
# Monitoring DoubleTake Availability

***eG Enterprise v6***

**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 2000, Windows 2003 and Windows 2008 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

# Table of Figures

Chapter 1

# Monitoring the Double-Take Availability Server

Double-Take Availability for Windows provides real-time high availability and immediate disaster recovery so you never have to worry about downtime or the lost revenue and chaos that ensue.

Double-Take Availability ensures the availability of critical workloads. Using real-time replication and failover, you can protect data, individual applications, entire servers, or virtual machines. Identify your critical workload on your production server, known as the source, and replicate the workload to a backup server, known as the target. The target server, on a local network or at a remote site, stores the copy of the workload from the source. Double-Take Availability monitors any changes to the source workload and sends the changes to the copy stored on the target server. By replicating only the file changes rather than copying an entire file, Double-Take Availability allows you to more efficiently use resources.

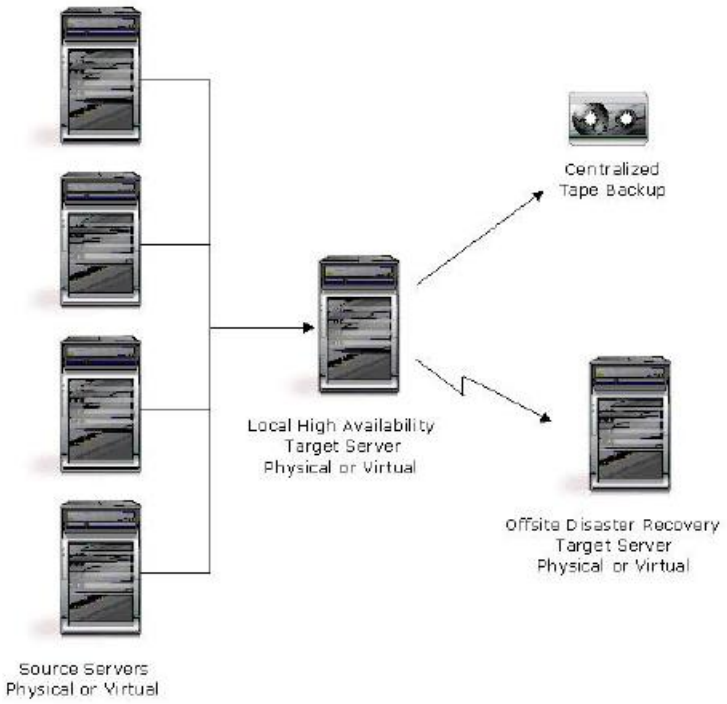


Figure 1.1: How does DoubleTake work?

In physical/virtual infrastructures that deliver mission-critical services to end-users, the 24x7 availability of data and applications is crucial for maximizing service quality, user satisfaction, and consequently, revenues. In such environments therefore, the uninterrupted functioning of DoubleTake is imperative. Issues such as intermittent breaks in the availability of DoubleTake, excessive load conditions, and delayed connectivity, if not promptly detected and resolved, can significantly impact the delivery of underlying services. You thus need to periodically monitor DoubleTake for such availability and operational snags, and initiate early measures to redress them.

eG Enterprise offers a specialized *DoubleTake* monitoring model, which monitors the uptime of, the connections to, and rate at which the DoubleTake server performs mirroring and replication operations, and proactively alerts administrators to current and potential deviations from desired performance levels.

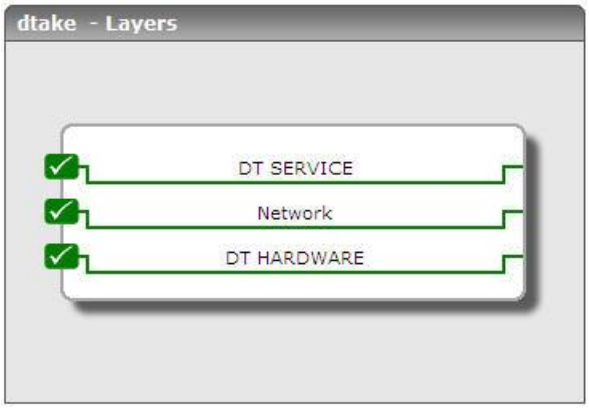


Figure 1.2: Layer model of the DoubleTake server

Each layer of Figure 1.2 above is mapped to a wide variety of tests that periodically poll the SNMP MIB of the DoubleTake server to capture errors and slowdowns in its functioning. Using the statistics so reported, administrators can infer the following:

- Is the Double-Take Availability server available over the network? If so, how quickly is it responding to requests?
- Are all network interfaces supported by the server operating at normal speeds?
- Is any network interface utilizing bandwidth excessively?
- Is the Double-Take server using too much memory from the reserved memory pool for its operations?
- Was the Double-Take server down recently?
- Has any connection to a target been active for an unusually long time?
- Is a target experiencing any errors in the connections to it?
- Does any connection have too many operations in queue? If so, what type of operations hog the queue - mirroring or replication?
- Have any logins to the Double-Take source and/or target failed? Did any of these login failures occur in the last measurement period?

The sections that follow will discuss each layer of Figure 1.2 in detail.

# 1.1 The DT HARDWARE Layer

The tests mapped to this layer monitor the uptime and the memory usage of the Double-Take Availability server.


Figure 1.3: Tests mapped to the DT HARDWARE layer

## 1.1.1 DT Memory Test

When the Double-Take service starts, it reserves a pool of user-addressable memory equal to the Double-Take pagefile size. This reserved pool of memory is the Double-Take pagefile. Although Double-Take has the pool of memory reserved, it only uses what is necessary at any given time. This test reports the amount of memory in the reserved memory pool that the Double-Take server currently uses, and thus enables you to track the memory usage of the Double-Take server.

| | |
|---|---|
| **Purpose** | Tracks the memory usage of the Double-Take server |
| **Target of the test** | Double-take server |
| **Agent deploying the test** | Remote agent |

| | |
|---|---|
| **Configurable parameters for the test** | 1. **TEST PERIOD** - How often should the test be executed<br>2. **Host** – The IP address of the Cisco Router.<br>3. **SNMPPort** - The port number through which the server exposes its SNMP MIB. The default value is 161.<br>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.<br>5. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the server. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear.<br>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.<br>7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**.<br>8. **confirm password** – Confirm the **authpass** by retyping it here.<br>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:<br>➢ **MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm<br>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.<br>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:<br>➢ **DES** – Data Encryption Standard<br>➢ **AES** – Advanced Encryption Standard<br>12. **encryptpassword** – Specify the encryption password here.<br>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. | | |
| **Outputs of the test** | One set of results for the Double-Take server being monitored. | | |
| **Measurements made by the test** | **Measurement** | **Measurement Unit** | **Interpretation** |
| | **Memory allocated:**<br>Indicates the amount of memory from the reserved memory pool that is currently allocated to the mirroring and/or replication operations of the Double-Take server being monitored. | MB | A very high value could indicate that the the server functions are over-utilizing the memory resources available to them.<br>In order to provide maximum Double-Take system performance, Double-Take servers should be configured with enough RAM to accommodate the maximum Double-Take pagefile (1GB) in addition to the server's other memory needs. |

## 1.1.2 DT Uptime Test

In most production environments, it is essential to monitor the uptime of the Double-Take Availability server, as the DR capability of the applications, data, physical, and virtual servers in such environments relies on the availability of the Double-Take server. By tracking the uptime of this server, administrators can determine what percentage of time Double-Take has been up and the percentage of time it was not. If the data on the source and target servers are not in sync at any given point in time, then, you need to know whether it is because the Double-Take server was down during that time period.

