P20 Directory Synchronisation

Identity Governance Service

Version 1.0.0

GEMEINSAM. DIGITAL. VERNETZT.

P20 Directory Synchronisation

Veröffentlicht 29.04.2023

von Sylvert Bernet

Dokumenteninformation	
Programm	Polizei 20/20
Programmleiter	Holger Gadorosi
Projektleiter/Verantwortlicher	Norbert Linde
Dokumententitel	P20 Directory Synchronisation
Version	1.0
Erstellt am **Erstellt von**	29.4.2023 Sylvert Bernet
Zuletzt bearbeitet am **Zuletzt bearbeitet von**	29.4.2023 Sylvert Bernet

Versionshistorie			
Version	**Datum**	**Autor**	**Verweis**
1.0	29.04.2023	Sylvert Bernet	Kein vorheriges Dokument

Inhaltsverzeichnis

Vorwort

Zweck dieses Dokuments

Dieses Dokument beschreibt die Nutzung der Directory Synchronization und richtet sich an Administratoren von Ressourcen und Teams für die Integration von Zielsysteme.

Typografische Konventionen

In diesem Dokument werden die folgenden typografische Konventionen verwendet.

Konvention	Bedeutung
fett	Fettschrift kennzeichnet Elemente der grafischen Benutzeroberfläche, die einer Aktion zugeordnet sind, oder Begriffe, die im Text oder im Glossar definiert sind.
kursiv	Kursivschrift kennzeichnet Buchtitel, Hervorhebungen oder Platzhaltervariablen, für die Sie bestimmte Werte angeben.
`monospace`	Monospace-Schrift kennzeichnet Befehle innerhalb eines Absatzes, URLs, Code in Beispielen, Text, der auf dem Bildschirm angezeigt wird, oder Text, den Sie eingeben.

Symbol Konventionen

In diesem Dokument werden die folgenden Konventionen für Symbole verwendet.

Symbol	Bedeutung
[ ]	Enthält optionale Argumente und Befehlsoptionen.
{ | }	Enthält eine Reihe von Auswahlm öglichkeiten für eine erforderliche Befehlsoption.
${ }	Referenziert eine Variable.
-	Verbindet gleichzeitig mehrere Tastenanschläge.
+	Verbindet mehrere aufeinanderfolgende Tastenanschläge.
>	Zeigt die Auswahl eines Menüpunkts in der grafischen Benutzeroberfläche an.

Einführung

Bei der Synchronisierung von Verzeichnisdiensten handelt es sich um einen Prozess, bei dem Daten von einem Verzeichnisdienst als Datenquelle in ein weiteren Verzechnisdienst als Datensenke übertragen werden. Der Daten fließen demzufolge nur in eine Richtung.

Zu den Datenkategorien, die bei der Synchronisierung berücksichtigt werden, geh?ren:

- Organisationsstrukturen
- Globale Rollen
- Scoped Rollen

Scoped Rollen stellen in diesem Zusammenhang Berechtigungsobjekte dar, die nur innerhalb einer bestimmten Organisationsebene wirksam sind.

Architektur

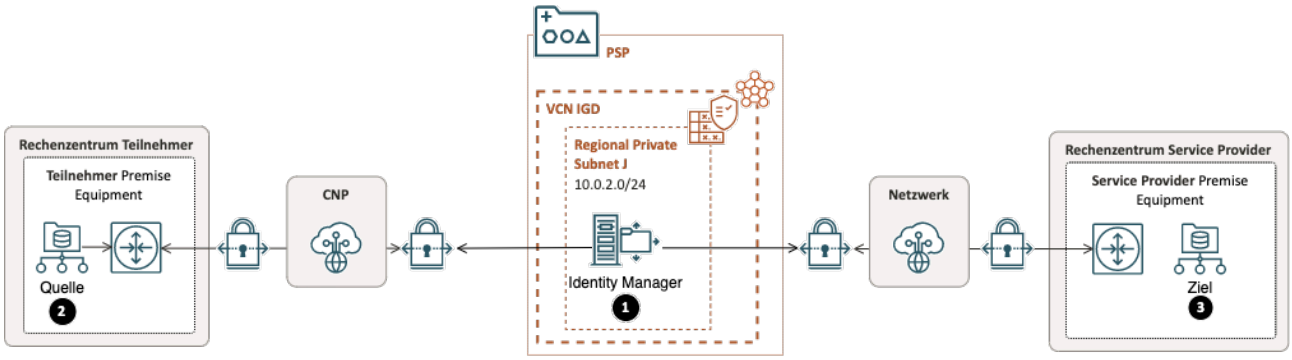
Die Architektur veranschaulicht die auf der PSP für die Verzeichnissynchronisierung bereitgestellten Komponenten.

