Manuel d’installation du logiciel du châssis Sun Fire™ B1600 pour serveurs Blade

Sun Microsystems, Inc.
4150 Network Circle
Santa Clara, CA 95054 U.S.A.
650-960-1300

Référence : 817-1887-10
Avril 2003, révision A

Envoyez vos remarques concernant ce document à l’adresse : docfeedback@sun.com

Papier
recyclable

Adobe PostScript

Table des matières

Préface

Ce manuel explique comment configurer le logiciel sur les composants du châssis Sun Fire B1600 pour serveurs Blade afin d'intégrer le châssis du système dans votre réseau.

Il est destiné aux administrateurs système Solaris expérimentés.

Avant de consulter ce manuel

Avant d'exécuter les instructions contenues dans ce manuel, vous devez avoir installé le châssis du système Blade dans une armoire et connecté tous les câbles nécessaires. Pour des informations sur l'installation matérielle du système, consultez le *Manuel d'installation des composants du châssis Sun Fire B1600 pour serveurs Blade.*

Organisation de ce manuel

Le Chapitre 1 fournit un aperçu du logiciel du châssis Sun Fire B1600 pour serveurs Blade et indique ce dont vous avez besoin avant de suivre les instructions données dans le reste du manuel.

Le Chapitre 2 présente les premières étapes de l'installation du châssis du système.

Le Chapitre 3 présente la méthode la plus rapide de configuration du châssis du système si vous souhaitez l'installer sur un simple réseau sans aucune séparation entre vos réseaux de données et de gestion.

Le Chapitre 4 explique comment mettre sous tension un serveur Blade, y connecter une console et exécuter des diagnostics préliminaires.

Le Chapitre 5 apprend comment introduire le châssis du système dans un environnement de réseau où le trafic de données et le trafic de gestion sont séparés.

Le Chapitre 6 explique comment affiner la configuration effectuée au Chapitre 5 en configurant le châssis du système de manière à permettre une gestion sécurisée des serveurs Blade directement à partir du réseau de gestion.

Le Chapitre 7 se destine aux FAU (Fournisseurs d'accès à Internet). Il explique comment affecter des serveurs Blade à différents clients (appelés tenants de serveur Blade) et leur permettre de gérer leurs propres serveurs Blade sans devoir accéder à ceux des autres clients.

Annexe A décrit certaines tâches que vous devrez effectuer pour exécuter les instructions des chapitres qui suivent.

Annexe B explique comment se connecter à l'interface de ligne de commande du châssis du système à partir d'un ordinateur portable.

Annexe C complète les instructions des manuels *Solaris Advanced Installation Guide* et *DHCP Administration Guide*. Elle permet d'achever la configuration du serveur DHCP sur votre réseau de données de sorte que les serveurs Blade installés dans le châssis puissent recevoir des adresses IP dynamiques.

Annexe D fournit des informations sur l"utilisation des Web Start Flash Archives pour répliquer l'environnement d'exploitation et les applications d'un serveur Blade sur d'autres serveurs Blade.

Annexe E énumère les commandes disponibles à partir de l'invite `sc>` du contrôleur système.

Annexe F fournit des informations détaillées sur la relation entre les contrôleurs système actifs et de secours.

Après avoir lu ce manuel

Après avoir lu ce livre, vous devrez peut-être consulter deux autres manuels relatifs au châssis du système Blade :

- Pour plus d'informations sur l'utilisation de l'interface de ligne de commande avec le contrôleur système sur le châssis, référez-vous au *Manuel d'administration du châssis Sun Fire B1600 pour serveurs Blade.*
- Pour plus d'informations sur la gestion des commutateurs intégrés sur le châssis, référez-vous au *Manuel d'administration des commutateurs du châssis Sun Fire B1600 pour serveurs Blade*. Ce manuel décrit le matériel et l'architecture du commutateur intégré (Chapitre 1). Il explique également comment effectuer la configuration initiale du commutateur (Chapitre 2), gérer le commutateur à l'aide de l'interface utilisateur web et/ou de SNMP (Chapitre 3) et utiliser toutes les commandes disponibles pour la gestion du commutateur à partir de interface de ligne de commande (Chapitre 4).

Utilisation des commandes UNIX

Ce document ne contient pas d'informations sur les commandes et procédures de base de UNIX®.

Pour ce type d'informations, consultez au choix :

- *Guide des périphériques Sun Solaris*
- documentation en ligne AnswerBook2™ pour le système d'exploitation Solaris™ ;

Conventions typographiques

Mise en forme*	Signification	Exemples
`AaBbCc123`	Noms des commandes, fichiers et répertoires ; sorties d'ordinateur sur écran	Modifiez votre fichier `.login`. Utilisez la commande `ls -a` pour lister tous les fichiers. `% Vous avez du courrier.`
`AaBbCc123`	Données saisies par l'utilisateur devant être différenciées des sorties d'ordinateur sur écran	`% su` `Password:`
AaBbCc123	Titres de manuels, termes nouveaux ou mis en évidence Remplace les variables de ligne de commande par des valeurs ou noms existants.	Lisez le chapitre 6 du *Guide de l'utilisateur*. Ces options sont appelées options de *classe*. Vous *devez* être connecté comme superutilisateur pour effectuer cette opération. Pour supprimer un fichier, tapez `rm` *nomdufichier*.

* Les réglages de votre navigateur peuvent différer de ceux indiqués ici.

Invites shell

Shell	Invite
Shell C	*nom de la machine*%
Shell C superutilisateur	*nom de la machine*#
Shell Bourne et shell Korn	$
Shell Bourne et shell Korn superutilisateur	#
Shell du contrôleur système	sc>
Shell du commutateur intégré	Console#

Documentation connexe

Application	Titre	Référence
Conformité et sécurité	*Sun Fire B1600 Blade System Chassis Compliance and Safety Manual*	816-3364
Synthèse de l'installation (affiche dépliable)	*Sun Fire B1600 Blade System Chassis Quick Start Guide*	816-3625
installation du matériel	*Manuel d'installation des composants du châssis Sun Fire B1600 pour serveurs Blade*	817-1903
Installation du logiciel	*Manuel d'installation du logiciel du châssis Sun Fire B1600 pour serveurs Blade* (ce manuel)	817-1887
Administration du châssis du système et remplacement des composants	*Manuel d'administration du châssis Sun Fire B1600 pour serveurs Blade*	817-1897
Administration des commutateurs	*Manuel d'administration des commutateurs du châssis Sun Fire B1600 pour serveurs Blade*	817-1892
Informations de dernière minute	*Sun Fire B1600 Blade System Chassis Product Notes*	816-4174

Accès à la documentation Sun

Vous pouvez consulter, imprimer ou acheter de nombreux titres de la documentation Sun, dont des versions localisées, à l'adresse :

`http://www.sun.com/documentation`

Vos commentaires sont les bienvenus

Dans le but d'améliorer sa documentation, Sun vous invite à lui faire part de vos commentaires et suggestions. Vous pouvez envoyer vos commentaires à l'adresse :

`docfeedback@sun.com`

Mentionnez le numéro de référence de votre documentation (817-1887-10) dans l'objet de votre message électronique.

CHAPITRE **1**

Préparation de la configuration du châssis du système

Ce chapitre fournit un aperçu des procédures à suivre pour configurer le châssis du système. Il présente ensuite le châssis du système et explique les rôles du contrôleur système et des commutateurs. Le reste du chapitre (hormis la dernière section) indique que faire avant de configurer le châssis du système. La dernière section explique comment effectuer la transition entre les différentes interfaces utilisateur à l'aide de la séquence d'échappement #.

Ce chapitre contient les rubriques suivantes :

1.1 Installation du logiciel : présentation générale

Cette section résume les procédures à suivre pour configurer le châssis du système.

Remarque - Pour configurer le châssis du système, vous devez utiliser l'interface de ligne de commande avec le contrôleur système. A partir de cette interface, vous devrez accéder aux consoles des deux commutateurs et aux consoles des serveurs Blade. Lorsque vous êtes à la console d'un commutateur ou d'un serveur Blade, tapez **#.** pour retourner à l'invite `sc>` du contrôleur système actif.

1. **Créez un serveur NIS (Network Install Server) pour charger l'environnement d'exploitation sur les serveurs Blade.**

   Pour installer l'environnement d'exploitation sur un serveur Blade, vous devez faire démarrer le serveur Blade à partir d'un serveur NIS. Par conséquent, avant de procéder à la configuration du logiciel sur le châssis, suivez les instructions relatives à la création d'un serveur NIS dans le manuel *Solaris Advanced Installation Guide* (fourni avec le kit de logiciels Solaris). Ou bien, s'il y a déjà un serveur NIS sur votre réseau, ajoutez-y l'image Solaris pour les serveurs Blade.

   Si vous souhaitez utiliser des adresses IP dynamiques pour les composants du châssis système, reportez-vous à :

   - Section 1.6, « Informations IP requises pour le châssis » à la page 1-11 et
   - Section 1.7, « Utilisation d'un serveur DHCP pour la fourniture automatique des adresses IP des SSC » à la page 1-12,

   et consultez les informations complémentaires contenues dans l'annexe C pour achever la configuration du serveur NIS et du serveur DHCP sur le réseau de données.

2. **Etablissez une connexion série avec un des contrôleurs système sur le châssis**

   Ou bien, configurez un serveur DHCP pour fournir des informations de configuration IP au contrôleur système. Vous pouvez alors accéder au contrôleur système via telnet.

   Pour établir une connexion avec un des contrôleurs système sur le châssis, référez-vous au *Manuel d'installation des composants du châssis Sun Fire B1600 pour serveurs Blade*.

3. **Connectez-vous au contrôleur système, définissez un mot de passe et réglez la date et l'heure**

   Vous devez définir un mot de passe et régler la date et l'heure (voir chapitre 2).

4. **Connectez-vous et définissez au moins un mot de passe pour chaque commutateur**

   Pour plus d'informations à ce sujet, consultez le chapitre 2.

5. **Préparez l'environnement IP**

   Vous devez préparer l'environnement IP sur votre réseau pour y recevoir les contrôleurs système du châssis, les commutateurs et les serveurs Blade (voir chapitre 3).

6. **Effectuez une configuration simple**

   Pour vous constituer une configuration opérationnelle à affiner par la suite, suivez les instructions du chapitre 3. Celles-ci indiquent comment tirer avantage de la présence de deux commutateurs dans le châssis du système pour donner aux serveurs Blade deux connexions vers votre réseau.

7. **Au besoin, configurez le châssis du système en vue d'un environnement où le trafic de données et le trafic de gestion sont séparés.**

   Pour ce faire, suivez les instructions du chapitre 5. Celles-ci indiquent comment tirer avantage de la présence de deux commutateurs dans le châssis du système en utilisant IPMP (Internet Network Multipathing) pour donner à chaque serveur Blade deux connexions entièrement redondantes vers votre réseau de données.

8. **Au besoin, configurez le châssis du système de sorte que chaque serveur Blade ait à la fois une connexion redondante vers le réseau de données (de la manière décrite au chapitre 5) et une connexion redondante vers le réseau de gestion.**

   Pour ce faire, suivez les instructions du chapitre 6.

9. **Au besoin, configurez le châssis du système de sorte que différents serveurs Blade soient affectés à différents propriétaires, chacun pouvant gérer ses propres serveurs Blade sans avoir accès au contrôleur système, aux commutateurs ou aux serveurs Blade d'autres propriétaires.**

   Pour ce faire, suivez les instructions du chapitre 7.

1.2 Châssis Sun Fire B1600 pour serveurs Blade

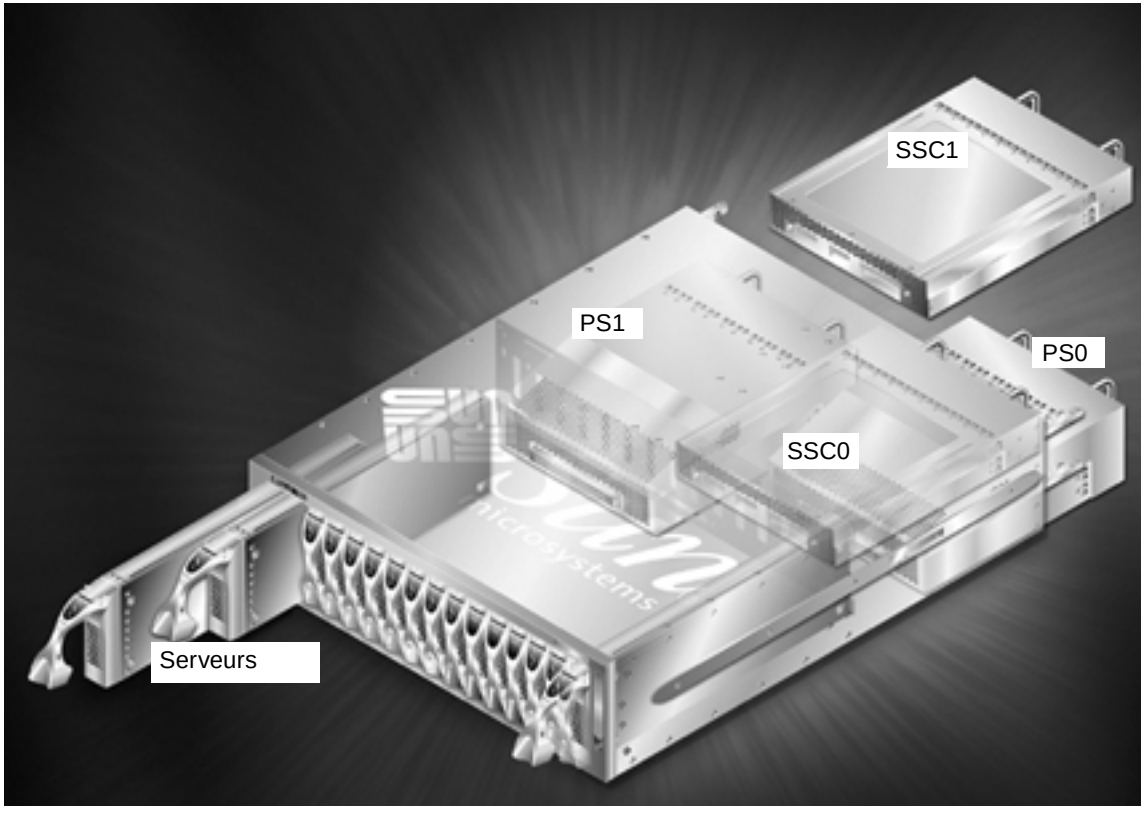

FIGURE 1-1 Châssis Sun Fire B1600 pour serveurs Blade

Le châssis Sun Fire B1600 pour serveurs Blade est un châssis de 3U de haut pour 16 serveurs, essentiellement conçu pour les fournisseurs d'accès à internet. Il convient également pour les réseaux clients d'entreprise où il faut maximiser la densité des serveurs hautes performances.

Pouvant recevoir jusqu'à 16 serveurs Blade, le châssis contient deux blocs d'alimentation (PSU) et deux unités SSC (Contrôleur de commutateur et du système).

1.3 Logiciel du châssis pour serveurs Blade

Les trois principaux composants logiciels du châssis pour serveurs Blade sont les logiciels destinés aux :

- deux contrôleurs système (un en SSC0, un en SSC1)
- deux commutateurs (un en SSC0, un en SSC1)
- serveurs Blade

1.3.1 Contrôleurs système actifs et de secours

Comme le montre la FIGURE 1-1, il y a deux unités SSC. Dans la configuration d'usine du châssis, le contrôleur système en SSC0 est « actif », tandis que le contrôleur en SSC1 est le contrôleur de secours.

Cependant, si le SSC qui contient le contrôleur système actif est retiré physiquement ou si l'application principale subit une défaillance majeure, le contrôleur système de secours (qui se trouve dans le SSC restant) devient automatiquement actif.

Il est également possible, à partir de la ligne de commande du contrôleur système actif, de demander que le contrôleur système de secours devienne le contrôleur actif. Pour plus d'informations à ce sujet, référez-vous au *Manuel d'administration du châssis Sun Fire B1600 pour serveurs Blade*.

Dans une version future du logiciel du contrôleur système, le contrôleur de secours prendra automatiquement le contrôle (et deviendra donc actif) si le contrôleur actif, qui surveille en permanence le contrôleur de secours, estime que ce dernier est mieux à même d'assumer ce rôle.

Les contrôleurs système partagent un alias d'adresse IP et peuvent avoir chacun une adresse IP privée. L'alias d'adresse IP est l'adresse du contrôleur système actif , quel que soit celui-ci. C'est cette adresse qui doit être spécifiée dans le Service de noms. Lorsqu'un contrôleur système prend le rôle de contrôleur actif, il s'attribue l'alias et s'annonce (via un message de diffusion contenant à la fois son adresse MAC et l'alias) au réseau comme étant le périphérique qui possède l'alias d'adresse IP.

Si vous attribuez une adresse IP privée à chaque contrôleur système, vous pouvez utiliser cette adresse IP privée (au lieu de l'alias) pour vous connecter au contrôleur système actif via telnet. Vous ne pouvez pas vous connecter au contrôleur système de secours via telnet, même s'il possède une adresse IP privée. Cependant, il est utile d'attribuer des adresses IP privées aux contrôleurs système (voir chapitre 3), car elles permettent à un administrateur de réseau de vérifier rapidement leur présence sur le réseau par un ping individuel.

1.3.2 Commutateurs redondants

Bien qu'un seul contrôleur système puisse être actif à la fois dans un châssis, les commutateurs contenus dans les deux SSC sont actifs en permanence. C'est une particularité importante des châssis pour serveurs Blade. Chaque serveur Blade possède deux interfaces réseau Gigabit – une pour chaque commutateur. Par conséquent, en cas de défaillance de la connectivité réseau sur une interface (par exemple, une panne du commutateur), l'autre interface continue à assurer le service.

Pour des informations sur la façon de tirer avantage de ces doubles connexions avec le réseau global pendant la configuration du châssis, consultez le chapitre 3 et le chapitre 5.

Remarque - Notez que les deux commutateurs du châssis sont actifs en permanence, même si un seul contrôleur système peut être actif à la fois.

1.3.3 Serveurs Blade

D'un point de vue logique, les serveurs Blade sont équivalents aux serveurs Sun standard d'entrée de gamme. Toutes les méthodes standard de configuration réseau et sysid (par exemple TFTP et DHCP) sont disponibles pour ces serveurs, de même que les méthodes suivantes d'installation réseau pour l'environnement d'exploitation Solaris :

- Installation avec Web Start
- Installation interactive
- Installation Jumpstart personnalisée
- Installation avec Web Start Flash

Pour des informations sur ces méthodes d'installation de Solaris, reportez-vous au chapitre 3 du *Guide d'installation avancée de SunPCi*.Section , « Pour des informations sur ces méthodes d'installation de Solaris, reportez-vous au chapitre 3 du Guide d'installation avancée de SunPCi.Rôles des contrôleurs système, commutateurs et serveurs Blade » à la page 1-6Rôles des contrôleurs système, commutateurs et serveurs Blade

1.4 Rôle des contrôleurs système, commutateurs et serveurs Blade

1.4.1 Rôle des contrôleurs système

Le contrôleur système actif remplit deux fonctions : il communique avec les sous-composants du châssis pour en surveiller l'état opérationnel ; et il fournit une interface de ligne de commande (disponible via une connexion série ou via telnet) avec le logiciel de configuration du châssis principal appelé « Advanced Lights Out Management Software » (Logiciel de gestion avancé hors courant). Ce logiciel est une application qui tourne sur le contrôleur système actif dans le châssis.

Le Chapitre 2 de ce manuel explique comment se connecter au logiciel de gestion avancé hors courant du contrôleur système.

Lorsque vous êtes connecté, vous avez accès :

- A l'ensemble de commandes spécifique au contrôleur système actif pour la surveillance et la gestion du châssis et de ses composants. Pour plus d'informations sur ces commandes, référez-vous à l'annexe E et au *Manuel d'administration du châssis Sun Fire B1600 pour serveurs Blade*.
- Aux consoles des deux commutateurs intégrés dans le châssis du système. Pour des informations sur les commandes spécifiques à l'interface de ligne de commande du commutateur, référez-vous au chapitre A et au *Manuel d'administration des commutateurs du châssis Sun Fire B1600 pour serveurs Blade*.
- Aux consoles des serveurs Blade que vous avez installés dans le châssis du système.

Ce manuel est conçu pour vous permettre, en premier lieu, de configurer un châssis pour serveurs Blade sans devoir vous référer aux autres manuels du CD de documentation fourni dans le kit.

Cependant, outre les versions en ligne de tous les documents papier que vous avez reçus dans le kit, le CD de documentation contient un guide en ligne du logiciel de gestion avancé hors courant (*Manuel d'administration du châssis Sun Fire B1600 pour serveurs Blade*) et un manuel de référence des commandes en ligne pour le commutateur intégré (*Manuel d'administration des commutateurs du châssis Sun Fire B1600 pour serveurs Blade*).

Pour une explication détaillée de la relation entre le contrôleur système actif et le contrôleur de secours, ainsi que sur les limitations de cette relation, voir annexe F.

1.4.2 Rôle du commutateur

La FIGURE 1-2 montre tous les ports Ethernet de chaque commutateur ainsi que les interfaces Ethernet de chaque serveur Blade. Chaque serveur Blade possède une interface avec le commutateur en SSC0 et une interface avec le commutateur en SSC1. Les commutateurs individuels ont un port pour chaque serveur Blade. Ces ports sont libellés SNP0 à SNP15. Les ports de liaison montante du réseau de données sont libellés NETP0 à NETP7.

Remarque - Il n'y a pas de relation directe entre des ports de liaison montante particuliers du réseau de données et des ports particulier des serveurs Blade. A la place, un midplane haute vitesse commute tout le trafic entre ces deux groupes de ports. Il est indiqué dans le diagramme par une ligne noire épaisse allant des ports SNP et ports NETP vers la matrice de commutation (switch fabric).

Le diagramme montre également le port de gestion interne (NETMGT) du commutateur et le port RJ-45 externe libellé NETMGT sur le fond de panier du SSC.

Le port NETMGT externe fournit une connexion Ethernet vers le contrôleur système (SC dans le diagramme) et le commutateur. (Le port de gestion interne du commutateur est également identifié comme NETMGT dans l'interface de ligne de commande du commutateur et son interface web.) Un mini-hub connecte le port NETMGT interne du commutateur et le contrôleur système au port NETMGT externe. Les numéros 1 et 2 à l'intérieur des ports Ethernet et de l'interface SC dans le diagramme indiquent la configuration VLAN par défaut[1] pour les ports des commutateurs. Le VLAN par défaut pour le réseau de données est VLAN 1. Le VLAN par défaut pour le réseau de gestion est VLAN 2.

L'identificateur VLAN du contrôleur système n'est pas configurable à partir du commutateur ; il se configure dans le cadre de la configuration interactive du contrôleur système avec la commande `setupsc` (voir chapitre 3). Lorsque vous exécutez cette commande, une série de questions vous sont posées, dont celle de savoir si vous souhaitez activer un VLAN pour le SC (contrôleur système). Si vous répondez oui, vous êtes invité à spécifier un ID VLAN pour l'interface SC ; la valeur par défaut est VLAN 2, conformément au VLAN de gestion par défaut sur le commutateur. L'interface SC n'est pas un port de commutateur. L'activation du VLAN sur cette interface lui fait accepter et transmettre uniquement les trames destinées au VLAN que vous spécifiez.

1. Un VLAN est un réseau local virtuel, autrement dit un réseau logique et domaine de diffusion autonome défini par la configuration logicielle d'un ensemble de ports sur un ou plus composants d'infrastructure de réseau.

Enfin, vous noterez que les commutateurs illustrés à la FIGURE 1-2 contiennent un filtre de paquets. Il s'agit avant tout d'une barrière entre le port NETMGT interne et tous les ports des serveurs Blade. Ce filtre protège votre réseau de gestion contre les attaques d'utilisateurs externes accédant aux serveurs Blade via le réseau de données.

Par défaut, aucun trafic réseau n'est autorisé à passer entre les serveurs Blade et le port NETMGT sur le commutateur. Cependant, vous pouvez autoriser le passage d'un certain trafic dans le filtre de paquets en spécifiand des règles concernant des protocoles particuliers. Pour plus d'informations à ce sujet, consultez le chapitre A.

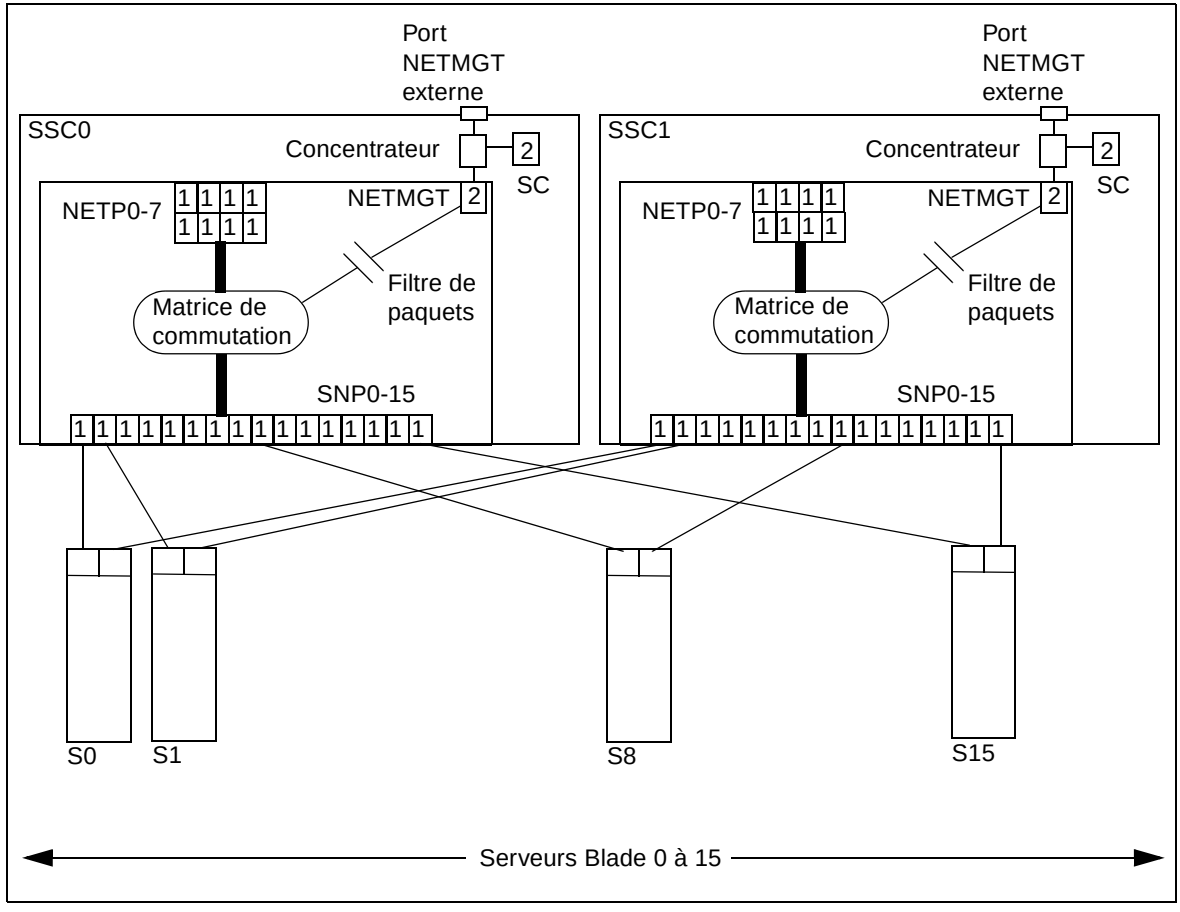

FIGURE 1-2 Ports et interfaces Ethernet du châssis du système et leurs numéros VLAN par défaut

1.4.3 Rôle des serveurs Blade

Les serveurs Blade fournissent la puissance de calcul requise pour exécuter des applications. Leur principal moyen d'E/S (entrée/sortie) est le réseau, mais vous pouvez les utiliser en mode console à partir de l'interface de ligne de commande du contrôleur système via une connexion série interne entre le contrôleur système et chaque serveur Blade.

Toutes les serveurs Blade possèdent une interface Gigabit Ethernet avec chacun des deux commutateurs internes du châssis, lesquels possèdent également une interface Gigabit Ethernet avec le réseau externe.

Les serveurs Blade possèdent généralement un stockage sur disque local pour contenir le logiciel du système d'exploitation et des informations de configuration. Les clients ne sont pas supposés stocker des données utilisateur sur les disques locaux des serveurs Blade mais utiliseront de préférence des unités de stockage distantes.

Dans leur état par défaut d'usine, les serveurs Blade démarrent à l'aide d'un stub de l'environnement d'exploitation stocké sur le disque dur local. Après le démarrage du stub, le serveur Blade cherche un serveur NIS sur le réseau pour installer l'environnement d'exploitation.

Une fois que vous avez fait démarrer le premier serveur Blade à partir du serveur NIS, vous pouvez ajouter l'application à exécuter sur le serveur Blade, puis suivre les instructions du *Solaris Advanced Installation Guide* pour créer une archive Web Start Flash. L'utilisation d'archives Web Start Flash sur les serveurs Blade Sun Fire B100s Solaris (dans le châssis système Sun Fire B1600 pour serveurs Blade) permet de répliquer l'environnement d'exploitation et les applications d'un serveur Blade sur les autres. Elle accélère par conséquent la configuration d'un châssis complet de serveurs Blade.

Pour plus d'informations sur l'utilisation d'archives Web Start Flash, reportez-vous à l'annexe D.

1.5 Avant de configurer le logiciel

Pour effectuer la configuration initiale après avoir installé et mis sous tension le châssis pour serveurs Blade, vous devez soit établir une connexion série avec SSC0 (le contrôleur système actif par défaut), soit configurer un serveur DHCP pour qu'il effectue automatiquement la configuration IP du contrôleur système actif du châssis. Si vous configurez un serveur DHCP de cette manière, vous pouvez vous connecter au contrôleur système actif via telnet pour configurer le châssis pour la première fois.

Pour plus d'informations sur le câblage d'une connexion série, référez-vous au *Manuel d'installation des composants du châssis Sun Fire B1600 pour serveurs Blade*.

Pour plus d'informations sur l'utilisation d'un serveur DHCP, reportez-vous à la Section 1.7, « Utilisation d'un serveur DHCP pour la fourniture automatique des adresses IP des SSC » à la page 1-12.

Remarque - Lorsque les deux SSC du châssis sont sous tension, fonctionnent normalement et ne sont pas endommagés, le contrôleur système actif par défaut est en SSC0 et le contrôleur système de secours en SSC1. Cela signifie que, pour configurer le châssis pour la première fois via une connexion série, vous devez avoir au moins une connexion série avec SSC0.

Cependant, pour le fonctionnement quotidien du châssis, nous recommandons d'établir des connexions série avec les deux SSC. De cette manière, si le SSC actif est inopérant pour une raison quelconque, vous ne perdrez pas la connexion série avec le châssis.

Le chapitre 2 et le chapitre 3 de ce manuel expliquent comment configurer le châssis après avoir établi une connexion série ou telnet avec SSC0 (en supposant que SSC0 contient le contrôleur système actif).

1.6 Informations IP requises pour le châssis

Pour permettre à votre environnement de réseau de recevoir un châssis système Sun Fire B1600 pour serveurs Blade, vous devez le configurer de sorte qu'il fournisse un alias d'adresse IP pour le contrôleur système actif, plus une adresse IP, un masque de réseau et une passerelle par défaut pour chacune des interfaces Ethernet sur le châssis.

L'alias d'adresse IP du contrôleur système est spécifié dans le Service de noms, mais les contrôleurs système peuvent également avoir chacun une adresse IP privée (que vous n'êtes pas obligé de spécifier dans le Service de noms). Lorsqu'un contrôleur système prend le rôle de contrôleur actif, il s'attribue l'alias d'adresse IP et s'annonce (via un message de diffusion contenant à la fois son adresse MAC et l'alias) au réseau comme étant le périphérique qui possède l'alias d'adresse IP.

Un châssis rempli utilise au moins 37 adresses IP (dont les deux adresses privées des SC) :

1. Un alias d'adresse IP pour le contrôleur système actif (l'adresse utilisée par le contrôleur système actif, qu'il soit en SSC0 ou en SSC1).
2. Une adresse IP privée pour le contrôleur système en SSC0.
3. Une adresse IP privée pour le contrôleur système en SSC1.

