
SVRHOL16: Microsoft Identity Lifecycle Manager 2007

Objectives

The goal of this lab is to:

Provide a hands-on experience on Microsoft Identity Lifecycle Manager 2007.

Demonstrate the potential usage scenarios of the product.

Show how easy it is to setup ILM 2007 to synchronize different directories and data sources

Demonstrate how to use ILM 2007 to automatically provision user accounts in connected directories, including how to automate certificate management.

Learn how to automate identity management tasks.

Use ILM 2007 to maintain a consistent state of the directories over the lifetime of accounts.

Estimated time to complete this lab: 60 minutes

Before you start the lab, please complete the following steps

Tasks	Detailed steps
1. Active Directory preparation	On the Start Menu, click Active Directory Users and Computers Navigate to the Users container and locate the miissvc account. Select Properties and then the Account tab. Check the Password never expires flag. Click OK .
2. Start MIIS and restart Certificate Services	a. On the Start Menu, Select Administrative Tools and then Services . Locate Microsoft Identity Integration Server and select Start . b. Locate Certificate Services . Select Restart the service .

Exercise 1

Using ILM 2007 to Provision New Employees

Scenario

Hire a new employee and create user accounts in the Human Resources database, Active Directory, a web-based ERP application, along with an Exchange mailbox, and the appropriate group membership in Active Directory.

Litware Inc. has an application that they use to add new employees. When a new employee's information is entered into the human resources application, the following activities need to take place automatically:

- An account in Active Directory is created.
- An Exchange mail box is created.
- Active Directory group membership, based on the new employee's title and department, is managed.
- Membership in a group which allows the new employee to enroll for digital certificates is granted.
- Access to certain modules in the ERP application, based on the new employee's job role, is granted.

You work in the Human Resources (HR) department and have just hired Jane Smith and Peter Pan for the Sales team.

What will we cover?

This workshop will demonstrate how ILM 2007 enables the creation and flow of the user identity data across directories. During this exercise you will:

- Create new employees in the HP application.
- See how ILM 2007 is configured to flow objects and attributes from source to target data sources and directories.
- Run a Management Agent (MA) to interactively trigger rules in ILM 2007.
- Connect to Active Directory, and WebERP, to view the results.

Logon credentials

To logon to the server, use the following credentials:

Username: Administrator

Password: password

Tasks	Detailed steps
<p>1. Add two new employees to the HR database.</p>	<p>a. On the Desktop, double-click Human Resources. Click New Employee, and then enter the following information:</p> <p style="padding-left: 20px;">Name: Ms Jane Smith Department: Sales Job Title: Clerk Mobile: 555-1111 Phone: 555-2222 Manager: 212-340 Ms Addy Hicks</p> <p>Click Save Changes. Repeat the steps above to add another employee using the following information:</p> <p style="padding-left: 20px;">Name: Mr Peter Pan Department: Accounting Job Title: Clerk Mobile: 555-3333 Phone: 555-4444 Manager: 212-340 Ms Addy Hicks</p> <p>You have now added records for Jane and Peter who are in different departments but who report to the same manager.</p> <p>Minimize HR Maintenance.</p>
<p>Start a management agent run in Microsoft Identity Integration Server.</p>	<p>a. On the Desktop, double-click Run MIIS Once.</p> <p>This step executes a script which causes MIIS to run a number of management agents in a specific order.</p> <p>Please wait until the script is complete before continuing to the next task.</p>
<p>Examine the results in Identity Manager.</p>	<p>a. On the Start Menu, click Identity Manager. You should see six new entries (with the current date in the Start Time and End Time columns). These represent the results of the MA runs executed by the Run MIIS Once script.</p> <p>b. On the Operations view, in the list of Management Agent Operations, click the entry for HumanResources with the Profile Name of Full Import and Delta Sync.</p> <p>At the bottom of the window, you will see the synchronization statistics Staging, Inbound Synchronization, and Outbound Synchronization. Note that 2 adds and 2 projections were reported. This indicates that the two new employee accounts have been successfully imported from the HR application and have been created in the MIIS Metaverse – which is the central identity store.</p> <p>Note also that 2 provisioning adds, and 2 export attribute flows occurred to both the ActiveDirectory and the WebERP management agents during outbound synchronization. This indicates that based on the two additions to the MIIS Metaverse, two new entries have been created in both Active Directory and the WebERP application.</p> <p>MIIS keeps track of all operations, inbound and outbound, in a SQL Server database.</p> <p>Click Group Management.</p>

