Présentation de Sun Identity Manager

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054
U.S.A.

Référence : 821–0059
Juillet 2009

090810@22749

Table des matières

Préface

Présentation de Sun Identity Manager 8.1 répond à la question *Qu'est-ce que Sun™ Identity Manager et quel en est le fonctionnement ?* Ce livre décrit l'architecture du produit Identity Manager et explique comment planifier un déploiement haute disponibilité.

Public

Ce guide a été conçu pour les professionnels des technologies de l'information qui veulent mieux comprendre Sun Identity Manager 8.1 et les logiciels associés. Il sera particulièrement utile à ceux cherchant à évaluer Identity Manager ou commençant à planifier un déploiement d'Identity Manager.

Organisation de ce guide

Ce guide se compose des chapitres suivants :

Le Chapitre 1, "Présentation du produit" décrit l'objectif d'Identity Manager et présente les principales fonctionnalités de l'application.

Le Chapitre 2, "Architecture du produit" décrit l'architecture d'Identity Manager, l'architecture de Service Provider et l'architecture des services Web. Il contient également des directives sur la séparation et la proximité physique des systèmes.

Le Chapitre 3, "Clustering et haute disponibilité" explique la mise en œuvre d'un environnement Identity Manager haute disponibilité/à tolérance de pannes (HA/FT). Il vous aidera aussi à estimer l'ampleur de la disponibilité requise par votre déploiement d'Identity Manager.

Manuels connexes

L'ensemble de documentation de Sun Identity Manager 8.1 se compose des manuels suivants.

Public principal	Titre	Description
Tous publics	*Présentation de Sun Identity Manager*	Présente les caractéristiques et les fonctionnalités d'Identity Manager. Contient des informations sur l'architecture du produit et explique l'intégration d'Identity Manager avec d'autres produits Sun tels que Sun Open SSO Enterprise et Sun Role Manager.
	Notes de version de Sun Identity Manager 8.1	Décrivent les problèmes connus et corrigés ainsi que les informations de dernière minute ne figurant pas encore dans l'ensemble de documentation d'Identity Manager.
Administrateurs système	*Installation Guide* (Guide d'installation)	Décrit l'installation de Identity Manager et des composants optionnels tels qu'Sun Identity Manager Gateway et PasswordSync.
	Upgrade Guide (Guide de mise à niveau)	Contient les instructions à suivre pour effectuer une mise à niveau d'une version plus ancienne d'Identity Manager vers une version plus récente.
	System Administrator's Guide (Guide de l'administrateur système)	Contient des informations et des instructions pour aider les administrateurs à gérer, régler et dépanner leur installation d'Identity Manager.
Administrateurs d'entreprise	*Business Administrator's Guide* (Guide de l'administrateur d'entreprise)	Explique l'utilisation des fonctionnalités de provisioning et de contrôle d'Identity Manager. Contient des informations sur les interfaces utilisateur, la gestion des utilisateurs et des comptes, la génération des rapports et bien plus encore.

Public principal	Titre	Description
Intégrateurs de systèmes	*Deployment Guide* (Guide de déploiement)	Explique le déploiement d'Identity Manager dans les environnements informatiques complexes. Les sujets traités incluent le travail avec les attributs d'identité, le chargement et la synchronisation des données, la configuration des actions des utilisateurs, l'application de stratégies de marques personnalisées, et ainsi de suite.
	Deployment Reference (Références de déploiement)	Contient des informations sur les flux de travaux, les formulaires, les affichages et les règles ainsi que sur le langage XPRESS.
	Resources Reference (Références pour les ressources)	Fournit des informations sur l'installation, la configuration et l'utilisation des adaptateurs de ressources.
	Service Provider 8.1 Deployment (Déploiement de Service Provider 8.1)	Explique le déploiement d'Sun Identity Manager Service Provider, et en quoi les affichages, les formulaires et les ressources diffèrent de ceux du produit Identity Manager standard.
	Web Services Guide (Guide des services Web)	Explique la configuration de la prise en charge de SPML, les fonctionnalités de SPML prises en charge (et la raison de cette prise en charge) et comment étendre la prise en charge sur le terrain.

Mises à jour de la documentation

Les corrections et mises à jour de cette et d'autres publications relatives à Sun Identity Manager sont désormais postées sur le site Web des mises à jour de la documentation d'Identity Manager :

`http://blogs.sun.com/idmdocupdates/`

Un lecteur de flux RSS peut être utilisé pour contrôler périodiquement le site Web et vous avertir lorsque de nouvelles mises à jour sont disponibles. Pour vous abonner, téléchargez un

lecteur de flux et cliquez sur un lien sous Feeds (Flux) sur la droite de la page. Depuis la version 8.0, des flux séparés sont disponibles pour chacune des versions majeures.

Références à des sites Web tiers

Des URL tiers pointant vers des informations complémentaires sont cités dans ce document.

Remarque – Sun ne saurait être tenu responsable de la disponibilité des sites Web tiers mentionnés dans ce manuel. Sun décline toute responsabilité en ce qui concerne le contenu, la publicité, les produits ou tout autre matériel disponibles dans ou par l'intermédiaire de ces sites ou ressources. Sun ne pourra en aucun cas être tenu pour responsable, directement ou indirectement, de tous dommages ou pertes, réels ou invoqués, causés par ou liés à l'utilisation des contenus, biens ou services disponibles dans ou par l'intermédiaire de ces sites ou ressources.

Documentation, support et formation

Le site Web de Sun fournit des informations sur les ressources additionnelles suivantes :

- Documentation (`http://www.sun.com/documentation/`)
- Support (`http://www.sun.com/support/`)
- Training (`http://www.sun.com/training/`)

Vos commentaires sont les bienvenus

Dans le souci d'améliorer notre documentation, nous vous invitons à nous faire parvenir vos commentaires et suggestions. Pour nous faire part de vos commentaires, accédez à l'adresse `http://docs.sun.com` et cliquez sur Envoyer des commentaires.

Conventions typographiques

Le tableau suivant indique les conventions typographiques utilisées dans cet ouvrage.

TABLEAU P–1 Conventions typographiques

Caractère ou symbole	Signification	Exemple
`AaBbCc123`	Noms de commandes, fichiers et répertoires ; messages système.	Modifiez le fichier `.login`. Utilisez `ls -a` pour dresser la liste des fichiers. `nom_machine% Vous avez du courrier.`
`AaBbCc123`	Caractères saisis par l'utilisateur, par opposition aux messages système.	`nom_machine%` **`su`** `Password:`
aabbcc123	Remplacez les variables de ligne de commande par des noms ou des valeurs réels.	Pour supprimer un fichier, tapez `rm` *nomfichier*.
AaBbCc123	Titres d'ouvrages, nouveaux mots ou termes, mots importants.	Lisez le chapitre 6 du *Guide de l'utilisateur*. Un *cache* est une copie qui est stockée localement. N'enregistrez *pas* le fichier. **Remarque :** certains éléments mis en évidence apparaissent en caractères gras.

Invites de shell dans les exemples de commande

Le tableau suivant indique l'invite système UNIX® et les invites de superutilisateur par défaut pour le C shell, le Bourne shell et le Korn shell.

TABLEAU P–2 Invites de shell

Shell	Invite
C shell	`nom_machine%`
C shell pour superutilisateur	`nom_machine#`
Bourne shell et Korn shell	`$`
Bourne shell et Korn shell pour superutilisateur	`#`

◆ ◆ ◆ CHAPITRE 1

1 Présentation du produit

Ce chapitre décrit l'objectif de Sun™ Identity Manager et présente les principales fonctionnalités de l'application. Il détaille aussi brièvement les autres offres de produits de gestion des identités de Sun.

Ce chapitre se compose des rubriques suivantes :

Présentation d'Identity Manager

Sun Identity Manager permet d'automatiser le processus de création, mise à jour et suppression de comptes utilisateurs entre plusieurs systèmes informatiques. Collectivement, ce processus est connu sous les noms de *provisioning* (c'est-à-dire la création et la mise à jour de comptes utilisateurs) et *deprovisioning* (la suppression de comptes utilisateurs).

Par exemple, à l'embauche d'un nouvel employé, Identity Manager exécute un flux de travaux qui récupère les approbations nécessaires pour lui octroyer des droits d'accès. Ces approbations obtenues, Identity Manager crée des comptes pour cet employé dans le système de ressources humaines (PeopleSoft) de la société, son système de messagerie électronique (Microsoft Exchange) et l'application de l'entreprise (SAP). Si l'employé en question change de poste dans l'entreprise, Identity Manager met à jour son compte utilisateur et en étend les droits d'accès aux ressources nécessaires à sa nouvelle fonction. Lorsque l'employé quitte la société, Identity Manager supprime automatiquement ses comptes utilisateur pour empêcher tout accès ultérieur.

Identity Manager peut également mettre en œuvre de manière continue des stratégies d'audit. Une *stratégie d'audit* spécifie les types d'accès dont un utilisateur peut ou peut ne pas bénéficier.

