

# **Global Information Assurance Certification Paper**

# Copyright SANS Institute Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

# Interested in learning more?

Check out the list of upcoming events offering "Security Essentials: Network, Endpoint, and Cloud (Security 401)" at http://www.giac.org/registration/gsec

# Securing Windows 20003 with ADAM and MIIS Feature Packs

GIAC Gold Certification

Author: Frederic Dumesle, crapaxon@hotmail.com

Adviser: Charles Hornat

Accepted:

#### 1. Introduction and scope

Windows 2003 has been released almost 5 years ago which is a long time in IT terms. Even though hundreds of article, white papers and case study are broadly available a significant number of scenarios involving Windows 2003 in Perimeter Design are scarce at best. This situation stems from a suspicious feeling towards the operating system in such scenarios. This paper will look at operating system optional components from a security stand point and how they can bring added value by leveraging their functionality. The paper will focus on a specific perimeter scenario and will provide an in depth case study with an end to end approach from design to deployment. The report will often refer to principles learned from SANS GIAC Security essentials track.

# 2. Windows 2003 feature packs

#### Summary description

There are 6 add-on components available for window 2003 and the R2 release for both 32bits and 64 bits version. These components are free and don't require a license outside of the core operating system one. The only exception is RMS which requires an RMS client license

Extensive detailed documentation can be found at
http://www.microsoft.com/windowsserver2003/techinfo/overview/def
ault.mspx

#### ADAM

This is an LDAP compliant directory service. This is basically Active Directory without the NOS (network operating system) component. The product is comparable to OpenLDAP. It supports LDAP over SSL, granular authorization model and features the

same management capability as Active Directory (ADSI, MMC, etc). It also supports web services for Directory through DSML<sup>1</sup>

#### MIIS

Stands for Microsoft Identity Integration Server. MIIS implements what is commonly called a Meta Directory. Its most powerful functionality aggregates data from multiple sources into a virtual space. The product supports business rules that will define data flow from sources to a virtual space and vice versa. The basic version called "Feature Pack" supports Active Directory, Exchange and ADAM while the enterprise edition brings extended sources like SAP, oracle PeopleSoft, Lotus, etc...

#### RMS

Right management services provide client with pki based authorization. The client is typically a RMS compatible client like outlook which brings the possibility for the end user to control whether outlook or office documents can be printed or forwarded.

#### ADFS

Active directory Federated Services provide single sign on for web applications relying on NT tokens. It provides an organization with flexibility for authenticating and authorizing external partners without exposing your internal Active Directory.

# 3. Generic Infrastructure Architecture and Approach

#### Generic Security Requirements

The matrix below describes generic security requirements that Morpheus would like to address

Strong Authentication	PKI or 2 Factor

http://msdn2.microsoft.com/en-us/library/aa813608.aspx

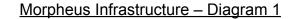
Audit Failed Log in	Log retention 60 days
Segregation of duties	Different teams with different roles
Strong Password Policy	At least 8 characters and password complexity
Physical Security	Restricted Zone for DMZ Infrastructure

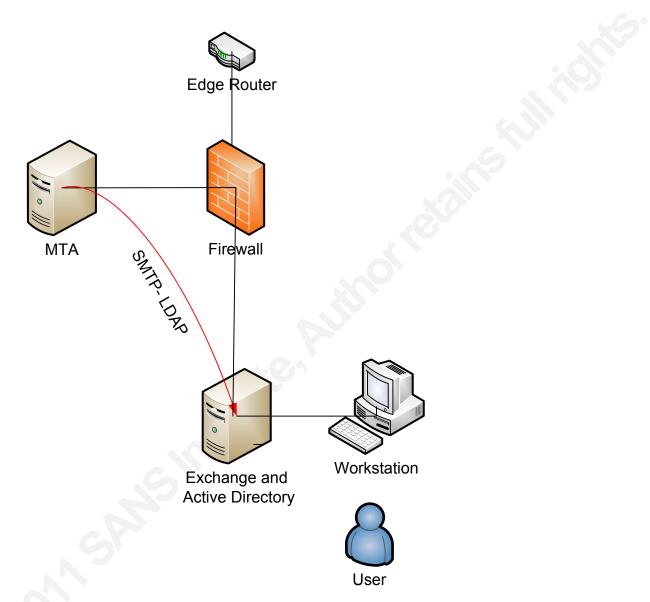
# 4.Case Study: "Morpheus Inc."

#### Design

Morpheus Incorporated is the typical medium to large enterprise with One Internal network, one DMZ and internet connectivity. They host an exchange organization and use a single Postfix or Sendmail UNIX based MTA in the DMZ. Additionally the MTA performs email check through LDAP as part of the SMTP transaction. In fact initially Morpheus would accept any mails as long as recipients were *morpheus.com addresses*. However as spammers were sending bulk mails to invalid morpheus.com recipients the company got blacklisted by ISPs as it was sending millions of NDRs. The LDAP check mitigates the issue even though Active Directory is exposed to the internet.

The Visio diagram 1 below describes Morpheus Infrastructure





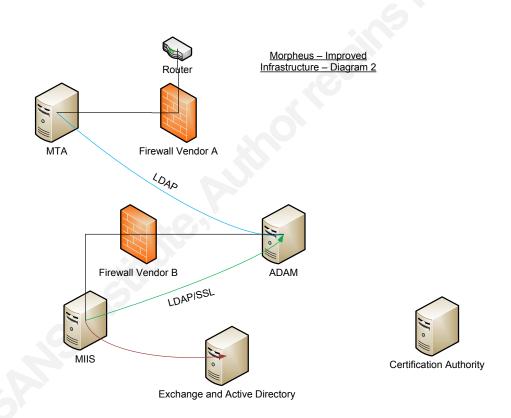
# Security Assessment

Morpheus Incorporated asked an external company to produce a security assessment report. The following issues have been identified:

• Single Firewall Vendor

- Single Point of failure for MTA, firewall, router, switches
- Active Directory exposure through LDAP from MTA

#### New Proposed Design



The above Visio diagram depicts a significantly improved design featuring new components. Although it looks more complex this infrastructure addresses the issues previously described and meets chapter 3 requirements.

#### Directory Component: ADAM

The ADAM component purpose is processing LDAP requests for email address initiated by the MTA. Instead of exposing Active Directory to the MTA and internet we only expose an ADAM

instance whose schema is customized with a minimum set of attributes and elements. Hence a compromised ADAM would not leak critical data like passwords and other important Active Directory Information.

A number of additional security measures are deployed:

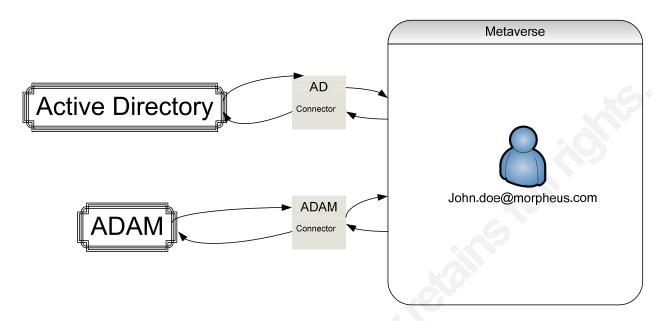
- ADAM is screened by a firewall(see later chapter) in a dedicated DMZ
- LDAP Security mechanism can be added( LDAP over SSL, stronger authentication)

#### Provisioning Component: MIIS

The Microsoft Identity Feature Pack component purpose is to aggregate data from active directory along with provisioning and de-provisioning of the ADAM Instance.

