Monitoring Cisco CSS

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The Cisco CSS 11150 content services switch is a compact, high-performance solution for small-to medium-sized Web sites. Featuring Cisco Web Network Services (Web NS) software, the Cisco CSS 11150 enables Web and application service providers, Web content providers, and enterprises engaged in e-commerce to build global Web Networks optimized for e-commerce transactions and Web content delivery. With its patented content switching technology, the Cisco CSS 11150 gives businesses maximum control in ensuring availability of their Web sites, securing Web site resources without compromising performance, and allocating Web site resources efficiently.

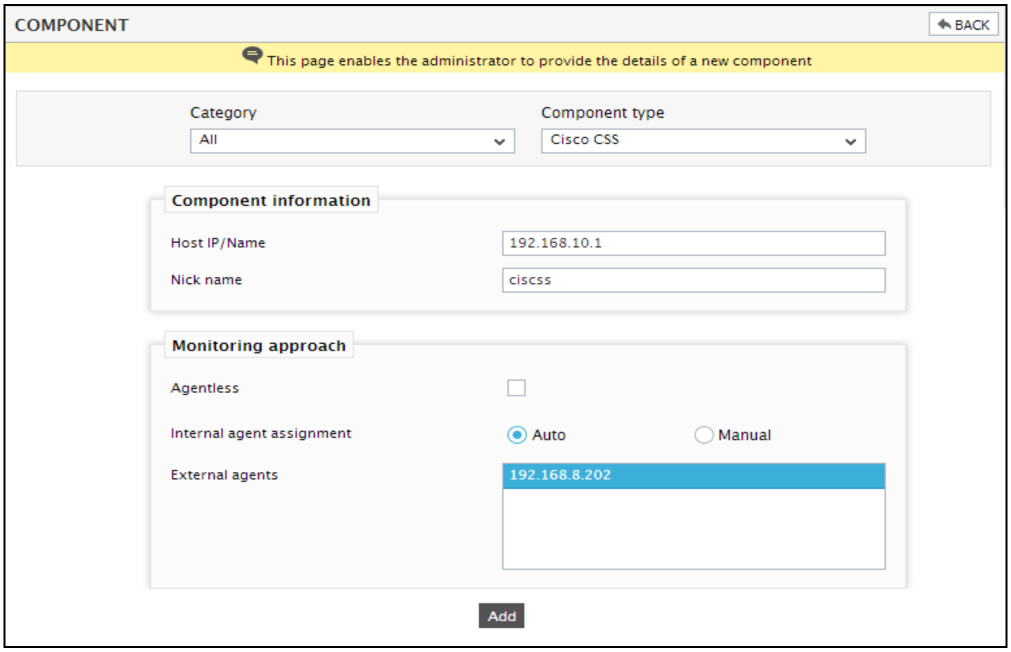
Cisco CSS 11000 series switches learn where specific content resides, either locally or remotely, and dynamically select the best Web server or cache for specific content requests. In a distributed Web site, Cisco CSS 11000 series switches perform comprehensive resource verification before routing user requests, ensuring they are directed to the location that has the best response time and the least load for the requested content. Local server selection is based on server load and application response time, as well as traditional least connections and round-robin algorithms. Global server load balancing is based on Domain Name System (DNS) and proximity by source IP address. Any application that uses standard Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) protocols can also be load-balanced including firewalls, mail, news, chat, and lightweight directory access protocol (LDAP), Simple Network Management Protocol (SNMP), remote monitoring (RMON), and log files.

Glitches in the Cisco CSS' operations can therefore cause serious errors in the load-balancing activity, resulting in requests being routed to slow / heavily loaded locations, and frustrating error messages such as "Server Not Found" becoming common-place! While such aberrations are unwelcome even in less critical environments, the occurrence of these anomalies in mission-critical infrastructures can significantly impact the quality and timely delivery of the important end-user services that overlay these infrastructures. To avoid prolonged service delays or outages, the continuous monitoring of the Cisco CSS is essential. The eG Enterprise Suite helps network administrators for the continuous monitoring of the Cisco CSS.

Chapter 2: Administering the eG Manager to monitor a Cisco CSS

To administer the eG Manager to monitor the Cisco CSS, do the following:

1. Log into the eG administrative interface.
2. eG Enterprise cannot automatically discover the Cisco CSS. You need to manually add the server using the **COMPONENTS** page (see Figure 2.1) that appears when the Infrastructure -> Components -> Add/Modify menu sequence is followed. Remember that components manually added are managed automatically.