The DT Uptime test included in the eG agent monitors the uptime of the Double-Take server.

| | |
|---|---|
| **Purpose** | Monitors the uptime of the Double-Take server |
| **Target of the test** | A Double-Take server |
| **Agent deploying the test** | A remote agent |

| | |
|---|---|
| **Configurable parameters for the test** | 1. **TEST PERIOD** - How often should the test be executed<br>2. **Host** – The IP address of the device.<br>3. **SNMPPort** - The port number through which the device exposes its SNMP MIB. The default value is 161.<br>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.<br>5. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear.<br>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.<br>7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**.<br>8. **confirm password** – Confirm the **authpass** by retyping it here.<br>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:<br>➢ **MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm<br>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.<br>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:<br>➢ **DES** – Data Encryption Standard<br>➢ **AES** – Advanced Encryption Standard<br>12. **encryptpassword** – Specify the encryption password here.<br>13. **confirm password** – Confirm the encryption password by retyping it here. |

| | | | |
|---|---|---|---|
| | 14. **TIMEOUT** – The maximum duration (in seconds) for which the test will wait for a response from the router | | |
| **Outputs of the test** | One set of results for the Double-Take server being monitored | | |
| **Measurements made by the test** | **Measurement** | **Measurement Unit** | **Interpretation** |
| | **Has system been rebooted**:<br>Indicates whether the server has been rebooted during the last measurement period or not. | Boolean | If this measure shows 1, it means that the server was rebooted during the last measurement period. By checking the time periods when this metric changes from 0 to 1, an administrator can determine the times when this server was rebooted. |
| | **Uptime during the last measure period**:<br>Indicates the time period that the system has been up since the last time this test ran. | Secs | If the server has not been rebooted during the last measurement period and the agent has been running continuously, this value will be equal to the measurement period. If the server was rebooted during the last measurement period, this value will be less than the measurement period of the test. For example, if the measurement period is 300 secs, and if the server was rebooted 120 secs back, this metric will report a value of 120 seconds. The accuracy of this metric is dependent on the measurement period – the smaller the measurement period, greater the accuracy. |
| | **Total uptime of the system**:<br>Indicates the total time that the server has been up since its last reboot. | Mins | Administrators may wish to be alerted if a server has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions. |

## 1.2 The Network Layer

Using the tests mapped to this layer, you can verify the network availability of the Double-Take server and measure the speed and bandwidth usage of each of the network interfaces supported by the server.


Figure 1.4: The tests mapped to the Network layer

Since the tests depicted by Figure 1.4 have already been extensively discussed in the *Monitoring Network Elements* document, let us proceed to the next layer.

## 1.3 The DT Service Layer

For each target that a replication set connects to, the **DT Connections** test mapped to this layer reports the state of the connection and the level of activity on the connection. In addition, using the **DT Logins** test mapped to this layer, you can accurately point to the unsuccessful login attempts to the Double-Take source and targets.


Figure 1.5: The tests mapped to the DT Service layer

### 1.3.1 DT Connections Test

Protecting specific data consists of two main tasks - creating a replication set (to identify the data to protect) and connecting that replication set to a target. A unique connection ID is associated with each target a replication set connects to. The connection ID provides a reference point for each connection. The connection ID is determined by sequential numbers starting at one (1). Each time a connection is established, the ID counter is incremented. It is reset back to one each time the Double- Take service is restarted. For example, if the Double-Take service was started and the same replication set was connected to five target machines, each connection would have a unique connection ID from 1 to 5.

This test monitors the current state of each Double-Take Availability connection and reports and reports the level of activity on each connection, so that the busiest/overloaded connections are revealed, and the operation (mirroring/replication) that is causing the overload can be identified.

| | |
|---|---|
| **Purpose** | Monitors the current state of each Double-Take Availability connection and reports and reports the level of activity on each connection, so that the busiest/overloaded connections are revealed, and the operation (mirroring/replication) that is causing the overload can be identified. |
| **Target of the test** | A Double-Take server |
| **Agent deploying the test** | A remote agent |

| | |
|---|---|
| **Configurable parameters for the test** | 1. **TEST PERIOD** - How often should the test be executed<br>2. **Host** – The IP address of the device.<br>3. **SNMPPort** - The port number through which the device exposes its SNMP MIB. The default value is 161.<br>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.<br>5. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear.<br>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.<br>7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**.<br>8. **confirm password** – Confirm the **authpass** by retyping it here.<br>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:<br>➢ **MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm<br>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.<br>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:<br>➢ **DES** – Data Encryption Standard<br>➢ **AES** – Advanced Encryption Standard<br>12. **encryptpassword** – Specify the encryption password here.<br>13. **confirm password** – Confirm the encryption password by retyping it here. |

