

AKIPS Network Monitor
User Manual
Version 16.x



AKIPS Pty Ltd

December 11, 2017

Copyright

Copyright © 2017 AKIPS Holdings Pty Ltd. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of AKIPS Holdings Pty Ltd. All right, title and interest in and to the software and documentation are and shall remain the exclusive property of AKIPS and its licensors.

All other trademarks contained in this document are the property of their respective owners.

AKIPS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL AKIPS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF AKIPS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Contact AKIPS

Web Site: <https://www.akips.com>
Email: info@akips.com

Contents

- 1 Backup / Restore** **4**
- 1.1 Features 4
- 1.2 How it works 4
- 1.3 Important Notes 4
- 1.4 Backup Setups 5
- 1.5 Backup Procedure 6
- 1.6 Restore Procedure 7

1 Backup / Restore

The AKIPS backup / restore is designed to be:

- Secure
- Robust
- Fast
- Simple to configure
- GUI only driven

Note: An AKIPS server can ONLY be backed up using the builtin backup mechanism. You can not just take a copy of the database files as they are constantly being modified by the poller and background database processing.

1.1 Features

- The backup is automatically triggered after the 80 minute database processing has completed. This ensures that the most recent data is backed up.
- Pre-backup filesystem and database integrity checks ensure only valid data is backed up.
- Secure ssh/scp data transfer to/from the backup server.
- Incremental backup only copies files which have changed.
- Backup logs accessed via the System Log Viewer.
- Warning in the GUI if a successful backup has not occurred for two hours.
- No messy copying of ssh keys between the servers as it is all handled by the GUI controls.

1.2 How it works

1. The backup runs as the *root* Unix user.
2. The ZFS file system is placed in *snapshot* mode.
3. The ZFS file system is validated for integrity.
4. The AKIPS databases are validated for integrity.
5. A backup *lock* is applied to the backup server.
6. All modified files are copied to the backup server using secure copy (ssh and scp).
7. The backup *lock* is removed from the backup server.
8. The ZFS snapshot is removed.

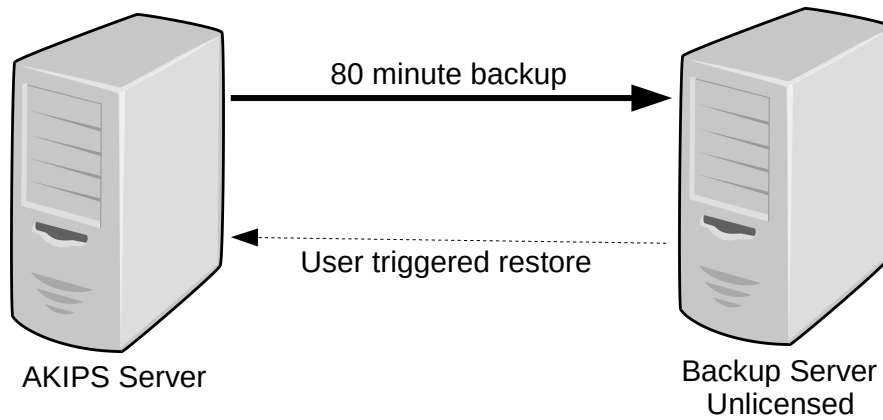
1.3 Important Notes

- A backup server only needs to be a VM with sufficient disk space to store the data from the main AKIPS server.
- A backup server does not require a licence key.
- A redundant server will need to be spec'ed similar to the main AKIPS server.
- A redundant server does require a licence key to be able to perform a restore, then go online.

1.4 Backup Setups

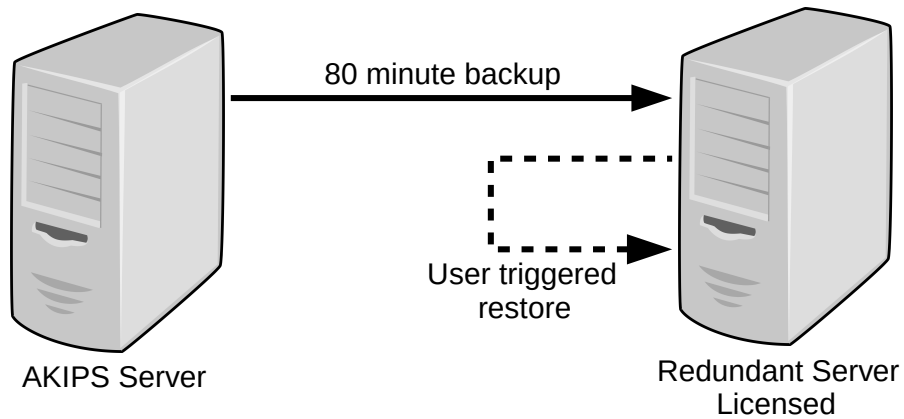
1.4.1 Setup 1

Backup to another copy of AKIPS installed on a separate VM or physical server. The backup server does not require a license. If a failure occurs on the main AKIPS server (eg. hardware fault, VM failure), then a user triggered restore can be performed after the fault has been rectified (eg. replace hard disk).



