Ahsay Replication Server

v6

Administrator's Guide

Ahsay Systems Corporation Limited

8 January 2015

Ahsay Replication Server

Administrator's Guide

Copyright Notice

© 2015 Ahsay Systems Corporation Limited All rights reserved.
The use and copying of this product is subject to a license agreement. Any other use is prohibited. No part of this publication may be reproduced, transmitted, transcribed, stored in a retrieval system or translated into any language in any form by any means without priori written consent of Ahsay Systems Corporation Limited Information in this manual is subject to change without notice and does not represent a commitment on the part of the vendor, Ahsay Systems Corporation Limited does not warrant that this document is error free. If you find any errors in this document, please report to Ahsay Systems Corporation Limited in writing.

This product includes software developed by the Apache Software Foundation (http://www.apache.org/).

Trademarks

Ahsay, Ahsay Online Backup Suite, Ahsay Offsite Backup Server, Ahsay Online Backup Manager, Ahsay A-Click Backup, Ahsay Replication Server, Ahsay BackupBox Firmware, Ahsay Universal Backup System, Ahsay NAS Client Utility are trademarks of Ahsay Systems Corporation Limited.

Microsoft, Windows, Microsoft Exchange Server and Microsoft SQL Server are registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Oracle 10g, Oracle 11g are registered trademarks of Oracle Corporation.

Lotus, Domino, Notes are registered trademark of IBM Corporation.

Red Hat, Red Hat Enterprise Linux, the Shadowman logo and JBoss are registered trademarks of Red Hat, Inc. www.redhat.com in the U.S. and other countries. Linux is a registered trademark of Linus Torvalds.

Apple and Mac OS X are registered trademarks of Apple Computer, Inc.

All other product names are registered trademarks of their respective owners.

Disclaimer

Ahsay Systems Corporation Limited will not have or accept any liability, obligation or responsibility whatsoever for any loss, destruction or damage (including without limitation consequential loss, destruction or damage) however arising from or in respect of any use or misuse of reliance on this document. By reading and following the instructions in this document, you agree to accept unconditionally the terms of this Disclaimer and as they may be revised and/or amended from time to time by Ahsay Systems Corporation Limited without prior notice to you.

Revision History

Date	Descriptions
8 April 2011	First Revision for AhsayOBS v6.3 release
30 June 2011	Updated: 1.3 System Requirements 11 Further Information Appendix A Product Documentations
30 July 2011	New: 3.15 AhsayOBS and Dual WAN Routers
22 August 2011	Updated: 7.2 Retention Feature
19 November 2011	Updated: 3.5 AhsayRPS Java Heap Size Setting 7.2 Retention Feature New: 3.16 Replication Using Cross Over Cable Appendix B How to restore files from AhsayRPS

Date	Descriptions	Type of modification
25 Jun 2012	9 Starting AhsayRPS as AhsayOBS	Modified
25 Jul 2012	10 Advanced Configuration	New
25 Jul 2012	10.1 Restricting access to system page by IP address	New
17 Aug 2012	3.11 Third Party Monitoring Software	Typo
04 Oct 2012	Copyright Notice	Modified
04 Jul 2013	3.4 Replication Performance Tuning	Typo
	3.11 Third Party Monitoring Software	Typo
	3.12 Do Not Operate AhsayOBS and AhsayRPS on a Single Machine	Typo
25 Jun 2014	1.3 System Requirements	Modified
	12 Further Information	Modified
12 Dec 2014	10.1 Restricting access to system page by IP address	Modified
	Copyright Notice	Modified

Table of Contents

1 Introduction 1
1.1 Conventions 1
1.2 Definitions, Acronyms and Abbreviation 1
1.3 System Requirements 3
2 Overview 4
2.1 Ahsay Replication Server 4
2.2 Ahsay Replication Server Administration Console 4
2.3 AhsayOBS Replication Module 6
2.4 Replication Scope 7
2.5 Replication Order 8
2.6 Replication Settings 8
2.7 Transaction Logging 8
2.8 Replication Mode of AhsayOBS 9
2.9 Monthly RESYNC 14
3 Best Practices and Recommendations 15
3.1 AhsayRPS Hardware Requirements 15
3.2 AhsayRPS Server Storage Requirements 15
3.3 AhsayOBS Replication Partitioning 15
3.4 Replication Performance Tuning 16
3.5 AhsayRPS Java Heap Size Setting 17
3.6 AhsayRPS and Multiple Receivers 17
3.7 Enable AhsayRPS CRC Checking 17
3.8 Avoid Using Dynamic IP Addresses 17
3.9 Using Different Ports for Different Receivers 18
3.10 Firewall Settings 18
3.11 Third Party Monitoring Software 18
3.12 Do Not Operate AhsayOBS and AhsayRPS on a Single Machine 18
3.13 Performing an AhsayOBS Seed Load 18
3.14 AhsayRPS Dedicated Restore Drive 19
3.15 AhsayOBS and Dual WAN Routers 19
3.16 Replication Using Cross Over Cable 19
4 Quick Start 20
4.1 Getting started 20
5 Installation 23
6 Manage AhsayRPS System 24
6.1 Server Configuration 24
6.2 System Log 25
7 Manage Receiver on AhsayRPS 26
7.1 Create Receivers 26
7.2 Retention Feature 27
7.2.1 Retention Settings 27
7.2.2 Retention Policy Considerations 28
7.2.3 Retention Policy Job 28
7.2.4 Disabling AhsayRPS Retention 29
7.3 CRC Redundancy Check (CRC) Checking 30
7.4 List all Receivers 34
7.5 Edit Receiver's Profile 35

7.6 File Explorer 37
7.7 Retention Recovery 37
7.8 Replication Log 39
8 Replication Configuration on AhsayOBS 40
8.1 Mandatory Replication Setting 40
8.2 Use Proxy 41
8.3 Traffic Limit 42
8.4 Selective User Replication 43
8.5 Replication Log 45
8.6 Enable/Disable Replication Service 45
9 Starting AhsayRPS as AhsayOBS 46
10 Advanced Configuration 48
10.1 Restricting access to system page by IP address 48
11 Troubleshooting 50
11.1 Connections Errors 50
11.2 Authentication Errors 51
11.3 Replication Always Restarting 51
11.4 Replication Connection Timeouts 52
12 Further Information 53
Appendix 54
Appendix A Product Documentations 54
Appendix B How to restore files from AhsayRPS 55

1 Introduction

Ahsay Replication Server (AhsayRPS) is a replication solution specially designed for AhsayOBS. With the use of AhsayOBS replication module, it can provide close to real time data protection to the data stored on the multiple AhsayOBS.

1.1 Conventions

Convention	Descriptions	Example
Bold	Important information	**WARNING: You must check the timestamp of obrA.jar before proceeding to step 2.**
Italic	Folder path or file path	*/usr/local/obs/conf*
[]	Graphical Interface Elements	[Manage Log]
%%	File path in Windows format	%OBSR_HOME%
$	File path in Linux/FreeBSD/Solaris format	$OBSR_HOME
italic	Command	*mkdir /usr/local/obs*

1.2 Definitions, Acronyms and Abbreviation

Term / Abbreviation	Definition
AhsayOBS	Ahsay™ Offsite Backup Server
AhsayRPS	Ahsay™ Replication Server
AhsayRDR	Ahsay™ Redirector Server
AhsayOBM	Ahsay™ Online Backup Manager
AhsayACB	Ahsay™ A-Click Backup
OBSR_HOME	The install location of AhsayOBS & AhsayRPS. Windows *C:\Program Files\AhsayOBS and AhsayRPS* Linux/FreeBSD/Solaris /usr/local/obs/
OBSR_HOME_BAK	The backup location of AhsayOBS & AhsayRPS. It is used temporary during the install/upgrade process. Windows *C:\Program Files\AhsayOBS and AhsayRPS.bak*

	Linux/FreeBSD/Solaris */usr/local/obs.bak/*
CONF_HOME	The backup location of AhsayOBS & AhsayRPS. It is used temporary during the install/upgrade process. Windows *%OBSR_HOME%\conf* Linux/FreeBSD/Solaris $OBSR_HOME/conf
USER_HOMES	The directories where AhsayOBS and AhsayRPS store the AhsayOBM & AhsayACB users accounts. The default location is: *%OBSR_HOME%\users*
POLICY_HOME	The directory where AhsayOBS and AhsayRPS store its system users and group policy information. Windows *%OBSR_HOME%\system\policy* Linux/FreeBSD/Solaris $OBSR_HOME\system\policy
SYSTEM_HOME	The directory where AhsayOBS and AhsayRPS store its system information. Windows *%OBSR_HOME%\system* Linux/FreeBSD/Solaris *$OBSR_HOME\system*
WEBAPPS_HOME	Location of the webapps directory inside the installation directory of AhsayOBS & AhsayRPS. Windows *%OBSR_HOME%\webapps.* Linux/FreeBSD/Solaris *$OBSR_HOME\webapps*
WEBAPP_HOME_BAK	A backup of the webapps directory inside AhsayOBS and AhsayRPS. Windows *%OBSR_HOME%\webapps.bak*

	Linux/FreeBSD/Solaris *$OBSR_HOME\webapps.bak*
RECEIVER_HOME	The location where the replicated data is stored for a particular replication receiver.
JAVA_HOME	The location where JAVA is installed

1.3 System Requirements

Please refer to the FAQ: Ahsay Software Compatibility List (SCL) for version 6.3 or above (2323) for the system requirements.

AhsayRPS v6 supports replication for AhsayOBS v5.5.3.0 or above.

2 Overview

This chapter introduces you to the AhsayOBS replication module and the AhsayRPS server.

2.1 Ahsay Replication Server

Ahsay Replication Server provides an additional layer of data protection by providing an offsite backup store for backing up data from either a single or multiple AhsayOBS servers. The Ahsay replication process is close to real-time and hence this will reduce the probability of significant data loss in the event of an AhsayOBS outage.

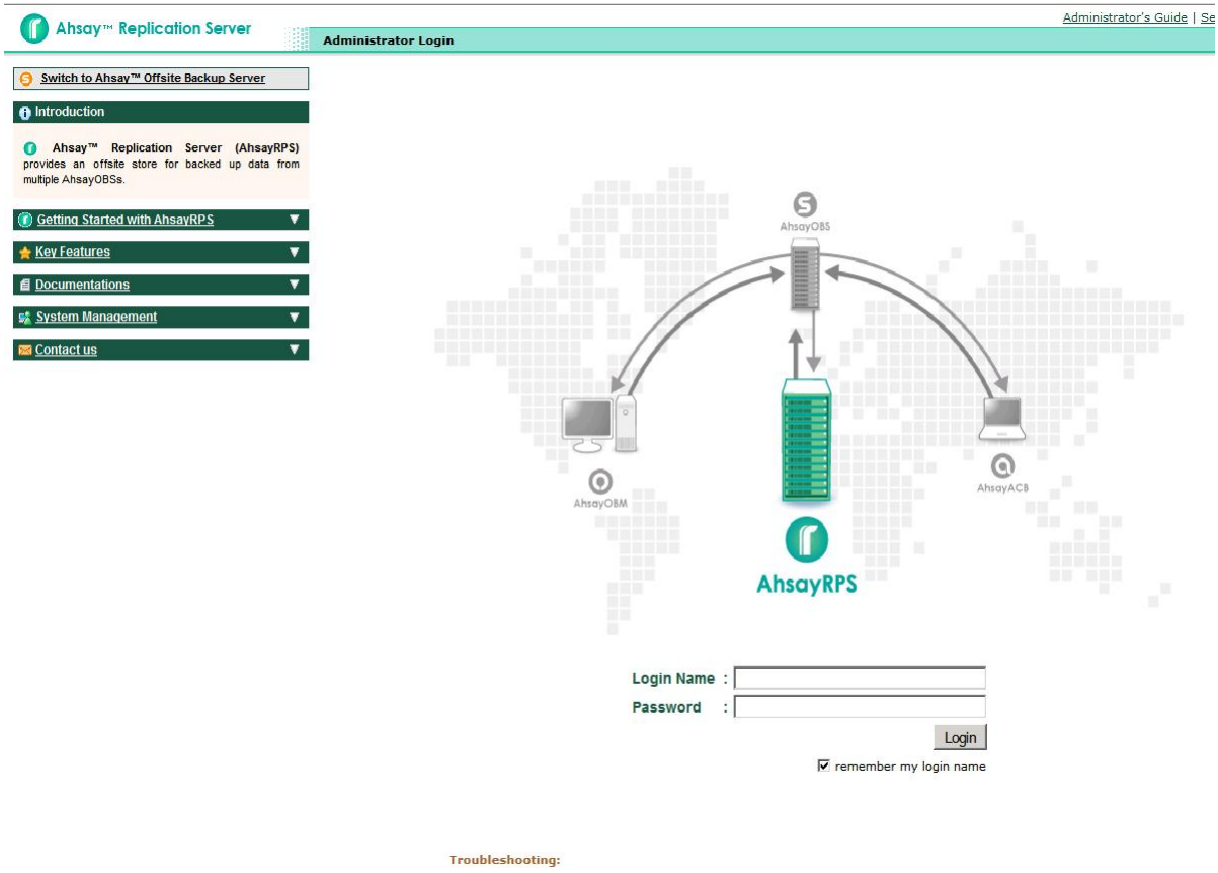
2.2 Ahsay Replication Server Administration Console

As both AhsayRPS and AhsayOBS features have been merged into one installer. Once installed you can choose which service you wish to activate either AhsayOBS or AhsayRPS service.

To access the AhsayRPS Administration Console, please do the following:

1. Point to http://<your-replication-server> on web browser and the AhsayOBS Administration Console will be shown.

2. Click on "Switch to Replication Server" to go to Ahsay Replication Server Administration Mode.



Alternatively, **you can access the AhsayRPS Administration Console page directly using the following URL** http://<your-replication-server>/rps-helper/index.jsp

2.3 AhsayOBS Replication Module

AhsayOBS replication module is specially designed for replicating both AhsayOBS user home data and AhsayOBS program or binary files to AhsayRPS server. It is designed to provide replication services for AhsayOBS only and it does not provide general replication service for other files within the system. This means that you cannot use AhsayOBS replication to replicate your Windows/Linux/Unix server to another machine.

Since it is an AhsayOBS aware replication module, it has the following benefits over using other external synchronizing software (e.g. rsync or Microsoft Replication Services) in the context of replicating backup data on AhsayOBS to another server.

Real Time Replication

When a backup block arrives at the backup server, it is automatically put into the replication queue. Data in the replication queue are replicated to AhsayRPS immediately (or at a delay of at most 1 minute). No replication schedules or extensive checking of whether each file should be replicated are required.

Platform Independence

As AhsayOBS and AhsayRPS supports Windows, Linux, FreeBSD, or Solaris platforms. This means that you can have AhsayOBS running on Windows and AhsayRPS running on Linux/FreeBSD/Solaris or other possible combinations.

No Interuption to Existing Backup Operations

Since AhsayOBS replication module will be replicating transaction log files, instead of the actual backup files, to the AhsayRPS, normal write access to the backup files will not be interrupted and this can ensure normal backup operation of AhsayOBS.

Secured and Compression Connection

Replication data are transported under a 128-bit SSL and compressed channel. Data transferred between AhsayOBS and AhsayRPS is secured and optimized.

Transaction Log Level Replication

AhsayOBS replication module logs all transaction made on AhsayOBS and replicates only the transaction log file to AhsayRPS. This means that only changes applies to the user data will be required to be replicated to AhsayRPS.

Replicating Selective Users from AhsayOBS to AhsayRPS

It is possible to select specific users from AhsayOBS to replicate to AhsayRPS, instead of just replicating all users on all the user homes.

