VISHNU D1.0 - Spécifications techniques des besoins



COL	1 4	0	באב		2
COL	.LA	Юυ	RΑ	IUN	

	TITLE : VISHNU D1.0 - Spécific besoins	cations techniques des		
ACTION	NAME	DATE	SIGNATURE	
WRITTEN BY	Benjamin Isnard, Daouda Traoré, and Eugène Pamba Capo-Chichi	12 janvier 2011		

PEVISIO	N HISTORY	
HE VISIO	IN TIIS TON I	

NUMBER	DATE	DESCRIPTION	NAME
01	07/12/2010	Exemple pour validation du format	B.Isnard
02	13/12/2010	Pre-delivrable	B.Isnard

Table des matières

1		sentation du document	1
	1.1	Objectifs	1
	1.2	Structure du document	
	1.3	Références	1
	1.4	Glossaire	1
2	Sécu	urité du système et des données	2
	2.1	Tableau des Exigences	2
	2.2		4
3	Envi	ironnement matériel et logiciel	5
	3.1	Tableau des Exigences	5
	3.2	Glossaire	7
4	Perf	formances, fiabilité et robustesse	8
	4.1	Tableau des Exigences	8
	42	Glossaire	10

Présentation du document

1.1 Objectifs

Ce document présente les spécifications techniques des besoins pour le système Vishnu. Elles sont basées sur les documents de Cahier des charges du système Vishnu (voir Références) et sur la proposition technique de la société Sysfera. Ces spécifications incluent les contraintes d'implémentation du logiciel. L'objectif principal de ces spécifications est de valider l'adéquation de la solution proposée par rapport aux contraintes de l'environnement d'utilisation.

Ce document pourra également contenir des prévisions sur les évolutions futures du logiciel et préciser quelles fonctions devraient être faciles à ajouter ou supprimer.

1.2 Structure du document

Le document est composé de 3 parties correspondant à des domaines techniques différents :

- Besoins liés à la sécurité du système et des données
- Besoins liés à l'environnement matériel et logiciel
- Besoins en performance, fiabilité et robustesse

Chaque partie contient un tableau des exigences qui fait l'inventaire des tous les besoins techniques concernant le domaine spécifié. Ce tableau est suivi d'un dictionnaire des termes techniques employés afin de les préciser le cas échéant.

1.3 Références

1.4 Glossaire

- UMS ("User Management System") : nom du module Vishnu de gestion des sessions et des utilisateurs
- TMS ("Tasks Management System"): nom du module Vishnu de gestion des tâches
- FMS ("Files Management System"): nom du module Vishnu de gestion des transferts de fichiers
- IMS ("Information Management System"): nom du module Vishnu de gestion des informations

Sécurité du système et des données

2.1 Tableau des Exigences

ID	Name	Text
1	Sessions et authentification	
1.1	Types d'utilisateurs	Les utilisateurs de l'intergiciel réparti VISHNU seront de deux types : utilisateurs ou administrateurs. Les administrateurs sont des utilisateurs avec des droits supplémentaires. L'identification dans le système d'un utilisateur se fera à l'aide d'un login unique et d'un mot de passe qui sera crypté.
1.2	Format des identifiants et mots de passe	Le login et le mot de passe respecteront respectivement les expressions régulières suivantes : ^[A-Za-z0-9_]{LOGIN_MIN_SIZE ,LOGIN_MAX_SIZE}\$ et ^[^s]{PASSWORD_MIN_SIZE ,PASSWORD_MAX_SIZE}\$
1.3	Caractéristique d'une authentification	Une authentification se fait à l'aide d'un login et d'un mot de passe qui doivent être au préalable enregistrés dans la base de données pour vérification. Le login est unique et le mot de passe enregistré est crypté en utilisant la fonction crypt de la librairie libcrypt de Linux. La procédure d'authentification est donc sécurisée en ce sens que le login est unique dans la base de données et que le mot de passe est crypté par un algorithme efficace SHA-512. Avant tout ajout d'un nouvel utilisateur via vishnu dans la base de données le système vérifie que le login n'est pas déjà utilisé.
1.4	Authentification unique	Une fois authentifié dans l'intergiciel, l'utilisateur n'aura plus à s'authentifier pour utiliser les services de l'intergiciel avec son propre compte. Un identifiant de session sera créé par le système et retourné à l'utilisateur. Cet identifiant est ensuite enregistré dans une variable VISHNU_SESSION_ID pour éviter d'avoir à fournir cette information pour chaque requête (dans le cadre du client shell Unix). La complexité de cet identifiant garantit son unicité mais surtout un niveau de sécurité pour une utilisation du système sans authentification systématique.
1.5	Fermeture de session	
1.5.1	Fermeture manuelle de session	L'utilisateur peut fermer manuellement la session dans laquelle il se trouve. Avant la fermeture, le système vérifie la présence de commandes en cours d'exécution dans la session. Si il existe une ou plusieurs commandes en cours d'exécution le système rend impossible la fermeture de session sinon la session est fermée. Cette fermeture est possible en utilisant l'identifiant de session défini dans la variable VISHNU_SESSION_ID.