4. Une adresse IP pour le commutateur en SSC0.
5. Une adresse IP pour le commutateur en SSC1.
6. 16 adresses IP pour l'interface principale (Gigabit Ethernet) `ce0` sur chaque serveur Blade.
7. 16 adresses IP pour l'interface secondaire (Gigabit Ethernet) `ce1` sur chaque serveur Blade.

Si vous prévoyez d'effectuer une des configurations de châssis décrites au chapitre 5, chapitre 6 ou chapitre 7, qui impliquent toutes l'utilisation de la fonction IPMP (Internet Multipathing), vous aurez besoin de plus de 64 adresses IP pour les serveurs Blade d'un châssis complet.

1.7 Utilisation d'un serveur DHCP pour la fourniture automatique des adresses IP des SSC

Par défaut, le contrôleur système du SSC actif tentera de découvrir à partir d'un serveur DHCP les informations de configuration IP tant pour lui-même que pour le contrôleur système de secours.

Les commutateurs des deux SSC tenteront également par défaut de découvrir leur configuration IP à partir d'un serveur DHCP.

Les contrôleurs système utilisent au maximum trois adresses IP :

- un alias d'adresse IP (adresse utilisée par le contrôleur système actif, qu'il soit en SSC0 ou en SSC1) ;
- une adresse IP privée (facultative) pour le contrôleur système en SSC0 ;
- une adresse IP privée (facultative) pour le contrôleur système en SSC1.

Chaque commutateur exige une adresse IP.

Remarque - Si vous prévoyez de séparer les réseaux de données et de gestion, le serveur DHCP utilisé pour configurer les SSC doit se trouver sur le réseau de gestion et le serveur DHCP utilisé pour configurer les serveurs Blade doit se trouver sur le réseau de données. Pour des informations sur la configuration d'un serveur DHCP pour fournir les adresses IP des serveurs Blade, reportez-vous à l'annexe C.

1.7.1 Configuration des SSC avec des adresses IP « permanentes »

Le contrôleur système actif envoie une requête DHCP demandant trois adresses IP (SSC0, SSC1 et un alias).

Chaque commutateur envoie une requête DHCP demandant une adresse IP.

Si vous souhaitez utiliser cinq adresses IP « permanentes » (cinq adresses IP qui ne changeront pas), vous devez associer cinq adresses spécifiques du serveur DHCP aux identificateurs de client des contrôleurs système et des commutateurs.

Des identificateurs de client sont donnés individuellement aux contrôleurs système (ainsi qu'au contrôleur système actif, quel qu'il soit) car les contrôleurs système peuvent avoir chacun une adresse IP privée en option. (Il est utile d'attribuer des adresses IP privées pour permettre aux administrateurs de réseau de tester la présence des SC sur le réseau via un ping individuel.)

Les identificateurs de client des contrôleurs système et des commutateurs contenus dans le châssis sont énumérés au TABLEAU 1-1.

TABLEAU 1-1 Identificateurs de client des contrôleurs système et commutateurs intégrés

Périphérique	Identificateur de client
Contrôleur système actif	SUNW,SSC_ID=*numéro de série du châssis*
Contrôleur système en SSC0 (IP privée)	SUNW,SSC_ID=*numéro de série du châssis*,0
Contrôleur système en SSC1 (IP privée)	SUNW,SSC_ID=*numéro de série du châssis*,1
Commutateur en SSC0	SUNW,SWITCH_ID=*numéro de série du châssis*,0
Commutateur en SSC1	SUNW,SWITCH_ID=*numéro de série du châssis*,1

Remarque - Le numéro de série du châssis est imprimé sur une étiquette à l'arrière du châssis (côté droit). Pour les identificateurs de client, vous devez utiliser uniquement les 6 derniers chiffres du numéro imprimé sur l'étiquette du châssis.

(Vous pouvez aussi trouver le numéro de série du châssis en exécutant la commande `showfru ch` à partir de la ligne de commande du contrôleur système : il se trouve dans le champ `/ManR/Sun_serial_No`.)

Référez-vous aux instructions du *Solaris DHCP Administration Guide* (806-5529) pour créer des adresses IP « permanentes » et configurer un serveur DHCP sur le même réseau que les SSC de manière à fournir un bloc de cinq adresses IP associées aux identificateurs de client ci-desssus. Notez l'adresse IP que vous associez à chaque identificateur de client. Vous devrez la connaître pour vous connecter au contrôleur système actif ou à l'un des commutateurs via telnet. Vous devrez également la connaître si vous souhaitez accéder à l'interface utilisateur graphique basée sur le web pour communiquer avec les commutateurs.

1.7.2 Configuration des SSC avec des adresses IP dynamiques

Si vous ne souhaitez pas attribuer des adresses IP « permanentes » aux contrôleurs système et aux commutateurs du châssis, vous pouvez configurer le serveur DHCP de sorte qu'il fournisse un bloc d'adresses IP dynamiques. Celles-ci seront liées à l'identificateur de client une fois que les périphériques auront adressé leurs requêtes DHCP. Pour plus d'informations à ce sujet, reportez-vous au *Solaris DHCP Administration Guide* (806-5529).

Si vous configurez le serveur DHCP pour qu'il fournisse un bloc d'adresses IP dynamiques, vous devrez découvrir l'adresse IP qu'il a attribuée au contrôleur système et aux deux commutateurs, avant de pouvoir vous connecter au contrôleur système ou à l'un des commutateurs via telnet et de pouvoir accéder à l'interface utilisateur graphique basée sur le web pour communiquer avec les commutateurs (voir Section 1.7.3, « Découverte des adresses IP du châssis pour pouvoir utiliser telnet » à la page 1-14).

1.7.3 Découverte des adresses IP du châssis pour pouvoir utiliser telnet

Si vous souhaitez vous connecter au contrôleur système actif pour la première fois via telnet (au lieu d'utiliser une connexion série) et que vous avez attribué des adresses dynamiques (plutôt que « permanentes ») aux composants du châssis, vous devrez découvrir l'adresse IP que le serveur DHCP a attribuée au contrôleur système.

Si le serveur DHCP que vous utilisez est un système Solaris, vous pouvez utiliser la commande `pntadm` pour produire la liste de tous les périphériques (et de leurs adresses IP) présents sur le réseau où se trouve le châssis.

Pour ce faire, tapez :

```
# pntadm -P adresse réseau
pntadm -P 129.156.203.0
Client ID                                    Flags Client IP        Server IP   Lease Expiration

53554E572C5353435F49443D313233343536[1]          00 129.156.203.240  129.156.202.163 01/03/2003
53554E572C5357495443485F49443D3132333435362C30[2] 00 129.156.203.241  129.156.202.163 01/03/2003
53554E572C5357495443485F49443D3132333435362C31[3] 00 129.156.203.242  129.156.202.163 01/03/2003
```

Explications :

1. ID client du contrôleur système actif
2. ID client du commutateur en SSC0
3. ID client du commutateur en SSC1

où *adresse réseau* est l'adresse réseau de votre réseau de gestion. Les périphériques énumérés sont identifiés chacun par une chaîne hexadécimale représentant leur identificateur de client.

Dans l'exemple ci-dessus, le premier périphérique énuméré est le contrôleur système actif (celui qui utilise l'alias d'adresse IP), le second est le commutateur en SSC0 et le troisième est le commutateur en SSC1. Vous devez convertir les chaînes hexadécimales de la liste en leur équivalent alphanumérique pour savoir quel périphérique a reçu quelle adresse IP.

(Remarque : dans l'exemple, deux colonnes situées à droite de « Lease Expiration » ont été omises par manque d'espace – ce sont les colonnes « Macro » et « Comments ».)

TABLEAU 1-2 Exemple de conversion d'ID client pour un contrôleur système actif

	Contrôleur système actif	Numéro de série du châssis
Hexa	53554E572C5353435F49443D	313233343536
Alphanumérique	SUNW,SSC_ID=	123456

TABLEAU 1-3 Exemple de conversion d'ID client pour (l'adresse IP privée optionnelle de) SC[1]en SSC0

	Contrôleur système actif	Numéro de série du châssis	Suffixe pour SSC0
Hexa	53554E572C5353435F49443D	313233343536	2C30
Alphanumérique	SUNW,SSC_ID=	123456	,0

1. Contrôleur système

TABLEAU 1-4 Exemple de conversion d'ID client pour un commutateur en SSC1

	Commutateur en SSC1	Numéro de série du châssis	Suffixe pour SSC1
Hexa	53554E572C5357495443485F49443D	313233343536	2C31
Alphanumérique	SUNW,SWITCH_ID=	123456	,1

1.7.4 Accès au contrôleur système via telnet

Pour vous connecter au contrôleur système actif via telnet lorsque vous avez configuré la fourniture des adresses IP par un serveur DHCP :

1. **Si votre châssis est déjà sous tension, vous devez éteindre et rallumer le châssis en retirant les câbles d'alimentation IEC.**
2. **Lorsque le châssis est sous tension, tapez la commande suivante sur un terminal distant :**

```
% telnet alias d'adresse ip ou nom d'hôte
Trying alias d'adresse IP
Connected to alias d'adresse ip ou nom d'hôte
Escape character is '^]'

Sun Advanced Lights Out Manager for Blade Servers 1.0
ALOM-B 1.0

username:
```

où *alias d'adresse ip* est l'adresse IP du contrôleur système actif. (Vous pouvez aussi spécifier un nom d'hôte sur la ligne de commande.)

1.8 Retour à l'invite sc> à partir d'une console de commutateur ou de serveur Blade

Avant de procéder à la configuration du châssis, il est utile de noter la séquence d'échappement nécessaire pour retourner à l'invite sc> du contrôleur système à partir d'une console de serveur Blade ou de commutateur. Cette séquence est #. (à savoir, le caractère dièse '#', suivi d'un point '.').

En suivant les instructions de ce manuel, vous serez amené à accéder aux consoles de serveur Blade et de commutateur à partir de l'invite sc>.

Que faire ensuite

Passez au chapitre 2, qui présente les premières étapes de l'installation du châssis du système.

CHAPITRE **2**

Réglage des mots de passe, de la date et de l'heure sur les SCC

Ce chapitre explique comment se connecter au contrôleur système actif et aux deux commutateurs pour effectuer les tâches préliminaires nécessaires avant de pouvoir configurer le châssis pour serveurs Blade en vue d'une utilisation dans votre environnement de réseau.

Vous devez configurer le contrôleur système actif, mais pas le contrôleur de secours. Le contrôleur actif propage les informations de configuration vers le contrôleur de secours de sorte que celui-ci puisse reprendre le contrôle en cas de besoin.

Les commutateurs emploient un nom d'utilisateur et un mot de passe distincts de ceux des contrôleurs système. Leur configuration doit donc se faire séparément.

Ce chapitre contient les rubriques suivantes :

Suivez les instructions des deux sections.

Remarque - Pour configurer le châssis du système, vous devez utiliser l'interface de ligne de commande avec le contrôleur système actif. A partir de cette interface, cependant, vous devrez accéder aux consoles des deux commutateurs et aux consoles des serveurs Blade. Lorsque vous êtes à la console d'un commutateur ou d'un serveur Blade, tapez **#.** pour retourner à l'invite `sc>` du contrôleur système actif.

2.1 Connexion au contrôleur système et réglage du mot de passe et de l'heure

Cette section explique comment se connecter au contrôleur système actif comme utilisateur `admin` (utilisateur par défaut) et comment spécifier un mot de passe pour cet utilisateur.

Remarque - Les contrôleurs système emploient un nom d'utilisateur et un mot de passe distincts de ceux des commutateurs. Pour des détails sur la configuration de ces informations sur les commutateurs, reportez-vous à la Section 2.2, « Connexion au commutateur en tant qu'utilisateur par défaut et réglage des mots de passe » à la page 2-4.

La présente section suppose que vous avez établi une connexion série ou telnet avec le contrôleur système actif. (Vous ne pouvez pas établir une connexion telnet avec le contrôleur système de secours.) Si vous vous êtes connecté via telnet à l'aide de l'alias d'adresse IP, vous serez connecté au contrôleur système actif, quel qu'il soit.

Si vous utilisez une connexion série, vous devez savoir que, dans la configuration d'usine du châssis, le contrôleur système actif est celui situé en SSC0. Si vous vous connectez à SSC1 (et que SSC1 contient toujours le contrôleur système de secours), un message vous signalera que vous êtes connecté au contrôleur système de secours. Dans ce cas, établissez une connexion avec SSC0. Dans tous les cas, nous vous recommandons de maintenir des connexions série avec les deux SSC.

Pour commencer la configuration du châssis pour serveurs Blade, procédez comme suit :

1. **A l'invite `username:`, tapez le nom d'utilisateur par défaut (`admin`).**

```
Sun Advanced Lights Out Manager for Blade Servers 1.0
ALOM-B 1.0

username: admin
```

2. **A l'invite `sc>`, définissez un mot de passe pour l'utilisateur par défaut.**

   L'utilisateur par défaut (`admin`) est pré-configuré et ne peut pas être supprimé. Initialement, cet utilisateur ne peut que définir son propre mot de passe. Une fois le mot de passe défini, l'utilisateur obtient des autorisations complètes. Pour pouvoir continuer la configuration du châssis pour serveurs Blade, vous devez définir un mot de passe pour l'utilisateur par défaut (`admin`).

   Le premier mot de passe que vous spécifiez doit :

   - commencer par une lettre majuscule ou minuscule et contenir au moins deux lettres majuscules ou minuscules,
   - compter au moins six caractères (huit maximum),
   - contenir au moins un caractère numérique, un point (.), un trait de soulignement (_) ou un tiret (-),
   - être différent du nom d'utilisateur par défaut (`admin`), de son inverse (`nimda`) ou de toute séquence de ces caractères dans un ordre permettant leur lecture en boucle (par exemple, `dmina`, `minad`, `inadm` et `nadmi`),

   Pour plus d'informations sur la configuration d'utilisateurs nommés pour le contrôleur système, référez-vous au *Manuel d'administration du châssis Sun Fire B1600 pour serveurs Blade*.

   Pour définir un mot de passe pour l'utilisateur `admin`, tapez :

```
sc> password
Enter current password:
Enter new password:
Enter new password again:
New password set for user admin successfully
sc>
```

3. **Réglez la date et l'heure sur le contrôleur système actif.**

Remarque - Lorsque vous réglez la date et l'heure, vous devez utiliser le temps universel coordonné (UTC). Les serveurs Blade déterminent l'heure locale de votre fuseau horaire par décalage par rapport à l'heure universelle coordonnée sur le contrôleur système. Ils reçoivent cette heure du contrôleur système.

La commande est la même pour le réglage de la date et pour celui de l'heure : c'est la commande setdate. La syntaxe de cette commande est la suivante :

```
sc> setdate [mmjj]HHMM[.SS] | mmjjHHMM[cc]aa[.SS]
```

où :

mm est le mois (deux chiffres)
jj est le jour (deux chiffres)
HH est l'heure (deux chiffres)
MM sont les minutes (deux chiffres)
SS sont les secondes (deux chiffres)

- **Pour régler l'heure (format 24 heures)**
  Tapez l'heure (deux chiffres), suivie des minutes (deux chiffres). Par exemple, pour régler l'heure sur 11:42, tapez :

```
sc> setdate 1142
```

- **Pour régler le mois, le jour et l'heure (format 24 heures à la minute la plus proche)**
  Tapez le numéro du mois (deux chiffres) dans l'année, suivi du numéro du jour (deux chiffres) dans le mois, puis de l'heure (deux chiffres) et des minutes (deux chiffres). Par exemple, pour régler la date et l'heure sur 11:42 le 27 mars, tapez :

```
sc> setdate 03271142
```

- **Pour régler le mois, le jour et l'heure (format 24 heures), l'année et les secondes**
  Tapez le numéro du mois (deux chiffres) dans l'année, suivi du numéro du jour (deux chiffres) dans le mois, puis de l'heure (deux chiffres), des minutes (deux chiffres), de l'année (quatre ou deux caractères, p. ex. « 2002 » ou « 02 ») et, éventuellement d'un point et des secondes (deux chiffres). Par exemple, pour régler la date et l'heure sur 11h42 et 47 secondes le 27 mars 2002, tapez :

```
sc> setdate 2703114202.47
```

2.2 Connexion au commutateur en tant qu'utilisateur par défaut et réglage des mots de passe

Cette section explique comment vous connecter au commutateur et comment définir et enregistrer ses mots de passe.

Remarque - Le nom d'utilisateur et le mot de passe que vous configurez sur les commutateurs sont totalement distincts de ceux que vous configurez sur les contrôleurs système.

1. **Tapez :**

```
sc> console sscn/swt
```

où *n* est 0 ou 1 selon que vous configurez le commutateur en SSC0 ou SSC1. Par exemple, pour configurer le commutateur en SSC0, tapez :

```
sc> console ssc0/swt
```

2. **Lorsque vous êtes invité à entrer un nom d'utilisateur et un mot de passe, tapez** `admin` **pour les deux.**

```
Username admin
Password *****

CLI session with the host is opened.
To end the CLI session, enter [Exit].
```

3. **A l'invite** `console#`**, tapez :**

```
Console#configure
```

4. **Définissez au moins le premier des trois mots de passe suivants du commutateur :**

   a. **Définissez un mot de passe pour vous donner accès au mode de commande Privileged Exec du commutateur.**

      C'est le mode de commande qui vous permet de voir et modifier toute la configuration du commutateur. L'utilisateur par défaut `admin` (voir étape 2) possède des droits Privileged Exec. Par sécurité, nous recommandons de changer le mot de passe de cet utilisateur. Tapez :

```
Console(config)#username admin password 0 mot de passe
```

      où *mot de passe* est une chaîne de 1 à 8 caractères de longueur. (Le 0 indique au commutateur que le mot de passe est spécifié en texte normal. Pour des informations sur l'utilisation de texte normal ou chiffré pour les mots de passe, référez-vous au *Manuel d'administration des commutateurs du châssis Sun Fire B1600 pour serveurs Blade*.

   b. **Définissez un mot de passe pour l'utilisateur `guest`.**

      L'utilisateur `guest` peut voir une partie des informations de configuration et d'état du commutateur et peut également exécuter des commandes ping. Cet utilisateur ne peut modifier aucun des paramètres de configuration du commutateur. Le mot de passe par défaut de cet utilisateur est `guest`. Pour définir un nouveau mot de passe pour cet utilisateur, tapez :

```
Console(config)#username guest password 0 mot de passe
```

      où *mot de passe* est une chaîne de 1 à 8 caractères de longueur. (Le 0 indique que le mot de passe est spécifié en texte normal.)

   c. **Définissez un mot de passe pour la commande `enable`.**

      La commande `enable` permet à un utilisateur connecté comme `guest` d'obtenir des droits Privileged Exec. Si cet utilisateur tape `enable` sur la ligne de commande, il sera invité à fournir un mot de passe. Le mot de passe par défaut de la commande `enable` est `super`. Pour définir un nouveau mot de passe pour cet utilisateur, tapez :

```
Console(config)#enable password level 15 0 mot de passe
```

      où *mot de passe* est une chaîne de 1 à 8 caractères de longueur. Le nombre 15 spécifie que quiconque est autorisé à exécuter la commande `enable` aura des droits Privileged Exec. Le 0 indique que le mot de passe est spécifié en texte normal.

Remarque - Pour plus d'informations sur les différents modes de commande du châssis intégré, référez-vous au *Manuel d'administration des commutateurs du châssis Sun Fire B1600 pour serveurs Blade*.

5. **Quittez le mode de configuration du commutateur en tapant :**

```
Console(config)#end
```

ou

```
Console(config)#exit
```

6. **Comme vous avez changé la configuration du commutateur, vous devez maintenant enregistrer la configuration.**

   Pour ce faire, vous devez copier le microprogramme de configuration courant vers le microprogramme de configuration de démarrage.

   Tapez :

```
Console#copy running-config startup-config
Startup configuration file name []:nomfichier
Write to FLASH Programming
-Write to FLASH finish
Success

Console#
```

   où *nomfichier* est le nom à donner au fichier qui contiendra la nouvelle configuration de démarrage.

7. **Si vous utilisez DHCP pour fournir la configuration IP du commutateur, nous recommandons de configurer le second commutateur maintenant :**

   - soit en répétant les étapes étape 1 à étape 6 ci-dessus sur le second commutateur,
   - soit en suivant les instructions de la Section A.9, « Copie de la configuration du premier commutateur vers le second » à la page A-10. Lorsque vous copiez la configuration du commutateur, le nom d'utilisateur et le mot de passe que vous avez configurés sont également copiés.

   Si vous n'utilisez pas DHCP, vous ne devez pas configurer le second commutateur à ce stade. Les instructions du chapitre 3 indiquent quand le faire, mais vous devez poursuivre la configuration du premier commutateur avant de copier la configuration.

Que faire ensuite

Allez au chapitre 3 pour effectuer une installation réseau simple, puis configurez les serveurs Blade en suivant les instructions du chapitre 4.

Si vous devez effectuer une configuration réseau plus sophistiquée, consultez les chapitre 5, chapitre 6 et chapitre 7

CHAPITRE **3**

Installation du châssis du système sur un réseau simple

Ce chapitre contient les rubriques suivantes :

3.1 Avantage d'avoir deux commutateurs dans le châssis du système

Ce chapitre explique comment configurer le châssis Sun Fire B1600 pour serveurs Blade en vue de son utilisation dans un réseau simple où il n'y a pas de séparation entre le réseau de données et le réseau de gestion. Les instructions qui suivent vous permettent de tirer avantage de la présence de deux commutateurs dans le châssis du système pour donner à chacun des serveurs Blade deux connexions vers votre réseau.

La FIGURE 3-1 illustre un exemple de réseau contenant un châssis Sun Fire B1600 pour serveurs Blade. Les sections suivantes se basent sur ce diagramme et sur les adresses IP qui y sont marquées pour illustrer les opérations à effectuer.

Ce chapitre comprend également un exemple de fichier `/etc/hosts` et des exemples de fichiers `/etc/ethers` et `/etc/netmasks`. Ces exemples illustrent la façon de modifier les fichiers sur un serveur de noms pour préparer votre environnement de réseau à recevoir le châssis. Utilisez ces exemples de fichiers administratifs comme guide, en remplaçant par vos propres adresses IP et nom d'hôtes ceux qui figurent dans l'exemple de réseau illustré à la FIGURE 3-1.

Remarque - Lorsque vous envisagez la façon d'intégrer le châssis du système dans votre environnement de réseau, rappelez-vous que le châssis contient deux commutateurs et que chaque serveur Blade possède une interface avec chaque commutateur. Alors qu'un seul contrôleur système est actif à la fois dans le châssis, les deux commutateurs sont actifs en permanence. Cela signifie que, dans un châssis qui fonctionne normalement, *les deux* commutateurs offrent aux serveurs Blade une connexion permanente avec le réseau. Cependant, si un commutateur devient inopérant, l'autre commutateur continue à assurer cette connectivité.

Ce chapitre explique comment tirer avantage de cet élément de redondance réseau en configurant des adresses IP différentes pour chaque interface Ethernet disponible sur les serveurs Blade. Notez également que, si le contrôleur système actif devient inopérant, le commutateur contenu dans le SSC dont le contrôleur système est défaillant continue à assurer la connectivité réseau.

Pour profiter de la redondance offerte par le second commutateur contenu dans le châssis du système, nous vous recommandons de :

- toujours utiliser le châssis du système avec deux SSC installés ;
- vous assurer que les connexions câblées entre les huit ports de liaison montante du réseau de données et les sous-réseaux de votre réseau général sont exactement dupliquées sur les huit ports de liaison montante du second commutateur ;

- dupliquer la configuration du premier commutateur sur le second commutateur. (Pour des informations à ce sujet, reportez-vous à la Section A.9, « Copie de la configuration du premier commutateur vers le second » à la page A-10) ;
- spécifier des adresses IP pour les deux interfaces Ethernet (`ce0` et `ce1`) sur chaque serveur Blade si vous utilisez un serveur DHCP pour la configuration IP du châssis ;
- spécifier des adresses IP pour les deux interfaces Ethernet (`ce0` et `ce1`) de chaque serveur Blade si vous utilisez un fichier `/etc/hosts` sur votre serveur de noms (voir FIGURE 3-2) pour fournir une configuration IP statique (sans DHCP) du châssis ;
- spécifier les adresses MAC et IP des deux interfaces Ethernet sur chaque serveur Blade lorsque vous utilisez un fichier `/etc/ethers` sur votre serveur d'amorçage pour fournir une configuration IP statique (sans DHCP) du châssis.
- Pour profiter au maximum des interfaces redondantes entre chaque serveur Blade et les deux commutateurs intégrés du châssis, vous devez utiliser IPMP (IP Network Multipathing). Pour plus d'informations, reportez-vous au chapitre 5.

3.1.1 Découverte des adresses MAC des deux interfaces Ethernet de chaque serveur Blade

Lorsque vous configurez un fichier `/etc/ethers` sur votre serveur d'amorçage, vous devez connaître l'adresse MAC des interfaces `ce0` et `ce1` de chaque serveur Blade. Pour ce faire :

1. **Connectez-vous au contrôleur système actif (reportez-vous au chapitre 2).**
2. **A l'invite `sc>`, tapez :**

```
sc> showplatform -v
```

3. **La sortie de cette commande contient l'adresse MAC des interfaces `ce0` de chaque serveur Blade (libellées s0 à s15).**

   Calculez l'adresse MAC de `ce1` en prenant le nombre hexadécimal qui suit immédiatement le nombre utilisé pour `ce0` sur chaque serveur Blade.

3.2 Préparation de l'environnement de réseau avec DHCP

Les serveurs Blade, les contrôleurs système et les commutateurs contenus dans le châssis du système peuvent recevoir leur adresse IP de manière dynamique d'un serveur DHCP.

Pour des informations sur la configuration du serveur DHCP pour fournir les adresses IP des modules SSC du châssis, reportez-vous au chapitre 1.

Pour des informations sur la configuration du serveur DHCP pour fournir les adresses IP des serveurs Blade, reportez-vous à l'annexe C.

Remarque - Si vous utilisez DHCP pour configurer les paramètres IP des serveurs Blade, vous ne pouvez pas utiliser IPMP pour assurer la résilience du réseau.

Veillez à configurer le serveur DHCP de sorte qu'il fournisse une adresse IP pour chaque interface de chaque serveur Blade. Pour des informations sur la configuration d'un serveur DHCP pour la fourniture de paramètres de configuration IP dynamiques, consultez le *Solaris DHCP Administration Guide* (806-5529). Ce document est disponible sur le site de documentation Sun :

`http://docs.sun.com`

Pour configurer le serveur NIS en vue de l'utilisation d'adresses IP dynamiques, vous devez compléter les informations du *Solaris Advanced Installation Guide* et du *Solaris DHCP Administration Guide* (806-5529) avec celles de l'annexe C.

3.3 Préparation de l'environnement de réseau avec des adresses IP et noms d'hôte statiques

La FIGURE 3-1 montre un châssis Sun Fire B1600 pour serveurs Blade avec deux SSC installés et des logements configurés pour 16 serveurs Blade. L'interface `ce0` de chaque serveur Blade monté dans un châssis possède une connexion avec le commutateur en SSC0 et l'interface `ce1`, avec le commutateur en SSC1. Un ou plusieurs des huit ports de liaison montante du commutateur sont connectés à un commutateur externe auquel est connecté un serveur NIS (qui contient également un serveur de noms). A ce commutateur externe est connecté un routeur (adresse IP 192.168.1.1) qui sert de passerelle par défaut entre le châssis Sun Fire B1600 pour serveurs Blade et le réseau général. Enfin, sur les deux SSC, le port de gestion réseau 100Mbps (marqué NETMGT à l'arrière du châssis) est également connecté au commutateur externe.

Toutes les adresses IP affectées au châssis du système se trouvent sur le même sous-réseau.

Pour préparer l'insertion du châssis dans un environnement de réseau simple (tel celui illustré à la FIGURE 3-1), vous devez modifier les fichiers `/etc/hosts`, `/etc/ethers` et `/etc/netmasks` sur votre serveur de noms Solaris :

- La FIGURE 3-2 montre un exemple de fichier `/etc/hosts` contenant des adresses IP et des noms d'hôtes pour la configuration de réseau illustrée à la FIGURE 3-1.
- La FIGURE 3-3 montre un exemple de fichier `/etc/netmasks` contenant des masques de réseau pour les numéros de réseau IP utilisés dans l'exemple de réseau de la FIGURE 3-1.

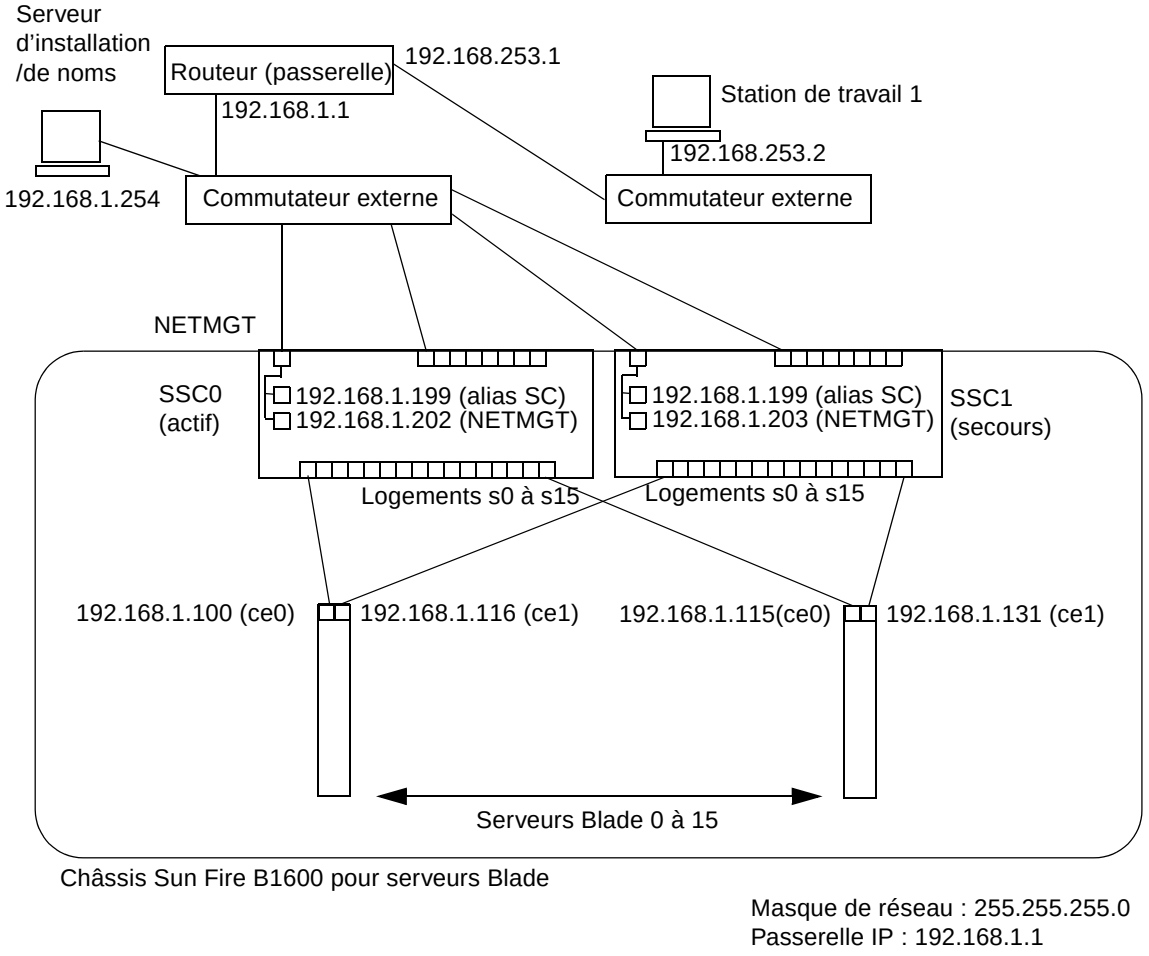

FIGURE 3-1 Exemple de configuration sans VLAN

```
# Internet host table
127.0.0.1   localhost
192.168.1.254 datanet-nameserver  # Data network name server
192.168.1.1  datanet-router-1     # Data network router (default gateway)
192.168.253.1 datanet-router-253  # Data network router (client side)
192.168.253.2 dataclient-ws1      # Data client network workstation

192.168.1.199  medusa-sc          # Medusa - active SC (alias IP address)
192.168.1.200  medusa-ssc0        # Medusa - SSC0/SC (private IP address)
192.168.1.201  medusa-ssc1        # Medusa - SSC1/SC (private IP address)
192.168.1.202  medusa-swt0        # Medusa - SSC0/SWT
192.168.1.203  medusa-swt1        # Medusa - SSC1/SWT

192.168.1.100  medusa-s0-0
192.168.1.101  medusa-s1-0
192.168.1.102  medusa-s2-0
192.168.1.103  medusa-s3-0
192.168.1.104  medusa-s4-0
192.168.1.105  medusa-s5-0
192.168.1.106  medusa-s6-0
192.168.1.107  medusa-s7-0
192.168.1.108  medusa-s8-0
192.168.1.109  medusa-s9-0
192.168.1.110  medusa-s10-0
192.168.1.111  medusa-s11-0
192.168.1.112  medusa-s12-0
192.168.1.113  medusa-s13-0
192.168.1.114  medusa-s14-0
192.168.1.115  medusa-s15-0
192.168.1.116  medusa-s0-1
192.168.1.117  medusa-s1-1
192.168.1.118  medusa-s2-1
192.168.1.119  medusa-s3-1
192.168.1.120  medusa-s4-1
192.168.1.121  medusa-s5-1
192.168.1.122  medusa-s6-1
192.168.1.123  medusa-s7-1
192.168.1.124  medusa-s8-1
192.168.1.125  medusa-s9-1
192.168.1.126  medusa-s10-1
192.168.1.127  medusa-s11-1
192.168.1.128  medusa-s12-1
192.168.1.129  medusa-s13-1
192.168.1.130  medusa-s14-1
192.168.1.131  medusa-s15-1
```

FIGURE 3-2 Exemple de fichier `/etc/hosts` sur le serveur de noms

```
#
# The netmasks file associates Internet Protocol (IP) address
# masks with IP network numbers.
#
#    network-number netmask
#
# The term network-number refers to a number obtained from the
# Internet Network Information Center. Currently this number is
# restricted to being a class A, B, or C network number. In the
# future we intend to support arbitrary network numbers
# as described in the Classless Internet Domain Routing
# guidelines.
#
# Both the network-number and the netmasks are specified in
# "decimal dot" notation, e.g:
#
#              128.32.0.0 255.255.255.0
#
192.168.1.0    255.255.255.0
192.168.253.0  255.255.255.0
#
```

FIGURE 3-3 Exemple de fichier `/etc/netmasks` sur le serveur de noms

3.4 Configuration des contrôleurs système et commutateurs

Pour exécuter les instructions de cette section, il vous faut une connexion série (ou telnet) avec le contrôleur système actif (par défaut, le contrôleur système en SSC0).

