# Protecting Oracle data in a modern way using IBM Spectrum Protect Plus

*Version 1.0*

Contents



 

## Executive summary

Database administrators and IT management personnel are faced with ensuring the availability of mission-critical business applications daily, for any number of stakeholders within the organization. Line-of-business owners, knowledge workers, developers or even the CxO all need timely access to Oracle databases 24x7x365. The production data center provides this access, but often a ticket must be issued, causing a delay. What if access can be provided by another means? A way to protect Oracle databases is to implement a modern data protection solution, providing operational recovery with very low recovery time objectives (RTOs) and offering multiple recovery point objectives (RPOs). Along with this operational recovery, the solution can offer a way to re-use the same production data that's protected.

## About this document

This white paper focuses on the deployment and setup of IBM® Spectrum® Protect Plus for protecting Oracle database environments. Readers will be taken through a step-by-step explanation of what is required to install and configure IBM Spectrum Protect Plus for the backup and recovery of Oracle databases.

Note that while IBM Spectrum Protect Plus also supports virtual machines, this aspect will not be covered in this document.

## The challenge

Protecting and recovering mission-critical Oracle data quickly and efficiently is a constant need for IT. Now more than ever, IT is struggling to meet the following Oracle backup and recovery challenges:

- Stricter service level agreements (SLAs) require more RPOs and lower RTOs
- Demand for data to support application development, reporting and analytics is higher than ever before
- Regulations and compliance require more intricate retention rules
- Archiving data in the cloud is becoming more prevalent
- Spending on IT goes to new projects, starving resources for backup and recovery operations
- Organizations need a simpler way to protect and recover mission-critical applications

One method to overcome these challenges is to deploy a solution designed with the challenges in mind. Implementing IBM Spectrum Protect Plus provides a modern approach to data protection focusing on operational recovery, data re-use and data management.

## Solution overview: IBM Spectrum Protect Plus

IBM Spectrum Protect Plus is a modern data protection solution that simplifies rapid virtual machine, file, database and application recovery. It unlocks the value of your data to facilitate data reuse and accelerate DevOps, analytics and much more.

Key value areas of IBM Spectrum Protect Plus are ease of use, high performance, efficiency and flexibility. Below are IBM Spectrum Protect Plus capabilities that are critical for modern data protection.

Unlike with many products, you don't have to be a backup expert to use IBM Spectrum Protect Plus. The software is simple to deploy and can be ready to start operations in as little as 15 minutes by installing a prebuilt virtual machine. You can realize a rapid time to value; after some simple configuration, IBM Spectrum Protect Plus can be up and running in as little as an hour. Compare this to some solutions that can take weeks to deploy and require costly professional services.

IBM Spectrum Protect Plus is SLA policy-based with "select, click and done" simplicity, whether selecting a recovery service level from a predefined set of gold, silver and bronze SLAs, or creating your own custom SLA to meet your specific needs. Once SLAs have been created, you then apply the appropriate SLA to your application or virtual machine.

Backups are stored as snapshot images, which allows you to recover data very quickly. There is no need to run a streaming restore that copies data to a target device. You just access backups directly and immediately from a simple mount point. Because data copies can be created fast and frequently, you have multiple recovery points to give you better RPOs.

IBM Spectrum Protect Plus recoveries can be used to restore operations in a number of data-loss scenarios, including inadvertent data deletion through human error; data loss due to hardware failures and data corruption; or more significant site-disaster scenarios.

While data protection is its main use case, IBM Spectrum Protect Plus is more than just a backup solution. You can use it to derive significant business value from your protected data. With IBM Spectrum Protect Plus, you can quickly and easily spin up an Oracle database, including on an alternate instance. This can then be used for any situation where users or developers need access to databases. Examples of these use cases are disaster recovery (DR), test-dev, reporting and analytics. Because IBM Spectrum Protect Plus also offers Representational State Transfer (RESTful) application programming interfaces (APIs), it can even be used as part of a DevOps workflow, helping to enhance modern, automated software development processes.

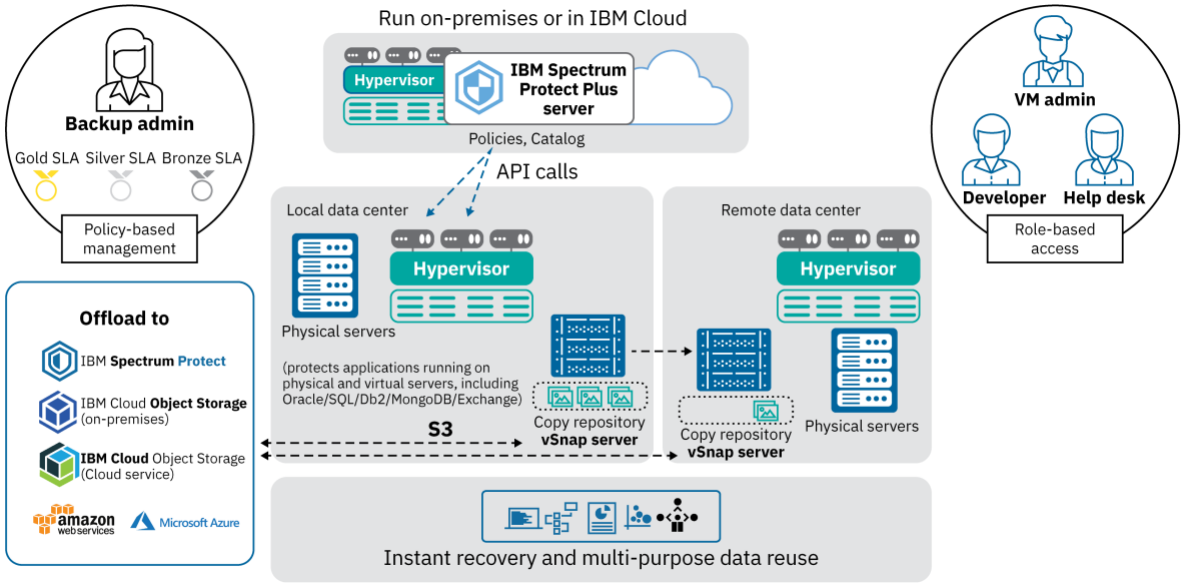


Figure 1: IBM Spectrum Protect Plus overview

# Product components

The IBM Spectrum Protect Plus solution is provided as a self-contained virtual appliance that includes storage and data movement components. Some environments might require more instances of these components to support greater workloads.