Louilisateur peut choisrie ritre deux options de fermeture automatique de session soit l'option de fermeture à la déconnexion du terminal, soit l'option de fermeture à la déconnexion du terminal, soit l'option de fermeture après expiration du délai d'inactivité (période sans aueun appel aux services de l'intergiciel). Le choix de enceptive dans la configuration permanente de l'utilisateur et peut également être modifié pour une session donnée. Le choix de fermeture à la déconnexion du terminal n'est possible que dans le cas d'une session de type "shell unix". Dans les deux cas, la présence de commandes en cours avant fermeture de session. Par contre, pour l'option de fermeture après expiration du délai d'inactivité. Il y a une refinit qualitation rend impossible la fermeture de session. Par contre, pour l'option de fermeture de session. Par contre pour l'option de fermeture de session de cours de la conserve de session pour l'option de fermeture de session. Par contre pour de la conserve de session en serve pas fermée avant la fin de l'exécution de toutes les commandes en cours, et elle sera fermée après expiration du délai d'inactivité. 1.6. Reconnection à une session sont terminées avant de fermer la session. Dans le cas où l'un des des sessions sont terminées avant de fermer la session. Dans le cas où l'un session en serve pas fermée avant la fin de l'exécution de toutes les commandes en cours, et elle sera fermée après expiration du délai d'inactivité. 1.7. Accès aux informations sur les session soit de distaint de l'un délai d'inactivité. 1.8. Accès aux informations sur les sessions de de l'un listateur normal, l'affichage des sessions (actives ou fermées) n'est possible que la bent de la conserver ouverte	ID	Name	Text
Soit l'option de fermeture après expiration du délai d'inactivité (période sans aucun appel aux services de l'intergiciel.) Le choix est enregistré dans la configuration permanente de l'utilisateur et peut également être modifié pour une session domée. Le choix de fermeture à la déconnexion du terminair s'est possible que dans le cas d'une session de trep "shell unix". Dans les deux cas, la présence de commandes en cours d'exécution rend impossible la fermeture de session. Par contre, pour l'option de fermeture après expiration du délai d'inactivité. Il y au me éfinitalisation du délai d'inactivité lorsqu'il y a des commandes en cours d'exécution. Le système vérifie que toutes les commandes lancées pendant la session en session. Dans le cas où l'utilisateur s'est déconnecté de son terminal et que la session doit être fermée automatiquement, la session ne sera pas fermée avant la fin de l'exécution de toutes les commandes en cours, et elle sera fermée après expiration du délai d'inactivité. Un utilisateur peut se connecter à une session déjà ouverte sur la même machine eliente en fournissant un identifiant unique de session une session ouverte, le système lui propose de fermer cette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur peut par contre accéder à toutes les informations de sessions (actives ou fermées) n'est possible qui après une authentification à partir du login et du mot de passe de l'utilisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. L'accès à une machine au travers de l'intergiciel Vishnu a son compte Unix sur une machine donnée en supprimant simplement la clef publique aux clefs autorisées sur son compte. L'utilisateur vi administrateur peut par contre accéder à toures les individuels L'accès au compte d'utilisateur vi une machine de varves de l'intergiciel Vishnu à son compte Unix sur une machine donnée en supprimant simplement la clef publi			L'utilisateur peut choisir entre deux options de fermeture automatique
1.5.2 Choix de l'option de fermeture automatique de session Choix de l'option de fermeture automatique de session Choix de l'option de fermeture automatique de session Choix de l'option de fermeture à la déconnexion du terminal n'est possible que dans le cas d'une session de type "shell unix". Dans les deux cas, la présence de commandes en cours d'exécution rend impossible la fermeture de session. Par contre, pour l'option de fermeture après expiration du délai d'inactivité, luy a une réinitalisation du délai d'inactivité lorsqu'il y a des commandes en cours d'exécution. Le système vérifie que toutes les commandes lancées pendant la session sont terminées avant de fermer la session. Dans le cas où l'utilisateur s'est déconnecté de son termine et que les sessions en sera pas fermée avant la fin de l'exécution de toutes les commandes en cours, et elle sera fermée après expiration du délai d'inactivité. 1.6			
1.5.2 Choix de l'option de fermeture automatique de session Choix de l'Option de fermeture automatique de session Choix de l'option de fermeture automatique de session Choix de l'option de fermeture à la déconnexion du terminal n'est possible que dans le cas d'une session de type "shell unix". Dans les deux cas, la présence de commandes en cours d'exécution rend impossible la fermeture de session. Par contre, pour l'option de fermeture après expiration du délai d'inactivité. Il y a une refinitalisation du délai d'inactivité lorsqu'il y a des commandes en cours d'exécution. Le système vérifie que toutes les commandes lancées pendant la session nes treminées avant la fin de l'exécution de toutes les commandes en cours, et elle sera fermée après expiration du délai d'inactivité. Le système vérifie que toutes les commandes lancées pendant la session de session de l'unitativité. Reconnection à une session de type de l'exécution de toutes les commandes en cours, et elle sera fermée après expiration du délai d'inactivité. L'un utilisateur peut se connecter à une session doit de l'exécution de toutes les commendes en cours, et elle sera fermée après expiration du délai d'inactivité. L'un utilisateur peut se connecter à une session doit de l'exécution de toutes les commendes en cours, et elle sera fermée après expiration du délai d'inactivité. L'un utilisateur peut se connecter à une session doit de l'exécution de toutes les connecter à une session de l'exécution de toutes les connecter à une session de l'exécution de toutes les informations de session de l'exécution en diffication d'accès aux machines. L'accès aux machines L'accès aux machine au travers de l'intergiciel Vishnu à son compte unix sur une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. L'accès aux compte de l'utilisateur un système Vish			
1.5.2 Création et modification d'accès au machines 1.8.1 Création d'un accès au compet unix par un utilisateur run au tilisateur peut se compete de la liste des cles au torrisces sur son compte Link; un tilisateur peut se compete de la liste des cles au système des communications et requêtes au système lu fireval un système lu fireval un permetal tile des communications et requêtes au système visinu sont authentification se fera avec le nouveur not terminées au session donnée. Le choix de fermeture à desconnexion donnée. Le choix de fermeture à desconnexion de par terméture de session de type s'hell unix''. Dans les deux cas, la présence de commandes en cours d'exécution du délai d'inactivité. Le système vérifie que toutes les commandes lancées pendant la session sont terminées avant de fermer la session. Dans le cas où l'utilisateur s'est déconnecté de son terminal et que la session douit être fermée automatique au tout être fermée automatique au tout être fermée automatique au tout de la d'inactivité. Un utilisateur peut se connecter à une session déjà ouverte sur la même machine cliente en fournissant un identifiant unique de session au bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. 1.8.1 Création et modification d'accès au machines en cur propriet au bes sessions de tous les utilisateurs. 1.8.2 Création et modification d'accès au machine au travers de l'intergiciel Vishnu s fera à l'aide d'un couple elé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur un un machine donnée en supprimant simplement la celé publique aux eles autorisées sur son compte Unix sur une			
fermeture automatique de session fermeture à la déconnexion du terminal n'est possible que dans le cas d'une session de type "shell unix". Dans les deux cas, la présence de commandes en cours d'exécution rend impossible la fermeture de session. Par contre, pour l'option de fermeture après expiration du délai d'inactivité, il y a une réinitialisation du délai d'inactivité lorsqu'il y a des commandes en cours d'exécution. Le système vérifie que toutes les commandes lancées pendant la session sont terminées avant de fermer la session. Dans cas où l'utilisateur s'est déconnecté de son terminal et que la session doit de l'exécution de toutes les commandes en cours, et elle sersion doit termine automatiquement, la session non cerra pas fermée avant la fin de l'exécution de toutes les commandes en cours, et elle sersion doit de l'exécution de toutes les commandes en cours, et elle sers fermée avant la fin de l'exécution de toutes les commandes en cours, et elle sersion ding que son login et mot de passes. S'il se trouve déjà dans une session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session de toute le sinchine du finactivité. 1.8		Choix de l'ontion de	
