Robert Norrlin

IT-Infrastruktuurin valvonta Nagioksen avulla

Metropolia Ammattikorkeakoulu

Insinööri (AMK)

Tietotekniikan koulutusohjelma

Insinöörityö

08.09.2015

Metropolia

Tekijä(t) Otsikko Sivumäärä Aika	Robert Norrlin IT-Infrastruktuurin valvonta Nagioksen avulla 47 sivua + 0 liitettä 01.10.2015
Tutkinto	Insinööri (AMK)
Koulutusohjelma	Tietotekniikan koulutusohjelmat
Suuntautumisvaihtoehto	Tietoverkkojen suuntaumisvaihtoehto
Ohjaaja(t)	Janne Salonen, Osaamisaluepäällikkö

Työn tavoitteena oli testata ja dokumentoida ohjeet Nagios XI:n toimivuuteen yrityksen IT-infrastruktuurin valvontaa varten. Tätä varten täytyi selvittää mahdollisten eri sovellusten, käyttöjärjestelmien ja laitetyyppien valvontojen toimivuus ja luotettavuus.

Työtapana oli valvontapalvelimen sekä testiympäristön rakentaminen, eri valvontatapojen testaaminen, mahdollisten ongelmien löytäminen valmiiksi ja näiden dokumentointi mahdollista tuotantoonottoa varten, jolloin ongelmat saadaan helposti korjattua tai kierrettyä.

Työn vaiheina oli aluksi Nagiokseen tutustuminen sekä sen eri menetelmistä lukeminen, minkä avulla varmistettiin soveltuvuus valvontaan. Dokumentteihin tutustumisen jälkeen asennettiin valvontasovellus virtuaalipalvelimelle testilisenssillä, sekä asennettiin palvelimia eri sovelluksilla ja käyttöjärjestelmiä ulko- ja sisäverkossa oleviin virtuaalipalvelimiin. Kun kaikki palvelimet olivat toiminnassa, asennettiin valvonnat yksi kerrallaan ja testattiin niiden toimivuus ja mahdolliset ongelmat. Verkkolaitteiden valvonnan testaaminen tehtiin GNS3-sovelluksen avulla, joka mahdollisti verkkolaitteiden virtualisoinnin ja virtuaalisten kytkinten sekä reitittimien kytkemisen sisäverkkoon ja valvontapalvelimeen.

Lopullisessa dokumentissa on toimiva pohja valvonnan käyttöönottoon ja ohje miten yleisimpiä sovelluksia ja verkkolaitteita voidaan valvoa. Dokumentin tekniikat soveltuvat pienten sekä keskisuurien yritysten valvonnan toteuttamiseen. Käyttöönotto kuitenkin vaihtelee aina yrityksen topologiasta ja tekniikoista riippuen.

Avainsanat	Nagios, verkonvalvonta, sovellusvalvonta

Author(s) Title Number of Pages Date	Robert Norrlin IT Infrastructure Monitoring with Nagios 47 pages + 0 appendices 1 October 2015
Degree	Bachelor of Engineering
Degree Programme	Information Technology
Specialisation option	Data Networks
Instructor(s)	Janne Salonen, Principal Lecturer

The purpose of this thesis and project was to test and document the monitoring capabilities of Nagios XI in a corporate environment. The objective was to find out if Nagios could monitor efficiently and reliably different software, hardware and operating systems.

The method for this was to build and configure the monitoring server, test servers, network equipment and different software. Once the devices were up and running, different monitoring setups were used and problems and installing phases were documented in order to ease the possible deployment in a live environment.

The phases for creating this document included first researching if Nagios itself was a possible choice to use as the monitoring software. After it was decided Nagios was sufficient, a monitoring application was installed on a virtual server with a test license. Other test servers were installed onto local and outside networks on virtual servers. The testing of the monitoring of the network equipment was done using GNS3-software, which allowed switches and routers to be virtualized for easy testing. Once all were installed and running, monitoring was added one by one on different software and hardware.

This document provides a framework and guidelines for implementing monitoring in small and medium-sized businesses. Many of the most commonly used operating systems, software and network devices can be added for monitoring by following the steps outlined in this document. Implementing the monitoring will still always vary in each company, depending on the topology and software used.

Keywords	Network monitoring, Nagios

Sisällys

Lyhenteet

SNMP = Simple Network Management Protocol. TCP/IP-verkkojen hallintaan käytettävä protokolla.

SMTP = Simple Mail Transfer Protocol. Sähköpostipalvelimien käyttämä protokolla viestien välittämiseen.

SLA = Service Level Agreement. Palvelutasosopimus

SSH = Secure Shell. Tietoliikenteen salaamiseen tarkoitettu protokolla.

NRPE = Nagios Remote Plugin Executor. Lisäosa Nagiokseen jonka avulla voidaan ajaa muita lisäosia Linux/Unix-koneilla.

DNS = Domain Name System. Nimipalvelinjärjestelmä, jonka avulla voidaan vaihtaa sivustojen ja koneiden nimet IP-osoitteiksi.

Daemon = Tietokonejärjestelmän taustaprosessi. Tulee sanoista”Disk And Execution MONitor”.

STDIN = Standard Input, usein tarkoitetaan näppäimistön painalluksia.

RRD = Round Robin Database. RRD:ssä vanhaa dataa poistetaan uuden tieltä.

CCM = Core Config Manager. Nagioksen tarkkojen sääntöjen hallintaan tarkoitettu työkalu.

YUM = Yellow Dog Updater, Modified. Red Hatin ja CentOS:n käyttämä paketinhallintaohjelma.

1 Johdanto

Nagios XI on Nagios Enterprises -yrityksen avoimeen lähdekoodiin perustuva IT-infrastruktuurin valvontaan tarkoitettu ohjelmisto. Se on suunniteltu skaalautumaan jopa tuhansien palveluiden ja laitteiden yhtäaikaiseen valvontaan. Nagios XI on maksullinen ohjelmisto, mutta siitä on myös olemassa ilmainen Core-versio. Core on pelkistetty versio XI:stä.

Tavoitteena oli tutkia Nagios XI:n mahdollisuuksia IT Infrastruktuurin valvontaan ja samalla dokumentoida miten itse valvontapalvelimen ja valvontojen asennus tapahtuu, sekä löytää yleisimmät puutteet ja virhetilanteet, jolloin käyttöönotto tuotantoon saataisiin mahdollisimman vähävikaiseksi.

2 Nagios XI

2.1 Laitevaatimukset

Nagios XI:tä on käytännössä mahdollista ajaa virtuaalikoneella tuhanteen laitteeseen tai 5000 palveluun asti yhdellä virtuaalikoneella. Tämän jälkeen on suositeltavaa siirtää palvelin fyysiseen laitteeseen tai jakaa monitorointia usealle palvelimelle.

Suositeltavaa on lisäksi ajaa levypakkaa RAID5-tilassa parempaa vikasietoisuutta varten. Prosessorien olisi hyvä olla 2+ Ghz per ydin.

Taulukko 1. Nagios XI:n laitevaatimukset

Laitemäärä	Palvelumäärä	Levytila	Prosessoriytimet	RAM
50	250	40 GB	1-2	1-4GB
100	500	40 GB	2-4	4-8GB
> 500	> 2500	120 GB	> 4	> 8GB

Valmiita levykuvia on Microsoftin Hyper-V:lle, Vmware ESX/vSpherelle sekä Vmware Serverille tai Vmware Playerille. Jos on tarvetta kääntää palvelu itse lähdekoodista, suositeltava käyttöjärjestelmä olisi 64-bittinen Redhat 7.x tai CentOS 7.x.

Valmiita levykuvia on Microsoftin Hyper-V:lle, Vmware ESX/vSphere:lle sekä Vmware Serverille tai Vmware Playerille. Jos on tarvetta kääntää palvelu itse lähdekoodista, suositeltava käyttöjärjestelmä olisi 64-bittinen Redhat 7.x tai CentOS 7.x.

Valvontapalvelimen suorituskykyä on mahdollista parantaa käyttämällä muutamia tekniikoita, kuten siirtämällä tietokanta erilliselle palvelimelle tai käyttämällä esimerkiksi Ramdisk-teknologiaa.

Nagios XI:ssä on vakiona asennettuna seuraavat komponentit, joista tärkeimmistä tarkemmin myöhemmin dokumentissa:

- Nagios XI UI
- Nagios Core
- NSCA
- NRPE
- Nagios Plugins
- PNP
- NDOUtils
- NagiosQL (muokattu versio)
- phpMyAdmin
- NCPA.

2.2 Nagioksen asennus ja alkukonfiguraatio

Valmiiden levykuvien avulla Nagios XI:n käyttöönotto on yksinkertaista: siihen voi lisätä uuden virtuaalikoneen ja sen kovalevyksi valita Nagioksen sivuilta ladattavan tiedoston.

Käyttöjärjestelmänä on Red Hat 6.6 kaikissa tämänhetkisissä levykuvissa. Kaikissa versioissa on oletussalasanat, ja ne olisi erittäin suositeltavaa vaihtaa toisiin heti, kun koneen ensimmäisen kerran käynnistää. Salasanat ovat:

Root-käyttäjän salasana: ”**nagiosxi”**

MySQL/MariaDB:n käyttäjätunnus on ”**root”** ja salasana ”**nagiosxi”**.

Nagios XI:n Admin-käyttäjätunnus on ”**nagiosadmin”**, salasana on satunaisgeneroitu asennuksen aikana.

Unohtuneen nagiosadmin-tunnuksen salasanan pystyy vaihtamaan kirjautumalla root-käyttäjänä koneelle ja antamalla komennon:

/usr/local/nagiosxi/scripts/reset_nagiosadmin_password.php --password=<salasana>

Config Manager -käyttäjätunnus on ”**nagiosadmin”** ja salasana ”**welcome**”. Tämä vaihdetaan suoraan asennuksen aikana.

Root-käyttäjän salasanan vaihto menee normaalilla CentOS:n ja RedHatin tavalla, eli kirjautumalla root-tunnukselle suoraan tai vaihtamalla siihen *sudo su* -komennolla ja antamalla komennon *passwd*.

Käyttöliittymän näppäimistöasettelu on vakiona English US -pohjalla, jolloin kirjoittaminen voi olla vierasta. Suomenkielisen asettelun saa vaihdettua asentamalla *system-config-keyboard* yumin avulla ja ajamalla sen. Eteen tulee valikko, josta saa haluamansa asettelun, suomenkieliselle ”Finnish”-valinta.

Palvelimelle olisi suotavaa asettaa staattinen IP, jotta esimerkiksi DNS:n vikatilanteissa itse valvontakone on käytettävissä. Red Hatissa ja CentOS:ssa staattisen IP:n saa asetettua tekemällä ifcfg-<verkkoliitännän nimi> -tiedoston /etc/sysconfig/network-scripts/ -polkuun. Esimerkkitapauksessa tiedosto olisi */etc/sysconfig/network-scripts/ifcfg-eth0*.

Tiedostoon pitää lisätä tai muokata rivit PREFIX, IPADDR, ONBOOT. Tiedostossa saattaa olla valmiina jo muutakin. Alla ovat testiympäristön käyttämät arvot:

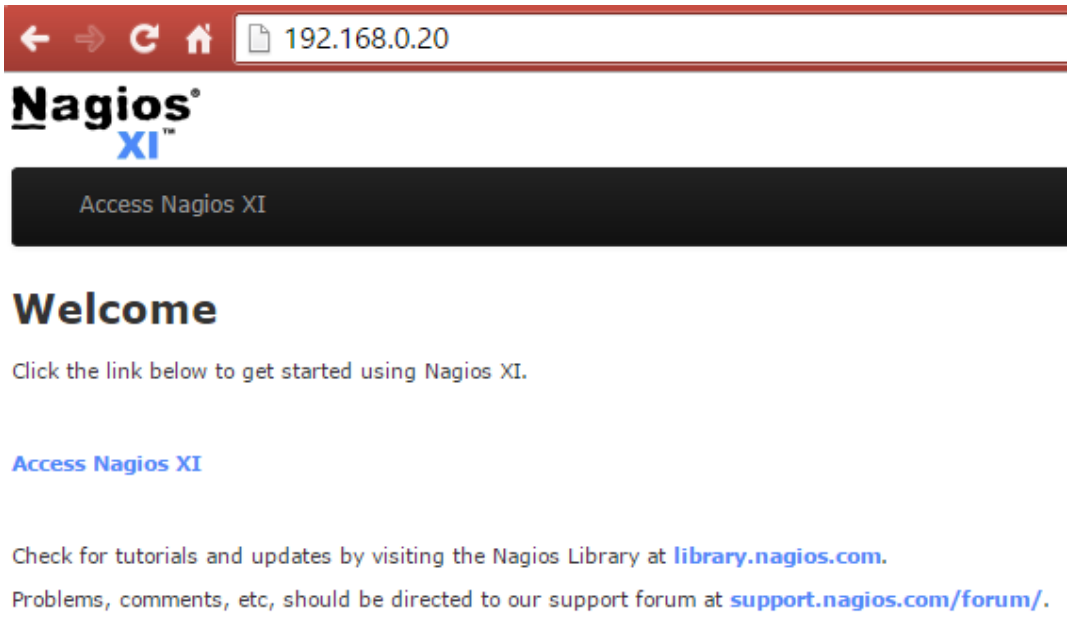
DEVICE="eth0"
NM_CONTROLLED="yes"
ONBOOT=yes
TYPE=Ethernet
BOOTPROTO=none
PREFIX=24
IPADDR=192.168.0.20
DEFROUTE=yes
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=yes
IPV6INIT=no
NAME="System eth0"
UUID=5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03

Kun tiedosto on tehty ja tallennettu, pitää verkkokomponetti käynnistää uudestaan */etc/init.d/network restart* -komennolla.

NagiosQL on tarkoitettu helpottamaan Nagioksen hallintaa ja konfiguraatioden tekemistä lisäämällä ne selainkäyttöliittymään. Se on erillisen tiimin ylläpitämä ja on ilmainen New BSD -lisenssiin pohjautuen.

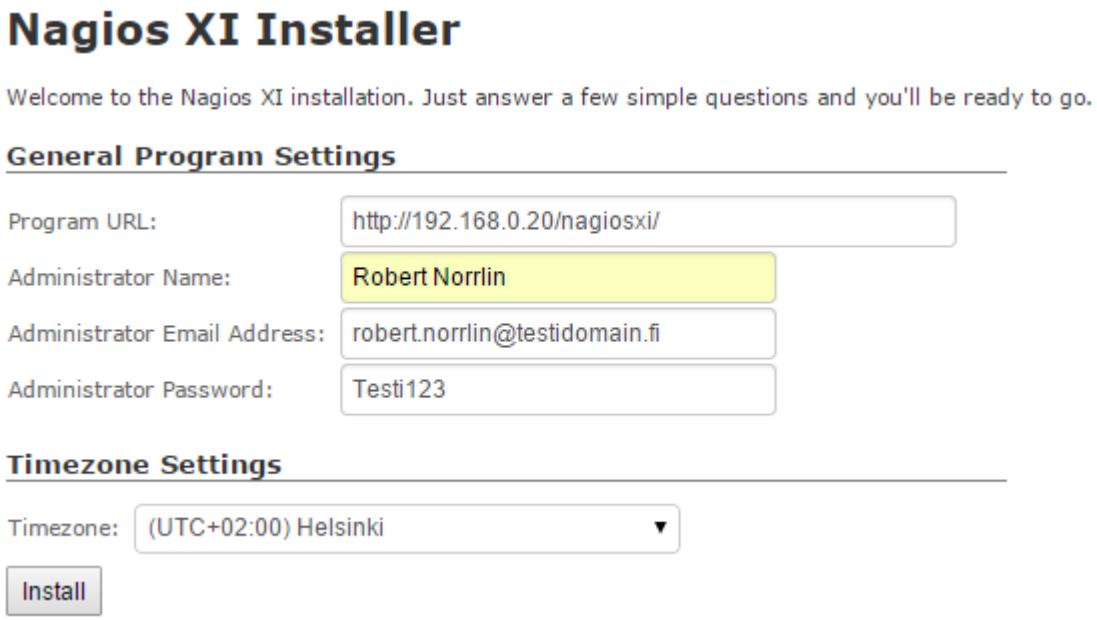
Palvelimen nimi olisi suotavaa myös vaihtaa. Tämän voi tehdä vaihtamalla HOSTNAME-kenttään haluamansa nimen */etc/sysconfig/network* -tiedostoon tai kirjoittamalla komennon *hostname <nimi>*. Kun nimi on vaihdettu, pitää verkkopalvelu käynnistää uudelleen */etc/init.d/network restart* -komennolla.