MIIS has the following core components

- SQL Database
  - o All MIIS data live inside a SQL Database (Locally
     or remote)
- Metaverse
  - o A place where aggregated data get ultimately persisted. It has its own schema
- Space connector
  - o A buffer space containing data from a specific source



Multiple filters can be defined at the connector space level and also in the metaverse through the usage of specific provisioning rules. The detailed implementation will be provided later in the document. What matters is that the software allows the infrastructure architect to define security mechanisms that address Integrity (ensuring active directory attributes meet specific criteria's), confidentiality (MIIS will use LDAP over SSL when connecting to AD and ADAM), authentication (MIIS uses a PKI certificate to authenticate with the ADAM server, Kerberos when authenticating with Active directory)

#### Second Firewall Layer

We apply the defense in depth principle by introducing an additional Firewall Layer. This layer will be from a different vendor. Depending on the vendor we could also filter at the application layer and implement specific LDAP filtering. Should the first firewall be compromised Morpheus internal network is still protected by the second layer.

#### Detailed Design and Implementation

#### Morpheus.int Domain

The Morpheus.int Active Directory is a regular out of box AD forest. It features an exchange extended schema allowing users to have mailboxes and email addresses.

## Mail Design

Morpheus Inc relies on the MTA in the DMZ and exchange for internal mails. Extended exchange attributes are used to implement external contractor and student policies. In fact the "extensionattribute1" is set to "active" to enable internet access. Matching user attributes will be processed and provisioned into the ADAM instance. Any other value will be skipped. Furthermore when a staff gets internet mail access denied the email address is automatically de-provisioned from the ADAM instance. These core processes are under MIIS control.

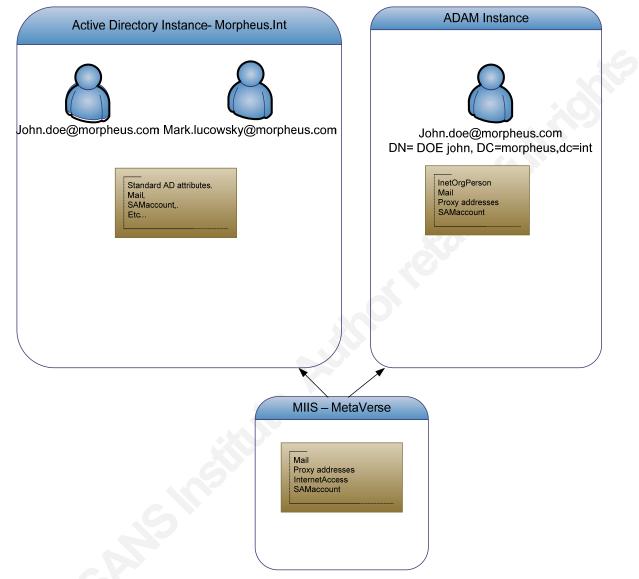
The relevant user attributes are the following for Morpheus.int

cn InstanceType ObjectCategory ObjectClass ObjectSID SAMaccountName Mail Extensionattribute1 proxyAddresses

The red attributes are mandatory ones. The mail attribute contains the user email address. The ExtensionAttribute1 is a string containing "active" or "inactive". This attribute role defines whether a user has the ability or not to send a mail to the internet.

proxyAddresses is used to store multivalue email addresses.

### Service View



The diagram above describes the logical view between the three components from a schema perspective.

#### ADAM Design

cn InstanceType ObjectCategory ObjectClass ObjectSID Mail proxyAddresses

Contrary to Active Directory ADAM schema is empty out of the box. The chosen schema will be an X.500 standard inetOrgPerson schema which will be imported through LDIF. Notice the mandatory attributes in RED along with the relevant attributes that are necessary for LDAP search performed by the MTA Client.

#### Application Partition

The application partition will be very simple and straight forward. We choose for **DC=Morpheus**, **DC=com**.

Since we need several users defined in the partition a hierarchical structure is the next logical step. We create an organizational unit called **Service Account**.

Let's now create several users:

Administrator	This account will have full		
	control on ADAM instance. Also		
	used by MIIS to update instance		
MTA Client xx	The account used by the MTA.		
	Notice we plan for future MTA.		
	One account per MTA server		

Monitoring	Support account for external
	party.read only

The DNs will list as follow:

CN=MTA Client01, OU=serviceaccount, DC=morpheus, DC=com

CN=Administrator, OU=serviceaccount, DC=morpheus, DC=com

CN=Monitoring, OU=serviceaccount, DC=morpheus, DC=com

Additionally the ADAM instance itself runs under the NETWORK Service account which has very limited privileges

#### Securing Adam Application

We need to secure ADAM communications with the external world as much as we can. Applying the defense in depth principle we will only allow LDAP over SSL at the firewall level. We will block standard LDAP port too and use packet filtering on the windows server (only allowing LDAP over SSL, ICMP and RDP for remote control)

#### PKI Deployment

We need to modify a file ACL to allow the ADAM instance service account to read the computer machine Keys. This is part of the LDAP over SSL ADAM implementation. If not setup properly ADAM will not open an SSL socket and will only listen on LDAP 389.

C:\Documents and Settings\All Users\Application Data\Microsoft\Crypto\RSA\MachineKeys.

#### **Offline** Certificate

We must now generate a certificate from a CA then import it in the ADAM server instance. The scenario assumes Morpheus Inc runs a Certification Authority on the internal LAN. The process would be similar Morpheus had chosen for an external trusted CA like VeriSign.

This is a 4 steps process:

- Generate an INF file
- Produce a REQ file
- CA generates a Certificate file using the REQ file as input
- Import the Certificate on the Target Machine

#### Generating an INF File

The INF file follows a standard for Certification Authority:

Open Notepad or your favorite text editor and paste the following text:

[Version]

Signature="\$Windows NT\$

Here the inf file

[NewRequest]

Subject = "CN=<DC fqdn>"; replace with the FQDN of the DC

KeySpec = 1

KeyLength = 1024 ; Can be 1024, 2048, 4096, 8192, or 16384.

; Larger key sizes are more secure, but have

; a greater impact on performance.

Exportable = TRUE

MachineKeySet = TRUE

SMIME = False

PrivateKeyArchive = FALSE

UserProtected = FALSE

UseExistingKeySet = FALSE

ProviderName = "Microsoft RSA SChannel Cryptographic Provider"

ProviderType = 12

RequestType = PKCS10

KeyUsage = 0xa0

[EnhancedKeyUsageExtension]

OID=1.3.6.1.5.5.7.3.1 ; this is for Server Authentication

Replace the "Subject" with appropriate LDAP path Server name.

Name the file serv.inf and save it somewhere on the hard disk (for instance %USERPROFILE%\)

#### Producing a REQ File

Open a command prompt and make sure you are in the previsously used directory (%USERPROFILE%\).

