

Kurs-Dokumentation



Zentrum für Informatik ZFI AG

Updating your Active Directory Technology

Skills to Windows Server 2008 (WS8A) - IT

Ausbildung nach Mass

<http://www.zfi.ch/WS8A>

Weitere Infos finden Sie unter www.zfi.ch oder via Adresse:

Zentrum für Informatik ZFI AG
Zentralsekretariat
Technoparkstrasse 1
CH-8005 Zürich
Telefon: 044 732 40 00
Telefax: 044 732 40 09

Zürich, Basel, Bern, Zürich, Schweiz

Titel	Updating your Active Directory Technology Skills to Windows Server 2008
Untertitel	AD Services, AD Federation Services, LDAP, Rights Management, RODC, Auditing, Certificate Services
Einleitung	<p>Zur Beachtung: Dieser Kurs ist durch den Kurs W8AU/6416B abgelöst worden und wird deshalb als öffentlicher Kurs nicht mehr eingeplant (bleibt als Firmenkurs jedoch weiterhin verfügbar). Der neue Kurs W8AU/6416B basiert auf dem Final Release von Windows Server 2008 und kombiniert die beiden bisherigen Kurse WS8U/6415 und WS8A/6416 in einem einzigen Kurs. Windows Server 2008 umfasst Verbesserungen bei den Active Directory-Domänendiensten, die die Verwaltung der Domänendienste vereinfachen und Administratoren mehr Flexibilität beim Erfüllen der Anforderungen von Filialen bieten. Dies sind einige der wichtigsten Verbesserungen bei der Verwaltung:- Ein aktualisierter AD DS-Installationsassistent (Active Directory-Domänendienste)- Änderungen an der Microsoft Management Console, die zum Verwalten von AD DS verwendet wird- Neue Installationsoptionen für Domänencontroller- Aktualisierter Installationsassistent, der die AD DS Installation vereinfacht- Verbesserte Schnittstelle und Verwaltungsoptionen für AD DS- Verbesserte Tools zur Suche nach Domänencontrollern im Unternehmen Beim neuen Installationsassistenten sind jetzt alle verwandten Funktionen zusammengefasst, sodass der Prozess rationalisiert und während der Bereitstellung Zeit gespart wird. Bei einer unbeaufsichtigten Installation in Windows Server 2008 ist eine Antwort des Benutzers auf Eingabeaufforderungen der Benutzeroberfläche nicht erforderlich, wodurch Remoteinstallationen noch weiter vereinfacht werden. Dies ermöglicht ausserdem die Installation von AD DS in einer Server Core-Installation. Um sicherzustellen, dass ein neu installierter DNS-Server ordnungsgemäss arbeitet, wird DNS automatisch für DNS-Clienteinstellungen, Weiterleitungen und Stamminweise, sofern notwendig, auf der Basis der ausgewählten Installationsoptionen konfiguriert. Diese in Windows Server 2008 angebotenen Verbesserungen bei der AD DS-Schnittstelle reduzieren die Zeit bei der IT-Administration, indem die anfängliche Bereitstellung rationalisiert wird, was die Verwaltung von Servern in Filialen vereinfacht.</p> <p>Read-Only-Domänencontroller Ein Read-Only-Domänencontroller (RODC) ist eine neue Art von Domänencontroller im Windows Server 2008-Betriebssystem, der hauptsächlich für die Bereitstellung in einer Umgebung mit Unternehmensniederlassungen entworfen wurde. Ein RODC kann die Risiken der Bereitstellung eines Domänencontrollers an Remotestandorten wie Filialen reduzieren, in denen die physische Sicherheit nicht garantiert werden kann. Mit Ausnahme von Kontokennwörtern sind alle Microsoft AD DS-Objekte und Attribute (Active Directory-Domänendienste), die in einem beschreibbaren Domänencontroller enthalten sind, in einem RODC enthalten. Clients können jedoch Änderungen nicht direkt auf einen RODC schreiben. Da Änderungen nicht direkt auf den RODC geschrieben und daher nicht lokal durchgeführt werden, müssen schreibbare Domänencontroller, die Replikationspartner sind, keine Änderungen vom RODC abrufen. Die Administratorrollentrennung bestimmt, dass jeder beliebige</p>

