

Active Directory Integration Manual

Fast and easy roll-out of BackupAgent platforms using Active Directory and web-panels

1. Online Backup for hosters

This whitepaper describes the unique and valuable features of combining BackupAgent's software with the Active Directory in a hosted environment. Worldwide hosting companies are adopting Microsoft platforms and technologies for their services. For provisioning purposes many hosters utilize the Active Directory and combine this with a web shop/panel software of Microsoft partners (e.g. Citrix CPSM v10).

The Hosting Community is adopting new value-add services on a global scale. One of the most popular services adopted is online backup. BackupAgent offers BackupAgent Server, which is a software platform for hosting online backup services based on Microsoft technology. This whitepaper will explicitly explain the possibilities of provisioning online backup services by using the Active Directory.

For general information about BackupAgent Server the following documents serve as recommended reading material to complement this whitepaper:

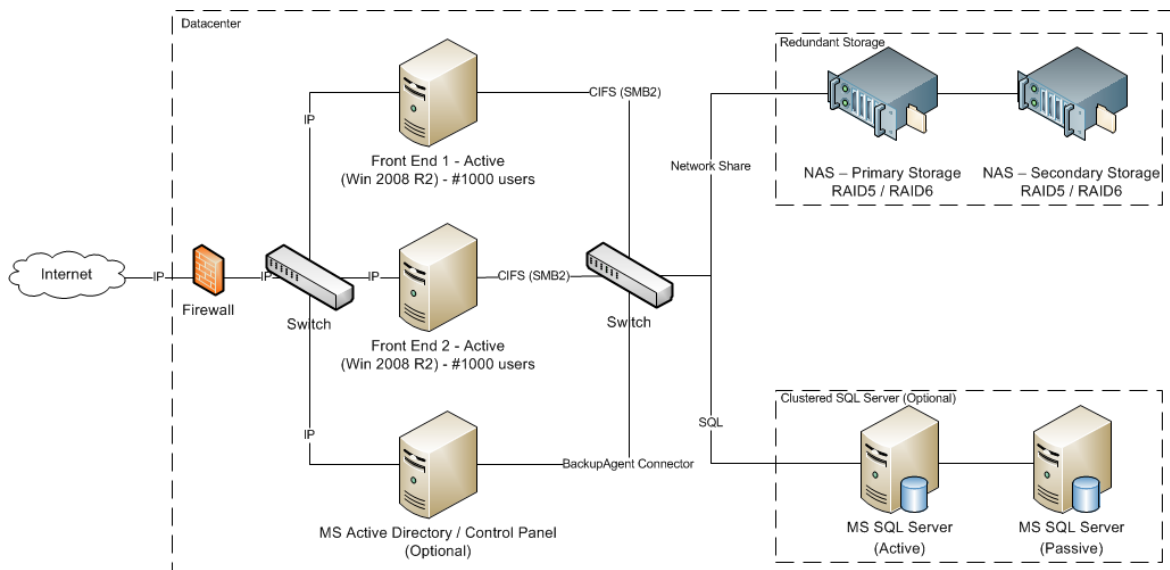
- BackupAgent Server Product Sheet
- BackupAgent Server Installation & Requirements
- BackupAgent Scalability Reference
- BackupAgent Provisioning Reference

Links to these documents can be found on the last page of this document.

1.1 Web Services

BackupAgent's server software architecture is based on web services, which allows the software to run on multiple load-balanced machines acting as a single instance. These web services run in IIS 7.0 and ASP.Net.

BackupAgent Server runs in BackupAgent's web servers will connect to one or more NAS's to store all backed up data coming in from BackupAgent's clients. The following picture gives an overview of this architecture:



The web servers also connect to a central database (BA Database), only to store account information. All data and metadata is stored in file sets on the NAS's. Backups are stored transparently in User Homes and can be moved around or copied to secondary locations or new NAS's at all-time.

Optionally, BackupAgent can synchronize the BA Database with an Active Directory (AD). This allows an end-user to immediately obtain a BackupAgent account on first login. The Web Servers can authenticate the user in the Active Directory and can immediately provision a backup account in the BA Database for the user.

2. Automated provisioning

The unique and innovative approach of BackupAgent in this sense is that BackupAgent Server can be implemented in the hosting environment without significant investments concerning

provisioning. This shortens the return on investment for adopting to a level where the hosting providers purchases and installs the BackupAgent Server software.

2.1 Scalability

BackupAgent allows system administrators to automatically provision backup accounts using their AD without involving any web shop or panel software. Best practice within hosting providers is to control authentication for various applications using the AD. Web shops and provisioning systems add or delete users in the AD. Subsystems authenticate and authorize users in the AD to grant or deny access to an application. BackupAgent applies these best practices.

2.2 Group memberships

BackupAgent Server authenticates users in the AD based on group memberships. A system administrator can add predefined groups in the AD and add group membership to a user to allow this user to backup data using an Online Backup Client. If a user accesses the BackupAgent web servers for the first time, web server will detect this group membership and will provision an account in the BA Database.

