(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété Intellectuelle
Bureau international

(43) Date de la publication internationale
04 avril 2019 (04.04.2019)

WIPO | PCT

(10) Numéro de publication internationale
WO 2019/063887 A1

(51) Classification internationale des brevets :
G06F 3/06 (2006.01) *G06F 11/14* (2006.01)

(21) Numéro de la demande internationale :
PCT/FR2017/052680

(22) Date de dépôt international :
29 septembre 2017 (29.09.2017)

(25) Langue de dépôt : français

(26) Langue de publication : français

(71) Déposant : **MATRIX APPLIANCES** [FR/FR] ; 2 Rue Saint Bruno, 13004 Marseille (FR).

(72) Inventeur : **PELLETIER, Stéphane** ; 4 chemin des Anémones, Villa 13, 13012 Marseille (FR).

(74) Mandataire : **HIRSCH& PARTNERS (GROUPEMENT 721)** ; 12-14 rue Jean Nicot, 75007 PARIS (FR).

(81) États désignés *(sauf indication contraire, pour tout titre de protection nationale disponible)* : AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DJ, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IR, IS, JO, JP, KE, KG, KH, KN, KP, KR, KW, KZ, LA, LC, LK, LR, LS, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) États désignés *(sauf indication contraire, pour tout titre de protection régionale disponible)* : ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, RW, SD, SL, ST, SZ, TZ, UG,

(54) **Title:** DEVICE AND METHOD FOR BACKING UP DATA IN A COMPUTER NETWORK

(54) **Titre :** DISPOSITIF ET PROCÉDÉ DE SAUVEGARDE DE DONNÉES DANS UN RÉSEAU INFORMATIQUE

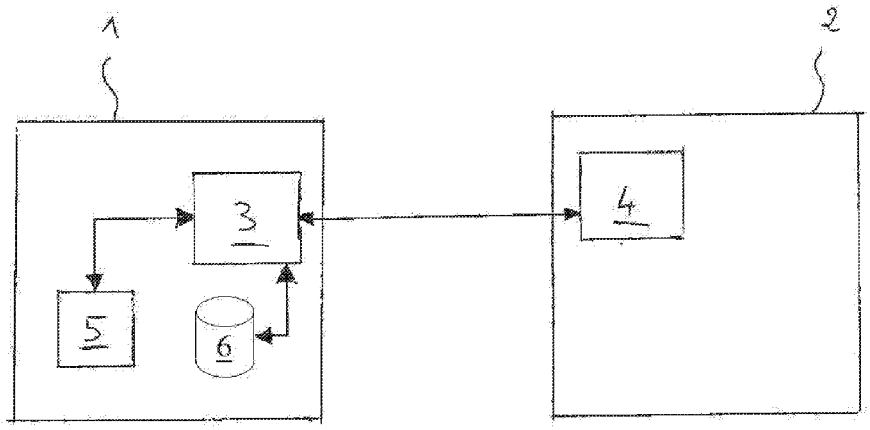

FIGURE UNIQUE

(57) **Abstract:** The invention relates to a device 1 and a method for backing up data in a computer network, said data 4 being stored in a machine 2, such as a server or a workstation. The backup device 1 is thus intended for being installed in a computer network comprising at least the machine 2, on which the data 4 to be backed up are stored. The device 1 comprises a backup module 3 and a backup zone 5 not shared with the machine 2. The backup module 3 is configured to access all or part of the data 4 of the machine 2 and to copy them locally in the backup zone 5.

(57) **Abrégé :** L'invention concerne un dispositif 1 et un procédé de saugarde de données dans un réseau informatique, lesdites données 4 étant stockées dans une machine 2, tel qu'un serveur ou un poste de travail. Le dispositif 1 de sauvegarde est donc destiné à être installé

WO 2019/063887 A1

[Suite sur la page suivante]

ZM, ZW), eurasien (AM, AZ, BY, KG, KZ, RU, TJ, TM), européen (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Publiée:

— *avec rapport de recherche internationale (Art. 21(3))*

dans un réseau informatique comprenant au moins la machine 2, sur laquelle sont stockées les données 4 à sauvegarder. Le dispositif 1 comprend un module de sauvegarde 3 et une zone de sauvegarde 5 non partagée avec la machine 2. Le module de sauvegarde 3 est configuré pour accéder à tout ou partie des données 4 de la machine 2 et pour les copier localement dans la zone de sauvegarde 5.

Dispositif et procédé de sauvegarde de données dans un réseau informatique

La présente invention concerne un dispositif et un procédé de sauvegarde de données dans un réseau informatique. Plus précisément, l'invention concerne la sauvegarde de données stockées dans une machine, tel qu'un serveur ou un poste de travail, installée dans un réseau informatique.

Par sauvegarde des données d'une machine physique ou virtuelle quelconque, on entend tout autant la sauvegarde de fichiers, de répertoires, de partitions ou de l'intégralité d'une machine.

Généralement, pour sauvegarder les données stockées sur une machine, on peut utiliser un outil logiciel de sauvegarde, qui s'exécute sur la machine. La sauvegarde des données peut être effectuée sur une partition du disque dur de la machine, ou sur un support de stockage amovible. Lorsque la machine est installée dans un réseau, on peut également sauvegarder les données de cette machine sur un dispositif de sauvegarde distant également installé dans le réseau.

Lorsque l'on administre un réseau comprenant plusieurs machines, tels des serveurs, des postes clients, etc…., il est intéressant d'utiliser un dispositif dédié, lui-même installé sur le réseau, pour réceptionner les différentes sauvegardes des données de ces différentes machines. Dans ce cas un outil de sauvegarde local est installé sur chacune des machines.

