


Solution de Gestion des Identités
CeVIF

Le Moteur de Synchronisation



Identity Manager

IdM est une solution de gestion des identités offrant une combinaison de solutions de gestion d'identités, de provisioning, de self service, de gestion de mot de passe, et d'audit

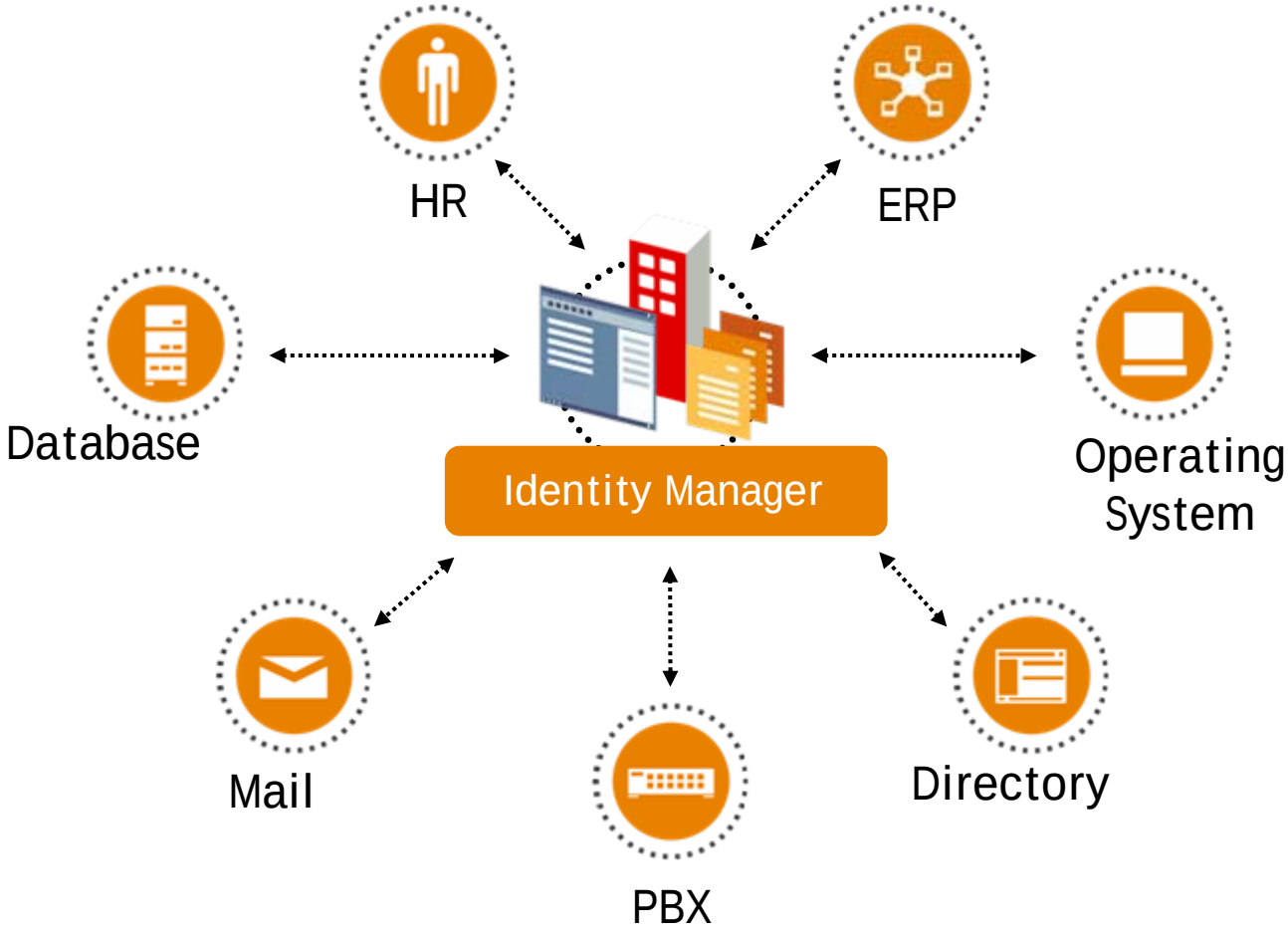
Identity Manager était connu dans sa première version sous le nom de DirXML®.

Fonctionnalités

- Identity Manager offre les fonctionnalités suivantes :
  - Le provisioning
  - La gestion des mots de passe
  - Un self-service utilisateur
  - Une configuration graphique des règles avec l'outil Policy Builder
  - Le gestion de rôles (RBAC)
  - L'audit et la gestion de rapports
  - Une fonction d'annuaire pages blanches

Les même types de données sont isolées dans différentes bases

Ces données sont accessibles depuis un annuaire consolidant l'ensemble des informations



Autorité sur les données

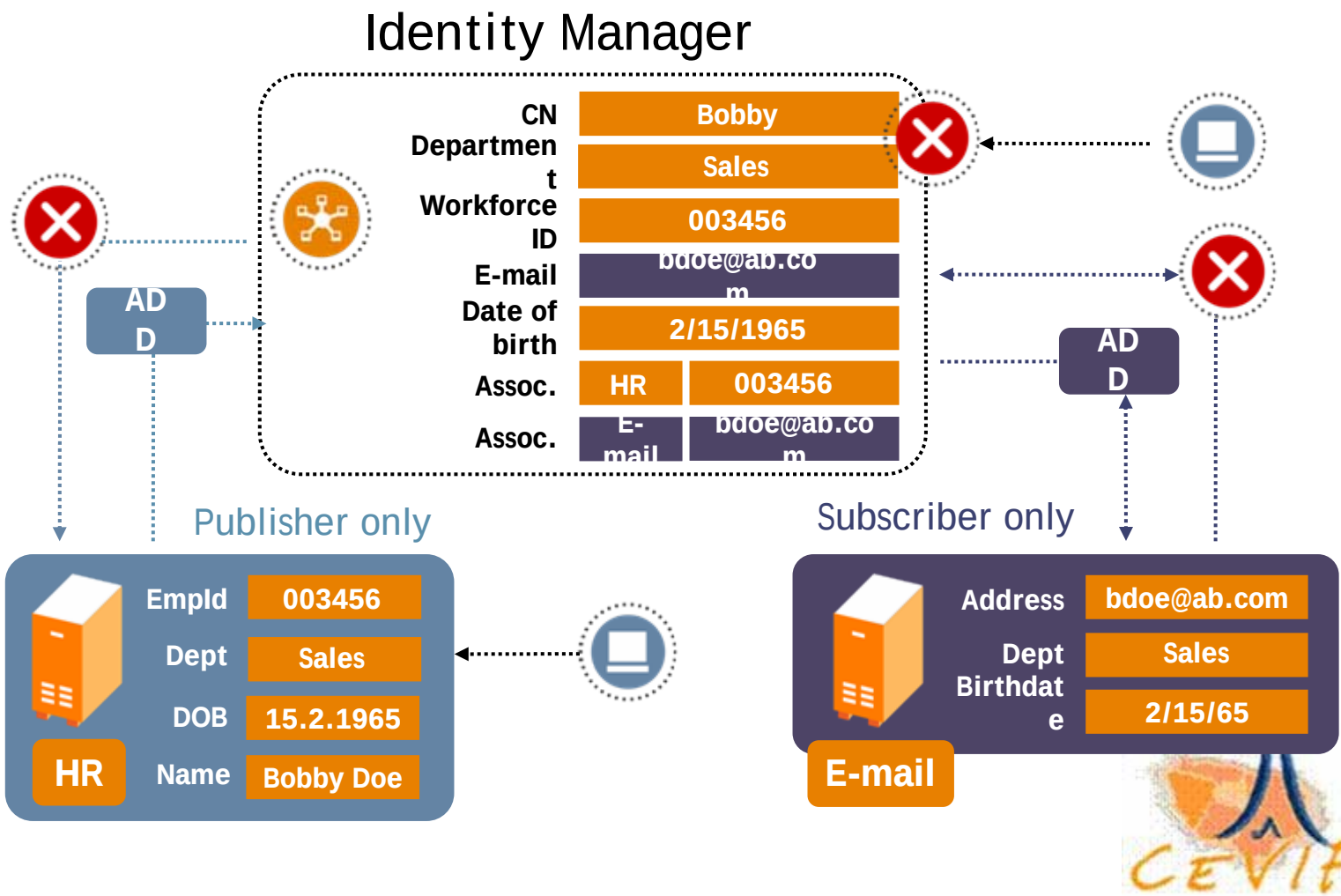
Les organisations doivent pouvoir contrôler les flux de données entre les applications

L'intégrité et la sécurité des données doivent être maintenues

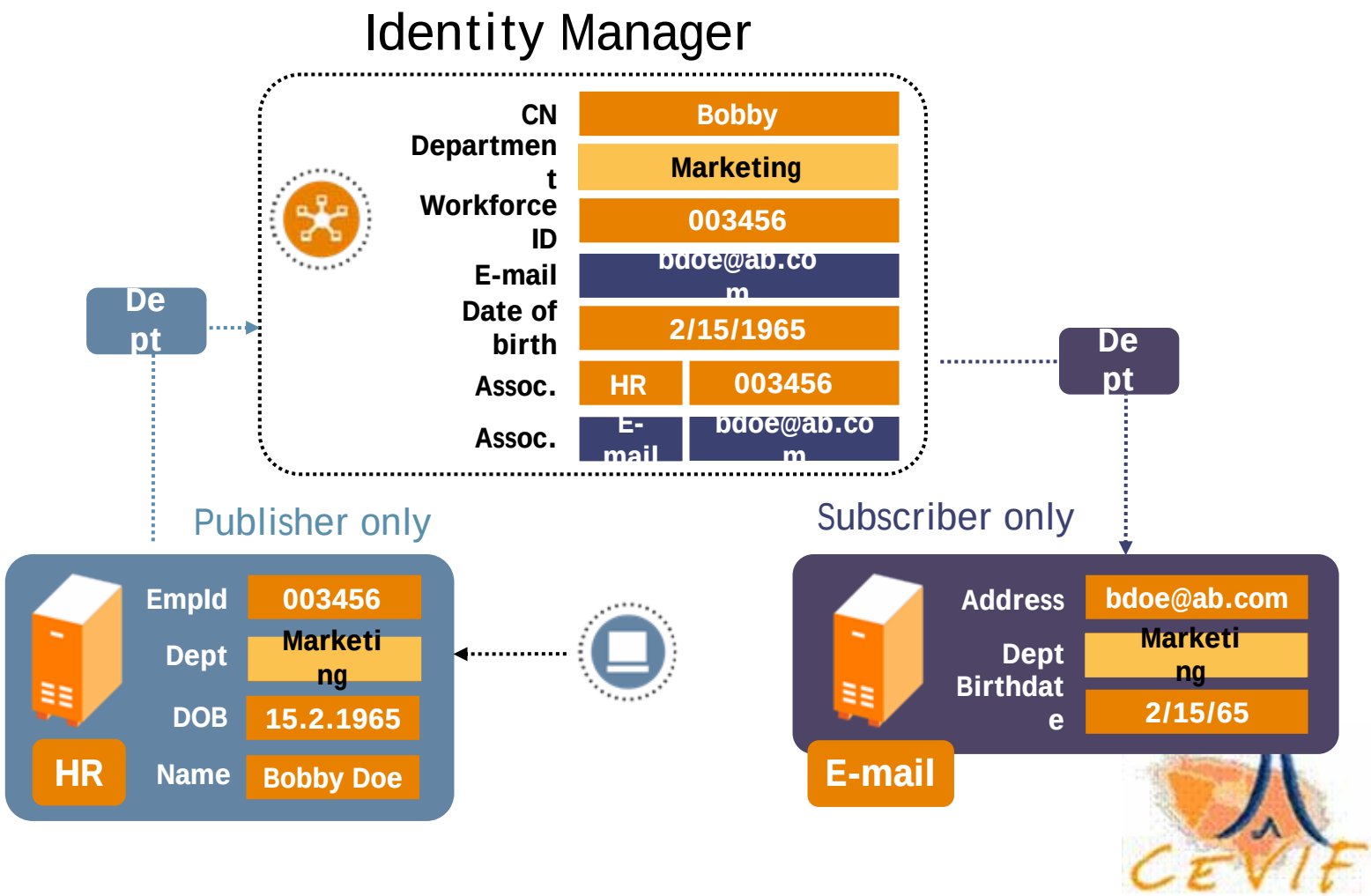
NIM fournit une solution permettant de contrôler de manière sécurisée les données par l'intermédiaire des stratégies de règles, les filtres et les connexions sécurisées