2.4 Replication Scope

The following folders are included in the replication process:

- %OBSR_HOME% (files only)
- %OBSR_HOME%\bin
- %OBSR_HOME%\conf
- %OBSR_HOME%\java
- %OBSR_HOME%\system (a.k.a. SYSTEM_HOME of AhsayRPS)
- %OBSR_HOME%\tomcat
- %OBSR_HOME%\webapps
- %OBSR_HOME%\work
- %USER_HOMES% (according to your replication settings, some users may not be included in the replication.

The index files (r-index.bdb and index.bdb) for each backupset are not replicated to AhsayRPS as part of the replication process. Since they are updated frequently, any copies on AhsayRPS would be outdated as soon as it is replicated. When replication skips an index files it will record in the replication log the following entries:

Skip replicating index BDB files '……/index.bdb'
Or
Skip replicating index BDB files '……./r-index.bdb

The following is an example of entries that you are likely to find on the ManageLog] -> [Replication Log] page.

364	12:55:21 PM	[N] Replicating '/data/user/acb2/db/Profile.xml.8' (3k, 2011-02-20 09:30)
365	12:55:21 PM	[N] Replicating '/data/user/acb2/db/Profile.xml.9' (3k, 2011-02-20 09:30)
366	12:55:21 PM	[N] Replicating '/data/user/acb2/db/RestoreLog/2011-02-07-13-43-24.log' (176, 2011-02-07 13:44)
367	12:55:21 PM	[N] Replicating '/data/user/acb2/db/StorageLog/2011-02.log' (578, 2011-02-25 09:55)
368	12:55:21 PM	[N] Replicating '/data/user/acb2/db/UserLog/2011-02-07.log' (6k, 2011-02-07 13:44)
369	12:55:21 PM	[N] Replicating '/data/user/acb2/files/-1297048893023/Current/root/3404278061' (1k, 2011-02-20 09:30)
370	12:55:21 PM	Skip replicating index BDB files '/data/user/acb2/files/-1297048893023/index.bdb'
371	12:55:21 PM	[N] Replicating '/data/user/acb2/files/-1297048893023/info.xml' (105, 2011-02-07 13:43)
372	12:55:21 PM	Skip replicating index BDB files '/data/user/acb2/files/-1297048893023/r-index.bdb'
373	12:55:21 PM	Skip replicating index BDB files '/data/user/acb2/files/0/index.bdb'
374	12:55:21 PM	[N] Replicating '/data/user/acb2/files/0/info.xml' (85, 2011-02-07 13:43)
375	12:55:21 PM	Skip replicating index BDB files '/data/user/acb2/files/0/r-index.bdb'
376	12:55:21 PM	Listing remote '/data/user/acb3'
377	12:55:21 PM	[N] Replicating '/data/user/acb3/db/Profile.xml' (3k, 2011-02-25 09:55)
378	12:55:21 PM	[N] Replicating '/data/user/acb3/db/Profile.xml.1' (3k, 2011-02-24 09:55)
379	12:55:21 PM	[N] Replicating '/data/user/acb3/db/Profile.xml.10' (3k, 2011-02-17 09:55)
380	12:55:21 PM	[N] Replicating '/data/user/acb3/db/Profile.xml.11' (3k, 2011-02-16 09:55)
381	12:55:21 PM	[N] Replicating '/data/user/acb3/db/Profile.xml.2' (3k, 2011-02-23 09:55)
382	12:55:21 PM	[N] Replicating '/data/user/acb3/db/Profile.xml.3' (3k, 2011-02-22 09:55)
383	12:55:21 PM	[N] Replicating '/data/user/acb3/db/Profile.xml.4' (3k, 2011-02-21 09:55)
384	12:55:21 PM	[N] Replicating '/data/user/acb3/db/Profile.xml.5' (3k, 2011-02-20 09:55)
385	12:55:21 PM	[N] Replicating '/data/user/acb3/db/Profile.xml.6' (3k, 2011-02-20 09:30)

2.5 Replication Order

For each user home the user accounts will be listed and replicated in the following order:

i. Numeric user accounts

ii. Upper case user accounts

iii. Lower case user accounts

2.6 Replication Settings

Replication settings are saved in *%OBSR_HOME%/conf/lfsconfig.xml* and *%OBSR_HOME%/conf/rpsSend.xml*.

2.7 Transaction Logging

When backup data arrives on the backup server, an extra copy of this data is saved in the transaction log files. (It only happens when AhsayOBS replication module is in LOGGING or SYNC mode. The transaction log file(s) will then be replicated to AhsayRPS and replayed into the affected backup files replicated to AhsayRPS ready to produce a consistent backup image of all data available on the backup server.

Transaction log files are saved in *%SYSTEM_HOME%/logfiles/log????.alf* (e.g. log log0395.alf where "0395" is the sequence number of the transaction log files).

When using AhsayOBS with replication module enabled, please make sure that the [Manage System] -> [Server Configuration] -> [System Home] setting is set in a disk partition with lots of free disk space.

To provide a consistent view of the backup file system while AhsayOBS is running in SYNC mode, AhsayOBS uses the %SYSTEM_HOME%/sync/*** directory to store many of the temporary files required. Please do not tamper with the files in this directory and make sure that it has lots of free space.

2.8 Replication Mode of AhsayOBS

When replication is running, there are four distinct replication modes : Resfreshing File, UNSYNC, SYNC, and LOGGING mode.

1. Refreshing File

When AhsayOBS replication module is started up, it first replicates AhsayOBS program binaries and configuration files to AhsayRPS during "Refreshing File" mode. No data under SYSTEM_HOME, POLICY_HOME and USER_HOMES will be replicated to AhsayRPS in this mode.

Since program binaries and configuration files rarely change and there are limited numbers of these files, this part is completed relatively quickly.

The following is an example of entries that you are likely to find on [Manage Log] -> [Replication Log] page during refreshing mode.

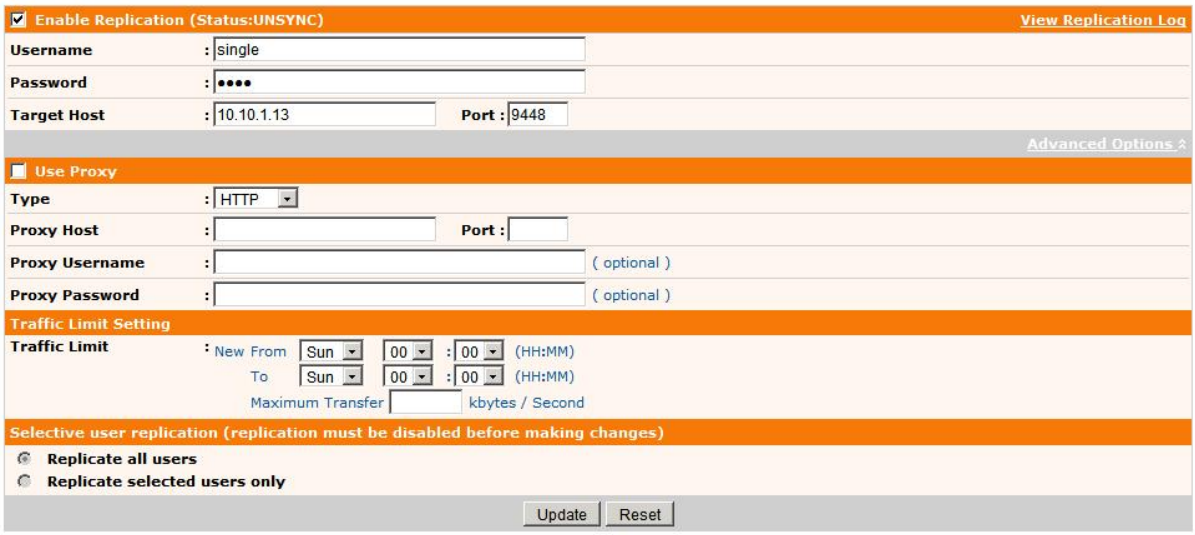
No.	Timestamp	Message
1	05:11:48 PM	[Start] Replication
2	05:11:48 PM	[Start] Refreshing File
3	05:11:49 PM	RPS Version: 6.2.3.0
4	05:11:49 PM	Listing remote '/'
5	05:11:49 PM	[N] Replicating '/usr/local/obs6/bin/ExtractBackupFileHeaders.sh' (2k, 2010-12-20 14:38)
6	05:11:49 PM	[N] Replicating '/usr/local/obs6/bin/ListBackupFileIndex.sh' (3k, 2010-12-20 14:38)
7	05:11:49 PM	[N] Replicating '/usr/local/obs6/bin/browse.sh' (108, 2008-08-15 11:51)
8	05:11:49 PM	[N] Replicating '/usr/local/obs6/bin/install.sh' (4k, 2011-01-26 18:52)
9	05:11:49 PM	[N] Replicating '/usr/local/obs6/bin/obsr' (1014, 2011-01-26 18:52)
10	05:11:49 PM	[N] Replicating '/usr/local/obs6/bin/obsr-bsd' (1k, 2011-01-19 11:18)
11	05:11:49 PM	[N] Replicating '/usr/local/obs6/bin/obsr-sysv' (1k, 2011-01-19 11:18)
12	05:11:49 PM	[N] Replicating '/usr/local/obs6/bin/shutdown.sh' (7k, 2010-09-24 14:45)
13	05:11:49 PM	[N] Replicating '/usr/local/obs6/bin/startup.sh' (12k, 2011-01-26 18:51)
14	05:11:49 PM	[N] Replicating '/usr/local/obs6/bin/uninstall.sh' (1k, 2011-01-19 11:18)
15	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/acb-config.xml' (1k, 2008-01-15 18:24)
16	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/acb-config.xml.original' (1k, 2008-01-15 18:24)
17	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/autoDiscovery.xml' (70, 2008-05-23 14:57)
18	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/autoDiscovery.xml.original' (70, 2008-05-23 14:57)
19	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/catalina.policy' (6k, 2002-06-11 13:09)
20	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/custom-port.jar' (12k, 2006-05-24 18:00)
21	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/debug.props' (93, 2006-07-28 16:19)
22	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/keystore' (14k, 2004-03-22 18:49)
23	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/lfsConfig.xml' (255, 2011-02-09 17:06)
24	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/lfsConfig.xml.1' (255, 2011-02-09 17:06)
25	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/lfsConfig.xml.10' (257, 2011-02-09 16:54)
26	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/lfsConfig.xml.2' (255, 2011-02-09 17:06)
27	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/lfsConfig.xml.3' (255, 2011-02-09 16:59)
28	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/lfsConfig.xml.4' (257, 2011-02-09 16:59)
29	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/lfsConfig.xml.5' (257, 2011-02-09 16:59)
30	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/lfsConfig.xml.6' (257, 2011-02-09 16:58)
31	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/lfsConfig.xml.7' (257, 2011-02-09 16:57)
32	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/lfsConfig.xml.8' (257, 2011-02-09 16:56)
33	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/lfsConfig.xml.9' (257, 2011-02-09 16:55)
34	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/license.xml' (562, 2011-02-09 11:33)
35	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/license.xml.1' (562, 2011-02-14 08:03)
36	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/license.xml.10' (562, 2011-02-04 08:01)
37	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/license.xml.11' (562, 2011-02-03 08:01)
38	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/license.xml.2' (562, 2011-02-13 18:00)
39	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/license.xml.3' (562, 2011-02-12 17:40)
40	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/license.xml.4' (562, 2011-02-10 17:40)
41	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/license.xml.5' (562, 2011-02-09 16:30)
42	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/license.xml.6' (562, 2011-02-08 08:01)
43	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/license.xml.7' (562, 2011-02-07 08:01)
44	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/license.xml.8' (562, 2011-02-06 08:01)
45	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/license.xml.9' (562, 2011-02-05 08:01)
46	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/logging.properties' (230, 2009-01-13 12:26)
47	05:11:49 PM	[N] Replicating '/usr/local/obs6/conf/mergeQueue.xml' (54, 2011-02-13 20:59)

During the execution of this process the transaction logging on AhsayOBS is disabled. Backup data is written directly to the backup files on the AhsayOBS user home.

Note : Although at this stage replication is in refreshing mode, the AhsayOBS web console [Manage System] -> [Replication Config] page under "Enabled Replication" checkbox. The replication status is shown as "Status: UNSYNC".

2. UNSYNC Replication (UNSYNC mode)

When replication is in UNSYNC mode, the AhsayOBS web console [Manage System] -> [Replication Config] page under "Enabled Replication" checkbox. The replication status is updated to "Status: UNSYNC".



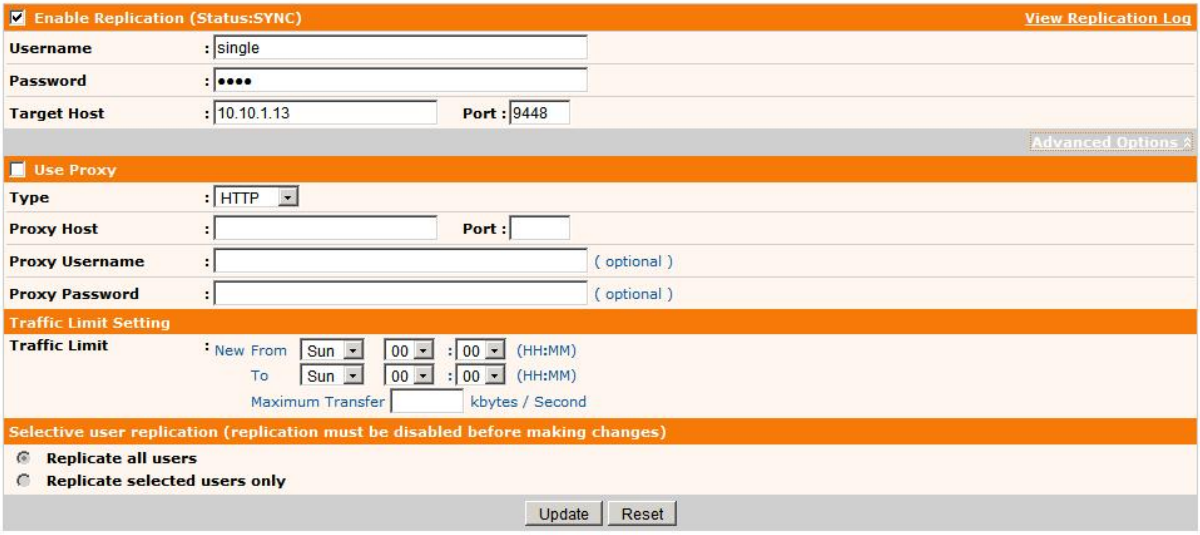
After the replication module has finished replicating all program binaries and configuration files, it will start replicating all files under the SYSTEM_HOME, POLICY_HOME and USER_HOMES directories to AhsayRPS. During the execution of this task, transaction logging of AhsayOBS is disabled. Backup data is written directly to the backup files on the AhsayOBS user home.

The following is an example of entries that you are likely to find on [Manage Log] -> [Replication Log] page during UNSYNC mode.

