# Centralizirana zaštita MS Windows računala

Igor Hitrec

SRCE

prosinac 2003

# Teme

- Centralizirana antivirusna zaštita SOPHOS programima
- Software Update Service (SUS)

# Demonstracija

- Server (Windows 2003 AD domena)
- Klijent (Windows XP Professional)

# Današnja tema nije:

- Kako virusi rade
- Kako napraviti virus
- Antivirusna zaštita ne-Windows platformi
- Ostali antivirusni proizvodi na tržištu

# Sadržaj - Sophos

- Uvod
- Centralna distribucija SAV klijenta
- **SAVAdmin** alat
- Nadogradnja **CID-a**
- Sophos Enterprise Manager (**SophosEM**)

# UVOD

- Antivirusna zaštita kao dio sigurnosne politike

- Više linija obrane
  - Na svakom klijentskom računalu
  - Na datotečnim i e-mail poslužiteljima

# Aktivna obrana

- "Pasivne" mjere
  - zabrana potencijalno opasnih (exe,com,pif,vbs..) privitaka
  - *patch management*
- "Aktivne" mjere
  - antivirusni SW

# Centralizirana distribucija SAV klijenta[1]

- poseban *account*
  - kakve ovlasti?
- instalacija centralne distribucije na serveru
- instalacija klijenta uz pomoć centralne distribucije

# Centralizirana distribucija SAV klijenta$^2$

## Demonstracija

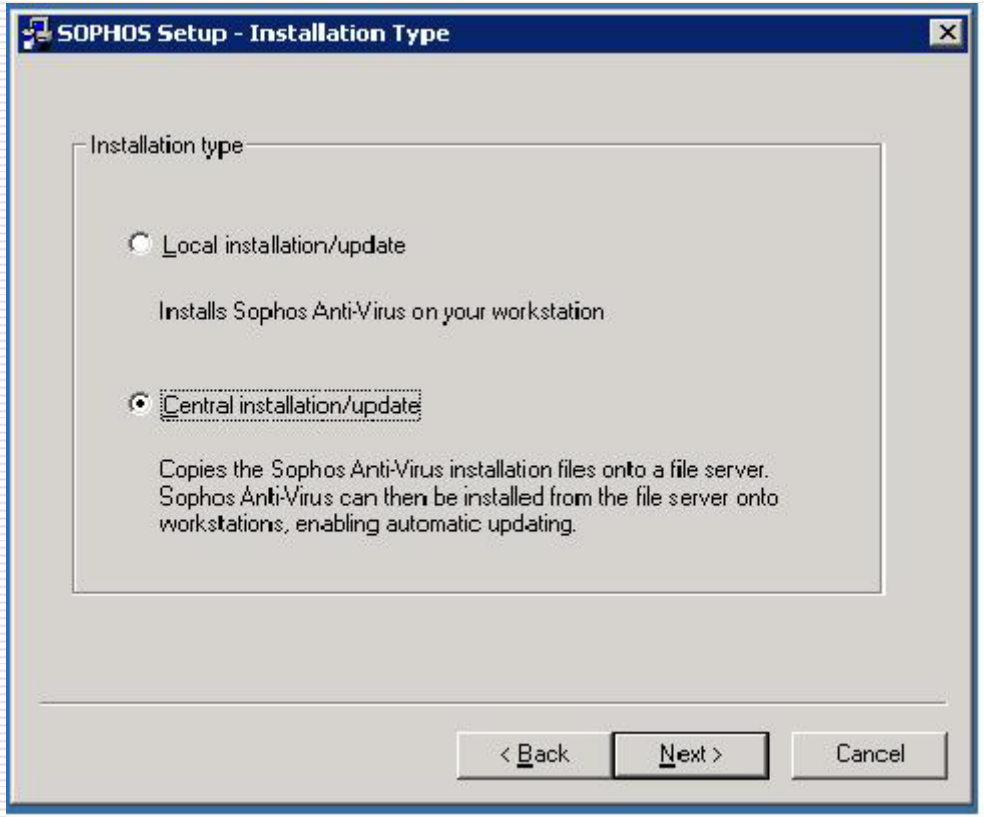
(5 min.)

