Monitoring Marathon Everrun PVM

eG Innovations Product Documentation

www.eginnovations.com

Total Performance Visibility

Table of Contents

Table of Figures

Chapter 1: Introduction

everRun VM delivers reliable protection for critical virtual workloads by providing redundant virtual machines and synchronized mirroring of the entire system – network, applications and data. It protects at the individual VM level, but runs below the VM, just above the hypervisor. This level of integration allows everRun to build redundancy that is completely transparent to the operating environment to seamlessly manage failures while the application continues to execute. This is called ComputeThru ® technology. Where Citrix XenServer is used to provision multiple Windows virtual machines on a single physical server, you can use everRun to protect the Windows VMs and their applications from failures.

To understand how everRun VM works, consider a simple case. Assume that two identical Intel or AMD-based physical servers are available in your environment. These servers are configured with Ethernet adapters for application use and either local (direct- attached) or shared storage. Redundant Ethernet paths, known as Availability Links, provide a private communications path used by everRun to maintain synchronization of storage and application operations for the virtual machines that everRun protects. Each server should run the XenServer Enterprise Edition virtualization software as the host environment. The everRun technology is loaded as a virtual appliance (the everRun Availability Manager). The Availability Manager runs within the XenServer environment as a purpose-built appliance that provides availability for other virtual machines on the host. The Availability Manager establishes a tightly-coupled relationship to the virtual machines it protects. It resides in the data path between the virtual machine and the control domain, which handles I/O for the virtual machines. To protect a virtual machine, the administrator uses the everRun Availability Center to indicate which virtual machine to protect with everRun and then selects the desired protection level and which host to use for protection. Once this is done, everRun transparently combines and manages the resources of two virtual machines running on different servers in a XenServer resource pool to create a single protected virtual machine environment. The protected virtual machine (PVM) appears and is managed just like a standard Windows server. Disk data is mirrored synchronously to redundant storage and network and server operations are protected from failure. The administrator can load and configure applications in the protected virtual machine, as though it was being loaded onto a physical server.

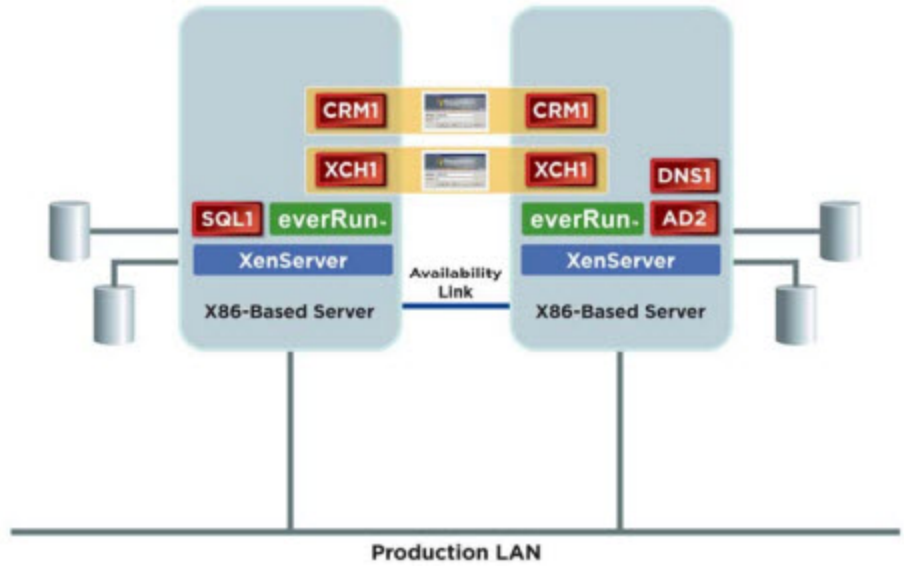

Figure 1.1: How everRun VM works

Since the PVM provides users with a fail-proof virtual machine environment, many enterprises host their mission-critical applications on VMs that are protected by everRun. Problems with the PVM therefore – eg., errors experienced by the PVM, disk and network failures suffered by the PVM – will lift the veil of protection that everRun offers, and expose the protected VMs, applications, network, and data to problems. To avoid this, you need to continuously track the status of the PVM, its disk and network resources, and the XenServer hosts it protects, so that potential errors in the functioning of the PVM are proactively detected and removed, and the protected VMs and applications operate without any interruptions. This is where eG Enterprise helps administrator.

