Automatisieren der Systemverwaltung

Wojciech Micka
Presales Consultant Microsoft Deutschland GmbH

Themen dieser Sitzung:

- Sammeln von Informationen mit Remote Helpdesk
- Remote Helpdesk-Verwaltung
- Active Directory-Verwaltung
- Druckerverwaltung
- WMIC-Verwaltung

Agenda

- Remote Helpdesk-Informationen
- Remote Helpdesk-Verwaltung
- Active Directory-Verwaltung
- Druckerverwaltung
- WMIC-Verwaltung

Remote Helpdesk-Informationen
Abrufen allgemeiner Systeminformationen

- Systeminfo.exe
  - Ruft grundlegende Systeminformationen ab
  - Betriebssystemversion und Funktion, Hardwareeinstellungen usw.
  - Beispiel: systeminfo /S \\wkstn1 >c:\sysinfo.txt
    - Abfrage von wkstn1, Ausgabe in c:\sysinfo.txt
- SC
  - Kommuniziert mit Dienststeuerungs-Manager
  - Ruft Dienste ab, die auf einem System ausgeführt werden
  - Beispiel: sc \\server2 query
    - Fragt Dienste ab, die auf Server2 ausgeführt werden

Remote Helpdesk-Informationen
Abrufen von Informationen aus Protokollen

- DriverQuery
  - Zeigt eine Liste der installierten Gerätetreiber an
  - Ruft Status von Gerätetreibern ab
  - Beispiel: driverquery /s server2
    - Zeigt eine Liste der Treiber auf Server2 an
- EventQuery
  - Listet Ereigniseigenschaften aus Ereignisprotokollen auf
  - Ausgabe in eine Datei möglich
  - Beispiel: eventquery /L anwendung
    - Listet Ereignisse aus dem Anwendungsereignisprotokoll auf

Remote Helpdesk-Informationen
Abrufen von Informationen zur Hardware

- Getmac
  - Zeigt die MAC-Adresse für ein System
  - Beispiel: getmac /s server2
    - Ermittelt die MAC-Adresse für Server2
- Freedisk
  - Zeigt den freien Speicherplatz auf einer Festplatte an
  - Bietet Informationen darüber, ob der erforderliche Speicherplatz verfügbar ist
  - Beispiel: freedisk /d c: 4GB
    - Zeigt an, ob 4 GB auf Laufwerk “c” frei sind

Remote Helpdesk-Informationen
Informationen zu Gruppenrichtlinien

- GPResult
  - Zeigt Richtlinienergebnissatz (Resultant Set of Policy oder RSoP) für Benutzer und Computer an
  - Kann kurze oder ausführliche Informationen anzeigen
  - Bietet Informationen darüber, ob die richtigen Gruppenrichtlinien angewendet wurden
  - Beispiel: gpresult /user KimA
    - Zeigt die Gruppenrichtlinien für den Benutzer KimA an

Agenda

- Remote Helpdesk-Informationen
- Remote Helpdesk-Verwaltung
- Active Directory-Verwaltung
- Druckerverwaltung
- WMIC-Verwaltung
- Sonstige Tools

Remote Helpdesk-Verwaltung

Abrufen von Informationen zu geöffneten Dateien

- Openfiles
  - Zeigt eine Liste der auf einem System geöffneten Dateien an
  - Kann genutzt werden, um zu überprüfen, ob eine Datei gerade verwendet wird
- Beispiel: openfiles /query –s server2
  - Zeigt eine Liste der auf Server2 geöffneten Dateien an
- Szenarien:
  - Überprüfen, welche Dateien geöffnet sind
  - Überprüfen, welche Dateien gesperrt sind

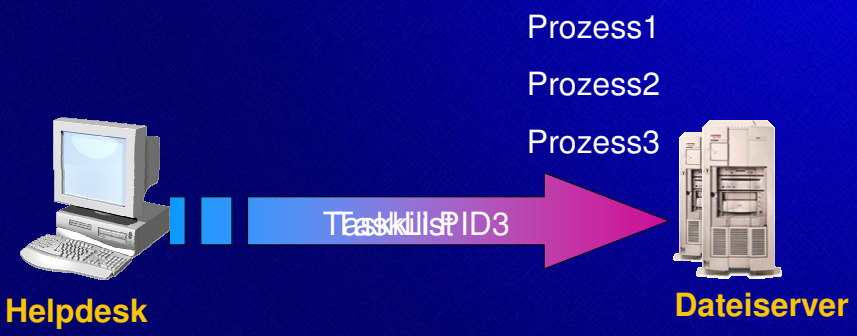
Remote Helpdesk-Verwaltung
Abrufen von Informationen zu Prozessen