Avec NIM il est possible de définir les applications propriétaires des données et les applications avec lesquelles ces données sont partagées.

Le provisioning et les sources de données



Le provisioning et les sources de données



Associations

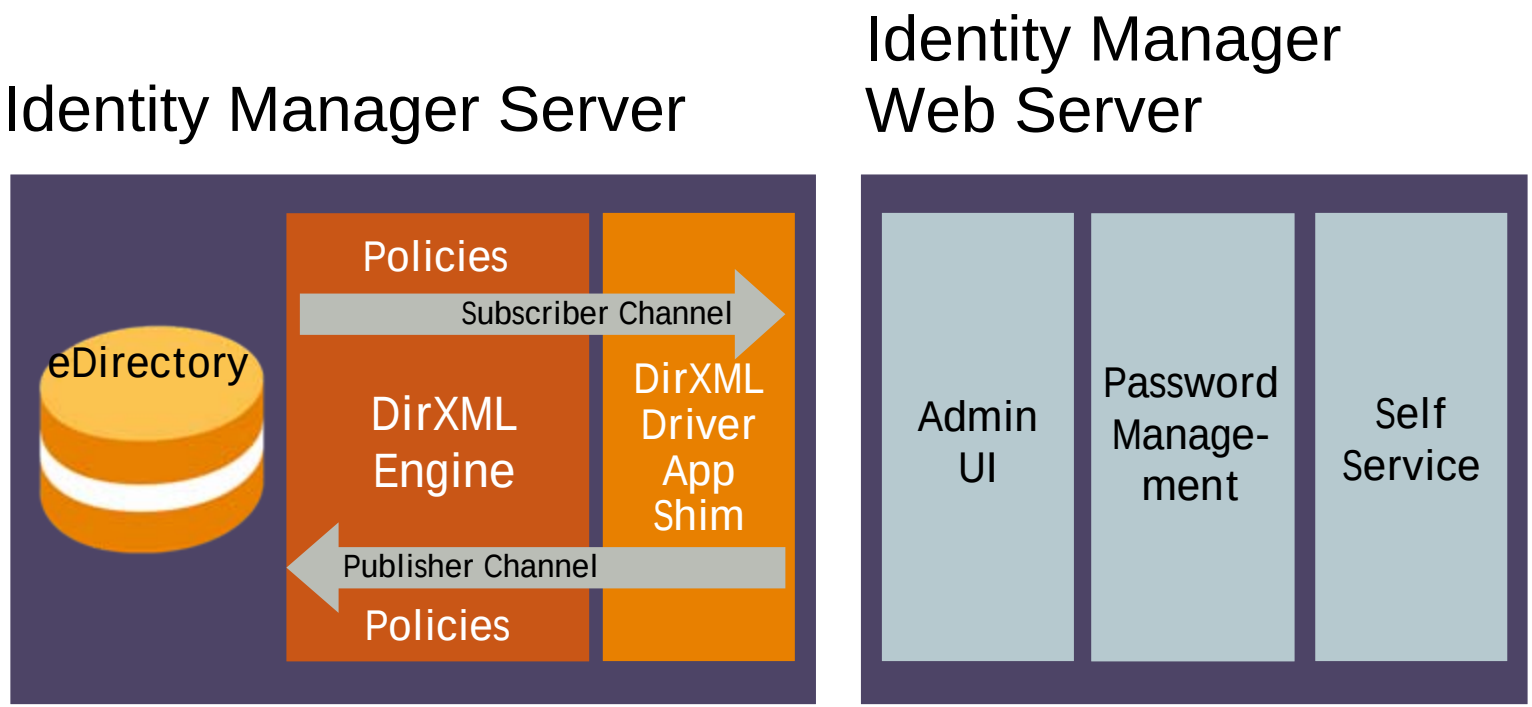
L’association est utilisé pour lier un objet présent dans une application connectée avec un objet correspondant dans l’annuaire eDirectory

L’application connectée (connecteur) fournit un “Unique Object Identification” qui est inscrit sur l’objet correspondant dans l’annuaire eDirectory. Cette référence correspond à l’ *association*.

NIM devient le “*hub”* et gère le processus de liens (association) avec un ou plusieurs systèmes connectés.

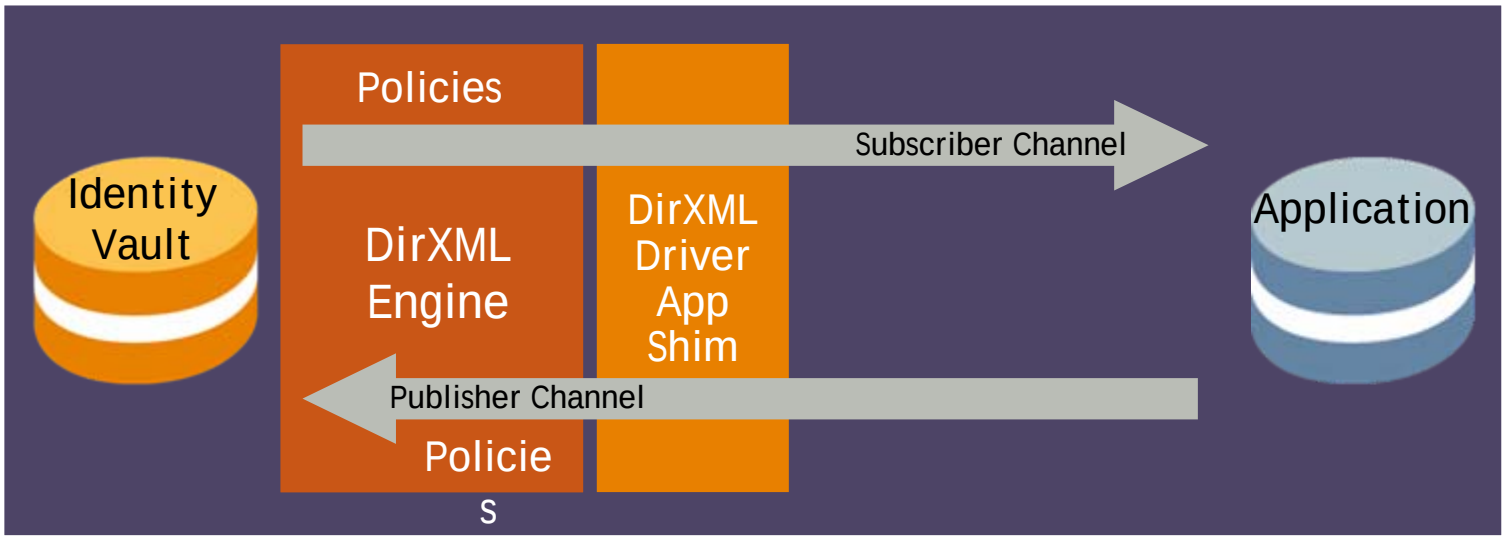
Cette association peut être réalisée sur la base de critères particuliers

