HRVATSKA AKADEMSKA I ISTRAŽIVAČKA MREŽA
CROATIAN ACADEMIC AND RESEARCH NETWORK

Analiza MonitorWare programskog paketa

CCERT-PUBDOC-2003-04-16

CARNet CERT u suradnji s LS&S

Sigurnosni problemi u računalnim programima i operativnim sustavima područje je na kojem CARNet CERT kontinuirano radi.

Rezultat toga rada ovaj je dokument koji je nastao suradnjom CARNet CERT-a i LS&S-a, a za koji se nadamo se da će Vam koristiti u poboljšanju sigurnosti Vašeg sustava.

CARNet CERT, www.cert.hr - nacionalno središte za **sigurnost računalnih mreža** i sustava.

LS&S, www.lss.hr - laboratorij za sustave i signale pri Zavodu za elektroničke sustave i obradbu informacija Fakulteta elektrotehnike i računarstva Sveučilišta u Zagrebu.

Sadržaj

1. Uvod

MonitorWare je programski alat namijenjen kontinuiranom praćenju sustava i pravodobnom obavještavanju mrežnih administratora o svim važnim događajima u sustavu. Osnova MonitorWare programskog paketa je MonitorWare Agent, program zadužen za prikupljanje i obavještavanje sistemskih administratora o događajima na sustavu u realnom vremenu.
MonitorWare Agent pokreće se na sustavu koji treba pratiti. Nakon što je pokrenut, agent prikuplja podatke iz različitih izvora kao što su Windows Event Log, Syslog ili tekstualne datoteke. Prikupljene informacije se filtriraju i na temelju unaprijed definiranih pravila se određuje što treba napraviti u slučaju pojave nekog događaja. Događaj može biti zanemaren, može se poduzeti neka akcija u slučaju njegove pojave, ili može biti proslijeđen dalje (npr. na udaljeni Syslog poslužitelj ili na drugi MonitorWare Agent).
U većim okruženjima svi prikupljeni podaci mogu se pohranjivati u centralni repozitorij koji može biti u obliku SQL baze podataka ili log datoteka u koje se upisuju događaji prikupljeni na lokalnoj mreži. Bazu podataka i log datoteke koriste ostali programi iz MonitorWare skupa alata koji dodaju funkcionalnosti kao što su praćenje događaja na cijeloj mreži u realnom vremenu, generiranje izvještaja i slično.
Neke od mogućnosti MonitorWare Agent-a su:

- praćenje svih događanja na Windows operacijskom sustavu – MonitorWare Agent konstantno prati Windows log datoteke (engl. *Windows Event Logs*) i log datoteke svih aplikacija koje imaju podršku za logiranje događaja u tekstualne datoteke.
- praćenje rada računala i poslužitelja u lokalnoj mreži – MonitorWare Agent koristi ping i port *probe* kako bi utvrdio da li je neko računalo u lokalnoj mreži 'živo' ili mrežni servis pokrenut. Ako neko računalo (ili mrežni servis) nije dostupno, MonitorWare Agent će to detektirati i po potrebi generirati upozorenje.
- praćenje rada Windows servisa – MonitorWare Agent može detektirati prestanak rada nekog Windows servisa i generirati upozorenje ili izvršiti neku korektivnu radnju na računalu (npr. ponovno pokretanje servisa).
- praćenje slobodnog prostora na tvrdom disku – u slučaju da se zapuni tvrdi disk na računalu, MonitorWare Agent može generirati upozorenje ili osloboditi prostor na disku (npr. brisanjem datoteka iz `Tmp` direktorija i slično).
- podrška za Syslog – MonitorWare Agent može pratiti događaje koji su zabilježeni pomoću Syslog poslužitelja pokrenutog na računalu tako da se mogu pratiti sva događanja na cjelokupnoj računalnoj mreži.
- pohranjivanje događaja – svi događaji koje prati MonitorWare Agent mogu biti trajno pohranjeni u SQL bazu podataka ili u tekstualnu datoteku.
- generiranje upozorenja – upozorenja o neregularnim događanjima mogu biti poslana ili pomoću elektroničke pošte ili pomoću Syslog poslužitelja.

