



Opsætning af Realtime Notification baseret på Syslog meddelelser I SolarWinds Orion NCM v6:

I Orion Network Configuration Manager applikationen kan man se alle syslog beskeder som bliver modtaget fra ens netværksudstyr. Disse meddelelser kan være meget nyttige hvis man ved hvad de kan bruges til. Denne guide vil vise dig hvordan - ved brug af syslog beskeder - du kan få en notifikation om at en konfiguration på din switch er ændret. Denne funktion vil fortælle dig hvornår ændringen er sket, hvem der har lavet ændringen og hvor ændringen er lavet fra. Alle disse oplysninger bliver automatisk downloadet til NCM databasen og en backup bliver taget på stedet.

Vi starter i Syslog Viewer. Her kan du se alle Syslog meddelelser som bliver modtaget i NCM. For at se en bestemt Syslog besked, i vores tilfælde en konfigurationsændring, så er der mulighed for at søge efter dette.

- Klik *View* og vælg *Search Messages ...*
- I *Message Type* feltet indsæt SYS-5-CONFIG_I

(Denne Syslog besked genereres når der laves ændringer på en Cisco router/switch)

*Venligst henvend dig til enhedens dokumentation for en beskrivelse af Syslog beskeder

Hvis der er lavet ændringer i konfigurationsfiler, som NCM har opfanget sidst den udførte et scan af alle overvåget netværksudstyr så vil du se Syslog detaljer blandt søge resultater.

Vi skal nu generere en notifikation for hver gang et sådant besked modtages i NCM.

- Klik *View* og vælg *Alerts/Filter Rules ...*
- Klik *Add New Rule* under *Alerts / Filter Rules*
- Angiv et navn for denne ny regel
- Under *Message* fanen, indsæt SYS-5-CONFIG_I ved *Message Type Pattern*
- Under *Severity / Facility*, fravælg alt i *Severity* kolonnen, undtagen **Notice**
- Under *Alert Actions* fanen, klik *Add New Action* og vælg *Execute an external program*

Programmet som downloader konfiguration filen er ConfigAutoDownload.exe

- Indsæt stien til programmet. Dette er typisk:

```
"C:\Program Files\Solarwinds\Configuration Management\ConfigAutoDownload.exe"
```

```
${IP},RealtimeNotification,${DateTime},${Message}
```

*\${IP} er variable som fortæller dig hvad IP adresse Syslog beskeden stammer fra

*\${DateTime} er variabelen som fortæller dig hvad er datoen og tid for denne Syslog

*\${Message} er variabelen som fortæller dig hvad Syslog beskeden indeholder

Aflust og klik OK

Sørg for at der er sat hak ved den nyoprettet *Alerts / Filter Rules*

Aktivering af Real-Time Change Detection:

For at kunne modtage en e-mail med Syslog beskeden om at konfigurationen er ændret skal du aktivere for Real-Time Detection. Dette gøres på følgende måde i Orion Network Configuration Manager:

- Klik *File* og vælg *Settings ...*
- Under Real-Time Change Detection, sæt hak I boksen for at aktivere denne funktion
- Udfyld alle underliggende felter for denne funktion

Når alt er sat op korrekt, så vil du modtage mail på den mail adresse som du har angivet i Real-Time Change Detection indstillinger. Du kan afprøve denne nye funktion ved at lave en midlertidig ændring i en af dine switche. Du kan enten bruge NCM til at gøre dette eller vba. cmd prompt.