VISHNU D1.0 - Spécifications techniques des besoins



COLLABORATO	RS
--------------------	----

	TITLE : VISHNU D1.0 - Spécifi besoins	cations techni <mark>ques de</mark> s		
ACTION	NAME	DATE	SIGNATURE	
WRITTEN BY	Benjamin Isnard, Daouda Traoré, and Eugène Pamba Capo-Chichi	14 décembre 2010		

REVISION HISTORY	
------------------	--

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	Prés	sentation du document	1
	1.1	Objectifs	1
	1.2	Structure du document	1
	1.3	Références	1
	1.4	Glossaire	1
2	Séci	urité du système et des données	2
	2.1	Tableau des Exigences	2
	2.2	Glossaire	4
3	Perf	Formances, fiabilité et robustesse	5
	3.1	Tableau des Exigences	5
	3.2	Glossaire	6
4	Env	ironnement matériel et logiciel	7
5	Inst	allation et maintenance	8

Présentation du document

1.1 Objectifs

Ce document présente les spécifications techniques des besoins pour le système Vishnu. Ces spécifications décrivent les caractéristiques techniques du système à réaliser du point de vue des utilisateurs d'une part et des administrateurs du système d'autre part. 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 également les contraintes d'implémentation du logiciel. L'objectif principal de ces spécifications est de valider l'adéquation de la solution proposée par rapport aux besoins des utilisateurs du système d'information et de ses administrateurs d'une part, et aux contraintes de l'environnement d'utilisation d'autre part.

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

Ces spécifications techniques des besoins sont un prérequis pour les spécifications générales dans le processus de développement suivi pour le projet Vishnu.

1.2 Structure du document

Le document est composé de 4 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
- Besoins pour l'installation et la maintenance du système

Chaque partie contient un tableau des exigences qui fait <u>l'inventaire</u> 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 une base de données Postgresql version 8.4 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 possbile en utilisant l'identifiant de session défini dans la variable VISHNU_SESSION_ID.	

