BACKUP & RESTORE

Backup & Restore

backup restore

1. Introduction

This document is intended to provide administrators with the best practices for maintaining RCDevs WebADM and related applications (such as OpenOTP Authentication Server). The reader should notice that this document is not a guide for installing WebADM and its applications. Specific guides are available through the RCDevs online documentation library on RCDevs Website.

WebADM installations and usage manuals are not covered by this guide and are documented in the RCDevs WebADM Installation Guide and WebADM administrator's Guide available in RCDevs website.

This guide covers backup and restore recommendations for a typical RCDevs solution deployment including WebADM, OpenOTP with Radius Bridge and RCDevs Directory Server. Recommendations for deployments with Microsoft ActiveDirectory and Novell eDirectory are covered by this document. RCDevs installation packages do not install any file on the OS file structure (but startup scripts and log rotation scripts) and does not require any software dependency to be installed. It is also easy to move one installation to another server installation simply by copying the RCDevs components to the new server and repair some permissions.

2. Application Components

Your RCDevs solution includes WebADM with Web Services and WebApps, OpenOTP Radius Bridge, RCDevs Directory Server (or another LDAP implementation), SQL databases (MySQL or PostgreSQL). All these components shall be part of your backup and restore plan for an efficient system maintenance plan.

WebADM and OpenOTP may rely on connections to other remote services such as SMSC connectors. It is highly recommended to back up any external service connection parameters as part of your backup plan.

2.1 WebADM Server

WebADM is the main component in your installation. It is composed of program files, flat configuration files, Web Services, WebApps, and log files. A WebADM system with its applications can be easily re-installed from scratch provided that configuration files can be recovered and that all previously-installed applications can be re-installed with the same package versions. It is recommended to keep all your installation packages as part of your backup plan to be able to restore specific application versions at any time.

2.2 OpenOTP Radius Bridge

Radius Bridge is a component which is provided with OpenOTP and provides a RADIUS interface for your OpenOTP authentication service. Radius Bridge is a standalone component which is installed separately and includes its own configuration files and log files. There is no user data stored by Radius Bridge to be backed-up, but only static configuration files.

2.3 LDAP Directories

The LDAP directories contain your user and group resources and WebADM application configurations. You may have deployed your WebADM server using a pre-existing LDAP directory or have installed a dedicated directory. In both cases, LDAP data are some of the most important data and shall be backed-up regularly.

WebADM applications store their work data directly on the user and group objects in the webadmAccount LDAP objectclass. There is also no dedicated databases for storing user metadata such as OpenOTP Tokens.

WebADM stores any graphically configured components in LDAP objects. WebADM Domains, Trusts, MountPoints, OptionSets and Client configurations are also stored in the following LDAP locations:

- WebADM Administrator Roles: dc=AdminRoles,dc=WebADM
- WebADM Client Policies: dc=Clients,dc=WebADM
- WebADM Access Devices: dc=Devices,dc=WebADM
- WebADM User Domains: dc=Domains,dc=WebADM
- WebADM LDAP Mount Points: dc=MountPoints,dc=WebADM
- WebADM LDAP Option Sets: dc=OptionSets,dc=WebADM
- WebADM Web Applications: dc=WebApps,dc=WebADM
- WebADM Web Services: dc=WebSrvs,dc=WebADM

> **Note**
>
> The locations may differ and are set in the WebADM main configuration file in `/opt/webadm/conf/webadm.conf`

2.4 SQL Databases

The SQL databases contain the following set of information:

- audit information contained in:
  - the Admin log table: this audit table records any administrative action performed by administrators from the WebADM Admin Portal.
  - the WebApp log table: this audit table records any user operation performed from RCDevs WebApps (ex. User Self-Service Desk).
  - the Web Services log table: this audit table records any operation or transaction performed by Web Services such as OpenOTP. It typically includes authentication failures and success to the system.
  - the Manag table: this audit contains all API action done through the Manager API
- localized messages contained in the Message table: this table contains language-specific end-user messages.
- inventory of hardware token contained in the Inventory table
- certificates issued by the ca of WebADM contained in the Certificate table

- alert when an issue is detected contained in the Alert table
- statistics of the different services/application per session server are stored in Statistic table
- record of SSH session is stored in Record table

> **Note**
>
> The content of the database tables shall be considered as part of your backup plan.

3. Detailed Backup Requirements

This section describes all the data to be included in your backup plan and the methods which are recommended for an effective backup.