Ainsi, la réception des sauvegardes de chaque machine est centralisée au niveau d'un dispositif dédié. Pour que ce dispositif dédié puisse recevoir les données des autres machines dans le réseau il est nécessaire que ses répertoires soient configurés pour être partagé sur le réseau, qu'un port spécifique d'accès à ce dispositif soit ouvert, et enfin que les machines à sauvegarder et leurs outils de sauvegarde respectifs installés localement possèdent les droits d'accès en écriture sur le dispositif dédié.

Un des problèmes posés par de tels systèmes de sauvegarde de données, est l'ouverture d'un port spécifique d'accès au dispositif dédié qui réceptionne les sauvegardes de chaque machine. Un autre de ces problèmes est le fait de donner les droits d'écriture à chaque machine ou au logiciel de sauvegarde installé sur cette machine. Cette ouverture de port spécifique et/ou le fait de donner les droits d'écriture, rendent un tel système de sauvegarde vulnérable aux virus et logiciels malveillants, en particulier aux logiciels de type « ransomware ». En effet, de tels logiciels malveillants peuvent facilement découvrir la présence du dispositif dédié, en prenant connaissance des informations relatives aux droits en écriture sur le dispositif dédié dont dispose une

des machines du réseau, ou au partage du dispositif dédié, ou encore à l'existence du port spécifique d'accès aux données à sauvegarder de la machine en question.

Un des buts de l'invention est donc de résoudre notamment les problèmes précités. Ainsi, l'invention a notamment pour objectif de proposer un dispositif et un procédé de sauvegarde qui permettent au dispositif d'être masqué aux yeux d'éventuels virus ou logiciels malveillants, tout en assurant une sauvegarde et une capacité de restauration complètes.

L'invention a ainsi pour objet, selon un premier aspect, un dispositif de sauvegarde de données destiné à être installé dans un réseau informatique comprenant au moins une machine, telle qu'un serveur ou un poste de travail, qui comprend un ensemble des données à sauvegarder dans leur entièreté ou partiellement. La machine peut tout aussi bien être une machine physique ou une machine virtuelle.

Le dispositif comprend un module de sauvegarde, et une zone de sauvegarde non partagée avec la machine. Le module de sauvegarde est configuré pour accéder à tout ou partie des données de la machine et pour les copier localement dans la zone de sauvegarde.

Ainsi, le dispositif peut sauvegarder les données de la machine sans qu'un ou plusieurs de ses répertoires ne soient partagés avec cette machine, donc sans que la zone de sauvegarde ne soit partagée avec cette machine, et sans qu'il soit nécessaire d'installer un logiciel ou agent de sauvegarde sur la machine à sauvegarder elle-même. Aucun programme, de copie ou autre, ni aucune machine, ne disposent donc des droits d'écriture dans le dispositif, notamment dans sa zone de sauvegarde.

Le module de sauvegarde du dispositif est ainsi installé localement dans le dispositif, et vient accéder aux données de la machine à sauvegarder, c'est-à-dire lire ces données, à travers le réseau, sans utilisation d'un agent ou programme installé sur la machine à sauvegarder.

Le module de sauvegarde possède la visibilité sur la machine à sauvegarder sans qu'aucun partage ou chemin réseau ne soit indiqué dans la machine à sauvegarder, empêchant en cela toute écriture depuis la machine vers le dispositif de sauvegarde. A l'inverse, le dispositif pouvant lire les données de la machine distante et pouvant écrire sur lui-même, il peut accéder aux données de la machine pour les copier localement sans qu'aucun droit d'écriture réseau ne soit nécessaire.

Suivant certains modes de réalisation, le dispositif comprend en outre une ou plusieurs des caractéristiques suivantes, prise(s) isolément ou suivant toutes les combinaisons techniquement possibles :

- des droits d'accès aux données sont définis dans la machine associés à un identifiant et un mot de passe déterminés, le module de sauvegarde étant configuré pour envoyer à la machine une requête d'accès aux données de cette machine, ladite requête contenant un nom ou une adresse de la machine dans le réseau, et un identifiant et un mot de passe, en sorte de pouvoir accéder aux données de la machine une fois l'identifiant et le mot de passe transmis dans la requête reconnus par la machine comme correspondant respectivement à l'identifiant et au mot de passe déterminés ;
- les machines installées dans le réseau sont regroupées par domaine, et le module de sauvegarde est configuré pour envoyer à la machine la requête d'accès aux données de la machine, ladite requête contenant en outre le nom du domaine auquel appartient la machine ;
- le dispositif comprend une base de données dans laquelle sont stockés le nom ou l'adresse de chaque machine du réseau sur laquelle sont stockées des données à sauvegarder, les identifiants et mots de passe déterminés associés respectivement aux droits d'accès aux données de chacune de ces machines, et éventuellement les noms de domaine respectifs auxquels appartiennent ces machines, le module de sauvegarde étant configuré pour obtenir dans ladite base de données le nom ou l'adresse de la machine, l'identifiant et le mot de passe déterminés associés aux droits d'accès aux données de la machine, et éventuellement le nom de domaine auquel appartient ladite machine (2), et pour transmettre ces dits nom ou adresse, identifiant et mot de passe déterminés, et éventuellement ce nom de domaine, obtenus dans la base de données, dans la requête d'accès aux données envoyée à la machine ;
- la base de données comprend un identifiant et un mot de passe par défaut, le module de sauvegarde étant configuré pour déterminer s'il existe, dans la base de données, un identifiant et un mot de passe déterminés associés aux droits d'accès aux données de la machine, et, si l'identifiant et le mot de passe déterminés associés aux droits d'accès aux données de la machine n'existent pas dans la base de données, obtenir dans cette base de données l'identifiant et mot de passe par défaut et transmettre ces dits identifiant et mot de passe par défaut obtenus dans la base de données, dans la requête d'accès aux données envoyée à la machine.