Kun Nagios on onnistuneesti asennettu ja tarvittavat muutokset tehty, pääsee palveluun kirjautumaan selaimella kirjoittamalla osoitteeksi palvelimen nimen (vaatii DNS:n ympäristössä) tai IP-osoitteen. Eteen aukeaa tervetuloa-sivu, josta pääsee jatkamaan klikkaamalla ”Access Nagios XI”.



Kuva 1. Nagios XI:n tervetuloa-ikkuna

Seuraavaksi aukeaa Nagioksen asennussivu, jossa määritellään muutamat perusasetukset palveluun liittyen. Program URL on osoite, josta palveluun pääsee kirjautumaan. Käytön helpottamiseksi voidaan osoitteeksi laittaa koneen nimi, joka asennusvaiheessa määriteltiin, esimerkiksi http://Nagios/nagiosxi/. Muihin tietoihin laitetaan järjestelmävastaanvan tiedot sekä salasana. Timezone-kenttään valitaan paikallinen aikavyöhyke. Kun asetukset ovat oikein, painetaan Install. Tämän jälkeen tulee vielä lisenssiehtojen hyväksyntä, josta pääsee laittamalla raksin hyväksyntään ehtojen lukemisen jälkeen ja painamalla Submit.

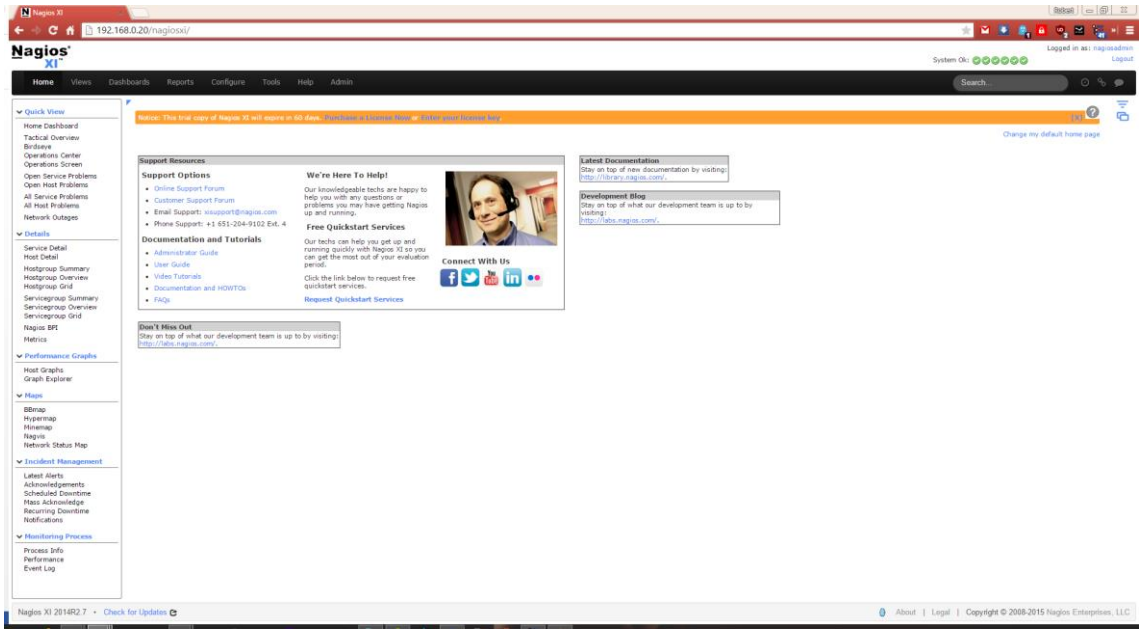


Kuva 2. Nagioksen perusasetukset

Install-painikkeen painamisen jälkeen selain saattaa antaa herjan yhteyden katkeamisesta, mutta tämä korjaantuu odottamalla noin 10 sekuntia ja lataamalla sivu uudelleen. Sama pätee, jos kirjautumissivun ylälaitaan tulee herjoja tietokannasta.

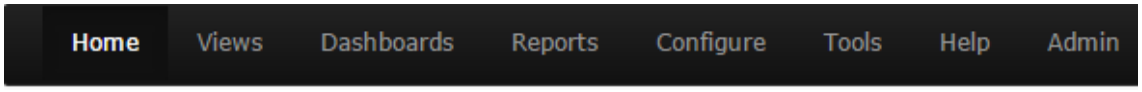
Kuva 3. Kirjatumisruutu

Kirjautuminen tapahtuu ensimmäisellä kerralla **nagiosadmin**-tunnuksella sekä edellisessä vaiheessa asetetulla salasanalla. Kirjautumisen jälkeen aukeaa Nagioksen hallintasivuston aloitussivu.



Kuva 4. Nagioksen aloitusnäkymä

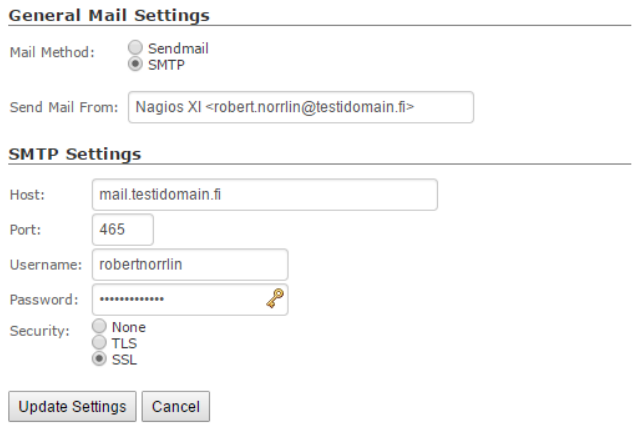
Kun aloitussivun ensimmäisen kerran saa auki, on suositeltavaa mennä ylälaidan suunnistuspalkin kautta Admin-sivustolle. Eteen ilmestyy ”Administrative Tasks” -laatikko, jossa on muutamia tärkeitä alkukonfiguraatioita, jotka olisi suotavaa tehdä aluksi. Näihin kuuluu tunnusten salasanojen vaihtoa sekä sähköpostiasetusten konfigurointia.



Kuva 5. Suunnistuspalkki

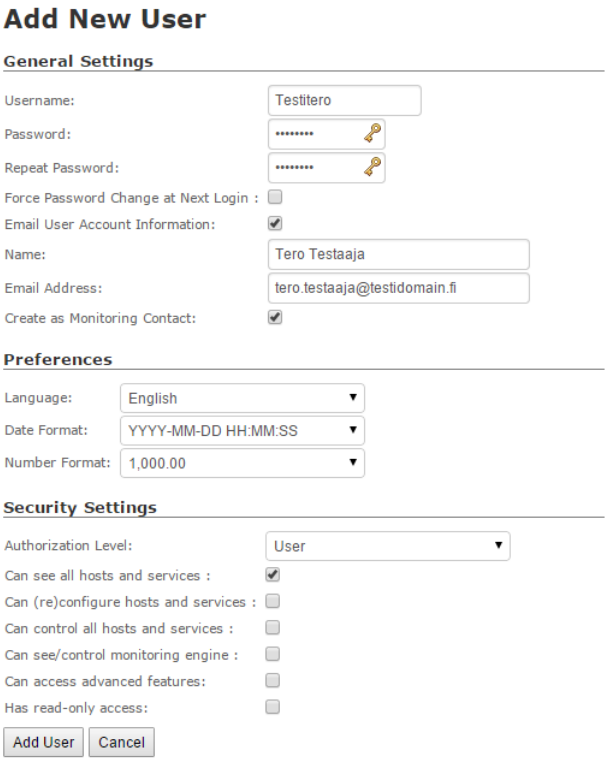
Dokumentissa usein viitataan polkuihin muodossa **Yläpalkin linkki**→vasemman palkin linkki. Eli esimerkiksi **Admin**→Manage Users olisi yläpalkin suunnistuspalkista Admin-linkki, jonka jälkeen vasemman laidan linkkivalikosta Manage Users -linkin kautta päästään halutulle sivulle.

Kun salasanat on vaihdettu kaikille pyydetyille tunnuksille ja sähköpostiasetukset laitettu yrityksen palvelinten mukaisesti, on jäljellä vielä käyttäjätunnusten luontia ja itse monitoroinnin asennus.



Kuva 6. Sähköpostiasetukset testiympäristössä.

Käyttäjätunnusten luonti ja muokkaus onnistuu suunnispalkin Admin-linkistä painamalla ja sen jälkeen suunnistamalla vasemmasta palkista ”Manage Users” -sivulle. Klikkaamalla Add New User aukeaa käyttäjätunnuksen luontiin tarkoitettu sivu, missä saadaan määritettyä tarkemmin oikeudet käyttäjälle. Kun tiedot ja halutut oikeudet on valittu, voidaan käyttäjätunnus luoda painamalla Add User -painiketta. Manage Users -sivulle ilmestyy äsken luotu käyttäjä nagiosadmin-tunnuksen lisäksi.



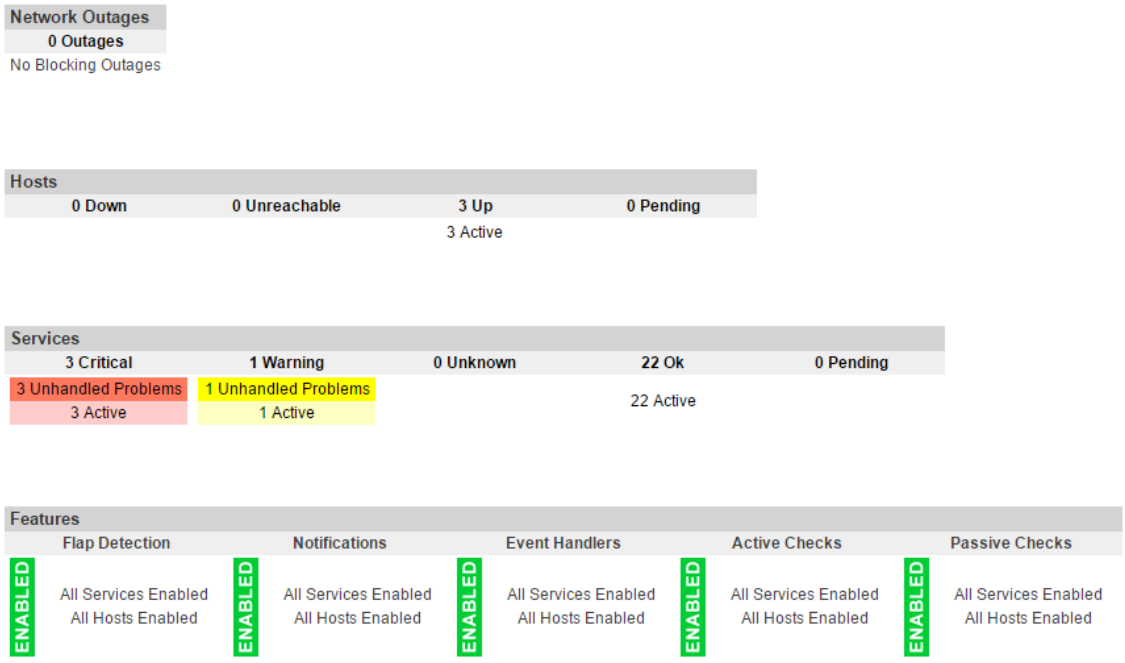
Kuva 7. Käyttätunnuksen luominen

3 Nagioksen käyttäminen

Nagioksen aloitussivulla on vakiona hieman huonosti esillä infoa, se olisi hyvä vaihtaa toiseen. Tämän pystyy tekemään aloitussivuston oikesta laidasta ”Change my default home page”-linkistä. Esimerkkinä paremmasta näkymästä olisi laittaa vakiosivuksi esimerkiksi ”Tactical Overview”, minkä saa vaihtamalla Home Page Destinationiksi Custom url ja osoitteeksi:

http://<palvelimen-osoite>/nagiosxi/includes/components/xicore/tac.php.

Tämän jälkeen kotinäkymänä on taktinen yleisnäkymä, jossa on listattu käynnissä olevat kriittiset ongelmat sekä varoitukset palveluista ja laitteista.



Kuva 8. Taktinen yleisnäkymä

Laitteita pääsee lisäämään valvontaan Configure-linkistä ylälaidan suunnistuspalkista. Monet yleisimmistä valvonnoista voidaan lisätä suoraan ”Run the Monitoring Wizard”-linkin takaa löytyvillä ohjatuilla asennuksilla. Vaativammissa valvonnoissa voidaan joutua käyttämään Core Configuration Manageria, jonka avulla voidaan Nagiokseen lisätä uusia ohjattuja asennuksia ja komentosarjoja, joita voidaan ajaa valvottavilla laitteilla.

3.1 Uuden ohjatun asennuksen lisääminen Nagiokseen

Jos on tarvetta lisätä uusi ohjattu asennus Nagiokseen, se voidaan hoitaa ensin lataamalla haluttu ohjattu asennus Nagioksen exchange.nagios.org-sivustolta, johon on kerätty tuhansia lisäosia ja muita toimintoja. Suurin osa on kuitenkin yksittäisen henkilön tekemiä, jolloin kyseisille lisäosille ei löydy virallista tukea tai takuuta toiminnasta.

Esimerkkinä asennetaan Dell OpenManage Nagios XI Wizard:

https://exchange.nagios.org/directory/Addons/Configuration/Configuration-Wizards/Dell-OpenManage-Nagios-XI-Wizard/details

Ladataan tiedosto koneelle, josta asennusta suoritetaan, jonka jälkeen sirrytään hallintasivustolla Admin-sivustolle ylälaidan suunnistuspalkin kautta, jonka jälkeen vasemman laidan palkissa on ”Manage Config Wizards” -linkki.

Tämän jälkeen painetaan Choose File -painiketta ja valitaan tiedostoksi äsken ladattu tiedosto. Tämän jälkeen painetaan Upload Wizard –painiketta, asennus on valmis. Ohjattu asennus löytyy nyt ”Run the Monitoring Wizard” -sivustolta.

