INTELLISNAP® TECHNOLOGY FIELD GUIDE

PURE STORAGE® FLASHARRAY™

COMMVAULT® SIMPANA 10

Prepared by Commvault

Distribution: Public

Publish Date: January 21, 2015

Version History

Version Number	Revision Date	Contributor's Name	Revision Description
1.0	January 21, 2016	Roy Child Jonathan Howard	Initial release

Table of Contents

IntelliSnap® Technology Field Guide Overview

The IntelliSnap® Technology Field Guide provides a detailed description for configuration hardware based snapshot protection within the Commvault® platform. This guide is an introductory overview of the Pure Storage FlashArray storage array, its associated architecture and features, along with licensing and configuration requirements to integrate these controls within Commvault software. This guide covers multiple storage environments and use cases in detail with best practices for configuring and scheduling policies to achieve consistent results for both operational recovery and protection requirements.

Commvault IntelliSnap technology enables a modernized approach to operational recovery by leveraging array based snapshot technology and making it an automated part of the protection/backup process. By automatically integrating with storage array technology, Simpana software is able to automatically discover volume/disk configurations for snapshot operations and coordinate these operations with proper application integration. This minimizes the administrative configuration and eliminates manual scripting requirements.

The IntelliSnap technology process is defined and scheduled to automatically quiesce the selected system or application, and to create a persistent snapshot within the production storage array. The speed at which these protection operations complete allows for consistent protection copies to be created in minutes, regardless of the size of the dataset, ensuring that critical RPO/RTO requirements can be adhered too. Once these primary protection operations have been completed the production system(s) are returned to normal operations and are not part of any secondary operations, thus insuring that load on the production system is minimized.

Unlike other hardware-based snapshot approaches IntelliSnap technology extends beyond just creating or deleting snapshots. Secondary operations are automatically mounted to a proxy server which will mount the snapshots for further processing, whether that is further indexing or cataloging of the data or creating longer term copies of the data to deduplicated disk, cloud copies, or tape. This content aware process provides rapid recovery options whether a full system recovery or a single file is required. The scheduling and retention is also managed inside of Commvault software to ensure that only the relevant amount of data is retained for recovery minimizing the overhead on the production arrays.

These recovery capabilities can be securely delegated to application and recovery users to ensure that this advanced technology can bring speed and efficiency of array technology directly into the hands of the end users, safely and securely.

IntelliSnap technology supports the leading storage solutions from Pure Storage, INFINIDAT, Dell, EMC, Fujitsu, Hitachi, HP, IBM, NetApp, and Oracle – and this list continues to expand. Please visit www.commvault.com for the most up to date revision of the supported hardware and software configurations.

Pure Storage FlashArray Storage Overview

Pure Storage's FlashArray line of storage systems enable customers to improve storage and application performance and simultaneously reduce their storage footprint. FlashArray combines the high throughput and low latency of flash storage with built-in deduplication and compression to provide extremely high application performance with effective density as high as 40TB per rack unit. Price points are competitive to spinning disk.

FlashArray is targeted primarily at database workloads, where the latency and throughput improve application response time, and virtual desktop and server workloads, where performance and scalability are increased. Pure Storage also markets a FlashStack architecture that combines FlashArray with Cisco UCS servers and networking.

In addition to high performance and density, FlashArray is designed to be simple to buy, deploy and manage. Products are aligned to small, medium and large configurations. Physical installation is intended to be appliance-like, with minimal cabling required. Capacity expansion and performance upgrades are transparent and non-disruptive. Provisioning takes just a couple of clicks, with no configuration of RAID groups or storage pools. The arrays self-tune and self-monitor and will proactively open support cases automatically when issues are detected.

Density is achieved through a combination of capabilities. All storage is thin provisioned, consuming only space as needed. All data is deduplicated and compressed on ingestion, with variable block size from 512B to 32KB (up to 128KB on //m) optimizing reduction across workloads. Compression and deduplication deliver an average of 5:1 reduction across all deployed arrays and workloads. Post-processing compression further reduces storage consumption. And because blocks are single instance, snapshots, clones and replication do not consume space without data change.

FlashArray includes additional features that protect data integrity and privacy. All data at rest is encrypted in hardware, with no performance penalty or key management required. Pure Storage's proprietary RAID-3D algorithm protects against data corruption and multiple drive loss with no significant performance impact.

FlashArray connectivity is available in fibre channel, iSCSI and combinations of the two. Specific available configurations vary depending on the array model.

FA-400 Series

//m Series

Model	Max Capacity (raw / effective*)	Max IOPS**	Max Throughput	Onboard Ports	Additional IO
FA-405	11TB / 35TB	100,000	3GB/s	2x1Gb/s Ethernet (Management) 2x1Gb/s Ethernet (Replication)	4x8Gb/s Fibre Channel or 4x10Gb/s iSCSI

Model	Max Capacity (raw / effective*)	Max IOPS**	Max Throughput	Onboard Ports	Additional IO
FA-420	35TB / 100TB	150,000	5GB/s	2x1Gb/s Ethernet (Management) 2x1Gb/s Ethernet (Replication)	8x8Gb/s Fibre Channel or 8x10Gb/s iSCSI or 8x8Gb/s Fibre Channel and 4x10GB/s iSCSI or 8x10Gb/s iSCSI and 4x8Gb/s Fibre Channel
FA-450	70TB / 200TB	200,000	7GB/s	2x1Gb/s Ethernet (Management) 2x1Gb/s Ethernet (Replication)	8x16Gb/s Fibre Channel or 8x10Gb/s iSCSI or 12x16Gb/s Fiber Channel or 12x10Gb/s iSCSI or 8x10Gb/s iSCSI and 4x16Gb/s Fiber Channel or 8x16Gb/s Fibre Channel and 4x10Gb/s Ethernet
//m20	40TB / 120TB	150,000	5GB/s	4x10Gb/s Ethernet (iSCSI or Replication) 4x1Gb/s Ethernet (Management) 8x12Gb/s SAS	6 IO Slots Mix and Match: 2-port 8Gb/s Fibre Channel 2-port 10GB/s iSCSI
//m50	88TB / 250TB	220,000	7GB/s	4x10Gb/s Ethernet (iSCSI or Replication) 4x1Gb/s Ethernet (Management) 8x12Gb/s SAS	6 IO Slots Mix and Match: 2-port 16Gb/s Fibre Channel 2-port 10GB/s iSCSI
//m70	136TB / 400TB	300,000	9GB/s	4x10Gb/s Ethernet (iSCSI or Replication) 4x1Gb/s Ethernet (Management) 8x12Gb/s SAS	6 IO Slots Mix and Match: 2-port 16Gb/s Fibre Channel 2-port 10GB/s iSCSI

*Effective capacity is estimated based on reduction through thin provisioning, deduplication and compression. Actual capacity may vary based on customer data.

**IOPS are based on 32KB writes.

This is **NOT** a Pure Storage Administrators / Maintenance Training and Manual Guide. For Pure Storage documentation, please visit www.purestorage.com.

FlashArray Volumes and Snapshots

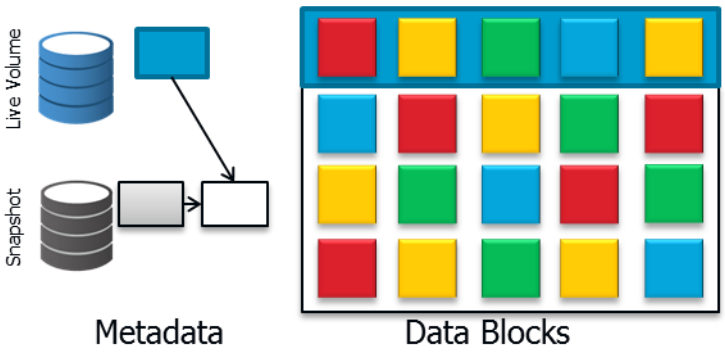
A Volume is the logical unit of storage presented to a host. Volumes are thin provisioned, and data blocks are deduplicated against all other blocks in the array. Volumes can have snapshots and copies created from them with zero additional initial storage use. As there are no storage pools, all volumes share the entire array and the deduplicated blocks. FlashArray maintains a multi-level metadata layer that tracks data block use by volumes. Metadata is constantly optimized to ensure peak performance. Volumes can be sized from 1MB to 4PB and can be resized on the fly.

FlashArray volumes can be copied to create new volumes identical to the original. The copy operation simply creates new metadata, making the operation instantaneous and consuming no additional storage. Copied volumes are independent of the original volume and can be mapped, unmapped and resized without affecting the original volume. Snapshots can also be created from copied volumes independent of the original volume.

Snapshots on FlashArray are effectively read-only volumes with a dependency on the source volume. Creating a snapshot is the same as copying a volume, with no additional storage consumption or performance impact. Volumes can be restored in hardware (reverted) to any snapshot, essentially another volume copy and snapshots can be copied into new volumes. Because all of these operations are in metadata they are all instantaneous, regardless of volume size or data change.

Snapshots on FlashArray are not deleted during revert operations. Volumes can be reverted to an older recovery point and then rolled forward to a later point.

Because snapshots are read-only they cannot be presented directly to a host. A snapshot must first be copied to a new volume. During mount operations, IntelliSnap software copies the snapshot to a new volume and maps that volume. The copy volume consists of pointers to the existing data blocks and consumes no additional space unless unique blocks are written to the new volume. The copy volume and any new data are deleted after the unmount operation is complete.



Integration Requirements for IntelliSnap® Technology

Required Pure Storage License

All FlashArray functionality is included in the license provided with the storage array. No additional licensing is required for IntelliSnap software integration.

Commvault® Licenses

Enabling IntelliSnap tehnology may require additional licensing in Simpana. The required licenses depend on whether the customer is under a capacity license agreement (CLA) or traditional agents and options licensing.

- For CLA, customers require enough Data Protection Snapshot licensing to cover the size of the application data being protected. For backup copy operations an equal amount of Data Protection Core or Data Protection Enterprise is required.
- For agents and options, customers require a Hardware Snapshot Enabler license for each client computer where IntelliSnap technology will be enabled. Note that only production hosts require the enabler license; it is not required for proxies unless they are also acting as production hosts.

Commvault® Software

IntelliSnap technology solutions will require the appropriate data agents as defined by the customer configuration. Below we will define a few terms in use going forward in this document:

- **Production Host** – Server hosting the actual production LUN for snapshot operations
- **Proxy Host** – Server mounting the snapshot for backup purposes off of the Production Host
- **Array** – Hardware Storage Array executing the snapshots
- **File System iDataAgent** – iDataAgent for protecting the file system of a host and is also a base requirement for most Application iDataAgents.
- **MediaAgent** – Agent for creating and managing snapshots as well as for writing data to backup targets
- **Application iDataAgent** – iDataAgents to protect applications such as SQL, Exchange, DB2, SAP and Oracle. Enables Application Aware snapshots to be created when protection operations are scheduled. See Simpana Documentation for a current list of agents supported on Pure Storage arrays.
- **Virtual Server Agent (VSA)** – iDataAgent providing protection of Virtualization Environments without installing backup iDataAgents internal to the guests
- **Commvault VSS Software Provider** – Commvault VSS Software Provider for Windows Guests to allow for programmatic controls of the Windows VSS components
- **Commvault VSS Hardware provider** – Commvault VSS Hardware Provider for Windows enables VSS snapshot control on Windows Server 2012 Hyper-V hosts

Basic File System Environments

As with all configurations, a CommServe, necessary storage capacity, and MediaAgents must exist to enable a completely functional solution. On top of the basic infrastructure components, the IntelliSnap software base configuration requires the following agents on the Production Host:

- File System iDataAgent (for the appropriate operating system)
- MediaAgent
- Commvault VSS Software Provider (Windows only)

For a configuration where snapshots mount off-host to a Proxy server, implement the following agents on the Proxy server:

- File System iDataAgent (Must be similar to production host operating system)
- MediaAgent

Application Environments

When implementing IntelliSnap technology for a specific application simply add the appropriate application iDataAgent to the base configuration as follows on the production host:

- File System iDataAgent (for the appropriate Operating System)
- MediaAgent
- Commvault VSS Provider Software Provider (Windows Only)
- Application iDataAgent for selected Application
  - Exchange – use the Exchange Database iDataAgent
  - DB2 – use the DB2 iDataAgent
  - Microsoft SQL – use the MSSQL iDataAgent
  - Oracle – use the Oracle iDataAgent

- SAP – use the SAP iDataAgent
- MySQL – use the MySQL iDataAgent
- PostgreSQL – use the PostgreSQL iDataAgent
- Lotus Notes – use the Notes iDataAgent
- Sybase – use the Sybase iDataAgent

For a configuration where snapshots mount off-host to a proxy server, implement the following agents on the proxy server:

- File System iDataAgent (operating system must be similar to the production host)
- MediaAgent
- Application-specific iDataAgent to enable proxy, if required for the application
- Application API (i.e. – Exchange Management Pack, Oracle for RMAN integration, etc.)

VMware Environments

IntelliSnap technology integration with the Virtual Server iDataAgent (VSA) for VMware enables point-in-time hardware snapshots to provide rapid data protection and recovery operations for virtual guests. Using a dedicated ESX server for selective copy to Tier 2 storage completely removes any utilization on the production ESX farm. The copy operation to Tier 2 storage enables granular recovery of individual files and folders. To enable IntelliSnap technology for the VMware environment ensure the following:

- File System iDataAgent for Windows
- MediaAgent
- Virtual Server Agent (VSA) iDataAgent

The Virtual Server Agent may be run as a physical proxy server in SAN transport mode. It may also be run as a Hot Add mode virtual guest external to the production farm to eliminate production processing. The Virtual Server Agent enables proxy capabilities with no agents installed on the ESX server.

Hyper-V Environments

IntelliSnap technology integration with the Virtual Server iDataAgent for Hyper-V enables point-in-time hardware snapshots to provide rapid data protection and recovery operations for virtual guests. Using a dedicated Hyper-V server for selective copy to Tier 2 storage completely removes any utilization on the production cluster. The copy operation to Tier 2 storage enables granular recovery of individual files and folders. To enable IntelliSnap technology for the Hyper-V environment ensure the following:

- File System iDataAgent for Windows
- MediaAgent
- Virtual Server Agent (VSA) iDataAgent
- Commvault VSS Hardware Provider on Windows Server 2012

In Hyper-V environments IntelliSnap software will create a hardware snapshot for each host connected sharing the Cluster Shared Volume hosting the protected guest(s) unless the VSA is configured for single snapshots. Ensure enough capacity and licensing exist on the array to contain the snapshot data. See Commvault Documentation for details and caveats on configuring single snapshots.

Supported Applications and Operating Environments

Please visit Commvault Documentation for a complete listing of Applications and Operating Environments supported with IntelliSnap technology and any potential solution caveats.

FlashArray Configuration Details

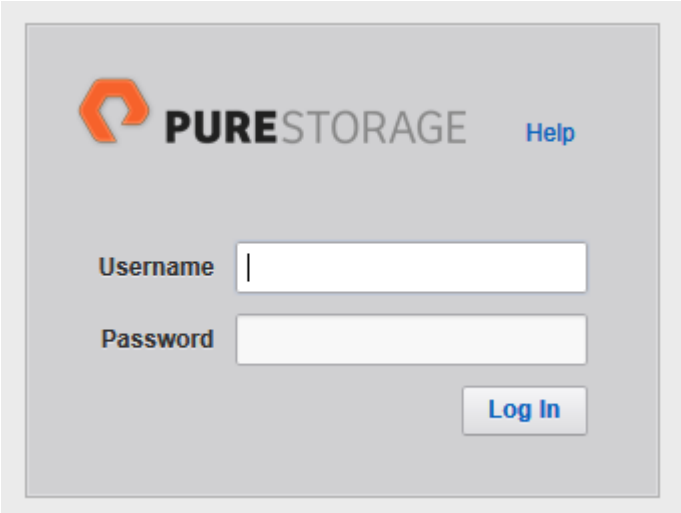
The Pure Storage FlashArray includes everything required to perform IntelliSnap software operations. To ensure proper functionality the following section describes how to create a volume, create a host, map the volume, check the Purity Operating System version and get the API Token that is utilized for authentication between Commvault software and the Pure Storage array.

To successfully provision storage for IntelliSnap technloogy, you require the following steps to create, assign and map logical devices for production host use as well as creating a device group for local replication use:

- Create a volume
- Create a host
- Map the volume to the host
- Create an API token

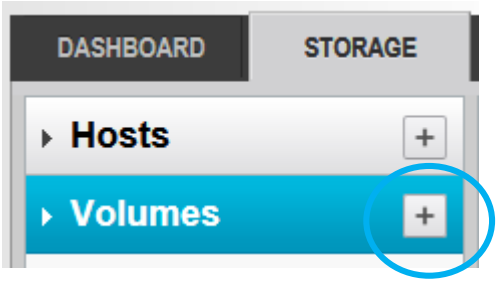
FlashArray Management Console

The FlashArray Management Console is a web application that is accessed from any browser. Enter the name or IP address of the FlashArray management virtual IP address in the address bar to access the GUI console. Enter the array credentials to login. If the password for the pureuser account has not been changed, you can login by pressing Ctrl+Q.

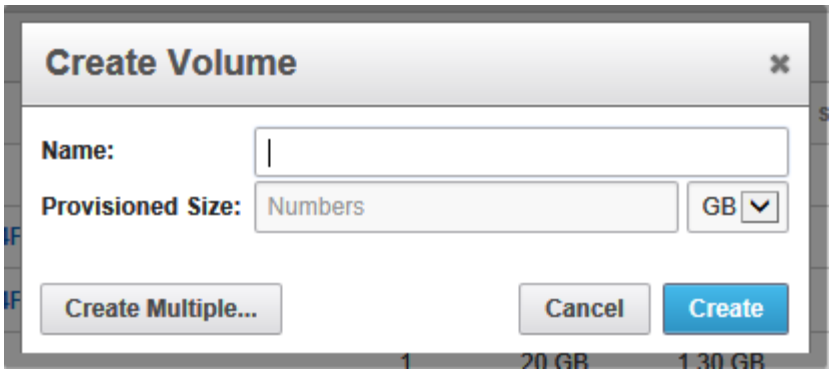


Creating a Volume

Volumes are created on the Storage tab. Click the + button on the Volumes bar to create a new volume or volumes.

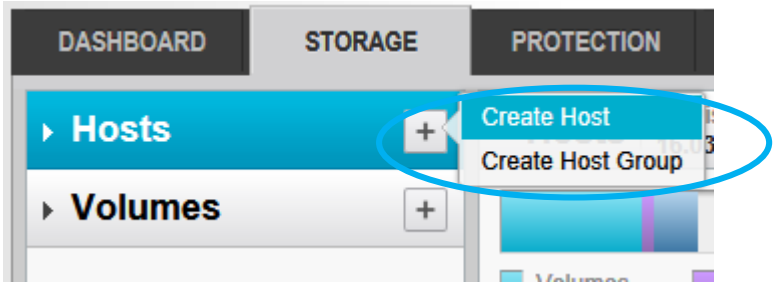


Enter a name and provisioned size for the volume and click OK. Note that all volumes are thin provisioned and deduplicated, so no space is consumed until unique blocks are written to the volume. To create multiple volumes with the same size click the Create Multiple button and enter the appropriate information.

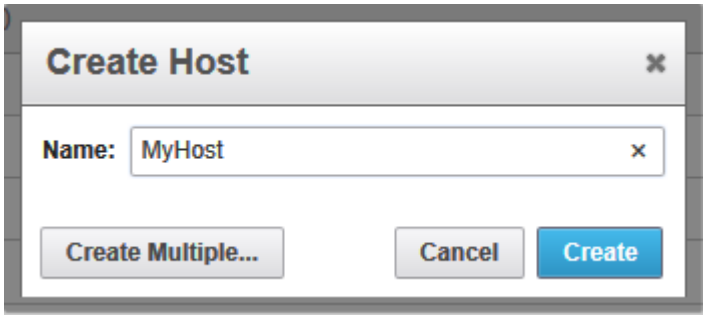


Creating a Host

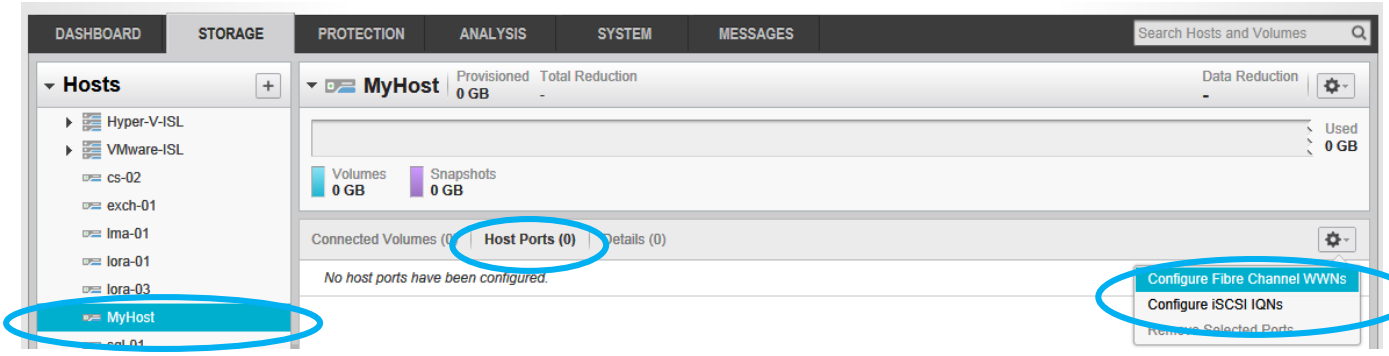
To create a host, from the Storage tab, click the + button on the Hosts bar and select Create Host.



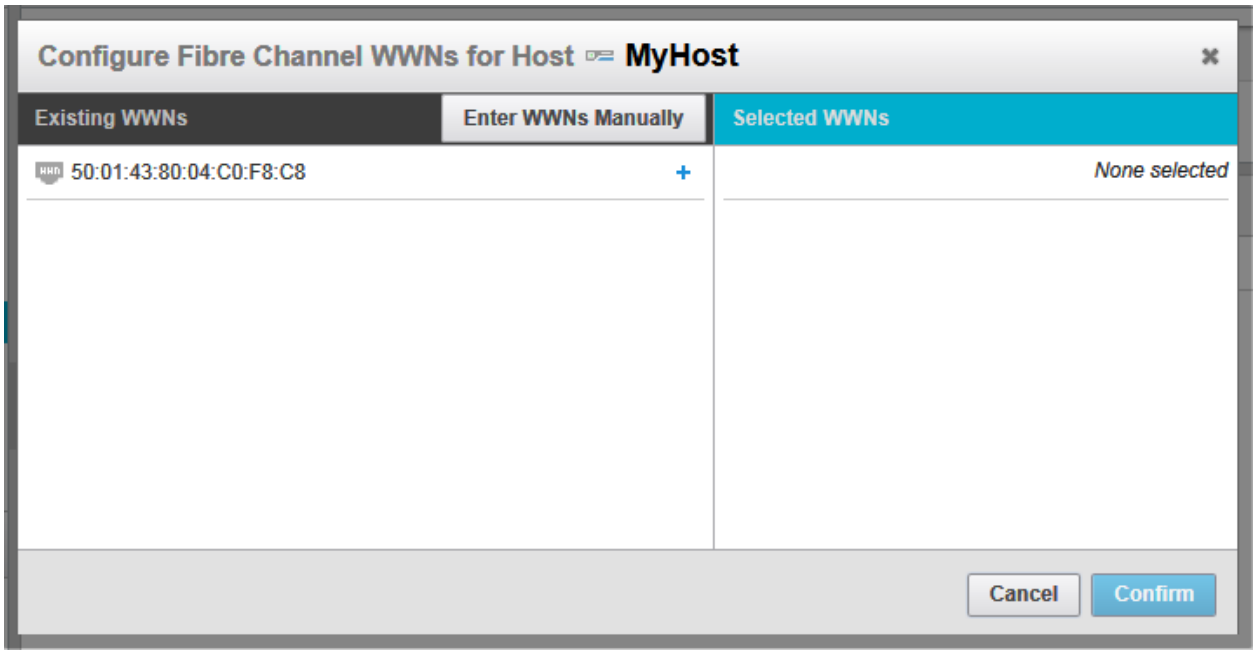
Enter a name for the host and click the Create button. To create multiple hosts using a naming pattern click the Create Multiple button and enter the appropriate information.



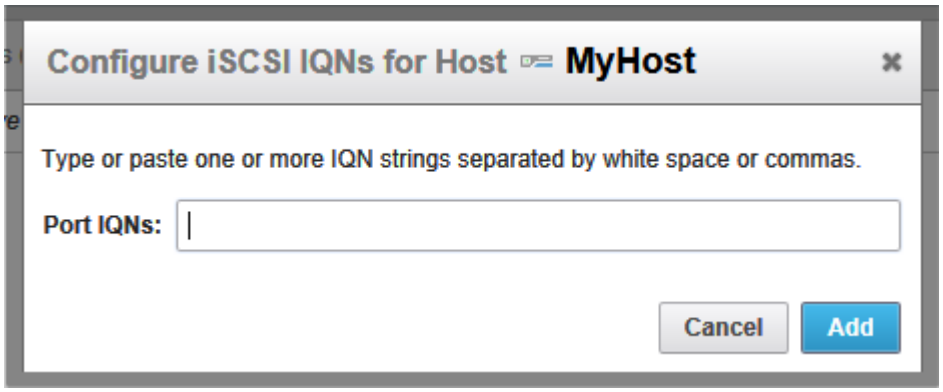
Once the host is created it needs fibre channel or iSCSI addresses need to be associated to it. To add addresses, select the host from the Hosts list, then click Host Ports. Click the gear icon at the right and select either Configure Fibre Channel WWNs or Configure iSCSI IQNs as appropriate. Follow the instructions on the screen that appears.



For fibre channel, unallocated logged-in WWNs will be listed. Either click the desired WWNs to select them, or click Enter WWNs Manually to add a WWN that is not logged in.



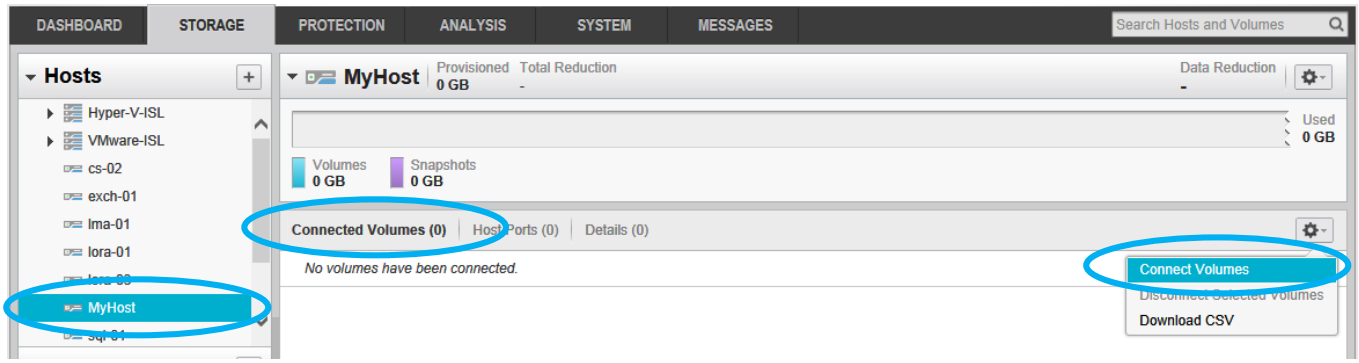
iSCSI IQNs must be added manually. Multiple IQNs can be added at the same time.



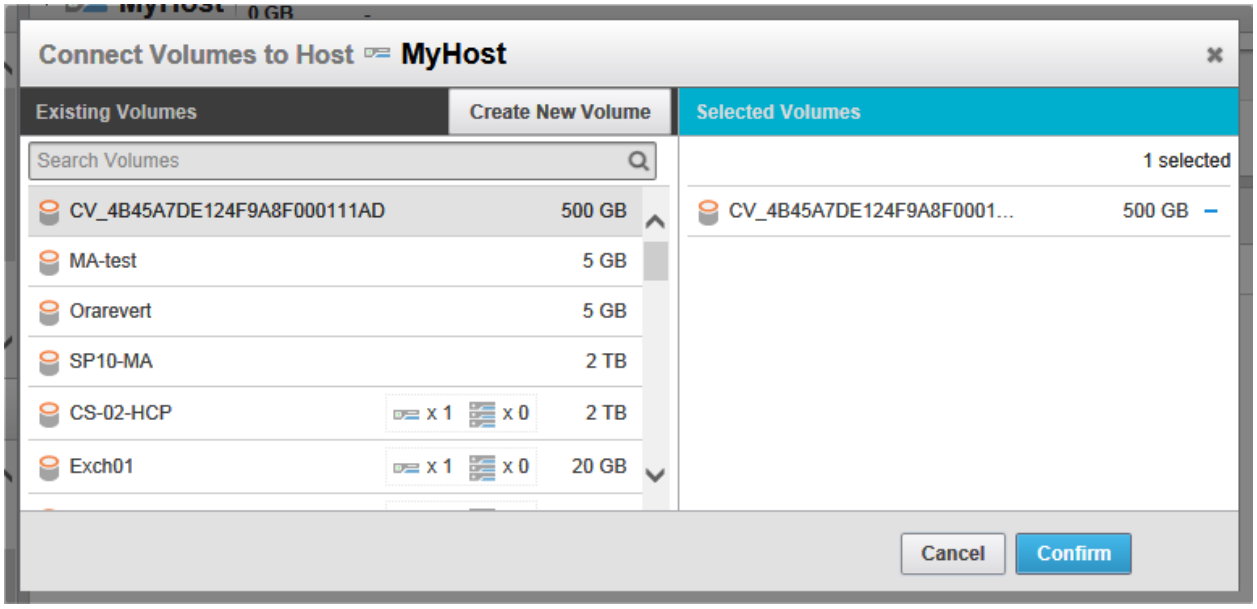
Repeat the process for all hosts where snapshots will be created or mounted.

Mapping a Volume to a Host

Volumes can be mapped from the Volume details or Host or Host Group details views. This section explains the Host view, but the process is nearly identical. From the Host details, switch to the Connected Volumes tab. Click the gear icon at the right and select "Connect Volumes."



Clicking a volume or volumes on the left will select them for mapping to the host. Volumes already mapped will show host and host group icons with the number of each to which the volume is mapped. Volumes without host and host group icons are unmapped. Click Confirm when all desired volumes are selected. The selected volumes will be mapped to all available paths to the host.



Creating an API Token

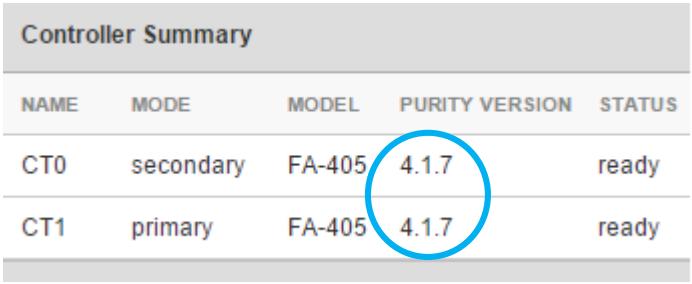
This is a one time configuration that will enable use of the Pure Storage Array within the Commvault environment. Every client that initiates snapshot operations on this Pure Storage array will utilize this configuration. If there are multiple Pure Storage FlashArrays in the environment, each one needs to be configured using this procedure.

1. Open a Web Browser and navigate to the Pure Storage Administrative Console. Login with a user that has administrative rights (e.g. "pureuser").

2. Once in the main web interface, navigate to **System**:

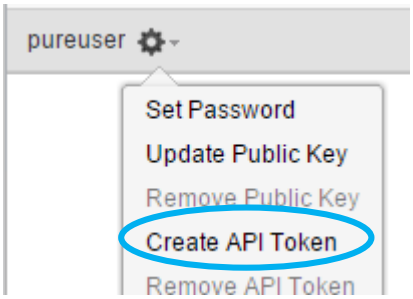
3. Select **Configuration > Array**.

4. Verify that the Purity Version is 4.1.1 (or higher) for proper IntelliSnap software functionality.

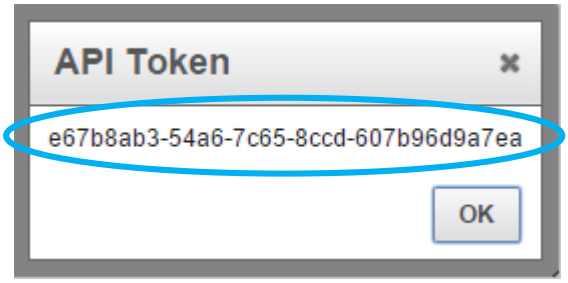


5. Select **Create API Token** from the **Dropdown Menu**. (Hover over the username to make the dropdown icon appear.)

   NOTE: If there is an existing API Token for this user, select **Show API Token** instead, and proceed to the next step.



6. The **API Token** will be displayed on the screen. Highlight it and copy it to the clipboard. This token is required for the Commvault software configuration.
   NOTE: The copy operation sometimes picks up a trailing space, which is not easily detected during paste operations. Paste into a text window such as Notepad to be sure only the API Token text was copied.



7. Click **OK**. The Pure Storage configuration is complete.

Under the Covers

IntelliSnap software interfaces with the FlashArray using the Pure Storage RESTful API. The API allows IntelliSnap software to create, copy, revert and delete snapshots. The nomenclature for snapshots created with IntelliSnap software is as follows:

<Volume Name>.SP-2-<Job ID>-<Epoch Time>

For example, a snapshot with the name Win-Test-01.SP-2-2512-1436834169 is composed as follows.

- The Primary Name of the Volume (Win-Test-01)
- SP-2 (CommCell ID #)
- Job ID (2512)
- Epoch Time (1436834169)

This naming convention is automatic, and ensures that no snapshots with identical names will be issued. The Job ID is useful to correlate specific snapshots to Job IDs in the future.

When a snapshot is copied to allow mapping to a host, the copied volume is named following the convention:

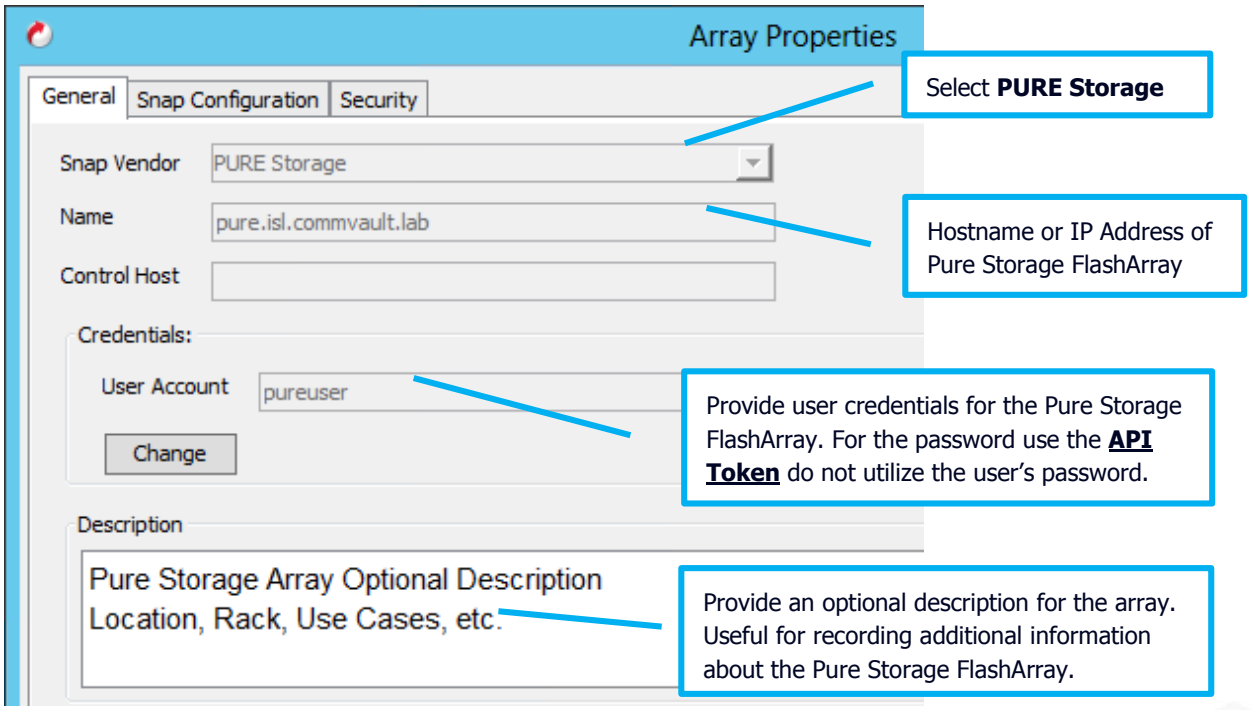
CV_<Unique ID>

- The Unique ID is generated at the time of creation.

Commvault® Array Management Configuration

The Array Management tool in the Commvault Administrative Interface records the configuration details for all arrays that will be utilized with IntelliSnap technology. This configuration is performed only one time per array, and all clients will inherit this configuration. IntelliSnap software will automatically detect the array on each client at the time of execution to ensure maximum flexibility in the configuration.

1. Open the Commvault Administrative Interface, login with a user that has administrative rights (e.g. "admin").
2. Once in the main interface, navigate to **Storage** -> **Array Management** on the top menu bar.
3. The **Array Management** menu will appear. Select **Add.**
4. The **Array Properties** menu will appear. Set options as follows to configure the Pure Storage Array:



5. Click **OK** to save the Pure Storage array configuration, and click **OK** again to exit the Array Management screen. The array is now configured in Commvault.

IntelliSnap® Technology Storage Policy Configuration

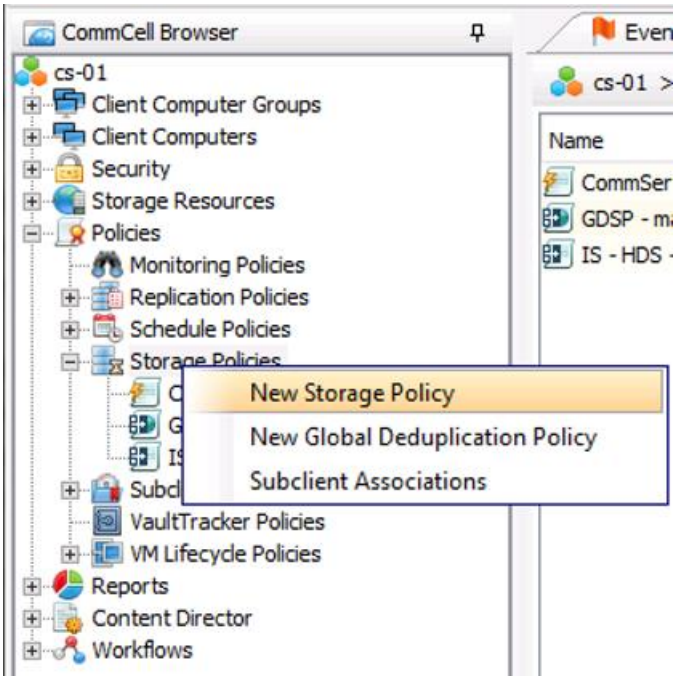
IntelliSnap software operations require a storage policy to define the retention and indexing location for the protection operation. IntelliSnap software operations can be added to an existing Storage Policy by adding a "Snapshot Copy" to it. The following sections walk through the creation and updating of a Storage Policy for use with IntelliSnap technology. There are a

number of different Storage Policy configurations, please refer to Commvault Documentation for additional options and configuration choices.

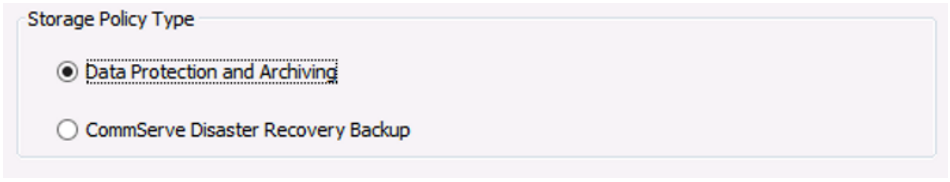
Create Storage Policy

Use the following steps to create a new Storage Policy for use with IntelliSnap technology:

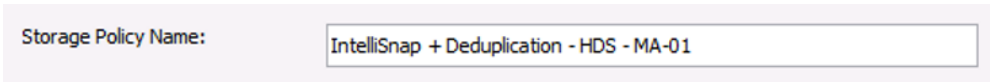
1. From the CommCell Browser, expand Policies. Right-Click on Storage Policies and select "New Storage Policy:



2. This will bring up the "Create Storage Policy Wizard" window, the default Storage Policy type is "Data Protection and Archiving", select "Next" to continue:



3. Specify the name of the Storage Policy and click Next:

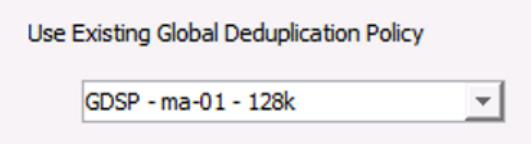


   Leave the Incremental Storage Policy, and Provide OnCommand Unified Manager Server Information blank.

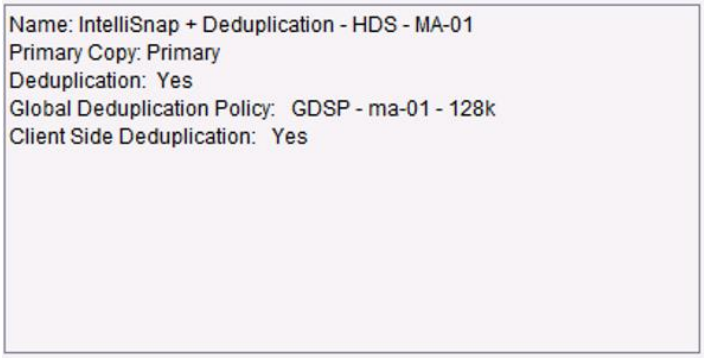
   NOTE: Storage Policies can be used to identify a number of attributes with them. In this example the Storage Policy Name shows that it is a Storage Policy that utilizes IntelliSnap technology and deduplication on HDS, utilizing MA-01. Pick a naming convention that enables ease of troubleshooting and no confusion or overlap.

4. If the usage of deduplication is planned enable the use of the Global Deduplication Storage Policy here:

5. Select the existing Global Deduplication Storage Policy:



6. Review your selections, and click Finish:

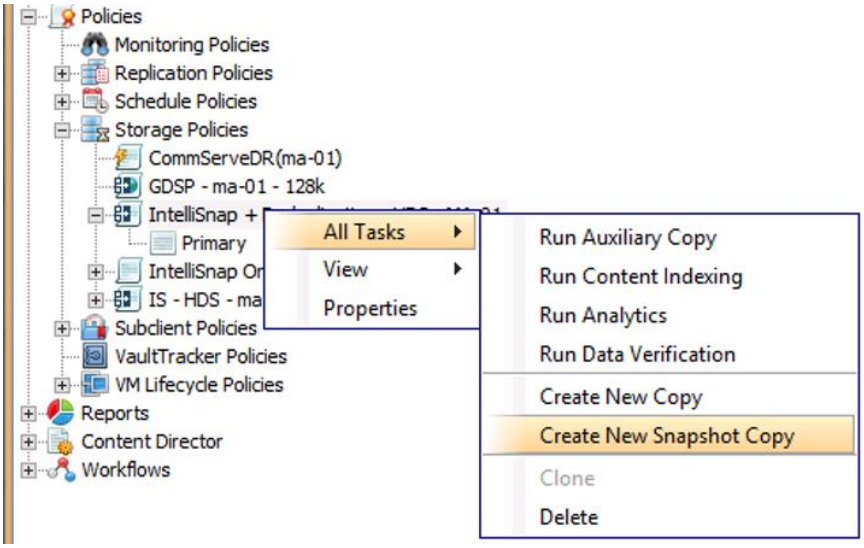


IntelliSnap® Technology Storage Policy Update

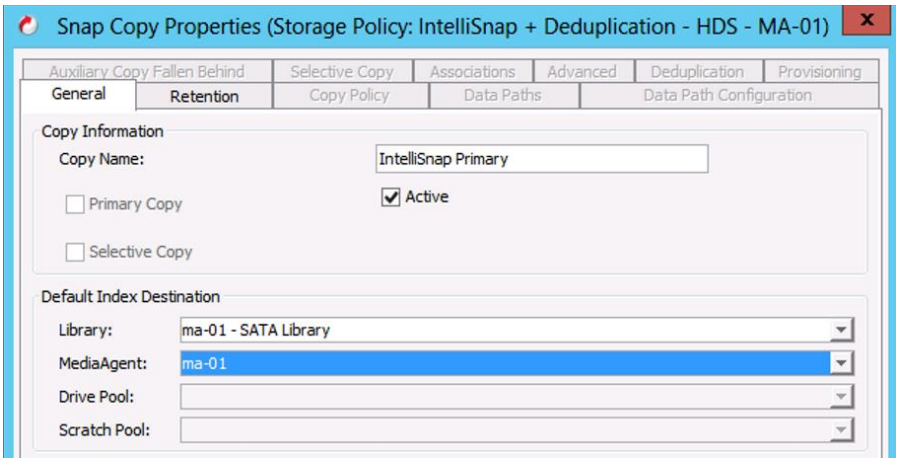
IntelliSnap software operations require a snapshot copy to house the indexing information and define the retention on the snapshots. Any currently defined storage or newly created data protection Storage Policy supports the addition of a snapshot copy.

Note: For detailed information on Storage Policy design and creation, please refer to CommVault Documentation

1. Right-Click on a Storage Policy, select "All Tasks", and then click on "Create New Snapshot Copy"



2. This will bring up the Snap Copy Properties menu for the newly create Snapshot Copy in the Storage Policy



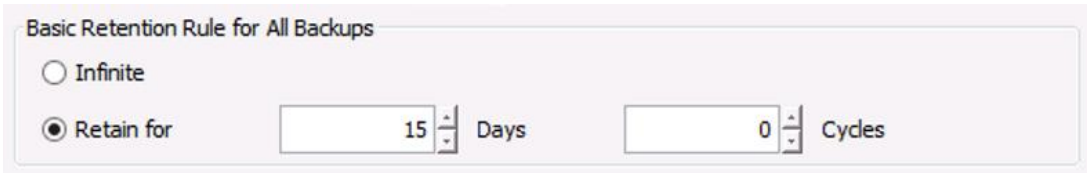
Under "Copy Name" enter a unique but easily identifiable name for this copy.

Under the "Default Index Destination" Section, define the Disk Library and corresponding MediaAgent that the IntelliSnap technology indexes will be kept.

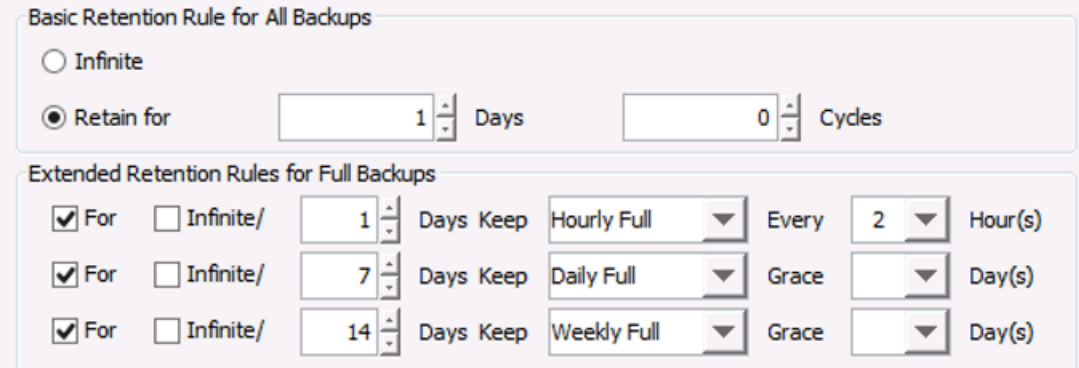
3. Select the "Retention" Tab

To store snapshots solely based on the amount of jobs that have been run, regardless of time passed, select the "Retain Snaps by Number of Jobs" setting:

To store snapshots based on days, set the amount of days under the Basic Retention Rule for All Backups, and set the Cycles to 0:



Extended Snapshots configurations can be enabled from this screen also. In the below configuration snapshots are kept for every 2 hours for the first day, and then an hourly snapshot becomes the daily snapshot and is retained for 7 days, and finally a daily snapshot is retain for 14 days as a weekly snapshot.



4. Click "OK" to create the Snapshot Copy in the Storage Policy

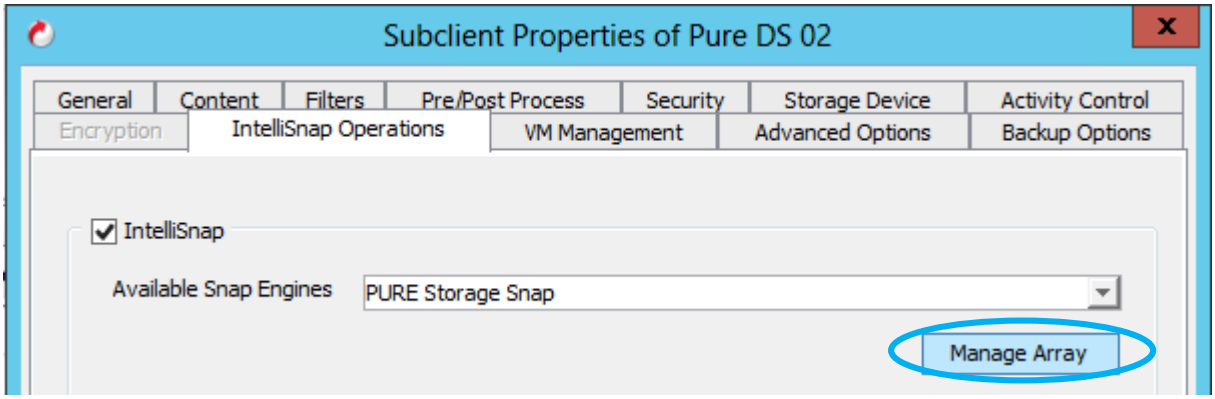
Note: Make sure the snapshot retention will not overrun the capabilities of the array.

Customizing Array Properties

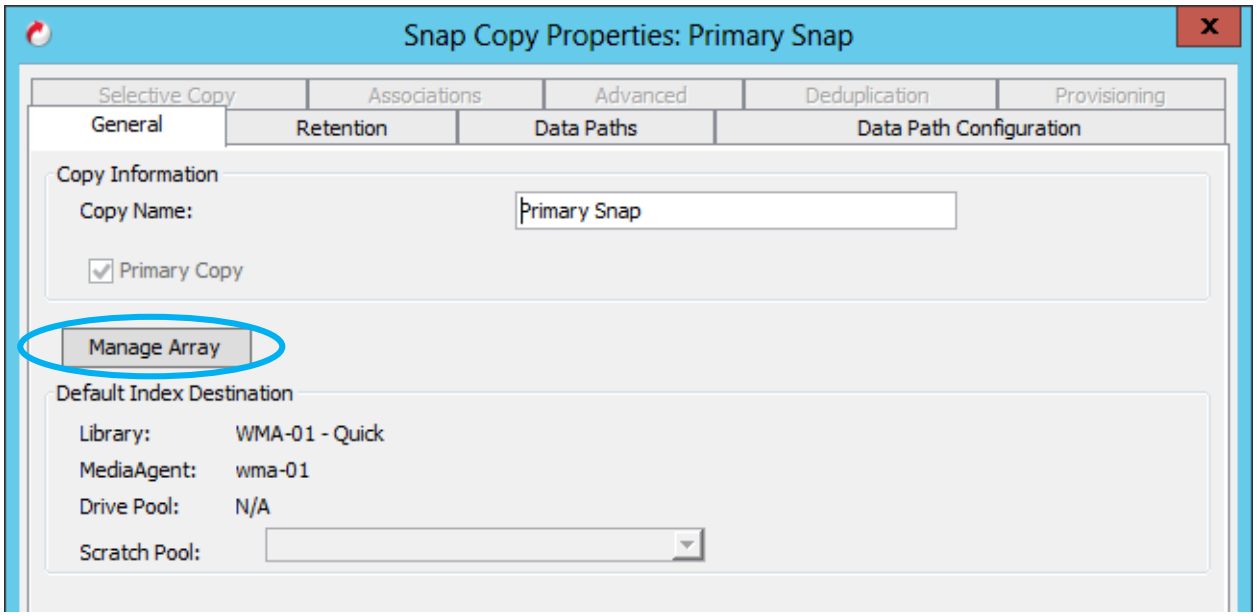
There are several Array Properties that can be set for Pure Storage arrays, however in certain instances there are some settings that are best suited to be specified at the Storage Policy or Subclient level to ensure that specific configurations are utilized only for those chosen host(s).

These types of configurations are good for changing mount and mapping behavior or enabling diagnostic logging of REST API calls.

To override at the Subclient, click the Manage Array button on the **IntelliSnap Operations** tab in the Subclient properties.

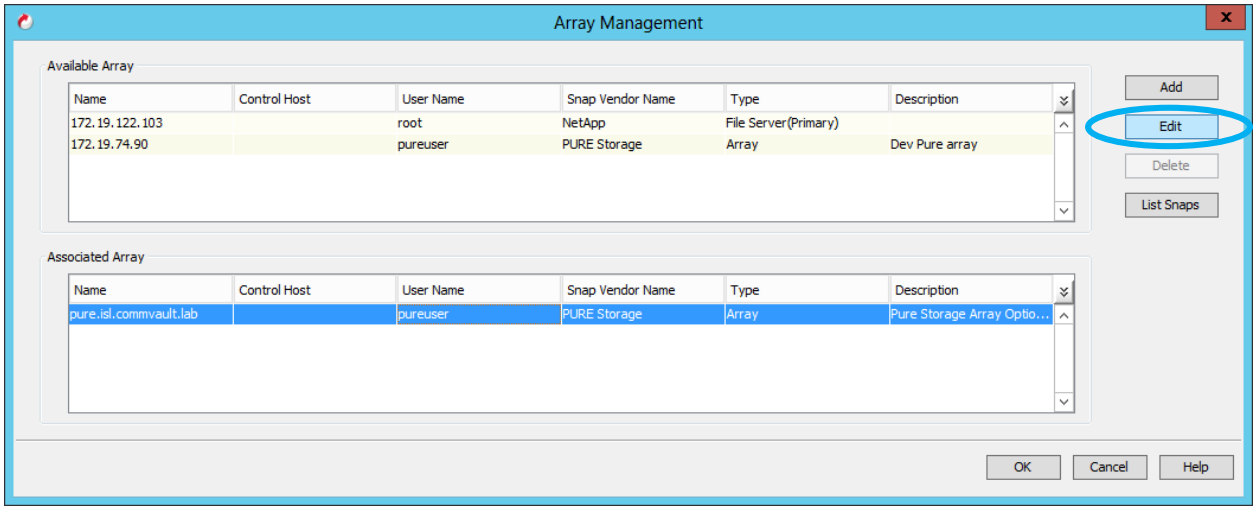


To override the settings for an entire Storage Policy Copy, edit the appropriate snapshot copy in the Storage Policy, and under the General tab click the Manage Array button:

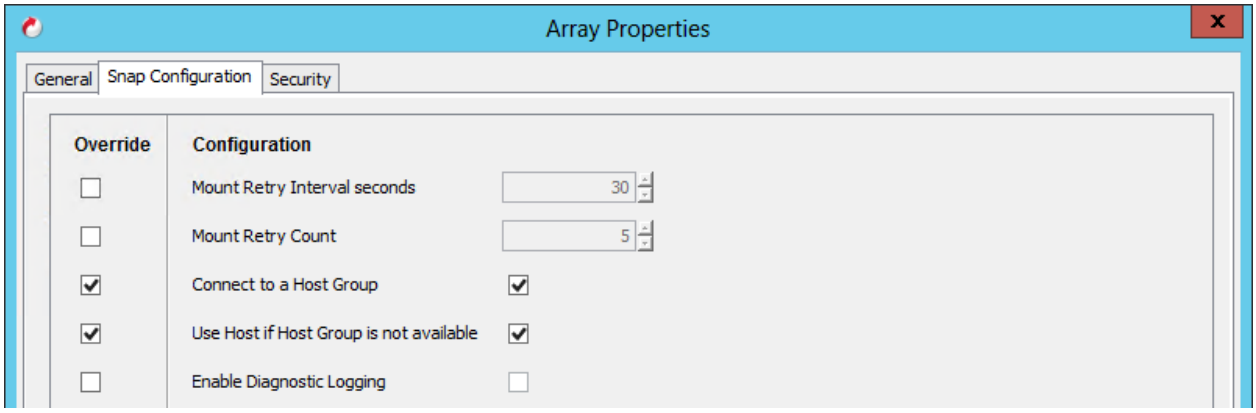


Both options will open up the Array Management screen. This version of the Array Management screen will identify the array(s) that are associated with the Subclient or the Storage Policy. Array settings can be overridden for arrays listed in either the Available Arrays or Associated Arrays section.

Highlight the Available Array or Associated Array and click on Edit.



The Array Properties screen will appear, select the Snap Configuration Tab.



On the bottom of the Array Properties screen it will notate if these settings are relating to a Storage Policy of a Subclient.

Storage Policy Settings:

Note: **The modification in Snap configuration values are specific to this Copy

Subclient Settings:

Note: **The modification in Snap configuration values are specific to this Subclient

Array Property Settings

Mount Retry Interval seconds

The "Mount Retry Interval seconds" setting controls how long the snapshot engine will wait to retry mount operations if a failure occurs. Typically this should not be changed from the default 30 seconds unless directed by Commvault Support.

Mount Retry Count

The "Mount Retry Count" setting controls how many times the snapshot engine will retry mount operations when a failure is encountered. Once the retry count is reached the Snap Backup job will go into pending state.

Connect to a Host Group

By default snapshots will be mapped to a Host within the Pure Storage array. The "Connect to a Host Group" setting allows mapping to a Host Group instead. Volumes mapped to Host Groups are visible to all Hosts in the group. This can be useful in virtualized environments in conjunction with the nClusterMount Additional Setting. This setting requires that the Host already belongs to a Host Group.

Use Host if Host Group is not available

The "Use Host if Host Group is not available" setting works in conjunction with the "Connect to a Host Group" setting. If selected and the Host does not belong to a Host Group the Snap Backup job will map snapshots to the Host instead. If deselected, the job will fail unless the Host belongs to a Host Group.

Enable Diagnostic Logging

With the "Enable Diagnostic Logging" setting enabled Snap Backup jobs will record all REST API commands sent to the array and all responses to aid in troubleshooting. Messages are recorded in the CVMA.log file on the client communicating with the array.

The IntelliSnap® Software Process

IntelliSnap® Technology Snap Backup Operation

IntelliSnap technology snapshot backups consist of the following operations:

1. The IntelliSnap software job initiates from the CommCell® Console via schedule or an on-demand job.
2. When the IntelliSnap software job starts, the file system, associated applications, or Virtual Machines properly quiesce, via VSS calls in Windows or through application interfaces such as RMAN to put the DB in a Hot Backup mode. In VMware configurations, vStorage APIs are called to create software snapshots and enable delta file creation for each of the guests targeted as contents of the snapshot.
3. The array API is called to:
    a. Verify the backup job contents, i.e. validating the underlying disk structure for file systems, databases, VM Datastores, etc. and any required log files
    b. Create a snapshot for the production volume.
    c. Create a clone from the snapshot and assign the clone to the appropriate host, either the production or the proxy host.
    d. Mount up the clone on the source or the selected proxy host for post-snapshot operations, e.g. scan & catalog for file system, integrity checks for Exchange database & backup to media if selected. For VMware, Hyper-V and RMAN proxy configurations, the Virtual Machines and database files are registered by the proxy application software.
4. Unmount the clone and delete it, protecting the original snap from any modifications

This snapshot now provides availability for backup copy operations and high speed restore / mount / revert operations.

Backup Copy Operation

A backup copy operation provides the capability to stream data from snapshots to disk media. This includes support for deduplication, enabling DASH copy functionality for further streaming copies to disk or cloud storage. Backup copy is enabled at the storage policy, and rules can be set to control how frequently snapshots will be written to media.

A backup copy execution occurs during the IntelliSnap software backup or at a later time, depending on the job options. The backup copy operations can be useful for creating additional standby copies of data. When selecting/deselecting a job for backup copy operations, ensure that all the dependent jobs (for example, incremental, differential, etc.) in the complete backup cycle are selected/deselected as the snapshots are copied to media in a sequential order. If a previously selected snapshot has not

been copied to media, an inline backup copy job will complete without creating the backup copy due to sequential order in which these copies must be made. On-demand offline backup copy operations must be scheduled for both the current backup and the previously non copied job to get the data to backup media. Backup Copy operations mount the selected snapshots in sequential fashion to execute a file system level backup of the snapshots. For Oracle and VMware, the backup copy operations will leverage RMAN and VADP to provide complete object integration (table level restore, single file access, etc.) in to the backup copy store.

During the Backup Copy operation:

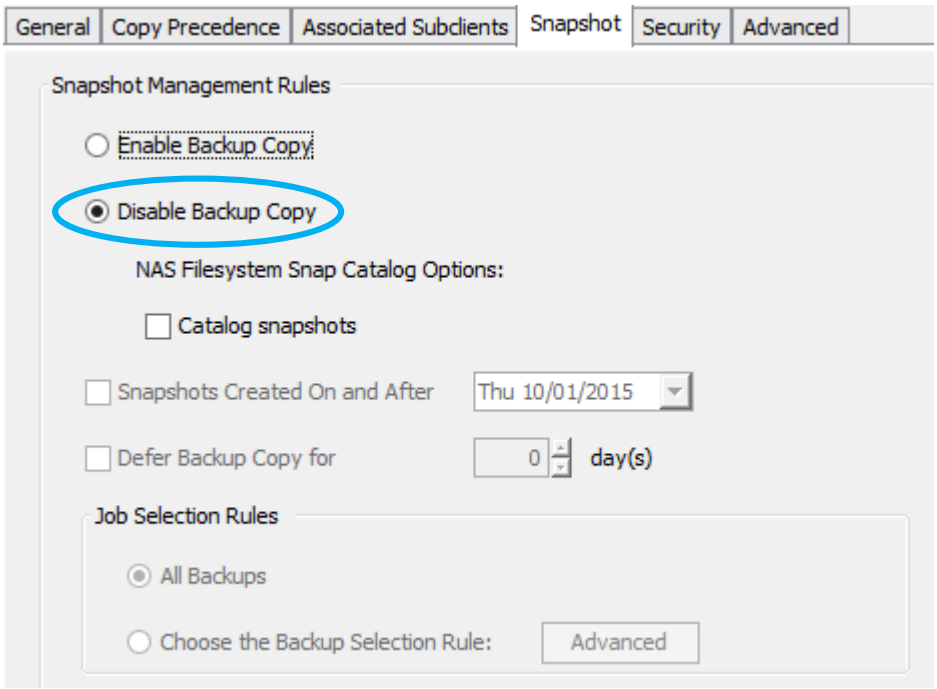
1. A linked copy of the clone or snapshot is created to protect the original from any modifications.
2. The linked copy is mounted to the source or proxy host. The mounted snapshot receives commands to scan and backup just like a normal file system and the required contents are read.
3. The file system backup is performed to the Primary copy of the storage policy for all defined files. The data is indexed and linked back to the original source paths on the production host.
4. When the backup copy job is finished, the linked copy is unmounted and destroyed. The original snapshot or clone is retained based upon Snapshot Copy retention settings.

Managing snapshots without Backup Copy

For data being managed only with snapshots, without streaming operations, Backup Copy must be disabled at the storage policy to ensure proper aging. When Backup Copy is enabled no snapshots will be aged until they have been streamed to media.

