**Microsoft Kurs**

**Windows Server: Bereitstellung, Konfiguration und Verwaltung**

**Sichere Verwaltung von Windows Server**

**Lernziele:**

* Erläutern von Verwaltungsmodellen der geringsten Rechte
  + Zugriffsrechte auf die Rechte zu beschränken, die zur Ausführung einer bestimmten Aufgabe oder Auftragsrolle erforderlich sind. (Benutzerkonten, Dienstkonten, Computerprozesse)
  + Im Active Directory Domain Services (AD DS) gibt es eine Reihe sensibler administrativer Gruppen (Organisationsadministratoren, Domänenadministratoren, Schema-Admins, Administratoren)
  + AD DS-Schema ist eine Sammlung von Objekten und deren Eigenschaften, die manchmal auch als Klassen und Attribute bezeichnet werden.
  + Ein Recht ist die Möglichkeit, eine administrative Aufgabe auszuführen. Eine Berechtigung ist die Möglichkeit, auf ein Objekt im Dateisystem, in AD DS oder an einem anderen Ort zuzugreifen.
  + TIPP: Weisen Sie eine Richtlinie immer einer Gruppe zu, nicht einem Benutzer direkt. Dies hilft bei der zukünftigen Verwaltung. Wenn sich das Aufgabengebiet einer Person ändert, müssen Sie nur ihre Gruppenmitgliedschaften ändern, anstatt alle dem Benutzerkonto zugewiesenen Benutzerrechte zu überprüfen und ggf. zu ändern.
  + Benutzerkontensteuerung (UAC) ist ein Sicherheitsfeature, das es Benutzern ermöglicht, den Status ihres Administratorkontos auf den Standardbenutzerkonten zu beschränken.
  + Just Enough Administration (JEA) ist eine Verwaltungstechnologie, mit der Sie Prinzipien der rollenbasierten Zugriffsteuerung (RBAC) über Windows PowerShell-Remote Sitzungen anwenden können.
  + JEA unterstützt nur Windows PowerShell-Remoting
* Implementieren delegierter Berechtigungen
  + Delegierte Berechtigungen stellen eine Möglichkeit dar, bestimmten Benutzern oder Gruppen begrenze Berechtigungen zu gewähren.
  + Der Assistent verfügt über diverse vordefinierten Aufgaben, die Sie zuweisen können. (Erstellen, Löschen und Verwalten von Benutzerkonten; Zurücksetzen von Benutzerkennwörtern und Erzwingen der Kennwortänderung bei der nächsten Anmeldung; Lesen aller Benutzerinformationen; Erstellen, Löschen und Verwalten von Gruppen; Ändern der Mitgliedschaft einer Gruppe; Hinzufügen eines Computers zur Domäne (nur auf Domänenebene verfügbar); Verwalten von Gruppenrichtlinienverknüpfungen; Generieren von Richtlinienergebnissätzen (Planung); Generieren von Richtlinienergebnissätzen (Protokollierung); Erstellen, Löschen und Verwalten von inetOrgPerson-Konten; Zurücksetzen von inetOrgPerson-Kennwörtern und Erzwingen der Kennwortänderung bei der nächsten Anmeldung; Lesen aller inetOrgPerson-Informationen;)
  + Starten des Assistenten: öffne Active Directory-Benutzer und –Computer > suchen Sie die Organisationseinheit (OU), über die Sie die Objektverwaltung delegieren möchten.
  + Sie können auch die Objektverwaltung für das Domänenobjekt delegieren
  + TIPP: Zum Delegieren der Objektverwaltung für einen Standort verwenden Sie das Tool Active Directory-Standorte und –Dienste, um die Kontrolle zu delegieren.
  + TIPP: Vermeiden Sie es, Rechte bestimmten Benutzern zuzuweisen. Verwenden Sie stattdessen Gruppen, auch wenn die Gruppe nur einen Benutzer enthält. Dadurch wird die zukünftige Verwaltung vereinfacht.
