

*Version 22*

**Reporting Guide**

Contents

[Introduction 5](#_Toc558758160)

[Modules 5](#_Toc1778987288)

[Home 6](#_Toc581388451)

[Backup Activity 7](#_Toc592818835)

[Backup Failure 8](#_Toc2081778255)

[Storage Monitoring 9](#_Toc1341629473)

[Storage Monitoring > Data Domain 10](#_Toc1640973100)

[Storage Monitoring > Store Once 11](#_Toc980505444)

[Normalized Asset Inventory Reporting 12](#_Toc222859819)

[Unprotected Inventory 12](#_Toc1001810042)

[Protected Inventory 12](#_Toc1587923276)

[Protected Non-Inventory 12](#_Toc560903358)

[All Assets 12](#_Toc602262461)

[Advanced > Policies 12](#_Toc331370051)

[Advanced > SLA 14](#_Toc1255404428)

[Configuration 16](#_Toc1046860444)

[Administration 16](#_Toc1867385826)

[Report Features 17](#_Toc846096821)

[Report Criteria 17](#_Toc1593180652)

[Criteria Definitions: 18](#_Toc634085824)

[18](#_Toc1014143476)

[18](#_Toc1352168158)

[19](#_Toc1321914395)

[19](#_Toc2138080954)

[19](#_Toc619128858)

[19](#_Toc116203419)

[19](#_Toc1060364819)

[19](#_Toc1877803746)

[19](#_Toc253577670)

[19](#_Toc334546927)

[19](#_Toc1429342325)

[19](#_Toc2041606037)

[20](#_Toc480011902)

[21](#_Toc2053989849)

[21](#_Toc385100795)

[22](#_Toc913476538)

[22](#_Toc1848699992)

[22](#_Toc29005687)

[22](#_Toc2066983762)

[22](#_Toc279378818)

[22](#_Toc352396456)

[22](#_Toc994389728)

[22](#_Toc301278123)

[22](#_Toc701903583)

[22](#_Toc453490414)

[22](#_Toc1088799670)

[22](#_Toc826700473)

[22](#_Toc1023766653)

[22](#_Toc562482522)

[22](#_Toc1903728021)

[22](#_Toc1942468999)

[22](#_Toc1093438437)

[23](#_Toc1297552707)

[23](#_Toc1985039646)

[23](#_Toc2022485375)

[23](#_Toc1167017762)

[23](#_Toc1678508327)

[23](#_Toc652295491)

[23](#_Toc1698599405)

[23](#_Toc130787122)

[23](#_Toc509435293)

[23](#_Toc201275006)

[23](#_Toc439360890)

[Saving Criteria 23](#_Toc148143163)

[Action Panel Functions 24](#_Toc330138807)

[25](#_Toc478221749)

[Exporting and Emailing 31](#_Toc2022879786)

[Tabular Grouping 32](#_Toc1403840797)

[Tabular Filtering 32](#_Toc2015412184)

[Tabular Column Selection 32](#_Toc1707008199)

[Custom Failure Icon 33](#_Toc2097453557)

[Detailed Report Explanations 35](#_Toc486970618)

[Alert Config 35](#_Toc2114071038)

[Annotations 38](#_Toc1761309239)

[Job Activity 38](#_Toc495377220)

[Backup Alert Activity 39](#_Toc511855962)

[Backup Duration Trends 40](#_Toc248719906)

[Backup Error Trends 40](#_Toc78865238)

[Backup Failures 41](#_Toc1372019647)

[Backup Health 42](#_Toc1116217605)

[Backup Health Trends 43](#_Toc2064684190)

[Backup Server Activity 43](#_Toc1486273029)

[Backup Servers 44](#_Toc1658215623)

[Backup Trends 46](#_Toc2117395190)

[Backup Trends Details 47](#_Toc1079610475)

[Storage Servers 47](#_Toc1345076010)

[Storage Clients 48](#_Toc777365574)

[Storage Trends 48](#_Toc1046954102)

[Storage Trends Tabular 49](#_Toc1099506661)

[Change Analysis (NBU / Spectrum Protect) 49](#_Toc1242900511)

[Chargeback 49](#_Toc846162093)

[Cohesity Storage Domains 50](#_Toc1248539211)

[Consecutive Failures 50](#_Toc1595112333)

[Executive Summary Report 51](#_Toc1683010283)

[In Progress Job Trends 51](#_Toc1115989837)

[In Progress Jobs 52](#_Toc74492625)

[Job Trends 53](#_Toc226710232)

[NBU Clients 54](#_Toc984396741)

[NBU Configuration 54](#_Toc939563219)

[NBU Lifecycle 54](#_Toc112059473)

[NBU SLP Trends 54](#_Toc1497941556)

[NBU SLP Configuration 54](#_Toc1617684373)

[Orphaned Clients 54](#_Toc428918479)

[Policy Configuration 55](#_Toc1646028610)

[Policy Clients 55](#_Toc346233339)

[Azure / DPM Recovery Point Status 56](#_Toc558260994)

[Azure DPM Recovery Point Summary 56](#_Toc179801374)

[Restore Activity 57](#_Toc2064909322)

[Restore Failures 57](#_Toc861337700)

[Restore Health 58](#_Toc867194508)

[Saved Reports 58](#_Toc2019585744)

[Schedules 60](#_Toc1607899533)

[Scheduled Actions 61](#_Toc1402755009)

[Scheduled Report Management 61](#_Toc2029059758)

[SLA Config 61](#_Toc570073227)

[SLA Impacts 64](#_Toc1786468452)

[SLA Metrics 64](#_Toc1983918810)

[SLA Trends 64](#_Toc1629529824)

[Summary (Dashboard) 64](#_Toc755773979)

[Spectrum Protect Filespaces 65](#_Toc1738948213)

[Spectrum Protect Clients 65](#_Toc714856436)

[Spectrum Protect Configuration 66](#_Toc774832650)

[VM Protection Analysis 67](#_Toc1813232656)

[67](#_Toc263549989)

[Support 68](#_Toc1169593547)

[Bocada Customer Support 68](#_Toc1927632797)

[Bocada Professional Services 68](#_Toc1885170061)

[Appendix A: Reporting Module Access 69](#_Toc433731676)

[Storage 70](#_Toc140502841)

[vCenter 70](#_Toc2010145721)

[Policies 71](#_Toc886979139)

[SLA 71](#_Toc1618858082)

[Operations 72](#_Toc1759516592)

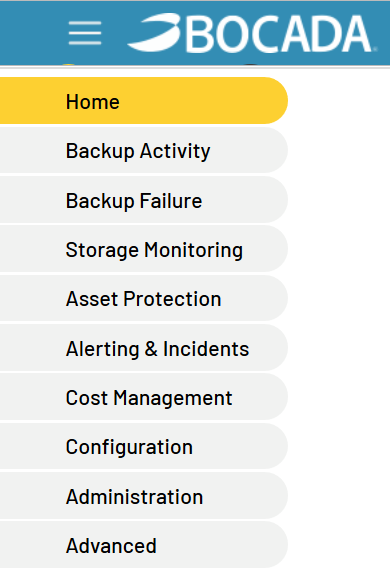
[Administration 73](#_Toc2031561425)

# Introduction

This Reporting Guide is intended for users who report on their data protection environment using Bocada. Administrative functionality documentation can be found in the *Administration Guide*.

# Modules

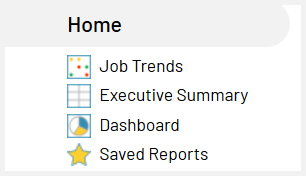
Bocada is divided into modules. These modules are found in the left column of the Bocada window, and each module can be expanded by selecting the module name. Under each module are that module’s report views, as well as any sub-modules.



Below is a brief synopsis of the reports contained within each module; greater detail can be found in the [Detailed Report Explanations](#_Detailed_Report_Explanations) section of this guide.

## Home

The Home module provides immediate visibility into recent and long-term operation of the environment, with Job Trends analysis to determine inconsistencies in backup performance and opportunities for improvement. Use the Executive Summary report to get a view of the overall backup environment at a glance.



#### Job Trends

*Job Trends* displays the daily successful, failed, and partially successful backup jobs. This report can be grouped up to four levels and is grouped by Backup Server/Client/Target by default.

#### Executive Summary

*Executive Summary* rolls up a variety of backup statistics across you chosen time period, serving as an assessment of a backup environment for measures such as amount of data backed up, number of backup servers and clients in the environment, and percent of successful backup jobs.

#### Dashboard

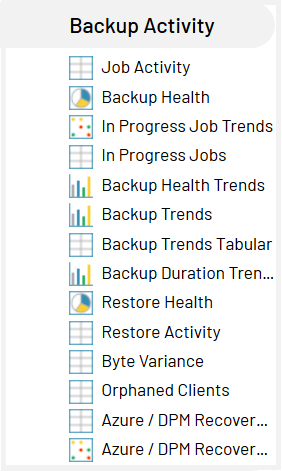
*Dashboard* provides an overview of the backup environment by displaying up to four graphical reports in one window.

#### Saved Reports

*Saved Reports* is a central interface for and running and managing reports with previously saved criteria. Reports that are saved can also be accessed via the folder icon from each report. You can see your default report of each type, although you cannot edit that attribute here.

## Backup Activity

The Backup Activity section includes the reports seen in this screenshot:



#### Job Activity

*Job Activity* lists backup attempts matching selected criteria over configurable periods of time.

#### Backup Health

*Backup Health* displays the percent of backups by status of successful, partially successful, and failed, in the form of a pie chart. Clicking on a section of the pie will take users to the related granular job details in Job Activity.

#### In Progress Job Trends

*In-Progress Job Trends* displays the next-future, currently-running, pending, successful, failed, and partially successful backup jobs. This report can be grouped up to four levels and is grouped by Backup Server/Client by default.

#### In Progress Jobs

*In-Progress Jobs* displays the currently-running, pending, and next-future jobs matching the selected criteria.

#### Backup Health Trends

*Backup Health Trends* displays the trend over time of backups that are successful, partially successful, and failed, in the form of a bar chart. Clicking on a section of a bar will take users to the related job details.

#### Backup Trends

*Backup Trends* displays the trend over time of bytes transferred for a variety of objects including backup servers, backup clients, and assets. Clicking on a bar will display the details contributing to the byte count for that period. See Backup Trends Details for a non-graphical version of this report

#### Backup Trends Details

*Backup Trends Details* displays the same data as in the Backup Trends graphical report: the trend over time of bytes transferred for a variety of objects including backup servers, backup clients, and assets.

#### Backup Duration Trends

*Backup Duration Trends* displays the backup jobs within each unit of time (defaults to Servers per Day) to show the length of time those jobs are running, in the form of a bar chart. Clicking on a section of the bar will take users to the related granular job details.

#### Restore Health

*Restore Health* shows the percent of restores that are successful, partially successful, and failed, in the form of a pie chart. Clicking on a section of the pie will take users to the related granular job details in Restore Activity.

#### Restore Activity

*Restore Activity* lists restore attempts matching selected criteria over configurable periods of time.

#### Orphaned Clients

*Orphaned Clients* is a depreciated feature.

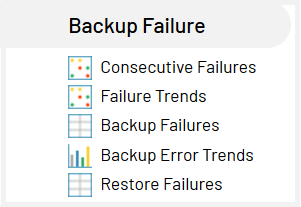
#### Azure / DPM Recovery Point Summary

*Azure / DPM Recovery Point Summary* displays the status of Microsoft Azure and Data Protection Manager (DPM) recovery points including whether each recovery point is expired. This report can be grouped up to four levels and is grouped by Server/Client/Target by default.

#### Azure / DPM Recovery Point Status

*Azure / DPM Recovery Point Status* displays recovery point information for each target protected by MS Azure or DPM.

## Backup Failure



#### Consecutive Failures

*Consecutive Failures* highlights the daily backup jobs for targets which have failed for a defined number of consecutive days since the most recent success. This report can be grouped up to four levels and is grouped by Server/Client/Target by default.

#### Failure Trends

A subset of the *Job Trends* report, *Failure Trends* displays failed (and partially failed) backup jobs as they trend over a period of time. While *Job Trends* displays all data specified in the criteria regardless of success, *Failure Trends* displays only data for which there were failures, thus filtering out rows that completely successful over that time. This report can be grouped up to four levels and is grouped by Backup Server/Client/Target by default.

The report will not show current backup day when using:

\* Show No Attempts as Failures + last X days or week/month-to-day

#### Backup Failures

*Backup Failures* is a subset of Job Activity that displays only failed and partially successful backups.

#### Backup Error Trends

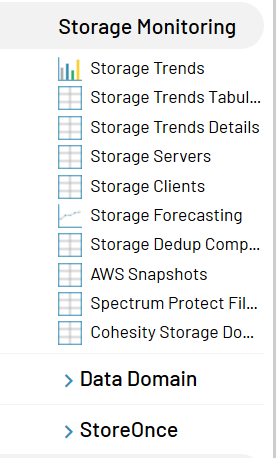
*Backup Error Trends* displays the trend over time of backup error count for selected criteria and drill down functionality for a granular view of errors.

#### Restore Failures

*Restore Failures* is a subset of Restore Activity that displays only failed and partially successful restores.

## Storage Monitoring

Note: Storage reporting is only available for products which can collect Storage data. See the Backup Product Plug-in Guides or Backup Product Version Support Matrix for details on which types of data collection are possible.



#### Storage Trends

*Storage Trends* displays the amount of unexpired data that is available for restore, trended over time. Clicking on a bar will display the details contributing to the byte count for that period.

#### Storage Trends Tabular

Tabular version of the data seen in the *Storage Trends* report.

#### Storage Servers

*Storage Servers* displays the Storage data by Media Library and Media Pool for each backup server.

#### Storage Clients

*Storage Clients* displays the Storage data by Media Library and Media Pool for each client server of each backup server.

#### Storage Dedup Compression

*Capacity Dedup Compression* provides a tabular report of the media capacity saved through compression and deduplication for each media pool.

#### AWS Snapshots

*This report is documented in the Bocada AWS Backup Plugin Configuration Guide*.

#### Spectrum Protect Filespaces

*Spectrum Protect Filespaces* displays how much data is protected on Spectrum Protect clients according to the Spectrum Protect Filespace table, by node, by filespace name, and by storage pool name.

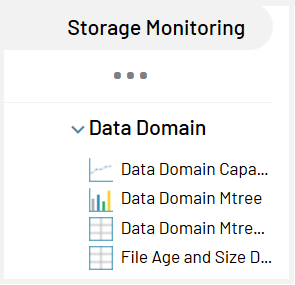
#### Cohesity Storage Domains

#### *Cohesity Storage Domains* provides a tabular report of storage capacity and storage capacity usage for Cohesity’s storage domains.

#### Data Domain Capacity

*Data Domain Capacity* is a line chart (2D or 3D) which displays the total Data Capacity, the Data Used Capacity, the Data Cleanable Capacity, and the Data Free Capacity of your Data Domains over time.

### Storage Monitoring > Data Domain



Data Domain dedicated reports are documented in the *Bocada Data Domain*

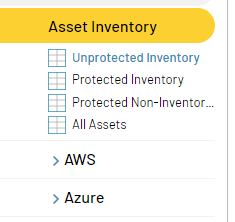
*Plugin Configuration Guide*.

### Storage Monitoring > Store Once



StoreOnce reporting is for this specific type of storage device.

## Normalized Asset Inventory Reporting



At the top of the Asset Inventory section of the left navigation panel there are four reports that represent normalized datasets of all Asset inventory accounted for by Bocada Reporting.

An "Asset" is typically a backup client-level item that may be protected. Some examples are various standalone computers / endpoints, servers of various types including as email or database servers, and VMs of various types, such as vCenter, Azure, or AWS machines.

The purpose of the top four reports in the Asset inventory is to pull together all "Assets" into four different sets of data.

Unprotected Inventoryincludes only Assets from an inventory system such as CMDB but for which no matching backup client is found in Bocada.

Protected Inventory includes Assets that are in an inventory system such as CMDB and also have a backup associated with the Asset in the Bocada backup datasets.

Protected Non-Inventory is any Asset in Bocada that is protected and not matched to an Asset in an inventory system.

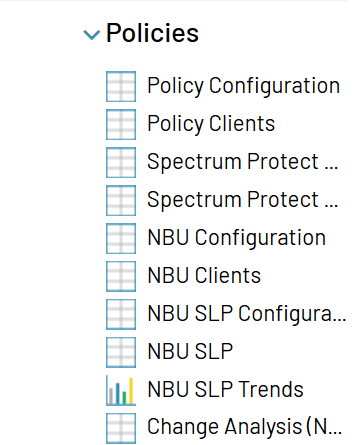
All Assets is the list of all normalized Assets that has been collected by Bocada, either from an inventory source like CMDB or from a backup server.

## Advanced > Policies

The Policy module enables all users to automatically view current policies and schedules, and periodically update users of any changes made to an existing policy so that they can review the impact of that policy change as it applies to overall backup success rates. The Policy Module enables all users to easily view information on numerous aspects of server and policy configuration, including schedules, storage, client details, and job and capacity trends. The Change Analysis feature automatically tracks changes in policies and shows the impact of any policy changes on backup performance and SLAs.

Policy reporting differs for each data protection application; Symantec NetBackup (NBU) and IBM Spectrum Protect (TSM) each have dedicated policy reports.

Note: Policy reporting is only available for products which can collect Policy data. See the Backup Product Plug-in Guides for details on which types of data collection are possible.



#### Policy Configuration

*Policy Configuration* displays backup configurations (policy) details for backup products supported with Bocada policy updates. Spectrum Protect and NBU policy information is contained in separate reports, and is not included in this report.

#### Policy Clients

*Policy Clients* displays backup clients assigned to policies for backup products supported with Bocada policy updates. Spectrum Protect and NBU policy information is contained in separate reports, and is not included in this report.

#### Spectrum Protect Configuration

*Spectrum Protect Configuration* displays details of Spectrum Protect policies.

#### Spectrum Protect Clients

*Spectrum Protect Clients* lists backup clients assigned to Spectrum Protect policies, along with related client details.

#### NBU Configuration

*NBU Configuration* displays details of the policy configurations of each NBU server, including what policies are configured, type of policy, storage devices associated, etc.

(Note: Policy Type includes an internal type identifier in parenthesis, not to be confused with quantity.)

#### NBU Clients

*NBU Clients* lists backup clients assigned to NBU policies along with related client details, whether a policy is active or inactive, if a client is assigned to more than one policy (i.e. is being backed up redundantly, the report will show one row for each policy the client is assigned), etc. Client versions and protected assets can also be viewed within this report.

#### NBU SLP Configuration

Specific to NBU, Storage Lifecycle Policies (SLP) reports provide a centralized view of vaulting and SLPs, including the ability to identify SLP-initiated backup jobs and their destination media to verify that backup copies were successful. *NBU SLP Configuration* displays a list of NBU SLPs along with a detail of each one when selected.

#### NBU SLP

*NBU SLP* displays the daily successful, failed or partially successful results of NBU lifecycle activities. This report is grouped to four levels and by Backup Server/Policy/Client/Schedule.

#### NBU SLP Trends

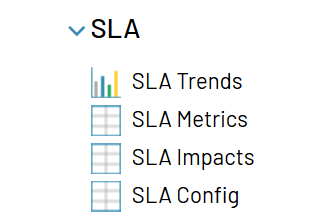
*NBU SLP Trends* shows the daily trend of successful, failed and partially successful results of NBU SLP Policies in the form of a bar chart. Clicking on a bar will display the *NBU SLP* report for the day clicked.

#### Change Analysis (NBU / Spectrum Protect)

*Change Analysis* highlights the changes to individual NBU or Spectrum Protect policies over time.

## Advanced > SLA

The SLA Module enables users to easily track SLA performance and share results with internal or external customers via the web. Bocada enables configuration of SLA profiles based on the needs of your business. Bocada delivers proactive SLA impact reports, showing how SLAs will be affected by policy or infrastructure changes, and SLA trending reports, giving administrators different views of their SLAs by zones, applications, clients and more. The SLA metrics report reveals which SLAs are and are not being met, and why.



#### SLA Trends

*SLA Trends* provides a bar trend report of the SLA compliance over a designated period of time, showing what percentage of jobs associated with an SLA fall within each SLA status (Met SLA, Did Not Meet SLA, and No Backup Attempts Yet). Click on each bar to drill into the related SLA Metrics report.

#### SLA Metrics

*SLA Metrics* displays a report of jobs for all clients associated with an SLA (as defined in Manage SLAs), and how well those SLAs are being fulfilled, showing which SLAs are being met, which are not, and identifying where the problem is within the data protection infrastructure.

#### SLA Impacts

*SLA Impacts* provides an overview of how SLAs will affected be by policy or infrastructure changes.

#### SLA Config

*SLA Config* allows Administrators to establish and edit SLA Profiles. Once configured here, SLA Profiles may be assigned to clients, prior to running SLA Compliance Reports.

## Configuration

Configuration views are for adding, managing and configuring the backup servers, clients, Scheduled Actions, etc. These functions are covered in the Bocada Administration Guide.

## Administration

The Administration module is only available to Bocada Administrators and is documented in the *Bocada Administration Guide*.