Architecture NIM

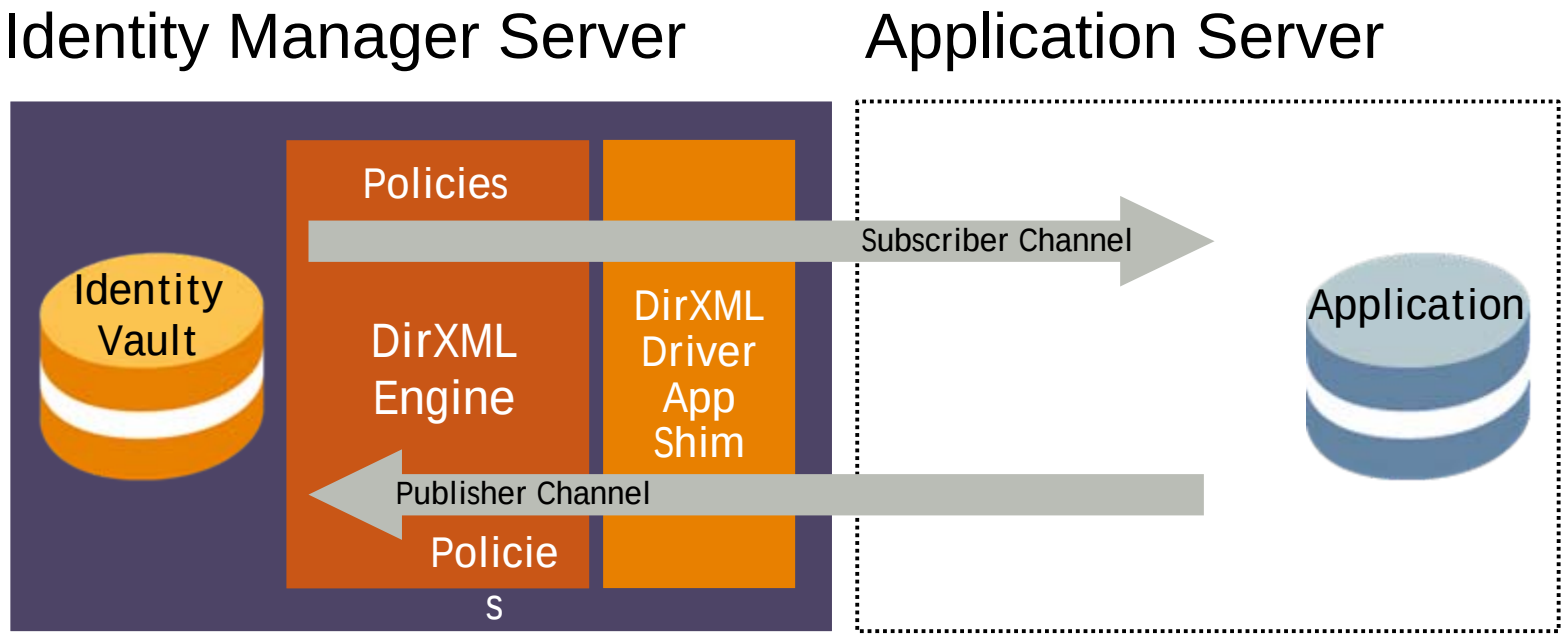


Architecture avec un serveur

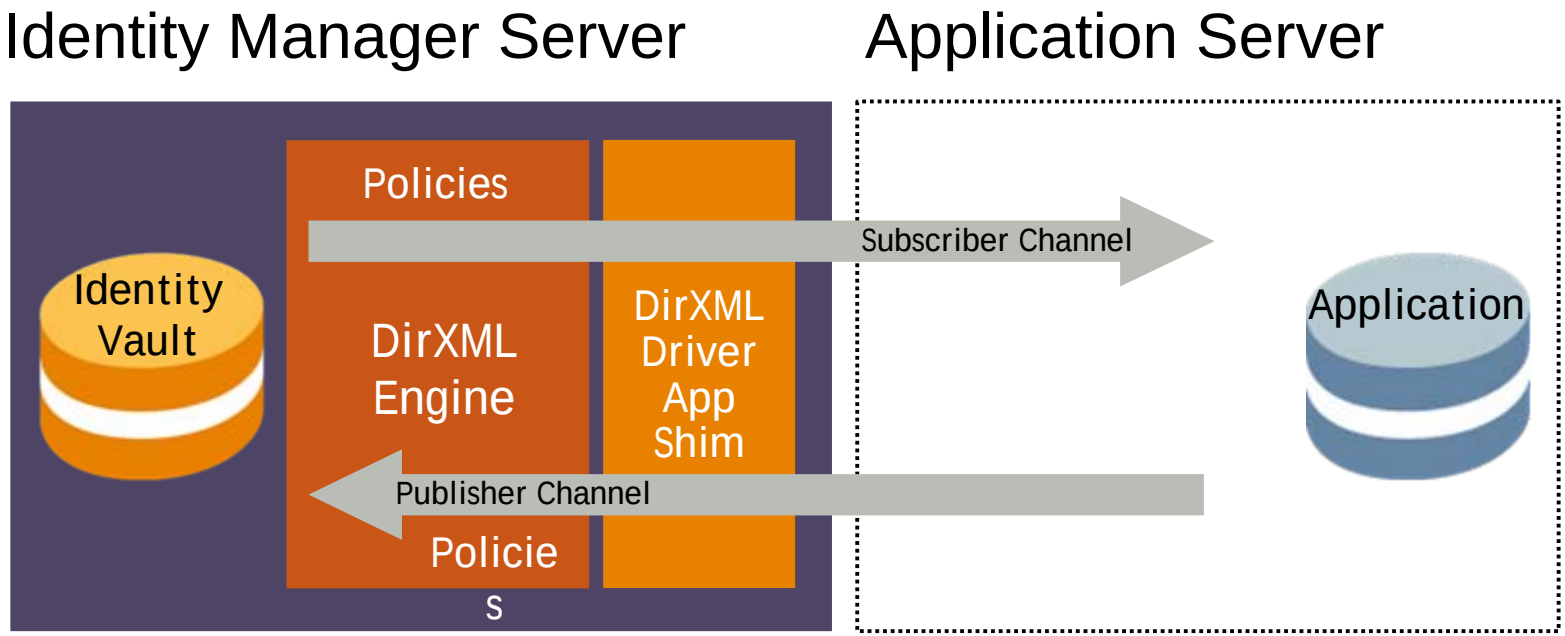
Identity Manager Server



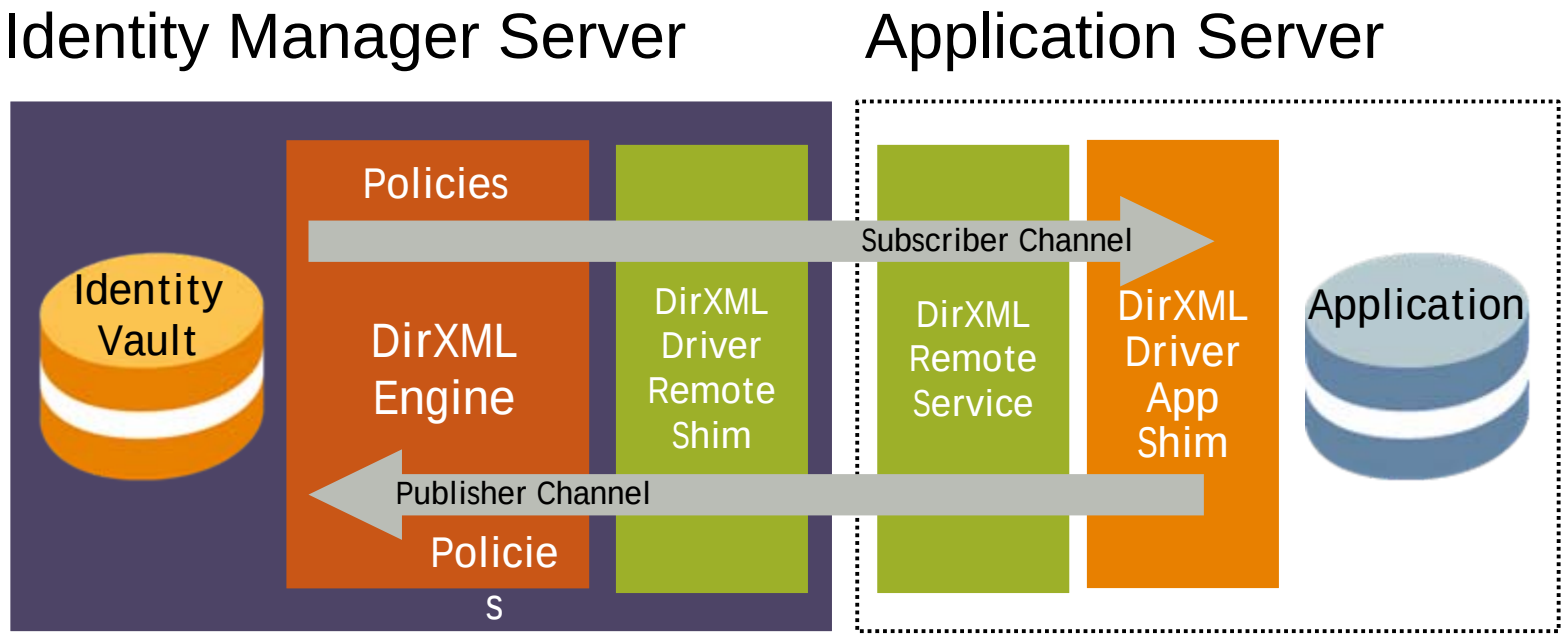
Architecture accès à distance



Architecture accès à distance



Architecture accès à distance



Le référentiel des identités

eDirectory

- Héberge les méta données
- Héberge les définitions de stratégies de règles pour un connecteur particulier
- Maintien les liens entre les utilisateurs et leur applications respectives
- Héberge les stratégies de gestion des mots de passe
- Gènère les évènements et les propage vers les applications abonnées.

Moteur DirXML

DirXML Engine

Interface avec eDirectory

- Supporte la gestion de connecteurs multiples
- Traite et assure la propagation des évènements de eDirectory
- Détection et gestion des “Event loop-back”

Moteur de jointure

- Réalise les transformations des données
- Réalise les processus basés sur les filtres
- Traite les stratégies de régles
- Processeur XSLT

DirXML Driver Shim

DirXML Driver App Shim

Interface XML

- Génère et reçoit les documents XML
- Document Object Model

API Application

Service de Remote Loader

Service de Remote Loader

- Est exécuté sur la machine distante
- Permet d'établir une connexion distante vis à vis de l'application
- Le moteur DirXML et le "Driver Shim" peuvent être exécutés sur différents systèmes d'exploitation (moteur sous Linux et Lotus Notes sous Windows)

Console du Remote Loader

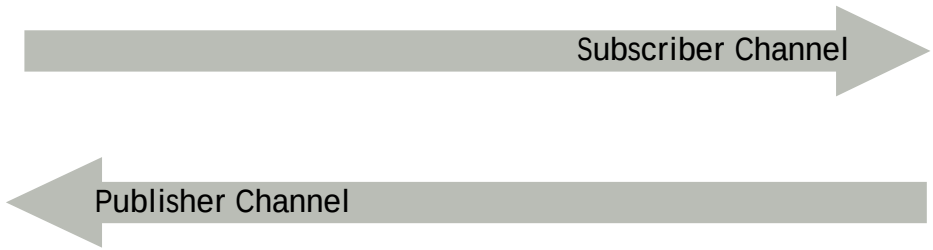
- Outil pour configurer et maintenir le service Remote Loader

Canaux de publication et d'abonnement

NIM est une technologie de type "publish" (publication) et "subscribe" (abonnement).

