

Unterrichtseinheit 14:

Verwalten eines Windows2000-Netzwerkes

Windows2000 bietet bei der Verwaltung des Netzwerkes sehr große Flexibilität. Es stellt unter anderem die folgenden Tools und Methoden bereit:

- Terminaldienste
- SNMP
- SNMP-Dienst

Terminaldienste

Mit Hilfe der Terminaldienste kann man interaktive Sitzungen auf einem Remoteserver starten und den Server von einem Clientcomputer aus verwalten. Der Desktop des Servers wird in einem Fenster auf dem Desktop des lokalen Computers angezeigt. Der Terminaldiensteclient sendet Tastenanschläge und Mausbewegungen an den Terminalserver und empfängt Bildschirmaktualisierungen vom Server.

Um die Terminaldienste für Remoteverwaltung verwenden zu können, muss der Computer über folgende Systemanforderungen verfügen:

- Windows2000 Server-Betriebssystem
- Terminaldienste auf dem Server und dem Clientcomputer installieren
- genügend großer Arbeitsspeicher (jede aktive Sitzung erfordert ca. 16MB RAM auf dem Server zuzüglich Programmressourcen)

Remoteverwaltungsmodus

Die Merkmale dieses Modus sind folgende:

- die Terminaldienste sind auf zwei gleichzeitige Verbindungen beschränkt
- zwei Terminaldienstelizenzen sind enthalten
- die Leistung der Terminaldienste ist für eine geringe Anzahl an Verbindungen optimiert
- für die Terminaldienste sind strengere Sicherheitseinstellungen als im Anwendungsservermodus konfiguriert
- standardmäßig haben nur die Mitglieder der Gruppe **Administratoren** die Berechtigungen zum Verbinden mit dem Remotecomputer

Zum Installieren der Terminaldienste sind folgende Schritte notwendig:

*Systemsteuerung → Software → Windows-Komponenten hinzufügen/entfernen → Windows-Komponenten → aktivieren des Kontrollkästchens **Terminaldienste** → Setup der Terminaldienste → Remoteverwaltungsmodus → Weiter → Fertig stellen → Ja*

Leistungsparameter, um die Leistung der Terminaldienstesitzung zu verbessern können wie folgt konfiguriert werden:

Systemsteuerung → System → Erweitert → Systemeigenschaften → Systemleistungsoptionen → Systemleistung optimieren für → Hintergrunddienste

Zum Optimieren der Ressourcenverfügbarkeit sollten die maximale Leerlaufdauer auf 10 Minuten und das Zeitlimit zum Beenden einer getrennten Sitzung auf 5 Minuten festgelegt werden.

*Programme → Verwaltung → Terminaldienstekonfiguration → Sitzungen → Eigenschaften von RDP-Tcp → aktivieren von **Benutzereinstellungen überschreiben** → **Maximale Leerlaufdauer auf 10 Minuten** und **Getrennte Sitzung beenden auf 5 Minuten** einstellen*

Der Administratorzugriff (Sicherheitsparameter) kann wie folgt konfiguriert werden:

*Programme → Verwaltung → Terminaldienstekonfiguration → Verbindungen → mit rechter Maustaste auf **RDP-Tcp** klicken → Eigenschaften → Berechtigungen → nur Gruppen ausgewählter Administratoren die Berechtigung Vollzugriff zuweisen → alle anderen Benutzerkonten und -gruppen (ausgenommen **System**) aus dem Feld **Name** entfernen*

Terminaldienstedaten werden in 3 Stufen verschlüsselt (Voraussetzung ist die vorherige Installation des Windows2000-128Bit-Verschlüsselungs-Pack):

*Programme → Verwaltung → Terminaldienstekonfiguration → Verbindungen → mit rechter Maustaste auf **RDP-Tcp** klicken → Eigenschaften → Allgemein → Hoch*

SNMP-Betrieb

SNMP (Simple Network Management Protocol) ist ein Tool zur Netzwerkverwaltung nach Industriestandard, mit dem Netzwerkknoten (Server, Arbeitsstationen, Router, Brücken und Hubs) von einem zentralen Host verwaltet werden können.

Es ermöglicht die Überwachung von Netzwerkgeräten und das Kommunizieren von Statusinformationen zwischen diesen.

SNMP verwendet eine verteilte Architektur, welche aus den beiden Komponenten „Verwaltungssystemen“ und „Agents“ besteht.

