TrueSight Operations Management - Veritas NetBackup Monitoring

Version 3.1.00

August 2016
Contacting BMC Software

You can access the BMC Software Web site at http://www.bmc.com. From this Web site, you can obtain information about the company, its products, corporate offices, special events, and career opportunities.

**United States and Canada**

<table>
<thead>
<tr>
<th>Address</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>BMC Software, Inc. 2101 CityWest Blvd. Houston TX 77042-2827</td>
<td>1 (713) 918 8800 or 1 (800) 841 2031 (Toll Free)</td>
</tr>
</tbody>
</table>

Copyright 2015 BMC Software, Inc. or licensors, as an unpublished work. All rights reserved.

BMC Software, the BMC Software logos, and all other BMC Software product or service names are registered trademarks or trademarks of BMC Software, Inc.

All other trademarks belong to their respective companies.

BMC Software considers information included in this documentation to be proprietary and confidential. Your use of this information is subject to the terms and conditions of the applicable End User License Agreement for the product and the proprietary and restricted rights notices included in this documentation.

**Restricted Rights Legend**

U.S. Government Restricted Rights to Computer Software. UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES. Use, duplication, or disclosure of any data and computer software by the U.S. Government is subject to restrictions, as applicable, set forth in FAR Section 52.227-14, DFARS 252.227-7013, DFARS 252.227-7014, DFARS 252.227-7015, and DFARS 252.227-7025, as amended from time to time. Contractor/Manufacturer is BMC Software, Inc., 2101 CityWest Blvd., Houston, TX 77042-2827, USA. Any contract notices should be sent to this address.
Customer Support

You can obtain technical support by using the Support page on the BMC Software Web site or by contacting Customer Support by telephone or e-mail.

Support Web Site

You can obtain technical support from BMC Software 24 hours a day, 7 days a week at http://www.bmc.com/support_home. From this Web site, you can:

- Read overviews about support services and programs that BMC Software offers
- Find the most current information about BMC Software products
- Search a database for problems similar to yours and possible solutions
- Order or download product documentation
- Report a problem or ask a question
- Subscribe to receive e-mail notices when new product versions are released
- Find worldwide BMC Software support center locations and contact information, including e-mail addresses, fax numbers, and telephone numbers

You can also access product documents and search the Knowledge Base for help with an issue at http://www.sentrysoftware.com

Support by Telephone or E-mail

In the United States and Canada, if you need technical support and do not have access to the Web, call 800 537 1813. Outside the United States and Canada, please contact your local support center for assistance. To find telephone and email contact information for the BMC Software support center that services your location, refer to the Contact Customer Support section of the Support page on the BMC Software Web site at http://www.bmc.com/support_home.
# Table of Contents

User Goals and Features .................................................................................................................. 9

Business Value ................................................................................................................................. 9

Requirements ................................................................................................................................... 10

- System Requirements .................................................................................................................... 10
- Software Requirements .................................................................................................................. 10
- Security Requirements ................................................................................................................... 10
- Remote Monitoring Requirements ................................................................................................. 11

Importing the Monitoring Solution into Central Administration ..................................................... 20

Creating the Installation Package ...................................................................................................... 21

Downloading the Installation Package ............................................................................................... 22

Installing the Package ......................................................................................................................... 22

Configuring Monitor Settings ........................................................................................................... 24

- Configuring Veritas NetBackup KM ................................................................................................. 26
  1. Configuring NetBackup Servers Monitoring ............................................................................... 26
  2. Configuring the User Account ....................................................................................................... 26
  3. Configuring Advanced Settings ..................................................................................................... 27
    - Configuring the NetBackup Server Discovery Overrides (Optional) ............................................. 28
    - Configuring the Remote Connection Settings ............................................................................. 29
    - Configuring the Maximum Number of Instances ........................................................................ 30
    - Configuring the Multi-Node Monitoring Mode ............................................................................ 31
    - Enabling the Debug Mode ........................................................................................................... 32

- Configuring Other Monitor Types .................................................................................................. 40
  - Filtering Elements to Monitor ....................................................................................................... 40
  - Configuring Jobs ............................................................................................................................ 41
  - Configuring the Log Scan Limit ..................................................................................................... 42
  - Configuring Mount Requests ........................................................................................................ 43
  - Configuring NetBackup Policies .................................................................................................. 44

- Blocking the Monitoring of Hosts ................................................................................................... 47

NetBackup Client ............................................................................................................................... 50

NetBackup Clients ............................................................................................................................ 51

NetBackup Daemon ........................................................................................................................... 52

NetBackup Daemons .......................................................................................................................... 53
Release Notes for v3.1.00
What's New

- **NBU-961** - The status of the NetBackup media servers is now monitored from the master server through the [NetBackup Media Servers](#) and [NetBackup Media Server](#) monitor types.

Changes and Improvements

- **NBU-665** – All Ksh scripts used in the monitoring solution for UNIX/Linux platforms, now support Bash as well. So if Ksh is not available on the target node, a softlink (/bin/ksh) to the Bash interpreter (/bin/bash) can be used as a workaround.

Fixed Issues

- **NBU-671** - To avoid false alarms, calendar-based backup policies are now excluded from the calculation of the next scheduled backup, allowing the State attribute of the [NetBackup Policy](#) monitor type to remain in “Idle” state instead of “Not Started”. The “Not Started” state is only set for policies that use a frequency-based backup schedule.
Key Concepts
The pages in this section provide a high-level overview of the product.

- **User Goals and Features**
- **Business Value**
- **Requirements**

**Note that for convenience and brevity, reference to TrueSight Operations Management - Veritas NetBackup Monitoring, may also be made as Veritas NetBackup KM.**

### User Goals and Features

Veritas NetBackup KM enables you to monitor the following in your environment:

- **Clients**: state and status
- **Daemons**: processor utilization, memory size, number of processes found, state and status
- **Catalog databases**: space utilization, state and status
- **Devices**: state and status, throughput of the standalone drive during the last backup activity
- **Disk pools**: up/down state and status, number of volumes
- **Jobs**: status, duration, data throughput and time elapsed since last backup, comparative statistics
- **Log Files**: size, content, growth rate, file system space utilization
- **Media Server availability**: status of local or remote media server.
- **Mounts**: elapsed time, state and status
- **Policy clients**: files and file systems excluded from and included in backup, throughput, full backup and incremental backup information
- **Policies**: elapsed time, throughput, full backup and incremental backup information
- **Robotic libraries and drives**: library and drive status, throughput, loaded media identification
- **Server availability**: status, memory and CPU time consumption
- **Disk storage and volume pools**: space utilization, status, count.

### Business Value

Veritas NetBackup KM provides current and historical information through a centralized console so you can easily view and manage your entire environment. The product collects and brings critical performance data and useful metrics into the BMC TrueSight Operations Management environment and enables Administrators to be warned whenever a problem occurs in their environment.

Veritas NetBackup KM:
ensures maximum backup application availability and maximum data protection
detects backup and restore errors
helps prevent backup system failures
detects disk or tapes space shortages
helps identify bottlenecks and optimize the backup policies.

Requirements

Before installing Veritas NetBackup KM, verify the:

- software requirements
- system requirements
- security requirements
- remote monitoring requirements.

System Requirements

The Veritas NetBackup KM supports the following operating systems:

<table>
<thead>
<tr>
<th>Operating System</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Oracle Solaris™</td>
<td>8, 9, 10, 11</td>
</tr>
<tr>
<td>HP-UX</td>
<td>11.00, 11.11, 11iv2, 11iv</td>
</tr>
<tr>
<td>IBM AIX™</td>
<td>5.1, 5.2, 5.3, 6.1</td>
</tr>
<tr>
<td>Red Hat Linux™</td>
<td>7.2</td>
</tr>
</tbody>
</table>

Software Requirements

Veritas NetBackup KM supports the following platforms:

<table>
<thead>
<tr>
<th>Platforms</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>Symantec NetBackup</td>
<td>5.0, 5.1, 6.0, 6.5, 7, 7.1, 7.5, 7.6</td>
</tr>
<tr>
<td>Veritas NetBackup</td>
<td>7.7</td>
</tr>
<tr>
<td>PATROL Agent</td>
<td>3.9.x, 9.x</td>
</tr>
<tr>
<td>BMC ProactiveNet Performance Manager</td>
<td>9.x</td>
</tr>
<tr>
<td>BMC TrueSight Operations Management</td>
<td>10.x</td>
</tr>
</tbody>
</table>
If you are running the Veritas NetBackup KM with sudo user account, or on AIX, LINUX, or Microsoft Windows x64 managed nodes, please verify these additional software requirements:

<table>
<thead>
<tr>
<th>Purpose</th>
<th>Software</th>
<th>Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>When running Veritas NetBackup KM with sudo user account on Solaris, HP-UX, AIX or Linux managed nodes</td>
<td>Sudo (superuser do)</td>
<td>1.6.7 or later</td>
</tr>
<tr>
<td>When running Veritas NetBackup KM on AIX managed nodes</td>
<td>Default <code>ncargs</code> value for processing <code>bpdbjobs</code> output may not be sufficient. Check this attribute using: `lsattr -EH -l sys0</td>
<td>grep ncargs<code>If the value is below 16, increase it using:</code>chdev -l sys0 -a ncargs=16`</td>
</tr>
<tr>
<td>When running Veritas NetBackup KM on Linux managed nodes</td>
<td>Korn shell binary <code>/bin/ksh</code></td>
<td>Any</td>
</tr>
<tr>
<td>When running Veritas NetBackup KM on Microsoft Windows x64 managed nodes</td>
<td>Reg.exe patch KB948698 (<a href="http://support.microsoft.com/kb/948698">http://support.microsoft.com/kb/948698</a>)</td>
<td>Any</td>
</tr>
</tbody>
</table>

⚠️ The Microsoft Windows x64 `Reg.exe` patch, **KB948698** is required to allow access to 64-bit registry keys from PATROL Agent. Access the above patch site from the managed node to obtain the correct patch for that platform.

### Security Requirements

A user account with administrative privileges must be configured in BMC TrueSight Operations Management to read and execute Veritas NetBackup application programs and access file systems. Depending on the operating systems used, several options will be available.

The following user accounts can be used:

- **On Unix platforms:**
  - a root user
  - a non-root user, such as patrol, that has sudo privileges on Veritas NetBackup to execute application programs and access file systems
  - a non-root account, such as patrol, configured in Veritas NetBackup application to administer the Veritas NetBackup application.

- **On Windows platforms:**
  - an administrator user
  - a non-administrator account, such as patrol, configured in Veritas NetBackup application to administer the Veritas NetBackup application. Refer to the Veritas NetBackup System Administrator’s Guide for details on how to set up this type of account.
- Users added to NBU_Admin user group in VxSS. Please make sure the credentials of this user do not expire using the utility nbac_cron.

The user login details are configured in the Veritas NetBackup KM. The password is encrypted and stored in the PATROL Agent.

**Access Permissions**

The Veritas NetBackup KM user needs “read & execute” permission to executable and library files under the paths listed below. The Veritas NetBackup installation path INSTALL_PATH, referenced in the tables below is normally /usr/openv or /opt/VRTSnetbp (on Unix) or C:\Program Files\Veritas (on Microsoft Windows).