Les canaux de Publication et de Subscription sont vus côté application connectée:

- L'application publie dans l'annuaire eDirectory
- L'application "subscribes" s'abonne aux données depuis eDirectory



Identity Manager Policies

Une **policy set** est une collection de policies sur un type de régle

- exemple placement policy

Une **policy** consiste en une liste de **rules**

Une **rule** est constituée de :

- Un ensemble de **conditions** à tester
- Un ensemble d'**actions** à réaliser si les conditions sont atteintes

Policy Builder

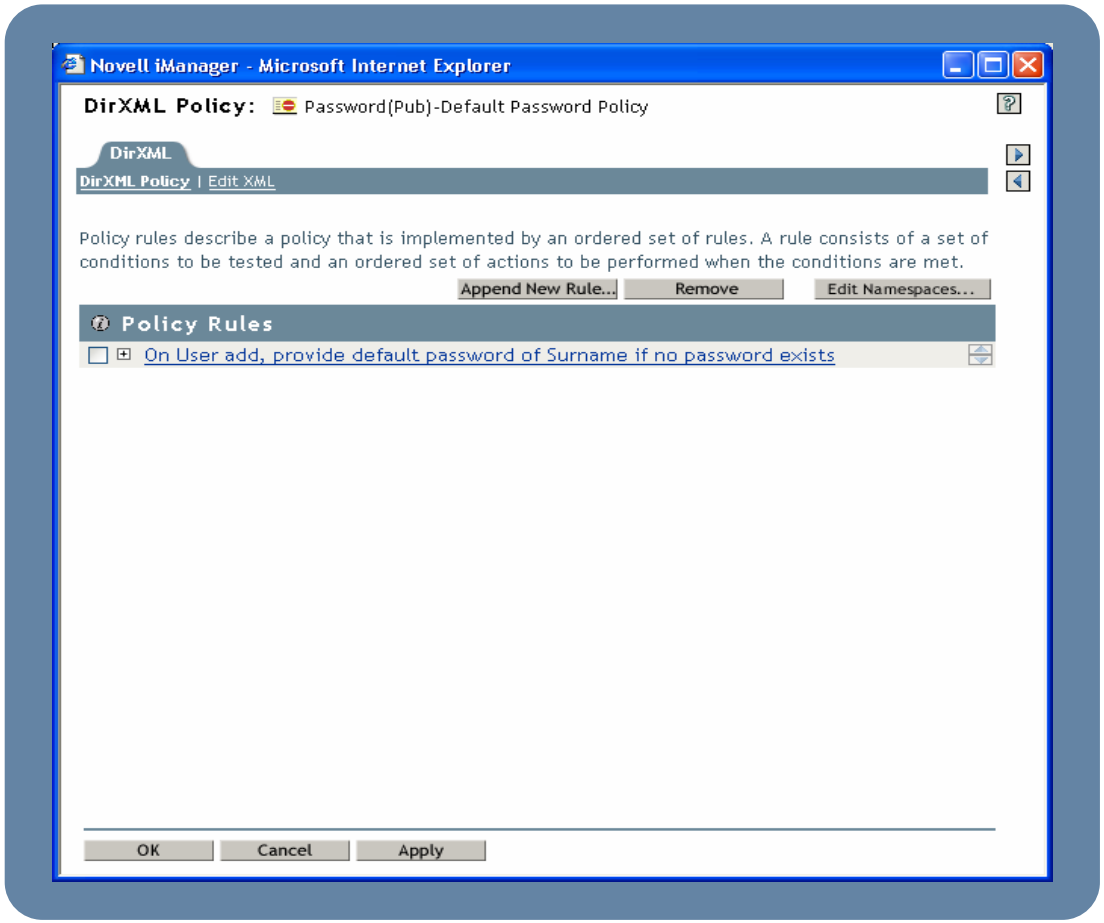
Policy Builder est une interface graphique pour administrer les scripts DirXML (accessible au travers d'une tâche iManager)

La syntaxe des scripts DirXML a été conçue pour être utilisée avec le Policy Builder plutôt qu'avec un éditeur XML traditionnel

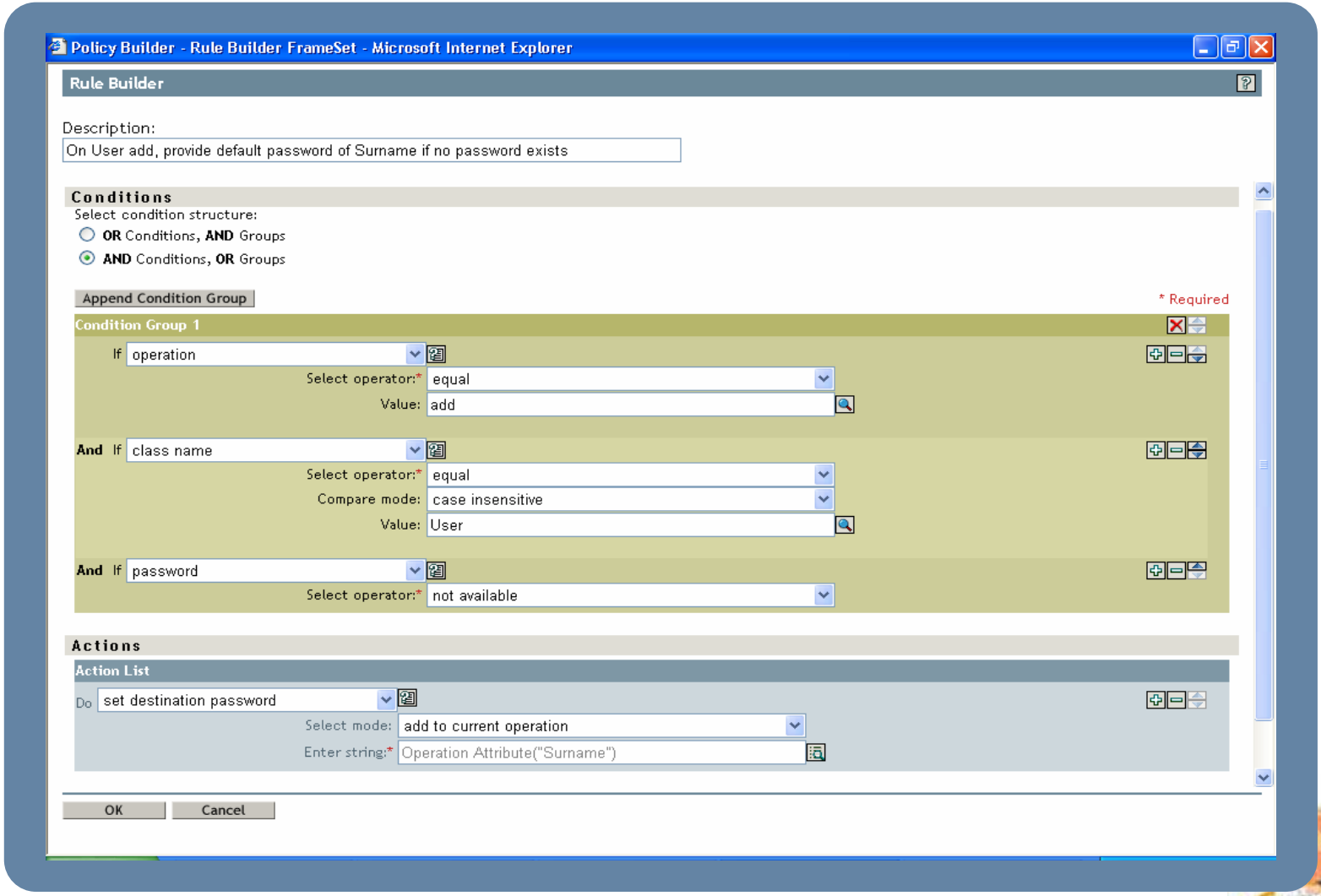
Le Policy Builder facilite la création de scripts DirXML valides en réduisant les erreurs de syntaxe et de policy

Les policies sont créées à partir d'éléments choisis dans des menus déroulants qui ne présentent que les options valides dans le contexte

Exemple de Policy Builder - Policy

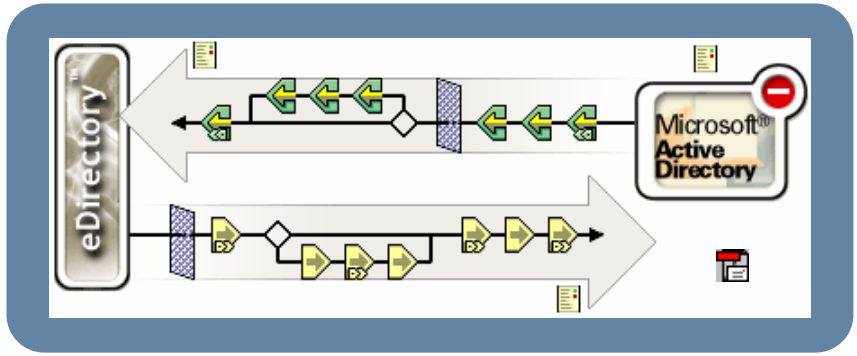


Exemple de Policy Builder - Règle



Policy Sets

- Transformation Policies
  - Entrée
  - Sortie
  - Evènement
  - Commande
- Mapping de schéma
- Correspondance
- Création
- Placement



Ordre des Policies

L’ordre dans lequel le moteur applique les policies est prédéfini. La bonne compréhension de cet ordre est critique pour être certain que la logique de fonctionnement de l’entreprise est implémentée correctement.

L’ordre des policies peut être visualisé en ouvrant l’outil de supervision des drivers dans iManager.

Policies de Transformation

Utilisées pour transformer les données ou les évènements quand l'information est partagée entre l'Identity Manager et l'application

- [Données] Transformation en sortie – Canal abonné
- [Données] Transformation en entrée – Canal de publication
- Transformation sur évènement – Les deux canaux
- Transformation sur commande – Les deux canaux

Policy du Schema de correspondance

La policy du schéma de correspondance définit les correspondances d'attributs entre l'Identity Manager et l'application.

Le pilote DirXML lit le schéma du système connecté

Les attributs doivent exister dans le filtre du pilote dans l'ordre dans lequel la correspondance sera établie

La policy du schéma de correspondance doit être liée à l'objet pilote

Policies de correspondance

Les policies de correspondance définissent les critères minimaux pour que deux objets puissent être considérés comme le même.

Utilisées pour déterminer si un objet dans l'Identity Manager est le même qu'un objet de l'application et associe ou lie ces objets l'un à l'autre.

Pour définir une policy de correspondance, on peut utiliser une combinaison de plusieurs attributs.

Policies de création

Une policy de création est chargée de définir l'ensemble minimum d'attributs nécessaires à la création d'un objet.

Une policy de création peut être différente entre le canal de publication et le canal d'abonnement.