Instalacija CIDa,

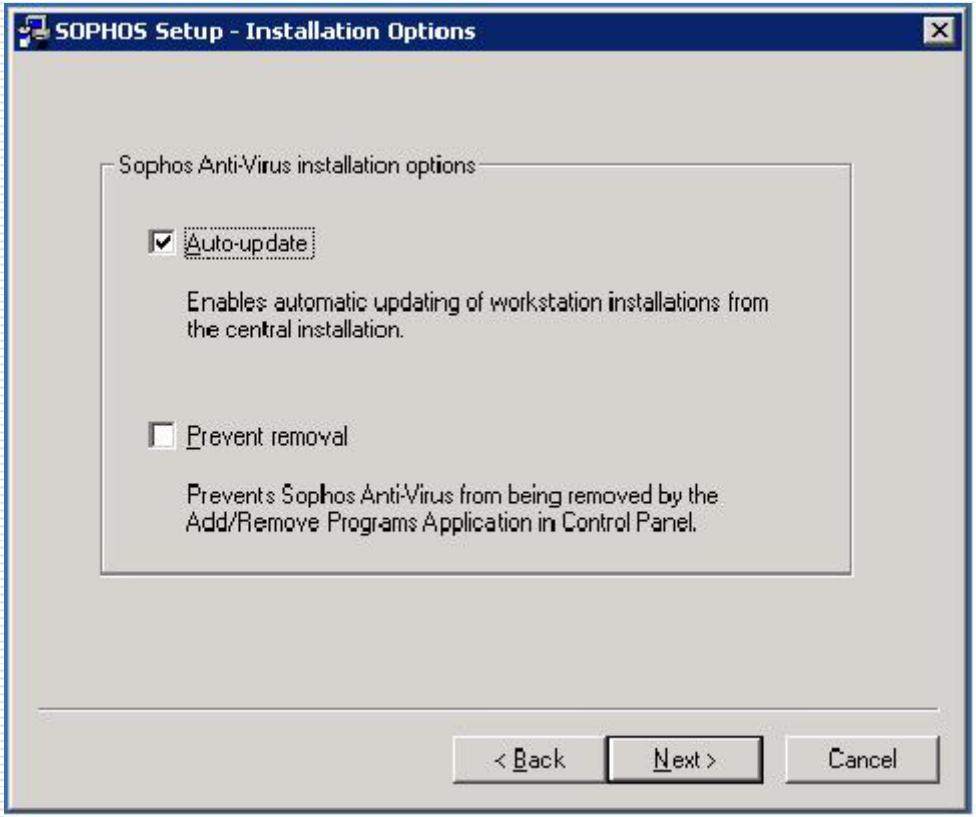
InterChk Servera i

InterChk klijenta

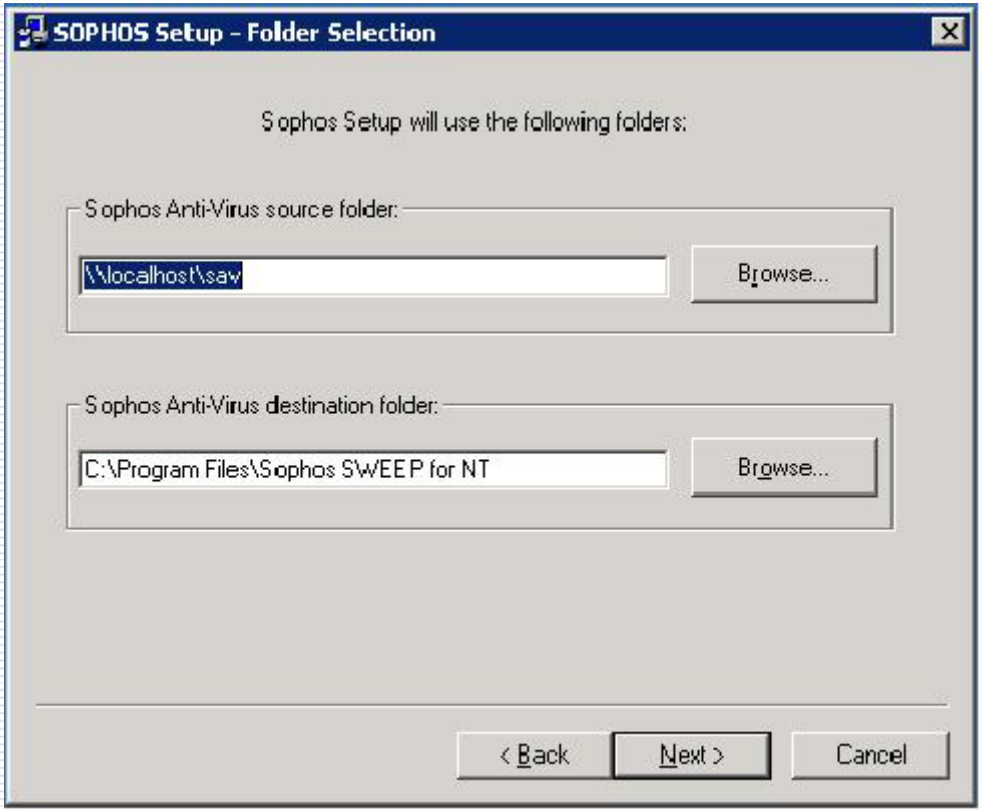
# CID – instalacija centralne distribucije



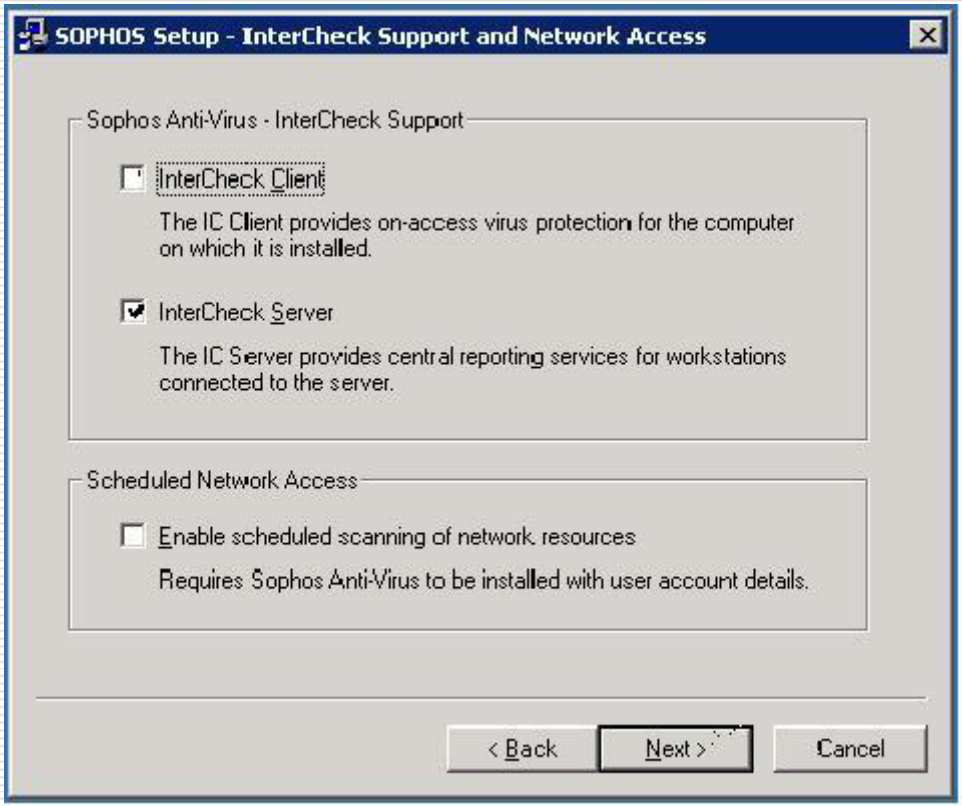
# CID – odabir AUTO-UPDATE opcije



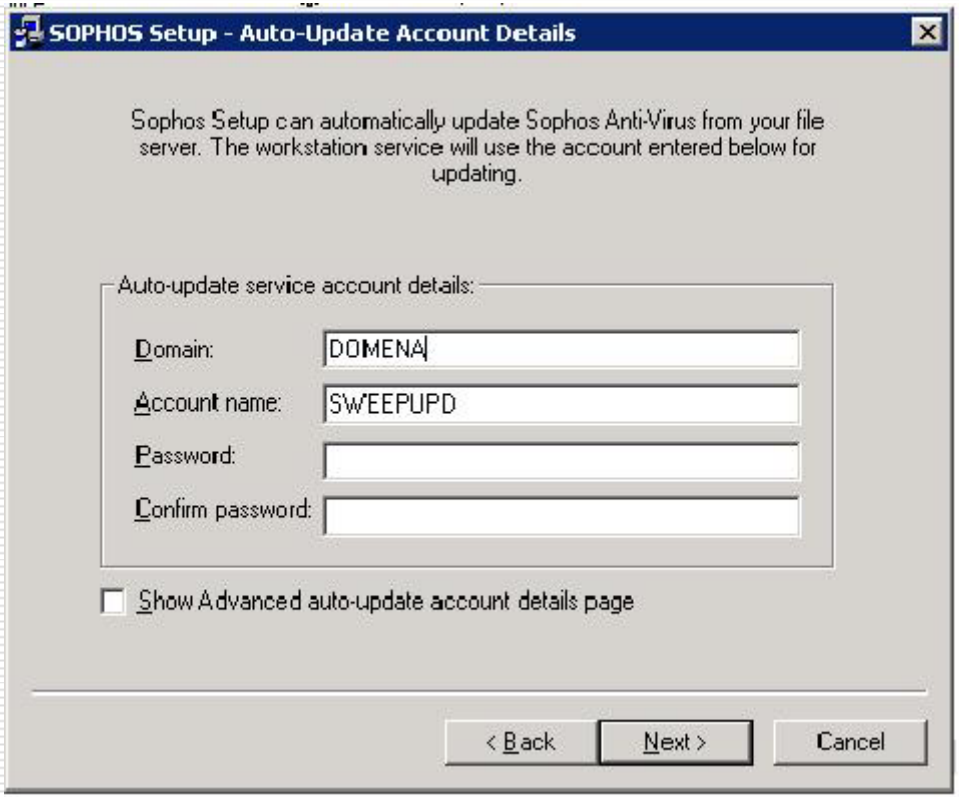
# CID – instalacija klijenta sa CIDa



# CID – odabir InterChk server opcije



# CID – odabir domenskog accounta



# CID – instalirani servisi

Instalirani servisi na SAV CID serveru i klijentu:

- SWEEPSRV.SYS (SAV servis)
- SWNETSUP.EXE (SAV Network)
  - SWUPD acc
- SWUPDATE.EXE (SAV Update)

# Nadzor i održavanje **SAVAdmin** alatom [1]

- Instalira se sa Sophos Enterprise Managerom ili kao zasebna aplikacija
- NADZOR: verzija SAV klijenta, broj& IDE datoteka, aktivnost InterCheck monitora...
- ODRŽAVANJE: generiranje skriptnih zadataka, ručna nadogradnja klijenata i servera, promjena dodjeljenog SAV CID servera, promjena servisnog accounta, pokretanje instalacije SAV klijenta na novom domenskom računalu...

