



chránime digitálne svety

NOD 32

antivirus system

**ESET NOD32 Antivírus
pre Novell Netware Server**

Inštalácia

Copyright © Eset, spol. s r. o.

Eset, spol. s r. o.
Svoradova 1
811 03 Bratislava
Slovensko

Obchodné oddelenie
e-mail: obchod@eset.sk
tel.: 02/59 30 53 11

Technická podpora
web: www.eset.sk/podpora
kontaktný formulár: <http://www.eset.sk/podpora/formular>
tel.: 02/59 30 53 53

Všetky práva vyhradené. Žiadna časť tejto publikácie nesmie byť reprodukováná žiadnym prostriedkom, ani distribuovaná akýmkoľvek spôsobom bez predchádzajúceho písomného povolenia spoločnosti Eset, spol. s r. o.

Spoločnosť Eset, spol. s r. o. si vyhradzuje právo zmien programových produktov popísaných v tejto publikácii bez predchádzajúceho upozornenia.

V knihe použité názvy programových produktov, firiem a pod. môžu byť ochrannými známkami alebo registrovanými ochrannými známkami príslušných vlastníkov.

REV.20071116-002

1. Úvod

Nasledujúca dokumentácia popisuje nasadenie produktu ESET NOD32 Antivírus pre Novell Netware Server, konkrétne:

- inštaláciu produktu,
- konfiguráciu jednotlivých modulov,
- zaistenie aktualizácie produktu.

ESET NOD32 Antivírus pre Novell Netware sa skladá z nasledujúcich NLM modulov:

- *AMON.NLM* – on-access skener, ktorý nepretržite kontroluje súbory, ku ktorým sa prístupuje zo siete alebo lokálne, prípadne súbory, ktoré sa na server ukladajú.
- *NOD32.NLM* – on-demand skener, ktorý môže byť správcom systému nasmerovaný k diagnostike určitej súborovej časti disku (obvykle adresáre, volume, resp. celého disku). V tomto prípade ide o jednorazovú akciu a po dokončení kontroly je modul *NOD32.NLM* z pamäte odstránený.
- *NOD32UP2.NLM* – modul zaisťujúci aktualizáciu vírusovej databázy pre moduly *AMON.NLM* a *NOD32.NLM*.

2. Inštalácia

Ideálne je vytvoriť napr. adresár *NOD32* na volume *SYS:* a nakopírovať do tohto adresára súbory z inštalačných balíkov ESET NOD32 Antivírus pre Novell Netware. Ďalej je vhodné zaistiť automatické zavedenie modulu *AMON.NLM* a *NOD32UP2.NLM* po každom štarte serveru. Ideálne je zavádzanie zaistiť pomocou systémového súboru *AUTOEXEC.NCF*, a to príkazmi:

```
LOAD SYS:/NOD32/AMON
```

```
LOAD SYS:/NOD32/NOD32UP2 [parametre]
```

Jednotlivé parametre sú uvedené v nasledujúcich kapitolách. Zároveň je v prípade modulu *AMON* vhodné zaistiť dostupnosť súboru *AMON.CFG*, z ktorého si *AMON* pri zavádzaní prevezme nastavenia.

Rýchly sprievodca kompletnou inštaláciou

Inštalčný balík rozbalíme napríklad do volume *SYS:/NOD32*. V tom istom adresári je vhodné vytvoriť súbor *AMON.CFG* a zapísať do neho nasledovné:

```
recipient=login_administratora_siete
notify
clean
delete
log
```

Potom je potrebné zapnúť v konzole Novell rezidentný štít *AMON* príkazom:

```
LOAD SYS:/NOD32/AMON.NLM
```

S vyššie uvedeným nastavením bude *AMON* zasielať informácie o infiltrácii užívateľovi *login_administratora_siete*, ale aj užívateľovi, ktorý s infikovaným súborom manipuloval (parameter *notify*). Zároveň sa *AMON* pokúsi infikovaný súbor vyličiť, a pokiaľ to nebude možné, tak tento súbor vymaže.