  + Nachdem Sie den delegierten Zugriff zugewiesen haben, können Sie den **Assistenten zum Zuweisen der Objektverwaltung** nicht verwenden, um Ihre Einstellungen zu überprüfen.
  + Der **Assistenten zum Zuweisen der Objektverwaltung** bietet eine einfache, vom Assistenten gesteuerte Schnittstelle für die Konfiguration von AD DS-Berechtigungen für AD DS-Objekte.
* Verwenden von Arbeitsstationen mit privilegiertem Zugriff
  + Eine privilegierte administrative Arbeitsstation (Privileged Administrative Workstations, PAW) ist ein Computer, den Sie für die Durchführung von Verwaltungsaufgaben verwenden können, z. B. für die Verwaltung von Identitätssystemen, Clouddiensten und anderen sensiblen Funktionen. Dieser Computer wird vor dem Internet geschützt und so eingeschränkt, dass nur die erforderlichen Verwaltungs-Apps ausgeführt werden können.
  + TIPP: Sie müssen privilegierte Server so konfigurieren, dass keine Verbindungen mit nicht privilegierten Arbeitsstationen akzeptiert werden.
  + Microsoft empfiehlt, Windows 10 Enterprise für Ihre PAWs zu verwenden.
  + Wenn Sie ein einziges Gerät verwenden, stellen Sie sicher, dass die PAW auf dem physischen Computer ausgeführt wird, während Ihre reguläre Arbeitsstation als VM ausgeführt wird. Dies bietet die richtige Sicherheit.
* Beschreiben von Sprungservern
  + Ein Sprungserver ist ein gehärteter Server, der für den Zugriff und die Verwaltung von Geräten in einer anderen Sicherheitszone verwendet wird, z. B. zwischen einem internen Netzwerk und einem Umkreisnetzwerk. Der Sprungserver kann als einzelner Kontakt- und Verwaltungspunkt fungieren.
  + TIPP: Normalerweise verwenden Sie eine PAW für den Zugriff auf einen Sprungserver, um einen sicheren Zugriff zu gewährleisten.
  + Durch die Verwendung von Sprungservern (entweder mit oder ohne PAWs) können Sie logische Sicherheitszonen erstellen. Die Computer innerhalb einer Zone verfügen über ähnliche Sicherheits- und Verbindungskonfigurationen. Sie können GPOs verwenden, um diese Einstellungen innerhalb einer Domänenumgebung zu konfigurieren.
  + TIPP: Administrative Benutzer können über das Remotedesktopprotokoll (RDP) und Smartcards eine Verbindung zu mit Ihren Sprungservern herstellen, um administrative Aufgaben auszuführen.
  + Wenn Sie Sprungserver implementieren, sollten Sie einige Überlegungen berücksichtigen. Dazu gehören:
    - Remotedesktopgateway. Wenn ein Administrator eine direkte Verbindung zu einem Zielserver (über RDP) herstellen muss, implementieren Sie ein Remotedesktopgateway. Damit können Sie Beschränkungen für Verbindungen zum Sprungserver und zu den für die Verwaltung verwendeten Zielservern implementieren.
    - Hyper-V. Erwägen Sie die Implementierung von virtuellen Computern für jeden Administrator auf Ihren Sprungservern. Jede VM kann so konfiguriert werden, dass sie eine bestimmte administrative Aufgabe oder eine Teilmenge administrativer Aufgaben zulässt. Daher sollten Sie Hyper-V auf ihren Sprungservern installieren.
  + TIPP: Sie können das Herunterfahren dieser VMs nach Abschluss der administrativen Aufgaben erzwingen. Indem Sie VMs herunterfahren, wenn sie nicht in Gebrauch sind, reduzieren Sie Ihre Angriffsfläche.
  + Server-Features. Um Sprungserver zu implementieren, müssen Ihre Servercomputer die folgenden Features unterstützen:
    - UEFI Secure Boot.
    - Virtualisierungsunterstützung.
    - Signierte Kernelmodustreiber.