<table>
<tr><td></td><td colspan="5">14. TIMEOUT – The maximum duration (in seconds) for which the test will wait for a response from the router</td></tr>
<tr><td>Outputs of the test</td><td colspan="5">One set of results for each Double-Take Availability connection being monitored</td></tr>
<tr><td rowspan="4">Measurements made by the test</td><td>Measurement</td><td>Measurement Unit</td><td colspan="3">Interpretation</td></tr>
<tr><td>Connection activity:<br>Indicates the amount of time this connection has been active.</td><td>Minutes</td><td colspan="3">A very high value for this measure could indicate that the data is taking too long to be transmitted to the target.</td></tr>
<tr><td rowspan="3">Connection state:<br>Indicates the current state of this connection.</td><td rowspan="3"></td><td colspan="3">The values reported by this measure, their description, and the numeric values that correspond to them have been discussed in the table below:</td></tr>
<tr><td>Measure Value</td><td>Numeric Value</td><td>Measure Description</td></tr>
<tr><td>conError</td><td>0</td><td>A transmission error has occurred. Possible errors include a broken physical line or a failed target service.</td></tr>
<tr><td></td><td>conActive</td><td>1</td><td>Indicates that the connection is functioning normally and has no scheduling restrictions imposed on it at this time. (There may be restrictions, but it is currently in a state that allows it to transmit.)</td></tr>
</table>

| | | | | | |
|---|---|---|---|---|---|
| | | | conPaused | 2 | Indicates a connection that has been paused. This implies that the network connection exists and is available for data transmission, but the replication and mirror data is being held in a queue and is not being transmitted to the target. |
| | | | conScheduled | 3 | indicates a connection that is not currently transmitting due to scheduling restrictions (bandwidth limitations, time frame limitations, and so on). |
| | | | conNone | 4 | Indicates that a connection has not been established. |
| | | | | | |
| | **Ops in Retransmit Queue**:<br>Indicates the number of operations (create, modify, or delete) currently in the retransmit queue on the source. | Number | | | |

| | | | |
|---|---|---|---|
| | **Ops Awaiting Acknowledgements:**<br>Indicates the number of of operations currently waiting in the acknowledgement queue. | Number | Each operation that is generated receives an acknowledgement from the target after that operation has been received by the target. This statistic indicates the number of operations that are yet to receive acknowledgement of receipt. |
| | **Replication Ops Queued:**<br>Indicates the number of replication operations currently waiting to be executed on the target. | Number | Replication is the real-time transmission of file changes to a target. These changes, instead of being replicated to a target, may be queued to disk, if a locked file on the target prevents the changes from being written to it, or if a file on the source changes faster than can be transmitted to the target. Typically, if the system memory allocated to queueing is utilized fully, then new file changes that are to be replicated to a target will be directly queued to disk, while old changes remain in the system memory. Data queued to disk is written to a transaction log.<br>The value of this measure indicates the number of file changes that are in queue, and are yet to be replicated to the target. A high value of this measure may indicate that too many file changes are awaiting processing or that one/more files on the target have been locked for too long a time. |
| | **Mirror Ops Queued:**<br>Indicates the number of mirroring operations currently in queue. | Number | Mirroring is the process of transmitting user-specified data from the source to the target, so that an identical copy of data exists on the target. When Double-Take Availability initially performs mirroring, it copies all of the selected data, including file attributes and permissions. Mirroring creates a foundation upon which Double-Take Availability can efficiently update the target server by replicating only file changes.<br>A high value of this measure indicates that many mirroring operations are pending processing, which could hint at a probable processing bottleneck. |

