TOPIC: IMPLEMENTING AND ADMINISTERING AD RMS

Objective:

Implement Active Directory Rights Management Services (AD RMS) to protect sensitive documents within an Active Directory environment, configure and distribute rights policy templates, and validate secure access for authorized users and groups.20742A-ENU-LAB.pdf

---

Prerequisites:

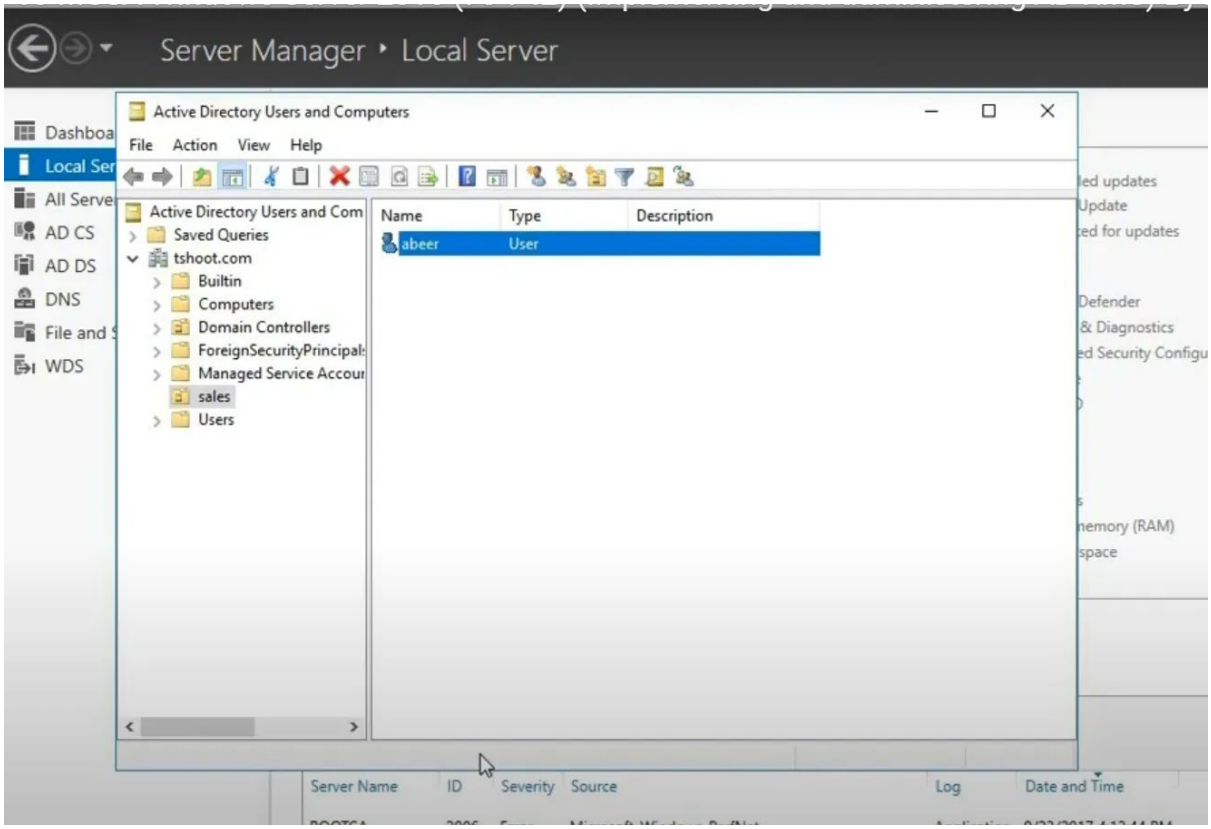
- VMware Workstation with virtual network configured
- 6 virtual machines: LON-DC1 (WS 2016 Datacenter), LON-SVR1 (WS 2016 Standard), LON-SVR2 (WS 2016 Standard), LON-CORE (WS 2016 CLI), LON-CL1 (Windows 10 Pro), LON-RHEL (RHEL 10)
- All Windows VMs (except LON-RHEL) are members of AD DS domain RPSLAB.COM
- Administrative access on all Windows systems
- Screenshots capability enabled.20742A-ENU-LAB.pdf