**Zusammenfassung**

Als Windows Server-Administrator bei Contoso sind Sie für die Verwaltung und Wartung der lokalen Serverinfrastruktur verantwortlich. Ihre erste Aufgabe war es, herauszufinden, wie Sie Windows Server am besten nach dem Prinzip der geringsten Rechte verwalten können.

In diesem Modul haben Sie gelernt, welche Benutzerkonten Sie für die Durchführung administrativer Aufgaben verwenden und wie Sie die Windows Server-Verwaltung sicher durchführen. Sie können nun das Prinzip der geringsten Rechte anwenden und integrierte privilegierte Konten identifizieren. Sie wissen auch, wann Sie Arbeitsstationen mit privilegiertem Zugriff verwenden sollten.

**Beschreiben der Windows Server-Verwaltungstools**

**Lernziele:**

* Windows Admin Center beschreiben.
  + Windows Admin Center ist eine modulare Webanwendung, die aus den folgenden vier Modulen besteht:
    - Server-Manager
    - Failovercluster
    - Hyperkonvergente Cluster
    - Windows 10-Clients
  + Windows Admin Center verfügt über zwei Hauptkomponenten:
    - **Gateway**. Das Gateway verwaltet Server mithilfe von PowerShell-Remoting und der Windows-Verwaltungsinstrumentation (WMI) über die Windows-Remoteverwaltung (WinRM).
    - **Webserver.** Die Webserver-Komponente überwacht HTTPS-Anforderungen und stellt die Benutzeroberfläche für den Webbrowser auf der Verwaltungsstation dar. Dabei handelt es sich nicht um eine vollständige Installation von Internetinformationsdienste (IIS), sondern um einen Mini-Webserver für diesen speziellen Zweck.
  + Da Windows Admin Center ein webbasiertes Tool ist, das HTTPS verwendet, ist ein X.509-Zertifikat erforderlich, um die SSL-Verschlüsselung zu ermöglichen. Mit dem Installations-Assistenten können Sie entweder ein selbstsigniertes Zertifikat verwenden oder Ihr eigenes SSL-Zertifikat bereitstellen. Das selbstsignierte Zertifikat läuft 60 Tage nach der Erstellung ab.
  + Vorteile von Windows Admin Center: Einfache Installation und Verwendung; Ergänzung zu vorhandenen Lösungen; Verwaltung über das Internet; Erhöhte Sicherheit; Azure-Integration; Erweiterungen; Keine externen Abhängigkeiten.
  + Nachdem Sie Windows Admin Center heruntergeladen und installiert haben, müssen Sie TCP-Port 6516 in der lokalen Firewall aktivieren.
  + Während des Setups werden Sie aufgefordert, einen TCP-Port auszuwählen.
  + Wenn Sie Windows Admin Center auf einem Arbeitsgruppencomputer installieren, werden Sie aufgefordert, Windows Admin Center die Verwaltung der TrustedHosts-Einstellung des lokalen Computers zu gestatten. Wenn Sie diese Einstellung umgehen, müssen Sie „TrustedHosts“ manuell konfigurieren.
  + Sie können die Einstellungen für die vertrauenswürdigen Hosts mithilfe des folgenden Windows PowerShell-Befehls in einem Windows PowerShell-Fenster mit erhöhten Rechten konfigurieren. Sie können die Remote Hosts über IP, FQDN oder den NetBIOS-Namen angeben:
    - Set-Item WSMan:localhost\Client\TrustedHosts -Value 'SEA-DC1.Contoso.com'
  + TIPP: Sie können auch eine Platzhaltereinstellung verwenden: Set-Item WSMan:\localhost\Client\TrustedHosts -Value '\*'
* Die Verwendung von Remoteserver-Verwaltungstools (RSAT) zum Verwalten von Servern beschreiben.
  + Sie können die aktuelle Version von Server-Manager verwenden, um den lokalen Server zu verwalten und bis zu 100 weitere Server remote zu verwalten.
  + In der Server-Manager-Konsole müssen Sie Remoteserver, die Sie verwalten möchten, manuell hinzufügen. IT-Administratoren verwenden Server-Manager häufig zur Remoteverwaltung von Server Core-Installationen.
  + Server-Manager ist im Lieferumfang von RSAT für Windows 10 enthalten. Sie können ihn jedoch nur zum Verwalten von Remoteservern verwenden. Sie können Server-Manager nicht zum Verwalten von Clientbetriebssystemen verwenden.
  + Server-Manager öffnet zunächst ein Dashboard, das den schnellen Zugriff auf folgende Komponenten ermöglicht:
    - Konfigurieren des lokalen Servers.
    - Hinzufügen von Rollen und Features.
    - Hinzufügen weiterer zu verwaltender Server.
    - Erstellen einer Servergruppe.
    - Herstellen einer Verbindung zwischen diesem Server und Clouddiensten.
  + Auf dem Knoten des „Lokaler Server“ können Sie verschiedene Arten der Erstkonfiguration durchführen, die mit denen vergleichbar sind, die Sie mit dem Sconfig-Tool konfigurieren können, beispielsweise:
    - Computername und Domänenmitgliedschaft
    - Windows-Firewall-Einstellungen
    - Remotedesktop
    - Netzwerkeinstellungen
    - Windows Update-Server
    - **Zeitzone**
    - Aktivierung von Windows
  + Sie müssen RSAT unter Windows 10 nicht mehr herunterladen und installieren. Ab Windows 10 1803 können Sie RSAT über die Einstellungen-App aktivieren.
  + Bis zur Einführung von Windows Admin Center waren die RSAT-Konsolen die hauptsächlichen grafischen Tools für die Verwaltung des Windows Server-Betriebssystems.
  + RSAT für Windows 10 besteht aus folgenden Verwaltungstools: Tools für Active Directory-Zertifikatdienste; AD DS-Tools (Active Directory Domain Services) und AD LDS-Tools (Active Directory Lightweight Directory Services); Verwaltungsdienstprogramme für die BitLocker-Laufwerkverschlüsselung; DHCP-Servertools; DNS-Servertools; Failoverclusteringtools; Tools für Dateidienste; Verwaltugnstools für Gruppenrichtlinien; Tools für die IP-Adressverwaltung (IPAM); Netzwerkcontroller-Verwaltungstools; Tools für Netzwerklastenausgleich; Tools für die Remotezugriffsverwaltung; Tools für Remotedesktopdienste; Server-Manager; Tools für geschützte VMs; Verwaltungstools für den Speichermigrationsdienst; Speicherreplikatmodul für Windows PowerShell; Volumenaktivierungstools; Windows Server Update Services-Tools.

