SENTRY SOFTWARE

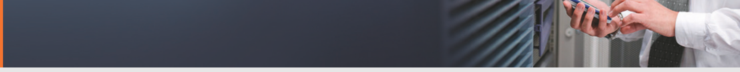
USER DOCUMENTATION

STORAGE MONITORING

TrueSight Operations Management - Veritas NetBackup Monitoring

Version 3.2.00

February 2018



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				
Address	BMC Software, Inc. 2101 CityWest Blvd. Houston TX 77042-2827		**Telephone**	1 (713) 918 8800 or 1 (800) 841 2031 (Toll Free)

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 UNPUBLISHED -- RIGHTS RESERVED UNDER THE COPYRIGHT LAWS OF THE UNITED STATES.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.

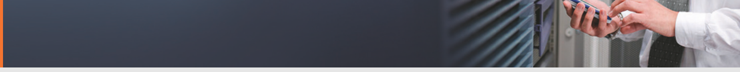


Table of Contents

Release Notes for v3.2.00

Important Information

The BMC patch 11.0.00.01: Patch 1 for BMC PATROL Agent 11.0.00 **must be installed** to use any version of TrueSight Operations Management - Veritas NetBackup Monitoring. Version 11.0.00i of the PATROL Agent on Windows prevents Veritas NetBackup KM from operating properly. While apparently successfully loaded, Veritas NetBackup KM fails to start and can neither monitor the local system or the remote systems. An error message is displayed stating that no hardware connectors are loaded and that the product needs to be re-installed.

What's New

- **NBU-608:** The multi-node mode failover supports the new remote monitoring architecture.
- **NBU-798**: Full support for Veritas NetBackup version 8 and higher.
- **NBU-809:** The monitoring of any additional log file can now be configured in TrueSight. The log filter can also be customized to indicate when Warnings and Alarms are triggered.

Changes and Improvements

- **NBU-791**: The Veritas NetBackup KM now properly takes user-configured log scan limit into account.
- **NBU-797**: The overall performance of Veritas NetBackup KM has been significantly improved.
- **NBU-799**: The monitoring of remote servers can be blocked from the remote node, to avoid unnecessary alerts and notifications.

Fixed Issues

- **NBU-806**: The Exit status of each command run by the KM on a remote Windows system is now properly verified and reported.
- **NBU-839**: The command used for monitoring NetBackup media servers has been modified to report only the relevant master and media servers and prevent false alarms.
- **NBU-879:** The Debug mode is now properly activated/deactivated according to the user's settings for all the monitored components.
- **NBU-840**: Enabling the Debug mode for Media Servers would also activate the debug for Servers.

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:

- System Requirements
- Software Requirements
- Security Requirements
- Remote Monitoring Requirements

System Requirements

The Veritas NetBackup KM supports the following operating systems:

Operating System	Version
Oracle Solaris™	8 and higher
HP-UX	11 and higher
IBM® AIX™	5.1 and higher
Linux®	All distributions
Microsoft® Windows®	2008 and higher

Software Requirements

Veritas NetBackup KM supports the following platforms:

Platforms	Version
Veritas NetBackup	5 and higher
PATROL Agent	Any version
BMC ProactiveNet Performance Manager	9.5 and higher
BMC TrueSight Operations Management	10 and higher

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:

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

⚠ **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

Unix	Microsoft Windows
INSTALL_PATH/netbackup	INSTALL_PATH\NetBackup
INSTALL_PATH/netbackup/bin	INSTALL_PATH\NetBackup\bin
INSTALL_PATH/netbackup/bin/admincmd	INSTALL_PATH\NetBackup\bin\admincmd
INSTALL_PATH/netbackup/bin/goodies	INSTALL_PATH\NetBackup\bin\goodies
INSTALL_PATH/volmgr/bin	INSTALL_PATH\Volmgr\bin
INSTALL_PATH/volmgr/bin/goodies	INSTALL_PATH\Volmgr\bin\goodie
INSTALL_PATH/lib	C:\Program Files\Common Files\VERITAS Shared
/usr/openwin/lib	INSTALL_PATH\NetBackup\lib

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)
vxdctl (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\nCommands used with sudo:\n%s",sort(sudoers)); }
    printf("\n\nOn %s:\n\n", 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(ntharg(scmd,1,">|"),"1-"," "," "));
  }
  printf("(%2d) %-30s %-40s: %s\n",i++,ntharg(var,fields,"/"),met,cmd);
  }
}

if((osp!="WINDOWS") && sudoers) { printf("\n\nCommands used with sudo:\n%s",sort(sudoers)); }
```

Paths and Files Accessed by PATROL Agent User

Unix	Microsoft Windows
INSTALL_PATH/netbackup/db	INSTALL_PATH\NetBackup\db
INSTALL_PATH/volmgr/database	INSTALL_PATH\Volmgr\database
INSTALL_PATH/var	INSTALL_PATH\NetBackup\var
INSTALL_PATH/netbackup/db/error/ daily_messages.log	INSTALL_PATH\NetBackup\db\error\log_date
/var/adm/messages (on Solaris)	
/var/adm/syslog/syslog.log (on HP-UX)	
/var/log/messages (on Linux)	

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,\
env_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.

Replace *PATROL_HOME*/lib/NBU/* with the **Remote Temp Directory Path**, default /var/tmp/*, when monitoring remotely.

On HP-UX

```
User_Alias NBUKMUSERS = user1, user2, user3
Defaults:NBUKMUSERS !lecture,!authenticate,!requiretty,\
env_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.

Replace *PATROL_HOME*/lib/NBU/* with the **Remote Temp Directory Path**, default /var/tmp/*, when monitoring remotely.