The following are the base components of IBM Spectrum Protect Plus:

IBM Spectrum Protect Plus server: This component manages the entire system and has several catalogs that track various system aspects such as restore points, configuration, permissions and customizations. Typically, there is one IBM Spectrum Protect Plus appliance in a

deployment, even if the deployment is spread across multiple locations. The IBM Spectrum Protect Plus server contains an onboard vSnap server and VMware vStorage API for Data Protection (VADP) proxy server. For smaller backup environments, these servers might be sufficient. However, for larger environments, more servers might be required.

Site: This component is an IBM Spectrum Protect Plus policy construct that is used to manage data placement in the environment. A site can be physical (a data center location) or logical (a department or organization). IBM Spectrum Protect Plus components are assigned to sites to localize and optimize data paths. A deployment always has at least one site per physical location. The preferred method is to localize data movement to sites by placing vSnap servers and VADP proxies together at a single site. The placement of backup data in a site is governed by SLA-based policies.

vSnap server: This component is a pool of disk storage that receives data from production systems for the purposes of data protection or reuse. The vSnap server consists of one or more disks and can be scaled up (adding disks to increase capacity) or scaled out (introducing multiple vSnap servers to increase overall performance). Each site can include one or more vSnap servers.

vSnap pool: This component is the logical organization of disks into a pool of storage space, which is used by the vSnap server component. This component is also referred to as a storage pool.

To determine how to size, build and place the components listed in these specifications for your IBM Spectrum Protect Plus environment, see the IBM Spectrum Protect Plus Blueprint.

For IBM Spectrum Protect Plus system requirements, please refer to the IBM Spectrum Protect Plus documentation in the IBM Knowledge Center, and select the appropriate version in the pull-down menu.

In addition to database and operating system version support (listed below), the configuration of the Oracle database server has prerequisites relating to software needed, connectivity requirements, authentication and privileges, Network File System (NFS) requirements, log backup requirements, IBM Spectrum Protect Plus agent user requirements, database discovery needs, block change tracking requirements and port requirements. These requirements can be found in the IBM Spectrum Protect Plus User's Guide, found in the IBM Knowledge Center.

# Oracle requirements

Before registering each Oracle server in IBM Spectrum Protect Plus, ensure it meets the following requirements.

These are the supported Oracle database versions:

- Oracle 11g R2
- Oracle 12c R1
- Oracle 12c R2

Note: For Oracle 12c multitenant databases, IBM Spectrum Protect Plus supports protection and recovery of the container database, including all pluggable databases under it. Granular recovery of specific pluggable databases (PDBs) can be performed via Instant Disk Restore recovery combined with Oracle Recovery Manager (RMAN). Oracle 12c multithreaded configurations are not supported.

Along with the supported Oracle database versions, the following operating system versions are supported:

- IBM AIX® 6.1 TL9+
- AIX 7.1+
- Red Hat Enterprise Linux / Centos 6.5+
- Red Hat Enterprise Linux / Centos 7.0+
- SUSE Linux Enterprise Server 11.0 SP4+
- SUSE Linux Enterprise Server 12.0 SP1+

Additional notes:

- Oracle DataGuard is not supported.
- Databases must be in ARCHIVELOG mode. IBM Spectrum Protect Plus cannot protect databases running in NOARCHIVELOG mode.
- Real Application Cluster (RAC) database recoveries are not server-pool-aware. IBM Spectrum Protect Plus can recover databases to a RAC, but not to specific server pools.

Please check the IBM Spectrum Protect Plus documentation for any updated Oracle server Database backup and restore requirements information at the link provided, below.
http://www.ibm.com/support/docview.wss?uid=swg22013790

# Registering your Oracle database server

To protect Oracle content, you first need to register the Oracle instance, so that IBM Spectrum Protect Plus recognizes it. When an Oracle application server is added, an inventory of the instances and databases that are associated with the application server is created and added to IBM Spectrum Protect Plus. This process enables you to complete backup and restore jobs, as well as run reports. To register the Oracle instance, please follow this procedure:

To register an Oracle application server, complete the following steps:

1. In the navigation pane, click **Manage Protection > Applications > Oracle > Backup**.

2. Click **Manage Application Servers**.

3. Click **Add Application Server**.

4. Populate the fields in the **Application Properties** pane:

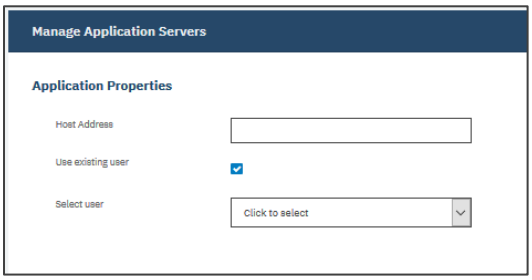


Figure 2: The Application Properties pane

   a. **Host Address**
      Enter the resolvable IP address or a resolvable path and machine name.

   b. **Use existing user**
      Enable to select a previously entered user name and password for the application server. Selecting this checkbox will replace the username and password text boxes with a pull-down menu to select previously used identities.

   c. **Username**
      Enter your user name for the application server.

d. **Password**
   Enter your password for the application server.

e. **Maximum concurrent databases**
   Set the maximum number of databases to back up concurrently on the server.

5. Click **Save**. IBM Spectrum Protect Plus confirms a network connection, adds the application server to the IBM Spectrum Protect Plus database and then catalogs the instance.