COMPONENT

This page enables the administrator to provide the details of a new component

Category: All

Component type: Cisco CSS

Component information

Host IP/Name: 192.168.10.1

Nick name: ciscss

Monitoring approach

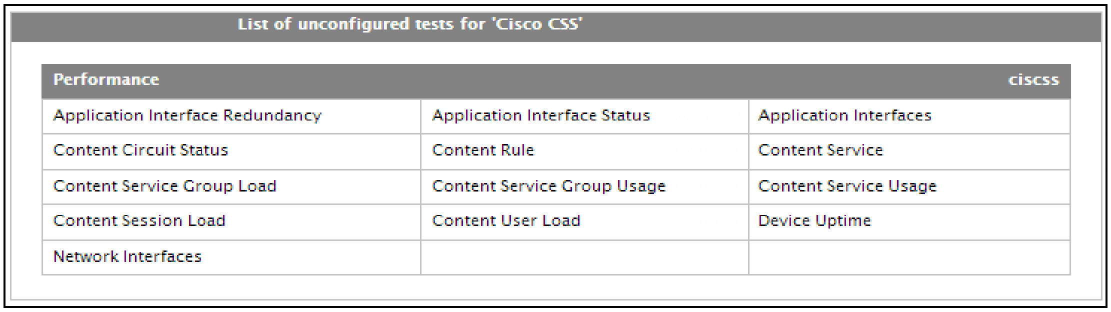
Agentless: □

Internal agent assignment: ● Auto ○ Manual

External agents: 192.168.8.202

Figure 2.1: Adding the Cisco CSS component

3. Specify the **Host IP** and the **Nick name** of the Cisco CSS in Chapter 2. Then click the **Add** button to register the changes. When you attempt to sign out, a list of unconfigured tests appears (see Figure 2.2).



List of unconfigured tests for 'Cisco CSS'

Performance		ciscss
Application Interface Redundancy	Application Interface Status	Application Interfaces
Content Circuit Status	Content Rule	Content Service
Content Service Group Load	Content Service Group Usage	Content Service Usage
Content Session Load	Content User Load	Device Uptime
Network Interfaces		

Figure 2.2: List of tests to be configured for the Cisco CSS component

4. Click on the **Content Session Load** test to configure it. To know how to configure the test, refer to **Monitoring the Cisco CSS**. Then, try to signout of the administrative interface. Now you will be prompted to configure the **Device Uptime** and **Network Interfaces** tests. To know how to configure these tests refer to the *Monitoring Cisco Routers* document.

5. Finally, signout of eG administrative interface.

Chapter 3: Monitoring the Cisco CSS

eG Enterprise provides a specialized *Cisco CSS* monitoring model that monitors the sessions to and services offered by the Cisco CSS, and promptly alerts administrators to deviations (if any) in performance.

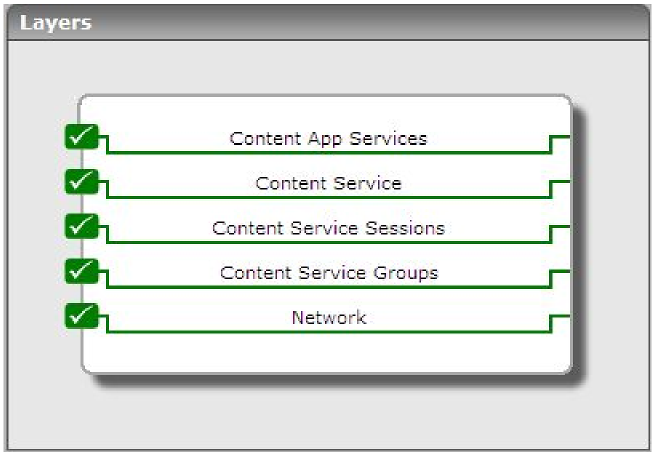


Figure 3.1: The layer model of the Cisco CSS

Every layer of Figure 3.1 is mapped to a wide variety of tests that connect to the SNMP MIB of the Cisco CSS to report useful statistics related to the health of the CSS. Using these metrics, the following questions can be easily answered:

- How many groups have been configured on CSS? Which destination services are associated with each group? What is the current state of each group service? How frequently was the group service accessed?
- Are any groups in a disabled state currently? How many users are currently connected to the enabled groups?
- Is the Cisco CSS overloaded with sessions? Which application IP has generated the maximum session activity on the CSS?
- Which owner frequently accessed the CSS?
- What are the services associated with each owner? How many of these services are currently alive?
- How many services have been configured on the CSS totally? What are they? Are any of these services dying currently? Which service has generated the maximum network traffic?
- Are the services able to process content requests well?

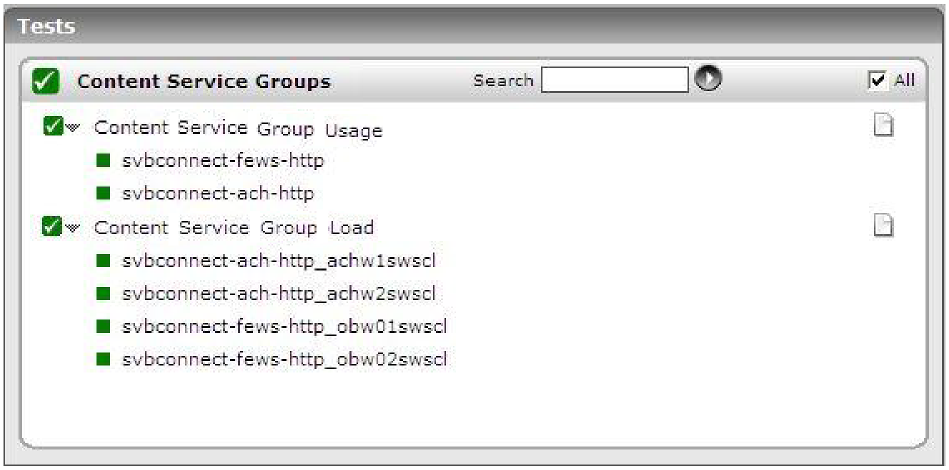
- What are the content rules configured on CSS? What is the current status of each content rule?
- What are the IP interfaces on CSS? Are any of them disabled or waiting for a circuit?
- How many VLAN circuits are configured on CSS?
- Has enough pool memory been allocated to the IP routing table?
- Is the CSS in a redundant state currently? What is the current state of the redundant link? Will the CSS be going into a failover soon?

