Monitoring Unitrend Enterprise Backup Server

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

Unitrend Enterprise Backup offers businesses an efficient and reliable solution to automate regular backups and offers great protection for data and systems residing on virtual, physical and cloud-based infrastructure.

In virtualized IT / cloud based infrastructures providing mission-critical services to end-users, an efficient backup and restore mechanism is necessary for ensuring that critical servers that are involved in the delivery of a service do not suffer any data loss. Unitrend Enterprise Backup servers are becoming very crucial to the normal functioning of such infrastructures. If the backup service of the server fails, or consumes too much time to backup or restore the data of one/more key infrastructure components, these components might not be able to function properly until such time that all its data is restored to it. This in turn could have a disastrous effect on the service delivery. If such an outcome is to be prevented, the Unitrend Enterprise Backup server needs to be closely monitored. This is where eG Enterprise lends helping hands to administrators.

Chapter 2: How does eG Enterprise Monitor Unitrend Enterprise Backup Server?

eG Enterprise monitors the Unitrend Enterprise Backup server in both agent-based and agentless manners.

2.1 Managing the Unitrend Enterprise Backup Server

The eG Enterprise cannot automatically discover the Unitrend Enterprise Backup server. Therefore, you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To manage a Unitrend Enterprise Backup component, do the following:

1. Log into the eG administrative interface.
2. Follow the Components -> Add/Modify menu sequence in the **Infrastructure** tile of the **Admin** menu.
3. In the **COMPONENT** page that appears next, select *Unitrend Enterprise Backup* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

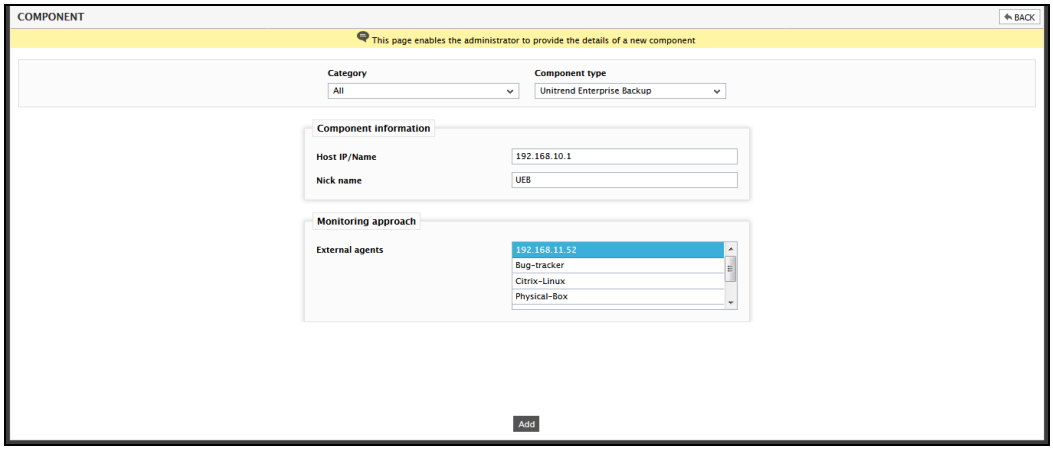
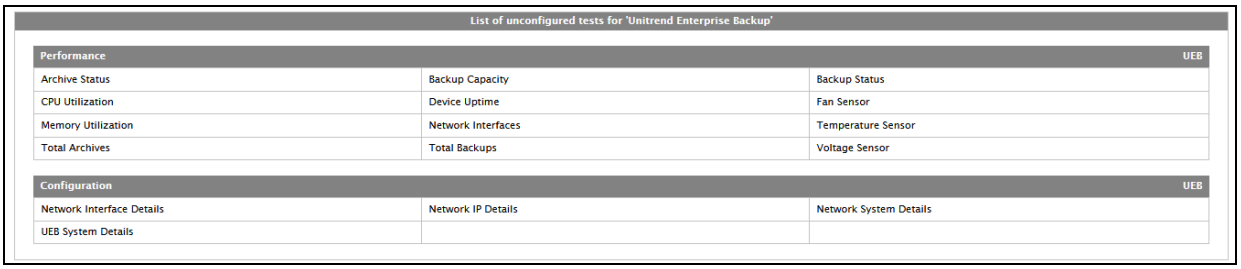


Figure 2.1: Adding a new Unitrend Enterprise Backup server

4. Specify the **Host IP/Name** and **Nick name** for the Unitrend Enterprise Backup server. Then, click on the **Add** button to register the changes.
5. Now, when you attempt to sign out of the eG administrative interface, Figure 2.2 appears, listing the tests that need to be configured for this component.