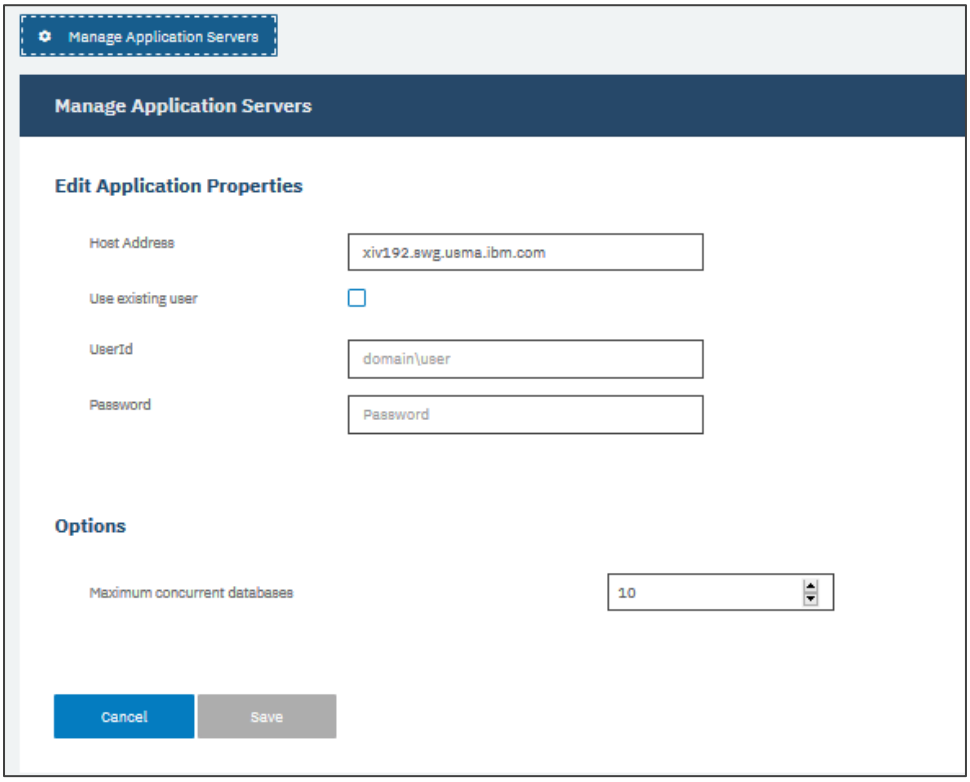


Figure 3: Registering the Oracle database server

### *Testing connection to an Oracle application server*

You can test the connection to an Oracle server. The test function verifies communication with the host and tests Domain Name System (DNS) settings between the IBM Spectrum Protect Plus virtual appliance and the host. It also tests that certain services are enabled and that the account used has sudo privileges.

To test the connection, complete the following steps:

1. In the navigation pane, click **Manage Protection > Applications > Oracle > Backup**.

2. Click **Manage Application Servers**.

3. In the list of hosts, click **Test** in the **Actions** menu for the host.

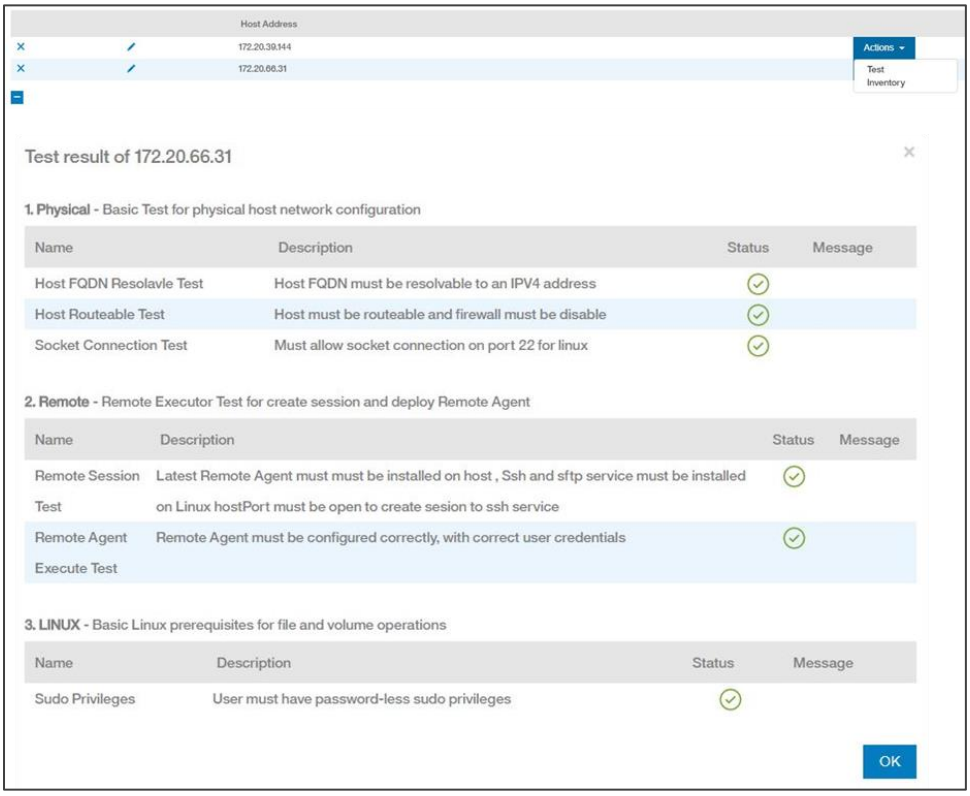

Figure 4: Testing registered server connections

# Protecting Oracle data

The following provides information on how to create an SLA policy to protect your Oracle data, with a specific frequency at which the data is backed up and a specified retention period. Also, a procedure is provided for setting up a backup job to protect the Oracle data.

### *Creating an SLA policy*

There are three default SLA policies (Gold, Silver and Bronze) available for selection for the backup job. You can use these policies as they are or modify them to meet your specific

requirements. You can also create custom SLA policies to define the backup frequency, retention and replication policies that are specific to your Oracle environment.