Run certreq -new. You will be prompted. Select your serv.inf file.

A new file has now been generated and is called serv.req.

#### CA Cert generation

Log in on the Microsoft CA web generation page using the URL: <a href="http://localhost/certsrv">http://localhost/certsrv</a>. You must be logged on the console through terminal services or interactively.

dress 🗃 http://localhost/certsrv/	• •	Go Links <sup>3</sup>
Microsoft Certificate Services Lab MS CA 2		Home
Velcome		
lse this Web site to request a certificate for your Web browser, e-mail client, or other p ertificate, you can verify your identity to people you communicate with over the Web, s nessages, and, depending upon the type of certificate you request, perform other secu	ign and encrypt	]a
ou can also use this Web site to download a certificate authority (CA) certificate, certi ertificate revocation list (CRL), or to view the status of a pending request.	ficate chain, or	
or more information about Certificate Services, see <u>Certificate Services Documentat</u>	ion.	
Select a task: <u>Request a certificate</u> <u>View the status of a pending certificate request</u> <u>Download a CA certificate, certificate chain, or CRL</u>		
	S local intra	pet
Start 🔀 进 📕 Windows Task Manager	Local intra	net 🕅 4:31 PM
Start 🕼 🧑 📕 Windows Task Manager 🎼 Microsoft Certificate elect request a certificate		
elect request a certificate Microsoft Certificate Services - Microsoft Internet Explorer ile Edit View Favorites Iools Help		
elect request a certificate Microsoft Certificate Services - Microsoft Internet Explorer jle Edit View Favorites Tools Help Back • • • • • • • • • • • • • • • • • • •		
elect request a certificate Microsoft Certificate Services - Microsoft Internet Explorer ile Edit View Favorites Iools Help		
elect request a certificate Microsoft Certificate Services - Microsoft Internet Explorer jle Edit View Favorites Tools Help Back • • • • • • • • • • • • • • • • • • •		
elect request a certificate Microsoft Certificate Services - Microsoft Internet Explorer je Edit View Favorites Tools Help Back • • • • • • • • • • • • • • • • • • •		
elect request a certificate Microsoft Certificate Services - Microsoft Internet Explorer jle Edit View Favorites Tools Help Back • • • • • • • • • • • • • • • • • • •		
elect request a certificate Microsoft Certificate Services - Microsoft Internet Explorer je Edit View Favorites Tools Help Back • • • • • • • • • • • • • • • • • • •		

Select Advanced certificate request

Advanced Certificate Request
The policy of the CA determines the types of certificates you can request. Click one of the following options to:
Create and submit a request to this CA.
Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.
Request a certificate for a smart card on behalf of another user by using the smart card certificate enrollment station. Note: You must have an enrollment agent certificate to submit a request on behalf of another user.
14 14

Select "Submit request by using a base64 or PKCS 10 file"

# Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certif PKCS #7 renewal request generated by an external source (such as a Web server) in the :

Saved Request:		
Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	■ ■ Browse for a file to insert.	
Certificate Temp	late:	$\searrow$
	Administrator	
Additional Attrib	utes:	
Attributes:		
	Submit >	
Paste the s	<u>erv.req</u> file content into "saved r	equest" dialog box
Select Web	<u>Server Template.</u>	
Microsoft Certif	icate Services Lab MS CA 2	
Certificate Is	sued	
The certificate	you requested was issued to you.	
$\odot$	DER encoded or OBase 64 encoded	
E Do	wnload certificate	
	wnload certificate chain	

ĸ

# Securing Windows 20003 with Feature Packs v 0 16

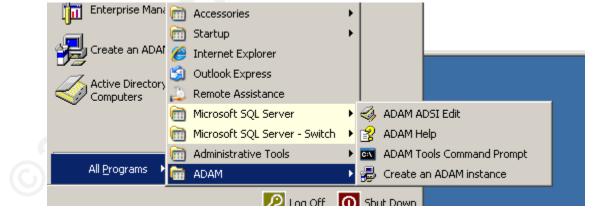
Download and copy the file to the ADAM Server. Use the certificate MMC to import it.

## Locking down the server

The Server itself will be secured using a specific template through the Local Policy: we only need a restricted number of services. A specific template should be used for each server (ADAM, MIIS).

#### ADAM Installation Guide

Install the default ADAM package then select menu to create a new Instance



This option autor	ce matically creates a new i	nstance of ADAM	I that uses the de	efault
	d schema partitions. The			
C A replica of an e	existing instance			
schema partition	tes a new instance of AD s replicated from another artitions to replicate.			

# Select "unique instance".

Active Directory Application Mode Setup Wizard	
Instance Name The instance name is used to differentiate this instance of ADAM from o instances on this computer.	ther ADAM
Type a name for this instance. The name should reflect the use for which of ADAM is intended.	h this instance
Instance name:	
maillookup	
Example: Addressbook1 The ADAM service name is created when the instance name is combine	d with the
product name. It will be displayed in the list of Windows services.	
ADAM service name: ADAM_maillookup	
Contract Contract	1 1.45
< <u>B</u> ack <u>N</u> ext > Cancel	Help

Provide a name

🖶 Active Directory Application Mode Setup Wizard 🛛 🗙	
Ports Computers will connect to this instance of ADAM using specific ports on all of the IP addresses associated with this computer.	
The ports displayed below are the first available for this computer. To change these ports, type the new port numbers in the text boxes below. If you plan to install Active Directory on this computer, do not use 389 for the LDAP port or 636 for the SSL port because Active Directory uses these port numbers. Instead, use available port numbers from the following range: 1025-65535.	
LDAP port number: SSS SSL port number: 636	
< <u>B</u> ack <u>N</u> ext > Cancel Help	

🖶 Active Directory Applicat	ion Mode Set	up Wizard		×
Application Directory Pa An application directory (		pplication-specifi	e data.	Ð
Do you want to create an ap	plication director	y partition for this	instance of ADAM	?
No, do not create an app Select this option if the ap upon installation, or if you	plication that yo	u plan to install ci	eates an applicatio	n directory
Yes, create an application Select this option if the ap directory partition upon ins not already exist in this ins CN=Partition1,DC=Woodg	plication that you tallation. A valid tance. Example	u plan to install de partition name is	any distinguished n	
Partition name: DC=morpheus,DC=com				
	< <u>B</u> ack	<u>N</u> ext>	Cancel	Help

Frederic Dumesle

20

We must create a partition that will be dedicated to serving the MTA

🖶 Active Directory Application Mode Setup Wizard 🛛 🔀	
File Locations You can specify a location for each type of file associated with this instance of ADAM.	
Specify the locations to store files associated with ADAM.	
Data files:	
C:\Program Files\Microsoft ADAM\maillookup\data     Browse       Data recovery files:	
C:\Program Files\Microsoft ADAM\maillookup\data Browse	
< <u>B</u> ack <u>N</u> ext > Cancel Help	
S	

🖶 Active Directory Application Mode Setup Wizard 🛛 🛛 🔀	
Service Account Selection ADAM performs operations using the permissions associated with the account you select.	
Set up ADAM to perform operations using the permissions associated with the following account.	
Network service account ADAM has the permissions of the default Windows service account.	
C Inis account: ADAM has the permissions of the selected account. Ensure that the account you select is set up to run as a service.	
User name: Browse	
Password:	
< <u>B</u> ack <u>N</u> ext > Cancel Help	

We apply the least privileged account principle: ADAM only needs "network service account"

🖶 Active Directory Application Mode Setup Wizard 🛛 🗙	
ADAM Administrators You can specify the user or group that will have administrative privileges for this instance of ADAM.	
Assign the following user or group of users administrative permissions for ADAM.	
<ul> <li>Currently logged on user: MORPHEUSINT Administrator The user that is installing ADAM will have administrative permissions for this instance of ADAM.</li> </ul>	
Ihis account The selected user or group will have administrative permissions for this instance of ADAM. You can choose any user or group from this computer, this computer's domain, or any domain that is trusted by this computer's domain.	
Account name:	
< <u>B</u> ack <u>N</u> ext > Cancel Help	

Let's now import the required schema.