* Server-Manager beschreiben.
  + Server-Manager ist eine Verwaltungskonsole in Windows Server, die IT-Experten dabei hilft, lokale und remote windowsbasierte Server aus ihren Desktops bereitzustellen und zu verwalten, ohne physischen Zugriff auf Server zu benötigen, oder die Notwendigkeit, Remotedesktopprotokollverbindungen (rdP) für jeden Server zu aktivieren.
  + Die Aufgaben des Service Managers sind vielfältig und er hat auch eine große Verantwortung: er ist der erste Ansprechpartner für den Kunden in die IT-Organisation er vertritt die Interessen des Kunden gegenüber der internen IT-Organisation, insbesondere zur Einhaltung der vereinbarten SLA.
* Die Verwendung von Windows PowerShell zum Verwalten von Servern beschreiben.
  + Mit dem folgenden Befehl wird eine Liste der Dienste angezeigt, die gerade ausgeführt werden.
    - Get-Service | Where-Object {$\_.Status -eq "Running"}
  + Mit dem folgenden Befehl wird eine Liste der Dienste angezeigt, deren Name mit „win“ beginnt, und der Dienst „WinRM“ ausgeschlossen.
    - Get-Service -Name "win\*" -Exclude "WinRM"
  + Der nächste Befehl gibt eine Liste aller Dienste in eine Textdatei aus, die für die HTML-Ausgabe formatiert ist.
    - Get-Service | ConvertTo-Html > File.html
  + Eine Variation des vorangehenden Befehls gibt nur ausgewählte Daten über Dienste aus und exportiert die Ausgabe dann in eine CSV-Datei.
    - Get-Service | Select-Object Name, Status | Export-CSV c:\service.csv
  + Der folgende Befehl ruft die angegebenen Informationen (Bürotelefonnummer und Benutzerprinzipalname) über Active Directory-Benutzer ab.
    - Get-ADUser -Filter \* -Properties OfficePhone | FT OfficePhone,UserPrincipalName
  + Dieses letzte Beispiel ruft eine Teilmenge der AD DS-Benutzer ab (die Benutzer in der Organisationseinheit „Marketing“) und ändert ihre Eigenschaften, indem jedem Konto eine Beschreibung hinzugefügt wird.
    - Get-ADUser -Filter 'Name -like "\*"' -SearchBase "OU=Marketing,DC=Contoso,DC=Com" | Set-ADUser -Description "Member of the Marketing Department"
  + Die ISE ist eine vollständig grafische Umgebung, die einen Skript-Editor, Debuggingfunktionen, eine interaktive Konsole und mehrere Tools bereitstellt, mit denen Sie neue Windows PowerShell-Befehle entdecken und erlernen können. Dieses Modul vermittelt ein grundlegendes Wissen über die Funktionsweise der ISE.
* Erklären, wie Sie Windows PowerShell verwenden, um einen Server remote zu verwalten.
  + Der Zweck von Windows PowerShell-Remoting besteht darin, eine Verbindung mit Remotecomputern herzustellen, damit Sie Befehle auf diesen Computern ausführen und die Ergebnisse dann zurück an den lokalen Computer weiterleiten können. Dies ermöglicht Ihnen, Windows PowerShell-Befehle auf mehreren Computern in Ihrem Netzwerk von Ihrem Clientcomputer aus auszuführen, anstatt mit jedem Computer eine Verbindung herzustellen zu müssen.
