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 událostí (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

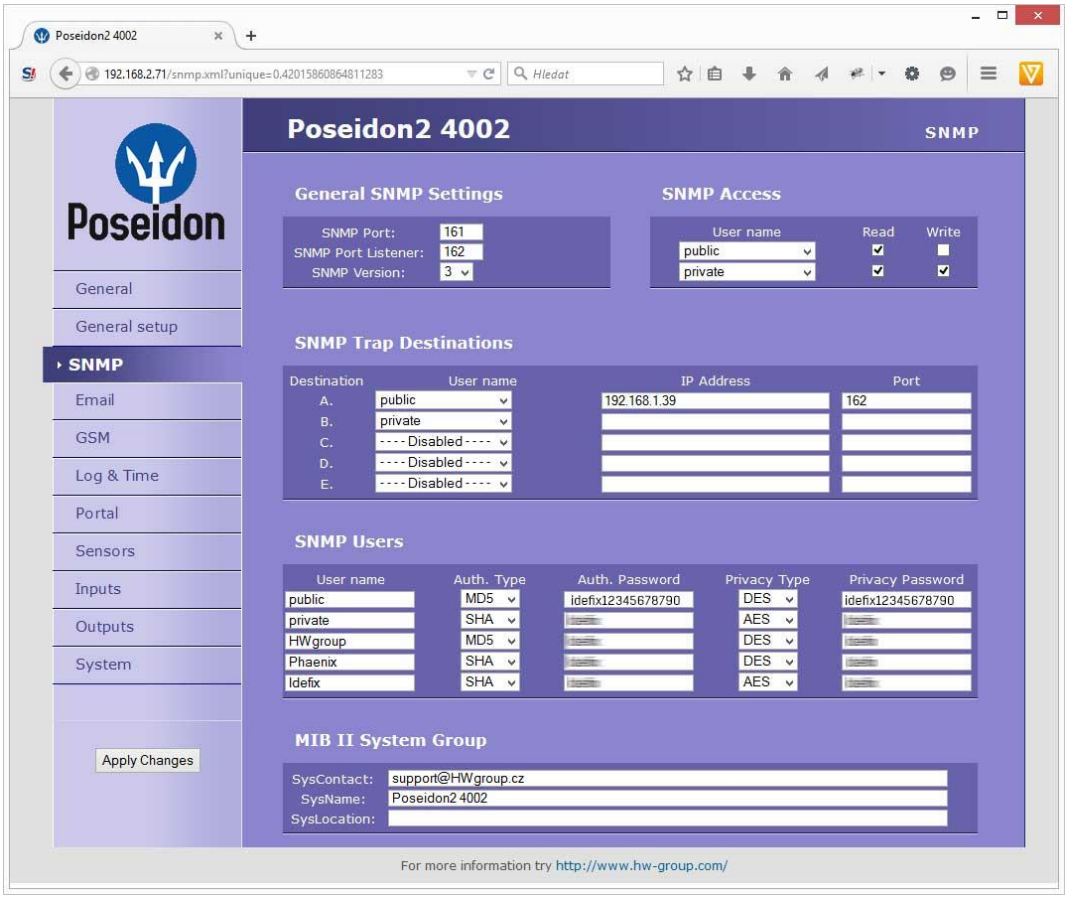
stává plnohodnotný management protokol i do nejnáročnějších korporátních sítí. Hlavní výhodou pak je, že MIB zůstává stejná, není tedy třeba žádných zvláštních úprav při přechodu na SNMPv3.

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:

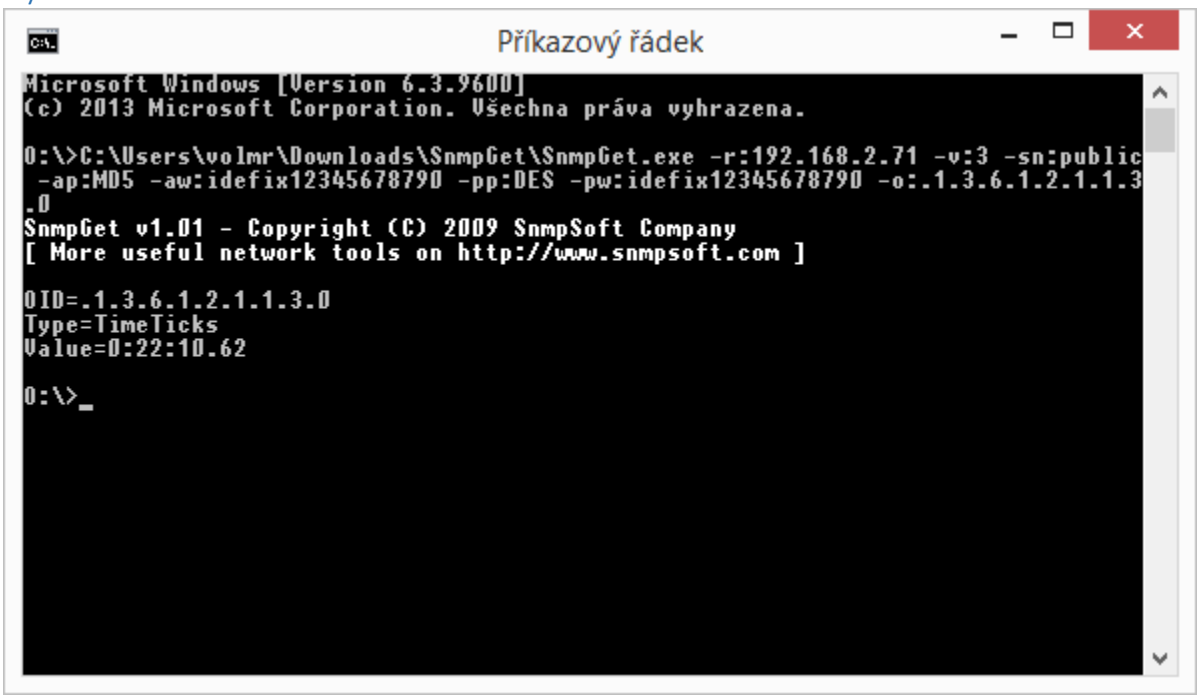
Webové rozhraní Poseidonu2 4002 se SNMP nastavením