Chapter 2: How to Monitor Marathon EverRun PVM Using eG Enterprise?

eG Enterprise monitors the Marathon EverRun PVM in an agent-based manner. An eG agent installed on the target PVM host periodically polls the SNMP MIB of the target PVM and extracts a wealth of performance information related to that PVM from its MIB.

2.1 Managing the Marathon EverRun PVM

The eG Enterprise cannot automatically discover the Marathon EverRun PVM. This implies that you need to manually add the component for monitoring. Remember that the eG Enterprise automatically manages the components that are added manually. To add a Marathon EverRun PVM, 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 *Marathon EverRun PVM* as the **Component type**. Then, click the **Add New Component** button. This will invoke Figure 2.1.

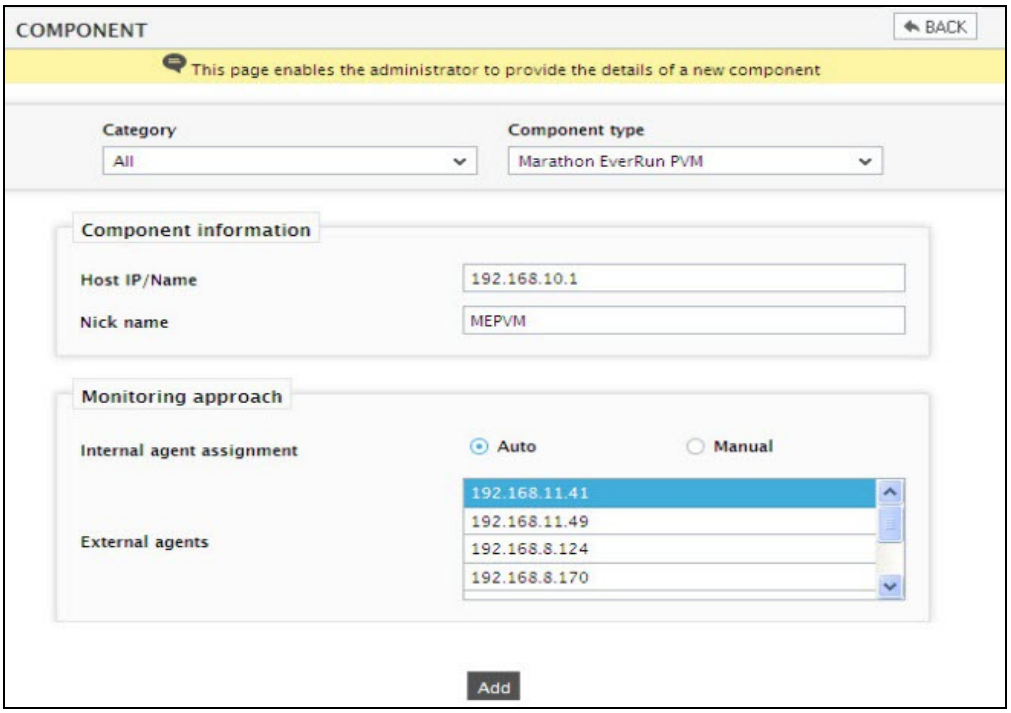

Figure 2.1: Adding a Marathon EverRun PVM component

3. Specify the **Host IP** and the **Nick name** of the Marathon EverRun PVM in Figure 2.1. Then, click on the **Add** button to add the Marathon EverRun PVM for monitoring.

2.2 Configuring the tests

1. When you attempt to sign out, a list of unconfigured tests appears (see Figure 2.2).

Figure 2.2: The list of tests that need to be configured

2. Click on any test in the list of unconfigured tests. For instance, click on the **PVM Disk Details** test to configure it. In the page that appears, specify the parameters as shown in Figure 2.3.

