ ein, und drücken Sie dann die EINGABETASTE.
4. Geben Sie an der Eingabeaufforderung die Zeichenfolge „**pnputil -a „E:\Labfiles\Mod02\HP Deskjet 960c series\hpf960k.inf”**“ ein, und drücken Sie dann die EINGABETASTE.
5. Geben Sie an der Eingabeaufforderung „**pnputil -e**“ ein, und drücken Sie dann die EINGABETASTE. Notieren Sie die Treiberversion und das Datum des Treibers, den Sie gerade in den Speicher installiert haben.

Lernzielkontrollen und Kernpunkte der Unterrichtseinheit

Fragen zur Lernzielkontrolle

Frage 1: Sie implementieren eine 64-Bit-Version von Windows 7 und müssen den Datenträger partitionieren, um 25 Volumes zu unterstützen, von denen einige größer als 2 TB sind. Können Sie diese Konfiguration mit einer einzigen Festplatte implementieren?

Antwort: Ja, Sie können den Datenträger für GPT statt für MBR formatieren. Ein GPT-Datenträger unterstützt bis zu 128 Volumes, jeweils weitaus größer als 2 TB. Außerdem können Sie von einem GPT-Datenträger 64-Bit-Versionen von Windows 7 starten.

Frage 2: Sie haben mit „diskpart.exe“ ein Volume auf einer neu installierten Festplatte erstellt. Im Anschluss daran möchten Sie mit „diskpart.exe“ die folgenden Aufgaben ausführen:

- Formatieren des Volumes für NTFS
- Zuweisen des nächsten verfügbaren Laufwerksbuchstabens
- Zuweisen der Volumebezeichnung „Umsatzdaten“

Welche beiden Befehle müssen Sie für diese Aufgaben verwenden?

Antwort: Die beiden Befehle lauten folgendermaßen:

```
format fs=ntfs label=Umsatzdaten
```

```
assign
```

Frage 3: Ihr Unternehmen hat vor kurzem Windows Update so konfiguriert, dass die Computer der Buchhaltungsabteilung um 03:00 Uhr automatisch aktualisiert werden. Dies steht mit der wöchentlichen Defragmentierung der Computer am Mittwochmorgen in Konflikt. Sie müssen die geplante Defragmentierungsaufgabe neu konfigurieren, sodass sie stattdessen am Dienstag um Mitternacht ausgeführt wird. Listen Sie die Schritte auf, die zum Ändern des Defragmentierungszeitplans erforderlich sind.

Antwort: Führen Sie folgende Schritte aus, um den Defragmentierungszeitplan zu ändern:

1. Klicken Sie in Windows-Explorer mit der rechten Maustaste auf ein Volume, klicken Sie auf **Eigenschaften**, klicken Sie auf die **Registerkarte Extras** und anschließend auf **Jetzt defragmentieren**.
2. Klicken Sie im Fenster Datenträgerdefragmentierung auf Zeitplan konfigurieren.
3. Klicken Sie im Fenster **Datenträgerdefragmentierung: Zeitplan ändern** den Wert für **Tag auswählen** in **Dienstag**, und ändern Sie den Wert für **Uhrzeit wählen** in **0:00 Uhr (Mitternacht)**. Klicken Sie auf **OK**.
4. Klicken Sie im Fenster **Datenträgerdefragmentierung** auf **Schließen** und anschließend im Fenster **Eigenschaften** auf **OK**.

Frage 4: Sie haben vor kurzem ein Upgrade auf Windows 7 durchgeführt, und gelegentlich treten Probleme mit den Tastenkombinationen auf der Tastatur auf. Beschreiben Sie die erste Aktion, die Sie ausführen würden, um das Problem zu lösen, und nennen Sie die einzelnen Schritte, die für diese Aktion erforderlich sind.

Antwort:

1. Aktualisieren des Gerätetreibers für die Tastatur. Führen Sie im Geräte-Manager folgende Schritte aus, um den für die Tastatur verwendeten Treiber manuell zu aktualisieren:
2. Doppelklicken Sie auf die Gerätekategorie **Tastatur**.
3. Klicken Sie mit der rechten Maustaste auf das Gerät, und klicken Sie dann auf **Treibersoftware aktualisieren**.
4. Befolgen Sie die Anweisungen im **Assistenten zum Aktualisieren von Treibersoftware**.

Häufige Probleme

Identifizieren Sie die Ursachen für die folgenden, häufig auftretenden Probleme und nennen Sie Tipps zur Problembehandlung. Antworten finden Sie in den entsprechenden Lektionen der Unterrichtseinheit oder im Inhalt der Kursbegleit-CD.

Problem	Tipps zur Problembehandlung
Konfigurieren von Datenträgerkontingenten auf mehreren Volumes	Wenn Sie ein Kontingent erstellt haben, können Sie dieses exportieren und anschließend für ein anderes Volume importieren. Neben der Einrichtung der Kontingenteinstellungen auf einem einzelnen Computer mit den oben genannten Methoden können Sie Kontingente auch mithilfe von Gruppenrichtlinieneinstellungen konfigurieren. Auf diese Weise können Administratoren mehrere Computer mit den gleichen Kontingenteinstellungen konfigurieren.
Überschreiten der Kontingentgrenze	Der Benutzer kann Folgendes versuchen, um nach Überschreiten der Kontingentgrenze mehr freien Speicherplatz zu erhalten: <ul style="list-style-type: none"> • Löschen unnötiger Dateien • Übernehmen der Eigentümerschaft für nicht benutzerspezifische Dateien durch einen anderen Benutzer • Erhöhen der Kontingentgrenze, wenn die Volumengröße und die Richtliniengenehmigungen dies zulassen
Wenn bei Ihnen ein Hardwareproblem auftritt, kann dieses von Hardware oder einem Gerätetreiber verursacht werden. Die Behandlung von Hardwareproblemen beginnt häufig mit der Problembehandlung bei Gerätetreibern.	Beantworten Sie die Fragen, um ein Gerätetreiberproblem zu identifizieren: <ul style="list-style-type: none"> • Haben Sie vor kurzem den Gerätetreiber oder andere Software aktualisiert, die mit der Hardware zusammenhängt? Wenn dies der Fall ist, stellen Sie den Treiber in der vorherigen Version wieder her. • Treten gelegentliche Probleme auf, oder ist das Gerät nicht mit der aktuellen Version von Windows kompatibel? Wenn dies der Fall ist, aktualisieren Sie den Gerätetreiber.

	<ul style="list-style-type: none"> • Hat die Hardware plötzlich aufgehört zu funktionieren? Wenn dies der Fall ist, aktualisieren Sie den Gerätetreiber. Wenn das Problem dadurch nicht behoben wird, installieren Sie den Gerätetreiber neu. Wenn das Problem weiterhin auftritt, versuchen Sie, das Hardwareproblem zu beheben.
Überprüfen, ob für einen Datenträger eine Defragmentierung erforderlich ist	Um zu überprüfen, ob für einen Datenträger eine Defragmentierung erforderlich ist, wählen Sie unter Defragmentierung den Datenträger aus, den Sie defragmentieren möchten, und klicken Sie dann auf Datenträger analysieren . Nachdem Windows die Analyse des Datenträgers beendet hat, kontrollieren Sie in der Spalte Zuletzt ausgeführt den Prozentsatz der Fragmentierung auf dem Datenträger. Bei einem hohen Prozentsatz sollten Sie den Datenträger defragmentieren.
Anzeigen von Schattenkopie-Speicherinformationen	Mit dem Verwaltungsbefehlszeilenprogramm des Volumeschattenkopiedienstes können Sie Schattenkopie-Speicherinformationen anzeigen. Öffnen Sie eine Eingabeaufforderung mit erhöhten Rechten, und geben Sie „vssadmin list shadowstorage“ ein. Für jedes Volume wird der verwendete, der zugeordnete und der maximale Schattenkopie-Speicherplatz angezeigt.

Best Practices

Ergänzen oder ändern Sie die folgenden bewährten Methoden abhängig von Ihren eigenen Arbeitssituationen:

- Zeichnen Sie jede Änderung auf, die an einem Computer vorgenommen wird. Diese Aufzeichnungen können in einem physischen Notizbuch erfolgen, das am Computer befestigt wird, oder in einer Tabelle oder Datenbank, die auf einer zentralen Freigabe mit nächtlicher Sicherung verfügbar ist.
- Wenn Sie ein Protokoll über alle Änderungen führen, die an einem Computer vorgenommen wurden, können Sie die Änderungen zurückverfolgen, um Probleme zu beheben und den Supportmitarbeitern die richtigen Konfigurationsinformationen mitzuteilen. Mit der Zuverlässigkeitsüberwachung können Änderungen am System, wie z. B. die Installation oder Deinstallation von Anwendungen, nachverfolgt werden.
- Beachten Sie bei der Entscheidung, welchen Volumetyp Sie erstellen möchten, die folgenden Fragen:
- Wie wichtig sind die Daten oder die Informationen auf dem Computer?
- Kann die automatische Replikation schnell und einfach eingerichtet werden?
- Welche Auswirkungen hätte es auf Ihr Geschäft, wenn Ihr Computer nicht mehr gestartet werden könnte?
- Erfüllt der Computer mehrere Funktionen?
- Werden die Daten auf dem Computer regelmäßig gesichert?
- Nehmen Sie bei Bedarf die Informationen aus der folgenden Tabelle zur Hilfe.

Aufgabe	Referenzmaterialien
Hinzufügen eines neuen Datenträgers	http://go.microsoft.com/fwlink/?LinkId=64100
Empfehlungen zur Datenträgerverwaltung	http://go.microsoft.com/fwlink/?LinkId=153231
Bestätigen Sie, dass Sie Mitglied der Sicherheitsoperatoren- oder der Administratorengruppe sind.	Suchen Sie in Hilfe und Support nach „Standardkonto“ und „Administratorkonto“. Informationen zu Gruppen: http://go.microsoft.com/fwlink/?LinkId=64099
Erstellen von Partitionen oder Volumes	http://go.microsoft.com/fwlink/?LinkId=64106 • http://go.microsoft.com/fwlink/?LinkId=64107
Verwaltung und Installation von Geräten	http://go.microsoft.com/fwlink/?LinkId=143990
Informationen zur Treibersignierung, einschließlich der Anforderungen, finden Sie auf der Seite Driver Signing Requirements for Windows im Windows Hardware Developer Central.	http://go.microsoft.com/fwlink/?LinkId=14507
Formatieren von Volumes auf dem Datenträger	http://go.microsoft.com/fwlink/?LinkId=64101 http://go.microsoft.com/fwlink/?LinkId=64104 http://go.microsoft.com/fwlink/?LinkId=64105
Übersicht über die Datenträgerverwaltung	http://go.microsoft.com/fwlink/?LinkId=64098
Leistungsoptimierungsrichtlinien	http://go.microsoft.com/fwlink/?LinkId=121171
Windows 7-Springboard-Reihe	http://go.microsoft.com/fwlink/?LinkId=147459
Windows-Gerätefunktion	http://go.microsoft.com/fwlink/?LinkId=132146
Empfehlungen zur Datenträgerverwaltung	http://go.microsoft.com/fwlink/?LinkId=153231

Tools

Tool	Verwendung	Bezugsquelle
Defrag.exe	Ausführen von Datenträgerdefragmentierungsaufgaben über die Befehlszeile	Eingabeaufforderung
Geräte-Manager	Anzeigen und Aktualisieren von Hardwareeinstellungen und Treibersoftware für Geräte, z. B. interne Festplatten, Laufwerke, Soundkarten, Video- oder Grafikkarten, Arbeitsspeicher, Prozessoren und andere interne Computerkomponenten	Systemsteuerung
Device Stage	Unterstützung bei der Interaktion mit beliebigen kompatiblen Geräten, die an den Computer angeschlossen werden In Device Stage können Sie in einem einzigen Fenster den Status des Geräts anzeigen und gängige Aufgaben ausführen. Abbildungen vereinfachen den Überblick über die vorhandenen Geräte.	Taskleiste

Geräte und Drucker	Bietet Benutzern einen zentralen Speicherort, an dem sie alle Geräte finden und verwalten können, die an einen Windows 7-basierten Computer angeschlossen sind. Bietet zudem schnellen Zugriff auf den Gerätestatus, Produktinformationen und wichtige Funktionen, z. B. Faxen und Scannen, um die Benutzerfreundlichkeit der mit Windows 7 verbundenen Geräte zu verbessern.	Systemsteuerung
Defragmentierung	Neuanordnung fragmentierter Daten, damit Datenträger und Laufwerke effizienter funktionieren können	Klicken Sie in Windows-Explorer mit der rechten Maustaste auf ein Volume, klicken Sie auf Eigenschaften , klicken Sie auf die Registerkarte Extras und anschließend auf Jetzt defragmentieren .
Datenträgerverwaltung	Verwalten von Datenträgern und Volumes (dynamische und Basisvolumes, lokal oder auf Remotecomputern)	Klicken Sie auf Start , geben Sie im Suchfeld „diskmgmt.msc“ ein, und klicken Sie dann in der Ergebnisliste auf diskmgmt.msc .
Diskpart.exe	Verwalten von Datenträgern, Volumes und Partitionen über die Befehlszeile oder in Windows PE	Öffnen Sie eine Eingabeaufforderung, und geben Sie „diskpart“ ein.
Fsutil.exe	Ausführen von Aufgaben im Zusammenhang mit der Dateizuordnungstabelle (FAT) und NTFS-Dateisystemen, z. B. Verwalten von Analysepunkten, Verwalten von Dateien mit geringer Dichte oder Aufheben der Bereitstellung eines Volumes	Eingabeaufforderung (mit erhöhten Rechten)
Pnputil.exe	Hinzufügen und Verwalten von Treibern im Gerätespeicher	Eingabeaufforderung (mit erhöhten Rechten)
Kontingenteinstellungen	Nachverfolgen und Einschränken der Datenträgerbelegung	Klicken Sie in Windows-Explorer mit der rechten Maustaste auf ein Volume, klicken Sie auf Eigenschaften , auf Kontingent und anschließend auf Kontingenteinstellungen anzeigen .
Dateisignaturverifizierung (Sigverf.exe)	Überprüfen, ob sich im Systembereich des Computers unsignierte Gerätetreiber befinden	Startmenü
Volumeschattenkopie-Dienst (Vssadmin.exe)	Anzeigen und Verwalten des Schattenkopiespeicherbereichs	Eingabeaufforderung (mit erhöhten Rechten)

Windows Update	Automatisches Anwenden von Updates für Software, die zur Vermeidung oder Behebung von Problemen beitragen oder die Funktionsweise oder Benutzerfreundlichkeit Ihres Computers verbessern können.	Online
----------------	--	--------

Allgemeine Begriffe, Definitionen und Beschreibungen

Begriff	Definition
Basisdatenträger	Ein Datenträger, der als Basisspeicher initialisiert wurde Ein Basisdatenträger enthält Basisvolumes, z. B. primäre Partitionen, erweiterte Partitionen und logische Laufwerke.
Dynamischer Datenträger	Ein Datenträger, der als dynamischer Speicher initialisiert wurde Ein dynamischer Datenträger enthält dynamische Volumes, z. B. einfache Volumes, übergreifende Volumes, Stripesetvolumes, gespiegelte Volumes und RAID 5-Volumes.
Volume	Eine Speichereinheit, die aus freiem Speicherplatz auf einem oder mehreren Datenträgern erstellt wurde. Sie können diese Speichereinheit mit einem Dateisystem formatieren und ihr einen Laufwerkbuchstaben zuweisen. Volumes auf dynamischen Datenträgern können jedes der folgenden Layouts haben: Alle Volumes auf einem physischen Datenträger müssen entweder Basisvolumes oder dynamische Volumes sein, und jeder Datenträger muss partitioniert sein. Sie können den Inhalt eines Volumes anzeigen, indem Sie in Windows-Explorer oder in Arbeitsplatz auf sein Symbol klicken. Eine einzelne Festplatte kann mehrere Volumes aufweisen, und Volumes können auch mehrere Datenträger umfassen.
Systemvolume	Das Datenträgervolume mit den hardwarespezifischen Dateien, die zum Starten von Windows benötigt werden. Auf x86-Computern muss das Systemvolume ein primäres Volume sein, das als „aktiv“ gekennzeichnet ist. Diese Anforderung kann auf jedem Laufwerk des Computers erfüllt werden, das beim Starten des Betriebssystems vom System-BIOS durchsucht wird. Das Systemvolume kann mit dem Startvolume identisch sein; diese Konfiguration ist nicht erforderlich. Es gibt nur ein Systemvolume.
Startvolume	Das Datenträgervolume, das die Windows-Betriebssystemdateien und die unterstützenden Dateien enthält. Das Startvolume kann mit dem Systemvolume identisch sein; diese Konfiguration ist nicht erforderlich. In einem Multistartsystem gibt es für jedes Betriebssystem ein Startvolume.
Partition	Ein zusammenhängender Speicherbereich auf einem physischen oder logischen Datenträger, der sich wie ein physisch getrennter Datenträger verhält
Datenträgerpartitionierung	Das Unterteilen des Speichers auf einem physischen Datenträger in überschaubare Abschnitte, die die Anforderungen eines Computerbetriebssystems erfüllen
LBA (Logical Block Address)	Eine Methode, eine Datenadresse auf einem Speichermedium auszudrücken. Wird in SCSI- und IDE-Laufwerken verwendet, um die Spezifikationen des Laufwerks in Adressen zu übersetzen, die vom erweiterten BIOS verwendet werden können. LBA wird mit Laufwerken verwendet, die größer als 528 MB sind.

Fragen und Antworten zur Lernzielkontrolle

Frage: In Übung 1 haben Sie in „Diskpart“ den Befehl „assign“ verwendet, um einem neu erstellten Volume einen Laufwerksbuchstaben zuzuweisen. Was können Sie außer dem Zuweisen von Laufwerksbuchstaben noch tun?

Antwort: Die Kursteilnehmer können das Volume in einem leeren Ordner auf einem vorhandenen NTFS-Volume aktivieren. Dies hat den Vorteil, dass Sie die durch das Alphabet vorgegebene Beschränkung auf 26 Treiberbuchstaben umgehen können.

Frage: In Übung 2 haben Sie die Datenträgerbelegung mithilfe von lokalen Datenträgerkontingenten verwaltet. Zwar ist dies ein nützliches lokales Verwaltungstool, doch welche anderen Tools zur Speicherplatzverwaltung können Sie in einem Unternehmensnetzwerk auf Windows Server® 2008-Basis verwenden?

Antwort: Die Dateidienste-Rolle „Ressourcen-Manager für Dateiserver“ ermöglicht Ihnen die Verwaltung von Datenträgerkontingenten und stellt zudem Kontingentvorlagen, Dateiprüfungen und Speicherberichtsfunktionen bereit.

Frage: In Übung 3 haben Sie die Treiberwiederherstellung verwendet, um ein zuvor durchgeführtes Treiberupdate rückgängig zu machen. Wie können Sie ein treiberbezogenes Problem beheben, wenn der Computer nicht ordnungsgemäß gestartet wird?

Antwort: Sie können den Computer im abgesicherten Modus starten und dann auf den Geräte-Manager zugreifen, um das Feature zur Treiberwiederherstellung zu verwenden. Wenn dies nicht funktioniert, können Sie versuchen, das Problem mithilfe der Windows RE zu beheben.

Unterrichtseinheit 3

Konfigurieren von Dateizugriff und Druckern auf Windows® 7-Clientcomputern

Inhalt:

Lektion 1: Übersicht über Authentifizierung und Autorisierung	55
Lektion 2: Verwalten des Dateizugriffs in Windows 7	57
Lektion 3: Verwalten von freigegebenen Ordnern	62
Lektion 4: Konfigurieren der Dateikomprimierung	65
Lektion 5: Verwalten von Druckfunktionen	68
Lernzielkontrollen und Kernpunkte der Unterrichtseinheit	71
Fragen und Antworten zur Lernzielkontrolle	74

Lektion 1

Übersicht über Authentifizierung und Autorisierung

Inhalt:

Fragen und Antworten

56

Fragen und Antworten

Authentifizierungs- und Autorisierungsverfahren

Frage: Welche Authentifizierungsmethode wird verwendet, wenn sich ein Clientcomputer, auf dem das Windows 7-Betriebssystem ausgeführt wird, bei Active Directory anmeldet?

Antwort: Es wird das Kerberos-Protokoll, Version 5, verwendet sofern keine Smartcards verwendet werden. Wenn Smartcards verwendet werden, ist die Authentifizierungsmethode die Zertifikatszuordnung.

Neue Authentifizierungsfeatures in Windows 7

Frage: Nennen Sie Verwendungsmöglichkeiten biometrischer Fingerabdruckgeräte in Windows 7?

Antwort: Unterschiedliche Antworten sind möglich. Drei primäre Verwendungen sind jedoch:

- Anmelden an Computern.
- Gewähren von Erhöhungsrechten durch die Benutzerkontensteuerung (UAC).
- Sie können Fingerabdruckgeräte in den Gruppenrichtlinieneinstellungen durch Aktivieren, Beschränken oder Blockieren ihrer Verwendung verwalten.

Lektion 2

Verwalten des Dateizugriffs in Windows 7

Inhalt:

Fragen und Antworten	58
Detaillierte Demoschritte	60

Fragen und Antworten

Was sind NTFS-Berechtigungen?

Frage: Müssen Sie Berechtigungen einrichten, um andere Personen am Zugriff auf Ihre Dateien zu hindern?

Antwort: Nein. Die NTFS-Standardberechtigungen ermöglichen es Standardbenutzern nicht, die Dokumente zu lesen, die andere Benutzer in ihrem Ordner „Eigene Dateien“ gespeichert haben. Administratoren können jedoch auf alle Dateien im System zugreifen. Wenn Sie vermeiden möchten, dass Administratoren auf eine Datei zugreifen, müssen Sie eine zusätzliche Sicherheitsmaßnahme, wie z. B. Verschlüsselung, verwenden.

Was ist die Vererbung von Berechtigungen?

Frage 1: Warum reduziert die Vererbung von Berechtigungen die Verwaltungszeit?

Antwort: Administratoren können Berechtigungen auf übergeordneter Ebene ändern und dieselben Berechtigungen an alle Unterordner weitergeben, ohne jedem einzelnen Ordner die Berechtigungen erneut zuweisen zu müssen.

Frage 2: Wenn einer Gruppe die NTFS-Berechtigung für eine bestimmte Ressource verweigert wird, einer anderen Gruppe jedoch die gleiche Berechtigung für diese Ressource gewährt wird, was geschieht mit den Berechtigungen einer Person, die Mitglied beider Gruppen ist?

Antwort: Dem Benutzer wird der Zugriff verweigert.

Auswirkungen des Kopierens und Verschiebens von Dateien und Ordnern auf festgelegte Berechtigungen

Frage: Warum wird der Zeitaufwand für die Verwaltung reduziert, wenn Dateien und Ordner innerhalb der gleichen Partition verschoben werden?

Antwort: Mehrere Antworten sind möglich. Mögliche Antworten: Administratoren müssen sich keine Gedanken um die Änderung der Berechtigungen machen, da diese beibehalten werden, wenn Dateien und Ordner innerhalb der gleichen Partition verschoben werden. Ebenso dürfen Administratoren die Berechtigungen des Zielordners nicht ändern, da dies Auswirkungen auf andere Dateien und Unterordner innerhalb des Ordners haben kann.

Was sind effektive Berechtigungen?

Frage: Wenn einer Gruppe die Berechtigung „Ändern“ für einen Ordner zugewiesen ist und einem Benutzer, der Mitglied dieser Gruppe ist, die Berechtigung „Ändern“ für denselben Ordner verweigert wird, wie lautet dann die effektive Berechtigung des Benutzers für den Ordner?

Antwort: Da die Berechtigung „Verweigern“ gegenüber der Berechtigung „Zulassen“ Vorrang hat, wird dem Benutzer die Berechtigung „Ändern“ für den Ordner verweigert.

Diskussion: Ermitteln von effektiven Berechtigungen

Frage 1: Die Gruppe „Benutzer“ verfügt über die Berechtigung „Schreiben“, die Gruppe „Vertrieb“ über die Berechtigung „Lesen“ für Ordner1. Welche Berechtigungen besitzt „Benutzer1“ für „Ordner1“?

Antwort: „Benutzer1“ verfügt über die Berechtigungen „Lesen“ und „Schreiben“ für „Ordner1“, da „Benutzer1“ Mitglied der Gruppe „Benutzer“ ist, die über die Berechtigung „Schreiben“ verfügt, und Mitglied der Gruppe „Vertrieb“ ist, die über die Berechtigung „Lesen“ verfügt.

Frage 2: Die Gruppe „Benutzer“ verfügt über die Berechtigung „Lesen“ für Ordner1. Die Gruppe Vertrieb verfügt über die Berechtigung „Schreiben“ für Ordner2. Welche Berechtigungen besitzt „Benutzer1“ für „Datei2“?

Antwort: Benutzer1 verfügt über die Berechtigungen „Schreiben“ und „Lesen“ für Datei2, denn Benutzer1 ist Mitglied der Gruppe „Benutzer“, die über die Berechtigung „Lesen“ für Ordner1 verfügt, und Mitglied der Gruppe „Vertrieb“, die über die Berechtigung „Schreiben“ für Ordner2 verfügt. „Datei2“ erbt Berechtigungen sowohl von „Ordner2“ als auch von „Ordner1“.

Frage 3: Die Gruppe „Benutzer“ verfügt über die Berechtigung „Ändern“ für Ordner1. Nur die Gruppe „Vertrieb“ kann auf „Datei2“ zugreifen, und deren Mitglieder können „Datei2“ auch nur lesen. Wie stellen Sie sicher, dass die Gruppe „Vertrieb“ nur über die Berechtigung „Lesen“ für „Datei2“ verfügt?

Antwort: Verhindern Sie die Vererbung von Berechtigungen für Ordner2 oder Datei2. Entfernen Sie die Berechtigungen für „Ordner2“ oder „Datei2“, die „Ordner2“ von „Ordner1“ geerbt hat. Gewähren Sie der Gruppe „Vertrieb“ nur die Berechtigung „Lesen“ für „Ordner2“ oder „Datei2“.

Detaillierte Demoschritte

Demo: Konfigurieren von NTFS-Berechtigungen für Dateien und Ordner

Detaillierte Demoschritte

Erstellen eines Ordners und einer Dokumentdatei

1. Melden Sie sich auf dem virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, klicken Sie auf **Computer**, und doppelklicken Sie dann auf **Lokaler Datenträger (C:)**.
3. Klicken Sie auf der Symbolleiste auf **Neuer Ordner**.
4. Geben Sie als Ordnername „Projektdokumente“ ein.
5. Doppelklicken Sie auf **Projektdokumente**, um den Ordner zu öffnen.
6. Klicken Sie mit der rechten Maustaste in einen leeren Bereich der Spalte **Name**, zeigen Sie auf **Neu**, und klicken Sie dann auf **Microsoft Office Word-Dokument**.
7. Geben Sie „Lieferleistungen“ ein, und drücken Sie dann die EINGABETASTE.

Ausgewählten Benutzern Schreibzugriff auf die Datei gewähren

1. Klicken Sie mit der rechten Maustaste auf die Datei **Lieferleistungen**, und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie im Dialogfeld **Eigenschaften von Lieferleistungen** auf der Registerkarte **Sicherheit** auf **Bearbeiten**.
3. Klicken Sie im Dialogfeld **Berechtigungen für Lieferleistungen** auf **Hinzufügen**.
4. Geben Sie im Dialogfeld **Benutzer, Computer, Dienstkonten oder Gruppen auswählen** im Feld **Geben Sie die zu verwendenden Objektnamen ein (Beispiele)** den Pfad „Contoso\Adam“ ein, klicken Sie auf **Namen überprüfen** und dann auf **OK**.
5. Klicken Sie im Feld **Gruppen- oder Benutzernamen** auf **Adam Carter (Contoso\Adam)**.
6. Aktivieren Sie im Dialogfeld **Berechtigungen für Lieferleistungen** neben **Schreiben** das Kontrollkästchen **Zulassen**, und klicken Sie anschließend auf **OK**.
7. Klicken Sie im Dialogfeld **Eigenschaften von Lieferleistungen** auf **OK**.

Ausgewählten Benutzern das Ändern der Datei verweigern

1. Klicken Sie mit der rechten Maustaste auf die Datei **Lieferleistungen**, und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie im Dialogfeld **Eigenschaften von Lieferleistungen** auf der Registerkarte **Sicherheit** auf **Bearbeiten**.
3. Klicken Sie im Dialogfeld **Berechtigungen für Lieferleistungen** auf **Hinzufügen**.
4. Geben Sie im Dialogfeld **Benutzer, Computer, Dienstkonten oder Gruppen auswählen** im Feld **Geben Sie die zu verwendenden Objektnamen ein (Beispiele)** den Pfad „Contoso\Martin“ ein, klicken Sie auf **Namen überprüfen** und dann auf **OK**.

5. Klicken Sie im Feld **Gruppen- oder Benutzernamen** auf **Martin Berka (Contoso\Martin)**.
6. Aktivieren Sie im Dialogfeld **Berechtigungen für Lieferleistungen** neben der Option **Ändern** das Kontrollkästchen **Verweigern**, und klicken Sie anschließend auf **OK**.
7. Klicken Sie im Dialogfeld **Windows-Sicherheit** auf **Ja**.
8. Klicken Sie im Dialogfeld **Eigenschaften von Lieferleistungen** auf **OK**.

Überprüfen der Berechtigungen vom Typ Verweigern für die Datei

1. Klicken Sie im Ordner Projektdokumente mit der rechten Maustaste auf **Lieferleistungen**, und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie im Dialogfeld **Eigenschaften von Lieferleistungen** auf der Registerkarte **Sicherheit** auf **Erweitert**.
3. Klicken Sie im Dialogfeld **Erweiterte Sicherheitseinstellungen für Lieferleistungen** auf der Registerkarte **Effektive Berechtigungen** auf **Auswählen**.
4. Geben Sie im Dialogfeld **Benutzer, Computer, Dienstkonto oder Gruppe auswählen** die Zeichenfolge „Contoso\Martin“ ein, klicken Sie auf **Namen überprüfen**, und klicken Sie dann auf **OK**.
5. Vergewissern Sie sich, dass keines der Attribute als Berechtigung verfügbar ist.
6. Klicken Sie im Dialogfeld **Erweiterte Sicherheitseinstellungen für Lieferleistungen** auf der Registerkarte **Effektive Berechtigungen** auf **Auswählen**.
7. Geben Sie im Dialogfeld **Benutzer, Computer, Dienstkonto oder Gruppe auswählen** die Zeichenfolge „Contoso\Adam“ ein, klicken Sie auf **Namen überprüfen**, und klicken Sie dann auf **OK**.
8. Überprüfen Sie, ob alle Attribute außer den Berechtigungen Vollzugriff, Ändern und Besitz übernehmen ausgewählt wurden.
9. Klicken Sie im Dialogfeld **Erweiterte Sicherheitseinstellungen für Lieferleistungen** auf **OK**.
10. Klicken Sie im Dialogfeld **Eigenschaften von Lieferleistungen** auf **OK**.
11. Schließen Sie das Fenster **Projektdokumente**.