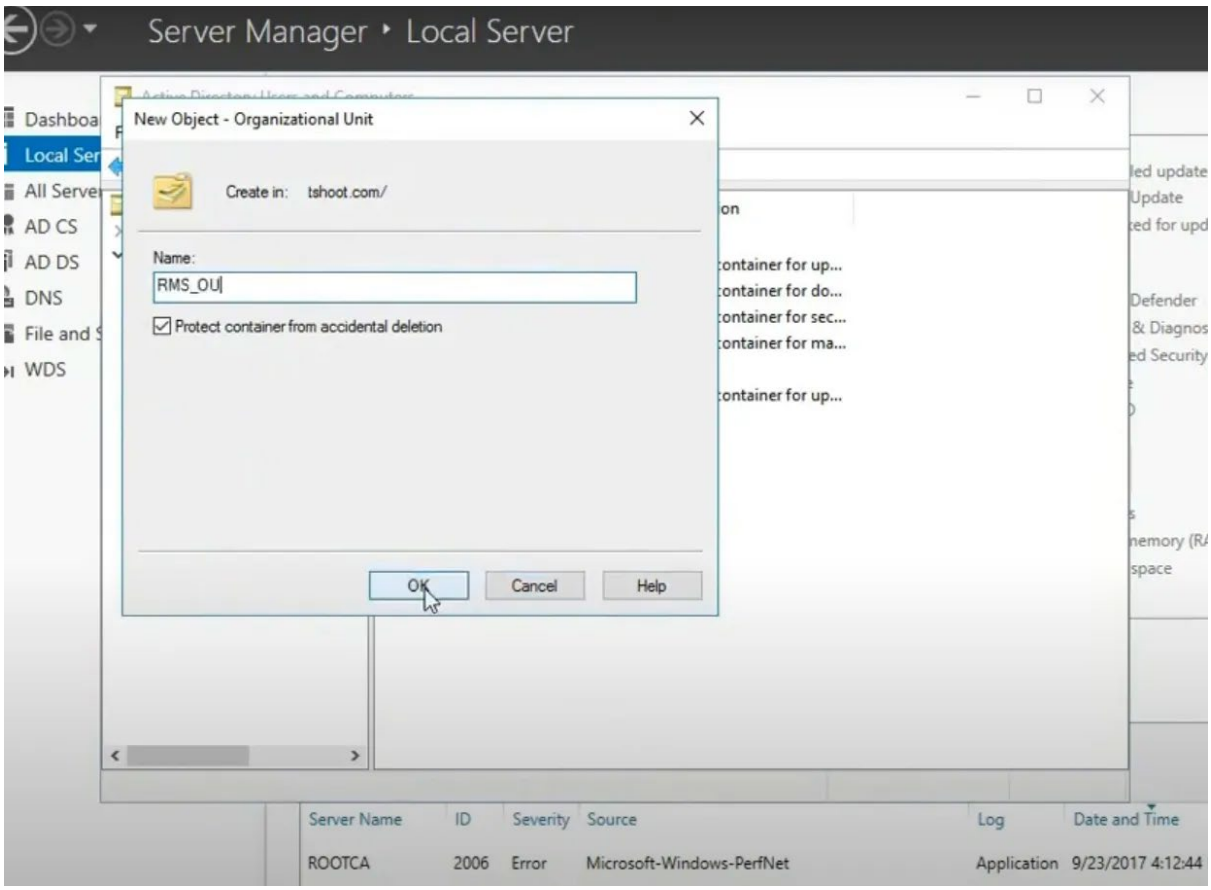
Exercise 1: Installing and Configuring AD RMS

Procedure:

Topic: Configure DNS and the AD RMS Service Accounts

1. Log in to **LON-DC1** as domain administrator.
2. Create a new Organizational Unit (OU) named **Service Accounts** in AD DS.
3. Create a user account, e.g., ADRMSSVC, in the Service Accounts OU, set password and disable expiry.
4. Create two groups: ADRMS_SuperUsers and Executives, add relevant users to Executives.
5. Create DNS 'A' record for AD RMS server (adrms.rpslab.com) pointed to LON-SVR1's IP.20742A-ENU-LAB.pdf

