**­ITRS OP5 Monitor**

***Notify VisionFlow***

**Borås Stad**

Innehållsförteckning

[Generell information 1](#_Toc94703928)

[Filer och sökvägar 1](#_Toc94703929)

[Loggning 2](#_Toc94703930)

[Körning 2](#_Toc94703931)

[Argument 3](#_Toc94703932)

[Kontakter (contacts) 3](#_Toc94703933)

[Schemaläggning 3](#_Toc94703934)

[API-anrop 3](#_Toc94703935)

[Versionshantering 4](#_Toc94703936)

[Regelverk 4](#_Toc94703937)

[Host groups 5](#_Toc94703938)

# Generell information

Detta dokument innehåller information som beskriver lösningen för den automatiserade ärendehanteringsfunktionen som skapas mellan ITRS OP5 Monitor och VisionFlow. Lösningen går under namnet: *Notify VisionFlow*

*Notify VisionFlow* används för att skapa ärenden i VisionFlow utav OP5-larm. *Notify VisionFlow* gör en nätverksöverblick i OP5, för att kunna undvika larmstormar till VisionFlow. Exempelvis ska OP5 inte generera ärenden för tjänster som är beroende av DNS, ifall DNS-tjänsten inte är tillgänglig.  
Detta löses genom att man innan ärenden skapas, kontrollerar samtliga övervakningspunkter i infrastrukturen, före ärende skapas.

*Notify VisionFlow* körs på *viop5.ad.boras.se* och skannar av OP5 Monitor varje minut för att upptäcka nya larm.

# Filer och sökvägar

*Notify VisionFlow* återfinns på servrarna **shop5** och **viop5** under katalog: **/opt/plugins/custom/notify-visionflow.**  
Följande filer används:

Tabell 1

|  |  |
| --- | --- |
| **Sökväg** | **Beskrivning** |
| *notify\_visionflow.py* | Mjukvara som läser av larm i OP5 och skapar ärenden i VisionFlow |
| *hostgroups\_alert.lst* | Lista med host group för hosts som anses vara ”Kritisk serverutrustning”.  Fyll på denna lista med host groups för att inkludera fler hosts inom automatiserad ärendehantering.  Viktigt att placera host group-namnet inom citationstecken för att filen ska läsa korrekt. |
| *bs\_hosts.lst* | Hosts som håller Business Services objekt.  Fyll på denna lista med hosts för att inkludera fler hosts inom automatiserad ärendehantering.  Viktigt att placera host-namnet inom citationstecken för att filen ska läsa korrekt. |
| *op5-visionflow.log* | Loggfil dit samtliga loggmeddelanden från *notify\_visionflow.py* skrivs. |
| */etc/cron.d/notify-visionflow* | Cron-jobb som schemalägger *Notify VisionFlow* för automatisk körning. Körs per default en gång per minut. |

## Loggning

Varje körning av *Notify VisionFlow* loggförs (se sökväg i [tabell 1](#_Filer_och_sökvägar)).

Följande händelser loggförs:

* Fel vid API-anrop (OP5 & VisionFlow)
* Ärende kan ej skapas p.g.a. för kort larmperiod
* Ärende kan ej skapas p.g.a. att parent-objekt har problem
* Ärende kan ej skapas p.g.a. att OP5 visar inga fel
* Ärende kan ej skapas p.g.a. att ärende redan existerar
* Ärende skapat

Då Notify VisionFlow körs varje minut, skrivs även loggmeddelanden varje minut. För att förhindra att loggfilen (*op5-visionflow.log*) växer i oändlighet, används logrotate för att rotera och komprimera loggfilen varje vecka. Komprimerade filer sparas i fyra veckor.

# Körning

Per default så körs mjukvaran en gång i minuten, 24x7.

Detta kan enkelt förändas genom att ändra i *cron*, se tabell 1.

