

reduxio

Reduxio Best Practices for  
**Splunk® Enterprise v6.x**

For more information, refer to Reduxio website at <http://www.reduxio.com>.  
If you have comments about this documentation, submit your feedback to [docs@reduxio.com](mailto:docs@reduxio.com).

Revisions:	Descriptions
<a href="#">Aug 4, 2016</a>	<a href="#">Initial version.</a>

© 2016 Reduxio Systems Inc. All rights reserved. No portions of this document may be reproduced without prior written consent of Reduxio.

Reduxio™, the Reduxio logo, NoDup™, BackDating™ and Tier-X™ are trademarks or registered trademarks of Reduxio in the United States and/or other countries.

Linux is a registered trademark of Linus Torvalds.

Windows is a registered trademark of Microsoft Corporation.

UNIX is a registered trademark of The Open Group.

ESX and VMWare are registered trademarks of VMWare, Inc.

All other brands or products are trademarks or registered trademarks of their respective holders and should be treated as such.

The Reduxio system hardware, software, user interface and/or information contained herein is Reduxio Systems Inc. proprietary and confidential. Any and all rights including all intellectual property rights associated therewith are reserved and shall remain with Reduxio Systems Inc. Rights to use, if any, shall be subject to the acceptance of the End User License Agreement provided with the system.

Information in this document is subject to change without notice.

Reduxio Systems, Inc.  
111 Pine Avenue  
South San Francisco, CA, 94080  
United States  
[www.reduxio.com](http://www.reduxio.com)

# Contents

Overview .....	4
Introduction.....	4
Benefits with Reduxio.....	4
Best Practices.....	4
Migrating Index to Reduxio .....	4
Recovering Index using BackDating .....	5
Conclusion .....	5

# Overview

## Introduction

Splunk® Enterprise is the leading platform for real-time operational intelligence. Streams of machine data generated by a wide range of supported content sources – log files, syslog outputs, HTTP sources, customized scripts and more. Hundreds of 3<sup>rd</sup>-party applications provide support for data collection from many IT systems available in the market.

Splunk provides an easy, fast and secure way to search, analyze and visualize the indexed data to help troubleshooting application problems and investigate security incidents.

## Benefits with Reduxio

Reduxio provides multiple benefits to Splunk customers:

- Space savings for index files.
- Simple recovery for the index files.

Observed savings ratio in testing: 5.2:1.

## Best Practices

### Migrating Index to Reduxio

To migrate the Splunk index files, perform the following steps:

- Create a new Reduxio volume and mount it on the Splunk server.
- Create a baseline copy using Rsync.
- Stop the Splunk service.
- Perform an incremental Rsync to copy the latest changes.
- Remount the Reduxio volume.
- Start the Splunk service.

To read more about Splunk instance migration, refer to:

<http://docs.splunk.com/Documentation/Splunk/6.4.2/Installation/MigrateaSplunkinstance>

First, configure the iSCSI initiator according to the instructions in Reduxio Support [iSCSI Interoperability Matrix](#).

```
# apt-get -y install open-iscsi open-iscsi-utils multipath-tools lsscsi
# cat /etc/iscsi/initiatorname.iscsi
# ssh rdxadmin@mango hosts create splunk -iscsi-name
# ssh rdxadmin@mango volumes create splunkdb -size 10240
# ssh rdxadmin@mango volumes assign splunkdb -host splunk
# iscsiadm --mode discovery -t st -p 10.46.216.11
# sudo iscsiadm -m node -l
# mkfs -t ext4 /dev/dm-0
# mkdir /splunknew
# mount /dev/dm-0 /splunknew/
# rsync -av /opt/splunk/ /splunknew/
# splunk stop
# rsync -av /opt/splunk/ /splunknew/
# mv /opt/splunk /opt/splunk.orig
# mv /opt/splunk /opt/splunk.orig
# umount /splunknew
# mkdir /opt/splunk
# mount /dev/dm-0 /opt/splunk
```

```
# splunk start
```

## Recovering Index using BackDating

Reduxio clone and revert can be used to recover a Splunk environment, or prepare a test sandbox.

To create a clone back in time and start Splunk from the clone:

```
# ssh rdxadmin@mango volumes clone splunkdb -name splunkdbc11 -timestamp 08/04/2016-07:30:00
# ssh rdxadmin@mango volumes assign splunkdbc11 -host splunk
# splunk stop
# umount /opt/splunk
# mount /dev/dm-1 /opt/splunk
# splunk start
```

## Conclusion

Reduxio storage provides many benefits to Splunk customers. The migration of the Splunk index files to Reduxio and the recovery of the index from any point in the past are both simple and straightforward processes.

### Reduxio Documentation

- Reduxio Support Portal - *Reduxio TimeOS™ Administration Guide*

### Splunk Documentation

- Splunk Enterprise Documentation - <http://docs.splunk.com/Documentation/Splunk>