	<p>Notice that below Outbound Synchronization there are 3 provisioning adds. These represent the creation of three new groups in Active Directory. Two of the new groups are based on the departments; Sales and Accounting, of the new employees, while the other new group is based on the new employee's title, Clerk. If you click the Provisioning Adds link you can see the new groups.</p> <p>Minimize Identity Manager.</p>
<p>View the results in Active Directory Users and Computers.</p>	<ol style="list-style-type: none"> From the Start Menu, click Active Directory Users and Computers. Navigate to the Employees organizational unit. Open the Accounting organizational unit. <p>Note that a user object, PPan, existing is the Accounting organizational unit. This is the user object for Peter Pan that has been automatically created by MIIS.</p> <p>In the details pane, double-click PPan.</p> <p>In the PPan Properties dialog box, on the General tab, note that the Telephone number has been populated from the HR application and that an E-mail address has been created for Peter Pan.</p> <p>On the Telephones tab, notice that the Mobile number has been populated from the HR application.</p> <p>On the Organization tab, notice that the Title, Department, and Manager attributes have been populated from the HR application.</p> <p>On the Member Of tab, notice that the user is a member of the Accounting Department, CLM Subscribers, and Title of Clerk groups.</p> <p>Click Cancel.</p> <p>Open the Sales organizational unit.</p> <p>Repeat step d for JSmith.</p> <p>Note that Jane Smith is a member of the Sales Department group rather than the Accounting Department group.</p> <p>Minimize Active Directory Users and Computers.</p>
<p>View the results in the WebERP application.</p>	<ol style="list-style-type: none"> On the Start Menu, click WebERP. Log in as admin with a password of password. Click Setup. In the General column, click User Accounts. <p>Notice that entries have been created for both Jane Smith, and Peter Pan, and that their Security Group membership matches the departments to which they belong.</p> <p>Click 0 Logout, and then minimize Internet Explorer.</p>
<p>Run the MIIS Management Agents again.</p>	<ol style="list-style-type: none"> On the Desktop, double-click Run MIIS Once. <p>Please wait until the script is complete before continuing to the next task.</p>
<p>Examine the results in the HR Maintenance application.</p>	<ol style="list-style-type: none"> Restore HR Maintenance. Select either of the two new employees. <p>Note that the Email field has now been populated and that the value matches the value from Active Directory. You may need to click Refresh in order to see the updated record.</p> <p>Confirm that the Email field has been populated for the other new</p>