On AIX & Linux

```
User_Alias NBUKMUSERS = user1, user2, user3
Defaults:NBUKMUSERS !lecture,!authenticate,!requiretty,\
env_keep+="PATH LIBPATH 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.

Replace *PATROL_HOME*/lib/NBU/* with the **Remote Temp Directory Path**, default /var/tmp/*, when monitoring remotely.

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.

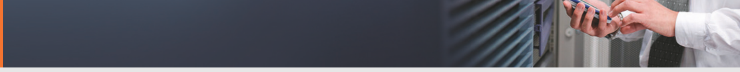
The requirements listed below must be met to be able to use remote monitoring.

JAVA

Veritas NetBackup KM requires Java 1.8 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.
5. From **TrueSight Operations Management**, click **Import** .
6. Select **Single solution**.
7. Browse to the .zip source file.
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

Once Veritas NetBackup KM is installed, you will have to configure the Veritas NetBackup KM Monitor Types through policies. Policies enable you to deploy configurations on PATROL Agents and monitoring solutions, such as Veritas NetBackup KM in an automated way. Policies are designed to define and configure monitoring criteria and apply them to the specified PATROL Agents. The configuration criteria are automatically pushed to the PATROL Agents on which the policy is applied. When a monitoring policy is applied to a PATROL Agent, the device is automatically added to the list of monitored devices.

To create a monitoring policy

1. Log on to the TrueSight console.
2. In the navigation pane, expand **Configuration** and select **Infrastructure Policies**.
3. In the **Infrastructure Policies** page, ensure that the **Monitoring** tab is selected and click **Create Policy**.
4. In the **Create Monitoring Policy** page, specify the monitoring policy properties:

Step 1 - Define the General Properties

Property	Description
Name	Name for the policy. The policy names must be unique. In an environment with tenants, the policy names must be unique for a single tenant. It is a mandatory field.
Description	(Optional) A brief description about the policy.
Associated User Group	Name of the user group that is associated with the PATROL Agents as defined in the Authorization Profile or in the PATROL Agent ACLs. The policy is applicable to these PATROL Agents.
Share with User Group	Specify whether this policy is to be shared with the users across the associated user group or not. This property can be viewed in READ-ONLY mode by other users of the associated user group. Only the owner of the policy can modify this property.
Precedence	Priority of the policy. Based on the precedence number that you configure, the configuration is applied to the PATROL Agents and the Infrastructure Management servers. The precedence number ranges from 0 to 999. A lower number indicates a higher precedence. The default value is 900. The configuration from a policy with a higher precedence overrides the configuration from a policy with a lower precedence. If two policies have the same precedence number, then the configuration from the latest created policy takes priority.
Enable Policy	Indicates whether the policy is enabled or disabled. By default, the policy is disabled. If you do not enable a policy when you create it, the policy configurations are not applied to the PATROL Agents and the Infrastructure Management Servers. If you disable any existing policy, the policy configurations are removed from the PATROL Agents and the Infrastructure Management servers, where the policy was applied.

Step 2 - Select the PATROL Agents

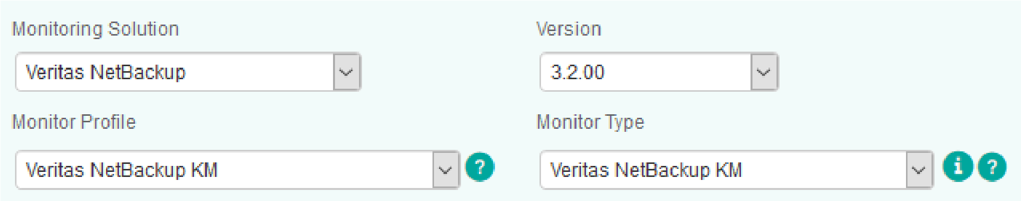
Define conditions to select the PATROL Agents on which you want to apply the policy:

1. Select a property.
2. Select an operator to create the condition. The available operators depend on the property that you select.
3. Specify a value for the selected property.
4. (Optional) To add more than one condition, click the ⊕ button, and perform the earlier steps.
5. (Optional) To group the conditions, use the parentheses and Boolean operators from their corresponding lists.

The **Add Monitor Types** dialog box presents configuration fields for compatible BMC PATROL monitoring solutions that are located in the Central Monitoring Repository.

Step 3 - Select the Required Monitor Type

1. Click the **Monitoring** tab.
2. Click **Add Monitoring Configuration**.
3. In the **Add Monitoring Configuration** dialog box, configure the properties:
   - From the **Monitoring Solution** menu, select **Veritas NetBackup KM**.
   - From the **Version** menu, select the required version.
   - The **Monitor Profile Veritas NetBackup KM** is automatically selected.



Monitoring Solution: Veritas NetBackup

Version: 3.2.00

Monitor Profile: Veritas NetBackup KM

Monitor Type: Veritas NetBackup KM

Selecting the Required Monitor Type

   - Refer to the table below to know which monitor types are available and their function

Monitor Type	Description
Veritas NetBackup KM **(REQUIRED)**	To set the general settings of the Veritas NetBackup monitoring solution (credentials, debug mode, instances, multi-node mode, etc.). ⚠ **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.**
NetBackup Client	To modify the client default monitoring.
NetBackup Daemon	To modify the daemons monitoring.
NetBackup Disk Pool	To modify the disk pools default monitoring.
NetBackup Disk Storage	To modify the disk storage default monitoring.
NetBackup Disk Volume	To modify the disks volume default monitoring.

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

Step 4 - Configure the Selected Monitor Type

1. Depending on the selected Monitor Type, the available fields will vary. Refer to appropriate section to know how to configure them.
2. Click **Save** to apply your changes to the selected PATROL Agent(s).

To edit a monitoring policy

1. Log on to the TrueSight console.
2. In the navigation pane, expand **Configuration** and select **Infrastructure Policies**.
3. In the **Infrastructure Policies** page, locate the monitoring policy you wish to modify, click its action button ⋮ and click **Edit**.
4. In the **Edit Monitoring Policy** page, locate the monitoring configuration you wish to modify and click its action button ⋮ to access the monitoring options panel.
5. Customize the configuration.
6. Click **Save** to apply your changes to the selected PATROL Agent(s).

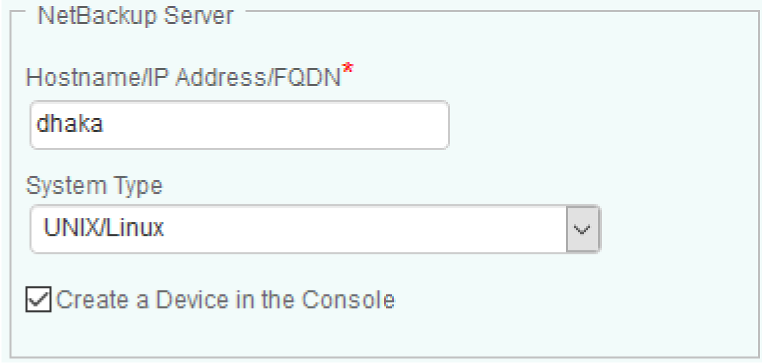
1. Configuring NetBackup Servers Settings

Before using Veritas NetBackup KM, you need to configure the monitoring settings for the Veritas NetBackup KM Monitor Type. You will then be able to create and customize other Monitor Types according to the component(s) you wish to monitor.

To configure the Veritas NetBackup KM monitoring settings

Specify the options that will constitute the NetBackup monitoring settings.

1. Create your monitoring policy.
2. In the **Add Monitoring Configuration** dialog box, configure the properties:
   - From the **Monitoring Solution** menu, select **Veritas NetBackup KM**
   - From the **Version** menu, select the required version
   - The **Monitor Profile Veritas NetBackup KM** is automatically selected
3. In the **NetBackup Monitoring Settings** section, click **Add.**
4. Specify the settings for the **NetBackup Host** to be monitored:
   - In the **Hostname/IP Address/FQDN** field:
     - for a local host, enter **localhost** to apply these settings to all PATROL Agents installed on the NetBackup Servers
     - for a remote host, enter a **hostname** or **IP address** to apply these settings to a specific server
   - Click the **Create a Device in the Console** box if you want the NetBackup server to appear as a separate device in TrueSight**.**



NetBackup Server

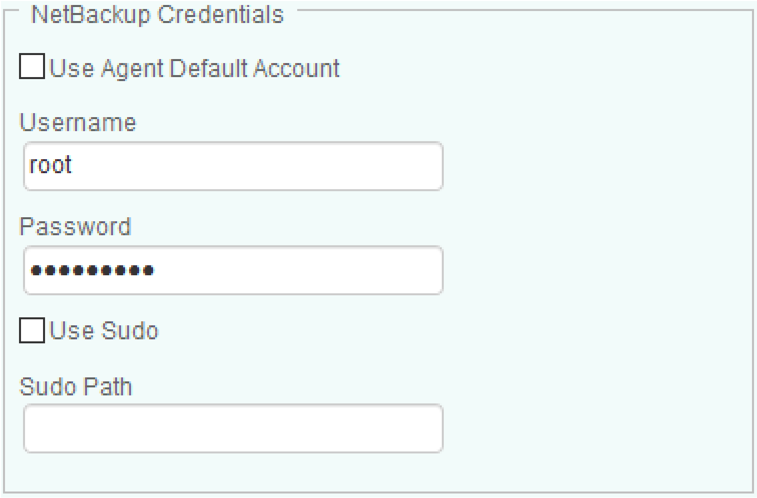
Hostname/IP Address/FQDN*: dhaka

System Type: UNIX/Linux

☑ Create a Device in the Console

Adding a NetBackup Host to the Monitoring Environment

5. Set the **NetBackup Credentials**:
   - To use the default PATROL Agent Account, check the **Use Agent Default Account** option
   - To use a different user account, enter the login details in the **Username** and **Password** fields
   - (**Unix Only**) If the user account has sudo privileges, check the **Use Sudo** box and indicate the sudo binary file path (by default: /usr/local/bin/sudo) menu, select Veritas NetBackup KM



NetBackup Credentials

☐ Use Agent Default Account

Username: root

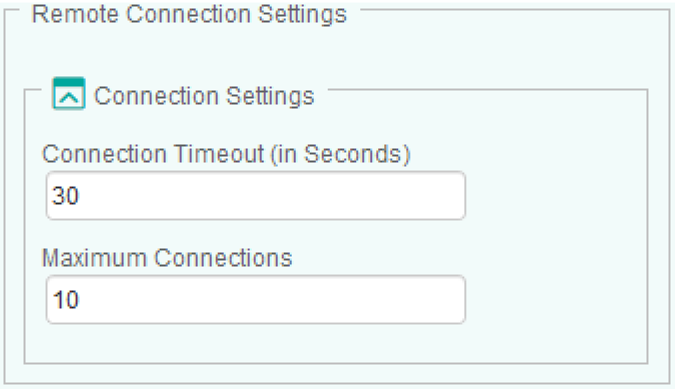
Password: ●●●●●●●●●

☐ Use Sudo

Sudo Path:

Configuring NetBackup User Account

6. *(Optional - Remote Monitoring Only)* Set the **Remote Connection Settings**:



Remote Connection Settings

Connection Settings

Connection Timeout (in Seconds): 30

Maximum Connections: 10

Configuring the Remote Connection Settings

- In the **Connection Timeout (in Seconds)** field, enter the number of seconds after which the connection to the remote node will time out
- In the **Maximum Connections** field, enter the maximum number of simultaneous connections allowed to the remote node

7. *(Optional)* Define the **Advanced Settings:**

- the debug mode
- the maximum number of instances
- the multi-node monitoring mode
- the NetBackup discovery overrides.

8. Click **OK** twice.
9. Click **Save**.

2. 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:

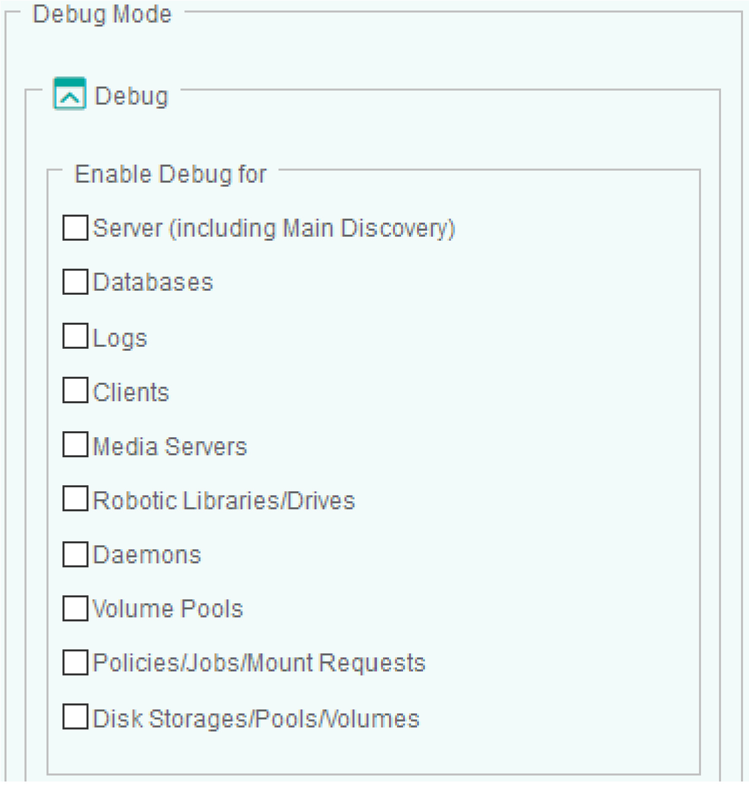
- The debug mode
- The maximum number of instances
- The multi-node monitoring mode
- The NetBackup server discovery overrides

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. Edit your monitoring policy.
2. Click the action button ⋮ of the VFS system for which you wish to enable the Debug Mode and click **Edit.**
3. In the **NetBackup Monitoring Settings** panel, scroll down to the **Debug** section.
4. Select all the elements for which you want to obtain debug information.



Debug Mode

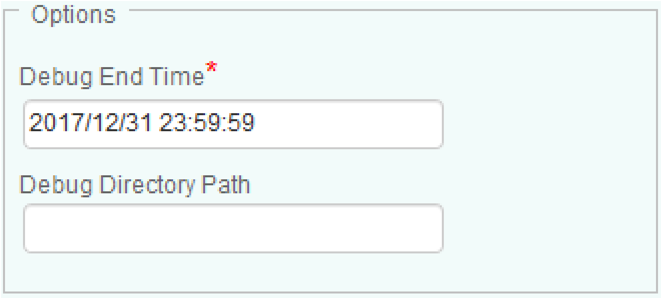
Debug

Enable Debug for

- □ Server (including Main Discovery)
- □ Databases
- □ Logs
- □ Clients
- □ Media Servers
- □ Robotic Libraries/Drives
- □ Daemons
- □ Volume Pools
- □ Policies/Jobs/Mount Requests
- □ Disk Storages/Pools/Volumes

Configuring the Debug Mode Settings

4. 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



Options

Debug End Time*

2017/12/31 23:59:59

Debug Directory Path

Setting the Debug End Time and Directory Path

5. Click **OK** to validate.

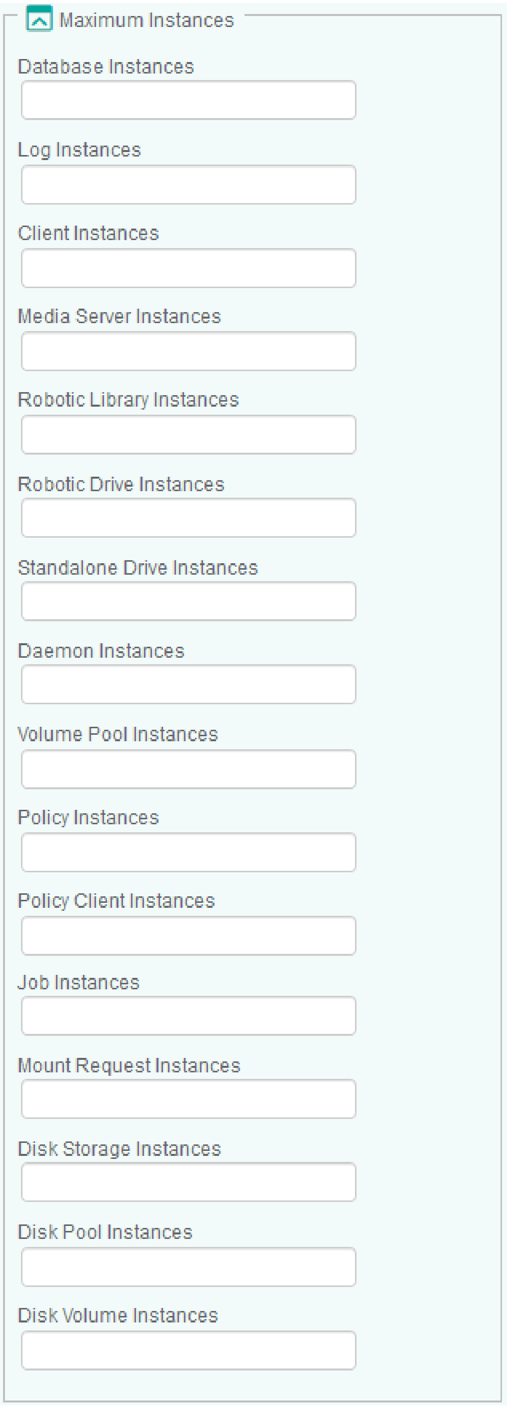
When the debug end time is reached, a tar/zip file is automatically created under <PATROL_HOME>/lib/NBU/ and can be sent to the BMC Support for help. It is also recommended to check the NBU_<port>.log file, stored in <PATROL_HOME>/log, for any error.

Configuring the Maximum Number of Instances

By default, the solution discovers and monitors all the instances. Because there may be a very large number of instances to monitor and this may represent a important workload to the agents and the TrueSight servers, it is recommended to only monitor the critical ones. This can be done by configuring the instance limits.

To configure the maximum number of instances

1. Edit your monitoring policy.