- **Tasklist**
  - Zeigt eine Liste der auf einem lokalen oder Remotesystem ausgeführten Prozesse an
  - Ersetzt Dienstprogramm "Tlist.exe" des Windows 2000 Resource Kits (Die technische Referenz)
  - Kann für ein lokales oder ein Remotesystem ausgeführt werden
- **Beispiel: tasklist /s server2**
  - Zeigt die auf Server2 ausgeführten Prozesse an
- **Szenarien:**
  - Ermitteln, welche Prozesse ausgeführt werden
  - Ermitteln von Prozesskennungen (Process IDs oder PIDs)

Remote Helpdesk-Verwaltung
Beenden der Prozessausführung

- **Taskkill**
  - Zum Beenden eines aktuellen Prozesses
  - Prozess wird auf der Basis der PID oder dem Abbildnamen beendet
  - Ersetzt Dienstprogramm "kill.exe" des Windows 2000 Resource Kits (Die technische Referenz)
  - Kann für ein lokales oder ein Remotesystem ausgeführt werden
- **Beispiel: taskkill /IM notepad.exe**
  - Beendet die Ausführung von "Notepad.exe" auf dem lokalen System
- **Szenarien:**
  - Beenden eines Prozesses, der Serverressourcen belegt
  - Beenden eines Prozesses mit gesperrten Datendateien

Remote Helpdesk-Verwaltung
Verwenden von Tasklist und Taskkill



Demo
Remote Helpdesk-Verwaltung

Verwenden von Tasklist und Taskkill zum Beenden eines Prozesses

Agenda

- Remote Helpdesk-Informationen
- Remote Helpdesk-Verwaltung
- Active Directory-Verwaltung
- Druckerverwaltung
- WMIC-Verwaltung

Active Directory-Verwaltung
Active Directory-Pfadnamen

- Komponenten des Active Directory-Pfades
  - dc= Domänenkomponente (Domain Component)
  - ou= Organisationseinheit (Organization Unit)
  - cn= Allgemeiner Name (Common Name) für Benutzer oder Container
- Beispiel:
  - cn=kima,cn=users,dc=worldwideimporters,dc=com
  - Das Benutzerkonto ist "kima", der Container "Users", die Domäne "WorldWideImporters.com"
- Beispiel:
  - cn=aaronc,ou=sales,dc=worldwideimporters, dc=com
  - Das Benutzerkonto ist "aaronc", die Organisationseinheit "Sales", die Domäne "WorldWideImporters.com"

Active Directory-Verwaltung
Hinzufügen von Objekten zu Active Directory

- DSAdd
  - Fügt Benutzer, Gruppen, Computer, Organisationseinheiten usw. hinzu
  - Kann zur Automatisierung von Massenänderungen am Verzeichnis verwendet werden
- Beispiel:
  - Benutzer dsadd "CN=KimA,OU=Sales,DC=worldwideimporters,DC=com"
  - Fügt den Benutzer KimA zur Organisationseinheit "Sales" in der Domäne "WorldWideImporters.com" hinzu

Active Directory-Verwaltung
Entfernen von Objekten aus Active Directory

- DSRM
  - Entfernt Objekte aus dem Verzeichnis
  - Kann sich wiederholende Aufgaben wie das Löschen von nicht mehr benötigten Konten automatisieren
- Beispiel:
  - dsrm -noprompt -c "cn=AndreasB,OU=Sales,DC=worldwideimporters,DC=com"
  - Entfernt AndreasB aus der Organisationseinheit "Sales" in der Domäne "WorldWideImporters.com"

Active Directory-Verwaltung
Abrufen von Daten aus Active Directory

- DSGet
  - Ruft Informationen zu einem einzelnen Objekt im Verzeichnis ab
  - Benutzereigenschaften wie Gruppenmitglieldschaften usw.
- DSQuery
  - Ruft Informationen zu mehreren Objekten in einem angegebenen Pfad ab (Container oder Organisationseinheit)
- Verwendungsmöglichkeiten
  - Generieren von Informationen und Statistiken zu Active Directory-Objekten
  - Gruppenmitgliedschaften, Telefonnummern usw.

