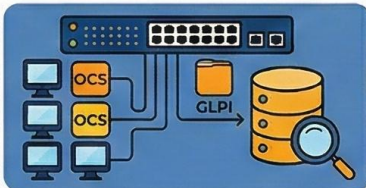


Réalisation 2

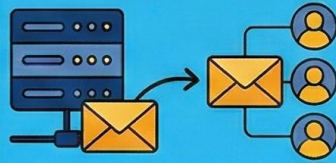


1. INVENTAIRE AUTOMATISÉ : OCS & GLPI

Déploiement des agents OCS sur les terminaux du VLAN 50. Configuration de la remontée automatique des données matérielles et logicielles vers le serveur GLPI.

2. MISE EN PLACE DE LA COMMUNICATION : Zimbra

Création d'une liste de diffusion sur Zimbra incluant le gérant et les responsables informatiques pour centraliser les échanges.



3. SUPERVISION RÉSEAU : Intégration Nagios

Intégration des bornes Wi-Fi dans le système de supervision Nagios.

4. GESTION DES ALERTES : ICMP & SNMP

Configuration d'alertes critiques envoyées par courriel au groupe de support DSI basées sur des requêtes ICMP (ping) et SNMP qui ne répondent plus.



Microsoft
Active Directory



Contexte :

La gestion des terminaux de commande et des caisses (POS) nécessite un inventaire centralisé pour un suivi efficace. Par ailleurs, la criticité du réseau Wi-Fi impose une supervision constante pour garantir la continuité de l'activité du restaurant.

Sommaire :

1. Inventaire automatisé (OCS & GLPI)
2. Mise en place de la communication (Zimbra)
3. Supervision du réseau (Nagios)
4. Gestion des Alertes

Mise en place de la communication (Zimbra)

Étape suivante (continue comme ça)

+ Créer les autres comptes

```
zmprov ca gerant@xmail.stadiumcompany.local Bts2024@
zmprov ca admin1@xmail.stadiumcompany.local Bts2024@
zmprov ca admin2@xmail.stadiumcompany.local Bts2024@
```

```
(root@xmail)-[~]
# su - zimbra
zimbra@xmail:~$ zmprov gad
xmail.stadiumcompany.local
zimbra@xmail:~$ zmprov ca gerant@xmail.stadiumcompany.local Bts2024@
d6197eb6-45c9-408a-86fd-3a371b75136d
zimbra@xmail:~$ zmprov ca admin1@xmail.stadiumcompany.local Bts2024@
6c4e8602-dc01-4b2c-86c4-f1785db088cf
zimbra@xmail:~$ zmprov ca admin2@xmail.stadiumcompany.local Bts2024@
00f22c81-cfe3-4727-9a27-8c24cf46f64c
zimbra@xmail:~$
```

Créer la liste de diffusion

```
zmprov cdl support-dsi@xmail.stadiumcompany.local
zimbra@xmail:~$ zmprov cdl support-dsi@xmail.stadiumcompany.local
fd10d1df-7f78-4734-ae5c-9660087a488a
```

Ajouter les membres

```
zmprov adlm support-dsi@xmail.stadiumcompany.local
gerant@xmail.stadiumcompany.local
zmprov adlm support-dsi@xmail.stadiumcompany.local
admin1@xmail.stadiumcompany.local
zmprov adlm support-dsi@xmail.stadiumcompany.local
admin2@xmail.stadiumcompany.local
```

```
zimbra@xmail:~$ zmprov adlm support-dsi@xmail.stadiumcompany.local gerant@xmail.stadiumcompany.local
zimbra@xmail:~$ zmprov adlm support-dsi@xmail.stadiumcompany.local admin1@xmail.stadiumcompany.local
zimbra@xmail:~$ zmprov adlm support-dsi@xmail.stadiumcompany.local admin2@xmail.stadiumcompany.local
zimbra@xmail:~$
```


