



Mac OS X Server

Administration de la
haute disponibilité
Pour la version 10.4
ou ultérieure

🍏 Apple Computer, Inc.

© 2005 Apple Computer, Inc. Tous droits réservés.

Le propriétaire ou l'utilisateur autorisé d'un exemplaire enregistré du logiciel Mac OS X Server peut reproduire cette publication aux fins d'apprentissage du logiciel. Cette publication ne peut être reproduite ou transmise en tout ou partie à des fins commerciales, comme la vente de copies de cette publication ou la fourniture d'un service d'assistance payant.

Tout a été mis en œuvre pour que les informations contenues dans ce manuel soient exactes. Apple Computer, Inc., n'est pas responsable des erreurs d'impression ou de typographie.

Apple
1 Infinite Loop
Cupertino CA 95014-2084
www.apple.com

Le logo Apple est une marque d'Apple Computer Inc. déposée aux États-Unis et dans d'autres pays. L'utilisation de ce logo à des fins commerciales via le clavier (Option-1) pourra constituer un acte de contrefaçon et/ou de concurrence déloyale.

Apple, le logo Apple, AppleShare, AppleTalk, Mac, Macintosh, QuickTime, Xgrid et Xserve sont des marques d'Apple Computer, Inc. déposées aux États-Unis et dans d'autres pays. Finder est une marque d'Apple Computer, Inc.

Adobe et PostScript sont des marques d'Adobe Systems Incorporated.

UNIX est une marque déposée aux États-Unis et dans d'autres pays, sous licence exclusive de X/Open Company Ltd.

Tous les autres noms de produits sont des marques de leurs propriétaires respectifs. Les produits commercialisés par des entreprises tierces ne sont mentionnés qu'à titre d'information, sans aucune intention de préconisation ni de recommandation. Apple ne se porte pas garant de ces produits et décline toute responsabilité quant à leur utilisation et à leur fonctionnement.

F019-0175/03-24-05

Table des matières

Préface	5	À propos de ce guide
	5	Nouveautés de la version 10.4
	5	Contenu de ce guide
	6	Utilisation de l'aide à l'écran
	6	La suite Mac OS X Server
	8	Obtenir des mises à jour de documentation
	8	Informations complémentaires
Chapitre 1	11	Vue d'ensemble de la haute disponibilité
	11	Qu'est-ce que la haute disponibilité ?
	12	Un très vaste domaine
	12	Solutions logicielles de haute disponibilité
	13	Solutions matérielles de haute disponibilité
Chapitre 2	15	Configuration du basculement IP
	16	Vue d'ensemble du basculement IP
	18	Acquisition d'une adresse maître — Chaîne d'événements
	19	Libération d'une adresse maître — Chaîne d'événements
	20	Configuration du basculement IP
	20	Connexion des serveurs maître et de sauvegarde au même réseau
	21	Connexion des serveurs maître et de sauvegarde entre eux
	21	Configuration du serveur maître pour le basculement
	22	Configuration du serveur de sauvegarde pour le basculement
	23	Consultation de l'historique Basculement IP
Chapitre 3	25	Configuration d'autres aspects de la haute disponibilité
	25	Élimination de points de défaillance uniques
	26	Utilisation de Xserve et de Xserve RAID
	26	Utilisation de Xserve
	27	Utilisation de Xserve RAID
	28	Utilisation de l'alimentation de secours
	28	Utilisation d'UPS avec Xserve RAID
	29	Utilisation d'UPS avec Xserve
	30	Configuration du redémarrage automatique de votre serveur

	31	Pour de bonnes conditions de fonctionnement
	31	Réplique Open Directory
	31	Protection de la sécurité d'un serveur
	32	Agrégation de liens
	34	Le protocole d'agrégation de liens (LACP, Link Aggregation Control Protocol)
	34	Scénarios d'agrégation de liens
	36	Configuration de l'agrégation de liens dans Mac OS X Server
	38	Contrôle de l'état de l'agrégation de liens
	39	Équilibrage de la charge
	40	Sauvegarde
	40	Développement d'une stratégie de sauvegarde
	42	Outils de ligne de commande de restauration et de sauvegarde
Chapitre 4	43	Contrôle de la disponibilité de serveur
	43	Console
	44	Contrôle de serveur
	44	Admin RAID
	44	Outils de contrôle de disque
	46	Outils de contrôle de réseau
Chapitre 5	47	Résolution de problèmes de basculement IP
	47	Le service ne bascule pas automatiquement lorsque le service primaire est indisponible
	48	Un destinataire de courriers électroniques ne reçoit pas de notifications
	48	La basculement a bien eu lieu mais les problèmes persistent
Glossaire	49	
Index	57	

À propos de ce guide

Ce guide explique comment assurer la haute disponibilité de vos services Mac OS X Server.

Dans ce guide, vous apprendrez comment utiliser le basculement IP, l'agrégation de liens, l'équilibrage de la charge et d'autres configurations matérielles et logicielles pour garantir la haute disponibilité de vos services Mac OS X Server.

Nouveautés de la version 10.4

Mac OS X Server 10.4 offre des améliorations majeures en matière de haute disponibilité :

- Agrégation de liens : Mac OS X Server gère désormais l'agrégation de liens, qui se configure dans la sous-fenêtre Réseau des Préférences Système.
- Nouveau gestionnaire de daemons : le daemon `launchd` a remplacé le processus `watchdog`. À l'instar de `watchdog`, `launchd` veille à ce que les processus censés fonctionner fonctionnent en permanence.

Contenu de ce guide

Ce guide comprend les chapitres suivants :

- Le chapitre 1, "Vue d'ensemble de la haute disponibilité" explique le concept de haute disponibilité.
- Le chapitre 2, "Configuration du basculement IP" est décrit la procédure de configuration du basculement IP dans Mac OS X Server.
- Le chapitre 3, "Configuration d'autres aspects de la haute disponibilité" explique comment utiliser l'agrégation des liens, l'équilibrage de la charge et d'autres configurations matérielles et logicielles pour garantir la haute disponibilité.
- Le chapitre 4, "Contrôle de la disponibilité de serveur" présente les divers outils que vous pouvez utiliser pour contrôler la disponibilité de vos services.
- Le chapitre 5, "Résolution de problèmes de basculement IP" décrit des problèmes courants et fournit des informations visant à les résoudre.
- Le glossaire donne de courtes définitions des termes utilisés dans ce guide.

Remarque : étant donné qu'Apple publie régulièrement de nouvelles versions et mises à jour de ses logiciels, les illustrations de ce document peuvent être différentes de celles qui s'affichent à l'écran.

Utilisation de l'aide à l'écran

Vous pouvez afficher des instructions et d'autres informations utiles sur la suite serveur en accédant à utilisant l'aide à l'écran.

Sur un ordinateur qui exécute Mac OS X Server, vous pouvez accéder à l'aide à l'écran après avoir ouvert le "Gestionnaire de groupe de travail" ou Admin Serveur. À partir du menu d'aide, sélectionnez l'une des options suivantes :

- *Aide Gestionnaire de groupe de travail* ou *Aide Admin Serveur* affiche des informations sur l'application.
- *Aide Mac OS X Server* affiche la page d'aide principale du serveur, à partir de laquelle vous pouvez rechercher des informations sur le serveur.
- *Documentation* vous permet d'accéder au site www.apple.com/fr/server/documentation, à partir duquel vous pouvez télécharger la documentation du serveur.

Vous pouvez également accéder à l'aide à l'écran à partir du Finder ou d'autres applications d'un serveur ou d'un ordinateur administrateur. (Un ordinateur administrateur est un ordinateur Mac OS X sur lequel est installé un logiciel d'administration de serveur.) Utilisez le menu Aide afin d'ouvrir Visualisation Aide, puis choisissez Bibliothèque > Aide Mac OS X Server.

Pour consulter les toutes dernières rubriques d'aide, assurez-vous que l'ordinateur serveur ou administrateur est connecté à Internet lorsque vous utilisez Visualisation Aide. Visualisation Aide extrait et met en cache automatiquement les toutes dernières rubriques d'aide sur Internet concernant le serveur. Lorsque vous n'êtes pas connecté à Internet, Visualisation Aide affiche les rubriques d'aide mises en cache.

La suite Mac OS X Server

La documentation de Mac OS X Server comprend une série de guides présentant les services offerts ainsi que les instructions relatives à leur configuration, leur gestion et leur dépannage. Tous les guides sont disponibles au format PDF via :

www.apple.com/fr/server/documentation/

Ce guide ...	explique comment :
<i>Mac OS X Server Premiers contacts pour la version 10.4 ou ultérieure</i>	installer Mac OS X Server et le configurer pour la première fois.
<i>Mac OS X Server Mise à niveau et migration vers la version 10.4 ou ultérieure</i>	utiliser les données et réglages des services actuellement utilisés sur les versions antérieures du serveur.

Ce guide ...	explique comment :
<i>Mac OS X Server Gestion des utilisateurs pour la version 10.4 ou ultérieure</i>	créer et gérer les utilisateurs, groupes et listes d'ordinateurs. Configurer les préférences gérées des clients Mac OS X.
<i>Mac OS X Server Administration des services de fichiers pour la version 10.4 ou ultérieure</i>	partager des volumes ou dossiers de serveur sélectionnés parmi les clients du serveur via les protocoles suivants : AFP, NFS, FTP et SMB/CIFS.
<i>Mac OS X Server Administration du service d'impression pour la version 10.4 ou ultérieure</i>	héberger les imprimantes partagées et gérer les files d'attente et travaux d'impression associés.
<i>Mac OS X Server Administration des images système et de la mise à jour de logiciels pour la version 10.4 ou ultérieure</i>	utiliser NetBoot et Installation en réseau pour créer des images disque à partir desquelles les ordinateurs Macintosh peuvent démarrer sur le réseau. Configurer un serveur de mise à jour de logiciels pour la mise à jour d'ordinateurs clients via le réseau.
<i>Mac OS X Server Administration du service de messagerie pour la version 10.4 ou ultérieure</i>	installer, configurer et administrer les services de courrier sur le serveur.
<i>Mac OS X Server Administration des technologies Web pour la version 10.4 ou ultérieure</i>	configurer et gérer un serveur Web, dont WebDAV, WebMail, et les modules Web.
<i>Mac OS X Server Administration des services réseau pour la version 10.4 ou ultérieure</i>	installer, configurer et administrer DHCP, DNS, VPN, NTP, coupe-feu IP et services NAT sur le serveur.
<i>Mac OS X Server Administration d'Open Directory pour la version 10.4 ou ultérieure</i>	gérer les services de répertoires et d'authentification.
<i>Mac OS X Server Administration du QuickTime Streaming Server pour la version 10.4 ou ultérieure</i>	configurer et gérer les services d'enchaînement QuickTime.
<i>Mac OS X Server Administration des services Windows pour la version 10.4 ou ultérieure</i>	configurer et gérer des services tels que PDC, BDC, fichiers et impression pour les utilisateurs d'ordinateurs Windows.
<i>Mac OS X Server Migration à partir de Windows NT pour la version 10.4 ou ultérieure</i>	déplacer des comptes, des dossiers partagés et des services à partir de serveurs Windows NT vers Mac OS X Server.
<i>Mac OS X Server Administration du serveur d'applications Java pour la version 10.4 ou ultérieure</i>	configurer et administrer un serveur d'applications JBoss sur Mac OS X Server.
<i>Mac OS X Server Administration de la ligne de commande pour la version 10.4 ou ultérieure</i>	utiliser les commandes et les fichiers de configuration pour exécuter les tâches d'administration du serveur via l'interpréteur de commandes UNIX.
<i>Mac OS X Server Administration des services de collaboration pour la version 10.4 ou ultérieure</i>	configurer et gérer Weblog, la discussion en ligne et d'autres services qui facilitent les interactions entre utilisateurs.

Ce guide ...	explique comment :
<i>Mac OS X Server Administration de la haute disponibilité pour la version 10.4 ou ultérieure</i>	gérer le basculement IP, l'agrégation des liens, l'équilibrage de charge et d'autres configurations matérielles et logicielles pour garantir la haute disponibilité des services Mac OS X Server.
<i>Mac OS X Server Administration Xgrid pour la version 10.4 ou ultérieure</i>	gérer des clusters de calcul Xserve à l'aide de l'application Xgrid.
<i>Mac OS X Server Glossaire : contient la terminologie relative à Mac OS X Server, Xserve, Xserve RAID et Xsan</i>	interpréter les termes utilisés pour les produits de serveur et les produits de stockage.

Obtenir des mises à jour de documentation

Apple publie régulièrement de nouvelles rubriques d'aide à l'écran, des guides révisés et des documents supplémentaires de solutions. Les nouvelles rubriques d'aide incluent des mises à jour des guides les plus récents.

- Pour afficher de nouvelles rubriques d'aide à l'écran, assurez-vous que votre ordinateur serveur ou administrateur est connecté à Internet et cliquez sur le lien Informations de dernière minute dans la page d'aide principale de Mac OS X Server.
- Pour télécharger les guides et documents de solutions les plus récents au format PDF, rendez-vous à la page Web de documentation de Mac OS X Server : www.apple.com/fr/server/documentation.

Informations complémentaires

Pour plus d'informations, consultez les ressources suivantes :

Documents Ouvrez-moi : mises à jour importantes et informations spécifiques. Recherchez-les sur les disques du serveur.