Active Directory-Verwaltung
Abrufen von Daten aus Active Directory

- Beispiel DSGet:
  - dsget user "CN=TomG,OU=Sales,DC=worldwideimporters, DC=Com" -memberof –expand
  - Ruft Informationen zum Benutzer TomG ab, einschließlich der Gruppen und Organisationen, in denen der Benutzer Mitglied ist
- Beispiel DSQuery:
  - dsquery user "OU=Sales,DC=worldwideimporters,DC=com"
  - Zeigt die Benutzer in der Organisationseinheit "Sales" an

Active Directory-Verwaltung
Verschieben von Active Directory-Objekten

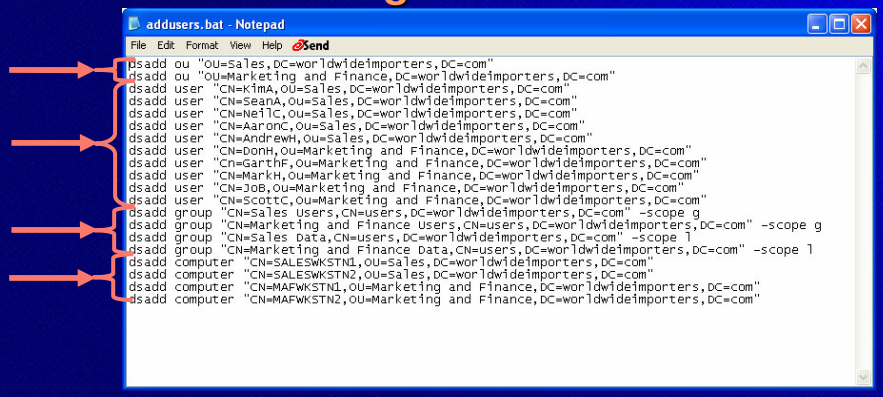
- DSMove
  - Verschiebt ein Objekt oder benennt es um
- Beispiel:
  - dsmove "CN=KimA, OU=Sales, DC=worldwideimporters, DC=com" -newparent "OU=Marketing and Finance, DC=worldwideimporters, DC=com"
  - Verschiebt den Benutzer KimA in die Organisationseinheit "Sales" aus der Organisationseinheit "Marketing and Finance"
- Verwendungsmöglichkeiten
  - Suche nach Benutzerkonten nach einer Neustrukturierung

Active Directory-Verwaltung
Ändern von Active Directory-Objekten

- DSMod
  - Ändert ein vorhandenes Objekt in Active Directory
  - Zum Ändern von Namen oder Gruppenmitgliedschaften
- Beispiel:
  - dsmod user "CN=SeanA, OU=Sales, DC=worldwideimporters, DC=com" -pwd Abcd123 -mustchpwd yes
  - Hierdurch wird das Benutzerkenntwort geändert, so dass es bei der nächsten Anmeldung neu festgelegt werden muss.
- Verwendungsmöglichkeiten
  - Ändern von Kennwörtern in großem Umfang
  - Aktualisieren von Gruppenmitgliedschaften in großem Umfang

Active Directory-Verwaltung

Verwenden von Skripts für sich wiederholende Aufgaben



Demo
Active Directory-Verwaltung

Automatisieren von Active Directory-Aufgaben

Agenda

- Remote Helpdesk-Informationen
- Remote Helpdesk-Verwaltung
- Active Directory-Verwaltung
- Druckerverwaltung
- WMIC-Verwaltung

Druckerverwaltung
Druckerkonfiguration

- Prncnfg
  - Zeigt die Druckerkonfiguration auf einem lokalen oder einem Remotesystem an
  - Legt Druckereigenschaften fest (Name, Priorität, Anschluss usw.)
- Beispiel:
  - prncnfg –g –s Server1 –p HPLaser
  - Zeigt die Konfiguration von HPLaser auf Server1 an
- Verwendungsmöglichkeiten
  - Festlegen und Überprüfen von Druckerkonfigurationseigenschaften