**Executable and Library Files accessed by the Veritas NetBackup KM User**

<table>
<thead>
<tr>
<th>Unix</th>
<th>Microsoft Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALL_PATH/netbackup</td>
<td>INSTALL_PATH\NetBackup</td>
</tr>
<tr>
<td>INSTALL_PATH/netbackup/bin</td>
<td>INSTALL_PATH\NetBackup\bin</td>
</tr>
<tr>
<td>INSTALL_PATH/netbackup/bin/admincmd</td>
<td>INSTALL_PATH\NetBackup\bin\admincmd</td>
</tr>
<tr>
<td>INSTALL_PATH/netbackup/bin/goodies</td>
<td>INSTALL_PATH\NetBackup\bin\goodies</td>
</tr>
<tr>
<td>INSTALL_PATH/volmgr/bin</td>
<td>INSTALL_PATH\Volmgr\bin</td>
</tr>
<tr>
<td>INSTALL_PATH/volmgr/bin/goodies</td>
<td>INSTALL_PATH\Volmgr\bin\goodie</td>
</tr>
<tr>
<td>INSTALL_PATH/lib</td>
<td>C:\Program Files\Common Files\VERITAS Shared</td>
</tr>
<tr>
<td>/usr/openwin/lib</td>
<td>INSTALL_PATH\NetBackup\lib</td>
</tr>
</tbody>
</table>

If the KM is enabled to failover in a clustered environment, the login user needs execute permissions to the following cluster commands:

- `/opt/VRTSvcs/bin/hagrp` (in Veritas Cluster Server)
- `vxctl` (in Veritas Cluster File System)
- `/usr/cluster/bin/clrg` (in Oracle Solaris Cluster)
- `cluster` (in Microsoft Cluster)

Veritas NetBackup KM includes some scripts which should be executable by the PATROL Agent user and the Veritas NetBackup KM user. These scripts are stored under KM_HOME path, normally PATROL_HOME/lib/NBU.
To list all OS commands used by Veritas NetBackup KM, execute the following PSL code from the PATROL Console, using PSL Task menu, after installing and loading the KM.

```
foreach var (grep("^/Runtime/NBU/.*CommandControls/",pconfig("LIST")))
{
  ctl=get(var);
  opt=ntharg(grep("^Option",ctl),"2-"," =");
  nsa=ntharg(grep("^NoSudoAttempt",ctl),"2-"," =");
  sua=ntharg(grep("^SingleUserAttempt",ctl),"2-"," =");
  typ=ntharg(grep("^CommandType",ctl),"2-"," =");
  cmd=nthargf(grep("^CommandText",ctl),"2-","=");";
  if(osp=="") { osp=trim(nthargf(grep("^OSPlatform",ctl),"2-","=")," "); }
  fields=lines(ntharg(var,"1-","/"));
  old_host=host;
  host=(fields == 5)? ntharg(var,"3","/"): "localhost";
  if(host!=old_host)
  {
    if((osp!="WINDOWS") && sudoers) { printf("\n\n%shas been run with sudo:
%s",osp,sudoers); } 
    printf("\n\n%shas been run on %s:
\n",osp,host);
    i=0; sudoers=""; osp="";
  }
  if((typ == "")||(typ == "OS"))
  {
    met="";
    if(opt == "NoLogin") { met = "(run as patrol user)"; }
    elsif(nsa == "YES") { met = "(run as configured user without sudo)"; }
    elsif(sua == "YES") { met = "(run as supplied user - used in menu)"; }
    else
    {
      scmd=cmd;
      s=index(scmd, "%sudo");
      if(s) { scmd=replace(substr(scmd,s,length(scmd)),"%sudo",""); }
      sudoers=union(sudoers,ntharg(nthargf(scmd,1,">"),"1-"," "," "));
    }
    printf("%2d \%-30s \%-40s: %s\n",i++,ntharg(var,fields,"/"),met,cmd);
  }
  if((osp!="WINDOWS") && sudoers) { printf("\n\n%shas been run with sudo:
%s",osp,sudoers); }
```

### Paths and Files Accessed by PATROL Agent User

<table>
<thead>
<tr>
<th>Unix</th>
<th>Microsoft Windows</th>
</tr>
</thead>
<tbody>
<tr>
<td>INSTALL_PATH/-netbackup-db</td>
<td>INSTALL_PATH\NetBackup-db</td>
</tr>
<tr>
<td>INSTALL_PATH/volmgr-database</td>
<td>INSTALL_PATH\Volmgr-database</td>
</tr>
<tr>
<td>INSTALL_PATH/var</td>
<td>INSTALL_PATH\NetBackup\var</td>
</tr>
<tr>
<td>INSTALL_PATH/netbackup-db/error/-daily-_messages.log</td>
<td>INSTALL_PATH\NetBackup\db\error-log_date</td>
</tr>
<tr>
<td>/var/adm/messages (on Solaris)</td>
<td></td>
</tr>
<tr>
<td>/var/adm/syslog/syslog.log (on HP-U_X)</td>
<td></td>
</tr>
<tr>
<td>/var/log/messages (on Linux)</td>
<td></td>
</tr>
</tbody>
</table>

On Windows platforms the Veritas NetBackup installation is identified by checking the Microsoft Windows Registry:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Veritas\NetBackup\  

The configured login user should have sufficient privileges to run regedit command on the managed node.

### Sudo User for Operating System Access

If a non-root user with sudo privileges is preferred as the Veritas NetBackup KM user, configure the account as a sudoer through the visudo utility using code appropriate for your platform as detailed below. This user should be able to execute NetBackup commands and OS commands listed in above.

The code below also applies to all non-root users who may execute NetBackup KM administration and report menu commands using their sudo privileges. The KM accepts any non-root user with the following sudo configuration in the sudoers file. Please replace user1, user2, user3 with appropriate KM user names. The Veritas NetBackup installation path INSTALL\_PATH, referenced below is normally /usr/openv or /opt/VRTSnetbp and PATROL\_HOME is the path where the PATROL Agent is installed (including the target, like /opt/bmc/Patrol3/Solaris29-sun4/).

⚠️ This non-root sudo user configured in Veritas NetBackup KM will be able to execute Veritas NetBackup commands. To prevent unauthorized access, ensure this user is only used within Veritas NetBackup KM and not made public for general use.
Entering the non-root sudo user with ‘Use Sudo’ option selected in to the login configuration dialog, before updating the sudoers file, will generate sudo errors. Also if the sudo user is configured differently, Veritas NetBackup KM may run sudo commands using incorrect sudo settings, which may expose the sudo user password.

On Solaris

User_Alias NBUKMUSERS = user1, user2, user3
Defaults:NBUKMUSERS !lecture,!authenticate,!requiretty,\nenv_keep+="PATH LD_LIBRARY_PATH INSTALL_PATH KM_HOME KM_TEMP",env_reset
NBUKMUSERS ALL=/bin/*,/sbin/*,/usr/bin/*,/usr/sbin/*,\INSTALL_PATH/netbackup/bin/*,\INSTALL_PATH/netbackup/bin/admincmd/*,\INSTALL_PATH/netbackup/bin/goodies/*,\INSTALL_PATH/volmgr/bin/*,\INSTALL_PATH/volmgr/bin/goodies/*,\PATROL_HOME/lib/NBU/*,PATROL_HOME/bin/*

user1, user2, user3 must be replaced with username(s) used by Veritas NetBackup KM; INSTALL_PATH and PATROL_HOME with the relevant paths. PATROL_HOME paths are only required for local monitoring.

On HP-UX

User_Alias NBUKMUSERS = user1, user2, user3
Defaults:NBUKMUSERS !lecture,!authenticate,!requiretty,\nenv_keep+="PATH SHLIB_PATH INSTALL_PATH KM_HOME KM_TEMP",env_reset
NBUKMUSERS ALL=/bin/*,/sbin/*,/usr/bin/*,/usr/sbin/*,\INSTALL_PATH/netbackup/bin/*,\INSTALL_PATH/netbackup/bin/admincmd/*,\INSTALL_PATH/netbackup/bin/goodies/*,\INSTALL_PATH/volmgr/bin/*,\INSTALL_PATH/volmgr/bin/goodies/*,\PATROL_HOME/lib/NBU/*,PATROL_HOME/bin/*

user1, user2, user3 must be replaced with username(s) used by Veritas NetBackup KM; INSTALL_PATH and PATROL_HOME with the relevant paths. PATROL_HOME paths are only required for local monitoring.
On AIX & Linux

User_Alias NBUKMUSERS = user1, user2, user3
Defaults:NBUKMUSERS !lecture,!authenticate,!requiretty,\nenv_keep+="PATH LIBPATH INSTALL_PATH KM_HOME KM_TEMP",env_reset
NBUKMUSERS ALL=/bin/*,/sbin/*,/usr/bin/*,/usr/sbin/*,\nINSTALL_PATH/netbackup/bin/admincmd/*,\nINSTALL_PATH/netbackup/bin/goodies/*,\nINSTALL_PATH/volmgr/bin/*,\nINSTALL_PATH/volmgr/bin/goodies/*,\nPATROL_HOME/lib/NBU/*,PATROL_HOME/bin/*

⚠️ user1, user2, user3 must be replaced with username(s) used by Veritas NetBackup KM; INSTALL_PATH and PATROL_HOME with the relevant paths. PATROL_HOME paths are only required for local monitoring.

Remote Monitoring Requirements

Remote monitoring is required for all servers or appliances on which no PATROL Agent can be installed. This feature is also interesting if you lack resources or time to deploy a PATROL Agent and Veritas NetBackup KM on several servers since it allows to monitor multiple hosts from one agent.

⚠️ Remote monitoring is not possible from a UNIX/Linux PATROL Agent system to a Windows-based NetBackup server.

The requirements listed below must be met to be able to use remote monitoring.

JAVA

Veritas NetBackup KM requires Java 1.6 or higher and a Java Runtime Environment (JRE) to be installed on the same system that runs the PATROL Agent.

The KM will automatically detect the JRE path if it has been installed in the default location or under the BMC PATROL Agent installation path. If it has been installed in a different location, you will have to set JAVA_HOME for the Patrol Agent default account before starting the PATROL Agent.

You can download the Java Runtime Environment along with the KM on the Sentry Software Web site.
NetBackup CLI User Account

A NetBackup CLI user is required to monitor NetBackup appliances. To create a NetBackup user account:

1. Open an SSH session on the NetBackup appliance
2. Log on as admin
3. Enter the following command:
   ```
   Main > Manage > NetBackupCLI > Create UserName
   ```
   where UserName is the name to be used for the new user.
4. Enter a password for this new user account
5. A confirmation message appears stating the new user account was created successfully.

This user should have the privileges to execute NetBackup and OS commands as described in the Security Requirements section. The following sudo settings are therefore required on a NetBackup appliance:

```
# Added for NetBackup KM
User_Alias NBUKMUSERS = UserName
Defaults:NBUKMUSERS !lecture,!authenticate,\
env_keep+="PATH LIBPATH INSTALL_PATH KM_HOME KM_TEMP",env_reset
```

SSH/WMI Connection

An SSH (UNIX/Linux platforms) or a WMI (Windows platforms) connection is required to monitor remote NetBackup servers and appliances. When using an SSH connection, the SSH host key authentication must be disabled on the remote host.

Disabling the SSH Host Key Authentication

SSH host key authentication is enabled by default on most NetBackup servers and appliances. To disable it:

1. Open the global SSH configuration file (ssh_config) stored in the `/etc/ssh/` directory on the remote host
2. Add the line `StrictHostKeyChecking no`
3. Save the file.
Installing the Monitoring Solution
Once the latest version of the solution has been loaded into Central Monitoring Administration, administrators can create all the installation packages required for their different operating systems and platforms and save them for later use in the Monitoring Installation Packages list. These packages can then be deployed to multiple computers. Administrators just have to connect to TrueSight Operations Management from the server where they want to install the package, download it and launch the installation.