Site Web de Mac OS X Server : passerelle vers des informations détaillées sur des produits et technologies.
www.apple.com/fr/macosx/server/

Site Web Service & Support AppleCare : accès à des centaines d'articles provenant de l'organisation d'assistance d'Apple.
www.apple.com/fr/support/

Formation des clients Apple : cours en salle et autoformations afin de développer vos compétences en termes d'administration de serveur.
train.apple.com/

Groupes de discussion Apple : moyen de partager des questions, des connaissances et des conseils avec d'autres administrateurs.
discussions.info.apple.com/

Répertoire de liste de diffusion Apple : abonnez-vous à des listes de diffusion afin de pouvoir communiquer par courrier électronique avec d'autres administrateurs.
discussions.info.apple.com/

Ce chapitre décrit le concept de haute disponibilité et explique ce que vous devez faire pour l'appliquer à vos déploiements Mac OS X Server.

En raison de garanties de niveau de service, d'exigences commerciales ou de réglementations industrielles établies, de nombreuses entreprises requièrent une disponibilité maximale des services informatiques. Les pannes imprévues, événements autrefois considérés comme de faible importance, peuvent aujourd'hui fortement compromettre les opérations commerciales. Les produits Mac OS X Server d'Apple offrent une réponse à cela puisqu'ils sont conçus pour garantir une haute disponibilité et gérer les pannes de système.

Qu'est-ce que la haute disponibilité ?

Dans le contexte des services réseau, la haute disponibilité fait référence à une disponibilité presque continue des services. Dans de nombreuses organisations, un système ou un service hautement disponible doit être utilisable 99 % du temps. Certaines organisations exigent même une disponibilité plus élevée : 99,99 % ou 99,999 % dans certains cas.

Le tableau ci-dessous met ces chiffres en perspective :

Disponibilité	Durée de fonctionnement (env.)	Temps d'arrêt (env.)
99 %	361,8 jours	84 heures
99,9 %	364,9 jours	8,5 heures
99,999 %	365,3 jours	5 minutes

Après avoir déterminé le niveau de disponibilité que doivent fournir vos services, vous pouvez calculer le temps d'arrêt admissible et utiliser le chiffre obtenu afin de déterminer comment configurer votre matériel et vos logiciels pour satisfaire à ce niveau de disponibilité.

Un très vaste domaine

La haute disponibilité est un très vaste domaine. Comme vous l'apprendrez en parcourant ce guide, la haute disponibilité demande une combinaison de solutions matérielles et logicielles.

Solutions logicielles de haute disponibilité

Mac OS X Server offre plusieurs fonctionnalités permettant de garantir la disponibilité la plus élevée possible :

- Le service de basculement IP vous permet de fournir de la redondance. Si le serveur maître tombe en panne, un serveur de sauvegarde assume automatiquement son rôle, avec une interruption minimale voire invisible pour les utilisateurs.
- Le daemon `launchd` veille à ce que l'exécution des processus spécifiés dans son fichier de configuration soit continue. Si l'un de ces processus se termine, `launchd` le redémarre. Pour en savoir plus sur `launchd`, reportez-vous au guide d'administration à l'aide de la ligne de commande.
- Le service Open Directory vous permet de répliquer vos services de répertoire et d'authentification de manière à ce que les utilisateurs ne puissent remarquer qu'une courte interruption des services si un système de répertoires tombe en panne ou devient inaccessible.
- La sous-fenêtre Économiseur d'énergie des Préférences Système vous permet de définir une option de redémarrage de l'ordinateur en cas de panne.
- Les utilitaires de contrôle tels que Contrôle de serveur et Admin RAID vous avertissent par courrier électronique lorsque les conditions de fonctionnement des composants dépassent les seuils que vous avez prédéfinis, et ce, afin que vous puissiez réagir rapidement en évitant ou résolvant le problème.
- Avec d'autres outils de tierces parties, la commande `rsync` vous permet de mettre vos données en miroir afin qu'en cas de panne du serveur, vous puissiez les restaurer sur un autre serveur, avec une interruption minimale pour les utilisateurs.
- L'agrégation de liens vous permet de conférer performances et tolérance de pannes à vos connexions réseau.

Solutions matérielles de haute disponibilité

Apple fournit des solutions matérielles offrant une meilleure fiabilité ce qui augmente la disponibilité :

- Xserve possède plusieurs fonctionnalités garantissant sa disponibilité, dont la mise en miroir RAID intégrée (qui permet une récupération rapide en cas de panne de disque) et la mémoire à code correcteur d'erreurs (ECC, Error Correcting Code), qui vise à éviter la corruption de données.
- Xserve RAID intègre plusieurs composants redondants qui permettent au système de fonctionner même si l'un d'entre eux est défectueux. Xserve RAID possède ainsi deux systèmes d'alimentation. Si l'un d'entre eux tombe en panne, le système continue malgré tout à fonctionner.
- Les périphériques de tierces parties d'équilibrage de la charge vous permettent de répartir la charge du réseau dans une grappe de serveurs et d'assurer ainsi l'extensibilité et la tolérance de pannes.

Ce chapitre traite du service de basculement IP et explique comment le configurer dans Mac OS X Server.

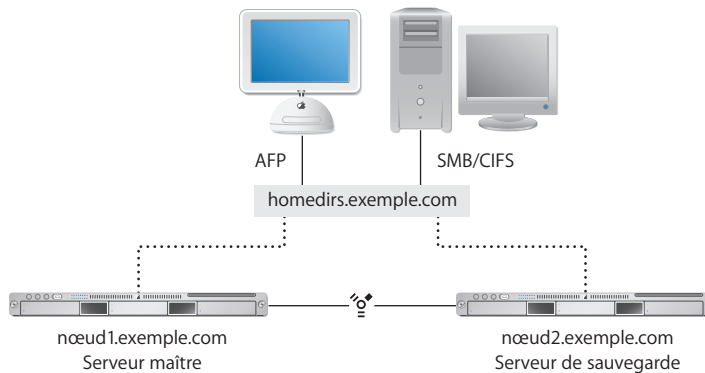
Le basculement IP est une technologie qui permet de configurer deux ordinateurs dans une relation maître-sauvegarde de sorte qu'en cas de panne de l'ordinateur maître, l'ordinateur de sauvegarde assume le rôle de l'ordinateur maître de façon transparente, avec une interruption minimale du service.

Par exemple, si vous avez un serveur de répertoires de départ doté de 1000 utilisateurs et ne possédez pas de serveur de sauvegarde, les utilisateurs ne pourront pas accéder à leurs fichiers en cas de panne du serveur. Mais si vous configurez un autre serveur en tant que serveur de sauvegarde, même en cas de panne du serveur maître, les utilisateurs pourront continuer à avoir accès à leurs fichiers via le serveur de sauvegarde, sans se rendre compte de l'interruption du service, dès lors que les données sont stockées sur un espace de stockage partagé accessible aux deux ordinateurs.

Mac OS X Server fournit une gestion intégrée du basculement IP. Dans ce chapitre, vous apprendrez comment le basculement IP fonctionne sous Mac OS X Server et comment le configurer.

Vue d'ensemble du basculement IP

Le basculement IP vous permet de garantir la haute disponibilité de vos serveurs. Une solution simple de basculement IP est possible avec deux ordinateurs Mac OS X Server : un ordinateur maître et un ordinateur de sauvegarde. L'ordinateur maître fournit des services tandis que l'ordinateur de sauvegarde attend en arrière-plan pour prendre le relais en cas de panne du maître.



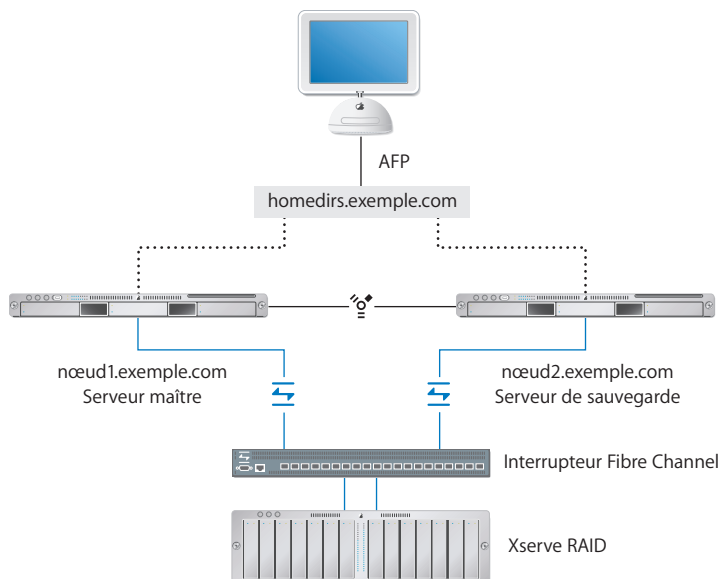
Dans ce scénario, les deux ordinateurs se connectent au même réseau que celui d'où proviennent les requêtes client. Chaque ordinateur a une adresse IP unique et éventuellement un nom de domaine ou DNS. Les ordinateurs sont directement connectés entre eux à l'aide d'IP via FireWire.

Pour assurer la gestion du basculement IP, Mac OS X Server utilise les daemons `heartbeatd` et `failoverd` :

- Le daemon `heartbeatd` est exécuté sur l'ordinateur maître et diffuse des battements de cœur toutes les secondes sur le port 1694 à partir des deux interfaces réseau, annonçant la disponibilité de l'hôte aux autres nœuds écoutant avec `failoverd`. L'envoi de battements de cœur sur les liens réseau primaire et secondaire permet d'éviter les fausses alarmes. `heartbeatd` utilise l'entrée `FAILOVER_BCAST_IPS` du fichier `/etc/hostconfig` pour déterminer à qui envoyer diffuser les battements de cœur.
- Le démon `failoverd` est exécuté sur l'ordinateur de sauvegarde et écoute le port 1694 pour repérer les diffusions provenant d'une adresse spécifique sur les deux interfaces. Dès l'instant que `failoverd` ne reçoit plus les battements de cœur sur les deux interfaces, il prend le contrôle de l'adresse IP publique du serveur maître, ce qui permet au serveur de basculement de répondre aux requêtes client entrantes, garantissant ainsi la disponibilité. `failoverd` utilise les entrées `FAILOVER_PEER_IP` et `FAILOVER_PEER_IP` du fichier `/etc/hostconfig` pour obtenir les adresses IP publique et privée du serveur maître.

Pour que le basculement IP fonctionne, vous devez maintenir la synchronisation de l'ordinateur de sauvegarde avec l'ordinateur maître. Par exemple, si vous utilisez l'ordinateur maître en tant que serveur de fichiers AFP, assurez-vous que l'ordinateur de sauvegarde ait les mêmes réglages de service AFP. Si ces réglages ne sont pas identiques, les utilisateurs risquent de ne pas pouvoir accéder au service de fichiers.

Pour garantir le fonctionnement du basculement IP, il faut également que l'ordinateur de sauvegarde puisse accéder aux données dont ont besoin les ordinateurs client. Pour assurer la disponibilité des données, vous devrez synchroniser les données des deux ordinateurs à l'aide des commandes `cron` et `rsync` ou d'autres solutions de tierces parties. Une autre possibilité consiste à utiliser des espaces de stockage partagés, tels que Xserve RAID, et à y stocker les données.



Pour tirer pleinement parti de Xserve RAID en cas de basculement IP, vous pouvez utiliser Xsan ou un logiciel de zone de stockage en réseau (SAN) de tierces parties grâce auquel vos serveurs maître et de sauvegarde pourront accéder au même volume sans le corrompre.

Vous pouvez également utiliser le masquage de numéro d'unité logique (LUN) au niveau Fibre Switch pour octroyer l'accès aux données partagées sur un Xserve RAID. Vous devrez créer des scripts pour indiquer à l'interrupteur de permuter l'accès entre un serveur et l'autre. Le masquage LUN au niveau interrupteur garantit qu'un seul serveur ait accès aux données, mais jamais les deux à la fois.

Avertissement : donner aux deux serveurs l'accès au même volume Xserve RAID sans Xsan ni logiciel SAN de tierces parties est susceptible de corrompre le volume.

Après avoir lancé les démons `heartbeatd` et `failoverd`, l'ordinateur maître commence à envoyer des battements de cœur au serveur de sauvegarde à intervalles réguliers. Dès lors que l'ordinateur de sauvegarde ne reçoit plus ces messages, il déclenche une chaîne d'événements au bout de laquelle le serveur de sauvegarde reprend l'adresse IP du serveur maître et assume le rôle de ce dernier.

Du point de vue du client, le basculement est transparent, avec une interruption minime du service. Cela est dû au fait que le client accède aux services à l'aide d'une adresse IP virtuelle (c'est-à-dire une adresse non associée à un ordinateur particulier) et/ou d'un nom de domaine virtuel (`homedirs.exemple.com` par exemple). Quand le serveur de sauvegarde assume le rôle du maître, le client ne remarque aucune différence tant que les services sont configurés de manière totalement identique sur les deux ordinateurs. Une brève interruption de service peut éventuellement être perceptible si le basculement IP a lieu alors que le client communique activement avec un service. Ainsi, si un utilisateur copie un fichier à partir d'un serveur et que ce dernier bascule, le processus de copie est interrompu et l'utilisateur doit alors recommencer le processus de copie depuis le début.