3.2 Uuden lisäosan asennus Nagiokseen

Uuden lisäosan asennus on pitkälti samalla tavalla kuin ohjatun asennuksen lisääminen. Asennetaan esimerkkinä *check_snmp_BlueCoatSG_usage* -lisäosa.

https://exchange.nagios.org/directory/Plugins/Network-Connections%2C-Stats-and-Bandwidth/check_snmp_BlueCoatSG_usage/details

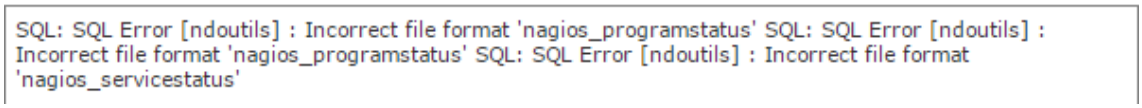
Ladataan tiedosto koneelle, josta asennusta suoritetaan. Sen jälkeen sirrytään hallintasivustolla Admin-sivustolle ylälaidan suunnistuspalkin kautta, jonka jälkeen vasemman laidan palkissa on ”Manage Plugins” -linkki.

Tämän jälkeen painetaan Choose File -painiketta ja valitaan tiedostoksi äsken ladattu tiedosto. Tämän jälkeen painetaan Upload Plugin -painiketta ja asennus on valmis. Lisäosa on nyt käytettävissä agenttien tai muiden ohjelmointisarjoja käyttävien osien avulla.

3.3 Valvontapalvelimen virhetilanteet ja niiden korjaus

Joskus kirjautuessa sisään hallintasivustolle voi ilmetä virheilmoituksia, tai jos palvelu muuten toimii epämääräisesti, voidaan joutua korjaamaan esimerkiksi tietokantaa. Tietoja virheistä saa muun muassa seuraavilla komennoilla:

```
Tail -25 /usr/local/nagios/var/nagios.log
Tail -25 /var/log/mysqld.log
Tail -25 /var/log/httpd/error_log
```



Kuva 9. Virheilmoitus palveluun kirjauduttaessa

Kuva 9:ssä on tietokannassa ilmennyt virheitä. Ongelmasta saa tietoa mysqld.log-tiedostosta aikaisemmin kerrotulla komennolla. Ongelmaa voi koittaa korjata komennoilla:

Service mysqld stop
service nagios stop
/usr/local/nagiosxi/scripts/repairmysqld.sh nagios
/usr/local/nagiosxi/scripts/repair_databases.sh
service mysqld start

3.4 Nagioksen korkea saatavuus ja valvonta

Usein on tarpeen valvoa itse valvontakonetta sen vikatilanteiden varalta tai käyttää korkean saatavuuden tekniikoita varmistamaan, että palvelu on aina käytössä. Korkean saatavuuden suhteen on suositeltavaa käyttää VMwaren tai Windows Hyper-V:n omia tekniikoita, jonka avulla saadaan palvelu pidettyä käynnissä vikatilanteiden varalta.

Nagioksen valvonta voidaan hoitaa erillisellä Nagios-palvelimella, joka on lisenssien puolesta ilmaista. Tämä hoituu asentamalla normaalisti uuden Nagios-palvelimen ja ”Monitor Nagios XI Server” -ohjatulla asennuksella (Ohjatusta asennuksesta ohjeet kohdassa 3.1).

4 Nagioksen vakiokomponentit

4.1 NRPE

NRPE eli Nagios Remote Plugin Executor on lisäosa Nagioksen asennukseen, joka löytyy vakiona mukana Nagios XI:ssä. NRPE:n avulla on mahdollista ajaa komentosarjoja ja muita Nagioksen lisäosia valvottavissa Linux/Unix-kohteissa. Yleisin syy NRPE:n käyttöön on sen mahdollistama lokaalien resurssien valvonta (RAM,

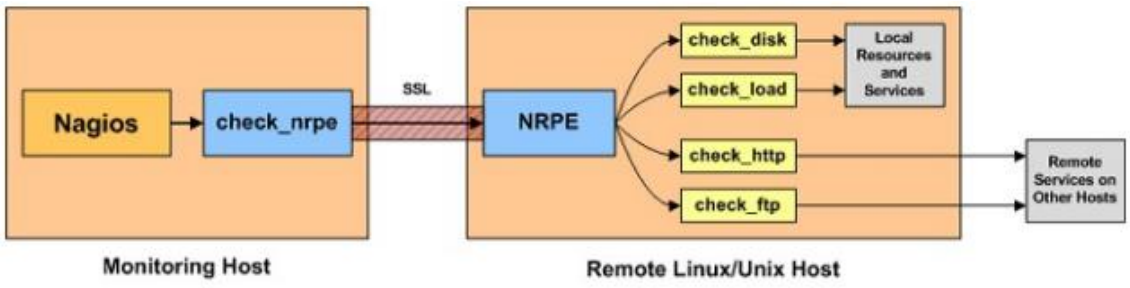
Prosessorikäyttö jne.). Vaikka NRPE on tarkoitettu pääsääntöisesti Linux-koneiden valvontaan, useat Windows-koneiden agentit tukevat NRPE:n käyttämää protokollaa, jolloin sama periaate pätee myös niihin.

NRPE:n käyttöön vaaditaan NRPE-agentin asennus kohdekoneille sekä *check_nrpe* -lisäosan asennus valvontapalvelimelle. Nagios XI:ssä palvelinkomponentti on vakiona asennettuna.

Nagios tekee pyynnön *check_nrpe*-lisäosan kautta, joka lähettää SSL-tunnelin kautta pyynnön kohdekoneelle, jossa NRPE-agentti ajaa nagioksen haluaman komennon ja/tai lisäosan kohdekoneella ja lähettää tiedot samaa reittiä takaisin valvontakoneelle. SSL-tunneli valvontakoneen ja kohteen välillä ei ole pakollinen, mutta erittäin suositeltava käyttää. Jos valvontaa joudutaan tekemään julkisen verkon yli, salaamaton yhteys on iso tietoturvariski.

Kohdekoneessa on oltava asennettu lisäosat mitä NRPE suorittaa, muuten ei ole mahdollista seurata sen avulla mitään.

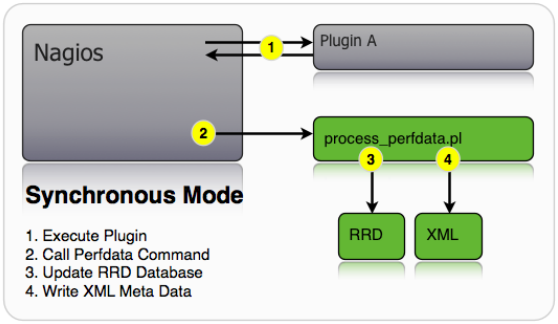
NRPE:n sijasta valvottavien koneiden lisäosia voidaan ajaa myös SSH:n kautta erillisellä *check_by_ssh*-lisäosalla (lisätietoa SSH-valvonnasta kohdassa 3.3), mutta se nostaa huomattavasti prosessorinkäyttöä per valvottava kone ja saattaa viedä liikaa tehoja, kun valvonnassa on satoja tai tuhansia valvottavia kohteita.



Kuva 10. NRPE:n toimintaan havainnollistava kaavio.[1]

4.2 PNP

PNP on työkalu graafien piirtämiseen ja suorituskyvyn analysointiin. Se käyttää lisäosien dataa ja tallentaa tiedot RRD-tietokantoihin RRDtool:n avulla. Siinä on mahdollisuus käyttää joko synkronisoitua tilaa tai bulkkimoodia. Synkronisoidussa tilassa *process_perfdata.pl*-komentosarja ajaa itseään viiden minuutin välein ja hakee valvottavilta koneilta dataa ja prosessoi sen. Kyseinen moodi on toimiva noin tuhanteen kohteeseen asti, jonka jälkeen se alkaa kuormittamaan liikaa ja olisi suositeltavaa vaihtaa käyttämään bulkkimoodia.

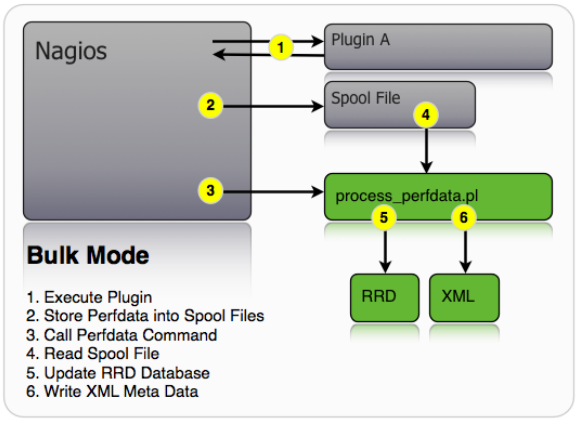


Kuva 11. PNP:n synkronisoidun tilan toimintaperiaate

Bulkkimoodissa viiden minuutin aikavälin sijaan dataa kerätään väliaikaiseen tiedostoon, joka määritellyn ajanjakson päästä prosessoidaan. Tämä vähentää *process_perfdata.pl* -komentosarjan kutsukertoja, mutta taasen nostaa komentosarjan ajamiseen kuluvaa aikaa. Kyseistä aikaa kannattaa pitää silmällä, koska sen ajon aikana Nagios ei aja mitään muita tarkistuksia. Normaalitilanteessa bulkkimoodin ajaminen ei kuitenkaan kestä kuin sekunnin murto-osia. Aikaa voi seurata */var/perfdata.log*-tiedostosta. Alla on PNP:n kehittäjän dokumentoinnin esimerkki:

```
2007-10-18 12:05:01 [21138] 71 Lines processed
2007-10-18 12:05:01 [21138] .../spool/service-perfdata-1192701894-PID-21138 deleted
2007-10-18 12:05:01 [21138] PNP exiting (runtime 0.060969s) ...
```

71 riviä tekstiä ajettiin noin 0.06 sekunnin aikana. Tämä vastaa noin 2000 palvelun tarkistusta. Tämän 0.06 sekunnin aikana ei Nagios suorittanut muita tarkistuksia.



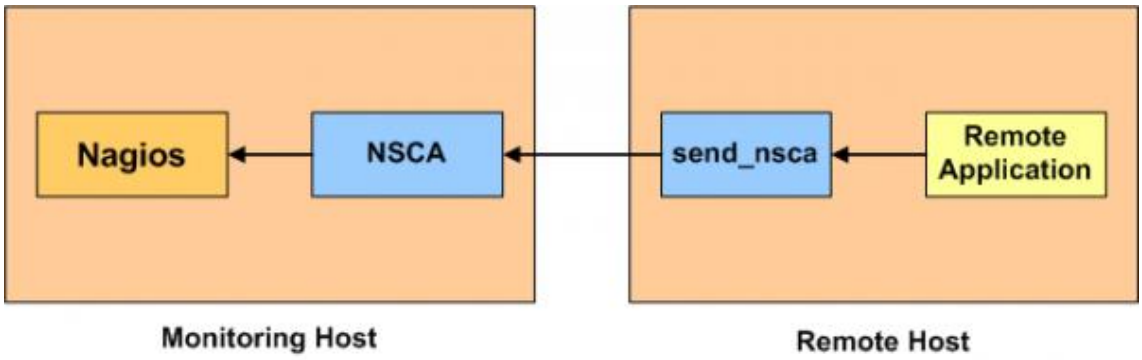
Kuva 12. PNP:n bulkkimoodin toimintaperiaate

4.3 NSCA

NSCA eli Nagios Service Check Acceptor on Unix/Linux -valvontaan tarkoitettu daemoni, joka mahdollistaa passiivisten tarkistusten käyttämisen etäpalvelimissa ja niiden palveluissa. NSCA on hyödyllinen ominaisuus esimerkiksi tietoturvahälytysten prosessointiin ja redunanttisten valvontaympäristöjen valvomiseen. NSCA on vakiona asennettunna Nagios XI:hin, mutta sitä ei ole otettu käyttöön. Jotta etäpalvelimet ja palvelut voivat lähettään dataa valvontakoneelle, täytyy */etc/xinetd.d/nsca*-tiedostosta muokata seuraavaa riviä:

only_from = 127.0.0.1 192.168.0.111 192.168.15.25

Kyseiselle riville listataan kaikki IP-osoitteet, joille sallitaan IP-liikenne valvontakoneelle. IP-osoitteet erotellaan välilyönnillä. Jos jostain syystä halutaan sallia kaikki liikenne, voidaan *only_from*-rivi poistaa tai kommentoida pois.



Kuva 13. NSCA:n toimintaperiaate

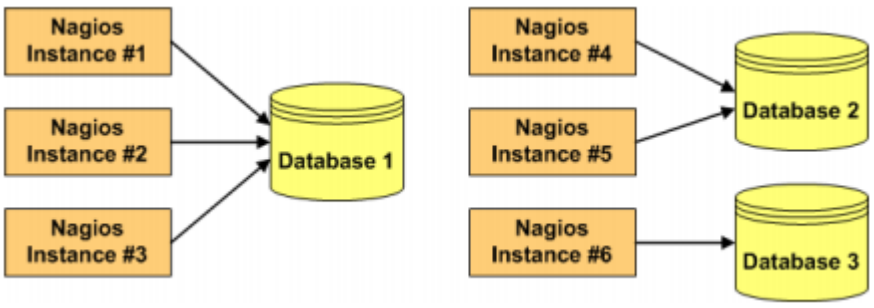
Valvontapalvelimelle tarvitsee myös konfiguroida salasana sekä salausmenetelmä. Tämän pääsee tekemään menemällä Nagioksen etusivun yläpalkista **Admin**-sivustolle ja sen jälkeen valitsemalla **Inbound Transfers** -sivuston vasemmasta palkista.

Valittavana on joko NRDP- tai NSCA-välilehdet. NSCA-välilehdellä saa aluksi varoituksen aikaisemman kohdan suorittamisesta. Kun varoituksen on rastittanut pois, voidaan valita alasvetovalikosta haluttu salausmenetelmä ja sen jälkeen kirjoittaa salasana, jota käytetään lähettämiseen. Suositeltavaa olisi generoida vahva salasana pelkästään NSCA:n käyttöön.

Palvelimet joista passiivisia hälytyksiä tai ilmoituksia halutaan lähettää tarvitsee agentin, joka tukee NSCA:ta. Agentteja on useita erilaisia ja ne löytää osoitteesta https://exchange.nagios.org.

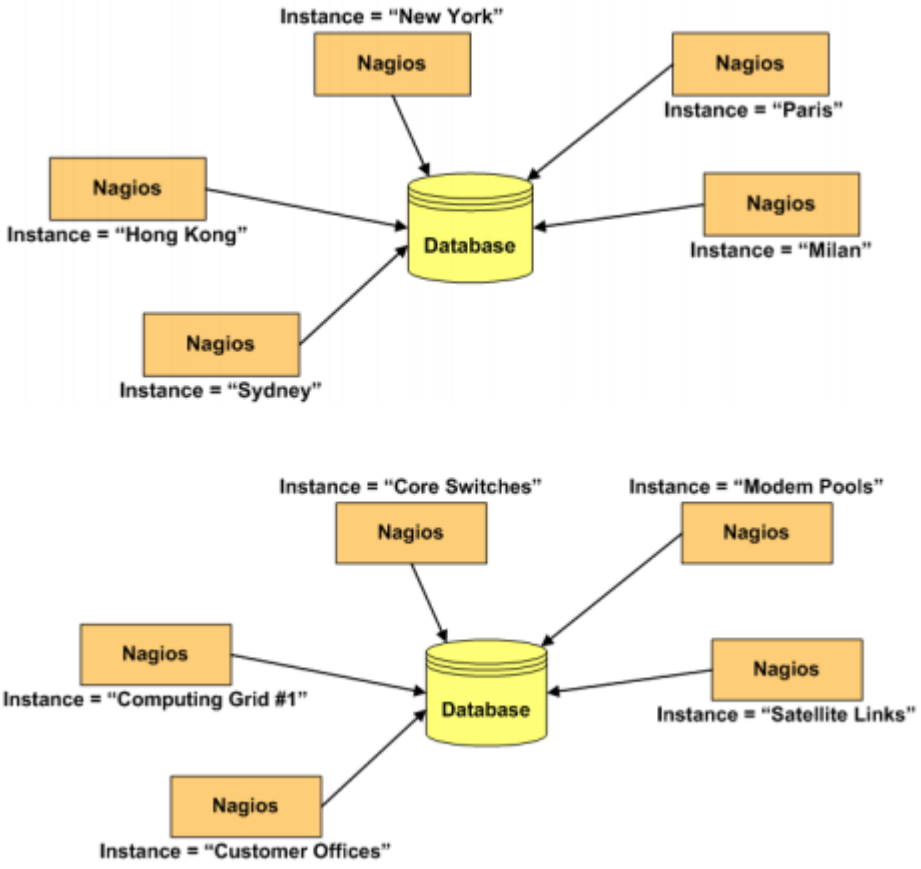
4.4 NDOUtils

NDOUtils on lisäosa Nagiokseen, jonka tarkoituksen on tallentaa kaikki kokoonpanoasetukset sekä tapahtumatiedot tietokantaan tai -kantoihin. Tämän tiedon avulla lisäosat ja useammat Nagios-palvelimet voivat nopeammin noutaa tietoja, ja ne toimivat Nagios XI -verkkohallintasivuston pohjana. Datat jokaisesta Nagioksen prosessista (tästä lähin puhutaan prosesseista termillä *instanssi*) voidaan joko tallentaa yhteiseen tietokantaan tai erillisiin kantoihin. Tulevaisuudessa on mahdollista tallentaa yhdestä instanssista useampaan tietokantaan. Tämä ei kuitenkaan ole vielä julkaistu ominaisuus.