De façon classique, pour pouvoir accéder à une machine donnée sur le réseau, le module de sauvegarde utilise, lors de l'envoi de la requête, le nom ou l'adresse de cette machine sur le réseau.

Ainsi, à la création d'une tâche de sauvegarde des données d'une machine déterminée, le nom ou d'adresse de cette machine dans le réseau, éventuellement le nom de domaine auquel cette machine appartient, et l'identifiant et mot de passe d'accès aux données de cette machine déterminée sont saisis, via une interface appropriée, puis restent stockés uniquement dans la base de données associée au module de sauvegarde. Seul le module de sauvegarde possède les droits de lecture, ces droits étant encapsulés dans la requête transmise à la machine à sauvegarder.

Le dispositif peut donc sauvegarder les données de la machine sans appartenir au domaine dans lequel sont situées les machines à sauvegarder.

L'invention a également pour objet, selon un deuxième aspect, un procédé de sauvegarde de données stockées dans une machine, tel qu'un serveur ou un poste de travail, installée dans un réseau informatique, par l'intermédiaire d'un module de sauvegarde d'un dispositif de sauvegarde installé dans ledit réseau informatique.

Le procédé comprend une étape d'accès par le module de sauvegarde à tout ou partie des données de la machine, et une étape de copie par ledit module de sauvegarde desdites données localement dans une zone de sauvegarde du dispositif non partagée avec la machine.

Suivant certains modes de mise en œuvre, le procédé comprend en outre une ou plusieurs des caractéristiques suivantes, prise(s) isolément ou suivant toutes les combinaisons techniquement possibles :

- des droits d'accès aux données sont définis dans la machine associés à un identifiant et un mot de passe déterminés, l'accès par le module de sauvegarde à tout ou partie des données de la machine comprenant l'envoi à la machine d'une requête d'accès aux données de la machine, ladite requête contenant un identifiant et un mot de passe, en sorte de permettre au module de sauvegarde d'accéder aux données de la machine une fois l'identifiant et le mot de passe transmis dans la requête reconnus par la machine comme correspondant respectivement à l'identifiant et au mot de passe déterminés ;
- les machines installées dans le réseau sont regroupées par domaine, et l'accès par le module de sauvegarde à tout ou partie des données de la machine comprend l'envoi à la machine de la requête d'accès aux données de la machine, ladite requête contenant en outre le nom du domaine auquel appartient la machine ;
- le dispositif comprend une base de données dans laquelle sont stockés le nom ou l'adresse de chaque machine du réseau sur laquelle sont stockées des données à sauvegarder, les identifiants et mots de passe déterminés associés respectivement aux droits d'accès aux données de ces machines respectives, et éventuellement les

noms de domaine respectifs auxquels appartiennent ces machines, le procédé comprenant l'obtention dans ladite base de données, par le module de sauvegarde, du nom ou de l'adresse de la machine, de l'identifiant et du mot de passe déterminés associés aux droits d'accès aux données de la machine, et éventuellement du nom de domaine auquel appartient ladite machine, ces dits nom ou adresse, identifiant et mot de passe déterminés, et éventuellement ce nom de domaine, obtenus dans la base de données, étant transmis dans la requête d'accès aux données envoyée à la machine ;

- la base de données comprend un identifiant et un mot de passe par défaut, le procédé comprenant une étape de détermination de l'existence, dans la base de données, d'un identifiant et d'un mot de passe déterminés associés aux droits d'accès aux données de la machine, et, si l'identifiant et le mot de passe déterminés associés aux droits d'accès aux données de la machine n'existent pas dans la base de données, une étape d'obtention dans cette base de données de l'identifiant et du mot de passe par défaut, ces dits identifiant et mot de passe par défaut, obtenus dans la base de données, étant transmis dans la requête d'accès aux données envoyée à la machine.

Grâce à des droits d'accès qui sont attribués uniquement au module de sauvegarde du dispositif, ce dernier peut lire les données de la machine à sauvegarder, et ensuite écrire ces données localement sur lui-même, sans aucun partage de tout ou partie de la zone de sauvegarde ou sans même être dans le même domaine. Aucun agent ou programme local sur la machine à sauvegarder n'est nécessaire, et donc aucun programme installé sur la machine ne possède des droits pour écrire sur le dispositif de sauvegarde.

Ainsi, le dispositif et le procédé de l'invention permettent de maintenir la machine de sauvegarde invisible sur le réseau vis-à-vis des virus et logiciels malveillants, en particulier dans le cas où le dispositif est hors domaine donc sans qu'aucun autre appareil n'ait de visibilité sur ce dispositif.

L'invention a enfin pour objet, selon un troisième aspect, un produit programme d'ordinateur comprenant des instructions qui, lorsqu'elles sont exécutées par une unité de traitement d'information d'un dispositif informatique, mettent en œuvre le procédé tel que présenté ci-dessus.

Les caractéristiques et avantages de l'invention apparaitront à la lecture de la description qui va suivre, donnée uniquement à titre d'exemple, et non limitative, en référence à la figure unique annexée, correspondant à une représentation schématique

d'un exemple de dispositif selon l'invention pour la mise en œuvre du procédé selon l'invention.