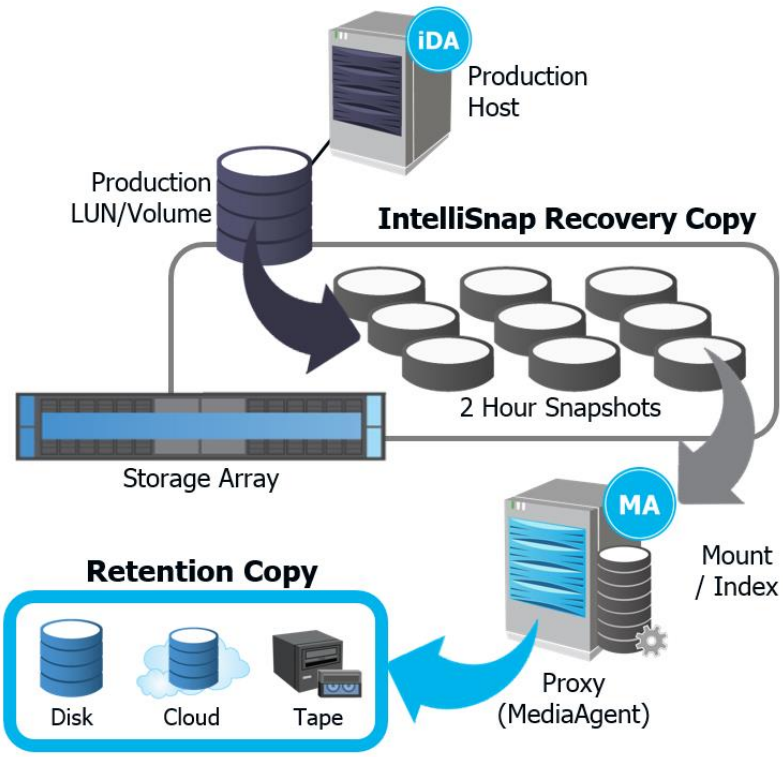
To disable Backup Copy for a storage policy:

1. Right-click the storage policy and select Properties
2. Select the Snapshot tab. Select the "Disable Backup Copy" option. Click OK.



Production Host Configuration

Protecting application databases and log volumes through an array snapshot provides fast access for recovery and many flexible options for data protection. IntelliSnap technology integrates key application awareness together with the array and our platform to deliver all of the benefits of traditional streaming backups with all of the performance and proxy capabilities of a snapshot. This application awareness allows true log-consistent "hot" backups with appropriate log management operations based off the contents of the data in the snapshot. IntelliSnap technology aligns all of the log and database volumes and snapshots, using them in concert to provide fast, low-impact recovery points through the array without scripts.



Before stepping through any configuration steps, deploy the proper agents on the production host requiring snapshot integration with the array. Application environments require:

- **File System iDataAgent (iDA)** – The Base agent that manages and protects the file system data from the production host. File system contents are supported for IntelliSnap software operations as well, but it is recommended to define application data sets with the application iDataAgent.

  If no supported application iDA is available, end-user written Pre and Post Snap scripts can be used to quiesce the unsupported application for IntelliSnap software integration through the File System iDA.

- **MediaAgent** – Provides media management capabilities to execute array functions and provide LAN-free access to snapshots for recovery

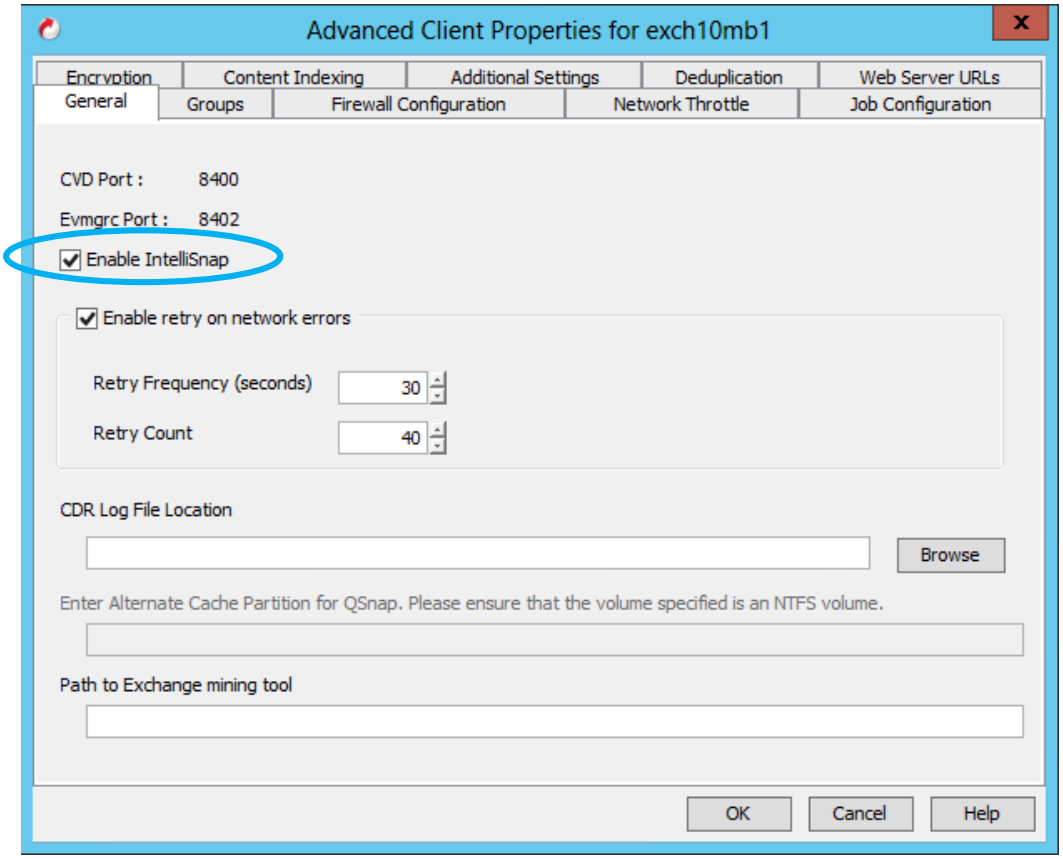
- **Commvault VSS Provider** – Provide VSS interaction with the array and the Simpana platform to ensure Microsoft applications are properly quiesced and protected during the snapshot process

- **Commvault VSS Hardware** Provider (only for Hyper-V on Windows Server 2012 and later) – Provide VSS interaction with the array and the Simpana platform to ensure Hyper-V virtual machines are properly quiesced and protected during the snapshot process

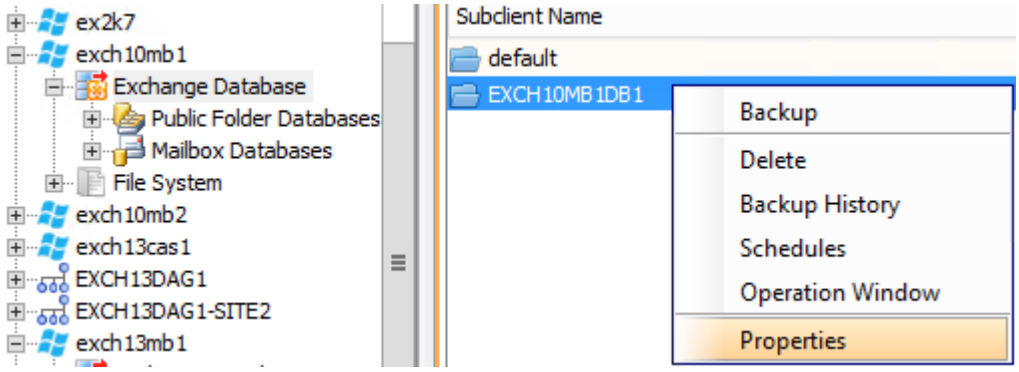
- **Application iDataAgent for selected Application** – Provides low-level application integration for Oracle, SQL, Exchange, MySQL, VMware, Hyper-V, DB2, SAP, etc., ensuring the appropriate APIs are called when quiescing and releasing the application during the snapshot operations. This iDataAgent will also align the volumes for snap based off the logical databases or contents defined in the subclient, including logs. If five databases all have separate LUNs assigned for databases and logs, the application agent will define the contents appropriately for all ten LUNs to be snapshotted together.

The following steps will configure the implemented application environment for IntelliSnap software operations:

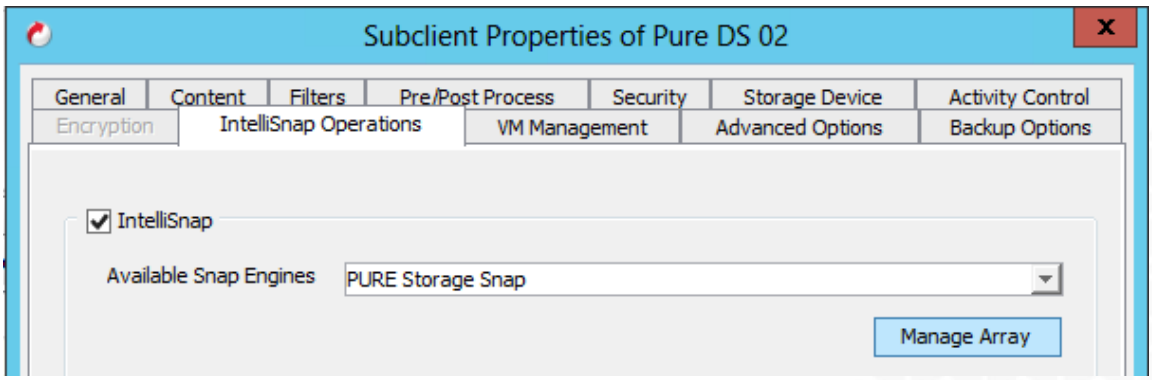
1. Enable IntelliSnap technology on the client computer acting as the production host in the CommCell GUI. Right Click on the client name, then select **Properties**.
2. Click the **Advanced** button and check the box marked **Enable IntelliSnap**. This will consume a Hardware Snapshot Enabler license from the license key. Click OK on the Advanced Client Properties and Client Computer Properties dialogs.



3. Browse to the Production Host Application iDA (in this case we are using Exchange Database iDA) and open the properties for the desired subclient to enable IntelliSnap Operations:



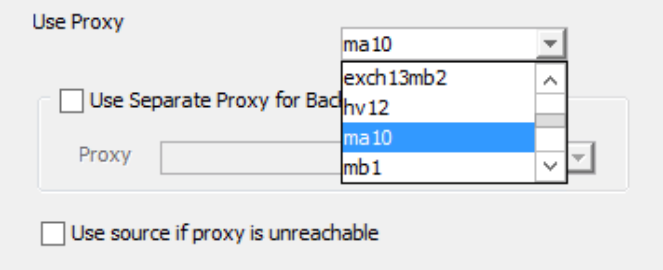
4. Browse to the IntelliSnap Operations tab; check the IntelliSnap box. Select PURE Storage Snapshot from the Available Snap Engines dropdown:



5. To define proxy configurations on the IntelliSnap Operations tab click on the drop down box next to Use Proxy. This provides available servers to use as the proxy during the index and backup copy operations. The selected server mounts the array snapshot when a backup copy operation executes.

   Checking the Use Separate Proxy for Backup Copy box will let you specify different proxies for operations at snap time, in this case database integrity checks, and streaming protection.

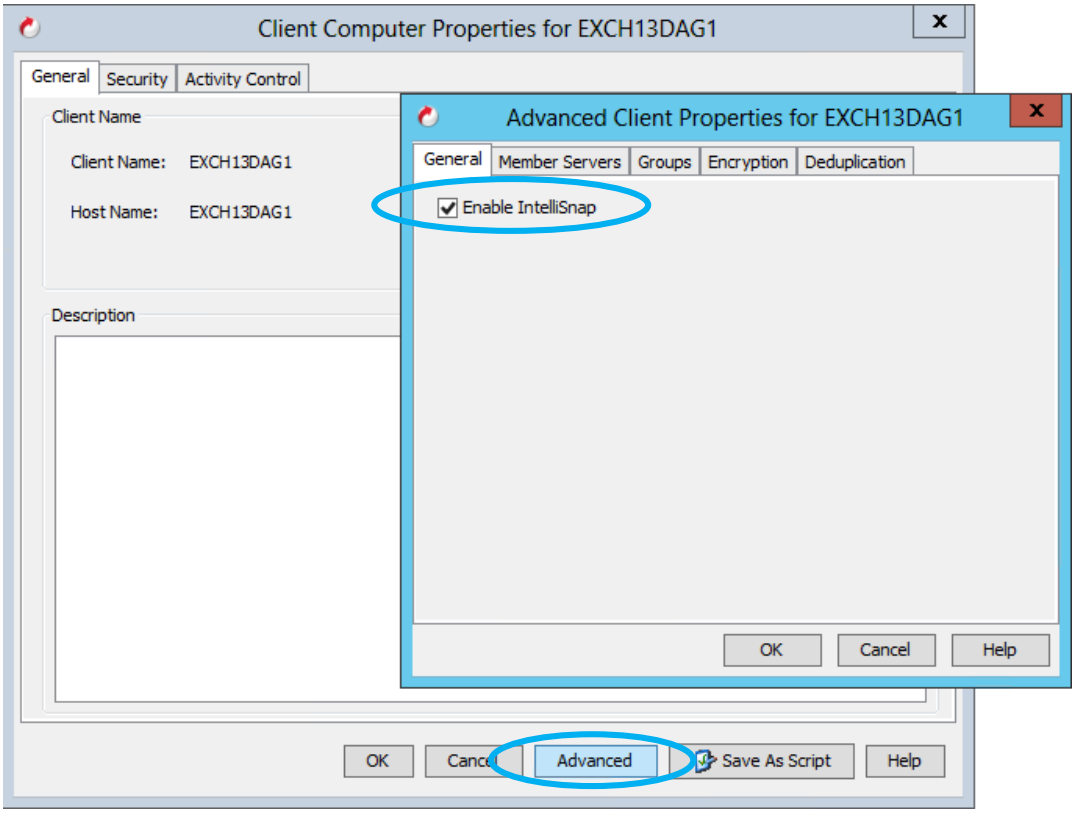
   If the Use source if proxy is unreachable box is selected, the snapshot will mount to the production host if the defined proxy server is unreachable for any reason:



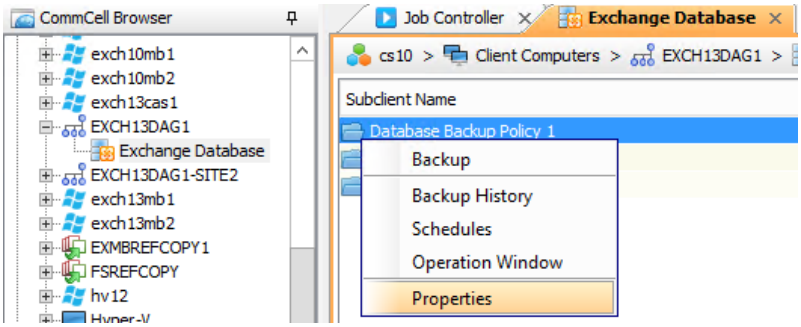
6. Ensure the Storage Device tab has a storage policy with a snap copy defined and click OK to close the Subclient properties.
7. To execute a snap operation for the application agent, simply schedule or generate a backup job for the previously configured Subclient. Simpana software will detect the configuration and automatically run a snap backup job. If a proxy is configured, ensure that it has all prerequisites set up before running the operation.

Exchange Database Configuration

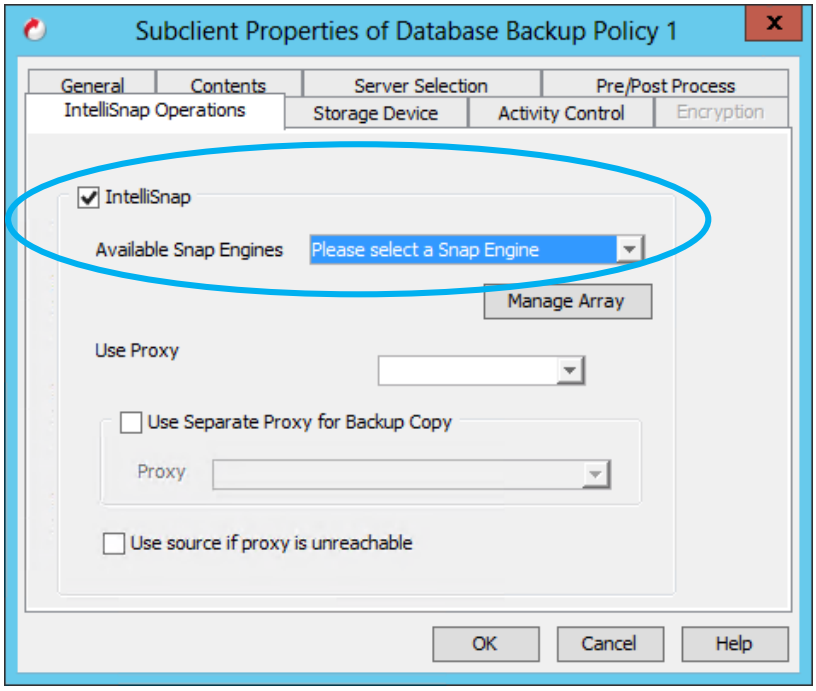
1. Enable IntelliSnap on the Exchange server client object in the CommCell console.
   - Right click on the server name, select All Tasks, and then select Properties.
   - Navigate to the advanced properties page and check the box marked Enable IntelliSnap. This will consume a Hardware Snapshot Enabler license from the license key.
   - In the case of Exchange DAG the client object in question is the master client.



2. Enable IntelliSnap for a Subclient policy
   - Browse to and highlight the Exchange Database iDataAgent then right click on the desired Subclient and select **properties**.



3. Click on the "IntelliSnap Operations" tab, check the IntelliSnap box, then select the appropriate array snapshot mechanism as the "Available Snap Engine."



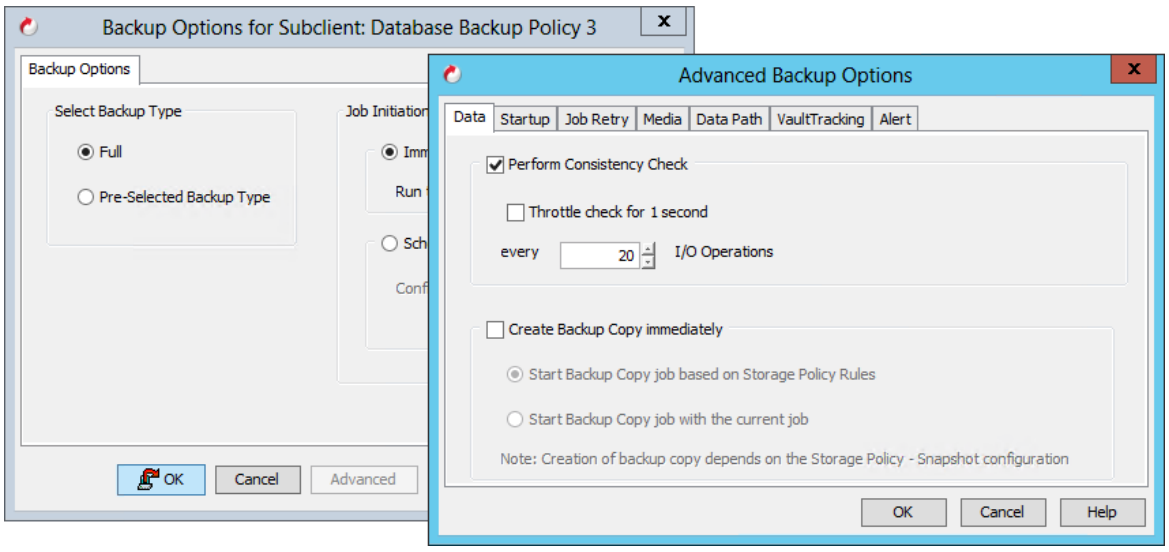
4. To define Proxy configurations on the "IntelliSnap Operations" tab click on the drop down box next to "Use Proxy." The list shows available servers to use as the proxy to offload index, backup copy, and consistency checking operations. The selected proxy server will mount the snapshot to perform these operations. A proxy host must have the Media Agent software installed and access to mount the snapshots taken from the source production host.
   - You can define a secondary proxy to separate the index and consistency checking operations from the backup copy operations by populating the "Use Separate Proxy for Backup Copy" option.
   - If the "Use source if proxy is unreachable" is selected all operations will default to the source host if the defined proxy server is unreachable for any reason.
5. Confirm the Storage Device tab has a Storage Policy with a Snap Copy defined and click OK to close the Subclient properties.

IntelliSnap Jobs

1. Execute an IntelliSnap Operation
   - Schedule or manually start a backup request for a configured Subclient policy.
   - Use the Advanced button when executing or schduling a backup to configure consistency checking. This option is on be default and will add considerable processing time to the job.

   With the advent of Exchange Database Availability Groups that replicate and manage multiple copies of a database the consistency checking option has become less critical then it was when there was only a single database copy. If you can afford the processing time to complete the consistency checks then leave them enabled but if operations are extending beyond the desired backup window administrators can disable the consistency check.

   The Exchange System Management Tools must be installed on any proxy host that needs to perform a consistency check.



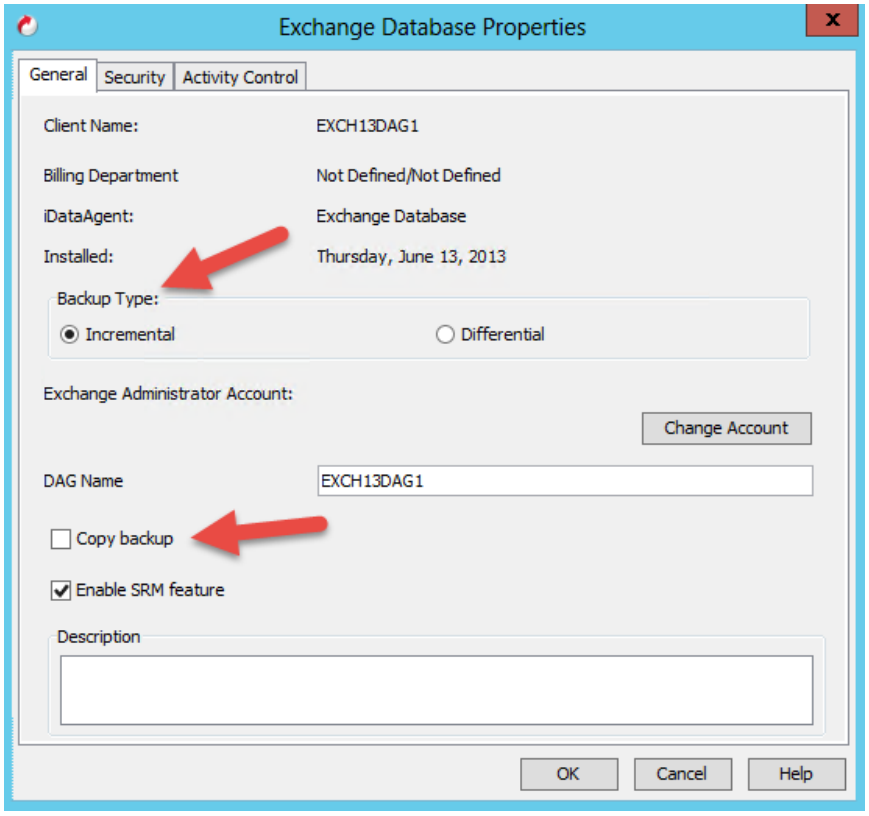
Note: For Exchange Database IntelliSnap software operations, an ESE consistency check is run on the snapshot copy to validate the integrity of the database files. This is enabled by default and can be found and modified under the Advanced Job Options dialog for the backup operation. It is highly recommended to leave this enabled to provide integrity checks to Exchange messaging environments.

2. Select the desired backup type for the operation.
   - A Full backup will snap both the database and transaction log volumes (if separate) and marks a full database recovery point in Exchange.
   - The Pre-selected backup type is configured at the Exchange Database iDataAgent properties page.
   - In almost all cases this should be set to Incremental. When an incremental snap is performed the transaction log volume is snapped and a transaction log backup is marked in Exchange.

   If the database and log files are hosted on the same volume and an incremental snapshot is executed the entire volume is still snapped but only an incremental backup is marked in Exchange and only the log files will be moved to media during a backup copy operation.

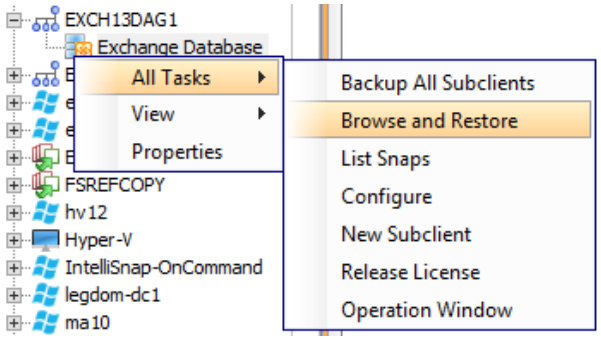
   Use the Copy Backup option to enable application consistent snap shots without truncating transaction logs. By default transaction logs will be marked for truncation following a successful Full or Incremental IntelliSnap operation. Use the Copy Backup option to avoid log truncation when desired.

   A common use case for the copy backup feature is a stretched DAG where an administrator wants snap database copy 1 in the data center 1 and then also snap database copy 2 in data center 2. This would provide the administrator with IntelliSnap history in both data centers. Using the copy backup option in one of the data centers allows for an application consistent snapshot to occur without interfering with the transaction log chain being managed by the IntelliSnap operations occurring in the other data center.


Exchange Database Properties
General
Security
Activity Control
Client Name:
EXCH13DAG1
Billing Department
Not Defined/Not Defined
iDataAgent:
Exchange Database
Installed:
Thursday, June 13, 2013
Backup Type:
Incremental
Differential
Exchange Administrator Account:
Change Account
DAG Name
EXCH13DAG1
Copy backup
Enable SRM feature
Description
OK
Cancel
Help

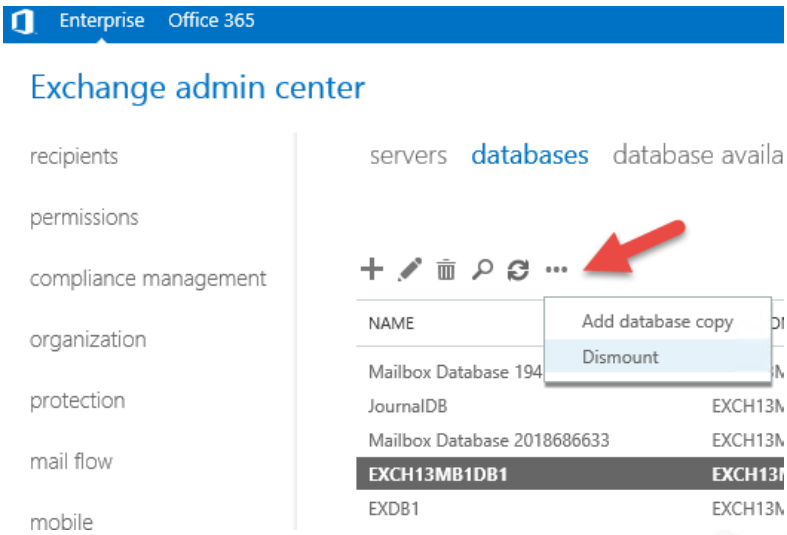
Access and Restore

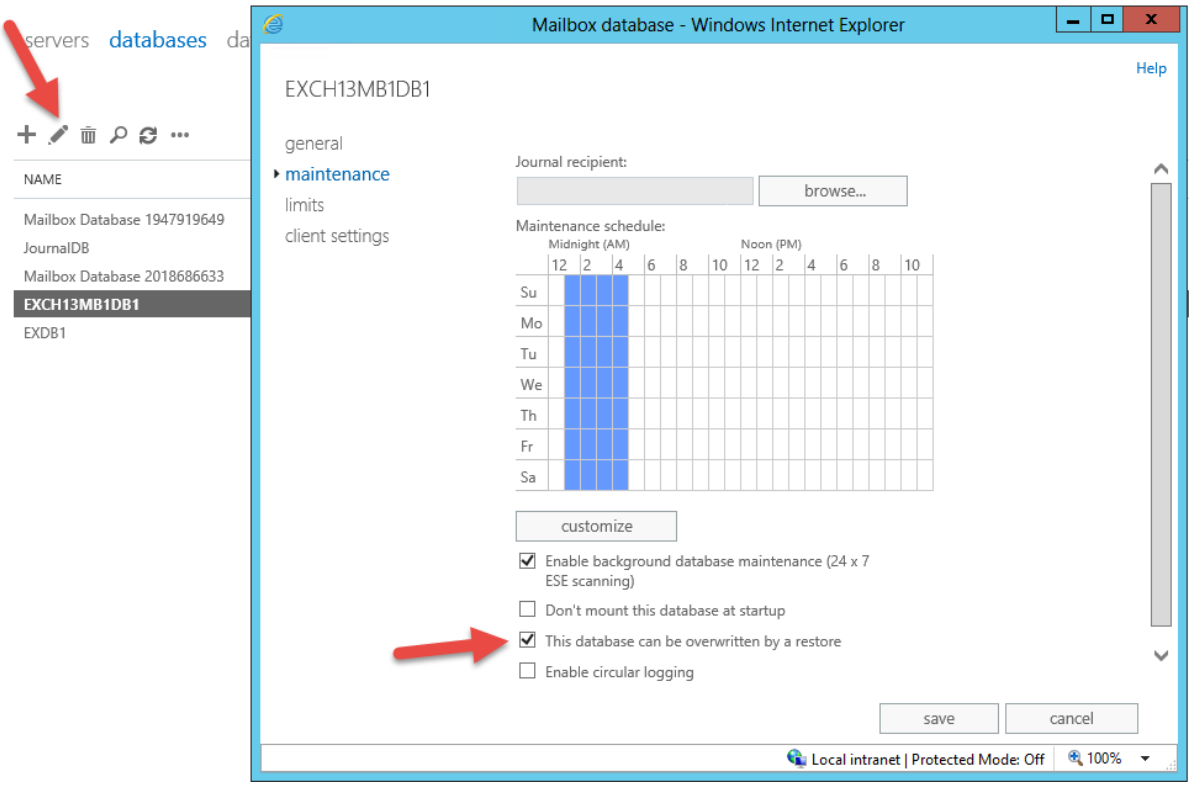
1. Browse and Restore
   - Right click on the Exchange Database iDataAgent and select Browse and Restore.
   - Enter the desired time frame and click View Content.
   - Select the database to restore and select Recover All Selected.



2. Browse by Job
   - Right click on the Exchange Database iDataAgent and select View then Backup History or right click on a specific Subclient policy and select Backup History.
   - Narrow the history returned via the "Backup History Filter" window or leave the default options to return all history and click Ok.
   - Right click on the desired job and select Browse and Restore.
3. Configure Restore Options for Exchange
   - Set the proper "Destination host" to receive the data being restored. Only hosts that have the Exchange Database iDataAgent will appear in the list.
   - Select Restore to same database to restore the database to the original location with the original database name.

   In order to overwrite an existing database, that database must be dismounted and must also have the "this database can be overwritten by a restore" option enabled. Both options are set in the Exchange System Manager/Exchange Admin Center or via PowerShell.

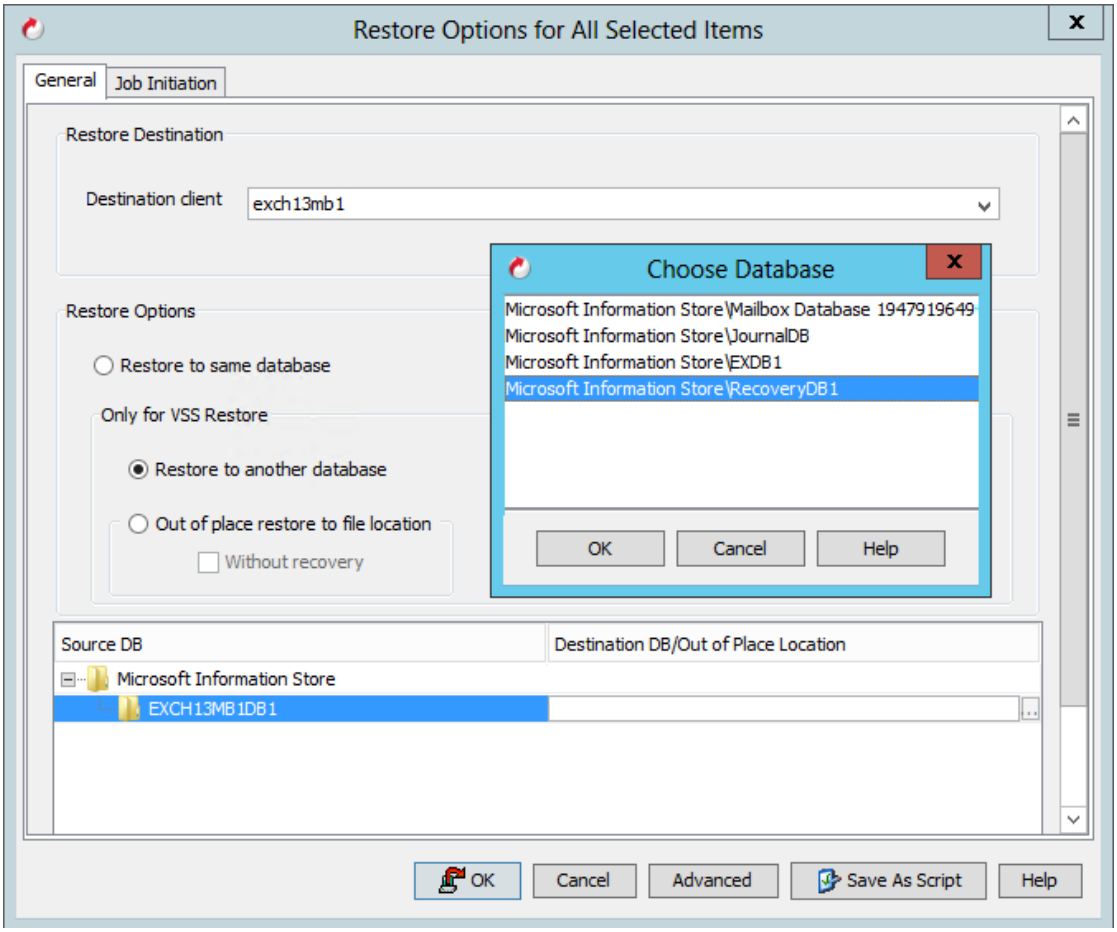




- Configure the "Only for VSS Restore" options. All Exchange database backups from Exchange 2010 and later required VSS. Exchange 2007 clusters required VSS for backup. All IntelliSnap operations will use VSS as well. The only non-VSS backups in history would be from non-clustered Exchange 2007 or prior.
- To restore to an alternate database: select **Restore to another database** then click on the **ellipsis** button under Destination DB/Out of Place Location to select a database to overwrite.

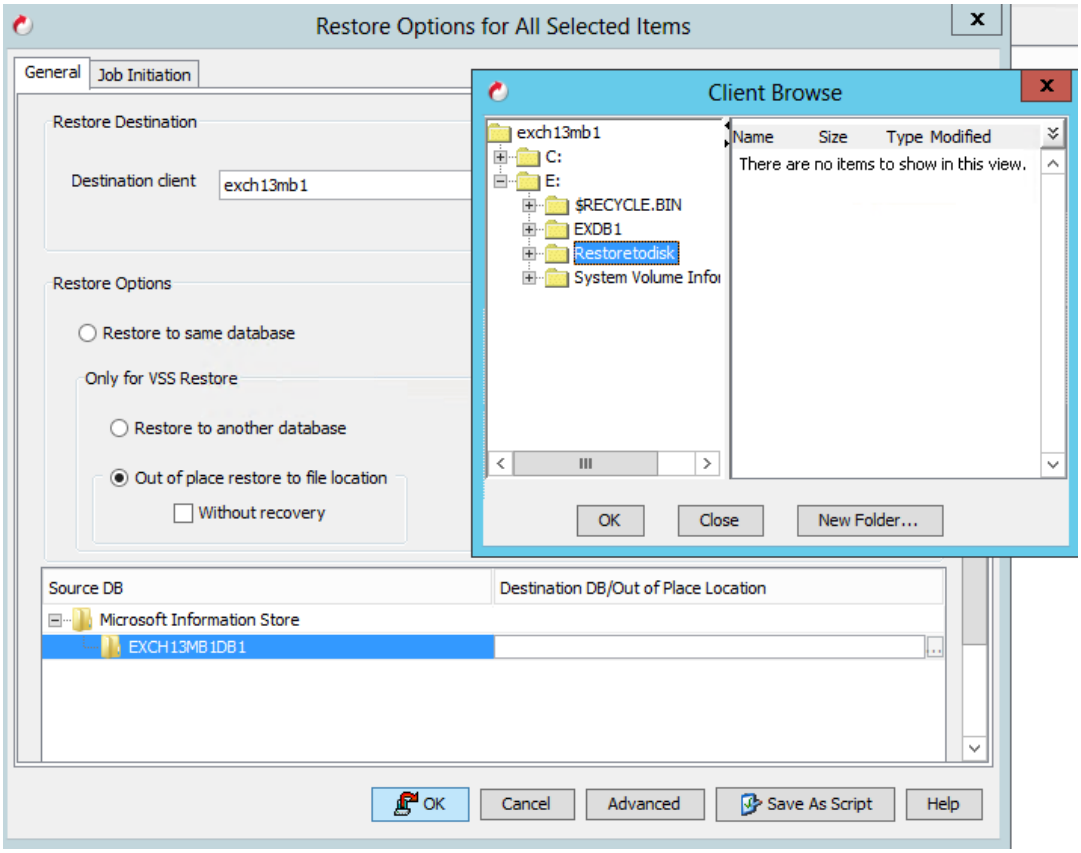
A common use case here will be to restore to an Exchange Recovery Database or Recovery Storage Group.

- The list returned will include all databases and storage groups currently hosted by the Exchange server selected in the Destination client drop down box.



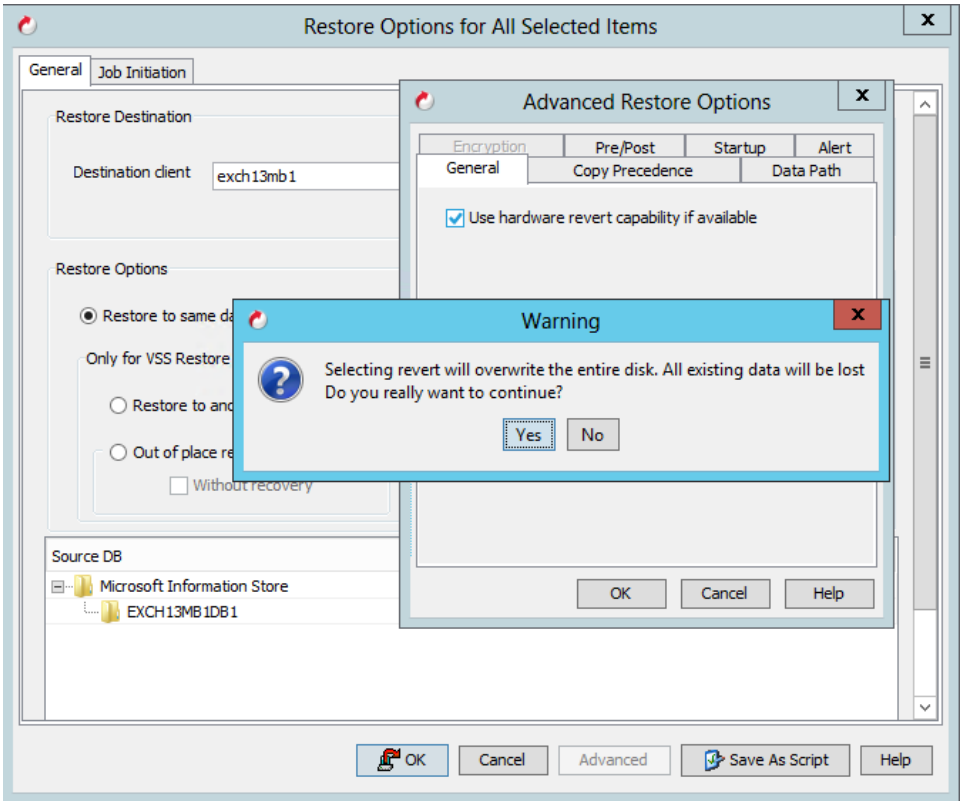
To restore to a file system location: select Out of place restore to file location then click the ellipsis button under "Destination DB/Out of Place Location" to select a file system location to restore the database and log files too.

- It is possible to restore to the file system of a non-Exchange client but you must first install the Exchange database iDataAgent for that server to be an available destination client
- Use the "Without Recovery" option to restore the database and transaction log files to disk without playing the transaction log files into the database. By default recovery, or playing the restored logs forward into the database, will automatically occur. This process requires the Exchange System Management tools to be installed on the target client.



To perform a hardware revert; select the **Advanced** button in the restore options window then select **Use hardware revert capability if available** option then click **Yes** to the warning.

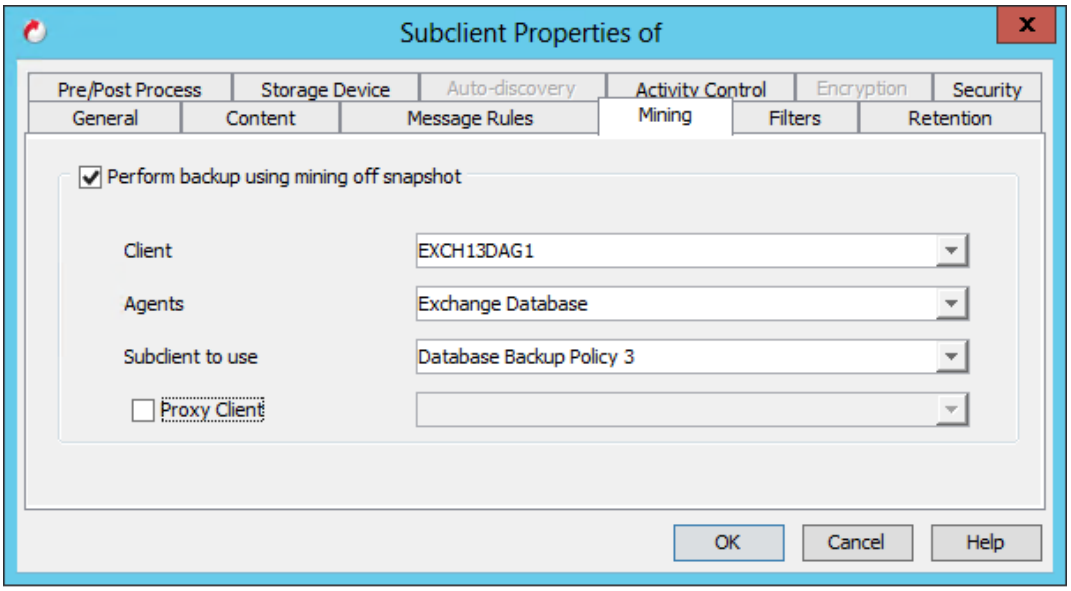
- The warning is informing the user that this operation will overwrite the entire volume. If there is more than one database on a volume and only one database is being restored, the entire volume is still reverted back. When there are multiple database on the same volume it is a best practice to group them together in the same Subclient for backup.
- The hardware revert feature is not available for all array types and configurations.


Restore Options for All Selected Items
General
Job Initiation
Restore Destination
Destination client
exch13mb1
Restore Options
Restore to same da
Only for VSS Restore
Restore to and
Out of place re
Without recovery
Source DB
Microsoft Information Store
EXCH13MB1DB1
OK
Cancel
Advanced
Save As Script
Help
Advanced Restore Options
Encryption
Pre/Post
Startup
Alert
General
Copy Precedence
Data Path
Use hardware revert capability if available
OK
Cancel
Help
Warning
Selecting revert will overwrite the entire disk. All existing data will be lost
Do you really want to continue?
Yes
No

Snap Mining - Mailbox OnePass from IntelliSnap

The snap mining feature in Simpana 10 allows for Mailbox OnePass operations to be run against a snapshot of the Exchange database rather than from the live production host.

1. Snap mining host requirements
   - Outlook x64
   - Exchange System Management Tools
   - Media Agent
   - Access to mount the corresponding Exchange database snap shots.
2. Configure the Exchange Mailbox Agent to use IntelliSnap
   - Navigate to and edit an Exchange Mailbox Subclient policy
   - Click on the Mining tab and check the box for Perform backup using mining off **snapshot** then enter out the following criteria
     - Client – Source of the Exchange Database snap.
     - Agents – Exchange Database
     - Subclient to use – The IntelliSnap enabled Exchange Database Subclient that contains the database to be mind.
     - Proxy Client – (optional) select another Exchange Mailbox client to process the operations through.



Exchange Offline Mining

Not to be confused with Snap Mining, Offline Mining in Simpana 10 allows administrators to browse through an offline exchange database file in order to search, find, and restore mailboxes, folders, and individual messages. While offline mining can work with any copy of an Exchange database file, IntelliSnap technology certainly provides a quick and easy way to make the Exchange database file available to the Exchange Offline Mining Tool.

1. Exchange Offline Mining Tool host requirements
   a. Outlook x64
   b. Exchange System Management Tools

c. Media Agent

d. Exchange Offline Mining Tool

e. Access to mount the corresponding Exchange database snap shots.

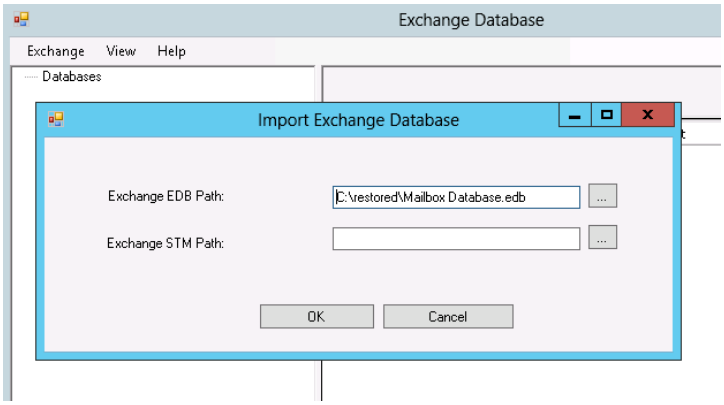
2. Mount the snap shot to the Offline Mining Tool host

   a. Use the List Snaps feature, see the section above, to mount the Exchange database snap shot to be mined to the Offline Mining Tool host.

3. Register the database file with the tool

   a. Start the Offline Mining Tool then click on Exchange then New.

   b. On the Import Exchange Database screen enter the path or browse to the recovered or mounted database (.EDB) file and click OK.

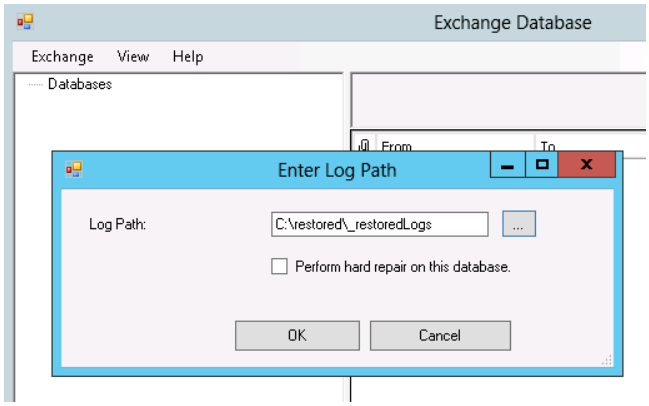


   c. If using Exchange 2007 add the path to the STM file as well.

   d. If prompted enter the path to the recovered or snapshot mounted log files and click OK.

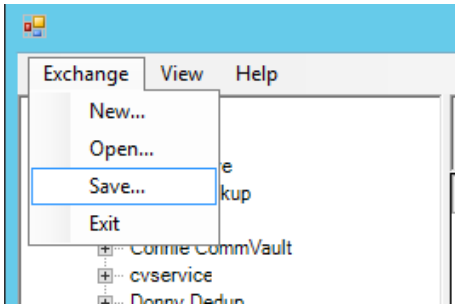
   e. Enter the database file path and stm file path if applicable (Exchange 2007 only) and click OK.

   f. Enter the log file path and click OK.



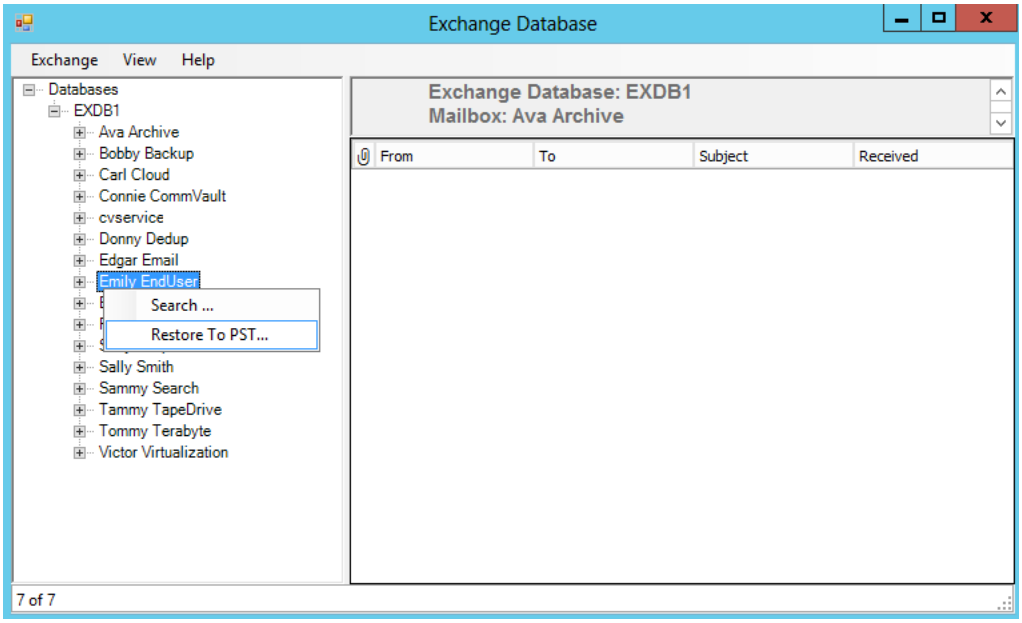
4. Open and Save Options

   a. The Save option allows administrators to save the currently registered databases to a configuration file. Use the Open option to open any saved configuration files which bypasses the need to reregister a database in the tool.

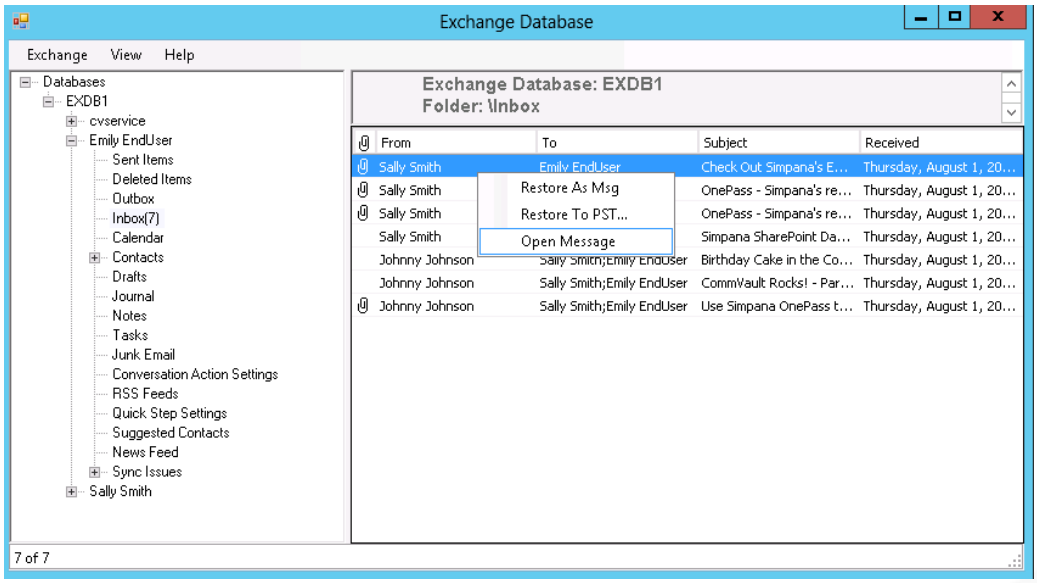


5. Browse and Restore

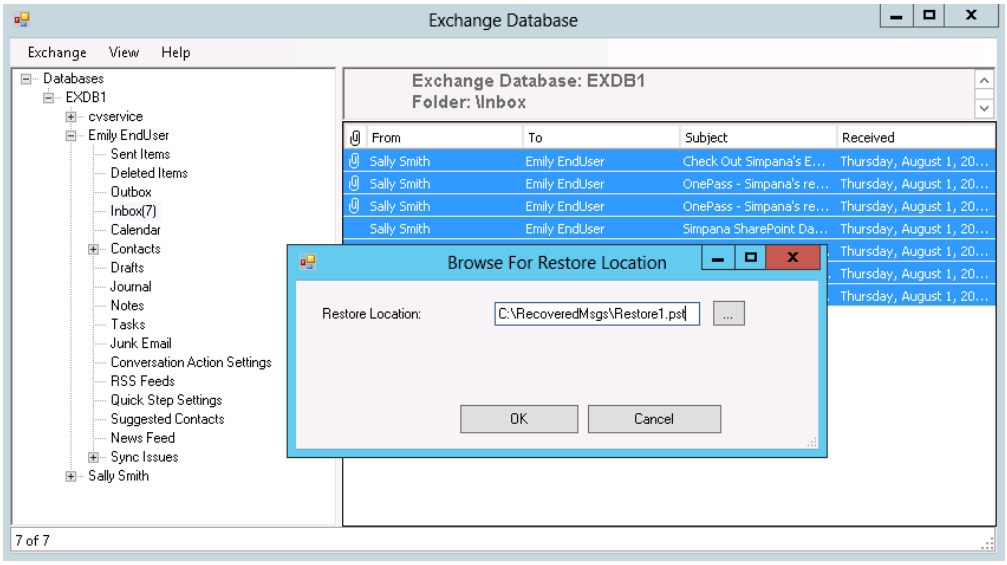
   a. Right click on a mailbox and select Restore to PST to recover the entire mailbox to a PST file.



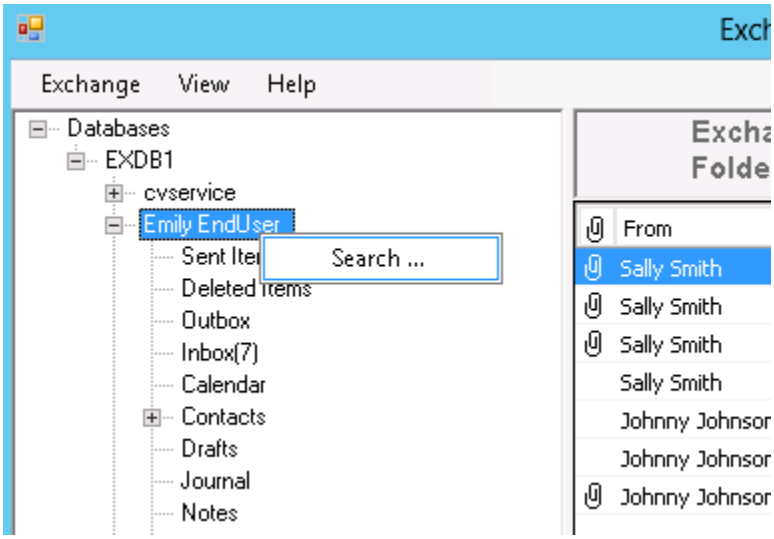
   b. Right click on individual messages or a group of messages to view or restore to MSG or PST.

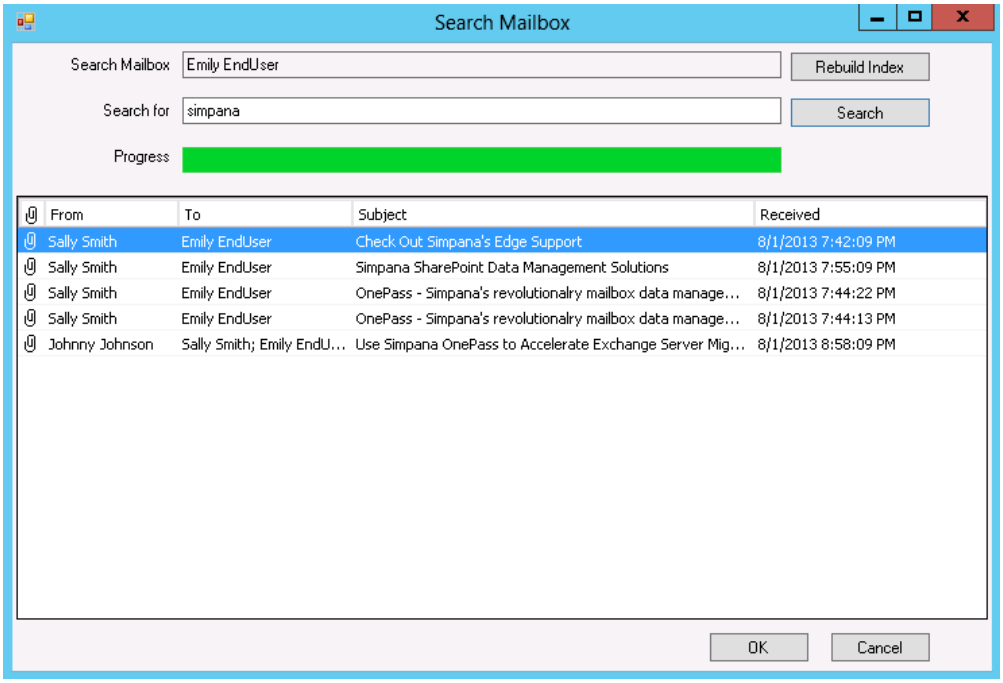


   c. Enter the recovery destination including file extension.



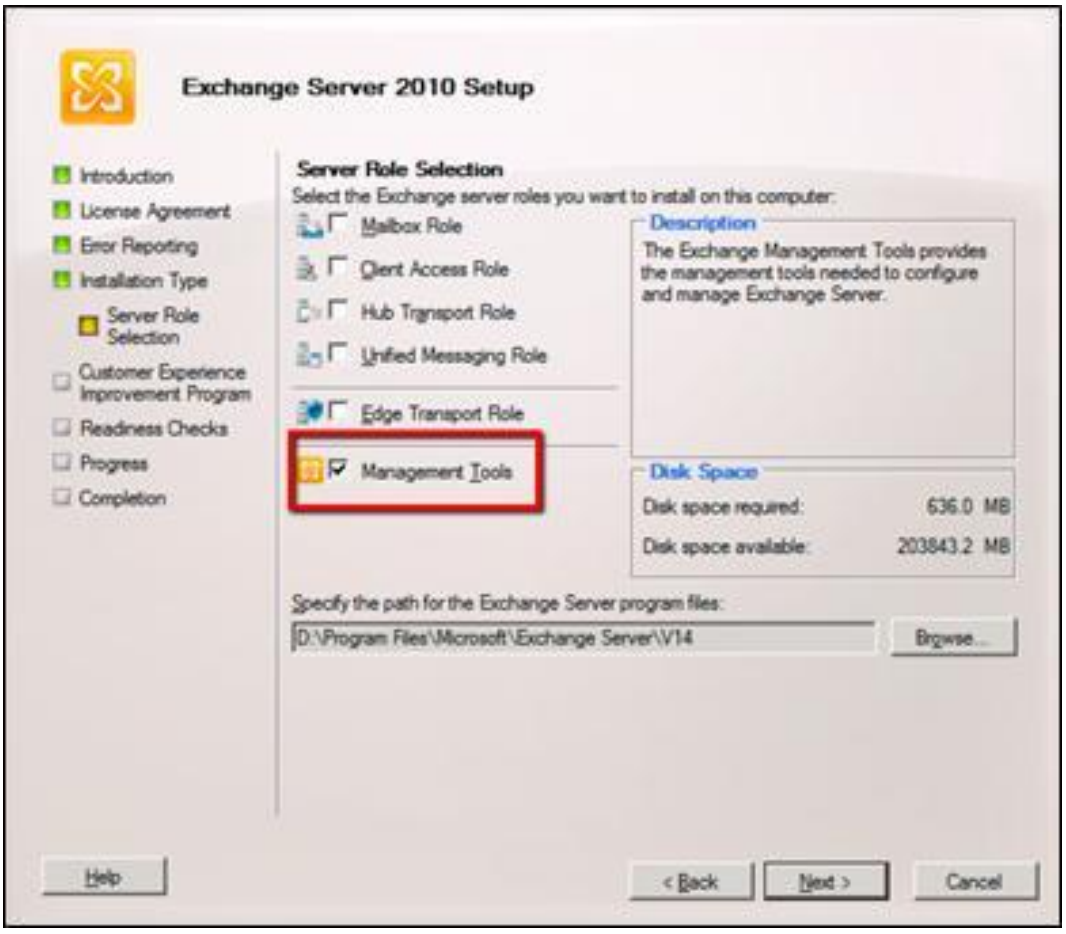
6. Search and Restore
    a. Right click on the root of a mailbox and select Search
    b. Enter search criteria then click Search
    c. Search results can be restored in the same manner as browse




Search Mailbox
Search Mailbox
Emily EndUser
Rebuild Index
Search for
simpana
Search
Progress
From
To
Subject
Received
Sally Smith
Emily EndUser
Check Out Simpana's Edge Support
8/1/2013 7:42:09 PM
Sally Smith
Emily EndUser
Simpana SharePoint Data Management Solutions
8/1/2013 7:55:09 PM
Sally Smith
Emily EndUser
OnePass - Simpana's revolutionalry mailbox data manage...
8/1/2013 7:44:22 PM
Sally Smith
Emily EndUser
OnePass - Simpana's revolutionalry mailbox data manage...
8/1/2013 7:44:13 PM
Johnny Johnson
Sally Smith; Emily EndU...
Use Simpana OnePass to Accelerate Exchange Server Mig...
8/1/2013 8:58:09 PM
OK
Cancel

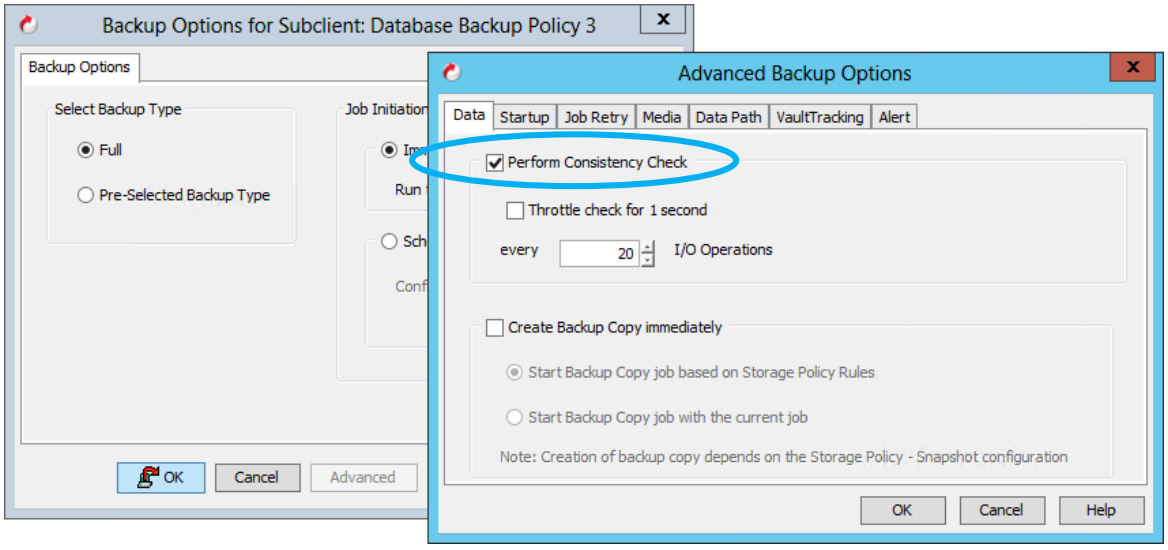
Exchange Proxy Configuration

Any proxy configuration interacting with Exchange databases provides the capability to execute an ESE integrity check against the Exchange database snapshot to ensure recoverability. To enable this capability, install the proper version of the Microsoft Exchange Management Tools from the Exchange installation media on to the proxy:



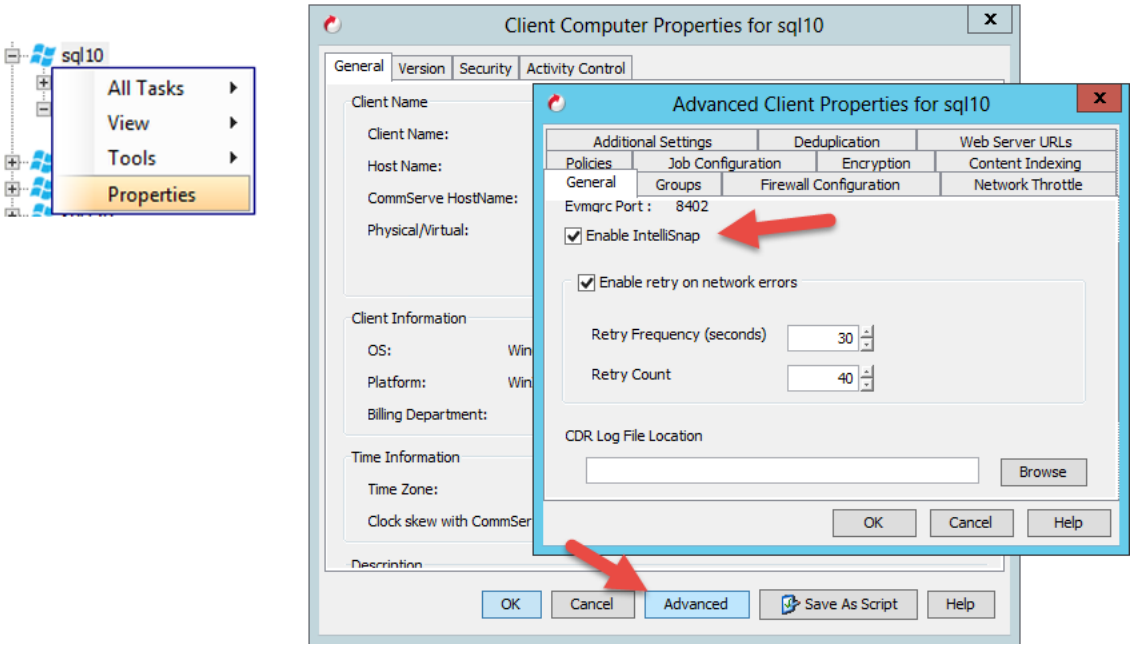
In addition to installing the Exchange management tools, verify the proper installation of the necessary MediaAgent and File System iDataAgent as well. These must be installed to allow the selecting the proxy as the proxy host in the application Subclient contents.