316	12:58:20 PM	[Start] Replicating files in UNSYNC mode
317	12:58:20 PM	RPS Version: 6.2.3.0
318	12:58:20 PM	Listing remote '/'
319	12:58:20 PM	Listing remote '/data'
320	12:58:20 PM	Listing remote '/data/user'
321	12:58:20 PM	Deleting remote '/data/user/1'
322	12:58:52 PM	Deleting remote '/data/user/a'
323	12:59:05 PM	Listing remote '/data/user/aa'
324	12:59:05 PM	[N] Replicating '/data/user/aa/db/Profile.xml' (1k, 2011-02-25 09:55)
325	12:59:05 PM	[N] Replicating '/data/user/aa/db/Profile.xml.1' (1k, 2011-02-24 09:55)
326	12:59:05 PM	[N] Replicating '/data/user/aa/db/Profile.xml.2' (1k, 2011-02-23 14:23)
327	12:59:05 PM	[N] Replicating '/data/user/aa/db/StorageLog/2011-02.log' (60, 2011-02-25 09:55)
328	12:59:05 PM	[N] Replicating '/data/user/aa/db/UserLog/2011-02-23.log' (745, 2011-02-23 14:23)
329	12:59:05 PM	Listing remote '/data/user/acb1'
330	12:59:05 PM	[N] Replicating '/data/user/acb1/db/Profile.xml' (3k, 2011-02-25 09:55)
331	12:59:05 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.1' (3k, 2011-02-24 09:55)
332	12:59:05 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.10' (3k, 2011-02-18 09:55)
333	12:59:05 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.11' (3k, 2011-02-17 09:55)
334	12:59:05 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.2' (3k, 2011-02-23 09:55)
335	12:59:05 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.3' (3k, 2011-02-22 09:55)
336	12:59:05 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.4' (3k, 2011-02-21 09:55)
337	12:59:05 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.5' (3k, 2011-02-20 09:55)
338	12:59:05 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.6' (3k, 2011-02-20 09:30)
339	12:59:05 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.7' (3k, 2011-02-20 09:30)
340	12:59:05 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.8' (3k, 2011-02-20 09:30)
341	12:59:05 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.9' (3k, 2011-02-19 09:55)
342	12:59:05 PM	[N] Replicating '/data/user/acb1/db/StorageLog/2011-02.log' (510, 2011-02-25 09:55)
343	12:59:05 PM	[N] Replicating '/data/user/acb1/db/UserLog/2011-02-07.log' (2k, 2011-02-07 11:28)
344	12:59:05 PM	Skip replicating index BDB files '/data/user/acb1/files/1297049299157/index.bdb'
345	12:59:05 PM	[N] Replicating '/data/user/acb1/files/1297049299157/info.xml' (97, 2011-02-07 11:28)
346	12:59:05 PM	Skip replicating index BDB files '/data/user/acb1/files/1297049299157/r-index.bdb'
347	12:59:05 PM	Listing remote '/data/user/acb2'

3. SYNC Replication (SYNC mode)

When replication reaches SYNC mode, the AhsayOBS web console [Manage System] -> [Replication Config] page under "Enabled Replication" checkbox. The replication status is updated to "Status: SYNC".

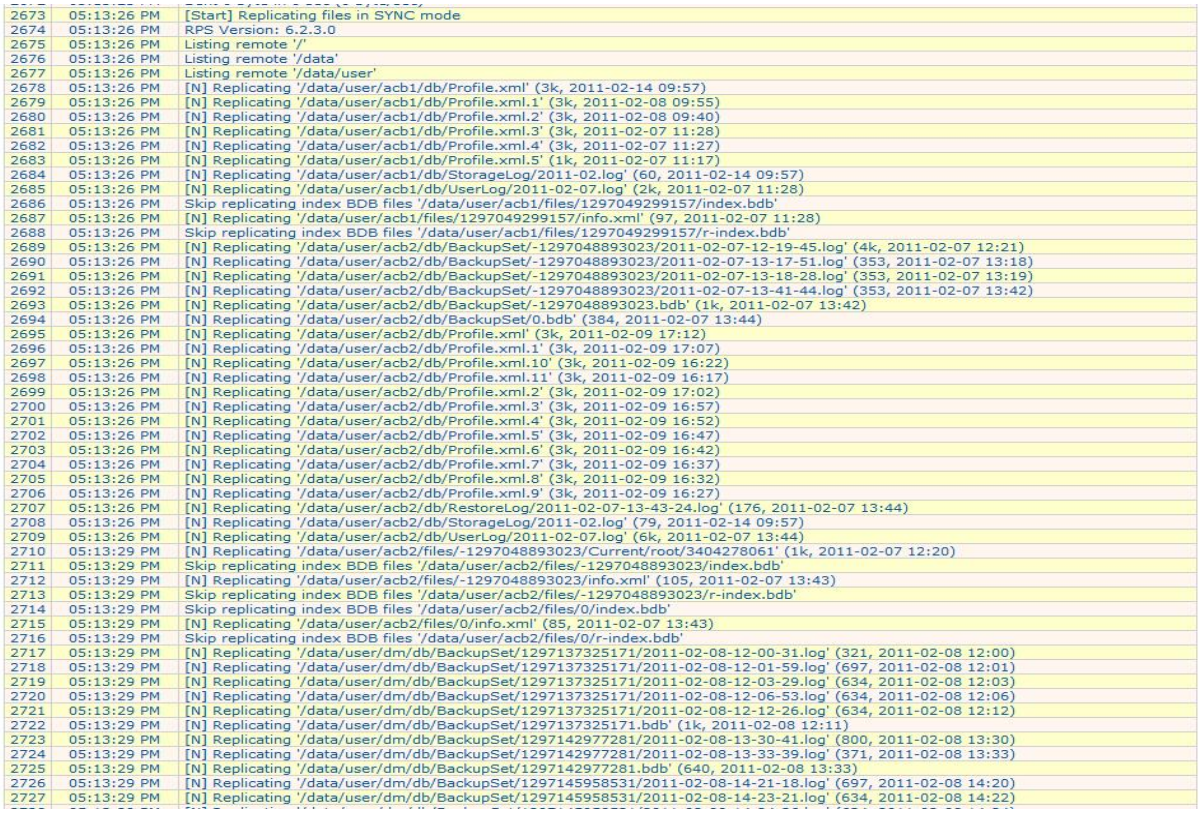


Since it could take hours (or even days) to replicate all backup data form AhsayOBS to AhsayRPS, by the time all files under SYSTEM_HOME, POLICY_HOME and USER_HOMES are replicated, some files might have been added/removed/updated from these directories. To ensure AhsayRPS contains an exact copy of all files available in SYSTEM_HOME, POLICY_HOME and USER_HOMES directories on AhsayOBS, we should make sure that there is no change to all files under these directories during the replication process. To do so, AhsayOBS replication module will put AhsayOBS into SYNC mode.

Once in SYNC mode:

- All files under the USER_HOMES, SYSTEM_HOME and POLICY_HOME directories that are updated after being replicated in UNSYNC replication are replicated again.
- During the execution of this task, transaction logging of AhsayOBS is enabled. Backup data is written directly to the respective backup files on the user home, in addition a copy of this data is made to the transaction log files.

The following is an example of entries that you are likely to find on [Manage Log] -> [Replication Log] page during SYNC mode

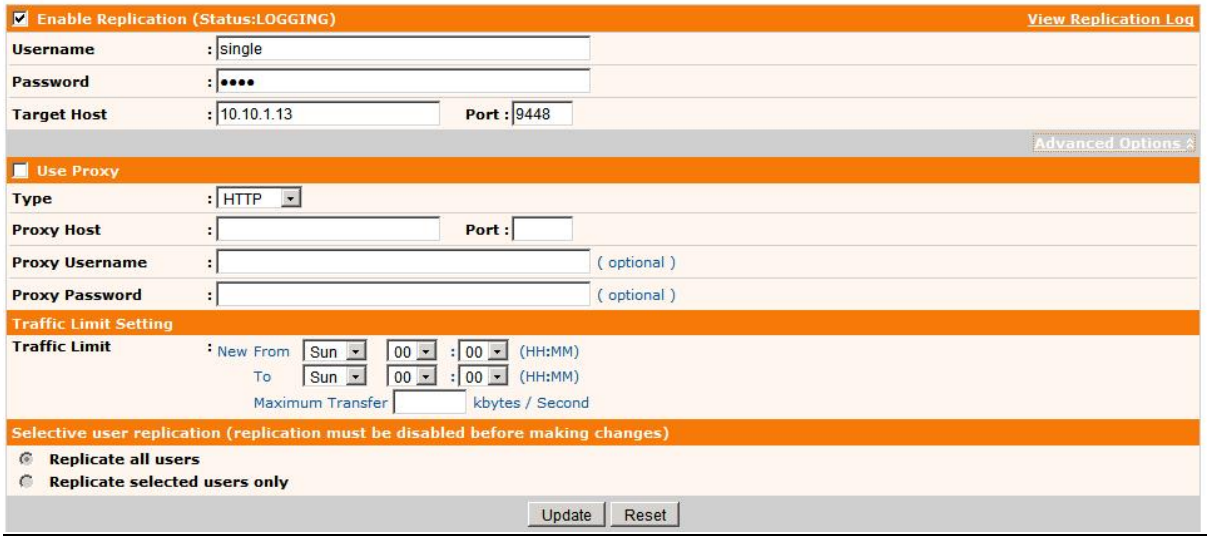


2673	05:13:26 PM	[Start] Replicating files in SYNC mode
2674	05:13:26 PM	RPS Version: 6.2.3.0
2675	05:13:26 PM	Listing remote '/'
2676	05:13:26 PM	Listing remote '/data'
2677	05:13:26 PM	Listing remote '/data/user'
2678	05:13:26 PM	[N] Replicating '/data/user/acb1/db/Profile.xml' (3k, 2011-02-14 09:57)
2679	05:13:26 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.1' (3k, 2011-02-08 09:55)
2680	05:13:26 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.2' (3k, 2011-02-08 09:40)
2681	05:13:26 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.3' (3k, 2011-02-07 11:28)
2682	05:13:26 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.4' (3k, 2011-02-07 11:27)
2683	05:13:26 PM	[N] Replicating '/data/user/acb1/db/Profile.xml.5' (1k, 2011-02-07 11:17)
2684	05:13:26 PM	[N] Replicating '/data/user/acb1/db/StorageLog/2011-02.log' (60, 2011-02-14 09:57)
2685	05:13:26 PM	[N] Replicating '/data/user/acb1/db/UserLog/2011-02-07.log' (2k, 2011-02-07 11:28)
2686	05:13:26 PM	Skip replicating index BDB files '/data/user/acb1/files/1297049299157/index.bdb'
2687	05:13:26 PM	[N] Replicating '/data/user/acb1/files/1297049299157/info.xml' (97, 2011-02-07 11:28)
2688	05:13:26 PM	Skip replicating index BDB files '/data/user/acb1/files/1297049299157/r-index.bdb'
2689	05:13:26 PM	[N] Replicating '/data/user/acb2/db/BackupSet/-1297048893023/2011-02-07-12-19-45.log' (4k, 2011-02-07 12:21)
2690	05:13:26 PM	[N] Replicating '/data/user/acb2/db/BackupSet/-1297048893023/2011-02-07-13-17-51.log' (353, 2011-02-07 13:18)
2691	05:13:26 PM	[N] Replicating '/data/user/acb2/db/BackupSet/-1297048893023/2011-02-07-13-18-28.log' (353, 2011-02-07 13:19)
2692	05:13:26 PM	[N] Replicating '/data/user/acb2/db/BackupSet/-1297048893023/2011-02-07-13-41-44.log' (353, 2011-02-07 13:42)
2693	05:13:26 PM	[N] Replicating '/data/user/acb2/db/BackupSet/-1297048893023.bdb' (1k, 2011-02-07 13:42)
2694	05:13:26 PM	[N] Replicating '/data/user/acb2/db/BackupSet/0.bdb' (384, 2011-02-07 13:44)
2695	05:13:26 PM	[N] Replicating '/data/user/acb2/db/Profile.xml' (3k, 2011-02-09 17:12)
2696	05:13:26 PM	[N] Replicating '/data/user/acb2/db/Profile.xml.1' (3k, 2011-02-09 17:07)
2697	05:13:26 PM	[N] Replicating '/data/user/acb2/db/Profile.xml.10' (3k, 2011-02-09 16:22)
2698	05:13:26 PM	[N] Replicating '/data/user/acb2/db/Profile.xml.11' (3k, 2011-02-09 16:17)
2699	05:13:26 PM	[N] Replicating '/data/user/acb2/db/Profile.xml.2' (3k, 2011-02-09 17:02)
2700	05:13:26 PM	[N] Replicating '/data/user/acb2/db/Profile.xml.3' (3k, 2011-02-09 16:57)
2701	05:13:26 PM	[N] Replicating '/data/user/acb2/db/Profile.xml.4' (3k, 2011-02-09 16:52)
2702	05:13:26 PM	[N] Replicating '/data/user/acb2/db/Profile.xml.5' (3k, 2011-02-09 16:47)
2703	05:13:26 PM	[N] Replicating '/data/user/acb2/db/Profile.xml.6' (3k, 2011-02-09 16:42)
2704	05:13:26 PM	[N] Replicating '/data/user/acb2/db/Profile.xml.7' (3k, 2011-02-09 16:37)
2705	05:13:26 PM	[N] Replicating '/data/user/acb2/db/Profile.xml.8' (3k, 2011-02-09 16:32)
2706	05:13:26 PM	[N] Replicating '/data/user/acb2/db/Profile.xml.9' (3k, 2011-02-09 16:27)
2707	05:13:26 PM	[N] Replicating '/data/user/acb2/db/RestoreLog/2011-02-07-13-43-24.log' (176, 2011-02-07 13:44)
2708	05:13:26 PM	[N] Replicating '/data/user/acb2/db/StorageLog/2011-02.log' (79, 2011-02-14 09:57)
2709	05:13:26 PM	[N] Replicating '/data/user/acb2/db/UserLog/2011-02-07.log' (6k, 2011-02-07 13:44)
2710	05:13:29 PM	[N] Replicating '/data/user/acb2/files/-1297048893023/Current/root/3404278061' (1k, 2011-02-07 12:20)
2711	05:13:29 PM	Skip replicating index BDB files '/data/user/acb2/files/-1297048893023/index.bdb'
2712	05:13:29 PM	[N] Replicating '/data/user/acb2/files/-1297048893023/info.xml' (105, 2011-02-07 13:43)
2713	05:13:29 PM	Skip replicating index BDB files '/data/user/acb2/files/-1297048893023/r-index.bdb'
2714	05:13:29 PM	Skip replicating index BDB files '/data/user/acb2/files/0/index.bdb'
2715	05:13:29 PM	[N] Replicating '/data/user/acb2/files/0/info.xml' (85, 2011-02-07 13:43)
2716	05:13:29 PM	Skip replicating index BDB files '/data/user/acb2/files/0/r-index.bdb'
2717	05:13:29 PM	[N] Replicating '/data/user/dm/db/BackupSet/1297137325171/2011-02-08-12-00-31.log' (321, 2011-02-08 12:00)
2718	05:13:29 PM	[N] Replicating '/data/user/dm/db/BackupSet/1297137325171/2011-02-08-12-01-59.log' (697, 2011-02-08 12:01)
2719	05:13:29 PM	[N] Replicating '/data/user/dm/db/BackupSet/1297137325171/2011-02-08-12-03-29.log' (634, 2011-02-08 12:03)
2720	05:13:29 PM	[N] Replicating '/data/user/dm/db/BackupSet/1297137325171/2011-02-08-12-06-53.log' (634, 2011-02-08 12:06)
2721	05:13:29 PM	[N] Replicating '/data/user/dm/db/BackupSet/1297137325171/2011-02-08-12-12-26.log' (634, 2011-02-08 12:12)
2722	05:13:29 PM	[N] Replicating '/data/user/dm/db/BackupSet/1297137325171.bdb' (1k, 2011-02-08 12:11)
2723	05:13:29 PM	[N] Replicating '/data/user/dm/db/BackupSet/1297142977281/2011-02-08-13-30-41.log' (800, 2011-02-08 13:30)
2724	05:13:29 PM	[N] Replicating '/data/user/dm/db/BackupSet/1297142977281/2011-02-08-13-33-39.log' (371, 2011-02-08 13:33)
2725	05:13:29 PM	[N] Replicating '/data/user/dm/db/BackupSet/1297142977281.bdb' (640, 2011-02-08 13:33)
2726	05:13:29 PM	[N] Replicating '/data/user/dm/db/BackupSet/1297145958531/2011-02-08-14-21-18.log' (697, 2011-02-08 14:20)
2727	05:13:29 PM	[N] Replicating '/data/user/dm/db/BackupSet/1297145958531/2011-02-08-14-23-21.log' (634, 2011-02-08 14:22)

At the end of SYNC mode, AhsayRPS does not contain changes in AhsayOBS. Synchronization can be easily done in the next mode, by replicating the transaction log file over from AhsayOBS to AhsayRPS and replaying these transaction logs on AhsayRPS.