Kuva 14. Tietokantojen tallennusvaihtoehdot havainnoillistettuna. [2]

Jokaisella instanssilla täytyy olla oma uniikki nimensä tallennettaessa yhteiseen tietokantaan datan ehyyden säilyttämiseksi. Instanssit voivat olla esimerkiksi eri lokaatioiden nimet tai eri laitteet omissa valvonnoissaan, esimerkiksi palvelimet ja verkkolaitteet omissaan.



Kuva 15. Esimerkkejä nimeämistavoista [2]

NDOUtilssissa on neljä pääkomponenttia, joiden avulla kyseinen lisäosa toimii:

- NDOMOD Event Broker Module
- LOG2NDO Utility
- FILE2SOCK Utility

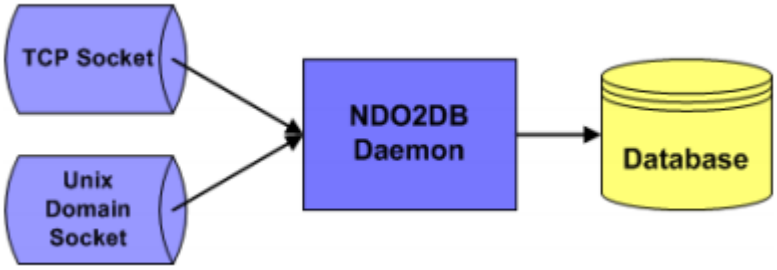
- NDO2DB Daemon.

NDOMOD on moduuli, joka hakee dataa Nagioksen daemonista. Moduuli on suunniteltu hakemaan konfiguraatiotiedot sekä vaihtelevat tapahtumat valvontaprosessiin liittyen Nagioksen daemonilta. NDOMOD kirjoittaa datan sellaisessa muodossa, että NDO2DB daemon ymmärtää sitä.

LOG2NDO-apuohjelma on suunniteltu viemään Nagioksen vanhempia lokitiedostoja tietokantaan NDO2DB daemon kautta.

FILE2SOCK-apuohjelma on suunniteltu pelkästään viemään dataa tiedostosta tai STDINin kautta TCP Socketin tai Unix Domain Socketin avulla.

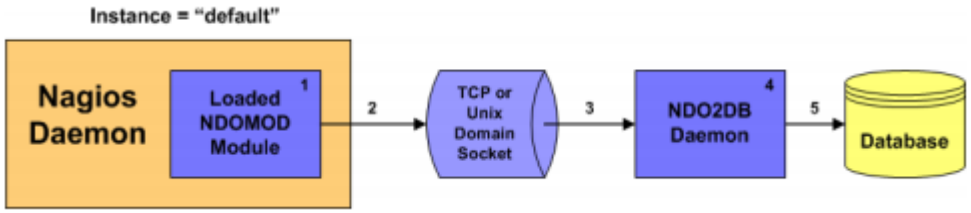
NDO2DB Daemon on suunniteltu ottamaan vastaan dataa NDOMOD ja LOG2NDO -komponenteilta ja tallentamaan sen tietokantaan.



Kuva 16. NDO2DB:n toimintaperiaate [2]

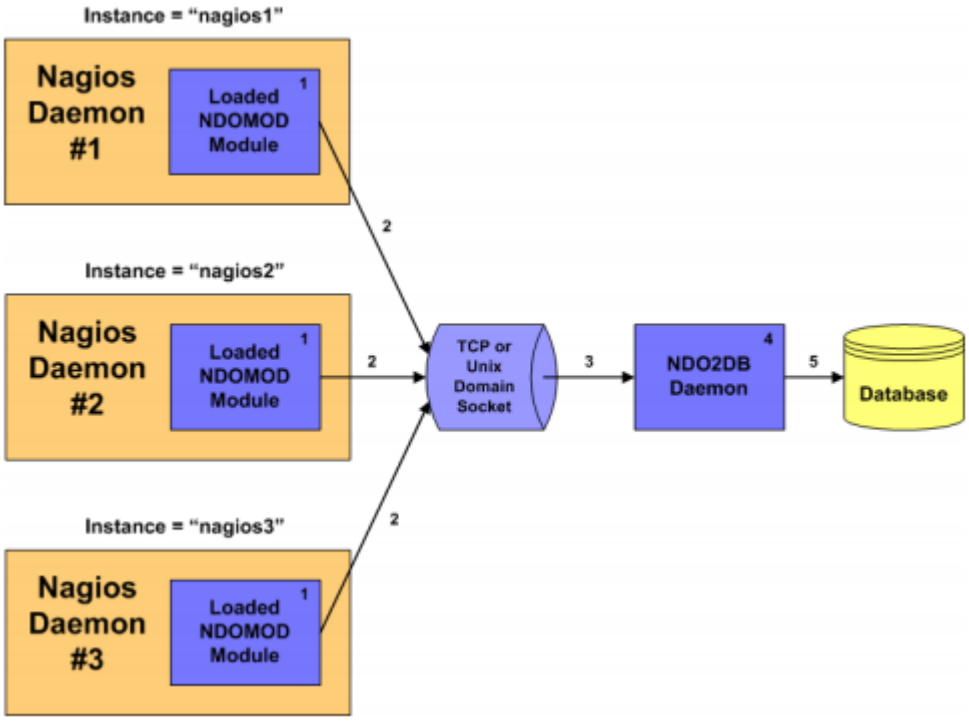
Esimerkkikonfiguraatioita NDOUtilssin käytöstä.

1. Yksittäinen palvelin ja instanssi



Kuva 17. Yksittäinen palvelin ja instanssi [2]

2. Yksi palvelin, useita instansseja



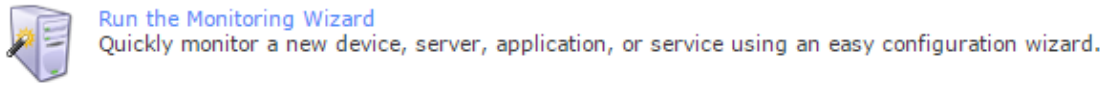
Kuva 18. Yksittäisen palvelimen ja usean instanssin toimintaperiaate [2]

5 Palveluiden ja laitteiden valvonta

Nagioksessa on mahdollista valvoa kymmeniä erilaisia palveluita ja laitteita. Seuraavana on listattuna muutama yleinen valvontakohde. Tässä dokumentissa kerrotut monitorointitavat vaativat kaikki ohjatun asennuksen (Monitoring wizard) käyttöä. Jokaisessa eri asennuspaketissa on muutamat yhteiset tekijät, joista tarkemmin tietoa alla.

5.1 Ohjatun asennuksen käyttö

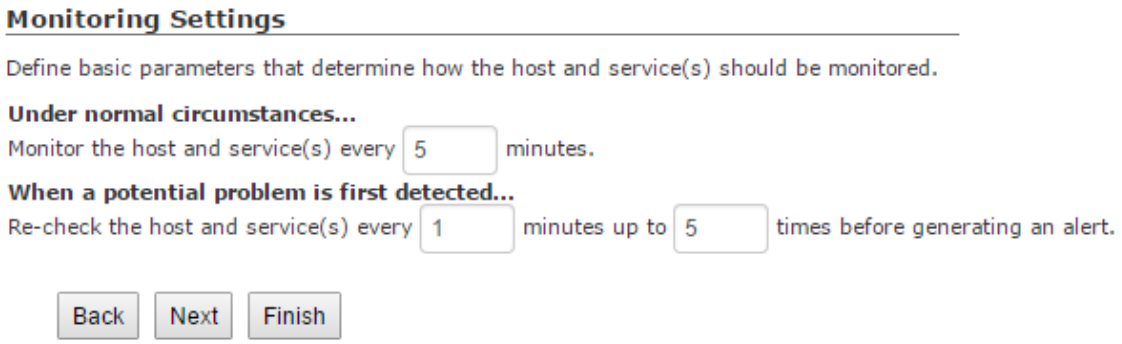
Ohjattu asennus löytyy suunnistuspalkin **Configure**-linkin takaa. Linkkiä klikkaamalla aukeaa sivu, missä on ohjatun asennuksen linkki sekä muun muassa Core Configuration Managerin (CCM) linkki. CCM:ssä pystyy hallita tarkemmin valvontakoneen asetuksia, mutta vaatii yksityiskohtaista osaamista systeemistä.



Kuva 19. Ohjatun asennuksen ikoni **Configure**-sivulla.

5.2 Monitorointiasetukset

Ensimmäiset sivut vaihtelevat asennuksen tyypistä riippuen, mutta ensimmäinen yhteinen sivu kaikilla on **Monitoring Settings** -vaihe. Tässä päätetään monitorointitiheys palvelulle / laitteelle. Ensin valitaan normaalitilanteessa olevan laitteen monitorointitiheys (vakiona 5 min.), sekä alempana vikatilassa olevan laitteen asetukset. Vakiona laite ei lähetä hälytystä heti ongelman ilmettyä, vaan odottaa muutamia minuutteja. Tämä asetus on vakiona tarkistus kerran minuutissa viiden minuutin ajan, jonka jälkeen lähetetään hälytys sähköpostilla ja/tai tekstiviestillä asetuksista riippuen.

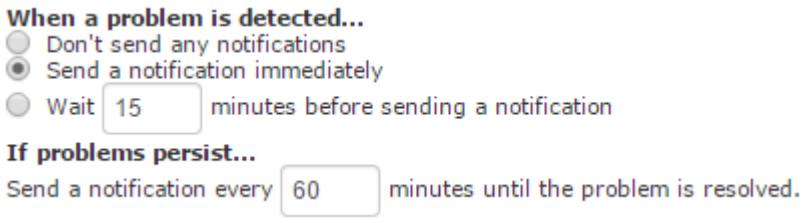


Kuva 20. Monitorointiasetukset

5.3 Ilmoitusasetukset

Kun monitorointitiheyden arvot on asetettu, päätetään, kenelle lähetetään vikailmoitukset, kun aikaisemmin päätetty aika on mennyt umpeen. Vakiona ei ole määriteltynä kuin palvelun lisääjä (Myself), joka voi useissa tapauksissa olla väärä henkilö ilmoituksille. Vastaanottajat voidaan määritellä yksitellen tai kontaktiryhmien avulla (Contact group). Contact grouppeja pääsee luomaan Core Config Managerin kautta.

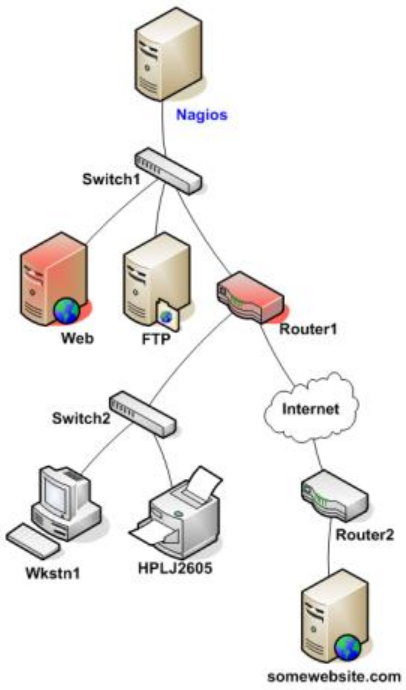
Sivulla voidaan myös määritellä, milloin hälytys ensimmäisen kerran lähetetään ja lähetetäänkö ongelmasta ylimääräisiä sähköposteja, kunnes ongelma on kuittaantunut. Nämä ajat tai ilmoitusten lähetykset eivät vaikuta näkymään hallintasivustolla, eli ongelma näkyy siellä, vaikka viestiä ei lähetettäisikään.



Kuva 21. Ilmoitusasetukset

5.4 Laite- ja palveluryhmät sekä isäntälaite

Ilmoitusasetusten jälkeen valitaan, mihin ryhmään palvelu tai laite kuuluu (jos kuuluu). Laitteiden tai palveluiden ryhmittäminen helpottaa hallinnointia varsinkin isoilla valvontakohdemäärillä. Voidaan myös valita, onko laitteella pääpalvelua tai -palvelinta. Tämä voi olla esimerkiksi kytkin tai reititin seuravaana verkkotopologiassa. Pääpalveluilla voidaan paremmin hallita hälytysten määrää, esimerkiksi jos yksi kytkin on tavoittamaton, ei kaikki palvelut sen takana aiheuta hälytyksiä tilalla DOWN, koska Nagios osaa katsoa että niiden tavoitettavuus on viallisesta kytkimestä johtuva. Sen sijaan kyseisille palveluille annetaan UNREACHABLE-tila.



Kuva 22. Isäntälaitteen toimintaperiaate. [3]

Kuvassa 22 Web-palvelin sekä Router1-reitin ovat alhaalla. Kaikille kohteille Router1 alla annetaan tilaksi UNREACHABLE, koska Nagios ei saa laitteisiin yhteyttä ja niille määritelty isäntälaite on tilassa DOWN. Web ja Router1 sen sijaan saavat tilaksi DOWN, koska polku niihin ei ole alhaalla, mutta itse laite ei vastaa.

5.5 Yleisimpien valvonta-agenttien erot

Ohessa on NCPA-kehittäjän rakentama vertailutaulukko eri valvonta-agenttien toiminnasta. NCPA on tekniikoista uusin ja sen myötä myös kaikkein monipuolisin. Listassa ei tosin mainina NRPE:n ja NSClient++:n mahdollisuutta ajaa komentoja etäkoneelle.