  + Ein wichtiges Ziel von Windows PowerShell-Remoting besteht darin, die Batchverwaltung zu aktivieren. Dadurch können Sie Befehle für eine Gruppe von Remotecomputern gleichzeitig ausführen. Remoting kann auf eine von drei Arten verwendet werden:
    - **1:1-Remoting:**
      * Im 1:1-Remotingszenario (auch als *interaktives Remoting* bezeichnet) stellen Sie eine Verbindung zu einem einzelnen Remotecomputer her und führen Windows PowerShell-Befehle auf diesem Computer aus, genau so, als ob Sie sich auf dem Computer angemeldet und ein Windows PowerShell-Fenster geöffnet hätten.
    - **1:n-Remoting:** 
      * Im 1: n-Remotingszenario (auch als *Fan*-*Out-Remoting* bezeichnet) geben Sie einen Befehl aus, der auf einem oder mehreren Remotecomputern parallel ausgeführt wird. Sie arbeiten nicht interaktiv mit jedem Remotecomputer. Stattdessen werden Ihre Befehle in einem Stapel ausgegeben und ausgeführt, und die Ergebnisse werden zur Weiterverwendung an Ihren Computer zurückgegeben.
    - **n:1-Remoting:**
      * Im n:1-Remotingszenario (auch als *Fan-In-Remoting* bezeichnet) stellen mehrere Administrator\*innen Remoteverbindungen mit einem einzelnen Computer her. Normalerweise verfügen diese Administratoren über unterschiedliche Berechtigungen für denselben Remotecomputer und arbeiten möglicherweise in einer eingeschränkten Windows PowerShell-Sitzung.
  + ACHTUNG: Wenn Sie Befehle auf mehreren Computern ausführen, beachten Sie die Unterschiede zwischen den Remotecomputern, wie z. B. unterschiedliche Betriebssysteme, Dateisystemstrukturen und Systemregistrierungen.
  + Viele Administratoren führen einige Ihrer Server in virtualisierten Umgebungen aus. Um eine einfachere Verwaltung von Hyper-V-VMs mit Windows 10 oder Windows Server zu ermöglichen, können Sie ein Feature namens PowerShell Direct verwenden.
  + Mit PowerShell Direct können Sie ein Windows PowerShell-Cmdlet oder -Skript innerhalb einer VM vom Hostbetriebssystem aus ausführen, unabhängig von Netzwerk-, Firewall- und Remoteverwaltungskonfigurationen.
  + Für Remoting muss Windows PowerShell auf dem lokalen Computer vorhanden und Windows-Remoteverwaltung auf allen Remotecomputern aktiviert sein, mit denen eine Verbindung hergestellt werden soll. Außerdem müssen Sie Windows PowerShell-Remoting aktivieren.
  + Zum Aktivieren von Windows PowerShell-Remoting führen Sie mit erhöhten Rechten oder als Admin folgenden Befehl aus:
    - Winrm quickconfig
    - **oder**
    - Enable-PSremoting –force
  + Um die Remoteverwaltung durchführen zu können, müssen Administratoren über folgende Berechtigungen verfügen:
    - Verbinden mit dem Remotecomputer
    - Ausführen von Windows PowerShell
    - Zugreifen auf Datenspeicher und die Registrierung auf dem Remotecomputer
  + ACHTUNG: Das Aktivieren von Remoting auf Computern mit einer Netzwerkschnittstellenkarte (NIC), die dem Netzwerkadressenprofil „Öffentlich“ zugeordnet ist, erzeugt einen Fehler. Sie können Enable-PSremoting -force verwenden, um diese Einschränkung zu umgehen und das Remoting auf einem Gerät mit einer öffentlichen NIC zu erzwingen.