# Nadzor i održavanje **SAVAdmin** alatom 2

## Demonstracija

Instalacija

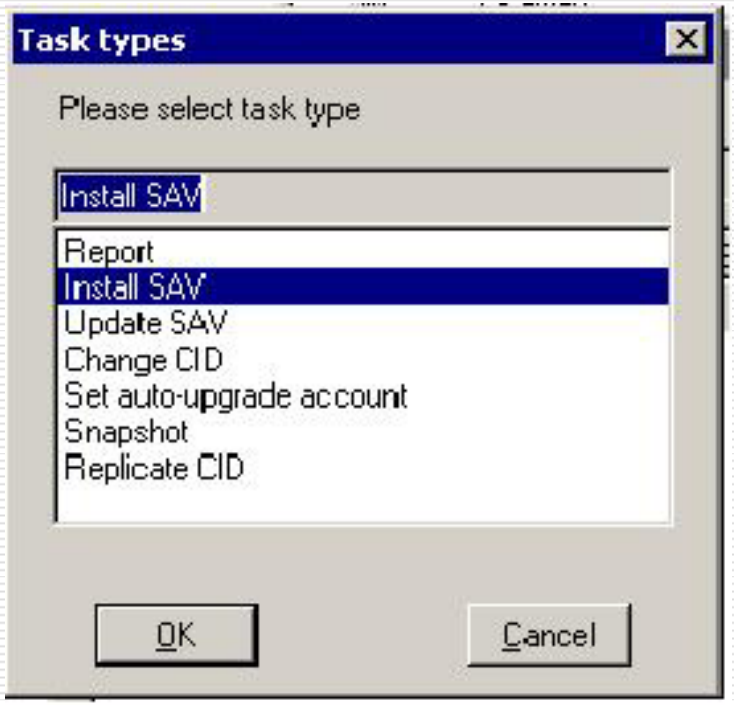
(5 min.)

# Nadzor i održavanje **SAVAdmin** alatom 3

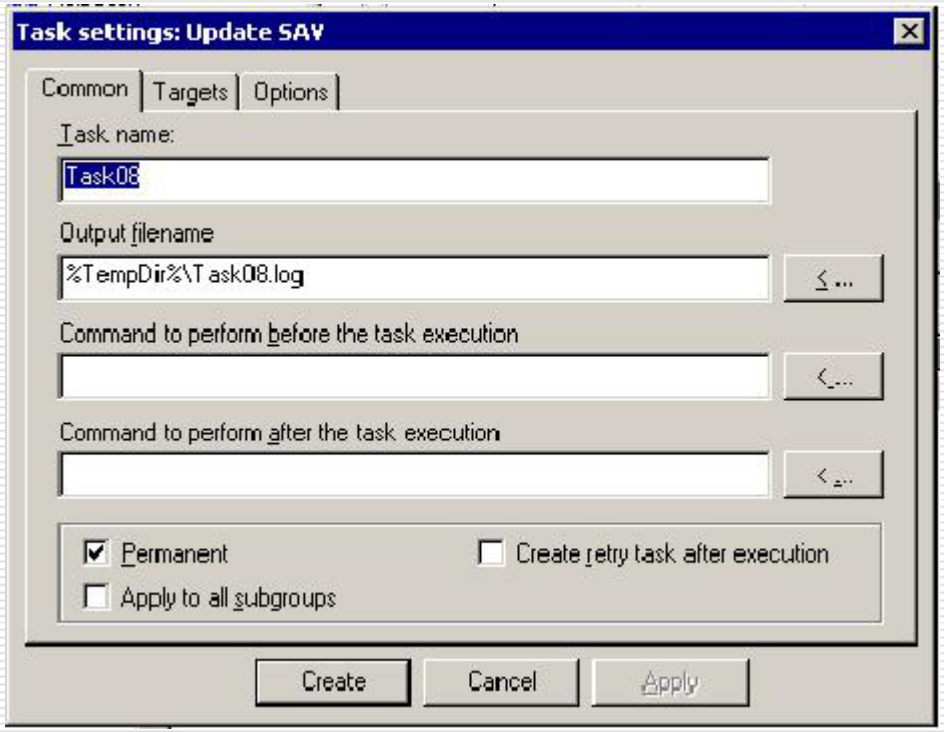
Demonstracija

taskovi, update, install, snapshot
(15 minuta)

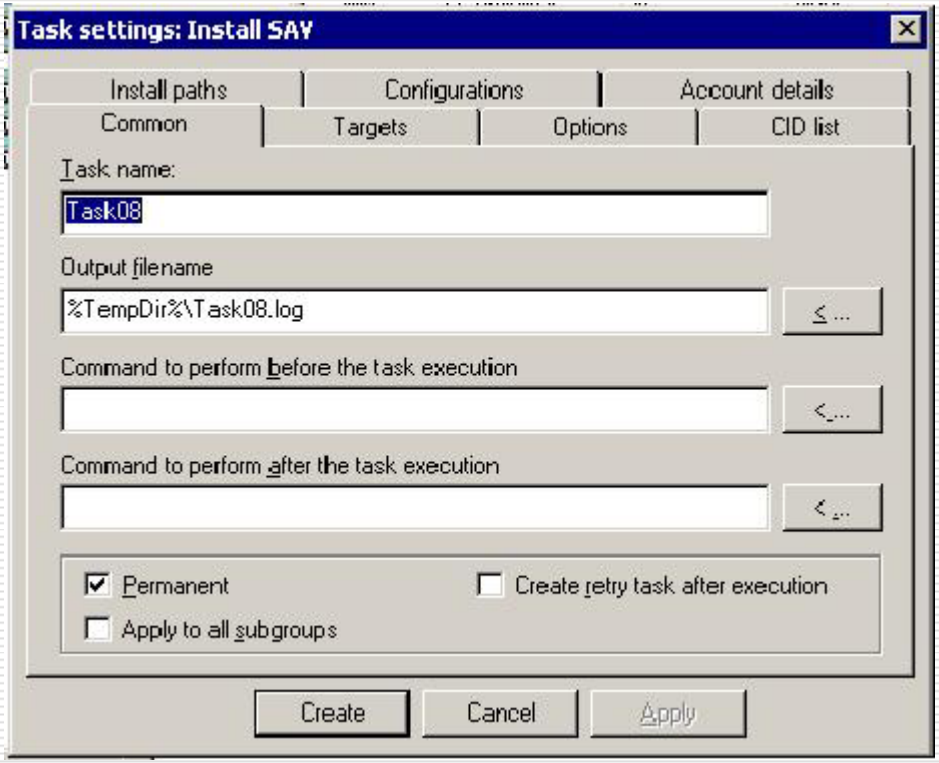
# Taskovi


Task types
Please select task type
Install SAV
Report
Install SAV
Update SAV
Change CID
Set auto-upgrade account
Snapshot
Replicate CID
OK
Cancel