Pour plus d'informations sur la connexion au contrôleur système, reportez-vous au chapitre 1 et au chapitre 2 ci-dessus.

Pour plus d'informations sur l'établissement de connexions série avec les contrôleurs système, référez-vous au *Manuel d'installation des composants du châssis Sun Fire B1600 pour serveurs Blade*.

Pour des informations sur l'établissement d'une connexion telnet avec le contrôleur système actif, reportez-vous au chapitre 1.

3.4.1 Configuration des contrôleurs système

Remarque - Vous pouvez uniquement accéder à l'interface de ligne de commande du contrôleur système actif. Cependant, la commande `setupsc` décrite dans cette section configure les deux contrôleurs système. Notez que, même si un seul contrôleur système est actif à la fois, les deux commutateurs sont toujours actifs.

---

1. **Connectez-vous au contrôleur système actif en suivant les instructions du chapitre 2.**

2. **Exécutez la commande `setupsc`.**

   A l'invite `sc>`, tapez :

```
sc> setupsc
Entering Interactive setup mode.
Use Ctrl-z to exit & save. Use Ctrl-c to abort.

Do you want to configure the enabled interfaces [y]?
Should the SC network interface be enabled [y]?
Should the SC telnet interface be enabled for new connections[y]?
Do you want to configure the network interface [y]?
```

   En réponse aux questions qui vous sont posées lorsque vous exécutez `setupsc`, appuyez sur [ENTREE] pour accepter la réponse par défaut (indiquée entre crochets droits à la fin de la question : `y` pour oui, `n` pour non).

   Acceptez la réponse `y` par défaut pour les quatre premières questions.

3. **A la question de savoir si le contrôleur système (SC) doit utiliser DHCP pour obtenir sa configuration réseau, répondez y ou n.**

   Si vous répondez oui (y), passez à l'étape 5.

   Si vous répondez non (n), aux questions qui suivent, répondez successivement :

   - l'adresse IP SC (adresse IP que le contrôleur système actif, qu'il soit en SSC0 ou en SSC1, utilisera pour communiquer avec le réseau général),
   - le masque de réseau IP du contrôleur système,
   - la passerelle par défaut pour le contrôleur système.

4. **Lorsque le système demande si vous souhaitez configurer les adresses IP privées des contrôleurs système, répondez oui (y) ou non (n).**

   Tant le contrôleur actif que le contrôleur de secours peuvent avoir une adresse IP privée. Ces adresses IP privées doivent différer l'une de l'autre et de l'adresse IP SC (spécifiée à l'étape 3).

   Il est utile de spécifier des adresses privées, car elles permettent de vérifier la présence des deux contrôleurs système via un ping. Vous pouvez également vous connecter au contrôleur système actif via telnet en utilisant son adresse IP privée (ainsi que l'adresse réseau annoncée du contrôleur système actif). Vous ne pouvez pas vous connecter au contrôleur système de secours via telnet même s'il possède une adresse IP privée.

5. **Lorsque le système demande si vous souhaitez activer un VLAN pour le contrôleur système, répondez oui (y) ou non (n).**

   Si vous répondez oui, le port Ethernet du contrôleur système acceptera et émettra uniquement des trames adressées au VLAN que vous spécifiez en réponse à la question suivante.

   a. **Lorsque vous y êtes invité, spécifiez l'ID (un nombre entre 1 et 4094) du VLAN de gestion.**

      Spécifiez le même numéro que celui que vous prévoyez d'utiliser pour le VLAN de gestion sur le commutateur. Le numéro par défaut du VLAN de gestion sur le commutateur est 2. Nous déconseillons d'utiliser VLAN 1, qui est le VLAN par défaut du réseau de données.

6. **A l'invite, spécifiez l'adresse IP d'un SMS (système de gestion de systèmes).**

   Appuyez sur [ENTREE] pour passer à la question suivante ou tapez l'adresse d'une station de gestion de réseau que vous utilisez pour exécuter le logiciel Sun Management Center pour le Sun Fire B1600 ou l'agent Sun SNMP Management pour Sun Fire B1600.

7. **Lorsque le système demande si vous souhaitez configurer l'interface système gérée, répondez oui (y) ou non (n).**

   Si vous répondez oui, les questions suivantes demandent si vous voulez que les composants du châssis redémarrent automatiquement en cas de blocage et si vous souhaitez que les serveurs Blade soient automatiquement mis sous tension dès qu'ils sont insérés dans le châssis.

   a. **Lorsque la question vous est posée, indiquez si vous souhaitez que toutes les FRU (les deux SSC et tous les serveurs Blade) redémarrent automatiquement en cas de blocage.**

      Si vous répondez non, à la question suivante, indiquez si aucune ("none") des FRU ne doit être configurée pour redémarrer automatiquement en cas de blocage. Si vous répondez non à nouveau, vous pouvez spécifier pour chacune des FRU si elle doit redémarrer automatiquement en cas de blocage.

b. Lorsque la question vous est posée, indiquez si vous souhaitez que tous les serveurs Blade soient configurés pour s'allumer automatiquement à la mise sous tension du châssis et dès qu'un serveur Blade est inséré dans un châssis sous tension.

Si vous répondez non, à la question suivante, indiquez si aucun ("none") des serveurs Blade ne doit être configurée pour s'allumer automatiquement lorsque le châssis est mis sous tension ou que le serveur est inséré dans le châssis. Si vous répondez non à nouveau, vous avez la possibilité de spécifier, pour chaque serveur Blade, s'il doit s'allumer automatiquement lorsque le châssis est mis sous tension ou que le serveur est inséré dans le châssis.

8. Lorsque le système demande si vous souhaitez configurer les paramètres des contrôleurs système, répondez oui (y) ou non (n).

Si vous répondez oui, les questions qui suivent concernent la production de rapports d'événements sur l'interface telnet, le réglage de l'invite de commande du contrôleur système, la période d'inactivité maximale des sessions utilisateur sur le contrôleur système, l'affichage de caractères * sur l'écran lorsqu'un utilisateur tape son mot de passe et l'utilisation du protocole NTP (Network Time Protocol) par le contrôleur système.

a. A la question de savoir si vous souhaitez activer les rapports d'événements CLI, tapez y **si vous souhaitez recevoir des rapports d'événements concernant les connexions telnet avec le SSC.**

Notez que la production de rapports d'événements sur la connexion série du SSC ne peut pas être désactivée.

b. Comme niveau d'événements à afficher (si vous avez tapé y **à l'étape a), acceptez la valeur par défaut pour voir les événements de niveau de gravité 2 et supérieur.**

Au niveau 2, les événements MINEURS, MAJEURS et CRITIQUES sont affichés.

c. Spécifiez l'invite de ligne de commande pour le contrôleur système ou acceptez la valeur par défaut.

d. Spécifiez le temps d'inactivité maximal pour l'interface de ligne de commande.

Avec la valeur par défaut, une session utilisateur n'expire pas, quelle que soit la durée de la période d'inactivité.

e. Indiquez si vous souhaitez que le logiciel affiche des caractères * sur l'écran lorsqu'un utilisateur tape son mot de passe.

f. Indiquez si vous souhaitez activer le protocole NTP.

Répondez oui si vous avez un serveur de temps sur le réseau et souhaitez l'utiliser. Ensuite, en réponse à la question qui apparaît, tapez l'adresse IP des serveurs NTP primaire et secondaire.

9. **A la question de savoir si vous voulez que les modifications du réseau prennent effet immédiatement, répondez oui (y) ou non (n).**

   Cette question n'est posée que si vous avez apporté des modifications aux paramètres réseau du contrôleur système. Si vous répondez oui et que vous configurez le contrôleur système à l'aide d'une connexion telnet, soyez conscient que vous risquez de perdre votre connexion telnet.

10. **Suivez les instructions de la Section 3.4.3, « Configuration des commutateurs en SSC0 et SSC1 » à la page 3-14 pour configurer le commutateur.**

```
sc> setupsc
Entering Interactive setup mode.
Use Ctrl-z to exit & save. Use Ctrl-c to abort.

Do you want to configure the enabled interfaces [y]?
Should the SC network interface be enabled [y]?
Should the SC telnet interface be enabled for new connections[y]?
Do you want to configure the network interface [y]?
Should the SC use DHCP to obtain its network configuration [n]?
Enter the SC IP address [192.156.203.139]:
Enter the SC IP netmask [255.255.255.0]:
Enter the SC IP gateway [192.168.1.1]:
Do you want to configure the the SC private addresses [y]?
Enter the SSC0/SC IP private address [192.168.1.200]:
Enter the SSC1/SC IP private address [192.168.1.201]:
Do you want to enable a VLAN for the SC [y]?
Enter VLAN ID [2]: 2
Enter the SMS IP address [0.0.0.0]:
Do you want to configure the managed system interface [y]? y
Should all frus be configured to be automatically restarted if hung
[y]?
Should all of the blades be configured to power on automatically [y]?
Do you want to configure the System Controller parameters [y]?
Do you want to enable CLI event reporting via the telnet interface [y]?
Enter the level of events to be displayed over the CLI.
(0 = critical, 1 = major, 2 = minor) [2]:
Enter the CLI prompt [sc>]:
Enter the CLI timeout (0, 60 - 9999 seconds) [0]:
Should the password entry echo *'s [y]?
Do you want to enable NTP [y]?
Enter the IP address of the primary NTP server [192.168.130.26]:
Enter the IP address of the secondary NTP server [192.168.130.26]:
Do you want the network changes to take effect immediately [y]?
sc>
```

FIGURE 3-4 Exemple de sortie et de réponses de `setupsc` (configuration sans DHCP)

```
sc> setupsc
Entering Interactive setup mode.
Use Ctrl-z to exit & save. Use Ctrl-c to abort.

Do you want to configure the enabled interfaces [y]?
Should the SC network interface be enabled [y]?
Should the SC telnet interface be enabled for new connections[y]?
Do you want to configure the network interface [y]?
Should the SC use DHCP to obtain its network configuration [n]? y
Do you want to enable a VLAN for the SC [y]?
Enter VLAN ID [2]: 2
Enter the SMS IP address [0.0.0.0]:
Do you want to configure the managed system interface [n]?
Do you want to configure the managed system interface [y]? n
Do you want to configure the System Controller parameters [y]? n
Do you want the network changes to take effect immediately [y]?
sc>
```

FIGURE 3-5 Exemple de sortie et de réponses de `setupsc` (configuration DHCP)

3.4.2 Affichage de la configuration du contrôleur système

Pour visualiser la configuration du contrôleur système, exécutez la commande `showsc -v`. Toutes les propriétés configurables du contrôleur système s'affichent.

- **Tapez :**

```
sc> showsc -v
Sun Advanced Lights Out Manager for Blade Servers 1.0
ALOM-B 1.0

Release: 0.2.0, Created: 2003.01.10.11.03

Parameter                                Running Value    Stored Value
-------------------------------------------------------------------
Bootable Image:                          0.2.0 (Jan 10 03)
Current Running Image:                   0.2.0 (Jan 10 03)
SC IP address:                           192.156.203.139  129.156.203.139
SC IP netmask address:                   255.255.255.0    255.255.255.0
SC IP gateway address:                   192.168.1.1      192.168.1.1
SSC1/SC (Active) IP private address:     192.168.1.200    192.168.1.200
SSC0/SC (Standby) IP private address:    192.168.1.201    192.168.1.201
SMS IP address:                          0.0.0.0          0.0.0.0
SC VLAN:                                 Disabled         Disabled
SC DHCP:                                 Enabled          Enabled
SC Network interface is:                 Enabled          Enabled
SC Telnet interface is:                  Enabled          Enabled
NTP:                                     Disabled         Disabled
Blade auto restart when hung:
S0                                       Disabled         Disabled
S1                                       Disabled         Disabled
S2                                       Disabled         Disabled
Blade auto poweron:
S0                                       Disabled         Disabled
S1                                       Disabled         Disabled
S2                                       Disabled         Disabled
The CLI prompt is set as:                sc>              sc>
Event Reporting via telnet interface:    Enabled          Enabled
The CLI event level is set as:           CRITICAL         CRITICAL
The CLI timeout (seconds) is set at:     0                0
Mask password with *'s:                  Disabled         Disabled

*Output continued on next page*
```

FIGURE 3-6 Configuration par défaut d'un châssis avec trois serveurs Blade (`showsc -v`)

```
FRU  Software Version      Software Release Date
-------------------------------------------------------
S0   v1.1T30-SUNW,Serverblade1  Oct 24 2002 16:22:2
S1   v1.1T30-SUNW,Serverblade1  Oct 24 2002 16:22:24
S2   v1.1T30-SUNW,Serverblade1  Oct 24 2002 16:22:24
S3   Not Present
S4   Not Present
S5   Not Present
S6   Not Present
S7   Not Present
S8   Not Present
S9   Not Present
S10  Not Present
S11  Not Present
S12  Not Present
S13  Not Present
S14  Not Present
S15  Not Present
sc>
```

FIGURE 3-7 Configuration par défaut d'un châssis avec trois serveurs Blade (*suite*)

3.4.3 Configuration des commutateurs en SSC0 et SSC1

Cette section explique comment configurer l'adresse IP, le masque de réseau et la passerelle par défaut des commutateurs. Par défaut, les commutateurs tentent d'obtenir leur configuration IP de DHCP. Dès lors, si vous avez configuré votre serveur DHCP pour qu'il fournisse les informations IP aux commutateurs, passez cette section.

1. **Pour vous connecter au commutateur en SSC0, tapez :**

```
sc> console ssc0/swt
```

2. **A l'invite, tapez le nom d'utilisateur et le mot de passe pour le commutateur.**

3. **Par défaut, l'adresse IP et le masque de réseau du commutateur sont définis par DHCP. Vous pouvez les définir manuellement en tapant :**

```
Console#configure
Console(config)#interface vlan id vlan
Console(config-if)#ip address adresse ip  masque réseau
Console(config-if)#exit
```

où *id vlan* est le numéro du VLAN contenant le port de gestion réseau du commutateur, NETMGT (si vous utilisez la configuration par défaut du commutateur, c'est le numéro 2), *adresse ip* est l'adresse IP à utiliser par le commutateur et *masque réseau* est le masque de réseau que vous souhaitez définir.

Par exemple, pour spécifier l'adresse IP et le masque de réseau du commutateur en SSC0 à la FIGURE 3-1, tapez :

```
Console#configure
Console(config)#interface vlan 2
Console(config-if)#ip address 192.168.1.202 255.255.255.0
Console(config-if)#exit
```

4. **Par défaut, la passerelle par défaut est définie par DHCP.**

Vous pouvez la définir manuellement en tapant :

```
Console(config)#ip default-gateway adresse ip
Console(config)#exit
```

où *adresse ip* est l'adresse IP du périphérique que vous spécifiez comme passerelle par défaut.

5. **Enregistrez la nouvelle configuration du commutateur.**

   Tapez la commande suivante à la console du commutateur :

```
Console#copy running-config startup-config
Startup configuration file name []:nomfichier
Write to FLASH Programming
-Write to FLASH finish
Success

Console#
```

   où *nomfichier* est le nom à donner au fichier qui contiendra la nouvelle configuration de démarrage.

6. **Tapez `exit` pour vous déconnecter du premier commutateur.**

   Tapez ensuite `#.` pour quitter l'interface de ligne de commande du commutateur et retourner à l'invite `sc>` du contrôleur système.

7. **Configurez à présent le second commutateur en suivant les instructions de la Section A.9, « Copie de la configuration du premier commutateur vers le second » à la page A-10.**

   Ou bien, répétez la procédure de l'étape 1 à l'étape 6 pour le commutateur en SSC1.

Que faire ensuite

Suivez les instructions du chapitre 4 pour configurer les serveurs Blade.

CHAPITRE **4**

Configuration des serveurs Blade et diagnostics initiaux

Ce chapitre explique comment mettre sous tension un serveur Blade et accéder à sa console, puis comment effectuer des diagnostics préliminaire à l'aide des différents outils disponibles (sauf le logiciel Advanced Lights-out Management décrit dans le *Manuel d'installation du logiciel du châssis Sun Fire B1600 pour serveurs Blade*).

Pour des informations générales sur l'exécution de diagnostics sur des systèmes Solaris, référez-vous aux manuels *OpenBoot Command Reference Manual* et *SunVTS Users Guide*. Ces manuels sont disponibles sur le CD Software Supplement fourni avec le kit de logiciels Solaris. Vous pouvez également y accéder sur :

`http://www.sun.com/documentation`

Ce chapitre contient les rubriques suivantes :

Remarque - Lorsque vous êtes à la console d'un serveur Blade, tapez **#.** pour retourner à l'invite `sc>` du contrôleur système actif.

4.1 Mise sous tension des serveurs Blade

Lorsque vous mettez sous tension un serveur Blade qui est dans son état d'usine par défaut, le serveur démarre automatiquement à partir d'un stub de l'environnement d'exploitation se trouvant sur son disque dur local. Il cherche ensuite un serveur NIS à partir duquel il peut achever l'installation de l'environnement d'exploitation.

Pour configurer un serveur NIS, suivez les instructions du *Solaris Advanced Installation Guide*.

Pour plus d'informations sur l'utilisation d'archives Web Start Flash pour accélérer la configuration d'une série de serveurs Blade dans un châssis système, référez-vous à l'annexe D de ce manuel.

Lorsque vous êtes prêt, mettez sous tension un serveur Blade et faites-le démarrer en suivant les instructions ci-dessous :

1. **Mettez sous tension le serveur Blade.**

   Tapez :

   ```
   sc> poweron sn
   ```

   où *n* est le numéro de logement contenant le serveur Blade.

2. **Connectez-vous à la console du serveur Blade pour afficher le processus d'amorçage (et/ou y participer).**

   Tapez la commande suivante à l'invite `sc>` pour accéder à la console du serveur Blade.

   ```
   sc> console sn
   ```

   où *n* est le numéro du logement contenant le serveur Blade.

   Votre action suivante dépend de la méthode d'installation Solaris choisie dans le *Solaris Advanced Installation Guide*.

3. **Au besoin, vous pouvez interrompre le processus d'amorçage pour le piloter vous-même ou pour exécuter des diagnostics.**

   Pour interrompre le processus d'amorçage[1], tapez :

```
sc> break sn
```

   où *n* est le numéro du logement contenant le serveur Blade.

4. **Suivez les instructions du reste de ce chapitre si vous souhaitez effectuer des diagnostics initiaux sur le serveur Blade.**

Remarque - Lorsque vous êtes à la console d'un serveur Blade, tapez **#.** pour retourner à l'invite `sc>` du contrôleur système actif.

4.2 Utilisation des diagnostics POST (auto-test à la mise sous tension)

Cette section explique comment contrôler le processus de diagnostic POST qui (par défaut) s'exécute sur un serveur Blade au démarrage.

4.2.1 Contrôle du niveau de diagnostic

Trois niveaux de tests sont disponibles pour les diagnostics POST :

- `max` (niveau maximal)
- `min` (niveau minimal)
- `off` (aucun test)

Définissez le niveau voulu à l'aide de la variable OpenBoot PROM `diag-level`. Le réglage par défaut de `diag-level` est `min`. Pour le définir, tapez :

```
ok diag-level niveau
```

où *niveau* est `min`, `max` ou `off`.

1. Pour des informations sur la configuration d'un serveur Blade pour qu'il n'accepte pas les commandes `break`, référez-vous à la page MAN `kbd(1)`.

4.2.2 Contournement des paramètres de diagnostic du serveur Blade à partir du contrôleur système

Vous pouvez utiliser la commande `bootmode` du contrôleur système pour supplanter temporairement les valeurs de `diag-level` et `diag-switch?`.

- **Pour faire démarrer le serveur Blade avec des diagnostics alors qu'il n'est pas configuré pour cela :**

  a. Tapez `#.` pour retourner à l'interface de ligne de commande du contrôleur système.

  b. Tapez :

```
sc> bootmode diag sn
```

  où *n* est le numéro du logement du serveur Blade à configurer.

  Cette commande revient à mettre le paramètre `diag-switch?` à `true` et `diag-level` à `min` pour un seul démarrage uniquement. (Si `diag-level` est à `max` ou `min` sur le serveur Blade, la commande `bootmode` n'en modifie pas le réglage.)

- **Pour faire démarrer le serveur Blade sans exécuter les diagnostics alors qu'il est configuré pour les diagnostics :**

  a. Tapez `#.` pour retourner à l'interface de ligne de commande du contrôleur système.

  b. Tapez :

```
sc> bootmode skip_diag sn
```

  où n est le numéro du logement du serveur Blade à configurer.

  Cette commande revient à mettre le paramètre `diag-switch?` à `false`.

4.2.3 Exécution des diagnostics POST

Si la variable OpenBoot PROM (OBP) `diag-switch?` est à `true`, les diagnostics POST s'exécuteront automatiquement à la mise sous tension du serveur. Cependant, le réglage par défaut de `diag-switch?` est `false`.

Pour initialiser les diagnostics POST, vous devez mettre la variable `diag-switch?` à `true` et `diag-level` à `max` ou `min` (pas `off`). Cela fait, vous devez réinitialiser le serveur Blade. Suivez les instructions ci-dessous :

1. **A l'invite** `ok` **du serveur Blade, tapez :**

```
ok setenv diag-switch? true
```

2. **Tapez** `#.` **pour retourner à l'interface de ligne de commande du contrôleur système.**

3. **Mettez le serveur Blade hors, puis sous tension :**

   Tapez :

```
sc> poweroff sn
```

   où *n* est le numéro de logement du serveur Blade.

   Tapez ensuite :

```
sc> poweron sn
```

4. **Dans les deux à trois secondes (si possible) qui suivent la mise sous tension du serveur Blade, accédez à la console du serveur Blade pour afficher les résultats des diagnostics.**

   Tapez :

```
sc> console sn
```

5. **A la fin du démarrage, vous pouvez vérifier la sortie de la console en tapant #. pour retourner à l'interface de ligne de commande du contrôleur système et en tapant :**

```
sc> consolehistory boot sn
```

   Si les tests POST détectent une erreur, ils affichent un message décrivant le problème.

   Si les tests POST détectent une erreur « fatale » (par exemple, un problème matériel lié à la mémoire sur carte ou au processeur), ils éteignent le serveur Blade et allument le témoin d'erreur correspondant).

4.3 Utilisation des diagnostics OpenBoot (obdiag)

Pour exécuter les diagnostics OpenBoot, procédez comme suit :

1. **A l'invite** `ok`**, tapez :**

```
ok setenv auto-boot? false
ok reset-all
```

2. **Tapez:**

```
ok obdiag
```

Cette commande affiche le menu OpenBoot Diagnostics :

```
                                obdiag
1 bscv@0,0            2 ide@d               3 network@a
4 network@b           5 ide@d               6 rtc@0,70
7 serial@0,3f8

      Commandes : test test-all except help what setenv exit

              diag-passes=1 diag-level=max test-args=
```

FIGURE 4-1 Le menu `obdiag`

Les tests sont décrits au TABLEAU 4-1. Notez le numéro correspondant au test à effectuer, et utilisez-le avec la commande `test`. Par exemple, pour effectuer un test sur le port Ethernet principal, tapez :

```
obdiag> test 3
Hit the spacebar to interrupt testing
Testing /pci@1f,0/network@a ..........................passed
Pass:1 (of 1) Errors:0 (of 0) Tests Failed:0 Elapsed Time: 0:0:0:2

Hit any key to return to the main menu.
```

3. **Lorsque vous avez terminé le test, quittez OpenBoot Diagnostics et remettez `auto-boot?` à true.**

Pour ce faire, tapez :

```
obdiag> exit
ok setenv auto-boot? true
ok auto-boot? true
ok boot
```

Le tableau ci-dessous indique la fonction de chaque test.

TABLEAU 4-1 Tests OpenBoot Diagnostics

1	`bscv@0,0`	teste la puce de support du serveur Blade
2	`ide@d`	teste le contrôleur IDE
3	`network@a`	teste l'interface Ethernet principale
4	`network@b`	teste l'interface Ethernet secondaire
5	`pmu@3`	teste l'unité de gestion d'énergie
6	`rtc@0,70`	teste l'horloge en temps réel
7	`serial@0,3f8`	teste l'interface série avec le contrôleur système

4.4 Utilisation d'autres commandes OpenBoot PROM

Cette section décrit les commandes OpenBoot PROM disponibles et explique la fonction de chacune.

Commande `show-devs`

Utilisez la commande OpenBoot PROM `show-devs` pour produire la liste des périphériques dans l'arborescence OBP.

Commande `printenv`

Utilisez la commande OpenBoot PROM `printenv` pour afficher les variables de configuration OpenBoot PROM stockées dans la NVRAM système. L'affichage indique les valeurs actuelles de ces variables, ainsi que les valeurs par défaut. Vous pouvez également spécifier une variable de manière à n'afficher que la valeur actuelle de cette variable. Par exemple, la commande `printenv diag-level` produit la valeur actuelle de la variable `diag-level`.

Commande `watch-clock`

La commande `watch-clock` affiche un nombre qui augmente une fois par seconde. En mode normal de fonctionnement, le compteur des secondes augmente progressivement de 0 à 59. L'exemple qui suit illustre la sortie d'une commande `watch-clock`.

```
ok watch-clock
Watching the 'seconds' register of the real time clock chip.
It should be 'ticking' once a second.
Type any key to stop.
4
```

Commandes `watch-net` *et* `watch-net-all`

Les commandes `watch-net` et `watch-net-all` surveillent les paquets Ethernet sur les interfaces Ethernet du serveur Blade. Les paquets corrects reçus sont indiqués par un point (.). Les erreurs telles que les erreurs de trame et les erreurs de contrôle de redondance cyclique (CRC) sont indiquées par un X et une description de l'erreur.

Les exemples qui suivent illustrent la sortie des commandes `watch-net` et `watch-net-all`.

```
ok watch-net
1000 Mbps FDXLink up
Link is -- up
Looking for Ethernet Packets.
'.' is a Good Packet. 'X' is a Bad Packet.
Type any key to stop.
.............................
ok
```

```
ok watch-net-all
/pci@1f,0/network@b
1000 Mbps FDXLink up
Link is -- up
Looking for Ethernet Packets.
‘.’ is a Good Packet. ‘X’ is a Bad Packet.
Type any key to stop.
.............................
/pci@1f,0/network@a
1000 Mbps FDXLink up
Link is -- up
Looking for Ethernet Packets.
‘.’ is a Good Packet. ‘X’ is a Bad Packet.
Type any key to stop.
.............................
ok
```

Commande `probe-ide`

La commande `probe-ide` demande au contrôleur IDE du serveur Blade d’envoyer une requête à chacun de ses quatre périphériques IDE possibles (en fait, il n’y a jamais qu’un seul périphérique connecté au contrôleur IDE). Si le résultat de la commande indique `not present` pour le périphérique maître principal, il y a un problème de disque dur ou de connexion au disque dur à partir du contrôleur IDE.

FIGURE 4-2 Message de sortie de `probe-ide`

```
ok probe-ide
 Device 0  ( Primary Master )
          ATA Model: TOSHIBA MK3019GAB

 Device 1  ( Primary Slave )
      Not Present

 Device 2  ( Secondary Master )
      Not Present

 Device 3  ( Secondary Slave )
      Not Present
```

4.5 Utilisation de SunVTS

SunVTS (Sun Validation and Test Suite) est un outil de diagnostic en ligne qui permet de vérifier la configuration et la fonctionnalité des contrôleurs, périphériques et plates-formes matériels. SunVTS est disponible sur le CD *Software Supplement for the Solaris Operating Environment*.

Vous devez l'exécuter à partir d'une invite Solaris :

- interface de ligne de commande
- interface graphique dans un environnement de bureau à fenêtres

Le logiciel SunVTS vous permet d'afficher et de contrôler une session de test sur un serveur connecté à distance. Voici un liste d'exemples de tests :

TABLEAU 4-2 Tests SunVTS

Test SunVTS	Description
disktest	Vérifie les disques locaux
fputest	Vérifie l'unité à virgule flottante
nettest	Vérifie le matériel de mise en réseau sur la carte processeur système et sur les adaptateurs réseau contenus dans le système
pmem	Teste la mémoire physique (lecture uniquement)
vmem	Teste la mémoire virtuelle (combinaison de la partition d'échange et de la mémoire physique)
bsctest	Teste la puce de support du serveur Blade sur le serveur Blade.

4.5.1 Vérification de l'installation de SunVTS

Pour vérifier si SunVTS est déjà installé sur un serveur Blade, tapez :

```
# pkginfo -l SUNWvts
```

- Si le logiciel SunVTS est chargé, des informations sur les modules s'afficheront.
- Si le logiciel SunVTS n'est pas chargé, le message d'erreur suivant s'affichera :

```
ERREUR : information for “SUNWvts” was not found
```

4.5.2 Installation de SunVTS

SunVTS est disponible sur le CD *Software Supplement for the Solaris Operating Environment*. Pour des informations sur son installation, référez-vous au *Sun Hardware Platform Guide*. Le répertoire par défaut à utiliser lors de l'installation du logiciel SunVTS est `/opt/SUNWvts.`

4.5.3 Exécution de SunVTS

Pour tester un serveur Blade Sun Fire B100s en exécutant une session SunVTS à partir d'un poste de travail avec l'interface utilisateur graphique SunVTS, procédez comme suit :

1. **Utilisez la commande `xhost` sur le poste de travail pour donner au serveur Blade l'accès à l'écran local.**

   Tapez :

   ```
   # /usr/openwin/bin/xhost + nomhôte_distant
   ```

   où *nomhôte_distant* est le nom d'hôte du serveur Blade.

2. **Connectez-vous à distance au serveur Blade en tant que superutilisateur ou root.**

3. **Tapez :**

   ```
   # cd /opt/SUNWvts/bin
   # ./sunvts -display nomhôte_local:0
   ```

   où *nomhôte_local* est le nom du poste de travail que vous utilisez.

Remarque - Le répertoire `/opt/SUNWvts/bin` est le répertoire par défaut du logiciel SunVTS. Si le logiciel est installé dans un autre répertoire, utilisez le chemin correspondant à la place.

Lorsque vous lancez le logiciel SunVTS, le noyau SunVTS sonde les périphériques de test et affiche les résultats sur l'écran de sélection des tests. Il y a un test SunVTS associé à chaque périphérique matériel de votre système.

Vous pouvez affiner les tests en sélectionnant les cases à cocher appropriées pour chacun des tests que vous souhaitez exécuter.