4. Transaction Logs Replication (LOGGING Mode)

When replication reaches LOGGING mode, the AhsayOBS web console [Manage System] -> [Replication Config] page under "Enabled Replication" checkbox. The replication status is updated to "Status: LOGGING".



During LOGGING mode, transaction logging of AhsayOBS is also enabled backup data is written directly to the backup files that they are supposed to go to as well as to transaction log files. In LOGGING mode the replication logs will show only transaction log (logxxxx.alf) files replicated from AhsayOBS to AhsayRPS in this mode.

The following is an example of entries that you are likely to find on [Manage Log] -> [Replication Log] page during LOGGING mode.

5357	05:14:14 PM	[End] Replicating files in SYNC mode
5358	05:14:14 PM	Sent 216.63M byte in 47 sec (4.61M byte/sec)
5359	05:14:15 PM	RPS Version: 6.2.3.0
5360	05:14:15 PM	Replicating '/usr/local/obs6/system/logfiles/log0001.alf' (373k, 2011-02-09 17:14)
5361	05:14:15 PM	Replicating '/usr/local/obs6/system/logfiles/log0002.alf' (16, 2011-02-09 17:14)
5362	05:14:16 PM	Sent 39k byte in 0 sec (0 byte/sec)
5363	05:15:17 PM	RPS Version: 6.2.3.0
5364	05:15:17 PM	Replicating '/usr/local/obs6/system/logfiles/log0003.alf' (18k, 2011-02-09 17:15)
5365	05:15:17 PM	Sent 2k byte in 0 sec (0 byte/sec)
5366	05:16:18 PM	RPS Version: 6.2.3.0
5367	05:16:18 PM	Replicating '/usr/local/obs6/system/logfiles/log0004.alf' (5k, 2011-02-09 17:16)
5368	05:16:19 PM	Sent 2k byte in 0 sec (0 byte/sec)
5369	05:17:20 PM	RPS Version: 6.2.3.0
5370	05:17:20 PM	Replicating '/usr/local/obs6/system/logfiles/log0005.alf' (9k, 2011-02-09 17:17)
5371	05:17:20 PM	Sent 2k byte in 0 sec (0 byte/sec)
5372	05:18:22 PM	RPS Version: 6.2.3.0
5373	05:18:22 PM	Replicating '/usr/local/obs6/system/logfiles/log0006.alf' (5k, 2011-02-09 17:18)
5374	05:18:22 PM	Sent 2k byte in 0 sec (0 byte/sec)
5375	05:19:23 PM	RPS Version: 6.2.3.0
5376	05:19:23 PM	Replicating '/usr/local/obs6/system/logfiles/log0007.alf' (461, 2011-02-09 17:19)
5377	05:19:24 PM	Sent 387 byte in 0 sec (0 byte/sec)
5378	05:20:25 PM	RPS Version: 6.2.3.0
5379	05:20:25 PM	Replicating '/usr/local/obs6/system/logfiles/log0008.alf' (463, 2011-02-09 17:20)
5380	05:20:25 PM	Sent 389 byte in 0 sec (0 byte/sec)
5381	05:21:26 PM	RPS Version: 6.2.3.0
5382	05:21:26 PM	Replicating '/usr/local/obs6/system/logfiles/log0009.alf' (6k, 2011-02-09 17:21)
5383	05:21:27 PM	Sent 2k byte in 0 sec (0 byte/sec)

Since data in the USER_HOMES, SYSTEM_HOME, and POLICY_HOME directories of AhsayOBS and AhsayRPS have been synchronized already in SYNC mode, it requires only replaying all transaction log files recorded after the beginning of the SYNC period on the AhsayRPS to bring AhsayRPS into a consistent state with AhsayOBS.

When there are no backup activities and all pending transaction log files have been replicated to AhsayRPS, transaction log files are replicated to AhsayRPS every 1 minute (even when empty). This will ensure that ~~partial record within~~ transaction log files get replicated to AhsayRPS in close to real-time. Since compression is enabled by default, replicating empty transaction log files will not use much network bandwidth.

Note: In the event of any errors encountered during LOGGING mode, replication will be restarted in SYNC mode, only if the replication has reached the LOGGING mode within the last 7 days. Otherwise, it restart from UNSYNC mode.

2.9 Monthly RESYNC

To ensure the data on the replication server is fully in sync with the backup server after lots of transaction logs have been applied on the replication server, a monthly RESYNC job will run on the first Saturday of each month at 1:00pm, if replication is in LOGGING mode. This involves running "Refreshing Files", "UNSYNC Replication" and "SYNC Replication" all over again.

In addition, AhsayOBS will perform a check every time replication is enabled. If AhsayOBS detects that more than 31 days has passed since the last monthly resync or SYNC mode, then an immediate resync initiated.

No.	Timestamp	Message
1	12:30:21 PM	[Start] Replication
2	12:30:21 PM	[MonthlyJob] Resyncing all files again because it hasn't been run for the past 31 days
3	12:30:21 PM	[MonthlyJob] Resyncing all files again
4	12:30:21 PM	[Start] Refreshing File
5	12:30:23 PM	RPS Version: 6.2.3.0
6	12:30:23 PM	Listing remote '/'
7	12:30:23 PM	Listing remote '/usr'
8	12:30:23 PM	Listing remote '/usr/local'
9	12:30:23 PM	Listing remote '/usr/local/obs6'
10	12:30:23 PM	Listing remote '/usr/local/obs6/bin'
11	12:30:23 PM	Listing remote '/usr/local/obs6/conf'
12	12:30:23 PM	[T] Replicating '/usr/local/obs6/conf/lfsConfig.xml' (252, 2011-08-06 12:30)
13	12:30:23 PM	[T] Replicating '/usr/local/obs6/conf/lfsConfig.xml.1' (252, 2011-06-04 13:28)
14	12:30:23 PM	[ST] Replicating '/usr/local/obs6/conf/lfsConfig.xml.10' (255, 2011-06-04 13:20)
15	12:30:23 PM	[ST] Replicating '/usr/local/obs6/conf/lfsConfig.xml.2' (255, 2011-06-04 13:28)
16	12:30:23 PM	[ST] Replicating '/usr/local/obs6/conf/lfsConfig.xml.3' (255, 2011-06-04 13:27)
17	12:30:23 PM	[ST] Replicating '/usr/local/obs6/conf/lfsConfig.xml.4' (255, 2011-06-04 13:26)
18	12:30:23 PM	[ST] Replicating '/usr/local/obs6/conf/lfsConfig.xml.5' (255, 2011-06-04 13:25)
19	12:30:23 PM	[ST] Replicating '/usr/local/obs6/conf/lfsConfig.xml.6' (255, 2011-06-04 13:24)
20	12:30:23 PM	[ST] Replicating '/usr/local/obs6/conf/lfsConfig.xml.7' (255, 2011-06-04 13:23)
21	12:30:23 PM	[ST] Replicating '/usr/local/obs6/conf/lfsConfig.xml.8' (255, 2011-06-04 13:22)
22	12:30:23 PM	[ST] Replicating '/usr/local/obs6/conf/lfsConfig.xml.9' (255, 2011-06-04 13:21)
23	12:30:23 PM	[T] Replicating '/usr/local/obs6/conf/license.xml' (562, 2011-08-06 12:30)
24	12:30:23 PM	[T] Replicating '/usr/local/obs6/conf/license.xml.1' (562, 2011-06-04 12:30)
25	12:30:34 PM	[End] Refreshing File
26	12:30:34 PM	Sent 3k byte in 13 sec (276 byte/sec)

3 Best Practices and Recommendations

This chapter outlines all the best practices and recommendations which you should consider before using AhsayRPS.

3.1 AhsayRPS Hardware Requirements

As the AhsayRPS server is used as a backup or a standby machine in case of an AhsayOBS server outage. The hardware specifications of your AhsayRPS server should be similar to your AhsayOBS server. To ensure that when you re-configure and startup your AhsayRPS server as an AhsayOBS server, there will not be any performance issues.

3.2 AhsayRPS Server Storage Requirements

There is a possibility that after your AhsayOBS data is replicated to AhsayRPS, the final data size on AhsayRPS may be larger than the original data size on AhsayOBS. This situation could arise if there are differences in the way each respective storage devices is formatted, i.e. different default block sizes or different files systems

The disk capacity of your AhsayRPS server should by default be greater than your AhsayOBS server in order to avoid such problems.

3.3 AhsayOBS Replication Partitioning

AhsayOBS replication module makes heavy use of the [Manage System] -> [System Home] directory to create a consistent view of the backup file system under SYNC replication mode. During SYNC mode copies of the backup data will be written to the [System Home] in the form of transaction log files

It is not recommended to use the O/S partition or drive as the [System Home]. If the [System Home] folder fills up, this will cause your O/S to become unstable and may even crash your AhsayOBS server. **It is strongly recommended the [System Home] directory should be located on a dedicated local drive.**

The [System Home] should have plenty of free space. There is no exact formula for estimating the size of the [System Home]. As the amount of space used in SYNC mode is dependent on:

i. The period of time the replication process is in SYNC mode
ii. The amount of daily backup data uploaded to your AhsayOBS server

For example, if daily customer backup jobs generate an average of 20GB of data daily. Your previous replication SYNC mode time period was 5 days

before it went into LOGGING mode, then your [System Home] partition will require at least 100GB (20GB x 5 days) of free disk space.

This is only a general rule of thumb, this estimation does not take into consideration the growth of daily backup data, or the accumulation of backup data on AhsayOBS which will result in a longer SYNC mode time period.

3.4 Replication Performance Tuning

Even with a fast and stable connection between AhsayOBS and AhsayRPS, replication performance is affected more by:

i. Poor AhsayOBS disk I/O – when scanning and retrieving data files to be sent to AhsayRPS.

ii. Poor AhsayRPS disk I/O – when receiving and committing files to the receiver home.

Poor disk I/O can be attributed to:

i. The use of network drives as AhsayOBS user and system homes

ii. The use of network drives as AhsayRPS receiver home(s)

iii. The use of a single large disk or volume for AhsayOBS user home

iv. The use of a single large disk or volume for multiple AhsayRPS receiver home(s)

v. Slow performing local hard drives or storage devices

In addition, on AhsayOBS certain routine system jobs such as the Cyclic Redundancy Check (CRC) Checking, weekly Rebuild User Storage, and multiple single Rebuild User Storage jobs will increase the I/O load on AhsayOBS user homes. On AhsayRPS, the Cyclic Redundancy Check (CRC) Checking routine job for each replication receiver will also affect replication performance.

In order to improve overall replication performance, the following is recommended:

i. A separate local drive for each AhsayOBS user home

ii. Distributing user accounts across multiple user homes to balance the I/O load

iii. A separate local drive for AhsayOBS system home

iv. A separate local drive for each AhsayRPS receiver

Both AhsayOBS and AhsayRPS servers should be running on separate dedicated machines.

3.5 AhsayRPS Java Heap Size Setting

Due to the additional AhsayRPS features such as retention policy and CRC checking. AhsayRPS may require more memory.

i. For a single receiver AhsayRPS server, a maximum Java heap size setting of at least 1024M is recommended.
ii. For a multiple receiver AhsayRPS server, a maximum Java heap size setting of at least 2048M is recommended.

When setting the maximum Java heap size for AhsayRPS please ensure this value does not exceed 50% of the RAM on the server, to allow sufficient memory for O/S processes and operations.

It is not recommended to set excessively high values for the maximum Java heap size, as this could result in AhsayRPS performance issues during internal Java VM garbage collection or memory recycling routines.

3.6 AhsayRPS and Multiple Receivers

If your AhsayRPS server is used by more than one AhsayOBS server, it is recommended that each receiver is located on it own individual disk. The advantages of this type of setup, is it will minimize the I/O on each disk and therefore improve replication performance.

Also, if one of the AhsayOBS servers suffers an outage, there is the option of swapping the disk to the affected AhsayOBS server.

3.7 Enable AhsayRPS CRC Checking

It is strongly recommended that you enable CRC checking for each receiver to ensure the integrity of the files on each AhsayRPS receiver.

3.8 Avoid Using Dynamic IP Addresses

The use of AhsayRPS domain names with dynamic IP addresses may result in the replication process restarting itself into UNYSNC mode whenever the IP address re-cycles.

It is strongly recommended to use a static IP address for the connection for both your AhsayOBS and AhsayRPS servers to ensure a stable and reliable replication service.

3.9 Using Different Ports for Different Receivers

If there are multiple receivers configured on your AhsayRPS Server, you must assign different ports for each receiver.

3.10 Firewall Settings

After you have finished setting up your replication server, please ensure you have updated your firewall settings to allow network traffic through the following ports:

- Port 80 - HTTP port for AhsayOBS and AhsayRPS web interface
- Port 443 – HTTPS for AhsayOBS and AhsayRPS web interface
- Any port(s) used by the AhsayRPS receiver(s), e.g. 9444, 9445

3.11 Third Party Monitoring Software

Avoid using monitoring software that checks for network traffic on the replication ports as some tools, e.g. Nagios have been known to affect the replication connection between AhsayOBS and AhsayRPS. The type of monitoring can cause the replication process to continually restart itself into UNSYNC mode, in some cases it may prevent AhsayOBS from connecting to AhsayRPS.

If you wish to use monitoring tools, make sure they are configured to scan the replication logs instead.

3.12 Do Not Operate AhsayOBS and AhsayRPS on a Single Machine

Although both AhsayRPS and AhsayOBS have been merged into one installer, both AhsayOBS and AhsayRPS services are activated post installation.

It is not recommended to configure and use both services on one machine, as they will compete for system resources, i.e. CPU and memory. This could affect the performance and stability of your backup service.

If both services are running on one machine, it will completely defeat the purpose of AhsayRPS as a backup or standby server to your AhsayOBS.

3.13 Performing an AhsayOBS Seed Load

In order to speed up the replication process and achieve LOGGING mode as quick as possible. It may be worth considering performing an initial AhsayOBS seed load to your AhsayRPS server.

3.14 AhsayRPS Dedicated Restore Drive

In order to facilitate a fast restore of snapshots from AhsayRPS retention area, it is recommended the files are not restored to an existing receiver home drive to avoid affecting replication performance. Your AhsayRPS server should be configured with a dedicated disk for restore purposes. Alternatively, an external USB drive can also be used.

3.15 AhsayOBS and Dual WAN Routers

For AhsayOBS servers which are connected to dual WAN routers for network load balancing. Please ensure that a static route is defined for network traffic via a single connection. As any switching between the two network connections will cause connection problems between AhsayOBS and AhsayRPS due to the change in IP address. This will result in the replication process restarting itself.

3.16 Replication Using Cross Over Cable

It is not recommended to setup AhsayOBS and AhsayRPS using a cross over cable for replication. As from our experience this setup will result in connection and performance issues.

If AhsayOBS and AhsayRPS servers are located on the same site they should be connected via a switch.

4 Quick Start

This chapter describes the minimum steps required to start using AhsayRPS. Please consult the information in the following chapters for a complete reference to all features available in AhsayRPS.

4.1 Getting started

To setup your AhsayRPS, please do the following:

Setup Replication Server

1. Point your browser to http://<your-replication-server-ip>/.
2. Switch to Replication Server Administration Interface.
3. Logon as administrator.

   The default login name and password are "system" and "system" respectively.
4. Set your hostname.
5. Set your SMTP Server.
6. Press the [Update] button.

Note: The SMTP server is required by AhsayRPS, so it can send alert emails to the system administrator when there are license issues.