2. Click the action button ⋮ of the NetBackup server for which you wish to configure the maximum number of instances and click **Edit.**
3. In the **NetBackup Monitoring Settings** panel, scroll down to the **Maximum Number of Instances** section.
4. For each monitored element, indicate the maximum number of instances to be displayed, or enter **0** in the relevant field to disable the monitoring of a specific element. (By default, the maximum number of instances is left empty to allow an unlimited number of instances).



Maximum Instances

Database Instances

Log Instances

Client Instances

Media Server Instances

Robotic Library Instances

Robotic Drive Instances

Standalone Drive Instances

Daemon Instances

Volume Pool Instances

Policy Instances

Policy Client Instances

Job Instances

Mount Request Instances

Disk Storage Instances

Disk Pool Instances

Disk Volume Instances

Configuring the Maximum Number of Instances

5. Click **OK** twice.
6. Click **Save**.

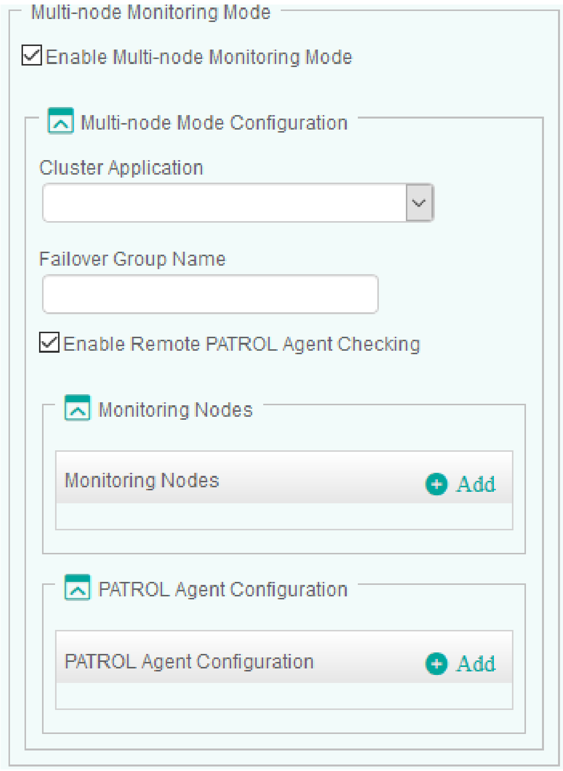
Configuring the Multi-Node Monitoring Mode

When an application is installed in a cluster environment, i.e. active on one cluster node and passive on others, false alarms and duplicate alerts may occur. To avoid such situation, users need to configure Veritas NetBackup KM in Multi-node monitoring mode, if NetBackup is installed in a supported cluster.

> The procedure below is generic. To learn more about all the configuration methods available, see **Configuring the Multi-node Monitoring Mode with the VCS KM**. Although the article refers to Veritas Cluster Server KM for PATROL, the monitoring concepts and principles remain valid for TrueSight Operations Management - Veritas NetBackup Monitoring.

To configure the multi-node monitoring mode

1. Edit your monitoring policy.
2. Click the action button ⋮ of the NetBackup server for which you wish to configure the multi-node monitoring mode and click **Edit.**
3. In the **NetBackup Monitoring Settings** panel, scroll down to the **Multi-node Monitoring Mode** section.


Multi-node Monitoring Mode

☑ Enable Multi-node Monitoring Mode

Multi-node Mode Configuration

Cluster Application:

Failover Group Name:

☑ Enable Remote PATROL Agent Checking

Monitoring Nodes

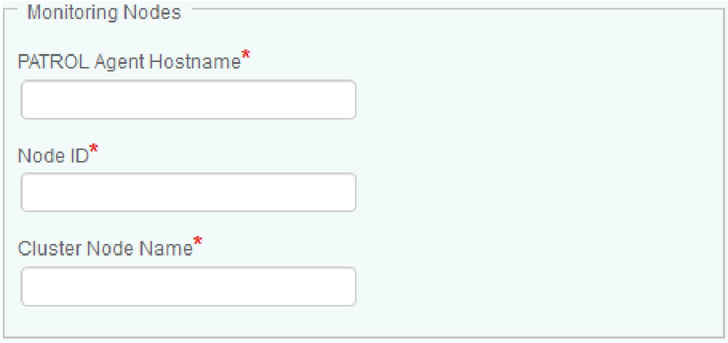
Monitoring Nodes

PATROL Agent Configuration

PATROL Agent Configuration

Configuring the Multi-Node Mode

3. Check the **Enable Multi-node Monitoring Mode** option.
4. Configure the Multi-node Mode:
   - Select the appropriate **Cluster Application**
   - Indicate the **Failover Group Name**. Leave this field blank if you have previously selected Veritas Cluster File System. Then the Veritas NetBackup KM will then monitor the NetBackup system 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
5. *(Optional)* Check the **Enable Remote PATROL Agent Checking** option to 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 cluster node or on the node where failover group is online and will not check the monitoring status of the Veritas NetBackup KM on the other PATROL Agent nodes.
6. In the **Monitoring Nodes** section:
   - Click **Add** to configure the details of all managed nodes of the cluster to be configured in the multi-node mode



Monitoring Nodes

PATROL Agent Hostname*

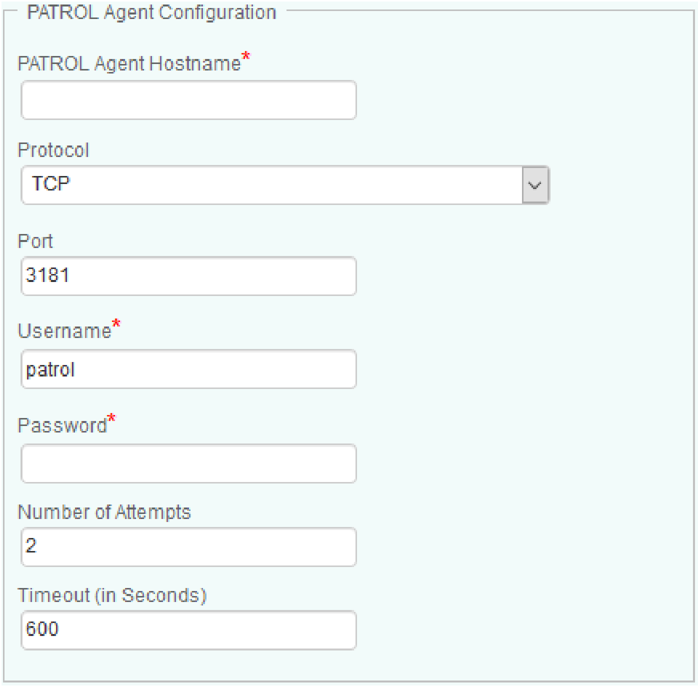
Node ID*

Cluster Node Name*

Identifying the Node to Monitor

   - Provide the **PATROL Agent Hostname** (host where the PATROL agent is installed), the **Node ID** (the unique ID of the NetBackup node derived from the hostname in the **NetBackup Server** configuration), and **Cluster Node Name** (the hostname defined in the selected **Cluster Application**)
   - Click **OK**
   - Repeat the procedure for each NetBackup node that is part of the multi-node mode configuration

7. If the **Enable Remote PATROL Agent Checking** option is selected, click **Add** in the **Remote Agent Configuration** section, to provide all the information required to communicate with the PATROL Agents. There should be one entry per each PATROL Agent.



PATROL Agent Configuration

PATROL Agent Hostname*

Protocol
TCP

Port
3181

Username*
patrol

Password*

Number of Attempts
2

Timeout (in Seconds)
600

Configuring the Remote Agent Communication Settings

- Provide the **PATROL Agent Hostname**
- Select the **Protocol** you wish to use to connect to the PATROL Agent
- Enter the **Port** number you wish to use to connect to the PATROL Agent
- Provide the **Username** and **Password** you wish to use to connect to the PATROL Agent
- In the **Number of Attempts** field, specify the number of times the solution will try to communicate with the remote PATROL Agent before failing over
- Enter the timeout you wish to set, in seconds, between each attempt

7. Click **OK** twice.
8. Click **Save**.

The NetBackup server will then be monitored through the master or online node in **Active Multi-node Mode**. The other nodes, which are standing by for a failover, will be in **Passive Multi-node Mode**, monitoring only the components that are not visible from the active node.

If a managed node is unable to check the monitoring status of the active managed node, it will change to **Temporary Single-node Mode** allowing a full NetBackup monitoring. It will remain in **Temporary Single-node Mode** until it finds the active node in full monitoring mode again.

If the **Remote PATROL Agent Checking** is **Disabled**, while there are more than one PATROL Agent involved, the managed node on the master or online node will be in **Active Multi-node Mode** and all others will be in **Passive Multi-node Mode**, without checking the monitoring status of the active node. In addition, the above procedure to configure Multi-node Mode needs to be repeated from each PATROL Agent involved.

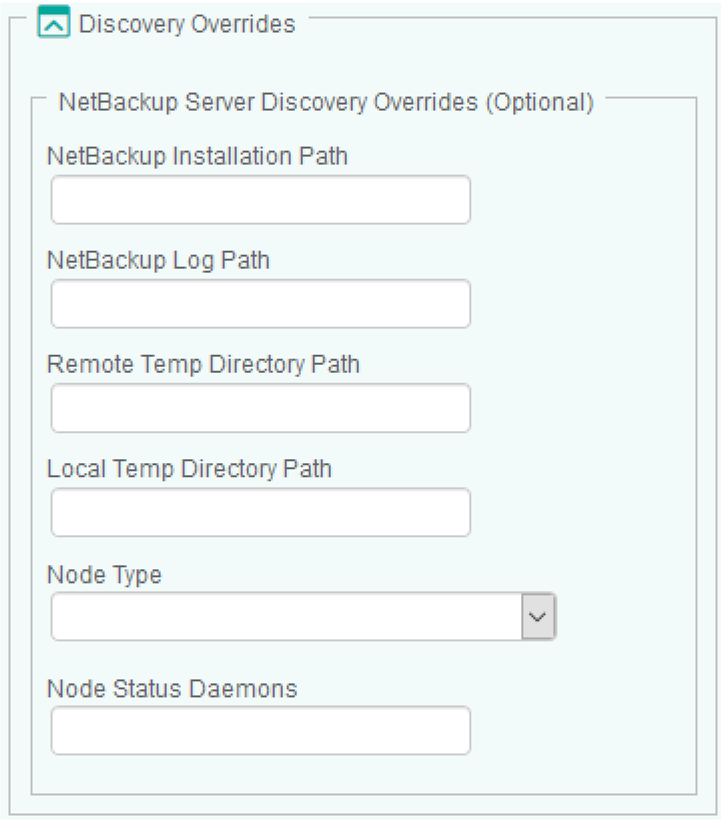
Configuring the NetBackup Server Discovery Overrides (Optional)

The solution automatically discovers the NetBackup installation, the temporary directory paths used by the Veritas NetBackup KM, and the node status. This information can however be overridden.

⚠ **Altering these paths may impact the operation of Veritas NetBackup KM.**

To configure NetBackup server discovery overrides

1. Edit your monitoring policy.
2. Click the action button ⋮ of the NetBackup server for which you wish to configure the discovery overrides and click **Edit.**
3. In the **NetBackup Monitoring Settings** panel, scroll down to the **Discovery Overrides** section.


Discovery Overrides
NetBackup Server Discovery Overrides (Optional)
NetBackup Installation Path
NetBackup Log Path
Remote Temp Directory Path
Local Temp Directory Path
Node Type
Node Status Daemons

Configuring NetBackup Discovery Overrides

3. Specify the **NetBackup Server Discovery Overrides** options:
   - **NetBackup Installation Path**: Provide the path to the directory where the NetBackup software is installed. By default, Veritas NetBackup KM automatically locates the NetBackup software installation directory if you have installed the solution with the default recommended settings. If you have chosen to install the solution in a custom directory, you are required to provide its location.
   - **Remote Temp Directory Path**: Provide the path to the directory where the temporary files are saved on remote nodes. Default is **/var/tmp** (on UNIX/Linux) or **C:\Windows\Temp** (on Windows).
   - **Local Temp Directory Path**: Provide the path to the directory where the temporary files are saved on the PATROL Agent node (Default is <PATROL_HOME>/lib/NBU/tmp where PATROL_HOME is the PATROL Agent installation path)
   - **Node Type**: Select the appropriate node type: media or master server. By default, Veritas NetBackup KM automatically discovers the type of node when the type is not user-specified.
   - **Node Status Daemons**: Specify the critical NetBackup node daemons in order to detect the node status. Daemon names must be comma-delimited. By default, daemons are automatically selected according on the node type.
5. Click **OK** twice.
6. Click **Save**.

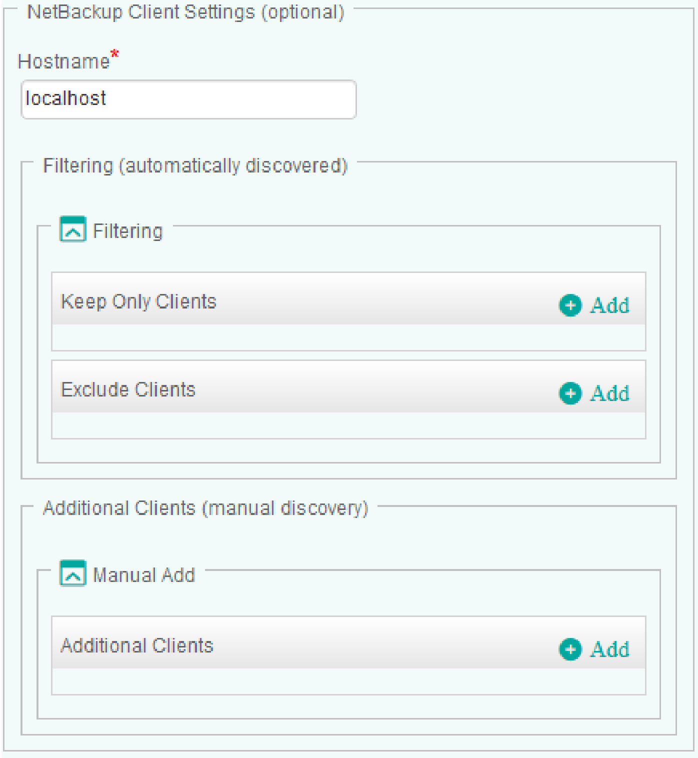
Configuring Other Monitor Types

Configuring NetBackup Clients

By default, the solution monitors all the NetBackup clients discovered, which may represent an important workload for the Agents and the TrueSight servers. Because the monitoring of some NetBackup clients may be irrelevant for various reasons, you can apply filters to specify the NetBackup clients that will be monitored or discarded.

To configure NetBackup clients

1. From the **Add Monitoring Configuration** panel, select **NetBackup Client** from the **Monitor Type** list.
2. In the **NetBackup Server Client** panel, click **Add**.



NetBackup Client Settings (optional)

Hostname*

localhost

Filtering (automatically discovered)

Filtering

Keep Only Clients

Exclude Clients

Additional Clients (manual discovery)

Manual Add

Additional Clients

Configuring NetBackup Clients

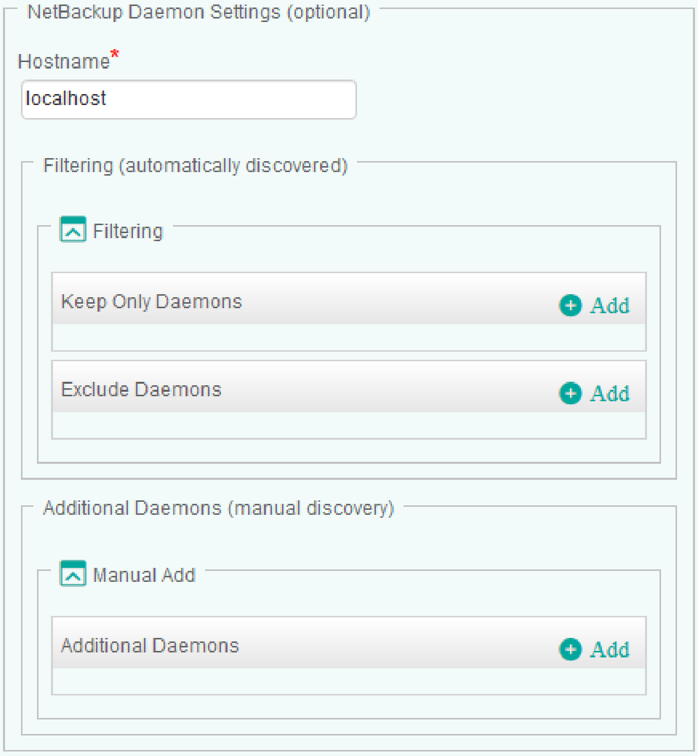
3. In the **Hostname** field, enter:
    - **localhost** to apply these settings to all PATROL Agents installed on NetBackup Servers
    - a **hostname** or **IP address** to apply these settings to a specific server.
4. Configure the **Filtering** options:
    - In the **Keep Only Clients...** section, click **Add** and identify the NetBackup client you wish to monitor. Enter the name of the NetBackup client or identify it by using a regular expression (example: prod-client*). Click **OK** to validate. Repeat the operation for any other NetBackup client you wish to include in the monitoring process.
    - In the **Exclude Clients...** section, click **Add** and identify the NetBackup client you do not want to monitor. Enter the name of the NetBackup client or identify it by using a regular expression (example: test-client*). Click **OK** to validate. Repeat the operation for any other NetBackup client you wish to exclude from the monitoring process.
5. The **Additional Clients** (manual discovery) allows you to add NetBackup clients manually, when they are not automatically discovered:
    - Click **Add** and enter the name of the NetBackup client you wish to add to the monitoring environment. Click **OK** to validate. Repeat the operation for each NetBackup client you want to monitor.
    - (Optional) Enter a short description that will allow you to quickly identify the added NetBackup client.
6. Click **OK** to validate.

Configuring NetBackup Daemons

By default, the solution monitors all the NetBackup daemons discovered, which may represent an important workload for the Agents and the TrueSight servers. Because the monitoring of some NetBackup daemons may be irrelevant for various reasons, you can apply filters to specify the NetBackup daemons that will be monitored or discarded.

To configure NetBackup daemons

1. From the **Add Monitoring Configuration** panel, select **NetBackup Daemon** from the **Monitor Type** list.
2. In the **NetBackup Server Daemon** panel, click **Add**.


NetBackup Daemon Settings (optional)
Filtering (automatically discovered)
Filtering
Keep Only Daemons
Add
Exclude Daemons
Add