This section describes the different steps to follow to install Veritas NetBackup KM:
- Importing Veritas NetBackup KM into Central Monitoring Administration
- Creating the Installation Package
- Downloading the Installation Package
- Installing the Package
Importing the Monitoring Solution into Central Administration

The TrueSight Central Monitoring Repository includes the current versions of TrueSight Operations Management - Veritas NetBackup Monitoring that you can use with BMC TrueSight. If the version available in the Repository does not correspond to the latest one, you will have to manually import it:

1. Log on to the **BMC TrueSight Operations Management** Console.
2. Launch **Central Monitoring Administration**.
3. Click the **Repository** drawer and select **Manage Repository**.
4. Check that the version of the BMC component available is actually the latest one. If not, download the latest version corresponding to your operating system (Windows or UNIX/Linux) available on the [Sentry Software Website](http://www.sentrysoftware.com).
5. From **TrueSight Operations Management**, click **Import**.
6. Select **Single solution**.
8. Click **Import**.

The selected archive file is imported to the repository.
Creating the Installation Package

The installation package to deploy to managed systems can be created directly from TrueSight Operations Management:

1. Log on to TrueSight Operations Management
2. Click the Repository drawer and select Deployable Package Repository.
3. Click Add.
4. Select the operating system and platform for which you want to create a package. The components available in the repository for the selected operating system and platform are displayed.
5. Select the Installation Package Component:
   - From the Available components list, select the relevant component.
   - From the Version list, select the latest version.
   - Click the right arrow button to move the component into the Selected Components list. By default, the appropriate BMC PATROL Agent for the operating system and platform that you chose is included in the Selected components list.
   - Click Next. The Add Component Installation Package wizard are displayed.
6. Go through the wizard and specify the required PATROL information. The Installation Package Details is displayed.
7. Verify that:
   - the operating system and platform are correct
   - the components that you want to include are listed in the Included Components list.
8. Provide the following information:
   - Name: Enter a unique name for the package.
   - (Optional) Description: Enter a description of the package. The description is displayed in the Monitoring Installation Packages list on the Monitoring Repository window.
   - Format: Select a file compression format for the package.
9. Click Save Installation Package.
10. Click Close. The package is now available in the Monitoring Installation Packages list.
Downloading the Installation Package

You can download an installation package and install the components on one or more hosts. The installation runs silently with the information entered during package creation.

**Recommendation**
If you defined the BMC TrueSight Integration Service variable for PATROL Agents in the installation package, ensure the agents are started in phases. Do not start newly deployed agents all at once. Start and configure monitoring for the agents in planned phases to reduce the performance impact on the Integration Service nodes and on the BMC TrueSight Server associated with the automatic workflow process.

1. Log on to TrueSight Operations Management from the computer on which the PATROL Agent is installed or to be installed.
2. Click the Repository drawer and select Deployable Package Repository.
3. (Optional) To filter the list of installation packages, select an operating system from the Filter by Operating System list.
4. Click the link for the installation package that you want to download.
5. Through the browser's download dialog box, save the installation package.

Installing the Package

This chapter provides a step by step procedure to install a monitoring solution package:

1. From the computer on which you want to install the package, log on to TrueSight Operations Management.
2. (Optional) To filter the list of installation packages, select an operating system from the Filter by Operating System list.
3. Click the link for the installation package that you want to download.
4. Through the browser's download dialog box, save the installation package in a temporary file.
5. Extract the installation package that is appropriate for your operating system. The package is extracted to the bmc_products directory on the current host.
6. From the bmc_products directory, run the installation utility for your operating system:
   - (UNIX or Linux) RunSilentInstall.sh
   - (Microsoft Windows) RunSilentInstall.exe

The package is installed on the current host. If the package includes a BMC PATROL Agent, the agent sends a configuration request by passing its tags to Central Monitoring Administration, via the Integration Service. Central Monitoring Administration evaluates policies that match the tags, determines the final configuration to be applied, and sends the configuration information back to the agent. Monitoring is based on the configuration information received by the agent.
Configuring After Installation
Configuring Monitor Settings

When you create a policy, you can configure monitor types. The **Add Monitor Types** dialog box presents configuration fields for compatible BMC PATROL monitoring solutions that are located in the Central Monitoring Repository.

To configure the Monitor Type settings

1. Log on to **Central Monitoring Administration**.
2. In the **Navigation** pane, click the **Policies** drawer and select a policy view (e.g. **All**).
3. Click **Add**.
4. Configure the policy general settings and click **Next**.
5. In the **Monitoring Policy Configuration** window, click **Add**.
6. From the **Monitoring Solution** menu, select **Veritas NetBackup**.
7. From the **Version** menu, select the required version.
8. From the **Monitor Type** menu, select the required monitor:

<table>
<thead>
<tr>
<th>Monitor Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Veritas NetBackup KM (REQUIRED)</td>
<td>To set the general settings of the Veritas NetBackup monitoring solution (credentials, debug mode, instances, multi-node mode, etc.).</td>
</tr>
<tr>
<td></td>
<td>✏ Once this monitor type is configured, all other monitor types are automatically monitored. Their default behavior can however be modified by selecting them from the Monitor Type list. No other monitor types can be configured as long as Veritas NetBackup KM is not configured.</td>
</tr>
<tr>
<td>NetBackup Client</td>
<td>To modify the client default monitoring.</td>
</tr>
<tr>
<td>NetBackup Daemon</td>
<td>To modify the daemons monitoring.</td>
</tr>
<tr>
<td>NetBackup Disk Pool</td>
<td>To modify the disk pools default monitoring.</td>
</tr>
<tr>
<td>NetBackup Disk Storage</td>
<td>To modify the disk storage default monitoring.</td>
</tr>
<tr>
<td>NetBackup Disk Volume</td>
<td>To modify the disks volume default monitoring.</td>
</tr>
</tbody>
</table>
| NetBackup Job           | To modify the job default monitoring. You can more especially indicate:  
  ✡ how long the jobs in OK, Suspicious, and Failure status will be monitored.  
  ✡ the status the jobs will have when the monitoring period is over. |
| NetBackup Log           | To modify the log default monitoring. You can more especially specify the number of KBytes of data to be scanned for each log file during each data collection cycle. By default: 500 KBytes |
| NetBackup Media Server  | To modify the media server default monitoring.                                                                                                                                              |
| NetBackup Mount Request | To modify the mount request default monitoring. You can more especially indicate:  
  ✡ how long the mount requests will be monitored. |

Configuring Monitor Settings
Configuring Monitor Settings

<table>
<thead>
<tr>
<th>Monitor Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>• the date/time format used in NetBackup mount request messages.</td>
</tr>
<tr>
<td><strong>NetBackup Policy</strong></td>
<td>To modify the policy default monitoring. You can more especially:</td>
</tr>
<tr>
<td></td>
<td>• specify the policy elements to be monitored.</td>
</tr>
<tr>
<td></td>
<td>• set backup restrictions.</td>
</tr>
<tr>
<td><strong>NetBackup Policy Client</strong></td>
<td>To modify the policy client default monitoring.</td>
</tr>
<tr>
<td><strong>NetBackup Robotic Drive</strong></td>
<td>To modify the robotic drives default monitoring.</td>
</tr>
<tr>
<td><strong>NetBackup Robotic Library</strong></td>
<td>To modify the robotic libraries default monitoring.</td>
</tr>
<tr>
<td><strong>NetBackup Standalone Drive</strong></td>
<td>To modify the standalone drives default monitoring.</td>
</tr>
<tr>
<td><strong>NetBackup Volume Pool</strong></td>
<td>To modify the volume pools default monitoring.</td>
</tr>
</tbody>
</table>
Configuring Veritas NetBackup KM

Before using Veritas NetBackup KM, you will have to configure its general settings:

- Specify the NetBackup servers to be monitored
- Configure the user account
- Possibly configure the advanced settings (Discovery Overrides, debug mode, number of instances, and multi-node monitoring mode)

1. Configuring NetBackup Servers Monitoring

To specify the NetBackup master/media server or the NetBackup appliance to be monitored:

1. Create a new monitor type
2. From the Monitor Type menu, select Veritas NetBackup KM
3. In the NetBackup Server section:

   - (Required) Enter the Hostname, IP Address, or FQDN of the NetBackup server to be monitored.
   - (Required) Specify whether the NetBackup server is a UNIX/Linux or Windows system.
   - Check Create a Device in the Console if you want the NetBackup server to appear as a separate device in TrueSight OM.

4. You will then have to configure the user account to be used.

2. Configuring the User Account

A user account with administrative privileges must be configured in BMC TrueSight Operations Management to read and execute Veritas NetBackup application programs and file systems. Depending on the operating systems used, several options will be available.

On Unix platforms, you can use the following user accounts:

- a root user
- a non-root user, such as patrol, that has sudo privileges on Veritas NetBackup to execute application programs and access file systems
- a non-root account, such as patrol, configured in Veritas NetBackup application to administer the Veritas NetBackup application.
On Windows platforms, you can use the following user accounts:

- an administrator user
- a non-administrator account, such as patrol, configured in Veritas NetBackup application to administer the Veritas NetBackup application.

**To configure the user account**

1. **Specify the NetBackup Server to be monitored.**
2. Locate the **NetBackup Credentials** section:

   ![](image)

3. To use:
   - the default PATROL Agent Account, check the **Use Agent Default Account** box and leave the **Username** and **Password** fields empty
   - a different user account, enter the login details in the **Username** and **Password** fields
4. **(UNIX Only)** If a sudo user account is used:
   - check the **Use Sudo** box
   - indicate the **Sudo** binary file **path** (by default: /usr/local/bin/sudo)
5. Click **Add to List**.
6. **(Optional)** You can now configure [advanced settings](#).

**3. Configuring Advanced Settings**

Once the Veritas NetBackup server to be monitored and the account to be used are specified, you can configure the following advanced settings:

- **The NetBackup server discovery overrides**
- **The remote connection settings**
- **The maximum number of instances**
- **The multi-node monitoring mode**
- **The debug mode**.
Configuring the NetBackup Server Discovery Overrides (Optional)

The solution automatically discovers the NetBackup installation path, the NetBackup log path, the remote temp directory path, the NetBackup temporary directory path, the node type, and the node status daemons. This information can however be overridden.

To configure NetBackup server discovery overrides

1. Specify the NetBackup Server to be monitored and the user account to be used
2. In the Advanced Settings section, click the Discovery Overrides button
3. Indicate:
   - the NetBackup Installation Path
   - the NetBackup Log Path
   - the Remote Temp Directory Path
   - the Node Type (media or master server)
   - the Node Status Daemons
4. Click Close
5. Click Add to List.
Configuring the Remote Connection Settings

If you configured the monitoring of a remote host, you may want to specify the time after which the connection to the remote node will timeout or the maximum number of simultaneous connections allowed to the remote node. This configuration is possible through the Advanced Settings options.

To configure the remote connection settings

1. Specify the NetBackup Server to be monitored and the user account to be used
2. In the Advanced Settings section, click the Advanced button

![Advanced Settings](image)
3. The **Advanced** dialog is displayed:

![Advanced Settings Dialog](image)

*Configuring Advanced Settings*
4. Click the **Connection Settings** button

```
  Connection Settings
  Connection Timeout (in Seconds)  30
  Maximum Connections              10
```

5. Enter the required values in the available fields:
   - **Connection Timeout (in Seconds)**: Enter the number of seconds after which the connection to the remote node will timeout.
   - **Maximum Connections**: Enter the maximum number of simultaneous connections allowed to the remote node.

6. Click **Close** on all pop-ups

7. Click **Add to List** in the main window.

### Configuring the Maximum Number of Instances

By default, the solution monitors all the elements discovered, which may represent an important workload to the agents and servers. Because the monitoring of some elements may be irrelevant for various reasons, you can configure the maximum number of instances to be monitored.

⚠️ Because increasing the number of instances may impact the performance of the solution, it is recommended to only monitor critical elements in large environments.

