Monitoring Dell Switch N Series

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

The Dell N Series is a family of energy-efficient, cost-effective 1GbE and 10GbE switches designed for modernising and scaling network infrastructure. Dell Networking N Series switches utilize a comprehensive enterprise-class feature set and deliver simplified management. The Dell N1500 switch series has options for 24 or 48 ports of PoE+ to deliver clean power to network devices such as wireless access points, Voice-over-IP handsets, video conferencing systems, and security cameras. PoE+ is useful in older buildings where installing power to multiple locations can be expensive.

If the switches malfunction or do not respond, then, data may not be transmitted from the data centers at a faster pace which would directly have an impact on the end users. Administrators should therefore monitor the switches in their environment 24*7. Let us now deep-dive into the procedure to monitor the Dell Switch N Series monitoring model in the forthcoming chapters.

Chapter 2: How to Monitor Dell Switch N-Series Using eG Enterprise?

eG Enterprise monitors the Dell Switch N Series using an eG external agent. This agent can be deployed on any remote host in the environment. This agent is capable of monitoring the performance of the switch by polling the SNMP-MIB of the switch at regular intervals. Ensure that the Dell Switch N Series is SNMP-enabled before you start monitoring the target switch.

2.1 Managing the Dell Switch N Series

The eG Enterprise cannot automatically discover the Dell Switch N Series. This implies that you need to manually add the component for monitoring. Remember that the components added manually will be manage automatically. To add a *Dell Switch N Series* 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 *Dell Switch N Series* as the **Component type**. Then, click the **Add New Component** button. This will invoke Chapter 2.

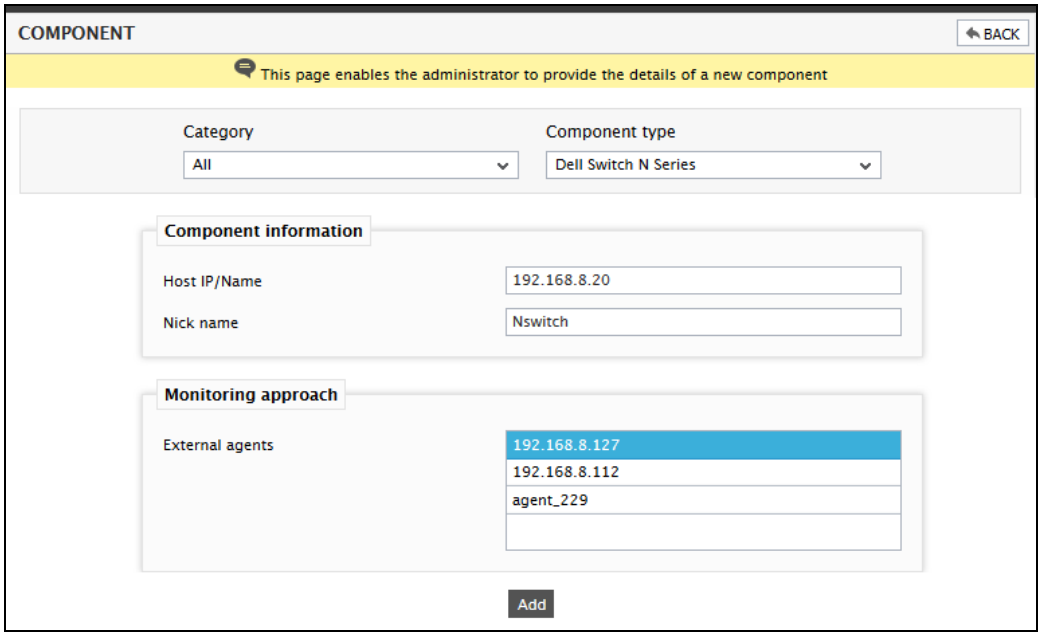

Figure 2.1: Adding the Dell Switch N Series

4. Specify the **Host IP/Name** and **Nick name** of the Dell Switch N Series component (see Chapter 2). Then, click on the **Add** button to register the changes.
5. When you attempt to sign out, a list of unconfigured tests appears.