À titre d'exemple, aux États-Unis le fait qu'un même utilisateur ait accès à la fois aux comptes fournisseurs et à la comptabilité clients constitue une violation de la loi Sarbanes-Oxley (SOX). On parle alors de violation du principe de séparation des fonctions. Identity Manager peut effectuer un examen d'audit pour contrôler l'existence de tout un éventail de types de violations et, selon la configuration, supprimer automatiquement les droits d'accès ou envoyer une notification à un administrateur lorsqu'une violation est détectée. Ce processus est connu sous le nom de *résolution*.

Interfaçage d'Identity Manager avec les autres systèmes informatiques

Dans Identity Manager, les applications gérées et les autres systèmes informatiques s'appellent des *ressources*. Identity Manager utilise des *adaptateurs* ou des *connecteurs* pour l'interfaçage avec les ressources.

Les adaptateurs et les connecteurs s'installent sur le serveur Identity Manager (aucun logiciel spécial (ou *agent*) n'est nécessaire pour installer Identity Manager sur des ressources cibles). Des douzaines d'adaptateurs et connecteurs Identity Manager sont disponibles et il est possible d'en créer de nouveaux pour communiquer avec pratiquement toute ressource en utilisant les protocoles standard ou des interfaces de programmation d'application (API) connues. Identity Manager est livré avec divers adaptateurs et connecteurs permettant de communiquer avec nombre des ressources les plus courantes. De plus, des modèles et du code squelette sont disponibles pour aider les programmeurs à créer des adaptateurs et connecteurs supplémentaires.

Certaines ressources ne permettant pas une communication directe requièrent l'utilisation de Sun Identity Manager Gateway. À titre d'exemple, les produits de Microsoft, tels qu'Exchange et Windows Active Directory, et ceux de Novell comme eDirectory (l'ancien Netware Directory Services) requièrent l'utilisation de Gateway. Dans ces cas, Identity Manager communique directement avec Gateway et Gateway s'interface avec la ressource.

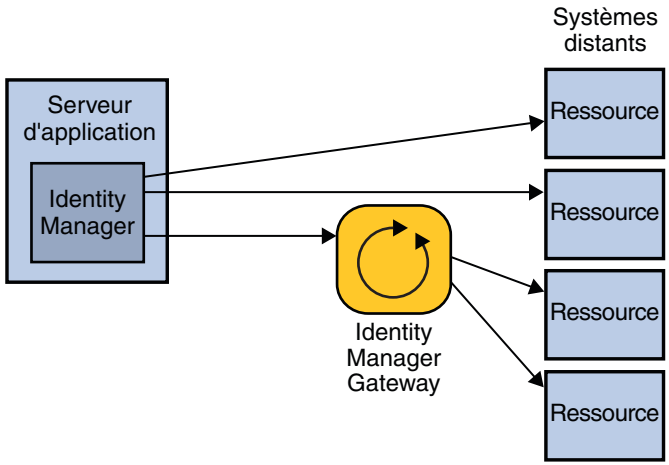

FIGURE 1–1 Identity Manager s'interface directement avec certaines ressources, mais Identity Manager Gateway est nécessaire pour d'autres.

Pour la liste des ressources prises en charge par Identity Manager, consultez la section "Ressources prises en charge" du *Notes de version de Sun Identity Manager 8.1*.

Connexion des utilisateurs à Identity Manager

Identity Manager a une interface utilisateur (IU) pour les administrateurs et une interface distincte pour les utilisateurs finaux. Pour utiliser Identity Manager, les administrateurs et les utilisateurs finaux doivent se servir d'un navigateur Web pour se connecter à Identity Manager.

- Les administrateurs utiliseront l'*interface administrateur* pour gérer les utilisateurs, configurer et assigner des ressources, définir des droits et des niveaux d'accès, établir des stratégies d'audit, gérer la compatibilité et effectuer d'autres fonctions d'administrateur d'entreprise et d'administrateur système.
- Les utilisateurs finaux utiliseront quant à eux l'*interface utilisateur final* pour effectuer toute une gamme de tâches « en libre service », telles que la modification de leurs mots de passe, la définition des réponses aux questions d'authentification, la demande d'accès aux systèmes informatiques et la gestion des assignations déléguées.

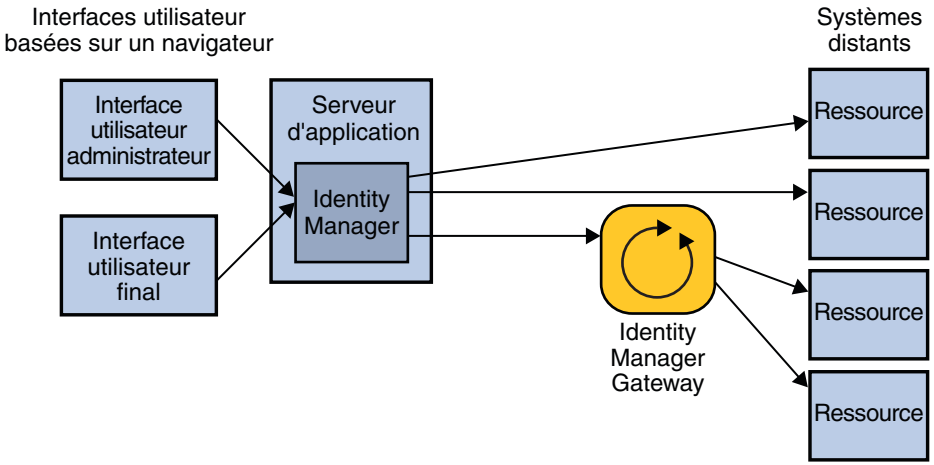

FIGURE 1–2 Les utilisateurs peuvent se connecter à Identity Manager en utilisant les interfaces administrateur et utilisateur final

Les entreprises peuvent également utiliser SPML (Service Provisioning Markup Language, langage de balisage de provisioning de services) pour, au choix, créer leurs propres interfaces utilisateur ou intégrer un système frontal existant avec Identity Manager.

Voici quelques autres interfaces d'Identity Manager :

- L'interface téléphonique IVR (Interactive Voice Response, serveur vocal interactif) permet aux utilisateurs finaux d'exécuter les fonctions d'Identity Manager en utilisant un téléphone.
- L'IDE (Integrated Development Environment, environnement de développement intégré) d'Identity Manager est utilisé par les développeurs de logiciels pour personnaliser Identity Manager.
- La console d'Identity Manager est une interface de ligne de commande à la disposition des administrateurs.

Présentation d'Identity Manager Service Provider

Identity Manager Service Provider est une fonctionnalité de gestion des identités hautement évolutive centrée sur l'extranet en mesure de provisionner et d'actualiser des millions de comptes utilisateurs stockés sur un serveur d'annuaire LDAP. Cette fonctionnalité peut aussi gérer des milliers de comptes administrateurs et synchroniser les données des comptes LDAP avec d'autres ressources.

La fonctionnalité Service Provider utilise un sous-ensemble des fonctions et fonctionnalités disponibles dans Identity Manager. Par exemple, la fonctionnalité de contrôle n'est pas disponible car elle est moins utile dans un environnement extranet.

Pour un compte-rendu détaillé des différences entre le produit Identity Manager standard et la fonctionnalité Service Provider, consultez la section "Service Provider Features" du *Sun Identity Manager Service Provider 8.1 Deployment* (Déploiement de Sun Identity Manager Service Provider 8.1).

Autrefois proposé sous la forme d'un produit add-on séparé, Service Provider fait désormais partie d'Identity Manager. Tirer parti des avantages de la fonctionnalité Service Provider requiert toutefois une planification spéciale.

- Pour toute information sur l'architecture de système d'Identity Manager Service Provider, reportez-vous à "Comprendre l'architecture de système d'Identity Manager Service Provider" à la page 22.
- Pour toute information sur la planification d'une architecture Identity Manager Service Provider hautement disponible, reportez-vous à "Comprendre l'architecture HA recommandée de Service Provider " à la page 32.
- Pour toute information sur le déploiement d'Identity Manager en vue de tirer parti de la fonctionnalité Service Provider, reportez-vous à *Sun Identity Manager Service Provider 8.1 Deployment*.

Présentation des autres produits de gestion des identités de Sun

En plus d'Identity Manager, Sun propose les solutions de gestion des identités Sun Java™ System Directory Server Enterprise Edition, Sun OpenSSO Enterprise et Sun Role Manager. Ces produits complètent Identity Manager et, dans le cas de Role Manager, peuvent en étendre les capacités.

Présentation de Sun Java System Directory Server Enterprise Edition

Sun Java System Directory Server Enterprise Edition est un magasin de données LDAP haute performance pour les informations d'identité. Directory Server Enterprise Edition fournit des services d'annuaire de base ainsi que d'autres services de données complémentaires. Microsoft Active Directory et Novell eDirectory sont des offres de services d'annuaire concurrentes.