List of unconfigured tests for 'Unitrend Enterprise Backup'

Performance		UEB
Archive Status	Backup Capacity	Backup Status
CPU Utilization	Device Uptime	Fan Sensor
Memory Utilization	Network Interfaces	Temperature Sensor
Total Archives	Total Backups	Voltage Sensor

Configuration		UEB
Network Interface Details	Network IP Details	Network System Details
UEB System Details		

Figure 2.2: The list of unconfigured tests

6. Click on any test in the list of unconfigured tests (see Figure 2.2) to configure it. To know how to configure these tests, refer to **Monitoring the Unitrend Enterprise Backup Server**.
7. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the Unitrend Enterprise Backup Server

eG Enterprise offers an exclusive Unitrend Enterprise Backup server monitoring model (see Figure 3.1), which keeps tabs on the backup and restore operations performed by the server, and reports deviations much before they impact the performance of the server as a whole, or the dependent service.

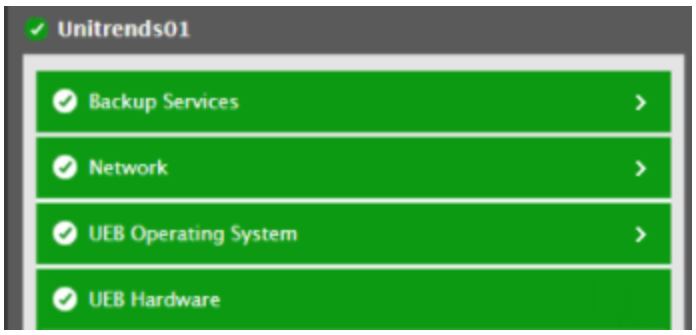


Figure 3.1: The layer model of the Unitrend Enterprise Backup server

Each layer of Figure 3.1 is mapped to a wide variety of tests that report a wealth of performance tests using which administrators can find quick and accurate answers to the following performance queries:

- What is the status of each client archiving data?
- What is the size of the data archived by each client?
- How well each device connected to the target backup server is utilized? Are there adequate resources in each device to ensure smooth backup process?
- What is the status of each client processing backup data using a particular backup mode?
- What is the size of backup data processed by each client using a particular backup mode?
- What is the percentage of CPU utilized by the backup server?
- What is the health of each fan in the target backup server?
- What is the speed at which each fan is operating?
- How well the memory resources of the target backup server is utilized?
- What is the current health of each temperature sensor?

- What is the temperature of each temperature sensor?
- How many times each client had archived the files on the target backup serv er?
- How many times backup was performed by each client using a particular backup mode?
- What is the current health of each voltage source?
- What is the voltage passing through each voltage source?

Since the Network layer has been discussed extensively in *Monitoring Unix and Windows Servers* document, let us now discuss the tests pertaining to the remaining layers mentioned in Figure 3.1 in detail in the forthcoming sections.

3.1 The UEB Hardware Layer

The tests mapped to this layer measure the health of the fans, voltage source and the hardware components. The voltage of the voltage source, speed of the fans and the temperature of the hardware components are also measured and abnormalities, if any are reported.

Figure 3.2: Tests running on the UEB Hardware Layer

3.1.1 Fan SensorTest

This test auto-discovers the fans operating on the target Unitrend Enterprise Backup server and reports the current health of each fan. This test also reports the status of the sensor on each fan and the speed at which each fan is operating. Using this test, administrators can isolate the fans that are operating at abnormal speed.