CHAPITRE **5**

Installation du châssis dans des réseaux de données et de gestion séparés

Ce chapitre contient les rubriques suivantes :

5.1 Avantage d'avoir deux commutateurs dans le châssis du système

Ce chapitre explique comment configurer le châssis Sun Fire B1600 pour serveurs Blade en vue de son utilisation dans un environnement qui sépare les réseaux de données et de gestion. Les instructions qui suivent vous permettent de tirer avantage de la présence de deux commutateurs dans le châssis du système pour donner à chacun des serveurs Blade deux connexions vers votre réseau.

La FIGURE 5-1 illustre un exemple de réseau contenant un châssis Sun Fire B1600 pour serveurs Blade ; les sections suivantes se basent sur ce diagramme et sur les adresses IP qui y sont marquées pour illustrer les opérations à effectuer.

Ce chapitre comprend également un exemple de fichier `/etc/hosts` et un exemple de fichier `/etc/netmasks`. Ces exemples montrent comment modifier les fichiers sur votre serveur de noms de manière à simplifier le processus (lorsque vous arrivez à la fin du chapitre) de configuration Solaris sur les serveurs Blade dans votre châssis. Utilisez ces exemples de fichiers administratifs comme guide, en remplaçant par vos propres adresses IP et nom d'hôtes ceux qui figurent dans l'exemple de réseau illustré à la FIGURE 5-1.

Remarque - Comme indiqué au chapitre 3, lorsque vous envisagez la façon d'intégrer le châssis du système dans votre environnement de réseau, n'oubliez pas que le châssis Sun Fire B1600 pour serveurs Blade contient deux commutateurs. Alors qu'un seul contrôleur système est actif à la fois dans le châssis, les deux commutateurs sont actifs en permanence. Cela signifie que, dans un châssis qui fonctionne normalement, les deux commutateurs offrent aux serveurs Blade une connexion permanente avec le réseau. Cependant, si un commutateur devient inopérant pour une raison quelconque, l'autre commutateur continue à assurer cette connectivité. (De même, si un des contrôleurs système devient inopérant, le commutateur contenu dans le même module SSC continue à assurer la connectivité réseau ; les commutateurs fonctionnent indépendamment des contrôleurs système, même s'ils sont situés physiquement dans le même boîtier.)

Ce chapitre indique comment tirer avantage de la présence de deux commutateurs en utilisant des VLAN en combinaison avec IPMP (Internet Network Multipathing) de manière à offrir deux connexions entièrement redondantes entre les serveurs Blade et les réseaux de données et de gestion.

Pour profiter de la redondance offerte par le second commutateur contenu dans le châssis du système, nous vous recommandons de :

- toujours utiliser le châssis du système avec deux SSC installés ;
- vous assurer que les connexions câblées entre les huit ports de liaison montante et les sous-réseaux de votre réseau général sont exactement dupliquées sur les huit ports de liaison montante du second commutateur ;
- copier le fichier de configuration du premier commutateur que vous configurez vers le commutateur redondant avant de définir l'adresse IP, le masque de réseau et la passerelle par défaut du commutateur (pour des informations à ce sujet, reportez-vous à la Section A.9, « Copie de la configuration du premier commutateur vers le second » à la page A-10) ;
- spécifier (dans le fichier `/etc/hosts` sur le serveur de noms) les adresses IP appropriées à une configuration IPMP (IP Network Multipathing) prenant en charge des interfaces redondantes avec le réseau de données et le réseau de gestion depuis chaque serveur Blade (voir FIGURE 5-2). Il y a moins d'adresses IP indiquées pour les serveurs Blade à la FIGURE 5-2 que dans l'exemple de fichier `/etc/hosts` au chapitre 3 (voir FIGURE 3-2). En effet, lorsque vous utilisez IPMP, une seule interface publiée est requise pour chaque serveur Blade.
- spécifier les adresses MAC et IP des deux interfaces Ethernet sur chaque serveur Blade lorsque vous utilisez un fichier `/etc/ethers` sur votre serveur de noms.

5.2 Préparation de l'environnement de réseau avec DHCP

Remarque - Si vous utilisez DHCP pour configurer les paramètres IP des deux interfaces sur chaque serveur Blade, vous ne pouvez pas utiliser IPMP pour configurer des connexions redondantes vers le réseau physique ou plusieurs connexions vers des VLAN.

Si vous utilisez DHCP, assurez-vous que le serveur DHCP des contrôleurs système et commutateurs se trouve sur le réseau de gestion et que le serveur DHCP des serveurs Blade se trouve sur le réseau de données.

Pour des informations sur la configuration des serveurs NIS et des serveurs DHCP, reportez-vous aux chapitre 1, chapitre 3 et annexe C.

5.3 Préparation de l'environnement de réseau avec des adresses IP statiques

La FIGURE 5-1 illustre un réseau similaire à l'exemple de configuration du chapitre précédent, mais avec le port de gestion réseau 100 Mbps (NETMGT) des deux SSC maintenant connecté à un commutateur différent des ports de liaison montante de données. Ce nouveau commutateur externe se trouve sur un autre sous-réseau que le commutateur auquel sont connectés les ports de liaison montante de données sur le châssis. C'est un sous-réseau dédié au trafic de gestion du réseau et, par conséquent, il contient également les deux contrôleurs système et les commutateurs du châssis. Un VLAN de gestion (VLAN 2) contient les deux interfaces de contrôleur système et les deux ports de gestion des commutateurs, tandis que tous les serveurs Blade et ports de liaison montante se trouvent sur VLAN 1.

La FIGURE 5-1 montre également la connexion entre l'interface `ce0` de chaque serveur Blade et le commutateur en SSC0 ainsi que la connexion entre l'interface `ce1` de chaque serveur Blade et le commutateur en SSC1. Notez que chaque interface de serveur Blade a maintenant quatre adresses IP associées au lieu d'une. Ces quatre adresses sont utilisées par le pilote IPMP pour permettre aux interfaces de fonctionner comme des connexions redondantes (voir Section 5.5, « Configuration des serveurs Blade avec IPMP pour assurer la résilience du réseau » à la page 5-9).

Comme à la FIGURE 3-1 (voir chapitre 3), un ou plusieurs des huit ports de liaison montante de chaque commutateur de la FIGURE 5-1 sont connectés à un commutateur externe auquel est connecté un serveur NIS (qui contient également un serveur de noms). A ce commutateur externe est également connecté un routeur (adresse IP 192.168.1.1) qui sert de passerelle par défaut entre le châssis Sun Fire B1600 pour serveurs Blade et le réseau général.

Remarque - Notez que, dans la FIGURE 5-1, il n'y a pas de connexion réseau directe entre le port de gestion (NETMGT) du commutateur et les ports des serveurs Blade. Cela signifie que, par défaut, vous ne pouvez pas gérer les serveurs Blade directement à partir du réseau de gestion. C'est une fonction de sécurité visant à protéger le réseau de gestion contre une éventuelle attaque provenant du réseau de données. Pour des informations sur l'autorisation d'un trafic spécifique entre les serveurs Blade et le port de gestion, reportez-vous aux annexe A et chapitre 6.

Avant d'installer le châssis Sun Fire B1600 dans un environnement de réseau tel celui illustré à la FIGURE 5-1 (autrement dit, un environnement où les réseaux de données et de gestion sont séparés), vous devez modifier les fichiers `/etc/hosts`, `/etc/ethers` et `/etc/netmasks` sur vos serveurs de noms Solaris des réseaux de données et de gestion :

- La FIGURE 5-2 montre un exemple de fichier `/etc/hosts` contenant des adresses IP et des noms d'hôtes pour le châssis situé dans le réseau de données dans l'environnement illustré à la FIGURE 5-1.
- La FIGURE 5-2 montre un exemple de fichier `/etc/hosts` contenant des adresses IP et des noms d'hôtes pour les composants du châssis (les deux SSC et leurs commutateurs) inclus dans le réseau de gestion illustré à la FIGURE 5-1.
- La FIGURE 5-3 montre un exemple de fichier `/etc/netmasks` contenant des masques de réseau pour les numéros de réseau IP utilisés dans l'exemple de réseau de la FIGURE 5-1.

Remarque - Pour chaque serveur Blade, seules les adresses IP publiées (pas les adresses IP de test utilisées par IPMP) doivent être enregistrées dans le fichier `/etc/hosts` du serveur de noms. Cependant, les adresses de test de chaque serveur Blade doivent être clairement réservées dans un commentaire de sorte que les autres administrateurs de réseau sachent qu'elles ne sont pas disponibles (voir FIGURE 5-2).

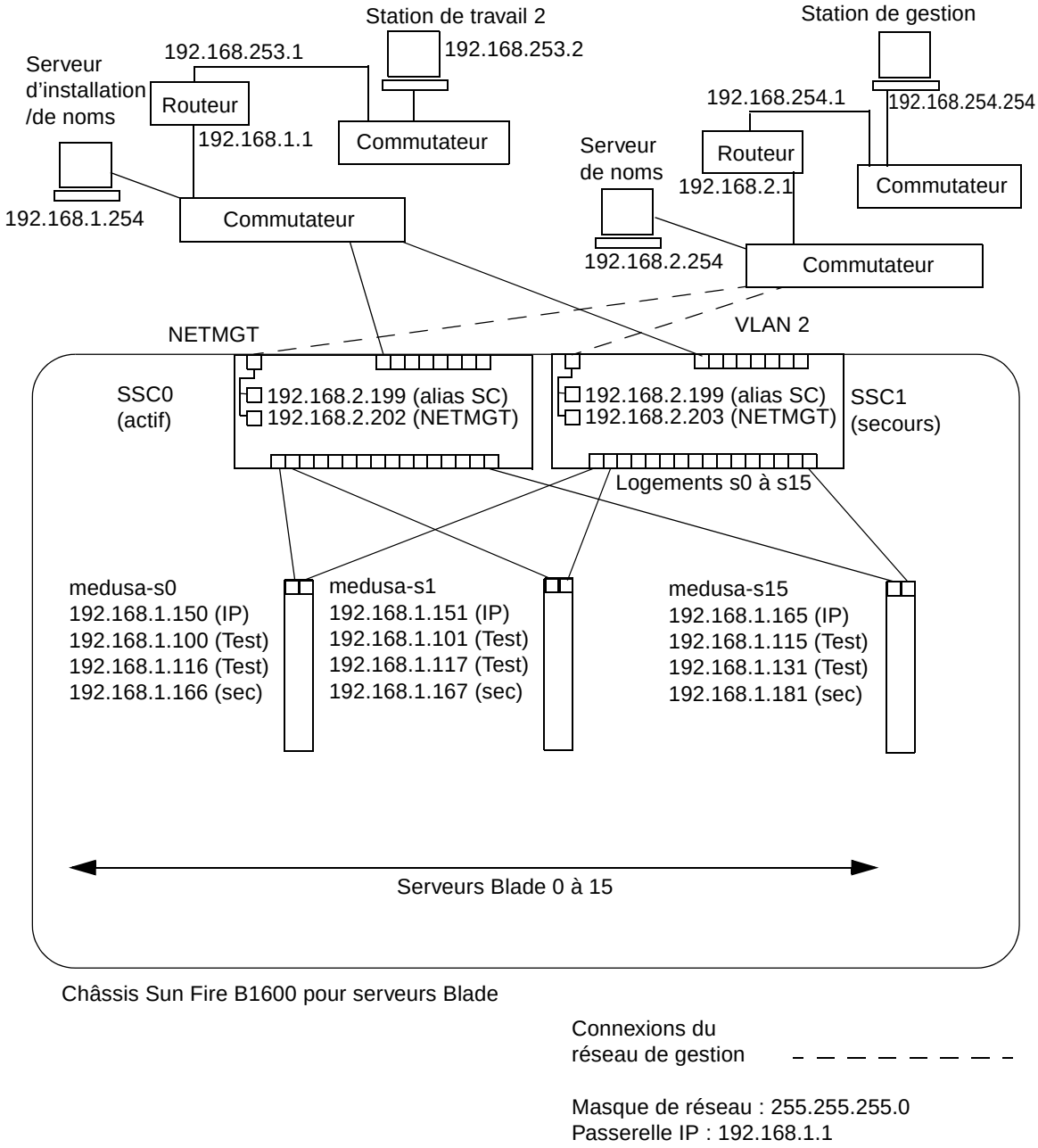

FIGURE 5-1 Exemple de configuration de réseau utilisant un VLAN de gestion

```
# Internet host table

127.0.0.1      localhost

192.168.1.254  datanet-nameserver  # loghost
192.168.1.1    datanet-router-1    # Data network router
                                   # (default gateway)
192.168.2.199  medusa-sc           # Medusa - alias address for active SC

192.168.253.1  datanet-router-253  # Data network router (client side)
192.168.253.2  dataclient-ws1      # Data client network workstation

# 192.168.1.100 -> 192.168.1.131 are reserved for private use by the
# Sun Fire B1600 Blade System Chassis called Medusa. They are test addresses for
# the IPMP driver on each server blade.
#
# Published IP addresses for server blades in Medusa.
192.168.1.150   medusa-s0
192.168.1.151   medusa-s1
192.168.1.152   medusa-s2
192.168.1.153   medusa-s3
192.168.1.154   medusa-s4
192.168.1.155   medusa-s5
192.168.1.156   medusa-s6
192.168.1.157   medusa-s7
192.168.1.158   medusa-s8
192.168.1.159   medusa-s9
192.168.1.160   medusa-s10
192.168.1.161   medusa-s11
192.168.1.162   medusa-s12
192.168.1.163   medusa-s13
192.168.1.164   medusa-s14
192.168.1.165   medusa-s15
```

FIGURE 5-2 Exemple de fichier `/etc/hosts` sur le serveur de noms (du réseau de données)

```
#
# The netmasks file associates Internet Protocol (IP) address
# masks with IP network numbers.
#
#    network-number netmask
#
# The term network-number refers to a number obtained from the
# Internet Network Information Center. Currently this number is
# restricted to being a class A, B, or C network number.
#
# Routing guidelines.
#
# Both the network-number and the netmasks are specified in
# "decimal dot" notation, e.g:
#
#        128.32.0.0 255.255.255.0
#
192.168.1.0   255.255.255.0

192.168.2.0   255.255.255.0
192.168.253.0  255.255.255.0
```

FIGURE 5-3 Exemple de fichier `/etc/netmasks` sur le serveur de noms (du réseau de données)

5.4 Configuration des contrôleurs système et commutateurs

Pour configurer les contrôleurs système et commutateurs pour le type de configuration illustrée à la FIGURE 5-1, suivez les instructions de la Section 3.4, « Configuration des contrôleurs système et commutateurs » à la page 3-7. Cependant, n'oubliez pas que les adresses IP que vous affectez aux contrôleurs système et aux commutateurs doivent se trouver sur le sous-réseau de gestion.

5.5 Configuration des serveurs Blade avec IPMP pour assurer la résilience du réseau

Les instructions de cette section expliquent comment utiliser la fonction IPMP (IP Network Multipathing) de Solaris pour profiter des connexions redondantes entre chaque serveur Blade et les commutateurs du châssis. Les deux interfaces Ethernet 1000Mbps d'un serveur Blade sont appelées respectivement `ce0` et `ce1` (l'interface `ce0` est connectée au commutateur en SSC0 et `ce1` au commutateur en SSC1). Lorsque le châssis Sun Fire B1600 pour serveurs Blade est entièrement opérationel, les deux commutateurs sont constamment actifs.

Le pilote IPMP du serveur Blade fonctionne en envoyant périodiquement un ping à la passerelle par défaut depuis les deux interfaces Ethernet. Si, pour une raison quelconque, un des pings échoue (ce qui indique que le chemin du réseau n'est plus disponible sur l'interface utilisée pour effectuer le ping), le pilote IPMP veille à ce que le trafic réseau utilise uniquement l'interface qui reste valable. Les deux interfaces peuvent être actives (auquel cas elles exigent chacune une adresse IP séparée). Ou bien, une des deux interfaces peut être une interface de secours qui reprend l'adresse IP de l'interface active si celle-ci devient inopérante.

La configuration active/active exige quatre adresses IP : une pour chaque interface plus une adresse de test pour chaque interface. La configuration active/secours exige trois adresses IP. Dans les deux cas, deux adresses de test sont utilisées en privé par le pilote IPMP pour le processus ping. S'il ne reçoit pas de réponse d'un ping sur l'adresse de test associée à une interface, il sait que cette interface est inopérante et il dirige tout le trafic réseau de chaque interface vers l'interface valide. Si vous avez un configuration active/active, il cesse simplement d'utiliser l'interface inopérante. Si vous avez une configuration active/secours et que l'interface inopérante est l'interface active, il affecte l'adresse IP à l'interface de secours, qui devient dès lors l'interface active.

Puisque les deux commutateurs du châssis sont actifs (lorsque le châssis fonctionne normalement), les instructions de ce chapitre vous indiquent comment effectuer une configuration active/active. Pour des informations sur la configuration active/secours, référez-vous au manuel *IP Network Multipathing Administration Guide* (816-0850).

Les adresses IP dont vous avez besoin pour chaque interface physique d'un serveur Blade sont :

- une adresse IP principale,
- une adresse IP secondaire (uniquement requise pour la configuration active/active).

  Les adresses IP principale et secondaire sont (ou peuvent être) toutes deux enregistrées sur un serveur de noms. Ce sont les adresses via lesquelles les autres périphériques du réseau communiquent avec le serveur Blade.

- Deux autres adresses IP sont nécessaires (une par interface) pour le process ping décrit plus haut. Ces deux adresses sont appelées ici « adresses de test ». Elles sont privées pour le pilote IPMP (autrement dit, elles ne sont pas enregistrées sur le serveur de noms).

Les instructions de ce chapitre indiquent comment configurer IPMP pour deux interfaces physiques. Le chapitre suivant explique comment configurer plusieurs paires d'interfaces IPMP virtuelles, chaque paire fournissant des interfaces redondantes pour des VLAN séparés.

5.5.1 Configuration du serveur Blade

Cette section explique comment configurer IPMP sur un serveur Blade de sorte que les deux interfaces Ethernet émettent et reçoivent activement des données. A des fins d'illustration, les instructions utilisent un exemple de configuration inspiré du scénario de réseau décrit à la Section 5.3, « Préparation de l'environnement de réseau avec des adresses IP statiques » à la page 5-4.

Le TABLEAU 5-1 résume les informations que vous devriez fournir au pilote IPMP sur le serveur Blade inséré dans le logement 0 du châssis illustré à la FIGURE 5-1.

Remarque - Vous devez exécuter les instructions de cette section sur chaque serveur Blade exigeant une connexion redondante avec le réseau.

TABLEAU 5-1 Exemple de configuration IPMP pour un serveur Blade

Variable de configuration IPMP	Valeur pour l'exemple de serveur Blade dans le logement 0
Interfaces de carte réseau	`ce0` (active) `ce1` (active)
Nom du groupe d'interfaces	`medusa_grp0`
Adresse IP et nom d'hôte (principaux)	192.168.1.150 (`medusa-s0`)
Adresse IP et nom d'hôte (secondaires)	192.168.1.166 (`medusa-s0-sec`)
Adresse IP de test et nom d'hôte (`ce0`)	192.168.1.100 (medusa-s0-0)
Adresse IP de test et nom d'hôte (`ce1`)	192.168.1.116 (medusa-s0-1)
Masque de réseau	255.255.255.0
Le serveur Blade doit-il assurer le routage réseau ?	Non

1. **Effectuez une configuration préliminaire de Solaris en suivant les instructions du chapitre 3.**

   Cela fait, tapez #. pour retourner à l'invite `sc>` à partir d'une console de serveur Blade.

2. **Connectez-vous comme utilisateur root à la console du serveur Blade dont vous souhaitez configurer les interfaces.**

   A l'invite `sc>`, tapez la commande suivante :

```
sc> console sn
```

   où *n* est le numéro de logement contenant le serveur Blade auquel vous voulez vous connecter.

3. **Modifiez le fichier `/etc/hosts` du serveur Blade pour ajouter ses deux adresses IP de test.**

   Pour un serveur Blade utilisant les exemples d'adresses indiquées au TABLEAU 5-1, vous devriez ajouter les deux dernières lignes du fichier suivant :

```
#
# /etc/hosts on the server blade in system chassis Medusa, slot 0
#
127.0.0.1    localhost    loghost

192.168.1.150  medusa-s0    # Data Address
192.168.1.166  medusa-s0-sec  # Secondary Data Address
192.168.1.100  medusa-s0-0   # Test Address for ce0
192.168.1.116  medusa-s0-1   # Test Address for ce1
```

4. **Définissez le masque de réseau dans le fichier `/etc/netmasks` du serveur Blade.**

   Pour un serveur Blade utilisant les exemples d'adresses indiquées au TABLEAU 5-1, vous devriez ajouter la ligne suivante :

```
192.168.1.0   255.255.255.0
```

5. **Désactivez le routage, car le serveur Blade n'est pas utilisé pour effectuer le routage.**

   Tapez :

```
# touch /etc/notrouter
# ndd -set /dev/ip ip_forwarding 0
```

6. **Créez les interfaces réseau en tapant :**

```
# ifconfig ce0 plumb
# ifconfig ce1 plumb
```

7. **Créez un groupe IPMP intitulé** `medusa_grp0` **et contenant les interfaces réseau** `ce0` **et** `ce1` **:**

```
# ifconfig ce0 group medusa_grp0
# ifconfig ce1 group medusa_grp0
```

Lorsque vous exécutez ces commandes, les messages `syslog` suivants peuvent apparaître :

```
Sep 3 00:49:58 medusa-s0 in.mpathd[298]: Failures cannot be
detected on ce0 as no IFF_NOFAILOVER address is available
```

Ces messages avertissent simplement que les pannes ne peuvent pas être détectées tant que des adresses test n'ont pas été définies sur les interfaces.

8. **Créez une adresse pour la transmission de données sur** `ce0` **et** `ce1` **et marquez-la comme** `failover` **en cas de détection d'une défaillance dans une interface.**

```
# ifconfig ce0 medusa-s0 netmask + broadcast + failover up
Setting netmask of ce0 to 255.255.255.0

# ifconfig ce1 medusa-s0-sec netmask + broadcast + failover up
Setting netmask of ce1 to 255.255.255.0
```

9. **Configurez une adresse de test sur chaque interface réseau.**

   Ces adresses seront utilisées par `mpathd` pour détecter des pannes d'interface. Vous devez utiliser l'indicateur `-failover`. Avec cet indicateur, `in.mpathd` utilise l'adresse comme adresse de test (autrement dit, une adresse qui ne peut pas être transférée à l'autre interface et n'offre donc pas de redondance) :

```
# ifconfig ce0 addif medusa-s0-0 netmask + broadcast + -failover
deprecated up
Created new logical interface ce0:1
Setting netmask of ce0:1 to 255.255.255.0

# ifconfig ce1 addif medusa-s0-1 netmask + broadcast + -failover
deprecated up
Created new logical interface ce1:1
Setting netmask of ce1:1 to 255.255.255.0
```

10. **Pour permettre à la nouvelle configuration des interfaces de survivre à un redémarrage, créez un fichier `hostname.ce0` et un fichier `hostname.ce1` dans le répertoire `/etc`.**

    Voici un exemple de fichier pour `hostname.ce0` :

```
medusa-s0 netmask + broadcast + \
group medusa_grp0 up \
addif medusa-s0-0 deprecated -failover \
netmask + broadcast + up
```

    Voici un exemple de fichier pour `hostname.ce1` :

```
medusa-s0-sec netmask + broadcast + \
group medusa_grp0 up \
addif medusa-s0-1 deprecated -failover \
netmask + broadcast + up
```

11. **Inspectez la configuration des deux adaptateurs de réseau.**

    Tapez :

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
        inet 127.0.0.1 netmask ff000000
ce0: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 2
        inet 192.168.1.150 netmask ffffff00 broadcast 192.168.1.255
        groupname medusa_grp0
        ether 0:3:ba:19:26:3
ce0:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4, NOFAILOVER> mtu 1500 index 2
        inet 192.168.1.100 netmask ffffff00 broadcast 192.168.1.255
ce1: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4> mtu 1500 index 3
        inet 192.168.1.166 netmask ffffff00 broadcast 192.168.1.255
        groupname medusa_grp0
        ether 0:3:ba:19:26:4
ce1:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4, NOFAILOVER> mtu 1500 index 3
        inet 192.168.1.116 netmask ffffff00 broadcast 192.168.1.255
```

La sortie ci-dessus montre que quatre adresses ont été définies (les exemples d'adresses du TABLEAU 5-1). Les deux adresses de test IPMP (associées à `ce0:1` et `ce1:1`, respectivement) sont marquées NOFAILOVER. Cela signifie qu'elles ne seront pas transférées vers l'interface restante en cas de défaillance.

12. **Testez IPMP en retirant temporairement un SSC du châssis.**

    Les messages d'erreur suivants apparaîtront sur la console :

```
Sep 3 01:08:50 medusa-s0 in.mpathd[29]: NIC failure detected on
ce0 of group medusa_grp0
Sep 3 01:08:50 medusa-s0 in.mpathd[29]: Successfully failed over
from NIC ce0 to NIC ce1
```

Remarque - Il faut environ 10 secondes au démon IPMP pour détecter et se remettre d'une panne réseau avec la configuration par défaut. La configuration du démon IPMP est définie dans le fichier `/etc/default/mpathd`.

CHAPITRE **6**

Ajout de la gestion des serveurs Blade et marquage des VLAN

Ce chapitre explique comment configurer le châssis du système de manière à permettre une gestion sécurisée des serveurs Blade à partir du réseau de gestion.

Ce chapitre contient les rubriques suivantes :

6.1 Introduction

Ce chapitre explique comment affiner la configuration définie au chapitre 5 pour permettre aux administrateurs de réseau d'effectuer des tâches de gestion sur les serveurs Blade à partir du réseau de gestion (au travers de connexions telnet directes avec les serveurs Blade) sans compromettre la sécurité du réseau de gestion.

Dans la FIGURE 6-1, des lignes pointillées relient les ports des serveurs Blade des commutateurs du châssis au port de gestion (NETMGT). Il y a également des lignes pointillées entre les serveurs Blade eux-mêmes et le port de gestion de chaque commutateur. Ces lignes pointillées représentent des liaisons entre des composants ou périphériques qui sont membres du VLAN de gestion (VLAN 2). Par défaut, VLAN 2, qui contient le port de gestion (NETMGT) du commutateur, ne comprend aucun port de serveur Blade. Dès lors, pour configurer le châssis de sorte qu'il prenne en charge un environnement de réseau tel que celui illustré à la FIGURE 6-1, vous devez reconfigurer ces ports manuellement. Pour plus d'informations à ce sujet, reportez-vous à la Section 6.3, « Configuration du contrôleur système et des commutateurs » à la page 6-5.

De même, par défaut, aucun trafic réseau n'est autorisé à passer des ports de serveur Blade (au travers du filtre de paquets du commutateur) au port de gestion. Cette restriction est une mesure de sécurité. Vous devez être prudent lorsque vous configurez le commutateur pour qu'il autorise le passage du trafic dans son filtre de paquets. La Section A.11, « Utilisation du filtre de paquets sur le commutateur pour assurer une gestion sûre des serveurs Blade » à la page A-16 explique comment n'autoriser que des protocoles spécifiques à passer au travers du filtre de paquets.

Enfin, puisque ce chapitre vous explique comment inclure les serveurs Blade dans le réseau de gestion (VLAN 2), il explique également comment modifier la configuration IPMP des serveurs Blade pour que chaque serveur Blade ait non seulement une connexion redondante avec le réseau de données (comme décrit au chapitre 5), mais aussi une connexion redondante avec le réseau de gestion (VLAN 2).

6.2 Préparation de l'environnement de réseau

Cette section reprend l'exemple de configuration du chapitre précédent, mais avec les améliorations décrites dans l'introduction ci-dessus, plus des exemples des informations IPMP requises pour créer les connexions redondantes entre chaque serveur Blade et le réseau de gestion. Cette section contient également un exemple de fichier `/etc/hosts` pour le serveur de noms du réseau de gestion. Les fichiers d'administration du réseau de données restent les mêmes qu'au chapitre 5. Cependant, le fichier `/etc/hosts` du serveur de noms du réseau de gestion doit contenir des adresses IP (sur le sous-réseau de gestion) pour chaque serveur Blade ainsi que pour les deux SSC et commutateures du châssis (voir FIGURE 6-2).

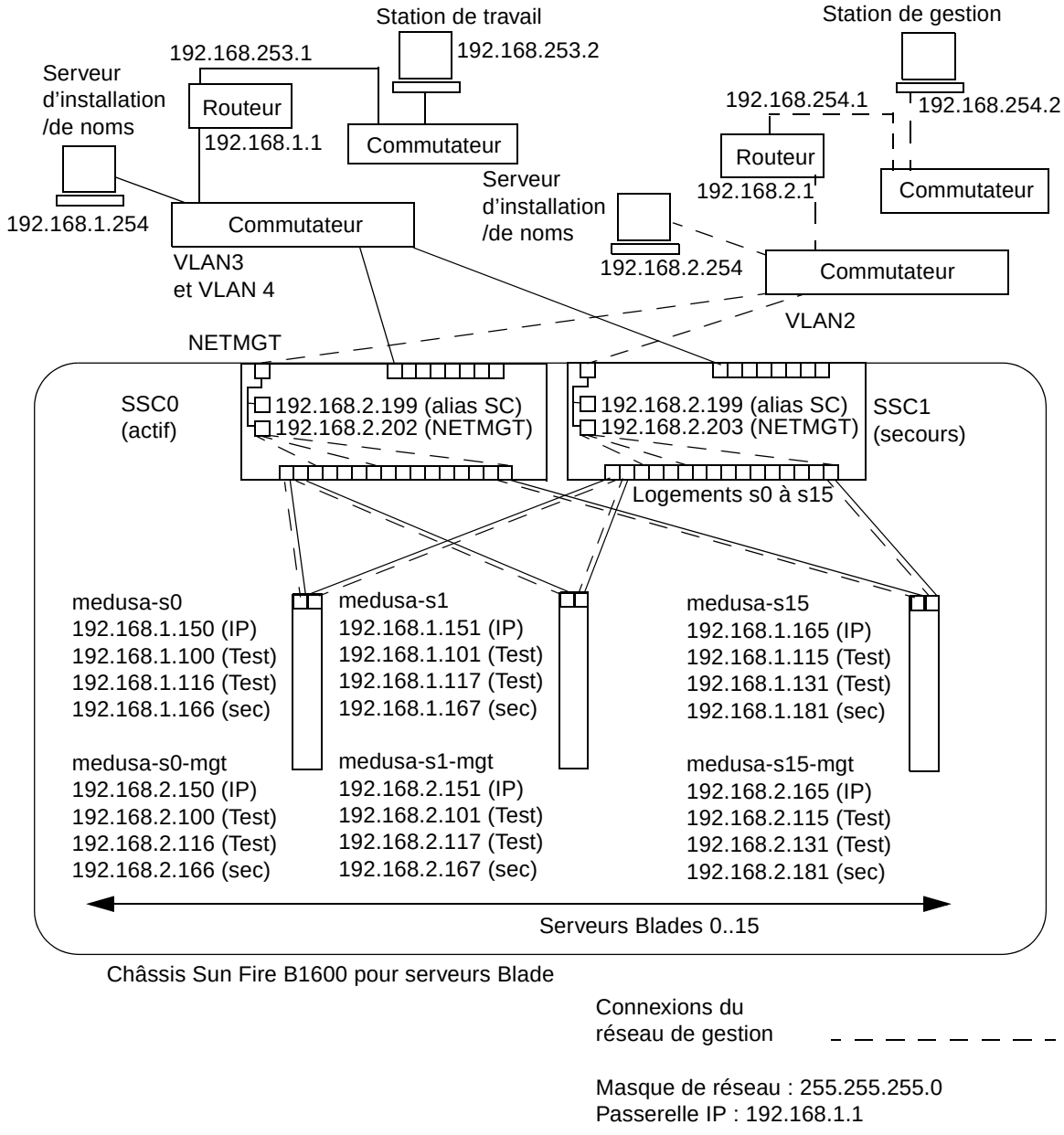

FIGURE 6-1 Exemple de configuration de réseau avec un VLAN de gestion qui inclut les serveurs Blade

```
# Internet host table
# This is the sample /etc/hosts file for the name-server on the management
# network.