Additional Daemons (manual discovery)
Manual Add
Additional Daemons
Add

Hostname*: localhost

Configuring NetBackup Daemons

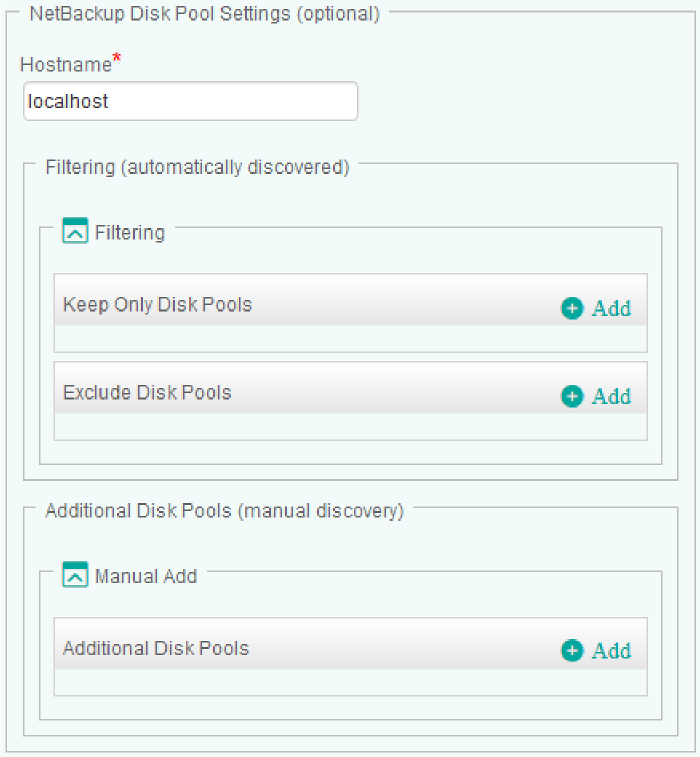
3. In the **Hostname** field, enter:
    - **localhost** to apply these settings to all PATROL Agents installed on NetBackup Servers
    - a **hostname** or **IP address** to apply these settings to a specific server.
4. Configure the **Filtering** options:
    - In the **Keep Only Daemon...** section, click **Add** and identify the NetBackup daemon you wish to monitor. Enter the name of the NetBackup daemon or identify it by using a regular expression (example: prod-daemon*). Click **OK** to validate. Repeat the operation for any other NetBackup daemon you wish to include in the monitoring process.
    - In the **Exclude Daemon...** section, click **Add** and identify the NetBackup daemon you do not want to monitor. Enter the name of the NetBackup daemon or identify it by using a regular expression (example: test-daemon*). Click **OK** to validate. Repeat the operation for any other NetBackup daemon you wish to exclude from the monitoring process.
5. The **Additional Daemons** (manual discovery) allows you to add NetBackup daemon manually, when they are not automatically discovered:
    - Click **Add** and enter the name of the NetBackup daemon you wish to add to the monitoring environment. Click **OK** to validate. Repeat the operation for each NetBackup daemon you want to monitor.
    - (Optional) Enter a short description that will allow you to quickly identify the added NetBackup daemon.
6. Click **OK** to validate.

Configuring NetBackup Disk Pools

By default, the solution monitors all the NetBackup disk pools discovered, which may represent an important workload for the Agents and the TrueSight servers. Because the monitoring of some NetBackup disk pools may be irrelevant for various reasons, you can apply filters to specify the NetBackup disk pools that will be monitored or discarded.

To configure NetBackup disk pools

1. From the **Add Monitoring Configuration** panel, select **NetBackup Disk Pool** from the **Monitor Type** list.
2. In the **NetBackup Disk Pool** panel, click **Add**.



NetBackup Disk Pool Settings (optional)

Hostname*: localhost

Filtering (automatically discovered)

Filtering

Keep Only Disk Pools

Exclude Disk Pools

Additional Disk Pools (manual discovery)

Manual Add

Additional Disk Pools

Configuring NetBackup Disk Pools

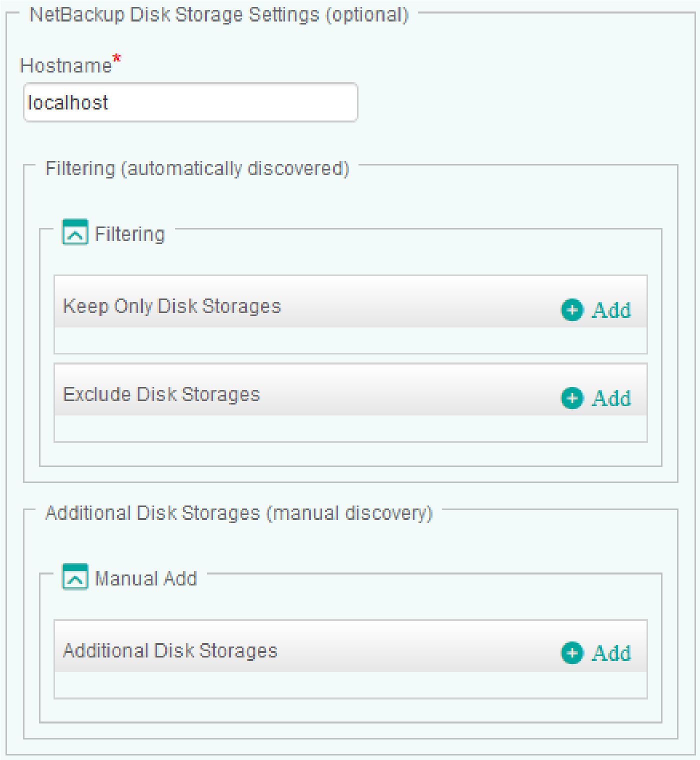
3. In the **Hostname** field, enter:
   - **localhost** to apply these settings to all PATROL Agents installed on NetBackup Servers
   - a **hostname** or **IP address** to apply these settings to a specific server.
4. Configure the **Filtering** options:
   - In the **Keep Only Disk Pools...** section, click **Add** and identify the NetBackup disk pool you wish to monitor. Enter the name of the NetBackup disk pool or identify it by using a regular expression (example: prod-diskpool*). Click **OK** to validate. Repeat the operation for any other NetBackup disk pool you wish to include in the monitoring process.
   - In the **Exclude Disk Pools...** section, click **Add** and identify the NetBackup disk pool you do not want to monitor. Enter the name of the NetBackup disk pool or identify it by using a regular expression (example: test-diskpool*). Click **OK** to validate. Repeat the operation for any other NetBackup disk pool you wish to exclude from the monitoring process.
5. The **Additional Disk Pools** (manual discovery) allows you to add NetBackup disk pool manually, when they are not automatically discovered:
   - Click **Add** and enter the name of the NetBackup disk pool you wish to add to the monitoring environment. Click **OK** to validate. Repeat the operation for each NetBackup disk pool you want to monitor.
   - (Optional) Enter a short description that will allow you to quickly identify the added NetBackup disk pool.
6. Click **OK** to validate.

Configuring NetBackup Disk Storage

By default, the solution monitors all the NetBackup disk storage discovered, which may represent an important workload for the Agents and the TrueSight servers. Because the monitoring of some NetBackup disk storage may be irrelevant for various reasons, you can apply filters to specify the NetBackup disk storage that will be monitored or discarded.

To configure NetBackup disk storage

1. From the **Add Monitoring Configuration** panel, select **NetBackup Disk Storage** from the **Monitor Type** list.
2. In the **NetBackup Disk Storage** panel, click **Add**.



NetBackup Disk Storage Settings (optional)

Hostname*: localhost

Filtering (automatically discovered)

Additional Disk Storages (manual discovery)

Configuring NetBackup Disk Storage

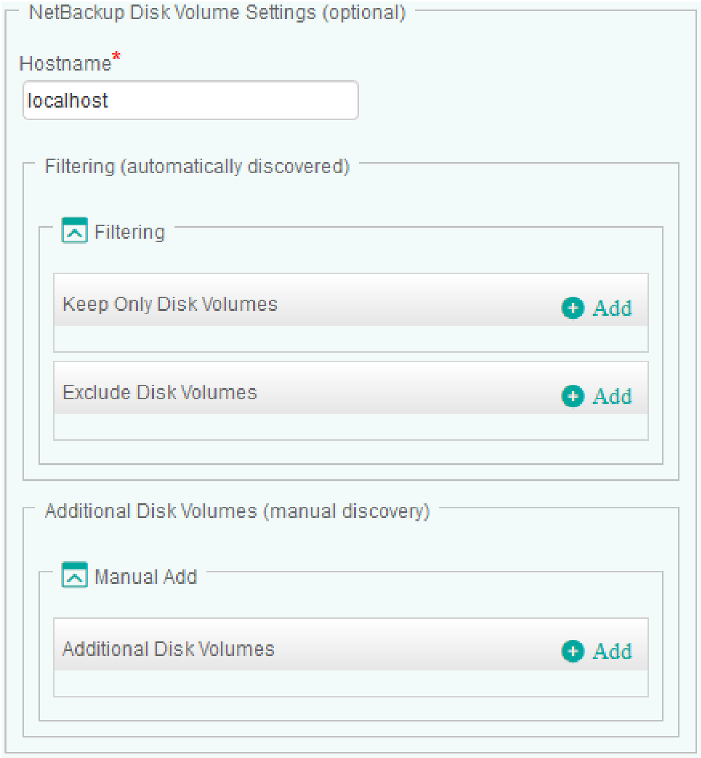
3. In the **Hostname** field, enter:
   - **localhost** to apply these settings to all PATROL Agents installed on NetBackup Servers
   - a **hostname** or **IP address** to apply these settings to a specific server.
4. Configure the **Filtering** options:
   - In the **Keep Only Disk Storage...** section, click **Add** and identify the NetBackup disk storage you wish to monitor. Enter the name of the NetBackup disk storage or identify it by using a regular expression (example: prod-diskstorage*). Click **OK** to validate. Repeat the operation for any other NetBackup disk storage you wish to include in the monitoring process.
   - In the **Exclude Disk Storage...** section, click **Add** and identify the NetBackup disk storage you do not want to monitor. Enter the name of the NetBackup disk storage or identify it by using a regular expression (example: test-diskstorage*). Click **OK** to validate. Repeat the operation for any other NetBackup disk storage you wish to exclude from the monitoring process.
5. The **Additional Disk Storage** (manual discovery) allows you to add NetBackup disk storage manually, when they are not automatically discovered:
   - Click **Add** and enter the name of the NetBackup disk storage you wish to add to the monitoring environment. Click **OK** to validate. Repeat the operation for each NetBackup disk storage you want to monitor.
   - (Optional) Enter a short description that will allow you to quickly identify the added NetBackup disk storage.
6. Click **OK** to validate.

Configuring NetBackup Disk Volumes

By default, the solution monitors all the NetBackup disk volumes discovered, which may represent an important workload for the Agents and the TrueSight servers. Because the monitoring of some NetBackup disk volumes may be irrelevant for various reasons, you can apply filters to specify the NetBackup disk volume that will be monitored or discarded.

To configure NetBackup disk volumes

1. From the **Add Monitoring Configuration** panel, select **NetBackup Disk Volume** from the **Monitor Type** list.
2. In the **NetBackup Disk Volume** panel, click **Add**.



Hostname*: localhost

NetBackup Disk Volume Settings (optional)
Filtering (automatically discovered)
Filtering
Keep Only Disk Volumes
Add
Exclude Disk Volumes
Add
Additional Disk Volumes (manual discovery)
Manual Add
Additional Disk Volumes
Add

Configuring NetBackup Disk Volumes

3. In the **Hostname** field, enter:
   - **localhost** to apply these settings to all PATROL Agents installed on NetBackup Servers
   - a **hostname** or **IP address** to apply these settings to a specific server.
4. Configure the **Filtering** options:
   - In the **Keep Only Disk Volumes...** section, click **Add** and identify the NetBackup disk volume you wish to monitor. Enter the name of the NetBackup disk volume or identify it by using a regular expression (example: prod-diskvolume*). Click **OK** to validate. Repeat the operation for any other NetBackup disk volume you wish to include in the monitoring process.
   - In the **Exclude Disk Volumes...** section, click **Add** and identify the NetBackup disk volume you do not want to monitor. Enter the name of the NetBackup disk volume or identify it by using a regular expression (example: test-diskvolume*). Click **OK** to validate. Repeat the operation for any other NetBackup disk volume you wish to exclude from the monitoring process.
5. The **Additional Disk Volumes** (manual discovery) allows you to add NetBackup disk volume manually, when they are not automatically discovered:
   - Click **Add** and enter the name of the NetBackup disk volume you wish to add to the monitoring environment. Click **OK** to validate. Repeat the operation for each NetBackup disk volume you want to monitor.
   - (Optional) Enter a short description that will allow you to quickly identify the added NetBackup disk volume.
6. Click **OK** to validate.

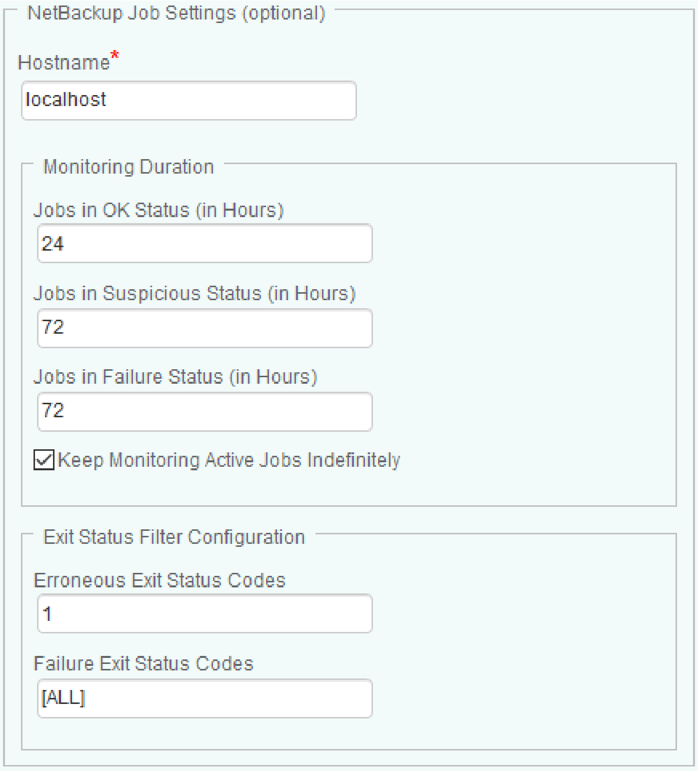
Configuring NetBackup Jobs

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 NetBackup jobs

1. From the **Add Monitoring Configuration** panel, select **NetBackup Job** from the **Monitor Type** list.
2. In the **NetBackup Job** panel, click **Add**.



NetBackup Job Settings (optional)

Hostname*
localhost

Monitoring Duration

Jobs in OK Status (in Hours)
24

Jobs in Suspicious Status (in Hours)
72

Jobs in Failure Status (in Hours)
72

☑ Keep Monitoring Active Jobs Indefinitely

Exit Status Filter Configuration

Erroneous Exit Status Codes
1

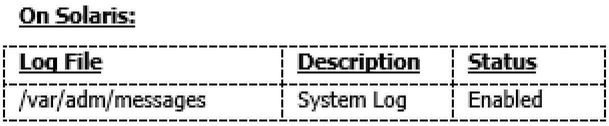
Failure Exit Status Codes
[ALL]

Configuring NetBackup Jobs

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.
6. Click **OK** to validate.

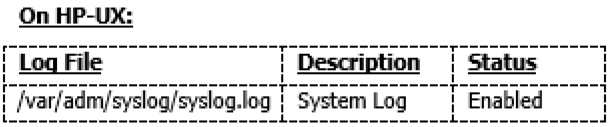
Configuring NetBackup Logs

By default, Veritas NetBackup KM monitors the following log files:



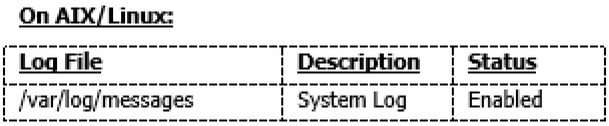
On Solaris:

Log File	Description	Status
/var/adm/messages	System Log	Enabled



On HP-UX:

Log File	Description	Status
/var/adm/syslog/syslog.log	System Log	Enabled



On AIX/Linux:

Log File	Description	Status
/var/log/messages	System Log	Enabled

A log filter is configured by default for the above log files to ensure warnings or alarms are triggered when a specific error message is found. This default configuration can however be modified in TrueSight if you need to monitor:

- error messages that are not included in the default filter. You will then have to customize the log filter
- any other log, such as Windows System Event Logs. In that case, you will have to:
  - specify the custom logs to be monitored
  - and customize the log filter to indicate the regular expressions that will generate a warning and/or an alarm.

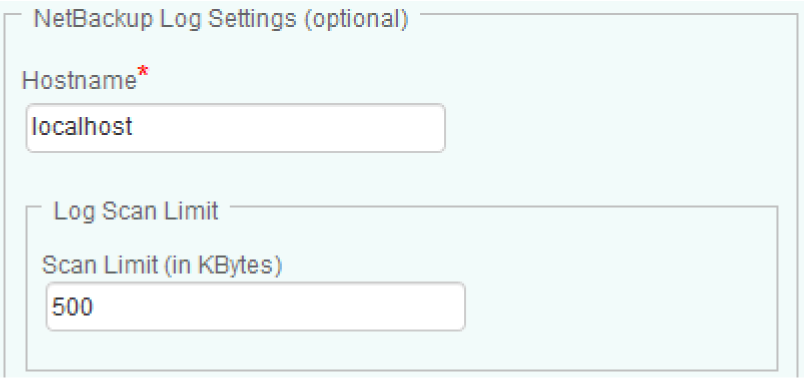
Configuring the Log Scan Limit

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. From the **Add Monitoring Configuration** panel, select **NetBackup Log** from the **Monitor Type** list.
2. In the **NetBackup Log Settings** panel, click **Add.**



NetBackup Log Settings (optional)

Hostname*: localhost

Log Scan Limit

Scan Limit (in KBytes): 500

Customizing the Log Scan Limit

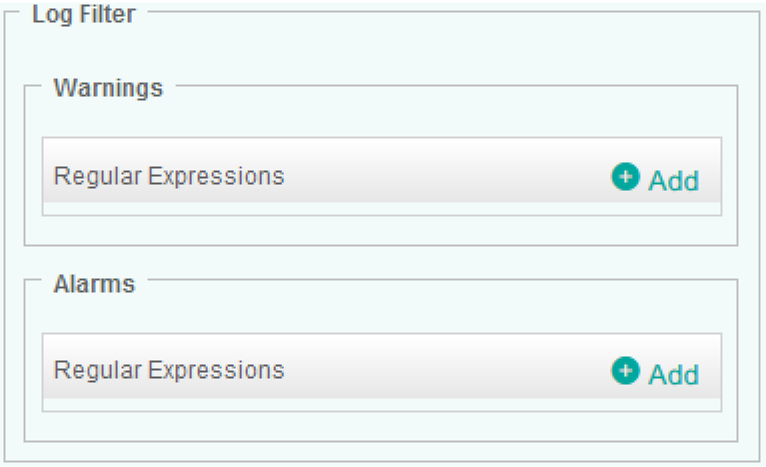
3. In the **Hostname** field, enter:
   - **localhost** to apply these settings to all PATROL Agents installed on the NetBackup server