Agent Comparison:

Features \ Edition	NCPA	NRDS Agent	NSClient ++	NRPE
Installs on Linux	✔	✔		✔
Installs on Windows	✔	✔	✔	
Installs on Mac OSX	✔	✔		✔
Graphical User Interface	✔			
Active Check Metrics	✔		✔	✔
Passive Check Capabilities	✔	✔	✔	
Flexible API Access	✔			
Seamless Integration with Nagios XI	✔		✔	✔
Integration with Nagios Core via NRDP	✔	✔	✔	
Official Nagios Enterprises Monitoring Agent	✔			
Pre-configured Monitoring Metrics	✔		✔	✔
Integration with NRDS Configuration Protocol	✔	✔		

Kuva 23. Agenttien eroavaisuuksia

5.6 NCPA

NCPA eli Nagios Cross Platform Agent on palvelinkäyttöjärjestelmästä riippumaton valvonta-agentti, joka pystyy sekä passiiviseen että aktiiviseen valvontaan. Nagios XI:ssä on uudemmissa versioissa valmiiksi asennettuna NCPA:n palvelinohjelmisto, joten valvonta vaatii ainoastaan agentin asentaminen valvottaville palvelimille ja ajamalla ohjatun asennuksen Nagioksen hallintasivustolta. Agentin asennusoperaatio vaihtelee hieman käyttöjärjestelmän mukaan, alla ohjeet eri käyttöjärjestelmille. Uusimmat agenttien asennuspaketit löytyvät osoitteesta:

https://assets.nagios.com/downloads/ncpa/download.php

5.6.1 Palomuuriavaukset Windowsille ja Linuxille

NCPA vaatii toimiakseen portin 5693 auki. Alla ovat ohjeet, kuinka sen saa avattua käyttöjärjestelmien puolelta. Mutta jos infrastruktuurissa on välissä palomuureja, tarvitsee ne erikseen avata.

Linuxille muurien avaus onnistuu muokkaamalla /etc/sysconfig/iptables-tiedostoa. Lisäämällä seuraavan rivin OUTPUT ACCEPT -kappaleeseen saadaan portti auki:

-A INPUT -p tcp --dport 5693 -j ACCEPT

Tämän jälkeen käynnistetään iptables uudestaan komennolla *service iptables restart*.

On muistettava, että CentOS7 ja Red Hat 7:ssa on käytössä firewalld, joka toimii eri tavalla kuin iptables. Firewalld:ssa saa portin avattua ja palvelun uudelleenkäynnistettyä komennoilla

```
firewall-cmd --zone=public --add-port=5693/tcp --permanent
firewall-cmd --reload
```

Windowsin palomuuriavaukset tehdään käyttöliittymän kautta. Avataan ensin Control Panel→System and Security→Windows Firewall→Advanced Settings

Valitaan Inbound Rules vasemmasta laidasta ja sen jälkeen oikeasta laidasta New Rule. Valitaan tyypiksi Port ja painetaan Next. Protokollaksi valitaan TCP ja Specific local ports, arvoksi 5693 ja valitaan Next.

Valitaan Domain-, Private- ja Public-vaihtoehdoista omaan ympäristöön oikeat vaihtoehdot ja Next. Annetaan säännölle vielä nimi (esimerkkinä Nagios NCPA) ja painetaan Finish.

Lisäksi kannattaa muistaa, että ulkopuolelta tulevat yhteydet eivät välttämättä vakiona ole toiminnassa. Tällöin Nagioksen palvelimelle pitää erikseen kertoa reitti muualle verkkoon. Alla on esimerkki vakioreiteistä:

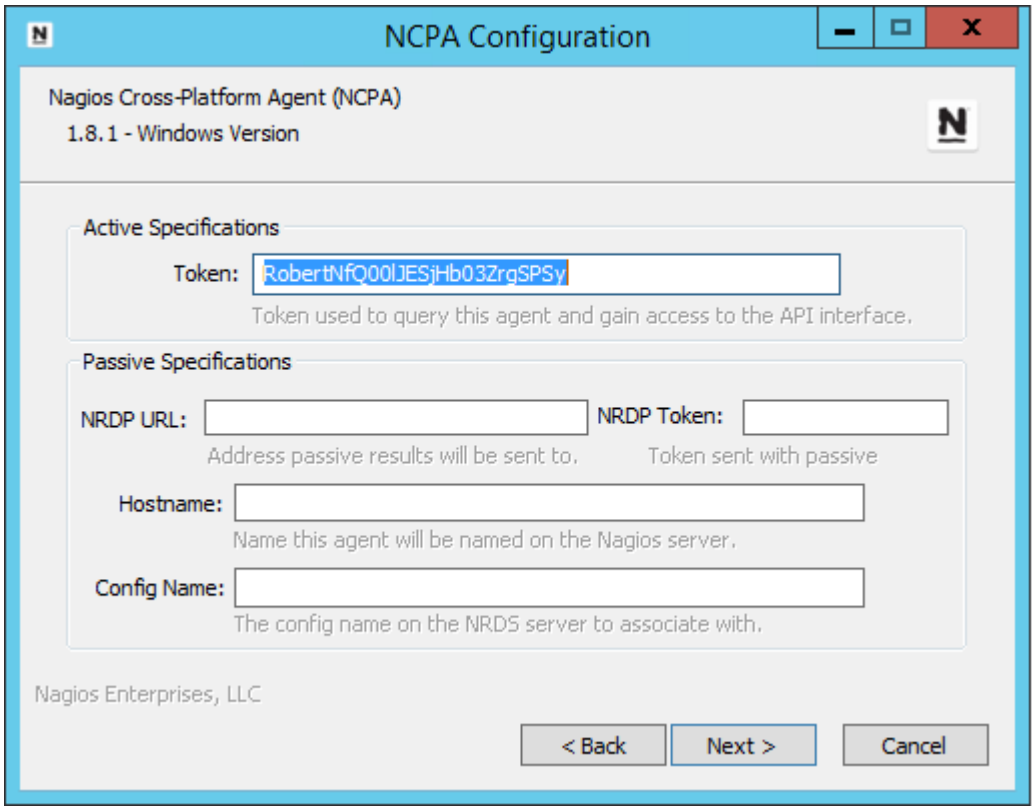
```
[root@Nagios ~]# netstat -nr
Kernel IP routing table
Destination     Gateway         Genmask         Flags   MSS Window  irtt Iface
192.168.0.0     0.0.0.0         255.255.255.0   U         0 0          0 eth0
169.254.0.0     0.0.0.0         255.255.0.0     U         0 0          0 eth0
```

Reitin ulkoverkkoon saa lisättyä komennolla */sbin/route add -net 0.0.0.0 gw <gatewayn-ip> eth0*.

eth0 on palvelimen verkkokortti, josta reitti halutaan ulkomaailmaan. Voidaan esimerkiksi varata toinen verkkokortti sisäverkolle ja toinen ulkomaailmaan. Kyseinen reitti kuitenkin katoaa aina uudelleenkäynnistyksen yhdeydessä, joten olisi hyvä lisätä /etc/sysconfig/network -tiedostoon kohta GATEWAY=<gatewayn IP>, esimerkiksi GATEWAY=192.168.0.1.

5.6.2 Windows Serverin aktiivinen valvonta

Agentin lataamisen jälkeen agentin asennus aloitetaan hyväksymällä lisenssiehdot. Ehtojen hyväksynnän jälkeen avautuu konfiguraatioikkuna, johon riippuen valvonnan tyypistä laitetaan pelkästään token, joka mahdollistaa aktiivisen valvonnan. Tämä token tuotantoverkossa hyvä generoida satunaiseksi ja laittaa muistii asentamisen ajaksi. Tokenia tarvitsee, kun konetta lisää valvontaan itse valvontapalvelimella.

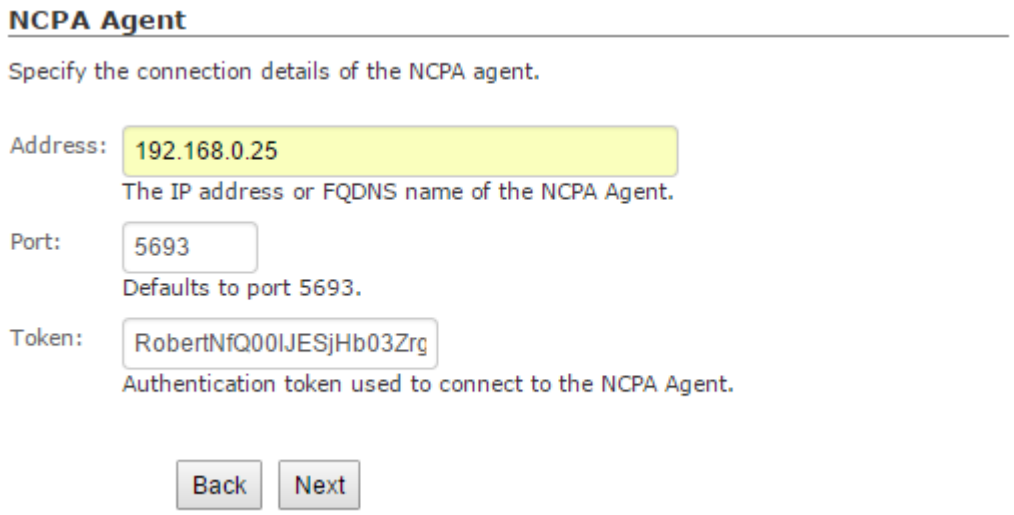


Kuva 24. NCPA-agentin asennus Windows-käyttöjärjestelmälle

Kun token on lisätty, jatketaan painamalla Next-painiketta, jonka jälkeen valitaan asennuskansio ja painetaan Install. Tämän jälkeen agentti on toiminnassa ja voidaan siirtyä Nagioksen hallintapaneeliin lisämään palvelin valvontaan ohjatun asennuksen kautta.

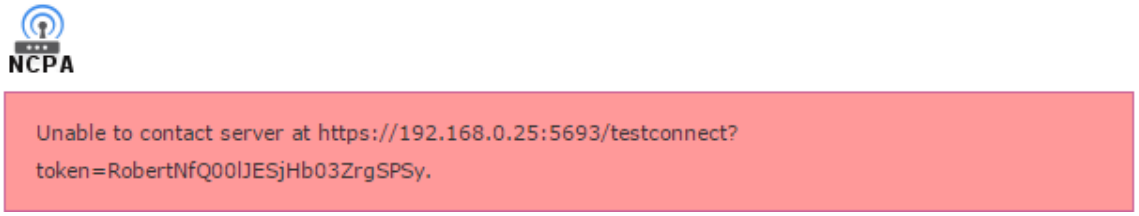
Kuva 25. NCPA Agent -kuvake ohjattujen asennusten listassa

Kun NCPA Agent on valittu ja siirrytty sivun alalaidasta seuraavalle sivulle, laitetaan Address-kenttään valvottavan koneen IP-osoite, portti (vakiona TCP 5693), sekä aikaisemmin generoitu token.



Kuva 26. Tarvittavat tiedot aktiivisen valvonnan lisäämiseen NCPA-agentilla

Jos valvonnan lisäämisessä saadaan virheilmoitus yhteydestä, kannattaa tarkistaa, että Nagios-palvelimelta, kohdekoneelta sekä mahdollisilta palomuureilta verkosta.



Kuva 27. Virheilmoitus valvontaa lisättäessä

Seuraavaksi aukeaa sivusto, josta voidaan valita, mitä halutaan monitoroida palvelimelta. Yleisimpiä ovat levytila, muistin ja prosessorin käyttöaste sekä verkon kuormitus. Voidaan myös esimerkiksi seurata, onko DNS:n tai DHCP:n palvelut käynnissä ja jos eivät ole, tulee siitä hälytys Nagiokselle.

Jos hallintasivusto antaa statukseksi ”UNKNOWN: Error occurred while running the plugin.”, on NCPA Agent jumissa palvelimella. NCPA-agentissa on bugi tällä hetkellä, jonka voi kiertää laittamalla NCPA Listener ja NCPA Passive -palvelut käynnistymään Delayed Start -tilassa

5.6.3 Windows Serverin passiivinen valvonta

Passiivinen valvonta menee pitkälti samalla tavalla kuin aktiivinen seuranta, mutta agentin asennusvaiheessa tokenin sijaan annetaan NRDP URL, NRDP Token, Hostname sekä Config Name.

NRDP URL löytyy hallintasivustolta Admin→Inbound Transfers→NRDP-välilehdeltä. Esimerkkinä **http://192.168.0.20/nrdp/**. NRDP Token löytyy samalta välilehdeltä ja olisi suositeltavaa tehdä jokaiselle valvontakohteelle tai ryhmälle erillinen token, mutta samalla voidaan myös valvoa useita kohteita. Hostname on nimi, jolla agentti lähettää tiedot Nagiokselle. Tämä on yleensä koneen nimi. Config Name on NRDS konfigurointitiedoston nimi. NRDS-konfigurointitiedosto on tiedosto Nagioksen palvelimella, mihin on kirjattu, mitä palveluita tai tietoja passiivisesti valvottavista kohteista halutaan tietää. NRDS-konfiguraatioita pääsee muokkaamaan hallintasivustolta menemällä **Admin**→NRDS Config Manager. Kyseiseltä sivulta voidaan painaa Create Config -linkkiä, jonka jälkeen valitaan käyttöjärjestelmä. Kun käyttöjärjestelmä on valittu, siirrytään seuraavalle sivulle, jossa voi tarkemmin määrittää muun muassa komennot, nimet, tokenin jota käytetään, sekä palvelimen osoitteen.

5.6.4 Windows Serverin hiljainen asennus

Massa-asennusta varten on usein tarpeellista tehdä asennus taustalla tai antaa parametrit suoraan komentoriviltä. Tämä onnistuu Windows-palvelimiin komentoriviltä seuraavalla tavalla:

ncpa-<versio>.exe /S /parametri=arvo

Esimerkkinä voidaan SCCM:n kautta ajaa asennuspaketti ja laittaa halutut parametrit etänä massakäyttöönottona.

Aktiivisella valvonnalla komento menisi aikaisemman esimerkkitapauksen kanssa:

Ncpa-1.8.1.exe /S /token=RobertNfQ00lJESjHb03ZrgSPSy

Passiivista valvontaa varten parametreinä voidaan käyttää NRDPURL, NRDPTOKEN, HOST sekä CONFIG.

5.6.5 Red Hat/CentOS/OpenSUSE aktiivisen agentin asennus

RPM-paketinhallintaa käyttäville käyttöjärjestelmille asennus hoituu seuraavilla komenoilla:

```
cd /tmp
wget <.rpm paketin sijainti ja versio>
rpm -ivh --nomd5 <ladattu .rpm-tiedosto>
```

Kun paketti on asennettu, täytyy /usr/local/ncpa/etc/ncpa.cfg-tiedostoa muokata. Aktiivista valvontaa varten tiedostosta löytyy rivi:

```
[api]
community_string=<generoitu token>
```

Kyseistä tokenia/community stringiä tarvitsee Windowsin tapaan palvelinta lisättäessä valvontaan Nagioksen hallintasivulla.

Passiivista valvontaa varten pitää muokata rivejä Windowsin passiivisen valvonnan kaltoin:

```
[nrds]
URL = None
CONFIG_VERSION = None
TOKEN = None
CONFIG_NAME = None
CONFIG_OS = None
```

Kun tiedosto on tallennettu, käynnistetään agentti uudestaan */etc/init.d/ncpa_listener restart.*

5.6.6 Ubuntu/Debian aktiivisen agentin asennus

DEB-paketinhallintaa käyttäville asennus on miltei yhtäläinen RPM-käyttöisten kanssa.

cd /tmp
wget <.deb tiedosto sijainti ja versio>
dpkg -i <ladattu .deb tiedosto>

Kun paketti on asennettu, täytyy /usr/local/ncpa/etc/ncpa.cfg-tiedostoa muokata kuten edellisessä kohdassa.

[api]
community_string=<generoitu token>

Kun tiedosto on tallennettu, käynnistetään aktiivisen valvonnan agentti uudestaan komennolla */etc/init.d/ncpa_listener restart* tai passiivisen valvonnan kohdalla komennolla */etc/init.d/ncpa_passive restart*.