Louissateur peut choisrie reture deux options de fermeture automatique de session so sit l'option de fermeture à la décomexión du terminal, soi l'option de fermeture après expiration du délai d'inactivité (période sans aucun appel aux services de l'intergiciel). Le choix est emegistré dans la configuration permanente de l'utilisateur et peut également être modifié pour une session donnée. Le choix de fermeture à la déconnexión 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 à de session. Par contre, pour l'option de fermeture après expiration du délai d'inactivité, il y a une réfinitulatisation de délai d'inactivité lorsqu'il y a des commandes en cours d'exécution. Le système vérific que toutes les commandes en cours avant fermeture de session. Par contre, estific que toutes les commandes en cours avant fermeture de session sont terminées avant de fermet au session. Dans le cas où l'utilisateur s'est déconnecté de son terminal et que la session dei tre-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. 1.6 Reconnection à une session Reconnection à une session une session déja ouverte sur la mème machine cliente en forunissant un identifiant unique de session ainsi que son login et mot de passe. S'il se trouve déjà duns une session avant les sessions sur les sessions sur les sessions et mot de passe. S'il se trouve déjà duss une session avant les sessions les des sessions (actives ou fermées) n'est possible qu'a près une authentification à partir du login et du mot de passe. D'utilisateur un identifiant unique de session ainsi que son login et mot de passe. S'il se trouve déjà durs une session de d'un couple de session son factives ou fermées pur de des sessions (actives ou mernées) n'est possible que au bette des consentes des suitorisées sur son compte. 1.8.1 Accès aux informations s	ID	Name	Text
Soit l'option de fermeture après expiration du delài 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 domnée. Le choix de fermeture à la déconnexion du terminal n'est possible que dans le cas d'une session de trype "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 delai d'inactivité, il y a une reinitialisation du delai d'inactivité lorsqu'il y a des commandes en cours d'exécution. Le système vérifie que toutes les commandes lancées pendant la session ne session. Dans le cas où l'utilisateur s'est déconnecté de son terminal et que les session de l'utilisateur s'est déconnecté de son terminal et que les session de l'exécution de toutes les commandes en cours, et elle sera fermée après expiration du delai d'inactivité. Un utilisateur peut se connecter à une session déjà ouverte sur la même machine cliente en fournissant un identifiant unique de session air 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 décomexion automatique au bout du temps maximum d'inactivité. Pour un utilisateur peut se connecter à une sessions (actives ou fermées) n'est possible qu'après une authentification à partir du logie et du mot de passe de l'utilisateur. Un administrateur peut par contre accéder à toures 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 vi salver le compte de l'utilisateur, un administrateur peut par de private publique aux clefs autorisées sur son compte. L'accès à une machine au travers de l'intergiciel Vishnu à son compte Unix sur une machine de une			L'utilisateur peut choisir entre deux options de fermeture automatique
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, ll y a une réinitalisation du délai d'inactivité lorsqu'il y a des commandes en cours d'exécution. Le sysème 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 terminet de value les ession au session 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. 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 ette session ou bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. 1.8.1 Accès aux machines 1.8.2 Création et modification d'accès au compte unix par un utilisateur la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. 2. Création et modification d'un accès au compte unix par un utilisateur la conserve de l'intergiciel Vishnu se fera à l'aide d'un couple clé SSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur sex de l'intergiciel Vishnu a son compte Unix sur une machine et aux informations d'accès au compte de l'unitilisateur sur une machine et aux informations d'accès au compte de l'unitilisateur vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix sur une machine et aux informations d'accès au compte d			
1.5.2 Choix de l'option de fermeture automatique de session Choix de l'option de fermeture automatique de session 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 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 reintitulisation 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 d'exécution. Le système vérifie que toutes les commandes lancées pendant la session de session de l'utilisateur s'est déconnecté de son terminal et que la session dout terminées 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 Reconnection à une session de treut peut se connecter à une session doit 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 sur termine de que la session son de l'exécution de toutes les connecter à une session doit de l'exécution de toutes les connecter à une session de ja ouverte sur la même machine cliente en fournissant un identifiant unique de session ain que son loigne et mot de passes. S'il se trouve déjà dans une session ouverte, le système lui propose de fermer cette session on bien de la conserver ouverte avec une déconnexion automatique au bout du temps maximum d'inactivité. 1.8 Accès aux machines 1.8.1 Création et modification d'accès aux machines. L'accès à une machine au travers de l'intergiciel Vishnu à dermé d'un couple cel sSH privée/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur du système Vishnu devra ajouter la clef publique aux elcis autorisées sur son compte Unix sur une machi			
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 run utilisateur run utilisateur run utilisateur run utilisateur run de modification d'accès au compet unix par un utilisateur run de face de compet a compet unix par un utilisateur run de face a compet unix par un utilisateur run de face a compet unix par un utilisateur run de face a compet unix par un utilisateur run de face a compet unix par un utilisateur pour supprimer l'accès au compet unix par un utilisateur pour supprimer l'accès au compet unix par un utilisateur pour supprimer l'accès au compet unix par un utilisateur pour supprimer l'accès au compet unix par un utilisateur pour supprimer l'accès au compet unix par un utilisateur pour pour pour pour pour pour pour po			