The sections to come will discuss the top 4 layers of Figure 3.1 only, as the **Network** layer has already been dealt with elaborately in the *Monitoring Cisco Router* document.

3.1 The Content Service Groups Layer

A **Group** represents a collection of local servers that are to be load-balanced. A **service** is a destination location where a piece of content resides physically (a local or remote server and port). Using the tests attached to the **Content Service Groups** layer, you can do the following:

- ➢ Determine the current status of the server groups configured on the Cisco CSS;
- ➢ Analyze the load on the server groups being load balanced by Cisco CSS;
- ➢ Know the current status of each of the services configured for a group;
- ➢ Understand how frequently requests were directed to each of the services.



Tests

☑ Content Service Groups Search ☑ All

☑ Content Service Group Usage
- 🟩 svbconnect-fews-http
- 🟩 svbconnect-ach-http

☑ Content Service Group Load
- 🟩 svbconnect-ach-http_achw1swscl
- 🟩 svbconnect-ach-http_achw2swscl
- 🟩 svbconnect-fews-http_obw01swscl
- 🟩 svbconnect-fews-http_obw02swscl

Figure 3.2: The tests mapped to the Content Service Groups layer

3.1.1 Content Service Group Load Test

As stated earlier, a service is a destination location where a piece of content resides physically (a local or remote server and port). While load-balancing content requests to a server group, the Cisco CSS identifies the location from which the requested content is to be provided using the service definitions on that group. The ContentServiceGroupLoad test reports the current status of the destination services configured for every group, and helps analyze the extent of usage of the service definitions by reporting the number of times each destination service was accessed for content by the Cisco CSS.

Target of the test : A Cisco CSS

Agent deploying the test : An external agent

Outputs of the test : One set of results for every *groupname_destination service* pair discovered by the Cisco CSS.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.

Parameters	Description
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Onlyup	If this flag is set to **Yes**, then only the network interfaces that are operational - i.e. whose MIB-II operStatus variable has a value "up" - are monitored. If this flag is set to **No**, all network interfaces that have an adminStatus of "up" will be monitored.

Parameters	Description
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Group service status	Indicates the current status of this destination service	Boolean	
Group service hits	Indicates the number of times since the last measurement period, user requests to this group load balanced to this service.	Number	This is a good indicator of the usage of the destination service.
Group service data sent	Indicates the number of bytes in transmission, which were source NATted using this destination service on this group, during this measurement period.	Bytes	This is a good indicator of the level of traffic handled by the destination service.

3.1.2 Content Service Group Usage Test

A group, as already explained, represents a collection of local servers that are to be load-balanced. This test auto-discovers the groups configured on CSS, and reports the status and usage of every group in terms of connections handled by the group and data sent by it.

Target of the test : A Cisco CSS

Agent deploying the test : An external agent

Outputs of the test : One set of results for every group load-balanced by the target Cisco CSS.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the

Parameters	Description
	AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Onlyup	If this flag is set to **Yes**, then only the network interfaces that are operational - i.e. whose MIB-II operStatus variable has a value "up" - are monitored. If this flag is set to **No**, all network interfaces that have an adminStatus of "up" will be monitored.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Group status	Indicates the current status of this group.	Number	While the value 0 for this measure indicates that the group is currently disabled, the value 1 indicates that the group is enabled.
No of group data sent	Indicates the number of bytes of group data sent since the last measurement period.	Number	
No of current group connections	Indicates the number of connections established through this group, currently.	Number	
No of total group connections	Indicates the total number of connections for this group during this measurement period.	Number	

3.2 Content Service Sessions Layer

The tests mapped to this layer enable you to keep track of the load on the Cisco CSS by periodically monitoring the sessions and user activity on the device.