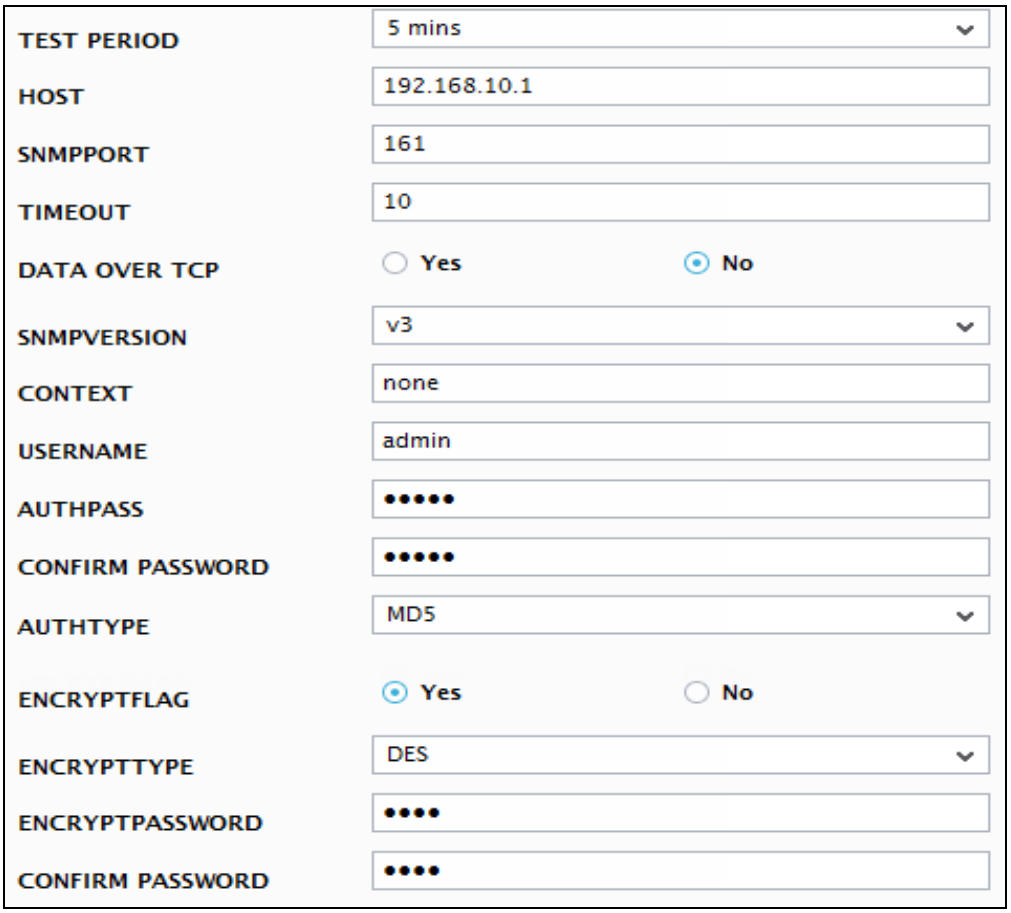

Figure 2.3: Configuring the PVM Disk Details test

3. To know how to configure parameters, refer to **Monitoring Marathon Everrun PVM** chapter.
4. Finally, sign out of the eG administrative interface.

Chapter 3: Monitoring Marathon Everrun PVM

eG Enterprise provides a specialized EverRun monitoring model, which keeps tabs on the state of a target PVM and the virtual environment it protects (which includes its disk and network resources).

