

Configuration Guide

Front Office for NetBackup v2

Guide to assist installation and configuration of the Front Office for NetBackup solution

Contents

1.0	Introduction.....	5
1.1	Overview of how the solution works	5
1.2	Selecting the right solution for your needs	5
2.0	Installation.....	6
2.1	Installation Checklist.....	6
2.2	Installation Overview.....	6
2.3	Pre-Requisites.....	7
2.4	Installing the Front Office Portal	7
2.5	Installing the Front Office for NetBackup Adapter.....	7
2.5.1	Extract Files.....	7
2.5.2	Create the Database	8
2.5.3	Create an Application Pool	8
2.5.4	Configure the Panels	8
2.5.5	Configure the Services.....	8
2.5.6	Encrypting Config Files	9
3.0	NetBackup Configuration (pre-requisites)	9
3.1	Setting up Communication with the NetBackup Master Server	9
3.1.1	Communication with a Windows NetBackup Master Server	10
3.1.2	Communication with a Unix NetBackup Master Server.....	10
3.2	Machine Driven NetBackup Template Policies.....	10
3.2.1	Scheduled Backup Policies.....	11
3.2.2	BackupNow Policies.....	11
3.3	vCloud Driven NetBackup Template Policies	12
3.3.1	Scheduled Backup Policy: Template-vCloud.....	12
3.3.2	BackupNow Policy: Template-vCloud-BackupNow	12
3.3.3	Retention Periods	12
3.3.4	vCloud Replication (AIR)	12
4.0	Adapter Configuration for Machine Driven Solutions	13
4.1	Machine Table	13
4.1.1	Column definitions	13
4.1.2	Supported Configurations	14
5.0	Front Office Configuration	14
5.1	Licensing	14

- 5.2 Integration Settings 15
 - 5.2.1 Machine Location Sections 15
 - 5.2.2 vCloud Location Sections 17
 - 5.2.3 Service Levels for Machine Driven Solutions 18
 - 5.2.4 NetBackup Adapter Section 19
- 5.3 Configuring Adapters 19
 - 5.3.1 Securing the Directa API 20
- 5.4 NetBackup Panels 20
 - 5.4.1 Configuring the Panels 21
- 6.0 New Client Take On 22**
 - 6.1 Clients and Users 22
 - 6.1.1 Creating a Client and First User 22
 - 6.1.2 Configuring a client for a Machine Driven Solution 23
 - 6.1.3 Configuring a client for a vCloud Driven Solution 23
 - 6.2 Report panel 23
- 7.0 Testing the Solution 24**
 - 7.1 Run Scheduled Task to populate Client Backup Cache 24
 - 7.2 Checking the Panels 24
 - 7.3 Raising a Request 24
 - 7.4 Troubleshooting 24
- 8.0 Pre-Configured Services in Front Office for NetBackup 24**
 - 8.1 Machine Driven Services 25
 - 8.1.1 “Protect Machine” 25
 - 8.1.2 “Restore VM” 25
 - 8.1.3 “Restore File / Folder” 26
 - 8.1.4 “Backup Now” 26
 - 8.1.5 “Unprotect Machine” 27
 - 8.2 vCloud Driven Services 27
 - 8.2.1 “Protect Machine” 27
 - 8.2.2 “Restore VM” 28
 - 8.2.3 “Restore File / Folder” 29
 - 8.2.4 “Backup Now” 30
 - 8.2.5 “Unprotect Machine” 30
 - 8.2.6 “Register VM for File Restore” 31

8.3	Configuring Retention Levels.....	31
8.4	Restoring to Default	31
9.0	Appendix A: Automating Client and First User Creation	32
10.0	Appendix B: Enabling Remote PowerShell to Multiple Master Servers	33
11.0	Appendix C: Simplifying the Front Office Portal Home Page	34
12.0	Appendix D: Configuring Diagnostic Tracing	35
13.0	Appendix E: Open Source Licenses	36
13.1	JQuery Data Tables	36
13.2	Renci SSH.NET Library.....	36

1.0 Introduction

This document describes the configuration of the Front Office for NetBackup solution.

Please contact Biomni for assistance, if required. The Biomni Community provides an ever increasing set of self-help resources. Support calls can also be logged here, accessible online:
<http://community.biomni.com/home>

1.1 Overview of how the solution works

The Front Office for NetBackup solution presents an end user with options to select a machine, and backup service level they want to apply to that machine. The Front Office adapter then identifies a preconfigured template policy on NetBackup (which will be inactive) and either copies it to create a new active policy or identifies an appropriate existing one, and adds the selected machine to it. In the basic model policies are created on a per tenant per retention/service level basis.

These additions to policies are then cached internally to the solution to provide end users with an indication in the front end of what machines are being “protected”, and which are “unprotected”. The cache is also fully updated daily to catch any manual policy changes.

Users may also ‘Backup Now’, which works in a similar way but creates a temporary policy and runs the backup immediately; the policy is then deleted once a backup is completed.

At a high level, machine (VM) and file restore work by browsing the NetBackup Catalog for backups of the tenant’s machine and then issuing a restore command according to the configuration for that machine.

1.2 Selecting the right solution for your needs

Front Office for NetBackup ships with 2 differing solutions.

Machine Driven Solution

The default configuration which uses a database of machines and their owners, to provide separation between Tenants. It supports a number of NetBackup Policy types. It can be used to manage all of a tenant’s backup needs, allowing tenants to create their own backup policies, or it can be configured to only provide restore services based off manually maintained backup Policies.

vCloud Driven Solution

For a vCloud based solution vCloud will provide the separation between tenants’ machines, and allow each to manage their own backup policy creation and restores.

2.0 Installation

2.1 Installation Checklist

Activity	Section	Machine driven Solution	vCloud driven Solution
Install Front Office Portal	2.4		
Install Netbackup Adapter	2.5		
Configure remote PowerShell for a Windows Master Server	3.1.1		
Configure SSH for a Unix Master Server	3.1.2		
Create Machine Driven Template Policies	3.2		
Create vCloud Driven Template Policies	3.3		
Populate Machine table	4.1		
Configure a Machine Location Section	5.2.1		
Configure a vCloud Location Section	5.2.2		
Configure a Service Level	5.2.3		
Create a Test Client	6.1.1		
Configure test Client's Customer Code	6.1.2		
Configure Test Clients vCloud login	6.1.3		
Create a Test User	6.1.1		
Setup URLs of Panels	5.4.1		
Run the cache generation scheduled task as admin	7.1		
Log in as test user, check panels	7.2		
Raise a 'Backup Now' request	7.3		

2.2 Installation Overview

Front Office for NetBackup consists of two main components: the core Front Office Portal and the adapter for adding specific NetBackup functionality. These are then broken down into sub components that for a secure implementation need to be installed with the appropriate level of protection.

- Front Office Portal
 - Web Site – This will be the internet facing Multi-Tenant (aka Multi Client) portal that your end clients will interact with. It should be running on SSL and be visible over the Internet.
 - Public Web Services – These are used by the adapter to access and update specific information on requests. They should be running on SSL but on a port that is not available over the internet. If the Public Web Services are available from outside the

server, you can set a User Name and Password for the “Directa API”. See 5.3.1 below for details.

- NetBackup Adapter
 - Panels – These are widgets that are displayed in the Front Office Portal to provide end clients with summary information about Protected Items. They should be running on SSL and be visible over the Internet
 - Services – These are Web Services that the Front Office Portal calls to lookup data for the end clients. They should be running on a port that is not available over the internet, and you may wish to consider only making them available locally.