# Report Features

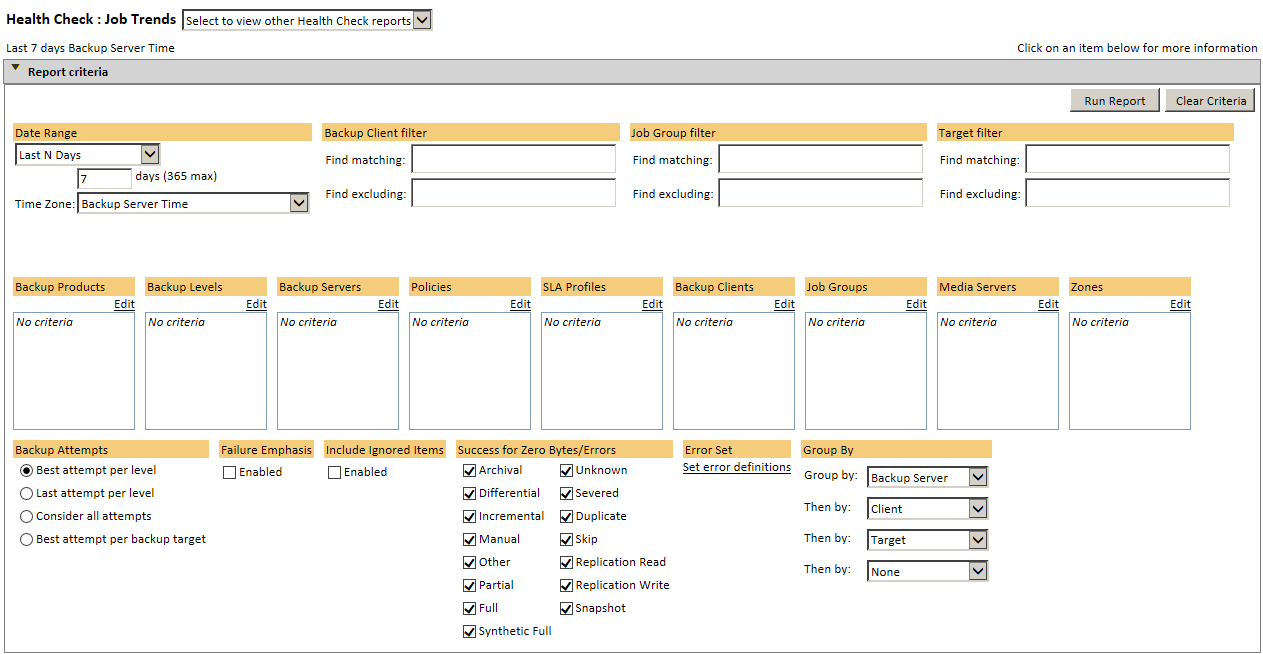
## Report Criteria

Each report can be edited to filter on specific criteria such as date range, client name, and backup application, etc. Criteria wizards allow for multiple criteria to be chosen to customize the report view.

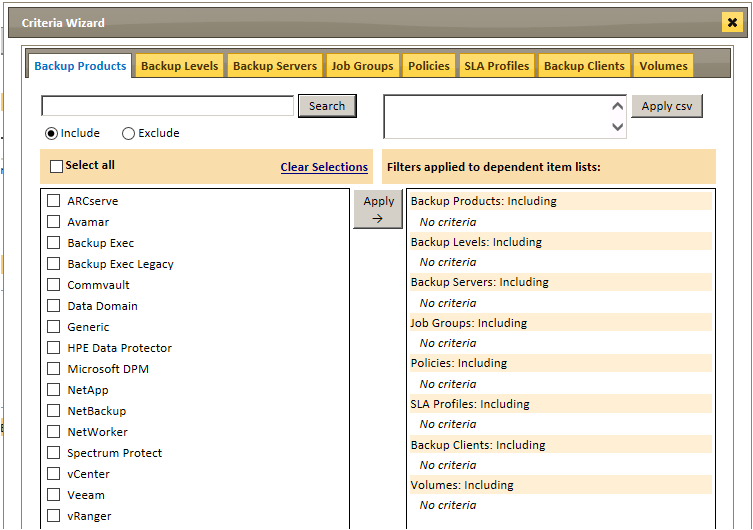
All reports have a *Report Criteria* menu in the header of the report (except dashboard views). Choosing Report Criteria will expand a wizard/dialog screen that allows the user to choose from a broad selection of criteria for filtering the report view; select the triangle or *Report Criteria* to expand the criteria menu for each report.

Closed (default):  Open: 

For example, here are the expanded report criteria in a *Health Check: Job Trends* report:



Note that many Criteria fields include both a text box to display current criteria and an Edit link to launch the Criteria Wizard:



Each tab within the wizard represents a criteria option; criteria appearing for each report are those relevant to that report type. They also only show related data to users based on the role and zoning permissions set in the Administration Users view.

Within the Criteria Wizard, it is possible to Search for criteria to include or exclude. The Search function allows use of the wildcard character \* so that, in the above example, a filter of \*Exec\* here would include (or exclude) both Backup Exec and Backup Exec Legacy. Exclude filters take precedence over Include filters. For example, including \*Backup\* and excluding \*Exec\* would result in only NetBackup, above.

A comma-separated list of values may also be entered in the text box and used as criteria by clicking the *Apply csv* button at top right.

Criteria used in reports can be saved by using the Save Report feature. The reports will now show up under the Saved Reports heading on the left navigation panel.

## Criteria Definitions:

Assets – The protected resource, also known as Targets, selections and sources. The criteria Assets lists all assets (backup targets) filtered by user role and zoned by client.

Backup Attempts – The criteria Backup Attempts is a multiple selection criteria. The options are:

* Best Attempt per Level – this option will evaluate all jobs per backup target and select the best outcome (most recent, most successful) attempt per asset per level per selected period (see Date Range, below) to display. The best attempt considers backup window, byte count, number of errors, and status. Note that this setting is per Level, therefore Full backup outcomes, for instance, are evaluated separately from Incremental backups for the same target.
* Last Attempt per Level – this option will only display the most recent backup attempt per asset per level per selected period.
* Consider all attempts – this option will consider all backup attempts per asset per selected period.
* Best Attempt per Backup Target Level – As with Best Attempt per Level, above, this option will evaluate all jobs per backup target and select the best outcome (most recent, most successful) attempt per asset per selected period, regardless of level. This option allows, for instance, a successful full backup for a target to override a previously failed partial backup.

Backup Clients – Usually a computer that is backed up by the backup server. All clients that meet the other criteria will be shown or you can filter the clients to include fewer in the report. Reports may also include text-boxes to filter the report by including or excluding Client names that match strings.

Backup Group Filter –This is used to select Job Group(s) matching a given string. Backup Group Filter supports wild cards (\*,%).

Backup Servers – Machine that is responsible for scheduling and running the data protection software. Lists backup servers that are configured for data collection.

Backup Products – The name of data protection software as configured for data collection. Lists backup products that are supported by the report.

Backup Levels – The level of the backup. Currently, Bocada reports include: Archival, Differential, Duplicate, Full, Incremental, Other, Replication Read, Replication Write, Synthetic Full, and Unknown.

Bar Style – Bar Style is used for bar reports to determine bar appearance. This can be set to either 2D stacked, 2D side-by-side, or 3D stacked.

Client Filter – This is used to select client(s) matching a given string. Client Filter supports wild cards (\*,%).

Data Center – Used to organize an aggregation of all the different objects needed to do work in a virtual infrastructure. Lists Data Centers collected from the Virtual Manager (vCenter).

Datastores – Representation of the physical storage of a data center. Lists data stores configured in the Virtual Manager and assigned to the Host servers.

Date Range – The Date Range criteria has the following options:

* **Current Backup day** – the current backup date displays data over the range determined by the administrative setting for the backup day.
* **Current week-to-day** – the current week to day starts on Monday at the beginning of the backup day.
* **Current month-to-day** - the current month to day starts on the 1st day of the month at the beginning of the backup day.
* **Last N Days** – Last N Days can be set to the number of days back from the time the report is run. The maximum number of days to go back is 45 days.
* **Last N Hours** – Last N hours can be set to the number of hours from the time the report is run. The maximum number of hours to go back is 72 hours.
* **Custom Date Range** – the custom date range allows users to select a range of dates. There is no limit to the number of dates that can be viewed.
* **Time Zone** – the time zone specified will determine when each day in the report begins or ends. Defaults to Backup Server Time, but may be changed if the report is needed in a different time zone than the one the server is in.

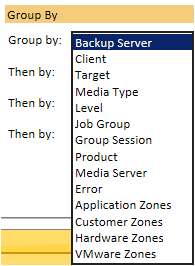
Error Sets – The criteria Error Sets pulls up a list of error definitions. These are an aggregation of data protection application error codes to one of sixteen normalized error sets (definitions). This criteria setting allows a user to determine if certain errors (example: File I/O error) should be ignored (green), normal, or a failure (red). By adjusting error sensitivity, reports can be created that reflect the organization’s backup policies.

Each error definition can be set on a per-report or global basis. If a user sets error sensitivity for a specific report (for example, Backup Trends) and saves that report with a specific name, the error sensitivity settings from the named report are not applied to any new Backup Trends reports. A user can configure the default error sensitivity settings. These default settings determine the initial settings that are applied to newly-created reports.

|  |  |
| --- | --- |
| **Error Set Category** | **Example of Error Type** |
| Aborted Backup Error (1) | Backup job was manually stopped by a user/operator. |
| Backup Configuration Error (2) | Installation or configuration of the backup product, either on the server or the client, resulted in an error (for example a missing client agent). |
| Backup File Busy Error (3) | File was in use during the backup job. |
| Backup File Corrupt Error (4) | Either a file changed while it was being saved to media (timestamp error), or the backup server detected a virus (infected file). |
| File I/O Error (5) | Server encountered an I/O error while reading a file (e.g. a client's hard disk crashed during the backup job). |
| Backup File Locked Error (6) | File was locked by another application during the backup job. |
| Backup File Permission Error (7) | Backup server had insufficient permissions to access a file (e.g. did not have read access). |
| Backup File Verification Error (8) | Files backup copy differed from its source (e.g. the file changed since backup). |
| Backup Group Error (9) | An error was recorded within this targets’ Job Group. |
| Backup Media Unavailable Error (10) | No writable media was available for this backup job (for example, all tapes belonged to the wrong media pool). |
| Backup Media I/O Error (11) | Storage device encountered an error while writing the backup job to media (e.g. insufficient free storage space on disk or tape). |
| Backup Network Error (12) | Network connectivity error occurred during the backup job (e.g. a client was unavailable). |
| Backup Software Error (13) | Backup software failed to operate property (e.g. the server encountered an access violation). |
| Backup Time-out Error (14 | Backup job was automatically terminated because it exceeded the expected amount of time (e.g. a stalled backup was timed out by the backup server). |
| Backup Unknown Error (15) | An error was recorded for this backup, but specific details are not available. |
| Backup Window Error (16) | Backup job was automatically terminated because it exceeded the backup window allotted for the job. |
| Backup X1 Error (17) | Supported product-specific error category. |
| Backup X2 Error (18) | Supported product-specific error category. |
| User Category 1 (19) | User-defined error category. For more information about how to set this error category, see the *Bocada Administrator Guide*. |
| User Category 2 (20) | User-defined error category. |
| User Category 3 (21) | User-defined error category. |
| User Category 4 (22) | User-defined error category. |
| User Category 5 (23) | User-defined error category. |
| User Category 6 (24) | User-defined error category. |

Failure Emphasis – The criteria “Failure Emphasis” is specific to the Job Trends family of reports (Job Trends, Failure Trends, and Consecutive Failures); With this option selected, combining successful jobs with failed jobs will roll up to a failed client instead of partially successful client.

Group By – The “Group By” criteria allows grouping, and sub-grouping up to three levels, in the Trends family of reports, by the following:



Note: The *Group By* criteria will also detect clients grouped into any custom Zone Types, and permit grouping by those zones.

Note: Grouping by Media Type will display Disk, Tape, Cloud, and other media types such as Data Domain if those media types are supported for the backup product performing the backup in question. Data Domain is a supported media type for Avamar, Backup Exec, CommVault, Data Protector, NetBackup, Networker, Spectrum Protect (TSM), and Veeam.

Hosts – The physical computer on which the hypervisor is installed. The Hosts criteria provide a list of virtual manager hosts.

Include Error Codes – Selecting the Include Error Codes check box adds an additional column to reports. The column is then populated with the proprietary error codes from the backup product. Note: The criteria to Include Error Codes may affect performance of the reports being run with this check box enabled.

Include Ignored Items – The criteria to Include Ignored Items can be enabled to show clients, targets, or jobs of backup targets that have been selected to be ignored within the Backup Client properties wizard.

Job Group – The name of an aggregation group for backups, e.g. schedule group, policy, or backup group. The criteria Job Group lists job groups for related backup products. Reports may include text-boxes to filter the report by including or excluding strings which match Job Group names.

Management Classes – The criteria Management Classes is specific to Spectrum Protect (TSM) policy collections. Management Classes is a grouping class for such backup clients. The Management Classes criteria lists all Management Classes associated and collected from a Spectrum Protect server during a policy collection.

Only Display Default Management Class – The criteria “Only Display Default Management Class” is specific to Spectrum Protect (TSM) policy collections.

Policies – Shared rules and settings used for running backups that are applied to a set of clients assigned to that policy. List of the backup policies as mined during the policy data collection.

***Note:*** *Not every job is assigned to a particular policy, and using the Policy criteria to include jobs with named policies will not include such jobs. Likewise, using this criteria to exclude certain named Policies will not exclude activity not associated with any named policy.*

Policy Domains – The criteria Policy Domain is specific to Spectrum Protect (TSM) policy collections. Used to determine shared rules and settings used for running backups that are applied to a set of clients assigned to that policy. The Policy Domain criteria lists all policy domains associated and collected from a Spectrum Protect server during a policy collection.

Policy Names – This criteria setting is specific to NetBackup policies. Used to determine shared rules and settings used for running backups that are applied to a set of clients assigned to that policy. The criteria Policy Name lists all NetBackup policies in the NetBackup Policy module reports.

Price Lists – A way of assigning prices to data backed up in the Bocada database. The criteria Price Lists will display all price lists created under the Administration Price List view.

Policy Types – A name given to a set of policies that have similar characteristics. This criteria setting lists policy type data for backup products where it’s applicable.

Protection Groups – This criteria setting is available only for Microsoft Data Protection Manager (DPM) reports and backup servers, and provides a list of DPM protection groups as configured on the DPM backup server. DPM protection groups provide encapsulation for backups with similar characteristics.

Recovery Point Types – This defines the recovery point type for Microsoft Data Protection Manager (DPM) backups. The criteria are a list of Recovery Point types for DPM reports.

Schedules – The criteria Schedules includes or excludes those schedules that are collected during a policy update (in Policy reports) or the Bocada schedules used (for Operations reports such as Data Collection).

**Server Groups** – This criteria setting enables filtering reports by Server Groups.

Show Policies – This criteria setting enables a user to filter reports by inactive or active policies.

SLA Profiles – The SLA Profile criteria lists SLA Profiles that were created in the SLA Config view.

Status (Data Collection) – This criteria setting enables filtering of the data collection view by the following statuses: Successful, In Progress, Failed, Pending, Never Processed or Stopped.

Status (Job Status) – Job Status refers to the status of a backup as displayed by Bocada as a red, green or yellow circle. The status criteria enables filtering by backup status: Failure, Partial Success and Success. The default meaning of the colors for a job are:

 Green Success: No errors.

 Red Failure: Errors occurred and no bytes were transferred.

 Yellow Partial: Some error was found, but bytes were backed up.

Storage Units – This NBU criteria provides a selection of Storage Units pulled from a NetBackup server during a policy data collection.  NetBackup uses a Storage Unit as a label for physical storage.

Storage Groups – This NBU criteria provides a listing of Storage Groups pulled during a policy data collection.  This is defined in NetBackup as groups of storage units.

Storage Lifecycle Policies – This NBU criteria is for policies that define the flow of backup data on NetBackup servers. The criteria “Storage Lifecycle Policies” lists storage lifecycle policies associated to a backup server.

Success for Zero Bytes/Errors – This criteria setting is optionally used to indicate whether to treat backups with zero bytes and zero errors as success or failure. This is set based on level (e.g. a full backup with zero bytes and zero errors might be a failure while a differential backup with zero bytes and zero errors would be treated as a success).

Targets – The protected resource, also known as Assets. Reports may include text-boxes to filter the report by including or excluding strings which match Target Names.

Time Zone – Seen under Date Range, the Time Zone criteria enables users to select the time zone in which the data should be displayed. This criteria setting can be set to a specific time zone or Backup Server Time. Backup Server Time represents the time zone of the backup server that performed the activity. Backups will be displayed in the time zone of the server (i.e. multiple time zones will be displayed in the report if the servers are in different time zones).

Update Types – The following types of data collection are supported by Bocada: Backup, Storage, or Policy. These criteria enables users to filter the data collection view by one or more of these collection types.

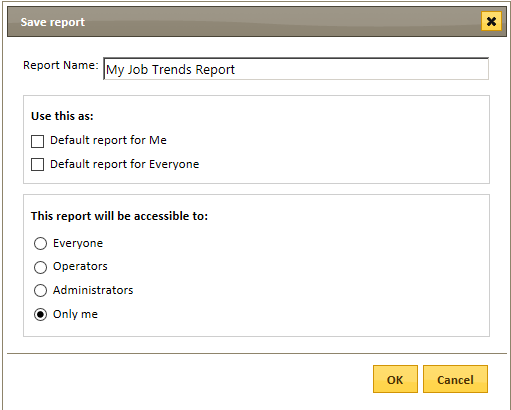
Virtual Managers – Central management for hypervisors. The criteria setting lists virtual managers added to the Bocada Application for virtual reporting.

VM Names – These are the virtual machine names that are assigned to data stores.

Volumes – Lists media volumes such as cloud, disk, or tapes.

## Saving Criteria

Criteria used in reports can be saved by using the Save Criteria feature on the right menu, allowing you to rename and save a report, as well as control who may view the report and whether it is the default report shown:



Note: Selecting “Default report for Everyone” will automatically make the report available to Everyone. Restricting the accessibility to less than “Everyone” will disallow selecting “Default report for Everyone”.

A report set as Default for Everyone will not override a user’s personal default report of that type; Global defaults will apply to users without personal default reports.

The saved reports will then appear under the [Saved Reports](#_Saved_Reports) view of the [Health Check](#_Health_Check) module.

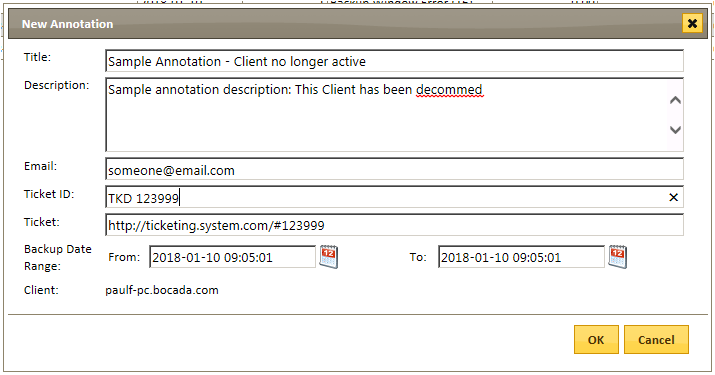
## Action Panel Functions

Bocada provides the ability to perform specific actions, including editing and saving reports, setting up alert criteria, creating email schedules for communicating results to stakeholders, and creating annotations to keep track of actions taken to resolve problems. The Action panel is found on the right of the screen and can be expanded to a full menu or collapsed to only the action icons. Actions available are dependent on the report or view that has been selected.

Add – Applies to a variety of actions that can be performed depending on the report area the user is viewing. This action is used to add Zones, SLA Profiles, Backup Servers, Users, Price Lists and Alerts.

Add Alert – Opens the Alerting wizard to create an email alert or ticketing system email alert based on multiple criteria options (See Alerts). This action is available for Job Activity or Restore Activity reports.

Add Annotation – Opens a new dialog box that will allow Operators and Administrators to add detailed information regarding any job/client selected. The intent of annotation is to enable Operators and Administrators to keep a record of actions taken to resolve issues with any particular job or client; multiple annotations can be added to any job/client selected. Annotations will be associated with the job/client in perpetuity and will be kept in a searchable knowledge base; the time, date and creator of the annotation are automatically tracked for reference. This action is available in the Health Check > Activity module.



***Add Annotation Dialog Box***

Annotation time windows may also be extended, so they can be displayed per backup client for a designated period.

Add User – This action is available to Administrators only, and can be found in the Users view under the Administration Module. The action “Add User” allows adding additional users (Administrators, Operators or Standard Users)

Add Zones – This action is available to Administrators only, under the Administrator Module, Zones view. This action will open a new dialog that allows Administrators to add a zone type or zone under a zone type for zoning of clients.

Archive – This action will archive an SLA profile from the Manage SLAs view. This action essentially decommissions the SLA; however, the history of SLA configuration and results are maintained. This action is only available on the Manage SLAs view.

Assign Clients – Similar to the Client Properties action (see below), however, Assign Clients is only related to specific reports. This action opens a wizard that allows Administrators and Operators to assign clients to SLA Profiles, zones, and price lists.

Assign Data Domain – This action, which appears in the Operations > Backup Servers view, allows Administrators and Operators to assign & unassign policies as Data Domain, with the effective start date. See the *Bocada Administration Guide* for details.

 Cancel Updates – This action allows Administrators and Operators to manually cancel running, pending or in progress data collections. This action is only available in the Operations > Data Collection view.

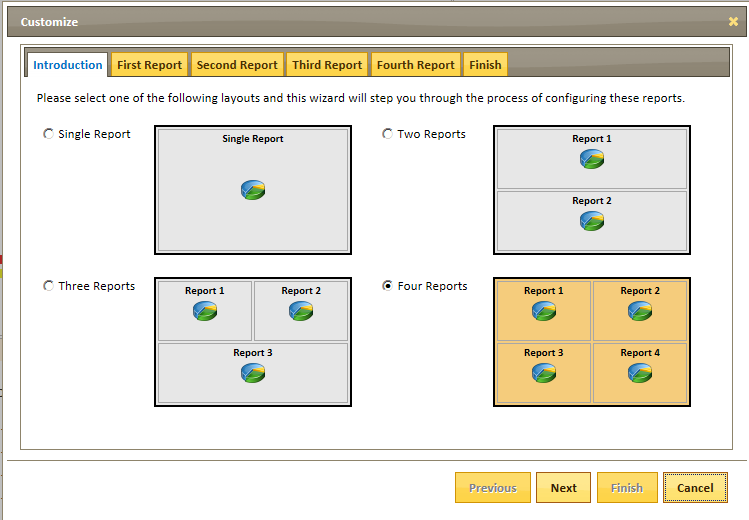
Copy Custom Report – This action copies customized SQL reports from the Saved Reports View. The copied report will copy the existing custom SQL settings to newly named reports.

Client Properties – This is a global action for assigning properties to any clients in the environment. This action is available in the Operations / Backup Clients setup area. This action will open a wizard that allows Administrators and Operators to assign clients to SLA profiles, zones, pricelists, or to be ignored or renamed.