Select MS-InetOrgPerson

🖶 Active Directory Application Mode Setup Wiz	ard 🗙	
Importing LDIF Files You can import data from Lightweight Directory I your ADAM application directory partition.	nterchange Format (LDIF) files into	
To configure the ADAM service in a specific way, imp below. © <u>D</u> o not import LDIF files for this instance of ADAM		
Import the selected LDIF files for this instance of a Available files:      MS-AZMan.LDF     MS-User.LDF     MS-UserProxy.LDF	Selected LDIF files: MS-InetOrgPerson.LDF	
< <u>B</u> ack <u>N</u>	ext > Cancel Help	

#### MIIS Design

#### Segregation of Duty and authorization model

To apply the segregation of duty principle the administrative model will be split into several business units. Typically the ADAM instances are managed by Security team while MIIS is maintained by Operation team. However the application owner is the security team.

The matrix below summarizes roles and responsibilities including the following levels:

R: Responsible

This is limited responsibility

A: Accountable

This is end to end complete responsibility

C: Consulted

This is being involved in the decision making Frederic Dumesle

24

#### I: Informed

This is just being informed about decision and information process

	Operations Unit	Security Team
High Level Design	I	A, R
Business Rule Change	I	A, R
Patching	R	A
Backup	A	Ι

#### Strong PKI based authentication

Since the ADAM server is located in a DMZ we cannot and should not rely on Windows Domain Authentication and Authorization. Pre shared key or NTLMv2 hashes must be ruled out because they are easily defeated. The chosen authentication will be certificate Based (PKI technology).

Morpheus Inc runs an enterprise wide Certification authority whose purpose is to provide company servers with computer and user certificates.

MIIS will connect to the ADAM instance using LDAP over SSL. The server will use its certificate to authenticate to the ADAM server. The SSL session will be successful if both certificates trust the same root CA.

#### **Defining Management Agents**

A management agent describes the connection between a data source (AD, ADAM) and some kind of temporary buffer area called

a connector space. The agent also controls data flow between the connector space and the metaverse.

# **Active Directory Agent**

Open the Identity Manager and select management agents- select create

M area	Ereate Management Agent	Create Management Agent
	agement Agent Designer	
	Create Management Agent	Management agent for:
	Connect to Active Directory Forest	Active Directory
	Configure Directory Partitions	With this management agent, you can synchronize with Active Directory forests.
	Select Object Types	
	Select Attributes	
	Configure Connector Filter	
	Configure Join and Projection Rules	Marra
	Configure Attribute Flow	Name:
	Configure Deprovisioning	Active Directory Management
	Configure Extensions	Description:
		[]
		< Back Next > Cancel Help

Management Agent       Connect to Active Directory Forest         Create Management Agent       To create a management agent for an Active Directory forest, you must connect to that forest by specifying a domain account and password with permissions to enumerate the forest's directory partitions. These credentials are then used by default to run the management agent. For moinformation about specific permissions required for synchronizing with this connected data source, see Microsoft Identity Integration Server Help.         Eorest name:       morpheus.int         Configure Extensions       Password:         Password:       morpheus.int         Domain:       morpheus.int	Create Management Agent <ul> <li>Connect to Active Directory Forest.</li> <li>Configure Directory Partitions</li> <li>Select Object Types</li> <li>Select Attributes</li> <li>Configure Domector Filter</li> <li>Configure Deprovisioning</li> <li>Configure Extensions</li> </ul> <ul> <li>Password:</li> <li>Password:</li> <li>Domain:</li> </ul>	Create Management Agent		
<ul> <li>Connect to Active Directory Forest         Configure Directory Partitions         Select Object Types         Select Attributes         Configure Connector Filter         Configure Deprovisioning         Configure Extensions         Password:         Password:         Password:         Domain:         Inorpheus.int         Inorpheus.int</li></ul>	<ul> <li>Connect to Active Directory Forest Configure Directory Partitions Select Object Types Select Attributes Configure Connector Filter Configure Attribute Flow Configure Deprovisioning Configure Extensions</li> <li>Configure Extensions</li> <li>P⊴ssword:</li> <li>Martine Section Server Help.</li> <li>Martine Section Server Help.</li> <li>Martine Section Server Help.</li> <li>Martine Section Server Help.</li> <li>Configure Extensions</li> <li>Martine Section Server Help.</li> <li>Martine Section Section Server Help.</li> <li>Martine Section Sect</li></ul>		Connect to Active Directo	ry Forest
Configure Join and Projection Rules       Imorpheus.int         Configure Attribute Flow       Imorpheus.int         Configure Deprovisioning       Imorpheus.int         Configure Extensions       Password:         Imorpheus.int       Imorpheus.int         Imorpheus.int       Imorpheus.int         Imorpheus.int       Imorpheus.int	Configure Join and Projection Rules	Connect to Active Directory Forest Configure Directory Partitions Select Object Types	that forest by specify enumerate the forest These credentials are information about spe	ng a domain account and password with permissions to s directory partitions and read the schema directory partition. s then used by default to run the management agent. For more ecific permissions required for synchronizing with this
Configure Deprovisioning     Password:     ************************************	Configure Deprovisioning       Password:       ************************************	Configure Join and Projection Rules	Eorest name:	morpheus.int
Password: Domain: morpheus.int	P <u>a</u> ssword: Domain: Morpheus.int	Configure Deprovisioning	<u>U</u> ser name:	srvmiis
	<u>A Back</u> <u>Next</u> Cancel Help	Configure Extensions	P <u>a</u> ssword:	**********
< <u>Back</u> <u>Next</u> > <u>Cancel</u> Help			Domain:	morpheus.int
				< Back Next > Cancel Help
	Click next			

	👸 Create Management Agent		X
	Management Agent Designer Create Management Agent	Configure Directory Partitions Select directory partitions:	Show All
👹 Select Cont	Connect to Active Directory Forest	×	
Builden Builde	mputers main Controllers eignSecurityPrincipals astructure MAndFound DS Quotas ServiceAccount Jsers ouLUX Servers V Users Users gram Data tem		n settings: controllers (optional) <u>Configure</u> ain controllers I Sign and encrypt LDAP traffic entials this directory partition <u>Set Credentials</u> artition: <u>Containers</u> a password synchronization source. ronization targets: <u>Largets</u>
<u>A</u> dvanced	. OK (	Cancel Help	ack <u>N</u> ext > Cancel Help

For security reasons we will instruct the agent to process users containers. This choice will not only increase the overall performance of the parsing engine but will also prevent unattended containers from being processed. In fact should support personnel create thousands of email addresses in new containers they will not be processed until an MIIS administrator (in our case the Security Team) updates the rule.

