



Podporujeme SNMPv3!

SNMP v3, jeho výhody a nasazení v jednotkách Poseidon

SNMP (Simple Network Management Protocol) je způsob rychlého a nenáročného dohledu zejména síťových prvků a služeb. Stále častěji je však nasazován rovněž pro dohled prostředí v němž tyto prvky pracují a to zejména díky možnosti sledovat teplotu, vlhkost a jiné veličiny ve stejném dohledovém software jako jiné provozní parametry systému. Protokol SNMP byl původně navržen jako extrémně úsporný a nad protokolem UDP čímž bylo zajištěné nízké zatížení sítě vlastním managementem. Dnes v dobách gigabitových a rychlejších sítích však jsou priority trochu jiné a protokol tak doznal řady rozšíření.

Protokol SNMP je asynchronní, transakčně orientovaný protokol založený na modelu klient/server. Strana, která posílá požadavky (snmp klient), může být např. jednoduchý snmp browser či složitý NMS (Network Management Systém), na straně zařízení je snmp agent (snmp server), který na požadavky odpovídá. Výjimku tvoří tzv. trapy, které agenti vysílají asynchronně při výskytu jednotlivých události (výpadek proudu, větráku, překročení mezních údajů, objevení nového zařízení). Samozřejmě je nutné předem definovat adresu, kam se informace posílá. Pro přenos dat se používá protokol UDP, přičemž je definováno přesně místo, kam se mohou připojovat uživatelské aplikace jednotlivých firem, které spravuje organizace IANA (Internet Assigned Numbers Authority - doslova: Internetová autorita pro přidělování čísel). Přes SNMP lze nejen zjišťovat aktuální hodnoty, ale rovněž zapisovat provozní hodnoty (konfigurovat zařízení).

Jednotlivé verze SNMP

Protokol SNMP se postupně vyvíjel: první verze (SNMPv1) zajišťuje základní funkcionalitu SNMP a patří mezi mimořádně úsporné verze. Se zrychlováním sítí došlo k potřebě vyššího zabezpečení a tak do SNMPv2 byla navíc doplněna jednoduchá autentizace (ochrana uživatelským jménem a heslem), která byla v poslední verzi protokolu (SNMPv3) doplněna o šifrování.

V SNMPv1 pro identifikaci „oprávněných“ agentů sloužila jen komunita (*community*). Ačkoliv její název byl uživatele uživatelsky definovatelný, zpravidla nabýval dvou hodnot – „*public*“ pro čtení a „*private*“ pro čtení i zápis.

V SNMPv2 došlo ke zlepšení v oblasti výkonu, bezpečnosti, důvěrnosti a správy komunikace. Standard SNMPv2 není příliš používán a více se používají jen jeho varianta SNMPv2c, která je kompatibilní se SNMPv1 a má jen kromě vyšší efektivity rozšířenou sadu příkazů. Varianta SNMPv2u se příliš neujala, byť se jednalo o první pokus zavést do SNMP prvky zabezpečení.

SNMPv3 je nastupující varianta standardu a již obsahuje nejen autentizaci uživatele, ale rovněž šifrování komunikace. K zabezpečení se používá *Uživatelské jméno* (de facto ekvivalent *Community*), *Heslo pro autorizaci* (*Authentisation password*) a *klíč* (*Privacy password*). Během autorizace lze komunikaci šifrovat pomocí MD5 či SHA, vlastní komunikace pak může být šifrována pomocí DES či AES. Ze SNMPv3 se tak

stává plnohodnotný management protokol i do nejnáročnějších korporátních sítí. Hlavní výhodou pak je, že MIB zůstává stejná, není tedy třeba žádných zvláštních úprav při přechodu na SNMPv3.

Uživatelů může být v rámci SNMPv3 neomezené množství, což umožňuje sledovat a logovat činnost jednotlivých operátorů. Každý uživatel má svoji kombinaci Username, Auth. password a Privacy password spolu s příslušným šifrováním, které dohromady tvoří profil.

Užití SNMPv3

Jednotky Poseidon podporují SNMPv3, které podporuje až 5 uživatelských profilů. Příklady jsou uvedeny níže:

Webové rozhraní Poseidonu2 4002 se SNMP nastavením

The screenshot displays the web interface for the Poseidon2 4002 device, specifically the SNMP configuration page. The interface is organized into several sections:

- General SNMP Settings:** Includes fields for SNMP Port (161), SNMP Port Listener (162), and SNMP Version (3).
- SNMP Access:** A table defining access for 'public' and 'private' users, with checkboxes for Read and Write permissions.
- SNMP Trap Destinations:** A table with columns for Destination (A-E), User name, IP Address, and Port.
- SNMP Users:** A table listing users with their authentication and privacy settings.
- MIB II System Group:** Fields for SysContact, SysName, and SysLocation.