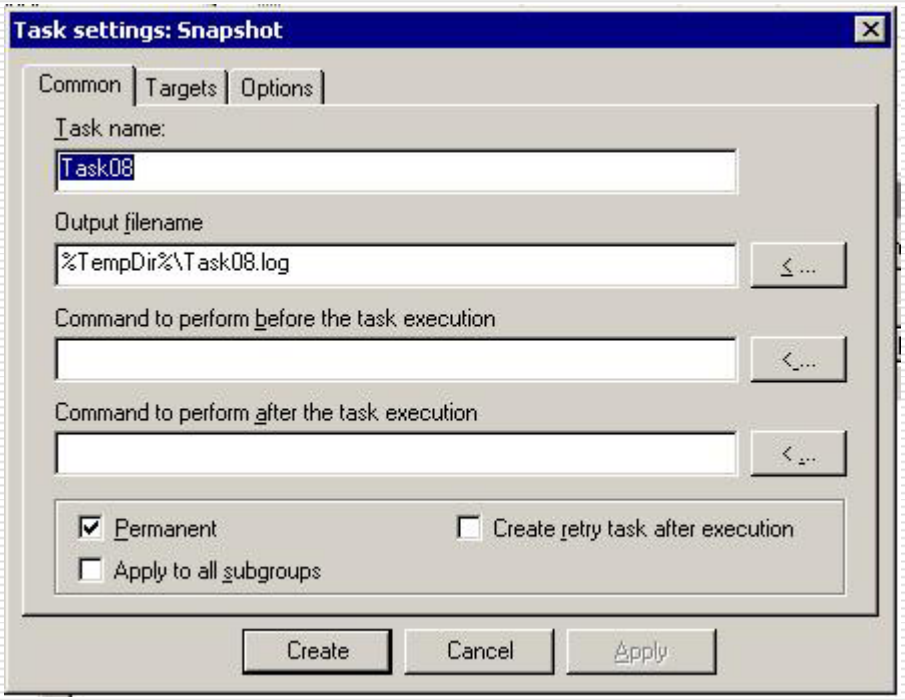
# Update


Task settings: Update SAV
Common
Targets
Options
Task name:
Task08
Output filename
%TempDir%\Task08.log
Command to perform before the task execution
Command to perform after the task execution
Permanent
Create retry task after execution
Apply to all subgroups
Create
Cancel
Apply

# Install


Task settings: Install SAY
Install paths
Configurations
Account details
Common
Targets
Options
CID list
Task name:
Task08
Output filename
%TempDir%\Task08.log
Command to perform before the task execution
Command to perform after the task execution
Permanent
Create retry task after execution
Apply to all subgroups
Create
Cancel
Apply

# Snapshot


Task settings: Snapshot
Common
Targets
Options
Task name:
Task08
Output filename
%TempDir%\Task08.log
Command to perform before the task execution
Command to perform after the task execution
Permanent
Create retry task after execution
Apply to all subgroups
Create
Cancel
Apply

# Nadogradnja **CID-a** [1]

- Iz CID-a se nadograđuju klijenti
- Kako nadograđivati CID?
- Wget, unzip

  http://www.sophos.com/downloads/ides/web_ides.zip
- Problem: stare IDE datoteke koje ne mogu biti zamjenjene novijom i ispravnijom verzijom -> riješenje je primjena Sophos Enterprise Manager

# Nadogradnja **CID-a** 2

- Primjer batch skripte za dogradnju novim IDE datotekama:

```
cd c:\Program Files\Sophos SWEEP for NT\NTInst\i386
wget http://www.sophos.com/downloads/ide/web_ides.zip
"c:\Program Files\winzip\wzunzip" -o web_ides.zip
del web_ides.zip
```

- Ostaje problem nadogradnje samog SAV klijenta -> primjena Sophos Enterprise Managera

# SophosEM

- Rješenje za problem automatske nadogradnje i manipulaciju SAV klijentima i SAV servera
- Prati više verzija SAV aplikacija, razmena podataka http ili file share-om, scheduler
- SophosEM – “baza/library  i  CID”

# SophosEM
# Prije nego počnemo

Preduvjeti:

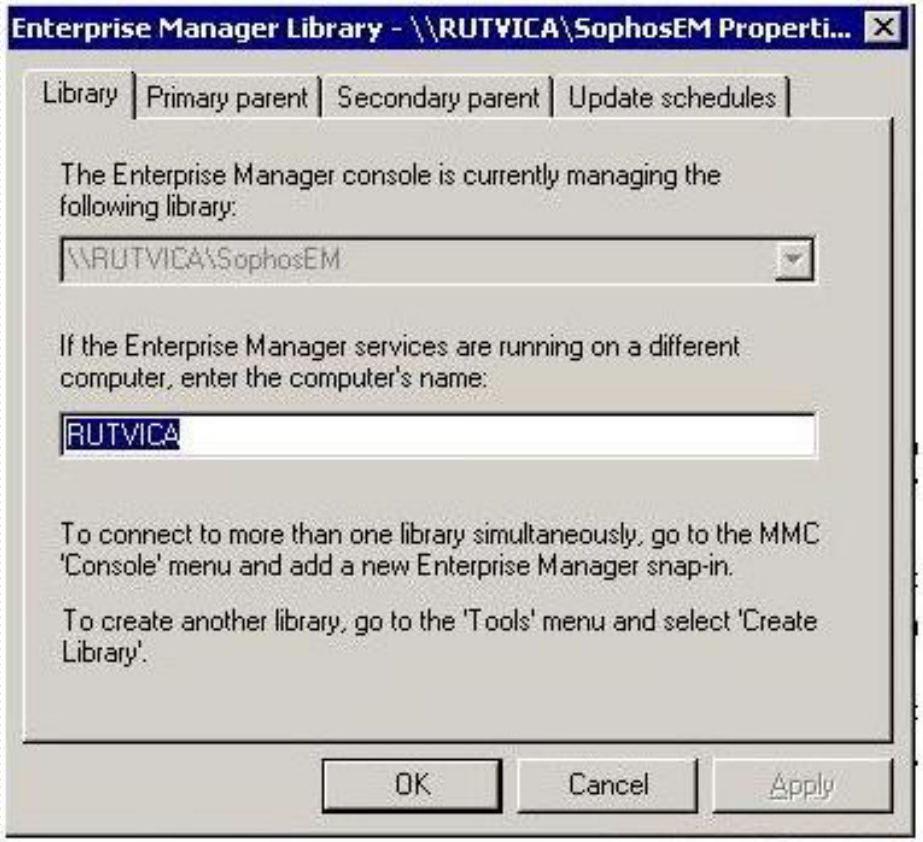
- provjeriti postojeće CID postavke
- obrisati postojeće IDE datoteke
- obrisati SAVAdmin alat
  - SophosEm će instalirati novu kopiju