# Object Types

Some objects are mandatory like containers or CN.

Management Agent Designer       Select Object Types         Properties       Diject types:         Configure Directory Partitions       Diject types:         Select Object Types       Select Object Types         Select Attributes       Configure Connector Filter         Configure Attribute Flow       group         Configure Deprovisioning       inetOrgPerson         Configure Extensions       user
Connect to Active Directory Forest         Configure Directory Partitions         → Select Object Types         Select Attributes         Configure Connector Filter         Configure Join and Projection Rules         Configure Attribute Flow         Configure Deprovisioning
Connect to Active Directory Forest         Configure Directory Partitions         ⇒ Select Object Types         Select Attributes         Configure Connector Filter         Configure Join and Projection Rules         Configure Attribute Flow         Configure Deprovisioning
⇒ Select Object Types       ✓ container         ⇒ Select Attributes       ✓ domainDNS         ⊆ configure Connector Filter       □ inetOrgPerson         Configure Join and Projection Rules       ✓ organizationalUnit         Configure Attribute Flow       ✓ user         Configure Deprovisioning       ✓ user
→ Select Object Types       ✓ domainDNS         Select Attributes       □ group         Configure Connector Filter       □ inetOrgPerson         Configure Join and Projection Rules       ✓ organizationalUnit         Configure Attribute Flow       ✓ user         Configure Deprovisioning       ✓
Select Attributes       group       Image: Configure Connector Filter       imatOrgPerson       Image: Configure Connector Filter       Image: Connector
Configure Connector Filter       ImiteDrgPerson
Configure Attribute Flow User
Configure Deprovisioning
Configure Extensions
OK Cancel Help

Next select the relevant attributes described in service view chapter

Attributes

CN

Mail

ProxyAddresses

Extensionattribute1

SAMAccount Name

# **Filters**

Filter for contact If an object satisfies this filter, it b remaining management agent rule Build Filter				cessed any	further by the	×	
Data source attribute: <dn> cn extensionAttribute1 mail proxyAddresses</dn>	Deperator: Equals Does not equal Starts with Does not start w Ends with Does not end with Contains Does not contain Is present Is not present	th th	<u>V</u> alue: active			⊐ §°	
	Add Condition	<u>R</u> emove C	ondition				
Data Source Attribute	Operator	Value					
extensionAttribute1	Equals	active					
		OK		Cancel	Help		

Email internet account must have the exchange extensionattribute1 set to "active" to be processed.

Join and Projection Rules

👹 Properties						×
Management Agent Designer	Configure Join and Project	tion Rules				
Properties	Data Causa Obicat Tur			Join	Desirent	
Connect to Active Directory Forest	Data Source Object Typ	e		No	Project No	
Configure Directory Partitions	contact container			No	No	
	domainDNS			No	No	
Select Object Types	organizationalUnit			No	No	
Select Attributes	user			Yes	Yes	
Configure Connector Filter						
⇒ Configure Join and Projection Rules						
Configure Attribute Flow						
Configure Deprovisioning	Join and projection rules	for: <b>user</b>				
						. — I I
Configure Extensions	Mapping Group	Action	Metaverse Object	Туре	Resolution	Ê
	□ 1	Join	Any		No	Ť
	n nail	Direct Direct	cn mail			
		Direct				
	sAMAccountName	Direct	employeeID			
	2	Project	person			
	1		1		· · ·	
	New <u>J</u> oin Rule	New <u>P</u> roje	ction Rule	<u>E</u> dit	<u>D</u> elete	
l]						
					1	
			OK	Cance	el Help	

# Attribute Flow

Properties Connect to Active Directory Forest	Data Source Attribute	Metaverse Attribute		
Connect to Active Directory Forest		histareise Attibute	Туре	Flow Nulls
Configure Directory Partitions Select Object Types Select Attributes Configure Connector Filter Configure Join and Projection Rules	Object Type: user     cn     mail     proxyAddresses     sAMAccountName	Object Type: perso → cn → mail → proxyAddresses → employeeID	on Direct Direct Direct Direct	
Configure Attribute Flow Configure Deprovisioning Configure Extensions	Build Attribute Flow Data <u>source</u> object type: user Data s <u>o</u> urce attribute: <dn> cn extensionAttribute1 mail proxyAddresses sAMAccountName</dn>	<ul> <li>Mapping Type</li> <li>Direct</li> <li>Advanced</li> <li>Flow Direction</li> <li>Import</li> <li>Export</li> <li>Allow Nglis</li> <li>Delete</li> </ul>	Metaverse object person Metaverse attrib <object-id> assistant c cn co comment company department</object-id>	•



Management Agent Designer     Construction       Properties     Connect to Active Directory Forest       Configure Directory Partitions     Select Object Types       Select Attributes     Select Attributes
Configure Connector Filter Configure Join and Projection Rules Configure Attribute Flow → Configure Deprovisioning Configure Extensions



🤯 Create Management Agent 🔀 🔀 🔀			
Management Agent Designer	Configure Directory Partitions		
Create Management Agent	Select directory partitions:		
Connect to Active Directory Applicati		- 1	
⇒ Configure Directory Partitions	CN=Configuration,CN={BB343939-25E0-4990-A537-52B0E4BB7E03}		
Select Object Types	CN=Schema,CN=Configuration,CN={BB343939-25E0-4990-A537-52B0E4 DC=morpheus,DC=com		
Select Attributes			
Configure Connector Filter			
Configure Join and Projection Rules			
Configure Attribute Flow			
Configure Deprovisioning		F	
Configure Extensions			
	J	_	
	Select Containers:		
	Containers		
	,		
	< <u>B</u> ack <u>N</u> ext > Cancel Help		



👹 Properties 🛛 🔀			
Management Agent Designer	Select Object Types		
Properties	Object types:	Show All	
Connect to Active Directory Application		<u></u>	
Configure Directory Partitions	container		
⇒ Select Object Types	domainDNS		
Select Attributes	inetOrgPerson		
Configure Connector Filter	organizationalUnit		
Configure Join and Projection Rules	user		
Configure Attribute Flow			
Configure Deprovisioning			
Configure Extensions			
I	P		
		OK Cancel Help	



👹 Properties			×
Management Agent Designer	Select Attributes		
Properties	A <u>t</u> tributes:	Show All	
Connect to Active Directory Applicati	division		1
Configure Directory Partitions	employeeID		-11-9
Select Object Types			
⇒ Select Attributes	facsimileTelephoneNumber		
Configure Connector Filter	🔲 🗖 givenName		1
Configure Join and Projection Rules	homePhone		
Configure Attribute Flow	initials		
Configure Deprovisioning			
Configure Extensions	III I mail IIII IIII manager		
	nTSecurityDescriptor		
	otherHomePhone		- 11
	otherTelephone		
	비밀애		
	pager		
	physicalDeliveryOfficeName		
	postalAddress		
			_
		OK Cancel Help	///