	employee, and then minimize HR Maintenance .
Examine the configuration of the management agents in Identity Manager .	<p>a. Restore Identity Manager and click Management Agents.</p> <p>b. In the list of Management Agents, double-click HumanResources.</p> <p>c. In the Properties dialog box, click Configure Attribute Flow.</p> <p>Note that an attribute flow is defined between the person object in the HR data source and the person object in the metaverse.</p> <p>Click the + icon to expand the attribute flow.</p> <p>This view shows in detail which attributes from the source and metaverse objects are flowed through MIIS and in which direction. Note that with the exception of the email/mail attributes, all attribute flows are defined as import flows, which means the values are flowed from the source to MIIS. The email/mail attributes flow from MIIS to the source.</p> <p>Click Cancel.</p> <p>Examine the attribute flow rules for the remaining management agents. Ensure that you do not make any changes to the existing attribute flow rules.</p> <p>Minimize Identity Manager.</p>
Examine how MIIS enforces business rules.	<p>In this scenario, the HR application is authoritative for the employee's phone number, Active Directory is authoritative for the employee's email address, and the organizational unit in which the employee's user account exists is dependant upon the department to which they belong. This task will illustrate how MIIS can be used to enforce these types of business rules.</p> <p>a. Restore Active Directory Users and Computers.</p> <p>b. In the Sales organizational unit, right-click JSmith, and then click Move.</p> <p>c. In the Move dialog box, expand Employees, click Engineering, and then click OK.</p> <p>d. Confirm that JSmith has been moved to the Engineering organizational unit.</p> <p>e. In the Engineering organizational unit, double-click JSmith.</p> <p>f. On the General tab, change the Telephone number to 555-5555, and then click OK.</p> <p>g. Minimize Active Directory Users and Computers.</p> <p>h. Restore HR Maintenance.</p> <p>i. Select the employee record for Ms Jane Smith.</p> <p>j. Change the Email address to Jane.Smith@litware.com, and then click Save Changes.</p> <p>k. Minimize HR Maintenance.</p> <p>l. On the Desktop, double-click Run MIIS Once.</p> <p>Please wait until the script is complete before continuing with the next step.</p> <p>m. On the Desktop, double-click Run MIIS Once again.</p> <p>Please wait until the script is complete before continuing with the next step.</p> <p>n. Restore Active Directory Users and Computers.</p> <p>o. In the console tree, select Sales, and then on the Action menu, click Refresh.</p> <p>Note that the JSmith user object has been moved back to the Sales</p>

	<p>organizational unit.</p> <p>p. Double-click JSmith.</p> <p>In the JSmith Properties dialog box, note that the Telephone number has been changed back to the correct value.</p> <p>q. Click Cancel, and then minimize Active Directory Users and Computers.</p> <p>r. Restore HR Maintenance.</p> <p>s. Ensure that the record for Ms Jane Smith is selected, and then click Refresh.</p> <p>Note that the email address has been changed back to the correct value.</p> <p>t. Minimize HR Maintenance.</p>
--	--

Summary

You have examined the synchronization of identity information between different data sources based on an HR driven provisioning scenario. You have seen how MIIS keeps track of the operations performed in different identity systems.

You have seen how Identity Manager allows you to easily define attribute flow between connected systems, and how business rules can be enforced.

Note that this is only one scenario that demonstrates some of the basic functionality of ILM 2007. You can use MIIS to build much more sophisticated identity integration and management applications.

To learn more about ILM 2007, continue with Exercise 2.

Exercise 2

Using ILM 2007 to Manage Digital Certificates

Scenario

In this exercise you will learn how to use ILM 2007 to manage digital certificates.

Continuing from Exercise 1, Litware Inc. needs to allow new employees to retrieve a digital certificate in order to use the Encrypting File System (EFS) feature in Windows.

What will we cover?

This exercise will demonstrate how ILM 2007 helps you manage digital certificates.

During this exercise you will:

Create and configure a Profile Template.

Import a management agent for Certificate Lifecycle Manager.

Update the provisioning code to enable the automatic provisioning of a request for a CLM profile based on the new profile template.

Examine the results of these changes to the system.

Tasks	Detailed steps
<p>1. Create a new profile template.</p>	<p>a. On the Start Menu, click Certificate Lifecycle Manager.</p> <p>Note that there is a delay the first time you access the CLM portal during a session. Please be patient while the portal is loading.</p> <p>b. Click the logo to enter the portal.</p> <p>c. In the Administration section, click Manage Profile Templates.</p> <p>d. In the Profile Template List, select the check box to the left of CLM Sample Profile Template, and then click Copy a selected profile template.</p> <p>e. In the New profile template name text box, replace the existing text with EFS and then click OK.</p> <p>Note that the provisioning code is dependant on the correct name for the profile template.</p> <p>A profile template is an object, stored in Active Directory, which contains, among other things, a list of certificate templates used to enroll certificates. In this scenario, you will configure the profile template to contain a custom version 2 certificate template which can be used for EFS.</p> <p>f. In the Certificate Templates section, click Add new certificate template.</p> <p>g. In the Certificate Authorities section, select the check box to the left of LITDCCA.</p> <p>CLM can be used to manage one or more Certification Authorities (CA). In this scenario, CLM is managing only a single CA.</p> <p>h. In the Available Certificate Templates section select the check box to the left of ArchiveEFS, and then at the bottom of the page, click Add.</p> <p>i. Select the check box to the left of User, and then click Delete selected</p>