# SophosEM Instalacija

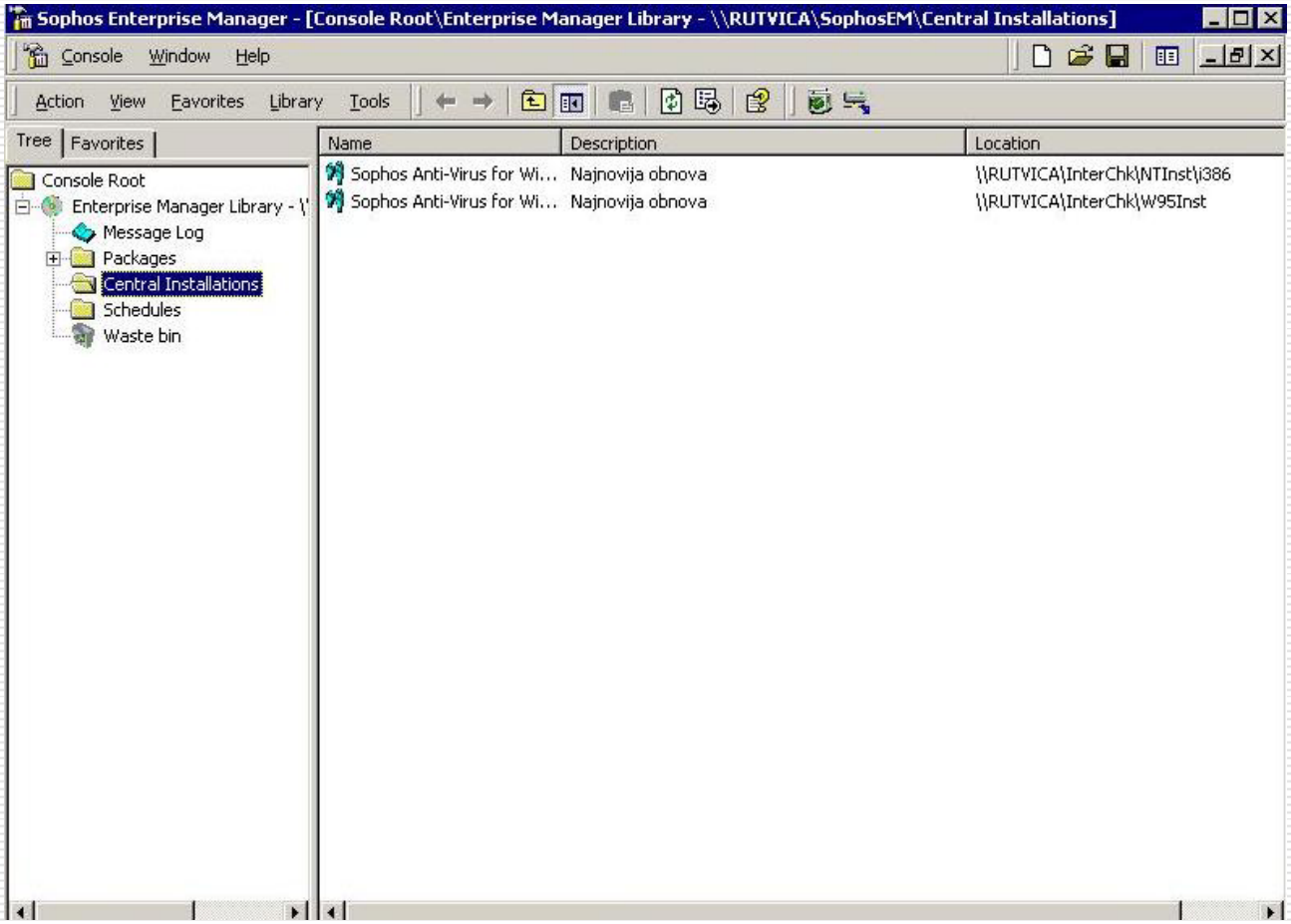
Demonstracija instalacije

(10 min.)

# SophosEM Library



# SophosEM
# CID



# SophosEM
# Aktivni servisi

- schdsrvc.exe (scheduler)
- rptsrv.exe (message logger)
- smsgsrv.exe (Sophos messages)
  - SWUPD acc

# SophosEM Deinstalacija

## 3 važna koraka

- %ProgramFiles%\Sophos Enterprise Manager\library\bin\setup.exe -remlib \\server\SophosEM\
- Uninstall /remove iz “Add/Remove Programs” ili “uninstall”
- Brisanje iz registry-a slijedeće stavke:
  \\HKLM\Software\Sophos\Sophos Enterprise Manager

restart nije potreban

*TEK SADA MOŽEMO PONOVO INSTALIRATI SophosEM*

# Opcije

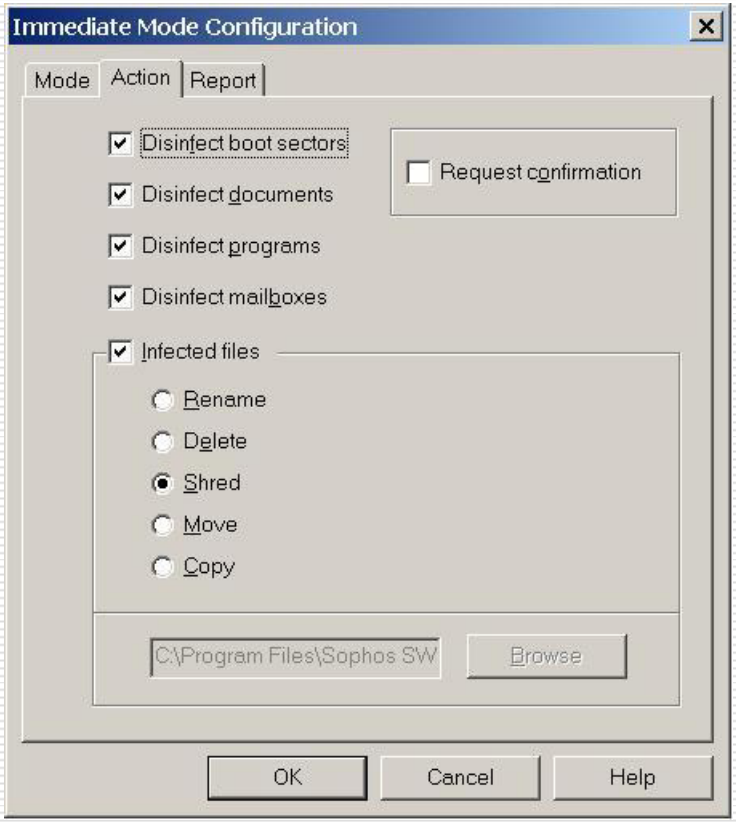
- All
- Unsubscribed
- Subscribed
- Published
- Central Installations (CID-s)
- Schedules

# SophosEM
# Problemi iz prakse

- distribucija bugovite SAV verzije
- “SAV account locked”
- “logon as a service right” prava preko group policy-a