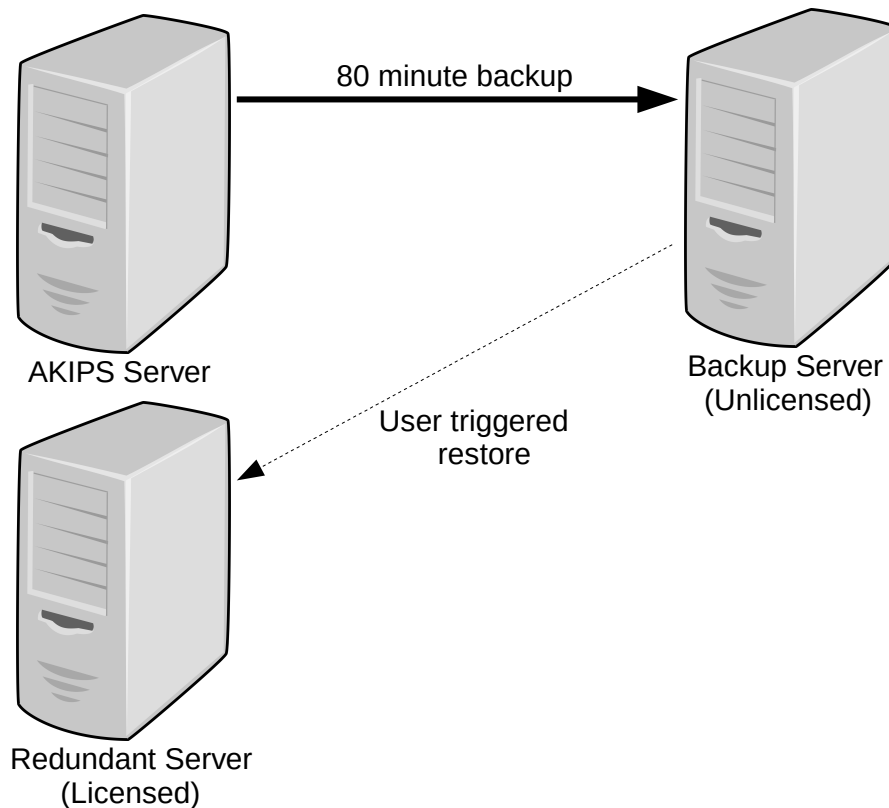
1.4.2 Setup 2

Backup to redundant copy of AKIPS installed on a separate VM or physical server. If a failure occurs on the main AKIPS server, then a user triggered restore can be performed on the backup server. The redundant server will require a software license.



1.4.3 Setup 3

Backup to another copy of AKIPS installed on a separate VM or physical server. The backup server does not require a license. If a failure occurs on the main AKIPS server (eg. hardware fault, VM failure), then a user triggered restore can be performed to the redundant server. The redundant server will require a valid software license.



1.5 Backup Procedure

1.5.1 Backup Server

A backup server:

1. requires enough disk space to store all the data in `/home/akips` on your main server
2. only needs a single CPU core and 1 GByte RAM
3. does NOT require a licence key

1.5.2 Redundant Server

A redundant server:

1. needs to be of a similar specification as your main production server
2. does require a licence key to perform a restore and go online

1.5.3 Configure a Backup

1. Install a copy of AKIPS Network Monitor on the backup VM or physical server.
2. On your main server
 - (a) Go to Admin -> AKIPS Software -> Backup
 - (b) Turn *State* to on.
 - (c) Enter the IP address of the backup server
 - (d) Enter the password for the 'akips' user on the backup AKIPS server.

NOTE: This password is NOT saved. It is only used to copy the ssh public authentication key to the backup server.

- (e) Click *Save Authentication*. This will copy the relevant ssh authentication key to the backup server.
- (f) Click *Test Authentication*. This will test the ssh connection to the backup server by logging in and creating an empty file.
- (g) Use the *Check Status* button to display:
 - Last successful backup
 - Backup disk usage
 - Backup server disk space
 - Backup file listing

1.6 Restore Procedure

1. Perform a clean install of AKIPS Network Monitor onto the server that data is to be restored to
2. Go to Admin -> AKIPS Software -> Restore
3. Enter the IP Address of the backup server
4. Enter the password for the 'akips' user on the backup server
5. Click *Restore*

Note: the restore time is highly dependent on the amount of data to be copied from the backup server to the redundant server.