192.168.2.1   mgtnet-router-1  # Management network router
#                 (default gateway)
192.168.2.254  mgtnet-nameserver # Management network install/name server
192.168.254.1  mgtnet-router-254 # Management network router (client side)
192.168.254.2  mgtnet-ws     # Management network workstation

192.168.2.199  medusa-sc     # Medusa - alias IP address for active SC
192.168.2.200  medusa-ssc0    # Medusa - ssc0/sc
192.168.2.201  medusa-ssc1    # Medusa - ssc1/sc
192.168.2.202  medusa-swt0    # Medusa - ssc0/swt
192.168.2.203  medusa-swt1    # Medusa - ssc1/swt

# 192.168.2.100 -> 192.168.2.131 are reserved for private use by the
# Sun Fire B1600 Blade System Chassis called medusa. They are test addresses for
# the IPMP driver on each server blade.

192.168.2.150  medusa-s0-mgt
192.168.2.151  medusa-s1-mgt
192.168.2.152  medusa-s2-mgt
192.168.2.153  medusa-s3-mgt
192.168.2.154  medusa-s4-mgt
192.168.2.155  medusa-s5-mgt
192.168.2.156  medusa-s6-mgt
192.168.2.157  medusa-s7-mgt
192.168.2.158  medusa-s8-mgt
192.168.2.159  medusa-s9-mgt
192.168.2.160  medusa-s10-mgt
192.168.2.161  medusa-s11-mgt
192.168.2.162  medusa-s12-mgt
192.168.2.163  medusa-s13-mgt
192.168.2.164  medusa-s14-mgt
192.168.2.165  medusa-s15-mgt
```

FIGURE 6-2 Exemple de fichier `/etc/hosts` sur le serveur de noms (du réseau de gestion)

6.3 Configuration du contrôleur système et des commutateurs

Si vous avez déjà configuré le contrôleur système et les commutateurs du châssis conformément aux instructions des chapitres précédents, passez directement à la Section 6.3.1, « Ajout des serveurs Blade au VLAN de gestion sur les commutateurs en SSC0 et SSC1 » à la page 6-5.

Sinon, suivez les instructions du chapitre 5, mais ne configurez pas le commutateur en SSC1, car les instructions ci-dessous (Section 6.3.1, « Ajout des serveurs Blade au VLAN de gestion sur les commutateurs en SSC0 et SSC1 » à la page 6-5) impliquent la copie de la configuration entière du commutateur en SSC0 vers le commutateur en SSC1.

6.3.1 Ajout des serveurs Blade au VLAN de gestion sur les commutateurs en SSC0 et SSC1

Les instructions de cette section expliquent comment ajouter les serveurs Blade au VLAN de gestion, qui est par défaut le VLAN 2 (autrement dit, par défaut, VLAN2 contient le port de gestion, NETMGT). VLAN 1 est également défini par défaut sur le commutateur. Ce VLAN contient tous les ports de serveur Blade et de liaison montante du commutateur. Cependant, pour illustrer l'utilisation des fonctions de configuration VLAN du commutateur, les instructions de cette section utiliseront VLAN 3 au lieu de VLAN 1 pour le réseau de données.

Dans ces instructions, le VLAN de gestion (VLAN 2) et le VLAN de données (VLAN 3) sont marqués. Cependant, les instructions vous invitent également à créer un VLAN supplémentaire pour le démarrage des serveurs Blade (VLAN 4). Ce VLAN supplémentaire traite le trafic non marqué généré par les serveurs Blade durant l'installation réseau de l'environnement d'exploitation Solaris.

Ce trafic sur le VLAN de démarrage (VLAN 4) peut être marqué ou non lorsqu'il quitte le châssis du système. Dans les exemples de commandes de cette section, il est marqué. (Les instructions supposent que les périphériques extérieurs au châssis reconaissent les VLAN et VLAN 4 est supposé contenir le serveur NIS utilisé par les serveurs Blade.)

Remarque - Si vous réinitialisez le commutateur alors que vous êtes en train d'exécuter les instructions de cette section, vous devez commencer par enregistrer la configuration. Si vous ne le faites pas, vous perdrez toutes les modifications apportées. Pour enregistrer la configuration, suivez les instructions de la Section A.8, « Enregistrement des paramètres du commutateur » à la page A-9.

---

1. **A partir de l'invite `sc>`, connectez-vous à la console pour configurer le commutateur en SSC0.**

   Pour vous connecter au commutateur en SSC0, tapez :

```
sc> console ssc0/swt
```

2. **A l'invite, tapez votre nom d'utilisateur et votre mot de passe.**

3. **A l'invite `Console#` de la ligne de commande, tapez :**

```
Console#configure
```

4. **Accédez à la base de données VLAN du commutateur en tapant :**

```
Console(config)#vlan database
```

5. **Configurez le VLAN pour le réseau de données et pour le réseau de démarrage en tapant :**

```
Console(config-vlan)#vlan 3 name Data media ethernet
Console(config-vlan)#vlan 4 name Boot media ethernet
```

6. **Quittez la base de données VLAN en tapant :**

```
Console(config-vlan)#end
```

7. **Ajoutez le port de serveur Blade `SNP0` au VLAN de gestion (VLAN 2), au VLAN de données (VLAN 3) et au VLAN que vous utilisez pour le démarrage (VLAN 4).**

   Pour ce faire, tapez les commandes suivantes :

```
Console#configure
Console(config)#interface ethernet SNP0
Console(config-if)#switchport allowed vlan add 2 tagged
Console(config-if)#switchport allowed vlan add 3 tagged
Console(config-if)#switchport allowed vlan add 4
Console(config-if)#switchport native vlan 4
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#exit
Console(config)#
```

Cette séquence a la signification suivante :

- La commande `interface ethernet SNP0` spécifie le port de serveur Blade que vous configurez (en l'occurrence, le port `SNP0`).
- La commande `switchport allowed vlan add 2 tagged` fait de ce port de serveur Blade un membre de VLAN 2 (le réseau de gestion) et lui permet de transmettre le trafic marqué au réseau de gestion.
- La commande `switchport allowed vlan add 3 tagged` fait du port un membre de VLAN 3 (le nouveau réseau de données) et lui permet de transmettre le trafic marqué au réseau de données.
- La commande `switchport allowed vlan add 4` fait du port un membre de VLAN 4. Elle enjoint au port d'accepter les paquets non marqués et de les marquer comme membres de VLAN 4. Ce faisant, vous fournissez un chemin permettant au trafic non marqué généré par le serveur Blade (pendant le démarrage) d'atteindre le serveur NIS. Dans la commande qui suit, vous allez faire de ce VLAN le VLAN naturel, autrement dit, le VLAN auquel sont transmises toutes les trames non marquées.
- La commande `switchport native vlan 4` enjoint au port de placer sur VLAN 4 toutes les trames non marquées qu'il reçoit. (OBP et Jumpstart impliquent des serveurs Blade dans l'envoi de trames non marquées.)
- La commande `switchport allowed vlan remove 1` supprime le port de VLAN 1 (le VLAN par défaut sur le commutateur pour tous les ports de serveur Blade et les ports de liaison montante).

Répétez l'étape 7 pour tous les ports de serveur Blade restants (`SNP1` à `SNP15`). Tous ces ports doivent être inclus à la fois dans le réseau de gestion et dans le réseau de données.

Pour inspecter le port que vous avez configuré, tapez :

```
Console#show interfaces switchport ethernet SNP0
Information of SNP0
 Broadcast threshold: Enabled, 256 packets/second
 Lacp status: Disabled
 VLAN membership mode: Hybrid
 Ingress rule: Disabled
 Acceptable frame type: All frames
 Native VLAN: 4
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan:  2(t), 3(t), 4(u)
 Forbidden Vlan:
Console#
```

8. **Si vous prévoyez de regrouper des ports de liaison montante de données, faites-le maintenant.**

   Suivez les instructions de la Section A.10, « Configuration de connexions groupées à des fins de résilience et de performances » à la page A-15.

9. **Ajoutez des ports de liaison montante de données (non regroupés) au VLAN de données (VLAN 3) et au VLAN de démarrage (VLAN 4) en tapant les commandes suivantes :**

```
Console#configure
Console(config)#interface ethernet NETP0
Console(config-if)#switchport allowed vlan add 3 tagged
Console(config-if)#switchport allowed vlan add 4
Console(config-if)#switchport native vlan 4
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#no switchport gvrp
Console(config-if)#switchport forbidden vlan add 2
Console(config-if)#end
Console(config)#
```

- La commande `interface ethernet NETP0` spécifie le port de liaison montante que vous configurez.
- La commande `switchport allowed vlan add 3 tagged` ajoute ce port de liaison montante au réseau de données (VLAN 3).
- La commande `switchport allowed vlan add 4` ajoute ce port de liaison montante à un VLAN non marqué que vous utilisez pour le démarrage des serveurs Blade (VLAN 4). Dans la commande qui suit, vous allez faire de ce VLAN le VLAN naturel (autrement dit, le VLAN auquel ce port de données transmet toutes les trames non marquées).
- La commande `switchport native vlan 4` enjoint au port de données externe de placer sur VLAN 4 toutes les trames non marquées qu'il reçoit. (L'effet de cette commande est temporaire ; les commandes qui suivent empêchent le port d'accepter les trames non marquées. Cette commande est néanmoins nécessaire, car le commutateur exige qu'un VLAN naturel soit disponible jusqu'à ce que la commande `switchport mode trunk` ait été exécutée.)
- La commande `switchport allowed vlan remove 1` retire ce port de liaison montante de VLAN 1 (le VLAN par défaut). Ce VLAN peut uniquement être supprimé à ce stade (après la création de VLAN 4 - le VLAN naturel, non marqué).
- Les commandes `switchport ingress-filtering`, `switchport mode trunk` et `switchport acceptable-frame-types tagged` enjoignent au port de rejeter toute trame non marquée pour le ou les VLAN particuliers dont il est membre.
- La commande `no switchport gvrp` empêche le port d'utiliser GVRP pour annoncer les VLAN dont il est membre (en l'occurrence, VLAN 3) à un autre commutateur auquel il est connecté.

- La commande `switchport forbidden vlan add 2` empêche l'ajout du port de liaison montante à VLAN 2 en réponse à une demande GVRP émanant d'un autre commutateur du réseau.

Pour inspecter un port que vous avez configuré, tapez :

```
Console#show interfaces switchport ethernet NETP0
Information of NETP0
 Broadcast threshold: Enabled, 256 packets/second
 Lacp status: Disabled
 VLAN membership mode: Trunk
 Ingress rule: Enabled
 Acceptable frame type: Tagged frames only
 Native VLAN: 4
 Priority for untagged traffic: 0
 Gvrp status: Disabled
 Allowed Vlan:  3(t), 4(t)
 Forbidden Vlan:  2,
Console#
```

10. Ajoutez tout groupe de connexions au VLAN de données (VLAN 3) en tapant les commandes ci-dessous.

Pour plus d'informations sur l'utilisation de connexions groupées, reportez-vous au chapitre A.

Dans l'exemple ci-dessous, le groupe est appelé port-channel 1. La commande interface port-channel 1 spécifie le groupe que vous vous apprêtez à configurer.

```
Console(config)#interface port-channel 1
Console(config-if)#switchport allowed vlan add 3 tagged
Console(config-if)#switchport allowed vlan add 4
Console(config-if)#switchport native vlan 4
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#no switchport gvrp
Console(config-if)#switchport forbidden vlan add 2
Console(config-if)#end
Console(config)#
```

11. **Ajoutez tous les ports de liaison montante à VLAN 3, individuellement ou en groupes (voir étape 9 et étape 10).**

    Par exemple, si les ports NETP1, NETP2 et NETP3 sont regroupés dans groupe 1 et si NETP4 et NETP5 sont regroupés dans groupe 2, vous devrez ajouter les ports NETP0, NETP6 et NETP7 ainsi que groupe 1 et groupe 2 à VLAN 3.

12. **Suivez les instructions de la Section A.11, « Utilisation du filtre de paquets sur le commutateur pour assurer une gestion sûre des serveurs Blade » à la page A-16.**

13. **Enregistrez les modifications apportées à la configuration du commutateur en SSC0.**

    Pour ce faire, suivez les instructions de la Section A.8, « Enregistrement des paramètres du commutateur » à la page A-9.

14. **Copiez la configuration du commutateur en SSC0 vers le commutateur en SSC1.**

    Suivez les instructions de la Section A.9, « Copie de la configuration du premier commutateur vers le second » à la page A-10.

15. **Tapez `#.` pour quitter l'interface de ligne de commande du commutateur et retourner au contrôleur système.**

16. **A partir de l'invite `sc>`, connectez-vous au commutateur en SSC1 en tapant :**

```
sc> console ssc1/swt
```

17. **Tapez votre nom d'utilisateur et votre mot de passe.**

18. **Réglez l'adresse IP, le masque de réseau et la passerelle par défaut pour le commutateur en SSC1.**

    Pour ce faire, suivez les instructions de la Section A.6, « Réglage de l'adresse IP, du masque de réseau et de la passerelle par défaut du commutateur » à la page A-6.

19. **Enregistrez les modifications apportées à la configuration du commutateur en SSC1.**

    Pour ce faire, suivez les instructions de la Section A.8, « Enregistrement des paramètres du commutateur » à la page A-9.

20. **Tapez `#.` pour quitter l'interface de ligne de commande du commutateur et retourner à l'invite `sc>`.**

21. **Suivez les instructions de la Section 6.4, « Configuration des serveurs Blade avec IPMP pour assurer la résilience du réseau (marquage VLAN) » à la page 6-11.**

6.4 Configuration des serveurs Blade avec IPMP pour assurer la résilience du réseau (marquage VLAN)

La configuration des commutateurs effectuée dans la section précédente utilise des VLAN marqués pour séparer les réseaux de données et de gestion. Pour qu'IPMP fonctionne avec cette configuration des commutateurs, il vous faut quatre adresses IP pour *chaque* VLAN dont le serveur Blade est membre. (Autrement dit, il vous faut huit adresses IP, quatre pour le VLAN de gestion et quatre pour le VLAN de données.)

En effet, le pilote IPMP prend en charge les VLAN marqués en utilisant une paire séparée d'interfaces logiques Ethernet pour chaque VLAN. Ces interfaces logiques doivent chacune être nommées manuellement selon une formule simple :

`ce`(*id VLAN* x 1000) + *instance*

où *id VLAN* est le numéro du VLAN (configuré sur les ports de commutateur auxquels le serveur Blade est connecté dans le châssis) et *instance* est 0 ou 1 selon que l'interface logique est associée à l'interface physique `ce0` ou `ce1`.

La création de ces paires d'interfaces Ethernet logiques fait en sorte que les trames destinées à un réseau parviennent à ce réseau et pas à un autre. Chaque fois que le pilote IPMP doit envoyer une trame au commutateur, il la marque en fonction du VLAN destiné à la recevoir, puis la transmet sur l'une des deux interfaces logiques disponibles pour ce VLAN. Un des commutateurs reçoit alors la trame (sur le port dédié au serveur Blade particulier qui l'a envoyée). Et, en supposant que le commutateur a été configuré pour accepter les trames destinées au VLAN indiqué, il transmet la trame à ce VLAN.

L'important est que le pilote IPMP du serveur Blade a transmis la trame à un VLAN particulier et, pour ce faire, a utilisé une connexion virtuelle redondante vers ce VLAN. Les autres VLAN dont le serveur Blade est membre ont été empêchés de recevoir la trame.

6.4.1 Configuration du serveur Blade (marquage VLAN)

Cette section explique comment configurer IPMP sur un serveur Blade de sorte que les deux interfaces Ethernet fournissent deux interfaces logiques actives (une avec le VLAN de données et une au VLAN de gestion).

A des fins d'illustration, les instructions ci-dessous utilisent un exemple de configuration inspiré du scénario de réseau décrit à la Section 6.2, « Préparation de l'environnement de réseau » à la page 6-2. Elles supposent que la configuration des serveurs Blade pour IPMP décrite au chapitre 5 a déjà été effectuée.

Le TABLEAU 6-1 résume les informations que vous devriez fournir au pilote IPMP sur le serveur Blade inséré dans le logement 0 du châssis illustré à la FIGURE 6-1.

Remarque - Vous devez exécuter les instructions de cette section sur chaque serveur Blade exigeant une connexion redondante avec le réseau de données et le réseau de gestion.

TABLEAU 6-1 Exemple de configuration IPMP pour un serveur Blade (marquage VLAN)

Variable de configuration IPMP	Valeur pour l'exemple de serveur Blade dans le logement 0
interfaces de carte réseau	`ce2000` (active) `ce2001` (active) `ce3000` (active) `ce3001` (active)
Noms de groupes d'interfaces	`medusa_grp0-mgt` `medusa_grp0`
Adresse IP de test et nom d'hôte (`ce2000/1`) Adresse IP de test et nom d'hôte (`ce3000/1`)	192.168.2.150 (medusa-s0-mgt) 192.168.1.150 (medusa-s0)
Adresse IP et nom d'hôte (réseau de gestion) Adresse IP et nom d'hôte (réseau de données)	192.168.2.150 (medusa-s0-mgt) 192.168.1.150 (medusa-s0)
Adresse IP et nom d'hôte secondaires (réseau de gestion) Adresse IP et nom d'hôte secondaires (réseau de données)	192.168.2.166 (medusa-s0-mgt-sec) 192.168.1.166 (medusa-s0-sec)
Adresse IP de test et nom d'hôte (`ce2000`) Adresse IP de test et nom d'hôte (`ce2001`)	192.168.2.100 medusa-s0-0 192.168.2.116 medusa-s0-1
Adresse IP de test et nom d'hôte (`ce3000`) Adresse IP de test et nom d'hôte (`ce3001`)	192.168.1.100 medusa-s0-0 192.168.1.116 medusa-s0-1
Masque de réseau	255.255.255.0
Le serveur Blade doit-il assurer le routage réseau ?	Non

1. **Effectuez une configuration préliminaire de Solaris en suivant les instructions du chapitre 3.**

   Cela fait, tapez #. pour retourner à l'invite `sc>` à partir d'une console de serveur Blade.

2. **Connectez-vous à la console du serveur Blade dont vous souhaitez configurer les interfaces.**

   A l'invite `sc>`, tapez la commande suivante :

```
sc> console sn
```

   où *n* est le numéro de logement contenant le serveur Blade auquel vous voulez vous connecter.

3. **Modifiez le fichier `/etc/hosts` du serveur Blade pour ajouter l'adresse IP des interfaces de gestion.**

   Pour un serveur Blade utilisant les exemples d'adresses indiquées au TABLEAU 6-1, vous devriez ajouter les deux dernières lignes du fichier suivant :

```
#
# /etc/hosts on the server blade in system chassis Medusa, slot 0
#
127.0.0.1    localhost     loghost

192.168.1.150  medusa-s0     # Data Address
192.168.1.166  medusa-s0-sec   # Secondary Data Address
192.168.1.100  medusa-s0-0    # Test Address for ce0
192.168.1.116  medusa-s0-1    # Test Address for ce1

192.168.2.150  medusa-s0-mgt    # Data Address
192.168.2.166  medusa-s0-mgt-sec  # Secondary Data Address
192.168.2.100  medusa-s0-mgt-0   # Test Address for ce0
192.168.2.116  medusa-s0-mgt-1   # Test Address for ce1
```

4. **Définissez le masque de réseau dans le fichier `/etc/netmasks` du serveur Blade.**

   Pour un serveur Blade utilisant les exemples d'adresses indiquées au TABLEAU 6-1, vous devriez ajouter la ligne suivante :

```
192.168.1.0   255.255.255.0
192.168.2.0   255.255.255.0
```

5. **Désactivez le routage car le serveur Blade n'est pas utilisé pour effectuer le routage.**

   Tapez :

```
# touch /etc/notrouter
# ndd -set /dev/ip ip_forwarding 0
```

6. **Déplombez les interfaces réseau existantes en tapant :**

```
# ifconfig ce0 unplumb
# ifconfig ce1 unplumb
```

Si une des interfaces n'a pas été préalablement configurée, vous pouvez recevoir le message d'erreur suivant :

```
ifconfig: unplumb: SIOCGLIFFLAGS: ce1: no such interface
```

7. **Créez les nouvelles interfaces en tapant :**

```
# ifconfig ce2000 plumb
# ifconfig ce2001 plumb
# ifconfig ce3000 plumb
# ifconfig ce3001 plumb
```

8. **Créez les groupes de reprise IPMP contenant les nouvelles interfaces :**

```
# ifconfig ce2000 group medusa_grp0-mgt
# ifconfig ce2001 group medusa_grp0-mgt
# ifconfig ce3000 group medusa_grp0
# ifconfig ce3001 group medusa_grp0
```

Lorsque vous exécutez ces commandes, des messages `syslog` du type suivant peuvent apparaître :

```
Sep 3 00:49:58 medusa-s0 in.mpathd[298]: Failures cannot be
detected on ce0 as no IFF_NOFAILOVER address is available
```

Ces messages avertissent simplement que les pannes ne peuvent pas être détectées tant que des adresses test n'ont pas été définies sur les interfaces.

9. **Créez une adresse pour la transmission de données sur chaque nouvelle interface et marquez-la comme `failover` en cas de détection d'une défaillance dans une interface.**

```
# ifconfig ce2000 medusa-s0-mgt netmask + broadcast + failover up
Setting netmask of ce2000 to 255.255.255.0
#
# ifconfig ce2001 medusa-s0-mgt-sec netmask + broadcast + failover
up
Setting netmask of ce2001 to 255.255.255.0
#
# ifconfig ce3000 medusa-s0 netmask + broadcast + failover up
Setting netmask of ce3000 to 255.255.255.0
#
# ifconfig ce3001 medusa-s0-sec netmask + broadcast + failover up
Setting netmask of ce3001 to 255.255.255.0
```

10. **Configurez une adresse de test sur chaque interface réseau.**

    Ces adresses seront utilisées par `mpathd` pour détecter des pannes d'interface. Pour éviter que ces adresses soient utilisées pour la communication de données par des applications hôtes, utilisées le mot `deprecated` sur la ligne de commande (voir ci-dessous).

    Vous devez en outre utiliser l'indicateur `-failover`. Avec cet indicateur, `in.mpathd` utilise l'adresse comme adresse de test (autrement dit, une adresse qui ne peut pas être transférée à l'autre interface et n'offre donc pas de redondance) :

```
# ifconfig ce2000 addif medusa-s0-mgt-0 netmask + broadcast +
-failover deprecated up
Created new logical interface ce2000:1
Setting netmask of ce2000:1 to 255.255.255.0
# ifconfig ce2001 addif medusa-s0-mgt-1 netmask + broadcast +
-failover deprecated up
Created new logical interface ce2001:1
Setting netmask of ce2001:1 to 255.255.255.0
# ifconfig ce3000 addif medusa-s0-0 netmask + broadcast + -failover
deprecated up
Created new logical interface ce3000:1
Setting netmask of ce3000:1 to 255.255.255.0
# ifconfig ce3001 addif medusa-s0-1 netmask + broadcast + -failover
deprecated up
Created new logical interface ce3001:1
Setting netmask of ce3001:1 to 255.255.255.0
```

11. **Pour permettre à la nouvelle configuration des interfaces de survivre à un redémarrage, créez des fichiers** `hostname.ce2000`, `hostname.ce2001`, `hostname.ce3000` **et** `hostname.ce3001` **dans le répertoire** `/etc`.

    Voici un exemple de fichier pour `hostname.ce2000` :

```
medusa-s0-mgt netmask + broadcast + \
group medusa_grp0-mgt failover up \
addif medusa-s0-mgt-0 netmask + broadcast + \
deprecated -failover up
```

    Voici un exemple de fichier pour `hostname.ce2001` :

```
medusa-s0-mgt-sec netmask + broadcast + \
group medusa_grp0-mgt failover up \
addif medusa-s0-mgt-1 netmask + broadcast + \
deprecated -failover up
```

    Voici un exemple de fichier pour `hostname.ce3000` :

```
medusa-s0 netmask + broadcast + \
group medusa_grp0 failover up \
addif medusa-s0-0 netmask + broadcast + \
deprecated -failover up
```

    Voici un exemple de fichier pour `hostname.ce3001` :

```
medusa-s0-sec netmask + broadcast + \
group medusa_grp0 failover up \
addif medusa-s0-1 netmask + broadcast + \
deprecated -failover up
```

12. Inspectez la configuration des deux adaptateurs de réseau en tapant :

```
# ifconfig -a
lo0: flags=1000849<UP,LOOPBACK,RUNNING,MULTICAST,IPv4> mtu 8232 index 1
    inet 127.0.0.1 netmask ff000000
ce2000: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 3
    inet 192.168.2.150 netmask ffffff00 broadcast 192.168.2.255
    groupname medusa_grp0-mgt
    ether 0:3:ba:19:26:3
ce2000:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER> mtu 1496 index 3
    inet 192.168.2.100 netmask ffffff00 broadcast 192.168.2.255
ce2001: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 4
    inet 192.168.2.166 netmask ffffff00 broadcast 192.168.2.255
    groupname medusa_grp0-mgt
    ether 0:3:ba:19:26:4
ce2001:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER> mtu 1496 index 4
    inet 192.168.2.116 netmask ffffff00 broadcast 192.168.2.255
ce3000: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 5
    inet 192.168.1.150 netmask ffffff00 broadcast 192.168.1.255
    groupname medusa_grp0
    ether 0:3:ba:19:26:3
ce3000:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER> mtu 1496 index 5
    inet 192.168.1.100 netmask ffffff00 broadcast 192.168.1.255
ce3001: flags=9040843<UP,BROADCAST,RUNNING,MULTICAST,IPv4>
mtu 1500 index 6
    inet 192.168.1.166 netmask ffffff00 broadcast 192.168.1.255
    groupname medusa_grp0
    ether 0:3:ba:19:26:4
ce3001:1: flags=1000843<UP,BROADCAST,RUNNING,MULTICAST,DEPRECATED,IPv4,NOFAILOVER> mtu 1496 index 6
    inet 192.168.1.116 netmask ffffff00 broadcast 192.168.1.255
```

La sortie ci-dessus montre que huit adresses ont été définies (les exemples d'adresses du TABLEAU 6-1). Les quatre adresses de test IPMP sont libellées NOFAILOVER. Cela signifie qu'elles ne seront pas transférées vers l'interface restante en cas de défaillance.

13. Testez IPMP en retirant temporairement un SSC du châssis.

Les messages d'erreur suivants apparaîtront sur la console :

```
Sep 4 20:12:16 medusa-s0 in.mpathd[31]: NIC failure detected on
ce3001 of group medusa_grp0
Sep 4 20:12:16 medusa-s0 in.mpathd[31]: Successfully failed over
from NIC ce3001 to NIC ce3000
```

Remarque - Il faut environ 10 secondes au démon IPMP pour détecter et se remettre d'une panne réseau avec la configuration par défaut. La configuration du démon IPMP est définie dans le fichier `/etc/default/mpathd`.

CHAPITRE 7

Exemples de configuration de commutateurs pour plusieurs tenants

Ce chapitre contient les rubriques suivantes :

Remarque - Si vous réinitialisez le commutateur alors que vous êtes en train d'exécuter les instructions de cette section, vous devez commencer par enregistrer la configuration. Si vous ne le faites pas, vous perdrez toutes les modifications apportées. Pour enregistrer la configuration, suivez les instructions de la Section A.8, « Enregistrement des paramètres du commutateur » à la page A-9.

7.1 Introduction

Ce chapitre se destine aux FAI (Fournisseurs d'accès à Internet) qui doivent :

- allouer des serveurs Blade à différents clients ;
- permettre à ces clients de gérer leurs propres serveurs Blade ;
- empêcher tout client de recevoir des données provenant du réseau d'un autre client ;
- empêcher tout client d'accéder à la console des serveurs Blade d'un autre client ;
- empêcher tout client d'accéder à la console d'un des commutateurs intégrés.

Il fournit deux exemples de configuration de commutateurs illustrant l'utilisation de VLAN pour allouer des serveurs Blade à différents clients. Dans le reste de ce chapitre, les clients d'un FAI seront appelés « tenants » de serveurs Blade particuliers.

Les configurations de commutateur supposent que seul le FAI a accès, par nom d'utilisateur et mot de passe, aux interfaces de ligne de commande des SC et des commutateurs. Les clients du FAI peuvent envoyer un `ping` au port NETMGT du commutateur, car ils ont leur propre réseau de gestion incluant le port NETMGT. Cependant, si vous ne leur donnez pas un accès par nom d'utilisateur et mot de passe, ils ne peuvent pas y accéder. La configuration VLAN signifie qu'aucun des clients n'a accès au port réseau du SC via telnet.

Si ce chapitre se destine avant tout aux FAI, il peut également être utile aux administrateurs de réseau intéressés d'une manière générale par l'utilisation de VLAN pour contrôler le trafic réseau sur le châssis Sun Fire B1600 pour serveurs Blade.

Ce chapitre n'explique pas comment configurer IPMP sur les serveurs Blade. Pour des instructions de configuration des interfaces IPMP pour des configurations VLAN complexes, reportez-vous au chapitre 6.

Remarque - Les instructions de ce chapitre concernent l'utilisation de VLAN. Elles supposent que votre réseau général utilise des VLAN marqués. Autrement dit, les configurations décrites dans ce chapitre ne prennent pas en charge l'installation de Solaris à travers le réseau (car cela exige que les VLAN du commutateur traitent du trafic non marqué). Les instructions de ce chapitre sont fournies uniquement pour illustrer l'utilisation des fonctions VLAN sur le commutateur.

Pour des informations sur la configuration du commutateur de manière à supprimer le marquage VLAN des trames qu'il envoie au réseau (sauf l'ajout d'un marqueur VLAN aux trames non marquées qu'il reçoit du réseau), reportez-vous à la Section 7.2.4, « Allocation de ports de réseau de données à chaque tenant » à la page 7-10 et à la Section 7.3.4, « Partage des ports de réseau de données entre les tenants » à la page 7-16.

7.2 Scénario A : Trois tenants différents avec leurs propres serveurs Blade et ports de données

Dans ce scénario, un FAI (Fournisseur d'accès à Internet) est supposé posséder le châssis pour serveurs Blade et assumer la responsabilité générale de sa gestion. Le FAI a par conséquent seul accès à l'interface de ligne de commande du commutateur sur NETMGT.

Le scénario suppose également la présence de trois tenants : Tenant 1, Tenant 2 et Tenant 3. Chaque tenant a un seul VLAN de données qui lui est affecté de manière exclusive. Ce VLAN de données inclut un certain nombre de serveurs Blade (une partie des ports de liaison descendante de serveur Blade du commutateur) et un certain nombre de ports de données externes.

Les tenants ont également chacun un VLAN de gestion qui leur offre un accès sécurisé à leurs propres serveurs Blade.

La configuration du commutateur est résumée dans le TABLEAU 7-1..

TABLEAU 7-1 Scénario A : Trois tenants avec leurs propres serveurs Blade et ports de données

Administrateur de réseau	Port de gestion	Ports de serveur Blade	Ports de liaison montante	ID de VLAN de données	ID de VLAN de gestion
Fournisseur d'accès à Internet	NETMGT	Aucun	Aucun	Aucun	2
Tenant 1	NETMGT	SNP0, SNP1, SNP2	NETP0, NETP1	11	21
Tenant 2	NETMGT	SNP3, SNP4, SNP5, SNP6, SNP7, SNP8, SNP9	NETP2, NETP3, NETP4	12	22
Tenant 3	NETMGT	SNP10, SNP11, SNP12, SNP13, SNP14, SNP15	NETP5, NETP6, NETP7	13	23

Le reste de cette section explique comment créer la configuration décrite au TABLEAU 7-1. Il se compose des sous-sections suivantes :

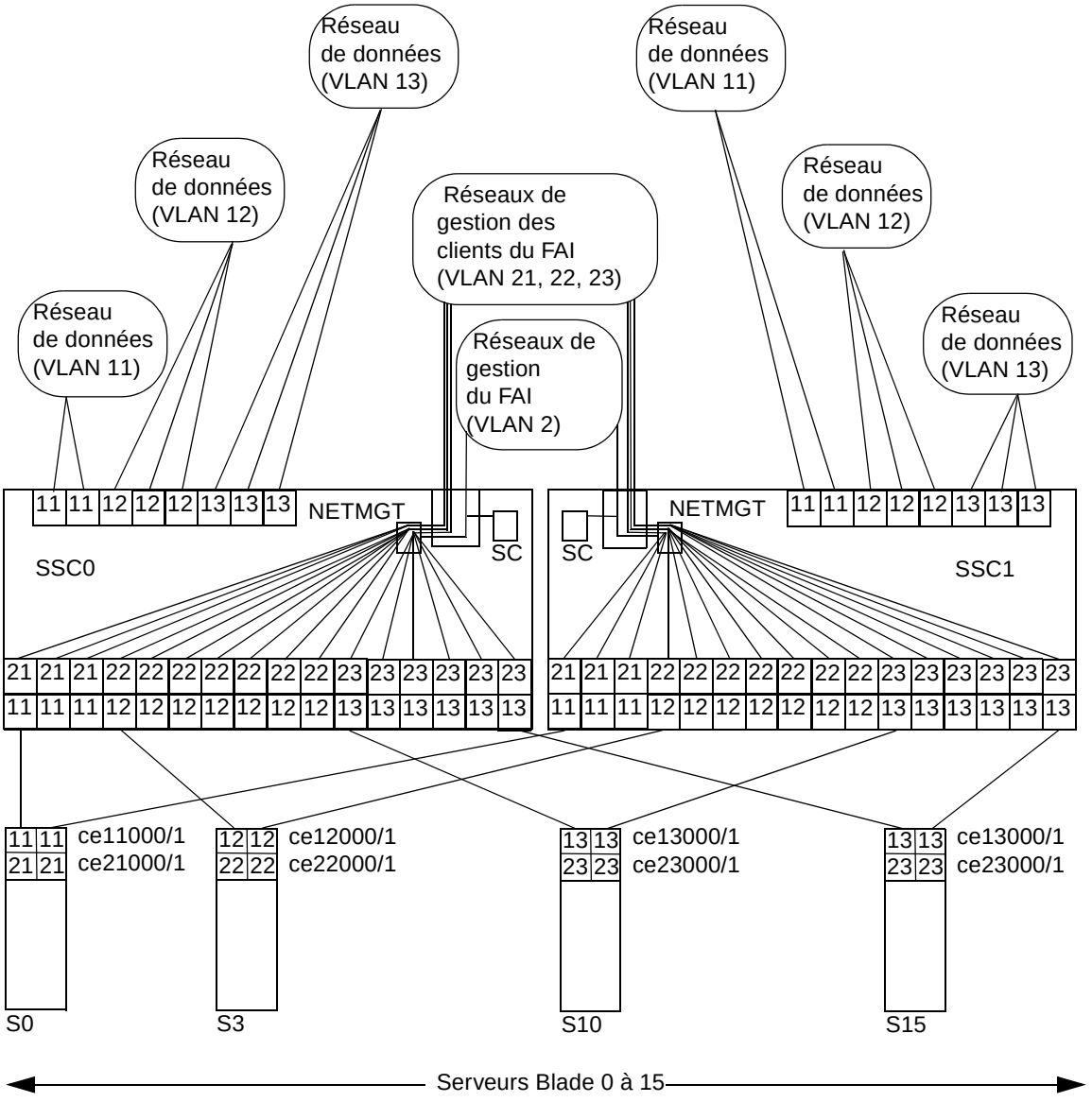

FIGURE 7-1 Scénario A : VLAN de données et de gestion des tenants et VLAN de gestion du FAI

La FIGURE 7-1 présente sous une forme graphique les mêmes informations que le TABLEAU 7-1. Au centre, se trouve le VLAN de gestion du FAI, VLAN 2. Ce VLAN est exclusivement accessible par l'administrateur de réseau du FAI. Il inclut le port NETMGT sur le commutateur (permettant ainsi à l'administrateur réseau du FAI de configurer tout le commutateur via une connexion telnet ou web). Il inclut également le contrôleur système (permettant ainsi au FAI de configurer l'ensemble du châssis et d'accéder à la console de tous les serveurs Blade et des deux commutateurs à partir de l'invite `sc>`). Notez cependant que l'appartenance du contrôleur système au VLAN se configure à partir de l'invite `sc>` (en particulier, avec la commande `setupsc`) : cet aspect ne fait pas partie du processus de configuration du commutateur.

Remarque - Dans ce scénario, on suppose que l'administrateur réseau du FAI ne donne à aucun de ses clients l'accès par mot de passe à l'interface de ligne de commande du contrôleur système ou du commutateur. Il incombe à l'administrateur réseau de contôler l'accès aux interfaces du contrôleur système et du commutateur.

Au-dessus de VLAN 2 dans le diagramme, figurent trois VLAN de gestion pour les clients individuels du FAI. Chacun de ces clients a accès, sur un VLAN de gestion dédié à ses propres serveurs Blade. Ainsi, par exemple, le Tenant 1 (qui a le VLAN de gestion 21) peut se connecter par telnet aux serveurs Blade des logements 0, 1 et 2. Le Tenant 2 (VLAN de gestion 22) peut se connecter par telnet aux serveurs Blade des logements 3 à 9. Et le Tenant 3 (VLAN de gestion 23) peut se connecter par telnet des logements 10 à 15.

Dans le bas du diagramme, figure le premier des serveurs Blade de chaque client. Ces serveurs Blade exigent chacun deux interfaces logiques avec leur réseau de données et deux interfaces logiques avec leur réseau de gestion. Ces interfaces logiques doivent être fournies par IPMP (voir chapitre 6). Le diagramme montre la numérotation des interfaces requise pour la configuration IPMP. Par exemple, les serveurs Blade du Tenant 1 contiennent deux interfaces logiques pour VLAN 11 (réseau de données) et deux interfaces logiques pour VLAN 21 (réseau de gestion). Suivant la formule indiquée au chapitre 6, la numérotation des interfaces pour chacun des serveurs Blade de Tenant 1 est `ce11000` et `ce21000` (pour la connexion sur `ce0` au commutateur en SSC0) et `ce11001` et `ce21001` (pour la connexion sur `ce1` au commutateur en SSC1).

Enfin, dans ce scénario, les clients du FAI ont chacun des ports de liaison montante réseau dédiés. Le Tenant 1 a les ports NETP0 et NETP1, le Tenant 2, les ports NETP2, NETP3 et NETP4, et le Tenant 3, les ports NETP5, NETP6 et NETP7. Ces ports sont rendus exclusifs à leur tenant par leur inclusion dans les VLAN de données où se trouvent les serveurs Blade de chaque tenant. Ainsi, par exemple, le VLAN de donnée du Tenant 3 (VLAN 13) inclut les ports de serveur blade SNP10 à SNP15, plus les ports de liaison montante NETP5, NETP6 et NETP7.

Remarque - Si les liaisons montantes appartenant aux différents tenants se connectent au même commutateur externe, le protocole Spanning Tree brisera certaines des connexions. Nous recommandons d'utiliser un commutateur externe différent pour chaque tenant. Ou bien, vous pouvez désactiver le protocole Spanning Tree (reportez-vous à la Section 7.2.5, « Désactivation du protocole Spanning Tree » à la page 7-11).

7.2.1 Création et dénomination de tous les VLAN

1. **Pour vous connecter au commutateur en SSC0, tapez :**