Acquisition d'une adresse maître — Chaîne d'événements

Lorsque le serveur maître bascule, la chaîne d'événements suivante a lieu sur le serveur de sauvegarde :

- 1 Le démon `failoverd` (situé dans `/usr/sbin/`) ne détecte aucune diffusion émanant du serveur primaire sur l'interface FireWire.
- 2 Le démon `failoverd` indique au script `NotifyFailover` (situé dans `/usr/libexec/`) d'envoyer des courriers électroniques aux utilisateurs répertoriés dans `/etc/hostconfig`. Si aucun destinataire n'est spécifié, un courrier électronique est envoyé à l'utilisateur racine.
- 3 `failoverd` exécute le script `ProcessFailover` (situé dans `/usr/libexec/`).
- 4 Le script `ProcessFailover` exécute le script `/Library/Failover/adresse_IP/Test`, où `adresse_IP` est l'adresse IP ou le nom de domaine du serveur maître.
 - a Si le script `Test` renvoie "faux", `ProcessFailover` quitte et le serveur de sauvegarde n'acquiert pas l'adresse IP du serveur maître.
 - b Si le script `Test` renvoie "vrai" (ou "n'existe pas"), `ProcessFailover` poursuit son exécution.

Remarque : par défaut, le script `Test` est vierge mais vous pouvez le personnaliser afin de l'adapter à vos besoins.

- 5 Le script `ProcessFailover` exécute, dans l'ordre alphabétique, tous les scripts portant le préfixe `PreAcq` dans le dossier `/Library/Failover/adresse_IP`.

Les scripts de type `PreAcq` préparent le serveur de sauvegarde à acquérir l'adresse IP du serveur maître. Par défaut, Mac OS X Server est fourni avec un certain nombre de scripts `PreAcq` mais vous pouvez toujours les personnaliser ou ajouter les vôtres.

- 6 Le script `ProcessFailover` configure l'interface réseau de sorte qu'elle utilise l'adresse IP du serveur maître.
- 7 Le script `ProcessFailover` exécute, dans l'ordre alphabétique, tous les scripts portant le préfixe `PostAcq` dans le dossier `/Library/Failover/adresse_IP`.

Les scripts `PostAcq` sont exécutés une fois que le serveur de sauvegarde a acquis l'adresse IP du maître. Tout comme c'est le cas avec les scripts `PreAcq`, Mac OS X Server est fourni avec un certain nombre de scripts de type `PostAcq`. Là aussi, vous pouvez ajouter les vôtres. Par exemple, un script `PostAcq` peut vous envoyer un courrier électronique afin de vous informer que le basculement a réussi.

Pour en savoir plus sur `failoverd`, `NotifyFailover` et `ProcessFailover`, consultez les pages correspondantes de ce manuel ou le chapitre portant sur la haute disponibilité du guide d'administration à l'aide de la ligne de commande.

Remarque : le basculement s'effectue en 30 secondes environ.

Libération d'une adresse maître — Chaîne d'événements

Voici ce qui se passe au niveau du serveur de sauvegarde lorsque vous déclenchez la restauration :

- 1 Le démon `failoverd` indique au script `NotifyFailover` (situé dans `/usr/libexec/`) d'envoyer des courriers électroniques aux utilisateurs répertoriés dans `/etc/hostconfig`. Si aucun destinataire n'est spécifié, un courrier électronique est envoyé à l'utilisateur racine.
- 2 `failoverd` exécute le script `ProcessFailover` (situé dans `/usr/libexec/`).
- 3 Le script `ProcessFailover` exécute le script `Test` (situé dans `/Library/Failover/adresse_IP`, où `adresse_IP` est l'adresse IP ou le nom de domaine du serveur maître).
 - a Si le script `Test` renvoie "faux", `ProcessFailover` se termine, et le serveur maître n'acquiert pas l'adresse IP du serveur de sauvegarde.
 - b Si le script `Test` renvoie "vrai" (ou "n'existe pas"), `ProcessFailover` poursuit son exécution.
- 4 Le script `ProcessFailover` exécute, dans l'ordre alphabétique, tous les scripts portant le préfixe `PreRel` dans le dossier `/Library/Failover/adresse_IP`.
- 5 Le script `ProcessFailover` libère l'adresse IP du serveur maître.
- 6 Le script `ProcessFailover` exécute, dans l'ordre alphabétique, tous les scripts portant le préfixe `PostRel` dans le dossier `/Library/Failover/adresse_IP`.

Remarque : par défaut, le script `Test` est vierge mais vous pouvez le personnaliser afin de l'adapter à vos besoins.

Configuration du basculement IP

Voici un aperçu de la marche à suivre pour configurer vos ordinateurs Mac OS X Server pour le basculement IP :

Étape 1 : Connectez les ordinateurs maître et de sauvegarde au même réseau et configurez leurs réglages TCP/IP

Cette étape permettra à vos serveurs de communiquer avec les ordinateurs client. Chaque serveur doit posséder sa propre adresse IP.

Étape 2 : Connectez directement les deux ordinateurs à l'aide d'une interface Ethernet secondaire ou IP via FireWire et configurez les réglages IP

Cette étape a pour but d'assurer la communication directe des événements de basculement IP entre les serveurs.

Étape 3 : Configurez et lancez le service de basculement IP sur les serveurs maître et de sauvegarde

Cette étape garantit le basculement et la restauration des ordinateurs maître et de sauvegarde.

Connexion des serveurs maître et de sauvegarde au même réseau

Pour configurer vos serveurs pour le basculement, la première chose à faire est de connecter les ordinateurs maître et de sauvegarde au même réseau et de configurer leurs réglages de réseau.

Pour connecter les serveurs maître et de sauvegarde au même réseau :

- 1 À l'aide de l'interface Ethernet primaire, connectez les serveurs maître et de sauvegarde au même réseau.
- 2 Dans la sous-fenêtre Réseau des Préférences Système, configurez les réglages TCP/IP des ordinateurs maître et de sauvegarde de sorte que chacun possède une adresse IP unique et que tous deux se trouvent sur le même sous-réseau.

Dans l'idéal, demandez à votre administrateur système de mapper l'adresse IP du serveur maître sur un nom DNS virtuel (homedirs.exemple.com par exemple) dont les utilisateurs pourront se servir pour se connecter à votre serveur. Cela vous permet ainsi de libérer l'adresse IP du serveur maître de façon transparente pour les utilisateurs.

Vous pouvez également mapper les adresses IP des serveurs maître et de sauvegarde sur des noms DNS (noeud1.exemple.com et noeud2.exemple.com, par exemple) que vous pourrez utiliser pour vous référer aux deux ordinateurs lors de la configuration du basculement IP.

Connexion des serveurs maître et de sauvegarde entre eux

Connectez entre eux les ordinateurs maître et de sauvegarde à l'aide d'une interface Ethernet secondaire ou d'IP via FireWire. Il s'agit là d'une étape importante car c'est par cette connexion que les deux ordinateurs communiquent les événements de basculement.

Pour connecter les serveurs maître et de sauvegarde entre eux :

- 1 Pour relier les ordinateurs maître et de sauvegarde ensemble, utilisez un câble Ethernet ou FireWire.
- 2 Dans la sous-fenêtre Réseau des Préférences Système, configurez les réglages TCP/IP de l'interface Ethernet secondaire ou de l'interface IP via FireWire sur les deux ordinateurs. Attribuez à chaque ordinateur une adresse IP de réseau privé (10.1.0.2 et 10.1.0.3, par exemple) et assurez-vous que tous deux se trouvent sur le même sous-réseau.

Configuration du serveur maître pour le basculement

Configurer un serveur maître pour le basculement IP est un jeu d'enfant. Il suffit en effet d'ajouter ou de modifier deux entrées dans le fichier `/etc/hostconfig`, puis de redémarrer le serveur.

Pour configurer le serveur maître pour le basculement IP :

- 1 Ajoutez ou modifiez l'entrée `FAILOVER_BCAST_IPS` dans `/etc/hostconfig` afin de spécifier les adresses auxquelles envoyer les messages de battements de cœur.

Par exemple, si l'adresse IP primaire du serveur maître est 171.0.50 et que l'adresse IP secondaire est 10.1.0.2, vous pouvez ajouter la ligne suivante à `/etc/hostconfig` afin de diffuser le message sur les deux réseaux :

```
FAILOVER_BCAST_IPS="10.1.0.255 17.1.0.255"
```

Mais votre commutateur réseau sera plus efficace s'il envoie les battements de cœur à des adresses spécifiques :

```
FAILOVER_BCAST_IPS="10.1.0.3 17.1.0.51"
```

Cette ligne ordonne au serveur maître d'envoyer les battements de cœur aux adresses IP primaire et secondaire du serveur de sauvegarde.

Remarque : pour modifier le fichier `/etc/hostconfig`, vous devez être l'utilisateur racine. Utilisez la commande `sudo` lorsque vous ouvrez ce fichier à l'aide de votre éditeur de lignes de commande favori.

- 2 Ajoutez ou modifiez l'entrée `FAILOVER_EMAIL_RECIPIENT` pour spécifier l'adresse électronique à laquelle envoyer les notifications.

Si vous n'ajoutez pas cette entrée, les notifications par courrier seront envoyées à l'utilisateur racine.

- 3 Redémarrez le serveur.

L'élément de démarrage `IPFailover` lance `heartbeatd` au cours du démarrage. Une fois le lancement effectué, `heartbeatd` contrôle sa liste d'arguments, se place en arrière-plan et envoie régulièrement des messages de "battements de cœur" aux adresses spécifiées dans l'entrée `FAILOVER_BCAST_IPS` de `/etc/hostconfig`.

Configuration du serveur de sauvegarde pour le basculement

Configurer le serveur de sauvegarde pour le basculement IP n'a rien de compliqué. Il suffit en effet d'ajouter ou de modifier deux entrées dans le fichier `/etc/hostconfig`, de déconnecter les serveurs maître et de sauvegarde, de redémarrer le serveur de sauvegarde et enfin de reconnecter les serveurs.

Pour configurer le serveur de sauvegarde pour le basculement IP :

- 1 Ajoutez ou modifiez l'entrée `FAILOVER_PEER_IP_PAIRS` dans `/etc/hostconfig` afin de spécifier l'adresse IP de l'interface réseau primaire sur le serveur maître.

Par exemple, si l'adresse IP de l'interface réseau primaire sur le serveur maître est 171.0.50, ajoutez l'entrée suivante :

```
FAILOVER_PEER_IP_PAIRS="en0:17.1.0.50"
```

Remarque : pour modifier le fichier `/etc/hostconfig`, vous devez être l'utilisateur racine. Utilisez la commande `sudo` lorsque vous ouvrez ce fichier à l'aide de votre éditeur de lignes de commande favori.

- 2 Ajoutez ou modifiez l'entrée `FAILOVER_PEER_IP` dans `/etc/hostconfig` afin de spécifier l'adresse IP de l'interface réseau secondaire sur le serveur maître.

Par exemple, si l'adresse IP du port FireWire sur le serveur maître est 10.1.0.2, ajoutez l'entrée suivante :

```
FAILOVER_PEER_IP="10.1.0.2"
```

- 3 Déconnectez la connexion directe entre le serveur de sauvegarde et le serveur maître.
Si vous utilisez IP via FireWire pour l'interface secondaire, déconnectez le câble FireWire reliant les deux ordinateurs.
- 4 Redémarrez le serveur de sauvegarde.
- 5 Une fois qu'il a redémarré, reconnectez-le au serveur primaire.

Consultation de l'historique Basculement IP

Mac OS X Server enregistre toute l'activité de basculement IP dans /Library/Logs/failoverd.log.

Pour consulter les historiques de service de basculement :

- 1 Ouvrez/Applications/Utilitaires/Console.
- 2 Sélectionnez Fichier > Ouvrir.
- 3 Localisez et sélectionnez l'historique failoverd.log dans le dossier /Library/Logs/.
- 4 Cliquez sur Ouvrir.

Vous pouvez utiliser le champ Filtre pour n'afficher que les entrées d'historique qui vous intéressent.

À partir de la ligne de commande

Vous pouvez également consulter le fichier failoverd.log à l'aide des commandes de Terminal. Pour automatiser le contrôle des historiques, pensez à utiliser `cron` et `grep` afin de chercher automatiquement des mots-clés liés au basculement IP dans les fichiers d'historique et envoyez ces entrées à votre adresse électronique. Pour en savoir plus, consultez le chapitre consacré au basculement IP du guide d'administration à l'aide de la ligne de commande.

Ce chapitre explique comment améliorer la disponibilité de vos solutions Mac OS X Server.

L'élimination de points de défaillance uniques et l'utilisation de Xserve et de Xserve RAID peuvent entre autres contribuer à augmenter la disponibilité de votre serveur. Vous pouvez aussi recourir à des options aussi bien simples, comme le recours à une alimentation de secours, le redémarrage automatique, la garantie de conditions de fonctionnement adéquates (niveaux de température et d'humidité adaptés par exemple), etc.), qu'avancées (agrégation de liens, équilibrage de charge, réplique Open Directory, sauvegarde de données, etc.).

Élimination de points de défaillance uniques

Pour améliorer la disponibilité de votre serveur, vous devez réduire ou éliminer les points de défaillance uniques. On qualifie de point de défaillance unique tout composant d'un environnement de serveur qui provoque la panne de ce dernier s'il est lui-même défaillant.

Voici quelques exemples de points de défaillance uniques :

- le système informatique ;
- le disque dur ;
- l'alimentation.