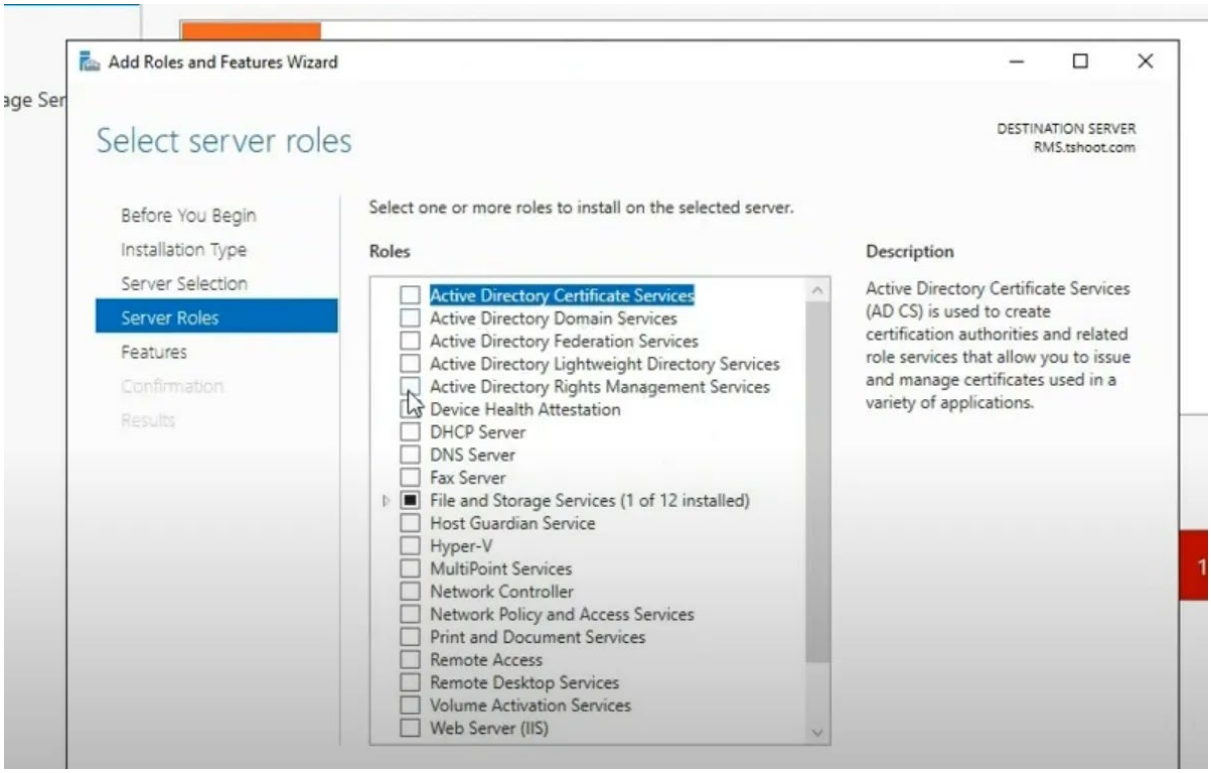


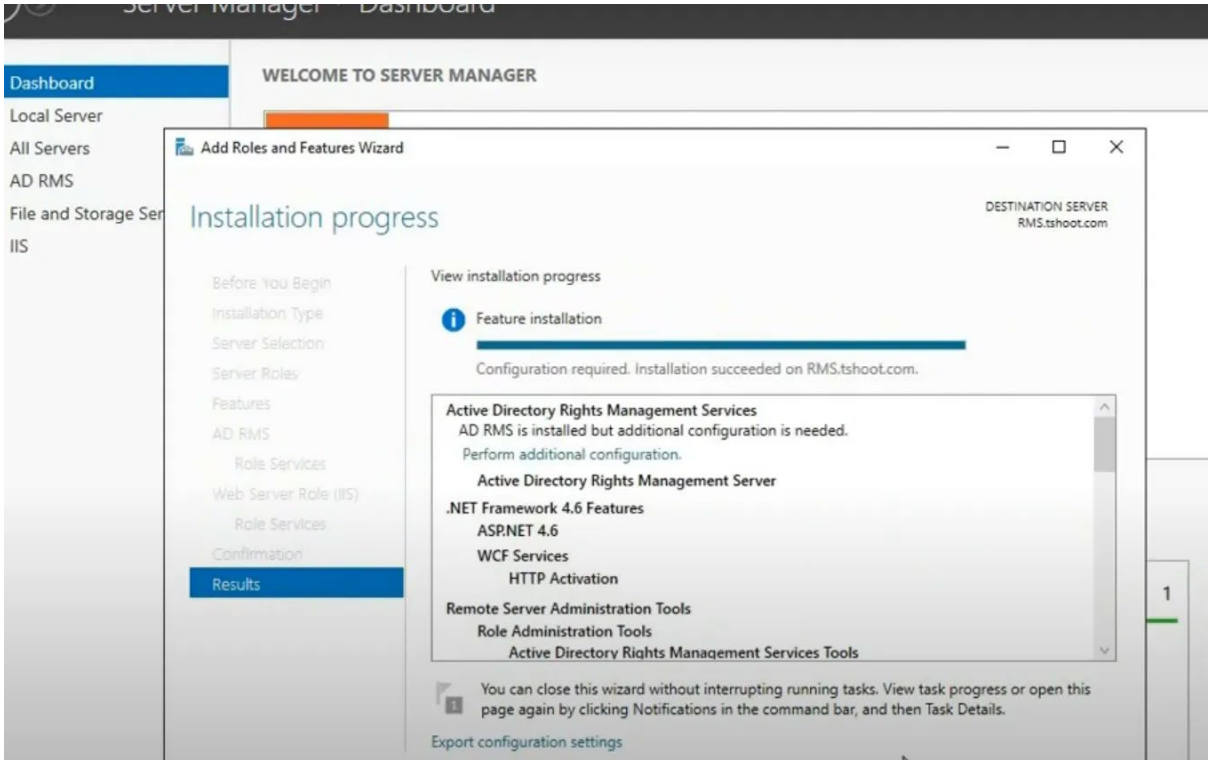


Topic: Install and Configure the AD RMS Server Role

1. Log in to **LON-SVR1** as domain administrator.

2. Open Server Manager, Add Roles and Features > Active Directory Rights Management Services.
3. Complete the role installation.
4. Configure AD RMS cluster: New root cluster, Windows Internal Database, specify ADRMSSVC as service account.
5. Select Cryptographic Mode 2, use centrally managed key storage (set password), bind to Default Web Site, configure cluster address as adrms.rpslab.com.
6. Register Service Connection Point (SCP), finish installation.
7. Enable Anonymous Authentication in IIS for _wmcs and licensing paths (for lab purposes).20742A-ENU-LAB.pdf





