

Unterhaltung mit Gemini

Librenms hyper v monitoren

Das Monitoring eines **Hyper-V Clusters** (insbesondere auf Ihrer **Terra Worthmann Hardware** mit **DataCore**) in LibreNMS erfordert ein paar spezifische Schritte, da Windows von Haus aus nur sehr rudimentäre SNMP-Daten liefert.

Hier ist der Leitfaden, wie Sie das Maximum herausholen, unterteilt in **Windows-Basics**, **Hyper-V Details** und die für Sie wichtige **Terra/DataCore-Hardware**.

1. Die Basis: SNMP auf Windows Server aktivieren

LibreNMS kommuniziert primär via SNMP. Windows Server hat diesen Dienst an Bord, er ist aber standardmäßig deaktiviert.

1. Feature installieren:

- Öffnen Sie den Server Manager oder PowerShell (als Admin): `Install-WindowsFeature SNMP-Service -IncludeManagementTools`

2. Konfiguration (Dienste):

- Öffnen Sie `services.msc` und suchen Sie den **SNMP-Dienst**.
- Reiter **Sicherheit**:
 - Fügen Sie Ihre Community-String hinzu (z. B. `public` oder besser etwas eigenes).
 - **Wichtig:** Wählen Sie "Pakete von diesen Hosts annehmen" und tragen Sie die IP Ihres LibreNMS-Servers ein.

3. Dienst neustarten:

Starten Sie den SNMP-Dienst neu, damit die Änderungen greifen.

2. Spezifisch für Ihre Hardware: Terra Worthmann & Intel

Da Sie einen **Terrascaler Datacore Cluster i3** nutzen, basiert dieser höchstwahrscheinlich auf Intel Server-Plattformen, die von Wortmann assembliert wurden. Windows sieht die Hardware-Sensoren (RAID-Status, redundante Netzteile, Temperaturen) nicht über das Standard-SNMP.

- **Intel SNMP Subagent:** Sie müssen oft den **Intel SNMP Subagent** (Teil der *Intel Active System Console* oder *Intel Server Management*) installieren.
 - Wortmann stellt diese Treiber oft im Terra-Download-Portal bereit.

- *Warum ist das wichtig?* Ohne diesen Agenten sieht LibreNMS nur "Windows läuft", aber nicht, ob z.B. ein Netzteil im Cluster ausgefallen ist oder ein RAID-Array "Degraded" ist.

3. Spezifisch für DataCore (SANsymphony)

Da Ihr Cluster "Datacore" heißt, läuft vermutlich **DataCore SANsymphony** für die Speicher-Virtualisierung. DataCore hat einen eigenen SNMP-Dienst, der oft manuell gestartet werden muss.

1. Prüfen Sie in den Windows-Diensten, ob der **DataCore SNMP Agent** (`DcsSNMP`) läuft. Stellen Sie ihn auf "Automatisch".
2. Dieser Agent stellt sicher, dass LibreNMS auch den Status Ihrer virtuellen Disks und Mirror-Verbindungen (Health) sehen kann.

4. Hyper-V VMs und Replikation (Der "Trick" mit SNMP-Extend)

Standard-SNMP zeigt Ihnen CPU/RAM des Hosts, aber oft nicht den detaillierten Status der VMs (z.B. Replikations-Probleme). Hierfür ist **SNMP-Extend** die beste Lösung in LibreNMS.

Sie erstellen ein kleines Skript, das LibreNMS via SNMP abfragt.

Schritt A: Das PowerShell-Skript (auf dem Hyper-V Host) Erstellen Sie ein Skript (z.B.

`C:\SNMP\check_hyperv.ps1`), das den Status prüft. Ein simples Beispiel:

```
# Gibt Anzahl der VMs und fehlgeschlagene Replikationen aus
$vms = Get-VM
$failedRep = Get-VMReplication | Where-Object { $_.Health -ne 'Normal' }

Write-Host "VM_Count:" $vms.Count
Write-Host "Replication_Errors:" $failedRep.Count
```

Schritt B: Einbinden in snmpd.conf Dies ist unter Windows etwas komplexer, da der Standard-Microsoft-SNMP-Dienst keine "Extends" wie Linux unterstützt.

- **Alternative:** Viele Admins nutzen hierfür **Net-SNMP für Windows** statt des Microsoft-Dienstes, ODER
- **Empfehlung für LibreNMS:** Nutzen Sie den **LibreNMS Agent** (Check_MK Agent), den LibreNMS auch unterstützt. Dieser ist oft einfacher, um PowerShell-Outputs direkt an LibreNMS zu senden.

Zusammenfassung der Schritte in LibreNMS

1. **Gerät hinzufügen:** Fügen Sie den Host via SNMP (v2c oder v3) in LibreNMS hinzu.
2. **OS-Erkennung:** LibreNMS sollte ihn automatisch als "Windows" erkennen.