Comme il est pratiquement impossible d'éliminer tous les points de défaillance uniques, essayez au moins de les réduire autant que possible. Par exemple, l'utilisation d'un système de sauvegarde et du basculement IP dans Mac OS X Server, comme mentionné dans le chapitre 2, "Configuration du basculement IP", permet d'éliminer l'ordinateur en tant que point de défaillance unique. Les ordinateurs maître et de sauvegarde peuvent certes présenter une défaillance simultanément ou l'un après l'autre mais de telles probabilités sont négligeables.

Une autre manière d'éviter la défaillance d'un ordinateur est d'utiliser une source d'alimentation de sauvegarde et d'utiliser le RAID matériel pour mettre le disque dur en miroir. Avec le RAID matériel, si le disque principal est victime d'une défaillance, le système peut toujours accéder aux mêmes données sur le disque miroir, comme c'est le cas avec Xserve.

Utilisation de Xserve et de Xserve RAID

Xserve et Xserve RAID ont été conçus de façon à garantir une fiabilité élevée et donc une haute disponibilité.

Utilisation de Xserve

Les ordinateurs de bureau, tels que le Power Mac G5, permettent certes d'assurer des services Mac OS X Server très fiables, mais Xserve possède quelques fonctionnalités supplémentaires qui le rendent idéal dans les situations requérant une haute disponibilité.

Voici quelques-unes de ces fonctionnalités :

- Xserve comporte huit ventilateurs. En cas de panne de l'un de ces ventilateurs, les sept autres accélèrent pour compenser la défaillance et permettre à votre serveur de continuer à fonctionner.
- Une architecture de disques indépendante isole électriquement les disques de façon à empêcher que la défaillance d'un seul des disques n'entraîne une indisponibilité ou une dégradation des performances des disques restants, un problème souvent rencontré avec les implémentations SCSI multidisque.
- Xserve G5 se base sur la logique de code correcteur d'erreurs (ECC, Error Correction Code) pour protéger le système contre les données endommagées et les erreurs de transmission. Chaque DIMM possède un module de mémoire supplémentaire qui stocke les données de somme de contrôle de chaque transaction. Le contrôleur système se sert de ces données ECC pour identifier les erreurs portant sur un seul bit et les corrige à la volée, évitant ainsi des arrêts système inopinés. Dans le cas très rare d'une erreur portant sur plusieurs bits, le contrôleur système détecte l'erreur et déclenche une notification système afin d'empêcher les mauvaises données de corrompre d'autres opérations. Vous pouvez configurer le logiciel Contrôle de serveur de manière à ce qu'il vous avertisse si le taux d'erreurs dépasse le seuil défini.
- Xserve G5 intègre l'écriture miroir, qui protège votre serveur contre toute défaillance si le disque principal tombe en panne.

Pour plus d'informations sur Xserve RAID, consultez le site www.apple.com/fr/xserve/.

Utilisation de Xserve RAID

Xserve RAID vous offre un espace de stockage partagé extrêmement fiable idéal pour les solutions haute disponibilité et particulièrement pour celles impliquant le basculement IP.

Voici quelques-unes des fonctionnalités de fiabilité/haute disponibilité de Xserve RAID :

- Fond de panier central doté d'un chemin de données passif. L'architecture de Xserve RAID a été conçue pour éviter toute vulnérabilité liée à des points de défaillance uniques. Xserve RAID est construit autour d'un fond de panier central doté d'un chemin de données passif, une caractéristique peu commune aux autres systèmes de stockage de ce type. Le fond de panier central est le connecteur central reliant les disques, les contrôleurs RAID, les systèmes d'alimentation et les modules de refroidissement. La plupart des systèmes RAID dépendent du fond de panier central pour transmettre les ensembles de données et d'instructions entre les disques, et une panne de cette dernière peut compromettre la disponibilité des données. Dans Xserve RAID, toutes les données transitent par les canaux de transfert indépendants, qui sont maintenus simplement en place par le fond de panier central.
- Double contrôleur RAID indépendant. Deux processeurs de stockage indépendants gèrent les fonctions RAID, les transferts de données et la protection contre les pannes pour chaque ensemble de sept disques. Ces deux contrôleurs ne sont pas redondants mais vous permettent de mettre les données en miroir de sorte que la moitié de Xserve RAID constitue un miroir pour l'autre moitié. Si un contrôleur tombe en panne, vous pouvez toujours accéder aux données par le biais du second.
- Modules de refroidissement redondants à remplacement à chaud. Les deux modules de refroidissement redondants à remplacement à chaud assurent un refroidissement automatique de l'avant vers l'arrière pour les environnements de rack. Si un module tombe en panne, vous pouvez le remplacer sans avoir à éteindre le système.
- Systèmes d'alimentation. L'un des deux systèmes d'alimentation à répartition des charges et remplacement à chaud peut assurer l'alimentation de Xserve RAID si l'autre tombe en panne.
- Disques de secours. Pour chaque contrôleur RAID, tout disque non affecté à une matrice est automatiquement utilisé en tant que disque de secours global. Si un disque tombe en panne, le contrôleur RAID peut automatiquement reconstruire ses données sur le disque de secours sans que l'intervention de l'administrateur soit nécessaire. La reconstruction s'effectue en arrière-plan tandis que le contrôleur traite les lectures et écritures normales d'hôte, ce qui évite l'interruption du service. L'administrateur a ainsi largement le temps de remplacer le disque défectueux. Xserve RAID configure automatiquement le disque en tant que nouveau disque de secours de la matrice.

Pour plus d'informations sur Xserve RAID, consultez le site www.apple.com/fr/xserve/raid/.

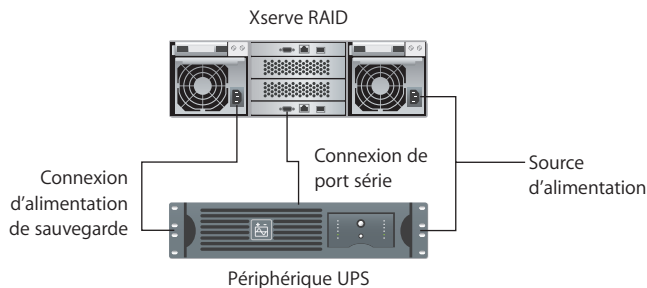
Utilisation de l'alimentation de secours

Dans l'architecture d'une solution de serveur, l'alimentation constitue un point de défaillance unique. Si l'alimentation est interrompue, vos serveurs s'éteignent sans prévenir. Pour éviter une interruption soudaine des services, envisagez l'ajout d'une source d'alimentation de sauvegarde. En fonction de votre application, vous pouvez choisir entre un générateur électrique de secours et un périphérique d'alimentation sans interruption (UPS), qui vous permettront au moins d'avoir assez de temps pour avertir les utilisateurs de l'interruption inopinée des services.

Utilisation d'UPS avec Xserve RAID

Xserve RAID assure un contrôle UPS intégré via son port série. La connexion de l'alimentation de Xserve RAID à un périphérique UPS peut s'effectuer par le biais du port série, ce qui permet à Xserve RAID de contrôler le périphérique UPS. Lorsque Xserve RAID détecte que l'alimentation fournie par le périphérique UPS est sur le point d'être épuisée, il fait automatiquement passer le mode cache de l'écriture différée haut débit à une écriture immédiate plus sûre. Ceci réduit le débit système global et donc la consommation d'énergie, en plus de protéger les transactions si l'alimentation fournie par le périphérique UPS s'épuise complètement.

Remarque : si vous utilisez un périphérique UPS APC (marque très populaire), Xserve RAID vous avertit par courrier électronique lorsque 20 % des réserves d'alimentation sont encore disponibles afin de vous donner tout le temps d'éteindre Xserve RAID.



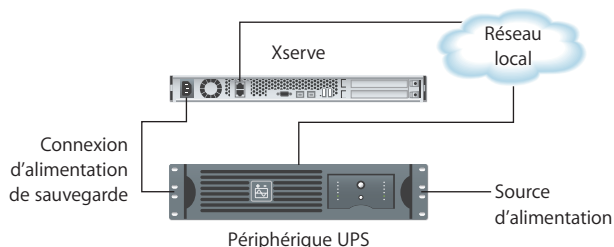
En plus d'un périphérique UPS, vous pouvez utiliser les batteries de sauvegarde de mémoire cache fournies en option avec Xserve RAID. Ces batteries conservent les données de transaction actuelles dans la mémoire cache pendant 72 heures au maximum, ce qui vous donne amplement le temps d'éteindre l'unité. Dès que vous rétablissez l'alimentation, Xserve RAID écrit sur le disque les transactions enregistrées dans le cache afin de garantir leur intégrité, puis commence à charger les batteries.

Tout en assurant le chargement des batteries de sauvegarde de la mémoire cache, Xserve RAID reste en mode écriture immédiate jusqu'à ce que plus de la moitié des batteries soit rechargée. Xserve RAID passe ensuite à nouveau en mode écriture différée.

Avertissement : si vous n'utilisez pas de périphérique UPS, désactivez le cache d'écriture de Xserve RAID (Xserve RAID opère une désactivation automatique lorsqu'il est connecté à un périphérique UPS) pour éviter toute perte de données. Les batteries de sauvegarde de la mémoire cache ne sauvegarderont que le cache de contrôleur, sans le cache d'écriture.

Utilisation d'UPS avec Xserve

Xserve n'assure pas la connectivité de port série aux périphériques UPS mais peut contrôler l'alimentation UPS via le réseau si l'unité UPS est équipée d'une carte réseau. Renseignez-vous auprès des fournisseurs de périphériques UPS pour en savoir plus.



Configuration du redémarrage automatique de votre serveur

Vous pouvez configurer les options Économiseur d'énergie de votre ordinateur Mac OS X Server afin que ce dernier redémarre automatiquement s'il s'éteint à cause d'une panne de courant ou en cas de blocage du système.



Les options de redémarrage automatique sont les suivantes :

- Redémarrage automatique après une panne de courant. L'unité de gestion de l'alimentation démarre le serveur automatiquement après une panne de courant.
- Redémarrage automatique si l'ordinateur "se bloque". L'unité de gestion de l'alimentation démarre automatiquement le serveur dès que le serveur ne répond plus, souffre d'une panique de noyau ou se bloque.

Lorsque vous sélectionnez l'option de redémarrage automatique après un "blocage", Mac OS X Server génère le démon `wdticklerd`, qui commande toutes les 30 secondes à votre ordinateur de redémarrer au bout de cinq minutes. À chaque fois que la commande est envoyée, la minuterie de redémarrage est réinitialisée. Ainsi, la minuterie n'atteint jamais cinq minutes tant que le serveur fonctionne. Mais si l'ordinateur se bloque, l'unité de gestion de l'alimentation le redémarre à l'issue des cinq minutes.

Pour activer le redémarrage automatique :

- 1 Ouvrez une session sur le serveur en tant qu'administrateur.
- 2 Ouvrez les Préférences Système et cliquez sur Économiseur d'énergie.
- 3 Cliquez sur Options.
- 4 Sous Autres options, sélectionnez les deux options de redémarrage.
- 5 Fermez les Préférences Système.

Pour de bonnes conditions de fonctionnement

La surchauffe est l'un des facteurs pouvant causer un dysfonctionnement de vos serveurs. Ce problème est particulièrement susceptible de survenir si vous regroupez des ordinateurs en grappe dans un espace réduit. D'autres facteurs, tels que l'humidité et les variations électriques importantes, peuvent être préjudiciables à votre serveur.

Pour protéger vos serveurs, vous devez veiller à les placer dans un endroit où vous pouvez contrôler ces facteurs et leur garantir des conditions de fonctionnement idéales. Pour connaître ces conditions, vérifiez quelles sont les consignes indiquées pour vos systèmes en matière d'électricité et d'environnement.

En outre, assurez-vous que le local dans lequel vous déployez votre serveur est équipé d'une alarme incendie, et établissez un plan de secours anti-incendie.

Réplique Open Directory

Si vous prévoyez de fournir des services Open Directory, vous devriez envisager de créer des répliques de votre maître Open Directory. Si le serveur maître est défectueux, les ordinateurs client pourront accéder à la réplique. Pour en savoir plus, consultez la section consacrée à la configuration de répliques Open Directory dans le guide d'administration Open Directory.

Protection de la sécurité d'un serveur

L'accès non autorisé d'attaquants constitue l'une des plus grandes menaces pour la disponibilité des serveurs.

Pour protéger vos serveurs contre des attaques de logiciel, procédez comme suit :

- **Activez le service de coupe-feu.** Le coupe-feu de votre serveur est sa première ligne de défense contre les accès non autorisés. Pour en savoir plus, consultez le chapitre consacré à la configuration du service de coupe-feu dans le guide d'administration des services réseau. Si votre serveur est particulièrement sujet aux attaques, envisagez l'achat d'un coupe-feu matériel de tierces parties comme ligne de défense supplémentaire.
- **Désactivez les services superflus.** L'activation d'un service ouvre un port à partir duquel les utilisateurs peuvent accéder à votre système. Si l'activation d'un service de coupe-feu contribue à repousser les accès non autorisés, un port ouvert constitue un point vulnérable dont un attaquant risque d'abuser.
- **Installez un logiciel antivirus.** Si les ordinateurs Mac sont beaucoup moins menacés par les virus que les ordinateurs Windows, les risques de contamination ne sont pas nuls.

- **Configurez des Listes de contrôle d'accès de service (SACL).** Servez-vous de ces listes pour spécifier qui peut accéder aux services.
- **Configurez des Listes de contrôle d'accès (ACL).** Servez-vous de ces listes pour contrôler qui peut accéder aux points de partage et à leur contenu.