### To configure the maximum number of instances

1. **Specify the NetBackup Server to be monitored** and the **user account to be used**
2. In the **Advanced Settings** section, click the **Advanced** button

```
  Advanced Settings
  Discovery Overrides  Advanced
```

---

*Sentry Software*
3. The **Advanced** dialog is displayed:

![Advanced Settings Dialog](image)

**Configuring Advanced Settings**
4. Click the **Maximum Instances** button

5. For each monitored element, indicate the number of instances to be displayed

6. Enter **0** in the relevant field to disable the monitoring of a specific element

7. Click **Close** on all pop-ups

8. Click **Add to List** in the main window.
Configuring the Multi-Node Monitoring Mode

If the Veritas NetBackup environment is installed in a cluster using Veritas Cluster Server, Veritas Cluster File System, Oracle Solaris Cluster, or Microsoft Cluster, Veritas NetBackup KM must be installed on all the cluster nodes to enable continuous monitoring and avoid single point of failure. To avoid duplicate alerts from multiple nodes, it is recommended to configure the solution to operate in multi-node monitoring mode.

⚠️ At that time, the Multi-node monitoring mode feature cannot be used if one or more cluster nodes are monitored remotely.

To configure the multi-node monitoring mode

1. Specify the NetBackup Server to be monitored and the user account to be used
2. In the Advanced Settings section, click the Advanced button

![Advanced Settings]

Configuring Advanced Settings
3. The **Advanced** dialog is displayed:

![Advanced Dialog](image)

4. Select **Enable Multi-node Monitoring Mode** and click **Multi-node Mode Config...**

![Multi-node Mode Configuration](image)
5. Configure the Multi-node Mode:
   - Select the appropriate **Cluster Application**.
   - Indicate the **Failover Group Name**. Leave this field blank if you previously selected Veritas Cluster File System. Then the Veritas NetBackup KM will monitor the entire cluster from the active master system, which is identified by “vxdctl -c mode” command. This method requires vxconfigd in enable mode with its clustered state active.
   - In the **Monitoring Node Names** field, name all the nodes where the solution is installed. The list must be delimited by commas.

6. (Optional) Allow the solution to check the monitoring mode of the remote PATROL Agents. If the **Remote PATROL Agent Checking** is disabled, the solution will monitor actively through active master system or on the node where failover group is online and will not check the monitoring status of the other nodes through PATROL Agent:
   - Check the **Enable Remote PATROL Agent Checking** box.
   - Click the **Remote Agent** button. The following dialog box is displayed:

   ![Remote Agent](image)
In the Monitoring Node Name field, indicate the cluster node used for multi-node mode failover.

Indicate all the information required to communicate with the remote PATROL Agent (protocol, port number, and credentials).

In the Number of Attempts field, indicate how many times the solution will try to communicate with the remote PATROL Agent before failing over.

Enter the timeout between attempts.

Click Add to List.

Resume the procedure for all the nodes previously listed.

7. Click Close on all pop-ups.
8. Click Add to List in the main window.

Veritas NetBackup will then be monitored through the master or online node. The other nodes, which are standing by for a failover, will be in passive multi-node mode and only the Veritas NetBackup components which cannot be monitored from the active node will be monitored.

⚠️ If a managed node is unable to determine the system which should be in Active Multi-node Mode, it will change to Temporary Single-node Mode. It will reset as soon as it detects a system in Active Multi-node Mode. If multiple managed nodes in a cluster runs in Single-node Mode or Temporary Single-node Mode, duplicate events may be triggered from shared components (clients, policies, jobs, requests, robotic libraries, drives, volume pools and storages).

Enabling the Debug Mode

When you encounter an issue and wish to report it to Sentry Software, you will be asked to enable the Debug Mode and provide the debug output to the Sentry Software support team.

To enable the debug mode

1. Specify the NetBackup Server to be monitored and the user account to be used.
2. In the Advanced Settings section, click the Advanced button.
3. The **Advanced** dialog is displayed:

![Advanced Settings Dialog](image)
4. Click the **Debug** button

5. Select all the elements for which you want to obtain debug information

6. In the **Options** section, indicate:
   - when the system must stop logging debug information. The required format is: `YYYY/MM/DD HH:MM:SS`
   - where the debug file will be stored. The default path is: `<PATROL_HOME>/lib/NBU/debug`

7. Click **Close** on all pop-ups

8. Click **Add to List** in the main window.

When the debug end time is reached, a tar/zip file is automatically created under `<PATROL_HOME>/lib/NBU` and can be sent to the BMC Support for help. It is also recommended to check the `NBU_<PATROLAgent-Port>.log` file, stored in `<PATROL_HOME>/log`, for any error.
Configuring Other Monitor Types
Filtering Elements to Monitor

By default, the solution monitors all the elements discovered, which may represent an important workload to the agents and the TrueSight OM servers. Because the monitoring of some elements may be irrelevant for various reasons, you can apply filters to indicate which elements will be monitored or not.

Filtering options are available for the following monitor types: NetBackup Client, NetBackup Daemon, NetBackup Disk Pool, NetBackup Disk Storage, NetBackup Disk Volume, NetBackup Policy, NetBackup Policy Client, NetBackup Media Server, NetBackup Robotic Drive, NetBackup Robotic Library, NetBackup Standalone Drive, and NetBackup Volume Pool.

To filter elements to monitor

1. **Add or edit a monitor type**
2. Select the **Monitor Type** for which you wish to apply filters.
   
   ! If you apply filters to the NetBackup Policy Monitor Type, only the backup/restore jobs of the monitored policies will be monitored.

3. In the **Hostname** field, enter:
   - `localhost` to apply these settings to all PATROL Agents installed on NetBackup Master and Media servers
   - a hostname or IP address to apply these settings to a specific server

4. Indicate which elements will be monitored:
   - Click the **Filtering** button
   - In the **Keep Only...** section, indicate the element to be monitored and click **Add to List**
   - In the **Exclude...** section, indicate the element not to be monitored and click **Add To List**
   - Resume procedure to keep and/or exclude as many elements as required
   - Click **Close**

5. If needed, manually add elements to be monitored:
   - Click the **Manual Add** button
   - Indicate the element to be monitored and click **Add to List**
   - Resume procedure to add as many elements as required
   - Click **Close**

6. Click **Add to List**
7. Click **Add**
8. Finally, **Update** the policy.
Configuring Jobs

By default, Veritas NetBackup KM monitors all scheduled jobs that completed successfully for 24 hours and any other scheduled job for 72 hours. This monitoring duration can however be modified to better suit your requirements.

⚠️ Increasing the monitoring duration may affect the performance of the application.

To configure jobs

1. Add or edit a monitor type and select NetBackup Job as a Monitor Type.

![Configuring NetBackup Jobs](image)
2. In the **Hostname** field, enter:
   - *localhost* to apply these settings to all PATROL Agents installed on NetBackup Master and Media servers
   - a hostname or IP address to apply these settings to a specific server
3. In the **Monitoring Duration** section:
   - Indicate how many hours the jobs in **OK**, **Suspicious**, and **Failure** status will be monitored
   - Select **Keep Monitoring Active Jobs Indefinitely** if you prefer to endlessly monitor active jobs
4. Under the **Exit Status Filter Configuration**, enter the exit status codes to either Erroneous Exit Status Codes or Failure Exit Status Codes, which will set the job state to Error or Failed respectively. By default, exit status code 1 sets the job state to Error and all other non-zero exit status codes (except 150 - terminated by administrator) set the job state to Failed. Multiple exit status codes can be entered, using a comma (,) as a separator or a range using a hyphen (-) between start and end values.
5. Click **Add to List**
6. Click **Add**
7. Finally, **Update** the policy.
Configuring the Log Scan Limit

**TrueSight Operations Management - Veritas NetBackup Monitoring** scans log files by reading the new log entries since the last data collection cycle. By default, only 500 KBytes of data is scanned for each log file during each data collection cycle. This log scan limit can however be modified to better suit your requirements.

⚠ Increasing the Log Scan Limit may impact the performance of the data collector (NBULogCollector), the monitoring solution, and the PATROL Agent.

**To customize the log scan limit**

1. **Add or edit a monitor type** and select **NetBackup Log** as a Monitor Type.

2. In the **Hostname** field, enter:
   - **localhost** to apply these settings to all PATROL Agents installed on Veritas NetBackup Servers
   - a hostname or IP address to apply these settings to a specific server

3. In the **Log Scan Limit** field, indicate the amount of data (in KBytes) that will be read by the monitoring solution during each data collection cycle

4. Click **Add to List**

5. Click **Add**

6. Finally, **Update** the policy.
Configuring Mount Requests

By default, Veritas NetBackup KM monitors all mount requests for 24 hours. This monitoring duration can however be modified to better suit your requirements.

⚠️ Increasing the monitoring duration may affect the performance of the application.

To configure mount requests:

1. **Add or edit a monitor type** and select **NetBackup Mount Request** as a Monitor Type.

2. In the **Hostname** field, enter:
   - `localhost` to apply these settings to all PATROL Agents installed on NetBackup Master and Media servers
   - A hostname or IP address to apply these settings to a specific server

3. In the **Mount Request Configuration** section, indicate how many hours the mount requests will be monitored.

4. If the date/time format returned by Veritas NetBackup commands is different from your local system time zone, you will have to configure it in the **Date/Time Format Configuration** section:
   - Indicate the **Expected Format**. Refer to the table below to know the valid formats:

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default Date/Time Format</td>
<td>Leave blank.</td>
</tr>
<tr>
<td>EPOCH</td>
<td>Set EPOCH, if the time format is the number of seconds that have elapsed since 00:00:00 GMT January 1, 1970</td>
</tr>
<tr>
<td>Year Formats</td>
<td></td>
</tr>
<tr>
<td>YY</td>
<td>Two digit figure</td>
</tr>
<tr>
<td>Format</td>
<td>Description</td>
</tr>
<tr>
<td>--------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| YYYY  | Four digit figure  
Example: 2012 |

**Month Formats**

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
</table>
| MO     | Two digit figure  
Example: 02 for February |
| MONTH  | Month full name  
Example: February |
| MON    | Three character name  
Example: Feb |

**Date Formats**

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
</table>
| DD     | Two digit figure  
Example: 05 |

**Day Formats**

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
</table>
| DAYFULL| Day full name  
Example: Friday |
| DAY    | Three character name  
Example: Fr |

**Hour Formats**

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>HH</td>
<td>Two digit figure</td>
</tr>
</tbody>
</table>

**Minute Formats**

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MM</td>
<td>Two digit figure</td>
</tr>
</tbody>
</table>

**Second Formats**

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SS</td>
<td>Two digit figure</td>
</tr>
</tbody>
</table>

**Time Formats**

<table>
<thead>
<tr>
<th>Format</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>[blank]</td>
<td>Time is in 24-hour format</td>
</tr>
</tbody>
</table>
| PM     | Time is in 12-hour format; am/pm is displayed  
Example: 10:15:00pm |
| P.M    | Time is in 12-hour format; a.m/p.m is displayed  
Example: 10:15:00p.m |

- Indicate a PSL-compatible Time Zone String (e.g.: NZDT, NZST, EDT, EST, GMT-1200, etc.)

5. Click **Add to List**
6. Click **Add**.
Configuring NetBackup Policies

By default, Veritas NetBackup KM monitors all policies configured on the master server, except the standard template policies. Filters can however be applied to better suit your requirements. Additionally, a restriction window can be configured for policy backups.

To configure policies

1. Add or edit a monitor type and select NetBackup Policy as a Monitor Type.

2. In the Hostname field, enter:
   - localhost to apply these settings to all PATROL Agents installed on NetBackup Master and Media servers
   - a hostname or IP address to apply these settings to a specific server

2. Set the filtering options. Refer to Filtering Elements to Monitor for more details.

3. If you want a warning to be triggered when a backup is started during a specific period of time, configure a backup restriction window:
   - Check the Enable Backup Restriction Window box
   - Indicate the Restriction Start and End Time. The format required is HH:MM:SS and the restriction window must at least last 5 minutes.