To create an SLA policy, complete the following steps:

1. In the navigation pane, click **Manage Protection > Policy Overview**.

2. Click **Add SLA Policy**. The **New SLA Policy** pane is displayed.

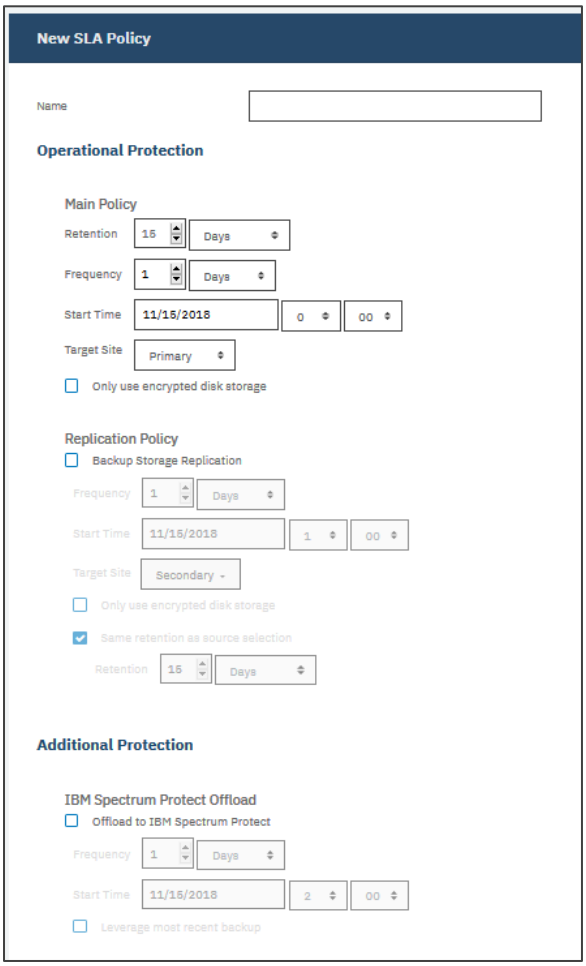


Figure 5: The New SLA Policy pane

3. In the **Name** field, enter a name that provides a meaningful description of the SLA policy.

 

4. In the **Operational Protection** section under **Main Policy**, set the following options for backup operations. These operations occur on the vSnap servers that are defined in the **System Configuration > Backup Storage > Disk** window.

    a. **Retention**
    Specify the retention period or the number of snapshots to keep.

    b. **Frequency**
    Enter a frequency for backup operations.

    c. **Start Time**
    Enter the date and time that you want the backup operation to start.

    d. **Target Site**
    Select a primary or secondary backup destination.

    e. **Only use encrypted disk storage**
    Select this checkbox to back up data to encrypted vSnap servers.

5. Under **Replication Policy**, set the following options to enable asynchronous replication from one vSnap server to another. For example, you can replicate data from the primary to the secondary backup site.

    a. **Replication partnerships requirement**
    These options apply to established replication partnerships.

    b. **Backup Storage Replication**
    Select this option to enable replication.

    c. **Frequency**
    Enter a frequency for replication operations.

    d. **Start Time**
    Enter the date and time that you want the replication operation to start.

    e. **Target Site**
    Select a primary or secondary replication destination.

If more than one primary or secondary storage site is available to IBM Spectrum Protect Plus, the replication destination with the largest amount of available storage is used first.

f. **Only use encrypted disk storage**
Select this check box to replicate data to encrypted vSnap servers.

g. **Same retention as source selection**
Select this option to use the same retention policy as the source vSnap server. To set a different retention policy, clear this option and set a different policy.

Note: **Additional Protection** is not applicable to the protection of Oracle databases.

6. Click **Save**. The SLA policy can now be applied to backup job definitions.

## Defining an Oracle backup job

Use a backup job to protect Oracle environments with snapshots. Oracle backups run in a "Base-Once-Incremental-Forever" scheme. Oracle block change tracking is required. If not present, it is enabled automatically during the first backup.

During the initial base (full) backup, IBM Spectrum Protect Plus creates a new vSnap volume and mounts it to the Oracle server using NFS. If the Oracle server has NFS disabled, the IBM Spectrum Protect Plus appliance will automatically enable it. A level 0 image copy of the database is created using RMAN, then a snapshot of the vSnap volume is created.

During incremental backups, the previously created volume is reused and mounted on the application server using NFS. The IBM Spectrum Protect Plus agent mounts the share on the Oracle server where the backup is to be completed. A level 1 incremental backup is created using RMAN and immediately applied to the previous image copy to bring it up to date. Then a snapshot of the vSnap volume is created.

During the definition of the backup job, you can select the "Enable Log Backup" checkbox. With the box checked, IBM Spectrum Protect Plus will automatically create a log backup volume and mount it to the application server. Then it uses cron to configure a scheduled job that completes a transaction log backup to that volume, and it manages the retention of logs in its

own log backup volume. After a successful database backup, older logs are deleted automatically from this log backup volume.

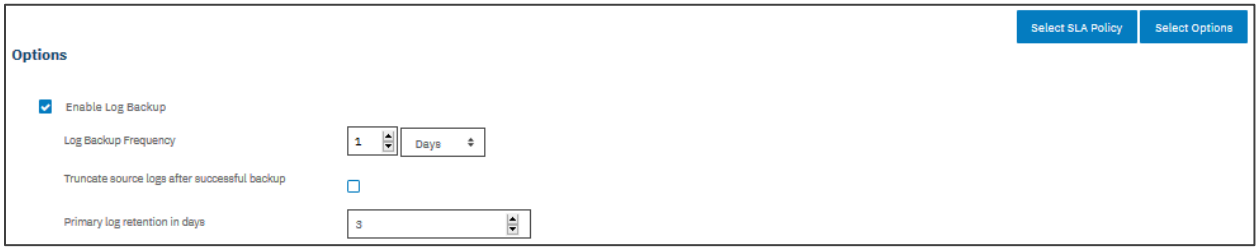


Figure 6: Enabling log backup

In the case of an Oracle RAC, the backup is completed from any one node in the cluster. When the backup is complete, the IBM Spectrum Protect Plus agent unmounts the share from the Oracle server and creates a vSnap snapshot of the backup volume. Also, for a RAC configuration, IBM Spectrum Protect Plus mounts the volume and configures the cron job on each of the cluster nodes. When the schedule is triggered, the jobs internally coordinate to ensure that any one active node completes the log backup and the other nodes take no action.