Příklad použití SNMPv3 v jednotce Poseidon se SNMPget:

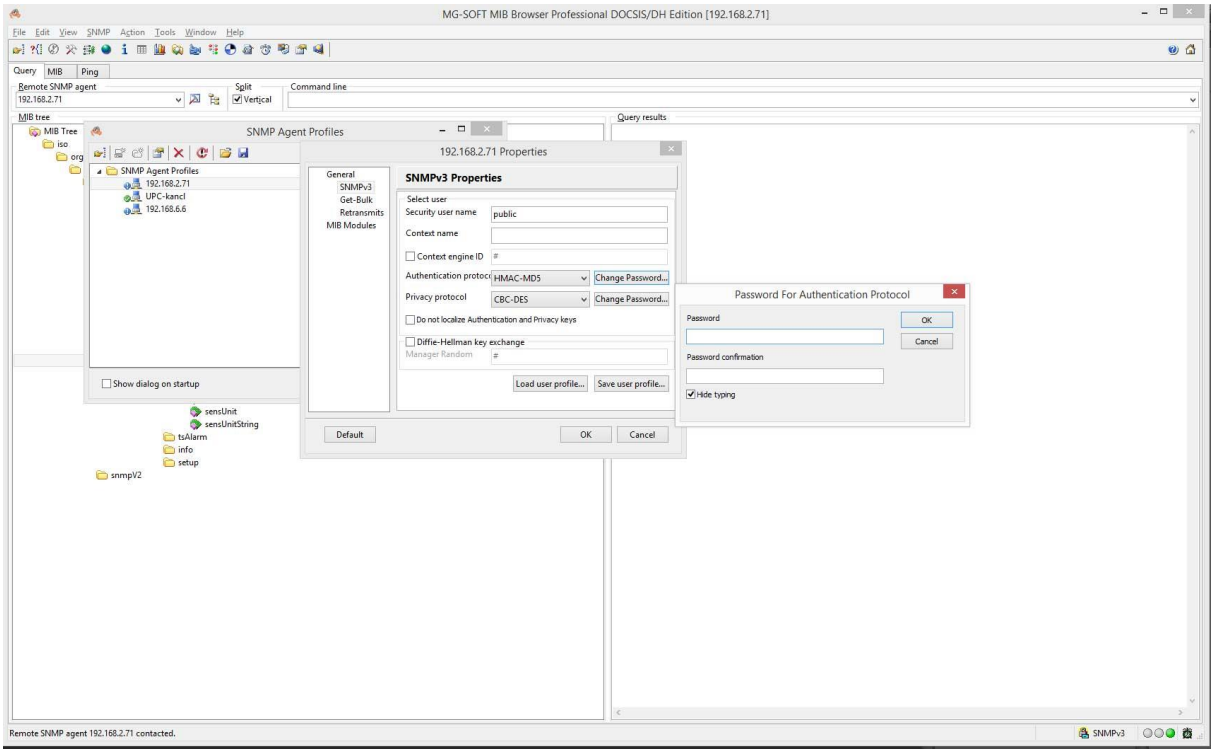
C:\Users\volmr\Downloads\SnmpGet\SnmpGet.exe -r:192.168.2.71 -v:3 -sn:public -ap:MD5 -aw:idefix12345678790 -pp:DES -pw:idefix12345678790 -o:.1.3.6.1.2.1.1.3.0

Výsledek:



Příklad použití SNMPv3 v jednotce Poseidon s MGSoft Mib Browser:

Nastavení



Výsledek příkazu Walk