Cyber-résilience

GUIDES COMPARATIFS

CONFORMITÉ DES ACCÈS IDENTITÉS, ANNUAIRES, MÉTA-ANNUAIRE, GESTION DES MOTS DE PASSE

LES GRANDS THÉMAS

Guides comparatifs

A PROPOS **DE CE GUIDE**

Conformité des accès : identité, annuaire, SSO

1 UTILISER CE GUIDE

La structure et le contenu de ces guides constituent une excellente base pour préparer un cahier des charges ou un comparatif.

En savoir plus

2 DROITS D'USAGE

guidescomparatifs.com autorise toute personne physique ou morale à utiliser et reproduire ce document pour son propre usage à condition d'en citer la source.

En savoir plus

3 COMMUNAUTÉ

Partagez votre expertise, échangez autour de vos projets IT et faites-nous part de vos retours d'expérience sur l'utilisation des modèles de cahiers des charges.

En savoir plus

4 INFOGRAPHIES

Des statistiques, comptes rendus d'étude, éléments de réflexion sur une cinquantaine de sujets IT. Téléchargez librement ces infographies sur guidescomparatifs.com.

En savoir plus

5 INTERVIEWS

Les responsables informatiques s'expriment sur la mise en œuvre opérationnelle de leurs projets : conseils, anecdotes pratiques, pièges à éviter…

En savoir plus

6 FORMATIONS

Une gamme de sessions d'une journée destinées à approfondir un sujet et à matérialiser la démarche de préparation d'un projet.

En savoir plus

INTRODUCTION

Contexte technologique, méthodologie et éléments de cadrage

La plupart des applications informatiques nécessitent une gestion des utilisateurs à des fins d'allocation des ressources propres à chacune d'elles (espaces disques, comptes applicatifs, etc.), de sécurité et de droits d'accès, ainsi que de personnalisation des services en fonction des profils et des rôles des individus.

Ainsi, que ce soit pour gérer les utilisateurs d'un réseau local d'entreprise, les prospects ou clients d'un site de commerce électronique, les extranets, les portails collaboratifs ou d'entreprise, les progiciels de gestion intégrés (PGI), les progiciels de gestion de la relation client (CRM), les applications décisionnelles, ou encore les solutions d'authentification forte à l'aide de PKI, il est nécessaire de disposer d'une base d'utilisateurs et d'un service de gestion des comptes applicatifs.
Mais la multitude des applications, des référentiels utilisateurs sous-jacents, et des outils d'administration associés, nuit à la sécurité du système d'information, à l'efficacité des opérations d'administration, ainsi qu'à l'accès rapide aux informations et aux services propres au rôle d'un utilisateur dans l'entreprise.

En effet, le retour d'expérience de ces dernières années a mis en évidence de nouveaux enjeux, qui sont devenus majeurs pour l'entreprise :
• La sécurité dont les menaces ont été favorisées par la prolifération des services en ligne et les réseaux de télécommunications mondiaux

• L'efficacité des opérations dont la complexité augmente considérablement avec le nombre d'utilisateurs et de services Gains de performances liés à un meilleur usage de l'information

• L'accessibilité à l'information gage d'adoption de la multitude de services offerts par l'entreprise, et ceci de façon ciblée par rapport aux attentes de chacun

Pour tous ces aspects, il est apparu durant ces dernières années des technologies, des standards et des outils qui apportent des solutions à l'ensemble des questions posées.

Qu'est ce que la gestion des identités

Lorsqu'on parle de « gestion des identités », on entend par là celle des utilisateurs d'un système d'information. Il ne s'agit donc pas de l'identité d'un individu au sens large, mais de celle nécessaire au fonctionnement des applications informatiques auxquelles il accède. Bien entendu, ces applications sont diverses et concernent aussi bien l'individu en tant qu'employé d'une entreprise, que client d'une autre ou citoyen. Un même individu pourra donc avoir plusieurs identités en fonction du rôle qu'il joue.

Le référentiel des identités

Tout d'abord, il est nécessaire de constituer un référentiel qui va contenir l'ensemble des informations partagées entre différentes applications. Ces informations vont être associées à un individu et vont contenir un ou plusieurs identifiants qui serviront d'index pour y accéder. La constitution de ce référentiel nécessite généralement un annuaire, basé sur la technologie LDAP.
Le référentiel des identités est généralement accompagné d'outils, comme les méta-annuaires, permettant de synchroniser l'ensemble des informations concernant les utilisateurs entre l'annuaire central (ou le référentiel) et celles qui se trouvent éparpillées dans le système d'information de l'entreprise. Ces outils permettent, soit de synchroniser les données avec un référentiel centralisé (par exemple, Microsoft MIIS, Novell Identity Manager, etc.), soit de rediriger en temps réel les requêtes vers la bonne source de données, constituant ainsi une sorte de référentiel virtuel (par exemple, Maxware Virtual Directory, Radiant Logic Virtual Directory Server, etc.). On parle alors d'annuaire ou de méta-annuaire « virtuel ».

La gestion du contenu du référentiel des identités Ce référentiel doit être accompagné d'outils qui vont permettre aux utilisateurs de consulter eux-mêmes les données qui les concernent et de les mettre à jour si nécessaire, en respectant les processus organisationnel de l'entreprise. Ces outils offrent des interfaces de saisie et de consultation des données de l'annuaire, à l'aide de formulaires qu'il est possible de créer et de modifier via des fichiers de paramétrage, voire d'une interface d'administration de l'outil.

Les outils savent généralement prendre en compte les règles de confidentialité de l'annuaire afin de protéger les données personnelles des utilisateurs lors de la consultation et de la saisie, et s'adaptent aux contraintes organisationnelles de l'entreprise, nécessitant l'intervention de plusieurs acteurs ou administrateurs, le cas échéant, pour mettre à jour ces données. Ils offrent, pour cela, des mécanismes

de workflow permettant d'associer chaque étape d'un processus à un ensemble d'acteurs. Par exemple, la mise à jour du mot de passe peut se faire par l'utilisateur lui-même, mais celle du nom de son responsable hiérarchique ou de sa fonction doit être validée par une personne faisant partie des Ressources Humaines.

L'identification et l'authentification électronique

Ce service est l'un des principaux usages de la gestion des identités. En effet, il constitue le premier niveau de sécurité à mettre en place afin de contrôler l'accès aux ressources de l'entreprise dont les applications informatiques.
L'identification permet de reconnaître l'utilisateur à partir d'un identifiant, généralement court et simple à retenir. L'authentification consiste à s'assurer de l'identité de l'utilisateur à l'aide d'un mot de passe, mais aussi à l'aide d'autres moyens plus sécurisés, comme un certificat électronique, une carte à puce ou encore une signature biométrique (empreinte digitale, forme du visage, etc.).

La gestion des mots de passe

La perte d'un mot de passe par un utilisateur peut s'avérer coûteuse pour les administrateurs s'ils gèrent des milliers de personnes, et si le système d'information est constitué de centaines d'applications.
La solution passe par des outils qui d'une part vont permettre de réduire le nombre de mots de passe, voire de les synchroniser automatiquement entre différentes applications, et d'autre part de permettre la réinitialisation du mot de passe par l'utilisateur lui-même et ceci à l'aide d'informations complémentaires qu'il devra fournir pour prouver son identité.

L'allocation et la dés-allocation automatisées de ressources
Pour tout nouvel arrivant dans une entreprise, qu'il soit client ou employé, il sera nécessaire d'activer des comptes dans les différentes applications et services auxquels il aura accès. Par exemple, il sera nécessaire de lui créer un compte de messagerie, un compte sur le serveur de fichiers et d'impression de l'entreprise, lui donner accès au portail documentaire sur l'intranet, etc.
De plus, la création, suppression et modification des comptes doivent être conforme aux processus organisationnels de l'entreprise. En effet, une filiale d'un groupe pourra gérer de façon autonome ses utilisateurs.
Ou encore, la création d'un nouvel employé dans le système de messagerie, doit normalement commencer par la création de celui-ci dans le système des ressources humaines.

De part la multiplicité des applicatifs et la complexité des processus organisationnel, la gestion de comptes applicatifs peut s'avérer fastidieuse dans les entreprises. Pour cela, il est utile de mettre en place des outils facilitant la création, modification et suppression de ces comptes et ceci de façon centralisée. On désigne aussi cette fonction par « e-provisionning ».

