

Citibank Kazakhstan

Backup and tape library management process

Revision History:

Version	Date	Reviewer	Changes / Comments
1.0	03.01.2004	Michael Topchin	Issued
2.0	28.01.2005	Dmitriy Petrenko, Rustem Milushev	Backup schedule, ETM control and a number of other major changes. Procedure was completely overwritten.
3.0	15.08.2005	Rustem Milushev	References to decommissioned servers have been removed.
3.1	03.10.2005	Dmitriy Petrenko	Wording has been changed in section "Backup media rotation schedule and retention time"
4.0	01.12.2005	Michael Topchin	Implantation of Legato Replistor part. Some minor changes: test tapes, check inventory log, etc

TABLE OF CONTENTS

- 1. Overview**
- 2. Backup Process Key Concepts**
- 3. Backup media rotation schedule and retention time**
- 4. Backup media transfer control**
- 5. Backup and restore procedures**
- 6. Signoffs**

1. Overview

Backups are the most important and effective form of protection from accidental and deliberate loss of data. Although there are many software utilities that claim to be able to unerase disks or recover data from damaged computers, such software no substitute for having an intact up-to-date copy of the data held in different locations.

This document covers the backup process and procedures for the backups of data, applications, database records, and executable programs on Servers. TI staff should follow these process and procedures for taking backup of servers under their responsibility and operation.

2. Backup Process Key Concepts

All business critical information kept in production computing systems (data, applications, database records, and executable programs on servers) must be backed up on a regular basis on other magnetic media (tapes) with keeping on site and Network backup with full replication to CoB servers. Network data link where data flows is encrypted in accordance with citigroup standards. NICECALL (voice recorder) tapes keep on site (HQ). Criticality of two buildings (HQ and CoB) is the same, because of both are active business centres and in this case not necessary to move NICECALL tapes to CoB.

Tape Library Management is a responsibility of **Tape Librarians** who handle the organization, control and security of the material related to network processing. The main role of the Tape Librarians is the custody over tape cartridges and system related documentation. The objective is to have an independent control over the Network Facility operational processing activities. This includes the following responsibilities:

- To ensure that cartridges required by the Network Facility are delivered on time;
- To ensure that all cartridges not in use by the Network Facility are properly stored and locked away;
- To maintain an updated inventory list of all cartridges and system related documentation under his/her custody, identifying the location of these cartridges and documentation;
- A physical inventory must be conducted semi-annually.

The backup media must be securely held and inventoried. Access to this media should be restricted and controlled.

There are the following steps for daily (monthly, yearly) process:

1. Every day between 8:00AM and 10:00AM Network Facilities should check completion status of nightly backups on all systems where it is applicable.
2. Tape Librarian in the morning (from 10:00 till 11.00) takes out the tapes with the previous day backup from devices and moves to the fireproof safe with sign the

Media Movement Log. NICECALL tapes (voice recorder) must be added to the set of delivered tapes every Tuesday.

3. Tape Librarian should take out from the safe the tapes for today's backup. These tapes were used for backup that was done during the previous week (e.g. if today is Monday the tapes with the previous Monday's backup should be taken). If it is the EOM backup Tape Librarian should take out the tapes that were used for backup that was done during the previous year (e.g. if it is January the tapes with the previous January's backup should be taken). And if it will be EOY backup Tape Librarian should deliver free tapes;
4. Librarian should insert all tapes into backup devices.

