STUDIJNÍ MATERIÁL PRO TECHNICKOU CERTIFIKACI
ESET Business Edition, ESET Remote Administrator

Eset software spol. s r.o., Meteor Centre Office Park, Sokolovská 100/94, 180 00 Praha 8
tel.: +420 233 090 233, fax: +420 233 090 230, obchod@eset.cz, www.eset.cz

Vzdálená správa

ESET Business Edition – “obchodní balík“, obsahuje:
- Klientská řešení (NOD32, ESS, + verze s Mirror)
- ESET Remote Administrator (ERA) – nástroj pro vzdálenou správu (dokonalý přehled o stavu klientů + údržba)

ERA v 2 - kompatibilita pro starší i novější klientská řešení
ESET Remote Administrator není antivirem (firewallem-antispamem!!!) – 2 součásti
- **server** (ERAS) – služba, sbírá informace od klientů na Windows stanicích, zasílá na ně požadavky, spolupracuje s konzolí
- **klient** – konzole (ERAC) – grafický nástroj pro správce sítě

ESET Remote Administrator Server (ERAS)

- nutný OS na bázi Windows NT (NT4 SP6 minimum)
- přítomnost komponenty Microsoft Data Access ComponentMDAC (problém u NT4)
- vlastní databáze (MDB), není potřeba externích DB
- pouze služba, žádné GUI

Standardně se instalujte do %ProgramFiles%\ESET\Eset Remote Administrator\Server
Činnost protokolována do ERA.LOG v %ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\logs
- ERAS může, ale nemusí běžet na stejném stroji s MIRROR serverem
- na stejném stroji by MĚLO běžet klientské řešení pro Windows (přejímání čísla aktuální virové databáze)

Od verze 2.0 je součastí ERAS i mirror!
Instalace:
- pozor na název serveru (měl by být „viditelný“ z LAN), eventuálně žádný neuvádět (doplní se)
- bude požadován .LIC soubor

Licenční klíč – soubor *.LIC

Omezuje množství „stanic“ spravovaných přes konzoli
- pokud počet převýšen, zobrazí se prvních x
- pokud klíč expirován, konzolí se nelze k ERAS připojit
- pokud klíč neexistuje, časově neomezená pro 2 stanice

Výměna klíče v ERA Console: Tools – Server Options – Renew License
- Alternativa: zkopírovat do %ALLUSERSPROFILE%\Application Data\Eset\Eset Remote Administrator\Server\license, restartovat službu ERA.EXE

Případné chyby jsou protokolovány do ERA.LOG

ESET Remote Administrator Console (ERAC)

Standardně v %ProgramFiles%\ESET\Eset Remote Administrator\Console\
Dvě instalační varianty:
- pro Win 98/ME
- pro systémy na bázi Windows NT

Součástí ERAC je ESET konfigurační editor, kompatibilní pro NOD32 i verzi 3

Připojení ERAC k ERAS

Komunikace standardně probíhá na portu TCP 2223 (výjimky ve firewallech)