The database integrity check is enabled by default, but it can be disabled to shorten the process or reduce overhead. This is not recommended since recoverability cannot be guaranteed without the integrity check. The integrity check is controlled in the advanced job options. To disable it, when scheduling the Microsoft Exchange IntelliSnap backup operation, click the Advanced button to bring up the Advanced Backup Options dialog. To enable the integrity check for the Exchange Backup job upon Snapshot Index completion:

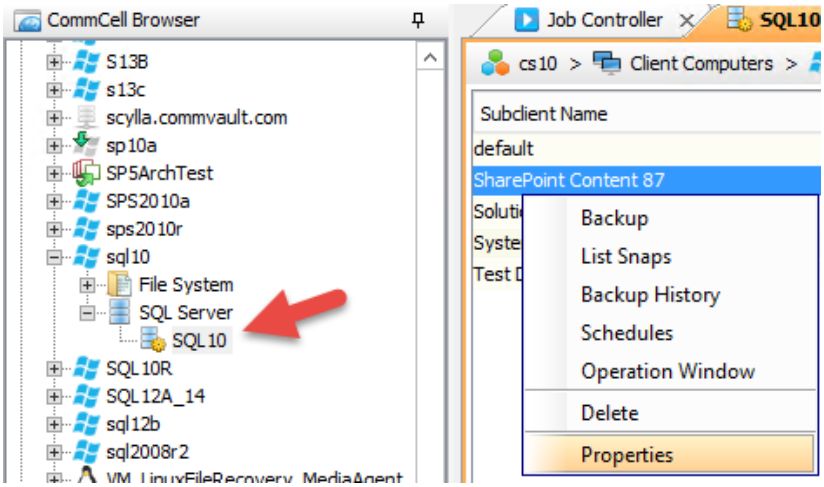


SQL Configuration

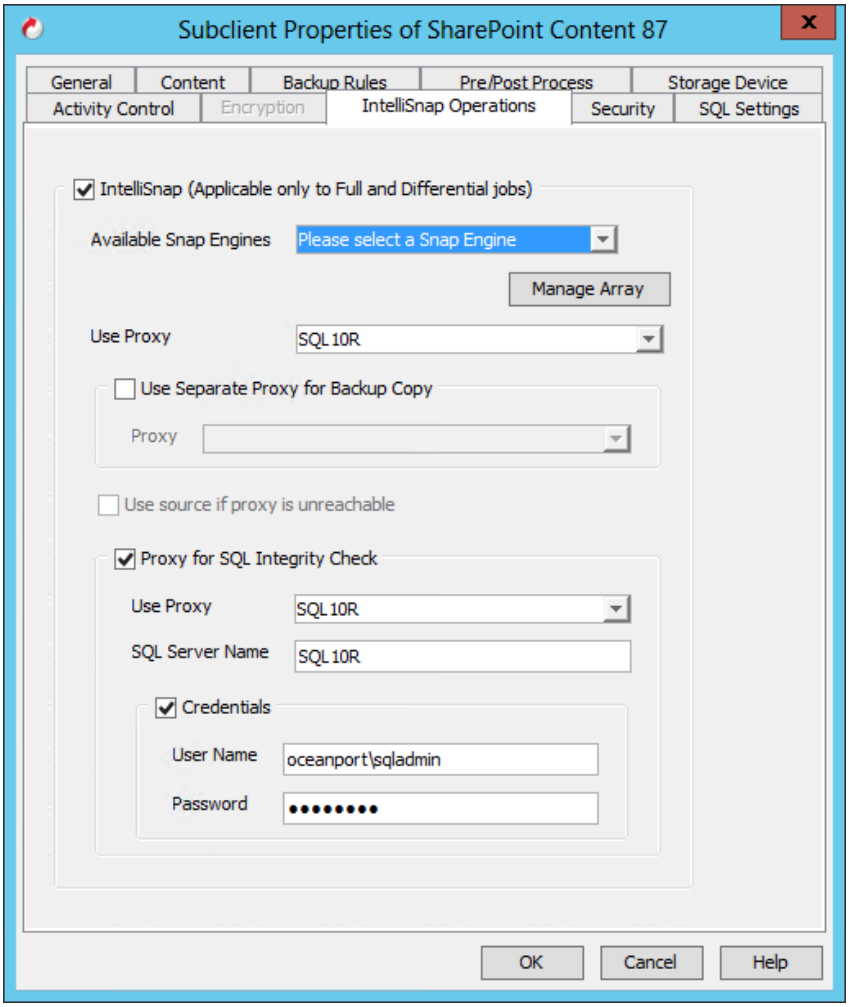
1. Enable IntelliSnap on the SQL server client object in the CommCell console.
   - Right click on the server name, select **All Tasks**, and then select Properties.
   - Navigate to the advanced properties page and check the box marked **Enable IntelliSnap**. This will consume a Hardware Snapshot Enabler license from the license key.
   - In the case of SQL cluster the client object in question is the master client.



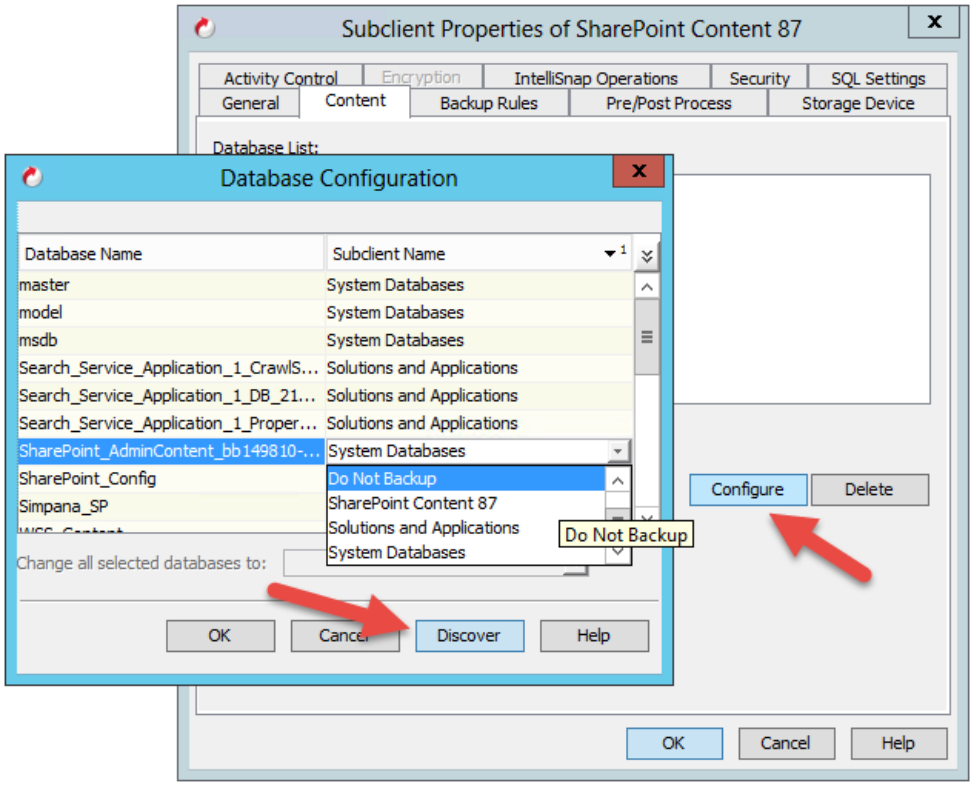
2. Enable IntelliSnap for a Subclient policy
   - Browse to and expand the SQL iDataAgent, highlight the SQL instance, then right click on the desired Subclient and select **Properties**.



- Check the box to enable IntelliSnap then select the appropriate snap engine in the drop down. The following defines optional IntelliSnap configuration options on the same tab.
  - Manage Array – Short cut to the Array Management control panel applet where snap shot capable storage arrays are registered with the commcell.
  - Use Proxy – designate a proxy server for indexing the backup
  - Use sepearte proxy for backup copy – assign a separate proxy for creating protection copies of the snap shots to disk, tape, or cloud media
  - Use source if proxy is unreachable – check this box to default processing to the source client if the proxy is unreachable for any reason
  - Proxy for SQL Integrity check – sepecify a system to perform integrity checks on the database snap shots
  - Credentials – logon credentials for the SQL instance that will be performing the integrity check when proxy is used.



3. Navigate to the Content tab and review any databases that exist and use the Discover feature to add databases to the policy.
   - All databases that exist on a single volume should be added to the contents to ensure all databases are quieced when the volume snap shot occurs.
   - Do not add databases on different volumes to the same subclient policy. While this is possible to do so it's a best practice in most cases to have each volume to be snapped dedicated to a unique subclient policy.



- Review the backup conversion rules tab and SQL Settings tab.
- Navigate to the Storage Device tab and configure both Data and Log storage policies, review data transfer and deduplication options and click OK.

Default subclient and Auto-Discovery

The default subclient will perform auto-discovery when executed. This ensures that any new databases that are added to the environment are automatically discovered, added to the default subclient, and protected.

As a best practice, administrators should create user-defined subclients for persistent databases that will be part of daily data protection operations and allow the default subclient to manage discovery or new databases.

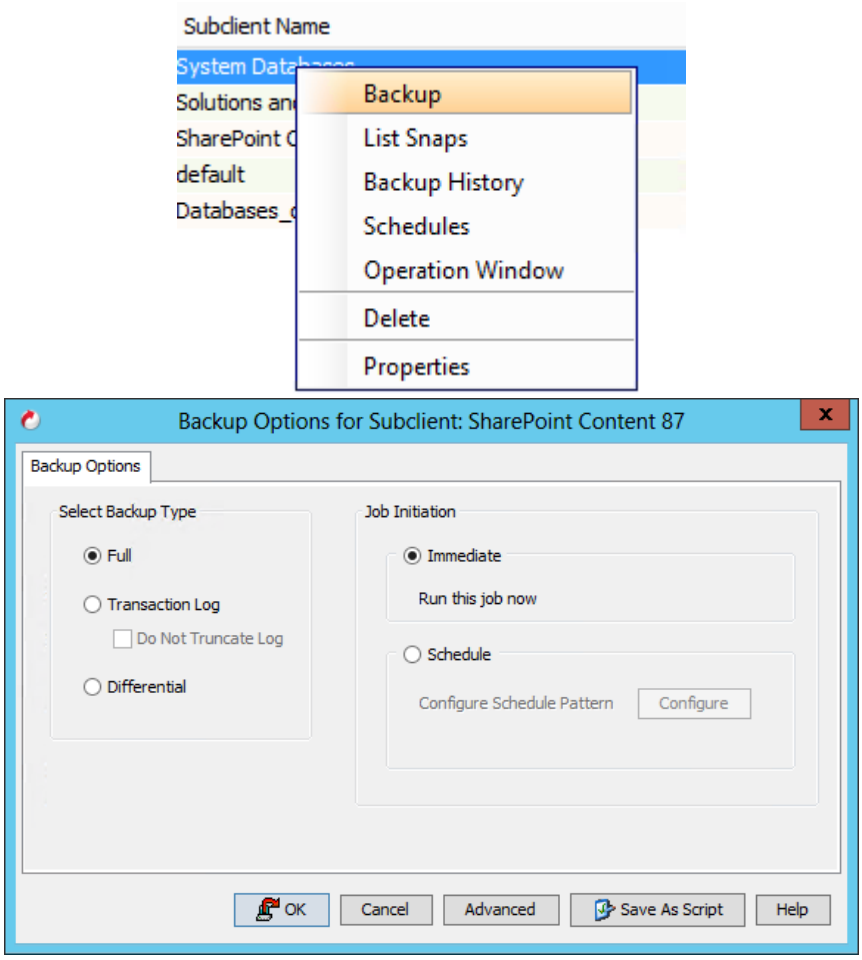
As new databases are discovered administrators can use the Contents tab in a subclient policy to move the databases from default and into a user-defined subclient.

Preventing backup for databases

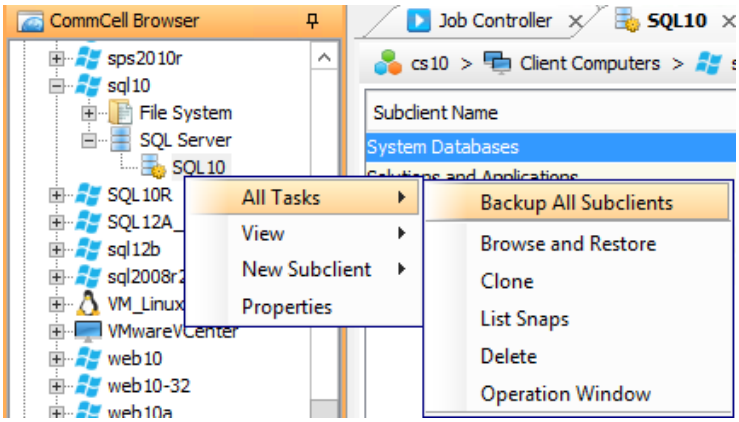
To prevent backup of a database administators can add the databases in quesiton to the hidden subclient called "Do Not Backup". Optionally administratosr can create their own user-defined subclient and add the databases to it then disable backup activity for the subclient or simply avoid scheduling any operations for it.

IntelliSnap Jobs

1. To start or schedule an IntelliSnap operation, right click on the Subclient policy and select Backup



- Optionally you can start or schedule the backup for all Subclients by right clicking on the Instance and selecting **Backup All Subclients**



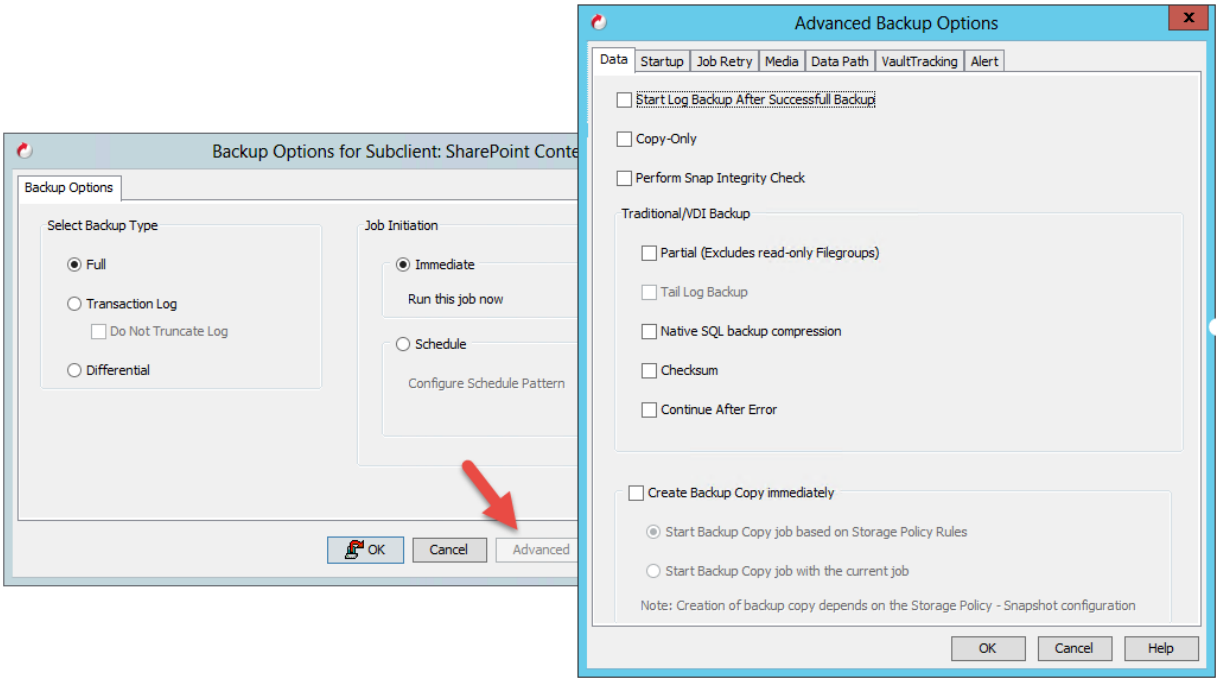
Backup options include:

- **Full** – A full database backup will be executed which includes quiescing the databases in the Subclient contents then executing a full snap shot of the source volume(s)
- **Transaction Log** – The corresponding transaction log files for the databases listed in the Subclient contents are protected and truncated. No hardware snap shot will occur during transaction log backups.
  - **Do Not Truncate Log** – use this option to perform a transaction log backup without truncating the transaction logs.
- **Differential** – A differential database backup is executed which includes quiescing the databases in the Subclient

contents then executing a full snap shot of the source volume(s). While a snap shot always includes the entire volume, a differential type backup is recorded in SQL and only the differential changes would be moved to the backup copy if taken.

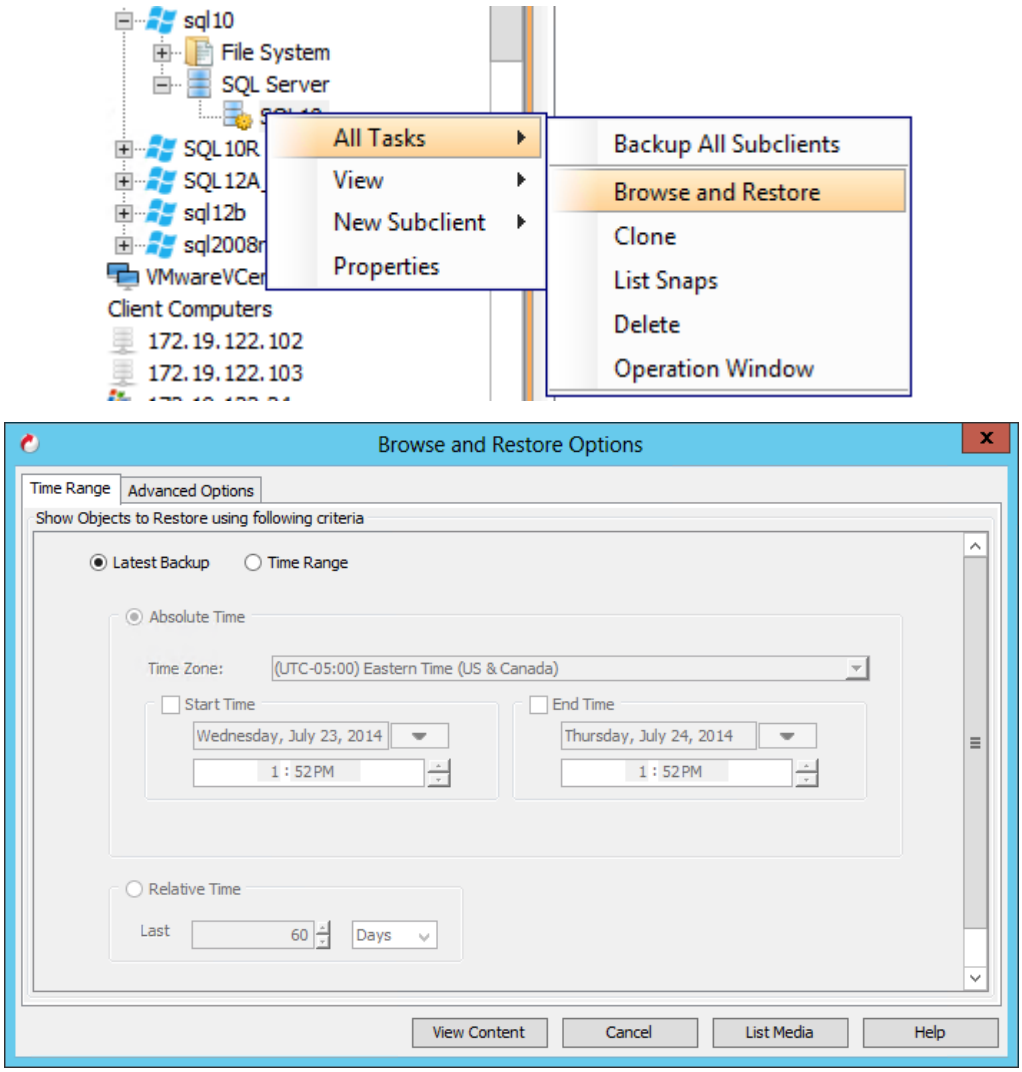
Advanced Backup Options – click the "Advanced" button on the Backup Options window to access optional features for the IntelliSnap or traditional backup operation.

- **Start Log Backup After Successful Backup** – When scheduling database backups use this option to automatically start a Transaction Log backup following a successful database backup (full or differential)
- **Copy Only** – A copy only backup captures an application consistent snap shot of the databases in the Subclient policy without writing into the SQL backup chain. This feature is useful when there is a need to take additional backups of a database, perhaps to alternate media or from an alternate CommCell, without interrupting the typical backup chain.
- **Perform Snap Integrity Check** – Execute an integrity check for the database(s) in the snap shot. This option requires the integrity check options to be enabled on the IntelliSnap tab for the Subclient.
- **Create Backup Copy Immediately** – Select this option to force a backup or protection copy of the snap shots immediately following the IntelliSnap job. The backup copy or protection copy will essentially backup the snap shot from the storage array to alternate media such as disk, tape, or cloud.

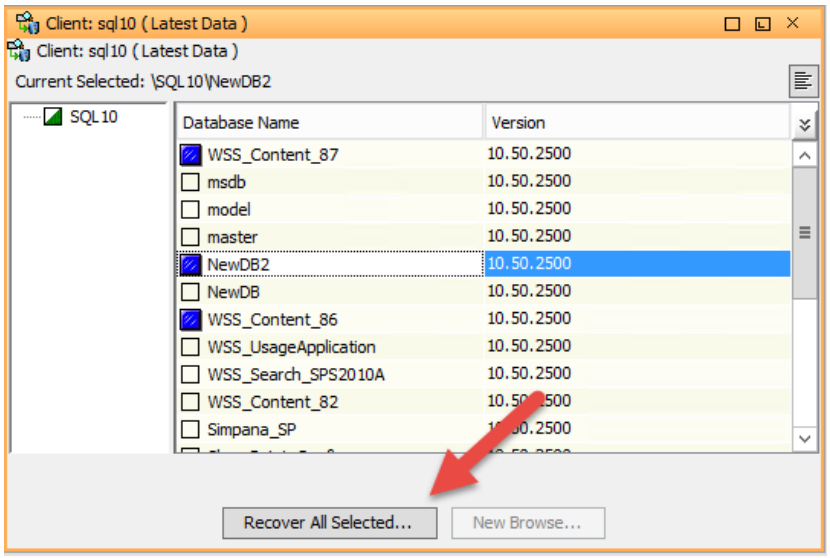


Access, Restore, and Clone

- Browse and Restore
- Navigate to and expand the SQL client in the CommCell Console then right click on the SQL instance and select **Browse and Restore**
- Enter the desired browse dates and click **View Content** to start the browse window
- The default options will show the latest backup data
- Use the **Time Range** option and enter specific backup start and end dates
- Use the **Relative Time** option to view data based on a recent number of days
- Use the **Advanced** tab to filter the browse to include database or file groups.

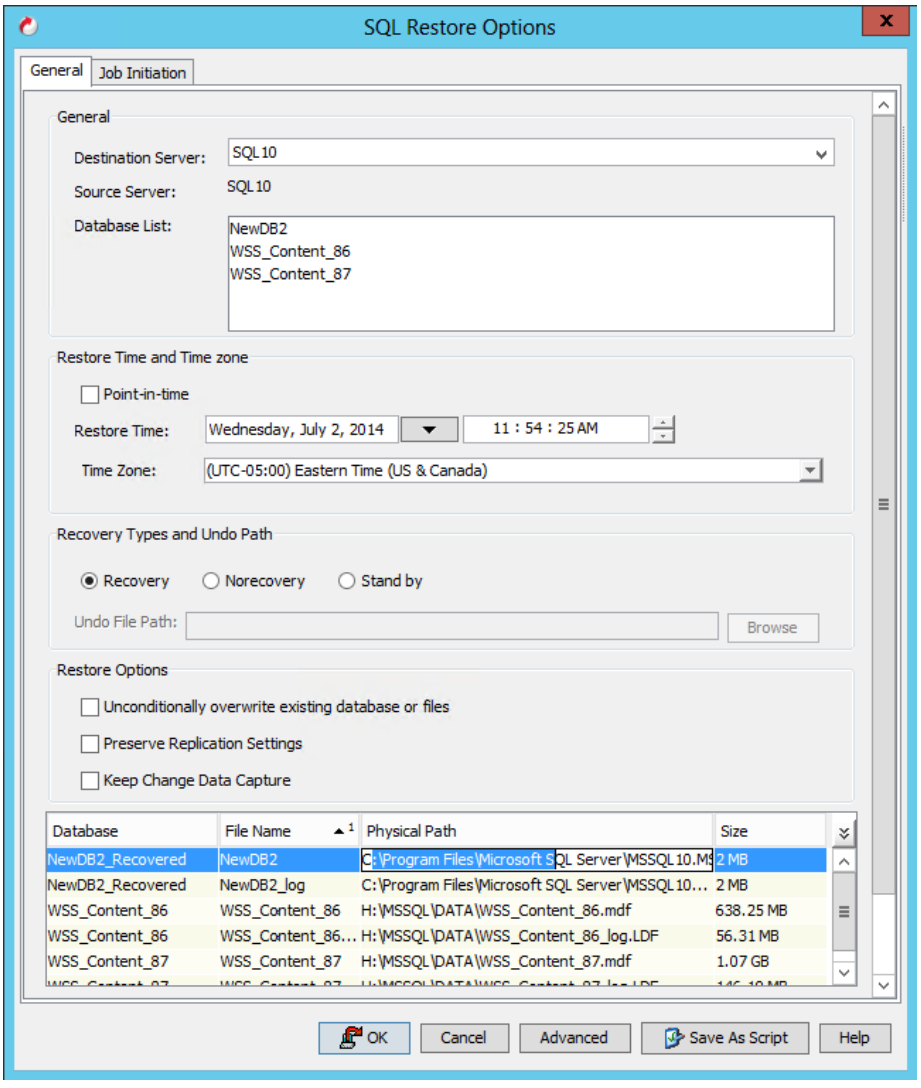


- Select the database(s) to be restored and click **Recover All Selected**



By default the restore options are configured to restore to the original server, instance, and database name and path with the latest backup data. The following defines restore options.

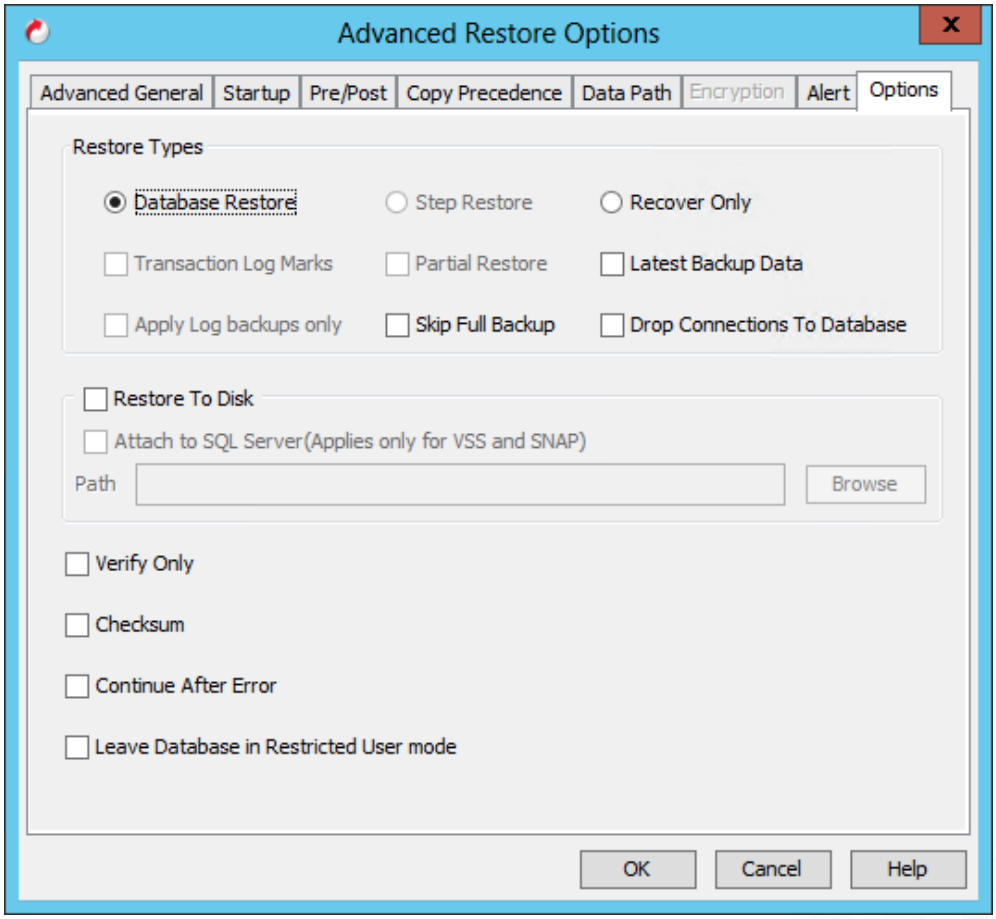
- **Destination Server** – The SQL server to restore the data too. Requires the SQL iDataAgent to be installed as well as Media Agent if a snap shot is to be mounted on that host.
- **Point-in-Time** – Set the restore time to the exact point in time desired. The restore of the database and transaction logs and the playing of the transaction logs to get the database to the exact point in time specified is fully automated.
- **Recovery types** – Controls the state of the database post restore.
  - Recovery – database is brought online.
  - No recovery – database is left in an offline state.
  - Standby – database is left in a standby state.
- **Restore Options** – Controls the behavior of the restore process
    - Click into the database and physical path fields to modify the database name and path if desired.



Additional advanced restore options are defined here.

- Restore type
  - **Database restore** – typical restore operation
  - **Step restore** – used with No Recovery and Standby restore options, step restore allows the administrator to restore the database and play the log sequence one step/log at a time.

- **Recover Only** – database is recovered to an online state. No data is written.
- **Transaction Log Marks** – the restore will recover transaction log marks in the database if they existed at the time of backup.
- **Partial Restore** – AKA Piecemeal Restore, restores file groups individually in a sequence.
- **Latest Backup Data** – Restores latest backup data.
  - **Apply Log backups only** – Restores only the transaction log backups created since the last restore operation. Used with the Latest Backup Data feature this allows administrators to keep a restored copy of a production data on another server (hot standby) and update it with the latest transaction.
- **Skip Full Backup** – Prevents the full database backup from being restored and applies only the transaction logs.
- Drop Connections to Database – Automatically drops connections for the database being restored.
- **Restore to Disk** – Restore the database and log files to a disk location. Allows for a database from VSS or IntelliSnap backup to be recovered to disk then manually added to an instance.
- **Attach to SQL server** – Automates the addition of a recovered database to a SQL instance. Used with VSS and IntelliSnap backups and the Restore to Disk option.
- **Verify Only** – validates the data in the backup. No data is restored.
- **Checksum** – checks database to ensure it has not been corrupted while stored on backup media.
- **Continue After Error** – Allows a job to complete if part of its contents is causing errors. Otherwise the job will go into a pending state.
- **Leave Database in Restricted User Mode** – Only the owner of the database will be able to access it post restore.



Browse by Job

1. Right click on the SQL iDataAgent or instance and select View then Backup History or right click on a specific Subclient policy and select **Backup History**.
    - Narrow the history returned via the "Backup History Filter" window or leave the default options to return all history and click Ok.
2. Right click on the desired job and select **Browse and Restore**.

Oracle Configurations

IntelliSnap backup enables you to create a point-in-time snapshot of the data used for backups. An effective way to back up live data is to quiesce it temporarily, take a snapshot, and then resume live operations. IntelliSnap backup works in conjunction with storage arrays to provide snapshot functionality for backup.

You can use the IntelliSnap backup to perform any level of backups (e.g. Full, Incremental). When you switch from a snap to a traditional backup or vice-versa, the next job is converted to a full backup. While performing an IntelliSnap backup or any subsequent operations, you can use a proxy server to reduce the load on the production server. Also, the backup copy operation will use the proxy to move the snap to backup media. Proxy server is supported with hardware storage arrays.

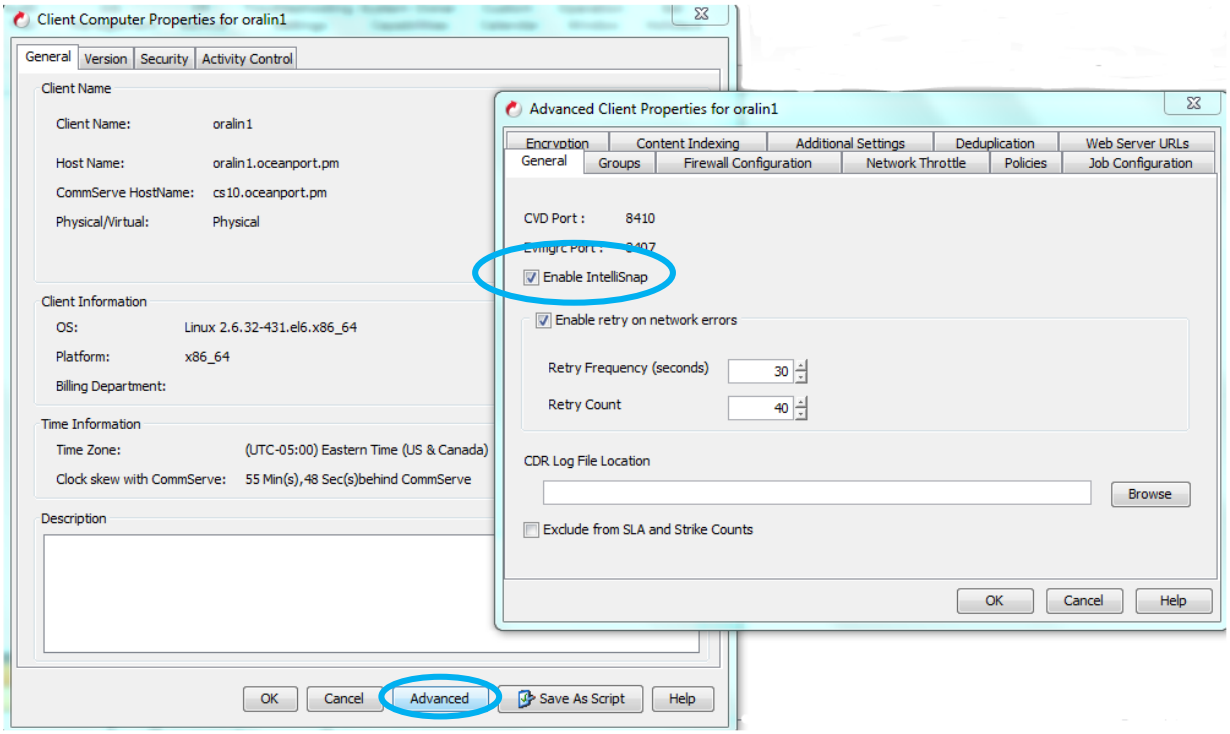
Oracle environments require the following agents:

- **Oracle iDA** on the proxy server and the database server
- **MediaAgent** on the proxy server and the database server

Oracle Client Configuration

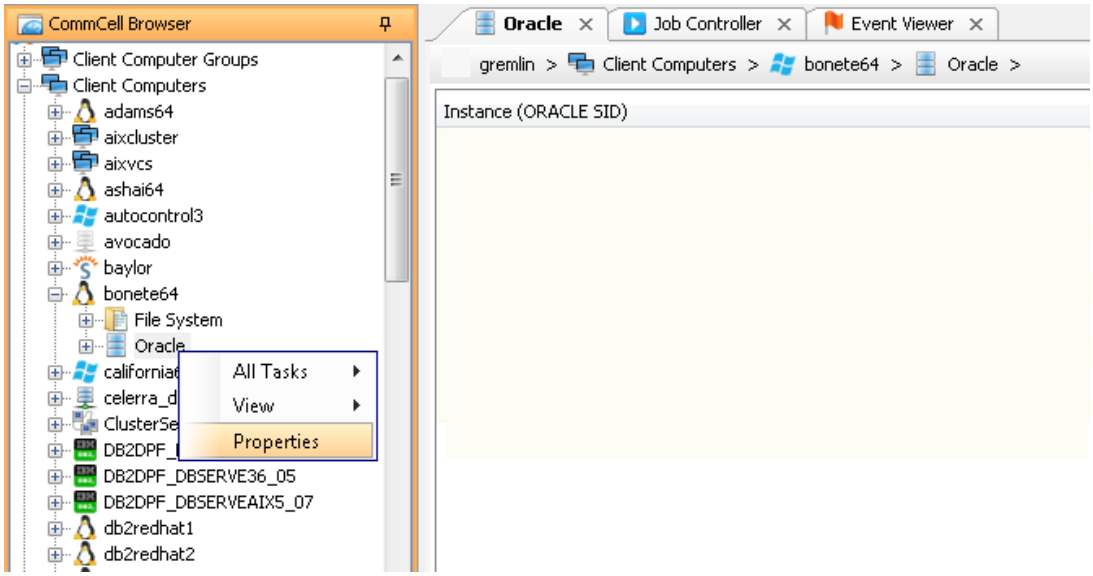
Enable IntelliSnap on the Oracle client object in the CommCell console.

- Right click on the server name, select All Tasks, and then select Properties.
- Navigate to the advanced properties page and check the box marked Enable IntelliSnap. This will consume a Hardware Snapshot Enabler license from the license key.
- In the case of Oracle RAC the client object in question is the master client.

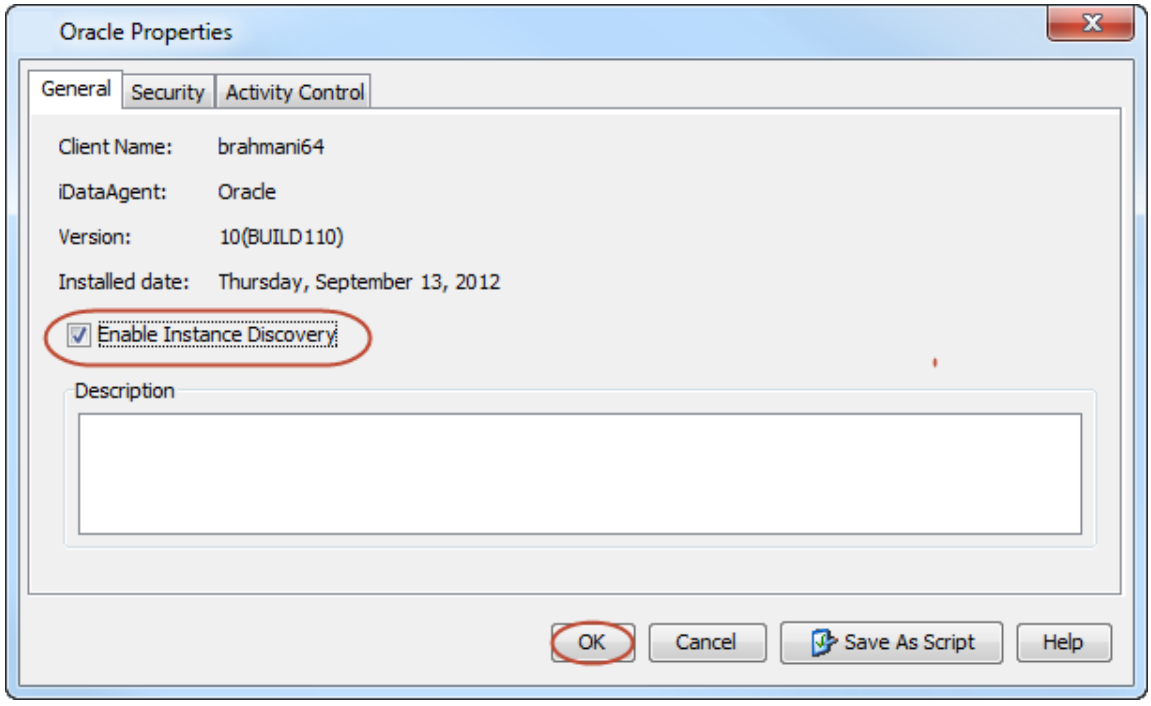


Oracle Instance Configuration

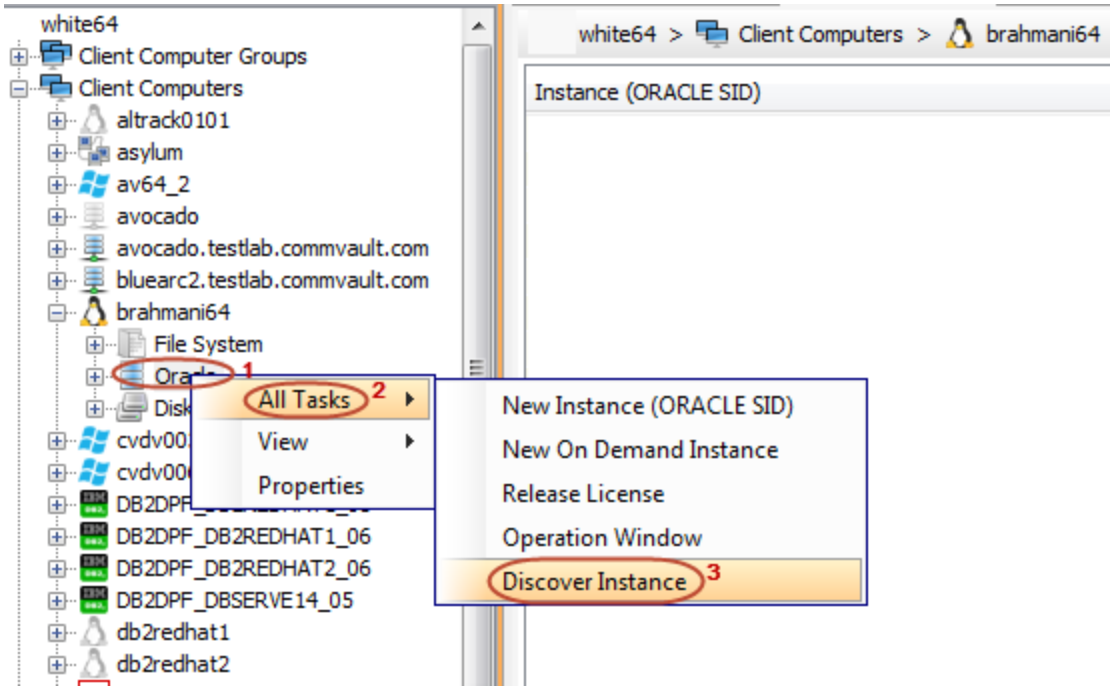
1. From the CommCell Browser, Navigate to Client Computers | <Client>
2. Right-click Oracle and then click Properties.



3. From the Agent Properties dialog box, select the "Enable Instance Discovery" checkbox.

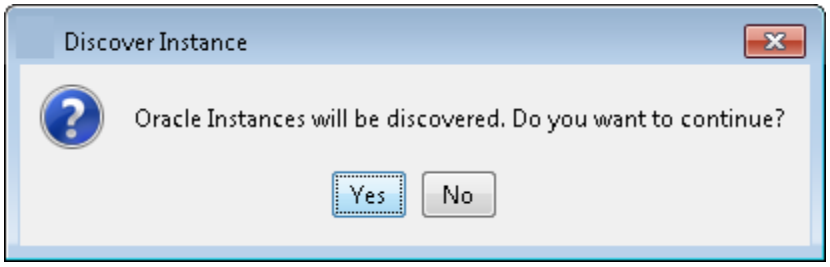


4. Click OK.
5. From the CommCell Browser, navigate to Client Computers | <Client>.
6. Right-click Oracle, point to All Tasks and then click Discover Instance.

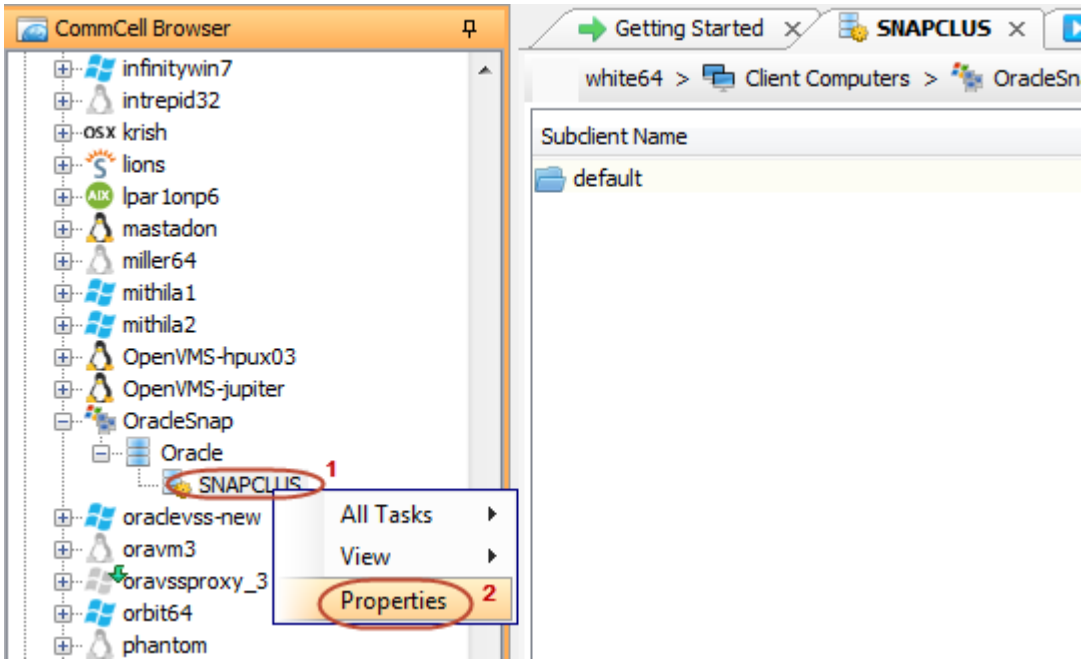


7. Click Yes.

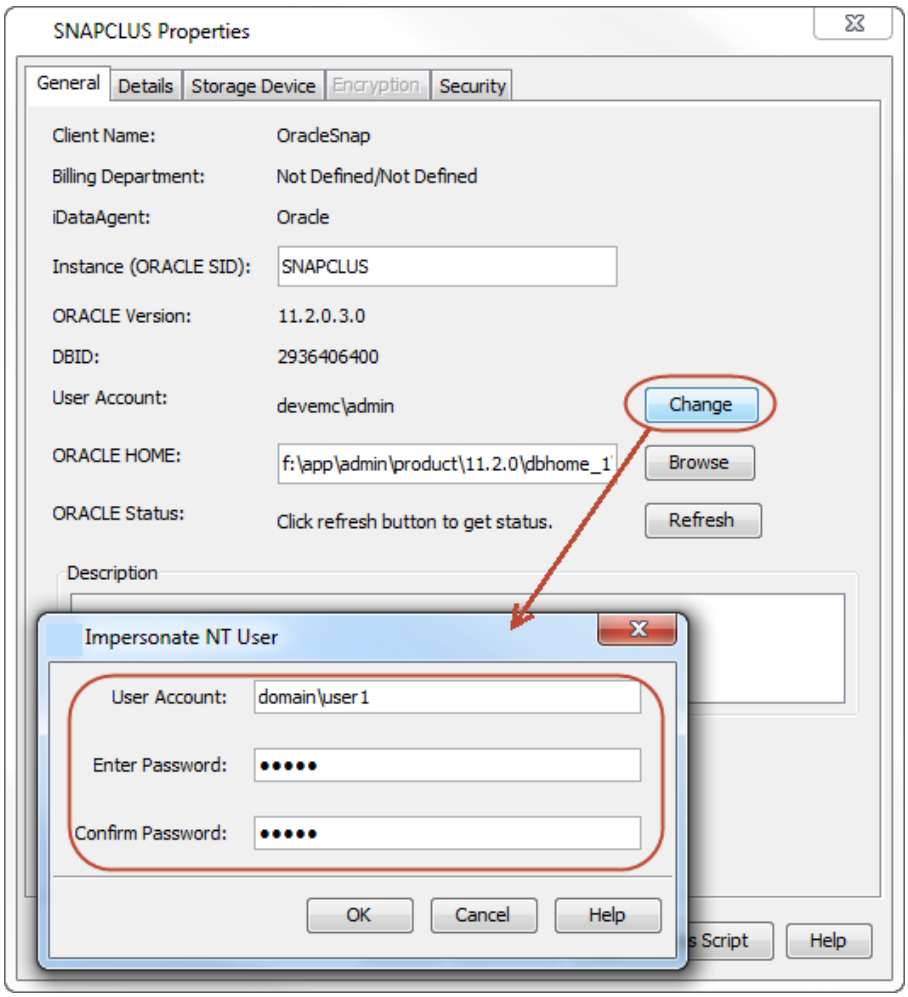
If your Oracle database uses an ASM instance and the instance is in a different Oracle Home, you may have to manually configure the ASM instance as the discovery operation may not find it. When configuring the instance, verify the database status shows as STARTED.



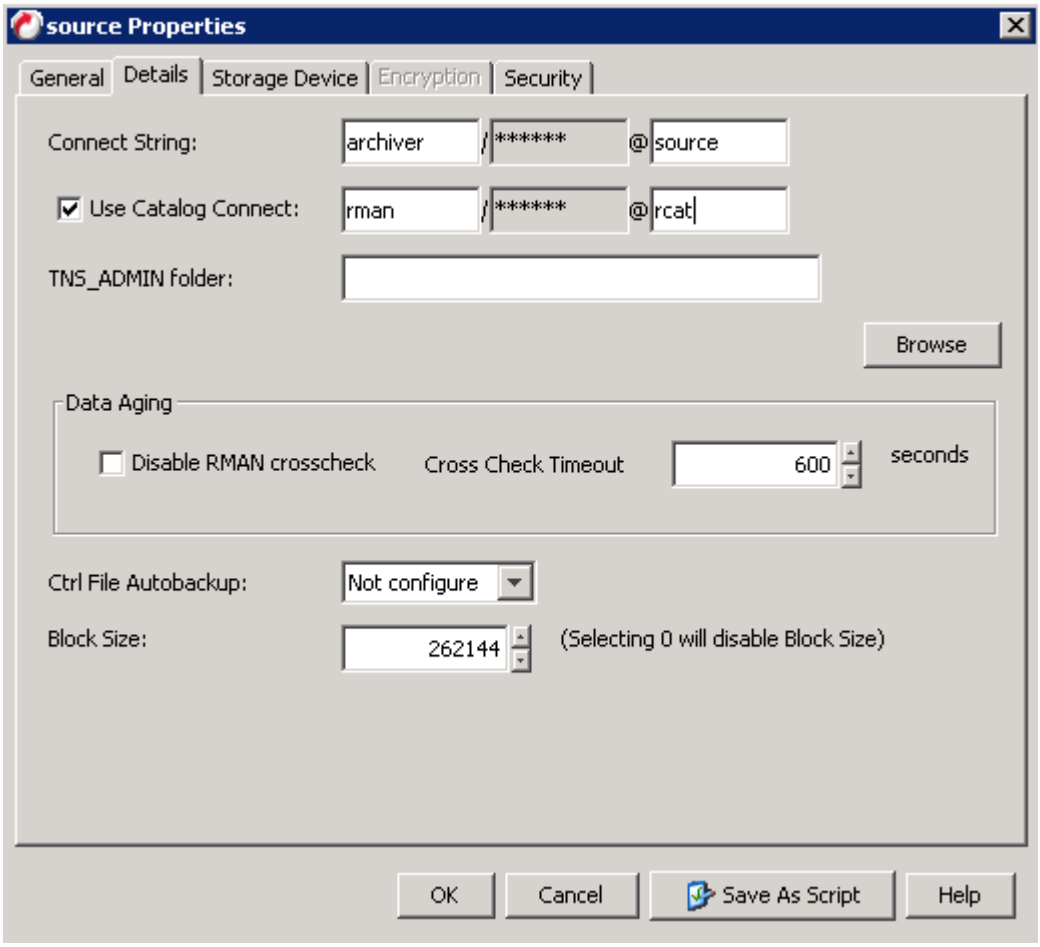
8. From the CommCell Browser, navigate to Client Computers | <Client>|Oracle.
9. Right-Click the <Instance> and then click Properties.


CommCell Browser
infinitywin7
intrepid32
krish
lions
lpar1onp6
mastadon
miller64
mithila1
mithila2
OpenVMS-hpux03
OpenVMS-jupiter
OracleSnap
Oracle
SNAPCLUS
1
oraclevss-new
oravm3
oravssproxy_3
orbit64
phantom
All Tasks
View
Properties
2
Getting Started
SNAPCLUS
white64 > Client Computers > OracleSn
Subclient Name
default

10. On Windows clients:
    - Click Change.
    - In the User Account box, enter the user name to access the Oracle application.
    - In the Password box, enter the password for the user account.
    - In the Confirm Password box, re-confirm the password.
    - Click OK.

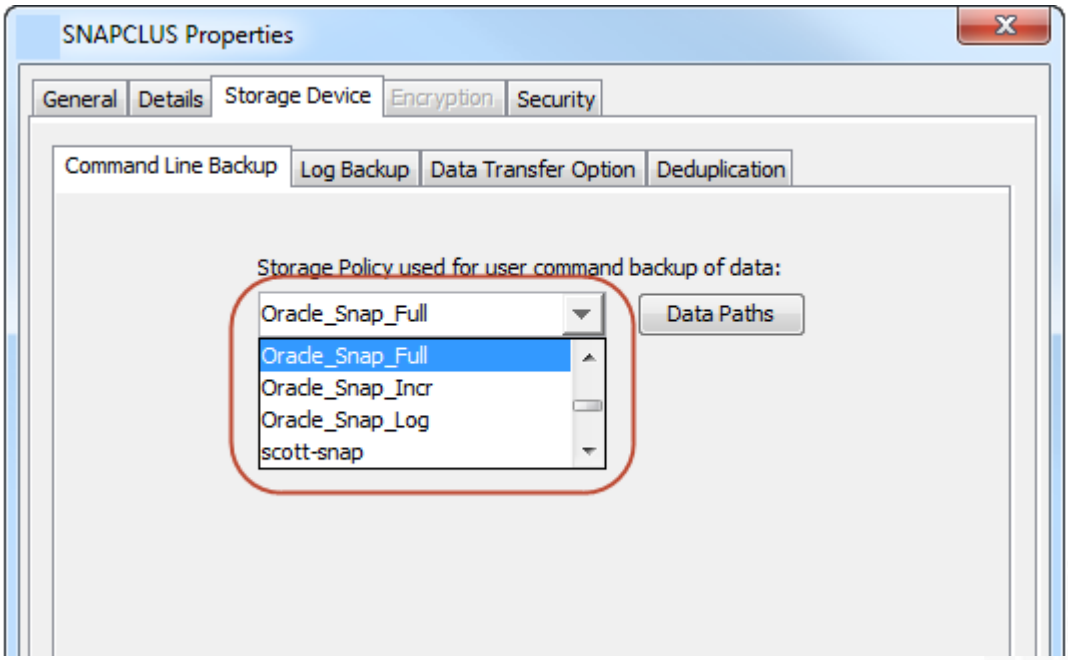


11. Click the Details tab.
    - In the Use Catalog Connect field, type the user name to connect to the Recovery Catalog database.
    - Click the grayed box in Use Catalog Connect.
    - In the Password field, type the password for the user to connect to the Recovery Catalog database.
    - In the Confirm Password box, re-type the password for the user.
    - Click OK.



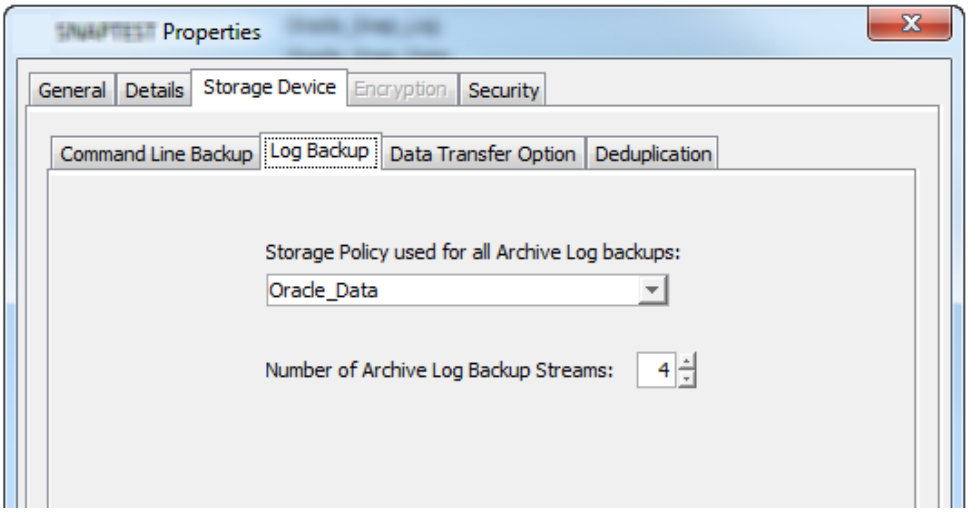
12. Click the Storage Device tab.

- In the Storage Policy used for user command backup of data box, select a storage policy name.

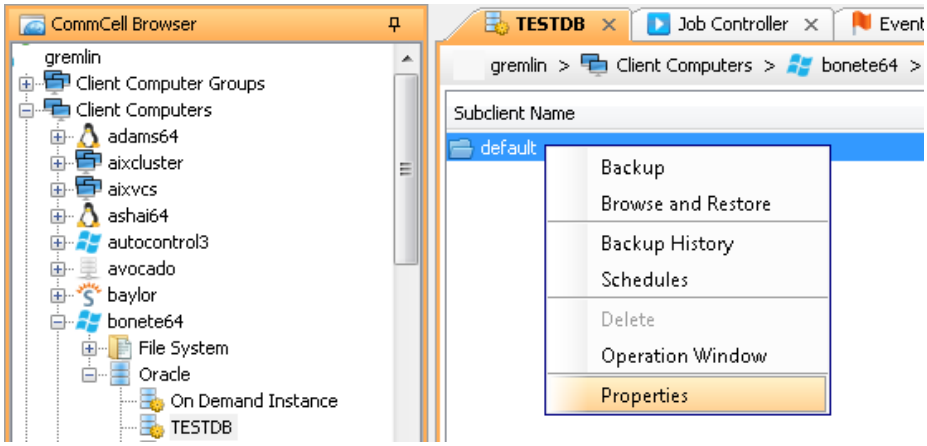


13. Click the Logs Backup tab.

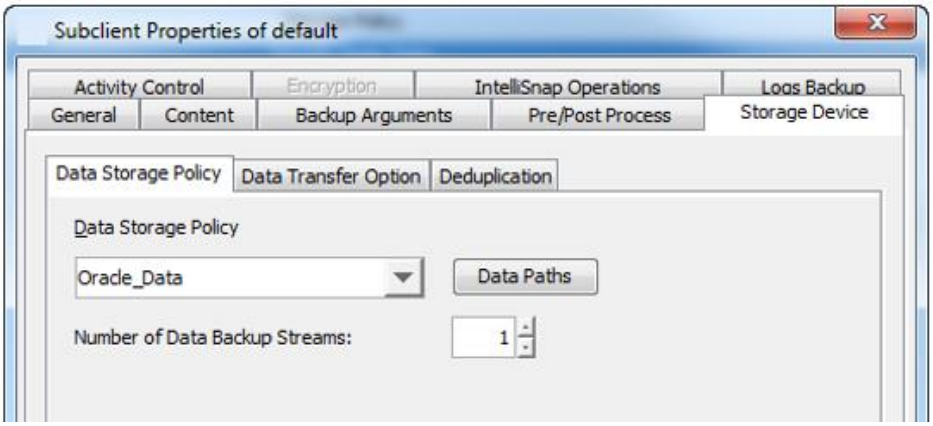
- In the Storage Policy used for all Archive Log backups box, select a storage policy name.
- Click OK.



14. From the CommCell Browser, navigate to Client Computers | <Client> | Oracle | <Instance>.
    - Right-click the default Subclient and then click Properties.



15. Click the Storage Device tab.
    - In the Data Storage Policy list, select a Storage Policy name.
    - Click OK to convert the next backup as a full backup.
    - Click OK.



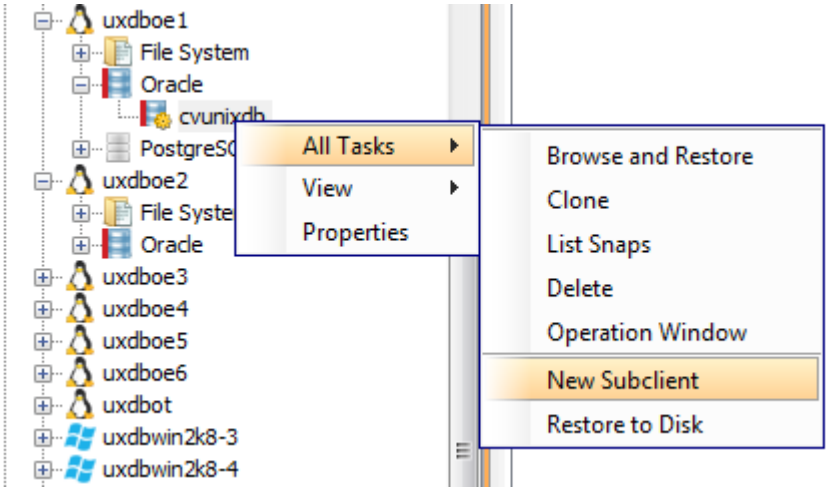
Please note: IntelliSnap can be enabled on the default subclient; however, best practice is to create a separate subclient when using IntelliSnap. This guide will describe the process for creating an IntelliSnap-enabled subclient.