Topic: Configure the AD RMS Super Users Group

1. Open AD RMS console on LON-SVR1, expand Security Policies.
2. Enable Super Users group, specify ADRMS_SuperUsers@rpslab.com as group.20742A-ENU-LAB.pdf

Conclusion:

After completing these steps, AD RMS is installed, initialized, and configured in your test domain. The Super Users group is enabled for document recovery and auditing.20742A-ENU-LAB.pdf

---

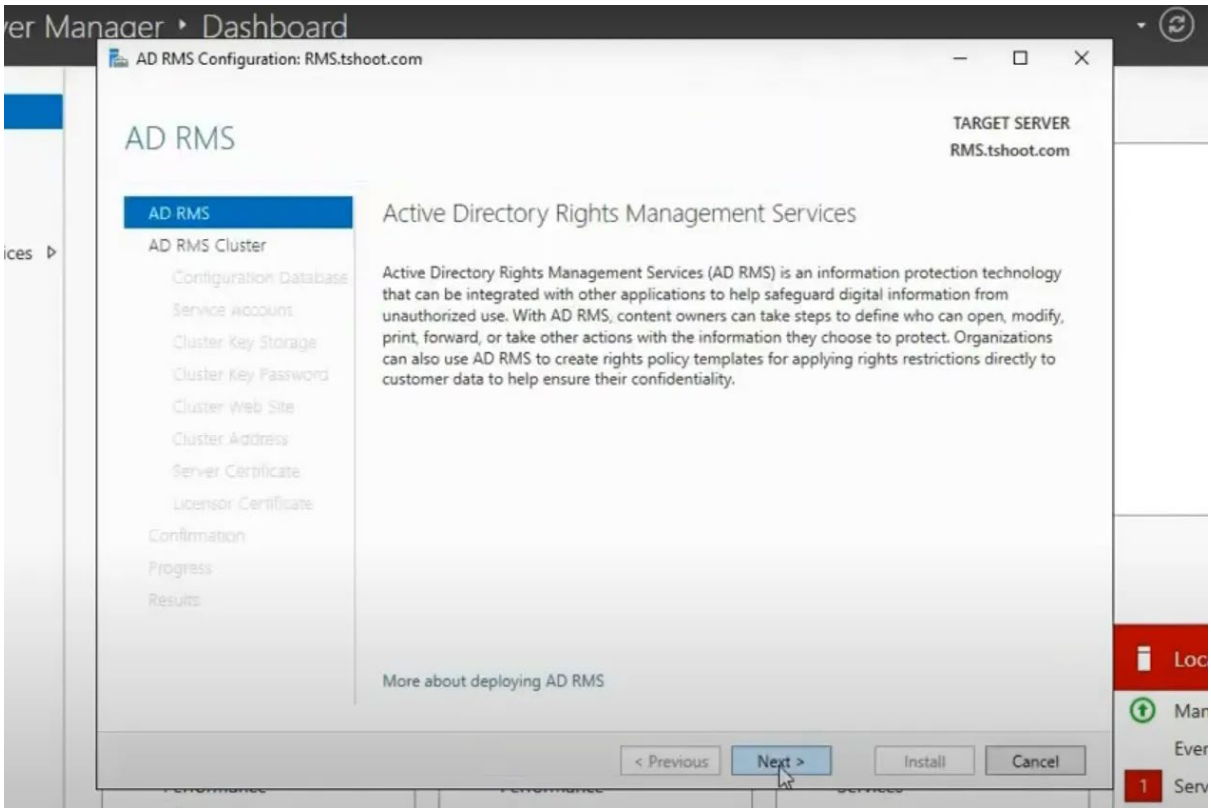
Exercise 2: Configuring AD RMS Templates

