

CYB 300 Module Four Lab Worksheet Two

Andree Salvo

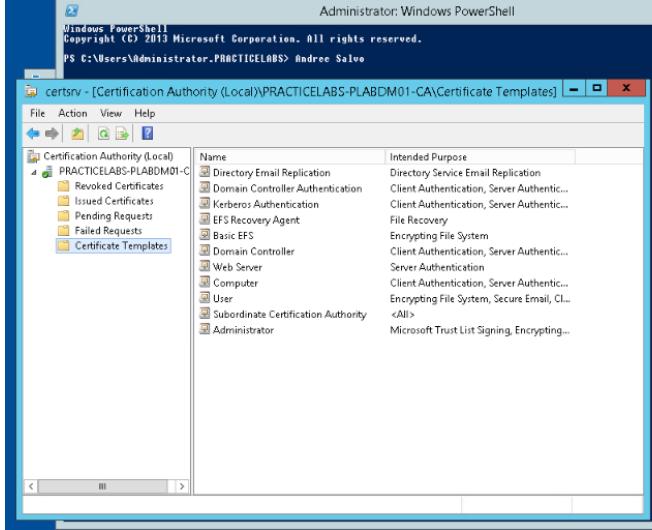
Southern New Hampshire University

CYB 300-14668

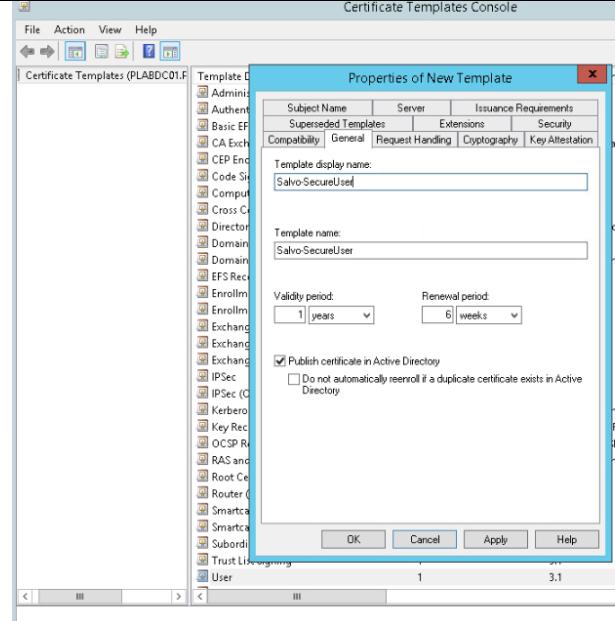
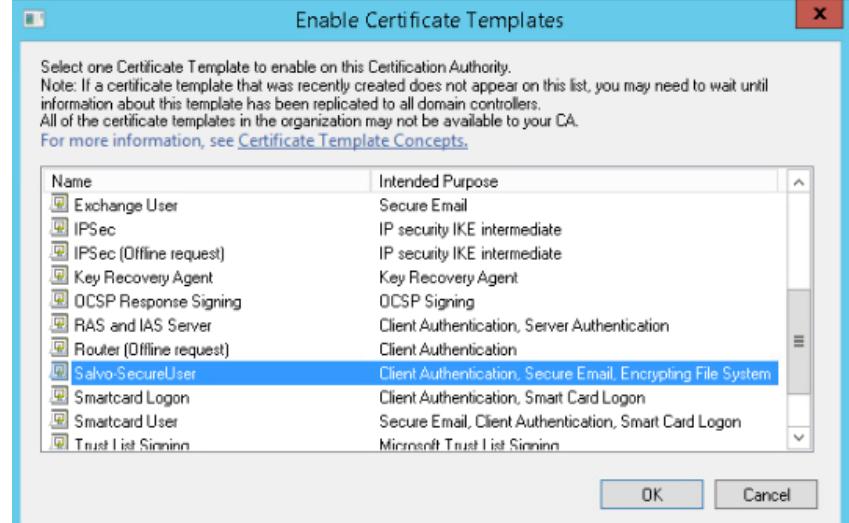
Instructor: Jason Keltner