Oracle Subclient Configuration

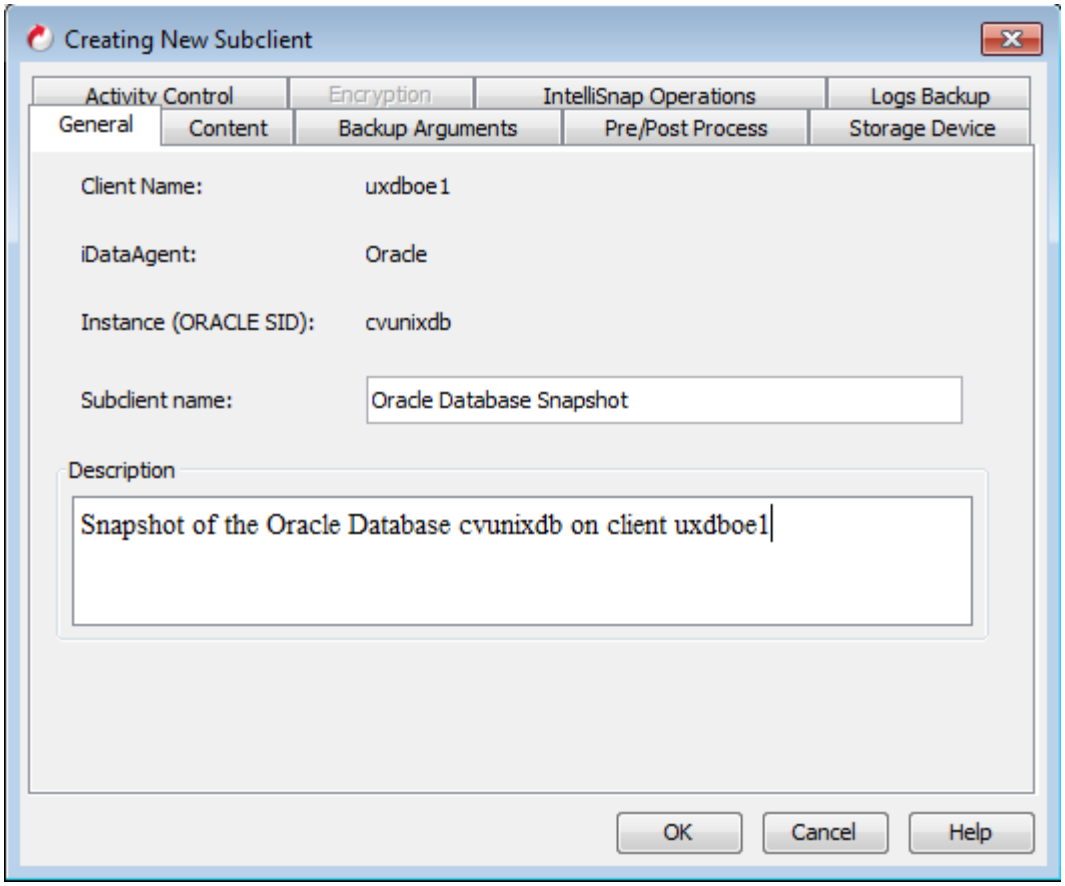
Once the Oracle iDataAgent is installed on a client, configure the Oracle instance and a Subclient to backup the database and /or archive logs.

The following sections provide the necessary steps to configure a Subclient to perform the IntelliSnap backup of a single Oracle database:

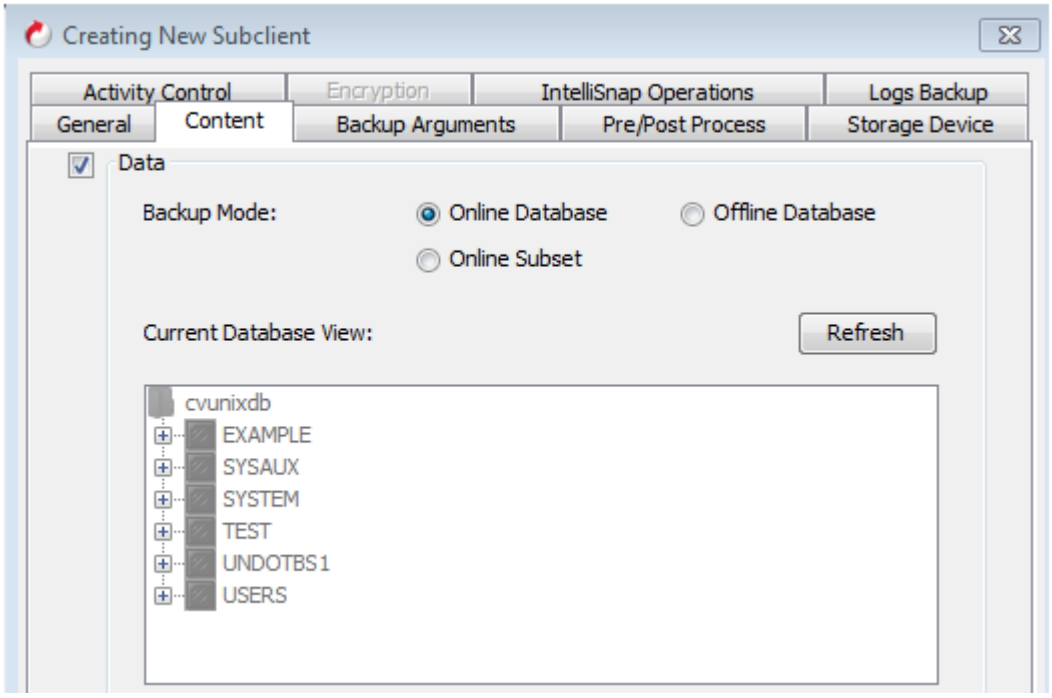
1. From the CommCell Browser, right-click Client Computers node and select All Tasks | New Subclient:



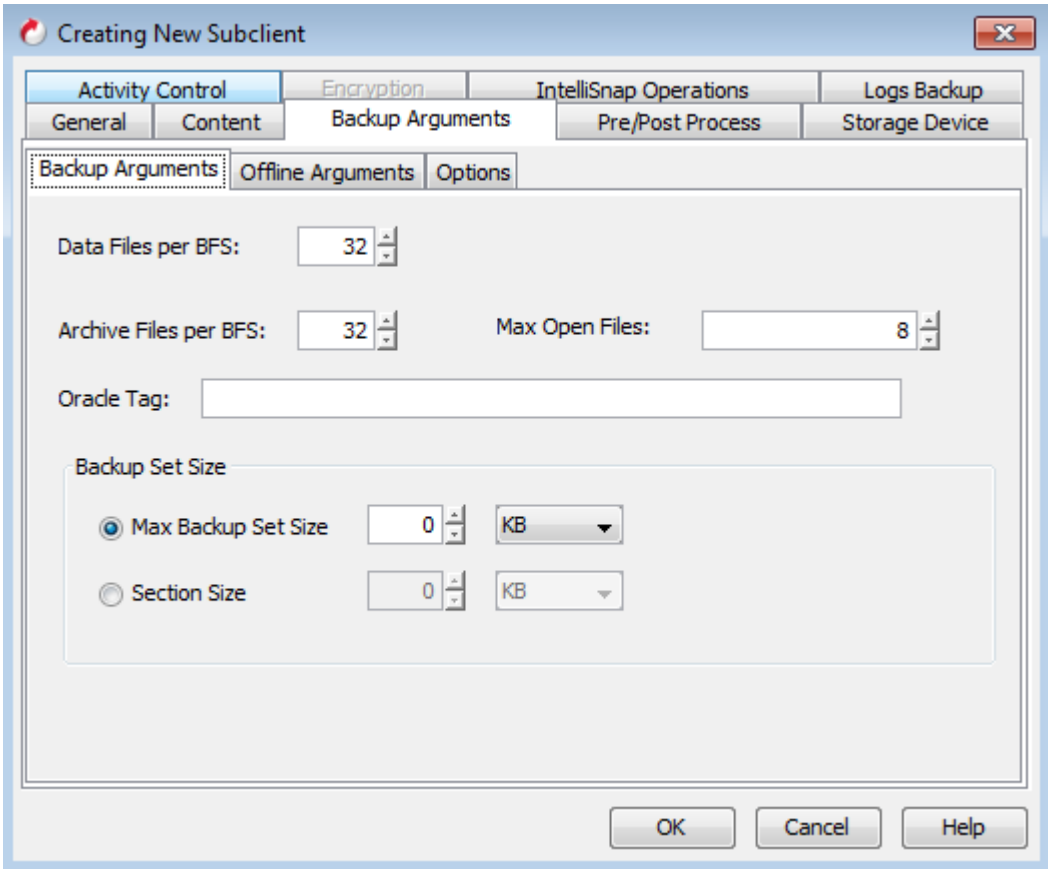
2. On the "General" tab, enter the name of the Subclient and, optionally, a user friendly description for the Subclient:



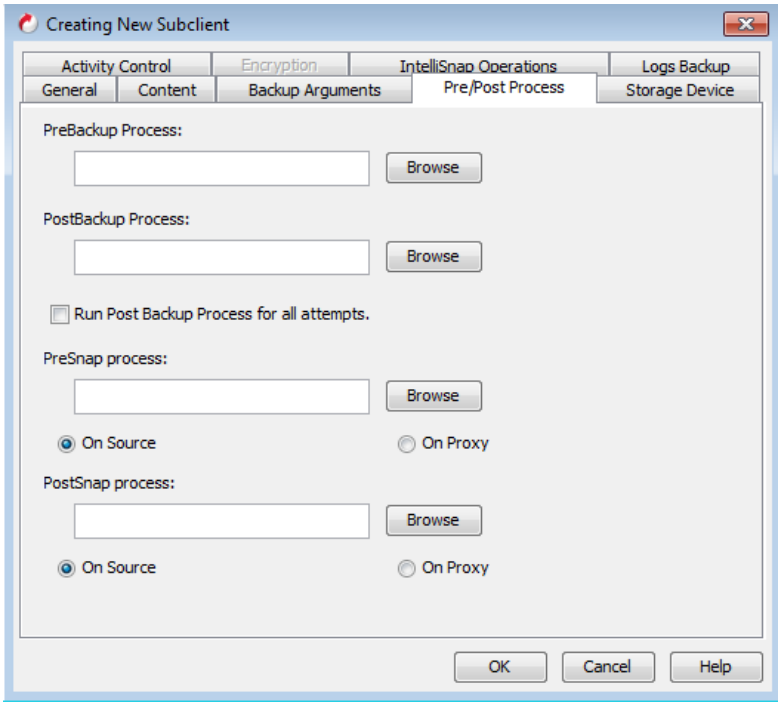
3. On the "Content" tab, select whether the backup will be Online or Offline:



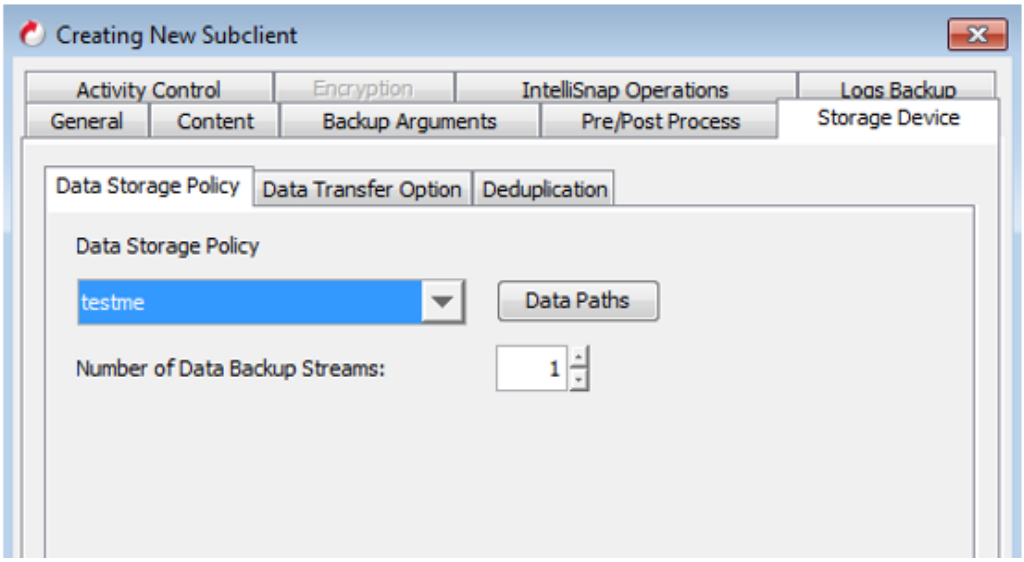
4. Optionally, on the "Backup Arguments" tab, RMAN parameters may be tuned here to help tune performance. Testing must be performed in each specific environment to optimize these RMAN parameters.



5. Optionally, on the "Pre/Post Process" tab, scripts may be called out to perform tasks during the operation, both pre/post snap and pre/post backup:

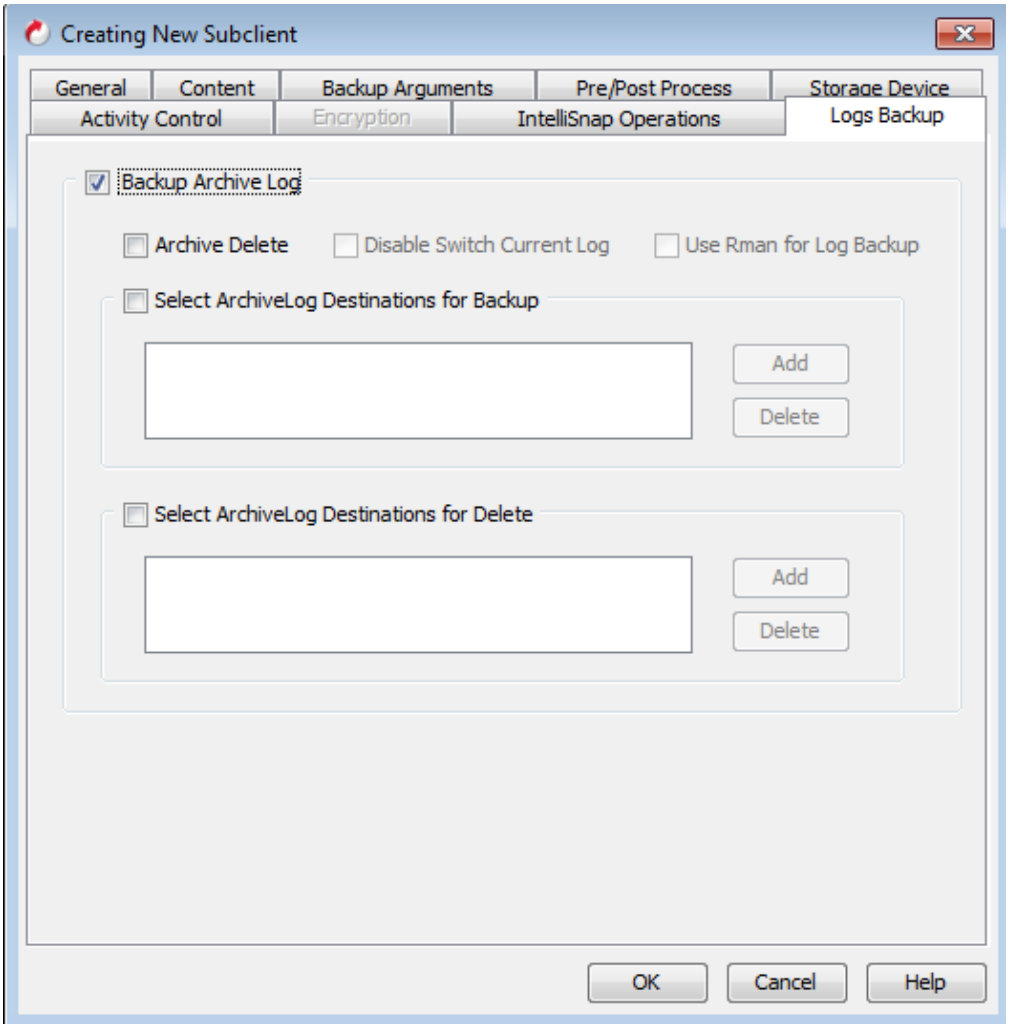


6. On the "Storage Device" tab, the storage policy is chosen and the number of streams is also configured. Compression and deduplication option can also be optionally configured on Storage Device tab:

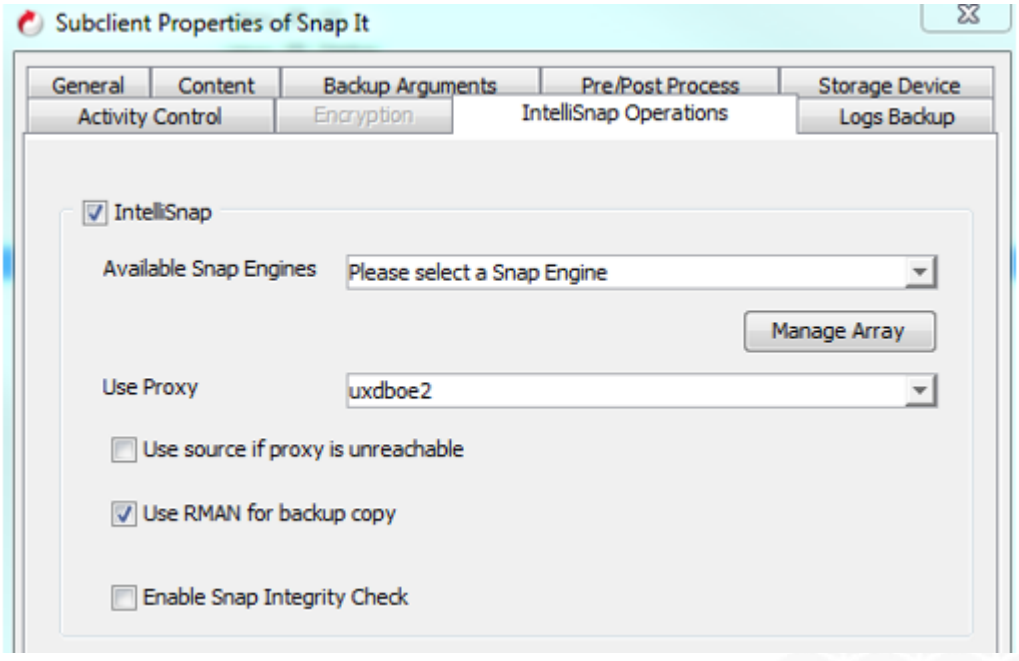


7. The "Logs Backup" tab contains the options for the Oracle Archive Logs. Options include whether or not to backup the archive logs and if the logs are to be deleted after backup. By default, the logs are not deleted after an IntelliSnap backup. Deletion of the logs has to be enabled.

   When you perform an IntelliSnap backup for archive logs, you can specify the location for which an IntelliSnap operation should be performed. This capability enables you to schedule IntelliSnap operations from different log destinations on the same Subclient. If necessary, you can also delete the logs after an IntelliSnap backup.



8. The "IntelliSnap Operations" tab controls the snap options. Enable the IntelliSnap checkbox. Next select the appropriate snap engine from the Available Snap Engines dropdown pick list. If the use of a proxy is desired for backup copy operations, select the proxy from the Use Proxy dropdown pick list.



By default, the backup copy uses the file system for copying data to the media. In this case, the Media Agent and File System iDataAgent must be installed on the proxy. By enabling the "Use RMAN for backup copy", the RMAN backup interface is used for block level backup operations. Also, these backup operations are recorded on the RMAN catalog. RMAN is required in the case of Automatic Storage Management (ASM) Oracle Databases, since ASM data is not available on the file system. You can also run RMAN restores/reports from these backups.

Prior to using RMAN for copying the data to the media, ensure the following:

- The Oracle iDataAgent and MediaAgent must be installed on the proxy computer.
- The Oracle instance on the proxy computer should have the same name as that in the source computer.
- The Oracle version installed on the proxy and source computers should be compatible. However, the major version of Oracle should be the same.
- For backups involving ASM instances, both ASM and the RDBMS instances have to be configured on the proxy computer.
- The catalog user and the catalog database must be the accessible by the source and the proxy Oracle instances.
- The proxy and source computer should have the same directory structure e.g. dump, diagnostic and data directories.
- Oracle database requires the ASM to be registered with Oracle Cluster Registry (OCR). It will ensure the RMAN to successfully mount the disk group.
- If multiple source client database instances are configured to run RMAN backup copy on the same proxy MediaAgent, the backup copy may fail due to instance and database name conflicts. The conflicting database and instances need to be moved to a different proxy MediaAgent in such cases.

  When performing IntelliSnap backup using a proxy, ensure that the operating system of the proxy server is either same or higher version than the client computer.

  For clustered environments, ensure the proxy you want to select is not part of a cluster setup.

During an RMAN backup copy, the proxy database is started in mount mode using the backup control file from the IntelliSnap backup. Additional Oracle licenses may be required for the proxy database. Please inquire with Oracle support to determine if additional Oracle licenses are required in your environment.

The "Enable Snap Integrity Check" option is disabled by default. When enabled, the following additional steps are performed after taking the snapshot:

1. The snapshot is mounted on the source and cataloging of datafiles/archived logs is performed from the mounted snapshot. This verifies whether all the datafiles/archived logs are properly captured during an IntelliSnap backup. RMAN catalog datafilecopy checks the datafile header and verify its authenticity before cataloging it.
2. Once the catalog is completed, an uncatalog happens and the snapshot is unmounted from the source.

ASM Considerations

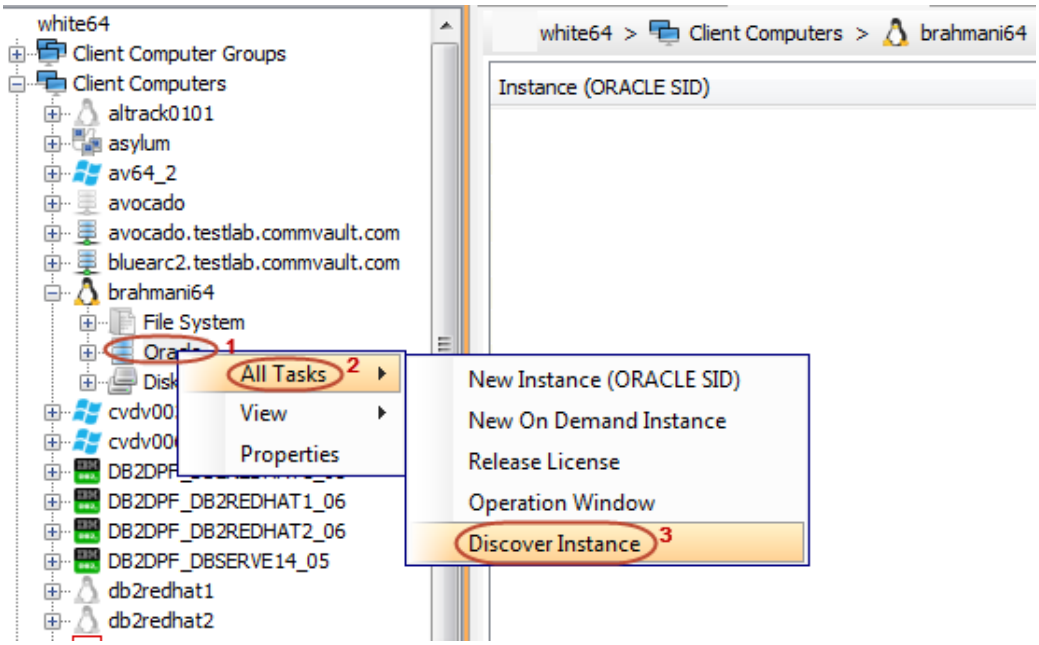
Make sure to separately configure an ASM instance on the CommCell Console in addition to an RDBMS instance.

- Make sure that the kfed utility resides under <Oracle ASM Home>/bin location. If the kfed utility do not exist, then build the kfed utility as shown in the following example:
  - cd <Oracle ASM Home>/rdbms/lib
  - make –f ins_rdbms.mk ikfed
  - Ensure that the ASM disk string is not empty.

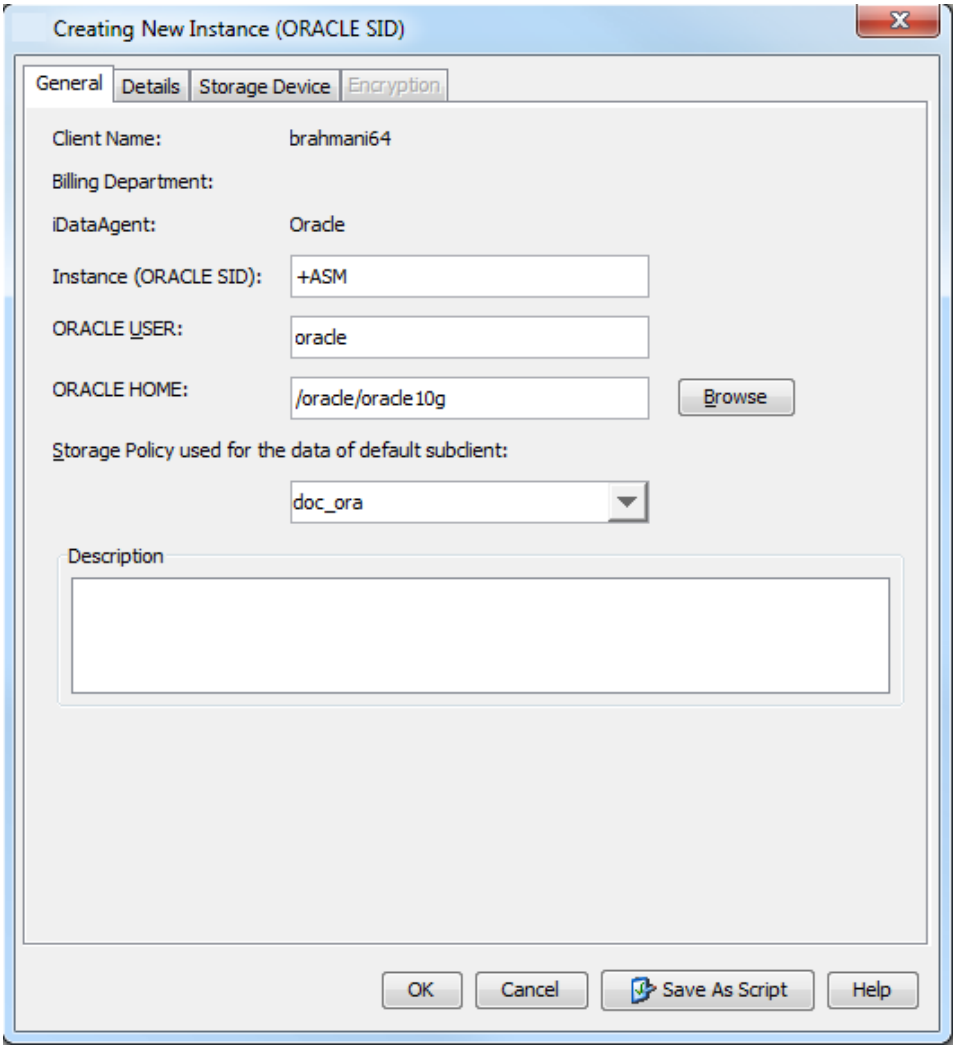
Use the following steps to configure the ASM instance:

1. From the CommCell Browser, navigate to Client Computers | <Client>.
2. Right-click Oracle, point to All Tasks and then click Discover Instance.

3. Click Yes.
4. If your instance is in a different Oracle Home, you may have to manually add the instance as the discovery operation may not find it. When configuring the instance, verify the database status shows as STARTED.



5. From the CommCell Browser, navigate to Client Computers |<Client>.
6. Right-click Oracle, point to All Tasks, and then click New Instance (ORACLE SID).
7. In the Instance (ORACLE SID) box, type the Instance name.
8. In the User Account box, type the login credentials to access the Oracle client.
9. In the ORACLE HOME box, type the Oracle application install path.
10. In the Storage Policy used for the data of default subclient box, select a storage policy name.
11. Click the Storage Device tab.
12. In the Storage Policy used for user command backup of data box, select a storage policy.
13. Click the Log Backup tab.
14. In the Storage Policy used for all Archive Log backups box, select a storage policy name.
15. Click OK.



16. Click the Details tab.
17. In the Connect String box, type the credentials to access the Oracle database. For example, sys/pwd12@orcl4.
18. Click the Storage Device tab.
19. In the Storage Policy used for user command backup of data box, select a storage policy.
20. In the Storage Policy used for all Archive Log backups box, select a storage policy name.
21. Click OK.

Once you create the ASM instance, you also need to create a corresponding RDBMS instance for the Oracle client. You can create Subclients for the regular RDBMS instance and perform IntelliSnap backup jobs. When creating the Subclient for IntelliSnap operations, you must manually refresh the database after enabling IntelliSnap. This will automatically select and grey out the Use RMAN for backup copy option on the Subclient. If the ASM disks are from a persistent snap engine, then you need to disable the snap integrity.

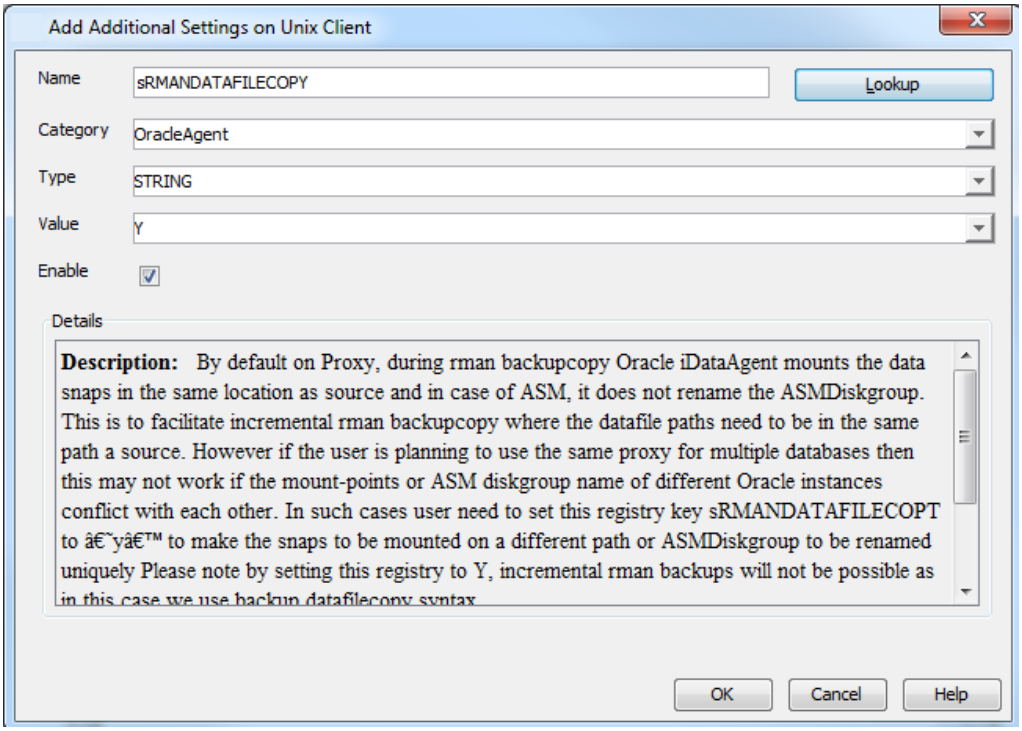
Preventing RMAN Backup Copy Failures due to Mount Point and ASM Disk Group Name Conflicts on a Proxy MediaAgent

By default, during RMAN backup copy the data snaps are mounted in the same location as source on proxy MediaAgents. In case of ASM databases, the ASM Disk Groups are **not** renamed during RMAN backup copy. This is to facilitate incremental RMAN backup copy where the datafile paths need to be in the same path as source. However, if you use the same proxy MediaAgent for multiple databases RMAN backup copy may fail if the file system mount points or ASM Disk Group names of different Oracle instances conflict with each other.

In such cases, use the following steps to make the data snaps to be mounted on a different path or in case of ASM databases, to rename the ASM Disk Groups uniquely:

From the CommCell Browser:

1. Navigate to **Storage Resources | MediaAgents**.
2. Right-click the **<Proxy MediaAgent>**, and then click **Properties**.
3. Click the **Additional Settings** tab.
4. Click **Add**.
5. In the **Name** box, type sRMANDATAFILECOPY.
6. In the **Category** box, type or select **OracleAgent** from the list.
7. In the **Type** box, select **String**.
8. In the **Value** box, type **Y** and then click **OK**.
9. RMAN incremental backups will not be possible if we set this registry key as we use BACKUP DATAFILECOPY syntax in this case.



Configuring RMAN Backup Copy Using Proxy for ASM Databases

When data is moved from snap to media, the RMAN backup interface is used for block level backup operations. Also, these backup operations are recorded on the RMAN catalog. RMAN is required in the case of Automatic Storage Management (ASM) Oracle Databases, since ASM data is not available on the file system. You can also run RMAN restores/reports from these backups.

Prerequisites

Prior to using RMAN for copying the data to the media, ensure the following:

- Both source and proxy machine should have the same O/S resources like directory structure, memory, and kernel.
- The Oracle iDataAgent must be installed on the proxy computer.
- The Oracle instance (RDBMS) on the proxy computer should have the same name as that in the source computer.

- The Oracle version installed on the proxy and source computers should be compatible. However, the major version of Oracle should be the same.
- For backups involving ASM instances, both ASM and the RDBMS instances have to be configured on the proxy computer.
- The ASM instance and RDBMS instance should be started.
- Also RDBMS and ASM instances should be configure on CommCell GUI for PROXY client.
- Using ASM storage, ASM data group should not be same as source database. For example, if source ASM instance has a disk group "DG1", proxy machine should not use "DG1" as disk group name.

  Use the following SQL Script to find data group names on both source and proxy computers:

```
SQlPLUS# select name,total_mb,free_mb from v$asm_diskgroup;
```

- The catalog user and the catalog database must be the accessible by the source and the proxy Oracle instances.
- Make sure the software has permissions to create a disk group on proxy machine similar to source.
- The proxy and source computer should have the same directory structure e.g. dump, diagnostic and data directories.
- Oracle database requires the ASM to be registered with Oracle Cluster Registry (OCR), since the ASM instance is a resource in CRS repository. It will ensure that the RMAN has successfully mounted the disk group.

Use the following steps to configure RMAN backup copy for ASM database:

10. Confirm Oracle Version is same on both Proxy and Source:

    Grid@dbproxy>sqlplus -v
    SQL*Plus: Release 11.2.0.1.0 Production.

11. Copy spfile<SID>.ora from source to target for both ASM instance and RDBMS instance.
12. Create a user for proxy ASM instance with SYSASM, SYSOPER privileges.

```
Grid@powerstar>sqlplus "/ as sysasm"

SQL>create user ASMDBA identified by test01;
User created.
SQL> grant SYSASM, SYSOPER to ASMDBA;
Grant succeeded.
SQL> select * from v$pwfile_users;
USERNAME SYSDBA SYSOPE SYSASM
———————— —— —— ——
SYS TRUE TRUE TRUE
ASMDBA FALSE TRUE TRUE
```

13. Startup the ASM instance and RDBMS instance.
14. Configure the ASM instance and RDBMS instance from the CommCell Console for proxy.

    Once configured, you can run inline or offline backup copy jobs on the CommCell Console.

Oracle Proxy Configuration

IntelliSnap technology supports ASM (Automatic Storage Management) and Recovery Manager (RMAN) backups with array-based snapshots. With this support IntelliSnap technology can leverage RMAN for the movement to media operation. This requires the installation and configuration of the Oracle binaries and the configuration of an Oracle instance on the proxy server. In order to perform a proxy-based IntelliSnap backup or restore operation, configure the following on the proxy computer:

- The Oracle database instance on the proxy machine should be the same version as the source. For example, if Oracle 10.2.0.4 is installed on source then the proxy should be 10.2.0.4.
- Use of ASM requires configuration of both ASM and RDBMS instances on the proxy.

- An RMAN recovery catalog database is required.
- The catalog user and the catalog database must be accessible by both the source and proxy Oracle instances.
- Best Practice is to mount the snapshots on the same ASM mount point as the source. When using the same proxy for multiple source instances, this means each source should have a different ASM mount point to avoid conflicts.
- Best Practice is to ensure that the data and log mount points do not overlap.
- Before executing any ASM based snapshot or movement to media jobs, run the following commands:

```
cd $ORACLE_HOME/rdbms/lib
gmake -f ins_rdbms.mk ikfed
```

Ensure that KFED utility is specified in the path.

After putting the above configurations and considerations in place, the configured server may enable RMAN for tape movement and properly manage ASM databases in a proxy configuration.

Table Level restores of IntelliSnap data is now supported.

Note: It is **highly recommended** to work with Professional Services to ensure successful implementation of IntelliSnap with Oracle databases, especially in proxy configuration.

Oracle IntelliSnap® and Backup Copy

An Oracle IntelliSnap is not an RMAN backup. The following steps are performed to protect the Oracle database:

Backup job is scheduled from the CommCell Console. When the backup job is started:

- List of data files, control files, and log files that make up the database are determined.
- List of physical disks that correspond to the datafiles are determined.
- The database is put in a hot backup mode using the following command:

```
alter database begin backup;
```

- An atomic Snapshot copy of all the Data volumes are created.
- The hot backup mode is stopped using following command:

```
alter database end backup;
```

- The active logs are flushed using the following command:

```
alter system archive log current;
```

- A backup controlfile is created in the archive log destination using following sql command.

```
alter database backup controlfile to 'logdest/backupctl.galaxy';
```

- A snapshot of archive log volumes are created.
- The snapshots for DATA and LOG volumes are mounted and the integrity of files on snap are verified by using RMAN interface for file cataloging. Once this is done, uncatalog operation is also done.
- Relevant file entries in the snapshot are indexed.
- The snapshot index is archived.

The IntelliSnap Backup Copy Operation is supported using two interfaces:

- File System Backup Copy
- RMAN Backup Copy

Depending on the requirements and resource availability, users can choose File Level Copy or Block level copy.

File System Backup Copy

During File System Backup Copy operations:

- The job type is always FULL.
- The snapshots for DATA and LOG are mounted.
- The snap device is cloned and Volume Group/Logical Volumes are automatically created to mount the snapshot.
- The Index created during snap is queried to identify files to backup to tape and generates collect file for backup copy.
- The files are backed up to tape or magnetic library.
- The Snapshot is unmounted.
- The index created for backup copy operations are archived.

RMAN Backup Copy

During Block Level Copy operations:

- Both FULL and incremental job types are supported. In this case, catalog configuration is mandatory.

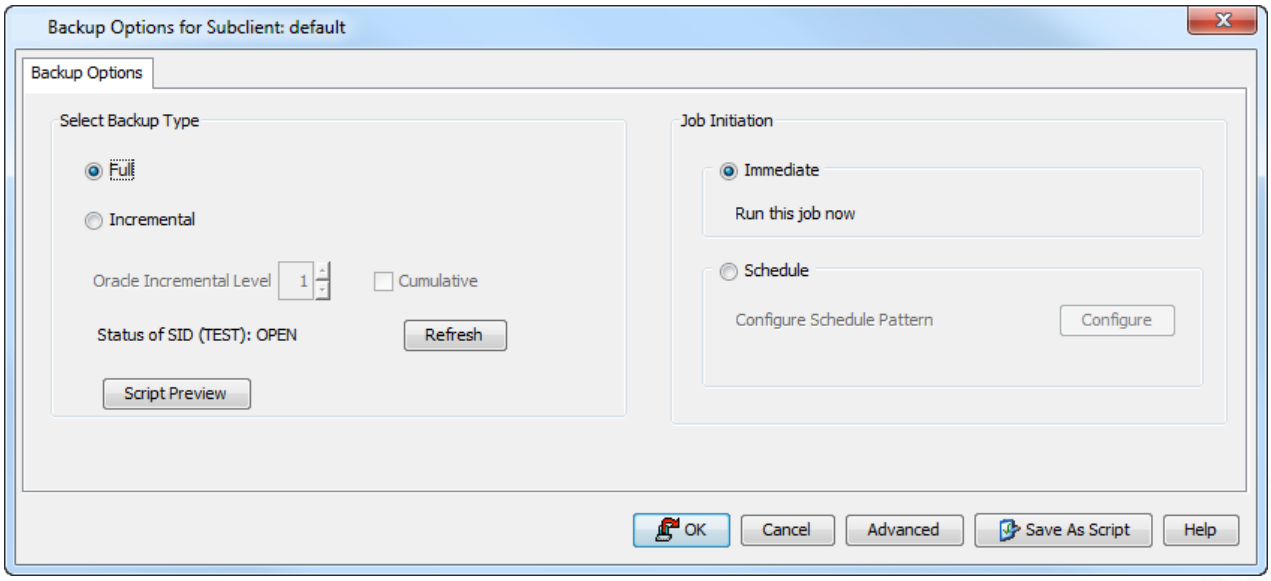
- If proxy is not selected, only FULL jobs are supported and RMAN 'backup datafilecopy' command is used. Also the snapshots are mounted in /opt/simpana/MediaAgent/SnapVolumeMounts/ path.
- If Proxy is selected, the snapshots are mounted in the same path as that of source and the backup database command is issued.
- The snapshots for DATA and LOG are mounted.
- The snap device is cloned and Volume Group/Logical Volumes are automatically created to mount the snapshot.
- The Index created during snap is queried to identify files to backup to tape and generates RMAN scripts for backup copy operations.
- The integrity of files on snap are verified by using RMAN interface for file cataloging. Once this is done, uncatalog operation is also done.
- Initiates the RMAN for backup copy operation.
- Once the uncatalog operation is performed, the Snapshots are unmounted.

There are two options when taking a backup copy, inline and offline.

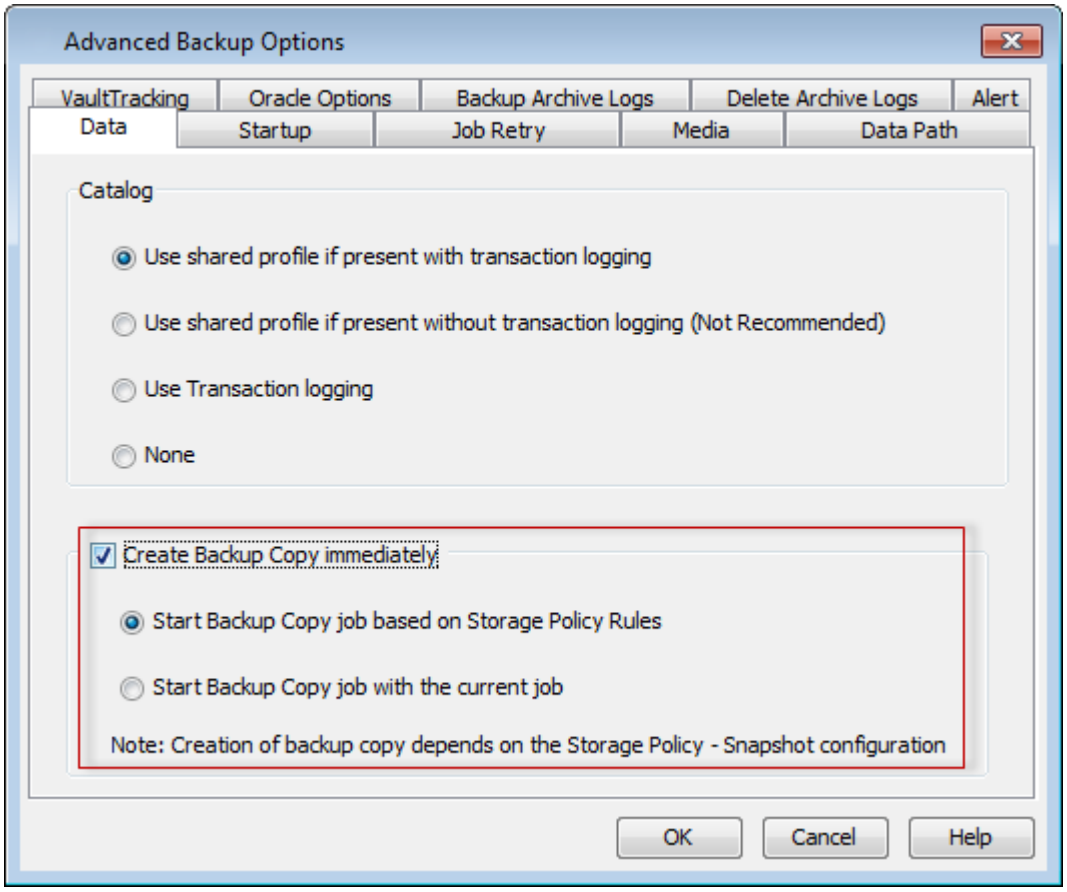
Inline Backup Copy

Backup copy operations performed during the IntelliSnap backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current IntelliSnap job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

1. From the CommCell Console, navigate to Client Computers | <Client> | <Agent> | <Instance>
   - Right click the default Subclient and click Backup.
   - Select Full as backup type.
   - Click Advanced.

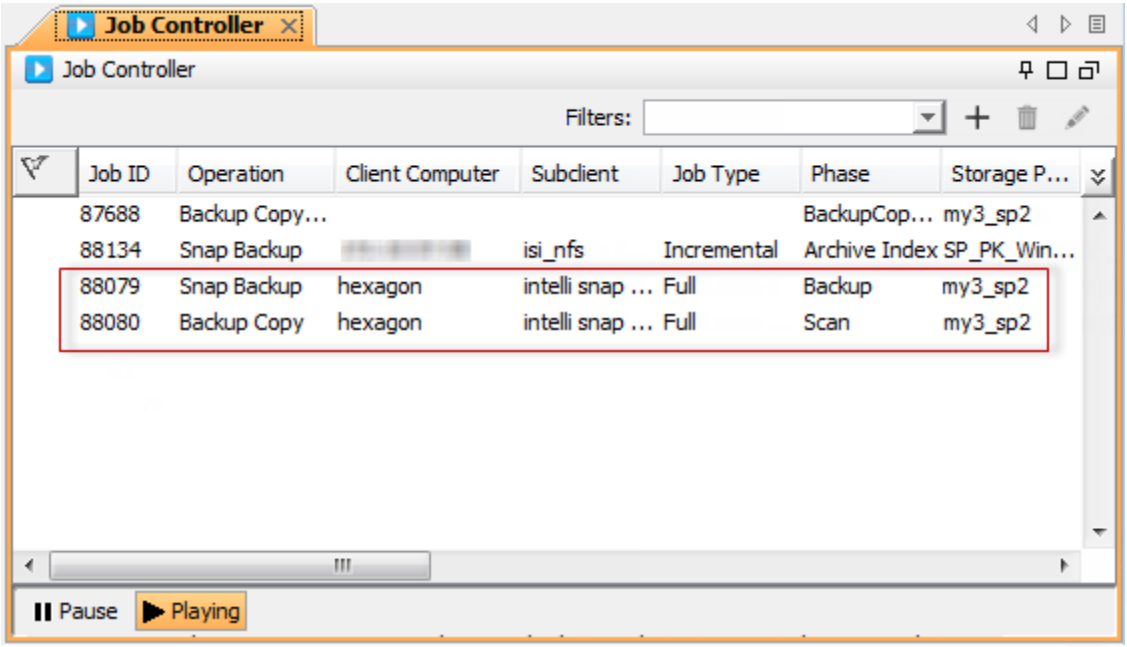


2. From the Advanced Backup Options dialog box, select Create Backup Copy immediately check box to create a backup copy.
   - Click OK.



3. You can track the progress of the Inline Backup Copy job from the Job Controller window.

- When job is initiated, two separate jobs (i.e., Snap Copy job and Backup Copy job) will be displayed in the Job Controller window.

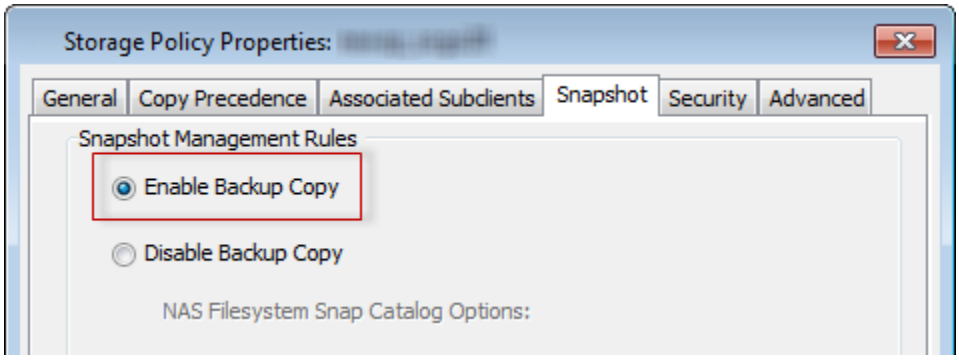


Offline Backup Copy

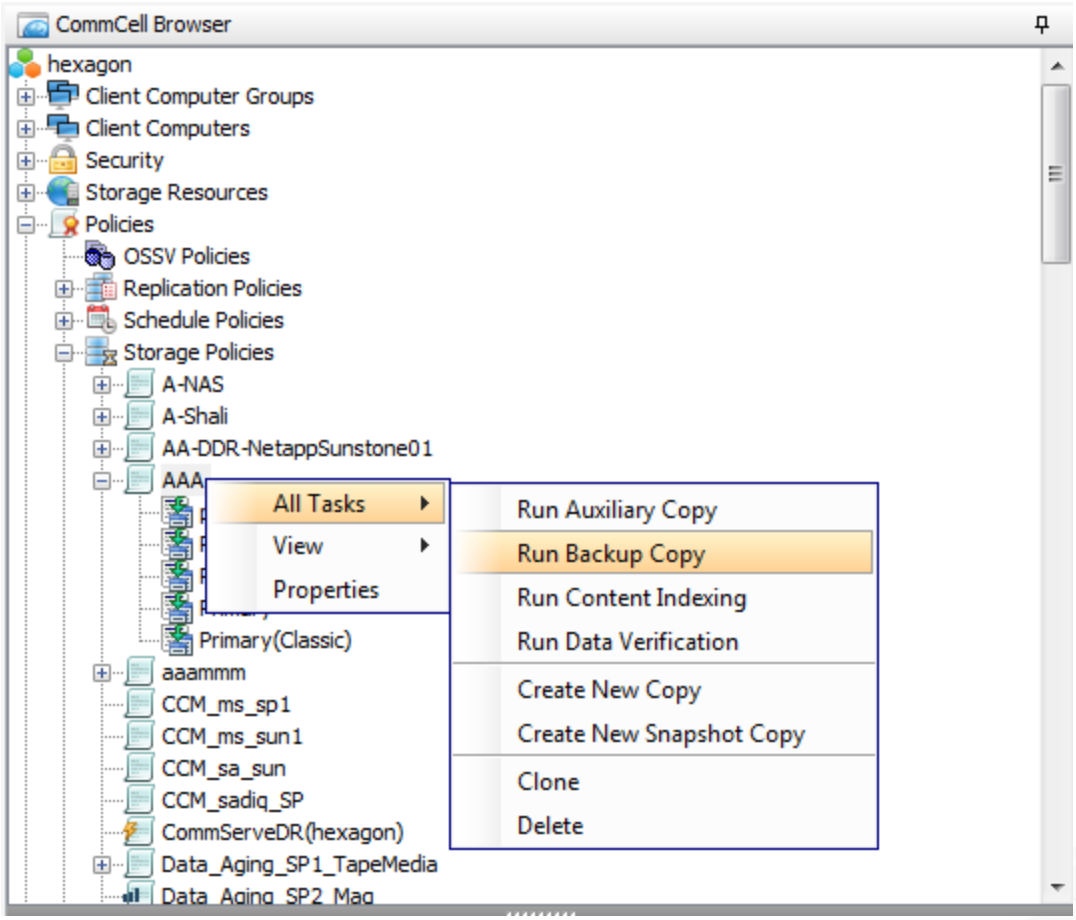
Backup copy operations performed independent of the IntelliSnap backup job are known as offline backup copy.

Use the following steps to run offline backup copy.

4. From the CommCell Console, navigate to Policies | Storage Policies.
   - Right-click the <storage policy> and click Properties.
   - Click the Snapshot tab.
   - Under Snapshot Management Rules, make sure that Enable Backup Copy is selected.
   - Click OK.

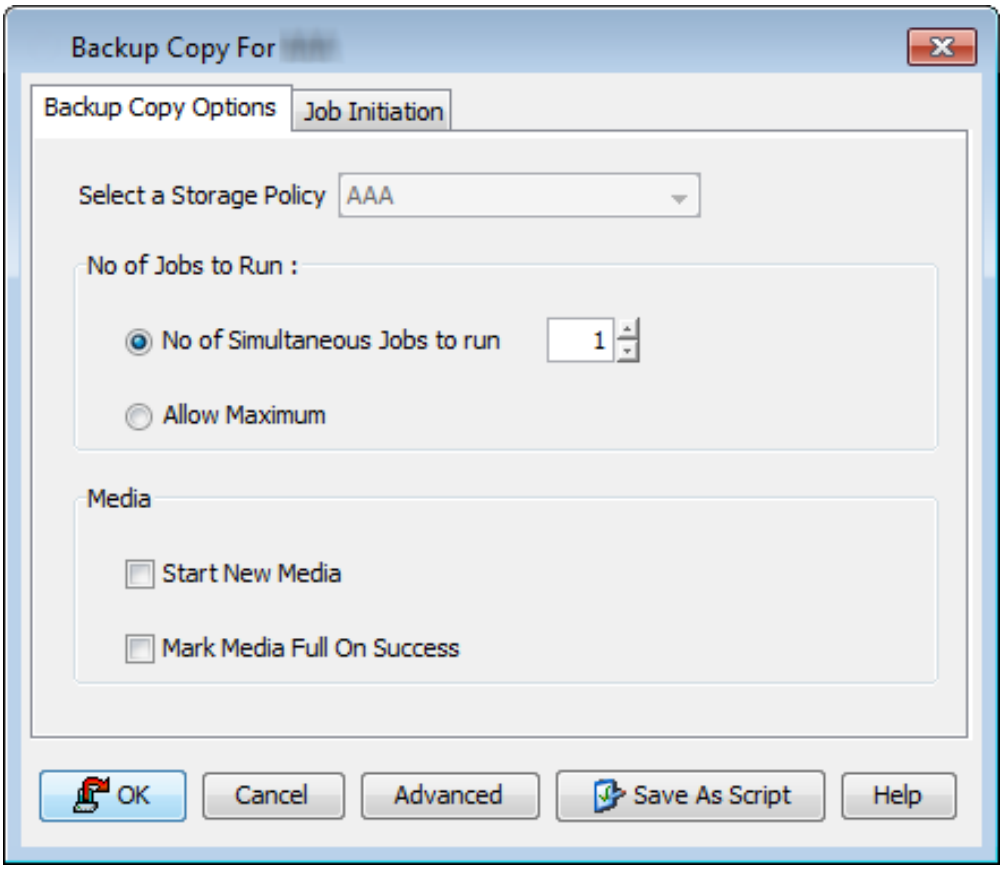


5. From the CommCell Console, navigate to Policies | Storage Policies.
   - Right-click the <storage policy> and click All Tasks | Run Backup Copy.



6. Select Start new media to copy the data to a different tape.

- Select Mark media full on Success to mark the media that is used for this operation after the snapshot copy operation has successfully completed.
- Click OK.



For Oracle iDataAgent the backup copy operations are performed using either the File System or RMAN scripts. By default, File System backup copy is performed. See Configuring Backup Copy Operations for detailed information.

SAP Oracle Configurations

When using SAP environments with BRTools version 7.1 and above, you can perform IntelliSnap backups using the util_vol or util_vol_online backup interfaces. These backup interfaces are provided by SAP to take volume level backups of the database.

Prerequisites for SAP Oracle specific IntelliSnap Backups

Oracle environments require the following agents:

- SAP Oracle iDA on the proxy server and the database server
- Media Agent on the proxy server and the database server

Prior to using the SAP specific IntelliSnap backups, configure the following parameters in the init<SID>.sap file.

For UNIX

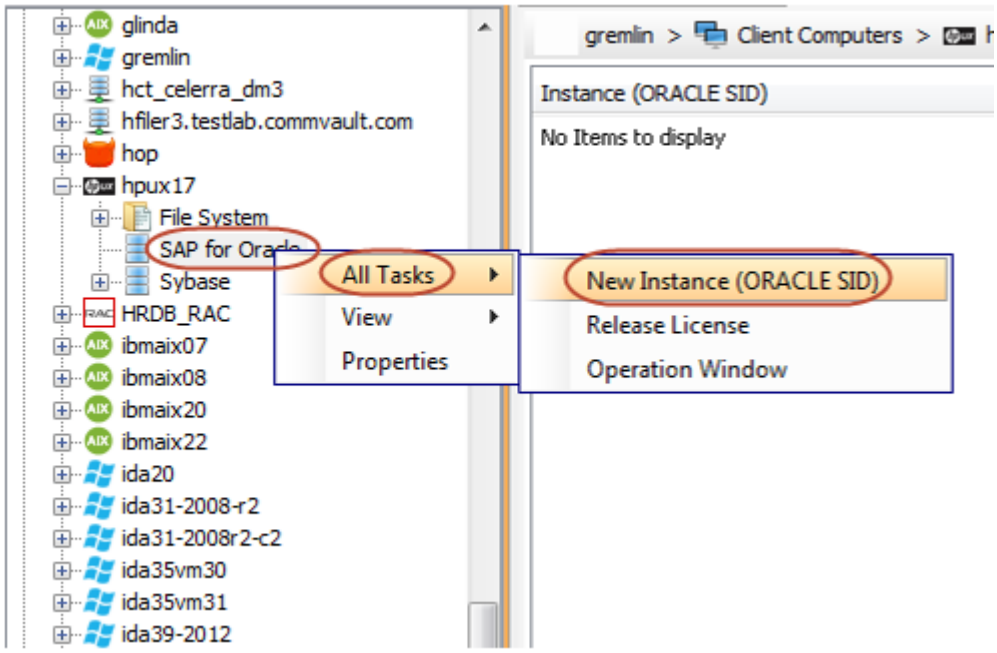
- util_vol_access = copy - specifies that the IntelliSnap backups can be copied to a different target location for verification purposes.
- util_vol_nlist = nocheck - disables the check for non-database files that reside in the volume but does not exist in the input file. Alternatively, you can also set this parameter to disable a specific non database file. For eg., util_vol_nlist = (/oracle/oracle10g/CER/sapdata6/non_db_file)
- util_vol_unit = sap_data - specifies that the smallest unit for the IntelliSnap backup will be the sapdata, origlog, ormirrorlog directories.

For Windows

- util_vol_access = copy - specifies that the IntelliSnap backups can be copied to a different target location for verification purposes.
- util_vol_unit = all_data

SAP Oracle Instance Configuration:

1. From the CommCell Browser,
   - Navigate to Client Computers | <Client>.
   - Right-click SAP for Oracle, point to All Tasks, and click New Instance (ORACLE SID).



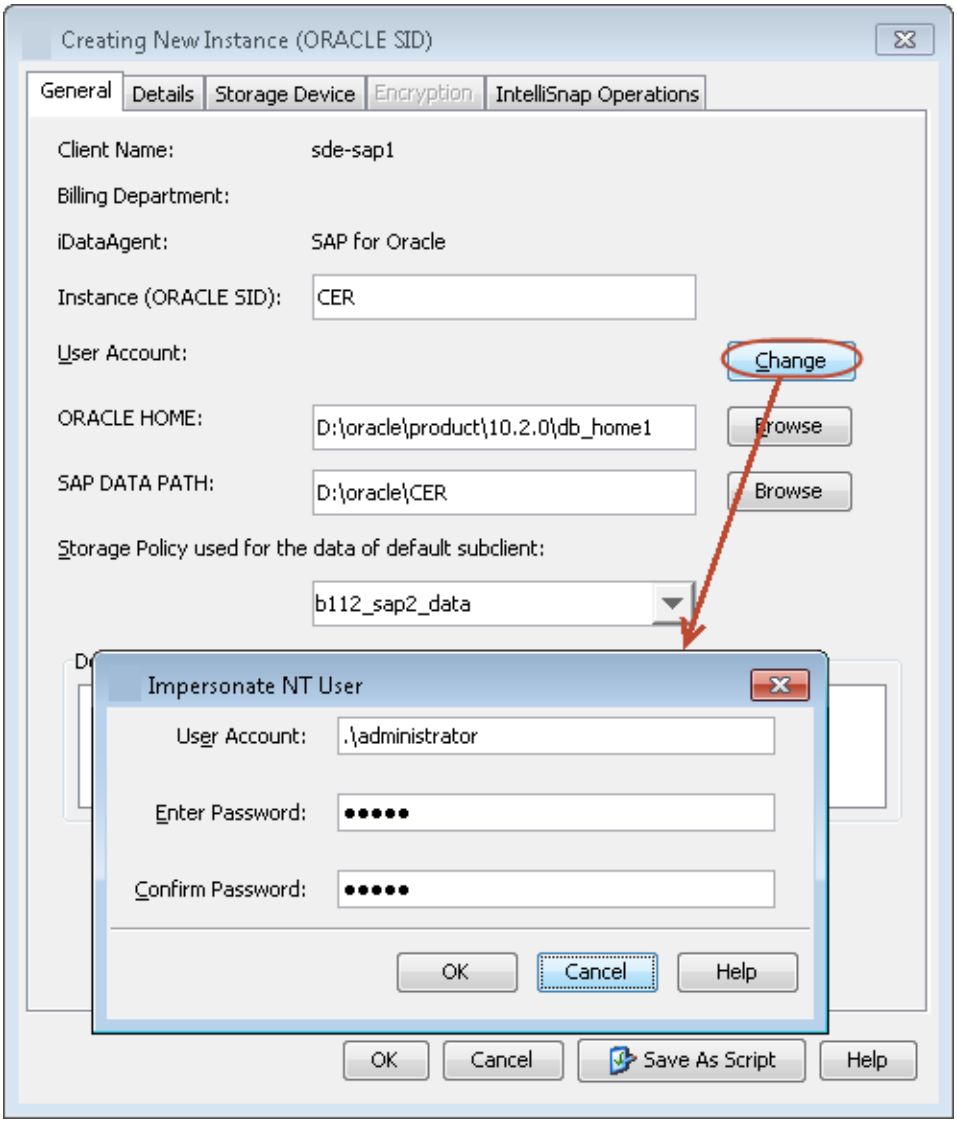
2. On Windows client:

- Enter the Instance Name.
- Click **Change**.
- In the **User Account** box, enter the user name to access the Oracle application.

Use <domainname>\<SID>adm, in order to perform backup and restore operations from CommCell Console for the associated instance.

Make sure that the user has administrator privileges to access the Oracle application.

- **Browse** or enter the path to the Oracle application files in **Oracle Home**.
- **Browse** or enter the path to the Oracle data and control files in **SAP DATA PATH**.
- Select a **Storage Policy** from the drop down list.