Il peut parfois exister des policies d'un autre type intégrées à une policy de création telles que des policies d'intégration à un groupe, de nommage, de positionnement d'ACL, etc…

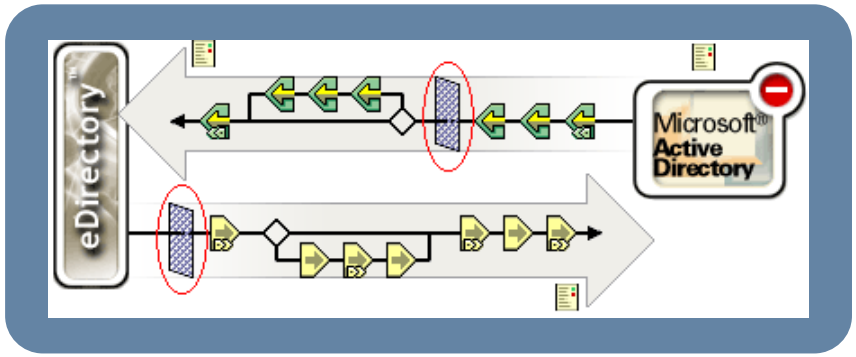
Policies de placement

Les policies de placement servent à déterminer où les nouveaux objets doivent être créés dans le référentiel d'identité de l'Identity Manager ou/et de l'application connectée

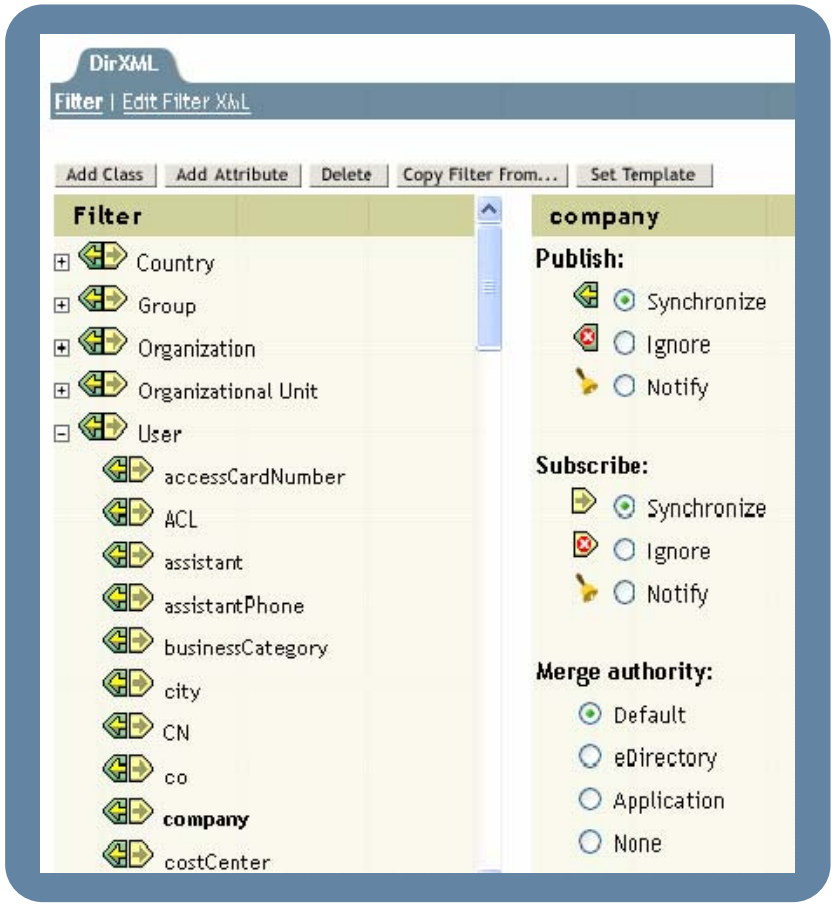
Si un pilote est paramètré pour être bi-directionnel une policy de placement est nécessaire à la fois pour le canal de publication et le canal abonné

Filtre

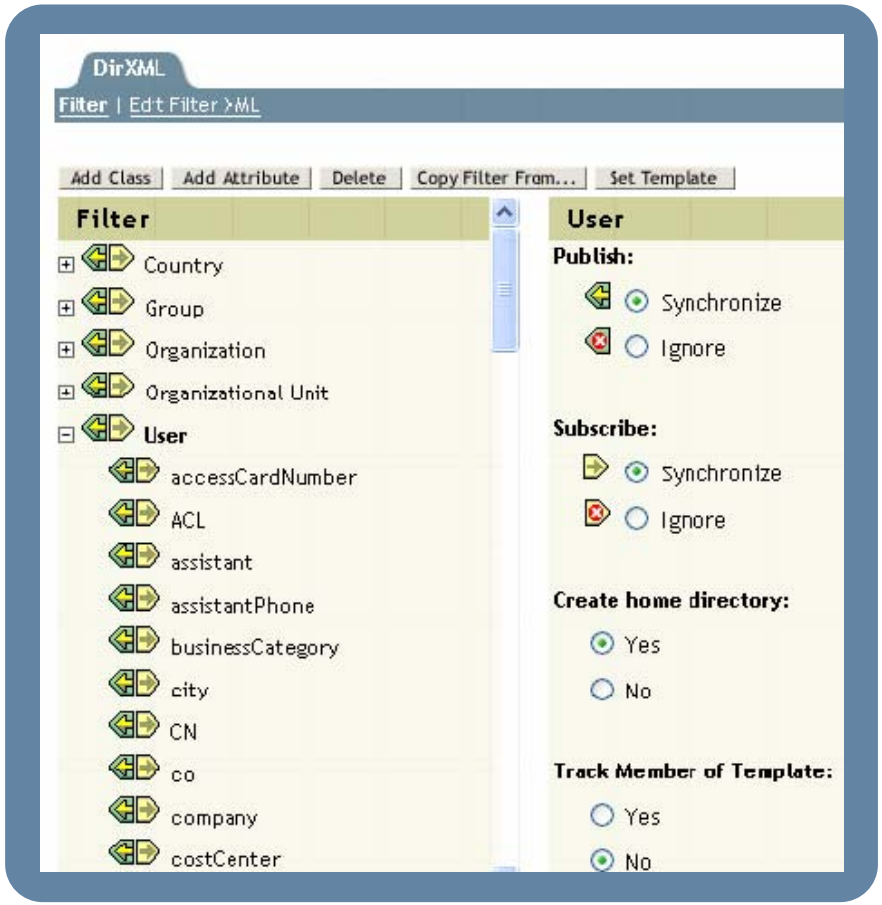
Un filtre est utilisé pour définir et contrôler les classes d'objet et les attributs à synchroniser entre une application et le référentiel d'identité de l'Identity Manager.



Exemple de filtre sur les attributs



Exemple de filtre sur les classes



Installation Simplifiée

Identity Manager est un produit distribué constitué d'éléments installés sur divers systèmes connectés au réseau.

Serveur DirXML

- Moteur DirXML, Pilotes de services DirXML , "Driver Shims", Composants NMAS, Agent d'audit Nsure,

Systémes serveurs connectés DirXML

- Chargeur DirXML distant, Outil de configuration du chargeur distantRemote, "Driver Shims" DirXML

Serveur d'administration Web

- Gestion de DirXML et des mots de passe. "Plug-ins"
- eGuide
- Fichiers de configuration des pilotes
- Self-service des mots de passes utilisateur final

Utilitaires DirXML

Gestion du mot de passe

Utilisation du gestionnaire de mot de passe

- Les utilisateurs peuvent avoir un mot de passe commun distribué de manière sécurisée à tous les systèmes supportés de l'entreprise
- Ce mot de passe commun respectera les règles de l'entreprise pour la constitution d'un mot de passe conforme
- Les utilisateurs ont la possibilité de traiter l'oubli de mots de passes sans faire appel à l'assistance

La gestion de mots de passes inclut les actions suivantes:

- **Politique de mots de passes :** établit les règles de mots de passe dans votre entreprise
- **Self-service mots de passe:** Permet le self-service pour les mots de passe, comme cela les utilisateurs peuvent traiter le cas du mot de passe oublié.
- **Distribution de mot de passe:** Spécifie quel système connecté au réseau recevra le mot de passe commun.
- **Publication du mot de passe dans l'Identity Manager:** Identifie de quelles manières le mot de passe commun peut être affecté.

Gestion de mot de passe
Règles sur les mots de passe

Les administrateurs spécifient les propriétés d'un mot de passe au format correct… Les règles sur les mots de passe.

Les examples de propriétés de mots de passe incluent:

- Nombre minimum de caractères
- Nombre maximum de caractères
- Nombre minimum de minuscules
- Nombre minimum de majuscules
- Nombre minimum de chiffres
- Ne doit pas être un mot de passe précédemment utilisé par l'utilisateur
- Ne doit pas être un mot qui se trouve dans la liste d'exclusion des mots de passe
- & etc.

La conformité à l'ensemble des propriétés est testée avant d'affecter le mot de passe dans le référentiel d'identités de l'Identity Manager.

Gestion de mot de passe
Self-Service mot de passe

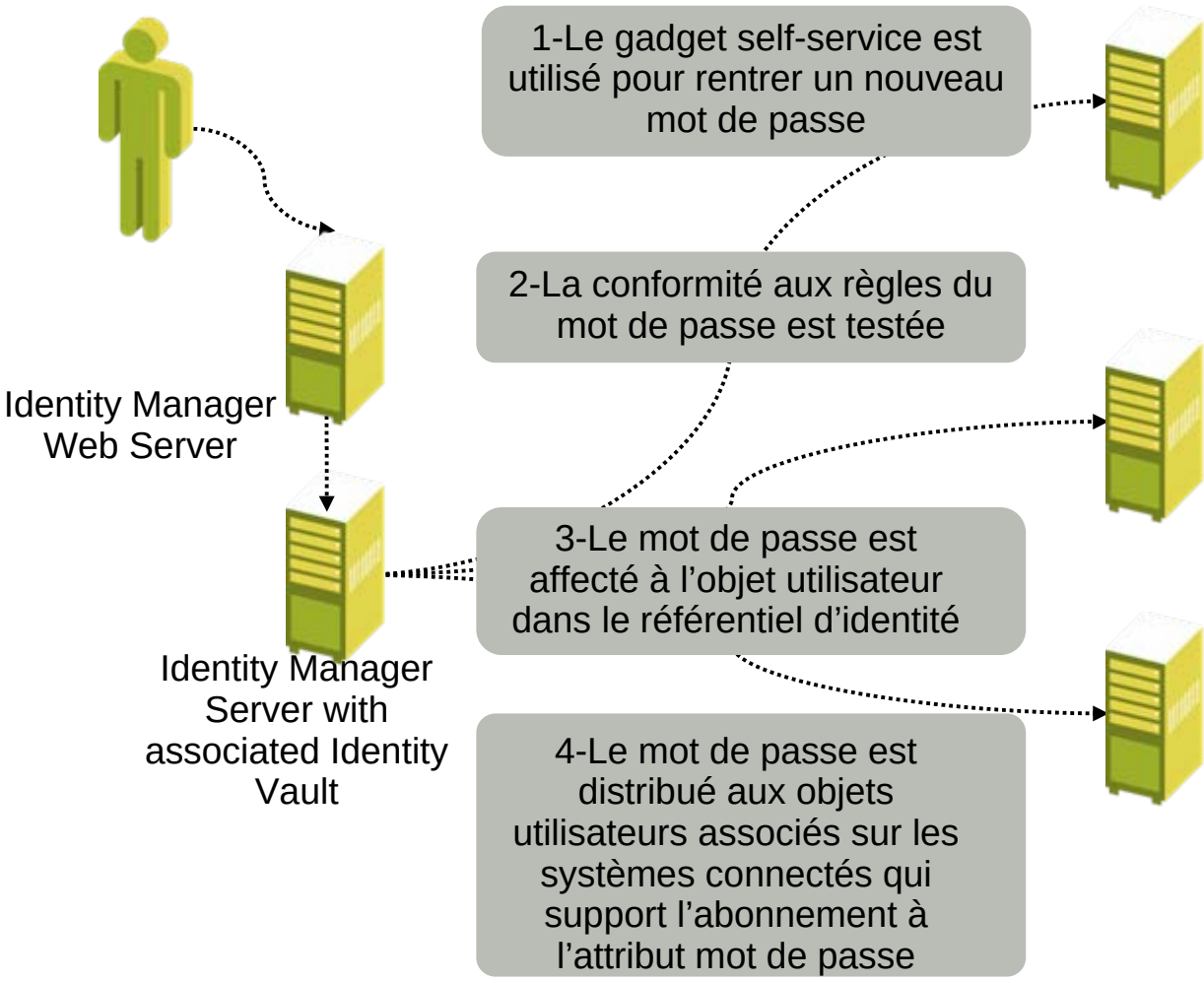
Les administrateurs configurent les règles de self-service pour chaque utilisateur à travers une tâche iManager