Sur la figure est représentée une partie d'un réseau informatique, dans lequel sont installés un dispositif 1 de sauvegarde selon l'invention, et une machine 2, tel qu'un serveur 2, contenant des données 4 stockées dans une zone de stockage de données.

La machine 2 contient également des programmes et modules opérationnels qui permettent d'assurer un certain nombre de fonctions et/ou de traiter les données 4.

Par extension, on entend par sauvegarde de données tout autant la sauvegarde des données 4 que des programmes et modules opérationnels mentionnés au paragraphe précédent, eux-mêmes stockés sous forme d'instructions. Dans la suite de la description, on utilise la référence 4 pour désigner toute donnée qui est à sauvegarder, qu'il s'agisse d'une donnée destinée à être traitée par un programme ou module opérationnel, ou d'un tel programme ou module opérationnel.

Une tâche de sauvegarde peut concerner un ou plusieurs fichiers de données spécifiques, un ou plusieurs répertoires spécifiques de stockage de fichiers, un ou plusieurs disques, une ou plusieurs partitions de disque, une machine physique ou virtuelle dans sa totalité, etc…

Le dispositif 1 comprend des moyens de traitement et des moyens de stockage d'instructions, non représentés sur la figure. Les moyens de stockage permettent de stocker des instructions, qui, lorsqu'elles sont exécutées par les moyens de traitement, permettent la mise en œuvre d'un certain nombre de fonctions, dont les fonctions de sauvegarde d'un module de sauvegarde 3.

Le dispositif 1 comprend par ailleurs une zone de sauvegarde 5 destinée à stocker les données 4 de la machine 2.

Les moyens de stockage d'instructions mentionnés plus haut et la zone de sauvegarde 5 peuvent indifféremment être des zones physiques de stockage distinctes ou faire partie de la même zone physique de stockage.

La zone de sauvegarde 5 n'est pas partagée avec la machine 2. Typiquement, la zone de sauvegarde 5 ne contient aucun répertoire partagé avec la machine 2. Autrement dit, la machine 2 ne possède aucun droit d'accès à la zone de sauvegarde 5, notamment aucun droit en écriture.

De préférence, le dispositif 1 n'est pas situé dans le domaine auquel appartient la machine 2.

Le module de sauvegarde 3 est configuré pour pouvoir accéder à au moins une partie, de préférence la totalité, des données 4, et pour copier ces données 4 localement

dans la zone de sauvegarde 5. Ces opérations d'accès, et de copie locale, sont ainsi réalisées sans utilisation d'un port spécifique d'accès par la machine 2 au dispositif 1.

De façon classique, pour accéder à une machine 2

Aucun agent ou programme de copie n'est installé sur la machine 2. Ainsi, aucun module de copie ne dispose des droits d'écriture ;

Le module de sauvegarde 3 met en œuvre les fonctions de sauvegarde, par l'intermédiaire d'instructions qui sont traitées par les moyens de traitement du dispositif 1, et réalise l'écriture des données sauvegardées localement dans la zone de sauvegarde 5, grâce à un partage administratif des données.

Pour l'accès aux données 4 de la machine 2, des droits d'accès sont définis dans cette machine 2, par exemple sous la forme d'un profil administrateur ou administrateur de sauvegarde. Ces droits d'accès sont associés à un identifiant et un mot de passe déterminés.

Pour accéder à ces données 4, le module de sauvegarde 3 est configuré pour envoyer à la machine 2 une requête d'accès contenant un identifiant et un mot de passe. Si cet identifiant et ce mot de passe transmis par le module de sauvegarde à la machine 2 dans la requête d'accès aux données 4, correspondent bien à l'identifiant et au mot de passe déterminé pour cette machine 2, c'est-à-dire si la machine 2 reconnaît ces identifiant et mot de passe comme étant bien ses identifiant et mots de passe déterminés, alors le module de sauvegarde peut accéder à ces données 4 de la machine 2.

Une base de données 6 est prévue dans le dispositif 1, associée au module de sauvegarde, dans laquelle sont stockés les noms ou adresses respectifs des machines du réseau sur lesquelles sont stockées des données à sauvegarder, et les identifiants et mots de passe déterminés associés respectivement aux droits d'accès aux données de chacune de ces machines.

Dans le cas où le dispositif 1 n'est pas installé dans le même domaine que l'une ou l'autre des machines 2 à sauvegarder, la base de données 6 stocke également le domaine auquel appartient chaque machine du réseau sur laquelle sont stockées des données à sauvegarder. La requête envoyée alors à la machine 2 par le module de sauvegarde 3 contient alors également le nom du domaine auquel appartient la machine 2.

Cette base de données 6 peut prendre la forme d'un simple tableau tel que le tableau 1 suivant :

Machine	Domaine	Identifiant d'accès	Mot de passe d'accès
SERVEUR1	Domaine1	IDServeur1	MDPServeur1
SERVEUR2	Domaine2	/	/
ADRESSESERVEUR3	Domaine2	IDServeur3	MDPServeur3
SERVEUR4	/	IDServeur4	MDPServeur4
POSTE1	Domaine1	IDPoste1	MDPPoste1
POSTE2	Domaine2	IDPoste2	MDPPoste2
POSTE3	Domaine2	IDPoste3	MDPPoste3
.....	.....	.....	.....

Tableau 1

Le module de sauvegarde est donc configuré pour aller chercher et obtenir dans la base de données 6 le nom ou l'adresse de la machine 2 dans le réseau, l'identifiant et le mot de passe déterminés associés aux droits d'accès aux données de cette machine 2, et éventuellement le nom de domaine auquel appartient la machine 2.