```
sc> console ssc0/swt
```

2. **Lorsqu'un nom d'utilisateur vous est demandé, tapez** `admin`**.**

   Tapez à nouveau `admin` comme mot de passe.

3. **Assurez-vous que le commutateur utilise la configuration d'usine par défaut.**

   Pour des informations à ce sujet, reportez-vous à la Section A.4, « Vérification de l'utilisation de la configuration par défaut d'usine du commutateur » à la page A-4.

4. **Si vous n'avez pas repris la configuration d'usine par défaut ou si vous n'avez pas encore défini votre propre mot de passe, faites-le maintenant.**

   Pour des informations à ce sujet, reportez-vous à la Section 2.2, « Connexion au commutateur en tant qu'utilisateur par défaut et réglage des mots de passe » à la page 2-4.

5. **Créez et donnez des noms aux VLAN de données des tenants.**

   Pour ce faire, tapez :

```
Console#configure
Console(config)#vlan database
Console(config-vlan)#vlan 11 name tenant1 media ethernet
Console(config-vlan)#vlan 12 name tenant2 media ethernet
Console(config-vlan)#vlan 13 name tenant3 media ethernet
Console(config-vlan)#end
```

6. **Créez et donnez des noms aux VLAN de gestion des tenants.**

   Tapez :

```
Console#configure
Console(config)#vlan database
Console(config-vlan)#vlan 21 name tenant1_managment media
ethernet
Console(config-vlan)#vlan 22 name tenant2_managment media ethernet
Console(config-vlan)#vlan 23 name tenant3_managment media ethernet
Console(config-vlan)#end
```

7.2.2 Allocation du port de gestion (NETMGT) à chaque tenant

1. **Configurez le port de gestion du commutateur (NETMGT) pour lui permettre de recevoir et émettre des trames en provenance et à destination du VLAN de gestion du FAI (2) et aux VLAN de gestion de tous les tenants (21, 22, 23).**

   Le FAI utilise le VLAN de gestion par défaut, VLAN 2.

   Tapez :

```
Console#configure
Console(config)#interface ethernet NETMGT
Console(config-if)#switchport allowed vlan add 21 tagged
Console(config-if)#switchport allowed vlan add 22 tagged
Console(config-if)#switchport allowed vlan add 23 tagged
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#no switchport gvrp
Console(config-if)#end
```

   Cette séquence a la signification suivante :

   - La commande `interface ethernet NETMGT` spécifie que vous configurez le port de gestion.
   - La commande `switchport allowed vlan add 21` ajoute NETMGT au VLAN de gestion (21) de Tenant 1 et lui permet de transmettre les trames marquées à ce VLAN.
   - La commande `switchport allowed vlan add 22` ajoute NETMGT au VLAN de gestion (22) de Tenant 2 et lui permet de transmettre les trames marquées à ce VLAN.
   - La commande `switchport allowed vlan add 23` ajoute NETMGT au VLAN de gestion (23) de Tenant 3 et lui permet de transmettre les trames marquées à ce VLAN.

- Les commandes `switchport ingress-filtering`, `switchport mode trunk` et `switchport acceptable-frame-types tagged`enjoignent au port NETMGT d'accepter et émettre uniquement les trames adressées aux VLAN particuliers dont il est membre (VLAN 21, 22 et 23 ainsi que le VLAN de gestion par défaut, VLAN 2).
- La commande `no switchport gvrp` empêche le port NETMGT d'utiliser GVRP pour annoncer les VLAN dont il est membre à un autre commutateur.

2. **Assurez-vous que le filtre de paquets IP du commutateur est configuré pour autoriser le passage du trafic des serveurs Blade au réseau de gestion.**

   Pour des informations à ce sujet, reportez-vous à la Section A.11, « Utilisation du filtre de paquets sur le commutateur pour assurer une gestion sûre des serveurs Blade » à la page A-16.

7.2.3 Allocation de ports de serveur Blade à chaque tenant

1. **Pour Tenant 1, configurez les ports de serveur Blade de sorte qu'ils émettent et reçoivent uniquement les trames marquées pour les VLAN 11 et 21.**

   Tapez :

```
Console#configure
Console(config)#interface ethernet SNP0
Console(config-if)#switchport allowed vlan add 11 tagged
Console(config-if)#switchport allowed vlan add 21
Console(config-if)#switchport native vlan 21
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#end
```

   Répétez ces commandes pour les deux autres ports de serveur Blade (SNP1 et SNP2) appartenant à Tenant 1.

2. **Pour Tenant 2, configurez les ports de serveur Blade de sorte qu'ils émettent et reçoivent uniquement les trames marquées pour les VLAN 12 et 22.**

   Tapez :

```
Console#configure
Console(config)#interface ethernet SNP3
Console(config-if)#switchport allowed vlan add 12 tagged
Console(config-if)#switchport allowed vlan add 22
Console(config-if)#switchport native vlan 22
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#end
```

   Répétez ces commandes pour les autres ports de serveur Blade (SNP4 à SNP9) appartenant à Tenant 2.

3. **Pour Tenant 3, configurez les ports de serveur Blade de sorte qu'ils émettent et reçoivent uniquement les trames marquées pour les VLAN 13 et 23.**

   Tapez :

```
Console#configure
Console(config)#interface ethernet SNP10
Console(config-if)#switchport allowed vlan add 13 tagged
Console(config-if)#switchport allowed vlan add 23
Console(config-if)#switchport native vlan 23
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#end
```

   Répétez ces commandes pour les autres ports de serveur Blade (SNP11 à SNP15) appartenant à Tenant 3.

7.2.4 Allocation de ports de réseau de données à chaque tenant

---

Remarque - Les périphériques réseau auxquels vous connectez le châssis Sun Fire B1600 pour serveurs Blade doivent reconnaître les VLAN. C'est pourquoi les instructions comprennent la commande `switchport mode trunk`, qui veille à ce qu'un port réseau n'émette et ne reçoive que les trames adressées aux VLAN particuliers (ou, en l'occurrence, au VLAN particulier) dont il est membre.

---

1. **Configurez les ports réseau pour Tenant 1 de sorte qu'ils émettent et reçoivent uniquement les trames marquées pour VLAN 11.**

   Pour NETP0, tapez :

```
Console#configure
Console(config)#interface ethernet NETP0
Console(config-if)#switchport allowed vlan add 11
Console(config-if)#switchport native vlan 11
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#switchport mode trunk
Console(config-if)#no switchport gvrp
Console(config-if)#end
```

   Répétez ces commandes pour NETP1.

2. **Configurez les ports réseau pour Tenant 2 de sorte qu'ils émettent et reçoivent uniquement les trames marquées pour VLAN 12.**

   Pour NETP2, tapez :

```
Console#configure
Console(config)#interface ethernet NETP2
Console(config-if)#switchport allowed vlan add 12
Console(config-if)#switchport native vlan 12
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#switchport mode trunk
Console(config-if)#no switchport gvrp
Console(config-if)#end
```

   Répétez ces commandes pour NETP3 et NETP4.

3. **Configurez les ports réseau pour Tenant 3 de sorte qu'ils émettent et reçoivent uniquement les trames marquées pour VLAN 13.**

   Pour NETP5, tapez :

```
Console#configure
Console(config)#interface ethernet NETP5
Console(config-if)#switchport allowed vlan add 13
Console(config-if)#switchport native vlan 13
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#switchport mode trunk
Console(config-if)#no switchport gvrp
Console(config-if)#end
```

   Répétez ces commandes pour NETP5, NETP6 et NETP7.

7.2.5 Désactivation du protocole Spanning Tree

Si les liaisons montantes appartenant aux différents tenants se connectent au même commutateur externe, le protocole Spanning Tree brisera certaines des connexions. Nous recommandons d'utiliser un commutateur externe différent pour chaque tenant. Ou bien, vous pouvez désactiver le protocole Spanning Tree. Pour désactiver le protocole Spanning Tree, tapez :

```
Console#configure
Console(config)#no spanning-tree
Console(config)#end
```

7.2.6 Enregistrement des paramètres du commutateur et copie de la configuration vers le second commutateur

1. **Enregistrez les paramètres de commutateur.**

   Pour ce faire, suivez les instructions du chapitre A.

2. **Copiez la configuration du commutateur vers le second commutateur.**

   Pour ce faire, suivez les instructions du chapitre A.

7.3 Scénario B : Deux tenants avec huit serveurs Blade chacun et quatre ports de données partagés

Dans ce scénario, un FAI (Fournisseur d'accès à Internet) est supposé posséder le châssis pour serveurs Blade et assumer la responsabilité générale de sa gestion. Il y a également deux tenants, Tenant 1 et Tenant 2. Les deux tenants ont un VLAN de données qui leur est affecté et le VLAN inclut huit serveurs Blade (autrement dit, huit des ports de serveur Blade du commutateur) plus quatre des ports de données externes du commutateur. En d'autres termes, les deux tenants partagent quatre des ports de données externes (aucun n'en a l'usage exclusif).

La configuration du commutateur pour ce scénario est résumée au TABLEAU 7-2.

TABLEAU 7-2 Quatre ports de données chacun

Administrateur réseau	Port de gestion	Ports de serveur Blade	Ports de données externes	ID de VLAN de données	ID de VLAN de gestion
Fournisseur d'accès à Internet	NETMGT	Aucun	Aucun	Aucun	2
Tenant 1	NETMGT	SNP0, SNP1, SNP2, SNP3, SNP4, SNP5, SNP6, SNP7	NETP0 à NETP3	11	21
Tenant 2	NETMGT	SNP8, SNP9, SNP10, SNP11, SNP12, SNP13, SNP14, SNP15	NETP0 à NETP3	12	22

Le reste de cette section explique comment créer la configuration décrite au TABLEAU 7-2. Il se compose des sous-sections suivantes :

- Section 7.3.1, « Création et dénomination de tous les VLAN » à la page 7-14
- Section 7.3.2, « Allocation du port de gestion (NETMGT) à chaque tenant » à la page 7-14
- Section 7.3.3, « Allocation de ports de serveur Blade à chaque tenant » à la page 7-15
- Section 7.3.4, « Partage des ports de réseau de données entre les tenants » à la page 7-16

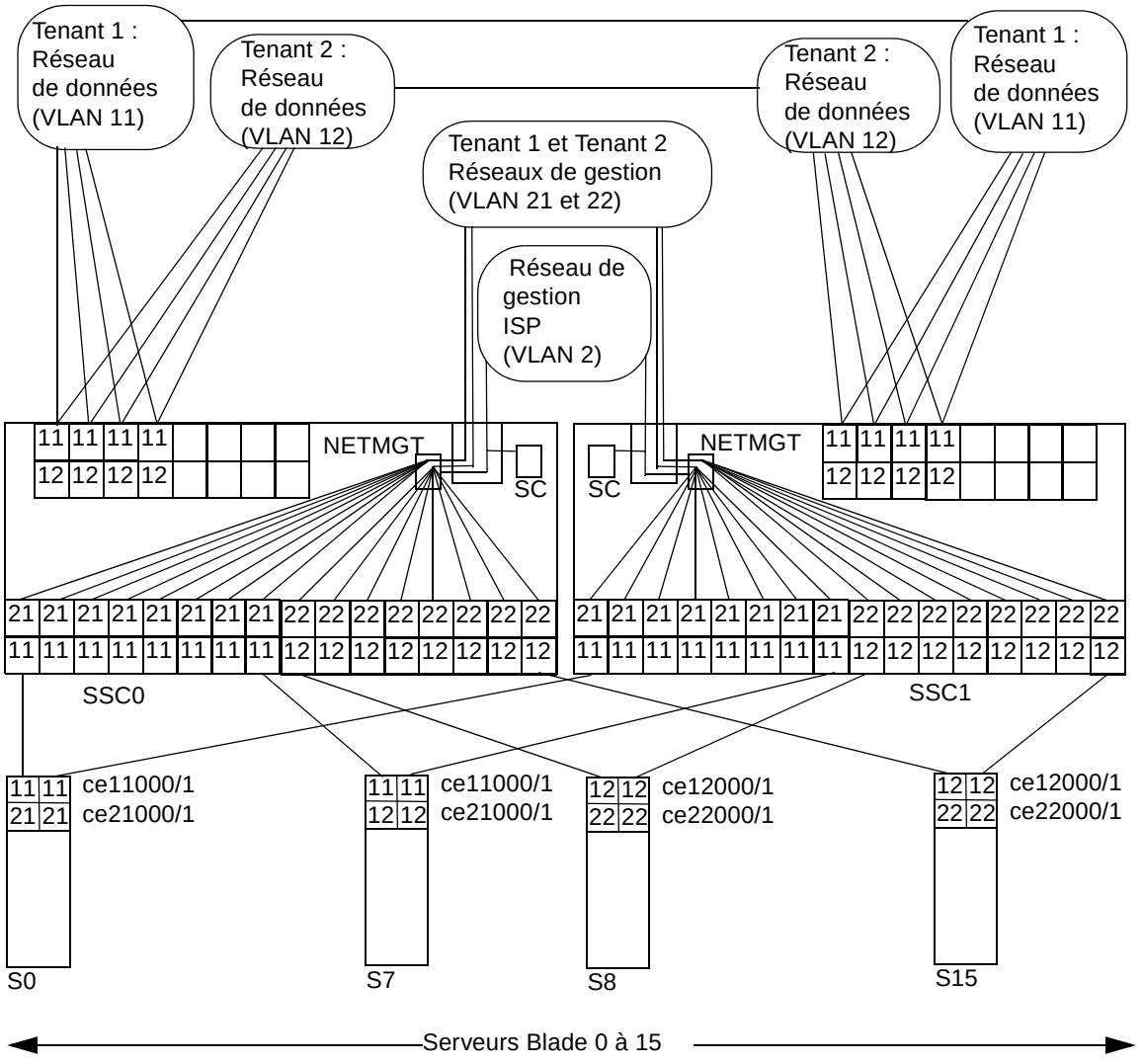

FIGURE 7-2 Scénario B : VLAN de données et de gestion de deux tenants avec ports de liaison montante partagés

La FIGURE 7-2 présente sous une forme graphique les mêmes informations que le TABLEAU 7-2. Dans ce scénario, les principes sont les mêmes que dans le scénario A, si ce n'est que tous les ports de liaison montante réseau sont partagés par les tenants des serveurs Blade. En d'autres termes, les deux VLAN de données des tenants (VLAN 11 pour Tenant 1 et VLAN 12 pour Tenant 2) incluent les ports de liaison montante NETP0 à NETP3. Cela n'implique pas que les tenants recevront les données des serveurs Blade l'un de l'autre, car toute trame sortant des ports NETP0 à NETP3 sera marquée comme destinée au VLAN 11 (Tenant 1) ou au VLAN 12 (Tenant 2).

7.3.1 Création et dénomination de tous les VLAN

1. **Créez et donnez des noms aux VLAN de données des tenants.**

   Pour ce faire, tapez :

```
Console#configure
Console(config)#vlan database
Console(config-vlan)#vlan 11 name tenant1 media ethernet
Console(config-vlan)#vlan 12 name tenant2 media ethernet
```

2. **Créez et donnez des noms aux VLAN de gestion des tenants.**

   Tapez :

```
Console#configure
Console(config)#vlan database
Console(config-vlan)#vlan 21 name tenant1_managment media
ethernet
Console(config-vlan)#vlan 22 name tenant2_managment media
ethernet
Console(config-vlan)#end
```

7.3.2 Allocation du port de gestion (NETMGT) à chaque tenant

1. **Configurez le port de gestion du commutateur (NETMGT) pour lui permettre de recevoir et émettre des trames en provenance et à destination du VLAN de gestion du FAI (2) et aux deux VLAN de gestion des tenants (21 et 22).**

   Tapez :

```
Console#config
Console(config)#interface ethernet NETMGT
Console(config-if)#switchport allowed vlan add 21 tagged
Console(config-if)#switchport allowed vlan add 22 tagged
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#switchport mode trunk
Console(config-if)#no switchport gvrp
Console(config-if)#end
```

2. **Assurez-vous que le filtre de paquets IP du commutateur est configuré pour autoriser le passage du trafic des serveurs Blade au réseau de gestion.**

   Pour des informations à ce sujet, reportez-vous à la Section A.11, « Utilisation du filtre de paquets sur le commutateur pour assurer une gestion sûre des serveurs Blade » à la page A-16.

7.3.3 Allocation de ports de serveur Blade à chaque tenant

1. **Pour Tenant 1, configurez les ports de serveur Blade de sorte qu'ils émettent et reçoivent uniquement les trames marquées pour les VLAN 11 et 21.**

   Tapez :

```
Console#configure
Console(config)#interface ethernet SNP0
Console(config-if)#switchport allowed vlan add 11 tagged
Console(config-if)#switchport allowed vlan add 21
Console(config-if)#switchport native vlan 21
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#end
```

   Répétez ces commandes pour les sept autres ports de serveur Blade (SNP1 à SNP7) appartenant à Tenant 1.

2. **Pour Tenant 2, configurez les ports de serveur Blade de sorte qu'ils émettent et reçoivent uniquement les trames marquées pour les VLAN 12 et 22.**

   Tapez :

```
Console#configure
Console(config)#interface ethernet SNP8
Console(config-if)#switchport allowed vlan add 12 tagged
Console(config-if)#switchport allowed vlan add 22
Console(config-if)#switchport native vlan 12
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport mode trunk
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#end
```

   Répétez ces commandes pour les sept autres ports de serveur Blade (SNP9 à SNP15) appartenant à Tenant 2.

7.3.4 Partage des ports de réseau de données entre les tenants

---

Remarque - Les instructions de cette section supposent que les périphériques réseau auxquels vous connectez le châssis Sun Fire B1600 pour serveurs Blade reconnaissent les VLAN. C'est pourquoi les instructions comprennent la commande `switchport mode trunk`, qui veille à ce qu'un port réseau n'émette et ne reçoive que les trames adressées aux VLAN particuliers dont il est membre.

---

1. **Configurez les ports réseau de sorte qu'ils émettent et reçoivent uniquement les trames marquées pour VLAN 11 et VLAN 12.**

   Pour NETP0, tapez :

```
Console#configure
Console(config)#interface ethernet NETP0
Console(config-if)#switchport allowed vlan add 11 tagged
Console(config-if)#switchport allowed vlan add 21
Console(config-if)#switchport native vlan 21
Console(config-if)#switchport allowed vlan remove 1
Console(config-if)#switchport ingress-filtering
Console(config-if)#switchport acceptable-frame-types tagged
Console(config-if)#switchport mode trunk
Console(config-if)#no switchport gvrp
Console(config-if)#end
```

2. Répétez ces commandes pour NETP1 à NETP3.

3. **Enregistrez les paramètres de commutateur.**

   Pour ce faire, suivez les instructions du chapitre A.

4. **Copiez la configuration du commutateur vers le second commutateur.**

   Pour ce faire, suivez les instructions du chapitre A.

ANNEXE **A**

Tâches utiles à effectuer sur les commutateurs

Cette annexe explique comment effectuer certaines tâches qui ne peuvent être exécutées que dans l'interface de ligne de commande d'un commutateur. Vous devrez vous y référer pendant la configuration du châssis pour serveurs Blade.

Pour des instructions concernant la connexion à l'interface de ligne de commande du commutateur, reportez-vous au chapitre 2.

Ce chapitre contient les rubriques suivantes :

A.1 Déplacement entre les invites de commande

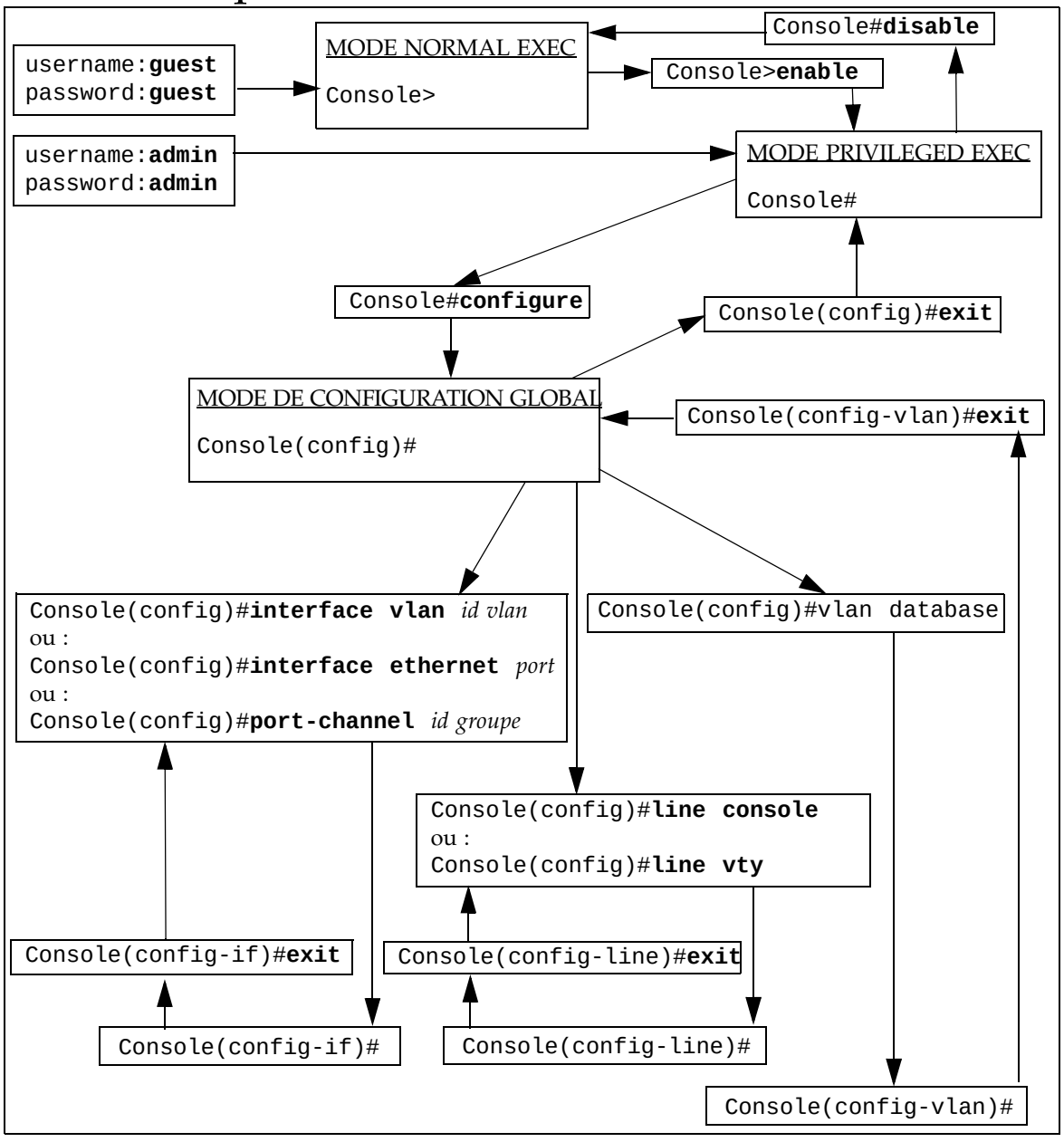

FIGURE A-1 Organisation des invites de commande du commutateur

A.2 Sortie de l'interface de ligne de commande

A.2.1 Sortie du commutateur vers le contrôleur système

- **Pour quitter l'interface de ligne de commande du commutateur et retourner à l'interface de ligne de commande du contrôleur système, tapez le caractère dièse (#) suivi immédiatement d'un point (.).**

  Lorsque vous êtes dans l'interface de ligne de commande du commutateur, la séquence « #. » permet de retourner à l'interface de ligne de commande du contrôleur système.

  Par exemple, tapez (notez que ces caractères ne sont pas affichés sur l'écran) :

```
Console(config)##.
```

A.2.2 Retour à l'invite de connexion du commutateur

- **Pour retourner à l'invite de connexion du commutateur, tapez** `exit` **ou** `end` **jusqu'à revenir à l'invite** `Console#`**, puis tapez :**

```
Console#exit
```

A.3 Affichage de l'aide en ligne de l'interface de ligne de commande du commutateur

- **Pour en savoir plus sur l'utilisation de l'aide en ligne, tapez `help` à tout moment.**
- **Pour afficher une aide en ligne contextuelle, tapez ? à tout moment. Cette commande affiche une liste de commandes ou de paramètres. Si vous êtes à une invite de commande, la commande ? affiche une liste des commandes disponibles dans le mode de commande actuel. Si vous souhaitez connaître le ou les paramètre(s) requis pour une commande, tapez le premier mot de la commande suivi d'un ?. Vous obtiendrez ainsi une liste descriptive des paramètres disponibles. Chaque fois que vous tapez ? à la suite d'une commande incomplète, la partie déjà introduite de la commande apparaît sur la console. Vous ne devez donc pas retaper ces informations.**

  Voici un exemple d'aide concernant l'utilisation de la commande `vlan database` pour accéder au mode de commande de configuration des VLAN :

```
Console(config)#vlan
% Incomplete command.
Console(config)#vlan ?
 database Enter VLAN database mode
Console(config)#vlan database ?
 <cr>
```

où `<cr>` indique qu'il n'y a pas d'autres paramètres requis et que vous devez appuyer sur [ENTREE] pour retourner à l'invite de commande.

A.4 Vérification de l'utilisation de la configuration par défaut d'usine du commutateur

Pour plus d'informations sur les paramètres par défaut d'usine du commutateur, référez-vous au *Manuel d'administration des commutateurs du châssis Sun Fire B1600 pour serveurs Blade*.

Pour rétablir la configuration par défaut d'usine du commutateur, procédez comme suit :

1. **Pour vérifier si le commutateur utilise sa configuration par défaut d'usine, tapez :**

```
Console#whichboot
           file name file type    startup size (byte)
 ------------------------ -------------- ------- --------
          diag74 Boot-Rom ima  Y   114248
      runtime_v00423 Operation Code Y   1429204
Factory_Default_Config.cfg Config File   Y   2574
```

   Si la dernière ligne de la sortie de cette commande comprend « `Factory_Default_Config.cfg` » dans la colonne `file name`, le commutateur utilise la configuration par défaut.

2. **Pour enjoindre au commutateur d'utiliser la configuration par défaut d'usine, tapez :**

```
Console#configure
Console(config)#boot system config Factory_Default_Config.cfg
Console(config)#exit
```

3. **Faites redémarrer le commutateur avec la configuration par défaut d'usine.**

   Tapez :