Select Mail, CN, Proxyaddresses, EmployeeID

🐉 Properties				×
Management Agent Designer	Configure Connector Filter			
Properties	Data Source Object Type	F	Filter Type	
Connect to Active Directory Applicat	container	1	None	
Configure Directory Partitions	domainDNS	1	None	
Select Object Types	inetOrgPerson	1	None	
Select Attributes	organizationalUnit	1	None	
➡ Configure Connector Filter				
Configure Join and Projection Rules				
Configure Attribute Flow	J			
Configure Deprovisioning	Filters for: container			
Configure Extensions	Filter Attribute	Operator	Value	
				Ŷ
				-
				-
				-
				-
		· · · · · · · · · · · · · · · · · · ·		
	Ne <u>w</u> <u>E</u> dit	<u>D</u> elete		
				1
		OK	Cancel Help	<u></u> //



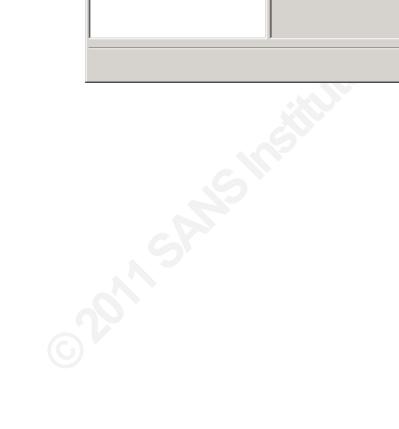
👹 Properties						×
Management Agent Designer	Configure Join and Proje	ction Rules				
Properties					<b>D</b> 1 1	
Connect to Active Directory Application	Data Source Object Ty	pe		Join	Project	
Configure Directory Partitions	container domainDNS			No No	No No	
2 ,	inetOrgPerson			Yes	Yes	
Select Object Types	organizationalUnit			No	No	
Select Attributes						
Configure Connector Filter						
⇒ Configure Join and Projection Rules						
Configure Attribute Flow	p					
Configure Deprovisioning	Join and projection rule	es for: inet(	DrgPerson			
Configure Extensions	Mapping Group	Action	Metaverse Object	Туре	Resolution	Ŷ
	⊡ 1	Join	Any		No	
	cn	Direct	cn			Î
	employeeID	Direct	employeeID			
	mail proxyAddresses	Direct Direct	mail proxyAddresses			
	proxyAddresses	Project	proxyAddresses			
			porton			
	New Join Rule	Nou Proie	ction Rule	Edit	Delete	
		New <u>F</u> lole		<u>c</u> ui(		
			ок	Cance	el Help	1
				Lance		



🐉 Properties					×
Management Agent Designer	Configure Attribute Flow				
Properties	Data Source Attribute		Metaverse Attribute	Туре	Flow Nulls
Connect to Active Directory Application	🗆 Object Type: inetOr_		Object Type: pers		
Configure Directory Partitions	cn III	-	cn	Direct	
Select Object Types	employeeID mail		employeeID mail	Direct Direct	
Select Attributes	proxyAddresses	Ţ	proxyAddresses	Direct	
Configure Connector Filter					
- Configure Join and Projection Rules					
⇒ Configure Attribute Flow					
Configure Deprovisioning	Build Attribute Flow				
Configure Extensions				Matana akia	
	Data <u>s</u> ource object type:		- Mapping Type	Metaverse objec	
	inetOrgPerson	-	Direct	person	<b>–</b>
	Data s <u>o</u> urce attribute:			Me <u>t</u> averse attrib	ute:
	<pre><dn></dn></pre>		C Advanced	<object-id></object-id>	<b></b>
	Cn , ,		- Flow Direction-	assistant	
	employeeID mail		Import	l c cn	
	proxyAddresses				
			C Export	comment	
			Allow N <u>u</u> lls	company department	-
	'		1		
	Ne <u>w</u> <u>E</u> dit		<u>D</u> elete		
	J				
			ОК	Cancel	Help



👹 Properties	X
Management Agent Designer	Configure Deprovisioning
Properties Connect to Active Directory Applicati Configure Directory Partitions Select Object Types Select Attributes Configure Connector Filter Configure Join and Projection Rules Configure Attribute Flow ➡ Configure Deprovisioning Configure Extensions	Specify what should happen to connector space objects when they are disconnected from the metaverse by either a provisioning rules extension or when the joined metaverse object is deleted.  Deprovisioning Options  Make them disconnectors Make them gxplicit disconnectors  Stage a delete on the object for the next export run Determine with a rules extension  Do not recall attributes contributed by objects from this management agent when disconnected.
	OK Cancel Help



👹 Properties		×
Management Agent Designer	Select Object Types	
Properties	Object types:	Show All
Connect to Active Directory Applicati		<u></u>
Configure Directory Partitions	container	
⇒ Select Object Types	domainDNS	
Select Attributes	inetOrgPerson	
Configure Connector Filter	organizationalUnit	
Configure Join and Projection Rules	user	
Configure Attribute Flow		
Configure Deprovisioning		
Configure Extensions		
l	P	
		OK Cancel Help



👹 Properties			×
Management Agent Designer	Select Attributes		
Properties	A <u>t</u> tributes:	🔲 <u>S</u> how All	
Connect to Active Directory Applicati	division	_	1
Configure Directory Partitions	employeeID		11.9
Select Object Types			
⇒ Select Attributes	facsimileTelephoneNumber		
Configure Connector Filter	givenName		
Configure Join and Projection Rules	homePhone		
Configure Attribute Flow	initials		
Configure Deprovisioning			
Configure Extensions	I ☑ mail □ manager		
	name		
	nTSecurityDescriptor		
	<b>  □</b> ∘		
	otherHomePhone		1
	otherTelephone		
	pager		
		•	
		-	1
		OK Cancel Help	///

Select Mail, CN, Proxyaddresses, EmployeeID

👹 Properties				×
Management Agent Designer	Configure Connector Filter			
Properties	Data Source Object Type		Filter Type	
Connect to Active Directory Applicati	container		None	
Configure Directory Partitions	domainDNS		None	-
Select Object Types	inetOrgPerson		None	
Select Attributes	organizationalUnit		None	
⇒ Configure Connector Filter				
Configure Join and Projection Rules				
Configure Attribute Flow	<u> </u>			
Configure Deprovisioning	Filters for: container			
Configure Extensions	Filter Attribute	Operator	Value	Ŷ
			Value	
				Î
	Ne <u>w</u> <u>E</u> dit	Delete		
		OK	Cancel Help	



