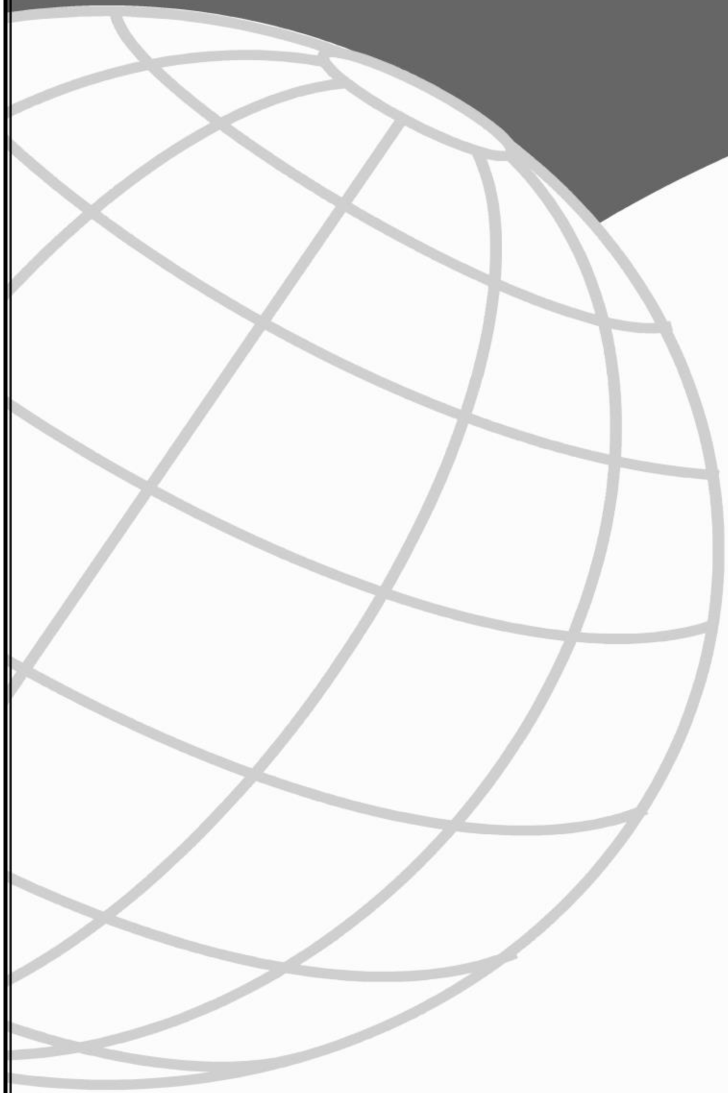


Enabling Service Excellence

Monitoring Bluecoat AV

eG Enterprise v6.0

Restricted Rights Legend

The information contained in this document is confidential and subject to change without notice. No part of this document may be reproduced or disclosed to others without the prior permission of eG Innovations, Inc. eG Innovations, Inc. makes no warranty of any kind with regard to the software and documentation, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose.

Trademarks

Microsoft Windows, Windows NT, Windows 2003, and Windows 2000 are either registered trademarks or trademarks of Microsoft Corporation in United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Copyright

Table of Contents

Chapter

1

Monitoring the Bluecoat AV

Blue Coat AV prevents viruses, trojans, worms, and spyware from entering your organization via the Web. Gateway anti-virus scanning secures rogue channels such as personal Web email and Web downloads.

This means that if the Bluecoat AV malfunctions, it can expose your mission-critical environment to malicious virus attacks that can cause significant data loss. To prevent this, the Bluecoat AV has to be monitored at all times.

eG Enterprise presents 100% web-based *Bluecoat AntiVirus* monitoring model that can promptly alert you to a sudden non-availability of the anti-virus or excessive resource usage by the anti-virus.