La gestion des droits d'accès aux applications

Il s'agit d'un part de décrire les droits d'accès des utilisateurs aux différentes applications de l'entreprise et d'autre part de contrôler l'accès à celles-ci en respectant ces règles.
La description des droits d'accès peut s'avérer complexe, car elle peut dépendre de plusieurs paramètres comme le rôle ou la fonction de l'individu, voire sa localisation géographique (accès de l'intérieur ou de l'extérieur de l'entreprise), le type de réseau qu'il utilise (l'Internet ou l'Intranet), ou encore le groupe de travail auquel il appartient, etc. Par exemple, il ne pourra accéder aux applications de veille concurrentielle que s'il fait partie de la Direction Marketing, ou encore aux applications financières de l'entreprise que s'il fait partie de la Direction Financière. Le contrôle d'accès aux applications doit par la suite être effectué au moment où l'utilisateur demande l'accès à une application ou à un service donné, et ceci quel que soit le canal de communication utilisé (Internet, intranet, PC ou téléphone mobile).

La fédération des identités

Toutefois, dans certaines situations, il sera utopique de centraliser la gestion des identités. Les cas les plus évidents sont relatifs à des partenaires et fournisseurs. Mettre en place un annuaire partagé entre une entreprise, ses partenaires et fournisseurs, est complexe et ne présente pas toujours beaucoup d'intérêt. Cela pose de nombreux problèmes, comme la définition d'un modèle de données commun et d'un identifiant unique, la synchronisation des données de l'annuaire avec les applications existantes, la maintenance et l'évolutivité de la solution pour répondre à de nouveaux besoins, etc.
La solution passe alors par un réseau de systèmes de gestion des identités, gérant chacun un sous-ensemble des données ou des services, et possédant des interfaces d'échanges standards et ouverts. On parle alors de fédération des identités.
Plusieurs technologies et standards permettent aujourd'hui de réaliser des services de fédération des identités. Ceux-ci s'appuient essentiellement sur les technologies issues de l'Internet comme les Web services et XML. Il s'agit de SAML, Liberty Alliance et WS-Federation.

Ces standards offrent les fonctionnalités suivantes :

• Identification et authentification croisée, permettant à un utilisateur d'accéder à un service via une authentification réalisée sur un autre service

• Echange d'attributs, permettant de transmettre d'un service à l'autre un ensemble d'attributs décrivant l'identité de l'utilisateur, comme par exemple son adresse de messagerie, sa langue ou encore son adresse postale ou une adresse de facturation

• Echange de règles d'habilitation, permettant de transmettre d'un service à l'autre une déclaration décrivant les droits de l'utilisateur sur une ou plusieurs ressources. Par exemple, il peut s'agir d'un droit de lecture sur une URL comme ftp://www.domaine.com/dossier

• Fédération de l'identifiant d'un utilisateur, permettant de signaler tout changement d'identifiant à l'ensemble des fournisseurs de services afin d'être en mesure de reconnaître l'utilisateur avec son nouvel identifiant, ainsi que d'associer différentes valeurs à celui-ci en fonction du service auquel il accède

• Gestion des sessions de bout en bout, permettant de déconnecter automatiquement un utilisateur de l'ensemble des sites auxquels il s'est connecté

• Gestion des pseudonymes, permettant de ne pas publier un nom et prénom lors des échanges entre sites afin de conserver l'anonymat à propos de l'utilisateur

Gouvernance des accès et gestion des risques

Les éléments techniques décrits ci-dessus doivent servir un approche plus globale dénommée « gouvernance des accès ».
La gouvernance des accès intègre l'ensemble des aspects technologiques liés à la gestion des identités tels que la gestion des annuaires, des mots de passe, de la sécurité des applications… dans une démarche globale ayant pour objectifs de :
• Définir des processus métier et des stratégies de sécurité
• Mettre en œuvre ces stratégies de sécurité
• Etre capable de prouver que ces stratégies de sécurité sont appliquées tel que défini par le management

Techniquement mis en œuvre par les équipes informatiques, la gestion de la gouvernance des accès bascule vers un processus conjoint mené par les équipes informatiques et les cadres fonctionnels. Il s'agit alors en première étape de définir des rôles métiers compréhensibles par les utilisateurs puis d'établir des processus de certification des droits d'accès par les managers fonctionnels.

Par exemple, un responsable comptable devra définir et valider dans les temps les autorisations d'accès détaillées des membres de son équipe.
L'automatisation peut ensuite être mise en place. Enfin, une traçabilité complète associée aux différents modèles d'habilitation et aux usages est centrale pour une gouvernance complète des accès.

La mise en œuvre d'une politique et de processus de gouvernance des accès associe trois populations au sein de l'entreprise :
• Les équipes IT
• Les managers fonctionnels
• Les cadres en charge du risque, de l'audit et de la conformité

Il s'agit d'un projet d'entreprise pour collecter, rationaliser mettre en place processus dont les sponsors sont la plupart du temps la direction générale ou la direction des ressources humaines..

A propos de ce guide

Depuis la rédaction initiale de ce modèle de cahier des charges, le paysage de la sécurité informatique et de la gestion des accès a connu des évolutions, avec l'émergence de nouvelles menaces, de technologies innovantes et de nouvelles normes de conformité. Afin de garantir la pertinence et la mise à jour de ce guide, nous avons résumé les différents aspects à prendre en compte dans un chapitre 5. Les principaux sujets d'actualisation incluent les évolutions des menaces de sécurité, l'importance croissante de l'authentification multi-facteurs (MFA), les nouvelles normes et réglementations en matière de sécurité, ainsi que l'impact des technologies émergentes telles que l'intelligence artificielle et la blockchain. Nous aborderons également des sujets tels que la gestion des identités et des accès dans le cloud, l'approche Zero Trust, la gestion des accès privilégiés et l'automatisation des processus.

SOMMAIRE

Gouvernance des accès : identités, annuaires, méta-annuaire et gestion des mots de passe

MODELE DE **CAHIER DES CHARGES**

Sélectionnez et pondérez les critères suivants en fonction de votre projet pour orienter vos choix technologiques

1. Politique de gouvernance des accès

1.1. Gestion des rôles

1.1.1. Collecte des données

La solution permet-elle de faire la collecte des modèles d'habilitation à partir de collecteurs automatisés ?
□ Non
□ Oui
Si Oui, quels sont les collecteurs disponibles ?
□ J2EE
□ LDAP
□ Ms Active Directory
□ ODBC
□ SAP
□ Weblogic
□ File system access control list
□ Fichier plat (CSV, Excel…)
□ MDB
□ XML
□ Autre(s) :

La solution permet-elle d'analyser les modèles d'habilitation et de détecter les incohérences ?
□ Non
□ Oui, détailler :

La solution permet-elle de collecter les comptes ouverts dans l'entreprise ?
□ Non
□ Oui, détailler :

1.1.2. Modélisation des modèles d'habilitation

La solution permet-elle de renommer les rôles selon un langage métier ?
□ Non
□ Oui, comment :

La solution de de modélisation est-elle en mesure de s'interfacer avec les solutions de gestion des identités du marché ?
□ Non
□ Oui

Si Oui, lesquelles ?
□ CA
□ Evidian - Bull
□ IBM
□ Ilex
□ Novell D Oracle D SAP
□ Sun
□ Autre(s) :

La solution permet-elle de prendre en compte la séparation des Tâches (SOD - Segragation of duty) dans la définition des rôles ?
□ Non
□ Oui, comment :

La solution permet-elle de définir des exceptions des tâches à l'intérieur de rôles paramétrés ?
□ Non
□ Oui, préciser :

1.1.3. Gestion des processus de certification

La solution est-elle en mesure de mettre en œuvre des processus de certification ?
□ Non
□ Oui, comment :

La solution permet-elle d'envoyer régulièrement aux utilisateurs une revue des utilisateurs sous leur responsabilité, afin de leur faire valider ou invalider les accès de leur équipe ?
□ Non
□ Oui, comment :

Si Oui :
□ Peut-on définir la fréquence :
□ Peut-on définir la forme :
□ Peut-on définir la périmètre :
□ Autre(s) paramètre(s) possible(s) :

La solution est-elle en mesure de mettre en œuvre des processus d'escalade dans le processus de certification des habilitations ?
□ Non
□ Oui, comment :

La solution produit-elle un reporting sur les revues d'habilitation ?
□ Non
□ Oui, détailler les informations et les éléments de paramétrage :

La solution permet-elle de générer des alertes ?
□ Non
□ Oui
Si Oui, sur quels types d'alertes :
□ Temps donné au processus de certification
□ Niveaux d'habilitations
□ Habilitations exceptionnelles
□ Autre(s) :

Lors de l'autorisation d'une personne à accéder à une application, une fonction de workflow est-elle disponible pour informer et faire valider par les personnes habilitées l'autorisation de cet accès ?
□ Non
□ Oui, détailler les paramètres de ce workflow :

La synchronisation des informations est-elle gérée par la solution :
□ De manière événementielle
□ Nécessite des actions manuelles
□ Autre(s) :

1.1.4. Gestion comptes privilégiés sur les systèmes

L'accès aux systèmes hébergeant des applications (compte Root) par les administrateurs du système, les administrateurs des applications… constituent de potentielles failles de sécurité.