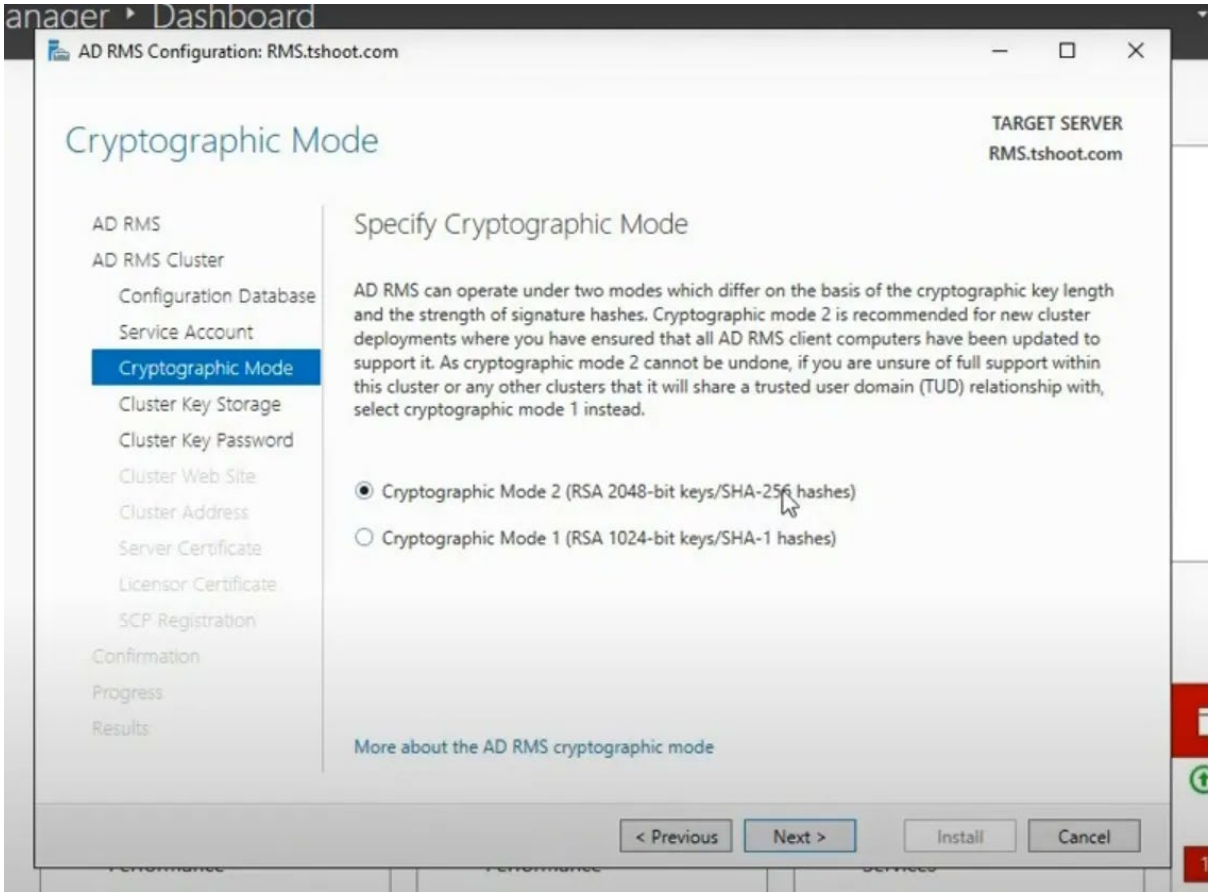
Procedure:

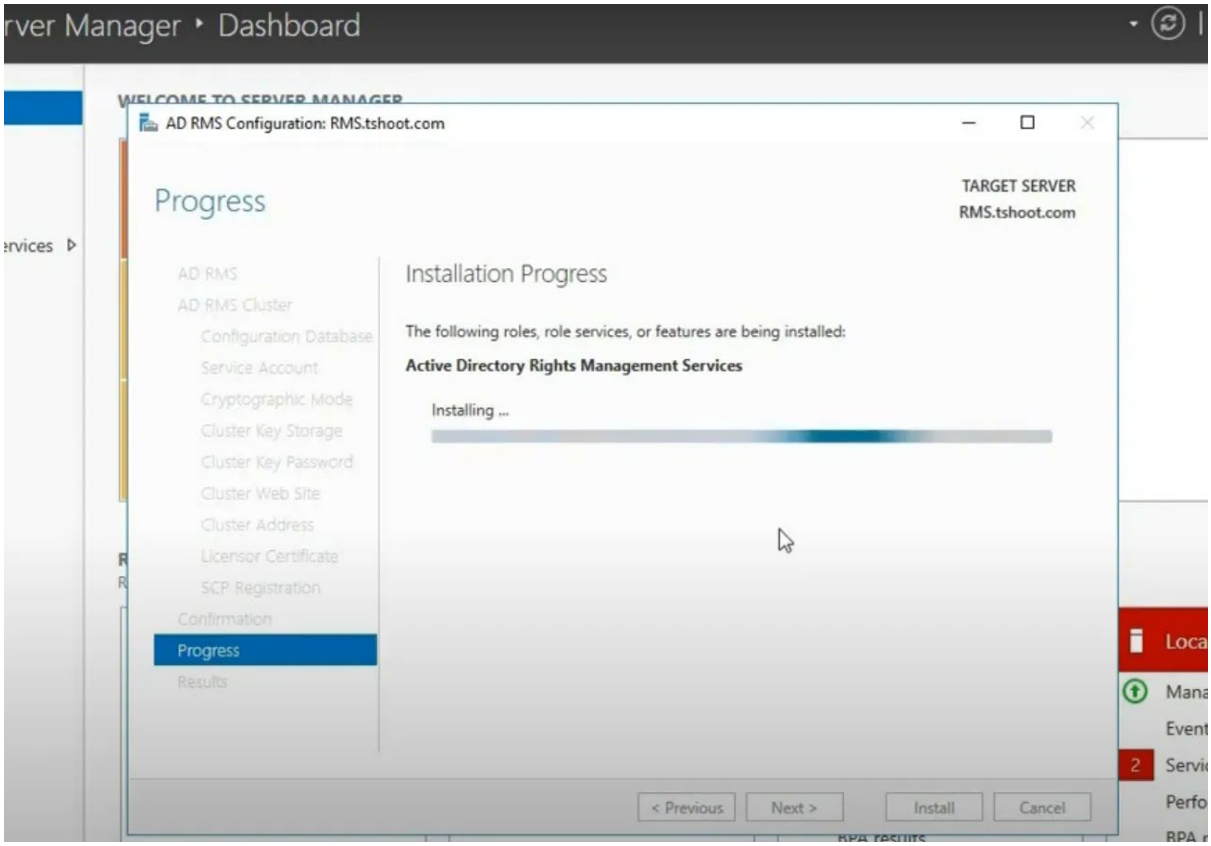
Topic: Configure a New Rights Policy Template

1. In AD RMS console, create a new Distributed Rights Policy Template.
2. Set language to English, name to ReadOnly, description to “Read-only access. No copy or print.”
3. Add Executives group, grant View right.
4. Set content and license expiration to 7 days.

