

Lab 9: Implement Identity Solutions

By: Ethan Holmes

Table of Contents

Introduction	3
Activity 9-1: Resetting Your Virtual Environment.....	3
Activity 9-2: Preparing for AD FS Deployment	3
Activity 9-3: Installing the AD FS Role	4
Activity 9-4: Installing the AD RMS role	5
Activity 9-5: Creating a Rights Policy Template	7
Activity 9-6: Exploring the Active Directory Rights Management Console	10
Conclusion	12

Introduction

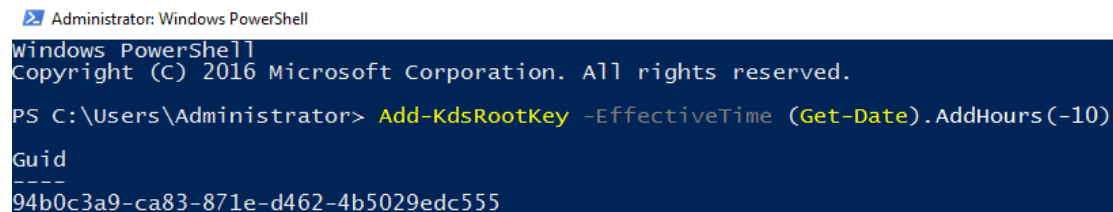
In this lab, we will be setting up and implementing an Active Directory Federation Service into our domain environment, we will also be creating a Rights Policy Template to use.

Activity 9-1: Resetting Your Virtual Environment

For this step, we will revert our VMs back to their initial config snapshot

Activity 9-2: Preparing for AD FS Deployment

For this activity, we can start with a powershell command to generate a managed service account password



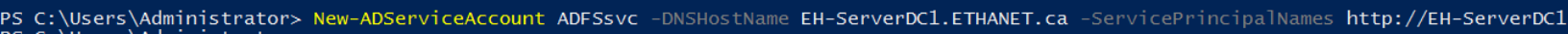
```
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-KdsRootKey -EffectiveTime (Get-Date).AddHours(-10)

Guid
----
94b0c3a9-ca83-871e-d462-4b5029edc555
```

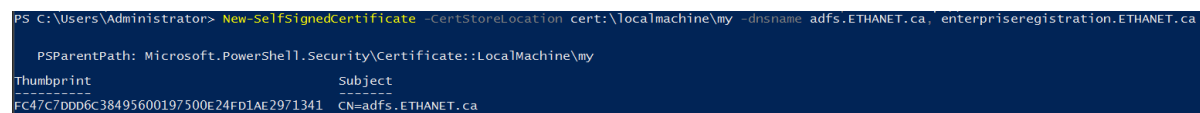
Figure 1: Create a service account password

After this, we can then create a self-signed certificate and the service account themselves



```
PS C:\Users\Administrator> New-ADServiceAccount ADFSsvc -DNSHostName EH-ServerDC1.ETHANET.ca -ServicePrincipalNames http://EH-ServerDC1
```

Figure 2: Create a ADFS account



```
PS C:\Users\Administrator> New-SelfSignedCertificate -CertStoreLocation cert:\localmachine\my -dnsname adfs.ETHANET.ca, enterpriseregistration.ETHANET.ca

PSParentPath: Microsoft.PowerShell.Security\Certificate::LocalMachine\my
Thumbprint           Subject
-----
FC47C7DD06C38495600197500E24FD1AE2971341  CN=adfs.ETHANET.ca
```

Figure 3: Self-Signed certificate

Activity 9-3: Installing the AD FS Role

In this portion of the lab, we will be installing the AD FS role and configuring it.

After installing the AD FS role on Server Manager, we can move on to the AD FS Config wizard, we can accept the defaults until “Specify Service Properties” where we will then add the self-signed certificate that we created earlier as well as a display name for logins.

