### **ZABBIXSNOV** From Monitoring to Incidents



# **INTRODUCTION**



### WHO ARE WE ?

# / Morten Moesgaard/ Certified Zabbix Specialist



/ Michael Andersen/ ServiceNow Specialist



3

### TV 2 DENMARK

- / TV Station
- / Established 1988
- **/ 5 TV Channels**
- / Online streaming and VOD service
- / Funded by commercials and subscription services

### **ZABBIX SPECS**

- / 1 Zabbix Server
- / 3 Zabbix Proxy
- / 600+ Mixed Virtual , physical, Synthetic hosts
- / 400+ items per sec
- / 15000+ Active triggers



### **SERVICES**

- / Webservers
- / Web Caches
- / Video Encoders
- / External services
- / Rancher (micro services)
- / Databases
- / And much more ..





### **ZABBIXSNOV** Zabbix & ServiceNOW



## ZABBIXSNOW IN SHORT:

What is ZabbixSnow ?

/ Inhouse script developed by Morten Moesgaard

- / Bridge between Zabbix And ServiceNow
  - / Reacts on Actions from Zabbix
  - / Creates incidents in ServiceNow
  - / Syncs hosts and triggers periodically (Zabbix to ServiceNow)



Who is in control?



### /Zabbix detects problems



/ ServiceNow handles the communication and Incidents

# Servicenuw

# **BENEFITS**



Investigation	n & Diagnosis Resolution	Closed
Identification Process		
INC0040463	State	New
Phone \$	Assignment group	Q
ā Q	Assigned to	Q
	Downtime start	09-08-2017 14:54:27
Categorisation		
None 🔶	Impact	3 - Low \$
Q	Urgency	3 - Low 🗘
	Priority	4 - Low
None 🜲	Watch list	
Incident Description		
Description +		
B I ⊻ ↔ ↔ Font Family -	- Font Sizes - ⊞ - A A & ½	
	INCO040463 Phone $ \begin{array}{c}                                     $	Investigation & Diagnosis     Resolution       Process     State       Phone     +       Image: Constrained and the state     Assignment group       Image: Constrained and the state     Constrine state       Image: Constrained and the state     Downtime state       Image: Constrained and the state     Image: Constrained and the state       Image: Constrained and the state     Constrained and the state       Image: Constrained and the state     Image: Constrained and the state       Image: Constrained and the state     Image: Constrained and the state       Image: Constrained and the state     Image: Constrained and the state       Image: Constrained and the state     Image: Constrained and the state       Image: Constrained and the state     Image: Constrained and the state       Image: Constrained and the state     Image: Constrained and the state       Image: Constrained and the state     Image: Constrained and the state       Image: Constrained and the state     Image: Constrained and the state       Image: Constrained and the state     Image: Constrained and the state       Image: Constrained and the state     Image: Constrained and the state       Image: Constrained and the state     Image: Constrained and the state       Image: Constrained and the state     Image: Constrained and the state       Image: Constrained and the state     Image: Constrained and the state



### SERVICENOW

- Adding value Reporting
- / Collaboration

### ZABBIX

/ Incentive for fine-tuning of triggers

- / Templates make incidents more consistent
  - / Relevant consistent info via trigger description
  - / Runbooks via URL field
  - / Trigger name is descriptive
- /No more guesstimating downtime

### **SUMMARY**

/ Non-technical people get info in a non-technical way

- / Better reports based on info given by Zabbix
- / Better pinpointing of reoccurring problems
- / Better knowledge sharing (runbooks)
- / Relevant triggers create incidents

# WHAT DID WE DO?



### ZABBIX

### / Action

### / Based on

- / Host Group
- / Trigger severity
- / Curl command to ZabbixSNOW

#### / Problem state

- / ZabbixSnow evaluates
- / Collects info from Zabbix
- / Collects info from ServiceNOW
- / Compares info
- / Creates incident / updates incident
- / Sets downtime start (on newly created incidents only)