Customize Dashboards – The action to customize the default dashboard allows Administrators to customize the reports and settings to be viewed in the dashboard. Administrators can also set up default dashboard views per user.

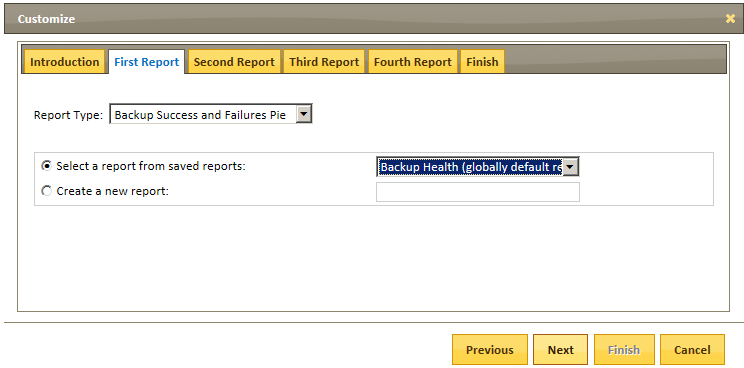
To customize the dashboard, click on the Customize icon in the right Action panel.

The Introduction tab allows users to choose up to four reports to be viewed in the summary dashboard:



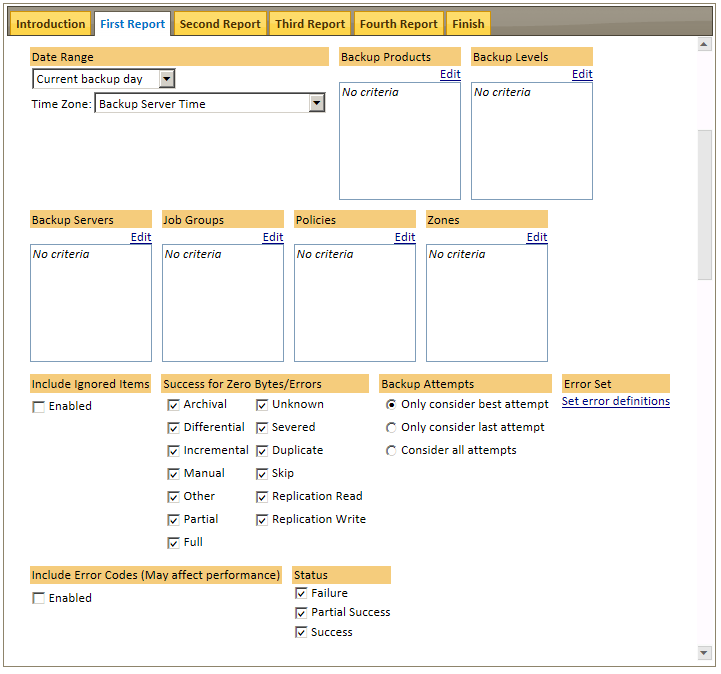
***Dashboard Customization Panel***

The following tabs, from First Report to Fourth Report, allow Administrators to select the type of report that will be displayed. The administrator can select a standard report, select an existing saved report, or create a new report for the dashboard.



***Dashboard Customization, Report Selection***

To create a new report for the dashboard, select the type of report from the drop-down menu, and select the “Create a new report” option. The new report requires a unique title. Administrators can then select the criteria desired for a new report and save the report.



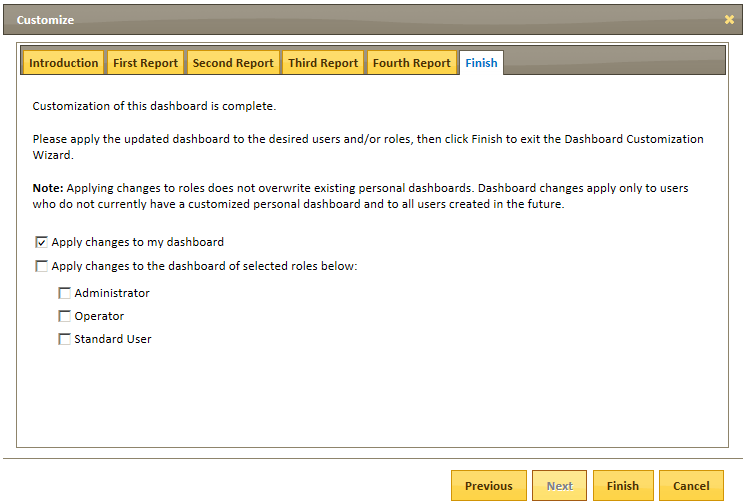
***Dashboard Customization: Criteria Selection***

The Finish tab of the Customize wizard allows Administrators to set which users can see the customized dashboard.The options are:

Apply changes to my dashboard

Apply changes to the dashboard of selected roles below:

* + Administrator
  + Operator
  + Standard User



***Dashboard Customization: Choose User Access***

**Note:** For additional information on Customizing Dashboards, please reference the *Bocada Administrator Guide*.

Delete –Allows for deleting of servers, schedules, zones, pricelists, saved reports, etc.

Delete Custom Report – Deletes customized SQL reports to be deleted from the Saved Reports View.

Edit –This action allows for editing of properties of server, schedules, SLA profiles, etc.

Note: The edit icon is only available for single editing. If multiple items or no item is selected the icon will be greyed out.

Edit Custom Report – This action allows Administrators to edit reports created with custom SQL properties. This action will open a new dialog for editing of the SQL. This action is only available in the Custom SQL Templates view.

 Export – Exports reports as HTML, PDF, CSV, or TXT depending on the type of report that is being viewed.

New Custom Report – Administrators may create a new report with custom SQL properties using this action. This action will open a new dialog area for adding custom SQL. This action is only available in the Custom SQL Templates view. Please see the *Custom SQL Reporting* section of the *Administration Guide* for further details.

Open – Opens a dialog area to view and select previously saved reports. Only saved reports of the type currently being viewed will be listed.

 Pause/Resume – With this action, found under Operations: Schedules, all scheduled actions may be temporarily suspended or resumed.

#### Refresh – This action will refresh the current view. The refresh will use the last saved criteria of the reports.

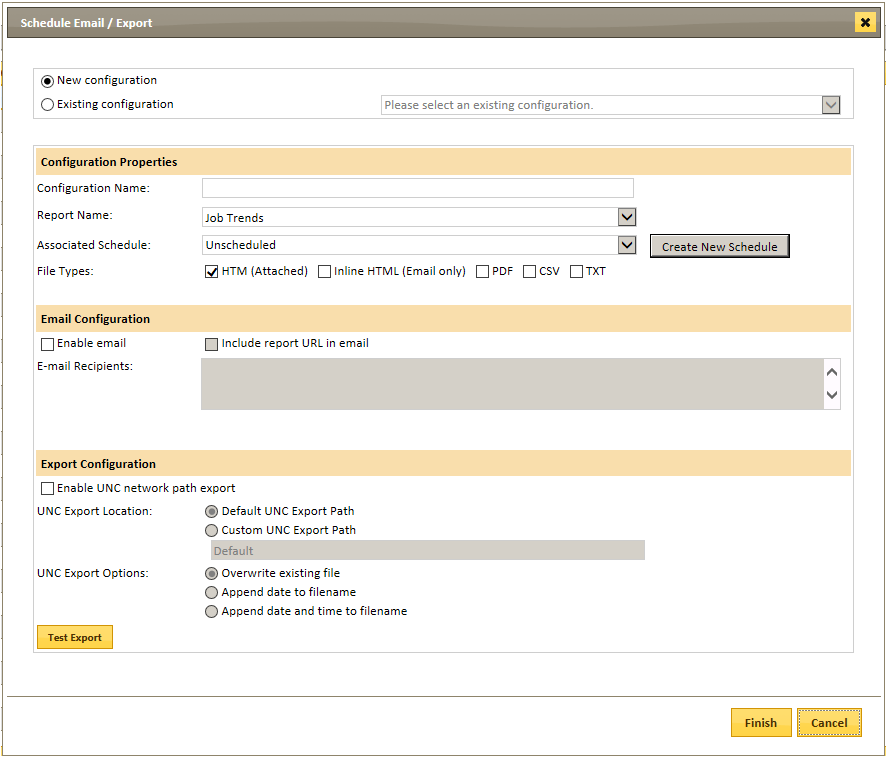
 Remove Users – With this action, an Administrator may remove Operators and Standard users. This action is only available from the Administration Module.

#### Run Report - Runs the report with the current specified criteria settings chosen in Report Criteria.

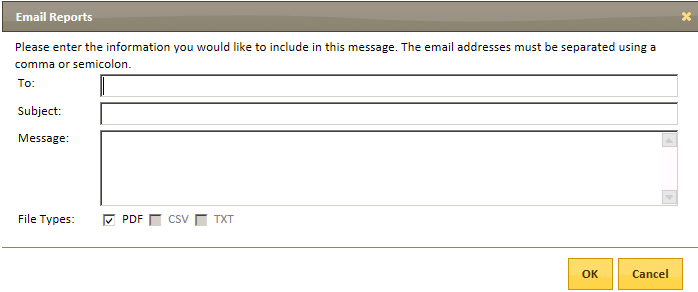
Run Updates – Allows Administrators and Operators to manually run data collections against selected backup servers and backup types. This action is only available in the Operation Module, Data Collection.

Save Criteria – Opens a dialog to save a new report or save the same report with new criteria set in the Edit Report Criteria.

Schedule Report – Opens a dialog to create a Scheduled Report configuration to associate a Report with a Schedule, or use an existing configuration for this report:



#### Send by Email – Sends an exported report view to any email address.



***Send Email Configuration Dialog***

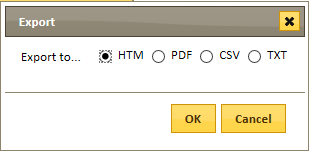
SLA Impacts – Opens a list of SLAs that may be impacted by job results.

View Annotations – Launches a dialog to view and search on existing annotations.

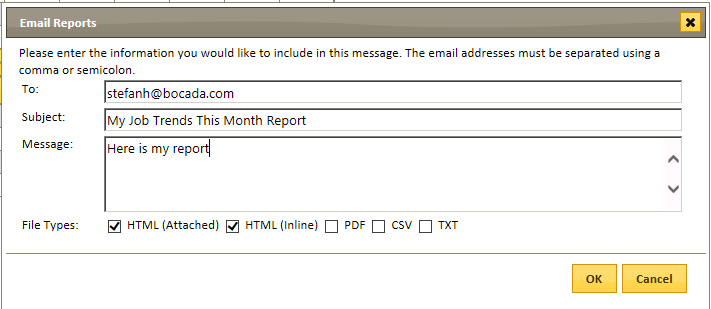
 Unassign Clients – This action opens a new dialog to select specific clients to remove them from existing SLA Profiles, Zones or pricelists. This action can be found on the Manage SLAs, Zones and Pricelist views.

## Exporting and Emailing

Report results can be exported to a variety of file formats by selecting the Export option from the Action Panel at right.  This will open an Export dialog to choose the file format:



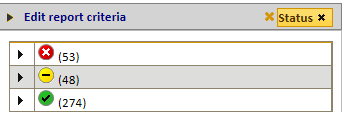
Report results can also be emailed directly to a report recipient in one or more file format(s) by selecting the Email option from the Action Panel.  This will open an Export dialog to choose the file format:



## Tabular Grouping

Grouping can be done on all tabular reports. Grouping is done by simply dragging any column header to the report title bar.





***Grouping Example: Group by Status***

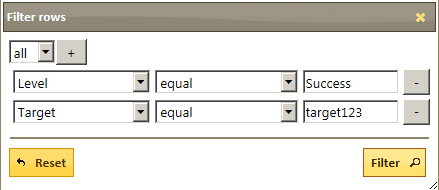
There is no maximum number of headers to group by within a report. Grouping order can also be changed by dragging the column header name to different order positions.

To remove the Group, click on the **X** next to the column header to be removed.

Reports can be saved with the columns grouping selected and emailed or exported.

## Tabular Filtering

Filtering can be done on all tabular reports by using the  in the lower left view of the report. Filtering differs from the criteria setting as the filtering option filters on data that is currently displayed (as opposed to determining what should be displayed). Users can filter on any of the columns that are on the current report display.

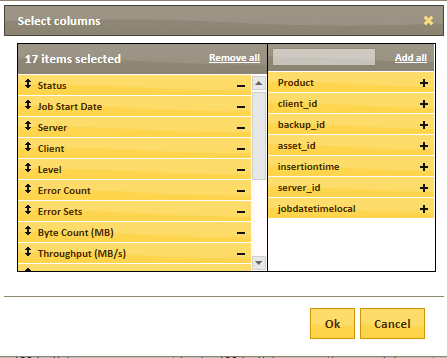


***Filtering Dialog Box***

## Tabular Column Selection

Adding or removing columns can be done on all tabular reports by using the  in the lower left view of the report. The selection of columns will be relevant to the report being viewed. How the report is viewed can be determined by which columns are chosen and the order they are listed.

Reports can be saved with the columns grouping selected and emailed or exported.



***Select Columns Dialog Box***

## Custom Failure Icon

Step: 1 Calculating the error code

There are 24 types of error code:

0: No Error

1: Aborted Backup Error (1)

2: Backup Configuration Error (2)

3: Backup File Busy Error (3)

4: Backup File Corrupt Error (4)

5: File I/O Error (5)

6: Backup File Locked Error (6)

7: Backup File Permission Error (7)

8: Backup File Verification Error (8)

9: Backup Group Error (9)

10: Backup Media Unavailable Error (10)

11: Backup Media I/O Error (11)

12: Backup Network Error (12)

13: Backup Software Error (13)

14: Backup Timeout Error (14)

15: Backup Unknown Error (15)

16: Backup Window Error (16)

17: Backup X1 Error (17)

18: Backup X2 Error (18)

19: User Category 1 (19)

20: User Category 2 (20)

21: User Category 3 (21)

22: User Category 4 (22)

23: User Category 5 (23)

24: User Category 6 (24)

In order to use custom failure icon for specific error, first need to get the HEX number which corresponds to the failure error code. This can be done by setting the number of bit corresponding to error code number.

For file only errors: 3, 4, 5, 6, 7, 8, setting the integer number 3, 4, 5, 6, 7, 8 bits, then transform binary to a HEX number.

Binary: 0000 0000 0000 0000 0000 0000 1111 1100

Hex: 0xFC

Step 2: Save error code in Bocada database zparams table.

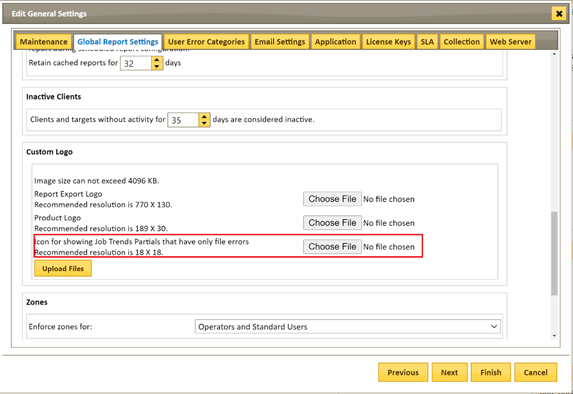
For file only errors run following SQL:

INSERT INTO zparams (paramname, paramvalue) values ('CustomFailureErrorCodeWithIcon', '0xFC')

Step 3: Upload the custom icon

(1) In order to upload custom icon, first need to go to WebUI\images folder, grant bocada domain user read, write and modify privilege.

(2) On left navigation menu click Administration -> Settings, click the on the right edit icon:



Click “Choose File” button choose the custom icon, needs to be in PNG format and size preferably in 18X18 pixel. Then click “Upload File” button. The custom icon file will be uploaded and saved in WebUI\images folder, the file name: “custom\_failure\_icon.png”

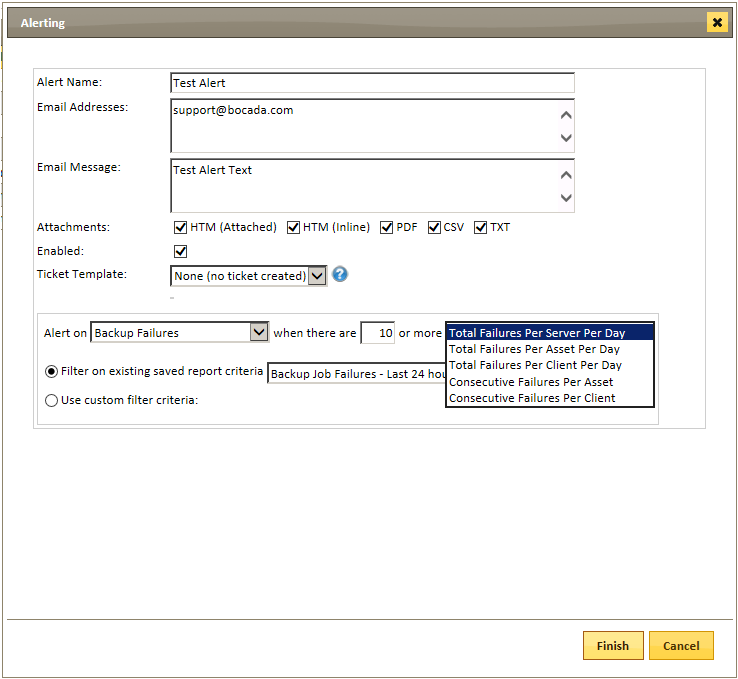
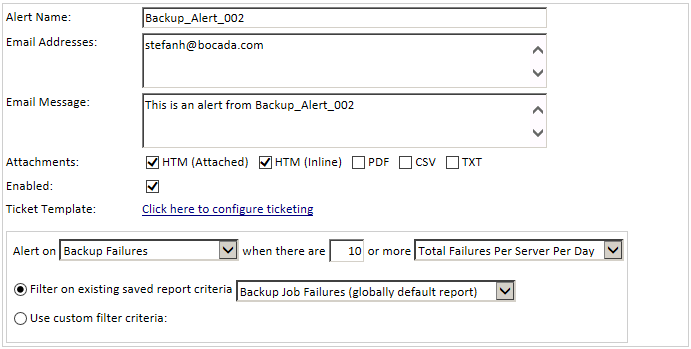
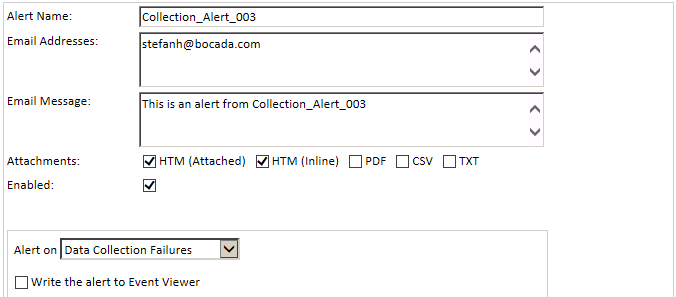
Step 4: Restart Bocada Service also refresh browser by “CTRL+F5”. The custom icon will show up in all activity and trend reports inside Bocada as well as exported reports in HTML format.

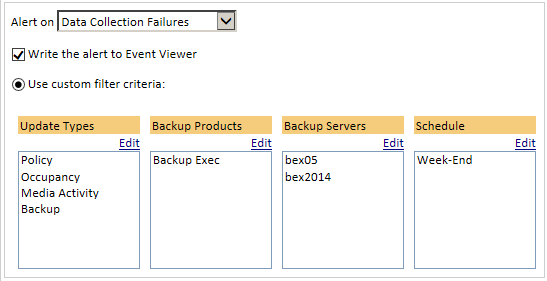
# Detailed Report Explanations

## Alert Config

Found in [Operations](#_Operations). *Alert Config* allows the user to configure alerts. Alerts are listed in the *Backup Alert Activity* or *Data Collection Alert Activity* reports, and can be emailed to users and sent to any trouble ticketing solution that can receive email. Backup and Restore Alerts notify when backup and restore failures match pre-defined criteria as data is collected from the backup servers into Bocada. Likewise, Data Collection Alerts can send email to users or to a trouble ticketing system when Bocada data collection updates have failed.

#### To Create or Edit an Alert:

1. Click the Add (or if editing an existing Alert, Edit) icon in the Action Panel.
2. The Alerting wizard will appear: 
3. Configure the alert:
4. Alert Name: (required).
5. Email Addresses: (optional).
6. Email Message: (optional).
7. Choose attachment types.
8. Enable or disable the Alert.
9. Ticket Template: (optional; Please reference the *Integrating Ticketing System Guide)*.
10. Define alert type and failure criteria:
    1. Backup / Restore alerts: Set number & type of failures 
    2. Data Collection alerts: Alert will be triggered for each data collection failure 
11. To filter the criteria which may trigger this Alert, choose a Saved report, or define custom filter criteria:

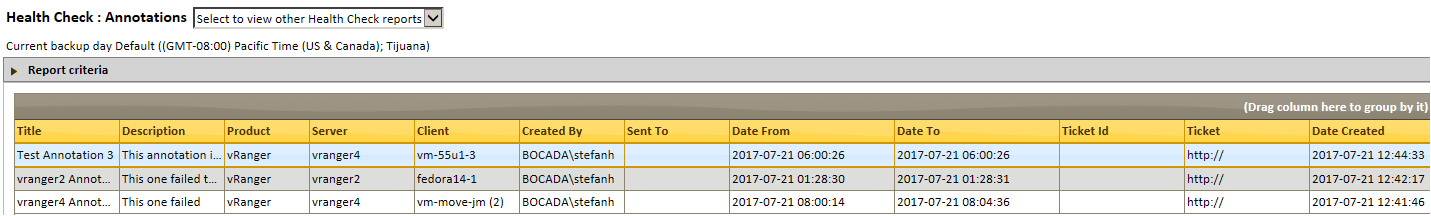


Details of any triggered Alerts can be reviewed. Backup and Restore Alerts are displayed in the *Backup Alert Activity* report. Data Collection Alerts are displayed in the *Data Collection Alert Activity* report.

For more on Alerts, please see the *Bocada Administration Guide* section on Alert Config.

## Annotations

*Annotations* provides the capability to keep permanent records or comments such as troubleshooting and resolution activity for backup clients.