Vérifier la liste

```
zmprov gdl support-dsi@xmail.stadiumcompany.local
```


```
zimbra@xmail:~$ zmprov gdl support-dsi@xmail.stadiumcompany.local
# distributionList support-dsi@xmail.stadiumcompany.local memberCount=3
mail: support-dsi@xmail.stadiumcompany.local
objectClass: zimbraDistributionList
objectClass: zimbraMailRecipient
uid: support-dsi
zimbraCreateTimestamp: 20260421094830.598Z
zimbraId: fd10d1df-7f78-4734-ae5c-9660087a488a
zimbraMailAlias: support-dsi@xmail.stadiumcompany.local
zimbraMailForwardingAddress: admin1@xmail.stadiumcompany.local
zimbraMailForwardingAddress: admin2@xmail.stadiumcompany.local
zimbraMailForwardingAddress: gerant@xmail.stadiumcompany.local
zimbraMailHost: xmail.stadiumcompany.local
zimbraMailStatus: enabled


members
admin1@xmail.stadiumcompany.local
admin2@xmail.stadiumcompany.local
gerant@xmail.stadiumcompany.local
zimbra@xmail:~$
```



Test final

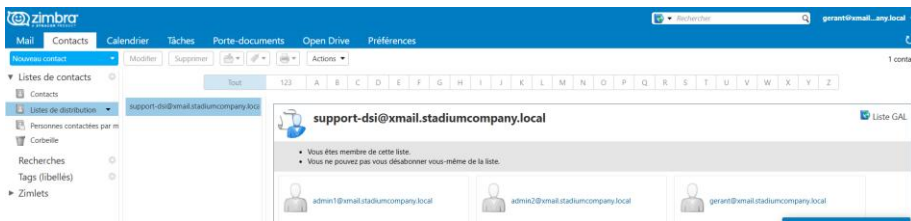
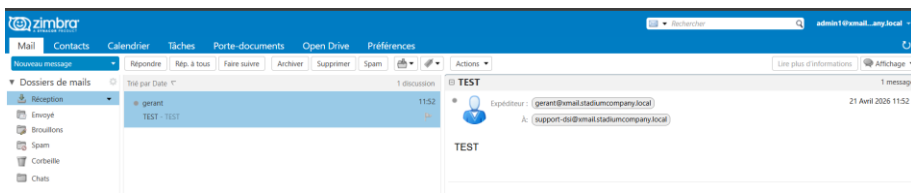
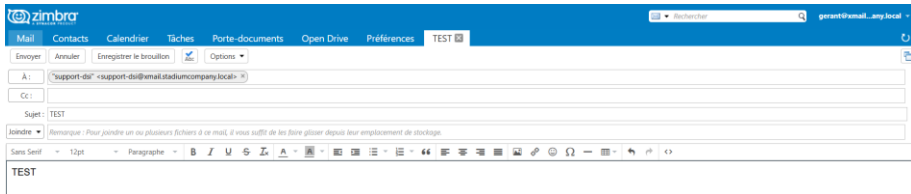
 envoie un mail à :

support-dsi@xmail.stadiumcompany.local

 Résultat attendu :

 tous les membres reçoivent

 Connexion Utilisateur <input type="text" value="gerant@xmail.stadiumcompany.local"/> Mot de passe <input type="password" value="....."/> <small>Afficher</small> <input type="button" value="Connexion"/> <input type="checkbox"/> Mémoriser mes valeurs d'accès Version Défaut <small>?</small>	 Connexion Utilisateur <input type="text" value="admin1@xmail.stadiumcompany.local"/> Mot de passe <input type="password" value="....."/> <small>Afficher</small> <input type="button" value="Connexion"/> <input type="checkbox"/> Mémoriser mes valeurs d'accès Version Défaut <small>?</small>
---	---



Commande : `zmprow -l gaa` = permet de vérifier les comptes.

```
zimbra@xmail:~$ zmprow -l gaa
admin@xmail.stadiumcompany.local
spam.pcadw4qh@xmail.stadiumcompany.local
ham.bga2yeug4@xmail.stadiumcompany.local
virus-quarantine.posjihdkf@xmail.stadiumcompany.local
galsync.iyk7a4pi@xmail.stadiumcompany.local
assistance@xmail.stadiumcompany.local
support@xmail.stadiumcompany.local
glpi@xmail.stadiumcompany.local
kaiser@xmail.stadiumcompany.local
cesar@xmail.stadiumcompany.local
annick@xmail.stadiumcompany.local
gerant@xmail.stadiumcompany.local
admin1@xmail.stadiumcompany.local
admin2@xmail.stadiumcompany.local
zimbra@xmail:~$
```

Supervision du réseau (Nagios)

1. Objectif de la Supervision

L'enjeu est de garantir une surveillance constante des infrastructures critiques.

- **Périmètre** : Intégration des bornes Wi-Fi dans le système Nagios.
- **Indicateurs** : Surveillance de la connectivité réseau et de l'état des services.