3. **Applikationen aktivieren:** Gehen Sie in den Einstellungen des Geräts auf *Modules* und prüfen Sie, ob "Applications" aktiviert ist.

Mein direkter Vorschlag für den nächsten Schritt

Möchten Sie, dass ich Ihnen ein **genaues PowerShell-Skript** erstelle, das speziell den **Replikationsstatus Ihrer DataCore-Disks** und Hyper-V VMs prüft und so formatiert ist, dass der LibreNMS-Agent es direkt lesen kann?

Bitte gebe mir eine Methode ohne SNMP, da SNMP von Microsoft deprecated ist

Das ist ein absolut valider Einwand. Microsoft hat den *Windows SNMP Service* seit Server 2012 als "Deprecated" markiert. Er funktioniert zwar noch, wird aber nicht mehr weiterentwickelt.

Die moderne und von LibreNMS voll unterstützte Alternative ist der **LibreNMS Agent** (basierend auf dem Check_MK Agent). Dieser nutzt **TCP Port 6556** statt UDP 161 und liefert deutlich detailliertere Daten als SNMP.

Hier ist Ihre Strategie ohne den *Microsoft* SNMP-Dienst:

Schritt 1: Das Grundproblem lösen (LibreNMS braucht einen "Heartbeat")

LibreNMS ist im Kern SNMP-basiert. Um ein Gerät "sinnvoll" hinzuzufügen, benötigt es meist *irgendeine* Antwort. Da Sie den Microsoft-Dienst nicht wollen, haben Sie zwei Optionen:

- **Option A (Empfohlen): Net-SNMP für Windows installieren.** Dies ist die Open-Source-Alternative zum Microsoft-Dienst. Sie ist **nicht deprecated**, wird aktiv gewartet und liefert die Basis-Daten (Uptime, Netzwerk), die LibreNMS für die Geräte-Erstellung braucht.
- **Option B (Agent Only):** Sie können das Gerät theoretisch als "Ping Only" hinzufügen und den Agenten manuell erzwingen, aber das schränkt die Funktionalität (z.B. Port-Statistiken der Netzwerkkarten) oft ein.

Meine Empfehlung: Installieren Sie **Net-SNMP** für die Basis-Erkennung und nutzen Sie den **Agenten** für die echten Daten (Hyper-V, DataCore).

Schritt 2: Den LibreNMS Agenten installieren

Dieser Agent führt lokale Skripte (PowerShell) aus und sendet die Ergebnisse an LibreNMS.

1. Laden Sie den **Check_MK Agent für Windows** herunter (LibreNMS nutzt genau diesen Agenten, `.msi` Datei).
2. Installieren Sie ihn auf Ihrem Hyper-V Host.
3. Öffnen Sie in der Windows-Firewall den Port **TCP 6556** (eingehend) für Ihren LibreNMS-Server.

Schritt 3: Das "Magische" PowerShell-Skript (Local Check)

Da Sie Hyper-V und DataCore nutzen, erstellen wir ein Skript, das diese Werte prüft und in einem Format ausgibt, das LibreNMS direkt als "Service" erkennt.

Erstellen Sie die Datei `C:\ProgramData\checkmk\agent\local\hyperv_datacore_mon.ps1`:

```
#<<<local>>>
# Überprüfung des Hyper-V Replikationsstatus
$failedRep = Get-VMReplication | Where-Object { $_.Health -ne 'Normal' }
$vmCount = (Get-VM).Count

if ($failedRep) {
    # Status 2 = Critical
    Write-Host "2 Hyper-V_Replication - CRITICAL: $($failedRep.Count) VMs with replication errors"
} else {
    # Status 0 = OK
    Write-Host "0 Hyper-V_Replication - OK: All $vmCount VMs replicating normally"
}

# Überprüfung DataCore Disk Status (Benötigt DataCore Cmdlets)
# Versuche DataCore Modul zu laden, falls vorhanden
try {
    Import-Module DataCore.Executive.Cmdlets -ErrorAction Stop
    $dcsDisks = Get-DcsVirtualDisk
    $unhealthyDisks = $dcsDisks | Where-Object { $_.DiskStatus -ne 'Online' }

    if ($unhealthyDisks) {
        Write-Host "2 DataCore_Disks - CRITICAL: $($unhealthyDisks.Count) Disks not Online"
    } else {
        Write-Host "0 DataCore_Disks - OK: All Disks Online"
    }
} catch {
    Write-Host "1 DataCore_Check - WARN: DataCore Cmdlets not found or script error"
}
```

Was tut dieses Skript?

- Es läuft automatisch durch den Agenten (sobald es im Ordner `local` liegt).
- Es gibt `0` (OK), `1` (Warnung) oder `2` (Kritisch) zurück.
- In LibreNMS erscheinen diese Checks automatisch unter dem Reiter **"Services"** beim Gerät.