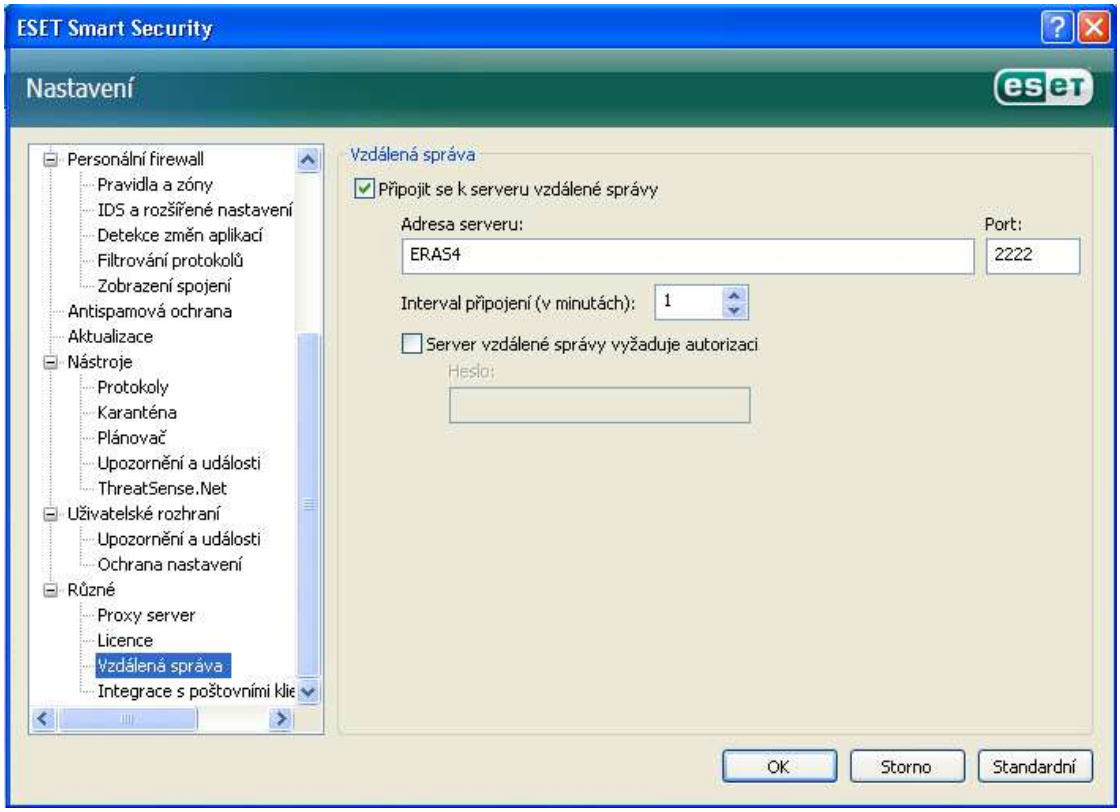
- ERAS identifikujeme jménem nebo IP adresou
- Komunikaci mezi ERAC a ERAS je šifrovaná
- možnost nastavení hesla pro přihlášení, standardně není žádné heslo

Připojení stanic k ERAS

Komunikace standardně probíhá na portu TCP 2222 (výjimky ve firewallech)

- ERAS identifikujeme jménem nebo IP adresou
- komunikace zahájena vždy stanicí, v pravidelných intervalech (standardně 5 minut)

Možnost ochránit připojení heslem Tools – Server Options – Security (zároveň šifrovaná komunikace) – na obou koncích!



stanice ---> ERAS, aktuální stav (verze, protokoly, alerty, konfigurace...)
stanice <--- ERAS, úlohy, požadavky na konfiguraci, vzdálenou instalaci...
Stanice jsou identifikovány

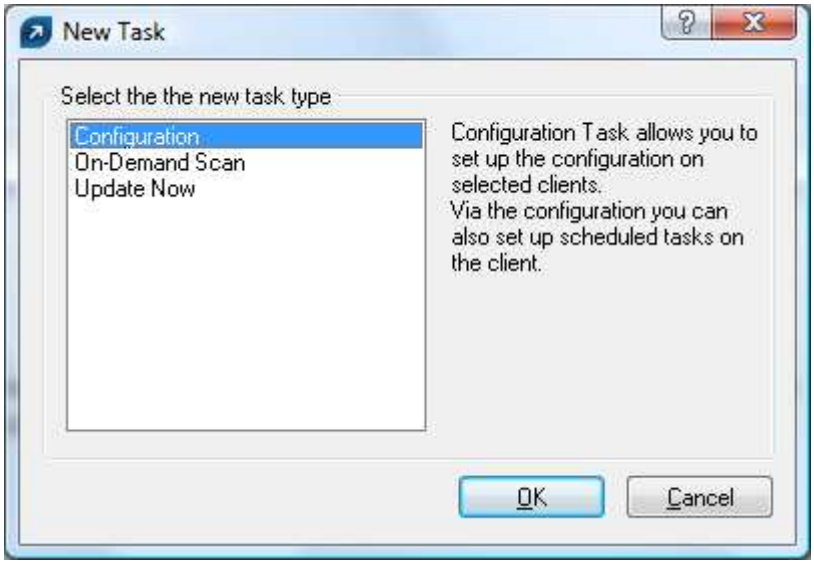
- Computer name +
- MAC address +
- Primary Server