👹 Properties						×
Management Agent Designer	Configure Join and Projec	ction Rules				
Properties	Data Causa Obiant Tu			Join	Designat	
Connect to Active Directory Application	Data Source Object Ty container	pe		No	Project No	
Configure Directory Partitions	domainDNS			No	No	
Select Object Types	inetOrgPerson			Yes	Yes	
	organizationalUnit			No	No	
Select Attributes						
Configure Connector Filter						
⇒ Configure Join and Projection Rules						
Configure Attribute Flow						
Configure Deprovisioning	$\Box$ Join and projection rule	s for: inet	OrgPerson			
Configure Extensions	Hereive Cours	d ation	- Holover Ohior	T	Resolution	
Configure Extensions	Mapping Group	Action	Metaverse Object	стуре		Î
	cn 🖾	Join Direct	Any cn		No	Ŧ
	employeeID	Direct	employeeID			<u> </u>
	mail	Direct	mail			
	proxyAddresses	Direct	proxyAddresses			
	2	Project	person			
	<u> </u>					
	New Join Rule	New <u>P</u> roje	ction Rule	<u>E</u> dit	<u>D</u> elete	
	F					
			ОК	Cance	el Help	



🐉 Properties					×
Management Agent Designer	Configure Attribute Flow				
Properties	Data Source Attribute		Metaverse Attribute	Туре	Flow Nulls
Connect to Active Directory Application	🗆 Object Type: inetOr_		Object Type: pers		
Configure Directory Partitions	cn III	-	cn	Direct	
Select Object Types	employeeID mail		employeeID mail	Direct Direct	
Select Attributes	proxyAddresses	Ţ	proxyAddresses	Direct	
Configure Connector Filter					
- Configure Join and Projection Rules					
⇒ Configure Attribute Flow					
Configure Deprovisioning	Build Attribute Flow				
Configure Extensions				Matana akia	
	Data <u>s</u> ource object type:		- Mapping Type	Metaverse objec	
	inetOrgPerson	-	Direct	person	<b>–</b>
	Data s <u>o</u> urce attribute:			Me <u>t</u> averse attrib	ute:
	<pre><dn></dn></pre>		C Advanced	<object-id></object-id>	<b></b>
	Cn , ,		- Flow Direction-	assistant	
	employeeID mail		Import	l c cn	
	proxyAddresses				
			C Export	comment	
			Allow N <u>u</u> lls	company department	-
	'		1		
	Ne <u>w</u> <u>E</u> dit		<u>D</u> elete		
	J				
			ОК	Cancel	Help



👹 Properties	X
Management Agent Designer	Configure Deprovisioning
Properties Connect to Active Directory Applicati Configure Directory Partitions Select Object Types Select Attributes Configure Connector Filter Configure Join and Projection Rules Configure Attribute Flow ➡ Configure Deprovisioning Configure Extensions	Specify what should happen to connector space objects when they are disconnected from the metaverse by either a provisioning rules extension or when the joined metaverse object is deleted.         Deprovisioning Options            • Make them disconnectors         • Make them gxplicit disconnectors         • Stage a delete on the object for the next export run         • Determine with a rules extension             • Do not recall attributes contributed by objects from this management agent when disconnected.
	OK Cancel Help

## **Agent Profiles**

Now that management agents are defined we need to tell them which steps are required to do their job. In fact an agent will use what is called "profiles" to execute a number of steps. A "profile" contains partition target, tasks such as import/export along with number of objects to process.

A "profile" will always contain a staging and synchronizing steps. The ADAM Agent profile adds an "export" step.

# Active Directory agent profiles

👹 Configure Run Profiles for "Activ	e directory agent"		×
Management agent run profiles:	Step details:		
Stage	Name	Value	<u>۱</u>
Synch	🗆 Step 1	Full Import (Stage Only)	_
	Log file	Stage_AD	Դ
	Number of Objects	0	- 1
	Number of Deletions		
	Partition	DC=morpheus,DC=int	
	Batch Size	100	
	Page Size	500	
	Timeout (seconds)	30	
			i i
			- P
			ł
New Profile Delete Profile		Ne <u>w</u> Step Edit Step Delete Step	
	0K <u>S</u> ci	ript Apply Cancel Help	

ADAM agent profile

👹 Configure Run Profiles for "ADAN	1 Agent"		×
Management agent run profiles:	Step details:		
Export	Name	Value	Ŷ
Stage	🗆 Step 1	Export	
Synch	Log file	export_adam	Ĵ
	Number of Objects	0	
	Number of Deletions		
	Partition	DC=morpheus,DC=com	
	Batch Size	100	
	Page Size	500	
	Timeout (seconds)	30	
New Profile Delete Profile		New Step Edit Step Delete Step	
	0K <u>S</u> ci	ript Apply Cancel Help	

## **Defining Metaverse Schema**

Let's add a "proxyAddress" attribute since it's missing in the default Metaverse schema. The main purpose will be to address multiple email addresses per user which is typical to any exchange infrastructure.

🐉 Identity Manager ( File Tools Actions H		EX						
Dperations 💡	Management.	Agents	🧾 Metav	verse Designer	🕡 Met	averse Searc	ch 🧾	Joiner
Metaverse Designer								
Object types								
Name		1	Add Atl	ribute To Obj	ect Type		X	
person			~					
organizationalUnit			<u>O</u> bject type	e name: 🛛 🗖	rson			
organization				lbe	13011			
locality			Available a	attributes:				
domain								
			밑ᇲ					нu
computer				Br				нu
printer								ĿШ
group								ĿШ
role								LU.
	0							EL
otal number of object typ Attributes	👸 New Attr	ibute				×		
Attributes								
Name	Attribute <u>n</u> an	ne:		roxyAddreses				
otherMailbox	<u></u>		l.	TONYHOUICSES				
ou	Attribute <u>type</u>		L.	tring (indexable)	1	<b>T</b>		
pager			13	ung (indexable)				
personalTitle								
physicalDeliveryOfficeN≀	🔽 Multi-valu	leđ						
postOfficeBox postalAddress						ttribu	ute	
postalCode	🔽 Indexed							
secretary								
seeAlso						I F	lelp	
sn								
st			OK	Cancel	Help	1 0		
street			OK			þ		
telephoneNumber		ang (naex		NU	NU			
title	9	tring (index	able)	No	No	0		

## **Provisioning engine rules**

One of the main purpose of the processes we are putting in place is to provision and de-provision the ADAM instance. The metaverse provisioning rule will meet this purpose. This component must be defined as a .NET assembly DLL. Only one assembly can be defined. The .NET technology is beyond the scope

of this document. However this report will focus on the specific MIIS implementation. Further details can be found at www.microsoft.com/miis

👹 Options		×
Metaverse Rules Extension		
Enable metaverse rules ext	ension	
Rules extension n <u>a</u> me:	MVProv_01 Browse	
<u>B</u> un this rules extension	in a separate process	
Enable Provisioning Ru	les Extension	
Create Rules Extension	n Project Re <u>s</u> et	
Global Rules Extension Set	tings	_
$\Box$ <u>U</u> nload extension if the dur	ation of a single operation exceeds: 60 📑 second	ls :
	Reset	
WMI Password Managemer	t Settings	<u> </u>
Sa <u>v</u> e last 24 💼	password change/set event details	
Password Synchronization		
Enable Password Synchror	ization	
	OK Cancel Help	

First provisioning capability must be selected into the metaverse options pane.

