

Configuración y ejecución de la Comprobación de estado del sistema ESA

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Parámetros de estado del sistema](#)

[Comprobación del estado del sistema](#)

[Analizar posibles problemas de actualización](#)

[Datos analizados por la Comprobación de estado del sistema](#)

[Plan de remediación](#)

[Conclusión](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo configurar los parámetros de estado del sistema y cómo ejecutar la Verificación de estado del sistema en un dispositivo de seguridad Cisco Email Security Appliance (ESA).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

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 tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Parámetros de estado del sistema

Los parámetros de estado del sistema son umbrales establecidos en el dispositivo para monitorear el uso de la CPU, el máximo de mensajes en la cola de trabajo y más. Estos parámetros tienen umbrales que se pueden configurar para enviar alertas una vez que se hayan cruzado. Los parámetros de estado del sistema se pueden localizar desde la GUI del dispositivo a través de **System Administration > System Health > Edit Settings** o puede ejecutar el comando CLI `healthconfig` . La comprobación de estado del sistema puede ejecutarse desde la GUI a través de **System Administration > System Health > "Run System Health Check..."** o puede utilizar el comando CLI

healthcheck.

Nota: Consulte la [guía del usuario de Cisco AsyncOS para correos electrónicos](#) para obtener información detallada y asistencia para la configuración de los parámetros de estado del sistema.

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

Figura 1: Parámetros predeterminados de mantenimiento del sistema

Con los parámetros implementados, el valor se representa en los gráficos de informes cuando se visualiza a través de la GUI. Por ejemplo, al ver el **Overall CPU Usage** grafo (Monitor > System Capacity > System Load), verá la línea roja que indica el umbral establecido del 85%:

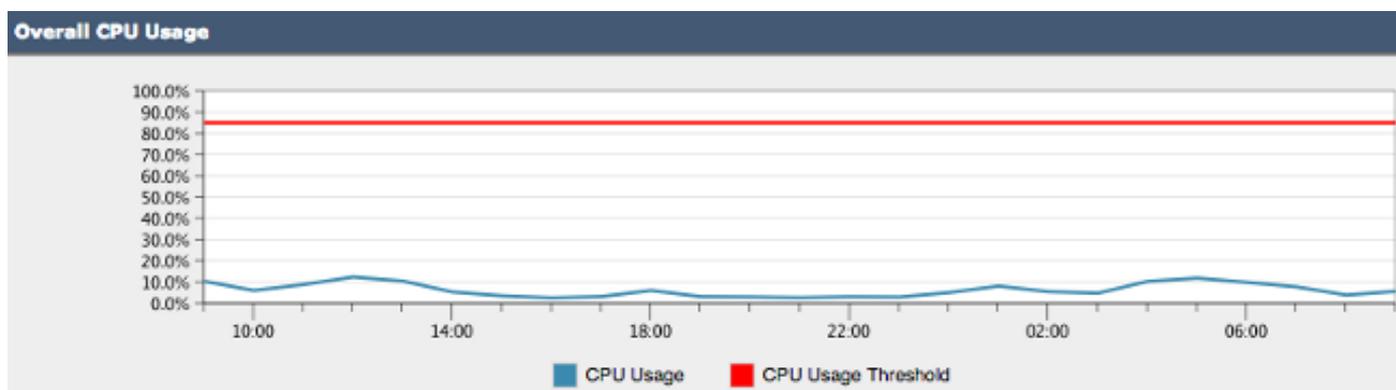


Figura 2: Ejemplo de Uso General de CPU

Después de atravesar el umbral, y si se habilitan las alertas, se envía un mensaje informativo similar al ejemplo de la Figura 3:

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.

Figura 3: Ejemplo de correo electrónico de alerta para el estado del sistema

Comprobación del estado del sistema

La comprobación de estado del sistema es una herramienta automatizada que analiza el historial de rendimiento de su ESA. Ayuda a determinar si el consumo de recursos histórico de la máquina le permite funcionar y ejecutarse estable después de actualizarse a la siguiente versión del código. La comprobación de estado del sistema es un subconjunto de los parámetros de mantenimiento del sistema.

Para el ESA que ejecuta 13.5.1 y revisiones anteriores, la Comprobación de estado del sistema se integra en el proceso de actualización y se ejecuta automáticamente. La comprobación de estado del sistema se puede ejecutar manualmente en cualquier momento: **System Administration > System Health > "Run System Health Check..."**

Para AsyncOS 13.5.2 y posteriores, la comprobación de estado del sistema ya no es automática y debe ejecutarse manualmente. Esto se hace desde la GUI: Elegir **System Administration > System Health > "Run System Health Check..."** . Desde la CLI, ejecute el `healthcheck` comando.

En la comprobación de estado, el dispositivo examina los datos de rendimiento históricos del ESA obtenidos de los registros de estado, lo que pone de relieve los posibles problemas.