2. Configuration Technique

Nagios utilise des protocoles standard pour interroger les équipements à distance:

- **ICMP (Ping)** : Pour vérifier si les bornes Wi-Fi sont allumées et joignables sur le réseau.
- **SNMP** : Pour obtenir des informations plus détaillées sur l'état interne des équipements qui ne répondraient plus correctement.

3. Gestion des Alertes et Réactivité

Le système est configuré pour être proactif plutôt que réactif:

- **Déclenchement** : Des alertes critiques sont générées dès qu'une requête ICMP ou SNMP échoue.
- **Notification** : Les alertes sont envoyées automatiquement par **courriel** au groupe de support DSI.
- **Interface** : Nagios offre un tableau de bord visuel permettant de voir en un coup d'œil l'état (Vert/Rouge) de chaque borne Wi-Fi.

4. Lien avec les autres outils

Cette étape boucle la boucle de ton projet:

- Les bornes à superviser sont préalablement identifiées dans l'**inventaire GLPI**.
- Les alertes Nagios sont reçues et traitées via la messagerie **Zimbra**.

2 Configurer Nagios pour envoyer des mails

👉 Sur ton serveur Nagios

📁 Fichier contacts

```
nano /usr/local/nagios/etc/objects/contacts.cfg
```

Exemple :

```
define contact {
    contact_name    dsi
    use              generic-contact
    alias           Equipe DSI
    email           support-dsi@xmail.stadiumcompany.local
}
```

👉 ⚠️ important :

➡️ tu mets la liste de diffusion, pas un utilisateur

3 Associer ce contact

👉 Dans :

nano /usr/local/nagios/etc/objects/contactgroups.cfg

```
define contactgroup {
    contactgroup_name    dsi-group
    alias                DSI
    members              dsi
}
```

4 Associer aux équipements

👉 Dans ton host ou service :

nano /usr/local/nagios/etc/objects/hosts.cfg

Exemple :

```
define host {
    host_name    borne_wifi
    address     172.20.X.X
    contact_groups    dsi-group
}
```

5 Activer les notifications

👉 Vérifie dans :

nano /usr/local/nagios/etc/nagios.cfg

Tu dois avoir :

```
enable_notifications=1
```

6 Redémarrer Nagios

```
systemctl restart nagios
```

🔧 7 TEST (le plus important)

👉 Simule une panne :

- éteins une machine
OU
- mets une mauvaise IP

👉 Résultat attendu :

📧 Nagios envoie un mail à :

support-dsi@xmail.stadiumcompany.local

👉 Et :

- le gérant reçoit ✓
- les admins reçoivent ✓

IMPORTANT : il faut installer postfix = bien le configurer tel quel : il faut que je refasse l'installation de postfix pour bien refaire les screens.

```
smtpd_relay_restrictions = permit_mynetworks permit_sasl_authenticated defer_unauth_destination
myhostname = nagiosxi.stadiumcompany.local
alias_maps = hash:/etc/aliases
alias_database = hash:/etc/aliases
myorigin = $myhostname
mydestination = _
relayhost = [xmail.stadiumcompany.local]
mynetworks = 127.0.0.0/8 [::ffff:127.0.0.0]/104 [::1]/128
mailbox_size_limit = 0
```

Faire restart ensuite et faire un test.

```
zimbra@xmail:~$ zmprov ms xmail.stadiumcompany.local zimbraMtaMyNetworks "127.0.0.0/8 172.20.1.0/24
172.20.4.0/24"
zimbra@xmail:~$ _
```

ICI : ça permet d'autoriser le reçu des mails du réseau lui-même, du VLAN 10 et du VLAN 40.

- ICMP → test de disponibilité réseau
- SNMP → supervision avancée des équipements
- Zimbra → diffusion centralisée des alertes

Supervision des bornes wifi via NAGIOS

Prérequis :

- Outils nagios
- Borne Wifi en IP Statique et SNMP actif

1°) Dans l'outil Nagios, se rendre sur le « Home Dashboard » et ajouter un nouvel équipement à superviser via le bouton « Run a Wizard ».