Il transmet ensuite ces nom ou adresse, identifiant et mot de passe déterminés, et éventuellement le nom de domaine, obtenus dans la base de données 6, dans la requête d'accès aux données 4 envoyée à la machine 2.

Ainsi, dans l'exemple du tableau 1 ci-dessus, lorsqu'une tâche de sauvegarde de la machine SERVEUR1 doit s'exécuter, le module de sauvegarde 3 interroge la base de données 6 et obtient l'identifiant déterminé IDServeur1 et le mot de passe déterminé MDPServeur1 associés à l'accès aux données de la machine SERVEUR1, ainsi que le nom de domaine Domaine1 auquel appartient la machine SERVEUR1, qu'il transmet dans la requête d'accès.

De façon classique, le nom ou l'adresse réseau de la machine est également utilisé par la requête pour pouvoir accéder à cette machine. Par exemple, dans le cas précédent, le nom SERVEUR1 est utilisé dans la requête, et un processus classique de résolution d'adresse permet d'accéder à la machine. Eventuellement, le nom de la machine peut être remplacé par son adresse sur le réseau, comme c'est le cas pour la machine SERVEUR3 dont le nom dans le tableau 1 ci-dessus est remplacé par l'adresse ADRESSESERVEUR3. Dans ce dernier cas, la requête utilise donc directement l'adresse de la machine sur le réseau pour accéder à cette machine.

Il peut aussi arriver que la machine à sauvegarder n'appartienne à aucun domaine, comme c'est le cas de la machine SERVEUR4 dans le tableau 1 ci-dessus. Dans ce cas, aucun nom de domaine n'est utilisé dans la requête.

Une interface utilisateur est prévue pour permettre à un utilisateur de renseigner le nom ou l'adresse de chaque machine du réseau, les identifiants et mots de passes

déterminés correspondant à chacun de ces machines, et éventuellement les noms de domaine respectifs auxquels appartiennent les machines 2, pour lesquelles une tâche de sauvegarde doit être planifiée. Ces couples identifiant/mot de passe correspondent respectivement à des couples identifiant/mot de passe associés à des profils utilisateurs, sur les machines respectives possédant les droits d'accès aux données de ces machines respectives.

Eventuellement, on prévoit que la base de données 6 comprennent un identifiant et un mot de passe par défaut (non représentés dans le tableau 1 ci-dessus).

Dans ce cas, le module de sauvegarde 3 détermine si un identifiant et un mot de passe déterminé associés aux droits d'accès aux données 4 de la machine 2, existent dans la base de données 6. Si le module de sauvegarde 3 ne trouve pas dans la base de données 6 d'identifiant et de mot de passe déterminés associés aux droits d'accès aux données 4 de la machine 2, alors il récupère l'identifiant et mot de passe par défaut, et transmet ces identifiant et mot de passe par défaut obtenus dans la base de données 6, dans la requête d'accès aux données 4 envoyée à la machine 2.

Dans l'exemple du tableau 1 ci-dessus, lorsque le module de sauvegarde exécute une tâche de sauvegarde de tout ou partie de la machine SERVEUR2, il interroge la base de données 6 et constate qu'aucun identifiant ni mot de passe n'est associé avec cette machine SERVEUR2. Il récupère alors l'identifiant et mot de passe par défaut et envoi la requête à la machine SERVEUR2 contenant le nom SERVEUR2, l'identifiant et mot de passe par défaut (ainsi que le nom de domaine Domaine2 dans cet exemple).

Ainsi, dans le cas où la machine 2 et le dispositif 1 sont installés sur le réseau en sorte d'appartenir à un même domaine déterminé de ce réseau, le dispositif 1 dispose automatiquement dans ce domaine de droits d'accès spécifiques aux données 4 de la machine 2. Ces droits sont renseignés dans la base de données 6, sous la forme de l'identifiant et du mot de passe correspondant. L'utilisation du nom de domaine dans la requête n'est alors pas indispensable

Cette configuration n'est cependant pas recommandée, car les droits d'accès permettant au dispositif 1 d'accéder aux données 4 de la machine 2 sont alors stockés dans la machine 2 sur un compte administrateur, c'est-à-dire un compte qui a lui-même accès au dispositif 1. Cette configuration offre donc une certaine visibilité, et un droit d'écriture potentiels, à une version évoluée d'un logiciel malveillant qui viendrait scanner les droits administrateurs et les partages administratifs liés.

Il est donc préférable de placer le dispositif 1 en dehors du domaine auquel appartient la machine 2 dans le réseau, ou dans ce même domaine mais sans que la

machine 2 ne possède des droits suffisants pour accéder au dispositif 1. Dans le premier cas, il est indispensable d'utiliser le nom de domaine dans la requête.

On note que le nom de domaine est présenté dans le tableau 1 ci-dessus dans un champ spécifique « Domaine », distinct des autres champs, notamment du champ « Machine » qui identifie chaque machine. Toutefois, ce nom de domaine peut également être concaténé d'une façon ou d'une autre avec l'identifiant de la machine, par exemple séparé d'un point, auquel cas un seul champ est nécessaire dans la base de données 6 pour stocker les deux données pour chaque machine à sauvegarder.

Un profil spécifique de sauvegarde peut alors être créé sur le dispositif 1 pour la machine 2 à sauvegarder, et l'identifiant et mot de passe correspondant peuvent être entrés dans la base de données 6, pour permettre ensuite au module de sauvegarde d'exécuter une tâche de sauvegarde sur la machine 2 tel qu'expliqué plus haut.