4. Click Add to list.

5. Click Add.
Blocking the Monitoring of Hosts

During maintenance work on the system, the NetBackup server owner/administrator may need to stop the monitoring of some NetBackup servers. When this situation occurs, the administrator will just have to:

1. Create an empty block file named **NBU_block**
2. Save this file either in:
   - `/var/tmp` (**UNIX/Linux**)
   - `C:\Windows\Temp\` (**Windows**)

The PATROL Agent monitoring this NetBackup server will detect the block file during the next discovery cycle and turn the server instance to NetBackup Setup (Monitoring Blocked).

To resume monitoring, the administrator will just have to delete the **NBU_block** file.
Reference Guide
Introduction

This chapter provides statistical information about resources, operating status, and performances managed by the Veritas NetBackup KM. It contains tables describing the attributes used in the KM, grouped by Monitor Types, and provides a brief description of each attribute and its default settings.

Monitor Types

- NetBackup Client
- NetBackup Daemon
- NetBackup Database
- NetBackup Disk Pool
- NetBackup Disk Storage
- NetBackup Disk Volume
- NetBackup Job
- NetBackup Log
- NetBackup Media Server
- NetBackup Mount Request
- NetBackup Policy
- NetBackup Policy Client
- NetBackup Robotic Drive
- NetBackup Robotic Library
- NetBackup Standalone Drive
- NetBackup Volume Pool
- NetBackup Volume KM

Baselines and Key Performance Indicators

Some attributes are identified by default as Key Performance Indicators (KPIs) and therefore automatically included in the base lining calculation. To learn more about auto baselining and KPIs, please refer to the Managing Baselines and Key Performance Indicators chapter.

In this guide, attributes flagged as KPIs are respectively identified by the following icon: 📈.
# NetBackup Client

## Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Displays the state of the client as reported in the command executed by the data collector.</td>
<td>0 = Running 1 = Connection Refused 2 = Access Denied 3 = Client Down -1 = Unknown</td>
<td>None</td>
<td>Availability</td>
</tr>
</tbody>
</table>
| Status | Monitors the status of the client. The following State to Status mapping rule is used:  
- Access Denied > Failure  
- Client Down > Failure  
- Unknown > Suspicious  
- Connection Failure > Suspicious  
- All other states > OK. | 0 = OK 1 = Suspicious 2 = Failure | Warning = 1 Alarm = 2 | Availability |
## NetBackup Clients

### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec Time</td>
<td>• This is a standard parameter which monitors the collector execution time.</td>
<td>seconds</td>
<td>Warning: &gt; preset value or observed maximum (default)</td>
<td>Collection Status</td>
</tr>
<tr>
<td></td>
<td>• It will run every minute and trigger a warning when the collector runs for more than the observed maximum time. This maximum time can be overridden by a preset value (example: 3600 seconds), using the PSL below:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>%PSL pconfig(&quot;REPLACE&quot;, &quot;/Runtime/NBU/&lt;node-id&gt;/NBUClientCollectorWarn&quot;, 3600);</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## NetBackup Daemon

### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU Duration</td>
<td>Displays the CPU seconds consumed by the daemon.</td>
<td>seconds</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>CPU Utilization</td>
<td>Displays the percentage of CPU used by the daemon.</td>
<td>Percentage (%)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Memory Size</td>
<td>Displays the core image size of the daemon in the virtual memory.</td>
<td>Kilobytes (KB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Process Count</td>
<td>Displays the number of daemon processes/threads found.</td>
<td>processes</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>State</td>
<td>Displays the state of the daemon as reported in the command executed by the data collector.</td>
<td>0 = Running, 1 = Sleeping, 2 = Waiting, 3 = Queued, 4 = Intermediate, 5 = Terminated, 6 = Stopped/Disabled, 7 = Growing, 8 = Nonexistent/Not Responding, 9 = Not Running, -1 = Unknown</td>
<td>None</td>
<td>Availability</td>
</tr>
<tr>
<td>Status</td>
<td>Monitors the status of the daemon. The following State to Status mapping rule is used:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Nonexistent/Not Responding &gt; Failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Not Running &gt; Failure</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Terminated, Stopped, Disabled &gt; Suspicious</td>
<td>0 = OK, 1 = Suspicious, 2 = Failure</td>
<td>Warning = 1, Alarm = 2</td>
<td>Availability</td>
</tr>
</tbody>
</table>
For detailed information about KPI, see Managing Baselines and Key Performance Indicators.

NetBackup Daemons

Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec Time</td>
<td>• This is a standard parameter which monitors the collector execution time.</td>
<td>seconds</td>
<td>Warning: &gt; preset value or observed maximum (default)</td>
<td>Collection Status</td>
</tr>
<tr>
<td></td>
<td>• It will run every minute and trigger a warning when the collector runs for more than the observed maximum time. This maximum time can be overridden by a preset value (example: 3600 seconds), using the PSL below:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>%PSL pconfig(&quot;REPLACE&quot;, &quot;/Runtime/NBU/&lt;node-id&gt;/NBUDaemonCollectorWarn&quot;, 3600);</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## NetBackup Database

### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Filesystem Space Used Percent</td>
<td>Monitors the percentage of space used by the file system where the database resides.</td>
<td>Percentage (%)</td>
<td>Warning between 95 and 98 ( \text{Alarm: } 98 \text{ and over} )</td>
<td>Statistics</td>
</tr>
<tr>
<td>Space Available</td>
<td>Monitors the amount of assigned space remaining available for use by the catalog database.</td>
<td>Megabytes (MB)</td>
<td>Warning: between 2 and 5 ( \text{Alarm when } &lt; 2 )</td>
<td>Availability</td>
</tr>
<tr>
<td>Space Growth Rate</td>
<td>Displays the growth rate of the space used by the catalog database.</td>
<td>Megabytes per second (MB/s)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Space Used Percent</td>
<td>Monitors the percentage of assigned space used by the catalog database.</td>
<td>Percentage (%)</td>
<td>Warning between 95 and 98 ( \text{Alarm: } 98 \text{ and over} )</td>
<td>Statistics</td>
</tr>
<tr>
<td>Space Used</td>
<td>Displays the amount of assigned space used by the catalog database.</td>
<td>Megabytes (MB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

For detailed information about KPI, see Managing Baselines and Key Performance Indicators.
## NetBackup Databases

### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Elapsed 📆</td>
<td>Displays the elapsed time since the last successful database backup.</td>
<td>hours</td>
<td>Alarm: -1  Warning: 24 and over</td>
<td>Statistics</td>
</tr>
<tr>
<td>Database Status</td>
<td>Monitors the status of the NetBackup database (NBDB)</td>
<td>0 = OK 1 = Suspicious 2 = Failure</td>
<td>Warning = 1 Alarm = 2</td>
<td>Availability</td>
</tr>
<tr>
<td>Exec Time</td>
<td>• This is a standard parameter which monitors the collector execution time.</td>
<td>seconds</td>
<td>Warning: &gt; preset value or observed maximum (default)</td>
<td>Collection Status</td>
</tr>
<tr>
<td></td>
<td>• It will run every minute and trigger a warning when the collector runs for more than the observed maximum time. This maximum time can be overridden by a preset value (example: 3600 seconds), using the PSL below:</td>
<td></td>
<td>%PSL pconfig(&quot;REPLACE&quot;, &quot;/Runtime/NBU/&lt;node-id&gt;/NBUDatabaseCollectorWarn&quot;, 3600);</td>
<td></td>
</tr>
</tbody>
</table>

For detailed information about KPI, see Managing Baselines and Key Performance Indicators.
# NetBackup Device

## Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Displays the state of the robotic drive. This is determined from the</td>
<td>0 = Idle</td>
<td>None</td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td>robotic drive control information.</td>
<td>1 = Mounted</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>2 = In Use</td>
<td>3 = Pending</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>4 = Invalid</td>
<td>5 = Down</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>6 = Missing</td>
<td>-1 = Unknown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Monitors the status of the robotic drive. This status is determined by</td>
<td>0 = OK</td>
<td>Warning = 1</td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td>the robotic drive status mapping rule defined in the KM command</td>
<td>1 = Suspicious</td>
<td>Alarm = 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration&gt;Robotic Drive(s) Status.</td>
<td>2 = Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Throughput</td>
<td>Displays the throughput of the robotic drive during the last backup activity.</td>
<td>Megabytes per second (MB/s)</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

For detailed information about **KPI**, see Managing Baselines and Key Performance Indicators.
## NetBackup Devices

### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec Time</td>
<td>- This is a standard parameter which monitors the collector execution time.</td>
<td></td>
<td>Warning &gt; preset value or observed maximum (default)</td>
<td>Collection Status</td>
</tr>
<tr>
<td></td>
<td>- It will run every minute and trigger a warning when the collector runs for more than the observed maximum time. This maximum time can be overridden by a preset value (example: 3600 seconds), using the PSL below:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>%PSSL pconfig(&quot;REPLACE&quot;, &quot;/Runtime/NBU/&lt;node-id&gt;/NBUDriveCollectorWarn&quot;, 3600);</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## NetBackup Disk Pool

### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up Down State</td>
<td>Displays the up/down state of the disk pool.</td>
<td>0 = Down</td>
<td>None</td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-1 = Unknown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up Down Status</td>
<td>Monitors the up/down status of the disk pool.</td>
<td>0 = OK</td>
<td>Warning = 1</td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Suspicious</td>
<td>Alarm = 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 = Failure</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Volume Count</td>
<td>Displays the number of volumes in the disk pool.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

For detailed information on KPIs, see Managing Baselines and Key Performance Indicators.
# NetBackup Disk Volume

## Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Read Stream Count</td>
<td>Displays the number of current read streams for the disk volume.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Space Available</td>
<td>Monitors the available disk volume space for the backup data to use.</td>
<td>Gigabytes (GB)</td>
<td>Warning between 0 and 1 Alarm: between -1 and 0</td>
<td>Availability</td>
</tr>
<tr>
<td>Space Growth Rate</td>
<td>Displays the growth rate of the disk space used by the backup data in this disk volume.</td>
<td>Gigabytes per second (GB/s)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Space Used</td>
<td>Displays the disk space occupied by the backup data in this disk volume.</td>
<td>Gigabytes (GB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Space Used Percent</td>
<td>Monitors the percentage of occupied disk space against the capacity of this disk volume.</td>
<td>Percentage (%)</td>
<td>Warning between 95 and 98 Alarm: 98 and over</td>
<td>Statistics</td>
</tr>
<tr>
<td>Up Down State</td>
<td>Displays the up/down state of the disk volume.</td>
<td>0 = Down 1 = Up -1 = Unknown</td>
<td>None</td>
<td>Availability</td>
</tr>
<tr>
<td>Up Down Status</td>
<td>Monitors the up/down status of the disk volume.</td>
<td>0 = OK 1 = Suspicious 2 = Failure</td>
<td>Warning = 1 Alarm = 2</td>
<td>Availability</td>
</tr>
<tr>
<td>Write Stream Count</td>
<td>Displays the number of current write streams for the disk volume.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

For detailed information, see Managing Baselines and Key.
NetBackup Disk Storage

Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Up Down State</td>
<td>Displays the up/down state of the storage.</td>
<td>0 = Down</td>
<td>None</td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Up</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-1 = Unknown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up Down Status</td>
<td>Monitors the up/down status of the storage.</td>
<td>0 = OK</td>
<td>Warning = 1</td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Suspicious</td>
<td>Alarm = 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 = Failure</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

NetBackup Disk Storages

Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec Time</td>
<td>• This is a standard parameter which monitors the collector execution time.</td>
<td>seconds</td>
<td>Warning &gt; preset value or observed maximum (default)</td>
<td>Collection Status</td>
</tr>
<tr>
<td></td>
<td>• It will run every minute and trigger a warning when the collector runs for more than the observed maximum time. This maximum time can be overridden by a preset value (example: 3600 seconds), using the PSL below:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>%PPL pconfig(&quot;REPLACE&quot;, &quot;/Runtime/NBU/&lt;node-id&gt;/NBUStorageCollectorWarn&quot;, 3600);</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# NetBackup Job

## Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Duration</td>
<td>Displays the duration of the job from the start.</td>
<td>seconds</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>File Count</td>
<td>Displays the number of files backed up for this job.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Size</td>
<td>Displays the amount of data backed up for the job.</td>
<td>Megabytes (MB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>State</td>
<td>Displays the state of the job. This is determined using the job completion state, job exit status code, last job operation, and the erroneous exit status filter.</td>
<td>0 = Completed 1 = Queued 2 = Mounting 3 = In Progress 4 = In Progress/Error 5 = Requeued 6 = Error 7 = Aborted 8 = Suspended 9 = Incomplete 10 = Failed -1 = Unknown</td>
<td>None</td>
<td>Availability</td>
</tr>
</tbody>
</table>
| Status     | Monitors the status of the job. The following State to Status mapping rule is used:  
- Aborted, Suspended, Incomplete, Failed > Failure  
- Errors, Unknown > Suspicious  
- Queued for more than 60 minutes > Suspicious  
- Mounting for more than 60 minutes > Suspicious | 0 = OK 1 = Suspicious 2 = Failure | Warning = 1 Alarm = 2 | Availability |
### Throughput
**Description:** Displays the throughput of this job.