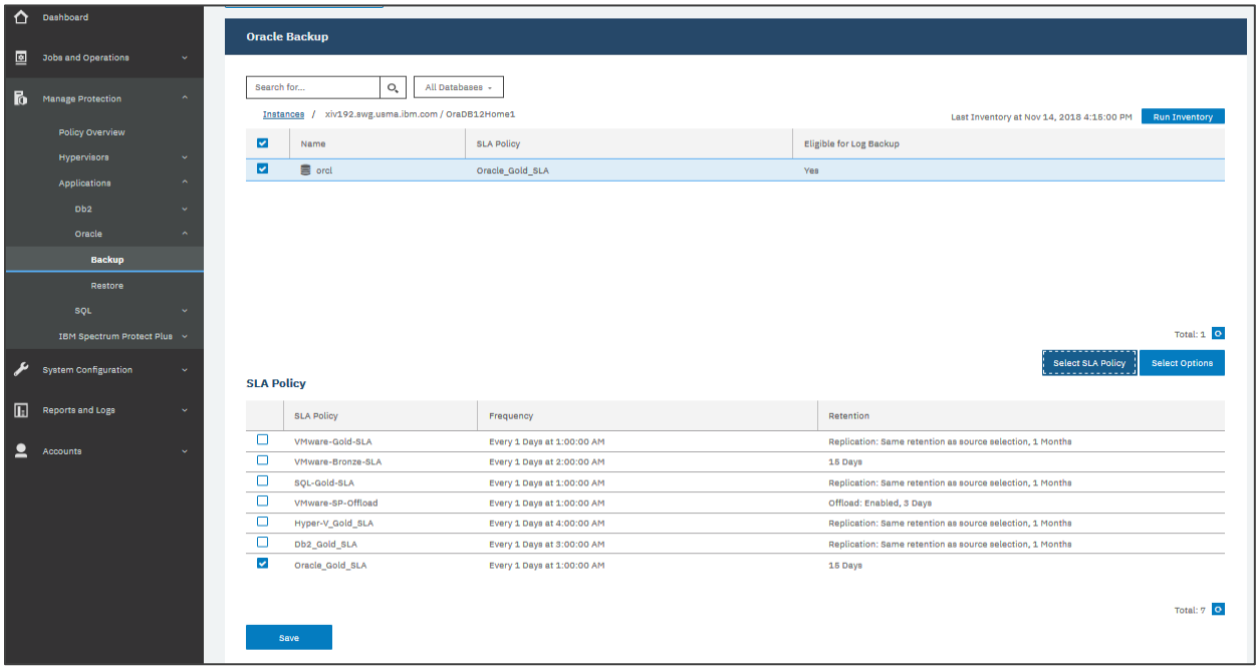


Figure 7: Creating an Oracle backup job

To define an Oracle backup job, complete the following steps:

1. In the navigation pane, click **Manage Protection > Applications > Oracle > Backup**.

 

2. Select Oracle homes, databases and Oracle Automatic Storage Management (ASM) disk groups to back up. Use the search function to search for available instances.

3. Click **Select SLA Policy** to add one or more SLA policies that meet your backup data criteria to the job definition.

4. To create the job definition by using default options, click **Save**.

   The job runs as defined by the SLA policies that you selected, or you can manually run the job by clicking **Jobs and Operations > Monitoring** and starting the job from the **Job Monitor** pane.

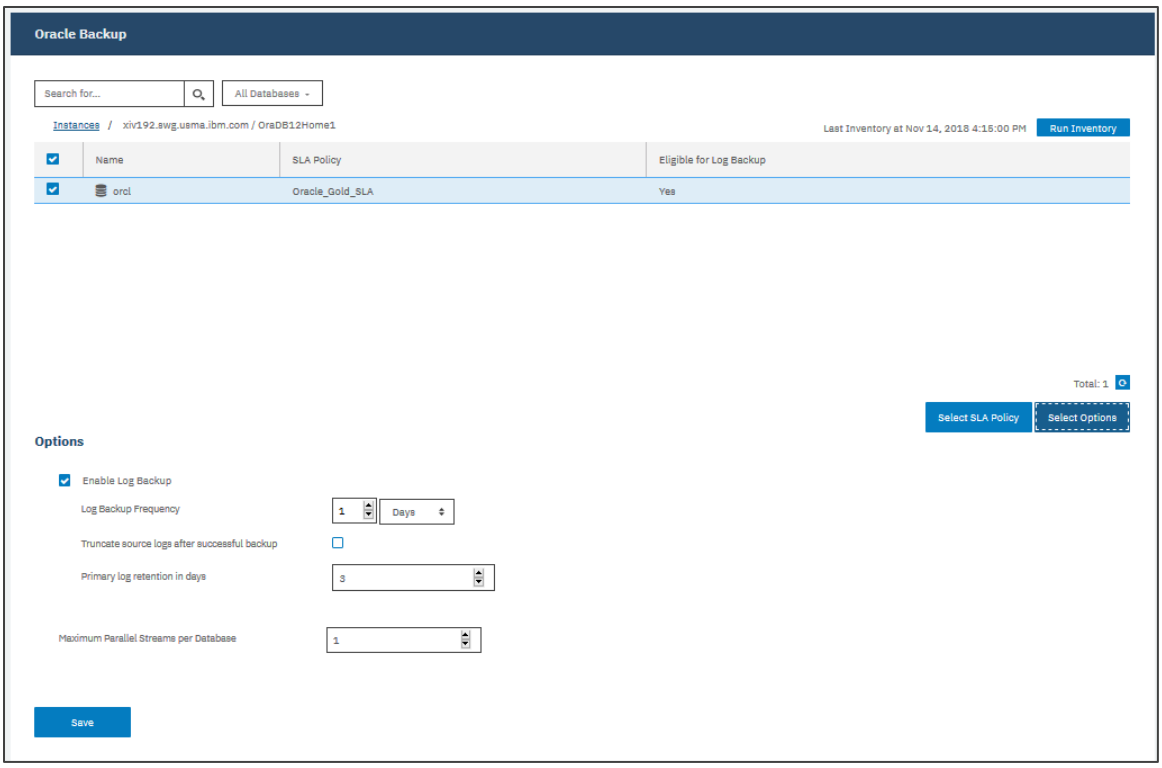


Figure 8: Creating an Oracle backup job with options

5. To edit options before you create the job definition, click **Select Options**. Set the job definition options.

   a. **Enable Log Backup**
      Select a frequency for log backups.