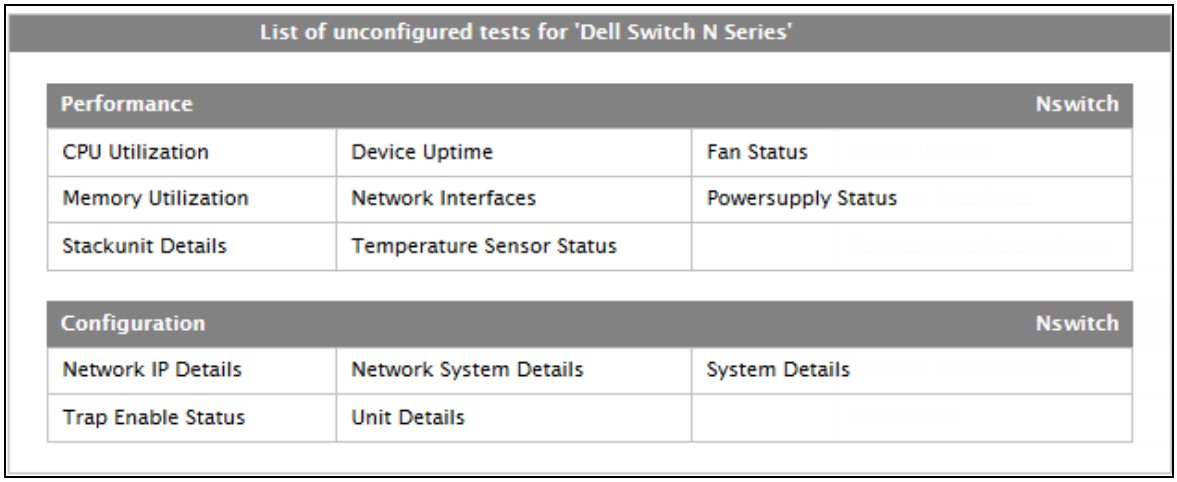

Figure 2.2: List of tests to be configured for Dell Switch N Series

6. Click on the test names to configure. To know how to configure the tests, refer to **Monitoring the Dell Switch N Series** chapter.
7. Finally, signout of the eG administrative interface.

Chapter 3: Monitoring the Dell Switch N Series

eG Enterprise has developed a dedicated *Dell Switch N Series* monitoring model which periodically checks the status of each stack unit and its uptime, the temperature detected on each temperature sensor, the memory utilization the CPU utilization etc, so that abnormalities can be detected and rectified before any irreparable damage occurs.

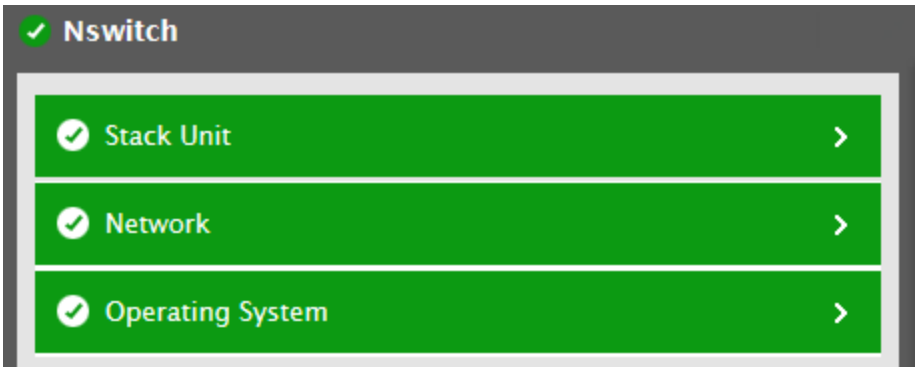

Figure 3.1: The layer model of the Dell Switch N Series

Every layer of Figure 3.1 is mapped to a variety of tests which connect to the SNMP MIBs of the target Dell Switch N Series to collect critical statistics pertaining to its performance. The metrics reported by these tests enable administrators to answer the following questions:

- What is the CPU utilization during the last second?
- What is the CPU utilization during the last minute?
- How well the CPU is utilized during the last 5 minutes?
- What is the current status of each fan available in each stack unit?
- How well the memory is utilized?
- What is the current status of the power supply unit within each stack unit?
- What is the current temperature of each stack unit?
- What is the current status of the switch available in each stack unit?
- How well each port transmits / receives power signals?
- What is the current status of each stack unit?
- What is the uptime of each stack unit and how many times was the stack unit rebooted?

Since the tests of the Network layer have already been discussed in the *Monitoring Unix and Windows servers* and *Monitoring Cisco Routers* documents in detail, the sections to come will discuss all other layers of Figure 3.1 in detail.

