Implementing AD RMS Infrastructure

Eli Chang

MSSA Cohort #2

Lab Summary 11

3/16/2020

Implementing AD RMS Infrastructure

The company wants to implement additional security for some documents from the Research department. The security team wants any users with reading access could modify and distribute them wherever they want to. The administrators should plan and implement the AD RMS solution to provide the level of protection. The AD RMS solution has many options depending on business and security requirements.

AD RMS

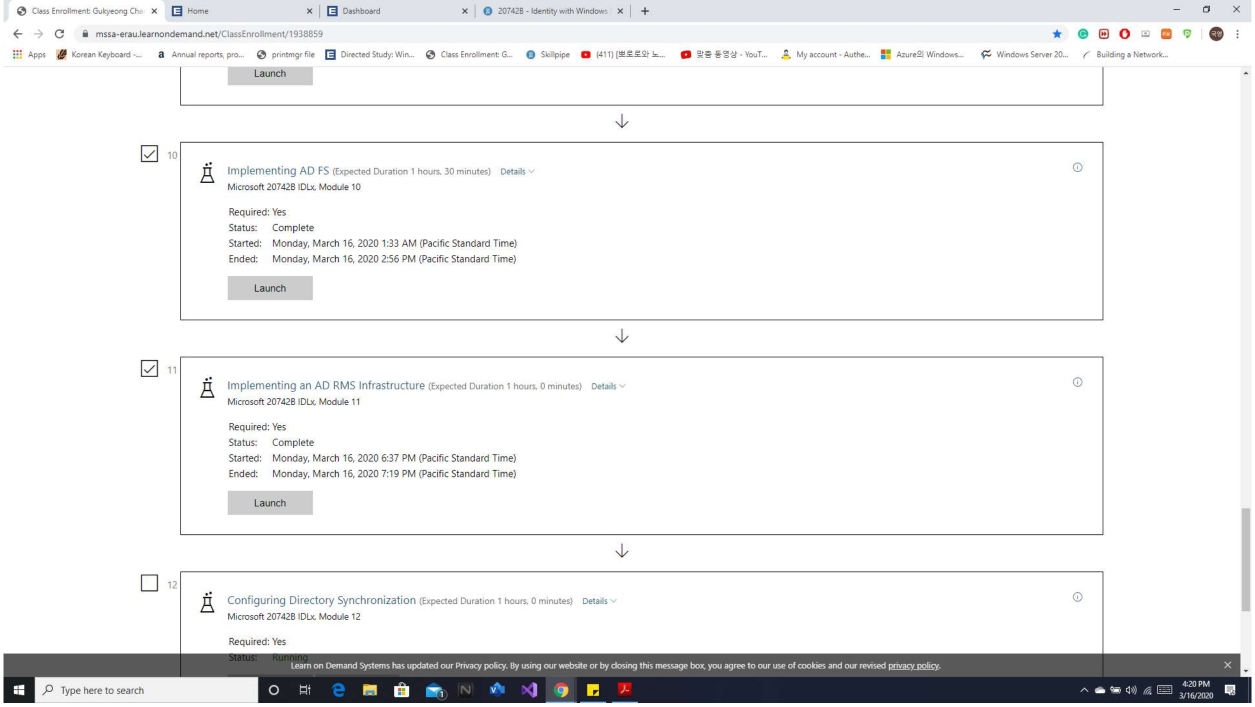
The Active Directory Rights Management Services (AD RMS) is an information protection technology in Windows Server 2016 to minimize the possibility of data leakage. This service helps protect data in transit and at rest. The AD RMS would help control the distribution of critical information so that it can prevent access to documents, uses action-based permissions, and prevent confidential emails that leave from the company. There are four different components in AD RMS: AD RMS cluster, AD RMS server, AD RMS client, and AD RMS-enabled applications. The AD RMS cluster should be created as the first AD RMS server, which must be a member of an AD DS domain. The AD RMS client allows the AD RMS-enabled applications to enforce the functionality. It means that the AD RMS-enabled applications cannot interact with AD RMS content without the AD RMS client.

AD RMS Templates

The AD RMS templates are also known as rights policy templates, which allows the users to configure standard AD RMS policies across the company. The rights policy templates could be stored in the AD RMS database as the XML format. There are thirteen different rights supported by AD RMS: full control (giving a full control), view (giving the ability to view), edit (allowing to modify), save (allowing to save), export (allowing save as function), print (allowing to be printed), forward (allowing recipients to forward the message), reply (allowing the recipients to reply), reply all (allowing recipients to reply all), extract (allowing to copy data), allow macros (utilizing macros), view rights (viewing te assigned rights), and edit rights (modifying the assigned rights). Also, AD RMS templates would configure the properties of content expiration, license expiration, enabling to view protected content, revocation policy, and requiring a new use license.

AD RMS Super User Group

The members of the super users group have full owner rights in all use licenses issued by the AD RMS cluster. This feature is a particular role, which means it is not configured by default. With this feature, the AD RMS-protected data or content can be recovered. The super user group can be enabled in the security policies under the AD RMS console.



☑ 10

Implementing AD FS (Expected Duration 1 hours, 30 minutes) Details
Microsoft 20742B IDLx, Module 10

Required: Yes
Status: Complete
Started: Monday, March 16, 2020 1:33 AM (Pacific Standard Time)
Ended: Monday, March 16, 2020 2:56 PM (Pacific Standard Time)

☑ 11

Implementing an AD RMS Infrastructure (Expected Duration 1 hours, 0 minutes) Details
Microsoft 20742B IDLx, Module 11

Required: Yes
Status: Complete
Started: Monday, March 16, 2020 6:37 PM (Pacific Standard Time)
Ended: Monday, March 16, 2020 7:19 PM (Pacific Standard Time)

☐ 12

Configuring Directory Synchronization (Expected Duration 1 hours, 0 minutes) Details
Microsoft 20742B IDLx, Module 12

Required: Yes
Status: Running

Learn on Demand Systems has updated our Privacy policy. By using our website or by closing this message box, you agree to our use of cookies and our revised privacy policy.

.. +