session d'une session de type "shell unix". Dans les deux cas, la présence de commandes en cours d'exécution rend impossible la fermeture de session. Par contre, pour l'option de fermeture après expiration du délai d'inactivité, il y a une réinitialisation du délai d'inactivité lorsqu'il y a des commandes en cours d'exécution. Le système vérifie que toutes les commandes pen cours avant fermeture de session sont terminées avant de fermer la session. Dans le cas où l'unitisateur s'est déconnecté de sont terminal et que la session doit être fermée automatiquement, la session no sera pas fermée avant la fin de l'exécution de toutes les commandes en cours, et elle sera fermée après expiration du délai d'inactivité. Un utilisateur peut se connecter à une session dója ouverte sur la même machine cliente en fournissant un identifiant unique de session ainsi que son login et mot de passe. S'il se trouve déjà dans une session ouverte, le système lui propose de fermer cette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur normal, l'affichage des sessions (actives ou fermées) n'est possible qu' après une authentification à partir du login et du mot de passe de l'utilisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de toutes les individuels d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux cléfs attorisées sur son compte Unix. L'accès au compte unix par un utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu de son compte Unix sur une machine donnée en supprimatismplement la clef publique de la liste des cles autorisées sur son compte Unix. L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu, Si c'est le cas, le système	152		
d'une session de type "shell univ". Dans les deux eas, la presence de commandes en cours d'exécution reul impossible la fermeture de session. Par contre, pour l'option de fermeture après expiration du délai d'inactivité lorsqu'il y a des commandes en cours d'exécution. Vérification des commandes en cours d'exécution. Le système vérifie que toutes les commandes lancées pendant la session sont terminées avant de fermet la session. Dans le cas où l'utilisateur s'est déconnecté de son terminal et que la session doit être fermée automatiquement, la session sont terminées avant la fin de l'exécution de toutes les commandes en cours, et elle sera fermée après expiration du délai d'inactivité. Un utilisateur peut se connecter à une session déjà ouverte sur la même machine cliente en fournissant un identifiant unique de session ainsi que son login et mot de passe. S'il se trouve déjà dans une session ouverte, le système lui propose de fermer cette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur peut se connecter à une session de toute les sinformations de sessions de tous les utilisateurs. L'accès aux machines Création et modification d'accès ucompte de l'utilisateur (La udipsin et du mot de passe de l'utilisateur la udipsin et du mot de passe de l'utilisateur la us système vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'accès à une machine au travers de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privé/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur que système vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès au compte de l'utilisateur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur vil sur me machine et aux infor	1.5.2		
Session Par contre, pour l'option de fermeture après expiration du delai d'inactivité lorsqu'il y a des commandes en cours d'exécution. Vérification des commandes en cours d'exécution. L'ayasème vérific que toutes les commandes lancées pendant la session sont terminées avant de fermet la session. Dans le cas où l'utilisateur s'est déconnecté de son terminal et que la session doit être fermée avant autilisateur peut se connecter à une session doit être fermée automatiquement, la session ne sera pas fermée avant la fin de l'exécution de toutes les commandes en cours, et elle sera fermée avers la fin de l'exécution de toutes les commandes en cours, et elle sera fermée avers expiration du délai d'inactivité. Un utilisateur peut se connecter à une session déjà ouverte sur la même machine cliente en fournissant un identifiant unique de session ausin que son login et mot de passe. S'il se trouve déjà dans une session ouverte, le système uni propose de fermer cette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur peut se connecter à une session se conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. L'accès à une machine au travers de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privé/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur us utilisateur les vistems es l'intergiciel Vishnu à son compte. Unix sur une machine donnée en supprimant simplement la clef publique aux clefs autorisées sur son compte. L'accès au compte de l'utilisateur sur une machine dura qiouter la clef publique aux clefs autorisées sur son compte. L'accès au compte de l'utilisateur une machine du sa vistem es vishnu doir refuser la création (ou modification) de l'accès at la machine. L'accès au compte de l'utilisateur sur une machine de aux informations y étant stockée		Session	
délai d'inactivité, il y a une réinitialisation du délai d'inactivité lorsqu'il y a des commandes en cours d'exécution. Vérification des commandes en cours d'exécution. Le système vérifie que toutes les commandes lancées pendant la session sont terminée au toute de la cession. Dans le cas où l'utilisateur s'est déconnecté de son terminal et que la session doit être fermée automatiquement, la session ne sera pas fermée avant la fin de l'exécution de toutes les commandes en cours, et elle sera fermée après expiration du délai d'inactivité. Un utilisateur pett se connecter à une session déjà ouvert se value son login et mot de passe. S'il se trouve déjà dans une session ouverte, le système lui propose de fermer cette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur normal, l'affichage des sessions (actives ou fermées) n'est possible qu' après une authentification à partir du login et du mot de passe de l'utilisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs d'un couple elé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'accès au compte unix par un utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à son compte Unix sur une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. Unix sur une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. Un utilisateur Vishnu in SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu in peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur			
Le système vérifie que toutes les commandes en cours d'exécution.			
Le système vérific que toutes les commandes lancées pendant la session sont terminées avant de fermer la session. Dans le cas où l'utilisateur s' est déconnecté de son terminal et que la session doit être fermée action à une session du delai d'inactivité. Reconnection à une session Un utilisateur peut se connecter à une session déjà dans une session ouverte, le système lui propose de fermer cette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur propose de fermer cette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur l'arbitisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. L'accès au une machine au travers de l'intergiciel Vishnu de gra a l'aide d'un couple clé SSH privée/publique a chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique e al la liste des cles autorisées sur son compte. Unix une machine donnée en supprimant simplement la clef publique e al la liste des cles autorisées sur son compte. L'accès au compte de l'utilisateur, tous les durisies par un autre utilisateur vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur vishnu. Si c'est le cas, le système Vishnu			
1.5.3 Session sont terminées avant de fermer la session. Dans le cas où l'utilisateur s'est déconnecté de son terminal et que la session doit être fermée automatiquement, la session ne sera pas fermée avant la fin de l'exécution de toutes les commandes en cours, et elle sera fermée avant la fin de l'exécution de toutes les commandes en cours, et elle sera fermée avant la fin de l'exécution de toutes les commandes en cours, et elle sera fermée avant la fin de l'exécution de toutes les connecter à une session déjà ouverte sur la même machine cliente en fournissant un identifiant unique de session ainsi que son login et mot de passe. S'il se trouve déjà dans une session ouverte, le système lui propose de fermer cette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur normal, l'affichage des sessions (actives ou fermées) n'est possible qu'après une authentification à paritr du login et du mot de passe de l'utilisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. L'accès à une machine au travers de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à son compte Unix sur une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur des sessions contrateur l'escès à la machine. Un utilisateur peut superimer l'escès à la machine. Les communication			
1.5.3 Verification des commandes en cours avant fermeture de session Reconnection à une session Reconnection à			
1.5.3 en cours avant fermeture de session en cours avant fermeture de l'exécution de toutes les commandes en cours, et elle sera fermée après expiration du délai d'inactivité. In utilisateur pus e connecter à une session déjà ouverte sur la même machine cliente en fournissant un identifiant unique de session ainsi que son login et mot de passe. S'il se trouve déjà dans une session ou verte, le système lui propose de fermer cette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur normal, l'affichage des sessions (actives ou fermées) n'est possible qu'après une authentification à partir du login et du mot de passe de l'utilisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. L'accès à une machine au travers de l'intergiciel Vishnu a fera à l'aide d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu dovra ajouter la clef publique aux clefs autorisées sur son compte Unix sur une machine donnée en suppriment simplement la clef publique aux clefs autorisées sur son compte. En compte de l'utilisateur sur une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. L'accès au compte de l'utilisateur, tous les droits d'accès système seront respecté. Un utilisateur Vishnu ne peut enregistrer un compte de l'utilisateur, tous les droits d'accès système seront respecté. Un utilisateur peut modifier son mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Changement de mot de passe. Communications à tra		Vérification des commandes	
