KOENIG
step forward

Implementing Microsoft Identity Manager (MIM) 2016

Duration: 4 Days

Module 1: Introducing Microsoft Identity Manager

This module involves a tour of many of the built-in features of MIM through the user experience, in which the student becomes familiar with the interface, the high level architecture, and the business needs MIM addresses. At this point you see the 'finished article' – the rest of the course is spent understanding how this works, and building the 'finished article' from a raw installation. The lab is a walkthrough of creating a new user and managing groups and credentials for that user – as well as the experience of that new user.

Module 2: The Synchronization Service Manager

In this module we introduce the MIM Synchronization Service Manager and explain its features through scenarios that do not use the MIM Portal. We introduce the main tools (Metaverse Designer, Operations Tool, Joiner etc.), and we cover basic configuration of a Management Agent along with run profiles, verifying results, and simple Metaverse searches. During the lab, a new Management Agent (MA) is created for a simple HR system.

Module 3: More about Synchronization

Here we look at various types of MA, including LDAP and file based sources, with the particular emphasis on Inbound and Outbound Synchronization. We cover in detail: filters, join and projection rules, connectors and disconnectors, provisioning, deprovisioning, different kinds of attribute flow etc. In the lab, two more MAs are created, and a simple data driven scenario for managing a directory (AD LDS) is established.

Module 4: The MIM Service and Portal

We then examine the MIM Service and application database, introducing key concepts such as sets, workflows and policies, and how permissions are granted. Next we look at how the MIM Service integrates with the MIM Synchronization Service, and how data flows between them. The labs build a MIM MA and flows our HR data from the Synchronization Service to the portal, and portal data to the Synchronization Service.

Module 5: Managing Synchronization from the Portal

In this module we cover the concept of portal based Synchronization Rules, and how they compare with the "Classic" Rules we have considered so far. We go on to consider how and

where to use Portal Synchronization Rules, Workflows, and Management Policy Rules (MPRs), including more complex attribute flows. We examine the special considerations required when managing Active Directory user accounts. The labs make use of Synchronization Rules. The lab also covers configuring MIM so that users are automatically created (provisioned) into AD, renamed, and removed (deprovisioned) as necessary.

Module 6: Credential management

Primarily this module is about passwords. We mention Certificate Management, but this is a large subject that has a course of its own. We discuss self-service password reset in detail (including text message, email and 'MFA' approaches) – we also discuss self-service account unlocking (new with MIM). We cover password synchronization. The labs cover nearly all aspects of password management in MIM, with the exception of some more advanced topics (like writing custom password management workflows and extensions), or configuration which is hard to do in a classroom environment (like Azure MFA).

Module 7: Group management

This module covers the management of distribution and security groups – including the relationship between groups in AD and other systems. More work is done on Synchronization Rules, Workflows, and MPRs. We cover the configuration of workflow approvals. The labs build on our scenario to include the management of various types of groups in AD.

Module 8: Other considerations

In this module we draw together the threads of what is perhaps the most important feature of the MIM Service – MPRs: the different types, different uses, how they are processed and how to troubleshoot them. We then look at some operational considerations, including the management of run cycles using scripts, and also backup, restore, and disaster recovery. Various labs cover additional features of MPRs and provide experience in the operational matters. The last of these labs puts the finishing touches on what has – perhaps surprisingly – turned out to be quite a thorough proof-of-concept system. This module also gives an overview of two "extensions" to MIM's capabilities: Roles Based Access Control, and Privileged Access Management.