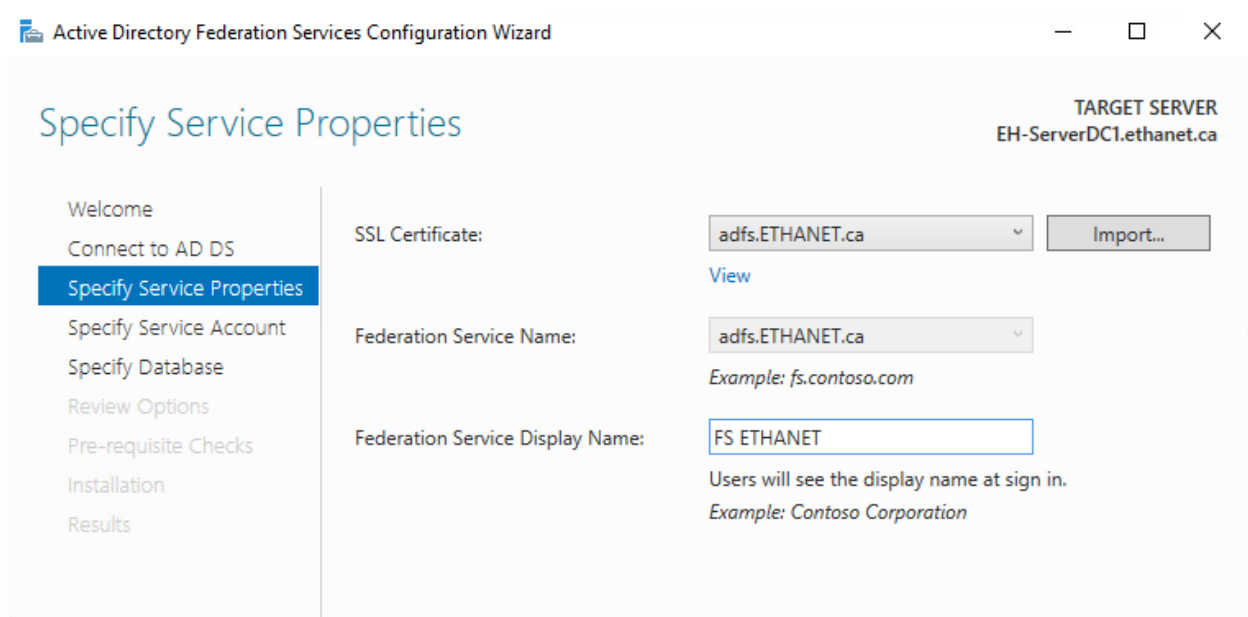


Figure 4: Creating the ADFS by adding the cert

We can then add the user that we created earlier (ADFSsvc) as the user account for the AD FS service, and then we can create a new Database using the Windows Internal Database

We can then complete the installation of the AD FS from that point forward.

Activity 9-4: Installing the AD RMS role

After installing the AD RMS role on our machines, we can then configure it

On the configuration database we can select the “Use Windows Internal Database on this server” and on the following page for “Specify Service Account”