Add Receiver

You need to add receiver to the system before you can start replication data to AhsayRPS. To add a receiver to the system, please do the followings:

1. Click the [Manage Receiver] link available at the top menu and choose [Add Receiver].

2. Enter the receive information for the new receiver account into the form provided.

Key	Description
Login Name	Login name of the AhsayRPS receiver.
Password	Password for the AhsayRPS receiver.
Alias	Alias for the AhsayRPS receiver.
Home Directory	Directory where the AhsayRPS receiver uses to store the data replicated by AhsayOBS.
Bind to IP address	IP address where an AhsayRPS receiver will wait for requests from the AhsayOBS. By default 0.0.0.0
Port	TCP port where this AhsayRPS receiver will wait for requests from the AhsayOBS.
Restore Point Interval	Minimum number of days between each retention snapshot. A retention snapshot will be created when data is received and time interval between current time and previous snapshot is over the specified period. No retention snapshot will be created if data is not received even when time interval is over.
Retention Customization Policy	Retention snapshots over the specified days will be removed by retention policy routine job runs everyday at 0:00 a.m.

3. The receiver is now ready.

Start Replication

1. Point your browser to http://<your-backup-server-ip>/.

2. Logon as administrator.

3. Go to [Manage System] -> [Replication Config].

4. Fill in the receiver information on the form.

5. Checked the [Enable Replication] checkbox and click the [Update] button to start the replication.

5 Installation

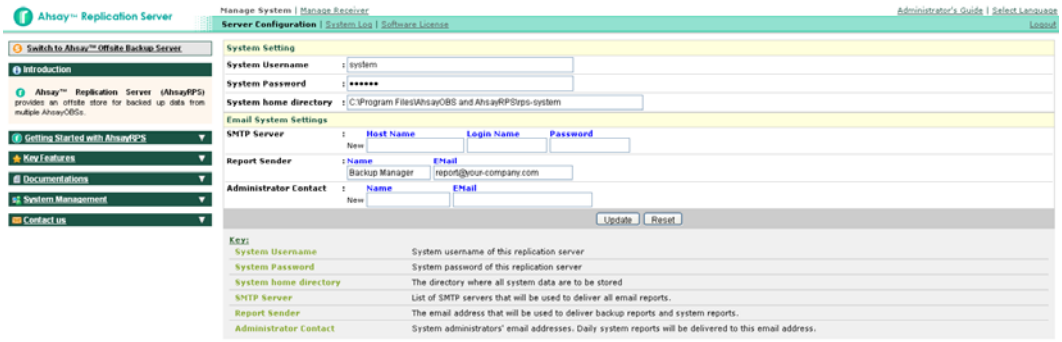
For instructions on how to install AhsayRPS on your computer, please refer to AhsayOBS & AhsayRPS Setup Guide.

6 Manage AhsayRPS System

This chapter describes how to use the [AhsayRPS Administration Console] -> [Manage System] menu to configure AhsayRPS.

6.1 Server Configuration

The [AhsayRPS Administration Console] -> [Manage System] -> [Server Configuration] page allows you to setup the system settings of an AhsayRPS.

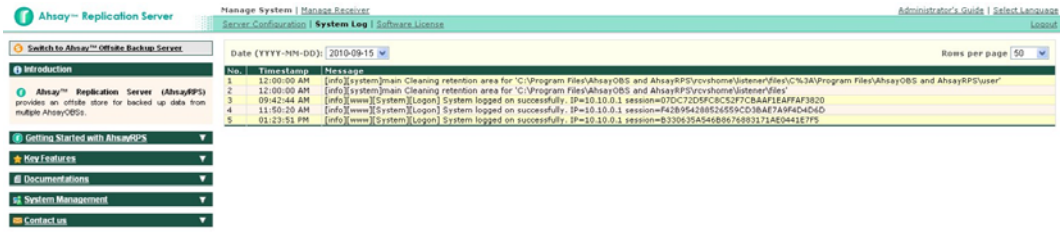


This section describes all settings under the [Server Configuration] menu.

Key	Description
System Username	Username for AhsayRPS Administration Console.
System Password	Password for AhsayRPS Administration Console.
System Home Directory	Location where all AhsayRPS system log and transaction log files are stored.
SMTP Server	SMTP server for sending AhsayRPS emails.
Report Sender	Email address for sending AhsayRPS emails.
Administrator Contact	Email address for AhsayRPS emails.

6.2 System Log

The [AhsayRPS Administration Console] -> [Manage System] -> [System Log] page shows you the running status of an AhsayRPS.



This section describes all settings under the [System Log] menu.

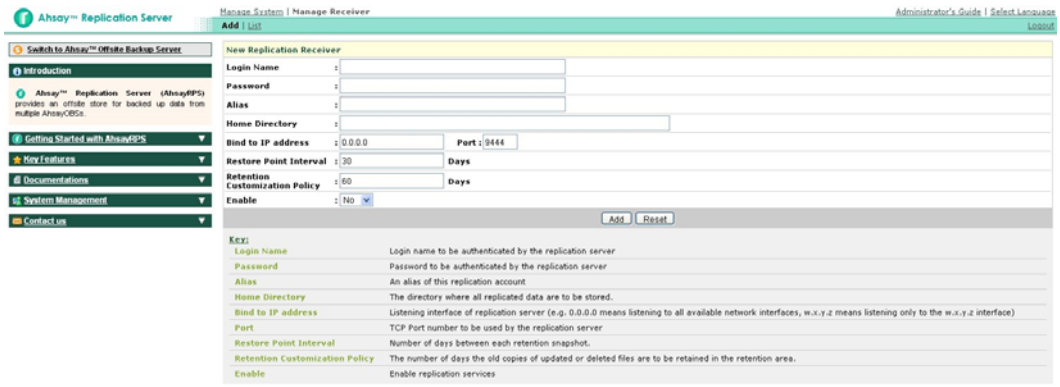
Key	Description
Date	The date when system log entries are recorded.
Rows per page	Maximum number of rows showing in a page.

7 Manage Receiver on AhsayRPS

This chapter describes how to use the [AhsayRPS Administration Console] -> [Manage Receiver] menu to configure receivers for AhsayRPS.

7.1 Create Receivers

To setup replication between AhsayOBS and AhsayRPS, the first step is to add a receiver to AhsayRPS using the [AhsayRPS Administration Console] -> [Manage Receiver] -> [Add] page. To create a new AhsayRPS receiver, simply fill in the form below and press the [Add] button.



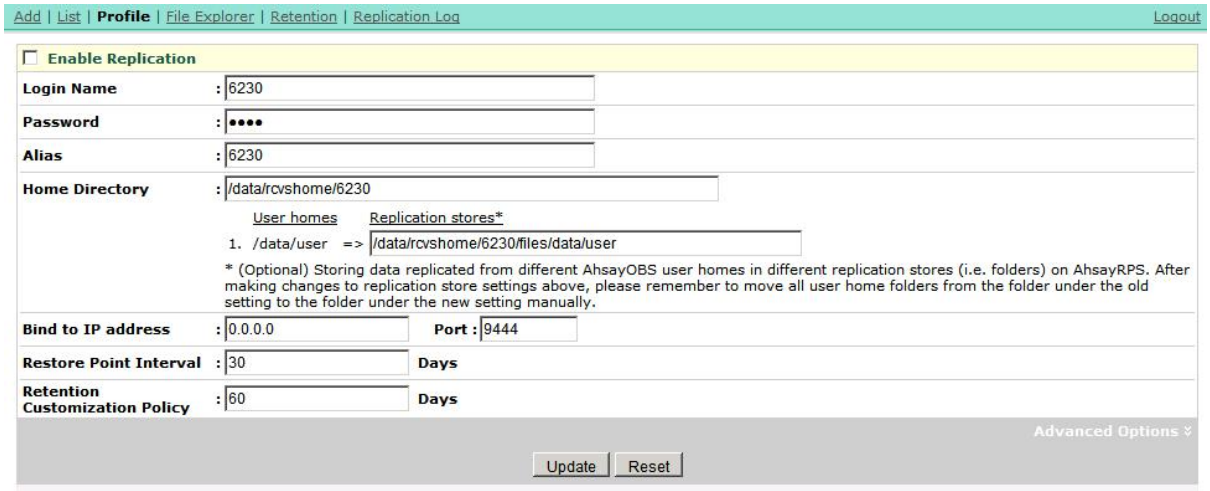
Key	Description
Login Name	Login name of an AhsayRPS receiver to create. E.g. Receiver1
Password	Password of an AhsayRPS receiver to create.
Alias	Alias of an AhsayRPS receiver to create. E.g. Receiver1
Home Directory	Directory where an AhsayRPS receiver will use to store all its data.
Bind to IP address	IP address where an AhsayRPS receiver will wait for requests from the AhsayOBS. The default value is 0.0.0.0.
Port	TCP port where this AhsayRPS receiver will wait for requests from the AhsayOBS. The default value is 9444.
Restore Point Interval	Minimum number of days between each retention snapshot. A retention snapshot will be created when data is received and time interval between current time and previous snapshot is over the specified period. No retention snapshot will be created if data is not received even when time interval is over. The default value is 30

	days.
Retention Customization Policy	Retention snapshots over the specified days will be removed by retention policy routine job runs everyday at 0:00 a.m. The default value is 60 days.
Enable	Enable replication service.

7.2 Retention Feature

7.2.1 Retention Settings

AhsayRPS will create a snapshot according to the settings in the AhsayRPS web console [Manage System] -> [Manage Receiver] -> [%RECEIVER_NAME%] page.



- Restore Point Interval – defines the number of days between each retention snapshot. The default value is 30 days and the minimum value is 1 day.
- Retention Customization Policy – defines the number of days before an existing retention snapshot is removed from the AhsayRPS receiver. The default value is 60 days and the minimum value is 0 days

When the replication starts, it will check if there is a retention snapshot available.

- If no retention snapshot is found, a new snapshot is created using the current time stamp. The files will be stored in both the snapshot folder and the current folder.
- If a retention snapshot already exists, it will check if it is still within the "Restore Point Interval". It will create a new snapshot if it is not.

Only the first version of a file uploaded to AhsayRPS is stored in a related snapshot located in the retention area

WARNING: Please make sure you have sufficient storage capacity to accommodate your retention policy. As setting the Restore Point Interval to a low value and or the Retention Customization Policy to a high value, could result in the disk where the receiver is located running out of space very quickly. This could cause the existing data on the receiver(s) to corrupt.

7.2.2 Retention Policy Considerations

In deciding on an appropriate AhsayRPS retention policy setting, you will need to weight the advantages of using smaller restore point intervals which allows for a greater chances of recovery and or the "Retention Customization Policy" setting is configured for a large number of days against your AhsayRPS server storage limitations.

Example:

Restore Point Interval: 10 Days
Retention Customization Policy: 60 Days

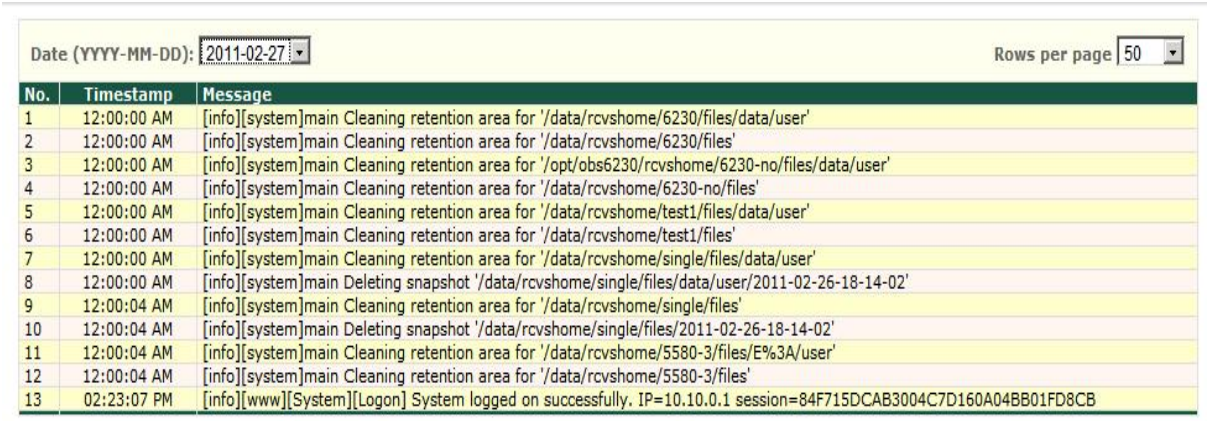
Assuming that every 10 days there is a 100GB change on your AhsayRPS receiver. After 60 days there will be six restore point intervals created (6 x 100 GB) totaling 600GB. Therefore, in order to implement this retention policy your AhsayRPS will require at least an additional 600GB of space.

This extra disk space does not take into account the normal data growth as a result of business expansion or change in client backup behaviour.

7.2.3 Retention Policy Job

In order to manage the retention snapshots on AhsayRPS, a retention policy system job runs at 12:00 AM daily to check if there are any retention snapshots which have exceeded the "Retention Customization Policy" for each receiver. If any snapshot has exceeded this setting it will be immediately deleted. All information regarding these operations is recorded in the AhsayRPS system log.

The following is an example of entries that you are likely to find on [Manage System] -> [System Log] page.



Date (YYYY-MM-DD): 2011-02-27 Rows per page 50

No.	Timestamp	Message
1	12:00:00 AM	[info][system]main Cleaning retention area for '/data/rcvshome/6230/files/data/user'
2	12:00:00 AM	[info][system]main Cleaning retention area for '/data/rcvshome/6230/files'
3	12:00:00 AM	[info][system]main Cleaning retention area for '/opt/obs6230/rcvshome/6230-no/files/data/user'
4	12:00:00 AM	[info][system]main Cleaning retention area for '/data/rcvshome/6230-no/files'
5	12:00:00 AM	[info][system]main Cleaning retention area for '/data/rcvshome/test1/files/data/user'
6	12:00:00 AM	[info][system]main Cleaning retention area for '/data/rcvshome/test1/files'
7	12:00:00 AM	[info][system]main Cleaning retention area for '/data/rcvshome/single/files/data/user'
8	12:00:00 AM	[info][system]main Deleting snapshot '/data/rcvshome/single/files/data/user/2011-02-26-18-14-02'
9	12:00:04 AM	[info][system]main Cleaning retention area for '/data/rcvshome/single/files'
10	12:00:04 AM	[info][system]main Deleting snapshot '/data/rcvshome/single/files/2011-02-26-18-14-02'
11	12:00:04 AM	[info][system]main Cleaning retention area for '/data/rcvshome/5580-3/files/E%3A/user'
12	12:00:04 AM	[info][system]main Cleaning retention area for '/data/rcvshome/5580-3/files'
13	02:23:07 PM	[info][www][System][Logon] System logged on successfully. IP=10.10.0.1 session=84F715DCAB3004C7D160A04BB01FD8CB

For AhsayRPS servers configured with multiple receivers, the retention policy job will run in the order they are listed in the %RPS_HOME%/conf/ rpsRecv.xml file.

7.2.4 Disabling AhsayRPS Retention

AhsayRPS retention is enabled by default, it is not possible to totally disable this feature. You can effectively "disable" it by configuring the receiver(s) with the following policy settings:

i. Restore Point Interval: 9999 Days
ii. Retention Customization Policy: 0 Days

Even with this workaround AhsayRPS will still create an initial snapshot, there maybe some data saved in this snapshot.