Présentation d'OpenSSO Enterprise

Sun OpenSSO Enterprise (les anciens Sun Java System Access Manager et Sun Java System Federation Manager) centralise et met en œuvre une stratégie de sécurité complète pour les applications internes et externes et les services Web. Cette solution fournit une fonctionnalité

de contrôle d'accès et de connexion unique (Single Sign-On, SSO) centralisée et sécurisée. Elle permet aussi la gestion d'identité fédérée, qui permet de partager des applications avec des entreprises ayant des technologies de services d'annuaire, de sécurité et d'authentification différentes. Les partenaires fédérés se font mutuellement confiance pour authentifier leurs utilisateurs respectifs et en vérifier les droits d'accès aux services.

Présentation de Sun Role Manager

Sun Role Manager (l'ancien Vaau RBACx) simplifie la compatibilité du contrôle d'accès en gérant l'accès sur la base des rôles d'un utilisateur au sein de l'entreprise et non pas par utilisateur. En créant des rôles basés sur les stratégies d'utilisation et d'entreprise, les sociétés peuvent bénéficier d'une majeure visibilité des accès et gérer ces derniers de manière plus efficace, plus sécurisée et plus conforme.

◆ ◆ ◆ CHAPITRE 2

Architecture du produit

Ce chapitre présente l'architecture du produit Sun™ Identity Manager.

Il se compose des rubriques suivantes :

Comprendre les composants d'Identity Manager

Identity Manager est une application Web J2EE (Java 2 Platform, Enterprise Edition™. La plate-forme J2EE consiste en un ensemble de services, API et protocoles standard du secteur qui fournissent les fonctionnalités nécessaires au développement d'applications d'entreprise Web multiniveaux.

L'architecture du système Identity Manager est distribuée sur quatre niveaux logiques :

- le niveau utilisateur ;
- le niveau d'application ;
- le niveau base de données ;
- le niveau ressources gérées.

Ces différents niveaux sont examinés dans les sections suivantes en commençant par le niveau d'application.

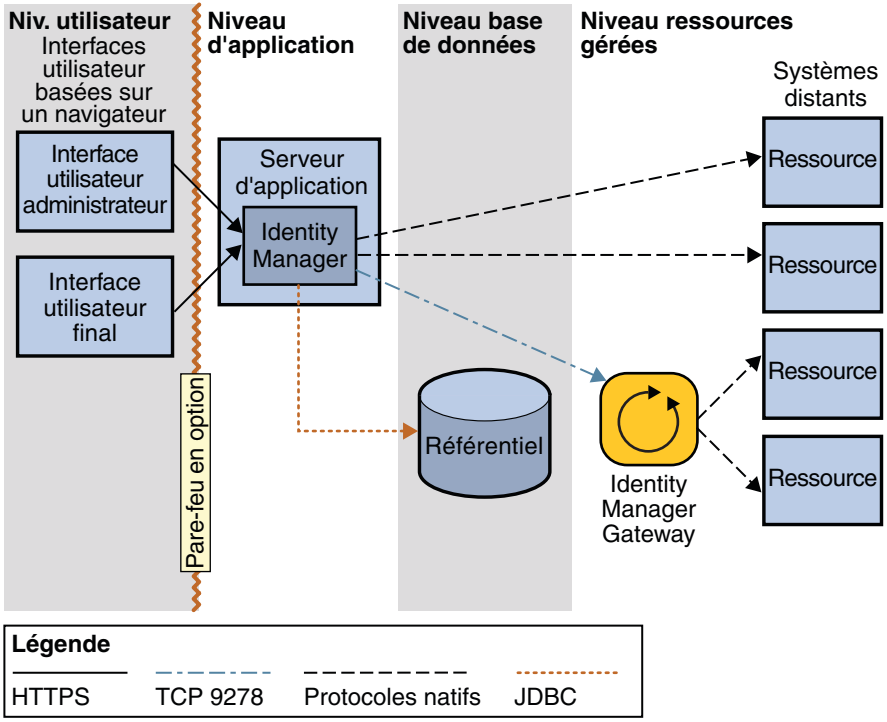

FIGURE 2–1 Architecture du système Identity Manager

Comprendre le niveau d'application

Identity Manager (aussi connu sous le nom de serveur Identity Manager) est installé dans un conteneur Web J2EE à l'intérieur d'un serveur d'application. Le serveur Identity Manager se compose de fichiers JSP™, HTML, d'images et de classes Java™. Les adaptateurs et les connecteurs, qui s'interfacent avec d'autres systèmes informatiques (que l'on appelle aussi des *ressources*), se trouvent également dans Identity Manager, sur le serveur de l'application.

Remarque – Reportez-vous à la section "Serveurs d'application" du *Notes de version de Sun Identity Manager 8.1* pour la liste des serveurs d'application pris en charge.

Étant donné qu'Identity Manager est une application Web, l'interface utilisateur réside sur le serveur d'application et les pages sont servies au niveau utilisateur requête par requête.

L'installation d'Identity Manager sur les serveurs d'application est simple : un programme d'installation graphique basé sur un assistant est fourni et, sur les systèmes UNIX®, un programme d'installation de ligne de commande est également disponible. Le serveur

d'application doit avoir un kit de développement Java (Java Development Kit, (JDK™) intégré ou installé pour exécuter les classes Java qui effectuent les actions au sein d'Identity Manager.

Comprendre le niveau base de données

Identity Manager stocke l'ensemble de ses informations de provisioning et d'état dans le *référentiel* d'Identity Manager. Ce référentiel se compose de tables où sont stockées toutes les données de configuration relatives à Identity Manager. Il constitue une source unique dans laquelle Identity Manager recherche les données et verrouille les objets. Ce référentiel contient également un journal d'audit qui est un historique des actions entreprises dans Product_IDMgr;. Les données d'Identity Manager sont stockées au format XML. Le référentiel peut se situer indifféremment dans des fichiers locaux ou une base de données relationnelle, sauf dans les environnements de production où la base de données relationnelle devient obligatoire.

Remarque – Pour la liste des serveurs de base de données pris en charge, reportez-vous à la section "Serveurs de bases de données de référentiel" du *Notes de version de Sun Identity Manager 8.1*.

Vous remarquerez qu'en dessous d'une quantité minimale d'informations d'identité relatives aux utilisateurs individuels, les données des utilisateurs ne sont pas conservées dans Identity Manager. Dans ce cas, seuls les attributs nécessaires pour identifier et différencier les utilisateurs au sein d'Identity Manager (par exemple, le *nom* et l'*adresse e-mail*) sont enregistrés dans le référentiel.

Identity Manager peut se connecter au référentiel via une connexion JDBC directe ou utiliser la fonctionnalité de source de données mise à disposition par votre serveur d'application.

La fonctionnalité Identity Manager Service Provider requiert un référentiel LDAP supplémentaire pour stocker les informations des utilisateurs. Pour de plus amples détails, reportez-vous à "Comprendre l'architecture de système d'Identity Manager Service Provider" à la page 22.

Comprendre le niveau ressources gérées

Le niveau ressources gérées se compose des applications et systèmes informatiques sur lesquels vous provisionnez et déprovisionnez les comptes utilisateurs. Il inclut Identity Manager Gateway, qui est un assistant permettant à Identity Manager d'interagir avec certaines ressources.

Les adaptateurs et les connecteurs fournissent des fonctions de gestion d'utilisateurs et permettent notamment de créer, mettre à jour, supprimer et lire des comptes utilisateurs ou

encore d'utiliser la fonctionnalité de gestion des changements de mots de passe. Les adaptateurs et les connecteurs peuvent également extraire des informations relatives aux comptes depuis un système distant.

Remarque – Dans la plupart des cas, Identity Manager gère les données utilisateur sur le système distant sans les conserver dans son propre magasin de données.

Certaines ressources courantes requièrent l'utilisation de Sun Identity Manager Gateway. C'est le cas notamment de Microsoft Exchange, Windows Active Directory, Novell eDirectory (l'ancien Netware Directory Services), Lotus Domino et de plusieurs autres solutions (pour la liste complète, reportez-vous à la section "Sun Identity Manager Gateway" du *Notes de version de Sun Identity Manager 8.1*). Gateway s'installe comme un service sous Windows et communique avec Identity Manager en utilisant le port TCP 9278. La communication est engagée depuis Identity Manager en utilisant un protocole chiffré propriétaire. Gateway s'interface ensuite avec les ressources gérées en utilisant les protocoles natifs de ces dernières.

Du point de vue de l'installation, il existe deux types d'adaptateurs et connecteurs : les adaptateurs et connecteurs *Identity Manager* et les *adaptateurs et connecteurs personnalisés*. Les adaptateurs et connecteurs Identity Manager sont préinstallés dans Identity Manager. Les adaptateurs et connecteurs personnalisés doivent quant à eux être copiés dans un répertoire désigné dans le répertoire d'installation d'Identity Manager qui se trouve sur le serveur d'application.