Click **Save**.

Select **Truncate source logs after successful backup** to automatically delete older archived logs that are no longer needed. Set the log retention through the **Primary log retention in days** setting.

When this option is selected, point-in-time restore options are available for Oracle restore operations.

b. **Maximum Parallel Streams per Database**
Set the maximum data streams per database to the backup storage. This setting applies to each database in the job definition. Note that multiple databases can still be backed up in parallel if the value of the option is set to 1. Multiple parallel streams may improve backup speed, but high bandwidth consumption may affect overall system performance.

6. When you are satisfied that the job-specific information is correct, click **Save**.

# Restoring Oracle databases by restore type

Use a restore job to recover Oracle databases from snapshots captured by the previous backups. IBM Spectrum Protect Plus creates a vSnap clone from the restore point version selected during the job definition creation and creates an NFS share. The IBM Spectrum Protect Plus agent then mounts the share on the Oracle server where the restore is to be performed. One of the following restore modes is selected in the restore job definition along with other options.

The restore modes available:

- **Test mode**
In Test mode, the agent creates a new database using the data files directly from the vSnap volume. The database is not actually restored; rather, a clone is created and presented from the vSnap server.

- **Production mode**
In Production mode, the agent first restores the files from the vSnap volume to the primary storage and then spins up the new database using the restored files.

 

- **Instant Access mode**
  In Instant Access mode, no further action is taken after mounting the share. Users can complete any custom recovery using the files in the vSnap volume.

## *Restoring an Oracle database*

To restore an Oracle database, the user logs in to IBM Spectrum Protect Plus, navigates to **Manage Protection** by clicking on it, selects the **Application** menu option, then **Oracle** and finally **Restore**. The procedure is shown below.

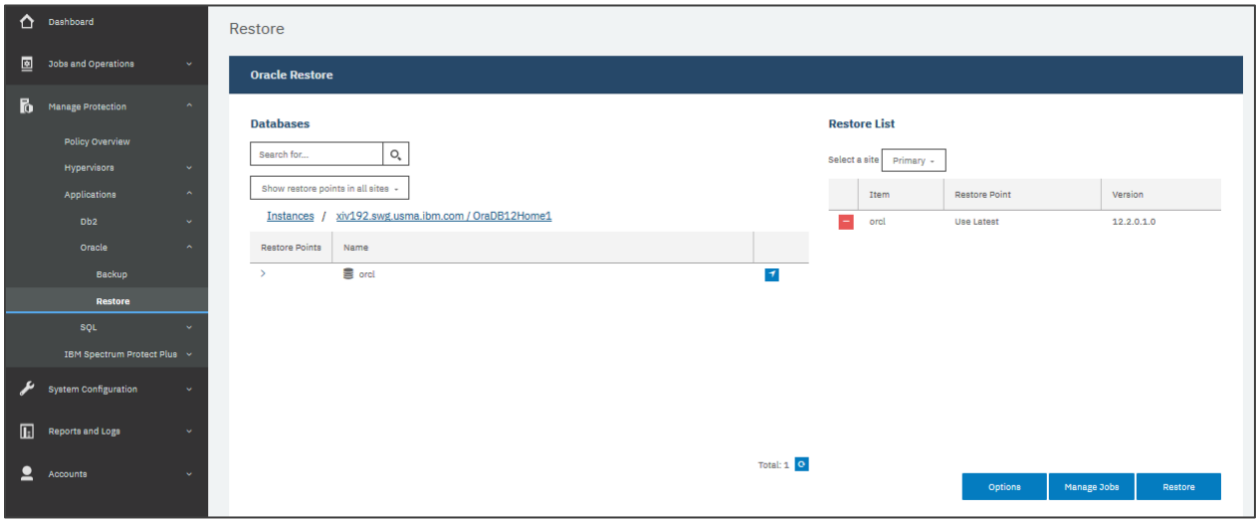


Figure 9: Restoring an Oracle database

To define an Oracle restore job, complete the following steps:

1. Navigate to **Application > Oracle > Restore**, under **Manage Protection**.

2. Select the desired database to recover.

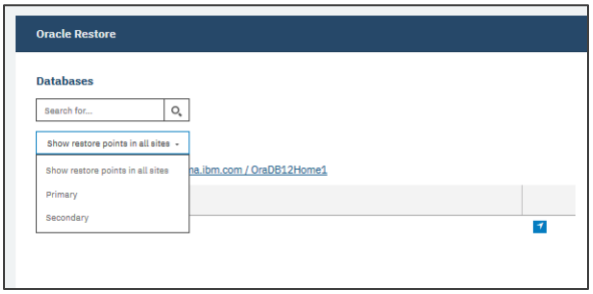


Figure 10: Selecting a site for restore

When selecting a restore point for recovery, there are options to “Show restore points in all sites” or to only show restore points from a specific site. For example, this figure shows a Primary and Secondary site. If a recovery point has been replicated through the assigned SLA policy, then that restore point is available for restore from either the Primary or Secondary site.

Click the icon to add the restore point to the Restore list. If a change is needed, click the icon to remove items from the Restore list.

Now that a restore point has been selected, the **Options**, **Manage Jobs** and **Restore** buttons are available for selection. The **Options** button provides the ability to define the restore type, such as Test, Production or Instant Access restores. It also provides the ability to restore to the original Oracle instance or an alternate instance, along with defining a new database name upon restore. Recovery options of **Recover until end of backup** or **Recover until a specific point-in-time** are also available.