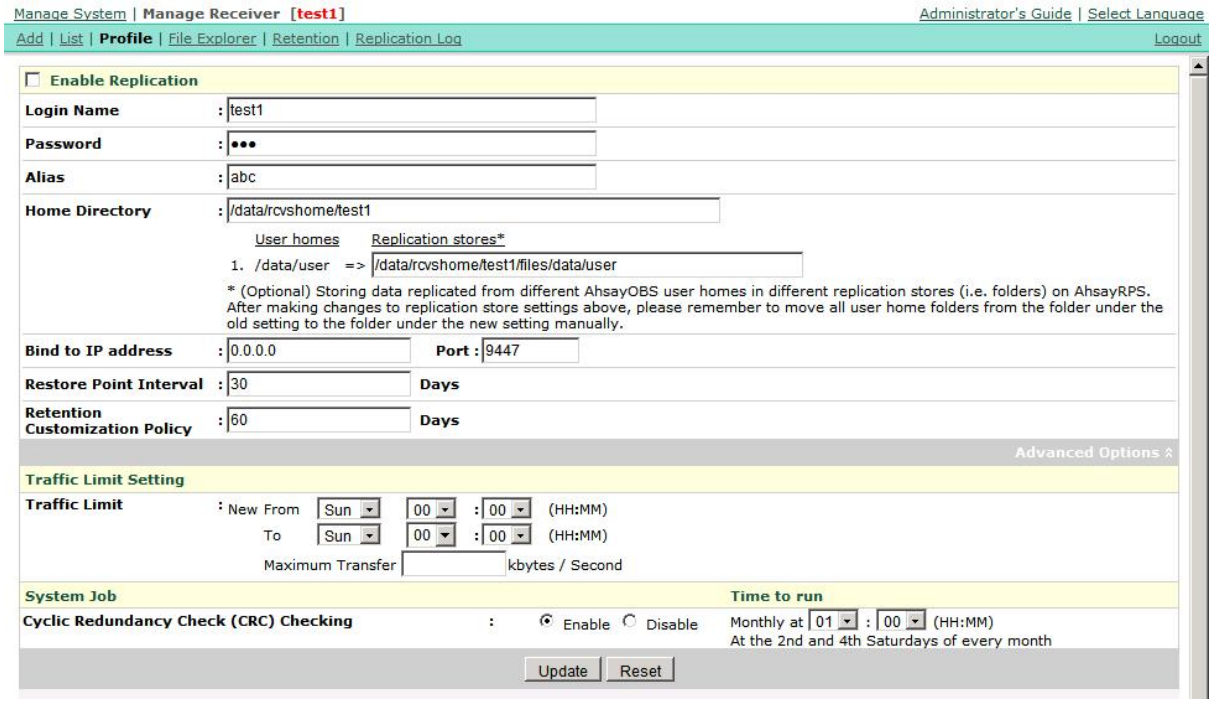
Another method is to limit the amount of disk space used by the AhsayRPS retention feature is to configure the receiver(s) with the following policy settings:

i. Restore Point Interval: 1 Days
ii. Retention Customization Policy: 1 Days

Note: The retention feature will work with AhsayOBS v5.5.3.0 or above.

7.3 CRC Redundancy Check (CRC) Checking

After an AhsayRPS receiver is created, clicking on the "Advanced Options" will show extra configuration settings for the receiver, the "Traffic Limit" settings and Cyclic Redundancy Check (CRC) job.



Traffic Limit	Define the maximum network bandwidth usage of a replication amount. By default, it is not set.
Cyclic Redundancy Check (CRC) Checking	Monthly job performing CRC of checking of backup files for each user. By default it is disabled.
Update	Update the configurations of a receiver.
Reset	Reset all values to its original values.

File Checking Criteria

The "Cyclic Redundancy Check (CRC) Checking" job will check all new files replicated to the AhsayRPS receiver since the last CRC job. When the AhsayRPS CRC job checks a file it will update the file header with a *'RPS CRC next check date'*. This is calculated as 180 + (random number of 0 to 60) days, so for existing files which have been checked previously. The next CRC check will be performed after 180 to 240 days.

Note: It is recommended that you enable the CRC checking for each receiver so that regular file integrity checks can be made.

Configuration

By default CRC checking is disabled. To Enable the CRC Check you need to go [Mange System] -> [Manage Receiver] -> [%Receiver%] -> [Advanced Options] and select "Enable" for "Cyclic Redundancy Check (CRC) Checking".

In order for the Cyclic Redundancy Check (CRC) Checking job to run properly both:

i. The "Cyclic Redundancy Check (CRC) Checking" must be set "Enable".
ii. The receiver must be enabled.

The CRC job checks the files on the receiver even if there is no replication traffic or if there is no AhsayOBS server connected to the receiver.

You can enable or disable the CRC check and or change the start time for each receiver without stopping the replication process. All you need to do is to make your changes to the receiver, then in [Mange System] -> [Manage Receiver] -> [%Receiver%] -> [Advanced Options] press the [Update] button to confirm. The new settings will be effective immediately.

CRC Job Scheduling and Multiple Receivers

As the CRC check is a single thread background job, it will only run on one receiver at a time.

Example 1: AhsayRPS server has three receivers enabled and configured for CRC check as follows:

i. RecX start time 09:00
ii RecY start time at 15:00
ii RecZ start time at 20:00

Then RecX will run first as it is configured to start at the earliest time. As the CRC process is a single thread process. RecY will start only after RecX has finished running. RecZ will start after RecY has finished running.

In effect for multiple receivers the start time of the following receiver is dependent on the end time of the previous receiver**.**

Example 2: AhsayRPS server has multiple receivers enabled and configured to start at 13:00.

If all receiver's are configured to start at the same time, i.e. 13:00 the CRC check will be run according to the receiver ordering as defined in the %RPS_HOME%/conf/rpsRecv.xml file.

CRC Checking

When the CRC job runs the start and end times, as well as the folders and files which have been checked, will be recorded in the AhsayRPS system and RPS_CONTEXT logs. There may be some further logs entries in the catalina.out log.

The following is an example of entries that you are likely to find on [Manage System] -> [System Log] page during the CRC check.

1	12:58:02 PM	[info][www][System][Logon] System logged on successfully. IP=10.10.0.1 session=A5EC6A011977B2823EBCB26C013ECCFA
2	01:01:54 PM	[info][www][System][Logon] System logged on successfully. IP=10.10.0.1 session=AE05F850947139D0910BA4C348F2D963
3	01:05:00 PM	[info][system]Start checking CRC of replicated files in '/data/rcvshome/single/files/data/user'
4	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0x75/0x5d /0x30/0x25'
5	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0x0b/0xcf /0xea/0x28'
6	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0x17/0x9c /0x8d/0xf9'
7	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0x34/0x0c /0x98/0x30'
8	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0xf2/0x0f /0x30/0x8a'
9	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0xfa/0x68 /0x60/0x91'
10	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0x4d/0xf3 /0xce/0xdd'
11	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0x11/0xa4 /0x4a/0x60'
12	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0xbd/0x63 /0x94/0x92'
13	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0xca/0xe9 /0x29/0x2d'
14	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0xec/0x14 /0xd1/0x73'
15	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0xaf/0xb0 /0xf5/0xfd'
16	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0xa9/0x34 /0xe7/0x40'
17	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0xb4/0xb2 /0xdf/0xee'
18	01:05:00 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/single/files/data/user/uota/files/1297152425000/Current/0x0e/0x44 /0xaa/0xf2'

Corrupted File Handling

When the CRC job encounters an invalid or corrupted file, the file will be immediately deleted from AhsayRPS, this action will be recorded in the RPS system and RPS_CONTEXT logs. There may be some further logs entries in the catalina.out log.

The following is an example of entries that you are likely to find on [Manage System] -> [System Log] page during the CRC check, when handling corrupted files.

25	01:06:02 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0xaa/0x72/0xa4/0xe2'
26	01:06:02 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x86/0x9e/0x4e/0xb4'
27	01:06:02 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x34/0x0c/0x98/0x30'
28	01:06:02 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x34/0x95/0xe6/0xfb'
29	01:06:02 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0xf2/0x14/0xd5/0x66'
30	01:06:02 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0xf2/0x0f/0x30/0x8a'
31	01:06:02 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0xa2/0x38/0x86/0x4e'
32	01:06:02 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0xa2/0x76/0x4f/0xe1'
33	01:06:02 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0xa2/0x54/0x7d/0xf9'
34	01:06:02 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x03/0x54/0x95/0x85'
35	01:06:02 PM	[info][system][Thread][Job][CRC_Check] Header corrupted. '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x03/0x54/0x95/0x85/2259281893' is deleted.
36	01:06:02 PM	[info][system][Thread][Job][CRC_Check] Header corrupted. '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x03/0x54/0x95/0x85/4149580587' is deleted.
37	01:06:02 PM	[info][system][Thread][Job][CRC_Check] Header corrupted. '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x03/0x54/0x95/0x85/3413822869' is deleted.
38	01:06:02 PM	[info][system][Thread][Job][CRC_Check] Header corrupted. '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x03/0x54/0x95/0x85/1439651456' is deleted.
39	01:06:02 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0xeb/0x91/0xff/0xec'
40	01:06:03 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x52/0xb8/0x21/0xe2'
41	01:06:03 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0xb3/0x50/0x20/0xae'
42	01:06:03 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0xfa/0x68/0x60/0x91'
43	01:06:03 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0xcc/0xf0/0x21/0x69'
44	01:06:03 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0xcc/0x3d/0x3c/0x66'
45	01:06:03 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x4d/0xf3/0xce/0xdd'
46	01:06:03 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x11/0xa4/0x4a/0x60'
47	01:06:03 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x11/0xf0/0x49/0x21'
48	01:06:03 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x0d/0x0b/0x37/0x0f'
49	01:06:03 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0x0d/0x23/0xc7/0xfd'
50	01:06:03 PM	[info][system]Checking CRC of replicated files in '/data/rcvshome/6230/files/data/user/uota/files/1297150596968/Current/0xa4/0x63/0x8f/0x43'

The deleted file(s) will be updated from AhsayOBS either during:

i. The next monthly RESYNC on the 1st Saturday of each month at 13:00
ii. If replication is in UNSYNC mode, then the files will be updated from AhsayOBS when in SYNC mode.
iii. When replication is restarted.

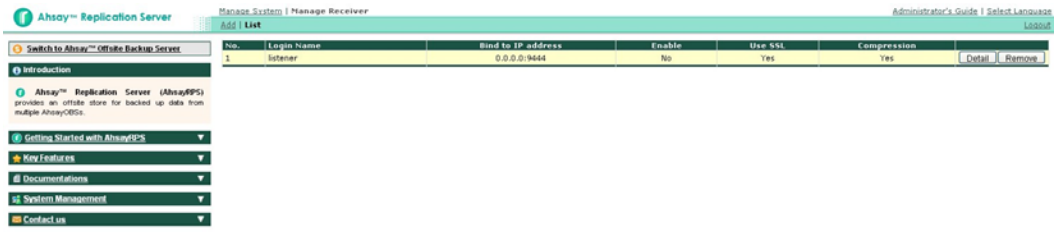
Note:

i. There will not be any updates during LOGGING mode.

ii. If the file on AhsayOBS is corrupted then during the next SYNC, RESYNC it will be replicated back to AhsayRPS.

7.4 List all Receivers

The [AhsayRPS Administration Console] -> [Manage Receiver] -> [List] page lists all receivers configured on AhsayRPS.



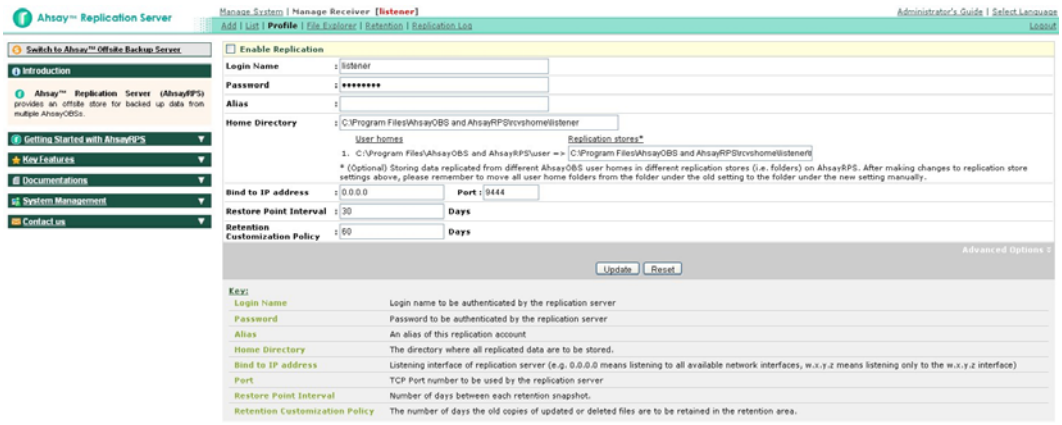
This section describes all settings under the [List] menu.

Key	Description
Login Name	Login name of an AhsayRPS receiver.
Bind to IP address	IP address and TCP port number of an AhsayRPS receiver.
Enable	Enable/Disable AhsayRPS receiver.
Use SSL*	Whether to use SSL on an AhsayRPS receiver.
Compression*	Whether to use compression on an AhsayRPS receiver.
Detail	Show the details of an AhsayRPS receiver.
Remove	Remove an AhsayRPS receiver.

* To ensure optimal replication performance and security. Both Compression & SSL settings are enabled by default and are mandatory as of AhsayRPS v5.5.3.0 or above.

7.5 Edit Receiver's Profile

The [AhsayRPS Administration Console] -> [Manager Receiver] -> [Profile] page shows the details of an AhsayRPS receiver.



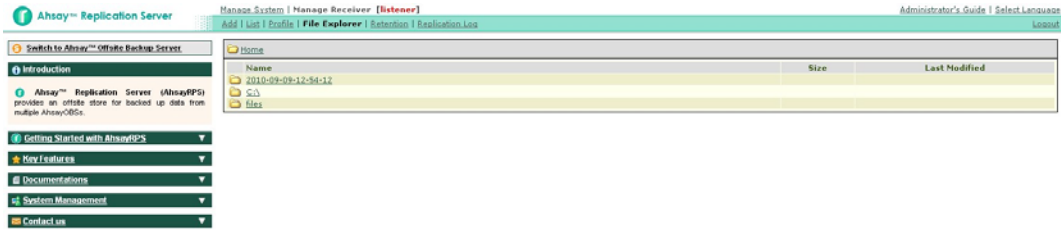
This section describes all settings under the [Profile] menu.

Key	Description
Enable Replication	Whether to enable/disable a receiver.
Login Name	Login name of a receiver.
Password	Password of a receiver.
Alias	Alias of a receiver.
Home Directory	Directory where all replicated data will be stored by a receiver.
Replication stores	Directory for storing data from the OBS user home.
Bind to IP address	IP address of a receiver.
Port	TCP port number of a receiver.
Restore Point Interval	Minimum number of days between each retention snapshot. A retention snapshot will be created when data is received and time interval between current time and previous snapshot is over the specified period. No retention snapshot will be created if data is not received even when time interval is over.
Retention Customization Policy	Retention snapshots over the specified days will be removed by retention policy routine job runs everyday at 0:00 a.m.
Traffic Limit	Define the maximum network bandwidth usage of a

	replication amount. By default, it is not set.
Cyclic Redundancy Check (CRC) Checking	Monthly job performing CRC of checking of backup files for each user. By default. It is disabled.
Update	Update the configurations of a receiver.
Reset	Reset all values to its original values.

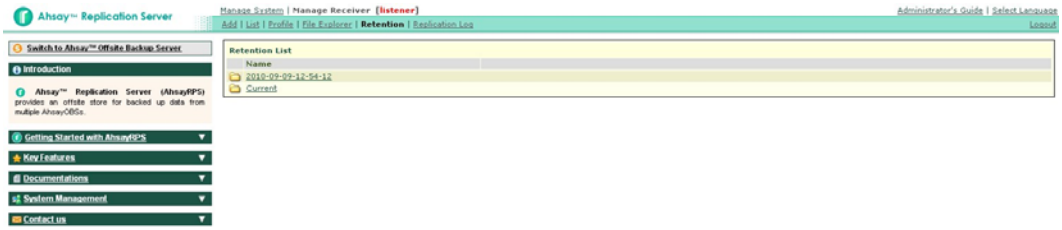
7.6 File Explorer

The [AhsayRPS Administration Console] -> [Manage Receiver] -> [File Explorer] page shows replication files at different retention snapshots of a select RPS receiver. It is currently not possible to restore replicated files from this page. As a workaround, you can restore replicated files from AhsayRPS using the [Decrypt] tools available in AhsayOBM.