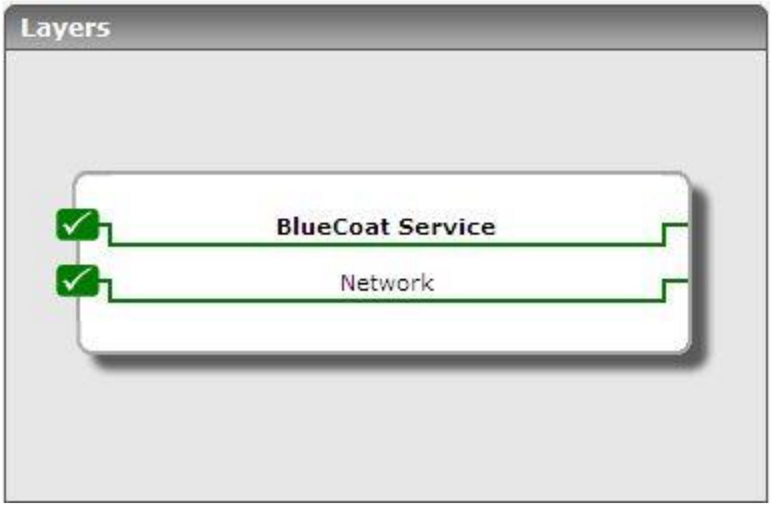


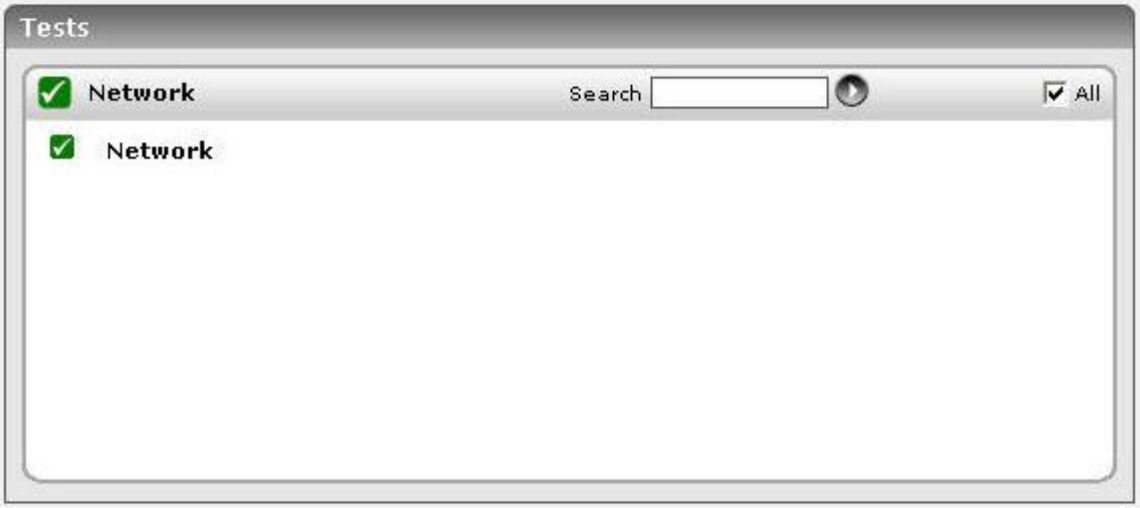
Figure 1.1: Layer model of Bluecoat AV

Each layer of Figure 1.1 is mapped to a set of tests that reports a variety of metrics that can provide accurate answers to the following performance queries:

- Is Bluecoat AV available over the network?
- Have any infected files been detected?
- Is the Bluecoat AV utilizing resources excessively? If so, which resource is it?

1.1 The Network Layer

This layer monitors the availability of the Bluecoat AV over the network, and alerts you to bad network connections (if any) to the anti-virus.



Tests

☑ Network Search ☑ All

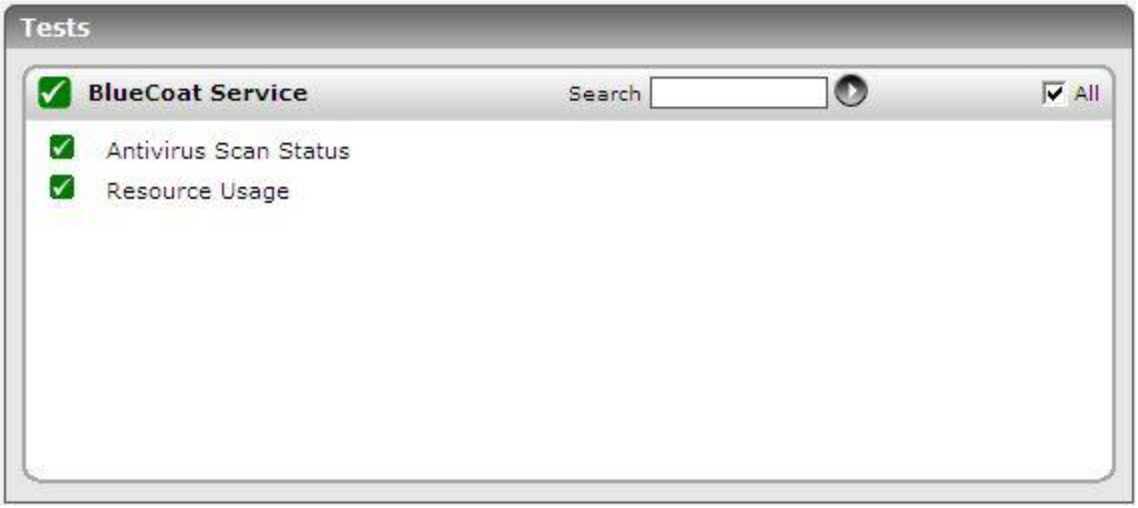
☑ Network

Figure 1.2: The test mape to he Network layer

Since this test has been dealt with elaborately in the *Monitoring Unix and Windows Servers* document, let us proceed to the next layer.