A quels niveaux, la solution permet-elle de limiter les restrictions d'accès aux systèmes ?
□ Restreindre au niveau de commandes sur le compte Root
□ Restreindre au niveau de la structure de répertoire
□ Restreindre au niveau des horaires d'accès
□ Restreindre au niveau des types de système
□ Autre(s) :

La solution permet-elle de la traçabilité de tout ce qui est fait sur les comptes systèmes :
□ Enregistrement des touches tapées
□ Enregistrement des commandes lancées
□ Autre(s) :

Sur quels types de systèmes cette gestion des comptes privilégiés est-elle possible ?
□ Unix
□ Linux
□ Windows
□ Autre(s) :

1.2. Contrôle et traçabilité

1.2.1. Fonctions de traçabilité

La solution dispose-t-elle de fonctions de traçabilité ?
□ Non
□ Oui
Si Oui :
□ De manière native ?
□ A travers l'intégration de solution tierce, laquelle ?
□ Autre(s) :

Quels sont les événements couverts par le module de traçabilité ?
□ Authentification
□ Gestion de mot de passe D Workflow d'approbation D Modification de rôle
□ Autre(s) :

La solution est-elle capable de stocker les logs ?
□ Non
□ Oui

La solution est-elle capable d'archiver les logs ?
□ Non
□ Oui

Comment est l'espace de stockage et d'archivage des logs ?
□ Espace de stock propriétaire
□ Espace d'archivage générique, détailler :

La solution permet-elle de « signer » les logs ?
□ Non
□ Oui

La solution est-elle capable de compresser les fichiers de logs ?
□ Non
□ Oui

La solution est-elle capable de faire des recherches :
□ Sur les logs en ligne
□ Sur les logs archivés
□ Sur les logs après ré-importation
□ Autre(s) :

Le format de gestion des logs de la solution, est-il :
□ Propriétaire
□ Ouvert, quel(s) format(s) :

1.2.2. Traçabilité et gestion des événements

Le module de supervision/traçabilité gère-t-il le temps réel ?
□ Non
□ Oui

Quel est le mode de gestion du module de supervision/traçabilité ?
□ Traçabilité passive
□ Gestion d'événement / réactivité sur événement

La solution intègre t-elle une fonction de corrélation et d'analyse automatisées des événements en provenance de gestion des identités et des autres sources de données ?
□ Non
□ Oui, détailler :

Dans le cas d'une gestion réactive sur événement, quel est le périmètre couvert par le déclenchement d'action ?
□ Echec sur identification (par exemple 3 échecs + 1 réussite sur 1 minute peuvent laisser supposer une tentative d'intrusion)
□ Autre(s) :

Le module de supervision/traçabilité peut-il couvrir d'autres applications ?
□ Non
□ Oui

Si Oui, lesquels :
□ Firewall
□ Antivirus
□ Base de données
□ Application métier
□ Autre(s) :

Quelles sont les actions possibles déclenchées par le module de supervision actif ?
□ Envoi de mail
□ Déconnexion d'accès
□ Autre(s) :

1.3. Reporting

La solution dispose-t-elle de modèles de rapports prédéfinis ?
□ Non
□ Oui

Si Oui, lesquels :
□ Taux/niveaux de provisionning
□ Echec à l'authentification
□ Autre(s) :

La solution permet-t-elle de personnaliser des rapports selon les besoins de l'entreprise ?
□ Non
□ Oui

La solution dispose-t-elle de modèles de rapports correspondant aux normes et réglementations gouvernementales suivantes ?
□ SOX
□ Bale II D HIPAA D PCI DSS
□ Autre(s) :

La solution est-elle ouverte à tout type de moteur de reporting ?
□ Non
□ Oui

2. Annuaires

2.1. Support des standards

2.1.1. Standard LDAP

La solution supporte-t-elle le standard LDAP ?
□ Non
□ Oui

Si Oui, quelle est la compatibilité ?
□ LDAP V2 (RFC 1777)
□ LDAP V3 (RFC 2251 à RFC 2256)

2.1.2. Standard DSML

La solution supporte-t-elle le standard DSML ?
□ Non
□ Oui

Si Oui, quelle est la compatibilité ?
□ DSML 1.0
□ DSML 2.0

La solution nécessite-t-elle un outil complémentaire à installer ?
□ Non
□ Oui

Si Oui, quel doit être cet outil ?
□ DSML Services for Windows de Microsoft
□ DSML for eDirectory de Novell
□ Autres :

2.1.3. Standard LDIF

La solution supporte-t-elle le standard LDIF ?
□ Non
□ Oui

Si Oui, comment ?
□ En natif
□ Via un outil complémentaire

2.1.4. Classe Inetorgperson

La solution permet-elle de supporter la classe Inetorgperson (RFC 2798) ?
□ Non
□ Oui

Si Non, quelle est la solution de remplacement proposée ?
□ Classe user
□ Autres :

Si Oui, comment ?
□ En natif
□ En ajoutant une extension (import d'une extension du schéma, passerelle, etc.)

2.1.5. Multilinguisme

La solution supporte-t-elle le multilinguisme (RFC 2296) ?
□ Non
□ Oui

Peut-on associer à un même attribut plusieurs valeurs dans différentes langues (RFC 2296) ?
□ Non
□ Oui

Peut-on effectuer une recherche en tenant compte de la langue ?
□ Non
□ Oui

2.2. Gestion des « referrals »

La solution gère-t-elle des « referrals » vers un serveur LDAP « père » ?
□ Non
□ Oui

Si Oui, comment est gérée l'authentification vers le serveur « père » ?

La solution gère-t-elle des « referrals » vers un ou plusieurs serveurs de sous- branche ?
□ Non
□ Oui

Si Oui, comment est gérée l'authentification vers les serveurs destinataires ?

La solution permet-elle de gérer des renvois de « referrals » en fonction du type de requête ?
□ Non
□ Oui

Si Oui, quels sont les critères possibles ?
□ Ecriture
□ Lecture
□ Suppression
□ Autres :

2.3. Gestion de la sécurité

2.3.1. Standard SSL pour les échanges LDAP

La solution supporte-t-elle le standard SSL pour les échanges LDAP ?
□ Non
□ Oui

Si Oui, quelle est la compatibilité ?
□ LDAPS
□ TLS (StartTLS dans une session LDAP non cryptée)

Peut-on gérer des certificats serveurs ?
□ Non
□ Oui

Peut-on gérer des certificats clients (authentification forte, X509) ?
□ Non
□ Oui

2.3.2. Standard SSL pour les échanges DSML

La solution supporte-t-elle le standard SSL pour les échanges DSML ?
□ Non
□ Oui

Peut-on activer le protocole SSL pour toutes les sessions DSML ?
□ Non
□ Oui

Peut-on activer le protocole SSL pendant une session non chiffrée DSML via StartTLS ?
□ Non
□ Oui

2.3.3. Standard SSL pour les réplications entre différentes instances de l'annuaire

La solution supporte-t-elle le standard SSL pour les réplications entre différentes instances de l'annuaire ?
□ Non
□ Oui

Peut-on activer le protocole SSL pour les échanges entre annuaires répliqués ?
□ Non
□ Oui

2.3.4. Possibilités offertes pour la gestion des ACL

Quels sont les critères de sélection de l'utilisateur authentifié ?
□ Nominatif
□ Appartenance à un groupe
□ Appartenance à un rôle
□ Valeurs données dans plusieurs attributs
□ Contrôle des adresses IP d'où se connecte l'utilisateur
□ Autres :