Komponente koje dolaze u osnovnom MonitorWare paketu su:

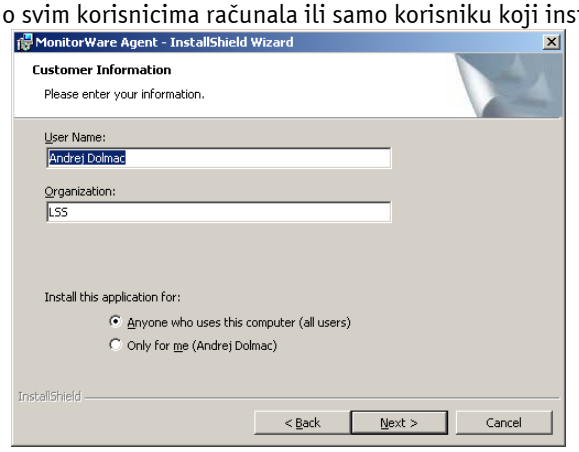
- MonitorWare Agent – osnova MonitorWare programskog paketa. Zadužen je za prikupljanje informacija. Nakon instalacije, ovaj program se na računalu pokreće kao klasični Windows servis.
- MonitorWare Configuration Client – namijenjen je za podešavanje svih opcija MonitorWare Agent-a.
- Interactive Syslog Server – Windows Syslog poslužitelj koji dolazi standardno s MonitorWare programskim paketom.
- MonitorWare Web Access – pomoću njega je pristup prikupljenim podacima omogućen i preko Web sučelja. Program dolazi standardno s MonitorWare paketom i automatski se instalira na računalo ako je na njemu pokrenut Microsoft-ov IIS Web poslužitelj.

MonitorWare programski paket moguće je instalirati na Windows NT 4.0, Windows 2000 i Windows XP operativnim sustavima.

2. Instalacija

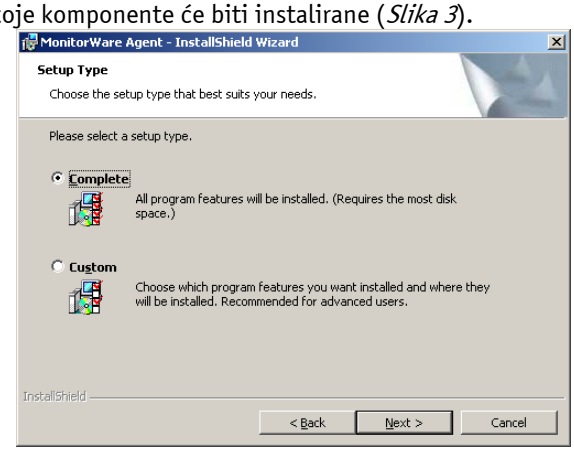
Instalacija programa vrlo je jednostavna. Nakon raspakiranja zip arhive u kojoj je MonitorWare programski paket, potrebno je pokrenuti izvršnu datoteku `Setup.exe` nakon čega se ostatak instalacije izvršava automatski.

Prilikom instalacije potrebno je unijeti neke osnovne korisničke podatke i odabrati da li će korištenje programa biti omogućeno svim korisnicima računala ili samo korisniku koji instalira program (Slika 1).

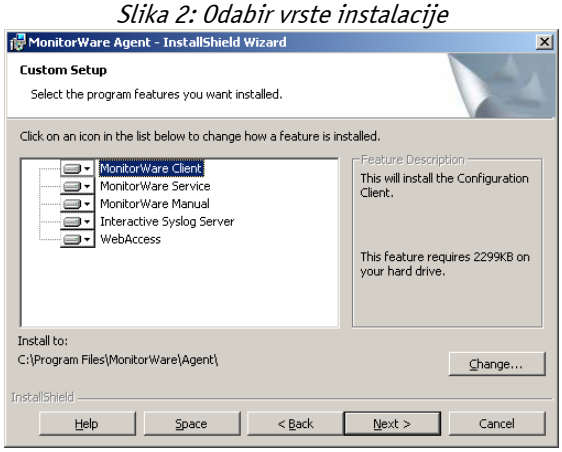


Slika 1: Postupak instalacije MonitorWare paketa

Tokom instalacije moguće je odabrati hoće li se instalirati svi programi iz MonitorWare paketa ili samo pojedine komponente (*Slika 2*). U slučaju da se odabere instalacija samo pojedinih komponenti, potrebno je selektirati koje komponente će biti instalirane (*Slika 3*).