Template of Media Movement Log is embedded:



Media_LOG_ON-SITE
.xls

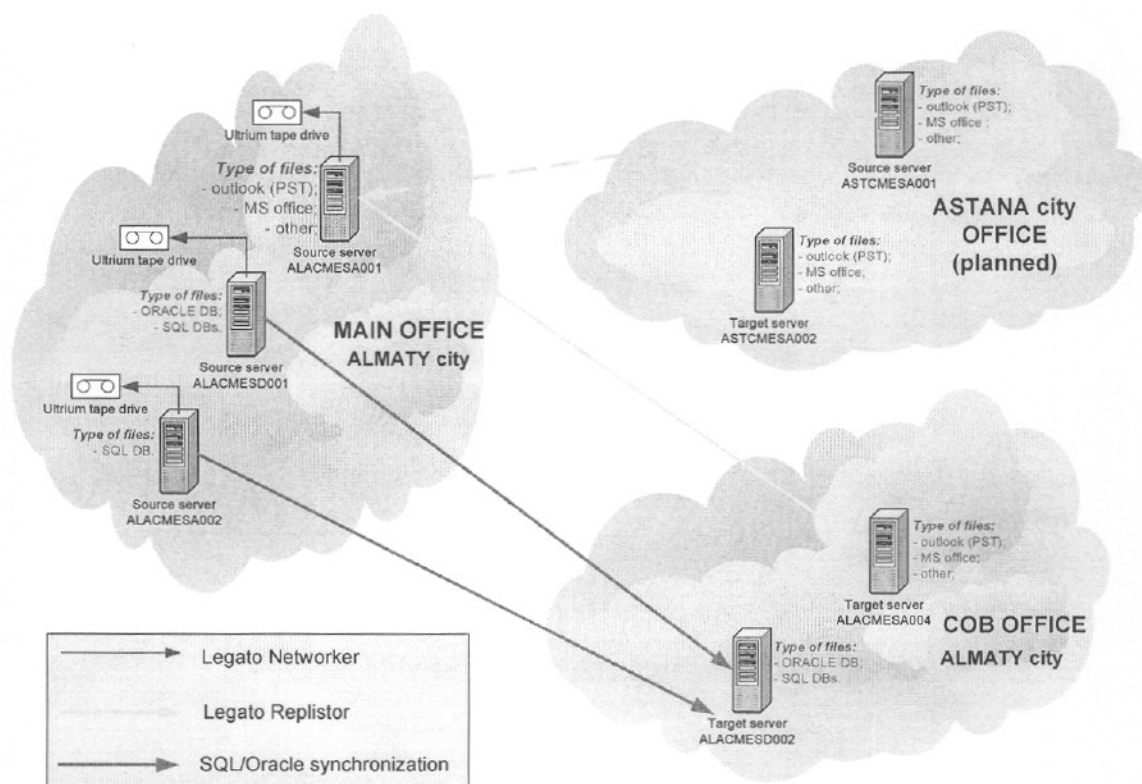
Backup process must be properly scheduled and monitored. All failures must be resolved through the problem management process.

A document on Network backup procedures and retention periods that contains signoffs from Network Facilities, business/operations management and user management must be retained and reviewed quarterly. IT manager is responsible for control over the schedules and procedures to ensure that backup process is performed according to the document's provisions and agreed standards.

The following is the list of software and hardware used to take backups:

System	Software	Backup scope	Hardware
ALACMESA001	Legato Networker 7.2	D:\ whole drive	HP Ultrium 100/200GB
ALACMESA001	Replistor 6.03	D:\APPS; D:\DATA_GRP; D:\PUD; D:\HOME;	N/a
ALACMESA002	Legato Networker 7.2 + SQL backup module	D:\ whole drive	HP Ultrium 100/200GB
ALACMESA002	SQL online replication	SQL DBs	N/a
ALACMESD001	Legato Networker 7.2 + SQL backup module	D:\ whole drive	HP AIT 50/100 GB
ALACMESD001	SQL & ORACLE online replication	SQL and ORACLE DBs	N/a
NICECALL	Built-in application	All recorded information	HP DAT DDS2

Diagram of backup infrastructure and data flow



3. Backup media rotation schedule and retention time

Backups of all critical data should be taken from production servers on the daily basis. Backup schedule should exist for every production system and ICU should be provided with the copy of this document (find below).

The following is the media rotation schemes for all production computing systems.