- Mode Challenge/Réponse
  - L'administrateur peut ou non l'activer
  - L'administrateur choisi les questions du challenge et les options qui s'y raportent.
- Actions possibles: (Les deux premières demandent un Challenge/Réponse)
  - Permet à l'utilisateur de changer son mot de passe
  - Envoie le mot de passe à l'utilisateur par mél.
  - Envoie un indice à l'utilisateur par mél.
  - Affiche l'indice sur la page

L'utilisateur configure son propre indice pour retrouver le mot de passe et la répones à la question du challenge en utilisant le Self-service mot de passe

- L'indice n'est pas autorisé à contenir le mot de passe

Gestion de mot de passe
Distribution du mot de passe



Systèmes Connectés

eDirectory

Legacy NDS

Active Directory/Exchange 2000

Windows NT Domains

Gestion des utilisateurs SAP

Network Information Service (NIS)

- Linux
- Solaris
- autres UNIX

GroupWise

Lotus Notes

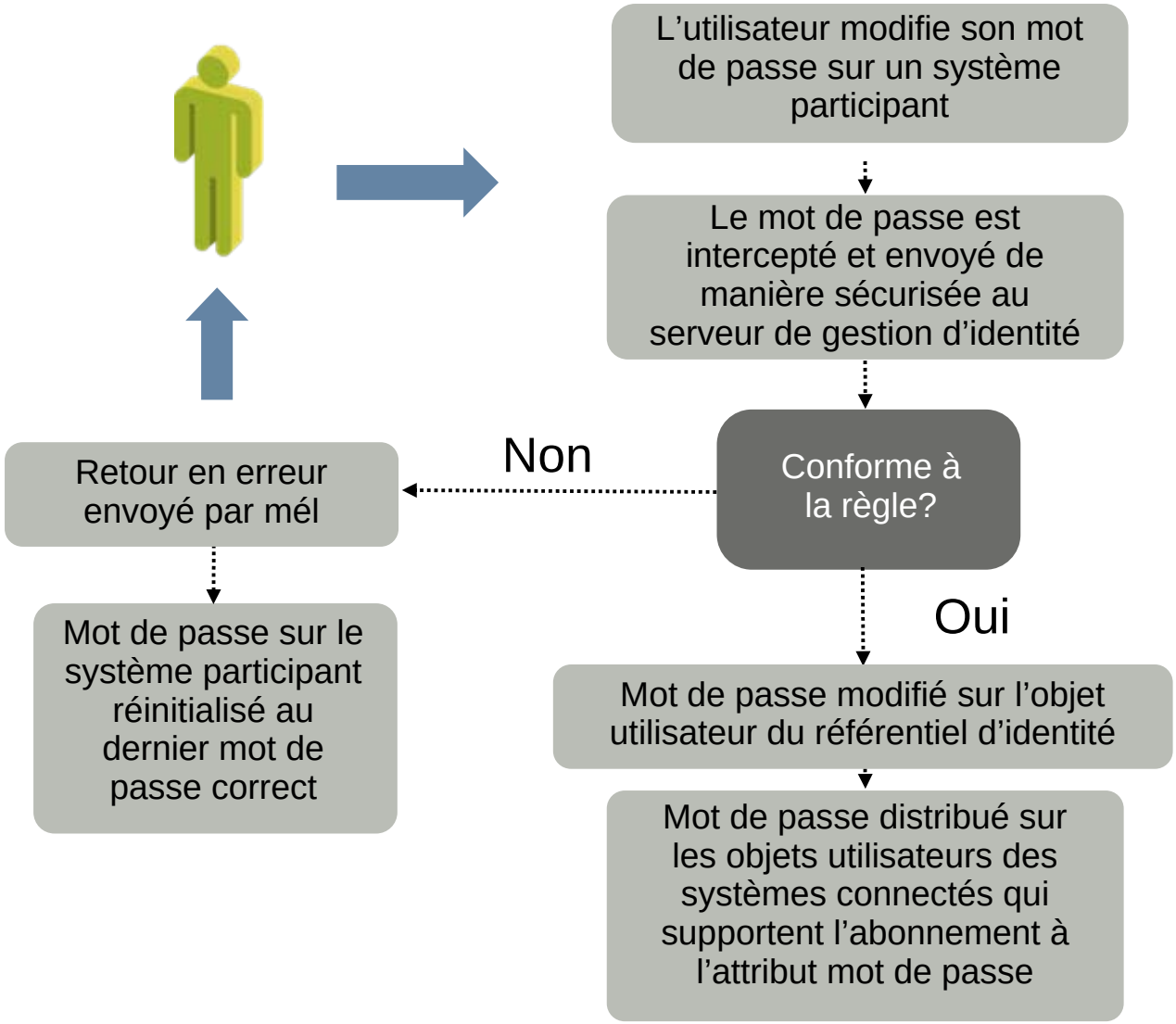
SunOne

Bases de données relationnelles

- Oracle
- DB2
- Sybase

Gestion de mots de passe

Publication du mot de passe à l'Identity Manager



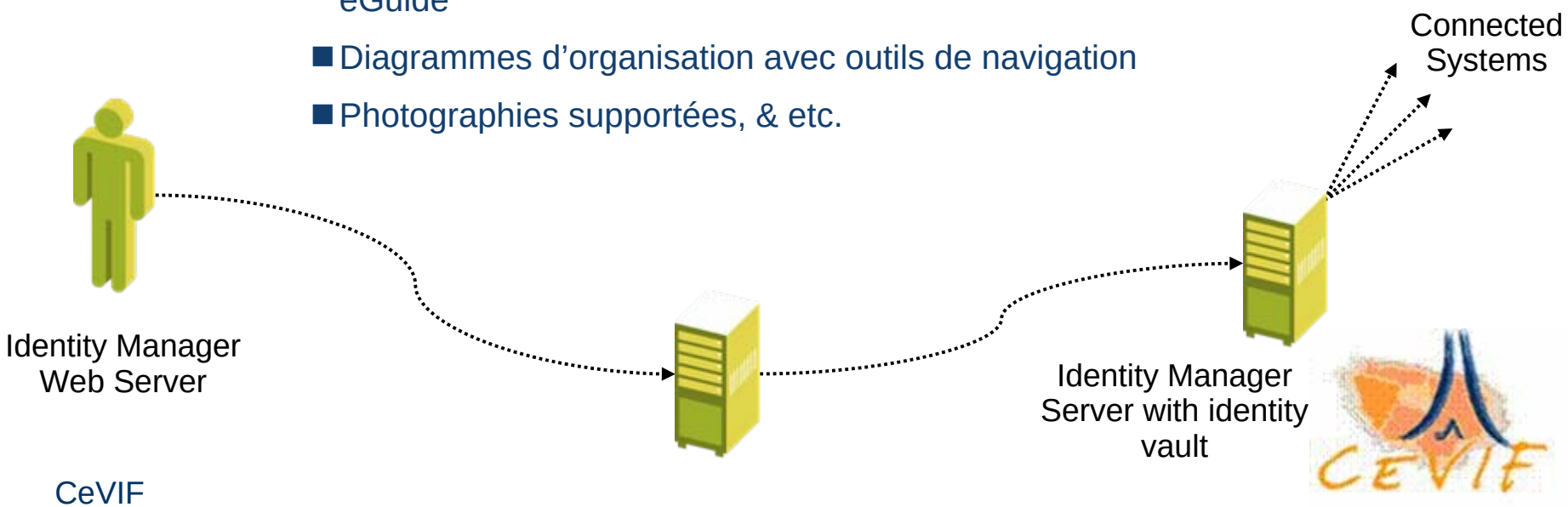
Systèmes participants

Active Directory
NT Domains
NIS (Unix)
eDirectory

eGuide Pages Blanches et Self Service

eGuide est utilisé pour administrer le carnet d'adresse de l'entreprise et le self-service utilisateur.

- Recherche d'informations sur les objets dans eDirectory ou d'autres référentiels LDAP
- Mode anonyme ou authentifié
- Permet aux utilisateurs de modifier des attributs désignés de leur objet utilisateur. Les attributs modifiés peuvent être propagés sur les systèmes connectés.
- Des guides de configuration rapide facilitent la configuration de eGuide
- Diagrammes d'organisation avec outils de navigation
- Photographies supportées, & etc.



Rapports, Log et Notification

Identity Manager comprend Nsure audit Rapports:

- Des filtres peuvent être définis pour signaler des évènements spécifiques
- Intégration avec Crystal Reports
- Exportation des données vers Excel ou un fichier texte

Log:

- Vous pouvez configurer de quelle manière les évènements DirXML seront mis dans un fichier log
  - **Evènements moteur** – Marche/arrêt pilote, erreurs moteur, avertissements moteur
  - **Evènements statuts** – Succés, erreurs, nouvelles tentatives, avertissements…
  - **Evènements operation** – Recherche, ajout, modification, effacement, etc.
  - **Evènements transformation** – Initialisation, placement, création, etc.
- Evènements stockés dans un fichier plat, Syslog, MySQL, Oracle, etc.