Pour protéger votre matériel de serveur contre le vol ou le sabotage, respectez les consignes suivantes :

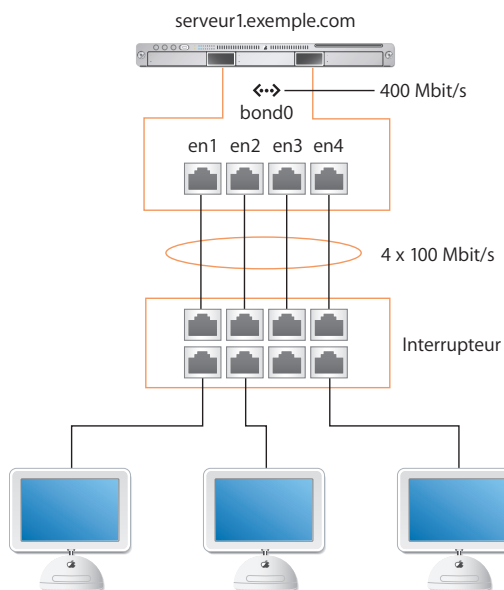
- Installez votre serveur dans un local sûr. Seul le personnel autorisé doit pouvoir y accéder.
- Administrez vos serveurs à distance. Assurez l'administration de vos serveurs à distance en vous servant d'applications telles que Admin Serveur, Contrôle de serveur, Admin RAID et Apple Remote Desktop. La réduction de l'accès physique aux systèmes limite les risques de mauvaises surprises.
- Utilisez des verrous de sécurité. Le verrouillage des systèmes est une autre mesure de sécurité à conseiller.

Agrégation de liens

Bien que peu fréquentes, les défaillances d'un interrupteur, d'un câble ou d'une interface réseau peuvent entraîner l'indisponibilité de votre serveur. Pour éliminer ce type de points de défaillance unique, vous pouvez utiliser l'agrégation de liens. Également appelée IEEE 802.3ad, cette technologie est intégrée à Mac OS X et à Mac OS X Server.

L'agrégation de liens consiste à agréger ou combiner dans un lien logique unique plusieurs liens physiques en connectant votre Mac à un périphérique d'agrégation de liens (un interrupteur ou un autre Mac). Le résultat est un lien à tolérance de pannes doté d'une bande passante égale à la somme des bandes passantes des liens physiques.

Par exemple, vous pouvez configurer un Xserve avec quatre ports 1 Gbit/s (en1, en2, en3 et en4) et utiliser la sous-fenêtre Réseau des Préférences Système pour créer une configuration de port d'agrégation de liens (bond0) combinant en1, en2, en3 et en4 en un seul lien logique. Le lien logique en résultant aura une bande passante de 4 Gbit/s. Ce lien offrira également une tolérance de pannes. Si un ou plusieurs liens physiques sont défectueux, la bande passante de votre Xserve rétrécira mais ce dernier pourra toujours gérer les requêtes dès lors que tous les liens physiques ne seront pas tous inopérants à la fois.



L'agrégation de liens vous permet également de tirer parti de votre matériel existant ou de matériel peu onéreux pour élargir la bande passante de votre serveur. Par exemple, vous pouvez former un agrégat de liens à partir d'une combinaison de plusieurs liens de 100 Mbit/s ou de liens de 1 Gbit/s.

Le protocole d'agrégation de liens (LACP, Link Aggregation Control Protocol)

L'agrégation de liens IEEE 802.3ad définit un protocole appelé protocole d'agrégation de liens (LACP, Link Aggregation Control Protocol) ; elle est utilisée par Mac OS X Server pour agréger (combinaison) plusieurs ports dans un agrégat de liens (un port virtuel) pouvant être utilisé pour les connexions TCP et UDP. Lorsque vous définissez un agrégat de liens, les nœuds situés de part et d'autre de ce dernier (un ordinateur et un interrupteur, par exemple) utilisent le protocole LACP sur chaque lien physique pour :

- déterminer si le lien peut être agrégé ;
- maintenir et contrôler l'agrégation.

Si un nœud ne reçoit pas régulièrement de paquets LACP de son homologue (l'autre nœud de l'agrégat), il considère que ce dernier n'est plus actif et supprime automatiquement le port de l'agrégat.

En plus de LACP, Mac OS X Server utilise un algorithme de distribution d'images pour mapper une "conversation" sur un port spécifique. Cet algorithme n'envoie de paquets au système situé à l'autre extrémité de l'agrégat que si la réception de paquets y est activée. En d'autres termes, l'algorithme n'envoie pas de paquets si l'autre système "n'écoute pas". Mapper une "conversation" sur un port en particulier garantit qu'aucune réorganisation de paquets n'aura lieu.

Scénarios d'agrégation de liens

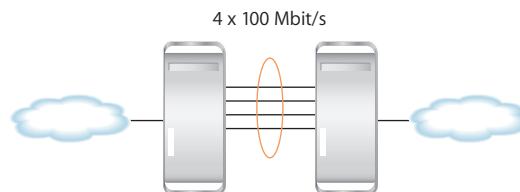
Voici trois scénarios courants d'agrégation qu'il est possible de configurer :

- Ordinateur-ordinateur
- Ordinateur-interrupteur
- Ordinateur-paire d'interrupteurs

Ces scénarios sont décrits dans les sections suivantes.

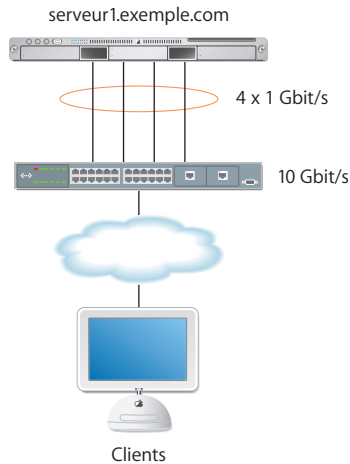
Ordinateur-ordinateur

Dans ce scénario, vous connectez directement les deux serveurs à l'aide des liens physiques de l'agrégat de liens. Cela permet aux deux serveurs de communiquer à une vitesse plus élevée sans l'aide d'un interrupteur. Cette configuration est idéale pour assurer la redondance dorsale.



Ordinateur-interrupteur

Dans ce scénario, vous connectez votre serveur à un interrupteur configuré pour l'agrégation de liens 802.3ad. L'interrupteur devra disposer d'une bande passante de traitement du trafic entrant égale ou plus importante que celle de l'agrégat de liens (lien logique) que vous définissez sur votre serveur.

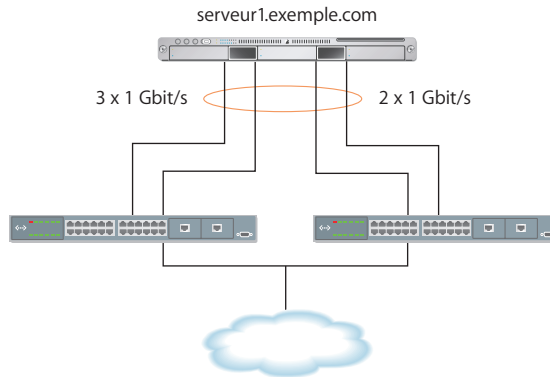


Par exemple, si vous créez un agrégat de quatre liens 1 Gbit/s, vous devrez utiliser un interrupteur pouvant traiter le trafic entrant (provenant de clients) à 4 Gbit/s ou plus. Faute de quoi, l'avantage que constitue une bande passante plus large dans l'agrégat de liens ne sera pas totalement accompli.

Remarque : pour en savoir plus sur la configuration de votre interrupteur pour l'agrégation de liens 802.3ad, reportez-vous à la documentation fournie par le fabricant de l'interrupteur.

Ordinateur-paire d'interrupteurs

Ce scénario constitue une version améliorée du scénario ordinateur-interrupteur puisque deux interrupteurs sont employés pour que l'interrupteur ne constitue plus un point de défaillance unique.



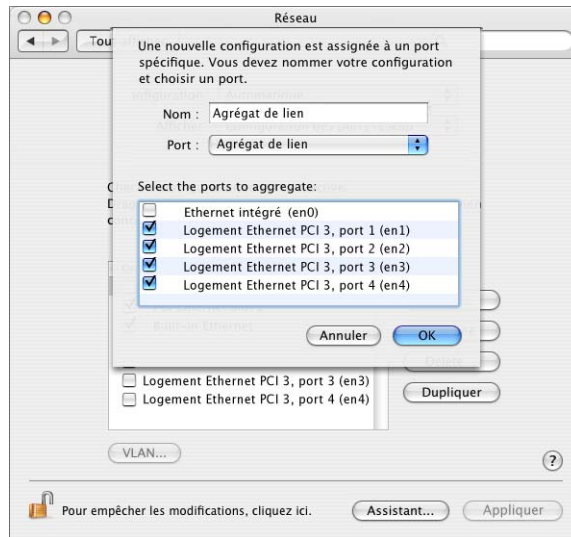
Par exemple, vous pouvez connecter deux liens de l'agrégat de liens sur l'interrupteur maître et le reste des liens sur l'interrupteur de sauvegarde. L'interrupteur de sauvegarde reste inactif tant que l'interrupteur maître est actif. Si ce dernier tombe en panne, l'interrupteur de sauvegarde prend le relais automatiquement et de façon transparente pour l'utilisateur.

Si ce scénario ajoute de la redondance, dont l'avantage est de protéger le serveur contre toute indisponibilité en cas de défaillance de l'interrupteur, il réduit en revanche la bande passante.

Configuration de l'agrégation de liens dans Mac OS X Server

Pour configurer votre Mac OS X Server pour l'agrégation de liens, vous devez disposer d'un Mac équipé d'au moins deux ports Ethernet compatibles IEEE 802.3ad. Vous devez également vous munir d'au moins un interrupteur compatible IEEE 802.3ad ou d'un autre ordinateur Mac OS X Server équipé du même nombre de ports.

Les agrégats de liens se créent sur votre ordinateur dans la sous-fenêtre Réseau des Préférences Système.



Pour créer un agrégat de liens :

- 1 Ouvrez une session sur le serveur en tant qu'utilisateur administrateur.
- 2 Ouvrez les Préférences Système.
- 3 Cliquez sur Réseau.
- 4 Choisissez "Configurations de port réseau" dans le menu local Afficher.
- 5 Cliquez sur Nouveau.
- 6 Choisissez Agrégat de liens dans le menu local Port.

Remarque : cette option n'apparaît que si vous disposez d'au moins deux interfaces Ethernet dans votre système.

- 7 Tapez le nom de l'agrégat de liens dans le champ Nom.
- 8 Sélectionnez les ports à agréger à partir de la liste.
- 9 Cliquez sur OK.
- 10 Cliquez sur Appliquer.

Par défaut, le système donne à l'agrégat de liens le nom d'interface bond<nbre>, où <nbre> est un nombre indiquant la priorité. Par exemple, le premier agrégat de liens sera appelé bond0, le deuxième bond1 et le troisième bond2.

Le nom d'interface `bond<nbre>` attribué par le système diffère du nom que vous donnez à la configuration de port d'agrégat de liens. Le nom d'interface est utilisé dans la ligne de commande tandis que le nom de la configuration de port est utilisé dans la sous-fenêtre réseau des Préférences Système.

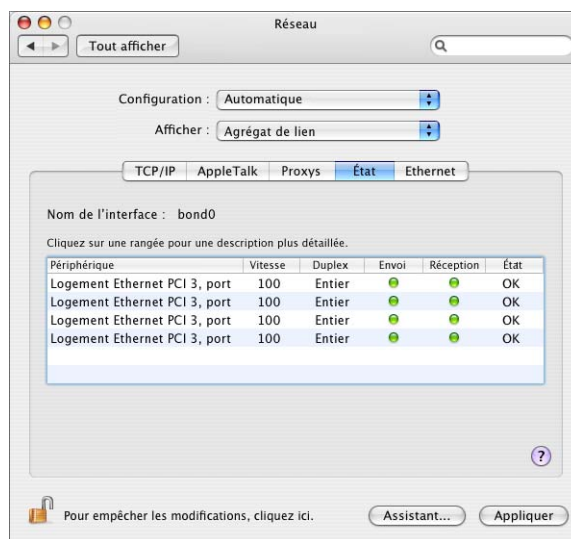
Par exemple, si vous saisissez la commande `ifconfig -a`, la sortie renvoie à l'agrégat de liens utilisant le nom d'interface et *non pas* au nom de la configuration de port :

...

```
bond0: flags=8843<UP,BROADCAST,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    inet6 fe80::2e0:edff:fe08:3ea6 prefixlen 64 scopeid 0xc
    inet 10.0.0.12 netmask 0xfffff00 broadcast 10.0.0.255
    ether 00:e0:ed:08:3e:a6
    media: autoselect (100baseTX <full-duplex>) status: active
    supported media: autoselect
    bond interfaces: en1 en2 en3 en4
```

Contrôle de l'état de l'agrégation de liens

Vous pouvez contrôler l'état d'un agrégat de liens dans Mac OS X et Mac OS X Server à l'aide de la sous-fenêtre État de la sous-fenêtre Réseau des Préférences Système.



Pour contrôler l'état d'un agrégat de liens :

- 1 Ouvrez les Préférences Système.
- 2 Cliquez sur Réseau.
- 3 Choisissez la configuration de port d'agrégat de liens dans le menu local Afficher.
- 4 Cliquez sur État.