Les adaptateurs personnalisés sont faciles à créer en utilisant le kit *Resource Extension Facility (REF)* d'Identity Manager. Le REF fournit l'API et un certain nombre de modèles d'adaptateurs utilisables par les entreprises pour accélérer le processus de développement. Une fonctionnalité de ressource simple peut être obtenue en implémentant huit méthodes Java seulement.

Comprendre le niveau utilisateur

Le niveau utilisateur se compose des administrateurs et utilisateurs finaux qui interagissent avec Identity Manager au travers de l'une des interfaces utilisateur. La principale interface utilisateur du produit est un navigateur Web qui communique avec Identity Manager via HTTPS. Les deux IU basées sur un navigateur, l'*interface utilisateur administrateur* et l'*interface utilisateur final*, sont principalement composées de pages HTML même si certaines fonctions peuvent utiliser des applets Java.

Pour des raisons de clarté, seule l'interface utilisateur administrateur et l'interface utilisateur final sont illustrées à la Figure 2–1. Le niveau utilisateur contient toutefois d'autres interfaces utilisateur. Par exemple : l'interface téléphonique IVR, l'IDE d'Identity Manager, l'interface de services Web SPML et la console d'Identity Manager.

Comprendre les directives de séparation des systèmes et de proximité physique

Cette section contient les directives de base précisant quels composants d'Identity Manager doivent s'exécuter sur tel ou tel serveur. Elle contient également les recommandations relatives aux composants qui doivent être installés à proximité les uns des autres pour minimiser les problèmes de performance susceptibles de se poser suite à la latence et à l'engorgement du réseau.

Remarque – Seules les directives de base sont indiquées. Pour toute information sur la conception d'une architecture Identity Manager haute disponibilité, reportez-vous au Chapitre 3, “Clustering et haute disponibilité”.

Dans un environnement de développement, le serveur d'application et la base de données peuvent être sur la même machine. Dans les environnements de test et de production toutefois, chaque instance d'Identity Manager doit être installée sur son propre serveur dédié. La base de données relationnelle a également besoin d'un serveur dédié.

Identity Manager Gateway, si requis, doit être installé sur une ou plusieurs machines Windows. La passerelle est un composant léger qui ne nécessite donc pas de serveur dédié. Tous les domaines Windows gérés par un Gateway doivent faire partie de la même forêt. La gestion de domaines à travers les limites d'une forêt n'est pas prise en charge. Si vous avez plusieurs forêts, installez au moins un Gateway dans chacune. Dans le cadre de la production, la passerelle doit être rendue hautement disponible. Pour de plus amples détails, reportez-vous à “Rendre la passerelle hautement disponible” à la page 30.

Dans un environnement de production, le gros du trafic réseau a lieu entre les serveurs de base de données et d'application. Ces deux environnements doivent être sur le même LAN avec la plus courte connexion réseau directe possible. Les instances de Gateway, de même que les ressources gérées, n'ont pas besoin d'être sur le même réseau qu'Identity Manager.

Si Identity Manager sera utilisé pour les utilisateurs externes dans une configuration Service Provider, un ensemble de serveurs Web doit être installé dans une DMZ. Pour de plus amples détails, reportez-vous à “Comprendre l'architecture HA recommandée de Service Provider ” à la page 32.

Comprendre SPML et l'architecture de système des services Web

SPML (Service Provisioning Markup Language) et les services Web d'Identity Manager peuvent être utilisés pour implémenter un front-end pour Identity Manager. Identity Manager envoie et reçoit des messages et des réponses SPML en utilisant le protocole HTTPS.

Pour plus d'informations sur SPML et les services Web, reportez-vous à la section *Sun Identity Manager 8.1 Web Services*.

Comprendre l'architecture de système d'Identity Manager Service Provider

Si la fonctionnalité Identity Manager Service Provider est implémentée, un cinquième niveau est requis. Ce niveau, qui s'appelle le niveau Web, se compose de un ou plusieurs serveurs situés dans une DMZ. Aucun composant d'Identity Manager n'est installé dans le niveau Web. À la place, les serveurs Web de la DMZ prennent en charge un ou plusieurs serveurs d'application du niveau d'application en répondant aux demandes de pages Web. Ajouter un ou plusieurs serveurs Web au niveau Web améliore l'évolutivité tandis que mettre les serveurs Web dans une DMZ renforce la sécurité du réseau.

La fonctionnalité Service Provider requiert également un référentiel LDAP. Ce référentiel réside dans le niveau base de données. Le référentiel LDAP pouvant être une ressource gérée, le serveur LDAP peut être compris comme résidant également dans le niveau ressources gérées.

Remarque – Dans une implémentation fournisseur de services uniquement, un référentiel Identity Manager est recommandé en plus du référentiel LDAP mais n'est pas obligatoire. Si aucun référentiel Identity Manager n'est déployé, certaines fonctionnalités, notamment certaines capacités de génération de rapports, ne seront pas disponibles.

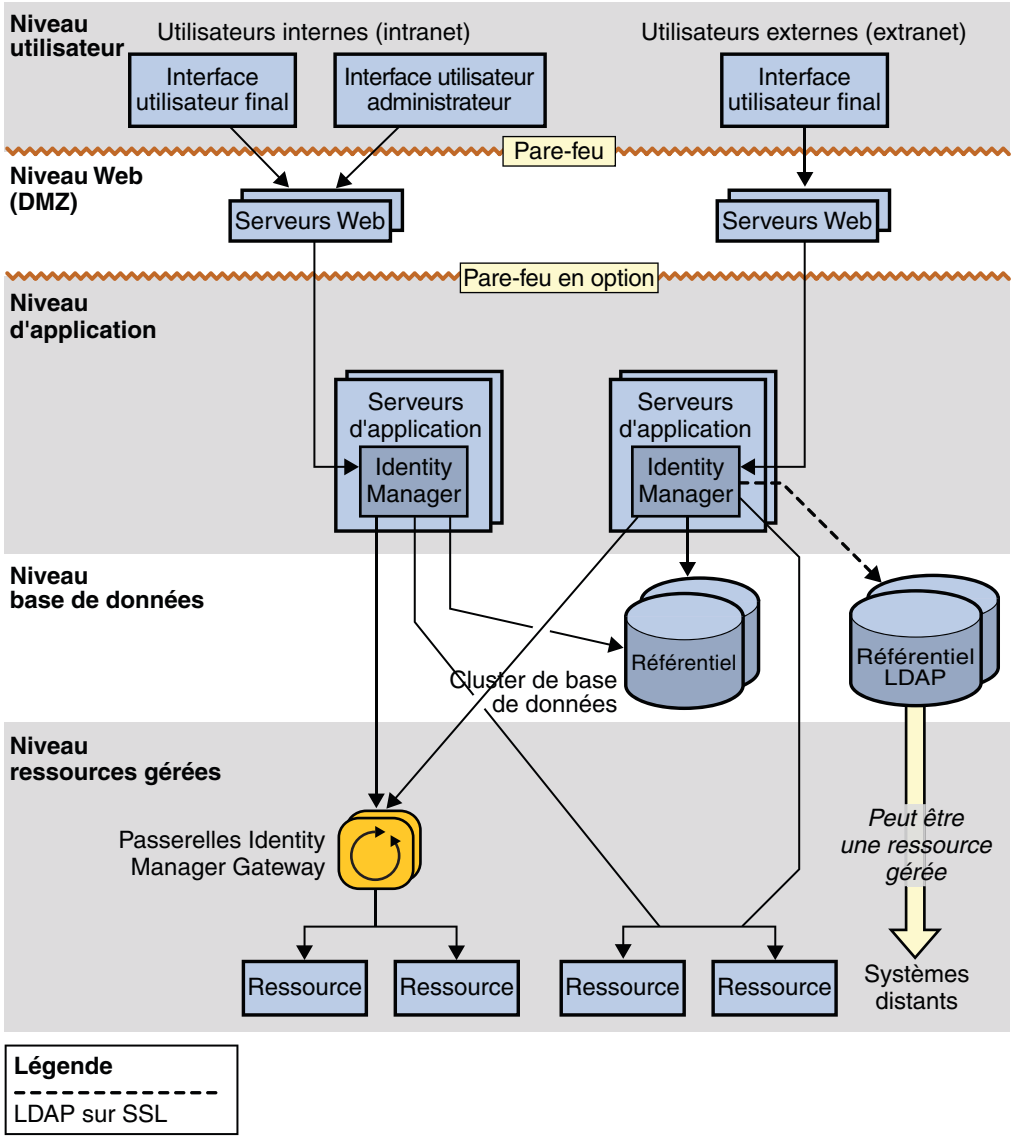

FIGURE 2–2 Architecture de système d'Identity Manager Service Provider

◆ ◆ ◆ CHAPITRE 3

Clustering et haute disponibilité

Ce chapitre explique la mise en œuvre d'un environnement Identity Manager haute disponibilité/à tolérance de pannes (HA/FT).