Lektion 3

Verwalten von freigegebenen Ordnern

Inhalt:

Fragen und Antworten

63

Fragen und Antworten

Was sind freigegebene Ordner?

Frage: Was ist der Vorteil der Freigabe von Ordnern in einem Netzwerk?

Antwort: Die Freigabe von Ordnern in einem Netzwerk ermöglicht die Aktualisierung von Informationen für eine Gruppe von Benutzern und vermindert das Risiko von Dateiduplikaten, da alle Dateien für ein Benutzerkonto in einer freigegebenen zentralen Datenablage gespeichert werden können.

Methoden der Ordnerfreigabe

Frage 1: Wann sollte die Freigabe des öffentlichen Ordners vermieden werden?

Antwort: Verwenden Sie die öffentliche Ordnerfreigabe nicht, wenn Sicherheit oder Datenschutz besonders wichtig sind. Denken Sie daran, dass es nicht möglich ist, Zugriff nur auf einige Dateien im öffentlichen Ordner zu gewähren. Da es eine Alles-oder-Nichts-Situation ist, können Benutzer auf alle Dateien einer öffentlichen Freigabe zugreifen.

Frage 2: Müssen Sie Berechtigungen anwenden, um die Dateien auf Ihrem Computer für andere Benutzer freizugeben?

Antwort: Nein. Eine empfohlene Methode zur Freigabe von Dateien ist die Freigabe eines einzelnen Ordners oder das Verschieben von Dateien in den öffentlichen Ordner. Je nachdem, wie Sie eine Datei oder einen Ordner freigeben, können Sie möglicherweise Berechtigungen auf einige Dateien anwenden.

Diskussion: Kombinieren von NTFS-Berechtigungen und Freigabeberechtigungen

Frage 1: Wenn einem Benutzer die NTFS-Berechtigung „Vollzugriff“ für eine Datei zugewiesen wurde, dieser jedoch über eine Freigabe mit der Berechtigung „Lesen“ auf die Datei zugreift, welche effektive Berechtigung hat der Benutzer für die Datei?

Antwort: Der Benutzer hat nur Lesezugriff auf die Datei, wenn er über das Netzwerk und die Freigabe darauf zugreift (Lesezugriff ist restriktiver als Vollzugriff). Der Benutzer hat Vollzugriff, wenn er an der Konsole des Computers angemeldet ist, auf der die Datei gespeichert ist, und lokal auf diese zugreift.

Frage 2: Wenn ein Benutzer alle Dateien in einem freigegebenen Ordner anzeigen, jedoch nur bestimmte Dateien im Ordner ändern können soll, welche Berechtigungen würden Sie erteilen?

Antwort: Die Freigabeberechtigungen müssen dem Benutzer die Änderung aller Dateien gestatten (das Ordnerfenster wird dadurch vollständig geöffnet, es ist jedoch durch NTFS-Berechtigungen gesperrt). Sie müssen die NTFS-Berechtigungen für den Ordner festlegen, um dem Benutzer nur Lesezugriff zu gewähren (der dann auf alle Dateien angewendet wird). Weisen Sie danach den einzelnen Dateien im Ordner, den der Benutzer ändern soll, die NTFS-Berechtigung „Ändern“ zu.

Frage 3: Ermitteln Sie ein Szenario in der Organisation, in dem NTFS- und Freigabeberechtigungen möglicherweise kombiniert werden müssen. Warum werden die Berechtigungen kombiniert?

Antwort: Die Antworten können abhängig von den Erfahrungen der einzelnen Kursteilnehmer unterschiedlich ausfallen.

Lektion 4

Konfigurieren der Dateikomprimierung

Inhalt:

Detaillierte Demoschritte

66

Detallierte Demoschritte

Demo: Komprimieren von Dateien und Ordnern

Detallierte Demoschritte

Erstellen von Ordnern im Ordner „Projektdokumente“

1. Klicken Sie auf auf LON-CL1 auf **Start** und anschließend auf **Computer**.
2. Doppelklicken Sie im Ordner **Computer** auf **Lokaler Datenträger (C:)**.
3. Doppelklicken Sie im Ordner Lokaler Datenträger (C:) auf **Projektdokumente**.
4. Klicken Sie im Menü des Ordners **Projektdokumente** auf **Neuer Ordner**.
5. Geben Sie „Komprimierte Dateien“ ein, und drücken Sie dann die EINGABETASTE.
6. Klicken Sie im Menü des Ordners **Projektdokumente** auf **Neuer Ordner**.
7. Geben Sie „Unkomprimierte Dateien“ ein, und drücken Sie dann die EINGABETASTE.

Komprimieren des Ordners C:\Projektdokumente\Komprimierte Dateien

1. Klicken Sie im Ordner **Projektdokumente** mit der rechten Maustaste auf **Komprimierte Dateien**, und klicken Sie dann auf **Eigenschaften**.
2. Klicken Sie im Dialogfeld **Eigenschaften von Komprimierte Dateien** auf **Erweitert**.
3. Aktivieren Sie das Kontrollkästchen **Inhalt komprimieren, um Speicherplatz zu sparen**, und klicken Sie dann auf **OK**.
4. Klicken Sie im Dialogfeld **Eigenschaften von Komprimierte Dateien** auf **OK**.

Kopieren von Dateien in den Ordner C:\Projektdokumente\Komprimierte Dateien

1. Klicken Sie auf **Start**, geben Sie im Dialogfeld **Programme/Dateien durchsuchen** die Zeichenfolge „C:\Programme\Microsoft Office\CLIPART\PUB60COR“ ein, und drücken Sie dann die **EINGABETASTE**.
2. Wählen Sie die folgenden Dateien aus, klicken Sie mit der rechten Maustaste auf die Dateien, und klicken Sie dann auf **Kopieren**:
 - **AG00004_**
 - **AG00011_**
3. Schließen Sie den Ordner **PUB60COR**.
4. Wechseln Sie zurück zum Ordner **C:\Projektdokumente**.
5. Klicken Sie mit der rechten Maustaste auf den Ordner **Komprimierte Dateien**, und klicken Sie dann auf **Einfügen**.
6. Doppelklicken Sie auf den Ordner **Komprimierte Dateien**.
7. Klicken Sie mit der rechten Maustaste auf **AG00004_**, und klicken Sie dann auf **Eigenschaften**.
8. Klicken Sie auf **Erweitert**.
9. Klicken Sie auf **Abbrechen** und anschließend erneut auf **Abbrechen**, um das Dialogfeld der Eigenschaften zu schließen.

Verschieben der komprimierten Dateien in den Ordner „C:\Projektdokumente\Unkomprimierte Dateien“

1. Klicken Sie auf **Start** und dann auf **Computer**.
2. Doppelklicken Sie im Ordner **Computer** auf **Lokaler Datenträger (C:)**.
3. Doppelklicken Sie im Ordner **Lokaler Datenträger (C:)** auf **Projektdokumente**.
4. Doppelklicken Sie im Ordner **Projektdokumente** auf **Unkomprimierte Dateien**.
5. Klicken Sie mit der rechten Maustaste auf die **Taskleiste**, und klicken Sie dann auf **Fenster nebeneinander anzeigen**.
6. Ziehen Sie im Ordner **Komprimierte Dateien** die Datei **AG00004_** in den Ordner **Unkomprimierte Dateien**.

Kopieren der komprimierten Dateien in den Ordner „C:\Projektdokumente\Unkomprimierte Dateien“

1. Klicken Sie im Ordner **Komprimierte Dateien** mit der rechten Maustaste auf **AG00011_**, und ziehen Sie die Datei dann in den Ordner **Unkomprimierte Dateien**.
2. Klicken Sie auf **Hierher kopieren**.

Komprimieren eines Ordners mit dem Feature „ZIP-komprimierter Ordner“

1. Klicken Sie auf **Start** und dann auf **Computer**.
2. Doppelklicken Sie im Ordner **Computer** auf **Lokaler Datenträger (C:)**.
3. Doppelklicken Sie im Ordner **Lokaler Datenträger (C:)** auf **Projektdokumente**.
4. Klicken Sie mit der rechten Maustaste auf **Unkomprimierte Dateien**, klicken Sie auf **Senden an**, und klicken Sie dann auf **ZIP-komprimierter Ordner**.
5. Geben Sie „Gezippte Daten“ ein, und drücken Sie die **EINGABETASTE**.
6. Ziehen Sie die **gezippte** Datendatei in den Ordner **Komprimierte Dateien**.
7. Doppelklicken Sie auf den Ordner **Komprimierte Dateien**.
8. Drücken Sie **STRG+Z**, um den Verschiebevorgang rückgängig zu machen.
9. Klicken Sie auf der Menüleiste auf den nach links weisenden Pfeil, um zum Ordner **Projektdokumente** zurückzukehren.
10. Klicken Sie mit der rechten Maustaste auf **Gezippte Daten**, und ziehen Sie sie in den Ordner **Komprimierte Dateien**.
11. Klicken Sie auf **Hierher kopieren**.
12. Doppelklicken Sie auf **Komprimierte Dateien**.
13. Schließen Sie alle geöffneten Fenster.

Lektion 5

Verwalten von Druckfunktionen

Inhalt:

Detaillierte Demoschritte

69

Detaillierte Demoschritte

Demo: Installieren und Freigeben eines Druckers

Detaillierte Demoschritte

Erstellen und Freigeben eines lokalen Druckers

1. Klicken Sie auf LON-CL1 auf **Start**, klicken Sie auf **Systemsteuerung**, und klicken Sie dann auf **Geräte und Drucker anzeigen**.
2. Klicken Sie im Menü auf **Drucker hinzufügen**.
3. Klicken Sie im **Druckerinstallations-Assistenten** auf **Einen lokalen Drucker hinzufügen**.
4. Klicken Sie auf der Seite **Einen Druckeranschluss auswählen** in der Liste **Vorhandenen Anschluss verwenden** auf **LPT1: (Druckeranschluss)**, und klicken Sie dann auf **Weiter**.
5. Klicken Sie auf der Seite **Druckertreiber installieren** in der Liste **Hersteller** auf **Epson**, klicken Sie in der Liste **Drucker** auf **Epson Stylus Photo RX630 (M)**, und klicken Sie dann auf **Weiter**.
6. Klicken Sie auf der Seite **Geben Sie einen Druckernamen ein** auf **Weiter**.
7. Akzeptieren Sie die Standardeinstellungen auf der Seite **Druckerfreigabe**, und klicken Sie auf **Weiter**.
8. Klicken Sie auf **Fertig stellen**, um den Assistenten zu beenden.

Festlegen von Berechtigungen und erweiterten Optionen für den Drucker

1. Klicken Sie unter **Geräte und Drucker** mit der rechten Maustaste auf **Epson Stylus Photo RX630 (M)**, und klicken Sie dann auf **Druckereigenschaften**.
2. Klicken Sie auf die Registerkarte **Sicherheit**, und klicken Sie dann auf **Hinzufügen**.
3. Geben Sie im Dialogfeld **Benutzer, Computer, Dienstkonten oder Gruppen auswählen** im Feld **Geben Sie die zu verwendenden Objektnamen ein (Beispiele)** den Pfad „Contoso\IT“ ein, klicken Sie auf **Namen überprüfen** und dann auf **OK**.
4. Klicken Sie im Feld **Gruppen- oder Benutzernamen** auf **IT (Contoso\IT)**.
5. Aktivieren Sie im Dialogfeld **Berechtigungen für IT** neben **Diesen Drucker verwalten** das Kontrollkästchen **Zulassen**.
6. Aktivieren Sie im Dialogfeld **Berechtigungen für IT** neben **Dokumente verwalten** das Kontrollkästchen **Zulassen**, und klicken Sie dann auf **Übernehmen**.
7. Klicken Sie auf die Registerkarte **Erweitert**.
8. Aktivieren Sie das Kontrollkästchen **Fehlerhafte Druckaufträge anhalten**.
9. Klicken Sie auf die Registerkarte **Allgemein**.
10. Geben Sie im Feld **Speicherort** den Text „Headquarters“ ein.
11. Klicken Sie auf **Einstellungen**.
12. Legen Sie die **Qualitätsoption** auf **Optimales Foto** fest.
13. Klicken Sie zum Schließen des Dialogfelds auf **OK** und dann erneut auf **OK**.
14. Klicken Sie auf **OK**, um das Feld **Eigenschaften von Epson Stylus Photo RX630 (M)** zu schließen.

Beibehalten von Druckereigenschaften

In dem in dieser Demo aktualisierten Dialogfeld „Druckereigenschaften“ können die folgenden Berechtigungen beibehalten werden:

- Drucken
- Diesen Drucker verwalten
- Dokumente verwalten

Im Dialogfeld Druckereigenschaften sind auch die folgenden Druckoptionen enthalten, die beibehalten werden können.

Pfad	Druckoptionen
Registerkarte Allgemein	Druckeinstellungen, wie z. B. die Hochformat-/Querformatoption und die Druckqualität
Registerkarte Anschlüsse	Konfigurieren des Druckeranschlusses
Registerkarte Erweitert	Zuweisen von Druckertreibern
Registerkarte Erweitert	Optionen für den Spoolingvorgang
Registerkarte Erweitert	Option für das Anhalten fehlgeschlagener Druckaufträge
Registerkarte Erweitert	Aktivieren von erweiterten Druckfeatures

Lernzielkontrollen und Kernpunkte der Unterrichtseinheit

Fragen zur Lernzielkontrolle

Frage 1: Sie möchten einen Ordner freigeben, der das Dokument zur Bewertung des Leistungsumfangs enthält sowie andere Planungsdateien, die Sie für die bevorstehende Microsoft Dynamics® CRM-Implementierung bei Fabrikam, Inc. erstellt haben. Sie möchten diese Planungsdateien jedoch nicht offline verfügbar machen. Welche erweiterten Freigabeoptionen müssen konfiguriert werden, um dieser Anforderung zu entsprechen?

Antwort: Sie müssen die Zwischenspeicherungsoptionen konfigurieren, die festlegen, wie die Offlineversionen von freigegebenen Dateien zur Verfügung gestellt werden, sofern dies überhaupt der Fall ist. Die Benutzer müssen standardmäßig angeben, welche Dateien und Programme offline verfügbar sein sollen.

Frage 2: Contoso installiert Microsoft Dynamics® GP und hat mit einem Anbieter einen Vertrag für kundenspezifische Programmierungsarbeiten abgeschlossen. Contoso hat Joseph, den verantwortlichen IT-Desktopexperten, aufgefordert, die NTFS-Berechtigungen für die sich ansammelnden GP-Plandateien zu konfigurieren. Contoso möchte, dass allen IT-Benutzern die Berechtigung „Ändern“ für den Planungsordner der GP-Implementierung zugewiesen wird. Es sollte jedoch nur eine ausgewählte Gruppe von Managern den Unterordner mit dem Titel „Anbieterverträge“ anzeigen können. Wie kann Joseph vorgehen, wenn er die Vererbung von Kontenberechtigungen berücksichtigen muss?

Antwort: Er kann eine Methode anwenden, die aus drei Schritten besteht. Zuerst weist er der IT-Benutzergruppe die Berechtigung Ändern für den Planungsordner der GP-Implementierung zu. Danach kann er die geerbten Berechtigungen für den Unterordner „Anbieterverträge“ blockieren. Schließlich kann er den Zugriff auf den Unterordner einschränken, indem er den ausgewählten Managern auf der Liste von Contoso Lesezugriff erteilt.

Frage 3: Peter ist ein IT-Spezialist, der bei Fabrikam arbeitet. Er kann auf eine bestimmte Datei nicht zugreifen und vermutet, dass die Ursache des Problems die NTFS-Berechtigungen der Datei sind. Wie kann er seine Dateiberechtigungen anzeigen?

Antwort: Peter kann auf der Eigenschaftenseite der Datei auf die Registerkarte **Sicherheit** und dann auf **Erweitert** klicken. Auf der Registerkarte Effektive Berechtigungen kann er seinen Benutzeralias eingeben und dann seine effektiven Berechtigungen anzeigen.

Frage 4: Robin hat vor kurzem ein Arbeitsblatt erstellt, dem sie explizit NTFS-Dateiberechtigungen zugewiesen und so den Dateizugriff nur auf sich beschränkt hat. Nach der Neuorganisation des Systems wurde die Datei in einen Ordner auf einer anderen NTFS-Partition verschoben, und Robin hat bemerkt, dass nun andere Benutzer auf das Arbeitsblatt zugreifen können. Was ist eine mögliche Ursache für diese Situation?

Antwort: Wenn eine Datei in einen Ordner auf einer anderen NTFS-Partition verschoben wird, erbt die Datei die Berechtigungen des neuen Ordners. In diesem Fall ist anderen Benutzergruppen der Zugriff auf den neuen Ordner gestattet, in den das Arbeitsblatt verschoben wurde.

Frage 5: Contoso hat vor kurzem Windows 7 auf seinen Clientcomputern installiert. Da viele Vertriebsmitarbeiter in jedem Monat zu verschiedenen Zweigstellen reisen und von dort arbeiten, möchte Contoso die Funktionalität zum Drucken am Aufenthaltsort in Windows 7 nutzen. Der Vertriebsmitarbeiter Michael war erfreut, dass er den Drucker nicht mehr jedes Mal neu konfigurieren musste, wenn er ein Dokument in einer Zweigstelle drucken wollte. Auf seiner letzten Reise hat er jedoch versucht, mithilfe der Terminaldienste eine Verbindung mit dem Firmennetzwerk herzustellen. Als er eine Datei drucken wollte, stellte er erstaunt fest, dass er den Drucker noch immer manuell auswählen musste. Warum hat das System den Drucker nicht automatisch erkannt?

Antwort: Das Drucken am Aufenthaltsort funktioniert nicht, wenn die Verbindung zum Netzwerk über Remotedesktop (Terminaldienste) hergestellt wird.

Best Practices für die Authentifizierung und Autorisierung

Ergänzen oder ändern Sie die folgenden bewährten Methoden abhängig von Ihren eigenen Arbeitssituationen:

- Wenn Sie einen Computer einrichten, müssen Sie ein Benutzerkonto erstellen. Dieses Konto ist ein Administratorkonto, das für die Einrichtung des Computers und zur Installation der erforderlichen Programme verwendet wird.

Nach Abschluss der Einrichtung des Computers empfiehlt sich die Verwendung eines Standardbenutzerkontos für die tägliche Arbeit mit dem Computer.

Die Verwendung eines Standardbenutzerkontos statt eines Administratorkontos bietet höhere Sicherheit, da dadurch verhindert werden kann, dass Benutzer Änderungen vornehmen, die sich auf alle Benutzer des Computers auswirken, besonders im Fall des Diebstahls der Anmeldeinformationen für das Benutzerkonto.

- Folgendes ist bei der Übernahme der Besitzrechte für eine Datei oder einen Ordner zu bedenken:
 - Der Administrator kann die Besitzrechte für jede beliebige Datei auf dem Computer übernehmen.
 - Die Besitzzuweisung für eine Datei oder einen Ordner erfordert möglicherweise eine Erhöhung der Berechtigungen über die Benutzerzugriffssteuerung.
 - Die Gruppe „Anonyme Anmeldung“ ist nicht mehr Mitglied der Gruppe „Jeder“.

Best Practices für die NTFS-Berechtigungen

Ergänzen oder ändern Sie die folgenden bewährten Methoden abhängig von Ihren eigenen Arbeitssituationen:

- Um die Zuweisung von Berechtigungen zu vereinfachen, können Sie der Gruppe „Jeder“ die Freigabeberechtigung „Vollzugriff“ für alle Freigaben gewähren und den Zugriff nur mit NTFS-Berechtigungen steuern. Schränken Sie Freigabeberechtigungen auf das erforderliche Minimum ein, damit für den Fall einer fehlerhaften Konfiguration der NTFS-Berechtigungen eine weitere Sicherheitsstufe zur Verfügung steht.
- Wenn die Berechtigungsvererbung blockiert wird, haben Sie die Möglichkeit, vorhandene Berechtigungen zu kopieren oder mit leeren Berechtigungen zu beginnen. Wenn Sie den Zugriff nur für eine bestimmte Gruppe oder für einen bestimmten Benutzer einschränken möchten, kopieren Sie die vorhandenen Berechtigungen, um die Konfiguration zu vereinfachen.

Best Practices für die Verwaltung von freigegebenen Ordnern

Ergänzen oder ändern Sie die folgenden bewährten Methoden abhängig von Ihren eigenen Arbeitssituationen:

- Wenn das Gastbenutzerkonto auf dem Computer aktiviert wird, enthält die Gruppe „Jeder“ alle Benutzer. In der Praxis entfernen Sie die Gruppe Jeder aus allen Berechtigungslisten und ersetzen sie durch die Gruppe Authentifizierte Benutzer.
- Bei Verwendung einer anderen als der in Windows 7 integrierten Firewall können Probleme mit der Netzwerkerkennung und den Dateifreigabefeatures auftreten.

Tools

Verwenden Sie die folgenden Eingabeaufforderungstools zur Verwaltung der Datei- und Druckerfreigabe:

Tool	Beschreibung
Net share	Freigeben von Ordnern über die Eingabeaufforderung
Net use	Erstellen einer Verbindung zu freigegebenen Ressourcen über die Eingabeaufforderung
Cacls.exe	Konfigurieren von NTFS-Berechtigungen für Dateien und Ordner über die Eingabeaufforderung
Compact.exe	Komprimieren von NTFS-Dateien und -Ordnern über die Eingabeaufforderung
Pnputil.exe	Vorinstallieren von Druckertreibern in den Treiberspeicher

Fragen und Antworten zur Lernzielkontrolle

Frage: Sie haben einen freigegebenen Ordner für alle Benutzer erstellt. Wie können Sie den Zugriffsvorgang auf diesen Ordner für die Benutzer vereinfachen?

Antwort: Sie können auf dem Benutzerdesktop eine Desktopverknüpfung für den freigegebenen Ordner erstellen oder den Benutzern zeigen, wie sie dem freigegebenen Ordner ein Netzlaufwerk zuordnen können. In einer Domänenumgebung können Sie auch das Laufwerk mithilfe von Gruppenrichtlinieneinstellungen zuordnen.

Frage: Sie müssen sicherstellen, dass nur bestimmte Benutzer über das Netzwerk auf einen freigegebenen Ordner zugreifen können, wenn sie beim Computer mit dem freigegebenen Ordner angemeldet sind. Wie werden Berechtigungen konfiguriert?

Antwort: Sie müssen NTFS-Berechtigungen verwenden. Berechtigungen für freigegebene Ordner werden nur angewendet, wenn Benutzer über das Netzwerk auf den Ordner zugreifen.

Frage: Sie müssen sicherstellen, dass Benutzer nur die Druckaufträge verwalten können, die sie an einen freigegebenen Drucker gesendet haben. Mitglieder der Gruppe „Helpdesk“ müssen in der Lage sein, alle Druckaufträge zu löschen. Wie werden die Druckerberechtigungen konfiguriert?

Antwort: Standardmäßig hat jeder die Berechtigung, mit einem Drucker zu drucken und eigene Druckaufträge zu verwalten. Sie müssen der Gruppe „Helpdesk“ die Berechtigung „Dokumente verwalten“ zuweisen.

Unterrichtseinheit 4

Konfigurieren der Netzwerkkonnektivität

Inhalt:

Lektion 1: Konfigurieren der IPv4-Netzwerkkonnektivität	76
Lektion 2: Konfigurieren der IPv6-Netzwerkkonnektivität	79
Lektion 3: Implementieren der automatischen IP-Adresszuordnung	82
Lektion 5: Beheben von Netzwerkproblemen	84
Lernzielkontrollen und Kernpunkte der Unterrichtseinheit	87
Fragen und Antworten zur Lernzielkontrolle	89

Lektion 1

Konfigurieren der IPv4-Netzwerkonnektivität

Inhalt:

Fragen und Antworten	77
Detaillierte Demoschritte	78

Fragen und Antworten

Was sind öffentliche und private IPv4-Adressen?

Frage: Welche der folgenden Adressen ist keine private IP-Adresse?

- a. 16.16.254
- b. 16.18.5
- c. 168.1.1
- d. 255.255.254

Antwort: A und B.

Demo: Konfigurieren einer IPv4-Adresse

Frage: Wann könnte es notwendig sein, die IPv4-Adresse eines Computers zu ändern?

Antwort: Sie müssen sicherstellen, dass alle Computer im Netzwerk über eine eindeutige IPv4-Adresse verfügen. Wenn zwei Computer über dieselbe IPv4-Adresse verfügen, muss die IPv4-Adresse auf einem der beiden Computer geändert werden.

Detaillierte Demoschritte

Demo: Konfigurieren einer IPv4-Adresse

Detaillierte Demoschritte

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Zubehör** und dann auf **Eingabeaufforderung**.
3. Geben Sie an der Eingabeaufforderung „**ipconfig /all**“ ein, und drücken Sie die EINGABETASTE. Dadurch wird die Konfiguration für alle Netzwerkverbindungen auf dem Computer angezeigt.
4. Schließen Sie die Eingabeaufforderung.
5. Klicken Sie auf **Start** und dann auf **Systemsteuerung**.
6. Klicken Sie unter **Netzwerk und Internet** auf **Netzwerkstatus und -aufgaben anzeigen**.
7. Klicken Sie in **Netzwerk- und Freigabecenter** rechts neben dem Domänennetzwerk „Contoso.com“ auf **LAN-Verbindung 3**. (Hinweis: Die Nummer der LAN-Verbindung kann anders lauten.)
8. Klicken Sie im Fenster **Status von LAN-Verbindung 3** auf **Details**. In diesem Fenster werden die gleichen Konfigurationsinformationen für diesen Adapter angezeigt wie mit dem Befehl „ipconfig“.
9. Klicken Sie in den Fenstern **Netzwerkverbindungsdetails** auf **Schließen**.
10. Klicken Sie im Fenster **Status von LAN-Verbindung 3** auf **Eigenschaften**. Mithilfe dieses Fensters können Protokolle konfiguriert werden.
11. Klicken Sie auf **Internetprotokoll Version 4 (TCP/IPv4)** und dann auf **Eigenschaften**. In diesem Fenster können Sie IP-Adresse, Subnetzmaske, Standardgateway und DNS-Server konfigurieren.
12. Klicken Sie auf **Erweitert**. Im Fenster Erweiterte TCP/IP-Einstellungen können Sie zusätzliche Einstellungen konfigurieren, z. B. weitere IP-Adressen, DNS-Einstellungen und WINS-Server für die NetBIOS-Namensauflösung.
13. Schließen Sie alle geöffneten Fenster, ohne die Einstellungen zu ändern.

Lektion 2

Konfigurieren der IPv6-Netzwerkconnectivität

Inhalt:

Fragen und Antworten	80
Detaillierte Demoschritte	81

Fragen und Antworten

Demo: Konfigurieren einer IPv6-Adresse

Frage: Weisen Sie einem Computer IPv6-Adressen in der Regel manuell zu?

Antwort: IPv6 muss in den meisten Fällen dynamisch konfiguriert werden. Mithilfe verbindungslokaler Adressen ist innerhalb eines IPv6-Netzwerks eine Kommunikation ohne jegliche Konfiguration möglich. Um jedoch den Zugriff auf Ressourcen anhand der IPv6-Adressen zu steuern, muss möglicherweise eine statische IPv6-Adresse zugewiesen werden.

Detaillierte Demoschritte

Demo: Konfigurieren einer IPv6-Adresse

Detaillierte Demoschritte

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Zubehör** und dann auf **Eingabeaufforderung**.
3. Geben Sie an der Eingabeaufforderung „**ipconfig /all**“ ein, und drücken Sie die EINGABETASTE. Es werden alle Netzwerkverbindungen für den Computer angezeigt. Beachten Sie, dass eine verbindungslokale IPv6-Adresse zugewiesen wurde.
4. Schließen Sie die Eingabeaufforderung.
5. Klicken Sie auf **Start** und dann auf **Systemsteuerung**.
6. Klicken Sie unter **Netzwerk und Internet** auf **Netzwerkstatus und -aufgaben anzeigen**.
7. Klicken Sie im **Netzwerk- und Freigabecenter** rechts neben dem Domänennetzwerk **Contoso.com** auf **LAN-Verbindung 3**.

Hinweis: Die Nummer der LAN-Verbindung kann anders lauten.

8. Klicken Sie im Fenster **Status von LAN-Verbindung 3** auf **Details**. In diesem Fenster werden die gleichen Konfigurationsinformationen für diesen Adapter angezeigt wie mit dem Befehl ipconfig.
9. Klicken Sie in den Fenstern **Netzwerkverbindungsdetails** auf **Schließen**.
10. Klicken Sie im Fenster **Status von LAN-Verbindung 3** auf **Eigenschaften**. Mithilfe dieses Fensters können Protokolle konfiguriert werden.
11. Klicken Sie auf **Internetprotokoll Version 6 (TCP/IPv6)** und dann auf **Eigenschaften**. In diesem Fenster können Sie die IPv6-Adresse, die Subnetzpräfixlänge, das Standardgateway und den DNS-Server konfigurieren.
12. Klicken Sie auf **Folgende IPv6-Adresse verwenden**, und geben Sie Folgendes ein:
 - IPv6-Adresse: 2001:0DB8:0000:0000:02AA:00FF:FE28:9C5A
 - Subnetzpräfixlänge: 64
13. Klicken Sie auf **Erweitert**. Im Fenster **Erweiterte TCP/IP-Einstellungen** können Sie weitere Einstellungen wie z. B. zusätzliche IP-Adressen und DNS-Einstellungen konfigurieren.
14. Klicken Sie im Fenster **Erweiterte TCP/IP-Einstellungen** auf **Abbrechen**.
15. Klicken Sie im Fenster **Eigenschaften von Internetprotokoll Version 6 (TCP/IPv6)** auf **OK**.
16. Klicken Sie im Fenster **Eigenschaften von LAN-Verbindung 3** auf **Schließen**.
17. Klicken Sie im Fenster **Status von LAN-Verbindung 3** auf **Details**. Überprüfen Sie, ob die neue IPv6-Adresse hinzugefügt wurde.
18. Schließen Sie alle geöffneten Fenster.