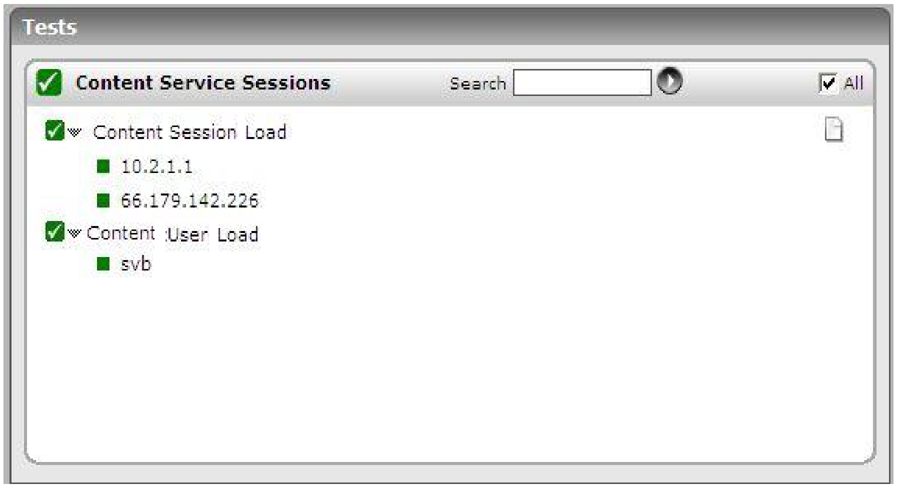


Figure 3.3: The tests mapped to the Content Service Sessions layer

3.2.1 Content Session Load Test

For every application that connects to the Cisco CSS for processing its load-balancing requests, this test reports the load generated on the Cisco CSS and the current state of the session initiated by the application.

Target of the test : A Cisco CSS

Agent deploying the test : An external agent

Outputs of the test : One set of results for every Application IP address served by the target Cisco CSS.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the

Parameters	Description
	SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Onlyup	If this flag is set to **Yes**, then only the network interfaces that are operational - i.e. whose MIB-II operStatus variable has a value "up" - are monitored. If this flag is set to **No**, all network interfaces that have an adminStatus of "up" will be monitored.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.

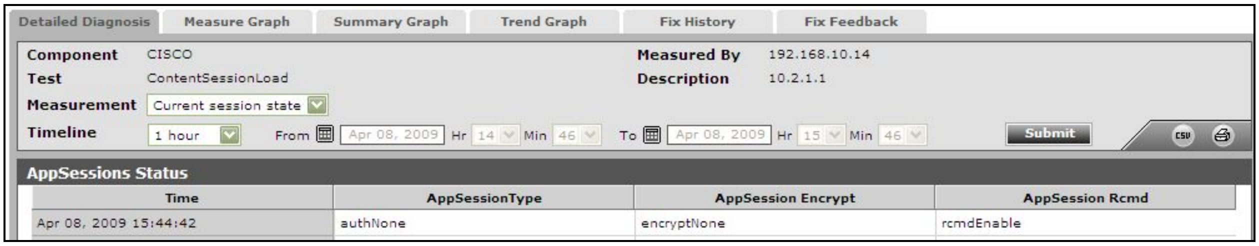
Parameters	Description
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormalfrequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Descrition	Measurement Unit	Interpretation
Application packets received	Indicates the number of application packets received by the CSS from this application IP, since the last measurement period.	Number	These measures are good indicators of the load generated by this application on the Cisco CSS. In the event of a slow-down of the Cisco CSS, you might want to compare the values of these measures across all application Ips to accurately identify the application that coud have overloaded the CSS.
Application packets transmitted	Indicates the number of application packets sent by the CSS to this application IP since the last measurement period.	Number	
Current session	Indicates the current state	Number	A session can be in any one of the

Measurement	Descrition	Measurement Unit	Interpretation
state	of the session initiated by this application.		following states: • 0 – stopped • 1 – Init • 2 – Opened • 3 – Auth • 4 – Up • 5 – Down. The detailed diagnosis of this measure, if enabled, reveals more details about the session.

The detailed diagnosis of the *Current session state* measure, if enabled, reveals more details about the session such as, the authentication type of the session, the encryption type of the session, and whether Rcmd is enabled/disabled for the session.



Component CISCO
Test ContentSessionLoad
Measurement Current session state
Timeline 1 hour From Apr 08, 2009 Hr 14 Min 46 To Apr 08, 2009 Hr 15 Min 46
Measured By 192.168.10.14
Description 10.2.1.1

AppSessions Status

Time	AppSessionType	AppSession Encrypt	AppSession Rcmd
Apr 08, 2009 15:44:42	authNone	encryptNone	rcmdEnable

Figure 3.4: The detailed diagnosis of the Current session state measure

3.2.2 Content User Load Test

This test monitors the owner activity on the Cisco CSS. An owner is generally the person or company who contracts the Web hosting service to host their Web content and allocate bandwidth as required. Rules are configured on the Cisco CSS for every owner indicating which content accessible by the owner and from where it is to be retrieved.

Target of the test : A Cisco CSS

Agent deploying the test : An external agent

Outputs of the test : One set of results for every owner configured on the Cisco CSS.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP

Parameters	Description
	transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Onlyup	If this flag is set to **Yes**, then only the network interfaces that are operational - i.e. whose MIB-II operStatus variable has a value "up" - are monitored. If this flag is set to **No**, all network interfaces that have an adminStatus of "up" will be monitored.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