Remarque – Veuillez consulter la documentation de vos serveurs Web et d'application ainsi que celle du fournisseur de votre base de données pour prende connaissance des pratiques recommandées pour assurer un déploiement hautement disponible avec chacune de ces technologies. Ce guide ne remplace pas les recommandations spécifiques des fournisseurs de vos serveurs Web.

Évaluation des besoins de disponibilité

Cette section explique comment évaluer l'ampleur de la disponibilité requise par votre déploiement spécifique.

Évaluation du coût de l'indisponibilité

Identity Manager ne se trouvant pas dans le chemin des transactions entre les utilisateurs généraux et les systèmes et applications auxquels ils ont déjà accès, l'indisponibilité d'Identity Manager n'est pas aussi dramatique que vous ne pourriez l'imaginer. Si Identity Manager n'est pas disponible, les utilisateurs finaux continuent à pouvoir accéder aux ressources au travers de leurs comptes provisionnés.

Le principal coût de l'indisponibilité d'Identity Manager est une faible productivité. Si Identity Manager est hors service, les utilisateurs finaux ne peuvent pas utiliser Identity Manager pour accéder aux systèmes qui sont verrouillés ou pour lesquels ils n'ont pas été provisionnés.

Pour calculer le coût de l'indisponibilité, le premier chiffre à prendre en compte est le coût moyen de la productivité perdue à cause de l'incapacité dans laquelle sont les utilisateurs d'accéder aux ressources informatiques au sein de l'entreprise. Dans le cadre de notre évaluation, ce chiffre est la *productivité par heure-personne*.

L'autre valeur à déterminer est le pourcentage d'utilisateurs finaux au sein de la population d'utilisateurs ayant besoin d'utiliser Identity Manager à l'instant t. Cette population se compose normalement des nouveaux embauchés devant encore être provisionnés et des utilisateurs finaux ayant oublié leur mot de passe, si la gestion de ceux-ci est incluse dans le déploiement.

Considérez la situation hypothétique suivante :

Nombre total d'employés	20 000
Nombre de réinitialisations de mots de passe par jour	130
Nombre de nouveaux embauchés par jour	30
Nombre d'heures dans un jour ouvrable	8

Dans ce cas de figure particulier, vous devez effectuer les calculs suivants :

- Nombre d'employés ayant besoin d'Identity Manager à toute heure h = (130 + 30) / 8 = 20
- Pourcentage d'employés ayant besoin d'Identity Manager à tout instant t = 20 / 20 000 = 0,1% ou 1 sur 1000

Ces chiffres peuvent vous permettre d'estimer le coût d'une panne d'Identity Manager :

Productivité par heure-personne	100 dollars	
Perte de productivité	0,5	(baisse de 50% de la productivité due à l'impossibilité d'accéder au système)
Nombre de personnes concernées	20	
Sous-total	1000 dollars	

Durée de la panne	2 heures
Perte immédiate totale	2000 dollars

Cet exemple montre que même si le nombre des utilisateurs gérés par Identity Manager est élevé, celui de ceux qui ont besoin d'Identity Manager pour pouvoir accéder aux systèmes à un instant t est en général bas.

Un autre point à prendre en compte est le temps nécessaire pour remettre en ligne un système comme Identity Manager qui est normalement inférieur à celui nécessaire pour exécuter les processus de provisioning manuels qu'Identity Manager automatise. Ainsi, tout en ayant un coût, l'indisponibilité d'Identity Manager est en général moins onéreuse que le coût de l'utilisation de processus manuels pour octroyer aux utilisateurs l'accès aux ressources.

Comprendre les causes de l'indisponibilité

Dans le cadre de la planification d'un déploiement haute disponibilité d'Identity Manager, il convient d'examiner les causes d'indisponibilité.

Celles-ci incluent les éléments suivants :

- erreur humaine ;
- panne de matériel ;
- panne de logiciel ;
- indisponibilité programmée (mises à niveau matérielles et logicielles) ;
- performance médiocre (indisponibilité perçue).

Calcul du retour sur investissement

Identity Manager automatise les processus et réduit la perte de productivité. Le retour sur investissement d'une architecture Identity Manager hautement disponible s'obtient en minimisant l'indisponibilité et en évitant les pertes de productivité.

Vous pouvez utiliser le coût d'indisponibilité pour déterminer l'ampleur de la disponibilité nécessaire pour Identity Manager. En général, un investissement modéré visant à rendre Identity Manager hautement disponible est justifié.

Lorsque vous calculez le coût de cet investissement, n'oubliez pas que l'achat de matériel et de logiciels HA/FT n'est qu'une partie de la mise en œuvre d'une solution disponible. La nécessité d'avoir une équipe compétente en mesure de maintenir la solution activée et en fonctionnement constitue un coût supplémentaire.

Comprendre l'ensemble des fonctionnalités haute disponibilité d'Identity Manager

Identity Manager est conçu pour tirer parti d'une eventuelle infrastructure HA existante. Par exemple, Identity Manager ne nécessite pas de cluster de serveurs d'application pour atteindre une haute disponibilité mais peut utiliser un cluster s'il y en a un.

Le diagramme suivant montre les principaux composants d'Identity Manager déployés dans une architecture non redondante. Les sections qui suivent décrivent la façon dont le référentiel, le serveur d'application et la passerelle d'Identity Manager peuvent être rendus hautement disponibles.

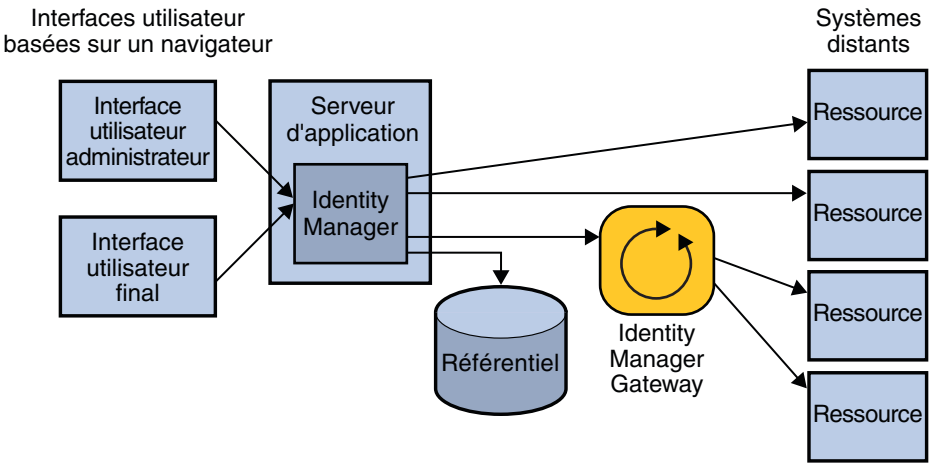

FIGURE 3–1 Architecture de système Identity Manager standard

Remarque – Reportez-vous à "Comprendre les directives de séparation des systèmes et de proximité physique" à la page 21 pour savoir quels composants doivent être installés à proximité l'un de l'autre pour minimiser les problèmes de performance susceptibles de se poser suite à la latence et à l'engorgement du réseau.

Rendre le référentiel hautement disponible

Identity Manager stocke l'ensemble de ses informations de provisioning et d'état dans le référentiel d'Identity Manager.

La disponibilité de l'instance de la base de données stockant le référentiel d'Identity Manager est l'élément le plus critique pour réaliser un déploiement hautement disponible d'Identity Manager. Le référentiel est la représentation de l'ensemble de l'installation d'Identity Manager et les données qu'il contient doivent être protégées comme dans le cas d'autres applications de base de données importantes. Au minimum, il faut effectuer des sauvegardes régulières.

Remarque – N'hébergez pas le référentiel d'Identity Manager sur un système virtuel tel qu'une machine virtuelle VMware car la performance (le nombre de transactions par seconde) serait considérablement réduite.

Il ne peut y avoir qu'une image du référentiel. Il n'est pas possible d'avoir deux bases de données séparées pour Identity Manager et de tenter de les synchroniser de nuit. Sun recommande d'utiliser les capacités de clustering ou de mise en miroir de votre base de données pour assurer la tolérance de pannes.

Rendre le serveur d'application hautement disponible

Identity Manager peut s'exécuter au sein d'un serveur d'application et profiter de la disponibilité accrue et de l'équilibrage de charge fournis par un cluster. Identity Manager n'utilise cependant aucune fonctionnalité J2EE nécessitant le clustering.

Identity Manager utilise l'objet de session HTTP disponible au travers de l'API Servlet. Cet objet de session suit la visite de tout utilisateur qui se connecte et effectue des actions. Dans un cluster, vous pouvez en option avoir plusieurs nœuds gèrant les demandes d'un utilisateur au cours d'une session donnée. Cela n'est toutefois en général pas recommandé et la plupart des installations sont configurées pour envoyer l'ensemble des demandes d'un utilisateur pour une session donnée au même serveur.