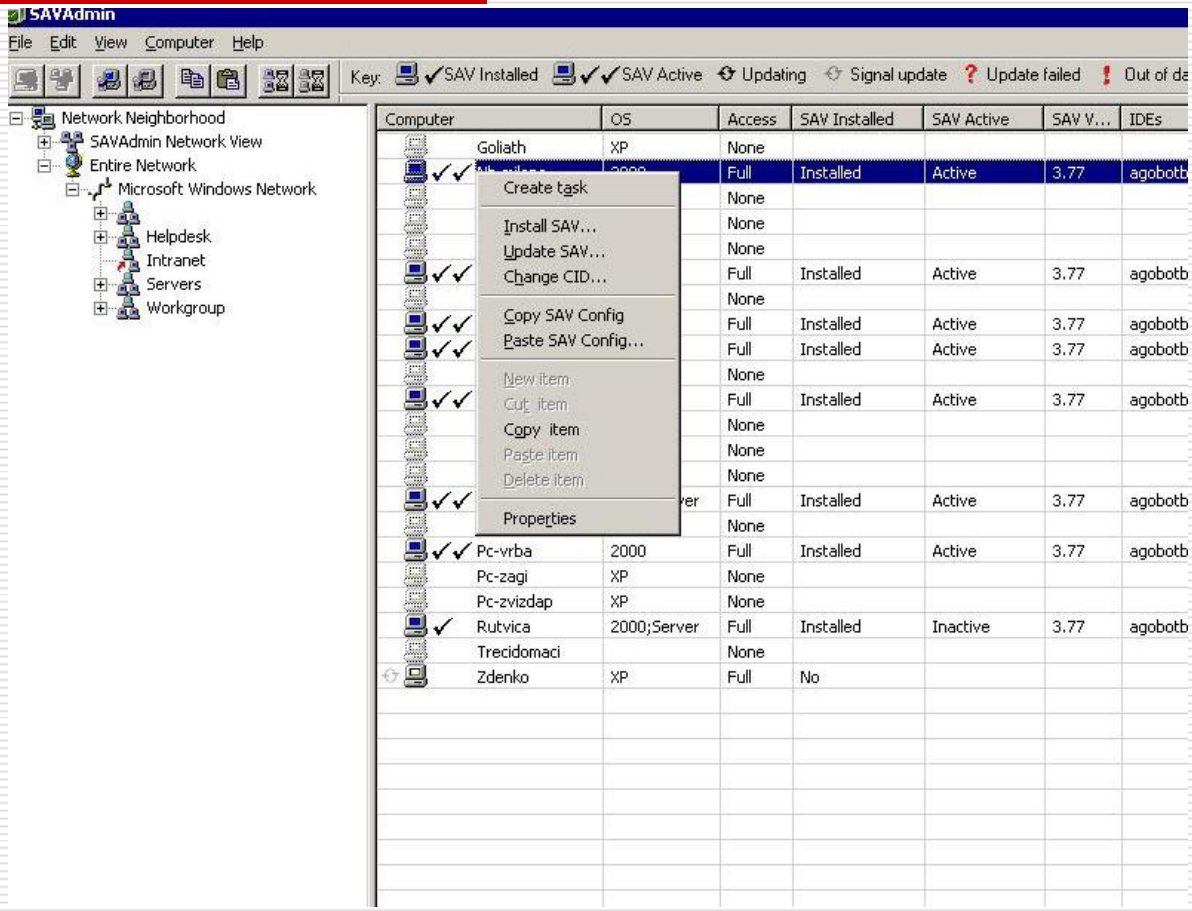
# SAV- korisno je znati...[1]

- distribucija CUSTOM konfiguracije SAVa



# SAV- korisno je znati...[2]

- distribucija CUSTOM konfiguracije SAVa



# SAV- korisno je znati...[3]

- podrška za RDP – MS Terminal Service (verzija 3.75 i viša)

- **instalacija** \\server\share\Setup.exe *-termclient*
- **update klijenta** x:\program files\Sophos SWEEP for NT\NTInst\i386\Setup.exe" *-termclient* -update

# Komentar

- Lucijan Carić, Qubis
- Preuzeto sa: BUG On Line
  http://www.bug.hr/ostav/caric9.asp

- “…velik broj administratora uopće nema potrebna ovlaštenja za primjenu sigurnosnih mjera. Vrlo često, umjesto da ih ohrabre i motiviraju, rukovodstva institucija djeluju protiv njih, jer prečesto staju na stranu prekršitelja pravila i izazivača problema, zato što se radi o "važnim" ljudima unutar institucije ili zato što jednostavno ne shvaćaju važnost zaštite informatičkih sustava - temeljne infrastrukture svake moderne institucije.

- Tako se malim bogovima u institucijama dodjeljuju administratorska prava na njihovim kompjuterima i segmentima mreže, modemi kojima se mogu spajati na Internet mimo "spore" zajedničke veze (zagušene brdom smeća kao što je pornografija, muzika, spam, te drugi "zabavni" sadržaji) i korporativnog firewalla, a njihova se prijenosna računala priljučuju na mrežnu strukturu institucije bez ikakve prethodne provjere.

- Suprotno pravilima i zdravom razumu omogućuje im se primanje izvršnih programa putem e-pošte i pristup ostalim zaposlenicima zabranjenim Internet stranicama. Nije rijetkost da takvi gurui zahtijevaju da se sa njihovih kompjutera deinstaliraju antivirusni i drugi zaštitni programi, jer im "usporavaju" rad i ograničavaju kreativnost, a kada izazovu nekakav problem koji informatičari danima ili tjednima moraju uklanjati, takvi junaci obično prvi prstom počnu pokazivati na nesposobne administratore sustava i njihove prevelike grijehove i propuste.

Pauza
(15 minuta)

# Software Update Service

# Sadržaj

- Patch management rješenja
- Karakteristike
- Prednosti/nedostaci
- Sistemski zahtjevi na klijentu/poslužitelju
- Instalacija
- Opcije konzole
- Načini distribucije
- SUS klijenti
- Konfiguriranje podrške za domenske klijente
- Konfiguriranje podrške za stand-alone klijente
- Windows Registry stavke
- Uočeni problemi
- Zaključak
- Pomoć

# SUS – patch management rješenja

**Patch management unutar okruženja ADa**

Microsoft Systems Management Server

http://www.microsoft.com/smserver/default.asp

PatchWorks

http://www.rippletech.com/products/PatchWorks/Prod_PW_Overview.htm

UpdateEXPERT

http://www.stbernard.com/products/updateexpert/products_updateexpert.asp

# SUS - karakteristike

- Koristi tzv “automatic update service”

- Windows 2000 SP3
- Windows XP SP1
- Windows 2003

# Prednosti

- Preusmjeravanje na lokalni CARNetov SUS poslužitelj

http://windowsupdate.carnet.hr

Umjesto na originalni

http://windosupdate.microsoft.com

# Prednosti

- Lokalna pohrana i praćenje izdanih zakrpi
- Kontrola nad distribucijom zakrpi
- Smanjeno opterećenje WAN linka

# Nedostaci

- Ne dozvoljava napredniji *patch management* deinstalacija zakrpi, praćenje stanja na klijentima
- MS Systems Management Server rješava nedostatke SUS-a

# SUS – sistemski zahtjevi na klijentu/poslužitelju

- **klijentska računala** - OS Windows 2000 SP4/ Windows XP SP1/Windows 2003 unutar Windows 2000/2003 Active Directory domene ili stand-alone računala, ostali klijenti zahtjevaju naknadnu instalaciju Automatic Update servisa
- **računalo SUS poslužitelj** - Windows 2000/2003 Server sa IIS 5.0/6.0, konfiguriran kao domain kontroler, member server ili stand-alone server