   - a **hostname** or **IP address** to apply these settings to a specific server
4. Indicate the amount of data (in KBytes) that will be read by the monitoring solution during each data collection cycle.
5. Click **OK** twice.
6. Click **Save**.

Customizing the Log Filter

By default, Veritas NetBackup KM only monitors the daily NetBackup messages file and the system log file. A log filter is configured by default to ensure warnings or alarms are triggered when a specific error message is found. You can however customize this default log filter to monitor any other error message in the NetBackup daily log or any other log files.

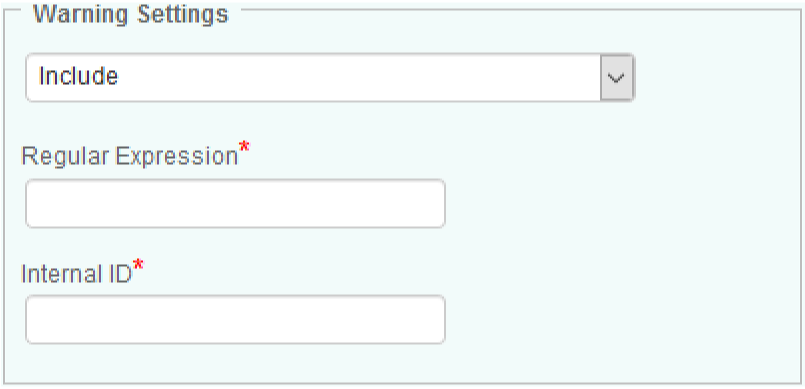
To customize the log filter

1. From the **Add Monitoring Configuration** panel, select **NetBackup Log** from the **Monitor Type** list.
2. In the **NetBackup Log Settings** panel, click **Add.**
3. In the **Log Filter** section, configure the conditions that will trigger a warning and/or an alarm:



Customizing the log filter

- In the **Warnings** section:
  - Click **Add**
  - Select the type of regular expression. **Include** will select all matching lines; **Exclude** will remove all matching lines
  - In the **Regular Expression** field, enter the expression that will trigger a warning
  - Provide your warning filter with an **Internal ID**
  - Click **OK** to validate.


Warning Settings

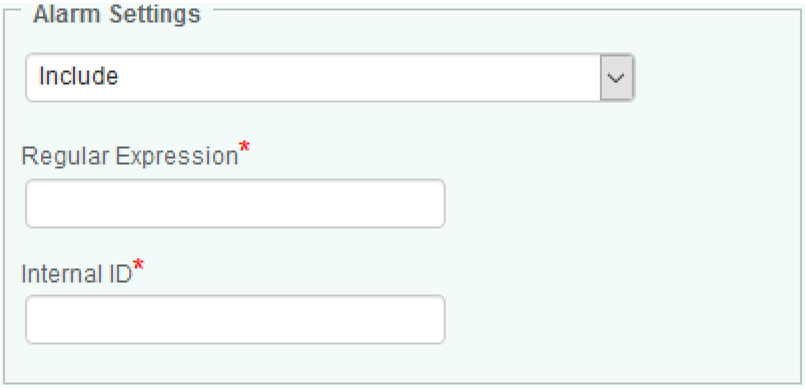
Include

Regular Expression*

Internal ID*

Expressions that will generate a warning

- In the **Alarms** section
  - Click **Add**
  - Select the type of regular expression. **Include** will select all matching lines; **Exclude** will remove all matching lines
  - In the **Regular Expression** field, enter the expression that will trigger an alarm
  - Provide your alarm filter with an **Internal ID**
  - Click **OK** to validate


Alarm Settings

Include

Regular Expression*

Internal ID*

Expressions that will generate an alarm

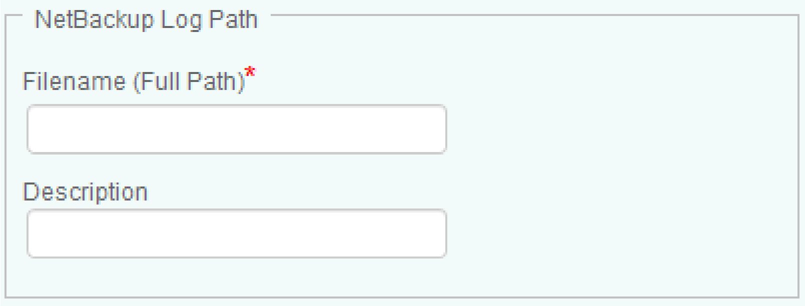
4. Click **OK** twice.
5. Click **Save**.

Configuring Custom NetBackup Logs Monitoring

By default, Veritas NetBackup KM only monitors the daily NetBackup messages file and the system log file. To override the default configuration and add additional log files, you will have to configure the custom NetBackup Logs monitoring.

To customize the NetBackup logs monitoring

1. From the **Add Monitoring Configuration** panel, select **NetBackup Log** from the **Monitor Type** list.
2. In the **NetBackup Log Settings** panel, click **Add.**
3. In the **Custom NetBackup Logs** section, click **Add.**


NetBackup Log Path

Filename (Full Path)*

Description

Configuring Custom NetBackup Logs

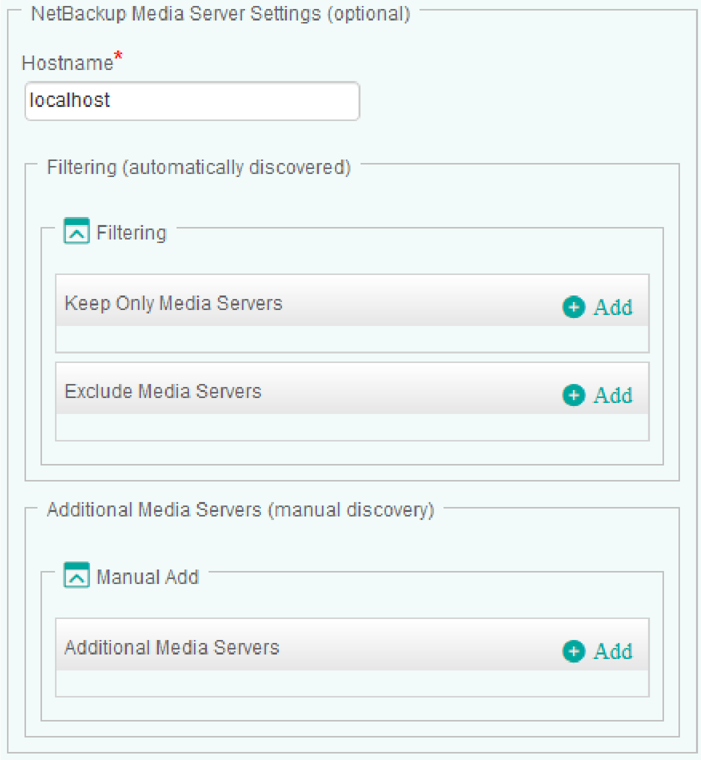
4. In the **Filename (Full Path)** field, enter the full path to the NetBackup Log file to be monitored using "\" as a separator (example:\var\adm\messages). For Windows events, prefix the filename with **Events -** (example: Events - Systems).
5. *(Optional)* Enter a brief description of the NetBackup log.
6. Click **OK.**
7. Customize the log filter to indicate the regular expressions that will generate a warning and/or an alarm when found in the custom NetBackup log.
8. Click **OK** twice.
9. Click **Save**.

Configuring NetBackup Media Servers

By default, the solution monitors all the NetBackup media servers discovered, which may represent an important workload for the Agents and the TrueSight servers. Because the monitoring of some NetBackup media servers may be irrelevant for various reasons, you can apply filters to specify the NetBackup media servers that will be monitored or discarded.

To configure NetBackup media servers

1. From the **Add Monitoring Configuration** panel, select **NetBackup Media Server** from the **Monitor Type** list.
2. In the **NetBackup Media Server** panel, click **Add**.



NetBackup Media Server Settings (optional)

Hostname*

localhost

Filtering (automatically discovered)

Additional Media Servers (manual discovery)

Configuring NetBackup Media Servers

3. In the **Hostname** field, enter:
   - **localhost** to apply these settings to all PATROL Agents installed on NetBackup Servers
   - a **hostname** or **IP address** to apply these settings to a specific server.
4. Configure the **Filtering** options:
   - In the **Keep Only Media Servers...** section, click **Add** and identify the NetBackup media server you wish to monitor. Enter the name of the NetBackup media server or identify it by using a regular expression (example: prod-server*). Click **OK** to validate. Repeat the operation for any other NetBackup media server you wish to include in the monitoring process.
   - In the **Exclude Media Servers...** section, click **Add** and identify the NetBackup media server you do not want to monitor. Enter the name of the NetBackup media server or identify it by using a regular expression (example: test-server*). Click **OK** to validate. Repeat the operation for any other NetBackup media server you wish to exclude from the monitoring process.
5. The **Additional Media Servers** (manual discovery) allows you to add NetBackup media servers manually, when they are not automatically discovered:
   - Click **Add** and enter the name of the NetBackup media server you wish to add to the monitoring environment. Click **OK** to validate. Repeat the operation for each NetBackup media server you want to monitor.
   - (Optional) Enter a short description that will allow you to quickly identify the added NetBackup media server.
6. Click **OK** to validate.

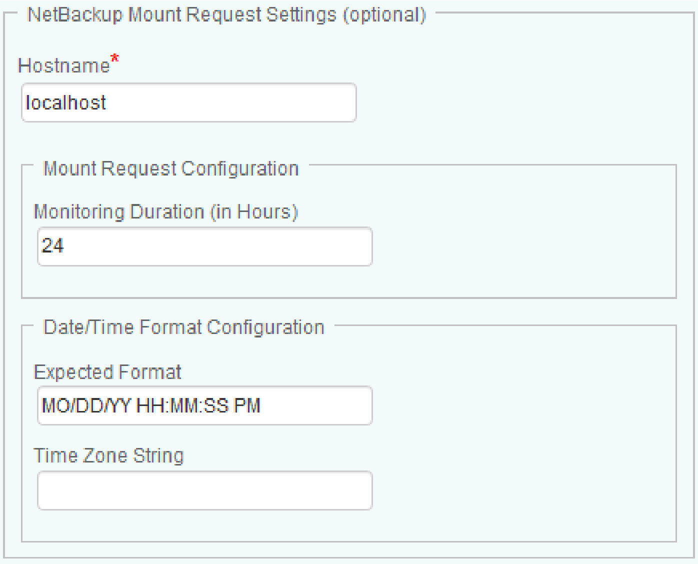
Configuring NetBackup Mount Requests

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 NetBackup mount requests

1. From the **Add Monitoring Configuration** panel, select **NetBackup Mount Request** from the **Monitor Type** list.
2. In the **NetBackup Mount Request** panel, click **Add**.



NetBackup Mount Request Settings (optional)

Hostname*: localhost

Mount Request Configuration

Monitoring Duration (in Hours): 24

Date/Time Format Configuration

Expected Format: MO/DD/YY HH:MM:SS PM

Time Zone String:

Configuring NetBackup Mont Requests

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. In the **Mount Request Configuration** section, indicate how many hours the mount requests will be monitored
5. If the date/time format returned by 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:

Format	Description
Default Date/Time Format	Leave blank.

Format	Description
EPOCH	Set EPOCH, if the time format is the number of seconds that have elapsed since 00:00:00 GMT January 1, 1970
Year Formats	
YY	Two digit figure Example: 12 for the year 2012
YYYY	Four digit figure Example: 2012
Month Formats	
MO	Two digit figure Example: 02 for February
MONTH	Month full name Example: February
MON	Three character name Example: Feb
Date Formats	
DD	Two digit figure Example: 05
Day Formats	
DAYFULL	Day full name Example: Friday
DAY	Three character name Example: Fr
Hour Formats	
HH	Two digit figure
Minute Formats	
MM	Two digit figure
Second Formats	
SS	Two digit figure
Time Formats	
[blank]	Time is in 24-hour format
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.)

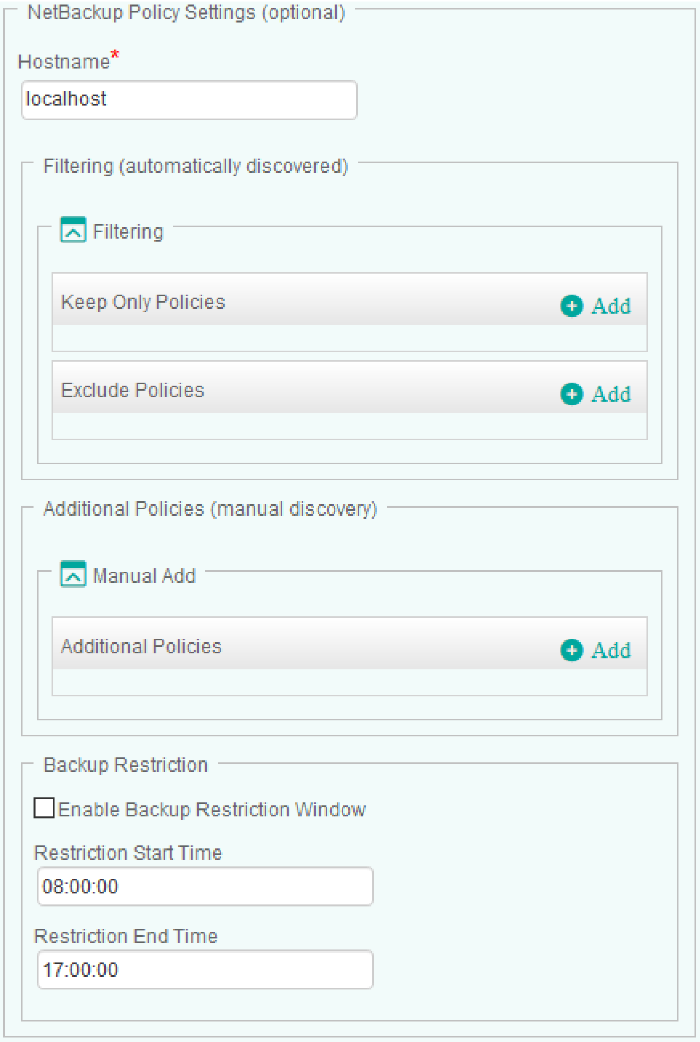
6. Click **OK** to validate.

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 NetBackup policies

1. From the **Add Monitoring Configuration** panel, select **NetBackup Policy** from the **Monitor Type** list.
2. In the **NetBackup Policy** panel, click **Add**.



NetBackup Policy Settings (optional)

Hostname*: localhost

Filtering (automatically discovered)

Filtering

Keep Only Policies — Add

Exclude Policies — Add

Additional Policies (manual discovery)

Manual Add

Additional Policies — Add

Backup Restriction

□ Enable Backup Restriction Window

Restriction Start Time: 08:00:00

Restriction End Time: 17:00:00

Configuring NetBackup Policies

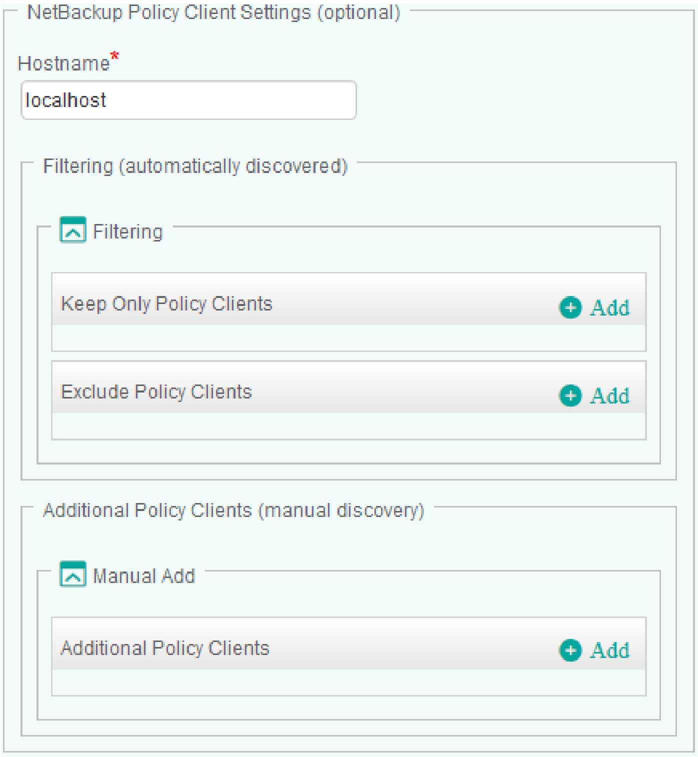
3. In the **Hostname** field, enter:
   - **localhost** to apply these settings to all PATROL Agents installed on NetBackup Servers
   - a **hostname** or **IP address** to apply these settings to a specific server.
4. Configure the **Filtering** options:
   - In the **Keep Only Policies...** section, click **Add** and identify the NetBackup policy you wish to monitor. Enter the name of the NetBackup policy or identify it by using a regular expression (example: prod-policy*). Click **OK** to validate. Repeat the operation for any other NetBackup policy you wish to include in the monitoring process.
   - In the **Exclude Policies...** section, click **Add** and identify the NetBackup policy you do not want to monitor. Enter the name of the NetBackup policy or identify it by using a regular expression (example: test-policy*). Click **OK** to validate. Repeat the operation for any other NetBackup policy you wish to exclude from the monitoring process.
5. The **Additional Policies** (manual discovery) allows you to add NetBackup policies manually, when they are not automatically discovered:
   - Click **Add** and enter the name of the NetBackup policy you wish to add to the monitoring environment. Click **OK** to validate. Repeat the operation for each NetBackup policy you want to monitor.
   - (Optional) Enter a short description that will allow you to quickly identify the added NetBackup policy.
6. 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** option
   - Indicate the **Restriction Start** and **End Time**. The format required is HH:MM:SS and the restriction window must at least last 5 minutes.
7. Click **OK** to validate.

Configuring NetBackup Policy Clients

By default, the solution monitors all the NetBackup policy clients discovered, which may represent an important workload for the Agents and the TrueSight servers. Because the monitoring of some NetBackup policy clients may be irrelevant for various reasons, you can apply filters to specify the NetBackup policy client that will be monitored or discarded.

To configure NetBackup policy clients

1. From the **Add Monitoring Configuration** panel, select **NetBackup Policy Client** from the **Monitor Type** list.
2. In the **NetBackup Policy Client** panel, click **Add**.



NetBackup Policy Client Settings (optional)

Hostname*

localhost

Filtering (automatically discovered)

Filtering

Keep Only Policy Clients

Exclude Policy Clients

Additional Policy Clients (manual discovery)

Manual Add

Additional Policy Clients

Configuring NetBackup Policy Clients

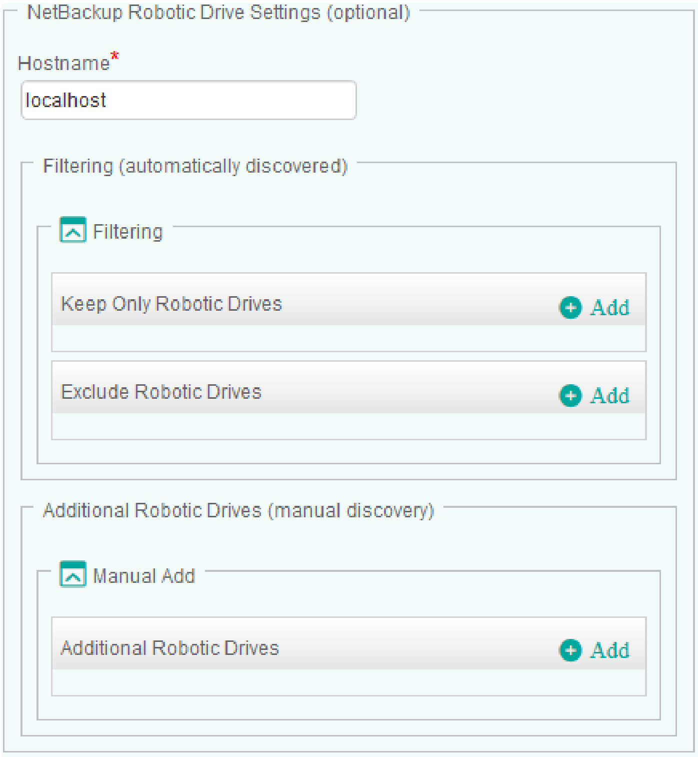
3. In the **Hostname** field, enter:
   - **localhost** to apply these settings to all PATROL Agents installed on NetBackup Servers
   - a **hostname** or **IP address** to apply these settings to a specific server.
4. Configure the **Filtering** options:
   - In the **Keep Only Policy Clients...** section, click **Add** and identify the NetBackup policy client you wish to monitor. Enter the name of the NetBackup policy client or identify it by using a regular expression (example: prod-policyclient*). Click **OK** to validate. Repeat the operation for any other NetBackup policy client you wish to include in the monitoring process.
