ESA System Health Parameters and System Health Check

Contents

Introduction

This document provides a high level overview of the System Health parameters and associated System Health Check on a Cisco Email Security Appliance (ESA).

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on an ESA that runs AsyncOS 9.5 for Email or later.

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. If your network is live, make sure that you understand the potential impact of any command.

System Health Parameters

The System Health parameters are thresholds set on the appliance in order to monitor CPU usage, maximum messages in the workqueue, and so on. These parameters have thresholds that can be configured to send alerts once they are crossed. The System Health parameters can be located from the appliance GUI via **System Configuration > System Health**, or from the CLI command **healthconfig**.

> **Note**: Review the Cisco AsyncOS for Email User Guide, Configuring Threshold for System

Health Parameters, for complete details and configuration assistance.

System Health

Edit System Health Configuration	
Overall CPU Usage:	Threshold: 85 ☑ Alert if exceeds threshold
Memory Page Swapping:	Threshold: 5000 ☑ Alert if exceeds threshold
Maximum Messages in Work Queue:	Threshold: 500 ☑ Alert if exceeds threshold

Cancel   Submit

Figure 1: The System Health Default Parameters

With the parameters in place, the value is then represented on the report graphs when you view via the GUI. For example, when you view the **Overall CPU Usage** graph (**Monitor > System Capacity > System Load)**, you will see the red line that indicates the set 85% threshold:
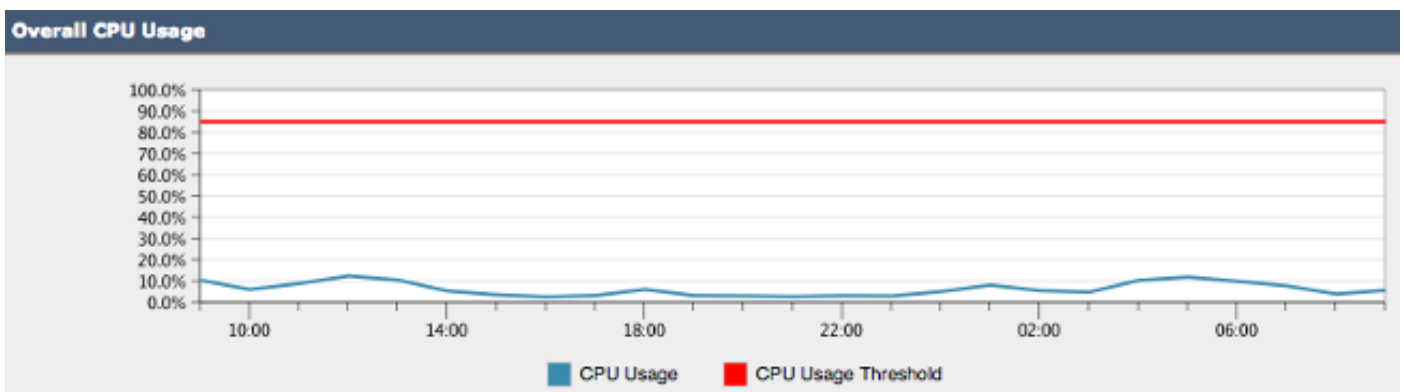

Figure 2: Overall CPU Usage Example

Once the threshold is crossed, and if alerts are enabled, an informational message similar to the example in Figure 3 is sent:

Overall CPU usage is above the configured threshold.

IronPort C100V Alert

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

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:
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: Alert Email Example for System Health

System Health Check

The System Health Check is an automated tool that looks at the performance history of your ESA in order to help determine if the machine's historical resource consumption allows it to perform and run stable once it is upgraded to the next version of code. The System Health Check is a subset of the System Health Parameters. The System Health Check is automatically triggered in an upgrade, but can also be run manually. From the GUI, choose **System Configuration > System Health > "Run System Health Check..."**. From the CLI, enter the **healthcheck** command.