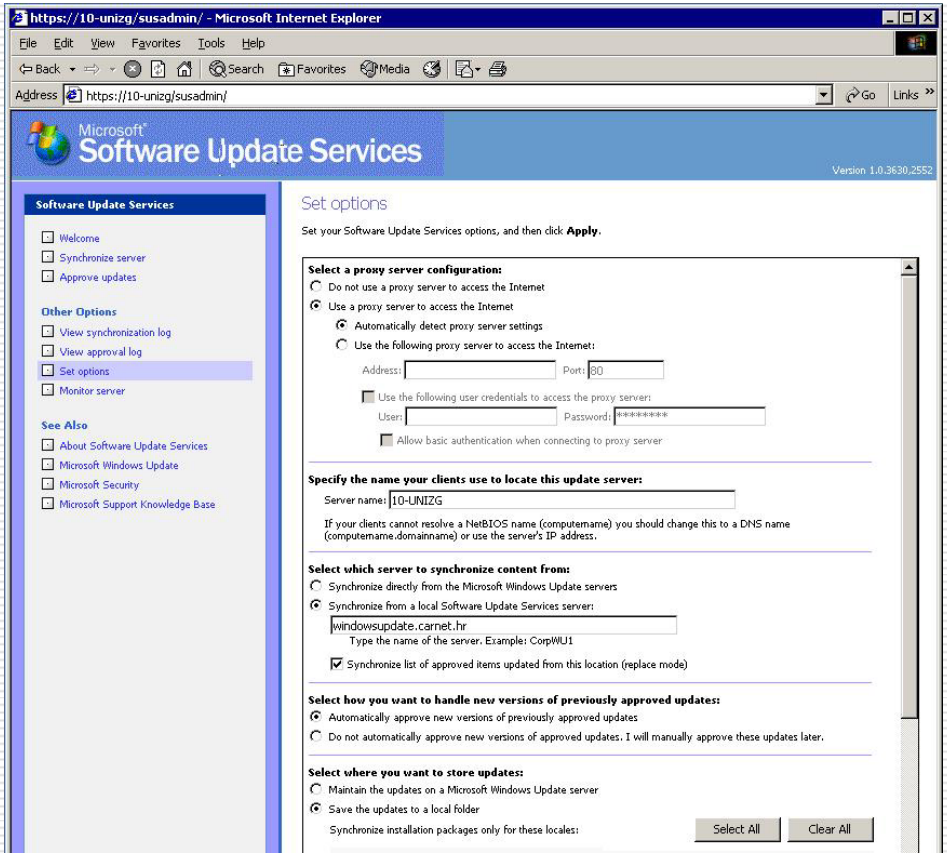
# SUS – instalacija servisa na poslužitelju

Instalacija servisa

(10 minuta)

# SUS – konzola

- opcije SUS servisa mogu se naknadno podesiti



# Opcije konzole

Demonstracija opcija SUS konzole

- Prvi korak – “Trusted site” ☺
- Opcije namještanja SUS-a
- NetBIOS/DNS ime

# SUS – načini distribucije

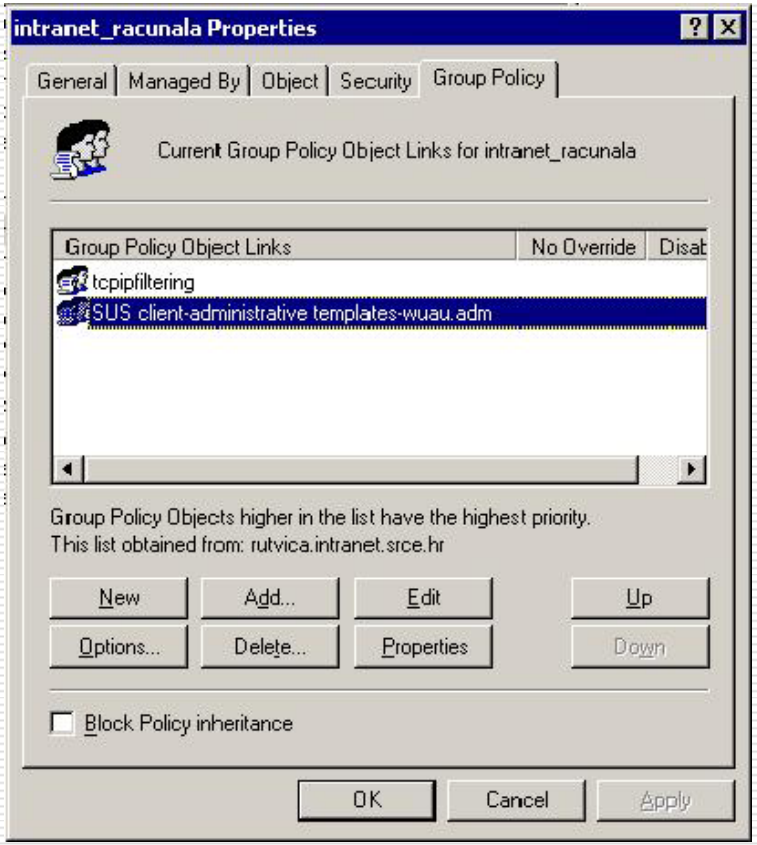
- Klijenti unutar domene
  - Poželjno!
- Samostojeći klijenti
  - stand-alone

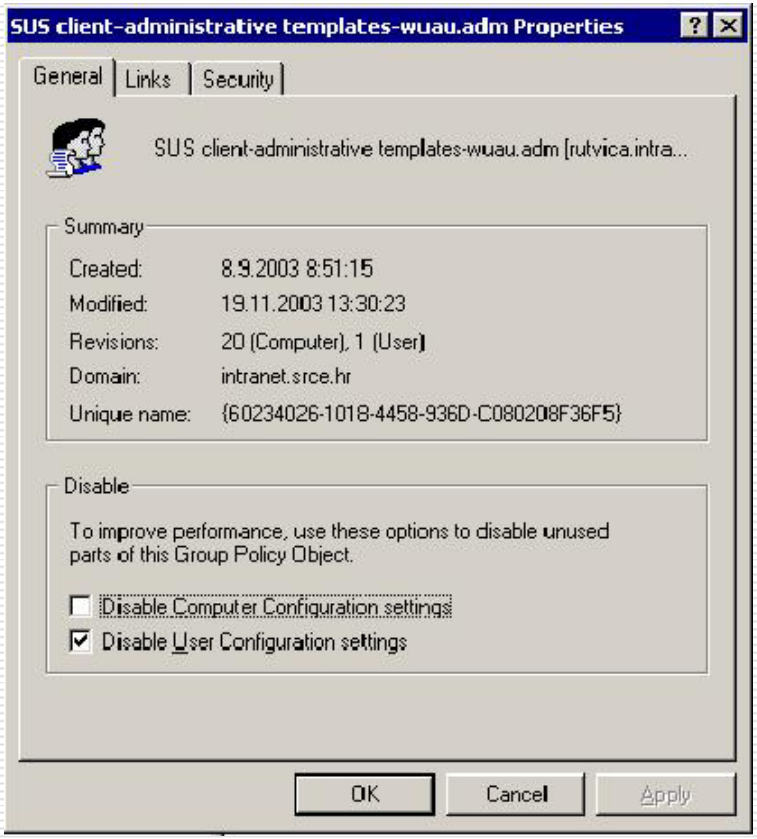
# SUS Klijenti

- potreban tzv. Automatic Update klijent (wuauserv)
- Windows 2000 sa SP2 i osnovni Windows XP zahtjevaju naknadnu instalaciju instalaciju Automatic Update klijenta