Slika 2: Odabir vrste instalacije



Slika 3: Odabir komponenti koje će biti instalirane

3. Uobičajene primjene MonitorWare paketa

MonitorWare Agent može obavljati sljedeće funkcije:

- prikupljanje podataka o događajima na lokalnom računalu i u mreži,
- generiranje upozorenja u realnom vremenu,
- automatske administrativne akcije u slučaju neregularnih pojava,
- pohrana prikupljenih podataka u lokalni repozitorij.

Navedene funkcije mogu se međusobno kombinirati, ovisno o potrebama i namjeni za koju je program instaliran. Nakon instalacije u programu su onemogućene sve navedene funkcije i prije pokretanja programa potrebno ga je konfigurirati tako da obavlja ono što korisnik želi.

Neke standardne primjene MonitorWare programa su:

- analiza događanja u mreži,
- pohrana informacija o događanjima u mreži,
- obavještavanje o neregularnim aktivnostima u mreži,
- pomoć pri rješavanju problema.

3.1. Analiza događanja u mreži

MonitorWare Agent sam po sebi posjeduje funkcionalnost za prikupljanje podataka o događanjima na lokalnom računalu i u računalnoj mreži, ali ne posjeduje funkcije za analizu prikupljenih podataka, tako da je za to potrebno koristiti druge programske pakete. Isto tako, MonitorWare Agent se može koristiti za integraciju podataka o događanjima na Windows operacijskim sustavima s Linux/UNIX sustavima za prikupljanje podataka koji su pretežno bazirani na korištenju Syslog poslužitelja.

Na sljedećoj slici (*Slika 4*) je prikazan shematski prikaz praćenja događanja na mreži baziranoj na Windows operacijskom sustavu. Na svim Windows baziranim računalima u mreži je instaliran MonitorWare Agent koji se konfigurira tako da sve događaje s lokalnog računala prosljeđuje na centralno računalo na kojem je centralni MonitorWare Agent. Centralni MonitorWare Agent prikuplja sve podatke i pohranjuje ih u lokalni repozitorij (SQL baza podataka ili log datoteke). Obavijesti o neregularnim događanjima u mreži prosljeđuju se dalje putem poruka elektroničke pošte, dok je pristup svim podacima koji se nalaze u centralnom repozitoriju omogućen preko Web sučelja.

Slika 4: Centralizirano prikupljanje podataka o događanjima u Windows baziranoj mreži

Slika 5 prikazuje prosljeđivanje podataka s računala baziranih na Windows operativnom sustavu na Linux/UNIX Syslog poslužitelj. Na svim Windows računalima instalirani su MonitorWare agenti, konfigurirani tako da sve prikupljene podatke samo prosljeđuju dalje na udaljeni Syslog poslužitelj. Time je ostvareno integrirano prikupljanje podataka i s Windows i s Linux/UNIX računala. Na taj se način mogu centralizirano pratiti događanja na cjelokupnoj računalnoj mreži.

Slika 5: Prosljeđivanje podataka s Windows baziranih računala na Linux/UNIX Syslog poslužitelj

MonitorWare paket može se koristiti isključivo za prikupljanje podataka, dok se za pregledavanje i obradu podataka mogu koristiti neki drugi programski paketi (najčešće su to skripte prilagođene potrebama određenog korisnika). U tom slučaju se MonitorWare Agent koristi samo za stvaranje lokalnog repozitorija podataka (SQL baza podataka ili tekstualne log datoteke).

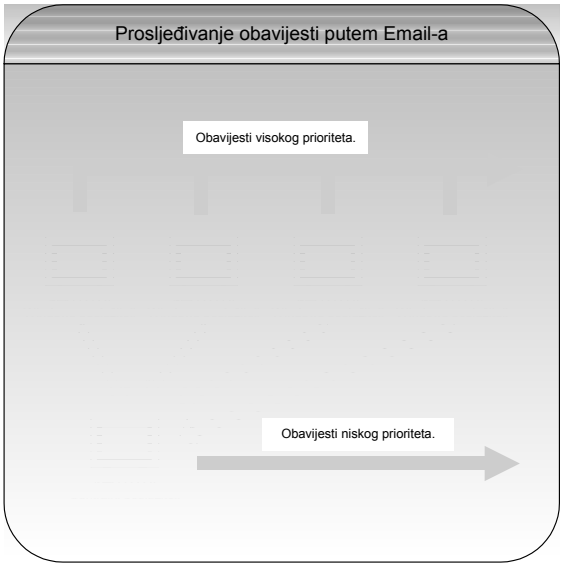
3.2. Obavijesti o neregularnim aktivnostima

