P20 POLIZEI 20/20

P20 Directory Synchronization

Identity Governance Service

Release 1.0.0

P20 GEMEINSAM. DIGITAL. VERNETZT.

P20 Directory Synchronization

Publication date 2023-06-17

by Sylvert Bernet

Program	Polizei 20/20
Program Director	Holger Gadorosi
Project Manager	Norbert Linde
Document Titel	P20 Directory Synchronization
Version	1.0
Creation Date **Created By**	2023-04-29 Sylvert Bernet
Latest Update **Latest Update By**	2023-04-29 Sylvert Bernet

Revision History

Revision	Date	Author	Reference
1.0	2023-04-29	Sylvert Bernet	No previous document

Table of Contents

Preface

Purpose of this document

This document describes the usage of the Directory Synchronization and is intended for resource administrators and system integration teams.

Typographical Conventions

The following table describes the typographic changes that are used in this document.

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Symbol Conventions

The following table explains symbols that might be used in this document.

Convention	Meaning
[ ]	Contains optional arguments and command options.
{ | }	Contains a set of choices for a required command option.
${ }	Indicates a variable reference.
-	Joins simultaneous multiple keystrokes.
+	Joins consecutive multiple keystrokes.
>	Indicates menu item selection in a graphical user interface.

Introduction

Directory service synchronization is a process in which data transferred from one directory service as a data source to another directory service as a data sink. The data therefore only flows in one direction.

The categories of data considered within the synchronization include:

- Organizational Structures
- Global Roles
- Scoped Roles

Scoped roles in this context represent authorization objects that are effective within a specific organizational level only.

Architecture

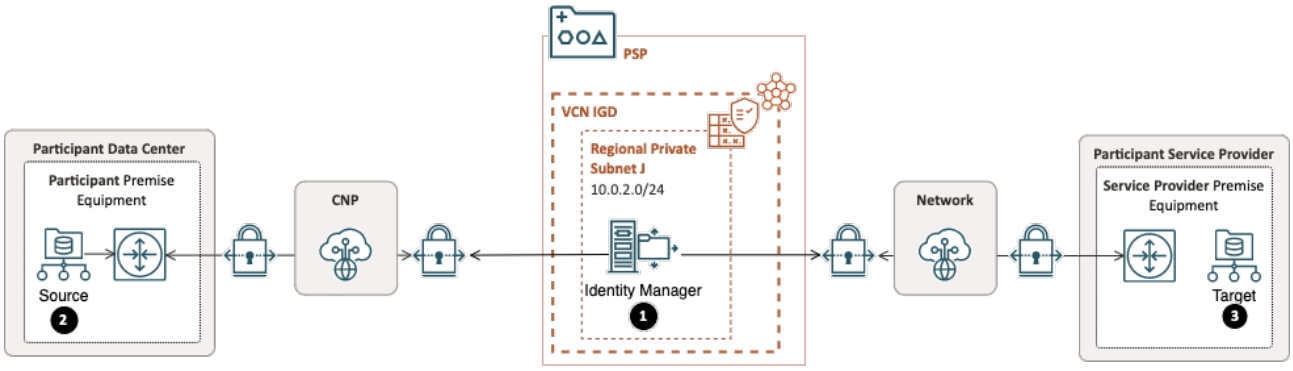
The architecture illustrates the components provisioned on the PSP for the Directory Synchronization.

Within the PSP VCN' there exist two types of subnets:

- public (Public Subnet)
- private (Subnet and Data Subnet)

Resources deployed into the public subnets will receive a public IP address and will be publicly visible on the CNP. There is no component deployed in this subnets.

Resources deployed into the private subnets receive only a private IP address and hence are not publicly visible on the CNP, improving the security of those resources. The Identity Manager deployed in private subnets.



Components

#	Component	Description
1	Identity Manager	This is the central part of the provided functionality. This is where the core functionality is implemented and the configuration endpoints of the source and destination directory services are hosted.Hier wird die Kernfunktionalit?t implementiert und die Konfigurationsendpunkte der Quell- und Zielverzeichnisdienste gehostet.
2	Source	The source of the syncronization process.
3	Target	The target of the syncronization process.

Process

Source

The source directory has to provide following branches in a subtree that belongs to a target directory.

Branch	Object Class	Description
Organization	organizationalUnit	Any entry in this subtree represents an organizational unit. The entries in this subtree **MAY** organized in hierarchy.
Global Roles	groupOfUniqueNames	Each entry in this subtree represents a global role. The entries in this subtree **MUST NOT** organized in hierarchy.
Scoped Roles	groupOfUniqueNames	Each entry in this subtree represents a global role mapped to an organizational unit (scoped role). The mappeing is provided by concatenating the name of the organizational unit the role belongs to and the name of the role itself separated by an underscore. The entries in this subtree **MUST NOT** organized in hierarchy.

Target

The target directory has to provide following branches in a subtree as a target of the synchronization process.

Branch	Object Class	Description
Organization	organizationalUnit	Any entry in this subtree represents an organizational unit.
Global Roles	groupOfUniqueNames	Each entry in this subtree represents a global role.
Scoped Roles	groupOfUniqueNames	Each entry in this subtree represents a global role mapped to an organizational unit (scoped role). The mappeing is provided by concatenating the name of the organizational unit the role belongs to and the name of the role itself separated by an underscore.