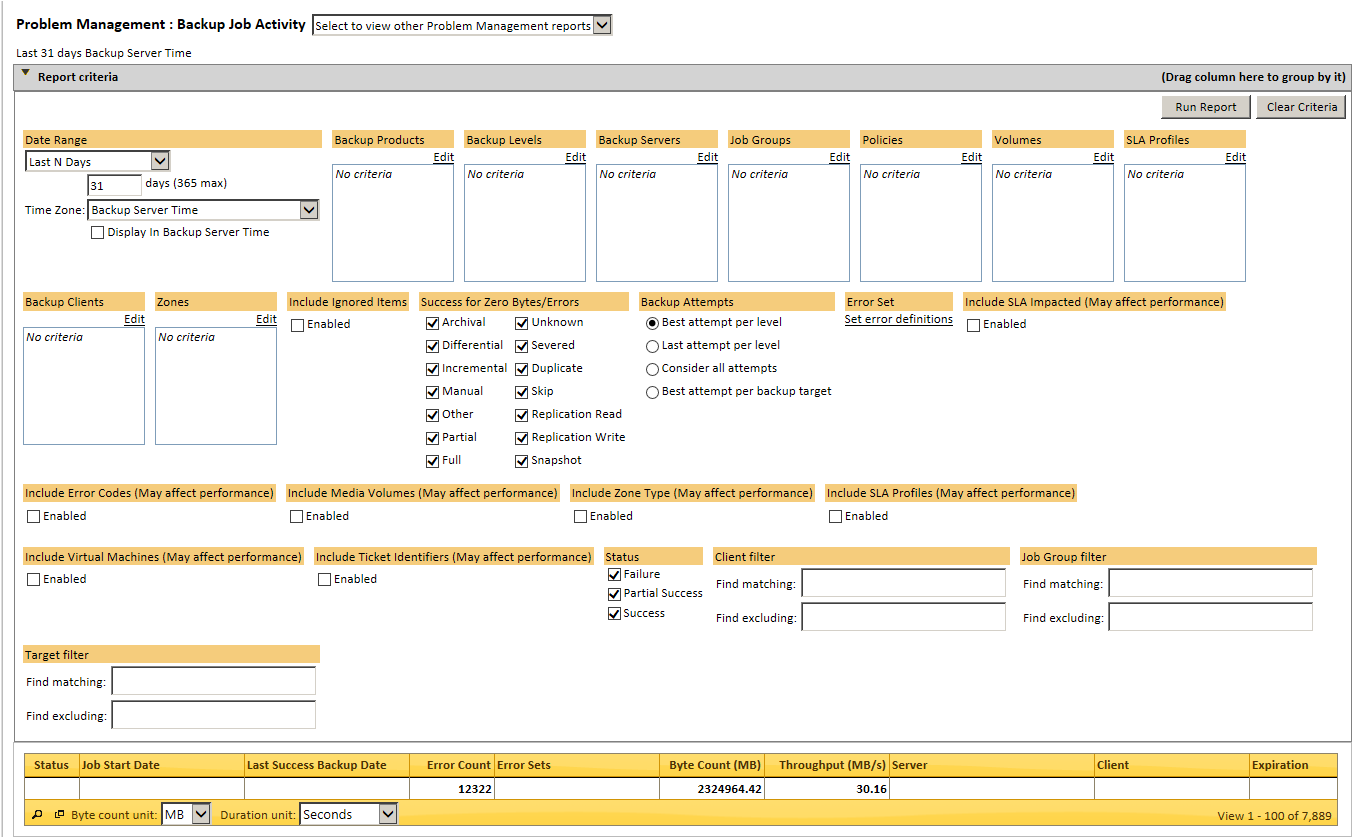
Annotations are entered and are viewable in reports such as *Job Activity, Backup Failures, Restore Activity,* or *Restore Failures*, the Annotations report allows easy filtering and grouping. The time, date, and creator of the annotation are automatically tracked for reference. To aid in filtering and grouping, a naming or ticket number convention for annotations may be desired.

Note: While the “Date From” and “Date To” fields of an annotation default to the start and end times of the activity which is annotated, the “Date Created” and “Date Modified” fields are displayed in your installation’s default time zone. In some cases, this may make the annotation appear to have been created before the activity.

## Job Activity

*Job Activity* lists backup attempts matching selected criteria over configurable periods of time, with the ability to drill down into exact details regarding the job activity by selecting the Status icon for that job.

The [Criteria](#_Report_Criteria) settings for the Backup Activity report are entirely customizable:



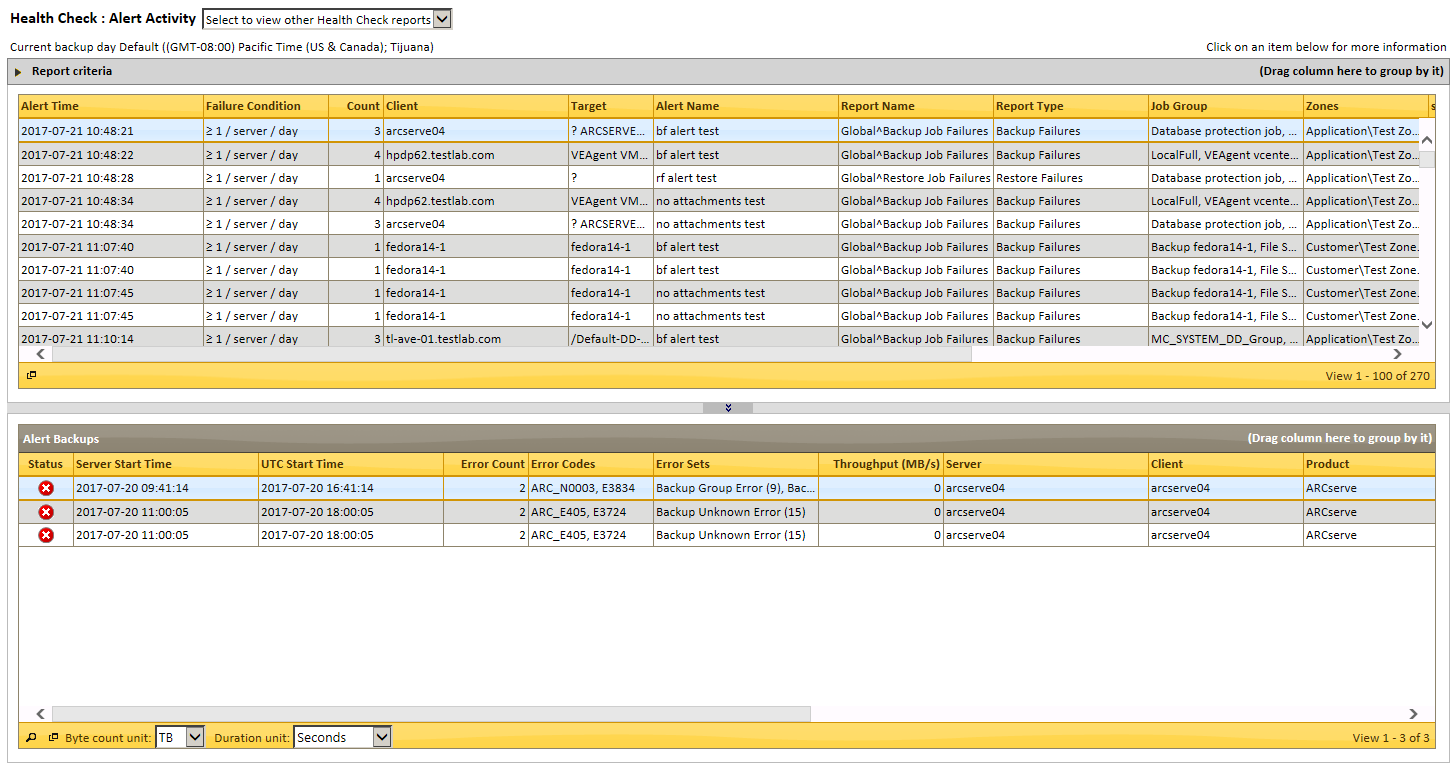
*Include Error Codes* adds an additional column to reports with the proprietary error codes from the backup product.

Note: In addition to most typical actions on the Action panel, the Job Activity report also includes the possible actions for adding and finding annotations, viewing SLA Impacts, and adding alerts.

Note: The default setting for Backup Attempts is to consider *Best Attempt per Level*. This setting displays the most recent, most successful job per level for each target for each backup day. If there are multiple attempts per target in that backup day it will display the most recent successful backup. If none of the attempts were successful, the most recent partially-successful attempt is displayed, or the most recent failure if there are no partially-successful backups. The criteria for *Consider all attempts* will display all attempts, *Last Attempt per Level* will display the most recent attempt that match the remaining criteria, and *Best Attempt per Backup Target* will display the most successful attempt regardless of backup level.

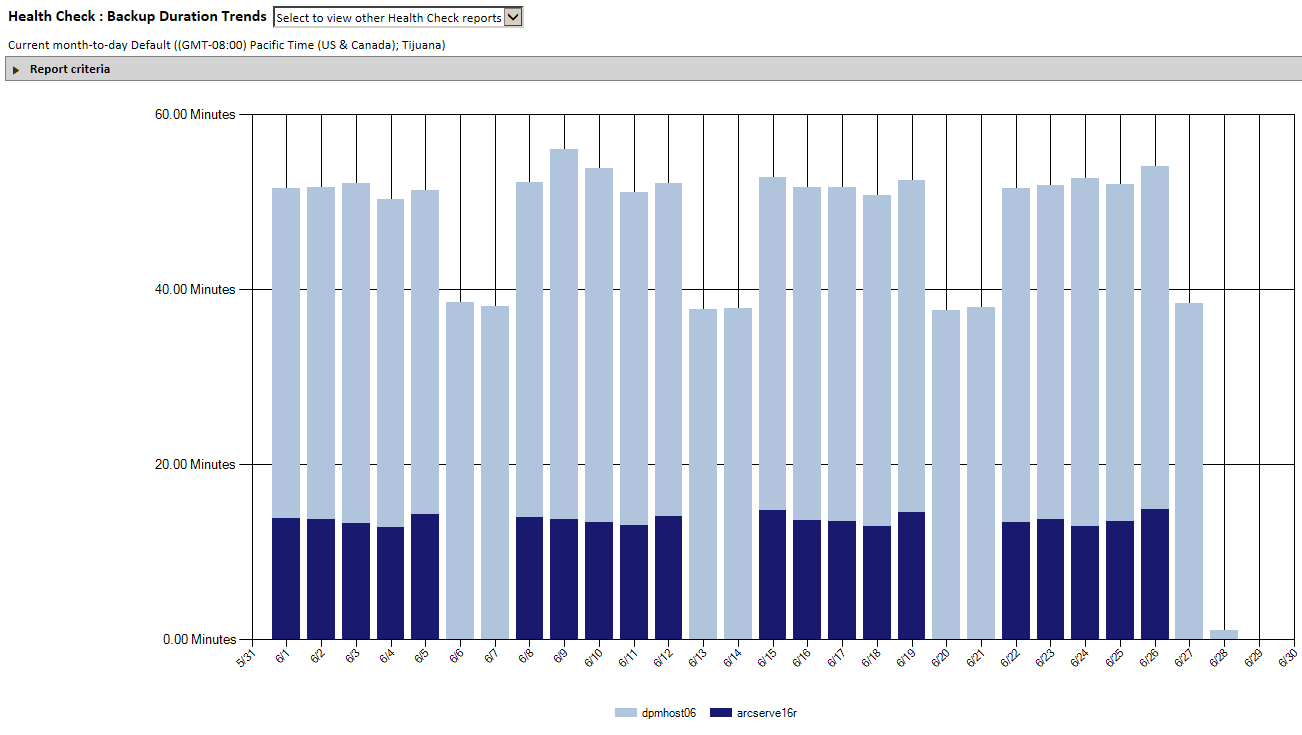
## Backup Alert Activity

The *Backup Alert Activity* lists alerts that have been triggered for backup or restore failures based on previously configured alert profiles (See *Alert Config*).

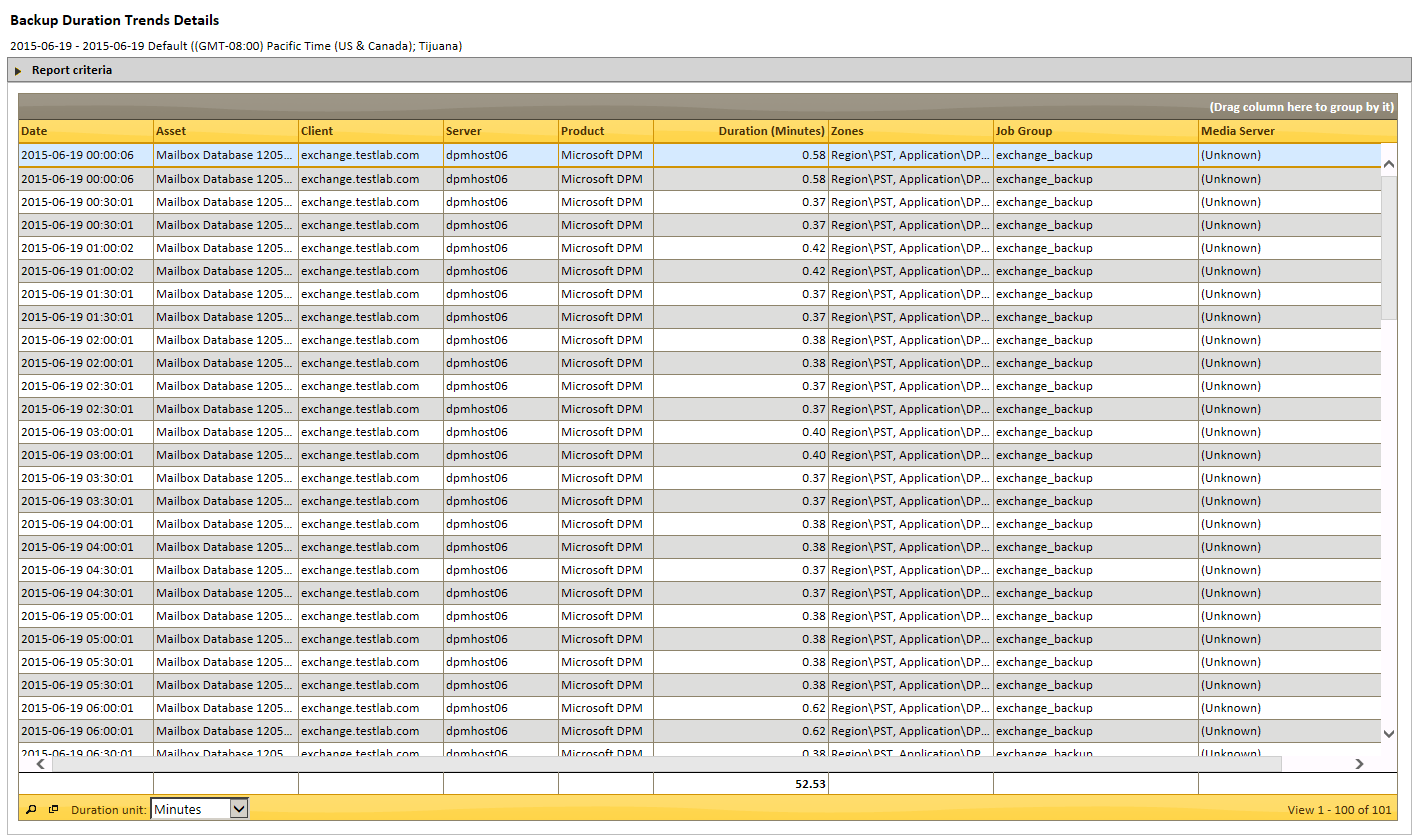


## Backup Duration Trends

*Backup Duration Trends* helps identify backup bottlenecks by showing the sum of the top ten backup durations per day over a selected period of time, in the form of a bar chart:

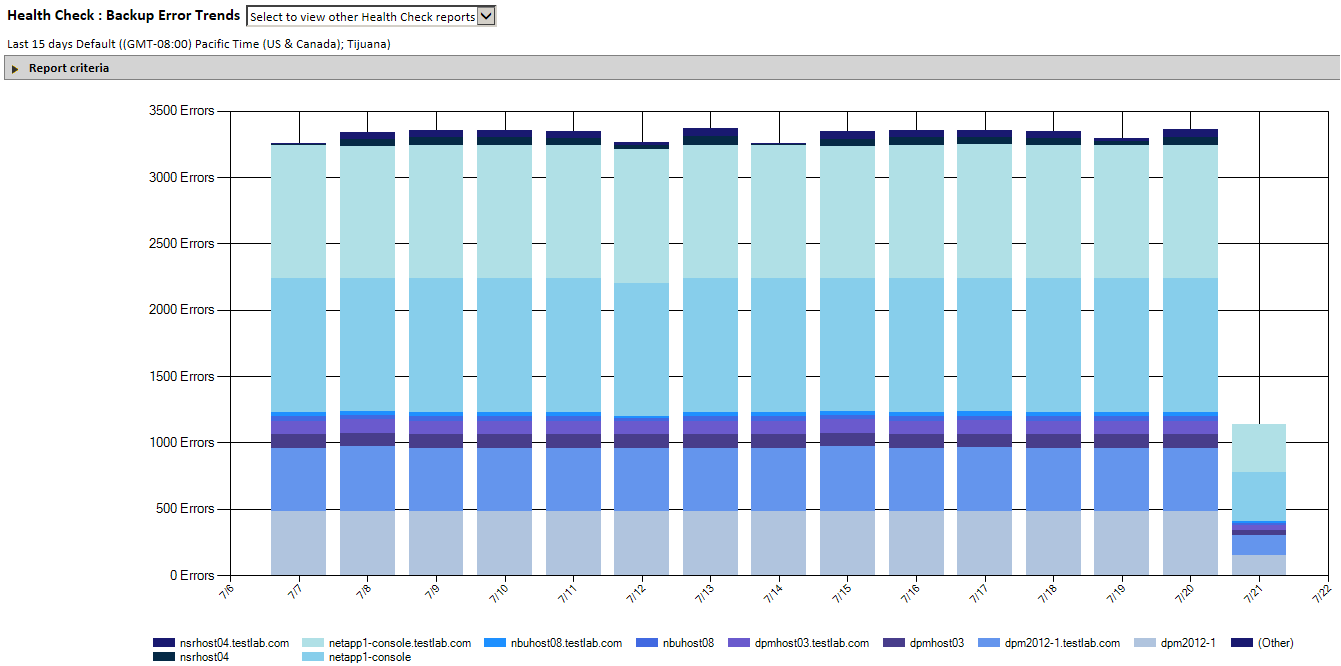


Problems are identified by observing spikes or excessive duration, and filtering by criteria. Clicking on a section of the bar will take users to the related granular job details:

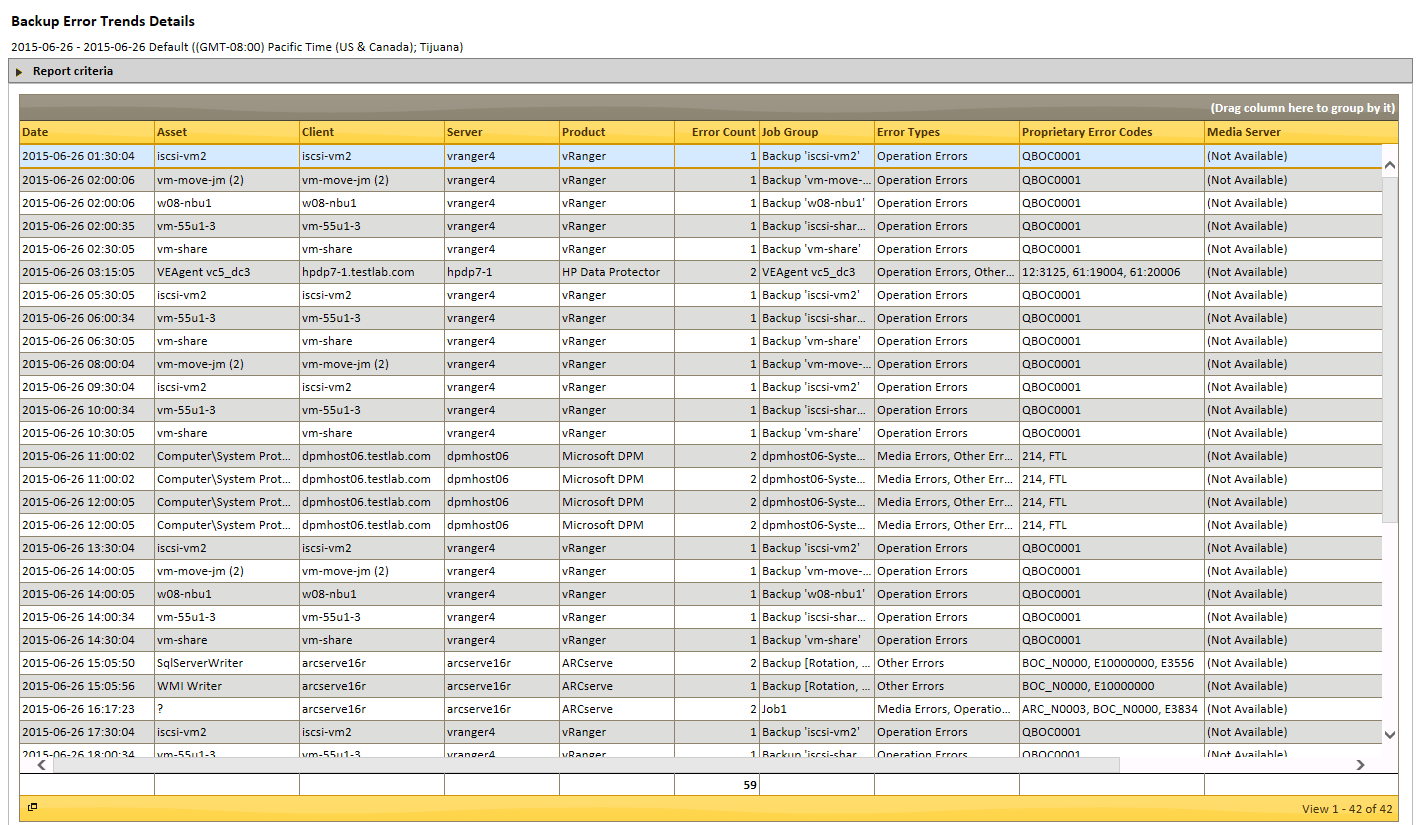


## Backup Error Trends

*Backup Error Trends* displays the trend over time of backup error count for selected criteria in the form of a bar graph:

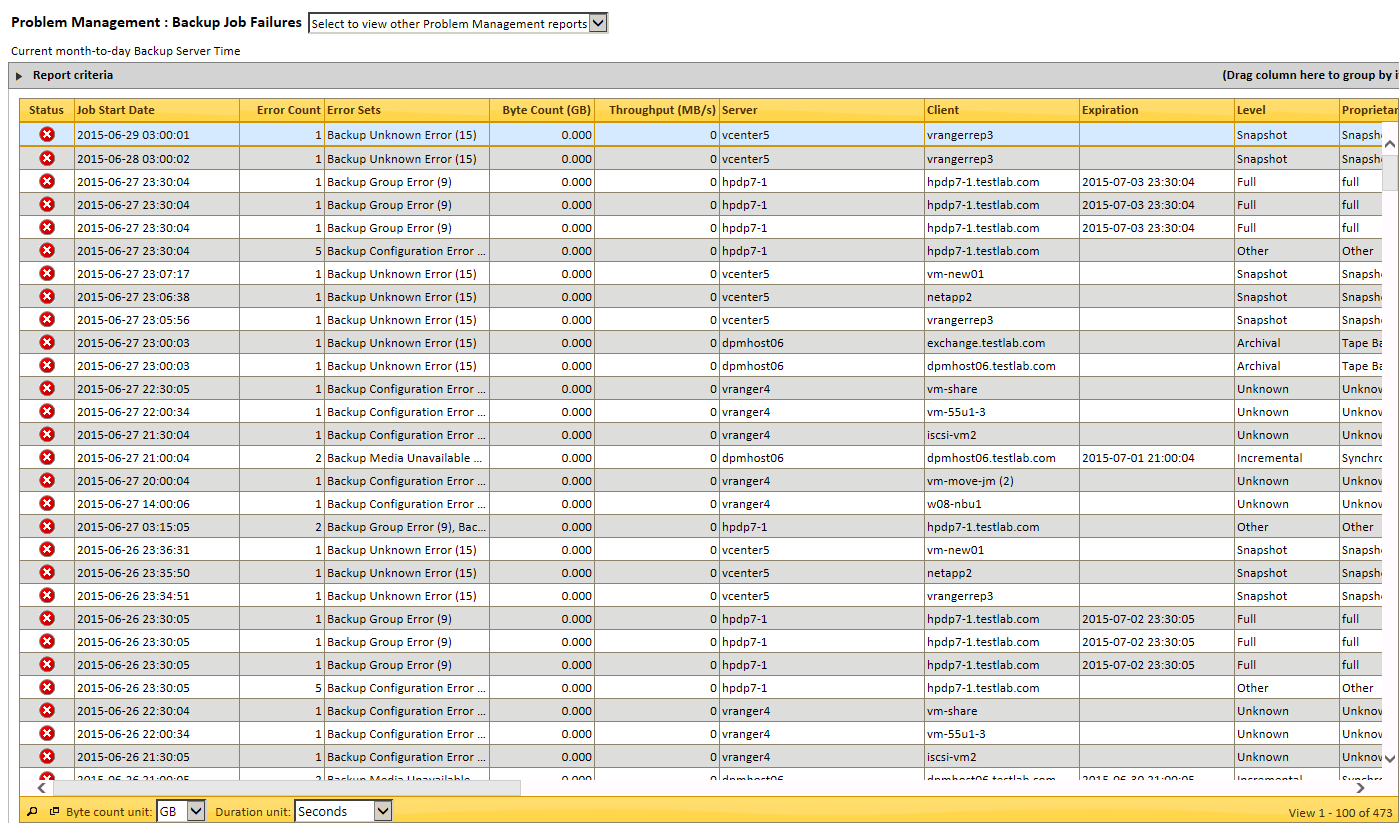


Mouse over any portion of a bar to view the date, server, and error count for that portion of the bar. Click on any portion of the bar graph for a granular view of the errors that contribute to that bar:



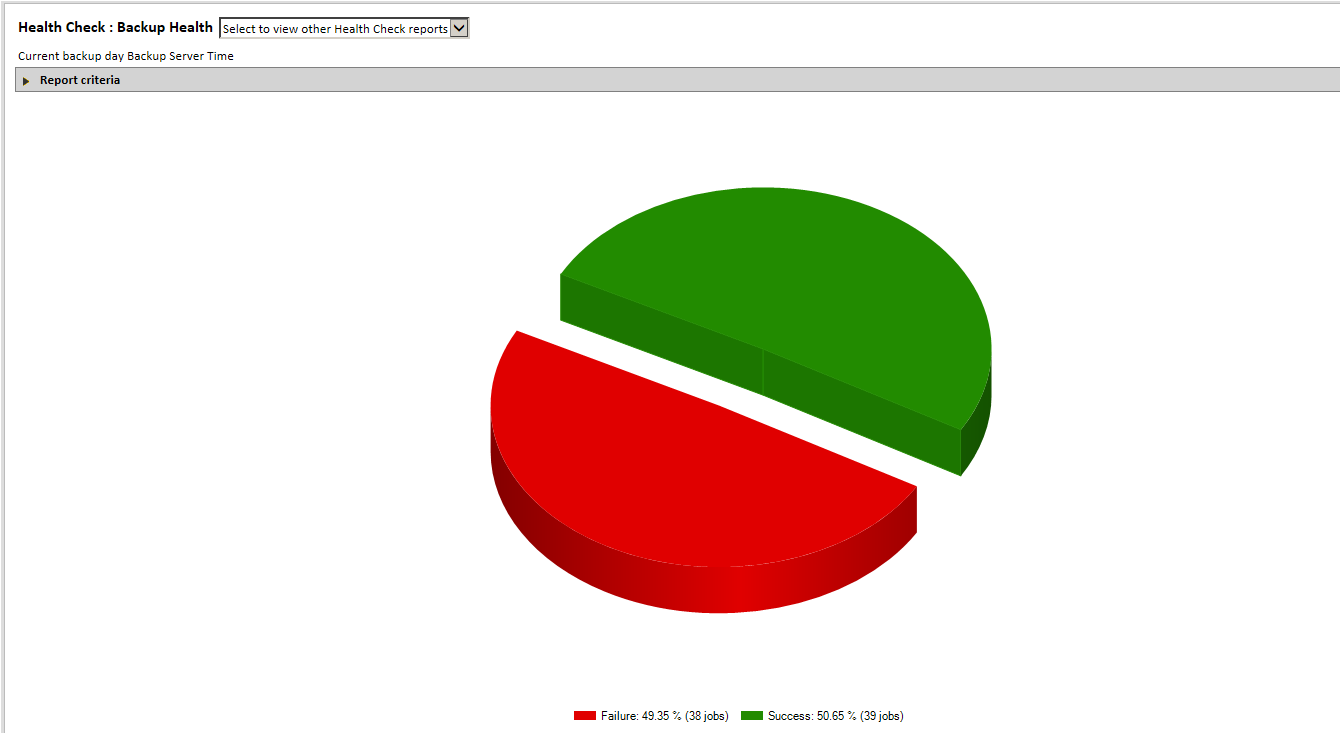
## Backup Failures

*Backup Failures* is a subset of Job Activity that displays only failed and partially successful backups. This report can be filtered and zoned to view specific jobs. Each failed job will include server, client and error information. Selecting a specific Status icon drills into details about the type & reason of failure to aid in problem resolution.



## Backup Health

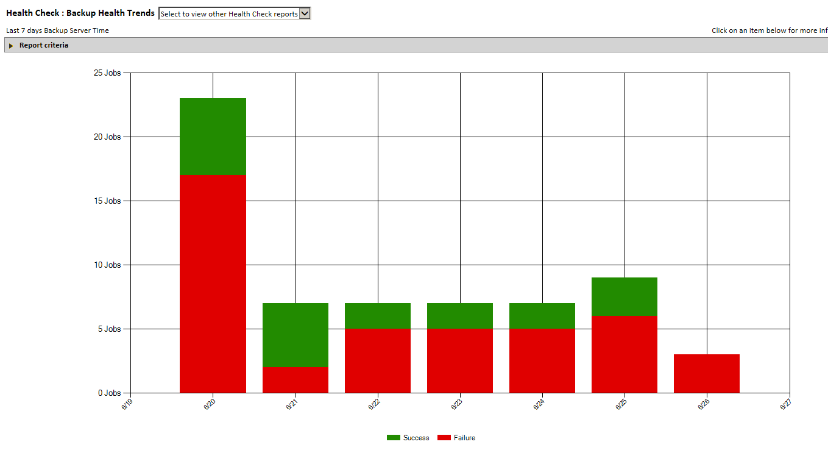
*Backup Health* displays all successes, failures and partial failures for backups, replications and snapshots. This report can be set for the entire environment or can be filtered by zone, backup application etc. Represented in a pie chart, the Backup Health report quickly provides an overview of success percentage (green), failure percentage (red), and partial failure percentage (yellow) for the environment:



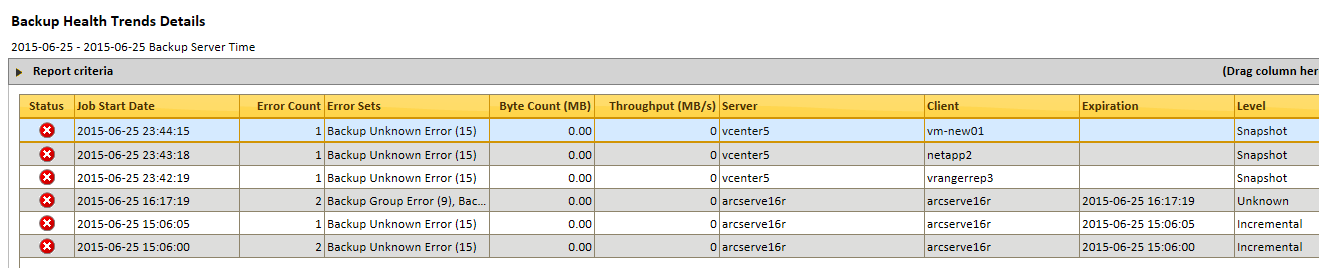
Clicking on a section of the pie will take users to the related granular job details in the Job Activity report.

## Backup Health Trends

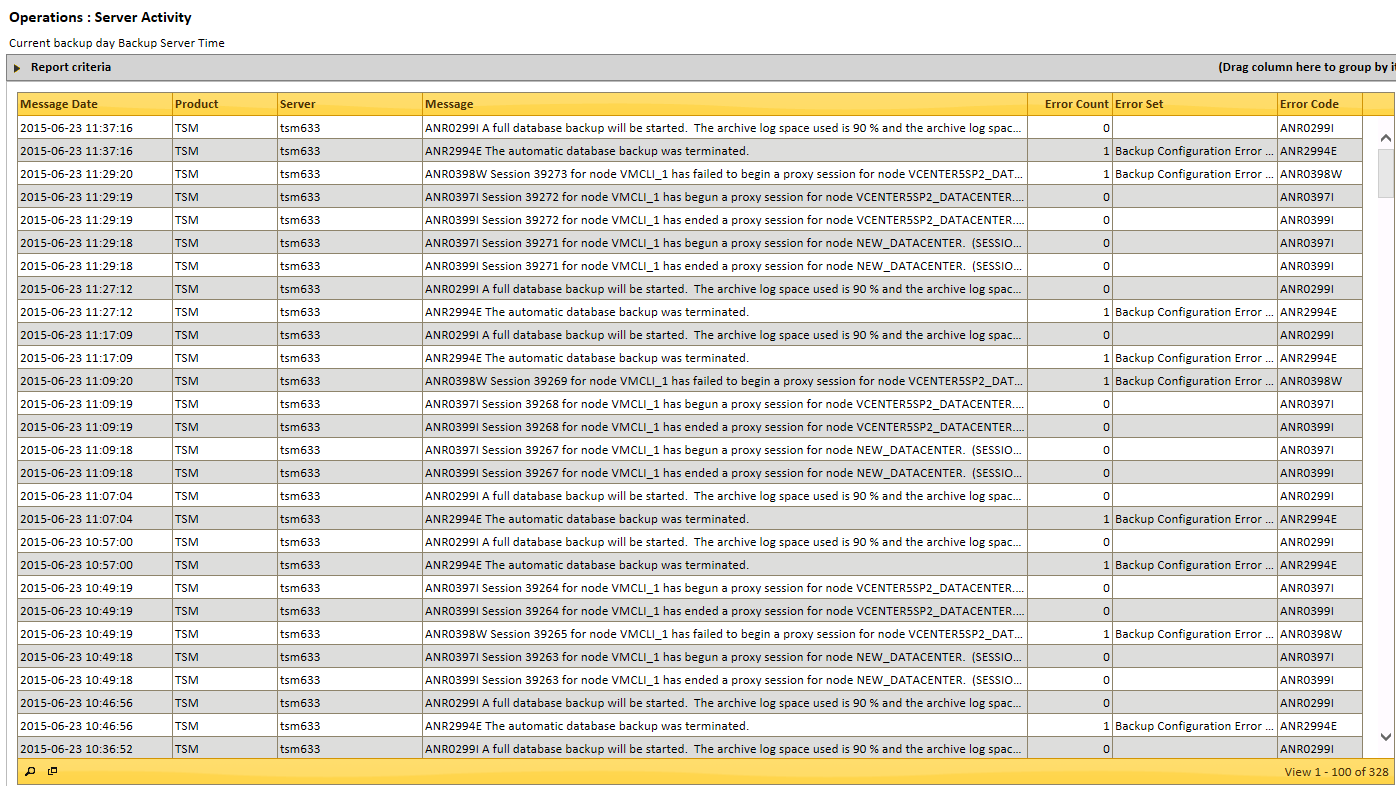
*Backup Health Trends* displays the trend over time of backups that are successful, partially successful and failure in the form of a bar chart:



Clicking on a section of a bar will take users to the related job details:



## Backup Server Activity

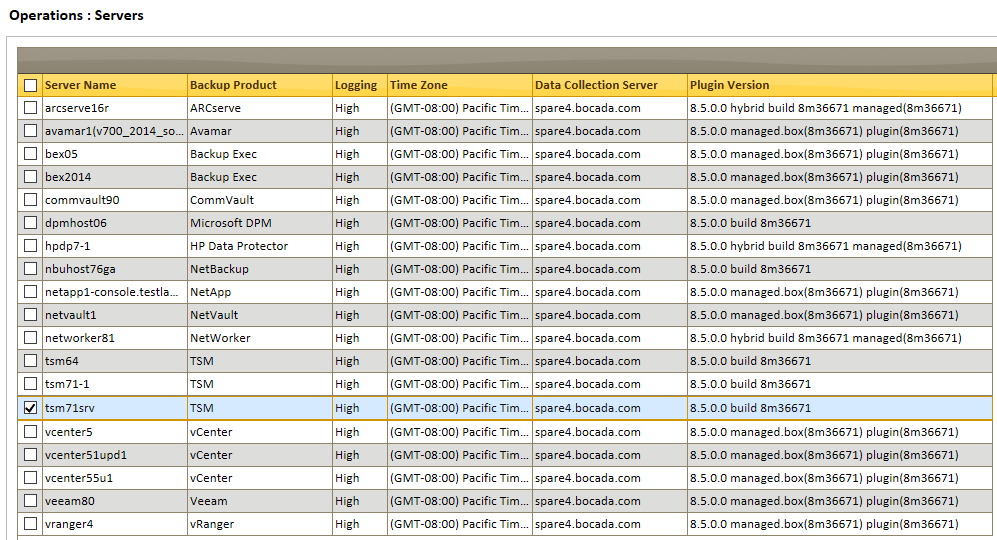
Found in Operations. *Backup Server Activity* displays a tabular report of all messages returned from the backup servers designated in *Backup Servers*. 

[Criteria](#_Report_Criteria) Selection: Server Activity can be narrowed by Date Range, by Backup Product, and by Backup Servers.

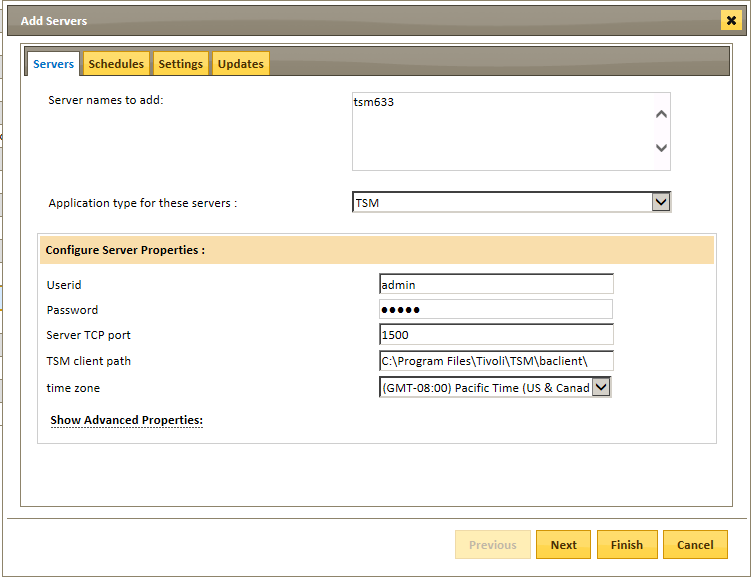
As with all tabular reports, it is possible to group the report by any column, by dragging that column header to the gray Report Criteria bar at top.

## Backup Servers

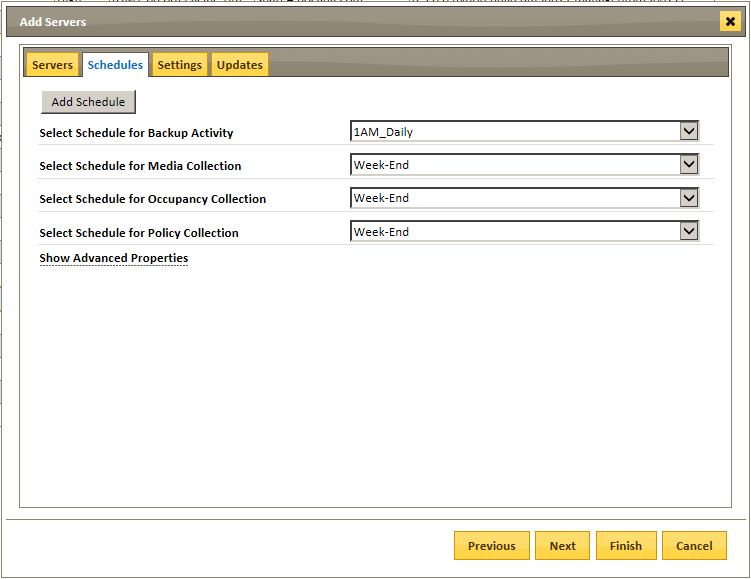
Found in [Operations](#_Operations). *Backup Servers* allows users to add, remove, or edit settings for backup servers.



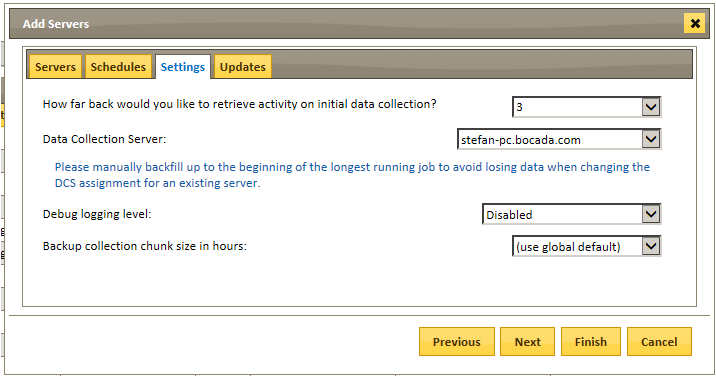
**Adding a Server:** Selecting the Add action will open the Add Servers wizard. On the initial *Servers* tab, you can configure a server and the backup application it is running, with the properties necessary to connect to it:



Scheduling server actions for Backup, Storage, and Policy collection is managed on the *Schedules* tab. Select a predefined schedule, or click the Add Schedule button to create a new [Schedule](#_Schedules).

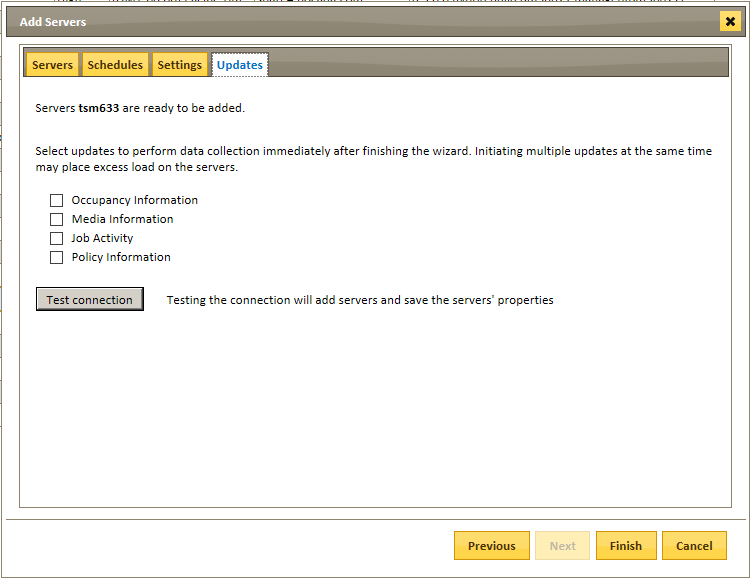


Setting the timespan for initial data collection, the DCS name, the level of logging (if any), and the time-span collected and committed in a single chunk, is managed on the *Settings* tab.



**Note:** Setting ‘Debug logging level’ should be set at ‘Disabled’ unless there are collection issues, as the log files can take up considerable server space if not pruned regularly. In the event of collection issues, please contact [Bocada Support](#_Bocada_Customer_Support).

The final tab, *Updates*, allows you to run data collection immediately, regardless of the schedule for the server configured. Selecting the Test Connection button will test the connection to the server using the names and credentials supplied in the wizard. Note: It is advisable to test the connection for each new server added, and refresh until the status shows ‘Successful’.