Notification:

- Configuration des conditions
- Specification du canal de notification (SMTP, fichier plat, etc.)

Droits basés sur des rôles

Accorde des droits aux utilisateurs basés sur leur appartenance à un rôle.

- Appartenance déterminée dynamiquement ou statiquement
  - Dynamic membership based on combinations of user attributes
  - Appartenance dynamique basée sur des combinaisons d'attributs utilisateurs
  - Appartenance statique basée sur une liste d'identifiants utilisateurs
- Les droits incluent:
  - Avoir un compte sur un système connecté
  - Etre inclu dans un groupe NOS
  - Etre inclu dans une liste de distribution de messagerie
- Les droits sont déterminés quand:
  - Un utilisateur est ajouté à un référentiel d'identité, soit directement, soit à partir d'une souirce autorisée.
  - Les attributs qui régissent l'appartenance à un rôle sont changés.
- Permettent la détermination automatique des:
  - Groupes NOS
  - Des listes de distribution de messagerie

Diverses Fonctionnalités

Paramètres de configuration globaux

Resynchronisation

Traces améliorées

Diverses fonctionnalités
Global Configuration Values (GCV)

Fourni une méthode pour ajouter des paramètres à un pilote

- Peuvent être définies au niveau d'un pilote ou d'un ensemble de pilotes
- Les pilotes héritent des GCV de leur ensemble de pilotes s'il n'y en a pas de définit au niveau du pilote.
- Utilisables avec la synchronisation des mots de passe, "heart beat", les droits basés sur les rôles, etc.
- Des GCV par défaut sont livrées avec les configurations des pilotes
- Créées, adaptées et maintenues en un seul point

Diverses fonctionnalités
Resynchronisation

Identity Manager amène deux nouvelles fonctionnalités de resynchronisation

- Suppression automatique de la resynchronisation quand on réactive un pilote désactivé
- Spécification d'une heure de démarrage pour la fenêtre de démarrage d'une synchronisation manuelle

Diverses nouvelles fonctionnalités
Enhanced Tracing

Traces par pilote

- Le niveau de trace peut être positionné individuellement
- La trace peut être faite dans un fichier à part
- Noms abrégés
- Si pas de niveau de trace du pilote spécifié, utilisation du niveau de trace de l'ensemble de pilotes

Chaque message est préfixé par un identifiant (vous pouvez créer le vôtre)

- EV: Message du système de cache d'évènement
- ET: Message du moteur non spécifique des pilotes
- ST: Message spécifique pilote relatif au flux abonné
- PT: Message spécifique pilote relatif au flux de publication

Recommandations pour le déploiement

Mettre en place un serveur Identity Manager avec sa propre arborescence

- Cette arborescence devient le référentiel d'identité de votre entreprise
- Vos arborescences NOS sont distinctes et indépendantes du référentiel d'identité
- Vos arborescences NOS pourront être prises en compte par une version plus ancienne de eDirectory
- Les données de référence alimentent le référentiel d'identité et sont ensuite distribués aux systèmes connectés conformément aux processus de l'entreprise

Utiliser eDirectory 8.7.3 pour le référentiel d'identités de l'Identity Manager

- 8.7.3 supporte les fonctionnalités de gestion de mot de passe de l'Identity Manager. Les versions précédentes ne supportent pas complètement toutes les fonctionnalités

Mettre en place un serveur Web Identity Manager pour l'administration et le self-service utilisateur

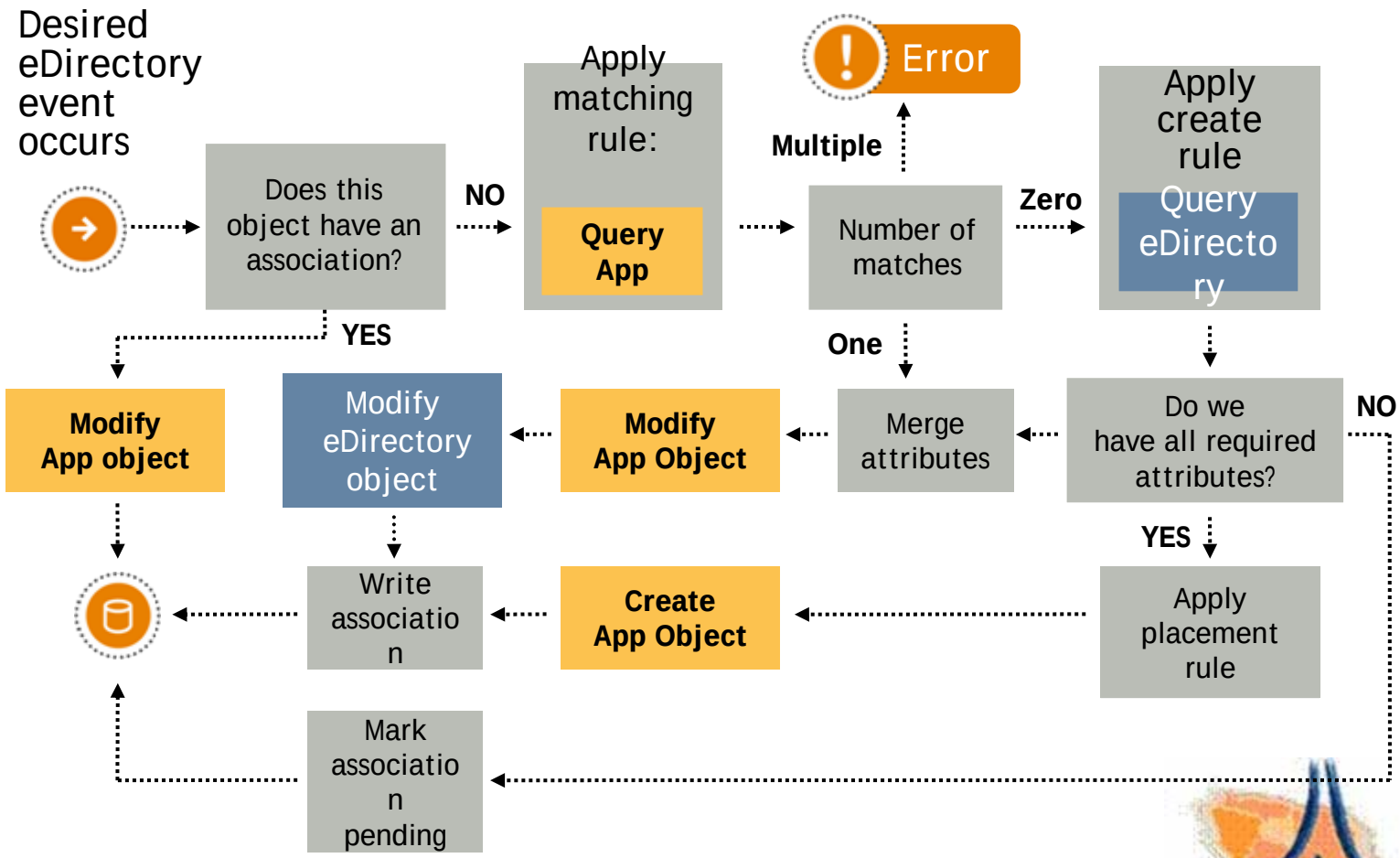
- Peut être sur la même machine que le serveur Identity Manager mais non obligatoire.
- Tous les composants Identity Manager en technologie Web (iManager, eGuide, Password self-service) s'éxécutent sur le serveur Web.
- Encourager fortement les utilisateurs à utiliser le gadget mot de passe self-service sur ce serveur pour gérer son mot de passe
- iManager est requis pour administrer Novell Nsure Identity Manager 2.

Questions/Réponses

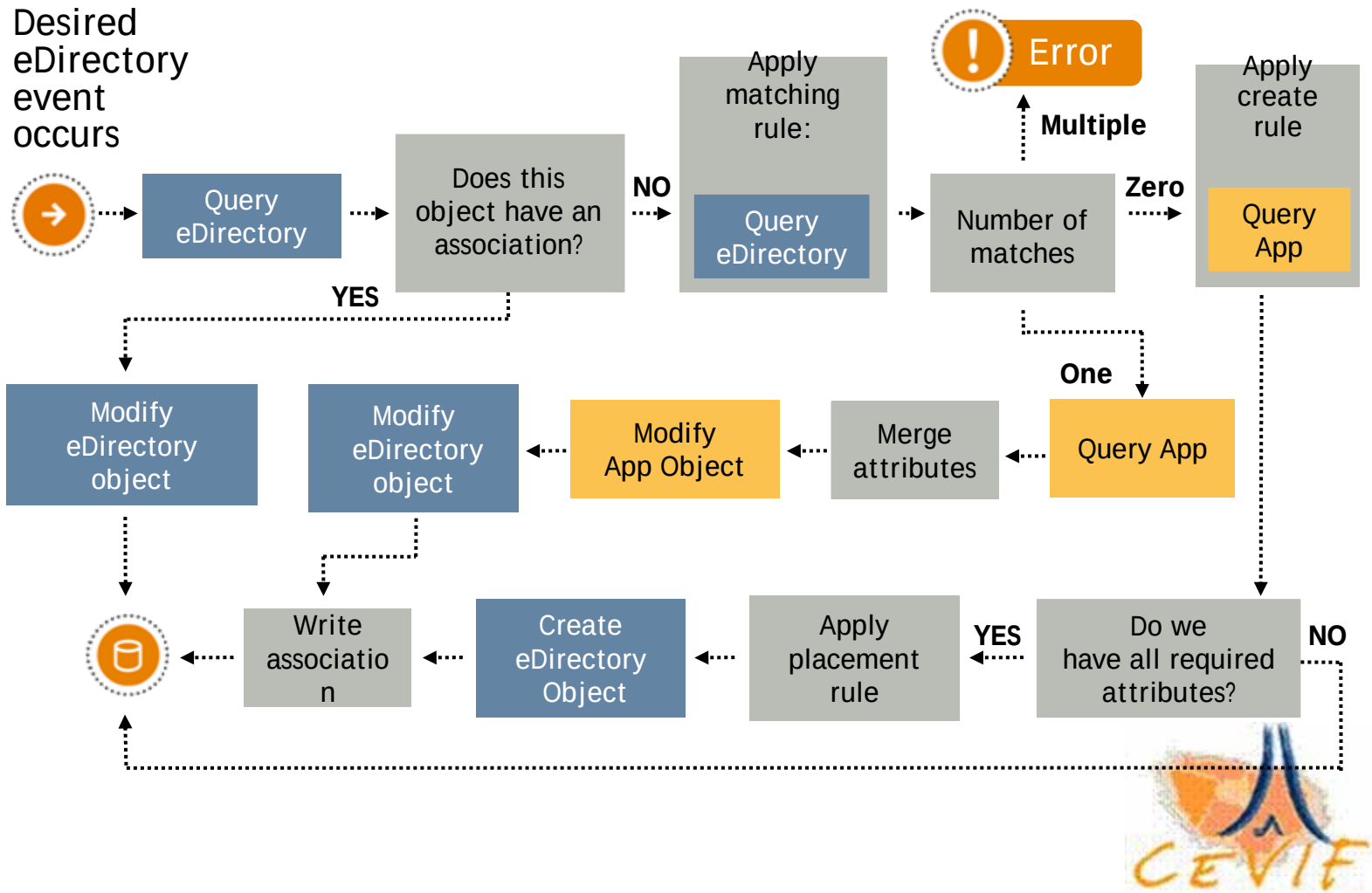
Appendix

The following slides represent additional technical notes of the product.