Innerhalb der PSP VCN's gibt es zwei Arten von Subnetzen:

- public (Öffentliches Subnet)
- private (privates Subnet und Daten-Subnet)

In den öffentlichen Subnetzen bereitgestellte Ressourcen erhalten eine öffentliche IP-Adresse und sind im CNP öffentlich sichtbar. In diesen Subnetzen ist keine Komponente bereitgestellt.

In den privaten Subnetzen bereitgestellte Ressourcen erhalten nur eine private IP-Adresse und sind daher im CNP nicht öffentlich sichtbar, was die Sicherheit dieser Ressourcen verbessert. Die Serviceinstanzen werden in privaten Subnetzen bereitgestellt.



Komponenten

#	Komponente	Beschreibung
1	Identity Manager	Dies ist der zentrale Teil der bereitgestellten Funktionalit?t. Hier ist die Kernfunktionalit?t implementiert und die Konfigurationsendpunkte der Quell- und Zielverzeichnisdienste gehostet.
2	Quelle	Die Datenquelle des Synchrinisationsprozesses.
3	Senke	Die Datenquelle des Synchrinisationsprozesses.

Prozess

Datenquelle

Das Quellverzeichnis muss folgende Zweige in einem Teilbaum bereitstellen, der zu einem Zielverzeichnis gehört.

Zweige	Objektklasse	Beschreibung
Organisation	organizationalUnit	Jeder Eintrag in diesem Teilbaum repräsentiert eine Organisationseinheit. Die Einträge in diesem Unterbaum **KÖNNEN** hierarchisch organisiert sein.
Globale Rollen	groupOfUniqueNames	Jeder Eintrag in diesem Teilbaum repräsentiert eine globale Rolle. Die Einträge in diesem Unterbaum **DÜRFEN NICHT** hierarchisch organisiert sein.
Scoped Roles	groupOfUniqueNames	Jeder Eintrag in diesem Teilbaum stellt eine globale Rolle dar, die einer Organisationseinheit zugeordnet ist (bereichsbezogene Rolle). Die Zuordnung erfolgt durch die Verkettung des Namens der Organisationseinheit, zu der die Rolle gehört, und des Namens der Rolle selbst, getrennt durch einen Unterstrich. Die Einträge in diesem Unterbaum **DÜRFEN NICHT** hierarchisch organisiert sein.

Datensenke

Das Zielverzeichnis muss folgende Zweige in einem Teilbaum als Ziel des Synchronisierungsprozesses bereitstellen.

Zweige	Objektklasse	Beschreibung
Organisation	organizationalUnit	Jeder Eintrag in diesem Teilbaum repräsentiert eine Organisationseinheit.
Globale Rollen	groupOfUniqueNames	Jeder Eintrag in diesem Teilbaum repräsentiert eine globale Rolle.
Scoped Roles	groupOfUniqueNames	Jeder Eintrag in diesem Teilbaum stellt eine globale Rolle dar, die einer Organisationseinheit zugeordnet ist (bereichsbezogene Rolle). Die Zuordnung erfolgt durch die Verkettung des Namens der Organisationseinheit, zu der die Rolle

Zweige	Objektklasse	Beschreibung
		gehört, und des Namens der Rolle selbst, getrennt durch einen Unterstrich.