Svaki MonitorWare Agent instaliran na računalnoj mreži može generirati obavijesti o neregularnim aktivnostima ili pojavi nekog specifičnog događaja. Isto tako, mreža se može konfigurirati tako da se sve obavijesti šalju na centralni MonitorWare Agent, koji onda porukom elektroničke pošte ili nekim drugim putem prosljeđuje te obavijesti administratoru sustava. Ova dva načina obavještavanja se mogu i kombinirati.

Prednost direktnog slanja obavijesti, bez posredovanja centralnog MonitorWare Agenta, je brzina obavještavanja. Poruka o neregularnoj aktivnosti ili događaju biti će poslana administratoru istog trena kad je detektirana. Prilikom ovog načina obavještavanja nema posrednika i stoga nema opasnosti da posrednik zakaže (npr. da nije dostupan centralni MonitorWare Agent). S druge strane, u tom slučaju je potrebno svaki pojedinačni MonitorWare Agent u lokalnoj mreži konfigurirati zasebno. To može biti dosta vremenski zahtjevno za veće mreže i povećava kompleksnost administriranja.

Prednost centraliziranog slanja obavijesti je jednostavnost administracije, ali u slučaju da neka instanca MonitorWare Agenta iz nekih razloga ne može proslijediti poruke centralnom MonitorWare Agentu ili je isti nedostupan, poruke uopće neće biti generirane.

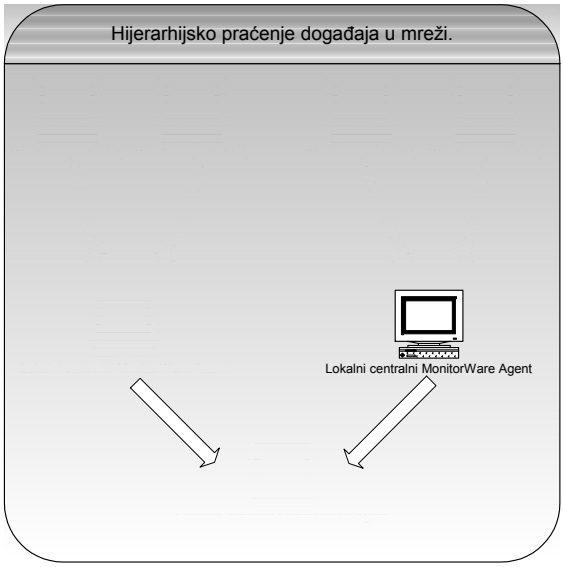
Najbolje rješenje je konfigurirati MonitorWare agente tako da se hitne poruke šalju direktno, a poruke s manjim prioritetom prosljeđuju na centralni MonitorWare Agent. Na sljedećoj slici (*Slika 6*) je prikazana takva konfiguracija sustava.