We can then specify domuser1 as our AD RMS user account for communication

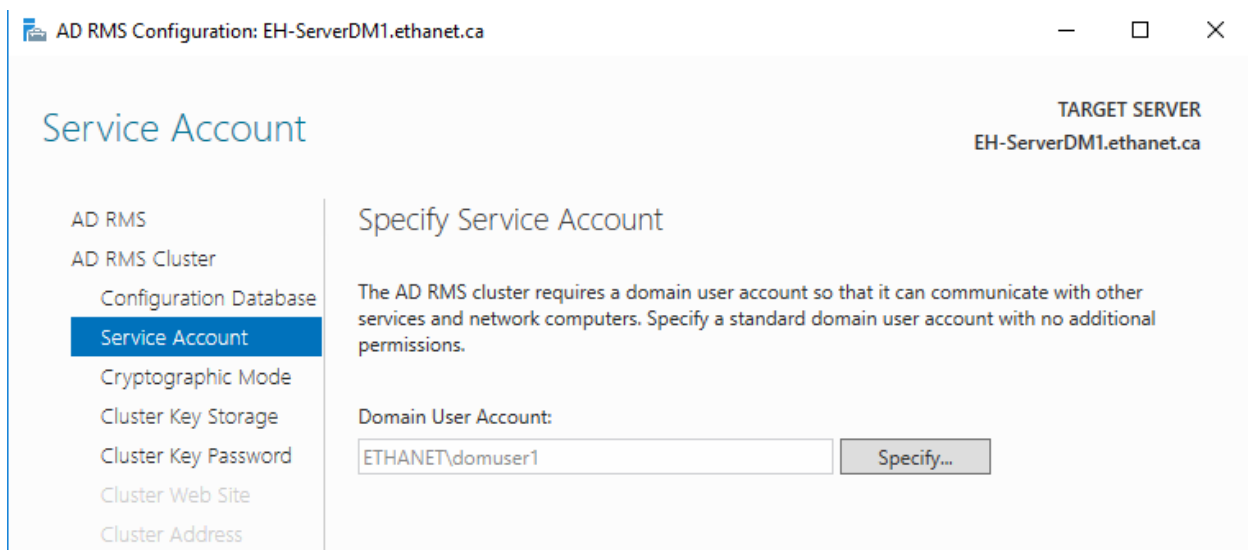


Figure 5: Selecting the service account to communicate

Next, we can then create our FQDN using the certificate we created earlier

Cluster Address

AD RMS

AD RMS Cluster

Configuration Database

Service Account

Cryptographic Mode

Cluster Key Storage

Cluster Key Password

Cluster Web Site

Cluster Address

Server Certificate

Licensor Certificate

SCP Registration

Confirmation

Progress

Specify Cluster Address

A cluster address makes it possible for AD RMS clients to communicate with this cluster over the network. We recommend that you configure AD RMS to use the Secure Sockets Layer (SSL) protocol to encrypt network traffic between AD RMS clients and this cluster. You must use an SSL-encrypted connection if you intend to federate this cluster.

Connection Type:

☒ Use an SSL-encrypted connection (https://)

☐ Use an unencrypted connection (http://)

Fully-Qualified Domain Name: Port:

i You cannot change this address or port number after AD RMS is installed and configured.

Figure 6: Creating the FQDN for communication

The server authentication screen that we will see next, we should see our SSL certificates, however, we will want to select the “Create a self-signed certificate for SSL Encryption”

Server Certificate

AD RMS

AD RMS Cluster

Configuration Database

Service Account

Cryptographic Mode

Cluster Key Storage

Cluster Key Password

Cluster Web Site

Cluster Address

Server Certificate

Licensor Certificate

SCP Registration

Confirmation

Choose a Server Authentication Certificate

When communicating with clients, AD RMS can use Secure Sockets Layer (SSL) to encrypt network traffic. For production deployments, choose an existing SSL certificate whose subject name matches the host name of the cluster. For test deployments, you can create and use a self-signed certificate instead.

☒ Choose an existing certificate for SSL encryption (recommended)

Issued To	Issued By	Expiration Date
EH-ServerDM1.ETHANET.ca	ethanet-EH-SERVERDM1-CA	2024-11-01
ethanet-EH-SERVERDM1-CA	ethanet-EH-SERVERDM1-CA	2027-11-02

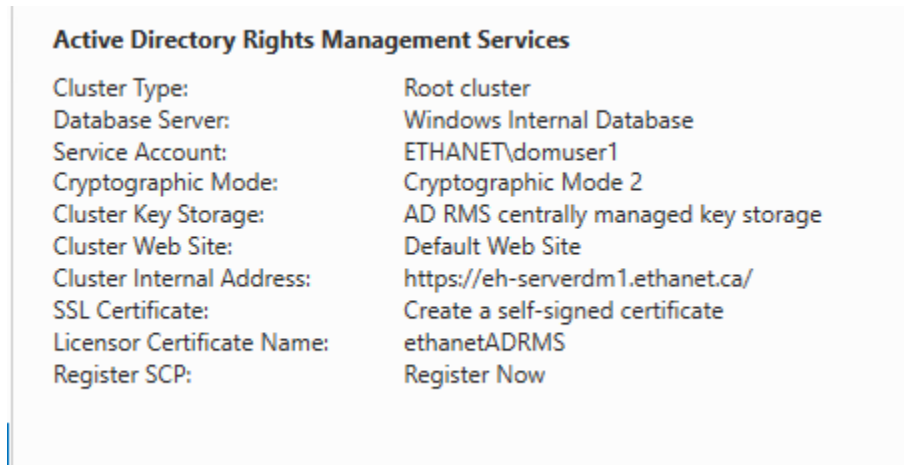
☐ Create a self-signed certificate for SSL encryption