	<p align="center">certificate templates.</p>
<p>2. Configure the Enroll Policy.</p>	<p>a. In the Select a view section, click Enroll Policy.</p> <p>The account that will be used for the CLM management agent is a member of the CLM Managers group. This account will be used to submit a request to initiate enrollment for new employees to CLM. In order to submit this request, the CLM Managers group needs to be granted the permission to initiate enrollment requests in the EFS profile template.</p> <p>In addition, since the request will be submitted through MIIS by the management agent, employees should not be allowed to submit their own requests.</p> <p>b. In the Workflow: General section, click Change general settings.</p> <p>c. Clear the check box to the left of Use self serve, and then click OK.</p> <p>d. In the Workflow: Initiate Enroll Requests, click Add a new principal for enroll request initiation.</p> <p>e. In the Principal text box, type Litware\CLM Managers and then click OK.</p> <p>f. Select the check box to the left of NT AUTHORITY\SYSTEM, and then click Delete principals for enroll request initiation, and then click OK.</p> <p>Note that a policy must have at least one security principal defined. You must add one or more security principals before you can remove the default NT AUTHORITY\SYSTEM security principal</p> <p>g. In the Data Collection section, select the check box to the left of Sample Data Item, click Delete data collection items, and then click OK.</p> <p>During different stages of certificate management, data can be collected and stored. For example, if you were issuing a smart card to an employee you might record information regarding the type of identification presented by the employee to prove their identity (driver's license, passport, etc.). This information is then stored in the CLM database.</p> <p>h. In the One-Time Passwords section, click Change password provider settings.</p> <p>i. In the Number of one-time passwords (password provider data) text box, change the value from 1 to 0 and then click OK.</p> <p>One-time passwords can be used to provide an additional level of security during a workflow. In this scenario, an account in Active Directory provides sufficient security.</p> <p>Note that there are a number of additional policies available which are not used in this scenario.</p> <p>j. Close Internet Explorer.</p>
<p>3. Modify the provisioning rules extension to enable the provisioning of CLM profile requests.</p>	<p>a. On the Start Menu, click Microsoft Visual Studio 2005.</p> <p>b. In the Recent Projects list, click MiisLab.</p> <p>c. Scroll to the top of the MiisLab.cs file, and then from the Edit menu, point to Find and Replace, and then click Quick Replace.</p> <p>d. In the Find and Replace dialog box, in the Find what text box, type //**</p> <p>e. Leave the Replace with text box empty, and then click Replace All.</p> <p>A message box is displayed indicating that 7 occurrences have been</p>