La sous-fenêtre État affiche une liste dans laquelle une rangée est attribuée à chaque lien physique de l'agrégat de liens. Pour chaque lien, vous pouvez voir le nom de l'interface réseau, sa vitesse, son réglage de duplex, les témoins d'état du trafic entrant et sortant et une évaluation d'ensemble de l'état.

Remarque : les témoins d'état Envoi et Réception possèdent un code couleur. La couleur verte signifie que le lien est actif et connecté. La couleur jaune signifie que le lien est actif mais n'est pas connecté. La couleur rouge signifie que le lien ne peut ni envoyer ni recevoir de trafic.

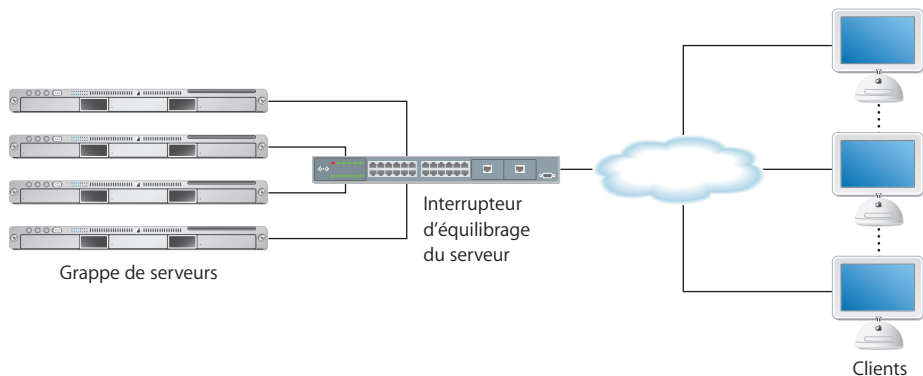
- 5 Pour consulter davantage d'informations à propos d'un lien, cliquez sur l'entrée correspondante dans la liste.

Équilibrage de la charge

La surcharge de serveur est l'un des facteurs pouvant entraîner l'indisponibilité de vos services. Un serveur a des ressources limitées et ne peut gérer qu'un nombre restreint de requêtes à la fois. Si le serveur est surchargé, il ralentit et risque même de se figer.

L'une des manières de résoudre ce problème est de répartir la charge au sein d'un groupe de serveurs (grappe de serveurs) à l'aide d'un périphérique d'équilibrage de la charge de tierces parties. Les clients envoient leurs requêtes au périphérique, qui les transmet au premier serveur disponible, une opération basée sur un algorithme prédéfini. Les clients ne voient qu'une adresse virtuelle unique, celle du périphérique d'équilibrage de la charge.

Nombreux sont les périphériques d'équilibrage de la charge qui font également office d'interrupteurs, offrant deux fonctions en une, ce qui réduit la quantité de matériel nécessaire.



Remarque : un périphérique d'équilibrage de la charge doit être capable de traiter le trafic agrégé (combiné) des serveurs qui y sont connectés. Sinon, le périphérique lui-même devient un goulet d'étranglement réduisant la disponibilité de vos serveurs.

L'équilibrage de la charge présente plusieurs avantages :

- **Haute disponibilité.** La répartition de la charge entre plusieurs serveurs contribue à réduire les risques qu'un serveur puisse tomber en panne du fait d'une surcharge de serveur.
- **Tolérance de pannes.** Si un serveur tombe en panne, le trafic est redirigé de façon transparente vers d'autres serveurs. Il pourra y avoir une brève interruption du service si, par exemple, un serveur tombe en panne alors qu'un utilisateur télécharge un fichier à partir du stockage partagé mais l'utilisateur pourra se reconnecter et relancer le processus de téléchargement de fichier.
- **Extensibilité.** Si la demande de services augmente, vous pouvez ajouter d'autres serveurs à votre grappe de façon transparente.
- **Performances accrues.** Vous pouvez répondre plus rapidement aux requêtes des utilisateurs en les envoyant aux serveurs les moins occupés.

Sauvegarde

Une défaillance de serveur ou une perte de données est parfois inévitable. Mais vous pouvez sauvegarder vos données importantes afin de pouvoir si nécessaire restaurer votre serveur en un minimum de temps.

Développement d'une stratégie de sauvegarde

Une bonne stratégie de sauvegarde est complète et tient compte de tous les aspects garantissant une récupération de données réussie. Une stratégie de sauvegarde complète inclut :

- la définition de l'étendue de la sauvegarde ;
- le choix d'une méthode sauvegarde ;
- le choix d'un schéma de rotation ;
- le choix du type de support ;
- la définition d'un mécanisme de vérification de sauvegarde.

Définition de l'étendue de la sauvegarde

Avant de déterminer le meilleur moyen de sauvegarder et restaurer les données, vous devez définir ce que vous souhaitez sauvegarder. À cette fin, vous pouvez par exemple créer une image d'un système entier. Ainsi, si le système principal tombe en panne, vous pourrez restaurer le système à partir de l'image au lieu d'avoir à restaurer des fichiers spécifiques éparpillés à l'intérieur. Il est des cas pourtant où seuls certains fichiers, par exemple les répertoires de départ ou les fichiers de configuration, doivent être sauvegardés.

Que vous souhaitiez sauvegarder un système entier ou seulement un petit ensemble de fichiers, la définition de l'étendue de la sauvegarde vous aidera à déterminer la quantité d'espace de sauvegarde et la fréquence des sauvegardes. Les données qui changent fréquemment doivent être sauvegardées plus souvent que celles qui ne changent qu'une ou deux fois par mois.

Choix d'une méthode sauvegarde

La méthode de sauvegarde définit ce que vous sauvegardez. Il existe trois méthodes de sauvegarde courantes :

- **Sauvegarde totale.** Dans le cadre d'une sauvegarde totale, vous copiez tous les fichiers, même ceux qui n'ont pas changé depuis la dernière sauvegarde. Les procédures de sauvegarde et de restauration sont simples mais la quantité d'espace de stockage nécessaire est élevée.
- **Sauvegarde différentielle.** Vous commencez par une sauvegarde totale puis ne sauvegardez que les fichiers qui ont changé depuis la sauvegarde "totale". Cela signifie qu'un fichier qui n'a changé qu'une fois depuis la sauvegarde totale sera sauvegardé à chaque fois que vous opérerez une sauvegarde différentielle, même s'il n'a pas changé depuis. Les procédures de sauvegarde et de restauration sont complexes car elles exigent de déterminer quels fichiers ont changé mais la quantité d'espace de stockage nécessaire est moyenne.
- **Sauvegarde incrémentielle.** Vous commencez par une sauvegarde totale puis ne sauvegardez que les fichiers qui ont changé depuis la dernière sauvegarde. Cette méthode est celle qui exige le moins d'espace de stockage mais, à l'instar de la sauvegarde différentielle, elle est plus complexe que la méthode de sauvegarde totale.

Choix d'un schéma de rotation de sauvegarde

Les schémas de rotation de sauvegarde déterminent la méthode la plus efficace de sauvegarde de données sur une période donnée. Un exemple de schéma de rotation est celui du grand-père / père / fils : selon ce schéma, vous procédez à des sauvegardes incrémentielles quotidiennes (fils), hebdomadaire totale (père) et mensuelle (grand-père).

Dans le schéma de rotation grand-père / père / fils, le nombre d'ensembles de données que vous utilisez par sauvegarde détermine la quantité d'historique de sauvegarde dont vous disposez. Par exemple, si vous utilisez huit ensembles de sauvegarde pour les sauvegardes quotidiennes, vous avez huit jours d'historique de sauvegarde hebdomadaire étant donné que vous recyclez les ensembles de données tous les huit jours.

Choix du type de support

Plusieurs aspects doivent être pris en compte lors du choix du type de support :

- **Coût.** Votre choix de support est fonction du coût par giga-octet. Par exemple, si vos besoins en stockage sont limités, vous pouvez justifier un coût par giga-octet plus élevé. Mais si vous avez besoin d'une grande quantité d'espace de stockage, le coût devient un facteur décisif dans votre décision. L'une des solutions de stockage les plus économiques est celle offerte par Xserve RAID. Elle vous garantit un faible coût par giga-octet sans exiger le traitement spécial requis par d'autres types de stockage économiques tels que les bandes magnétiques.

- **Capacité.** Si vous ne sauvegardez qu'une petite quantité de données, un support de stockage de faible capacité fera l'affaire. Mais si vous avez besoin de sauvegarder de grandes quantités de données, utilisez des périphériques de haute capacité tels que Xserve RAID.
- **Vitesse.** Lorsque votre objectif est de rendre votre serveur disponible la majorité du temps, la vitesse de restauration devient un facteur déterminant pour le choix du support. Les systèmes de sauvegarde sur bande magnétique peuvent être très économiques mais leur vitesse est nettement inférieure à celle de Xserve RAID.
- **Fiabilité.** Une rotation réussie est l'objectif de toute bonne stratégie de sauvegarde. Si vous ne pouvez pas restaurer les données perdues, les efforts et l'argent que vous aurez investis dans la sauvegarde des données seront gâchés, et la disponibilité de vos services sera compromise. Pour éviter la perte de données, il est donc essentiel que vous choisissiez un support très fiable. Les bandes magnétiques sont en ce sens plus sûres que les disques durs car elles ne contiennent pas de pièces mobiles.
- **Durée de vie des archives.** Vous ne pouvez jamais savoir quand vous aurez besoin des données sauvegardées. Vous devez donc choisir un support conçu pour résister pendant longtemps. Certains facteurs, tels que la poussière et l'humidité, peuvent endommager les supports de stockage et entraîner la perte de données.

Définition d'un mécanisme de vérification de sauvegarde

Une sauvegarde n'a pas d'intérêt si vous ne pouvez pas l'utiliser pour restaurer des données perdues. Nous vous conseillons d'avoir une stratégie de restaurations test régulières. Certains fournisseurs de logiciels de tierces parties gèrent cette fonctionnalité. Mais si vous utilisez vos propres solutions de sauvegarde, vous devrez développer les procédures de test nécessaires.

Outils de ligne de commande de restauration et de sauvegarde

Mac OS X Server fournit plusieurs outils de ligne de commande de sauvegarde et restauration de données :

- `rsync`. Utilisez cette commande pour conserver une copie de sauvegarde de vos données synchronisée avec l'original. `rsync` ne copie que les fichiers qui ont changé et ne copie pas les fichiers de ressources.
- `ditto`. Utilisez cette commande pour exécuter des sauvegardes totales.
- `asr`. Utilisez cette commande pour sauvegarder et restaurer un volume entier.

Pour en savoir plus sur ces commandes, reportez-vous au guide d'administration à l'aide de la ligne de commande.

Remarque : vous pouvez utiliser la commande `cron` pour automatiser la sauvegarde des données à l'aide des commandes sus-mentionnées. Pour en savoir plus sur l'utilisation de `cron`, reportez-vous au guide d'administration à l'aide de la ligne de commande.

Un contrôle efficace vous permet de détecter les problèmes potentiels avant leur apparition et d'en être averti suffisamment tôt lorsqu'ils se concrétisent.

La détection des problèmes potentiels vous permet de prendre les mesures nécessaires pour les résoudre avant qu'ils n'influencent la disponibilité de vos serveurs. De plus, être averti tôt de l'apparition d'un problème vous permet de prendre rapidement les mesures qui s'imposent et de réduire l'interruption des services.

Ce chapitre décrit brièvement les outils de contrôle disponibles et vous indique où trouver des informations supplémentaires :

- Console
- Contrôle de serveur
- Admin RAID
- Outils de contrôle de disque
- Outils de contrôle de réseau

Console

Utilisez Console pour contrôler les fichiers d'historique pouvant révéler d'éventuels problèmes susceptibles de provoquer la défaillance de votre serveur.

Par exemple, vous pouvez contrôler le fichier `/var/log/httpd/access_log` de votre serveur Web à la recherche de signes de déni d'attaques de service. Si vous détectez ces signes, vous pouvez immédiatement mettre en œuvre une réponse préplanifiée afin d'empêcher l'indisponibilité de votre serveur Web.

Pour améliorer l'efficacité de votre contrôle des fichiers d'historique, envisagez de l'automatiser à l'aide des commandes AppleScript ou Terminal telles que `grep` et `cron`. Reportez-vous au guide d'administration à l'aide de la ligne de commande pour en savoir plus sur l'utilisation de `grep` et `cron`.

Contrôle de serveur

Dès qu'elle détecte des problèmes critiques, l'application Contrôle de serveur peut émettre des avertissements via courrier électronique, téléphone portable ou notification par récepteur. Des capteurs intégrés détectent les facteurs de fonctionnement essentiels tels que l'alimentation, la température et l'état de fonctionnement de plusieurs composants clés, et en établissent le rapport.

L'interface utilisateur Contrôle de serveur vous donne la possibilité de détecter rapidement les problèmes. Dans la fenêtre principale, Contrôle de serveur répertorie sur une ligne séparée chaque serveur ainsi que les informations de température correspondantes et l'état de ses composants : ventilateurs, disques, modules de mémoire, systèmes d'alimentation et connexions Ethernet. Le témoin d'état vert indique que le composant est OK, le témoin jaune signale un avertissement et le témoin rouge est synonyme d'erreur.

Pour en savoir plus sur Contrôle de serveur, choisissez Aide Contrôle de serveur dans le menu d'Aide de Contrôle de serveur.