Slika 6: Obavještavanje o događanjima putem poruka elektroničke pošte

3.3. Hijerarhijski ustroj praćenja događanja u mreži

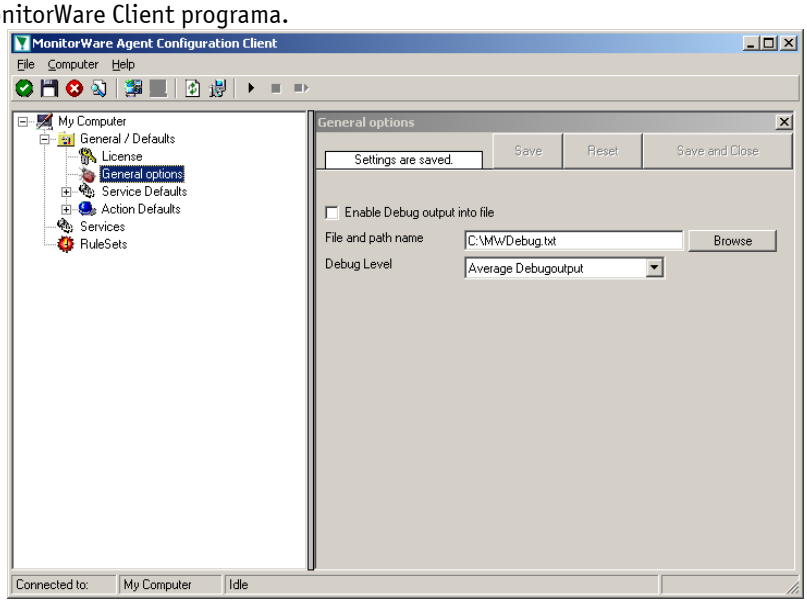
U velikim i kompleksnim sustavima i mrežama moguće je uspostaviti hijerarhijsko praćenje događanja na mreži i obavještavanje o neregularnim aktivnostima. U tom se slučaju koristi više lokalnih centralnih MonitorWare Agent-a od kojih je svaki zadužen za dio računala u mreži. Svako računalo u mreži prosljeđuje podatke o svojim aktivnostima na svoj lokalni centralni MonitorWare Agent. Nakon toga se određeni podaci sa lokalnih centralnih MonitorWare Agent-a mogu proslijediti na jedan globalni MonitorWare Agent na kojem se zatim mogu pratiti sva događanja na računalnoj mreži. Prednosti ovakve konfiguracije su lakše administriranje i manje opterećenje globalnog MonitorWare Agenta na koji se prosljeđuju samo najvažniji podaci. Na lokalnim centralnim MonitorWare Agent-ima se mogu pratiti događanja samo na dijelu mreže za koji je taj agent zadužen što uvelike olakšava odvojeno praćenje različitih dijelova mreže. Shema takve konfiguracije prikazana je na sljedećoj slici (*Slika 7*).



Slika 7: Hijerarhijsko praćenje događanja u mreži

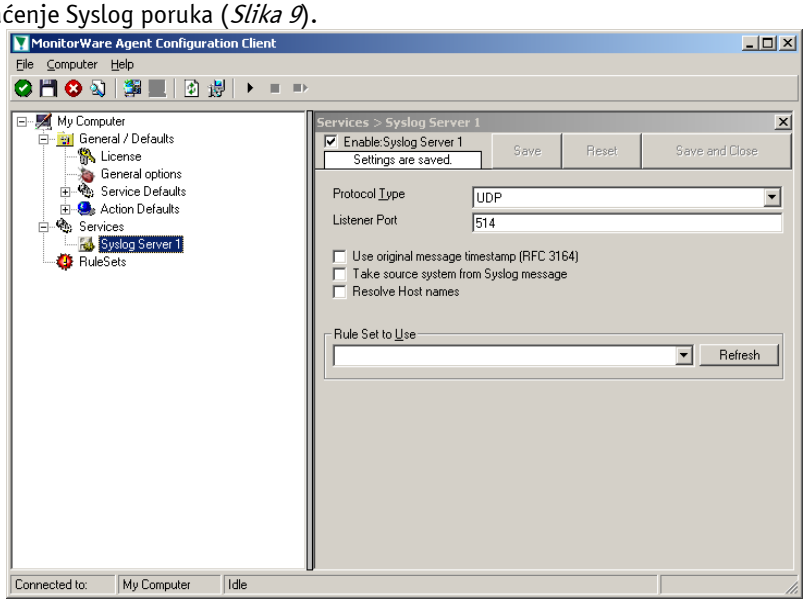
4. Konfiguracija MonitorWare Agent-a

Nakon instalacije MonitorWare Agent-a na računalo potrebno ga je konfigurirati tako da obavlja željene funkcije (prikupljanje podataka o događajima i pohranjivanje ili prosljeđivanje istih). Konfiguracija MonitorWare Agent-a obavlja se pomoću klijentske aplikacije MonitorWare Client. Sučelje MonitorWare Client programa prikazano je na sljedećoj slici (*Slika 8*). Inicijalno, nakon instalacije, je MonitorWare Agent konfiguriran tako da ne obavlja nikakav koristan posao i prije pokretanja programa potrebno je uključiti željene servise. U nastavku je naveden kratki prikaz korištenja MonitorWare Client programa.