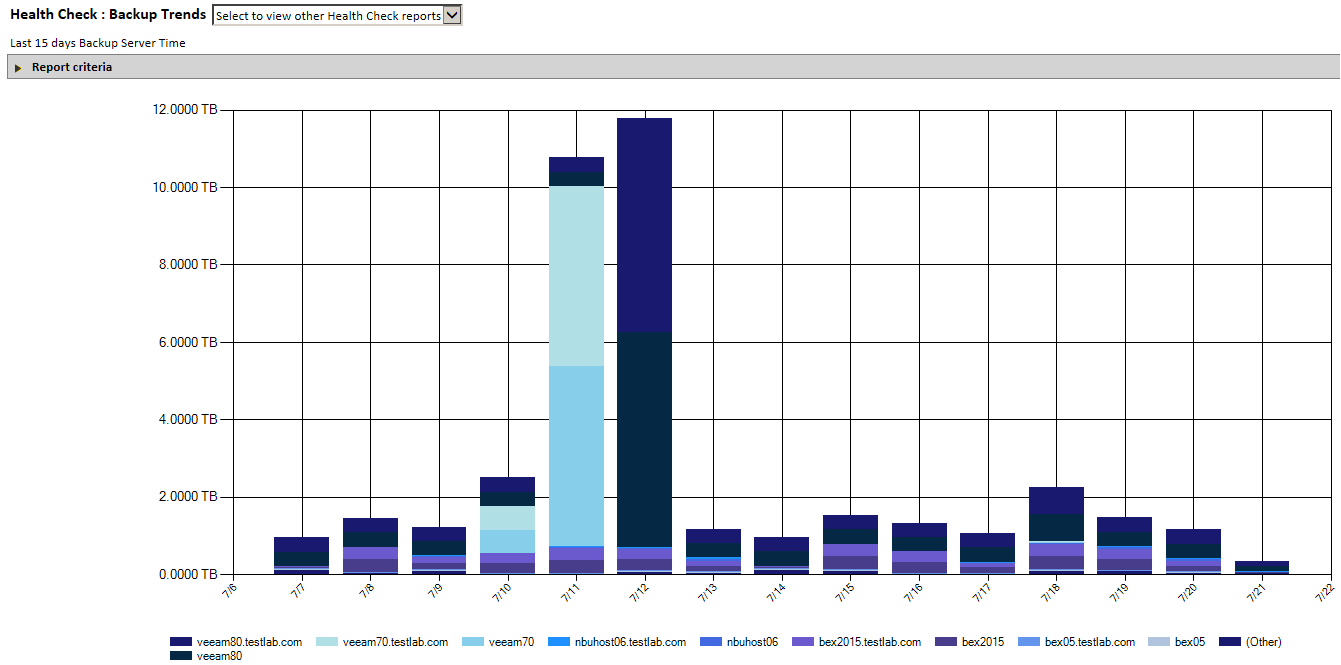
**Edit a Server:** Selecting a server and then selecting the Edit action will open the Edit Servers wizard. This is functionally identical to the Add Server wizard, above.

**Remove a Server:** Selecting a server and then selecting the Delete action will remove a server and all its settings from the list.

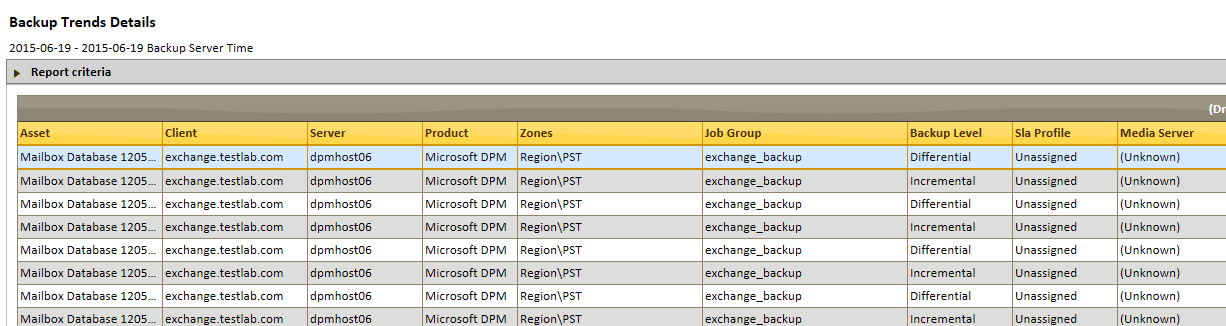
**Assign Data Domain:** See the *Bocada Administration Guide* for details on this action.

## Backup Trends

*Backup Trends* displays the count over time of bytes transferred by successful backup jobs. This helps to determine the demands placed on system resources by a variety of objects including backup servers, backup clients, and assets, in the form of a bar chart:

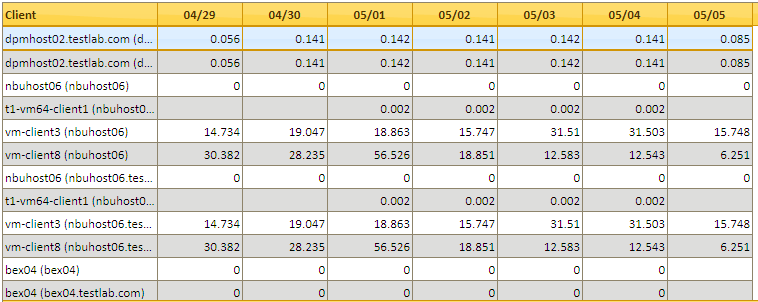


Clicking on a bar will display the details contributing to the byte count for that period:



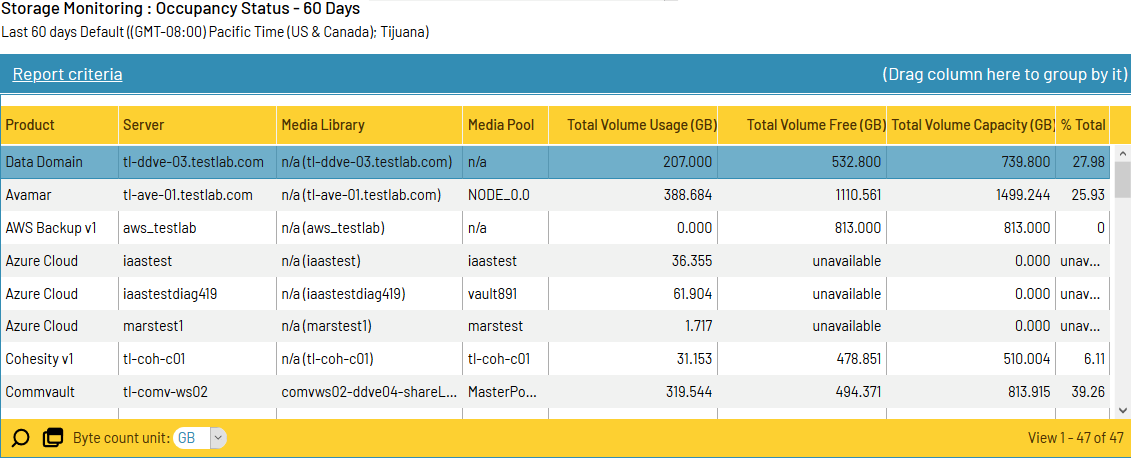
## Backup Trends Details

*Backup Trends Details* displays in table format the same data as the *Backup Trends* graphical report: the trend over time of bytes transferred to determine the demands placed on system resources by a variety of objects including backup servers, backup clients, and assets, in tabular form. Failed backup jobs are ignored in this report:



## Storage Servers

*Storage Servers* provides details on storage usage and storage capacity by backup server.



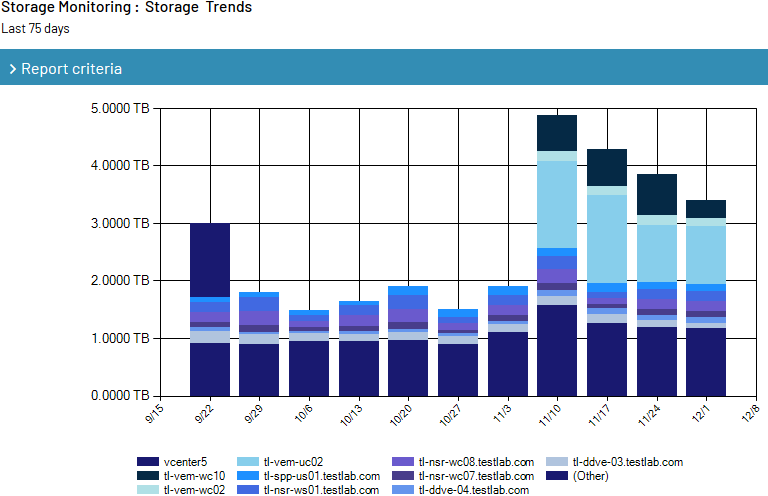
Storage usage can be displayed for the entire environment, specific backup servers or media libraries, or for particular media pools whether cloud, disk, or tape. The report allows users to view how available tape capacity is used, to determine whether sufficient media volumes are available, and to identify conditions such as full or frozen volumes.

## Storage Clients

Similar to *Storage Servers*, this report splits out capacity data at the Client level.

## Storage Trends

*Storage Trends* displays the amount of unexpired data that is available for restore, trended over time, in the form of a bar chart.Each bar in the chart represents the total amount stored per grouping, per day, week or month. Grouping can be done by Application, Media Pool, Backup Server, etc. This report makes it possible for a user to assess the current level of disk or tape library utilization and anticipate the need for future drives by measuring changes in usage over time:



Clicking on a bar will drill down and display the details contributing to the byte count for that time period.

## Storage Trends Tabular

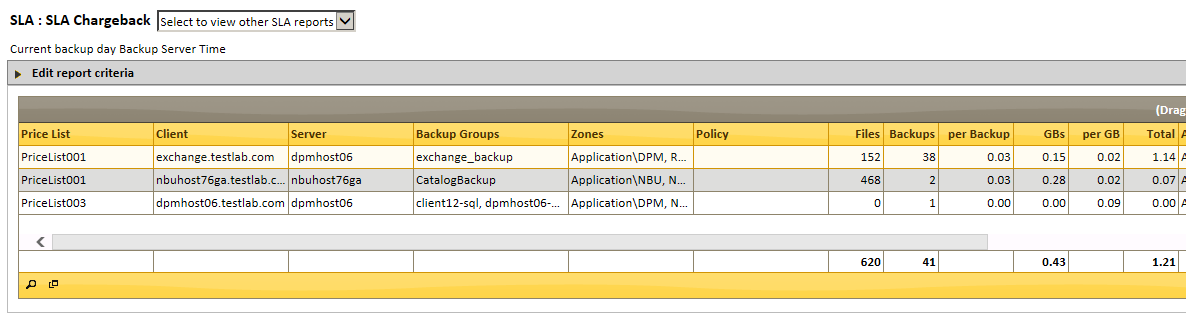
*Storage Trends Tabular* displays the amount of unexpired data that is available for restore just as the Storage Trends report does, in a tabular report format.

## Change Analysis (NBU / Spectrum Protect)

*Change Analysis* highlights the changes to individual NBU or Spectrum Protect (TSM) policies over time. For instance, creating a new policy, assigning/removing a client to a policy, or a schedule change will appear here, allowing users to see impacts of such policy changes.

## Chargeback

*Chargeback* displays a report of the backups performed on a client within that client’s designated SLA for that client’s designated Price List, and provides subtotals and totals:



## Cohesity Storage Domains

Found in Storage. Cohesity Storage Domains shows the basic configuration information, namely the storage capacity and storage capacity used for Cohesity’s configured storage domains.

## Consecutive Failures

*Consecutive Failures* highlights the daily backup jobs for targets which have failed for a specified number of consecutive days (defined in the report criteria) since the most recent success. This report is a subset of the Job Trends report so please see documentation on the Job Trends report. The overall date range must be longer than the number of consecutive failure days that are checked for.

You can also configure the report to detect missing or “no attempt” backups. When you do that, the current day (today) in a last N days report will not count the final day as a missed backup because the backup for that day may not have run yet. The backup target must have had at least one attempt in the overall date range.

## Executive Summary Report

*Executive Summary* rolls up a variety of backup statistics across chosen time periods, serving as an assessment of a backup environment for measures such as amount of data backed up, number of backup servers and clients in the environment, and percent of successful backup jobs. Some of the columns in the Executive Summary report include:

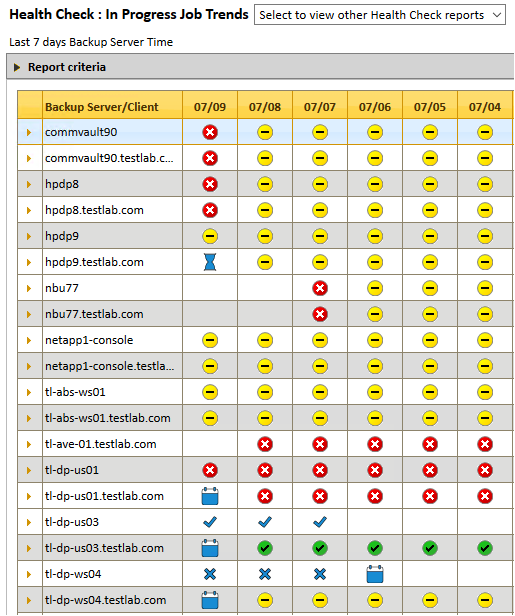
**% Target Success**: This is calculated using the result of the job using the best attempt per backup target per day logic. For example, suppose that you have a schedule where on each day if 10 targets were backed up multiple times per day. On a particular day, if 9 targets had both some successful jobs and some failure jobs ,and one target had only failed jobs, then your *% Target Success* is 90 percent.

## In Progress Job Trends

The *In-Progress Job Trends* report displays the currently running, pending, and expected jobs, as well as the status of those jobs over time as they complete, and their status is resolved to Success/Partial Success/Failure.

The In-Progress reports introduce new icons for new job Statuses, as shown in the table below:

|  |  |  |
| --- | --- | --- |
| Icon | Status | Long description also shown in Mouseover |
| cid:image001.png@01D48730.52B34F90 | Failed | Backup has failed.  Run backup data collection to get more details. |
| cid:image002.png@01D48730.52B34F90 | Future | Next-future jobs scheduled to run. |
| cid:image003.png@01D48730.52B34F90 | Running | Backup is running. |
| cid:image004.png@01D48730.52B34F90 | Missed window | Backup failed due to missed backup window.  Run backup data collection to get more details. |
| cid:image005.png@01D48730.52B34F90 | Severed | Backup failed due to severed network connection.  Run backup data collection to get more details. |
| cid:image006.png@01D48730.52B34F90 | Pending | Backup is queued by schedule but has not started. |
| cid:image007.png@01D48730.52B34F90 | Restarted | Backup was restarted and is running. Run backup data collection to get more details. |
| cid:image008.png@01D48730.52B34F90 | Successful | Backup has successfully completed.  Run backup data collection to get more details. |

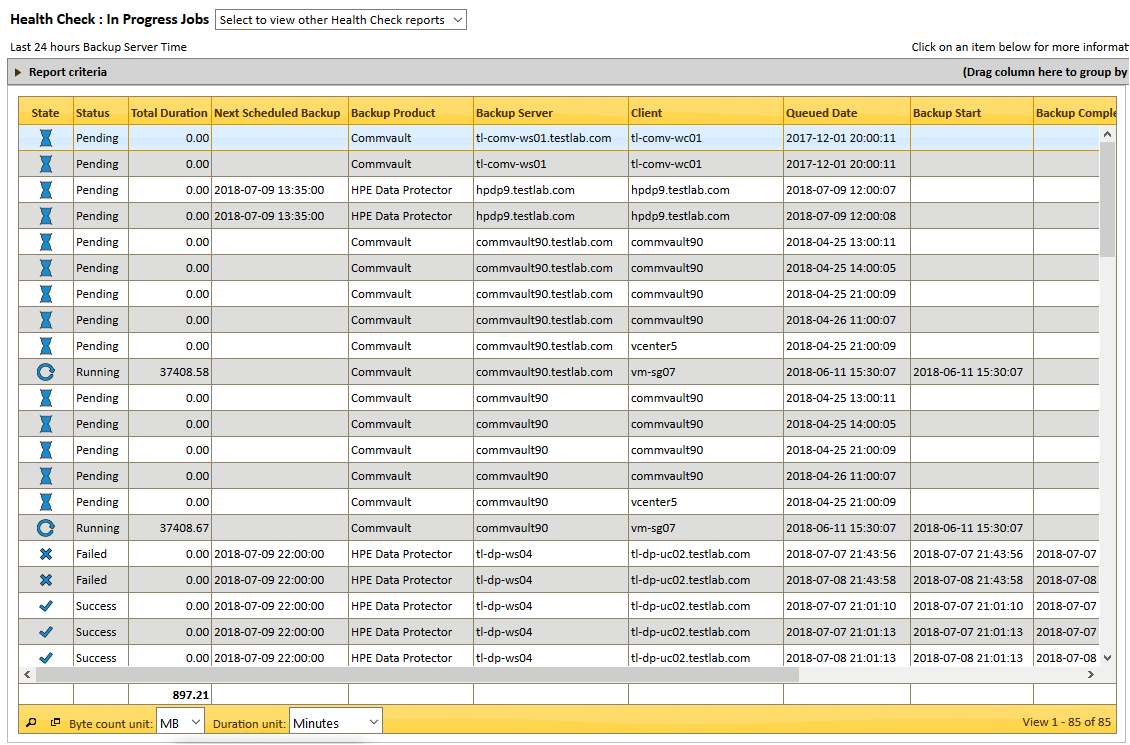


## In Progress Jobs

The *In-Progress Jobs* report displays a tabular report of currently running, pending, and expected jobs.

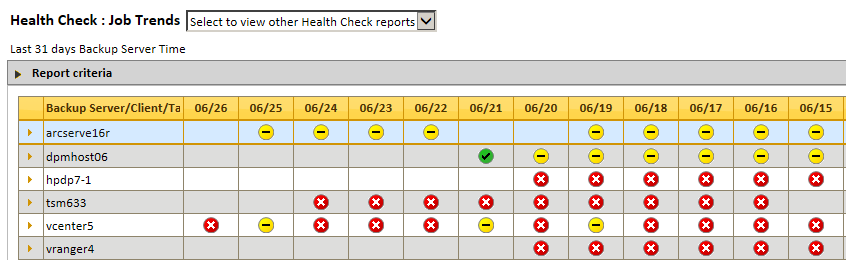
The selectable status criteria for *In-Progress Jobs* are different than the Success/Partial/Failure status seen for most other reports. See section above for the meaning of the new outcome statuses.

*Note:* The In-Progress Jobs report only displays the most recent Active jobs per server or client, as there may be many of these expected or running at the same time.



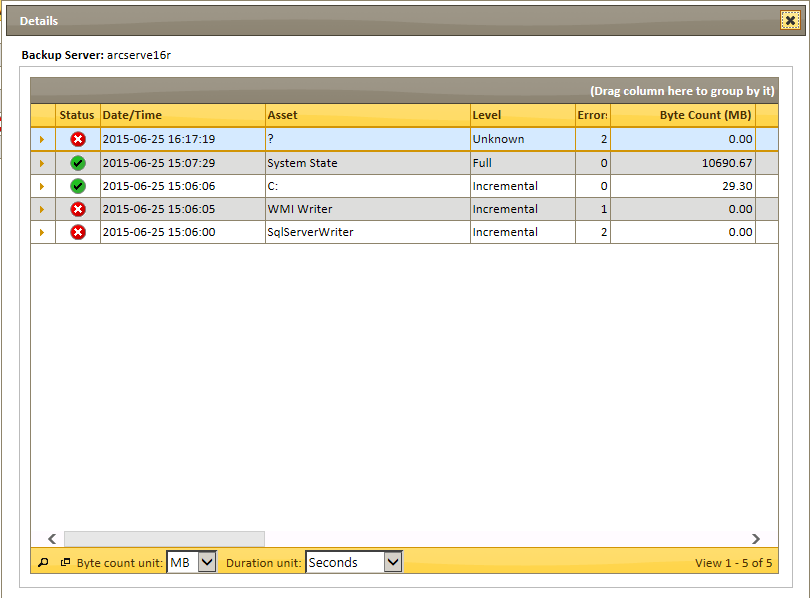
## Job Trends

*Job Trends* displays the daily failed, successful, and partially successful backup jobs, to highlight systemic backup problems in easily scanned matrices of backup servers, clients, and targets. Backup error trends become clear, allowing users to identify problems and take corrective action.



This report can be grouped up to four levels and is grouped by Backup Server/Client/Target by default.

Select any circle icon to drill into the Details for that backup job:



Expanding the Status on job details exposes the messages generated by the backup job.

## NBU Clients

Found in Policies. *NBU Clients* lists backup clients assigned to NetBackup Policies along with related client details.

## NBU Configuration

Found in Policies. *NBU Configuration* displays details of NetBackup Policies. Select any policy to get further details on that policy. (Note: Policy Type includes an internal type identifier in parenthesis, not to be confused with quantity.)

## NBU Lifecycle

Found in Policies. *NBU Lifecycle* displays the daily successful, partially successful, or failed results of NetBackup lifecycle activities; red or yellow status icons indicate that a job failed at one or all stages of the data protection lifecycle. By default, this report is grouped to four levels, by Backup Server/Policy/Client/Schedule.