A name of an assembly DLL must be submitted.

Provision Rule between the Metaverse and ADAM Connectors.

This rule is executed whenever a change occurs in the metaverse or joining or disconnecting occurs between MetaVerse and Space Connectors.

It means we only need to implement "provision" method from IMVSynchronization Interface

using System;

using Microsoft.MetadirectoryServices;

```
namespace Mms Metaverse
```

{

```
/// <summary>
```

 $///\ {\rm This}$  implements the metaverse business rule to properly provision ADAM space connector

/// </summary>

{

public class MVExtensionObject : IMVSynchronization

{

public MVExtensionObject()

// TODO: Add constructor logic here

```
void IMVSynchronization.Initialize ()
```

{

// TODO: Add initialization logic here

Frederic Dumesle

11

11

```
}
           void IMVSynchronization.Terminate ()
            {
                 11
                 // TODO: Add termination logic here
                 11
            }
           void IMVSynchronization.Provision (MVEntry mventry)
            {
                 ConnectedMA ManagementAgent; // Management Agent Object
                                             // Distinguished name
                 ReferenceValue DN;
attribute
                 string Container;
                                           // Container name
                 string RDN;
                                               // Relative distinguished
name strings
                 CSEntry csentry;
                                              // Connector space entry
objects
                 // let's first determine the state of the metaverse object.
                 // let's check whether an employee has a mail attribute
                 if (mventry["mail"].IsPresent)
                      // ok employeestatus has been provisioned in the MV
                  {
```

```
Container = "DC=morpheus,DC=int";
RDN = "CN=" + mventry["cn"].Value;
try
{
    // it's alright let's build container and
```

rdn

// let's work on ADAM

ManagementAgent =

mventry.ConnectedMAs["ADAM"];

DN= ManagementAgent.EscapeDNComponent(RDN).Concat(Container);

csentry =
ManagementAgent.Connectors.StartNewConnector("inetOrgPerson");

}

{

}

}

}

Frederic Dumesle

csentry.DN = DN;

csentry.CommitNewConnector();

```
catch (ObjectAlreadyExistsException e)
```

// the object is already there we just

skip it

53

bool IMVSynchronization.ShouldDeleteFromMV (CSEntry csentry, MVEntry mventry)

```
{
    //
    // TODO: Add MV deletion logic here
    //
    throw new EntryPointNotImplementedException();
    }
}
```

#### Deployment

The MIIS product does not feature a built in task scheduler. Specific actions must be either manually triggered or scripted through WMI or invoked through .NET Code. The next paragraph will focus on c# Generated code. The main reason is that the .NET framework security infrastructure will provide us with more advanced security options than the vbscript engine even though we will lose some flexibility. Furthermore this implementation is a perfect example of defense in-depth principles.

#### Code Security and "agent profile" invocation

We need to execute a number of steps for each agent at least daily.

The Active Directory management agent must execute a stage step once and a synch step. The ADAM management agent must process a stage once and synch and export step. We will rely on windows operating system scheduler but let's generate the c# code first. Open the management agent and select the relevant profile click

```
Securing Windows 20003 with Feature Packs v 0 16
"script" and save your file selecting "c#". Here is the output
file
using System;
using System.Management;
class Sample ExecuteMA
{
   public static int Main( string[] args )
    {
        try
        {
            11
            // Credentials must only be specified when Microsoft
Identity Integration Server is on remote system.
            11
            ConnectionOptions opt = new ConnectionOptions();
            opt.Authentication =
AuthenticationLevel.PacketPrivacy;
            // opt.Username = "Domain\\Me";
            // opt.Password = "MyPassword";
            // ManagementScope myScope = new ManagementScope(
"\\\MyServer\\root\\MicrosoftIdentityIntegrationServer", opt );
            11
            ManagementScope myScope = new ManagementScope(
"root\\MicrosoftIdentityIntegrationServer", opt );
```

Frederic Dumesle

55

```
SelectQuery myQuery = new SelectQuery(
"MIIS ManagementAgent", "GUID='{3C222539-6284-4F18-94E4-
6EDF88364759}'");
            ManagementObjectSearcher searcher = new
ManagementObjectSearcher( myScope, myQuery );
            foreach ( ManagementObject ma in searcher.Get() )
            {
                Console.WriteLine( "Active directory
agent.Execute( \"Synch\" )..." );
                ma.InvokeMethod( "Execute", new object[1] {
"Synch" } );
            }
        }
        catch ( Exception ex
        {
            Console.WriteLine( "Error: " + ex.Message );
        }
        return 0;
}
This working sample can be fine-tuned to more advance logging
(log to event viewer, etc...). Once compiled you get an
executable. You can then use the .NET security wizard to adjust
```

Securing Windows 20003 with Feature Packs v 0 16

by the scheduler using a limited service account. The only requirement is being part of the MIIS Operators local group.

the executable security. Furthermore this task will be executed

#### Monitoring and Logging and Troubleshooting

The MIIS Identity manager provides you with detailed statistical information about agent execution, object statistics, etc....You can also explore freely each connector space from the GUI.

In a production environment you would rely on professional products like (MOM, NetIQ, etc...) to gather statistics from either the event viewer, WMI or your own mechanism.

### MIIS Installation Guide

🙀 Identity In	itegration Feature Pack Setup Wizard 🛛 🛛 🔀
	erform either a complete or custom installation of the Identity In Feature Pack.
Select the	type of installation you want to perform:
<b>i</b> ∰	C Cu <u>s</u> tom You can select the Identity Integration Feature Pack components you want to install.
	< <u>B</u> ack <u>N</u> ext > Cancel

🖁 Identity Integration Feature Pack S	etup Wizard	_ 🗆 X
Service Account Information Service account information is needed for to operate in the correct security contex		
Provide the service account name, pass service account the Identity Integration	word, and domain or local computer nan Feature Pack currently uses.	ne of the
Service account:	SrvMIIS	
<u>P</u> assword:	****	
Domain or local computer name:	morpheus.int	
	< <u>B</u> ack <u>N</u> ext >	Cancel

MIIS will run under a service account that will also be used to authenticate to active directory

### Scalability and Redundancy Factor

The ADAM software supports scalability through Microsoft Layer 3 NLB cluster implementation. This allows higher load and redundancy. It's also possible to deploy multiple instances of ADAM replicas. They will automatically replicate using the same mechanisms as the one used by Active Directory

MIIS being involved as an asynchronous process (it's not a real time process) it's not required to have high availability at the service level. What can be done is ensuring that the SQL database is hosted on highly available clusters.

#### **Operational Readiness**

The updated infrastructure brings updated processes. Mainly a separated staging environment will be used to qualify any Frederic Dumesle

Securing Windows 20003 with Feature Packs v 0 16

change. A separated lab environment will be setup as well as part of new change control.

#### Back-up

All components are backed up regularly on removable media. Furthermore annual exercises are practiced in the lab infrastructure to ensure data can be successfully recovered.

ADAM data is located in a single place while MIIS complete configuration lives at the SQL level.

#### Monitoring

ADAM LDAP directory is easy to monitor from an external source. The application runs as a service thus any windows operating system service monitoring tool is available.