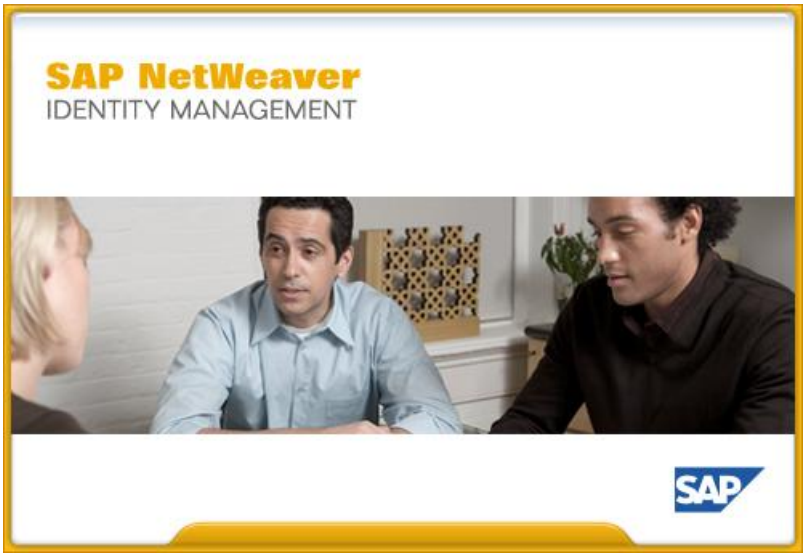
# SAP NetWeaver® Identity Management Connector Development Kit

## Overview




Version 7.2 Rev 2

# Preface

## The product

The SAP NetWeaver Identity Management Connector Development Kit enables independent software vendors (ISVs) or SAP partners to create an Identity Management connector for their application, and to integrate the application into the Identity Management landscape.

The Connector Development Kit contains information necessary for development of an Identity Management connector – criteria, guidelines, templates, test tool, certification guide, etc.

## The reader

This manual is written for people who wish to create the Identity Management connector for their application.

## Prerequisites

To get the most benefit from this manual, you should have the following knowledge:

- Thorough knowledge of the Identity Center.
- Thorough knowledge of the Virtual Directory Server or other vendor specific module.

## The manual

This manual gives an overview of the Identity Management connector architecture and the creation process – from the design to the certification of the connector.

## Related documents

You can find useful information in the following documents:

- *SAP NetWeaver Identity Management Security Guide.*
- *SAP NetWeaver Identity Management Operations Guide.*
- *SAP NetWeaver Identity Management Connector Development Kit Implementing the Virtual Directory Server Connector*.
- *SAP NetWeaver Identity Management Connector Development Kit Virtual Directory Server Connector Testing Tool*.
- *SAP NetWeaver Identity Management Connector Development Kit Certification.*

Virtual Directory Server tutorials:

- *SAP NetWeaver Identity Management Virtual Directory Server Tutorial Accessing databases.*
- *SAP NetWeaver Identity Management Virtual Directory Server Tutorial Accessing LDAP servers.*

- *SAP NetWeaver Identity Management Virtual Directory Server Tutorial Joining data sources.*
- *SAP NetWeaver Identity Management Virtual Directory Server Tutorial Performing dynamic add operations.*

Identity Center tutorials:

- *SAP NetWeaver Identity Management Identity Center Tutorial – Provisioning.*
- *SAP NetWeaver Identity Management Identity Center Tutorial – Working with roles and privileges.*

# Table of contents

# Introduction

The SAP NetWeaver Identity Management is a general purpose identity management application which provides the functions and services needed to integrate distributed identity data in the system landscape to efficient, heterogeneous identity lifecycle management. The prime objective is to centrally manage and keep all identity data within the enterprise up-to-date. You can use SAP NetWeaver Identity Management for processing identity information in a variety of ways, depending on your system landscape. Some typical identity management operations are:

- Create and delete accounts (users).
- Set password on an account.
- Disable account, to prevent login.
- Update/modify account, e.g. new telephone number, address or other user information.
- Grant and revoke authorization to use a resource.
- Create and delete group objects.
- Add/remove users to/from groups.

## The purpose of the Identity Management Connector Development Kit

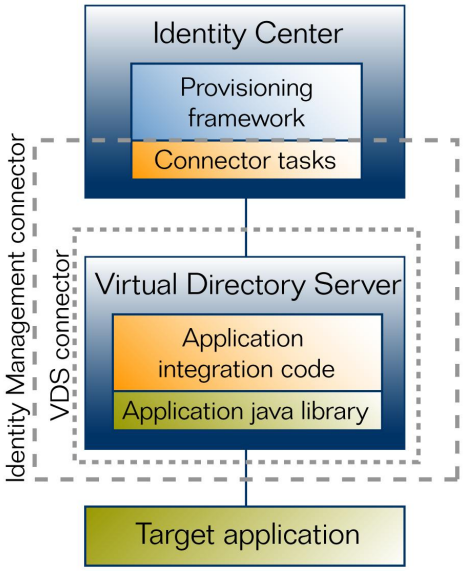
The purpose of the Connector Development Kit (CDK) is to enable the independent software vendors (ISVs) or SAP partners to create an Identity Management connector for their application, and to integrate the application in the Identity Management landscape.