Ainsi, chaque profil ou tâche de sauvegarde peut disposer d'un identifiant et mot de passe spécifique associés à un nom ou une adresse de machine dans le réseau, qui sont des paramètres renseignés lors du paramétrage des tâches de sauvegarde dans le module de sauvegarde 3.

En envoyant la requête à la machine 2, tel qu'expliqué ci-dessus, le module de sauvegarde 3, obtient les droits nécessaires pour accéder aux données 4, le temps de la sauvegarde seulement. Une fois que les données 4 sont récupérées par le module de sauvegarde 3 en vue de les copier localement, les droits d'origines sont rétablis, c'est-à-dire que les droits d'accès utilisés ne sont valables que le temps de l'exécution de l'accès aux données 4 (donc de la lecture des données 4).

Seul le module de sauvegarde 3 possède les droits de lecture des données 4 de la machine 2, ces droits étant encapsulés dans la requête transmise par le module de sauvegarde 3 à la machine 2 lors de l'exécution de la tâche de sauvegarde correspondante.

Le dispositif 1 reste donc invisible à tout virus ou logiciel malveillant qui pénétrerait le réseau même en possédant des droits d'administrateur de ce réseau. Théoriquement, lors de l'exécution de la requête d'accès aux données 4, le dispositif 1 devient potentiellement visible pour un logiciel malveillant suffisamment évolué. Toutefois, l'imperméabilité du dispositif 1 perdure même dans cette phase, car aucun droit en écriture sur le dispositif 1 (zone de sauvegarde 5) n'est concédé à aucune machine 2 du réseau.

On notera que les droits d'accès aux données 4 d'une machine 2 sont généralement non seulement des droits de lecture mais également d'écriture. En effet, le droit en écriture est également nécessaire pour lire certaines données contenues dans

des fichiers ouverts, en cours d'utilisation par d'autres processus de la machine 2, et qui continuent à recevoir des données pendant la sauvegarde (c'est le cas par exemple des fichiers de messageries ou de bases de données).

La présente description est donnée à titre d'exemple, et n'est pas limitative de l'invention.

En particulier, le module de sauvegarde 3 n'est pas nécessairement localisé physiquement dans un seul dispositif. Il peut être réparti dans plusieurs dispositif, la pluralité de ces dispositifs constituant alors le dispositif 1 selon l'invention.

De même, le dispositif 1 de sauvegarde peut lui-même prendre la forme d'une machine virtuelle comprenant un système d'exploitation et un module de sauvegarde

Par ailleurs, le module de sauvegarde 3 et la base de données 6 sont présentés séparément dans la représentation fonctionnelle de la figure. Cependant, la base de données et le module de sauvegarde peuvent tout aussi bien être intégrés physiquement dans un unique ensemble logiciel exécutable sur le dispositif 1. Par extension, dans ce dernier cas, on utilise l'expression module de sauvegarde également pour désigner cet unique ensemble logiciel

REVENDICATIONS

1.- Dispositif (1) de sauvegarde de données destiné à être installé dans un réseau informatique comprenant au moins une machine (2), telle qu'un serveur ou un poste de travail, sur laquelle sont stockées des données (4), caractérisé en ce qu'il comprend un module de sauvegarde (3), et une zone de sauvegarde (5) non partagée avec la machine (2), ledit module de sauvegarde (3) étant configuré pour accéder à tout ou partie des données (4) de la machine (2) et pour les copier localement dans ladite zone de sauvegarde (5).

2. Dispositif (1) selon la revendication 1, des droits d'accès aux données (4) étant définis dans la machine (2) associés à un identifiant et un mot de passe déterminés, caractérisé en ce que le module de sauvegarde (3) est configuré pour envoyer à la machine (2) une requête d'accès aux données (4) de la machine (2), ladite requête contenant un nom ou une adresse de la machine (2) dans le réseau, un identifiant et un mot de passe, en sorte de pouvoir accéder aux données (4) de cette machine (2) une fois l'identifiant et le mot de passe transmis dans la requête reconnus par la machine (2) comme correspondant respectivement à l'identifiant et au mot de passe déterminés.

3. Dispositif (1) selon la revendication 2, les machines installées dans le réseau étant regroupées par domaine, caractérisé en ce que le module de sauvegarde (3) est configuré pour envoyer à la machine (2) la requête d'accès aux données (4) de la machine (2), ladite requête contenant en outre le nom du domaine auquel appartient la machine (2).

4. Dispositif (1) selon l'une quelconque des revendications 2 et 3, caractérisé en ce qu'il comprend une base de données (6) dans laquelle sont stockés les noms ou adresses de chaque machine du réseau sur laquelle sont stockées des données à sauvegarder, les identifiants et mots de passe déterminés associés respectivement aux droits d'accès aux données de chacune de machines, et éventuellement les noms de domaine respectifs auxquels appartiennent ces dites machines, le module de sauvegarde (3) étant configuré pour :

- obtenir dans ladite base de données (6) le nom ou l'adresse de la machine (2) dans le réseau, l'identifiant et le mot de passe déterminés associés aux droits d'accès aux données de cette machine (2), et éventuellement le nom de domaine auquel appartient cette machine (2),

- transmettre ces dits nom ou adresse, identifiant et mot de passe déterminés, et éventuellement ce nom de domaine, obtenus dans la base de données (6), dans la requête d'accès aux données (4) envoyée à la machine (2).