1.2 The Bluecoat Service Layer

This layer measures the overall efficiency of the Bluecoat AV in isolating virus infected files, and also reveals how resource-efficient the anti-virus is.



Tests

☑ BlueCoat Service Search ☑ All

☑ Antivirus Scan Status

☑ Resource Usage

Figure 1.3: The test mapped to the BlueCoat Service layer

1.2.1 Antivirus Scan Status Test

This test measures the effectiveness of the Bluecoat AV software in isolating file infections.

Purpose	Measures the effectiveness of the Bluecoat AV software in isolating file infections
Target of the test	Bluecoat AV
Agent deploying the test	A remote agent

Configurable parameters for the test	1. **TEST PERIOD** - how often should the test be executed 2. **HOST** – The IP address of the Cisco Router. 3. **SNMPPORT** - The port number through which the Cisco router exposes its SNMP MIB. The default value is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the Cisco router. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here.

	14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds. 15. **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 equalizer over TCP (and not UDP). For this, set the **DATA OVER TCP** flag to **Yes**. By default, this flag is set to **No**.		
Outputs of the test	One set of results for Bluecoat AV being monitored.		
Measurements made by the test	**Measurement**	**Measurement Unit**	**Interpretation**
	Number of files scanned: Indicates the number of files scanned by Bluecoat AV for virus attacks.	Number	
	Number of files infected: Indicates the number of files infected.	Number	Ideally, the value of this measure should be 0. A non-zero value indicates the existence of one/more viruses on the target host.

1.2.2 Resource Usage Test

This test reveals whether the Bluecoat AV is utilizing each of the resources available to it optimally.

Purpose	Reveals whether the Bluecoat AV is utilizing each of the resources available to it optimally
Target of the test	Bluecoat AV
Agent deploying the test	A remote agent

Configurable parameters for the test	1. **TEST PERIOD** - how often should the test be executed 2. **HOST** – The IP address of the Cisco Router. 3. **SNMPPORT** - The port number through which the Cisco router exposes its SNMP MIB. The default value is 161. 4. **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. 5. **SNMPCOMMUNITY** – The SNMP community name that the test uses to communicate with the Cisco router. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **SNMPVERSION** chosen is **v3**, then this parameter will not appear. 6. **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 the **USERNAME** parameter. 7. **AUTHPASS** – Specify the password that corresponds to the above-mentioned **USERNAME**. This parameter once again appears only if the **SNMPVERSION** selected is **v3**. 8. **CONFIRM PASSWORD** – Confirm the **AUTHPASS** by retyping it here. 9. **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 10. **ENCRYPTFLAG** – This flag appears only when **v3** is selected as the **SNMPVERSION**. By default, the eG agent does not encrypt SNMP requests. Accordingly, the **ENCRYPTFLAG** is set to **NO** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **YES** option. 11. **ENCRYPTTYPE** – If the **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 12. **ENCRYPTPASSWORD** – Specify the encryption password here. 13. **CONFIRM PASSWORD** – Confirm the encryption password by retyping it here. 14. **TIMEOUT** - Specify the duration (in seconds) within which the SNMP query executed by this test should time out in the **TIMEOUT** text box. The default is 10 seconds.

<table>
<tr><td></td><td colspan="3">15. <b>DATA OVER TCP –</b> 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 equalizer over TCP (and not UDP). For this, set the <b>DATA OVER TCP</b> flag to <b>Yes</b>. By default, this flag is set to <b>No</b>.</td></tr>
<tr><td><b>Outputs of the test</b></td><td colspan="3">One set of results for each resource available to the Bluecoat AV</td></tr>
<tr><td><b>Measurements made by the test</b></td><td><b>Measurement</b></td><td><b>Measurement Unit</b></td><td><b>Interpretation</b></td></tr>
<tr><td></td><td><b>Resource usage</b>:
Indicates the status of usage of this resource.</td><td></td><td>The states reported by this measure and the numeric values that correspond to the states are as follows:
<table>
<tr><th>State</th><th>Numeric Value</th></tr>
<tr><td>Normal</td><td>1</td></tr>
<tr><td>Usage High</td><td>2</td></tr>
</table>
<b>Note:</b>
By default, this measure reports the <b>States</b> listed in the table above to indicate the status of a resource. The graph of this measure however, represents the status using the numeric equivalents - <i>1 or 2</i>.</td></tr>
<tr><td></td><td><b>Resource utilization</b>:
Indicates the percent utilization of this resource.</td><td>Percent</td><td>A high value is indicative of excessive utilization of the corresponding resource. For instance, if the resource is 'CPU', then a high value indicates high CPU usage.</td></tr>
</table>

Chapter

2

Conclusion

This document has clearly explained how eG Enterprise monitors the Bluecoat AV. For more information on eG Enterprise, please visit our web site at www.eginnovations.com or write to us at sales@eginnovations.com.