Target of the test : A Unitrend Enterprise Backup server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each fan operating on the target Unitrend Enterprise Backup server that is being monitored

Configurable parameters for the test

Parameter	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 storage. 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

Parameter	Description
	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.
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
Health status	Indicates the current health of this fan.		The values reported by this measure and its numeric equivalents are mentioned in the table below:

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Normal</td><td>3</td></tr>
<tr><td>Non-Critical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
<tr><td>Non- Recov-erable</td><td>6</td></tr>
<tr><td>Lower-Critical</td><td>7</td></tr>
<tr><td>Upper-Critical</td><td>8</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current health of this fan. The graph of this measure however, represents the status of the fan using the numeric equivalents only - 1 to 8.
</td></tr>
<tr><td>Sensor status</td><td>Indicates the current status of the sensor of this fan.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Unknown</td><td>0</td></tr>
<tr><td>Initiating</td><td>1</td></tr>
<tr><td>Ok</td><td>2</td></tr>
<tr><td>Degraded</td><td>3</td></tr>
<tr><td>Error</td><td>4</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			above to indicate the current status of the sensor of this fan. The graph of this measure however, represents the status of the fan using the numeric equivalents only - 0 to 4.
Speed	Indicates the current speed of this fan.	Rpm	The speed of the fan should be within admissible range. An abnormal/high/low value of this measure indicates malfunctioning of the fan.

3.1.2 Temperature Sensor Test

Abnormal temperature of the hardware components often lead to the malfunctioning of the target backup server which when left unnoticed may affect the overall health. This test auto-discovers the hardware components on the target server and for each hardware component, this test reports the overall health and temperature. The current status of the sensor on each hardware component is also monitored. Using this test, administrators can figure out the hardware component that is not within the admissible temperature range and is malfunctioning.

Target of the test : A Unitrend Enterprise Backup server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each hardware component of the target Unitrend Enterprise Backup server that is being monitored

Configurable parameters for the test

Parameter	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

Parameter	Description
	list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the storage. 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 **Yes** option.

Parameter	Description
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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Health status</td><td>Indicates the current health of this temperature sensor.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Other</td><td>1</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Normal</td><td>3</td></tr>
<tr><td>Non-Critical</td><td>4</td></tr>
<tr><td>Critical</td><td>5</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Non-Recoverable</td><td>6</td></tr>
<tr><td>Lower-Critical</td><td>7</td></tr>
<tr><td>Upper-Critical</td><td>8</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current health of each temperature sensor. The graph of this measure however, represents the status of the fan using the numeric equivalents only - 1 to 8.
</td></tr>
<tr><td>Sensor status</td><td>Indicates the current status of this temperature sensor.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Unknown</td><td>0</td></tr>
<tr><td>Initiating</td><td>1</td></tr>
<tr><td>Ok</td><td>2</td></tr>
<tr><td>Degraded</td><td>3</td></tr>
<tr><td>Error</td><td>4</td></tr>
</table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of each temperature sensor. The graph of this measure however, represents the status of the fan using the numeric equivalents only - 0 to 4.
</td></tr>
<tr><td>Current temperature</td><td>Indicates the current</td><td>Celsius</td><td>The temperature of the sensors should</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
	temperature of this temperature sensor.		be within admissible range.

3.1.3 Voltage Sensor Test

For each voltage source on the target Unitrend Enterprise Backup server, this test reports the health of the voltage source and the voltage passing through the voltage source. This test also reports the current status of the sensor available in the voltage source. Using this test, administrators can figure out the voltage source that is not functioning abnormally.

Target of the test : A Unitrend Enterprise Backup server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each voltage source on the target Unitrend Enterprise Backup server that is being monitored

Configurable parameters for the test

Parameter	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 storage. 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

Parameter	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.

Parameter	Description
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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>Health status</td><td>Indicates the current health of this voltage source.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Other</td><td>1</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Normal</td><td>3</td></tr><tr><td>Non-Critical</td><td>4</td></tr><tr><td>Critical</td><td>5</td></tr><tr><td>Non- Recov-erable</td><td>6</td></tr><tr><td>Lower-Critical</td><td>7</td></tr><tr><td>Upper-Critical</td><td>8</td></tr></table>
Note:

By default, this measure reports the Measure Values listed in the table above to indicate the current health of each voltage source. The graph of this</td></tr>
</table>