Schritt 4: Aktivierung in LibreNMS

1. Gehen Sie auf das Gerät in LibreNMS.
2. Wählen Sie **Edit -> Modules**.

3. Aktivieren Sie `unix-agent` (Ja, das heißt auch bei Windows so).
4. Warten Sie 5-10 Minuten (Polling-Zyklus).
5. Prüfen Sie den Reiter **Services**. Dort sollten nun "Hyper-V_Replication" und "DataCore_Disks" mit ihrem Status erscheinen.

Zusammenfassung

Sie umgehen den veralteten Microsoft-Dienst komplett, indem Sie den **Check_MK Agenten** als Datenlieferanten nutzen. Das gibt Ihnen präzise Kontrolle über Ihre DataCore- und Hyper-V-Umgebung via PowerShell, ohne auf veraltete Protokolle angewiesen zu sein.

Monitoring Windows in Checkmk

Dieses Video zeigt die Installation des Checkmk-Agenten auf Windows; da LibreNMS exakt denselben Agenten verwendet, ist die gezeigte Vorgehensweise 1:1 auf Ihr Szenario übertragbar.

Erkläre mir bitte detailliert die Installation von net-snmp auf einem Windows 2022 server.

Die Installation von **Net-SNMP** auf Windows Server 2022 ist ein hervorragender Weg, um eine stabile, moderne SNMP-Implementierung zu erhalten, ohne auf den veralteten Microsoft-Dienst angewiesen zu sein.

Da Net-SNMP ursprünglich aus der Unix/Linux-Welt stammt, ist die Installation auf Windows etwas "handwerklicher" als ein typisches `Weiter -> Weiter -> Fertig` Setup.

Hier ist die Schritt-für-Schritt-Anleitung.

Vorbereitung: Konflikte vermeiden

Bevor Sie beginnen: Stellen Sie sicher, dass der **Windows SNMP Service** (der von Microsoft) entweder deinstalliert oder **deaktiviert** ist. Beide können nicht gleichzeitig auf Port 161 (UDP) lauschen.

1. `services.msc` öffnen.
2. Nach "SNMP-Dienst" suchen.
3. Status auf **Beendet** und Starttyp auf **Deaktiviert** setzen.

Schritt 1: Download der Binaries

Net-SNMP wird nicht offiziell von Microsoft gehostet. Die gängigste Quelle für kompilierte Windows-Binaries ist SourceForge.

1. Gehen Sie zu SourceForge: [Net-SNMP Binaries](#)

2. Suchen Sie die neueste stabile Version (aktuell oft im Bereich 5.7.x oder neuer).
3. Laden Sie die **64-bit Version** (z.B. `net-snmp-5.7.0-1-x64.exe`) herunter.
 - *Hinweis: Die Versionen sind oft etwas älter, funktionieren aber tadellos unter Server 2022.*

Schritt 2: Die Installation

Führen Sie die `.exe` als Administrator aus.

1. **Welcome Screen:** Next.
2. **License:** Accept.
3. **Components:** Hier ist es wichtig. Wählen Sie mindestens:
 - `Base Components`
 - `Net-SNMP Agent Service` (Das installiert es als Windows-Dienst).
 - *Optional:* `Perl SNMP` (wird meist nicht benötigt, es sei denn, Sie nutzen Perl-Skripte).
4. **Install Location:**
 - **WICHTIG:** Belassen Sie den Pfad idealerweise auf `C:\usr` .
 - *Warum?* Net-SNMP hat viele Unix-Wurzeln. Wenn der Pfad Leerzeichen enthält (wie "Program Files"), kann das später zu Problemen bei der Konfiguration oder beim Laden von MIBs führen. `C:\usr` ist der Standard, der am wenigsten Kopfschmerzen bereitet.
5. **Start Menu Folder:** Next.
6. **Finish.**

Schritt 3: Die Konfiguration (snmpd.conf)

Anders als bei Windows-Diensten gibt es hier keine GUI. Sie müssen eine Textdatei bearbeiten.

1. Navigieren Sie zu: `C:\usr\etc\snmp`
2. Dort finden Sie vermutlich eine `snmpd.conf.example` oder ähnlich. Erstellen Sie eine **neue Datei** namens `snmpd.conf` (ohne `.txt` Endung!).
3. Öffnen Sie diese mit Notepad oder VS Code.