Name	Server and type of backup	Rotation scheme	Retention time
Daily	ALACMESA001 (replication);	In on-line mode all changes (creation, changing or deletion of files and databases) reflect to CoB servers in 1 hour interval.	N/a
Daily	ALACMESA002 (replication);	SQL DB replication every 2H on CoB server ALACMESD001	N/a

Daily	ALACMESD001 (replication);	ORACLE online replication based to CoB server ALACMESD001 (when changes reach 100Mb size); SQL DBs replication every 2H on CoB server ALACMESD001.	N/a
• Daily	ALACMESA001 (full backup); ALACMESA002 (full backup); ALACMESD001 (full backup); NICECALL	Five tapes are used to take daily backups every night on Tuesday, Wednesday, Thursday, Friday and Saturday on each production server. Media is changed on the basis of weekly rotation scheme. NICECALL backup tapes are not the subjects of rotation. Every Thursday NICECALL tapes are delivered to Off-Site Library and kept there during one year.	1 week (server backups)/1 year (NICECALL backups)
• Monthly	ALACMESA001 (full backup); ALACMESA002 (full backup); ALACMESD001 (full backup);	Eleven tapes are used to take monthly backups every first night of months from February to December on each production server. Media is changed on the basis of annual rotation scheme.	1 year
• Annually	ALACMESA001 (full backup); ALACMESA002 (full backup); ALACMESD001 (full backup);	New tape is used to take annual backups every first night of January on each production server	5 years
• New release/major configuration changes	ALACMESA001 (full backup); ALACMESA002 (full backup); ALACMESD001 (full backup);	Temporary tape is used to take unscheduled backups. This media is kept until next scheduled backup.	temporary

All backup logs should be kept at least during one quarter where it is applicable.

Backup results must be reflected in the maintained hardcopy journal by the Network Facilities or designated Server Operator every morning after checking. These Logs should be reviewed by BISO on Semi-annual basis.



template.xls

Each tape that is used for regulatory backup should properly labeled with a meaningful abbreviation describing the target server, backup rotation scheme mark and tape physical expiration date.

Expiration date is calculated on the basis of the tape rotation schedule and official tape life cycle declared by vendor. Upon expiration, every tape should be properly destructed (either physically or by means of logical data erasing and following complete demagnetization process). Two personnel should evidence the destruction and Destruction memorandum should be filled. The following is the life cycles for common HP tapes:

- DDS2/DDS3/DDS4/AIT – 2000 passes or 100 full backups
- DLT3/DLT4/Ultrium – 1 million passes or 260 full backups

Example of SOE server stickers is embedded:



stickers.doc

5. Backup and restore procedures

Backup procedures should be performed by the Network Facilities or designated Backup Operator. Restore Procedure must be performed by the Network Facilities. It is their responsibility to backup and restore LAN data as it is described in these procedures.

Backup procedure for the production servers

Backup is done by special backup script which contains four main blocks:

- stop services (only for Oracle);
- perform FULL backup with verification ;
- start all services.

Normally, this script will start automatically at 23:30. Depending on volume of data it will run for 2-4 hours.

NICECALL backup procedure:

- run the commands: EXIT\ADMIN\EJECT
- mark the date and time of unloading on cassette itself
- switch on write protection on cassette
- ensure that this cassette is included in set of tapes that are to be delivered to safe (T-COM room)
- prepare new cassette
- mark date and time of loading on cassette itself
- load cassette
- run the following commands: EXIT
\VIEW
- if everything is OK display will show: 100% FREE .

Backup Operator must ensure that all tapes are inserted properly and tape drive indicators "READY" are active.

Restore procedure for the production servers

- Insert labeled tape cartridge into the tape unit on target server.
- Run the Restoration software (Legato on SOE servers) and perform restoration of required data.
- Wait till the operation is completed. After completion check the operation log. If there are any errors investigate the reason and make appropriate actions. This may require the repetition of the operation.

Tapes Readability Test

Tape readability tests are performed on monthly basis.