5. Dispositif (1) selon la revendication 4, caractérisé en ce que la base de données (6) comprend un identifiant et un mot de passe par défaut, et en ce que le module de sauvegarde (3) est configuré pour :

- déterminer s'il existe, dans la base de données (6), un identifiant et un mot de passe déterminés associés aux droits d'accès aux données (4) de la machine (2),

- si l'identifiant et le mot de passe déterminés associés aux droits d'accès aux données (4) de la machine (2) n'existent pas dans la base de données (6), obtenir dans cette base de données (6) l'identifiant et mot de passe par défaut, et transmettre ces dits identifiant et mot de passe par défaut obtenus dans la base de données (6), dans la requête d'accès aux données (4) envoyée à la machine (2).

6.- Procédé de sauvegarde de données stockées dans une machine (2), tel qu'un serveur ou un poste de travail, installée dans un réseau informatique, par l'intermédiaire d'un module de sauvegarde (3) d'un dispositif (1) de sauvegarde installé dans ledit réseau informatique, caractérisé en ce qu'il comprend une étape d'accès par le module de sauvegarde (3) à tout ou partie des données (4) de la machine (2), et une étape de copie par ledit module de sauvegarde (3) desdites données (4) localement dans une zone de sauvegarde (5) du dispositif (1) non partagée avec la machine (2).

7. Procédé selon la revendication 6, des droits d'accès aux données (4) étant définis dans la machine (2) associés à un identifiant et un mot de passe déterminés, caractérisé en ce que l'accès par le module de sauvegarde (3) à tout ou partie des données (4) de la machine (2) comprend l'envoi à la machine (2) d'une requête d'accès aux données (4) de la machine (2), ladite requête contenant un nom ou une adresse de la machine (2) sur le réseau, un identifiant et un mot de passe, en sorte de permettre au module de sauvegarde (4) d'accéder aux données (4) de la machine (2) une fois l'identifiant et le mot de passe transmis dans la requête reconnus par la machine (2) comme correspondant respectivement à l'identifiant et au mot de passe déterminés.

8. Procédé selon la revendication 7, les machines installées dans le réseau étant regroupées par domaine, caractérisé en ce que l'accès par le module de sauvegarde (3) à tout ou partie des données (4) de la machine (2) comprend l'envoi à la machine (2) de la

requête d'accès aux données (4) de la machine (2), ladite requête contenant en outre le nom du domaine auquel appartient la machine (2).

9. Procédé selon l'une quelconque des revendications 7 et 8, le dispositif (1) comprenant une base de données (6) dans laquelle sont stockés les noms ou adresse de chaque machine du réseau sur laquelle sont stockées des données à sauvegarder, les identifiants et mots de passe déterminés associés respectivement aux droits d'accès aux données de chacune de ces machines, et éventuellement les noms de domaine respectifs auxquels appartiennent ces dites machines, caractérisé en ce que le procédé comprend l'obtention dans ladite base de données (6), par le module de sauvegarde (3), du nom ou de l'adresse de la machine (2), de l'identifiant et du mot de passe déterminés associés aux droits d'accès aux données de cette machine (2), et éventuellement du nom de domaine auquel appartient cette machine (2), et en ce que ces dits nom ou adresse, identifiant et mot de passe déterminés, et éventuellement ce nom de domaine, obtenus dans la base de données (6), sont transmis dans la requête d'accès aux données (4) envoyée à la machine (2).

10. Procédé selon la revendication 9, la base de données (6) comprenant un identifiant et un mot de passe par défaut, caractérisé en ce qu'il comprend :

- une étape de détermination de l'existence, dans la base de données (6), d'un identifiant et d'un mot de passe déterminés associés aux droits d'accès aux données (4) de la machine (2),
- si l'identifiant et le mot de passe déterminés associés aux droits d'accès aux données (4) de la machine (2) n'existent pas dans la base de données (6), une étape d'obtention dans cette base de données (6) de l'identifiant et du mot de passe par défaut, ces dits identifiant et mot de passe par défaut, obtenus dans la base de données (6), étant transmis dans la requête d'accès aux données (4) envoyée à la machine (2).

11. Produit programme d'ordinateur (3) comprenant des instructions qui, lorsqu'elles sont exécutées par une unité de traitement d'information d'un dispositif informatique (1), mettent en œuvre le procédé selon l'une quelconque des revendications 6 à 10.