This approach will allow a hosting provider to integrate BackupAgent Server with an AD without tedious and risky schema updates. Web shop software can provision users by assigning applicable group memberships based backup plans.

To accomplish this, the AD groups work with predefined names. These names resemble a complete backup plan for a specific user. The plan holds:

- A standard prefix 'CloudBackup'
- The type of user¹: 'Workstation' or 'Server'
- The maximum storage space in gigabytes or megabytes: '10GB' or '5MB'
- The ID of the storage group² on a NAS: '1003'

¹A user can be Workstation user (allowing only data backup on Windows XP, Vista, Windows 7 and Windows 8) or a Server user (allowing backup on all supported Windows operating systems and backups of Exchange and SQL Server)

²BackupAgent Server can store data of users on multiple storage locations which can be uniquely identified by a numerical ID

The fields are separated by an underscore. For a 10 GB Workstation plan on a storage location with ID 1003 this will result in a group name 'CloudBackup_Workstation_10GB_1003'. Both new accounts and upgrades can take place by creating groups in AD and assign a single group membership to an appropriate group. Upgrading a backup plan from 10GB to 20GB will result in removing a group membership in the 10Gb group and adding it to the 20Gb group.

Note: A user can have only one 'CloudBackup_X_X_X' group membership. In case of multiple memberships the old plan will apply until the problem is corrected.

Note: If the user has no group membership for a CloudBackup group, this user will obtain a limited trial account.

Note: Users cannot change storage ID once the user account is provisioned from the AD.

2.3 Resellers or customer groups

Additionally some hosting providers will have resellers to resell their services. The resellers often obtain an Organizational Unit (OU) in the AD. BackupAgent Server can map these OU's to a subgroup in the BackupAgent Server system. A reseller can login using the administrator user of the OU and can monitor a subset of backup accounts using the BackupAgent Server Management Console.

Mapping OU's to subgroups in BackupAgent Server is also done through group membership. Predefined CloudBackup Active Directory groups will be used to map its administrator in BackupAgent Server system as a subgroup if the following criteria's are met:

- Have one and only one predefined CloudBackup Active Directory group.
- (CloudBackup_Group@OU's name or CloudBackup_PrivateLabelGroup@OU's name)
- Predefined CloudBackup Active Directory group has to be within a _Private container directly below the OU's root.
- Have a valid administrator defined for that predefined CloudBackup Active Directory group. This user should belong to the same OU.

A subgroup in BackupAgent Server can also be fully private label. A reseller can then fully customize these private label settings for the Management Console as would be the case when BackupAgent Server is running in a stand-alone environment.

Users that are part of the OU and have a group membership for a backup plan can be monitored by the administrator of the OU from the BackupAgent Server Management Console.

3. Technical implementation

This chapter will explain the working of the Active Directory integration module as per version 4.3.1 of the BackupAgent server software.

3.1 Creating users

This section describes how to create users in Active Directory for integration with BackupAgent. These can be trial users or users belonging to a certain group.

3.1.1 Trial users

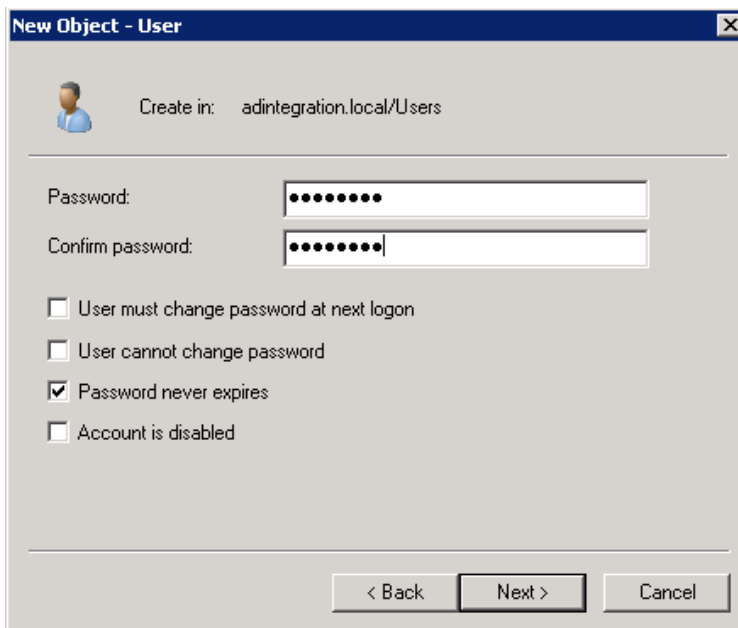
Trial users can be created in the Organizational Unit called 'Users'.

Note: Any user will obtain a trial account if it exists in Active Directory unless the option to provision trial accounts have been switched off in the BackupAgent server settings.

First you need to create a User logon name for this user.