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>measure however, represents the status of the fan using the numeric equivalents only - 1 to 8.</td></tr>
<tr><td>Sensor status</td><td>Indicates the current status of the sensor on this voltage source.</td><td></td><td>The values reported by this measure and its numeric equivalents are mentioned in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Unknown</td><td>0</td></tr><tr><td>Initiating</td><td>1</td></tr><tr><td>Ok</td><td>2</td></tr><tr><td>Degraded</td><td>3</td></tr><tr><td>Error</td><td>4</td></tr></table>Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of each voltage source. The graph of this measure however, represents the status of the voltage source using the numeric equivalents only - 0 to 4.</td></tr>
<tr><td>Current voltage</td><td>Indicates the current voltage passing through this voltage source.</td><td>Volts</td><td>If the voltage is not within admissible range, then the voltage source may be damaged leading to the damage of the server.</td></tr>
</table>

3.2 The UEB Operating System Layer

Using the tests mapped to this layer, administrators can determine the physical CPU/memory utilization of the target server.

Figure 3.3: The tests mapped to the UEB Operating System layer

Let us discuss each test of this layer (see Figure 3.3) in detail in the forthcoming sections.

3.2.1 CPU Utilization Test

This test reports the percentage of CPU utilized by the target server.

Target of the test : A Unitrend Enterprise Backup server

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Unitrend Enterprise Backup server that is being monitored

Configurable parameters for the test

Parameter	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 storage. 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

Parameter	Description
	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.
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

Parameter	Description
	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
CPU usage	Indicates the percentage of CPU utilized by the server.	Percentage	A low value is desired for this measure.

3.2.2 Memory Utilization Test

This test monitors the current memory utilization of the target Unitrend Enterprise Backup server and promptly alerts administrators to a potential memory contention on the server.

Target of the test : A Unitrend Enterprise Backup server

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Unitrend Enterprise Backup server that is being monitored

Configurable parameters for the test

Parameter	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

Parameter	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 storage. 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

Parameter	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.
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
Total memory	Indicates the total memory of the Unitrends Enterprise Backup server.	GB	
Used memory	Indicates the amount of memory already utilized by the Unitrend Enterprise Backup server.	GB	A high value for this measure indicates that the server is running out of memory resources.
Free memory	Indicates the amount of memory that is available for use in the Unitrend Enterprise Backup server.	GB	A high value is desired for this measure.

Measurement	Description	Measurement Unit	Interpretation
Memory usage	Indicates the percentage of memory utilized by the Unitrend Enterprise Backup server.	Percent	A value close to 100 percent for this measure indicates that the memory resources are depleting at a faster pace. Administrators can either increase the allocation of memory resources or clean up the disks to free the memory resources.

3.3 The Backup Services Layer

The tests mapped to this layer measure the level of efficiency with which the Unitrend Enterprise Backup server performs backups.

Figure 3.4: Tests pertaining to the Backup Services Layer

3.3.1 Archive Status Test

For each client archiving data from this server, this test reports the status of the clients and the size of the data archived. By continuously monitoring the size and status of the archived data, administrators can identify the client that is most/least active to perform archives.

Target of the test : A Unitrend Enterprise Backup server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Operating System Type/Server: Client ID* that is to be monitored

Configurable parameters for the test

Parameter	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 storage. 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

Parameter	Description
	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.
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
Status	Indicates the current status of this client archiving data from this		The values reported by this measure and its numeric equivalents are mentioned in the table below:

Measurement	Description	Measurement Unit	Interpretation
	server.		<table><tr><th>Measure value</th><th>Numeric Value</th></tr><tr><td>Failed</td><td>0</td></tr><tr><td>Success</td><td>1</td></tr></table> **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the current state of this client archiving data from this server. The graph of this measure however, represents the status of a fan sensor using the numeric equivalents only - 0 or 1.
Size	Indicates the current size of the archive performed by this client.	MB	Comparing the value of this measure across the clients helps administrators to figure out the client that is more active in performing archives.

3.3.2 Total Archives Test

This test auto-discovers the clients that are configured to archive their files to the target server and for each client, this test reports the number of times the client archived the files on the target server. Administrators can figure out the client that is consistently archiving the files on the target server and also figure out the client that has failed to archive the files.