**Units:** Megabytes per second (MB/s)

**Recommended Alert Conditions:** None

**Type:** Statistics

---

### NetBackup Jobs

#### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active Backup Count</td>
<td>Displays the number of active backup jobs currently discovered and monitored.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Active Backup Reduction</td>
<td>Displays the reduction in number of active backup jobs since the last collection cycle.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Active Count</td>
<td>Displays the number of active jobs currently discovered and monitored.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Active Non-Backup Count</td>
<td>Displays the number of active non-backup jobs currently discovered and monitored.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

**Exec Time**
- This is a standard parameter which monitors the collector execution time.
- It will run every minute and trigger a warning when the collector runs for more than the observed maximum time. This maximum time can be overridden by a preset value (example: 3600 seconds), using the PSL below:

**Units:** seconds

**Recommended Alert Conditions:**
- Warning > preset value or observed maximum (default)

**Type:** Collection Status

---

For detailed information about **KPI**, see Managing Baselines and Key Performance Indicators.
<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Queued Backup Count</td>
<td>Displays the number of backup jobs in &quot;Queued&quot; state.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Queued Backup Reduction</td>
<td>Displays the reduction in number of queued backup jobs since the last collection cycle.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

For detailed information about KPI, see Managing Baselines and Key Performance Indicators.
# NetBackup Log

## Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alarm Message Count</td>
<td>Monitors the number of alarm messages.</td>
<td>count</td>
<td>Alarm: more than or equal 1</td>
<td>Statistics</td>
</tr>
<tr>
<td>File Space Growth Rate</td>
<td>Displays the growth rate of the amount of space used by the log file.</td>
<td>Kilobytes per second (KB/s)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>File Space Used</td>
<td>Displays the amount of space used by the log file.</td>
<td>Kilobytes (KB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Filesystem Space Used Percent</td>
<td>Monitors the percentage of space used by the file system (where the log file resides).</td>
<td>Percentage (%)</td>
<td>Warning: between 95 and 98 Alarm: 98 and over</td>
<td>Statistics</td>
</tr>
<tr>
<td>Space Available</td>
<td>Monitors the available space for the log file to use (this is also the available space on the file system).</td>
<td>Megabytes (MB)</td>
<td>Warning: between 2 and 5 Alarm: 2 or less</td>
<td>Availability</td>
</tr>
<tr>
<td>Space Used Percent</td>
<td>Monitors the percentage of capacity used by the log file.</td>
<td>Percentage (%)</td>
<td>Warning: between 95 and 98 Alarm: 98 and over</td>
<td>Statistics</td>
</tr>
<tr>
<td>Warning Message Count</td>
<td>Monitors the number warning messages.</td>
<td>count</td>
<td>Warning: more than or equal to 1</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

For detailed information about XPI, see Managing Baselines and Key Performance Indicators.
# NetBackup Logs

## Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
</table>
| Exec Time | • This is a standard parameter which monitors the collector execution time.  
  • It will run every minute and trigger a warning when the collector runs for more than the observed maximum time. This maximum time can be overridden by a preset value (example: 3600 seconds), using the PSL below:  
  %PSL pconfig("REPLACE", "/Runtime/NBU/<node-id>/NBULogCollectorWarn", 3600); | seconds | Warning > preset value or observed maximum (default) | Collection Status |
NetBackup Media Server

Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>State</td>
<td>Displays the state of the media server as reported in the command executed by the data collector.</td>
<td>Units</td>
<td>Default Alert Conditions</td>
<td>Type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 = Not Reachable By Master; 8 = Not Active For Tape Or Disk Jobs; 12 = Active For Disk Jobs; 13 = Administrative Pause; 14 = Active For Tape And Disk Jobs; -1 = Unknown</td>
<td>None</td>
<td>Availability</td>
</tr>
<tr>
<td>Status</td>
<td>Monitors the status of the media server. The following State to Status mapping rule is used: Not reachable by master &gt; Failure Not active for tape or disk jobs &gt; Failure Administrative pause &gt; Suspicious Unknown &gt; Suspicious All other states &gt; OK</td>
<td>Units</td>
<td>Default Alert Conditions</td>
<td>Type</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 = OK 1 = Suspicious 2 = Failure</td>
<td>Warning = 1 Alarm = 2</td>
<td>Availability</td>
</tr>
</tbody>
</table>

NetBackup Media Servers

Attribute

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Default Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec Time</td>
<td>This is a standard parameter which monitors the collector execution time.</td>
<td>seconds</td>
<td>Warning &gt; preset value or observed maximum (default)</td>
<td>Collection Status</td>
</tr>
</tbody>
</table>
NetBackup Media Servers

TrueSight Operations Management - Veritas NetBackup Monitoring Version 3.1.00

Name | Description | Units | Default Alert Conditions | Type
--- | --- | --- | --- | ---
- | - | - | - | -

- It will run every minute and trigger a warning when the collector runs for more than the observed maximum time. This maximum time can be overridden by a preset value (example: 3600 seconds), using the PSL below:

```
%PSL pconfig("REPLACE", "/Runtime/NBU/<node-id>/NBU_MEDIA_SERVER_COLLECTOR_WARN", 3600);
```

NetBackup Mount Request

Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elapsed</td>
<td>Displays the elapsed time since the mount request was issued.</td>
<td>minutes</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>State</td>
<td>Displays the state of the mount request as reported in the command executed by the data collector.</td>
<td>0 = Completed 1 = Pending -1 = Unknown</td>
<td>None</td>
<td>Availability</td>
</tr>
</tbody>
</table>
| Status | Monitors the status of the mount request. The following State to Status mapping rule is used:
- Pending for more than 30 minutes > Failure
- Pending or Unknown > Suspicious
- All other states > OK | 0 = OK 1 = Suspicious 2 = Failure | Warning = 1 Alarm = 2 | Availability |

For detailed information about KPI, see Managing Baselines and Key Performance Indicators.
## NetBackup Mount Requests

### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
</table>
| Exec Time | - This is a standard parameter which monitors the collector execution time.  
- It will run every minute and trigger a warning when the collector runs for more than the observed maximum time. This maximum time can be overridden by a preset value (example: 3600 seconds), using the PSL below:  
  `%PSL pconfig("REPLACE", "/Runtime/NBU/<node-id>/NBURequestCollectorWarn", 3600);` | seconds | Warning > preset value or observed maximum (default)                                           | Collection Status |
# NetBackup Policy

## Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Elapsed</td>
<td>Displays the elapsed time since the last backup for this policy, regardless of completion status of the backup.</td>
<td>hours</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Backup Throughput</td>
<td>Displays the throughput of the last backup for this policy.</td>
<td>Gigabytes per second (GB/s)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Full Backup Duration</td>
<td>Displays the duration of the last successful full backup for this policy.</td>
<td>seconds</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Full Backup Elapsed</td>
<td>Displays the elapsed time since the last successful full backup for this policy.</td>
<td>hours</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Full Backup File Count</td>
<td>Displays the number of files backed up in the last successful full backup for this policy.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Full Backup Size</td>
<td>Displays the size of the last successful full backup for this policy.</td>
<td>Gigabytes (GB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Incremental Backup Duration</td>
<td>Displays the duration of the last successful incremental backup for this policy.</td>
<td>seconds</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Incremental Backup Elapsed</td>
<td>Displays the elapsed time since the last successful incremental backup for this policy.</td>
<td>hours</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Incremental Backup File Count</td>
<td>Displays the number of files backed up in the last successful incremental backup for this policy.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Incremental Backup Size</td>
<td>Displays the size of the last successful incremental backup for this policy.</td>
<td>Gigabytes (GB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Units</td>
<td>Recommended Alert Conditions</td>
<td>Type</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>--------------</td>
<td>------------------------------</td>
<td>------------</td>
</tr>
<tr>
<td>State</td>
<td>Displays the state of the policy.</td>
<td></td>
<td>None</td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td></td>
<td>0 = Idle</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>1 = Running</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>2 = Running in Restricted Window</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>3 = Not started</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>4 = Inactive</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>-1 = Unknown</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Monitors the status of the policy. The following State to Status mapping rule is used:</td>
<td></td>
<td>Warning = 1</td>
<td>Availability</td>
</tr>
<tr>
<td></td>
<td>• Running in Restricted Window &gt; Failure</td>
<td></td>
<td>Alarm = 2</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Running for more than 600 minutes &gt; Suspicious</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Unknown &gt; Suspicious</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• All other states &gt; OK.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Successful Backup Elapsed 📘</td>
<td>Displays the elapsed time since the last successful backup for this policy.</td>
<td>hours</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

For detailed information about 📘 KPI, see Managing Baselines and Key Performance Indicators.
# NetBackup Policies

## Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec Time</td>
<td>This is a standard parameter which monitors the collector execution time.</td>
<td>seconds</td>
<td>Warning &gt; preset value or observed maximum (default)</td>
<td>Collection Status</td>
</tr>
<tr>
<td></td>
<td>It will run every minute and trigger a warning when the collector runs for more than the observed maximum time. This maximum time can be overridden by a preset value (example: 3600 seconds), using the PSL below:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>%PSL pconfig(&quot;REPLACE&quot;, &quot;/Runtime/NBU/&lt;node-id&gt;/NBUPolicyCollectorWarn&quot;, 3600);</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## NetBackup Policy Client

### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Backup Throughput</td>
<td>Displays the throughput of the last backup for this policy client.</td>
<td>Megabytes per second (MB/s)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Last Full Backup Duration</td>
<td>Displays the duration of the last successful full backup for this policy client.</td>
<td>seconds</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Last Full Backup File Count</td>
<td>Displays the number of files backed up in the last successful full backup for this policy client.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Last Full Backup Size</td>
<td>Displays the size of the last successful full backup for this policy client.</td>
<td>Megabytes (MB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Last Incremental Backup Duration</td>
<td>Displays the duration of the last successful incremental backup for this policy client.</td>
<td>seconds</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Last Incremental Backup File Count</td>
<td>Displays the number of files backed up in the last successful incremental backup for this policy client.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Last Incremental Backup Size</td>
<td>Displays the size of the last successful full backup for this policy client.</td>
<td>Megabytes (MB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