Lektion 3

Implementieren der automatischen IP-Adresszuordnung

Inhalt:

Detaillierte Demoschritte

83

Detaillierte Demoschritte

Demo: Konfigurieren eines Computers zum dynamischen Beziehen einer IPv4-Adresse

Detaillierte Demoschritte

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Zubehör**, und klicken Sie dann auf **Eingabeaufforderung**.
3. Geben Sie an der Eingabeaufforderung „ipconfig /all“ ein, und drücken Sie die EINGABETASTE. Es werden alle Netzwerkverbindungen für den Computer angezeigt.
4. Schließen Sie die Eingabeaufforderung.
5. Klicken Sie auf **Start** und dann auf **Systemsteuerung**.
6. Klicken Sie unter **Netzwerk und Internet** auf **Netzwerkstatus und -aufgaben anzeigen**.
7. Klicken Sie im **Netzwerk- und Freigabecenter** rechts neben dem Domänennetzwerk **Contoso.com** auf **LAN-Verbindung 3**.
8. Klicken Sie im Fenster **Status von LAN-Verbindung 3** auf **Eigenschaften**. Mithilfe dieses Fensters können Protokolle konfiguriert werden.
9. Klicken Sie auf **Internetprotokoll Version (TCP/IPv4)** und dann auf **Eigenschaften**.
10. Klicken Sie auf **IP-Adresse automatisch beziehen**. Beachten Sie, dass die Registerkarte **Alternative Konfiguration** verfügbar wird, sobald Sie diese Einstellung vornehmen.
11. Klicken Sie auf **DNS-Serveradresse automatisch beziehen**.
12. Klicken Sie auf die Registerkarte **Alternative Konfiguration**. Die Konfigurationsinformationen auf dieser Registerkarte werden verwendet, wenn kein DHCP-Server verfügbar ist.
13. Klicken Sie auf **OK**, um die Änderungen zu speichern.
14. Klicken Sie im Fenster **Eigenschaften von LAN-Verbindung 3** auf **Schließen**.
15. Klicken Sie im Fenster **Status von LAN-Verbindung 3** auf **Details**. Beachten Sie, dass DHCP aktiviert und die IP-Adresse des DHCP-Servers angezeigt wird.
16. Schließen Sie alle geöffneten Fenster.

Lektion 5

Beheben von Netzwerkproblemen

Inhalt:

Fragen und Antworten	85
Detaillierte Demoschritte	86

Fragen und Antworten

Demo: Beheben von häufigen Netzwerkproblemen

Frage: In welcher Weise ist der Ping-Befehl für die Problembehandlung hilfreich?

Antwort: Der Ping-Befehl kann verwendet werden, um die Konnektivität zwischen Hosts zu überprüfen. Beachten Sie jedoch, dass eine Firewall zwar Ping-Pakete blockieren, die Pakete anderer Anwendungen jedoch weiterhin zulassen kann. Wenn Sie eine Antwort auf einen Ping-Versuch erhalten, wird der Host definitiv ausgeführt. Wenn Sie keine Antwort auf einen Ping-Versuch erhalten, kann der Host dennoch funktionieren.

Detaillierte Demoschritte

Demo: Beheben von häufigen Netzwerkproblemen

Detaillierte Demoschritte

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Zubehör**, und klicken Sie dann auf **Eingabeaufforderung**.
3. Geben Sie an der Eingabeaufforderung „`ipconfig /all`“ ein, und drücken Sie die EINGABETASTE. Es werden alle Netzwerkverbindungen für den Computer angezeigt. Es werden alle Netzwerkadapter-Konfigurationsinformationen angezeigt.
4. Geben Sie an der Eingabeaufforderung „`ipconfig /displaydns`“ ein, und drücken Sie die EINGABETASTE. Es wird der Inhalt des DNS-Caches angezeigt.
5. Geben Sie an der Eingabeaufforderung „`ipconfig /flushdns`“ ein, und drücken Sie die EINGABETASTE. Der Inhalt des DNS-Caches wird gelöscht.
6. Geben Sie an der Eingabeaufforderung „`ping 127.0.0.1`“ ein, und drücken Sie die EINGABETASTE. Es wird ein Ping-Signal an den lokalen Host gesendet.
7. Geben Sie an der Eingabeaufforderung „`ping 10.10.0.10`“ ein, und drücken Sie die EINGABETASTE. Die Verbindung mit LON-DC1 mit einer IPv4-Adresse wird geprüft.
8. Geben Sie an der Eingabeaufforderung „`ping LON-DC1`“ ein, und drücken Sie die EINGABETASTE. Die Verbindung mit LON-DC1 wird mit einem Hostnamen geprüft.
9. Geben Sie an der Eingabeaufforderung „`nslookup -d1 LON-DC1`“ ein, und drücken Sie die EINGABETASTE. Es werden ausführliche Informationen zur Hostnamensauflösung angezeigt. Sie können die Option **-d2** verwenden, um noch ausführlichere Informationen anzuzeigen.
10. Schließen Sie die Eingabeaufforderung.

Lernzielkontrollen und Kernpunkte der Unterrichtseinheit

Fragen zur Lernzielkontrolle

Frage 1: Nach dem Start ihres Computers bemerkt Amy, dass sie nicht auf ihre Unternehmensressourcen zugreifen kann. Mit welchem Tool kann sie herausfinden, ob sie eine gültige IP-Adresse besitzt?

Antwort: Führen Sie **IPConfig /All** aus, oder senden Sie ein **Ping**-Signal an die IP-Adresse des Domänencontrollers.

Frage 2: Bei der Übermittlung von Debitorenaktualisierungen an einen für die Abrechnung zuständigen Geschäftspartner in China bemerkt Amy, dass die Dateien sehr langsam übermittelt werden. Mit welchem Tool kann sie den Pfad und die Latenzzeit des Netzwerks bestimmen?

Antwort: Verwenden Sie die **Windows-Diagnose**, um das Problem zu identifizieren, oder **Pathping.exe**, um die Wartezeit zu überprüfen.

Frage 3: Amy bemerkt, dass sie nicht auf die normale Unternehmenswebsite zugreifen kann. Sie weiß, dass sie eine gültige IP-Adresse besitzt und will eine Problembehandlung für den DNS-Zugriff ihres Computers durchführen. Welches Tool muss sie verwenden?

Antwort: Verwenden Sie **NSLookup.exe**, um Probleme mit dem DNS-Zugriff zu beheben.

Frage 4: Was ist die IPv6-Entsprechung einer IPv4-APIPA-Adresse?

Antwort: Verbindungslokale IPv6-Adressen

Frage 5: Sie beheben ein Netzwerkproblem und vermuten, dass es sich um ein Problem mit der Namensauflösung handelt. Vor dem Durchführen von Tests möchten Sie den DNS-Auflösungscache löschen. Wie gehen Sie dabei vor?

Antwort: Verwenden Sie **IPConfig /flushdns**, um den DNS-Auflösungscache zu löschen.

Frage 6: Sie beheben ein Netzwerkproblem. Die IP-Adresse des Hosts, auf dem Sie die Problembehandlung ausführen, lautet 169.254.16.17. Worin besteht eine mögliche Ursache des Problems?

Antwort: Der DHCP-Server ist für den Host nicht verfügbar.

Häufige Probleme in Zusammenhang mit der Netzwerkkonnektivität

Identifizieren Sie die Ursachen für die folgenden, häufig auftretenden Probleme und nennen Sie Tipps zur Problembehandlung. Antworten finden Sie in den entsprechenden Lektionen der Unterrichtseinheit oder im Inhalt der Kursbegleit-CD.

Problem	Tipps zur Problembehandlung
Ein Windows 7-Host kann keine Verbindung zu einer SharePoint-Site herstellen	Identifizieren Sie das Problem mithilfe von Windows-Diagnose .
Ein Windows 7-Host kann nicht auf den Datenbankserver zugreifen.	Verwenden Sie das Tool IPConfig , um eine IP-Adresse anzuzeigen, zu erneuern oder freizugeben.
Ein Windows 7-Host kann keine Verbindung mit dem Internet herstellen.	Testen Sie die Konnektivität zum DNS-Server mithilfe von Ping .
Der DNS-Server löst vollqualifizierte Domännennamen (FQDNs) nicht ordnungsgemäß auf.	Verwenden Sie die flushdns -Option mit IPConfig .

Tools

Sie können die folgenden Tools verwenden, um Probleme mit Netzwerkverbindungen zu beheben:

Tool	Beschreibung
Netzwerk- und Freigabecenter	Das Netzwerk- und Freigabecenter stellt Informationen über das Netzwerk bereit und überprüft, ob Ihr Computer auf das Internet zugreifen kann. Anschließend werden diese Informationen in Form einer Netzwerkübersicht zusammengefasst.
Netsh.exe	Ein Befehl, mit dem Sie Netzwerkeigenschaften über die Befehlszeile konfigurieren können.
Pathping.exe	Dieses Befehlszeilentool kombiniert die Funktionalität von „Ping“ und „Tracert“ und kann für die Behandlung von Netzwerklatenzproblemen und zur Bereitstellung von Informationen zu Pfaddaten verwendet werden.
NSlookup.exe	Ein Befehlszeilentool, das Sie zum Testen und Behandeln von Problemen mit der DNS- und Namensauflösung verwenden können.
IPConfig.exe	Eine allgemeines Tool zur IP-Konfiguration und Problembehandlung.
Ping.exe	Ein grundlegendes Befehlszeilentool, das Sie zum Überprüfen der IP-Konnektivität verwenden können.
Tracert.exe	Stellt ähnlich wie „Pathping“ Informationen zu Netzwerkrouuten bereit.

Fragen und Antworten zur Lernzielkontrolle

Frage: Inwieweit ähneln APIPA-Adressen für IPv4 den verbindungslokalen Adressen von IPv6?

Antwort: Beide APIPA-Adressen ermöglichen es Computern, automatisch im lokalen Netzwerk ohne die Verwendung eines DHCP-Servers oder einer anderen IP-Adresskonfiguration zu kommunizieren. Eine APIPA-Adresse wird jedoch nur verwendet, wenn kein DHCPv4-Server verfügbar ist. Eine verbindungslokale IPv6-Adresse wird immer für einen IPv6-Host generiert. Zusätzliche IPv6-Adressen können für die Kommunikation außerhalb des lokalen Netzwerks nach wie vor abgerufen werden.

Frage: Wie können Sie einen Windows 7-Computer so aktualisieren, dass die richtigen Informationen verwendet werden, wenn ein Hostdatensatz in DNS aktualisiert wurde, der Windows 7-Computer jedoch den Namen nach wie vor in die frühere IP-Adresse auflöst?

Antwort: Wenn ein Computer mit DNS einen Namen in eine IP-Adresse auflöst, werden der Name und die IP-Adresse lokal zwischengespeichert. Sie können diesen Cache an einer Eingabeaufforderung mit dem Befehl „ipconfig /flushdns“ löschen.

Unterrichtseinheit 5

Konfigurieren von Verbindungen mit einem Drahtlosnetzwerk

Inhalt:

Lektion 2: Konfigurieren von Drahtlosnetzwerken	91
Lernzielkontrollen und Kernpunkte der Unterrichtseinheit	96
Fragen und Antworten zur Lernzielkontrolle	98

Lektion 2

Konfigurieren von Drahtlosnetzwerken

Inhalt:

Fragen und Antworten	92
Detaillierte Demoschritte	93

Fragen und Antworten

Demo: Herstellen der Verbindung mit einem Drahtlosnetzwerk

Frage: Welche erweiterten Drahtloseinstellungen ziehen Sie zur Verbesserung der Sicherheit in Betracht?

Antwort: Eine Liste mit MAC-Adressen, die eine Verbindung mit dem Drahtloszugriffspunkt herstellen dürfen.

Frage: Kann ein Benutzer einen Computer mit einem nicht aufgeführten Netzwerk verbinden, wenn ihm die SSID nicht bekannt ist?

Antwort: Ja, der Benutzer kann nach Netzwerken suchen, und von einigen Tools werden Informationen zu nicht aufgeführten Netzwerken bereitgestellt. Wenn die SSID ausgeblendet oder nicht übertragen wird, bietet dies nur grundlegenden Schutz.

Frage: Welche Probleme können bei Verbindungen mit ungesicherten Netzwerken entstehen?

Antwort: Ihre Informationen können von anderen Personen im Netzwerk angezeigt werden.

Verbessern der Drahtlossignalstärke

Frage: Welche Geräte können ein Drahtlosnetzwerksignal beeinträchtigen?

Antwort: Der IEEE 802.11b- und der IEEE 802.11g-Standard verwendet das S-Band des ISM-Frequenzbereichs (Industrial, Scientific and Medical; Industrie, Wissenschaft und Medizin), der die Bereiche von 2,4 bis 2,5 GHz umfasst. Dieser Frequenzbereich wird auch für Geräte, wie z. B. Mikrowellenherde, Schnurlostelefone, Babyfone, drahtlose Videokameras und Bluetooth-Adapter, verwendet, die eine Störung des Drahtlosnetzwerksignals verursachen können.

IEEE 802.11a verwendet den Frequenzbereich C-Band-ISM, der den Bereich von 5,725 bis 5,875 GHz umfasst. Ein Drahtlosnetzwerk, das diesen Standard verwendet, unterliegt dadurch weniger Störungen durch andere Geräte.

Detaillierte Demoschritte

Demo: Herstellen der Verbindung mit einem Drahtlosnetzwerk

Detaillierte Demoschritte

Konfigurieren eines Drahtloszugriffspunkts

Die Demo enthält folgende Schritte:

1. Klicken Sie auf **Start** und anschließend auf **Netzwerk**, um eine Liste der verfügbaren Geräte anzuzeigen.
2. Klicken Sie mit der rechten Maustaste auf den **Drahtloszugriffspunkt**, und klicken Sie dann auf **Gerätewebseite anzeigen**, um das Gerät zu konfigurieren.
3. Geben Sie die erforderlichen Anmeldeinformationen ein. Diese werden normalerweise vom Hersteller des Geräts bereitgestellt. Es wird empfohlen, diese Anmeldeinformationen nach der erstmaligen Konfiguration des drahtlosen Zugriffspunkts zu ändern.
4. Klicken Sie auf **Wireless Settings** (Drahtloseinstellungen). Dies ist ein Netgear-Router. Beachten Sie, dass andere Geräte möglicherweise über andere Verwaltungsschnittstellen verfügen, die jedoch ähnliche Einstellungen enthalten.
5. Geben Sie **ADATUM** in **Name (SSID)** ein, um die Standard-SSID in einen Namen mit Bezug zu Ihrer Organisation zu ändern.
6. Sie können den Kanal ändern, um durch andere Geräte verursachte Störungen zu vermeiden.
7. Wählen Sie als Modus nur g aus, um den 802.11-Modus zu konfigurieren. Wenn Sie über ältere 802.11b-Geräte verfügen, können Sie Unterstützung für diese aktivieren.
8. Deaktivieren Sie **Allow Broadcast of Name (SSID)** (Broadcast des Namens (SSID) zulassen), um zu verhindern, dass der Drahtloszugriffspunkt seine SSID überträgt.
9. Wählen Sie **WPA2 mit PSK** aus. Die verfügbaren Sicherheitsoptionen variieren je nach Hersteller, normalerweise sind jedoch die folgenden enthalten: WEP, WPA und WPA2 sowie Unterstützung der Optionen PSK und Enterprise.

Hinweis: Wenn Sie eine Enterprise-Option auswählen, müssen weitere Informationen darüber bereitgestellt werden, wie die Authentifizierung innerhalb der Organisation behandelt wird. Dazu zählen der Name eines RADIUS-Servers sowie andere Einstellungen.

10. Geben Sie **Pa\$\$w0rd** unter **Network Key** (Netzwerkschlüssel) ein.
11. Klicken zum Speichern der Einstellungen auf **Apply** (Übernehmen). Die meisten drahtlosen Zugriffspunkte verfügen über einen separaten permanenten Speicher, sodass die Einstellungen auch nach dem Aus- und wieder Einschalten beibehalten werden.
12. Die meisten drahtlosen Zugriffspunkte bieten auch erweiterte Einstellungen. Dazu zählen MAC-Adressfilterung und Bridging, die in dieser Demo jedoch nicht behandelt werden.
13. Schließen Sie alle geöffneten Fenster.

Herstellen einer Verbindung mit einem nicht aufgeführten Drahtlosnetzwerk

Die Demo enthält folgende Schritte:

1. Klicken Sie mit der rechten Maustaste auf das Drahtlosnetzwerksymbol auf der Taskleiste, und klicken Sie auf **Netzwerk- und Freigabecenter öffnen**.
2. Klicken Sie auf **Drahtlosnetzwerke verwalten**.
3. Klicken Sie auf **Hinzufügen**, um den Assistenten zum Definieren der Eigenschaften des Netzwerks zu starten.
4. Klicken Sie zum Konfigurieren eines Infrastrukturnetzwerks auf **Ein Netzwerkprofil manuell erstellen**.
5. Geben Sie **ADATUM** unter **Netzwerkname** ein, wählen Sie **WPA2-Personal** als **Sicherheitstyp** aus, wählen Sie **AES** als **Verschlüsselungstyp** aus, und geben Sie **Pa\$\$w0rd** als **Sicherheitsschlüssel/Passphrase** ein, um die entsprechende SSID und die Sicherheitseinstellungen übereinstimmend mit den auf dem Drahtloszugriffspunkt definierten Einstellungen festzulegen.

Hinweis: Die Einstellungen variieren je nach Netzwerk. Außerdem werden die verfügbaren Optionen möglicherweise durch Gruppenrichtlinien eingeschränkt. Eventuell ist für Sie die Möglichkeit der Herstellung einer Netzwerkverbindung eingeschränkt.

6. Klicken Sie zum Herstellen einer Verbindung mit dem Netzwerk auf **Weiter** und dann auf **Schließen**.
7. Klicken Sie mit der rechten Maustaste auf das Drahtlosnetzwerksymbol auf der Taskleiste, und klicken Sie auf **Netzwerk- und Freigabecenter öffnen**. Klicken Sie auf **Drahtlosnetzwerkverbindung (ADATUM)**, um den Netzwerkstatus anzuzeigen.
8. Klicken Sie auf **Schließen**, um das Dialogfeld **Status der Drahtlosnetzwerkverbindung** zu schließen.
9. In der Standardeinstellung werden alle Netzwerke im öffentlichen Netzwerkprofil platziert. Dabei handelt es sich um das restriktivste Profil. Klicken Sie im **Netzwerk- und Freigabecenter** auf **Öffentliches Netzwerk**.
10. Klicken Sie auf **Arbeitsplatznetzwerk** und dann auf **Schließen**. Wenn Sie für eine Netzwerkverbindung ein Netzwerkstandortprofil definieren, behält Windows dieses für nachfolgende Verbindungen mit diesem Netzwerk bei.
11. Schließen Sie alle geöffneten Fenster.

Herstellen einer Verbindung mit einem öffentlichen Drahtlosnetzwerk

Die Demo enthält folgende Schritte:

1. Klicken Sie auf der Taskleiste mit der rechten Maustaste auf das Drahtlosnetzwerksymbol, und klicken Sie zur Anzeige der verfügbaren Netzwerke auf **Netzwerk- und Freigabecenter öffnen**. Sie können auch auf der Taskleiste auf das Drahtlosnetzwerksymbol klicken, um die verfügbaren Netzwerke anzuzeigen.
2. Beachten Sie, dass ein Drahtlosnetzwerk verfügbar ist. Das Schildsymbol neben dem Symbol für das Drahtlossignal weist darauf hin, dass das Drahtlosnetzwerk offen ist. Dies kann u. U. zu einem Sicherheitsproblem führen. Gehen Sie beim Verbinden mit öffentlichen Netzwerken immer vorsichtig vor.

3. Klicken Sie auf das Drahtlosnetzwerk, wählen Sie **Verbindung automatisch herstellen** aus, und klicken Sie dann auf **Verbinden**. Dadurch werden Sie mit dem Drahtlosnetzwerk verbunden.
4. Windows fordert den Benutzer auf, das Netzwerkstandortprofil zu definieren. Wählen Sie **Öffentlich** aus.
5. Klicken Sie auf **Schließen**, und schließen Sie dann das Netzwerk- und Freigabecenter.

Lernzielkontrollen und Kernpunkte der Unterrichtseinheit

Häufige Probleme beim Erkennen von Drahtlosnetzwerken und Verbessern der Signalstärke

In der folgenden Tabelle sind häufige Probleme beim Erkennen von Drahtlosnetzwerken und Verbessern der Signalstärke aufgeführt.

Problem	Tipps zur Problembehandlung
Nähe oder physisches Blockieren	<ul style="list-style-type: none"> • Stellen Sie sicher, dass sich der Clientcomputer so nah wie möglich am drahtlosen Zugriffspunkt befindet. • Wenn kein kleinerer Abstand zum drahtlosen Zugriffspunkt möglich ist, sollten Sie eventuell eine externe Antenne am Drahtlosnetzwerkadapter installieren. • Achten Sie auf physische Objekte, die Störungen verursachen könnten, wie z. B. eine dicke Wand oder ein Metallschrank, und entfernen Sie diese Objekte, oder positionieren Sie den drahtlosen Zugriffspunkt oder den Client anders. • Fügen Sie dem Drahtlosnetzwerk je nach Möglichkeit drahtlose Zugriffspunkte hinzu.
Störung durch ein anderes Signal	<ul style="list-style-type: none"> • Achten Sie auf Geräte, die Störungen verursachen können, wie z. B. schnurlose Telefone, Bluetooth-Geräte oder andere drahtlose Geräte. Schalten Sie sie aus, oder positionieren Sie sie weiter entfernt. • Ändern Sie ggf. die Einstellungen des drahtlosen Zugriffspunkts so, dass ein anderer Drahtloskanal verwendet wird, oder legen Sie die automatische Auswahl des Kanals fest, wenn dieser auf eine bestimmte Kanalnummer festgelegt ist.
Drahtlosnetzwerk wird nicht erkannt	<ul style="list-style-type: none"> • Überprüfen Sie, ob der Drahtlosnetzwerkadapter über den richtigen Treiber verfügt und ordnungsgemäß funktioniert. • Suchen Sie am Computer nach einem externen Schalter für den Drahtlosnetzwerkadapter. • Überprüfen Sie, ob der drahtlose Zugriffspunkt eingeschaltet ist und ordnungsgemäß funktioniert. • Überprüfen Sie, ob der drahtlose Zugriffspunkt für das Veröffentlichen der SSID konfiguriert ist.
Windows ist nicht für die Verbindung mit dem richtigen Netzwerktyp konfiguriert.	<ul style="list-style-type: none"> • Überprüfen Sie die Informationen zu Ihrem Router oder Zugriffspunkt, um herauszufinden, auf welchen Verbindungsmodus das Gerät festgelegt ist. Der Modus muss entweder Ad-hoc (wenn die Geräte direkt ohne einen Router oder Zugriffspunkt miteinander kommunizieren) oder Infrastruktur (wenn die Geräte über einen Router oder Zugriffspunkt miteinander kommunizieren) sein. Stellen Sie sicher, dass die Einstellung für dieses Netzwerk in Windows mit der Einstellung auf dem Gerät übereinstimmt.
Der Router oder der Drahtloszugriffspunkt ist ausgelastet.	<ul style="list-style-type: none"> • Wenn weitere Computer mit dem Netzwerk verbunden sind, versuchen Sie, diese vorübergehend zu trennen.

Der Drahtlosnetzwerkadapter befindet sich im Überwachungsmodus.	<ul style="list-style-type: none"> • Wenn auf Ihrem Computer ein Netzwerküberwachungsprogramm ausgeführt wird, wird der Drahtlosnetzwerkadapter auf den Überwachungsmodus festgelegt. Dadurch wird verhindert, dass Windows eine Verbindung mit Drahtlosnetzwerken herstellt. Um eine Verbindung mit einem Drahtlosnetzwerk herzustellen, schließen Sie das Netzwerküberwachungsprogramm und befolgen die Anweisungen im Programm, um den Überwachungsmodus zu beenden.
---	--

Praxisnahe Probleme und Szenarios

Frage 1: Sie implementieren ein Drahtlosnetzwerk in Ihrer Organisation. Welche Technologiestandards für Drahtlosnetzwerke und welchen Sicherheitstyp (Authentifizierung und Verschlüsselung) wählen Sie?

Antwort: Bei der Auswahl einer Standarddrahtlostechnologie sollten zwei Punkte besonders berücksichtigt werden: Geschwindigkeit und Kosten. Wählen Sie nach Möglichkeit den neuesten Standard 802.11n aus, da dieser eine optimale Signalstärke und die höchste Geschwindigkeit bietet.

Einer der Nachteile dieses Standards besteht darin, dass er sich noch in der Entwicklung befindet. Dennoch wird dieser Standard auf Basis von „Vorschlagsentwurf 2“ bereits von vielen Geräten unterstützt. Sie sollten auch berücksichtigen, dass Geräte mit Unterstützung für diesen Standard meist teurer sind als Geräte, die 802.11g unterstützen.

Entscheiden Sie sich stets für die höchstmögliche Sicherheit. In diesem Fall bieten sowohl WPA als auch WPA2 sichere Authentifizierung und Verschlüsselung. Wählen Sie den Enterprise-Modus für WPA/WPA2 aus, da dieser die zentrale Verwaltung der Authentifizierung mit RADIUS-Servern ermöglicht.

Frage 2: Die Organisation verfügt bereits über ein Drahtlosnetzwerk. Die Benutzer klagen, dass die Leistung des Drahtlosnetzwerks schlechter als die des Kabelnetzwerks ist. Wie können Sie die Leistung des Drahtlosnetzwerks erhöhen?

Antwort: Die Leistung des Drahtlosnetzwerks kann in drei Bereichen verbessert werden: Nähe, Hindernisse und Störungen. Auf Grundlage dieser Bereiche können Sie verschiedene Lösungen implementieren, z. B. Drahtloszugriffspunkte hinzufügen oder Hindernisse und Störungen beseitigen. Weitere Informationen finden Sie im Thema „Verbessern der Drahtlossignalstärke“.

Tools

Tool	Use to	Where to find it
Netzwerk- und Freigabecenter	Konfigurieren von Netzwerkeinstellungen	Systemsteuerung Systray
Verbindung mit einem Netzwerk herstellen	Konfigurieren eines Windows 7-Clients zum Herstellen einer Verbindung mit einem Drahtlosnetzwerk	Netzwerk- und Freigabecenter – Taskleiste
Netsh	Konfigurieren von lokalen oder Remote-Netzwerkeinstellungen	Eingabeaufforderung
Windows-Netzwerkd Diagnose	Problembehandlung beim Zugriff auf Drahtlosnetzwerke	Netzwerk- und Freigabecenter – Taskleiste

Fragen und Antworten zur Lernzielkontrolle

Frage: In den Übungseinheiten war es Ihre Aufgabe, das Drahtlosnetzwerk so sicher wie möglich zu machen. Ist dieses Vorgehen auch dann sinnvoll, wenn beliebige Personen Zugriff auf das Drahtlosnetzwerk haben sollen, z. B. in einem Café? Wie konfigurieren Sie die Drahtlosinfrastruktur für einen solchen Zugriff?

Antwort: Nein, wenn Sie die in den Übungseinheiten beschriebenen Einstellungen vornehmen, können nur ausdrücklich autorisierte Benutzer und Computer auf das Netzwerk zugreifen. Damit beliebige Personen auf das Netzwerk zugreifen können, aktivieren Sie die SSID-Übertragung, um das Netzwerk besser sichtbar zu machen. Legen Sie die Netzwerksicherheit auf „Offen“ fest. Dies bedeutet, dass kein Zertifikat, freigegebener Schlüssel oder anderer Authentifizierungsmechanismus zur Herstellung einer Verbindung erforderlich ist.

Frage: Sollte dieses weniger eingeschränkte Drahtlosnetzwerk mit dem Unternehmensnetzwerk verbunden werden?

Antwort: Nein, dies ist nicht empfehlenswert. Da Sie wenig Kontrolle darüber haben, welche Personen eine Verbindung mit dem Netzwerk herstellen bzw. keine Informationen über den Status ihrer Computer haben, würde ein uneingeschränkter Zugriff auf das Unternehmensnetzwerk ein Sicherheitsrisiko darstellen.

Frage: Fällt Ihnen eine Lösung ein, mit der rechtmäßige Benutzer Ihrer Organisation im Café eine drahtlose Verbindung mit Ihrer Infrastruktur herstellen können, während anonyme Benutzer nicht über denselben Zugriff verfügen?

Antwort: Stellen Sie zwei drahtlose Zugriffspunkte bereit, und konfigurieren Sie die Computer Ihrer Benutzer mit einem Gruppenrichtlinienobjekt, das nur eine Verbindung mit den definierten Drahtlosnetzwerken gestattet. Für diese Netzwerke sind die in der Übungseinheit erläuterten Authentifizierungseinstellungen mit hoher Sicherheitsstufe erforderlich. Anonyme Benutzer hingegen sehen nur das geöffnete Netzwerk. Es muss unbedingt gewährleistet sein, dass keine Interferenzen zwischen den zwei Netzwerken auftreten.

Unterrichtseinheit 6

Sichern des Windows® 7-Desktops

Inhalt:

Lektion 1: Übersicht über die Sicherheitsverwaltung in Windows 7	100
Lektion 2: Sichern eines Windows 7-Clientcomputers über die Einstellungen der lokalen Sicherheitsrichtlinie	102
Lektion 3: Sichern von Daten mit EFS und BitLocker	109
Lektion 4: Konfigurieren von Anwendungseinschränkungen	114
Lektion 5: Konfigurieren der Benutzerkontensteuerung	119
Lektion 6: Konfigurieren der Windows-Firewall	123
Lektion 7: Konfigurieren von Sicherheitseinstellungen in Internet Explorer 8	129
Lektion 8: Konfigurieren von Windows Defender	133
Lernzielkontrollen und Kernpunkte der Unterrichtseinheit	137
Fragen und Antworten zur Lernzielkontrolle	144

Lektion 1

Übersicht über die Sicherheitsverwaltung in Windows 7

Inhalt:

Detaillierte Demoschritte

101

Detaillierte Demoschritte

Demo: Konfigurieren der Wartungscentereinstellungen

Detaillierte Demoschritte

Ändern der Wartungscentereinstellungen

1. Melden Sie sich auf dem virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start** und dann auf **Systemsteuerung**.
3. Klicken Sie in der Systemsteuerung auf **System und Sicherheit**, und klicken Sie dann auf **Wartungscenter**.
4. Klicken Sie neben **Sicherheit** auf den Pfeil nach unten, und führen Sie einen Bildlauf nach unten durch, um die Einstellungen zu überprüfen.
5. Klicken Sie im linken Fensterbereich auf **Wartungscentereinstellungen ändern**.
6. Stellen Sie unter **Wartungsmeldungen** sicher, dass die Kontrollkästchen **Windows-Problembehandlung und Windows-Sicherung** deaktiviert sind, und klicken Sie dann auf **OK**.

Ändern der Einstellungen der Benutzersteuerung

1. Klicken Sie im linken Fensterbereich auf **Einstellungen der Benutzerkontensteuerung ändern**.
2. Setzen Sie den Schieberegler um einen Schritt herunter, und klicken Sie dann auf **OK**.

