

Configurer et exécuter le contrôle d'intégrité du système ESA

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Paramètres d'intégrité système](#)

[Vérification de l'intégrité du système](#)

[Analyser les problèmes potentiels de mise à niveau](#)

[Données analysées par le contrôle d'intégrité du système](#)

[Plan de correction](#)

[Conclusion](#)

[Informations connexes](#)

Introduction

Ce document décrit comment configurer les paramètres d'intégrité du système et comment exécuter le contrôle d'intégrité du système sur un dispositif de sécurité de la messagerie Cisco (ESA).

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Paramètres d'intégrité système

Les paramètres d'intégrité du système sont des seuils définis sur l'appliance afin de surveiller l'utilisation du processeur, le nombre maximal de messages dans la file d'attente de travail, etc. Ces paramètres ont des seuils qui peuvent être configurés pour envoyer des alertes une fois qu'ils sont dépassés. Les paramètres d'intégrité du système peuvent être localisés à partir de l'interface utilisateur graphique de l'appliance via **System Administration > System Health > Edit Settings** , OU VOUS pouvez exécuter la commande CLI `healthconfig` . Le contrôle d'intégrité du système lui-même peut être exécuté à partir de l'interface utilisateur graphique via **System Administration > System Health > "Run**

System Health Check..." , ou vous pouvez utiliser la commande CLI `healthcheck`.

Note: Consultez le [Guide de l'utilisateur de Cisco AsyncOS for Email](#) pour obtenir des détails complets et une aide à la configuration pour les paramètres d'intégrité du système.

System Health

| Edit System Health Configuration | |
|----------------------------------|----------------------------------------------------------------------------------------------------------------|
| Overall CPU Usage: | Threshold: <input type="text" value="85"/> <input checked="" type="checkbox"/> Alert if exceeds threshold |
| Memory Page Swapping: | Threshold: <input type="text" value="5000"/> <input checked="" type="checkbox"/> Alert if exceeds threshold |
| Maximum Messages in Work Queue: | Threshold: <input type="text" value="500"/> <input checked="" type="checkbox"/> Alert if exceeds threshold |

Figure 1 : Paramètres d'intégrité système par défaut

Lorsque les paramètres sont en place, la valeur est alors représentée sur les graphiques de rapport lorsque vous les affichez via l'interface utilisateur graphique. Par exemple, lorsque vous affichez le **Overall CPU Usage** graphique (Monitor > System Capacity > System Load), vous voyez la ligne rouge qui indique le seuil défini de 85 % :

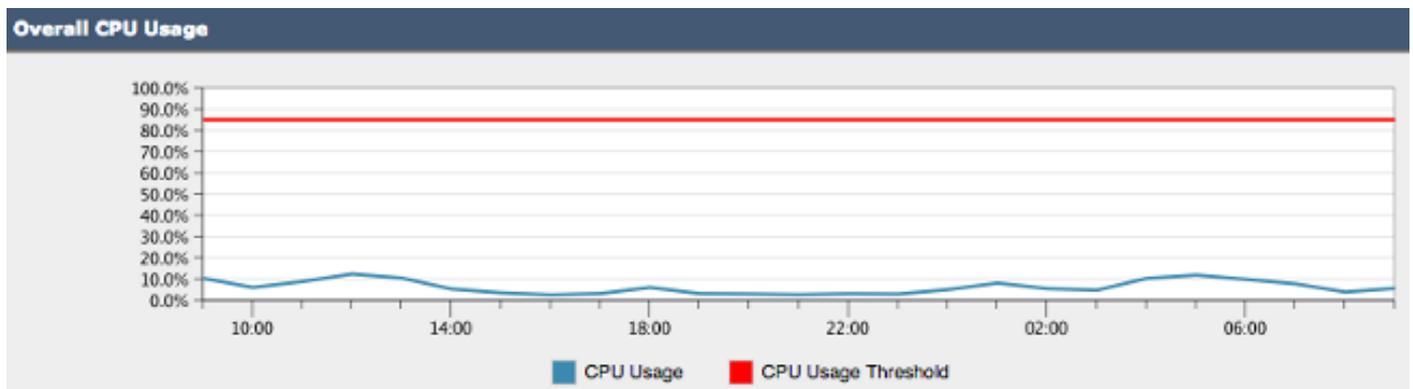


Figure 2 : Exemple d'utilisation globale du CPU

Une fois le seuil franchi et si les alertes sont activées, un message d'information similaire à l'exemple de la Figure 3 est envoyé :

Overall CPU usage is above the configured threshold.