3.1 WebADM Server

3.1.1 Configuration Files

The configuration files are stored in the /opt/webadm/conf/ folder. The whole configuration directory shall be backed-up. The most important files are:

- The webadm.conf file: This file provides the main configurations and includes the WebADM master key used for LDAP and session encryption. This secret key shall be kept carefully as any LDAP sensitive data would become unusable without it. Because of this key, the webadm.conf file contains very sensitive information and the backup file shall be protected against any unauthorized access.
- The servers.xml file: This file contains connection parameters to remote services such as LDAP directories, SQL databases, session managers, PKI server and HTTP proxies. The connection parameters include login names and passwords. The backup file shall also be protected against any unauthorized access. Configuration files can be simply copied to a backup location or archived using UNIX tools like GNU TAR. The configuration files are set once and should remain unmodified most of the time. We recommend backing up the configurations directly on the server and encrypting the archive with GnuPG (GNU Privacy Guard) or a similar file encryption tool.
- Backup the configuration folder with:

```
tar -cvf /root/webadm_config.tar /opt/webadm/conf/
gpg -c /root/webadm_config.tar
```

In this example, we create a configuration archive and encrypt it locally with GnuPG and a secret passphrase. You can store the encrypted archive on a backup drive, and it cannot be read without the encryption passphrase.

- Backup the PKI folder with:

```
tar -cvf /root/webadm_pki.tar /opt/webadm/pki
gpg -c /root/webadm_pki.tar
```

3.1.2 WebADM WebApps

The WebADM WebApps' resources are located in the /opt/webadm/webapps/ folder. Consider archiving the whole folder as part of your backup plan. The application files are static, do not contain any file configuration file and get never modified. You can back up your application with GNU TAR or similar UNIX commands once deployed and every-time you upgrade or add a new application.

Example:

```
tar -cvf /root/webadm_webapps.tar /opt/webadm/webapps/
gpg -c /root/webadm_webapps.tar
```

3.1.3 WebADM Web Services

The WebADM Web Services are located in the /opt/webadm/websrvs/ folder. Consider archiving the whole folder as part of your backup plan. The application files are static, do not contain any configuration file and get never modified. You can back up your application with GNU TAR or similar UNIX commands once deployed and every-time you upgrade or add a new Web Service.

Example:

```
tar -cvf /root/webadm_websrvs.tar /opt/webadm/websrvs/
gpg -c /root/webadm_websrvs.tar
```

3.1.4 Other Alternative

You can alternatively back up the whole WebADM folder in /opt/webadm/ for a simpler backup procedure which includes configuration files, WebApps and Web Services.

Example:

```
cd /opt/
tar -cvf /root/webadm.tar /opt/webadm/
gpg -c /root/webadm.tar
```

Note

WebADM setup created a system user (webadm) at the OS level and created permissions in the WebADM installation folder. On a complete disaster recovery situation, you would have to reinstall a new server with the same IP addresses and DNS names and re-create the webadm system user for restoring your WebADM server.

You can include the log files in /opt/webadm/logs/ as part of your backup or not. Log files provide runtime information which is useful for troubleshooting WebADM and its applications. Restoring the log files is not required for normal operations.

3.2 Radius Bridge

Radius Bridge includes RADIUS server configuration files in the /opt/radiusd/conf/ folder. The configuration files are:

- radiusd.conf: This file should never be modified and contains the mains RADIUS server configurations.
- openotp.conf: This file contains the OpenOTP settings such as the OpenOTP server URL, password concatenation parameters…
- clients.conf: This file contains your RADIUS client specifications with their RADIUS secrets.

Because of the RADIUS secrets, it contains sensitive information and the backup files shall also be protected against unauthorized access.

Example:

```
tar -cvf /root/radiusd_config.tar /opt/radiusd/conf/
gpg -c /root/radiusd_config.tar
```

3.2.1 Other Alternative

You can alternatively back up the whole Radius Bridge folder in /opt/radiusd/ for a simpler backup procedure.

Example:

```
tar -cvf /root/radiusd.tar /opt/radiusd/
gpg -c /root/radiusd.tar
```

Note

Radius Bridge setup created a system user (radiusd) at the OS level and created permissions in the installation folder. On a complete disaster recovery situation, you would have to re-install a new server with the same IP addresses and DNS names, and re-create the radiusd system user for restoring your Radius Bridge server.