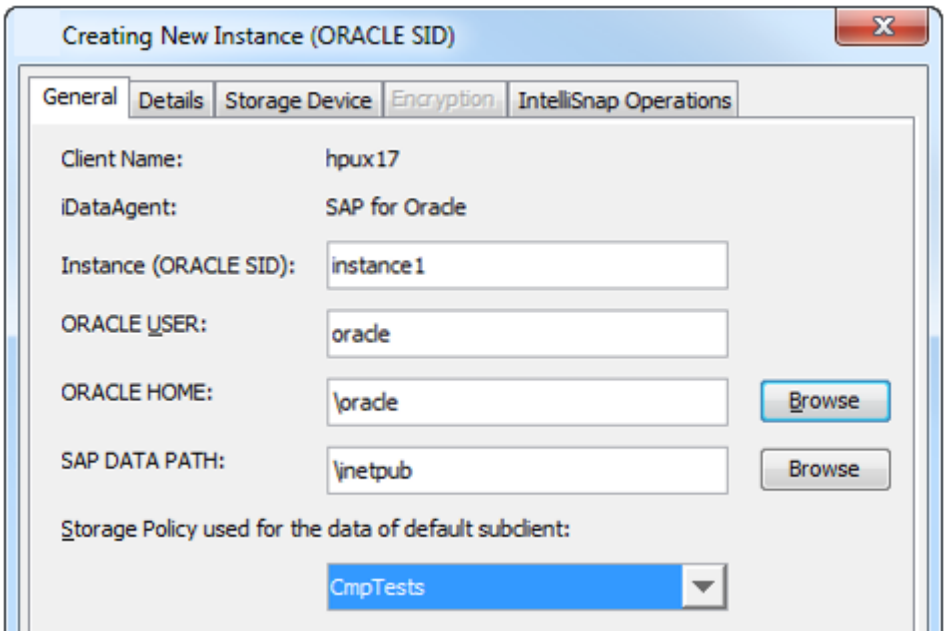
On UNIX Client:

- Enter the **Instance Name**.
- Enter the user name in **User Account** to access the Oracle application on a UNIX client.

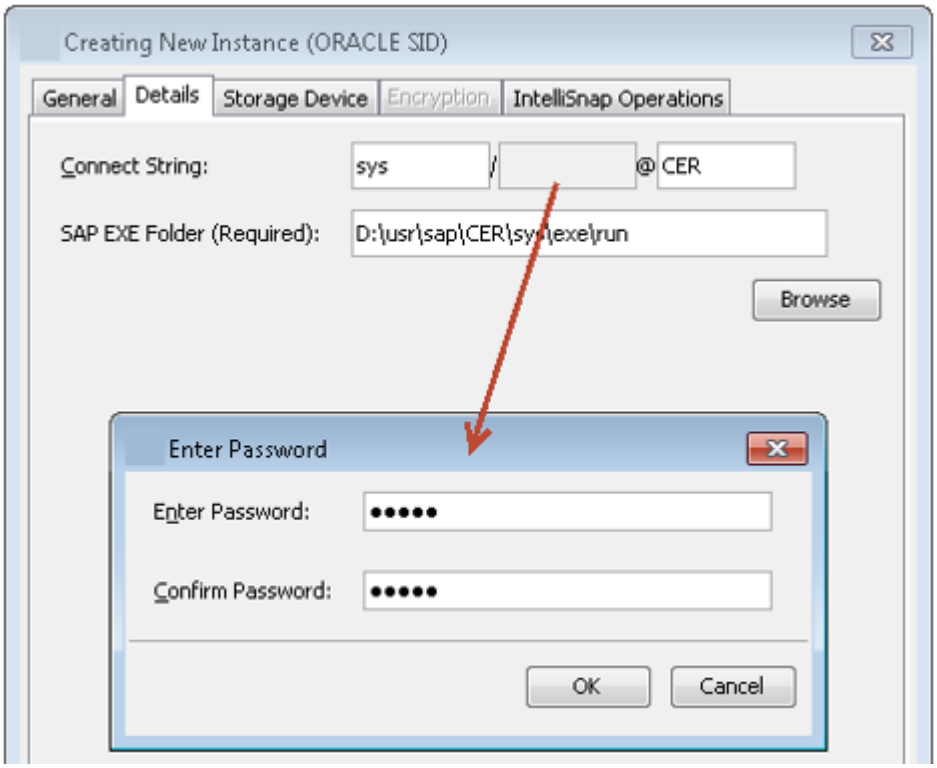
Use <SID_name>adm in order to perform backup and restore operations from CommCell Console for the associated instance.

Make sure that the user has administrator privileges to access the Oracle application.

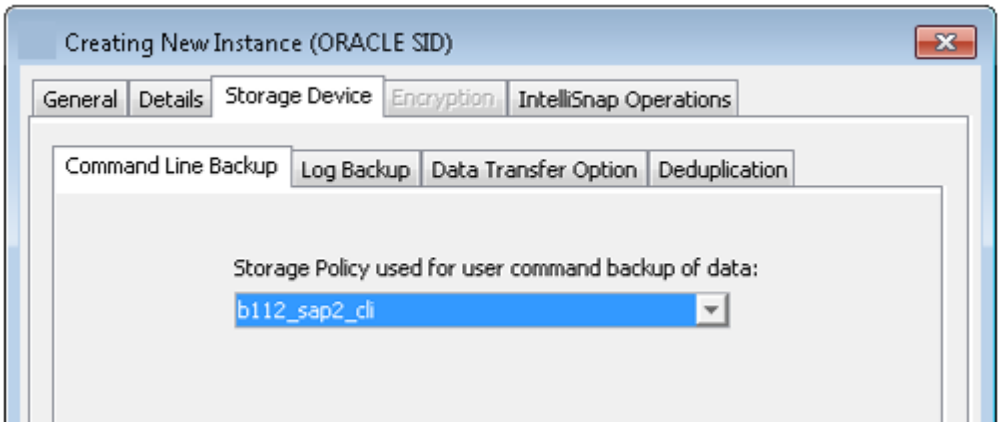
- **Browse** or enter the path to the Oracle application files in **Oracle Home**.
- **Browse** or enter the path to the Oracle data and control files in **SAP DATA PATH**.
- Select a **Storage Policy** from the drop down list.



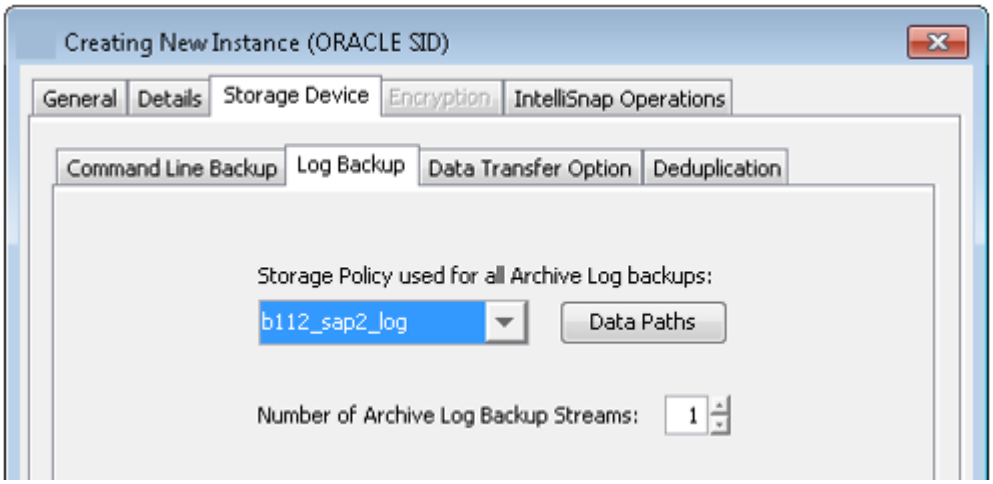
3. Click **Details** tab and add the following information:
   - Enter the target database connect string in **Connect String**.
   - **Browse** or enter the path to the SAP EXE folder in **SAP EXE Folder (Required)**.



4. Click the **Storage Device** tab.
   - In the **Storage Policy used for user command backup of data** box, select a storage policy name.



5. Click the **Logs Backup** tab.
   - In the **Storage Policy used for all Archive Log backups** box, select a storage policy name.
   - Click **OK**.



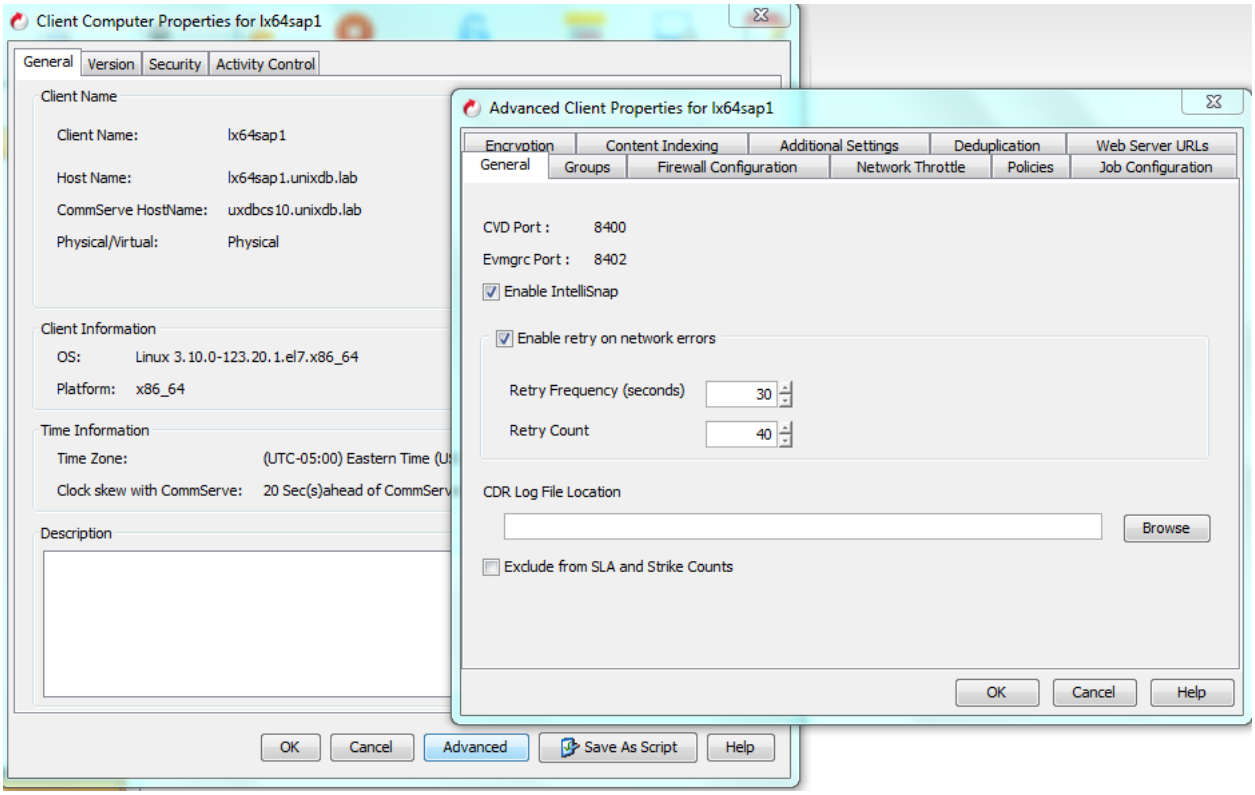
Please note: IntelliSnap can be enabled on the default subclient; however, best practice is to create a separate subclient when using IntelliSnap. This guide will describe the process for creating an IntelliSnap-enabled subclient.

SAP Oracle Client Configuration

Enable IntelliSnap on the SAP Oracle client object in the CommCell console.

- Right click on the server name, select All Tasks, and then select Properties.

Navigate to the advanced properties page and check the box marked Enable IntelliSnap. This will consume a Hardware Snapshot Enabler license from the license key.

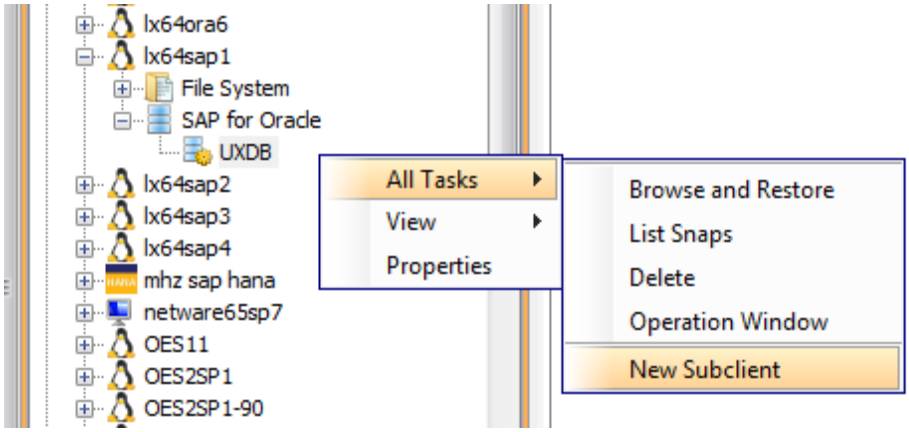


SAP Oracle Subclient Configuration

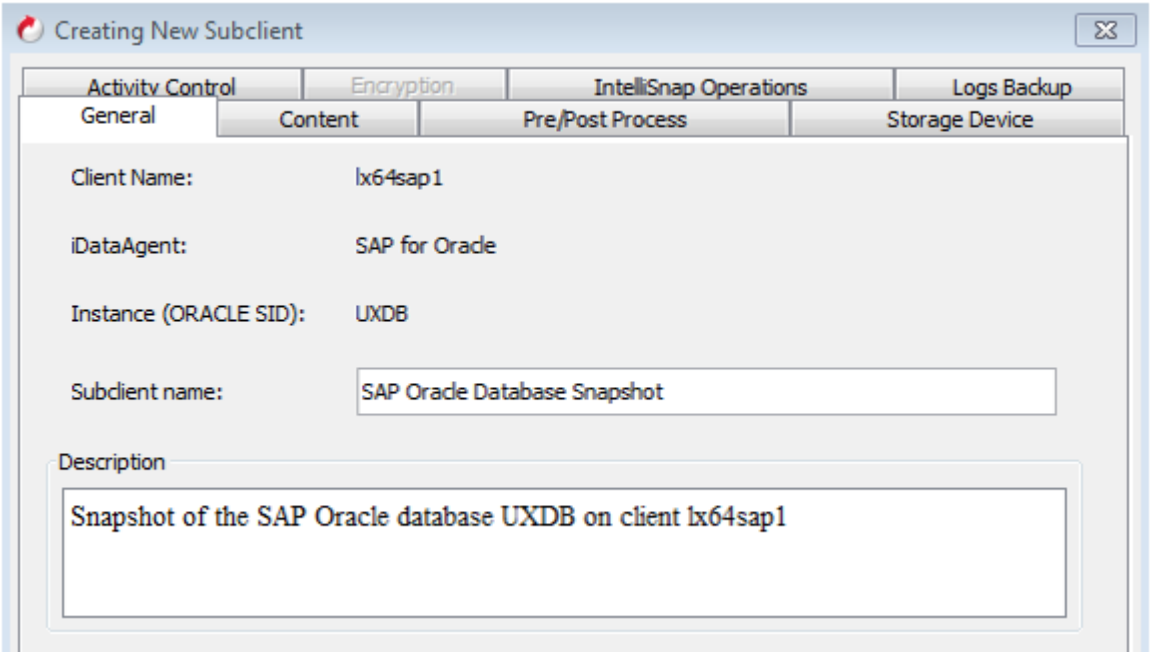
Once the SAP Oracle iDataAgent is installed on a client and the Oracle instance is defined, configure a Subclient to backup the SAP Oracle database and /or archive logs.

The following sections provide the necessary steps to configure a Subclient to perform the IntelliSnap backup of a single Oracle database:

1. From the CommCell Browser, right-click the SAP Oracle instance and select **All Tasks | New Subclient**:

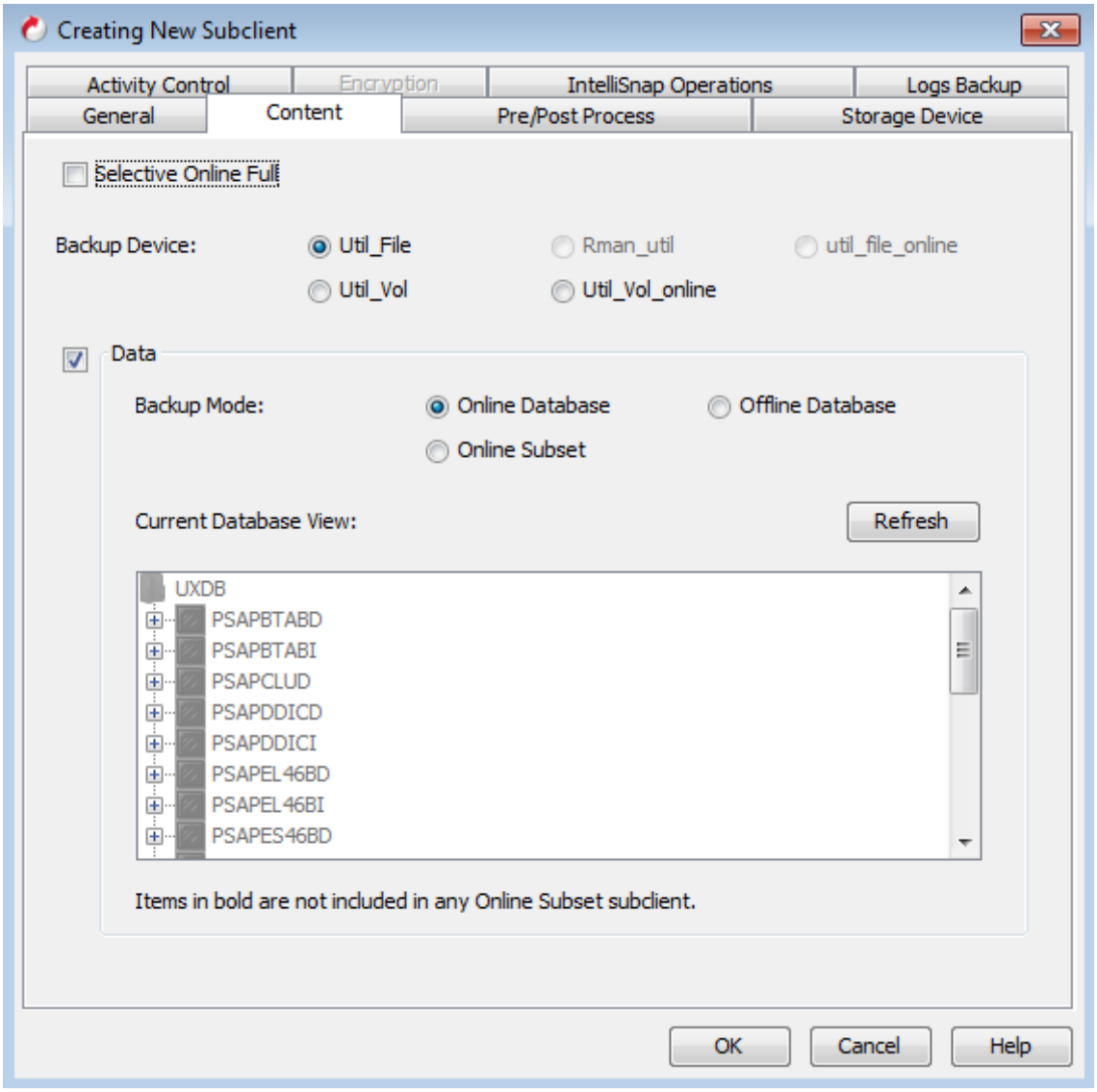


2. On the "**General**" tab, enter the name of the Subclient and, optionally, a user friendly description for the Subclient:

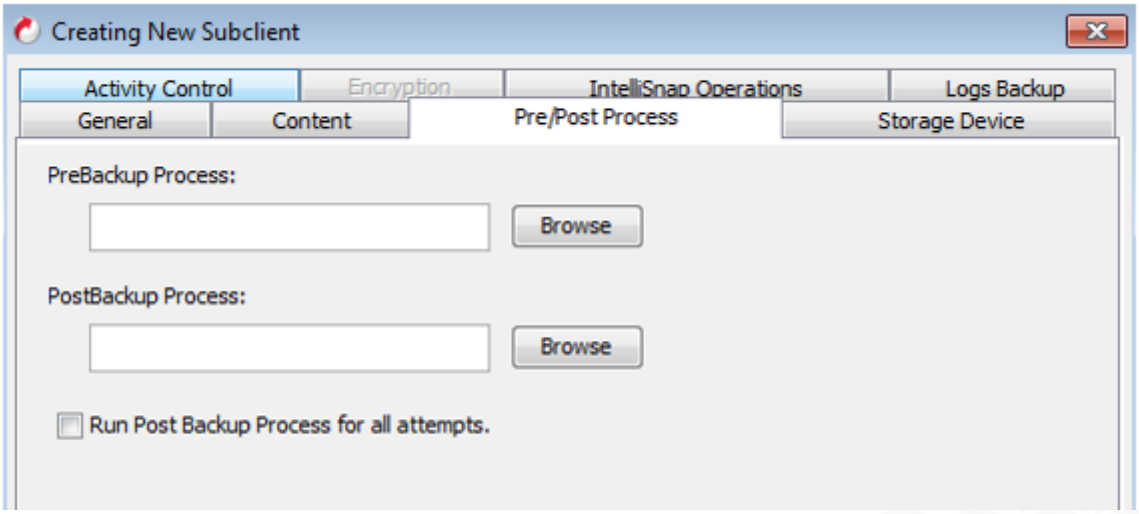


3. On the "**Content**" tab, select whether the backup will be Online or Offline. Also note that when the IntelliSnap option is selected, the only "Backup Device" options which are available are:

   - **Util_File** - Specifies that a backup is performed file-by-file using a backup program specified by the BACKINT interface.
   - **Util_Vol** - Specifies that a backup is performed at disk-volume level.
   - **Util_Vol_online** - Specifies that a backup is performed at disk-volume level with dynamic switching of tablespace backup status.
   - The Util_File is a default option when you select IntelliSnap Operations. However, you can select the option as per your requirement.
   - The Util_Vol, Util_Vol_online options will not be available in the following circumstances:
     - If the Snap is not setup
     - If the Snap Engine is DDR
     - If the BR*Tools version is below 7.10

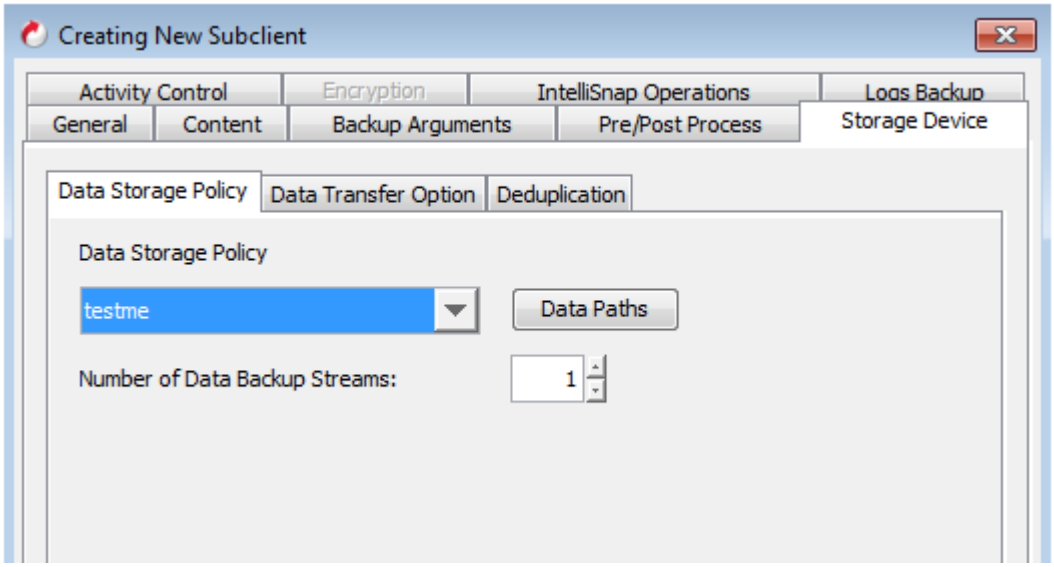


4. Optionally, on the "**Pre/Post Process**" tab, scripts may be called out to perform tasks during the operation, both pre/post snap and pre/post backup:



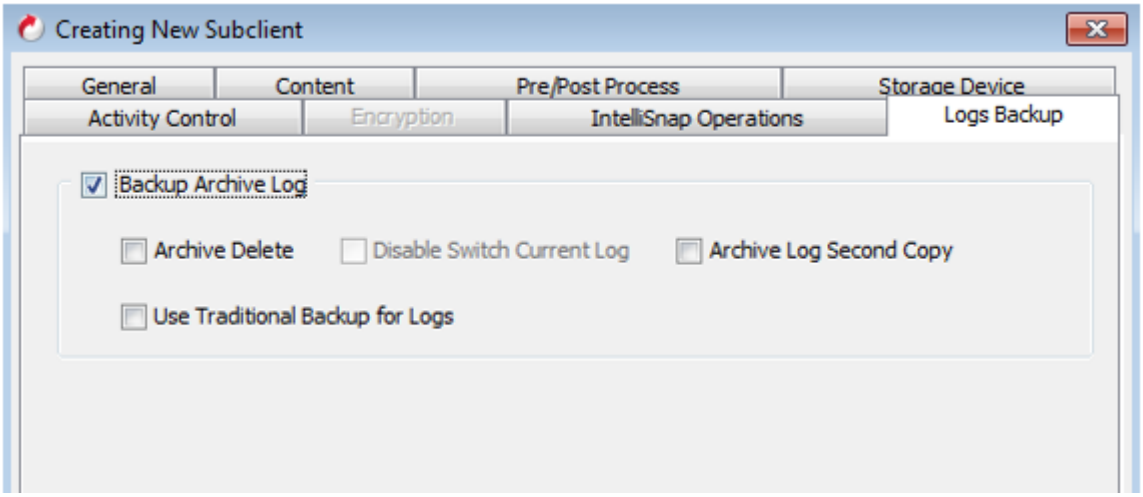
5. On the "**Storage Device**" tab, the storage policy is chosen and the number of streams is also configured. Compression

and deduplication option can also be optionally configured on Storage Device tab:

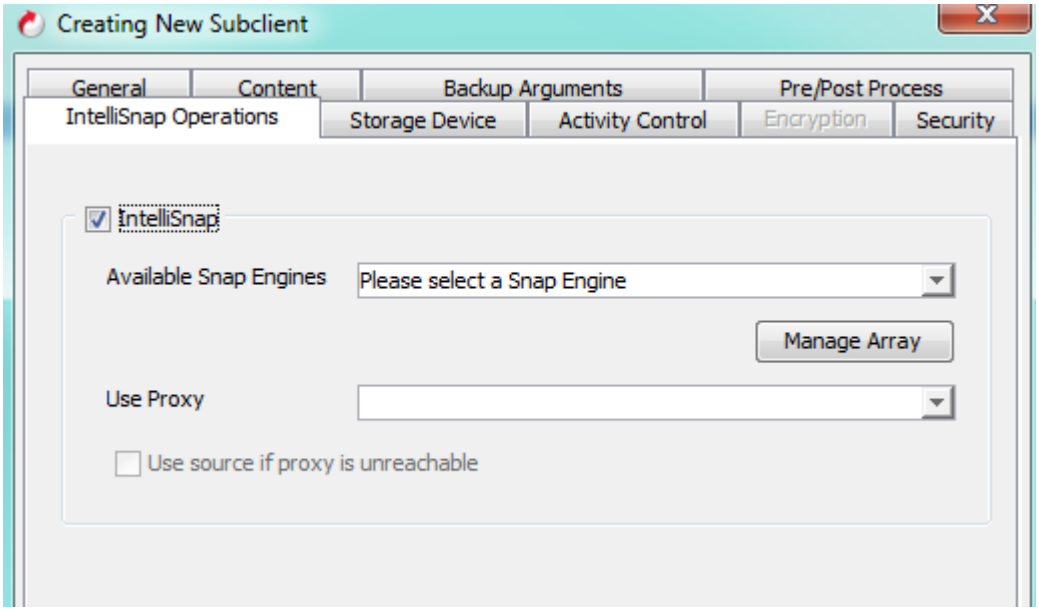


6. The "Logs Backup" tab contains the options for the SAP Oracle Archive Logs. Options include whether or not to backup the archive logs and if the logs are to be deleted after backup. By default, the logs are not deleted after an IntelliSnap backup. Deletion of the logs has to be enabled.

   When you perform an IntelliSnap backup for archive logs, you can specify the location for which an IntelliSnap operation should be performed. This capability enables you to schedule IntelliSnap operations from different log destinations on the same Subclient. If necessary, you can also delete the logs after an IntelliSnap backup.



7. The "**IntelliSnap Operations**" tab controls the snap options. Enable the IntelliSnap checkbox. Next select the appropriate snap engine from the Available Snap Engines dropdown pick list. If the use of a proxy is desired for backup copy operations, select the proxy from the **Use Proxy** dropdown pick list.



Note: When performing IntelliSnap software backup using proxy, ensure that the operating system of the proxy server is either same or higher version than the client computer.

By default, the backup copy uses the file system for copying data to the media. In this case, the Media Agent and File System iDataAgent must be installed on the proxy. By enabling the "Use RMAN for backup copy", the RMAN backup interface is used for block level backup operations. Also, these backup operations are recorded on the RMAN catalog. RMAN is required in the case of Automatic Storage Management (ASM) Oracle Databases, since ASM data is not available on the file system. You can also run RMAN restores/reports from these backups.

Prior to using RMAN for copying the data to the media, ensure the following:

- The Oracle iDataAgent and MediaAgent must be installed on the proxy computer.
- The Oracle instance on the proxy computer should have the same name as that in the source computer.
- The Oracle version installed on the proxy and source computers should be compatible. However, the major version of Oracle should be the same.
- For backups involving ASM instances, both ASM and the RDBMS instances have to be configured on the proxy computer.
- The catalog user and the catalog database must be the accessible by the source and the proxy Oracle instances.
- The proxy and source computer should have the same directory structure e.g. dump, diagnostic and data directories.
- Oracle database requires the ASM to be registered with Oracle Cluster Registry (OCR). It will ensure the RMAN to successfully mount the disk group.
- If multiple source client database instances are configured to run RMAN backup copy on the same proxy MediaAgent, the backup copy may fail due to instance and database name conflicts. The conflicting database and instances need to be moved to a different proxy MediaAgent in such cases

During an RMAN backup copy, the proxy database is started in mount mode using the backup control file from the IntelliSnap backup. Additional Oracle licenses may be required for the proxy database. Please inquire with Oracle support to determine if additional Oracle licenses are required in your environment.

The "Enable Snap Integrity Check" option is disabled by default. When enabled, the following additional steps are performed after taking the snapshot:

- The snapshot is mounted on the source and cataloging of datafiles/archived logs is performed from the mounted snapshot.

This verifies whether all the datafiles/archived logs are properly captured during an IntelliSnap backup. RMAN catalog datafilecopy checks the datafile header and verify its authenticity before cataloging it.

- Once the catalog is completed, an uncatalog happens and the snapshot is unmounted from the source.

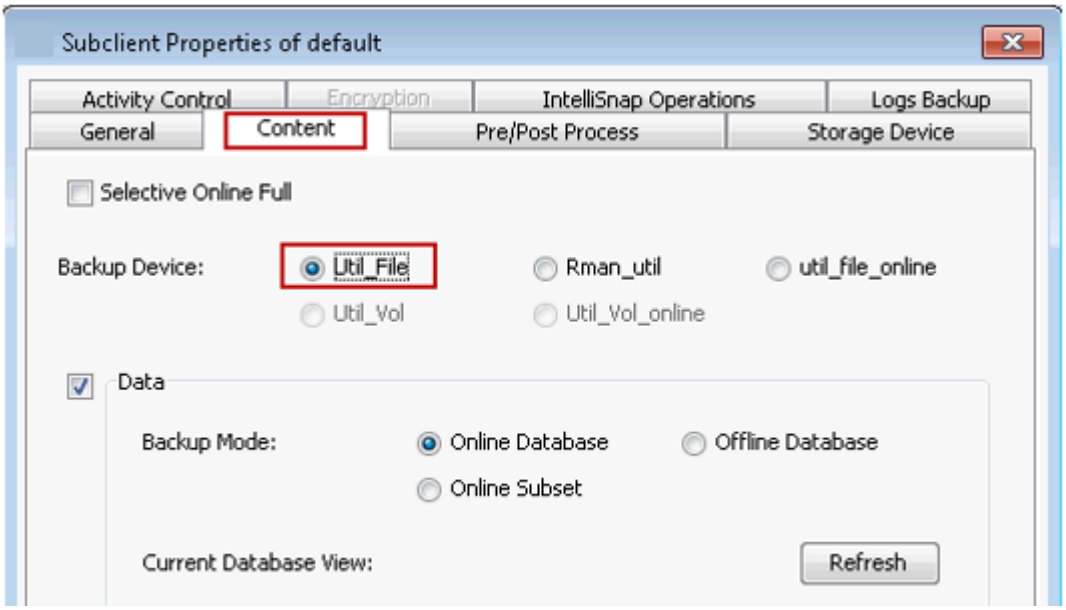
SAP Oracle IntelliSnap and Backup Copy

An SAP Oracle IntelliSnap backup utilizes one of the following SAP backup devices:

Util_File

The util_file interface is used when you need to perform a full backup or a selective online full backup operation. When selecting this option for online backup, the Oracle database is locked till the full backup operation is completed.

1. From the CommCell Browser, right-click the **Subclient** and click **Properties**.
   - Click **Content** tab.
   - Select **util_file** to perform a full backup of SAP for Oracle data.
   - Click **OK** to save your settings.

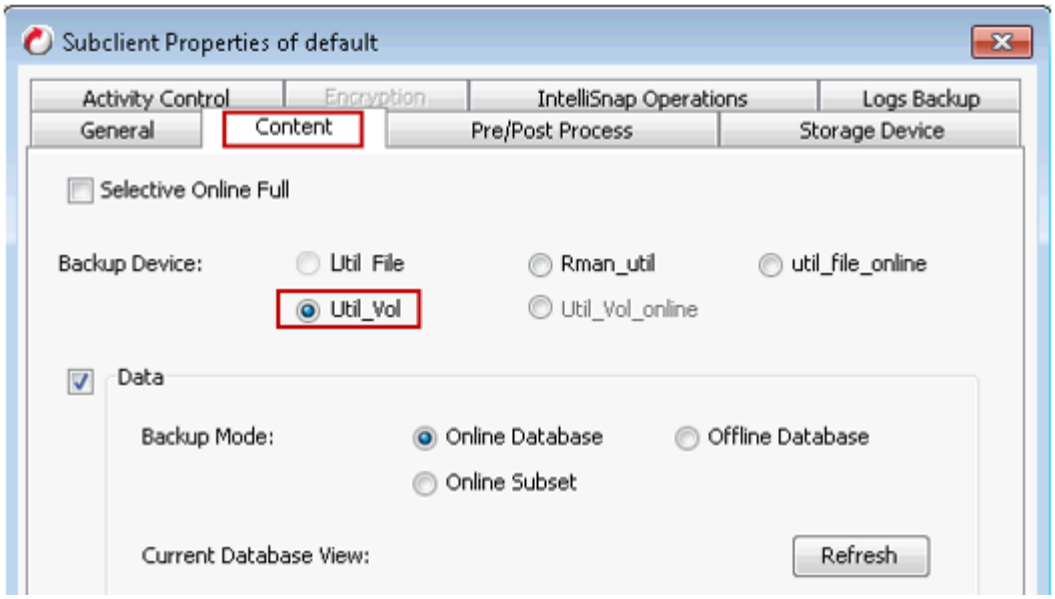


Util_Vol

When you perform backups using the util_vol backup interface, the entire database is locked till the backup operation is completed.

Use the following steps to configure backups using util_vol backup interface:

1. From the CommCell Browser, navigate to **<Client> | SAP for Oracle | <Instance>**
2. Right-click the Subclient and click **Properties**.
3. Click **Content** tab.
4. Select **util_vol** to perform a backup operation.
5. Click **OK** to save your settings.

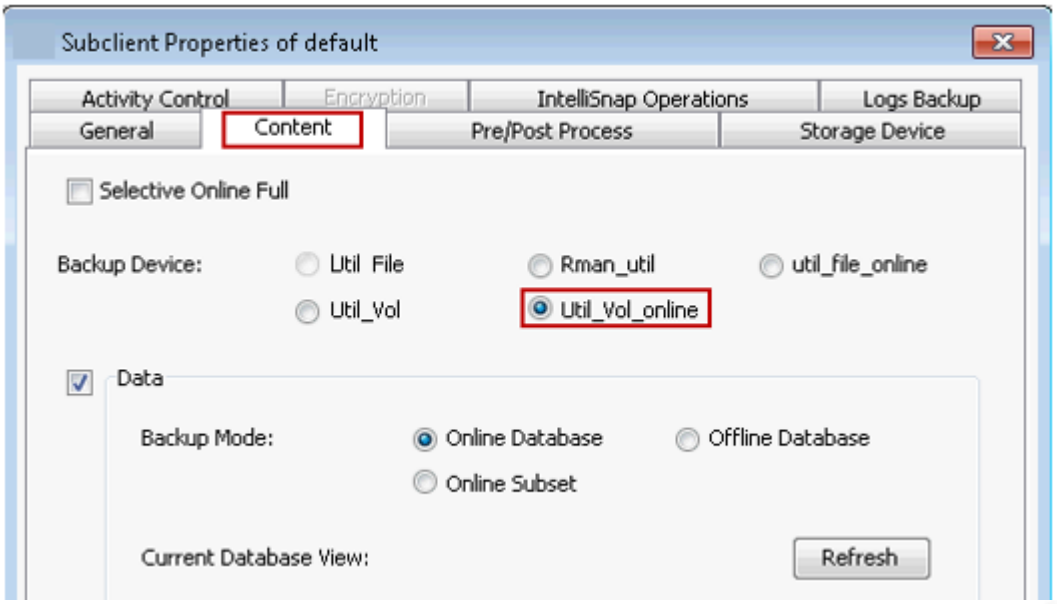


Util_Vol_Online

The util_vol_online backups are similar to the util_vol backups. However, when using these type of backups, each volume that is being backed up is locked during the backup and is released once the backup is completed.

Use the following steps to configure backups using util_vol_online backup interface:

1. From the CommCell Browser, navigate to **<Client> | SAP for Oracle | <Instance>**
2. Right-click the Subclient and click **Properties**.
3. Click **Content** tab.
4. Select **util_vol_online** to perform a backup operation.
5. Click **OK** to save your settings.

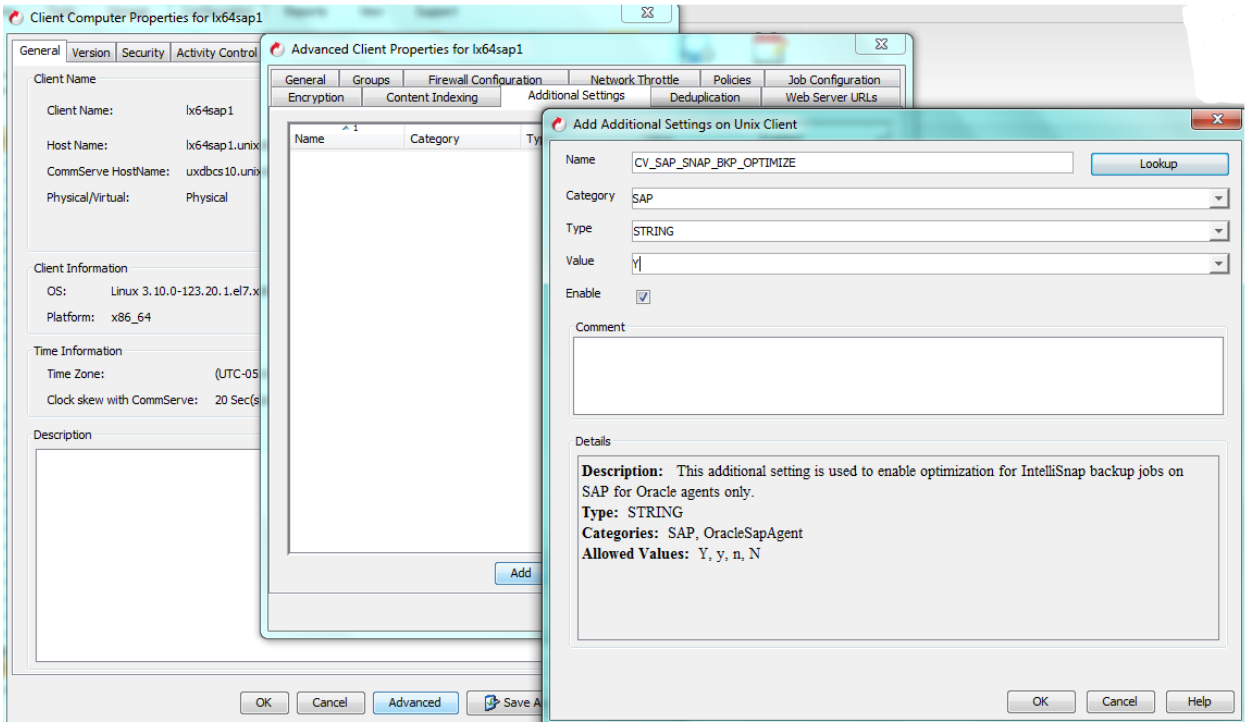


Optimizing IntelliSnap® Backup

Each IntelliSnap backup job snaps many volumes that are used for data, archive logs, detail and summary files, database init files etc. A large number of IntelliSnap backup jobs can quickly consume the snap data reserve. To overcome this, use the CV_SAP_SNAP_BKP_OPTIMIZE additional setting to reduce the total number of snapshots per job.

Follow these steps to enable snapshot optimization:

1. From the CommCell Browser, navigate to **Client Computers**.
2. Right-click the **<Client>** to be configured and then click **Properties**.
3. Click **Advanced**.
4. Click the **Additional Settings** tab and then click **Add**.
5. In the **Name** field, type CV_SAP_SNAP_BKP_OPTIMIZE.
6. In the **Value** field, type **Y**.
7. Click **OK** to save the key.
8. Click **OK**.



IntelliSnap® Backup for SAP Split-Mirror Disks (Splitint Support)

You can perform IntelliSnap backups on the SAP Oracle database files of the split-mirror disks. You must perform these backups on a backup (proxy) server instead of a production server using BRBACKUP tool through the Splitint Interface. This will allow you to offload your production server from data protection operations as these operations are now moved and performed on the proxy server. You can control the splitting and synchronization of the split-mirror disks using BRBACKUP. BRBACKUP also communicates with the production database to obtain the information about the database structure and stores all results of the backups. This process allows the Computing Center Management System (CCMS) to monitor the backups in the SAP production system.

You can use the backint util_file interface to perform an IntelliSnap backup of the split-mirror disks on the production server. Later, you can even mount these snapshots on the proxy or production server and copy any data file needed. You can also

perform restores on the production or proxy server either from the snapshots or the snap copies depending upon the selected copy precedence.

Configuring BRBACKUP for Split-Mirror Disk Backups

You must configure a SAP Oracle instance for both the source and proxy client. You must configure the following on the production and proxy servers before performing split-mirror disk backups using BRBACKUP:

1. We would need to create the SAP Instance from CommCell GUI for both Source and Proxy client. Install the Oracle SID on both the production and proxy servers. Make sure to install the same Oracle SID and maintain the same directory structure on both the production and proxy servers.

   - Add the following parameter:

```
$ORACLE_HOME/dbs/init<SID>.utl file:

CvSrcClient

<Source_Client_Name>
```

   Example:

```
Production=tigersnap
Proxy=tigersnap2
$ORACLE_HOME/dbs/init<SID>.utl file on the Proxy
CvSrcClient
tigersnap
```

2. Configure the Snap-able volumes on the production server.

   Example:

```
[root@tigersnap ~]# df -k
Filesystem 1K-blocks Used Available Use% Mounted on
/dev/mapper/VolGroup00-LogVol00
32408432 30528060 207568 100% /
/dev/sda1 101086 14827 81040 16% /boot
tmpfs 972264 0 972264 0% /dev/shm
/dev/sdj1 1031888 17736 961736 2% /home/oracle/product/10g/dbs
/dev/sdg1 5156292 1373028 3521336 29% /home/oracle/product/10g/CER
/dev/sdh1 3093976 831496 2105312 29% /home/oracle/product/10g/CER/DATA
/dev/sde1 2062716 118036 1839900 7% /home/oracle/product/10g/CER/LOG
[root@tigersnap ~]# ls -l /home/oracle/product/10g/CER
total 48
drwxrwx--- 9 oracle oracle 4096 Apr 27 17:52 DATA
drwxrwx--- 7 oracle oracle 4096 May 29 16:34 LOG
drwxrwxrwx 2 oracle oracle 16384 Apr 27 10:56 lost+found
drwxrwxr-x 3 oracle oracle 4096 May 30 02:00 saparch
drwxrwxr-x 2 oracle oracle 4096 May 29 16:37 sapbackup
drwxrwxr-x 2 oracle oracle 4096 Apr 27 11:13 sapcheck
drwxrwxr-x 2 oracle oracle 4096 Apr 30 11:11 sapreorg
drwxrwxr-x 3 oracle oracle 4096 Apr 27 11:13 sapscripts
drwxrwxr-x 4 oracle oracle 4096 Apr 27 11:13 saptrace
[root@tigersnap ~]# ls -l /home/oracle/product/10g/CER/LOG
total 76
drwxrwxr-x 2 oracle oracle 4096 May 29 16:34 mirrlogA
drwxrwxr-x 2 oracle oracle 4096 May 29 16:34 mirrlogB
-rw-r----- 1 oracle oracle 2560 Oct 22 2010 orapwCER
drwxrwx--- 2 oracle oracle 4096 May 29 16:34 origlogA
drwxrwx--- 2 oracle oracle 4096 May 29 16:34 origlogB
-rw-r----- 1 oracle oracle 2560 May 29 11:59 orapwCER
[root@tigersnap ~]#
```

3. Configure the volumes on the proxy server. Make sure that the data, logs, control files and the mirror are configured on separate volumes. This is to ensure that the sapbackup directory on the proxy is not replaced when you mount the snapshots /split-mirror disks on the proxy server.

4. Configure the SSH with user equivalence (RSA Key sharing) between OraSID's on both the proxy server and production server. If you do not configure the SSH sharing, you will be prompted for the account passwords multiple times.

   You should meet the following User equivalency requirements:

   - You should have the same user name, UID and password on both the production and proxy servers.
   - You should belong to the same group with the same group ID.

   Make sure you get the same results on the production and the proxy:

   Example:

```
[oracle@tigersnap 10g]$ id oracle
uid=501(oracle) gid=501(oracle) groups=501(oracle),502(dba)
[oracle@tigersnap2 10g]$ id oracle
uid=501(oracle) gid=501(oracle) groups=501(oracle),502(dba)
```

5. Configure the Oracle Parameters on SID of both the production and proxy servers. Setup *.ora, *.sap, *.utl parameters on both the Production and Proxy servers.

6. Configure the TNS names on the production and proxy servers.

   Example:

```
[oracle@tigersnap admin]$ pwd
/home/oracle/product/10g/network/admin
[oracle@tigersnap admin]$ more tnsnames.ora
# tnsnames.ora Network Configuration File:
/home/oracle/product/10g/network/admin/tnsnames.ora
# Generated by Oracle configuration tools.

ORCL =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = tigersnap.commvault.com)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = orcl)
)
)

CER =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = tigersnap.commvault.com)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = CER)
)
)

CER.tigersnap =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = tigersnap.commvault.com)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = CER)
)
)
```

```
CER.tigersnap2 =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP)(HOST = tigersnap2.commvault.com)(PORT = 1521))
(CONNECT_DATA =
(SERVER = DEDICATED)
(SERVICE_NAME = CER)
)
)

EXTPROC_CONNECTION_DATA =
(DESCRIPTION =
(ADDRESS_LIST =
(ADDRESS = (PROTOCOL = IPC)(KEY = EXTPROC1))
)
(CONNECT_DATA =
(SID = PLSExtProc)
(PRESENTATION = RO)
)
)
```

7. Add the service name entries on the production server.

   Example:

```
[oracle@tigersnap 10g]$ lsnrctl stop
LSNRCTL for Linux: Version 10.2.0.1.0 - Production on 06-OCT-2011 03:00:02
Copyright (c) 1991, 2005, Oracle. All rights reserved.
Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC1)))
The command completed successfully

[oracle@tigersnap 10g]$ sqlplus "/ as sysdba" SQL*Plus: Release 10.2.0.1.0 -
Production on Thu Oct 6 03:00:13 2011
Copyright (c) 1982, 2005, Oracle. All rights reserved.
Connected to:
Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 - Production
With the Partitioning, OLAP and Data Mining options
SQL> shutdown immediate;
Database closed.
Database dismounted.
ORACLE instance shut down.
SQL> startup nomount
ORACLE instance started.
Total System Global Area 88080384 bytes
Fixed Size 1217836 bytes
Variable Size 79694548 bytes
Database Buffers 4194304 bytes
Redo Buffers 2973696 bytes
SQL> show parameters service_names
NAME TYPE VALUE
------------------------------------ ----------- ------------------------------
service_names string CER
SQL> alter system set service_names='CER,CER.tigersnap'
2 ;
System altered.

SQL> show parameters service_names;
NAME TYPE VALUE
------------------------------------ ----------- ------------------------------
service_names string CER,CER.tigersnap
SQL> shutdown immediate
```

```
ORA-01507: database not mounted
ORACLE instance shut down.
SQL> startup
ORACLE instance started.
Total System Global Area 88080384 bytes
Fixed Size 1217836 bytes
Variable Size 79694548 bytes
Database Buffers 4194304 bytes
Redo Buffers 2973696 bytes
Database mounted.
Database opened.
SQL> quit
Disconnected from Oracle Database 10g Enterprise Edition Release 10.2.0.1.0 -
Production
With the Partitioning, OLAP and Data Mining options

[oracle@tigersnap 10g]$ lsnrctl start

LSNRCTL for Linux: Version 10.2.0.1.0 - Production on 30-MAY-2012 21:12:37

Copyright (c) 1991, 2005, Oracle. All rights reserved.

Starting /home/oracle/product/10g/bin/tnslsnr: please wait...

TNSLSNR for Linux: Version 10.2.0.1.0 - Production
System parameter file is /home/oracle/product/10g/network/admin/listener.ora
Log messages written to /home/oracle/product/10g/network/log/listener.log
Listening on: (DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1)))
Listening on:
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=tigersnap.commvault.com)(PORT=1521)))

Connecting to (DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=EXTPROC1)))
STATUS of the LISTENER
------------------------
Alias LISTENER
Version TNSLSNR for Linux: Version 10.2.0.1.0 - Production
Start Date 30-MAY-2012 21:12:39
Uptime 0 days 0 hr. 0 min. 0 sec
Trace Level off
Security ON: Local OS Authentication
SNMP OFF
Listener Parameter File /home/oracle/product/10g/network/admin/listener.ora
Listener Log File /home/oracle/product/10g/network/log/listener.log
Listening Endpoints Summary...
(DESCRIPTION=(ADDRESS=(PROTOCOL=ipc)(KEY=EXTPROC1)))
(DESCRIPTION=(ADDRESS=(PROTOCOL=tcp)(HOST=tigersnap.commvault.com)(PORT=1521)))
Services Summary...
Service "CER" has 1 instance(s).
Instance "CER", status UNKNOWN, has 1 handler(s) for this service...
Service "PLSExtProc" has 1 instance(s).
Instance "PLSExtProc", status UNKNOWN, has 1 handler(s) for this service...
The command completed successfully
[oracle@tigersnap 10g]$
```

8. Configure the InitSID.* on the Production server.
   - Add the following to initCER.sap

```
RMAN_PARMS="BLKSIZE=1048576,SBT_LIBRARY=/opt/simpana2/Base/libobk.so,
ENV=(CvClientName=tigersnap,CvInstanceName=instance001)"
_rman_sess_stmt = ("alter session set optimizer_mode=RULE")
```

- Add the following to initCER.ora

```
remote_login_passwordfile = EXCLUSIVE
control_file_record_keep_time = 100
```

- Add the following to initCER.utl

```
CvInstanceName
Instance001
snapBackup
1
numstreams
1
CV_restCopyPrec
0
```

9. Configure the InitSID.* on the Proxy server.

- Add the following to initCER.sap

```
primary_db = CER.tigersnap
stage_copy_cmd = scp
pipe_copy_cmd = ssh
rman_channels = 1
rman_filesperset = 64
```

For example:

```
RMAN_PARMS="BLKSIZE=1048576,SBT_LIBRARY=/opt/simpana2/Base/libobk.so,
ENV=(CvClientName=tigersnap2,CvInstanceName=instance001,CvSrcClient=tigersnap)"
_rman_sess_stmt = ("alter session set optimizer_mode=RULE")
```

- Add the following to initCER.ora

```
control_file_record_keep_time = 100
```

- Add the following to initCER.utl

```
CvInstanceName
Instance001
snapBackup
0
numstreams
1
```

10. The Snapshots/Split-mirror disks will be mounted (in place) on the proxy server. Make sure that those pertinent directories are empty on the proxy.
11. Install the SAP Oracle iDataAgent on both the production and proxy servers.
12. Configure the instance for the production server in the CommCell Console. See Configuration for step-by-step instructions on how to configure an instance.

Additional Configuration Required for Offline Mirror on the Production Server:

1. Create an Oracle password file using the following command.

```
orapwd file=<ORACLE_HOME>/dbs/orapw<DBSID> password=<SYS password> entries=10
```

For example:

```
oracle@tigersnap 10g]$ orapwd file=/home/oracle/product/10g/dbs/orapwCER
password=manager entries=10 force=Y
```

2. Configure the remote_login_passwordfile parameter to exclusive in the init<DBSID>.ora profile.
3. Authorize the system user with SYSOPER authorization in the production server.
4. Start the SQLPLUS as user SYS and execute the Oracle command:

```
If needed, change the password for the system user.

SQL> connect / as sysdba SQL> grant sysoper to system;
```

Changing the password for the system user:

```
SQL> alter user system identified by <password>;
```

Performing Split-Mirror Disk Backups Using BRBACKUP

Use the BRBACKUP tool through Splitint interface on the proxy server instead of production server with either an online_mirror or offline_mirror for performing split-mirror disk backups. Use the util_file interface to perform these backups.

- Use the following BRBACKUP command to perform split-mirror disk backups with online_mirror using util_file interface:

```
brbackup -d util_file -t online_mirror -m all -c
```

- Use the following BRBACKUP command to perform split-mirror disk backups with offline_mirror using util_file interface:

```
brbackup -d util_file -t offline_mirror -m all -c
```

IntelliSnap® Backup on NFS Volume

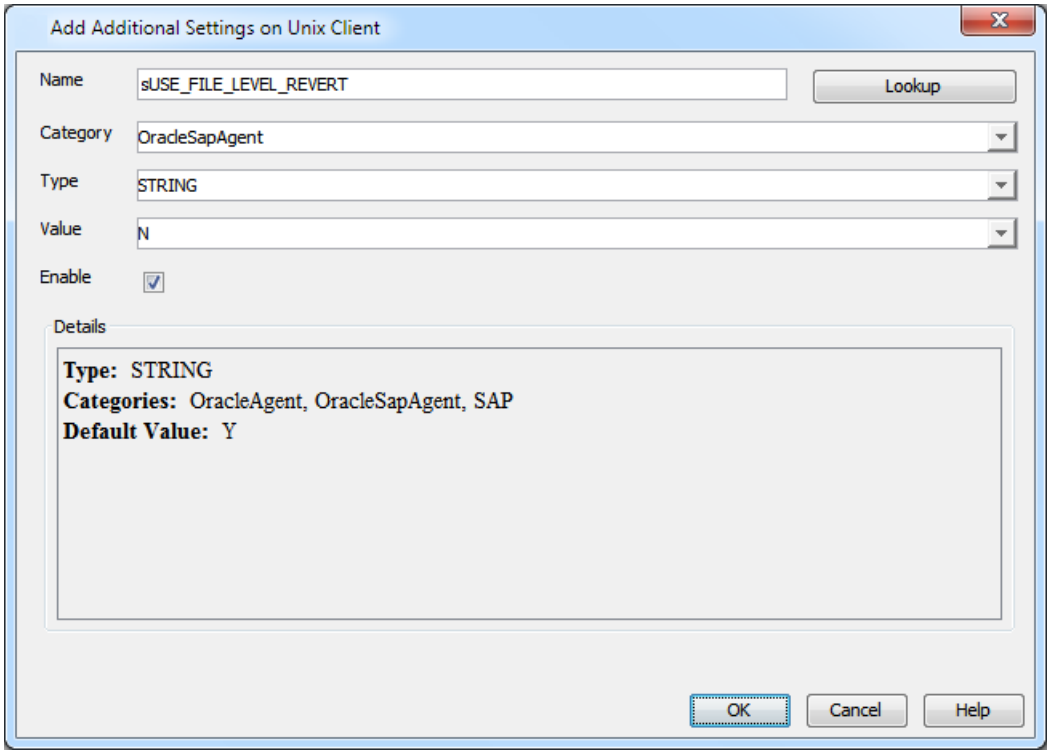
You can perform IntelliSnap backup of SAP for Oracle when the database is on a NFS Volume. However, you will require a root access in the storage device's NFS configuration to be able to read and write on the accessible SAP for Oracle files i.e., the host on which the NFS Volume is mounted.

You can also perform IntelliSnap backup of SAP for Oracle if the database resides on a Direct NFS volume. IntelliSnap backup supports volumes using the Oracle Direct NFS (dNFS) protocol.

File level revert is performed by default when revert restore is run on NFS volumes. For Volume Level revert on NFS volumes, use the sUSE_FILE_LEVEL_REVERT registry key. File level revert cannot be performed when the database resides on regular SAN Volumes (LUNs).

Consider the following while performing an IntelliSnap backup for data or databases that reside on an NFS Volume:

- The export name on the storage device should be the same as the storage path on the storage device.
- E.g., if the storage path of the storage device is /vol/Volume/Qtree, use /vol/Volume/Qtree as the export name and not an alias such as /ExportName.
- You can use the exports both at the root of a NetApp volume and at subdirectory levels below the root of the volume.
- Make sure that the storage device is accessible from the source and proxy machine (even if they exist in different domains) using the storage device's short name while mounting NFS exports from the storage device. Make sure to enter the storage device credentials using its short name. Do not use an IP address or the fully qualified domain name.
    - E.g., use a short name for the server such as server1 or server2.



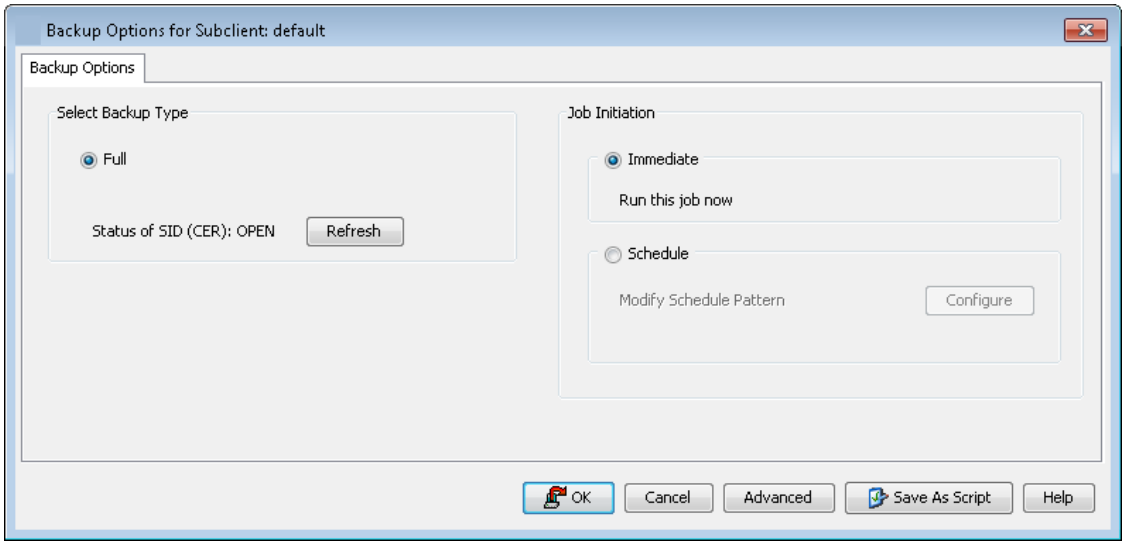
Backup Copy Operations

A backup copy operation provides the capability to copy snapshots of the data to any media. It is useful for creating additional standby copies of data and can be performed during the IntelliSnap backup or at a later time. Note that if primary snap copy is configured as Spool copy (copy with no retention rules) then the snapshots will be automatically deleted after the backup copy operation completes successfully.

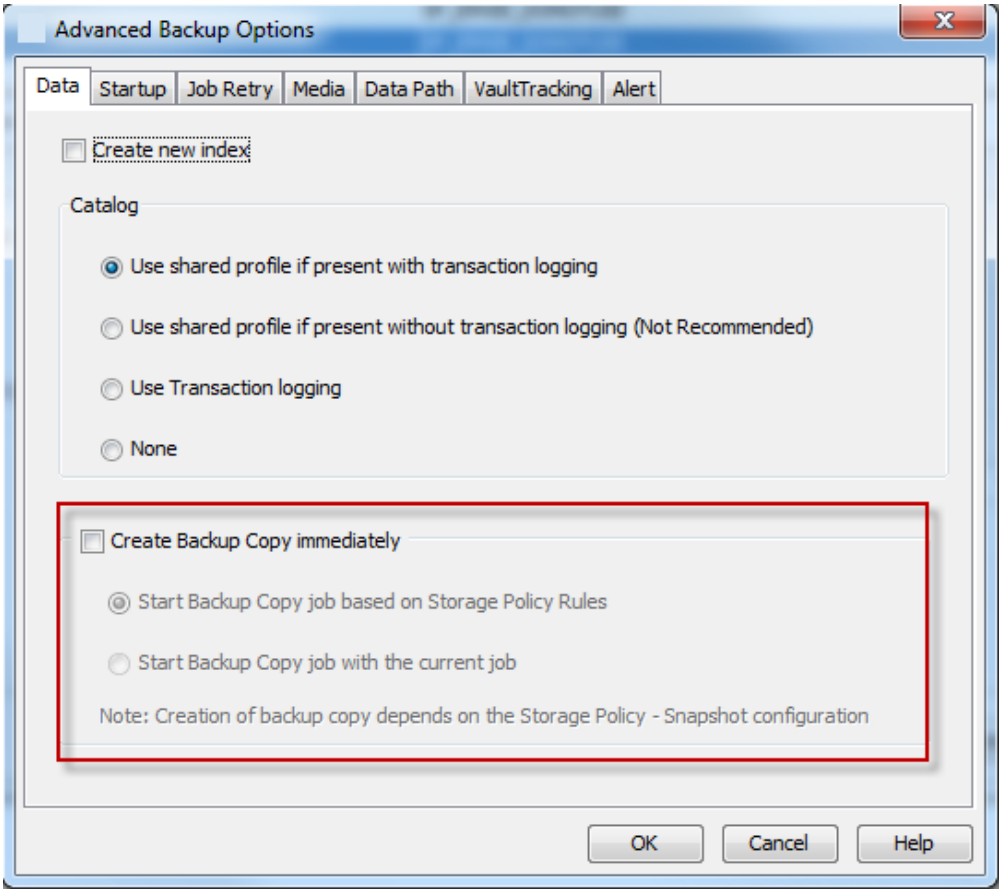
Inline Backup Copy

Backup copy operations performed during the IntelliSnap backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current IntelliSnap job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

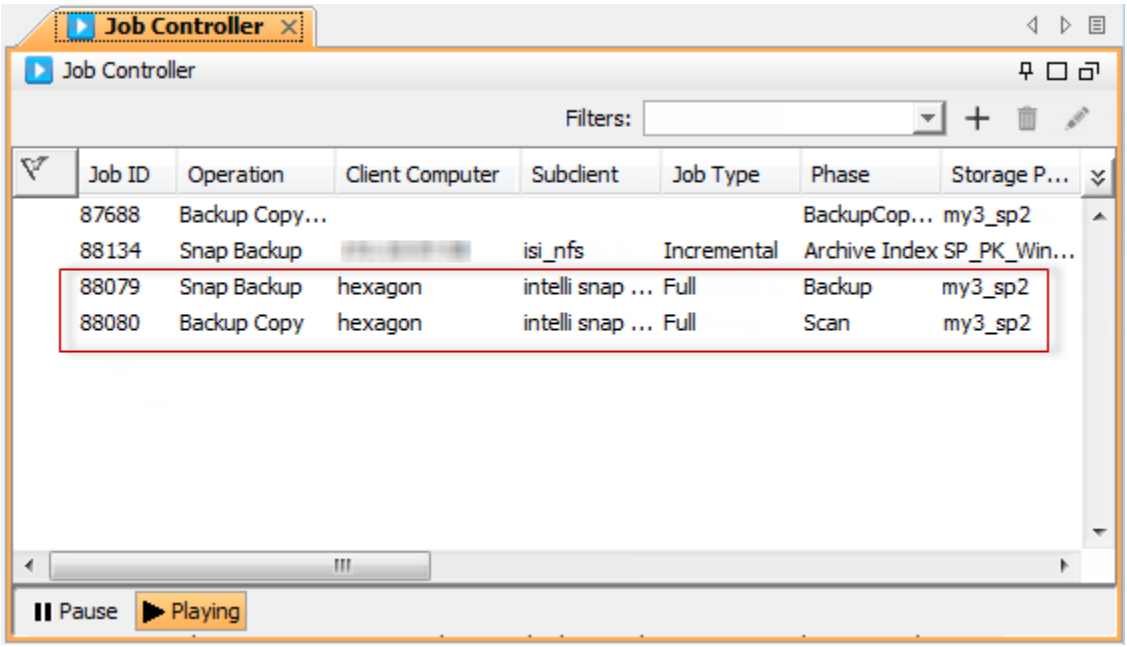
1. From the CommCell Console, navigate to Client Computers | <Client> | <Agent> | <Instance>
2. Right click the default Subclient and click Backup.
3. Select Full as backup type.
4. Click Advanced.