| | | | |
|---|---|---|---|
| | **Replication Ops Queued Data:**<br>Represents the amount of data that was associated with the queued replication operations during the last measurement period. | KB | |
| | **Mirror Ops Queued Data:**<br>Represents the amount of data that was associated with the queued mirror operations during the last measurement period. | KB | |
| | **Operations Transmitted:**<br>Indicates the total number of operations that are currently transmitted to the target. | Number | |
| | **Data Sent:**<br>Indicates the total number of bytes sent to the target since the last measurement period. | KB | |
| | **Operations Received:**<br>Indicates the total number of operations (create, modify, or delete) currently received from the target. | Number | |
| | **Data Received:**<br>Indicates the total number of bytes received from the target during the last measurement period. | KB | |
| | **Resent operations:**<br>Indicates the number of operations that were resent because they were not acknowledged. | Number | |

### 1.3.2 DT Logins Test

To ensure protection of your data, Double-Take Availability offers multi-level security using native operating system security features. Privileges are granted through membership in user groups defined on each machine running Double-Take Availability. To gain access to a particular Double-Take Availability source or target, the user must provide a valid operating system user name and password and the specified user name must be a member of one of the Double-Take Availability security groups. Once a valid user name and password has been provided and the Double-Take Availability source or target has verified membership in one of the Double-Take Availability security groups, the user is granted appropriate access to the source or target and the corresponding features are enabled in the client.

Using this test, you can promptly detect a failed login attempts to a Double-Take source or target.

| | |
|---|---|
| **Purpose** | Helps promptly detect a failed login attempts to a Double-Take source or target |
| **Target of the test** | A Double-Take server |
| **Agent deploying the test** | A remote agent |

| | |
|---|---|
| **Configurable parameters for the test** | 1. **TEST PERIOD** - How often should the test be executed<br>2. **Host** – The IP address of the device.<br>3. **SNMPPort** - The port number through which the device exposes its SNMP MIB. The default value is 161.<br>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.<br>5. **SNMPCommunity** – The SNMP community name that the test uses to communicate with the device. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the **snmpversion** chosen is **v3**, then this parameter will not appear.<br>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.<br>7. **authpass** – Specify the password that corresponds to the above-mentioned **username**. This parameter once again appears only if the **snmpversion** selected is **v3**.<br>8. **confirm password** – Confirm the **authpass** by retyping it here.<br>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:<br>➢ **MD5** – Message Digest Algorithm<br>➢ **SHA** – Secure Hash Algorithm<br>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.<br>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:<br>➢ **DES** – Data Encryption Standard<br>➢ **AES** – Advanced Encryption Standard<br>12. **encryptpassword** – Specify the encryption password here.<br>13. **confirm password** – Confirm the encryption password by retyping it here. |

| | | | |
|---|---|---|---|
| | 14. **TIMEOUT** – The maximum duration (in seconds) for which the test will wait for a response from the router | | |
| **Outputs of the test** | One set of results for each Double-Take Availability server being monitored | | |
| **Measurements made by the test** | **Measurement** | **Measurement Unit** | **Interpretation** |
| | **Total Successful Logins**:<br>Indicates the total number of successful logins to the server. | Number | |
| | **Total Failed Logins:**<br>Indicates the total number of failed logins to the server. | Number | Ideally, the value of this measure should be 0. |
| | **Current Successful Logins:**<br>Indicates the number of login attempts that were successful during the last measurement period. | Number | |
| | **Current Failed Logins:**<br>Indicates the number of login attempts that failed during the last measurement period. | Number | Ideally, the value of this measure should be 0. |

Chapter 2

# Conclusion

This document has described in detail the monitoring paradigm used and the measurement capabilities of the eG Enterprise suite of products with respect to **Double-Take Availability Servers**. For details of how to administer and use the eG Enterprise suite of products, refer to the user manuals.

We will be adding new measurement capabilities into the future versions of the eG Enterprise suite. If you can identify new capabilities that you would like us to incorporate in the eG Enterprise suite of products, please contact support@eginnovations.com. We look forward to your support and cooperation. Any feedback regarding this manual or any other aspects of the eG Enterprise suite can be forwarded to feedback@eginnovations.com.