**Zusammenfassung**

Die IT-Mitarbeiter bei Contoso sind damit beschäftigt, lokale Contoso-Server zu Windows Server 2022 zu migrieren. Als Windows Server-Administrator sind Sie für die Verwaltung und Wartung der Serverinfrastruktur zuständig, die Contoso dabei hilft, die Geschäftsziele zu erreichen. Sie haben die verfügbaren Windows Server-Verwaltungstools untersucht, einschließlich Windows Admin Center, Remoteserver-Verwaltungstools, Server-Manager und Windows PowerShell. Sie können jetzt die verschiedenen für die Verwaltung einer Windows Server-Bereitstellung zur Verfügung stehenden Verwaltungstools beschreiben und das geeignete Tool für eine bestimmte Situation auswählen.

**Konfigurieren von Windows Server nach der Installation**

**Lernziele:**

* Erläutern der Konfiguration nach der Installation und Beschreiben der verfügbaren Tools für die Konfiguration nach der Installation
  + Wenn Sie Windows Server mit den Standardeinstellungen des lokalen Installationsmediums installieren, werden einige Einstellungen automatisch konfiguriert:
    - Computername
    - Arbeitsgruppe
    - Netzwerkeinstellungen
    - Zeitzone
    - Gebietsschema und Spracheinstellungen
    - Rollen und Features
    - Firewalleinstellungen
    - Aktivierung
  + Einige Einstellungen müssen neu konfiguriert werden. Verfügbare Tools dafür sind:
    - Server-Manager
    - Windows Admin Center
    - Desired State Configuration (DSC)
    - Antwortdateien (XML-Textdateien)
* Verwenden von SCONFIG zum Konfigurieren von Windows Server.
  + SCONFIG ist ein textbasiertes Tool, mit dem Sie die grundlegende Konfiguration von Server Core zur Vorbereitung auf die Verwendung in Ihrer Produktionsumgebung durchführen können.
  + In der Regel wird SCONFIG verwendet, um die Erstkonfiguration direkt nach Abschluss der Installation durchzuführen. Sie können das Tool jedoch jederzeit ausführen, um die Einstellungen nach Bedarf zu ändern.
  + SCONFIG bietet verschiedene Optionen:
    - Domäne/Arbeitsgruppe
    - Computername
    - Lokalen Administrator hinzufügen
    - Remoteverwaltung konfigurieren
    - Windows Update-Einstellungen
    - Updates herunterladen und installieren
    - Netzwerkeinstellungen
    - Datum und Uhrzeit
    - Telemetrieeinstellungen
    - Aktivierung von Windows
    - Benutzer abmelden
    - Server neu starten
    - Server herunterfahren
    - Beenden und zurück zur Befehlszeile
* Beschreiben von DSC (Desired State Configuration) und Erläutern der Verwendung von DSC zum Konfigurieren von Windows Server
  + DSC ist eine auf PowerShell basierende Verwaltungsplattform, mit der Sie Ihre Server und die zugehörige IT-Infrastruktur verwalten können. DSC besteht aus drei Komponenten:
    - Configurations
    - Ressourcen
    - LCM
  + Die LCM Komponente wird intensiv genutzt, diese dient als Ausführungs-Engine für die Windows PowerShell DSC-Skripts.
  + LCM ist zuständig für:
    - Koordinieren der Implementierung von Einstellungen, die in DSC-Skripts definiert sind