You can include the log files in `/opt/radiusd/logs/` as part of your backup or not. Log files provide runtime information which is useful for troubleshooting Radius Bridge. Restoring the log files is not required for normal operations.

3.3 LDAP Directory

The LDAP backup procedure depends on your LDAP implementation. We are assuming backup procedures are already in place to back up the whole user directories.

For backing-up WebADM shared configurations, you shall extract the content of the WebADM LDAP container (ex. The contents of the dc=WebADM subtree). As described above, this container includes all WebADM configuration object such as the WebADM Domains. And it contains the application configurations (ex. OpenOTP server configuration). In WebADM Admin Portal, you can export the dc=WebADM subtree in an LDIF file.

With RCDevs Directory Server, we included a backup script in /opt/slapd/bin/backup. The script dumps the whole LDAP database in a local LDIF file. The backup includes all LDAP objects and all the WebADM LDAP configurations. You can easily restore the whole LDAP tree with the provided restore script in /opt/slapd/bin/restore.

Example:

```
cd /opt/slapd/bin/
./backup /root/ldap.ldif
gpg -c /root/ldap.ldif
```

Note

A restore will destroy any LDAP modification done after the backup file was created. RCDevs Directory Server includes one configuration files: /opt/slapd/conf/slapd.conf. This file contains your first administrator password and the backup files shall also be protected against unauthorized access.

Example:

```
tar -cvf /root/slapd_config.tar /opt/slapd/conf/
gpg -c /root/slapd_config.tar
```

3.3.1 Other Alternative

You can alternatively back up the whole RCDevs Directory Server folder in /opt/slapd/ for a simpler backup procedure. In this case, be sure to stop the LDAP server before backing-up.

Example:

```
cd /opt/slapd/bin/
./slapd stop
tar -cvf /root/slapd.tar /opt/slapd/
gpg -c /root/slapd.tar
./slapd start
```

> **Note**
>
> RCDevs Directory Server setup created a system user (slapd) at the OS level and created permissions in the installation folder. On a complete disaster recovery situation, you would have to re-install a new server with the same IP addresses and DNS names, and re-create the slapd system user for restoring your directory server.

You can include the log files in /opt/radiusd/logs/ as part of your backup or not. Log files provide runtime information which is useful for troubleshooting RCDevs Directory Server. Restoring the log files is not required for normal operations.

3.4 SQL Databases

The SQL backup procedure depends on your database implementation (MySQL, PostgreSQL…). We are assuming backup procedures are already in place to back up the whole SQL databases. You can locally back up the WebADM MySQL database with the mysqldump command. Example:

```
mysqldump webadm > /root/mysql.sql
gpg -c /root/mysql.sql
```

Restore the WebADM MySQL database backup with the mysql command.

```
mysql webadm < /root/mysql.sql
```

4. Other Considerations

4.1 WebADM Customizations

Some WebADM WebApps and Web Services such as OpenOTP SMSHub may contain customized scripts like custom SMS connectors. Backing-up the whole Web Services' folder will ensure your customizations will be included in your backup plan.

For example, you may have edited the SMSHub SMSC custom scripts `/opt/webadm/websrvs/smshub/lib/smshub_custom1.php.` WebADM will keep your modifications on any customizable script during an upgrade. But you need a backup of your modifications in the event of a full reinstallation. Be sure to keep your script modifications as part of your backup plan.

4.2 Additional Components

You may have installed other components on your servers. For example, you may have installed a third party SMSC client program on your server for use in the SMSHub custom scripts. Be sure to back up any such program which is required for normal WebADM operations as part of your backup plan.

Note

Do not add binaries and file resources other than customizable scripts in the RCDevs software folders. The RCDevs software installers will automatically remove additional files during an upgrade.

4.3 Cluster Installations

In a cluster installation, you should back up the configuration files of all cluster nodes. Most of the configurations should be identical but some files may differ (ex. WebADM servers.xml).

Your cluster should have LDAP and SQL real-time replication in place, and you also do not need to back up LDAP and SQL data on each cluster node.

5. Restoring from a Backup

You may restore configuration files at any time for any RCDevs software. Be sure to restore configurations from backup which were made on the same version as the currently installed software. If you need to restore configurations for another software version, reinstall the corresponding software version first from a backup or using the installation package for the version. Be sure to stop all the affected services before a restore and to restart them after the restore is completed.

Note for GnuPG

GnuPG is a free software and can be downloaded at GnuPG website You can decrypt GPG encrypted file by calling the command:

```
gpg myfile.tar.gpg
```