cockpit
IT Service Manager

Supervision - Configuration des alertes externes

Document FAQ

Table des matières

Introduction

I. Principes

Le menu des « alertes externes » permet de recevoir et de gérer les messages générés par des éléments tiers (équipements, applications, scripts, etc.) via différents protocoles :

- Envois d'emails
- Envois de TRAPS SNMP
- Envois de messages API

II. Objectifs du document

- Paramétrer les boîtes de réception d'emails.
- Paramétrer les moteurs pour qu'ils réceptionnent des TRAPS SNMP.
- Paramétrer les accès API et expliquer comment injecter un message.

Boîtes de réception

Menu : Supervision > Alertes externes > Boîtes de réception

Principe : Cockpit IT Service Manager contrôle régulièrement la présence de nouveaux emails dans une boîte de réception, chaque email correspondant aux critères de recherche est utilisé pour générer une alerte dans le menu « Supervision / Alertes externes / Alertes en attente ».

Fonctionnement :

- Au premier contrôle (à la création de la boîte de réception), tous les emails du jour (date du jour à partir de 00h00) sont relevés.
  Aux contrôles suivants, Cockpit IT Service Manager vérifie la présence de nouveaux emails depuis le contrôle précédent.
- Les emails sont relevés toutes les 2 minutes.
- Les emails relevés sont envoyés dans les alertes en attente du menu « Alertes externes ».
- Les emails relevés ne sont pas marqués comme lu dans le boîte de réception.
- Quand une boîte de réception est réactivée après une période d'inactivité, tous les emails réceptionnés pendant la période d'inactivité sont relevés.

Principaux paramètres	
Champs	**Informations**
Organisation	Sélection d'une organisation : les alertes ne sont visibles que par les opérateurs accédant à l'organisation. Sélection « Sans organisation » : l'alerte n'est pas attribuée à une organisation, tous les opérateurs la visualisent.
Statut	Non coché : les emails ne sont pas relevés Coché : les emails sont relevés
Protocole	Sélection du protocole de connexion à la messagerie : POP3 POP3 (SSL) IMAP IMAP (SSL)
Empreinte SHA-1 du certificat SSL	Empreinte du certificat SSL de format SHA-1. L'empreinte du certificat doit être renseignée pour les certificats auto-signés ou expirés.
Serveur	Serveur de messagerie Exemple : pop.myserver.com
Port	Port de connexion à la messagerie
Utilisateur / Mot de passe	Identifiants
Termes dans le sujet	Indiquer les termes qui seront recherchés dans le sujet des emails, seuls les emails contenant ces termes génèreront une alerte. Pour une recherche distincte sur plusieurs termes, séparer les termes par un « ; ». Champ vide : tous les emails sont pris en compte
Options	Cocher les options pour les activer : Supprimer les emails remontés du serveur

	Ignorer messages marqués comme lus

Gestion du menu :

- La suppression d'une boîte de réception n'impacte pas les alertes générées.
- Le test de connexion manuel à la boîte de réception n'impacte pas le contrôle des emails, il vérifie juste la possibilité de la connexion.

TRAPS SNMP

Menu : Administration > Liste des moteurs

Principe : Des TRAPS SNMP peuvent être envoyées à un moteur (déporté ou local), toutes les TRAPS reçues génèrent une alerte dans menu « Supervision / Alertes externes / Alertes en attente ».

Configuration : Sélectionner un moteur, cliquer sur « Configurer », aller dans l'onglet « Paramètres fonctionnels », partie « Supervision et Infrastructure > Trappe SNMP » :

- Statut : Statut (Actif / inactif) de l'écoute du port. Quand le statut est inactif aucune trappe SNMP n'est remontée.
- Port : Port d'écoute pour la réception des trappes SNMP (16100 par défaut). S'assurer que les équipements envoyant les trappes SNMP accèdent au port du moteur.
- Version :
  - V1 / V2c : Renseigner le « community string » qui sert d'authentification, il est utilisé pour les versions SNMPv1 et SNMPv2c. Par convention les équipements envoient les trappes SNMP avec le « community string » « public » mais il peut être différent, il faut vérifier quel « community string » est utilisé par les agents SNMP émetteurs des trappes SNMP.
  - V3 : La version SNMPv3 utilise une authentification. Renseigner les champs de protocoles, d'identifiants et de chiffrement.

Exemple :

Il est possible d'utiliser un outil de génération de TRAPS SNMP pour vérifier le paramétrage, par exemple SnmpTrapGen détaillé dans le lien ci-dessous :

https://snmpsoft.com/shell-tools/snmp-trap-gen/

Utiliser la commande suivante :

SnmpTrapGen.exe -r:127.0.0.1 -p:162 -t:10 -v:2c -c:"public" -to:.1.3.6.1.2.1.1.4.0

- « -r » : adresse IP de l'équipement
- « -p » : port, par défaut les TRAPS SNMP sont envoyées sur le port 162
- « -v » : version, par défaut la version 1 est utilisée
- « -t » : timeout en secondes (1 – 600)
- « -c » : community string, par défaut « public » est utilisé, ne concerne que les version SNMP v1 / v2c
- « -to » : OID envoyée par la TRAP SNMP

API

I. Principes

Les messages peuvent être envoyés à l'API du portail via une URL. Chaque message reçu est injecté dans la file d'attente des alertes externes.

II. Accès à l'API

Menu : Supervision > Alertes externes > Accès API

Configuration :

Afin de créer un accès API, il suffit de cliquer sur « Nouveau ».

- La clé API est générée automatiquement.
- Il est possible d'associer un accès à une organisation, tous les messages reçus seront associés à cette organisation.
- Une fois que l'accès est créé, il est possible d'effectuer un test d'injection de message.

Il est possible de modifier un accès existant en modifiant la clé, dans ce cas il faudra mettre à jour la clé de tous les éléments externes qui utilisent l'accès.

III. Injection d'un message

L'injection d'un message via l'API se fait par le protocole HTTPS. Il suffit d'appeler une URL avec les bons paramètres pour injecter un message.

Lorsque le message est injecté, l'API renvoie le message « OK ».

Les paramètres de l'URL sont contenus dans le tableau suivant.

Paramètres	
Paramètre	**Informations**
URL	Il s'agit de lURL du portail suivi de « /alert-api » https://adresse_du_portail/alert-api
key	Clé d'accès à l'API. Paramètre obligatoire.
message	Message à injecter. Paramètre obligatoire. 255 caractères maximum.
sender	Permet d'indiquer la source du message. Paramètre optionnel. 255 caractères maximum.
structure	Nom de l'organisation liée au message. Paramètre optionnel. Si l'accès API est déjà lié à une organisation, ce paramètre ne sera pas pris en compte.
environment	Nom de l'environnement lié au message.

	Paramètre optionnel.

Exemples :

Injection du message « hello » sans aucun paramètre :

https://support.cockpit-itsm.com/alert-api?key=598ksoze5-35b8-4ef4-b280-a605faf04d91&message=hello

Injection du message « hello world! » avec les paramètres suivants :

- Source : My script
- Organisation : ALBATROS
- Environnement : Production

https://support.cockpit-itsm.com/alert-api?key=598ksoze5-35b8-4ef4-b280-a605faf04d91&message=Hello%20world!&sender=My%20script&structure=ALBATROS&environment=Production