remee automatiquement, la session in sera pas fermee avant la fin de l'exécution de toutes les communications et apas fermee avant la fin de l'exécution de toutes les communications et au passe expiration du délai d'inactivité. Un utilisateur peut se connecter à une session déjà ouverte sur la même machine cliente en fournissant un identifiant unique de session ainsi que son login et mot de passe. S'il se trouve déjà dans une session ouverte, le système lui propose de fermer cette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur normal, l'affichage des sessions (actives ou fermés) n'est possible qu' après une authentification à partir du login et du mot de passe de l'utilisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. L'accès à une machine au travers de l'intergiciel Vishnu se fera à l'aide d'un couple cél SSH privéc/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à son compte Unix sur une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte d'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utili	1.5.3		
Reconnection à une session Respect des autoriset une utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à son compte Unix sur une machine donnée en supprimant simplement la clef publique aux clefs autorisées sur son compte. L'accès auc ompte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès L'accès auc ompte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès sur son compte. L'accès auc ompte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès sur son compte. L'accès auc ompte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès sur son compte. L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès au terregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà uti			
Reconnection à une session Ciente en fournissant un identifiant unique de session ainsi que son login et mot de passe. S'il se trouve déjà dans une session ouverte, le système lui propose de fermer cette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur normal, l'affichage des sessions (actives ou fermées) n'est possible qu'après une authentification à partir du login et du mot de passe de l'utilisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. L'accès à une machine au travers de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à conompte unix par un utilisateur une utilisateur une utilisateur une utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à conompte unix par un utilisateur une utilisateur une utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à conompte unix par un utilisateur une une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est p			
Reconnection à une session machine cliente en fournissant un identifiant unique de session ainsi que son login et mot de passe. S'il se trouve déjà dans une session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur normal, l'affichage des sessions (actives ou fermées) n'est possible qu'après une authentification à partir du login et du mot de passe de l'utilisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. L'accès à une machine au travers de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). Révocation d'un accès au compte unix par un utilisateur L'accès à une machine au travers de l'intergiciel Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à son compte Unix sur une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe es ractif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe es actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe est actif immédiatement c'est-à-dire q			
Reconnection à une session que son login et mot de passe. S'il se trouve déjà dans une session ouverte, le système lui propose de fermer cette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Accès aux informations sur les sessions Pour un utilisateur normal, l'affichage des sessions (actives ou fermées) n'est possible qu' après une authentification à partir du login et du mot de passe de l'utilisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. L'accès à une machine au travers de l'intergiciel Vishnu se fera à l'aide d'un couple elé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à son compte Unix sur une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte Unix sur une machine et aux informations y étant stockées se faisant via SSH avec le compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur put modifier son mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Communications Les requêtes au système vishnu sont authentificées mais non cryptées. Système un firewall permettant les communications on figurées pour traverser un firewall permettant les communications			
ouverte, le système lui propose de fermer cette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur normal, l'affichage des sessions (actives ou fermées) n'est possible qu'après une authentification à partir du login et du mot de passe de l'utilisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. L'accès à une machine au travers de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à son compte Unix sur une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. 2 Sécurité des communications Données des requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications			
conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. 1.7 Accès aux informations sur les sessions 1.8 Accès aux machines 1.8.1 Création et modification d'accès 1.8.2 Révocation d'un accès au compte unix par un utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. 1.8.3 Respect des autorisations d'accès 1.8.4 Utilisation de comptes individuels 1.8.4 Utilisation de comptes individuels 1.8.5 Changement de mot de passe 1.8.6 Changement de mot de passe 2. Sécurité des communications 2. Communications 2. Communications 2. Communications à travers un firewall 2. Communications a firewall	1.6	Reconnection à une session	
Maximum d'inactivité.			
Accès aux informations sur les sessions les sessions Accès aux informations sur les sessions les sessions Accès aux machines 1.8.1 Accès aux machines Création et modification d'un cocès au compte unix par un utilisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. L'accès à une machine au travers de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. Révocation d'un accès au compte unix par un unitisateur un utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à son compte Unix sur une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. 2 Sécurité des communications Données des requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications			
1.8.1 Accès aux informations sur les sessions 1.8 Accès aux machines 1.8.1 Création et modification d'accès 1.8.2 Révocation d'un accès au compte unix par un utilisateur 1.8.3 Respect des autorisations d'accès 1.8.4 Utilisation de comptes individuels 1.8.5 Changement de mot de passe 1.8.6 Changement de mot de passe 2. Sécurité des communications 2. Données des requêtes au système 2. Communications à travers un freewall 2. Communications à travers un freewall permettant les communications on représed in fire wall permettant les communications on representations of travers un freewall permettant les communications on representations of tarces un firewall permettant les communications on formations a travers une freewall passe of the formations of tarces au système vishnu sont authentification à partir du login et du mot de passe ole 1 utilisateur. Un administrateur peut par contre accéder à toutes les informations de l'utilisateurs. Un administrateur peut par contre accéder à toutes les informations de vous les droits des passe birofrantions a une machine au travers de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur pur supprimer l'accès au travers de l'intergiciel Vishnu à clef publique aux clefs autorisées sur son compte Unix. 1.8.1 L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à son compte Unix sur une machine donnée en supprimant simplement a clef publique aux clefs autorisées sur son compte. 1.8.2 L'accès au compte de l'utilisateur sur une machine donnée en supprimant simplement a clef publique de l'utilisateur vishnu a SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. 1.8.4 Utilisation de comptes individuels une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. 1.9 Changement de mot de passe est actif i			
les sessions let du mot de passe de l'utilisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. L'accès à une machine au travers de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. Révocation d'un accès au compte unix par un utilisateur Respect des autorisations d'accès Respect des autorisations d'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Communications Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications		A code our informations our	
accéder à toutes les informations de sessions de tous les utilisateurs. 1.8	1.7		