Fügen Sie folgenden Inhalt ein (passen Sie `IHR_COMMUNITY_STRING` an, z.B. etwas Komplexes für LibreNMS):

Librenms hyper v monitoren

```
# --- SYSTEM INFORMATION ---
# Kontakt und Ort für LibreNMS
syslocation      Terra Cluster Rack 1
sysContact       Admin <admin@ihrefirma.de>

# --- ACCESS CONTROL ---
# Definiert, wer Daten lesen darf (ro = read only)
# Syntax: rocommunity [CommunityString] [Source IP]
# Erlaubt localhost (für Tests) und Ihren LibreNMS Server

rocommunity public 127.0.0.1
rocommunity IHR_GEHEIMER_STRING 192.168.1.100

# Falls Sie keine IP-Einschränkung wollen (weniger sicher):
# rocommunity IHR_GEHEIMER_STRING default

# --- VIEW SETTINGS ---
# Stellen Sie sicher, dass der Agent alles sieht (systemview)
# Manchmal nötig, damit LibreNMS Host-Ressourcen sieht
view      systemview      included      .1.3.6.1.2.1.1
view      systemview      included      .1.3.6.1.2.1.25.1.1

# --- LOGGING ---
# Windows Eventlog deaktivieren, um Spam zu vermeiden (optional)
dontLogTCPWrappersConnects yes
```

Ersetzen Sie `192.168.1.100` durch die IP Ihres LibreNMS Servers.

Schritt 4: Den Dienst registrieren

Der Installer kopiert die Dateien, aber registriert den Dienst nicht immer sauber. Net-SNMP liefert ein Skript dafür mit.

1. Öffnen Sie die **Eingabeaufforderung (CMD)** als **Administrator**.
2. Navigieren Sie in den `bin` Ordner: `cd C:\usr\bin`
3. Führen Sie das Registrierungs-Skript aus: `registeragent.bat` (Sie sollten eine Meldung sehen: "The operation completed successfully.")

Schritt 5: Windows Firewall öffnen

Da dies nicht der eingebaute Windows-Dienst ist, öffnet Windows den Port nicht automatisch.

1. Öffnen Sie **Windows Defender Firewall mit erweiterter Sicherheit**.
2. **Eingehende Regeln -> Neue Regel**.

3. Regeltyp: **Port**.
 4. Protokoll: **UDP**, Bestimmte lokale Ports: **161**.
 5. Aktion: **Verbindung zulassen**.
 6. Profil: Domäne, Privat, Öffentlich (je nach Ihrer Netzwerkkonfiguration, meist "Domäne").
 7. Name: `Net-SNMP (UDP 161)`.
-

Schritt 6: Dienst starten und testen

1. Öffnen Sie `services.msc`.
2. Suchen Sie den Dienst **Net-SNMP Agent**.
3. Rechtsklick -> **Starten**. (Stellen Sie sicher, dass er auf "Automatisch" steht).

Lokaler Test: Öffnen Sie CMD und testen Sie, ob der Agent antwortet: `C:\usr\bin\snmpwalk -v 2c -c public 127.0.0.1 system`

Wenn Sie eine Liste von Ausgaben sehen (SysName, SysUpTime, etc.), läuft der Agent erfolgreich.

Schritt 7: Einbindung in LibreNMS

Jetzt können Sie in LibreNMS das Gerät hinzufügen:

- **Hostname:** IP oder DNS Ihres Servers.
- **SNMP Version:** v2c.
- **Community:** `IHR_GEHEIMER_STRING` (aus der `snmpd.conf`).

Nächster Schritt: Sobald Net-SNMP läuft und LibreNMS den Server sieht, sollten Sie wie im vorherigen Teil besprochen den **Check_MK Agenten** installieren, um die spezifischen Hyper-V und DataCore Details abzugreifen. Net-SNMP liefert Ihnen jetzt die solide Basis (Netzwerktraffic, Uptime, CPU-Grundlast).

Soll ich Ihnen helfen, die `snmpd.conf` noch spezifischer für Sicherheit (SNMPv3 mit Verschlüsselung) anzupassen?

Die neuste net-smtp version ist von 2011. gibt es keine aktuelleren?

Das ist eine sehr aufmerksame Beobachtung. Sie haben völlig recht: Die **offiziellen** Windows-Binaries auf SourceForge wurden vom Net-SNMP-Projektteam seit ca. 2011 (Version 5.5/5.7) nicht mehr aktualisiert, obwohl der Quellcode selbst (für Linux) viel weiter ist (Version 5.9.x).

Das liegt daran, dass die Entwickler primär Linux-fokussiert sind und niemand mehr die Windows-Installer offiziell baut.

Es gibt jedoch **Lösungen**, um nicht die uralte 2011er Version nutzen zu müssen:

Option 1: Inoffizielle, aktuelle Builds (Empfohlen für Ihren Fall)

Da der offizielle Installer veraltet ist, springt die Community ein. Ein sehr bekannter und vertrauenswürdiger Build stammt von **Eli Fulkerson**. Er kompiliert die aktuellen Versionen regelmäßig für Windows.

- **Version:** Meist 5.9.x (viel neuer als 2011).
- **Quelle:** Suchen Sie nach "Eli Fulkerson Net-SNMP" oder nutzen Sie seine Seite. Er bietet stabile `.exe` Installer an, die genau wie die offiziellen funktionieren, aber aktuelle Sicherheitsupdates und Features enthalten.
- **Vorteil:** Sie schließen Sicherheitslücken, die in der 2011er Version noch offen waren.