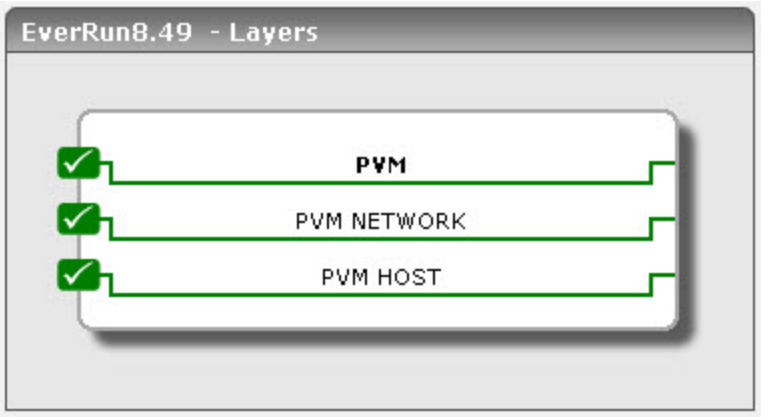

Figure 3.1: The layer model of the Everrun PVM

Each layer of is mapped to a series of tests. The eG agent, which should be deployed on a particular PVM, executes these tests at configured intervals. These tests then poll the SNMP MIB of the target PVM and extract a wealth of performance information related to that PVM from its MIB. Using these metrics, administrators can find quick and accurate answers to the following questions:

- What is the current state of the PVM - good, unknown, or failed?
- Is the PVM's disk in a good state currently,or has it failed?
- How are each of the XenServer hosts in the pool doing? Is any host in the degraded or failed state currently?
- Is any host experiencing any disk failures currently?
- Is any link adapter on any host in an error/failed state currently?
- Which ethernet path is being used by every link adapter on each host in a pool? Is the path used, the primary or secondary path of a redundant setup?
- Which ethernet adapter of this PVM is currently disabled?
- Has any ethernet adapter failed? Is the failed adapter used by the host or the PVM?

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

3.1 The PVM HOST Layer

The tests mapped to this layer reveal the current operational state and health state of every XenServer host in a pool that everRun protects, and points you to failures/errors/degradations experienced by the disks and link adapters attached to each host. In addition, the test also sheds light on the health of disks attached to the target PVM.