☐ Choose a certificate for SSL encryption later

Properties Refresh

Figure 7: Creating a new self-signed certificate

At the creation page, we should have something that looks like this



The screenshot shows the 'Active Directory Rights Management Services' configuration page. It lists various settings for a root cluster, including the database server, service account, cryptographic mode, key storage, web site, internal address, SSL certificate, licensor certificate name, and the option to register the SCP.

Active Directory Rights Management Services	
Cluster Type:	Root cluster
Database Server:	Windows Internal Database
Service Account:	ETHANET\domuser1
Cryptographic Mode:	Cryptographic Mode 2
Cluster Key Storage:	AD RMS centrally managed key storage
Cluster Web Site:	Default Web Site
Cluster Internal Address:	https://eh-serverdm1.ethanet.ca/
SSL Certificate:	Create a self-signed certificate
Licensor Certificate Name:	ethanetADRMS
Register SCP:	Register Now

Figure 8: Final settings for the AD RMS

Activity 9-5: Creating a Rights Policy Template

In this activity, we will create a rights policy template

In the AD RMS console, we can click “Rights Policy Templates” and then, “Create Distributed Rights Policy Template”

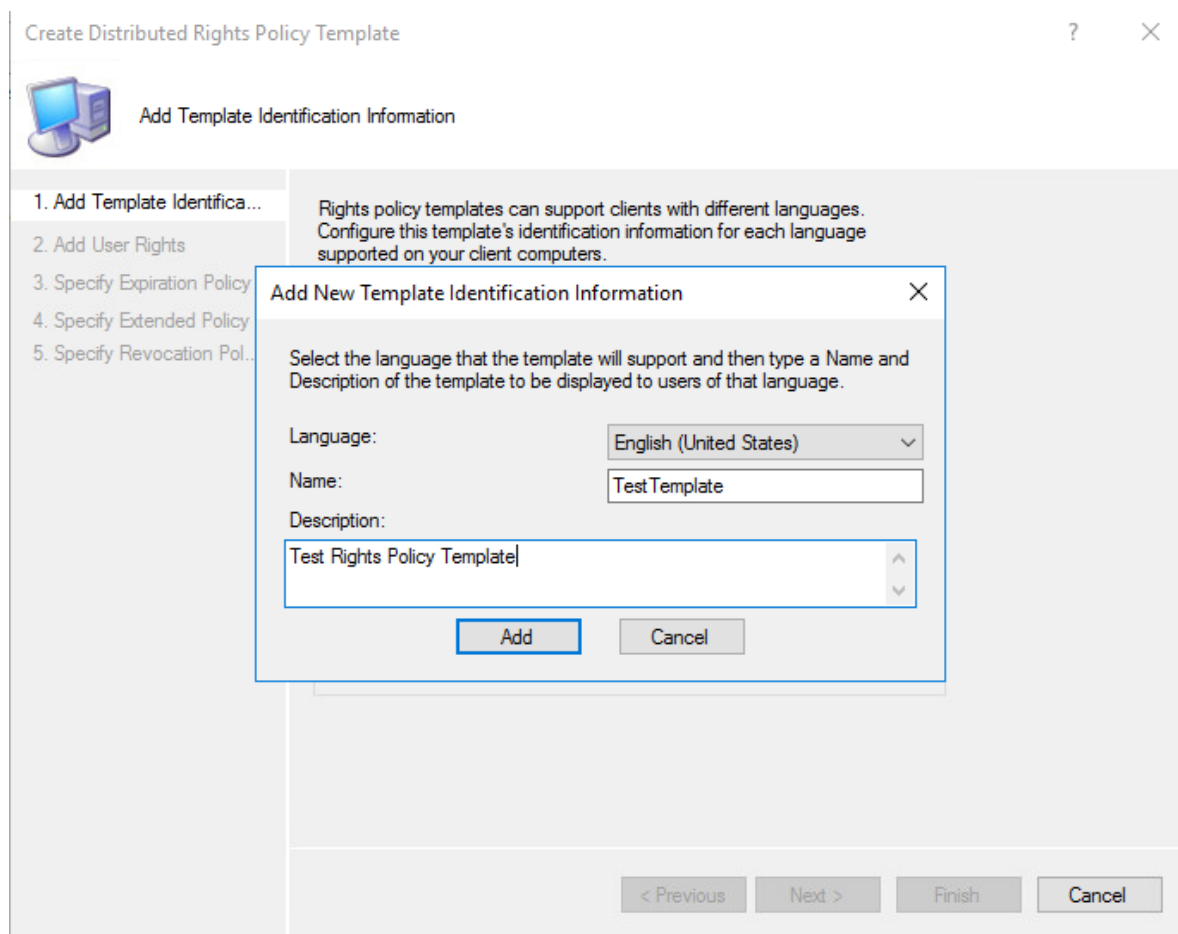


Figure 9: Creating the policy

In the User Rights section, we can select Anyone as our user

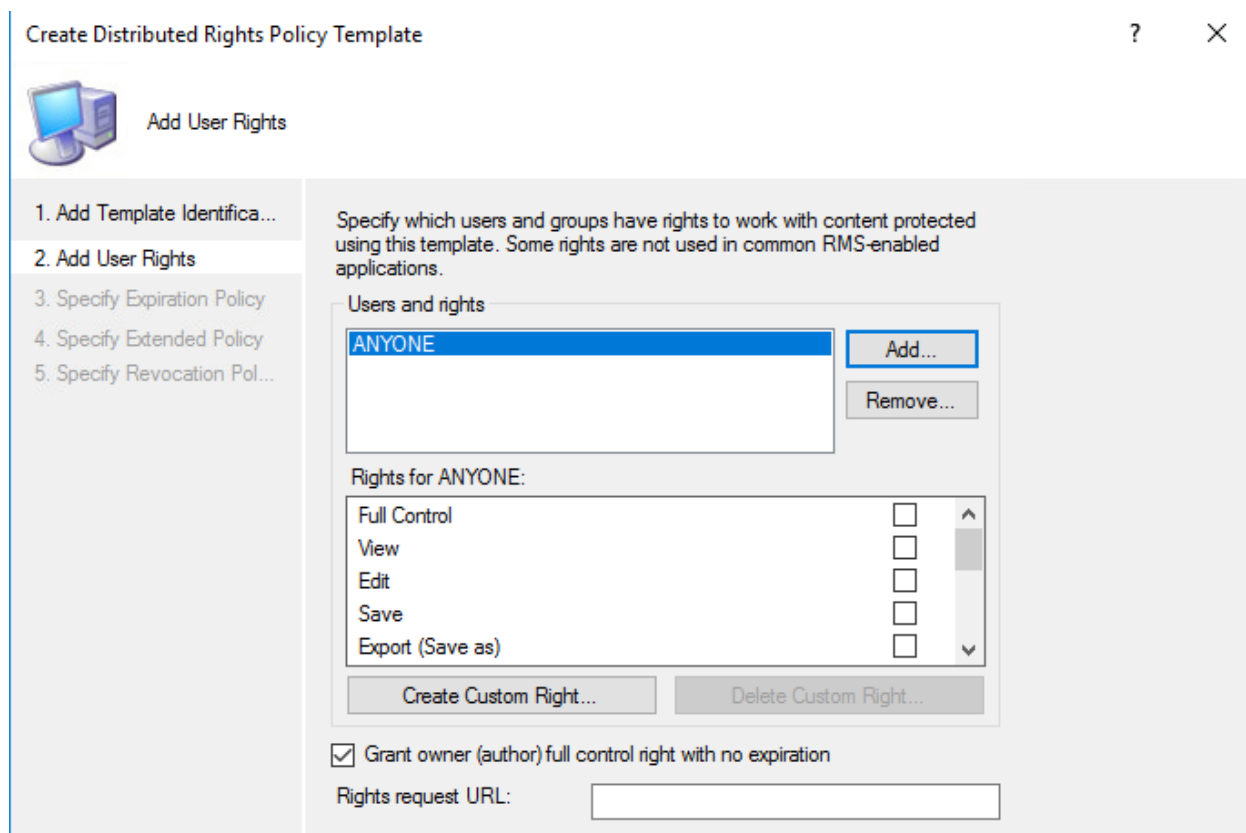


Figure 10: Using the "Anyone" group to create the template

In the Expiration Policy, we can set the expiration date for the policy to be 10 days from today's date. We now have our completed template.

Activity 9-6: Exploring the Active Directory Rights Management Console

In this activity, we will just be exploring the AD rights management console.

In the Console, we can select the Trust Policies and click the “Manage Trusted User Domains” and from here select “Export Trusted User Domains” where we can export a binary file