Um Informationen eines SNMP-Verwaltungssystems anzufordern stehen vier Befehlsoptionen zur Verfügung:

| | |
|-----------------|--------------------------------------------------|
| get | fordert einen bestimmten Wert an |
| get-next | fordert den nächsten Wert an |
| get-bulk | fordert eine große Menge von Verwaltungsdaten an |
| set | ändert einen Wert |

Beim Auftreten eines ungewöhnlichen Ereignisses werden vom Agent Verwaltungsoperationen (Trap-Nachrichten) an die Systeme gesandt. Diese Trap-Nachrichten sind die einzigen Verwaltungsoperationen, die ein Agent initiieren kann.

Windows2000-SNMP-Dienst

Für den Windows2000-SNMP-Dienst gilt Folgendes:

- er protokolliert bei Auftreten bestimmter Ereignisse Trap-Nachrichten, die er an einen oder mehrere Hosts sendet
- er behandelt Anforderungen für Statusinformationen von SNMP-Verwaltungssystemen
- er kann auf einem beliebigen Computer unter Windows2000 mit TCP/IP oder IPX/SPX installiert und verwendet werden
- er verwendet Hostnamen und IP-Adressen zum Identifizieren der Hosts, an die Informationen gesendet und von denen Anforderungen empfangen werden

Windows2000 erzeugt in folgenden Fällen Traps:

- ein Verwaltungssystem versucht, mit Hilfe eines ungültigen Communitynames eine Verbindung zu einem Agent herzustellen
- ein Verwaltungssystem versucht, von einem nicht autorisierten Host aus eine Verbindung zu einem Agent herzustellen

MIB

Eine MIB (Management Information Base) definiert, welche Daten ein Verwaltungssystem von einem Agent anfordern kann, wie das Verwaltungssystem die Daten anfordern muss und wie der Agent die Informationen formatiert, die er zurückgibt. SNMP-Verwaltungssysteme und –Agents können nur miteinander kommunizieren, wenn Sie das gleiche Wissen über MIB-Objekte (Internet-MIB II, Lan Manager-MIB II, DHCP-MIB, WINS-MIB) haben.

Hierarchische Namensstruktur

Der Namensraum für MIB-Objekte ist hierarchisch strukturiert; jedem verwaltbaren Objekt wird ein globaler eindeutiger Name zugewiesen.

Die Objektkennung wird in der Hierarchie als Sequenz von Bezeichnungen (welche durch Punkte voneinander getrennt werden – siehe Kapitel 15/Seite 17) dargestellt, die mit dem Stamm beginnen und beim Objekt enden.

Definieren von SNMP-Communities

SNMP-Agents und Verwaltungssysteme gehören Gruppen (Communities), welche eine einfache Sicherheits- und Kontextüberprüfung für diese bereitstellt, an.

Nur Agents (können auch Mitglied mehrerer Communities sein) und Verwaltungssysteme, die Mitglied derselben Community sind, können miteinander kommunizieren.

Die Standardcommunity ist **public**, welcher allerdings bei Verwendung in einen anderen Namen geändert werden sollte, um Sicherheitsprobleme zu vermeiden.

Installieren des SNMP-Dienstes

Einstellungen → Systemsteuerung → Software → Windows-Komponenten hinzufügen/entfernen → das Kontrollkästchen „Verwaltungs- und Überwachungsprogramme“ aktivieren → Details → das Kontrollkästchen „SNMP (Simple Network Management Protocol)“ aktivieren → OK → Windows-Komponenten → Weiter → Fertig stellen

Konfigurieren von Sicherheit für Agent-SNMP-Dienst

Programme → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → mit rechter Maustaste auf „SNMP-Dienst“ klicken → Eigenschaften → Sicherheit → Konfigurieren von „Authentifizierungstrap senden“, „Angenommene Communitynamen“, „SNMP-Pakete von jedem Host annehmen“ und „SNMP-Pakete von diesem Host annehmen“

Konfigurieren von SNMP-Agent-Eigenschaften

Programme → Verwaltung → Computerverwaltung → Dienste und Anwendungen → Dienste → mit rechter Maustaste auf „SNMP-Dienst“ klicken → Eigenschaften → Agent → Felder ausfüllen → Dienst → Kontrollkästchen für die Dienstypen aktivieren → OK

Um die Kommunikation des SNMP-Dienstes zu überprüfen, stellt Windows2000 im Server-Resource-Kit das Dienstprogramm **SNMPUTIL** bereit.

Syntax: **snmputil** *Befehl Community Objektkennung_(OID)*

Es gibt drei SNMPTUIL-Befehle: **get**, **get-next**, **walk**.