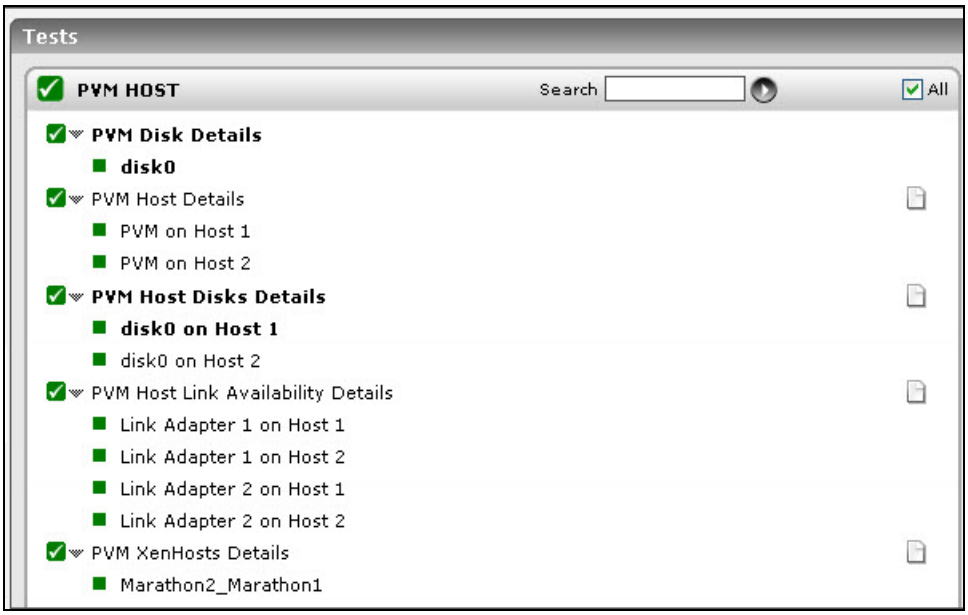

Figure 3.2: The tests mapped to the PVM HOST layer

3.1.1 PVM Disk Details Test

To protect against device and hardware failures and to remove any single-pointsof-failure, everRun creates redundancy for each device that is made available to the virtual environment. For example, drive C: in the PVM may appear as just a single disk/partition; however, everRun may have paired two separate virtual disks (one from each VM on each of the XenServers in a pool, if only two XenServers are in the pool) together to provide data redundancy. Applications need only write the data once as everRun ensures that it is written to both disks simultaneously. If one disk fails, everRun immediately and automatically uses the other without interruption to the application. However, if the PVM's disk fails or is unavailable or is experiencing errors, it is bound to adversely impact the performance and even the operations of the application running on the PVM. To avoid such an outcome, you need to continuously track the state of the PVM's disk. You can use the **PVM Disk Details** test for this purpose. The test monitors the disk partitions that are available to the PVM and reports the current state of each partition, so that potential disk failures can be proactively detected and averted.

Target of the test : An everRun PVM

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each mirrored disk of the target PVM.

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 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	Description
	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>Disk capacity</td><td>Indicates the current capacity of this mirrored disk.</td><td>MB</td><td></td></tr>
<tr><td>Disk state</td><td>Indicates the current operational state of this mirrored disk.</td><td></td><td>The values that this measure can take and their corresponding numeric values are discussed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Good</td><td>0</td></tr><tr><td>Transitioning</td><td>5</td></tr><tr><td>Unknown</td><td>7</td></tr><tr><td>Idle</td><td>8</td></tr><tr><td>Disabled</td><td>13</td></tr><tr><td>Degraded</td><td>14</td></tr><tr><td>offline</td><td>81</td></tr><tr><td>Failed</td><td>91</td></tr></table>Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current operational state of a disk. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.</td></tr>
<tr><td>Severity</td><td>Indicates the current health state of this mirrored disk.</td><td></td><td>The values that this measure can take and their corresponding numeric values are discussed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Good</td><td>0</td></tr><tr><td>Unknown</td><td>2</td></tr></table></td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Informational</td><td>4</td></tr><tr><td>Warning</td><td>81</td></tr><tr><td>Error</td><td>91</td></tr></table> **Note:** By default, this measure reports the above-mentioned **Measure Value**s while indicating the current health state of a disk. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.

3.1.2 PVM Hosts Disk Details Test

This test monitors the disks of the XenServer host that is hosting the Protected Virtual Machine and reports the current disk capacity of the host, current operational state of each disk, and if any disk is experiencing errors currently.

Target of the test : An everRun PVM

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each physical disk 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 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.

Parameter	Description
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.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by

Parameter	Description
	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
Disk capacity	Indicates the current capacity of this disk.	MB	
Disk state	Indicates the current operational state of this disk.		The values that this measure can take and their corresponding numeric values are discussed in the table below: **Measure Value** / **Numeric Value** Good – 0 Transitioning – 5 Unknown – 7 Idle – 8 Disabled – 13

<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>Degraded</td><td>14</td></tr>
<tr><td>offline</td><td>81</td></tr>
<tr><td>Failed</td><td>91</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current operational state of a disk. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.
</td></tr>
<tr><td>Severity</td><td>Indicates the current health state of this disk.</td><td></td><td>
The values that this measure can take and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Good</td><td>0</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Informational</td><td>4</td></tr>
<tr><td>Warning</td><td>81</td></tr>
<tr><td>Error</td><td>91</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current health state of a disk. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.
</td></tr>
</table>

3.1.3 PVM Host Link Availability Details Test

everRun VM requires a dedicated network link, called the “Availability Link”, in order to provide the component-level protection. These links are established via redundant Ethernet paths, which provide everRun with a private communications path to maintain synchronization of storage and application operations for the protected VMs. You need to know which host in the pool is connected via which Ethernet path (whether the primary or secondary), so that you can quickly understand which host and VMs will be affected if the primary path goes down. The **PVM Host Link Availability Details** test reveals this. For each redundant link adapter on a host, this test reports the path (path 1 or path 2) using which that adapter connects to the host and whether that path is the primary path, secondary path, or both.

Target of the test : An everRun PVM

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each link adapter on each host.