2.3 Pre-Requisites

In order to install and run the Front Office for NetBackup solution you require:

- Microsoft Windows Server 2008 or above
 - Microsoft .NET Framework 4.5
 - Internet Information Services
 - WCF HTTP Activation
 - ASP.NET 4.5
 - PowerShell 3.0
- Microsoft SQL Server 2008 or above
- Symantec NetBackup 7.6
- VMware vCloud Director 5.1 or 5.5

2.4 Installing the Front Office Portal

Follow the Instructions in the “Front Office 8.1 Install and Upgrade Guide.pdf” to install the Front Office Portal. The installer is “Front Office for NetBackup 8.1.0002.exe”. The default installation location is C:\Program Files (x86)\Biomni\Front Office 8.1\

This document assumes you choose the default Site Name of “FrontOffice”. If you change this, you will need to update the values you use below.

2.5 Installing the Front Office for NetBackup Adapter

This document assumes there are two websites available on the server. A publically available site, and a purely internal site.

2.5.1 Extract Files

Right click and look at the properties of your NetBackupAdapter.zip file, if there is an ‘Unblock’ option, unblock before extracting the file.

Unzip “NetBackupAdapter v2.0.zip” and copy the folder to your install location (for example C:\Program Files (x86)\Biomni\NetBackupAdapter)

2.5.2 Create the Database

Navigate to the NetBackupAdapter folder.

- Launch “DatabaseInstaller”
- Choose “Install a New NetBackup Adapter Database”
- Follow the instructions to create the database and make a note of the SQL Connection string you are given when the installer completes

2.5.3 Create an Application Pool

Open IIS and navigate to Application Pools.

- Add Application Pool
 - Name: Front Office NetBackup Adapter
 - .NET CLR version: 4.0
 - Managed pipeline mode: Integrated

2.5.4 Configure the Panels

Open IIS and navigate to the publicly available Web Site.

- Add Application...
 - Alias: FrontOfficeNetBackupAdapterPanels
 - Application pool: Front Office NetBackup Adapter (created earlier)
 - Physical Path: browse to “C:\Program Files (x86)\Biomni\NetBackupAdapter\NetBackupAdapterPanels”

Configure the Web.config, edit “C:\Program Files

(x86)\Biomni\NetBackupAdapter\NetBackupAdapterPanels\Web.config”

- In <connectionStrings> where name=AdapterDb set connectionString to value given by installer
 - e.g.
"Server=(local);Database=FrontOfficeNetBackupAdapter;Trusted_Connection=False; User ID=FrontOfficeNetBackupAdapterUser;Password=password;"
- Relevant <appSettings> are:
 - DapiUserName – Used if you have secured the Directa Api in Front Office
 - DapiPassword – Used if you have secured the Directa Api in Front Office
 - DapiUrl – Update this to the URL of the DirectaApi.svc in the Front Office Public Web Services. The default is “http://localhost/FrontOfficePublicWebService/DirectaApi.svc”, you can check the configured Url within the Front Office Portal, select *Admin > Settings > Configuration Check*, the Public Web Services URL is displayed here, this value with “DirectaApi.svc” appended is your DapiUrl value.

2.5.5 Configure the Services

Open IIS and navigate to the Internal Web Site.

- Add Application...
 - Alias: FrontOfficeNetBackupAdapterServices
 - Application pool: Front Office NetBackup Adapter (created earlier)
 - Physical Path: browse to “C:\Program Files (x86)\Biomni\NetBackupAdapter\NetBackupAdapterServices”

Configure the Web.config. Edit “C:\Program Files (x86)\Biomni\NetBackupAdapter\NetBackupAdapterServices\Web.config”

- In <connectionStrings> where name=AdapterDb set connectionString to value given by installer
 - e.g.
"Server=(local);Database=FrontOfficeNetBackupAdapter;Trusted_Connection=False; User ID=FrontOfficeNetBackupAdapterUser;Password=password;"
- Relevant <appSettings> are:
 - DapiUserName – Used if you have secured the Directa Api in Front Office
 - DapiPassword – Used if you have secured the Directa Api in Front Office
 - DapiUrl – Update this to the URL of the DirectaApi svc in the Front Office Public Web Services as per the panel configuration above.
 - vCloudIgnoreSSLCertificateErrors – If using vCloud and any of the vCloud Director instances do not have a valid SSL certificate that matches the site name you can set this value to “true” and Front Office will ignore SSL errors when communicating with vCloud.

2.5.6 Encrypting Config Files

You can enhance the security of the adapter by encrypting the settings in the config files.

If you would like to do this, there are some helpers which will encrypt/decrypt the 'connectionStrings' and 'appSettings' sections.

- <Install Location>\MSBuild\ConfigEncrypt.bat
- <Install Location>\MSBuild\ConfigDecrypt.bat

3.0 NetBackup Configuration (pre-requisites)

The following needs to be configured in NetBackup in order for the solution to operate correctly. NetBackup 7.6 must already be installed and configured.

3.1 Setting up Communication with the NetBackup Master Server

Front Office runs Windows PowerShell scripts for communicating with vCloud Director and NetBackup. In order to enable these scripts to run and communicate with the NetBackup Master server a number of steps need to be carried out.

The Front Office server requires Windows PowerShell 3 to be installed. Windows Server 2012 and above come with that by default, for Windows Server 2008 it is available as part of [Windows Management Framework 3](#).

The Front Office server also needs to be able to run the PowerShell scripts. This may be blocked by current server policy. To enable running of scripts:

- Launch a Windows PowerShell window as Administrator
- Set-ExecutionPolicy -ExecutionPolicy Unrestricted -Scope LocalMachine

Communication with the NetBackup Master server depends on the Operating System that NetBackup is running on.

3.1.1 Communication with a Windows NetBackup Master Server

Front Office uses [Windows PowerShell Remoting](#) to communicate with a Windows NetBackup Master Server. Windows PowerShell will need to be installed on the Master Server (this is likely to be installed by default).

To enable PowerShell Remoting (see <http://technet.microsoft.com/en-us/magazine/ff700227.aspx>)

- Login to the NetBackup Master Server
- Launch a Windows PowerShell window as Administrator
- Enable-PSRemoting -Force
- Open Required Firewall ports
 - By Default PowerShell Remoting uses HTTP on Port 5985 or HTTPS on Port 5986

To Test Communication

- Login to the Front Office Server
- Launch a Windows PowerShell window
- New-PSSession -ComputerName <NbuMaster> -Credential <domain\user>
 - <NbuMaster> is the name of the Master Server
 - <domain\user> is the user account Front Office will be using to manage NetBackup
- You will be prompted to fill in the password for the <domain\user> entered, on success you will be shown a row with the ComputerName of the NetBackup master server.

If the NetBackup account is not a Domain account, you will either have to use HTTPS or add all the Windows Master servers to the Trusted Hosts in Windows Remote Management. See 10.0 for more information.

3.1.2 Communication with a Unix NetBackup Master Server

Front Office uses Secure Shell (SSH) to communicate with a Unix NetBackup Master Server. Configuration of SSH is outside the scope of this guide, but Front Office will require the credentials to talk to the SSH Server on the master server

- By default SSH uses Port 22
- Front Office runs NetBackup commands on the master server using sudo. Ensure the account has the rights to run all NetBackup command lines using sudo. It also runs “cat”, “rm” and “tee” using sudo.