## Architecture overview

SAP NetWeaver Identity Management consists of two components:

- Identity Center (IC): The Identity Center is the primary component used for identity management. The Identity Center includes functions for identity provisioning (based on roles and rules, it will create accounts and give access rights in target applications), entry modifications, access right revoking, and deleting of entries, workflow, password management, logging, and reporting. It uses a centralized repository, called the identity store, to provide a uniformed view of the data, regardless of the data's original source. The Identity Center retrieves the data from these various repositories, consolidates it, transforms it into the necessary formats, and publishes it back to the various decentralized repositories.
- Virtual Directory Server (VDS): The Virtual Directory Server is a component provided by SAP NetWeaver Identity Management that acts as a single access point for clients retrieving or updating data in multiple data repositories, as it provides a uniformed view of the data in real-time. It logically presents information in a virtual directory tree. Different users and applications can, based on their access rights, get different views of the information. You can use the Virtual Directory Server e.g. to consolidate multiple repositories and then as a data source for the Identity Center. You then use Identity Center for provisioning and performing identity management functions.

The Identity Management Connector Development Kit makes it possible for the independent software vendors (ISVs) to create a connector for their application, and to integrate the application in the Identity Management landscape. It is recommended that the new connectors are created using the architecture model shown below. The dotted gray rectangles in the illustration show what is considered the connector.




The integration work (creation of the Identity Management connector) involves the following:

- The connector tasks from the provisioning framework in the Identity Center: A set of default tasks need to be customized to work together with the target application.
- The application integration: The generic core Virtual Directory Server code is extended – a code is written to interface the Virtual Directory Server with the application Java library (it must be a Java library), which the Virtual Directory Server again uses to connect to the target application. A Virtual Directory Server connector (VDS connector) is created with an LDAP/SPML interface to the application, which is used by the Identity Center for provisioning.

The provisioning framework in the Identity Center is the core of the provisioning, and will call the basic tasks to perform the operations in the target systems, i.e. the framework populates the Identity Center with a set of basic tasks for performing provisioning.

The Identity Center connects to the Virtual Directory Server using either LDAP or SPML. The Virtual Directory Server processes the incoming requests, executes them on dedicated target applications (in usually different form/protocol than received) and returns the results of the operations. Among other features, the generic core VDS code will do the following:

- Enforce authentication and authorization.
- Execute (multiple) attribute mappings.
- Enforce the processing rules as configured in the Virtual Directory Server configuration.
- Route the request to appropriate target application (using the Virtual Directory Server virtual tree), etc.

The processing of the requests is then handed over to the application integration code invoking the appropriate connector operation. The connector has the information about the target application and has the necessary knowledge to transform the input requests from the original format to the target format and execute requested operations, but depends on the target drivers for low-level knowledge. Normally such low-level target drivers are delivered in form of multiple JAR files that expose low-level target application API. The application integration code can be viewed as the glue between the core VDS code and the target drivers. It will accept the requests from the core code and, implementing the low-level target application API from the driver, carry out operation on the target application.

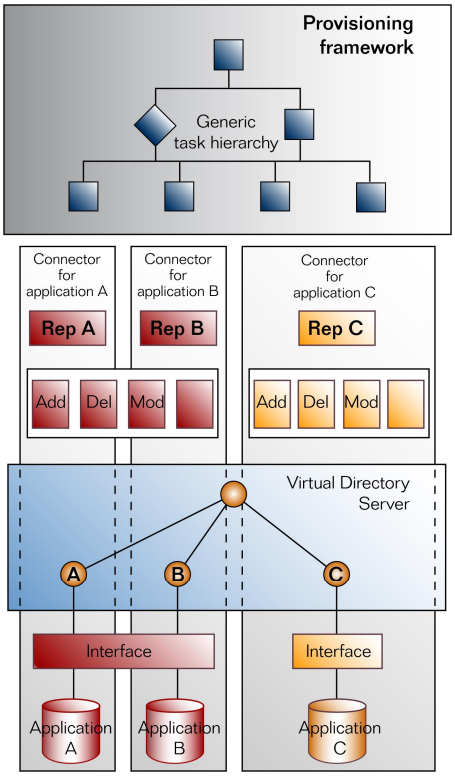
Using the Virtual Directory Server for the integration gives some advantages:

- Standard protocols (LDAP and SPML) are being used, which means that a generic interface to the application is created, which can also be used for other integration purposes than identity management.
- The Virtual Directory Server connector (application integration code and the application Java library) implementation can be done stand-alone with the Virtual Directory Server without having to deploy a complete identity management solution.