Domänenbenutzer als lokaler Administrator eines RODC delegiert werden kann, ohne dass diesem Benutzer Benutzerrechte für die Domäne selbst oder andere Domänencontroller gewährt werden. Server- und Domänenisolierung In einem Microsoft Windows-basierten Netzwerk können Administratoren Server- und Domänenressourcen logisch isolieren, um den Zugriff auf authentifizierte und autorisierte Computer zu isolieren. Ein logisches Netzwerk kann beispielsweise innerhalb des vorhandenen physischen Netzwerks erstellt werden, in dem Computer einen gemeinsamen Satz an Anforderungen für die sichere Kommunikation nutzen. Jeder Computer in diesem logisch isolierten Netzwerk muss anderen Computern Anmeldeinformationen zum Authentifizieren im isolierten Netzwerk bereitstellen, um eine Verbindung herzustellen. Diese Isolierung hindert nicht autorisierte Computer und Programme daran, auf nicht ordnungsgemäße Weise auf Ressourcen zuzugreifen. Anforderungen von Computern, die nicht Teil des isolierten Netzwerks sind, werden ignoriert. Die Server- und Domänenisolierung kann dazu beitragen, bestimmte hochwertige Server und Daten sowie verwaltete Computer vor nicht verwalteten oder nicht autorisierten Computern und Benutzern zu schützen. Zum Schutz eines Netzwerks können zwei Arten der Isolierung verwendet werden: - Serverisolierung: In einem Serverisolierungsszenario werden bestimmte Server mithilfe der IPsec-Richtlinie so konfiguriert, dass nur authentifizierte Kommunikation von anderen Computern angenommen wird. Der Datenbankserver kann beispielsweise so konfiguriert werden, dass nur Verbindungen vom Webanwendungsserver angenommen werden. - Domänenisolierung: Zum Isolieren einer Domäne können Administratoren die Active Directory-Domänenmitgliedschaft verwenden, um sicherzustellen, dass Computer, die Mitglieder einer Domäne sind, nur authentifizierte und gesicherte Kommunikation von anderen Computern annehmen, die Domänenmitglieder sind. Das isolierte Netzwerk besteht nur aus Computern, die Teil der Domäne sind. Bei der Domänenisolierung wird die IPsec-Richtlinie verwendet, um Schutz für den Datenverkehr zwischen Domänenmitgliedern, einschliesslich aller Clients und Servercomputer, zu aktivieren. Unternehmens-PKI (PKIView) Beim Windows Server 2008- und Windows Vista-Betriebssystem gibt es eine Reihe von Verbesserungen bei der Infrastruktur für öffentliche Schlüssel (Public Key Infrastructure, PKI). Die Verwaltbarkeit bei allen Aspekten von Windows PKI wurde verbessert, die Sperrungsdienste wurden überarbeitet, und die Angriffsfläche bei der Registrierung wurde verringert. Die PKI-Verbesserungen umfassen folgende: - Unternehmens-PKI (PKIView): PKIView war ursprünglich Teil des Microsoft Windows Server 2003 Ressource Kit und wurde als PKI Health-Tool bezeichnet. Heute ist es ein MMC-Snap-In (Microsoft Management Console) für Windows Server 2008 und dient zur Analyse des Zustands von Zertifizierungsstellen und zum Anzeigen der Einzelheiten von Zertifikaten, die in AD CS veröffentlicht wurden. - Online Certificate Status-Protokoll (OCSP): Ein Onlineantwortdienst auf der Basis des Online Certificate Status-Protokolls (OCSP) kann zum Verwalten und Verteilen von Informationen zum Sperrstatus in Fällen verwendet werden, in denen die Verwendung von konventionellen CRLs keine ideale Lösung ist. Onlineantwortdienste können auf einem