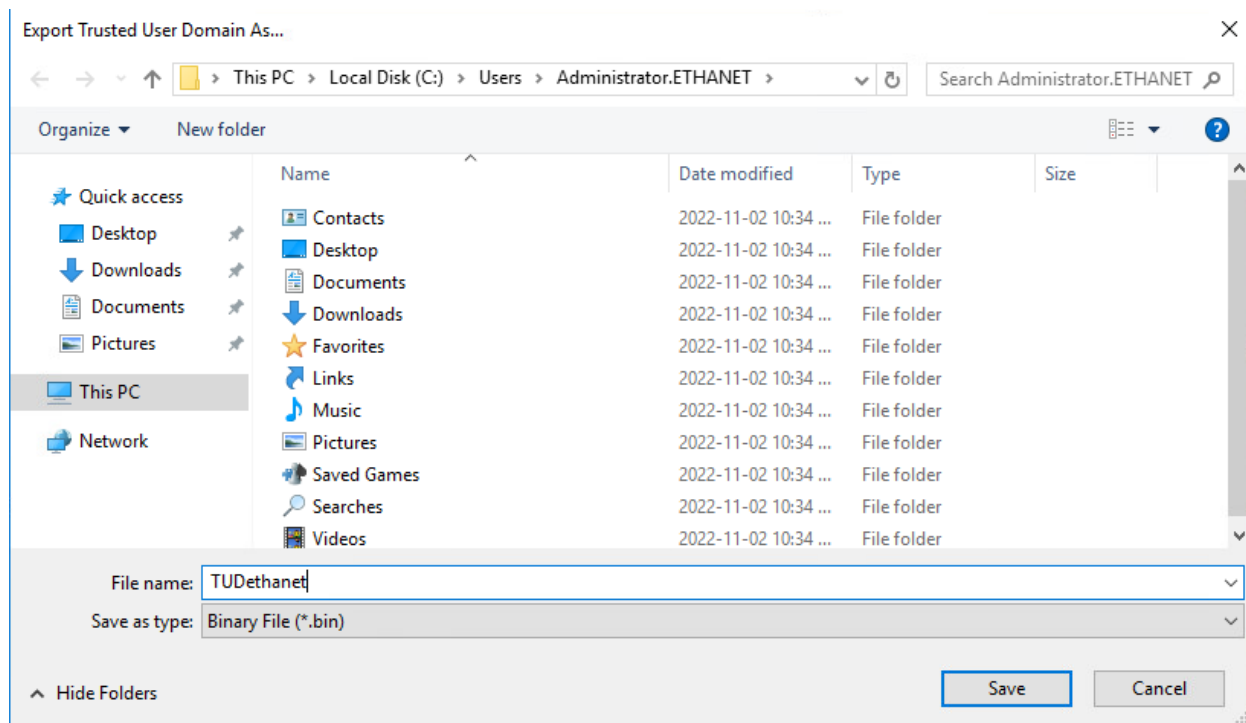


Figure 11: Exporting the Trusted Users Domain

We can then import this file with the “Import Trusted User Domain” option

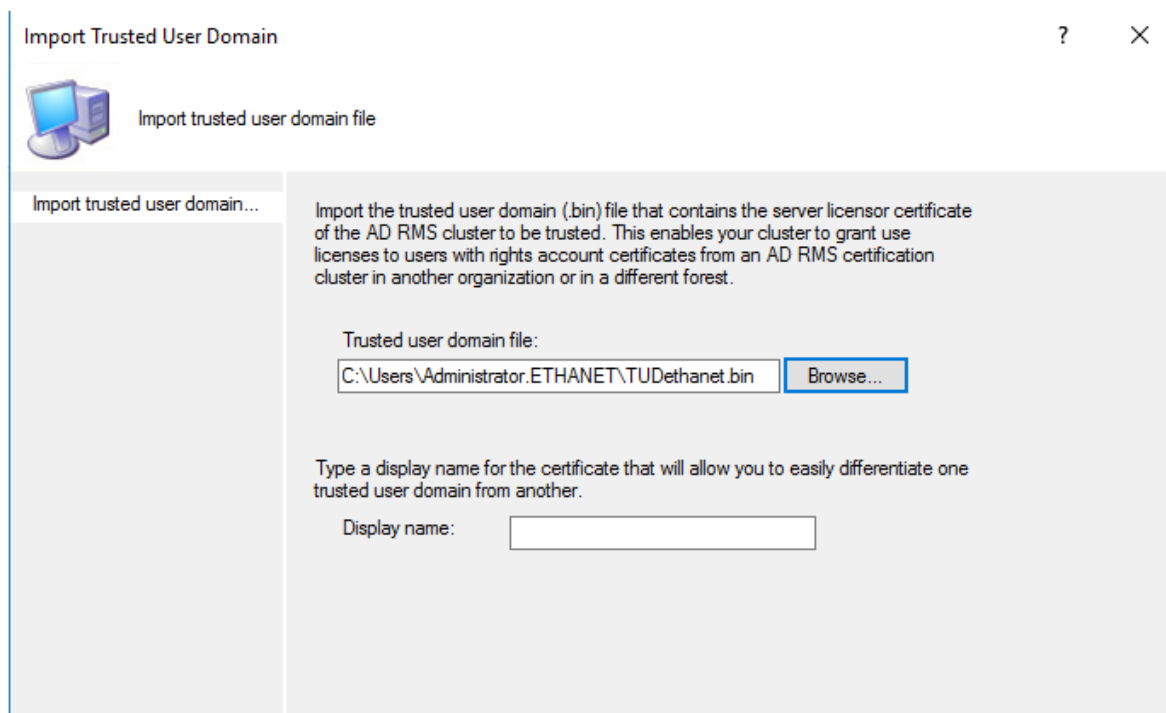


Figure 12: Importing the Trusted User Domain