   - In the **Exclude Policy Clients...** section, click **Add** and identify the NetBackup policy client you do not want to monitor. Enter the name of the NetBackup policy client or identify it by using a regular expression (example: test-policyclient*). Click **OK** to validate. Repeat the operation for any other NetBackup policy client you wish to exclude from the monitoring process.
5. The **Additional Policy Clients** (manual discovery) allows you to add NetBackup policy client manually, when they are not automatically discovered:
   - Click **Add** and enter the name of the NetBackup policy client you wish to add to the monitoring environment. Click **OK** to validate. Repeat the operation for each NetBackup policy client you want to monitor.
   - (Optional) Enter a short description that will allow you to quickly identify the added NetBackup policy client.
6. Click **OK** to validate.

Configuring NetBackup Robotic Drives

By default, the solution monitors all the NetBackup robotic drives discovered, which may represent an important workload for the Agents and the TrueSight servers. Because the monitoring of some NetBackup robotic drives may be irrelevant for various reasons, you can apply filters to specify the NetBackup robotic drives that will be monitored or discarded.

To configure NetBackup robotic drives

1. From the **Add Monitoring Configuration** panel, select **NetBackup Robotic Drive** from the **Monitor Type** list.
2. In the **NetBackup Robotic Drive** panel, click **Add**.



NetBackup Robotic Drive Settings (optional)

Hostname*

localhost

Filtering (automatically discovered)
Filtering
Keep Only Robotic Drives
Add
Exclude Robotic Drives
Add
Additional Robotic Drives (manual discovery)
Manual Add
Additional Robotic Drives
Add

Configuring NetBackup Robotic Drives

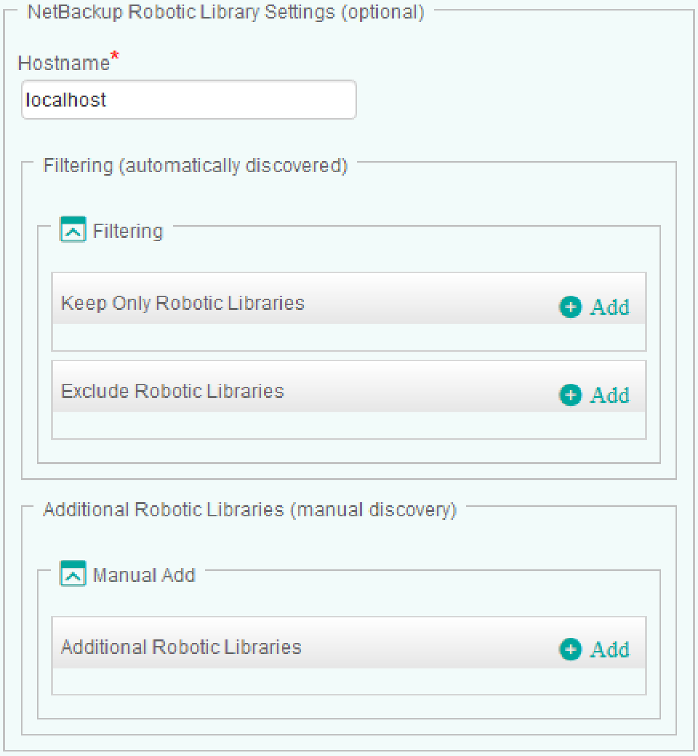
3. In the **Hostname** field, enter:
   - **localhost** to apply these settings to all PATROL Agents installed on NetBackup Servers
   - a **hostname** or **IP address** to apply these settings to a specific server.
4. Configure the **Filtering** options:
   - In the **Keep Only Robotic Drives...** section, click **Add** and identify the NetBackup robotic drive you wish to monitor. Enter the name of the NetBackup robotic drive or identify it by using a regular expression (example: prod-drive*). Click **OK** to validate. Repeat the operation for any other NetBackup robotic drive you wish to include in the monitoring process.
   - In the **Exclude Robotic Drives...** section, click **Add** and identify the NetBackup robotic drive you do not want to monitor. Enter the name of the NetBackup robotic drive or identify it by using a regular expression (example: test-drive*). Click **OK** to validate. Repeat the operation for any other NetBackup robotic drive you wish to exclude from the monitoring process.
5. The **Additional Robotic Drives** (manual discovery) allows you to add NetBackup robotic drives manually, when they are not automatically discovered:
   - Click **Add** and enter the name of the NetBackup robotic drive you wish to add to the monitoring environment. Click **OK** to validate. Repeat the operation for each NetBackup robotic drive you want to monitor.
   - (Optional) Enter a short description that will allow you to quickly identify the added NetBackup robotic drive.
6. Click **OK** to validate.

Configuring NetBackup Robotic Libraries

By default, the solution monitors all the NetBackup robotic libraries discovered, which may represent an important workload for the Agents and the TrueSight servers. Because the monitoring of some NetBackup robotic libraries may be irrelevant for various reasons, you can apply filters to specify the NetBackup robotic libraries that will be monitored or discarded.

To configure NetBackup robotic libraries

1. From the **Add Monitoring Configuration** panel, select **NetBackup Robotic Library** from the **Monitor Type** list.
2. In the **NetBackup Robotic Library** panel, click **Add**.



NetBackup Robotic Library Settings (optional)

Hostname*

localhost

Filtering (automatically discovered)
Filtering
Keep Only Robotic Libraries
Add
Exclude Robotic Libraries
Add
Additional Robotic Libraries (manual discovery)
Manual Add
Additional Robotic Libraries
Add

Configuring NetBackup Robotic Libraries

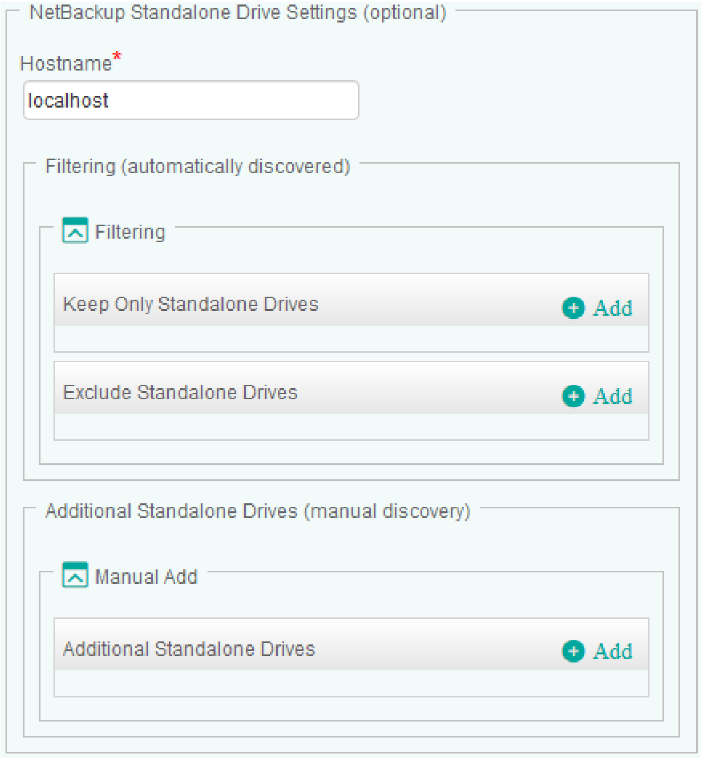
3. In the **Hostname** field, enter:
    - **localhost** to apply these settings to all PATROL Agents installed on NetBackup Servers
    - a **hostname** or **IP address** to apply these settings to a specific server.
4. Configure the **Filtering** options:
    - In the **Keep Only Robotic Libraries...** section, click **Add** and identify the NetBackup robotic library you wish to monitor. Enter the name of the NetBackup robotic library or identify it by using a regular expression (example: prod-library*). Click **OK** to validate. Repeat the operation for any other NetBackup robotic library you wish to include in the monitoring process.
    - In the **Exclude Robotic Libraries...** section, click **Add** and identify the NetBackup robotic library you do not want to monitor. Enter the name of the NetBackup robotic library or identify it by using a regular expression (example: test-library*). Click **OK** to validate. Repeat the operation for any other NetBackup robotic library you wish to exclude from the monitoring process.
5. The **Additional Robotic Libraries** (manual discovery) allows you to add NetBackup robotic libraries manually, when they are not automatically discovered:
    - Click **Add** and enter the name of the NetBackup robotic library you wish to add to the monitoring environment. Click **OK** to validate. Repeat the operation for each NetBackup robotic library you want to monitor.
    - (Optional) Enter a short description that will allow you to quickly identify the added NetBackup robotic library.
6. Click **OK** to validate.

Configuring NetBackup Standalone Drives

By default, the solution monitors all the NetBackup standalone drives discovered, which may represent an important workload for the Agents and the TrueSight servers. Because the monitoring of some NetBackup standalone drives may be irrelevant for various reasons, you can apply filters to specify the NetBackup standalone drives that will be monitored or discarded.

To configure NetBackup standalone drives

1. From the **Add Monitoring Configuration** panel, select **NetBackup Standalone Drive** from the **Monitor Type** list.
2. In the **NetBackup Standalone Drive** panel, click **Add**.



NetBackup Standalone Drive Settings (optional)

Hostname*: localhost

Filtering (automatically discovered)
Filtering
Keep Only Standalone Drives
Add
Exclude Standalone Drives
Add
Additional Standalone Drives (manual discovery)
Manual Add
Additional Standalone Drives
Add

Configuring NetBackup Standalone Drives

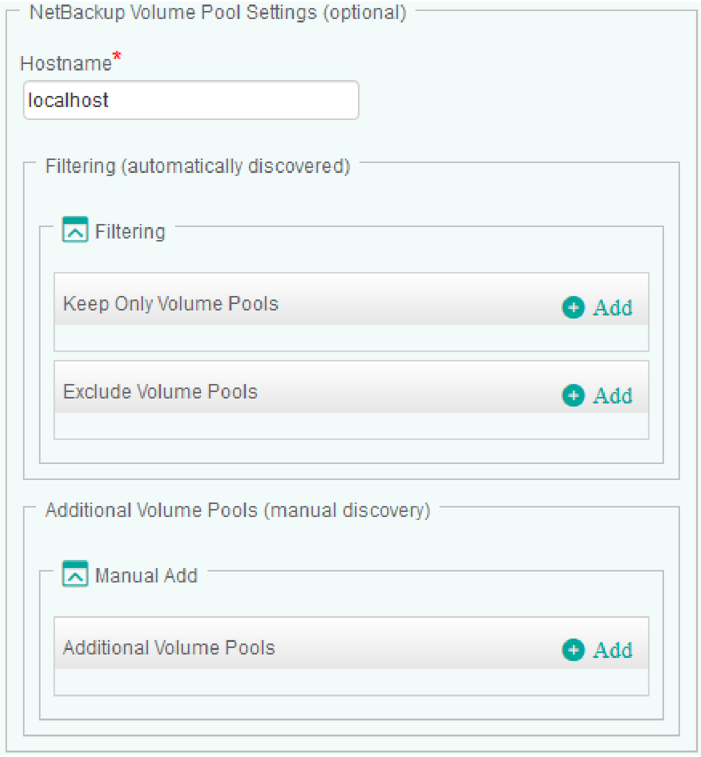
3. In the **Hostname** field, enter:
   - **localhost** to apply these settings to all PATROL Agents installed on NetBackup Servers
   - a **hostname** or **IP address** to apply these settings to a specific server.
4. Configure the **Filtering** options:
   - In the **Keep Only Standalone Drives...** section, click **Add** and identify the NetBackup standalone drive you wish to monitor. Enter the name of the NetBackup standalone drive or identify it by using a regular expression (example: prod-standalone*). Click **OK** to validate. Repeat the operation for any other NetBackup standalone drive you wish to include in the monitoring process.
   - In the **Exclude Standalone Drives...** section, click **Add** and identify the NetBackup standalone drive you do not want to monitor. Enter the name of the NetBackup standalone drive or identify it by using a regular expression (example: test-standalone*). Click **OK** to validate. Repeat the operation for any other NetBackup standalone drive you wish to exclude from the monitoring process.
5. The **Additional Standalone Drives** (manual discovery) allows you to add NetBackup standalone drives manually, when they are not automatically discovered:
   - Click **Add** and enter the name of the NetBackup standalone drive you wish to add to the monitoring environment. Click **OK** to validate. Repeat the operation for each NetBackup standalone drive you want to monitor.
   - (Optional) Enter a short description that will allow you to quickly identify the added NetBackup standalone drive.
6. Click **OK** to validate.

Configuring NetBackup Volume Pools

By default, the solution monitors all the NetBackup volume pools discovered, which may represent an important workload for the Agents and the TrueSight servers. Because the monitoring of some NetBackup volume pools may be irrelevant for various reasons, you can apply filters to specify the NetBackup volume pools that will be monitored or discarded.

To configure NetBackup volume pools

1. From the **Add Monitoring Configuration** panel, select **NetBackup Volume Pool** from the **Monitor Type** list.
2. In the **NetBackup Volume Pool** panel, click **Add**.



NetBackup Volume Pool Settings (optional)

Hostname*

localhost

Filtering (automatically discovered)

Filtering

Keep Only Volume Pools ⊕ Add

Exclude Volume Pools ⊕ Add

Additional Volume Pools (manual discovery)

Manual Add

Additional Volume Pools ⊕ Add

Configuring NetBackup Volume Pools

3. In the **Hostname** field, enter:
   - **localhost** to apply these settings to all PATROL Agents installed on NetBackup Servers
   - a **hostname** or **IP address** to apply these settings to a specific server.
4. Configure the **Filtering** options:
   - In the **Keep Only Volume Pools...** section, click **Add** and identify the NetBackup volume pool you wish to monitor. Enter the name of the NetBackup volume pool or identify it by using a regular expression (example: prod-volumepool*). Click **OK** to validate. Repeat the operation for any other NetBackup volume pool you wish to include in the monitoring process.
   - In the **Exclude Volume Pools...** section, click **Add** and identify the NetBackup volume pool you do not want to monitor. Enter the name of the NetBackup volume pool or identify it by using a regular expression (example: test-volumepool*). Click **OK** to validate. Repeat the operation for any other NetBackup volume pool you wish to exclude from the monitoring process.
5. The **Additional Volume Pools** (manual discovery) allows you to add NetBackup volume pool manually, when they are not automatically discovered:
   - Click **Add** and enter the name of the NetBackup volume pool you wish to add to the monitoring environment. Click **OK** to validate. Repeat the operation for each NetBackup volume pool you want to monitor.
   - (Optional) Enter a short description that will allow you to quickly identify the added NetBackup volume pool.
6. Click **OK** to validate.

Blocking the Monitoring of Hosts