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 le cas où l'utilisateur s'est déconnecté de son terminal et que la session du felai d'inactivité. Un utilisateur peut se connecter à une session de ja ouverte sur la même machine cliente en fournissant un identifiant unique de session au verte, le système lui propose de fermer cette session ouverte, le système lui propose de fermer cette session dui delai d'inactivité. 1.8.1 1.8.1 1.8.2 1.8.3 1.8.4 1.8.4 1.8.4 1.8.4 1.8.4 1		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 Reconnection à une session Accès aux informations sur les sessions Reconnection à une session Reconnection à une session Le système lui propose de fermer cette session un bien de la conserver ouvret 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 informations de session du delai 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 mo de passe de l'utilisateur. Un administrateur peut par contre accéde à toutes les informations de sessions de toute les uniformations de sessions de toute les uniformations de sessions de toute les informations de session de l'utilisateur du neu de la liste des cles autorisées sur son compte. L'accès au compte unit par un un autilisateur vishau contre le d'utilisateur sur une machin	152		
d une session de type 'shell unix'. Dans les deux as, la presence de commandes en cours d'exécution reul impossible la fermeture de 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. 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 de fermet le sera 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 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. Pour un utilisateur peut peut peut 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 privérpublique 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 de l'utilisateur sur une machine de aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès ucompte de l'utilisateur une machine de taux 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 de taux informations y étant stockées se faisant via SSH avec le compte de l'utilisat	1.5.2		
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 fermet la session. Dans le cas où l'utilisateurs 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 cliente en fournissant un identifiant unique de session anisi que son login et mot de passe. E'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 deitout du login et du mot de passe de l'utilisateur. In administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. Révocation d'un accès au compte de l'utilisateur un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. Révocation d'un accès au compte de l'utilisateur un utilisateur l'utilisateur un utilisateur l'utilisateur un un machine donnée en supprimant simplement la clef publique aux clefs autorisées sur son compte. L'accès au compte de l'utilisateur sur une machine donnée en supprimant simplement la clef publique du la liste des cles autorisées sur son compte. L'accès au compte de l'utilisateur un en machine donnée en supprimant simplement la clef publique de la liste des cles autorisées sur son compte. L'accès au compte de l'utilisateur 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 donnée en supprimant simplement la clef		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 terminées avant de fermer la session. Dans le cas où l'utilisateur s'est déconnecté de son terminal et que la session doit être fernée 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 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 fer du mot de passe de l'utilisateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs en d'une 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'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. 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, les système vishnu doit refuser la création (ou modification) de l'accès à la machine. Un utilisateur vishnu. Si c'est le ca			
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 au delai d'inactivité. Reconnection à une session Le système lu 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 pour se 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 accèder à toutes les informations de sessions de tous les utilisateurs. Révocation d'un accès au compte unix par un utilisateur 1.8.2 Révocation d'un accès au compte unix par un utilisateur 1.8.3 Respect des autorisations d'accès Respect des autorisations d'accès 1.8.4 Utilisation de comptes individuels Changement de mot de passe 1.8.5 L'utilisation de comptes individuels Changement de mot de passe Sécurité des communications Données des requêtes au système Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications on firewall permetant les communications on monte fire configurées pour traverser un firewall permetant les communications on monte fire configurées pour traverser un firewall permetant les communications on monte fire configurées pour traverser un firewall permetant les communications on monte fire configurées pour traverser un firewall permetant les communications on travers un firewall permetant les communications on munications on traverser un firewall permetant les communication			
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 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 parit du login et du mot de passe e 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 privéc/publique spécifique à chaque couple (machine, utilisateur). L'utilisateur but système Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'accès au 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 et aux informations y étant stockées se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès vystème seront respectés. Un utilisateur Vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'ext pas déjà utilisé par un autre utilisateur vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte n'ext pas déjà utilisé par un au			
1.5.3 Verification des commandes en cours avant fermeture de session 1.5.3 Provinciation de scommandes en cours avant 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. 1.6 Reconnection à une session 1.7 Accès aux informations sur les sessions 1.8 Accès aux informations sur les sessions 1.8 Accès aux machines 1.8.1 Création et modification d'accès en compte unix par un utilisateur 1.8.2 Révocation d'un accès au compte unix par un utilisateur 1.8.3 Respect des autorisations d'accès 1.8.4 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. 1.8.4 Utilisation de comptes individuels 1.8.5 Changement de mot de passe 2 Changement de mot de passe. 2 Communications 1.8.6 Communications 2.7 Communications à travers 2.8 Communications à travers 2.9 Communications à travers 2.0 Communications à travers 2.1 Communications à travers 2.2 Communications à travers 2.3 Communications à travers 2.4 Communications à travers 2.5 Communications à travers 2.6 Communications à travers 2.7 Communications à travers 2.8 Communications à travers 2.9 Communications à travers 2.0 Le scenario du délai d'inactivité. 2.1 Un utilisateur puut su connecte ta unidentification se fera avec la mession déjà dans une session déjà duris de session ainsi que son login et mot de passe lo unidentivité. 2.8 Pour un utilisateur pour suprave avec une déconnexion automatique au bout du temps maximum d'inactivité. 2.9 Pour un utilisateur pour suprimer l'accès au travers de l'intergiciel Vishnu à del d'un couple clé SSH privée/publique aux clefs autorisées sur son compte Unix. 2.0 L'utilisateur puut modifier son mot de passe est actif immédiatement c'est-à-dire que t			
