Monday, 4. June 2007

RDP-Verbindungen per SNMP zÃ¤hlen

Warum sollte man das wollen? Weil man kann. Aber was auf den ersten Blick und fÃ¼r einen in der Unix-Welt sozialisierten Admin trivial erscheint, stellte sich bei nÃ¤herer Betrachtung als durchaus schwieriges Unterfangen dar. Ok, vielleicht mangelte es mir auch an der dafÃ¼r nÃ¶tigen Ausbildung oder anstÃ¤ndigen Dokus/Anleitungen, aber bei Letzterem kann ja Onkel Google helfen.

Gegeben sei also ein Windows 2003 Server mit aktiviertem Terminal Service (plus Lizenz-Server und TSCALs), sowie ein Cacti auf einem anderen Host. Letzteres soll nun die Anzahl der aktiven RDP-Verbindungen darstellen. Ok., man kÃ¶nnte auch einfach nur die Anzahl der Benutzer (hrSystemNumUsers) zÃ¤hlen, aber am Ende des Tages ist es eben doch irgendwie nicht das Selbe.
Im Cacti-Forum wird empfohlen die Werte per WMI (mittels Perl und Win32::OLE) abzufragen, doch entspricht dies nicht der hier greifenden Policy und hÃ¤sslich wÃ¤re es IMHO obendrein. SNMP soll also zur Kommunikation genutzt werden. Der Wert findet sich aber leider nicht in der MIB des mit Windows ausgelieferten SNMP-Dienstes und drum muss sie erweitert werden. Dies leistet z.B. der Advanced Agent von SNMP Informant, aber leider nicht in der freien Version. Die $50 kann man sich aber sparen, denn Microsoft liefert mit dem NT4 Ressource Kit hÃ¶chstselbst eine Erweiterung, mit der man den SNMP-Dienst and die Perfmon-Werte ankoppeln kann:
perf2mib runterladen und entpacken
perfmib.dll nach %SystemRoot%\system32 kopieren
perfmib.ini erstellen und an die selbe Stelle platzieren: C:\> perf2mib perfmib.mib perfmib.ini "terminal service" 30 tssrv
dem SNMP-Dienst die neue Erweiterung bekannt machen: Per Regedit in HKLM\SYSTEM\CurrentControlSet\Services\SNMP\Parameters\ExtensionAgents einen weiteren String mit dem Wert SOFTWARE\Microsoft\PerformanceAgent\CurrentVersion eintragen
einen Key HKLM\SOFTWARE\Microsoft\PerformanceAgent\CurrentVersion anlegen und dort eine "erweiterbare Zeichenfolge" namens Pathname mit %SystemRoot%\System32\perfmib.dll als Wert speichern
SNMP-Dienst neu starten

Ãœber diesen Weg kann man wohl so ziemlich jeden Wert aus der Windows-Leistungsanzeige (perfmon) in den MIB-Tree bekommen, aber hier gehts ja erstmal nur um RDP, dessen aktuelle Anzahl aktiver Verbindungen sich nach den oben beschriebenen Schritten hoffentlich im OID WINDOWS-NT-PERFORMANCE::ms-tssrv-ActiveSessions.0 (aka. .iso.org.dod.internet.private.enterprises.microsoft.software.systems.os.winnt.performance.terminal-Services.ms-tssrv-ActiveSessions.0, aka. 1.3.6.1.4.1.311.1.1.3.1.1.30.2.0) finden lÃ¤sst.

Der Rest ist dann nur noch das Abfragen durch Cacti. Hier exemplarische Templates dafÃ¼r.

Geschrieben von Oliver Paulzen in work um 17:31

wie kann ich denn werte mit snmpwalk auslesen?
Anonym am Jun 27 2008, 20:28

So wie mit jedem anderen Device auch?

E.g. snmpwalk -v1 -c $community $device SNMPv2-SMI::enterprises.311.1.1.3.1.1
Anonym am Jun 28 2008, 09:34