Analizar posibles problemas de actualización

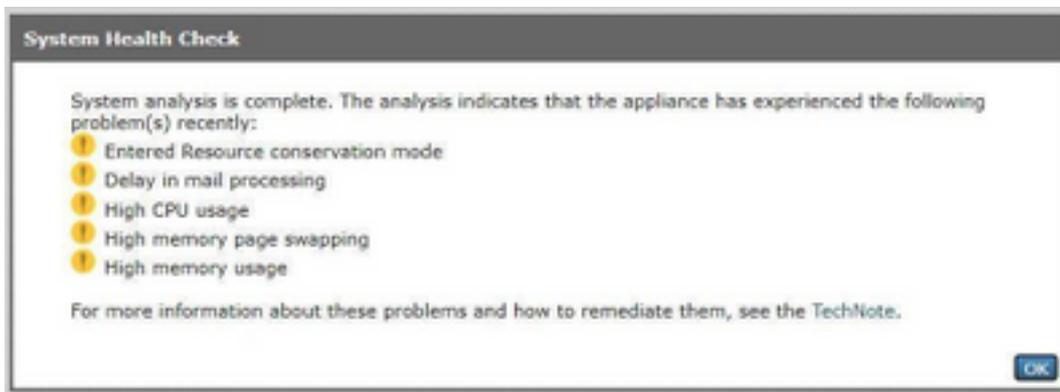


Figura 4: La herramienta de comprobación de estado del sistema y los posibles resultados del análisis

Datos analizados por la Comprobación de estado del sistema

La comprobación de estado del sistema lee los datos históricos del tráfico de correo de los registros de estado del ESA, en particular las métricas clave enumeradas en esta tabla:

Métrico	Umbral	Descripción
Cola de trabajo	500	WorkQ es la métrica clave de medición del rendimiento del ESA. WorkQ es una medida de los mensajes que esperan en una <i>cola de trabajo</i> prioritaria para que los motores de seguridad del dispositivo los analicen (es decir, Antispam, Antivirus, etc.). Cuando la cola de trabajo tiene un historial de un retraso con un recuento de 500 en promedio, la verificación de actualización muestra "Retraso en el procesamiento de correo".
CPULd	85	Porcentaje de carga de CPU o utilización de CPU: Si la CPU alcanza el 85% o más de manera consistente, el dispositivo ingresa al <i>Modo de Conservación de Recursos</i> , que devuelve el resultado "Modo de Conservación de Recursos" en la Verificación de Estado.
RAMUtil	45	Porcentaje De Utilización De Ram: Si la RAM utilizada por el dispositivo supera el 45% en promedio, la comprobación de estado muestra "Uso elevado de la memoria".
Umbral de intercambio	5000	Umbral de intercambio: Un número derivado de los registros de estado ($SwPgIn + SwPgOut = SwapThreshold$). A continuación, la herramienta Comprobación de estado examina los datos del registro de estado histórico y calcula un porcentaje de entradas que superan el umbral de página de intercambio. El resultado de la comprobación de estado es "Intercambio de página de memoria alta".

Nota: Para AsyncOS 11.0.2 para Email Security, SwapThreshold se compara directamente con una variable del sistema y no con el número de páginas intercambiadas desde la memoria en un minuto, como se describe. El valor predeterminado de SwapThreshold es 10.

Plan de remediación

Un plan de remediación puede consistir en diferentes enfoques, desde la optimización de los filtros de mensajes hasta la decisión de que su entorno de correo electrónico podría utilizar dispositivos adicionales para gestionar la carga.

En cuanto a la arquitectura, recuerde aprovechar la función Centralized Management o Cluster incluida con su versión del software. La función Clúster es especialmente beneficiosa en el

mantenimiento de una arquitectura de correo electrónico de alta disponibilidad ya que simplifica el trabajo administrativo cuando copia los ajustes de configuración/cambios en todos los dispositivos del clúster.

En la tabla encontrará una lista de recursos para ayudar a resolver los problemas resaltados por la comprobación de actualización.

El centro de asistencia técnica Cisco Technical Assistance Center (TAC) acoge con satisfacción sus preguntas e ideas para mejorar. No dude en iniciar un nuevo caso de Cisco TAC con la función de solicitud de soporte del ESA (ejecute el `supportrequest` y también a través de `Contact Technical Support` en la GUI web.

Resultado de verificación de actualización

Descripción / Opciones de remediación

Retraso en el procesamiento de correo	La demora en el procesamiento de correo, también conocida como copia de seguridad de cola de trabajo, se resuelve normalmente al analizar su arquitectura de correo electrónico y considerar dispositivos adicionales para manejar la carga de correo, configurar la limitación de velocidad y limitar las conexiones simultáneas al dispositivo en el receptor. El dispositivo también se puede configurar para liberar recursos cuando se desactivan determinados servicios, como antispam para correo saliente.
Modo de conservación de recursos	Lea más acerca del Modo de conservación de recursos en Preguntas frecuentes de ESA: ¿Qué es el modo de conservación de recursos en el ESA?
Uso elevado de memoria	El uso elevado de la memoria significa normalmente que una configuración de caché como la caché del protocolo ligero de acceso a directorios (LDAP) se configura más alta que la predeterminada. Revise la configuración del umbral en el dispositivo y tenga en cuenta los valores cercanos a la configuración predeterminada.
Intercambio de página de alta memoria	A menudo indicativo de "filtros de mensajes caros", un resultado de "Intercambio de páginas de memoria alta" podría significar que hay una oportunidad de analizar los filtros de mensajes y considerar alternativas para los filtros que utilizan una gran cantidad de RAM como diccionarios.

Conclusión

Si tiene preguntas o preocupaciones adicionales sobre la Comprobación de estado del sistema, revise las [Notas de la versión](#) y la [Guía del usuario](#) para ver la versión de AsyncOS que ejecuta su dispositivo.

Información Relacionada

- [Guías de usuario final del dispositivo de seguridad de correo electrónico](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)