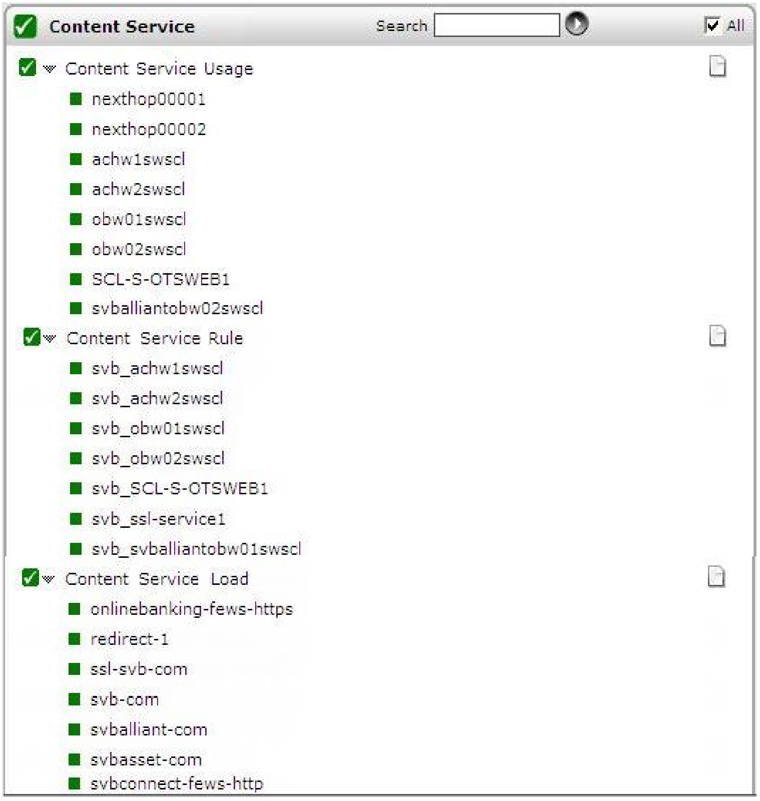
Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Load balancer hits	Indicates the number of	Number	This is a good indicator of the load generated by this owner on the Cisco

Measurement	Description	Measurement Unit	Interpretation
	times during this measurement period the owner accessed the load balancer with requests for content.		CSS.
HTTP redirects sent	Indicates the number of HTTP redirects sent for this owner during this measurement period.	Number	HTTP redirects have long been an option to maintain server stickiness in load-balanced environments. Redirects are very reliable and ensure that an Internet/Intranet client stays on a specific server for the duration of a session. The CSS 11000 allows a network administrator to have the CSS 11000 send the HTTP redirect, which eliminates the need for the Web server administrator to redesign a Web site to accommodate HTTP redirects.
Load balancer drops	Indicates the total number of requests from this owner that were dropped by the load balancer during this measurement period.	Number	Ideally, this value should be low.
Data sent	Indicates the total number of bytes sent for this owner during this measurement period.	Bytes	

3.3 The Content Service Layer

The tests associated with the **Content Service** layer and the measures reported by them provide in-depth insights into the status, load, usage, and overall effectiveness of the destination services configured on a Cisco CSS, and the content rules within which the services are configured.



☑ Content Service Search ☑ All

- ☑ Content Service Usage
  - 🟩 nexthop00001
  - 🟩 nexthop00002
  - 🟩 achw1swscl
  - 🟩 achw2swscl
  - 🟩 obw01swscl
  - 🟩 obw02swscl
  - 🟩 SCL-S-OTSWEB1
  - 🟩 svballiantobw02swscl
- ☑ Content Service Rule
  - 🟩 svb_achw1swscl
  - 🟩 svb_achw2swscl
  - 🟩 svb_obw01swscl
  - 🟩 svb_obw02swscl
  - 🟩 svb_SCL-S-OTSWEB1
  - 🟩 svb_ssl-service1
  - 🟩 svb_svballiantobw01swscl
- ☑ Content Service Load
  - 🟩 onlinebanking-fews-https
  - 🟩 redirect-1
  - 🟩 ssl-svb-com
  - 🟩 svb-com
  - 🟩 svballiant-com
  - 🟩 svbasset-com
  - 🟩 svbconnect-fews-http

Figure 3.5: The tests mapped to the Content Service layer

3.3.1 Content Service Usage Test

This test reports critical statistics indicating the current status and extent of usage of the content providing services on a Cisco CSS. As already mentioned, a service is a destination location where a piece of content resides physically (a local or remote server and port).

Target of the test : A Cisco CSS

Agent deploying the test : An external agent

Outputs of the test : One set of results for every service configured on the Cisco CSS.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.

Parameters	Description
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG

Parameters	Description
	agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Onlyup	If this flag is set to **Yes**, then only the network interfaces that are operational - i.e. whose MIB-II operStatus variable has a value "up" - are monitored. If this flag is set to **No**, all network interfaces that have an adminStatus of "up" will be monitored.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Service state	Indicates the current state of this service.	Number	The value of this measure can be any one of the following: • 1 – Suspended • 2 – Down • 4 - Alive

Measurement	Description	Measurement Unit	Interpretation
			- 5 – Dying
Service enabled	Indicates whether this service is currently enabled or not.	Boolean	The value 0 for this measure indicates that the service is disabled. The value 1 on the other hand implies that the service is enabled.
Service avg min bandwidth	Indicates the average minimum data sent through this service.	Bytes	
Service total bandwidth	Indicates the total data sent through this service.	Bytes	This measure is a good indicator of the network traffic generated through this service.
Max service connections	Indicates the maximum number of connections permissible to this service.	Number	
Total service connections	Indicates the total number of connections to this service during this measurement period.	Number	Ideally, this value should be less than the Max service connections measure.
Average service load	Indicates the number of content requests serviced by this service during this measurement period.	Number	This is a good indicator of the workload and content processing ability of the service.
Service status	Indicates the current status of this service.	Number	The value of this measure can be any one of the following: - 1 – Suspended - 2 – Down - 4 - Alive - 5 – Dying

3.3.2 Content Service Test

A content rule is a hierarchical rule set containing individual rules that describe which content (for example, .html files) is accessible by visitors to the Web site, how the content is mirrored, on which server the content resides, and how the CSS should process requests for the content. Each rule set must have an owner.

