Oracle® Secure Backup

Readme

Release 12.2

E85993-01

January 2018

Readme

Image Contents

The image for each platform contains all necessary tools, documentation, and software to install and operate Oracle Secure Backup on the selected platform.

You can access the installation files from a downloaded file from the following product site:

https://edelivery.oracle.com

Release Components

The only product in this release is Oracle Secure Backup.

Licensing Information

Refer to *Oracle Secure Backup Licensing Information* for licensing terms.

Supported Tape Devices and Platforms

Supported platforms, web browsers, NAS devices, tape drives, and tape libraries are listed at the following URL:

http://www.oracle.com/technetwork/database/database-technologies/secure-backup/learnmore/index.html

Upgrading to Oracle Secure Backup Release 12.2

You can upgrade only Oracle Secure Backup 10.4.0.3 or Oracle Secure Backup 12.1 to Oracle Secure Backup 12.2. If you are using an earlier version, then you must upgrade to Oracle Secure Backup 12.1 prior to upgrading to Oracle Secure Backup 12.2.

Oracle Secure Backup 12.2 is backward compatible with Oracle Secure Backup 12.1 clients only.

Oracle Secure Backup 12.2 supports Oracle Secure Backup 12.1 features and is interoperable with its functionality.

All media servers must be at the Oracle Secure Backup 12.2 version level.

Access to any new commands and options introduced in Oracle Secure Backup 12.2 are not supported from a 12.1 client. The new commands must be accessed from an Oracle Secure Backup 12.2 host or via the Oracle Secure Backup Web Tool.

A database backup to a cloud storage device from an Oracle Secure Backup 12.1 client is not supported. That backup is restricted to disk or tape.

The new 12.2.0.1 backup compression levels are not supported on an Oracle Secure Backup 12.1 client.

See Also:

- *Oracle Secure Backup Installation and Configuration Guide* for more information on Client Backward Compatibility
- *Oracle Secure Backup Installation and Configuration Guide* for more information on how to upgrade Oracle Secure Backup 12.1 to Oracle Secure Backup 12.2

Readme Information for Oracle Secure Backup 12.2.0.1

This information in this section applies only to Oracle Secure Backup 12.2.0.1.

This section contains the following topics:

New Features

This section lists the new features in Oracle Secure Backup 12.2.0.1.

This topic contains the following sections:

Staging Data

New staging commands let you temporarily store one or more backup image instances in a disk pool storage container in preparation for automatically copying or moving the backup image instances to another container. For example, a backup instance can be moved from a disk pool to a tape volume or a cloud container.

Staging can involve multiple backup image instances, and can be configured to run based on specified conditions.

Cloud Support

Oracle Secure Backup now supports backup to Oracle Cloud Infrastructure Object Storage Classic. Backup data can be written to either Oracle Cloud Object Storage or Archive Storage. Oracle Cloud storage is accessed and managed using Oracle Secure Backup cloud storage devices in a manner similar to other Oracle Secure Backup devices.

All backup data is securely written to cloud storage devices by encrypting the backup data at the client host, with encryption keys being managed by the Oracle Secure Backup administrative server.

Cloud storage devices can also be used as targets for staging, which allows you to back up your data to a faster disk pool and then move it to the cloud.

You can also copy backup instances from Oracle Cloud Infrastructure Object Storage Classic to Oracle Cloud Infrastructure Archive Storage Classic for long-term retention.

Enhanced Software Compression

Oracle Secure Backup software compression has been enhanced to offer multiple levels of compression: `low`, `medium`, `basic`, and `high`. These new options are more efficient, in terms of compression ratio and speed, than the existing compression method using the obtar `-Z` option. (Note that as of Oracle Secure Backup 12*c* Release 2 (12.2.0.1), new backups are not allowed to compress data using the obtar `-Z` option. The `-Z` option is retained only for use in restoring older compressed legacy backups with the restore command.)