Option 2: Warum die "alte" Version oft trotzdem reicht

Der Grund, warum viele Anleitungen noch auf die alte Version verweisen, ist simpel: SNMP v2c hat sich seit Jahrzehnten kaum verändert.

- Wenn Sie Net-SNMP nur als "Türsteher" nutzen, damit LibreNMS den Server erkennt (Hostname, Uptime), reicht selbst die 2011er Version technisch aus.
- **Aber:** Aus Sicherheitsgründen (OpenSSL-Bibliotheken) ist auf einem modernen Windows Server 2022 definitiv ein neuerer Build (wie der von Fulkerson) ratsam.

Zusammenfassung & Vorgehen

Für Ihren **Windows Server 2022** würde ich folgendes tun:

1. Laden Sie **nicht** die alten SourceForge-Dateien von 2011.
2. Suchen Sie nach dem **"Net-SNMP 5.9.1 Windows Binary by Eli Fulkerson"**.
3. Die Installation läuft exakt so ab wie in meiner vorherigen Anleitung beschrieben (Pfad `C:\usr` etc.).

Damit haben Sie eine saubere, moderne SNMP-Basis, ohne auf "Legacy"-Software zurückzugreifen.

Haben Sie den Installer gefunden oder soll ich Ihnen beim Config-File helfen?

Hier ist ein Video, das den Installationsprozess eines (wenn auch älteren) SNMP-Setups zeigt, um die Schritte zu visualisieren. Beachten Sie, dass Sie statt der gezeigten Quelle die neuere Datei verwenden.

[Net-SNMP Installation on Windows](#)

Dieses Video zeigt die grundlegende Installation und Einrichtung von Net-SNMP auf Windows, was hilfreich ist, um die Schritte nachzuvollziehen, auch wenn Sie eine neuere Installationsdatei verwenden sollten.

bitte beim cfg file helfen

Gerne. Die Konfigurationsdatei `snmpd.conf` ist das Herzstück von Net-SNMP. Da Sie die neuere Version (z.B. von Eli Fulkerson) nutzen, können wir eine sehr saubere und moderne Konfiguration verwenden.

Hier ist eine Vorlage, die für **Windows Server 2022** optimiert ist und unnötigen Ballast vermeidet.

Speicherort der Datei

Erstellen oder bearbeiten Sie die Datei unter: `C:\usr\etc\snmp\snmpd.conf` (*Achten Sie darauf, dass Windows nicht versehentlich `.txt` anhängt. Die Datei muss genau `snmpd.conf` heißen.*)

Der Inhalt für Ihre snmpd.conf

Kopieren Sie den folgenden Block in die Datei. Die Zeilen mit `#` sind Kommentare. **Ändern Sie unbedingt die Werte in den eckigen Klammern `[...]`.**

```
#####
# Net-SNMP Konfiguration für Windows Server 2022 (Hyper-V / DataCore)
#####

# -----
# 1. SYSTEM INFORMATIONEN
# -----
# Diese Infos erscheinen oben in LibreNMS.
# Passen Sie den Standort und Kontakt an.
sysLocation    [Terra Cluster / Rack 1 / Serverraum]
sysContact     [IT-Admin <admin@ihrefirma.de>]

# -----
# 2. ZUGRIFFSKONTROLLE (Sicherheit)
# -----
# Hier definieren wir, wer lesen darf ("ro" = Read Only).
# Syntax: rocommunity [Community-String] [Erlaubte-IP]

# a) Lokaler Zugriff für Tests (wichtig für Fehlersuche)
rocommunity public 127.0.0.1

# b) Zugriff für Ihren LibreNMS Server
# Ersetzen Sie 'public' durch ein starkes Passwort (Community String).
# Ersetzen Sie '192.168.x.x' durch die IP Ihres LibreNMS-Servers.
rocommunity [IHR_GEHEIMER_STRING] [192.168.10.50]

# Falls Sie ein ganzes Subnetz erlauben wollen (z.B. Admin-Netz):
# rocommunity [IHR_GEHEIMER_STRING] 192.168.10.0/24

# -----
# 3. PERFORMANCE & LOGGING (Wichtig für Windows)
# -----
# Verhindert, dass das Windows Event-Log mit Verbindungs-Infos geflutet wird.
dontLogTCPWrappersConnects yes

# Welche Festplatten sollen überwacht werden?
# Wenn Sie diese Zeile weglassen, zeigt er meist alle an.
# Falls 'C:' fehlt, können Sie es erzwingen:
disk C: 10%

# -----
# 4. AGENT VERHALTEN
# -----
# Stellt sicher, dass der Agent auf allen Interfaces auf Port 161 hört
agentaddress udp:161

# (Optional) Eventuelle Fehlerbehandlung für Interface-Erkennung
interface_fadeout 2000
```