```
Console#reload
```

4. **Lorsque vous êtes invité à entrer un nom d'utilisateur et un mot de passe, tapez** `admin` **pour les deux.**

A.5 Réinitialisation du commutateur

Une réinitialisation du commutateur peut être nécessaire par exemple pour revenir à la configuration de démarrage après avoir modifié la configuration courante (si vous ne souhaitez pas conserver ces modifications).

Vous pourriez aussi vouloir réinitialiser le commutateur après avoir créé ou téléchargé un nouveau fichier de configuration que vous souhaitez désigner comme fichier de démarrage par défaut.

Remarque - Avant de réinitialiser le commutateur, enregistrez les changements de configuration que vous souhaitez conserver.

- **Pour réinitialiser le commutateur à partir de sa ligne de commande, tapez :**

```
Console#reload
```

- **Ou bien, vous pouvez réinitialiser le commutateur à partir de la ligne de commande du contrôleur système.**

  A l'invite `sc>`, tapez la commande suivante :

```
sc>reset sscn/swt
```

où *n* vaut 0 ou 1 selon que vous réinitialisez SSC0 ou SSC1.

A.6 Réglage de l'adresse IP, du masque de réseau et de la passerelle par défaut du commutateur

1. **Définissez l'adresse IP et le masque de réseau en tapant :**

```
Console#configure
Console(config)#interface vlan id vlan
Console(config-if)#ip address adresse ip  masque réseau
Console(config-if)#exit
```

où :

- *id vlan* est le numéro du VLAN (2, par défaut) contenant le port de gestion réseau du commutateur, NETMGT. Si vous utilisez la configuration par défaut d'usine, spécifiez 2.
- *adresse ip* est l'adresse IP que le commutateur doit utiliser.
- *masque de réseau* est le masque de réseau à définir (par exemple, 255.255.255.0).

2. **Pour définir la passerelle par défaut, tapez :**

```
Console(config)#ip default-gateway adresse ip
Console(config)#exit
```

où *adresse ip* est l'adresse IP du périphérique que vous spécifiez comme passerelle par défaut.

3. **Pour confirmer la modification apportée au paramètre de passerelle par défaut, tapez :**

```
Console#show running-config
building running-config, please wait.....
:
!
interface ethernet NETMGT
 description External RJ-45 connector NETPMGT
 switchport allowed vlan add 2 untagged
 switchport native vlan 2
 switchport allowed vlan remove 1
 switchport forbidden vlan add 1
 spanning-tree edge-port
!
interface vlan 2
 ip address 129.156.203.3 255.255.255.0
 ip dhcp client-identifier text SUNW,SWITCH_ID=900002,0
!
!
!
ip default-gateway 129.156.203.8
:
Console#
```

Les caractères : dans l'exemple de sortie ci-dessus indiquent des informations omises. Le réglage de la passerelle par défaut apparaît vers la fin de la sortie de la commande `show running-config`.

A.7 Configuration des VLAN

Par défaut, le commutateur possède un VLAN de gestion (VLAN 2) contenant son port de gestion (NETMGT) et un VLAN de données contenant tous les autres ports.

Pour plus d'informations sur l'utilisation des VLAN, reportez-vous aux chapitre 5, chapitre 6 et chapitre 7.

Pour créer un VLAN supplémentaire, vous devez le configurer et y ajouter des ports individuellement.

1. **A l'invite `Console#`, tapez :**

```
Console#configure
```

2. **Passez au mode de configuration de VLAN en tapant :**

```
Console(config)#vlan database
```

3. **Créez le VLAN :**

```
Console(config-vlan)#vlan id vlan media ethernet
```

où *id vlan* est un nombre entre 1 et 4094.

4. **Pour donner un nom au VLAN, tapez :**

```
Console(config-vlan)#vlan id vlan nom media ethernet
```

où *id vlan* est le numéro du VLAN et *nom* est le nom à utiliser pour le VLAN.

5. **Remplissez le VLAN en y ajoutant des ports individuels.**

   a. **Pour ce faire, commencez par retourner au mode de configuration en tapant :**

```
Console(config-vlan)#exit
```

b. Passez au mode d'interface de configuration en tapant :

```
Console(config)#interface ethernet port
```

où *port* est le nom du port à inclure dans le VLAN.

c. Ajoutez le VLAN à un port en tapant :

```
Console(config-if)#switchport allowed vlan add id vlan
```

d. Répétez les étapes a à c pour chaque port à inclure dans le nouveau VLAN.

A.8 Enregistrement des paramètres du commutateur

Remarque - Veillez à enregistrer les paramètres de commutateur que vous souhaitez conserver après le prochain redémarrage du commutateur.

- **Pour enregistrer vos modifications, copiez le microprogramme de configuration courant vers le microprogramme de configuration de démarrage.**

  Pour ce faire, tapez la commande suivante à la console du commutateur :

```
Console#copy running-config startup-config
Startup configuration file name [nomfichier par défaut]:nomfichier
Write to FLASH Programming
-Write to FLASH finish
Success

Console#
```

où *nomfichier par défaut* est le fichier de configuration de démarrage actuel et *nomfichier* est le nom à donner au nouveau fichier. Si vous tapez [ENTREE] au lieu de spécifier un nouveau nom de fichier, la configuration courante sera enregistrée dans le fichier de configuration de démarrage actuel.

A.9 Copie de la configuration du premier commutateur vers le second

Le transfert d'un fichier de configuration d'un commutateur vers l'autre exige TFTP. Un serveur TFTP doit donc être disponible sur votre réseau. Les instructions qui suivent expliquent comment vous y prendre. Elles expliquent ensuite comment effectuer le transfert du fichier.

Si le commutateur utilise des VLAN pour séparer les différentes régions de votre réseau et si vous utilisez IPMP (IP Network Multipathing) pour offrir à vos serveurs Blade des connexions redondantes avec le réseau, vous devez veillez à ce que la configuration du second commutateur corresponde à celle du premier.

Attention - Si la configuration VLAN du second commutateur intégré ne correspond pas à celle du premier, les données passant par le second commutateur ne seront pas régies par les définitions de VLAN du premier commutateur. De même, toute protection du réseau de gestion mise en place via le filtre de paquets du premier commutateur sera annihilée si vous ne la reproduisez pas sur le second commutateur.

Pour faire en sorte que le second commutateur du châssis Sun Fire B1600 pour serveurs Blade utilise la même configuration que le premier, suivez les instructions ci-dessous.

A.9.1 Configuration d'un serveur TFTP

Pour configurer sur votre réseau un système Solaris qui servira les requêtes TFTP, procédez comme suit :

1. **Sur le système que vous souhaitez configurer comme serveur TFTP, connectez-vous en tant que root.**
2. **Utilisez un éditeur de texte pour enlever la marque de commentaire de la ligne suivante dans le fichier** `/etc/inetd.conf` **:**

```
tftp dgram udp6 wait root /usr/sbin/in.tftpd in.tftpd -s /tftpboot
```

3. **Sur le même système, créez un répertoire d'accueil TFTP en tapant les commandes suivantes à l'invite de Solaris :**

```
# mkdir /tftpboot
# chown root /tftpboot
# chmod 755 /tftpboot
# cd /tftpboot
# ln -s . tftpboot
```

4. **Relancez `inetd` en tapant :**

```
# pkill -HUP inetd
```

5. **Vérifiez que TFTP fonctionne.**

   Pour ce faire, utilisez TFTP pour aller chercher un fichier dans le répertoire `/tftpboot`. Suivez les instructions ci-dessous :

   a. **Sur le système que vous utilisez comme serveur TFTP, copiez un fichier (par exemple, le fichier Solaris `/etc/release`) vers le répertoire `/tftpboot`.**

      Pour copier le fichier `/etc/release`, à l'invite Solaris, tapez :

```
# cp /etc/release /tftpboot/nomfichier
```

      où *nomfichier* est le nom du fichier à rendre disponible sur le serveur TFTP.

   b. **Faites en sorte que le fichier que vous venez de copier soit accessible à tous en lecture seule :**

```
# chmod 444 /tftpboot/nomfichier
```

      où *nomfichier* est le nom du fichier à rendre disponible sur le serveur TFTP.

   c. **Allez chercher le fichier sur le serveur TFTP que vous avez créé.**

      A l'invite Solaris d'un autre système, tapez les commandes suivantes :

```
% tftp serveur tftp
tftp>get nomfichier
```

      où *serveur tftp* est le nom d'hôte ou l'adresse IP du système où tourne le serveur TFTP que vous avez défini et *nomfichier* est le nom du fichier à obtenir du serveur TFTP.

d. Toujours sur le système Solaris que vous avez utilisé pour lancer la commande `get`, vérifiez le contenu du fichier en tapant :

```
# cat nomfichier
```

où *nomfichier* est le nom du fichier que vous avez transféré depuis le serveur TFTP.

Remarque - Notez que TFTP n'est pas FTP. Il n'affiche pas les mêmes messages d'erreur que FTP et vous ne pouvez pas utiliser les commandes `cd ou ls` (ni la plupart des autres commands) disponibles dans FTP.

A.9.2 Transfert du fichier de configuration de commutateur

Après avoir créé un serveur TFTP et terminé de configurer le commutateur en SSC0 ou SSC1, copiez la configuration de ce commutateur vers l'autre commutateur.

Pour ce faire, suivez les instructions ci-dessous. (Ces instructions supposent que vous copiez la configuration du commutateur en SSC0 vers le commutateur en SSC1, mais vous pouvez bien entendu faire l'inverse.)

1. **Configurez le commutateur 0 selon vos besoins en suivant les instructions des chapitre 2, chapitre 3, chapitre 5, chapitre 6 et/ou chapitre 7.**

2. **Enregistrez la configuration du commutateur 0 dans un fichier appelé, par exemple, `standard.cfg`.**

   Pour ce faire, à l'invite `Console#` du commutateur, tapez :

```
Console#copy running-config file
Destination configuration file name : standard.cfg
Write to FLASH Programming
-Write to FLASH finish
Success.

Console#
```

3. **Téléchargez le fichier** `standard.cfg` **vers le serveur TFTP.**

   Procédez comme suit :

   a. **Connectez-vous au serveur TFTP comme root.**

   b. **Placez-vous dans le répertoire** `/tftpboot`.

   c. **Créez un fichier vide appelé** `standard.cfg`.

```
#>standard.cfg
```

4. **Rendez ce fichier accessible en écriture par tous :**

```
#chmod 666 standard.cfg
```

5. **A l'interface de ligne de commande du commutateur, tapez :**

```
Console#copy file tftp
Choose file type :
1. config : 2.opcode : <1-2>:1
Source file name : nomfichier
TFTP server ip address : adresse IP
Desitination file name : nomfichier
Console#
```

   où *nomfichier* est, dans les deux cas, `standard.cfg` (si ce nom est celui sous lequel vous avez enregistré votre configuration de commutateur) et *adresse IP* est l'adresse IP du serveur TFTP.

6. **Sur le serveur TFTP, utilisez un éditeur de texte pour ouvrir le fichier `standard.cfg`.**

   Changez l'entrée indiquant le nom d'hôte du commutateur 0 pour le remplacer par celui du commutateur 1 :

```
!
hostname nom d'hôte du commutateur 1
```

   Si vous avez choisi d'utiliser des adresses IP affectées manuellement pour les commutateurs, vous devez changer l'entrée correspondant à l'adresse IP et au masque de réseau pour y faire figurer ceux du commutateur 1 au lieu de ceux du commutateur 0 :

```
interface vlan 2
 ip address adresse ip  masque de réseau
```

   Si vous utilisez DHCP, il n'est pas nécessaire de changer l'adresse IP et le masque de réseau ou l'identificateur de client DHCP. L'adresse IP et le masque de réseau seront automatiquement affectés par le serveur DHCP. L'identificateur de client DHCP sera automatiquement attribué par le contrôleur système actif à chaque réinitialisation du commutateur.

7. **Enregistrez ce fichier sous un nom approprié, par exemple `standard1.cfg`.**

8. **Connectez-vous au commutateur 1 et (si le commutateur n'a pas reçu une adresse IP de DHCP) définissez-y une adresse IP de gestion temporaire.**

   Si vous avez déjà configuré le nom d'utilisateur et le mot de passe pour le commutateur 1, connectez-vous avec ces informations. Sinon, connectez-vous en utilisant le nom d'utilisateur par défaut d'usine (`admin`) et son mot de passe (`admin`).

   Pour définir les paramètres IP, suivez les instructions de la Section A.6, « Réglage de l'adresse IP, du masque de réseau et de la passerelle par défaut du commutateur » à la page A-6.

9. **Téléchargez `standard1.cfg` du serveur TFTP vers Commutateur 1.**

   Pour ce faire, tapez :

```
Console#copy tftp file
TFTP server ip address:adresse IP
Choose file type :
1. config : 2.opcode : <1-2>:1
Source file name :standard1.cfg
Destination file name :standard1.cfg
Console#
```

10. **Faites de cette configuration la configuration de démarrage de commutateur 1.**

    Tapez :

```
Console#configure
Console(config)#boot system config standard1.cfg
Console(config)#exit
Console#
```

11. **Rechargez le microprogramme du commutateur.**

    Tapez :

```
Console#reload
```

A.10 Configuration de connexions groupées à des fins de résilience et de performances

Si vous avez des ports de données externes connectés au même commutateur, nous vous recommandons de les regrouper. Cela permet d'obtenir une résilience et des performances accrues.

Par exemple, si vous avez quatre connexions séparées vers le même commutateur externe et qu'une de ces connexions devient inopérante en raison d'un problème de câblage, toute communication sur la connexion rompue sera perdue. En revanche, si vous configurez un groupe incluant les quatre connexions au commutateur externe et qu'une des connexions devient inpérante, la communication reste possible sur les connexions restantes définies dans le groupe.

Tant qu'aucune connexion n'est rompue, le commutateur intégré traite toutes les connexions du groupe comme une seule connexion à large bande vers le même réseau.

Remarque - Si vous avez plusieurs connexions à un commutateur, concentrateur ou routeur externe et que vous ne les regroupez pas, la fonction Spanning Tree du commutateur intégré les bloquera toutes sauf une. Par conséquent, votre réseau continuera à bénéficier de la redondance, mais aucune des connexions en double ne sera active tant que la seule connexion non bloquée restera opérationnelle.

Dans l'exemple qui suit, un groupe est créé avec les ports NETP2, NETP3 et NETP4:

```
Console(config)#interface port-channel 1
Console(config-if)#exit
Console(config)#interface ethernet NETP2
Console(config-if)#channel-group 1
Console(config-if)#exit
Console(config)#interface ethernet NETP3
Console(config-if)#channel-group 1
Console(config-if)#exit
Console(config)#interface ethernet NETP4
Console(config-if)#channel-group 1
Console(config-if)#exit
Console(config)#
```

A.11 Utilisation du filtre de paquets sur le commutateur pour assurer une gestion sûre des serveurs Blade

Le commutateur contient un filtre de paquets qui, par défaut, bloque tout trafic allant des serveurs Blade vers le port de gestion du commutateur (NETMGT). Cela empêche de lancer d'éventuelles attaques contre votre réseau de gestion à partir d'un serveur Blade (dans le cas, par exemple, d'un hacker tentant d'accéder à un serveur Blade à partir du réseau public). Cependant, cela vous empêche aussi de communiquer directement avec les serveurs Blade au travers du port de gestion tant que vous n'avez pas configuré le filtre de paquets pour qu'il autorise le passage du trafic de gestion des serveurs Blade vers le port de gestion. Cette section explique comment remédier à la situation.

Remarque - Par défaut, le filtre de paquets n'autorise aucun trafic réseau des serveurs Blade vers le port de gestion (NETMGT). Soyez prudent lorsque vous décidez d'autoriser le passage de trafic au travers du filtre de paquets et, dans tous les cas, n'autorisez que les protocoles que vous savez nécessaires.

Les instructions qui suivent expliquent les commandes à utiliser pour autoriser les trames DHCP, BOOTP, TFTP, SUNRPC, SNMP et NFS à passer des serveurs Blade vers le port de gestion au travers du filtre de paquets. C'est l'ensemble minimum de protocoles requis pour permettre la gestion des serveurs Blade via le port de gestion :

1. **Autorisez le passage des trames DHCP et BOOTP dans le filtre de paquets.**

   A la console du commutateur, tapez :

```
Console#configure
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 67-68
```

2. **Autorisez le passage des trames TFTP dans le filtre de paquets.**

   Tapez :

```
Console#configure
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 69
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 1024-65535
0.0.0.0 0.0.0.0 1024-65535
```

3. **Autorisez le passage des trames SunRPC dans le filtre de paquets.**

   Tapez :

```
Console#configure
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 111
Console(config)#ip filter permit tcp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 111
```

4. **Autorisez le passage des trames SNMP dans le filtre de paquets.**

   Tapez :

```
Console#configure
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.00,0 69
Console(config)#ip filter permit tcp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.00,0 111
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 162
Console(config)#ip filter permit tcp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 162
```

Remarque - Notez que le port 161 est le port utilisé pour les requêtes SNMP sur une unité gérée et que le port 162 est le port des interruptions SNMP sur une unité gérée. Les interruptions SNMP proviennent de l'unité gérée. Les commandes SNMP sont émises sur une station de gestion SNMP.

5. **Autorisez le passage des trames NFS dans le filtre de paquets.**

   Tapez :

```
Console#configure
Console(config)#ip filter permit udp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 2049
Console(config)#ip filter permit tcp 0.0.0.0 0.0.0.0 0.0.0.0
0.0.0.0 2049
```

Remarque - Pour plus d'informations sur l'utilisation de la commande `ip filter permit`, référez-vous au *Manuel d'administration du châssis Sun Fire B1600 pour serveurs Blade*. Pour une liste des numéros de ports associés à des protocoles particuliers, référez-vous au fichier `/etc/services` ou au fichier `/etc/inet/services` sur un système Unix. Pour une liste complète des numéros de ports associés aux services IP, référez-vous au site web de l'Internet Assigned Numbers Authority (`http://www.iana.org`).

A.12 Configuration d'un utilisateur nommé sur le commutateur

1. **A la console du commutateur, tapez :**

```
Console#configure
```

2. **Tapez :**

```
Console(config)#username nomutilisateur access-level 15
```

où *nomutilisateur* est le nom que l'utilisateur doit fournir pour se connecter.

Le nombre `15` de la première commande signifie que le nouvel utilisateur aura accès au mode Privileged Exec. (Pour ne lui donner que l'accès au mode Normal Exec, tapez `0` au lieu de `15`.)

3. **Tapez :**

```
Console(config)#username nomutilisateur password 0 mot de passe
```

où *nomutilisateur* est le nom que l'utilisateur doit fournir pour se connecter et *mot de passe* est le mot de passe du nouvel utilisateur.

Le `0` dans cette commande signifie que la valeur tapée pour *mot de passe* n'est pas chiffrée. (Si vous tapez une valeur sous une forme chiffrée, vous devez l'indiquer en tapant `7` avant le text chiffré que vous spécifiez comme mot de passe.)

A.12.1 Noms d'utilisateurs et mots de passe par défaut du commutateur

Le nom d'utilisateur par défaut (bénéficiant d'autorisations complètes) est `admin`.
Le mot de passe correspondant est `admin`.

Le nom d'utilisateur par défaut pour un invité (aux autorisations limitées) est `guest`.
Le mot de passe correspondant est `guest`.

Le mot de passe par défaut de la commande `enable` (pour passer du statut de `guest` à un accès complet) est `super`.

A.13 Affichage d'informations sur le commutateur et sa configuration

Cette section contient les informations suivantes :

A.13.1 Vérification de l'adresse IP et de l'ID VLAN

- **Pour vérifier l'adresse IP et l'ID VLAN du port de gestion, à l'invite `Console#`, tapez :**

```
Console#show ip interface
 IP address and netmask : 129.156.223.215 255.255.255.0 on VLAN 2,
 and address mode : User specified.
```

A.13.2 Vérification de la configuration VLAN

- **Pour vérifier la configuration VLAN du commutateur, à l'invite** `Console#`**, tapez :**

```
Console#show vlan

VLAN Type    Name             Status    Ports/Channel groups
---- ------- ---------------- --------- ---------------------------------
  1  Static      DefaultVlan  Active    SNP0  SNP1  SNP2  SNP3  SNP4
                                         SNP5  SNP6  SNP7  SNP8  SNP9
                                         SNP10  SNP11  SNP12  SNP13  SNP14
                                         SNP15  NETP0  NETP1  NETP2  NETP3
                                         NETP4  NETP5  NETP6  NETP7
  2 Static           MgtVlan  Active    NETMGT
```

A.13.3 Identification des utilisateurs connectés

- **Pour savoir qui est connecté aux interfaces de ligne de commande et web, à l'invite** `Console#`**, tapez :**

```
Console#show users
Username accounts :
 Username Privilege
 -------- ---------
   admin    15
   guest     0

 Online users :
 Line        Username Idle time (h:m:s) Remote IP addr.
 ----------- -------- ----------------- ---------------
* 0  console  admin      0:00:00
```

A.13.4 Contrôle de la configuration actuelle ou de démarrage

- **Pour visualiser la configuration actuelle du commutateur, à l'invite** `Console#`**, tapez :**

```
Console#show running-config
```

Si quelqu'un a modifié les paramètres du commutateur depuis le dernier démarrage de celui-ci, la configuration courante différera de la configuration de démarrage.

- **Pour visualiser la configuration reçue par le commutateur au dernier démarrage (et qu'il recevra au prochain démarrage), à l'invite** `Console#`**, tapez :**

```
Console#show startup-config
```

A.13.5 Identification des numéros de version des microprogrammes

- **Pour connaître la l'adresse MAC ainsi que la version du microprogramme (et d'autres composants), à l'invite** `Console#`**, tapez :**

```
Console#show version

Unit1
 Serial number     :
 Service tag      :
 Hardware version    :r0b
 Number of ports    :25
 Main power status   :up
 Redundant power status :not present

Agent(master)
 Unit id        :1
 Loader version     :0.0.6.7
 Boot rom version    :1.0.0.8
 Operation code version :1.0.0.6
Console#
```

A.13.6 Affichage de l'adresse MAC et des informations générales du système

- **Pour connaître la version du microprogramme (et d'autres composants), à l'invite** `Console#`**, tapez :**

```
Console#show system

System description: Sun Fire B1600
System OID string: 1.3.6.1.4.1.42.2.24.1

System information

 System Up time: 0 days, 7 hours, 41 minutes, and 4.4 seconds
 System Name        : [NONE]
 System Location    : [NONE]
 System Contact     : [NONE]
 MAC address        : 08-00-20-7A-92-0B
 Web server         : enable
 Web server port    : 80
 Web secure server  : enable
 Web secure server port : 443

 POST result

--- Performing Power-On Self Tests (POST) ---
UART Loopback Test ..................... PASS
Timer Test ............................. PASS
DRAM Test .............................. PASS
I2C Initialization ..................... PASS
Runtime Image Check .................... PASS
PCI Device Check ....................... PASS
AN983 Initialization ................... PASS
AN983 Internal Loopback Test ........... PASS
Switch Driver Initialization ........... PASS
Switch Internal Loopback Test .......... PASS
------------------- DONE --------------------
Console#
```

ANNEXE **B**

Configuration d'une liaison série au contrôleur système avec un portable

Cette annexe explique comment connecter un ordinateur portable à un des deux modules SSC (commutateur et contrôleur système) du châssis Sun Fire B1600 pour serveurs Blade afin d'accéder à interface de ligne de commande de gestion du châssis.

Elle contient les sections suivantes:

Remarque - Avant de suivre les instructions de ce chapitre, vérifiez que vous avez installé le châssis pour serveurs Blade dans une armoire (voir *Manuel d'installation des composants du châssis Sun Fire B1600 pour serveurs Blade*).

B.1 Connexion à un portable

Remarque - N'essayez pas d'utiliser le port parallèle (25 broches) du portable au lieu de son port série. Le port série est un connecteur mâle type D à 9 broches.

1. **Connectez le câble de brassage RJ-45 vers RJ-45 (fourni avec le châssis) au port série du SSC.**
2. **Connectez l'autre extrémité du câble de brassage au connecteur RJ-45 de l'adaptateur argenté DB25 (RJ-45 Sub-D mâle/femelle 25 voies 8 POS, référence 530-2889-0x) fourni avec le Sun Fire B1600.**

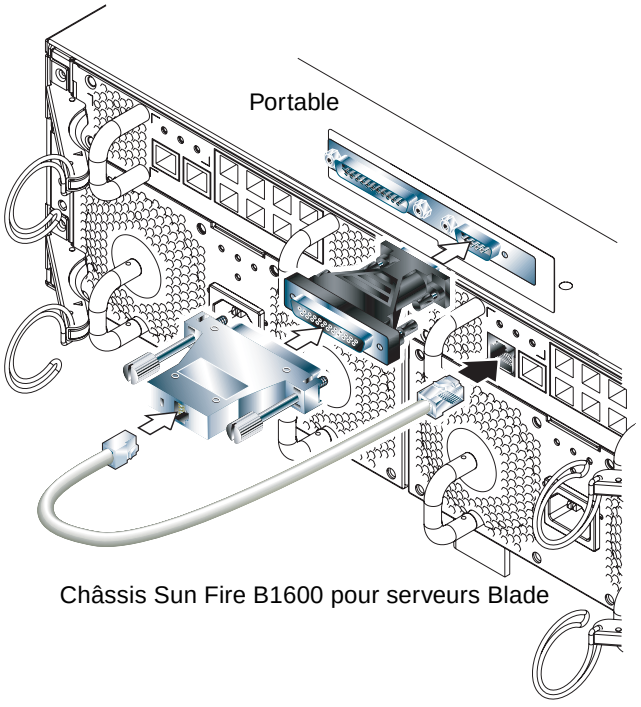

FIGURE B-1 Connexion du SSC au port série d'un portable

3. **Connectez le connecteur mâle 25 voies type D à un adaptateur équipé d'un connecteur femelle 25 voies et un connecteur femelle 9 voies type D.**

   Sun ne fournit pas d'adaptateur F/F 25x9 voies type D. Cependant, des adaptateurs de ce type sont disponibles dans les magasins d'informatique et d'électronique.
   Le brochage de l'adaptateur doit assurer les interconnexions indiqués au TABLEAU B-1.

TABLEAU B-1 Interconnexions à assurer par l'adaptateur femelle/femelle 25x9 voies type D

Connecteur femelle 9 voies	Connecteur femelle 25 voies
Broche 1	Broche 8
Broche 2	Broche 3
Broche 3	Broche 2
Broche 4	Broche 20
Broche 5	Broche 7
Broche 6	Broche 6
Broche 7	Broche 4
Broche 8	Broche 5
Broche 9	Broche 22

4. **Enfin, branchez le connecteur femelle 9 voies sur le port série du portable.**

B.1.1 Utilisation de Microsoft Windows HyperTerminal

Remarque - Si vous connectez normalement le port série de votre portable à un terminal portatif, vous devez fermer Hot Sync Manager avant de suivre les instructions de cette section. Sinon, vous ne pourrez pas utiliser le port série pour communiquer avec le châssis Sun Fire B1600 pour serveurs Blade.

Les instructions de cette section ont été vérifiées sur un PC portable sous Microsoft Windows 98 avec HyperTerminal Applet version 3.0.

1. **Exécutez l'utilitaire Windows HyperTerminal.**
2. **Dans la fenêtre de HyperTerminal, cliquez deux fois sur l'icône de Hypertrm.exe.**
3. **Dans la fenêtre Description de la connexion, spécifiez un nom pour la connexion HyperTerminal que vous allez créer sur le portable.**

   Sélectionnez ensuite une icône pour cette connexion et cliquez sur OK.

4. **Dans la fenêtre Connecter à..., cliquez sur la flèche de l'option « Se connecter en utilisant » et sélectionnez le port que vous utilisez pour votre connexion au serveur.**

   A moins d'avoir une raison particulière d'utiliser un autre port, sélectionnez DIRECT TO COM1. Cliquez sur OK.

5. **Dans la fenêtre Paramètres du port COM1, réglez les paramètres comme suit :**

   Bits par seconde : 9600
   Bits de données : 8
   Parité : Aucune
   Bits d'arrêt : 1
   Contrôle de flux : spécifiez « Xon/Xoff » ou « Aucun ».

   Remarque - Ne choisissez pas « Matériel » comme option de contrôle de flux.

   Cliquez sur OK.

6. **La session HyperTerminal est maintenant active. Dans le menu Fichier, sélectionnez Propriétés.**

7. **Dans la fenêtre Propriétés, cliquez sur l'onglet Paramètres.**

   Dans l'onglet Paramètres, cliquez sur la flèche de l'option « Emulation » et sélectionnez VT100. Pour l'option « Telnet terminal », spécifiez VT100. Cliquez sur OK.

   Remarque - Vous êtes maintenant prêt à configurer le logiciel sur le châssis Sun Fire B1600 pour serveurs Blade et sur les serveurs blades (voir chapitre 2).

ANNEXE **C**

Utilisation de DHCP pour configurer les adresses IP des serveurs Blade

Cette annexe est un complément des instructions fournies dans les manuels *Solaris Advanced Installation Guide* et *DHCP Administration Guide*. Elle vous permettra d'achever la configuration du serveur NIS et du serveur DHCP sur votre réseau de données de sorte que les serveurs Blade placés dans le châssis du système puissent recevoir des adresses IP dynamiques.

Ces instructions supposent que vous avez placé l'image de Solaris sur un serveur NIS et que vous avez un serveur DHCP sur le réseau de données.

Cette annexe comporte les sections suivantes :

C.1 Tâches du serveur NIS

- **Sur le serveur NIS, exécutez** `add_install_client` **avec l'option** `-d`**.**

  Cette commande copie un fichier `inetboot` compatible DHCP à partir de l'image de Solaris vers le répertoire `/tftpboot`. Pour exécuter la commande, tapez :

```
# cd chemin/Solaris_8/Tools
# ./add_install_client -d -s installserv:/images/2.8 -c
configsrv:/config -p configsrv:/config SUNW.Serverblade1 sun4u

To enable SUNW.Serverblade1 in the DHCP server, add an entry to
the server with the following data:

Install server      (SinstNM)  : installserv
Install server IP   (SinstIP4) : 192.168.160.12
Install server path (SinstPTH) : /images/2.8
Root server name    (SrootNM)  : installserv
Root server IP      (SrootIP4) : 192.168.160.12
Root server path    (SrootPTH) : /images/2.8/Solaris_8/Tools/Boot
Profile location    (SjumpsCF) : configsrv:/config
sysidcfg location   (SsysidCF) : configsrv:/config
```

  où *chemin* est l'emplacement de l'image de Solaris sur le serveur NIS. (Notez que la seconde commande dans l'exemple ci-dessus occupe deux lignes de texte.)
  Les données figurant dans la sortie ci-dessus sont des exemples.

C.2 Tâches du serveur DHCP

1. **Sur le serveur DHCP, créez les options que vous souhaitez transmettre aux serveurs Blade durant l'installation Jumpstart de Solaris.**

   (Ce sont les informations qui seraient recueillies du fichier `/etc/bootparams` durant une installation Jumpstart autre que celle de DHCP.)

Les options requises sont énumérées au TABLEAU C-1.

TABLEAU C-1 Options DHCP à transmettre au serveur Blade pendant l'installation Jumpstart

Nom de l'option	Description
`SrootIP4`	Adresse IP du serveur root
`SrootNM`	Nom d'hôte du serveur root
`SrootPTH`	Chemin de l'image d'amorçage (par exemple `/images/2.8/Solaris_8/Tools/Boot`)
`SinstIP4`	Adresse IP du serveur NIS
`SinstNM`	Nom d'hôte du serveur NIS
`SsysidCF`	Emplacement du fichier `sysidcfg` (par exemple, `configsrv:/config`)
`SjumpsCF`	Emplacement du profil et du répertoire `rules.ok` (par exemple, `configsrv:/config`)
`SbootFIL`	Chemin du noyau (par exemple, `/platform/sun4u/kernel/sparcv9/uni`)
`Sterm`	Type de terminal utilisé durant l'installation

Les exemples qui suivent illustrent les commandes utilisées pour créer les options indiquées au TABLEAU C-1:

```
# dhtadm -A -s SrootIP4 -d 'Vendor=SUNW.Serverblade1,2,IP,1,1'
# dhtadm -A -s SrootNM -d 'Vendor=SUNW.Serverblade1,3,ASCII,1,0'
# dhtadm -A -s SrootPTH -d 'Vendor=SUNW.Serverblade1,4,ASCII,1,0'
# dhtadm -A -s SbootFIL -d 'Vendor=SUNW.Serverblade1,7,ASCII,1,0'
# dhtadm -A -s SinstIP4 -d 'Vendor=SUNW.Serverblade1,10,IP,1,1'
# dhtadm -A -s SinstNM -d 'Vendor=SUNW.Serverblade1,11,ASCII,1,0'
# dhtadm -A -s SinstPTH -d 'Vendor=SUNW.Serverblade1,12,ASCII,1,0'
# dhtadm -A -s SsysidCF -d 'Vendor=SUNW.Serverblade1,13,ASCII,1,0'
# dhtadm -A -s SjumpsCF -d 'Vendor=SUNW.Serverblade1,14,ASCII,1,0'
# dhtadm -A -s Sterm -d 'Vendor=SUNW.Serverblade1,15,ASCII,1,0'
```

2. **Créez des macros contenant les options requises (y compris les options créées à l'étape 1).**

TABLEAU C-2 Macros à créer

Nom de la macro	Contenu de la macro (une macro peut contenir d'autres macros)
`Solaris`	`SrootIP4`, `SrootNM`, `SinstIP4`, `SinstNM`, `Sterm`, `SjumpsCF`, `SsysidCF`
`sparc`	`SrootPTH`, `SinstIP4`
`sun4u`	`Solaris`, `sparc`
`SUNW.Serverblade1`	`SbootFIL`, `sun4u`
*nom réseau**	`Subnet`, `Router`, `Broadcst` et `BootSrvA`

**nom réseau* est l'adresse IP qui identifie le réseau contenant les clients. Vous devez créer une de ces macros pour chaque sous-réseau client à l'exception du sous-réseau contenant l'interface principale du serveur DHCP.

Les exemples qui suivent illustrent les commandes utilisées pour créer les macros requises :

```
# dhtadm -A -m Solaris -d ':SrootIP4=192.168.160.12:SrootNM=
"bootsrv":SinstIP4=192.168.160.15:SinstNM="installsrv":Sterm=
"xterm":SjumpsCF="configsrv:/config":SsysidCF=
"configsrv:/config":'
# dhtadm -A -m sparc -d ':SrootPTH=
"/images/2.8/Solaris_8/Tools/Boot":SinstPTH="/images/2.8":'
# dhtadm -A -m sun4u -d ':Include=Solaris:Include=sparc:'
# dhtadm -A -m SUNW.Serverblade1 -d ':SbootFIL=
"/platform/sun4u/kernel/sparcv9/unix":Include=sun4u:'
# dhtadm -A -m 192.168.160.0 -d ':Subnet=255.255.255.0:Router=
192.168.160.254:Broadcst=192.168.160.255:BootSrvA=
192.168.160.12:'
```

3. **Ajoutez le nom d'hôte du client et son adresse IP à la base de données d'hôtes (à savoir `/etc/hosts`).**

4. **Associez la macro `SUNW.Serverblade1` au client.**

   Tapez :

```
# pntadm -A dhcpclient01 -i 01adresseMAC -m SUNW.Serverblade1 -s
serveur DHCP nom réseau
```

où :

adresseMAC est l'adresse MAC du client,

serveur DHCP est le nom d'hôte du serveur DHCP et

nom réseau est l'adresse IP qui identifie le réseau contenant le client (notez que l'exemple de commande ci-dessus occupe deux lignes de texte).

C.3 Tâches des serveurs Blade

Lorsque l'environnement de réseau est configuré de manière à fournir deux adresses IP à chacun des deux serveurs Blade, suivez les instructions fournies dans cette section. Ces instructions supposent que le serveur Blade que vous configurez a démarré à partir du réseau et a reçu une configuration IP pour son interface principale (`ce0`).

1. **A partir de l'invite `sc>` du contrôleur système, accédez à la console de serveur Blade.**

   Tapez :

   ```
   sc> console sn
   ```

   où *n* est le numéro de logement du serveur Blade à configurer.

2. **A partir de l'invite de Solaris, tapez :**

   ```
   # ifconfig ce1 plumb
   ```

3. **Enfin, tapez :**

   ```
   # ifconfig ce1 auto-dhcp up
   ```

ANNEXE **D**

Configuration de serveurs Blade Solaris à l'aide d'archives Web Start Flash

Cette annexe est un complément des instructions fournies dans le manuel *Solaris 8 Advanced Installation Guide* concernant la configuration d'un serveur NIS.

Une fois que vous avez fait démarrer le premier serveur Blade Solaris à partir du serveur NIS, vous pouvez ajouter l'application à exécuter sur le serveur Blade, puis suivre les instructions du *Solaris Advanced Installation Guide* pour créer une archive Web Start Flash.

L'utilisation d'archives Web Start Flash sur les serveurs Blade Sun Fire B100s Solaris (dans le châssis système Sun Fire B1600 pour serveurs Blade) permet de répliquer l'environnement d'exploitation et les applications d'un serveur Blade sur les autres.

Cette annexe comporte les sections suivantes :

D.1 Utilisation d'archives Web Start Flash pour accélérer la configuration des serveurs Blade

Une archive Flash est un instantané d'un système Solaris et contient donc tous les fichiers de ce système (ou, plus exactement, tous les fichiers que vous avez demandé d'y inclure). Vous devez créer l'archive Flash après l'installation de tous les logiciels sur le serveur Blade mais avant la mise en service de ce dernier. Selon les logiciels concernés et l'utilisation prévue du serveur Blade, il peut être nécessaire de créer l'archive Flash après l'installation des logiciels mais avant leur configuration. Par exemple, pour un serveur de base de données, l'archive flash Archive devrait être créée après l'installation du logiciel de gestion de bases de données, mais avant la création des bases de données.

Si vous ne savez pas encore quels logiciels vous souhaitez exécuter sur les serveurs Blade, vous pouvez quand-même utiliser la méthode des archives Web Start Flash pour répliquer Solaris sur plusieurs serveurs Blade. Ce sera plus rapide que d'effectuer des installations Jumpstart individuelles.

D.1.1 Création de l'archive Web Start Flash

Pour créer une archive Flash du logiciel se trouvant sur un serveur Blade, suivez les instructions relatives à la création d'archives Flash contenues dans le *Solaris Advanced Installation Guide*.

D.1.2 Installation de l'image d'un serveur Blade sur d'autres serveurs

Pour installer l'image archivée sur d'autres serveurs Blade, suivez les instructions relatives à l'installation d'une archive Flash contenues dans le *Solaris Advanced Installation Guide*.

D.1.3 Augmentation des performances de l'installation via une archive Web Start Flash

Vous pouvez profiter de la connexion Gigabit entre les serveurs Blade pour augmenter les performances de l'installation d'une archive Web Start Flash.

Pour ce faire, utilisez NFS afin de partager l'emplacement de l'archive Flash créée (donc partager l'image archivée du logiciel du premier serveur Blade). Suivez les instructions ci-dessous :

1. **A l'invite Solaris du serveur Blade dont vous voulez répliquer l'image, tapez :**

```
#share -F ufs emplacement flash
```

où *emplacement flash* est l'emplacement de l'archive Flash du serveur Blade. Par exemple :

```
#share -F ufs /var/tmp
```

2. **Sur le serveur NIS, modifiez le profil d'installation de sorte qu'il pointe vers l'emplacement de l'archive Flash sur le premier serveur Blade.**

ANNEXE **E**

Commandes du contrôleur système

Cette annexe énumère les commandes disponibles à partir de l'invite `sc>` du contrôleur système.

Elle contient les sections suivantes :

E.1 Commandes d'alimentation de l'ensemble du châssis

Remarque - Vous pouvez mettre hors tension (ou ramener à un état « prêt au retrait » ou de veille) tous les composants à la fois à l'exception du contrôleur système actif. Le châssis pour serveurs Blade est conçu de manière à empêcher la mise hors tension ou la mise en veille du contrôleur système actif en une seule commande. Pour des informations sur la mise en veille du contrôleur système actif, référez-vous au *Manuel d'administration du châssis Sun Fire B1600 pour serveurs Blade*.

TABLEAU E-1 Commandes de mise sous/hors tension ou de mise en veille de tous les composants

Commande et option (éventuelle)	Effet de la commande
`sc> poweron ch`	Met tous les composants sous tension. Utilisez cette commande pour remettre tous les composants à la fois sous tension après un état d'attente, de préparation au retrait ou de veille.
`sc> poweroff ch`	Met hors tension tous les composants du châssis à l'exception du contrôleur système actif.
`sc> poweroff -f ch`	Met hors tension tous les composants (à l'exception du contrôleur système actif) même si un arrêt ordonné du système d'exploitation a échoué sur un composant.
`sc> poweroff -y ch`	Met hors tension tous les composants (à l'exception du contrôleur système actif) sans afficher la demande de confirmation.
`sc> poweroff -s ch`	Met à l'état de veille tous les composants (à l'exception du contrôleur système actif) (équivaut à la commande `standbyfru ch`).
`sc> poweroff -r ch`	Met tous les composants (à l'exception du contrôleur système actif) dans un état permettant leur retrait en sécurité. L'option `-r` active également le témoin « prêt au retrait » de chaque composant (équivaut à la commande `removefru ch`).
`sc> standbyfru ch`	Met tous les composants (à l'exception du contrôleur système actif) à l'état de veille (équivaut à la commande `poweroff -s ch`).

TABLEAU E-1 Commandes de mise sous/hors tension ou de mise en veille de tous les composants

Commande et option (éventuelle)	Effet de la commande
`sc> standbyfru -f ch`	Met à l'état de veille tous les composants (à l'exception du contrôleur système actif) même si un arrêt ordonné du système d'exploitation a échoué sur un composant.
`sc> standbyfru -y ch`	Met tous les composants (à l'exception du contrôleur système actif) à l'état de veille sans afficher la demande de confirmation.
`sc> removefru ch`	Met tous les composants (à l'exception du contrôleur système actif) dans un état permettant leur retrait en sécurité ; cette commande active également le témoin « prêt au retrait » de chaque composant (équivaut à la commande `poweroff -r ch`).
`sc> removefru -f ch`	Met tous les composants (à l'exception du contrôleur système actif) dans un état permettant leur retrait en sécurité, même si un arrêt ordonné du système d'exploitation a échoué sur le contrôleur système. Cette commande active également le témoin « prêt au retrait » de chaque composant.
`sc> removefru -y ch`	Met tous les composants (à l'exception du contrôleur système actif) dans un état permettant leur retrait en sécurité, mais sans afficher préalablement la demande de confirmation. Cette commande active également le témoin « prêt au retrait » de chaque composant.

E.2 Commandes d'alimentation pour les contrôleurs système

Remarque - Vous ne pouvez mettre hors tension ou à l'état de veille que le contrôleur système de secours. Pour des informations sur la mise en veille du contrôleur système actif, référez-vous au *Manuel d'administration du châssis Sun Fire B1600 pour serveurs Blade*.

TABLEAU E-2 Commandes de mise sous/hors tension ou de mise en veille d'un SSC

Commande et option (éventuelle)	Effet de la commande
`sc> poweron sscn`	Met sous tension le SSC *n* (où *n* désigne le SSC de secours et vaut 0 ou 1 selon que le contrôleur système de secours est en SSC0 ou SSC1). Utilisez cette commande pour remettre le SSC de secours sous tension après un état d'attente, de préparation au retrait ou de veille.
`sc> poweroff sscn`	Met hors tension le SSC *n* (où *n* vaut 0 ou 1 selon que le contrôleur système de secours est en SSC0 ou SSC1).
`sc> poweroff -f sscn`	Met hors tension le contrôleur système de secours (SSC0 ou SSC1) même si un arrêt ordonné du système d'exploitation a échoué pour le contrôleur système.
`sc> poweroff -y sscn`	Met hors tension le contrôleur système de secours (SSC0 ou SSC1) sans afficher la demande de confirmation.
`sc> poweroff -s sscn`	Met le contrôleur système de secours (SSC0 ou SSC1) à l'état de veille (équivaut à la commande `standbyfru`).
`sc> poweroff -r sscn`	Met le contrôleur système de secours dans un état permettant son retrait en sécurité ; l'option `-r` allume également le témoin « prêt au retrait » (équivaut à la commande `removefru`).
`sc> standbyfru sscn`	Met le contrôleur système de secours à l'état de veille (équivaut à la commande `poweroff -s`).
`sc> standbyfru -f sscn`	Met le contrôleur système de secours à l'état de veille, même si un arrêt ordonné de son système d'exploitation a échoué.

TABLEAU E-2 Commandes de mise sous/hors tension ou de mise en veille d'un SSC

Commande et option (éventuelle)	Effet de la commande
`sc> standbyfru -y sscn`	Met le contrôleur système de secours à l'état de veille sans afficher la demande de confirmation.
`sc> removefru sscn`	Met le contrôleur système de secours dans un état permettant son retrait en sécurité ; cette commande allume également le témoin « prêt au retrait » sur le panneau arrière du SCC (équivaut à la commande `poweroff -r`).
`sc> removefru -f sscn`	Met le contrôleur système de secours dans un état permettant son retrait en sécurité, même si un arrêt ordonné de son système d'exploitation a échoué. Cette commande allume également le témoin « prêt au retrait » sur le panneau arrière du SSC.
`sc> removefru -y sscn`	Met le contrôleur système de secours dans un état permettant son retrait en sécurité, mais sans afficher préalablement la demande de confirmation. Cette commande allume également le témoin « prêt au retrait » sur le panneau arrière du SSC.

E.3 Commandes d'alimentation des serveurs Blade

TABLEAU E-3 Commandes de mise sous/hors tension ou de mise en veille d'un serveur Blade

Commande et option (éventuelle)	Effet de la commande
`sc> poweron s`*n*	Met sous tension le serveur Blade dans le logement *n*. Utilisez cette commande pour remettre le serveur Blade sous tension après un état d'attente, de préparation au retrait ou de veille.
`sc> poweroff s`*n*	Met hors tension le serveur Blade dans le logement *n*.
`sc> poweroff -f s`*n*	Met hors tension le serveur Blade dans le logement *n*, même si un arrêt ordonné du système d'exploitation a échoué pour le contrôleur système.
`sc> poweroff -y s`*n*	Met hors tension le serveur Blade dans le logement *n* sans afficher la demande de confirmation.
`sc> poweroff -s s`*n*	Met le serveur Blade du logement *n*à l'état de veille (équivaut à la commande `standbyfru`).
`sc> poweroff -r s`*n*	Met le serveur Blade du logement *n* dans un état permettant son retrait en sécurité ; l'option `-r` allume également le témoin bleu « prêt au retrait » à l'avant du serveur Blade (équivaut à la commande `removefru`).
`sc> standbyfru s`*n*	Met le serveur Blade du logement *n*à l'état de veille (équivaut à la commande `poweroff -s`).
`sc> standbyfru -f s`*n*	Met le serveur Blade du logement *n* à l'état de veille, même si un arrêt ordonné du système d'exploitation du serveur a échoué.
`sc> standbyfru -y s`*n*	Met le serveur Blade du logement *n* à l'état de veille sans afficher la demande de confirmation.

TABLEAU E-3 Commandes de mise sous/hors tension ou de mise en veille d'un serveur Blade

Commande et option (éventuelle)	Effet de la commande
`sc> removefru s`*n*	Met le serveur Blade du logement *n* dans un état permettant son retrait en sécurité ; cette commande allume également le témoin bleu « prêt au retrait » à l'avant du serveur Blade (équivaut à la commande `poweroff -r`).
`sc> removefru -f s`*n*	Met le serveur Blade du logement *n* dans un état permettant son retrait en sécurité. Cette commande effectue une mise en veille du serveur Blade même si un arrêt ordonné de son système d'exploitation a échoué. Cette commande allume également le témoin bleu « prêt au retrait » à l'avant du serveur Blade.
`sc> removefru -y s`*n*	Met le serveur Blade du logement *n* dans un état permettant son retrait en sécurité, mais sans afficher préalablement la demande de confirmation. Cette commande allume également le témoin bleu « prêt au retrait » à l'avant du serveur Blade.

E.4 Commandes de réinitialisation des contrôleurs système, commutateurs et serveurs Blade

TABLEAU E-4 Commandes de réinitialisation des composants du châssis

Commande et option (éventuelle)	Effet de la commande
`sc> reset s`*n*	Réinitialise le serveur Blade dans le logement *n*.
`sc> reset s`*n sy*	Réinitialise les serveurs Blade dans les logements *n* et *y*. (Enumérez les serveurs Blade à réinitialiser en les séparant par des espaces.)
`sc> reset -y s`*n*	Réinitialise le serveur Blade dans le logement *n* sans afficher la demande de confirmation.
`sc> reset -x s`*n*	Exécute une réinitialisation externe du serveur Blade dans le logement *n*.
`sc> reset ssc`*n*`/swt`	Réinitialise le commutateur en SSC*n* (où *n* vaut 0 ou 1).
`sc> reset -y ssc`*n*`/swt`	Réinitialise le commutateur en SSC*n* sans afficher la demande de confirmation.
`sc> reset -x ssc`*n*`/swt`	Exécute une réinitialisation externe du commutateur en SSC*n*.
`sc> reset ssc`*n*`/sc`	Réinitialise le contrôleur système de secours (où *nn* vaut 0 ou 1 selon que le contrôleur système de secours est en SSC0 ou SSC1).
`sc> reset -f ssc`*n*`/sc`	Force la réinitialisation du contrôleur système de secours même s'il n'est pas possible d'arrêter proprement son système d'exploitation (où *n* vaut 0 ou 1 selon que le contrôleur système de secours est en SSC0 ou SSC1). Lorsque vous exécutez cette commande, vous provoquez également la réinitialisation du commutateur se trouvant dans le même module SSC.
`sc> resetsc`	Réinitialise le contrôleur système actif. Aucun des commutateurs n'est affecté par cette réinitialisation. Vous perdez votre session utilisateur si vous réinitialisez le contrôleur système avec cette commande.

TABLEAU E-4 Commandes de réinitialisation des composants du châssis

Commande et option (éventuelle)	Effet de la commande
`sc> reset sscn`	Réinitialise le contrôleur système de secours (*n* ne peut pas être le contrôleur système actif), les deux commutateurs et tous les serveurs Blade installés dans le châssis.
`sc> resetsc -y`	Réinitialise le contrôleur système actif sans afficher la demande de confirmation.
`sc> break sn`	Si Solaris est en cours d'exécution (et est configuré pour traiter les interruptions de cette manière), la commande `break` fait passer un serveur Blade Solaris de Solaris à kadb ou OBP, selon le mode dans lequel Solaris a démarré.
`sc> break -y sn`	Comme ci-dessus, mais l'option -y signifie que vous n'êtes pas invité à confirmer la commande `break` que vous avez lancée.
`sc> break sn sy sx`	Comme ci-dessus, mais cette commande applique l'interruption aux serveurs Blade *n*, *y* et *x*.

E.5 Commandes de surveillance

TABLEAU E-5 Commandes de surveillance du châssis et de ses composants

Commande et option (éventuelle)	Effet de la commande
`showsc [-v]`	Affiche une synthèse de la configuration du contrôleur système actif.
`showplatform [-v]`	Affiche l'état (Ok, Faulty, Not Present) de chaque composant. Cette commande affiche également l'état du système d'exploitation dans tous les domaines du châssis (contrôleurs système, commutateurs et serveurs Blade). Si vous utilisez l'option -v, elle indique également l'adresse MAC principale et le numéro de série des composants.
`showenvironment [-v] {[ssc`*n*`][ps`*n*`][s`*n*`]}`	Affiche l'état des capteurs d'environnement dans les différents composants du châssis. Par exemple, cette commande indique les températures internes des composants, la vitesse des ventilateurs et le niveau de courant sur les rails d'alimentation.
`showfru [-g] {ssc`*n*`|s`*n*`|ch|ps`*n*`}`	Affiche le contenu de la base de données FRUID d'un (ou de tous les) composant(s). Chaque composant tient à jour des informations détaillées le concernant. Ces informations comprennent des données statiques (par exemple, version du matériel) et dynamiques (par exemple, messages d'événement récents générés par le composant). L'option `-g` permet de spécifier le nombre de lignes de sortie à visualiser avant de suspendre l'affichage.
`showdate`	Affiche la date et l'heure actuelles (au format UTC) selon le contrôleur système.
`showlogs [-b]|[-e] [-g] [-v] {ssc`*n*`|s`*n*`}`	Affiche les événements qui ont été consignés pour un serveur Blade, commutateur ou contrôleur système spécifique. Spécifiez `-b` pour afficher les *n* premiers événements, `-e` pour voir les *n* derniers événements, `-g` pour spécifier le nombre de lignes de sortie à visualiser avant une pause dans l'affichage et `-v` pour voir tous les événements contenus dans le journal.
`showlocator`	Indique si le témoin de localisation est allumé ou éteint.

TABLEAU E-5 Commandes de surveillance du châssis et de ses composants

Commande et option (éventuelle)	Effet de la commande
`consolehistory [-b]|[-e] [-g] [boot|run] sscn/swt|sn`	Affiche le contenu du tampon de démarrage ou d'exécution de la console du commutateur ou du serveur Blade. Spécifiez `-b` pour afficher les *n* premières lignes d'information, `-e` pour voir les *n* dernières lignes et `-g` pour spécifier le nombre de lignes de sortie à visualiser avant une pause dans l'affichage.
`showusers`	Affiche les utilisateurs actuellement connectés au contrôleur système.
`usershow [`*nomutilisateur*`]`	Affiche les détails du compte de l'utilisateur spécifié. Si aucun utilisateur n'est spécifié, la commande affiche les détails de tous les comptes utilisateur. La sortie indique les autorisations des utilisateurs et si un mot de passe leur est affecté ou pas.

E.6 Commandes de configuration du contrôleur système

TABLEAU E-6 Commandes de configuration du contrôleur système

Commande et option (éventuelle)	Effet de la commande
`setupsc`	Permet de configurer interactivement le contrôleur système actif. (Aucune méthode non interactive n'est disponible.) Le contrôleur système de secours utilise automatiquement la même configuration que le contrôleur actif.
`flashupdate -s` *adresse IP* `-f` *chemin* `[-v] ssc`*n*`|s`*n*	Permet de mettre à niveau le microprogramme d'un contrôleur système ou serveur Blade. *adresse IP* est l'adresse IP du serveur TFTP sur lequel est stocké le microprogramme. *Chemin* est l'emplacement du microprogramme sure le serveur TFTP. L'option `-v` affiche des informations sur la mise à niveau pendant celle-ci.
`setfailover`	Indique quel contrôleur système est actif et lequel est le contrôleur système de secours. La commande vous demande également de confirmer que vous souhaitez forcer le contrôleur système de secours actuel à prendre le rôle de contrôleur actif. Si vous utilisez la commande uniquement pour savoir quel contrôleur système est actif, répondez simplement non (n).
`setdefaults [-y]`	Rétablit les paramètres par défaut d'usine du contrôleur système actif (mais pas de son commutateur). L'option -y demande au SSC de rétablir ses paramètres par défaut d'usine sans demander de confirmation.
`setdate [`*mmjj*`]`*HHMM*`[.`*SS*`]|` *mmjjHHMM*`[`*cc*`]`*aa*`[.`*SS*`]`	Permet de définir l'heure sur le contrôleur système, les commutateurs et les serveurs Blade actuellement installés. Lorsque vous réglez la date et l'heure, vous devez utiliser le temps universel coordonné (UTC). Les serveurs Blade Solaris déterminent l'heure locale de votre fuseau horaire par décalage par rapport au temps universel coordonné (UTC). Les serveurs Blade reçoivent cette heure UTC du contrôleur système. Les variables sont les suivantes : *mm* est le mois (deux chiffres) *jj* est le jour (deux chiffres) *HH* est l'heure (deux chiffres) *MM* sont les minutes (deux chiffres) *SS* sont les secondes (deux chiffres)
`setlocator on|off`	Active et désactive le témoin de localisation du châssis.

E.7 Commandes liées aux commutateurs et aux serveurs Blade

Remarque - Lorsque vous êtes à la console d'un commutateur ou d'un serveur Blade, tapez **#.** pour retourner à l'invite `sc>` du contrôleur système actif.

TABLEAU E-7 Commandes d'accès et de configuration des commutateurs et serveurs Blade

Commande et option (éventuelle)	Effet de la commande
`console [-f]|[[-r] ssc`*n*`/swt|s`*n*	Permet d'accéder à la console d'un commutateur ou d'un serveur Blade. Utilisez la commande `-f` pour faire passer de force au mode « lecture seule » tout autre utilisateur actuellement connecté. Utilisez la commande `-r` pour vous connecter vous-même en mode « lecture seule ».
`consolehistory [-b]|[-e] [-g] [boot|run] ssc`*n*`/sc|ssc`*n*`/swt|s`*n*	Affiche le contenu du tampon de démarrage ou d'exécution de la console du contrôleur système, commutateur ou serveur Blade spécifié. Spécifiez `-b` pour afficher les *n* premières lignes d'information, `-e` pour voir les *n* dernières lignes et `-g` pour spécifier le nombre de lignes de sortie à visualiser avant une pause dans l'affichage.
`bootmode reset_nvram|diag|skip_diag| normal|bootscript="string" s`*n* `{s`*n*`}`	Cette commande permet de spécifiez le mode de démarrage d'un serveur Blade. Pour plus d'informations, référez-vous au *Manuel d'administration du châssis Sun Fire B1600 pour serveurs Blade*.
`flashupdate -s` *IP adresse* `-f` *chemin* `[-v] ssc`*n*`|s`*n*	Permet de mettre à niveau le microprogramme du contrôleur système actif ou d'un serveur Blade. *adresse IP* est l'adresse IP du serveur TFTP sur lequel est stocké le microprogramme. *chemin* est l'emplacement du microprogramme sure le serveur TFTP. L'option `-v` affiche des informations sur la mise à niveau pendant celle-ci.

E.8 Commandes d'administration des comptes utilisateurs

TABLEAU E-8 Commandes d'administration des comptes utilisateurs

Commande et option (éventuelle)	Effet de la commande
`useradd` *nomutilisateur*	Ajoute un utilisateur nommé à la liste des utilisateurs autorisés du contrôleur système.
`userdel` *nomutilisateur*	Supprime un utilisateur de la liste des utilisateurs autorisés du contrôleur système.
`userpassword` *nomutilisateur*	Cette commande permet à un utilisateur ayant des autorisations de niveau `a` de modifier le mot de passe d'un autre utilisateur.
`password`	Cette commande permet à un utilisateur de modifier son propre mot de passe (autrement dit, de modifier le mot de passe de l'utilisateur sous le nom duquel il est actuellement connecté).
`userperm` *nomutilisateur* [a][u][c][r]	Cette commande spécifie les niveaux de permission de l'utilisateur nommé. `c` donne un accès console aux serveurs Blade et commutateurs : `a` octroie des privilèges d'administration (permettant à l'utilisateur nommé de modifier la configuration du contrôleur système), `u` octroie des privilèges d'administration utilisateur (permettant à l'utilisateur nommé d'administrer les comptes utilisateurs) et `r` octroie des permissions de réinitialisation (permettant à l'utilisateur nommé de réinitialiser des composants du châssis ou de les mettre sous/hors tension).
`usershow` [*nomutilisateur*]	Affiche les détails du compte de l'utilisateur spécifié. Si aucun utilisateur n'est spécifié, la commande affiche les détails de tous les comptes utilisateur. La sortie indique les autorisations des utilisateurs et si un mot de passe leur est affecté ou pas.
`showusers`	Affiche les utilisateurs actuellement connectés au contrôleur système.

ANNEXE **F**

Les contrôleurs système actif et de secours

Cette annexe fournit des informations détaillées sur la relation entre les contrôleurs système actif et de secours du châssis. Il décrit également les limitations de cette relation.

F.1 Evénements entraînant un basculement

Le châssis pour serveurs Blade contient deux contrôleurs système. Un seul de ces contrôleurs est actif à la fois ; un seul est donc accessible via l'interface de ligne de commande ALOM. Cependant, même si l'autre contrôleur système est au repos (en mode d'attente), le commutateur y associé reste actif et le contrôleur système de secours peut reprendre le rôle de contrôleur actif dans les cas suivants :

- retrait du contrôleur système actuellement actif,
- défaillance majeure de l'application du contrôleur système sur le contrôleur système actif ou erreur fatale du matériel,
- exécution de la commande `setfailover` par l'utilisateur afin de forcer l'interversion des rôles des contrôleurs système.

F.2 Activités du contrôleur système de secours

Le contrôleur système de secours remplit les fonctions suivantes alors que son application principale est en mode de repos :

- Il surveille la santé du contrôleur système actif et en reprend le rôle si celui-ci est physiquement retiré, si son application principale subit une défaillance majeure, si une erreur fatale de matériel se produit ou en réponse à une commande `setfailover` émise sur le contrôleur système actif.
- Il reçoit les paramètres de configuration que l'utilisateur fournit sur le contrôleur système actif dans le cadre de la commande `setupsc`. Cela lui permet de reprendre le rôle de contrôleur actif en toute transparence.
- Il reçoit tous les messages d'événement, tenant à jour les journaux d'événements sur le contrôleur système de secours.
- Il permet un accès console, à partir du contrôleur système actif, au commutateur contenu dans le module SSC où se trouve le contrôleur système de secours. Remarque : si le démarrage du contrôleur système de secours est interrompu pour une raison quelconque, le contrôleur système de secours ne peut pas assurer l'accès console au commutateur qui lui est associé.

- Il aide à maintenir l'intégrité des données de connexion utilisateur et d'ID hôte pour l'ensemble du châssis. (L'ID hôte est requis pour les serveurs Blade ; les données de connexion utilisateur sont requises pour les contrôleurs système.) Ces deux ensembles d'informations sont stockés principalement sur le panneau central. Cependant, les deux contrôleurs système sont impliqués dans leur préservation.

  Au cas où un nouveau SSC (dans son état par défaut d'usine) est introduit dans un châssis déjà utilisé, le nouveau SSC hérite simplement des données de connexion utilisateur et d'ID hôte actuellement stockées sur le panneau central.

  Dans la situation inverse, lorsque le châssis est nouveau (et ses données de connexion utilisateur et d'ID hôte ne sont donc pas configurées) mais que le SSC a déjà été utilisé, le panneau central obtient les données de connexion utilisateur et d'ID hôte du contrôleur système.

  Cependant, si un SSC est introduit dans le châssis alors que tous deux contiennent déjà des données de connexion utilisateur et d'ID hôte mais que celles-ci diffèrent entre le SSC et le châssis, le résultat est plus compliqué à prédire. Dans ce case, le contrôleur système de secours, s'il est disponible, joue un rôle d'arbitrage. Il compare ses propres données de connexion utilisateur et d'ID hôte avec celles du SSC contenant le contrôleur système actif et celles du panneau central. Si ses propres données d'ID hôte correspondent à celles du SSC actif ou du panneau central, ces informations prévalent. De même, si ses propres données de connexion utilisateur correspondent à celles du SSC actif ou du panneau central, ces informations prévalent. Pour chaque série d'informations, si le contrôleur système de secours découvre que ses propres données diffèrent à la fois de celles du SSC actif et de celles du panneau central, les données stockées dans le panneau central prévalent.

F.3 Limitations de la relation de basculement entre les deux contrôleurs système

Il n'y a pas d'impact sur l'exécution des serveurs Blade ni des commutateurs durant le basculement. Toutefois, vous devez savoir que :

- Lorsque les contrôleurs système échangent leurs rôles, le châssis est temporairement sans contrôleur système actif (pendant une quinzaine de secondes). (Le basculement exige en effet une réinitialisation des deux contrôleurs système.) Par conséquent, aucun journal console ne sera collecté pendant le basculement et, lorsque vous vous connecterez au nouveau contrôleur système actif, tous les journaux d'événements des deux contrôleurs système seront vides.

  Pendant le basculement, aucune gestion utilisateur des composants du châssis n'est possible via les contrôleurs système. En revanche, il est toujours possible de se connecter aux commutateurs ou aux serveurs Blade via telnet et d'utiliser l'interface utilisateur graphique basée sur le web du commutateur.

  Enfin, pendant le basculement, il n'est pas possible d'effectuer des mises à niveaux du microprogramme sur les composants du châssis. Par conséquent, pour mettre à niveau le microprogramme d'un contrôleur système, vous devez faire de ce contrôleur système le contrôleur actif (avec la commande `setfailover` à l'invite `sc>` du contrôleur système actuellement actif).
- Aucun accès au contrôleur système de secours n'est autorisé via telnet. Utilisez l'alias d'adresse IP à la place. Cependant, vous devez savoir que les connexions telnet sont perdues en cas de basculement d'un contrôleur système vers un autre.

Index

D

E

F

H

I

L

V

W