5. From the **Advanced Backup Options** dialog box, select **Create Backup Copy** immediately check box to create a backup copy.
   - Click OK.



6. You can track the progress of the Inline Backup Copy job from the Job Controller window. When job is initiated, two separate jobs (i.e., Snap Copy job and Backup Copy job) will be displayed in the Job Controller window.

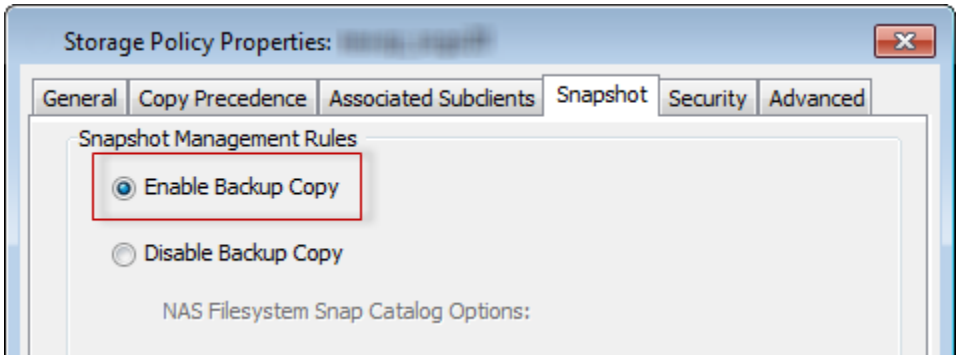


Offline Backup Copy

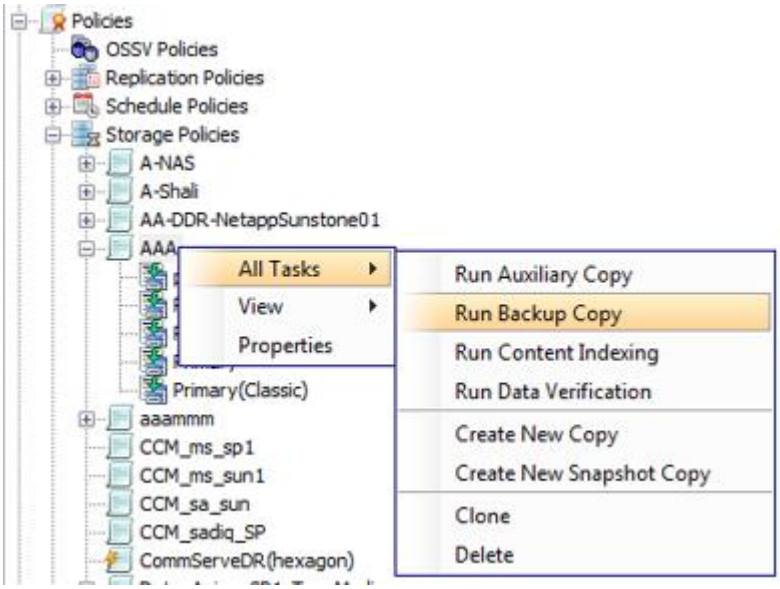
Backup copy operations performed independent of the IntelliSnap backup job are known as offline backup copy.

Use the following steps to run offline backup copy.

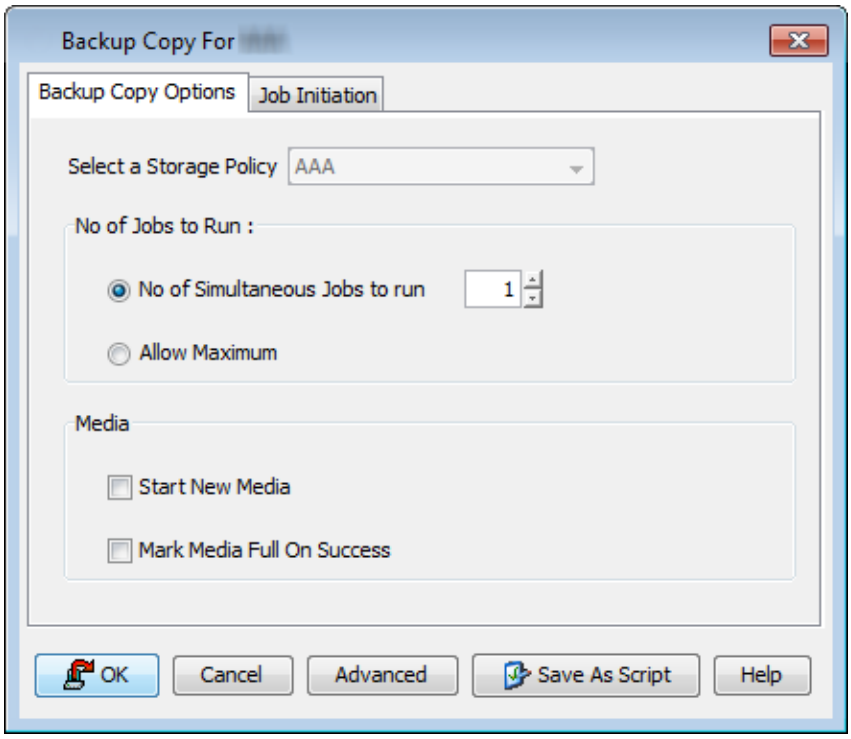
1. From the CommCell Console, navigate to **Policies | Storage Policies**.
2. Right-click the **<storage policy>** and click **Properties**.
3. Click the **Snapshot** tab.
4. Under **Snapshot Management** Rules, make sure that **Enable Backup Copy** is selected.
5. Click **OK**.



6. From the CommCell Console, navigate to **Policies | Storage Policies**.
7. Right-click the **<storage policy>** and click **All Tasks | Run Backup Copy**.



8. Select **Start New Media** to copy the data to a different tape.
9. Select **Mark Media Full On Success** to mark the media that is used for this operation after the snapshot copy operation has successfully completed.
10. Click **OK**.



DB2 Configurations

IntelliSnap backup enables you to create a point-in-time snapshot of the data used for backups. An effective way to back up live data is to quiesce it temporarily, take a snapshot, and then resume live operations. IntelliSnap backup works in conjunction with storage arrays to provide snapshot functionality for backup.

You can use the IntelliSnap backup to perform a Full Backup. While performing an IntelliSnap backup or any subsequent operations, you can use a proxy server to reduce the load on the production server. Also, the backup copy operation will use the proxy to move the snap to backup media. Proxy server is supported with hardware storage arrays.

The IntelliSnap backup includes the following operations:

Backup job is scheduled using the CommCell Console. When the backup job is started:

- The array is accessed to create a snapshot.
- The database is quiesced using db2 write suspend command
- An automatic snapshot of all the database volumes is created.
- The database operations are resumed
- The DB2 online log can be configured on the same/different snap volumes as you configure for snap database.
- Data could be moved from the SNAP to a library either on the same client or using a proxy.

This snapshot is used for backup copy operations. This can also be used for restore/mount operations.

During the Backup Copy operations:

- The snapshot is mounted to the source or proxy computer.
- The mounted snapshot is treated like file system and the required contents are read.
- The file system backup is performed to Primary Copy of the storage policy.
- When the backup copy job is finished, the snapshot is unmounted.

DB2 Parameters

You can automatically update DB2 parameters (LOGARCHMETH1, LOGARCHOPT1, VENDOROPT, TRACKMOD, etc.,) using Db2_config.sh on UNIX and Db2_config.ps1 on windows to perform backups and restores. See the Commvault Documentation on "Automatically updating DB2 parameters" for more information.

You can manually configure the following parameters to back up any type of DB2 database online or offline, update the database configuration parameters when DB2 agent is installed on a cluster or multiple instances of Simpana are installed.

From the DB2 console, type the following command to set the LOGARCHOPT1 parameter:

```
db2 update db cfg for <database name> using LOGARCHOPT1
"'CvClientName=<CvClientName>,CvInstanceName=<CvInstanceName>'"
```

Example:

```
db2 update db cfg for test_db using LOGARCHOPT1
"'CvClientName=testhost,CvInstanceName=Instance001'"
```

Type the following command to set the VENDOROPT parameter:

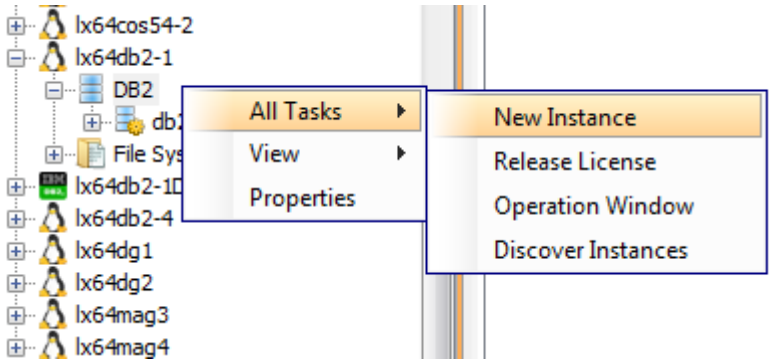
```
db2 update db cfg for <database name> using VENDOROPT
"'CvClientName=<CvClientName>,CvInstanceName=<CvInstanceName>'"
```

Example:

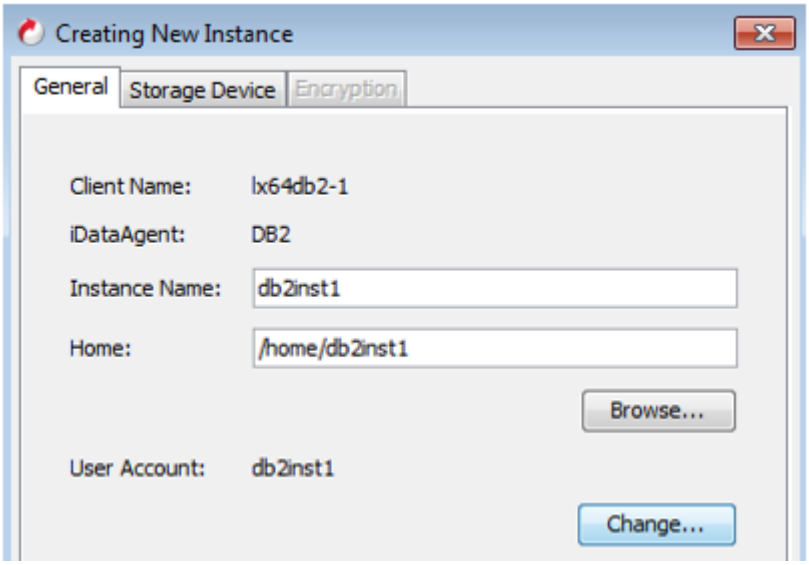
```
db2 update db cfg for test_db using VENDOROPT
"'CvClientName=testhost,CvInstanceName=Instance001'"
```

Configure the DB2 Instance

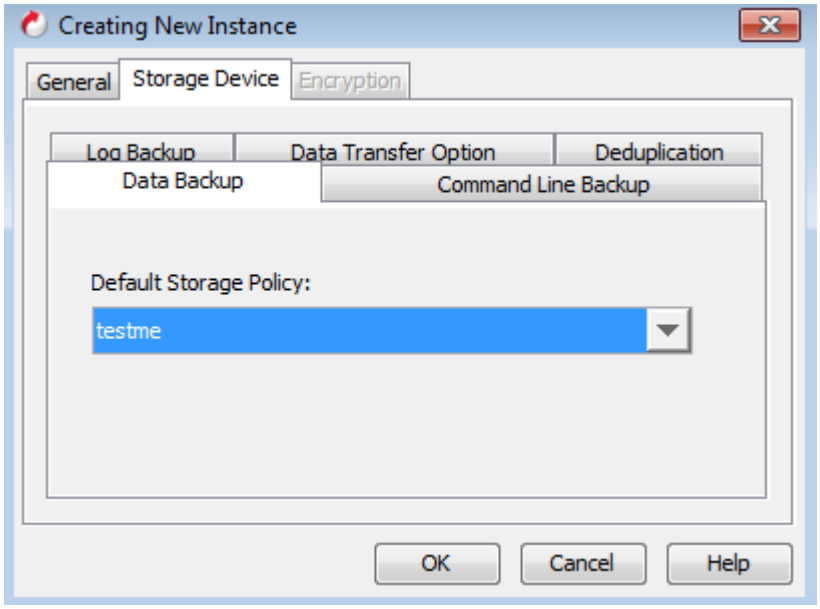
1. From the CommCell Browser, navigate to **Client Computers | <Client>**.
2. Right-click **DB2** and click **All Tasks | New Instance**.



3. On the **General** tab of the **Creating New Instance** dialog box:
   - Enter the Instance Name.
   - In the **Home** box, click **Browse** or enter the path to the DB2 application files.
   - In the **User Account** section, click **Change**.
   - In the **User Account** field, type the user name and password to access the DB2 application. Click **OK**.



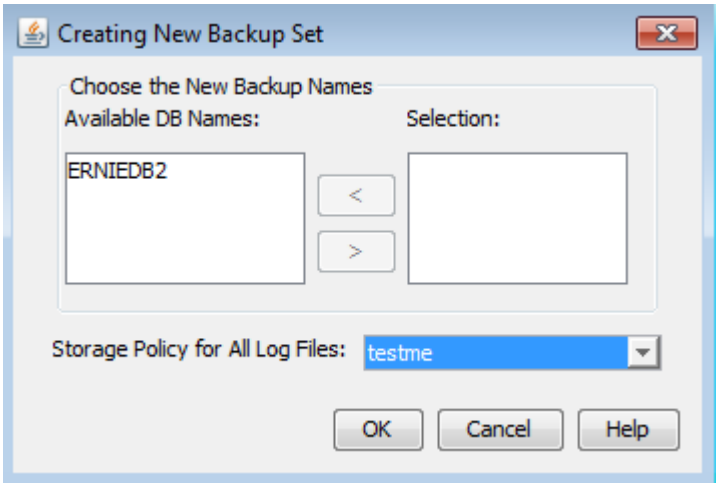
4. On the **Data Backup** tab under the **Storage Device** tab of the **Creating New Instance** dialog box:
   - In the **Default Storage Policy** box, select a storage policy name for data backups



5. On the Command Line Backup tab under the Storage Device tab of the **Creating New Instance** dialog box:
   - In the **Storage Policy for Command Line Backup** box, select a storage policy name.
6. On the **Log Backup** tab under the **Storage Device** tab of the **Creating New Instance** dialog box:
   - In the **Storage Policy for All Log Files** box, select a storage policy name for log backups.
7. Click **OK**.

Create the DB2 Backup Set

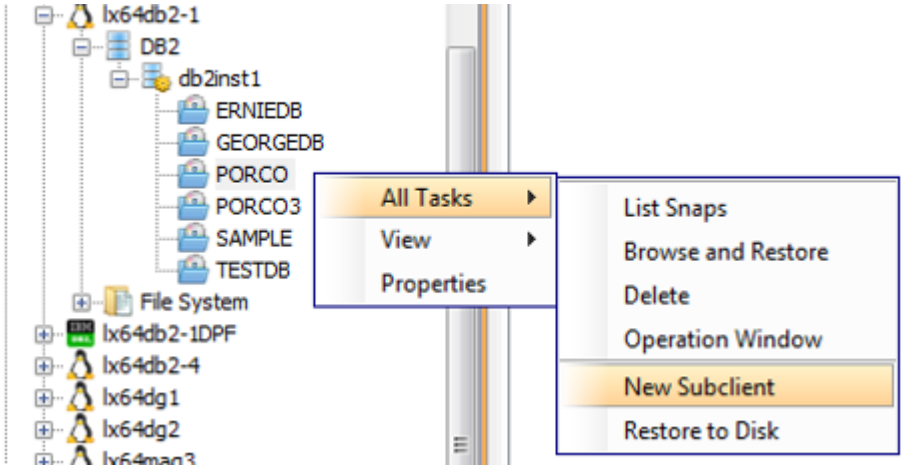
8. From the CommCell Browser, navigate to **Client Computers | <Client> | DB2**.
9. Right-click the **<Instance>** and click **All Tasks | Create New Backup Set**.
10. On the **Creating New Backup Set** dialog box, under **Available DB Names**, click the database name, and then click the arrow button to move the database name to the **Selection** box.
11. Click **OK**.



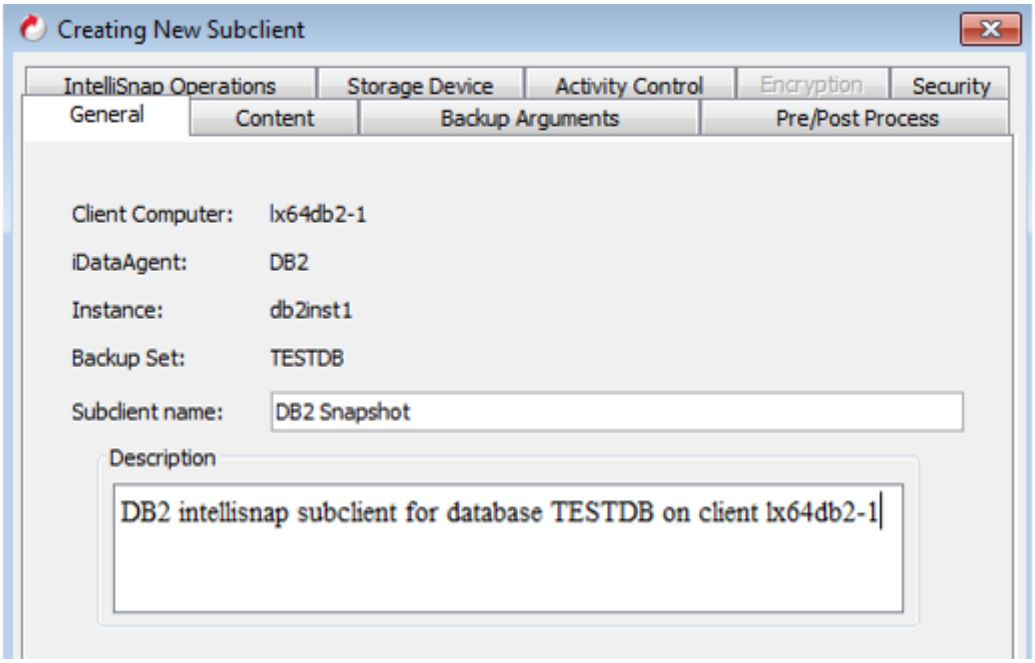
Create the DB2 Subclient

1. From the CommCell Browser, navigate to Client Computers |< Client > | DB2 | <Instance>.

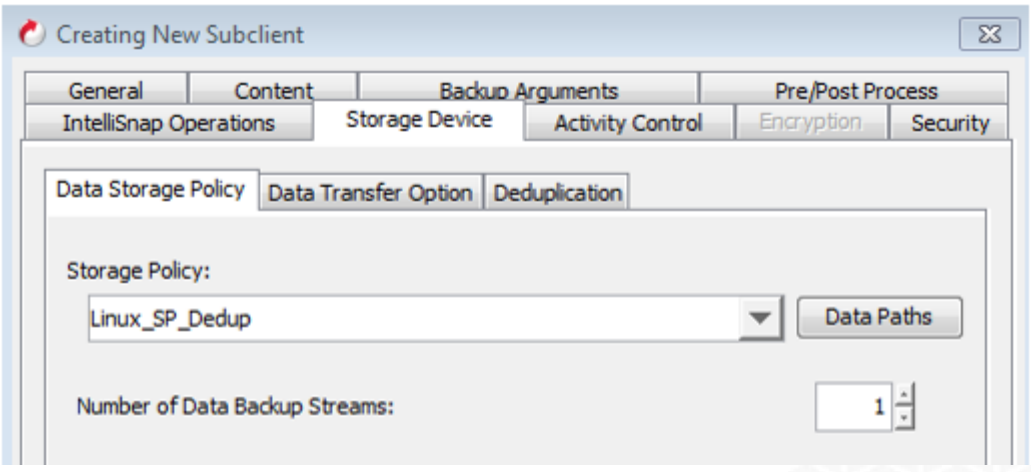
2. Right-click the <BackupSet>, point to All Tasks, and then click New Subclient.



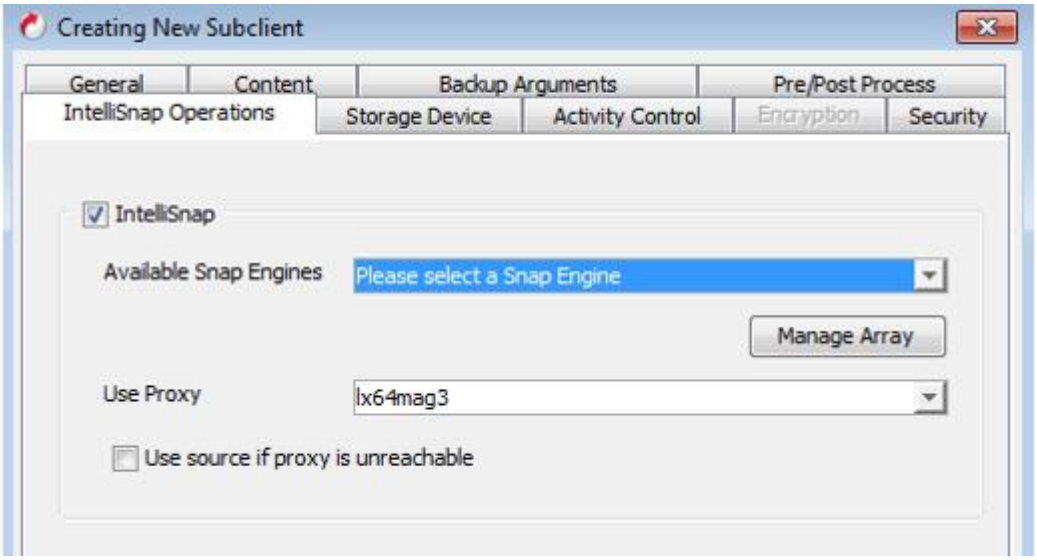
3. On the Creating New Subclient dialog box, navigate to the General tab and enter the Subclient name.



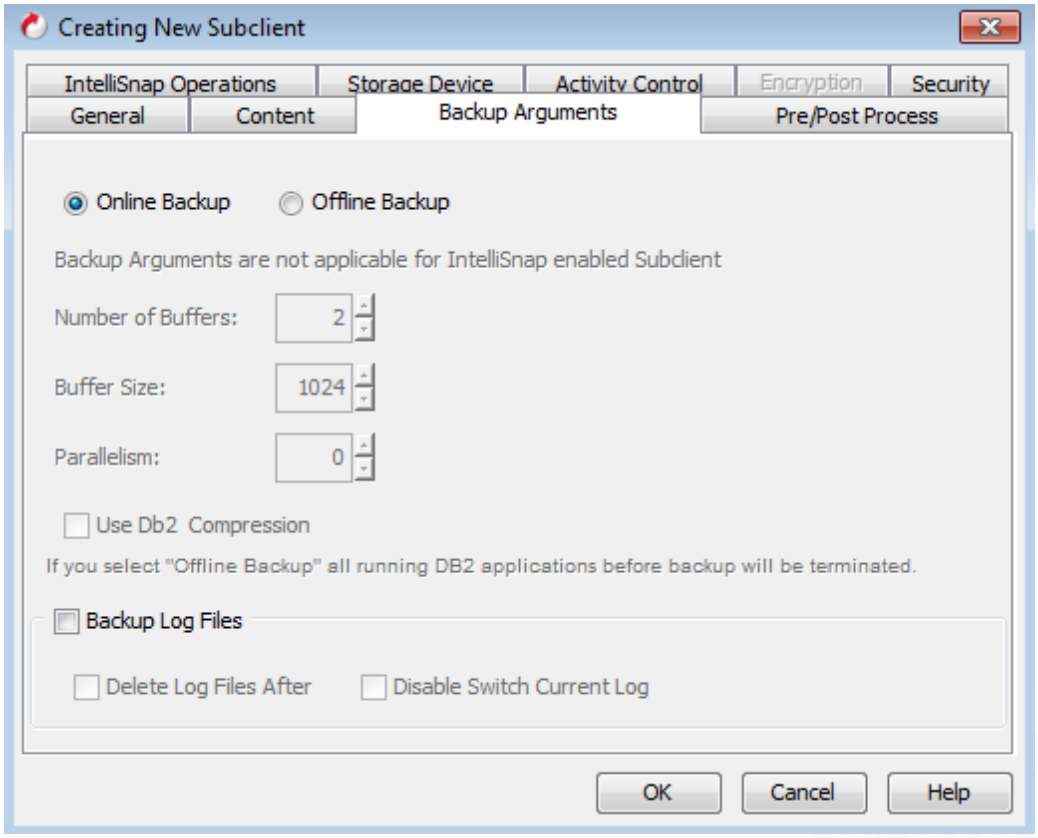
4. On the Creating New Subclient dialog box, navigate to the Storage Device tab and select or type the Storage Policy in the combo box.



5. On the Creating New Subclient dialog box, navigate to the IntelliSnap Operations tab and select the IntelliSnap check box and the Snap engine from Available Snap Engines list.
   - From the Use Proxy list, select the MediaAgent where IntelliSnap and backup copy operations will be performed.
   - When performing IntelliSnap backup using proxy, ensure that the operating system of the proxy server is either same or higher version than the client computer.



6. On the **Creating New Subclient** dialog box, navigate to the **Backup Arguments** tab:
   - To create an offline backup, select **Offline Backup**.
   - To create an online backup, select **Online Backup**.



7. Click **OK**.

DB2 IntelliSnap® and Backup Copy

During an IntelliSnap backup for DB2, the database is quiesced by putting the database in a write suspend mode. All the data volumes that are included in the result set from the command

db2 "select dbpartition, type, path from sysibmadm.dbpaths"

are snapped.

The database operations are then resumed. The archived log files are not included with the snapshot. The logs are streamed after the data snapshot is taken.

The following content is backed up with an IntelliSnap backup:

- DB2 database objects
- History files
- Online Redo Log Files
- Archived Log Files (traditional streamed backed AFTER snap is taken)

To initiate an IntelliSnap backup, perform the following steps:

1. Navigate to Client Computers | <Client> | DB2 | <Instance> | | <Backup Set>.
2. Right-click the Subclient and click Backup.
3. On the Backup Options for Subclient dialog:
   - Click Full as backup type and then click Immediate.
4. Click OK.

Backup Copy Operations

A backup copy operation provides the capability to copy snapshots of the data to any media. It is useful for creating additional standby copies of data and can be performed during the IntelliSnap backup or at a later time. Note that if primary snap copy is configured as Spool copy (copy with no retention rules) then the snapshots will be automatically deleted after the backup copy operation completes successfully.

Inline Backup Copy

Backup copy operations performed during the IntelliSnap backup job are known as inline backup copy. You can perform inline backup copy operations for primary snapshot copies and not for secondary snapshot copies. If a previously selected snapshot has not been copied to media, the current IntelliSnap job will complete without creating the backup copy and you will need to create an offline backup copy for the current backup.

1. Navigate to Client Computers | <Client> | DB2 | <Instance> | <Backup Set>.
2. Right-click the <Subclient> and click Backup.
3. On the Backup Options dialog box, select Full as the Backup Type and Immediate for the Job Initiation.
4. On the Backup Options dialog box, click Advanced.
5. On the Data tab of the Advanced Backup Options dialog box, select the Create Backup Copy immediately check box to create a backup copy.
6. Click OK.

You can view the progress of the job, by going to the CommCell Console ribbon, clicking the **Home** tab, and then clicking **Job Controller**.

Offline Backup Copy

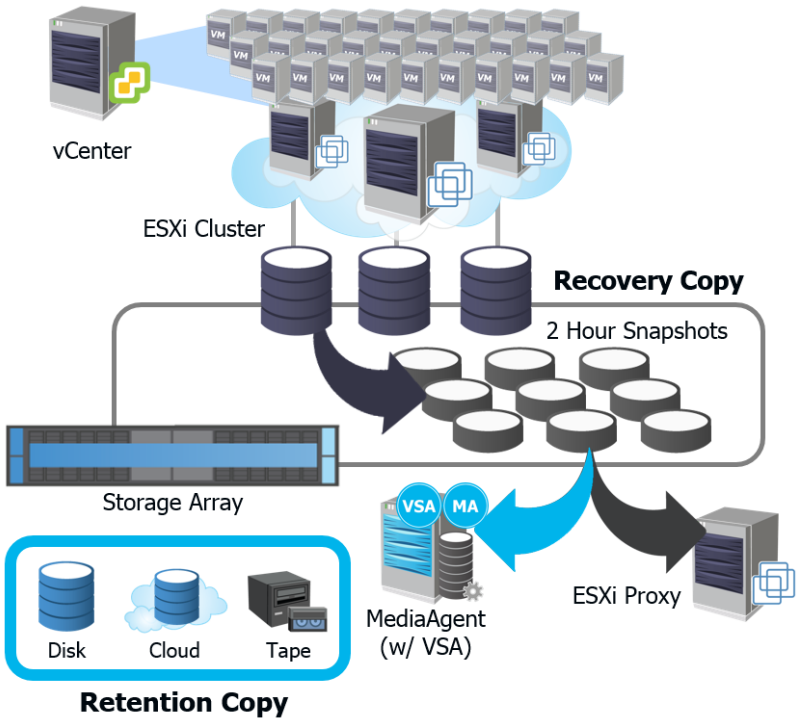
Backup copy operations performed independent of the IntelliSnap backup job are known as offline backup copy.

Use the following steps to run offline backup copy.

1. From the CommCell Console, navigate to **Policies | Storage Policies**.
2. Right-click the **<Storage Policy>** and click **Properties**.
3. On the **Storage Policy Properties** dialog box, navigate to the **Snapshot** tab.
4. Under **Snapshot Management Rules**, select the **Enable Backup Copy** option.
5. Click **OK**.
6. From the CommCell Console, navigate to **Policies | Storage Policies**.
7. Right-click the **<storage policy>** and click **All Tasks | Run Backup Copy**.
8. On the **Backup Copy For** dialog box, select the **Start New Media** check box to copy the data to a different tape.
9. Select **Mark Media Full On Success** to mark the media that is used for this operation after the snapshot copy operation has successfully completed.
10. Click **OK**.

VMware Configurations

IntelliSnap technology enables fast protection of large or volatile VMware environments without placing load on the production vSphere Farm. IntelliSnap technology integration with the Virtual Server Agent (VSA) enables the array to perform backups in minutes even with large numbers of virtual machines and sizable data stores. A dedicated ESX server for proxy data movement completely removes any utilization on the ESX farm with granular access providing individual file and folder recovery from the secondary tier of storage.

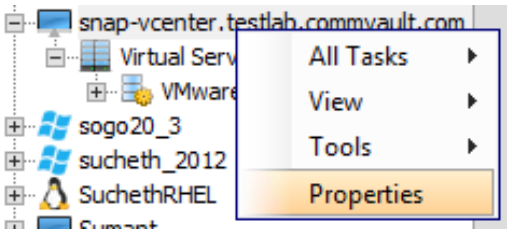


Prior to configuring the VMware environment, deploy the proper agents requiring snapshot integration with the Array. VMware requires more security rights beyond the typical VADP use case. See the Commvault Documentation for security details in creating proper security environment for IntelliSnap. VMware environments require the following agents:

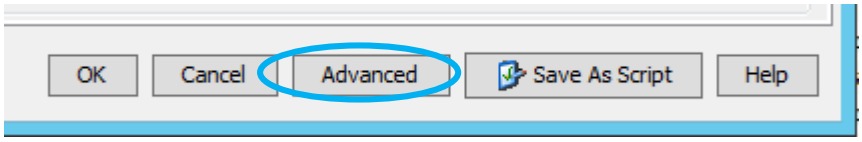
- Virtual Server Agent (VSA) on the Windows physical server(s) or virtual hot-add guest(s)
- File System iDataAgent on the Windows physical server(s) or virtual hot-add guest(s)
- MediaAgent on the Windows physical server(s) or virtual hot-add guest(s)

The following steps will configure the implemented VMware Environment for IntelliSnap operations:

1. A vCenter pseudoclient should be created if one does not already exist. See Commvault Documentation – Virtual Server Agent for VMware for instructions on adding a vCenter virtualization client.
2. Enable IntelliSnap on the vCenter virtualization client. Right-click on the vCenter server name, then select **Properties**.

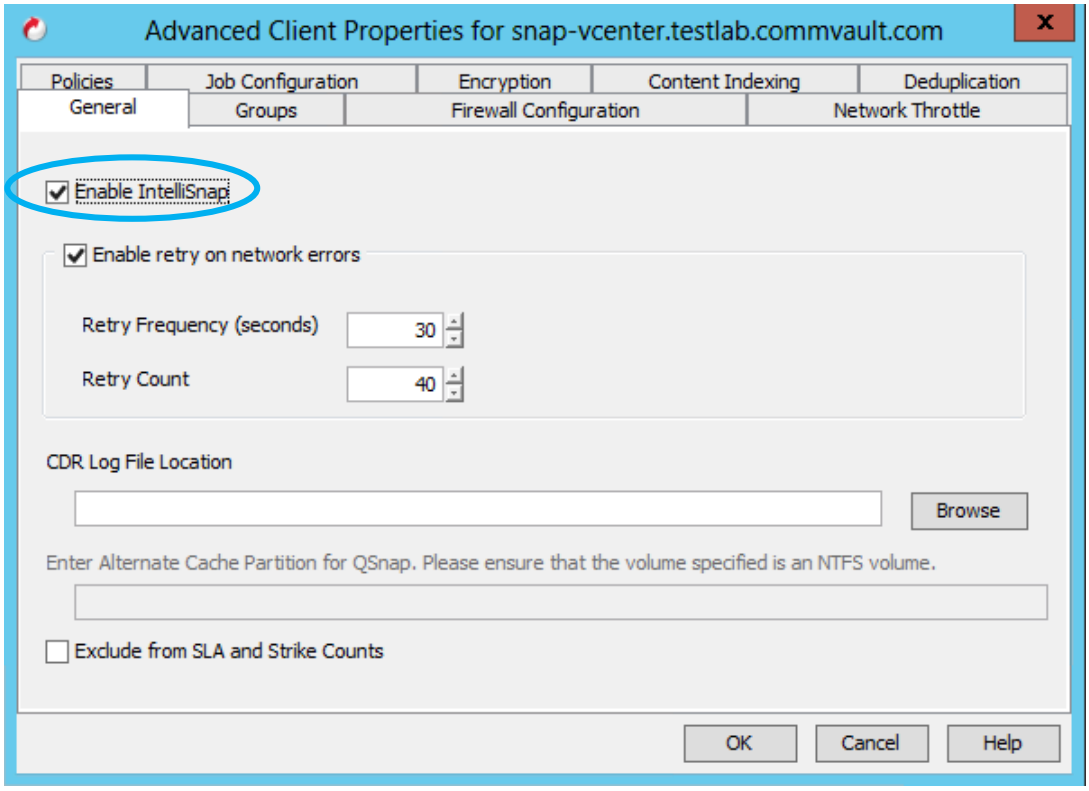


3. Click the Advanced button.



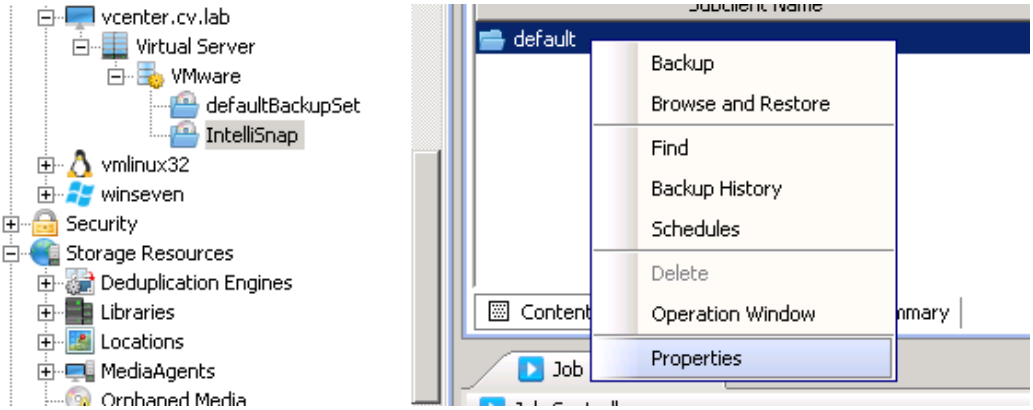
4. On the General tab, check the box marked **Enable IntelliSnap**.

   This will consume a Hardware Snapshot Enabler license from the license key.

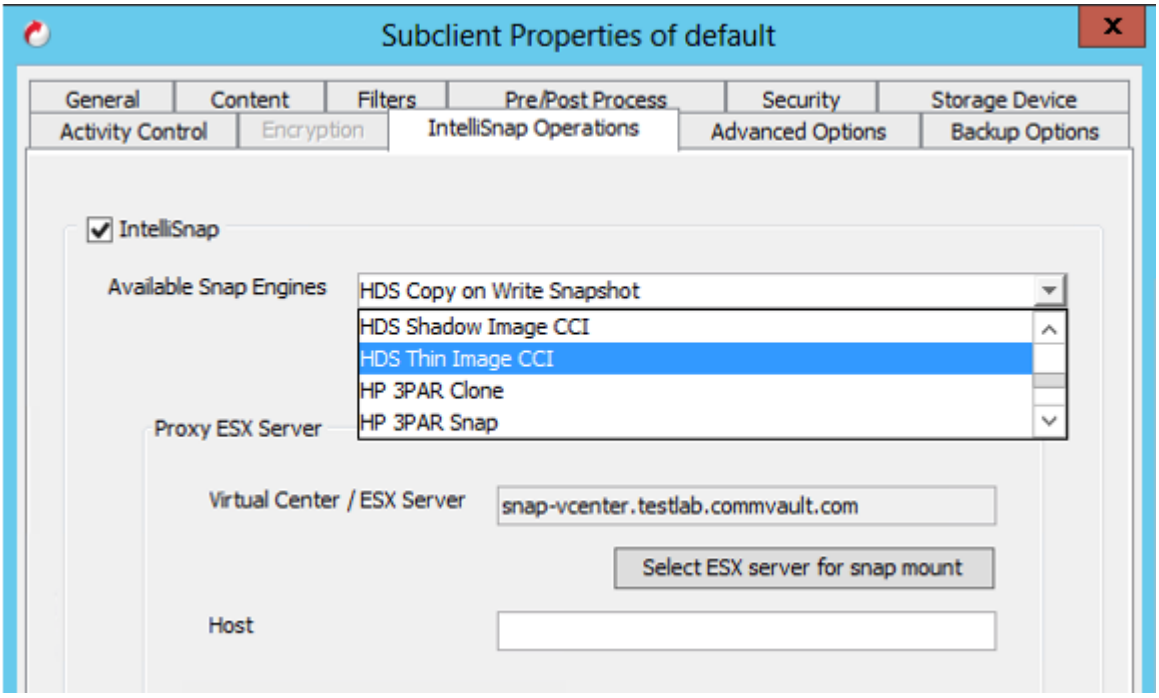


5. Click **OK** to close the Advanced Client Properties window, and again on **OK** to close the Client Computer Properties window.

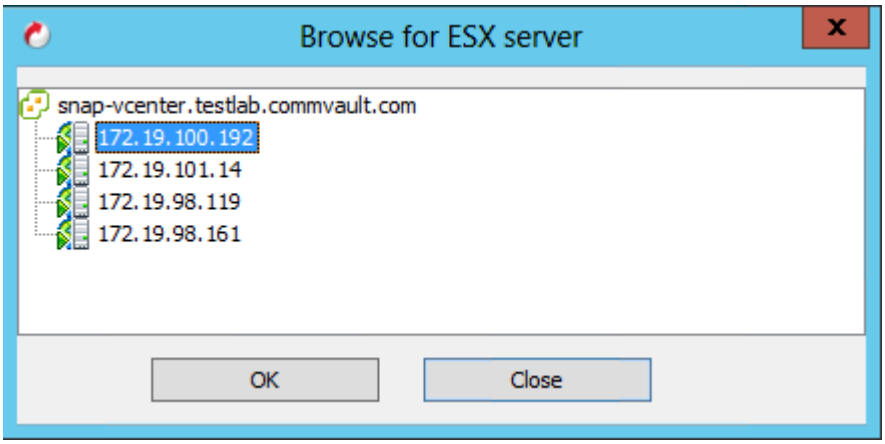
6. Browse through the VSA iDataAgent to the desired VMware backup set and then access the properties of the desired subclient to enable IntelliSnap Operations:



7. Browse to the **IntelliSnap Operations** tab, check the **IntelliSnap** box. Select the appropriate snap engine as the **Available Snap Engines**.



8. To define proxy configurations on the **IntelliSnap Operations** tab, below the **Proxy ESX Server**, click on **Select ESX server for snap mount**. This opens a dialog box with the available ESX servers in the environment. Select the desired ESX server to perform the Proxy operations for generating granular backups to disk/tape/cloud. The selected ESX server mounts the array snapshot when a backup copy operation executes.



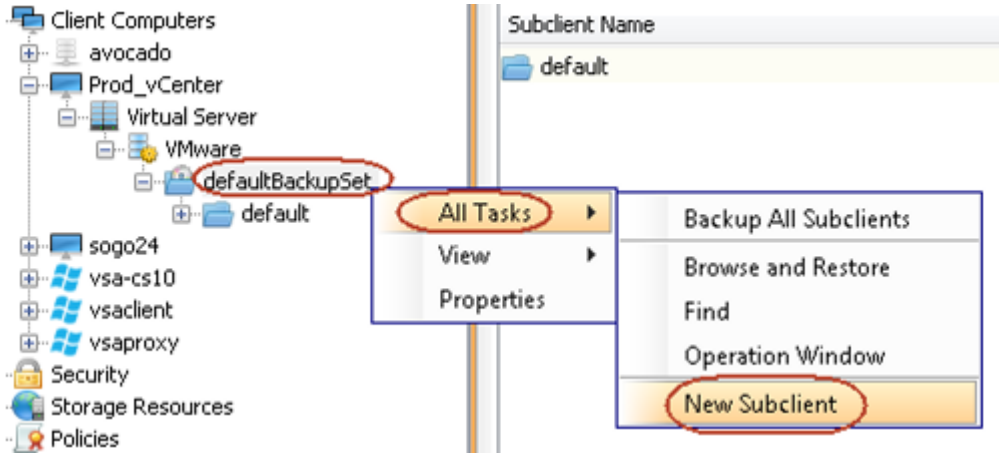
9. Ensure the **Storage Device** tab has a storage policy with a Snap Copy defined and click OK to close the Subclient properties.

10. To execute a snap operation for the VSA agent, simply schedule or generate a backup job for the previously configured Subclient. Simpana will detect the configuration and automatically run a snap backup job. If a proxy is configured, ensure that it has all prerequisites set up before running the operation.

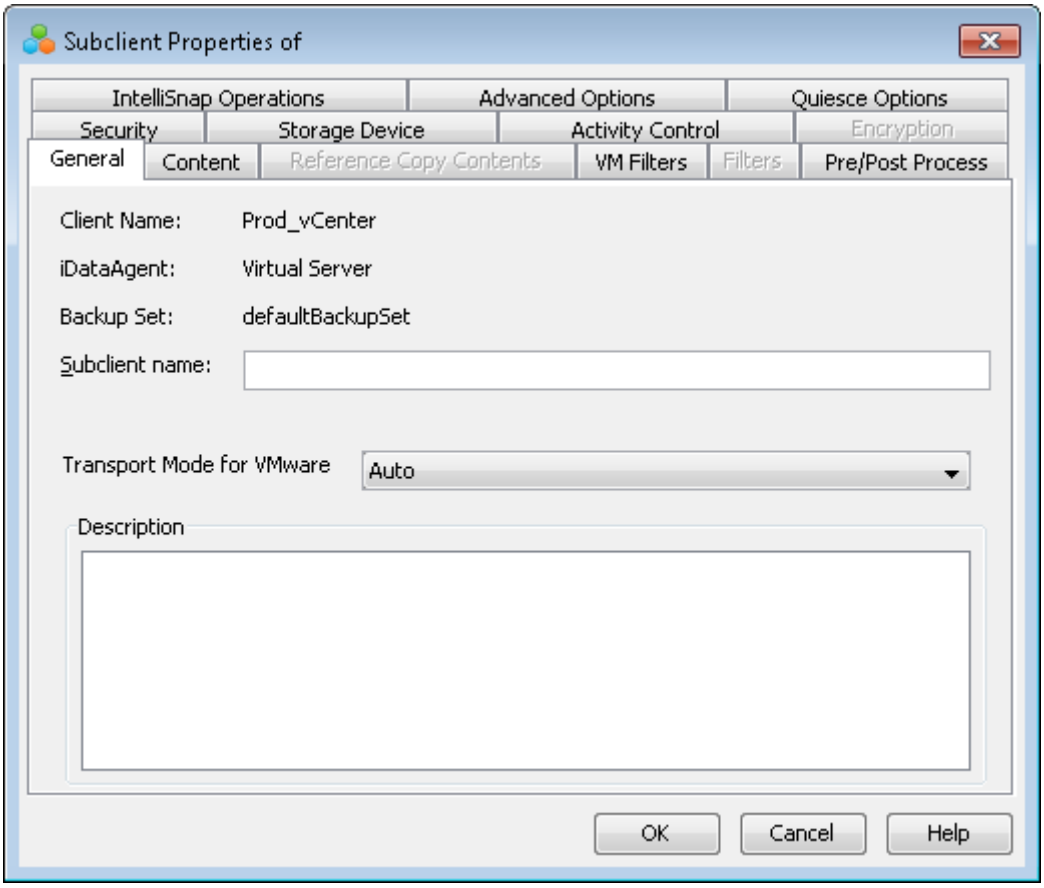
Discover Virtual Machines from a Host

If you want to back up all the virtual machines from a specific host, configure a Subclient as follows:

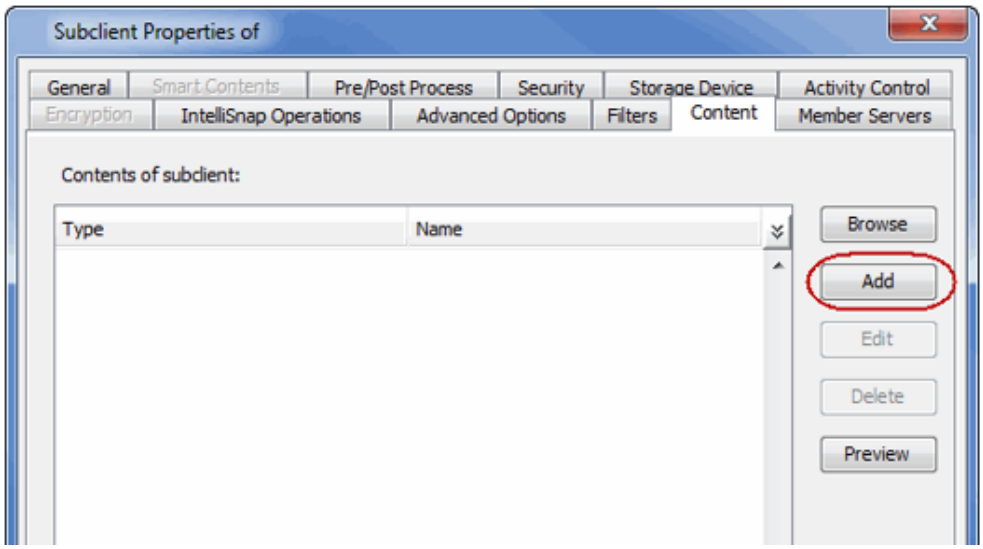
1. From the CommCell Browser, navigate to Client Computers | <vCenter Client> | Virtual Server | VMware. Right-click the defaultBackupSet and click New Subclient.



2. Enter the Subclient name.

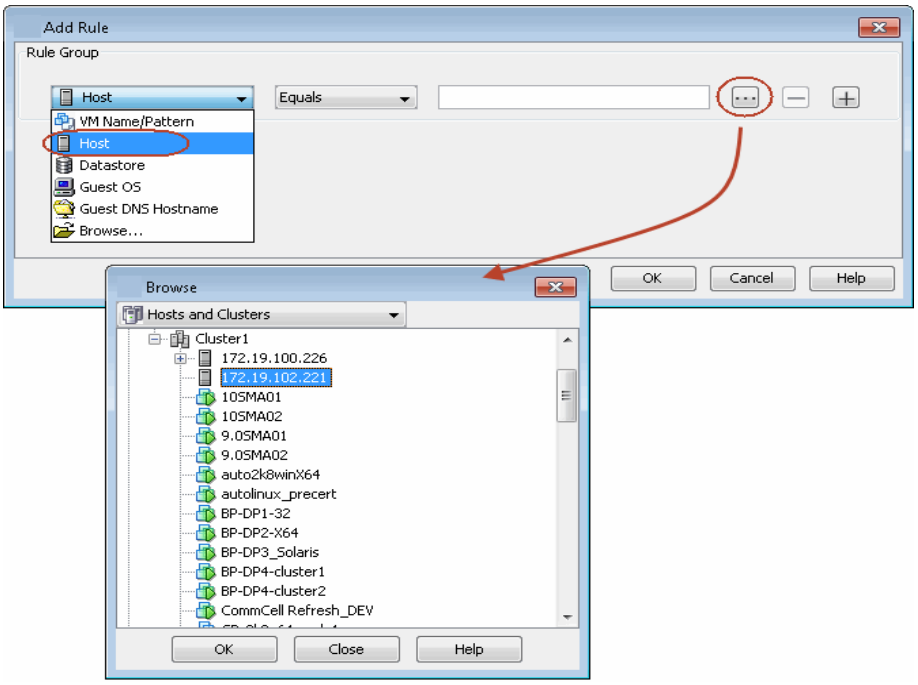


3. Click the **Content** tab. Click **Add**.



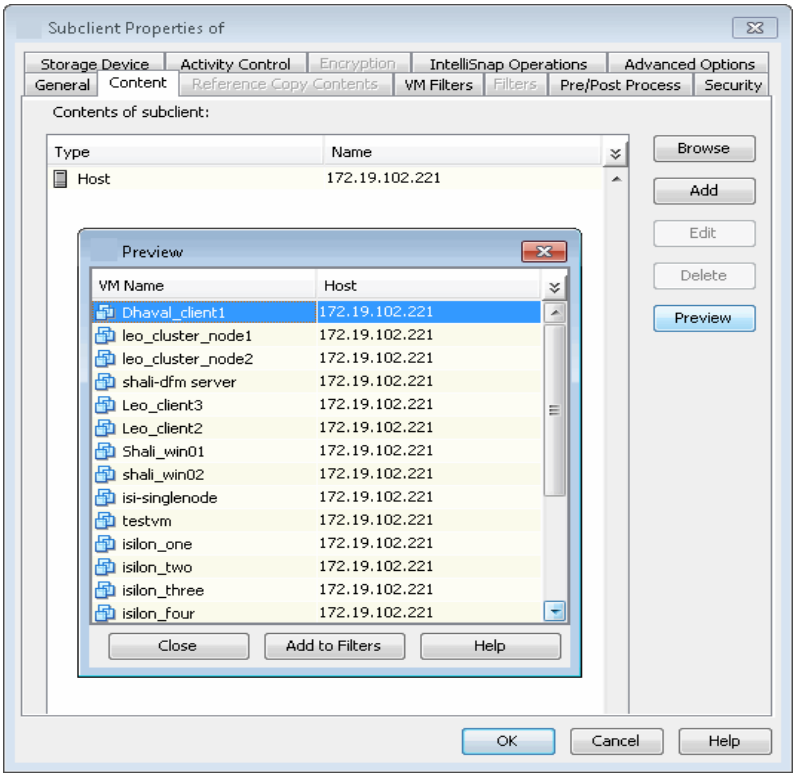
4. Click the available list and select **Host** from the list. Enter the host name which appears in the vCenter or IP address of the host.

   Otherwise, click "…" to open the **Browse** dialog box. Navigate to the required host and select the host. Click **OK**.



   The selected host will appear in the **Contents of Subclient** list on the **Content** tab.

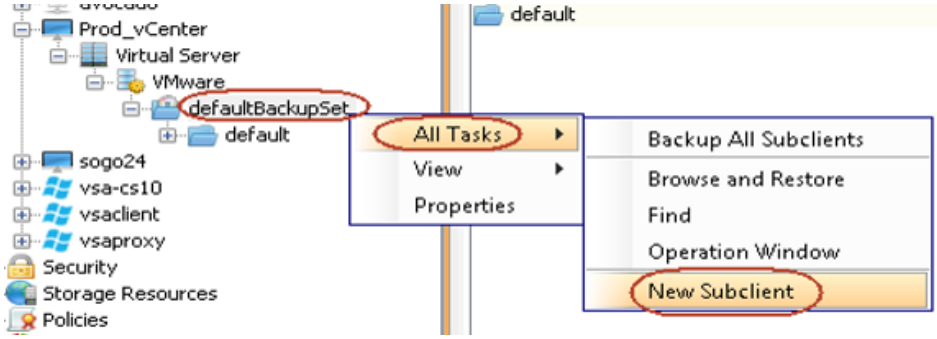
5. Click **Preview** to view all the virtual machines on the host. These virtual machines will get backed up when you perform the backup of the Subclient. Click **OK**.



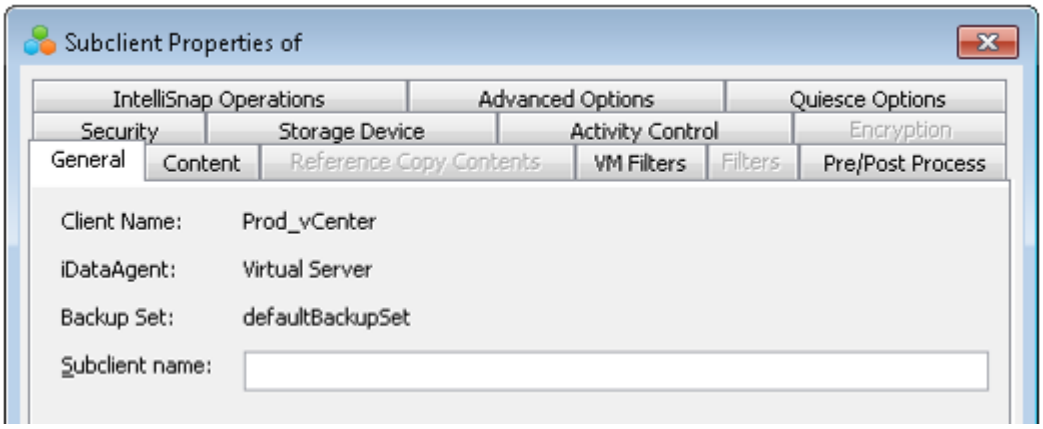
Discover Virtual Machines from a Datastore

If you want to back up all the virtual machines from a specific Datastore, set the criteria as follows:

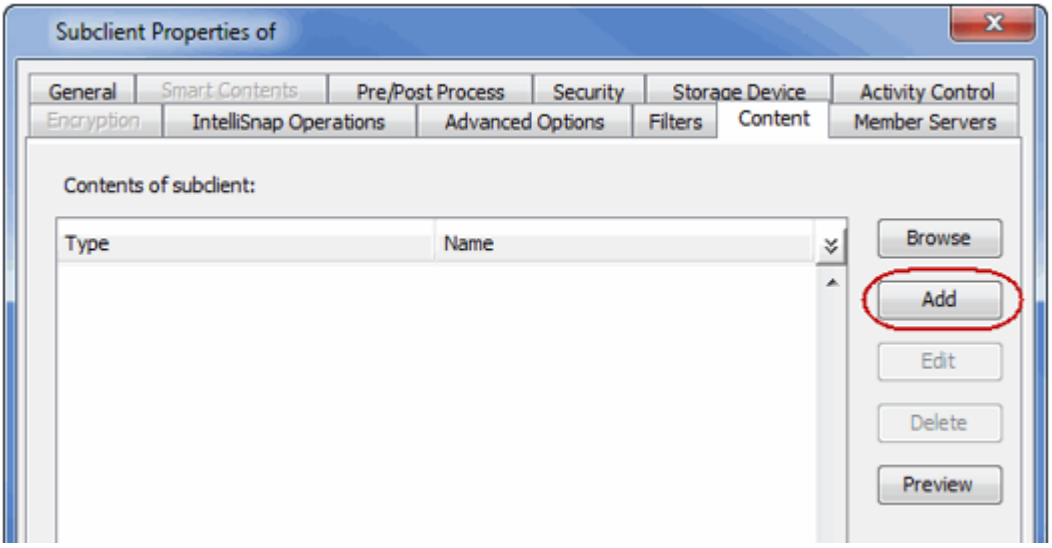
1. From the CommCell Browser, navigate to **Client Computers | <vCenter Client> | Virtual Server | VMware.**
2. Right-click the **defaultBackupSet** and click **New Subclient**:



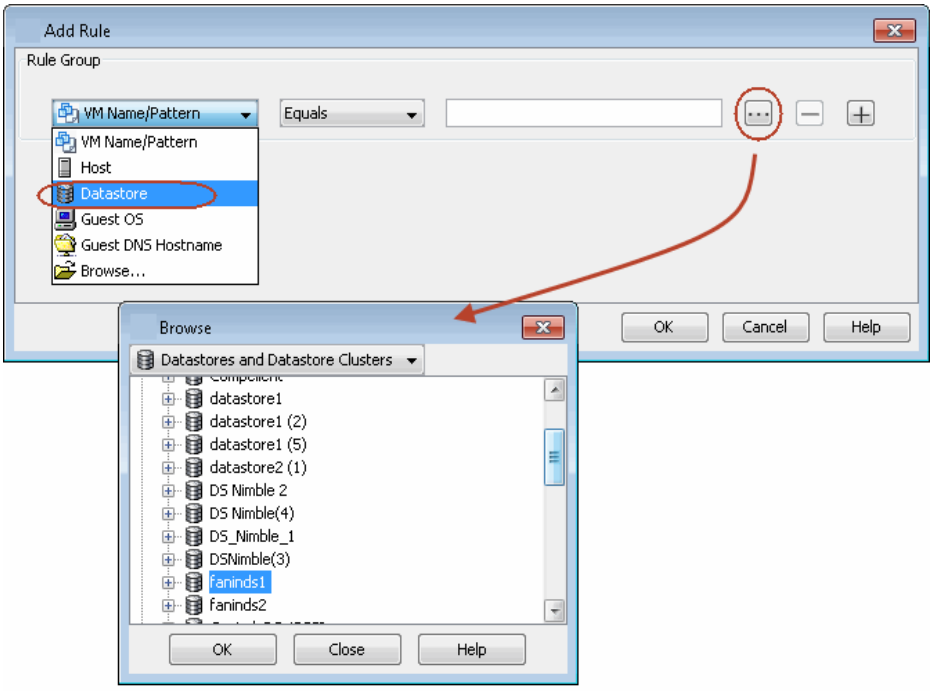
3. Enter the **Subclient** name.



4. Click the **Content** tab. Click **Add**.

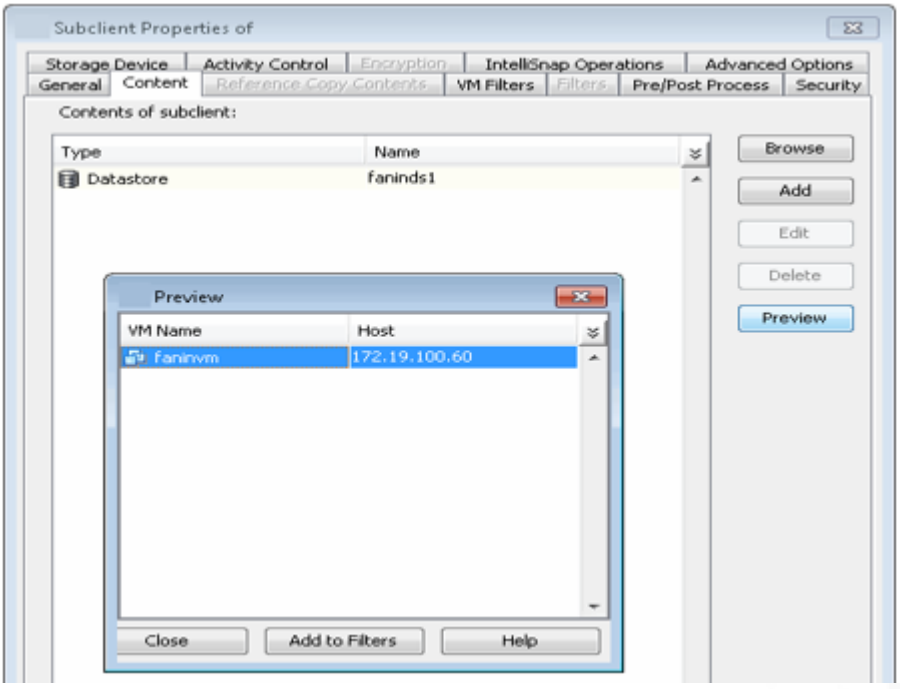


5. Click the available list and select **Datastore** from the list. Enter the Datastore name.
6. Otherwise, click "…" to open the **Browse** dialog box.
7. Select the Datastore from the available list. Navigate to the required Datastore and select the host. Click **OK** on the Browse dialog box. Click **OK** on the Add Rule dialog box.



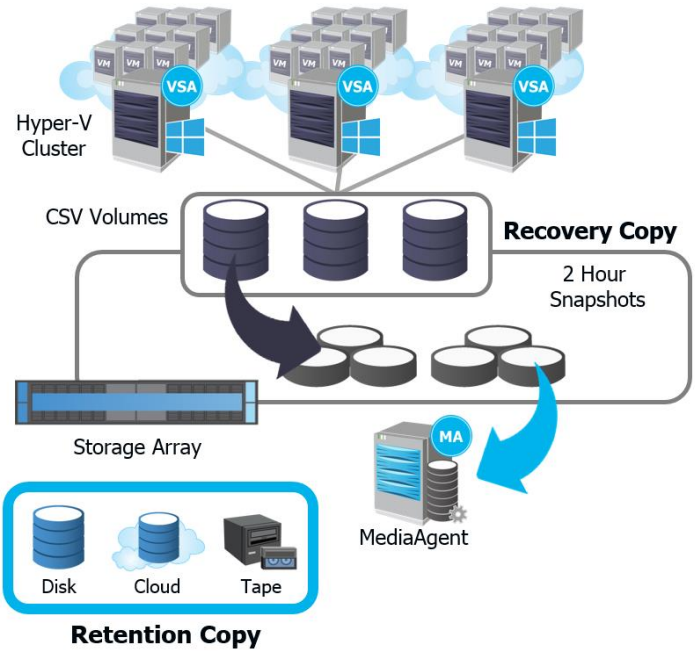
8. The selected Datastore will appear in the **Contents of Subclient** list on the **Content** tab.
9. Click **Preview** to view all the virtual machines in the Datastore. These virtual machines will get backed up when you perform the backup of the Subclient. Click **OK**.