To Test Communication

- Install an SSH Client on the Front Office Server (e.g. [PuTTY](#)). This is not needed by Front Office.
- Establish a connection to the NetBackup Master Server using the supplied credentials
- Run a simple command, such as
 - echo ‘hello world’

3.2 Machine Driven NetBackup Template Policies

The solution uses template policies as the basis for the creation of new end tenant-specific policies. Templates are inactive policies and the solution requires multiple policies to be created on the Master Server.

Template policies should match the following naming conventions:

Scheduled Backup Policies: *Template<-PolicyModifier>-<PolicyType>-<ServiceLevel>*

BackupNow Policies: *Template<-PolicyModifier>-<PolicyType>-<BackupNow>*

Naming of these policies is case sensitive and all policies should be inactive.

PolicyModifier

The policy modifier is optional. It can be used to provide separate templates for a number of scenarios such as different media servers, geographic locations of tenant-specific configuration. See 4.1 below for more details.

PolicyType

The policy type code for Netbackup, e.g. 0 for standard, 13 for windows, 40 for VMware.

For any type 40 (VMware) template policy:

1. On the Clients tab, Virtual Machine Selection should be set to “select automatically through query” and “Reuse VM selection query results for” should be set to 0 hours.
2. On the VMware tab, the Primary VM identifier must be “VM display name”.

ServiceLevel

Service Level is used to select between templates with different Schedules or Retentions configured.

For example: If you are supporting standard (0) and windows (13) policies, with two different service levels options, and not using Policy modifiers, you would need to create six template policies:

Template-0-SL1

Template-0-SL2

Template-0-BackupNow

Template-13-SL1

Template-13-SL2

Template-0-BackupNow

3.2.1 Scheduled Backup Policies

Scheduled Backup policies should be configured with all the options required for a given service level. For instance, if you are configuring Service Level Gold (SL1) with a weekly full backup retained for a year and a daily partial backup retained for a month, you would configure the appropriate schedules and retentions against template policies for each of the policy types you are using. In the example above this would be on Template-0-SL1 and Template-13-SL1. You could then proceed to configure Silver (SL2) accordingly.

3.2.2 BackupNow Policies

BackupNow policies should be created for each Policy Type you are supporting; they should have no backup window on their schedule, which should be called ‘Default’.

Front Office is configured out of the box to use the default NetBackup retention levels for BackupNow policies. If these are changed in NetBackup, modifications must be made in the Front Office Portal, see 8.3.

3.3 vCloud Driven NetBackup Template Policies

The solution uses template policies as the basis for the creation of new end client specific policies. Templates are inactive policies and the solution requires multiple policies to be created on the Master Server.

When configuring a Front Office for Netbackup vCloud solution you need to configure two template policies:

Scheduled Backup Policies: Template-vCloud

BackupNow Policies: Template-vCloud-BackupNow

Naming of these policies is case sensitive, and all policies should be inactive.

3.3.1 Scheduled Backup Policy: Template-vCloud

This policy is used as a template to create new policies for scheduled backups. The template must be configured as follows, create a new policy:

3. On the Attributes tab, Policy Type should be set to VMware.
4. On the Schedules tab, there is a single schedule called Default, with your desired default schedule.
5. On the Clients tab, Virtual Machine Selection should be set to “select automatically through query” and “Enable vCloud Directa Integration” should be ticked. “Reuse VM selection query results for” should be set to 0 hours.
6. On the VMware tab, the Primary VM identifier must be “VM display name”.

3.3.2 BackupNow Policy: Template-vCloud-BackupNow

This policy is used as a template to create temporary policies when a user requests a Backup Now Service, when the request is completed the temporary policy is deleted.

Repeat the setup for the vCloud-Template policy, but do not select any backup window for the schedule; the schedule must be called ‘Default’.

3.3.3 Retention Periods

Front Office is configured out of the box to use the default NetBackup retention levels. If these are changed in NetBackup, modifications must be made in the Front Office Portal, see 8.3.

3.3.4 vCloud Replication (AIR)

Replication (AIR) is only supported in a vCloud solution. If replication is required, appropriate SLP policies need to be defined with the following naming convention:

[retentionlevel]-[sourcelocation]-[targetlocation] e.g. 1-UK-Spain

[sourcelocation] and [targetlocation] must correspond to the Locations configured within the Front Office Portal, see 5.2.2.3

4.0 Adapter Configuration for Machine Driven Solutions

4.1 Machine Table

In the database created in 2.5.2 (by default called FrontOfficeNetBackupAdapter) there is a table called “Machine”, this table needs to be populated with information about each tenant’s machines. This is the table that provides the separation between tenants.

4.1.1 Column definitions

Name

The name used to identify the machine to the user in the Front Office Portal. This field is the primary key and so is mandatory and needs to be unique across all customers.

CustomerCode

The Customer Code of the Front Office Client that this machine belongs to. This field is mandatory and must match the “Customer Code” integration setting for the client.

Location

The name of the Location in Front Office which identifies the NetBackup master server responsible for this machine. This maps to the Integration Section in Front Office that starts with “Machine Location”. This field is mandatory.

PolicyType

The NetBackup Policy Type number. Supported values are:

0 – Standard

13 – Windows

40 – VMware

To allow Front Office to back up the machine, the Policy Type is mandatory.

To allow Front Office to restore a Virtual Machine you need to specify a policy type of 40.

Hardware / OS

These fields are required to support backup for all Policy Types except 40 (VMware). These two fields should contain the values that would be entered through the NetBackup Admin console when adding a Client to a policy.

PolicyModifier

This field allows the system to choose a different template policy for the machine. This enables differentiation by datacenter location, specific policy templates for an individual tenant, or many other uses.

NetBackupClientName

The name of the Client in NetBackup. This field will be used as the Client Name for agent based backup, and as the destination client name for File Restore.

VMDisplayName

The Display Name of a virtual machine in VMware. This is the name used to backup and restore virtual machines for VMware policies. If specified it will also be used as the source client name in NetBackup for File Restore.

4.1.2 Supported Configurations

The table below shows examples of which columns must be populated to support different usage scenarios.

	Policy Type	Hardware	OS	NetBackup Client Name	VM Display Name
Physical Unix machine Backup and File Restore	0	Linux	RedHat2.6.18	Nile.ri	
Physical Windows machine Backup and File Restore	13	Windows-x86	Windows	Amazon.ri	
Physical Machine File Restore only				Yangtze.ri	
Virtual Machine File Restore only				Mississippi.ri	Mississippi
VMware VM Backup and VM Restore	40				Mekong
VMware VM Backup, VM Restore and File Restore	40			Danube.ri	Danube

5.0 Front Office Configuration

The following needs to be configured in the Front Office Portal in order for the solution to operate correctly. The Administration Guide and the MultiClient Solution Guide contain further detail on configuration options.

5.1 Licensing

On first accessing your installed Front Office Portal, you will be required to register your details. You will immediately receive a product activation code by return email, which must be entered to allow full access to the site.

Your Front Office Portal includes a 90 day trial license out of the box but post activation you will be sent a full personalized license. This license should be applied to the License page in Admin > Settings.

5.2 Integration Settings

Integration Settings are used to configure the integration between the Front Office Portal and NetBackup. Individual Settings are grouped within Sections. Integration Settings are accessed via *Admin > Settings > More... > Integration Settings*.