Erklärung der kritischen Teile

1. `rocommunity` : Das ist der wichtigste Befehl.
 - Er ersetzt die komplizierte `com2sec / group / view / access` Kette von früher.
 - Er sagt einfach: "Wenn jemand von der IP `[192.168.10.50]` kommt und das Passwort `[IHR_GEHEIMER_STRING]` kennt, zeig ihm alles."
 - **Sicherheitstipp:** Nutzen Sie *nicht* "public" als String für den LibreNMS Server.
2. `dontLogTCPWrappersConnects yes` : Ohne diese Zeile schreibt Net-SNMP bei jedem einzigen Abfrage-Zyklus (Polling) von LibreNMS einen Eintrag in das Windows-Ereignisprotokoll. Das müllt das Log extrem zu.
3. `agentaddress` : Standardmäßig hört er auf allen IPs. Falls Sie mehrere Netzwerkkarten haben (z.B. iSCSI für DataCore und Management), und Sie wollen SNMP *nur* auf dem Management-LAN, könnten Sie hier auch `agentaddress udp:192.168.10.20:161` eintragen (die feste IP des Servers).

Nächste Schritte nach dem Speichern

Damit die Änderungen wirksam werden:

1. **Dienst neustarten:** Öffnen Sie `services.msc`, suchen Sie **Net-SNMP Agent**, Rechtsklick -> **Neu starten**.
2. **Testen (Lokal):** Öffnen Sie eine CMD und tippen Sie: `C:\usr\bin\snmpwalk -v 2c -c public 127.0.0.1 system` (Das testet die lokale Regel).
3. **In LibreNMS testen:** Fügen Sie das Gerät jetzt hinzu oder lassen Sie es neu abfragen ("Rediscover").

Möchten Sie wissen, wie man zusätzlich noch prüft, ob der **DataCore-Dienst** selbst läuft (via Prozess-Überwachung in dieser Config), oder lassen wir das alles über den Agenten laufen (was ich weiterhin empfehle)?

Ich habe diese seite gefunden: <https://www.elifulkerson.com/articles/net-snmp-windows-binary-unofficial.php>
 ich weiß aber nicht wie ich mit diesen dateien snmp auf einem windows 2022 server installieren soll. Bitte gebe eine detaillierte anleitung

Das ist das "Problem" bei den inoffiziellen Builds von Eli Fulkerson (und anderen): Es sind oft keine bequemen `.msi` -Installer, sondern einfache **ZIP-Archive** mit den nackten Programmdateien ("Binaries"). Das bedeutet, wir müssen die "Installation" manuell vornehmen, indem wir die Dateien an den richtigen Ort legen und den Dienst per Hand registrieren.

Das ist auf einem Windows Server 2022 aber kein Problem. Hier ist die exakte Anleitung für diese spezifischen Dateien.

Schritt 1: Die Ordnerstruktur vorbereiten

Net-SNMP ist historisch so programmiert, dass es seine Dateien standardmäßig unter `C:\usr` sucht. Wir sollten diesen Pfad nutzen, um Konfigurationsärgern zu vermeiden.

1. Öffnen Sie den Windows Explorer auf Ihrem Server.
2. Erstellen Sie auf Laufwerk `C:` einen Ordner namens `usr`.
3. Im Ordner `C:\usr` erstellen Sie zwei Unterordner:
 - `bin` (Hier kommen die heruntergeladenen Programmdateien rein)
 - `etc` -> und darin einen Unterordner `snmp` (Hier kommt die Config rein).

Ihre Struktur muss so aussehen:

- `C:\usr\bin\`
- `C:\usr\etc\snmp\`

Schritt 2: Dateien platzieren

1. Laden Sie von der Eli Fulkerson Seite die Datei herunter (meistens heißt sie `net-snmp-5.9.1-1-x64.zip` oder ähnlich).
2. Öffnen Sie die ZIP-Datei.
3. Kopieren Sie **alle** Dateien aus dem ZIP-Archiv (Dateien wie `snmpd.exe`, `snmpwalk.exe`, `netsnmp.dll` etc.) direkt in den Ordner: `C:\usr\bin\`

Schritt 3: Die Konfiguration erstellen

Falls Sie es noch nicht gemacht haben, erstellen Sie jetzt die Konfigurationsdatei.

1. Gehen Sie in den Ordner `C:\usr\etc\snmp\`.
2. Erstellen Sie eine neue Datei namens `snmpd.conf`. (*Achtung: Stellen Sie sicher, dass sie nicht `snmpd.conf.txt` heißt! Blenden Sie dazu im Explorer unter "Ansicht" die "Dateinamenerweiterungen" ein*).
3. Öffnen Sie die Datei mit einem Editor (Notepad) und fügen Sie den Inhalt ein, den ich Ihnen vorhin erstellt habe (hier nochmal die Kurzform):

```
rocommunity public 127.0.0.1
rocommunity IHR_GEHEIMER_STRING 192.168.x.x
dontLogTCPWrappersConnects yes
agentaddress udp:161
```

(Denken Sie daran, `IHR_GEHEIMER_STRING` und die IP anzupassen).