1.5.3 en cours avant fermeture de session 1.6 Reconnection à une session 1.6 Reconnection à une session 1.7 Accès aux informations sur les sessions 1.8 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 2.7 Changement de mot de passe 2.8 Sécurité des communications à travers un firewall 2.9 Communications à travers 1.0 Configurées pour traverse un prievall 1.10 Changement de mot de passe 2.0 Communications à travers 1.10 Configurées pour traverse du système Vishnu pourront être configurées pour travers du système Vishnu pourront être configurées pour traverse un firevall permettant les communications		Vérification des commandes	
remee automatiquement, la session ne sera pas fermee avant la fine of exceution de toutes les communications et alle 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 acce avec une déconnexion automatique au bout du temps maximum d'inactivité. Pour 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 a ser a 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 à ucompte 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 pas déjà utilisé par un autre utilisateur vishnu ne peut enregistrer un compte Unix sur une machine donnée que si ce compte	1.5.3		
Reconnection à une session Respect des autoriset Respect des autorisations d'accès Respect des autorisations d'accès se faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès sus faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès sus faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès sus faisant via SSH avec le compte de l'utilisateur, tous les droits d'accès sus 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 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 communications entre machines du système Vishnu pourront être configurées pour traverser un			
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 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. Utilisation de comptes individuels Utilisateur 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 pour sudifier son mot de passe or la 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 sont de passe est actif immédiatement c'est-à-dire que toute nouveau mot de passe est actif immédiatement c'est-à-dire que toute n			
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 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 elé SSH privée/publique spécifique à chaque couple (machine, utilisateur). Révocation d'un accès au compte unix par un utilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu à 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 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 de l'utilisateur, tou les droits d'accès système seront respectés. 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 compturiations entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications			
1.6 Reconnection à 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. 1.7 Accès aux informations sur les sessions 1.8 Accès aux machines 1.8.1 Création et modification d'accès 1.8.1 Révocation d'un accès au compte unix par un utilisateur 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 de l'utilisateur sur une machine et un tavers de l'intergiciel Vishnu à son compte unix par un utilisateur 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 sur une machine et aux informations y étant stockées se faisant via SSH avec le compte Units sur une machine et aux informations y étant stockées se faisant via SSH avec le compte Units sur une machine et aux informations y étant stockées se faisant via SSH avec le compte Units sur une machine et aux informations y étant stockées se faisant via SSH avec le compte Units sur une machine et aux informations y étant stockées se faisant via SSH avec le compte Units 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. 1.9 Changement de mot de passe. 2 Sécurité des communications 2 Sécurité des communications 2 Les requêtes au système vishnu sont authentificées mais non cryptées. Système un firewall permettant les communications on 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. 1.7 Accès aux informations sur les sessions les sessions 1.8 Accès aux machines 1.8.1 Création et modification d'un accès au compte unix par un utilisateur 1.8.2 Création 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 e 1.8.6 Changement de mot de passe 2 Sécurité des communications Données des requêtes au système 2.2 Communications à travers une firewall 1.8.7 Accès aux machines 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 el rosqu'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 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 autorisées sur son compte Unix. 1.8.3 Respect des autorisations d'accès 1.8.4 Utilisation de comptes individuels 1.8.5 Utilisation de comptes individuels 1.8.6 Changement de mot de passe 1.8.7 Changement de mot de passe 2 Sécurité des communications 2.1 Données des requêtes au système 2.2 Communications à travers une faccion d'incevall 2.2 Communications à travers une faccion que report accompunications on the firewall 2.2 Communications à travers 2.2 Communications à travers 1.8.8 Accès aux informations sur les des unitsiateur. Un administrateur peut par contre accéder à toutes les informations de sessions de tous les utilisateurs. 2.2 Communications a travers 2.3 Accès aux machines 2.4 Communications à travers 2.5 Communications à travers 2.6 Communications a travers 2.7 Communications à travers 2.7 Communications a travers 2.8 Communications a travers 2.9 Communications a travers 2.0 Communications a travers 2.1 Communications a travers 2.2 Communications a travers 2.3 Communications a travers 2.4 Communications à travers 2.5 Communications à travers 2.6 Communications a travers 2.7 Communications a travers 2.8 Communications a travers 2.9 Communications a travers 2.0 Communications a travers 2.1 Communications a travers 2.2 Communications a travers 2.3 Communications a travers 2.4 Communications a travers 2.5 Communications a travers 2.6 Communications a travers 2.7 Communications a travers 2.8 Communications a travers 2.9 Communications a travers 2.0 Communications a travers 2.1 Communications a travers 2.2 Communications a travers 2.3 Communications a travers 2.4 Communications a travers 2.5 Communications a travers 2.7 Communications a travers 2.8 Communications a travers 2.9	1.6	Reconnection à une session	