5. Enable “Require new use license every time content is consumed”.20742A-ENU-LAB.pdf





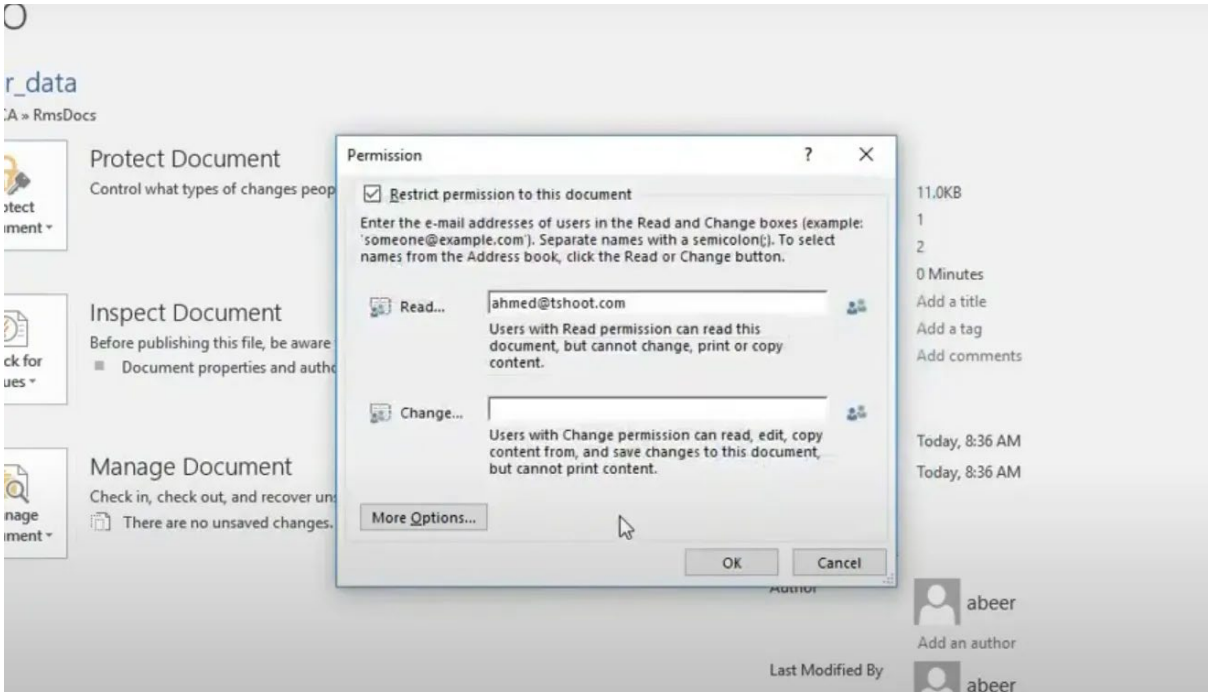


Topic: Configure the Rights Policy Template Distribution

1. On LON-SVR1, open PowerShell, create directories: c:\rmstemplates and c:\docshare.
2. Create SMB shares: RMSTEMPLATES (for ADRMSSVC – full access), docshare (for Everyone).
3. Enable export and set rights policy templates location to \LON-SVR1\RMSTEMPLATES.
4. Confirm ReadOnly.xml template is exported.20742A-ENU-LAB.pdf

Topic: Configure Exclusion Policy

1. In AD RMS console, open Exclusion Policies.
2. Exclude Powerpnt.exe (Microsoft PowerPoint) version 14.0.0.0–16.0.0.0 from protection.20742A-ENU-LAB.pdf



Conclusion:

AD RMS templates are created, exported, and distributed, enforcing targeted document protection policies and exclusion rules as required for RPSLAB.COM.20742A-ENU-LAB.pdf

---

Exercise 3: Using AD RMS on Clients

Procedure:

Topic: Create a Rights-Protected Document

1. On **LON-CL1** (Windows 10), sign in as an Executive group member.
2. Add adrms.rpslab.com to Local Intranet zone in Internet Options for SSO.
3. Open Word 2016, create and edit a confidential document.
4. Apply ReadOnly protection using the new RMS template.
5. Save document to \LON-SVR1\docshare as “Executives Only.docx”.20742A-ENU-LAB.pdf