The server owner/administrator may want to stop the monitoring of a remote NetBackup Node when performing maintenance work on this server. The monitoring can be blocked from the relevant NetBackup Node and will not require making any change from the monitoring PATROL Agent system(s). The administrator will just have to create a file named **NBU_block** under the **Remote Temp Directory Path**. By default, this path is set to **/var/tmp** (on UNIX/Linux) or **C:\Windows\Temp** (on Windows).

The PATROL Agent monitoring this NetBackup Node will detect the block file during the next discovery cycle and turn the node instance to **NetBackup Setup: <node-id> (Monitoring Blocked)**.

To resume monitoring, simply 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
- Veritas NetBackup 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: 🔑.

Veritas NetBackup KM

Attributes

Name	Description	Units	Recommended Alert Conditions	Type

Login Status	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.	0 = OK
		1 = Suspicious
		2 = Failure
			Warning = 1
			Alarm = 2
				Collection Status

Monitoring Mode	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.	0 = Permanent Single-node Mode 1 = Temporary Single-node Mode 2 = Active Multi-node Mode 3 = Passive Multi-node Mode -1 = Unknown	None	Collection Status

Name	Description	Units	Recommended Alert Conditions	Type

Node Status	Monitors error messages for the Veritas NetBackup application on this managed system. If the node is unreachable or If any of the Veritas NetBackup application daemons is not running, this parameter will be set to Failure state. If there are any suspicious command exits due to an error from the master/media server, this parameter will be set to Suspicious state.	0 = OK
		1 = Suspicious
		2 = Failure
			Warning = 1
			Alarm = 2
				Availability

NetBackup Client

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
State	Displays the state of the client as reported in the command executed by the data collector.	0 = Running 1 = Connection Refused 2 = Access Denied 3 = Client Down -1 = Unknown	None	Availability

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

Name	Description	Units	Recommended Alert Conditions	Type
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>/NBUClientCollectorWarn", 3600);	seconds	Warning: > preset value or observed maximum (default)	Collection Status

NetBackup Daemon

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
CPU Duration	Displays the CPU seconds consumed by the daemon.	seconds	None	Statistics
CPU Utilization🔑	Displays the percentage of CPU used by the daemon.	Percentage (%)	None	Statistics
Memory Size🔑	Displays the core image size of the daemon in the virtual memory.	Kilobytes (KB)	None	Statistics
Process Count 🔑	Displays the number of daemon processes/ threads found.	processes	None	Statistics
State	Displays the state of the daemon as reported in the command executed by the data collector.	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	None	Availability

Status	Monitors the status of the daemon. The following State to Status mapping rule is used:
	• Nonexistent/Not Responding > Failure
	• Not Running > Failure
		0 = OK
		1 = Suspicious
		2 = Failure
			Warning = 1
			Alarm = 2
				Availability

Name	Description	Units	Recommended Alert Conditions	Type
	- Terminated, Stopped, Disabled > Suspicious - Growing, Unknown > Suspicious - All other states > OK			

For detailed information about 🔑 *KPI*, see Managing Baselines and Key Performance Indicators.

NetBackup Daemons

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
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>/NBUDaemonCollectorWarn", 3600);	seconds	Warning: > preset value or observed maximum (default)	Collection Status

NetBackup Database

Attributes

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

For detailed information about 🔑 *KPI*, see Managing Baselines and Key Performance Indicators.

NetBackup Databases

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
Backup Elapsed 🔑	Displays the elapsed time since the last successful database backup.	hours	Alarm: -1 Warning: 24 and over	Statistics

Database Status	Monitors the status of the NetBackup database (NBDB)	0 = OK
		1 = Suspicious
		2 = Failure
			Warning = 1
			Alarm = 2
				Availability

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>/NBUDatabaseCollectorWarn", 3600);	seconds	Warning: > preset value or observed maximum (default)	Collection Status

For detailed information about 🔑 *KPI*, see Managing Baselines and Key Performance Indicators.

NetBackup Device

Attributes

Name	Description	Units	Default Alert Conditions	Type
State	Displays the state of the robotic drive. This is determined from the robotic drive control information.	0 = Idle 1 = Mounted 2 = In Use 3 = Pending 4 = Invalid 5 = Down 6 = Missing -1 = Unknown	None	Availability

Status	Monitors the status of the robotic drive. This status is determined by the robotic drive status mapping rule defined in the KM command **Configuration>Robotic Drive(s) Status**.
	
	If this status parameter changes to warning or alarm state, the recovery action will trigger an event and annotate the last data point.
		0 = OK
		1 = Suspicious
		2 = Failure
			Warning = 1
			Alarm = 2
				Availability

Throughput 🔑	Displays the throughput of the robotic 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 Devices

Attributes

Name	Description	Units	Default Alert Conditions	Type
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>/NBUDriveCollectorWarn", 3600);	seconds	Warning > preset value or observed maximum (default)	Collection Status

NetBackup Disk Pool

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
Up Down State	Displays the up/down state of the disk pool.	0 = Down 1 = Up -1 = Unknown	None	Availability

Up Down Status	Monitors the up/down status of the disk pool.	0 = OK
		1 = Suspicious
		2 = Failure
			Warning = 1
			Alarm = 2
				Availability

Volume Count 🔑	Displays the number of volumes in the disk pool.	count	None	Statistics

For detailed information 🔑 *KPI*, see Managing Baselines and Key Performance Indicators.

NetBackup Disk Volume

Attributes

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

Up Down Status	Monitors the up/down status of the disk volume.	0 = OK
		1 = Suspicious
		2 = Failure
			Warning = 1
			Alarm = 2
				Availability

Write Stream Count 🔑	Displays the number of current write steams for the disk volume	count	None	Statistics

For detailed information 🔑 *KPI*, see Managing Baselines and Key

NetBackup Disk Storage

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
Up Down State	Displays the up/down state of the storage.	0 = Down 1 = Up -1 = Unknown	None	Availability

Up Down Status	Monitors the up/down status of the storage.	0 = OK
		1 = Suspicious
		2 = Failure
			Warning = 1
			Alarm = 2
				Availability

NetBackup Disk Storages

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
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>/NBUStorageCollectorWarn", 3600);	seconds	Warning > preset value or observed maximum (default)	Collection Status

NetBackup Job

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
Duration	Displays the duration of the job from the start.	seconds	None	Statistics
File Count	Displays the number of files backed up for this job.	count	None	Statistics
Size	Displays the amount of data backed up for the job.	Megabytes (MB)	None	Statistics
State	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.	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	None	Availability

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
		0 = OK
		1 = Suspicious
		2 = Failure
			Warning = 1
			Alarm = 2
				Availability

Name	Description	Units	Recommended Alert Conditions	Type
	• Mounting for more than 60 minutes > Suspicious • In progress for more than 300 minutes > Suspicious • Requeued for more than 60 minutes > Suspicious • All other states > OK			
Throughput 🔑	Displays the throughput of this job.	Megabytes per second (MB/s)	None	Statistics

For detailed information about 🔑 *KPI*, see Managing Baselines and Key Performance Indicators.

NetBackup Jobs

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
Active Backup Count 🔑	Displays the number of active backup jobs currently discovered and monitored.	count	None	Statistics
Active Backup Reduction 🔑	Displays the reduction in number of active backup jobs since the last collection cycle.	count	None	Statistics
Active Count 🔑	Displays the number of active jobs currently discovered and monitored.	count	None	Statistics
Active Non-Backup Count 🔑	Displays the number of active non-backup jobs currently discovered and monitored.	count	None	Statistics
Exec Time	• This is a standard parameter which monitors the collector execution time.	seconds	Warning > preset value or observed maximum (default)	Collection Status

Name	Description	Units	Recommended 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>/NBUJobCollectorWarn", 3600);			
Queued Backup Count 🔑	Displays the number of backup jobs in "Queued" state.	count	None	Statistics
Queued Backup Reduction 🔑	Displays the reduction in number of queued backup jobs since the last collection cycle.	count	None	Statistics

For detailed information about 🔑 *KPI*, see Managing Baselines and Key Performance Indicators.

NetBackup Log

Attributes

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

For detailed information about 🔑 *KPI*, see Managing Baselines and Key Performance Indicators.

NetBackup Logs

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
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

Name	Description	Units	Default Alert Conditions	Type
State	Displays the state of the media server as reported in the command executed by the data collector.	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	None	Availability

Status	Monitors the status of the media server. The following State to Status mapping rule is used:
	• Not reachable by master > Failure
	• Not active for tape or disk jobs > Failure
	• Administrative pause > Suspicious
	• Unknown > Suspicious
	• All other states > OK
		0 = OK
		1 = Suspicious
		2 = Failure
			Warning = 1
			Alarm = 2
				Availability

NetBackup Media Servers

Attribute

Name	Description	Units	Default Alert Conditions	Type
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>/NBUMediaServerCollectorWarn", 3600);	seconds	Warning > preset value or observed maximum (default)	Collection Status

NetBackup Mount Request

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
Elapsed 🔑	Displays the elapsed time since the mount request was issued.	minutes	None	Statistics
State	Displays the state of the mount request as reported in the command executed by the data collector.	0 = Completed 1 = Pending -1 = Unknown	None	Availability

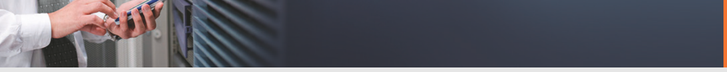
Status	Monitors the status of the mount request. The following State to Status mapping rule is used:
	• Pending for more than 30 minutes > Failure
	• Pending or Unknown > Suspicious
	• All other states > OK
		0 = OK
		1 = Suspicious
		2 = Failure
			Warning = 1
			Alarm = 2
				Availability

For detailed information about 🔑 *KPI*, see Managing Baselines and Key Performance Indicators.