Destination	User name	IP Address	Port
A.	public	192.168.1.39	162
B.	private		
C.	---- Disabled ----		
D.	---- Disabled ----		
E.	---- Disabled ----		

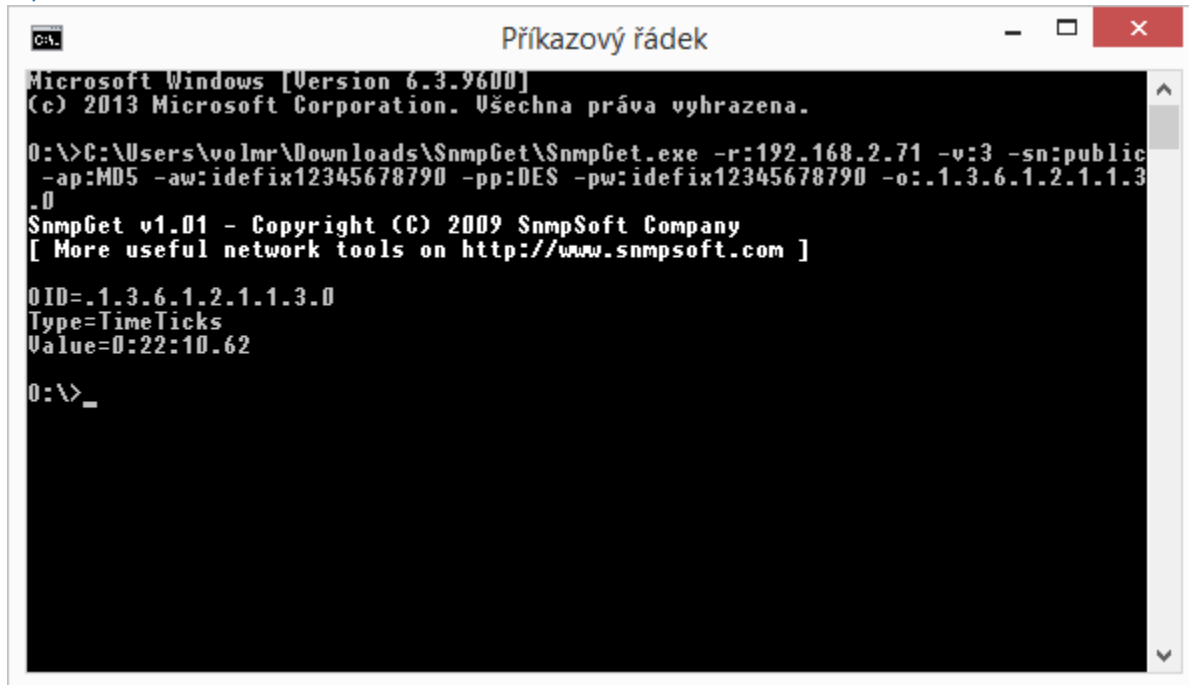
User name	Auth. Type	Auth. Password	Privacy Type	Privacy Password
public	MD5	idefix1234567890	DES	idefix1234567890
private	SHA		AES	
HWgroup	MD5		DES	
Phaenix	SHA		DES	
Idefix	SHA		AES	

Field	Value
SysContact	support@HWgroup.cz
SysName	Poseidon2 4002
SysLocation	

Příklad použití SNMPv3 v jednotce Poseidon se SNMPget:

```
C:\Users\volmr\Downloads\SnmGet\SnmGet.exe -r:192.168.2.71 -v:3 -sn:public -ap:MD5 -aw:idefix12345678790 -pp:DES -pw:idefix12345678790 -o:.1.3.6.1.2.1.1.3.0
```

Výsledek:



```
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. Všechna práva vyhrazena.

O:\>C:\Users\volmr\Downloads\SnmGet\SnmGet.exe -r:192.168.2.71 -v:3 -sn:public
-ap:MD5 -aw:idefix12345678790 -pp:DES -pw:idefix12345678790 -o:.1.3.6.1.2.1.1.3
.0
SnmGet v1.01 - Copyright (C) 2009 SnmpSoft Company
[ More useful network tools on http://www.snmpsoft.com ]

OID=.1.3.6.1.2.1.1.3.0
Type=TimeTicks
Value=0:22:10.62

O:\>_
```

Příklad použití SNMPv3 v jednotce Poseidon s MGSoft Mib Browser: Nastavení

The screenshot shows the MG-SOFT MIB Browser Professional interface. The main window displays the MIB tree on the left and the 'SNMP Agent Profiles' list in the center. A dialog box titled '192.168.2.71 Properties' is open, showing the 'SNMPv3 Properties' tab. The 'Security user name' is set to 'public'. The 'Authentication protocol' is set to 'HMAC-MD5' and the 'Privacy protocol' is set to 'CBC-DES'. A 'Password For Authentication Protocol' dialog is also open, showing a password field and a 'Hide typing' checkbox.