However, using Virtual Directory Server to create Identity Management connector is not mandatory, and optionally a vendor specific module can be used instead. The subsections below are describing the deployment architecture and the data flow of the recommended solution using the Virtual Directory Server.

## The deployment architecture

One Virtual Directory Server can be used to connect to multiple applications. The top layer of the figure shows a sample provisioning framework responsible for issuing of the calls to the connectors. Each connector consists of a number of connector tasks, which are called as part of the provisioning framework, and connects to the Virtual Directory Server using LDAP or SPML.



The Virtual Directory Server will, based on the starting point of the operation, forward the request to the correct target application, shown at the bottom in the illustration.

### Data flow

Upon invocation of the connector (as a result of the request operation), the generic core VDS code delivers the following to the integration code:

- All known properties about the processed request.
- All configuration properties that may influence the execution of the request on the target application.

The information that the core VDS code passes to the application integration code depends on the type of the operation that is processed (add/modify/delete/search), but there are also generic pieces of the information that are always passed (e.g. a standard set of attributes).

The application integration code will utilize API exposed by the target driver. The main task is to obtain and prepare the data needed by the target application API for successful execution of the operation on the target application.

After successful processing of the request, the results of the executed requests are delivered to the core VDS code (where they later can be post-processed and delivered to target application). Since the core VDS code cannot cope with various data structures returned by the target application, the integration code (together with the target application API) is responsible for preparing and converting of the low-level results to well defined Virtual Directory Server structures.

## Terminology

| | |
|---|---|
| Core VDS code | Generic Virtual Directory Server code that needs to be extended in order to integrate with the target application. |
| Application integration code | A code that is written to interface the Virtual Directory Server with the target application Java library. The application integration code can be viewed as the glue between the core VDS code and the target drivers. It will accept the requests from the core code and, implementing the low-level target application API from the driver, carry out operation on the target application. |
| Application Java library | The target application API. The connector depends on the target drivers for low-level knowledge. Normally such low-level target drivers are delivered in form of multiple JAR files that expose low-level target application API, which Virtual Directory Server again uses to connect to the target application. |
| VDS connector | This is the Virtual Directory Server part of the Identity Management connector extending the Virtual Directory Server with application integration code and application Java library. |

| | |
|---|---|
| Target application | The application the connector is created for. |
| Connector tasks | A set of default tasks from the provisioning framework that need to be customized to work together with the target application. |
| VDS structures | Data structures recognized by the Virtual Directory Server (the core VDS code), i.e. data returned by the target application needs to be converted to these well defined Virtual Directory Server structures in order to be recognized by the Virtual Directory Server. |
| (Identity Management) connector | Consists of default connector tasks from the provisioning framework in the Identity Center and the Virtual Directory Server connector – core VDS code, application integration code with the target application API in the Virtual Directory Server. |
| Virtual Directory Server Connector Testing Tool | The Virtual Directory Server Connector Testing Tool is developed to test the VDS connectors. It has the capacity to test both the connector functionality and the connector performance with high precision. In addition, it is possible to run instructions testing, and instructions and expected results testing. |
| Provisioning framework | The provisioning framework for SAP systems provides a set of templates that you can reference when you set up the system-specific jobs used for your provisioning use case. It is the core of the provisioning, and will call the basic tasks to perform the operations in the target systems. |

# Creating the Identity Management Connector: Process overview

This section describes the steps involved in creating an Identity Management connector. It is recommended to start with a simple approach, and add more advanced functionality over time.

Using Virtual Directory Server for creation of Identity Management connector is optional. A vendor specific module can be used instead, and it that case should all the Virtual Server Directory steps defined in the process be replaced with the vendor specific module details.

# Defining the interface

First step is designing the interface, which operations the new connector will support. The following needs to be considered:

- Which identity object types exist in the target application, and which of these will be implemented in the first version
  - Basic identities (i.e. people).
  - Does the application also have a concept of groups, which the users can belong to, and do the groups have to be managed?
- Which attributes need to be exposed in the interface
  - It needs to be defined which attributes are single value, multi value, which attributes have special syntax, which attributes are mandatory etc.
  - How are authorizations handled? In the Identity Center, there will be a privilege object for each authorization in the target system. When the privilege object is assigned, a task is executed which will call the interface to create the authorization in the target system.

## The interface tasks

The interface consists of a number of tasks, each serving a specific purpose. These tasks are called as part of the provisioning framework for SAP systems, e.g. Create (add) user, Delete user, etc.