Under “Trusted Publishing Domains” we can do similar actions

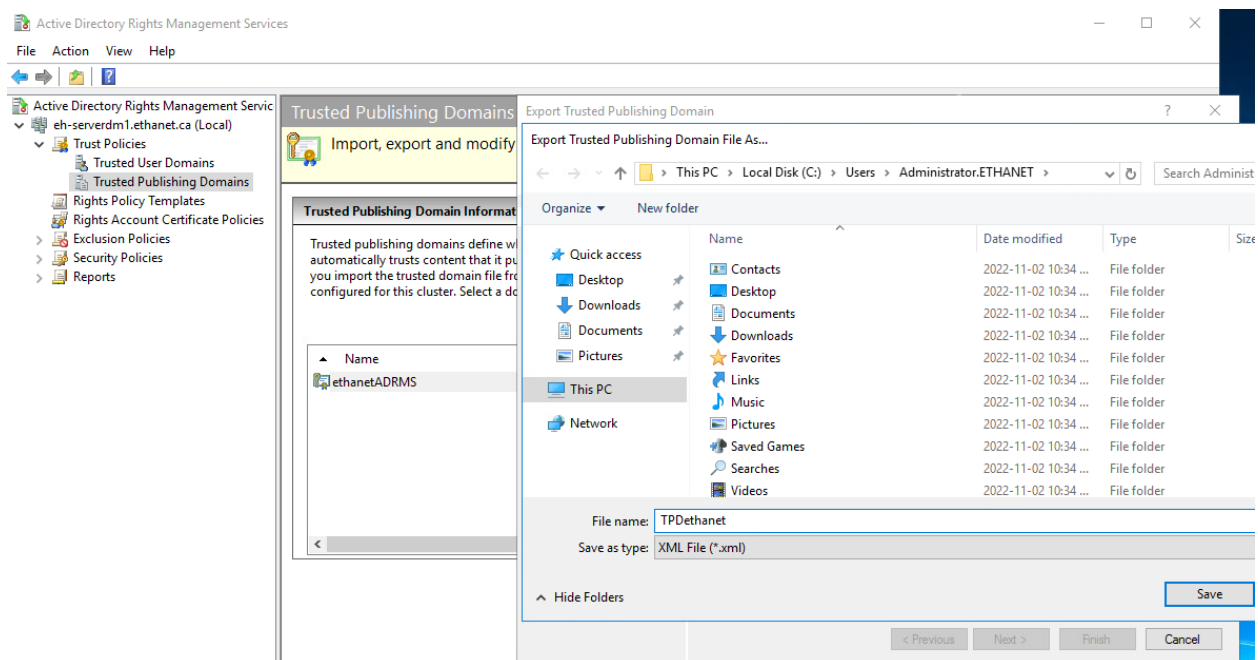


Figure 13: Exporting a trusted publisher

User Exclusion Policies which prevent user accounts from Obtaining use licenses and finally we can reset password for AD RMS cluster keys