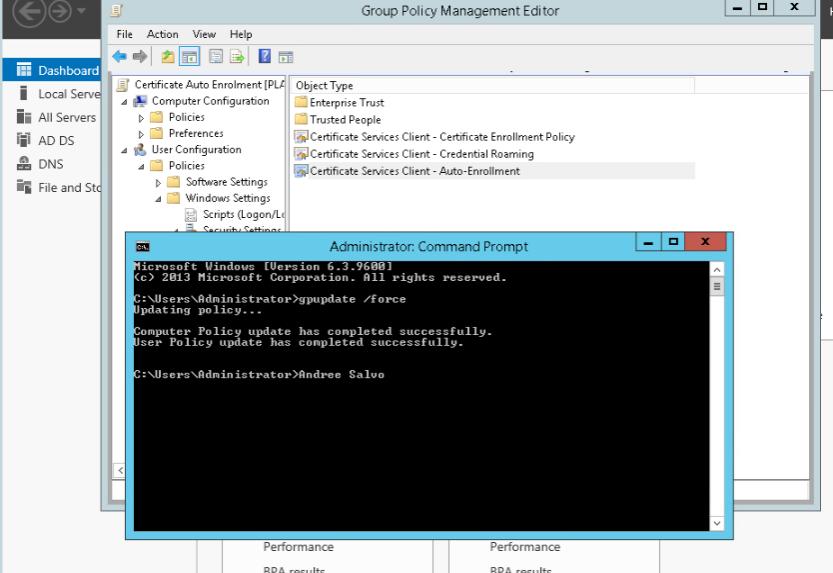
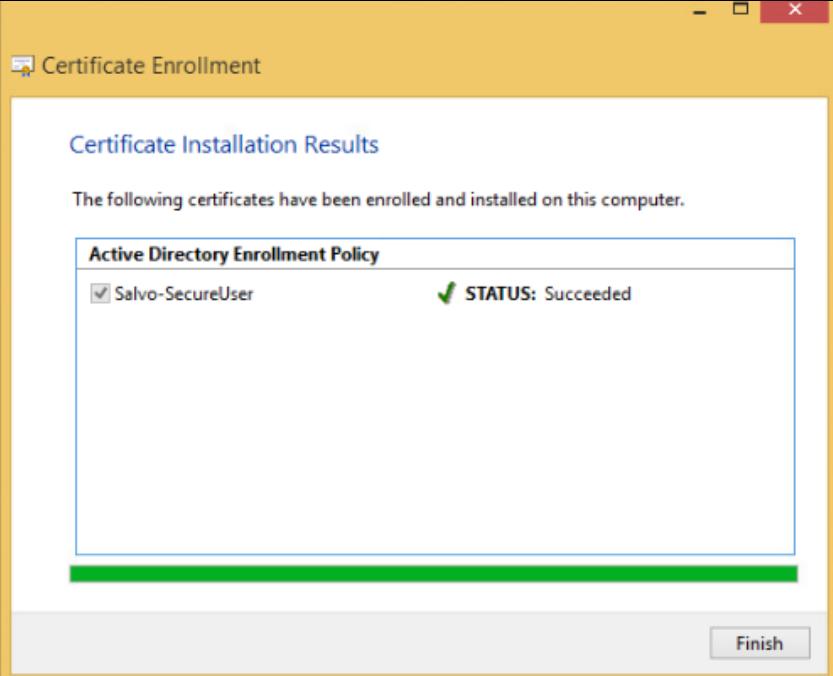
Lab: Manage Certificates

Exercise 1: Manage Certificate Templates

Prompt	Response																								
<p>Task 1: Take a screenshot of step 8 showing the details of the new user cert template. Add your name in the command line.</p>	 <p>The screenshot shows a Windows PowerShell window titled 'Administrator: Windows PowerShell' running on a server named 'certsrv'. The command line shows 'PS C:\Users\Administrator.PRACTICELABS> Andree Salvo'. The window displays a list of certificate templates under 'PRACTICELABS-PLABDM01-C'. The table lists the template names and their intended purposes:</p> <table border="1"> <thead> <tr> <th>Name</th> <th>Intended Purpose</th> </tr> </thead> <tbody> <tr> <td>Directory Email Replication</td> <td>Directory Service Email Replication</td> </tr> <tr> <td>Domain Controller Authentication</td> <td>Client Authentication, Server Authentic...</td> </tr> <tr> <td>Kerberos Authentication</td> <td>Client Authentication, Server Authentic...</td> </tr> <tr> <td>EFS Recovery Agent</td> <td>File Recovery</td> </tr> <tr> <td>Basic EFS</td> <td>Encrypting File System</td> </tr> <tr> <td>Domain Controller</td> <td>Client Authentication, Server Authentic...</td> </tr> <tr> <td>Web Server</td> <td>Server Authentication</td> </tr> <tr> <td>Computer</td> <td>Client Authentication, Server Authentic...</td> </tr> <tr> <td>User</td> <td>Encrypting File System, Secure Email, Cl...</td> </tr> <tr> <td>Subordinate Certification Authority</td> <td><All></td> </tr> <tr> <td>Administrator</td> <td>Microsoft Trust List Signing, Encrypting...</td> </tr> </tbody> </table>	Name	Intended Purpose	Directory Email Replication	Directory Service Email Replication	Domain Controller Authentication	Client Authentication, Server Authentic...	Kerberos Authentication	Client Authentication, Server Authentic...	EFS Recovery Agent	File Recovery	Basic EFS	Encrypting File System	Domain Controller	Client Authentication, Server Authentic...	Web Server	Server Authentication	Computer	Client Authentication, Server Authentic...	User	Encrypting File System, Secure Email, Cl...	Subordinate Certification Authority	<All>	Administrator	Microsoft Trust List Signing, Encrypting...
Name	Intended Purpose																								
Directory Email Replication	Directory Service Email Replication																								
Domain Controller Authentication	Client Authentication, Server Authentic...																								
Kerberos Authentication	Client Authentication, Server Authentic...																								
EFS Recovery Agent	File Recovery																								
Basic EFS	Encrypting File System																								
Domain Controller	Client Authentication, Server Authentic...																								
Web Server	Server Authentication																								
Computer	Client Authentication, Server Authentic...																								
User	Encrypting File System, Secure Email, Cl...																								
Subordinate Certification Authority	<All>																								
Administrator	Microsoft Trust List Signing, Encrypting...																								