Admin RAID

Comme avec Contrôle de serveur, vous pouvez configurer Admin RAID de façon à ce qu'il vous envoie un courrier électronique ou une page lorsqu'un composant est en difficulté. Admin RAID affiche l'état de chaque unité et de chacun de ses composants, disques, fibre channel et connexions réseau notamment. Admin RAID utilise des témoins d'état verts, jaunes et rouges. Vous pouvez également le configurer de façon à ce qu'il vous envoie un courrier électronique ou une page lorsqu'un composant est en difficulté.

Pour en savoir plus sur Admin RAID, choisissez Aide Admin RAID dans le menu d'Aide d'Admin RAID.

De plus, Admin RAID vous fournit une vue d'ensemble de l'état des unités Xserve RAID apparaissant dans la fenêtre principale.

Outils de contrôle de disque

Si votre espace disque est épuisé, votre serveur risque de ne plus être fiable et il tombera probablement en panne. Pour empêcher un tel désagrément, vous devez contrôler constamment l'utilisation de l'espace disque sur vos serveurs et supprimer ou sauvegarder des fichiers afin de libérer de l'espace.

Mac OS X Server est fourni avec de nombreux outils de ligne de commande que vous pouvez utiliser pour contrôler l'espace disque sur votre ordinateur :

- **df.** Cette commande vous indique la quantité d'espace utilisée et la quantité disponible sur chaque volume monté.
Par exemple, la commande suivante répertorie les volumes locaux et affiche l'utilisation des disques sous un format utilisateur :

```
df -Hl
Filesystem      Size  Used Avail Capacity  Mounted on
/dev/disk0s9    40G   38G   2.1G    95%      /
```

Dans cet exemple, le disque dur est presque rempli puisque seuls 2,1 Go sont encore disponibles. Il serait donc bon que vous réagissiez immédiatement afin de libérer de l'espace sur votre disque dur avant que sa capacité ne soit dépassée et que cela n'entraîne des problèmes pour vos utilisateurs.

- **du.** Cette commande vous indique la quantité utilisée par des répertoires ou fichiers donnés.

Par exemple, la commande suivante vous indique la quantité d'espace occupée par le répertoire de départ de chaque utilisateur :

```
sudo du -sh /Users/*
3.2M   /Users/Shared
9.3M   /Users/omar
8.8M   /Users/jay
1.6M   /Users/lili
...
```

En sachant qui consomme le plus d'espace sur le disque dur, vous pouvez contacter les utilisateurs concernés par courrier électronique pour leur demander de supprimer les fichiers dont ils n'ont pas l'utilité.

Remarque : avec Gestionnaire de groupe de travail, vous pouvez définir des quotas de disque pour les utilisateurs et générer des rapports d'utilisation des disques. Reportez-vous au guide de gestion des utilisateurs pour en savoir plus.

- **diskspacemonitor.** Cette commande vous permet d'automatiser le processus de contrôle de l'utilisation de l'espace disque. Dès que la quantité d'espace libre descend en-dessous du niveau que vous avez spécifié, `diskspacemonitor` exécute des scripts shell qui vous envoient une notification. Cette commande définit deux niveaux d'action :
 - **Alerte :** vous envoie un message d'avertissement lorsque l'utilisation de l'espace disque atteint 75 %.
 - **Récupération :** archive les fichiers rarement utilisés et supprime les fichiers superflus lorsque l'utilisation de l'espace disque atteint 85 %.

Pour en savoir plus sur ces commandes, consultez les pages correspondantes de ce manuel ou le chapitre portant sur la haute disponibilité du guide d'administration à l'aide de la ligne de commande.

Outils de contrôle de réseau

Une dégradation des performances de réseau et d'autres problèmes de réseau peuvent avoir un impact négatif sur la disponibilité de vos services. Plusieurs outils de contrôle réseau peuvent vous avertir suffisamment tôt d'éventuels problèmes afin que vous puissiez prendre les mesures nécessaires pour éviter ou réduire la durée de la panne.

- Pour contrôler l'activité du réseau, vous pouvez utiliser l'utilitaire `tcpdump` de Mac OS X Server. Cet utilitaire imprime les en-têtes des paquets entrants et sortants sur une interface réseau qui concorde avec les paramètres spécifiés.
- L'utilisation de `tcpdump` pour contrôler le trafic sur le réseau est particulièrement judicieuse lorsque l'on tente de détecter des dénis d'attaque de service. Par exemple, la commande suivante contrôle l'ensemble du trafic entrant au niveau du port 80 de votre ordinateur :

```
sudo tcpdump -i en0 dst port 80
```

Si vous détectez un nombre inhabituel de requêtes émanant d'une même source, vous pouvez utiliser le service de coupe-feu pour bloquer l'ensemble du trafic de cette dernière.

Pour en savoir plus sur `tcpdump`, consultez les pages correspondantes de ce manuel ou le chapitre portant sur la haute disponibilité du guide d'administration à l'aide de la ligne de commande.

- Utiliser `tcpdump` pour contrôler le trafic peut prendre du temps. C'est pourquoi nous vous recommandons d'utiliser des AppleScripts ou des scripts shell pour automatiser le processus de contrôle.
- Envisagez également l'utilisation d'Ethereal, un outil Open Source X11 de reniflage de paquets qu'il est possible d'exécuter dans l'environnement X11 sous Mac OS X Server. À la différence de `tcpdump`, cet outil possède une interface utilisateur graphique et un ensemble d'outils performants d'analyse de réseau.
Pour en savoir plus sur Ethereal, rendez-vous sur le site www.ethereal.com/.
- En complément, vous pouvez utiliser d'autres outils de tierces parties qui analysent automatiquement le trafic sur le réseau et vous avertissent des problèmes.

Essayez les solutions suggérées ici pour résoudre ou éviter les problèmes de basculement lors de la configuration ou de l'utilisation du service de basculement.

Le service ne bascule pas automatiquement lorsque le service primaire est indisponible

- Vérifiez que le numéro de série du logiciel du serveur a été saisi correctement et n'a pas expiré. Pour vérifier ce numéro, ouvrez Admin Serveur, sélectionnez le serveur dans la liste Ordinateurs et services, puis cliquez sur Vue d'ensemble. Pour saisir un numéro de série mis à jour, cliquez sur Réglages.
- Vérifiez le fichier d'historique du basculement IP (/Library/Logs/failoverd.log) afin d'y trouver des indications à propos du problème.
- Assurez-vous que les câbles sont correctement reliés aux composants matériels.
- Vérifiez que les réglages réseau sont correctement configurés sur le serveur maître et sur le serveur de sauvegarde.
- Vérifiez que l'entrée `FAILOVER_BCAST_IPS` du fichier `/etc/hostconfig` est correctement configurée sur le serveur maître.
- Vérifiez que les entrées `FAILOVER_PEER_IP_PAIRS` et `FAILOVER_PEER_IP` du fichier `/etc/hostconfig` sont correctement configurées sur le serveur de sauvegarde.

Un destinataire de courriers électroniques ne reçoit pas de notifications

- Vérifiez que les adresses électroniques spécifiées par l'entrée `FAILOVER_EMAIL_RECIPIENT` du fichier `/etc/hostconfig` sont correctes.
- Assurez-vous que votre interface réseau publique fonctionne.
- Assurez-vous que vous avez correctement configuré le basculement IP.

La basculement a bien eu lieu mais les problèmes persistent

- Veillez à éteindre le serveur maître après le basculement.

adaptateur Ethernet Adaptateur permettant de connecter un périphérique à un réseau Ethernet. Généralement appelé carte Ethernet ou carte réseau Ethernet.

administrateur Utilisateur disposant d'autorisations d'administration de serveur ou de domaine de répertoires. Les administrateurs sont toujours membres du groupe "admin" prédéfini.

adresse Nombre ou tout autre identifiant identifiant de façon unique un ordinateur sur un réseau, un bloc de données stockées sur un disque, ou un emplacement de la mémoire d'un ordinateur. Voir aussi **adresse IP**.

adresse IP Adresse numérique unique qui identifie un ordinateur sur Internet.

AFP Apple Filing Protocol. Protocole client/serveur utilisé par le service de fichiers Apple sur les ordinateurs compatibles Macintosh pour partager des services de fichiers et de réseau. AFP utilise TCP/IP et d'autres protocoles pour les communications entre ordinateurs d'un réseau.

agrégation Combinaison d'objets ou de ressources similaires (disques ou connexions réseau, par exemple) dans une unique ressource logique, le but étant d'atteindre de meilleures performances. Par exemple, deux disques ou plus peuvent être agrégés dans un disque logique unique afin d'obtenir un volume unique de plus grande capacité.

agrégation de liens Configuration de plusieurs liens réseau physiques en un lien logique unique, le but étant d'améliorer la capacité et la disponibilité des connexions réseau. Avec l'agrégation de liens, le même identifiant est attribué à tous les ports. À comparer au **multi-acheminement**, dans lequel chaque port conserve sa propre adresse.

Apple Filing Protocol Voir AFP.

AppleScript Langage de script à la syntaxe proche de l'anglais utilisable pour écrire des fichiers de scripts pouvant contrôler votre ordinateur. AppleScript fait partie du système d'exploitation Mac et est intégré à chaque ordinateur Macintosh.

attaque par déni de service Voir **attaque par DoS**.

attaque par DoS Attaque par déni de service. Attaque Internet utilisant des milliers de pings réseau pour empêcher l'utilisation légitime d'un serveur.

bande passante Capacité d'une connexion réseau, mesurée en bits par seconde ou en octets par seconde, pour le transfert de données.

basculement automatique Basculement qui a lieu sans intervention humaine.

bit Unité d'information unique de valeur égale à 0 ou 1.

client Ordinateur (ou utilisateur de l'ordinateur) qui demande des données ou des services auprès d'un autre ordinateur ou d'un serveur.

Common Internet File System Voir SMB/CIFS.

connecté Qualifie des données, périphériques ou connexions réseau disponibles pour être utilisés immédiatement.

daemon Programme exécuté en arrière-plan et qui fournit d'importants services système tels que le traitement du courrier électronique entrant ou la gestion des requêtes provenant du réseau.

débit Quantité d'informations transmises par seconde.

débit Vitesse à laquelle les bits sont transmis sur un réseau, habituellement exprimée en bits par seconde.

déconnecté Qualifie des données qui ne sont pas immédiatement disponibles ou des périphériques physiquement connectés mais dont l'utilisation n'est pas disponible.

déni de service Voir **attaque par DoS**.

déployer Consiste à placer des systèmes informatiques configurés dans un environnement spécifique ou à rendre leur utilisation disponible dans cet environnement.

disponibilité Durée pendant laquelle un système est disponible durant les périodes où il est censé être disponible. Voir aussi **haute disponibilité**.

disque Périphérique réinscriptible de stockage de données.

disque de secours Disque de secours qui fonctionne et est prêt à être inscrit, et auquel un système RAID peut avoir recours instantanément en remplacement d'un disque défectueux.

DNS Domain Name System. Base de données distribuée qui fait correspondre des adresses IP à des noms de domaines. Un serveur DNS, appelé également serveur de noms, conserve la liste des noms et des adresses IP associées à chaque nom.

Domain Name System Voir **DNS**.

domaine Partie du nom de domaine d'un ordinateur sur Internet. N'inclut pas la désignation du domaine de premier niveau (par exemple, .com, .net, .us, .uk). Le nom de domaine "www.exemple.com" est constitué du sous-domaine ou nom d'hôte "www", du domaine "exemple" et du domaine de premier niveau "com".

domaine DNS Nom unique d'un ordinateur, utilisé dans le système DNS (Domain Name System) pour convertir les adresses IP et les noms. Également appelé **nom de domaine**.

en miroir Renvoie à une matrice de disques qui utilise RAID 1, ou la mise en miroir.

équilibrage de la charge Processus qui consiste à répartir sur plusieurs services les demandes de services réseau effectuées par les ordinateurs clients, afin d'optimiser les performances.

Ethernet Technologie de mise en réseau locale avec laquelle les données sont transmises sous forme d'unités appelées paquets à l'aide de protocoles tels que TCP/IP.

Fibre Channel Architecture sur laquelle la plupart des implémentations SAN sont construites. Fibre Channel est une norme technologique qui permet aux données d'être transférées d'un nœud réseau à l'autre à des vitesses très élevées.

Gigabit Ethernet Groupe de normes Ethernet avec lesquelles les données sont transmises à raison d'1 gigabit par seconde (Gbit/s). Abréviation : GBE.

gigaoctet Voir **Go**.

Go Gigaoctet. 1 073 741 824 (2³⁰) octets.

grappe Ensemble d'ordinateurs interconnectés afin d'améliorer la fiabilité, la disponibilité et les performances. Les ordinateurs regroupés en grappe exécutent souvent des logiciels spéciaux afin de coordonner leurs activités. Voir aussi **grappe informatique**.

grappe informatique Groupe d'ordinateurs ou de serveurs réunis pour partager le traitement d'une tâche à un haut niveau de performances. Une grappe informatique peut assumer des tâches bien plus importantes qu'un seul ordinateur et un tel groupe d'ordinateurs (ou de "nœuds") peut atteindre des performances élevées comparables à celles d'un superordinateur.

haute disponibilité Capacité d'un système à fonctionner en continu (sans interruption).

HTTP Hypertext Transfer Protocol. Protocole client/serveur pour le Web. Le protocole HTTP constitue pour un navigateur Web un moyen d'accès à un serveur Web et de requête de documents hypermedia HTML.