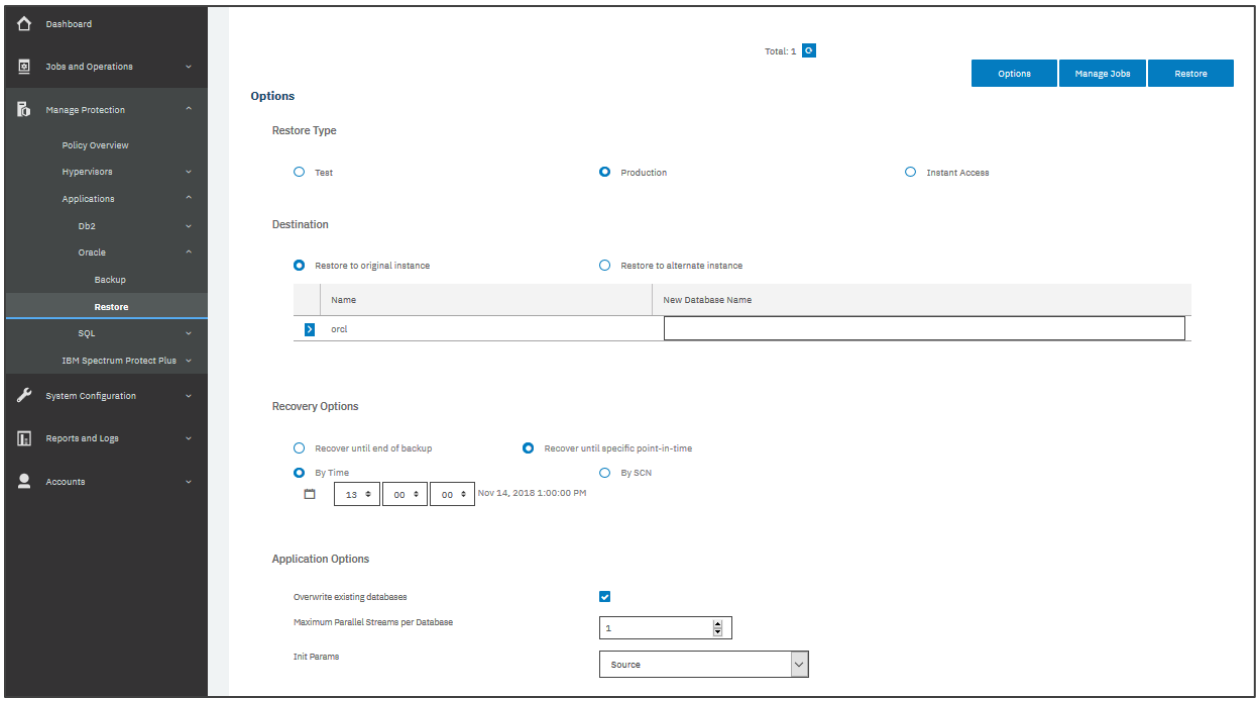

Figure 11: Restore options

To edit options before you create the job definition:

1. Select **Options**.

2. Click on the **Restore Type** radio button.

   Selecting the **Test** restore type, the restore process does not actually restore the original database files to the indicated original or alternate Oracle instance. The database is presented by the selected instance by creating a clone with the files on the vSnap server. Enter a new name in the **New Database Name** field.

   When you select **Production** restore, you are intending to restore the database to the production Oracle database server. To overwrite the original database, ensure you select the **Overwrite existing database** checkbox. If you wish to give the restored database a different name, then this checkbox is not required. Enter a new name in the **New Database Name** field.

   The selection of **Instant Access** restore will provide access to the associated database files by mounting a share of the files on the vSnap server. Other Oracle database tools can be used to perform the intended custom recovery tasks with these files. Disks will be mounted on /mnt/spp/.

3. Now select the recovery options needed by selecting the **Recover until end of backup** or **Recover until specific point-in-time** radio button, based on the RPO required.

   The **Recover until end of backup** option will restore the selected database to the state at the time the backup was created.

   When log backup is enabled through an Oracle backup job definition, the **Recover until specific point-in-time** restore option will be available when creating an Oracle restore job definition. Select one of the following options: **By Time**—to configure a point-in-time recovery by a specific date and time, or **By SCN**—to configure a point-in-time recovery by System Change Number (SCN).

4. Select the application options needed, such as **Overwrite existing databases** and/or **Init Params**. The **Overwrite existing databases** checkbox indicates the restore job will overwrite the databases on the selected original or alternate Oracle database restore location. **Init Params** controls the initialization parameters that are used to start up the recovered database in Oracle **Test** and **Production** restore workflows. Two **Init Params** options are available and they are **Source** and **Template**.

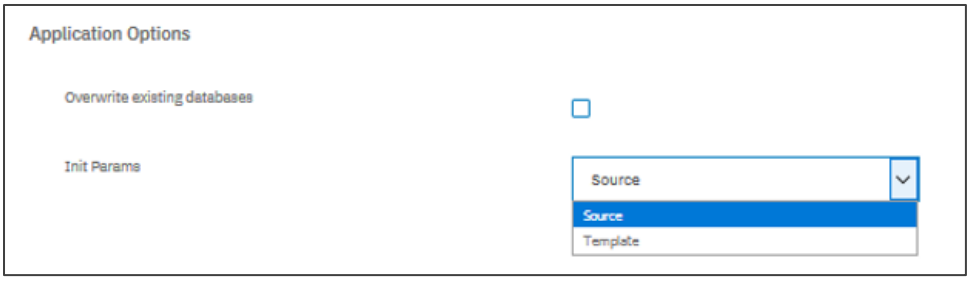

Figure 12: Application options for test and production restores

**Source**: This is the default option. IBM Spectrum Protect Plus uses the same initialization parameters as the source database, but with the following changes:

Parameters that contain paths such as control_files, db_recovery_file_dest, or log_archive_dest_* are updated to reflect the new paths based on the renamed mount points of the recovered volumes.

Parameters such as audit_file_dest and diagnostic_dest are updated to point to the appropriate location under the Oracle Base directory on the destination server if the path differs from the source server.

The db_name and db_unique_name are updated to reflect the new name of the database if a new name is specified.

Cluster-related parameters such as instance_number, thread and cluster_database are set automatically by IBM Spectrum Protect Plus depending on the appropriate values for the destination.

**Template**: Customize the initialization parameters by specifying a template file containing the initialization parameters that IBM Spectrum Protect Plus should use.