Exercise 2: Manage Certificate Enrollment

Prompt	Response																								
<p>Task 1: In Step 4, replace the name in the “Template display name” with your last name - SecureUser (LastName-SecureUser).</p> <p>Then, in Step 13, scroll down until you see LastName-SecureUser and take a screenshot of the Enable Certificate Templates window.</p>	  <table border="1"> <thead> <tr> <th>Name</th> <th>Intended Purpose</th> </tr> </thead> <tbody> <tr> <td>Exchange User</td> <td>Secure Email</td> </tr> <tr> <td>IPSec</td> <td>IP security IKE intermediate</td> </tr> <tr> <td>IPSec (Offline request)</td> <td>IP security IKE intermediate</td> </tr> <tr> <td>Key Recovery Agent</td> <td>Key Recovery Agent</td> </tr> <tr> <td>OCSP Response Signing</td> <td>OCSP Signing</td> </tr> <tr> <td>RAS and IAS Server</td> <td>Client Authentication, Server Authentication</td> </tr> <tr> <td>Router (Offline request)</td> <td>Client Authentication</td> </tr> <tr> <td>Salvo-SecureUser</td> <td>Client Authentication, Secure Email, Encrypting File System</td> </tr> <tr> <td>Smartcard Logon</td> <td>Client Authentication, Smart Card Logon</td> </tr> <tr> <td>Smartcard User</td> <td>Secure Email, Client Authentication, Smart Card Logon</td> </tr> <tr> <td>Trust List Signing</td> <td>Microsoft Trust List Signing</td> </tr> </tbody> </table>	Name	Intended Purpose	Exchange User	Secure Email	IPSec	IP security IKE intermediate	IPSec (Offline request)	IP security IKE intermediate	Key Recovery Agent	Key Recovery Agent	OCSP Response Signing	OCSP Signing	RAS and IAS Server	Client Authentication, Server Authentication	Router (Offline request)	Client Authentication	Salvo-SecureUser	Client Authentication, Secure Email, Encrypting File System	Smartcard Logon	Client Authentication, Smart Card Logon	Smartcard User	Secure Email, Client Authentication, Smart Card Logon	Trust List Signing	Microsoft Trust List Signing
Name	Intended Purpose																								
Exchange User	Secure Email																								
IPSec	IP security IKE intermediate																								
IPSec (Offline request)	IP security IKE intermediate																								
Key Recovery Agent	Key Recovery Agent																								
OCSP Response Signing	OCSP Signing																								
RAS and IAS Server	Client Authentication, Server Authentication																								
Router (Offline request)	Client Authentication																								
Salvo-SecureUser	Client Authentication, Secure Email, Encrypting File System																								
Smartcard Logon	Client Authentication, Smart Card Logon																								
Smartcard User	Secure Email, Client Authentication, Smart Card Logon																								
Trust List Signing	Microsoft Trust List Signing																								

<p>Task 2: In Step 10, run the gpupdate /force command to propagate the new user Group Policy to the domain. Add your name after the command prompt and take a screenshot of the output and your name.</p>	 <pre>Administrator: Command Prompt Microsoft Windows [Version 6.3.9601] (c) 2013 Microsoft Corporation. All rights reserved. C:\Users\Administrator>gpupdate /force Updating policy... Computer Policy update has completed successfully. User Policy update has completed successfully. C:\Users\Administrator>Andree Salvo</pre>				
<p>Task 3: In Step 10, take a screenshot of the Certificate Installation Results window.</p>	 <p>Certificate Enrollment</p> <h3>Certificate Installation Results</h3> <p>The following certificates have been enrolled and installed on this computer.</p> <table border="1"> <thead> <tr> <th colspan="2">Active Directory Enrollment Policy</th> </tr> </thead> <tbody> <tr> <td><input checked="" type="checkbox"/> Salvo-SecureUser</td> <td>✓ STATUS: Succeeded</td> </tr> </tbody> </table> <p>Finish</p>	Active Directory Enrollment Policy		<input checked="" type="checkbox"/> Salvo-SecureUser	✓ STATUS: Succeeded
Active Directory Enrollment Policy					
<input checked="" type="checkbox"/> Salvo-SecureUser	✓ STATUS: Succeeded				
<p>What is the importance of creating custom self-signed certificates for your organization? For example, are settings customized depending on the type or business of the organization?</p>	<p>The importance of creating a custom self-signed certificate let's organizations control security settings like key strength, validity, and usage, tailoring them to business needs and compliance requirements.</p>				