Il est possible d'accroître la disponibilité et la capacité du serveur d'application exécutant Identity Manager même si vous ne configurez pas de cluster. Pour cela, vous devez installer plusieurs serveurs d'application connectés via Identity Manager au même référentiel et mettre un équilibreur de charge avec *affinité de session* devant tous les serveurs d'application.

Remarque – Pour plus d'informations sur l'affinité de session, consultez la "Foire aux questions relative à l'affinité de session et à la persistance des sessions" à la page 40.

Identity Manager exécute certaines tâches en arrière-plan. C'est le cas, par exemple, des tâches de réconciliation programmées. Ces tâches sont stockées dans la base de données et peuvent être sélectionnées par n'importe quel serveur Identity Manager qui les exécutera. Identity Manager utilise la base de données pour assurer que ces tâches sont toujours exécutées jusqu'à la fin même en cas de basculement sur un autre nœud.

Configuration d'Active Sync Clustering sur les nœuds de serveur d'application

Le paramètre `sources.hosts` du fichier `Waveset.properties` contrôle les hôtes qui, dans un environnement multi-instance, sont utilisés pour exécuter les demandes Active Sync. Ce paramètre fournit la liste des hôtes sur lesquels les adaptateurs de ressources peuvent s'exécuter. Mettre ce paramètre sur *localhost* ou *null* permettra aux adaptateurs de source de s'exécuter sur tout hôte de la ferme de serveurs (ceci est le comportement par défaut). En listant un ou plusieurs hôtes, vous pouvez restreindre l'exécution à cette liste. Si vous avez des mises à jour entrantes provenant d'un autre système allant vers un hôte particulier, utilisez le paramètre `sources.hosts` pour enregistrer les noms des hôtes.

De plus, vous pouvez définir une propriété nommée `sources.` *nomRessource* `.hosts`, qui contrôlera où la tâche Active Sync de la ressource sera exécutée. Remplacez *nomRessource* par le nom de l'objet ressource que vous voulez spécifier.

Rendre la passerelle hautement disponible

Identity Manager requiert une passerelle légère pour gérer les ressources auxquelles il n'est pas possible d'accéder directement depuis le serveur. Ces ressources peuvent être, par exemple, des systèmes qui requièrent des appels d'API côté client spécifiques de la plate-forme. Par exemple, si Identity Manager s'exécute sur un serveur d'application UNIX basé sur UNIX, il n'est pas possible d'effectuer des appels NTLM ou ADSI en direction de domaines NT ou Active Directory gérés. Étant donné qu'Identity Manager a besoin d'une passerelle pour gérer ces ressources, il est important de s'assurer qu'Identity Manager Gateway a été rendu hautement disponible.

Pour empêcher que Gateway ne constitue un point de panne unique, Sun recommande d'avoir plusieurs machines exécutant une instance de Gateway. Un périphérique de routage réseau doit être configuré pour assurer le basculement si l'instance principale de Gateway s'arrête. Le périphérique de basculement doit être configuré pour l'affinité de session et utiliser un modèle à tour de rôle. Ne placez pas Gateway derrière un périphérique qui procède à l'équilibrage de charge ! Une telle configuration ne serait pas prise en charge et entraînerait l'échec de certaines fonctionnalités d'Identity Manager.

Tous les domaines Windows gérés par un Gateway doivent faire partie de la même forêt. La gestion de domaines à travers les limites d'une forêt n'est pas prise en charge. Si vous avez plusieurs forêts, installez au moins un Gateway dans chacune.

Les outils de contrôles Win32 peuvent être configurés pour observer le processus `gateway.exe` sur l'hôte Win32. En cas de panne de `gateway.exe`, le processus peut être redémarré automatiquement.

Comprendre l'architecture HA recommandée

Le diagramme suivant illustre l'architecture d'Identity Manager recommandée par Sun en l'absence d'infrastructure d'application Web existante.

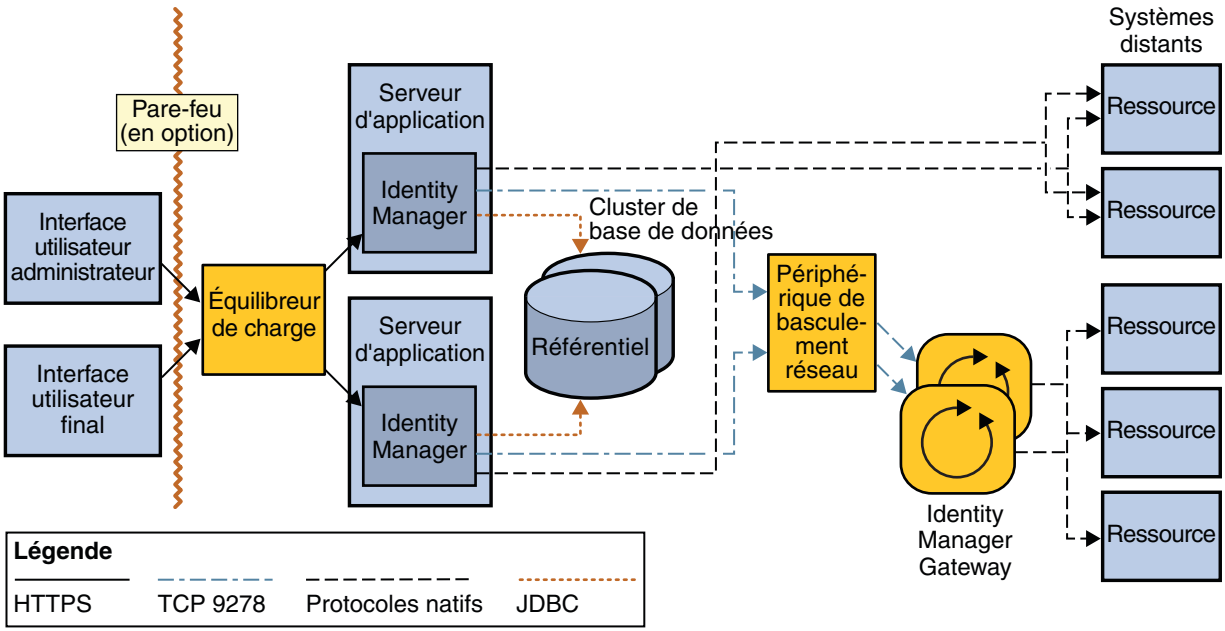

FIGURE 3–2 Architecture haute disponibilité d'Identity Manager

Dans un développement réel, l'infrastructure de serveur d'application redondante existante doit être utilisée autant que possible. L'avantage de cette architecture est qu'elle utilise uniquement des équilibreurs de charge pour assurer la redondance au niveau du serveur d'application. Les équilibreurs de charge avec affinité de session détectent les instances de serveur d'application en panne et basculent sur des instances actives. Les équilibreurs de charge sont également utilisés pour fournir une mise à l'échelle horizontale dans l'environnement Web en répartissant les demandes des utilisateurs dans un cluster de serveurs.

Même s'il s'agit là d'une architecture simple, les caractéristiques de temps de disponibilité sont comparables à celles de déploiements plus complexes. Compte tenu par ailleurs de cette simplicité, il y a moins d'éléments logiciels à actualiser et contrôler et moins d'éléments risquant de tomber en panne. Par ailleurs, l'erreur humaine étant la première cause d'indisponibilité, une solution relativement simple peut permettre d'obtenir de meilleures caractéristiques de temps de disponibilité qu'une autre plus complexe. Ces réponses ne sont toutefois pas universellement valides. L'essentiel est de comprendre toutes les causes d'indisponibilité et de choisir l'architecture se traduisant par la meilleure disponibilité pour l'investissement envisagé.

Remarque – Il serait impossible de décrire toutes les architectures HA différentes possibles avec une application Web telle qu'Identity Manager.

Étant donné qu'Identity Manager peut être déployé selon tout un éventail de combinaisons, il pourra être plus économique d'identifier l'infrastructure existante et de l'utiliser le plus possible pour déployer Identity Manager.

Comprendre l'architecture HA recommandée de Service Provider

Si la fonctionnalité Identity Manager Service Provider doit être utilisée, Sun recommande d'ajouter un niveau Web entre le niveau utilisateur et le niveau d'application. Ce niveau Web sera constitué de un ou plusieurs serveurs Web résidant dans une zone démilitarisée (DMZ) séparée par un pare-feu du niveau d'application.

Un référentiel LDAP est obligatoire si la fonctionnalité Service Provider est utilisée. Si Identity Manager prendra uniquement en charge des clients de l'extranet, un référentiel Identity Manager standard est recommandé mais pas obligatoire. Sinon, si Identity Manager doit prendre en charge à la fois les utilisateurs de l'intranet et ceux de l'extranet, un référentiel LDAP et un référentiel Identity Manager standard sont nécessaires.