Anzeigen der archivierten Meldungen

1. Wählen Sie im linken Fensterbereich **Archivierte Meldungen anzeigen** aus.
2. Zeigen Sie sämtliche archivierten Meldungen zu Computerproblemen an, und klicken Sie dann auf **OK**.
3. Schließen Sie das Fenster Wartungscenter.

Lektion 2

Sichern eines Windows 7-Clientcomputers über die Einstellungen der lokalen Sicherheitsrichtlinie

Inhalt:

Fragen und Antworten	103
Detaillierte Demoschritte	104

Fragen und Antworten

Funktionsweise mehrerer lokaler Gruppenrichtlinien

Frage: Ein Administrator deaktiviert die Einstellung mit dem Namen „Sicherheitsseite deaktivieren“ im lokalen Gruppenrichtlinienobjekt. Anschließend aktiviert der Administrator die gleiche Einstellung in einem benutzerspezifischen lokalen Gruppenrichtlinienobjekt. Der Benutzer, der sich am Computer anmeldet, ist kein Administrator. Welche Richtlinieneinstellung wird auf dieses lokale Gruppenrichtlinienobjekt angewendet?

Antwort: Windows liest zuerst das lokale Gruppenrichtlinienobjekt, anschließend das lokale Nicht-Administrator-Gruppenrichtlinienobjekt, gefolgt vom benutzerspezifischen lokalen Gruppenrichtlinienobjekt. Der Status der Richtlinieneinstellung wird deaktiviert, wenn Windows das lokale Gruppenrichtlinienobjekt liest. Die Richtlinieneinstellung ist nicht im lokalen Nicht-Administrator-Gruppenrichtlinienobjekt konfiguriert. Da dies keine Auswirkungen auf den Status der Einstellung hat, bleibt diese aktiviert. Die Richtlinieneinstellung wird im benutzerspezifischen lokalen Gruppenrichtlinienobjekt aktiviert. Dies ändert den Status der Einstellung auf **Aktiviert**. Windows liest das benutzerspezifische lokale Gruppenrichtlinienobjekt zuletzt, daher hat es den höchsten Rang. Die lokale Computerrichtlinie hat einen niedrigeren Rang.

Detaillierte Demoschritte

Demo: Erstellen von mehreren lokalen Gruppenrichtlinien

Detaillierte Demoschritte

Erstellen einer benutzerdefinierten Verwaltungskonsole

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, und geben Sie im Feld **Programme/Dateien durchsuchen** „mmc“ ein, und drücken Sie dann die EINGABETASTE.
3. Klicken Sie im Fenster **Konsole1 – [Konsolenstamm]** auf **Datei**, und klicken Sie dann auf **Snap-In hinzufügen/entfernen**.
4. Klicken Sie im Dialogfeld **Snap-Ins hinzufügen bzw. entfernen** in der Liste **Verfügbare Snap-Ins** auf **Gruppenrichtlinienobjekt-Editor** und dann auf **Hinzufügen**.
5. Klicken Sie im Dialogfeld **Gruppenrichtlinienobjekt auswählen** auf **Fertig stellen**.
6. Klicken Sie im Dialogfeld **Snap-Ins hinzufügen bzw. entfernen** in der Liste **Verfügbare Snap-Ins** auf **Gruppenrichtlinienobjekt-Editor** und dann auf **Hinzufügen**.
7. Klicken Sie im Dialogfeld **Gruppenrichtlinienobjekt auswählen** auf **Durchsuchen**.
8. Klicken Sie im Dialogfeld **Gruppenrichtlinienobjekt suchen** auf die Registerkarte **Benutzer**.
9. Klicken Sie in der Liste **mit den lokalen Benutzern und Gruppen**, die kompatibel mit der lokalen Gruppenrichtlinie sind, auf **Administratoren**, und klicken Sie dann auf **OK**.
10. Klicken Sie im Dialogfeld **Gruppenrichtlinienobjekt auswählen** auf **Fertig stellen**.
11. Klicken Sie im Dialogfeld **Snap-Ins hinzufügen bzw. entfernen** in der Liste **Verfügbare Snap-Ins** auf **Gruppenrichtlinienobjekt-Editor** und dann auf **Hinzufügen**.
12. Klicken Sie im Dialogfeld **Gruppenrichtlinienobjekt auswählen** auf **Durchsuchen**.
13. Klicken Sie im Dialogfeld **Gruppenrichtlinienobjekt suchen** auf die Registerkarte **Benutzer**.
14. **Klicken Sie in der Liste mit den lokalen Benutzern und Gruppen, die kompatibel mit der lokalen Gruppenrichtlinie sind**, auf **Nicht-Administratoren** und dann auf **OK**.
15. Klicken Sie im Dialogfeld **Gruppenrichtlinienobjekt auswählen** auf **Fertig stellen**.
16. Klicken Sie im Dialogfeld **Snap-Ins hinzufügen bzw. entfernen** auf **OK**.
17. Klicken Sie im Fenster **Konsole1 – [Konsolenstamm]** im Menü auf **Datei** und dann auf **Speichern**.
18. Klicken Sie im Dialogfeld **Speichern unter** auf **Desktop**.
19. Geben Sie im Feld **Dateiname** „**Editor für mehrere lokale Gruppenrichtlinien**“ ein, und klicken Sie dann auf **Speichern**.

Konfigurieren der lokalen Computerrichtlinie

1. Erweitern Sie in der Struktur von **Editor für mehrere lokale Gruppenrichtlinien - [Konsolenstamm]** die **Richtlinie für „Lokaler Computer“**.

2. Erweitern Sie **Benutzerkonfiguration** und **Windows-Einstellungen**, und klicken Sie dann auf **Skripts (Anmelden/Abmelden)**.
3. Doppelklicken Sie im Ergebnisbereich auf **Anmelden**.
4. Klicken Sie im Dialogfeld **Eigenschaften von Anmelden** auf **Hinzufügen**.
5. Klicken Sie im Dialogfeld **Hinzufügen eines Skripts** auf **Durchsuchen**.
6. Klicken Sie im Dialogfeld **Durchsuchen** mit der rechten Maustaste auf den leeren Ordner, zeigen Sie auf **Neu**, klicken Sie auf **Textdokument**, und drücken Sie anschließend die EINGABETASTE.
7. Klicken Sie mit der rechten Maustaste auf **Neues Textdokument**, und klicken Sie dann auf **Bearbeiten**.
8. Geben Sie „msgbox „Standardcomputerrichtlinie““ ein, klicken Sie auf **Datei**, klicken Sie auf **Speichern unter**.
9. Geben Sie **ComputerScript.vbs** ein, ändern Sie **Dateityp**: auf **Alle Dateien**, und klicken Sie dann auf **Speichern**.
10. Schließen Sie **ComputerScript.vbs**.
11. Klicken Sie im Dialogfeld **Durchsuchen** auf die Datei **ComputerScript** und dann auf **Öffnen**.
12. Klicken Sie im Dialogfeld **Hinzufügen eines Skripts** auf **OK**.
13. Klicken Sie im Dialogfeld **Eigenschaften von Anmelden** auf **OK**.

Konfigurieren der lokalen Computerrichtlinie für Administratoren

1. Erweitern Sie in der Struktur von **Editor für mehrere lokale Gruppenrichtlinien - [Konsolenstamm]** die **Richtlinien für Lokaler Computer\Administratoren**.
2. Erweitern Sie **Benutzerkonfiguration** und **Windows-Einstellungen**, und klicken Sie dann auf **Skripts (Anmelden/Abmelden)**.
3. Doppelklicken Sie im Ergebnisbereich auf **Anmelden**.
4. Klicken Sie im Dialogfeld **Eigenschaften von Anmelden** auf **Hinzufügen**.
5. Klicken Sie im Dialogfeld **Hinzufügen eines Skripts** auf **Durchsuchen**.
6. Klicken Sie im Dialogfeld **Durchsuchen** mit der rechten Maustaste auf den leeren Ordner, klicken Sie auf **Neu**, klicken Sie auf **Textdokument**, und drücken Sie dann die EINGABETASTE.
7. Klicken Sie mit der rechten Maustaste auf **Neues Textdokument**, und klicken Sie dann auf **Bearbeiten**.
8. Geben Sie „msgbox „Standardrichtlinie des Administrators““ ein, klicken Sie auf **Datei**, und klicken Sie dann auf **Speichern unter**.
9. Geben Sie den Dateinamen „AdminScript.vbs“ ein, ändern Sie **Dateityp** auf **Alle Dateien**, und klicken Sie dann auf **Speichern**.
10. Schließen Sie **AdminScript.vbs**.
11. Klicken Sie im Dialogfeld **Durchsuchen** auf die Datei **AdminScript** und dann auf **Öffnen**.
12. Klicken Sie im Dialogfeld **Hinzufügen eines Skripts** auf **OK**.
13. Klicken Sie im Dialogfeld **Eigenschaften von Anmelden** auf **OK**.

Konfigurieren der lokalen Computerrichtlinie für Nicht-Administratoren

1. Erweitern Sie in der Struktur von **Editor für mehrere lokale Gruppenrichtlinien - [Konsolenstamm]** die **Richtlinien für Lokaler Computer\Nicht-Administratoren**.
2. Erweitern Sie **Benutzerkonfiguration** und **Windows-Einstellungen**, und klicken Sie dann auf **Skripts (Anmelden/Abmelden)**.
3. Doppelklicken Sie im Ergebnisbereich auf **Anmelden**.
4. Klicken Sie im Dialogfeld **Eigenschaften von Anmelden** auf **Hinzufügen**.
5. Klicken Sie im Dialogfeld **Hinzufügen eines Skripts** auf **Durchsuchen**.
6. Klicken Sie im Dialogfeld **Durchsuchen** mit der rechten Maustaste auf den leeren Ordner, klicken Sie auf **Neu**, klicken Sie auf **Textdokument**, und drücken Sie dann die EINGABETASTE.
7. Klicken Sie mit der rechten Maustaste auf **Neues Textdokument**, und klicken Sie dann auf **Bearbeiten**.
8. Geben Sie „msgbox „Standardbenutzerrichtlinie““ ein, klicken Sie auf **Datei**, und klicken Sie dann auf **Speichern unter**.
9. Geben Sie „UserScript.vbs“ ein, ändern Sie **Dateityp:** auf **Alle Dateien**, und klicken Sie dann auf **Speichern**.
10. Schließen Sie **UserScript.vbs**.
11. Klicken Sie im Dialogfeld **Durchsuchen** auf die Datei **UserScript** und dann auf **Öffnen**.
12. Klicken Sie im Dialogfeld **Hinzufügen eines Skripts** auf **OK**.
13. Klicken Sie im Dialogfeld **Eigenschaften von Anmelden** auf **OK**.
14. Melden Sie sich von LON-CL1 ab.

Testen mehrerer lokaler Gruppenrichtlinien

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Adam** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **OK, wenn die Meldung angezeigt wird, und klicken Sie dann erneut auf OK**.
3. Melden Sie sich ab.
4. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
5. Klicken Sie auf **OK, wenn die Meldung angezeigt wird, und klicken Sie dann erneut auf OK**.
6. **Klicken Sie auf dem Desktop mit der rechten Maustaste auf Editor für mehrere lokale Gruppenrichtlinien, und klicken Sie dann auf Öffnen.**
7. Erweitern Sie in der Struktur von **Editor für mehrere lokale Gruppenrichtlinien - [Konsolenstamm]** die **Richtlinien für Lokaler Computer\Nicht-Administratoren**.
8. Erweitern Sie **Benutzerkonfiguration** und **Windows-Einstellungen**, und klicken Sie dann auf **Skripts (Anmelden/Abmelden)**.
9. Doppelklicken Sie im Ergebnisbereich auf **Anmelden**.
10. Klicken Sie im Dialogfeld **Eigenschaften von Anmelden** auf **Entfernen und dann auf OK**.

11. Erweitern Sie in der Struktur von **Editor für mehrere lokale Gruppenrichtlinien - [Konsolenstamm]** die **Richtlinien für Lokaler Computer\Administratoren**.
12. Erweitern Sie **Benutzerkonfiguration** und **Windows-Einstellungen**, und klicken Sie dann auf **Skripts (Anmelden/Abmelden)**.
13. Doppelklicken Sie im Ergebnisbereich auf **Anmelden**.
14. Klicken Sie im Dialogfeld **Eigenschaften von Anmelden** auf **Entfernen** und dann auf **OK**.
15. Erweitern Sie in der Struktur von **Editor für mehrere lokale Gruppenrichtlinien - [Konsolenstamm]** die **Richtlinie für „Lokaler Computer“**.
16. Erweitern Sie **Benutzerkonfiguration** und **Windows-Einstellungen**, und klicken Sie dann auf **Skripts (Anmelden/Abmelden)**.
17. Doppelklicken Sie im Ergebnisbereich auf **Anmelden**.
18. Klicken Sie im Dialogfeld **Eigenschaften von Anmelden** auf **Entfernen und dann auf OK**.
19. Schließen Sie das Snap-In **Editor für mehrere lokale Gruppenrichtlinien - [Konsolenstamm]**.
20. Klicken Sie auf **Ja, wenn Sie zum Speichern aufgefordert werden**.
21. Melden Sie sich ab.

Demo: Konfigurieren der Einstellungen von lokalen Sicherheitsrichtlinien

Detaillierte Demoschritte

Überprüfen der Einstellungen der lokalen Sicherheitsgruppenrichtlinie

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, geben Sie im Feld **Programme/Dateien durchsuchen** die Zeichenfolge „gpedit.msc“ ein, und drücken Sie dann die EINGABETASTE.
3. Erweitern Sie im **Editor für lokale Gruppenrichtlinien** die Knoten **Computerkonfiguration**, **Windows-Einstellungen** und **Sicherheitseinstellungen**.
4. Erweitern Sie **Kontorichtlinien**, und klicken Sie anschließend auf **Kennwortrichtlinie**.
5. Klicken Sie auf **Kontosperrungsrichtlinie**.
6. Erweitern Sie im linken Bereich **Lokale Richtlinien**, und klicken Sie dann auf **Überwachungsrichtlinie**.
7. Klicken Sie im Hauptfenster mit der rechten Maustaste auf **Kontenverwaltung überwachen**, und wählen Sie dann **Eigenschaften** aus.
8. Wählen Sie im Dialogfeld **Eigenschaften von Kontenverwaltung überwachen** die Option **Erfolg und Fehler** aus, und klicken Sie dann auf **OK**.
9. Klicken Sie auf **Zuweisen von Benutzerrechten**.
10. Klicken Sie auf **Sicherheitsoptionen**.
11. Erweitern Sie im linken Bereich **Windows-Firewall mit erweiterter Sicherheit**, und klicken Sie dann auf **Windows-Firewall mit erweiterter Sicherheit - Lokales Gruppenrichtlinienobjekt**.
12. Klicken Sie im linken Bereich auf **Netzwerklisten-Manager-Richtlinien**.

13. Erweitern Sie im linken Bereich **Richtlinien öffentlicher Schlüssel**, und klicken Sie dann auf **Verschlüsselndes Dateisystem**.
14. Klicken Sie auf **BitLocker-Laufwerkverschlüsselung**.
15. Klicken Sie im linken Bereich auf **Richtlinien für Softwareeinschränkung**.
16. Erweitern Sie im linken Bereich **Anwendungssteuerungsrichtlinien**.
17. Erweitern Sie **AppLocker**.
18. Klicken Sie im linken Bereich auf **IP-Sicherheitsrichtlinien auf Lokaler Computer**.
19. Erweitern Sie im linken Bereich **Erweiterte Überwachungsrichtlinienkonfiguration**.
20. Erweitern Sie **Systemüberwachungsrichtlinien - lokales Gruppenrichtlinienobjekt**.
21. Schließen Sie den **Editor für lokale Gruppenrichtlinien**.
22. Melden Sie sich bei LON-CL1 ab.

Lektion 3

Sichern von Daten mit EFS und BitLocker

Inhalt:

Fragen und Antworten	110
Detaillierte Demoschritte	112

Fragen und Antworten

Was ist EFS?

Frage: Erklären Sie, weshalb Systemordner nicht für die Verschlüsselung gekennzeichnet werden können.

Antwort: Während des Startvorgangs sind keine EFS-Schlüssel verfügbar. Daher kann die Systemdatei nicht gestartet werden, wenn Systemdateien verschlüsselt sind.

Was ist BitLocker?

Frage: BitLocker sorgt für eine vollständige Volumeverschlüsselung. Was bedeutet das?

Antwort: Vollständige Volumeverschlüsselung bedeutet: 1) Das gesamte Windows-Betriebssystemvolumen kann verschlüsselt werden, und 2) feste Datenvolumen können verschlüsselt werden (dafür muss auch das Betriebssystemvolumen verschlüsselt sein).

BitLocker-Modi

Frage: Was ist der Nachteil beim Ausführen von BitLocker auf einem Computer ohne TPM 1.2?

Antwort: Computer ohne TPMs können die von BitLocker bereitgestellte Systemintegritätsüberprüfung während des Starts nicht verwenden.

Konfigurieren von BitLocker

Frage: Zu welchem Zweck wird ein Wiederherstellungskennwort gespeichert, wenn BitLocker auf einem Computer mit TPM Version 1.2 aktiviert wird?

Antwort: Wenn sich das TPM ändert oder nicht darauf zugegriffen werden kann, wenn sich wichtige Systemdateien ändern oder wenn jemand versucht, den Computer von einer Produkt-CD oder -DVD zu starten, um das Betriebssystem zu umgehen, wechselt der Computer in den Wiederherstellungsmodus und bleibt dort, bis der Benutzer das Wiederherstellungskennwort angibt. Durch das Speichern des Wiederherstellungskennworts, sodass der Benutzer darauf zugreifen kann, erhält dieser die Möglichkeit, den Startvorgang abzuschließen.

Konfigurieren von BitLocker To Go

Frage: Wie wird BitLocker To Go für ein USB-Flashlaufwerk aktiviert?

Antwort: Schließen Sie das Laufwerk an, klicken Sie in Windows-Explorer mit der rechten Maustaste auf das Laufwerk, und klicken Sie dann auf **BitLocker aktivieren**.

Wiederherstellen von mit BitLocker verschlüsselten Laufwerken

Frage: Was ist der Unterschied zwischen dem Wiederherstellungskennwort und der Kennwort-ID?

Antwort: Das Wiederherstellungskennwort ist ein 48-stelliges Kennwort, das verwendet wird, um ein System im Wiederherstellungsmodus zu entsperren. Das Wiederherstellungskennwort ist für eine bestimmte BitLocker-Verschlüsselung eindeutig und kann in Active Directory gespeichert werden. Bei der Kennwort-ID eines Computers handelt es sich um ein 32 Zeichen langes Kennwort, das für einen Computernamen eindeutig ist. Suchen Sie die Kennwort-ID unter den Eigenschaften eines Computers, mit dem Sie in Active Directory gespeicherte Wiederherstellungskennwörter suchen können.

Detaillierte Demoschritte

Demo: Verschlüsseln und Entschlüsseln von Dateien und Ordnern mit EFS

Detaillierte Demoschritte

Verschlüsseln von Dateien und Ordnern

1. Melden Sie sich auf dem virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start** und dann auf **Computer**.
3. Doppelklicken Sie auf **Lokaler Datenträger (C:)**.
4. Klicken Sie mit der rechten Maustaste in den leeren Bereich unterhalb der Spalte **Name**, zeigen Sie auf **Neu**, und klicken Sie dann auf **Ordner**.
5. Geben Sie als Ordnername „Verschlüsselt“ an, und drücken Sie dann die EINGABETASTE.
6. Doppelklicken Sie auf **Verschlüsselt**, klicken Sie dann mit der rechten Maustaste in einen leeren Bereich der Spalte **Name**, zeigen Sie auf **Neu**, und klicken Sie dann auf **Microsoft Office Word-Dokument**.
7. Geben Sie „Privat“ ein, und drücken Sie dann die EINGABETASTE.
8. Klicken Sie in der Menüleiste auf den nach links weisenden Pfeil, um zu **Lokaler Datenträger (C:)** zurückzukehren.
9. Klicken Sie mit der rechten Maustaste auf den Ordner **Verschlüsselt**, und klicken Sie dann auf **Eigenschaften**.
10. Klicken Sie auf der Registerkarte **Allgemein** auf **Erweitert**.
11. Aktivieren Sie das Kontrollkästchen **Inhalt verschlüsseln, um Daten zu schützen**, und klicken Sie dann auf **OK**.
12. Klicken Sie im Dialogfeld **Verschlüsselte Eigenschaften** auf **OK** und dann im Dialogfeld **Änderungen der Attribute bestätigen** auf **Änderungen für diesen Ordner, untergeordnete Ordner und Dateien übernehmen**.
13. Klicken Sie auf **OK**.
14. Klicken Sie auf **OK**, um das Dialogfeld **Verschlüsselte Eigenschaften** zu schließen, und melden Sie sich anschließend ab.

Überprüfen der Verschlüsselung von Dateien und Ordnern

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Adam** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start** und dann auf **Computer**.
3. Doppelklicken Sie auf **Lokaler Datenträger (C:)**.
4. Doppelklicken Sie auf den Ordner **Verschlüsselt**.
5. Doppelklicken Sie auf **Privat**.
6. Klicken Sie auf **OK**, wenn Sie dazu mit einer Meldung aufgefordert werden.

7. Klicken Sie auf **OK**, um das Feld Benutzername zu schließen.
8. Schließen Sie die Datei.
9. Melden Sie sich ab.

Entschlüsseln von Dateien und Ordnern

1. Melden Sie sich auf dem virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, klicken Sie auf **Computer**, und doppelklicken Sie dann auf **Lokaler Datenträger (C:)**.
3. Klicken Sie mit der rechten Maustaste auf den Ordner **Verschlüsselt**, und klicken Sie dann auf **Eigenschaften**.
4. Klicken Sie auf der Registerkarte **Allgemein** auf **Erweitert**.
5. Deaktivieren Sie das Kontrollkästchen **Inhalt verschlüsseln, um Daten zu schützen**, und klicken Sie dann auf **OK**.
6. Klicken Sie auf **OK**, um das Dialogfeld **Verschlüsselte Eigenschaften** zu schließen.
7. Klicken Sie im Dialogfeld **Änderungen der Attribute bestätigen** auf **OK**.
8. Melden Sie sich ab.

Überprüfen der Entschlüsselung von Dateien und Ordnern

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Adam** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start** und dann auf **Computer**.
3. Doppelklicken Sie auf **Lokaler Datenträger (C:)**.
4. Doppelklicken Sie auf den Ordner **Verschlüsselt**.
5. Doppelklicken Sie auf **Privat**.
6. Geben Sie in der Datei „entschlüsselt“ ein.
7. Speichern und schließen Sie die Datei.
8. Melden Sie sich ab.

Lektion 4

Konfigurieren von Anwendungseinschränkungen

Inhalt:

Fragen und Antworten	115
Detaillierte Demoschritte	116

Fragen und Antworten

Was ist AppLocker?

Frage: Welche Anwendungen sind zum Anwenden einer AppLocker-Regel geeignet?

Antwort: Die Lösungsvorschläge der Klasse werden unterschiedlich ausfallen.

AppLocker-Regeln

Frage: Wenn Sie AppLocker testen, sollten Sie beim Organisieren von Regeln zwischen verknüpften Gruppenrichtlinienobjekten vorsichtig vorgehen. Was machen Sie, wenn ein Gruppenrichtlinienobjekt die AppLocker-Standardregeln nicht enthält?

Antwort: Wenn ein Gruppenrichtlinienobjekt die Standardregeln nicht enthält, müssen die Regeln dem Gruppenrichtlinienobjekt direkt hinzugefügt werden oder einem Gruppenrichtlinienobjekt hinzugefügt werden, das darauf verweist.

Demo: Erzwingen von AppLocker-Regeln

Frage: Mit welchem Befehl wird die Richtlinie des Computers aktualisiert, und wo wird er ausgeführt?

Antwort: Der Befehl lautet **gpupdate /force** und wird als Administrator an der Eingabeaufforderung ausgeführt.

Was sind Softwarebeschränkungsrichtlinien?

Frage: Warum müssen AppLocker-Regeln in einem Gruppenrichtlinienobjekt separat von SRP-Regeln definiert werden?

Antwort: AppLocker-Regeln sind vollkommen von SRP-Regeln getrennt und können nicht zur Verwaltung von Computern verwendet werden, die Vorgängerversionen von Windows 7 nutzen. Zudem sind die zwei Richtlinien getrennt. Wenn AppLocker-Regeln in einem Gruppenrichtlinienobjekt definiert wurden, werden nur diese Regeln angewendet. Erstellen Sie AppLocker-Regeln deshalb in einem separaten Gruppenrichtlinienobjekt, damit die Interoperabilität zwischen SRP- und AppLocker-Richtlinien gewährleistet wird.

Detaillierte Demoschritte

Demo: Konfigurieren von AppLocker-Regeln

Detaillierte Demoschritte

Erstellen einer neuen ausführbaren Regel

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, geben Sie im Feld **Programme/Dateien durchsuchen** die Zeichenfolge „gpedit.msc“ ein, und drücken Sie dann die EINGABETASTE.
3. Erweitern Sie im **Editor für lokale Gruppenrichtlinien** die Knoten **Computerkonfiguration**, **Windows-Einstellungen** und **Sicherheitseinstellungen**.
4. Erweitern Sie **Anwendungssteuerungsrichtlinien**, und doppelklicken Sie dann auf **AppLocker**.
5. Klicken Sie auf **Ausführbare Regeln**, klicken Sie dann mit der rechten Maustaste, und wählen Sie **Neue Regel erstellen** aus.
6. Klicken Sie auf **Weiter**.
7. Wählen Sie auf der Seite **Berechtigungen** die Option **Verweigern** aus, und klicken Sie dann auf die Schaltfläche **Auswählen....**
8. Geben Sie im Dialogfeld **Gruppe oder Benutzer auswählen** im Feld **Geben Sie die zu verwendenden Objektnamen ein (Beispiele)** den Pfad „Contoso\Marketing“ ein, klicken Sie auf **Namen überprüfen** und dann auf **OK**.
9. Klicken Sie auf **Weiter**.
10. Wählen Sie auf der Seite **Bedingungen** die Option **Pfad** aus, und klicken Sie auf **Weiter**.
11. Klicken Sie auf die Schaltfläche **Dateien durchsuchen...** und dann auf **Lokaler Datenträger (C:)**.
12. Doppelklicken Sie auf **Windows**, wählen Sie **Regedit** aus, und klicken Sie dann auf **Öffnen**.
13. Klicken Sie auf **Weiter**.
14. Klicken Sie erneut auf **Weiter** und dann auf **Erstellen**.
15. Klicken Sie auf **Ja**, wenn Sie zur Erstellung von Standardregeln aufgefordert werden.

Erstellen einer neuen Windows Installer-Regel

1. Wählen Sie **Windows Installer-Regeln** aus, klicken Sie dann mit der rechten Maustaste, und wählen Sie **Neue Regel erstellen** aus.
2. Klicken Sie auf **Weiter**.
3. Klicken Sie auf der Seite **Berechtigungen** auf **Verweigern** und dann auf **Weiter**.
4. Wählen Sie auf der Seite **Bedingungen** die Option **Herausgeber** aus, und klicken Sie auf **Weiter**.
5. Klicken Sie auf die Schaltfläche **Durchsuchen...**, wechseln Sie zu **E:\Labfiles\Mod06**, wählen Sie **Microsoft Artikelerstellungs-Add-In** aus, und klicken Sie dann auf **Öffnen**.

6. Bewegen Sie den Schieberegler auf der Seite **Herausgeber** um drei Stufen nach oben, sodass die Einstellung **Betrifft alle Dateien, die vom angegebenen Herausgeber signiert wurden** für den Regelbereich ausgewählt ist.
7. Klicken Sie auf **Weiter**.
8. Klicken Sie erneut auf **Weiter** und dann auf **Erstellen**.
9. Klicken Sie auf **Ja**, wenn Sie zur Erstellung von Standardregeln aufgefordert werden.

Automatisches Generieren der Skriptregeln

1. Wählen Sie **Skriptregeln** aus, klicken Sie dann mit der rechten Maustaste, und wählen Sie die Option **Regeln automatisch generieren...** aus.
2. Klicken Sie im Bereich **Skriptregeln automatisch generieren** auf der Seite **Ordner und Berechtigungen** auf **Weiter**.
3. Klicken Sie erneut auf **Weiter**.
4. Klicken Sie auf **Erstellen**.
5. Klicken Sie auf **Ja**, wenn Sie zur Erstellung von Standardregeln aufgefordert werden.
6. Schließen Sie den **Editor für lokale Gruppenrichtlinien**, und melden Sie sich dann ab.

Demo: Erzwingen von AppLocker-Regeln

Detaillierte Demoschritte

Erzwingen von AppLocker-Regeln

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, geben Sie im Feld **Programme/Dateien durchsuchen** die Zeichenfolge „gpedit.msc“ ein, und drücken Sie dann die EINGABETASTE.
3. Erweitern Sie im **Editor für lokale Gruppenrichtlinien** die Knoten **Computerkonfiguration**, **Windows-Einstellungen** und **Sicherheitseinstellungen**.
4. Erweitern Sie **Anwendungssteuerungsrichtlinien**.
5. Klicken Sie auf **AppLocker**, und klicken Sie dann mit der rechten Maustaste, und wählen Sie **Eigenschaften** aus.
6. Aktivieren Sie auf der Registerkarte **Erzwingen** unter **Ausführbare Regeln** das Kontrollkästchen **Konfiguriert**, und wählen Sie dann **Regeln erzwingen** aus.
7. Aktivieren Sie auf der Registerkarte **Erzwingen** unter **Windows Installer-Regeln** das Kontrollkästchen **Konfiguriert**, und wählen Sie dann **Nur überwachen** aus.
8. Klicken Sie auf **OK**.
9. Schließen Sie den Editor für lokale Gruppenrichtlinien.