The specified path must be to a plain text file that exists on the destination server and is readable by the IBM Spectrum Protect Plus user. The file must be in Oracle pfile format consisting of lines in the form name = value. Comments beginning with the # character are ignored.

IBM Spectrum Protect Plus reads the template pfile and copies the entries to the new pfile that will be used to start up the recovered database. However, the following parameters in the template are ignored. Instead, IBM Spectrum

Protect Plus sets their values to reflect appropriate values from the source database or to reflect new paths based on the renamed mount points of the recovered volumes. These are the parameters in the template that are ignored:

control_files
db_block_size
db_create_file_dest
db_recovery_file_dest
log_archive_dest
spfile
undo_tablespace

Additionally, cluster-related parameters like instance_number, thread and cluster_database are set automatically by IBM Spectrum Protect Plus depending on the appropriate values for the destination.


Figure 13: Advanced Options for Test and Production restores

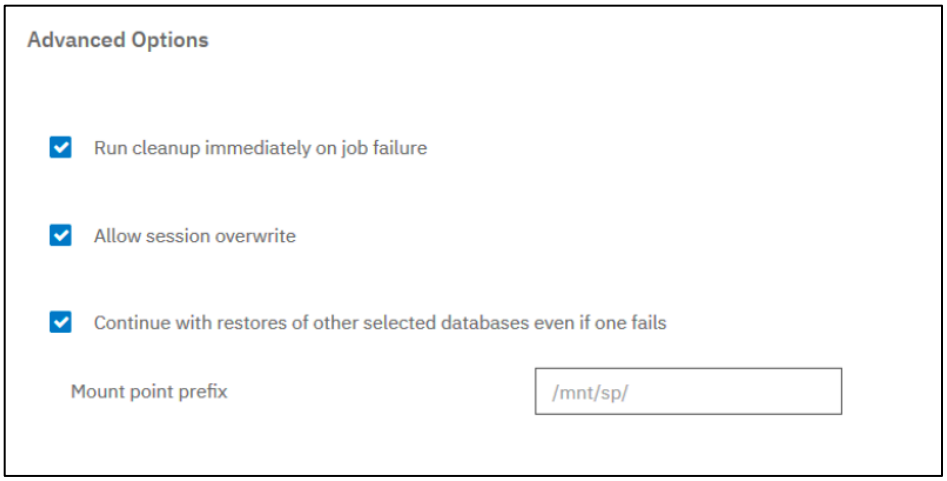


Figure 14: Advanced Options for Instant Access restores

There are Advanced Options, such as **Run Cleanup immediately after job failure, Allow session overwrite**, and **Continue with restores of other selected databases even if one fails**, that can be selected for all restore types, and then finally **Mount point prefix**, for instant access restore operations, specify the prefix for the path where the mount point is to be directed.


Figure 15: Script Settings performed during restores

In the **Pre-Script** and/or **Post-Script** section, select an uploaded script and a script server where the script will run. Scripts and script servers are configured through the **System > Scripts** pane.

Pre-scripts and post-scripts are scripts that can be run before or after a job runs at the job-level. Windows-based machines support batch and PowerShell scripts, while Linux-based machines support shell scripts.

Continue scripts on error—When enabled, if a pre-script completes with a non-zero return code, the backup or restore is attempted and the pre-script task status returns COMPLETED. When disabled, the backup or restore is not attempted, and the pre-script task status returns FAILED. If a post-script completes with a non-zero return code, the post-script task status returns COMPLETED. When disabled, the post-script task status returns FAILED.

See the IBM Spectrum Protect Plus User's Guide, found in the IBM Knowledge Center, for more details.

5. Click **Save** to save the restore job options. If the job is to be scheduled, select **Manage Jobs** and define a trigger for the job definition.

6. After you have performed all the required restore selections on the restore screen, click **Restore**.

IBM Spectrum Protect Plus finds the indicated restore point selected in the job. In the case of a **Point-in-Time** selection for a Production or Test restore, a temporary restore point is created if the point in time is after the last backup. During the recovery, the data backup volume and the log backup volume are mounted. That restore point is then presented by the Oracle database server, either through a share on the vSnap server for Test restores or the files are copied to the Oracle database server for Production restores.

Also, with Production restores, a new database instance is created using the original or alternate name specified by the user. If restoring with the same name and same directory paths, a control file is restored from backup and the data files are restored from backup using RMAN. If restoring with a new name and/or new directory paths, a new control file is created, containing the new database name and/or new data paths. If new paths point to filesystem directories, they are created if they do not already exist. If new paths point to ASM, the specified disk groups must already exist. The data files are restored from backup to the specified new paths. Media recovery is performed to make the database consistent using the log backups present under the NFS share, and the database is opened in read/write mode. When the restore completes (whether successful or not), the NFS share is unmounted.

In the case of Oracle RAC, the Production restore is performed on all nodes in the cluster. The main restore steps are performed only on the first node. On all other nodes, the instance is started, and the database is opened in read/write mode.

For additional information on restoring Oracle databases, refer to the IBM Knowledge Center for the latest version of the IBM Spectrum Protect Plus User's Guide.

# Summary

Protecting Oracle databases with the use of IBM Spectrum Protect Plus is simple and quick, requiring only a few mouse clicks. Accessing and re-using Oracle database data is just as simple with Instant Access and Test restores. And, IBM Spectrum Protect Plus restores your production data just as easily. As a result, your business enjoys greater protection, and your Oracle data can quickly and easily be used for multiple purposes.

IBM Systems
New Orchard Road
Armonk, NY 10504

Produced in the United States of America
March 2019



This document is current as of the initial date of publication and may be changed by IBM at any time.

It is the user’s responsibility to evaluate and verify the operation of any other products or programs with IBM products and programs.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED “AS IS” WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NON-INFRINGEMENT. IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

The client is responsible for ensuring compliance with laws and regulations applicable to it. IBM does not provide legal advice or represent or warrant that its services or products will ensure that the client is in compliance with any law or regulation. Statements regarding IBM’s future direction and intent are subject to change or withdrawal without notice, and represent goals and objectives only.