Druckerverwaltung
Hinzufügen von Druckern und Anschlüssen

- Prnport
  - Zum Erstellen eines TCP/IP-Druckeranschlusses
  - Beispiel: prnport –a –s Server1 –r 10.0.1.24
  - Erstellt einen neuen TCP/IP-Anschluss mit der Adresse 10.0.1.24 auf Server1
- Prnmngr
  - Verwaltet lokale und Remotedrucker
  - Zum Löschen eines Druckers, Abrufen von Druckerinformationen usw.
  - Beispiel: prnmngr –d HPLaser –s Server1
    - Löscht HPLaser von Server1

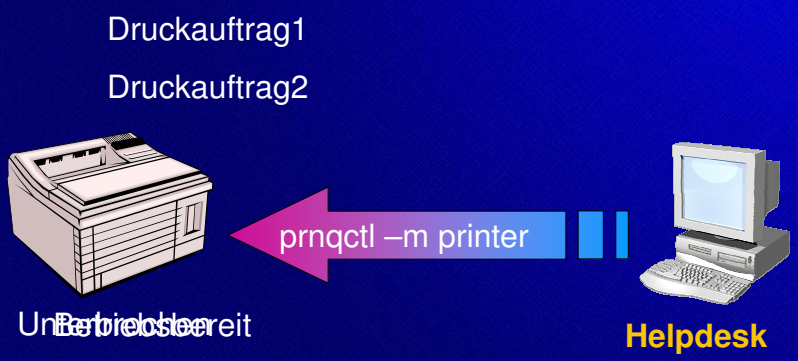
Druckerverwaltung
Verwaltung von Druckertreibern

- Prndrvr
  - Zum Verwalten von Druckertreibern
  - Zum Hinzufügen/Überprüfen/Löschen von installierten Druckertreibern
- Beispiele:
  - prndrvr –l –s Server1
    - Listet die auf Server1 installierten Druckertreiber auf
  - Prndrvr –a –m "PrinterDriver" –v X –e "Windows NT X86" –s Server1
    - Fügt einen Druckertreiber PrinterDriver (Version X) auf Server1 hinzu und legt ihn als Windows NT-Treiber fest

Druckerverwaltung
Verwaltung von Druckaufträgen

- Prnjobs
  - Zum Verwalten von Druckaufträgen
    - Anhalten, Fortsetzen, Abbrechen, Liste anzeigen usw.
  - Beispiel: prnjobs –l –s Server1
    - Zeigt eine Liste der Druckaufträge auf Server1 an
- Prnqctl
  - Dieser Befehl verwaltet Druckerwarteschlangen
  - Beispiel: prnqctl –m HPLaser –s Server1
    - Setzt den Druckvorgang des Druckers HPLaser auf Server1 fort

Druckerverwaltung
PRNQCTL zum Fortsetzen eines Druckvorgangs



Agenda

- Remote Helpdesk-Informationen
- Remote Helpdesk-Verwaltung
- Active Directory-Verwaltung
- Druckerverwaltung
- WMIC-Verwaltung

WMIC-Verwaltung
Windows-Verwaltungsinstrumentation

- Einfache Befehlszeilenschnittstelle für Windows-Verwaltungsinstrumentation (Windows Management Instrumentation oder WMIC)
- Bietet eine einfache Befehlszeilenschnittstelle
  - Unterstützt interaktiven Modus
- Interoperabilität mit vorhandenen Shells und Dienstprogrammen
- Kann durch Skripts erweitert werden

WMIC-Verwaltung
Anzeigen von Prozesskennungen

- Anzeigen von Prozesskennungen (Process IDs oder PIDs) für die Ausführung von Prozessen
- Zum Identifzieren von Prozessen, die beendet werden sollen
- Beispiel: WMIC PROCESS WHERE Name="svchost.exe" GET name, processid
  - Stellt PIDs für alle Prozesse mit dem Namen "svchost.exe" zur Verfügung