Quels sont les droits qu'il est possible de contrôler ?
□ Lecture
□ Ecriture

□ Suppression
□ Modification
□ Autres :

Est-il possible d'utiliser des plages de temps pour limiter l'accès à l'annuaire dans les ACL ?
□ Non
□ Oui

Sur quels objets peuvent s'effectuer les contrôles ?
□ Entrée
□ Attribut
□ Classe d'objet
□ Branche de l'arbre
□ Autres :

Quels sont les mécanismes d'import / export offerts pour échanger ou sauvegarder et restaurer les ACL ?
□ Import / Export dans un fichier LDIF
□ Import / Export dans un fichier DSML
□ Autres :

2.3.5. Autres aspects de la sécurité

Peut-on chiffrer un attribut autre que le mot de passe ?
□ Non
□ Oui

Si Oui, quels sont les mécanismes de chiffrement autorisé ?
□ SSHA
□ SHA
□ Autres :

Peut-on désactiver temporairement un utilisateur ou un groupe (pas d'authentification possible) ?
□ Non
□ Oui

Si Oui, quelles sont les possibilités offertes ?
□ Période de désactivation
□ Désactivation d'un utilisateur
□ Désactivation d'un groupe ou d'un rôle
□ Autres :

Quels sont les mécanismes d'authentifications fortes supportés ?
□ Support de SASL
□ PKI et Certificat X509
□ Kerberos
□ Autre(s) :

2.4. Gestion des mots de passe

La solution permet-elle de chiffrer les mots de passe ?
□ Non
□ Oui
Si Oui, quels sont les mécanismes de chiffrement autorisé ?
□ En clair
□ SHA
□ Autres :

La solution gère-t-elle l'historique du mot de passe ?
□ Non
□ Oui

Si Oui, peut-on paramétrer la limite de l'historique (par exemple, 10 derniers mots de passe) ?
□ Non
□ Oui

La solution permet-elle de gérer le changement du mot de passe ?
□ Non
□ Oui

Si Oui, peut-on forcer le changement du mot de passe à la première connexion ?
□ Non
□ Oui

En cas de gestion de mot de passe, peut-on forcer le changement du mot de passe régulièrement ?
□ Non
□ Oui

Si Oui, comment ?
□ En fonction d'une période donnée
□ A l'issue d'une période d'inactivité
□ Autres :

La solution gère-t-elle l'expiration du mot de passe ?
□ Non
□ Oui

Si Oui, peut-on définir une période de validité (ou d'expiration) du mot de passe ?
□ Non
□ Oui

La solution permet-elle de contrôler le contenu du mot de passe ?
□ Non
□ Oui

Si Oui, quels paramètres peut-on forcer ?
□ Le contenu du mot de passe
□ Des lettres et des chiffres obligatoires
□ Autres :

La solution permet-t-elle le blocage d'un compte en cas d'erreur de mot de passe ?
□ Non
□ Oui

Si Oui, peut-on bloquer un compte au delà d'un nombre paramétrable de tentatives (mot de passe erroné) ?
□ Non
□ Oui

Quels sont les critères qu'il est possible de paramétrer ?
□ Le nombre de tentatives
□ Le délai entre deux tentatives
□ Autres :

Peut-on gérer plusieurs stratégies (historique, changement, contenu, blocage, etc.) de mot de passe ?
□ Non
□ Oui

Si Oui, en fonction de quels critères ?
□ Par utilisateur
□ Par groupe d'utilisateurs
□ Par branche de l'arbre
□ Autres :

La solution permet-elle de répliquer des stratégies de mot de passe ?
□ Non
□ Oui

Si Oui, doit-elle le faire entre différents serveurs LDAP ?
□ Non
□ Oui

2.5. Gestion des groupes et des rôles

2.5.1. Support des groupes dynamiques (groupe contenant une requête et non une liste statique de membres)

La solution supporte-t-elle des groupes dynamiques ?
□ Non
□ Oui

L'appel d'une fonction de lecture est-elle nécessaire pour récupérer les membres ?
□ Non
□ Oui

Peut-on exécuter la requête automatiquement au moment de la lecture du groupe ?
□ Non
□ Oui

2.5.2. Support des rôles (constitution d'un groupe à partir d'un attribut utilisateur)

La solution supporte-t-elle des rôles ?
□ Non
□ Oui

Si Oui, sous quelle forme ?
□ Groupe dynamique
□ Groupe dynamique avec mise à jour automatique d'un attribut pour tous les membres d'un même rôle

2.5.3. Gestion de l'intégrité référentielle

La solution permet-elle de gérer l'intégrité référentielle (c'est-à-dire, suppression automatique d'un membre d'un groupe en cas de suppression de l'entrée utilisateur associée) ?
□ Non
□ Oui

Si Oui, quelles sont les possibilités de paramétrage ?
□ Désactivation temporaire de l'intégrité référentielle
□ Définition des attributs assurant l'intégrité référentielle comme member, uniquemember, etc.
□ Autres :

2.6. Réplication d'annuaires

2.6.1. Support de la réplication maître-esclaves

La solution supporte-t-elle la réplication maître-esclaves ?
□ Non
□ Oui

Si Oui, quelles sont les possibilités maximales ou les limites ?
□ Nombre d'esclaves maximum
□ Attributs non répliqués
□ Topologie en cascade avec réplication d'un esclave vers plusieurs autres esclaves
□ Autres :

2.6.2. Support de la réplication multi-maître

La solution supporte-t-elle la réplication multi-maître ?
□ Non
□ Oui

Si Oui, quelles sont les possibilités maximales ou les limites ?
□ Nombre de maîtres maximums
□ Attributs non répliqués entre maîtres
□ Autres :

2.6.3. Support de la réplication partielle de l'annuaire (maître-esclaves et multi-maître)

La solution supporte-t-elle la réplication partielle de l'annuaire ?
□ Non
□ Oui

Si Oui, quelles sont les possibilités offertes ?
□ Réplication d'une partie de l'arbre
□ Réplication d'un sous-ensemble des attributs
□ Autres :

2.6.4. Réplication des attributs techniques

La solution gère-t-elle la réplication des attributs techniques (par exemple, date de mise à jour d'un objet, identifiant utilisé pour la mise à jour, stratégie du mot de passe) ?
□ Non
□ Oui

Si Oui, quelles sont les possibilités et limites ?

2.6.5. Contrôle de la réplication

Peut-on définir les dates et heures de réplication ?
□ Non
□ Oui

Peut-on répliquer au fil de l'eau ?
□ Non
□ Oui

Quels paramètres de sécurité peut-on définir pour l'accès à un annuaire répliqué ?
□ Identification
□ Authentification
□ Chiffrement
□ Autres :

2.6.6. Protocole de réplication

Le protocole utilisé pour répliquer les données entre annuaires s'appuie-t-il sur un standard ?
□ Non, sur un protocole d'échange propriétaire
□ Oui, expliquer de quel standard s'agit-il ? (fichiers LDIF, standard LDUP, etc.)

2.7. Performances et volumétrie

2.7.1. Nombres d'entrées

Quel est le nombre d'entrées maximum supporté ?
□ Moins de 100 000
□ Jusqu'à 500 000

□ Jusqu'à 1 000 000
□ Jusqu'à 5 000 000
□ Jusqu'à 10 000 000
□ Plus de 10 000 000

2.7.2. Temps de réponse en lecture

Combien de requêtes simultanées maximum est-il possible d'effectuer sur une même machine ?

Quel est le temps de réponse moyen d'une requête de lecture sur une machine ?

Est-ce que ce temps de réponse dépend du nombre d'entrées dans l'annuaire ?
□ Non
□ Oui

Quels sont les leviers possibles sur un serveur donné ?
□ Augmentation de la mémoire
□ Suppression des index
□ Répartition de charge sur plusieurs serveurs d'annuaires
□ Autres :

2.7.3. Temps de réponse en écriture

Combien de requêtes simultanées maximum est-il possible d'effectuer sur une même machine ?

Quel est le temps de réponse moyen d'une requête d'écriture sur une machine ?