3.1 The Operating System layer

Using this layer administrators can track the CPU utilization and memory utilization of the Dell Switch N Series. In addition, administrators can also track the current temperature of each stack unit and determine the stack units that are not operating within the admissible temperature range.

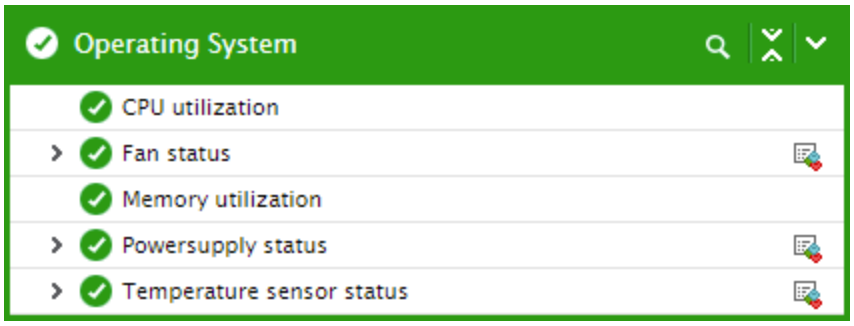

Figure 3.2: The tests associated with the Operating System layer

The sections that follow discusses each test of this layer in detail.

3.1.1 Memory Utilization Test

This test reports the memory utilization of the target Dell Switch N Series.

Target of the test : Dell Switch N Series

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Dell Switch N Series being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the 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

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

Parameters	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

Measurement	Description	Measurement Unit	Interpretation
Total memory	Indicates the total amount of memory allocated to the switch.	MB	
Used memory	Indicates the amount of memory utilized by the switch.	MB	A low value is desired for this measure. A value close to the *Total memory* measure indicates that the memory resources are depleting rapidly.
Free memory	Indicates the amount of memory that is currently available for use in the switch.	MB	A high value is desired for this measure.
Memory utilization	Indicates the percentage of memory utilized by the	Percent	A low value is desired for this

Measurement	Description	Measurement Unit	Interpretation
	switch.		measure. A high value or a consistently increasing value is a cause of concern, as it could indicate a gradual erosion of memory in the switch. In such cases, you may want to resize the memory of the switch or investigate the cause of memory erosion and find a way to arrest the memory erosion.

3.1.2 CPU Utilization Test

This test monitors the current CPU utilization of the target Dell Switch N Series. If the CPU resources are found to b consumed excessively, then, this test will help administrators to determine when exactly did the CPU utilization peak - during the last 5 sec? or 1 minute? or 5 minutes? This revelation helps administrators troubleshoot the CPU spikes better.

Target of the test : Dell Switch N Series

Agent deploying the test : An external agent

Outputs of the test : One set of results for the target Dell Switch N Series being monitored

Configurable parameters for the test

Parameters	Description
Test period	How often should the test be executed
Host	The host for which the test is to be configured.
SNMPPort	The port at which the monitored target exposes its SNMP MIB; the default is *161*.
SNMPversion	By default, the eG agent supports SNMP version 1. Accordingly, the default selection in the SNMPversion list is **v1**. However, if a different SNMP framework is in use in your environment, say SNMP **v2** or **v3**, then select the corresponding option from this list.
SNMPCommunity	The SNMP community name that the test uses to communicate with the firewall. This parameter is specific to SNMP **v1** and **v2** only. Therefore, if the snmpversion chosen is **v3**, then this parameter will not appear.
Username	This parameter appears only when **v3** is selected as the SNMPVersion. SNMP version

Parameters	Description
	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: • **DES** – Data Encryption Standard

Parameters	Description
	• **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
CPU utilization in 5 seconds	Indicates the percentage of CPU utilized during the last 5 seconds.	Percent	By comparing the values of these measures, you can quickly figure out when exactly was the CPU usage maximum. Using this analysis, administrators can further investigate the real reason behind the sudden spike in the CPU utilization.
CPU utilization in 1 minute	Indicates the percentage of CPU utilized during the last 1 minute.	Percent	
CPU utilization in 5 minutes	Indicates the percentage of CPU utilized during the last 5 minutes.	Percent	

3.1.3 Fan Status Test

This test reports the current operational state and speed of each fan available in the stack units of the Dell Switch N Series. Using this test, administrators can identify the fan that is not operational and replace the same before the stack unit starts malfunctioning.