Backups are compressed based on the value of the `--compression` option as part of the `backup` or `mksched` command at the job level and as part of the `mkhost` command at the host level. It can also be specified at the domain level using the `backupcompression` global policy.

Bugs Fixed in Oracle Secure Backup 12.2.0.1

This section lists the bugs that have been fixed in Oracle Secure Backup 12.2.0.1

Table 1-1 Oracle Secure Backup 12.2.0.1 Fixed Bugs

Oracle Secure Backup 12.2.0.1 Fixed Bugs

Bug Number	Subject
17721345	CREATE UTILITY THAT UPGRADES WEB SERVER KEY AND CERTIFICATE.
18222820	DISK DELETION FAILS IF MEDIASERVER IS REMOVED FROM THE DOMAIN.
18312851	BACKUP TO ZFS FILER DISKPOOL FAILS WITH ALTERED BLOCKING FACTOR
18355199	ON ADMIN HOST, UNINSTALL/KEEP DATA DOES NOT ENTIRELY REMOVE THE APACHE DIRECTORY
18677982	CHUSER - WINDOWS DOMAINS: LOGINS THAT ARE NOT PASSWORD PROTECTED ARE MIS-HANDLED
19126023	HELP MESSAGE MISSING FOR <TEXT> TAG FOR RPYJOB OBTOOL COMMAND
20889726	OBTAR -Z ON NDMP TAPE THROWS "UNABLE TO USE CURRENT VOLUME: BARCODE REQUIRED"
21974986	DIAGNOSTIC ENHANCEMENT: OBCM TESTS SHOULD RETAIN INTERMEDIATE CLIENT LOGS.
22096715	BACKUP HANGS/FAILS DURING CATALOG COPY IF LOCAL RDMA CONNECTION IS USED.
22283586	DOS IN THE SECURE BACKUP OBSCHEDULED DAEMON.
22385055	TBRSFPSECUREINPUT FAILURE: PLEASE ENTER DATA ... PARSED BY THE SECURE_INPUT STEP
22536209	RATAPE - [ERROR] BACKUP OBJECT ID = 0
23718641	SOLARIS.X64 - SERVICE DAEMON IS NOT STARTED WHEN HOST IS REBOOTED
23724910	WEB TOOL DOESN'T RESTORE CORRECTLY USING AN "AS OF" DATE
24340005	INSTALLER: USE NETSTAT TO REPORT ERROR IF PORTS 400 AND 10000 ARE USED.
24447393	LINUX INSTALL: OSB TEMP DIRECTORY SHOULD DEFAULT TO THE WRAPPER TEMP DIRECTORY.
24525401	RMINSTANCE COMMAND HELP TEXT DOES NOT SHOW --UUID OPTION.
24757210	BACKUP OF NONEXISTENT "/STEVE/BIN" DIRECTORY REPORTS BACKUP OF /BIN CONTENTS
24790639	IDENTIFYVOL AND IMPORTVOL --IDENTIFY LEAVES ARCHIVES DATABASE IN INCORRECT STATE
24925890	ENHANCEMENT: DO NOT DELETE APACHE CONFIGURATION DIRECTORY IN CERTAIN SCENARIOS.
25084206	OSB WEBUI DISPLAY IS IMPROPER WHILE SHOWING CONFIGURED DEVICES
25136518	WINDOWS.X64: DURING INSTALL, CONFIGURATION SCRIPT SHOULD BE USED TO APPLY ACLS.
25142852	MOVE EOB WRITE TO DATA SERVICE FOR CATALOG ON TAPE