Some settings have “Allow Client Override” set to ‘yes’. These settings need to be configured on a per client (tenant) basis and should not normally be completed in the top level Integration Settings, instead they are configured under the details for the specific client.

Client Integration settings are accessed from the *Admin > Organization > Client* on a separate tab within each client. Accessing from within a client, you will only see the settings that can be edited at the client level.

The different sections are:

Machine Location <ABC>

These sections contain details for connecting to a NetBackup Master Server that is configured for the Machine driven solution. You can have many of these sections, one for each Master Server.

vCloud Location <ABC>

These sections contain details for connecting to a NetBackup Master Server that is configured for the vCloud driven solution. You can have many of these sections, one for each Master Server.

Service Level <ABC>

Service Levels define a service offering for protecting customer machines. Each Service Level section maps to a set of Machine driven template policies in NetBackup, and are used to drive different backup options such as retention levels and frequencies, see o above. You can have many Service Level sections.

NetBackup Adapter

There should be only one of these sections. It is used to configure settings which affect the whole of the solution.

5.2.1 Machine Location Sections

Details to allow the Front Office Portal to communicate with different NetBackup Master Servers are stored as Location Sections within Integration Settings.

A newly installed system will start with a section called “Machine Location Default”, with blank settings for everything that needs configuring to connect.

5.2.1.1 System Wide Settings

NetBackup Server

The NetBackup Master server for this location.

NetBackup OS

The Operating system of the NetBackup server. Supported values are “unix” or “windows”. If not set, will default to “windows”

NetBackup Folder

The Location on the NetBackup Master server that the NBU Commands are installed in. Default values are:

“C:\Program Files\Veritas\NetBackup” for Windows

“/usr/opensv/netbackup” for Unix

NetBackup UserName

The UserName to connect to the NetBackup Master server, for windows this user must be able to connect with Remote PowerShell, for Unix it must be able to connect via SSH. See section 3.1 above for more details.

NetBackup Password

Corresponding password for connection to the NetBackup server.

NetBackup TimeZone

If the server time zone for the Front Office NetBackup Adapter and your NetBackup Master server are the same you do not need to configure the timezone.

If you need to configure the time zone, it must be set with a Microsoft TimeZoneIdentifier Id.

These are used as keys in the registry in

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion\Time Zones

For further information see:

<http://msdn.microsoft.com/en-us/library/system.timezoneinfo.getsystemtimezones.aspx>

Note: the NBU Master server must always be configured as US date format equivalent (Month / Day / Year).

5.2.1.2 Adding Machine Locations

Each NetBackup Master needs its own Machine Location section configured. In order to add a second, and subsequent Master Server, you will need to create a new Machine Location section.

It should be named “Machine Location <ABC>”, where <ABC> is how it is referenced in the Machine table in the adapter database, see 4.1 above. Settings must be created within the new section matching the settings in the existing section, i.e.

Setting Name	Settings Type	Allow Client Override
NetBackup Server	Text	No
NetBackup UserName	Text	No
NetBackup Password	Password	No
NetBackup Folder	Text	No
NetBackup OS	Text	No
NetBackup TimeZone	Text	No

These will then need populating with values for the new Server(s).

5.2.2 vCloud Location Sections

vCloud Location Sections contain all the settings found in a Machine Location Section, and extra settings for configuring a vCloud. All the NetBackup settings should be configured as per a Machine Location Section.

5.2.2.1 System Wide Settings

In addition the settings normally configured for a Machine Location, you must also configure the following:

vCloud API

This should be set to the URL of the vCloud API, in the format of “https://<hostname>/api”. Note: if your API does not have a valid SSL certificate such as in a test or UAT environment, see 2.5.5 above for additional configuration steps.

File Restore Domain Suffix

The File Restore Domain Suffix is only required if using the File Restore request type.

When restoring files to a NetBackup client, the client machine must be addressable from the NetBackup media server through a DNS name in the format:

`<VM name>.<vApp name>.<vDC name>.<vOrg Name><Domain Suffix>`

The Domain Suffix is this setting, and should start with a ‘.’, e.g. “.vcloud.local”

5.2.2.2 Client Specific Settings

Client specific settings must be set for each client using the solution; setting them up should be part of a client take-on process.

vCloud vOrg

The client’s vOrg in vCloud.

vCloud UserName

The vCloud username that will be used by Front Office to access the vCloud API (specified in the General Integration Settings above). Each client / tenant must have their own credentials. It must be in the format “userid@vOrg”.

vCloud Password

The clients corresponding vCloud password.

5.2.2.3 Adding vCloud Locations

Each NetBackup Master Server / vCloud combination needs its own Location section configured. In order to add a second, and subsequent Master Server connected to vCloud, you will need to create a new vCloud Location section.

It should be named “vCloud Location <ABC>”, where <ABC> is how it will appear named to end users. Settings must be created within the new section matching the settings in the existing section, i.e.

Setting Name	Settings Type	Allow Client Override
vCloud Api	Text	No
vCloud vOrg	Text	Yes
vCloud UserName	Text	Yes
vCloud Password	Password	Yes
NetBackup Server	Text	No
NetBackup UserName	Text	No
NetBackup Password	Password	No
File Restore Domain Suffix	Text	No
NetBackup Folder	Text	No
NetBackup OS	Text	No
NetBackup TimeZone	Text	No

These will then need populating with values for the new Server(s).

5.2.3 Service Levels for Machine Driven Solutions

When using Service Levels each level must be configured as an Integration Section. Service Levels are not currently supported in vCloud solutions; if you need to use Service Levels within a vCloud solution please contact Biomni Support for additional help.

The settings within a Service Level section are:

Name

The name used to identify the Service Level to end users.

Sequence

An integer number, this sets the order of the service level in dialog boxes, in ascending order.

Description

A text description of the Service Level.

Icon

URL of an image to be used against the service level in popups.

Visible

This setting can be set to ‘True’ or ‘False’, when false the service level will not be available for users to select when protecting machines. Setting this to false is preferable to deleting the service level as it will allow existing protected items to show with the correct name, rather than ‘Unknown’.

TemplateSuffix

The template suffix is to select a template policy when protecting a machine. It is also included in any policies created based off it. See section o above on configuring NetBackup policies for more details.

At a minimum, the TemplateSuffix must be configured.

5.2.3.1 Shipped Service Levels

The Front Office Portal ships with three example Service Levels configured: Gold, Silver, and Bronze. You may edit or delete these sections as you need to meet your requirements.

5.2.3.2 Adding Service Levels

Each Service Level needs its own section configured. In order to add more Service Levels you will need to add new sections.

The title of the section should be named “Service Level <ABC>” where <ABC> is a unique name. This name only needs to be unique and is not displayed to users.

Settings must be created within the new section matching the settings in the existing section, i.e.

Setting Name	Settings Type	Allow Client Override
Name	Text	No
Sequence	Text	No
Description	Text	No
Icon	Text	No
Visible	Text	No
TemplateSuffix	Text	No

5.2.4 NetBackup Adapter Section

Customer Code

Only used for Machine driven Solutions. A Unique value identifying the tenant in the Machine table.

Report Customer Root

The path of a folder on the webserver where this customers reports are stored. See 6.2 below for more details.

Report File Extensions

A semi colon separated list of file extensions can be specified e.g. .pdf;.txt;.htm;.html. See 6.2 below for more details.