Target of the test : A Unitrend Enterprise Backup server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Client* from which backup was being initiated on the target Unitrend Enterprise Backup server being monitored

Configurable parameters for the test

Parameter	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 storage. 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

Parameter	Description
	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.
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
Total archives	Indicates the number of times this client had archived the files on the server.	Number	By comparing the value of this measure across the clients, administrators can figure out the client that is efficiently archiving the files.

Measurement	Description	Measurement Unit	Interpretation
			The detailed diagnosis of this measure lists the status of the archive for each client, the time of archiving and the error message if errors were encountered during archiving process.

3.3.3 Backup Capacity Test

This test auto-discovers the storage devices that are connected to the target Unitrend Enterprise Backup server and for each device, this test reports the resource utilization. Using this test, administrators may be alerted to the device that is running out of space.

Target of the test : A Unitrend Enterprise Backup server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *device* on which backup would be performed from the target Unitrend Enterprise Backup server that is being monitored

Configurable parameters for the test

Parameter	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 storage. 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

Parameter	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

Parameter	Description
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
Total capacity	Indicates the total space allocated to this device for backup.	GB	
Used space	Indicates the amount of space that is already used by this device for backup.	GB	A high value indicates that the backup device is running out of space.
Space usage	Indicates the percentage of space that is already utilized by this device for backup.	Percent	A high value for this measure is an indication of the device running out of space and is a warning sign for the administrators to add additional resources.
Free space	Indicates the amount of space that is available for use in this device for backup.	GB	A high value is desired for this measure.
Space free	Indicates the percentage of space that is available for use in this device for backup.	Percent	

3.3.4 Backup Status Test

For each client processing the backups using each backup mode, this test reports the status of the clients and the size of the backup performed. By continuously monitoring the size and status of the backups, administrators can identify the client that is most/least active to perform backup.

Target of the test : A Unitrend Enterprise Backup server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Backup mode:Client* that is to be monitored

Configurable parameters for the test

Parameter	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 storage. 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

Parameter	Description
	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.
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

Parameter	Description
	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
Status	Indicates the current status of this client that is processing the backup files using this backup mode.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure value** / **Numeric Value** None – 0 Success – 1 Warning – 2 Failure – 3 **Note:** By default, this measure reports the **Measure Value**s listed in the table above to indicate the current state of this client. The graph of this measure however, represents the status of a fan sensor using the numeric equivalents only - 0 to 3.
Size	Indicates the current size of the backup performed by this client using this backup mode.	MB	Comparing the value of this measure across the clients helps administrators to figure out the client that is more active in performing backups.

3.3.5 Total Backups Test

Unitrends uses backups to create recovery points for your data. Backups are run in different modes and are organized into backup groups. Your backup strategies determine which modes you will use. Unitrends backups fall into two general categories: local backups and backup copies.

Local backups are stored on the appliance. These backups are immediately accessible and enable you to meet low RTOs. Backup copies are stored on an offsite target. These backups are duplicates (hence, "copies") of your local backups, and are used for long-term retention and disaster recovery.

Backup modes determine what data to include in the backup. These modes protect all types of data and apply to asset-level backups, host-level backups, application backups, NAS backups, and iSeries backups. While creating backup jobs, you can select the following backup modes: full, incremental, differential, selective, and bare metal. In addition to these, the server automatically creates synthetic backups as needed.

In environments where multiple clients/servers are connected to the target backup server, administrators may often fail to figure out what type of backup was being performed by the client/server and when the backup was performed. The Total Backups test helps administrators in this regard!.

This test auto-discovers the backup modes using which clients/servers are performing backup on the target backup server, and for each backup mode, this test report the number of times backup was performed using that particular backup mode. Administrators can compare the values across the backup modes and figure out the most commonly used mode for backups.

Target of the test : A Unitrend Enterprise Backup server

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *Backup mode* using which backup was performed on the target Unitrend Enterprise Backup server that is being monitored

Configurable parameters for the test

Parameter	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 storage. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the SNMPVersion chosen

Parameter	Description
	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 **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:

Parameter	Description
	• **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
Total backups	Indicates the number of times backup was performed using this backup mode on the backup server.	Number	Compare the value of this measure across the backup modes to determine the backup mode that was most commonly used for backup purposes. The detailed diagnosis of this measure lists the ID, the name of the client who performed the backup, the time at which the backup was performed and the total number of files that were backed up.

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.