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. 1.8.1			
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. 1.8.1 Création et modification d'un coès au compte unix par un d'accès 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. 1.8.2 Révocation d'un accès au compte unix par un unitisateur L'atilisateur pour supprimer l'accès au travers de l'intergiciel Vishnu son compte Unix unitisateur la clef publique aux clefs autorisées sur son compte Unix. 1.8.3 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. 1.8.4 Utilisation de comptes individuels Utilisateur Vishnu ne peut erregistrer 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 al machine. 1.8.4 Utilisateur pour unix sur une machine de passe le requires la création (ou modification) de l'accès in amachine. 1.8.4 Utilisateur put 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 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 2. Sécurité des communications 2. Sécurité des communications 2. Communications à travers un freewall 2. Communications aux chies passe de l'utilisateur. Un administrateur peut par contre accéder à toutes les informations de tous les informations accéder à toutes les informations aucéder à toutes les informations aucéder à toutes les informations 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.			
les sessions 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 est actif immédiatement c'est-à-dire que toute nouvelle authentification se fera avec le nouveau mot de passe. Changement de 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		A coès aux informations sur	
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 d'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 Sécurité des communications 2 Sécurité des communications 2 Sécurité des communications 2 Sécurité des communications 2 Communications à travers un firewall 2.2 Communications à travers un firewall 2.3 Communications à travers un firewall 2 Communications à travers un firewall		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 à chaque couple (machine, utilisateur la clef publique spécifique à chaque couple (machine, utilisateur la visitisateur sur une machine de l'intergiciel Vishnu à son compte Unix. L'accès au travers de l'intergiciel Vishnu devra ajouter la clef publique aux clefs autorisées sur son compte Unix. L'accès au travers de l'intergiciel Vishnu à chaque couple (machine, utilisateur pur supprimer l'accès au travers de l'intergiciel Vishnu à chaque couple (machine, utilisateur pur supprimer l'accès au travers de l'intergiciel Vishnu à son compte Unix. L'accès au travers de l'intergiciel Vishnu à chef publique aux clefs autorisées au travers de l'intergiciel Vishnu à son compte Unix. L'accès au travers de l'intergiciel Vishnu à son compte Unix. L'accès au compte de l'utilisateur sur une machine en suppriment au tilisateur sur une machine en suppriment simplement aux on compte Unix sur une machine de nox es passe est actif intergiciel Vishnu à son compte Unix sur une machine de l'accès au travers une machine en suppriment au travers de l'intergiciel vishnu à son compte de l'utilisateur sur une machine en suppriment sur pur une machine en sur priment sur pur une m	1.8	Accès aux machines	acceder a toutes les informations de sessions de tous les utilisateurs.
1.8.1 Création et modification d'accès 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 la clef publique de la liste des cles autorisées sur son compte. 1.8.3 Respect des autorisations d'accès 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. 1.8.4 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. 1.9 Changement de mot de passe Changement de mot de passe Changement de mot de passe Sécurité des communications 2.1 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	reces dux macinies	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 Un utilisateur 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 pricevall 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 vishus 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	1.8.1		
Révocation d'un accès au compte unix par un utilisateur 1.8.2 Respect des autorisations d'accès 1.8.3 Respect des autorisations d'accès 1.8.4 Utilisation de comptes individuels 1.8.4 Changement de mot de passe Communications Données des requêtes au système Communications Communications à travers 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. 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 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		Révocation d'un accès au	
1.8.3 Respect des autorisations d'accès 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 2.1 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. 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 vishnu sont authentifiées mais non cryptées. Les communications entre machines du système Vishnu pourront être configurées pour traverser un firewall permettant les communications		Description to describe	
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. 2 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 individuels 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 Les communications entre machines du 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	1.6.4		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	1 9		
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		
2.1 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			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 requetes au système Vishnu sont authentmees mais non cryptees. Les communications entre machines du système Vishnu 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	Sécurité de le configuration du système	
3.1.1	Consultation et modification de la configuration UMS	Un administrateur peut consulter et modifier l'ensemble de le configuration des utilisateurs.
3.1.2	Sauvegarde et restauration de la configuration UMS	L'ensemble de la configuration des utilisateurs peut être sauvegardée dans un fichier et restaurée. La nouvelle configuration vient remplacer la configuration existante. La restauration a lieu sans redémarrage de l'intergiciel.
3.1.3	Prise en compte des modifications	La prise en compte des modifications de la configuration est immédiate sans redémarrage de l'intergiciel
3.2	Configuration du délai max. d'inactivité	Un administrateur peut définir la valeur maximum du délai d'inactivité pris en compte pour la déconnexion automatique.
3.3	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
3.4	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