WO 2019/063887 PCT/FR2017/052680

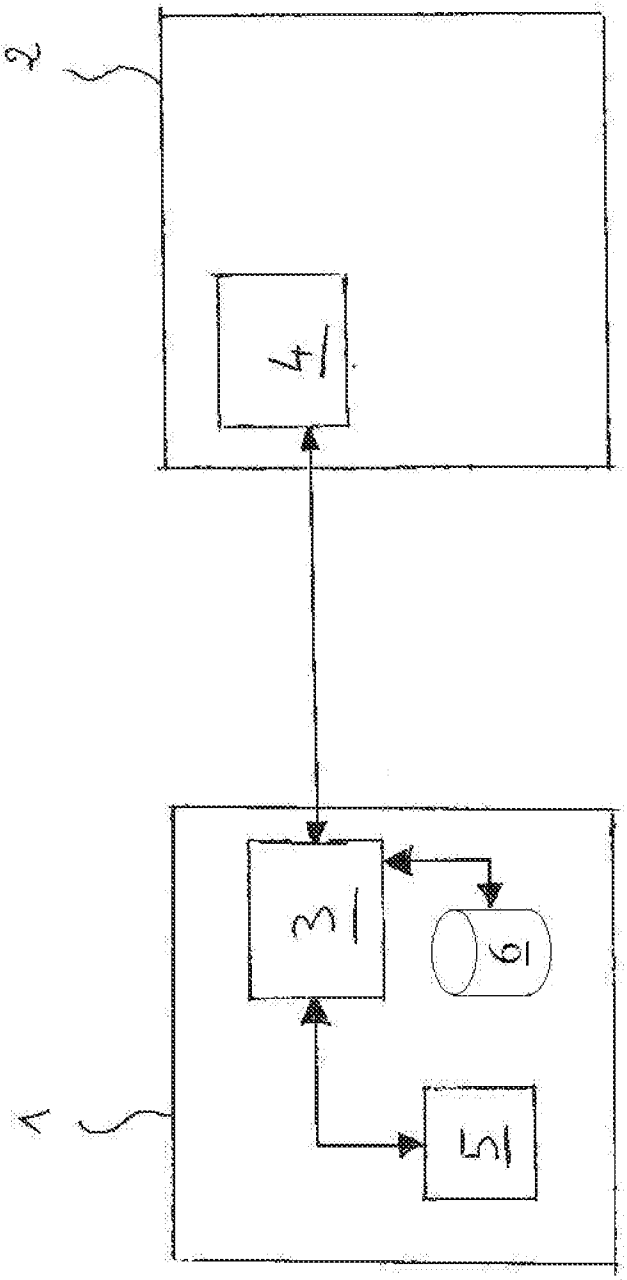

FIGURE UNIQUE

INTERNATIONAL SEARCH REPORT

International application No
PCT/FR2017/052680

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06F3/06 G06F11/14
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/041726 A1 (STEUBING EDMUND G [US]) 23 February 2006 (2006-02-23) figures 1-2 paragraph [0011] - paragraph [0029] paragraph [0041] paragraph [0047] -----	1-11
X	US 2007/220319 A1 (DESAI ASIT A [US] ET AL) 20 September 2007 (2007-09-20) figures 1,3 paragraph [0019] - paragraph [0020] paragraph [0026] -----	1-11

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
6 June 2018	15/06/2018

Name and mailing address of the ISA/	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Alliot, Sylvain

3

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/FR2017/052680

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2006041726 A1	23-02-2006	NONE	
US 2007220319 A1	20-09-2007	NONE	

RAPPORT DE RECHERCHE INTERNATIONALE

Demande internationale n°
PCT/FR2017/052680

A. CLASSEMENT DE L'OBJET DE LA DEMANDE
INV. G06F3/06 G06F11/14
ADD.

Selon la classification internationale des brevets (CIB) ou à la fois selon la classification nationale et la CIB

B. DOMAINES SUR LESQUELS LA RECHERCHE A PORTE

Documentation minimale consultée (système de classification suivi des symboles de classement)
G06F

Documentation consultée autre que la documentation minimale dans la mesure où ces documents relèvent des domaines sur lesquels a porté la recherche

Base de données électronique consultée au cours de la recherche internationale (nom de la base de données, et si cela est réalisable, termes de recherche utilisés)
EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie*	Identification des documents cités, avec, le cas échéant, l'indication des passages pertinents	no. des revendications visées
X	US 2006/041726 A1 (STEUBING EDMUND G [US]) 23 février 2006 (2006-02-23) figures 1-2 alinéa [0011] - alinéa [0029] alinéa [0041] alinéa [0047] -----	1-11
X	US 2007/220319 A1 (DESAI ASIT A [US] ET AL) 20 septembre 2007 (2007-09-20) figures 1,3 alinéa [0019] - alinéa [0020] alinéa [0026] -----	1-11

☐ Voir la suite du cadre C pour la fin de la liste des documents

☒ Les documents de familles de brevets sont indiqués en annexe

* Catégories spéciales de documents cités:

"A" document définissant l'état général de la technique, non considéré comme particulièrement pertinent

"E" document antérieur, mais publié à la date de dépôt international ou après cette date

"L" document pouvant jeter un doute sur une revendication de priorité ou cité pour déterminer la date de publication d'une autre citation ou pour une raison spéciale (telle qu'indiquée)

"O" document se référant à une divulgation orale, à un usage, à une exposition ou tous autres moyens

"P" document publié avant la date de dépôt international, mais postérieurement à la date de priorité revendiquée

"T" document ultérieur publié après la date de dépôt international ou la date de priorité et n'appartenant pas à l'état de la technique pertinent, mais cité pour comprendre le principe ou la théorie constituant la base de l'invention

"X" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme nouvelle ou comme impliquant une activité inventive par rapport au document considéré isolément

"Y" document particulièrement pertinent; l'invention revendiquée ne peut être considérée comme impliquant une activité inventive lorsque le document est associé à un ou plusieurs autres documents de même nature, cette combinaison étant évidente pour une personne du métier

"&" document qui fait partie de la même famille de brevets

Date à laquelle la recherche internationale a été effectivement achevée	Date d'expédition du présent rapport de recherche internationale
6 juin 2018	15/06/2018

Nom et adresse postale de l'administration chargée de la recherche internationale	Fonctionnaire autorisé
Office Européen des Brevets, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016	Alliot, Sylvain

RAPPORT DE RECHERCHE INTERNATIONALE

Renseignements relatifs aux membres de familles de brevets

Demande internationale n°
PCT/FR2017/052680

Document brevet cité au rapport de recherche	Date de publication	Membre(s) de la famille de brevet(s)	Date de publication
US 2006041726 A1	23-02-2006	AUCUN	
US 2007220319 A1	20-09-2007	AUCUN	