The CSS uses content rules to determine:

- Where the content physically resides, whether local or remote
- Where to direct the request for content (which service or services)
- Which load balancing method to use

Owners can have multiple content rules. For each service discovered from the content rules associated with an owner, this test reports the current status of the service and whether the service has been effectively utilized or not.

Target of the test : A Cisco CSS

Agent deploying the test : An external agent

Outputs of the test : One set of results for every *owner_service* pair discovered from the content rules configured on the Cisco CSS .

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the

Parameters	Description
	required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.

Parameters	Description
Confirm Password	Confirm the encryption password by retyping it here.
Onlyup	If this flag is set to **Yes**, then only the network interfaces that are operational - i.e. whose MIB-II operStatus variable has a value "up" - are monitored. If this flag is set to **No**, all network interfaces that have an adminStatus of "up" will be monitored.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
No of Content service hits	Indicates the number of times during this measurement period requests from this owner were served by this service.	Number	This measure is a good indicator of the effectiveness of the service.
Content service data sent	Indicates the amount of data sent through this service for this owner during this measurement period.	Bytes	This measure is a good indicator of the network traffic generated through this service.
Content service status	Indicates the current status of this service	Number	
Content service state	Indicates the current state of this service.	Number	The value of this measure can be any one of the following: • 1 – suspended • 2 - up • 4 - alive

3.3.3 Content Rule Test

A content rule is a hierarchical rule set containing individual rules that describe which content (for example, .html files) is accessible by visitors to the Web site, how the content is mirrored, on which server the content resides, and how the CSS should process requests for the content. Each rule set must have an owner.

The CSS uses content rules to determine:

- Where the content physically resides, whether local or remote
- Where to direct the request for content (which service or services)
- Which load balancing method to use

This test auto-discovers the content rules configured on a CSS, and reports the current status and usage patterns pertaining to every content rule.

Target of the test : A Cisco CSS

Agent deploying the test : An external agent

Outputs of the test : One set of results for every content rule discovered on the Cisco CSS.

Configurable parameters for the test

Parameters	**Description**
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote

Parameters	Description
	SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard

Parameters	Description
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Onlyup	If this flag is set to **Yes**, then only the network interfaces that are operational - i.e. whose MIB-II operStatus variable has a value "up" - are monitored. If this flag is set to **No**, all network interfaces that have an adminStatus of "up" will be monitored.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

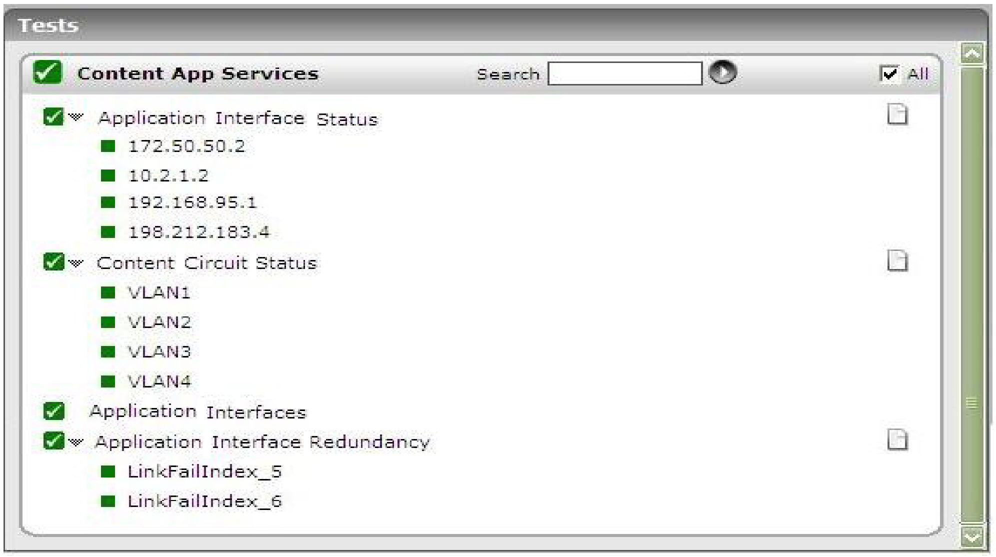
Measurement	Description	Measurement Unit	Interpretation
Content status	Indicates the current status of this content rule.	Number	If the value of this measure is , it indicates that the content rule is enabled. The value 0 on the other hand indicates that the content rule is disabled.
Content hits count	Indicates the number of user requests during this measurement period that invoked this content rule.	Bytes	Ideally, the value of this measure should be high.
Content drops count	Indicates the number of times the content rule was not able to establish a connection during this measurement period.	Number	Ideally, this value should be low.
Content byte count	Indicates the number of bytes of data that passed through this content rule	Number	

Measurement	Description	Measurement Unit	Interpretation
	during this measurement period.		