Bestätigen der Erzwingung der ausführbaren Regel

1. Klicken Sie auf **Start**, geben Sie im Dialogfeld **Programme/Dateien durchsuchen** die Zeichenfolge „cmd“ ein, und drücken Sie dann die EINGABETASTE.
2. Geben Sie im Eingabeaufforderungsfenster die Zeichenfolge „gpupdate /force“ ein, und drücken Sie die EINGABETASTE. Warten Sie, bis die Richtlinie aktualisiert wird.
3. Klicken Sie auf **Start**, dann mit der rechten Maustaste auf **Computer**, und klicken Sie nun auf **Verwalten**.
4. Erweitern Sie zunächst **Ereignisanzeige** und dann **Windows-Protokolle**.
5. Klicken Sie auf **System**.
6. Suchen Sie im Ergebnisbereich nach dem letzten Ereignis mit der **Ereignis-ID 1502**, und klicken Sie darauf.
7. Überprüfen Sie die Details der Ereignismeldung auf der Registerkarte **Allgemein**.
8. Erweitern Sie **Dienste und Anwendungen**, und klicken Sie dann auf **Dienste**.
9. Klicken Sie mit der rechten Maustaste im Bereich des Hauptfensters auf den Dienst **Anwendungsidentität**, und klicken Sie dann auf **Start**.
10. Schließen Sie die Eingabeaufforderung.
11. Erweitern Sie in der **Ereignisanzeige** zunächst **Anwendungs- und Dienstprotokolle** und dann **Microsoft**.
12. Erweitern Sie **Windows**, erweitern Sie **AppLocker**, und klicken Sie dann auf **EXE** und **DLL**.
13. Überprüfen Sie die Einträge im Ergebnisbereich.
14. Schließen Sie die Computerverwaltung.
15. Melden Sie sich ab.

Lektion 5

Konfigurieren der Benutzerkontensteuerung

Inhalt:

Fragen und Antworten	120
Detaillierte Demoschritte	121

Fragen und Antworten

Funktionsweise der Benutzerkontensteuerung

Frage: Welche Unterschiede bestehen zwischen einer Zustimmungsaufforderung und einer Anmeldeaufforderung?

Antwort: Eine Zustimmungsaufforderung wird Administratoren angezeigt, wenn sie im Administratorbestätigungsmodus versuchen, eine administrative Aufgabe auszuführen. Sie fordert eine Genehmigung des Benutzers an, um mit der ausgeführten Aufgabe fortzufahren. Eine Anmeldeaufforderung wird Standardbenutzern angezeigt, wenn sie versuchen, eine administrative Aufgabe auszuführen.

Demo: Konfigurieren von Gruppenrichtlinieneinstellungen für die Benutzerkontensteuerung

Frage: Welches Element der Benutzerkontensteuerung erkennt, wenn eine Anwendung in Windows 7 installiert wird?

Antwort: Benutzerkontensteuerung: Anwendungsinstallationen erkennen und erhöhte Rechte anfordern.

Konfigurieren der Benachrichtigungseinstellungen für die Benutzerkontensteuerung

Frage: Welche zwei Konfigurationsoptionen werden kombiniert, um das Verhalten für erhöhte Rechte für Endbenutzer zu bestimmen?

Antwort: Sicherheitseinstellungen für die Benutzerkontensteuerung, die in der lokalen Sicherheitsrichtlinie konfiguriert werden, und Einstellungen zur Benutzerkontensteuerung, die im Wartungscenter in der Systemsteuerung konfiguriert werden.

Detaillierte Demoschritte

Demo: Konfigurieren von Gruppenrichtlinieneinstellungen für die Benutzerkontensteuerung

Detaillierte Demoschritte

Erstellen einer Gruppenrichtlinieneinstellung der Benutzerkontensteuerung zum Verhindern der Zugriffserhöhung

1. Melden Sie sich auf dem virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, geben Sie im Feld **Programme/Dateien durchsuchen** die Zeichenfolge „**gpedit.msc**“ ein, und drücken Sie dann die EINGABETASTE.
3. Erweitern Sie im Editor für lokale Gruppenrichtlinien unter Computerkonfiguration die Knoten **Windows-Einstellungen**, **Sicherheitseinstellungen** und **Lokale Richtlinien**, und klicken Sie dann auf **Sicherheitsoptionen**.
4. Doppelklicken Sie im Ergebnisbereich auf **Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer**.
5. Klicken Sie im Dialogfeld **Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer** auf **Anforderungen für erhöhte Rechte automatisch ablehnen** und dann auf **OK**.
6. Schließen Sie die Konsole **Editor für lokale Gruppenrichtlinien**.
7. Melden Sie sich ab.

Testen der Einstellungen der Benutzerkontensteuerung

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Adam** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, klicken Sie mit der rechten Maustaste auf **Computer**, und klicken Sie dann auf **Verwalten**.
3. Klicken Sie auf **OK**, wenn Sie dazu aufgefordert werden.
4. Melden Sie sich ab.

Erstellen einer Gruppenrichtlinieneinstellung der Benutzerkontensteuerung zum Auffordern der Eingabe von Anmeldeinformationen

1. Melden Sie sich auf dem virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, geben Sie im Feld **Programme/Dateien durchsuchen** die Zeichenfolge „**gpedit.msc**“ ein, und drücken Sie dann die EINGABETASTE.
3. Erweitern Sie im **Editor für lokale Gruppenrichtlinien** unter **Computerkonfiguration** die Knoten **Windows-Einstellungen**, **Sicherheitseinstellungen** und **Lokale Richtlinien**, und klicken Sie dann auf **Sicherheitsoptionen**.
4. Doppelklicken Sie im Ergebnisbereich auf **Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer**.

5. Klicken Sie im Dialogfeld **Benutzerkontensteuerung: Verhalten der Eingabeaufforderung für erhöhte Rechte für Standardbenutzer** auf **Eingabeaufforderung zu Anmeldeinformationen** und dann auf **OK**.
6. Schließen Sie die Konsole **Editor für lokale Gruppenrichtlinien**.
7. Melden Sie sich ab.

Testen der Einstellungen der Benutzerkontensteuerung

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Adam** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, klicken Sie mit der rechten Maustaste auf **Computer**, und klicken Sie dann auf **Verwalten**.
3. Geben Sie im Feld **Benutzername** „Administrator“ ein.
4. Geben Sie im Feld **Kennwort** die Zeichenfolge Pa\$\$w0rd ein.
5. Klicken Sie auf **Ja**.
6. Schließen Sie die Konsole **Computerverwaltung**.
7. Melden Sie sich ab.

Lektion 6

Konfigurieren der Windows-Firewall

Inhalt:

Fragen und Antworten	124
Detaillierte Demoschritte	126

Fragen und Antworten

Diskussion: Was ist eine Firewall?

Frage: Welcher Firewalltyp wird in Ihrem Unternehmen derzeit verwendet?

Antwort: Mehrere Antworten sind möglich.

Frage: Aus welchen Gründen wurde dieser Typ ausgewählt?

Antwort: Mehrere Antworten sind möglich.

Konfigurieren der Basisfirewalleinstellungen

Frage: Listen Sie die drei Netzwerkstandorte auf. Wo ändern Sie sie, und mit welchem Feature von Windows 7 können Sie mehrere davon verwenden?

Antwort: Es gibt folgende drei Netzwerkstandorte:

- **Heim- oder Arbeitsplatznetzwerke (privat):** Für private oder geschäftliche Netzwerke, bei denen die Teilnehmer und Geräte im Netzwerk bekannt und vertrauenswürdig sind. Wenn Heim- oder Arbeitsplatznetzwerke (privat) ausgewählt ist, wird die Netzwerkerkennung aktiviert. Computer in einem Heimnetzwerk können zu einer Heimnetzgruppe gehören.
- **Domänennetzwerke:** Für Netzwerke am Arbeitsplatz, die zu einer Domäne gehören. Wenn diese Option ausgewählt wird, ist die Netzwerkerkennung standardmäßig aktiviert, und Sie können keine Heimnetzgruppen erstellen oder ihnen beitreten.
- **Öffentliche Netzwerke:** Für Netzwerke an öffentlichen Orten. Dieser Standort verhindert, dass der Computer für andere Computer sichtbar ist. Wenn der ausgewählte Netzwerkstandort ein öffentlicher Ort ist, ist die Option Heimnetzgruppe nicht verfügbar, und die Netzwerkerkennung ist deaktiviert.

Sie können die Firewalleinstellungen für jeden Netzwerkstandorttyp auf der **Windows-Firewall**-Hauptseite ändern. Um Netzwerkstandortprofileinstellungen einzurichten oder zu ändern, klicken Sie im linken Bereich des Netzwerk- und Freigabecenters auf **Erweiterte Freigabeeinstellungen ändern**.

Durch mehrere aktive Firewallrichtlinien können Computer Domänenprofilinformationen für die Firewall abrufen und anwenden, unabhängig von den Netzwerken, die auf den Computern aktiv sind.

Windows-Firewall mit erweiterten Sicherheitseinstellungen

Frage: Es gibt drei Typen von Regeln, die in der Windows-Firewall mit erweiterter Sicherheit erstellt werden können. Führen Sie die Typen auf, und geben Sie jeweils die Regeltypen an, die dafür erstellt werden können.

Antwort: Im Folgenden finden Sie die drei Typen mit ihren zugeordneten Typen:

- Eingehende und ausgehende Regeln
 - Programmregeln
 - Portregeln
 - Vordefinierte Regeln
 - Benutzerdefinierte Regeln

- Verbindungssicherheitsregeln
 - **Isolutionsregeln**
 - **Authentifizierungsausnahmeregeln**
 - Server-zu-Server
 - Tunnelregeln
 - **Benutzerdefinierte Regeln**

Bekannte von Anwendungen verwendete Ports

Frage: Welcher TCP-Port wird von einem Webserver für HTTP verwendet?

Antwort: Der TCP-Port ist 80.

Detaillierte Demoschritte

Demo: Konfigurieren von Gruppenrichtlinieneinstellungen für die Benutzerkontensteuerung

Detaillierte Demoschritte

Konfigurieren einer eingehenden Regel

1. Melden Sie sich auf dem virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start** und dann auf **Systemsteuerung**.
3. Klicken Sie auf **System und Sicherheit**.
4. Klicken Sie auf **Windows-Firewall**.
5. Klicken Sie im linken Fensterbereich auf **Erweiterte Einstellungen**.
6. Wählen Sie unter **Windows Firewall mit erweiterter Sicherheit** im linken Bereich **Eingehende Regeln** aus.
7. Überprüfen Sie die vorhandenen eingehenden Regeln, klicken Sie mit der rechten Maustaste auf **Eingehende Regeln**, und klicken Sie dann auf **Neue Regel**.
8. Wählen Sie im **Assistenten für neue eingehende Regeln** auf der Seite **Regeltyp** die Option **Vordefiniert** aus, und wählen Sie dann im Dropdownmenü die Option **Remoteverwaltung geplanter Aufgaben** aus.
9. Klicken Sie auf **Weiter**.
10. Wählen Sie beide Regeln unter **Remoteverwaltung geplanter Aufgaben (RPC)** aus, und klicken Sie auf **Weiter**.
11. Wählen Sie **Verbindung blockieren** aus, und klicken Sie dann auf **Fertig stellen**.

Konfigurieren einer ausgehenden Regel

1. Klicken Sie auf LON-CL1 auf **Start** und dann auf **Alle Programme**.
2. Klicken Sie auf **Internet Explorer**.
3. Wenn Sie im **Assistenten "Willkommen zu Internet Explorer 8"** dazu aufgefordert werden, klicken Sie auf **Später nachfragen**.
4. Geben Sie „http://LON-DC1“ in das **Adressfeld** ein, und drücken Sie die EINGABETASTE, um auf LON-DC1 eine Verbindung mit der Standardwebsite herzustellen.
5. Schließen Sie **Internet Explorer**.
6. Wählen Sie in der Konsole **Windows-Firewall mit erweiterter Sicherheit** im linken Bereich **Ausgehende Regeln** aus.
7. Überprüfen Sie die vorhandenen ausgehenden Regeln, klicken Sie mit der rechten Maustaste auf **Ausgehende Regeln**, und klicken Sie dann auf **Neue Regel**.
8. Wählen Sie im **Assistenten für neue ausgehende Regeln** auf der Seite **Regeltyp** die Option **Port** aus, und klicken Sie dann auf **Weiter**.

9. Wählen Sie **TCP** und anschließend **Bestimmte Remoteports** aus, und geben Sie die Zeichenfolge „80“ ein.
10. Klicken Sie auf **Weiter**.
11. Wählen Sie **Verbindung blockieren**, und klicken Sie dann auf **Weiter**.
12. Klicken Sie auf der Seite **Profil** auf **Weiter**.
13. Geben Sie „HTTP – TCP 80“ im Feld **Name** ein, und klicken Sie dann auf **Fertig stellen**.

Testen der ausgehenden Regel

1. Klicken Sie auf LON-CL1 auf **Start** und dann auf **Alle Programme**.
2. Klicken Sie auf **Internet Explorer**.
3. Geben Sie „http://LON-DC1“ in das **Adressfeld** ein, und drücken Sie die EINGABETASTE, um eine Verbindung mit der Standardwebsite auf LON-DC1 herzustellen.
4. Schließen Sie Internet Explorer.

Erstellen einer Verbindungssicherheitsregel

1. Wählen Sie in der **Windows-Firewall mit erweiterter Sicherheit** im linken Bereich **Verbindungssicherheitsregeln** aus.
2. Klicken Sie mit der rechten Maustaste auf **Verbindungssicherheitsregeln**, und wählen Sie dann die Option **Neue Regel...** aus.
3. Wählen Sie **Server-zu-Server** aus, und klicken Sie dann auf **Weiter**.
4. Klicken Sie auf der Seite **Endpunkte** auf **Weiter**.
5. Wählen Sie **Authentifizierung für eingehende und ausgehende Verbindungen erforderlich** aus, und klicken Sie auf **Weiter**.
6. Wählen Sie **Erweitert** aus, und klicken Sie dann auf die Schaltfläche **Anpassen...**
7. Klicken Sie unter **Erste Authentifizierung** auf die Schaltfläche **Hinzufügen...**
8. Wählen Sie im Dialogfeld **Erste Authentifizierungsmethode hinzufügen** die Option **Computer (Kerberos V5)** aus, und klicken Sie auf **OK**.
9. Klicken Sie unter **Zweite Authentifizierung** auf die Schaltfläche **Hinzufügen...**
10. Wählen Sie im Dialogfeld **Zweite Authentifizierungsmethode hinzufügen** die Option **Benutzer (Kerberos V5)** aus, und klicken Sie dann auf **OK**.
11. Klicken Sie unter **Erweiterte Authentifizierungsmethoden anpassen** auf **OK**.
12. Klicken Sie auf **Weiter** und dann erneut auf **Weiter**.
13. Geben Sie „Verbindungssicherheitsregel für Kerberos“ ein, und klicken Sie dann auf **Fertig stellen**.

Überprüfen der Überwachungseinstellungen der Windows-Firewall

1. Wählen Sie in der **Windows-Firewall mit erweiterter Sicherheit** im linken Bereich **Überwachung** aus.
2. Erweitern Sie **Überwachung**, und wählen Sie dann **Firewall** aus.
3. Klicken Sie auf **Verbindungssicherheitsregeln**.

4. Klicken Sie auf **Sicherheitszuordnungen**.
5. Wählen Sie im linken Bereich **Ausgehende Regeln** aus.
6. Wählen Sie die Regel **HTTP – TCP 80** aus, klicken Sie anschließend mit der rechten Maustaste, und wählen Sie **Regel deaktivieren** aus.
7. Wählen sie **Verbindungssicherheitsregeln** aus.
8. Wählen Sie **Verbindungssicherheitsregel für Kerberos** aus, klicken Sie mit der rechten Maustaste, und klicken Sie dann auf **Regel deaktivieren**.
9. Schließen Sie Windows-Firewall mit erweiterter Sicherheit.
10. Melden Sie sich ab.

Lektion 7

Konfigurieren von Sicherheitseinstellungen in Internet Explorer 8

Inhalt:

Fragen und Antworten	130
Detaillierte Demoschritte	131

Fragen und Antworten

Diskussion: Kompatibilitätsfeatures in Internet Explorer 8

Frage: Mit welchen Kompatibilitätsproblemen rechnen Sie beim Aktualisieren von Internet Explorer?

Antwort: Mehrere Antworten sind möglich.

Verbesserte Datenschutzfeatures in Internet Explorer 8

Frage: Beschreiben Sie den Unterschied zwischen InPrivate-Browsen und InPrivate-Filterung.

Antwort: Mit InPrivate-Browsen werden Daten und Privatsphäre geschützt, indem der Browserverlauf, temporäre Internetdateien, Formulardaten, Cookies, Benutzernamen und Kennwörter vom Browser nicht lokal gespeichert oder beibehalten werden. Mit der InPrivate-Filterung wird die Häufigkeit aller Inhalte von Drittanbietern überwacht, mit der diese auf allen vom Benutzer besuchten Websites angezeigt werden.

Das SmartScreen-Feature in Internet Explorer 8

Frage: Welches Internet Explorer 7-Feature wird durch den SmartScreen-Filter in Internet Explorer 8 ersetzt?

Antwort: Der SmartScreen-Filter ersetzt den Phishingfilter in Internet Explorer 7.

Andere Sicherheitsfeatures in Internet Explorer 8

Frage: Beschreiben Sie, wie der XSS-Filter funktioniert.

Antwort: Der XSS-Filter hat Einblick in alle Anforderungen und Antworten, die über den Browser laufen. Wenn der Filter ein mögliches siteübergreifendes Skript in einer Anforderung erkennt, wird der Angriff identifiziert und neutralisiert, wenn er in der Antwort des Servers wiedergegeben wird. Der XSS-Filter trägt dazu bei, Benutzer vor Sicherheitsrisiken auf Websites zu schützen; er stellt keine schwierigen Fragen, die Benutzer nicht beantworten können und schadet auch nicht der Funktionalität auf der Website.

Detaillierte Demoschritte

Demo: Konfigurieren der Sicherheit in Internet Explorer 8

Detaillierte Demoschritte

Aktivieren der Kompatibilitätsansicht für alle Websites

1. Melden Sie sich auf dem virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf der Taskleiste auf das Symbol **Internet Explorer**.
3. Wenn das Fenster **Windows Internet Explorer 8 einrichten** angezeigt wird, klicken Sie auf **Später nachfragen**.
4. Klicken Sie im Menü **Extras** auf Einstellungen der Kompatibilitätsansicht.
5. Aktivieren Sie das Kontrollkästchen **Alle Websites in Kompatibilitätsansicht anzeigen**, und klicken Sie dann auf **Schließen**.

Löschen des Browserverlaufs

1. Klicken Sie im Menü **Extras** auf **Internetoptionen**.
2. Klicken Sie auf der Registerkarte **Allgemein** unter **Browserverlauf** auf **Löschen**.
3. Wählen Sie **Bevorzugte Websitedaten beibehalten und Verlauf** aus. Deaktivieren Sie alle anderen Optionen.
4. Klicken Sie auf **Löschen**.
5. Klicken Sie auf **OK**, und schließen Sie Internet Explorer.

Konfigurieren von InPrivate-Browsen

1. Klicken Sie auf der Taskleiste von LON-CL1 auf das **Internet Explorer**-Symbol.
2. Geben Sie „http://LON-DC1“ in die Adressleiste ein, und drücken Sie dann die EINGABETASTE.
3. Klicken Sie auf der Adressleiste auf den nach unten weisenden Pfeil, um zu bestätigen, dass die in die Adressleiste eingegebene Adresse gespeichert wurde.
4. Klicken Sie in Internet Explorer auf die Schaltfläche **Extras** und dann auf **Internetoptionen**.
5. Klicken Sie auf die Registerkarte **Allgemein**. Klicken Sie unter **Browserverlauf** auf **Löschen**.
6. Deaktivieren Sie im Dialogfeld **Browserverlauf löschen** die Option **Bevorzugte Websitedaten beibehalten**, aktivieren Sie **Temporäre Internetdateien**, **Cookies** und **Verlauf**, und klicken Sie dann auf **Löschen**.
7. Klicken Sie auf **OK**, um Internetoptionen zu schließen.
8. Vergewissern Sie sich, dass keine Adressen in der Adressleiste gespeichert sind, indem Sie neben der Adressleiste auf den nach unten weisenden Pfeil klicken.
9. Klicken Sie im Menü **Sicherheit** auf **InPrivate-Browsen**.
10. Geben Sie „http://LON-DC1“ in die Adressleiste ein, und drücken Sie dann die EINGABETASTE.

11. Vergewissern Sie sich, dass die eingegebene Adresse nicht gespeichert wurde, indem Sie neben der Adressleiste auf den nach unten weisenden Pfeil klicken.
12. Schließen Sie das Fenster **InPrivate-Browsen**.
13. Schließen Sie Internet Explorer.

Konfigurieren der InPrivate-Filterung

1. Klicken Sie auf der Taskleiste auf das Symbol **Internet Explorer**.
2. Klicken Sie im Menü **Sicherheit** auf **InPrivate-Filterung**.
3. Klicken Sie auf **Auswählen, welche Anbieter Informationen erhalten**, um die Inhalte auszuwählen, die blockiert oder zugelassen werden sollen.
4. Klicken Sie im Fenster **Einstellungen der InPrivate-Filterung** auf **Automatisch blocken**.
5. Klicken Sie auf **OK**.

Anzeigen der Add-On-Verwaltungsoberfläche

1. Klicken Sie im Menü **Extras** auf **Add-Ons verwalten**.
2. Stellen Sie sicher, dass **Symbolleisten und Erweiterungen** aktiviert ist, und klicken Sie auf **Recherchieren**.
3. Klicken Sie auf **Suchanbieter**.
4. Klicken Sie auf **Bing**.
5. Klicken Sie auf **Schnellinfos**.
6. Führen Sie einen Bildlauf nach unten durch, um alle verfügbaren Schnellinfos anzuzeigen.
7. Klicken Sie auf **InPrivate-Filterung**.
8. Klicken Sie auf **Schließen**.
9. Schließen Sie Internet Explorer, und melden Sie sich ab.

Lektion 8

Konfigurieren von Windows Defender

Inhalt:

Fragen und Antworten	134
Detaillierte Demoschritte	135

Fragen und Antworten

Was ist Malware?

Frage: Welche allgemeinen Sicherheitsrisiken müssen bei der Bereitstellung eines neuen Betriebssystems berücksichtigt werden?

Antwort: Während einer Desktopbereitstellung muss auf alle Sicherheitsrisiken eingegangen werden, die sich auf Anwendungscompatibilität, Datenverluste und Benutzerfunktionalität auswirken. Einige der häufiger auftretenden Sicherheitsrisiken werden folgendermaßen kategorisiert:

- Malwarerisiken: Viren, Trojanische Pferde, Spyware
- Datenrisiken: Diebstahl von Laptops oder USB-Wechselfestplatten
- Webbrowserrisiken: Schädliche Websites, Phishing
- Netzwerkrisiken: Interne Wurmangriffe, interne Arbeitsstationen, die nicht den Sicherheitsrichtlinien der Organisation entsprechen

Frage: Wie können Sie sicherstellen, dass Sie vor und nach der Desktopbereitstellung auf einschlägige Sicherheitsrisiken eingegangen sind?

Antwort: Halten Sie sich an ein strukturiertes Verfahren für das Sicherheitsrisikomanagement. Sie können dadurch Risiken genauer erkennen und einschätzen, Kontrollmechanismen identifizieren und bewerten, geeignete Kontrollmechanismen implementieren und die Effektivität der Schadensbegrenzung quantifizieren. Wenn Sicherheitsrisiken vor der Desktopbereitstellung identifiziert werden, können Sie vorausschauend Maßnahmen zur Schadensbegrenzung ergreifen und Lösungen implementieren.

Was ist Windows Defender?

Frage: Nennen Sie die vier Warnstufen von Windows Defender. Was sind die möglichen Antworten?

Antwort: Die vier Warnstufen lauten „Schwerwiegend“, „Hoch“, „Mittel“ und „Niedrig“. Mögliche Antworten sind „Quarantäne“, „Entfernen“ und „Zulassen“. Für potenzielle Änderungen an Windows-Einstellungen lauten die möglichen Antworten „Genehmigen“ und „Verweigern“.

Scanoptionen in Windows Defender

Frage: Warum sollten Sie einen Wiederherstellungspunkt erstellen, bevor Sie Aktionen für erkannte Elemente anwenden?

Antwort: Da Windows Defender so eingerichtet werden kann, dass erkannte Elemente automatisch entfernt werden, können Sie mit dieser Option Systemeinstellungen wiederherstellen, wenn Sie Software verwenden möchten, die unbeabsichtigt gelöscht wurde.

Detaillierte Demoschritte

Demo: Konfigurieren der Windows Defender-Einstellungen

Detaillierte Demoschritte

Festlegen von Windows Defender-Optionen

1. Melden Sie sich auf dem virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, klicken Sie auf **Programme/Dateien durchsuchen**, geben Sie „Windows Defender“ ein, und drücken Sie die EINGABETASTE.
3. Klicken Sie im Menü von **Windows Defender** auf **Extras**.
4. Klicken Sie unter **Einstellungen und Extras** auf **Optionen**.
5. Wählen Sie unter **Optionen** die Option **Automatische Überprüfung** aus.
6. Stellen Sie im Hauptfenster sicher, dass das Kontrollkästchen **Computer automatisch überprüfen (empfohlen)** aktiviert ist.
7. Legen Sie die **Häufigkeit** auf **Montag** fest.
8. Legen Sie die **Geschätzte Zeit** auf **06:00:00** Uhr fest.
9. Legen Sie den **Typ** auf **Schnellüberprüfung** fest.
10. Vergewissern Sie sich, dass das Kontrollkästchen **Vor Überprüfung nach aktualisierten Signaturen suchen** aktiviert ist.
11. Wählen Sie unter **Optionen** die Option **Standardaktionen** aus.
12. Legen Sie für **Elemente der Warnstufe "Schwerwiegend"** die Einstellung **Entfernen** fest.
13. Legen Sie für **Elemente der Warnstufe "Niedrig"** die Einstellung **Zulassen** fest.
14. Stellen Sie sicher, dass das Kontrollkästchen **Empfohlene Aktionen anwenden** aktiviert ist.
15. Wählen Sie unter **Optionen** die Option **Echtzeitschutz** aus.
16. Wählen Sie unter **Optionen** die Option **Ausgeschlossene Dateien und Ordner** aus.
17. Wählen Sie unter **Optionen** die Option **Ausgeschlossene Dateitypen** aus.
18. Wählen Sie unter **Optionen** die Option **Erweitert** aus.
19. Klicken Sie auf **E-Mail überprüfen**.
20. Klicken Sie auf **Wechseldatenträger überprüfen**.
21. Wählen Sie unter **Optionen** die Option **Administrator** aus.
22. Klicken Sie auf **Speichern**.

Anzeigen von Quarantäneelementen

1. Klicken Sie in **Einstellungen und Extras** auf **Unter Quarantäne**.
2. Klicken Sie auf **Anzeigen**.
3. Klicken Sie in der oberen Menüleiste auf den Zurück-Pfeil.

Microsoft SpyNet

1. Klicken Sie unter Einstellungen und Extras auf **Microsoft SpyNet**.
2. Wählen Sie **Einfaches Mitglied werden** aus.
3. Klicken Sie auf **Speichern**.

Windows Defender-Website

1. Verweisen Sie in Einstellungen und Extras auf den Link **Windows Defender-Website**.
2. Besprechen Sie die Inhalte der Windows Defender-Website.

Lernzielkontrollen und Kernpunkte der Unterrichtseinheit

Fragen zur Lernzielkontrolle

Frage 1: Was geschieht bei Standardbenutzern und Administratoren, wenn die Benutzerkontensteuerung implementiert ist und eine Aufgabe ausgeführt wird, für die Administratorrechte erforderlich sind?

Antwort: Standardbenutzer werden von der UAC aufgefordert, Anmeldeinformationen eines Benutzers mit Administratorrechten anzugeben. Bei Administratoren fordert UAC den Benutzer auf, die Berechtigung zum Ausführen der Aufgabe anzugeben.

Frage 2: Unter welchen Voraussetzungen kann Windows BitLocker eigene Schlüssel für die Verschlüsselung und Entschlüsselung auf einem Hardwaregerät speichern, das von der Festplatte getrennt ist?

Antwort: Ein Computer mit einem TPM (Trusted Platform Module) oder einem USB-Wechselspeichergerät (USB), z. B. einem USB-Flashlaufwerk. Wenn der Computer nicht über ein TPM ab Version 1.2 verfügt, wird der Schlüssel von BitLocker auf dem Speichergerät gespeichert.

Frage 3: Was müssen Sie beim Implementieren von Windows AppLocker tun, bevor Sie neue Regeln manuell erstellen oder für bestimmte Ordner automatisch generieren?

Antwort: Erstellen der Standardregeln

Frage 4: Sie entscheiden sich, die Messaginganwendung eines Drittanbieters auf den Laptops des Unternehmens bereitzustellen. Diese Anwendung verwendet POP3, um E-Mails vom E-Mail-Server des Unternehmens abzurufen, und SMTP, um E-Mails an das E-Mail-Relay des Unternehmens zu senden. Welche Ports müssen in der Windows-Firewall geöffnet werden?

Antwort: Sie müssen eingehendes POP3, für das TCP-Port 110 verwendet wird, und ausgehendes SMTP, für das TCP-Port 25 verwendet wird, aktivieren. Sie können die Firewallregeln mit konkreten Portzuweisungen oder durch Angabe des Programms konfigurieren.

Frage 5: Beschreiben Sie, wie der SmartScreen-Filter in Internet Explorer 8 funktioniert.

Antwort: Bei aktiviertem SmartScreen-Filter führt Internet Explorer 8 eine ausführliche Prüfung der gesamten URL-Zeichenfolge aus und vergleicht die Zeichenfolge mit einer Datenbank von Websites, die für die Weitergabe von Schadsoftware bekannt sind. Wenn die Website als unsicher gilt, wird sie blockiert, und der Benutzer wird mit einer auffälligen SmartScreen-Blockierungsseite benachrichtigt, auf der eine leicht verständliche Anleitung zum Schutz vor als unsicher bekannten Websites angezeigt wird.

Frage 6: Was macht Windows Defender mit Software, die in die Quarantäne verschoben wird?

Antwort: Windows Defender verschiebt die Software an einen anderen Speicherort auf dem Computer und verhindert dann die Ausführung der Software, bis Sie entscheiden, ob sie wiederhergestellt oder vom Computer entfernt werden soll.

Frage 7: Welche Konfigurationsoptionen sind in Windows Defender verfügbar, wo legen Sie sie fest, und zu welchem Zweck?

Antwort: Aktivieren Sie den Windows Defender-Echtzeitschutz, und wählen Sie alle Echtzeitschutzoptionen aus, um das Ausführen von Spyware und anderer unerwünschte Software auf dem Computer zu verhindern. Sie werden gewarnt, wenn Programme Installationsversuche durchführen, auf dem Computer ausgeführt werden oder wichtige Windows-Einstellungen ändern.

Aktivieren Sie den Echtzeitschutz, indem Sie auf **Extras**, auf **Optionen** und dann auf **Echtzeitschutz** klicken. Führen Sie im Bereich **Optionen** die folgenden zusätzlichen Aufgaben aus:

- Konfigurieren Sie die automatische Überprüfung.
- Geben Sie Standardaktionen für bestimmte Warnstufen an.
- Passen Sie eine Überprüfung durch Ausschließen von Dateien, Ordnern und Dateitypen an.
- Verwenden Sie **Erweiterte Optionen**, um archivierte Dateien, E-Mails und Wechseldatenträger zu überprüfen, Heuristiken zu verwenden und einen Wiederherstellungspunkt zu erstellen.