# Implementing the Virtual Directory Server Connector

A Java code needs to be written in the Virtual Directory Server, to forward the incoming LDAP or SPML requests received by the Virtual Directory Server to the API of the target application. This implementation can be done stand-alone, and the result of this implementation is creating an LDAP/SPML interface toward the application.

The simplest way of creating the new Virtual Directory Server connector is to use the Generic Data Source.xml template provided in the Virtual Directory Server.

See document *SAP NetWeaver Identity Management Connector Development Kit Implementing the Virtual Directory Server Connector* available on the SAP Developer Network (SDN).

# Stand-alone testing

When the application integration code and the API are created, the Virtual Directory Server connector can be tested to verify the core functionality. This can be done using any LDAP or SPML application, or by using the sample test application, Virtual Directory Server Connector Testing Tool, which is part of the development kit.

In order to test your VDS connector (independently of the way the code is created), you will have to create a Virtual Directory Server configuration that will at least have the following properties:

- Data source with connection properties details for your target application.
- Configured connector name (the one you are developing).
- Virtual tree and at least one node that points to the data source in question.

See document *SAP NetWeaver Identity Management Connector Development Kit Virtual Directory Server Connector Testing Tool* available on the SAP Developer Network (SDN).

# Certification

SAP offers integration and certification support for their partners and independent software vendors (ISVs) that wish to certify their products.

SAP partners and ISVs are assisted by SAP during their product integration projects. They are offered consulting, certification testing and test system access services independently. The actual development is executed by the ISVs. It is recommended that ISVs build up some knowledge about the relevant SAP solutions and on integration topics in-house, attend SAP training classes or work with SAP Service Partners.

See document *SAP NetWeaver Identity Management Connector Development Kit Certification* available on the SAP Developer Network (SDN) for more.

# Packaging and documentation

Before the product is ready for shipment, it must be packaged. The following is required:

- Necessary target application Java libraries.
- An initial data set needs to be provided by the partner (the number of entries has to be at least 300). It is a partner's responsibility also to provide the necessary documentation for the correct installation of the initial data set.
- Identity Center, including the Identity Management User Interface, deliverables:
    - Job and the connector tasks in the Identity Center necessary for the certification process (a repository definition, a job which reads entries from the target application and a search job, a job for creating of account privilege, tasks for adding, modifying and deleting a user, and a User Interface task for editing of a user), with installation and configuration documentation as described in *SAP NetWeaver Identity Management Connector Development Kit Certification.*
    - (Optional) Identity store schema extension: if the connector requires any identity store schema extensions, these need to be provided for import (an exported .mcc file). Store the exported schema file the folder *IC files* in the connector certification package as described in *SAP NetWeaver Identity Management Connector Development Kit Certification.*

- Virtual Directory Server deliverables (Optional, not to be delivered if vendor specific (connector) module is used instead of Virtual Directory Server):
  - Virtual Directory Server (VDS) configuration (as template): as explained in *SAP NetWeaver Identity Management Connector Development Kit Implementing the Virtual Directory Server Connector*.
  - (Optional) Data Source configuration (as template): as explained in *SAP NetWeaver Identity Management Connector Development Kit Implementing the Virtual Directory Server Connector*.
  - Connector class (compiled for JDK 1.4 or 1.5) or as source file (stored in the Virtual Directory Server configuration file). The class is stored in <VDS_dir>\configurations in a folder with the same name as your configuration file.

  ***Note:***
  *Whether the class should be compiled for JDK 1.4 or 1.5 will depend on which AS Java version the connector class is to be deployed on. Compiling the class for JDK 1.4, the Virtual Directory Server configuration that utilizes this class will be deployable on AS Java versions 7.0, EHP 1 for SAP NW CE 7.1, SAP NW CE 7.2 and SAP NW 7.3. Compiling for JDK 1.5 will result in connector not being deployable on AS Java 7.0 versions.*
- Vendor specific (connector) module (Optional, only delivered if used instead of Virtual Directory Server).
- Documentation deliverables:
  - Functionality description sheet which documents the purpose of the connector, which features are supported, as well as entry types and attributes. The documentation must be submitted in English only (PDF) as described in *SAP NetWeaver Identity Management Connector Development Kit Certification.*
  - Installation and configuration documentation for the connector tasks and jobs, and the repository definitions in the Identity Center. The documentation must be submitted in English only (PDF) as described in *SAP NetWeaver Identity Management Connector Development Kit Certification.*
  - Installation and configuration documentation for the Virtual Directory Server connector (configuration with the code and the API) need to be included in the documentation. The documentation must be submitted in English only (PDF). Optionally, if a vendor specific connector is used instead of Virtual Directory Server connector, then a detailed installation and configuration documentation for the vendor connector is necessary instead, as described in *SAP NetWeaver Identity Management Connector Development Kit Certification.*