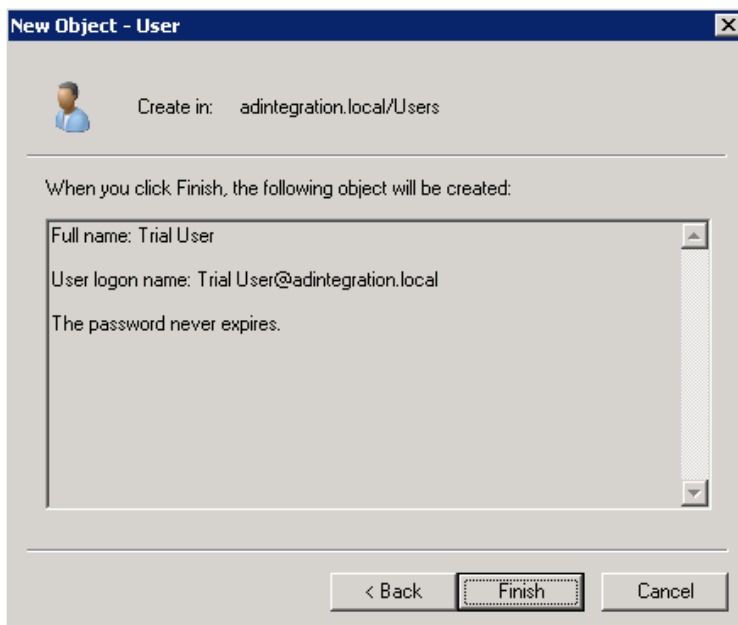
The screenshot shows a 'New Object - User' dialog box. At the top, it says 'Create in: adintegration.local/Users'. Below this, there are several input fields: 'First name' with 'Trial User', 'Initials' (empty), 'Last name' (empty), 'Full name' with 'Trial User', 'User logon name' with 'Trial User' and a dropdown menu showing '@adintegration.local', and 'User logon name (pre-Windows 2000)' with 'ADINTEGRATION\' and 'Trial User'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

You then need to create a password for this user.



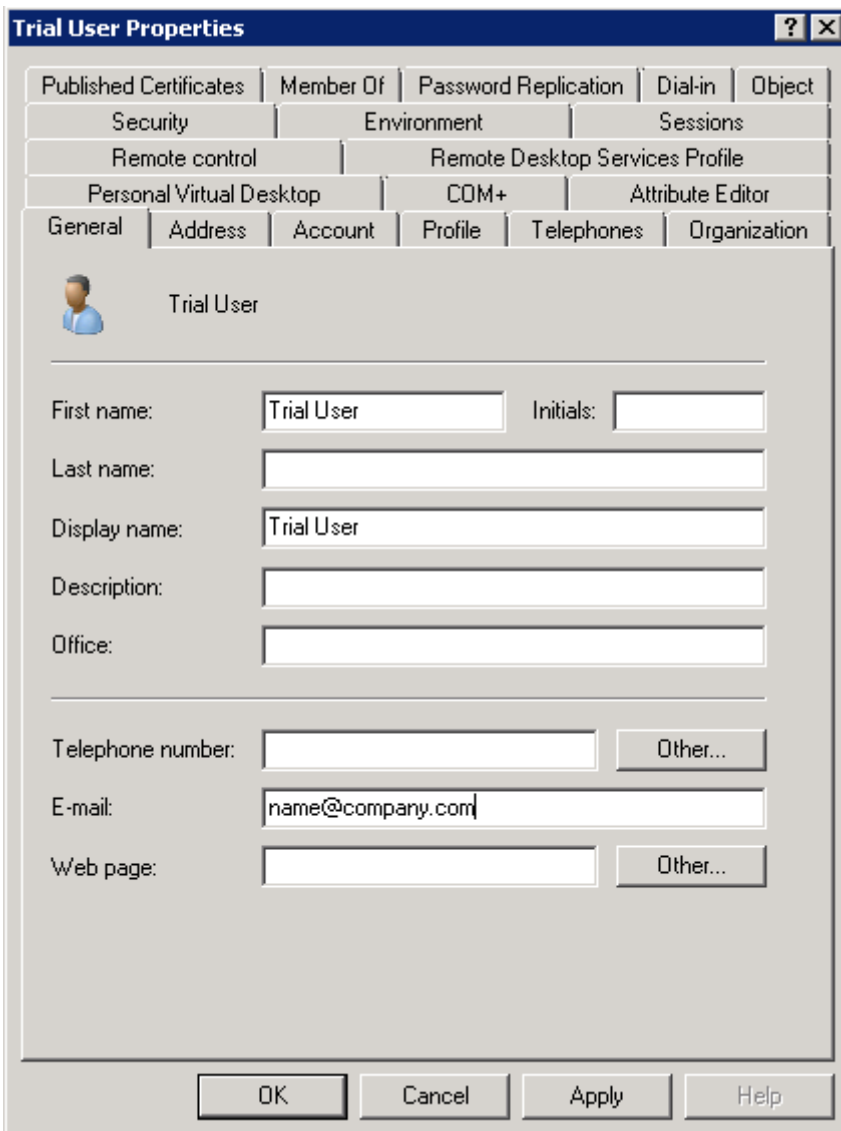
The screenshot shows a dialog box titled "New Object - User" with a close button in the top right corner. Below the title bar, there is a user icon and the text "Create in: adintegration.local/Users". The main area contains two password input fields: "Password:" and "Confirm password:", both filled with black dots. Below these fields are four checkboxes: "User must change password at next logon" (unchecked), "User cannot change password" (unchecked), "Password never expires" (checked), and "Account is disabled" (unchecked). At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

After this has been done, the user has been created.