The screenshot shows the Nagios XI interface. The top navigation bar includes 'Views', 'Dashboards', 'Reports', 'Configure', 'Tools', 'Admin', and 'Enterprise'. The left sidebar has a 'Quick View' section with 'Home Dashboard' highlighted. Below it are 'Details' and 'Graphs' sections. The main content area is titled 'Home Dashboard' and contains several widgets: 'Host Status Summary' with a table showing 3 Up, 0 Down, 0 Unreachable, and 0 Pending; 'Service Status Summary' with 3 OK, 0 Warning, and 0 Unknown; 'Trial Resources' with 430 Days Left in Trial; 'Getting Started' with a 'Run a Wizard' button highlighted; and 'Account Settings'.

Up	Down	Unreachable	Pending
3	0	0	0
Unhandled		Problems	
0		3	

Ok	Warning	Unkn
3	0	0
Unhandled		
21		

2°) On recherche SNMP dans la barre de recherche, afin de trouver l'option SNMP, et on clique pour ajouter un équipement en supervision via SNMP.

Configuration Wizards - Select a Wizard

Start monitoring your infrastructure in minutes. Configuration wizards guide you through the process of setting up your devices, servers, applications, services, and more.

Show:

- Linux SNMP**
Monitor a Linux workstation or server using SNMP.
- SNMP**
Monitor a device, service, or application using SNMP.
- SNMP Walk**
Scan an SNMP-enabled device for elements to monitor.
- Windows SNMP**
Monitor a Microsoft® Windows workstation or server using SNMP.

3°) Ensuite, il faut indiquer l'adresse IP que l'on souhaite ajouter, dans notre cas 172.20.5.151

SNMP Configuration Wizard Step 1

SNMP Information

* Device Address ⓘ

4°) On sélectionne bien 2c pour la version SNMP et public pour le SNMP Community

SNMP Configuration Wizard Step 2

Device Details

Device Address

* Host Name ⓘ

SNMP Settings

Specify the settings used to monitor the server or device via SNMP



* SNMP Version ⓘ

SNMP Port ⓘ

SNMP Version Settings

* SNMP Community ⓘ

5°) On sélectionne bien 2c pour la version SNMP et public pour le SNMP Community

 **SNMP Configuration Wizard** Step 3 

Monitoring Settings

Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances:


Monitor the host and service(s) every minutes


When a potential problem is first detected:

Re-check the host and service(s) every minutes up to times before sending a notification

[< Back](#) [Next >](#) [Finish with Defaults](#)

6°) Puis, on as une confirmation pour dire que notre SNMP à bien étai ajouter

 **SNMP Configuration Wizard**

 Configuration verification failed.

Configuration Error
An error occurred while attempting to apply your configuration to the monitoring engine. Contact your Nagios administrator if this problem persists.

- [Run this monitoring wizard again](#)
- [Run another monitoring wizard](#)

[View the latest configuration snapshots](#)

Commenté [RK1]: Message d'erreur qui n'as pas lieu d'être
La commande
`/usr/local/nagiosxi/scripts/repair_databases.sh` fixe la database et, malgré l'erreur, l'ap est ajouter dans nagios

7°) Dans le home dashboard, la quantité de host « UP » à étáis augmenter,

Home Dashboard ⚙

Host Status Summary			
Up	Down	Unreachable	Pending
5	0	0	0
Unhandled	Problems	All	
0	0	5	

Last Updated: 2023-01-01 00:17:59

8°) Et quand on clique sur les hosts, on retrouve notre host, ici 172.20.5.151

Host	Status	Duration	Attempt	Last Check	Status Information
172.20.5.151	Up	32m 15s	1/5	2023-01-01 00:15:45	OK - 172.20.5.151 rta 0,377ms lost 0%

9°) On peut avoir plus de détail en cliquant sur le nom du host

Host Status Detail

172.20.5.151

Overview

OK - 172.20.5.151 rta 0,377ms lost 0%

Address: 172.20.5.151

Status Details	
Host State:	Up
Duration:	31m 15s
Host Stability:	Unchanging (stable)
Last Check:	2023-01-01 00:15:45
Next Check:	2023-01-01 00:20:45

Quick Actions	
Disable notifications	Force an immediate check
Ping this host	Connect to 172.20.5.151
Traceroute to this host	

Misc: No notes or misc info

Acknowledgements and Comments: No comments or acknowledgements.