Slika 8: Sučelje MonitorWare Client programa.

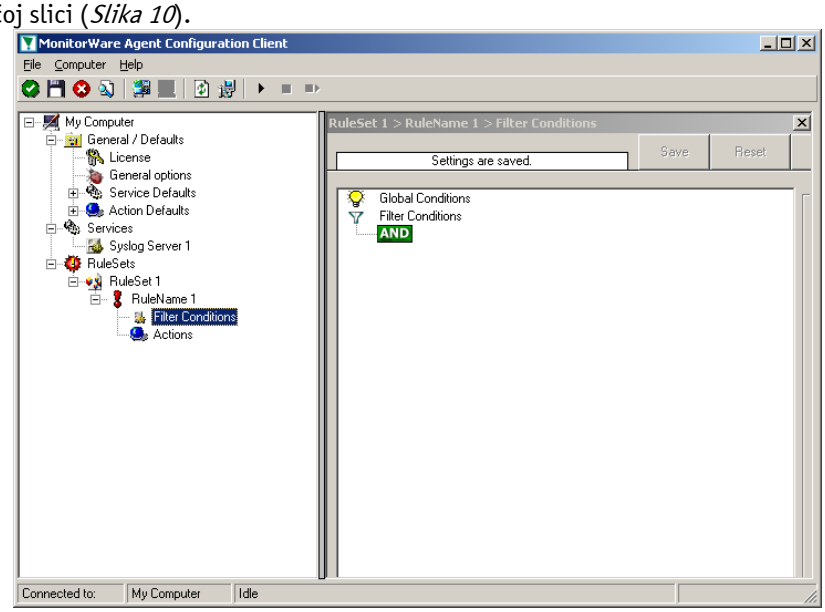
Za početak je potrebno uključiti servise koje će MonitorWare Agent pratiti. To može biti primanje Syslog poruka, praćenje Windows log datoteka ili nekih drugih tekstualnih datoteka, *Ping Probe*, *Port Probe* i slično. Uključivanje servisa obavlja se desnim klikom miša na karticu **Services** u lijevom dijelu prozora i odabirom opcije **Add Service**. Slika prikazuje izgled MonitorWare Client prozora nakon što je uključeno praćenje Syslog poruka (*Slika 9*).



Slika 9: Uključivanje praćenja Syslog poruka

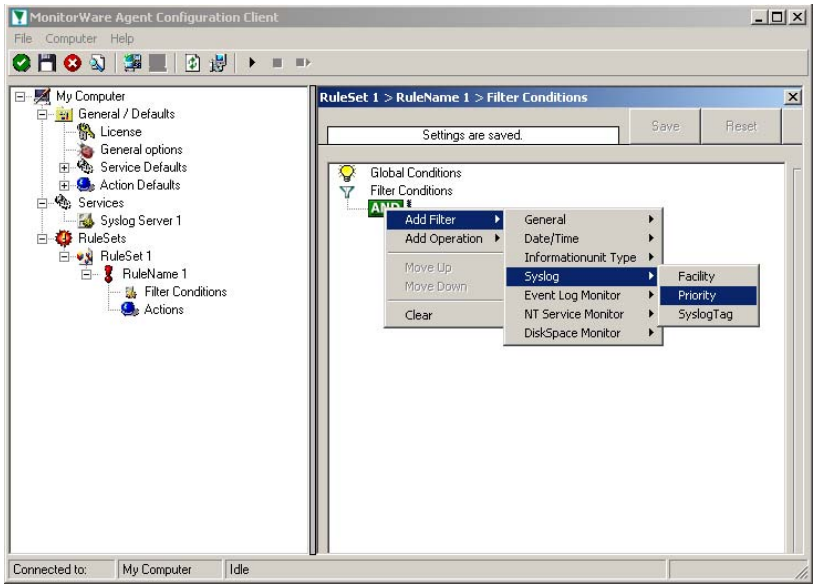
U desnom dijelu prozora nalaze se opcije kojima se konfiguriraju parametri servisa koji se uključuje. U prikazanom primjeru za primanje Syslog poruka moguće je odabrati koji će se protokol koristiti za primanje poruka, na kojem portu će se slušati poruke i slično. Parametri koji se ovdje nalaze ovise o