#### / OK

- / ZabbixSnow evaluates
- / Information from Zabbix
- / Information from ServiceNOW
- / Adds comment / info
- / Sets downtime end
- / No database to keep track of states

## **THE TECHNICAL PART** Aka the how



```
Shell
            🔵 🕱 🕹 🛛 🗧 🗧 🔍 😌 🔍 🔍 🔍 🔍
                                              bash
                                                       ● ೫3
private STval = '':
private $Ack = '';
private $AckHist = '';
function __construct()
   global $SnowApi, $ZabbixApi, $Convert, $Groupids, $typerel, $Snowtablehost, $Snowtabletrigger, $Snowtablecirel;
   $this->Sapi = $SnowApi;
   $this->Zapi = $ZabbixApi;
   $this->Tid = $_GET['tid'];
   $this->Eid = $_GET['evid'];
   $this->Tval = $_GET['tval'];
   $this->Ack = $_GET['ack'];
   $this->AckHist = $_POST['hist'];
   $method = 'host.get';
   $params = array('output'=> ['hostid'], 'proxy_hosts' => 1);
   $addons = '';
   $this->zProxy = $this->Zapi->get_zabbix_reg($method,$params,$addons);
   $method = 'host.get';
   $params = array('output' >> 'extend', 'triggerids' -> $this->Tid);
   $addons = '';
   $this->zHost = $this->Zapi->get_zabbix_req($method,$params,$addons);
   //We fetch Info from ServiceNow so we can identify the trigger
   $this->Info = $this->Sapi->snow_action('&sysparm_query=u_zbx_triggerid='.$this->Tid.'',$Snowtabletrigger,'');
   //check for if proxy has an incident or this is a proxy
   if($this->isproxy($this->Hid) == true){
        $this->case_proxy_exists();
   }else{
       //if no proxy case we add +1 to our shared memory
        $shm_id = shmop_open(0xdeadf, 'c', 777, 1024);
       $shm_data = shmop_read($shm_id, 0, 8);
       if($shm_data <= 59 ){
            if (empty($shm_data)) {
               $shm_bytes_written = shmop_write($shm_id, 0, 1);
            } else {
               $shm_bytes_written = shmop_write($shm_id, (int)$shm_data+1, 0);
       }else{
            // if we exceed 60 we simple just return OK to zabbix
            shmop_close($shm_id);
            die("ok");
       shmop_close($shm_id);
       //if we came thrue the loop we go to incident creation
        $this->createIncident();
   }
```

```
function isproxy($proxy){
    foreach($this->zProxy->result as $key => $value){
        if($value->hostid == $proxy){
            return true;
        }
    }
    return false;
}
```

function case\_proxy\_exists(){

/ Problem.php

- / Everytime the Zabbix Action run Problem parameter
  - / Collects info from Zabbix and ServiceNow
  - / Evaluates if it is a failed proxy trigger
  - / Evaluates if our limiter has gotten more than 60 triggers
  - / Denies when limiter is 60 (resets every 60 seconds)
  - / Creates incident in service now when no incident is active
  - / Adds comment on existing incidents



#### / OK.php

- / Everytime the Zabbix Action run OK parameter
  - / Collects info from Zabbix and ServiceNow
  - / Evaluates if it is a failed proxy trigger
  - / Adds OK comment on existing incidents
  - / Adds Downtime End

- / Addhosts.php
- / Run by CRON every 1 hour
  - / Zabbix host to ServiceNow sync
  - / Zabbix trigger to ServiceNow sync
  - / New hosts added
  - / New trigger added

/ Addhosts.php

- / Run by CRON every 24 hour
  - / Full sync
- / Syncing
  - / Zabbix triggers are connected to individual host
  - / Triggers are identified in ServiceNow
  - / Find if Relation is there
  - / Prepare relations
  - / Reset all Hosts and triggers
  - / Insert active Hosts and triggers and set "True" in active in zabbix else set false
  - / Set relations between host and triggers in ServiceNow

# **ANY QUESTIONS??**