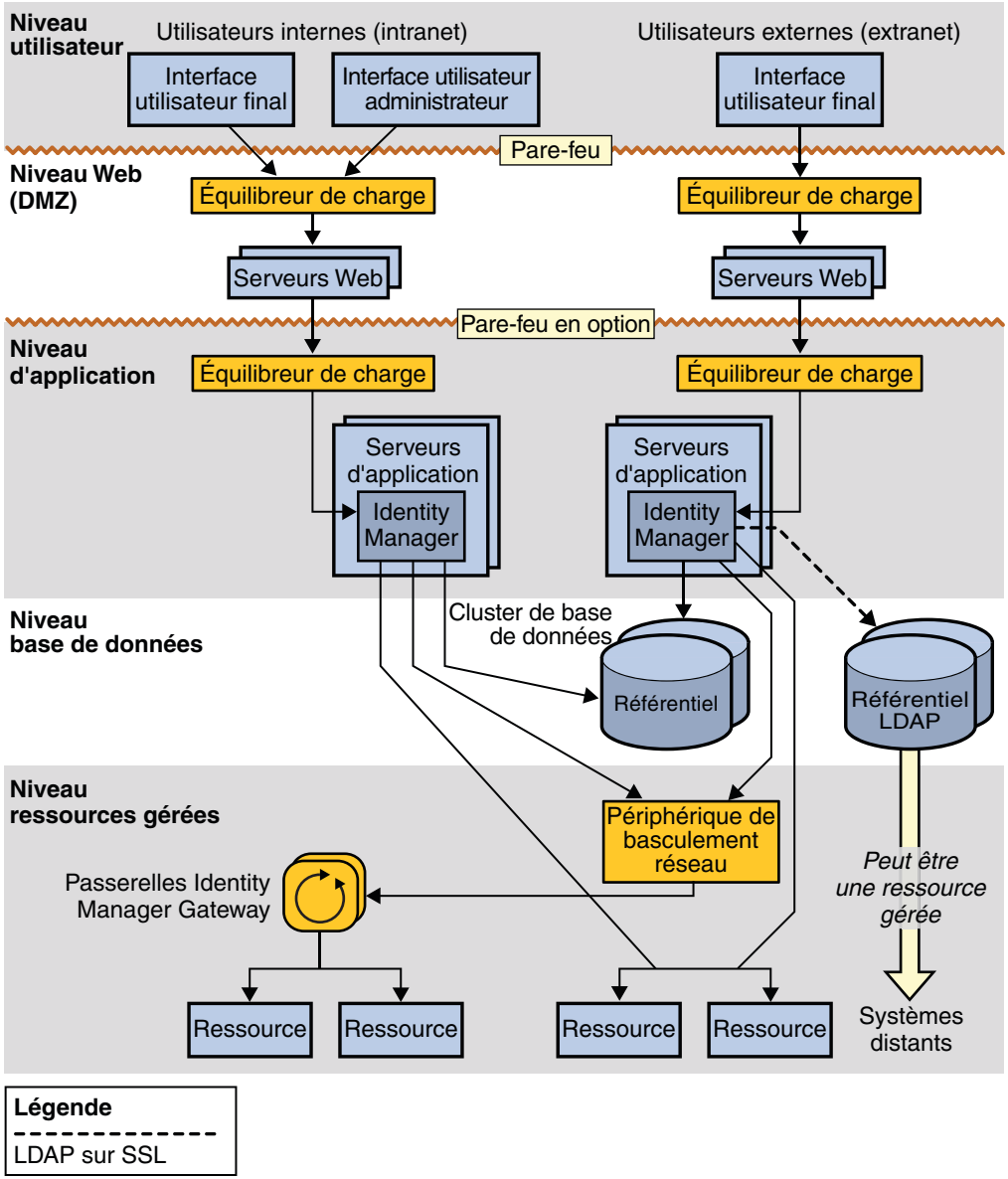

FIGURE 3–3 Architecture haute disponibilité d'Identity Manager Service Provider

Comprendre les scénarios de panne

Cette section contient huit scénarios de panne et compare deux déploiements, l'un avec persistance des sessions, l'autre sans.

- Le déploiement *avec* persistance des sessions assure l'affinité de session au travers d'un équilibreur de charge. Ce déploiement a dans un cluster plusieurs instances ayant une forme de persistance des sessions activée de sorte que les changements de session sont écrits dans un nœud de référentiel physiquement distinct.
- Le déploiement *sans* persistance des sessions assure l'affinité de session au travers d'un équilibreur de charge et a plusieurs instances ne faisant pas partie d'un cluster.

Scénario 1 : Scénario Pas de flux de travaux

Description du scénario

L'utilisateur final ou l'administrateur édite un formulaire ne faisant pas partie d'un flux de travaux. L'instance sur laquelle l'utilisateur a une session établie tombe en panne.

Sans persistance des sessions

Expérience utilisateur : basculement non transparent. Lorsqu'il envoie le formulaire, l'utilisateur est ramené à la page de connexion.

Étapes de reprise : l'utilisateur entre de nouveau son nom d'utilisateur et son mot de passe. Identity Manager traite alors le formulaire et présente les résultats dans la page suivant immédiatement la connexion.

Avec persistance des sessions

Expérience utilisateur : le formulaire de l'utilisateur est envoyé et les résultats sont retournés sans que l'utilisateur ne soit déconnecté ni doive consécutivement se reconnecter.

Étapes de reprise : aucune action de l'utilisateur n'est nécessaire.

Autres exemples de scénarios

- Un utilisateur final s'est connecté et a récupéré des résultats de recherche pour des utilisateurs ou d'autres objets du référentiel lorsque l'instance tombe en panne.
- Un administrateur est sur le point d'envoyer une demande « Réinitialiser le mot de passe » ou « Éditer l'utilisateur » en utilisant l'interface Administrateur lorsque l'instance tombe en panne.

Scénario 2 : Scénario Flux de travaux en cours

Description du scénario

L'utilisateur final ou l'administrateur a édité un formulaire qui a déclenché un flux de travaux. L'instance sur laquelle le flux de travaux s'exécute est en général la même que celle sur laquelle la session de l'utilisateur se trouve sauf dans le cas de certaines tâches programmées où ces instances peuvent différer. Ces instances tombent en panne alors que le flux de travaux est en cours.

Sans persistance des sessions

Expérience utilisateur : basculement non transparent. L'envoi du formulaire ramène l'utilisateur à la page de connexion. L'instance de la tâche de flux de travaux en cours d'exécution devrait figurer dans le référentiel mais comme le nœud d'exécution est en panne, le statut du flux de travaux sera « arrêté ».

Étapes de reprise : le flux de travaux doit être envoyé de nouveau. Cela doit se faire en revenant au même formulaire et en entrant de nouveau les informations déjà utilisées pour déclencher le flux de travaux avant la défaillance du nœud.

L'envoi des mêmes données de demande peut fonctionner dans certains cas mais pas dans tous. Si le flux de travaux provisionne pour plusieurs ressources pendant son exécution et que certaines de ces ressources étaient provisionnées avant la défaillance, le nouvel envoi du flux de travaux par l'utilisateur devra tenir compte des ressources « déjà provisionnées ». Vous remarquerez que le flux de travaux arrêté reste dans le référentiel jusqu'à ce que `resultLimit` expire sur l'objet `TaskInstance`.

Avec persistance des sessions

Expérience utilisateur : basculement non transparent. L'utilisateur n'est pas déconnecté car sa session est continuée et rétablie dans la nouvelle instance. L'envoi du formulaire, toutefois, se traduira probablement par une erreur car le flux de travaux sera arrêté. Ce basculement n'est pas transparent car des actions de reprise sont nécessaires.

Étapes de reprise : identiques à celles du mode Sans persistance des sessions. L'utilisateur doit envoyer de nouveau la demande qui a déclenché le flux de travaux précédent avec des paramètres identiques ou modifiés.

Autres exemples de scénarios

- Un utilisateur final vient d'envoyer une demande d'auto-enregistrement pour créer un compte Identity Manager quand l'instance tombe en panne.
- Un administrateur vient d'envoyer une demande « Réinitialiser le mot de passe » qui est en cours quand l'instance tombe en panne.

Scénario 3 : Scénario Flux de travaux en suspens ou endormi

Description du scénario

Ce scénario couvre les cas de figure dans lesquels le flux de travaux a démarré mais attend une action manuelle de la part d'un approbateur.

Sans persistance des sessions

Expérience utilisateur : basculement transparent en ce qui concerne l'approbateur, du moment que ce dernier ne s'est pas encore connecté. Après la défaillance du nœud, l'approbateur se connectant verra quand même la demande d'approbation dans sa boîte de réception et ce, même si cette demande a été déclenchée depuis un nœud qui n'est plus activé.

Étapes de reprise : aucune action de l'utilisateur n'est nécessaire.