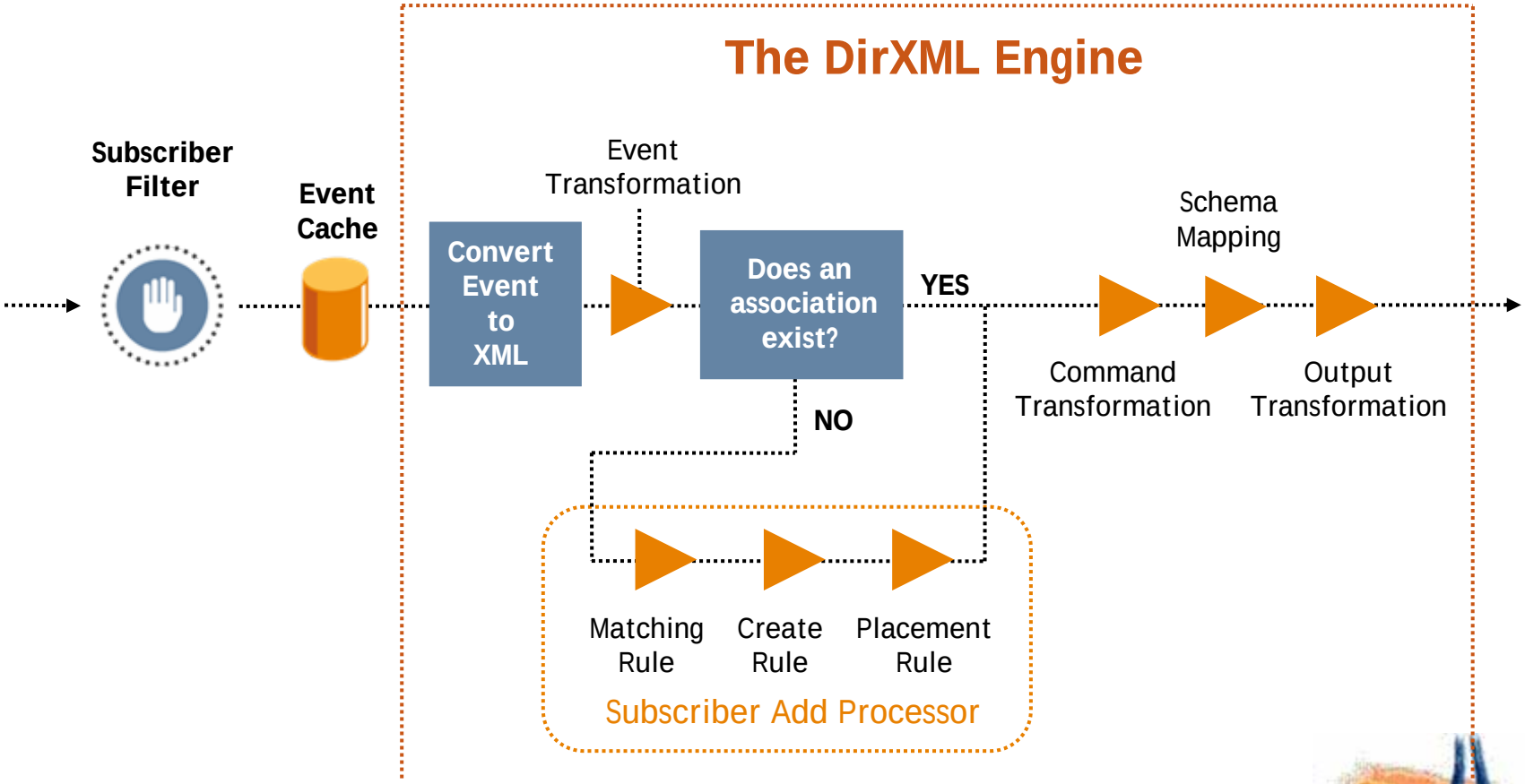
Building Associations
Subscriber



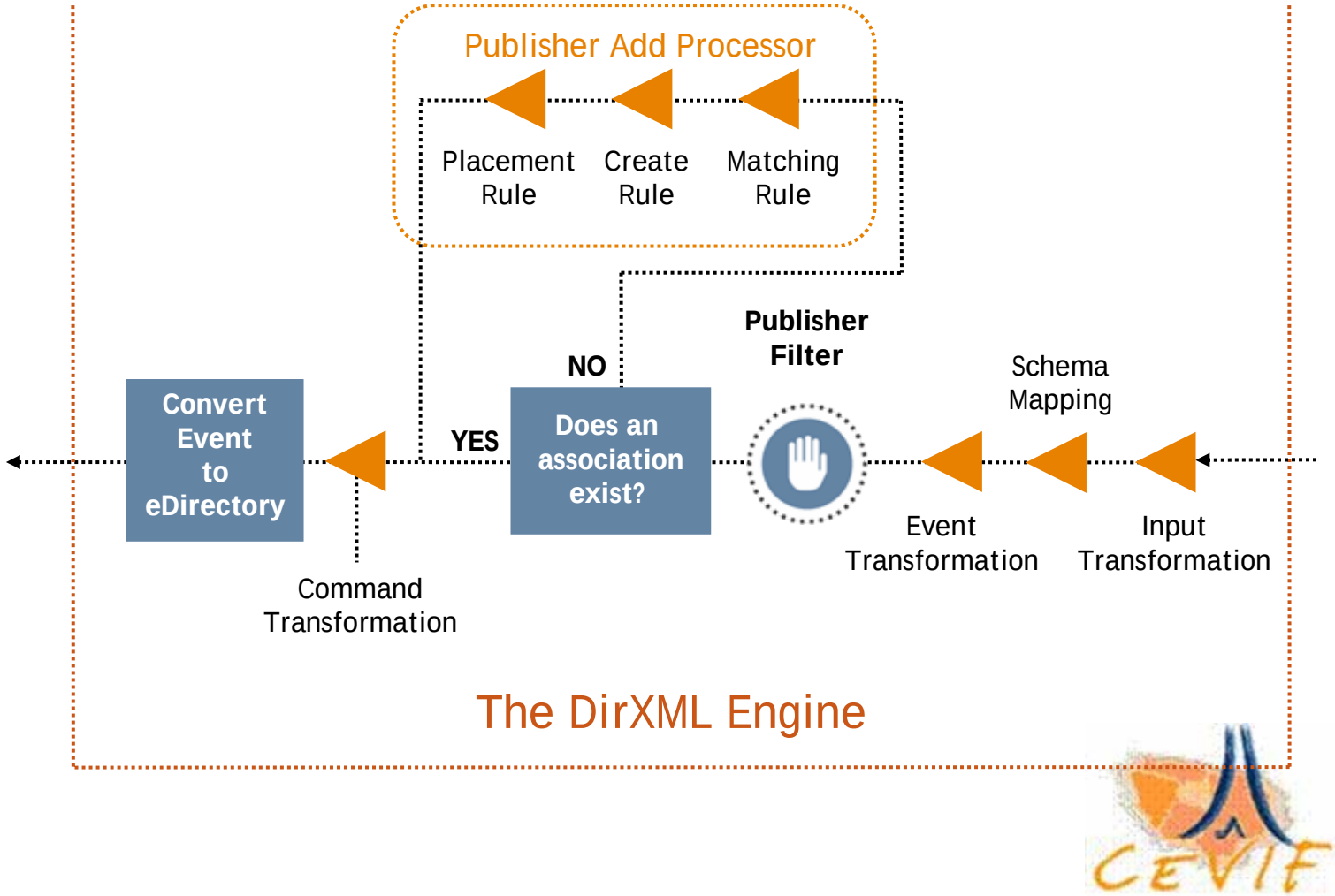
Building Associations
Publisher



Policy Processing Order
Subscriber



Policy Processing Order
Publisher



Platform Support for Identity Manager

Novell Nsure Identity Manager 2 Server components and Web-based components are supported on the following platforms:

Platforms	Support packs	eDirectory	iManager
Novell NetWare® 6	SP3	8.7.3	2.0.2
Novell NetWare 6.5	<none>	8.7.3	2.0.2
Microsoft Windows NT 4	SP6a	8.7.3	<not supported>
Microsoft Windows 2000	SP4	8.7.3	2.0.2
Red Hat Enterprise Linux AS or ES	Recommended Patches	8.7.3	2.0.2
SuSE Linux Enterprise Server 8	Recommended Patches	8.7.3	2.0.2
Sun Solaris 8	Recommended Patches	8.7.3	2.0.2
Sun Solaris 9	Recommended Patches	8.7.3	2.0.2

Connected Systems

Connected System Drivers	NW	Win	Unix
DirXML Driver 3.0 for Active Directory	N	Y	N
DirXML Driver 1.1 for Delimited Text	Y	Y	Y
DirXML Driver 2.0 for eDirectory	Y	Y	Y
DirXML Driver 1.6 for Exchange 5.5	N	Y	N
DirXML Driver 2.1 for GroupWise	Y	Y	N
DirXML Driver 1.6 for JDBC	Y	Y	Y
DirXML Driver 1.6 for LDAP	Y	Y	Y
DirXML Driver 2.0 for Lotus Notes	N	Y	Y
DirXML Driver 2.0 for NIS	N	N	Y
DirXML Driver 3.6 for PeopleSoft	N	Y	N
DirXML Driver 4.0 for PeopleSoft	N	Y	N
DirXML Driver 1.0 for SAP HR	N	Y	Y
DirXML Driver 1.0 for SAP User	N	Y	Y
DirXML Driver 1.0 for SIF	Y	Y	N
DirXML Driver 1.4 for Windows NT 4	N	Y	N

Service Drivers	NW	Win	Unix
Move Proxy Service Driver	Y	Y	Y
Entitlements Service Driver	Y	Y	Y
Manual Task Service Driver	Y	Y	Y