For detailed information about KPI, see Managing Baselines and Key Performance Indicators.
## NetBackup Robotic Drive

### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Drive Throughput</td>
<td>Displays the throughput of the robotic drive during the last backup activity.</td>
<td>Megabytes per second (MB/s)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>State</td>
<td>Displays the state of the robotic drive. This is determined from the robotic drive control information.</td>
<td>0 = Idle 1 = Mounted 2 = In Use 3 = Pending 4 = Down -1 = Unknown</td>
<td>None</td>
<td>Availability</td>
</tr>
</tbody>
</table>
| Status           | Monitors the status of the robotic drive. The following State to Status mapping rule is used:  
- Down > Failure  
- Pending for more than 5 minutes > Failure  
- In Use for more than 600 minutes > Suspicious  
- Unknown > Suspicious  
- All other states > OK  
0 = OK 1 = Suspicious 2 = Failure | Warning = 1 Alarm = 2 | Availability |

For detailed information about KPI, see Managing Baselines and Key Performance Indicators.
## NetBackup Robotic Library

### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Assigned Count</td>
<td>Displays the number of assigned media loaded in this robotic library.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td></td>
<td>Assigned media are tape media assigned to a non-scratch volume pool.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Available Count</td>
<td>Displays the number of media available to use in this robotic library. This includes unassigned and scratch media.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Available Percent</td>
<td>Monitors the percentage of available media against the total number of media loaded in this robotic library.</td>
<td>Percentage (%)</td>
<td>Warning: between 2 and 5 Alarm: 2 or less</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Cleaning Left</td>
<td>Monitors the number of cleaning left on the cleaning media available in this robotic library.</td>
<td>count</td>
<td>Warning: 2 or less Alarm: 0</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Count</td>
<td>Displays the total number of media loaded in this robotic library.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Scratch Count</td>
<td>Displays the number of scratch media loaded in this robotic library. (Scratch media are tape media assigned to the scratch volume pool.)</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Scratch Percent</td>
<td>Monitors the percentage of scratch media against the total number of media loaded in this robotic library.</td>
<td>Percentage (%)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Unassigned Count</td>
<td>Displays the number of unassigned media loaded in this robotic library. (Unassigned media are tape media not assigned to a volume pool.)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Media Unassigned Percent</td>
<td>Monitors the percentage of unassigned media against the total number of media loaded in this robotic library.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>State</td>
<td>Displays whether the inquiry for the robotic library is valid or invalid. It will not perform any remote robotic library test command on the media server.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Status</td>
<td>Monitors the status of the robotic library.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Throughput</td>
<td>Displays the total throughput of each robotic library drive during the last backup activities within the last hour.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Up Drive Count</td>
<td>Displays the number of up / online state drives in this robotic library.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Units: count
Recommended Alert Conditions: None
Type: Statistics

States: 0 = Online, 1 = Remote, 2 = Offline, 3 = Invalid, -1 = Unknown

For detailed information about KPIs, see Managing Baselines and Key Performance Indicators.
# NetBackup Robotic Libraries

## Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec Time</td>
<td>This is a standard parameter which monitors the collector execution time. It will run every minute and trigger a warning when the collector runs for more than the observed maximum time. This maximum time can be overridden by a preset value (example: 3600 seconds), using the PSL below: %PSL pconfig(&quot;REPLACE&quot;, &quot;/Runtime/NBU/&lt;node-id&gt;/NBU/LibraryCollectorWarn&quot;, 3600);</td>
<td>seconds</td>
<td>Warning &gt; preset value or observed maximum (default)</td>
<td>Collection Status</td>
</tr>
</tbody>
</table>
# NetBackup Standalone Drive

## Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
</table>
| State      | Displays the state of the standalone drive. This is determined from the standalone drive control information. | 0 = Idle  
1 = Mounted  
2 = In Use  
3 = Pending  
4 = Down  
-1 = Unknown | None                         | Availability                           |
| Status     | Monitors the status of the standalone drive.                                 | 0 = OK  
1 = Suspicious  
2 = Failure | Warning = 1  
Alarm = 2         | Availability                           |
| Throughput | Displays the throughput of the standalone drive during the last backup activity. | Megabytes per second (MB/s) | None                         | Statistics  |

For detailed information about KPI, see Managing Baselines and Key Performance Indicators.
# NetBackup Standalone Drives

## Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec Time</td>
<td>• This is a standard parameter which monitors the collector execution time.</td>
<td>seconds</td>
<td>Warning &gt; preset value or observed maximum (default)</td>
<td>Collection Status</td>
</tr>
<tr>
<td></td>
<td>• It will run every minute and trigger a warning when the collector runs for more than the observed maximum time. This maximum time can be overridden by a preset value (example: 3600 seconds), using the PSL below:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>%PSL pconfig(&quot;REPLACE&quot;, &quot;/Runtime/NBU/&lt;node-id&gt;/NBUCollectorWarn&quot;, 3600);</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
# NetBackup Volume Pool

## Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Media Active Count</td>
<td>Displays the number of active media in this volume pool. (Active media are available tape media with a status of Active, where data has been written but the media is not yet full.)</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Active Percent</td>
<td>Monitors the percentage of active media against the total number of media in this volume pool.</td>
<td>Percentage (%)</td>
<td>Warning between 2 and 5 Alarm when &lt; 2</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Count</td>
<td>Displays the total number of media in this volume pool.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Frozen Count</td>
<td>Displays the number of frozen media in this volume pool. Frozen is a possible status for a tape media.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Full Count</td>
<td>Displays the number of full media in this volume pool. Full is a possible status for a tape media.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Full Percent</td>
<td>Monitors the percentage of full media against the total number of media in this volume pool.</td>
<td>Percentage (%)</td>
<td>Warning: between 95 and 98 Alarm: 98 and over</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Loaded Count</td>
<td>Displays the number of media in this volume pool, currently loaded to a robotic library.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Loaded Empty Count</td>
<td>Displays the number of empty media in this volume pool, currently loaded to a robotic library.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Units</td>
<td>Recommended Alert Conditions</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>---------</td>
<td>------------------------------</td>
<td>----------</td>
</tr>
<tr>
<td>Media Loaded Empty Percent</td>
<td>Monitors the percentage of empty media against the total number of empty media in this volume pool.</td>
<td>Percentage (%)</td>
<td>Warning:2-5 Alarm:0-2</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media ReadOnly Count</td>
<td>Displays the number of media in this volume pool, currently read-only. A media turns read-only when it has reached the maximum allowed mounts.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Scratch Count</td>
<td>Displays the number of scratch media in this volume pool. The parameter is visible and set only for scratch volume pools.</td>
<td>count</td>
<td>Warning when &lt; 2 Alarm = 0</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Suspended Count</td>
<td>Displays the number of suspended media in this volume pool. Suspended is a possible status for a tape media.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Unassigned Count</td>
<td>Displays the number of media in unassigned state in this volume pool.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Unassigned Percent</td>
<td>Monitors the percentage of unassigned media against the total number of media in this volume pool. If this parameter changes to warning or alarm state, the recovery action will trigger an event.</td>
<td>Percentage (%)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Media Unknown Count</td>
<td>Displays the number of media in unknown state in this volume pool.</td>
<td>count</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Space Available</td>
<td>Monitors the available media space for the backup data to use amongst the assigned media in this volume pool.</td>
<td>Gigabytes (GB)</td>
<td>None</td>
<td>Availability</td>
</tr>
<tr>
<td>Name</td>
<td>Description</td>
<td>Units</td>
<td>Recommended Alert Conditions</td>
<td>Type</td>
</tr>
<tr>
<td>-----------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>------------------------------</td>
<td>--------</td>
</tr>
<tr>
<td>Space Growth Rate</td>
<td>Displays the growth rate of the total media space used by the backup data in this volume pool.</td>
<td>Gigabytes per second (GB/s)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Space Used</td>
<td>Displays the total media space occupied by the backup data in this volume pool.</td>
<td>Gigabytes (GB)</td>
<td>None</td>
<td>Statistics</td>
</tr>
<tr>
<td>Space Used Percent</td>
<td>Monitors the percentage of total occupied media space against the total media capacity of this volume pool (not including any scratch media).</td>
<td>Percentage (%)</td>
<td>Warning: between 95 and 98 Alarm: 98 and over</td>
<td>Statistics</td>
</tr>
</tbody>
</table>

For detailed information about KPI, see Managing Baselines and Key Performance Indicators.
## NetBackup Volume Pools

### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exec Time</td>
<td>• This is a standard parameter which monitors the collector execution time.</td>
<td>seconds</td>
<td>Warning &gt; preset value or observed maximum (default)</td>
<td>Collection Status</td>
</tr>
<tr>
<td></td>
<td>• It will run every minute and trigger a warning when the collector runs for more than the observed maximum time. This maximum time can be overridden by a preset value (example: 3600 seconds), using the PSL below:</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>%PSL pconfig(&quot;REPLACE&quot;, &quot;/Runtime/NBU/&lt;node-id&gt;/NBUPoolCollectorWarn&quot;, 3600);</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## Veritas NetBackup KM

### Attributes

<table>
<thead>
<tr>
<th>Name</th>
<th>Description</th>
<th>Units</th>
<th>Recommended Alert Conditions</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Login Status</td>
<td>Monitors the status of the NetBackup KM login details (username/password) for the operating system. If no valid username/password is detected for the operating system, this parameter will be set to Failure state. If there are any suspicious command exits, this parameter will be set to Suspicious state.</td>
<td>0 = OK 1 = Suspicious 2 = Failure</td>
<td>Warning = 1 Alarm = 2</td>
<td>Collection Status</td>
</tr>
<tr>
<td>Monitoring Mode</td>
<td>Monitors failover mode of the NetBackup KM. By default NetBackup KM runs in Permanent Single-node Mode. Refer to Configuring the Multi-Node Monitoring Mode for more details.</td>
<td>0 = Permanent Single-node Mode 1 = Temporary Single-node Mode 2 = Active Multi-node Mode 3 = Passive Multi-node Mode -1 = Unknown</td>
<td>None</td>
<td>Collection Status</td>
</tr>
</tbody>
</table>

83

NetBackup Volume Pools
### Managing Baselines and Key Performance Indicators

To detect abnormalities on the monitored environment, BMC TrueSight Operations Management calculates baselines per attribute based on values collected over a specified period of time to determine a normal operating range. When the collected values for these parameters are out of range, an alert is triggered. Some attributes are identified by default as Key Performance Indicators (identified with the ⚙️ icon) and automatically included in the base lining calculation.

**Managing baselines**

The baseline is the expected normal operating range for an attribute of a monitor. There are two baselines: **Baseline High** and **Baseline Low**. **Baseline High** represents the point at which 95% of the weighted average of the historical values fall below this value for the selected time period; **Baseline Low** represents the point at which 90% of the weighted average of historical values for the selected time period fall above this line.

Baselines are generated for KPI attributes that have an active abnormality thresholds.

**Managing Key Performance Indicators**

Starting from v9.5 of BPPM, attributes that have not been initially designated in the KM as Key Performance Indicators (KPIs) cannot be flagged as KPIs from BPPM/TrueSight. Although enabling
baseline is possible through the **Options > Administration > Intelligent Event Thresholds** feature available in the Infrastructure Management Server operator console, **BMC does not** recommend doing it.