Wählen Sie aus, ob Windows Defender verwendet werden soll und welche Informationen für alle Benutzer des Computers angezeigt werden sollen. Verlauf, zugelassene Elemente und Quarantäneelemente werden standardmäßig ausgeblendet, um die Privatsphäre der Benutzer zu schützen.

Praxisnahe Probleme und Szenarios

Frage 1: Ein Administrator konfiguriert Gruppenrichtlinien, damit Daten nur auf von BitLocker geschützten Datenvolumen gespeichert werden können. Insbesondere aktiviert der Administrator die Richtlinie **Schreibzugriff auf Wechseldatenträger verweigern, die nicht durch BitLocker geschützt sind** und stellt diese in der Domäne bereit. Daraufhin schließt ein Endbenutzer ein USB-Flashlaufwerk an, das nicht mit BitLocker geschützt ist. Was geschieht, und wie kann der Benutzer die Situation auflösen?

Antwort: Da das USB-Flashlaufwerk nicht durch BitLocker geschützt wird, zeigt Windows 7 in einem Informationsdialogfeld an, dass das Gerät mit BitLocker verschlüsselt werden muss. In diesem Dialogfeld kann der Benutzer entweder den BitLocker-Assistenten starten, um das Volume zu verschlüsseln, oder das Gerät weiterhin schreibgeschützt verwenden.

Frage 2: Trevor hat Windows AppLocker implementiert. Vor der Erstellung der Standardregeln hat er eine benutzerdefinierte Regel erstellt, durch die alle Windows-Prozesse mit Ausnahme von Regedit.exe ausgeführt werden dürfen. Da er die Standardregeln nicht zuerst erstellt hat, wird er für das Durchführen von Verwaltungsaufgaben blockiert. Wie kann er das Problem beheben?

Antwort: Trevor muss den Computer im abgesicherten Modus neu starten, die Standardregeln hinzufügen, alle Ablehnungsregeln löschen, die den Zugriff verhindern, und anschließend die Computerrichtlinie aktualisieren.

Frage 3: Ein Server verfügt über mehrere Netzwerkschnittstellenkarten (Network Interface Cards, NICs), eine der NICs ist jedoch nicht verbunden. In Windows Vista blieb der Computer dadurch im öffentlichen Profil hängen (die restriktivste Regel). Wie wird dieses Problem in Windows 7 gelöst?

Antwort: Das neue Feature für mehrere aktive Firewallprofile in Windows 7 löst das Problem, indem die entsprechenden Regeln auf das entsprechende Netzwerk angewendet werden. In diesem Fall wird das Profil angewendet, das der verbundenen NIC zugeordnet ist.

Häufige Probleme in Bezug auf Internet Explorer 8-Sicherheitseinstellungen

IT-Fachleute müssen sich mit den allgemeinen Problemen in Bezug auf Internet Explorer 8-Sicherheitseinstellungen vertraut machen.

Schaltfläche „Diagnose von Verbindungsproblemen“

Mit der Schaltfläche Diagnose von Verbindungsproblemen können Benutzer Probleme identifizieren und lösen, möglicherweise ohne das Helpdesk in Anspruch zu nehmen. Wenn Internet Explorer 8 mit einer Website keine Verbindung herstellen kann, wird die Schaltfläche Diagnose von Verbindungsproblemen angezeigt. Durch Klicken auf die Schaltfläche können Benutzer das Problem anhand von Informationen zur Fehlerbehebung lösen. Diese Option war in Internet Explorer 7 bereits verfügbar, sie ist in Internet Explorer 8 jedoch einfacher zu finden.

Zurücksetzen der Internet Explorer 8-Einstellungen

Wenn sich Internet Explorer 8 auf dem Computer eines Benutzers in einem instabilen Zustand befindet, können Sie mit der Funktion „Internet Explorer-Einstellungen zurücksetzen“ die Standardeinstellungen vieler Browserfunktionen wiederherstellen. Zu diesen zählen beispielsweise:

- Suchbereiche
- Darstellungseinstellungen
- Symbolleisten
- ActiveX-Steuerelemente (Zurücksetzen in den Anmeldezustand, bis sie erneut genehmigt werden)
- Mit IEAK 8 erstellte Brandingeinstellungen

Sie können persönliche Einstellungen mit der Option „Persönliche Einstellungen löschen“ für folgende Elemente zurückzusetzen:

- Startseiten
- Browserverlauf
- Formulardaten
- Kennwörter

Mit „Internet Explorer-Einstellungen zurücksetzen“ werden alle benutzerdefinierten Symbolleisten, Browsererweiterungen und Anpassungen deaktiviert, die in Internet Explorer 8 installiert wurden. Um diese deaktivierten Anpassungen zu verwenden, müssen sie einzeln über das Dialogfeld „Add-Ons verwalten“ aktiviert werden.

Folgendes wird durch „Internet Explorer-Einstellungen zurücksetzen“ nicht durchgeführt:

- Löschen der Favoritenliste
- Löschen der RSS-Feeds
- Löschen der Web Slices
- Zurücksetzen von Verbindungs- oder Proxyeinstellungen
- Beeinflussen von angewendeten Gruppenrichtlinieneinstellungen für administrative Vorlagen

Hinweis: Wenn Sie die Gruppenrichtlinieneinstellung mit dem Namen „Verarbeitung der Richtlinie für die Internet Explorer-Wartung“ nicht aktivieren, gehen Einstellungen des Browsers im Modus Normal, die mit der Internet Explorer-Wartung erstellt wurden, mit der Verwendung von Internet Explorer-Einstellungen zurücksetzen verloren.

Um „Internet Explorer-Einstellungen zurücksetzen“ in Internet Explorer 8 zu verwenden, führen Sie folgende Schritte aus:

1. Klicken Sie im Menü **Extras** auf **Internetoptionen**.
2. Klicken Sie auf der Registerkarte **Erweitert** auf **Zurücksetzen**.
3. Klicken Sie im Dialogfeld **Internet Explorer-Einstellungen zurücksetzen** auf **Zurücksetzen**. Um persönliche Einstellungen zu entfernen, aktivieren Sie das Kontrollkästchen **Persönliche Einstellungen löschen**. Um Branding zu entfernen, aktivieren Sie das Kontrollkästchen **Branding entfernen**.
4. Klicken Sie auf **Schließen** und dann zweimal auf **OK**, nachdem Internet Explorer 8 das Wiederherstellen der Standardeinstellungen abgeschlossen hat.
5. Schließen Sie Internet Explorer 8. Die Änderungen werden beim nächsten Öffnen von Internet Explorer 8 wirksam.

Hinweis: Um zu verhindern, dass Benutzer die Funktion „Internet Explorer-Einstellungen zurücksetzen“ verwenden, aktivieren Sie die Richtlinie **Zurücksetzen von Internet Explorer-Einstellungen nicht zulassen** in den administrativen Vorlagen für Gruppenrichtlinien.

Best Practices für die Benutzerkontensteuerung

- Die Sicherheitseinstellungen der Benutzerkontensteuerung können im lokalen Sicherheitsrichtlinien-Manager (secpol.msc) oder im Editor für lokale Gruppenrichtlinien (gpedit.msc) konfiguriert werden. In den meisten Unternehmensumgebungen werden jedoch Gruppenrichtlinien bevorzugt, da sie zentral verwaltet und gesteuert werden können. Es gibt neun Gruppenrichtlinienobjekteinstellungen, die für die Benutzerkontensteuerung konfiguriert werden können.
- Da das vom Benutzer wahrgenommene Verhalten mit Gruppenrichtlinien konfiguriert werden kann, kann dies, je nach Richtlinieneinstellungen, sehr unterschiedlich sein. Die in der Umgebung getroffenen Konfigurationsentscheidungen beeinflussen die Eingabeaufforderungen und Dialogfelder, die Standardbenutzer, Administratoren oder beide anzeigen können.

Sie können z. B. Administratorberechtigungen anfordern, um die Einstellung der Benutzerkontensteuerung in „Immer benachrichtigen“ oder „Die Benutzerkontensteuerung sendet immer eine Benachrichtigung, und es wird auf eine Antwort gewartet“ zu ändern. Bei diesem Konfigurationstyp wird am unteren Rand der Seite mit den „Einstellungen der Benutzerkontensteuerung“ eine gelbe Benachrichtigung mit der Anforderung angezeigt.

Best Practices für Windows BitLocker

- Da BitLocker seine eigenen Verschlüsselungs- und Entschlüsselungsschlüssel auf einem Hardwaregerät speichert, das von der Festplatte getrennt ist, müssen Sie über eines der folgenden Geräte verfügen:

- Ein Computer mit TPM (Trusted Platform Module)
- Ein USB (Universal Serial Bus)-Wechselspeichergerät, z. B. ein USB-Flashlaufwerk. Wenn der Computer nicht über ein TPM ab Version 1.2 verfügt, wird der Schlüssel von BitLocker auf dem Speichergerät gespeichert.
- Die sicherste Implementierung von BitLocker nutzt die verbesserten Sicherheitsfunktionen des TPM (Trusted Platform Module) Version 1.2.
- Auf Computern ohne TPM Version 1.2 können Sie BitLocker dennoch zum Verschlüsseln des Windows-Betriebssystemvolumens verwenden. Bei dieser Implementierung muss der Benutzer jedoch einen USB-Systemstartschlüssel anschließen, um den Computer zu starten oder den Ruhezustand zu beenden. Außerdem ist die Überprüfung der Systemintegrität vor dem Start nicht möglich, die von BitLocker in Verbindung mit einem TPM bereitgestellt wird.

Best Practices für Windows AppLocker

- Erstellen Sie die Standardregeln, bevor Sie neue Regeln manuell erstellen oder Regeln für einen bestimmten Ordner automatisch generieren. Mit Standardregeln wird sichergestellt, dass wichtige Betriebssystemdateien für alle Benutzer ausgeführt werden können.
- Wenn Sie AppLocker testen, sollten Sie beim Organisieren von Regeln zwischen verknüpften Gruppenrichtlinienobjekten vorsichtig vorgehen. Wenn ein Gruppenrichtlinienobjekt die Standardregeln nicht enthält, müssen die Regeln dem Gruppenrichtlinienobjekt direkt hinzugefügt werden oder einem Gruppenrichtlinienobjekt hinzugefügt werden, das darauf verweist.
- Nach dem Erstellen neuer Regeln müssen die Erzwingung für die Regelsammlungen konfiguriert und die Richtlinie des Computers aktualisiert werden.
- In der Standardeinstellung der AppLocker-Regeln können Benutzer keine Dateien öffnen oder ausführen, die nicht ausdrücklich zugelassen sind. Administratoren müssen eine aktuelle Liste zulässiger Anwendungen verwalten.
- Wenn AppLocker-Regeln in einem Gruppenrichtlinienobjekt definiert werden, werden nur diese Regeln angewendet. Um die Interoperabilität zwischen Regeln der Richtlinien für Softwareeinschränkung und AppLocker-Regeln sicherzustellen, sollten Sie Regeln der Richtlinien für Softwareeinschränkung und AppLocker-Regeln in unterschiedlichen Gruppenrichtlinienobjekten definieren.
- Wird eine AppLocker-Regel auf Nur überwachen festgelegt, wird die Regel nicht erzwungen. Wenn ein Benutzer eine Anwendung ausführt, die in der Regel enthalten ist, wird die Anwendung geöffnet und normal ausgeführt, und dem AppLocker-Ereignisprotokoll werden Informationen zu dieser Anwendung hinzugefügt.
- Mindestens ein Windows Server 2008 R2-Domänencontroller ist zum Hosten der AppLocker-Regeln erforderlich.

Best Practices für Windows Defender

- Für die Verwendung von Windows Defender müssen aktuelle Definitionen vorhanden sein.
 - Um die Definitionen auf dem neuesten Stand zu halten, installiert Windows Defender mit Windows Update automatisch neue Definitionen bei deren Veröffentlichung. Sie können Windows Defender auch so einrichten, dass vor dem Überprüfen online nach aktualisierten Definitionen gesucht wird.

- Beim Überprüfen des Computers wird empfohlen, die erweiterte Option **Einen Wiederherstellungspunkt erstellen, bevor Aktionen auf gefundene Elemente angewendet werden** auszuwählen. Da Sie Windows Defender so einrichten können, dass erkannte Elemente automatisch entfernt werden, können Sie mit dieser Option Systemeinstellungen wiederherstellen, wenn Sie Software verwenden möchten, die unbeabsichtigt gelöscht wurde.

Best Practices für EFS (Encrypting File System, Verschlüsselndes Dateisystem)

Nachfolgend sind die Best Practices für EFS-Benutzer aufgeführt:

- Benutzer sollten ihre Zertifikate und privaten Schlüssel auf Wechselmedien exportieren und diese sicher lagern. Für größtmögliche Sicherheit muss der private Schlüssel immer vom Computer entfernt werden, wenn dieser nicht in Verwendung ist. Dies schützt vor Angreifern, die in physischen Besitz des Computers gelangen und versuchen, auf den privaten Schlüssel zuzugreifen. Wenn auf die verschlüsselten Dateien zugegriffen werden muss, kann der private Schlüssel einfach von den Wechselmedien importiert werden.
- Verschlüsseln Sie den Ordner „Eigene Dokumente“ für alle Benutzer (BenutzerprofilDokumente). Dadurch wird sichergestellt, dass der persönliche Ordner, in dem die meisten Dokumente gespeichert werden, standardmäßig verschlüsselt wird.
- Benutzer sollten Ordner anstelle einzelner Dateien verschlüsseln. Programme arbeiten auf verschiedene Arten mit Dateien. Durch konsistente Verschlüsselung auf Ordnersebene wird sichergestellt, dass Dateien nicht unbeabsichtigt entschlüsselt werden.
- Die privaten Schlüssel, die Wiederherstellungszertifikaten zugeordnet werden, sind äußerst vertraulich. Diese Schlüssel müssen entweder auf einem physisch gesicherten Computer generiert werden, oder die zugehörigen Zertifikate müssen in eine PFX-Datei exportiert werden, die mit einem sicheren Kennwort geschützt und auf einem Datenträger gespeichert wird, der an einem physisch sicheren Ort gelagert wird.
- Zertifikate des Wiederherstellungs-Agents müssen speziellen Wiederherstellungs-Agentkonten zugewiesen werden, die für keinen anderen Zweck verwendet werden.
- Vernichten Sie Wiederherstellungszertifikate oder private Schlüssel nicht, wenn Wiederherstellungs-Agents geändert werden. (Agents werden in regelmäßigen Abständen geändert.) Bewahren Sie sie so lange auf, bis alle Dateien, die möglicherweise mit ihnen verschlüsselt wurden, aktualisiert sind.
- Legen Sie je nach Größe der Organisationseinheiten zwei oder mehr Wiederherstellungs-Agentkonten pro Organisationseinheit fest. Legen Sie zwei oder mehr Computer zur Wiederherstellung fest, einen für jedes zugewiesene Wiederherstellungs-Agentkonto. Gewähren Sie verantwortungsvollen Administratoren die Berechtigungen zur Verwendung der Wiederherstellungs-Agentkonten. Für die Redundanz bei der Dateiwiederherstellung wird empfohlen, zwei Wiederherstellungs-Agentkonten zu verwalten. Zwei Computer, auf denen diese Schlüssel gespeichert sind, bieten mehr Redundanz, um die Wiederherstellung verlorener Daten zu ermöglichen.
- Implementieren Sie ein Archivprogramm für Wiederherstellungs-Agents, um sicherzustellen, dass verschlüsselte Dateien mit älteren Wiederherstellungsschlüsseln wiederhergestellt werden können. Die Wiederherstellungszertifikate und privaten Schlüssel müssen exportiert und auf kontrollierte, sichere Art gespeichert werden. Idealerweise sollten die Archive wie alle sicheren Daten an einem Ort mit kontrolliertem Zugang gelagert werden, und es müssen zwei Archive vorhanden sein: Master und Sicherung. Das Masterarchiv wird vor Ort gelagert, während sich das Sicherungsarchiv an einem gesicherten externen Standort befindet.

- Vermeiden Sie die Verwendung von Druckspooldateien in der Druckserverarchitektur, oder stellen Sie sicher, dass Druckspooldateien in einem verschlüsselten Ordner generiert werden.
- Das verschlüsselnde Dateisystem beansprucht bei jedem Verschlüsseln und Entschlüsseln einer Datei durch einen Benutzer einen Teil der CPU. Teilen Sie die Servernutzung ein. Stellen Sie einen Lastenausgleich für die Server bereit, wenn viele Clients EFS verwenden.

Konfigurationsrichtlinien für die Windows-Firewall mit erweiterter Sicherheit

- Sie können die Windows-Firewall mit erweiterter Sicherheit auf folgende Arten konfigurieren:
 - Konfigurieren Sie einen lokalen Computer oder Remotecomputer mit dem Snap-In „Windows-Firewall mit erweiterter Sicherheit“ oder dem Befehl „Netsh advfirewall“.
 - Konfigurieren Sie die Einstellungen der Windows-Firewall mit erweiterter Sicherheit mit der Gruppenrichtlinien-Verwaltungskonsolle (GPMC) oder dem Befehl „Netsh advfirewall“.
 - Wenn Sie die Firewall mithilfe von Gruppenrichtlinien konfigurieren, muss sichergestellt werden, dass der Windows-Firewalldienst durch die SID (Service Security Identifier) über expliziten Schreibzugriff auf den angegebenen Speicherort verfügt.
 - Wenn Sie die Windows-Firewall mit erweiterter Sicherheit mithilfe von Gruppenrichtlinien bereitstellen und anschließend ausgehende Verbindungen blockieren, muss sichergestellt werden, dass die ausgehenden Regeln der Gruppenrichtlinie aktiviert sind. Führen Sie außerdem vor der Bereitstellung umfangreiche Tests in einer Testumgebung durch. Andernfalls verhindern Sie u. U., dass sämtliche Computer, die die Richtlinie erhalten, diese zu einem späteren Zeitpunkt aktualisieren, wenn Sie nicht manuell eingreifen.

Ressourcen für Internet Explorer 8

Verwenden Sie bei Bedarf die folgenden Informationen:

- Weitere Informationen zu IANA-Standards für die Portzuweisung finden Sie auf der [IANA-Website](#)
- [Übersicht über die Windows Internet Explorer 8-Technologie für Enterprise- und IT-Experten](#)
- [Internet Explorer 8-Supportseite](#)
- [Internet Explorer 8: Startseite](#)
- [Häufig gestellte Fragen zu Internet Explorer 8](#)
- [Internet Explorer 8-Newsgroups](#)
- [Internet Explorer 8-Forum auf TechNet](#)
- [Internet Explorer 8: Hilfe und Support](#)
- [Das neue Toolkit für Anwendungskompatibilität mit Unterstützung für Internet Explorer 8 ist auf MSDN verfügbar.](#)
- [Dem Toolkit für Anwendungskompatibilität liegt ein Whitepaper bei, in dem die vom Tool identifizierten Kompatibilitätsprobleme erläutert werden.](#)
- [Informationen zu Antiphishing-Strategien](#)
- [Informationen zum RIES-Feature](#)
- [Internet Explorer Anwendungskompatibilität](#)

Fragen und Antworten zur Lernzielkontrolle

Frage: Wie lauten die Arten von Regeln, die Sie für die Windows-Firewall konfigurieren können?

Antwort: Sie können eingehende und ausgehende Firewallregeln auf der Grundlage von Verbindungen mit einem Programm oder einem TCP/UDP-Port erstellen, sowie vordefinierte und benutzerdefinierte Regeln.

Frage: Wie lauten einige neue Sicherheitseinstellungen in Internet Explorer 8?

Antwort: Zu den neuen Sicherheitseinstellungen in Internet Explorer 8 gehören die Kompatibilitätsansicht, InPrivate-Browsen und InPrivate-Filterung.

Frage: Lassen die Standardeinstellungen für Windows Defender die Überprüfung auf neue Definitionen, die regelmäßige Überprüfung auf Spyware und andere potenziell unerwünschte Software zu?

Antwort: Ja, Windows Defender ist in den Standardeinstellungen für die Überprüfung auf neue Definitionen und zur Durchführung regelmäßiger Scans konfiguriert. Sie haben die Möglichkeit, bei Bedarf eigene Einstellungen zu konfigurieren.

Frage: Welche Überprüfungen kann Windows Defender zur Erkennung böswilliger und unerwünschter Software durchführen?

Antwort: Windows Defender kann zur Überprüfung von E-Mails, Archiven, komprimierten Dateien und dem Inhalt von Wechsellaufwerken verwendet werden.

Unterrichtseinheit 7

Optimieren und Warten von Windows 7-Clientcomputern

Inhalt:

Lektion 1: Gewährleisten der Systemleistung mithilfe der Windows 7-Tools zur Leistungsüberwachung	146
Lektion 2: Gewährleisten der Zuverlässigkeit mit den Windows 7-Diagnosetools	151
Lektion 3: Sichern und Wiederherstellen von Daten mit der Windows-Sicherung	154
Lektion 4: Wiederherstellen eines Windows 7-Systems mit Systemwiederherstellungspunkten	158
Lektion 5: Konfigurieren von Windows Update	162
Lernzielkontrollen und Kernpunkte der Unterrichtseinheit	164
Fragen und Antworten zur Lernzielkontrolle	166

Lektion 1

Gewährleisten der Systemleistung mithilfe der Windows 7-Leistungstools

Inhalt:

Fragen und Antworten	147
Detaillierte Demoschritte	148

Fragen und Antworten

Leistungsüberwachung und Sammlungssätze

Frage: Welche Ressourcen können zu Leistungsproblemen führen, wenn sie nicht ausreichend vorhanden sind?

Antwort: CPU, Arbeitsspeicher (RAM), Datenträger und Netzwerk.

Demo: Verwenden des Ressourcenmonitors

Frage: Wie können Sie die Überwachungsaktivitäten für einen Prozess vereinfachen, der sich über mehrere Registerkarten erstreckt?

Antwort: Wenn Sie das Kontrollkästchen für einen Prozess aktivieren, befindet sich dieser Prozess oben in der Liste, wenn Sie die Registerkarten wechseln. Dadurch können Sie verschiedene Eigenschaften eines bestimmten Prozesses anzeigen. Dies kann nützlich sein, wenn Sie eine Ressource suchen, die einen Leistungsengpass für einen Prozess darstellt.

Demo: Analysieren der Systemleistung mithilfe von Sammlungssätzen und der Leistungsüberwachung

Frage: Wie kann die Leistungsüberwachung zur Problembehandlung verwendet werden?

Antwort: Mithilfe der Leistungsüberwachung können Sie Ressourcen überwachen, wenn beim Ausführen einer Anwendung Probleme auftreten. Wenn ein Problem zu einem bestimmten Zeitpunkt auftritt, können Sie die Ausführung des Sammlungssatzes so planen, dass sie zu dieser Zeit stattfindet und weitere Informationen zur Ressourcenverwendung gesammelt werden, während das Problem auftritt.

Detaillierte Demoschritte

Demo: Verwenden des Ressourcenmonitors

Detaillierte Demoschritte

In dieser Demo wird die Verwendung des Ressourcenmonitors erläutert.

Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.

1. Klicken Sie auf **Start**. Geben Sie im Suchfeld „res“ ein, und klicken Sie dann auf **Ressourcenmonitor**. Auf der Registerkarte **Übersicht** werden für jeden Prozess Informationen zu CPU-Auslastung, Datenträger-E/A, Netzwerkverwendung und Speicherauslastung angezeigt. Zusammenfassungsinformationen werden in einer Leiste oberhalb der einzelnen Abschnitte angezeigt.
2. Klicken Sie im Abschnitt **Datenträger** auf den Pfeil nach unten, um ihn zu erweitern.
3. Klicken Sie auf die Schaltfläche **Ansichten** und anschließend auf **Mittel**. Dadurch wird die Größe der Diagramme gesteuert, in denen CPU-Auslastung, Datenträger-E/A, Netzwerkverwendung und Arbeitsspeicheraktivität angezeigt werden.
4. Klicken Sie auf die Registerkarte **CPU**. Auf dieser Registerkarte werden ausführlichere CPU-Informationen aufgeführt, die nach Prozess gefiltert werden können.
5. Aktivieren Sie im Bereich **Prozesse** das Kontrollkästchen für einen Prozess, und erweitern Sie dann den Bereich **Zugeordnete Handles**. Hier werden die Dateien angezeigt, die von diesem Prozess verwendet werden. Zudem werden die ausgewählten Prozesse zur problemlosen Überwachung oben in der Liste aufgeführt.
6. Klicken Sie auf die Registerkarte **Arbeitsspeicher**. Auf dieser Registerkarte werden ausführliche Informationen zur Arbeitsspeicherverwendung der einzelnen Prozesse bereitgestellt. Beachten Sie, dass der zuvor ausgewählte Prozess immer noch ausgewählt ist, sodass Sie mehrere Arten von Informationen zu einem Prozess überprüfen können, indem Sie zwischen den Registerkarten wechseln.
7. Klicken Sie auf die Registerkarte **Datenträger**. Auf dieser Registerkarte werden Prozesse mit kürzlicher Datenträgeraktivität angezeigt.
8. Erweitern Sie den Bereich **Datenträgeraktivität**, und deaktivieren Sie das Kontrollkästchen **Abbild**, um den Filter zu entfernen und alle Prozesse mit aktueller Datenträgeraktivität anzuzeigen. Im Bereich **Datenträgeraktivität** werden ausführliche Informationen zu den aktuell verwendeten Dateien aufgeführt. Im Bereich **Speicher** werden allgemeine Informationen zu den einzelnen logischen Datenträgern bereitgestellt.
9. Klicken Sie auf die Registerkarte **Netzwerk**. Auf dieser Registerkarte werden Informationen zu allen Prozessen mit aktueller Netzwerkaktivität bereitgestellt.
10. Erweitern Sie den Bereich **TCP-Verbindungen**. Hier werden die aktuellen TCP-Verbindungen sowie entsprechende Informationen angezeigt.

11. Erweitern Sie den Bereich **Überwachungsports**. Hier werden die Prozesse, die Netzwerkverbindungen abhören, sowie die von ihnen abgehörten Ports angezeigt. Zudem wird der Firewallstatus dieser Ports angezeigt.
12. Schließen Sie den **Ressourcenmonitor**.

Demo: Analysieren der Systemleistung mithilfe von Sammlungssätzen und der Leistungsüberwachung

Detaillierte Demoschritte

In dieser Demo wird gezeigt, wie die Systemleistung mithilfe der Sammlungssätze und der Leistungsüberwachung analysiert wird.

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, geben Sie im Suchfeld „**per**“ ein, und klicken Sie dann auf **Leistungsüberwachung**.
3. Klicken Sie im Fenster **Leistungsüberwachung** auf den Knoten **Leistungsüberwachung**. Beachten Sie, dass in der Standardeinstellung nur die Prozessorzeit (%) angezeigt wird.
4. Klicken Sie auf der Symbolleiste auf das Symbol „+“, um einen zusätzlichen Leistungsindikator hinzuzufügen.
5. Erweitern Sie im Bereich **Verfügbare Leistungsindikatoren** den Eintrag **Physischer Datenträger**, und klicken Sie dann auf **Leerlaufzeit (%)**.
6. Klicken Sie im Feld **Instanzen des ausgewählten Objekts** auf **0 C:**, auf **Hinzufügen** und dann auf **OK**.
7. Klicken Sie mit der rechten Maustaste auf **Leerlaufzeit (%)**, und klicken Sie anschließend auf **Eigenschaften**.
8. Klicken Sie im Feld **Farbe** auf **Grün** und dann auf **OK**.
9. Erweitern Sie im linken Bereich den Eintrag **Sammlungssätze**, und klicken Sie dann auf **Benutzerdefiniert**.
10. Klicken Sie mit der rechten Maustaste auf **Benutzerdefiniert**, zeigen Sie auf **Neu**, und klicken Sie dann auf **Sammlungssatz**.
11. Geben Sie im Feld **Name** die Bezeichnung **CPU- und Datenträgeraktivität** ein, und klicken Sie anschließend auf **Weiter**.
12. Klicken Sie im Feld **Vorlagensammlungssatz** auf **Standard** und dann auf **Weiter**. Das Verwenden einer Vorlage wird empfohlen.
13. Klicken Sie auf **Weiter**, um den Standardspeicherort für die Daten zu übernehmen.
14. Klicken Sie auf **Eigenschaften für diesen Sammlungssatz öffnen** und anschließend auf **Fertig stellen**. Auf der Registerkarte **Allgemein** können Sie allgemeine Informationen zum Sammlungssatz sowie die Anmeldeinformationen konfigurieren, die beim Ausführen verwendet werden.
15. Klicken Sie auf die Registerkarte **Verzeichnis**. Auf dieser Registerkarte können Sie definieren, wie die gesammelten Daten gespeichert werden.

16. Klicken Sie auf die Registerkarte **Sicherheit**. Auf dieser Registerkarte können Sie konfigurieren, welche Benutzer diesen Sammlungssatz ändern dürfen.
17. Klicken Sie auf die Registerkarte **Zeitplan**. Auf dieser Registerkarte können Sie definieren, wann der Sammlungssatz aktiv ist und Daten sammelt.
18. Klicken Sie auf die Registerkarte **Stoppbedingung**. Auf dieser Registerkarte können Sie definieren, wann die Datensammlung aufgrund der Dauer oder der gesammelten Daten beendet wird.
19. Klicken Sie auf die Registerkarte **Aufgabe**. Auf dieser Registerkarte können Sie eine geplante Aufgabe ausführen, wenn der Sammlungssatz beendet ist. Dies kann zum Verarbeiten der gesammelten Daten verwendet werden.
20. Klicken Sie auf **Abbrechen**.
21. Beachten Sie, dass im rechten Bereich drei Typen von Protokollen aufgeführt sind.
 - Der Leistungsindikator sammelt Daten, die in der Leistungsüberwachung angezeigt werden können.
 - Die Kernel-Ablaufverfolgung sammelt ausführliche Informationen zu Systemereignissen und -aktivitäten.
 - Die Konfiguration zeichnet Änderungen an Registrierungsschlüsseln auf.
22. Doppelklicken Sie im rechten Bereich auf **Leistungsindikator**. Beachten Sie, dass in der Standardeinstellung alle Leistungsindikatoren für Prozessoren gesammelt werden.
23. Klicken Sie auf **Hinzufügen**.
24. Klicken Sie im Bereich **Verfügbare Leistungsindikatoren** auf **Physischer Datenträger**, auf **Hinzufügen** und dann auf **OK**. Alle Leistungsindikatoren für das Objekt Physischer Datenträger werden jetzt hinzugefügt.
25. Klicken Sie im linken Bereich mit der rechten Maustaste auf **CPU- und Datenträgeraktivität**, und klicken Sie dann **Start**.
26. Warten Sie einen Moment, bis der Sammlungssatz automatisch beendet wird.
27. Klicken Sie mit der rechten Maustaste auf **CPU- und Datenträgeraktivität**, und klicken Sie dann auf **Aktuellster Bericht**. In diesem Bericht werden die vom Sammlungssatz gesammelten Daten angezeigt.
28. Schließen Sie die Leistungsüberwachung.