Est-ce que ce temps de réponse dépend du nombre d'entrées dans l'annuaire ?
□ Non
□ Oui

Quels sont les leviers possibles sur un serveur donné ?
□ Augmentation de la mémoire
□ Suppression des index
□ Répartition de charge sur plusieurs serveurs d'annuaires
□ Autres :

2.7.4. Mécanisme de répartition de charge

Comment sont réalisés les mécanismes de répartition de charge sur plusieurs serveurs répliqués en lecture ?
□ Via un routeur de type Altéon
□ Via un proxy LDAP
□ Autre mécanisme :

Comment sont réalisés les mécanismes de répartition de charge sur plusieurs serveurs répliqués en écriture ?
□ Via un routeur de type Altéon
□ Via un proxy LDAP
□ Autre mécanisme :

2.7.5. Bases de stockage

Peut-on gérer plusieurs bases de stockage ?
□ Non
□ Oui

Si Oui, quels sont les critères de création d'une base ?
□ Par suffixe
□ Par branche
□ Autres :

2.8. Administration et exploitation

2.8.1. Console d'administration

Quel type de console d'administration la solution doit-elle intégrer ?
□ Une console graphique livrée en standard
□ Une console graphique via un produit tiers

2.8.2. Lignes de commande

Quelles sont les possibilités des lignes de commandes livrées avec le produit ?
□ Import d'un fichier LDIF
□ Export d'un fichier LDIF
□ Modification des entrées de l'annuaire
□ Lecture des entrées de l'annuaire
□ Autres :

Dans quels systèmes d'exploitation les lignes de commande pour LDAP sont- elles compatibles ?
□ Windows
□ Linux
□ Unix
□ Autres :

2.8.3. Modification du schéma

Peut-on modifier ou étendre le schéma sans relancer le serveur ?
□ Non
□ Oui

Peut-on supprimer un attribut ou une classe d'objet ?
□ Non
□ Oui

Si Oui, quelles sont les contraintes éventuelles ?
□ Suppression de toutes les valeurs de l'attribut supprimé
□ Suppression de toutes les entrées correspondantes à la classe d'objet supprimée

2.8.4. Gestion du contenu de l'annuaire

Peut-on supprimer une branche avec tout son contenu ?
□ Non
□ Oui

Peut-on déplacer une branche ?
□ Non
□ Oui

Peut-on renommer une branche ?
□ Non
□ Oui

Peut-on modifier des utilisateurs dans l'annuaire ?
□ Non
□ Oui

Peut-on supprimer des utilisateurs dans l'annuaire ?
□ Non
□ Oui

Peut-on créer des utilisateurs dans l'annuaire ?
□ Non
□ Oui

Peut-on modifier des groupes dans l'annuaire ?
□ Non
□ Oui

Peut-on supprimer des groupes dans l'annuaire ?
□ Non
□ Oui

Peut-on créer des groupes dans l'annuaire ?
□ Non
□ Oui

Quels autres types d'entrées peut-on modifier / supprimer / créer dans l'annuaire ?
□ Les organisations
□ Les classes spécifiques
□ Autres :

2.8.5. Gestion des journaux

Quels sont les indicateurs de suivi proposés ?
□ Temps de réponse
□ Nombre de lecture par seconde
□ Autres :

Peut-on tracer toutes les modifications effectuées dans l'annuaire ?
□ Non
□ Oui

Si Oui, quel est le niveau de détail proposé ?
□ Date et heure de la modification
□ DN utilisé pour s'identifier à l'annuaire lors de la modification
□ Adresse IP de l'utilisateur identifié lors de la modification

Quels sont les critères pour archiver et purger les journaux manuellement ou automatiquement ?
□ Nombre d'entrées dans le journal
□ Date de début et de fin
□ Taille en octet du fichier journal
□ Possibilité d'avoir un fichier journal par jour

□ Possibilité d'avoir un nouveau fichier journal à chaque lancement de l'annuaire
□ Autres :

Existe-t-il une interface graphique de lecture des indicateurs (via la console de supervision de l'annuaire par exemple) ?
□ Non
□ Oui

2.8.6. Gestion des index

Quels sont les types d'indexation supportés ?
□ La recherche phonétique «~=»
□ La recherche d'un numéro de téléphone
□ Ignorer certains caractères comme les parenthèses, les espaces et les virgules pour les numéros de téléphone
□ Autres :

Peut-on choisir les attributs à indexer ?
□ Non
□ Oui

Peut-on désactiver l'indexation sur un serveur ?
□ Non
□ Oui

Peut-on régénérer les index à tout moment ?
□ Non
□ Oui

2.8.7. Supervision SNMP de l'annuaire

La solution gère-t-elle la supervision SNMP de l'annuaire ?
□ Non
□ Oui

La solution support-elle le protocole SNMP ?
□ Non
□ Oui
Si Oui, quelles sont les possibilités offertes ?

3. Méta-annuaires

3.1. Référentiel intégré

3.1.1. Utilité d'un référentiel intégré

La solution peut-elle utiliser un référentiel intégré ?
□ Non
□ Oui

Si Oui, de quel type est ce référentiel ?
□ Annuaire LDAP
□ Base de données relationnelle
□ Autres :

3.1.2. Cas d'un annuaire LDAP

Le schéma de l'annuaire doit-il être modifié ?
□ Non
□ Oui

Faut-il une instance d'annuaire spécifique au méta-annuaire ?
□ Non
□ Oui

Si Non, peut-on utiliser une instance existante ?
□ Non
□ Oui

3.1.3. Cas d'une base de données

Quel est l'outil que la solution doit intégrer ?
□ Microsoft SQL Server 7.0 ou SQL Server 2000
□ Oracle8i Database, Oracle9i Database ou Oracle 10g Database
□ Sybase
□ IBM DB2
□ Autres :

3.2. Connecteurs

La solution intègre-t-elle des connecteurs ?
□ Non
□ Oui

Quels sont les connecteurs vers d'autres annuaires supportés ?
□ Active Directory
□ Active Directory Application Mode (ADAM)
□ Active Directory global address list (GAL)
□ Microsoft Exchange Server 5.5
□ Microsoft Exchange Server 2000
□ Lotus Notes release 4.6 ou 5.0
□ Netscape Directory Server 4.1 ou 6.01
□ Novell eDirectory 8.6.2 ou 8.7
□ Novell Netware
□ Sun ONE Directory Server 4.12, 4.13, 5.0, 5.1 ou 5.2
□ Windows NT 4.0
□ NIS
□ OpenLDAP V2
□ Autres:

Quels sont les connecteurs fichiers supportés ?
□ Attribute-value pair text files
□ Delimited text files
□ Fixed-width text files
□ LDAP Data Interchange Format (LDIF)
□ Autres :

Quels sont les connecteurs bases de données supportés ?
□ Microsoft SQL Server 7.0 ou SQL Server 2000
□ Oracle8i Database, Oracle9i Database ou Oracle 10g Database
□ Sybase
□ IBM DB2
□ Informix
□ Autres :

Quels sont les autres connecteurs supportés ?
□ Directory Services Markup Language (DSML) 2.0
□ ERP, préciser lesquels : SAP, PeopleSoft, HR Access, JD Edwards, etc.
□ CRM, préciser lesquels : Oracle, PeopleSoft, Siebel, etc.
□ Autres :

Peut-on développer ses propres connecteurs ?
□ Non
□ Oui
Si Oui, comment ?
□ Via une API
□ A partir d'un connecteur existant
□ Uniquement pour les connecteurs de type fichiers textes
□ Autres :

La solution nécessite-t-elle de recopier toutes les données externes pour chaque connecteur dans le référentiel ?
□ Non
□ Oui

Si Non, dans quel cas ?
□ Pour un annuaire LDAP externe
□ Pour une base de données relationnelle (Oracle, SQL Server, etc.)
□ Autres :

Si Oui, dans quel cas ?
□ Pour un fichier texte (LDIF, DSML, CSV, etc.)
□ Pour un annuaire LDAP
□ Pour une base de données relationnelle (Oracle, SQL Server, etc.)
□ Autres :

La solution permet-elle de détecter des changements dans les sources de données ?
□ Non
□ Oui, à la volée pour certains types de connecteurs (voir plus bas)

Dans le cas de détection des changements à la volée, quelles sont les sources de données supportées ?
□ Active Directory
□ Active Directory Application Mode (ADAM) D Active Directory global address list (GAL) D Microsoft Exchange Server 5.5
□ Microsoft Exchange Server 2000
□ Lotus Notes release 4.6 ou 5.0
□ Netscape Directory Server 4.1 ou 6.01
□ Novell eDirectory 8.6.2 or 8.7
□ Novell Netware
□ Sun ONE Directory Server 4.12, 4.13, 5.0, 5.1 ou 5.2
□ Windows NT 4.0
□ NIS
□ OpenLDAP V2
□ Attribute-value pair text files
□ Delimited text files
□ Fixed-width text files
□ LDAP Data Interchange Format (LDIF)
□ Microsoft SQL Server 7.0 ou SQL Server 2000
□ Oracle8i Database ou Oracle9i Database
□ Sybase
□ IBM DB2
□ ERP, préciser lesquels : SAP, PeopleSoft, HR Access, etc
□ CRM, préciser lesquels : Oracle, PeopleSoft, Siebel, etc
□ Autres :

Peut-on appliquer un filtre à un connecteur afin de ne traiter qu'un sous- ensemble des données lors de la synchronisation ?
□ Non
□ Oui

Si Oui, comment est définit le filtre ?
□ Requête LDAP
□ Requête SQL
□ Autres :

La solution permet-elle de gérer la synchronisation d'attributs chiffrés comme le mot de passe ?
□ Non
□ Oui

Si Oui, comment ?

