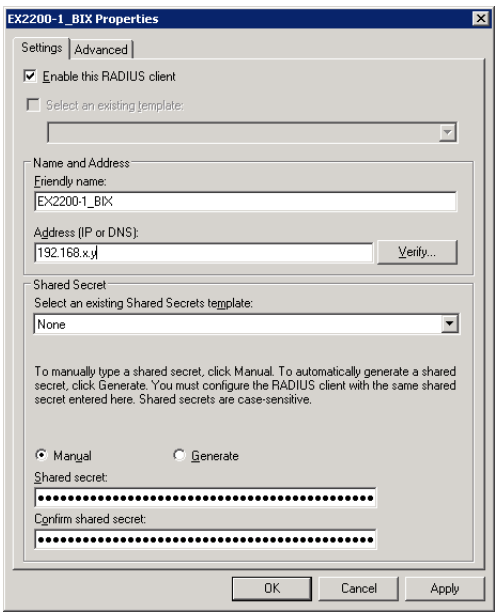
JUNOS Radius Authentikáció és Authorizáció Windows Server 2008 R2 NPS-sel

A RADIUS AA (Authentikáció és Authorizáció) azért jó, mert ha van sok-sok Juniper eszközünk, nem kell mindegyiken local felhasználókat létrehoznunk különféle jelszavakkal, hanem központilag már létező (Windows AD) felhasználók (pl. rendszergazdák) hozzáférhetnek az eszközökhöz tartományi jelszavukkal. Az előnyök a teljesség felsorolása nélkül:

- nincs local user / password, egyszerűbb konfig
- központi felhasználó ellenőrzés, pl. kirugott rendszergazda központilag kitiltható minden eszközből
- csak tartományi jelszó házirendnek megfelelő jelszavak használhatóak
- jelszó lejárat, account lockout házirend érvényes
- központilag látható az eszközökre történő belépés
- NPS policy-kkel szabályozható a belépés (pl. csak hétköznap 08:00-17:00)
- könnyű jogosultsági audit

Windows 2008 R2 NPS beállítása

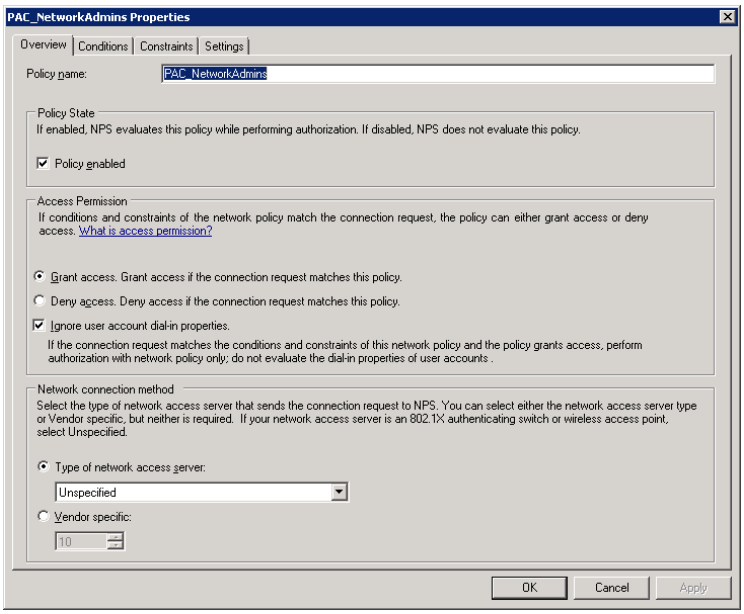
Ha feltelepítettük az NPS role-t, akkor elsőnek vagyük fel RADIUS kliensként az eszközünket:



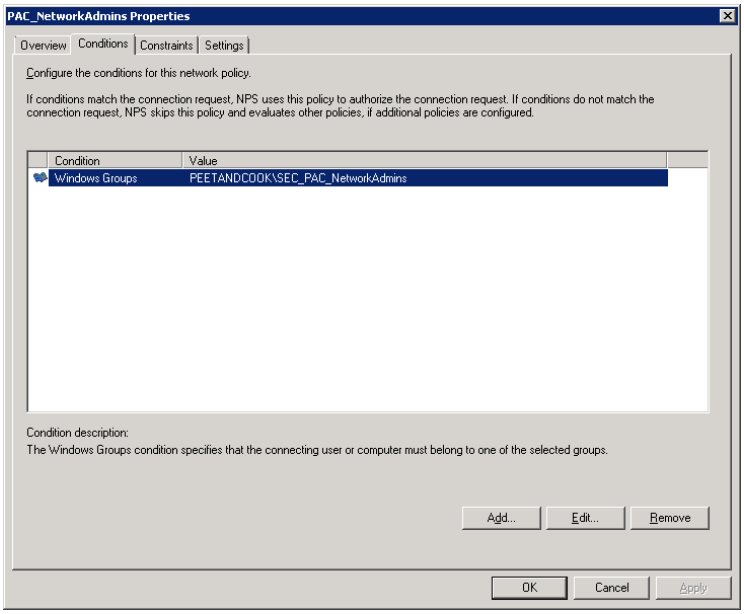
Ezután engedélyzzük az alapértelmezett „Use Windows authentication for all users” connection request policy-t.

Következő lépésben hozzunk létre két AD csoportot: egyik csoport tagjai full, a másik tagjai read-only jogokat fognak kapni.

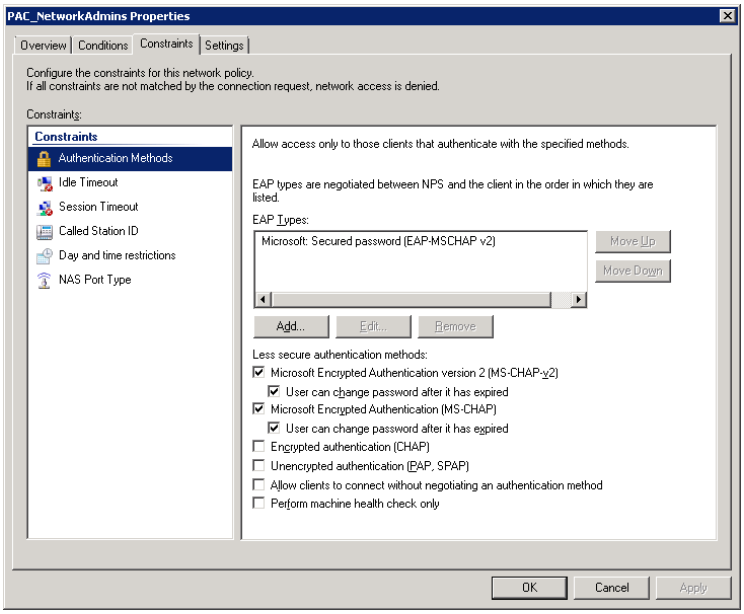
Hozzunk létre egy Network Policy-t:



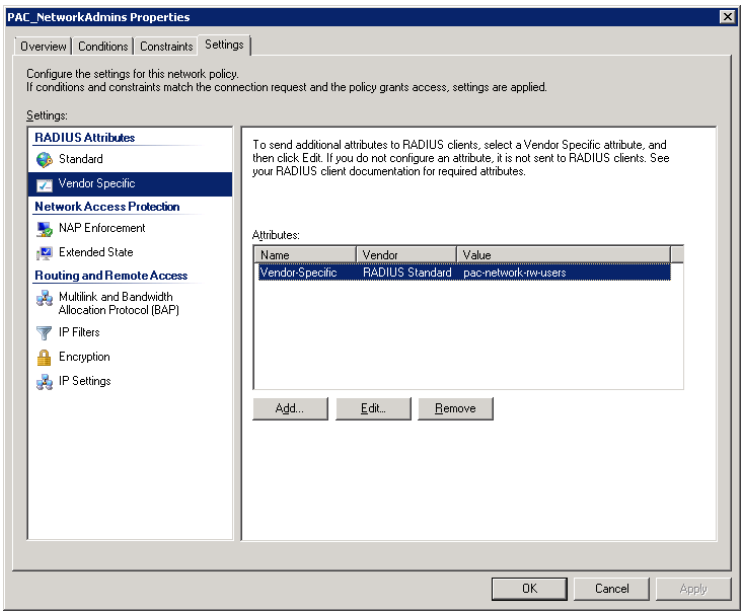
Állítsuk be feltételnek a Conditions fülön a Windows csoportunk tagságát:



Fontos beállítás a Constrains fülön a hitelesítési lehetőség:

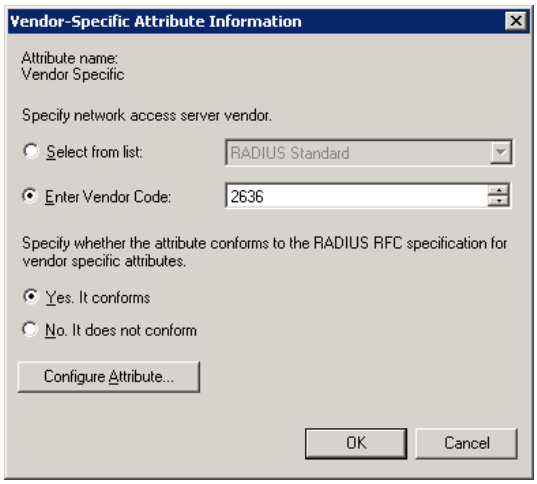


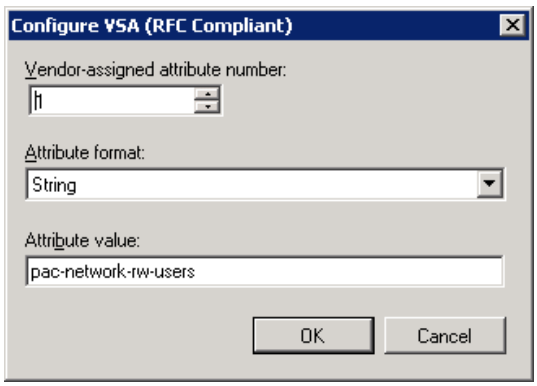
Következő lépés a VSP attribútumok felvétele, ezt a Setting fülön tehetjük meg:



Itt az alábbi beállítások szükségesek:

- Event vendor code: 2636
- RFC conform
- Attribute type: string
- Attributum





Az Attribute value értéke bármi lehet; majd a Junos konfigban erre az értékre hivatkozunk.

Értelemszerűen két Network Policy-t készítünk; a kettő közötti különbség csak a Windows csoporttagsági feltétel és az Attribute value értéke.

Junos konfiguráció

Ezután konfigurálhatjuk a Junos-t, itt nincs semmi extra, a konfig magától értetődik:

```
[edit system]
radius-server {
    192.168.x.y {
        port 1812;
        secret
"$9$9UmFCtOrlM7dbIENdVs4o5TznCpKvLVwgUjmTFnu0M8XxVYjiqm5Q8XDHkPzFp0BEcrlK8-
dwLx2oGUkqpuOBSe8L7Y2oAp01hSKvjik.Qn1IhvWx/Cu1IESy24aGi.n/CBRcKMZUiq5TlKvLX
NgoGqPTp0VYoaGU3n/tpORhyleW69EylKx7ZUj"; ## SECRET-DATA
    }
}
radius-options {
    password-protocol mschap-v2;
}
```

```
login {
    class PAC_Admins {
        idle-timeout 30;
        login-alarms;
        permissions all;
    }
    user pac-network-ro-users {
        uid 2002;
        class read-only;
    }
    user pac-network-rw-users {
        uid 2003;
        class PAC_Admins;
    }
```

Értelemszerűen a radius-server IP-je a Windows 2008 R2 NPS szerver; a secret a Radius kliens jelszó, amit a Windows oldalon is beállítottunk. A user { } tag egyezik meg a RADIUS attribútummal. A class direktívával állítjuk be a jogosultsági szintet. A konfigurációban azért csináltam külön PAC_Admins szerepkört (holott a super-user beépített szerepkör használható lenne), mert így külön definiálva lett az idle-timeout, illetve belépéskor az adminisztrátorok automatikusan megkapják az alert event-eket.

Ha mindent jól csináltunk, felhasználói fiókunk csoporttagsága alapján kapjuk meg a jogokat a Junos alatt is.

Természetesen lehetséges több jogosultsági szintet is felépíteni, a Junos erre lehetőséget ad, illetve a Network Policy-n több authentikációs feltételt is megadhatunk (Conditions fül) – itt az egyes feltételek között ÉS kapcsolat van.