5.3 Configuring Adapters

The Front Office for NetBackup solution uses a number of smaller adapters to communicate with NetBackup in different ways. These are referenced within the Request Types (configured below) but they must be configured to point to your internal website separately.

In the Front Office Portal in *Admin > Settings > Adapter* you will see all the adapters:

System Type	Adapter Display Name	Version	
Directa API	Directa API		Deactivate 
External Listbox	NetBackup External Listbox	7.1	Deactivate 
Field Value changed by User hook	NetBackup Field Changed Hook	8.0	Deactivate 
Request Fulfillment Hook	NetBackup Fulfillment Hook	8.0	Deactivate 
Scheduled Task Hook	NetBackup Scheduled Task	8.0	Deactivate 
Tree View	NetBackup TreeView	8.0	Deactivate 

Each of these, except for the Directa API, should have their URLs modified as per the table below. Click on each adapter and modify their 'Web Service URI' as follows, where <InternalWebsite> is the public facing website configured in section 2.2.

Adapter	Web Service URI
NetBackup External Listbox	http://<InternalWebsite>/FrontOfficeNetBackupAdapterServices/FlexiField.svc
NetBackup Field Changed Hook	http://<InternalWebsite>/FrontOfficeNetBackupAdapterServices/UIFieldChanged.svc
NetBackup Fulfillment Hook	http://<InternalWebsite>/FrontOfficeNetBackupAdapterServices/FulfillmentHook.svc
NetBackup Scheduled Task	http://<InternalWebsite>/FrontOfficeNetBackupAdapterServices/ScheduledTask.svc
NetBackup TreeView	http://<InternalWebsite>/FrontOfficeNetBackupAdapterServices/TreeView.svc

5.3.1 Securing the Directa API

The Directa API is used by the NetBackup adapter to access and update details on requests as part of providing backup and restore services. The API gives a high degree of control over the system and for this reason you may wish to secure it with a username and password.

In the Front Office Portal in *Admin > Settings > Adapter* select the 'Directa API' adapter and change the Authentication Mode to 'Basic Authentication'. You can now enter a username and password for the API.

These credentials will need to be configured in the NetBackup Adapter's Panels and Services. See sections 2.5.4 and 2.5.5.

5.4 NetBackup Panels

The Solution includes a number of Pre-configured panels, you can remove any that you are not using from *Admin > Service Catalog > Service Catalog* within the portal.

Protected

In the Machine driven Solution, a list of the tenant's (aka client's) machines that are included in scheduled policies.

Unprotected

In the Machine driven Solution, a list of the tenant’s Machines that are not part of a scheduled backup policy.

vCloud Protected

In the vCloud driven Solution, a list of the tenant’s vCloud VMs that are included in scheduled policies.

vCloud Unprotected

In the vCloud driven Solution, a list of the tenant’s vCloud VMs that are not part of a scheduled backup policy.

Reports

A panel displaying categorised files as reports.

5.4.1 Configuring the Panels

The NetBackup panels will need to be configured for the URL of the public facing website configured in 2.5.4 . Configure the panels that are relevant to your solution; the ones you are not using can be deleted.

Within the Front Office Portal, select *Admin > Service Catalog* and then for each of “Under Protection”, “Unprotected Items” and “Reports” hover over their names and select *Edit* from the drop-down menu.

The Panel URL of each will need editing as below, where <PublicWebsite> is the public facing website configured in 2.5.42.5.4 above.

Protected	http://<PublicWebsite>/FrontOfficeNetBackupAdapterPanels/DB-ProtectedItems.aspx?SecurityToken=##Session.SecurityToken##
Unprotected	http://<PublicWebsite>/FrontOfficeNetBackupAdapterPanels/DB-UnprotectedItems.aspx?SecurityToken=##Session.SecurityToken##
Reports	http://<PublicWebsite>/FrontOfficeNetBackupAdapterPanels/FileReports/ReportList.aspx?SecurityToken=##Session.SecurityToken##
vCloud Protected	http://<PublicWebsite>/FrontOfficeNetBackupAdapterPanels/VCD-ProtectedItems.aspx?SecurityToken=##Session.SecurityToken##
vCloud Unprotected	http://<PublicWebsite>/FrontOfficeNetBackupAdapterPanels/VCD-UnprotectedItems.aspx?SecurityToken=##Session.SecurityToken##

5.4.1.1 Reports Panel

Files are displayed from a folder specified in Integration Settings (see below). Files can be displayed in the root of the folder specified and / or in sub folders whose names are displayed as categories for the reports.

By default PDF files are displayed but this can be optionally overridden in Integration Settings. The panel has been tested with PDF, text and html files but other file types may be viewed if the browser supports their display.

The user’s browser must support the display of PDF files to view them in the panel. A download link is available for viewing the report if the browser does not support their display.

Integration settings

Integration Settings are in a section named “NetBackup Adapter”.

Setting Name	Description
Report Customer Root	<p>Mandatory.</p> <p>Client override should be allowed and no default set at the system level for security reasons.</p> <p>For each client a folder should be created on disk and files deposited there for display. The setting should then be set to this path.</p> <p>Ideally the folder should be on the web server(s) to avoid network traffic of moving files from another server repeatedly.</p> <p>Note: For security reasons, client folders must not be created as sub folders of other client folders.</p>
Report File Extensions	<p>Optional.</p> <p>Client override can be allowed and can be set at system level and optionally overridden at client level.</p> <p>If this setting does not exist or is empty, only PDF files are displayed.</p> <p>A semi colon seperated list of file extensions should be specified e.g. .pdf;.txt;.htm;.html</p>

6.0 New Client Take On

When new clients are taken on, various things need to be configured during that process. This section details those.

6.1 Clients and Users

Within the context of the Front Office Portal you may create a number of end clients; each client is isolated from other clients and can have a number of its own users. Normally an end client will be represented as a client within the portal, with one or more user logins to the system.

6.1.1 Creating a Client and First User

Clients can be created within *Admin > Organization > Client*, click *New* and give the client a name. Switch to the *Users* tab and click *New* to create an Admin User for the client, fill in the mandatory fields for the user (User ID, User Name, and Email Address) and set the Access Profile to “Administrator”.

For further information on Clients see *Admin > Support > Documents > Multi Client Solution Guide*.

For Information about automating creation of clients and users see 9.0 Appendix – Automating Client and First User Creation.

6.1.2 Configuring a client for a Machine Driven Solution

Clients require the following Integration Settings to be set at a client level (*Admin > Organization > Client > Select a client > Integration Settings*)

Section	Setting	Value
NetBackup Adapter	Customer Code	A Unique value identifying the tenent in the Machine table
NetBackup Adapter	Report Customer Root	The path of a folder on the webserver where this customers reports are stored.

6.1.3 Configuring a client for a vCloud Driven Solution

Clients require the following Integration Settings to be set at a client level (*Admin > Organization > Client > Select a client > Integration Settings*)

Section	Setting	Value
NetBackup Adapter	Report Customer Root	The path of a folder on the webserver where this customers reports are stored.
vCloud Location <ABC>*	vCloud vOrg	The client’s vOrg in vCloud
vCloud Location <ABC>*	vCloud UserName	The vCloud username that will be used by Front Office to access the vCloud. Each tenant must have their own credentials. It must be in the format “userid@vOrg”
vCloud Location <ABC>*	vCloud Password	The corresponding vCloud password

**Where <ABC> is a location name – each location a tenant is using must be setup*

6.2 Report panel

A new folder must be created on the server for generated reports to be dropped in for the client. This folder must not be a sub folder of another client’s report folder, and set in their Integrations Settings (see 6.1 above).