Lektion 2

Gewährleisten der Zuverlässigkeit mit den Windows 7-Diagnosetools

Inhalt:

Fragen und Antworten	152
Detaillierte Demoschritte	153

Fragen und Antworten

Demo: Beheben von Startproblemen

Frage: Wann führen Sie Systemreparaturen manuell mithilfe der Eingabeaufforderung aus?

Antwort: Sie führen Systemreparaturen mithilfe der Eingabeaufforderung manuell aus, wenn die automatisierten Tools das System nicht reparieren können.

Detaillierte Demoschritte

Demo: Beheben von Startproblemen

Detaillierte Demoschritte

In dieser Demo wird gezeigt, wie Startprobleme behoben werden.

1. Verbinden Sie das DVD-Laufwerk von LON-CL1 mit der Windows 7-Installations-DVD.
 - C:\Programme\Microsoft Learning\10225\drives\Windows7_32bit.iso
2. Starten Sie LON-CL1 neu, und drücken Sie eine Taste, um von der DVD zu starten, wenn Sie dazu aufgefordert werden.
3. Klicken Sie auf der Seite **Windows 7** auf **Weiter**.
4. Klicken Sie auf **Computer reparieren**.
5. Lesen Sie im Fenster **Systemwiederherstellungsoptionen** die Liste der gefundenen Betriebssysteme, und klicken Sie dann auf **Weiter**.
6. Lesen Sie die aufgeführten Optionen.
 - Die Systemstartreparatur versucht, ein Windows-System, das nicht ordnungsgemäß gestartet wird, automatisch zu reparieren.
 - Die Systemwiederherstellung wird verwendet, um Systemkonfigurationseinstellungen auf Grundlage eines Wiederherstellungspunkts wiederherzustellen.
 - Die Systemabbild-Wiederherstellung wird verwendet, um eine vollständige Wiederherstellung der Windows-Sicherung auszuführen.
 - Die Windows-Speicherdiagnose wird verwendet, um physische Speicher auf Fehler zu überprüfen.
 - Mit der Eingabeaufforderung können Sie manuell auf die lokale Festplatte zugreifen und Reparaturen ausführen.
7. Klicken Sie auf **Eingabeaufforderung**.
8. Geben Sie an der Eingabeaufforderung „**C:**“ ein, und drücken Sie die EINGABETASTE.
9. Geben Sie an der Eingabeaufforderung „**dir**“ ein, und drücken Sie die EINGABETASTE. Beachten Sie, dass sich auf Laufwerk C: keine Dateien vorhanden sind.
10. Geben Sie an der Eingabeaufforderung „**E:**“ ein, und drücken Sie die EINGABETASTE.
11. Geben Sie an der Eingabeaufforderung „**dir**“ ein, und drücken Sie die EINGABETASTE. Beachten Sie, dass es sich bei diesem Laufwerk um Laufwerk C: handelt, wenn Windows 7 ausgeführt wird.
12. Schließen Sie die Eingabeaufforderung, und klicken Sie auf **Neustart**.

Lektion 3

Sichern und Wiederherstellen von Daten mit der Windows-Sicherung

Inhalt:

Fragen und Antworten	155
Detaillierte Demoschritte	156

Fragen und Antworten

Demo: Durchführen einer Sicherung

Frage: Welche Dateien müssen auf einem Computer gesichert werden?

Antwort: Sichern Sie alle Datendateien auf einem Computer. Darüber hinaus können Sie mithilfe eines vollständigen Systemabbilds den Computer wiederherstellen, wenn ein Festplattenfehler auftritt.

Demo: Wiederherstellen von Daten

Frage: Wann erfordert die Wiederherstellung einen alternativen Speicherort?

Antwort: Führen Sie die Wiederherstellung an einem anderen Speicherort aus, um die aktuelle Version einer Datei zu behalten und gleichzeitig eine Kopie einer früheren Version zu Vergleichszwecken zu erhalten. Beispielsweise können seit einer Sicherung Informationen zu einer Datei hinzugefügt oder aus ihr gelöscht worden sein. Wenn Sie die neu hinzugefügten Informationen beibehalten möchten und gleichzeitig die gelöschten Informationen benötigen, müssen Sie über beide Versionen der Datei verfügen.

Detaillierte Demoschritte

Demo: Durchführen einer Sicherung

Detaillierte Demoschritte

In dieser Demo wird die Durchführung einer Sicherung dargestellt.

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start** und dann auf **Dokumente**.
3. Klicken Sie mit der rechten Maustaste im Fenster **Dokumente** auf einen geöffneten Bereich, zeigen Sie auf **Neu**, und klicken Sie dann auf **Textdokument**.
4. Geben Sie „Wichtiges Dokument“ ein, und drücken Sie dann die EINGABETASTE.
5. Doppelklicken Sie auf **Wichtiges Dokument**, geben Sie im Dokument einen beliebigen Text ein, und schließen Sie dann den Editor.
6. Klicken Sie auf **Speichern**, um die Datei zu speichern, und schließen Sie dann das Fenster **Dokumente**.
7. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Wartung** und dann auf **Sichern und Wiederherstellen**.
8. Klicken Sie auf **Sicherung einrichten**.
9. Klicken Sie auf **Allfiles (E:)** und dann auf **Weiter**.
10. Klicken Sie auf **Jetzt auswählen** und dann auf **Weiter**. Beachten Sie, dass in der Standardeinstellung sowohl die Bibliotheken für alle Benutzer als auch ein Systemabbild ausgewählt sind.
11. Deaktivieren Sie alle Kontrollkästchen im Fenster, **aktivieren Sie das fett formatierte Kontrollkästchen für die Bibliotheken des Administrators**, und klicken Sie dann auf **Weiter**.
12. Klicken Sie auf **Zeitplan ändern**.
13. Stellen Sie sicher, dass das Kontrollkästchen **Sicherung auf Basis eines Zeitplans ausführen (empfohlen)** aktiviert ist; überprüfen Sie die verfügbaren Optionen für **Häufigkeit**, **Tag der Sicherung** und **Uhrzeit**, und klicken Sie dann auf **OK**.
14. Klicken Sie auf **Einstellungen speichern und Sicherung ausführen**.
15. Die Sicherung wird nun ausgeführt. Klicken Sie auf **Details anzeigen**, um ausführliche Statusinformationen anzuzeigen.
16. Schließen Sie das Fenster **Sichern und Wiederherstellen**.

Demo: Wiederherstellen von Daten

Detaillierte Demoschritte

In dieser Demo wird das Wiederherstellen von Daten dargestellt.

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Wartung** und dann auf **Sichern und Wiederherstellen**.
3. Klicken Sie auf **Eigene Dateien wiederherstellen** und dann auf **Nach Dateien suchen**.
4. Klicken Sie im Fenster **Sicherung nach Dateien durchsuchen** auf **Sicherung von Administrator.CONTOSO**, doppelklicken Sie dann im rechten Bereich auf **Dokumente**, klicken Sie auf **Wichtiges Dokument** und dann auf **Dateien hinzufügen**.
5. Klicken Sie auf **Weiter**.
6. Klicken Sie auf **Am Ursprungsort** und dann auf **Wiederherstellen**.
7. Wenn angezeigt wird, dass die Datei bereits vorhanden ist, klicken Sie auf **Kopieren und ersetzen**.
8. Klicken Sie auf **Fertig stellen**.
9. Schließen Sie **Sichern und Wiederherstellen**.

Lektion 4

Wiederherstellen eines Windows 7-Systems mit Systemwiederherstellungspunkten

Inhalt:

Fragen und Antworten	159
Detaillierte Demoschritte	160

Fragen und Antworten

Funktionsweise der Systemwiederherstellung

Frage: Welche Situationen machen die Verwendung der Systemwiederherstellung erforderlich?

Antwort: Wenn der Computer nur langsam oder nicht ordnungsgemäß arbeitet, können Sie mithilfe der Systemwiederherstellung und eines Wiederherstellungspunkts die Systemdateien und Einstellungen des Computers auf einen früheren Zeitpunkt zurücksetzen.

Frage: Wann stellen Sie eine Datei eher von einem Wiederherstellungspunkt als aus einer Sicherung wieder her?

Antwort: Sie verwenden die Systemwiederherstellung, wenn alle Systemdateien des Computers zu einem bestimmten Datum und einer Uhrzeit wiederhergestellt werden müssen. Bei der Systemwiederherstellung werden nur Systemdateien und keine gelöschten oder beschädigten persönlichen Dateien wiederhergestellt.

Was sind Vorgängerversionen von Dateien?

Frage: Welche Vorteile bieten Vorgängerversionen von Dateien?

Antwort: Falls Sie eine Datei oder einen Ordner versehentlich ändern oder löschen, können Sie eine frühere Version wiederherstellen, die als Teil eines Wiederherstellungspunkts gespeichert ist.

Demo: Wiederherstellen eines Systems

Frage: Wann ist keine Vorgängerversion für eine Datei verfügbar?

Antwort: Die frühere Version einer Datei ist nicht verfügbar, wenn sie auf der lokalen Festplatte gespeichert wird. Wenn die lokale Festplatte ausfällt oder beschädigt wird, müssen Sie diese Daten von einer Sicherung wiederherstellen.

Detaillierte Demoschritte

Demo: Wiederherstellen eines Systems

Detaillierte Demoschritte

In dieser Demo wird gezeigt, wie ein System wiederhergestellt wird.

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start** und dann auf **Dokumente**.
3. Doppelklicken Sie auf **Wichtiges Dokument**, geben Sie etwas neuen Text ein, und schließen Sie dann den Editor.
4. Klicken Sie auf **Speichern**, und schließen Sie dann das Fenster **Dokumente**.
5. Klicken Sie auf **Start**, klicken Sie mit der rechten Maustaste auf **Computer**, und klicken Sie dann auf **Eigenschaften**.
6. Klicken Sie im Fenster **System** auf **Computerschutz**.
7. Klicken Sie im Bereich **Schutzeinstellungen** auf **Lokaler Datenträger (C:) (System)** und dann auf **Konfigurieren**.
8. Klicken Sie im Bereich **Einstellungen wiederherstellen** auf **Systemeinstellungen und vorherige Dateiversionen wiederherstellen** und dann auf **OK**.
9. Klicken Sie im Bereich **Schutzeinstellungen** auf **Allfiles (E:)** und dann auf **Konfigurieren**.
10. Klicken Sie im Bereich **Einstellungen wiederherstellen** auf **Systemeinstellungen und vorherige Dateiversionen wiederherstellen** und dann auf **OK**.
11. Klicken Sie im Fenster **Systemeigenschaften** auf **Erstellen**. Dieser Vorgang muss in der Regel nicht manuell durchgeführt werden, sondern wird automatisch vom System vor der Softwareinstallation durchgeführt.
12. Geben Sie im Fenster **Computerschutz** die Zeichenfolge „**Wiederherstellungspunkt 1**“ ein, und klicken Sie dann auf **Erstellen**.
13. Klicken Sie nach Abschluss der Erstellung des Wiederherstellungspunkts auf **Schließen**.
14. Klicken Sie im Fenster **Systemeigenschaften** auf **OK**, und schließen Sie dann das Fenster **System**.
15. Klicken Sie auf **Start** und dann auf **Dokumente**.
16. Klicken Sie mit der rechten Maustaste auf **Wichtiges Dokument** und auf **Vorgängerversionen wiederherstellen**. Diese Version der Datei wurde während der Erstellung des Wiederherstellungspunkts erstellt.
17. Klicken Sie auf **Abbrechen**, und schließen Sie das Fenster **Dokumente**.
18. Klicken Sie auf **Start**, und zeigen Sie auf **Alle Programme**. Klicken Sie auf **Zubehör**, **Systemprogramme** und dann auf **Systemwiederherstellung**.
19. Klicken Sie im Fenster **Systemdateien und -einstellungen wiederherstellen** auf **Weiter**.
20. Klicken Sie auf **Wiederherstellungspunkt 1** und dann auf **Weiter**.
21. Klicken Sie auf der Seite **Wiederherstellungspunkt bestätigen** auf **Fertig stellen**.

22. Klicken Sie auf **Ja**, um den Vorgang fortzusetzen. Beachten Sie, dass dabei nur Systemdateien und keine Datendateien wiederhergestellt werden.
23. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
24. Lesen Sie die Nachricht im Fenster **Systemwiederherstellung**, und klicken Sie auf **Schließen**.

Lektion 5

Konfigurieren von Windows Update

Inhalt:

Fragen und Antworten

163

Fragen und Antworten

Was ist Windows Update?

Frage: Inwiefern ist das Feature Automatische Updates nützlich?

Antwort: Dieser Onlinekatalogdienst stellt sicher, dass sich der Computer immer auf dem neuesten Stand befindet.

Windows Update-Gruppenrichtlinieneinstellungen

Frage: Welchen Vorteil hat es, Windows Update mithilfe der Gruppenrichtlinien anstatt über die Systemsteuerung zu konfigurieren?

Antwort: Die Verwendung einer Gruppenrichtlinie ermöglicht es Ihnen, die Konfigurationseinstellungen durch Ausführen einer einzelnen Aktion für mehrere Computer zu übernehmen. Außerdem wird verhindert, dass Benutzer die Einstellungen außer Kraft setzen.

Lernzielkontrollen und Kernpunkte der Unterrichtseinheit

Fragen zur Lernzielkontrolle

Frage 1: Angenommen, es tritt ein Leistungsproblem mit dem Computer auf. Wie erstellen Sie einen Sammlungssatz, um das Leistungsproblem zu analysieren?

Antwort: Sie können einen Sammlungssatz aus den Leistungsindikatoren in der Leistungsüberwachung, aus einer Vorlage oder manuell erstellen.

Frage 2: Nachdem Sie eine E-Mail-Nachricht von einer unbekannten Person erhalten haben, befindet sich ein Virus auf dem Computer, und Sie müssen eine Wiederherstellung ausführen.

1. Welche Art von Systemwiederherstellung müssen Sie verwenden?
2. Wird auf dem Computer Software wiederhergestellt, die vor zwei Tagen installiert wurde?
3. Wie lange werden Wiederherstellungspunkte gespeichert?
4. Was können Sie tun, wenn das Problem nicht durch die Systemwiederherstellung behoben wird?

Antwort:

1. Sie müssen eine Systemwiederherstellung erstellen, um Ihre Dateien auf einen Zeitpunkt vor dem Virus zurückzusetzen.
2. Ja, ein Wiederherstellungspunkt wird vor einem wichtigen Systemereignis automatisch erstellt.
3. Wiederherstellungspunkte werden gespeichert, bis die Systemspeicherreserven erschöpft sind. Beim Erstellen neuer Wiederherstellungspunkte werden alte gelöscht.
4. Wenn das Problem durch die Systemwiederherstellung nicht behoben wird, können Sie diese rückgängig machen oder versuchen, einen anderen Wiederherstellungspunkt auszuwählen.

Tools

Tool	Verwendung	Bezugsquelle
Leistungsinformationen und -tools	<ul style="list-style-type: none"> • Zeigt Informationen zu Geschwindigkeit und Leistung an 	Systemsteuerung
Leistungsüberwachung	<ul style="list-style-type: none"> • Mehrere Diagrammansichten zur Leistung 	Verwaltung
Ressourcenmonitor	<ul style="list-style-type: none"> • Überwacht die Verwendung und Leistung von CPU, Datenträger, Netzwerk und Arbeitsspeicher 	Erweiterte Tools in Leistungsinformationen und -tools
Windows-Leistungsindex	<ul style="list-style-type: none"> • Misst die Hauptkomponenten des Computers 	Leistungsinformationen und -tools
Überwachungstools	<ul style="list-style-type: none"> • Leistungsüberwachung 	Leistungsüberwachung

Sammlungssatz	<ul style="list-style-type: none"> • Leistungsindikatoren • Daten der Ereignisablaufverfolgung und der Systemkonfiguration 	Leistungsüberwachung
Windows-Speicherdiagnose	<ul style="list-style-type: none"> • Überprüft den Computer auf Arbeitsspeicherprobleme 	Verwaltung
Netzwerkprobleme beheben	<ul style="list-style-type: none"> • Netzwerkprobleme behandeln 	Netzwerk- und Freigabecenter
Zuverlässigkeitsüberwachung	<ul style="list-style-type: none"> • Zuverlässigkeit und Problemverlauf des Computers prüfen 	Wartungscenter
Tool für Problemberichte und -lösungen	<ul style="list-style-type: none"> • Wählen Sie aus, wann nach Lösungen für Problemberichte gesucht werden soll. 	Wartungscenter
Systemstartreparatur	<ul style="list-style-type: none"> • Überprüft den Computer auf Startprobleme 	Windows 7-DVD
Tool zum Sichern und Wiederherstellen	<ul style="list-style-type: none"> • Sichert Benutzer- und Systemdateien, oder stellt sie wieder her 	System und Sicherheit
Abbildsicherung	<ul style="list-style-type: none"> • Eine Kopie der für die Ausführung von Windows erforderlichen Treiber 	Sichern und Wiederherstellen
Systemreparaturdatenträger	<ul style="list-style-type: none"> • Wird verwendet, um den Computer zu starten 	Sichern und Wiederherstellen
Systemwiederherstellung	<ul style="list-style-type: none"> • Stellt einen früheren Zustand des Computers wieder her 	Systemsteuerung
Vorgängerversionen von Dateien	<ul style="list-style-type: none"> • Kopien von Dateien und Ordnern, die Windows automatisch als Teil eines Wiederherstellungspunkts speichert 	Systemeigenschaften
Wiederherstellungspunkt	<ul style="list-style-type: none"> • Ein gespeicherter Status der Systemdateien des Computers 	Systemeigenschaften
Speicherplatznutzung	<ul style="list-style-type: none"> • Maximalen Speicherplatz für den Computerschutz anpassen 	Systemeigenschaften
Windows Update	<ul style="list-style-type: none"> • Dienst, der Softwareupdates bereitstellt 	System und Sicherheit
Update-Einstellungen ändern	<ul style="list-style-type: none"> • Einstellungen für Windows Update ändern 	Windows Update
Updateverlauf anzeigen	<ul style="list-style-type: none"> • Updateverlauf des Computers überprüfen 	Windows Update

Fragen und Antworten zur Lernzielkontrolle

Frage: Welche Vorteile bietet die Erstellung eines Sammlungssatzes?

Antwort: Bei der Konfiguration eines Sammlungssatzes können Sie die im Sammlungsdatensatz enthaltenen Informationen sowie den Zeitpunkt der Datenerfassung anpassen. Dies ist hilfreich, wenn Sie zu einem bestimmten Zeitpunkt ein bestimmtes Computerleistungsproblem analysieren müssen.

Frage: Unter welchen Umständen würden Sie die Systemwiederherstellungspunkte auf allen Windows 7-Computern der Umgebung deaktivieren?

Antwort: Sie würden die Systemwiederherstellungspunkte auf den Windows 7-Computern deaktivieren, wenn Sie im Fall eines Computerfehlers über einen zentral verwalteten Prozess zum Verwalten von Daten und der Wiederherstellung von Computern verfügen. Wenn beispielsweise alle Benutzer ihre Dateien auf einem Dateiserver speichern, müssen Sie die Benutzerdaten nicht mit Systemwiederherstellungspunkten wiederherstellen. Anstelle der Wiederherstellung von Computern mit Systemwiederherstellungspunkten kann auch die Wiederherstellung von Windows 7-Computern mithilfe von Abbildern durchgeführt werden. Der Aufwand zur Wiederherstellung von Systemdateien entfällt in diesem Fall.

Unterrichtseinheit 8

Konfigurieren von mobilen Computern und Remotezugriff unter Windows® 7

Inhalt:

Lektion 1: Konfigurieren der Einstellungen für mobile Computer und Geräte	168
Lektion 2: Konfigurieren des Remotedesktops und der Remoteunterstützung für den Remotezugriff	173
Lektion 3: Konfigurieren von DirectAccess für den Remotezugriff	177
Lektion 4: Konfigurieren von BranchCache für den Remotezugriff	179
Lernzielkontrollen und Kernpunkte der Unterrichtseinheit	183
Fragen und Antworten zur Lernzielkontrolle	187

Lektion 1

Konfigurieren der Einstellungen für mobile Computer und Geräte

Inhalt:

Fragen und Antworten	169
Detaillierte Demoschritte	170

Fragen und Antworten

Tools zum Konfigurieren der Einstellungen für mobile Computer und Geräte

Frage: Wie kann, abgesehen von USB, eine Verbindung zum Synchronisieren eines Windows Mobile-Geräts hergestellt werden?

Antwort: Sie können eine Verbindung herstellen, um ein Windows Mobile-Gerät mit seriellen, Bluetooth-, Drahtlos- und Infrarotverbindungen zu synchronisieren.

Demo: Konfigurieren von Energiesparplänen

Frage: Warum kann das **Verhalten beim Zuklappen** nicht unter **Drahtlosadaptoreinstellungen, Energiesparmodus** konfiguriert werden?

Antwort: Dieser virtuelle Computer emuliert einen Desktopcomputer, und diese Optionen sind auf Desktopcomputern nicht verfügbar.

Detaillierte Demoschritte

Demo: Erstellen einer Synchronisierungspartnerschaft

Detaillierte Demoschritte

In dieser Demo wird gezeigt, wie das Windows Mobile-Gerätecenter konfiguriert und ein Windows Mobile-Gerät synchronisiert wird.

Starten der virtuellen Computer „LON-DC1“ und „LON-CL1“. Lassen Sie sie für die Dauer der Unterrichtseinheit eingeschaltet.

Erstellen von Terminen und Kontakten in Outlook

1. Melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Microsoft Office**, und klicken Sie anschließend auf **Microsoft Office Outlook 2007**.
3. Klicken Sie im **Outlook 2007-Start-Assistenten** auf **Weiter**.
4. Klicken Sie auf der Seite **E-Mail-Konten** auf **Nein**, und klicken Sie dann auf **Weiter**.
5. Aktivieren Sie auf der Seite **Datendatei erstellen** das Kontrollkästchen **Fortfahren ohne E-Mail-Unterstützung**, und klicken Sie dann auf **Fertig stellen**.
6. Klicken Sie im Dialogfeld **Benutzername** auf **OK**.
7. Klicken Sie bei Aufforderung unter Willkommen bei 2007 Microsoft Office System auf **Weiter**, klicken Sie auf **Ich möchte Microsoft Update nicht verwenden**, und klicken Sie dann auf **Fertig stellen**.
8. Klicken Sie bei Aufforderung im Dialogfeld **Microsoft Office Outlook** auf **Nein**.
9. Klicken Sie im linken Abschnitt von Outlook auf **Kalender**.
10. Klicken Sie im Ergebnisbereich auf die Registerkarte **Monat**, und doppelklicken Sie anschließend auf **Morgen**.
11. Geben Sie im Dialogfeld **Unbenannt – Ereignis** im Feld **Betreff** die Zeichenfolge „vierteljährliche Besprechung“ ein.
12. Geben Sie im Feld **Speicherort** die Zeichenfolge „Besprechungsraum 1“ ein, und klicken Sie dann auf **Speichern und Schließen**.
13. Wenn eine Erinnerung für den Termin angezeigt wird, klicken Sie auf **Schließen**.
14. Klicken Sie im linken Abschnitt von Outlook auf **Kontakte**.
15. Klicken Sie im Menü auf **Neu**.
16. Geben Sie im Dialogfeld **Unbenannt – Kontakt** im Feld **Vollständiger Name** die Zeichenfolge „Amy Rusko“ ein.
17. Geben Sie im Feld **Position** die Zeichenfolge „Produktionsleiter“ ein, und klicken Sie dann auf **Speichern und Schließen**.
18. Schließen Sie Outlook.

Konfigurieren des Windows Mobile-Gerätecenters

1. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, und klicken Sie dann auf **Windows Mobile-Gerätecenter**.
2. Klicken Sie im Dialogfeld **Windows Mobile-Gerätecenter** auf **Annehmen**.
3. Klicken Sie im Dialogfeld **Windows Mobile-Gerätecenter** auf **Einstellungen des Mobilgeräts**, und klicken Sie dann auf **Verbindungseinstellungen**.
4. Klicken Sie im Dialogfeld **Verbindungseinstellungen** in der Liste **Verbindung zu folgenden Anschlüssen zulassen** auf **DMA** und anschließend auf **OK**.
5. Geben Sie im Dialogfeld **Benutzerkontensteuerung** im Feld **Benutzername** die Zeichenfolge „Administrator“ ein.
6. Geben Sie im Feld **Kennwort** das Kennwort Pa\$\$w0rd ein, und klicken Sie anschließend auf **Ja**.
7. Schließen Sie das Windows Mobile-Gerätecenter.

Verbinden des Windows Mobile-Geräts

1. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Windows Mobile 6 SDK**, klicken Sie auf **Eigenständige Emulatorabbilder**, klicken Sie auf **Englisch (USA)**, und klicken Sie anschließend auf **WM 6.1.4 Professional**.
2. Warten Sie, bis der Start des Emulators abgeschlossen ist.
3. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Windows Mobile 6 SDK**, auf **Tools** und dann auf **Geräteemulator-Manager**.
4. Klicken Sie im Dialogfeld **Geräteemulator-Manager** auf das Symbol **Wiedergabe**.
5. Klicken Sie im Menü auf **Aktionen**, und klicken Sie dann auf **Basisstation**.
6. Schließen Sie den Geräteemulator-Manager.

Synchronisieren des Windows Mobile-Geräts

1. Klicken Sie im Dialogfeld **Windows Mobile-Clubseite** auf **Nicht registrieren**.
2. Klicken Sie im Windows Mobile-Gerätecenter auf **Gerät einrichten**.
3. Klicken Sie im Assistenten **Windows Mobile-Partnerschaft einrichten** auf der Seite **Welche Elemente möchten Sie synchronisieren?** auf **Weiter**.
4. Klicken Sie auf der Seite **Die Windows Mobile-Partnerschaft kann nun festgelegt werden** auf **Einrichten**.
5. Nachdem die Synchronisierung abgeschlossen ist, schließen Sie das Windows Mobile-Gerätecenter.

Überprüfen, ob die Daten synchronisiert wurden

1. Klicken Sie auf dem Windows Mobile-Gerät auf **Start** und anschließend auf **Kalender**.
2. Klicken Sie auf das morgige Datum. Wird die vierteljährliche Besprechung angezeigt?
3. Klicken Sie auf **Start** und dann auf **Kontakte**. Werden Kontakte aufgeführt?
4. Schließen Sie alle geöffneten Fenster. Speichern Sie keine Änderungen.

Demo: Konfigurieren von Energiesparplänen

Detaillierte Demoschritte

In dieser Demo wird gezeigt, wie ein Energiesparplan konfiguriert wird.

Erstellen eines Energiesparplans für Amys Laptop

1. Klicken Sie auf LON-CL1 auf **Start** und dann auf **Systemsteuerung**.
2. Klicken Sie auf **System und Sicherheit**, klicken Sie auf **Energiesparoptionen**, und klicken Sie dann auf der linken Seite auf **Energiesparplan erstellen**.
3. Klicken Sie auf der Seite **Energiesparplan erstellen** auf **Energiesparmodus**.
4. Geben Sie im Feld **Energiesparplanname** die Zeichenfolge „Amys Plan“ ein, und klicken Sie dann auf **Weiter**.
5. Klicken Sie auf der Seite **Einstellungen für Energiesparplan ändern: Amys Plan** im Feld Bildschirm ausschalten auf **5 Minuten**, und klicken Sie dann auf **Erstellen**.

Konfigurieren von Amys Energiesparplan

1. Klicken Sie in den **Energieoptionen** unter **Amys Plan** auf **Energiesparplaneinstellungen ändern**.
2. Klicken Sie auf der Seite **Einstellungen für Energiesparplan ändern: Amys Plan** auf **Erweiterte Energieeinstellungen ändern**.
3. Konfigurieren Sie die folgenden Einstellungen für den Plan, und klicken Sie anschließend auf **OK**.
 - **Festplatte ausschalten nach:** 10 Minuten
 - **Drahtlosadaptoreinstellungen, Energiesparmodus:** Maximaler Energiesparmodus
 - **Netzschalter und Zuklappen, Netzschalteraktion:** Herunterfahren
4. Klicken Sie auf der Seite **Einstellungen für Energiesparplan ändern: Amys Plan** auf **Abbrechen**.
5. Schließen Sie die **Energieoptionen**.

Lektion 2

Konfigurieren des Remotedesktops und der Remoteunterstützung für den Remotezugriff

Inhalt:

Fragen und Antworten	174
Detaillierte Demoschritte	175

Fragen und Antworten

Demo: Konfigurieren der Remoteunterstützung

Frage: Unter welchen Umständen werden Remotedesktopverbindung oder Remoteunterstützung verwendet?

Antwort: Verwenden Sie Remotedesktop, um Zugriff auf einen Computer mit einer Remoteverbindung von einem anderen Computer zu erhalten. Mit Remotedesktop können Sie beispielsweise von Ihrem Heimcomputer aus auf den Computer an Ihrem Arbeitsplatz zugreifen. Sie haben dann denselben Zugriff auf Programme, Dateien und Netzwerkressourcen wie an Ihrem Computer im Büro.

Verwenden Sie die Remoteunterstützung, um remote Unterstützung zu bieten oder in Anspruch zu nehmen. Zum Beispiel kann ein Freund oder ein Mitarbeiter des technischen Supports remote auf Ihren Computer zugreifen, um Ihnen mit einem Computerproblem zu helfen oder Ihnen zu zeigen, wie etwas gemacht wird. Und Sie können jemandem auf dieselbe Weise helfen. In beiden Fällen sehen sowohl Sie als auch die andere Person denselben Computerbildschirm, und beide sind in der Lage, den Mauszeiger zu steuern.

Detaillierte Demoschritte

Demo: Konfigurieren der Remoteunterstützung

Detaillierte Demoschritte

In dieser Demo wird gezeigt, wie die Remoteunterstützung aktiviert und verwendet wird. Amy benötigt Unterstützung bei einem Microsoft® Office Word-Feature. Sie fordert Unterstützung an, und Sie stellen eine Anleitung zu der Funktion mit Remoteunterstützung bereit.