IronPort C100V Alert

Sent: Thursday, April 16, 2015 at 4:36 PM

To: [REDACTED]

The Info message is:

Thu Apr 16 19:36:16 2015 : The CPU usage (85.0761058775%) has exceeded the configured threshold (85%).

Version: 9.5.0-035

Serial Number: [REDACTED]

Timestamp: 16 Apr 2015 19:36:16 -0400

To learn more about alerts, please visit our Knowledge Base. In many cases, you can find further information about this specific alert. Please click the Knowledge Base link after logging into our Support Portal at:

<http://www.cisco.com/cisco/web/support/index.html>

If you desire further information, please contact your support provider.

To open a support request for this issue, access the IronPort C100V and issue the "supportrequest" command. The command sends an email with diagnostic information directly to Cisco IronPort Customer Support to facilitate a rapid diagnosis of the problem.

Thank you.

Figure 3 : Exemple d'e-mail d'alerte pour l'intégrité du système

Vérification de l'intégrité du système

Le contrôle d'intégrité du système est un outil automatisé qui examine l'historique des performances de votre ESA. Il aide à déterminer si la consommation de ressources historiques de la machine lui permet d'effectuer et d'exécuter stable après avoir été mis à niveau vers la version suivante du code. Le contrôle d'intégrité du système est un sous-ensemble des paramètres d'intégrité du système.

Pour les ESA qui exécutent 13.5.1 et les versions antérieures, le contrôle d'intégrité du système est intégré au processus de mise à niveau et s'exécute automatiquement. Le contrôle d'intégrité du système peut être exécuté à tout moment manuellement : **System Administration > System Health > "Run System Health Check..."**

Pour AsyncOS 13.5.2 et versions ultérieures, le contrôle d'intégrité du système n'est plus automatique et doit être exécuté manuellement. Ceci est fait à partir de l'interface utilisateur graphique : Choisir **System Administration > System Health > "Run System Health Check..."** . À partir de l'interface de ligne de commande, exécutez la commande `healthcheck erasecat4000_flash:`

Dans le contrôle d'intégrité, la solution matérielle-logicielle examine les données de performances historiques de l'ESA obtenues à partir des journaux d'état, qui mettent en évidence les problèmes potentiels.

Analyser les problèmes potentiels de mise à niveau

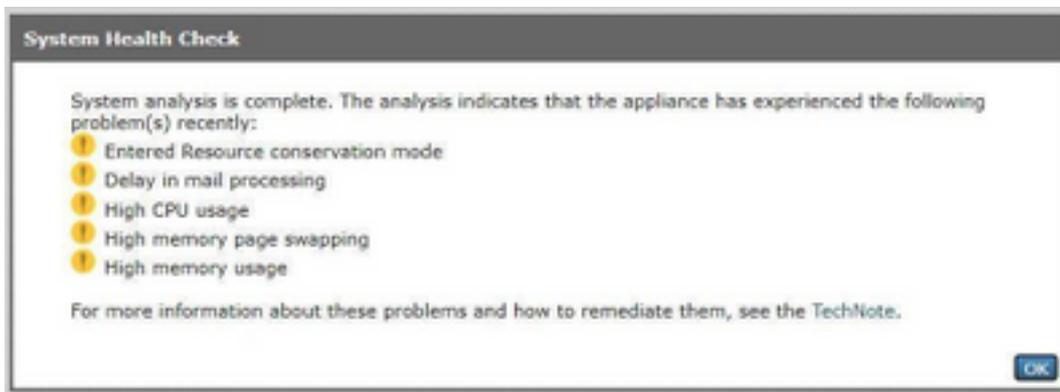


Figure 4 : Outil de contrôle de l'état du système et résultats de l'analyse potentielle