Ďalej je nutné zaistiť aktualizáciu ESET NOD32 Antivírus pre Novell Netware. Tento produkt neshťahuje vírusové aktualizácie priamo z aktualizáčnych serverov na Internete, ale používa pre aktualizáciu *mirror* adresár, ktorý je možné vytvoriť napr. pomocou produktu *NOD32* pre Windows Professional Edition. Tento *mirror* adresár sa musí fyzicky nachádzať na tom istom disku, ako inštalácia ESET NOD32 Antivírus pre Novell Netware (ak vychádzame z ďalšieho postupu, mal by byť *mirror* adresár vytvorený v *SYS:/PUBLIC/MIRROR*). Ak bude *mirror* adresár vytvárať *NOD32* pre Windows Professional Edition 2.7 alebo novší, potom je potrebné patrične nastaviť a zaviesť modul *NOD32UP2.NLM* príkazom z konzoly:

```
LOAD SYS:/NOD32/NOD32UP2.NLM SYS:/PUBLIC/MIRROR/ -update-period=60
```

Takto sa bude ESET NOD32 Antivírus pre Novell Netware aktualizovať z *mirror* adresára *SYS:/PUBLIC/MIRROR* každú hodinu (parameter *-period=60*).

Moduly *AMON.NLM* a *NOD32UP2.NLM* je vhodné zavádzať automaticky po každom štarte serveru prostredníctvom systémového súboru *AUTOEXEC.NCF*.

3. Moduly

AMON.NLM

Modul AMON.NLM je možné zaviesť z konzoly príkazom:

LOAD SYS:/NOD32/AMON

a ukončiť nasledujúcim:

UNLOAD AMON

AMON.CFG

Ak je k dispozícii súbor *AMON.CFG* v adresári spoločne s modulom *AMON.NLM*, bude z neho prevzaté nastavenie pri zavádzaní AMONu.

Syntax súboru AMON.CFG je nasledovná (prepínače je potrebné uvádzať v riadkoch samostatne, t.j. jeden riadok = jeden prepínač):

onread+ (štandardné nastavenie)

Súbory budú testované v momente, keď bude zistený príkaz na ich otvorenie / čítanie.

Opak: *onread-*

onwrite+ (štandardné nastavenie)

Súbory budú testované v momente, keď sú modifikované.

Opak: *onwrite-*

onrename+ (štandardné nastavenie)

Súbory budú testované v prípade pokusu o ich premenovanie.

Opak: *onrename-*

all (štandardné nastavenie)

Testované budú všetky súbory. V opačnom prípade, t.j. *all-* budú testované len súbory s príponami, ktoré sú definované spoločnosťou Eset.

notify

Ak bude odhalená infiltrácia modulom AMON, bude o tejto skutočnosti informovaná osoba, ktorá s infikovaným súborom manipulovala (prostredníctvom služby *NetWare Message PopUp Service*).

recipient=úžívateľ1, užívateľ2 ...

Ak bude odhalená infiltrácia modulom AMON, bude o tejto skutočnosti informovaná osoba s login name *užívateľ 1* a *užívateľ 2*. Väčšie množstvo užívateľov je potrebné oddeľovať čiarkou, ako znázorňuje príklad.

Ďalšie parametre:

pattern

log

logappend

logrewrite

clean

rename

delete

heur

heursafe

heurstd

heurdeep

sú spoločne s modulom *NOD32.NLM* a ich význam je uvedený nižšie (parametre je potrebné v súbore *AMON.CFG* zadávať bez symbolu „-“).

NOD32.NLM

Diagnostiku a prípadné odstraňovanie infiltrácie on-demand skenerom je možné zahájiť príkazom:

LOAD SYS:/NOD32/NOD32 [parametre] [cesta]

Ak nie je [cesta] uvedená, je automaticky zahájená kontrola celého disku.

Parametre:

-? -h -help

Zobrazí prehľad parametrov s popisom.

-subdir+ (štandardné nastavenie)

Povolí testovanie podadresárov.

Opak: *-subdir-*

-pack+

Povolí testovanie interne komprimovaných súborov.

Opak: *-pack-* (štandardné nastavenie)

-arch+

Povolí testovanie archívov (ZIP, RAR, ARJ...).

Opak: *-arch-* (štandardné nastavenie)

-pattern+ (štandardné nastavenie - neodporúčame meniť)

Využitie vírusových signatúr pri detekcii.