## NBU SLP Trends

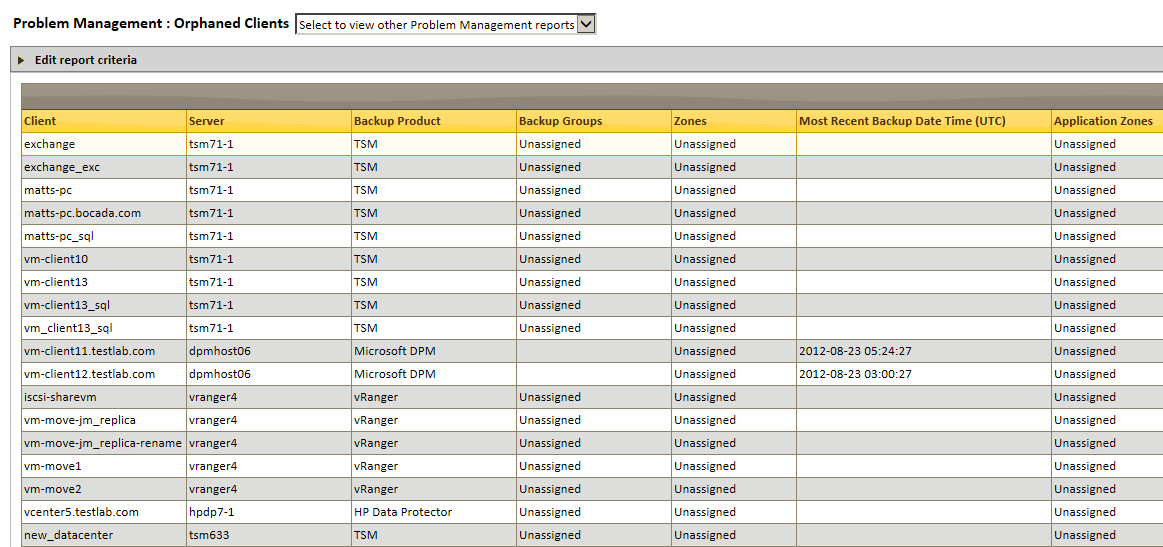
Found in Policies. *NBU SLP Trends* shows the daily trend of successful, failed and partially successful results of NetBackup Lifecycle Policies in the form of a bar chart. Clicking on a bar will display the NBU Lifecycle report for the day clicked.

## NBU SLP Configuration

Found in Policies. *NBU SLP Configuration* displays a list of NetBackup Storage Lifecycle policies along with a detail of each one when selected.

## Orphaned Clients

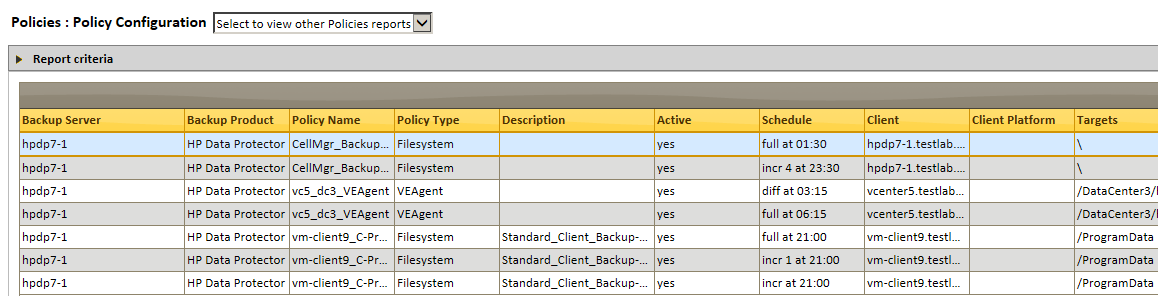
*Orphaned Clients* is a report of those clients which are mined from a backup server, yet have no backup jobs mined for them:



For instance, clients may be registered with a backup server yet have no backup policy assigned, or may have been decommissioned yet not removed from the backup server.

## Policy Configuration

Found in Policies. *Policy Configuration* displays backup configuration (policy) details for backup products supported with Bocada policy updates.



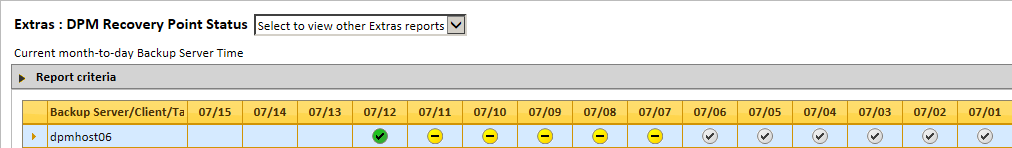
Spectrum Protect (TSM) and NetBackup policy information is contained in the [Policies](#_Policies) Module, but in separate reports for those products, and that information is not included in this report.

## Policy Clients

Found in Policies. *Policy Clients* displays backup clients assigned to policies for backup products supported with Bocada policy updates. If a client is associated to more than one policy, that client will appear more than once. Spectrum Protect (TSM) and NetBackup policy information is contained in separate reports and is not included in this report.

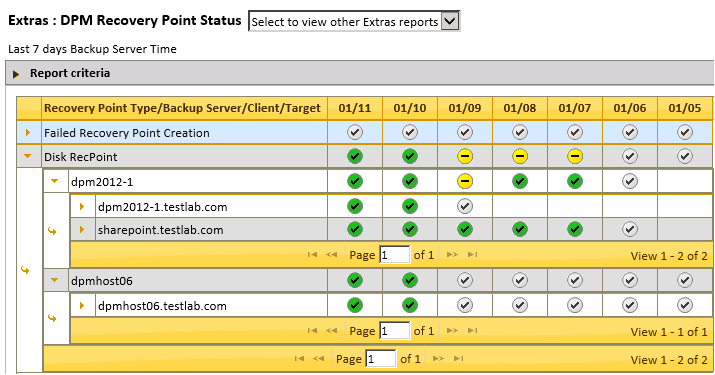
## Azure / DPM Recovery Point Status

Found in Backup Activity, these reports are specifically tailored to Microsoft Data Protection Manager (DPM). *DPM Recovery Point Status* displays current recovery point information for each target protected by DPM:



The report grouping is selected through criteria settings and may be grouped by server, client, recovery point type, protection group, or target. Select any status icon to drill into details for that backup.

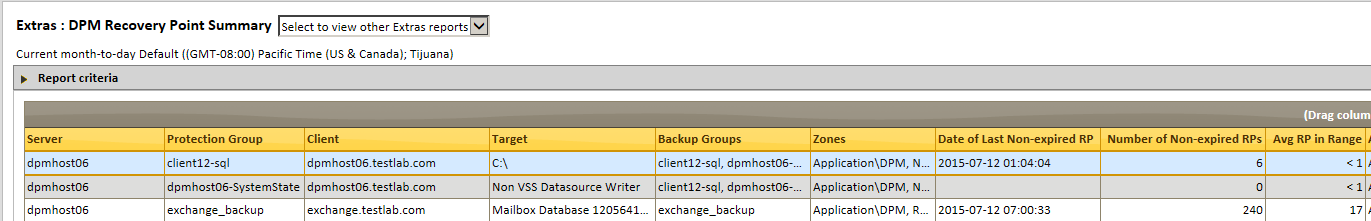
In addition to the usual colored success indicators (green = successful, yellow = partial success, red = failed) the Recovery Point Status also includes a gray indicator for those recovery points which have expired. Note that any expired Recovery Points are treated as failures for roll-up purposes, so that the report will display Green + Gray = Yellow.



Also note that the Recovery Point Status changes as currently successful recovery points become expired.

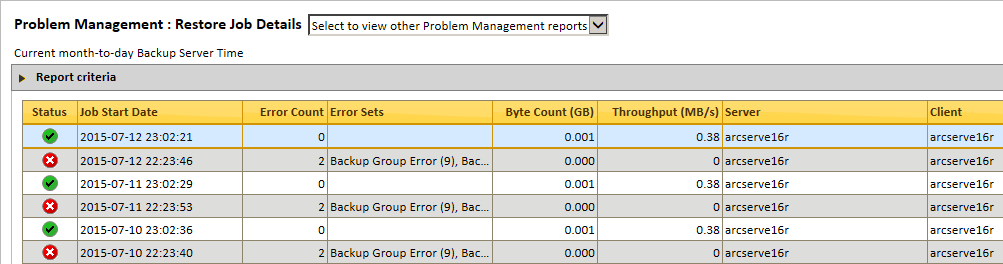
## Azure DPM Recovery Point Summary

Found in Backup Activity, these reports are specifically tailored to Microsoft Data Protection Manager (DPM). *DPM Recovery Point Summary* displays the status of DPM recovery points including whether each recovery point is expired. This report can be grouped up to four levels and is grouped by Server/Client/Target by default:



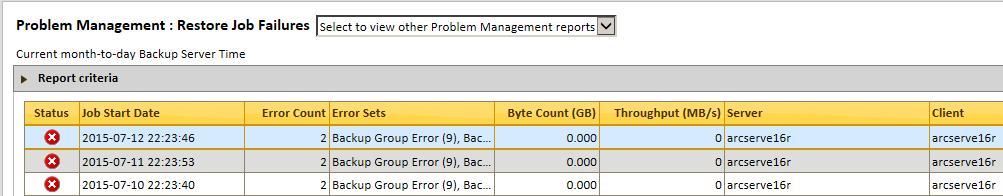
## Restore Activity

Found in Backup Activity. *Restore Activity* lists restore attempts matching selected criteria over configurable periods of time:



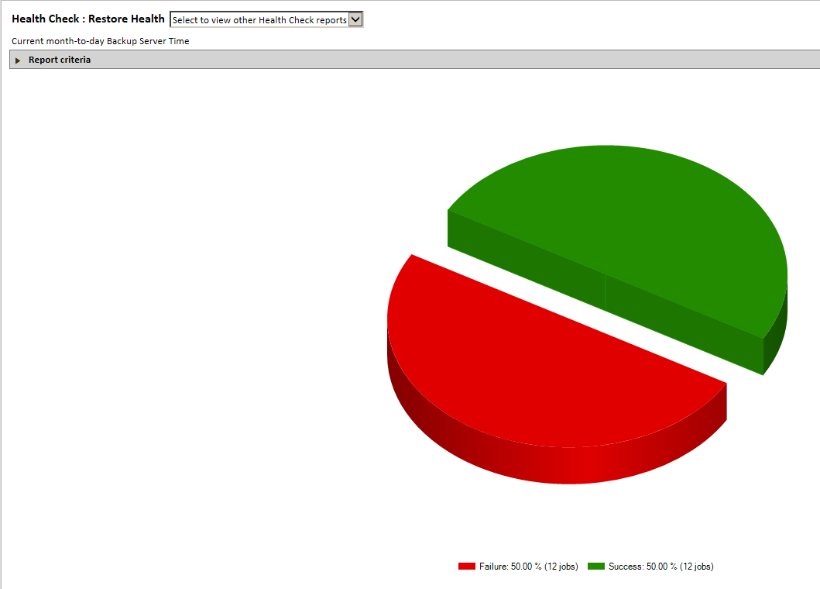
## Restore Failures

Found in Backup Failures. *Restore Failures* is a subset of Restore Activity that displays only failed and partially successful restores:



## Restore Health

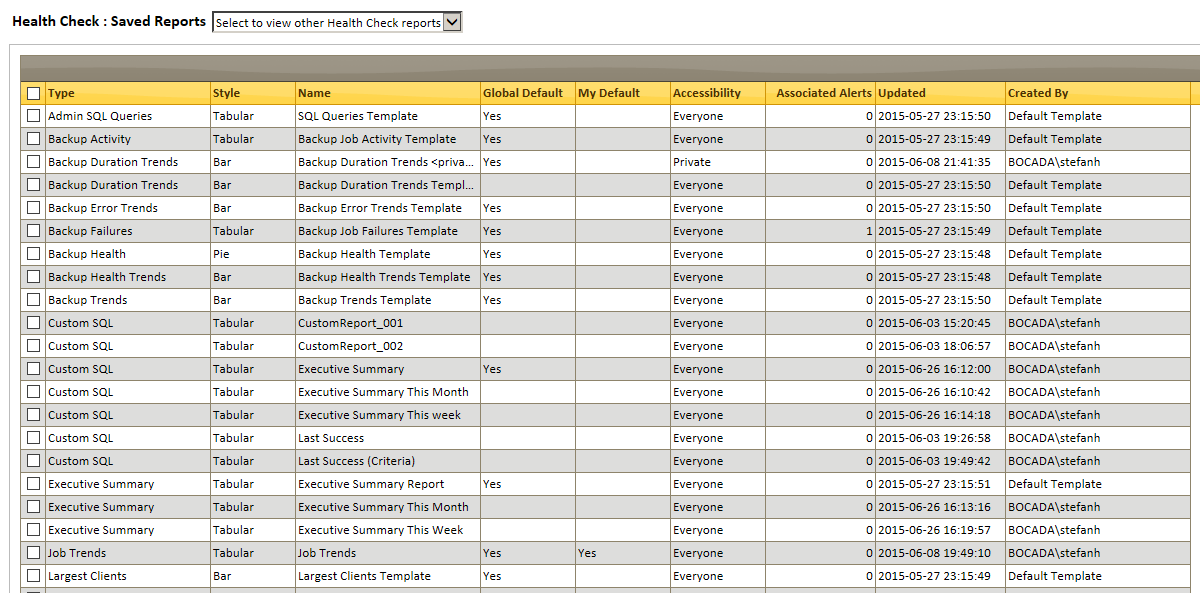
Found in Backup Activity. *Restore Health* shows the percent of restores that are successful, partially successful and failure in the form of a pie chart.



Clicking on a section of the pie will take users to the related granular job details in Restore Activity.

## Saved Reports

Found under Home. *Saved Reports* is a central interface for and running and managing reports with previously saved criteria.



This view also provides the capability to create, modify and delete Custom SQL reports.

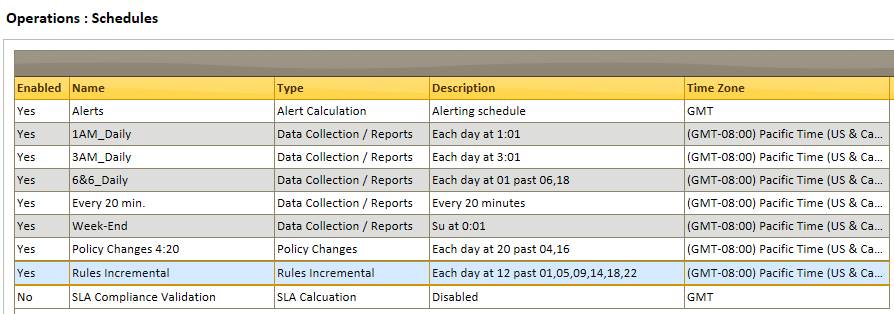
To create a new report, select the New Custom Report icon from the right Action panel. This will launch an Edit wizard to allow you to insert custom SQL code for this report.

However, you cannot change which is your default report in this view, only see which your default for each report type. To change your default report of any type, go to that report type and follow the instructions for saving a report elsewhere in this document.

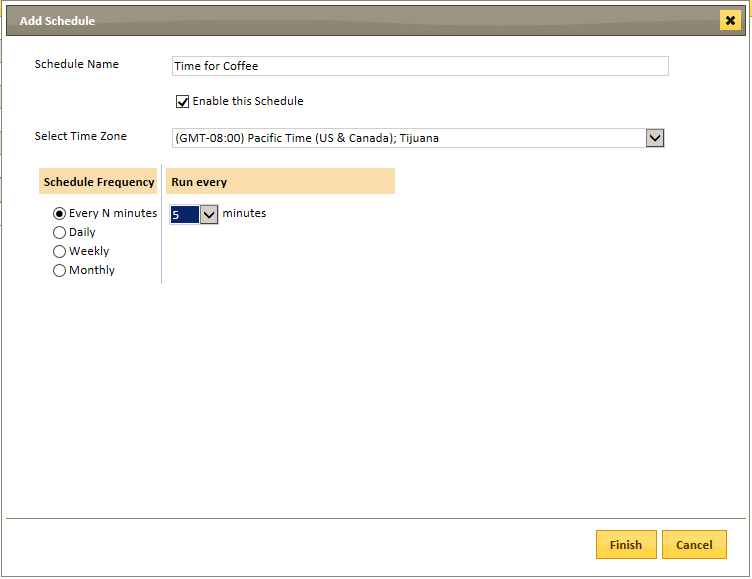
Reports that are saved can also be accessed via the folder icon from each report.

## Schedules

Found in Configuration > Advanced Config. *Schedules* lists the schedules that have been established for various events to occur at set times. This view can be used to manage existing schedules, add new schedules of various types, or remove unneeded schedules. Schedules can be sorted by Enabled, Name, Type (default), Description, Schedule ID or Time Zone.



To add a Data Collection / Reports schedule, select the Add action from the right Action Panel. The Add Schedule wizard will appear:



Give your schedule a Name, Time Zone, and select the Frequency. Options appear depending upon the frequency:

* **Every N minutes:** Run every 5, 10, 15, 20, 30, 45, 60, 90, 120, 180, 240 minutes.
* **Daily:** At these times (select hours to initiate), Run at (select minutes after the hour(s) selected).
* **Weekly:** On these days (select days of the week to initiate), Run at (select hours and minutes on the day(s) selected).
* **Monthly:** On these days (select Nth day of the month or the Nth Day of week (e.g., First Saturday of a month)), Run at (select hours and minutes on the day(s) selected).

Edit Schedule: Select any schedule, then select the Edit action from the right Action Panel. Options as Add Schedule, above.

Delete Schedule: Select any schedule, then select the Delete action from the right Action Panel. **Warning:** Any activity that was scheduled according to a Schedule that has been deleted will revert to Unscheduled.

Note: The Schedules report also includes the Action “Pause / resume all schedules”.

## Scheduled Actions

Found in Configuration > Advanced Config. *Scheduled Actions* lists the schedules that have been established for various events to occur at set times. This view can be used to manage existing schedules, add new schedules of various types, or remove unneeded schedules.

## Scheduled Report Management

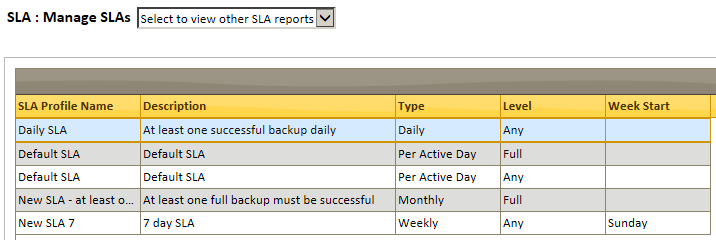
Found in [Operations](#_Operations). *Scheduled Report Management* lists the configurations of reports that have been associated with a schedule. This view can be used to view and manage which reports are being emailed (and to whom) and / or exported (and to where), and in what format the report is sent.

This report displays and allows for editing of scheduled report configuration properties, including:

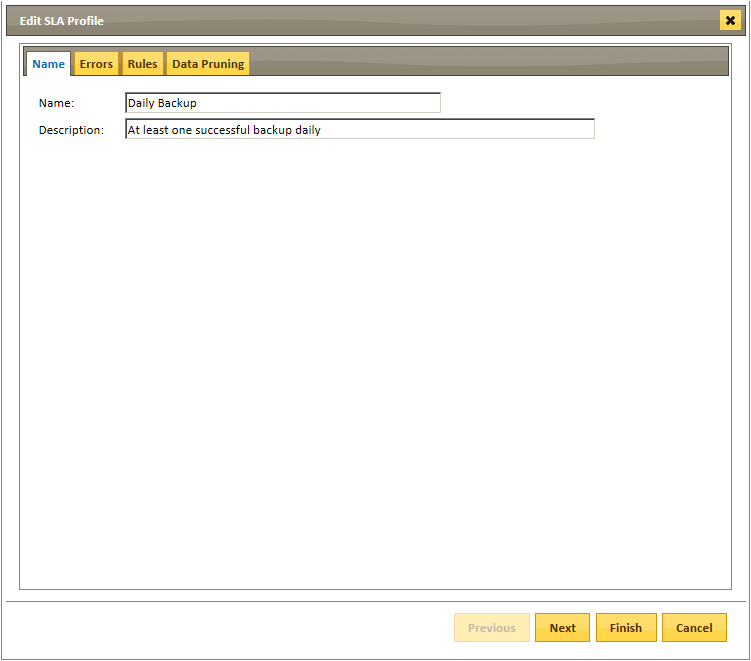
* Status of most recent attempt and last error if any.
* Configuration Name.
* Report Type.
* Report Name.
* Types of files for export, if any.
* If email is configured and to which addresses.
* Export location.
* Schedule name and description.
* User that configured the scheduled report.

## SLA Config

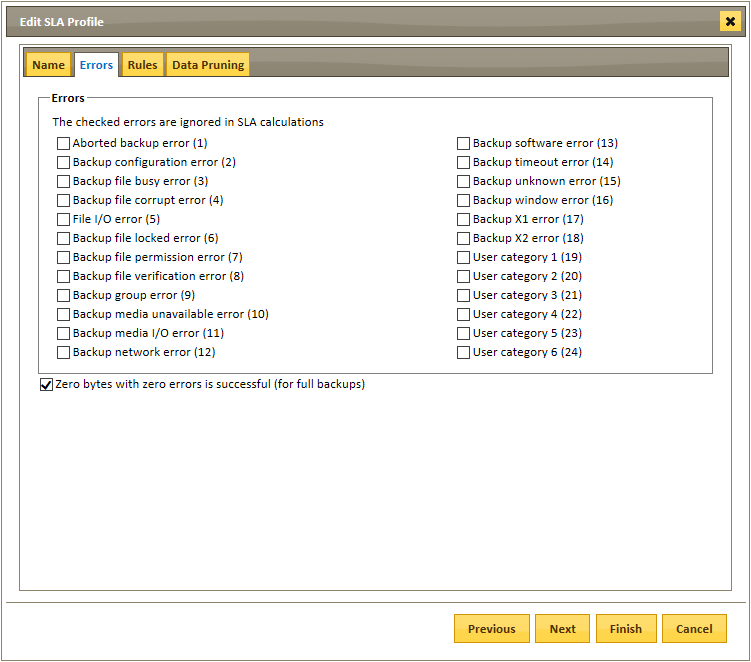
Found in SLA. *SLA Config* allows Administrators to establish and edit SLA Profiles. Note that two rows may appear for the same profile, one for each frequency you define:



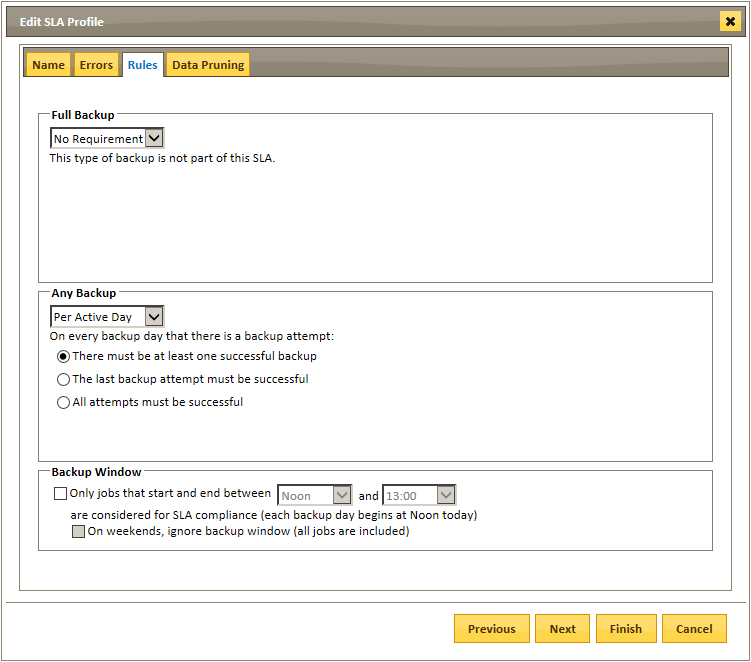
To configure a new SLA profile, select the Add action from the right Action panel. This will open the Add SLA Profile wizard:



On the Name tab, enter a Name (required) and Description for this profile, then click *Next*.