7.0 Testing the Solution

7.1 Run Scheduled Task to populate Client Backup Cache

The Front Office for NetBackup Adapter maintains a cache of the client's currently backed up items in order to respond to user actions quickly. This cache is refreshed daily at midnight for all clients, and on a per client basis after user operations. A manual refresh can be triggered after configuration, so that you do not have to wait until midnight for initial population, and is a good first test of system connectivity.

Navigate to *Admin > Settings > More... > Scheduled Task* and select the Machine or vCloud adapter from the Custom Tasks section, click the *Run Now* button.

Check the progress of the task by navigating to *Admin > Support > Other Logs* you should be able to see an entry with the message "Calling WebService Custom scheduled Task". Check that there are no errors after this. You can also check the Error Log at *Admin > Support > Error Log*.

7.2 Checking the Panels

If you log in with a Client user account, the relevant Protected and Unprotected panels should now be populated with machines.

7.3 Raising a Request

While logged in as a Client User you should now be able raise a request from the home page. A *Backup Now* request is a good first test. Complete the form to backup a client machine. Wait for the request to complete and check the Error Log (*Admin > Support > Error Log*) for any errors.

7.4 Troubleshooting

If any errors are encountered during testing and the cause is not clear, after checking the configuration, you may need to enable tracing in the NetBackup Adapter, see 0 Enabling Diagnostic Tracing.

Further assistance can be obtained from <http://community.biomni.com/home>

8.0 Pre-Configured Services in Front Office for NetBackup

A client user can log in to the Front Office Portal and see the pre-configured services and reports displayed on the home page. The user must be logged in as an end client to create a request or view the protected / unprotected listings on the home page.

For all services, * denotes a required field.

8.1 Machine Driven Services

8.1.1 “Protect Machine”

This service creates a policy based on a predefined template that will backup selected machines on a schedule.

On selecting Protect Machine, a form is displayed with the fields:

- **Select machine to backup*** – all machines in the Machine table available for backup are displayed in a list; a single machine can be selected. Already protected machines are indicated by an image.
The machine list is retrieved via an adapter.
- **Service Level*** – the policy settings for the backup e.g. the frequency and retention period for the new backup.
Service Levels are configured and editable in 5.2.3.
Available Service Levels are retrieved via an adapter.
- **Your reference** – a text entry field to allow any appropriate reference to be associated.

Once submitted, Front Office will then:

- Create a new policy based on a template or add to a policy if a policy exists.
- Update the home page protected / unprotected panels.

8.1.2 “Restore VM”

This service allows a previously protected VM to be restored to the original location. The type of backup available for a given date / time is indicated to the user.

On selecting Restore VM, a form is displayed with the fields:

- **Select VM*** - the machines that are protected, either through a policy or as a one-off. A single VM can be selected. An adjacent image indicates the type of backup and a location in brackets indicates it is replicated.
The machine list is retrieved via an adapter.
- **Backup date*** - a date on which to base the search. Results will reflect +/- 7 days.
- **Select backup*** - a list of all the backups for the selected VM.
Available backups are retrieved via an adapter.
- **Confirm overwrite if exists*** - If a VM with the same name already exists in the requested location, the user is required to confirm that an over-write is acceptable.
- **Your reference** – a text entry field to allow any appropriate reference to be associated.

Front Office will then:

- Restore the selected VM to its original location.
- Start the VM
- Email the requester notifying of success or failure.

8.1.3 “Restore File / Folder”

This service allows a file or folder from a protected VM to be restored to a Windows or Unix machine. The type of backup available for a given date / time is indicated to the user. It can be restored to its original location or a sub folder within the original location.

Note: the machine must have the NetBackup agent installed, which is a requirement for any file or folder restore.

On selecting Restore File or Folder, a form is displayed with the fields:

- **Backup date*** - a date on which to base the search. Results will reflect +/- 7 days.
- **Select machine to restore from*** - the machines that are protected, either through a policy or as a one-off. A single machine can be selected.
The machine list is retrieved via an adapter.
- **File selection type*** - option to browse a list or search by name.
Depending on *File selection type*:
- **Browse for file or folder** -
 - Tree view displays with root nodes of the backup dates in the specified date range. Subsequent folders / files are available as single select.
 - Folders will be listed alpha-sorted, followed by files alpha-sorted. Files display with sub nodes giving size and last modified date.
 - The type of backup (full, incremental or cumulative) available for a given date / time is indicated to the user.
- **Search for file or folder** -
 - A list of backups and the type (full, incremental or cumulative) in the data range is displayed for selection in a filter.
 - Files or folders can be searched by name. Search will automatically wildcard if *Partial Match* (default) is selected for Search Type. If *Exact Match* is selected, wildcard will not automatically be added but the user can still add their own.
 - Files are sorted by path.
 - Results are capped at 500 records, with a message shown.
 - User are prevented from only searching by ‘*’ or ‘* and spaces’.
 - Results can be filtered by size, or restricted to folders only
- **Restore to original location?** - By default the file or folder will be restored to the original location but the user can choose for it to be restored to a new sub folder.
- **Confirm overwrite if exists*** - The user is required to confirm that an over-write is acceptable if a file or folder with the same name already exists.
- **Your reference** – a text entry field to allow any appropriate reference to be associated.

Front Office will then:

- Restore the file or folder to the Windows or Unix machine.
- Email the requester notifying of success or failure.

8.1.4 “Backup Now”

This is similar to Protect Machine but the backup is immediate and happens only once i.e. no backup schedule is created.

On selecting Backup Now, a form is displayed with the fields:

- **Select machine to backup*** – all machines in the Machine table available for backup are displayed in a list and a single machine can be selected. Already protected machines are indicated by an image.
The machine list is retrieved via an adapter.
- **Backup retention*** – the retention period for the new backup.
Retention periods are configured and editable in NetBackup. The Listbox Item Code must match the NetBackup Retention Level and the Listbox Item Description should be the Retention Period. See 8.3 for details.
- **Your reference** – a text entry field to allow any appropriate reference to be associated.

Once submitted, Front Office will then:

- Create a temporary policy, which runs immediately and is then deleted.
- Email the requester notifying of success or failure.

8.1.5 “Unprotect Machine”

This service removes a currently protected vCloud object from the backup schedule.

On selecting Remove Backup, a form is displayed with the fields:

- **Select machines to unprotect*** – shows the machines that are protected. Already protected nodes within the machine list are indicated by an image. Multiple selections may be made.
The machine list is retrieved via an adapter.
- **Your reference** – a text entry field to allow any appropriate reference to be associated.

Once submitted, Front Office will then:

- Either update the policy or if all items are removed, delete the policy. This will be done for non-replication and replication location policies, as appropriate.
- Update the home page protected / unprotected panels.

8.2 vCloud Driven Services

8.2.1 “Protect Machine”

This service creates a policy based on a predefined template that will backup selected vCloud objects on a schedule.