7.7 Retention Recovery

The [AhsayRPS Administration Console] -> [Manage Receiver] -> [Retention] page lists all replication snapshots recorded by the receiver at an interval defined at receiver profile. Click [yyyy-MM-dd-HH-mm-ss] snapshot link to recover replicated files up to the time specified.

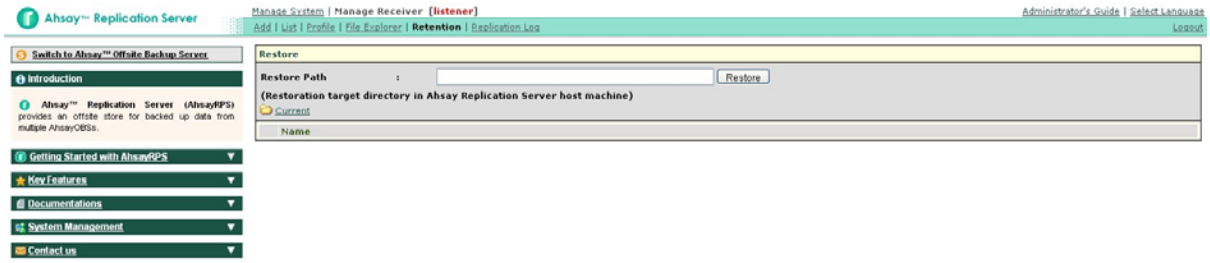


Key	Description
Retention List	Listing of replication snapshots that can be recovered. Current snapshot contains the latest files received by this receiver.

Replication Snapshot Recovery

This feature will restore the snapshot of selected user account files from the receiver home path to another location on the AhsayRPS server.

To restore a snapshot enter the destination restore path on AhsayRPS host machine and click [Restore] button to begin snapshot recovery. It will restore replicated files up to the time specified on snapshot. Limit the recovery by selecting users from the name list and click [Restore] button. If you click the [Current] link in the [AhsayRPS Administration Console] -> [Manage Receiver] -> [Retention] or [yyyy-MM-dd-HH-mm-ss] link, it will return to the [Retention] page.



Key	Description
Restore Path	Any location on Ahsay Replication Server host machine with enough disk space for replicated file recovery.
Name	Name of users to be recovered. Check the [Name] checkbox to select user for recovery.

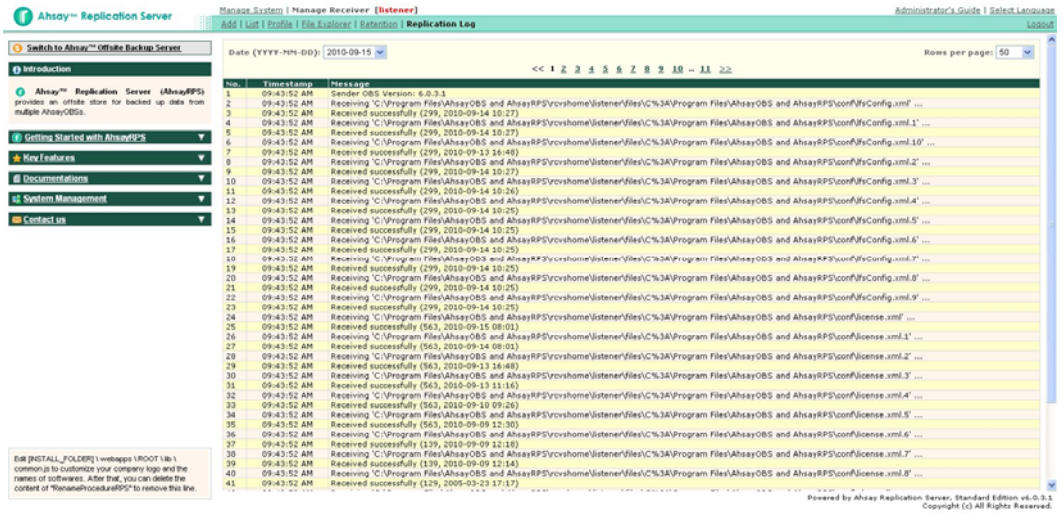
Recovery Process

The recovery process begins after clicking the [Restore] button. During the recovery process, AhsayRPS will restore both the AhsayOBS system files and selected user files. By default system files will be recovered first, followed by the file of users. The recovery files and status will be shown during recovery process. Recovery can be terminated at any time. Click [Stop] button to terminate and remove all recovered files from the restore path.

Note: If you specify a non-existent or incorrect path as the restore path AhsayRPS will restore the snapshot to the %AhsayRPS_HOME% path. This could result in server instability or even a server crash if the size of the snapshot exceeds the free disk space on the %AhsayRPS_HOME% partition or drive.

7.8 Replication Log

The [AhsayRPS Administration Console] -> [Manage Receiver] -> [Replication Log] page lists all logs recorded by this receiver.



Key	Description
Date	The date when log entries are recorded.
Rows per page	Maximum number of rows showing on a page.

8 Replication Configuration on AhsayOBS

This chapter describes how to use [Manage System] -> [Replication Config] page to manage the AhsayOBS replication module which allows you to perform real-time replication of all backup data and application or binary files from AhsayOBS to AhsayRPS.

Note: Please logon to the AhsayOBS web interface before proceeding to the next step.

8.1 Mandatory Replication Setting

To setup replication on AhsayOBS, please browse to [Manage System] -> [Replication Config] page on the web interface and do the followings:

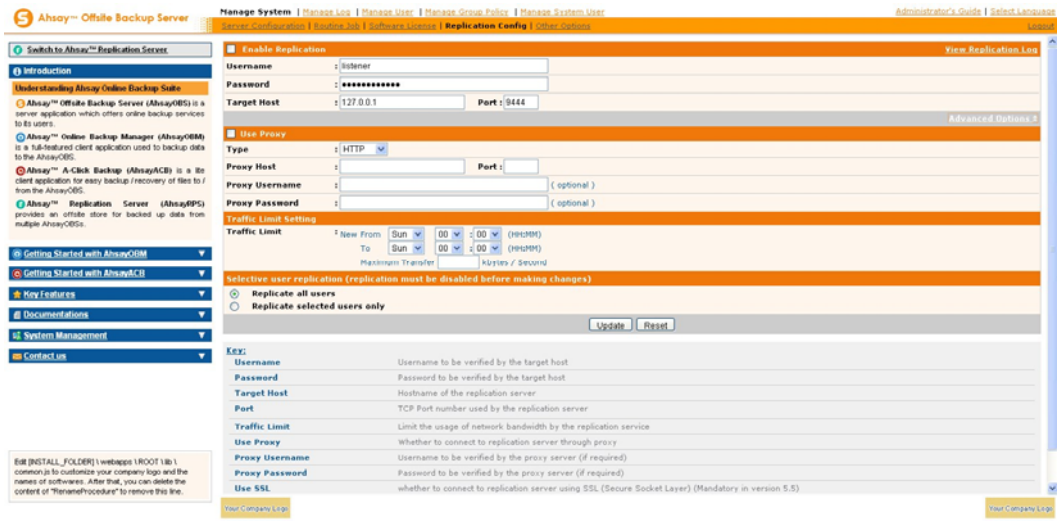
1. Make sure that you have setup and started a receiver for this AhsayOBS on the replication server.

2. Enter the [Username], [Password], [Target Host] and [Port] textbox on the configuration page.

3. Check the [Enable Replication] checkbox.

4. Press the [Update] button at the button of the page.

5. The setup is now completed. You can now use the [View Replication Log] link to review the replication logs.



Key	Description
Username	Username of the replication receiver on the replication server.
Password	Password of the replication receiver on the replication server.
Target Host	Host name (or IP address) of the replication server.
Port	TCP port number used by the replication server for this receiver.

The [View Replication Log] link will bring you to the Replication Log page. The [Advanced Options] link will open up some other optional configuration parameters on the page. The descriptions of these parameters are described in the following sections.

8.2 Use Proxy

You can use the [Use Proxy] section under the [Manage System] -> [Replication Config] page to configure whether you want to use proxy for replication traffic between AhsayOBS and AhsayRPS. There are a few configurable parameters available and they are described in the following table.

Proxy setting is an optional setting.

Key	Description
Use Proxy	Whether to use Proxy for replication traffic.
Type	Proxy Type, e.g. HTTP or SOCKS.
Proxy Host	Hostname or IP address of the proxy server.
Proxy Port	TCP port number of the proxy server.
Proxy Username (optional)	Username for the proxy server (if proxy authentication is required).
Proxy Password (optional)	Password for the proxy server (if proxy authentication is required).

Note: When implementing replication via a proxy server, please ensure your proxy server is capable of handling the replication traffic flow. Otherwise this could result in replication performance issues or network connection stability problems.

8.3 Traffic Limit

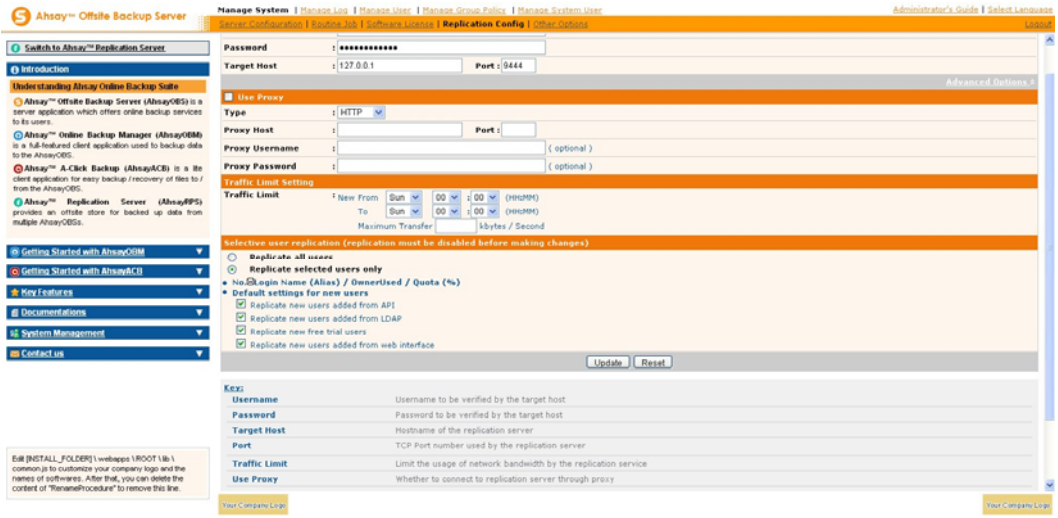
You can use the [Traffic Limit] section under the [Manage System] -> [Replication Config] page to limit the amount of bandwidth used by replication traffic between specified times. There are a few configurable parameters available and they are described in the following table. Traffic Limit is an optional setting.

You can set an all-time traffic limit by setting both [From] and [To] parameters to [Sun, 00:00].

Key	Description
Traffic Limit	Bandwidth Throttling for replication traffic.
From	Start time of enforced traffic limit period.
To	End time of enforced traffic limit period.
Maximum Transfer	Maximum bandwidth used between the [From] and [To] period.

8.4 Selective User Replication

You can use the [Selective user replication] section under [Manage System] -> [Replication Config] page to select specific users for replication.



The definitions of keywords related to the settings in this section are shown in the table below:

Key	Description
Replicate all users	Replicate all the users in the user home without selection.
Replicate selected user only	Replicate users selected only.
No.	The count of user.
Login Name (Alias/Owner)	The login name of the user, with Alias of the user bracketed behind, and the creator of the user.
Used / Quota (%)	The size of data stored on the server by the user and defined quota of size of the user. The percentage of used size over quota is also included at the end.
Replicate new users added from API	For any new user created by the Ahsay API, the user account will be replicated.
Replicate new users added from LDAP	For any new user created by Windows Active Directory and added to AhsayOBS, the user account will be replicated.
Replicate new free trial users	For any new trial users created, the user account will be replicated.
Replicate new users	For any new trails users created by AhsayOBS web-

added from web interface	console, the user account will be replicated.

To enable this function, simply select the [Replicate selected users only] under the section of [Selective user replication], and check the boxes next to the users which are going to be replicated..

Once the specific users have been selected and replication is enabled. If you wish specify additional existing users to the list or make change to the user list, you will have to disable or stop the replication process to make your re-selection.

Selective user replication also provides options for configuring the default replication settings for newly created users:

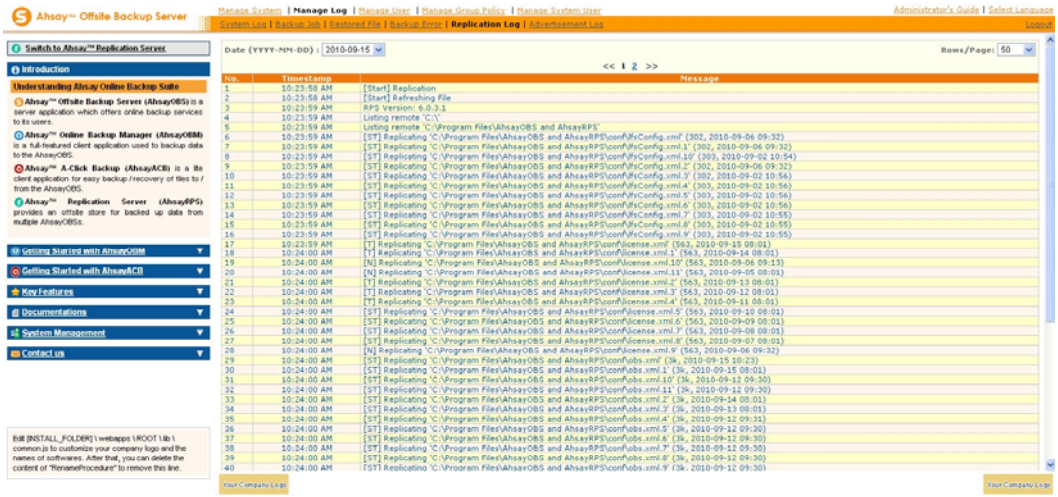
i. Replicate new users added from API
ii. Replicate new users added from LDAP
iii. Replicate new free trial users
iv. Replicate new users added from web interface

The default replication settings for new users can be changed without disabling or stopping the replication process.

Note: If selective replication is enabled but the previous replication mode was "replicate all users". Any user accounts which were previously replicated to AhsayRPS but have not been currently selected will be removed from the AhsayRPS current data area. Recovery of the data is dependent on your AhsayRPS retention settings.

8.5 Replication Log

You can review the logs by visiting the [Manage Log] -> [Replication Log] page.



8.6 Enable/Disable Replication Service

You can restart the replication process completely from the beginning by doing the following:

1. On AhsayRPS, uncheck the [Manage Receiver] -> [Profile] -> [Enable Replication] checkbox and press the [Update] button.

2. On AhsayOBS, uncheck the [Manage System] -> [Replication Config] -> [Enable Replication] checkbox and press the [Update] button.

3. On AhsayRPS, check the [Manage Receiver] -> [Profile] -> [Enable Replication] checkbox and press the [Update] button.

4. On AhsayOBS, check the [Manage Receiver] -> [Replication Config] -> [Enable Replication] checkbox and press the [Update] button.

5. On AhsayOBS, visit the [Manage Log] -> [Replication Log] page to check if replication starts running.

9 Starting AhsayRPS as AhsayOBS

This chapter describes the information on how you can start up AhsayRPS as AhsayOBS.