Úlohy - Tasks

Vzdálená správa ESET umožňuje zasílat na stanice požadavky k

- změně konfigurace - Configuration
- vykonání testu – On-demand Scan
- okamžité aktualizaci – Update Now

Pozor na rozdíl volání úloh přes kontextové menu, tj. pravým tlačítkem myši na klienta vs. volání z menu /CTRL + N/

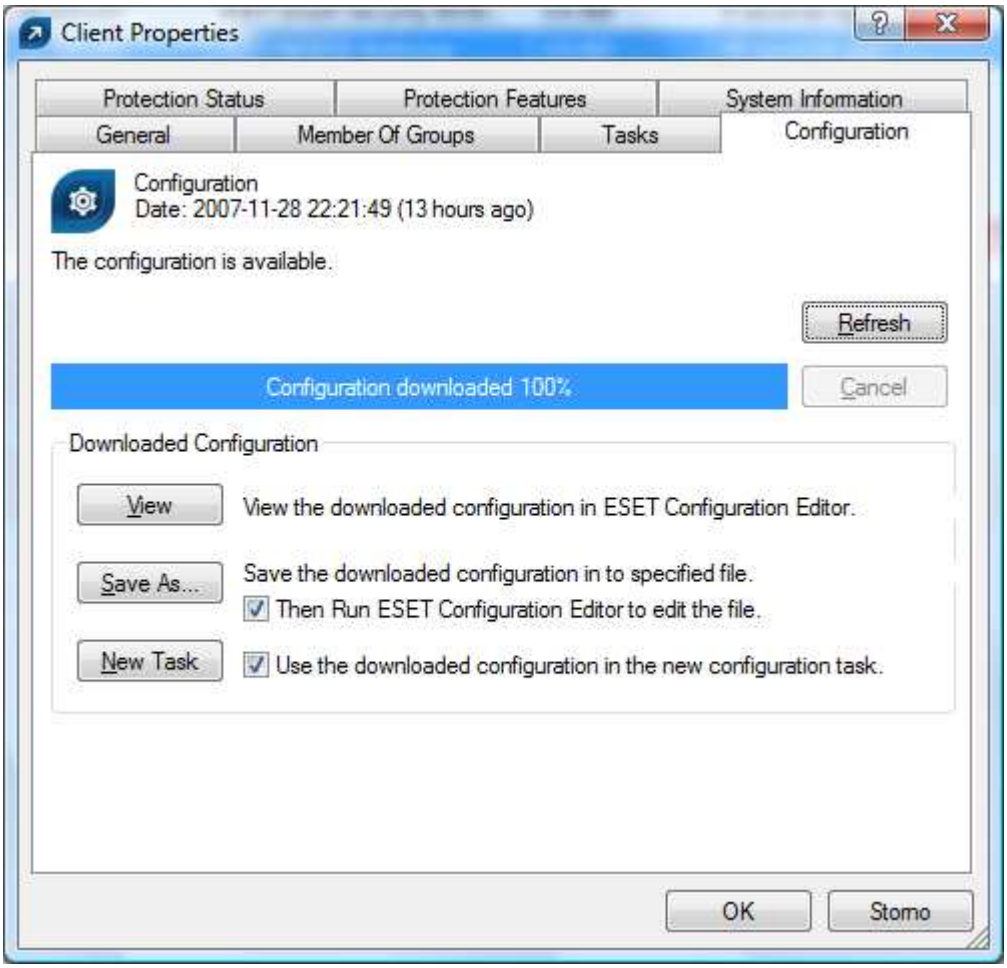


DOPORUČENÍ:
Vytvořte si sadu XML šablon pro různé úlohy

Úloha – KONFIGURACE

Pracuje s konfiguračním editorem. Je možné:

1. **vytvořit nové xml počas tvorby úlohy**
2. **použít vlastní xml šablonu**
3. **použít existující konfiguraci klienta a upravit ji:**
   - klik pravým tlačidlem na PC v záložce Clients ---> Configuration
   - zatrhnout obě zaškrtávací políčka
   - klik na New Task ---> Edit
   - upravit konfigurace, klik na Console
   - Odeslat



Pozor na změnu úloh v plánovači - vazba na RegID

Úloha – ON-DEMAND SCAN

UPOZORNĚNÍ:
Pozor na volbu “Scan without cleaning” – standardně probíhá kontrola bez léčení/mazání souborů.

Vzdálená instalace

MSI formát
Více metod

- PUSH instalace pro NT systémy
- instalace prostřednictvím „agenta“ (email, logon skript)
- využití metod, které jdou mimo program

Postup vzdálené instalace

Vytvoření instalačního MSI balíčku (klíčová nastavení) – package:
- identifikován názvem
- obsahuje „instalačky“ pro klienty (NOD32/ESS, NT/9x)
- obsahuje předdefinovanou .XML konfiguraci
- obsahuje parametry volané při instalaci (SETUP.EXE)

Samotná distribuce balíčku na cílové stanice

PUSH metoda vzdálené instalace

Podmínky:
- cílová stanice musí být „viditelná“ („okolní počítače“)
- cílová stanice musí být v provozu
- musíme znát účet administrátora (domén.admina)
- povoleno sdílení (i ve firewallu (XP)
- zakázáno jednoduché sdílení souborů (XP, vlast. složky)

Proces instalace:
1. **autorizace /jméno a heslo zadané adminem/**
2. **připojení k ADMIN$ & kopírování agenta einstaller.exe**
3. **registrace agenta jako služby & spuštění**
4. **připojení agenta k serveru (TCP 2224) & stáhnutí balíku (package) & zahájení instalace**

Instalační Agent – einstaller.exe

Každý balík má svého agenta (einstaller.exe)
V einstaller.exe je pevně zakódováno
- k jakému balíku patří (jeho jméno)
- z jakého serveru „pochází“ (jeho hostname)

Proto je důležité správné jméno ERAS!
Činnost agenta je protokolována do %TEMP%\einstaller.log

Vzdálená instalace prostřednictvím e-mailu, logon skriptu

Není nutno použít funkce přímo v konzoli - einstaller.exe lze spustit jinou libovolnou cestou
Export agenta pomocí ERAC:
- záložka Remote Install - Export... (do souboru nebo logon skriptu)

Jiná než PUSH metoda na NT systémech
- pozor na autorizaci (volba Set default logon... na záložce Remote Install)

Chybové stavy při vzdálené PUSH instalaci

Může se vrátit chyba s SC a GLE kódem
- SC, interní
- GLE – Win32 Error Code (seznam na stránkách Microsoftu)

!	***Could not set up IPC connection to target computer (SC error code 6, GLE error code 1326)***
1.	Nesprávné jméno a heslo /pro přístup k dané stanici/

Chybové stavy v „závěrečné části“ vzdálené instalace **=** chyby einstaller.exe
Protokol v %TEMP%\einstaller.log

Replikace

Umožňuje vytvářet hierarchii ERA serverů cation
- TCP port 2846

Replikaci je potřeba povolit na obou koncích:

- na podřazených serverech Replication to
- na nadřazených Replication from

Eset software spol. s r.o., Meteor Centre Office Park, Sokolovská 100/94, 180 00 Praha 8
tel.: +420 233 090 233, fax: +420 233 090 230, obchod@eset.cz, www.eset.cz