Table 1-1 (Cont.) Oracle Secure Backup 12.2.0.1 Fixed Bugs

Bug Number	Subject
25217822	CAN'T EDIT A TRIGGER VIA THE WEB TOOL
25248364	REDESIGN THE WEB TOOL MENUS TO PROVIDE EASIER NAVIGATION.
25292555	WEB TOOL - FIX FORMATTING OF SCHEDULE PAGE
25293502	CREATE VSS SUPPORT SCRIPT
25317720	SBT NOT REPORTING AUTOCONTROL, INCREMENTAL SBTOBJECT TYPES
25341698	AFTER 12.1 -> 12.2 UPGRADE, CERTIFICATE FILES REMAIN AFTER A CLEAN UNINSTALL.
25353474	THE SCHEDULER'S PREVIEW CALENDAR DISPLAYS THE WRONG YEAR FOR THE MONTH
25353612	WEBUI - EDITING A TRIGGER CAN DELETE THE TRIGGER.
25381091	OB_ROBOTS UPDATE FOR THE QUANTUM I3-I6 LIBRARY NEED TO BE ADDED TO LABELS
25388193	UPDATE HTTPS CERTIFICATES (REMOVE SHA-1)
25389496	DURING A 12.1.02 -> 12.10.3 UPGRADE, TRANSCRIPT FILES COULD BE LOST.
25444532	CERTAIN CONFIGURATION STEPS SHOULD BE EXECUTED IN ALL INSTALL SEQUENCES.
25456512	OBPOOLMGR DELETING ACTIVE BACKUP IMAGES AS ORPHANS WHEN DELETEDISKORPHANS = YES
25499198	CPINSTANCE FAILS WHILE PROCESSING BACKUP NAMES CONTAINING A PERIOD "."
25505032	INSTALL FAILS WITH SCRIPT ERROR ON "NON-ENGLISH" VERSIONS OF WINDOWS.
25510588	OSB 12.1.0.3.0 DUPLICATES BACKUP JOBS SOME MINUTES AFTER THE SCHEDULED JOB
25518184	WEBUI SETTING THE USER OPTION IN A SCHEDULE OR ON DEMAND BACKUP
25523977	OSB RAW RESTORE WITH GUI DON'T TAKE EFFECT REPLACEEXISTING AND REPLACEINUSE
25552602	INTERNAL ENHANCEMENT: PRIOR_OSB_VERSION SHOULD BE SET IN OBCONFIG_OSB_VERSION.
25557396	SUPPORT FOR HP LTO-7 NEEDS TO BE ADDED TO OB_DRIVES AFTER QUAL TESTING
25638709	LINUX/UNIX INSTALLER: ADD SUPPORT FOR "--INSTALL_ROLE CLIENT" PARAMETER
25649909	SPANNED DB BACKUPS TO BE HANDLED WELL DURING UPGRADE - OSB 10.4 TO 12.1
25660448	LINUX/UNIX INSTALLER SHOULD CONTAIN KEYSTORE PASSWORD WARNING.
25674962	IN CERTAIN SCENARIOS, MISSING REQUIRED DATA IS NOT FLAGGED IMMEDIATELY.
25715098	OBCTL SHOULD FAIL WITH A CLEAR ERROR MESSAGE IF USER IS NOT ADMIN.

Table 1-1 (Cont.) Oracle Secure Backup 12.2.0.1 Fixed Bugs

Bug Number	Subject
25733221	PIECES NOT BEING REMOVED AFTER REQUESTED WITH AND WITHOUT CONFIRMATION FROM OSB
25733986	"OBCTL RESTART" COMMAND FAILS ON WINDOWS.X64 ADMIN HOST.
25918381	RESTORE POSITIONING DOES NOT WORK FOR FILE SERVICE
26000341	CHANGE NAME OF RESTORE PAGE FROM "NEW RESTORE" TO "ADD RESTORE PATH"
26030301	CONCURRENT RMAN RESTORES FAILING WITH 'ERROR WAITING FOR RESOURCE'
26080531	CHANGE VOLUME ROTATION POLICY VIA OB BUI STARTS RUNAWAY PROCESS, FILLS /TMP
26107959	WEB TOOL CATALOG RESTORE OF WINDOWS FILES PREPENDS THE DIRECTORY NAME TWICE.
26360438	WINDOWS.X64: ADMIN HOST INSTALL FAILS WHEN USING ALTERNATE DB DIRECTORY.
26401894	WINDOWS.X64: "OBCTL RESTART" FAILS WITH "INTERNAL ERROR -6".
26849757	TITLE ELEMENT FOR EACH WEB TOOL PAGE SHOULD DESCRIBE ITS PURPOSE
26910909	ERROR: VOLUME <VOLUME> NOT FOUND FOR RECOVERY - OBJECT NOT FOUND
26913212	ERROR: CAN'T PASS ARGUMENTS TO OSB NDMP FILE SERVICE-CONNECTION NOT AUTHORISED
26949396	CHANGE DEFAULT FREE SPACE GOAL TO 75%
26993026	BYTES RECIEVED OVERFLOWS OUTPUT - INCORRECT RECIEVED BYTES REPORTED