Target of the test : Dell Switch N Series

Agent deploying the test : An external agent

Outputs of the test : One set of results for every *stack unit:fan* combination in the Dell Switch N Series monitored

Configurable parameters for the test

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

Parameters	Description
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 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 fan.		The values reported by this measure and its numeric equivalents are

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>mentioned in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Not present</td><td>1</td></tr><tr><td>Operational</td><td>2</td></tr><tr><td>Powering</td><td>4</td></tr><tr><td>No power</td><td>5</td></tr><tr><td>Not powering</td><td>6</td></tr><tr><td>Incompatible</td><td>7</td></tr><tr><td>Failed</td><td>8</td></tr></table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status each fan. The graph of this measure however, is represented using the numeric equivalents mentioned in the table above.</td></tr>
<tr><td>Speed</td><td>Indicates the current speed of this fan.</td><td>Rpm</td><td>The speed of the fan should be well within admissible range.
If there is a sudden/gradual increase/decrease in the speed of the fan, then it indicates that the fan is malfunctioning.
By comparing the speed of the fans, administrators can figure out the fans that are running abnormally and replace them before the stack unit starts malfunctioning.</td></tr>
</table>

3.1.4 Powersupply Status Test

This test reveals the current status of each power supply unit available in the stack units of the target Dell Switch N Series. Using this test, administrators can easily identify the power supply units that

are non-operational and have failed.

Target of the test : Dell Switch N Series

Agent deploying the test : An external agent

Outputs of the test : One set of results for each *stack unit:power supply unit* combination on the target Dell Switch N Series being monitored

Configurable parameters for the test

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

Parameters	Description
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 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>Status</td><td>Indicates the current status of this power supply unit.</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>Not present</td><td>1</td></tr><tr><td>Operational</td><td>2</td></tr><tr><td>Powering</td><td>4</td></tr><tr><td>No power</td><td>5</td></tr><tr><td>Not powering</td><td>6</td></tr><tr><td>Incompatible</td><td>7</td></tr><tr><td>Failed</td><td>8</td></tr></table>
Note:
By default, this measure reports the Measure Values listed in the table above to indicate the current status of each power supply unit. The graph of this measure however, is represented using the numeric equivalents mentioned in the table above.</td></tr>
</table>

3.1.5 Temperature Sensor Status Test

This test auto-discovers the temperature sensors of the target Dell Switch N Series and reports the current temperature of each temperature sensor. By carefully analyzing the temperature of the stack units, administrators can figure out the stack units that are malfunctioning due to the temperature being out of the admissible range.

Target of the test : Dell Switch N Series

Agent deploying the test : An external agent

Outputs of the test : One set of results for every *stack unit:temperature sensor* combination of the target Dell Switch N Series being monitored

Configurable parameters for the test

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

Parameters	Description
	• **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
Temperature Sensor Status	Indicates the current status of this temperature sensor.		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>Not present</td><td>1</td></tr>
<tr><td>Operational</td><td>2</td></tr>
<tr><td>Powering</td><td>4</td></tr>
<tr><td>No power</td><td>5</td></tr>
<tr><td>Not powering</td><td>6</td></tr>
<tr><td>Incompatible</td><td>7</td></tr>
<tr><td>Failed</td><td>8</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, is represented using the numeric equivalents mentioned in the table above.
</td></tr>
<tr><td>Temperature</td><td>Indicates the current temperature recorded by this temperature sensor.</td><td>Celsius</td><td>Ideally, the temperature should be well within admissible range. A sudden / gradual increase / decrease in the temperature is a cause of concern and warrants the immediate attention of the administrator.</td></tr>
</table>

3.2 The Stack Unit layer

This layer helps administrators to track the current status and the uptime of each stack unit of the Dell Switch N Series.

Figure 3.3: The tests associated with the Stack unit layer

The tests associated with this layer are discussed in the forthcoming sections.

3.2.1 Stackunit Details Test

This test auto-discovers the stack units of the target Dell Switch N Series and reports the current status of each stack unit. This test also reports the uptime of each stack unit and the number of times each stack unit was rebooted.

Target of the test : Dell Switch N Series

Agent deploying the test : An external agent

Outputs of the test : One set of results for every stack unit in the Dell Switch N Series monitored.