NetBackup Mount Requests

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
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

Name	Description	Units	Recommended Alert Conditions	Type
Backup Elapsed 🔑	Displays the elapsed time since the last backup for this policy, regardless of completion status of the backup.	hours	None	Statistics
Backup Throughput 🔑	Displays the throughput of the last backup for this policy.	Gigabytes per second (GB/s)	None	Statistics
Full Backup Duration 🔑	Displays the duration of the last successful full backup for this policy.	seconds	None	Statistics
Full Backup Elapsed 🔑	Displays the elapsed time since the last successful full backup for this policy.	hours	None	Statistics
Full Backup File Count🔑	Displays the number of files backed up in the last successful full backup for this policy.	count	None	Statistics
Full Backup Size 🔑	Displays the size of the last successful full backup for this policy.	Gigabytes (GB)	None	Statistics
Incremental Backup Duration 🔑	Displays the duration of the last successful incremental backup for this policy.	seconds	None	Statistics
Incremental Backup Elapsed 🔑	Displays the elapsed time since the last successful incremental backup for this policy.	hours	None	Statistics
Incremental Backup File Count 🔑	Displays the number of files backed up in the last successful incremental backup for this policy.	count	None	Statistics

Name	Description	Units	Recommended Alert Conditions	Type
Incremental Backup Size 🔑	Displays the size of the last successful incremental backup for this policy.	Gigabytes (GB)	None	Statistics
State	Displays the state of the policy.	0 = Idle 1 = Running 2 = Running in Restricted Window 3 = Not started 4 = Inactive -1 = Unknown	None	Availability

Status	Monitors the status of the policy. The following State to Status mapping rule is used:
	• Running in Restricted Window > Failure
	• Running for more than 600 minutes > Suspicious
	• Unknown > Suspicious
	• All other states > OK.
		0 = OK
		1 = Suspicious
		2 = Failure
			Warning = 1
			Alarm = 2
				Availability

Successful Backup Elapsed 🔑	Displays the elapsed time since the last successful backup for this policy.	hours	None	Statistics

For detailed information about 🔑 *KPI*, see Managing Baselines and Key Performance Indicators.

NetBackup Policies

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
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>/NBUPolicyCollectorWarn", 3600);	seconds	Warning > preset value or observed maximum (default)	Collection Status

NetBackup Policy Client

Attributes

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

For detailed information about 🔑 *KPI*, see Managing Baselines and Key Performance Indicators.

NetBackup Robotic Drive

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
Drive Throughput 🔑	Displays the throughput of the robotic drive during the last backup activity.	Megabytes per second (MB/s)	None	Statistics
State	Displays the state of the robotic drive. This is determined from the robotic drive control information.	0 = Idle 1 = Mounted 2 = In Use 3 = Pending 4 = Down -1 = Unknown	None	Availability

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

Name	Description	Units	Recommended Alert Conditions	Type
Media Assigned Count 🔑	Displays the number of assigned media loaded in this robotic library. Assigned media are tape media assigned to a non-scratch volume pool.	count	None	Statistics
Media Available Count 🔑	Displays the number of media available to use in this robotic library. This includes unassigned and scratch media.	count	None	Statistics
Media Available Percent 🔑	Monitors the percentage of available media against the total number of media loaded in this robotic library.	Percentage (%)	Warning: between 2 and 5 Alarm: 2 or less	Statistics
Media Cleaning Left 🔑	Monitors the number of cleaning left on the cleaning media available in this robotic library.	count	Warning: 2 or less Alarm: 0	Statistics
Media Count 🔑	Displays the total number of media loaded in this robotic library.	count	None	Statistics
Media Scratch Count 🔑	Displays the number of scratch media loaded in this robotic library. (Scratch media are tape media assigned to the scratch volume pool.)	count	None	Statistics

Name	Description	Units	Recommended Alert Conditions	Type
Media Scratch Percent 🔑	Monitors the percentage of scratch media against the total number of media loaded in this robotic library.	Percentage (%)	None	Statistics
Media Unassigned Count 🔑	Displays the number of unassigned media loaded in this robotic library. (Unassigned media are tape media not assigned to a volume pool.)	count	None	Statistics
Media Unassigned Percent 🔑	Monitors the percentage of unassigned media against the total number of media loaded in this robotic library.	Percentage (%)	None	Statistics
State	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.	0 = Online 1 = Remote 2 = Offline 3 = Invalid -1 = Unknown	None	Availability

Status	Monitors the status of the robotic library.	0 = OK
		1 = Suspicious
		2 = Failure
			Warning = 1
			Alarm = 2
				Availability

Throughput	Displays the total throughput of each robotic library drive during the last backup activities within the last hour.	Megabytes per second (MB/s)	None	Statistics
Up Drive Count	Displays the number of up / online state drives in this robotic library.	count	None	Statistics

For detailed information about 🔑 *KPI*, see Managing Baselines and Key

NetBackup Robotic Libraries

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
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>/NBULibraryCollectorWarn", 3600);	seconds	Warning > preset value or observed maximum (default)	Collection Status

NetBackup Standalone Drive

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
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

Name	Description	Units	Recommended Alert Conditions	Type
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>/NBUDriveCollectorWarn", 3600);	seconds	Warning > preset value or observed maximum (default)	Collection Status

NetBackup Volume Pool

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
Media Active Count 🔑	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.)	count	None	Statistics
Media Active Percent 🔑	Monitors the percentage of active media against the total number of media in this volume pool.	Percentage (%)	Warning between 2 and 5 Alarm when < 2	Statistics
Media Count 🔑	Displays the total number of media in this volume pool.	count	None	Statistics
Media Frozen Count 🔑	Displays the number of frozen media in this volume pool. Frozen is a possible status for a tape media.	count	None	Statistics
Media Full Count 🔑	Displays the number of full media in this volume pool. Full is a possible status for a tape media.	count	None	Statistics
Media Full Percent 🔑	Monitors the percentage of full media against the total number of media in this volume pool.	Percentage (%)	Warning: between 95 and 98 Alarm: 98 and over	Statistics
Media Loaded Count 🔑	Displays the number of media in this volume pool, currently loaded to a robotic library.	count	None	Statistics

Name	Description	Units	Recommended Alert Conditions	Type
Media Loaded Empty Count🔑	Displays the number of empty media in this volume pool, currently loaded to a robotic library.	count	None	Statistics
Media Loaded Empty Percent🔑	Monitors the percentage of empty media against the total number of empty media in this volume pool.	Percentage (%)	Warning:2-5 Alarm:0-2	Statistics
Media ReadOnly Count 🔑	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.	count	None	Statistics
Media Scratch Count 🔑	Displays the number of scratch media in this volume pool. The parameter is visible and set only for scratch volume pools.	count	Warning when < 2 Alarm = 0	Statistics
Media Suspended Count 🔑	Displays the number of suspended media in this volume pool. Suspended is a possible status for a tape media.	count	None	Statistics
Media Unassigned Count 🔑	Displays the number of media in unassigned state in this volume pool.	count	None	Statistics
Media Unassigned Percent 🔑	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.	Percentage (%)	None	Statistics

Name	Description	Units	Recommended Alert Conditions	Type
Media Unknown Count 🔑	Displays the number of media in unknown state in this volume pool.	count	None	Statistics
Space Available	Monitors the available media space for the backup data to use amongst the assigned media in this volume pool.	Gigabytes (GB)	None	Availability
Space Growth Rate	Displays the growth rate of the total media space used by the backup data in this volume pool.	Gigabytes per second (GB/s)	None	Statistics
Space Used 🔑	Displays the total media space occupied by the backup data in this volume pool.	Gigabytes (GB)	None	Statistics
Space Used Percent 🔑	Monitors the percentage of total occupied media space against the total media capacity of this volume pool (not including any scratch media).	Percentage (%)	Warning: between 95 and 98 Alarm: 98 and over	Statistics

For detailed information about 🔑 *KPI*, see Managing Baselines and Key Performance Indicators.

NetBackup Volume Pools

Attributes

Name	Description	Units	Recommended Alert Conditions	Type
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>/NBUPoolCollectorWarn", 3600);	seconds	Warning > preset value or observed maximum (default)	Collection Status

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

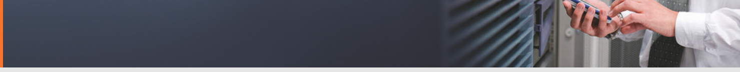
The baseline is the expected normal operating range for an attribute of a monitor. There are two baselines: **Baseline High** and **Baseline Low**. **Baseline High** represents the point at which 95% of the weighted average of the historical values fall below this value for the selected time period;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

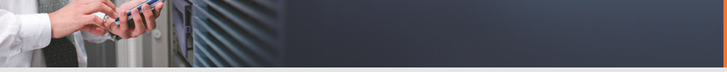
Managing Key Performance Indicators

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.*



Index



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.

The combination of its monitoring, automation, and capacity optimization capabilities for IT

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.

ABOUT MARKETZONE DIRECT PRODUCTS

BMC SOFTWARE VALIDATED MARKETZONE

The BMC MarketZone Direct program sells and supports third-party products that complement and/or augment BMC solutions. MarketZone Direct products are available under BMC license and support terms.

BUSINESS RUNS ON I.T.
I.T. RUNS ON BMC SOFTWARE

Business thrives when IT runs smarter, faster and stronger. That's why the most demanding IT organizations in the world rely on BMC Software across distributed, mainframe, virtual and cloud environments. Recognized as the leader in Business Service Management, BMC offers a comprehensive approach and unified platform that helps IT organizations cut cost, reduce risk and drive business profit. For the four fiscal quarters ended September 30,2011, BMC revenue was approximately $2.2 billion.

LEARN MORE

To learn more about our solutions, please visit : www.sentrysoftware.com/solutions

Like us on Facebook: facebook.com/sentrysoftware

Follow us on Twitter: twitter.com/sentrysoftware