1.8.1 Accès aux machines 1.8.1 Création et modification d'accès au compte de l'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. 1.8.2 Révocation d'un accès au compte unix par un utilisateur 1.8.3 Respect des autorisations d'accès 1.8.4 Utilisation de comptes individuels 1.8.4 Utilisation de comptes individuels 1.8.5 Changement de mot de passe 2.6 Sécurité des communications 2.7 Sécurité des communications 2.8 Sécurité des communications 2.9 Communications à travers un firewall 2.0 Communications à travers un firewall 2.1 Communications à travers un firewall 2.2 Communications à travers un firewall 2.3 Accès aux machine au travers de l'intergiciel Vishnu de van l'accès au travers de l'intergiciel Vishnu à clef publique aux clefs autorisées sur son compte Unix. 1.8 L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à clef publique aux clefs autorisées sur son compte Unix. 1.8 L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à clef publique aux clefs autorisées sur son compte Unix. 1.8 L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à clef publique aux clefs autorisées sur son compte Unix. 1.8 L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à clef publique de la liste des cles autorisées sur son compte Unix. 1.8 L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à clef publique de la liste des cles autorisées sur son compte Unix. 1.8 L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à clef publique de la liste des cles autorisées sur son compte Unix. 1.8 L'accès au compte de l'utilisateur sur une machine de aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur sur une machine de aux information s' étant s		les sessions	
L'accès à une machine au travers de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. Révocation d'un accès au compte unix par un utilisateur 1.8.2 Respect des autorisations d'accès Respect des autorisations d'accès Utilisation de comptes individuels 1.8.4 Utilisation de comptes individuels Changement de mot de passe Sécurité des communications Données des requêtes au système 2.2 Communications à travers un firewall L'accès à une machine au travers de l'intergiciel Vishnu de chaque couple (machine, utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe est actif immédiatement c'est-à-dire que toute nouveal mot de passe est actif immédiatement c'est-à-dire que toute nouveal mot de passe est actif immédiatement c'est-à-dire que toute nouveal authentification se fera avec le nouveau mot de passe. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications	1.8	Accès aux machines	acceder a toutes les informations de sessions de tous les utilisateurs.
1.8.1 Création et modification d'an couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. 1.8.2 Révocation d'un accès au compte unix par un utilisateur la clef publique de la liste des cles autorisées sur son compte. 1.8.3 Respect des autorisations d'accès 1.8.4 Utilisation de comptes individuels 1.8.4 Utilisation de comptes individuels 1.8.5 Changement de mot de passe 1.8.6 Changement de mot de passe 2. Sécurité des communications 2. Sécurité des communications a système 2. Communications à travers un firewall 2. Communications à travers un firewall 2. Communications à travers un firewall 2. Communications a travers un comple Chix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. 2. Communications à travers un firewall permettant les communications	110	Troop duri macmies	L'accès à une machine au travers de l'intergiciel Vishnu se fera à l'aide
d'accès (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. Révocation d'un accès au compte unix par un utilisateur Respect des autorisations d'accès Respect des autorisations d'accès Utilisateur bur vishnu ne peut enregistrer un compte Unix sur une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Sécurité des communications Communications à travers un firewall Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications		Création et modification	
clef publique aux clefs autorisées sur son compte Unix. Révocation d'un accès au compte unix par un utilisateur Respect des autorisations d'accès Utilisation de comptes individuels 1.8.4 Utilisation de comptes individuels Changement de mot de passe Sécurité des communications Données des requêtes au système Communications à travers un firewall Communications à travers un firewall Communications à travers un firewall L'utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à son compte Unix sur une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. L'utilisateur vishru sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Les requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications	1.8.1		
Révocation d'un accès au compte unix par un utilisateur 1.8.2 Respect des autorisations d'accès 1.8.4 1.8.4 1.8.4 Respect des autorisations d'accès Changement de mot de passe Changement de mot de passe Communications Données des requêtes au système Communications Communications à travers Utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à son compte Unix sur une machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe est actif immédiatement c'est-à-dire que toute nouveal mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. 2.1 Communications Les requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications			
1.8.2 compte unix par un utilisateur Respect des autorisations d'accès 1.8.3 Respect des autorisations d'accès Utilisation de comptes individuels 1.8.4 Utilisation de comptes individuels Changement de mot de passe Changement de mot de passe Données des requêtes au système 2.1 Données des requêtes au système Communications à travers un firewall L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Les requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications		Révocation d'un accès au	
1.8.3 Respect des autorisations d'accès 1.8.4 Utilisation de comptes individuels Changement de mot de passe Sécurité des communications Données des requêtes au système 2.2 Utilisateur L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. 2 Sécurité des communications Les requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications	1.8.2	compte unix par un	
Respect des autorisations d'accès Respect des autorisations d'accès L'accès au compte de l'utilisateur sur une machine et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Sécurité des communications Données des requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications			1 1
d'accès d'accès d'accès les droits d'accès système seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Sécurité des communications Données des requêtes au système Les requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications		Donate de la contraction de la	
Utilisation de comptes individuels Utilisation de comptes individuels Utilisation de comptes individuels Utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Sécurité des communications Données des requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications	1.8.3	_	y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous
1.8.4 Utilisation de comptes individuels machine donnée que si ce compte n'est pas déjà utilisé par un autre utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Sécurité des communications Données des requêtes au système vishnu sont authentifiées mais non cryptées. Les requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications		d acces	les droits d'accès système seront respectés.
1.9 Changement de mot de passe Changement de mot de passe Sécurité des communications Données des requêtes au système Communications à travers un firewall Cindividuels utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Les requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications			Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une
1.9 Changement de mot de passe Changement de mot de passe Sécurité des communications Données des requêtes au système Communications à travers un firewall Les communications Un utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Les requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications	101	Utilisation de comptes	
Un utilisateur peut modifier son mot de passe lorsqu'il a déjà ouvert une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Sécurité des communications Données des requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications	1.0.4	individuels	utilisateur Vishnu. Si c'est le cas, le système Vishnu doit refuser la
Changement de mot de passe une session. Le nouveau mot de passe est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Sécurité des communications Données des requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications			
passe c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Sécurité des communications Données des requêtes au système vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications			
2 Sécurité des communications 2.1 Données des requêtes au système Communications à travers un firewall Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications	1 9	Changement de mot de	
2 Sécurité des communications 2.1 Données des requêtes au système Les requêtes au système vishnu sont authentifiées mais non cryptées. 2.2 Communications à travers un firewall 2.3 Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications	1.7	passe	
2.1 Données des requêtes au système Les requêtes au système vishnu sont authentifiées mais non cryptées. Communications à travers un firewall Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications			mot de passe.
2.1 Données des requêtes au système vishnu sont authentifiées mais non cryptées. Communications à travers un firewall Communications à travers configurées pour traverser un firewall permettant les communications	2		
système Communications à travers un firewall Les requétes au système Visiniu sont authentinées mais non cryptees. Les communications entre machines du système Visiniu pourront être configurées pour traverser un firewall permettant les communications			
2.2 Communications à travers un firewall Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications	2.1	_	Les requêtes au système vishnu sont authentifiées mais non cryptées.
2.2 Communications a travers configurées pour traverser un firewall permettant les communications		système	
2.2 configurees pour traverser un firewall permettant les communications	2.2	Communications à travers	· · · · · · · · · · · · · · · · · · ·
cryptées.	2.2		
			cryptees.