	<p>replaced.</p> <ul style="list-style-type: none"> f. In the Microsoft Visual Studio message box, click OK. g. In the Find and Replace dialog box, click the X icon to close the dialog box. h. On the Build menu, click Rebuild MiisLab. <p>This recompiles the provisioning code to reflect the changes you have made.</p> <ul style="list-style-type: none"> i. Close Microsoft Visual Studio.
<p>4. Import the Certificate Lifecycle Manager management agent.</p>	<ul style="list-style-type: none"> a. Restore Identity Manager. b. On the Management Agents view, in the Actions list, click Import Management Agent. <p>The management agent was created previously and exported to an XML file. The XML file contains the complete management agent configuration, including any Run Profiles, but not any connection passwords.</p> <ul style="list-style-type: none"> c. In the Open dialog box, select Certificate Lifecycle MA.xml, and then click Open. d. In the Create Management Agent dialog box, leave the name value as it appears, and then click Next. e. On the Configure Connection Information page, in the Password text box, type password and then click Next, without making any additional changes, until the Configure Extensions page appears. f. On the Configure Extensions page, click Finish. <p>The new management agent is now ready to run.</p>
<p>5. Run the new management agent once to import the clmConfig object.</p>	<ul style="list-style-type: none"> a. Before the CertificateLifecycleManager management agent can be used to provision profile requests, you must run it once with the Full Import run profile in order to import the clmConfig object. b. Ensure that the CertificateLifecycleManager management agent is selected, and then from the Action list, click Run. c. In the Run Management Agent dialog box, select Full Import, and then click OK. d. While the Full Import run profile is executing, minimize Identity Manager.
<p>6. Modify the Run MIIS Once script to execute the new management agent.</p>	<ul style="list-style-type: none"> a. Navigate to C:\Documents and Settings\Administrator\My Documents\MiisLab. b. Right-click runMIIS-Once.cmd, and then click Edit. c. Change C:\MiisLabRunSequenceDeltas.xml to C:\MiisLabRunSequenceCLM.xml. d. Save the file, and then close Notepad.
<p>7. Add a new employee to the HR application.</p>	<ul style="list-style-type: none"> a. On the Desktop, double-click Human Resources. b. Click New Employee, and then enter the following information: Name: Mr Paul Adare Department: Sales Job Title: Clerk Mobile: 555-8888 Phone: 555-9999

	<p>Manager: 212-340 Ms Addy Hicks</p> <ul style="list-style-type: none"> c. Click Save Changes. d. Minimize HR Maintenance.
<p>8. Verify that the Full Import run has completed, and then execute the Run MIIS Once script.</p>	<ul style="list-style-type: none"> a. Restore Identity Manager and verify that the Full Import run has completed successfully. b. When the run has completed successfully, minimize Identity Manager, and then on the desktop, double-click Run MIIS Once. <p>Please wait until the script has finished executing before continuing with the next step.</p>
<p>9. Log on in the Client virtual machine with the new user account and examine the results.</p>	<ul style="list-style-type: none"> a. Start the Client virtual machine. b. In the Client virtual machine, log on to the Litware domain as padare with a password of password. c. Open http://dc1/clm. d. In the Microsoft Phishing Filter message box, click Ask me later, and then click OK. c. Click the logo to enter the portal. d. In the Requests list, click Executable. <p>This request was created automatically by the CertificateLifecycleManager management agent when you executed the Run MIIS Once script.</p> <ul style="list-style-type: none"> e. Click [Execute]. f. In the Potential Scripting Violation dialog box, click Yes. g. In the second Potential Scripting Violation dialog box, click Yes. <p>Note that the ArchiveEFS template shows an Action of Installed and a check mark appears in the Status column.</p> <ul style="list-style-type: none"> h. Click Next, and then close Internet Explorer.
<p>10. Verify that the certificate has been successfully installed.</p>	<ul style="list-style-type: none"> a. On the Start Menu, click Run. b. In the Run dialog box, type certmgr.msc and then click OK. c. In the console tree, expand Personal, and then click Certificates. d. In the details pane, double-click the certificate. e. In the Certificate dialog box, on the General tab. <p>Note that the certificate Allows data on disk to be encrypted.</p> <ul style="list-style-type: none"> f. On the Details tab, select Certificate Template Information. <p>Note that the certificate is based on the ArchiveEFS certificate template that you added previously to the profile template.</p> <ul style="list-style-type: none"> e. Click OK, and then log off.

Summary

You have learned how to create a CLM profile template in order to issue and manage digital certificates. In addition, you have learned how to import a management agent to MIIS and how to configure a management agent to issue requests to CLM when a new employee is added.

As with the previous exercise, this has been a simply demonstration of how MIIS and CLM can be used together in ILM 2007 in order to issue and manage certificates.