]HackingTeam[

Remote Control System

Da Vinci

Migrating from version 7

INTRODUCTION

Remote Control System daVinci is a complete new product. Upgrading from RCS 7.6 is not performed automatically as you were used to upgrade from 6.x or from 7.x. This is due to the fact that the underlying database was changed to better suite the scalability needs of today's interception. All the data will need to be migrated from the old database to the new one. This task will require lot of disk space; make sure to have enough disk space before starting the migration.

RCS daVinci is RAM intensive, so we highly recommend upgrading the RAM of the database server. If you have any question about the system requirement feel free to ask to the HT support team.

It is completely safe to install daVinci on a production server. RCS 7 and daVinci can run side-by-side on the same machine without any problems. Should you encounter any issue during the migration phase you can always fall back to the running RCS 7.

Read this document carefully before the upgrade; if in doubt ask to the HT support team.

NAMING CONVENTION

With RCS daVinci we have changed the name of some entities you were used to:

Activity -> Operation

Target -> Target

Backdoor -> Agent

Agents -> Modules (in the configuration)

Logs -> Evidence (data collected by the agents)

ASP -> Frontend

ASP (RSS) -> Collector

ASP (RLD) -> Worker

ASP (RNC) -> Network Controller

ASP (RSSM) -> does not exist any more

RCSDB -> Backend

BEFORE STARTING

There is some IMPORTANT information that must be taken into consideration before migrating to daVinci:

The Backend must be updated to version 7.6 before starting the migration to daVinci.

If you have any agent which is older than 7.2 (2011032101), upgrade it to 7.6. Old agents will not be able to communicate with the new daVinci Collector.

Agents older than 7.6 (2012013101) that are not upgradable (blackberry, android and symbian) will continue to communicate with daVinci but you will not be able to change their configuration. Make any configuration change before the migration.

Agents running on OSX Lion cannot be updated from 7.x to daVinci. Starting from daVinci you will be able to update them again when 8.x will be released.

All the agents on the field will need to be upgraded to daVinci (2012041601) before being able to change their configuration again.

MIGRATION PROCEDURE

BACKEND

1- Perform a backup

Perform a full backup of the C:\RCSDB directory in a safe place. Just in case you want to go back in case of disaster.

2- Mount External Storage

If your server is connected to an external storage (NAS) that is used to store the data of RCSDB, follow these instructions (otherwise skip to step 3):

- Mount the NAS under a new directory named C:\RCS.

- Check that the content of C:\RCSDB and C:\RCS is the same.

3- Install RCS daVinci

Execute the daVinci installer and choose the correct installation setup:

- "Distributed Installation" -> "Master node" (if you have 2 or more servers).
- "All-in-one" (if you have one single server)

Is everything ok?

Install the RCS console and try to login into the new system with the admin account created during the installation. If you are able to login you can proceed, otherwise refer to the installation manual for troubleshooting or ask to HT support team.

4- Migrate metadata

Metadata are the information needed by the system to receive new evidence from agents: encryption keys, configurations, the descriptions of the objects, users, groups… basically all the information stored into the database except for the agents' evidence.

Migrating the metadata enables you to see your RCS 7 installation inside the new look of daVinci. You can explore it in the new console and familiarize with it.

To migrate the metadata do the following:

- Retrieve the database root password

- Open a command prompt and execute:

```
- rcs-db-migrate -u root -p <password> -d localhost
```

If you want to check other options you can execute:

```
rcs-db-migrate --help
```

Once the metadata is migrated you are ready to make the full switch to daVinci. You don't need to migrate all the evidence to be ready to use the system. The evidence can be migrated later.

Is everything ok?

Login into the system. This time you will need an account that was active in the RCS 7 installation or if you use the 'admin' account, you have to insert the new password created during the daVinci installation. The migration of the metadata has overwritten the new admin just created.

Check that everything was migrated correctly and familiarize with the new interface and the new configuration for the agents.

Until you go live, you can always fallback to a RCS 7 or start from scratch with a new daVinci installation. You will not loose any data.

Ready to go live?

At this point you can migrate the frontend and start receiving the new evidence. See the next section for the frontend migration. Once the new Collector starts receiving data and storing it in the daVinci backend the new evidence will be available only in daVinci. There is no path backward to RCS 7 for that data.

5- Migrate Evidence

The evidence migration from RCS 7 to daVinci can take a considerable amount of time. All the old evidence must be converted into the new format and stored into the daVinci database. To ease this process the migration script can be used to migrate one activity at a time. If the migration process is interrupted for some reason, executing it again will restart from the last evidence migrated.

To get the list of operations ready to be migrated you can execute:

```
rcs-db-migrate -u root -p <password> -d localhost -L
```

Then you can start the evidence migration for each operation:

```
rcs-db-migrate -u root -p <password> -d localhost -l
<operation name>
```

Once the operation has been migrated you can iterate for all the remaining operations. The system is perfectly usable during the migration process. You can notice a slightly slowness since it is crunching a lot of evidence.

6- Uninstall RCS 7

Once all the evidence are migrated to the new RCS daVinci you can safely uninstall RCS 7.

If your system is connected to a NAS do the following:

- Uninstall RCS 7 from the windows control panel and choose the flag to NOT DELETE data

- Manually delete old unneeded files by running the script:

```
 rcs-remove-version-seven
```

- Unmount the C:\RCSDB directory

If RCS 7 was installed locally on your server:

- Uninstall RCS 7 from the windows control panel and choose to DELETE the data

FRONTEND

1- Uninstall ASP

Before uninstalling the ASP service you must be sure that all the pending evidence are flushed into the database.

In order to do this:

- Stop the RSS service; the agents will not be able to send new evidences

- Wait until RLD has processed the entire directory into C:\RCSASP\LOGREPO; each directory should have the enc and dec sub-directory empty.

- Uninstall RCSASP from the windows control panel

2- Install the Collector

If you installed the “All-in-one” RCS, after migrating the metadata from RCS 7, you need to execute this command:

```
rcs-collector-config -u <user> -p <password> -d <master CN> -t -s
```

to retrieve again the new server signature that has been changed during the migration of the metadata.

If you have chosen the distributed installation during the backend installation, execute the RCS installer and choose the "distributed installation" -> "Collector" and "Network Controller"

If you have multiple ASP servers, repeat the same procedure on each server but this time install only the "Collector".

There must be ONLY ONE "Network Controller" for each RCS installation.

3- Migrate the Anonymizers

If you have an anonymizing chain in front of the Collector, you need to update it in order to receive the data from the Agents.

Perform the following steps:

- *Go to the “system” section of the console and download the installer for the anonymizer*

- *Uninstall the old anonymizer. Remove the files in /opt and the services*

- *Execute the installer on each anonymizer*

- *Check in the monitor section that every anonymizer is green*

- *Apply the configuration to the whole topology*