The screenshot shows the same "New Object - User" dialog box, but now it displays a summary of the created user. The text "When you click Finish, the following object will be created:" is followed by a scrollable text area containing: "Full name: Trial User", "User logon name: Trial User@adintegration.local", and "The password never expires." At the bottom, the buttons are "< Back", "Finish", and "Cancel".

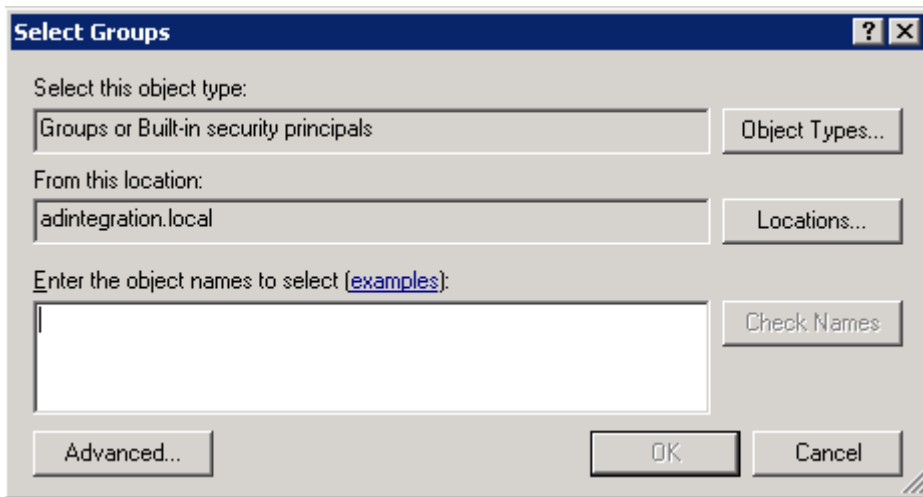
The next step is to add an e-mail address for this user. You can do this by selecting the properties of the trial user you just created.



After these steps you are ready to log on to the Management Console with this user and start using the account.

3.1.2 Active users

Active users are created the same way as a trial user. The only difference is that they are a member of a specified group. This group determines the size of the account and whether the account is a server or a workstation account. You can make this user a member of a group by selecting the properties of the user and make it a member of the group you prefer.



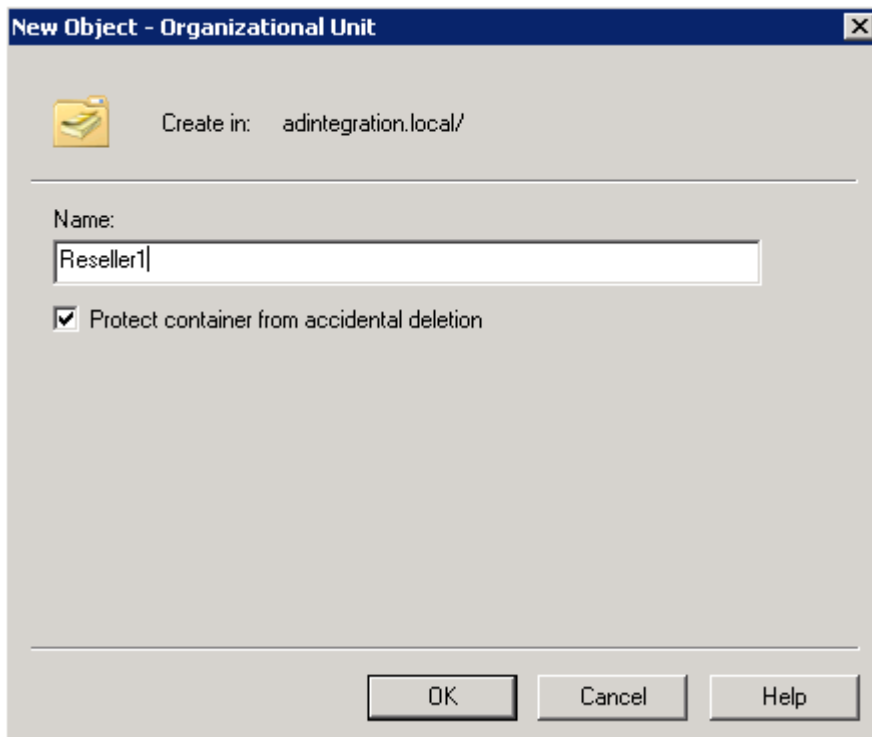
An explanation on how to create groups can be found from chapter 3 onward.