Výsledek příkazu Walk

The screenshot shows the MG-SOFT MIB Browser Professional interface with the 'Query results' pane displaying the output of an SNMPv3 Walk command. The results are as follows:

```

72: inpAlarmSetup.8 (InputAlarmSetup) inactive(0)
73: inpAlarmSetup.10 (InputAlarmSetup) inactive(0)
74: inpAlarmSetup.11 (InputAlarmSetup) inactive(0)
75: inpAlarmSetup.12 (InputAlarmSetup) inactive(0)
76: inpAlarmSetup.13 (InputAlarmSetup) inactive(0)
77: inpAlarmState.1 (InputAlarmState) normal(0)
78: inpAlarmState.2 (InputAlarmState) normal(0)
79: inpAlarmState.3 (InputAlarmState) normal(0)
80: inpAlarmState.4 (InputAlarmState) normal(0)
81: inpAlarmState.5 (InputAlarmState) normal(0)
82: inpAlarmState.6 (InputAlarmState) normal(0)
83: inpAlarmState.7 (InputAlarmState) normal(0)
84: inpAlarmState.8 (InputAlarmState) normal(0)
85: inpAlarmState.9 (InputAlarmState) normal(0)
86: inpAlarmState.10 (InputAlarmState) normal(0)
87: inpAlarmState.11 (InputAlarmState) normal(0)
88: inpAlarmState.12 (InputAlarmState) normal(0)
89: inpAlarmState.13 (InputAlarmState) normal(0)
90: outValue.1 (OnOff) error(0)
91: outValue.2 (OnOff) error(0)
92: outValue.3 (OnOff) error(0)
93: outValue.4 (OnOff) error(0)
94: outName.1 (ObjectName) BinOut 1 142.69.6E.4F.75.74.20.31 (hex) Size = 8)
95: outName.2 (ObjectName) BinOut 2 142.69.6E.4F.75.74.20.32 (hex) Size = 8)
96: outName.3 (ObjectName) BinOut 3 142.69.6E.4F.75.74.20.33 (hex) Size = 8)
97: outName.4 (ObjectName) BinOut 4 142.69.6E.4F.75.74.20.34 (hex) Size = 8)
98: outType.1 (OutputType) onOROff(0)
99: outType.2 (OutputType) onOROff(0)
100: outType.3 (OutputType) onOROff(0)
101: outType.4 (OutputType) onOROff(0)
102: outMode.1 (OutputMode) manual(0)
103: outMode.2 (OutputMode) manual(0)
104: outMode.3 (OutputMode) manual(0)
105: outMode.4 (OutputMode) manual(0)
106: sensAlarm.1 (SensorAlarm) Sensor 240 [03.05.6E.73.0F.72.20.32.34.30 (hex) Size = 10]
107: sensState.1 (SensorState) normal(1)
108: sensString.1 (SensorString) 22 2 C [32.32.2E.32.20.43 (hex) Size = 8]
109: sensValue.1 (SensorValue) 222
110: sensValueRaw.1 (SensorValue) 222
111: sensID.1 (SensorID) 00073
112: sensUnit.1 (UnitType) unitless(12)
113: sensUnitString.1 (SensorUnitString) C [43 (hex) Size = 1]
114: poseidon.30.1.0 (Integer) 0
115: poseidon.30.2.0 (Integer) 141 days 14h:10m:00s.00h (1223340000)
116: poseidon.30.3.0 (Integer) 300
117: poseidon.30.4.0 (Integer) 1
118: poseidon.30.5.0 (InstanceName) no such instance
119: takAlarmEvent.0 (GroupID) 0
120: infoAddressMAC.0 (DisplayString) 00.0A.59.04.04.6E [30.3A.30.41.3A.35.39.3A.30.34.3A.30.34.3A.45.30 (hex)]
121: unitType.0 (UnitType) unknown(0)
122: sensSetupName.1 (SensorName) Sensor 240 [03.05.6E.73.0F.72.20.32.34.30 (hex) Size = 10]
123: sensFlags.1 (SensorFlag) 8
124: sensLimitMax.1 (SensorValue) 0
125: sensLimitMin.1 (SensorValue) 0
126: snmpTrapOID.0 (OBJECT IDENTIFIER) 2.20.32768.49714.13380.58.12340
127: snmpTrapOID.0 (OBJECT IDENTIFIER) 2.20.32768.49714.13380.58.12340
128: [Lasted: 1915.155.581] snmpTrapEnterprise.0 (OBJECT IDENTIFIER) null
Start time : 14. 4. 2019 10:48:50
End time : 14. 4. 2019 10:48:52
Duration : 24.687ms
----- SNMP QUERY FINISHED -----
    
```