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 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

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
Adapter Path1 Usage	Indicates whether this link adapter on this host is currently using Path1 or not, and if so, what type of path is Path1 – primary, secondary, or both.		The values that this measure can take and their corresponding numeric values are discussed in the table below: **Measure Value** / **Numeric Value** None – 1 Primary – 2 Secondary – 3 Both – 4 **Note:** By default, this measure reports the above-mentioned **Measure Value**s while indicating the usage of path 1. However, in the graph of this measure, the same will be represented using the corresponding numeric equivalents only.
Adapter Path2 Usage	Indicates whether this link adapter on this host is currently using Path2 or not, and if so, what type of path is Path2 – primary, secondary, or both.		The values that this measure can take and their corresponding numeric values are discussed 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>None</td><td>1</td></tr>
<tr><td>Primary</td><td>2</td></tr>
<tr><td>Secondary</td><td>3</td></tr>
<tr><td>Both</td><td>4</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the usage of path 2. However, in the graph of this measure, the same will be represented using the corresponding numeric equivalents only.
</td></tr>
<tr><td>Adapter Path1 speed</td><td>Indicates the current speed measured at path 1 of this link adapter on this host.</td><td>Mbps</td><td></td></tr>
<tr><td>Adapter Path2 speed</td><td>Indicates the current speed measured at path 2 of this link adapter on this host.</td><td>Mbps</td><td></td></tr>
<tr><td>State</td><td>Indicates the current operational state of this link adapter on this host.</td><td></td><td>The values that this measure can take and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Good</td><td>0</td></tr>
<tr><td>Transitioning</td><td>5</td></tr>
<tr><td>Unknown</td><td>7</td></tr>
<tr><td>Idle</td><td>8</td></tr>
<tr><td>Disabled</td><td>13</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>Degraded</td><td>14</td></tr>
<tr><td>offline</td><td>81</td></tr>
<tr><td>Failed</td><td>91</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current operational state of a link adapter. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.
</td></tr>
<tr><td>Severity</td><td>Indicates the current health state of this link adapter on this host.</td><td></td><td>
The values that this measure can take and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Good</td><td>0</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Informational</td><td>4</td></tr>
<tr><td>Warning</td><td>81</td></tr>
<tr><td>Error</td><td>91</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current health state of a link adapter. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.
</td></tr>
</table>

3.1.4 PVM Host Details Test

Use this test to determine the current operational state of every XenServer host on which one/more protected VMs are running. If any host is in an *Error* state currently, this test will accurately point you to such a host, so that you can instantly initiate remedial actions.

Target of the test : An everRun PVM

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each ethernet adapter on each host.

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 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

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
State	Indicates the current operational state of this host.		The values that this measure can take and their corresponding numeric values are discussed in the table below: **Measure Value** / **Numeric Value** Good: 0 Transitioning: 5 Unknown: 7 Idle: 8 Disabled: 13 Degraded: 14 offline: 81 Failed: 91 **Note:** By default, this measure reports the above-mentioned **Measure Value**s while indicating the current operational state of a host. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.
Severity	Indicates the current health state of this host.		The values that this measure can take and their corresponding numeric values are discussed in the table below:

Measurement	Description	Measurement Unit	Interpretation
			<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Good</td><td>0</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Informational</td><td>4</td></tr><tr><td>Warning</td><td>81</td></tr><tr><td>Error</td><td>91</td></tr></table> **Note:** By default, this measure reports the above-mentioned **Measure Value**s while indicating the current health state of a host. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.

3.1.5 PVM XenHosts Details Test

This test reports the current operational state and health state of the XenServer master in every XenServer pool.

Target of the test : An everRun PVM

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each XenServer pool master.