Outstanding Bugs and Known Issues

This section discusses Oracle Secure Backup release 12.2.0.1 outstanding bugs and known issues.

Bug 26382658

The cloud/segmentsize policy setting is in bytes only. The minimum size of 1024 bytes is not enforced when setting the policy. The default size is 10485760 bytes.

Workaround:

Input for the cloud/segmentsize policy needs to be in bytes.

Bug 26256513

A backup or copy instance job fails when the target cloud container has reached its storage quota and there are expired backup image instances in the cloud container.

The expired instances are not automatically deleted from the disk pool to allow the backup or copy job to continue.

Workaround:

Expired backup image instances are removed from the cloud container during the midnight cleanup, after which the backup can be run again. The expired instances can also be deleted on demand with the obtool command `managedev –deleteexpired`.

Bug 26188127

Backup to a cloud container fails if the media server attached to the cloud device uses an RDS/ RDMA connection.

Workaround:

Disable RDS on the media servers that are connected to the cloud container. The obtool command `chhost --disablerds yes` *`hostname`* will disable RDS on the specified host.

Bug 27157413

If compression cannot be applied to a backup, as in the cases of an NDMP filer backup, RMAN backup, or down version client, then the backup job statistics report that “high” compression was applied.

Workaround:

Ignore compression status for NDMP filer backups and RMAN backups.

Bug 27176491

Modifying a client’s IP name resets the client’s compression setting.

Workaround:

Reset the client’s compression setting after changing its IP name.

Bug 27273828

The Windows install fails if the user requests a temp directory other than the default and that temp directory does not exist.

Workaround:

Create the temporary directory before running the installer.

Bug 26939448

RMAN encrypted backup instances written directly to a cloud device cannot be catalogued and restored into a another Oracle Secure Backup domain.

Workaround:

Write RMAN encrypted backups to a disk pool and then copy the backup instances to a cloud device. That cloud device can be cataloged into another domain.

Bug 27047826

A copy instance or copy from stage job fails if the target device is a cloud device and the media server attached to the source device is not connected to the cloud.

Workaround:

The media server that is attached to the source device must also be attached to the target cloud device.

Bug 27013962

Cataloguing a Cloud Archive device with the Oracle Secure Backup `catalog` command is not supported in this release.

Workaround:

The backup instances contained in a Cloud Archive container can be recovered by restoring the `OSB_CATALOG` backup.

Bug 27298615

The `lsdev -long` command takes a long time to time out when there are cloud devices in the domain.

Workaround:

The `lsdev -long` command must be run from the administrative server or a media server that is connected to the cloud.

Bug 27285801

The Windows 2016 native tape driver automatically reclaimed the tape device, rendering the tape device unusable by Oracle Secure Backup.

Workaround:

There is no workaround at this time to disable Window's automatic reclaiming of the tape device. This issue does not affect disk pool devices or cloud devices.

Documentation Accessibility

For information about Oracle's commitment to accessibility, visit the Oracle Accessibility Program website at http://www.oracle.com/pls/topic/lookup?ctx=acc&id=docacc.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Oracle® Secure Backup Readme, Release 12.2
E85993-01