- 1) Take randomly selected tape from the safe.
 - 2) Identify, what server backup is stored on the tape and what is the date of that backup.
 - 3) Place the tape in the library and restore randomly selected file to any temporary location.
 - 4) Verify that restored file is readable.
 - 5) Delete restored file.
 - 6) Remove the tape from the library and place it back in the safe.
 - 7) Prepare the "Tapes Readability Test Results Memo" with the information about:
 - Tape ID
 - Server name
 - Backup date
 - Full path to the restored file and the file name.
 - Test results.
- Sign the memo and give to CTI Head manager or CTI Helpdesk supervisor for approval.

This test applicable to NICALL tapes – business check it during RCSA process.

If any regular, user-requested file restore is performed in the last month, it is assumed that tape readability test was successfully performed and no additional activity is required. however, if the restore was unsuccessful test recover is performed for randomly taken 5% of EOM tapes. The Virtual Request ticket is test evidence in this case.

Tapes Destruction

All backup tapes, which are identified as unreadable, mechanically damaged or passed its retention level, should be destroyed. Tapes are destroy by CTI Helpdesk specialists using demagnetizer "KCY-2C-994" device. This must be done in presence of two employees. After destruction memo (with name of destroyed tapes) must be sent to CTI Head manager or CTI Helpdesk supervisor.

Tapes Inventory Verification

Tapes inventory is verified on quarterly basis.

- Prepare the list of the media from safe.
- Obtain the results of previous tape inventory verification.
- Investigate all discrepancies between actual contents of the safes and the results of previous check.

Prepare the report and present it to CTI Head manager or CTI Helpdesk for verification and approval.

Reporting

Each backup system (NICALL exclude) has its own reporting facility, which is used to check the status of overnight backups. Backup status (only in case backup is missing or something wrong is happened) sends in the morning to VT system (ticket on CTI Helpdesk assigned automatically). In that case (when something is wrong) CTI Helpdesk personnel must conduct full investigation of backup log and add report of actions what took a place into corresponded VT ticket and then close it.

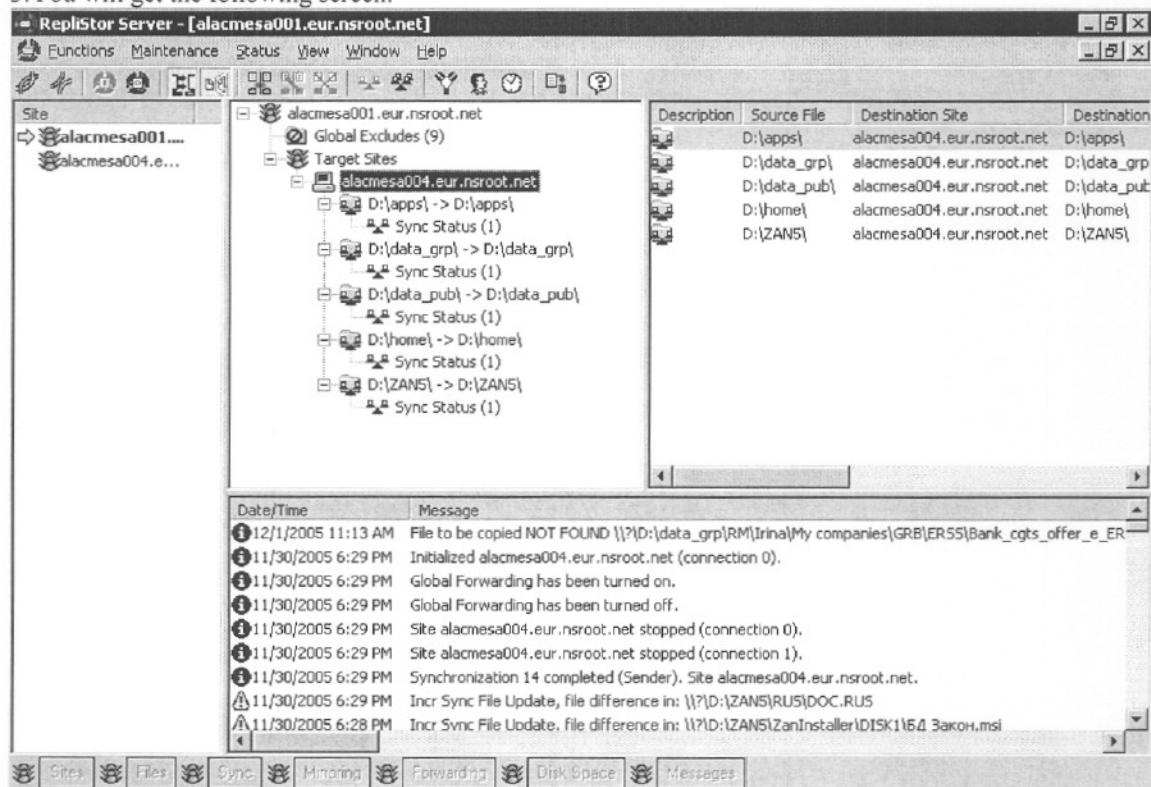
Additionally, to ensure that the data replicated with Legato RepliStor ORACLE replication and SQL replication from HQ branch servers to CoB servers is complete and consistent, the replication process needs to be monitored.