Est-ce que le méta-annuaire offre des connecteurs spécifiques à la synchronisation des mots de passe ?
□ Non
□ Oui (compléter le chapitre sur la gestion des mots de passe plus loin dans ce guide)

3.3. Transformation

Peut-on traiter les données en entrée et en sortie d'un connecteur ?
□ Non (passer au sous-chapitre suivant)
□ Oui

Quelles sont les possibilités de traitement des données offertes ?
□ Via une interface graphique permettant d'effectuer des opérations simples sur les attributs
□ A l'aide d'un langage de programmation interprété ou compilé (voir plus bas)

Dans le cas d'une interface graphique quels sont les types d'opérations possibles ?
□ Concaténation de chaîne D Opérations arithmétiques D Extraction de chaînes
□ Autres :

Quel langage de programmation est supporté pour le traitement des données ?
□ Perl
□ PHP

□ C
□ C++
□ C#
□ Visual Basic
□ C#.Net
□ Visual Basic.Net
□ VB Script
□ XSLT
□ Java
□ JavaScript
□ Autres :

Dans le cas où un langage de programmation est supporté, est-il possible d'utiliser le debogueur associé (par exemple Visual Studio ou Eclipse) dans l'environnement du méta-annuaire à des fins de test du code ?
□ Non
□ Oui

La solution intègre-t-elle des outils de déploiement automatique du code d'un environnement de test à un environnement de production ?
□ Non
□ Oui

Si Non, faut-il copier les fichiers manuellement ?
□ Non
□ Oui

Faut-il arrêter l'environnement de production ou pas ?
□ Non
□ Oui

Peut-on définir des règles de transformation différentes pour un attribut donné en fonction du sens de la synchronisation (du connecteur vers le référentiel ou vice versa) ?
□ Non
□ Oui

Peut-on définir des règles de transformation génériques, c'est-à-dire commune à plusieurs connecteurs ?
□ Non
□ Oui

3.4. Jointure

La solution intègre-t-elle un moteur de jointure ?
□ Non
□ Oui

Peut-on définir des règles de jointure entre les entrées des connecteurs et celles du référentiel ?
□ Non (passer au sous-chapitre suivant)
□ Oui

Comment sont définies les règles de jointure ?
□ Via une interface graphique permettant d'effectuer des recherches et comparaisons simples sur les attributs
□ A l'aide d'un langage de programmation interprété ou compilé (voir plus bas)

Dans le cas d'une interface graphique quels types d'opérations sont possibles ?
□ Opérations arithmétiques
□ Comparaison de chaînes
□ Autres :

Quel langage de programmation est supporté pour les règles de jointure ?
□ Perl
□ PHP
□ C
□ C++
□ C#
□ Visual Basic
□ C#.Net
□ Visual Basic.Net
□ VB Script
□ XSLT
□ Java
□ JavaScript
□ Autres :

Dans le cas où un langage de programmation est supporté, est-il possible d'utiliser le debogueur associé (par exemple Visual Studio ou Eclipse) dans l'environnement du méta-annuaire à des fins de test du code ?
□ Non
□ Oui

La solution intègre-t-elle des outils de déploiement automatique du code d'un environnement de test à un environnement de production ?
□ Non
□ Oui

Si Non, faut-il copier les fichiers manuellement ?
□ Non
□ Oui

Faut-il arrêter l'environnement de production ou pas ?
□ Non
□ Oui

Peut-on définir des règles de jointure différentes, fonction du sens de la synchronisation (du connecteur vers le référentiel ou vice versa) ?
□ Non
□ Oui

Peut-on définir des règles de jointure génériques, c'est-à-dire commune à plusieurs connecteurs ?
□ Non
□ Oui

Peut-on effectuer la jointure manuellement à l'aide d'une interface d'administration si la règle de jointure renvoie plusieurs entrées ?
□ Non
□ Oui

Peut-on créer des extensions de règles pour résoudre les cas de conflits si la règle de jointure renvoie plusieurs entrées ?
□ Non
□ Oui

Quelles sont gérées les règles de création du DN ?
□ A l'aide d'un langage de programmation
□ A l'aide d'un langage de script

Quelles sont gérées les règles de transformation éventuelles des attributs ?
□ A l'aide d'un langage de programmation
□ A l'aide d'un langage de script

La solution intègre-t-elle un outil d'analyse des jointures ?
□ Non
□ Oui

Peut-on rechercher les entrées non jointes du référentiel ?
□ Non
□ Oui

Peut-on lister les cas de conflits (plusieurs jointures possibles, etc.) ?
□ Non
□ Oui

Peut-on joindre ou disjoindre manuellement une ou plusieurs entrées ?
□ Non
□ Oui

3.5. Provisioning

Peut-on créer, supprimer et modifier des entrées dans les applications via les connecteurs ?
□ Non (passer au sous-chapitre suivant)
□ Oui

Quels sont les connecteurs supportés (parmi ceux donnés plus haut) ?
□ Active Directory
□ Microsoft Exchange 5.5
□ Novell Netware
□ SPML
□ Autres :

Peut-on mettre en place un processus de création, modification ou suppression des comptes applicatif au travers des différents connecteurs (par exemple, création de l'entrée dans l'application de ressources humaines en premier, puis dans Active Directory, puis dans Novell Netware) ?
□ Non
□ Oui

Si Oui, comment est réalisé l'ordonnancement des actions via les connecteurs ?
□ Par configuration graphique à l'aide d'un outil adéquat
□ Par programmation au niveau des règles de jointure et de transformation ?

Existe-t-il une interface homme/machine qui permette à un utilisateur ou à un administrateur de démarrer ou d'activer manuellement une des étapes du processus (workflow) ?
□ Non
□ Oui
Si Oui, comment ?
□ En natif
□ Via un produit tiers, préciser dans ce cas le type d'outil et l'architecture

3.6. Performances et volumétrie

Quel est le nombre maximum d'entrées supporté par le méta-annuaire ?
□ Moins de 100 000
□ Jusqu'à 500 000
□ Jusqu'à 1 000 000
□ Jusqu'à 5 000 000
□ Jusqu'à 10 000 000
□ Plus de 10 000 000

Quel est le nombre maximum d'entrées supporté par connecteur ?
□ Moins de 100 000
□ Jusqu'à 500 000
□ Jusqu'à 1 000 000
□ Jusqu'à 5 000 000
□ Jusqu'à 10 000 000
□ Plus de 10 000 000

Quel est le nombre maximum de connecteurs supporté par machine ?
□ Moins de 5
□ Jusqu'à 10
□ Jusqu'à 20
□ Jusqu'à 50
□ Jusqu'à 100
□ Plus de 100

Temps d'alimentation du référentiel à l'aide d'un méta-annuaire configuré avec plusieurs connecteurs et des règles de jointure entre connecteurs :
□ Donner les performances atteignables en ms sur un seul serveur avec des hypothèses de dimensionnement (par exemple, deux connecteurs de 100 000 entrées chacun avec règles de jointure) :

□ Expliquer les leviers possibles sur un serveur donné (augmentation de la mémoire, séparation des bases pour le référentiel et pour les connecteurs, etc.) :

Temps d'extraction des données du référentiel à l'aide du méta-annuaire vers un des connecteurs :
□ Donner les performances atteignables en ms sur un seul serveur avec des hypothèses de dimensionnement (par exemple, 100 000 entrées à extraire du référentiel et règles de transformation) :
□ Expliquer les leviers possibles sur un serveur donné (augmentation de la mémoire, séparation des bases pour le référentiel et pour les connecteurs, etc.) :

Existe-t-il des mécanismes de répartition de charge du méta-annuaire ?
□ Non
□ Oui

Si Oui, comment répartir la charge sur plusieurs instances du méta-annuaire ?
□ Par Cluster de serveur
□ Autres :

Existe-t-il une fonction de sauvegarde et de restauration de la totalité du méta- annuaire, y compris les règles et les données ?
□ Non
□ Oui

Si Oui, quels sont les temps moyens de sauvegarde (en fonction du volume d'entrées dans le méta-annuaire) (par exemple pour 10 000, puis pour 100 000, puis pour 1 000 000, etc.) ?