Per default så behöver ett larm ligga aktivt och ej i *Schedule downtime* i 30 minuter. Detta kan enkelt förändas genom argument till *notify\_visionflow.py*.

Ärende skapas om larmet både är ”*Acknowledged*” eller ”*Unacknowledged*”. Ifall larmet är ”*Acknowledged*” skickas kommentar och användarnamn med i ärendet.

## Argument

*notify\_visionflow.py* tar följande argument.

Tabell 2

|  |  |
| --- | --- |
| **Argument** | **Beskrivning** |
| --help | Visar samtliga argument och dess funktion |
| --op5host | OP5 Monitor IP/FQDN |
| --op5user | OP5 Monitor API User |
| --op5pass | OP5 Monitor API Password |
| --vflowhost | VisionFlow IP/FQDN |
| --vflowuser | VisionFlow API User |
| --vflowpass | VisionFlow API Password |
| --duration | Tid larm måste varit aktivt (Default 30min) |

## Kontakter (contacts)

*Notify VisionFlow* använder *contacts* i OP5 för att hämta de e-postadresser ärenden ska skickas till.

För att få ärenden i VisionFlow från OP5, skapa en kontakt och ange e-postadressen i fältet ”**address1**”, och lämna fältet ”**email**” tomt.  
Anledningen till att **address1** används framöver **email**, är för att inte skapa dubbletter av ärenden i VisionFlow. Används **email** kommer OP5’s standardnotis-system att initieras, och då tar OP5 inte hänsyn till *Notify VisionFlow,* som är en ovanpåliggande API-driven mjukvara. Därav används endast **address1**.

Applicera därefter kontakten på de service-objekt i OP5 där man önskar få ärenden från. Notera att det finns ett regelverk för vilka service-objekt detta omfattar, se tabell 3 & 4.

## Schemaläggning

*notify\_visionflow.py* är schemalagt m.h.a. *cron* på shop5.ad.boras.se att köras varje minut under: **/etc/cron.d/notify-visionflow**

## API-anrop

Koden kommunicerar med både OP5 Monitor API och VisionFlow Service API.

OP5’s API används för att hämta nyinkomna larm.  
VisionFlow API används för att skapa ärenden samt verifiera att inte ärenden redan finns.

## Versionshantering

Koden är skriven i python3.6, vilket är den version som körs i CentOS 7.9.

När systemet uppgraderas till version 8, används i skrivande stund python3.8, vilket bör vara med i beräkningen inför uppgraderingen, då detta kan kräva kod-förändringar.

# Regelverk

Regelverket för när ärenden ska skapas är byggt efter följande schema. Kan även refereras i dokumentet: ITRS OP5 Monitor – Borås Stad – Estimat – Automatiserad ärendehantering.

Tabell 3

|  |  |  |
| --- | --- | --- |
| **Objekttyp** | **Status** | **Ärende (Ja / Nej)** |
| Business Services | WARNING | Nej |
| Business Services | CRITICAL | Ja |
| Services | WARNING | Nej |
| Services | UNKNOWN | Nej |
| Services | CRITICAL | Ja |
| Host | DOWN | Nej |
| Host | UNREACHABLE (parent is down) | Nej |

När larmen återgår till status OK/RECOVERY, kommer ärenden inte att stängas automatiskt, utan ska manuellt stängas av användare i VisionFlow.

Larm som genereras under ”*Schedule downtime*” ska inte skapa ärenden.  
Larm som genererats och satts i ”*Acknowledgement*”, ska skapa ärenden.

Kommentar och användarnamn från ”*Acknowledgement*” följer med i larmet från OP5 till VisionFlow.

# Host groups

För närvarande genereras endast ärenden från host- och service-objekt i följande host groups:

Tabell 4

|  |
| --- |
| **Namn** |
| Kritisk Serverutrustning |

Använd filen *hostgroups\_alert.lst (tabell 1)* för att fylla på med fler host groups (separering med ny rad).