10°) Et ainsi effectuer des commandes de test tel que « Ping this host »

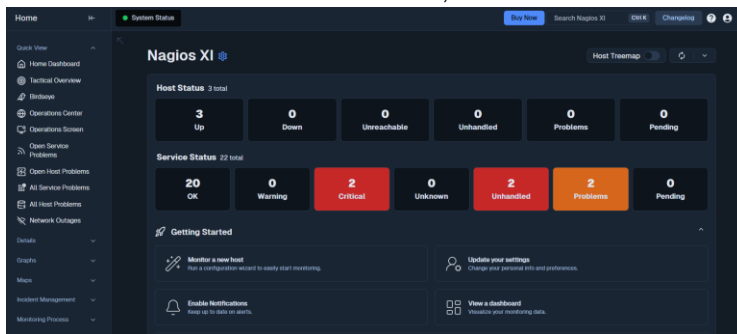
Ping Output

[Close This Window](#)

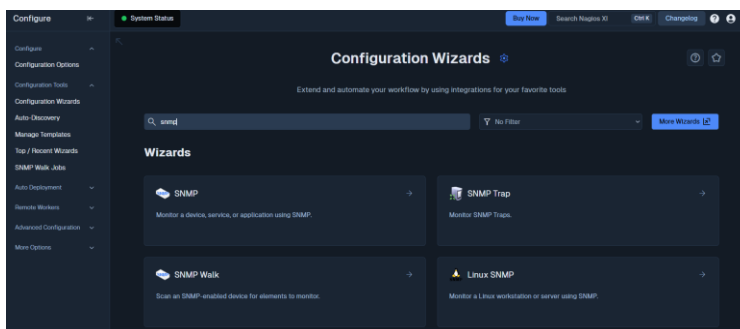
```
PING 172.20.5.151 (172.20.5.151) 56(84) bytes of data.  
64 bytes from 172.20.5.151: icmp_seq=1 ttl=254 time=0.506 ms  
64 bytes from 172.20.5.151: icmp_seq=2 ttl=254 time=0.485 ms
```

Avec le NOUVEAU NAGIOS !!

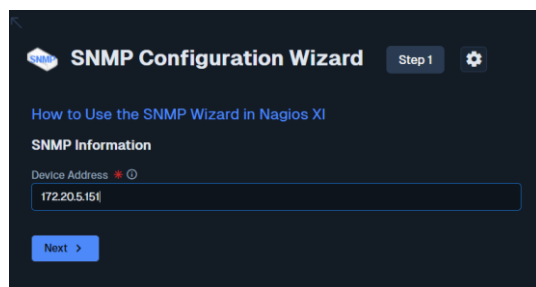
Dans le menu « HOME » on va faire, « Monitor a new host »



On recherche SNMP, puis on sélection, le SNMP car c'est cette solution de supervision qu'on va utiliser



On rentre l'adresse ip de notre AP, 172.20.5.151



On sélection la version 2c de SNMP et le port 161 (Choix par défaut) :

SNMP Configuration Wizard Step 2

Device Details

Device Address
172.20.5.151

Host Name * ⓘ
172.20.5.151

SNMP Settings

Specify the settings used to monitor the server or device via SNMP

SNMP Version * ⓘ
2c

SNMP Port ⓘ
161

Et il est important de juste coché la première ligne, sinon Nagios ne nous laisse pas faire suivant.

SNMP Services

Specify any OIDs you would like to monitor via SNMP. Sample entries have been provided as examples

OID ⓘ	Display Name ⓘ	Data Label ⓘ	Data Units ⓘ (Optional) ⓘ	Match Type	Warning Range ⓘ	Critical Range ⓘ	String To Match ⓘ	MIB To Use ⓘ
<input checked="" type="checkbox"/>	sysUpTime.0	Uptime		None				
<input type="checkbox"/>	ifOperStatus.1	Port 1 Status		String			↑	RFC1213-MIB
<input type="checkbox"/>	1.3.6.1.4.1.2.2.51.1.2.1.5.1.0	IBM RSA II Adaptor Temperat	Ambient Tem	C	Numeric	29	35	
<input type="checkbox"/>	1.3.6.1.4.1.3076.2.12.17.1.7.0	Cisco VPN Sessions	Active Sess	Numeric	70,8	75,10		
<input type="checkbox"/>				None				
<input type="checkbox"/>				None				

Add Row | Delete Row

< Back Next > Cancel

Ici, on choisi de faire un check toute les 5 minutes, et si un problème est détecter, il regarde toute les minutes, 3 fois, pour ensuite nous envoyer une alerte