On selecting Protect Machine, a form is displayed with the fields:

- **Select location*** (region) - all the available regions but if they are not configured for a region an appropriate message is displayed.
Available locations sourced via an adapter found in *Admin > Settings Adapter* and configured in *Admin > Settings > More... > Integration Settings*.
- **Select backup items*** – all vDCs/vApps/VMs available in vCloud for backup displayed in a tree list. Multiple selections at any level can be made; selecting a vDC or vApp selects all child nodes. Already protected nodes within the tree view are indicated by an image.
The vCloud structure is retrieved via an adapter.

- **Backup retention*** – the retention period for the new backup. Retention periods are configured and editable in NetBackup. The Listbox Item Code must match the NetBackup Retention Level and the Listbox Item Description should be the Retention Period. See 8.3 for details.
- **Replicate backup?** – offers the option for the backup to be replicated to another region. Note: the user does not need to be configured in that region. If selected, a list of secondary locations / regions is displayed. Available locations are sourced via an adapter, using values from Integration Settings.
- **Your reference** – a text entry field to allow any appropriate reference to be associated.

Once submitted, Front Office will then:

- Create a new policy based on a template or add to a policy if a policy exists.
- Update the home page protected / unprotected panels.

The policy name always contains the client vOrg name, the retention period and the region.

8.2.2 “Restore VM”

This service allows a previously protected VM to be restored, either to the original or an alternative (existing) location within vCloud. The type of backup available for a given date / time is indicated to the user.

On selecting Restore VM, a form is displayed with the fields:

- **Select location*** (region) - all the available regions but if they are not configured for a region an appropriate message is displayed. Available locations sourced via an adapter found in *Admin > Settings Adapter* and configured in *Admin > Settings > More... > Integration Settings*.
- **Backup date*** - a date on which to base the search. Results will reflect +/- 7 days.
- **Select VM to restore*** - the vDCs/vApps/VMs within a tree view that are protected, either through a policy or as a one-off. A single VM can be selected. An adjacent image indicates the type of backup and a location in brackets indicates it is replicated. The vCloud structure is retrieved via an adapter.
- **Restore to vApp:** Original or Other location. If ‘Other’ is selected, all vDCs and vApps available in vCloud are displayed in a tree list. Replicated restores are always restore to ‘Other’. If a VM with the same name already exists in the requested location, the user is required to confirm that an over-write is acceptable. The vCloud structure is retrieved via an adapter.
- **Your reference** – a text entry field to allow any appropriate reference to be associated.

Front Office will then:

- If local, restore the selected VM to the specified restore location.
- Email the requester notifying of success or failure.
- If replicated, email the system administrator with information about the selected VM and the required vApp to restore to, for manual resolution.

8.2.3 “Restore File / Folder”

This service allows a file or folder from a protected VM to be restored to a Windows or Unix machine. The type of backup available for a given date / time is indicated to the user. It will be restored to its original location.

Note: the VM must have the NetBackup agent installed, which is a requirement for any file or folder restore.

On selecting Restore File or Folder, a form is displayed with the fields:

- **Select location*** (region) - all the available regions but if they are not configured for a region an appropriate message is displayed.
Available locations sourced via an adapter found in *Admin > Settings Adapter* and configured in *Admin > Settings > More... > Integration Settings*.
- **Backup date*** - a date on which to base the search. Results will reflect +/- 7 days.
- **Select VM to restore from*** - the vDCs/vApps/VMs within a tree view that are protected, either through a policy or as a one-off. A single VM can be selected. An adjacent image indicates the type of backup and a location in brackets indicates it is replicated. The vCloud structure is retrieved via an adapter.
- **File selection type*** - option to browse a list or search by name.
Depending on *File selection type*:
- **Browse for file or folder** -
 - Tree view displays with root nodes of the backup dates in the specified date range. Subsequent folders / files are available as single select.
 - Folders will be listed alpha-sorted, followed by files alpha-sorted. Files display with sub nodes giving size and last modified date.
 - The type of backup (full, incremental or cumulative) available for a given date / time is indicated to the user.
- **Search for file or folder** -
 - A list of backups and the type (full, incremental or cumulative) in the data range is displayed for selection in a filter.
 - Files or folders can be searched by name. Search will automatically wildcard if *Partial Match* (default) is selected for Search Type. If *Exact Match* is selected, wildcard will not automatically be added but the user can still add their own.
 - Files are sorted by path.
 - Results are capped at 500 records, with a message shown.
 - User are prevented from only searching by ‘*’ or ‘* and spaces’.
 - Results can be filtered by size, or restricted to folders only
- **Confirm overwrite if exists*** - The user is required to confirm that an over-write is acceptable if a file or folder with the same name already exists.
- **Your reference** – a text entry field to allow any appropriate reference to be associated.

Front Office will then:

- Restore the file or folder to the Windows or Unix machine.
- Email the requester notifying of success or failure.

8.2.4 “Backup Now”

This is similar to Protect Machine but the backup is immediate and happens only once i.e. no backup schedule is created.

On selecting Backup Now, a form is displayed with the fields:

- **Select location*** (region) - all the available regions but if they are not configured for a region an appropriate message is displayed.
Available locations sourced via an adapter found in *Admin > Settings Adapter* and configured in *Admin > Settings > More... > Integration Settings*.
- **Select backup items*** – all vDCs/vApps/VMs available in vCloud for backup displayed in a tree view. Multiple selections at any level can be made; selecting a vDC or vApp selects all child nodes. Already protected nodes within the tree list are indicated by an image. The vCloud structure is retrieved via an adapter.
- **Backup retention*** – the retention period for the new backup.
Retention periods are configured and editable in NetBackup. The Listbox Item Code must match the NetBackup Retention Level and the Listbox Item Description should be the Retention Period. See 8.3 for details.
- **Replicate backup?** – offers the option for the backup to be replicated to another region.
Note: the user does not need to be configured in that region. If selected, a list of secondary locations / regions is displayed.
Available locations sourced via an adapter, using values from Integration Settings.
- **Your reference** – a text entry field to allow any appropriate reference to be associated.

Once submitted, Front Office will then:

- Create a temporary policy, which runs immediately and is then deleted.
- Email the requester notifying of success or failure.

8.2.5 “Unprotect Machine”

This service removes a currently protected vCloud object from the backup schedule.

On selecting Unprotect Machine, a form is displayed with the fields:

- **Select location*** (region) - all the available regions but if they are not configured for a region an appropriate message is displayed.
Available locations sourced via an adapter found in *Admin > Settings Adapter* and configured in *Admin > Settings > More... > Integration Settings*.
- **Select backups to remove*** – the vDCs/vApps/VMs within a tree view that are protected via a policy. Multiple selections at any level can be made; selecting a vDC or vApp selects all child nodes. Already protected nodes within the tree list are indicated by an image. The vCloud structure is retrieved via an adapter.
- **Your reference** – a text entry field to allow any appropriate reference to be associated.

Once submitted, Front Office will then:

- Either update the policy or if all items are removed, delete the policy. This will be done for non-replication and replication location policies, as appropriate.
- Update the home page protected / unprotected panels.

8.2.6 “Register VM for File Restore”

This service can be used where first time networking NetBackup / vCloud is required. This request is not integrated to NetBackup, but sends an email to a specified endpoint for manual action. This is considered a non-standard service so is not included in the out-of-the-box end user offering, however it is available as a template request type if needed.

8.3 Configuring Retention Levels

The vCloud Driven Protect Machine and Backup Now, and Machine Driven Backup Now request types, come pre-configured with NetBackup’s default Retention levels. If you wish to use different retention levels, they must be modified to match any configuration changes within NetBackup.