Schritt 4: Den Dienst registrieren (Der wichtigste Teil)

Da es keinen Installer gab, weiß Windows noch nichts von dem Programm. Wir müssen Windows sagen: "Nimm diese `.exe` und mache einen Dienst daraus."

1. Öffnen Sie die **Eingabeaufforderung (CMD)** als **Administrator** (Rechtsklick auf CMD -> Als Admin ausführen).
2. Wechseln Sie in das Verzeichnis: `cd C:\usr\bin`
3. Führen Sie folgenden Befehl aus, um den Dienst zu registrieren:

```
snmpd.exe -register -Lf "C:/usr/log/snmpd.log"
```

(Der Parameter `-register` sagt dem Programm, es soll sich als Dienst eintragen. `-Lf ...` sagt ihm, wo er Fehler hinschreiben soll, falls etwas nicht klappt. Falls der Ordner `Log` unter `C:\usr` noch nicht existiert, erstellen Sie ihn kurz).

Alternativ: Oft liegt bei Eli Fulkerson im ZIP auch eine Datei namens `registeragent.bat`. Wenn diese Datei im `bin` Ordner liegt, können Sie auch einfach diese als Administrator ausführen. Sie tut das Gleiche.

4. Wenn es geklappt hat, kommt meistens **keine** Rückmeldung oder nur "Service registered".

Schritt 5: Firewall öffnen

Wie vorhin beschrieben, müssen Sie Port 161 freigeben, sonst blockt Windows Server 2022 alles ab.

1. **PowerShell als Admin** öffnen.
2. Diesen Befehl reinkopieren (geht schneller als Klicken):

```
New-NetFirewallRule -DisplayName "Net-SNMP (UDP 161)" -Direction Inbound -Protocol UDP -
LocalPort 161 -Action Allow
```

Schritt 6: Dienst starten und Testen

1. Drücken Sie `Win + R` und tippen Sie `services.msc`.
2. Suchen Sie in der Liste nach **Net-SNMP Agent**.
3. Rechtsklick -> **Eigenschaften**.
4. Stellen Sie den Starttyp auf **Automatisch**.
5. Klicken Sie auf **Starten**.

Funktionstest: Gehen Sie zurück in Ihre Administrator-CMD (immer noch im Ordner `C:\usr\bin`) und testen Sie lokal:

```
snmpwalk.exe -v 2c -c public 127.0.0.1 system
```

Wenn jetzt eine Liste mit Text rattert (Systemname, Uptime etc.), haben Sie es geschafft!

Mögliche Fehlerquelle: "VCRUNTIME140.dll fehlt"

Da Sie einen Windows Server 2022 nutzen, kann es sein, dass Ihnen die **Visual C++ Redistributables** fehlen, die diese Programme brauchen.

- **Fehlerbild:** Wenn Sie `snmpwalk` oder `snmpd` starten wollen, kommt eine Fehlermeldung, dass eine `.dll` fehlt.
- **Lösung:** Laden Sie das "Microsoft Visual C++ Redistributable latest supported downloads" (x64 Version) direkt bei Microsoft herunter und installieren Sie es. Dann klappt es.

Ich möchte den "Net-SNMP 5.9.1 Windows Binary by Eli Fulkerson" auch für alle clients in eine windows domain installieren per gpo. Wie führe ich das durch?

Das ist eine hervorragende Idee. Da wir hier keinen `.msi`-Installer haben, ist das Vorgehen etwas "manueller" als bei Standard-Software, aber mit **Group Policy Preferences (GPP)** und einem **Startup-Script** sehr sauber lösbar.

Wir bauen eine GPO, die drei Dinge tut:

1. **Dateien verteilen:** Die Binaries und die Config auf die Clients kopieren.
2. **Dienst registrieren:** Ein kleines Skript beim Booten, das den Dienst installiert, falls er fehlt.
3. **Firewall öffnen:** Den Port 161 freigeben.

Hier ist der detaillierte Fahrplan.

Schritt 1: Vorbereitung (Der "Verteiler-Ordner")

Sie benötigen einen Netzwerkpfad, auf den alle Computer Lesezugriff haben. Der einfachste Ort ist das **NETLOGON** Verzeichnis Ihrer Domain Controller, da jeder Client dort Zugriff hat. Alternativ geht jeder andere Share.