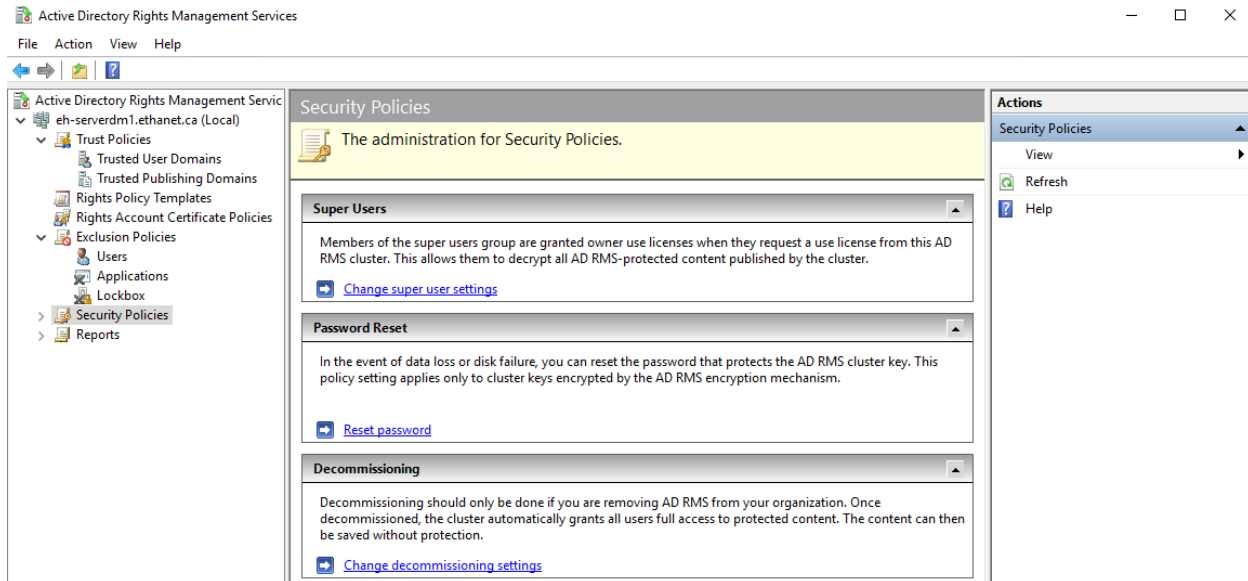


Figure 14: Security Policies available

Conclusion

In this lab, I learned how to set up AD RMS and AD FS and learned how they can be very useful and helpful for setting up one-way trusts for applications on domains.