ID	Name	Text
2.3	Fichiers des utilisateurs	Les fichiers des utilisateurs sont transférés en utilisant le cryptage SSH avec les clefs de l'utilisateur. Pour qu'un transfert puisse avoir lieu entre deux machines l'utilisateur doit avoir configuré ses clefs SSH (indépendamment de Vishnu) pour permettre une communication entre ces deux machines.
2.4	Informations stockées par le système	Le système Vishnu stockera toutes les informations relatives aux utilisateurs, aux tâches, transferts de fichiers, mesures de performance et trace des requêtes dans une base de données PostgreSQL sans être cryptées. L'accès du système Vishnu à la base de données sera authentifié par login/mot de passe dont l'envoi au travers de la connexion sera réalisé après hachage MD5. Les communications entre le système Vishnu et la base de données pourront être cryptées si nécessaires par le protocole SSL en configurant le système Vishnu et la base de données.
3	Sécurité des fonctions administrateurs	
3.1	Configuration de l'option par défaut de fin de session	Un administrateur peut définir quelle est l'option par défaut pour la fermeture automatique d'une session utilisateur : soit terminaison en cas de déconnexion de l'utilisateur du client, soit terminaison après expiration du délai d'inactivité
3.2	Utilisation d'un compte tiers	Un administrateur de l'intergiciel pourra ouvrir une session VISHNU avec le compte d'un utilisateur n'étant pas administrateur lui-même.