Note: If a virtual machine has only one disk in the selected Datastore and remaining disks and VMX files are located on other Datastores, the virtual machine will be added to the Subclient.



Hyper-V Configurations

IntelliSnap enables fast protection of large or volatile Hyper-V environments without placing load on the production Hyper-V cluster. IntelliSnap technology integration with the Virtual Server Agent (VSA) enables the array to perform backups in minutes even with large numbers of virtual machines and sizable Cluster Shared Volumes (CSVs). A dedicated Hyper-V host for proxy data movement completely removes any utilization on the production cluster, with granular access providing individual file and folder recovery from the secondary tier of storage.

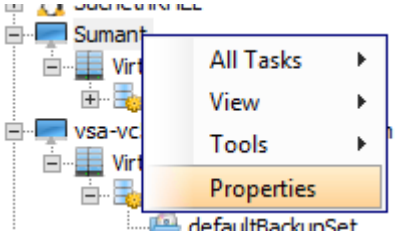


Prior to configuring the Hyper-V environment, deploy the proper agents requiring snapshot integration with the Array.

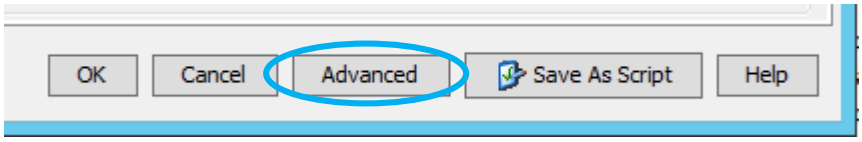
- **Virtual Server Agent (VSA)** on the physical server(s) or virtual hot-add guest(s)
- **File System iDataAgent** on the physical server(s) or virtual hot-add guest(s)
- **MediaAgent** on the physical server(s) or virtual hot-add guest(s)

The following steps will configure the implemented Virtualization Environment for IntelliSnap operations:

1. A Hyper-V pseudoclient should be created if one does not already exist. See Books Online (http://documentation.commvault.com/commvault/v10/article) for instructions on adding a Hyper-V pseudoclient.
2. Enable IntelliSnap on the Hyper-V pseudoclient. Right-click on the Hyper-V cluster/server name, then select **Properties**.

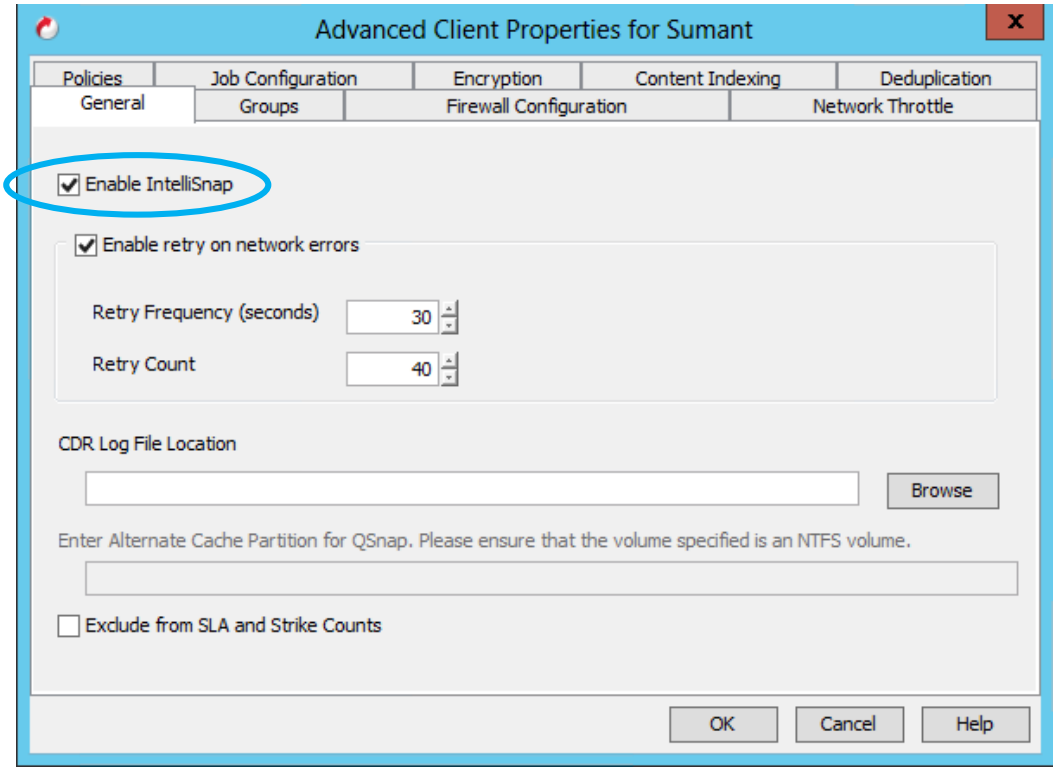


3. Click the Advanced button.



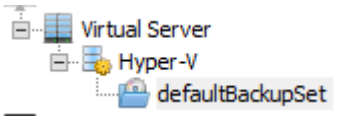
4. On the General tab, check the box marked **Enable IntelliSnap**.

   This will consume a Hardware Snapshot Enabler license from the license key.

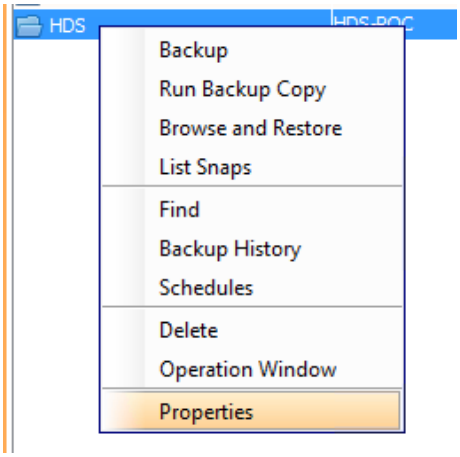


5. Click **OK** to close the Advanced Client Properties window, and again on **OK** to close the Client Computer Properties window.

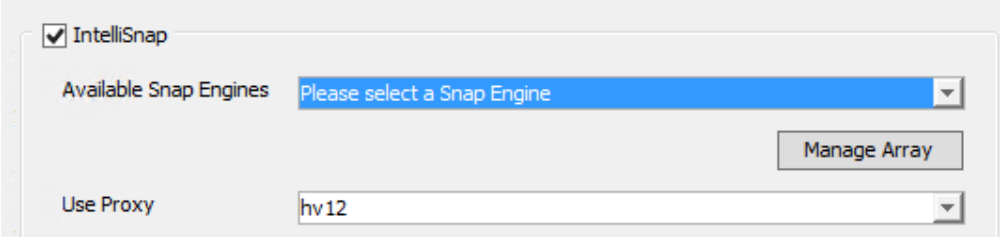
6. Browse through the VSA to the desired Hyper-V BackupSet



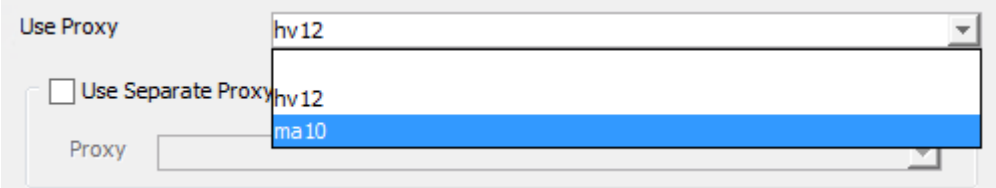
7. Right-Click on the desired Subclient, and select Properties



8. Browse to the **IntelliSnap Operations** tab, then check the **IntelliSnap** box. Select the snap engine from the **Available Snap Engines** dropdown.



9. To define proxy configurations on the **IntelliSnap Operations** tab, select the desired VSA from the **Use Proxy** dropdown.



10. Ensure the **Storage Device** tab has a storage policy with a snap copy defined and click OK to close the Subclient properties.
11. To execute a snap operation for the VSA agent, simply schedule or generate a backup job for the previously configured Subclient. Simpana will detect the configuration and automatically run a snap backup job. If a proxy is configured, ensure that it has all prerequisites set up before running the operation.

Hyper-V and Non-Persistent Snap Engines

Due to differences in the Hyper-V VSS stack, Hyper-V snapshots require multiple mounts to ensure application consistency. This leads to challenges with non-persistent snapshot engines, where changes are discarded after snapshots are deleted. Commvault software gets around this limitation by retaining both the initial snapshot and the volume copied or cloned from the snapshot. Both the snapshot and copy are deleted during aging operations.

Proxy Configuration

IntelliSnap technology provides a modernized architecture for handling data protection operations within the datacenter. Proxy capabilities enable an array-based snapshot to mount off-host, eliminating backup processes on the production servers. Allowing for multiple snapshots from different source servers across high-speed FC and IP networks eliminates any compression, deduplication, and encryption load on the production servers and centralizes streaming protection to a dedicated tier of services. Each OS with an IntelliSnap software client requires a similar OS (i.e. Windows to Windows, Linux to Linux, etc.) for proxy execution. Simpana will automatically link indexing information for data protected through the proxy back to the original host, enabling recovery back to the production host within the production application context. Application integrity checks may also be executed on the proxy servers to validate the consistency of snapped data prior to streaming protection operations.

For a configuration where snapshots mount off-host to a proxy server, implement the following agents on the proxy server.

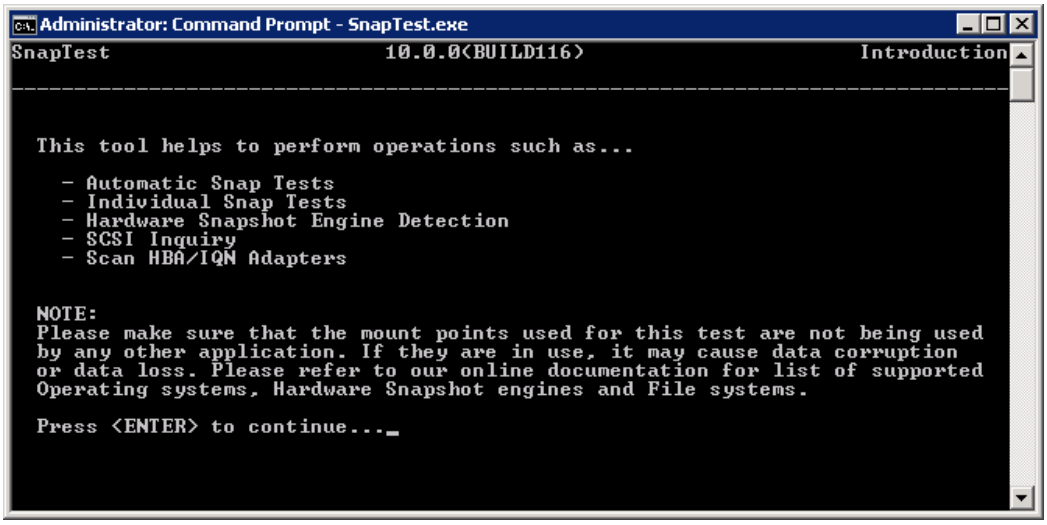
- File System iDataAgent (must be similar to production host operating system)
- MediaAgent
- Application-specific binaries for proxy if required (i.e. – Exchange Management Pack, Oracle for RMAN integration, etc.)
- Application iDataAgent if required

Verification of Configuration Using SnapTest

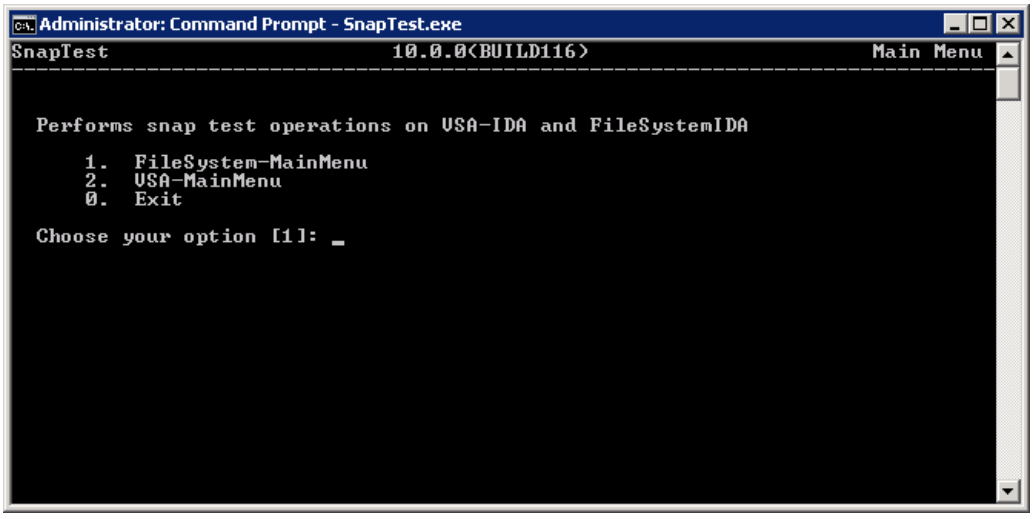
Validation of the IntelliSnap software configuration prior to running production jobs occurs through the SnapTest utility. This tool is located in the Base folder of the Simpana installation, allows one to check array connectivity and exercise the hardware snap engine to create and remove snapshots. Running this prior to productions routines will validate the configuration is properly defined on the Production Host side.

1. Locate the SnapTest executable in the base directory, and execute it:

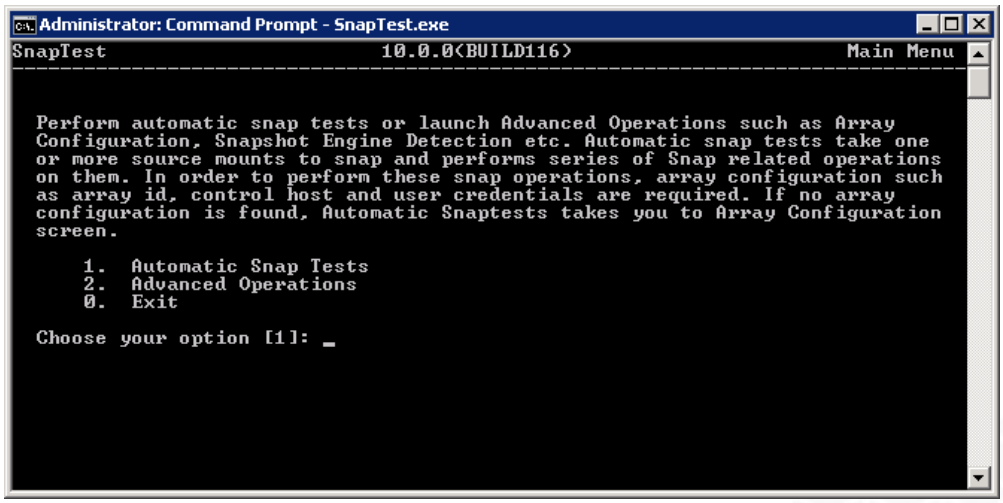
- For Windows - <Installation Directory>\Simpana\Base\SnapTest.exe
- For UNIX/Linux - <Installation Directory>/Simpana/Bases/SnapTest



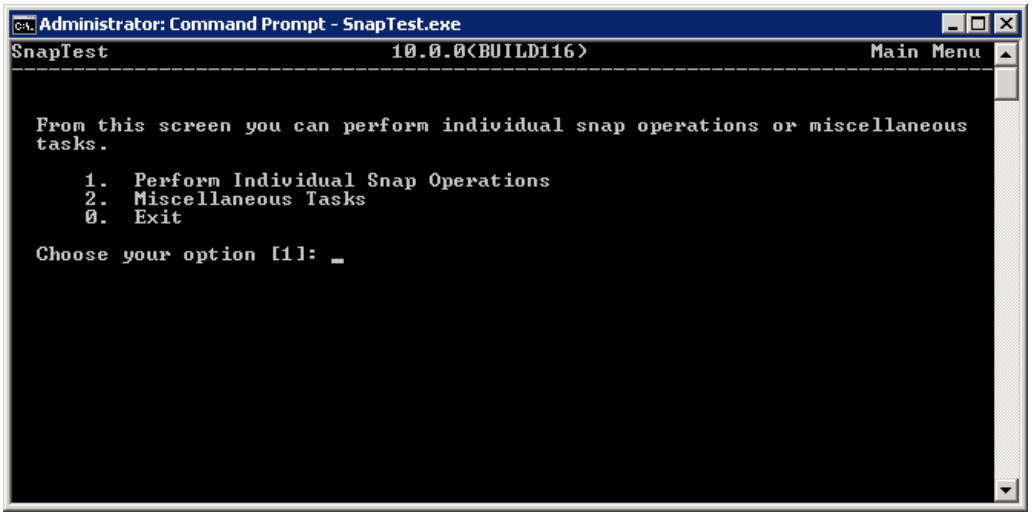
2. For this example we are utilizing a Windows host, we will be selecting the File System - Main Menu, Option 1.



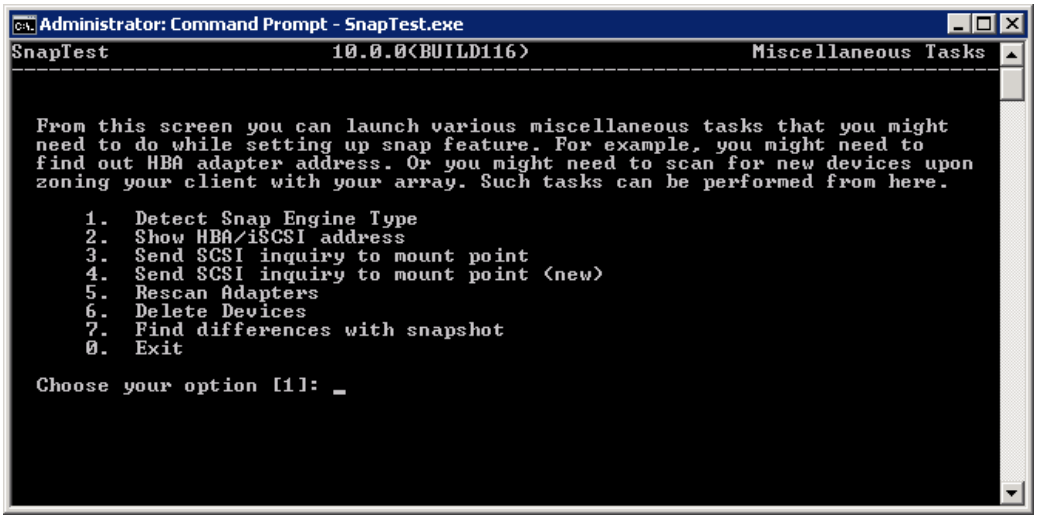
3. To prevent automatic reverts or to prevent automated tests, select Advanced Operations. Option 2:



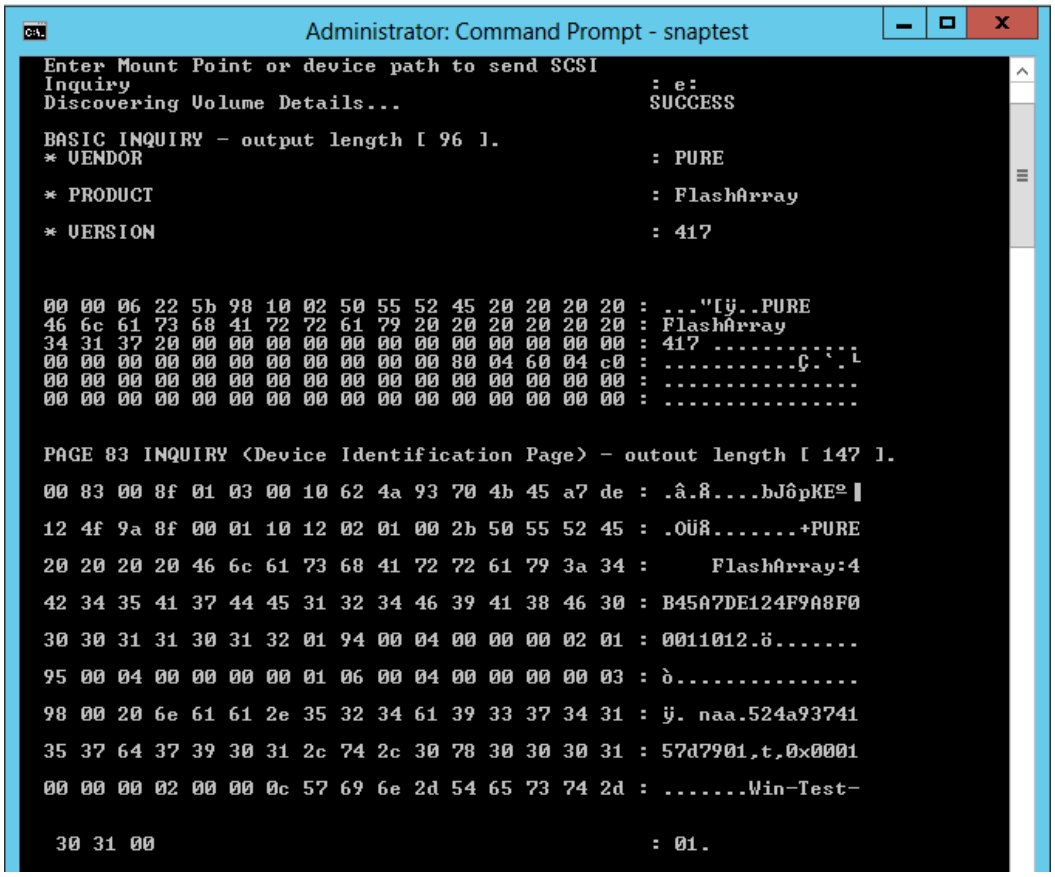
4. Select Option 2 for Miscellaneous Tasks



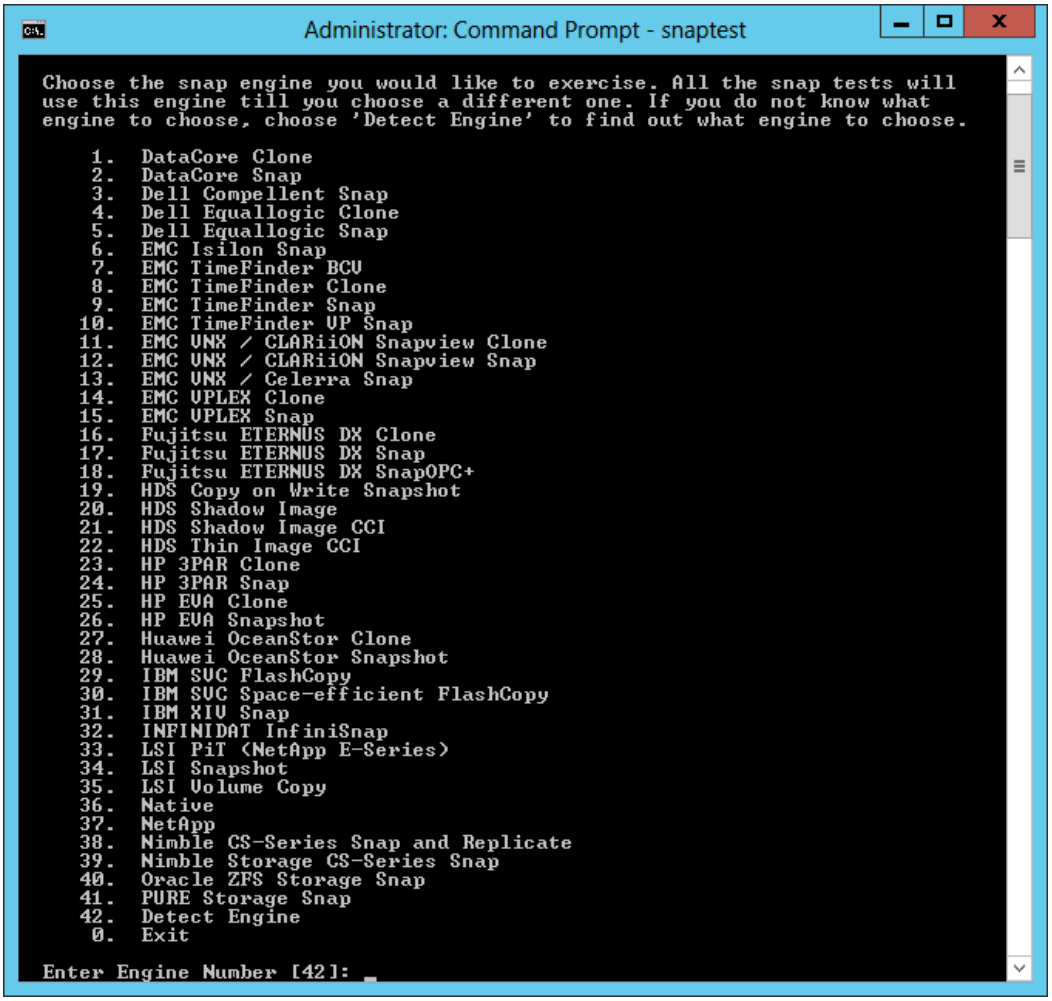
5. Check if we can send a SCSI inquiry to the storage device by selecting Option 4:



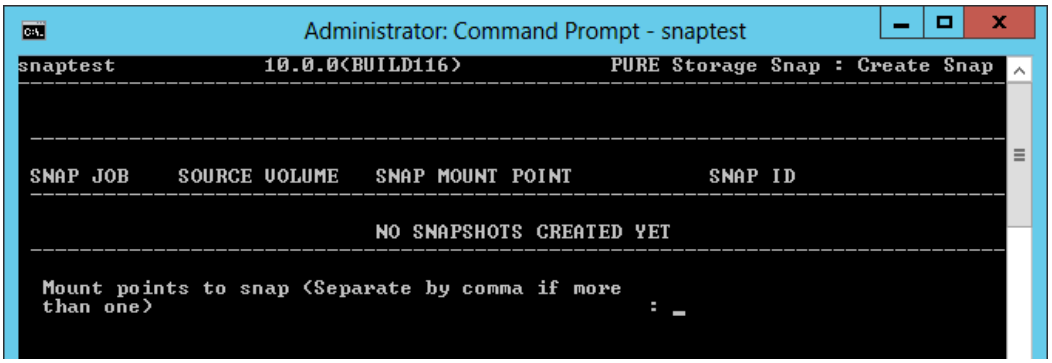
6. Enter the mount point for the FlashArray volume.
   - On Windows you must enter a drive letter or a mount path (junction point), without the trailing slash.
   - On a UNIX/Linux environment, enter the mount path location, e.g. /mnt/path, not the underlying device name under /dev.
   - You will now get a result similar to the following:



7. From the Main Menu (use option 0 to return), choose option 1: Perform Individual Snap Operations.
8. Select the PURE Storage Snap option (this will change as engines are added; it is 41 as of V10 SP12):



9. Exercise the selected Snapshot Engine by selecting Option "1". Enter the mount path to the FlashArray volume:

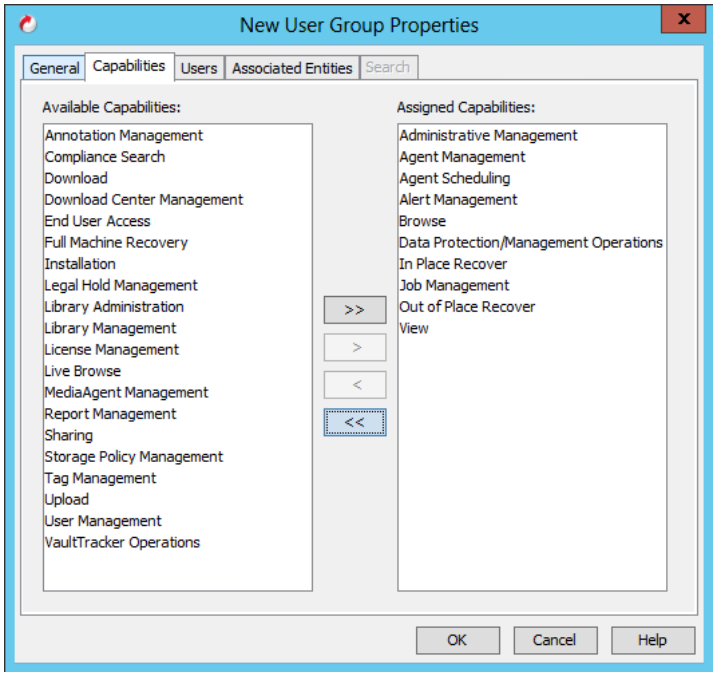


This will create a new snapshot based on the engine you have selected and will give you the necessary information to confirm all works. You may also test mounting and unmounting snapshots. Make sure to delete any snapshots you create with the SnapTest tool to avoid using unintended storage space.

Security & Storage Policy Best Practices

Security Roles

The power of a Storage Array in providing fast full volume recovery changes data architectures and SLA alignment. Any technology providing fast sweeping recovery directly linked to production data can be potentially dangerous without proper controls. Revert operations are perfect for massive data corruptions on productions volumes that require fast recoveries, assuming the proper controls are in place to allow only those who understand what the defined action will do for/to the business. Typical script based tools lack these controls and expose environments to high risk side effects with very little oversight or reporting. A single misaligned scripted argument could bring an entire production database environment down and cause catastrophic data loss. Further, restoring data through array based reverts when a single file/database is all that is necessary can destroy entire collections of data resetting the environment back hours or days if done incorrectly. Recent mail, revenue transactions, business data, etc. would all be lost due to a simple mistake in operation.



Rather than risking the business to make or beat the backup window with scripts or standalone tool sets, an integrated data management platform should provide proper safety controls to allow critical actions to entrust the right users at the right time while ensuring a reporting and audit system to overlay the full end-to-end view. In most medium to large environments, application operational responsibilities, backup, DR, compliance and audit may be distributed functions that need to be coordinated into a single policy. The embedded role based security system native to Simpana automates this function.

For Example, a customer may have three specific roles within an operations environment:

- Backup Admins
- Application owners (DBAs)
- Audit & Business Compliance

Each of these roles "owns" specific responsibilities for managing and protecting the enterprise. Backup Admins are the typical day to day operators with access to perform standard backup and recoveries, manage media, issue reports, etc. However, the Backup Admin role may not be the right team to execute application-level recoveries or have the capabilities to issue array-based reverts for recoveries due to knowledge and awareness of the application architecture. The Application Owner role is not so concerned about the general day to day backup environment, but is laser focused on the application space they own. They need to know what tools are available to them and who has the capabilities to execute on those toolsets at any time as they manage the applications running the business. Any recovery operations involving their applications, especially powerful techniques such as array reverts and snapshots must be managed from their group to mitigate any risk to the business. The Audit role simply needs to eliminate red flag events and provide security, operational, and process proof of who can perform what and how.

To meet this requirement specific roles should be defined solely for the IntelliSnap technology client and application iDA's within the CommCell. An example of this basic security structure as defined in Simpana Security Roles as noted here:

Security Roles (For Application Clients or Groups)	Backups	Application	Audit Team
Administrative Management		X	
Agent Managements	X	X	
Agent Scheduling	X	X	
Alert Management	X	X	
Browse	X	X	
Browse and In-Place Recover		X	
Browse and Out of Place Recover		X	
Compliance Search			X
Data Protection	X	X	
Data Protection Management	X	X	
End User Search			X
Job Management	X	X	
Library Management	X		
Library Administration	X		
License Management	X		
MediaAgent Management	X		
Report Management	X	X	X
Storage Policy Management	X	X	
User Management			
Vault Tracker Operations	X		

Separate groups may provide this grouping of users more rights to other objects in the CommCell. This chart solely illustrates the ability to lock down capabilities for the applications to ensure that an entire volume is not inadvertently reverted with IntelliSnap integration.

Storage Policies

Managing proper retention on the snapshot copies becomes another critical requirement. Improper retention either increases the amount of tier 1 storage that is holding recovery points, or it causes the snapshots to fall short of fully meeting SLA requirements for the business. Simpana Storage Policies are broken down into copies for managing retention on the proper tier of storage. In the typical Storage Policy for IntelliSnap technology, three copies will be available, the primary snap copy, the primary backup to disk copy, and the offsite disk/tape copy. Properly meeting SLA requirements for the business requires proper alignment for the retention characteristics of each of the storage tiers. For example, SLAs for sub-24hr RPO/RTO drastically lower the returns on leveraging snapshot technology on copies beyond 48 hours.

The typical best practice for storage policy configuration will vary from environment to environment. The standard retention for the snap copy should align to the primary recovery SLA, with the backup to disk and tape copies providing SLA coverage for

complete site-based disasters. For example, with the previous description, retention may be set as follows to meet customer requirements:

- Primary SnapCopy – 2days & 0 Cycles, or number of snaps to cover 48 hours
- Primary Disk Copy – 28days & 1 Cycle
- Offsite Disk/Tape Copy – 60days & 1 Cycle

This definition allows snapshot retention on a 48-hour rotation, providing multiple high-speed recovery points on the array to meet the SLA requirement. This configuration requires sufficient storage space allocated to maintain two days' worth of changes for the associated clients. Note that when setting "cycles" to 0, the removal of old snapshots occurs regardless of success, so proper alerting and monitoring is required.

Another recommended option for snap copy retention sets the "days" variable to 0 and focuses solely on the Number of cycles. In this configuration full backups must occur frequently to allow for proper snap management. With this setup, the number of snapshots retained will be determined based on the number of cycles configured. The scheduled frequency becomes very important to defining the environment conditions. Assume a cycle consists of eight snapshots. If those eight snapshots execute over a week timeframe, then 7 days of delta change must be available in the Array configuration. If the eight Snapshots execute in a 48-hour period, only 48 hours of delta change must be available in the Array configuration. Fully understanding the schedule and process configurations enables making the proper retention setting when keying off of "cycles." Improperly setting retention and effects of days and cycles can adversely affect the available recovery scenarios for the business applications.

The other recommended option for snap copy retention sets a specific number of snapshots to retain, regardless of days and cycles. This configuration aligns best to storage teams' practices. If retention is set to eight snapshots, eight snapshots will always be retained, regardless of how long it takes to reach eight. It is therefore important to understand the rate of change for the application to determine how much delta change must be accounted for. It is also important to note that because cycles are not factored it is possible to end up with an incomplete cycle in a snap-only scenario, so secondary copies on disk or tape are recommended with this option.

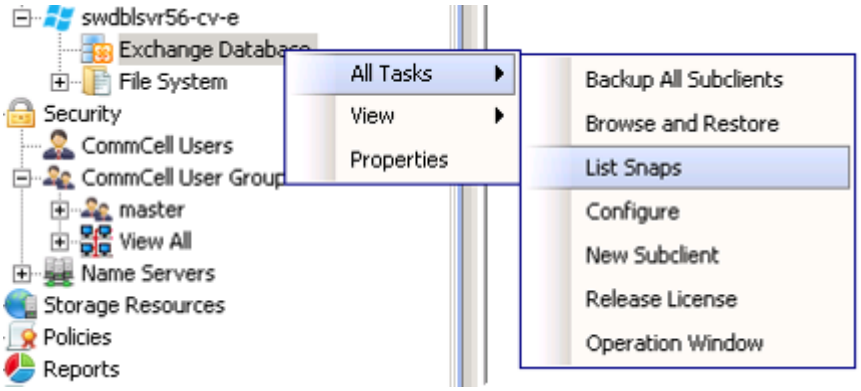
This definition will then enable the Primary and Secondary backup to disk and tape copies. Backup Copies should follow a standard backup schedule for the production (i.e. daily backups should equate into at least one Snap Copy Point in time to drive local and offsite backups). Remember, backup copies will execute synchronously, and the failure to "backup" Snap Copies to disk/tape will extend the storage requirement on the Array, as snapshots selected for Backup Copy will not prune until they are moved to disk/tape. Application data will always be consistent on this data movement. Backup Copy operations will always use File System mechanisms to protect the properly quiesced applications, except in the instance of RMAN proxies in an Oracle configuration. The rest of the copies in the storage policy follow the standard days and cycles rules for data aging.

Snapshots should not be deleted from the array outside of Simpana software's control, but there are situations where this might happen. Snapshots may be deleted from the array due to factors like low disk space on the array, number of snapshots exceeds the threshold etc., and the jobs corresponding to these deleted snapshots can no longer be used for any data recovery or backup copy operations. Simpana can be configured to reconcile differences between the available snapshots on the array and records in the database. With the nRunSnapRecon registry key set, snap reconciliation will execute once every 24 hours to check for missing snapshots and mark any jobs corresponding to the missing snapshots as invalid. See Appendix for detailed information.

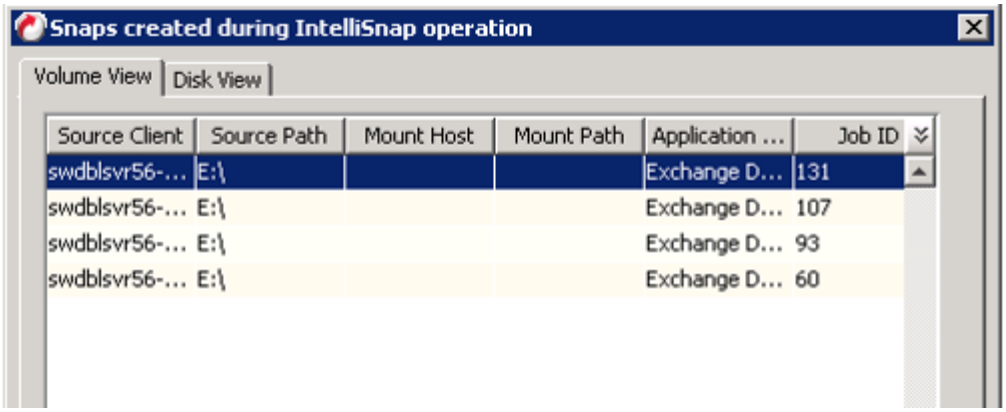
Manipulating Snapshots

Part of the value of creating and leveraging snapshots is the flexibility it provides IT for typical tasks by calling on the high speed storage infrastructure. Out of place refresh, single file recoveries, mount and browse capabilities, etc. accelerate daily IT operations. The following sections describe how to perform these operations for hosts protected with IntelliSnap technology.

1. Snapshot access is always achieved via right clicking on your defined object and selecting the **All Tasks** option and selecting **List Snaps**

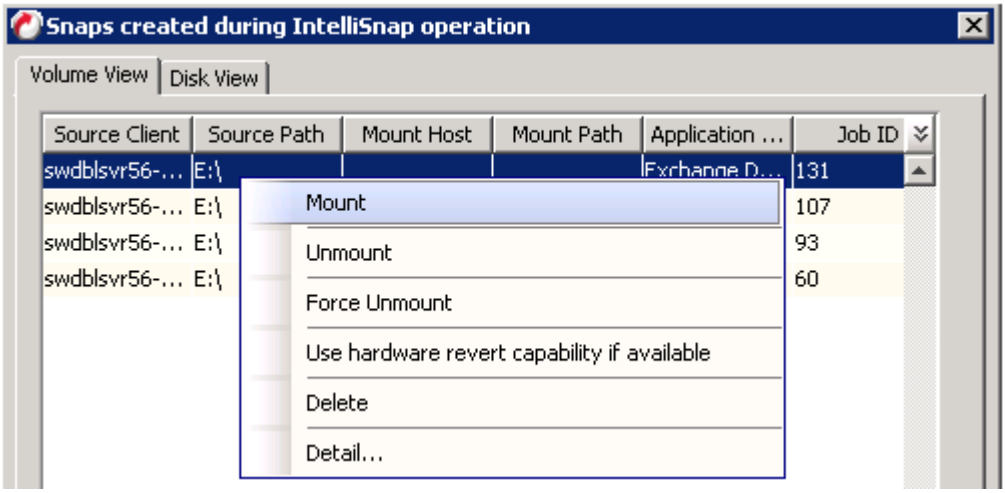


2. The snapshot list for the client application is displayed when the List Snaps item is selected. From the dialog several snapshot operations are available.

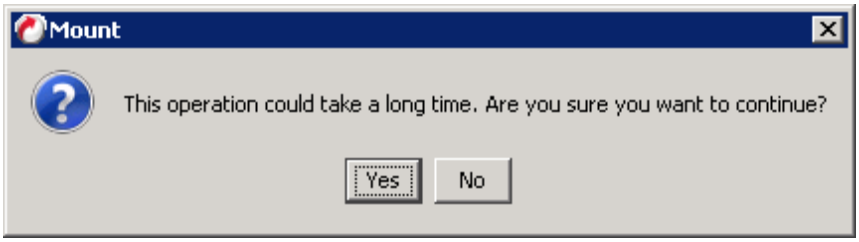


Mount/Dismount Snaps for Manual Browse

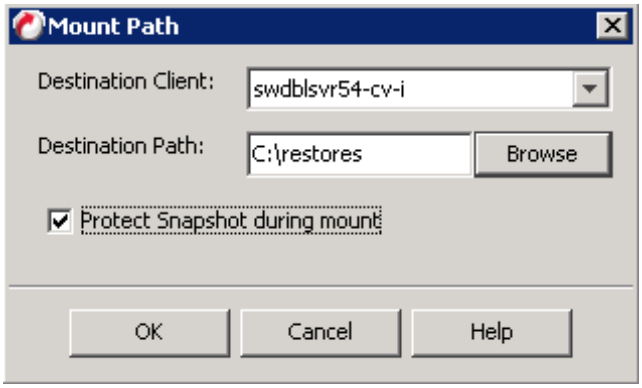
1. After accessing the available snapshots for the selected client, mount the desired snapshot by a right click on the snapshot shown in the menu. Select the mount operation to continue.



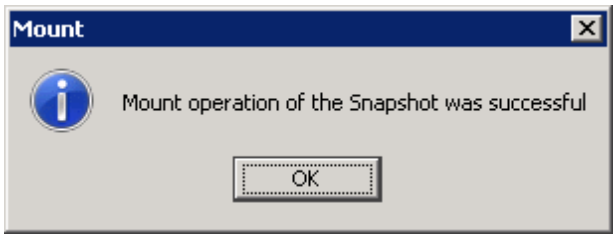
2. The following dialog appears. Click "Yes" to continue. On Pure Storage arrays the mount time rarely will exceed 1 – 2 minutes.



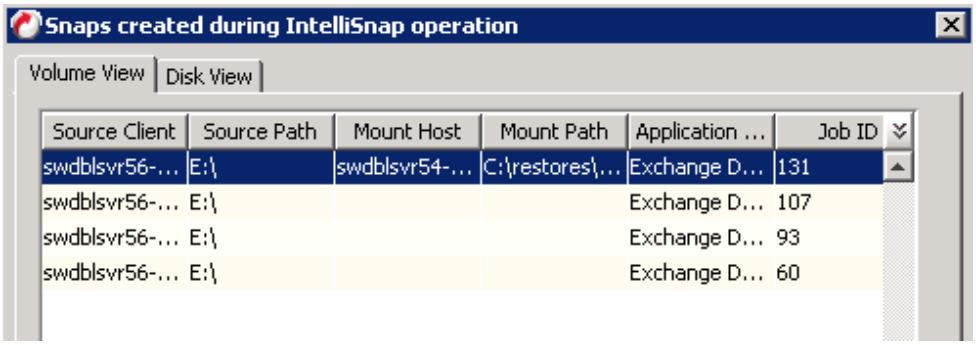
3. Define the host you wish to mount the snapshot to (this must be a MediaAgent with a similar OS to the source). Ensure the host has the appropriate Storage Zoning to mount this snapshot. If this is an iSCSI volume log in the initiator for this host if not already done, otherwise the mount will fail. For Destination Path, enter or browse to a mount point. This must be a folder, and is recommended to be empty folder.



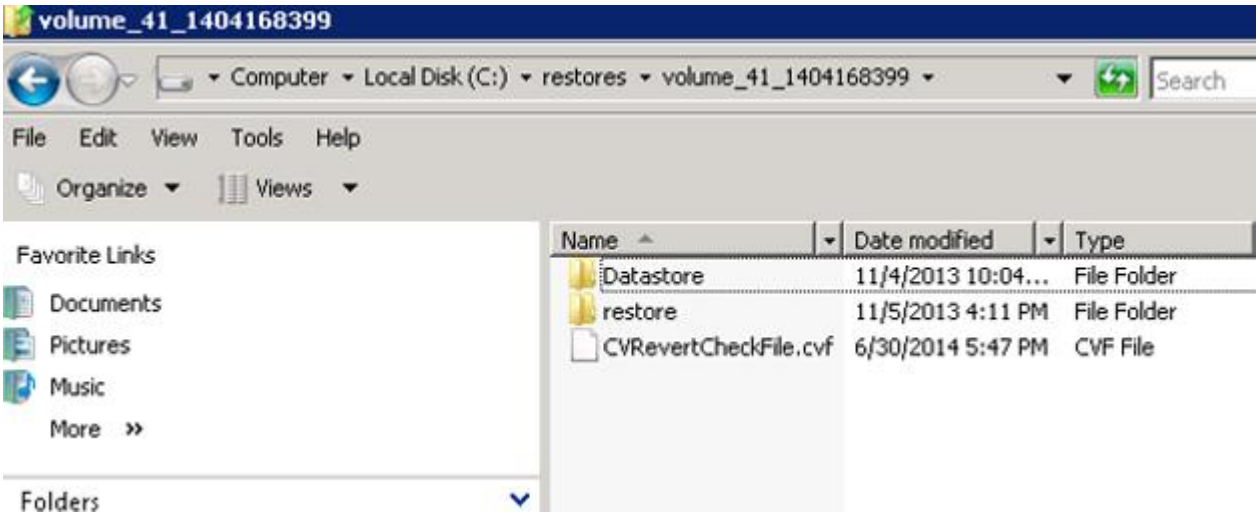
4. Once the snapshot is mounted the following dialog will appear. Click OK.



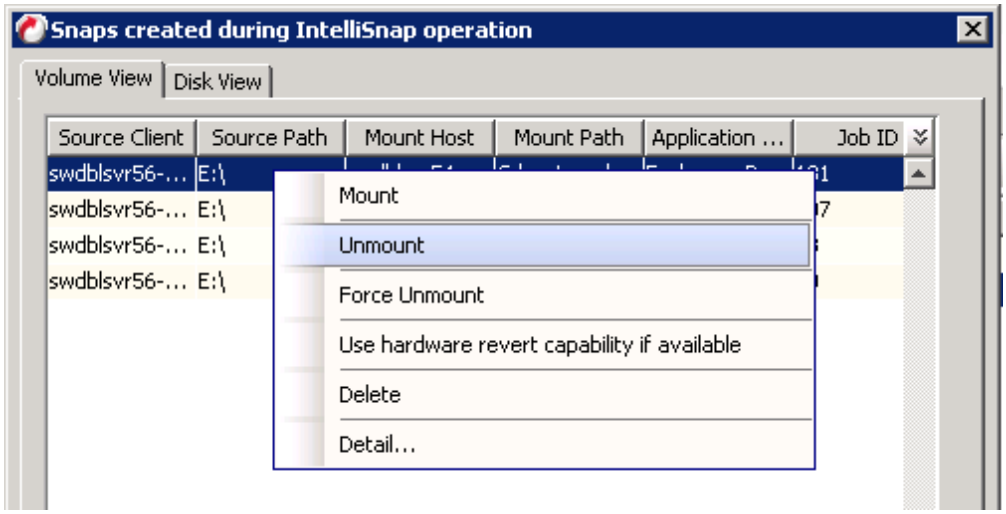
5. The Snapshot list updates with the current information on the snap which will include the mount path and the updated time of the mount operation.



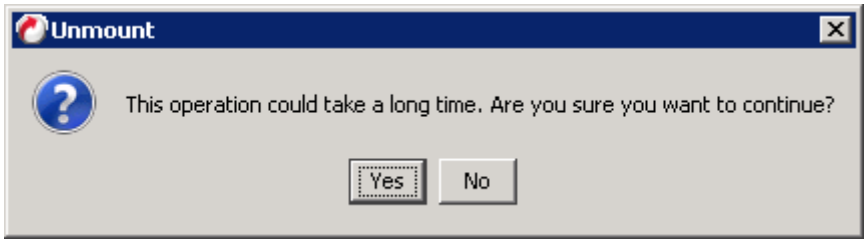
6. The mounted snapshot can now be accessed from the mount host.



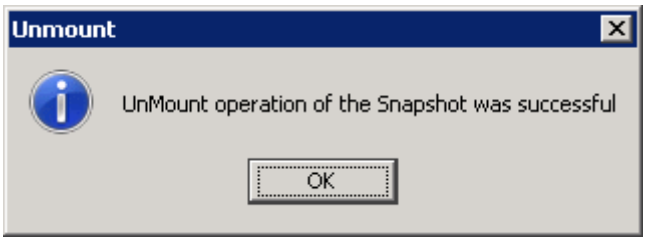
7. Dismount of the snapshot is a simple process. Select the mounted snapshot and use the right click menu to select the Unmount option.



8. The following dialog will appear. Click OK to continue.



9. Once completed the following dialog will appear.



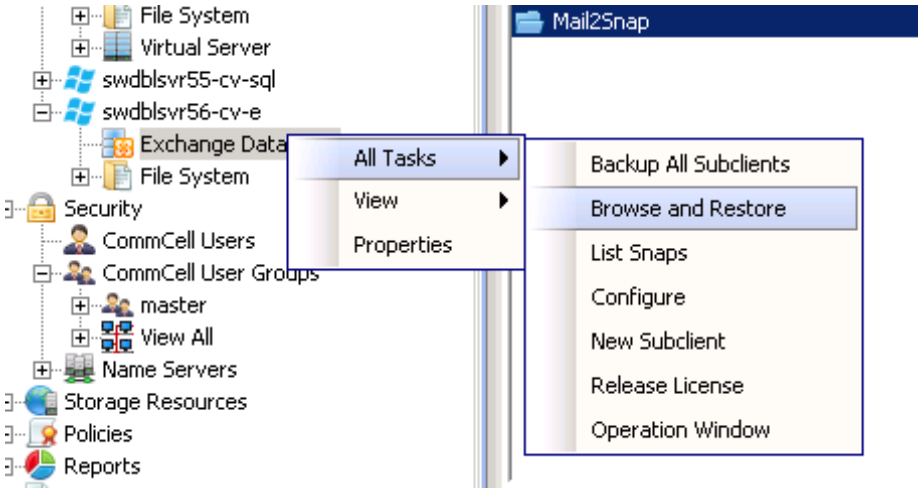
It is important to remember to dismount the snapshot once finished. If a snapshot has been manually mounted it will not be pruned until it no longer is being accessed.

Reverting a Snapshot

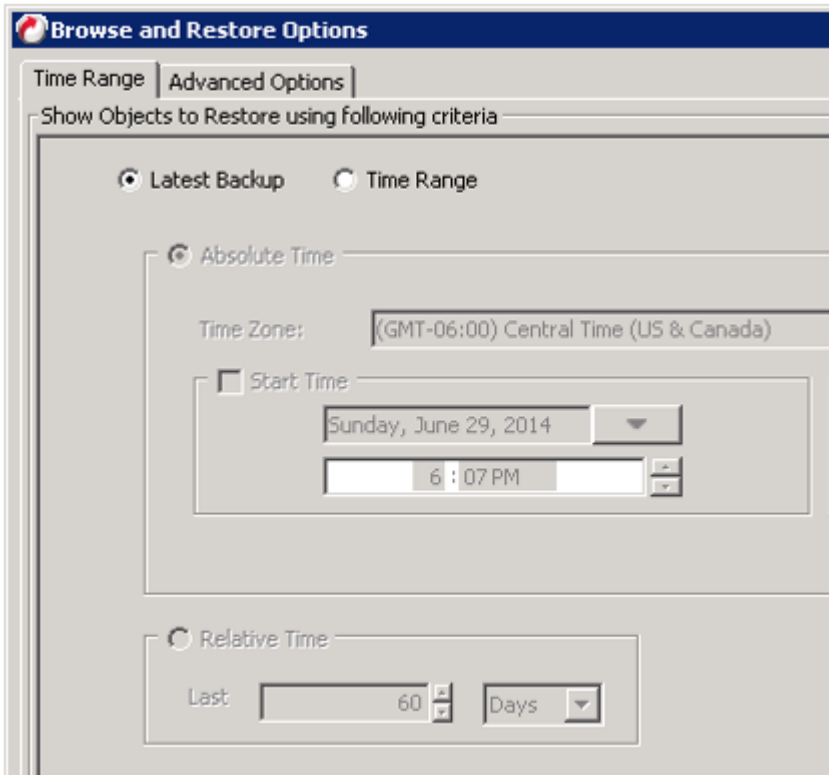
There are two ways to revert a snapshot. One is application aware and one is not. Generally the application aware revert is the mechanism to use.

Application-aware Revert

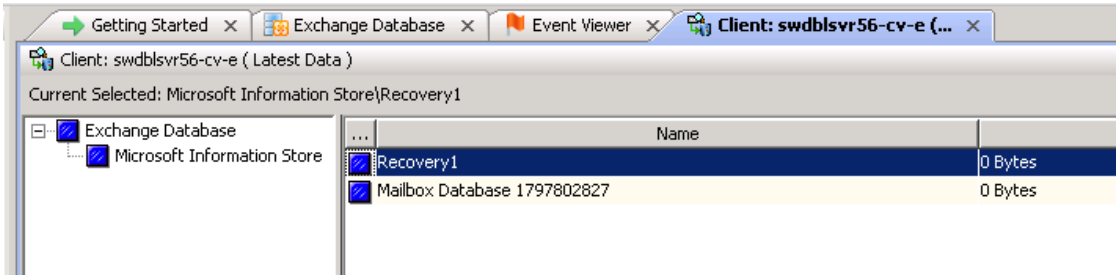
1. An application-aware revert is done in the context of a standard recovery. This starts with browsing for the application data to be restored. Click the **All Tasks** menu item, then select **Browse and Restore**.



2. The backup selection dialog appears to choose the time frame from which the restore will take place.
3. Here the latest backup will be used. Click **View Content**.

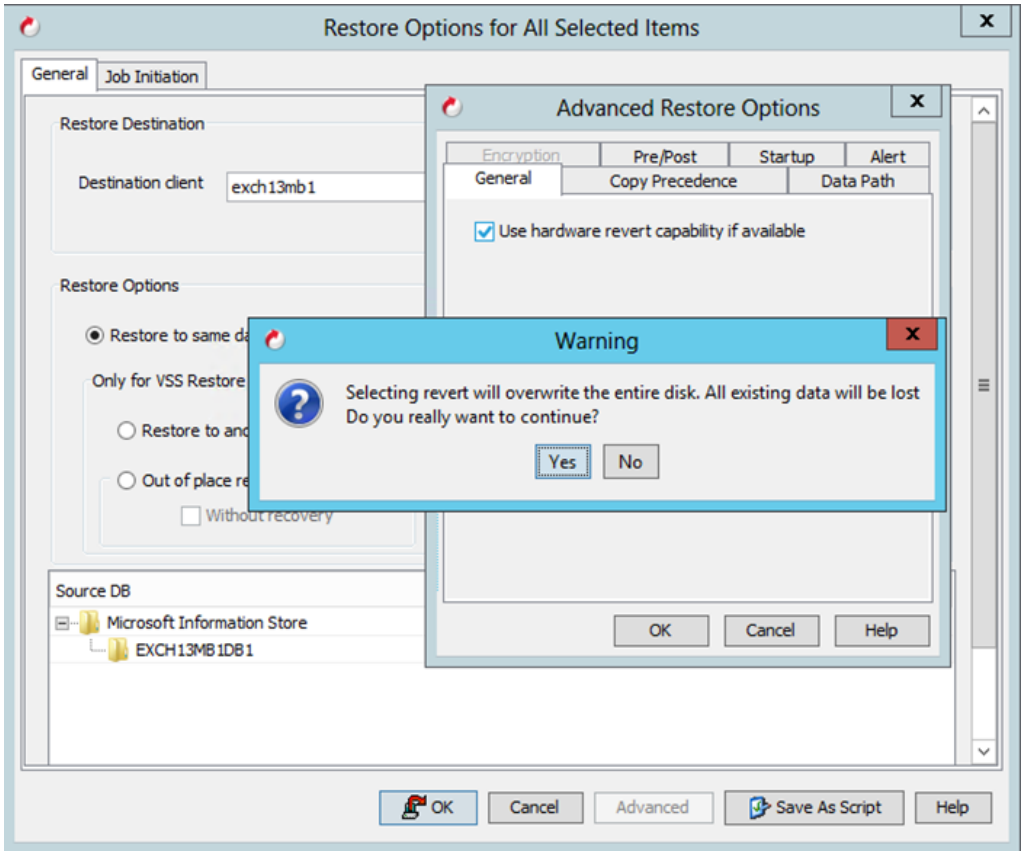


4. The browse window will appear from which the appropriate application data can be selected for restore. Select all the content contained in the snapshot(s) being reverted; the revert may fail if not all content is selected. Click the **Recover All Selected** button.

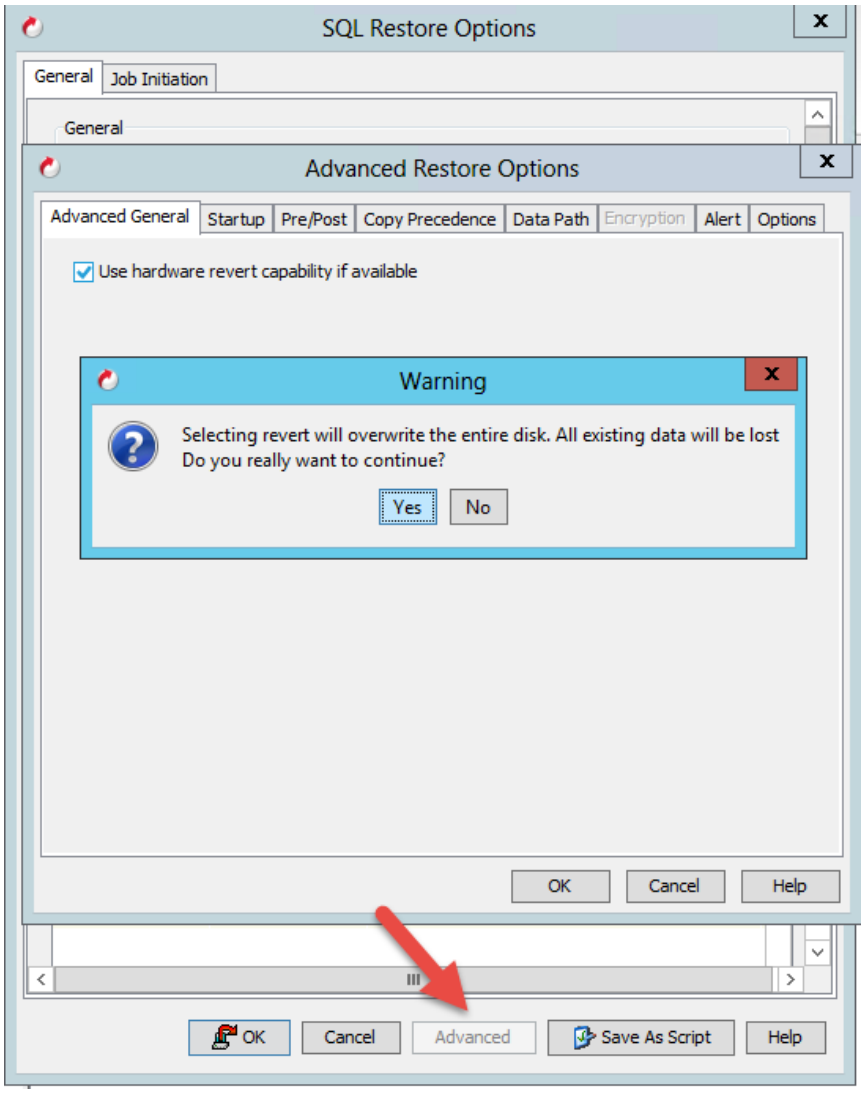


5. The Recovery dialog box appears. Click the **Advanced** button to open the Advanced Restore Options dialog. The dialog will vary based on the application type.