3.2 Creating groups

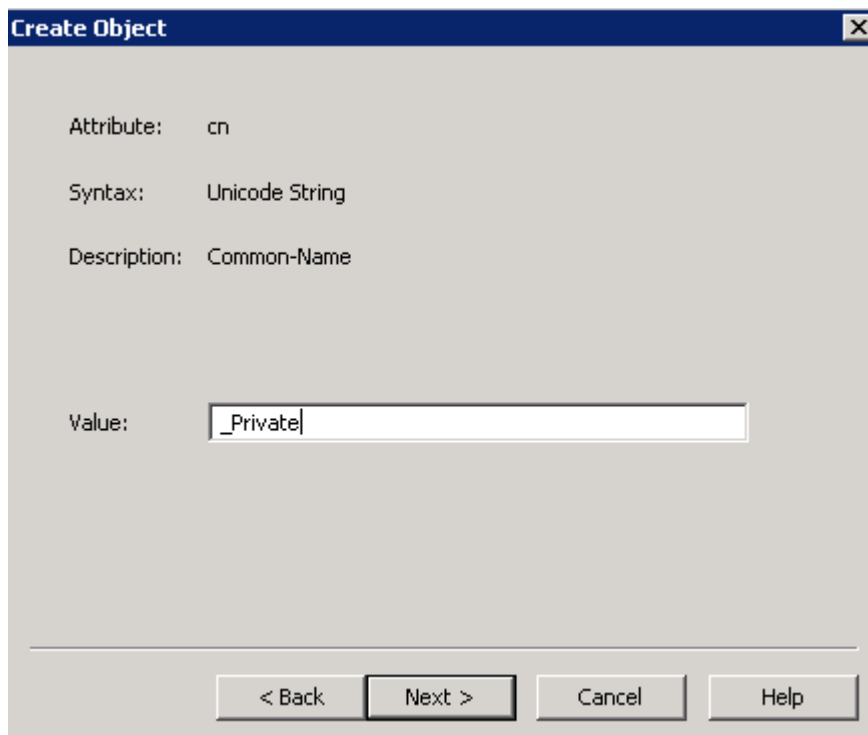
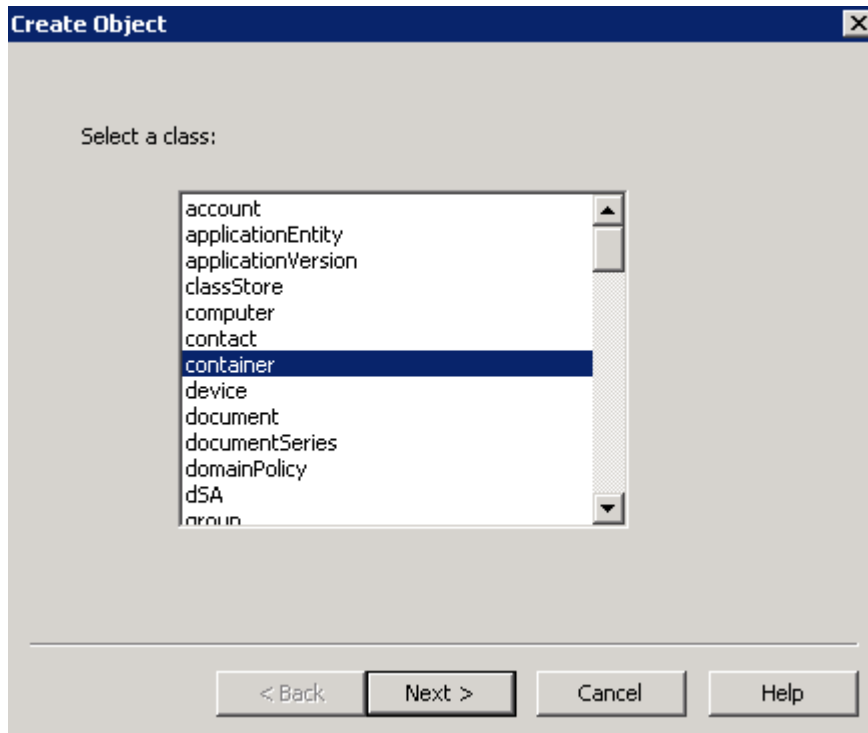
This section explains how to create reseller groups and group accounts in Active Directory.

3.2.1 Reseller groups

In order to create a reseller group, you first need to create an Organizational Unit and give it a name.