2.2 Glossaire

- Firewall (ou pare-feu en français) : est un matériel ou un logiciel qui impose une politique de sécurité pour protéger un réseau en constituant une barrière (un filtre) avec d'autres réseaux.
- MD5: est un acronyme de Message Digest 5. C'est une fonction de hachage cryptographique.
- SHA-512 : SHA-512 est un acronyme de Secure Hash Algorithm avec une empreinte de 512 bits. C'est une fonction de hachage cryptographique dérivée de SHA-1.
- SSH : à la fois programme exécutable et protocole de communication sécurisé utilisant un échange de clés de chiffrement en début de connexion.

Environnement matériel et logiciel

3.1 Tableau des Exigences

ID	Name	Text
1.	Plateformes supportées	
1.1	Machines clientes	
1.1.1	Système d'exploitation	Debian Linux v5 (Lenny) ou ultérieure
1.1.2	Architecture matérielle	Intel x86
1.1.3	Nombre et vitesse des processeurs	Monoprocesseur ou multiprocesseur, 2GHz minimum
1.1.4	Mémoire vive	Minimum 1Go
1.1.5	Espace disque	Minimum 1Go disponible
1.1.6	Logiciels requis	SysFera DS, OmniORB, SSH (client/serveur), RSync
1.1.7	Variables d'environnement	La clé RSA ou DSA du serveur SSH (chemin complet sur la clé publique) afin d'identifier le client
1.1.8	Interface réseau	Adresse IP dynamique et nom DNS dynamique
1.2	Serveurs de calcul ou de stockage	
1.2.1	Système d'exploitation	Debian Linux v5 (Lenny) ou ultérieure
1.2.2	Architecture matérielle	Intel x86 ou IBM BlueGene/P® (PPC 32-bits)
1.2.3	Nombre et vitesse des processeurs	Monoprocesseur ou multiprocesseur, 2GHz minimum
1.2.4	Mémoire vive	Minimum 1Go
1.2.5	Espace disque	Minimum 10 Go disponible
1.2.6	Logiciels de gestion de jobs batch supportés	- Torque - IBM LoadLeveler
1.2.7	Logiciels requis	SysFera DS, OmniORB, SSH (client/serveur), RSync, Client database (Oracle ou PostGreSQL)
1.2.8	Ports pour tunnel(s) SSH	1 port réseau disponible pour un tunnel SSH si serveur placé derrière un firewall
1.2.9	Interface réseau	Adresse IP et nom DNS statiques
1.3	Serveurs dédiés VISHNU	
1.3.1	Nombre de serveurs	Au minimum 2 serveurs dédiés. Un ratio de 1 serveur supplémentaire pour 5 serveurs de calcul ou stockage est conseillé.
1.3.2	Plateforme	
1.3.2.1	Système d'exploitation	Debian Linux v5 (Lenny) ou ultérieure
1.3.2.2	Architecture matérielle	Intel x86
1.3.2.3	Nombre et vitesse des processeurs	Monoprocesseur ou multiprocesseur, 2GHz minimum
1.3.2.4	Mémoire vive	Minimum 2 Go

ID	Name	Text
1.3.2.5	Espace disque	Minimum 10 Go disponibles
1.3.2.6	Ports pour tunnel(s) SSH	N ports réseau disponibles pour un/des tunnel(s) SSH où N est le nombre de serveurs de calcul ou de stockage placés derrière un firewall.
1.3.2.7	Interface réseau	Adresse IP et nom DNS statiques
1.4	Serveur Web (pour API Web Services)	
1.4.1	Plateforme	
1.4.1.1	Système d'exploitation	Debian Linux v5 (Lenny) ou ultérieure
1.4.1.2	Architecture matérielle	Intel x86
1.4.1.3	Nombre et vitesse des processeurs	Monoprocesseur ou multiprocesseur, 2GHz minimum
1.4.1.4	Mémoire vive	Minimum 2Go
1.4.1.5	Espace disque	Minimum 500 Go (espace nécessaire au stockage de fichiers temporaires)
1.4.1.6	Interface réseau	Adresse IP et nom DNS statiques
1.4.2	Standard de publication des services web	WSDL 1.1
1.4.3	Machine virtuelle Java	Java SDK v1.6.0 ou ultérieure
1.4.4	Serveur web d'applications	JBoss AS 5.1.0 ou ultérieure
1.4.5	Module Web Services	Module JBossWS version Stack CXF Server 3.3.1.GA ou ultérieure
1.4.6	Autres logiciels requis	SysFera DS, OmniORB, SSH (client/serveur), RSync
1.5	Serveur de Base de données	
1.5.1	Plateforme	
1.5.1.1	Système d'exploitation	Debian Linux v5 (Lenny) ou ultérieure
1.5.1.2	Architecture matérielle	Intel x86
1.5.1.3	Mémoire vive	Minimum 2Go
1.5.1.4	Nombre et vitesse des processeurs	Monoprocesseur ou multiprocesseur, 2GHz minimum
1.5.1.5	Espace disque	Minimum 500 Go
1.5.1.6	Ports pour tunnel(s) SSH	N ports réseau disponibles pour un/des tunnel(s) SSH où N est le nombre de serveurs de calcul ou de stockage placés derrière un firewall.
1.5.1.7	Interface réseau	Adresse IP et nom DNS statiques
1.5.2	Bases de donnée supportées	L'une des deux database suivantes doit être installée : - PostGreSQL version 8.0 ou ultérieure - Oracle Database 11g (v11.1.0.6 minimum)
1.5.3	Réplication de la base de donnée	Afin de garantir un temps de réponse maximum aux requêtes des machines de la plateforme Vishnu, la base de donnée sera éventuellement répliquée selon une architecture maître-esclave (écriture sur un seul serveur, lecture sur plusieurs serveurs).
1.6	Infrastructure réseau	
1.6.1	Connexion entre serveurs (calcul/stockage/VISHNU) et serveur de base de données	
1.6.1.1	Débit	Minimum 100Mb/s
1.6.1.2	Temps de réponse	Maximum 100ms
1.6.1.3	Protocoles autorisés	TCP SSH (port 22) minimum
1.6.2	Connexion entre clients (ou serveur web) et serveurs	
1.621	(calcul/stockage/VISHNU)	Marin 10MI
1.6.2.1	Débit	Minimum 10Mb/s
1.6.2.2	Temps de réponse	Maximum 200ms
1.6.2.3	Protocoles autorisés	TCP SSH (port 22) minimum