servisu koji se uključuje, tako da će za druge servise (npr. praćenje tekstualne datoteke) ovi parametri biti drugačiji.
Nakon što su definirani servisi koji će biti uključeni, potrebno je definirati pravila za filtriranje koja će biti primijenjena na podacima koji se prikupljaju. Sustav za filtriranje može se podesiti tako da se nebitne informacije zanemaruju, neke manje bitne samo zapisuju u repozitorij dok se za važne događaje generiraju obavijesti putem elektroničke pošte. Isto tako, pomoću filtara se određuje hoće li se i koji će se podaci proslijediti na centralni MonitorWare Agent (ako takav postoji). Koji podaci će se prikupljati i što će se s njima raditi ovisi isključivo o korisniku.
Novi skup pravila, koji će se primjenjivati na određeni servis, dodaje se desnim klikom miša na karticu **RuleSets** u lijevom dijelu prozora i odabirom opcije **Add RuleSet**. Nakon što se stvori novi skup pravila za filtriranje podataka određenog servisa, u njega se proizvoljno mogu dodavati pravila za filtriranje. Nova pravila se dodaju desnim klikom miša na ime novog skupa pravila i odabirom opcije **Rules -> Add Rule**. Izgled ekrana nakon dodavanja novog skupa pravila i dodavanja jednog pravila u njega prikazan je na sljedećoj slici (*Slika 10*).



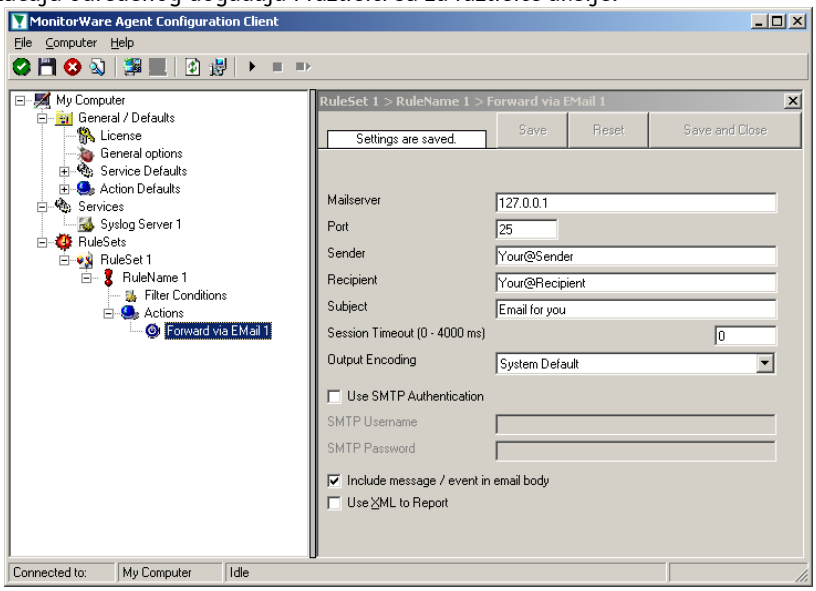
Slika 10: Primjer dodavanja pravila za filtriranje prikupljenih podataka

Za svako novo pravilo potrebno je definirati dvije stvari. Prvo je potrebno definirati parametre na temelju kojih će se selektirati samo određeni podaci iz svih primljenih podataka. To se postiže odabirom kartice **Filter Conditions** ispod imena novog pravila. Nakon toga se u desnom dijelu MonitorWare Client programa mogu podesiti parametri za filtriranje prikupljenih podataka. Desnim klikom miša otvara se meni u kojem je moguće dodavati nove uvijete za filtriranje ili logičke operacije koje će biti primijenjene na tim uvjetima (*Slika 11*). Uvjeti za filtriranje mogu biti vrlo jednostavni ali mogu biti i kompleksni. Podatke se može filtrirati po samom sadržaju, vremenu kad su primljeni, u ovisnosti o računalu ili servisu s kojeg su pristigli i slično. Nad uvjetima za filtriranje se mogu primijeniti logičke operacije (AND, OR, XOR itd.) što pruža dodatne mogućnosti za profinjeno filtriranje prikupljenih podataka.