Configurable parameters for the test

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

Parameters	Description
	SNMPEngineID value of the entity hosting the management information (also called a contextEngineID) and a context name that identifies the specific context (also called a contextName). If the Username provided is associated with a context name, then the eG agent will be able to poll the MIB and collect metrics only if it is configured with the context name as well. In such cases therefore, specify the context name of the Username in the Context text box. By default, this parameter is set to *none*.
Authpass	Specify the password that corresponds to the above-mentioned Username. This parameter once again appears only if the SNMPversion selected is **v3**.
Confirm password	Confirm the Authpass by retyping it here.
Authtype	This parameter too appears only if **v3** is selected as the SNMPversion. From the Authtype list box, choose the authentication algorithm using which SNMP v3 converts the specified username and password into a 32-bit format to ensure security of SNMP transactions. You can choose between the following options: • **MD5** – Message Digest Algorithm • **SHA** – Secure Hash Algorithm
Encryptflag	This flag appears only when **v3** is selected as the SNMPversion. By default, the eG agent does not encrypt SNMP requests. Accordingly, the this flag is set to **No** by default. To ensure that SNMP requests sent by the eG agent are encrypted, select the **Yes** option.
Encrypttype	If this Encryptflag is set to **Yes**, then you will have to mention the encryption type by selecting an option from the Encrypttype list. SNMP v3 supports the following encryption types: • **DES** – Data Encryption Standard • **AES** – Advanced Encryption Standard
Encryptpassword	Specify the encryption password here.
Confirm Password	Confirm the encryption password by retyping it here.
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

Parameters	Description
	environments, you can instruct the eG agent to conduct the SNMP data traffic related to the monitored target over TCP (and not UDP). For this, set this flag to **Yes**. By default, this flag is set to **No**.
Detailed Diagnosis	To make diagnosis more efficient and accurate, the eG Enterprise suite embeds an optional detailed diagnostic capability. With this capability, the eG agents can be configured to run detailed, more elaborate tests as and when specific problems are detected. To enable the detailed diagnosis capability of this test for a particular server, choose the **On** option. To disable the capability, click on the **Off** option. The option to selectively enable/disable the detailed diagnosis capability will be available only if the following conditions are fulfilled: • The eG manager license should allow the detailed diagnosis capability • Both the normal and abnormal frequencies configured for the detailed diagnosis measures should not be 0.

Measurements made by the test

Measurement	Description	Measurement Unit	Interpretation
Status	Indicates the current status of this stack unit.		The values reported by this measure and its numeric equivalents are mentioned in the table below: **Measure Value** / **Numeric Value** Ok – 100 Unsupported – 2 Code Mismatch – 3 Config Mis-match – 4 SDM Mismatch – 5 Not present – 6 Code update – 7 STM Mismatch – 8 **Note:**

Measurement	Description	Measurement Unit	Interpretation
			By default, this measure reports the **Measure Value**s listed in the table above to indicate the current status of the stack unit. The graph of this measure however, is represented using the above-mentioned numeric equivalents only.
Has the stack unit been rebooted?	Indicates whether this stack unit has been rebooted during the last measurement period or not.		If the value of this measure is *Yes*, it means that the stack unit was rebooted during the last measurement period. By checking the time periods when this metric changes from *No* to *Yes*, an administrator can determine the times when this stack unit was rebooted. The Detailed Diagnosis of this measure, if enabled, lists the *TIME, SHUTDOWN DATE, RESTART DATE, SHUTDOWN DURATION, and IS MAINTENANCE*.
Uptime during the last measure period	Indicates the time period that this stack unit has been up since the last time this test ran.	Secs	If the stack unit 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 stack unit 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 stack unit 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 stackunit	Indicates the total time that this stack unit has		This measure displays the number of years, months, days, hours, minutes

Measurement	Description	Measurement Unit	Interpretation
	been up since its last reboot.		and seconds since the last reboot. Administrators may wish to be alerted if the stack unit has been running without a reboot for a very long period. Setting a threshold for this metric allows administrators to determine such conditions.

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.

Copyright © 2018 eG Innovations Inc. All rights reserved.

This document may not be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the prior written consent of eG Innovations. eG Innovations 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. The information contained in this document is subject to change without notice.

All right, title, and interest in and to the software and documentation are and shall remain the exclusive property of eG Innovations. All trademarks, marked and not marked, are the property of their respective owners. Specifications subject to change without notice.