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 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

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 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

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
State	Indicates the current operational state of this pool master.		The values that this measure can take and their corresponding numeric values are discussed in the table below: **Measure Value** / **Numeric Value** Good – 0 Transitioning – 5 Unknown – 7 Idle – 8 Disabled – 13

<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>Degraded</td><td>14</td></tr>
<tr><td>offline</td><td>81</td></tr>
<tr><td>Failed</td><td>91</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current operational state of a pool master. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.
</td></tr>
<tr><td>Severity</td><td>Indicates the current health state of this XenServer pool master.</td><td></td><td>
The values that this measure can take and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Good</td><td>0</td></tr>
<tr><td>Unknown</td><td>2</td></tr>
<tr><td>Informational</td><td>4</td></tr>
<tr><td>Warning</td><td>81</td></tr>
<tr><td>Error</td><td>91</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current health state of a pool master. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.
</td></tr>
</table>

3.2 The PVM Network Layer

Using the test mapped to this layer, you can instantly isolate which Ethernet adapter on which XenServer host (in a resource pool) is currently experiencing errors / degradations / failures.

Figure 3.3: The tests mapped to the PVM Network layer

3.2.1 PVM NIC Details Test

This test auto-discovers the Ethernet adapters of a host and reports the current operational and health state of each Ethernet adapter.

Target of the test : An everRun PVM

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each Ethernet adapter on each host.

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 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.

Parameter	Description
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.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by

Parameter	Description
	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
State	Indicates the current operational state of this Ethernet adapter connected to the host.		The values that this measure can take and their corresponding numeric values are discussed in the table below: **Measure Value** / **Numeric Value** Good – 0 Transitioning – 5 Unknown – 7 Idle – 8 Disabled – 13 Degraded – 14 offline – 81 Failed – 91

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>Note:

By default, this measure reports the above-mentioned Measure Values while indicating the current operational state of an Ethernet adapter. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.</td></tr>
<tr><td>Severity</td><td>Indicates the current health state of this Ethernet adapter.</td><td></td><td>The values that this measure can take and their corresponding numeric values are discussed in the table below:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Good</td><td>0</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Informational</td><td>4</td></tr><tr><td>Warning</td><td>81</td></tr><tr><td>Error</td><td>91</td></tr></table>
Note:

By default, this measure reports the above-mentioned Measure Values while indicating the current health state of an Ethernet adapter. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.</td></tr>
</table>

3.3 The PVM Layer

This layer determines the current operational and health status of the monitored PVM.

Figure 3.4: The tests mapped to the PVM layer

3.3.1 PVM Link Availability Details Test

Redundant Ethernet paths, known as Availability Links, provide a private communications path used by everRun to maintain synchronization of storage and application operations for the virtual machines that everRun protects. By periodically checking the operational and health state of each of these A-links, you can be forewarned of link failures and can endeavour to prevent such failures. This way, you can make sure that the storage and application operations of the protected VMs (PVMs) are always in sync. The **PVM Link Availability Details** test helps in this regard. This test monitors and reports the current operational state of each A-link, and also reveals which A-link is currently in an abnormal state.

Target of the test : An everRun PVM

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each availability link 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 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.

Parameter	Description
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.
EncryptType	If this EncryptFlag is set to **Yes**, then you will have to mention the encryption type by

Parameter	Description
	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
State	Indicates the current operational state of this availability link.		The values that this measure can take and their corresponding numeric values are discussed in the table below: Measure Value / Numeric Value Good 0 Transitioning 5 Unknown 7 Idle 8 Disabled 13 Degraded 14 offline 81 Failed 91

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td></td><td></td><td></td><td>Note:

By default, this measure reports the above-mentioned Measure Values while indicating the current operational state of this link. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.</td></tr>
<tr><td>Severity</td><td>Indicates the current health state availability link.</td><td></td><td>The values that this measure can take and their corresponding numeric values are discussed in the table below:

<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Good</td><td>0</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Informational</td><td>4</td></tr><tr><td>Warning</td><td>81</td></tr><tr><td>Error</td><td>91</td></tr></table>
Note:

By default, this measure reports the above-mentioned Measure Values while indicating the current health state of this link. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.</td></tr>
</table>

3.3.2 PVM Ethernet Details Test

To provide redundancy for the network, everRun selects a single network adapter – say, an Ethernet adapter - from a protected VM on each XenServer in a pool to create a single network interface in the virtual environment. This virtual adapter can then be treated and configured as any other adapter. It presents a single IP address, a single MAC address, and a single hostname to the network. To accomplish this, everRun replaces the MAC address from each Ethernet adapter it selects with a single MAC address and controls the I/O to transmit out of only one at any given time.

