Disaster Recovery Preparation for AD RMS

The three steps that you can do today that will allow you to recover from any AD Rights Management Server failure in the future:

- **Know your cluster key password and store it somewhere safe**
- **Export Trusted Publishing Domain**
- **Create database backups**

Know your Cluster Key Password and store it somewhere safe

If this is a new install, note the cluster key password and put it in a safe place.

If you inherited the server and the cluster key password isn't documented, you should change it to something known before backing everything up. To do this, go into the Active Directory Rights Management Services console under ServerName->Security Policies->Cluster Key Password. Choose the link to "Change Cluster Key Password".

Export the Trusted Publishing Domain

Saving a copy of the trusted publishing domain can be done from within the AD RMS administration console.

To export the trusted publishing domain

1. Open the AD RMS administration console.
2. In the console tree view, select **Trusted Publishing Domains**.
3. In the details pane on the right, select **Export Trusted Publishing Domain**.
   This will bring up the Export Trusted Publishing Domain box.
4. From the Export Trusted Publishing Domain dialog, click **Save As**.
   This will bring up the Export Trusted Publishing Domain File Save As box. On the left, select the folder where you want to save the trusted publishing domain.
5. Under File name enter a filename and make sure that **XML File (*.xml)** is selected for **Save As Type**.
6. Click **Save**.
   This will close the Export Trusted Publishing Domain As box.
7. From the Export Trusted Publishing Domain box, enter password in the **Password** box.
8. Enter password again in the **Confirm Password** box.
9. Click **Finish.**

Create a backup of the AD RMS database

AD RMS uses three databases in the database server, so it's a good idea to understand what they are for:

- The configuration database – The configuration database is a critical component of an AD RMS installation because it stores, shares, and retrieves all configuration data and other data that the service needs to manage account certification, licensing, and publishing services for a whole cluster.

- The directory services database contains information about users, identifiers (such as e-mail addresses), security ID (SID), group membership, and alternate identifiers. This information is a cache of directory services data.
- The logging database – This is all the historical data about client activity and license acquisition. For each root or licensing-only cluster, by default, AD RMS installs a logging database in the same database server instance that hosts the configuration database.

To create backups of the AD RMS databases

1. Log on to the SQL server.
2. Click **Start**, select **All Programs**, click **Microsoft SQL Server 2008** and select **SQL Server Management Studio**.
   This will bring up the Connect to Server dialog box. Ensure that the server name is correct and that authentication is set to use Windows Authentication.
3. Click **Connect**.
4. Expand the **Databases** node.
5. Right-click *DRMS_Config_rms_domain_com_443*, select **Tasks** and then select **Back Up**.
6. Click **Add** in the **Destination** section and select the location.
7. Click **OK** to finish the backup.
8. Repeat the above steps to backup logging and directory services cache database.

Note Even if you can't restore the database, you can recover your AD RMS infrastructure with the exported TPD and the Cluster Key Password, but a database restore is preferable.