3.4 The Content App Services Layer

A circuit on the CSS is a logical entity that maps IP interfaces to a logical port or group of logical ports, for example, a VLAN. Each VLAN circuit requires an IP address. Assigning an IP address to each VLAN circuit allows the CSS to route Ethernet interfaces (ports) from VLAN to VLAN.

The tests mapped to the **Content App Services** layer reports key statistics related to the performance of the circuits and IP interfaces configured on CSS.


Tests

☑ Content App Services   Search [   ]   ☑ All

☑ Application Interface Status
- 172.50.50.2
- 10.2.1.2
- 192.168.95.1
- 198.212.183.4

☑ Content Circuit Status
- VLAN1
- VLAN2
- VLAN3
- VLAN4

☑ Application Interfaces

☑ Application Interface Redundancy
- LinkFailIndex_5
- LinkFailIndex_6

Figure 3.6: The tests mapped to the Content App Services layer

3.4.1 Application Interface Status Test

This test reports the current status of each IP interface on CSS.

Target of the test : A Cisco CSS

Agent deploying the test : An external agent

Outputs of the test : One set of results for every IP interface on CSS.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP

Parameters	Description
	transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Onlyup	If this flag is set to **Yes**, then only the network interfaces that are operational - i.e. whose MIB-II operStatus variable has a value "up" - are monitored. If this flag is set to **No**, all network interfaces that have an adminStatus of "up" will be monitored.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Interface state	Indicates the current state of this interface.	Number	The value that this measure can report and the states they represent are

Measurement	Description	Measurement Unit	Interpretation
			discussed below: • 1 – Active • 2 – Disabled • 3 – Nocircuit; this implies that the interface is waiting for an underlying circuit.
Interface redirects enabled	Indicates whether redirects are enabled or not for this interface.	Boolean	The value of this measure indicates whether or not the interface enables the transmission of ICMP packets. If the transmission is enabled, then the value of this measure will be 1. If not, then this measure will return the value 2.
Interface status	Indicates the current status of this interface.	Number	

3.4.2 Content Circuit Status Test

This test reports the current status of each VLAN circuit configured on CSS.

Target of the test : A Cisco CSS

Agent deploying the test : An external agent

Outputs of the test : One set of results for every VLAN circuit configured on CSS.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in

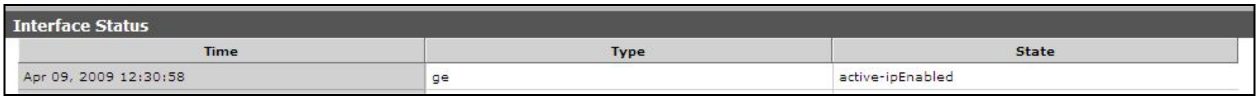
Parameters	Description
	your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the

Parameters	Description
	Yes option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Onlyup	If this flag is set to **Yes**, then only the network interfaces that are operational - i.e. whose MIB-II operStatus variable has a value "up" - are monitored. If this flag is set to **No**, all network interfaces that have an adminStatus of "up" will be monitored.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Interface type	Indicates the type of interface associated with this circuit.	Number	The values that this measure can take and the types they denote are available below: • 6 - Ethernet • 18 - ds1 • 22 – console • 23 - ppp • 30 - ds3 • 32 - frameRelay • 81 - ds0 • 82 - ds0Bundle • 108 - pppMultilink • 117 - ge (Gigabit Ethernet Interface) • 1000 – tunnel and • 1001 - Vlan The detailed diagnosis of this measure provides additional details about this circuit.
Logical link count	Indicates the total number of logical links configured for this circuit.	Number	

The detailed diagnosis of the *Interface type* measure indicates what the value of the measure stands for, and also indicates the current state of the circuit.



Interface Status

Time	Type	State
Apr 09, 2009 12:30:58	ge	active-ipEnabled

Figure 3.7: The detailed diagnosis of the Interface type measure

3.4.3 Application Interfaces Test

The CSS forwards VLAN circuit traffic to the IP interface. The IP interface passes the traffic to the IP forwarding function where the CSS compares the destination of each packet to information contained in the routing table. The routing table typically contains the output interface and the next-hop address. Once the CSS resolves the packet addresses, it forwards the packet to the appropriate VLAN and destination port.

This test reports useful statistics related to the VLAN-VLAN communication that CSS enables via the IP interfaces configured on it.