5.6.7 Passiivisen valvonnan lisäys Linuxille

Passiivisen valvonnan lisääminen Linuxillle menee alusta samalla tavalla kuin aktiivisen valvonnan lisääminen eli asennetaan .rpm- tai .deb-tiedosto. Tämän jälkeen mennään Nagioksen hallintasivulle NRDS Config Manageriin kohdan 5.1 mukaisesti. Kyseiseltä sivulta tehdään uusi konfiguraatio ”Create Config” -linkin kautta. Valitaan käyttöjärjestelmäksi Linux ja painetaan Next. Seuraavaksi annetaan konfiguraatiolle nimi sekä valitaan Token, mitä halutaan käytettävän. Valikkoon saa lisää Tokeneita Inbound Transfers -hallintasivulta. Kun on asetettu halutut komennot ja asetukset, valitaan alalaidasta Save.


Create Config

Config Name	Directory	Owner	Group	Permissions	Last Changed	Actions
Linuxtesti	configs	48	500	rw-rw----	2015-05-19 00:41:06	

Kuva 28. Konfiguraatioiden hallinta

Päästään takaisin Config Manageriin, jossa äsken tehty konfiguraatio pitäisi näkyä. Klikataan Actions-valikosta toista ikonia ”Client Install Instructions”, jolloin sivulle tulee näkyviin komennot, jolla aktiivinen seuranta saadaan toimintaan. Alla ovat testiympäristön komennot:

```
cd /tmp
wget -O Linuxtesti.tar.gz "http://192.168.0.20/nrdp/?cmd=nrdsgetclient&token=Testi123&con-
figname=Linuxtesti"
gunzip -c Linuxtesti.tar.gz | tar xf -
cd clients
./installnrds HOSTNAME INTERVAL
```

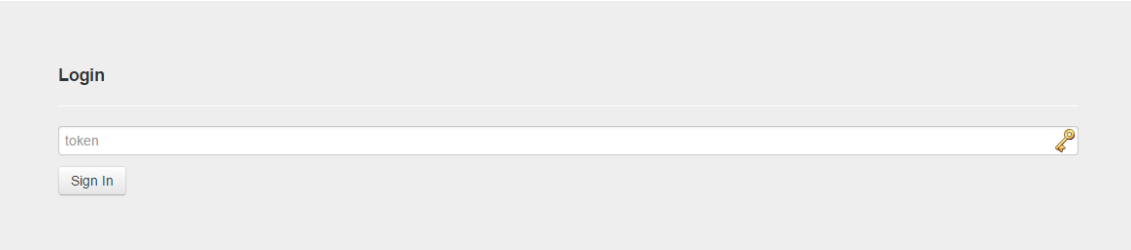
Komennot voidaan viimeistä lukuunottamatta suoraan kopioida ja liittää terminaaliin. Viimeiseen annetaan HOSTNAME-kenttään valvottavan palvelimen osoite ja INTERVAL-kenttään aika minuutteina, kuinka usein palvelin lähettää dataa Nagiokselle.

Kun asetukset on ajettu palvelimelle, voidaan mennä takaisin hallintapaneeliin ja valita vasemmasta reunasta Unconfigured Objects. Palvelimen, jolle passiivinen seuranta laitettiin, pitäisi ilmestyä hetken päästä listaan. Valitaan palvelin listasta ja painetaan sinistä nuolta sen alla. Painetaan Nextiä pari kertaa, ja palvelin ilmestyy valvottavien listaan.

Jos konfiguraatioon tehdään muutoksia, esimerkiksi lisätään valvontakomentoja tai lisäosia, kaikki kyseistä konfiguraatiota käyttävät lataavat muutokset ja lisäosat automaattisesti käyttöönsä, kun seuraavan kerran dataa lähetetään.

5.6.8 Agentin testaaminen

Agentin toimivuutta voi testata menemällä selaimella osoitteeseen https://<palvelimen ip>:5693 ja antamalla tokenin / community stringin, jota asennusvaiheessa käytettiin. Sivusto yleensä antaa SSL-herjan, mutta sen voi ohittaa. Sivuston kautta voi myös katsoa reaaliaikaista dataa palvelimelta. Jos tulee virheviestejä koittaessa päästä sivulle, kannattaa tarkistaa palomuuriavaukset.



Kuva 29. Agentin testaaminen verkkoselaimella

5.6.9 Ulkoverkossa olevan koneen valvonta

Usein ulkoverkossa olevat koneet ovat estäneet ICMP:n käytön, jolloin check_icmp (ping) ei toimi ja laitteen statukseksi tulee DOWN, vaikka palvelut ja palvelin toimisi moitteetta. Tämä voidaan kiertää Windows-palvelimissa NCPA-agentin ja monitorointikomennon vaihtamisella. Kun aktiivinen valvonta on toiminnassa palvelimella, mennään hallintapaneelista halutulle laitteelle ja sieltä Configure-välilehdelle. Valitaan Re-Configure this host, jonka jälkeen voidaan avata Monitoring-välilehti. Vaihdetaan **Monitor the host with this command …** -kohtaan komento (huutomerkit kuuluvat komentoon):

check_tcp!5693!-t 50!!!!!!

Kyseinen komento käyttää TPC-tarkistusta NCPA-agentin käynnistämään pienehköön webbipalveluun, joka antaa statukseksi ok, eikä laite hälytä DOWN-tilassa enää.

Linux-palvelimissa voidaan käyttää SSH-tarkistusta. Tämä saadaan vaihtamalla **Monitor the host with this command ...** -kohtaan:

check_xi_service_ssh!!!!!!!!

Tämä vaatii linux-koneelta aktiivisen ssh-palvelun, joka vakiona on käynnissä.

5.7 NRPE:n lisääminen Linux-palvelimelle

NRPE:n lisääminen valvottavalle koneelle on tehty helpoksi, eikä se vaadi erityistä Linux-osaamista. Ajetaan vain seuraavat komennot valvottavalle palvelimelle:

```
cd /tmp
wget          http://assets.nagios.com/downloads/nagiosxi/agents/linux-nrpe-agent.tar.gz
tar xzf linux-nrpe-agent.tar.gz
cd linux-nrpe-agent
sudo ./fullinstall
```

NRPE-agentin asentamisen komennot RHEL/CentOS 5+, Fedora 14+, SLES 11+, OpenSUSE 11+, Ubuntu 12+, and Debian 6+ -käyttöjärjestelmillle.

./fullinstall hoitaa automaattisesti tarvittavat toimenpiteet, johon kuuluu muun muassa tarvittavien käyttäjien ja ryhmien luonti, tarvittavien pakettien ja pakettivarastojen lisäämisen sekä itse NRPE-agentin ja sen yleisimpien lisäosien asentamisen.

5.8 Verkkolaitteiden lisääminen valvontaan

Verkkolaitteita voidaan valvoa pelkästään pelkän pingin avulla, mutta tehokkaampi ja yleisempi tapa on käyttää SNMP:tä laitteissa, jotka sitä tukevat. Näitä on muun muassa reittittimet, palomuurit sekä kytkimet. Miltei kaikki nykypäivän valmistajat ja laitteet tukevat SNMP:tä laitteissaan. Uusin versio tekniikasta on versio 3, eli SNMPv3.

SNMP:n kautta hoidettava valvonta voidaan hoitaa joko SNMP Trap -valvonnan tai pelkän SNMP -valvonnan avulla. SNMP Trap:ssa valvottava laite itse lähettään tietoja valvontapalvelimelle, kun taas perinteisessä SNMP-valvonnassa valvontapalvelin lähettää kyselyitä laitteelle säännöllisin väliajoin. SNMP Trapit vaativat UDP-portin 162 auki palomuurista sisäänpäin palvelimelle.

5.8.1 SNMP-valvonnan lisäys

SNMP:tä varten täytyy valvottavalle laitteelle lisätä SNMP Community String, jota käyttämällä valvontapalvelin saa haettua tietoa laitteelta. Kyseisen stringin laitto

vaihtelee eri valmistajien ja valmistajien omien käyttöjärjestelmien kesken, mutta esimerkkinä Ciscon IOS-ohjelmistossa sen asettaminen käy seuraavasti:

Kirjaudutaan normaalisti laitteelle SSH:n, telnetin tai konsoliyhteyden kautta ja kirjaudutaan enable-modeen komennolla *enable*. Siirrytään konfiguraatiomoodiin *configure terminal* -komennolla.

Lisätään string komennolla *snmp-server community NagiosRobertN ro*, jossa NagiosRobertN on haluttu string. Kyseistä stringiä käytetään, kun palvelua lisätään valvontaan. Ro rivin lopussa tarkoittaa Read-Only, eli laitteelta voi ainoastaan lukea statistiikkaa, eikä sillä voi tehdä muutoksia.

SNMPv3 vaatii Community Stringin lisäksi mahdollisesti autentikoinnin. Tämä tehdään seuraavalla tavalla:

snmp-server group <Nimi> v3 <Haluttu turvataso> . Turvatasoja on kolme eri:

- auth, jossa on MD5 ja SHA-autentikointi käytössä.
- noauth, jossa ei ole suojauksia käytössä. Tämä on oletusasetus jos ei valita erikseen muuta
- *priv*, lisää suojaukseen DES-kryptauksen. Tämä vaatii erillisen kryptograafi-tuen laitteelta. Tunnetaan myös nimellä Privacy.

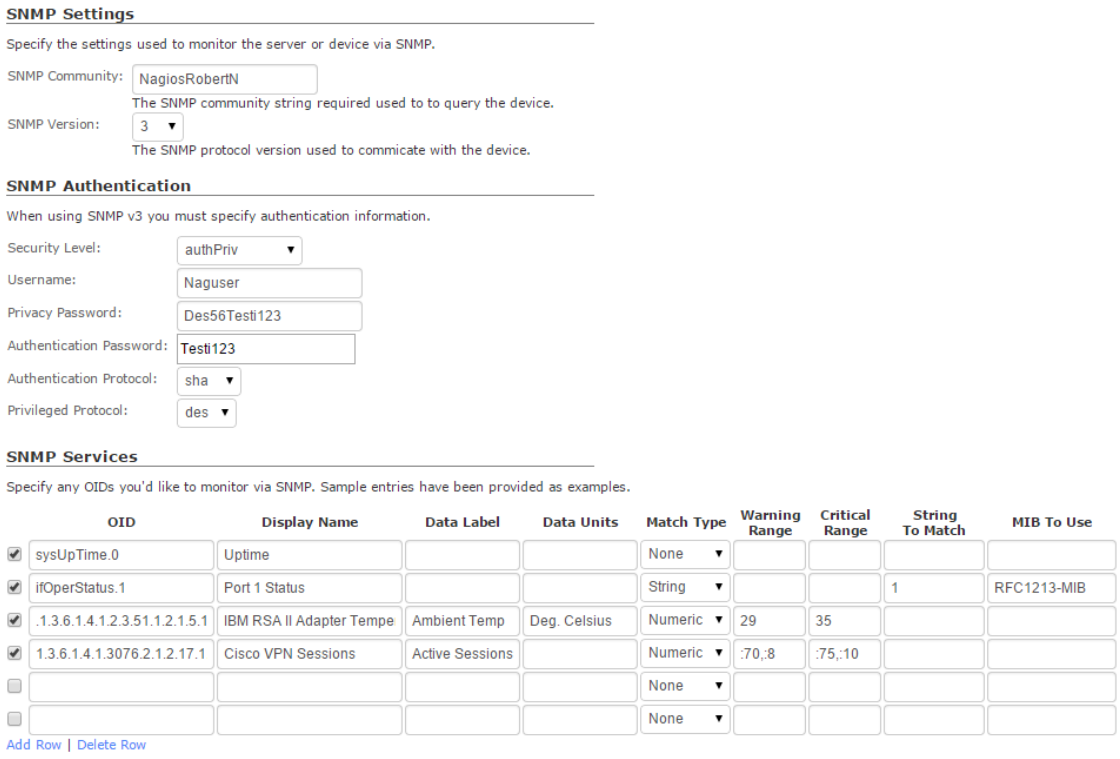
Esimerkkinä käytetään snmp-server group Nagios v3 priv.

Lisätään seuraavaksi käyttäjä tehtyyn ryhmään:

snmp-server user Naguser Nagios v3 auth sha Testi123 priv des56 Des56Testi123

Komennossa tehdään käyttäjä Naguser, joka lisätään ryhmään Nagios (luotiin yläpuolella). Tämän jälkeen valittiin SNMP:n versioksi 3, autentikointitavaksi sha ja autentikointisalasanaksi Testi123 sekä kryptausmenetelmäksi des56 ja privacyn salasanaksi Des56Testi123.

Kun käyttäjä on luotu, voidaan laite lisätä valvontaan ohjatun asennuksen avulla. Täytetään tiedot, joita aikaisemmin luotiin, ja valitaan, joita valvotaan. OID:t löytää valmistajien omilta sivuilta. Esimerkiksi Ciscon haku OID:lle on osoitteessa http://tools.cisco.com/Support/SNMP/do/SearchOID.do?local=en&step=1



Kuva 30. SNMP-valvonnan asetukset

Jos valvonnan lisäyksen jälkeen Service Status näyttää tilaksi ”Usage:”, joudutaan valvontakomentoa muokkaamaan käsin. Tämä onnistuu kohdan 5.6.9 tavoin, eli muokataan Monitor this service with command … -kenttää. Esimerkiksi Port Status 1 -kohdan komento on luonnin jälkeen

check_xi_service_snmp! -o ifOperStatus.1 -P 3 --seclevel=authPriv --secname=Naguser --authproto=sha --authpasswd='Testi123' --privpasswd='Des56Testi123' --protocols=sha,des -m RFC1213-MIB -r "1"

Tämä muokataan muotoon:

check_xi_service_snmp! -P 3 -o ifOperStatus.1 -L authPriv -U Naguser -a sha -A 'Testi123' -X 'Des56Testi123' -x des -m RFC1213-MIB -r "1"

Eli parametrit muutettiin toiseen muotoon. Tämä on mitä luultavammin ohjelmointivirhe ohjelmistossa ja tullaan korjaamaan tulevaisuudessa.

Jos ei ole tiedossa, mitä OID:ta halutaan mahdollisesti valvoa, voidaan myös käyttää SNMP Walk -asennusta. Tähän laitetaan kaikki samat tiedot kuin SNMP-valvontaan, mutta valvontapalvelin skannaa valvottavan koneen läpi ja listaa kaikki OID:t, mitä löytyy. Näistä voidaan sen jälkeen valita halutut ja edetä asennuksessa.

5.8.2 SNMP Trap -valvonnan lisäys

SNMP Trapit ovat tehokkaita keinoja valvoa verkkolaitteita, mutta vaativat suhteellisen paljon osaamista ja perehtymistä eri OID ja MiB -tietoihin. Jokainen valvottava laite vaatii trap-määritykset itse laitteelle, ja näiden asettaminen vaihtelee laitteiden kesken.

Aluksi SNMP-trappeja varten joudutaan asentamaan muutamia lisäosia palvelimelle. Tämä onnistuu palvelimen kirjoittamalla palvelimen terminaaliin:

cd /tmp
wget *http://assets.nagios.com/downloads/nagiosxi/scripts/NagiosXI-SNMPTrap-setup.sh*
sh ./NagiosXi-SNMPTrap-setup.sh

Kuten dokumentissa aikaisemmin todettiin, SNMP Trapit vaativat UDP 162 portin auki sisäänpäin. Äsken ajettu komentosarja avaa sen itse valvontapalvelimella, mutta jos ympäristössä on välissä palomuureja, tarvitsee ne avata erikseen.