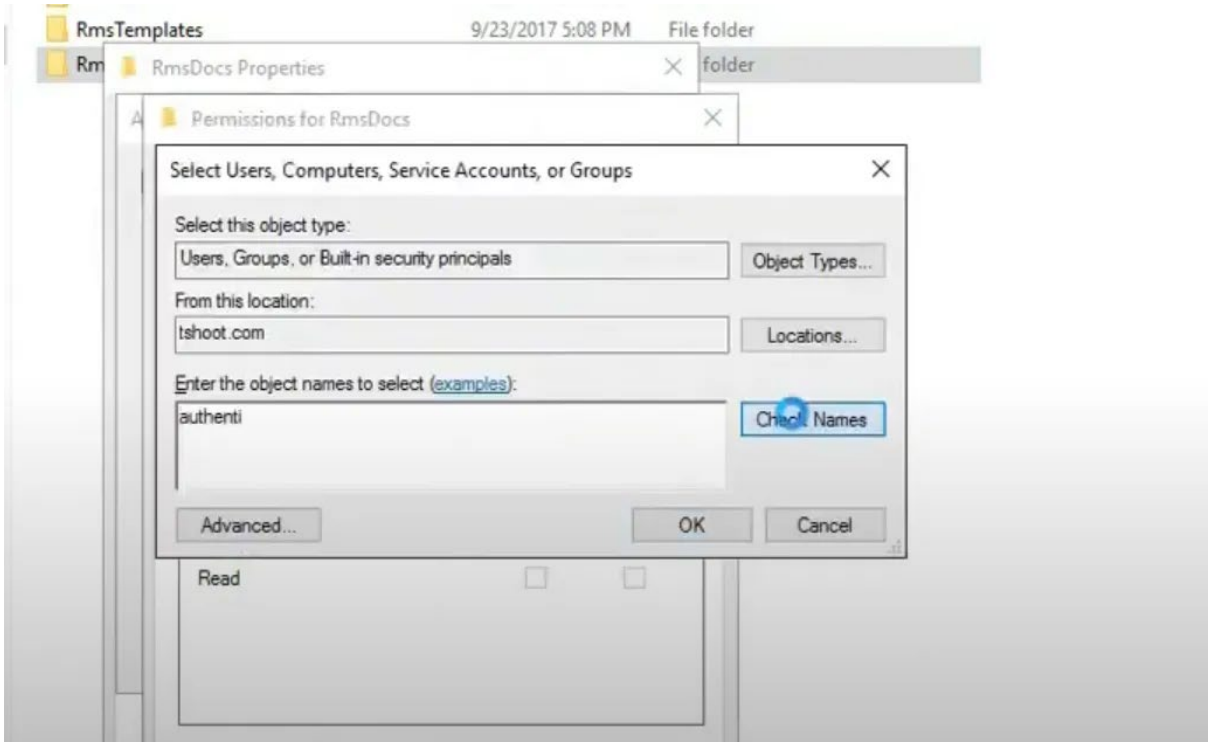
Topic: Verify Internal Access as Authorized User

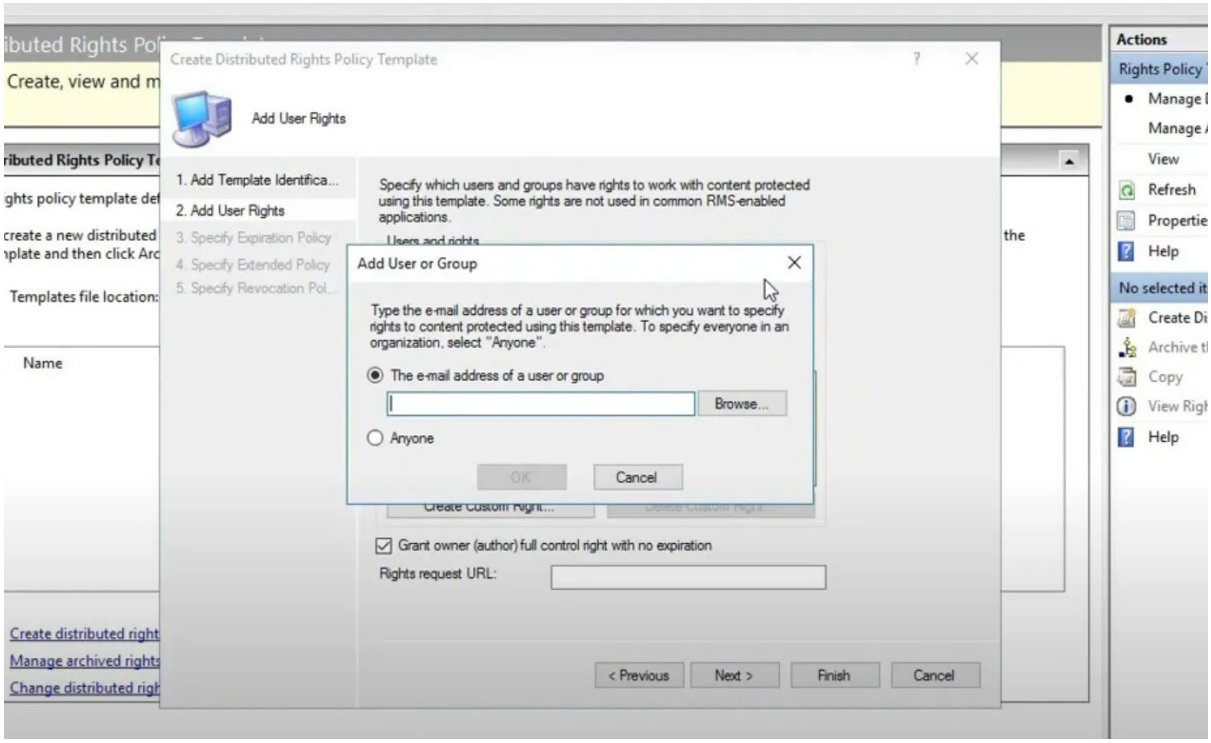
1. Sign in as another Executive user on LON-CL1.
2. Access \LON-SVR1\docshare and open the protected document.