In the health check, the appliance looks at the historical performance data of the ESA obtained from the status logs and calculates an upgrade check result, which highlights potential issues.
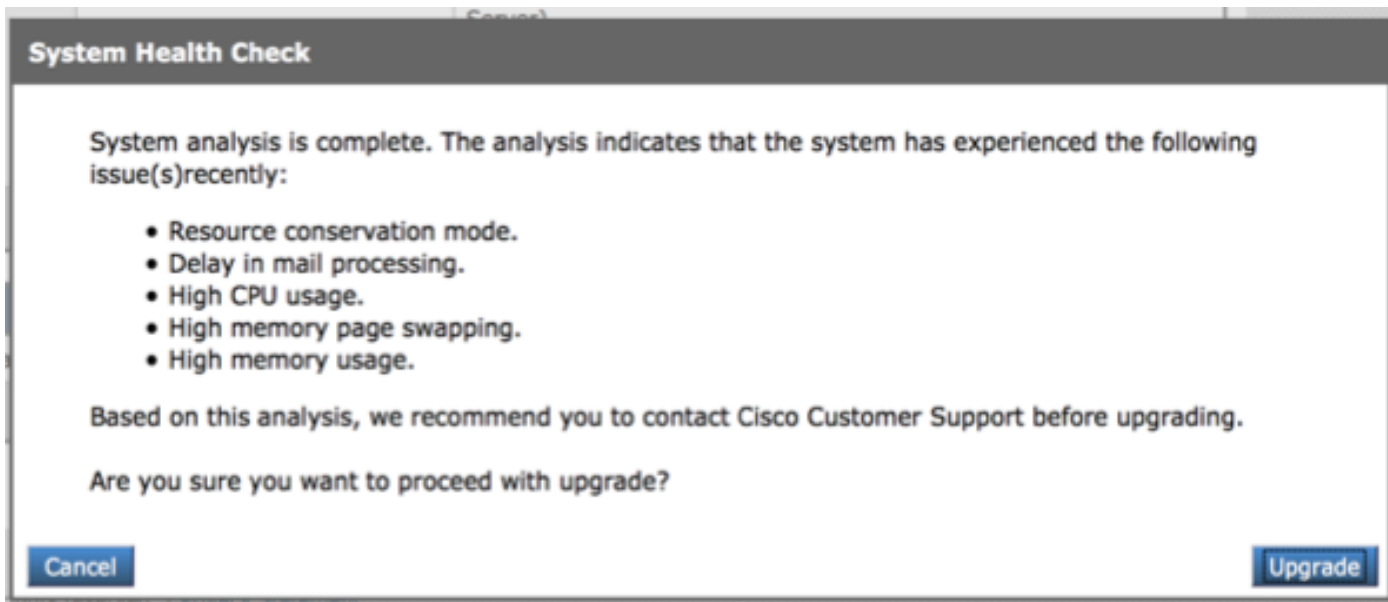
Analyze Potential Upgrade Issues

Figure 4: The System Health Check Tool and Potential Analysis Results

Data analyzed by the System Health Check

The System Health Check reads historical mail traffic data from the status logs of the ESA, particularly the key metrics listed in this table:

Metric	Threshold	Description
WorkQ	500	WorkQ is the key performance measurement metric of the ESA. WorkQ is a measure of the messages that wait in a priority *work queue* for analysis by the security engines of the appliance (that is, Antispam, Antivirus, and so on). Wh the Workqueue has a history of a backlog with a count of 500 on average, the Upgrade Check shows "Delay in mail Processing".
CPULd	85	Percentage CPU Load or CPU Utilization: If the CPU reaches 85% or or more consistently, the appliance goes into *Resource Conservation Mode*, which ret the result "Resource Conservation Mode" in the Health Check.
RAMUtil	45	Percentage Ram Utilization: If the RAM used by the appliance exceeds 45% average, the Health Check displays "High Memory Usage".
SwapThreshold	5000	SwapThreshold: A derived number from the status logs (SwPgIn + SwPgOut SwapThreshold). The Health Check tool then looks at the historical status log and calculates a percentage of entries that are greater than the swap page threshold. The health check result is "High Memory Page Swapping"

Note: For AsyncOS 11.0.2 for Email Security, SwapThreshold is compared directly with a system variable and not the number of pages swapped from memory in a minute, as described. The default SwapThreshold value is 10.

Remediation Plan

A remediation plan can consist of different approaches, from optimization of the message filters to the decision that your email environment could use additional appliances in order to handle the load.

In regards to architecture, remember to take advantage of the Centralized Management or Cluster feature included with your version of the software. The Cluster feature is especially beneficial in

the maintenance of a high availability email architecture, since it simplifies the administrative work when it copies configuration settings/changes to all appliances in the cluster.

A list of resources to help solve the issues highlighted by the Upgrade Check is available in the table.

The Cisco Technical Assistance Center (TAC) welcomes your questions and ideas for improvement. Feel free to initiate a new Cisco TAC case with the support request feature of the ESA (enter the **supportrequest** command) and also via the Web GUI's Help: **Contact Technical Support.**

Upgrade Check Result	Description / Remediation Options
Delay in Mail Processing	Mail Processing Delay, also known as Workqueue Backup, is typically resolved when you analyze your email architecture and consider additional appliances in order to handle mail load, configure rate limiting, and limit concurrent connections to the appliance at the listener. The appliance could also be configured to free up resources when you disable certain services, such as antispam for outbound mail.
Resource Conservation Mode	Read More about Resource Conservation Mode in ESA FAQ: What is Resource Conservation mode on the ESA?.
High memory usage	High memory usage typically means a cache setting such as Lightweight Directory Access Protocol (LDAP) cache is configured higher than the default. Review threshold settings on the appliance and consider staying close to default settings.
High memory page swapping	Often indicative of "expensive message filters", a result of "High memory page swapping" could mean there is an opportunity to analyze your message filters and consider alternatives for filters that utilize a large amount of RAM such as dictionaries.

Related Information

- **Email Security Appliance End User Guides**
- **Technical Support & Documentation - Cisco Systems**