On mahdollista että tulee tarve ylimääräisille MiB-komponenteille tiettyjen valvottavien laitteiden kanssa. Näitä voi lisätä terminaalista komennolla addmib <polku tiedostoo> tai hallintasivuston **Admin**→Manage MiB-sivuston kautta.

Tämän jälkeen voi olla tarpeen muokata eri hälytyksiä omiin tarpeisiin /etc/snmp/snmptt.conf-tiedostossa. Voidaan esimerkiksi muokata Link Down -vakavuutta kirjoittamalla muokkaamalla Normal → Critical -statukseen.

Kun nämä on tehty, mennää ohjattuun asennukseen ja valitaan SNMP Trap-vaihtoehto. Saadaan lista laitteista ja valitaan, mitä halutaan valvoa. Tämän jälkeen jatketaan suoraan ohjattua asennusta.

Jos SNMP Trap -palvelun lisäämisen jälkeen kannattaa testata esimerkiksi yhden portin sammuttamista testimielessä valvotulta laitteelta. Jos tilana on edelleen ”Waiting for traps…” -ei trap ole tullut perille. Tällöin voidaan aloittaa tarkastamalla /var/log/snmptt/snmpttunknown.log- ja /var/log/snmptt/snmptt.log-tiedostot. Jos kummassakaan ei ole mitään tai tiedostoja ei ole lainkaan, eivät trapit tule palvelimelle asti. Tällöin kannattaa tarkistaa palomuuriasetukset ja valvottavien laitteiden SNMP Trap -asetukset.

Jos snmpttunknown.log-tiedostossa näkyy rivejä, tarkoittaa se, että snmptt.conf-tiedosto ei osaa lukea hälytystä oikein. Tällöin snmptt.conf-tiedostoon täytyy lisätä hälytyksen OID ja muut tiedot manuaalisesti tai lisätä oikea MiB järjestelmään. Tämän jälkeen systeemi osaa lukea hälytykset oikein.

Jos snmptt.log-tiedostossa on rivejä laitteille, jotka on valvonnassa, voi vika olla joko snmptt.ini-konfiguraatiotiedostossa, väärässä snmptt-versiossa tai net-snmp-perl-paketin puuttumisesta.

Net-snmp-perl-paketin saa asennettu yum install net-snmp-perl -komennolla. Snmptt.ini-tiedostosta kannattaa tarkistaa mode, dns_enable, strip_domain sekä net_snmp_perl_enable. Mode pitäisi olla standalone, dns_enable ja strip_domain omaan ympäristöön sopivat sekä net_snmp_perl_enable arvona 1.

NagiosXi-SNMPTrap-setup.sh-asennuskomentosarja asentaa liian uuden version snmptt:stä, joka hajoittaa SNMP Trappien toimintaa. Komentosarja asentaa version 1.4, kun toimiva versio on snmptt-1.3-3.nagios.noarch. 1.4-version saa poistettua komennolla *yum remove snmptt*. Oikean version saa ladattua osoitteesta:

https://assets.nagios.com/downloads/nagiosxi/packages/snmptt-1.3-3.nagios.noarch.rpm

Asennus tapahtuu komennolla *rpm -ivh snmptt-1.3-3.nagios.noarch.rpm*.

Konfiguraatiotiedostojen muokkausten tai uuden paketin asennuksen jälkeen pitää käynnistää snmptt-prosessi uudestaan *service snmptt restart* -komennolla. Testiympäristössä tämäkään ei tosin auttanut, ja Trappien toimintaan saanti vaati valvontapalvelimen uudelleenkäynnistyksen

5.9 Oracle-tietokannan valvonta

Oraclelle on vakiona kolme ohjattua asennusta: Query, Tablespace sekä Serverspace ja näiden valvonnat vaativat lisenssisyistä erikseen ladattavia lisäosia Nagiokseen. Nämä Oraclen lisäosat löytyvät Oraclen verkkosivuilta http://www.oracle.com/.

Vaadittava osa on Oracle Instant Client, ja se löytyy .rpm-muodossa Linuxia varten. Oman Nagioksen asennuksen Linux-version voi tarkistaa terminaalista *uname -i* -komennolla. x86_64 tarkoittaa 64 bitin käyttöjärjestelmää, ja i?86 tarkoittaa 32 bitin käyttöjärjestelmää.

Kun käyttöjärjestelmän bittisyys on tiedossa, ladataan ensin Nagioksen asennuskomentosarja Oraclea varten komennoilla

cd /tmp
wget http://assets.nagios.com/downloads/general/scripts/oracleinstall.sh

Tämän jälkeen pitää latada erikseen kolme eri .rpm-pakettia:

- Instant Client Package - SQL*Plus: Additional libraries and executable for running SQL*Plus with Instant Client
- Instant Client Package - Basic: All files required to run OCI, OCCI, and JDBC-OCI applications
- Instant Client Package - SDK: Additional header files and an example makefile for developing Oracle applications with Instant Client

Paketit täytyy ladata samaan kansioon, mihin aikaisemmin ladattu komentosarja ladattiin, eli tässä tapauksessa /tmp. Lataaminen onnistuu esimerkiksi *wget*-komennon avulla.

Kun asennuskomentosarja sekä kaikki kolme .rpm-pakettia on ladattu samaan kansioon, ajetaan komentosarja ensin antamalla sille suoritusoikeudet ja sen jälkeen käynnistämällä se seuraavilla komennoilla:

chmod +x oracleinstall.sh
./oracleinstall.sh

Komentosarja kysyy muutaman kerran, annetaanko sen suorittaa kaikki itsenäisesti ja, jos vastataan kyllä, komentosarja suorittaa suurimman osan asennuksesta automaattisesti, mukaanlukien muutamien riippuvaisuuksien lataamisen sekä konfiguroinnin. Asennuksen lopuksi terminaaliin tulee Oraclen muuttujia näkyviin, jotka pitää kopioida talteen seuraavia vaiheita varten. Testiympäristössä muuttujat olivat seuraavat:

ORACLE_HOME=/usr/lib/oracle/12.1/client64
LD_LIBRARY_PATH=/usr/lib/oracle/12.1/client64/lib

Kun asennus on ok, ja muuttujat ovat tiedossa, kirjaudutaan hallintasivustolle takaisin ja mennään yläpalkin Configure-sivustolle. Siirrytään sen jälkeen Core Config Manageriin ja tämän jälkeen vasemmasta laidasta Commands-sivustolle. Laitetaan hakukenttään oracle, jolloin kolme komentoa tulee näkyviin. Seuraavaksi joudutaan yksitellen vaihtamaan polut oikeisiin kaikille kolmelle komennolle. Aloitetaan *check_xi_oraclequery*-komennosta, jota pääsee muokkaamaan sivun oikean laidan ruuvari/jakoavain-ikonin kautta. Command Line -riville vaihdetaan oikeat LD_LIBRARY_PATH sekä ORACLE_HOME. Painetaan “Save”-kuvaketta ja tehdään sama kahdelle muulle komenolle. Kun kaikki kolme on vaihdettu, painetaan komentojen alla olevaa ”Apply Configuration” -kuvaketta.

Kuva 31. Oraclen kolme komentoa

Tämän jälkeen voidaan Oraclen tietokantoja monitoroida ohjattujen asennusten kautta.

Yleisiä ongelmatilanteita voivat olla virheilmoituset:

“install_driver(Oracle) failed: Can't load '/usr/lib/perl5/site_perl/5.8.8/i386-linux-thread-multi/auto/DBD/Oracle/Oracle.so' for module DBD::Oracle: libocci.so.11.1: cannot open shared object file: No such file or directory at /usr/lib/perl5/5.8.8/i386-linux-thread-multi/DynaLoader.pm line 230.”

Tämä johtuu yleensä viallisista muuttujapoluista, joita aikaisemmin muutettiin. Nämä kannattaa varmistaa kirjoitusvirheiden tai esimerkiksi ylimääräisien välilyöntien varalta.

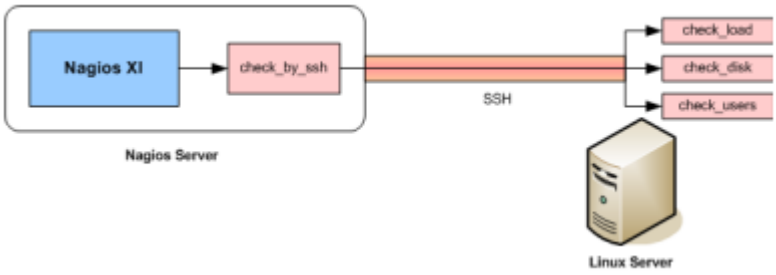
CRITICAL - cannot connect to 192.168.5.55:1521. install_driver(Oracle) failed: Can't locate DBD/Oracle.pm in @INC (@INC contains: /usr/local/nagios/libexec /usr/lib/perl5/site_perl/5.8.8/i386-linux-thread-multi /usr/lib/perl5/site_perl/5.8.8 /usr/lib/perl

Tämä johtuu väärin asennetusta Perl-moduulista. Moduulin saa korjattua komennoilla:

export ORACLE_HOME=<Oraclen asennuskomentosarjan antama ORACLE_HOME -polku>
export LD_LIBRARY_PATH=$ORACLE_HOME/lib
cpan -i DBD::Oracle

5.10 Linux-palvelinten valvonta SSH:n avulla

Linux-palvelinten valvonta SSH:n ylitse suoritetaan tietoturvallisesti SSH-avainten avulla, jolloin kirjautumistunnuksia ei tarvita. Valvonta suoritetaan *check_by_ssh*-komentosarjan avulla, joka pystyy ajamaan tarkistuksia agenttien tapaan ja ilmoittamaan niistä takaisin valvontakoneelle.



Kuva 32. SSH-valvontaa havainnollistava kuva

Itse valvonnan lisääminen aloitetaan kirjautumalla valvontapalvelimelle SSH:n ylitse root-tunnuksella. Tämän jälkeen ajetaan seuraavat komennot:

su nagios
ssh-keygen

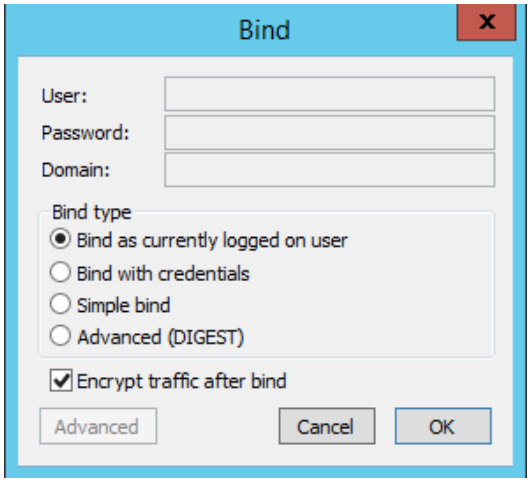
ssh-keygenin kysymyksiin voidaan vain painaa ENTER-näppäintä jolloin tulee oletusasetuksilla. Tämä generoi ja tallentaa julkisen sekä yksityisen avaimen /home/nagios/.ssh-polun alle. Kun kyseiset avaimet on generoitu, kirjaudutaan seuraavaksi valvottavalle koneelle SSH:lla. Luodaan koneelle uusi käyttäjä Nagios komennolla *adduser Nagios* ja vaihdetaan sen salasana komennolla *passwd Nagios*. Kun käyttäjä on luotu, siirrytään takaisin valvontakoneelle ja annetaan komento *ssh-copy-id nagios@<valvontapalvelimen nimi tai IP>*. Komento kysyy valvottavan koneen nagios-tunnuksen salasanaa ja varoittaa RSA-avaimen sormenjäljestä. Tämä siirtää aikaisemmin luodun avaimen valvottavalle koneelle. Tämän jälkeen voidaan testata toimintaa ajamalla esimerkiksi komento */usr/local/nagios/libexec/check_by_ssh -H <valvottavan koneen nimi tai IP> -C uptime*.

17:51:40 up 1:08, 4 users, load average: 2.09, 0.65, 0.26

Terminaalin pitäisi antaa vastaus ylläolevan esimerkin mukaisesti. Tämän jälkeen voidaan siirtyä hallintasivustolle, josta voidaan ohjatun asennuksen kautta lisätä kone valvontaan. Haluttu ohjattu asennus on nimeltään *SSH Proxy*.

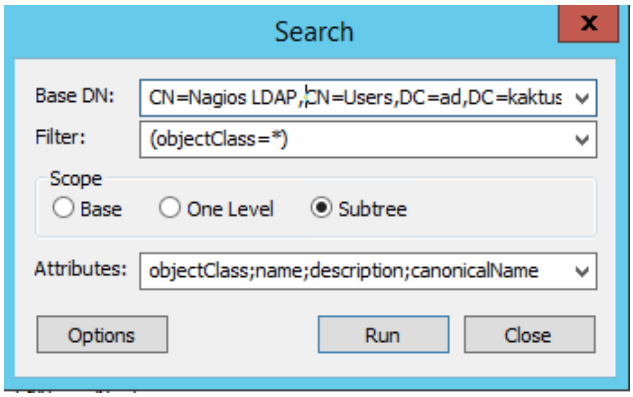
5.11 Active Directoryn valvonta

Active Directoryn valvonta luonnistuu LDAP-protokollan avulla. Tällä voidaan varmistaa, että kirjautuminen ja autentikointi Active Directoryn kautta toimii. Valvontaa varten kannattaa active directoryyn luoda uusi tunnus, jolla ei ole oikeuksia ”Domain Users” -ryhmää enempää. Tunnukselle kannattaa asettaa luodessa asetukset, että salasana ei vanhene koskaan ja ettei sitä pysty vaihtamaan. Oikea polku ja tiedot tunnukseen on hyvä tarkistaa, ja se luonnistuu seuraavalla tavalla. Kun tunnus on luotu, avataan domain controllerilla LDP-ohjelma. Yläpalkista valitaan Connection→Bind ja kirjaudutaan nykyisellä tunnuksella.



Kuva 33. LDAP Bindin avaus

Kun yhteys on avattu, avataan Browse→Search -kenttä näkyviin. Base DN-kenttään kirjoitetaan domainin tiedot sekä ”polku” käyttäjätunnuksen sijaintiin. Testiympäristössä käyttäjä on nimeltään Nagios LDAP, ja se sijaitsi Users-OU:ssa. Domain controllerin nimi on AD ja domain kaktusritari.fi.



Kuva 34. Haun asetukset testiympäristössä

Haun pitäisi löytää tunnus, mitä hakukentässä ilmoitettiin. Jos tunnusta ei jostain syystä löydy, kannattaa tarkistaa hakukriteerit kirjoitusvirheiden varalta.