    - Überwachen des aktuellen Status dieser Einstellungen
    - Aktualisieren des Status eines Computers entsprechend einem gewünschten Status
  + Jedes Mal, wenn der LCM ausgeführt wird, werden die folgenden Schritte ausgeführt:
    - **Abrufen**: Damit wird der aktuelle Status des Computers abgerufen.
    - **Testen**: Damit wird der aktuelle Status des Computers mithilfe eines kompilierten DSC-Skripts (MOF-Datei) mit dem gewünschten Status abgeglichen.
    - **Festlegen**: Damit wird die Konfiguration des Computers entsprechend dem gewünschten Status geändert, der in der MOF-Datei beschrieben ist.
  + Sie können DSC-Konfigurationen entweder im Pushmodus oder im Pullmodus bereitstellen:
    - **Push:**
      * In diesem Modus senden (*pushen*) Sie die gewünschten Konfigurationen manuell an einen oder mehrere verwaltete Computer. Die LCM-Komponente stellt sicher, dass der Status aller verwalteten Computer mit Ihren Konfigurationsvorgaben übereinstimmt.
    - **Pull:** 
      * In diesem Modus befinden sich die Konfigurationsinformationen auf einem *Pullserver*. Die LCM-Komponente auf den einzelnen verwalteten Computern fragt den Pullserver in regelmäßigen Abständen ab (das Standardintervall sind 15 Minuten), um die neuesten Konfigurationsdetails abzurufen. Der Pullserver sendet dann die Details zu etwaigen Konfigurationsänderungen zurück an alle verwalteten Computer.
  + Anforderungen für DSC mit Windows:
    - Betriebssystem: Auf den verwalteten Computern muss Windows 8.1 oder höher bzw. Windows Server 2012 R2 oder höher ausgeführt werden.
    - Windows-Remoteverwaltung: Auf verwalteten Computern muss die Windows-Remoteverwaltung (WinRM) aktiviert sein.
  + Mit DSC können Sie den gewünschten Status für Folgendes definieren:
    - Ein Betriebssystem
    - Eine Anwendung
  + Sie können ein Skript verwenden, um DSC zu definieren. Wenn Sie Ihre Konfiguration erstellt und kompiliert haben, können Sie sie Computern zuweisen, die dann diese Konfiguration erhalten.
* Verwenden von Windows Admin Center zum Durchführen der Konfiguration nach der Installation
  + Sie können auch Windows Admin Center zum Durchführen der Konfiguration nach der Installation verwenden. Der Vorgang beginnt, wenn Sie den neu bereitgestellten Server zur Windows Admin Center-Konsole hinzufügen.
  + Nachdem Sie den neu bereitgestellten Server hinzugefügt und diesen verbunden haben, können Sie die erforderlichen Konfigurationsänderungen mit Windows Admin Center vornehmen. Aktualisieren Sie zunächst den Computernamen und die Domänenmitgliedschaft.
    - Wählen Sie auf der Registerkarte Übersicht im Bereich Übersicht die Schaltfläche Computer-ID bearbeiten aus.
    - Geben Sie auf dem Blatt Computer-ID bearbeiten den Namen des neuen Computers ein, und wählen Sie anschließend Domäne aus.
    - Geben Sie den Domänennamen ein, und wählten Sie „Weiter“ aus.
* Implementieren von Antwortdateien zum Durchführen der Konfiguration