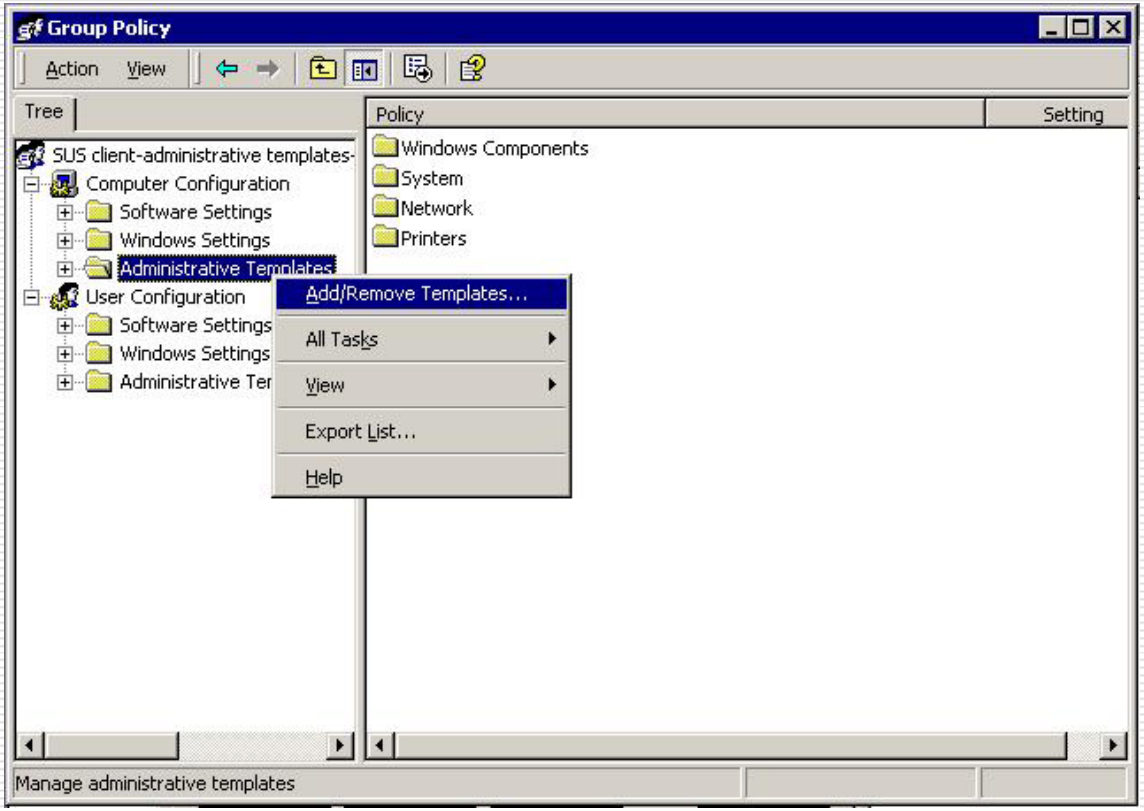
http://www.microsoft.com/windows2000/downloads/recommended/susclient

# SUS – instalacija klijentske strane (domain group policy) – policy properties

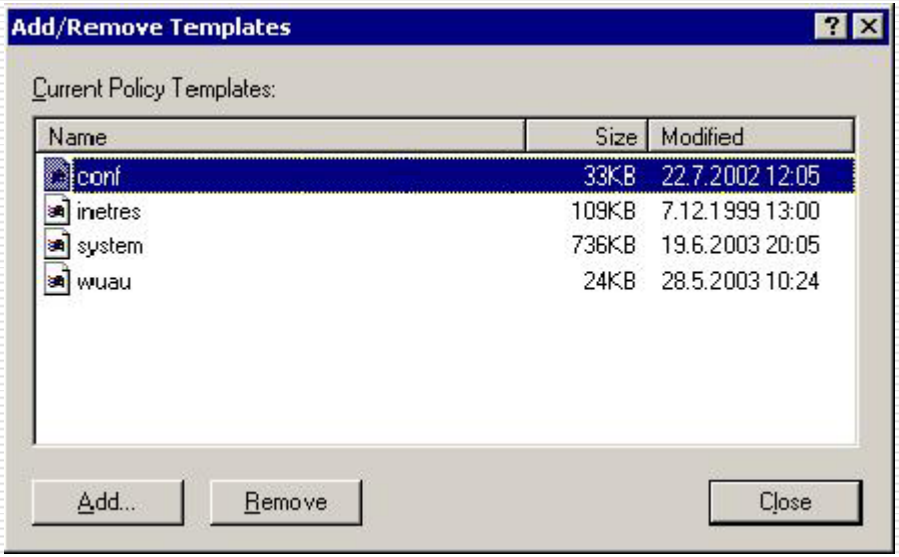


# SUS – instalacija klijentske strane (domain group policy) – add policy template



# SUS – instalacija klijentske strane (domain group policy) – odabir policy predloška



# SUS – konfiguracija podrške za stand-alone klijente

*Windows Registry Editor Version 5.00*

*[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate]*
*"WUServer"="http://**ime_SUS_poslužitelja**" **ili***
*"http://**ime_SUS_poslužitelja.domena.hr**"*
*"WUStatusServer"="http://**ime_SUS_poslužitelja**" **ili***
*"http://**ime_SUS_poslužitelja.domena.hr** "*

*[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU]*
*"UseWUServer"=dword:00000001*
*"NoAutoUpdate"=dword:00000000*
*"AUOptions"=dword:00000004*
*"ScheduledInstallDay"=dword:00000000*
*"ScheduledInstallTime"=dword:00000003*
*"RescheduledWaitTime"=dword:00000001*
*"NoAutoRebootWithLoggedOnUsers"=dword:00000000*

- *COPY/PASTE -> MERGE*

# SUS – Windows Registry stavke

- **Configure Automatic Updates** – opisuje način preuzimanja ispravki sa SUS servisa (obavijest o preuzimanju/instalaciji, automatsko preuzimanje/ručna instalacija, automatsko preuzimanje/instalacija) i vremenu instalacije dan u tjednu ili svaki dan u točno određeno vrijeme)
- **Specify Intranet Microsoft Update Service Location** – određuje http adrese SUS servisa sa kojega će klijenti preuzimati ispravke

# SUS – Windows Registry stavke

- **Reschedule Automatic Updates Scheduled Installation** – omogućuje da sustav nakon instalacije ispravki čeka do 60 minuta prije nego krene u restart.
- **No auto-restart for scheduled Automatic Updates Installations** – ukoliko je omogućena, ova stavka osigurava da korisnik lokiran na klijent računalo može izbjeći restart računala nakon instalacije ispravki

# SUS – uočeni problemi

- Učitavanje group policy-a nije uspjelo

  Win2000 - secedit /refreshpolicy machine_policy /enforce

  WinXP - gpupdate /force

- Redeploy već instaliranih zakrpi
  - potrebno je maknuti postojeću zakrpu i dozvoliti instalaciju nove
- Problem pristupa SUS konzoli preko web browsera
  - web adresu SUS servera je potrebno prijaviti kao “Trusted site” adresu

# Zaključak

- Windows klijent računala valja održavati kroz centralizirane sustave
- Automatiziran patch management i AV zaštita na klijentskim računalima
- Sigurnost manje ovisi o dobroj volji ili znanju korisnika
- Dodatna zaštita kroz sustav Active Directory-a (tema nekog drugog tečaja☺)

# Pomoć

- http://www.susserver.com
- Helpdesk za sistemce

  sistemac@carnet.hr
- http://sistemac.carnet.hr
- http://sav.srce.hr
- MS RefCentar

  http://www.srce.hr/MicrosoftSW/mshelpdesk