⚠️ For more information, refer to the BMC TrueSight Operations Management documentation available from [docs.bmc.com](http://docs.bmc.com).
Index

- A -

Abnormalities 84
Access
  Executable Files 11
  Files 11
  Library Files 11
  Paths 11
  Permissions 11
AIX 11
Application Class
  NBU_SERVER 83
Attributes
  Active Backup Count 62
  Active Backup Reduction 62
  Active Count 62
  Active Non-Backup Count 62
  Alarm Message Count 64
  Backup Elapsed 55, 69
  Backup Throughput 69, 72
  CPU Duration 52
  CPU Utilization 52
  Database Status 55
  Drive Throughput 73
  Duration 61
  Elapsed 67
  Exec Time 51, 53, 55, 57, 60, 62, 65, 66, 68, 71, 76, 78, 82
  File Count 61
  File Space Growth Rate 64
  File Space Used 64
  File System Space Used Percent 54
  Filesystem Space Used Percent 64
  Full Backup Duration 69
  Full Backup Elapsed 69
  Full Backup File Count 69
  Full Backup Size 69
  Incremental Backup Duration 69
  Incremental Backup Elapsed 69
  Incremental Backup File Count 69
  Incremental Backup Size 69
  Last Full Backup Duration 72
  Last Full Backup File Count 72
  Last Incremental Backup Duration 72
  Last Incremental Backup File Count 72
  Last Incremental Backup Size 72
  Media Active Count 79
  Media Active Percent 79
  Media Assigned Count 74
  Media Available Count 74
  Media Available Percent 74
  Media Cleaning Left 74
  Media Count 74, 79
  Media Frozen Count 79
  Media Full Count 79
  Media Full Percent 79
  Media Loaded Count 79
  Media Loaded Empty Count 79
  Media Loaded Empty Percent 79
  Media Read Only Count 79
  Media Scratch Count 74, 79
  Media Scratch Percent 74
  Media Suspended Count 79
  Media Unassigned Count 74, 79
  Media Unassigned Percent 74, 79
  Media Unknown Count 79
  Memory Size 52
  Process Count 52
  Queued Backup Count 62
  Queued Backup Reduction 62
  Read Stream Count 59
  Size 61
  Space Available 54, 59, 64, 79
  Space Growth Rate 54, 59, 79
  Space Used 54, 59, 79
  Space Used Percent 54, 59, 64, 79
  State 50, 52, 56, 61, 66, 67, 69, 73, 74, 77
  Status 50, 52, 56, 61, 66, 67, 69, 73, 74, 77
  Successful Backup Elapsed 69
  Summary 56
  Throughput 56, 61, 74, 77
  Up Down State 58, 59, 60
  Up Down Status 58, 59, 60
  Up Drive Count 74
  Volume Count 58
  Warning Message Count 64
  Write Stream Count 59
- **B** -

Backup
- Restriction 46
- Baseline 49
- Baselines
  - BMC ProactiveNet Performance Management 84
  - Generation 84
  - Manage 84
  - Requirements 84
- Block
  - Monitoring 47
  - BMC ProactiveNet Performance Management
    - Abnormalities 84
    - Baselines 84
    - Key Performance Indicators 84
    - KPI 84
- Business Value 9

- **C** -

Client
- Maximum Instances 31
- Clients
  - Debug 37
- Cluster Application 34
- Component Installation package
  - creating 21
  - downloading 22
- Configure
  - Date format 44
  - Hostname 41
  - Jobs 41
  - Log Scan Limit 43
  - Maximum Instances 31
  - Monitor Type 24
  - Monitoring Duration 41
  - Mount Request 44
  - Multi-node monitoring mode 34
  - Overrides 28
  - Time format 44

- **D** -

Daemon
- Maximum Instances 31
- Daemons
  - Debug 37
- Database
  - Maximum Instances 31
- Databases
  - Debug 37
- Date
  - Configure 44
  - Format 44
- Debug
  - Clients 37
  - Daemons 37
  - Databases 37
  - Debug 37
  - Directory Path 37
  - Disk Storages 37
  - Enable 37
  - End 37
  - Jobs 37
  - Logs 37
  - Mount Requests 37
  - Policies 37
  - Pools 37
  - Robotic Libraries/Drives 37
  - Server 37
  - Volume Pools 37
  - Volumes 37
- Disk Pool
  - Maximum Instances 31
- Disk Storage
  - Maximum Instances 31
- Disk Storages
  - Debug 37
- Disk Volume
  - Maximum Instances 31
- Downloading 22
- Duration
  - Duration 44
  - Monitoring 44

- **E** -

Enable
- Backup Restriction 46
- Erroneous Exit Status 41
- F -

Failover Group Name 34
Features 9
Filtering Options
  NetBackup Client 40
  NetBackup Daemon 40
  NetBackup Disk Pool 40
  NetBackup Disk Storage 40
  NetBackup Disk Volume 40
  NetBackup Media Server 40
  NetBackup Policy 40
  NetBackup Policy Client 40
  NetBackup Robotic Drive 40
  NetBackup Robotic Library 40
  NetBackup Standalone Drive 40
  NetBackup Volume Pools 40

Filters
  NetBackup Client 40
  NetBackup Daemon 40
  NetBackup Disk Pool 40
  NetBackup Disk Storage 40
  NetBackup Disk Volume 40
  NetBackup Media Server 40
  NetBackup Policy 40
  NetBackup Policy Client 40
  NetBackup Robotic Drive 40
  NetBackup Robotic Library 40
  NetBackup Standalone Drive 40
  NetBackup Volume Pools 40

- G -

Generate
  Baselines 84
Goals 9

- H -

HP-UX 11

- I -

Importing the Monitoring Solution 20
InfoBox
  Application Name 83

- J -

Job
  Maximum Instances 31
Jobs
  Active 41
  Configure 41

Application Version 83
Binary Path 83
Copyright 83
Host Name 83
Installation Path 83
Library Path 83
Master Server(s) 83
Media Server(s) 83
Monitoring Mode 83
Monitoring Node 83
Node Name(s) 83
Node Type 83
Operating System 83
PATROL Agent Version 83
Platform 83
Product Name 83
Product Release Date 83
Product Version 83
Support 83
Web Site 83

Installing 22
Installing the Monitoring Solution 19
Instances
  Client 31
  Configure 31
  Daemon 31
  Database 31
  Disk Pool 31
  Disk Storage 31
  Disk Volume 31
  Job 31
  Log 31
  Maximum 31
  Mount Request 31
  Policy 31
  Policy Client 31
  Robotic Drive 31
  Robotic Library 31
  Standalone Drive 31
  Volume Pool 31
Jobs
  Debug 37
  Monitoring 41

- K -

Key Concepts 9
Key Performance Indicators 49
  BMC ProactiveNet Performance Management 84
  Manage 84
KPI 49
  BMC ProactiveNet Performance Management 84
  Manage 84

- L -

Linux 11
Log
  Maximum Instances 31
Log Scan Limit
    Configure 43
Logs
  Debug 37

- M -

Maintenance 47
Manage
  Baselines 84
  Key Performance Indicators 84
  KPI 84
Menu Commands
  About 83
  Administration 83
  Debug 83
  Force Discovery 83
  Instance Limits 83
  KM Status 83
  Login 83
  Monitoring Mode 83
  Node Status 83
  Node Type 83
  Paths 83
  Preloading 83
  Refresh Parameters 83
  Refresh Process Cache 83
  Reload Commands 83
  Start Master Server 83
  Start Media Server 83
  Stop Master Server 83
  Stop Media Server 83
Monitor Types
  Configure 24
  NetBackup Client 24, 49, 50
  NetBackup Clients 51
  NetBackup Daemon 24, 49, 52
  NetBackup Database 49, 54
  NetBackup Databases 55
  NetBackup Deamons 53
  NetBackup Device 56
  NetBackup Devices 57
  NetBackup Disk Pool 24, 49, 58
  NetBackup Disk Storage 24, 49, 60
  NetBackup Disk Volume 24, 49, 59
  NetBackup Job 24, 49, 61
  NetBackup Jobs 62
  NetBackup Libraries 76
  NetBackup Log 49, 64
  NetBackup Logs 65
  NetBackup Media Server 66
  NetBackup Media Servers 66
  NetBackup Mount Request 24, 49, 67
  NetBackup Mount Requests 68
  NetBackup Policies 71
  NetBackup Policy 24, 49, 69
  NetBackup Policy Client 24, 49, 72
  NetBackup Robotic Drive 24, 49, 73
  NetBackup Robotic Library 24, 49, 74
  NetBackup Standalone Drive 24, 49, 77
  NetBackup Standalone Drives 78
  NetBackup Storages 60
  NetBackup Volume Pool 24, 49, 79
  NetBackup Volume Pools 82
  Symantec NetBackup KM 24, 49
  Veritas NetBackup KM 26
Monitoring
  Block 47
  Blocked 47
  Configure 44
  Duration 44
  Stop 47
  Stopped 47
Monitoring Duration
  Jobs 41
  Monitoring Node Names 34
Mount Request
  Configure 44
  Maximum Instances 31
  Monitoring Duration 44
Mount Requests
  Debug 37
  Multi-node monitoring mode
    Configure 34

- N -

NBU_SERVER
  Application Class 83
NetBackup
  Policies 46
NetBackup Policies
    Configure 46
NetBackup Server Discovery
  Overrides 28

- O -

Overrides
  Configure 28
  NetBackup Server Discovery 28

- P -

Package 21, 22
Parameters
  ExtraFilesList 83
  NBUClientCollector 83
  NBUCreateDistribution 83
  NBUDaemonCollector 83
  NBUDatabaseCollector 83
  NBUDriveCollector 83
  NBUJobCollector 83
  NBULibraryCollector 83
  NBULogCollector 83
  NBULogInStatus 83
  NBUMonitoringMode 83
  NBUNodeStatus 83
  NBUPolicyCollector 83
  NBUPoolCollector 83
  NBURemoveTempFiles 83
  NBURequestCollector 83
  NBUStorageCollector 83
  NBUUpdateAgent 83
Path
  Debug 37
Permissions
  Access 11
Platforms
  Supported 10
  Symantec NetBackup 10
Policies
  Configure 46
  Debug 37
  NetBackup 46
Policy
  Maximum Instances 31
Policy Client
  Maximum Instances 31
Pools
  Debug 37

- R -

Reference Guide 49
Remote PATROL Agent Checking 34
Requirements 10
  Security 11
  System 10
Restriction
  Backup 46
  End Time 46
  Start Time 46
  Window 46
Robotic Drive
  Maximum Instances 31
Robotic Libraries/Drives
  Debug 37
Robotic Library
  Maximum Instances 31

- S -

Security
  Requirements 11
Server
  Debug 37
Solaris 11
Standalone Drive
  Maximum Instances 31
Sudo 26
- T -
Time
Configure 44
Format 44

- U -
UNIX 26
User Account
Configure 26
patrol 26
Privileges 26
Sudo 26

- V -
Veritas NetBackup KM
Configure 26
Monitor Type 26
Volume Pool
Maximum Instances 31
Volume Pools
Debug 37
Volumes
Debug 37

- W -
Windows 26
About Sentry Software™
Sentry Software, a strategic Technology Alliance Partner of BMC Software, provides comprehensive multi-platform monitoring solutions that enable management of the hardware and software aspects of all servers and SANs and covering up to 100% of custom applications within the BMC TrueSight environment. Sentry Software also develops adapters for BMC Atrium Orchestrator that enables IT administrators to automate the execution of common requests and tasks that occur in the daily course of IT operations. Combined with BMC’s servers and network automation tools, the adapters allow IT administrators to implement provisioning and decommissioning workflows that cover all layers of their IT infrastructure. Finally, Sentry Software designs connectors that bring storage capacity metrics into BMC TrueSight Capacity Optimization to ensure IT administrators that their storage infrastructure is properly sized for their current and future needs.

About BMC Software™
BMC Software helps leading companies around the world put technology at the forefront of business transformation, improving the delivery and consumption of digital services. From mainframe to cloud to mobile, BMC delivers innovative IT management solutions that have enabled more than 20,000 customers to leverage complex technology into extraordinary business performance—increasing their agility and exceeding anything they previously thought possible. For more information about BMC Software, visit www.bmc.com.