ID	Name	Text
2.	Versions des logiciels requis	
2.1	SSH	serveur ssh et client ssh - version minimum TBD
2.2	CORBA	OmniORB v4.1.4 minimum
2.3	Librairie BOOST C++	v1.35 minimum
2.4	Librairies des Batch schedulers	Torque API / LoadLeveler API
2.5	Logiciels de transferts de fichiers	RSync v3.0 ou ultérieure
2.6	SysFera-DS	Une version de SysFera-DS supérieure ou égale à 2.6 et strictement inférieure à la version 3.0 doit être disponible
2.7	Modules SysFera-DS	Le module LogService de SysFera-DS devra faire partie de l'installation de SysFera-DS.
2.8	Client database	- Oracle Database Client 11g (v11.1.0.6 minimum) - PostgreSQL client v8.0
3.	Outils de compilation	
3.1	CMake	CMake v2.6 minimum
3.2	GCC	GCC v3.4.3 minimum

3.2 Glossaire

- TODO

Performances, fiabilité et robustesse

4.1 Tableau des Exigences

ID	Name	Text
1	Fiabilité	
1.1	Réponse aux requêtes	Toute requête lancée à travers le système Vishnu conduit à une réponse. Cette réponse peut être soit le résultat prévu, soit un message d'erreur. Pour chaque message d'erreur, le système vishnu associe un code d'erreur (type entier) correspondant. Un code égal à zero correspondra à un résultat correct. Les interfaces de programmation de Vishnu fourniront un mécanisme d'exceptions permettant à l'utilisateur de traiter séparément les erreurs selon leur cause.
1.2	Enregistrement des requêtes	le cas d'une requête soumise via l'API Web Services, la machine cliente sera le serveur web lui-même.
1.3	Reproductibilité des requêtes	Le système Vishnu peut ré-executer une ou plusieurs requêtes à partir des traces enregistrées. Pour chaque requête, les paramètres de la requête seront les mêmes que lors de la soumission initiale à l'exception de l'utilisateur et de la machine cliente qui proviendront de la session courante (remarque : un administrateur peut ouvrir une session en tant qu'un autre utilisateur).
1.4	Erreurs dues à l'infrastructure	Lorsqu'une machine de l'infrastructure est arrêtée ou injoignable le système répond aux requêtes des utilisateurs concernant cette machine avec un message d'erreur indiquant que la machine n'est pas disponible.
1.5	Erreurs d'utilisation	Une requête lancée avec des paramètres incorrects sera rejetée par le système Vishnu, et pour chaque paramère incorrect, le système Vishnu indiquera le motif du rejet. Le système Vishnu indiquera à l'utilisateur l'utilisation correcte de la requête avec les bons paramètres.

ID	Name	Text
1.6	Erreurs dues à l'intergiciel	Lorsqu'un processus serveur fournissant un service de l'intergiciel Vishnu crashe pendant l'exécution de ce service le système Vishnu informe l'utilisateur de l'arrêt de ce service par un message d'erreur ou une exception. Dans le cas d'un appel de service asynchrone, après que la requête utilisateur a été lancée, un arrêt du service ne sera pas signalé à l'utilisateur. Si le service est redémarré avant une requête d'interrogation de l'utilisateur alors l'utilisateur recevra des informations sur l'état de ses requêtes sans être informé de l'arrêt temporaire du service.
1.7	Erreurs dues aux droits d'accès	L'accès à certaines informations nécessite des permissions en lecture ou écriture. Si un utilisateur n'a pas les droits nécessaires pour accéder à ces informations, le système Vishnu l'en informera par un message indiquant la nature de la permission manquante et l'objet concerné.
2.1	Capacité Nombre de requêtes simultanées	Le système pourra supporter au minimum 100 requêtes simultanées.
2.2	Nombre d'utilisateurs	Le système pourra supporter au minimum 1000 utilisateurs enregistrés.
2.3	Nombre de machines serveur	Le système pourra supporter au minimum 10 machines serveurs (supercalculateurs ou frontales de cluster)
2.4	Nombre de machines clientes	Le système pourra supporter au minimum 1000 machines clientes (postes scientifiques)
3	Performance	
3.1	Latence	En fonctionnement normal (ressources des machines non saturées), avec l'interface d'utilisation en ligne de commande, la latence sera inférieure ou égale à celle obtenue par une commande ssh ayant le même effet en termes de soumission de job ou transfert de fichiers.
3.2	Consommation de ressources	
3.2.1	Consommation mémoire moyenne des processus VISHNU	La consommation moyenne des processus VISHNU ne devra pas dépasser 500Mb de mémoire virtuelle
3.2.2	Consommation CPU moyenne des processus VISHNU	La consommation CPU des processus VISHNU ne devra pas dépasser 10% lorsque le système n'est pas soumis à des requêtes utilisateur (la consommation étant essentiellement dûe aux processus de supervision)
3.2.3	Consommation ponctuelle pour l'exécution d'une requête utilisateur	L'utilisation de Vishnu pour exécuter des requêtes sur un gestionnaire de jobs (soumission de job ou interrogation) ne devra pas consommer en moyenne davantage de ressources sur le serveur que l'utilisation d'un client en ligne de commande (client "lourd" du gestionnaire de jobs).
4	Robustesse	
4.1	Absence de plantage intempestif	Les processus du système ne doivent pas s'interrompre en fonctionnement "de croisière" (c'est-à-dire hors de toute défaillance logicielle ou matérielle du système hôte).
4.2	Résistance aux défaillances	Le système doit rester disponible en cas de défaillance de l'infrastructure n'affectant pas la connection de l'utilisateur aux point(s) d'entrée du système. Plusieurs points d'entrée pourront être configurés mais le nombre de processus lancés par le système sur les machines sera alors augmenté.
4.3	Délestage	Le délestage permettra à un administrateur de réduire de manière immédiate la charge générée par l'intergiciel sur une machine de l'infrastructure. Deux niveaux de délestage seront possible.
4.3.1	Délestage "soft"	Au niveau "soft", le délestage interrompra les activités en cours sur la machine concernée (activités contrôlées par le système Vishnu uniquement). Ces activités pourront être relancées par le système lors de la commande de fin de délestage executée par l'administrateur.

ID	Name	Text
		Au niveau "hard", le délestage interrompra tous les processus de
		l'intergiciel sur la machine concernée sans effectuer d'actions
4.3.2	Délestage "hard"	éventuellement nécessaires à leur redémarrage. Le redémarrage de
		Vishnu sur la machine utilisera la même procédure qu'un démarrage "à
		froid" standard.

4.2 Glossaire

- TODO