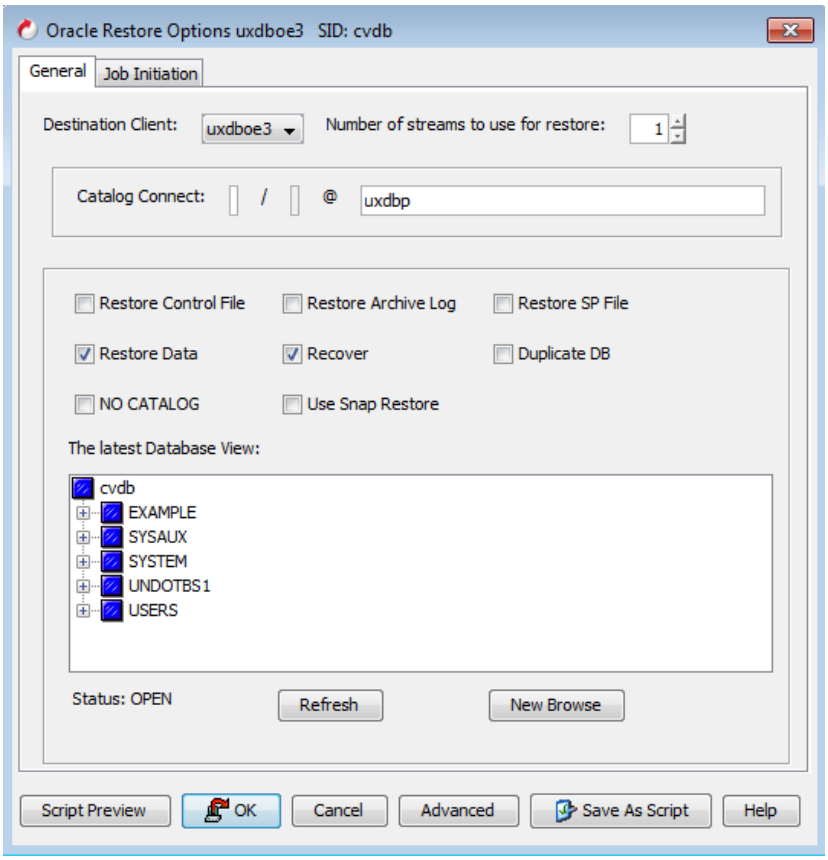
For Exchange:



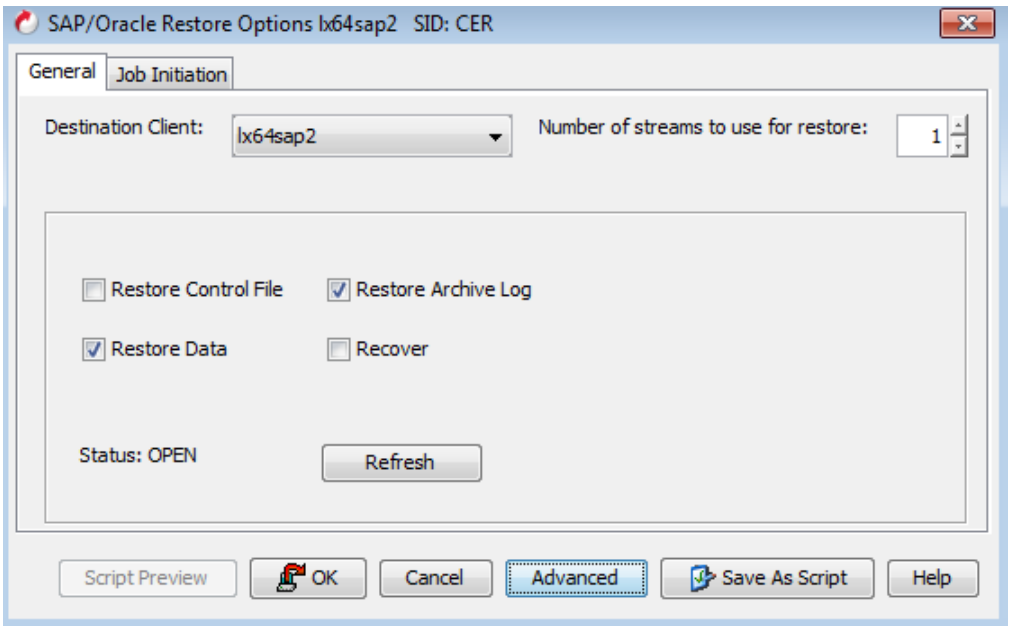
For SQL:


SQL Restore Options
General
Job Initiation
General
Advanced Restore Options
Advanced General
Startup
Pre/Post
Copy Precedence
Data Path
Encryption
Alert
Options
Use hardware revert capability if available
Warning
Selecting revert will overwrite the entire disk. All existing data will be lost
Do you really want to continue?
Yes
No
OK
Cancel
Help
OK
Cancel
Advanced
Save As Script
Help

For Oracle:

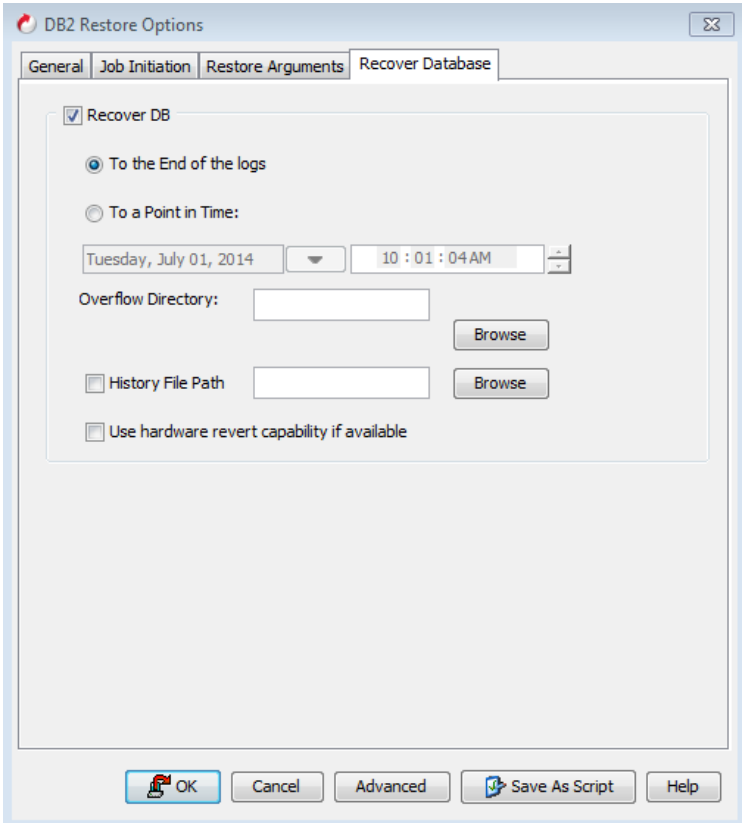


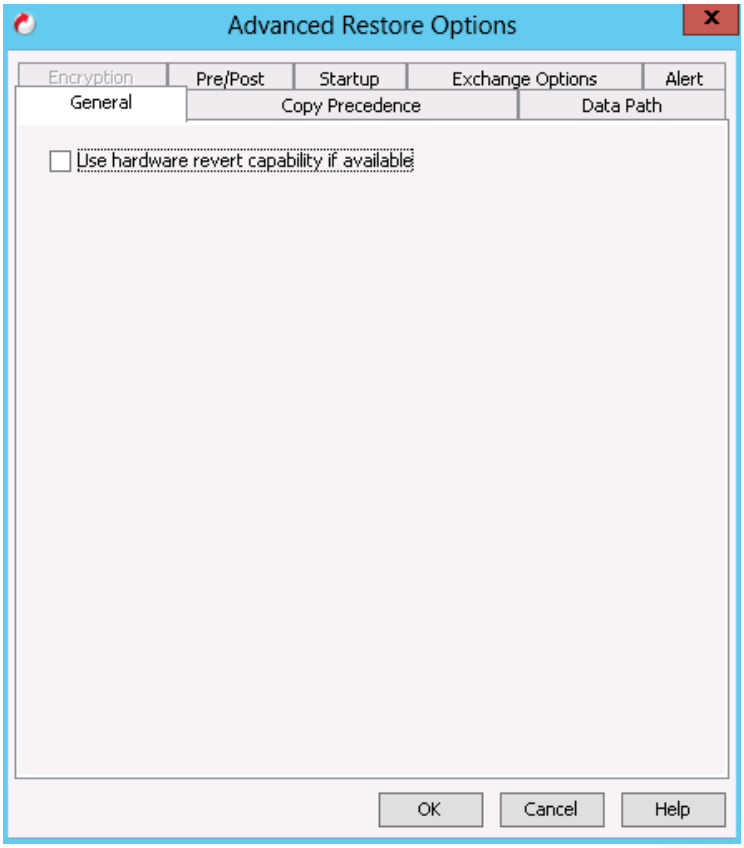
For SAP Oracle:



For DB2

The "use hardware revert" option is on the "Recover Database" tab of the DB2 Restore Options dialog box:





This will execute a LUN revert from the latest snapshot back to the production server.

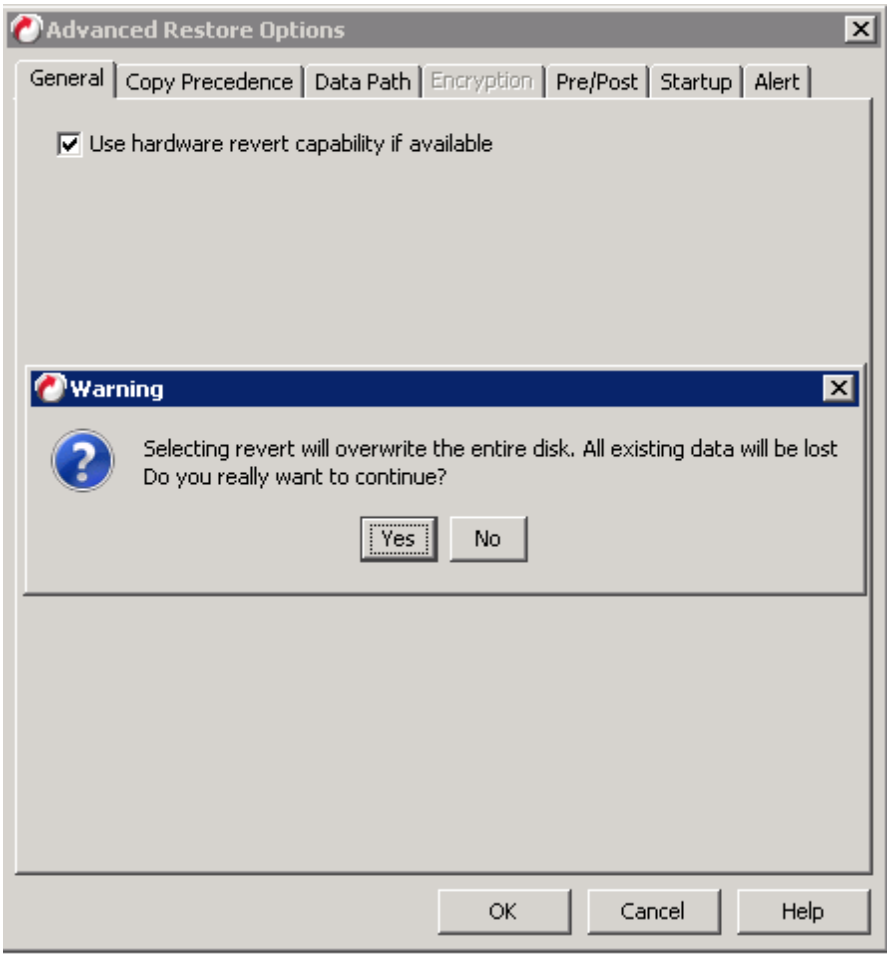
DB2 Snapshot Revert Considerations

You can use the revert operation to bring the data back to the point-in-time when the snapshot was taken. This operation overwrites any modifications to the data since the time when the snapshot was created. This option is only available if the storage array that you are using supports revert. You can either perform an application aware revert or a hardware specific revert. We recommend you to use an application aware revert.

Review the following before performing a revert operation:

- It is recommended to perform an application aware revert operation to prevent a possible loss of data.
- Log revert is not supported.
- Make sure the volume is not being used during the revert operation.
- Revert operations are not supported on Windows clusters.
- Ensure that the online log files and their mirror log files reside on the same array volume.
- After a revert operation is completed successfully, the roll forward to end of logs will be performed by default. The revert operation will include all the latest logs that are recovered to the current database status. If you want to revert the DB2 snap to a point-in time, you have to select the roll forward and log point-in-time.
- On Windows clients, disable automount using the following command:
- diskpart> automount disable
- On UNIX clusters, use pre/post scripts to freeze and unfreeze the cluster for revert operations. For example, on Red Hat Linux cluster, use the following command in the pre/post scripts:
- clusvcadm -Z <group> to freeze the cluster
- clusvcadm -U <group> to unfreeze the cluster
- This is required because during revert the application is shut down and corresponding volumes are unmounted. In that case, the cluster will automatically failover to another node thus preventing the revert operation.
- It is recommended to verify the contents of the backup and ensure that you want to perform a revert operation as it is an irreversible operation.
- If you plan to perform a revert operation, you will not be able to use the associated storage policy for further auxiliary copy operations.

6. Click Yes to the warning dialog to proceed with the revert operation. Click OK to close the dialog and OK again to start the recovery.



This will execute a LUN revert from the latest snapshot back to the production server.

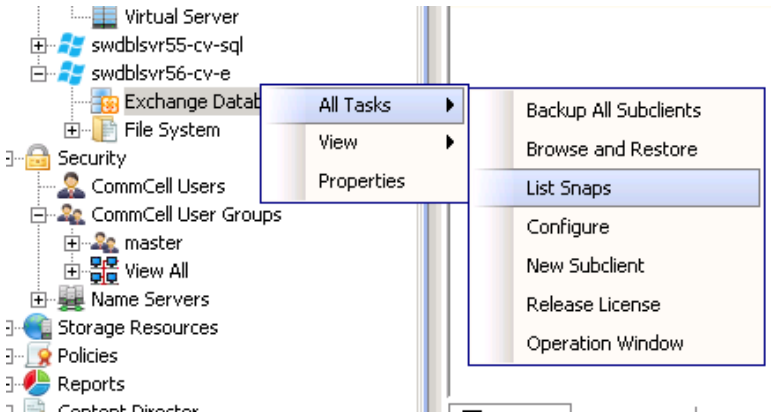
Some Applications require an overwrite option for any restore to occur, including LUN-based reverts. Ensure applications like Exchange and others have the appropriate "overwrite" settings defined for this to execute properly

Note: ALL FILES and DATABASES on the LUN will be rolled back to the point in time of the snapshot. DO NOT REVERT UNLESS ALL DATA REQUIRES TO BE ROLLED BACK TO THE PREVIOUS POINT IN TIME

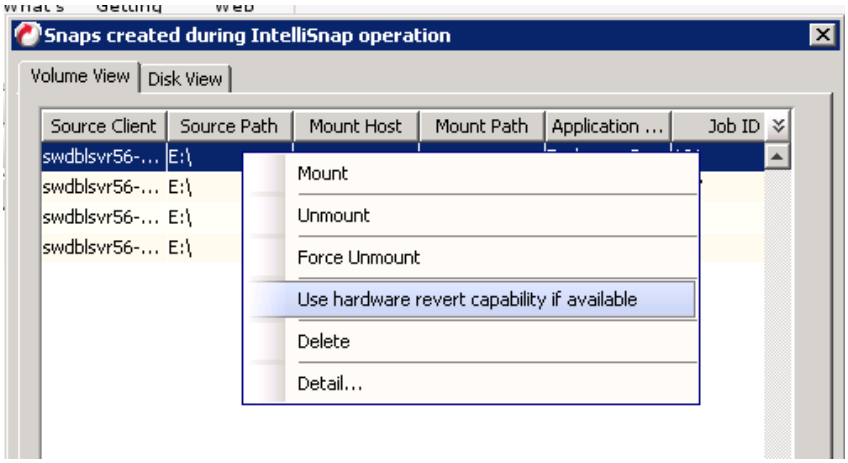
Hardware-specific Revert

A hardware revert can also be performed without application awareness. This is done directly from the snapshot list. This process initiates a rollback for the selected volumes instantly to the desired point in time, but without communicating with applications for a graceful restore. This option may be leveraged for file systems and application environments that have been shut down.

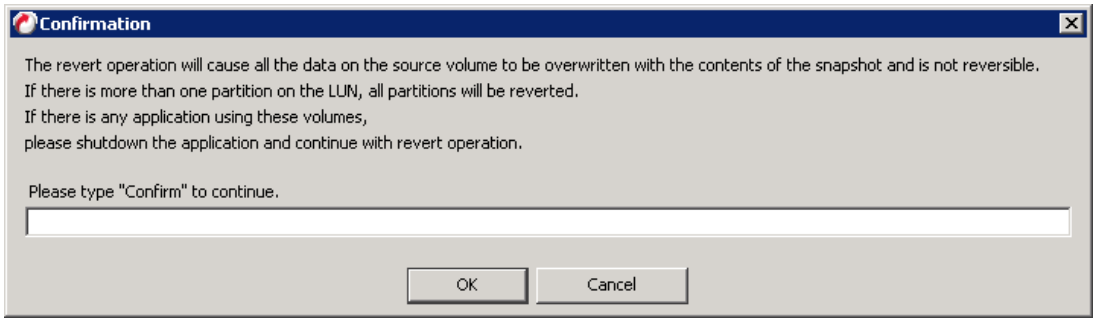
1. The process begins by selecting the List Snaps menu item to bring up the list of snapshots dialog.



2. When the dialog appears, select the desired snap and use the right click menu to select the "Use hardware revert …" option to revert the snap. The following confirmation dialog will appear.



3. Validate this operation is correct and type "Confirm" in the dialog box and click OK to perform the operation.

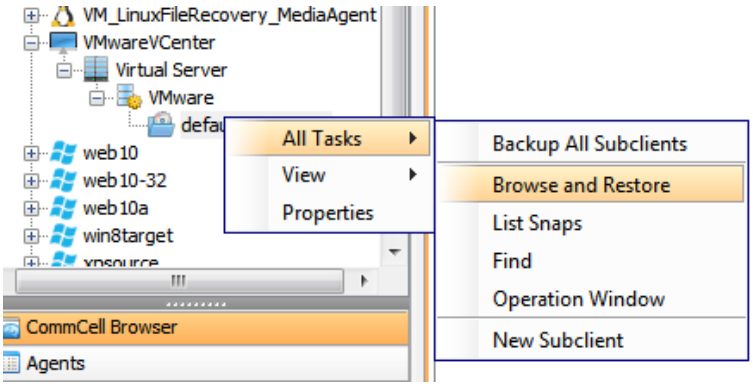


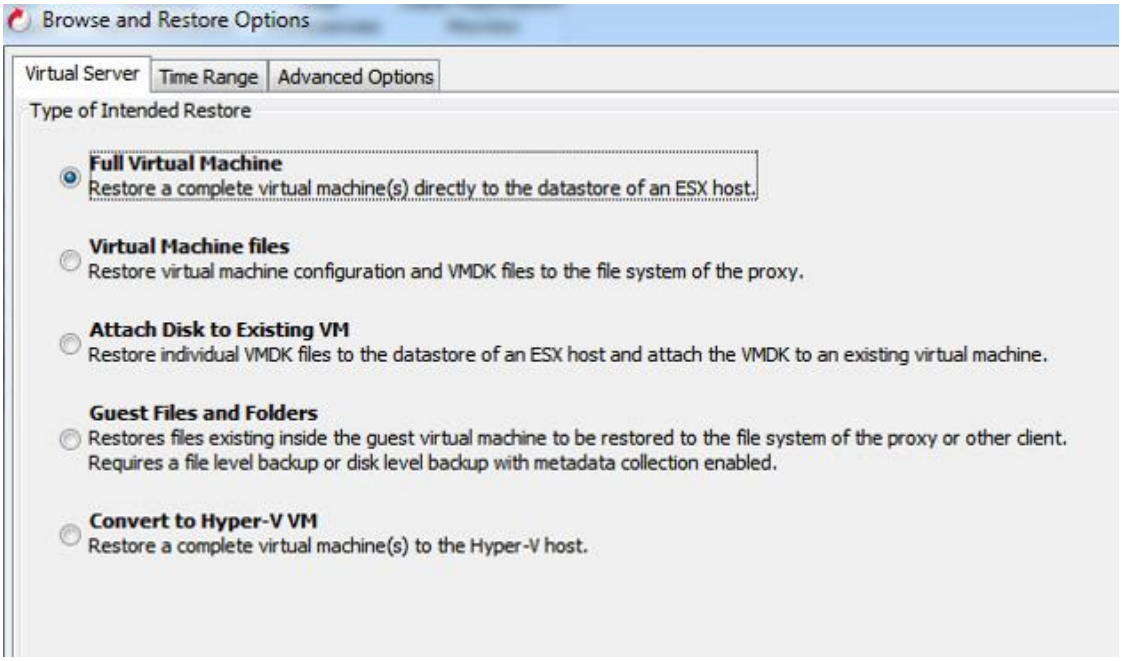
Caution should be taken when using the non-application aware revert functionality as you can corrupt a running application because of this operation. You should be sure that you will not cause any data corruption issues before using this option.

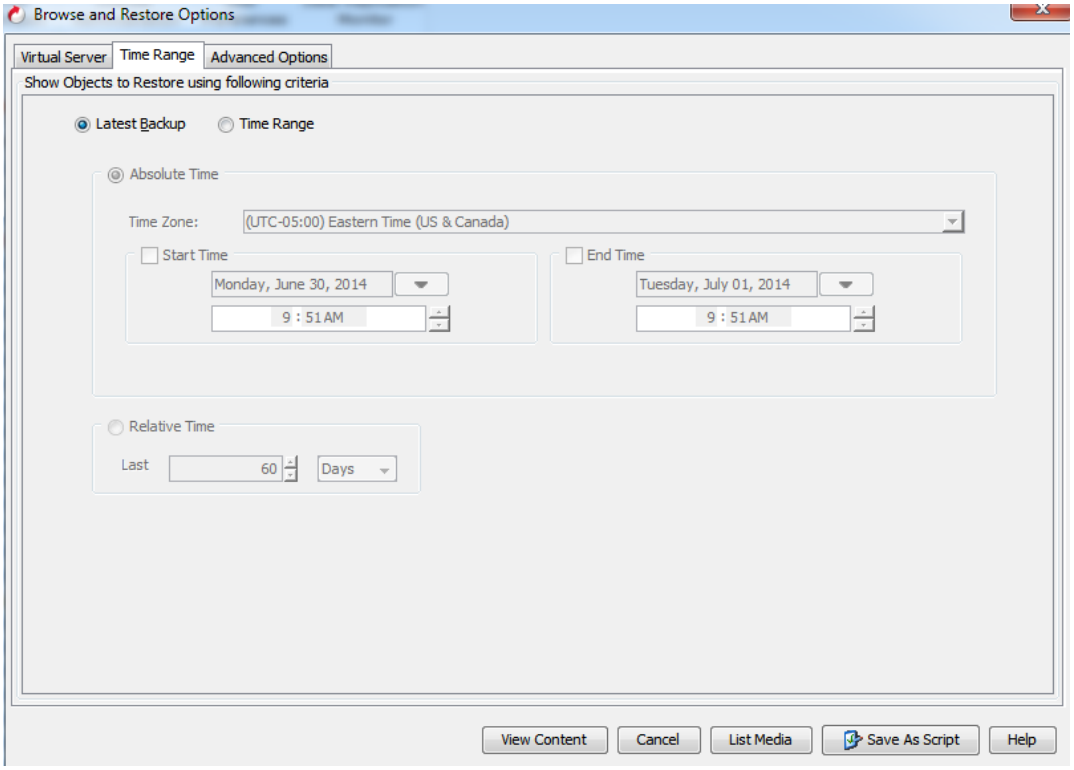
Out of Place Restore – VMware Example

Snapshots can be used for recovery out of place just like any other media based backup. LAN and LAN-free recovery are both supported. For LAN-free recovery the target must have access to the array hosting the snapshots, and MediaAgent and any required iDataAgent software must be installed.

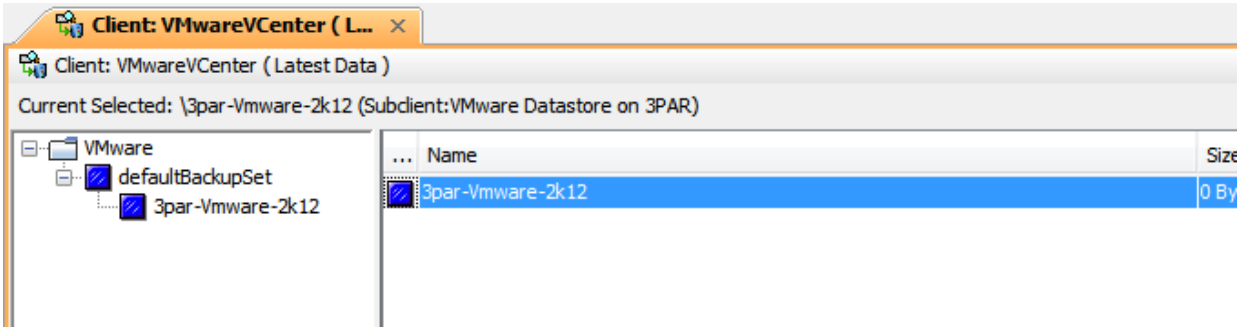
1. To restore out of place, select the **Browse and Restore** option for the desired data set. Select the appropriate time or the latest backup. For some agent types, primarily virtualization, you will also need to choose the type of restore.


VM_LinuxFileRecovery_MediaAgent
VMwareVCenter
Virtual Server
VMware
web10
web10-32
web10a
win8target
CommCell Browser
Agents
All Tasks
View
Properties
Backup All Subclients
Browse and Restore
List Snaps
Find
Operation Window
New Subclient

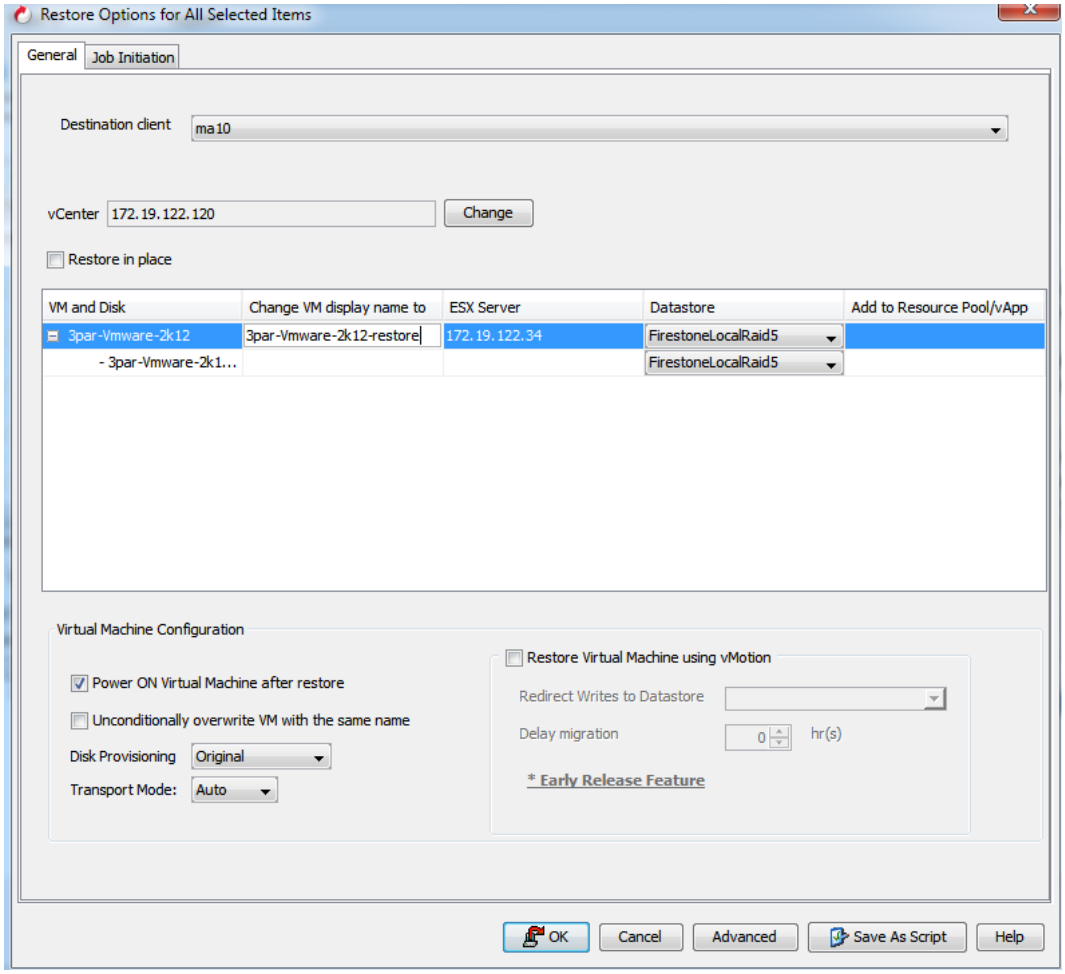

Browse and Restore Options
Virtual Server
Time Range
Advanced Options
Type of Intended Restore
Full Virtual Machine
Restore a complete virtual machine(s) directly to the datastore of an ESX host.
Virtual Machine files
Restore virtual machine configuration and VMDK files to the file system of the proxy.
Attach Disk to Existing VM
Restore individual VMDK files to the datastore of an ESX host and attach the VMDK to an existing virtual machine.
Guest Files and Folders
Restores files existing inside the guest virtual machine to be restored to the file system of the proxy or other client.
Requires a file level backup or disk level backup with metadata collection enabled.
Convert to Hyper-V VM
Restore a complete virtual machine(s) to the Hyper-V host.



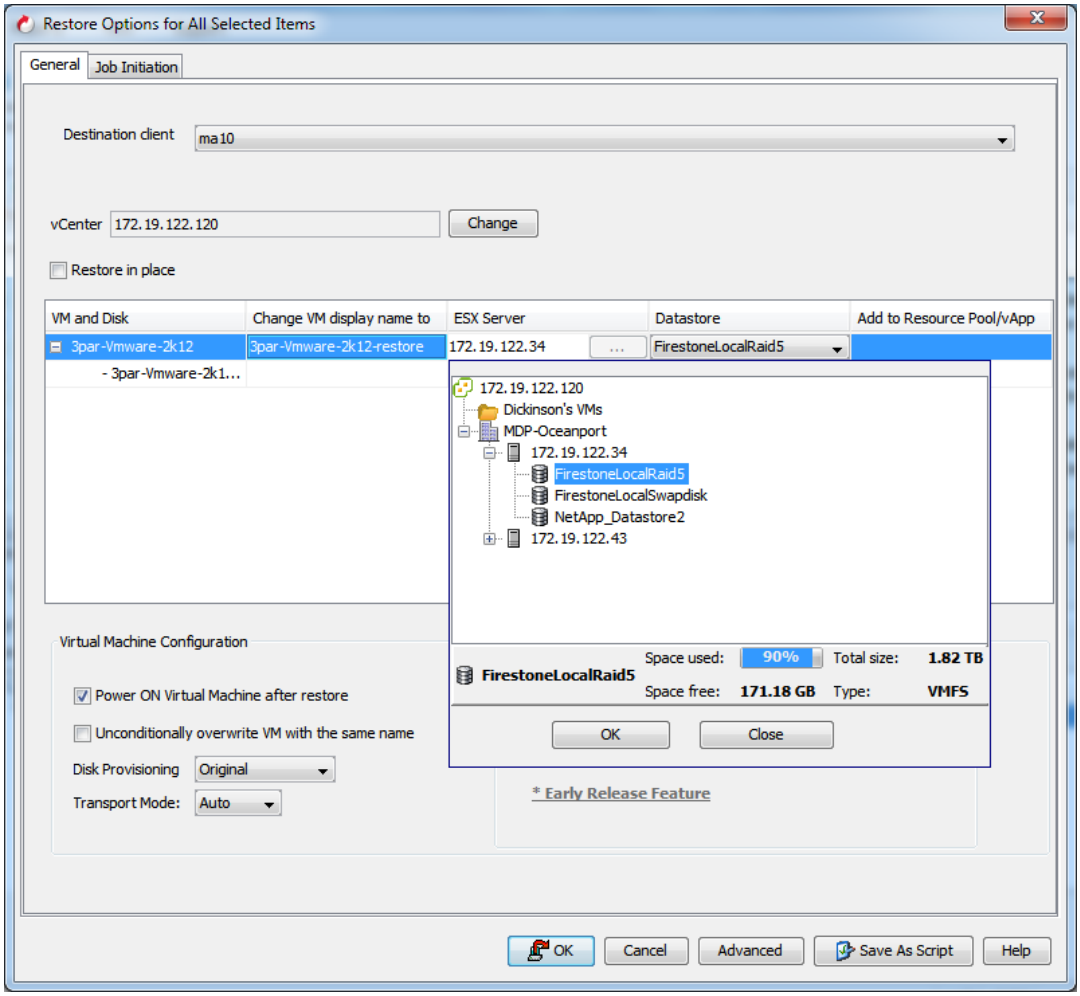
2. Depending on the application different options are available for out of place restore. Browse into the Subclient contents and select the data to be recovered out of place. In this case the selection is a virtual machine.



3. When the **Recover All Selected** button is clicked the following dialog appears to direct the restore activity. Note the VM Name. A variety of options is available for out of place restore, including changing the VM display name, ESX host, or Datastore. You can also change vApp and resource pool membership, provisioning policy, and transport mode. The VM can be powered on automatically after restore by checking the **Power ON Virtual Machine after restore** box.



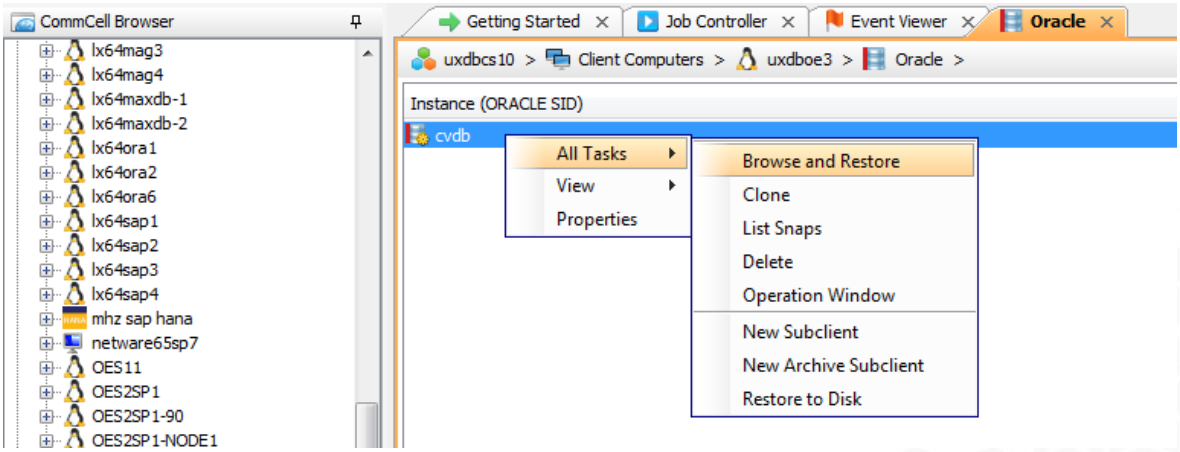
4. Clicking the browse (…) button in the **ESX Server** field provides out of place selections. Here FirestoneLocalRaid5 on ESX server 172.19.122.34 is the location for the VM recovery. Select OK, and then OK again on the Restore Options windows to execute the recovery, out of place.



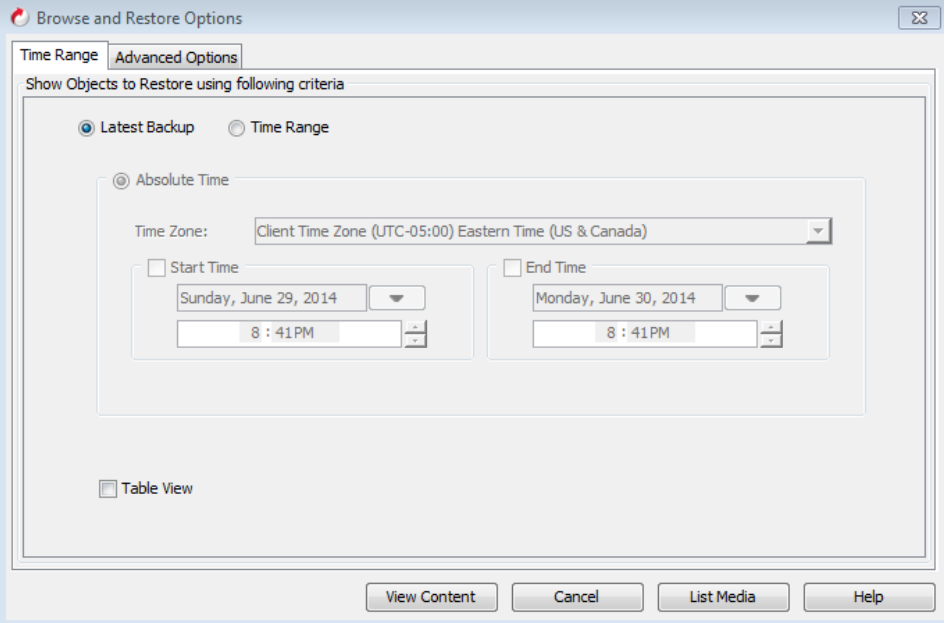
Out of Place Restore – Oracle Example

Snapshots can be used for recovery out of place just like any other media based backup. LAN and LAN-free recovery are both supported. For LAN-free recovery the target must have access to the array hosting the snapshots, and MediaAgent and any required iDataAgent software must be installed.

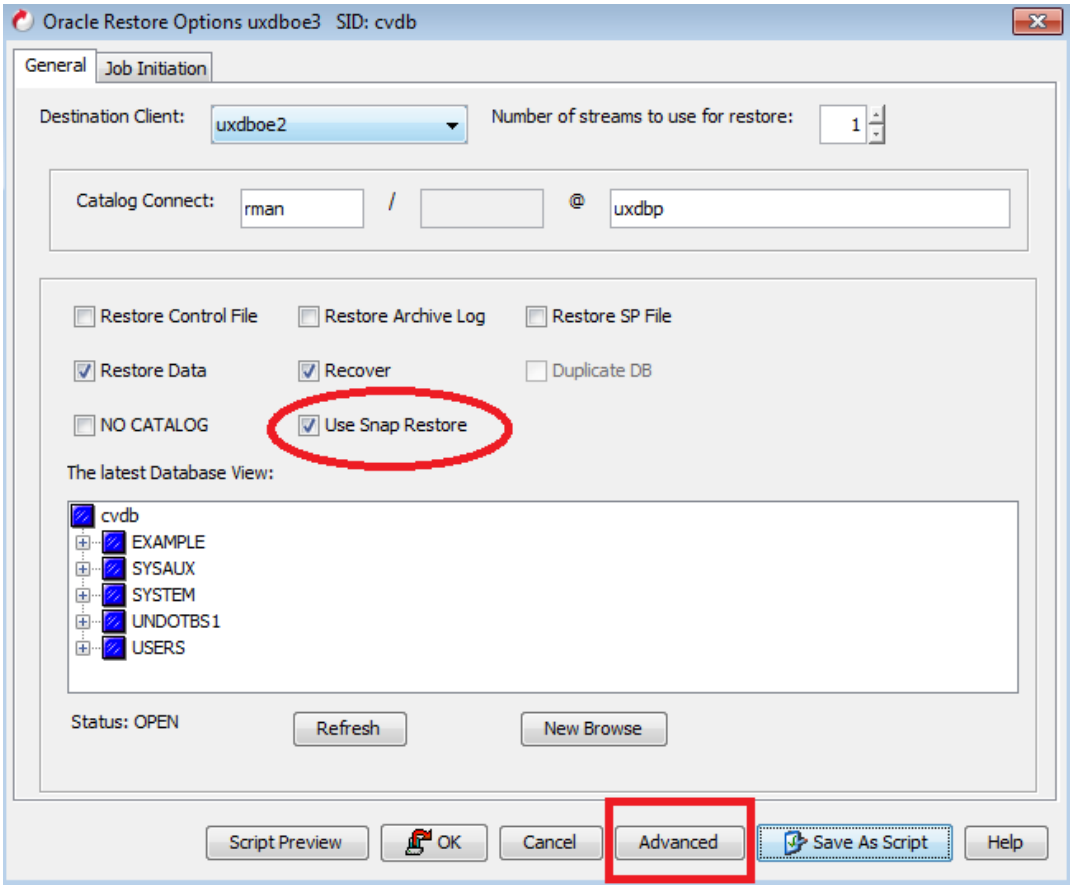
1. To restore out of place select the Browse Backup Data option for the desired data set, select "All Tasks" > "Browse and Restore" when right-clicking the desired Oracle database instance. Select the appropriate time or the latest backup.



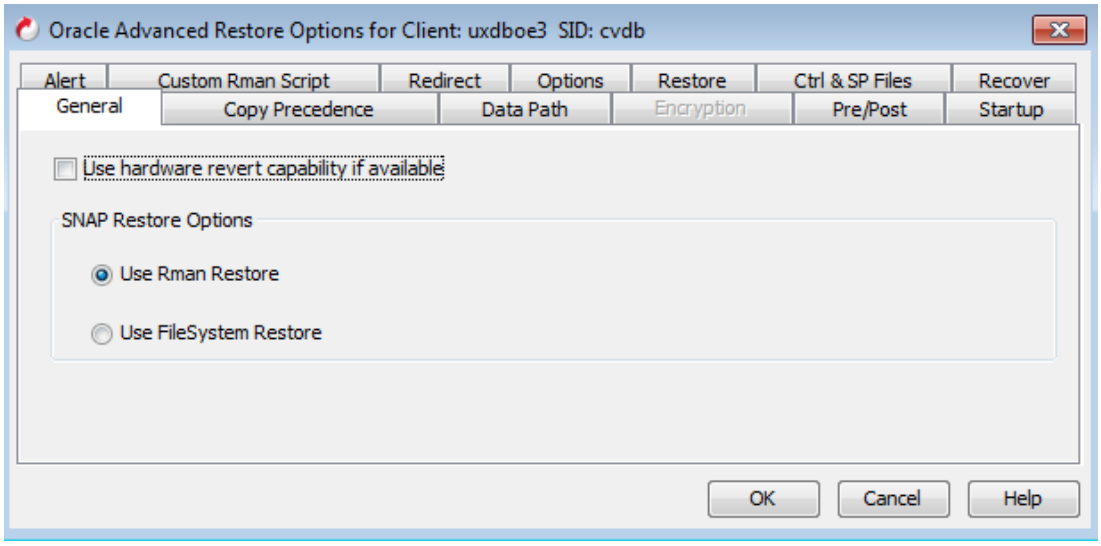
2. Select either latest backup or the desired time range to restore from and click "View Content":



3. Enable the "Use Snap Restore" checkbox as shown in below and then select the "Advanced" button:



4. In the advanced tab, the choice to use RMAN or File System methods for restoring the database is given, along with all of the usual RMAN restore options that are available during a non-snap Oracle iDA restore:

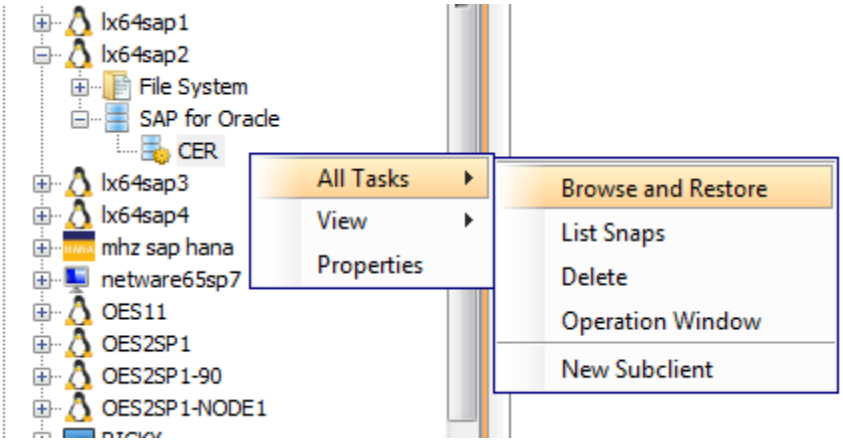


Out of Place Restore – SAP Oracle Example

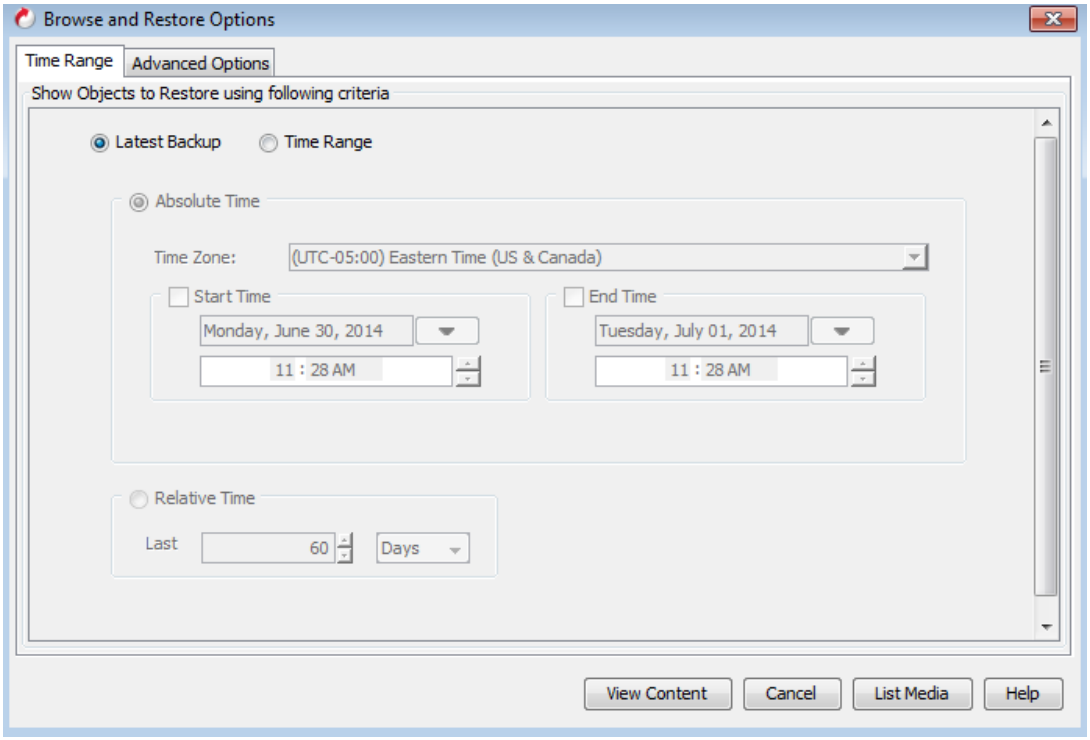
Snapshots can be used for recovery out of place just like any other media based backup. LAN and LAN-free recovery are both supported. For LAN-free recovery the target must have access to the array hosting the snapshots, and MediaAgent and any required iDataAgent software must be installed.

For SAP Oracle restores, copy precedence governs which copy (snap vs. backup) is used for the restore. To choose the desired copy for restore, perform the following steps:

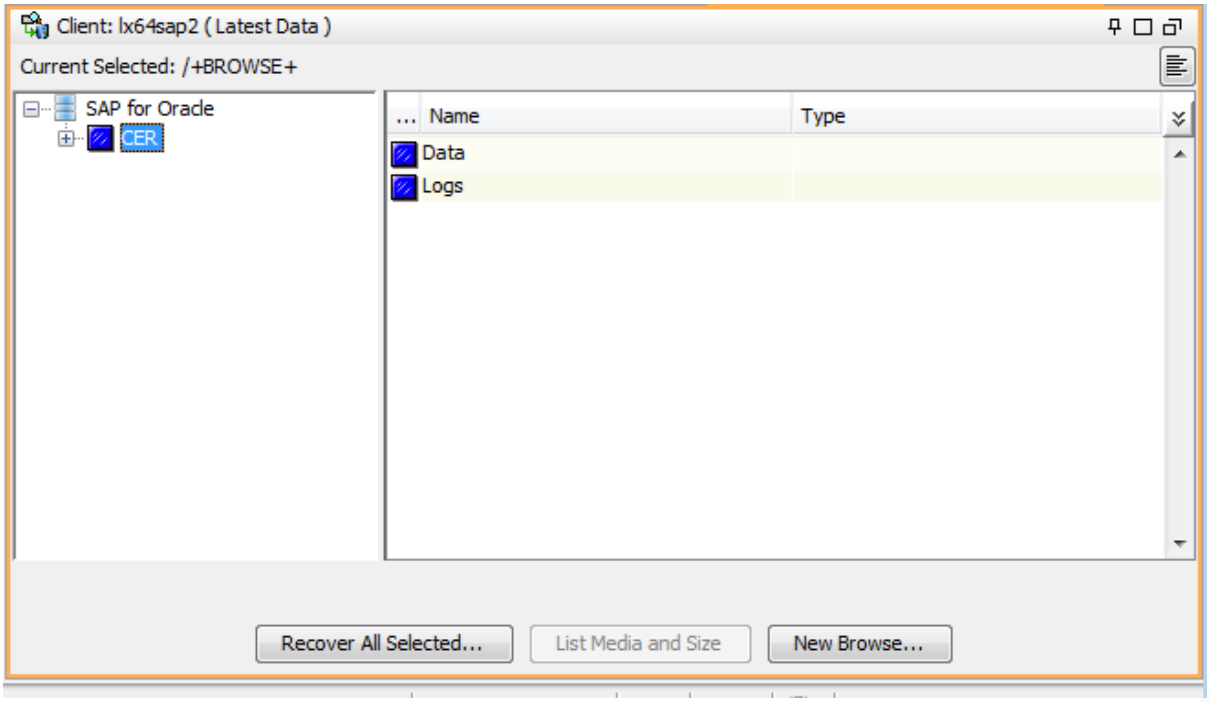
5. Right-click the entity that contains the snapshots you want to restore, and point to **All Tasks | Browse and Restore**.



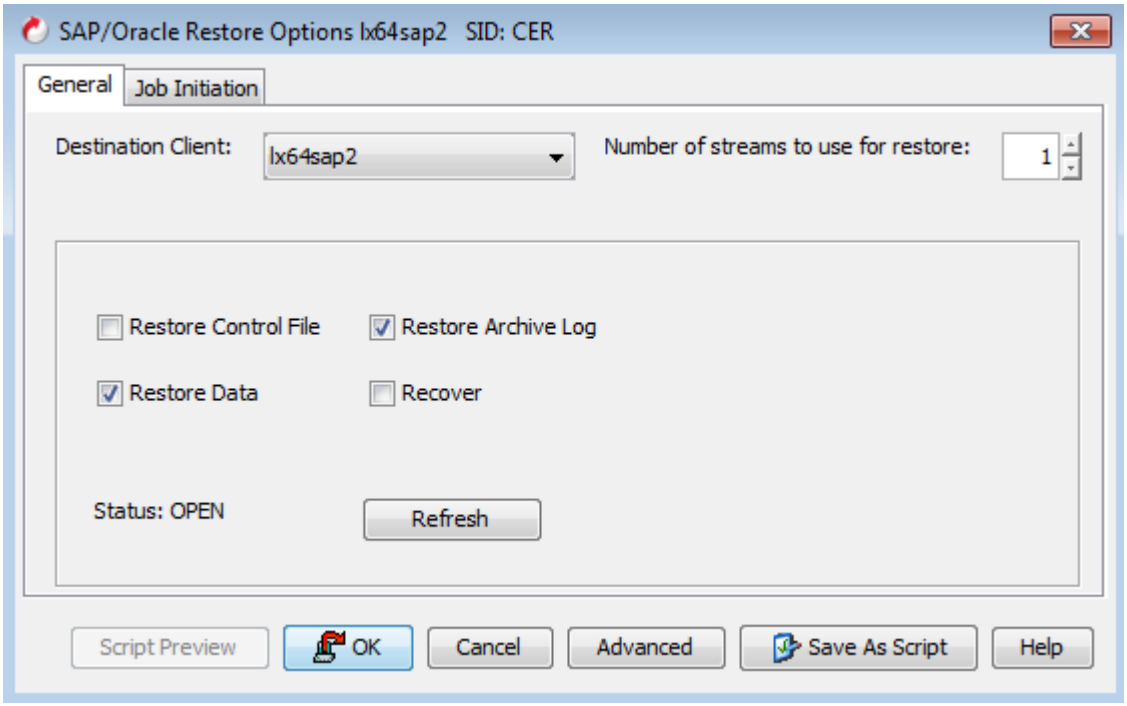
6. Click View Content.



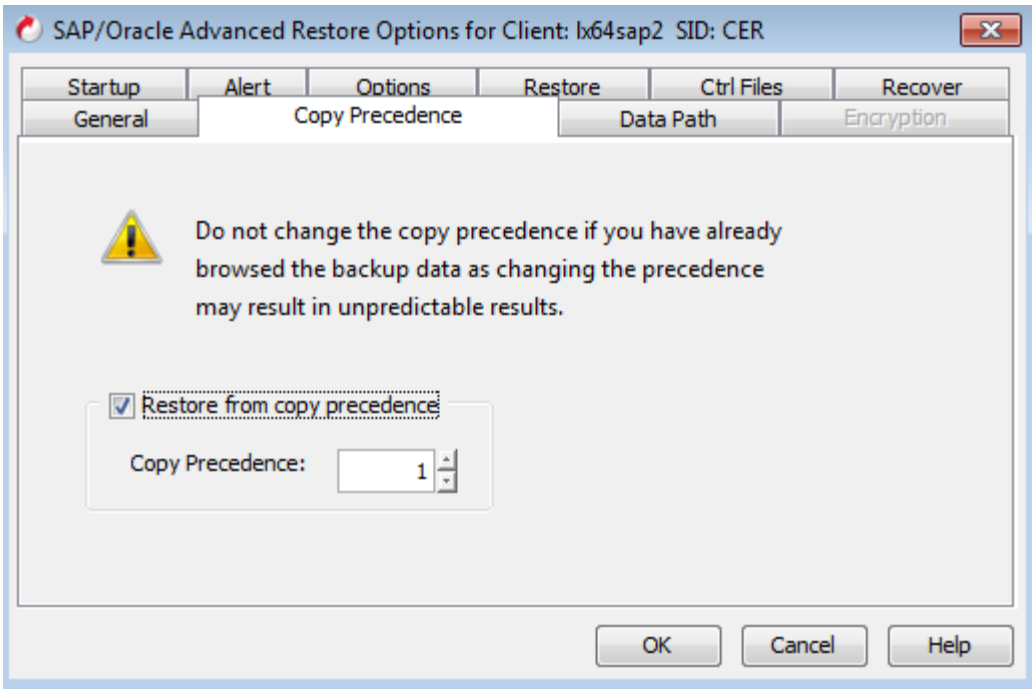
7. From the **Browse** window, select the data you want to restore in the right pane and click **Recover All Selected**.



8. From the **Restore Options for All Selected Items** window, select the correct destination client and the desired restore/recover options. Click **Advanced**.



9. Click the Copy Precedence tab and select the Restore from Copy Precedence checkbox.
10. In the Copy Precedence box, type the copy precedence number for the backup copy.



11. Click **OK**.
12. Click **OK** to close the **Restore Options** window and start the restore job.

Out of Place Restore – DB2 Example

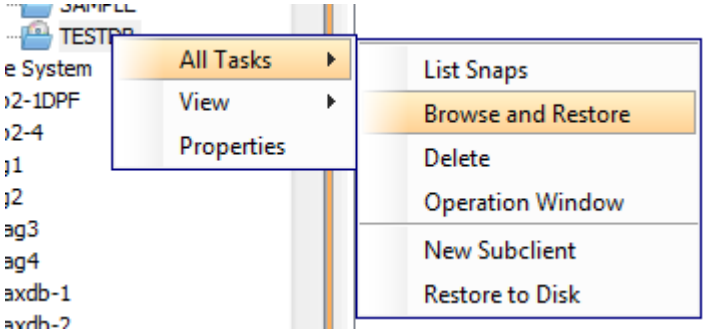
Snapshots can be used for recovery out of place just like any other media based backup. LAN and LAN-free recovery are both supported. For LAN-free recovery the target must have access to the array hosting the snapshots, and MediaAgent and any required iDataAgent software must be installed.

When restoring the databases to a new client, ensure the following:

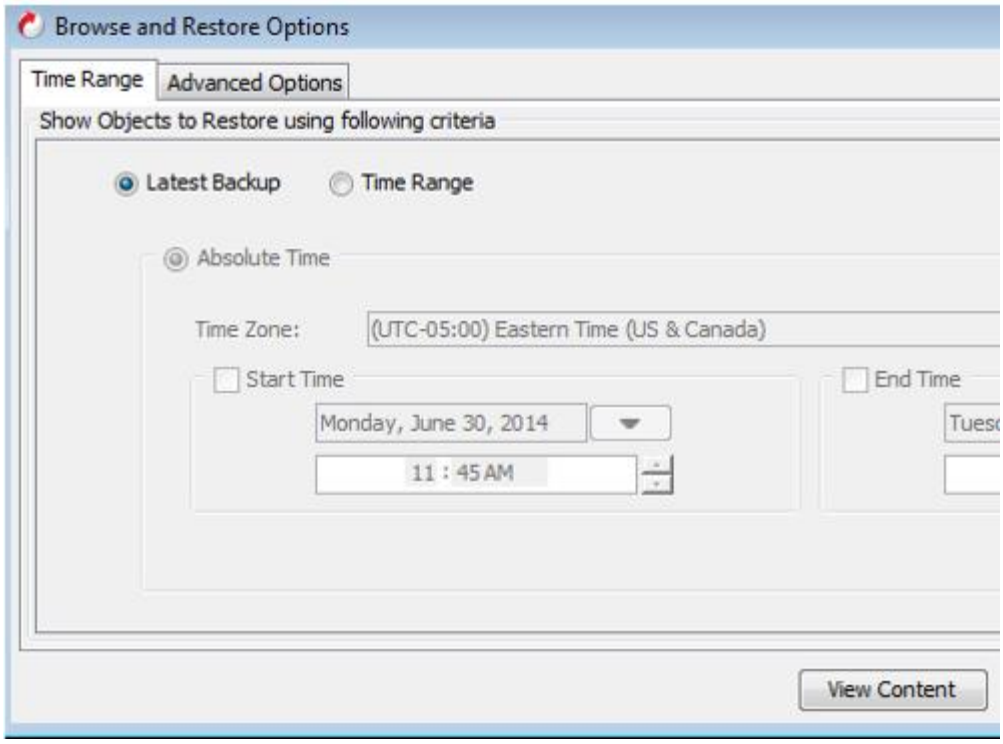
- On Windows configurations, make sure there are no databases existing on the destination's directory. If there are databases, the restore will destroy the databases because the SQLDBDIR information from the source database overwrites the destination information.
- The operating system on the destination client must be the same as that in the source client.
- The DB2 application on the destination client must be the same (or later) version as that in the source client.
- The DB2 user must have sufficient rights to restore the database. See Configuring User Accounts for more information.
- The database path (db_path) and storage path must be the same on the destination for redirected restores.
- When performing a restore for storage paths, the number of storage paths on the destination must be equal or less than the number on the source because the Simpana software provides a source to destination mapping to restore and relocate.
- When you restore the database to a new client, use the same user/group IDs of the DB2 instance.
- Install the DB2 iDataAgent on both the source client and the destination client.
- Create and configure an instance of DB2 on both the source client and the destination client on the CommCell.
- Run a DB2 database backup on the source client.
- When the original database is removed from the DB2 system, after the redirect restore on the same instance of the same host, you must manually clean the original data files on the source.

Use the following steps to restore the database to a new client:

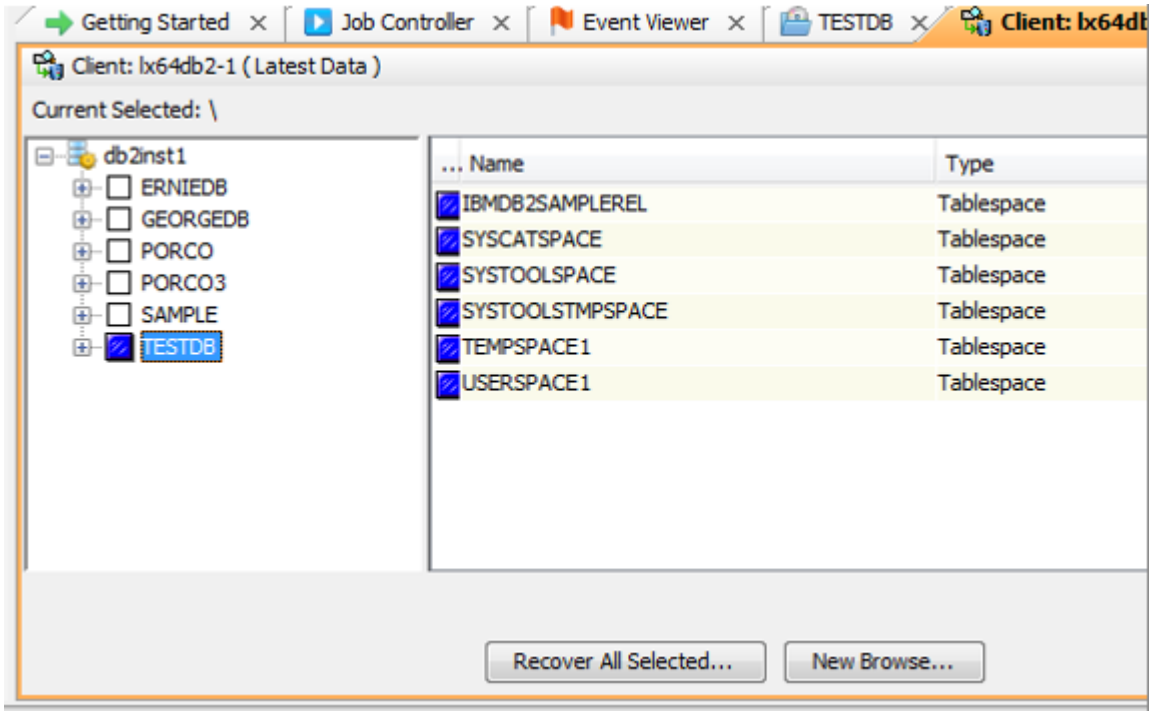
1. From the CommCell Browser, navigate to Client Computers | <SourceClient> | DB2 | <Instance>.
2. Right-click the <BackupSet>, point to All Tasks and then click Browse and Restore.



3. Select Latest Backup and click View Content.

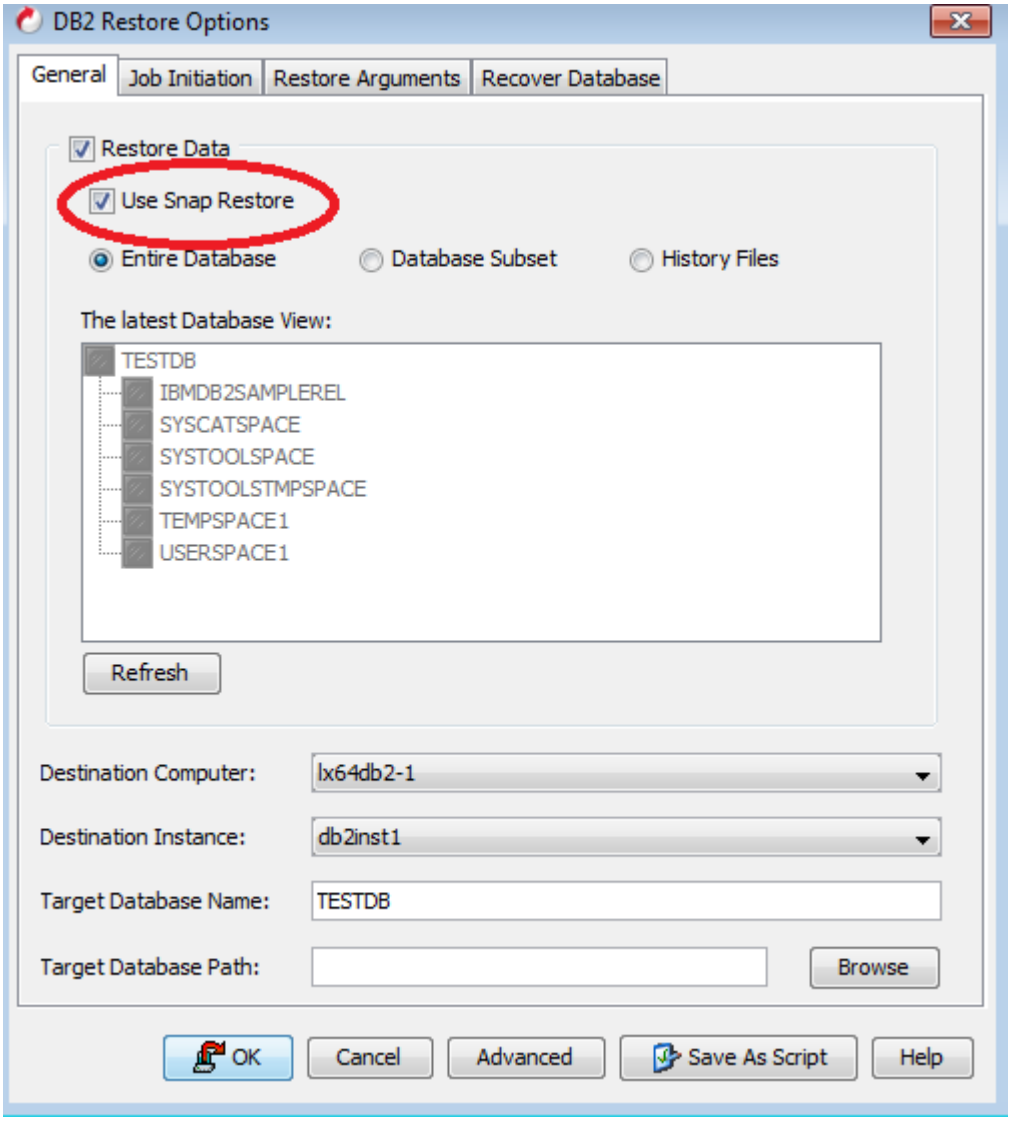


4. Select the database and click Recover All Selected.



5. On the **General** tab of the **Restore Options** dialog box:
6. Select the **Use Snap Restore** check box.
7. Select the **Entire Database** option.
8. Select the destination client name from the **Destination Computer** list.
9. To change the instance, select the **Destination Instance** from the destination instance list.

10. To change the target database name and location, enter it in the **Target Database Name** or click **Browse** to select the **Target Database Path**.



11. For Windows clients, the Target Database Path is the drive letter (for example: E:\).
12. Click **OK**.

Appendix

Contacting Pure Storage support

Contact	support@purestorage.com
Support site	http://www.purestorage.com/support/

Snap Reconciliation Registry Key

This key validates snapshot created by Simpana have not been altered or deleted externally of Simpana's management calls, potentially invalidating recovery options within Simpana.

Location	
Windows	HKEY_LOCAL_MACHINE\SOFTWARE\CommVault Systems\Galaxy\Instance<xxx>\MediaManager
Unix	Not Applicable
NetWare	Not Applicable
Key	nRunSnapRecon (optional)
Value	Not Applicable
Value Type	DWORD
Valid Range	1 or x, where 'x' is any other value than 1
Default Value	None
Created in	CommServe
Description	To enable Snap Reconciliation from the Media Manager. When this registry key is set to 1, the snap reconciliation is enabled and the MM will run the snap reconciliation every 24 hours. When this registry key is set to 0, the snap reconciliation is disabled. Also, the absence of this registry key is considered as if the value is set to 0 and hence the snap reconciliation will not be started.
Additional Information	N/A
Applies To	IntelliSnap Software Backup