Slika 11: Podešavanje uvjeta za filtriranje

Druga stvar koju je potrebno definirati za novo pravilo je akcija koja će se poduzeti u slučaju da se pojavi događaj koji odgovara uvjetima za filtriranje. Akcija koja će biti poduzeta odabire se desnim klikom miša na karticu **Actions** u lijevom dijelu ekrana i odabirom opcije **Add Action**. Nakon toga je potrebno odabrati određenu akciju iz liste ponuđenih. U slučaju pojave određenog događaja informacija o tome se može zapisati u bazu podataka, tekstualnu datoteku ili *Windows Event Log*. Isto tako, moguće je tu informaciju proslijediti udaljenom Syslog poslužitelju ili MonitorWare Agent-u, obavijestiti administratora putem Email ili Net Send poruke, a postoji i mogućnost pokretanja nekog programa na lokalnom računalu. Nakon što je odabrana željena akcija, potrebno je podesiti njene parametre. Podešavanje parametara za određenu akciju obavlja se u desnom dijelu MonitorWare Client prozora. *Slika 12* prikazuje parametre koje je potrebno podesiti za slanje obavijesti administratoru putem poruke elektroničke pošte. Parametri koje je potrebno podesiti ovise o akciji koja će biti poduzeta u slučaju određenog događaja i različiti su za različite akcije.



Slika 12: Podešavanje parametara za slanje obavijesti putem poruke elektroničke pošte

Prilikom definiranja pravila treba voditi računa o tome da se pravila za manipulaciju prikupljenim podacima primjenjuju slijedno od prvog prema zadnjem. Na svaki novi podatak program pokušava primijeniti prvo pravilo za filtriranje. Ako se na njega ne mogu primijeniti uvjeti za filtriranje definirani u prvom pravilu, program prelazi na sljedeće i tako sve dok ne dođe do pravila koje odgovara tom podatku. Nakon što je program pronašao odgovarajuće pravilo, sva daljnja pravila za filtriranje

biti će zanemarena. Ako na pristigli podatak nije moguće primijeniti niti jedno pravilo za filtriranje on će biti zanemaren. O tome treba voditi računa prilikom definiranja novog skupa pravila za manipulaciju nad podacima koji se prikupljaju.

5. Zaključak

U ovom dokumentu je samo ukratko prikazan način konfiguracije MonitorWare Agent-a. Detaljni opis svih njegovih funkcija i parametara konfiguracije može se naći u dokumentaciji koja dolazi sa samim programom. U dokumentaciji programa navedeni su i gotovi primjeri različitih konfiguracija MonitorWare Agent-a koji se, uz male modifikacije, mogu odmah koristiti tako da je poželjno dobro proučiti priloženu dokumentaciju prije korištenja samog paketa.

MonitorWare programski paket može se koristiti za praćenje događanja na pojedinačnim računalima ili na lokalnoj mreži baziranoj na Windows operativnom sustavu. Svako Windows računalo sa instaliranim MonitorWare programskim paketom može pratiti događaje koji su zapisani u *Windows Event Log* datotekama ili običnim tekstualnim datotekama (ovo je korisno za praćenje rada programa koji svoje logove zapisuju u tekstualne datoteke).

Isto tako, računalo na kojem je pokrenut MonitorWare Agent može primati Syslog poruke s ostalih računala u mreži. Budući da je Syslog poslužitelj osnova za logiranje događaja i praćenje rada računala baziranih na Linux/UNIX operativnom sustavu, MonitorWare Agent se može koristiti i u lokalnim mrežama koje se sastoje od Windows i Linux/UNIX računala.

Sva događanja koja prati MonitorWare Agent mogu se pohraniti u SQL bazu podataka ili u tekstualne datoteke, ali se isto tako mogu proslijediti na udaljeni Syslog poslužitelj ili drugi MonitorWare Agent. Ovo omogućava centralizirano praćenje događanja na svim računalima u mreži samo s jednog računala.

Svi prikupljeni podaci mogu se filtrirati čime se postiže praćenje samo određenih događaja. U slučaju pojave neregularnih aktivnosti, program može o tome obavijestiti administratora putem poruke elektroničke pošte ili Net Send-a. U nekim slučajevima moguće je i automatsko pokretanje nekih korektivnih akcija (ponovno pokretanje nekog programa ili servisa, brisanje `Tmp` direktorija u slučaju da se napunio tvrdi disk i slično).