Hypertext Transfer Protocol Voir **HTTP**.

image Voir **image disque**.

image disque Fichier qui, une fois ouvert, crée sur un bureau Mac OS une icône dont la présentation et le comportement sont similaires à ceux d'un véritable disque ou volume. Les ordinateurs clients peuvent, à l'aide de NetBoot, démarrer via le réseau à partir d'une image disque basée sur un serveur et contenant un logiciel système. Les fichiers d'image disque présentent l'extension .img ou .dmg. Les deux formats d'image sont similaires et sont représentés par la même icône dans le Finder. Le format .dmg ne peut pas être utilisé sur les ordinateurs qui exécutent Mac OS 9.

interface de ligne de commande Manière d'interfacer avec l'ordinateur (par exemple, pour exécuter des programmes ou modifier des autorisations de système de fichiers) en saisissant des commandes de texte à une invite de shell.

interface réseau Connexion matérielle de votre ordinateur à un réseau. Les connexions Ethernet, les cartes AirPort et les connexions FireWire en sont des exemples.

Internet Ensemble de réseaux d'ordinateurs interconnectés, qui communiquent via un protocole commun (TCP/IP). Internet (notez la majuscule) est le système public le plus étendu au monde de réseaux d'ordinateurs interconnectés.

Internet Protocol Voir **IP**.

interrupteur Matériel de mise en réseau qui connecte plusieurs nœuds (ou ordinateurs) entre eux. Les interrupteurs sont utilisés avec la mise en réseau Ethernet et Fibre Channel afin d'assurer des connexions rapides entre les périphériques.

IP Internet Protocol. Également désigné par IPv4. Méthode utilisée conjointement avec le protocole TCP (Transmission Control Protocol) pour envoyer des données d'un ordinateur à un autre via un réseau local ou via Internet. Le protocole IP envoie les paquets de données, alors que le protocole TCP se charge de leur suivi.

kilo-octet Voir **Ko**.

Ko Kilo-octet. 1 024 (2¹⁰) octets.

lien Connexion physique active (électrique ou optique) entre deux nœuds d'un réseau.

logical unit number Voir **LUN**.

LUN Logical unit number. Identifiant SCSI d'un périphérique de stockage logique. Sous Xsan, un périphérique de stockage logique non formaté tel qu'une tranche ou une matrice Xserve RAID.

Mac OS X La dernière version du système d'exploitation d'Apple. Mac OS X allie la fiabilité d'UNIX à la facilité d'emploi de Macintosh.

Mac OS X Server Plate-forme de serveur puissante, capable de gérer immédiatement les clients Mac, Windows, UNIX et Linux et offrant un ensemble de services de réseau et de groupes de travail extensible, ainsi que des outils perfectionnés de gestion à distance.

mappage LUN Moyen d'éviter des inscriptions simultanées sur une matrice en attribuant un LUN spécifique à un ordinateur hôte unique. Le mappage LUN a lieu au niveau RAID. À comparer avec le masquage LUN.

masquage LUN Moyen d'éviter des inscriptions simultanées sur une matrice en "cachant" ou masquant l'accès à un LUN aux ordinateurs hôte indésirables dans une zone spécifique. Le masquage LUN s'effectue au niveau de l'interrupteur Fibre Channel. À comparer avec le mappage LUN.

matrice RAID Groupe de disques physiques, organisés et protégés par un schéma RAID, et présentés par le matériel ou le logiciel RAID comme un disque logique unique. Dans Xsan, les matrices RAID apparaissent sous forme de LUN, lesquelles sont associées afin de constituer des réserves de stockage.

Mbit Abréviation de mégabit.

Mbit/s Abréviation de mégabits par seconde.

mégaoctet Voir **Mo**.

mise en miroir Écriture de copies identiques de données sur deux disques physiques. La mise en miroir protège les données contre la perte due aux défaillances de disque et est le moyen le plus simple d'obtenir la redondance de données.

Mo Mégaoctet. 1 048 576 (2²⁰) octets.

Mo/s Abréviation de mégaoctets par seconde.

Network File System. Voir **NFS**.

NFS Network File System. Protocole client/serveur utilisant le protocole IP (Internet Protocol) pour permettre aux utilisateurs distants d'accéder à des fichiers comme s'ils se trouvaient sur leur disque. Le service NFS exporte les volumes partagés vers les ordinateurs en fonction de l'adresse IP, plutôt que du nom et mot de passe utilisateur.

niveau RAID Schéma d'allocation de stockage utilisé pour le stockage des données dans une matrice RAID. Défini par un nombre, par exemple RAID 3 ou RAID 0+1.

nom d'hôte Nom unique d'un serveur, autrefois appelé nom d'hôte UNIX. Le nom d'hôte Mac OS X Server est essentiellement utilisé pour l'accès client aux répertoires de départ NFS. Un serveur détermine son nom d'hôte en utilisant le premier nom disponible dans les sources suivantes : le nom spécifié dans le fichier /etc/hostconfig (HOSTNAME=nom d'hôte quelconque) ; le nom fourni par le serveur DHCP ou BootP pour l'adresse IP principale ; le premier nom retourné par une requête DNS inverse (adresse vers nom) pour l'adresse IP principale ; le nom d'hôte local ; le nom "hôte local".

nom de domaine Voir **nom DNS**.

nom de port Identifiant unique attribué à un port Fibre Channel.

nom DNS Nom unique d'un ordinateur, utilisé dans le système DNS (Domain Name System) pour convertir les adresses IP et les noms. Également appelé **nom de domaine**.

octet Unité basique de mesure des données équivalant à huit bits (ou chiffres binaires).

Open Directory Architecture des services de répertoires Apple qui peut accéder à des informations de référence sur les utilisateurs et les ressources réseau à partir de domaines de répertoire utilisant les protocoles LDAP, NetInfo, ou Active Directory, les fichiers de configuration BSD et les services de réseau.

open source Terme désignant le développement coopératif de logiciels par la communauté Internet. Le principe de base consiste à impliquer le maximum de personnes dans l'écriture et la mise au point du code en publiant le code source et en encourageant la formation d'une large communauté de développeurs qui feront part de leurs modifications et améliorations.

ouvrir une session Action consistant à démarrer une session sur un système (généralement en s'authentifiant en tant qu'utilisateur disposant d'un compte sur le système) afin d'obtenir des services ou d'accéder à des fichiers. Faites bien la différence entre l'ouverture de sessions et la connexion, qui implique simplement d'établir un lien physique avec le système.

par défaut Action automatique exécutée par un programme à moins que l'utilisateur n'en décide autrement.

port Sorte d'emplacement de messagerie virtuel. Un serveur utilise des numéros de port pour déterminer quelle application doit recevoir les paquets de données. Les coupe-feu utilisent des numéros de port pour déterminer si les paquets de données sont autorisés à transiter par un réseau local. Le terme "port" fait généralement référence à un port TCP ou UDP.

protocole Ensemble de règles qui déterminent la manière dont les données sont échangées entre deux applications.

RAID Redundant Array of Independent (or Inexpensive) Disks. Groupement de plusieurs disques durs physiques dans une matrice de disques dont le rôle est soit de fournir un accès haute vitesse aux données stockées, soit de mettre en miroir les données de façon à ce qu'elles puissent être reconstruites en cas de défaillance de disque, soit les deux. La matrice RAID est présentée au système de stockage en tant qu'unité de stockage logique unique. Voir aussi **matrice RAID** et **niveau RAID**.

RAID 1 Schéma RAID qui crée une paire de disques en miroir avec des copies identiques des mêmes données. Il fournit un degré élevé de disponibilité des données.

redondance Duplication de données ou inclusion de composants supplémentaires (des disques durs, par exemple) dans un système afin de récupérer les données ou d'assurer la poursuite du fonctionnement du système après la défaillance d'un composant de ce dernier.

répertoire de départ Dossier destiné à l'usage personnel d'un utilisateur. Entre autres, Mac OS X utilise également le répertoire de départ pour stocker des Préférences Système et des réglages d'utilisateur gérés pour les utilisateurs Mac OS X.

routeur Périphérique de mise en réseau d'ordinateurs qui réexpédie les paquets de données vers leur destination. Un routeur est une forme particulière de passerelle qui relie des segments réseau liés. Dans le contexte familial ou de petite entreprise, le terme routeur renvoie fréquemment à une passerelle Internet souvent dotée de fonctions de traduction d'adresses réseau (NAT, Network Address Translation). Généralement bien utilisé, le terme routeur fait référence plus exactement à un périphérique de réseau à matériel de routage dédié.

sauvegarde Ensemble de données stockées à des fins de récupération pour le cas où la copie originale des données serait perdue ou deviendrait inaccessible.

sauvegarde automatique Sauvegarde déclenchée par un événement (horaire programmé ou dépassement d'une limite de stockage, par exemple) et non par une action humaine.

sauvegarder Action consistant à créer une sauvegarde.

Server Message Block/Common Internet File System Voir **SMB/CIFS**.

serveur Ordinateur fournissant des services (service de fichiers, service de courrier électronique ou service Web, par exemple) à d'autres ordinateurs ou périphériques de réseau.

serveur de noms Serveur d'un réseau qui tient à jour une liste des noms de domaines et des adresses IP associées à chaque nom. Voir aussi **DNS**.

SMB/CIFS Server Message Block/Common Internet File System. Protocole permettant à des ordinateurs clients d'accéder à des fichiers et à des services de réseau. Il peut être utilisé via TCP/IP, Internet ou d'autres protocoles. Les services Windows utilisent le protocole SMB/CIFS pour fournir l'accès aux serveurs, imprimantes et autres ressources réseau.

support Dans un périphérique de stockage, matériel sur lequel les données sont enregistrées.

système de fichiers Schéma de stockage de données sur des périphériques de stockage et qui permet aux applications de lire et d'écrire des fichiers sans s'occuper de détails de niveau inférieur.

tolérance de pannes Capacité d'un système à continuer à fonctionner lorsqu'un ou plusieurs de ses composants sont défectueux.

tranche Subdivision logique d'une matrice RAID. Chaque tranche est un LUN distinct et apparaît sous forme de volume séparé sur un ordinateur hôte.

Index

A

- Admin RAID 12, 32, 44
- Admin Serveur 32
- adresse virtuelle 39
- agrégation de liens 5, 12
 - algorithme de distribution d'images 34
 - configuration 36
 - contrôle 38
 - définie 32
- algorithme de distribution d'images 34
- alimentation sans interruption
 - Voir aussi* UPS 28
- antivirus 31
- Apple Remote Desktop 32
- asr 42

B

- basculement IP
 - configuration 20
 - définition 15
 - dépannage 47
 - historique 23
 - serveur de sauvegarde 16
 - serveur maître 16
 - Xserve RAID 17

C

- Console 43
- Contrôle de serveur 12, 32, 44
- coupe-feu 31
- cron 42

D

- daemons
 - failoverd 16
 - heartbeatd 16
 - launchd 5, 12
 - watchdog 5
- ditto 42
- documentation 6

E

- entrées de configuration d'hôte
 - FAILOVER_BCAST_IPS 16
 - FAILOVER_PEER_IP 16
- équilibrage de la charge 39
- Ethereal 46

F

- FAILOVER_BCAST_IPS 16
- FAILOVER_PEER_IP 16
- failoverd 16
- failoverd.log 23
- FireWire 21

G

- grep 43
- guides d'administration du serveur 6

H

- haute disponibilité, définition 11
- heartbeatd 16

I

- interrupteur 36
- IP via FireWire 21

L

- LACP 34
- launchd 5, 12
- listes de contrôle d'accès 32
 - Voir aussi* ACL 32
- listes de contrôle d'accès de service
 - Voir aussi* SACL 32

M

- méthodes de sauvegarde 41
- mise en miroir 13

N

- nom DNS virtuel 20
- NotifyFailover 18, 19

O

- Open Directory 31
- outils de contrôle
 - Admin RAID 12, 32, 44
 - Apple Remote Desktop 32
 - Console 43
 - Contrôle de serveur 32, 44
 - outils de contrôle de disque 44
 - outils de contrôle réseau 46
- outils de contrôle de disque
 - df 45
 - diskspacemonitor 45
 - du 45
- outils de contrôle de réseau 44
 - Ethereal 46
 - tcpdump 46

P

- périphériques d'équilibrage de la charge 13
- points de défaillance uniques 25
- port virtuel 34
- PostAcq 19
- PreAcq 19
- ProcessFailover 18
- Protocole d'agrégation de liens (Aggregation Control Protocol)
 - Voir aussi* LACP 34

R

- RAID 26
- redémarrage automatique 30
- rsync 12, 42

S

- SACL 32
- sauvegarde 40
 - asr 42

- cron 42
- ditto 42
- mécanisme de vérification 42
- rsync 12, 42
- schémas de rotation 41
- support 41
- sauvegarde différentielle 41
- sauvegarde incrémentielle 41
- sauvegarde totale 41
- schéma de rotation
 - grand-père - père - fils 41
- scripts
 - NotifyFailover 18, 19
 - PostAcq 19
 - PreAcq 19
 - ProcessFailover 18
 - Test 18
- Sécurité 31
- sous-fenêtre Économiseur d'énergie 12

T

- TCP 34
- tcpdump 46
- Test 18

U

- UDP 34
- UPS 28
 - APC 28

W

- watchdog 5

X

- Xserve 13, 26
- Xserve RAID 13, 17, 26