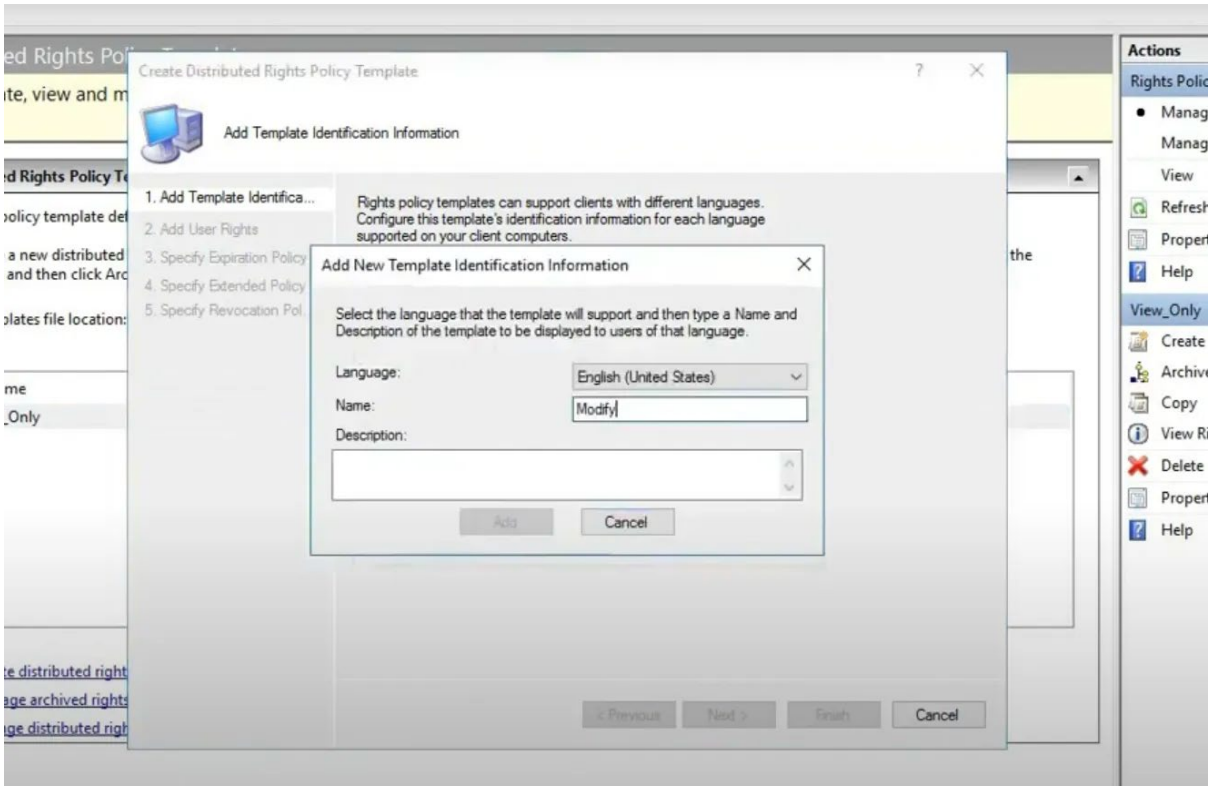
3. Verify inability to edit, copy, or print; confirm View permission only.20742A-ENU-LAB.pdf

Topic: Open the Document as Unauthorized User

1. Sign in as an unauthorized user on LON-CL1.
2. Attempt to open the ReadOnly protected document; confirm access is denied.20742A-ENU-LAB.pdf







Conclusion:

AD RMS ensures only authorized group members can access and view protected documents. Unauthorized users are successfully blocked, validating secure information sharing.20742A-ENU-LAB.pdf

---

Overall Conclusion:

Active Directory Rights Management Services (AD RMS) was successfully deployed in the RPSLAB.COM domain. The configuration included creation of service accounts, rights policy templates, exclusion policies, and validation of access controls. Screenshots should be provided at each key step for evidence in documentation. This module proves AD RMS as an effective solution for safeguarding sensitive corporate information and controlling document access using Windows Server 2016 technology.20742A-ENU-LAB.pdf