SNMP Configuration Wizard Step 3

Monitoring Settings

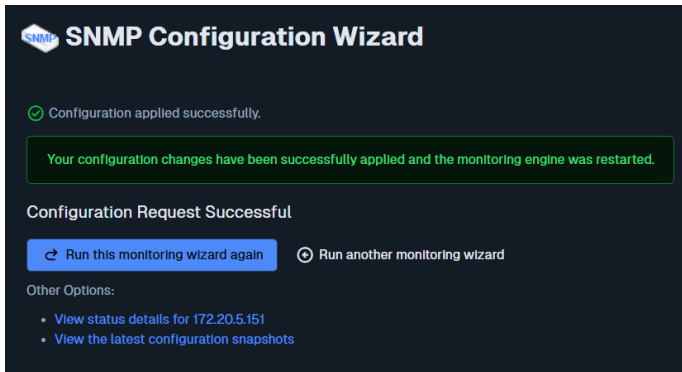
Define basic parameters that determine how the host and service(s) should be monitored.

Under normal circumstances: Monitor the host and service(s) every 5 minutes

When a potential problem is first detected: Re-check the host and service(s) every 1 minutes up to 3 times before sending a notification

< Back Next > Finish with Defaults Cancel

Et voila la mise en place du SNMP sur notre AP CISCO terminer

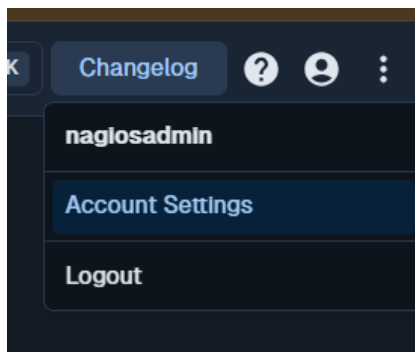


Ajoute du système d'alerte par mail :

Configuration du mail sur nagios :

nano /etc/postfix/main.cf

On va dans account setting



Dans Email address, on met notre mail de diffusion « support-dsi@xmail.stadiumcompany.local »

Account Information

Update your account information.

General Account Settings

Email Address

This is your email address in Nagios XI.

[Update Settings](#) [Cancel](#)

Ensuite, on active les notifications dans : Configure → Core Config Manager → Contacts

Core Config Manager

CCM Object Summary

Hosts	4	Host Groups	4	Services	23	Service Groups	2
Contacts	1	Contact Groups	2	Commands	177	Host Dependencies	0
		Service Dependencies	0				

Contacts

Displaying 1 of 1 results

[+ Add New](#)

<input type="checkbox"/>	Contact Name	Alias	Active	Actions	ID
<input type="checkbox"/>	nagiosadmin	Nagios Admin	Yes	View Edit Delete	1

With checked [Go](#) Results per page 15

[+ Add New](#) [Apply Configuration](#)

[Common Settings](#) [Alert Settings](#) [Misc Settings](#)

Contact Username *

nagiosadmin


Alias


Nagios Admin

Email Address

support-dsl@xmail.stadiumcompany.local

Pager Number

 **Manage Contact Groups** 0

 **Manage Contact Templates** 1

Active ⓘ

[Save](#) [Cancel](#)

Contact Management Help Options

Common Settings **Alert Settings** Misc Settings

Host Notifications Enabled

On Off Skip Null

Host Notifications Timeperiod

24x7

Host Notification options

Down Unreachable Up Flapping Scheduled Downtime None

Manage Host Notification Commands

Retain status Information

On Off Skip Null

Retain non-status Information

On Off Skip Null

Service Notifications Enabled

On Off Skip Null

Service Notifications Timeperiod

24x7

Service Notification options

Warning Unknown Critical Flapping Scheduled Downtime Ok None

Manage Service Notification Commands

Can Submit Commands

On Off Skip Null

Save Cancel

Manage

Filter...

- check-host-alive-ftp
- check_none
- notify-host-by-email-xi
- notify-service-by-email
- notify-service-by-email-xi
- process-host-perfdata-file-bulk
- process-host-perfdata-file-prp-bulk
- process-host-perfdata-prp-normal

Add Selected > Relationship defined elsewhere Inactive object

Assigned Remove All

- notify-host-by-email

+ Null Standard

Close

⚠ Changes detected! Apply Configuration for new changes to take effect.

Apply Configuration

Use this feature to apply any outstanding configuration changes to Nagios Core. Changes will be applied and the monitoring engine will be restarted with the updated configuration.

Apply Configuration

Apply Configuration

✔ Configuration applied successfully.

Nagios Core was **restarted** with an updated configuration.

[View configuration snapshots](#)

Show Written Confgs