1. Erstellen Sie auf dem Share einen Ordner, z.B. `\\IhreDomain\NETLOGON\deploy\snmp`.
2. Kopieren Sie **alle** Dateien aus dem Eli Fulkerson ZIP in diesen Ordner.
3. Legen Sie auch Ihre fertige `snmpd.conf` in diesen Ordner.
4. Erstellen Sie in diesem Ordner eine neue Textdatei `install_snmp.bat` mit folgendem Inhalt (das ist unser Installations-Logik-Skript):

```
@echo off
:: Prüfen, ob der Dienst schon existiert
sc query "Net-SNMP Agent" >nul 2>&1
if %errorlevel% EQU 0 goto END

:: Wenn nicht, dann registrieren
cd /d "C:\usr\bin"
snmpd.exe -register -Lf "C:/usr/log/snmpd.log"
net start "Net-SNMP Agent"

:END
exit
```

Schritt 2: Die GPO erstellen

Öffnen Sie die **Gruppenrichtlinienverwaltung** (Group Policy Management) auf Ihrem DC. Erstellen Sie eine neue GPO, z.B. "Software_Deploy_NetSNMP".

A. Dateien verteilen (GPO Files)

Wir müssen die Ordnerstruktur auf dem Client nachbauen und die Dateien kopieren.

1. Navigieren Sie zu: **Computerkonfiguration -> Einstellungen -> Windows-Einstellungen -> Dateien** (Files).
2. Rechtsklick -> **Neu -> Datei**.
3. **Schritt A1 (Binaries):**
 - **Quelldatei(en):** `\\IhreDomain\NETLOGON\deploy\snmp*.*` (Das Sternchen ist wichtig!)
 - **Zielfile:** `C:\usr\bin\`

- **Aktion:** Aktualisieren (Update).
- *Hinweis:* Falls er meckert, dass der Zielordner nicht existiert: GPP erstellt Ordner meist automatisch. Sicherer ist es, unter "Ordner" (Folders) vorher `C:\usr\bin` erstellen zu lassen.

4. Schritt A2 (Config):

- Rechtsklick -> Neu -> Datei.
- **Quelldatei:** `\\IhreDomain\NETLOGON\deploy\snmp\snmpd.conf`
- **Zieldatei:** `C:\usr\etc\snmp\snmpd.conf`
- **Aktion:** Ersetzen (Replace) – *Warum Ersetzen?* So können Sie die Config zentral im NETLOGON ändern und beim nächsten GPO-Update erhalten alle Clients die neue Version.

B. Dienst registrieren (Startup Script)

Damit der Dienst installiert wird, nutzen wir das Batch-Skript von vorhin.

1. Navigieren Sie zu: **Computerkonfiguration -> Richtlinien -> Windows-Einstellungen -> Skripts -> Starten** (Startup).
2. Klicken Sie auf **Hinzufügen**.
3. Bei "Skriptname" geben Sie den UNC-Pfad an: `\\IhreDomain\NETLOGON\deploy\snmp\install_snmp.bat`.

C. Firewall öffnen

Der Agent nützt nichts, wenn die Firewall ihn blockt.

1. Navigieren Sie zu: **Computerkonfiguration -> Richtlinien -> Windows-Einstellungen -> Sicherheitseinstellungen -> Windows Defender Firewall mit erweiterter Sicherheit**.
2. Rechtsklick auf **Eingehende Regeln -> Neue Regel**.
 - **Typ:** Port
 - **Protokoll:** UDP, Port 161
 - **Aktion:** Verbindung zulassen
 - **Profil:** Domäne (privat/öffentlich je nach Bedarf, Domäne reicht meist).
 - **Name:** "Net-SNMP Agent (GPO)"

Schritt 3: VC++ Runtime (Die Stolperfalle)

Wie erwähnt, benötigen die Binaries oft die **Visual C++ Redistributables**.

- Testen Sie auf einem nackten Client manuell, ob `snmpd.exe` startet. Wenn ein Fehler ("VCRUNTIME140.dll missing") kommt, müssen Sie auch die VC++ Redistributable verteilen.
- Das geht am einfachsten per **Softwareinstallation** (MSI) in derselben GPO:
 - Laden Sie die `vc_redist.x64.exe` herunter. Tipp: Nutzen Sie Argumente `/install /quiet /norestart` in einem Startup-Skript ODER suchen Sie nach einem MSI-Wrapper für die Redistributables, um sie sauber über "Softwareinstallation" zu verteilen.

Schritt 4: Verknüpfung und Test

1. Verknüpfen Sie die GPO mit einer **Test-OU**, in der sich ein Computer befindet.
2. Starten Sie den Test-Client neu (Startup-Skripte laufen nur beim Booten, nicht beim Login!).
3. Prüfen Sie nach dem Neustart:
 - Existiert `C:\usr\bin`?
 - Läuft der Dienst "Net-SNMP Agent" (`services.msc`)?
 - Können Sie von LibreNMS aus den Client erreichen?

Wenn das klappt, können Sie die GPO auf die ganze Domain (oder Server-OU) ausrollen.

[Install Software via GPO](#)

Dieses Video erklärt anschaulich die Grundlagen der Softwareverteilung per Gruppenrichtlinie (GPO), inklusive der Erstellung von MSI-Paketen und der Zuweisung an Clients, was Ihnen helfen kann, falls Sie zusätzlich die C++ Runtimes verteilen müssen.