	<p>einzelnen Computer oder in einem Onlineresponderarray konfiguriert werden. - Network Device Enrollment Service (NDES): In Windows Server 2008 ist der Network Device Enrollment Service (NDES) die Microsoft-Implementierung des Simple Certificate Enrollment-Protokolls (SCEP), eines Kommunikationsprotokolls, das die Ausführung von Software auf Netzwerkgeräten wie Routern und Switches ermöglicht, die andernfalls im Netzwerk nicht authentifiziert werden können, um X.509-Zertifikate von einer Zertifizierungsstelle zu registrieren. - Webregistrierung: Die neue Webregistrierungssteuerung ist sicherer, die Skriptprogrammierung ist einfacher, und sie lässt sich leichter als vorherige Versionen aktualisieren. - Gruppenrichtlinie und PKI: Mithilfe der Zertifikateinstellungen in der Gruppenrichtlinie können Administratoren Zertifikateinstellungen von einem zentralen Standort aus für alle Computer in der Domäne verwalten. Dies ist das Aufbau-Seminar für Microsoft Windows Server 2008 System-Administratoren.</p>
Ihr Nutzen	<p>After completing this course, students will be able to: Describe and configure server roles with Active Directory Services in Windows Server 2008. Plan for and deploy Active Directory Domain Services. Install, configure, and manage the Server Core role as a domain controller. Manage accounts, subnets, Site-Links, Group Policy, and DNS configuration with Active Directory Domain Services. Manage new Active Directory services, including Active Directory Federation Services, Active Directory Lightweight Directory Services, and Active Directory Rights Management Services. Set up and manage Read-Only Domain Controllers (RODC). Use auditing features in Active Directory Domain Services. Manage credentials with Active Directory Certificate Services, including Credential Roaming.</p>
Voraussetzungen	<p>Before attending this course, students must have one or more of the following: On-the-job experience in planning, implementing, managing, or supporting Microsoft Windows Server 2000 or 2003, including Active Directory and Network Infrastructure Working knowledge of networking, for example, TCP/IP and Domain Name System (DNS). Designed a Microsoft Windows Server 2003 Active Directory and Network Infrastructure Designed Security for a Microsoft Windows Server 2003 Network Installed, Configured, and Administered Microsoft Windows 2000, Windows XP Professional, or Microsoft Vista.</p>
Teilnehmerkreis	<p>This course is intended for IT Professionals experienced on the technologies included in Windows Server 2000 and Windows Server 2003, and who hold an MCSE or MCSA certification and/or equivalent knowledge.</p>
Unterlagen	<p>Original-Microsoft-Kursunterlagen</p>
Folgekurse	
Inhalt	<ul style="list-style-type: none"> - Introduction to Active Directory Technology in Windows Server 2008 - Active Directory Improvements - Lab1 1: Introduction to Active Directory Technology in Windows Server 2008 - Planning for Windows Server 2008 Active Directory Services

- **Planning for ADDS Deployment**
- **Upgrade Considerations**
- **Lab 1: Installing Windows Server 2008 Forest**
- **Installing Windows Server 2008 in an Existing Forest**

- **Server Core Domain Controllers**
- **Server Core Domain Controller**
- **Lab 1: Server Core Domain Controller**

- **Active Directory Domain Services**
- **What's New in AD DS**
- **Improved Security**
- **Manageability and Reliability**
- **Lab 1: Exploring Active Directory Domain Services**

- **Active Directory Federation Services, Active Directory Lightweight Directory Services, Active Directory Rights Management Services**
- **Active Directory Federation Services**
- **Active Directory Lightweight Directory Services**
- **Active Directory Rights Management Services**
- **Lab 1: Active Directory Federation Services**
- **Lab 2: Active Directory Rights Management Services**

- **Read-Only Domain Controllers**
- **Read-Only Domain Controllers**
- **Read-Only Domain Controller Operation**
- **Lab 1: Read-Only Domain Controllers**

- **Auditing Active Directory Domain Services Changes**
- **What's new in AD DS auditing**
- **Who should use this new feature**
- **Benefits of auditing changes in AD DS**
- **Summary of new AD DS auditing events**
- **Summary of attribute syntaxes**
- **Lab 1: Auditing Active Directory Domain Services Changes**

- **Enterprise PKI (PKIView) Active Directory Certificate Services (ADCS)**
- **Certificate Authority**
- **Certificate Policy Settings**
- **Microsoft Simple Certificate Enrollment Protocol**
- **Online Revocation Services**
- **Network Device Enrollment Services**
- **Web Enrollment Services**
- **Lab 1: Enterprise PKI (PKIView) Active Directory Certificate Services (ADCS)**

Beitrag

Der Teilnehmerbeitrag versteht sich rein netto. Das ZFI ist (gemäss MwSt-Gesetz) nicht Mehrwertsteuerpflichtig und erhebt somit keine MwSt. Bei länger als einen Monat dauernden Lehrgängen ist die Zahlung des Teilnehmerbeitrages in mehreren Raten möglich (pro rata temporis).

Bildungsweg Microsoft Server 2008

Microsoft Windows Server 2008