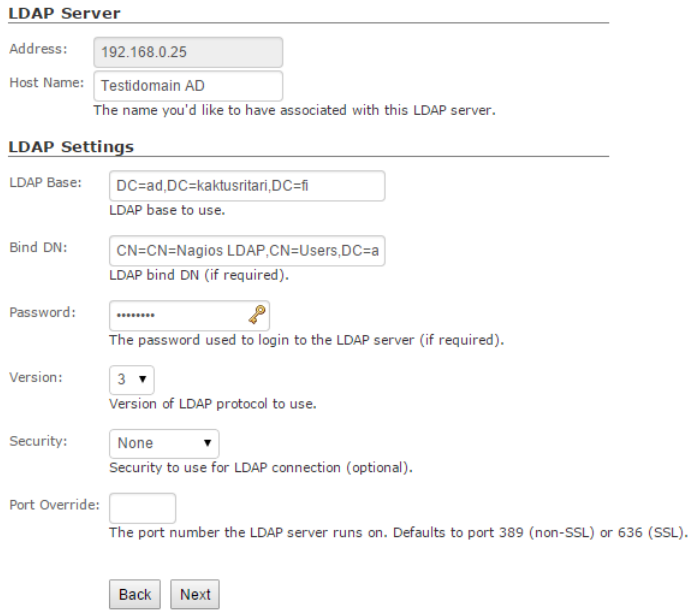
```
----------
***Searching...
ldap_search_s(ld, "CN=Nagios LDAP,CN=Users,DC=ad,DC=kaktusritari,DC=fi", 2, "(objectClass=*)", attrList,  0, &msg)
Getting 1 entries:
Dn: CN=Nagios LDAP,CN=Users,DC=ad,DC=kaktusritari,DC=fi
      name: Nagios LDAP;
      objectClass (4): top; person; organizationalPerson; user;

----------
```

Kuva 35. Onnistunut haku

Ylläolevasta hakutuloksesta saadaan selville, että tunnus löytyy moitteetta ja voidaan siirtyä hallintasivustolle lisäämään palvelu valvontaan. Tämä onnistuu ohjatun asennuksen kautta, ja haluttu palvelu on LDAP Server.

LDAP Base -kenttään annetaan toimialueen tiedot

Bind DN -kenttään annetaan valvontaan käytettävän tunnuksen ”polku”. Salasana-kenttään annetaan kyseisen tunnuksen salasana ja versioksi on suositeltavaa laittaa 3, jollei kyseessä ole pelkästään vanhaa LDAP-versiota tukeva domain controller. Valvontaa varten voidaan määrittää SSL-salaus, joka ei vaadi erityisiä muutoksia asennuksen yhteydessä. Iso määrä SSL-salauksia voi tosin kuormittaa palvelimia niiden vaatiman salauksenpurun vuoksi.



Kuva 36. LDAP Server -valvonnan vaatimat asetukset

5.12 Valvontahälytyksien muokkaaminen ja ajastaminen

Joskus on tarpeen ajastaa tai mahdollistaa hälytysten saaminen esimerkiksi pelkästään toimistotyöaikoina. Nagioksesta voi erikseen säätää jopa jokaiselle palvelulle tai laitteelle omat hälytysajat, jolloin sähköposteja ja/tai tekstiviestejä lähetetään.

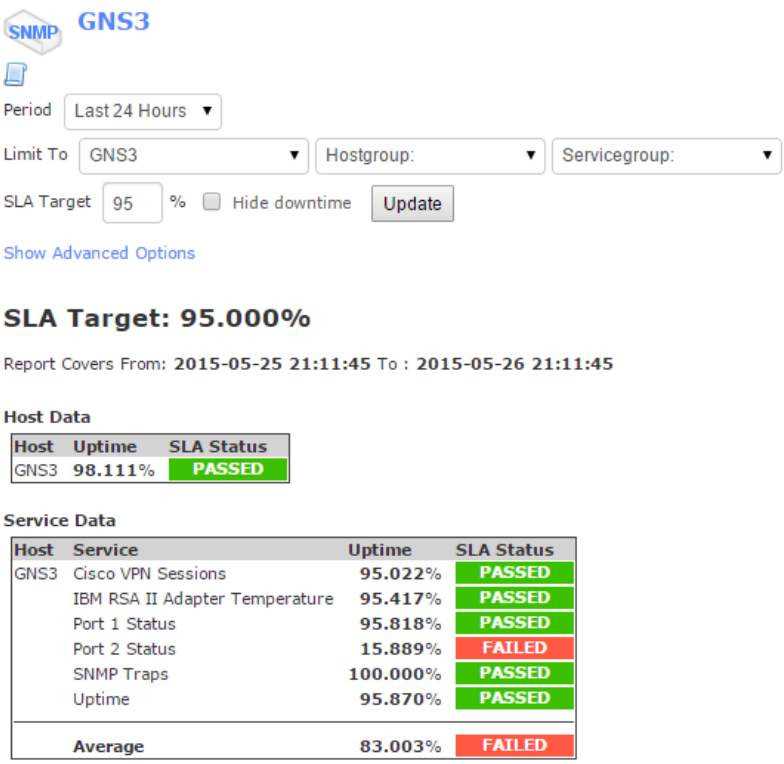
Hälytysten hallinta löytyy Admin→Notification Management -polun alta.

Hälytysten hallintasivulta voidaan luoda pohjia eri hälytyksille. Esimerkkinä tietyille palveluille voidaan määrittää omat henkilöt, joille hälytys lähtee ja milloin se lähtee. Samoin sähköposti- ja tekstiviestipohjaa pystyy muokkaamaan.

Kun haluttu pohja on luotu tietyillä asetuksilla, voidaan sitä käyttää määrittämään käyttäjille asetukset. Jos halutaan tietylle ryhmälle tiettyyn aikaan hälytyksiä, suositeltavaa on luoda käyttäjäryhmä, lisätä siihen halutut käyttäjät ja tälle ryhmälle hälytyspohjan avulla luoda aikarajat ja lisätä käyttäjäryhmä hälytyksien saajaksi palveluita laitettaessa valvontaan.

5.13 Raporttien generointi

Raporttien luontiin pääsee ylälaidan suunnistuspalkin ”Reports”-linkin kautta. Vasemmasta laidasta löytyy useita erilaisia raportteja, joista yksi tärkeä on SLA Report. Tällä saadaan esimerkiksi asiakkaalle annettua tiedot, miten palvelut ovat pysyneet pystyssä. Raportteja voidaan ajaa eri laiteryhmille, palveluryhmille tai yksittäisille laitteille. Raportit saa myös ajastettua, lähetettyä sähköpostilla tai tallennettua PDF-muodossa sivun oikeasta laidasta raportin ollessa auki.

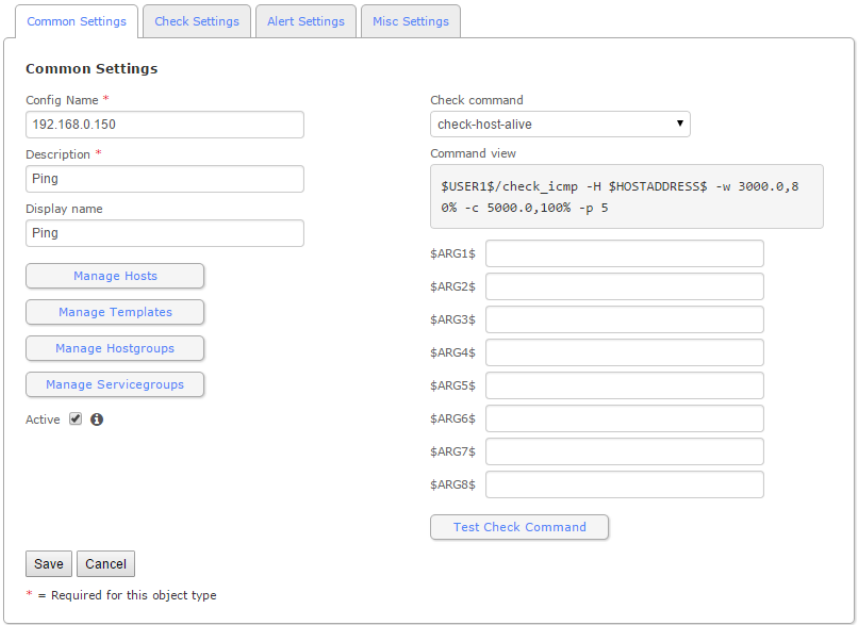


Kuva 37. SLA-raporttien luonti

5.14 Palveluiden lisääminen jo valvottavaan kohteeseen

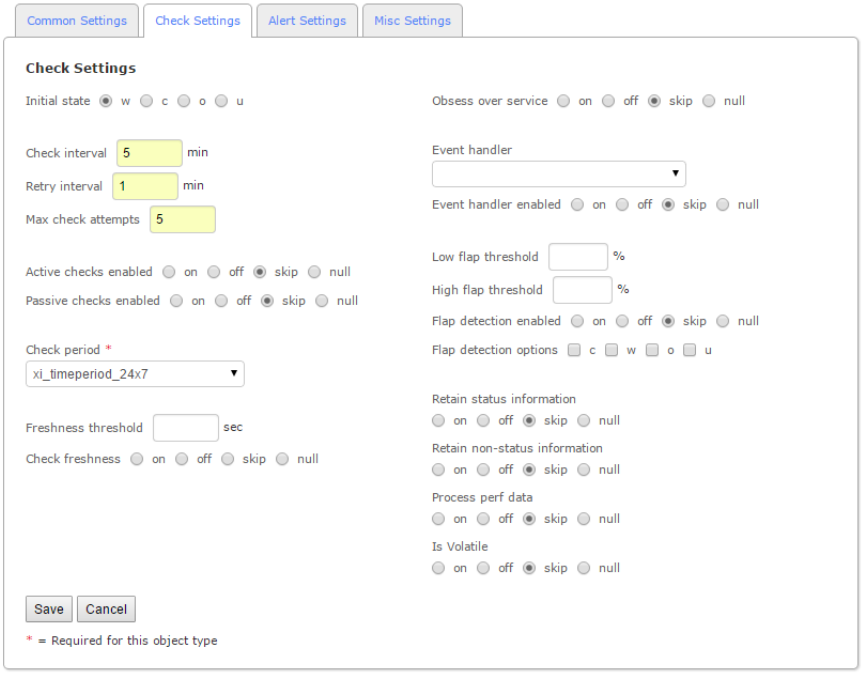
Jos tulee tarve lisätä tai poistaa valvottavia palveluita tietystä kohteesta, voidaan tämä hoitaa Core Config Managerin kautta. CCM:n vasemmassa laidassa on ”Services”-linkki, jota kautta pääsee katsomaan tämänhetkiset valvotut palvelut. Alalaidassa on ”Add New” -linkki. Lisätään haluttu komento, Config Nameksi voidaan lisätä oma nimi konfiguraatiolle, ja Description on nimi joka valvontanäkymässä tulee näkymään.

Valitaan Manage Hosts -ikkuna ja valitaan listasta laitteet, joihin uusi palvelu halutaan lisätä.



Kuva 38. Uuden palveluvalvonnan lisäys

Kun komento, sen argumentit ja nimet on laitettu, mennään Check Settings -välilehdelle. Voidaan vakiona laittaa suurimmalle osalle vaihtoehdoista skip, sillä nämä vaihtoehdot tulevat muualta. Check periodiin voidaan valita xi_timeperiod_24x7, joka on vakiona Nagios XI:ssä.



Kuva 39. Check Settings -välilehden asetukset

Lähteet

1 NRPE Documentation. 2007. <http://nagios.sourceforge.net/docs/nrpe/NRPE.pdf> Luettu 10.05.2015.

2 NDOUTILS Documentation. 2007. <http://nagios.source-forge.net/docs/ndoutils/NDOUtils.pdf> Luettu 10.05.2015.

3 About RRD. 30.09.2014. <http://oss.oetiker.ch/rrdtool/> Luettu 16.05.2015.

4 NDOUtils Database Model. 29.08.2007. <http://nagios.source-forge.net/docs/ndoutils/NDOUtils_DB_Model.pdf> Luettu 10.05.2015.

5 Nagios XI – Introduction to Event Handlers. 2014. <https://assets.nagios.com/downloads/nagiosxi/docs/Introduction-To-Event-Handlers-in-Nagios-XI.pdf> Päivitetty 01.10.2015. Luettu 20.05.2015.

6 Determining Status and Reachability of Network Hosts <http://nagios.source-forge.net/docs/3_0/networkreachability.html> Luettu 5.2015

7 PNP 4 Nagios Documentation.30.07.2014. <http://docs.pnp4nagios.org/> Luettu 25.05.2015.

8 NSCA – Nagios Service Check Acceptor. 04.11.2011. <https://exchange.nagios.org/directory/Addons/Passive-Checks/NSCA--2D-Nagios-Service-Check-Acceptor/details> Luettu 30.04.2015.

9 Nagios XI – How to use the NSCA Addon. 2014 <https://assets.nagios.com/downloads/nagiosxi/docs/Using-and-Configuring-NSCA-With-Nagios-XI.pdf> Päivitetty 10.10.2015. Luettu 10.04.2015.

10 Nagios XI – How to monitor devices using the NCPA Agent and Wizard. 2014. <https://assets.nagios.com/downloads/nagiosxi/docs/Monitoring-Devices-Using-The-NCPA-Agent-And-Nagios-XI.pdf> Päivitetty 01.10.2015. Luettu 13.04.2015.

11 NCPA – Agent Installation Instructions. 2014. <https://assets.nagios.com/down-loads/ncpa/docs/Installing_NCPA.pdf> Päivitetty 01.10.2015. Luettu 01.04.2015.

12 Centos 7 – open firewall port. 2014. <http://stackoverflow.com/ques-tions/24729024/centos-7-open-firewall-port> Luettu 20.05.2015.

13 Nagios Remote Data Sender (NRDS). <https://exchange.nagios.org/directory/Addons/Components/Nagios-Remote-Data-Sender-(NRDS)/details?utm_source=Nagios%2520Labs&utm_medium=Text%2520Link&

utm_content=How%2520To%2520Passively%2520Monitor%2520Linux%2520Machines%2520With%2520NRDS%2520&%2520Nagios%2520XI&utm_campaign=Nagios%2520XI> Luettu 15.04.2015.

14 Nagios XI – How to integrate SNMP Traps with Nagiox XI. 2015. <https://assets.nagios.com/downloads/nagiosxi/docs/Integrating_SNMP_Traps_With_Nagios_XI.pdf> Luettu 25.05.2015.

15 Dell OpenManage Nagios XI Wizard. 05.06.2015. <https://exchange.nagios.org/directory/Addons/Configuration/Configuration-Wizards/Dell-OpenManage-Nagios-XI-Wizard/details> Luettu 15.05.2015.

16 Connect: Network is Unreachable. 16.01.2006. <https://www.how-toforge.com/community/threads/connect-network-is-unreachable.2098/> Luettu 18.05.2015.

17 Nagios XI- Monitoring Hosts using SSH. 2015. <https://assets.nagios.com/downloads/nagiosxi/docs/Monitoring_Hosts_Using_SSH.pdf> Luettu 13.05.2015.

18 Nagios XI – How to Install & Configure the Oracle Client & Plugins. 2015. <https://assets.nagios.com/downloads/nagiosxi/docs/Installing-Oracle-Plugins-in-Nagios-XI.pdf> Luettu 10.05.2015.

19 Nagios XI – Monitor Active Directory with LDAP. 2015. <https://assets.nagios.com/downloads/nagiosxi/docs/Monitoring_Active_Directory_with_LDAP.pdf> Luettu 20.05.2015.

20 SNMP Configuration Guide. 2013. <http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/snmp/configuration/xe-3se/3850/snmp-xe-3se-3850-book/nm-snmp-snmpv3.html> Luettu 25.05.2015.

21 Receiving SNMP Traps in Nagios. 22.12.2010. <http://askaralikhan.blogspot.fi/2010/12/receiving-snmp-traps-in-nagios.html> Luettu 17.05.2015.

22 Nagios – Agent Comparison. 2014. <https://assets.nagios.com/downloads/ncpa/docs/NCPA-Agent-Comparison.pdf> Luettu 10.05.2015.

23 SNMP Traps are not getting reported, “Waiting for trap”. 24.01.2013 <http://support.nagios.com/forum/viewtopic.php?f=16&t=9034> Luettu 26.05.2015.