If any Ethernet adapter fails, everRun immediately and automatically uses the other without interruption to the application. However, if the PVM's virtual adapter fails or experiences errors, then network redundancy also be affected. To avoid such eventualities, the network adapter should be closely monitored. This what exactly the PVM Ethernet Details test does.

Target of the test : An everRun PVM

Agent deploying the test : An internal agent

Outputs of the test : One set of results for each Ethernet adapter 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 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

Parameter	Description
	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 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>State</td><td>Indicates the current operational state of this PVM Ethernet adapter.</td><td></td><td>The values that this measure can take and their corresponding numeric values are discussed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Good</td><td>0</td></tr><tr><td>Transitioning</td><td>5</td></tr><tr><td>Unknown</td><td>7</td></tr><tr><td>Idle</td><td>8</td></tr><tr><td>Disabled</td><td>13</td></tr><tr><td>Degraded</td><td>14</td></tr><tr><td>offline</td><td>81</td></tr><tr><td>Failed</td><td>91</td></tr></table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current operational state of an Ethernet adapter. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.</td></tr>
<tr><td>Severity</td><td>Indicates the current health state of this Ethernet adapter.</td><td></td><td>The values that this measure can take and their corresponding numeric values are discussed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Good</td><td>0</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Informational</td><td>4</td></tr><tr><td>Warning</td><td>81</td></tr><tr><td>Error</td><td>91</td></tr></table>
Note:</td></tr>
</table>

Measurement	Description	Measurement Unit	Interpretation
			By default, this measure reports the above-mentioned **Measure Value**s while indicating the current health state of an Ethernet adapter. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.

3.3.3 PVM State Details

Whenever everRun fails over a protected VM, you may want to know which protected VM is currently in an unavailable or unknown state, and which PVM is operational. You can determine this using the **PVM State Details** test. For every PVM, this test reports the current operatonal and health state of that PVM.

Target of the test : An everRun PVM

Agent deploying the test : An internal agent

Outputs of the test : One set of results for the target PVM 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 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

Parameter	Description
	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 • **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

<table>
<tr><th>Measurement</th><th>Description</th><th>Measurement Unit</th><th>Interpretation</th></tr>
<tr><td>State</td><td>Indicates the current operational state of this PVM.</td><td></td><td>The values that this measure can take and their corresponding numeric values are discussed in the table below:
<table>
<tr><th>Measure Value</th><th>Numeric Value</th></tr>
<tr><td>Good</td><td>0</td></tr>
<tr><td>Transitioning</td><td>5</td></tr>
<tr><td>Unknown</td><td>7</td></tr>
<tr><td>Idle</td><td>8</td></tr>
<tr><td>Disabled</td><td>13</td></tr>
<tr><td>Degraded</td><td>14</td></tr>
<tr><td>offline</td><td>81</td></tr>
<tr><td>Failed</td><td>91</td></tr>
</table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current operational state of a PVM. However, in the graph of this measure, state will be</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>represented using the corresponding numeric equivalents only.</td></tr>
<tr><td>Severity</td><td>Indicates the current health state of this PVM.</td><td></td><td>The values that this measure can take and their corresponding numeric values are discussed in the table below:
<table><tr><th>Measure Value</th><th>Numeric Value</th></tr><tr><td>Good</td><td>0</td></tr><tr><td>Unknown</td><td>2</td></tr><tr><td>Informational</td><td>4</td></tr><tr><td>Warning</td><td>81</td></tr><tr><td>Error</td><td>91</td></tr></table>
Note:
By default, this measure reports the above-mentioned Measure Values while indicating the current health state of a PVM. However, in the graph of this measure, state will be represented using the corresponding numeric equivalents only.</td></tr>
</table>

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.