Avec persistance des sessions

Expérience utilisateur : identique à celle du mode Sans persistance des sessions.

Étapes de reprise :identiques à celles du mode Sans persistance des sessions.

Autres exemples de scénarios

- Le flux de travaux est à l'état de sommeil, il s'agit par exemple d'une action manuelle qui reste endormie jusqu'à une date d'ouverture ou de clôture pour un employé.
- Un administrateur a envoyé une demande de création d'utilisateur qui attend qu'un approbateur se connecte et l'approuve. Le nœud depuis lequel la demande a été envoyée est tombé en panne avant que l'approbateur n'approuve la demande.

Scénario 4 : Scénario Édition d'un élément de travail

Description du scénario

Ce scénario inclut les cas de figure dans lesquels un utilisateur est en train d'éditer un élément de travail et où le nœud sur lequel l'utilisateur a une session tombe en panne avant qu'il puisse envoyer l'élément de travail en question.

Sans persistance des sessions

Expérience utilisateur : basculement non transparent. Lorsque le formulaire d'édition de l'élément de travail est envoyé, l'utilisateur est déconnecté et ramené à la page de connexion.

Étapes de reprise : lors du renvoi des données d'identification de connexion, l'élément de travail de l'utilisateur est marqué comme étant terminé et le flux de travaux peut reprendre à partir de

ce point. Le flux de travaux doit être sélectionné par le nouveau mode pour l'exécution à partir du point où l'action manuelle de l'utilisateur est marquée comme étant terminée.

Avec persistance des sessions

Expérience utilisateur : lorsque le formulaire d'édition de l'élément de travail est envoyé, l'utilisateur voit l'effet de son envoi, par exemple le formulaire suivant dans le flux de travaux personnalisés s'il y en a un, ou un message de réussite.

Étapes de reprise : aucune action de l'utilisateur n'est nécessaire.

Autres exemples de scénarios

- Un utilisateur final remplit un formulaire associé à une action manuelle dans un flux de travaux personnalisé, par exemple pour demander l'accès à des ressources spécifiques. Le nœud sur lequel réside la session de l'utilisateur tombe en panne avant que ce dernier ne parvienne à envoyer sa demande.
- Un administrateur s'est connecté à Identity Manager et a ouvert une demande d'approbation d'édition. Le nœud sur lequel réside la session de l'administrateur tombe en panne avant que ce dernier ne parvienne à envoyer sa demande.

Scénario 5 : Scénario Tâches programmées en cours

Description du scénario

Ces scénarios couvrent les cas de figure dans lesquels une panne de nœud se produit alors qu'une réconciliation est en cours ou qu'un rapport est en cours d'exécution.

Sans persistance des sessions

Expérience utilisateur : la tâche programmée s'arrête en cours.

Étapes de reprise : la tâche programmée qui était en cours doit être redémarrée. La tâche recommencera au début (pas à partir du point de panne). Cela revient à créer et démarrer une nouvelle tâche.

Avec persistance des sessions

Expérience utilisateur : identique à celle du mode Sans persistance des sessions.

Étapes de reprise : identiques à celles du mode Sans persistance des sessions.

Autres exemples de scénarios

- Un adaptateur Active Sync est configuré pour s'exécuter sur le nœud en panne.

Scénario 6 : Scénario Tâche programmée en suspens

Description du scénario

Ces scénarios couvrent les cas de figure dans lesquels le flux de travaux personnalisé d'un utilisateur a programmé une tâche pour qu'elle s'exécute à une date ultérieure sur un nœud spécifique. Le nœud sur lequel la tâche a été programmée tombe en panne avant la date prévue.

Sans persistance des sessions

Expérience utilisateur : le basculement est transparent en ce qui concerne les actions de reprise requises pour assurer que la tâche en question s'exécute à l'heure programmée.

Étapes de reprise : la tâche programmée est reprise par un nœud actif lorsque l'heure d'exécution programmée arrive.

Avec persistance des sessions

Expérience utilisateur : identique à celle du mode Sans persistance des sessions.

Étapes de reprise : identiques à celles du mode Sans persistance des sessions.

Autres exemples de scénarios

- Dans le processus de création d'un compte utilisateur, le scannage des tâches différées est utilisé pour implémenter l'activation du compte à une date d'ouverture ou sa désactivation à une date de clôture. Le nœud sur lequel la tâche a été programmée tombe en panne avant la date d'ouverture ou de clôture prévue.
- Un rapport est programmé pour s'exécuter à une heure ultérieure ou une réconciliation est programmée pour s'exécuter à une heure spécifique et, le nœud sur lequel la tâche a été programmée tombe en panne avant l'heure prévue.

Scénario 7 : Scénario Demande de services Web pas encore reçue par Identity Manager

Description du scénario

Ces scénarios couvrent les cas de figure dans lesquels l'IUG d'Identity Manager n'est pas utilisée pour lancer le provisioning. À la place, l'interface utilisateur est fournie par une application qui émet en interne un appel vers Identity Manager en utilisant SPML ou une autre interface de service Web personnalisée. Ici, la session utilisateur relative à l'utilisateur qui suit l'IG est gérée au moyen de l'application appelante. Pour Identity Manager, les demandes sont toutes lancées en tant qu'objet « soapadmin ».

Dans un tel cas d'utilisation, ce scénario de panne couvre le cas dans lequel la demande par l'intermédiaire du point d'extrémité Identity Manager n'a pas encore été reçue et où le nœud ciblé est tombé en panne.

Sans persistance des sessions

Expérience utilisateur : basculement transparent. Les données d'identification de l'administrateur SOAP sont transférées pour chaque demande SOAP, soit via câble soit au sein d'Identity Manager par le biais du paramètre `Waveset.properties`. Du moment que le nœud qui devait recevoir cette demande SOAP ne l'a pas reçue avant de tomber en panne, le basculement est transparent avec ou sans persistance des sessions.

Étapes de reprise : aucune action n'est nécessaire. La demande SOAP est envoyée à un nœud actif qui l'exécute.

Avec persistance des sessions

Expérience utilisateur : identique à celle du mode Sans persistance des sessions.

Étapes de reprise : identiques à celles du mode Sans persistance des sessions.

Scénario 8 : Scénario Demande de services Web en cours par Identity Manager

Description du scénario

Ce scénario est similaire au scénario sept. La seule différence est que le flux de travaux est en cours quand le nœud tombe en panne, ou que le nœud a reçu la demande SOAP avant de tomber en panne.

Sans persistance des sessions

Expérience utilisateur : ce scénario est similaire au scénario deux (flux de travaux en cours). Le flux de travaux est marqué comme étant arrêté et l'utilisateur voit une erreur en tant que résultat de la demande SOAP.

Étapes de reprise : l'utilisateur doit renvoyer le formulaire avec des paramètres similaires ou modifiés (selon le point du flux de travaux auquel la panne s'est produite) en utilisant l'interface utilisateur dans l'application tiers.

Avec persistance des sessions

Expérience utilisateur : identique à celle du mode Sans persistance des sessions.

Étapes de reprise : identiques à celles du mode Sans persistance des sessions.

Foire aux questions relative à l'affinité de session et à la persistance des sessions

L'affinité de session doit-elle être activée lors de la mise à l'échelle horizontale des serveurs d'application ?

Oui.

Devez-vous activer la persistance des sessions lors de la mise à l'échelle horizontale des serveurs d'application ?

À moins que les exigences de votre entreprise ne mettent l'accent sur la nécessité d'un basculement transparent dans les situations limitées où la persistance des sessions peut faire une différence, Sun recommande de ne pas utiliser la persistance des sessions. La persistance des sessions a un coût en matière de performance et à moins que les basculements transparents ne soient strictement requis par les exigences de fonctionnement, laissez la persistance des sessions désactivée.

Si vous étudiez les scénarios de panne documentés dans "Comprendre les scénarios de panne" à la page 34, dans six des huit scénarios il n'y a pas de différence au niveau de l'expérience de l'utilisateur final ou des actions de reprise requises, que la persistance des sessions soit activée ou non. Seuls les scénarios un et quatre comprennent des différences entre les scénarios avec persistance des sessions et ceux sans persistance des sessions.

Dans ces deux scénarios, la persistance des sessions peut fournir une certaine transparence des basculements mais elle influe négativement sur la performance. Selon la taille des objets de session, le référentiel utilisé pour la persistance des sessions et l'optimisation du code de gestion de sessions de votre serveur d'application spécifique, la baisse de performance peut être comprise entre 10 et 20 %, voire plus.

Devez-vous avoir plusieurs instances du serveur d'application dans un cluster en cas de mise à l'échelle horizontale ?

Il n'est absolument pas nécessaire d'avoir plusieurs instances du serveur d'application à moins que vous ne vouliez bénéficier de la persistance des sessions. Un basculement sans persistance des sessions peut être obtenu même si tous les nœuds de serveur d'application ne sont pas dans un cluster.