Données analysées par le contrôle d'intégrité du système

Le contrôle d'intégrité du système lit les données historiques du trafic de messagerie à partir des journaux d'état de l'ESA, en particulier les mesures clés répertoriées dans ce tableau :

| Métrique | Seuil | Description |
|---------------------------|-------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| File d'attente de travail | 500 | WorkQ est la mesure de performance clé de l'ESA. WorkQ est une mesure des messages qui attendent dans une <i>file d'attente</i> de <i>travail</i> prioritaire pour analyse par les moteurs de sécurité de l'appliance (c'est-à-dire Antispam, Antivirus, etc.). Lorsque la file d'attente de travail a un historique d'arriéré avec un nombre de 500 en moyenne, la vérification de mise à niveau affiche « Délai dans le traitement du courrier ». Pourcentage de charge processeur ou d'utilisation du processeur : Si le processeur atteint 85 % ou plus de manière cohérente, l'appliance passe en <i>mode Conservation des ressources</i> , qui renvoie le résultat « Mode Conservation des ressources » dans le contrôle d'intégrité. |
| CPULd | 85 | Pourcentage D'Utilisation De La Mémoire Vive : Si la mémoire vive utilisée par l'appliance dépasse 45 % en moyenne, le bilan de santé affiche « Utilisation élevée de la mémoire ». |
| RAMUtil | 45 | SwapThreshold : Numéro dérivé des journaux d'état (SwPgIn + SwPgOut = SwapThreshold). L'outil Contrôle d'intégrité examine ensuite les données du journal d'état historique et calcule un pourcentage d'entrées qui sont supérieures au seuil de page d'échange. Le résultat du contrôle d'intégrité est « Échange de page à mémoire élevée ». |

Note: Pour AsyncOS 11.0.2 pour la sécurité de la messagerie, SwapThreshold est comparé directement à une variable système et non au nombre de pages échangées de la mémoire en une minute, comme décrit. La valeur par défaut de SwapThreshold est 10.

Plan de correction

Un plan de correction peut consister en différentes approches, allant de l'optimisation des filtres de messages à la décision que votre environnement de messagerie pourrait utiliser des appliances supplémentaires pour gérer la charge.

En ce qui concerne l'architecture, n'oubliez pas de profiter de la fonction de gestion centralisée ou de cluster incluse dans votre version du logiciel. La fonctionnalité de cluster est particulièrement utile pour la maintenance d'une architecture de messagerie à haute disponibilité, car elle simplifie

le travail administratif lorsqu'elle copie les paramètres de configuration/modifications de tous les appareils du cluster.

Une liste des ressources permettant de résoudre les problèmes mis en évidence par le contrôle de mise à niveau est disponible dans le tableau.

Le centre d'assistance technique (TAC) de Cisco accueille vos questions et vos idées d'amélioration. N'hésitez pas à lancer un nouveau dossier du TAC Cisco avec la fonction de demande d'assistance de l'ESA (exécutez la `supportrequest`) et aussi via **Contact Technical Support** dans l'interface utilisateur graphique Web.

Résultat du contrôle de mise à niveau

Options de description/correction

| | |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Délai de traitement du courrier | Le délai de traitement des messages, également appelé Sauvegarde de la file d'attente de travail, est généralement résolu lorsque vous analysez votre architecture de messagerie et que vous envisagez d'autres appliances afin de gérer la charge des messages, de configurer la limitation du débit et de limiter les connexions simultanées à l'appliance au niveau de l'écouteur. L'appliance peut également être configurée pour libérer des ressources lorsque vous désactivez certains services, tels que l'antispam pour les messages sortants. |
| Mode de conservation des ressources | En savoir plus sur le mode de conservation des ressources dans ESA FAQ : Qu'est-ce que le mode Conservation des ressources sur l'ESA? . |
| Utilisation élevée de la mémoire | Une utilisation élevée de la mémoire signifie généralement qu'un paramètre de cache tel que le cache LDAP (Lightweight Directory Access Protocol) est configuré plus haut que le paramètre par défaut. Vérifiez les paramètres de seuil sur l'appliance et prenez en compte les valeurs proches des paramètres par défaut. |
| Échange de pages à mémoire élevée | Souvent révélateur de « filtres de messages coûteux », un résultat de « remplacement de pages à mémoire élevée » peut signifier qu'il y a une opportunité d'analyser vos filtres de messages et d'envisager des alternatives pour les filtres qui utilisent une grande quantité de mémoire vive, comme les dictionnaires. |

Conclusion

Si vous avez d'autres questions ou préoccupations concernant le contrôle d'intégrité du système, consultez les [notes de version](#) et le [Guide de l'utilisateur](#) pour connaître la version d'AsyncOS exécutée par votre appareil.

Informations connexes

- [Guides de l'utilisateur final du dispositif de sécurité de la messagerie](#)
- [Support et documentation techniques - Cisco Systems](#)