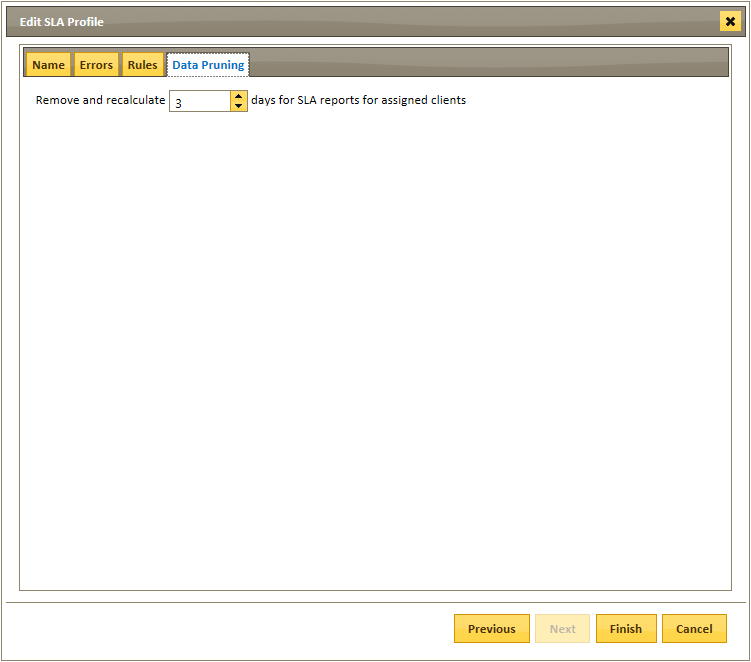
On the Errors tab, designate any errors which are to be ignored under this profile.



On the Rules tab, select the criteria for compliance with the SLA:

* Full or Any Backup
* Per Active Day (per day a backup is attempted), Daily (designate specific days), Weekly (designate specific days), or Monthly
* Backup Window (designate specific backup times). For instance, you can create a profile to monitor clients that are expected to successfully complete at least one Full Backup each Sunday between Midnight and 2 a.m.

On the Data Pruning tab, select the number of days to remove and recalculate clients. This should be set for longer than the longest backup, i.e. at least 7 days for a weekly requirement, or at least 31 days for a monthly requirement. If set for less than the SLA duration, some clients with backup attempts may appear as “No Backup Attempts Yet” in SLA reporting.



Once configured here, SLA Profiles may be assigned to clients, prior to running SLA Compliance Reports.

Note: The schedule *SLA Compliance Validation* is enabled by default and set to run daily at 0:00.

For further information on SLA monitoring, please see the *Bocada* *Administration Guide*.

## SLA Impacts

Found in SLA. *SLA Impacts* provides an overview of those jobs which are affecting SLAs as defined in *SLA Config*. This report lists each client’s non-compliant asset that the pre-defined SLA the client is associated with, and the reason the asset is not meeting compliance.

## SLA Metrics

Found in SLA. *SLA Metrics* displays a report of SLAs as defined in *SLA Config*, and how well those SLAs are fulfilled.

## SLA Trends

Found in SLA. *SLA Trends* displays the trend over time of SLAs that are met or not met in the form of a bar chart.

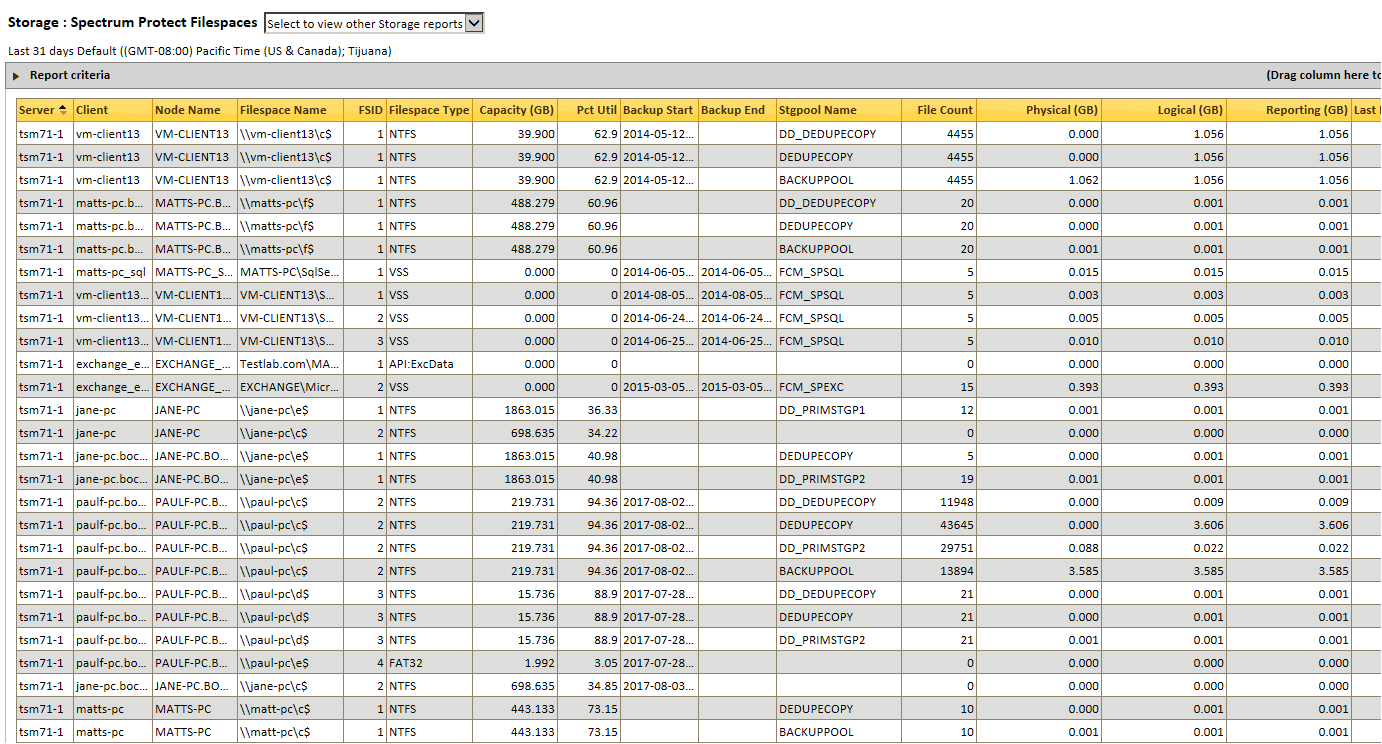
## Summary (Dashboard)

Under Home. *Summary* provides an overview of the backup environment by displaying up to four graphical reports in one window.

To customize the reports in your Summary, select the Customize icon from the right Action panel. This will launch the Customize wizard. See [Customize](#_Customize_Dashboards_–) for details.

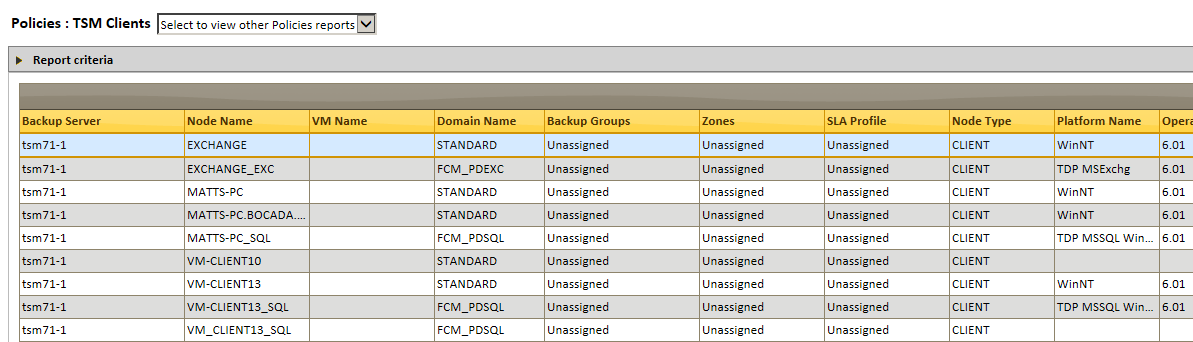
## Spectrum Protect Filespaces

Found in Storage. The *Spectrum Protect Filespaces* report is a tabular view of the space protected on Spectrum Protect (TSM) client servers, by node, filespace name, and storage pool name, according to Spectrum Protect (TSM) Filespace queries. Includes query results for capacity, percent utilized, and Physical vs. Logical space.



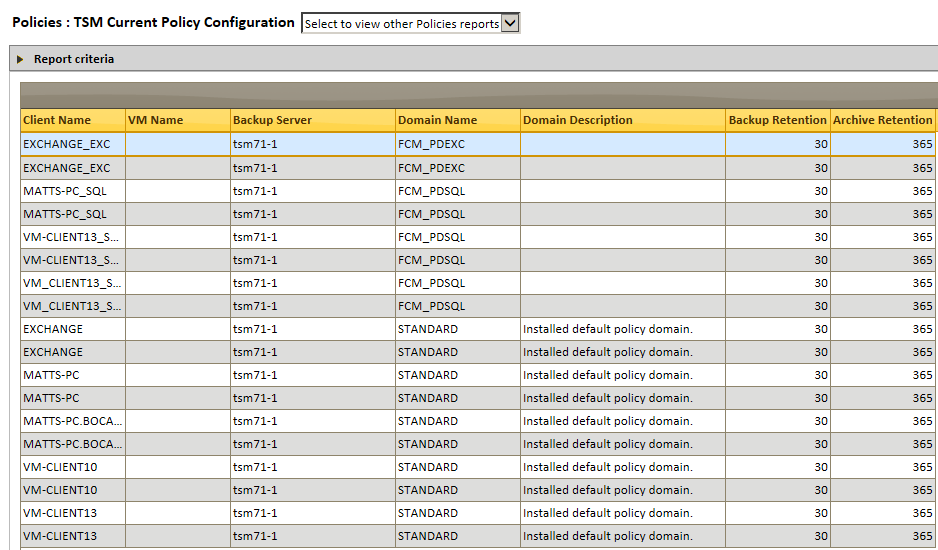
## Spectrum Protect Clients

Found in Policies. *Spectrum Protect Clients* lists backup clients assigned to Spectrum Protect policies, along with related client details. This report uses the TSM\_policy\_nodes table and the most recent snapshot per Spectrum Protect (TSM) server to provide data.



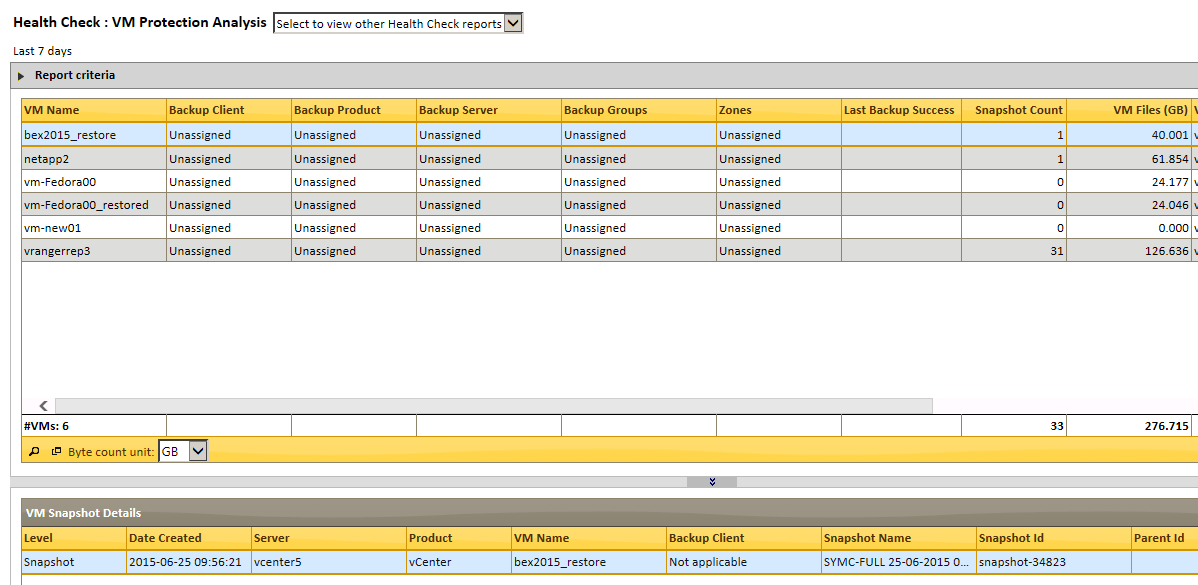
## Spectrum Protect Configuration

Found in Policies. *Spectrum Protect Configuration* displays the Spectrum Protect (TSM) policy configurations of Spectrum Protect servers: What policies are configured, policy domain, domain retentions, and domain archive values, as well as other Spectrum Protect policy-related information.



## VM Protection Analysis

*VM Protection Analysis* provides an overview of the VMs used and shows data protection status for each, with indication if a VM is protected by snapshots, backup applications, or is unprotected. When a client is highlighted in the upper panel, the lower panel will show all snapshots and /or backups that are being run against the client within the date range selected in report criteria.



Note: The Bocada VM Protection Analysis and Licensing reports reference Unassigned VMs.  Unassigned VMs are Virtual Machines for which Bocada does not have a record for being backed up as a full Virtual Machine backup.

VM Protection Analysis provides virtual reporting for Backup Exec, CommVault, Data Protector, IBM Spectrum Protect (TSM), NetBackup, and Veeam. VMs that are backed up by traditional physical machine methods will be reported in non-virtual reports and as non-virtual backup clients.

# Support

## Bocada Customer Support

E-mail: [support@bocada.com](mailto:support@bocada.com)

Phone: 425-898-2400

Both new and existing customers, who have purchased annual support and maintenance, have full access to post-installation support:

* Online knowledge base and problem ticketing system
* E-mail and toll-free telephone assistance Monday through Friday, 6 a.m. to 6 p.m. Pacific, US Time (except holidays)
* Product documentation and documentation updates
* Program error fixes, hotfixes, and service packs
* Product upgrades for the Bocada application

To access the support portal, click on “Customer Support Portal” from the following URL <https://www.bocada.com/product-support/>

## Bocada Professional Services

Bocada offers Professional Services assistance for installation and continuing support of our products. Bocada solutions are built with an open architecture that allows for custom reporting and integration with third party solutions, please consult with our sales or support team to determine if your organization would benefit from Bocada Professional Services.

* Backup Assessments (delivered by Value Added Partners)
* Deployment Planning and Guided Assistance
* Migrations
* Training
* Custom Report Design, Review and Delivery
* Installation and Configuration

# Appendix A: Reporting Module Access

X = can perform action

P = can perform action on universal and Private Reports

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Reports** | **Action** | **Administrator** | **Operator** | **Standard User** |
| Summary | Refresh | x | x | x |
| Export | x | x | x |
| Send by Email | x | x |  |
| Customize | x | P |  |
| Saved Reports | Refresh | x | x | x |
| Run Report | x | x | P |
| Save Default View | x |  |  |
| Delete | x | P | P |
| Re-Assign Saved Report Owner | x |  |  |
| Edit Criteria | x | P | P |
| Executive Summary, Annotations, Backup Alert Activity, Chargeback Job Trends, Backup Health, Backup Health Trends, Backup Trends, Backup Trends Details, Backup Duration Trends, Restore Health, Orphaned Clients, Azure/DPM Recovery Point Summary, Azure/DPM Recovery Point Status, Consecutive Failures, Failure Trends, Backup Error Trends | Run Report | x | x | x |
| Open | x | x | x |
| Save Report | x | x | x |
| Export | x | x | x |
| Send by Email | x | x |  |
| Schedule Report | x | x |  |
| Job Activity, Restore Activity, Backup Failures, Restore Failures | Run Report | x | x | x |
| Open | x | x | x |
| Save Report | x | x | x |
| Export | x | x | x |
| Send by Email | x | x |  |
| Schedule Report | x | x |  |
| Add Annotation | x | x |  |
| Find Annotations | x | x | x |
| SLA Impacts | x | x | x |
| Add Alert | x | x |  |

## Storage

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Reports** | **Action** | **Administrator** | **Operator** | **Standard User** |
| Storage Trends, Storage Servers, Storage Clients, Media Usage Trends, Most Used Volumes, Data Domain Capacity | Run Report | x | x | x |
| Open | x | x | x |
| Save Report | x | x | x |
| Export | x | x | x |
| Send by Email | x | x |  |
| Schedule Report | x | x |  |

## vCenter

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Reports** | **Action** | **Administrator** | **Operator** | **Standard User** |
| VM Protection Analysis | Run Report | x | x | x |
| Open | x | x | x |
| Save Report | x | x | x |
| Export | x | x | x |
| Send by Email | x | x |  |
| Schedule Report | x | x |  |

## Policies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Reports** | **Action** | **Administrator** | **Operator** | **Standard User** |
| Policy Configuration, Policy Clients, Spectrum Protect Configuration, Spectrum Protect Clients, NBU Configuration, NBU Clients, NBU SLP Configuration, NBU SLP (Lifecycle), NBU SLP Trends, Change Analysis | Run Report | x | x | x |
| Open | x | x | x |
| Save Report | x | x | x |
| Export | x | x | x |
| Send by Email | x | x |  |
| Schedule Report | x | x |  |

## SLA

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Reports** | **Action** | **Administrator** | **Operator** | **Standard User** |
| SLA Trends, SLA Metrics, SLA Impacts | Run Report | x | x | x |
| Open | x | x | x |
| Save Report | x | x | x |
| Export | x | x | x |
| Send by Email | x | x |  |
| Schedule Report | x | x |  |
| SLA Configuration | Add | x |  |  |
| Edit | x |  |  |
| Archive | x |  |  |
| *Assign Clients* | x |  |  |
| *Unassign Clients* | x |  |  |

## Operations

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Reports** | **Action** | **Administrator** | **Operator** | **Standard User** |
| Data Collection | Refresh | x | x |  |
| Open | x | x |  |
| Save Report | x | x |  |
| Run Manual Updates | x | x |  |
| Cancel Updates | x | x |  |
| Edit Server | x |  |  |
| Export | x | x |  |
| Send by Email | x | x |  |
| Schedule Report | x | x |  |
| Backup Servers | Refresh | x | x |  |
| Add | x |  |  |
| Delete | x |  |  |
| Edit Server | x |  |  |
| Export | x | x |  |
| Open | x | x |  |
| Save Report | x | x |  |
| Export | x | x |  |
| Send by Email | x | x |  |
| Schedule Report | x | x |  |
| Backup Clients | Run Report | x | x |  |
| Open | x | x |  |
| Save Report | x | x |  |
| Export | x | x |  |
| Send by Email | x | x |  |
| Schedule Report | x | x |  |
| Client Properties | x | x |  |
| Ignore Client | x |  |  |
| Run Rules | x |  |  |
| Data Collection Alert Activity, Data Collection Servers, Backup Server Activity, | Run Report | x | x |  |
| Open | x | x |  |
| Save Report | x | x |  |
| Export | x | x |  |
| Send by Email | x | x |  |
| Schedule Report | x | x |  |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Reports** | **Action** | **Administrator** | **Operator** | **Standard User** |
| Schedules | Run Report | x | x |  |
| Open | x | x |  |
| Save Report | x | x |  |
| Export | x | x |  |
| Send by Email | x | x |  |
| Schedule Report | x | x |  |
| Add | x | x |  |
| Delete | x | x |  |
| Edit | x | x |  |
| Scheduled Actions | Refresh | x | x |  |
| Open | x | x |  |
| Save Report | x | x |  |
| Cancel Action | x | x |  |
| Export | x | x |  |
| Send by Email | x | x |  |
| Schedule Report | x | x |  |
| Scheduled Report Management | Run Report | x | x |  |
| Open | x | x |  |
| Save Report | x | x |  |
| Export | x | x |  |
| Edit Configuration | x | x |  |
| Delete | x | x |  |
| Alert Configuration | Add | x | x |  |
| Delete | x | x |  |
| Edit | x | x |  |
| Export | x | x |  |
| Send by Email | x | x |  |
| Schedule Report | x | x |  |

## Administration

All reports and actions in this module are accessible to Administrators only and will not be visible to Operators or Standard Users.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Reports** | **Action** | **Administrator** | **Operator** | **Standard User** |
| All Reports | All Actions | x |  |  |

**Copyright © 2022 Bocada LLC.** All Rights Reserved. Bocada and BackupReport are registered trademarks of Bocada LLC. Vision, Prism, vpConnect, and the Bocada logo are trademarks of Bocada LLC. Other product names mentioned herein may be trademarks or registered trademarks of their respective companies.

Protected by U.S patents 6,640,217; 6,708,188; 6,745,210; 7,457,833; 7,469,269; 7,496,614; 8,407,227

The material in this manual is for information only and is subject to change without notice. While efforts have been made to ensure accuracy, Bocada LLC assumes no liability resulting from errors or omissions in this document, or from the use of information contained herein.

Bocada LLC reserves the right to make changes in the product design and documentation without reservation and without notification to its users. 2022-05-12