SSH : à la fois programme exécutable et protocole de communication sécurisé utilisant un échange de clés de chiffrement en début de connexion.

Performances, fiabilité et robustesse

3.1 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.
1.2	Enregistrement des requêtes	de la requête. Dans 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.
1.6	Erreurs dues à l'intergiciel	Lorsqu'un processus de l'intergiciel Vishnu crashe pendant l'exécution d'un service le système Vishnu informera l'utilisateur de l'arrêt de ce 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	Capacité	
2.1	Nombre de requêtes simultanées	Le système pourra supporter au minimum 100 requêtes simultanées.

ID	Name	Text
2.2	Nombre d'utilisateurs	Le système pourra supporter au minimum 1000 utilisateurs enregistrés.
2.3	Nombre de machines	Le système pourra supporter au minimum 10 machines serveurs
	serveur	(supercalculateurs ou frontales de cluster)
2.4	Nombre de machines	Le système pourra supporter au minimum 1000 machines clientes
2 .4	clientes	(postes scientifiques)
3	Performance	
		En fonctionnement normal (ressources des machines non saturées),
3.1	Latence	avec l'interface d'utilisation en ligne de commande, la latence sera
3.1	Latence	inférieure ou égale à celle obtenue par une commande ssh ayant le
		même effet en termes de soumission de job ou transfert de fichiers.
		La charge sur les machines serveur (hors serveur de base de données)
		dûe aux processus du système Vishnu n'augmentera pas de manière
3.2	Consommation de	significative (<10% d'augmentation) la charge générée par des
3.2	ressources	requêtes identiques soumises en direct (par des commandes du batch
		schedule <mark>r envoyé</mark> es par ssh) à un gestionnaire de jobs figurant parmi
		les gesti <mark>onnaire</mark> de jobs supportés par Vishnu.
4	Robustesse	
	Absence de plantage	Les processus du système ne doivent pas s'interrompre en
4.1	intempestif	fonctionnement "de croisière" (c'est-à-dire hors de toute défaillance
	monpesti.	logicielle ou matérielle du système hôte).
		Le système doit rester disponible en cas de défaillance de
		l'infrastructure n'affectant pas la connection de l'utilisateur aux
4.2	Résistance aux défaillances	
		configurés mais le nombre de processus lancés par le système sur les
		machines sera alors augmenté.
İ		Le délestage permettra à un administrateur de réduire de manière
4.3	Délestage	immédiate la charge générée par l'intergiciel sur une machine de
		l'infrastructure. Deux niveaux de délestage seront possible.
		Au niv <mark>eau "s</mark> oft", le délestage interrompra les activités en cours sur la
4.3.1	Délestage "soft"	machine concernée (activités contrôlées par le système Vishnu
	Dolosingo Bolt	uniquement). Ces activités pourront être relancées par le système lors
		de la commande de fin de délestage executée par l'administrateur.
		Au niveau "hard", le délestage interrompra tous les processus de
	Délestage "hard"	l'intergiciel sur la machine concernée sans effectuer d'actions
4.3.2		éventuellement nécessaires à leur redémarrage. Le redémarrage de
		Vishnu sur la machine utilisera la même procédure qu'un démarrage "à
		fr <mark>oid"</mark> st <mark>and</mark> ard.

3.2 Glossaire

- TODO

Environnement matériel et logiciel

TODO

Installation et maintenance

TODO