Target of the test : A Cisco CSS

Agent deploying the test : An external agent

Outputs of the test : One set of results for the CSS monitored.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote

Parameters	Description
	SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard

Parameters	Description
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Onlyup	If this flag is set to **Yes**, then only the network interfaces that are operational - i.e. whose MIB-II operStatus variable has a value "up" - are monitored. If this flag is set to **No**, all network interfaces that have an adminStatus of "up" will be monitored.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
No of reachable routes	Indicates the current number of reachable routes.	Number	
Total no of reachable routes	Indicates the total number of reachable routes during this measurement period.	Number	
No of reachable hosts	Indicates the number of hosts that are currently reachable.	Number	
Total no of reachable hosts	Indicates the total number of reachable hosts during this measurement period.	Number	
Pool memory	Indicates the total amount of memory in bytes allocated for the IP routing table.	Bytes	When there are no additional free entries in the memory pool, more memory is allocated to the pool.

Measurement	Description	Measurement Unit	Interpretation
Redundant state	Indicates the current redundancy state of the monitored CSS.	Number	If this measure reports the value 1, it indicates the 'Init' state. The value 2 on the other hand, indicates the 'Backup' state.
Total alive uplinks	Indicates the number of alive uplinks during this measurement period.	Number	Within a redundant configuration, CSS allows you to create one/more uplink services with a router's IP address. An uplink service enables the master CSS to monitor the router with a keepalive (ICMP). If the keepalive fails, the master relinquishes control and the backup CSS takes control. The master CSS uses all redundancy uplinks when making the failover decision. If the value of this measure is 0, it indicates that there are no live uplink services. In such a case, the CSS goes into failover.

3.4.4 Application Interface Redundancy Test

CSSs participate in a redundant configuration when a physical redundancy link has been defined between the CSSs. The CSSs use this link to maintain contact and activity status with one another. If the physical link goes down, the master CSS fails over to the backup CSS.

This test monitors the status of the redundancy links configured on a CSS.

Target of the test : A Cisco CSS

Agent deploying the test : An external agent

Outputs of the test : One set of results for every redundancy link on the CSS monitored.

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed

Parameters	Description
Host	The IP address of the host for which this test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPVersion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPVersion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version 3 (SNMPv3) is an extensible SNMP Framework which supplements the SNMPv2 Framework, by additionally supporting message security, access control, and remote SNMP configuration capabilities. To extract performance statistics from the MIB using the highly secure SNMP v3 protocol, the eG agent has to be configured with the required access privileges – in other words, the eG agent should connect to the MIB using the credentials of a user with access permissions to be MIB. Therefore, specify the name of such a user against this parameter.
Context	This parameter appears only when v3 is selected as the SNMPVersion. An SNMP context is a collection of management information accessible by an SNMP entity. An item of management information may exist in more than one context and an SNMP entity potentially has access to many contexts. A context is identified by the SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
AuthPass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm Password	Confirm the AuthPass by retyping it here.
AuthType	This parameter too appears only if **v3** is selected as the SNMPversion. From the AuthType list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm

Parameters	Description
	- **SHA** – Secure Hash Algorithm
EncryptFlag	This flag appears only when **v3** is selected as the SNMPVersion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the EncryptType list. SNMP v3 supports the following encryption types: - **DES** – Data Encryption Standard - **AES** – Advanced Encryption Standard
EncryptPassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
Timeout	Specify the duration (in seconds) within which the SNMP query executed by this test should time out in this text box. The default is 10 seconds.
Data Over TCP	By default, in an IT environment, all data transmission occurs over UDP. Some environments however, may be specifically configured to offload a fraction of the data traffic – for instance, certain types of data traffic or traffic pertaining to specific components – to other protocols like TCP, so as to prevent UDP overloads. In such environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Redundant link status	Indicates the current status of this redundant link.	Boolean	While the value 1 indicates that the link is up, the value 0 indicates that it is down. There are two main conditions detected on this redundancy link that drive master and backup states on the CSSs:

Measurement	Description	Measurement Unit	Interpretation
			• The first condition is maintaining the heartbeat, which is an advertisement every second. The master CSS provides this heartbeat on the redundancy link, and the backup CSS keeps track of the heartbeat every three seconds (default). If the heartbeat times out (for example, heartbeats are not detected in this period), then link goes down and the backup takes over as master. • The second condition is that of a VRRP switch priority change. The CSS advertising the highest priority is negotiated to become master. This is the mechanism used by the uplink services, and some of the special commands (described below) for initiating a failover event.

About eG Innovations

eG Innovations provides intelligent performance management solutions that automate and dramatically accelerate the discovery, diagnosis, and resolution of IT performance issues in on-premises, cloud and hybrid environments. Where traditional monitoring tools often fail to provide insight into the performance drivers of business services and user experience, eG Innovations provides total performance visibility across every layer and every tier of the IT infrastructure that supports the business service chain. From desktops to applications, from servers to network and storage, from virtualization to cloud, eG Innovations helps companies proactively discover, instantly diagnose, and rapidly resolve even the most challenging performance and user experience issues.

eG Innovations is dedicated to helping businesses across the globe transform IT service delivery into a competitive advantage and a center for productivity, growth and profit. Many of the world's largest businesses use eG Enterprise to enhance IT service performance, increase operational efficiency, ensure IT effectiveness and deliver on the ROI promise of transformational IT investments across physical, virtual and cloud environments.

To learn more visit www.eginnovations.com.

Contact Us

For support queries, email support@eginnovations.com.

To contact eG Innovations sales team, email sales@eginnovations.com.