Scenario

- You want to start AhsayOBS by using the replication data and using the same AhsayOBS & AhsayRPS service on the replication server side.
- *AhsayOBS & AhsayRPS is installed in C:\Program Files\AhsayOBS and AhsayRPS* on the backup server side.
- AhsayOBS & AhsayRPS is installed in C:*Program Files\AhsayOBS and AhsayRPS* on the replication server side.
- The RECEIVER_HOME of the receiver of AhsayOBS configured on AhsayRPS is *D:\RepHome*.
- The USER_HOMES of AhsayOBS are *E:\Users* and *F:\Users* on AhsayOBS.
- The SYSTEM_HOME of AhsayOBS is *E:\System* on AhsayOBS.
- The POLICY_HOME of AhsayOBS is *E:\Policy* on AhsayOBS.

To startup the replication server as a backup server, please follow the steps below:

1. Shutdown the AhsayOBS & AhsayRPS service on the replication server side.

2. Copy the CONF folder, i.e. copy the *D:\RepHome\files\C%3A\Program Files\AhsayOBS and AhsayRPS\conf* to *C:\Program Files\AhsayOBS and AhsayRPS\conf*, exclude rps.xml, rpsRecv.xml, rpsLicense.xml and server.xml.

3. Copy the WEBAPPS folder, i.e. copy *D:\RepHome\files\C%3A\Program Files\AhsayOBS and AhsayRPS\webapps\obs* to *C:\Program Files\AhsayOBS and AhsayRPS\webapps\obs*.

4. Copy the USER_HOMES, i.e. copy *D:\RepHome\files\E%3A\Users* to *E:\Users*, *D:\RepHome\files\F%3A\Users* to *F:\Users* and *D:\RepHome\files\E%3A\System* to *E:\System*.

   If the partitions for E:\ or F:\ are not available, you can copy these directories to any location you want. However, you must remember to open *C:\Program Files\AhsayOBS and AhsayRPS\conf\obs.xml* and modify the entries for "user-home" and "system-home" with the correct paths.

5. Copy the POLICY_HOME, i.e. copy *D:\RepHome\files\E%3A\Policy* to *E:\Policy*.

6. Startup AhsayOBS & AhsayRPS service on the replication server. This service is running both AhsayOBS service from the original backup server and the AhsayRPS service now.

7. Perform a system rebuild for the User Home data afterward.

   Select [Manage System] -> [Routine Job], and then [Rebuild User Storage], modify the [Time to run] setting to begin the rebuild as soon as possible.

Note: Please take a look at *%OBSR_HOME%\logs\obs*.log* and *%OBSR_HOME%\logs\cat*.log* if you run into any problem.

10 Advanced Configuration

10.1 Restricting access to system page by IP address

For better security, you can restrict access to the system administration console by IP addresses. To do so, please do the followings:

1. Open %OBSR_HOME%\webapps\rps\WEB-INF\web.xml.

2. Add the following SystemConsole filter under "filter" section

web.xml

```
….
  <filter>
    <filter-name>SystemConsole</filter-name>
    <filter-class>com.ahsay.ars.www.IPFilter</filter-class>
    <init-param>
      <param-name>Range1</param-name>
      <param-value>localhost</param-value>
    </init-param>
    <init-param>
      <param-name>Range2</param-name>
      <param-value>127.0.0.1-127.0.0.1</param-value>
    </init-param>
  </filter>
  <filter-mapping>
    <filter-name>SystemConsole</filter-name>
      <url-pattern>/system/*</url-pattern>
  </filter-mapping>
….
```

3. Change the "Range2" parameter value from "127.0.0.1-127.0.0.1" (shown in red and bold above) to a range of IP addresses from where access to the system administration console is allowed.

   For example, changing [Range2] value from "127.0.0.1-127.0.0.1" to "192.168.1.1-192.168.1.255" to allow the 192.168.1.x network to invoke the APIs.

web.xml (Updated)

```
….
  <filter>
    <filter-name>SystemConsole</filter-name>
    <filter-class>com.ahsay.ars.www.IPFilter</filter-class>
    <init-param>
      <param-name>Range1</param-name>
      <param-value>localhost</param-value>
    </init-param>
```

```
    <init-param>
      <param-name>Range2</param-name>
      <param-value>192.168.1.1-192.168.1.255</param-value>
    </init-param>
  </filter>
  <filter-mapping>
    <filter-name>SystemConsole</filter-name>
      <url-pattern>/system/*</url-pattern>
  </filter-mapping>

….
```

Please note that you can configure more than one IP range by adding additional init parameters (i.e. "Range3", "Range4" and so do) to the filter XML tag. For example:

```
  <filter>
    <filter-name>SystemConsole</filter-name>
    <filter-class>com.ahsay.obs.www.IPFilter</filter-class>
    <init-param>
      <param-name>Range1</param-name>
      <param-value>localhost</param-value>
    </init-param>
    <init-param>
      <param-name>Range2</param-name>
      <param-value>192.168.1.1-192.168.1.255</param-value>
    </init-param>
    <init-param>
      <param-name>Range3</param-name>
      <param-value>192.168.2.1-192.168.2.255</param-value>
    </init-param>
  </filter>
  <filter-mapping>
    <filter-name>SystemConsole</filter-name>
      <url-pattern>/system/*</url-pattern>
  </filter-mapping>
```

4. Restart AhsayOBSR.

11 Troubleshooting

If you are running into problems when making the replication process work as stated in previous sections.

11.1 Connections Errors

1237	05:25:41 AM	Sent 0 byte in 10 sec (0 byte/sec)
1238	05:25:41 AM	com.ahsay.obs.X: [RPSSender.refreshUnloggedFile][Exception] [SendHandler.connect][Unable to connnect] [IOException] Reason=Connection refused
1239	05:25:41 AM	com.ahsay.obs.ae.i(Unknown Source)
1240	05:25:41 AM	com.ahsay.obs.ae.a(Unknown Source)
1241	05:25:41 AM	com.ahsay.obs.ae.m(Unknown Source)
1242	05:25:41 AM	com.ahsay.afc.util.n.run(Unknown Source)
1243	05:25:41 AM	java.lang.Thread.run(Thread.java:619)
1244	05:25:41 AM	com.ahsay.obs.gw: [SendHandler.connect][Unable to connnect] [IOException] Reason=Connection refused
1245	05:25:41 AM	com.ahsay.obs.as.e(Unknown Source)
1246	05:25:41 AM	com.ahsay.obs.ah.c(Unknown Source)
1247	05:25:41 AM	com.ahsay.obs.ae.i(Unknown Source)
1248	05:25:41 AM	com.ahsay.obs.ae.a(Unknown Source)
1249	05:25:41 AM	com.ahsay.obs.ae.m(Unknown Source)
1250	05:25:41 AM	com.ahsay.afc.util.n.run(Unknown Source)
1251	05:25:41 AM	java.lang.Thread.run(Thread.java:619)
1252	05:26:41 AM	[Start] Refreshing File
1253	05:26:52 AM	[End] Refreshing File
1254	05:26:52 AM	Sent 0 byte in 10 sec (0 byte/sec)
1255	05:26:52 AM	com.ahsay.obs.X: [RPSSender.refreshUnloggedFile][Exception] [SendHandler.connect][Unable to connnect] [IOException] Reason=Connection refused
1256	05:26:52 AM	com.ahsay.obs.ae.i(Unknown Source)
1257	05:26:52 AM	com.ahsay.obs.ae.a(Unknown Source)
1258	05:26:52 AM	com.ahsay.afc.util.n.run(Unknown Source)
1259	05:26:52 AM	java.lang.Thread.run(Thread.java:619)
1260	05:26:52 AM	com.ahsay.obs.gw: [SendHandler.connect][Unable to connnect] [IOException] Reason=Connection refused
1261	05:26:52 AM	com.ahsay.obs.as.e(Unknown Source)
1262	05:26:52 AM	com.ahsay.obs.ah.c(Unknown Source)
1263	05:26:52 AM	com.ahsay.obs.ae.i(Unknown Source)
1264	05:26:52 AM	com.ahsay.obs.ae.a(Unknown Source)
1265	05:26:52 AM	com.ahsay.afc.util.n.run(Unknown Source)
1266	05:26:52 AM	java.lang.Thread.run(Thread.java:619)

i. Ensure the connection from AhsayOBS to AhsayRPS is not blocked by your firewall. You can test if the connection is blocked by your firewall by using the telnet command on AhsayOBS server:

telnet < your-replication-server-ip > PORT_NO

your-replication-server-ip = IP address of AhsayRPS.
PORT_NO = TCP port used for replication receiver

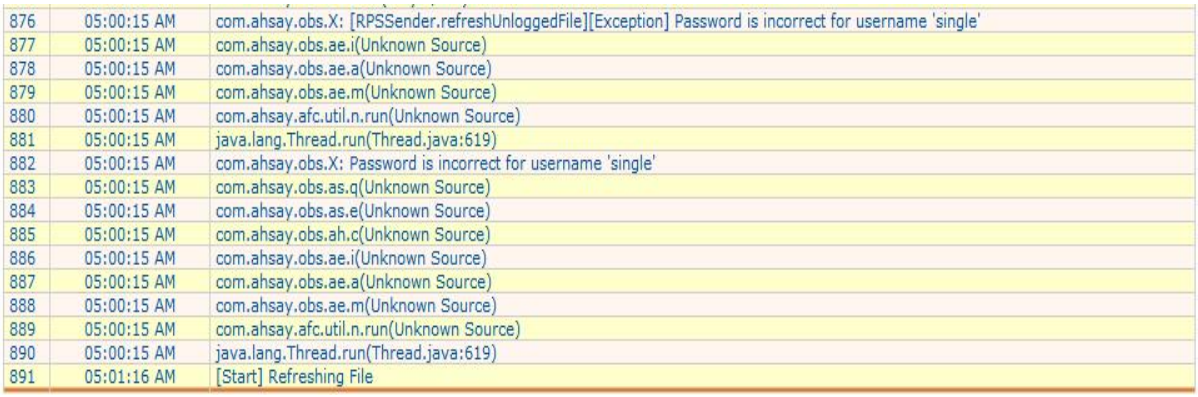
ii. Make sure the <PORT_NO> is not already in use by another receiver on the AhsayRPS server. You can the a list of receivers on AhsayRPS in [Manage System] -> [Manage Receiver]

iii. Make sure the receiver is enabled on AhsayRPS. You check the status of receivers on AhsayRPS in [Manage System] -> [Manage Receiver]

iv. Disk related problems on AhsayRPS server could also result in connection issues to be reported on AhsayOBS. Please make sure the disk for the receiver home is not out of disk space. Check for physical errors with the disk, if the receiver home is a network drive make sure the connection is stable.

11.2 Authentication Errors

[RPSSender.refreshUnloggedFile][Exception] Password is incorrect for username 'xxxxxxx'



876	05:00:15 AM	com.ahsay.obs.X: [RPSSender.refreshUnloggedFile][Exception] Password is incorrect for username 'single'
877	05:00:15 AM	com.ahsay.obs.ae.i(Unknown Source)
878	05:00:15 AM	com.ahsay.obs.ae.a(Unknown Source)
879	05:00:15 AM	com.ahsay.obs.ae.m(Unknown Source)
880	05:00:15 AM	com.ahsay.afc.util.n.run(Unknown Source)
881	05:00:15 AM	java.lang.Thread.run(Thread.java:619)
882	05:00:15 AM	com.ahsay.obs.X: Password is incorrect for username 'single'
883	05:00:15 AM	com.ahsay.obs.as.q(Unknown Source)
884	05:00:15 AM	com.ahsay.obs.as.e(Unknown Source)
885	05:00:15 AM	com.ahsay.obs.ah.c(Unknown Source)
886	05:00:15 AM	com.ahsay.obs.ae.i(Unknown Source)
887	05:00:15 AM	com.ahsay.obs.ae.a(Unknown Source)
888	05:00:15 AM	com.ahsay.obs.ae.m(Unknown Source)
889	05:00:15 AM	com.ahsay.afc.util.n.run(Unknown Source)
890	05:00:15 AM	java.lang.Thread.run(Thread.java:619)
891	05:01:16 AM	[Start] Refreshing File

i. Verify if the username and password entered on the AhsayOBS [Manage System] -> [Replication Config] page is the same as the values defined in replication receiver on AhsayRPS

ii. The port number could be valid but for another active receiver.
Verify if the port number entered on the AhsayOBS [Manage System] -> [Replication Config] page is the same as the value defined in replication receiver on AhsayRPS.

11.3 Replication Always Restarting

For cases where the replication is always restarting itself into UNSYNC mode, please check in the replication logs on AhsayOBS under %OBS_HOME%\system\ReplicationLog. A quick way to track down problems is to open the log for the day of the restart in a text editor, and use the find feature to locate "UNSYNC" phrase.

If this step is repeated on the replication logs for the previous restarts, you can check to see if there are any patterns such as replication is restarting when it tries to replicate the same backupset or the same file/folders. This could indicate a problem with the user home drive itself:

i. Physical disk errors on the user home drive. In which case a disk check should be performed on the affected drive.

ii. It could be due to high I/O loading on the particular user home drive which is causing a read time out.

iii. If the user home is a network drive, check if the connection between AhsayOBS and network drive is stable. This could cause a replication read time out.

11.4 Replication Connection Timeouts

If replication is experiencing persistent connection timeouts which is causing the process to restart itself in UNSYNC mode. But this issue is not setup or hardware related.

Error=[RPSSender.replicateFileUnsync][Exception][SendHandler.sendFile] Stop resending '\User_Home\File' Reason='Failed to send file after XX retries' Exception='Software caused connection abort: socket write error'

You can try to increase the connection time out values on both the AhsayOBS and AhsayRPS services.

AhsayOBS

1. Disable replication on AhsayOBS
2. Shutdown the AhsayOBS service
3. Edit the %OBS_HOME%\conf\rpsSend.xml file
4. Change the default timeout="1800000" (3 minutes) value to larger value, i.e. timeout="9000000" (15 minutes)
5. Restart the AhsayOBS service for the setting to take effect

AhsayRPS

1. Shutdown the AhsayRPS service
2. Edit the %RPS_HOME%\conf\rpsRecv.xml file
3. Change the default timeout="3600000" (6 minutes) value to larger value, i.e. timeout="9000000" (15 minutes)
4. Restart the AhsayRPS service for the setting to take effect

12 Further Information

If you need further assistance, please contact our support team by submitting a ticket to our Forum.

Appendix

Appendix A Product Documentations

Please visit this link for the documentations of Ahsay Products.

Appendix B How to restore files from AhsayRPS

As backup files replicated from AhsayOBS to AhsayRPS are identical, you can use the Decrypt Files Wizard tool available on AhsayOBM to restore backup files from AhsayRPS.

Please use the following instructions:

1. Copy the user account folder or backup set to another on drive on the AhsayRPS server

2. Install AhsayOBM onto the computer running AhsayRPS.

3. Open [AhsayOBM] from the system tray and logon to any AhsayOBS server available (Make sure that you have set the [Control Panel] -> [Administrative Tools] -> [Services] -> [Online Backup Scheduler] service to disable. Otherwise, scheduled backup job configured under this backup account will run on AhsayRPS, possibly causing backup data deletion)

4. Choose [Tools] -> [Decrypt File Wizard]

5. Use the [Browse] button to select the "files" directory which contains all backup files stored under a backup account (i.e. browse to the replicated user home, go down to the "files" directory, go further down to the [User Home] directory as specified on AhsayOBS, find the user account with the backup files you want to restore and finally select the "files" directory)

6. Select the [Backup Set] (shown as numeric ID) containing the backup files you want to restore

7. Select the files that you want to restore and press the [Next] button

8. Set the [Decrypt files to] section, enter a valid decrypting key and press the [Start] button.

As replicated backup sets on AhsayRPS do not contain any index files (index.bdb), the Decrypt File Wizard will first perform a rebuild of the selected backup set in order to generate the index files. Depending on the number of files/folders in the backup set and other factors like disk speed, this could take some time. Only after the index has been generated will the actual decrypt process take place.