Erstellen eines Microsoft Office Word 2007-Dokuments

1. Falls erforderlich melden Sie sich beim virtuellen Computer LON-CL1 als **Contoso\Don** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, zeigen Sie auf **Alle Programme**, klicken Sie auf **Microsoft Office**, und klicken Sie anschließend auf **Microsoft Office Word 2007**.
3. Geben Sie im Dokumentfenster die Zeichenfolge „Das ist mein Dokument“ ein, und klicken Sie anschließend auf die **Office**-Schaltfläche.
4. Klicken Sie auf **Speichern** und anschließend erneut auf **Speichern**.

Anfordern von Remoteunterstützung

1. Klicken Sie auf **Start**, und geben Sie im Feld **Suche** die Zeichenfolge „Remoteunterstützung“ ein.
2. Klicken Sie in der Liste **Programme** auf **Windows-Remoteunterstützung**.
3. Klicken Sie im Assistenten für die **Windows-Remoteunterstützung** auf **Eine vertrauenswürdige Person zur Unterstützung einladen**.
4. Klicken Sie auf der Seite **Wie möchten Sie jemanden einladen, Ihnen zu helfen?** auf **Einladung als Datei speichern**.
5. Geben Sie auf der Seite **Speichern unter** im Feld **Dateiname** die Zeichenfolge „\\LON-dc1rs\Public\Don's-Invitation.msrcincident“ ein, und klicken Sie dann auf **Speichern**.
6. Notieren Sie das Kennwort.

Bereitstellen von Remoteunterstützung

1. Wechseln Sie zum virtuellen Computer 10225A-LON-DC1, und melden Sie sich als Administrator mit dem Kennwort Pa\$\$w0rd an.
2. Öffnen Sie Windows-Explorer, navigieren Sie zu „C:\Users\Public“, und doppelklicken Sie dann auf **Dons-Einladung.msrcincident**.
3. Geben Sie im Dialogfeld **Remoteunterstützung** im Feld **Kennwort eingeben** das in der vorherigen Aufgabe notierte Kennwort ein, und klicken Sie anschließend auf **OK**.
4. Wechseln Sie zum virtuellen Computer LON-CL1.
5. Klicken Sie im Dialogfeld **Windows-Remoteunterstützung** auf **Ja**.
6. Wechseln Sie zum virtuellen Computer LON-DC1.
7. Klicken Sie im **Menü** auf **Steuerung anfordern**.
8. Wechseln Sie zum virtuellen Computer LON-CL1.

9. Klicken Sie im Dialogfeld **Windows-Remoteunterstützung** auf **Ja**.
10. Wechseln Sie zum virtuellen Computer LON-DC1.
11. Klicken Sie in **Word** auf das Menü **Überprüfen**, und wählen Sie den Text im Dokumentfenster aus.
12. Klicken Sie im **Menü** auf **Neuer Kommentar**, und geben Sie „So werden Kommentare in einem Dokument erstellt“ ein.
13. Platzieren Sie den Cursor an einer anderen Stelle im Dokumentfenster und klicken Sie.
14. Klicken Sie im Menü **Windows-Remoteunterstützung – Don helfen** auf **Chat**.
15. Geben Sie im Fenster **Chat** die Zeichenfolge „Hilft das?“ ein, und drücken Sie anschließend die EINGABETASTE.
16. Wechseln Sie zum virtuellen Computer LON-CL1.
17. Beachten Sie die Meldung.
18. Geben Sie „Ja, danke“ ein, drücken Sie die EINGABETASTE, und klicken Sie dann im **Menü** auf **Freigabe beenden**.
19. Schließen Sie alle geöffneten Fenster.
20. Verwerfen Sie die Dateiänderungen, und melden Sie sich bei LON-CL1 ab.
21. Wechseln Sie zum virtuellen Computer LON-DC1.
22. Schließen Sie alle geöffneten Fenster, und melden Sie sich bei LON-DC1 ab.

Lektion 3

Konfigurieren von DirectAccess für den Remotezugriff

Inhalt:

Fragen und Antworten

178

Fragen und Antworten

DirectAccess-Anforderungen

Frage: Wofür wird das Zertifikat in DirectAccess verwendet?

Antwort: Zur Bereitstellung der Authentifizierung.

Frage: Nennen Sie drei Bereitstellungsmöglichkeiten für DirectAccess.

Antwort: Die drei Möglichkeiten der Bereitstellung von DirectAccess sind

- DirectAccess-Bereitstellungs-Assistent - vereinfacht die Bereitstellung. Der Assistent kann Skripts erstellen und exportieren, die dann überprüft, weiter angepasst und manuell übernommen werden können.
- Benutzerdefinierte Skripts - verwendet hauptsächlich „netsh.exe“ und ist komplexer, bietet jedoch enorme Entwurfsflexibilität.
- Gruppenrichtlinie - wird nur zum Konfigurieren von Clients unterstützt, nicht von DirectAccess-Servern.

Lektion 4

Konfigurieren von BranchCache für den Remotezugriff

Inhalt:

Fragen und Antworten	180
Detaillierte Demoschritte	181

Fragen und Antworten

Was ist BranchCache?

Frage: Wie hindert BranchCache böswillige Benutzer daran, auf Inhalte zuzugreifen?

Antwort: Böswillige Benutzer können nicht auf Inhalte zugreifen, für die sie nicht berechtigt sind, da zwischengespeicherte Inhalte verschlüsselt werden.

Funktionsweise von BranchCache

Frage: Welcher Cachemodus von BranchCache hat eine Peer-zu-Peer-Architektur?

Antwort: Der verteilte oder kooperative Zwischenspeichermodus hat eine Art Peer-zu-Peer-Architektur. Inhalte werden auf den Computern von Windows 7-Clients zwischengespeichert, nachdem diese von einem Windows Server 2008 R2 abgerufen wurden. Anschließend werden sie bei entsprechendem Bedarf direkt an andere Windows 7-Clients gesendet, ohne dass diese Clients dieselben Inhalte über die WAN-Verbindung abrufen müssen.

BranchCache-Anforderungen

Frage: Welches der folgenden Betriebssysteme ist für die Verwendung von BranchCache auf Clientcomputern erforderlich?

Antwort: Die Antwort(en) sind fett formatiert.

- Windows Server® 2008 R2
- Windows Vista®
- **Windows® 7**
- Windows XP®

Demo: Konfigurieren von BranchCache auf einem Windows 7-Clientcomputer

Frage: Welche Auswirkungen hat es, wenn der Wert **BranchCache für Netzwerkdateien konfigurieren** auf null (0) festgelegt wird?

Antwort: Dies ist die akzeptable Roundtripverzögerung, bevor Zwischenspeichern aktiviert wird. Wenn Sie einen hohen Wert festlegen, wird die Zwischenspeicherung möglicherweise nicht durchgeführt. Wenn der Wert auf 0 (null) festgelegt wird, werden alle Dateien in einer Freigabe zwischengespeichert, unabhängig von der Verzögerung.

Detaillierte Demoschritte

Demo: Konfigurieren von BranchCache auf einem Windows 7-Clientcomputer

Detaillierte Demoschritte

In dieser Demo wird gezeigt, wie BranchCache aktiviert und konfiguriert wird.

Erstellen und Schützen eines freigegebenen Ordners

1. Melden Sie sich beim virtuellen Computer LON-DC1 als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, klicken Sie auf **Computer**, und doppelklicken Sie auf **Lokaler Datenträger (C:)**.
3. Klicken Sie im Menü auf **Neuer Ordner**.
4. Geben Sie „BranchCache“ ein, und drücken Sie die EINGABETASTE.
5. Klicken Sie mit der rechten Maustaste auf **BranchCache**, und klicken Sie anschließend auf **Eigenschaften**.
6. Klicken Sie im Dialogfeld **Eigenschaften von BranchCache** auf der Registerkarte **Freigabe** auf **Erweiterte Freigabe**.
7. Aktivieren Sie im Dialogfeld **Erweiterte Freigabe** das Kontrollkästchen **Diesen Ordner freigeben**, und klicken Sie dann auf **Berechtigungen**.
8. Klicken Sie auf **Entfernen** und dann auf **Hinzufügen**.
9. Geben Sie im Dialogfeld **Benutzer, Computer, Dienstkonten oder Gruppen auswählen** im Feld **Geben Sie die zu verwendenden Objektnamen ein (Beispiele)** die Zeichenfolge „Authentifizierte Benutzer“ ein, klicken Sie auf **Namen überprüfen**, und klicken Sie anschließend auf **OK**.
10. Aktivieren Sie in der Liste **Berechtigungen für authentifizierte Benutzer** das Kontrollkästchen **Zulassen** neben **Vollzugriff**, und klicken Sie anschließend auf **OK**.
11. Klicken Sie im Dialogfeld **Erweiterte Freigabe** auf **Zwischenspeichern**.
12. Aktivieren Sie das Kontrollkästchen **BranchCache aktivieren**, und klicken Sie dann auf **OK**.
13. Klicken Sie im Dialogfeld **Erweiterte Freigabe** auf **OK**.
14. Klicken Sie im Dialogfeld **Eigenschaften von BranchCache** auf die Registerkarte **Sicherheit**.
15. Klicken Sie auf **Bearbeiten** und dann auf **Hinzufügen**.
16. Geben Sie im Dialogfeld **Benutzer, Computer, Dienstkonten oder Gruppen auswählen** im Feld **Geben Sie die zu verwendenden Objektnamen ein (Beispiele)** die Zeichenfolge „Authentifizierte Benutzer“ ein, klicken Sie auf **Namen überprüfen**, und klicken Sie anschließend auf **OK**.
17. Aktivieren Sie in der Liste **Berechtigungen für authentifizierte Benutzer** das Kontrollkästchen **Zulassen** neben **Vollzugriff**, und klicken Sie anschließend auf **OK**.
18. Klicken Sie im Dialogfeld **Eigenschaften von BranchCache** auf die Schaltfläche **Schließen**.

Konfigurieren der BranchCache-Gruppenrichtlinieneinstellungen

1. Klicken Sie auf LON-DC1 auf **Start**, zeigen Sie auf **Verwaltung**, und klicken Sie anschließend auf **Gruppenrichtlinienverwaltung**.
2. Erweitern Sie in der Gruppenrichtlinienverwaltung den Eintrag **Gesamtstruktur: Contoso.com**, erweitern Sie **Domänen**, **Contoso.com** und **Gruppenrichtlinienobjekte**, klicken Sie auf **BranchCache**, klicken Sie mit der rechten Maustaste auf **BranchCache**, und klicken Sie dann auf **Bearbeiten**.
3. Erweitern Sie **Computerkonfiguration** und **Richtlinien**, erweitern Sie **Administrative Vorlagen** und **Netzwerk**, und klicken Sie anschließend auf **BranchCache**.
4. Doppelklicken Sie auf **BranchCache aktivieren**, klicken Sie auf **Aktiviert** und dann auf **OK**.
5. Doppelklicken Sie auf **BranchCache-Modus "Verteilter Cache" festlegen**, klicken Sie auf **Aktiviert** und dann auf **OK**.
6. Doppelklicken Sie auf **BranchCache für Netzwerkdateien konfigurieren**, klicken Sie auf **Aktiviert**, geben Sie den Wert „0“ unter **Optionen** ein, und klicken Sie dann auf **OK**.
7. Doppelklicken Sie auf **Prozentuale Speicherplatzbelegung durch Clientcomputer-cache festlegen**, klicken Sie auf **Aktiviert**, geben Sie den Wert „10“ unter **Optionen** ein, und klicken Sie dann auf **OK**.
8. Schließen Sie den Gruppenrichtlinienverwaltungs-Editor.
9. Schließen Sie Group Policy Management.
10. Schließen Sie alle geöffneten Fenster.

Konfigurieren des Clients

1. Wechseln Sie zum Computer LON-CL1, und melden Sie sich als **Contoso\Administrator** mit dem Kennwort **Pa\$\$w0rd** an.
2. Klicken Sie auf **Start**, **Systemsteuerung**, **System und Sicherheit** und dann auf **Windows-Firewall**.
3. Klicken Sie unter Windows-Firewall auf **Ein Programm oder Feature durch die Windows-Firewall zulassen**.
4. Aktivieren Sie unter **Zugelassene Programme und Features** in der Liste **Name** die folgenden Kontrollkästchen, und klicken Sie dann auf **OK**. Stellen Sie außerdem sicher, dass das Kontrollkästchen unter „Domäne“ aktiviert ist.
 - **BranchCache – Inhaltsabruf (verwendet HTTP)**
 - **BranchCache – Peerermittlung (verwendet WSD)**
5. Schließen Sie die Windows-Firewall.
6. Öffnen Sie ein Eingabeaufforderungsfenster.
7. Geben Sie an der Eingabeaufforderung „gpupdate /force“ ein, und drücken Sie dann die EINGABETASTE.
8. Geben Sie an der Eingabeaufforderung „netsh branchcache set service mode=DISTRIBUTED“ ein, und drücken Sie dann die EINGABETASTE.

Überprüfen des Status von BranchCache

Geben Sie an der Eingabeaufforderung die Zeichenfolge „netsh branchcache show status“ ein, und drücken Sie die EINGABETASTE.

Lernzielkontrollen und Kernpunkte der Unterrichtseinheit

Fragen zur Lernzielkontrolle

Frage 1: Amy versucht vergeblich, eine Drahtlosverbindung mit dem Netzwerk herzustellen, und ruft deshalb das Windows-Mobilitätscenter auf, um den Drahtlosnetzwerkadapter einzuschalten. Der Adapter wird nicht im Windows-Mobilitätscenter angezeigt. Warum ist das so?

Antwort: Wenn eine Einstellung nicht im Windows-Mobilitätscenter angezeigt wird, könnte dies daran liegen, dass die angeforderte Hardware (z. B. ein Drahtlosnetzwerkadapter) oder die Treiber fehlen.

Frage 2: Sie haben einen Computer mit Windows 7 Home Edition gekauft. Wenn Sie Remotedesktop für den Zugriff auf einen anderen Computer verwenden, wird dieser im Betriebssystem nicht gefunden. Worin besteht das Problem?

Antwort: Remotedesktop ist in Windows 7 Home Edition nicht verfügbar.

Frage 3: Sie haben einige wichtige Dateien auf dem Desktopcomputer an Ihrem Arbeitsplatz, auf die Sie mit dem Laptop zugreifen müssen, wenn Sie bei einem Kunden sind. Welche Aktionen sind auf dem Desktopcomputer erforderlich, um sicherzustellen, dass Sie die Dateien vom Kundenstandort aus herunterladen können?

Antwort: Sie müssen Remotezugriff auf dem Desktopcomputer konfigurieren. Wählen Sie in der Systemsteuerung unter **System und Sicherheit** auf der Registerkarte Remoteeinstellungen eine Option aus.

Frage 4: Ihr Unternehmen hat vor kurzem einen Windows Server 2008-Computer gekauft. Sie haben die Konvertierung von einem Datenbankserver auf einen DirectAccess-Server beschlossen. Was müssen Sie tun, bevor Sie diesen Computer mit DirectAccess konfigurieren können?

Antwort: Sie müssen ein Upgrade auf Windows Server 2008 R2 durchführen, möglicherweise auf eine IPv6-Infrastruktur upgraden und gegebenenfalls einen zweiten Netzwerkadapter auf dem Server installieren.

Frage 5: Amy muss ihren Windows 7-Clientcomputer für den Zugriff auf BranchCache konfigurieren. Wie muss Amy den Client für diesen Zweck konfigurieren?

Antwort: In Windows 7 ist BranchCache standardmäßig deaktiviert. Clientkonfigurationen können entweder mithilfe von Gruppenrichtlinien oder manuell pro Clientcomputer ausgeführt werden.

Häufige Probleme

Problem	Tipps zur Problembehandlung
<p>BytesAddedToCache wird auf dem ersten Client beim Zugriff auf den für BranchCache aktivierten Server nicht größer.</p>	<p>Der Clientcomputer ruft möglicherweise Inhalt aus dem Internet Explorer-Cache ab. Löschen Sie den IE-Cache, indem Sie im Menü Extras die Option Internetoptionen auswählen, und klicken Sie dann auf Löschen. Stellen Sie sicher, dass BranchCache auf dem ersten Client aktiviert ist, indem Sie den Befehl netsh branchcache show status verwenden. Wenn Sie versuchen, auf eine Dateifreigabe zuzugreifen, überprüfen Sie, ob die Wartezeit zwischen dem Client und dem Server höher als der minimale Schwellenwert ist. Stellen Sie sicher, dass die BranchCache-Funktion auf dem Server installiert und für das zu testende Protokoll aktiviert ist. Überprüfen Sie, ob der Server peerdistsvc sowohl auf dem Client, als auch auf dem Server ausgeführt wird. Durch einen Zwischenproxy wird die HTTP-Anforderung des Clients möglicherweise geändert. Vergewissern Sie sich, dass der Proxy den ACCEPT-ENCODING-HTTP-Header nicht ändert. Durch einen Zwischenproxy wird die ausgehende Anforderung von HTTP 1.1 möglicherweise zu HTTP 1.0 herabgestuft. Wenn das Symptom nur bei Dateidatenverkehr auftritt, stellen Sie sicher, dass die Datei nicht im transparenten Cache ist. Der transparente Cache ist ein sekundärer Cache, in dem die Datei zusätzlich zum BranchCache gespeichert wird. Das Speichern der Datei im transparenten Cache ermöglicht nachfolgende lokale Lesevorgänge der Datei und verbessert Endbenutzerantwortzeiten und Einsparungen bei der WAN-Bandbreite. Um zwischengespeicherte Daten transparent zu löschen, suchen Sie in der Systemsteuerung das Applet für Offlinedateien. Klicken Sie auf die Registerkarte Datenträgerverwendung, und klicken Sie auf Temporäre Dateien löschen. Beachten Sie, dass dies den BranchCache-Cache nicht löscht.</p>
<p>BytesAddedToCache wird auf dem ersten Client beim Zugriff auf den für BranchCache aktivierten Server größer. BytesFromCache wird auf dem zweiten Client beim Zugriff auf den für BranchCache aktivierten Server nicht größer. Die Bereitstellung ist auf den Modus Verteilter Cache festgelegt.</p>	<p>Stellen Sie sicher, dass BranchCache aktiviert wird, und dass beide Clients so konfiguriert werden, dass sie denselben Zwischenspeichermodus mithilfe des Befehls netsh branchCache show status verwenden. Stellen Sie mithilfe des Befehls netsh branchcache Show Status sicher, dass auf beiden Clients die richtigen Firewallausnahmen festgelegt werden. Stellen Sie mithilfe des Befehls ipconfig sicher, dass beide Clients mit dem gleichen Subnetz verbunden sind. Überprüfen Sie, dass der Clientcache nicht voll ist, indem Sie den Befehl netsh branchcache show status ALL verwenden.</p>

<p>BytesAddedToCache wird auf dem ersten Client beim Zugriff auf den für BranchCache aktivierten Server größer. BytesFromCache wird auf dem zweiten Client beim Zugriff auf den für BranchCache aktivierten Server nicht größer. Die Bereitstellung ist auf den Modus Gehosteter Cache festgelegt.</p>	<p>Stellen Sie mithilfe des Befehls netsh branchcache show status sicher, dass BranchCache aktiviert ist und beide Clients so konfiguriert sind, dass sie denselben Zwischenspeichermodus verwenden. Überprüfen Sie mithilfe des Befehls ping die grundlegende Konnektivität beider Clientcomputer mit dem gehosteten Cache. Stellen Sie mithilfe des Befehls netsh branchcache Show Status sicher, dass auf beiden Clients die richtigen Firewallausnahmen festgelegt werden. Stellen Sie mithilfe des Befehls netsh branchcache show status sicher, dass die richtigen Firewallausnahmen auf dem gehosteten Cacheserver festgelegt sind. Stellen Sie sicher, dass das Zertifikat ordnungsgemäß installiert ist und an Port 443 auf dem Computer mit dem gehosteten Cache gebunden ist.</p>
<p>Netsh zeigt an, dass die BranchCache-Firewallregeln nicht festgelegt wurden, obwohl sie mithilfe der Gruppenrichtlinie konfiguriert wurden.</p>	<p>Netsh überprüft die vordefinierte BranchCache-Firewallregelgruppe. Wenn Sie die für BranchCache unter Windows 7 definierten Standardausnahmen nicht aktiviert haben, meldet Netsh Ihre Konfiguration nicht ordnungsgemäß. Dieser Fehler tritt in der Regel auf, wenn Sie mithilfe einer Gruppenrichtlinie Firewallregeln für Clients definiert haben und das Gruppenrichtlinienobjekt auf einem Computer definiert wurde, der ein älteres Betriebssystem als Windows 7 oder Windows Server 2008 R2 (das die BranchCache-Firewallregelgruppe nicht enthält) ausführt. Dies bedeutet jedoch nicht, dass BranchCache nicht funktioniert.</p>
<p>Ein Clientcomputer läuft sehr langsam. Liegt dies an BranchCache?</p>	<p>Wenn viele Computer große Mengen an Inhalten von einem Client in einem kurzen Zeitraum beziehen, kann sich das auf die Desktopleistung auswirken. Überprüfen Sie mithilfe der Leistungsüberwachung, ob hohe Dienstraten zu Peers vorliegen. Untersuchen Sie das Verhältnis von BytesServedToPeers zu BytesFromCache und BytesFromServer. Der BranchCache-Dienst wird isoliert in einem eigenen Diensthost ausgeführt. Überprüfen Sie die CPU-Auslastung und den Speicherverbrauch des Diensthostprozesses, in dem der Zwischenspeicherdienst der Zweigstelle ausgeführt wird. Anhaltend hohe Dienstraten zu Peers sind möglicherweise ein Hinweis auf ein Konfigurationsproblem in der Zweigstelle. Überprüfen Sie dies, um sicherzustellen, dass die anderen Clients Dienstdaten verarbeiten können. Löschen Sie den Cache des betroffenen Clients mithilfe des Befehls netsh branchcache flush, oder reduzieren Sie die Cachegröße des betroffenen Clients.</p>

<p>Eine Seite wird nicht geladen, oder es kann nicht auf eine Freigabe zugegriffen werden.</p>	<p>Wenn BranchCache keine Daten aus einem Peer oder dem gehosteten Cache abrufen kann, wird das Protokoll der oberen Schicht an den Server zurückgegeben, um Inhalte abzurufen. Wenn ein Fehler in der Zwischenspeicherkomponente auftritt, muss das Protokoll der oberen Schicht nahtlos Inhalte vom Server herunterladen. Die Anzeige einer Webseite oder die Verbindung zu einer Freigabe wird nicht durch eine fehlerhafte BranchCache-Konfiguration oder sonstige Fehler verhindert. Wenn ein Fehler auftritt, verwenden Sie die von Windows-Explorer oder Internet Explorer bereitgestellte Schaltfläche Netzwerkdiagnoseframework/Diagnose.</p>
<p>Der Clientcomputer kann auch dann nicht auf die Dateifreigabe zugreifen, wenn eine Verbindung mit dem Server besteht.</p>	<p>Wenn der Clientcomputer aufgrund des Offlinefehlers (Netzwerkverbindung getrennt) nicht auf eine Dateifreigabe auf dem Server zugreifen kann, starten Sie den Clientcomputer neu und greifen Sie wieder auf die Freigabe zu. Wenn der Clientcomputer aufgrund des Offlinefehlers (langsame Verbindung) nicht auf eine Dateifreigabe auf dem Server zugreifen kann, löschen Sie die vorübergehend zwischengespeicherten Daten, starten Sie den Computer neu und greifen Sie auf die Freigabe zu. Um vorübergehend zwischengespeicherte Daten (dieselben wie der oben beschriebene transparente Cache) zu löschen, suchen Sie in der Systemsteuerung nach dem Applet für Offlinedateien. Klicken Sie auf die Registerkarte Datenträgerverwendung, und klicken Sie auf Temporäre Dateien löschen.</p>

Fragen und Antworten zur Lernzielkontrolle

Frage: In Übung 2 haben Sie das Remotedesktopfeature in der Firewall durch Bearbeiten der lokalen Firewallregeln aktiviert. Gibt es eine alternative Methode für diese Änderung?

Antwort: Ja, Sie können die Einstellungen durch eine Gruppenrichtlinie auf einem Domänencontroller konfigurieren. Dadurch werden die Einstellungen in einem einzigen Verwaltungsschritt für eine größere Gruppe von Computern angewendet.

Frage: Wenn Sie von einem Computer im Internet auf Dons Computer zugreifen möchten, welche zusätzlichen Einstellungen müssten Sie erwägen?

Antwort: Sie müssen wahrscheinlich zusätzlich zu den Firewallregeln auf Dons Computer die Firewall des Unternehmens konfigurieren oder deren Konfiguration anfordern. Sie müssen den TCP-Port 3389 zur Unterstützung von Remotedesktop aktivieren. Es können auch andere Ports zur Herstellung einer Verbindung mit Remotedesktop verwendet werden, diese müssen jedoch auf dem Computer konfiguriert werden, mit dem Sie eine Verbindung herstellen möchten.

Frage: In Übung 3 haben Sie die erforderlichen Einstellungen zur Unterstützung von BranchCache im Modus „Verteilter Cache“ festgelegt. Wie kann BranchCache noch implementiert werden, wenn in Slough ein Dateiserver installiert ist?

Antwort: Im Modus „Gehosteter Cache“, in dem der lokale Server zum Speichern von Dokumenten für den nachfolgenden Abruf verwendet werden kann. Auf dem Dateiserver muss Windows Server 2008 ausgeführt werden.

Ressourcen

Inhalt:

Microsoft Learning	189
TechNet- und MSDN-Inhalte	190
Communitys	191

Microsoft Learning

In diesem Abschnitt werden verschiedene Microsoft Learning-Programme und -Angebote beschrieben.

- [Microsoft Know-how-Beurteilungen](#) (Diese Website ist möglicherweise nur auf Englisch verfügbar.)

Beschreibt die von Microsoft bereitgestellten Angebote, mit deren Hilfe Sie Ihr Know-how bewerten lassen können.

- [Microsoft Learning](#)

Beschreibt die von Microsoft bereitgestellten Trainingsangebote, die als klassisches Training in einer Schulungseinrichtung oder als Training zum Selbststudium verfügbar sind.

- [Microsoft-Zertifizierungsprogramm](#)

Beschreibt, wie Sie eine Zertifizierung als Microsoft Certified Professional, Microsoft Certified Database Administrator und zahlreiche andere Zertifizierungen erhalten können.

- Microsoft Learning Support
 - Wenn Sie Kommentare oder Feedback zum Kurs abgeben möchten, senden Sie bitte eine E-Mail an folgende Adresse: support@mscourseware.com.
 - Bei Fragen zum Microsoft-Zertifizierungsprogramm können Sie auch eine E-Mail an mcphelp@microsoft.com senden.

TechNet- und MSDN-Inhalte

- [Verwaltung und Installation von Geräten](#)
- [Windows 7-Springboard-Reihe](#)
- [Übersicht über die Windows Internet Explorer 8-Technologie für Enterprise- und IT-Experten](#)
- [Microsoft-Anwendungskompatibilitäts-Toolkit \(ACT\), Version 5.5](#)
- [Empfehlungen zur Datenträgerverwaltung](#)
- [Suchen Sie in Hilfe und Support nach „Standardkonto“ und „Administratorkonto“. Informationen zu Gruppen:](#)
- [Hinzufügen eines Datenträgers](#)
- [Auswählen eines Dateisystems NTFS, FAT oder FAT32](#)
- [Formatieren eines Basisvolumes](#)
- [Partitionsstile](#)
- [Formatieren eines dynamischen Volumes](#)
- [Erstellen einer Partition oder eines logischen Laufwerks](#)
- [Technische Referenz zu Windows-Systemabbild-Manager](#)
- [Exemplarische Vorgehensweise: Erstellen eines benutzerdefinierten Windows PE-Abbilds](#)
- [Kopieren](#)
- [Befehlszeilenoptionen von Oscdimg](#)
- [Empfehlungen zur Datenträgerverwaltung](#)

MSDN

Dieser Abschnitt enthält MSDN-Inhalte für diesen Kurs.

- [Richtlinien zur Leistungsoptimierung für Windows Server 2008](#)
- [Grundlagen zu Windows Geräteklassen](#)
- [Treibersignierungsanforderungen für Windows](#)
- [Das neue Toolkit für Anwendungskompatibilität mit Unterstützung für Internet Explorer 8 ist auf MSDN verfügbar.](#)
- [Internet Explorer Anwendungskompatibilität](#)

Communitys

Dieser Abschnitt enthält Community-Inhalte für diesen Kurs.

- [Hardwareanforderungen für Windows 7](#)
- [Liste der Device Stage-Funktionen](#)
- [ACT 5.5](#)
- [Treibersignierungsanforderungen für Windows](#)
- [Hardwareanforderungen für Windows](#)
- [Internet Explorer 8: Startseite](#)
- [Internet Explorer 8-Newsgroups](#)
- [Internet Explorer 8-FAQ](#)
- [Informationen zu Antiphishing-Strategien](#)
- [Internet Explorer 8: Hilfe und Support](#)
- [Internet Explorer 8-Forum auf TechNet](#)
- [Internet Explorer 8-Hilfe, Microsoft Knowledge Base-Artikel 923737](#)
- [Portnummern](#)

Senden Sie uns Ihr Feedback

Bevor Sie Feedback senden, können Sie die Microsoft Knowledge Base unter [Microsoft Hilfe und Support](#) nach bekannten Problemen durchsuchen. Verwenden Sie beim Suchen entweder die Kursnummer mit dem Versionsbuchstaben oder den Kurstitel.

Hinweis: Nicht für alle Schulungsprodukte ist ein Knowledge Base-Artikel vorhanden. Fragen Sie in diesem Fall Ihren Kursleiter, ob Fehlerprotokolleinträge vorhanden sind.

Feedback zu den Kursen

Senden Sie Feedback zu den Kursen an support@mscourseware.com. Wir wissen es zu schätzen, dass Sie Zeit und Mühe investieren, um uns Feedback zu geben. Alle eingehenden E-Mails werden gelesen, und die Informationen werden an das entsprechende Team weitergeleitet. Da wir sehr viele E-Mails erhalten, können wir Ihnen leider nicht antworten. Ihr Feedback fließt aber möglicherweise in die Verbesserung der Microsoft Learning-Produkte ein, sodass Sie in Zukunft davon profitieren.

Berichten von Fehlern

Geben Sie beim Feedback Titel und Nummer des Schulungsprodukts im Betreff der E-Mail-Nachricht an. Geben Sie in Ihren Kommentaren und Fehlerberichten die folgenden Informationen an:

- Artikelnummer des Dokuments oder der CD
- Seitenzahl oder Textstelle
- Vollständige Beschreibung des Fehlers oder des Änderungsvorschlags

Geben Sie alle erforderlichen Informationen an, um eine Überprüfung des Problems zu ermöglichen.

Wichtig Alle Fehler und Vorschläge werden ausgewertet, doch werden nur die überprüften Fehler dem Knowledge Base-Artikel zu diesem Produkt hinzugefügt.