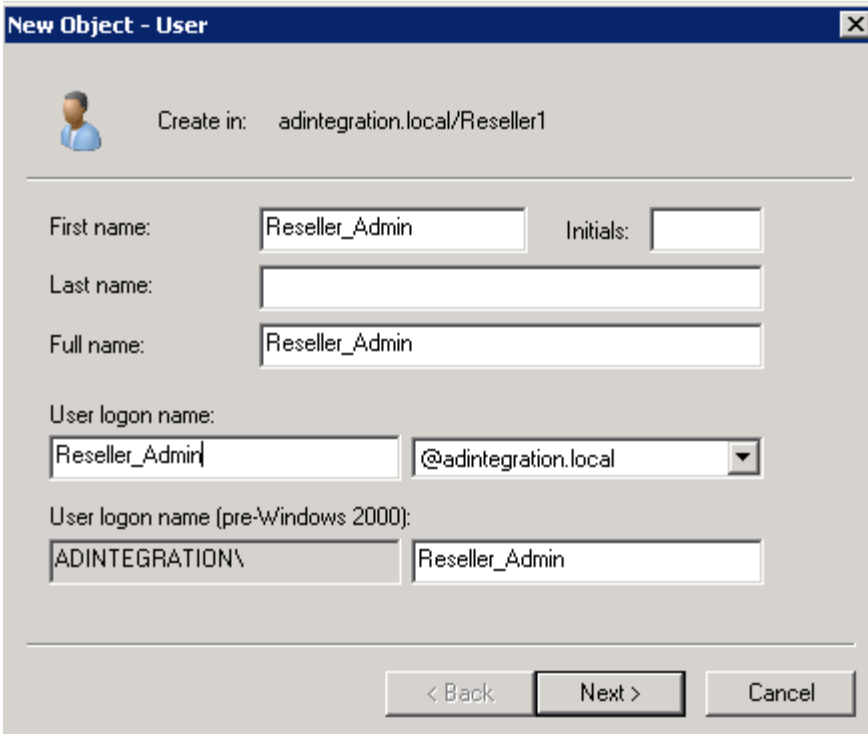
Having done this, you will need to create a Container called `_Private` using ADSI Edit. You create this container in the reseller OU you have created before.



You are now ready to determine whether this group will be a default group or a private labeled group. Go to Active Directory again and create a group in the container called `_Private` you just created with ADSI Edit, belonging to the reseller group. If you want to create a default group,

you name it CloudBackup_Group@OU and if you want to create a private labeled group you name it CloudBackup_PrivateLabelGroup@OU . In this case we made a reseller group called Reseller1, so this would result in CloudBackup_Group@Reseller1 or CloudBackup_PrivateLabelGroup@Reseller1 .

Having done this, you need to create an administrative user for this group account within this OU in Active Directory.



New Object - User

Create in: adintegration.local/Reseller1

First name: Reseller_Admin Initials:

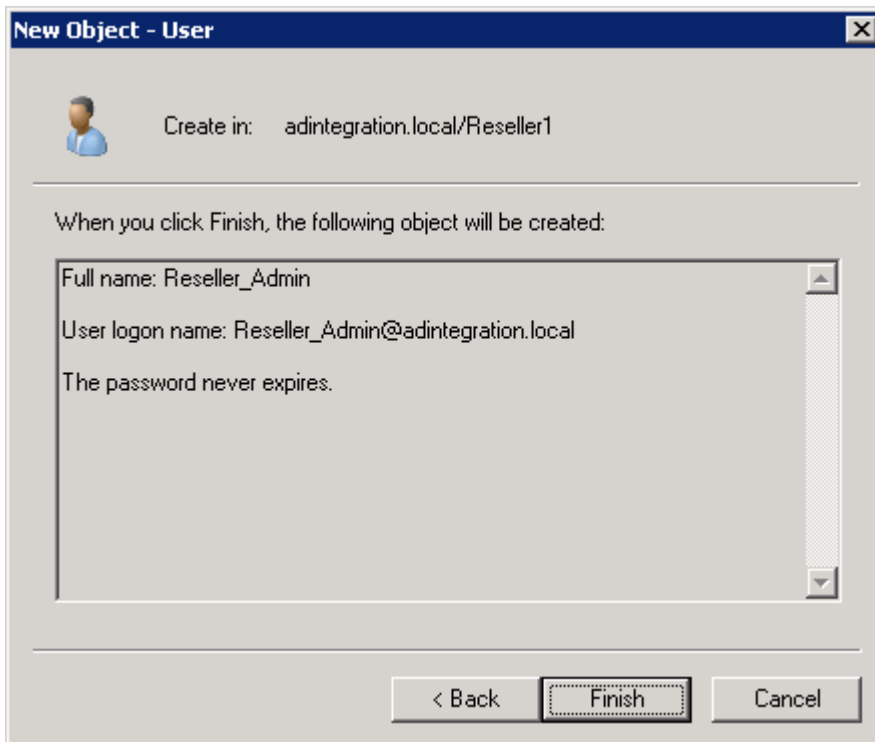
Last name:

Full name: Reseller_Admin

User logon name: Reseller_Admin @adintegration.local

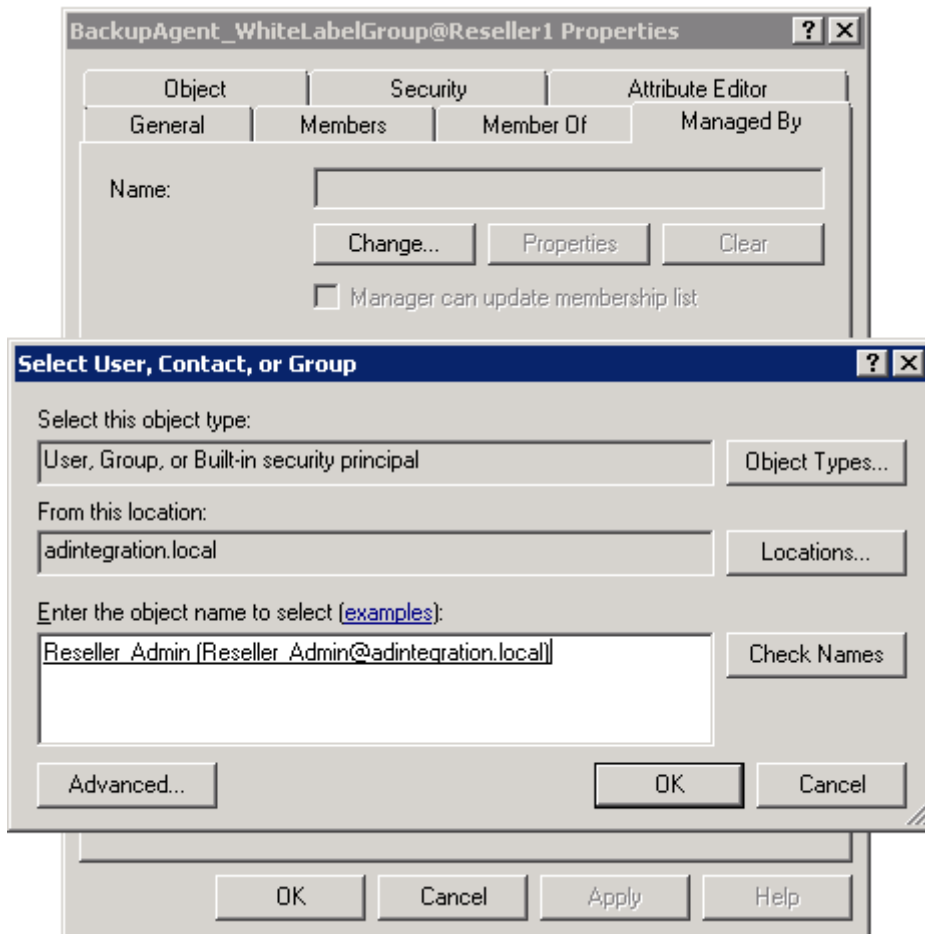
User logon name (pre-Windows 2000): ADINTEGRATION\ Reseller_Admin

< Back Next > Cancel



Do not forget to set an e-mail address of for this administrative user after you are done creating it. You can do this by selecting the properties of this user.

When you are finished, go to properties of the default or private labeled group you created and at the tab 'Managed By' set the administrative user you just created.



You are now ready to log on with this administrative user to the Management Console.

Note: If an OU is configured as such and has a parent OU in the Active Directory that is also configured as a group in BackupAgent that hierarchy will be inherited and visualized in the BackupAgent system.

Also: Any user in a child OU of an OU which is set up to be a CloudBackup group will end up being a user in the Administrator group, due to limitations in the security model of Active Directory.

3.3 Creating Account types

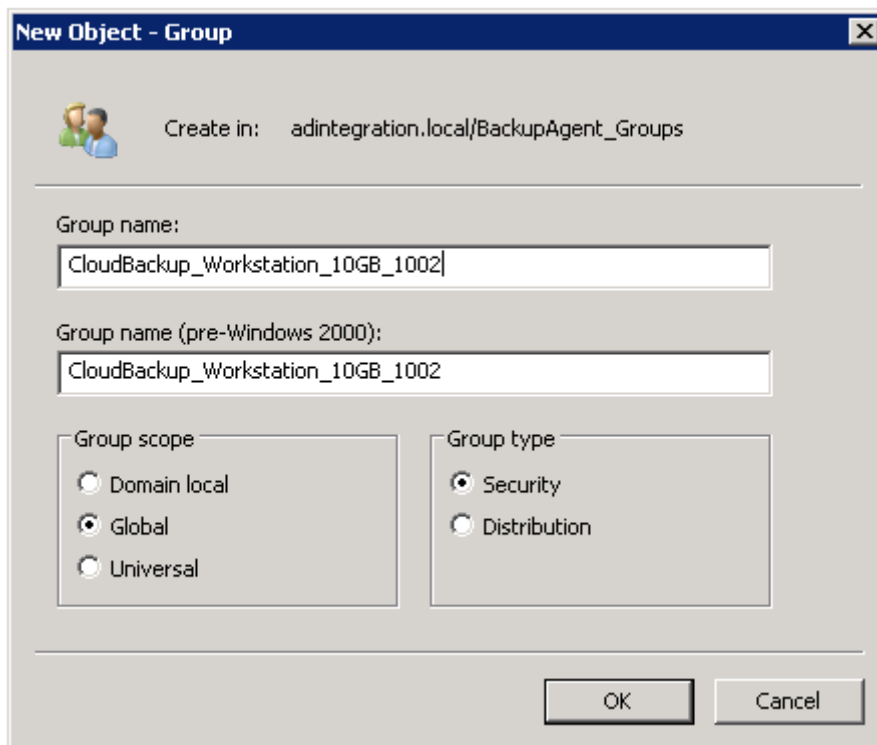
In order to determine the size and the type of each account you create, you need to make each user a member of a certain group in which the size and type is determined. This section explains how to create such groups.