REPLICATION STATUS CHECK

The details how to check and report backup status for each backup system are described below.

Legato RepliStor CHECK

1. login on server ALACMESA001.
2. Run Replisotr application by the following path: START\PROGRAMS\REPLISTOR.
3. You will get the following screen:



4. Check that all traffic lights are GREEN (on the button of the page). If YELLOW or RED – refer to user manual to get explanation of error and ways to troubleshoot then.

ORACLE REPLICATION CHECK

- 1. run this script (see below) under administrator (sys or system) using query analyzer.
- 2. Check SEQUENCE# for dest_ids 1 and 2, if equal - log was transferred to standby
- 3. Check APPLIED for DEST_ID 2, if YES - log was applied on standby
- 4. If 2. and 3. are OK replication works properly

```
select name, dest_id, sequence#, standby_dest, archived, applied from v$archived_log
```



status_check.sql

SQL REPLICATION CHECK

Procedure of checking MSSQL Log shipping

MSSQL Log Shipping using log backup method for restoring information on COB site. MSSQL use jobs for making log backup and JT jobs for file transferring.

Transfer use robocopy.exe application and rcopy.bat for starting.

All executing and log files placed by path "D:\JTFTP" on ALACMESA002 and ALACMESD001

Backup files placed by paths:

Server: ALACMESA002

D:\mssql2k\TransactionLogs\ <DIRS> \

Server: ALACMESD001

D:\mssql\TransactionLogs\ <DIRS> \

On the COB server – ALACMESD002, all files are uploading to the next folders:

D:\mssql\mssql\TransactionLogs\ <DIRS> \

Where <DIRS> are folders where is placed transaction log backup files.

Backup makes and transfers every 2 hours from 8:00 till 20:00

Restore also makes every 2 hours from 8:30 till 20:30

Below are steps for checking of work MSSQL Log Shipping.

Servers: ALACMESA002 and ALACMESD001

- Check that backup files were transferred
 - Login to the server, open explorer and look every backup directories. Each folder should be empty.
 - If folders are not empty, check log files ("D:\JTFTP\Rcopy*.log") that transaction log backup files are transferring.

If problem with transferring, check connection to COB server and that COB Server is running.

6. Signoffs

The undersigned have reviewed and approved this Manual

Senior Country Operations Officer

Technology Head

BISO

SIGN OFF DATE _____

6. Signoffs

The undersigned have reviewed and approved this Manual



05.12.2005

Senior Country Operations Officer



Technology Head



BISO

SIGN OFF DATE 01.12.2005