3.7. Administration et exploitation

3.7.1. Console d'administration

Quel type de console d'administration la solution intègre-t-elle ?
□ Une console graphique livrée en standard
□ Une console graphique via un produit tiers

3.7.2. Lignes de commande

Quelles sont les possibilités des lignes de commandes livrées avec le produit ?
□ Arrêt du méta-annuaire
□ Démarrage du méta-annuaire
□ Autres :

3.7.3. Règles de transformation, de jointure et connecteurs

Peut-on modifier et étendre les règles de transformation, de jointure et les connecteurs ?
□ Non
□ Oui

Si Oui, est-il nécessaire de relancer le serveur ?
□ Non
□ Oui

3.7.4. Suppression d'une règle ou d'un connecteur

Peut-on purger automatiquement les données du référentiel associé ?
□ Non
□ Oui

Peut-on purger manuellement les données du référentiel associé ?
□ Non
□ Oui

Si Oui, comment lister ces entrées à l'aide d'une requête ?
□ A l'aide de la console d'administration
□ A partir d'un fichier journal

3.7.5. Gestion des journaux

Quels sont les types de journaux proposés ?
□ Journaux d'erreurs de jointure
□ Journaux d'audit
□ Autres :

Peut-on archiver et purger les journaux manuellement ou automatiquement en fonction de critères suivants ?
□ Le nombre d'entrées dans le journal
□ La date de début et de fin
□ Autres :

Existe-t-il une interface graphique de lecture des journaux (via la console de supervision de l'annuaire par exemple) ?
□ Non
□ Oui

Existe-t-il des balises qui permettent de traiter les fichiers journaux à l'aide d'une application informatique (balises XML, import dans une base de données, etc.) ?
□ Non
□ Oui

3.7.6. Supervision SNMP

La solution permet-elle une supervision SNMP du méta-annuaire ?
□ Non
□ Oui

Si Oui, quelles sont les possibilités offertes par le protocole SNMP ?

Peut-on suivre en temps réel les indicateurs de supervision à l'aide de la console ou d'une ligne de commande ?
□ Non
□ Oui

Si Oui, comment ?
□ Via la console
□ Via une ligne de commande

Quels sont les indicateurs de supervision ?
□ Le nombre de jointure en cours de traitement
□ Le nombre de jointure en attente
□ Autres :

Existe-t-il un moyen de générer une alerte sur critères si un connecteur ne répond plus ?
□ Non
□ Oui

Existe-t-il un moyen de générer une alerte sur critères si le méta-annuaire ne répond plus ?
□ Non
□ Oui

Existe-t-il un moyen de générer une alerte sur critères s'il existe un décalage trop important entre un connecteur et le référentiel (plus de 1 000 entrées non synchronisées par exemple) ?
□ Non
□ Oui

Existe-t-il d'autres moyens de générer une alerte sur critères ?
□ Non
□ Oui

Si Oui, lesquels ?

4. Gestion des mots de passe

4.1. Mécanismes de synchronisation des mots de passe

Quel est le mécanisme retenu pour synchroniser les mots de passe ?
□ Mise à jour centralisée à partir de l'outil, et mono-directionnelle (outil de gestion des mots de passe vers les différents connecteurs et systèmes associés)
□ Mise à jour bi-directionnelle à l'aide d'agents intrusifs capables de détecter les changements de mots de passe à la source
□ Autres :

Existe-t-il une API permettant de demander le changement de passe via l'outil à partir d'une application quelconque ?
□ Non
□ Oui

Si Oui, quelle est cette API ?
□ Net
□ Java
□ WMI de Windows
□ Autres :

Peut-on contrôler la stratégie des mots de passe à partir de l'outil ?
□ Non
□ Oui

Peut-on paramétrer le format du mot de passe (longueur, nombre de caractères numériques, etc.) ?
□ Non
□ Oui

Peut-on paramétrer l'historique du mot de passe ?
□ Non
□ Oui

Peut-on paramétrer l'obligation de changer le mot de passe à la première connexion ?
□ Non
□ Oui

Peut-on paramétrer la période d'expiration du mot de passe ?
□ Non
□ Oui

Peut-on définir un mot de passe par défaut en cas de création d'un nouvel utilisateur ?
□ Non
□ Oui

Est-il possible de synchroniser la stratégie des mots de passe avec les applications concernées ?
□ Non
□ Oui

Est-il possible de contrôler le comportement de l'outil en cas d'impossibilité de synchronisation du mot de passe dans une des applications ?
□ Non
□ Oui

Si Oui, peut-on annuler le changement du mot de passe pour toutes les applications ?
□ Non
□ Oui

Si Oui, peut-on continuer le changement du mot de passe pour les autres applications ?
□ Non
□ Oui

Existe-t-il une application Web permettant à un gestionnaire de changer les mots de passe des utilisateurs ?
□ Non
□ Oui

Peut-on modifier l'interface homme/machine (langue, look & feel, etc.) ?
□ Non
□ Oui

Peut-on contrôler la liste des gestionnaires ayant accès à cette application ?
□ Non
□ Oui

Peut-on contrôler la liste des entrées accessibles en fonction du gestionnaire ?
□ Non
□ Oui

Peut-on lister et rechercher les utilisateurs dont il faut modifier le mot de passe ?
□ Non
□ Oui

Peut-on effectuer des changements sur un ensemble d'utilisateurs (par exemple remise à zéro d'un ensemble de mots de passe) ?
□ Non
□ Oui

Peut-on envoyer le nouveau mot de passe à l'utilisateur par email, SMS, ou autre mécanisme ?
□ Non
□ Oui

Existe-t-il une application Web permettant à un utilisateur de réinitialiser son mot de passe ?
□ Non
□ Oui

Peut-on paramétrer les informations qui seront demandées à l'utilisateur avant la réinitialisation du mot de passe (adresse de messagerie, question secrète, etc.) ?
□ Non
□ Oui

Peut-on vérifier l'identité de l'utilisateur par email, SMS, ou autre mécanisme avant l'envoi du nouveau mot de passe ?
□ Non
□ Oui

Peut-on envoyer le nouveau mot de passe par email, SMS, ou autre mécanisme ?
□ Non
□ Oui

Peut-on mettre en place un workflow de validation du changement par un gestionnaire ?
□ Non
□ Oui

Peut-on notifier le changement d'un mot de passe par un utilisateur à un ou plusieurs gestionnaires ?
□ Non
□ Oui

Peut-on demander la saisie d'un nombre affiché dans une image graphique « flou » afin d'éviter l'automatisation du changement par une application ?
□ Non
□ Oui

4.2. Connecteurs

Quels sont les connecteurs de changement de mot de passe supportés ?
□ Active Directory
□ Active Directory Application Mode (ADAM) D Active Directory global address list (GAL) D Microsoft Exchange Server 5.5
□ Microsoft Exchange Server 2000
□ Lotus Notes release 4.6 ou 5.0
□ Netscape Directory Server 4.1 ou 6.01
□ Novell eDirectory 8.6.2 or 8.7
□ Novell Netware
□ Sun ONE Directory Server 4.12, 4.13, 5.0, 5.1 ou 5.2
□ Windows NT 4.0
□ NIS
□ OpenLDAP V2
□ Autres :

Quels sont les connecteurs bases de données supportés ?
□ Microsoft SQL Server 7.0 ou SQL Server 2000
□ Oracle8i Database, Oracle9i Database ou Oracle 10g Database
□ Sybase
□ IBM DB2
□ Autres :