3.3.1 Account type

For each account type you want, you need to make a new group. It is possible to create additional OU's to maintain the different account types. To create a group that determines the size and type of the account, it needs to contain the types and sizes, as well as the ID of the storage location you want the user to be a part of.

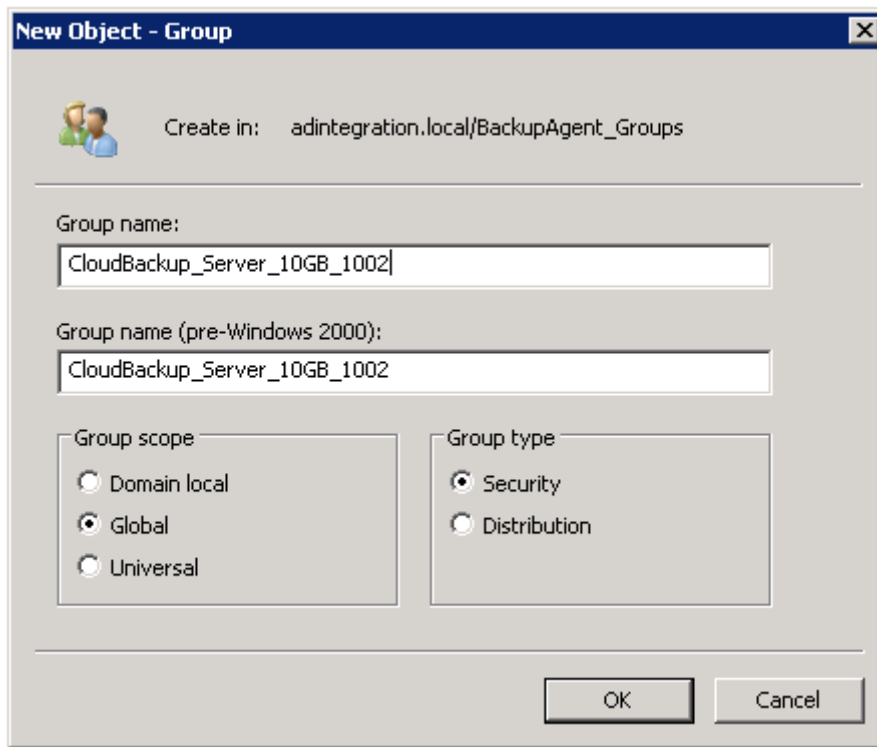
Say you want to create a workstation user account, with a size of 10 GB, where the storage ID is 1002. You then create a group with the following name:

CloudBackup_Workstation_10GB_1002

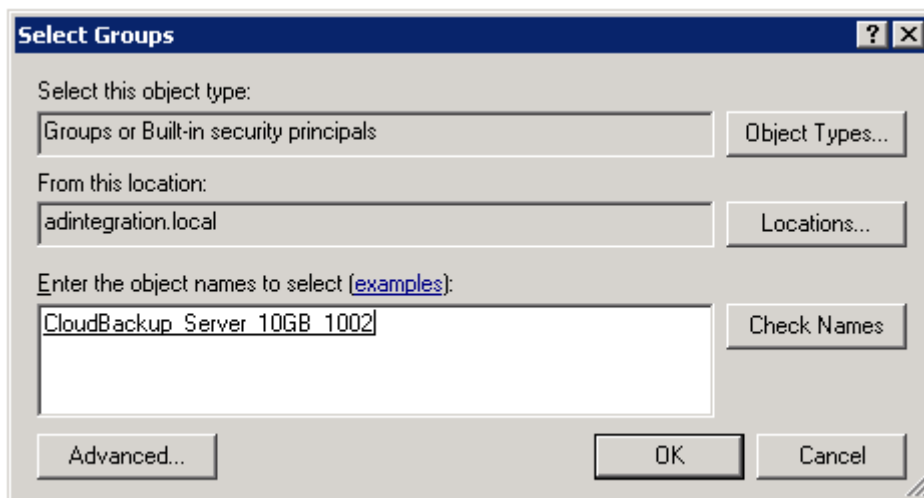


If you want to create a professional user account, with a size of 10 GB, where the storage ID is 1002, you create a group with the following name:

CloudBackup_Server_10GB_1002



After having created a group, you can now make a user a member of this group.



After having done this, you can now log on to the Management Console with this user. Do not forget to assign an e-mail address to this user, or you will not be able to log on.