Opak: *-pattern-*

-heur+ (štandardné nastavenie – neodporúčame meniť)

Využitie heuristickej analýzy pri detekcii.

Opak: *-heur-*

Heuristickú analýzu je možné nastaviť v troch úrovniach citlivosti:

-heursafe

-heurstd (štandardné nastavenie - neodporúčame meniť)

-heurdeep

Správanie pri objavení infiltrácie je možné ovplyvniť nasledovnými parametrami. Parametre je možné vhodne kombinovať. Napríklad spojenie parametrov *-clean -delete* zabezpečí, že v prípade nemožnosti vyliečenia infikovaného súboru bude súbor zmazaný. V prípade modulu AMON.NLM a neuvedenie žiadneho z nasledujúcich troch parametrov bude prístup k infikovaným súborom len zablokovaný.

-clean

Infikovaný súbor bude liečený.

-rename

Infikovaný súbor bude premenovaný.

-delete

Infikovaný súbor bude zmazaný.

-prompt (tento parameter nie je možné uplatniť v prípade modulu AMON.NLM)

Konzola sa opýta, čo sa má s infikovaným súborom vykonať.

-log+ (štandardné nastavenie)

O činnosti modulu bude vedený protokol (súbor NOD32.LOG, alebo AMON.LOG).

Opak: *-log-*

Spôsob vedenia protokolu:

-logappend (štandardné nastavenie)

Nové informácie budú pridávané na koniec existujúceho protokolu.

-logrewrite

Protokol bude vyprázdnený pri každom zavedení modulu.

-log=<subor>

Tento parameter umožňuje definovať vlastný súbor, do ktorého bude protokol zapisovaný.

Ďalšie parametre:

-list+

Vypisovať všetky súbory prechádzajúce testom.

Opak: *-list-* (štandardné nastavenie)

Príklad použitia:

LOAD SYS:/NOD32/NOD32 -pack+ -arch+ -clean -delete

(Kontrola celého disku vrátane interne komprimovaných súborov a archívov. V prípade odhalenia infiltrácie bude infikovaný súbor vyliečený, alebo zmazaný).

NOD32UP2.NLM

Aktualizačný modul nestahuje vírusové aktualizácie priamo z aktualizáčnych serverov na Internete, ale používa pre aktualizáciu mirror adresár, ktorý je možné vytvoriť napríklad pomocou produktu ESET NOD32 Antivirus 2.7 Mirror Server. Tento mirror adresár sa musí fyzicky nachádzať na tom istom serveri ako ESET NOD32 Antivirus pre Novell Netware.

Syntax je nasledovný:

LOAD SYS:/NOD32/NOD32UP2 mirror_adresár [adresár_s_NLM_modulmi] [parametre]

Minimum je uvedenie časti *mirror_adresár*, teda cesty do mirror adresára, odkiaľ bude tento modul preberať aktualizácie pre moduly NOD32.NLM a AMON.NLM.

[adresár_s_NLM_modulmi] je nepovinnou súčasťou príkazu v prípade, že NOD32UP2.NLM sa nachádza v adresári spolu s NOD32.NLM a AMON.NLM.

Možné parametre:

-update

Zaisť vykonanie aktualizácie (v opačnom prípade budú len vypísané dostupné aktualizácie).

-period=n

Zaisť, že aktualizácia z mirror adresára bude prevedená vždy po n minútach. Odporúčame aktualizáciu prevádzať každú hodinu (*-period=60*).

-show_retvals

Vypíše všetky návratové hodnoty s krátkymi komentármi.

-help

Vypíše zoznam všetkých parametrov s krátkymi komentármi.

Špeciálne parametre:

-no_signature

Tento parameter je možné použiť počas aktualizácie,

ak dochádza k chybe 107. Táto chyba znamená, že aktualizáčn é súbory sú chybn e podpísané elektronickým podpisom.

Príklad použítia:

*LOAD SYS:/NOD32/NOD32UP2.NLM SYS:/PUBLIC/MIRROR/
-update -period=60*

(Moduly AMON.NLM a NOD32.NLM budú aktualizované každú hodinu z mirror adresára *SYS:/PUBLIC/MIRROR/*).