WMIC-Verwaltung
Starten einer Anwendung

- Zum Starten und Beenden von Prozessen
  - Helpdesk-Mitarbeiter können eine Anwendung (z. B. einen Sicherungsvorgang) von einem Remotestandort aus starten
- Beispiel: WMIC PROCESS CALL Create "calc.exe"
  - Hierdurch wird der Windws Rechner gestartet
- Dies sind nur einige der vielen Verwendungsmöglichkeiten von WMIC

WMIC-Verwaltung
Verwendungsmöglichkeiten

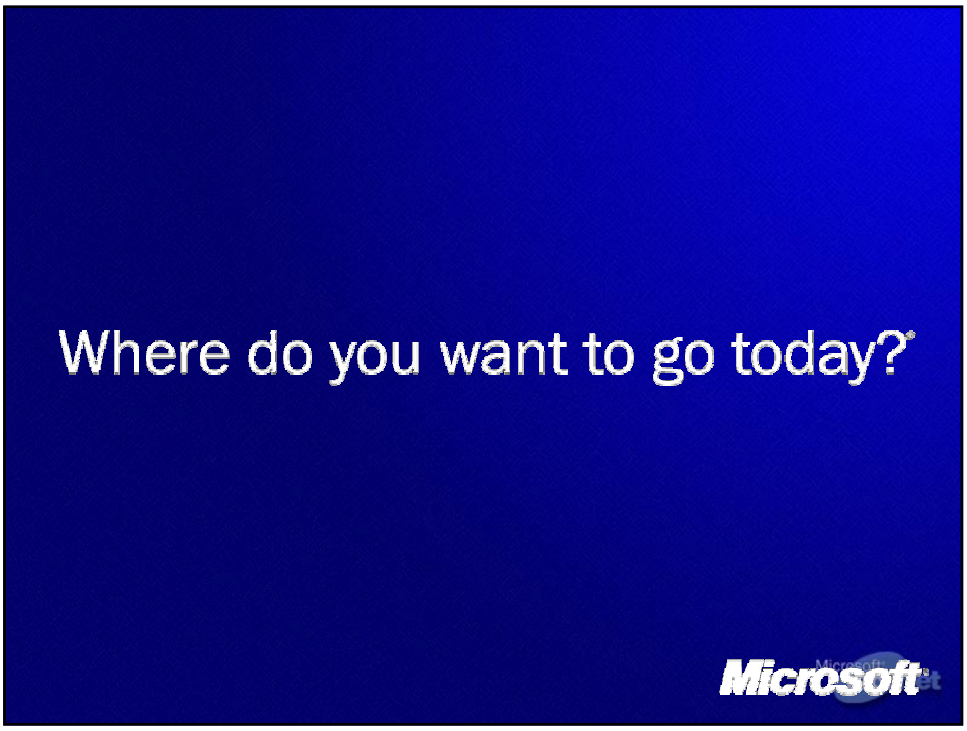
- Einfaches Erstellen von Skripts für Verwaltungsaufgaben
- Konfigurieren von Computereinstellungen
- Starten, Beenden und Steuern von Systemprozessen
- Abfragen von lokalen und von Remotecomputern
  - Anzeigen von Informationen zum Betriebssystem und zur Festplatte
- Ereignisabfragen und Ausgaben mit Ergebnissen in formatierten HTML-Tabellen

Sonstige Tools

- Delprof – W2k3 Resource Kit Tool zum Löschen von Benutzerprofilen
  - Delprof /p /c:Server2 /d:100
    - löscht alle Profile auf Server2, die seit mind. 100 Tagen nicht mehr aktiv waren

Zusammenfassung

- Mehr als 60 neue Befehlszeilenprogramme
  - Verwalten und Abrufen der Systemkonfiguration
- Tools sind auf Remotecomputern einsetzbar
  - Arbeiten auf lokalen und auf Remotesystemen
  - Abrufen von Anmeldeinformationen zur Laufzeit
- Automatisieren häufiger oder komplexer Aufgaben
  - Abrufen von Tools über Skripts
- Schnellere Skripterstellung
  - Verwenden dieser Tools für komplexe Aufgaben


Where do you want to go today?
Microsoft