Quels sont les autres connecteurs supportés ?
□ ERP, préciser lesquels : SAP, PeopleSoft, HR Access, etc.
□ CRM, préciser lesquels : Oracle, PeopleSoft, Siebel, etc.
□ Autres :

Est-il possible de développer ses propres connecteurs ?
□ Non
□ Oui

Si Oui, comment ?
□ Via une API
□ Autres :

Dans le cas de détection des changements de mot de passe dans les systèmes sources, quels sont les systèmes supportés ?
□ Active Directory
□ Active Directory Application Mode (ADAM)
□ Active Directory global address list (GAL)
□ Microsoft Exchange Server 5.5
□ Microsoft Exchange Server 2000
□ Lotus Notes release 4.6 ou .0
□ Netscape Directory Server 4.1 ou 6.01
□ Novell eDirectory 8.6.2 or 8.7
□ Novell Netware
□ Sun ONE Directory Server 4.12, 4.13, 5.0, 5.1 ou 5.2
□ Windows NT 4.0
□ NIS
□ OpenLDAP V2
□ Microsoft SQL Server 7.0 ou SQL Server 2000
□ Oracle8i Database ou Oracle9i Database
□ Sybase
□ IBM DB2
□ ERP, préciser lesquels : SAP, PeopleSoft, HR Access, etc.
□ CRM, préciser lesquels : Oracle, PeopleSoft, Siebel, etc.
□ Autres :

4.3. Administration et exploitation

4.3.1. Console d'administration

Quel type de console d'administration la solution intègre-t-elle ?
□ Une console graphique livrée en standard
□ Une console graphique via un produit tiers

4.3.2. Lignes de commande

La solution permet-elle d'intégrer des lignes de commande ?
□ Non
□ Oui
Si Oui, quelles sont les possibilités des lignes de commandes livrées avec le produit ?

4.3.3. Gestion des journaux

Quels sont les types de journaux proposés ?
□ Historiques des demandes de changement de mot de passe
□ Autres :

Peut-on archiver et purger les journaux manuellement ou automatiquement en fonction de critères suivants ?
□ Le nombre d'entrées dans le journal
□ La date de début et de fin
□ Autres :

Existe-t-il une interface graphique de lecture des journaux (via la console de supervision de l'annuaire par exemple) ?
□ Non
□ Oui

Existe-t-il des balises qui permettent de traiter les fichiers journaux à l'aide d'une application informatique (balises XML, import dans une base de données, etc.) ?
□ Non
□ Oui

4.3.4. Supervision SNMP

La solution permet-elle une supervision SNMP du gestionnaire de mot de passe ?
□ Non
□ Oui
Si Oui, quelles sont les possibilités offertes par le protocole SNMP ?

Peut-on suivre en temps réel les indicateurs de supervision à l'aide de la console ou d'une ligne de commande ?
□ Non
□ Oui

Si Oui, comment ?
□ Via la console
□ Via une ligne de commande

Quels sont les indicateurs de supervision ?
□ Le nombre de jointure en cours de traitement
□ Le nombre de jointure en attente
□ Autres :

Existe-t-il un moyen de générer une alerte sur critères si un connecteur ne répond plus ?
□ Non
□ Oui

Existe-t-il un moyen de générer une alerte sur critères si un mot de passe est changé régulièrement ?
□ Non
□ Oui

5. Cloud, Zero Trust, Automatisation et IA : un point sur les dernières avancées

5.1. Évolution des menaces de sécurité

La solution de gestion des accès intègre-t-elle des mesures de sécurité pour faire face aux nouvelles menaces de sécurité informatique ?

……

5.2. Authentification multi-facteurs (MFA) :

La solution propose-t-elle une prise en charge complète de l'authentification multi-facteurs (MFA) ?

□ Non
□ Oui

Quels sont les types de facteurs d'authentification pris en charge et comment assurez-vous leur fiabilité et leur convivialité pour les utilisateurs ?

……

5.3. Normes et réglementations

Comment la solution garantit-elle la conformité avec les normes et réglementations actuelles en matière de sécurité, telles que le RGPD, la directive NIS, etc. ?

.....

La solution offre-t-elle des fonctionnalités spécifiques pour aider les entreprises à respecter ces exigences ?

□ Non
□ Oui

5.4. Gestion des identités et des accès dans le cloud

Comment votre solution prend-elle en charge la gestion des identités et des accès dans des environnements cloud ?

.....

Comment gérez-vous la sécurité des accès aux services cloud et la synchronisation des identités entre les environnements locaux et cloud ?

.....

5.5. Approche Zero Trust

La solution adopte-t-elle les principes de l'approche Zero Trust pour renforcer la sécurité des accès ?

□ Non
□ Oui

Comment assurez-vous la vérification continue de l'identité et l'accès aux ressources en fonction des politiques définies ?

.....

5.6. Gestion des accès privilégiés :

Comment la solution permet-elle la gestion sécurisée des accès privilégiés aux systèmes et aux données sensibles ?

.....

Comment garantissez-vous la traçabilité et la surveillance des activités des utilisateurs disposant d'accès privilégiés ?

.....

5.7. Automatisation des processus

Comment la solution gère-t-elle l'automatisation des processus de gestion des accès ?

.....

Quels processus spécifiques peuvent être automatisés pour améliorer l'efficacité opérationnelle et minimiser les risques d'erreurs ?

.....

5.8. IA et blockchain

Comment votre solution intègre-t-elle les technologies que l'intelligence artificielle et la blockchain pour améliorer la sécurité des accès ?

.....

Quels sont les avantages et les nouvelles fonctionnalités apportées par ces technologies ?

.....

Utiliser les guides

Les guides proposés en téléchargement sont des introductions aux principales fonctionnalités des solutions technologiques. La structure et le contenu de ces guides constituent une excellente base pour la prise en main de ce sujet et pour disposer d'une base solide pour préparer un cahier des charges ou un comparatif.

Ce guide a pour principale vocation de faciliter l'appropriation d'une telle démarche par les acteurs du projet. Il représente le meilleur compromis entre une démarche standardisée et une démarche personnalisée de choix.

Un projet de choix et de mise en oeuvre d'une solution s'appuie sur une démarche d'analyse, de compréhension et de modélisation des besoins. Chaque critère présenté se doit d'être qualifié, personnalisé et soumis à une évaluation comparative, au plus près des spécificités de l'entreprise.

En fonction de ces analyses, il sera possible de sélectionner et pondérer les critères du guide pour bâtir une grille d'évaluation personnalisée dont le remplissage et la lecture conduiront aux choix technologiques.

En résumé, un projet de choix et de mise en oeuvre d'une application de gestion intégrée s'appuie sur une démarche d'analyse, de compréhension et de modélisation des métiers de l'entreprise et de leurs interactions : ce guide a pour principale vocation de faciliter l'appropriation d'une telle démarche.

Notations et classements d'offres

Les guides n'intègrent pas de notation, classement ou jugement de valeur sur les offres.

En matière de projet d'entreprise, tout classement universel est inadapté et faux : une offre est parfois plus adaptée que d'autres au contexte d'un projet ou d'une entreprise. Cette même offre sera peut-être moins adaptée que les autres pour un projet différent. C'est en ce sens que les guides ont été conçus. Sélectionner et pondérer les critères du guide en fonction de chaque projet permet de bâtir une grille d'évaluation personnalisée dont le remplissage et la lecture orienteront les choix technologiques.

Il n'y a donc volontairement aucune note ni classement dans les documents, comme on peut en trouver dans les comparateurs d'appareils numériques, caméscopes, matériels électroménagers...

Reprendre les textes des documents

La société guidescomparatifs.com autorise toute personne physique ou morale, à utiliser et reproduire lesdits documents pour son propre usage.

Nous vous invitons à citer les sources utilisées en faisant mention du nom guidescomparatifs.com.

La société guidescomparatifs.com est titulaire de droits d'auteur sur lesdits documents en application des articles L.111-1 et suivants du Code la Propriété intellectuelle.

La société guidescomparatifs.com se réserve néanmoins la possibilité de poursuivre sur le fondement de la contrefaçon de ses droits d'auteur toute personne physique ou morale utilisant ces documents dans le cadre de son activité à des fins commerciales (facturation de prestations de conseil sur la base des documents, vente de la réalisation d'un cahier des charges reprenant les documents guidescomparatifs.com...).