Access the *Form* tab via *Admin > Request & Approval > Request Type*. For each request type select the *Retention Period* field and within the *Configuration* tab, edit the Listbox Item Code to match the NetBackup Retention Level and the Listbox Item Description to the Retention Period.

8.4 Restoring to Default

In the event that a request type has been edited erroneously, a pre-configured Request Type can be returned to its default state. In the Install location of the NetBackup Adapter there is a folder called RequestTypes, e.g: “C:\Program Files (x86)\Biomni\NetBackupAdapter\RequestTypes”. Files prefixed VCD are for the vCloud Driven Solution and files prefixed DB are for the Machine Driven Solution.

The XML files contained here can be used to restore a pre-configured service to its original state. Within the Front Office Portal go to *Admin > Request & Approval > Request Type* and click the *Import* button; browse to one of the XML files (they will need to be on your local file system) and follow the on screen prompts to restore the Request Type.

9.0 Appendix A: Automating Client and First User Creation

The following PowerShell script is provided as a starting point for automating the creation of clients and their users. It makes use of the Front Office SDK to call the Public Web Services. Further information about the SDK is available in the help files which can be found in the install location of the Front Office Portal e.g. C:\Program Files (x86)\Biomni\Front Office 8.1\Sdk\

The SDK can be used from PowerShell or in your own .Net code to integrate into an existing client take-on process.

The first two lines of this example script will need modifying with the location of your install, the URL of your public web services, and any security configured against them.

```

Import-Module 'C:\Program Files (x86)\Biomni\Front Office 8.1\Sdk\Biomni.FrontOffice.Sdk.dll'
$dapi = Get-DirectaApi -DirectaApiUrl
"http://localhost/FrontOfficePublicWebService/DirectaApi.asmx" -UserName 'DapiUser' -Password
'DapiPassword'

#region Create Client.
$client = New-Object Biomni.FrontOffice.Sdk.Services.Dapi.Organisation.NewClient
$client.Name = 'Customer1'
$client.IsActive = $true
$clientId = $dapi.CreateClient($client)
#endregion

#region Create Client Admin user.
$user = New-Object Biomni.FrontOffice.Sdk.Services.Dapi.Organisation.NewUser
$user.ClientId = $clientId
$user.UserName = 'Customer1Admin'
$user.UserId = 'Customer1Admin'
$user.EmailAddress = 'Customer1Admin@example.com'
$user.AccessProfileId = 'BIOMNI_CLIENTADMIN'
$dapi.CreateUser($user)
$dapi.SetPassword($user.UserId, 'Password1')
#endregion

#region Configure client for vCloud infrastructure (delete if not running a vCloud
infrastructure).
$dapi.SetIntegrationSettingValueForClient($clientId, "vCloud Location Windows", "vCloud vOrg",
"customer1vorg")
$dapi.SetIntegrationSettingValueForClient($clientId, "vCloud Location Windows", "vCloud
UserName", "username@customer1vorg")
$dapi.SetIntegrationSettingValueForClient($clientId, "vCloud Location Windows", "vCloud
Password", "Password123")
#endregion

#region Configure client for Machine infrastructure (delete if not running a Machine
infrastructure).
$dapi.SetIntegrationSettingValueForClient($clientId, "NetBackup Adapter", "Customer Code",
"CS1")
#endregion

#region Configure Reports panel (delete if not using the Reports panel).
$dapi.SetIntegrationSettingValueForClient($clientId, "NetBackup Adapter", "Report Customer
Root", "C:\Reports\Customer1")
#endregion
  
```

10.0 Appendix B: Enabling Remote PowerShell to Multiple Master Servers

When configuring the system to communicate with NetBackup via remote PowerShell, if you are not using domain accounts to log in to the NetBackup Master server, you may need to add the Master Server, or Multiple master servers, to the trusted hosts on the adapter's server.

This can be accomplished in PowerShell with the following command; you will need to run PowerShell as an administrator.

```
winrm set winrm/config/client '@{TrustedHosts="machine1,machine2"}'
```

Add extra machines as needed in the comma separated list.

The number of remote connections is limited by settings on the NetBackup Master Server. The server defaults are typically sufficient.

In high usages installations it may be necessary to increase this limit. If the limit is exceeded the following error may occur:

[<NetBackup server name>] Connecting to remote server <NetBackup server name> failed with the following error message : The WS-Management service cannot process the request. The maximum number of concurrent shells for this user has been exceeded. Close existing shells or raise the quota for this user. For more information, see the about_Remote_Troubleshooting Help topic.

To increase the limit:

- On the NetBackup Master Server, run the following PowerShell command to determine the number of “connections” allowed:
- `Get-Item WSMAN:\localhost\Shell\MaxShellsPerUser`
- On the NetBackup Master Server, run the following command to increase the number of “connections” allowed:
- `Set-Item WSMAN:\localhost\Shell\MaxShellsPerUser <integer value>`

11.0 Appendix C: Simplifying the Front Office Portal Home Page

Deleting Categories

Once you have configured a Machine or vCloud Driven Solution, you can remove the parts of the homepage for the other solution. When logged in as an Admin user goto *Admin > Service Catalog > Service Catalog* there are drop down menus on each category that you can use to delete unwanted functionality.

Removing the Basket and Search from the UI

The install of Front Office Portal contains a file called z-override.css, the default install location is "C:\Program Files (x86)\Biomni\Front Office 8.1\". This can be used to insert css into the website.

To remove the basket, add:

```
#basketContainer {
    display: none !important;
}
.PageTop .CustomerDetail {
    right: 0px;
}
```

To remove Search from the front page, add:

```
.serviceCatQuickSearchBox {
    display:none;
}
```

12.0 Appendix D: Configuring Diagnostic Tracing

In the event of any problems, or to diagnose configuration issues, it is possible to enable tracing on the NetBackup Adapter. Tracing will record informational messages from the Adapters, as well as NetBackup commands being executed on the Master Servers.

Each component of the Adapter, the Services and the Panels, need configuring for Tracing separately. To enable tracing, edit the web.config file for the relevant component:

C:\Program Files (x86)\Biomni\NetBackupAdapter\NetBackupAdapterPanels\Web.config

C:\Program Files (x86)\Biomni\NetBackupAdapter\NetBackupAdapterServices\Web.config

In the <appSettings> section the relevant keys are:

- TraceLevel – Defaults to 'Off', set this to 'verbose' to enable full tracing.
- TraceFilePrefix – Defaults to '~\Logs\NetBackupAdapterServices' or '~\Logs\NetBackupAdapterPanels', this is the location of each trace file.

When tracing is enabled the IIS_IUSRS group must have 'Modify' permissions on the log folder specified.

Tracing logs can grow large very quickly and care should be taken to disable tracing when it is no longer needed.

13.0 Appendix E: Open Source Licenses

In addition to the Open Source Licenses specified in the *About* page of the Front Office Portal, the Front Office for NetBackup solution also uses the following components.

13.1 JQuery Data Tables

(<http://www.datatables.net/>) is licensed under the following license.

Copyright (c) 2008-2013, Allan Jardine
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- Neither the name of Allan Jardine nor SpryMedia may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT HOLDERS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

13.2 Renci SSH.NET Library

(<http://sshnet.codeplex.com/>) is licensed under the following license.

New BSD License (BSD)

Copyright (c) 2010, Renci
All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of RENCi nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.